European Solar Manufacturing Council AISBL
146 rue Royale | 1000 Brussels – Belgium

Date: June 7, 2024

From the European PV inverter manufacturing industry:

Remote controllability of the European PV systems through the inverters requires stringent regulations and EU-wide policy measures to mitigate energy security risks

I. CURRENT STATUS – 80% OF INVERTERS FROM CHINA

As solar PV in the EU continue to set new annual deployment records, it is clear that PV is becoming the cheapest and most significant sources of electricity generation in the EU, which are in line with the targets set by e.g. the REPowerEU framework. A crucial component of PV systems is the PV inverter. Modern PV inverters do not only convert the direct current (DC) electricity generated by PV modules into alternating current (AC) used in the electricity grid, but they also manage and control the entire PV system. Consequently, the software, the communication interfaces and the access capabilities to change the behaviour of millions of these units installed in Europe are critical to the system's operation, generation, maintenance, and potential temporal or even lengthy shutdowns.

European PV inverter manufacturers, such as Fronius, Ingeteam, Kaco New Energy, Kostal, Power Electronics, Gamesa Electric (SGRE), and SMA, are at the forefront of technological advancements, particularly in energy and cybersecurity. However, a significant risk is emerging as Chinese inverter manufacturers has gained in a very short time an over 80% market share of newly built European PV systems (65% in 2022 – Table 1). Within every day the dependency on imported PV inverters is increasing meaning that as the EU is successfully moving towards the increase of solar PV generation, the technological and energy security risks increase as the operation and software updates of the PV systems can largely be controlled by companies supplying the inverters. In the case of Chinese inverter manufacturers some (Huawei, Sungrow, GoodWe) are reportedly directly connected or managed by the Government of China or have at least the obligation to obey to the requirements of Chinese Government directly or through China Communist Party.

Table 1. S&P Global Inverter Market Tracker from 2023 about the European market inverter market shares.

Company Name	2018	2019	2020	2021	2022
Huawei	12.5%	24.5%	24.2%	30.0%	24.9%
Sungrow	6.3%	7.3%	11.8%	20.0%	21.3%
SMA	19.7%	17.1%	18.1%	8.1%	6.6%
SolarEdge	7.2%	7.9%	7.8%	6.7%	6.5%
Growatt	<2%	<2%	2.4%	3.5%	4.8%
Ginlong	<2%	<2%	2.0%	2.3%	4.0%
SOFAR	<2%	<2%	2.8%	2.9%	3.7%
Fronius	5.9%	5.1%	5.4%	4.7%	3.7%
GoodWe	<2%	<2%	<2%	2.5%	3.5%
NingBo Deye	<2%	<2%	<2%	<2%	2.2%
Others	29.9%	26.6%	18.5%	13.8%	18.9%
Total GW Shipped	**21.65**	**34.61**	**38.72**	**55.24**	**91.88**

Although the NZIA provisions aim to strengthen the competitiveness of the entire PV manufacturing industry in the EU, the risks and threats associated with the deployment of imported PV inverters requires special considerations and EU-wide policy measures to prevent and mitigate the risks to the EU energy security.

II. RISKS and THREATS

Inverters, and consequently the entire control of PV systems, are managed by the manufacturers of these inverters. These manufacturers have the capability to remotely control the majority of their devices installed across Europe.

The control centres of the inverter manufacturing companies hold the authority for software-updates and to modify operational performance through grid code configurations, such as:

- Shut-down commands
- Charge/discharge commands
- Frequency control
- Grid export limits

While the risks of a critical data security breach — such as an unsecured login to an inverter — isn't dependent on a product's country of manufacturer, having most of the inverters installed in the EU controlled by entities outside the EU introduces additional and a different kind of remote-control energy security risks. While this remote-control possibility is not typically considered a cyber threat due to the cybersecurity measures implemented by most inverter producers, it nonetheless creates a substantial security of supply risks. For instance, the sudden accidental or intentional (by an ill-disposed stakeholder) shutdown of 4 GW of running solar PV capacity could seriously jeopardize the stability of the electricity grid, potentially leading to a system-wide blackout.

The challenges of technological data and cyber security should be differentiated from the risks associated with the remote-control of the inverters. The data and cyber security are shared interests of all the inverters producers, while the latter risks arising from the remote-control of the inverters by entities outside of EU become a threat in the case of a potential conflict. Consequently, the remote controllability might be used as a blackmail instrument in the hands of external entities.

