Technical Information

PUBLIC CYBER SECURITY

Guidelines for a Secure System Communication

Table of contents

1 Information on this Document

1.1 Validity

This document applies to all products (e.g. inverters, batteries, communication products) of a PV system. These products can be connected to the Internet directly or indirectly via communication media. This includes products from SMA as well as from other manufacturers.

This document supplements the documents that are enclosed with each product and does not replace any locally applicable codes or standards. Read and observe all documents supplied with the products.

1.2 Target Group

The information in this document is intended for installers and operators of PV systems with SMA products as well as for PV system planners.

1.3 Content and Structure of this Document

This document describes technical and organizational measures that must be implemented by installers and operators of SMA products for the safe operation of PV systems. As a manufacturer, SMA is aware of its responsibility and implements a high level of cyber security in its devices based on the SMA Secure Development Life Cycle. A Secure Development Live Cycle encompasses all security measures throughout the entire life cycle of a product, from design to decommissioning. The SMA Secure Development Life Cycle is aligned with IEC 62443-4-1.

However, in order to reduce risks as far as possible, the support of all parties involved is required. SMA therefore strongly recommends that installers, operators and planners of PV systems observe and implement the requirements listed in this document.

2 Introduction

2.1 Aims of Cyber Security

Cyber security is crucial for protecting data, privacy and maintaining business operations. SMA pursues the following goals in cyber security:

- **Protection of sensitive data**: Data collected by SMA products or stored on these products cannot be misused by cyber criminals.
- **Avoidance of financial losses**: Financial losses due to cyber attacks can lead to financial losses for both individuals and companies.
- **Adherence to compliance and legal obligations**: Companies comply with cybersecurity standards and regulations when using SMA products. This avoids legal consequences and preserves the trust of stakeholders.
- **Ensuring business continuity**: Effective cyber security measures prevent interruptions caused by cyber incidents and thus ensure smooth operations. They ensure a continuous energy supply for energy systems.

When using the Internet infrastructure, the systems connected to the Internet are entering a basically unsecure area. Potential attackers constantly seek vulnerable systems. Usually, they are criminally motivated, have a terrorist background or aim to disrupt business operations. Without taking any measures to protect PV systems and other systems from such misuse, a data communication system should not be connected to the Internet.

2.2 Applications of PV systems in the global communication system

Most operating activities such as monitoring and control of systems can be done locally by the PV system operator or service department without the need for data communication via public Internet infrastructure. These operating activities include data communication between system operators, the service department and PV inverters, data loggers or additional equipment. They can be made via local displays, keypads or local access to the webserver of a device in the local network (LAN) of the PV system or the house.

In some use cases of PV systems, the PV system is also part of the global communication system, which is based on Internet infrastructures. The data communication via Internet is an up-to-date, economically viable and customer-friendly approach in order to enable easy access for the following modern applications such as:

- Cloud platforms (e.g. Sunny Portal)
- Smartphones or other mobile terminals (iOS or Android apps)
- SCADA systems, which are remotely connected
- Utility interfaces for grid management services

Alternatively, selected and secured communication interfaces may be used. These solutions are no longer state of the art and are very expensive to use. This applies, for example, to dedicated communication interfaces or separate wide area networks (WAN).

Also see:

- Hardening ⇒ page 7

3 Scenarios for Cyber Attacks

Cybersecurity risk assessment involves evaluating the likelihood and impact of attacks on specific devices or systems. In order to maintain an overview, it is crucial to evaluate all potential attack scenarios. This is achieved by outlining possible attack scenarios for a device or system. The intended use and ambient conditions of the device or system must be taken into account.

Below you will find a non-exhaustive list of important attack scenarios, possible consequences for devices and systems as well as their operators and some countermeasures. Note that actual attacks usually involve a combination of different scenarios.

