Securing Photovoltaic Systems as Critical Infrastructure. A Multi-Layered Assessment of Risk, Safety, and Cybersecurity

Simona Riurean * , Nicolae-Daniel Fîță , Dragoș Păsculescu , Răzvan Slușariuc

Posted Date: 4 April 2025

doi: 10.20944/preprints202504.0357.v1

Keywords: critical infrastructure; risk management; cyber-security; NIS2; SWOT analysis; CVE; CWE; Maturity Model

 doi:10.20944/preprints202504.0357.v1

Article

Securing Photovoltaic Systems as Critical Infrastructure. A Multi-Layered Assessment of Risk, Safety, and Cybersecurity

Simona Riurean *, Nicolae-Daniel Fîță, Dragoș Păsculescu and Răzvan Slușariuc

University of Petrosani, Romania; SimonaRiurean@upet.ro (SR), DanielFita@upet.ro (NDF), DragosPasculescu@upet.ro (DP), RazvanSlusariuc@upet.ro (RS)

* Correspondence: SimonaRiurean@upet.ro

Abstract: This paper provides a comprehensive analysis of photovoltaic (PV) systems, their development and security issues in the past decade in Europe and Romania. It begins with the presentation of the PV systems development in the two regions, and proceeds with the critical risk evaluation of PV systems as essential components of the energy infrastructure of Romania. The article presents the authors' arguments in support of the proposal to include PV systems in the critical infrastructure category, reflecting their strategic importance to national energy resilience. This is achieved through a comprehensive assessment of the current levels of safety, security, cybersecurity, and physical protection of PV systems, highlighting potential vulnerabilities that may compromise operational continuity. The evaluation of cybersecurity risks leads to the conclusion that PV systems face increasing exposure to digital threats, reinforcing the urgent need for robust cyber defense mechanisms in this rapidly evolving sector.This study aims to create an entire set of guidelines for enhancing the security and resilience of PV systems as they increasingly form a critical component of sustainable energy infrastructure.

Keywords: critical infrastructure; risk management; cyber-security; NIS2; SWOT analysis; CVE; CWE; Maturity Model

1. Introduction

Energy is a fundamental factor in economic development, the functioning of public and private institutions, as well as in maintaining the social order and defense capabilities of a state. In this context, energy security directly contributes to the stability and prosperity of a nation. Many countries depend on energy imports, such as natural gas, oil, and electricity, to meet their public and domestic needs. This dependency can pose a risk to national security, as fluctuations in prices, economic sanctions, or international conflicts can disrupt access to essential energy resources. Therefore, diversifying energy sources, including the development of renewable sources, becomes a strategic priority for many states. A constant and stable access to energy is essential for maintaining a functional economy, and sudden energy price increases can severely affect purchasing power, lead to inflation, and create economic instability. Additionally, periods of energy shortages can generate social protests and disrupt public order, negatively impacting national security. Measures to reduce greenhouse gas emissions and transition to renewable energy sources may present both an opportunity and a challenge in the context of energy security. Decarbonization policies and the development of green energy must be balanced with the need to sustainably ensure a continuous and secure energy supply.

Climate change can amplify instability risks in regions dependent on natural energy resources, leading to forced migration and resource-related conflicts [1,2].

In a complex geopolitical and economic context, ensuring a stable and secure energy source is essential to protecting national interests and adapting to future challenges.

 doi:10.20944/preprints202504.0357.v1

As societies became more dependent on interconnected systems and technologies, therefore, safeguarding critical infrastructure has never been more important. Critical infrastructure encompasses the vital systems, networks, and assets that are fundamental to the operation of a society and its economy. Any disruption or destruction of these components could severely impact national security, public safety, and the overall stability and well-being of the nation [3,4].

Critical infrastructures include energy (power plants, electrical substations, energy transmission with distribution networks, oil and natural gas stations, oil, and natural gas pipelines, refineries, offshore platforms, hydrocarbon extraction facilities, storage installations, etc.), transportation, water supply and sanitation, healthcare, telecommunications and information technology (IT), finance and economy, public safety and order, and food industry and agriculture [5].

The importance of critical infrastructures lies in their role in ensuring the functioning of society by maintaining essential services for citizens and businesses. They contribute to national security by preventing cyber, terrorist, or natural threats and attacks. Additionally, they support economic stability by protecting the financial system and supply chains. Critical infrastructures also play a key role in public health protection by ensuring access to medical services and clean drinking water. Finally, they enhance resilience in crises, enabling effective responses to natural disasters, pandemics, or cyberattacks.

Romanian energy infrastructure is part of national as well as European critical infrastructure, and protecting it is crucial given all the threats it is vulnerable to, including: cyber-attack, with the increasing danger of cyber-attacks that could impact the functionality of the IT system of the energy infrastructure; natural hazard, such as earthquake, flood, or other natural disasters causing damage to equipment or transmission lines; geopolitical risks, including reliance on energy imports and potential regional tension that could impact the availability of resources; and physical attack or terrorism against critical points in electricity generation, transmission, distribution, and storage [6–9].

Recognizing the crucial importance of energy infrastructures with critical implications, the Romanian state, through companies owning or managing critical infrastructures, must develop protection and security strategies for these infrastructures, through measures and action plans, including: identifying and assessing risks—conducting security assessments and identifying vulnerabilities within the critical energy infrastructure; implementing physical security measures—protecting critical assets through physical barriers, video surveillance, controlled access, and monitoring equipment; cybersecurity—deploying advanced IT security systems to prevent and respond to cyberattacks; institutional cooperation—collaborating between national institutions (such as SRI, DSU, ANRE) and international partners, including NATO and the EU, to develop common security strategies; personnel preparation—training and qualifying staff to act promptly and effectively in crisis situations; and implementing continuity plans—developing plans that allow for the rapid restoration of essential activities in the event of an incident [10,11].

Solar energy will continue to play a crucial role in the global energy transition, with the potential to become the main source of renewable energy in the future. The growth of PV technology worldwide has been impressive over the last decade, driven by falling costs, improved efficiency of solar panels, and government support through subsidies and green energy policies. Some key aspects of this growth include expansion of the installed capacity, cost reduction, emerging technologies, and wide adoption of PV systems.

The PV systems we refer in this article, are typically categorized based on their installed capacity (power output in kW or MW) and application type (Table 1) [12].

 doi:10.20944/preprints202504.0357.v1

Table 1. PV System Categories with Cost, Efficiency, and Return on Investment.

Category	Power Range	Application	Characteristics	Cost per Watt ($)	Efficiency (%),	ROI (Years)
Residential 	<10 kW	Installed on rooftops of homes.	- Used for self-consumption and grid-tied systems. - May include battery storage for backup.	2.50 - 3.50	15-22%	5-10
Commercial 	<250 kW	Found on business buildings, schools, and shopping centers.	- Used to offset electricity costs. - Often connected to local grids with net metering	1.50 - 2.50	16-22%	4-8
Industrial 	<1000 kW (1 MW)	Used in factories, manufacturing plants, and data centers.	- Supports high energy demands and may include on-site battery storage. - May be grid-connected or hybrid	1.20 - 2.00	17-23%	3-7
Utility-Scale 	>1000 kW (1 MW+)	Large-scale, ground-mounted solar farms.	- Generates electricity for utility grids. - Includes centralized inverters and tracking systems for maximum efficiency. - Requires high-voltage grid connections	0.90 - 1.50	18-24%	2-6

The global installed capacity of PV energy has grown exponentially. According to the International Energy Agency (IEA), solar PV energy has become one of the fastest-growing sources of renewable energy, reaching hundreds of gigawatts (GW) installed annually. The cost of solar panels has dropped by more than 80% in the last 10-15 years due to technological advancements and economies of scale. This makes solar energy more accessible than traditional sources like coal or gas. The perovskite solar cells promise higher efficiency and lower costs. Bifacial panels are capable of capturing light from both sides, increasing energy production. Building-integrated PVs can be achieved by integrating solar panels into windows or facades.

Batteries are also essential for storing solar energy to be used at night or during periods without sunlight. Integrating solar energy into electrical grids requires solutions for efficient energy flow management. As installations grow, managing solar waste is also an increasing concern.

Countries with the largest installed PV capacity are China, USA and some European countries. China is a global leader, with the largest installed capacity and a strong manufacturing industry. USA records a massive investment in solar energy, supported by federal and state policies. In Europe,

 doi:10.20944/preprints202504.0357.v1

there are some pioneers (Germany, Spain, Italy) in the energy transition, with favorable renewable energy policies.

The purpose of this study is to highlight three elements of strategic value.

Firstly, it addresses the *identification of photovoltaic (PV) parks as critical energy infrastructures*. The identification is in the interest of the European Union as it allows for the creation of new job opportunities, increased technological innovation, energy resource diversity and their protection through European funds. It also assists in the transition towards greater reliance on renewable energy sources, which can provide energy independence and general economic security. PV systems help to reduce environmental impact and play a vital role in ensuring the stability of electricity transmission and distribution lines in the National Energy System. In addition, their ability to be interconnected with other critical infrastructures highlights their strategic position in ensuring national and economic security as well as social welfare.

The second scope of the study involves a *comprehensive evaluation of the safety, security, and physical protection of major PV infrastructures in Romania*. This is achieved by conducting a detailed SWOT analysis that identifies the strengths, weaknesses, opportunities, threats, risks, vulnerabilities, and hazards of PV systems. Apart from that, the study quantifies photovoltaic parks' risk of blackout by examining various constituents of a PV system, for example, panels, inverters, meters, transformers, substations, storage systems, and Supervisory Control and Data Acquisition (SCADA). The study screens natural, technical, and human sources of risk, examines their likely consequences, and determin the probability and size for each given instance. Based on this analysis, the level of risk is calculated, followed by the proposal and implementation of mitigation measures. The effectiveness of these measures is then evaluated by recalculating the severity and risk levels to validate system resilience improvement.

Lastly, the research conducts an in-depth *assessment of the cybersecurity posture of critical PV infrastructures*. This entails the determination of specific cyber threats to PV systems and evaluating their susceptibility to risks from digital connectivity and remote monitoring capabilities. Gap analysis is done to compare current protection levels against established international standards such as ISO/IEC 27001, the NIST Cybersecurity Framework, the EU NIS2 Directive and national OUG 155/2024. Hardware, software, and communications protocol vulnerabilities—specifically, those in devices like inverters, SCADA devices, and remote access—are also examined. The study also addresses the current cybersecurity measures and best practices that should be followed by PV operators. Finally, it estimates the probable implications of successful cyberattacks on operational continuity, national energy security, and economic stability and concludes with recommendations for integrating strict cybersecurity measures in national critical infrastructure protection strategies.

2. A Decade of Photovoltaic Installations in Europe and Romania

The EU countries added solar PV systems annually in recent years significantly, driven largely by rising electricity prices. The lifting of trade barriers on Chinese PV modules in 2018 was also significant to boost growth. With electricity prices now stabilizing and growth slowing in 2024, policymakers may need to implement novel strategies to further installations to meet the energy targets.

The annual solar PV installed capacity in the EU-27 has seen a significant increase over the years. Installations accelerated notably after 2018, following the end of EU trade barriers on Chinese PV modules.

The major growth phases were 2020-2022 when a rapid increase in installations (+41% in 2020, +45% in 2021 and +53% in 2022) and 2023-2024 when the growth slowed down but remained positive (+4% increase from 2023 to 2024 and 65.5 GW installed in 2024, compared to 62.8 GW in 2023) [12].

 doi:10.20944/preprints202504.0357.v1

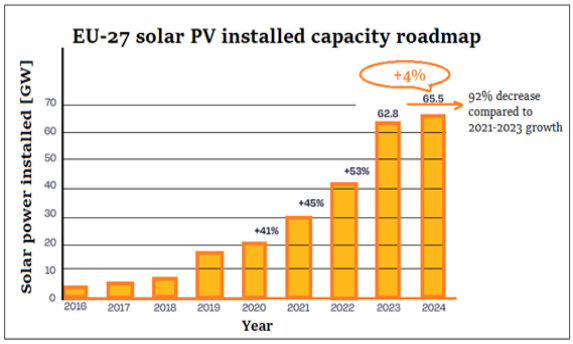


Figure 1. The 27 European countries roadmap for solar PV systems. Source: Adapted from [12].

Regarding the impact of electricity prices, there has been an unexpected electricity prices surge between June 2021 and May 2023, (+131% for non-household consumers and +79% for household consumers). The high prices likely stimulated investment in solar energy. From June 2023 - June 2024, electricity prices stabilized with a -22% decrease for non-household consumers and a 9% for household consumers, therefore this stabilization may have slowed the growth in solar PV systems. At the end of 2021, approximately 44% of the total energy production in Romania was represented by renewable energy sources of which 2% by PV solar energy [13].

The REPowerEU Target underlined that the EU needs an average annual installation of 69 GW (2025-2030). The 2024 figure of 65.5 GW suggests progress but also highlights the challenge of maintaining consistent growth. The growth rate in 2024 is much lower compared to 2021-2023 and there is a 92% decrease in growth compared to the 2021-2023 period suggesting that the market momentum is slowing [14].

Europe needs to install approximately 70 GW per year to achieve its 2030 targets. SolarPower Europe's [12] forecast for 2025 to 2028 is for growth to stabilize between 3% to 7% for the next couple of years. Growth rates will decelerate to 3% in 2026, with 72.3 GW of new solar capacity, as developers respond to grid constraints and market uncertainty. Medium Scenario of SolarPower Europe estimate an improvement of 6% to 76.5 GW in 2027 and 7% to 81.5 GW in 2028.

In Romania, during 2016-2021 the installed capacity remained relatively stable, with minimal growth. In 2022 there is a slight increase in capacity, reaching approximately 1,413 MW, in 2023 there is a significant growth, with capacity nearly doubling to around 2,900 MW, and in 2024 the expansion continued with total installed capacity reaching approximately 4,600 MW (Figure 2).

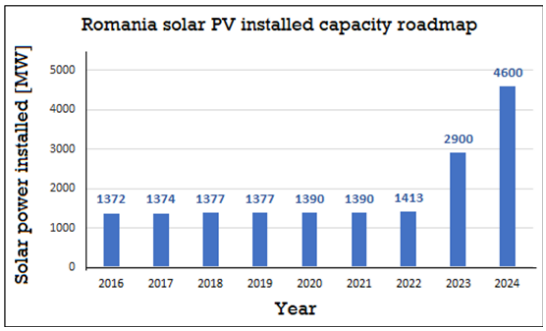


Figure 2. The roadmap of the solar PV system in Romania. Source: Authors' elaboration.

The data reflects a steady growth until 2022, followed by a rapid increase in 2023 and 2024, with 1.7 GW added in 2024, bringing the total capacity to 4.6 GW. As of early 2025, Romania accounts for approximately 0.23% of the total global installed solar photovoltaic (PV) capacity, and around 1.48% of the total installed PV capacity within the European Union. These estimates are based on Romania's cumulative installed solar capacity of approximately 4,6 gigawatts (GW) by the end of 2024, in comparison to the global total of roughly 2,200 GW and the EU total of about 338 GW [15].

 doi:10.20944/preprints202504.0357.v1

Romania's geographical position, policy support, and increased investments are factors contributing to the growth. Romania's geographical position offers considerable solar potential, with an annual solar energy flow between 1,000 and 1,300 kWh/m²/year (Figure 3) [16].

The practical solar PV potential (PVOUT) (figure 3, (a)) represents the amount of power generated per unit of the installed PV capacity over the long-term In the PVOUT refers to the long-term average energy output generated per unit of installed PV capacity. It is typically measured in kilowatt-hours (kWh) per kilowatt-peak (kWp) of system capacity, providing a standardized metric for assessing the performance and efficiency of PV installations [17].

