# Cybersecurity for critical PV systems

**Words:** Max Miller, Information Security Officer (ISO) and Vivian Bullinger, Product Marketing Manager, Solar-Log GmbH

The digitalisation of photovoltaic systems is steadily increasing, offering significant advantages such as remote monitoring, performance optimisation and predictive maintenance. However, greater connectivity also introduces heightened security risks. Without adequate protection, hackers could exploit vulnerable PV systems, gaining access to sensitive data, manipulating system operations, or potentially destabilising the power grid.

Recent studies indicate that over 76% of exposed solar power devices worldwide are located in Europe, with Germany and Greece each accounting for approximately 20% of the global total of unintentionally exposed systems.[1]

Nevertheless, there are effective methods available to actively protect PV systems and secure sensitive data. To ensure robust security, it is essential to identify the potential points of attack and vulnerabilities clearly in advance. The primary vulnerabilities are summarised below.

## Points of attack for PV systems

There are various points of attack for unauthorised access to PV systems. In order to protect them effectively, it is important to know and identify these in advance. We have summarised the biggest vulnerabilities here:

### Insufficient password protection

Some inverters, monitoring devices or gateways are publicly accessible via standard passwords or without VPN and are therefore vulnerable to attack.

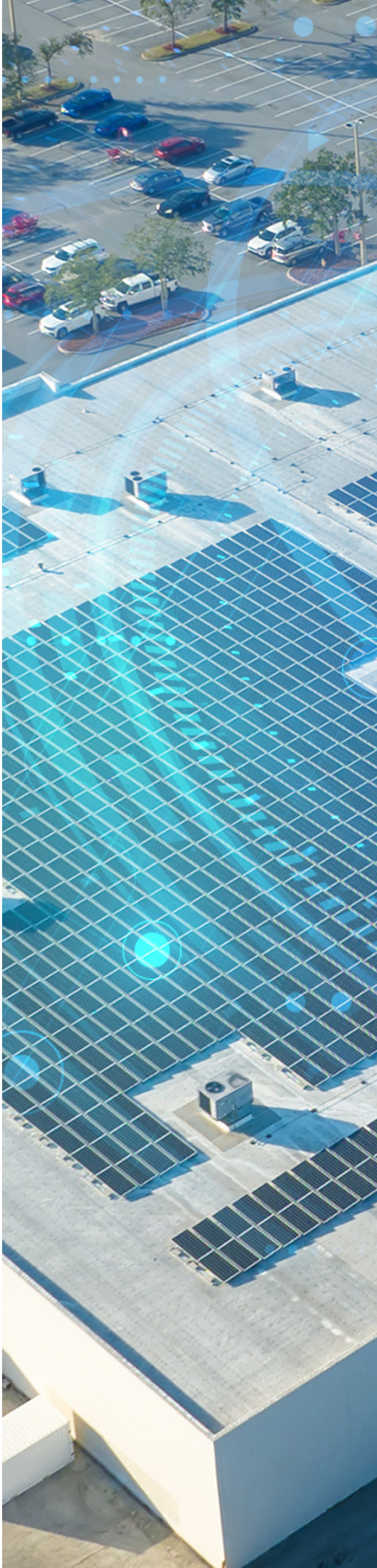
### Weak authentication

Weak authentication practices exacerbate the general password security issue. Simple passwords used without additional verification procedures are frequently targeted by attackers.

Two-factor authentication (2FA) is increasingly implemented to strengthen password security. With 2FA, users must provide an additional method of verification beyond their primary password to successfully log in.

### Firmware updates

Firmware updates from manufacturers are frequently overlooked by users. Manufacturers regularly release updates containing new features, bug fixes and essential cybersecurity improvements.



Max Miller

Failure to install these updates can expose systems to security vulnerabilities, potentially allowing attackers to infiltrate with malware such as Trojans.

## Main risks of cyber attacks for PV systems

If unauthorised persons have gained access to the PV system, there are various options for misusing this access. The targets can be very different. Knowing these helps to protect the systems.

### Manipulation of power & grid stability

Successful attacks on PV systems can influence feed-in power and, in extreme cases, lead to grid instability or power outages. The impact in such a case would be serious.

### Ransomware and sabotage

Ransomware attacks can encrypt PV control systems. The operator is then often

Vivian Bullinger

blackmailed into shutting down the system, which is then only released again after payment of high demands.