Attack scenario	Possible targets of the attacker	Possible consequences for operators	Countermeasures
Spear phishing: The attacker contacts the victim directly by email or telephone to obtain login information for a device, for example.	• Manipulation of the device or the system • Inflicting damage	• Loss of control over the system • Financial losses • Specifications of the grid operator and normative specifications are no longer complied with	• Do not pass on any login information. • Keep login information safe and inaccessible to third parties.
Remote access with standard access data: The attacker searches for devices that are connected to the Internet, e.g. because port forwarding is activated in the router. The devices were not commissioned correctly.	• Manipulation of the energy supply of an entire region • Inflicting damage	• Loss of control over several plants in one region or plants with products from one manufacturer • Financial losses • Grid failures	• Never activate port forwarding in the system's router. • Carry out commissioning as described in the manuals for the devices or the system.
Advanced Persistent Threats (APT): The attacker installs technically sophisticated malware on the target device or system. The malware is not detected. The attacker triggers the attack at a later suitable time.	• Manipulation of the energy supply of an entire region • Inflicting damage	• Loss of control over several plants in one region or plants with products from one manufacturer • Destruction of the target device or system • Financial losses • Grid failures	• Perform hardening of the devices and systems (see Section 5.1, page 7). • Segment the network. • Set extended access restrictions for installations. • Use intrusion detection systems (IDS).

4 Example of a cyber attack: Downgrade attack

Real attacks consist of several attack steps, all of which together are referred to as an 'attack vector'. A possible concrete attack vector for an attack on a PV system is described below. This example describes a downgrade attack. This refers to attacks that reset a firmware to an outdated version so that security gaps that have already been closed are reopened by new versions.

This is not a description of a real attack or a real system or device, but a theoretical example.

Target of the attacker: An attacker wants to gain access to an inverter in order to switch it off. In an earlier firmware version, there was a publicly known vulnerability that allowed login without a password. In addition, the device's user interface enables updates without authentication.

Procedure of attackers:

1. The attacker uses a specialized international search engine to identify a target inverter that is connected to the Internet via port forwarding. The attacker establishes a connection to the target device.
2. The attacker uses public and device-specific information to evaluate which firmware version is being used on the device. The software used is a newer version in which the security vulnerability has already been fixed.
3. The attacker searches for an old firmware version that has the vulnerability. The attacker searches for this version in various Internet resources and finally obtains it in a special discussion forum.
4. The attacker uses the old firmware version and attempts to upload this firmware via the user interface. This is possible because the device allows an update without authentication.
5. Now the attacker must wait until the device is restarted. The target device only carries out updates at night.
6. The device installs the old firmware including the vulnerability. Since the device does not check the version of an update, the downgrade is possible. This is the main reason why this attack is possible.
7. The attacker gains access to the inverter via the vulnerability in the old firmware version and manipulates parameters so that the inverter no longer feeds into the grid.

5 Measures for cyber security

5.1 Hardening

As cyber threats continue to evolve, cyber security is critical for individuals, organizations and governments worldwide. Hardening is an effective means of significantly reducing the risk of cyber attacks. Hardening is a technique to reduce the attack surface of a system to a minimum by reducing entry points for attacks on a device. For example, the security of a system can be increased by only using software that is necessary for the operation of the system and whose secure operation can be guaranteed.

The recommendations must be followed in all installations.

5.2 Responsibility of the system operator for cyber security

In order to effectively protect PV systems from unwanted attacks by unauthorized persons (e.g. criminals or secret services), the local network must be kept as clean and closed as possible. When a PV system or a similar system is being connected to the Internet, the PV system operator or network administrator has the following responsibilities:

- Knowledge of all devices active in the local network (asset management)
- Knowledge of the communication requirements and features of all devices (secure communication, hardening)
- Knowledge of possible vulnerabilities of all devices (e.g. automatic updates)
- Knowledge of all accounts that access the systems (identity and access management)
- Knowledge of options to limit access to the local network and the devices (e.g. by using secure passwords)
- Installing and configuring all necessary security measures relating to cybersecurity (router, firewall, proxy server, network segmentation)
- Examining and, if necessary, improving the security measures with regard to being up to date and suitable

Also see:

- Asset Management ⇒ page 8
- Hardening ⇒ page 7

5.3 Behind the fence strategy (BTF)

If the system operator fulfills its responsibility with regard to cyber security (see Section 5.2, page 7), it can be assumed that the PV system is operated in a system that has the status 'behind the fence' (BTF). Direct access from the outside is not possible immediately.