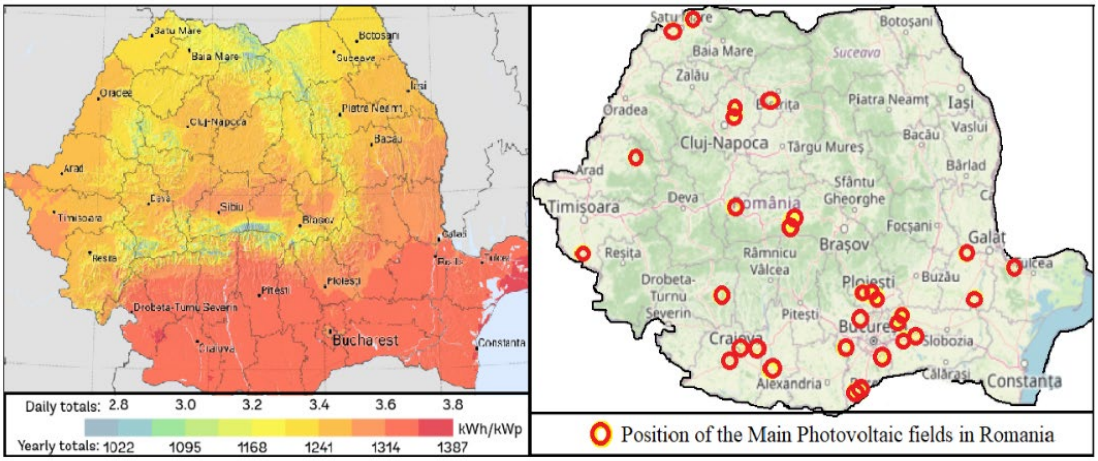


Figure 3. (a) Long term average of PVOUT in Romania and (b) The main PV fields. Source: Adapted from [17].

The introduction of supportive government policies, including contracts-for-difference (CfD) auctions and funding programs, stimulated investments in solar energy [18]. Both domestic and international investors have shown heightened interest in Romania's solar sector, leading to the development of large-scale PV projects [19]. Efforts to simplify and expedite the permitting process have facilitated the rapid deployment of solar installations. Romania's regulatory framework for PV is already well streamlined, as most projects take 1.5 to 2 years from permitting to grid connection. However, the system could be strengthened by increasing accountability for delays through stricter timelines, penalties for non-compliance, and transparent reporting mechanisms.

According to GlobalData [20], the highest PV power potential is found in regions where a unique combination of factors—such as persistent clear sky conditions, clean air, low ambient temperatures, and high altitude—results in a thinner atmosphere compared to lower elevation areas, thereby enhancing solar energy conversion efficiency. Values of solar resource and PV power potential in Romania is presented in figure 4.

Unlike the theoretical potential, it simulates the conversion of the available solar resource to electric power considering the impact of air temperature, terrain horizon, and albedo, as well as module tilt, configuration, shading, soiling, and other factors affecting the system performance.

PVOUT is 3,7 seasonality index (range for Romania) is 3.07 (2.09 – 4.10). The long-term energy content of the solar resource available at a certain location defines the theoretical solar PV potential. For PV technology, the energy content is well quantified by the physical variable of GHI. It is the sum of direct and diffuse irradiation components received by a horizontal surface, measured in kWh/m2 [21]. PVOUT measures (as seen in Figure 4) are: $P0_{MIN}$ = Level 0: Minimum value; $P1_{MIN}$ = Level 1: Percentile 0.5 value; $P1_{P25}$ = Level 1: Percentile 25 value; $P1_{MED}$ = Level 1: Percentile 50 (median) value; $P1_{MEAN}$ = Level 1: Mean value; $P1_{P75}$ = Level 1: Percentile 75 value; $P1_{MAX}$ = Level 1: Percentile 99.5 value; $P0_{MAX}$ = Level 0: Maximum value.

 doi:10.20944/preprints202504.0357.v1

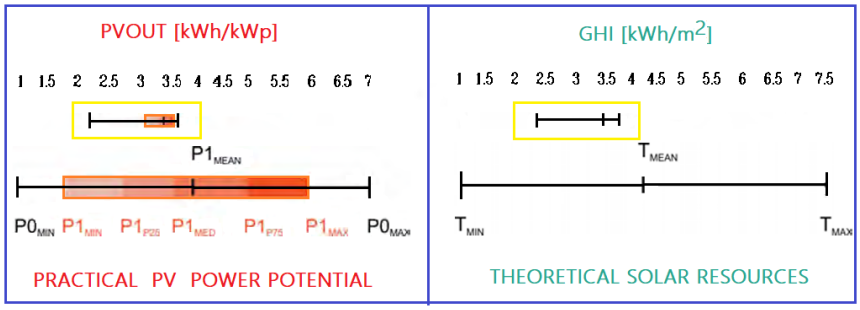


Figure 4. Practical PV power potential (PVOUT) and the theoretical solar resource (GHI - global horizontal irradiation) in Romania. Source: Adapted from [21].

GHI enables a comparison of the conditions for PV technology without considering a specific power plant design and mode of operation. GHI is the first approximation of the PV power production in a particular region, but it disregards important additional factors. Theoretical solar resource (GHI – the global horizontal irradiation, if integrated solar energy is assumed), as as seen in figure 4 are between: T_{MIN} = Minimum value; T_{MEAN} = Mean value; and T_{MAX} = Maximum value [21].

Romania is foreseen to achieve an unprecedented rise in the PV sector in the near future, boosted by financing programs such as "Casa Verde" [22] and RePower EU [23], the liberalization of energy prices (that will come into effect on April 1, 2025), and the general increased interest of Romanians in getting rid of the worries of bills and becoming energy independent.

The steady hike in tariffs for electricity has triggered demand for alternative sources of energy, especially in the domestic market, where solar panels are a smart and economical long-term investment. There are over 170,000 prosumers accounting for

2.2. GW of Installed Capacity.

While the solar PV sector is thriving, the energy storage capacity is outdated, which affects the grid efficiency and stability. The new benchmark solution on the domestic market is the lithium-iron-phosphate (LiFePO4) battery, characterized by a safer and more effective technology than lithium-ion batteries, which reduces the risk of fires. Once the Romanian government published new technical regulations for energy storage on January 18, 2025, the newest energy storage and conversion solutions are implemented into the Romanian market, including Livoltek inverters [24]. Also, ENPHASE microinverters and batteries [25], produced in the USA and developed with the help of Romanian inventor Nelu Mihai from Silicon Valley, revolutionize the solar energy conversion and use process. The microinverters allow direct AC production, eliminating the risk of conversion and increasing efficiency [26].

 doi:10.20944/preprints202504.0357.v1

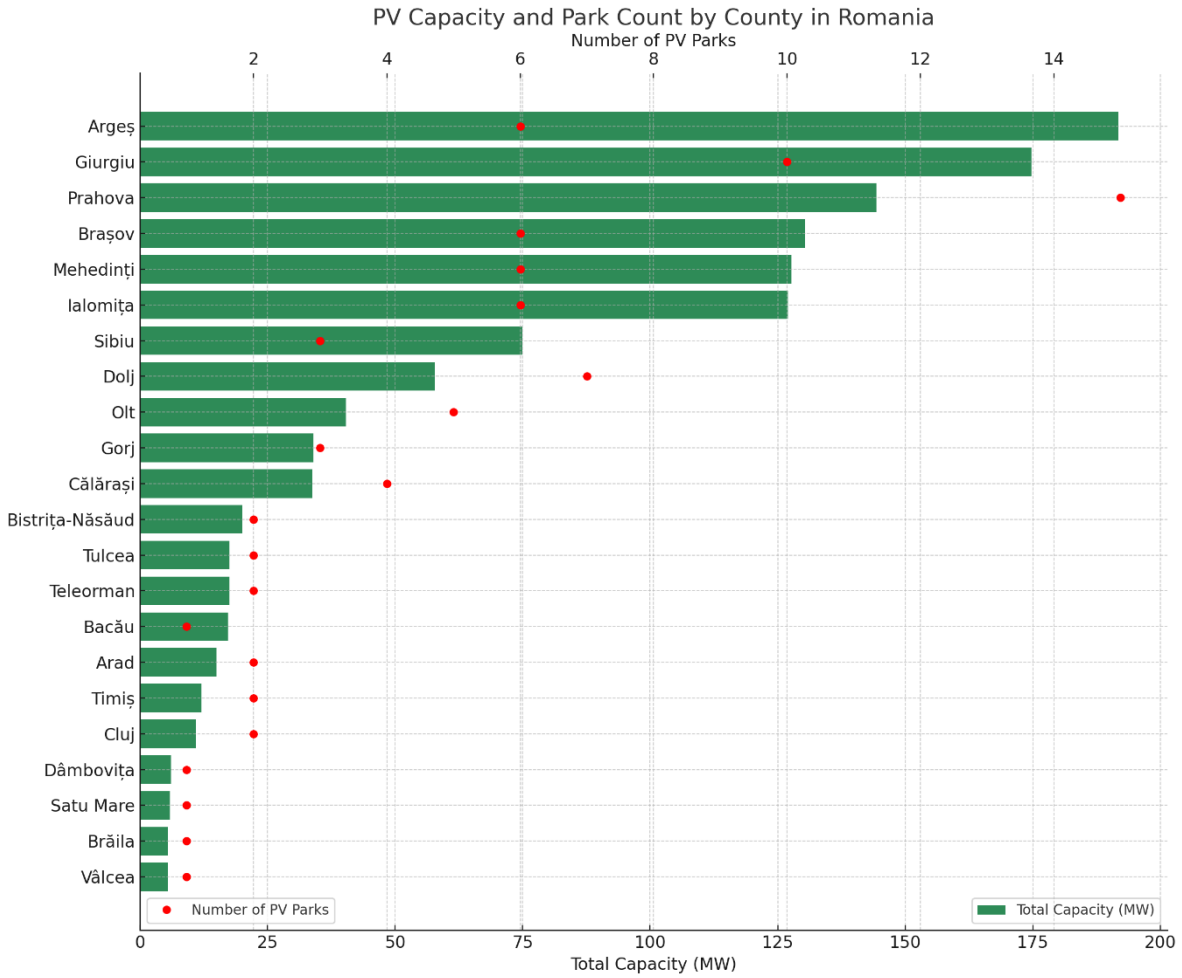


Figure 5. PV parks installed in Romania analized by counties.

Projects for PV parks to be installed (in near future in Romania) are presented in table 2.

Table 2. PV parks to be installed in Romania [15].

County	**Location** (commune) **in Romania**	**Capacity [MW]**
Dolj	Piscu Sadovei	1,500.00
Dolj	near Calafat	1,050.00
Arad	Pilu și Grăniceri	1,044.00
(Grasshopper Romania Solar PV Park)		1,000.00
Teleorman	Băbăita	710.00

As of March 21, 2025, the total installed power capacity in Romania is reported to be 19,118.32 MW, according to ANRE [27]. The cumulative electricity production capacity of the country is illustrated in Figure 6 and Table 3.

Among the various energy sources, solar PV systems account for 2,307.35 MW, contributing, so far, with approximately 12% of the total installed capacity in Romania.

 doi:10.20944/preprints202504.0357.v1

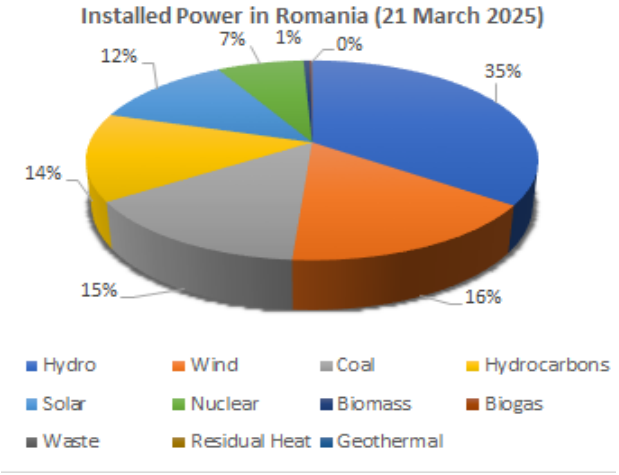


Figure 6. Total installed power in Romania on 21 March 2025 [27].

Table 3. Installed power in Romania [27].

Type of Energy	MW	%
Hydro	6,687.78	34.9810
Wind	3,095.31	16.1903
Coal	2,762.2	14.4479
Hydrocarbons	2,713.78	14.1946
Solar	2,307.35	12.0688
Nuclear	1,413	7.3908
Biomass	106.27	0.5559
Biogas	22.46	0.1175
Waste	6.03	0.0315
Residual Heat	4.1	0.0214
Geothermal	0.05	0.0003

3. Assessing the Security and Safety of PV Systems as Critical Energy Infrastructure in Romania

3.1. SWOT Analysis

3.1.1. Strengths

a) Sustainability and low environmental impact
- produce clean energy, without CO_2 emissions;
- do not generate noise pollution or hazardous waste;
- have a minimal impact on biodiversity, especially if they are harmoniously integrated into the landscape.

b) Energy efficiency and independence:
- reduce dependence on fossil fuels and their price fluctuations;
- can contribute to the energy independence of a country or region;
- are scalable, and can be expanded according to needs.

c) Low long-term costs:
- After the initial investment, operating and maintenance costs are relatively low;
- Photovoltaic panels have a lifespan of 25-30 years, offering long-term returns;
- Government subsidies and support schemes can make the investment even more profitable.

d) Easy installation and maintenance:
- Installing a PV system is faster compared to other types of power plants;

 doi:10.20944/preprints202504.0357.v1

- Requires little maintenance, as the panels have no moving parts that wear out quickly.

e) Flexibility and diversification of land use:

- Can be installed on unproductive or unused land;
- Coexist with other activities, such as agriculture (agrivoltaics);
- Can be integrated into smart-grid networks to optimize consumption.

3.1.2. Weaknesses

a) Dependence on weather conditions. The efficiency of the panels decreases on cloudy or rainy days, and the energy production is zero at night;

b) The need for large land areas. To produce a significant amount of energy, photovoltaic parks require large areas of land, which can lead to deforestation or the reduction of agricultural land;

c) Relatively low efficiency. The conversion of solar energy into electricity is not 100% efficient, with most panels having efficiencies of 15-22%;

d) High initial costs. Although the prices of solar panels have decreased in recent years, the initial investment for a photovoltaic park remains significant;

e) Environmental impact. Although solar energy is considered clean, the production and disposal of photovoltaic panels can generate toxic waste and CO_2 emissions;

f) Dependence on batteries for storage. To ensure continuous energy, storage systems (batteries) are needed, which are expensive and have their own environmental impact;

g) Issues related to grid integration. Production fluctuations can create difficulties in the stability of the electricity grid and require solutions to balance supply and demand;

h) Limited lifespan. PV panels have a lifespan of approximately 25-30 years, after which their efficiency decreases, requiring replacement and recycling;

i) Possible maintenance issues. Although they are relatively easy to maintain, the panels must be cleaned periodically and monitored for defects or loss of efficiency;

j) Impact on biodiversity. In certain cases, the construction of photovoltaic parks can affect local flora and fauna, especially in protected natural areas.

