Information technique

CYBERSÉCURITÉ PUBLIQUE

Directives pour une communication sûre avec les installations photovoltaïques

Table des matières

1 Remarques relatives à ce document

1.1 Champ d'application

Le présent document s'applique à tous les produits qui sont connectés les uns aux autres au sein du réseau de communication d'une installation photovoltaïque et qui peuvent être connectés directement ou indirectement à Internet par le biais de moyens de communication.

Ce document complète les documents fournis avec les produits et ne remplace pas les normes ou directives applicables sur site. Lisez et suivez toute la documentation fournie avec le produit.

1.2 Groupe cible

Les informations dans ce document sont destinées aux installateurs, aux exploitants et aux concepteurs d'installations photovoltaïques avec des onduleurs SMA.

1.3 Informations complémentaires

Pour de plus amples informations, consultez les sites Internet d'organismes de sécurité comme :

Organisme de sécurité	Document	Lien
BSI (Bundesamt für Sicherheit in der Informationstechnik - Office fédéral allemand de la sécurité des technologies de l'information)	Sichere Passwörter in Embedded Devices (Mots de passe sûrs pour les appareils embarqués)	https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_069.pdf?__blob=publicationFile
BSI (Bundesamt für Sicherheit in der Informationstechnik - Office fédéral allemand de la sécurité des technologies de l'information)	Industrial Control System Security: Top 10 Bedrohungen und Gegenmaßnahmen v1.2 (Sécurité des systèmes de commande industriels : les 10 menaces principales et leurs contre-mesures, v1.2)	https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005.pdf?__blob=publicationFile&v=4
NIST (National Institute of Standards and Technology - Institut national américain des normes et de la technologie)	10 Basic Cybersecurity Measures (10 mesures de cybersécurité basiques)	https://ics-cert.us-cert.gov/sites/default/files/documents/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_S508C.pdf

Pour obtenir des informations complémentaires, consultez le site www.SMA-Solar.com :

Titre du document	Type de document
« Installations Webconnect sur le Sunny Portal »	Manuel d'utilisation
« BUS DE TERRAIN SMA SPEEDWIRE »	Information technique
« Surveillance de l'installation - Concept de sécurité et de mot de passe SMA pour les installations photovoltaïques protégées par mot de passe avec Bluetooth® Wireless Technology »	Description technique

Titre du document	Type de document
« Interface SMA Modbus® »	Information technique
« Interface SunSpec® Modbus® »	Information technique

2 Introduction

La plupart des activités opérationnelles, telles que la surveillance et la commande des installations photovoltaïques, peuvent être réalisées en local par l'exploitant de l'installation ou les techniciens de service, sans qu'une communication de données ne soit nécessaire par le biais de l'infrastructure Web publique. Ces activités opérationnelles, telles que la communication de données entre l'exploitant de l'installation, les techniciens de service et l'onduleur photovoltaïque, l'enregistreur de données ou des équipements supplémentaires, s'effectuent en utilisant des écrans et des claviers locaux ou l'accès local au serveur Web d'un appareil du réseau local (LAN) de l'installation photovoltaïque ou de la maison.

Dans d'autres cas d'application des installations photovoltaïques, elles font également partie du système de communication global, basé sur une infrastructure Web.

La communication de données via Internet est une approche moderne, judicieuse en termes de rentabilité et pratique pour les clients, car elle donne par exemple facilement accès aux technologies modernes suivantes :

- plateformes basées sur le cloud (par ex. Sunny Portal)
- smartphones ou autres appareils mobiles (applications iOS ou Android)
- systèmes SCADA reliés à distance
- interfaces fournisseurs pour les systèmes de gestion du réseau

Il est également possible d'utiliser des interfaces de communication choisies et sécurisées. Ces solutions ne sont toutefois plus à la pointe de la modernité et leur utilisation est coûteuse (interfaces de communication spéciales, réseaux étendus séparés etc.).

De par l'utilisation d'une infrastructure Web, les systèmes connectés à Internet se retrouvent dans une zone à la sécurité fondamentalement incertaine. Les pirates sont sans cesse à la recherche de systèmes vulnérables. Leurs objectifs sont souvent de nature criminelle ou terroriste ou visent à nuire au bon fonctionnement des entreprises. Aucun système de communication de données ne devrait être connecté à Internet sans que des mesures de protection des installations photovoltaïques et autres équipements n'aient été prévues pour éviter ce genre d'attaques.

Pour éviter efficacement que des personnes non autorisées (par ex. des criminels ou des services de renseignement) n'accèdent aux installations photovoltaïques, le réseau local doit être maintenu aussi organisé et hermétique que possible. En cas de connexion d'une installation photovoltaïque ou d'un système comparable à Internet, l'exploitant de l'installation ou l'administrateur réseau doit :

- connaître tous les appareils actifs au sein du réseau local
- connaître les exigences de communication et les fonctions de chaque appareil
- connaître les faiblesses potentielles de chaque appareil
- connaître tous les comptes accédant aux systèmes
- connaître les possibilités pour limiter l'accès au réseau local et aux appareils (par ex. par le biais de mots de passe sécurisés)
- installer et configurer toutes les mesures de protection nécessaire en termes de cybersécurité (routeur, pare-feu, serveur proxy)
- vérifier l'actualité et l'adéquation des mesures de protection et les améliorer si nécessaire.