Most industrial communication systems mainly use standardized fieldbus communication protocols. Due to this fact, a BTF strategy is indispensable because most fieldbus systems do not have any built-in security mechanisms and need to be secured by additional means. This also applies to both of the fieldbus communication protocols SMA Data2+ and Modbus TCP used in SMA Solar Technology AG communication solutions.

The password protection of the Data2+ communication protocol provides a security function for SMA products. As an exception, the WAN communication protocol Webconnect provides a secure communication with end-to-end encryption. However, Webconnect is not used in local networks. It is designed to be used for secure Internet communication between PV inverters or data loggers to Sunny Portal or to the mobile solutions.

i Security risk due to Modbus TCP

Modbus TCP is included in most SMA products as a public customer interface. Modbus TCP cannot be securely transmitted over the Internet without further ado. Within a PV system, the missing authentication of Modbus TCP can present a potential security risk. For this reason, Modbus TCP is deactivated in SMA products by default. If required, Modbus TCP must be activated in the user group "Installer". This activation is not to be carried out carelessly, but additional measures should always be taken to secure the overall system.

5.4 Defense in Depth Concept

For maximum security of your PV system, SMA recommends a Defense in Depth concept.

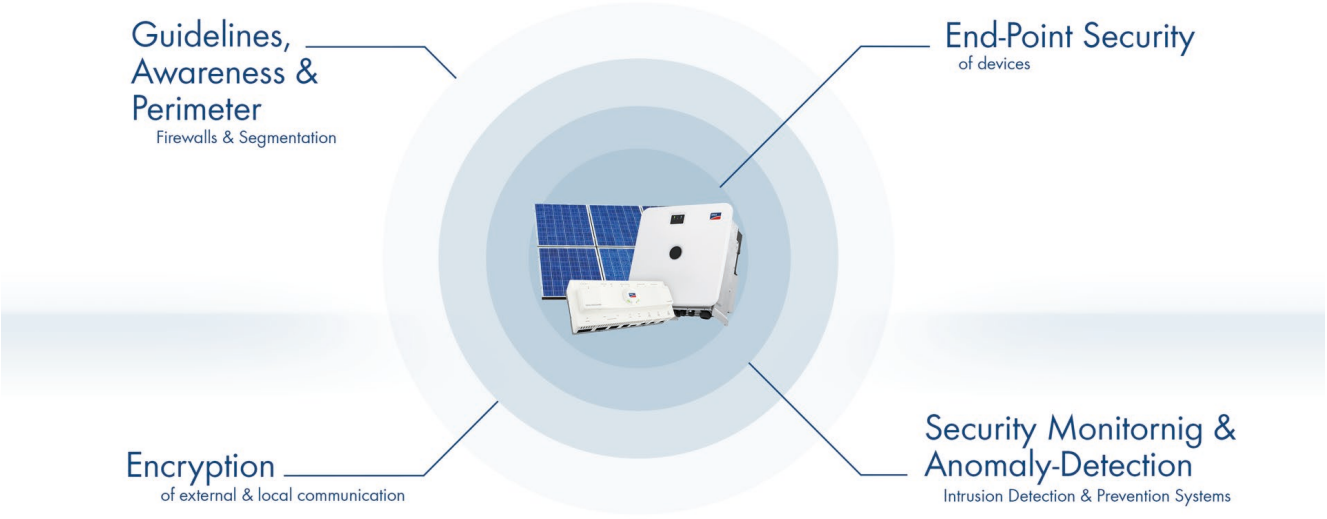

Figure 1: Illustration of the Defense in Depth concept

A holistic safety concept should be developed in accordance with IEC 62443. This standard is aimed at all those involved in the system, including operators, planners and manufacturers, and aims to establish an overall concept based on specific security levels for different zones and their connections.

5.5 Asset Management

5.5.1 Asset Management

Asset management refers to the management of all components located in the system and in the network. Up-to-date asset management is crucial for protecting a company's digital infrastructure. This is necessary for:

- **Detection of vulnerabilities**: Effective asset management helps to identify vulnerabilities in hardware, software, data and network resources. By understanding the asset and its value, location and vulnerability, companies can develop and prioritize security measures.
- **Minimization of risks**: Asset management ensures the functionality, availability and confidentiality of assets. It minimizes the risk of unauthorized access, security problems and data leaks.
- **Transparency and control**: Asset management provides insights into digital assets and enables companies to monitor and protect them throughout their lifecycle. Without proper management, companies may lack knowledge of key assets.