III. PROPOSED SOLUTIONS

The telecommunications sector of the EU is a pivotal example of smart step-by-step European approach in curbing or blocking certain Chinese companies' appearance in the EU due to security reasons. In June 2023 the European Commission urged EU Member States to join the efforts to curb or block Huawei and ZTE equipment from the bloc's 5G telecommunications networks. Estonia, Denmark, France, Germany, Italy, Latvia, Lithuania, Portugal, Romania, Sweden followed the recommendations to restrict the suppliers from connectivity services and EU funding instruments. As reported by the European Commission in February 2024, just these ten Member States excluded Chinese hardware makers from networks. Although the impact of the recommendations has been limited, the Member States have received concrete guidelines from the European Commission. Recognizing the parallels in risk potential between the telecommunications sector and the inverters sector — and leveraging the toolbox already developed for telecommunications — could serve as a starting point for implementing a holistic approach addressing the increasing energy security risks within the EU PV inverters market.

1. Short-term measures in the interests of European energy security:

In terms of energy security, it is necessary that the sovereignty for data and remote control of the PV systems is located exclusively in the EU. Effective measures should be taken step-by-step immediately to reduce the massive dependency that already exists and is constantly getting worse. For all PV inverters installed in the EU, the following requirements should be fulfilled:

- **Performing an EU coordinated risk assessment for "PV Security". Assess the risk profile of manufacturers and apply relevant restrictions for suppliers considered as high risk. Products from manufacturers that are rated as high risk must be banned from the European market. The risks evaluation should include key essential criteria like the extent of remote controllable power in Europe (e.g. > 100 MW aggregated PV capacity), the proximity to governmental control and data security — including respective measures in addressing the risks for EU energy security.** It is important to stress that the PV security risk assessment shouldn't be limited to auctions and public procurement only. Most systems are not implemented using these schemes. Accordingly, the provisions of NZIA would be applicable in raising the level of competitiveness of European-produced PV inverters but does not address the energy security risks in a holistic EU-wide approach.
- **Product and service providers must host their control centres within the EU.** These designated control centres must exclusively hold the authority and the keys for software-updates and to modify operational performance. European cybersecurity legislation should make non-EU service and technology providers (e.g. component manufacturers, cloud-service operators and etc.) at least as accountable as European ones.
- **Data sovereignty must be within the EU.** PV systems are measuring numerous values and generate corresponding data. All critical data that is used, stored and/or forwarded must remain exclusively in the EU.

2. Long-term measures to maintain Europe's energy security, resilience, and value creation:

According to the NZIA, Europe must produce at least 40% of its own demand by 2030 to avoid dependence on a single source. This requires urgent action, as the market share of European manufacturers in Europe is already below 15% and the trend is unfortunately unbroken. About 80% of new built PV systems in Europe are equipped with inverters manufactured in China. Europe still has a strong PV inverter production industry, but the production capacities available in Europe can currently only be utilized partially, as there is no fair global competition anymore. The following actions are necessary:

- **To gradually place higher demand on European manufacturing value creation and to accomplish the respective measures without delay in line with the provisions of NZIA.** The NZIA provides the framework for defining resilience criteria — PV inverters are a sector where the resilience criteria should be applied in the strictest form.
- **Support EU manufacturing industry of PV inverters until the other measures will take effect** (temporal OPEX support or any other similar measures should be applied). Other regions of the world are subsidizing the domestic production of PV inverters, accordingly, there is the need to balance the support in order to achieve or at least to move to the level playing field.

- **Implement the necessary changes in Electricity Regulation or adopt strict requirements in respective separate legislative framework** — requirements and energy security criteria should be defined for the installed PV inverters. It is necessary to take even more advanced and stronger leveraging measures compared to 5G cybersecurity Toolbox to minimize any potential energy security risks in the EU.

The EU manufacturing industry of PV inverters has been strong historically and survived during recent challenges, however, to ensure competitiveness and level playing field, holistic measures are necessary starting with thorough evaluation of the energy security risks. It is of utmost importance in addition to the provisions of NZIA to ensure diversity of service and technology providers and avoid large deployment of inverters from single supply source or country that in a worst-case scenario of a hostility or conflict or other alternative leveraging measures can use those as a means to attack the EU electricity system or threaten/blackmail EU energy security.