## Effective protection of the points of attack

How do you protect yourself against attacks and the possible consequences? The responsibility here lies not only with the manufacturers but also with the operators. They must implement the manufacturer's measures and constantly keep an eye on whether the systems are up to date.

### Strong authentication

Standard passwords must be changed immediately. All applications should use multi-factor authentication (MFA) to prevent identity theft.

### Regular updates & patches

Firmware and software updates are mandatory. Manufacturers are continuously working on so-called manufacturer patches, i.e. updates for software that address security vulnerabilities. The patches are included in the firmware updates and must be installed by the operators.

### Monitoring & logging

All access and configuration changes must be auditable. Special monitoring tools help here by recognising anomalies and unauthorised access at an early stage.

### Backup & incident response

An emergency plan for data leaks or system failures is essential. Data must be backed up and those responsible must know how to respond correctly to incidents.

### Employee training

It is important that technical employees and operators are regularly trained in cybersecurity and sensitised accordingly, for example, about phishing attacks, social engineering or social media risks.

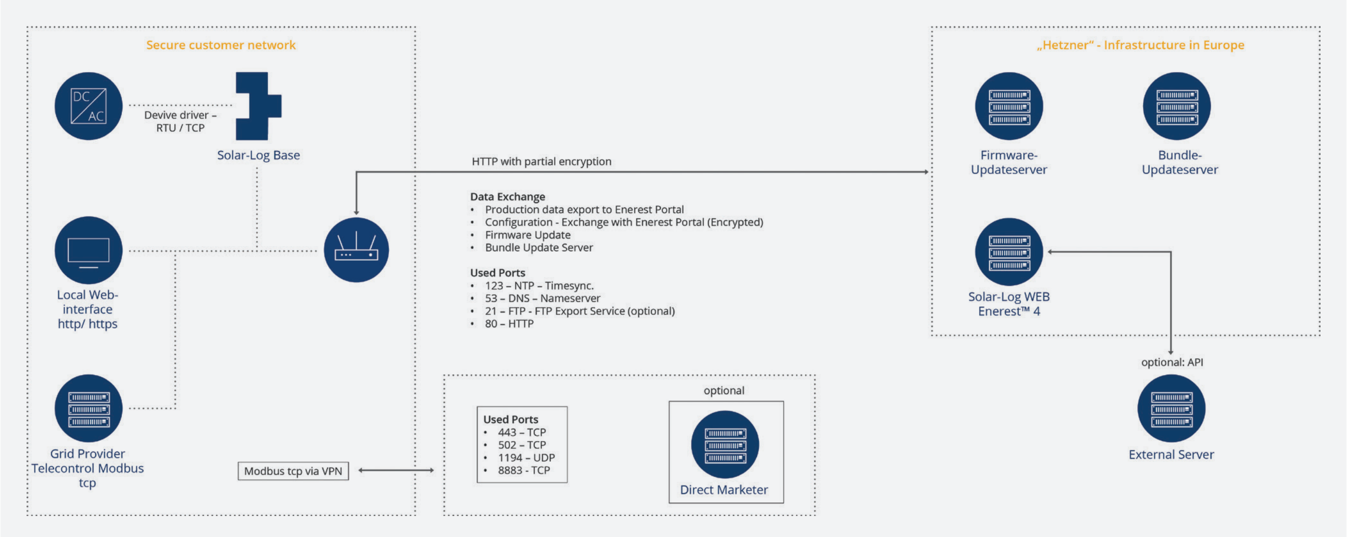
### Data protection & GDPR

Always ensure that manufacturers comply with applicable data protection regulations. Live electricity data contains personal information and therefore requires special protection. Such data may only be shared if there is a valid contractual and legal basis, consistent with GDPR requirements.

## Security measures in PV monitoring

The vulnerabilities listed above apply to all components within a PV system, including inverters, gateways and monitoring and management systems. Energy management systems, such as those from Solar-Log, are particularly critical, as they form the interface between PV systems and energy suppliers, and therefore require robust protection.

A key issue in protecting the PV system is securing data transmission. Solar-Log relies on modern encryption standards such as



The diagram shows the network communication of the Solar-Log™ Base PV energy management system in a secure customer network. This is where data is transferred to the Solar-Log WEB Enerest™ online portal and firmware and bundle updates are carried out. This architecture ensures secure, structured communication between local devices, cloud services and optional partners such as direct marketers or external servers

> **Only a holistic approach, from hardware, software and networking to organisational and compliance aspects, can make PV systems future-proof and resistant to threats.**

Transport Layer Security (TLS) to ensure secure communication between devices, portals and mobile applications. In addition, the data in the cloud is also protected by encryption. The cloud service providers used are certified in accordance with ISO 27001, which guarantees high standards of security and availability.