3.1.3. Opportunities

a) Economic opportunities

- Energy cost reduction – Own solar energy production can lead to lower costs for consumers and businesses;
- Profitable investments – The financial returns of photovoltaic parks are attractive due to the decrease in the prices of solar panels and their increase in efficiency;
- Job creation – The installation and maintenance of solar panels generates jobs in the renewable energy sector;
- Subsidies and financing – Governments and international organizations offer various financial support schemes for the development of renewable energy.

b) Environmental opportunities:

- CO_2 emission reduction – Solar energy is clean and contributes to reducing dependence on fossil fuels;
- Long-term sustainability – The sun is an inexhaustible resource, and its use does not negatively affect the environment;
- Reuse of degraded land – Photovoltaic parks can be located on unproductive or abandoned land, giving it a new utility.

c) Technological Opportunities:

- Innovations in Energy Storage – Modern batteries allow the storage of solar energy for use at night or on cloudy days;
- Integration into smart grids – Photovoltaic parks can be connected to smart grids, optimizing energy distribution;

 doi:10.20944/preprints202504.0357.v1

- Increased automation and efficiency – New technologies, such as artificial intelligence and cleaning robots, improve the performance and maintenance of solar parks.

d) Security Opportunities:

Critical Energy Infrastructure – The possibility that photovoltaic parks can become critical energy infrastructure, with a role in ensuring energy and national security

3.1.4. Threats, Risks, Vulnerabilities and Hazards

A. Threats

- Natural factors – Storms, hail, wildfires, earthquakes or floods can damage solar panels and park infrastructure;
- Vandalism and theft – Solar panels, inverters and cables are attractive to thieves, and vandalism can affect energy production;
- Cyber-attacks – Control and monitoring systems can be targets for cyber attacks, affecting the operation of the park;
- Regulations and policies – Changes in legislation, new taxes or land restrictions can threaten the economic viability of the project.

B. Risks

- Decreased efficiency – Dust, dirt or degradation of panels over time can reduce energy production;
- Technical problems – Failures in inverters, connections or energy storage system can affect the continuity of production;
- Dependence on weather conditions – The performance of a photovoltaic park depends directly on the intensity of sunlight, with the risk of lower production on cloudy days;
- Impact on the environment and biodiversity – Deforestation for the installation of the park or changes to the ecosystem can affect local fauna and flora;
- Unforeseen costs – Increased maintenance costs, repairs or price changes to equipment can affect profitability.

C. Vulnerabilities

- Physical security – A poorly protected park is vulnerable to vandalism and theft;
- Dependence on supply chains – Problems with suppliers of panels, inverters or batteries can delay projects and increase costs;
- Lack of infrastructure – Connecting the park to the electricity grid can be difficult if the local infrastructure is not ready for such integration;
- Long payback period – The amortization of the initial costs can take years, and fluctuations in the price of electricity can affect profitability.

D. Hazards

1. Environmental Impact:

- Deforestation and habitat loss – PV parks are sometimes built on agricultural land or forests, affecting biodiversity;
- Impact on wildlife – Animals may be disturbed by changes in habitat or by the reflection of solar panels;
- Impact on soil and water – Changes to the land for the installation of panels can lead to erosion or changes in water runoff.

2. Economic and social issues:

- Agricultural land use – If installed on fertile land, they can reduce the agricultural area available for food production;
- Visual impact – PV parks can alter the landscape and may be considered unsightly by local communities;
- Noise and nuisance – Although the panels themselves do not produce noise, auxiliary equipment such as inverters and cooling systems can generate some level of noise pollution.

3. Recycling and waste management issues:

 doi:10.20944/preprints202504.0357.v1

- Difficulty in recycling panels – Solar panel components (glass, silicon, heavy metals) are difficult to recycle, which may lead to environmental problems in the future;
- Use of rare materials – Panels contain metals such as cadmium or tellurium, the extraction of which may have a negative impact on the environment.

4. Technical, safety and security aspects:

- Fire risk – Solar panels and electrical equipment can present hazards in case of overload or technical defects;
- Material degradation – Solar panels have a limited lifespan (around 25-30 years), and managing the resulting waste can be problematic;
- Electromagnetism – Some studies suggest that equipment used in photovoltaic parks could generate electromagnetic fields, but the effects on health are still debated;
- Blackout risk – Some inverters can be remotely controlled by certain manufacturing companies, which makes the risk of disconnection of photovoltaic parks very likely and with a very serious gravity and impact on energy and national security.

3.1.5. Security, Safety and Protection Measures

A. Physical protection and security

- Fencing and access control – Installation of security fences and controlled access gates to prevent intrusion;
- Video surveillance systems – Use of surveillance cameras with motion detection and 24/7 monitoring;
- Detection sensors – Implementation of sensors to detect movement, vibration or opening of panels;
- Security patrols – Presence of security personnel or drones for regular inspections;
- Anti-theft and anti-vandalism systems – GPS tracking devices for panels, alarms and invisible markings for components.

B. Electrical safety and equipment protection:

- Grounding system – Prevention of electric shock and protection of equipment against atmospheric discharges;
- Lightning protection – Installation of lightning rods and surge arresters;
- Circuit breakers and overload protection – Installing safety equipment to prevent short circuits and fires;
- Adequate ventilation and cooling – Preventing equipment from overheating through efficient cooling systems;
- Periodic maintenance and inspection – Checking connections, wiring and panels to prevent failures.

C. Protection against natural factors and disasters:

- Wind and weather protection – Installation resistant to strong gusts, hail and floods;
- Fire prevention – Using fire-retardant materials and a rapid-fire response plan;
- Weather monitoring – Alert systems for extreme conditions that can affect production and park safety.

3.2. Black-Out Risk Assessment

3.2.1. Parts of the PV systems

The electrical systems and equipment that are part of a PV system (critical energy infrastructure) are listed and described below:

A. PV panels

- monocrystalline: Mono-Si;
- polycrystalline: Poly-Si;
- thin-film: Thin-Film;

 doi:10.20944/preprints202504.0357.v1

- bifacial: captures light on both sides;
- with PERC technology: Passivated Emitter Rear Cell.

B. Inverters

- centralized: used in large PV systems and connect several strings of solar panels to a single large inverter;
- string: each string of panels has its own inverter and is used in large commercial and residential installations;
- microinverters: each panel has its own inverter and is used in residential systems and small PV systems;
- hybrid: can operate both with the electrical grid and with energy storage batteries and is used in PV systems that include energy storage solutions.

C. Electricity meters

- production measurement: measures the electrical energy generated by PV panels;
- auxiliary consumption measurement: records the consumption of auxiliary equipment in the park (inverters, cooling systems, lighting, surveillance, etc.);
- bidirectional: monitors both the energy delivered to the grid and the energy consumed from the grid, being essential for self-consumption and grid injection systems;
- smart meters: allows real-time monitoring in integration with SCADA systems to optimize energy management.

D. Electrical transformers

- role:
- voltage boosting: PV panels generate direct current (DC), converted into alternating current (DC) by inverters; this current usually has a voltage of 400V-690V, which must be raised to an appropriate level for efficient transport through the grid (e.g. 20 kV or 110 kV);
- loss reduction: increasing the voltage reduces losses on the power line and allows the efficient transport of electricity over long distances;
- grid connection: ensures compatibility between the PV park and the electricity distribution or transport network.
- types:
- boosters: raise the voltage from the level generated by the inverters (400V-690V) to 20 kV or 110 kV, to allow injection into the grid.
- distribution: are used to power auxiliary equipment in the park (monitoring systems, lighting, air conditioning, etc.);
- isolation: to protect the system against faults and to avoid the occurrence of ground fault currents.

E. Power substations:

- medium voltage: 20 kV;
- high voltage: 110 kV or 220 kV/400 kV.

F. Electrical energy storage systems:

- types:
- electrochemical batteries: Li-Ion, Lithium-Iron-Phosphate, Lead-Acid, Redox Flow, etc.;
- supercapacitors;
- hydrogen;
- pumped storage;
- compressed air, etc.
- benefits:
- grid balancing: reduces fluctuations caused by variations in solar intensity;
- consumption maximization: allows the use of the energy produced even when the panels are not generating electricity;

 doi:10.20944/preprints202504.0357.v1

- reduction of balancing costs: minimizes the need to import electricity from other sources during peak hours;
- energy security: ensures constant power supply in microgrids or isolated areas.

G. Electrical lines for discharging electrical energy into the distribution or transmission network

- underground or overhead medium voltage power lines;
- underground or overhead high voltage power lines.

H. SCADA system:

- by system architecture:
- centralized: all data is collected and processed in a single control center and provides complete visibility over the entire PV park;
- distributed: control is divided between several local nodes that communicate with each other, ensures redundancy and great flexibility, can operate independently in the event of a failure of the central system and is suitable for large PV systems with multiple conversion stations.
- by type of communication and technology:
- based on industrial protocol (Modbus, DNP3, IEC 61850): uses communication protocols for industrial equipment and is compatible with most equipment used in solar energy (inverters, energy meters, weather sensors);
- cloud-based (IoT – Enabled SCADA: data is transmitted and processed in a cloud environment, allows remote access, advanced data analysis and integration with AI and machine learning.
- by automation level:
- passive (monitoring, no control): only collects data (generated power, temperature, solar radiation level), decisions are made by human operators and is used in smaller PV systems or in the initial phase of implementation;
- active (monitoring and automated control): can adjust system parameters in real time (optimizing the operation of inverters, changing the angle of solar panels), includes advanced functions such as energy efficiency management and protection against faults
- by scope:
- for Energy Management (EMS – Energy Management System): monitors and optimizes electricity production, integrates with battery systems for energy storage and helps balance the load on the grid;
- for diagnostics and predictive maintenance: uses artificial intelligence algorithms to identify possible defects in equipment and can detect efficiency losses of PV panels caused by dirt or defects;
- for integration with the electrical grid: ensures compliance with the requirements of grid operators and regulates voltage and frequency to avoid imbalances in the system.

3.2.2. Causes and Effects in Black-Out Risk Scenario

A. Causes

a). Natural risk factors

- Storms and extreme weather events: strong winds, torrential rains, heavy snow, hail, lightning, which can damage electrical systems and equipment in PV systems (PV panels, electrical inverters, electrical meters, electrical transformers, energy storage systems, electrical power evacuation lines);
- Earthquakes or landslides: which can damage electrical and mechanical infrastructure;
- Extreme temperatures: excessive heat or cold, which can overload the electrical grid or damage PV panels.

b). Technical risk factors:

- Defects or poor quality of PV panels;
- Damage to step-up transformers or overhead or underground cables: age or wear of equipment;

 doi:10.20944/preprints202504.0357.v1

- Overload in the PV park: excessive electricity consumption in the power station;
- Short circuits: in the electrical power lines or in the electrical power distribution panels;
- Efficiency, life span and low quality of energy equipment;
- Lack of electrical energy storage systems;
- Lack or precariousness of SCADA systems;
- Lack of or poor cybersecurity programs.

c). Human risk factors:

- Lack or precariousness of maintenance or repair work;
- Human errors in the operation or management of the PV park or electrical networks;
- Acts of vandalism, theft, or sabotage;
- lack of investments;
- Wrong configuration: PV panels, inverters, transformers, electricity evacuation lines;
- Wrong maneuvers performed by operational or dispatching personnel;
- Lack of specialized and/or trained operational personnel;
- Lack of communication or poor communication with DET – Territorial Energy Dispatcher or DEN – National Energy Dispatcher;
- Lack of working procedures during a crisis;
- Lack/non-compliance/ignorance of national/European procedures in case of serious damage (black out);
- Lack of training in the field of Risk Management;
- Lack of physical security of PV systems. Effects:
- Lack of electricity in the distribution or transport networks: possible local, zonal, regional or national black-out of the National Energy System;
- Enormous material damage generated by the lack of electricity to critical consumers, households and industries;
- Enormous material damage resulting from the interdependence of other systems on electricity;
- State of energy, economic and national insecurity.

B. Effects

- Lack of electricity in the distribution or transmission networks: possible local, zonal, regional or national blackout of the National Energy System;
- Enormous material damage resulting from the lack of electricity to critical consumers, households and industries;
- Enormous material damage resulting from the interdependence of other systems on electricity;
- State of energy, economic and national insecurity.

3.2.3. The Probability Scale

With the aim to establish the probability of occurrence, the probability scale was adopted, according to table 4.

Table 4. The probability scale [28].

LEVEL / ASSOCIATED SCORE	DEFINITION OF PROBABILITY	PERIODS
1. Very low	There is a very low probability of occurring. Normal measures are required to monitor the evolution of the event.	over 13 years
2. Low	The event has a low probability of occurring.	10 – 12 years

 doi:10.20944/preprints202504.0357.v1

		Efforts are being made to reduce the probability and/or mitigate the impact.	
X	**3. Medium**	**The event has a significant probability of occurring. Significant efforts are required to reduce the probability and/or mitigate the impact.**	**7 – 9 years**
	4. High	The event has a probability of occurring. Priority efforts are required to reduce the probability and mitigate the impact produced.	4 – 6 years
	5. Very high	The event is considered imminent. Immediate and extreme measures are required to protect the objective, evacuation to a safe location if the impact requires it.	1 – 3 years

3.2.4. The Severity of the Consequences

The severity of the consequences is given by the most unfavorable level of risks and their impact. The risk analysis, according to table 5.

Table 5. Impact.

RISK SCENARIO: BLACK-OUT RISKS	LEVEL
1. Natural hazards • Storms and extreme weather events: strong winds, torrential rain, heavy snow, hail, lightning, which can damage electrical systems and equipment in PV systems (PV panels, electrical inverters, electrical meters, electrical transformers, energy storage systems, electrical power evacuation lines); • Earthquakes or landslides: which can damage electrical and mechanical infrastructure; • Extreme temperatures: excessive heat or cold, which can overload the electrical grid or damage PV panels.	Very low Low Medium High **Very High**
2. Technical risks • Defects or poor quality of PV panels; • Damage to step-up transformers or overhead or underground cables: age or wear of equipment; • Overload in the PV park: excessive electricity consumption in the power station; • Short circuits on electrical power lines or on electrical power distribution panels; • Low efficiency, lifespan and quality of energy equipment; • Lack of electrical energy storage systems; • Lack or precariousness of SCADA systems; • Lack of or poor cybersecurity programs.	Very low Low Medium High **Very High**
3. Human risk factors: • Lack or precariousness of maintenance or repair works; • Human errors in the operation or management of the PV park or the electrical networks; • Acts of vandalism, theft, or sabotage; • Lack of investments; • Wrong configuration: PV panels, inverters, transformers, electrical energy evacuation lines; • Wrong maneuvers performed by the operational or dispatching staff; • Lack of specialized and/or trained operational staff; • Lack of communication or poor communication with DET – Territorial Energy Dispatcher or DEN – National Energy Dispatcher; • Lack of working procedures during a crisis; • Llack/non-compliance/ignorance of national/European procedures in case of serious damage (black out); • Lack of training in the field of Risk Management; • Lack of physical security of the PV systems.	Very low Low Medium High **Very High**

A. Impact Analysis

 doi:10.20944/preprints202504.0357.v1

The impact analysis is an analysis that identifies the impact of the loss of a PV systemfacility (critical infrastructure) of national importance. The highest level of severity levels related to the impacts will be chosen, according to table 6.

Table 6. Impact analysis and its level.

IMPACTS	Level	
Enormous damage caused by lack of electricity	1. Vey low	temporary
	2. Low	significant damage
	3. Medium	average damage
	4. High	high damage
	5. Very high	**very heavy damage**
Enormous damage generated by the interdependence of other systems	1. Vey low	0 – 10% of RIC
	2. Low	11 – 20% of RIC
	3. Medium	21 – 30% of RIC
	4. High	31 – 40% of RIC
	5. Very high	**over 41% of RIC**
Potential environmental damage	1. Vey low	0 – 20%
	2. Low	21 – 40%
	3. Medium	41 – 60%
	4. High	61 – 80%
	5. Very high	**over 81%**
High social impacts	1. Vey low	0 – 10% of PT
	2. Low	11 – 20% of PT
	3. Medium	21 – 30% of PT
	4. High	31 – 40% of PT
	5. Very high	**over 41% of PT**

RIC– Return on Invested Capital; PT – Public Trust.

Table 7. Levels of severity consequences [28].

