Solutions for PV Cyber Risks to Grid Stability

solarpowereurope.org

SolarPower Europe

Knowledge partner:

DNV

BECOME A MEMBER OF SOLARPOWER EUROPE

SolarPower Europe is the leading European solar association. Join our solar community today to unlock a world of shining benefits for your organisation.

Industry Influence
Help us shape the solar policy framework in Europe, by joining forces with industry leaders.

Networking Opportunities
Connect with 300+ members from across the entire solar value chain. Join exclusive networking opportunities at our events.

Expert Knowledge
Get access to the latest solar best practices, comprehensive market intelligence, weekly policy update, quarterly market updates webinars and knowledge exchange within our workstreams.

Visibility and Promotion
Be visible in front of an engaged solar audience of 34K+ monthly unique visitors on our website, 95K+ followers on social media, 28,5K+ newsletter subscribers, and more.

Amazing Discounts
Get exclusive member discounts for SolarPower Europe and partner events, advertising on partner media outlets, sponsorship opportunities and more.

Join SolarPower Europe today

www.solarpowereurope.org/membership

SolarPower Europe

Contents

SolarPower Europe Report

Developed by:
Ryan Davidson, Matthias Müller-Mienack, Kai Kamphöfener, Klaus Kursawe, Al-Karim Govindji, Paul Raats, Lauri Salonen, DNV

Commissioned by SolarPower Europe:
Project manager: Jan Osenberg, SolarPower Europe
Overseen by Walburga Hemetsberger, Dries Acke, SolarPower Europe

Please cite as:
SolarPower Europe (2025): *Solutions for PV Cyber Risks to Grid Stability*

Date of publication: April 2025

Contact: info@solarpowereurope.org.

For media use and queries: Bethany Meban, SolarPower Europe, b.meban@solarpoweurope.org.

Design: Onehemisphere AB, Sweden. contact@onehemisphere.se

Cover image: © Shutterstock

Executive Summary

Cyber attacks from criminals and nation-state attackers on power grid infrastructure are increasing. This necessitates enhanced security and resilience in energy infrastructure. By embracing distributed generation, particularly from renewable sources like solar, Europe significantly reduces dependence on single, high-impact targets and increases power grid resilience. This move to a more diversified and resilient energy infrastructure is echoed in the EU Energy Security Strategy and more recent RePower EU plan, which rightfully describes renewables as playing a critical role in providing greater European energy independence and lessening reliance on foreign energy sources.[1]

In response, the cybersecurity landscape for the energy sector is undergoing a significant transformation, driven by the recent expansion of regulatory frameworks such as the Network and Information Security Directive (NIS2), the Network Code on Cyber Security (NCCS) and others. These efforts are, however, focused on traditional energy infrastructure such as large, centralised power plants and, therefore, do not adequately address all specific security needs of distributed energy sources (DER), such as comparably small rooftop solar installations. The Cyber Resiliency Act (CRA) will apply to solar equipment as it covers all digital devices sold in Europe. However, even the CRA is limited in addressing the full end-to-end infrastructure.

These unique aspects of grid-relevant devices like rooftop solar and other DER are not adequately addressed by existing regulations:

- Current regulations place security responsibilities on the operator, who is expected to enforce supply chain security for its service and component providers. However, many PV systems are too small to be classified as critical infrastructure and are not managed by professional operators like utilities.

- Such rooftop PV systems and other DER are often "operated" by homeowners or small businesses. Installers, aggregators, and manufacturers increasingly have remote access, for example, to enable flexibility services, but they're currently not subject to the typical requirements for operators of critical infrastructure.

- Most rooftop solar, from a communications and cybersecurity perspective, resembles Internet of Things (IoT) devices rather than centralised energy infrastructure. Therefore, many traditional industrial security controls and network architectures are not applicable. The EU needs tailored approaches.

Although there have been multiple attacks in the solar industry, they do not compare to those seen in other parts of the energy sector, such as attacks on utilities or grid operators. There, industrial espionage, ransomware, and attacks leading to public grid blackouts have occurred with increasing frequency over the past decade. However, solar's role in the EU's generation mix is rapidly increasing. It is expected that cyberattacks will increase as a consequence. Many stakeholders within the industry recognise the impact they have on public infrastructure and consider cybersecurity a priority. Manufacturers, service providers, etc. have made significant progress in improving not just the security of their installed PV infrastructure, but also their own IT systems and promote a healthy cyber culture. However, without proper regulation, the cyber maturity of the industry will remain heterogeneous. A baseline for cybersecurity is therefore critical to ensure gaps in the security of this infrastructure are identified and adequately addressed.

As a first step in identifying these threats within the industry, an industry cyber risk assessment was performed for this report. The types of risks are divided into three categories: (i) device-level security; (ii) risks arising from the compromise of an industry stakeholder; (iii) and the intentional misuse of installed capacity by a nation-state threat actor with the cooperation of the vendor. These threats were then quantified through market and grid analysis. The risks, when accounting for future security controls under existing regulations, are above acceptable limits for all PV installations that export electricity to the grid. Power system simulations suggest that a targeted compromise of 3 GW can have significant implications for Europe's power grid. Over a dozen Western and non-Western manufacturers control significantly more than 3 GW of installed inverter capacity. Other critical actors are large PV asset operators, installers, and selected third-party service providers.

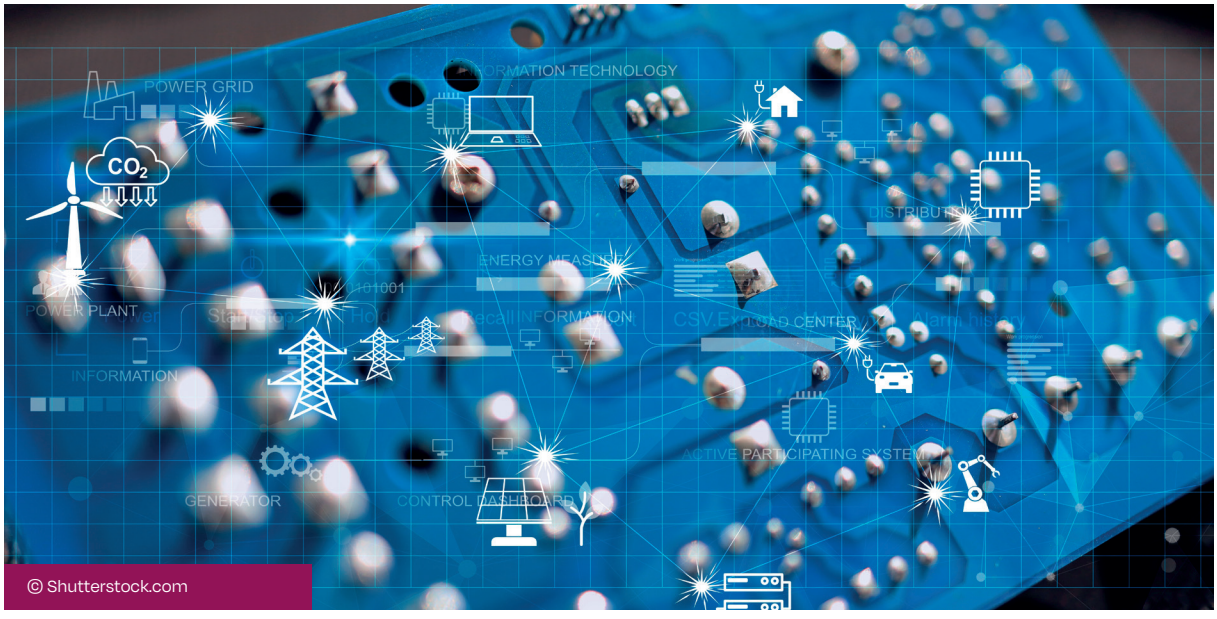
To address these risks and provide the baseline for cybersecurity for a more homogenous maturity across the industry, a framework is presented in Section 8 of the report. The framework follows generally accepted cybersecurity practices. They include prevention of cyberattacks, methods for early detection, response, and recovery from an attack. Prevention includes measures to secure and protect the installed infrastructure as well as measures to improve the security of the organisations that manage and have remote access to this infrastructure. Recommendations for monitoring and recovery include measures that can be implemented in the infrastructure that supports future monitoring and recovery efforts. Recovery includes both measures that facilitate the recovery of the PV itself as well as the recovery of the grid from a black-start scenario.

Policy makers should take action to address cybersecurity gaps in grid-relevant devices. This includes, for example, the aggregation of distributed energy resources, remote access capabilities of inverter manufacturers, and other relevant service providers. Solutions exist and are used in other industries. Together, they can substantially mitigate solar-related cybersecurity risks to grid stability. The two main mitigation measures are:

- **Develop industry-specific guidelines for securing PV infrastructure.** While many standards exist for cybersecurity, such as ISO 27001 or IEC 62443, they are not industry-specific. Some efforts, such as IEEE 1547.3 include industry-specific guidance. However, more work is needed to provide additional details for the implementation of secure PV infrastructure from end-to-end. This should build on relevant European certification processes. This includes not just the inverters but also the cloud and communication infrastructure used for the monitoring and management. Details are provided in chapter 7.2.1.

- **Limit remote access and data storage from outside of the European Union, mirroring steps taken by other countries.** The EU should prevent remote control of aggregated energy devices above critical thresholds by stakeholders outside the EU's jurisdiction unless they are based in other secure jurisdictions with strong enforcement.[a] These limitations should cover direct controls and delayed control through firmware and software updates. The Commission should implement this via the Network Code for Cybersecurity (NCCS), as detailed below, or define a fast-track procedure. High-risk entities may then develop solutions, subject to approval by the competent authorities, to adequately manage the cyber risk. A similar approach is explored in Lithuania, where high-risk entities are asked to rely on third-party providers for remote maintenance and updates. Details are provided in the chapters 7.2.1 and 7.1.1.

The European Commission should enforce these security requirements for PV infrastructure via the NCCS to accelerate implementation. All actors with remote-control capabilities above critical thresholds must adopt appropriate security measures. The Commission should convene stakeholders to define a clear implementation path. One approach could be establishing a product whitelist for grid connection with an appropriate certification process in place. Policy makers could enforce this for grid-exporting devices through NCCS supply chain controls. Another option is linking security requirements to national requirements for devices that export electricity to the grid. Details are provided in the chapter 7.2.2.



© Shutterstock.com

a The European Commission within the context of Regulation 2016/679 (GDPR) is already listing third countries outside the EEA (EU, Norway, Liechtenstein and Iceland) that can provide an adequate level of security and are thus to be considered as a secure jurisdiction. Those countries are Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland , the United Kingdom, the United States and Uruguay.

01

© Shutterstock.com

Introduction and Problem Statement

1.1 Introduction

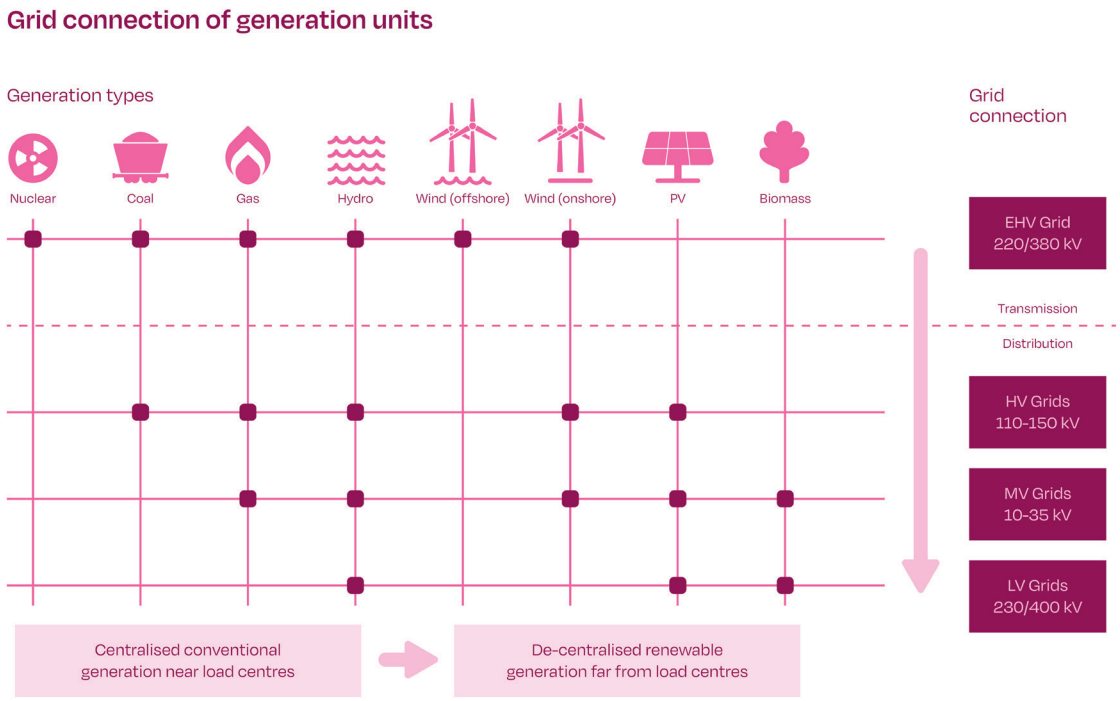
This report aims to develop technical and non-technical recommendations to mitigate residual cyber and energy security risks for inverters. The cyber risks and their associated mitigations in the solar industry vary greatly from those in traditional energy infrastructure. From a cybersecurity perspective, inverters often function more as IoT devices than traditional power plants. They are accessed and controlled by multiple actors—including OEMs, installers, and demand response providers—via cloud systems, exposing them to vulnerabilities not well mitigated under existing regulatory frameworks. This report enumerates these industry-specific risks, determines the residual risk after the application of existing and developing regulatory actions, and finally provides recommendations to address the remaining unmitigated risks.

1.2 Situation

The European power grid is undergoing a profound transformation driven by the adoption of renewable energy sources, particularly solar and wind power. The generation mix is shifting from centralized fossil fuel-based power plants to a decentralized model characterized by Distributed Energy Resources (DERs), as shown in Figure 1. As of 2024, renewables accounted for 47% of Europe's electricity generation with solar representing 11% of the total energy mix.[2] Solar energy plays a pivotal role in this generation mix. This transition is aligned with Europe's commitments to carbon neutrality by 2050 the European Green Deal, and the European Energy Security Strategy.

Figure 1

Shift from a centralized to decentralized grid



Source: DNV

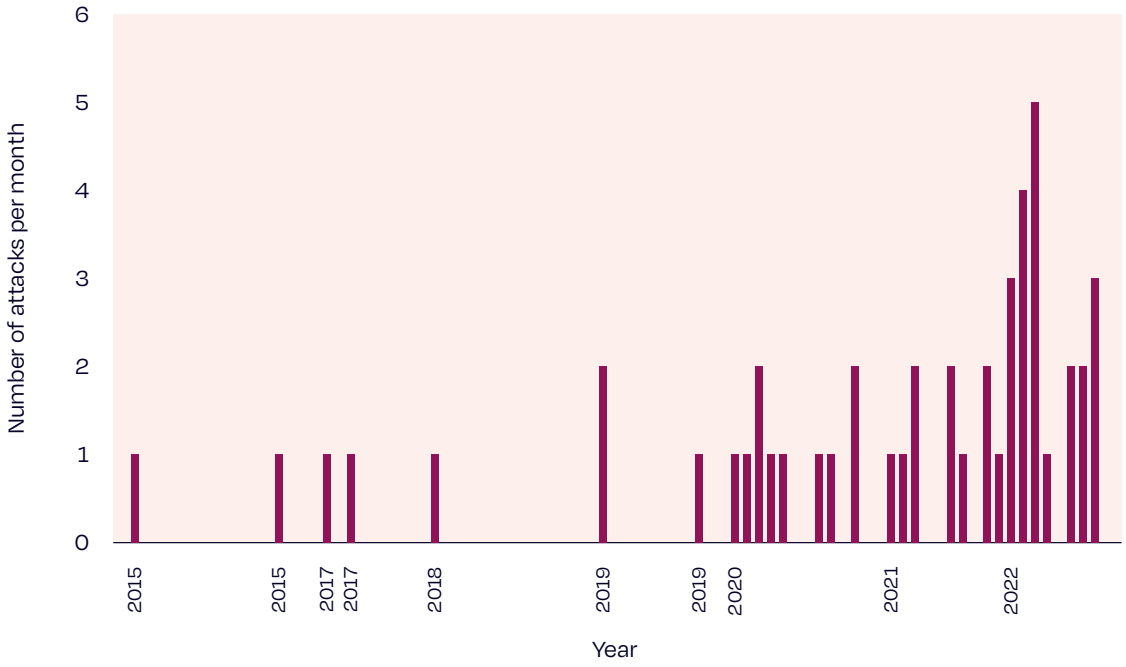
Energy infrastructure has seen a significant rise in the prevalence of cyber-attacks and physical sabotage in recent years. Major components make easy targets for disruption, as evidenced by the 2013 incident when 17 transformers were damaged at the Metcalf substation by gunmen. Similar attacks are commonplace during armed conflict, as critical infrastructure is a primary target of enemy forces. The frequency of cyber-attacks on energy infrastructure has increased, primarily comprising attacks with the intent of financial gain, such as ransomware, and nation-state attacks like those seen in Ukraine. Other publicly known attacks are summarized in Section 3.2. Figure 2 from a recent report by Danish EnergiCert, shows the clear increase in attack frequency. To date, however, cyber-attacks in the solar industry have been limited and are summarized in Section 3.2.3.

Although there have been no significant attacks on solar infrastructure, the rise in adoption of solar energy may make it more of a target. As is the case for most markets, the renewable energy sector in Europe is highly competitive, sometimes prioritizing cost efficiency over cybersecurity. Companies with a cost-differentiation market strategy may rely on low-cost components, some of which may not adhere to stringent European cybersecurity standards. Therefore, under the market forces of cost competition, cybersecurity controls are sometimes minimal. Current cybersecurity legislation will make significant improvements to the cyber maturity of traditional energy infrastructure; however, cyber risks will remain in the solar industry, as shown in Section 6.2.

The general digitalization of the power grid and the introduction of a higher number of smaller generation assets increase the attack surface of the grid. However, with the right approach, the transition to a decentralized grid can enhance rather than compromise security. Europe can address vulnerabilities proactively and ensure that DERs contribute to a more robust grid by reducing reliance on large single assets such as traditional power plants and transmission substations, which are critical targets.

Figure 2

Number of cyber-attacks per month on European energy infrastructure



Source: EnergiCert report "Cyber attacks against European energy & utility companies" September 2022

1.3 Need

By taking decisive action, Europe can safeguard its power grid and ensure a secure, sustainable energy future. It is well understood that existing regulatory actions will not adequately address the unique cyber risks associated with distributed energy resources. Through a deep understanding of the existing risks and what current regulations will and will not address, the next steps can be planned to ensure the secure integration of more solar and other renewables, thereby improving the security and resiliency of the European power grid.

SolarPower Europe has recognized these regulatory gaps and provided recommendations in the position paper "A Harmonized Cybersecurity Baseline for Solar PV"[3] aimed at mitigating cyber and energy security challenges, particularly for smart inverters. Building on SolarPower Europe's previous work, this report performs a comprehensive assessment of the risks, quantifies the threat to grid stability, and provides more detailed and specific recommendations to reduce the cyber risk associated with solar and other distributed energy resources.

1.4 Methodology

To determine the cyber risk profile and how the grid can be impacted, a threat model that examines how and what can be manipulated for different categories of solar plants is developed. This information is then used to identify which entities have access to take such actions. Through qualitative and quantitative grid analysis, each scenario is examined to determine its potential to cause damage or destabilization of the European power grid. The relative risk of each scenario is then assessed, and considering current and upcoming regulations, the residual risk for each scenario is determined. The scenarios with the highest residual risk represent the threats that future efforts should focus on.

Once the risks are well defined, the recommendations can be evaluated against the residual risk of the various threats. Final recommendations also consider the market impacts of specific actions, the timeline and resources needed for implementation, and their efficacy in mitigating solar cyber risks.

1.5 Scope

Cybersecurity is a broad topic. Only the relevant topics that have a direct and largely unmitigated impact on grid stability, as the penetration of solar in the generation mix increases, are considered in this report. The following restrictions to the scope of this study have been taken:

1. **The cyber risk assessment focuses only on the solar industry.** Although there are other means of remote manipulation of grid connected assets, such as the compromise of the transmission or distribution system operator or compromise of a plant operator, these attack vectors are better understood and the regulatory framework to protect against these threats is already in progress. There are however other aspects of the grid that are vulnerable but are not within the scope of this report. These include other renewable energy sources, electric car and charging infrastructure, and large remote controllable loads such as heat pumps.