In home systems, it is usually sufficient to keep a document with a list of the components integrated in the home network. In large systems, professional, tool-based asset management is important for identifying risks, protecting critical system components and planning the resources required to manage the energy system. In many regions of the world, such asset management is required by law for certain types of investments.

5.5.2 Asset Management Checklist

The following list can be used to check the configuration of your PV system after initial commissioning. The test should also be repeated regularly to ensure that your system is protected against cybercrime throughout its entire life cycle.

- ☐ An up-to-date list of devices with the required information (IP address, device type, device name, etc.) must be available. This list can be maintained manually or automatically (recommended).
- ☐ An asset management service that collects all the necessary information and informs you of any changes should be integrated into your network.
- ☐ A process should be implemented to regularly check the Asset Management Service reports.

5.6 Identity and Access Management

5.6.1 Identity and Access Management

All access to electronic devices or sensitive premises should be secured by suitable authentication mechanisms and the allocation of usage rights depending on the user's role (authorization). This applies to any type of energy system or PV system (Home, Commercial & Industrial, Large Scale).

For more complex systems in the industrial or large-scale sector, there is a need for additional measures to achieve an appropriate level of security in terms of authentication and authorization. In such cases, tools for identity and access management should be implemented. These are an important part of a holistic cyber security strategy. This prevents unauthorized access, enables centralized automation and monitoring and activates an alarm in the event of incidents.

5.6.2 Checklist for Identity and Access Management

The following list can be used to check the configuration of your PV system after initial commissioning. The test should also be repeated regularly to ensure that your system is protected against cybercrime throughout its entire life cycle.

- ☐ All devices in your energy system must have appropriate identity management, e.g. by enforcing a login on all applications and assigning corresponding rights (role-based access control).
- ☐ A connection to a central user administration system, e.g. via LDAPS to an Active Directory (AD) system, should be available.
- ☐ User accounts should not be shared.
- ☐ If account sharing cannot be avoided, there must be a list of accounts and individual users who are allowed to use these accounts. There must be binding guidelines for the use of the accounts and processes for monitoring their use.

5.7 Segmentation

5.7.1 Segmentation

Network segmentation is a cybersecurity technique used to divide a network into smaller, isolated areas. This reduces the risk of malware or malicious attacks spreading across the entire network. In addition, network segmentation helps to separate sensitive data and applications from less secure components. It is an essential component of the network security architecture and improves control and resilience against cyber threats.

Some best practices are:

- **Continuous monitoring and testing of networks:** regular assessment of network segments to identify vulnerabilities and ensure proper configuration
- **Avoid over- or under-segmentation:** strive for a balance; too many segments can be complex, while too few can compromise safety
- **Limitation of third-party access points:** control external access to certain segments to prevent unauthorized access
- **Identify and tag assets:** Clarity on the importance of assets in each segment to prioritize protection (risk-based approach)
- Combination of similar network resources: Consolidation of related resources to simplify management and reduce complexity

5.7.2 Checklist for segmentation

The following list can be used to check the configuration of your PV system after initial commissioning. The test should also be repeated regularly to ensure that your system is protected against cybercrime throughout its entire life cycle.

- ☐ Create a network diagram that contains all relevant devices in your network.
- ☐ Add boundary lines around groups of devices ('segments') that should have the same security level, e.g. the home network or the company IT network and the energy system network.
- ☐ Implement the network separation for all segments defined in the diagram above. This is known as 'segmentation'.
- ☐ Check the effectiveness of the segmentation.

5.8 Secure Communication

5.8.1 Secure Communication

SMA implements different communication options (protocols) in its devices, depending on the requirements for the intended use of the respective device. In accordance with the 'Security by Design' rule, SMA's aim is to provide precisely those protocols that have up-to-date security mechanisms in order to achieve the security objectives of confidentiality, integrity and authentication. Common examples of such secure communication protocols are HTTPS (for websites and web applications) and FTPS/SFTP (for file exchange). In some cases, this goal cannot be achieved for reasons of interoperability or the availability of suitable alternatives.