	LEVEL / SCORE	THE SEVERITY OF THE CONSEQUENCES
	1. Very low	The event causes a minor disruption to the activity, without material damage.
	2. Low	The event causes minor property damage and limited disruption to business
	3. Medium	Injuries to personnel, and/or some loss of equipment, utilities, and delays in service provision.
	4. High	Serious injuries to personnel, significant loss of equipment, facilities, and delays and/or interruption of service provision.
X	**5. Very high**	**The consequences are catastrophic resulting in fatalities and serious injuries to personnel, major loss of equipment, facilities, and services, and interruption of service provision.**

B. Assessing risk severity

Table 8. Risk matrix.

PROBABILITY						
	Very high 5					
	High 4					
	Medium 3					**Risk scenario**
	Low 2					
	Very low 1					
	0	Very low 1	Low 2	Medium 3	High 4	**Very high 5**
		SEVERITY / CONSEQUENCES				

 doi:10.20944/preprints202504.0357.v1

Note: Risk is given by the product of the probability of occurrence of a hazard/threat and the severity of its consequences.

Table 9. Calculated risk level.

The calculated risk has the value **15**
(probability **5** x severity **3**)
Therefore, there is a
High Risk
for the event to occur

CALCULATED RISK LEVEL	
LEVEL	SCORE
Very low	1 – 3
Low	4 – 6
Medium	7 – 12
High	**13 – 16**
Very hight	17 – 25

3.5. Risk Management

To reduce risks, measures are required to decrease, stop or eliminate them, as seen in Table 10.

Table 10. Risk management.

TYPES OF RISK	PROPOSED MEASURES
1. Natural risk factors • Storms and extreme weather events: strong winds, torrential rains, heavy snow, hail, lightning, which can damage electrical systems and equipment in photovoltaic parks (photovoltaic panels, electrical inverters, electrical meters, electrical transformers, energy storage systems, electrical power evacuation lines); • Earthquakes or landslides: which can damage electrical and mechanical infrastructure; • Extreme temperatures: excessive heat or cold, which can overload the electrical grid or damage PV panels.	• major investments in photovoltaic parks (critical energy infrastructure) due to seismic risk; • predictability of natural disasters (links with state institutions in the field of emergency situations); • training and advanced training courses for operational, maintenance and security personnel in the field of Emergency Situations; • analysis of events in the natural calamities section; • simulations of interventions (very short time) in case of fires; • provision of individual fire extinguishing means and equipment.
2. Technical risks • Defects or poor quality of photovoltaic panels; • Damage to step-up transformers or overhead or underground cables: age or wear of equipment; • Overload in the photovoltaic park: excessive electricity consumption in the power station; • Short circuits: in the electrical power lines or in the power distribution panels; • Low efficiency, lifespan and quality of energy equipment; • Lack of electricity storage systems; • Lack or precariousness of SCADA systems; • Lack of or poor cybersecurity programs.	• high-quality photovoltaic panels; • high-quality step-up transformers and underground and overhead electrical cables; • high-quality electrical equipment and devices (inverters, meters, etc.) • high-quality hibrid electricity storage systems; • high-performance SCADA systems; • high-quality cybersecurity programs; • high-performance and secure hardware and software systems; • analysis of events, incidents, etc.
3. Human risk factors • Lack or precariousness of maintenance or repair works; • Human errors in the operation or management of the PV system or the electrical networks;	• major investments in national and European critical infrastructure; • predictability (security) of the political system;

 doi:10.20944/preprints202504.0357.v1

- Acts of vandalism, theft, or sabotage;
- lack of investments;
- Wrong configuration: PV panels, inverters, transformers, electrical energy evacuation lines;
- Wrong maneuvers performed by the operational or dispatching staff;
- Lack of specialized and/or trained operational staff;
- Lack of communication or precarious communication with DET – Territorial Energy Dispatcher or DEN – National Energy Dispatcher;
- Lack of working procedures during a crisis;
- Lack/non-compliance/ignorance of national/European procedures in case of serious damage (black out);
- Lack of training in the field of Risk Management;
- Lack of physical security.

- accessing European funds regarding the security of European critical infrastructures;
- training and advanced training courses for operational, maintenance and security personnel;
- analysis of events, incidents, etc.;
- control of installations on the operating line and performance of preventive maintenance;
- compliance and monitoring of physical security norms<
- training and advanced training courses for personnel with Critical Infrastructure Protection Management responsibilities;
- training personnel in cybersecurity.

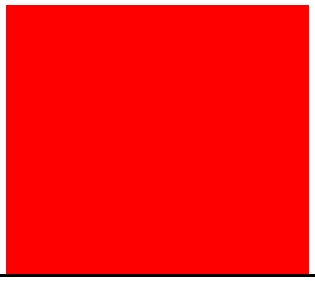
Following the implementation of risk reduction measures, the results, are shown in Table 11.

Table 11. Risks management.

RISKS	IDENTIFIED	RESULTS AFTER MEASUREMENT IMPLEMENTATION
1. Natural risk factors • Storms and extreme weather events: strong winds, torrential rains, heavy snow, hail, lightning, which can damage electrical systems and equipment in photovoltaic parks (photovoltaic panels, electrical inverters, electrical meters, electrical transformers, energy storage systems, electrical power evacuation lines); • Earthquakes or landslides: which can damage electrical and mechanical infrastructure; • Extreme temperatures: excessive heat or cold, which can overload the electrical grid or damage PV panels.	1. Very low 2. Low 3. Medium 4. High **5. Very high**	1. Very low 2. Low **3. Medium** 4. High 5. Very high
2. Technical risks • Defects or poor quality of PV panels; • Damage to step-up transformers or overhead or underground cables: age or wear of equipment; • Overload in the PV systems: excessive electricity consumption in the power station; • Short circuits: in the electrical power lines or in the power distribution panels; • Low efficiency, lifespan and quality of energy equipment; • Lack of electricity storage systems; • Lack or precariousness of SCADA systems; • Lack of or poor cybersecurity programs	1. Very low 2. Low 3. Medium 4. High **5. Very high**	1. Very low 2. Low **3. Medium** 4. High 5. Very high
3. Human risk factors • Lack or precariousness of maintenance or repair works; • Human errors in the operation or management of the PV system or the electrical networks; • Acts of vandalism, theft, or sabotage; • lack of investments; • Wrong configuration: PV panels, inverters, transformers, electrical energy evacuation lines; • Wrong maneuvers performed by the operational or dispatching staff;	1. Very low 2. Low 3. Medium 4. High **5. Very high**	1. Very low 2. Low **3. Medium** 4. High 5. Very high

 doi:10.20944/preprints202504.0357.v1

- Lack of specialized and/or trained operational staff;
- Lack of communication or precarious communication with DET – Territorial Energy Dispatcher or DEN – National Energy Dispatcher;
- Lack of working procedures during a crisis;
- Lack/non-compliance/ignorance of national/European procedures in case of serious damage (black out);
- Lack of training in the field of Risk Management;
- Lack of physical security



3.5. Reevaluation of the Consequence Severity

Table 12. Level of severity of the consequences.

	LEVEL / SCORE	THE SEVERITY OF THE CONSEQUENCES
	1. Very low	The event causes a minor disruption to the activity, without material damage.
	2. Low	The event causes minor property damage and limited disruption to business
X	**3. Medium**	**Injuries to personnel, and/or some loss of equipment, utilities, and delays in service provision.**
	4. High	Serious injuries to personnel, significant loss of equipment, facilities, and delays and/or interruption of service provision.
	5. Very high	The consequences are catastrophic resulting in fatalities and serious injuries to personnel, major loss of equipment, facilities, and services, and interruption of service provision.

3.6. Risk Level After Application of Mitigation Measures

Table 13. Risk matrix.

PROBABILITY						
	Very high 5					
	High 4					
	Medium 3			**Risk scenario**		
	Low 2					
	Very low 1					
	0	Very low 1	Low 2	Medium 3	High 4	**Very high 5**
		SEVERITY / CONSEQUENCES				

Note: Risk is given by the product of the probability of occurrence of a hazard/threat and the severity of its consequences.

Table 14. Calculated risk level.

The calculated risk has the value **9**

(probability **3** x severity **3**)

Therefore, there is a

Medium Risk

for the event to occur according

to the scenario analyzed

CALCULATED RISK LEVEL	
LEVEL	SCORE
Very low	1 – 3
Low	4 – 6
Medium	**7 – 12**
High	13 – 16
Very hight	17 – 25

4. Addressing PV Systems' Vulnerabilities to Cyber-Attacks

4.1. Specific Cyber Threats in PV Systems

 doi:10.20944/preprints202504.0357.v1

PV systems, particularly recent industrial and utility-scale installations, are becoming more vulnerable to a broad spectrum of cyber threats. One of the most widely recognized threats is the unauthorized remote access, where cyber attackers exploit weak or default passwords in inverters, SCADA devices, or energy management systems. In the majority of cases, poorly configured VPNs or remote desktops provide easy entry points into core system components, where attackers can gain control over operations.

Another serious threat comes from malware and ransomware attacks. These can potentially infect operator workstations, SCADA servers, or gateways and cause serious disruption.

Ransomware, in particular, can shut down operations by encrypting critical control software, thereby halting energy generation and cutting real-time monitoring capabilities. Similarly, denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks can overwhelm smart inverters or communication gateways with traffic, rendering them nonresponsive and significantly affecting the availability of monitoring and remote control functions.

SCADA vulnerabilities themselves are also a major threat. The majority of attackers target SCADA or HMI platforms known vulnerabilities, such as SIMATIC WinCC OA, to corrupt operational data or trigger unexpected shutdowns. It goes hand-in-hand with spoofing and manipulating data attacks when attackers feed them with incorrect sensor readings—such as false irradiance or production values—to mislead the operators or autonomous control systems to take out-of-place responses like shutdowns or output adjustments.

Supply chain integrity is also a weak link. Vulnerability to third-party software components or compromised firmware enables backdoors into PV equipment such as inverters and controllers to establish enduring threats. Similarly, the vulnerability in communication protocols of Modbus, DNP3, or SunSpec, the majority of which have no encryption or authentication, opens avenues for exploitation by man-in-the-middle or replay attacks, hijacking secure data exchange among system components.

Internal attacks, either malicious or accidental, complicate the cybersecurity picture. Users, integrators, or contractors might inadvertently or maliciously share login information, disable security settings, or expose sensitive config files. At the same time, the rise of cloud-monitoring platforms and mobile/web APIs introduces new channels for exploitation, particularly when such interfaces are not well secured or inappropriately configured.

Also, firmware vulnerabilities are an invisible, but dangerous risk. Malicious use of inverter firmware or battery management system bugs by attackers to gain low-level access control of devices with the ability to cause physical damage or cascade failure through the grid, is a serious concern. Solar PV systems employ common IT computing and networking equipment and the Internet to perform all operations and maintenance functions, including but not limited to revenue metering, condition monitoring, remote diagnostics, virtual power plant aggregation, and grid support feature control such as reactive power control [29].

The integration of PV systems in Internet introduces numerous cybersecurity threats to the electric grid. These threats include theft or redirection of financial assets, DoS, illegal access to confidential or proprietary information belonging to companies, customers, or suppliers, as well as ransomware attacks that can disrupt the operation of automated equipment. Furthermore, malicious actors may attempt to gain control over PV system operations, potentially causing equipment damage or endangering personnel [30]. Attackers often exploit control messages from sensors or employ phishing and spoofing techniques to gain initial access, subsequently escalating their privileges using advanced tactics to pursue financial gain or to deliberately destabilize grid operations [31].

Cyberattacks may not necessarily result in direct disruption of operations or physical damage to plant equipment. However, the consequences can extend to the broader electric grid, which was not originally designed to accommodate variable generation or bidirectional power flow. The range of threats has expanded significantly, now encompassing both opportunistic and highly sophisticated adversaries. Unsophisticated attacks often exploit known vulnerabilities and are typically motivated

 doi:10.20944/preprints202504.0357.v1

by mischief, disruption for entertainment, or mess. In contrast, sophisticated attackers pursue financial gain, reputational damage, or strategic disruption.

These actors may engage in corporate espionage to extract sensitive business strategies, pricing models, or intellectual property. More advanced and persistent threats, including those potentially sponsored by nation-states, target the information and control layers of DER systems. Their objective is to weaponize these systems by progressing through multiple attack stages—initial infiltration, privilege escalation, data collection, exfiltration, and ultimately, command and control [32].

Ambitious IT innovation has left behind older systems with weaknesses that expose them increasingly to modern cyberattacks. More advanced IT exploits have evolved more rapidly than the defenses of much of the aging infrastructure. But all of these developments are relatively equal opportunities to enhance cybersecurity. Cloud security platforms, mobile and edge computing, 5G communications able to 'slice' data, and quantum computing are all upgrades to more robust defenses. In particular, quantum technologies enable genuinely random number generation and tamper-evident communication as well as machine learning for quick detection and neutralization of attack patterns, together rendering certain attack vectors less viable. [33].

PV solar systems, as part of the modern energy infrastructure, face increasing cyber threats due to their digital and connected nature. These vulnerabilities can compromise both the operational technology (OT) and IT components of PV systems. The dominance of certain countries in manufacturing PV components raises concerns about potential backdoors or embedded vulnerabilities in hardware and software, which could be exploited for malicious purposes. Also, integration of numerous small-scale PV systems into the grid increases the attack surface. Each connected device represents a potential entry point for cyber threats, making centralized security management more complex [34].

4.2. PV Key Components Vulnerable to Cyber Attacks

In PV systems, there are vulnerabilities in every hardware, software, and communications layer, each of which is a potential entry point for cyberattacks. Hardware components such as inverters, energy meters, controllers, and gateways are often installed in remote or physically accessible locations. Physical accessibility may allow direct tampering, incorrect setup, or even hardware replacement. Most inverters contain firmware that includes no secure boot operations and therefore are susceptible to code injection. Hardware security modules and the presence of default credentials can lead to the theft of cryptographic keys or unauthorized control function access.

Software vulnerabilities are of particular concern for SCADA systems, local controllers, and web-based monitoring stations. Most of the PV management software is based on legacy software that is never or rarely patched or updated, leaving them vulnerable to exploitation of known vulnerabilities. Insecure authentication mechanisms, hard-coded credentials, and insecure APIs also compromise the platforms, potentially allowing attackers to take unauthorized control or manipulate business data. Remote code execution and data manipulation could, in other cases, be caused by unvalidated user inputs within interfaces through injection attacks. Cloud services used for remote monitoring can also expose information if APIs are not properly secured or if access logs and alerts are not being closely monitored.

Communication protocols used in PV systems are another major vulnerability. These protocols are designed mostly for functionality and do not typically include encryption or authentication features. This allows interception and data manipulation in a straightforward manner via man-in-the-middle or replay attacks. Even more advanced protocols, like IEC 61850, can be broken if they are poorly configured or installed without robust key and certificate management practices. The use of insecure communication media, such as open HTTP or Telnet sessions, also enhances the risk factor, especially where remote access or wireless backhaul connections are concerned.

Poor segmentation among networks also makes it possible for attackers to laterally move around the PV infrastructure after gaining an initial foothold.

 doi:10.20944/preprints202504.0357.v1

The key components of a solar PV system possible to be vulnerable to cyber threats are presented in figure 7.

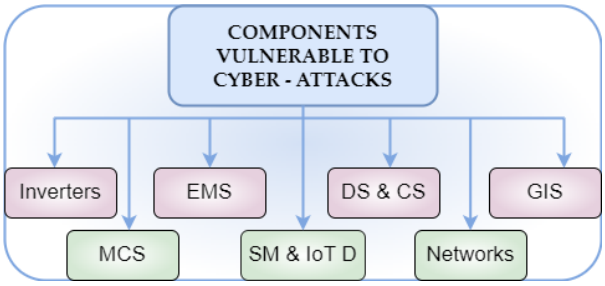


Figure 7. Components of solar PV systems vulnerable to cyber-attacks. Source: Authors' elaboration.