Lorsque ces conditions sont réunies, on peut partir du principe qu'aucun accès direct à l'installation photovoltaïque depuis l'extérieur n'est possible immédiatement.

La plupart des systèmes de communication industriels utilisent des protocoles de communication par bus de terrain en grande partie standardisés. Par conséquent, il est indispensable d'adopter une stratégie BTF, car la majorité des systèmes avec bus de terrain ne possèdent pas de mécanismes de sécurité intégrés et doivent être protégés par des mesures supplémentaires. Cela vaut également pour les deux protocoles de communication par bus de terrain SMA Data2+ et Modbus TCP, qui sont utilisés dans les solutions de communication de SMA Solar Technology AG. Avec le protocole de communication Data2+, une protection par mot de passe assure la sécurité des produits SMA. Le protocole de communication WAN Webconnect fait figure d'exception car il permet une connexion sécurisée avec un chiffrement de bout en bout. Webconnect n'est cependant pas utilisé dans les réseaux locaux. Il est conçu pour assurer une communication sûre entre les onduleurs photovoltaïques ou les enregistreurs de données et le Sunny Portal ou les solutions mobiles.

i Risque pour la sécurité en raison de Modbus TCP

Modbus TCP, interface client publique, équipe la plupart des produits SMA. Modbus TCP ne peut être transférée via Internet de manière sûre sans prendre certaines mesures. Modbus TCP ne requiert pas d'authentification, ce qui peut représenter un risque pour la sécurité au sein d'une installation photovoltaïque. De ce fait, Modbus TCP est désactivé par défaut dans les produits SMA. Modbus TCP doit être activé si nécessaire dans le groupe d'utilisateurs « Installateur ». L'activation ne doit toutefois pas être effectuée à la légère, elle doit toujours être accompagnée de mesures supplémentaires visant à sécuriser le système dans son ensemble.

3 Risques

Les systèmes connectés à Internet mais qui ne font pas l'objet d'une protection spéciale peuvent être utilisés pour pénétrer dans le réseau du client (derrière le routeur Internet). Par ce biais, presque tous les appareils du réseau peuvent être la cible d'attaques. Une fois que les pirates ont réussi à accéder au réseau, il faut compter avec les risques suivants :

- espionnage des noms d'utilisateurs, des mots de passe et d'autres données confidentielles
- accès aux appareils connectés au réseau afin d'installer des botnets ou de mener des attaques de type cross-site scripting
- accès aux appareils connectés au réseau afin de manipuler leur comportement (par ex. par le biais d'attaques de l'homme du milieu ou de rejeu)
- accès aux appareils connectés au réseau afin de manipuler les données transmises et ainsi déclencher des réactions erronées des systèmes maîtres
- accès aux appareils connectés au réseau afin d'évaluer le comportement des utilisateurs (par ex. pour planifier des cambriolages et des vols)
- accès aux appareils connectés au réseau afin d'évaluer le comportement des utilisateurs pour proposer des publicités personnalisées

Conséquences potentielles :

- Pertes financières dues :
  - à une production d'énergie minime
  - à des tarifs d'injection réseau et de consommation utilisés de manière erronée
  - à un endommagement des appareils
- Usurpation d'identité
- Effets négatifs sur la stabilité du réseau électrique public (dans la mesure où le nombre et la taille des systèmes touchés sont suffisants pour cela)
  - Retrait de l'autorisation de connexion au réseau électrique public
  - Conséquences juridiques

4 Contre-mesures

Afin de satisfaire aux exigences fondamentales d'un système sécurisé, SMA Solar Technology AG recommande de prendre un certain nombre de précautions. Celles-ci, associées aux fonctions de sécurité des produits SMA, permettent un fonctionnement sûr de l'installation photovoltaïque. Observez les régulations suivantes afin d'assurer le fonctionnement sûr de l'installation photovoltaïque :