2. **Only a compromise of the remote access capabilities to smart inverters is analysed.** This study focuses on the remote manipulation of smart inverters used in solar and solar+battery generation plants. The focus has been placed on inverters particularly as they often serve as the gateway for all communications to the solar plants and include the digital and security components needed for these communications. Any plant with components, such as batteries, that are also communicating with external infrastructure should either communicate via the secure communications gateway associated with the inverter or use another communications gateway with the same level of security.

3. **Recommendations focus on addressing the regulatory gaps that do not account for the unique nature of solar, particularly rooftop solar infrastructure.** The European Union has established sweeping new regulation over the past several years to enhance the cyber security of critical infrastructure across Europe. However, this effort has been broadly targeted and therefore does not address some specific characteristics that are unique in the solar industry. Namely, rooftop solar generally falls below thresholds to be considered by the previous legislation and there is often not one single entity, such as an operator or owner, that would be ultimately responsible for the security of the infrastructure. Therefore, the recommendations in this report focus on address those specific gaps not addressed by the broader regulation.

4. **Cyber risks include both malicious compromise of systems by hackers as well as the intentional misuse of access.** Cyber risk offer refers to cyber-attacks by hackers aiming to compromise systems for malicious purposes such as theft, disruption, or damage. For the purposes of this report, cyber risk also includes the intentional misuse of access by legitimate entities, such as vendors or service providers, through insider threats or in the event of collaboration with nation states to conduct espionage or sabotage.

1.5.1 Assumptions

The following substantiated assumptions are necessary to manage the scope of the assessment. While each assumption may not be accurate for every solar installation, they represent most installations and/or bound the worst-case scenario to be evaluated as part of this assessment.

1. **Any remote access to the installation is assumed to include control and configuration changes to the smart inverter.** This study assumes that any access to the installation includes access to start-stop, set point updates, uploading of configuration settings, and software updates. This assumption is substantiated by DNV experience through assessments of sites and components in the solar industry, primarily based on the lack of access control, including password control, network access control, network segregation, and role-based access control mechanisms observed during DNV technical assessment engagements. Note that while this access can be limited by the manufacturer, and for many brands this is implemented, it is not a regulatory requirement. A lack of access control is a common finding during assessments. It is therefore bounding to assume that a third-party stakeholder would have remote control access to a significant capacity of a single manufacturer's installed base.

2. **Solar inverters communicate with cloud servers which are assumed to be commonly hosted outside the EU.** This study assumes that many solar inverters communicate with cloud servers hosted outside the EU. The inverters can be operated via these cloud services without any restriction of the host following EU legislation. It is noted, however, that tier-1 manufacturers generally host data within the EU and other secure jurisdictions that ensure a baseline level of physical and cyber security for the cloud infrastructure. This assumption is substantiated by DNV Cyber experience through assessments of sites and components in the solar industry, primarily based on the knowledge that the vendors of the inverters are allowed to use their own cloud platform.

3. **For residential and smaller scale commercial plants, the installation company, service partner and/or the vendor are assumed to have limited IT and cybersecurity knowledge.** This study assumes that many smaller stakeholders who sell, purchase, install and even service rooftop solar do not have the in-house IT and cyber security expertise to ensure adequate security controls are implemented in these installations. This assumption is substantiated by DNV experience through assessments of sites and components in the solar industry, interviews with various industry stakeholders, and the understanding that these organizations are unregulated and often operate with a relatively small staff compared to other stakeholders such as operators and manufacturers.

4. **An assumed 70% of residential and small scale commercial solar installations are connected to the internet.** It is not possible to determine an accurate percentage of residential and commercial solar installations that are connected to the internet. An assumed and conservative value of 70% is therefore used. It is however estimated that the actual value is greater than 90%. This is based on manufacturer warranty programs that limit warranty when not connected, input from various inverter manufacturers and installers, as well as observations from cyber security assessments.

© Shutterstock.com

Solar Plant Design and Remote Access Capabilities

In this chapter, we define the types of solar plants considered, the various types of remote access available, and which entities typically have each type of access. Solar installations generally fall into one of several categories. For this study, we classify solar installations into the two categories outlined below.

2.1 Solar Plant Categories

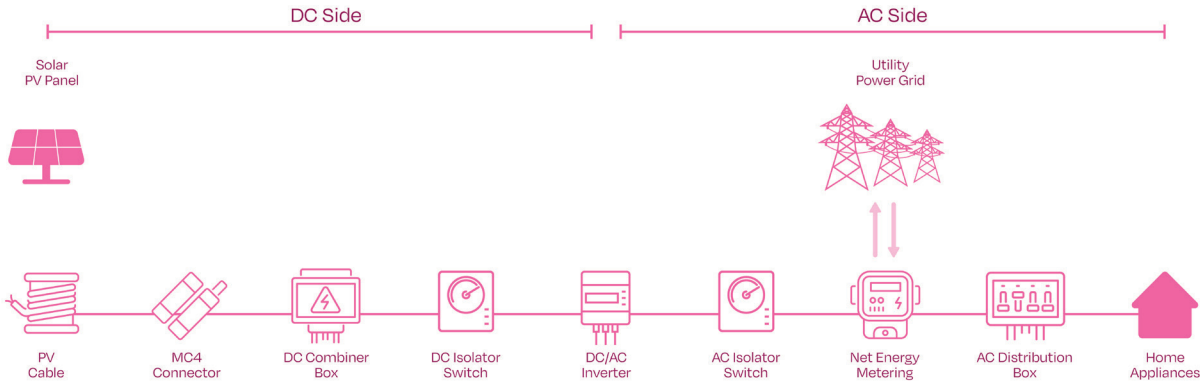
2.1.1 Residential and commercial size

Residential and commercial-sized solar plants are often overlooked as significant contributors to the energy infrastructure when considered individually. However, collectively, they generate a noticeable and growing amount of power for the grid daily. These photovoltaic (PV) installations are distributed across multiple Distributed Service Operator (DSO) service areas and connect to the grid, often through existing customer interconnections.

The owners of these solar plants are typically consumer households or small and medium-sized businesses, such as shopping malls or warehouses. The size of these individual plants can range from a single solar module of 300 Wp to solar plants of up to 1,000 kWp. Most of these plants use the same internet access as the facility they are installed in. The procurement of these solar plants usually involves a direct business transaction between the sales/installation company and the facility owner. Installation of this kind of plant can be on a tilted roof of households, a larger flat roof of companies, or sometimes on land near the facility. Figure 3 shows the typical components of this style of installation, while Figure 4 depicts a standard method for connecting the PV for remote access and to the management platform for the device. Note that the inverter itself is the primary digital component that facilitates communication with the entire plant.

Figure 3

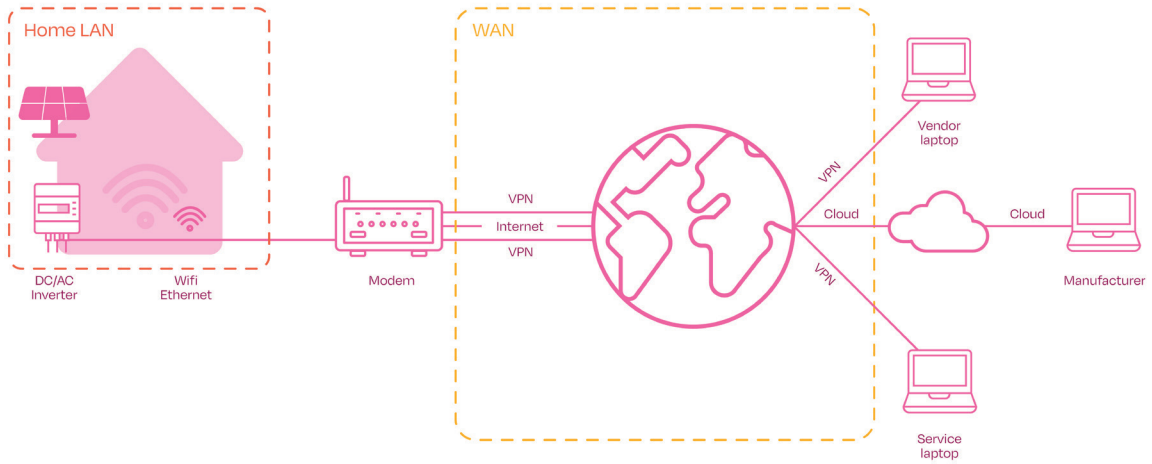
Typical layout of a grid-connected PV system for residential rooftop application



Source: https://www.sfpe.org/publications/periodicals/sfpeeuropedigital/sfpeeurope21/europeissue21feature5

Figure 4

Data flow diagram of a residential PV system



Source: DNV

2.1.2 Utility size PV systems

Utility-scale PV systems generate energy on a large scale, connecting locally to the Transmission System Operator (TSO) or Distribution System Operator (DSO). These solar fields are often located in remote areas and rely on multiple remote access methods for servicing and engineering.

Ownership of utility-scale plants typically includes Independent Power Producers (IPPs), utilities, and investment funds. These solar plants range in size from one to several hundred MW. Unlike smaller installations, large-scale solar farms often have restricted internet access, yet the number of stakeholders requiring remote data access is usually greater. Their procurement process involves multiple parties, frequently incorporating third-party advisory.

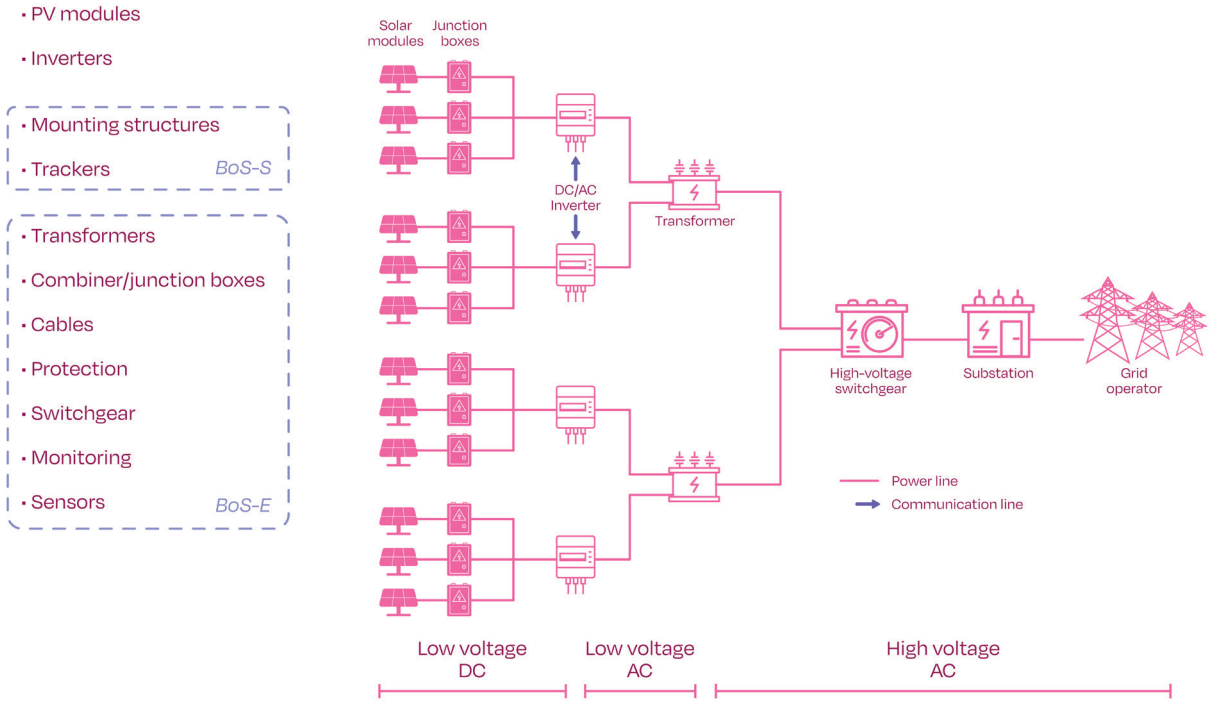
When above a certain size to qualify as critical energy infrastructure, utility-scale solar parks must adhere to strict standards for control and access. Given their significance, remote accessibility is often considered a potential risk to investment. As a result, these plants are owned and operated by experienced professionals who generally prioritize secure and efficient operations. It should be noted, however, that utility-owned plants are often more secure as the utilities have been heavily regulated for years and therefore have the in-house resources to ensure cybersecurity requirements are included in the design of the plant. This may not always be true in the case of IPPs and investor-owned plants, but these organizations recognize the impact of the upcoming regulations and are actively making improvements to prepare for compliance.

Figure 5 shows the typical components of a utility scale PV plant. Network design however varies greatly from site to site. Figure 6 depicts DNV's recommended network reference design, which is based on the Purdue model for control system segmentation. However, as noted in Section 3.1, the network design is often much simpler and less secure.

Figure 5

Typical utility scale solar power plant

Overview of a solar PV system

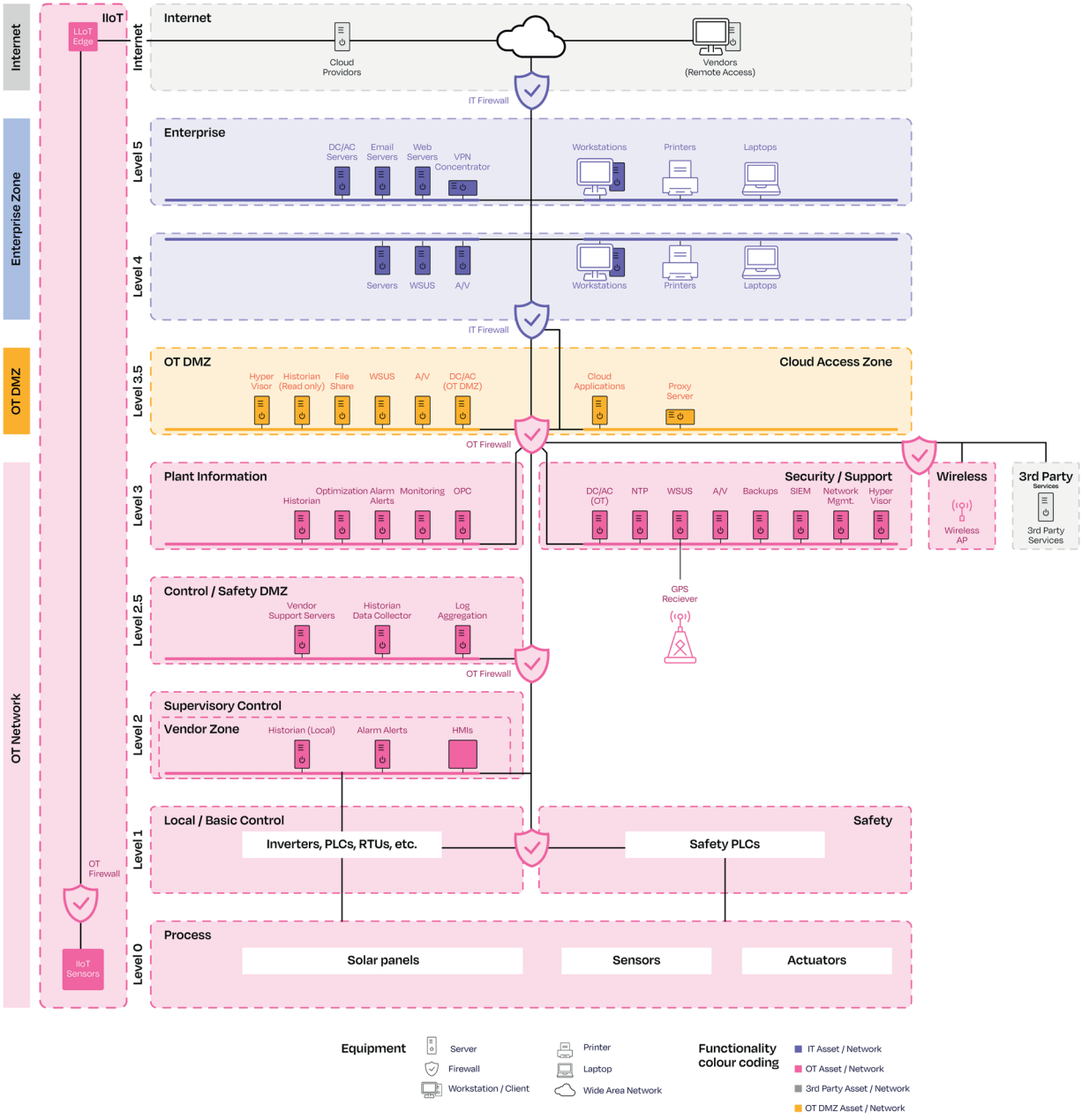


Source: DNV

© Shutterstock.com

Figure 6

OT Network Reference architecture for solar fields



Source: DNV

2.2 Remote connection

2.2.1 Typical Stakeholders and Access Permissions

Many stakeholders throughout the solar supply chain require access to the plants for various reasons. Below are several specific examples to highlight the need for access following by a summary of access permissions.

The use case for remote connections differs for every user. Several examples include:

- **Inverter manufacturers** are responsible for ensuring optimal inverter performance, addressing security vulnerabilities, and rolling out new features. They typically require the highest level of access, including firmware updates, configuration changes, and control actions for troubleshooting.

- **Plant owners** are not always the operators, they remain concerned with plant status and overall health. They often require read-only access to monitor real-time data but do not necessarily need control permissions.

- **A servicing partner** or EPC (installer) is responsible for commissioning, maintenance, and troubleshooting, servicing partners and installers require both read and write access to control functions. They need the ability to modify configurations and perform system diagnostics.

- **TSOs and DSOs** typically do not have direct access to smaller-scale plants, but they control and monitor large-scale solar plants. Their access is critical for grid stabilization and balancing, ensuring that solar energy integration does not disrupt the power system.

- **Virtual Power Plant (VPP)** operators aggregate multiple distributed solar plants, battery storage systems, and other renewable sources into a flexible, dispatchable energy resource. To manage energy distribution efficiently, they require control access to adjust solar plant output as needed.

- **Other third-party service** providers can be for example smart home applications which consumers use to optimize their energy usage. In such cases, service providers are often granted full access to the solar plant to enable seamless energy management and automation.

In the Table 1 below, you can see the parties that most often has access to the solar plant of certain size. This is overall market average from DNV's perspective, but the access capabilities can differ on a case-by-case basis.

Table 1

Parties with access to a certain scale of plants

Party	Residential and commercial <1 000 kWp	Utility scale >1 000 kWp
Inverter manufacturer	Yes	No access after commissioning [a]
Plant owner	Normally limited to end user functions	Yes
EPC (installer)	Generally limited to own installations	No access after commissioning
VPP, aggregator	Yes	Yes
TSO/DSO VPP, aggregator	No direct access [b]	Yes
O&M operator / Tech. asset management	Often same as installer	Yes, but generally restricted and controlled through the operator
Other third party service	Yes	Generally no direct access

a: Inverter manufacturers usually don't have direct remote access to the plant following commissioning. Power plant operators use a SCADA system to check commands going in and out. However, in these scenarios, the manufacturer is still responsible for providing firmware updates and often troubleshooting and service support.
b: Recent regulation in Germany (Solarspitzengesetz or Solar Peak Law) will require solar installations as small as 100kW include the ability to be controlled remotely. Over the following decades, this trend is expected to continue in other member states as solar becomes a primary source of generation.

2.2.2 Connection Options

Locally operated and serviced
At commissioning, the solar inverters are configured locally with an engineering PC. The engineering PC has software installed to communicate with the solar inverter and set setpoint and configure good operation. After commissioning, malfunctions on the solar inverters are likely to happen. A service engineer can be onsite to repair inverters or change configurations while using his PC and setup a direct communication with the inverter. Another option for connection is a local HMI (Human Machine Interface), usually built into the inverter, see Figure 7.

Remote operated and serviced by using a secure access
Remote operations and servicing rely on secure access methods to prevent unauthorized access. Various technologies facilitate restricted and encrypted connections, with Virtual Private Networks (VPNs) and Remote Desktop Services (RDS) being among the most used solutions.

Remote operated and services by using a cloud
Inverters can be connected to internet via local router with WLAN or Ethernet, there is also 3G/4G/5G SIM card options to connect to the internet. The inverter uploads data to the manufacturer's cloud service, allowing different parties to monitor and control the solar plant remotely through a mobile app or web portal. Third party access and add-on third party services generally interface with the data through an API developed by the manufacturer. Therefore, it is the manufacturer who controls the level of access by all stakeholders.