Inverters (I) are crucial components in PV systems that convert direct current (DC) produced by solar panels into alternating current (AC) for use in the grid or by consumers. Unauthorized access can disrupt energy production and potentially damage equipment. Their vulnerabilities to cyber threats are weak authentication and access control, insecure communication protocols, firmware vulnerabilities. Inverters with default or weak passwords can be easily accessed by cybercriminals. The use of unsecured communication protocols for remote monitoring and control, make them susceptible to eavesdropping or manipulation. Products with outdated or unpatched firmware can have vulnerabilities that can be exploited by attackers. Therefore, malicious actors could gain unauthorized control, alter operational parameters, or even damage the inverter's functionality [33].

Monitoring and Control Systems (MCS) allow to remotely monitor the performance of the PV system and permit operators to control the operation of inverters, storage systems, and other components. Cyber actors can hijack these monitoring devices, leading to data breaches or manipulation of system operations. Their vulnerabilities to cyber threats are remote access, data manipulation, inadequate encryption. A secured remote access (e.g., via virtual private networks - VPN, secure shell - SSH) forbidden attackers to compromise the system. A lack of a secured access would allow attackers to manipulate data, leading to incorrect system analysis or false alarms. The lack of encryption during transmission of sensitive data (e.g., performance metrics, financial data) can lead to data breaches. Unauthorized access could lead to operational disruptions. [34].

Energy Management Systems (EMS) manage the flow of energy within a PV system and between the PV system and the grid, optimizing energy production and storage. Their vulnerabilities to cyber threats are poorly configured security settings, the lack of real-time monitoring, and the unpatched software. EMS often control critical system processes, making them a high-value target for attackers. An insufficient monitoring can allow cyber intrusions to go unnoticed for extended periods. Vulnerabilities in EMS software can be exploited if is not regularly updated or patched, therefore attackers can manipulate energy distribution, potentially causing financial loss or destabilization of the grid.

Smart Meters and IoT Devices (SM & IoT D) that monitor energy usage, production, and system health, which are frequently used in residential and commercial PV systems. Their vulnerabilities to cyber threats are weak authentication, insecure communication, and the lack of regular updates. IoT devices usually have weak or hardcoded passwords, making them easy targets for attackers therefore many devices communicate over unsecured protocols, allowing attackers to intercept and manipulate data. Also, many IoT devices are not regularly updated, leaving them exposed to known exploits.

The compromised devices could lead to unauthorized access, data leakage, or even the manipulation of energy data.

Data Storage and Cloud Systems (DS&CS) often store the performance data and financial information for analysis and reporting. Their vulnerabilities to cyber threats are data breaches, unsecured APIs, and weak access controls. Sensitive data stored in the cloud is a potential target for cybercriminals, especially if not properly encrypted. The cloud systems that use APIs for remote

 doi:10.20944/preprints202504.0357.v1

access can be vulnerable to attack if those APIs are not properly secured. An insufficient access control mechanisms for cloud-based systems can allow unauthorized users to access sensitive data, thus a breach could lead to the loss of proprietary data, financial information, or manipulation of performance data, potentially damaging the PV system operator's business reputation.

Networks (N) that connect all the components of the PV system (e.g., inverters, sensors, monitoring platforms) are based on wireless or wired networks. Their vulnerabilities to cyber threats are unencrypted data transmission, insecure wireless networks and exposed ports. When the transmission between devices and the monitoring platform is not encrypted, attackers could intercept or manipulate data. Wireless communication channels, such as Wi-Fi, Bluetooth Low Energy (BLE) or cellular connections, can be vulnerable to eavesdropping or man in the middle (MITM) attacks. Also, open ports on devices that are part of the communication network can serve as entry points for cyber attackers. Hence data interception or system control could allow cybercriminals to manipulate the functioning of the PV system.

The Grid Integration Systems (GIS) interface the PV systems with the larger electricity grid, enabling full duplex communication and ensuring the stability of the grid when integrating solar energy. Their vulnerabilities to cyber threats are grid communication and lack of isolation. Insecure communication with grid management systems (e.g., SCADA systems) could allow attackers to inject malicious commands or manipulate grid operations and insufficient isolation between the PV system and grid control systems increases the risk of cyberattacks spreading. Compromised grid integration could destabilize the electricity grid, disrupt energy flow, and cause financial loss due to system downtime.

4.3. A Brief Literature Review on Cyber Treats and Security Solutions in PV systems

Scientific literature has extensively examined the vulnerabilities of PV systems, particularly concerning cybersecurity threats.

PV systems are vulnerable to cyberattacks that compromise data integrity and exploit software weaknesses. Such attacks can disrupt operations and compromise system reliability [36]. The integration of remote monitoring and control applications in PV systems introduces potential cyber-attack vectors. Ensuring the Confidentiality, Integrity, and Availability (CIA) of data in these applications is crucial to maintaining system security [37]. The Potential-Induced Degradation (PID) is a phenomenon where high voltage stress causes performance degradation in PV modules, leading to power losses of up to 30%. Factors such as system voltage, temperature, and humidity can accelerate PID, affecting the longevity and efficiency of PV systems [34]. Studies identified potential vulnerabilities in distributed inverter VAR (voltage-ampere reactive) control within PV-integrated distribution networks [38]. Cyber-attacks exploiting these weaknesses can disrupt voltage regulation and destabilize the power grid [39]. Machine Learning-Based Intrusion Detection research indicates that ML techniques can effectively detect hidden cyber-attacks on PV systems. By analyzing aggregated measurements, these methods can identify anomalies even when attackers manipulate individual system data to remain undetected [40].

In 2020, a study analyzed the impact of cyberattacks on smart grids distribution with high penetration of PV resources. The research identified potential attack strategies, such as power injection attacks, which could destabilize the grid and disrupt PV system operations [41]. A study published in 2022 highlighted vulnerabilities in Energy Management Systems used in PV systems. Weak authentication and insecure communication protocols were identified as potential entry points for cyberattacks, which could lead to unauthorized control over energy distribution and consumption [35]. Research in 2022 examined the cybersecurity challenges associated with Distributed Energy Resources, including PV systems. The study found that the interconnected nature of these resources increases the attack surface, making them susceptible to various cyber threats [42]. In 2023, cybersecurity experts identified vulnerabilities in the firmware of certain solar inverters, which are critical components in PV systems. These flaws could have been exploited to disrupt communication

 doi:10.20944/preprints202504.0357.v1

between inverters and monitoring systems, potentially compromising the entire solar installation [43].

In paper "Cyber Security Risk Assessment of Solar PV Units with Reactive Power Control Capabilities" is investigated the impact of cyberattacks on voltage regulation in distribution grids with PV units. It highlights how malicious actors can exploit vulnerabilities in reactive power control to destabilize the grid [44]. The review [36] presents potential cyberattacks on PV systems, including scenarios where attackers could falsify power generation data by spoofing sensor inputs to the PV inverter. Such manipulations can lead to incorrect power output readings and impact grid stability. The study [45] analyzes security oversights in distributed energy resources, including PV systems, and discusses how protocol and device-level vulnerabilities can lead to cyberattacks affecting power system operations. This work [46] provides an overview of the cybersecurity challenges associated with PV systems, highlighting their vulnerability to anomalies and cyber threats, where the urgency of implementing robust cybersecurity measures to protect the integrity and reliability of PV systems are highlighted. The research [47] explores how the integration of solar PV affects the vulnerability of power grids to cyberattacks. It examines potential attack scenarios and their impacts, providing insights into securing distributed generation assets against cyber threats

A number of cyber security methods have been developed in order to shield grid connected PV systems from evolving cyber threats. There are two large categories into which these methods come: model-based and data-based approaches [36].

Model-based approaches use analytical models in order to identify anomalies as well as threats. A study that presents a quantitative threat analysis framework that utilizes Semantic Web technologies to systematically investigate potential attack vectors targeting emerging power generation facilities, such as PV power plants, from multiple dimensions has been conducted by Bai et al. [48]. A robust control framework for AC microgrids based on Kullback-Liebler divergence aiming to neutralize data-driven attacks has been presented [49]. In order to identify cyber anomalies in microgrids with a high percentage of renewable energy, a defense mechanism with dynamic watermarking has been introduced. Its effectiveness has been proved via simulation in an actual microgrid [50]. A dynamic loop wide-area damping control scheme to enhance the robustness of power systems against detectable and stealth cyber-attacks has been proposed [51]. A cross-layer control mechanism to improve the resilience of microgrids against DoS and False Data Injection (FDI) attacks has also been presented. The authors tested the stability and efficiency of this mechanism via simulation experiments [52]. A physics-data-driven method by utilizing power electronics-based harmonic state space models to detect multi-type cyber-attacks in PV farms with guaranteed detection and precise attack source localisation was investigated by Zhang et al. [53].

Dynamics-based methods use models to detect and mitigate cyber-attacks on PV plants. But it is challenging to construct accurate models for large PV systems as they are dynamic and complex.

Data-driven cybersecurity measures in PV systems utilize past data to construct predictive models and identify anomalies. Through statistical techniques and ML models, they analyze system performance, transmission patterns, and operation behavior using data previously acquired. Using big data, this method has better performance and is highly attractive for large-capacity PV power plants, where it might not be convenient to construct accurate analytical models. Certain data-driven cybersecurity methods targeting PV systems have been introduced in recent years. One uses Parametric Time-Frequency Logic (PTFL) to detect anomalies like False Data Injection (FDI) attacks, DoS attacks, and malfunctioning of power electronics devices under microgrid scenarios through controller/hardware-in-the-loop simulations [54]. Another approach uses synchro-phasor measurements along with network packet characteristics to construct cyber-physical anomaly-based intrusion detection systems (IDS) such that remedial actions can be implemented [55]. Additionally, significant research has examined detection and diagnosis of cyber-attacks on PV arrays by time-frequency domain characteristics, enabling discrimination between normal operation modes, open-circuit and short-circuit faults, and malicious cyber activity [56].

 doi:10.20944/preprints202504.0357.v1

Apart from the above, there are also other research studies focusing on cybersecurity strategies for PV systems. These researches contribute to improving the cybersecurity of the PV systems to make them stable and resilient against potential cyber-attacks [57].

4.4. Cyber Incidents in Solar PV Systems

There are a number of recent real-world instances where cybersecurity vulnerabilities in PV systems have been identified and addressed, as well as actual cyberattacks and security breaches.

In May 2024, researchers at Bitdefender found a series of critical vulnerabilities in PV plant management platforms operated by Solarman and Deye. The platforms oversee the production activities of millions of solar installations worldwide, accounting for approximately 195 GW of solar power—roughly 20% of the global solar production.. [58]. If exploited, the vulnerabilities would allow attackers to change inverter settings, which could take portions of the electrical grid offline and increase the risk of widespread. These vulnerabilities were disclosed to the vulnerable vendors and have been patched [59].

Because of hijacking, remote monitoring devices for PV systems were compromised in Japan (2024), highlighting vulnerabilities in solar power infrastructure. This incident underscored the potential for attackers to disrupt operations or gather sensitive data from compromised systems [60].

U.S. electrical utilities experienced a 70% increase in cyberattacks, with many incidents targeting renewable energy components, including PV systems. These attacks aimed to disrupt power generation and compromise grid stability [61]. FBI issued a warning about potential cyberattacks on the renewable energy sector, emphasizing that hackers could disrupt operations, steal intellectual property, or hold critical information for ransom. This alert highlighted the increasing interest of cybercriminals in exploiting vulnerabilities within PV systems [62].

Nordic utility company Fortum reported daily cyberattacks and occasional drone surveillance targeting its power assets, including PV systems, in Finland and Sweden. These incidents reflect the growing threats to energy infrastructure in the region [63].

A white-hat hacker in the Netherlands has exposed vulnerabilities in PV systems, highlighting their susceptibility to cyber-attacks.

These events have prompted the European solar industry to advocate for more rigorous security assessments, especially as it seeks to strengthen its position against dominant global players like China. The Dutch hacker successfully gained control over millions of solar panel systems by exploiting a "backdoor" in the inverters. These inverters, often connected to the internet for monitoring and management purposes, were found to be easily accessible to unauthorized users [64].

4.5. Common Vulnerabilities and Exposures (CVE) and Common Weakness Enumeration (CWE) in PV systems

With the goal of identifying some of the known vulnerabilities related to the main parts of the PV solar systems (inverters, monitoring and control systems, energy management systems, smart meters and IoT devices, data storage and cloud systems, communication networks, and grid integration systems) we used the public sources National Vulnerability Database (NVD) [65] and MITRE [66]. These sources host reported CVE (in software and firmware components), with the related CWE, offering a reliable representation of known issues within software systems. Given the lack of specific releases concerning PV system-related vulnerabilities, our data collection process involved performing an up-to-date keyword-based searches within these databases and then filtering the results we reach to identify some of those that are relevant to PV systems [67].

The most recent notified vulnerability is CVE-2025-24865. On 13rd of February 2025 the US National Coordinator for Critical Infrastructure Security and Resilience [68] published an alert (code ICSA-25-044-16) and then DNSC (on 19 February 2025) [69] released the alert regarding critical cybersecurity vulnerability (CVE-2025-24865) identified at the level of some mySCADA products also used in the PV infrastructure. mySCADA and its component myPRO Manager are utilized in industrial systems for monitoring and control purposes. mySCADA provides a comprehensive

 doi:10.20944/preprints202504.0357.v1

SCADA solution designed to monitor the performance, efficiency, and status of solar power plants and other industrial applications. mySCADA offers a professional HMI/SCADA system designed for real-time visualization and management of industrial processes, including those in the power and energy sectors. myPRO Manager serves as a tool within the mySCADA suite that allows users to license the mySCADA PRO software, manage deployments, and switch between different versions of mySCADA PRO. It also facilitates the setup of SMTP (Simple Mail Transfer Protocol) for notifications, enhancing the operational efficiency of PV systems by providing seamless management and monitoring capabilities [70]. There are vulnerabilities identified in certain versions of mySCADA products. For instance, versions of myPRO Manager prior to 1.3 and myPRO Runtime prior to 9.2.1 were found to have vulnerabilities that could allow remote attackers to execute arbitrary commands or disclose sensitive information. The Common Vulnerability Scoring System CVSS 3.1 vulnerability's score is 10 of 10 (critical). The attack complexity is low, CIA are all high with no privileges required.

The CVSS assigns a numerical value (Base Score) to indicate the severity of a vulnerability. This score ranges from 0 to 10, with higher scores representing more severe vulnerabilities. The severity levels are categorized as in Table 15 [65]:

Table 15. Severity levels.

Score	Range		Severity
	From	To	
None	0	0	
Low	0.1	3.9	
Medium	4.0	6.9	
High	7.0	8.9	
Critical	9.0	10	

CVE-2025-24865 is a vulnerability affecting the administrative web interface of mySCADA myPRO Manager. The interface can be accessed without requiring authentication, making it possible for unauthorized attackers to gain access and retrieve sensitive information. Furthermore, they can upload files without the need for a password, posing a significant security risk. This vulnerability could potentially allow attackers to launch further attacks or steal confidential data. Organizations using mySCADA myPRO Manager are advised to apply the necessary patches or updates to mitigate this risk. An attacker who exploits this vulnerability can access the administration interface without authentication, view and exfiltrate sensitive data, upload malicious files to the system, and/or also compromise the security of the entire mySCADA infrastructure [71]. Users are advised to update to the latest versions to mitigate these risks.

Following a short overview of the CVE-2025-24865 vulnerability, results four weaknesses:

1. Weakness ID: CWE-78 - There is an improper neutralization of special elements used in an Operating System OS Command - OS command injection (OSCI).