The recommendations for secure communication must be followed in all installations.

5.8.2 List of insecure protocols and remedial measures

Below we provide some information and recommendations for those protocols that do not have adequate security mechanisms. Please note that not all of the protocols listed here may be available in your specific product. List of insecure protocols and remedial measures:

Log	Purpose	Risks	Risk mitigation measures
Modbus	Data exchange between different devices	• **No authentication**: It is unclear who is sending Modbus commands, possibly an attacker. • **No encryption**: Information can be disclosed and an attacker can intercept the communication.	• Modbus is deactivated by default in SMA devices. • Only activate Modbus if required and if communication within your local network is protected by a properly configured firewall. • Grid segmentation should be available for your PV system grid. • Never configure port forwarding in your local network or the network segment of your PV system.
FTP Push (File Transfer Protocol)	File exchange between different systems. No service is provided on the device for FTP push, only a connection option to third-party FTP servers.	• **No encryption**: The attacker can eavesdrop on the FTP communication and intercept the login data (ID, password). In a next step, he can use these credentials to log on to the FTP server and start manipulating or destroying files or uploading malicious files.	• Set up connections to third-party FTP servers that provide secure versions of FTP such as SFTP or FTPS. • If a third-party server does not provide a secure FTP version, only transfer unclassified data, in particular no secret data or passwords.

5.8.3 Checklist for Secure Communication

The following list can be used to check the configuration of your PV system after initial commissioning. The test should also be repeated regularly to ensure that your system is protected against cybercrime throughout its entire life cycle.

☐ Ensure that all protocols that are not required for the intended use of a device are deactivated.

☐ Prevent the use of unencrypted protocols. If they are absolutely necessary, network disconnection should be implemented as a corrective measure.

☐ Ensure that all physical connections (e.g. USB) are deactivated if they are not required and deactivation is possible.

☐ If USB ports are provided that are not required and cannot be deactivated by software, you can use so-called 'port blockers'.

5.9 Updates

Most cyber security risks stem from software or software components (libraries) that have vulnerabilities. These risks can be eliminated by updating a device as soon as a software version is available that no longer contains the vulnerability. Therefore, it is first important to ensure that all your devices can be updated. This is the case with all SMA products.

In the next step, it is crucial to keep all your devices and especially all SMA products up to date. Security gaps are closed with updates to prevent attackers from exploiting vulnerabilities in the product. This also protects your data and prevents data breaches. Currently, more and more IoT (Internet of Things) devices are being misused by attackers to carry out attacks such as DDoS (Distributed Denial of Service) attacks. This is an attack that is carried out by many IP addresses simultaneously in order to overload the attacked service to such an extent that it can no longer be used by legitimate users.

IoT devices are also used to attack other systems on the Internet. By keeping your products up to date, you not only protect yourself, but also contribute to a safer Internet for everyone.

SMA recommends automatic updates where possible. All SMA devices can be updated automatically. If you decide against automated updates, you must implement an update strategy and an update process that defines people and responsibilities as well as a schedule for manual updates.

The recommendations for updates must be followed in all installations.

5.10 Logging and Monitoring

5.10.1 Logging and Monitoring

Even if all the recommendations in this document are followed, there may be situations in which a breach of security or an attack cannot be prevented. Additional measures should be provided for such cases, which at least enable attacks to be detected. Logging and monitoring is the main prerequisite for a quick and effective response to any type of incident. In the event of an incident, the speed of response and the effectiveness of the measures taken will determine the severity of the impact of such an attack.

5.10.2 Checklist for Logging and Monitoring

The following list can be used to check the configuration of your PV system after initial commissioning. The test should also be repeated regularly to ensure that your system is protected against cybercrime throughout its entire life cycle.