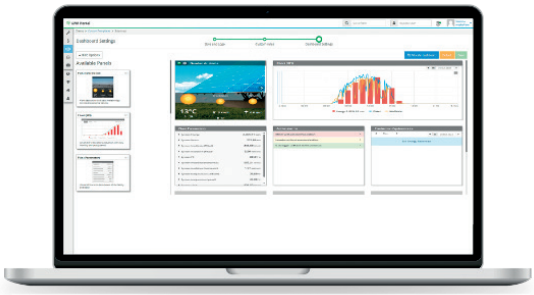
Figure 7

Solar inverter with local HMI

Source: DNV

Figure 8

Website based monitoring portal on a laptop



Source: DNV

The table below illustrates the different types of connections commonly used by two different sizes of solar plants. The plant sizes are indicative averages, and the specific control method may vary based on infrastructure and plant-specific configurations.

As shown in the table, both small and large-scale solar plants can utilize local access, where the inverter is fully controlled on-site without external connectivity. In residential and commercial-scale installations, cloud-based services provided by the inverter manufacturer are more commonly used. These cloud monitoring platforms, included with the hardware, enable installers, sales teams, and manufacturers to efficiently diagnose and resolve potential inverter issues.

Table 2

Comparison table for the types of connections

Type of connection	Residential and commercial <1 000 kWp	Utility scale >1 000 kWp
Local access	Yes	Yes
Restricted remote access, Virtual Desktop Interface (VDI)	No	Yes
Cloud service via router/sim-card	Yes	Generally no unless centrally managed as part of a VPP

2.3 Grid-profile of solar inverter

The grid profile of a solar inverter can be adjusted through its settings. This profile includes key parameters such as grid voltage, grid frequency, and power factor, all of which can be modified remotely or locally. In the EU, the grid profile of solar inverters is primarily defined by the EN 50549-1 and EN 50549-2 standards. These standards provide comprehensive guidelines on the parameters that need to be adjusted for proper integration of solar inverters into the grid.

EN 50549-1 covers inverters connected to low-voltage grids, for residential and commercial-scale solar plants. EN 50549-2 focuses on medium-voltage grids. These standards define the key parameters that inverter manufacturers must implement to comply with grid integration requirements.

Key Parameters Defined by EN 50549 Standards

1. **Voltage Range - EN 50549-1 & EN 50549-2:** These standards define acceptable voltage ranges for inverters connected to the grid. The typical voltage range is **85% to 110%** of the nominal grid voltage. Inverters must disconnect if the grid voltage exceeds **110%** or falls below **85%** for extended periods to protect both the inverter and the grid.

2. **Frequency Range** - Inverters must operate within the **frequency range of 47.5 Hz to 51.5 Hz** to maintain grid stability. If the grid frequency falls below **47.5 Hz** or rises above **51.5 Hz**, the inverter is required to disconnect, as these frequencies indicate an unstable grid.

3. **Active Power Control** - EN 50549-1 / EN 50549-2 require inverters to support **active power control**. This feature allows the inverter to adjust its power output to match grid needs, either by **reducing** or **increasing** power generation.

4. **Reactive Power Control** - Inverters must be able to provide **reactive power** (VAR) support to the grid to help regulate voltage.

5. **Low-Voltage Ride-Through (LVRT)** and **High-Voltage Ride-Through (HVRT)** - These features ensure that the inverter remains connected to the grid during short-term voltage fluctuations, such as sags or spikes.

6. **Anti-Islanding Protection - EN 50549** mandates **anti-islanding protection** to ensure the inverter disconnects from the grid during a power outage.

7. **Frequency-Watt and Voltage-Watt Control** - These control functions allow inverters to adjust active power output in response to changes in grid frequency or voltage.

Multiple postulated scenarios are possible through malicious manipulation of the parameters. For example, inverters may be shut off or the active and reactive power outputs may be changed which would impact the local grid frequency or voltage respectively. If disturbances are significant enough through manipulation of a mass of inverters, then others in the local area may also disconnect if the voltage and frequency parameters of the local grid go outside of the required parameters. This scenario applies to other types of generation as well and such a scenario presents challenges for the grid operator in balancing the generation and consumption of power in the grid. This is analysed further in Section 6.

© Shutterstock.com

03

Solar Industry Cyber Security Risk Assessment

3.1 Solar Industry Cyber Security Overview

The current maturity level of cyber security programs across the industry varies significantly. Utility scale and some aggregated rooftop installations fall under NIS2 requirements. Additionally, some manufacturers and other stakeholders recognize the impact a major security event could have on their business. As a result, many large vendors and other stakeholders have made significant improvements to their security programs. There are however also low-cost options that have flourished under the intense competition to generate power at the lowest possible price per kW. Additionally, many stakeholders involved in the installation, servicing and operation of smaller residential and commercial plants lack the staff and resources to adequately address or even understand the cyber risks.

The specific level of security for each installation is heavily dependent on several factors. The greatest difference being the lower security maturity of rooftop solar compared to utility scale plants. However, there is also generally a gap between security maturity for utility owned plants and those at the utility scale but owned and developed by startups and investors that lack adequate in-house cyber expertise of more established and regulated organizations such as a transmission system operator for example. However, several general observations can be made with the caveat that they are more commonly found in installations associated with parts of the industry with generally lower cyber security maturity. Through assessments of solar installations and penetration testing of solar inverters and similar components in critical infrastructure applications, DNV has made the following observations:

- Default usernames and passwords are very common for all plant types.
- Residential and commercial scale Inverters are sometimes connected to cloud platforms directly either with poorly configured VPNs or in some instances without any protection of the transmitted data.
- Often networks for utility scale plants lack necessary protections such as network segmentation and network access control mechanisms.
- System hardening is uncommon for residential and commercial systems. In some instances, security is actively undermined in lieu of operational efficiency.
- Firmware and other system updates are not common with low-cost manufacturers and there is no pressure on installers and service companies to implement updates except with higher value brands.
- Cyber security programs for most stakeholders are poorly documented and not well followed. This often includes owners and operators of utility scale plants.
- Many stakeholders with remote access to inverters are unregulated for cyber security. This applies to nearly every entity that would not be considered an operator of critical infrastructure, meaning also those plants that do not exceed the capacity threshold of the nation in which it operates. Stakeholders therefore include installers, service providers, manufacturers and in some cases the owners.

To best address the existing gaps in security throughout the industry, an understanding of the specific threats and their probability to cause widespread power grid disruption or damage is necessary. To define the specific industry cyber risks, a threat model is developed in the following section with a full risk register including residual risk levels with upcoming regulations and with recommended additional actions. A full summary of the risk register is included in Annex B.

3.2 Relevant Cyber Attacks on Critical Infrastructure

Cyberattacks on critical infrastructure, especially in energy and solar sectors, are rising. Recent incidents on power grids, wind farms, and solar systems demonstrate the growing threat. Coupled with the increasing use of cyber in modern warfare, these attacks highlight the urgent need for stronger cybersecurity to protect vital systems. Following is a summary of the most relevant attacks to understand the existing threat landscape and some lessons learned from past cyber-attacks on critical infrastructure.

3.2.1 Summary of Attacks on Critical Power Infrastructure

Attacks on Ukrainian Power Infrastructure (2015-2022): The 2015 and 2016 attacks on Ukraine's power grid involved the use of BlackEnergy and Industroyer/CrashOverride malware, respectively. These attacks demonstrated the ability to manipulate industrial control systems (ICS) to cause widespread blackouts. In 2015, attackers used spear-phishing to gain initial access, followed by the deployment of BlackEnergy malware to disable substations and disrupt customer service. The 2016 attack leveraged Industroyer malware, which was specifically designed to target electrical substations, causing a more extensive blackout. Subsequent attacks, especially during the 2022 Russian invasion, involved attempts to disrupt power generation and distribution through various cyber means, including malware deployment and denial-of-service attacks.

Attack on Danish Energy Infrastructure (2023): In May 2023, Denmark's critical energy infrastructure experienced a large-scale, coordinated cyberattack targeting 22 companies involved in managing essential energy services. The attacks unfolded in distinct waves, with the initial wave capitalizing on a critical vulnerability (CVE-2023-28771) within Zyxel firewalls. This vulnerability allowed attackers to gain remote control of the firewalls by sending specially crafted network packets.

SektorCERT, Denmark's organization responsible for cybersecurity in critical sectors, played a crucial role in detecting and mitigating the attacks. Their sector-wide monitoring and information-sharing capabilities enabled them to identify the coordinated nature of the intrusions using their sensor network. Later in May, a second wave of attacks was observed. Attribution of the attack to specific actors has been complex, and while there were some indicators of possible state-sponsored involvement, particularly with some possible links to the Russian Sandworm APT group, conclusive attribution has been difficult.

While the attacks were significant, the rapid detection and response by SektorCERT and the affected companies prevented widespread disruption of energy services.

Cyberattack on German Wind Turbine Operations (2022-2023): Three separate attacks on the German wind industry took place all within months of each other. The first attack was the byproduct of an attack on satellite infrastructure that was also used for remote monitoring and control of wind farms in Germany. Many plants were shutdown as a result that did not have a backup means of communication.

The next attack, in March 2022 was an attack on the IT infrastructure of Nordex, a manufacturer and service provider for wind turbines. During the attack, all communications to the wind farms were immediately severed and the attack was contained on the IT infrastructure. Similarly, in April 2023, Deutsche Windtechnik, a major third-party service provider for wind turbines, was also attacked and as a resulted needed to immediately sever all remote connections. In both instances, the organizations were not the operators of the plants, and therefore the plants were able to continue operations.

Other notable attacks include:

- **Davis-Besse Nuclear Power Plant, 2003** – IT systems compromised, and redundant safety monitoring system was temporarily unavailable
- **Stuxnet Attack on Nuclear Program of Iran, 2010** – Attack destroyed uranium enrichment centrifuges
- **Korea Hydro and Nuclear Power, 2014** – Hackers demanded plant be shut down and funds be sent otherwise stolen data would be released after the IT systems were compromised and data was exfiltrated.
- **Triton attack on Safety Instrumented System 2017** – A potentially significant cyber-physical attack was uncovered when malware on a safety PLC at a petrochemical plant in Saudi Arabia accidently shut-down the plant. The hackers had been in the IT systems at the plant as early as 2014 and reports suggest that intent was to further compromise control systems to later disable the safety PLC and then force the system into an unsafe condition.
- **Kudankulam Nuclear Power Plant, 2019** North Korea state hackers exfiltrated data from the plant IT systems.
- **Randsomware Attack on Uk Electricity Market, 2020** - IT systems at Elexon, providers of balancing services for Great Britain's national grid, were compromised.

3.2.2 Role of Cyber in Modern Warfare

In addition to the described attacks, a broader spectrum of cyber threats continues to target power infrastructure globally. Cyber warfare has become a central tactic in modern warfare, as showcased by the war in Ukraine. According to the US Cybersecurity and Infrastructure Security Agency (CISA), offensive capabilities have evolved over recent years highlighted by the capabilities and attacks carried out by APT groups Volt Typhoon, affiliated with the Chinese Government, and Dragonfly or Energetic Bear who is associated with Russia. These nation-state hacking groups have been tracked for years with a focus on attacking critical infrastructure in the Unites States and Europe.[4,5] Additionally, most developed nations now include an offensive cyber unit in their nations military or other government organizations such as the United States NSA and U.S. Army Cyber Command, the British Government Communications Headquarters (GCHQ), Israels Unit 8200, or the German Cyber- und Informationsraum (CIR) which is a part of the German Bundeswehr (Armed Forces).

3.2.3 Summary of Attacks in the Solar Industry

While attacks continue to occur with more regular frequency across critical infrastructure, to date, attacks in the solar industry specifically, have been limited. Solar Industry attacks have been previously summarized in a report from DER Security Corp that includes the four following attacks up to October 2024.[6]

- 2019 Denial of Service on a Cisco firewall that prevented visibility of 500MW of renewables including solar.
- 2023 Romanian solar customers modified mandatory configurations using installer login credentials to disable the voltage active function. This action prevented the utilities' ability to curtail output in a high grid voltage scenario while allowing the customer to make more money from their output of their panels.

- 2024 A remote code execution vulnerability was exploited in a Contec SolarView Compact remote monitoring device to add the devices to an IOT Botnet. The Botnet, consisting of approximately 800 of the devices, was then used to hide bank account thefts and suspected to be linked to nation-state activity.

- Pro-Russian hacktivist group, Just Evil, stole credentials to 22 client sites in Lithuania and posted the credentials on the Dark Web. The credentials allowed access to the management portal of the PV sites; however the access was not used to carry out any further attack.

Although there have been attacks in the solar industry, they do not compare to those seen in other parts of the energy sector where industrial espionage, ransomware and attacks leading to public grid blackouts have occurred. There is however growing concern for potential damage as the industry grows. Recent research into the Solarman platform has highlighted these concerns. Solarman is a third-party cloud application for the remote management of PV and as an industry leader has access to roughly 200GW of capacity. Researchers at Bitdefender were able to identify several critical vulnerabilities that allowed takeover of any account on the platform. Left unaddressed, these kinds of vulnerabilities may remain and eventually be targeted by cyber criminals and nation state attackers.

3.3 Solar Industry Risk Assessment

3.3.1 Risk Assessment Methodology

To assess the threats to the power grid from attacks on the solar industry, the risk will be calculating by using three metrics: impact, ease of compromise, and likelihood. This approach allows for comparison of the attack scenarios and can determine their relative risk. Metrics include the potential damage each attack scenario could cause to the grid (impact), how difficult it would be to execute (ease of compromise), and how probable it is to happen (likelihood). Each metric is assigned a value between 1 and 5 based on the following criteria and the final risk score is the product of the three metrics (Impact x ease of compromise x likelihood).

Impact
The risk determination of 'impact' is the potential impact to grid stability. Threat scenarios that provide the greatest access to the largest capacity of inverters is considered the higher risk. It is also considered more impactful when execution of the events may occur simultaneously, such as triggered at a particular time in software versus manual interactions that introduce time variability to allow electrical parameters to stabilize (via remaining generation output controls) and automatic grid stabilization controls (transformer tap changes, load shedding, etc.) to respond to the transients. Table 3 shows the criteria for the scoring of the impact.

Table 3

Impact Scoring

Score	Value
1	Insignificant - Disruption of <3GW
2	Minor - Disruption of 3-10 GW
3	Moderate - Sudden disruption of 3-10GW
4	Major - Disruption of >10GW
5	Critical - Sudden disruption of >10GW

Note: a threshold of 3GW is chosen as the control reserve required for the European grid. The critical threshold of 10GW is chosen as an estimated amount of total capacity lost that would most likely trigger a cascading outage. Further research would be necessary to determine a more precise critical threshold based on the grid stability limits, which is also likely to vary in different areas of the grid.

Ease of Compromise

Ease of compromise is related to the level of complexity or the amount of resource that would be needed to carry out the attack type. A threat scenario that requires significant resources and time is a lower risk while an attack that is trivial to implement is considered high ease of compromise and therefore a higher risk. Table 4 shows the criteria for the ease of compromise scoring.

Table 4

Ease of Compromise Scoring

Score	Value
1	Very difficult - Requires 0-day exploits, insider operatives, physical access and/or significant time and resources
2	Difficult - Significant time and resources needed
3	Moderate -Moderate time and resources needed
4	Easy - Basic skills and toolsets with minimal time
5	Trivial

Likelihood

The likelihood of a particular attack scenario is impossible to predict accurately. However, an indication may be determined by looking at past events and whether there is a precedence for such an attack and the past frequency of such an event. Note however that the cyber threat landscape is constantly evolving and is further influenced by a complex geopolitical landscape. It is therefore only an indication and does not accurately show the probability of any particular event. Note that in this analysis, the precedence is considered for the attack scenario having occurred on any critical infrastructure and is not particular to solar installations.

Table 5

Likelihood Scoring

Score	Value
1	Very Unlikely – there is no current precedence and the event could be seen as a declaration of war
2	Unlikely – there is no current publicly known precedence set for the scenario
3	Possible – scenario has occurred in the past
4	Likely – scenario occurs sporadically without a regular frequency
5	Very Likely – scenario has occurred in the past with regular frequency

The following risk assessment scale is used to designate a risk level with the particular risk score. The risk score calculation is an estimate of the risk, based on a qualitative and perceived threat which includes uncertainty. Therefore, threat scenarios with the same risk level are considered to be equivalent even when one has a higher calculated risk score.

Risk Assessment Scale

Risk Score	Risk Level
1-9	Low
10-24	Medium
25-39	High
40+	Critical

3.3.2 Threat scenarios

Threat scenarios have been determined and categorized based on three primary vectors, compromise of a device itself, compromise through an organization without cooperation of the organization and finally compromise of systems with the support of the vendor.

Compromise of Device, Application or Infrastructure
The first series of threats relate to direct compromise of the inverter or supporting software applications and IT infrastructure. These threats are common for most devices that include user interfaces and could control a physical process.

Gain Unauthorized Access through Vulnerabilities in Authentication Mechanisms

Threat	Impact	Ease of Compromise	Likelihood	Risk Score	Risk Level
Gain Unauthorized Access through Vulnerabilities in Authentication Mechanisms.	3	3	4	36	High

Unauthorized access can be gained through software vulnerabilities that bypass authentication mechanisms on different management applications, affecting manufacturer or third-party APIs. This could be achieved by manipulating a vulnerable system to obtain legitimate authentication tokens either through weak session management, exposed endpoints or insecure transmission channels. In this scenario, the least severe impact would be gaining access to an owner with a single installation. However, the most critical risk involves compromising accounts with installer or manufacturer roles, which could manipulate multiple devices with widespread impact. Vulnerabilities are commonly found in all applications and are not often patched quickly if at all in most industrial applications. Therefore, the ease of compromise is expected to be somewhat low. Attacks of this type are also very common in the industry and occur with somewhat regular frequency in the energy industry.

Tampering Inverters Through API's

Threat	Impact	Ease of Compromise	Likelihood	Risk Score	Risk Level
Tampering Inverters Through API's.	3	3	4	36	High

APIs can provide functionality to retrieve performance metrics, configure system settings, adjust power output or other parameters related to the PV system for monitoring or maintenance purposes. However, APIs can also introduce potential attack surfaces if not secured. For example, insecure APIs that lack adequate access controls may enable unauthorised users to perform these actions. In such cases, actions requiring higher-level privileges are poorly implemented or easily bypassed, allowing attackers to elevate the privileges and tamper with the inverter's settings. A common weakness in these endpoints is weakly designed IDs, following predictable patterns, such as sequential numbering or easily guessable IDs. This lack of security design can allow threat actors to systematically enumerate by guessing or deriving valid IDs of inverters to gain unauthorized access multiple devices. Attackers could then escalate their actions by misusing endpoints to issue commands that disconnect inverters simultaneously, reducing the solar power generation.

Direct Access to Inverter Through Intentional and Non-intentional Backdoor

Threat	Impact	Ease of Compromise	Likelihood	Risk Score	Risk Level
Direct Access to Inverter Through Intentional and Non-intentional Backdoor	3	3	2	18	Medium

DNV pentesting has in the past included review of components for signs of a back door. Although no direct evidence has been found of intentional backdoors in a solar inverter, it is common practice to include additional means of communication to industrial devices such as cellular to improve reliability and support capabilities. In many cases, these additional means of communication may not be well documented and therefore can be missed during a high-level cyber security assessment or ignored if the manufacturer may self-attest to the security of the device. While often these additional means are not malicious in nature, they may be compromised and used for malicious purposes if not secured or disabled. However, mass exploitation of any backdoor has not been seen in the energy industry and is therefore considered to be unlikely.

Destruction or Compromise of Physical Command and Control Infrastructure

Threat	Impact	Ease of Compromise	Likelihood	Risk Score	Risk Level
Destruction or Compromise of Physical Command and Control Infrastructure	3	3	3	27	High

Currently a great deal of infrastructure supporting applications and hosting component information resides outside of the European Union. This means that in many instances, namely those with non-European manufacturers, the data that interacts with the system must traverse infrastructure such as subsea fiber optic cables. Severing such a cable has long been regarding as a serious risk to communication infrastructure and in this instance would impact the ability to remotely access and control assets in Europe in the event of a crisis. Additionally, data centers hosted outside of the European Union may not include the same strict security requirements and may be susceptible to sabotage or local access to applications and information hosted on those servers. The access to a single command and control server may grant access to significant resources. Additional concerns include the access of sensitive grid data including real-time operational data or sensitive customer data that would otherwise fall under the protections of GDPR. While the intentional sabotage of physical IT infrastructure is not prevalent in the industry, mining of sensitive data is common.