The product constructs a complete or part of an operating system (OS) command out of externally-controllable input received from an upstream component. But it does not properly sanitize or remove special characters that can be used to change the intended action of the command when passed on to a downstream component. This makes the product vulnerable to OS command injection, which allows an attacker to inject arbitrary OS commands with potentially escalated privileges. A conceptual representation is presented in Figure 8 [72].

 doi:10.20944/preprints202504.0357.v1

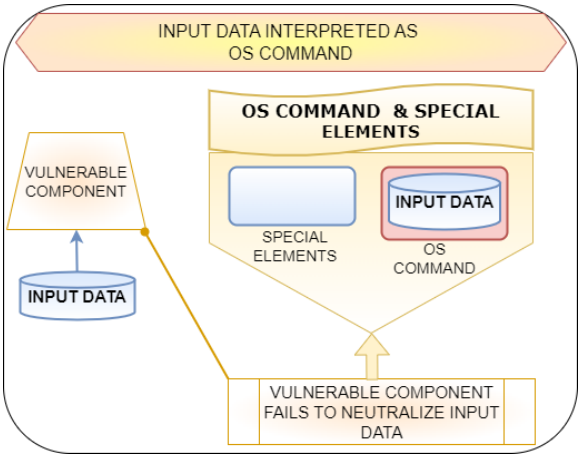


Figure 8. Conceptual representation of the CWE-78 weakness. Adapted from [72].

The base score CVSS v3.1 is 9.8 according to [73]. A CVSS v4 score has also been calculated and the base score is 9.3 (critical) according to [74]. This vulnerability is caused by this weakness when the attacker does not have direct access to the OS or, if the weakness occurs within a privileged program, it may enable an attacker to execute commands that would otherwise be inaccessible, or invoke other processes with elevated privileges beyond their authorization. The risk is significantly heightened when the targeted application fails to adhere to the principle of least privilege, as attacker-controlled commands could then be executed with system-level permissions—greatly amplifying the potential impact of the attack [72].

2. Weakness ID: CWE-306 - Missing authentication for critical function (MACF).

A CVSS v3.1 base score of 10.0 has been classified as critical, calculated according to [75]. As per the CVSS vector string [76] its base score is calculated as critical with the score 10.0.

The technical impact can be gaining privileges or assuming identity by the attacker, since the product does not verify any functionality that requires a verifiable user identity or consumes a significant number of resources (Figure 9).

Figure 9. Conceptual representation of the CWE-306 weakness. Adapted from [72].

Depending on the associated functionality, the effect differs but can extend from reading/modifying sensitive data, accessing administrative or other privileged functionality, or even executing arbitrary code.

3. Weakness ID: CWE-312 - Cleartext storage of sensitive information (CSSI).

The product that is affected stores credentials in cleartext, allowing an attacker to gain sensitive information. Since data is stored in cleartext (i.e., not encoded), attackers potentially can read the data. Although the data could be encoded to make it invisible to humans, some techniques will determine what encoding is being applied, then break the data back out. It can be easier for attackers when organizations deploy cloud services to reach the data anywhere on the Internet. In some environments (such as cloud), double encryption (software and hardware) may be necessary and the

 doi:10.20944/preprints202504.0357.v1

developer might have exclusive responsibility for both, not shared responsibility with the administrator of the broader environment [72].

4. Weakness ID: CWE-352 - Cross-Site Request Forgery (CSRF).

The exposed product is vulnerable to cross-site request forgery (CSRF), which can permit an attacker to steal sensitive information. The attacker can trick the victim to visit a site controlled by the attacker. The technical impact is gaining privileges or assume identity. Also bypass protection mechanism, read application data, modify application data, DoS, crash, exit, or restart. The effect varies depending on what kind of functionality is exposed to CSRF. The attacker will be able to perform any action on the victim's behalf. If the victim is an administrator or a user with privileges, the effect may be gaining complete control of the web application - stealing or destroying data, removing the product, or employing it to mount other attacks on every one of the product's users. As the attacker has the victim's identity, the scope of CSRF is only limited by the victim's privileges [72].

Therefore, a complete image of the CVE-2025-24865 cyber vulnerability is presented in Figure 10.

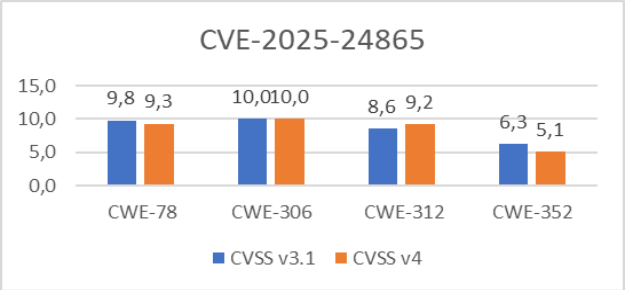


Figure 10. Score overview of CVE-2025-24865 vulnerability. Source: Authors' elaboration.

CVSS v3.1 (Common Vulnerability Scoring System, version 3.1 was released in 2019 as a continuation of version 3.0. It was a significant revision of the CVSS standard to provide a more accurate and easier-to-understand risk assessment of vulnerabilities. Its components are (i) base score (evaluates the overall impact of a vulnerability on a system and how it could be exploited by an attacker. Factors like exploit complexity, required access level, and impact on confidentiality, integrity, and availability are considered), (ii) temporal score (reflects short term changes to a vulnerability, such as the availability of a public exploit or the presence of a patch, (iii) environmental score (based on factors specific to an organization, such as existing protections and the impact on the system or IT environment). The final score generates a numerical score between 0 and 10, where 0 represents a very low vulnerability and 10 indicates a very severe vulnerability.

CVSS v4 is a newly developing version aimed at addressing some of the perceived limitations of version 3.1. Its primary goal is to improve vulnerability scoring and adapt to the new security challenges, including the complexity of modern technological environments. The proposed components (i) enhanced flexibility (include updates to allow for more precise assessments of the impact on distributed systems, cloud systems, and complex infrastructures), (ii) more detailed scoring (additional options to reflect more scenarios and security aspects, such as industrial control systems, IoT, and others), (iii) improved temporal and environmental scoring (better reflection of vulnerabilities' evolution over time and the ability to add more details about environmental risks and external infrastructure). The final score provides a score between 0 and 10, but with a more detailed methodology to assess the impact and likelihood of exploitation for vulnerabilities.

CVSS v3.1 is still the globally used standard for evaluating vulnerabilities, and CVSS v4 is under development to address new challenges in cybersecurity.

The cybersecurity landscape of PV systems (Table 16) has evolved significantly over the past decade, revealing numerous vulnerabilities that threaten operational continuity, data integrity, and infrastructure resilience.

 doi:10.20944/preprints202504.0357.v1

The year 2022 brought attention to CVE-2022-33139, affecting Siemens' Cerberus DMS, Desigo CC, and SIMATIC WinCC OA platforms. These systems, widely used in building and energy management—including large-scale PV farms—were found to rely on client-side authentication unless explicitly configured otherwise. Without server-side authentication or Kerberos, these platforms allowed attackers to impersonate users or manipulate communication flows, severely compromising system trust.

In 2019, vulnerabilities in Enphase and Fronius inverters (e.g., CVE-7676, CVE-7677, CVE-7678, CVE-19228, CVE-19229) revealed improper access control and input validation flaws. These included command injection, directory traversal, and exposure of sensitive files, all of which could be exploited via network ports (e.g., TCP 8888). Similar to earlier cases, the reliance on insecure configuration and failure to protect internal paths and files underscored poor implementation of basic security controls.

A significant cluster of vulnerabilities was reported in 2017, notably in SMA Solar Technology's inverter products. CVEs 9851 to 9864 exposed a broad attack surface, including hardcoded credentials, default password use, weak cryptographic algorithms, insecure communication protocols (e.g., SIP), and lack of proper authentication and authorization. These weaknesses (mapped to CWE-798, CWE-521, CWE-287, CWE-311, and CWE-200) allowed attackers to bypass security checks, intercept sensitive data, inject malicious firmware, and fully compromise device integrity. Many of these issues were rooted in weak password policies, deterministic authentication codes (e.g., Grid Guard), and a failure to implement encrypted communication.

Table 16. A reverse chronological order presentation of weaknesses noticed in CVE.

Year	CWE	Explanation	CVE	Base score	CVSS severity
2025	306	Missing authentication for critical function (MACF)	CVE-2025-24865	10	critical
	312	Cleartext storage of sensitive information (CSSI)			
	352	Cross-Site Request Forgery (CSRF)			
	78	Improper neutralization of special elements used in an OS Command (OS Command Injection)			
2022	603	Use of Client-Side Authentication	CVE-2022-33139	9.8	critical
	287	Improper Authentication - SCADA system only uses client-side authentication, allowing adversaries to impersonate other users.			
2019	521	Weak Password Requirements	CVE-2019-7676	7.2	high
	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting' XSS)	CVE-2019-7677	6.1	medium
	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	CVE-2019-7678	9.8	critical
			CVE-2019-19229	6.5	medium
	312	Cleartext Storage of Sensitive Information	CVE-2019-19228	9.8	critical
2018	200	Exposure of Sensitive Information to an Unauthorized Actor	CVE-2018-12735	7.5	high
			CVE-2018-12927	7.5	high
2017	noinfo	Insufficient Information	CVE-2017-9851	7.5	high
			CVE-2017-9864	7.5	high
	798	Use of Hard-coded Credentials	CVE-2017-9852	9.8	critical
	521	Weak Password Requirements - Allows brute-force attacks on the password	CVE-2017-9853	9.8	critical

 doi:10.20944/preprints202504.0357.v1

2012	311	Missing Encryption of Sensitive Data - Lack of encryption compromises CIA	CVE-2017-9854	9.8	critical
	311	Incorrect Authorization	CVE-2017-9855	9.8	critical
	256	Plaintext Storage of a Password - Storing a password in plaintext may result in a system compromise	CVE-2017-9856	3.4	low
	287	Improper Authentication	CVE-2017-9857	8.1	high
			CVE-2017-9860	9.8	critical
	200	Exposure of Sensitive Information to an Unauthorized Actor	CVE-2017-9858	7.5	high
			CVE-2017-9862	7.5	high
	327	Use of a Broken or Risky Cryptographic Algorithm	CVE-2017-9859	9.8	critical
	74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	CVE-2017-9861	9.8	critical
	352	Cross-Site Request Forgery (CSRF)	CVE-2017-9863	8.8	high
	89	Improper Neutralization of Special Elements used in an SQL Command	CVE-2012-5861	7.5	high
	310	Cryptographic issues	CVE-2012-5862	-	high
	264	Permissions, Privileges, and Access Control	CVE-2012-5863	-	high

The earliest reported vulnerabilities, dating back to 2012, targeted the Sinapsi eSolar Light and Schneider Electric's Ezylog SCADA systems. These included high-severity SQL injection flaws (CVE-2012-5861) and improper authentication (CVE-2012-5862, CVE-2012-5863), which enabled remote attackers to obtain administrative privileges and execute arbitrary commands. These vulnerabilities were primarily due to insufficient input sanitization and the lack of authentication mechanisms.

The analysis of reportedCVEs from 2012 to 2022 highlights recurring weaknesses in both system design and implementation, affecting software, firmware, hardware, and communication protocols across several manufacturers and platforms.

According to the findings above, an analysis filling the gap between current protection levels and standards (e.g., ISO/IEC 27001, NIST guidelines, EU NIS2 Directive, OUG 155/2024) and the status of current implementation with the recommended actions is presented in Table 17 [.

Table 17. Gap analysis.

Control Area	Control Requirement	Standard Reference	Current Implementation Status	Gap Description	Risk Level	Recommended Action
Access Control	Implement MFA for remote access.	NIST PR.AC-7 / ISO 27001 A.9.4.2	N/A	Remote access protected only by username/password	High	Implement MFA using tokens or authenticator apps
Asset Management	Maintain an up-to-date asset inventory.	ISO 27001 A.8.1.1 / NIST ID.AM-1	Partially implemented	No centralized inventory of PV components	Medium	Deploy asset management system and conduct full inventory
Incident Response	Establish an incident response plan (IRP) and test it regularly.	ISO 27001 A.16.1.1 / NIST RS.RP-1	N/A	No formal plan for responding to cyber incidents	High	Develop and regularly test an IRP

 doi:10.20944/preprints202504.0357.v1

The vulnerabilities reported across this decade demonstrate a consistent pattern: insecure default configurations, lack of authentication, weak or absent encryption, and a failure to follow secure software development principles. These systemic issues highlight the urgent need for PV system vendors and operators to adopt secure coding standards, enforce access control, and comply with international cybersecurity frameworks. Without these measures, PV systems will remain exposed to multi-vector attacks capable of disrupting energy production and threatening national infrastructure resilience.

5. Strategies for Cyber Threats Mitigation in solar PV systems

5.1. Cyber Security Risk Management in PV systems

Risk management is a structured and ongoing process attempting to identify, assess, and mitigate risks to reduce the impact of threats and vulnerabilities against an organization. While risks cannot be prevented, they can be brought under control to manageable levels by balancing the probable impact of a threat against the control cost. Importantly, the cost of a control should never be greater than the worth of the asset to be protected.

Cybersecurity threats specific to solar PV systems require innovative defense strategies. To address these challenges, the integration of advanced technologies such as Artificial Intelligence (AI) and Machine Learning (ML) is essential. These emerging technologies offer new opportunities for enhancing the security of PV infrastructures. By analyzing vast volumes of data, AI and ML can detect patterns and anomalies that may indicate an impending cyberattack, enabling timely and proactive countermeasures

The risk management process involves the key steps presented in table 18.

Table 18. Risk management process table.

Step	Description	Explanation/Methods
Framing the Risk	Defining threats that give rise to overall risk	Threats may arise due to - flawed processes; - insecure products; - cyber attacks; - disruption of services; - legal exposure; - loss of confidential intellectual property.
Assessing the Risk	Consider the severity of each threat identified	Quantitative assessment (e.g., financial loss) and/or qualitative assessment (e.g., impact on operations).
Responding to the Risk	Reduce exposure to the risks	Each risk needs to be eliminated,-decreased, transferred, or accepted based on its assessed impact and available resources.
Planning for Incident Response	Developing and keeping incident response plans, defining roles, responsibilities, and procedures in clear terms	Conducting simulations and drills optimizes organizational preparedness.
Risk Monitoring	Risk management is continuous	Risks must still be monitored, and any remaining (accepted) risk should be monitored carefully to ensure that it remains acceptable.

 doi:10.20944/preprints202504.0357.v1

5.2. Security Policy for PV Systems

The vulnerabilities identified in PV systems highlight the need for a general and integrated security policy. Repairing hardware security is insufficient if the channels of communication remain vulnerable, just as protecting software via patching is futile if outdated protocols continue to be utilized without defensive wrappers. The interdependence of these layers places PV systems at high risk from multi-vector attacks, which can alter data integrity, disrupt energy production, and threaten the stability of the global energy system.

The purpose of a security policy (SP) for PV systems is to establish a framework for protecting PV systems against cyber threats, physical security risks, and operational disruptions. This policy ensures compliance with Romanian energy regulations (ANRE, GDPR, application of NIS2 Directive as OUG 155/2024) and international security standards (ISO/IEC 27001, ISO 31000, IEC 62443, IEEE 1547.3-2023 [77]). Additionally, it aligns with the Industrial Solar Alliance, launched by the European Commission in December 2022, which aims to develop an autonomous and resilient European solar supply chain. This initiative targets a 30 GW manufacturing capacity by the end of 2025, supporting EU-based production of modules, ingots, wafers, and related technologies to meet both domestic and international demands. The Alliance also focuses on diversifying raw materials sourcing and promoting research and innovation to strengthen Europe's PV industry.