Another focus is on user and access management. Solar-Log utilises the principle of least privilege and introduces role-based access control. Users must use strong passwords and two-factor authentication (2FA) is offered on request. Access processes are fully logged and can be analysed if required.

Strict security principles are also followed in software development. The source code is checked internally, regularly scanned for vulnerabilities and checked by external penetration tests. This is to ensure that vulnerabilities are discovered and eliminated at an early stage. Customers are informed about security-relevant updates and receive clear instructions on how to install new firmware.

In the event of a security incident, Solar-Log has its own incident response team. This team analyses and evaluates detected security problems, coordinates countermeasures and informs affected users as quickly as possible.

Solar-Log also pays attention to security aspects during product development ('Security by Design'). This includes, for example, the use of Proof Key for Code Exchange (PKCE) for web authentication. The integration of secure technologies and the protection of local device interfaces against unauthorised access are also standard.

To summarise, it is clear that a holistic approach to cybersecurity is being pursued. This combines technical measures with organisational processes and focuses on transparency and continuous improvement.

## Supplementary measures by manufacturers and authorities

In addition to users and manufacturers, the topic of 'cybersecurity in PV systems' is also an important issue for public authorities.

### National recommendations

The German Federal Office for Information Security (BSI) expressly warns against authorising grid-serving control via internet-enabled components from abroad. Instead, decentralised technologies such as smart metering systems are recommended in order to minimise potential backdoors.[2]

### Classification as critical infrastructure

Large PV parks of 104 MW are considered critical infrastructures (KRITIS). Operators must comply with IT security standards, enable regular audits and take special measures against sabotage.

### Best practices & frameworks

Recommended guidelines:

- NIST Cybersecurity Framework: is a voluntary collection of guidelines and best practices developed by the National Institute of Standards and Technology (NIST) to help organisations manage and mitigate their cybersecurity risks. It provides a structured approach to cybersecurity risk management that integrates existing standards, guidelines and best practices.
- Cybersecurity and Infrastructure Security Agency (CISA) Recommendations: issues recommendations and guidance on various aspects of cybersecurity aimed at organisations and individuals. These include general cybersecurity practices as well as specific recommendations for the protection of critical infrastructure and the secure procurement of technology.
- Zero Trust Architecture (ZTA): Assumption that every device on the network is considered potentially compromised. It is a cybersecurity framework based on the principle of 'never trust, always verify'. It assumes that no user or device, even within a conventional network, should automatically be categorised as trustworthy.

### Summary

Photovoltaic systems today are far more than just modules made of glass and silicon, they are part of complex cyber-physical systems. Increasing digitalisation offers many opportunities, but the risks range from data breaches to critical disruptions to the energy infrastructure.

Operators should be vigilant and secure their systems, install updates and carry out regular staff training if necessary. Providers such as Solar-Log GmbH offer operators a solid technical basis for protecting their systems: role-based access, MFA, pen tests, IDS and Incident Response are the cornerstones of their security concept.

Last but not least, politicians and authorities have also made their contribution: the BSI demands decentralised control and trustworthy technologies; large systems are subject to KRITIS standards.

Only a holistic approach, from hardware, software and networking to organisational and compliance aspects, can make PV systems future-proof and resistant to threats.

solar-log.com

**Reference**

[1] Forescout Technologies, Inc. 'Sun Down Research Report,' available at: https://www.forescout.com/resources/sun-down-research-report

[2] Source: pv-magazine.de

**Recommended actions for PV system operators**

1. Inventory of all PV components, identification of sensitive interfaces.
2. Firmware audit: Are all systems up to date? Replace outdated devices if necessary.
3. Network segmentation: PV devices are only accessible via VPN - isolated from the main network.
4. Password hygiene & MFA introduction.
5. Configure and regularly analyse logging & monitoring.
6. Ensure backup concepts for logs and configuration data.
7. Set up a strong firewall, IDS/IPS and anti-malware.
8. Establish cyber insurance & emergency plans.
9. Compliance audit for large systems (>104 MW) according to KRITIS standards.