It should however also be noted that physical security risks vary greatly depending on whether dedicated IT infrastructure is used or when applications and data are hosted in the cloud. When data is hosted in data centers on premise or on dedicated IT infrastructure in a co-location data center, it is possible to target specific individual servers and supporting infrastructure that would result in a direct impact on operations. However, with data hosted in a public cloud such as Azure, AWS, google and others, the risk of compromise or attack through physical means are greatly reduced.

Compromise of an Organization

This subset of threats includes those that are possible through nation-state actor compromise of trusted organizations within the supply chain or less resourced hackers compromising a vendor's access. There is a long history of attacks that include compromise of various players within a supply chain. The impact of a threat depends on the security awareness of the affected organization and their level of access to grid connected inverters. For this reason, a differentiation may be made between the compromise of an inverter manufacturer and that of a third-party service provider with less access to installed capacity.

Control Inverters through Compromise of Third-Party Access Rights

Threat	Impact	Ease of Compromise	Likelihood	Risk Score	Risk Level
Control Inverters through Compromise of Third-Party Access Rights	2	4	4	32	High

The management portal of a group of inverters may be compromised through various methods with a very common method being the compromise of credentials. Many third parties have limited access to management portals to install, configure and service the inverters. Credentials for this level of access may be obtained in many ways and often requires relatively low effort as the security practices of many third-party providers are weak. Although this type of compromise is considered low effort, it also results in less access to capacity as access to third parties are generally restricted by the manufacturer to reduce operational risk. Additionally, in most instances, secure VPNs or other network controls are implemented which provide an additional layer of security if the credentials are compromised. Further protection is possible through better password security; however, it is very common to use default or shared credentials that are not routinely changed.

Control Inverters through Compromise of Manufacturer Access Rights

Threat	Impact	Ease of Compromise	Likelihood	Risk Score	Risk Level
Control Inverters through Compromise of Manufacturer Access Rights	4	3	3	36	High

A similar attack of inverter access to the management portal would be through the manufacturer itself. The manufacturer will have full access to every inverter of their brand which often includes 10s of GW. While this level of access would be considered critical, the complexity and level of effort for this attack is higher for most manufacturers. It should however be noted that low-cost manufacturers often do not include the same level of cyber security within their organization and may be more easily compromised as fewer resources are available to invest into cyber security to maintain lower operational costs. Supply chain attacks, and attacks that target and disrupt manufacturing such as ransomware, is common across all industries. Specific targeting of manufacturers in the energy industry does occur periodically, although generally by cyber criminals as ransomware. Compromise of a manufacturer, with the intent to disrupt energy distribution and supply has not been seen in the industry, although a ransomware attack on an inverter manufacturer may still negatively impact generation if not managed properly.

Control Inverters through Malicious Firmware without Vendor Support

Threat	Impact	Ease of Compromise	Likelihood	Risk Score	Risk Level
Control Inverters through Malicious Firmware without Vendor Support	5	2	3	30	High

Through compromise of a manufacturer, the source code for the firmware for a series of inverters may also be manipulated. This type of attack is complex and could require:

- Gaining high-level privileges to the cloud services managing these PV systems.
- Chaining known exploits and unknown vulnerabilities (using 0-day exploit).
- Access to secure development environments and bypassing security control for code review

Malicious firmware can be injected in many ways, some that require manipulation of code within the manufacturer's internal development servers or through side channels and may be successful if the necessary controls such as integrity checks or cryptographic protections are not in place and there is no effective measure to verify the authenticity of the firmware. Combined, these vulnerabilities would allow executing a full-scale inverter takeover.

This type of attack has the potential for a significant impact on the grid if it is exploited on a large scale. It is however a very complex attack that requires significant effort. It is also easily prevented through requirements to follow best practices for software development, device security, and secure update mechanisms.

Compromise with Support and Cooperation of the Manufacturer
This subset of attack scenarios assumes cooperation between the vendor and a hacking group. This distinction of cooperation of the vendor is critical. The level of effort is high to compromise a manufacturer with a mature security program, obtain access to their source code or remote access platforms, and execute an attack that includes several complex steps that must be carried out while evading monitoring and detection measures. In comparison, with the cooperation of one of the many large manufacturers within China, the level of effort to execute a large-scale cyber-attack is trivial.

The determination of the likelihood of a future conflict between Europe and China is out of the scope of this report but is generally considered to be very low. However, most installed inverter capacity is from Chinese vendors and several points justify special consideration of this cyber threat, which include:

- There are reports of telecommunications companies within China that have allegedly cooperated with the state government in matters of espionage.[8] The Chinese National Intelligence Law also includes the controversial Article 7, which requires citizens and organizations to support national intelligence efforts.[18]

- In the telecommunications industry, under the rollout of 5G infrastructure, technology from vendors consider to be "high-risk" has been prohibited in many member states based on risk assessment criteria outlined in the 5G toolbox, which the European Commission developed. Specifically, this has included the ban of 5G equipment from Huawei, which is also the leading manufacturer of inverters in Europe, based on market share.[17] In the future, the European Commission needs to decide whether the concept of such a toolbox will be expanded to other technologies relevant for Europe's critical infrastructure, such as inverters. Such a tooldbox doesn't necessarily have to be linked to a ban.

- The Chinese nation-state Advanced Persistent Threat (APT) Volt Typhoon has been active in compromising and establishing a foothold in the critical infrastructure of western countries, primarily the United States, as a matter of pre-positioning for potential future attacks.[4]

- Several European member states have expressed concern over Chinese access to critical European infrastructure, in both the telecommunications and energy industry, and have passed regulations to this effect. [9,17,19,20]

Control Inverters through Malicious Firmware with Vendor Support

Threat	Impact	Ease of Compromise	Likelihood	Risk Score	Risk Level
Control Inverters through Malicious Firmware with Vendor Support	5	5	1	25	High

With direct and unrestricted access to the source code of the manufacturer, malicious lines of code may be introduced into the firmware. This code may include special instructions that execute based on a certain trigger such as a date and time, local grid conditions, or any combination of external inputs. The actions taken could include the full capabilities of the inverter to include disabling protections, changing operational parameters, sudden shutdown and power on, and abrupt changes in inverter output.

The impact of such an attack is very high and the effective controls against this type of attack are very limited. Penetration testing has limited ability to detect hidden code unless it accesses this function. A full source code review is needed but often not feasible as it requires surrendering intellectual property and significant effort of a third party to perform the review for initial and each subsequent update.

Direct Control of Inverters through Vendor Access Rights

Threat	Impact	Ease of Compromise	Likelihood	Risk Score	Risk Level
Direct Control of Inverters through Vendor Access Rights	5	5	1	25	High

With direct and unrestricted access to the manufacturers management portal of their entire installed base, the malicious actor may through very low effort, send commands to a fleet of inverters to perform and available control actions like adjustments to operational status and mode, or changes to frequency and voltage outputs.

This threat poses a high risk of damage or destabilization to the grid with very low effort.

© Shutterstock.com

04

Solar Industry Market Analysis

4.1 Solar Market Players

Previous sections have introduced the typical plant design, how they are remotely accessed, and how they may be compromised. This section now provides insight into the magnitude of the risk. More specifically, the analysis of the solar market in Europe provides insight into how much installed capacity a potential hacker may theoretically compromise.

4.1.1 Solar PV value chain

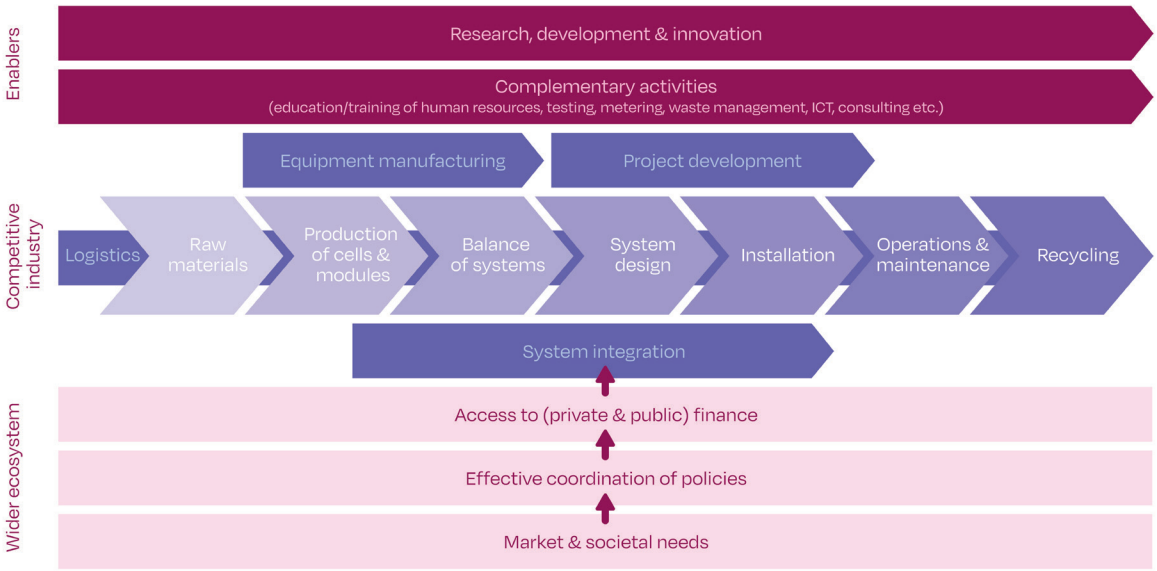
The solar industry includes a great deal of different market players. Figure 9 presents an illustration of the PV value chain showcasing the key market players. The value chain can be divided into three basic blocks: (i). Enablers; (ii) PV industry value chain; and (iii). Wider ecosystem level factors including access to finance, public policies, and market and societal needs which ultimately sets the framework for the PV value chain.

The industrial value chain begins with providers of raw materials. The raw materials are turned into solar cells and modules of wide variety. The Balance of system (BoS) is formed by manufacturing of the rest of the components needed for a PV system, most important being the inverters. The costs of a PV system are thus composed of the PV module cost and the BoS cost. The BoS cost includes cost of the structural installation, costs of the electrical system integration including inverters, transformers, wiring etc.

The project development phase is aimed at planning the PV project so that it optimises the PV energy yield and lifetime, mitigating the technological risks including the steps of system design and installation. The system integration process in which PV modules are joined with grid infrastructure, system infrastructure (e.g. buildings, vehicles or mobile devices) forms a part of the activities of both system design and installation. The PV operation and maintenance target towards enabling PV plants to perform efficiently and in compliance with applicable rules and regulations.

Figure 9

The extended PV value chain



Source: DNV 2016

This study focuses on cyber security related to solar PV inverters. Therefore, only stakeholders with remote access capabilities are considered. The respective involved market players are therefore:

- Inverter manufacturer
- Installer / EPC contractor
- PV system owner
- Aggregator
- O&M contractor
- DSO / TSO
- Other third party service providers

For DSOs, TSO, and aggregators operating any significant capacity, the level of risk is relatively small compared to the other market players since they are already subject to strict regulation as operators of critical infrastructure. Of the remaining stakeholders, most have limited access rights in terms of capabilities as well as limited access to installed capacity. Therefore, the stakeholder representing the highest level of risk is the inverter manufacturer who has typically full remote access to their entire installed base. Therefore, the market analysis focuses on the manufacturers.

It should be noted, however, that there may be instances where a large installer or service provider also has remote access to enough installed capacity to present an unacceptable level of risk to grid stability.

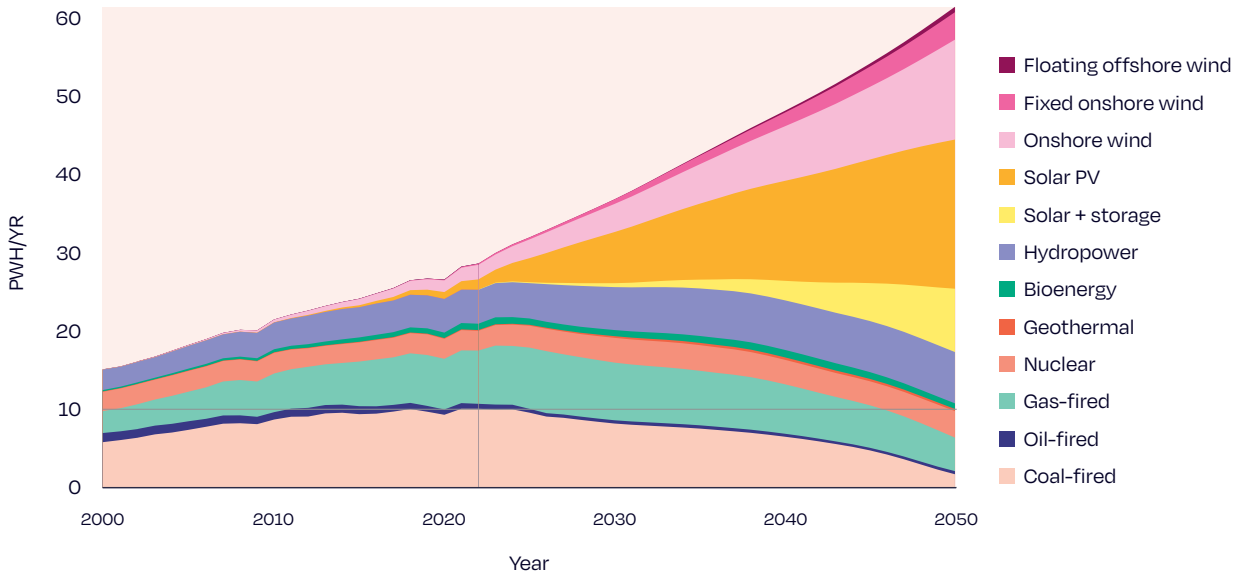
4.2 Solar PV in the power system

4.2.1 Uptake of residential / C&I versus utility-scale PV systems

Solar is an emerging powerhouse for electricity supply given the plummeting costs per kWh. In the DNV 2024 Energy Transition Outlook, solar PV is estimated to form 44% of the grid-connected electricity generation by 2050 globally. Figure 10 shows how the trajectory of the generation mix from 2000 through 2050.

Figure 10

Grid-connected electricity generation by power station type

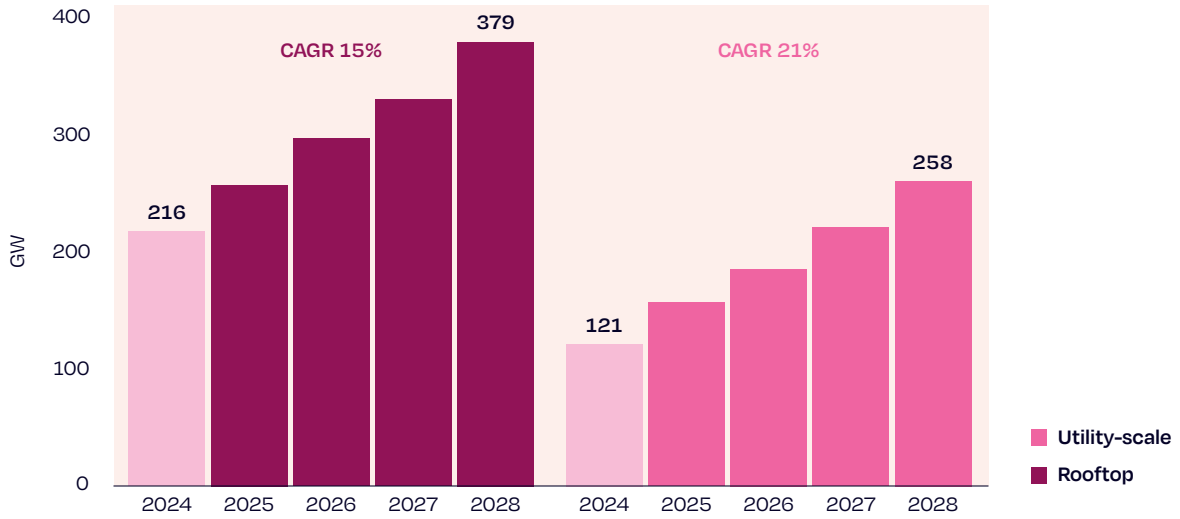


Source: DNV Energy Transition Outlook 2024

In 2024 Europe had around 337 GW of solar PV systems installed. 65% of the capacity mounted on roofs and 35% at utility-scale. SolarPower Europe expects that ratio will change towards 59%/41% over the next four years. This means that the majority of the installed base will remain on rooftops and be less secure and more vulnerable to attack. Figure 11 shows the split in the market between rooftop versus utility and how it is expected to evolve over the coming years.

Figure 11

Annual solar PV rooftop and utility-scale segment scenarios

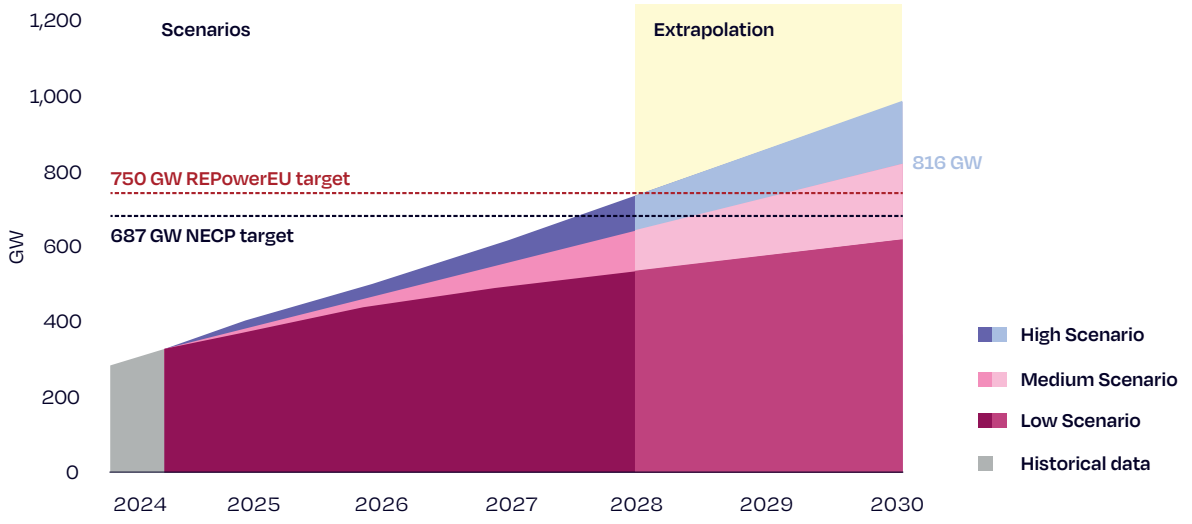


Source: SolarPower Europe

The current installed capacity of almost 350 GW is insignificant compared to projected PV installations. Europe has recently reached annual installations of more than 60 GW. By 2030, the EU will have 816 GW of PV installed across all segments, according to the medium scenario of SolarPower Europe's EU Market Outlook 2024 - 2028, more than doubling the existing installed capacity.

Figure 12

EU-27 cumulative PV installations until 2030

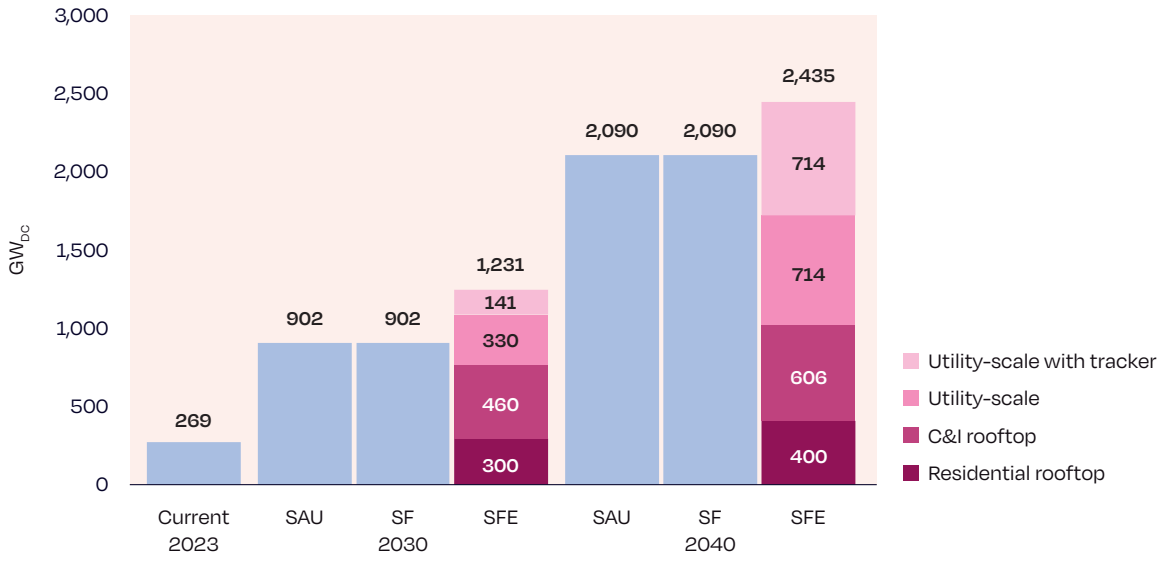


Source: SolarPower Europe
Note: Installation volumes beyond 2028 are based on a simple extrapolation of each 2025-2028 scenario to 2030.