This policy should apply to:

- All PV systems' assets (solar panels, inverters, SCADA systems, monitoring platforms, sensors, and network infrastructure);
- Personnel (employees, contractors, and third-party service providers handling PV operations);
- Data security (grid connectivity, energy production data, remote monitoring, and communication channels).

The SP objectives are to ensure CIA of PV systems, prevent unauthorized access to control systems (SCADA, inverters), mitigate cyber threats (malware, phishing, DDoS attacks, ransomware), protect against physical security risks (theft, vandalism, weather damage), ensure compliance with legal and regulatory frameworks, and align with EU strategies to enhance solar supply chain security and resilience.

Cybersecurity policy states to access control and authentication, network security patch management & system hardening, and incident response and recovery.

All access to PV monitoring and control systems must be role-based (RBAC) and the MFA for SCADA, remote access, and administrative accounts must be implement. Also, the least privilege principle must be used for employees that should have access only to the systems required for their job. A regularly revision and users' access rights must be compulsory. Also, the use firewalls and VPNs for remote access, deployment of IDS and Intrusion Prevention Systems (IPS) and application of encryption (Transport Layer Security -TLS, VPNs) for data communication between PV systems should be enforced. IDS/IPS systems vigilantly monitor the activity of the PV system and also in networks, observing behavior patterns and outliers so as to discover real-time suspected attacks. With early discovery, PV system managers are able to respond immediately to reduce destruction, safeguard vital operations. Even so, in the absence of stringent security features like firewalls and encryption, PV systems invite malicious attacks while vulnerable security systems with protected data leave rooms for cyberattacks, thereby causing a potential disruption on their activities [78,79]. All software and firmware must be regularly updated. Unused ports and services on SCADA and IoT devices must be disabled. Endpoint security solutions (antivirus, anti-malware, Endpoint Detection and Response – EDR) should be implemented [80].

An IRP for cyber and physical threats must be maintained up-to-date. Cybersecurity drills and penetration tests must be conducted every 6 months. Backup and disaster recovery procedures should be applied regularly.

Physical security policy mentions the perimeter security and asset protection to:

- Install fencing, gates, and surveillance cameras (CCTV) around PV fields;
- Use motion sensors and intrusion alarms for unauthorized access detection;

 doi:10.20944/preprints202504.0357.v1

- Maintain security patrols in high-risk areas;
- GPS tracking on high-value assets (inverters, transformers);
- Lightning protection systems for weather-related risks;
- Fire detection and suppression systems at critical sites.

Operational security policy consists of data protection & compliance and employee training & awareness by:

- Encrypt energy production data before transmission;
- Ensure compliance with GDPR for personal data collected from monitoring systems;
- Store logs and audit trails for at least 1 year for forensic analysis;
- Conduct mandatory security training for all employees and contractors;
- Simulated phishing tests to improve awareness;
- Strict onboarding and offboarding procedures for access control.

The compliance and review policy must be revised annually, must be conducted by a third-party security audit at least once per year, and must ensure compliance with ISO 27001, IEC 62443 (Industrial Cybersecurity), Directive (EU) 2022/2555 of the European Parliament and of the Council (protection of Network and Information Systems - NIS2) and align with the Industrial Solar Alliance objectives for enhancing EU solar manufacturing security. As a response to increasing European exposure to cyber-attack, Directive 2022/2555 or NIS2 replaced its immediate predecessor, Directive 2016/1148 or NIS1. With NIS2, the ambition of EU cyber-security increases through an expansion of scope, more defined rules and stricter supervision measures. It encourages all EU Member States to strengthen their cybersecurity capabilities through the introduction of risk management and reporting obligations on organisations across various sectors, and also establishes requirements on cooperation, exchange of information, oversight and enforcement of cybersecurity practices [81].

5.3. Compulsory Security Measures

As PV systems become more integral to energy infrastructure, addressing these cyber threats is crucial to maintaining their reliability and safety. The key main strategies are (i) robust cybersecurity measures (strong encryption, regular software updates, and IDS to protect from unauthorized access and attacks), (ii) supply chain vigilance (acquiring main components from reputable manufacturers with transparent security practices can reduce the risk of embedded vulnerabilities), and (iii) regulatory compliance (adhering to established cybersecurity standards and guidelines can enhance the resilience of PV systems against potential threats).

PV systems are increasingly vulnerable to cybersecurity threats as they become more connected and automated. The key components of a PV system can be exploited if not properly secured.

To protect PV systems from cyber threats, operators should consider a number of compulsory security measures:

- ensuring that all software and firmware in the system are up-to-date by regular updates and patch management;
- the use of MFA and enforce strong passwords for remote access to devices and control systems for a strong authentication;
- encrypting data both at rest and during transmission to protect sensitive information.
- isolate critical components (e.g., inverters, energy management systems) from less critical systems to reduce the attack surface using the network segmentation principle;
- deploy IDS to monitor any unusual activity and potential cyberattacks in real-time;
- secure physical assets with locks, surveillance cameras, and restricted access areas to prevent tampering;
- ensuring that PV components are sourced from reputable manufacturers with transparent security practices can reduce the risk of embedded vulnerabilities as part of a strong supply chain vigilance;
- adhering to established cybersecurity standards and guidelines can enhance the resilience of PV systems against potential threats.

 doi:10.20944/preprints202504.0357.v1

5.3. Cybersecurity Capability Maturity Model (C2M2) for PV Systems

A very useful self-evaluation tool for the companies managing PV systems, is the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) [82]. The ten domains of the model are an ordered collection of cybersecurity practices. Each collection dictates activities an organization must undertake to develop and sustain its capability in that domain. The Risk Management domain, for example, outlines practices to develop and enhance an organization's cybersecurity risk management capability. Each field in the framework includes a purpose statement and an overarching description of its associated practices, providing concise guidance on how to map cybersecurity actions to organizational objectives [81].

This model offers a formal structure for assessing and ranking the cybersecurity posture of an organization with the allocation of maturity indicator levels for ten distinct domains, as shown in Figure 11.

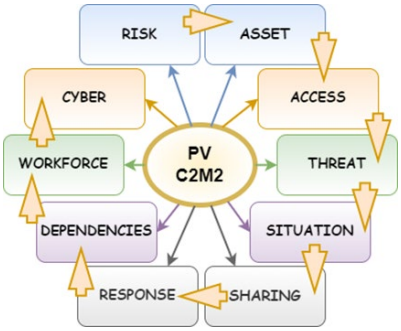


Figure 11. Cybersecurity Capability Maturity Model for solar power PV systems (C2M2). Source: Authors' elaboration.

1. Risk Management (RISK)

The goal of this framework is to ensure the secure operation of PV systems by managing OT and IT assets in a way that aligns with the risk to critical infrastructure and organizational objectives. Each identified risk is evaluated based on its likelihood and impact to establish priorities as seen in table 19.

Table 19. C2M2.

Risk type	Likelihood	Impact	Risk level
Unauthorized Remote Access	High	Critical	High
Malware/Ransomware Attack	High	High	Critical
Physical Theft or Vandalism	Medium	High	High
Weather-Related Damage	Medium	Medium	Medium
Regulatory Non-Compliance	Low	High	Medium

2.Asset, Change, and Configuration Management (ASSET)

Asset management focuses on maintaining a secure, updated, and properly configured inventory of all hardware, software, and infrastructure components in a PV system, change management ensures that any modifications to PV systems (hardware, software, or infrastructure) do not introduce security vulnerabilities or operational risks. Configuration management refers to Risk-based access control and incident response. Risk-based access control relies on controlling access to assets based on risk to ensure that only authorized personnel can interact with critical PV systems. Incident response and continuous improvement refers to access breach response, continuous risk assessment and user training and awareness.

3. Identity and Access Management (ACCESS)

 doi:10.20944/preprints202504.0357.v1

It establishes and maintains technologies, procedures, and plans to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities. The policy ensures that practices are proportionate with the risk to critical infrastructure, IT, and OT assets within PV systems.

4. Threat and Vulnerability Management (THREAT)

This policy establishes and maintains activities and technologies to collect, analyze, alarm, present, and use operational and cybersecurity information. It integrates data from various security domains to form a Common Operating Picture (COP) for the proactive identification and mitigation of threats and vulnerabilities in PV systems.

5. Situational Awareness (SITUATION)

Establishes and maintains relationships with external and internal organizations to acquire and provide cybersecurity information related to vulnerabilities and threats. The purpose is to reduce threats and maximize operational resilience within PV systems and complement the organizational and critical infrastructure protection objectives.

6. Information Sharing and Communications (SHARING)

Develop and implement procedures, plans, and technologies to detect, analyze, and respond to cybersecurity incidents and to maintain operations under the threat of a cybersecurity incident, commensurate with the risk to critical infrastructure and organizational missions.

7. Event and Incident Response, Continuity of Operations (RESPONSE)

Manage the organization's OT and IT assets, including both hardware and software, in relation to the risk to critical infrastructure and organizational objectives.

8. Supply Chain and External Dependencies Management (DEPENDENCIES)

Implement and maintain ongoing controls for monitoring cybersecurity threats of services and assets from third parties. These controls should be proportionate to the potential risk to critical infrastructure and aligned with the organization's strategic objectives.

9. Workforce Management (WORKFORCE)

Create and implement technologies, processes, and strategic plans for advancing a culture of cybersecurity, assuring current appropriateness and competency of personnel—proportional to the level of risk to critical infrastructure according to objectives of the organization.

10. Cybersecurity Program Management (CYBER)

Establish and maintain a company-wide information security program that fosters effective governance, strategic planning, and executive sponsorship of the company's security efforts, linking information security objectives to broader organizational goals and the evolving threat environment to critical infrastructure [82].

6. Results

Following examination of Romanian PV systems and their role in ensuring energy security, the authors recommend their designation (conversion) as critical energy infrastructures since they have a strategic role to play regarding the stability and solidity of the National Energy System and, at the same time, in ensuring national security and welfare.

Upon performing the SWOT analysis of the photovoltaic parks, 5 strengths, 10 weaknesses, 4 opportunities, 4 threats, 5 risks, 4 vulnerabilities, 4 hazards, 5 physical protection and security measures, 5 electrical safety and equipment protection measures and 3 natural factors and disaster protection measures were identified.

The assessment of blackout risk of photovoltaic parks in Romania (critical energy infrastructures) rezulted that the calculated risk level is 15 (probability 5 x severity 3), i.e., a High-risk level. For preventing or suppressing these kinds of risks, the authors developed and suggested 6 measures related to natural risk factors, 8 measures following technical risk factors, and 9 measures following human risk factors. After recalculation of the risk level, the value reduced to 9 (3 x 3), i.e. a Medium risk level.

The risk impact and likelihood analysis names unauthorized remote access and malware/ransomware attacks as the most serious cybersecurity threats to PV infrastructure. Both are

 doi:10.20944/preprints202504.0357.v1

given high likelihood and high impact ratings, with malware/ransomware attacks being extremely serious, assigned a critical risk rating. Both threats highlight the importance of using strong access controls, MFA, and active cybersecurity defense to protect PV infrastructure from cyber exploitation. Physical danger such as destruction or robbery has a high threat level due to their high impact rate, although their likelihood is lower than in the case of cyber threats. Weather loss, while not preventable, has a mid-level threat, which requires environmental watching, resilience building, and also possessing disaster preparedness to mitigate possible downtime. Regulatory non-compliance in the areas of energy and cybersecurity is a low-likelihood high-impact risk. While offenses may be few in frequency, their incidence may be harmful to the company in the form of significant fines, disruption of business, or damage to brand reputation. Ensuring adherence to industry standards, compliance frameworks, and national energy policy is essential in controlling this risk. Generally, the greatest short-term threats to PV systems are posed by cyber risks, requiring strong cybersecurity planning, real-time monitoring, and risk-reduction programs. Physical security and environmental toughness must not be neglected, though, as these support overall PV system stability and dependability.

European Union's PV industry association, emphasized the need for stronger cybersecurity protocols for distributed energy resources, as well. The association underlines the need of systems capable of centralized coordination or management, such as aggregated rooftop solar PV systems, to undergo authorized European or national-level monitoring. The industry suggests that while existing laws, such as the updated EU NIS2 directive and the Cyber Resilience Act, that provide a foundation of aggregated rules, additional measures are necessary.

Therefore, the authors recommend classifying PV systems as critical energy infrastructure, emphasizing the need of a stringent evaluations and proper protections. Devices that can be centrally coordinated or managed must be subject to an authorized European or national level of monitoring.

Author Contributions: Conceptualization, S.R. and ND.F.; methodology, S.R. and ND.F; investigation, R.S.; writing—original draft preparation, S.R.; writing—review and editing, ND.F.; supervision, D.P.;. All authors have read and agreed to the published version of the manuscript.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Nicolae Daniel Fîță, Mila Ilieva Obretenova, Adrian Mihai Șchiopu, Național Security – Elements regarding the optimisation of energy sector, *LAP – Lambert Academic Publishing*, UK, ISBN: 978-620-7-45693-2, 2024.
2. Nicolae Daniel Fîță, Adina Tătar, Mila Ilieva Obretenova, Security risk assessment of critical energy infrastructures, LAP – *Lambert Academic Publishing*, UK, ISBN: 978-620-7-45824-0, 2024.
3. Nicolae Daniel Fîță, Mila Ilieva Obretenova, Florin G. Popescu, Romanian Power System – European energy security generator *LAP – Lambert Academic Publishing*, UK, ISBN: 978-620-7-46269-8.
4. Daniel N. Fîță, Dan C. Petrilean, Ioan L. Diodiu, Analysis of the National Power Grid from Romania in the context of identifying vulnerabilities and ensuring energy security, Proceedings of Renewable Energy and Power Quality Journal (RE&PQJ), 22nd International Conference on Renewable Energies and Power Quality – ICREPQ 2004, Bilbao (Spain), ISSN 2172-038 X, Volume No.22 https://www.icrepq.com/icrepq24/386-24-fita.pdf, DOI: 10.24084/reepqj24.386.
5. Nicolae Daniel Fîță, Dan Codrut Petrilean, Ioan Lucian Diodiu, Andrei Cristian Rada, Adrian Mihai Schiopu, Florin Muresan-GrecuAnalysis of the causes of power crises and theit impacts on energy security, Proceedings of International Conference on Electrical, Computer ad Energy Technologies – ICECET 2204, July 2024, Sydney, Australia, Publisher IEEE, Date added to IEEE Explore: 08 October 2024, www.icecet.com, DOI: 10.1109/ICECET61485.2024.10698524, https://ieeexplore.ieee.org/document/10698524
6. Pasculescu D, Niculescu T., „Study of transient inductive-capacitive circuits using data acquisition systems", International Multidisciplinary Scientific GeoConference: SGEM. 2015;2(1):323-9.