- ☐ For home systems, check whether your router offers any kind of logging and monitoring. If so, activate it and check the logs at least once a month.
- ☐ Implement an intrusion detection system (IDS).
- ☐ Regularly test the monitoring tools and measures, including an IDS.
- ☐ Implement a process to define responsibilities and regularly review the effectiveness of your monitoring measures

5.11 Device and User Secrets

5.11.1 Device and User Secrets

To protect your assets from unauthorized access, it is important to secure your device and user secrets such as passwords or the WiFi PSK (Pre Shared Key). This includes not only protecting these secrets from unauthorized access, but also using strong passwords that make it difficult for an attacker to guess the password or determine it by means of a brute force attack, i.e. trying out all possible passwords.

The recommendations must be followed in all installations.

5.11.2 Checklist for Device and User Secrets

The following list can be used to check the configuration of your PV system after initial commissioning. The test should also be repeated regularly to ensure that your system is protected against cybercrime throughout its entire life cycle.

- ☐ Do not write secrets on paper.

- ☐ If passwords are printed on paper, keep the paper in a safe place (e.g. a safe).
- ☐ Use a password manager (special software for storing passwords in an encrypted database or file).
- ☐ Never pass on passwords to third parties or other systems.
- ☐ Change all default passwords to individual passwords.
- ☐ Do not use simple passwords (such as 1234).
- ☐ Create complex passwords consisting of at least 8 characters, letters, numbers and special characters.
- ☐ Use a passphrase to create your password.
- ☐ Do not use the same password for different accounts.
- ☐ Use a password manager to generate random passwords and store them securely.

5.12 Checklist for Further Measures

The following list can be used to check the configuration of your PV system after initial commissioning. The test should also be repeated regularly to ensure that your system is protected against cybercrime throughout its entire life cycle.

Segmentation:

- ☐ Ensure that the firewall and the proxy server are configured correctly.
- ☐ Use physically (or at least logically) separate grid segments for the grid connections of the PV system (e.g. separation of home or office grid).

Network settings and logs:

- ☐ Do not use any port forwarding or the like between WAN and LAN.
- ☐ Deactivate all protocols in all devices that are not required for communication within your system.
  - Deactivate Modbus if possible (this protocol does not support encryption or authentication).
  - Speedwire: If all devices support Speedwire encrypted communication, make sure that you activate the encrypted version in the system manager.
  - WiFi access point: Deactivate the WiFi access point after the initial setup.
- ☐ Do not use any unsecure external FTP servers. Instead, use SFTP (Secure FTP) to transfer data with encryption.
- ☐ Use WPA or WPA2 encryption for Wi-Fi connections. Older encryption methods (e.g. WEP) are compromised.

Login data:

- ☐ Change all default passwords.
- ☐ Keep your device-specific login information private.
  - RID (Registration ID - for registering the device in Sunny Portal)
  - PIC (Product Identification Code - for registering the device in Sunny Portal)
  - Product key (user-generated - for resetting the password)
  - Device key (for resetting the password of the admin account)
  - WiFi PSK (for the WiFi access point of the device)
- ☐ Change WiFi PSK. If supported by the device, change the PSK after the initial setup.
- ☐ Ensure that you assign the required access rights to the right people.

Miscellaneous:

- ☐ Activate automatic updates.
- ☐ Deactivate service access. Only activate service access if you require support from SMA Service and the service requires access to your system.
- ☐ Protect your device from physical access to prevent malicious tampering.
- ☐ Check log files regularly for suspicious activity.

- ☐ Do not connect any unknown storage devices (USB sticks, SD or CF memory cards) to your devices. Check such storage devices for malware before you use them.
- ☐ Regularly check whether there are any unknown devices in your network.
- ☐ Create regular backups.
- ☐ Always keep your remote access equipment up to date. Install security patches regularly and use an up-to-date virus scanner.
- ☐ Ensure that you log out of your PV system after each access. Active Internet sessions could be taken over by a man-in-the-middle attack.
- ☐ Ensure that all employees receive cyber security training.

Shutdown:

- ☐ Reset your device to the factory settings to delete all personal data and access data (e.g. your Wi-Fi password).
- ☐ Remove your device from Sunny Portal.

5.13 Important Information

If you suspect or discover that your system has been attacked, have the damage assessed by a specialist to prevent further consequences.

Should you suspect or detect that an attack on SMA products has occurred, please inform us promptly. Please use the following e-mail address: Information-Security@sma.de

ENERGY
THAT
CHANGES

SMA

www.SMA-Solar.com