By 2040, SolarPower Europe expects the cumulative installed PV capacity to reach between 2 and 2.4 TW, depending on the flexible electrification of Europe's energy system. That's roughly six times the current installed capacity. Solar-as-usual (SAU) reflects limited electrification or flexibility. Solar flexibility (SF) reflects the increased deployment of utility-scale storage and interconnectors. Solar flexible electrification (SFE) reflects increased flexible demand from electric heating, EVs, and hydrogen.

Figure 13

2030 and 2040 projections for cumulative PV installations depending on different scenarios.



Source: SolarPower Europe
Note: . Solar-as-usual (SAU), Solar flexibility (SF) and Solar flexible electrification (SFE) have different power system flexibility assumptions

4.2.2 Market shares

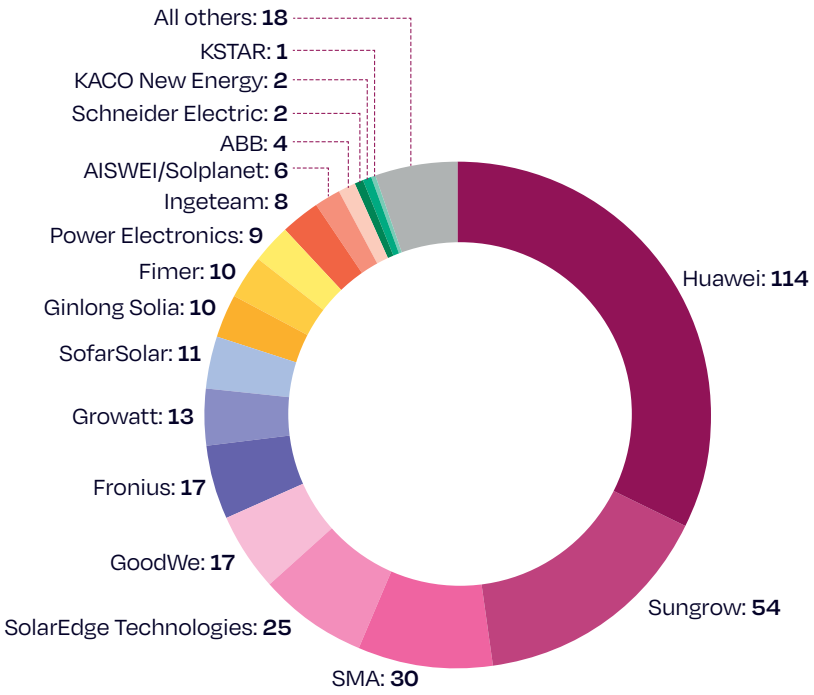
There are many different players in the global solar inverter market. However, it is dominated by a few companies and countries. Market data showing the actual installed capacity per manufacturer is not readily available. However, the market can be characterized by looking at available shipping data from WoodMcKenzie. DNV analysis of this data shows that 536 GWac of solar PV inverters were shipped in the year 2023. As of 2023, the top 12 manufacturers accounted for 85% of this volume, with nine out of the twelve coming from China. That year, 78% of the PV inverters shipped, originated from China.

4.2.2 Makeup of installed capacity in Europe

By analysing available market data, we can characterize the installed capacity of PV inverters in Europe. The analysis covers data from 2015 to 2023. Similar to global trends, Chinese manufacturers dominate the European market, though their dominance is somewhat less pronounced. Figure 14 shows the market shares of the major players in Europe over this period.

Figure 14

PV inverter shipments to Europe over 2015-2023 in GW_{ac} (total 350,000 GW_{ac})



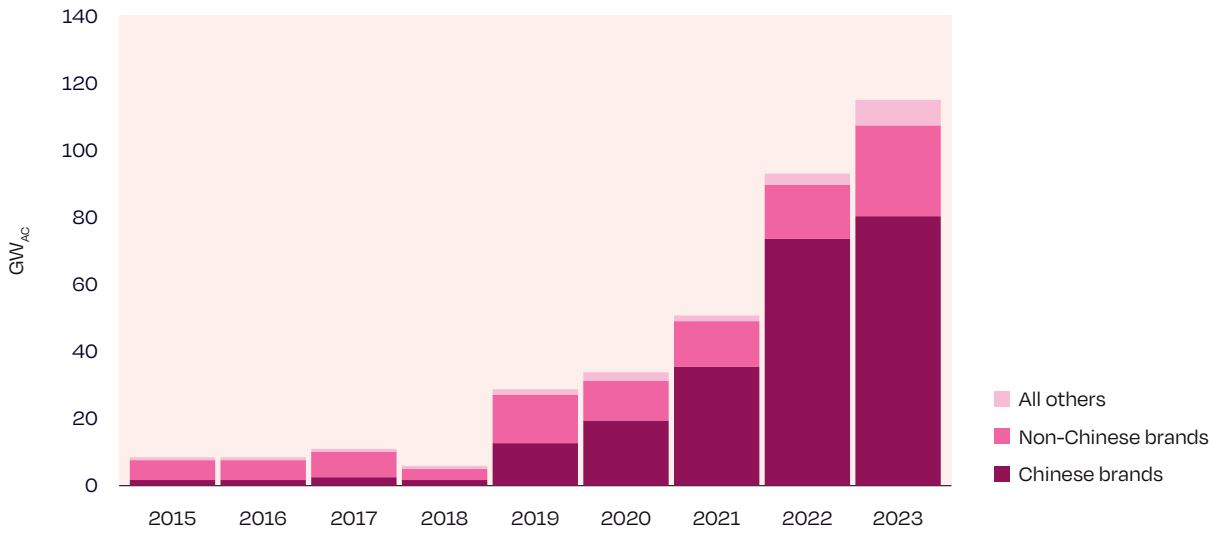
Source: DNV analysis on WoodMacKenzie data

Assuming that each manufacturer has remote access to 70% of their entire installed base, or can send firmware updates, as of 2023, there would be seven manufacturers with the ability to remotely manipulate more than 10GW of generation capacity and 13 manufacturers with expected remote access above 5GW across Europe. It is suspected that a compromise of any one of these companies could have a significant impact on the stability of the grid. The potential impact is analysed and quantified in Section 5.

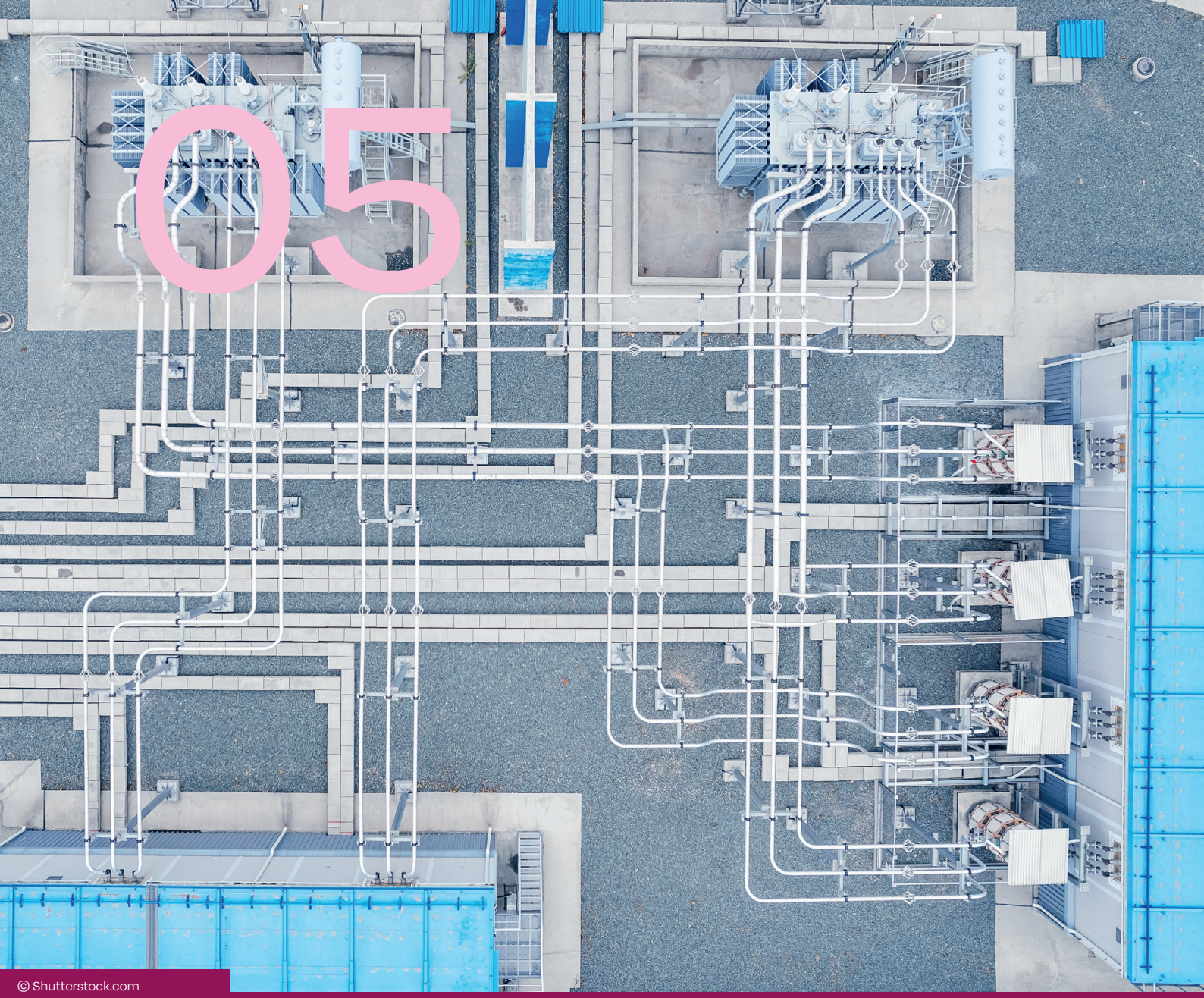
It is also useful to view how the market has evolved during that time. Since 2019, the amount of capacity connected to the grid each year continues to grow. Figure 15 shows this trend.

Figure 15

Total PV inverter shipments to Europe (MW_{ac})



Source: DNV analysis on WoodMacKenzie data



© Shutterstock.com

05

Grid Impact Analysis

5.1 Introduction to the power system impact analyses

The installed PV power in Europe has increased so significantly in recent years that this PV power potentially represents a system-critical factor not only in certain regions but in the entire European interconnected system. This makes it even more important that this PV power, which is distributed across millions of individual units, is operated properly and without manipulation. Various simulations were carried out to characterize the possible system impact of manipulations of PV inverter controls.

First, static system analysis was performed on an archetypical regional power system. Load flow simulations in the transmission grid model for a sudden manipulation of PV production power in the gigawatt range in the local or regional area were performed. These simulations are used to analyze possible line overloads and voltage band violations (overvoltages or undervoltages) in the extra-high voltage levels 380 and 220 kV, as would necessarily lead to countermeasures being taken by the control room personnel during system operation. Next, dynamic analyses are also used to highlight risks to frequency stability, such as those that could occur due to these manipulation in the gigawatt range.

5.2 Scenarios and model base for power system impact analyses

In the first step, specific steady-state load flow simulations at the transmission grid level are of particular interest to highlight the fundamental risks for load flows and system voltages. The archetype region, where installed PV capacity is growing considerably, is chosen as the basis for modelling. The investigations focus in particular on load flow-related overloading of transmission lines and voltage band violations, which can result from manipulation of PV converter controls.

The official grid model used for the steady-state grid impact simulations is the starting grid model of the European Network of Transmission System Operators for Electricity (ENTSO-E) for the 10-year network development plan (TYNDP) in the latest version provided (2022), which includes a complete mapping of the transmission grid level in the planning status for 2030. Even if this model from 2022 doesn't represent the very latest planning of the transmission system, it still represents a fairly useful official data set for the simulations envisaged.

In the frame of this study, ENTSO-E agreed that DNV also applies their latest dynamic model (2024 release) for the synchronous area of Continental Europe. In discussion with ENTSO-E this dynamic model was tested and adjusted to the special study scope. Based on this dynamic model, the frequency stability impact of a sudden more local and a more regional outage of PV production in gigawatt scale was compared, evaluating especially the results for Rate-of-Change-of-Frequency (RoCoF) as well as for the frequency nadir (i.e. frequency drop). In a further step, the possible risk of inter-area oscillation due to PV inverter manipulations was qualitatively discussed.

Due to its sensitive nature, a detailed description of applied assumptions and scenarios (and results) is part of Appendix C of the report. **This information will not be made available in the public version of this report.**

5.3 High-level summary of grid simulation results

Based on the conducted grid simulations, critical system impacts concerning the system stability of the Continental European synchronous area have been identified as a consequence of massive inverter manipulation scenarios. The analysis does show that the European grid is quite resilient against sudden losses of significant amounts of generation, a fact confirmed also by the loss of 2.66 GW of generation after the simultaneous tripping of two nuclear power plants in France in 2023 where the frequency dropped only to about 49.88 Hertz, well above the threshold for triggering automatic load shedding procedures. There are however some scenarios analyzed that may may cause significant grid disturbances with the potential to cause cascading effects due to activation of protection systems of other grid-connected assets.

These are concerns associated with sudden changes in the voltage profile. If large quantities of capacity are simultaneously switched between inductive and capacitive reactive power outputs, the sudden change in system power factor results in rapid swings in grid voltage. It is possible that these rapid changes in voltage trigger nearby protective devices for other larger generators on the rate of change of voltage protection. This may also trigger feeder protective devices at nearby substations. Sudden changes in load and generation profiles can lead to cascading outages. There are mechanisms in place to correct for grid voltages. However, it is unclear exactly to what extent, and how quickly, this would counteract the voltage swings. Efforts to further qualify this potential risk through physical and experimental means are not feasible at scale. Additional analysis could be performed, however, general cybersecurity measures should remain a priority regardless.

Due to its sensitive nature, a detailed interpretation and explanation of the grid simulation results are not available in the public version of this report. They are in part of Appendix C of the report.

© Shutterstock.com

06

Summary of Existing EU Cybersecurity Regulations & Relevant Policies in Other Regions

Cyber risk across all infrastructure has previously been identified as a critical weakness of European and most infrastructure worldwide. Sweeping regulation that strengthens the resilience of European infrastructure, to include first of a kind regulation such as the Cyber Resiliency Act, will provide a great base for essential cyber security requirements, to improve the security of critical infrastructure, including energy. However, these regulations are general and apply to all infrastructure, including telecommunications and manufacturing for example, and therefore do not address more nuanced issues that will remain to be a risk in the energy infrastructure and more specifically in distributed energy resources such as solar. A summary of relevant regulation is as follows.

6.1 Existing EU Regulatory Overview

6.1.1 NIS2

The NIS2 Directive introduces several key requirements to bolster Europe's resilience against cyber threats and ensure a higher level of cybersecurity across critical sectors.

The NIS2 Directive primarily targets sectors that are critical to the economy and society, such as energy, transport, banking, and healthcare, among others. While it does include new sectors like ICT service management, it doesn't specifically mention DER system deployments. However, if a DER installer provides services that fall under the broader categories of critical infrastructure, they might be indirectly affected.

The applicability of NIS2 depends on factors such as the size of the business, the nature of the services provided, and the criticality of those services. In general, however, requirements are applied directly to the operators of critical infrastructure as strictly defined under the directive and nation state regulation. All other service providers are then indirectly impacted through requirements passed by through supply chain security measures.

The main areas addressed are:

1. **Risk Management:** Organizations must implement measures to minimize cyber risks, including incident management, supply chain security, network security, access control, and encryption.

2. **Corporate Accountability:** Management must oversee and approve cybersecurity measures, receive training on cyber risks, and address these risks. There are penalties for non-compliance, including potential liability and temporary bans from management roles.

3. **Reporting Obligations:** Entities must have processes for promptly reporting significant security incidents. This includes specific notification deadlines, such as a 24-hour "early warning"

4. **Business Continuity:** Organizations need plans to ensure business continuity during major cyber incidents. This includes system recovery, emergency procedures, and setting up a crisis response team.

5. **Baseline Security Measures:** Essential and important entities must implement security measures like risk assessments, security policies, cryptography, incident handling, and employee training.

6.1.2 EU Cyber Resilience Act (CRA)

The EU Cyber Resilience Act (CRA) applies to all products with digital elements that are sold within the European Union. This includes hardware, software, and services that have a digital component. The goal is to ensure that these products meet stringent cybersecurity standards throughout their lifecycle, from design to disposal.

The EU Cyber Resilience Act (CRA) applies to installers as well. The CRA covers all products with digital elements, including their installation and maintenance. This means that installers must ensure that the products they install comply with the CRA's cybersecurity requirements and that they follow best practices to maintain the security of these products throughout their lifecycle. (Article 13, 14) The CRA officially went into effect in December of 2024 and therefore the CE marking and compliance with cyber security requirements will become applicable in December 2027 with reporting requirements starting in September 2026.

Key Requirements from CRA are:

1. **Secure by Design:** Ensure that all products are designed with robust cybersecurity measures from the outset. This includes secure coding practices, regular security testing, and vulnerability assessments.

2. **Lifecycle Security:** Maintain cybersecurity standards throughout the product's lifecycle. This involves regular updates, patch management, and continuous monitoring for new vulnerabilities.

3. **Risk Assessment:** Conduct comprehensive risk assessments to identify potential security threats and implement appropriate mitigation strategies.

4. **Transparency and User Information:** Provide clear and transparent information to users about the cybersecurity measures in place. This includes detailed documentation and user guides on how to maintain security.

6.1.3 Network Code on Cyber Security

The EU Network Code on Cybersecurity (NCCS) for the electricity sector builds on the NIS2 Directive by providing additional, sector-specific guidance to enhance the security of cross-border electricity flows. It requires risk management, incident response, and information sharing for TSOs, DSOs, and major generators. A core component of the NCCS is the Electricity Cybersecurity Impact Index (ECII), which enables competent authorities to classify entities by cyber risk, ensuring stronger protections are applied for high-risk entities.

The code mandates risk assessments, the development of security policies, and the implementation of technical and organizational security measures, including access control, encryption, and supply chain security. Incident response planning and reporting are also critical, with a strong emphasis on information sharing among stakeholders to enhance collective resilience. Furthermore, the NCCS promotes collaboration between ENTSO-E, the EU DSO Entity, and ENISA, fostering a unified approach to cybersecurity across the EU. Compliance is enforced through conformity assessments, market surveillance, and potential penalties, ensuring adherence to the code's requirements.

Key elements of the NCCS are:

- **ECII risk classification:** Ensuring the level of controls applied are proportionate to the entities risk profile.
- **Mandatory incident reporting:** Enables rapid response and better awareness across the industry.
- **Supply chain security:** Addresses vendor and third-party risks.
- **Strict remote access rules:** Limits unauthorized access.
- **Cross-border cooperation:** Ensures unified EU defense.
- **Asset management requirements:** Ensuring all critical assets are identified and protected.
- **Vulnerability management processes:** Requiring timely patching and mitigation of known security flaws.

6.1.4 EU General Data Protection Regulation (GDPR)

This EU regulation focuses on data protection and privacy for individuals within the European Union and the European Economic Area. It also addresses the transfer of personal data outside these areas. GDPR sets strict guidelines on data handling, requiring organizations to ensure data privacy and security, and to report data breaches within 72 hours.

Although the DER ecosystem must comply with GDPR, a data confidentiality incident would not directly affect grid operations. However, the GDPR framework may serve as a useful guide in determining the eligibility of storing and processing data and applications in jurisdictions outside of the European Union.

6.2 Residual Risk Profile with Exiting Regulatory Controls

While the current EU cyber regulations, such as CRA, NIS2, NCCS, and to a lesser extent GDPR, provide comprehensive frameworks for securing system integrity and availability, they do not address all potential risks, leaving some areas exposed to emerging threats. Some specific examples of regulatory shortcomings are provided in Table 6 while the residual risk profile of the industry, after the implementation of existing regulation is provided in Table 7.