 doi:10.20944/preprints202504.0357.v1

7. Pasculescu VM, Radu SM, Pasculescu D, Niculescu T., „Dimensioning the intrinsic safety barriers of electrical equipment intended to be used in potentially explosive atmospheres using the SimPowerSystems software package", International Multidisciplinary Scientific GeoConference: SGEM. 2013;1:417.
8. Pana L, Grabara J, Pasculescu D, Pasculescu VM, Moraru RI., „Optimal quality management algorithm for assesing the usage capacity level of mining tranformers", *Polish Journal of Management Studies*. 2018;18(2):233-44.
9. Popescu FG, Pasculescu D, Marcu MD, Pasculescu VM., „Analysis of current and voltage harmonics introduced by the drive systems of a bucket wheel excavator", *Mining of Mineral Deposits*. 2020 Dec 30.
10. Ilieva-Obretenova, M., "Information System Functions for SmartGrid Management", *Sociology Study*, Volume 6, Number 2, February 2016, (Serial Number 57) pp. 96-104, ISSN 2159-5526 (Print), ISSN 2159-5534 (Online), DOI: 10.17265/2159-5526/2016.02.002
11. Ilieva-Obretenova M. Impact of an energy conservation measure on reducing CO2 emissions. *Electrotechnica & Electronica* (E+E), Vol. 56 (3-4), 2021, pp.46-54, ISSN: 0861-4717 (Print), 2603-5421 (Online).
12. Rossi R, Mehan B., EU Market Outlook for Solar Power 2024-2028, 17 December 2024, https://www.solarpowereurope.org/insights/outlooks/eu-market-outlook-for-solar-power-2024-2028, (accessed on 20 March 2025)
13. Dumitrașcu, M., Grigorescu, I., Vrînceanu, A. et al. An indicator-based approach to assess and compare the environmental and socio-economic consequences of PV systems in Romania's development regions. *Environ Dev Sustain* (2024). https://doi.org/10.1007/s10668-024-04585-7
14. Available online: https://ioplus.nl/en/posts/europes-solar-panel-installations-saw-a-significant-slowdown-in-2024 (accessed on 15 Febr 2025).
15. Available online: https://www.power-technology.com/data-insights/top-5-solar-pv-plants-in-development-in-romania (accessed on 10 Febr 2025).
16. Suri,Marcel; Betak,Juraj; Rosina,Konstantin; Chrkavy,Daniel; Suriova,Nada; Cebecauer,Tomas; Caltik,Marek; Erdelyi,Branislav., Global PV Power Potential by Country (English). Energy Sector Management Assistance Program (ESMAP) Washington, D.C. : World Bank Group. http://documents.worldbank.org/curated/en/466331592817725242
17. Available online: https://globalsolaratlas.info/global-pv-potential-study, accessed (10 Feb 2025)
18. Patrick Jowett, Romania's 2024 solar additions hit 1.7 GW, January 31, 2025 https://www.pv-magazine.com/2025/01/31/romanias-2024-solar-additions-hit-1-7-gw/?utm_source=chatgpt.com
19. Niculescu G., Avăcăriței G., Mihăilescu M., Mihai I., Radu V., Dulamea R., Nagy-Bege Z., Monitor of the Romanian PV Projects, March 2024 https://www.energynomics.ro/wp-content/uploads/2024/03/Report-Energynomics-PV-Monitor-March-2024-0.2.pdf?utm_source=chatgpt.com
20. Available online: https://www.globaldata.com/, accessed (02 Feb 2025)
21. Available online: https://documents1.worldbank.org/curated/en/466331592817725242/pdf/Global-PV-Power-Potential-by-Country.pdf (accessed 20 March 2024)
22. Available online: https://www.afm.ro/sisteme_fotovoltaice.php (accessed 20 Dec 2024)
23. Available online: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal/repowereu-affordable-secure-and-sustainable-energy-europe_en, (accessed 20 Jan 2025)
24. Available online: https://livoltek.com/products/, (accessed 10 Feb 2025)
25. Available online: https://support.enphase.com/, (accessed 05 Feb 20250)
26. Available online: https://energyworld.ro/2025/02/06/romania-romania-remains-extremely-deficient-in-energy-storage/
27. Available online: https://anre.ro/puteri-instalate/, (accessed 01 Feb 2025)
28. Marius Nicolae Badica, Carmen Matilda Marinescu (Badica), Silvian Suditu, Monica Emanuela Stoica, Identification, evaluation and minimization of industrial risks relating to gas pipelines, E3S Web of Conf. 225 02004 (2021), DOI: 10.1051/e3sconf/202122502004
29. Teymouri, A., A. Mehrizi-Sani, and C.-C. Liu. 2019. "Cyber Security Risk Assessment of Solar PV Units with Reactive Power Capability." Proceedings of IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society: 2,872–2,877. https://doi.org/10.1109/IECON.2018.8591583

 doi:10.20944/preprints202504.0357.v1

30. Moldovan D., Riurean S. Cyber-Security Attacks, Prevention and Malware Detection Application. J. Digit. Sci. 4(2), 3 – 23 (2022). https://doi.org/10.33847/2686-8296.4.2_1
31. Riurean P., Bolog G., Riurean S., The Rise of Sophisticated Phishing. How AI Fuels Cybercrime. JDS, 6(2), 15-25, (2024). https://doi.org/10.33847/2686-8296.6.2_2
32. Jay Johnson, "Roadmap for PV System Cyber Security", December 2017, Report number: SAND2017-13262Affiliation: Sandia National Laboratories https://www.researchgate.net/publication/322568290_Roadmap_for_PV_Cyber_Security
33. Walker, Andy, Jal Desai, Danish Saleem, and Thushara Gunda. 2021. Cybersecurity in Photovoltaic Plant Operations. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5D00-78755. https://www.nrel.gov/docs/fy21osti/78755.pdf. Available online: https://www.energy.gov/eere/solar/solar-cybersecurity
34. Cynthia Brumfield, Hijack of monitoring devices highlights cyber threat to solar power infrastructure, May 2024, https://www.csoonline.com/article/2119281/hijack-of-monitoring-devices-highlights-cyber-threat-to-solar-power-infrastructure.html
35. J. Ye et al., "A Review of Cyber–Physical Security for PV Systems," in IEEE Journal of Emerging and Selected Topics in Power Electronics, vol. 10, no. 4, pp. 4879-4901, Aug. 2022, doi: 10.1109/JESTPE.2021.3111728
36. Călin, A.-M.; Cotfas, D.T.; Cotfas, P.A. A Review of Smart PV Systems Which Are Using Remote-Control, AI, and Cybersecurity Approaches. Appl. Sci. 2024, 14, 7838. https://doi.org/10.3390/app14177838
37. Volker Naumann, Dominik Lausch, Angelika Hähnel, Jan Bauer, Otwin Breitenstein, Andreas Graff, Martina Werner, Sina Swatek, Stephan Großer, Jörg Bagdahn, Christian Hagendorf, Explanation of potential-induced degradation of the shunting type by Na decoration of stacking faults in Si solar cells, Solar Energy Materials and Solar Cells,Volume 120, Part A,2014,Pages 383-389,ISSN 0927-0248, https://doi.org/10.101
38. A. M. Saber, A. Youssef, D. Svetinovic, H. Zeineldin and E. El-Saadany, "Learning-Based Detection of Malicious Volt-VAr Control Parameters in Smart Inverters," *IECON 2023- 49th Annual Conference of the IEEE Industrial Electronics Society*, Singapore, Singapore, 2023, pp. 1-6, doi: 10.1109/IECON51785.2023.10312615.
39. Sourav, S., Biswas, P. P., Chen, B., & Mashima, D. (2022). Detecting Hidden Attackers in PV Systems Using Machine Learning. ArXiv. https://arxiv.org/abs/2210.05226
40. Lindström, M., Sasahara, H., He, X., Sandberg, H., & Johansson, K. H. (2020). Power Injection Attacks in Smart Distribution Grids with PVs. ArXiv. https://arxiv.org/abs/2011.05829
41. Zografopoulos, I., Hatziargyriou, N. D., & Konstantinou, C. (2022). Distributed Energy Resources Cybersecurity Outlook: Vulnerabilities, Attacks, Impacts, and Mitigations. ArXiv. https://doi.org/10.1109/JSYST.2023.3305757
42. Thomas Feenstra Helin, Solar cybersecurity vulnerabilities: 6 ways in which hackers target solar installations, October 15, 2024, https://www.helindata.com/blog/solar-cybersecurity-vulnerabilities
43. A. Teymouri, A. Mehrizi-Sani and C. -C. Liu, "Cyber Security Risk Assessment of Solar PV Units with Reactive Power Capability," IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society, Washington, DC, USA, 2018, pp. 2872-2877, doi: 10.1109/IECON.2018.8591583
44. I. Zografopoulos, N. D. Hatziargyriou and C. Konstantinou, "Distributed Energy Resources Cybersecurity Outlook: Vulnerabilities, Attacks, Impacts, and Mitigations," in IEEE Systems Journal, vol. 17, no. 4, pp. 6695-6709, Dec. 2023, doi: 10.1109/JSYST.2023.3305757
45. Harrou Fouzi, Taghezouit Bilal, Bouyeddou Benamar, Sun Ying; Cybersecurity of PV systems: challenges, threats, and mitigation strategies: a short survey, *Frontiers in Energy Research*, Vol 11, 2023, DOI=10.3389/fenrg.2023.1274451
46. Maghami, M.R., Mutambara, A.G.O. & Gomes, C. Assessing cyber-attack vulnerabilities of distributed generation in grid-connected systems. *Environ Dev Sustain* (2025). https://doi.org/10.1007/s10668-024-05929-z
47. Bai, X., Liu, L., Wei, D., and Cao, J. “Research on security threat and evaluation model of new energy plant and station,” in Proceedings - 2020 International Conference on Computer Communication and Network Security, Xi'an, China, August 2020. doi:10.1109/CCNS50731.2020.00025

 doi:10.20944/preprints202504.0357.v1

48. Mustafa, A., Poudel, B., Bidram, A., and Modares, H. (2020). Detection and mitigation of data manipulation attacks in AC microgrids. IEEE Trans. Smart Grid 11, 2588–2603. doi:10.1109/TSG.2019.2958014
49. Huang, T., Wang, B., Ramos-Ruiz, J., Enjeti, P., Kumar, P. R., and Xie, L. "Detection of cyber-attacks in renewable-rich microgrids using dynamic watermarking," in Proceedings of the IEEE Power and Energy Society General Meeting, Montreal, QC, Canada, August 2020. doi:10.1109/PESGM41954.2020.9282071
50. Patel, A., Roy, S., and Baldi, S. (2021). Wide-area damping control resilience towards cyber-attacks: A dynamic loop approach. IEEE Trans. Smart Grid 12, 3438–3447. doi:10.1109/TSG.2021.3055222
51. Zhao, L., Li, J., Li, Q., and Li, F. (2022). A federated learning framework for detecting false data injection attacks in solar farms. IEEE Trans. Power Electron 37, 2496–2501. doi:10.1109/TPEL.2021.3114671
52. Zhang, J., Guo, L., and Ye, J. (2022). Cyber-attack detection for PV farms based on power-electronics-enabled harmonic state space modeling. IEEE Trans. Smart Grid. 13, 3929–3942. doi:10.1109/TSG.2021.3121009,
53. Beg, O. A., Nguyen, L. V., Johnson, T. T., and Davoudi, A. (2019). Signal temporal logic-based attack detection in DC microgrids. IEEE Trans. Smart Grid 10, 3585–3595. doi:10.1109/TSG.2018.2832544
54. Singh, V. K., and Govindarasu, M. (2021). A cyber-physical anomaly detection for wide-area protection using machine learning. IEEE Trans. Smart Grid. 12, 3514–3526. doi:10.1109/TSG.2021.3066316
55. Guo, L., Zhang, J., Ye, J., Coshatt, S. J., and Song, W. (2022). Data-driven cyber-attack detection for PV farms via time-frequency domain features. IEEE Trans. Smart Grid 13, 1582–1597. doi:10.1109/TSG.2021.3136559
56. Rahim, FA, et.al., Cybersecurity Vulnerabilities in Smart Grids with Solar Photovoltaic: A Threat Modelling and Risk Assessment Approach, International Journal of Sustainable Construction Engineering and Technology, Vol. 14, Iss. 3, 210-220, DOI: 10.30880/ijscet.2023.14.03.018
57. Ioan Alexandru MELNICIUC, Alexandru LAZĂR, George CABĂU, Radu Alexandru BASARABA, Bitdefender Disclosure Report, Solarman Platform Vulnerability https://blogapp.bitdefender.com/labs/content/files/2024/08/Bitdefender-PReport-solarman-creat7907.pdf
58. Eduard Kovacs, Vulnerabilities Exposed Widely Used Solar Power Systems to Hacking, Disruption, August 8, 2024, https://www.securityweek.com/vulnerabilities-exposed-widely-used-solar-power-systems-to-hacking-disruption/
59. Available online: https://www.csoonline.com/article/2119281/hijack-of-monitoring-devices-highlights-cyber-threat-to-solar-power-infrastructure.html, (accessed 15 Dec 2024)
60. Available online: https://www.climatesolutionslaw.com/2025/02/cybersecurity-and-solar-power-vulnerability, (accessed 28 Febr 2025)
61. Available online: https://www.investopedia.com/solar-power-stocks-fall-on-concerns-about-potential-hackers-8685365, (accessed 20 Oct 2024)
62. Available online: https://www.reuters.com/business/energy/finnish-utility-fortums-power-assets-targeted-with-surveillance-cyber-attacks-2024-10-10/, accessed 20 Dec 2024
63. Nikolaus J. Kurmayer, White hat hacker shines spotlight on vulnerability of solar panels installed in Europe, Oct 1, 2024, https://www.euractiv.com/section/energy-environment/news/hacker-shines-spotlight-on-vulnerability-of-solar-panels-installed-in-europe
64. Available online: https://nvd.nist.gov/, (accessed 28 Feb 2025)
65. Available online: https://cve.mitre.org/, (accessed 05 Feb 2025)
66. Y. Dubasi, A. Khan, Q. Li and A. Mantooth, "Security Vulnerability and Mitigation in Photovoltaic Systems," 2021 IEEE 12th International Symposium on Power Electronics for Distributed Generation Systems (PEDG), Chicago, IL, USA, 2021, pp. 1-7, doi: 10.1109/PEDG51384.2021.9494252
67. Available online: https://www.cisa.gov/news-events/ics-advisories/icsa-25-044-16, (accessed 12 Feb 2025)
68. Available online: https://dnsc.ro/citeste/alerta-vulnerabilitati-critice-de-securitate-cibernetica-identificate-la-nivelul-unor-produse-myscada, (accessed 08 Feb 2025)
69. Available online: https://www.myscada.org/, (accessed 20 Feb 2025)
70. Available online: https://www.cisa.gov/news-events/ics-advisories/icsa-25-044-16, (accessed 08 Feb 2025)
71. Available online: https://cwe.mitre.org/., (accessed 20 Feb 2025)

 doi:10.20944/preprints202504.0357.v1

72. Available online: https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H, (accessed 20 Feb 2025)
73. Available online: https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N, (accessed 20 Feb 2025)
74. Available online: https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H, (accessed 20 Feb 2025)
75. Available online: https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H, (accessed 20 Feb 2025)
76. Tatiana Antipova, Simona Riurean, Managing cyber resilience literacy for consumers, *International Journal of Informatics and Communication Technology (IJ-ICT)* 122 Vol. 14, No. 1, April 2025, pp. 122~131 ISSN: 2252-8776, DOI: 10.11591/ijict.v14i1.pp122-131
77. "IEEE Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems," in *IEEE Std 1547.3-2023 (Revision of IEEE Std 1547.3-2007)* , vol., no., pp.1-183, 11 Dec. 2023, doi: 10.1109/IEEESTD.2023.10352402
78. Peng, S., Liu, M., Zuo, K., Tan, W., and Deng, R. "Stealthy data integrity attacks against grid-tied PV systems," in Proc. - 2023 IEEE 6th Int. Conf. Ind. Cyber-Physical Syst. ICPS, Wuhan, China, May 2023, 1–7. doi:10.1109/ICPS58381.2023.10128033
79. Simona Riurean, Tatiana Antipova, Prebunking, An Effective Defense Mechanism To Strengthen Consumers' Cyber Awareness, *Annals of the University of Petrosani*, Electrical Engineering, 26 (2024)
80. Available online: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive, (accessed 20 Dec 2024)
81. Available online: https://www.energy.gov, (accessed 20 Feb 2025)
82. Jay Johnson, Roadmap for PV Cyber Security. Report number: SAND2017-13262, Affiliation: Sandia National Laboratories, Available from: https://www.researchgate.net/publication/322568290_
83. Available online: https://indiasmartgrid.org/upload/201705Wed174314.pdf, (accessed 28 Feb 2025)