- Assurez-vous que le pare-feu et le serveur proxy ont été configurés de manière sûre.
- Assurez-vous d'utiliser des segments de réseau physiquement séparés pour les connexions réseau de l'installation photovoltaïque (séparation du réseau du domicile ou du bureau).
- Assurez-vous qu'aucune personne non autorisée ne peut avoir accès physique ou virtuel aux produits SMA et aux autres appareils connectés au réseau.
  - Empêchez toute manipulation physique du système depuis le réseau local.
  - Empêchez l'utilisation d'appareils d'espionnage sur le réseau local (par ex. de points d'accès au réseau local sans fil tiers/inconnus).
  - Empêchez l'espionnage du code d'enregistrement (RID) pour le Sunny Portal (généralement indiqué sur le produit). Le code d'enregistrement est un code aléatoire spécifique à chaque appareil qui atteste de l'accès physique au produit.
  - Conservez les informations sur les détails du système (types des appareils, mots de passe, RID) selon le principe « autant que nécessaire, aussi peu que possible ». Conservez ces informations aussi confidentielles que possible.
  - Conservez tous les mots de passe, RID Webconnect et le code Grid Guard de SMA confidentiels. Le code Grid Guard identifie les installateurs autorisés lorsque ces derniers modifient des paramètres système influant sur le réseau.
  - Vérifiez régulièrement les fichiers journaux système de tous les appareils importants du point de vue de la sécurité.
  - Ne connectez aucun support de stockage inconnu (clés USB, cartes SD ou CF) à vos appareils. Avant de les utiliser, vérifiez que ces supports ne soient pas infectés par des programmes malveillants.
  - N'utilisez aucun appareil inconnu et non sécurisé dans votre réseau.
  - Faites des sauvegardes régulières des systèmes.
  - Élaborez des solutions et procédés redondants pour les systèmes pour lesquels cela s'applique. Une solution simple : une pièce de rechange pré-configurée doit être disponible pour chaque composant essentiel du système.
- Assurez-vous de n'utiliser aucune redirection de port ou élément similaire entre le WAN et le réseau local.

  - Pour accéder au système depuis l'extérieur, utilisez une connexion VPN ou Webconnect. Toute connexion à distance (maintenance, assistance, vente directe, systèmes de gestion du réseau) doit se faire exclusivement par le biais de ces méthodes de communication sécurisées.
- Assurez-vous que tous les ports IP non utilisés sont bloqués dans le pare-feu. Les ports IP non utilisés d'autres systèmes doivent être désactivés. Tout port IP ouvert présente un risque d'intrusion dans le système.
- Assurez-vous d'utiliser des serveurs SFTP (serveurs FTP sécurisés) et non des serveurs FTP externes non sécurisés. Les serveurs FTP transmettent les fichiers sans chiffrement. Avec les serveurs SFTP, les fichiers sont chiffrés pendant la transmission.
- Assurez-vous d'utiliser des serveurs de messagerie externes sécurisés pour la communication par e-mail. La plupart des fournisseurs de services de messagerie actuels n'acceptent plus que la connexion TLS (ou similaire).
- Assurez-vous que les produits ne provenant pas de SMA Solar Technology AG sont sûrs. Des produits non sûrs peuvent permettre à des pirates d'accéder au réseau local.
  - Actualisez en permanence les logiciels antivirus et de protection contre les programmes malveillants ainsi que les règles pour le routeur et le pare-feu.
  - N'autorisez que les exceptions aux mécanismes de protection qui sont absolument nécessaires.
  - Respectez les recommandations de mises à jour de sécurité du système d'exploitation.
- Assurez-vous que les droits d'accès à l'installation photovoltaïque octroyés soient organisés clairement (quels droits d'accès pour quel utilisateur).
  - Dans la plupart des cas, le groupe d'utilisateurs « Utilisateur » est suffisant pour la surveillance de l'installation photovoltaïque. Le groupe d'utilisateurs « Installateur » ne doit être utilisé que pour la mise en service et le paramétrage du produit.
- Assurez-vous que les mots de passe définis en usine soient remplacés par des mots de passe personnalisés au plus tard lors de la mise en service. Les mots de passe définis en usine sont bien connus.
- Assurez-vous de n'utiliser que des mots de passe sûrs, conformes aux directives usuelles.
  - Le mot de passe doit comporter au minimum huit caractères, dont des lettres, des chiffres et des caractères spéciaux usuels (!=?#+-:;*).
  - Le mot de passe ne doit pas être facile à deviner (par ex. 1?deFa-7).
- Assurez-vous que chaque mot de passe ne soit utilisé que pour une seule installation photovoltaïque.
- Assurez-vous de vous déconnecter après chaque accès à l'installation photovoltaïque. Des sessions Internet actives peuvent être exploitées, par ex. pour des attaques de l'homme du milieu.
- Assurez-vous que le chiffrement WPA ou, mieux encore, le chiffrement WPA2 soit utilisé pour l'accès au réseau local sans fil de chaque appareil.
  - N'utilisez pas de méthodes de chiffrement plus anciennes, comme par exemple WEP.

  - Recourez impérativement à une méthode de chiffrement.
- Assurez-vous que tous les collaborateurs aient été sensibilisés à l'importance de la cybersécurité.
  - Assurez la formation des collaborateurs aux thèmes relevant de la cybersécurité.
- Si vous suspectez ou constatez une attaque sur votre système, faites appel à un spécialiste pour évaluer les dommages et prévenir d'autres répercussions.
- Si vous suspectez ou constatez une attaque sur un produit SMA, informez-en immédiatement SMA Solar Technology AG. Utilisez pour cela l'adresse e-mail suivante :
  - Information-Security@SMA-Solar.com