Table 6

Summary of Gaps in Existing EU Cyber Regulation

Issue	Consequence
Under the CRA, DER systems are currently considered as default and therefore not classified according to their security risk.	DER systems are not secured according to their risk posture and do not require third party audits and verification of security controls to assure compliance.
The security governance operating model cannot effectively be applied to residential and C&I DER.	No clear security accountability and responsibilities during system life cycle.
Consumers are generally unaware of security risks and use insufficient cybersecurity hygiene for their residential and C&I DER .	Consumers do not contract through professional services and often use poor security hygiene such as default passwords and insecure configurations unless the system comes secure by default by the manufacturer.
No EU cybersecurity standard specifically addresses the complete DER system with the local assets and its connectivity to IT/cloud infrastructure.	Insecure configurations and use of APIs, cloud platforms and channels to operate DERs.

Table 7

Risk Matrix with Residual Risk after Existing Controls

Threat	Risk Level	Existing Mitigations	Residual Risk
Compromise of Device, Application, or Physical Infrastructure			
Gain Unauthorized Access through Vulnerabilities in Authentication Mechanisms.	High	CRA default classification w/ self attestation	Medium
Tampering Inverters Through API's.	High	The end-to-end security of the infrastructure and management platforms is not ensured and third party attestation is needed to ensure risk is necessary to guarantee cyber risk is adequately addressed.	Medium
Direct Access to Inverter Through Intentional and Non-intentional Backdoor	Medium	CRA default classification w/ self attestation	Medium
Destruction or Compromise of Physical Infrastructure	High	CRA default classification w/ self attestation	High
Compromise via Supply Chain **without** Vendor Support – Rooftop			
Control Inverters through Compromise of Third Party Access Rights	High	Most 3rd parties will be regulated only indirectly through supply chain security measures. CRA requirements for "secure by default" implementations should address some concerns of password security and least privileged access.	Medium
Control Inverters through Compromise of Manufacturer Access Rights	High	Manufacturers will be regulated indirectly through supply chain security measures.	Medium
Control Inverters through Malicious Firmware without Vendor Support	High	Manufacturers will be regulated indirectly through supply chain security measures.	Medium
Compromise via Supply Chain **without** Vendor Support – Utility Scale			
Control Inverters through Compromise of Third Party Access Rights	High	Specific security controls applied to PV installations considered "critical infrastructure" are expected to considerably restrict unauthorized access to inverters.	Medium
Control Inverters through Compromise of Manufacturer Access Rights	High	Requirements for access management and other security controls are anticipated to be in place for nearly all utility scale plants after the implementation of NIS2 and the improvement of procurement and management practices by the relevant stakeholders.	Medium
Control Inverters through Malicious Firmware without Vendor Support	High	Manufacturers will be regulated indirectly through supply chain requirements from the owners and operators of critical infrastructure. Therefore, there will continue to be a general improvement in manufacturer cyber security practices that will also include software development best practices.	Medium

Table 7

Risk Matrix with Residual Risk after Existing Controls *continued*

Threat	Risk Level	Existing Mitigations	Residual Risk
Compromise via Supply Chain **with** Vendor Support – Rooftop			
Control Inverters through Malicious Firmware with Vendor Support	High	Non-EU manufacturers are not subject to regulatory oversight and there are mechanisms required to ensure that firmware development is done in a secure way or checked and verified prior to installation.	High
Direct Control of Inverters through Vendor Access Rights	High	Non-EU manufacturers are not subject to regulatory oversight. Additionally, in most rooftop PV installations, direct access by the manufacturer is possible without any intervention with the local grid balancing authority or another party.	High
Compromise via Supply Chain **with** Vendor Support – Utility Scale			
Control Inverters through Malicious Firmware with Vendor Support	High	Non-EU manufacturers will be subject to supply chain security controls, however, the controls may be circumvented or ignored by the vendor if coerced to do so by their respective governments. Plants may implement roll back capabilities with the ability to sever communications with third parties, however this is not a regulatory requirement and not anticipated to cover all scenarios.	High
Direct Control of Inverters through Vendor Access Rights	High	It is anticipated, that under NIS2, controls will be more routinely in place that more tightly control remote access from all third-party service providers. However, this is not an explicit requirement and therefore likely to still be a systemic issue in many PV plants.	High

6.3 Relevant Policies in Other Regions or Industries

This section highlights several policy or industry efforts that may serve as a pilot for European solar actions. Several EU countries are progressing on cybersecurity policies for solar PV. A deeper analysis would shed light on potential elements that can be replicated at the EU level.

Germany's approach to demand response and solar curtailment

In Germany, smart metering infrastructure has been used as the backbone for critical communications for remote control of grid-edge assets. Critical communications to be used to curtail loads for demand response for example are to be secured through the communication channel to the smart meter infrastructure. This requirement is a part of new legislation under the EnwG 14a law that requires grid operators to make smart meter infrastructure available to end-users and to start implementing systems that can then curtail loads to improve grid stability. This infrastructure is owned by the local grid operator and is managed by them or a regulated and authorized third party that has proven they meet certain cyber security requirements. Strict requirements also exist for the implementation of the smart meter communication gateway. The implementation of this infrastructure is ongoing and may serve as a proof of concept for securing communications to residential and small commercial installations across Europe.

The issue however remains that only loads can be controlled and therefore in scenarios with low demand and high solar output, overproduction and high grid voltages are possible. Recent legislation was introduced to in February of 2025 to address this under the Solarspitzengesetz (Solar Peak Law) that incentivises owners of PV under 100kW to use storage solutions and adds requirements for PV over 100kW to include means of remote control to allow for the future curtailment of such plants in times of high production.

Lithuania's Wind and Solar remote control cybersecurity law

Article 733: Security Requirements for the Control Systems of Electricity Devices" will prohibit manufacturers from countries it deems as high risk from accessing the systems they provide that connect to the grid and exceed 100kW. This includes Chinese inverter manufacturers and their access to rooftop solar over 100kW. New installations will be required to follow this new law in May of 2025 while existing systems will be required to comply by May of 2026.

The law does not ban the sale or installation of these components in Lithuania. It only impacts the remote access the manufacturer has to make changes, perform remote maintenance, and to directly perform updates without including a third party service provider.[9]

China's Multi-Level Protection for Cyber Security (MLPS) regulation that limits remote control of critical energy systems for cybersecurity reasons

Under the Chinese national cyber security law (CSL), the MLPS is defined and requires organizations to implement a level of security controls that aligns with the criticality of those systems and organizations on a scale from 1-5. Critical Information Infrastructure Operators (CIIOs) are also clearly defined and must comply with additional cyber security requirements.[10]

The regulation includes requirements such as cloud service providers must use data centers based in China. There are also specific requirements for industrial control systems that cover the cyber security controls and are applied proportionately based on the risk profile of the system or entity.

Taiwan's push for energy independence and resiliency

Taiwanese energy infrastructure has faced repeated cyber-attacks originating in China with increasing frequency. In its unique position, Taiwan has pushed for an independent energy system that is however still very dependant on imported coal.[11] As a result of geopolitical tensions, there has been a push to prohibit or strongly deter the use of Chinese made products in Taiwan. One such example is the recent prohibition of the use of Chinese made large language model DeepSeekAI, as was announced by the Taiwan Ministry of Digital Affairs (MODA).[12]

South Australia Power Networks Consumer Energy Resource (CER) compliance program

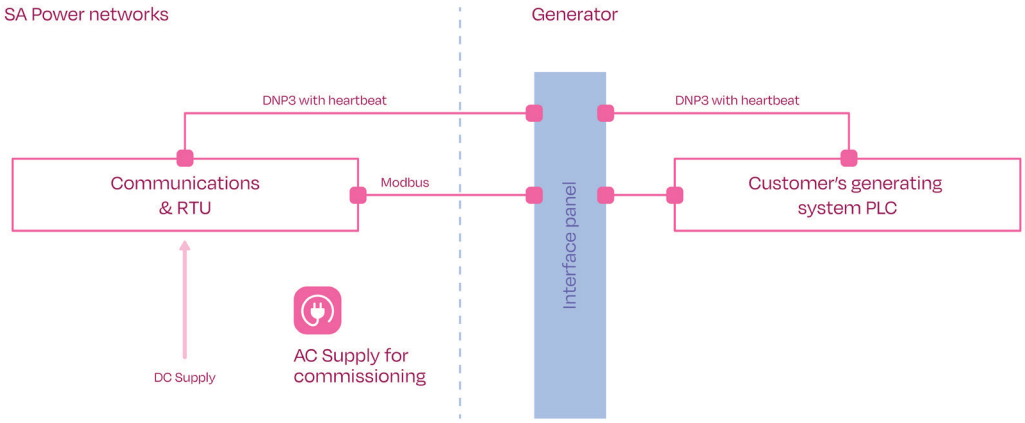
Australia has a world leading level of solar integration as part of the generation mix and realizes the importance of securing their installed generation capacity. A major component of their approach includes the requirement for consumer owned Small Embedded Generation (SEG) to be compliant new regulations and SA Power technical standard TS-129.[13]

Additionally, SA Power requires each installer to ensure the rooftop PV can interface with the SA Power communications network via an SA Power owned communications gateway that is installed at each site. Details for the installation are included in SA Power Technical Standard 134 "Communication Systems (inc. SCADA) for Embedded Generation". The details for the interface are shown in Figure 16.[14]

Figure 16

Block Diagram of SCADA/Telecommunications solution for generating systems without inter-trip

Customer's Site



Source: DNV

TikTok proposal to host US user data only on Oracle cloud within the US

Under pressure from the US government, Tik Tok, a Chinese based social media platform owned by ByteDance, agreed to store American user data only in a trusted Oracle cloud service and over time delete user data from their own data centres located in the US and Singapore. Pressure from the US was a result of concern over the potential threat to national security posed by the company's country of origin.[15]

United States prioritizes security of the digital grid ecosystem

The previous US administration under President Biden were taking proactive steps to securing the U.S. power grid against cyberattacks focused on the rapidly expanding clean energy sector. Recognizing the increased digital integration of modern energy resources, the administration prioritized cybersecurity in critical technologies like batteries, inverters, distributed control systems, building energy management systems, and electric vehicles. In a press release from the White House,[16] key initiatives were outlined such as the establishment of the Energy Threat Analysis Center (ETAC), development of robust standards such as Securing Solar for the Grid (S2G) or other industry standards such as UL 2941

Not named in the release is also the development of UL 2941 "Standard for Cybersecurity of Distributed Energy and Inverter-Based Resources"

European bans use of Chinese made 5G network equipment in core communication infrastructure

In Europe, guidance for risk assessments under the 5G toolbox was used by each member state to make decisions to secure their critical communications infrastructure. As a result, nearly half of European member states, and many other countries worldwide, have banned the use of Chinese made 5G telecommunications equipment in their core national communication infrastructure.[17] The bans come amid allegations that Chinas National Intelligence Law gives the Chinese government the power to mobilize individuals and organizations to carry out espionage on behalf of the government.[18]

Central collection and monitoring of inverter data in Hungary

Hungary has recently started to set up the infrastructure to collect various information on all rooftop solar installations across the country and aggregate it in a central state-owned data center. Information collected includes nameplate information, energy created, energy used, and other electrical parameters.[19] While the information is useful for grid operators, there are concerns raised about customer data privacy and billing or financial concerns. Although the concerns are likely easily addressed through proper controls and maintaining the use of existing meter infrastructure for billing and payment.

Romania to introduce mandatory cyber audit for solar power plants

Romania's Ministry of Energy drafted an executive order mandating cybersecurity audits for solar power plants to prevent cyberattacks on the national power grid. This order requires periodic audits of inverters and IT components in photovoltaic systems. This is a measure designed to protect the national infrastructure against digital vulnerabilities, given the risks related to imported equipment and their potential to transmit data to state and non-state actors hostile to Romania without the consent of the operators. The proposed decree aims to establish a sustainable framework for energy storage development, strategic electricity production projects, and cybersecurity measures for photovoltaic systems. Minister of Energy Sebastian Burduja emphasized the urgency of the energy transition, highlighting the need for investments in energy storage and hydropower projects to enhance energy security.[20]

© Shutterstock.com

07

Recommendations to Ensure a Cybersecurity Baseline across the Solar Industry

This section outlines the recommendations to address the residual risk to the solar industry to protect against evolving cyber threats. These recommendations are based on established best practices and draw from the SolarPower Europe Position Paper "A harmonized Cybersecurity Baseline for Solar PV" and draft requirements in the latest version of the Net-Zero Industry Act. The recommendations span across three critical domains: protection, detection, and recovery. These subsections will provide actionable strategies to mitigate risks, identify intrusions, and ensure swift restoration of operations, reflecting the industry's need for a robust and layered cybersecurity defense. Finally, the recommendations are mapped to the risk matrix to ensure risk levels are reduced to an acceptable threshold.

7.1 Minimum Requirements for a Secure Solar Baseline

Securing solar infrastructure requires several key elements:

- All solar infrastructure from end-to-end is developed, configured and managed securely with the support of all stakeholders (vendors, manufacturers, operators, owners, etc.)
- Remote access and control of infrastructure is managed and maintained within the EU and other secure jurisdictions
- The infrastructure is capable of swift containment and recover in the event of a cyber incident.

7.1.1 Increase End-to-End Cybersecurity Requirements Across the Industry

The first and most critical step to providing a secure and resilient distributed generation source is addressing the security of the infrastructure itself. Insecure password practices and other basic cyber security practices are common across most industrial infrastructure. These recommendations outline the methods that will ensure the essential cyber security practices, such as stronger access control and secure configurations, are more common across solar infrastructure:

7.1.1.1 Develop Industry Guidelines to Align with CRA Requirements

The CRA requires that for devices listed as critical products, an industry specific guideline be available to evaluate components against that aligns with the requirements listed in the CRA. This guideline does not currently exist and must be developed.

Assessment of products against this guideline would be required for any inverter that is to be sold in Europe. The requirements within the CRA are limited and do not address all device and infrastructure risks, however this still significantly improves the security of installed infrastructure. To address the remaining vulnerabilities identified in the end-to-end command and control of the PV installations, additional controls would be needed. These may be included in the guideline as advanced controls or may be included in a separate guideline describe in chapter 7.1.1.2.

7.1.1.2 Develop Industry-Specific Guidelines for End-to-End Security for Small-Scale PV Installations

To build on the essential requirements of the CRA and provide more timely guidance, further security controls are needed to ensure the security of the full system. This includes command and control infrastructure, web applications, third-party software, etc. The recommended practice would build on existing standards such as NIST IR 8498, UL 2941, IEEE 1547.3, and others and provide comprehensive guidance that addresses the remaining security gaps identified.

Further research will be necessary to identify the remaining security gaps. However at a minimum, it is likely to include:

1. Secure network and cloud architecture
2. Security and access control for management portals with a recommendation to use web application firewalls
3. Education and awareness information for installers and homeowners regarding cybersecurity-relevant information such as how and when to disable certain features, password security, and other relevant controls
4. Recovery and rollback capabilities

7.1.2 Limited remote access from outside of the European Union

Remote access from outside of the European Union should be restricted to only be from jurisdictions with similar risk profiles and where cyber security of the infrastructure used can be assured. As part of the risk assessment and mitigation process, competent authorities should limit remote control by stakeholders outside the EU's jurisdiction unless they are based in secure jurisdictions with strong enforcement. High-risk entities may then develop solutions, subject to approval by the competent authorities, to adequately manage the cyber risk. A similar approach is explored in Lithuania, where high-risk entities are asked to rely on third-party providers for remote maintenance and updates.

There are various options to implement this requirement. An indicative list is presented in chapter 7.1.4. Beyond these measures, a commonly discussed solution is to separate hardware from software. This would allow hardware from all over the world while relying on software from the EU or equivalent secure jurisdictions.

7.1.3 Host Data and Applications in Secure Jurisdictions

Given the escalating cybersecurity threats targeting critical infrastructure, it is imperative to also ensure physical IT infrastructure that hosts sensitive data and control applications is located in the EU or other secure jurisdictions. While current EU regulations indirectly encourage this through risk management and data security principles, they fall short of explicitly mandating the use of secure jurisdictions. Additionally, there is no single entity currently responsible for risk ownership of rooftop solar installations. This ambiguity, coupled with the prevalence of hosting data and remote management applications in jurisdictions that are considered potentially less secure, exposes critical infrastructure to significant vulnerabilities. GDPR includes guidance on hosting data within the European Economic Area and includes additional countries with adequacy decisions considered to be secure enough to also host data that may be sensitive. Additionally, a global precedent has already been set where nations increasingly prioritize data sovereignty and restrict foreign hosting of critical infrastructure data, such as through China's Cybersecurity Law, Lithuania's Article 733, and the EU's own Net Zero Industry Act.

Therefore, it is recommended to implement a regulatory framework that explicitly requires the storage and processing of all operational PV power plant data, including rooftop solar and other DER. In particular, real-time data influencing grid stability or information that characterizes the grid and connected generation assets, should be hosted within EU-based data centers or secure, equivalent jurisdictions. This measure will reduce the risks associated with data theft, manipulation, and unauthorized access, improving the integrity and reliability of Europe's energy infrastructure.

7.1.4 Technical Barriers to Ensure Secure and Resilient Remote Control

The need to remotely control and update PV and similar DER is critical and will be necessary to maintain grid balance as solar continues to provide a larger percentage of the generation mix. Efforts are already underway to improve the controllability of solar and other DER through regulatory actions such as the Network Code on Demand Response and many national regulations. For example, Germany's EnWG §14a and the more recent Solarspitzengesetz (Solar Peak Law) outline requirements for the remote control of large loads and solar installations above 100 kW.

This section provides recommendations to ensure the security and resilience of this control will be maintained and help ensure a unified and homogenous approach is taken across the EU, In particular, the risks associated with the remote access capabilities of stakeholders not subject to direct oversight by national competent authorities are addressed.

Barriers must be in place to address three primary concerns related to remote influence over the output of the inverter. These include:

1. Remote changes to the operating mode
2. Remote changes to the setpoints of configuration parameters
3. Updates to the software/firmware that impacts the electrical output characteristics and device functionality

7.1.4.1 Require Trusted Execution Environments in the Hardware

The application of firmware and software updates are critical to patch vulnerabilities in products and to make fixes and improvements to device functionality. However, updating a device with malicious software is also a cyber security risk. Basic patch management and application of updates is covered under the requirements of the CRA. However, for critical functions in the inverter, such as processes that impact the power output, require additional security controls such as Trusted Execution Environments.

Such additional controls would likely require modification of the hardware and may be enhanced with other mechanisms such as Hardware Security Modules (HSMs), which are commonly used in smartphones and other industries with extremely high security standards. With such an implementation, critical processes may be protected within the trusted execution environment and would not be impacted by even intentional malicious updates.

Other approaches to ensure update integrity may be considered, however, for routine and timely security relevant updates, third-party escrow review is not considered an effective technical barrier. The effort required to review each release requires a lot of additional effort and resources which results in added costs and slows the release of critical security patches. Additionally, malicious code and backdoors may be hidden and missed by code review through obfuscation.

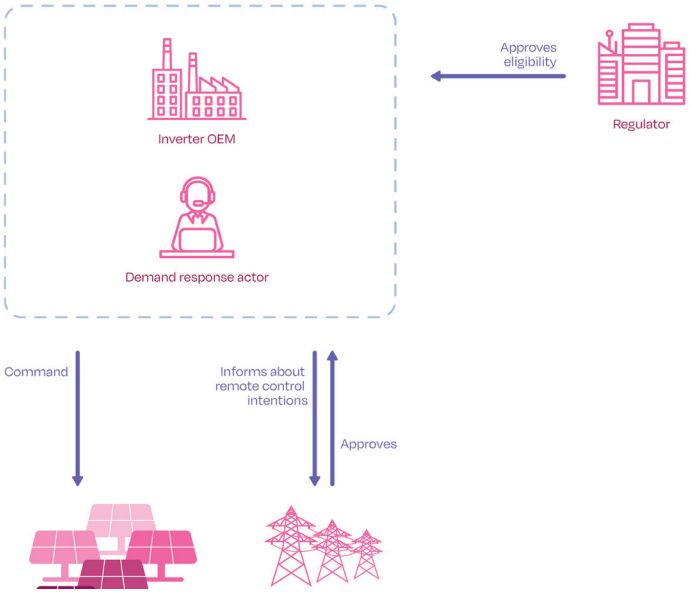
7.1.4.2 Introduce Regulated Intermediaries for Secure Communications and Control

The previous section provides a technical control for managing risk through patches. The introduction of a regulated intermediary addresses the risk associated with remote changes to operating mode or configuration settings. A secure approach to protecting the remote access to critical capacities of rooftop solar, is to mandate the control and access of critical functions through a regulated operator of critical infrastructure. This regulated and trusted entity would serve as the barrier between the inverter and less secure, unregulated entities. Such an operator would serve as the supplier of the aggregated generation resource that may participate in the energy market and therefore also carry the requirement to ensure the stability and security of their resources. The regulatory approach for enforcement of this concept is outlined in Section 7.2.2.

