Technical Information

PUBLIC CYBER SECURITY

Guidelines for a Secure PV System Communication

Table of Contents

1 Information on this Document

1.1 Validity

This document applies to all products that are interconnected within a network for PV system communication and can be connected to the Internet directly or indirectly via communication media.

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 product.

1.2 Target Group

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

1.3 Additional Information

For further information, visit the websites of safety organizations such as:

Safety organization	Document	Hyperlink
German Federal Office for Information Technology (BSI, Bundesamt für Sicherheit in der Informationstechnik)	Sichere Passwörter in Embedded Devices	https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_069.pdf?__blob=publicationFile
German Federal Office for Information Technology (BSI, Bundesamt für Sicherheit in der Informationstechnik)	Industrial Control System Security: Top 10 Threats and Countermeasures 2016	https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005E.pdf?__blob=publicationFile&v=3
NIST (USA, National Institute of Standards and Technology)	10 Basic Cybersecurity Measures	https://ics-cert.us-cert.gov/sites/default/files/documents/10_Basic_Cybersecurity_Measures-Water-ISAC_June2015_S508C.pdf

Links to additional information can be found at www.SMA-Solar.com:

Document title	Document type
"Webconnect Systems in Sunny Portal"	User Manual
"SMA SPEEDWIRE FIELDBUS"	Technical Information
"System Monitoring - SMA Safety and Password Concept for Password-protected PV Plants with Bluetooth® Wireless Technology"	Technical Description
"SMA Modbus® Interface"	Technical Information
"SunSpec® Modbus® Interface"	Technical Information

2 Introduction

Most operating activities such as monitoring and control of PV systems can be done locally by the PV system operator or service personnel without the need for data communication via public Internet infrastructure. These operating activities, including data communication between PV system operator/service personnel and PV inverter, data logger or additional equipment, can be accessed by using local displays, keypads or using local access of the webserver of a device in the LAN of the PV system or of the building.

In other use cases of PV systems, the PV systems are 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 devices (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 (special communication interfaces, separate wide area networks and more).

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.

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
- Knowledge of the communication requirements and features of all devices
- Knowledge of possible vulnerabilities of all devices
- Knowledge of all accounts that access the systems
- 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)
- Examining and, if necessary, improving the security measures with regard to being up to date and suitable

If these requirements have been met, it can be assumed that the PV system is used in a system which is "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.

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.

3 Risks

Systems connected to the Internet that are not specifically secured can be used to gain access to the customer's network (behind the Internet router). This can result in attacks on almost all devices within the network. Once the potential attackers have been given the opportunity to gain access to the network, the following risks occur:

- Spying on user names, passwords and other confidential data
- Accessing the devices connected to the network to install Botnet agents or to carry out cross-site scripting attacks
- Accessing the devices connected to the network to manipulate device behavior (e.g. by using man-in-the-middle or replay attacks)
- Accessing the devices connected to the network to manipulate transmitted data which are to trigger false reactions of superordinate systems
- Accessing the devices connected to the network to evaluate user behavior (e.g. for planning burglaries and thefts)
- Accessing the devices connected to the network to evaluate user behavior for the use of personalized advertising

The consequences can be:

- Financial losses due to:
  - Missing yields from energy generation
  - Incorrectly used grid feed-in or consumption tariffs
  - Damage to devices
- Identity theft
- Negative impacts on the stability of the utility grid (provided that the amount and size of compromised systems is large enough)
  - Loss of permission to operate connected to the utility grid
  - Legal consequences

4 Countermeasures

In order to meet the basic requirements of a secure system, SMA Solar Technology AG recommends a minimum of security measures. In combination with the security features provided by the SMA products, a secure operation of the PV system can be achieved. Observe the following rules for the secure operation of a PV system:

- Ensure that the firewall and proxy server are configured correctly.
- Ensure that you use physically separated network segments for the network connections of the PV system (separation of home or office network).
- Ensure that unauthorized persons cannot physically or virtually access SMA products and other devices connected to the network.
  - Prevent the physical manipulation of the system from the local network.
  - Avoid using spyware devices in the local network (e.g. foreign/unknown WLAN access points).
  - Prevent that the registration ID (RID) for the registration in Sunny Portal, which is usually attached to the product, is illegally collected. The registration ID is a device-specific, randomly assigned ID, which proves the physical access to the product.
  - Store the knowledge of system details (device types, passwords, RID) according to the principle: "As much as necessary, as little as possible." Keep this information as secret as possible.
  - Keep all passwords, Webconnect RID and the SMA Grid Guard code secret. The Grid Guard code identifies authorized installers when they are changing grid-relevant system parameters.
  - Regularly check the system log files of all devices which are relevant for IT security.
  - Do not connect unknown memory devices (USB flash drives, SD or CF memory cards) to your devices. Check such media for malware prior to using them.
  - Do not use any unknown or unsecure devices in your network.
  - Create regular backups of the systems.
  - Create redundant solutions and procedures for relevant systems. A simple solution: each critical system element should have a pre-configured spare part as a backup.
- Make sure not to use any port forwarding or the like between WAN and LAN.

  - Connect via VPN or Webconnect for external access. Each remote connection (maintenance, support, direct marketing, grid management services) shall be made exclusively via such secure methods of communication.
- Ensure that all unused IP ports in the firewall are blocked. Unused IP ports in other systems should be deactivated. Each open IP port is a potential risk for system intrusion.
- Do not use unsecured external FTP servers, but make sure that SFTP servers (secure FTP servers) are used. FTP servers transmit files unencrypted. If using SFTP servers, the files are encrypted while they are transmitted.
- Make sure that you use secure external mail servers for e-mails. Nowadays, most e-mail providers only permit TLS (or similar) access anyway.
- Ensure that products not originating from SMA Solar Technology AG are secure. Unsecure products can allow attackers unwanted access to the local network.
  - Always keep antivirus/anti-malware software and router and firewall rules up-to-date.
  - Only allow absolutely necessary exceptions to security mechanisms.
  - Follow the operating system recommendations for security updates.
- Ensure that the assigned access rights to the PV system have been clearly organized (which user gets which access rights).
  - In most cases, the user group "User" is sufficient for monitoring the PV system. The user group "Installer" should only be used during commissioning and parameterization of the product.
- Ensure that all default passwords are changed to personal passwords upon commissioning at the latest. Default passwords are commonly known.
- Ensure that you only use passwords according to the common guidelines.
  - The password should consist of at least eight characters, including letters, numerals and common special characters (!=?#+-:;*).
  - The password should be difficult to guess (e.g. "1?deFa-7").
- Ensure that each password is only used for a single PV system.
- 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 you use at least the WPA encryption or, better still, the WPA2 encryption for the WLAN access of all devices.
  - Do not use older encryption methods such as WEP.
  - Never forgo encryption methods completely.
- Ensure that all employees have been sensitized concerning cybersecurity issues.

  - Ensure that employees receive cybersecurity training.
- Should you suspect or detect that an attack on your system has occurred, have a specialist assess the damage and prevent further impact.
- Should you suspect or detect that an attack on SMA products has occurred, please inform us promptly SMA Solar Technology AG. Please use the following e-mail address for this purpose:
  - Information-Security@SMA-Solar.com