Critical actions would include the ability to start, stop, and adjust active and reactive power. These functions would only be available to the operator and may require input or permission from the local grid operator to apply. A similar approach has been to some extent already implemented in Germany. The regulatory framework is in place and the implementation is currently underway. Figure 17, from the SolarPower Europe position paper, illustrates how the DSO approves control commands by the demand response operator before changes to the grid may be made in order to preserve stability.

Figure 17

Workflow for Approval of Remote Control of PV in Germany

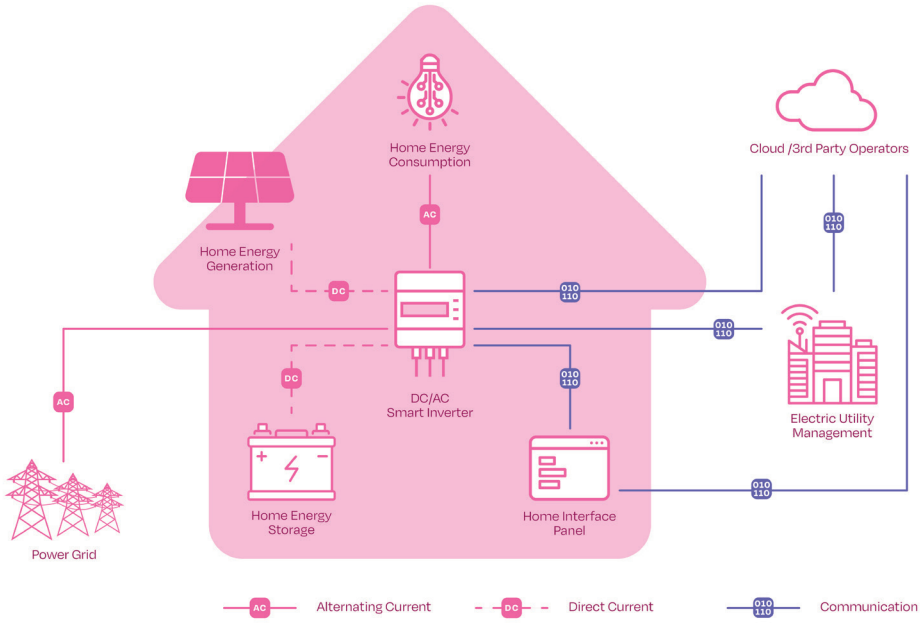


Source: DNV

Non-critical access may still be allowed in this scenario. Non-critical functions would include performance monitoring, software updates, and similar functions. These could be managed by non-regulated parties; however, it would then be necessary that this communication channel be capable of suspension by the operator in the event of a compromise or other scenario the dictates the need to operate in a more secure "safe" mode. The various communication types can be seen in Figure 18, from NIST Interagency Report 8489. Communications would be handled through a single secure communications gateway which is managed by a regulated body such as the DSO, VPP, or supplier. This is like Germanys approach of using the smart meter gateway for control of demand response, control of rooftop solar in Australia through a secure communications gateway owned by the grid operator, and in the US in states such as California under requirements of Rule 21 that require the certification of inverters against standards for device operation and security of the communications. The process of establishing and managing these communications may be automated which reduces the burden of management and allows for a secure method of remote connection.

Figure 18

NIST IR 8489 Architecture for Smart Inverters



Source: DNV

In most instances, new infrastructure would be needed at each installation that includes a managed communications gateway and supporting business infrastructure and processes to manage the responsibility. Technology exists on the market, such as those now being implemented in Lithuania, following the ban of remote connections by high-risk entities.

Germany has already started to require DSOs to manage demand response through Smart Meter Gateways in response to regulation EnWG 14a ("Netzorientierte Steuerung von steuerbaren Verbrauchseinrichtungen und steuerbaren Netzanschlüssen" / "Grid-oriented control of controllable consumption devices and controllable grid connections"). The implementation of 14a is ongoing, as well as the rollout of the smart metering infrastructure. The requirements are, however only for controllable loads and do not include the inverters. However, the same infrastructure may also be used to manage the secure communications with the inverters and other generation sources as well. This has the benefit that the infrastructure installed for secure communications is managed either directly or indirectly by the system operator, thus ensuring cyber due diligence in the procurement and installation.

The exact approach must be made at the member state level as in many instances, for example in Germany, which includes more than 800 small municipal utilities, many of whom have a staff of less than 500, the additional burden would be unmanageable. A free market participant, such as an aggregator, could more quickly adapt to manage the responsibility, but legislation would be needed to define the specific requirements for the management of such risk and in which scenarios this should apply, for example only when the PV installation is network connected and capable of exporting power onto the grid.

7.1.5 Improving Resilience in the Event of an Attack

The previous measures have contributed to the protection of critical infrastructure. Effective cyber risk management however also includes measures for the response to and recovery from a cyber-attack. This point is clearly shown by the structure of most cyber security standards, such as the NIST Cyber Security Framework which includes Identify, Protect, Detect, Respond and Recover. Response and recovery are also a focus of existing regulation. Specific guidance for the solar industry exists in guidelines such as IEEE 1547.3, however there are no regulatory requirements which enforce such mechanisms across the industry.

7.1.5.1 Enhancing Early Detection of Cyber Incidents through Enabling Logging of Security Related Events for Later Integration with Monitoring and Detection Efforts

The first critical element of response to a cyber incident is the early detection of the event. Several efforts are ongoing at various levels to provide increased visibility and information sharing across the EU and energy industry. To support this effort, PV owners, operators and manufacturers should also support these efforts. Additional research is needed to determine the most effective approach for enhancing early detection capabilities and how to best integrate the PV industry into those efforts. Many TSOs and larger DSOs have already begun to integrate DER into existing detection and monitoring efforts. There are other higher-level efforts such as through information sharing organizations like EE-ISAC or country organizations that aggregate data from multiple organizations, such as the Danish SektorCert, and private companies that aggregate data across multiple organizations to improve early detection efforts.

Regardless of the specific approach, immediate steps may still be taken to enable better security related detection and monitoring. Logging of security related events is still uncommon in many devices. As part of the develop of NIST IR 8498,[21] five inverters were analyzed to determine their ability to support certain cyber security best practices. Of the five inverters tested, only one supported the ability to log security related events. Therefore, as part of efforts to improve the security of devices, additional requirements for security logging should be included so this data may be used in the higher level detection efforts.

7.1.5.2 Limiting Attack Impact Through Decentralized Control of Grid Connected DER with Export Capabilities

The first and most critical response to a cyber incident is to contain the incident and limit the impact of the attack. Common practice is to segment communication networks and include security controls between segments. A similar approach is also applied in traditional engineering of any structure in the event of a fire. The same concept should be applied to the control of critical infrastructure.

Many use cases exist that must be addressed to prevent the sudden loss of a large capacity of generation. Several recommendations related to reducing the impact of a single compromise include:

1. **Aggregated capacity limits** – Traditional generation plants generally do not exceed 1.5GW. The control and operations for each plant is isolated from other plants, including those owned and operated by the same organization. Therefore, there has traditionally been a natural limit to how much capacity can be controlled from a single control system. To maintain this level of redundancy and segmentation in the generation mix, it is recommended to impose an aggregated capacity limit for a single control system or control center. Organizations may operate a total capacity above the determined threshold; however it should be required to do so with isolated systems with not interdependencies or common cause failure mechanisms.

2. **Segmentation of manufacturer access** – Vendors maintain access to enough installed capacity of their own inverters to cause significant disruptions. If this access is abused by an insider threat, or the organization is compromised, technical controls shall already be in place to inhibit the simultaneous control of capacity up to a threshold that is yet to be determined. This may include the segmentation of networks, command and control servers, and segmentation of

cloud applications. The specific mechanisms should be determined by the manufacturer and be included in part of their risk mitigation plans for addressing cyber risk.

3. **Batch application of firmware updates** – As is common practice in most industries, the application of updates to a running system should be done methodically and systematically. Technical controls should be in place to prohibit the sudden update of all inverters simultaneously to allow time for human intervention in the event the update fails or is found to be malicious or unauthorized.

4. **Intentional random time delays in some controls** – grid analysis shows that the sudden and simultaneous loss of generation is the worst-case scenario. With an intentional time delay, the power transients in a local region are offset and therefore the cumulative impact is reduced. This approach however should be handled through standards that develop the technical and engineering controls to ensure that all power system impacts from an engineering perspective are accounted for.

7.1.5.3 Backup Contingency Operations Plan

The final control is the recovery of a system after the incident. To enable an effective recovery, the system must be designed in such a way that allows and simplifies this effort. The exact recovery procedure will depend on local conditions and therefore must be determined by the responsible entities such as the local grid operator and the PV operator. However, certain functions and activities may be implemented now that are relevant for every scenario. These include:

Require Relay Protection Devices for safe shutdown in the event of a compromise EU countries should mandate relay protection devices, which provides additional protections at the installed facility and local grid and is independent of the software and therefore not vulnerable to compromise. A relay protection device is an electrical safety device used in power systems to monitor parameters like voltage, current, and frequency. When it detects abnormal conditions—such as short circuits, overvoltage, undervoltage, or frequency deviations—it triggers protective actions, such as disconnecting a circuit or isolating faulty equipment, to prevent damage and ensure grid stability. These devices are commonly used in substations, transmission lines, and generation plants to protect electrical infrastructure.

In some instances, a complete and total shutdown is desired for safety reasons. Some theoretical attacks include those that could pose a fire risk for the installation. It is therefore recommended that it become standard practice to include a electrical protective device on the input and output of the inverter that can shut down the system in the event that the electrical parameters are out of specification. Additionally, it may also be desired to enable such a safe emergency shutdown in the event of a cyber-attack. The addition of this feature could potentially add an additional target for an attacker, however, if normal shutdown of the device is also possible through remote access, this safe shutdown mode would not result in a more vulnerable system. Finally, the safe shutdown mode provides additional protection against non-malicious failures such as software errors or component failures.

Enable the disconnection of all communications and set an emergency mode for operation
In the event of an attack, or in the scenario where the output of the inverter is unpredictable, to ensure grid stability, it would be useful for the system operator or entity responsible for the secure communication to have some mechanism to force the invertor to a predictable output. The specific output may vary from region to region. Additionally, all communications should be able to be severed to prevent infection of new devices that are not yet impacted. This practice is common in other industrial environments for example when the IT infrastructure is subject to a ransomware attack, the operational technology may be completely severed from the infected network to preserve the operating status of the plant.

The function would also be useful for utilities in the event of a “black-start” when the grid must be restored after a complete outage.

Enable backup of configuration and settings to a separate location and capability to restore from backup If the firmware has been, or was suspected of being compromised, the corrupt firmware will need to be removed. For industrial control systems and nearly all IT systems, it is common practice to restore from a trusted backup. As part of the backup process, the main system firmware and software is installed followed by all relevant settings and configuration files. However, as noted in the testing results in NIST IR 8498, only one of the five inverters supported this function.[21] Therefore, each inverter would require a technician to recommission the system and manual update the desired settings. Often, the configuration of rooftop solar is not documented further complicating bringing the PV back into operation. Additionally, this process would likely be carried out in mass and therefore effort should be taken to make the process as simple as possible and support the ability to do so through secure remote mechanisms.

In some instances, the trustworthiness of the available backup may be in question. For example in the event an intentional backdoor in a product is found, conflict between the EU and the country of origin for a particular manufacturer, or other scenarios may trigger the need for further verification to trust the integrity of the backup. Therefore, it is recommended for manufacturers outside the European Union or secure jurisdictions, the source code for the latest major version release be made available to a third-party escrow agent, capable of code review. Triggers for release of the code may be agreed upon that only include such significant scenarios as previously mentioned, as to protect the intellectual property of the manufacturer.

7.2 Enforce Requirements via the EU's Policy Framework

7.2.1 Develop Industry-Specific Guidance for End-to-End Cybersecurity

Immediate action should be taken to ensure the timely development of the guideline introduced in Sections 7.1.1.1and 7.1.1.2. A body of cybersecurity experts should detail the requirements in chapter 7.1 to facilitate compliance. This should be done within the next three years. Development of the standard by a traditional standards organization will likely not deliver timely results. The authority for development of and publishing of the guideline requires further discussion that includes manufacturers, service providers and system operators.

The final guideline may then serve as a basis to show compliance with the unique industry specific requirements for procurement of generation sources from rooftop solar and similar DER. Reliance on existing general cyber security standards , such as ISO 27001 or IEC 62443, and even existing industry specific guidelines, such as IEEE 1547.3, do not provide enough guidance on the end-to-end infrastructure and therefore would result in a heterogenous landscape that is more difficult to manage and is less interoperable across device manufacturers and national regulation.A full guideline may be developed that includes an annex that aligns with the minimum-security requirements of the CRA that may be used as a basis for CRA certification.

7.2.2 Enforce a Cyber Security Baseline through Supply Chain Requirements in the Network Code for Cyber Security

There exists a significant number of stakeholders that are not governed by existing cyber security regulation. These stakeholders, such as large installers, suppliers, manufacturers, and third-party service providers often have remote access to capacities that exceed the critical thresholds often determined by members states to be relevant for regulation under NIS2 (104MW in Germany for example). The risk therefore remains that this access, although secured at a technology level, will continue to exist since the organization itself is not subject to oversight and audit by local competent authorities. These stakeholders will be unlikely to fall under the strict definitions for operators of critical or important infrastructure under NIS2.

However, under the NCCS, these stakeholders may fall under the supply chain requirements for critical electricity undertakings. This would allow tackling this issue swiftly. National Competent Authorities may identify electricity undertakings, such as grid operators or suppliers, which compensate grid exports of PV-generated electricity as critical entities via the risk assessment processes foreseen under Article 24. PV installations would then be part of the supply chain for the electricity undertakings.

> 3. Each competent authority may identify additional entities in its Member State as high-impact or critical-impact entities if the following criteria are met:
>
> a. the entity is part of a group of entities for which there is a significant risk that they will be affected simultaneously by a cyber-attack;
>
> b. The Electricity Cybersecurity Impact Index (ECII) aggregated over the group of entities is above the high-impact or critical-impact threshold.

Once organizations have been determined to be high or critical impact, the NCCS will require critical electricity undertakings to develop risk treatment plans. It's then the responsibility of the local competent authorities to decide if these plans are sufficient. National Competent Authorities can define transparent requirements for such supply chain security controls of electricity undertakings. These requirements would apply to product or service providers for PV installations. ENTSO-E and the EU DSO Entity must account for this use case in the methodology for the risk assessment processes.

National Competent Authorities should only greenlight risk treatment plans where supply chain requirements fulfill the requirements in chapter 7.1. To facilitate grid connection procedures, National Competent Authorities should establish a whitelist of products and infrastructure that meets the requirements of a PV security guideline.

7.2.3 Clearer Assignment of Risk Ownership in Future Regulation

Future versions and amendments of NIS2, the Network Code for Cybersecurity, and member state implementations must clarify risk responsibility in the event of a cyber-attack. The detour of imposing supply chain requirements on electricity undertakings via the Network Code for Cybersecurity could prove complex or difficult. Requirements would be much simpler if imposed through primary legislation.

In such future clarifications, the EU should emphasize the owner of the asset as being liable and therefore responsible for ensuring appropriate security controls are in place. In such scenarios where it is not feasible for the owner to bear the responsibility, such as with rooftop solar, this responsibility should be contractually delegated as a prerequisite to monetize the energy export. Additionally, in the context of utility scale solar, the operator is the entity to register as the "operator of critical infrastructure". However, in many instances, the operator is only under contract for a limited scope and may not necessarily have the authority to make decisions that include enforcement of supply chain security and similar security controls.

7.2.4 Classify Inverters as Critical Products with Digital Elements in the Cyber Resilience Act

A very effective measure to improve the security of the solar industry is to improve the security of the infrastructure itself. Likely the most effective route is through the new Cyber Resilience Act. In its current form, most digital items sold in the EU will be considered under the default category. However some products may be listed as Important Class 1, Important Class 2, or Critical Products. The cyber security requirements increase with each successive category.

Class 1 products includes many general-purpose security and network applications and hardware and other IOT devices that may include sensitive information such as children's toys and personal wearables. Class 2 then includes more critical security components such as firewalls and intrusion detection systems. Critical products however include the more sensitive components whose compromise may have the most significant impact. Smart Meter Gateways for example are among the few products listed.

According to the CRA, to qualify as a critical product, it must meet the following definition.

> "The categories of critical products with digital elements set out in this Regulation have a cybersecurity-related functionality and perform a function which carries a significant risk of adverse effects in terms of its intensity and ability to disrupt, control or cause damage to a large number of other products with digital elements through direct manipulation. Furthermore, those categories of products with digital elements are considered to be critical dependencies for essential entities as referred to in Article 3(1) of Directive (EU) 2022/2555."

As the analysis within this report has shown, compromise of inverters poses a serious risk to grid stability, but also potentially to households and personnel. Additionally, as solar continues to become a more significant part of the generation mix for many grid operators, they will become, if not already, a critical dependency for DSOs (who are considered essential entities under NIS2) for grid balancing.

Classification as a critical product will then require products to comply with an adopted European cyber security certification scheme relevant to the product according to Article 8(1) that meets the requirements listed in Annex 1 or third-party assessment if a certification scheme is not available. Currently there is not an industry specific certification scheme that adequately addresses the risks or that aligns with the CRA minimum security requirements. Therefore, recommendations are included to develop such a guideline in Section 7.1.1.1.

7.3 Recommendations for Addressing Existing Installations

Most actions will only impact new systems to be added after an implementation phase of any of the recommendations. Legacy systems will however remain connected to the grid. In some instances, the risk of significant grid impacts from legacy systems may be low enough to accept. In other scenarios, of high legacy PV penetration, other methods may be needed. The decision for the specific approach will depend on the local grid condition and is therefore best to be made by each member state and local system operator.

Most inverters currently installed, based on the market data from Section 4.2, are expected to be 0-5 years old. The typical expected life expectancy of most inverters is 10-15 years. With swift action to introduce only regulated and secure infrastructure, legacy infrastructure will become a smaller percentage of the overall installed capacity. However, in some areas of high penetration, legacy solar installations will remain a significant enough source of generation to pose some risk. Therefore, it is strongly recommended to introduce such a technical barrier that is capable of interfacing with most legacy systems. Grid operators are already looking at implementing this to ensure grid stability in grids with high shares of renewables in the context of grid balancing and demand response.

The technical barriers described in chapters 7.1.4.2 and 7.1.5.3 can significantly reduce the risk even for legacy devices. This includes the requirement that communications are managed through modern secure communication gateways that are capable of interfacing with the legacy inverters. It also includes requiring manufacturers to provide secure and tested software versions to trusted entities who can cut the internet connection to the attacker and recover a basic inverter software version in the case of a successful compromise.

Grid operators are already developing interfaces to be able to control inverters in case of grid emergencies, such as from natural disasters, unexpected load decreases or the unexpected failure of a nuclear power plant. For example, Germany requires all PV installations above 100 kW to be capable of communicating with the grid operator. We anticipate this trend to continue. These opportunities should be used to build redundancies into the power grid, as was also common practice for operating power grids dominated by centralised generation.

7.4 Risk Summary with Increased Mitigation Measures in Place

Table 8

Risk Matrix with Residual Risk with Additional Recommended Controls

Threat	Risk Level	Recommended Mitigations	Residual Risk
Compromise of Device, Application, or Physical Infrastructure			
Gain Unauthorized Access through Vulnerabilities in Authentication Mechanisms.	Medium	Addition of inverters to the Critical Product list under the CRA. (Section 7.1.1.1) Development of an industry specific product certification scheme that includes requirements for a secure management portal and communication methods with cloud instances. (Section 7.1.1.2)	Low
Tampering Inverters Through API's.	Medium	Addition of inverters to the Critical Product list under the CRA. (Section 7.1.1.1) Development of an industry specific product certification scheme that includes requirements for a secure management portal and communication methods with cloud instances. (Section 7.1.1.2)	Low
Direct Access to Inverter Through Intentional and Non-intentional Backdoor	Medium	Addition of inverters to the Critical Product list under the CRA. (Section 7.1.1.1) Development of an industry specific product certification scheme that includes requirements for a secure management portal and communication methods with cloud instances. (Section 7.1.1.2) Localization of the code development process to be maintained within secure jurisdictions decreases the potential for the introduction of intentional backdoors in products. (Section 7.1.2)	Low
Destruction or Compromise of Physical Infrastructure	High	Implementation of data localization concept and assurance that critical infrastructure that hosts data and applications for PV is hosted within secure jurisdictions. (Sections 7.1.2 and 7.1.3)	Low
Compromise via Supply Chain **without** Vendor Support – Rooftop			
Control Inverters through Compromise of Third Party Access Rights	High	Tighter control of access rights and role based authentication requirements under the industry specific certification scheme (Section 7.1.1.2) Decentralization of control to limit impact of a compromise and central monitoring for early detection. (Sections 7.1.5.1 and 7.1.5.2) Clear ownership of cyber risk defined with established technical barriers for entities not subject to auditing of security programs by competent authorities. (Sections 7.1.4 and 7.2.3)	Low

Table 8

Risk Matrix with Residual Risk with Additional Recommended Controls *continued*

Threat	Risk Level	Recommended Mitigations	Residual Risk
Compromise via Supply Chain **without** Vendor Support – Rooftop *continued*			
Control Inverters through Compromise of Manufacturer Access Rights	High	Decentralization of control to limit impact of a compromise and central monitoring for early detection. (Sections 7.1.5.1 and 7.1.5.2) Clear ownership of cyber risk defined with established technical barriers for entities not subject to auditing of security programs by competent authorities. (Sections 7.1.4 and 7.2.3)	Low
Control Inverters through Malicious Firmware without Vendor Support	High	Decentralization of control to limit impact of a compromise and central monitoring for early detection. (Sections 7.1.5.1 and 7.1.5.2) Clear ownership of cyber risk defined with established technical barriers for entities not subject to auditing of security programs by competent authorities. (Sections 7.1.4 and 7.2.3)	Low
Compromise via Supply Chain **without** Vendor Support – Utility Scale			
Control Inverters through Compromise of Third Party Access Rights	Medium	Tighter control of access rights and role based authentication requirements under the industry specific certification scheme (Section 7.1.1.2) Clear ownership of cyber risk defined with established technical barriers for entities not subject to auditing of security programs by competent authorities. (Sections 7.1.4 and 7.2.3) Decentralization of control to limit impact of a compromise and central monitoring for early detection. (Sections 7.1.5.1 and 7.1.5.2)	Low
Control Inverters through Compromise of Manufacturer Access Rights	Medium	Tighter control of access rights and role based authentication requirements under the industry specific certification scheme (Section 7.1.1.2) Clear ownership of cyber risk defined with established technical barriers for entities not subject to auditing of security programs by competent authorities. (Sections 7.1.4 and 7.2.3) Decentralization of control to limit impact of a compromise and central monitoring for early detection. (Sections 7.1.5.1 and 7.1.5.2)	Low
Control Inverters through Malicious Firmware without Vendor Support	High	Clear ownership of cyber risk defined with established technical barriers for entities not subject to auditing of security programs by competent authorities. (Sections 7.1.4 and 7.2.3) Backup contingency planning to recover and maintain grid stability in the event of a firmware based attack. (Section 7.1.5.3) Code signing and other patching best practices requirements included in the certification scheme to ensure only valid updates are applied. (Section 7.1.1.2) Decentralization of control to limit impact of a compromise and central monitoring for early detection. (Sections 7.1.5.1 and 7.1.5.2)	Low

Table 8

Risk Matrix with Residual Risk with Additional Recommended Controls *continued*

Threat	Risk Level	Recommended Mitigations	Residual Risk
Compromise via Supply Chain **with** Vendor Support – Rooftop			
Control Inverters through Malicious Firmware with Vendor Support	Critical	Backup contingency planning to recover and maintain grid stability in the event of a firmware based attack. (Section 7.1.5.3) Clear ownership of cyber risk defined with established technical barriers for entities not subject to auditing of security programs by competent authorities. (Sections 7.1.4 and 7.2.3) Decentralization of control to limit impact of a compromise and central monitoring for early detection. (Sections 7.1.5.1 and 7.1.5.2)	Low
Direct Control of Inverters through Vendor Access Rights	Critical	Backup contingency planning to recover and maintain grid stability in the event of a firmware based attack. (Section 7.1.5.3) Clear ownership of cyber risk defined with established technical barriers for entities not subject to auditing of security programs by competent authorities. (Sections 7.1.4 and 7.2.3) Decentralization of control to limit impact of a compromise and central monitoring for early detection. (Sections 7.1.5.1 and 7.1.5.2)	Low
Compromise via Supply Chain **with** Vendor Support – Utility Scale			
Control Inverters through Malicious Firmware with Vendor Support	Critical	Backup contingency planning to recover and maintain grid stability in the event of a firmware based attack. (Section 7.1.5.3) Clear ownership of cyber risk defined with established technical barriers for entities not subject to auditing of security programs by competent authorities. Technical barriers may include segregation of critical tasks in a trusted execution environment, secure software development in the EU, or other potential measures to be controlled through supply chain requirements (Sections 7.1.4 and 7.2.3) Decentralization of control to limit impact of a compromise and central monitoring for early detection. (Sections 7.1.5.1 and 7.1.5.2)	Low
Direct Control of Inverters through Vendor Access Rights	High	Backup contingency planning to recover and maintain grid stability in the event of a firmware based attack. (Section 7.1.5.3) Clear ownership of cyber risk defined with established technical barriers for entities not subject to auditing of security programs by competent authorities. (Sections 7.1.4 and 7.2.3) Decentralization of control to limit impact of a compromise and central monitoring for early detection. (Sections 7.1.5.1 and 7.1.5.2)	Low

Additional Topics for Investigation

Through this research several areas have been identified as areas for further research. Further investigation for each area is necessary to inform regulatory and industry decisions to best address the associated cyber security risk. These topics include:

- **Impact of a compromise for EV charging stations and Heat Pumps** – Ongoing efforts have already begun to understand potential impacts of a cyber attack on EV charging infrastructure and large controllable loads. Both are similar in operation and face many similar challenges as securing rooftop solar but with some minor differences. These differences should be further explored and an approach that address solar and these other areas should be adopted to simplify approach while still covering all relevant cyber-risks.

- **Grid Stability Limits** – determine in more detail what level of capacities are needed for a compromise and which functions pose the greatest risk and should therefore be more tightly restricted. Under dynamic grid conditions, additional analysis may be done to ensure thresholds set for ECII and other thresholds are sufficient to ensure impacts to the grid are limited.

- **Theoretical cyber-physical attacks on individual devices** - Potential backfeed attacks have been theorized by some inverter vendors. This means, with changes to the source code, solar panels and wiring may be overloading leading to fires. There are potential other local physical impacts that could be realized. Additional research into the failure modes could identify engineering controls that protect against potentially fatal failure modes.

References

1. European Commission. "EU Energy Security Strategy." Communication from the Commission to the European Parliament and the Council, SWD(2014) 330 Final.

2. Eurostat. (2025, March 19). *Electricity from renewable sources reaches 47% in 2024*. Retrieved from Electricity from renewable sources reaches 47% in 2024 - News articles - Eurostat

3. SolarPower Europe. "A Harmonised Cybersecurity Baseline for Solar PV." SolarPower Europe Position Paper, July 11, 2024.

4. Cybersecurity and Infrastructure Security Agency (CISA). (2024, February 7). *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*. Retrieved from PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure | CISA

5. Cybersecurity and Infrastructure Security Agency (CISA). (2022, April 20). *Russian State-Sponsored and CriminalCyber Threats to Critical Infrastructure*. Retrieved from Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure | CISA

6. Johnson, Jay, "Public History of Solar Energy Cyber Attacks and Vulnerabilities", DER Security Corp, 20, October 2024

7. Bitdefender. "60 Hurts per Second – How We Got Access to Enough Solar Power to Run the United States." August 7, 2024. Retrieved from 60 Hurts per Second – How We Got Access to Enough Solar Power to Run the United States

8. Rogers, M., & Ruppersberger, C. A. D. (2012, October 8). Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE. *U.S. House of Representatives Permanent Select Committee on Intelligence*. Retrieved from huawei-zte investigative report (final).pdf

9. Jowett, P. (2024, November 18). Lithuania bans remote Chinese access to solar, wind, storage devices. pv magazine International. Retrieved from Lithuania bans remote Chinese access to solar, wind, storage devices – pv magazine International

10. Ning, Susan, and Wu, Han. "China: Law & Practice and Trends & Developments." Chambers Global Practice Guides, 2024.

11. Kramer, Franklin D., Yu, Philip W., Webster, Joseph, and Sizeland, Elizabeth. "Strengthening Taiwan's Resiliency." Atlantic Council, July 2, 2024. Retrieved from Strengthening Taiwan's resiliency - Atlantic Council

12. Ministry of Digital Affairs. "DeepSeek Prohibited in Government Agencies to Prevent Cybersecurity Risk." Press Releases - News and Releases, January 31, 2025. Retrieved from DeepSeek Prohibited in Government Agencies to Prevent Cybersecurity Risk | Press Releases - News and Releases | Ministry of Digital Affairs

13. SA Power Networks. "CER Compliance." Retrieved from CER Compliance - SA Power Networks

14. SA Power Networks. "Technical Standard - TS134." May 12, 2022. Retrieved from Technical Standard - TS134

15. TikTok. "Delivering on our US Data Governance." January 2023. Retrieved from Delivering on our US data governance | TikTok

16. The White House. "Fact Sheet: Biden-Harris Administration Announces Priorities for Enhancing the Digital Ecosystem to Support a Secure Energy Future." Office of the National Cyber Director (ONCD), August 9, 2024. Retrieved from Fact Sheet: Biden-Harris Administration Announces Priorities for Enhancing the Digital Ecosystem to Support a Secure Energy Future | ONCD | The White House

17. Euronews. "Eleven EU Countries Took 5G Security Measures to Ban Huawei, ZTE." Retrieved from Eleven EU countries took 5G security measures to ban Huawei, ZTE | Euronews

18. Quartz. "What You Need to Know About China's Intelligence Law That Takes Effect Today." June 2017. Retrieved from What you need to know about China's intelligence law that takes effect today

19. Solar & Solar Wholesale Group. "Big Changes Ahead for Home Solar Owners in Hungary: What You Need to Know About New Regulations." December 30, 2024. Retrieved from Big Changes Ahead for Home Solar Owners in Hungary: What You Need to Know About New Regulations – Solar & Solar Wholesale Group

20. Spasic, Vladimir. "Romania to Introduce Mandatory Cyber Audit for Solar Power Plants." Balkan Green Energy News, October 2024. Retrieved from Romania to introduce mandatory cyber audit for solar power plants

21. NIST. "Cybersecurity of Smart Inverters: Guidelines for Residential and Light Commercial Solar Energy Systems." NIST Interagency Report 8498, December 2024.

22. Wired. "How 30 Lines of Code Blew Up a 27-Ton Generator." October 2020. Retrieved from How 30 Lines of Code Blew Up a 27-Ton Generator | WIRED

23. Slovik, Joe. "CHRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack." Dragos Whitepaper, 2019.

24. ENTSO-E. (2024). *Grid Forming Capability of Power Park Modules: First Interim Report on Technical Requirements.* Retrieved from https://www.entsoe.eu/Documents/Publications/SOC/20240503_First_interim_report_in_technical_requirements.pdf

Appendix A: Risk Matrix

Risk Matrix with Residual Risk with Additional Recommended Controls

Threat	Impact	Ease of Comp.	Likelihood	Risk Score	Risk Level	Existing Mitigations	Residual Risk	Recommended Mitigations	Residual Risk
Compromise of Device, Application or Infrastructure									
Gain Unauthorized Access through Vulnerabilities in Authentication Mechanisms.	3	3	4	36	High	CRA w/ self attestation	Med.	Addition of inverters to the Critical Product list under the CRA. (Section 7.1.1.1) Development of an industry specific product certification scheme that includes requirements for a secure management portal and communication methods with cloud instances. (Section 7.1.1.2)	Low
Tampering Inverters Through API's.	3	3	4	36	High	CRA w/ self attestation	Med.	Addition of inverters to the Critical Product list under the CRA. (Section 7.1.1.1) Development of an industry specific product certification scheme that includes requirements for a secure management portal and communication methods with cloud instances. (Section 7.1.1.2)	Low
Direct Access to Inverter Through Intentional and Non-intentional Backdoor	3	3	2	18	Med.	CRA w/ self attestation	Med.	Addition of inverters to the Critical Product list under the CRA. (Section 7.1.1.1) Development of an industry specific product certification scheme that includes requirements for a secure management portal and communication methods with cloud instances. (Section 7.1.1.2) Localization of the code development process to be maintained within secure jurisdictions decreases the potential for the introduction of intentional backdoors in products. (Section 7.1.2)	Low
Destruction or Compromise of Physical Command and Control Infrastructure	3	3	3	27	High	None	High	Implementation of data localization concept and assurance that critical infrastructure that hosts data and applications for PV is hosted within secure jurisdictions. (Sections 7.1.2 and 7.1.3)	Low

Risk Matrix with Residual Risk with Additional Recommended Controls *continued*

Threat	Impact	Ease of Comp.	Likelihood	Risk Score	Risk Level	Existing Mitigations	Residual Risk	Recommended Mitigations	Residual Risk
4.3.2.2 Compromise of an Organization – Rooftop									
Control Inverters through Compromise of Third-Party Access Rights	2	4	4	32	High	Most 3rd parties will be regulated only indirectly through supply chain security measures. CRA requirements for "secure by default" implementations should address some concerns of password security and least privileged access.	Med.	Tighter control of access rights and role based authentication requirements under the industry specific certification scheme (Section 7.1.1.2) Decentralization of control to limit impact of a compromise and central monitoring for early detection. (Sections 7.1.5.1 and 7.1.5.2) Clear ownership of cyber risk defined with established technical barriers for entities not subject to auditing of security programs by competent authorities. (Sections 7.1.4 and 7.2.3)	Low
Control Inverters through Compromise of Manufacturer Access Rights	4	3	3	36	High	Manufacturers will be regulated indirectly through supply chain security measures.	Med.	Decentralization of control to limit impact of a compromise and central monitoring for early detection. (Sections 7.1.5.1 and 7.1.5.2) Clear ownership of cyber risk defined with established technical barriers for entities not subject to auditing of security programs by competent authorities. (Sections 7.1.4 and 7.2.3)	Low
Control Inverters through Malicious Firmware without Vendor Support	5	2	3	30	High	Manufacturers will be regulated indirectly through supply chain security measures.	Med.	Decentralization of control to limit impact of a compromise and central monitoring for early detection. (Sections 7.1.5.1 and 7.1.5.2) Clear ownership of cyber risk defined with established technical barriers for entities not subject to auditing of security programs by competent authorities. (Sections 7.1.4 and 7.2.3)	Low

Risk Matrix with Residual Risk with Additional Recommended Controls *continued*

Threat	Impact	Ease of Comp.	Likelihood	Risk Score	Risk Level	Existing Mitigations	Residual Risk	Recommended Mitigations	Residual Risk
4.3.2.2 Compromise of an Organization – Utility Scale									
Control Inverters through Compromise of Third-Party Access Rights					High	Specific security controls applied to PV installations considered "critical infrastructure" are expected to considerably restrict unauthorized access to inverters.	Med.	Tighter control of access rights and role based authentication requirements under the industry specific certification scheme (Section 7.1.1.2) Clear ownership of cyber risk defined with established technical barriers for entities not subject to auditing of security programs by competent authorities. (Sections 7.1.4 and 7.2.3) Decentralization of control to limit impact of a compromise and central monitoring for early detection. (Sections 7.1.5.1 and 7.1.5.2)	Low
Control Inverters through Compromise of Manufacturer Access Rights					High	Requirements for access management and other security controls are anticipated to be in place for nearly all utility scale plants after the implementation of NIS2 and the improvement of procurement and management practices by the relevant stakeholders.	Med.	Tighter control of access rights and role based authentication requirements under the industry specific certification scheme (Section 7.1.1.2) Clear ownership of cyber risk defined with established technical barriers for entities not subject to auditing of security programs by competent authorities. (Sections 7.1.4 and 7.2.3) Decentralization of control to limit impact of a compromise and central monitoring for early detection. (Sections 7.1.5.1 and 7.1.5.2)	Low
Control Inverters through Malicious Firmware without Vendor Support					High	Manufacturers will be regulated indirectly through supply chain requirements from the owners and operators of critical infrastructure. Therefore, there will continue to be a general improvement in manufacturer cyber security practices that will also include software development best practices.	Med.	Clear ownership of cyber risk defined with established technical barriers for entities not subject to auditing of security programs by competent authorities. (Sections 7.1.4 and 7.2.3) Backup contingency planning to recover and maintain grid stability in the event of a firmware based attack. (Section 7.1.5.3) Code signing and other patching best practices requirements included in the certification scheme to ensure only valid updates are applied. (Section 7.1.1.2) Decentralization of control to limit impact of a compromise and central monitoring for early detection. (Sections 7.1.5.1 and 7.1.5.2)	Low

Risk Matrix with Residual Risk with Additional Recommended Controls *continued*

Threat	Impact	Ease of Comp.	Likelihood	Risk Score	Risk Level	Existing Mitigations	Residual Risk	Recommended Mitigations	Residual Risk
4.3.2.3 Compromise with Support and Cooperation of the Manufacturer – Rooftop									
Control Inverters through Malicious Firmware with Vendor Support	5	5	1	25	High	Non EU manufacturers are not subject to regulatory oversight and there are no available mechanisms to ensure firmware development is done in a secure way or checked and verified prior to installation.	High	Backup contingency planning to recover and maintain grid stability in the event of a firmware based attack. (Section 7.1.5.3) Clear ownership of cyber risk defined with established technical barriers for entities not subject to auditing of security programs by competent authorities. (Sections 7.1.4 and 7.2.3) Decentralization of control to limit impact of a compromise and central monitoring for early detection. (Sections 7.1.5.1 and 7.1.5.2)	Low
Direct Control of Inverters through Vendor Access Rights	5	5	1	25	High	Non EU manufacturers are not subject to regulatory oversight. Additionally, in most rooftop PV installations, direct access by the manufacturer is possible without any intervention with the local grid balancing authority.	High	Backup contingency planning to recover and maintain grid stability in the event of a firmware based attack. (Section7.1.5.3) Clear ownership of cyber risk defined with established technical barriers for entities not subject to auditing of security programs by competent authorities. (Sections 7.1.4 and 7.2.3) Decentralization of control to limit impact of a compromise and central monitoring for early detection. (Sections 7.1.5.1 and 7.1.5.2)	Low

Risk Matrix with Residual Risk with Additional Recommended Controls *continued*

Threat	Impact	Ease of Comp.	Likelihood	Risk Score	Risk Level	Existing Mitigations	Residual Risk	Recommended Mitigations	Residual Risk
4.3.2.3 Compromise with Support and Cooperation of the Manufacturer – Utility Scale									
Control Inverters through Malicious Firmware with Vendor Support					High	Non-EU manufacturers will be subject to supply chain security controls, however, the controls may be circumvented or ignored by the vendor if coerced to do so by their respective governments. Plants may implement roll back capabilities with the ability to sever communications with third parties, however this is not a regulatory requirement and not anticipated to occur all scenarios.	High	Backup contingency planning to recover and maintain grid stability in the event of a firmware based attack. (Section 7.1.5.3) Clear ownership of cyber risk defined with established technical barriers for entities not subject to auditing of security programs by competent authorities. Technical barriers may include segregation of critical tasks in a trusted execution environment, secure software development in the EU, or other potential measures to be controlled through supply chain requirements (Sections 7.1.4 and 7.2.3) Decentralization of control to limit impact of a compromise and central monitoring for early detection. (Sections 71.5.1 and 7.1.5.2)	Low
Direct Control of Inverters through Vendor Access Rights					High	It is anticipated, that under NIS2, controls will be more routinely in place that more tightly control remote access from all third-party service providers. However, this is not an explicit requirement and therefore likely to still be a systemic issue in many PV plants.	High	Backup contingency planning to recover and maintain grid stability in the event of a firmware based attack. (Section 7.1.5.3) Clear ownership of cyber risk defined with established technical barriers for entities not subject to auditing of security programs by competent authorities. (Sections 7.1.4 and 7.2.3) Decentralization of control to limit impact of a compromise and central monitoring for early detection. (Sections 7.1.5.1 and 7.1.5.2)	Low

SolarPower Europe

Leading the Energy Transition

Rond-point Robert Schuman 3,
1040 Brussels, Belgium

info@solarpowereurope.org
www.solarpowereurope.org