Cybersecurity of SolBrid inverters

Whitepaper — 11 June 2025

Introduction

The operation of photovoltaic systems and battery storage systems is inconceivable without inverters. They are the central components that regulate energy flows and monitor diverse normative requirements. They are being used in increasing numbers in a wide range of sizes in private households, commercial and industrial operations or large PV power plants and are therefore a key component of the energy transition.

Modern inverters are networked and usually have an internet connection. Not only as part of the energy infrastructure, but also as devices that aggregate sensitive data in private households or businesses, they are potentially worthwhile targets for hackers and other actors.

Individual inverters may not have a relevant impact on the power grid, but if a large number of devices are manipulated in a concerted manner, it is theoretically possible to cause large-scale grid disruptions. The recent grid failures in Spain, Portugal and southern France have shown how vulnerable the grid infrastructure can be.

Protection against unauthorised access and data loss is therefore very important. Kontron is aware of this responsibility towards its customers, including its responsibility as a manufacturer of devices in the field of security-relevant infrastructure. SolBrid inverters, the Kontron sunCloud and the Kontron SOL app naturally comply with European legislation and its strict regulations on data and consumer

kontron solar

protection. Our inverters, data infrastructure and software have a robust security architecture and offer a very high level of cyber security.

In contrast to many comparable products on the market, SolBrid inverters can also be operated permanently without an internet connection, and software updates can also be installed offline without any problems.

Data interfaces

SolBrid inverters have many interfaces, each of which is optimised for very specific tasks and can therefore be consistently protected.

RS485 interfaces

Communication with the other devices in the local system, such as batteries, energy meters, the grid disconnector or control boxes (VNB telecontrol technology), takes place via local point-to-point connections on individual RS485 lines that cannot be accessed from outside.

LAN connection (RJ45) and WiFi

The existing LAN connection (RJ45) and the integrated WiFi functionality are used both for the SolBrid inverter's Internet connection and for local connections. A local access point mode is also available, which does not allow an external connection. It can be used for configuration during commissioning or for offline installation of firmware updates.

kontron
solar

The SolBrid Inverter's Cybersecurity

Whitepaper — 11 June 2025

Communication and cyber security

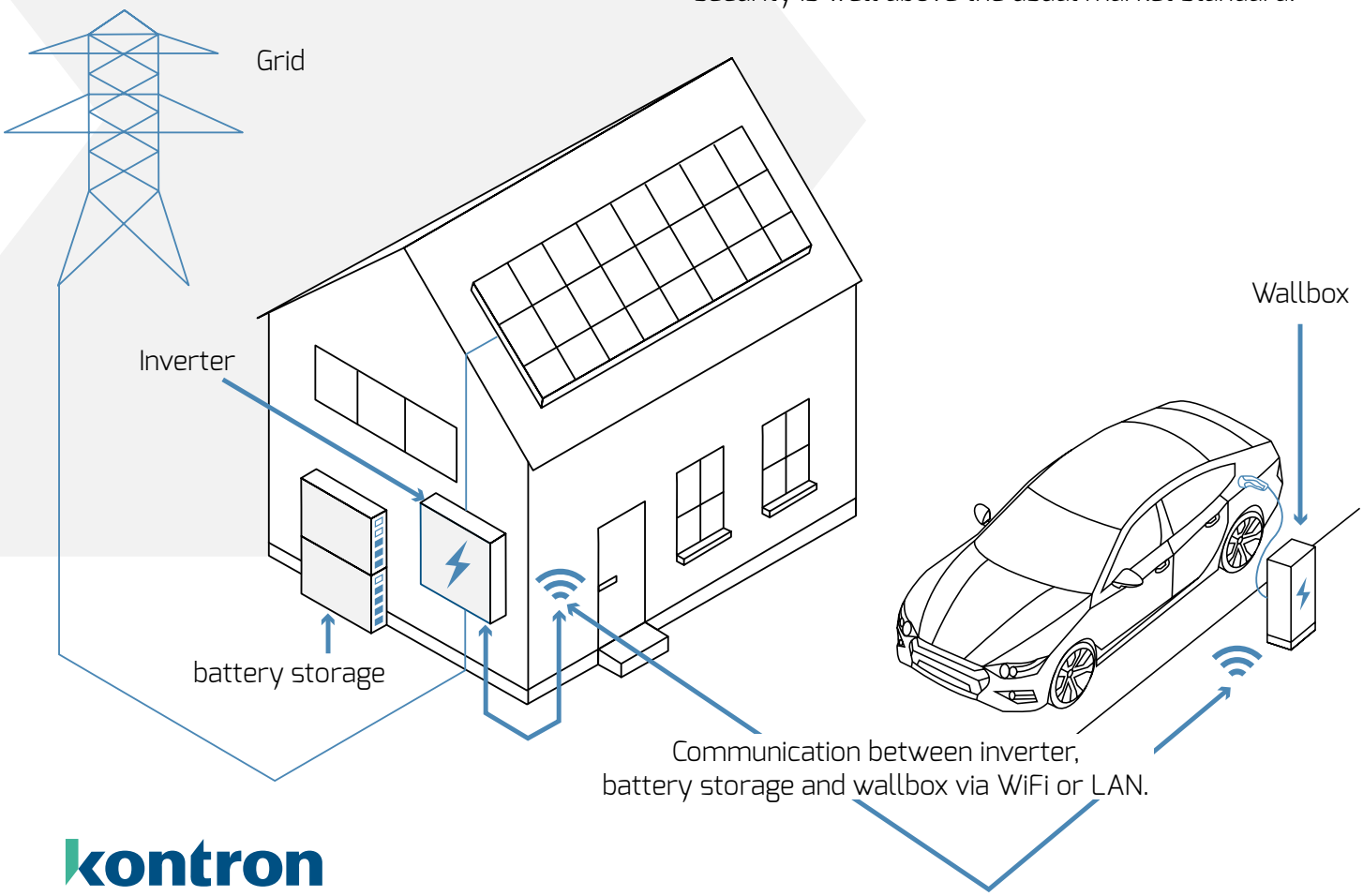
One feature of the security architecture of SolBrid inverters distinguishes them fundamentally from most comparable products on the market: any external communication can only take place after the system operator has given their consent. Alternatively, SolBrid inverters can even be operated completely offline, i.e. without any internet connection, reliably and efficiently. In either case, SolBrid users can be sure that no unauthorised data is read or devices are manipulated in any other way.

A SolBrid inverter can send operating data to the user monitoring portal (Kontron sunCloud) via an active Internet connection and after authorisation by the user. The data is only transmitted in one direction, meaning that the device cannot be manipulated via this connection. The SunCloud servers are hosted exclusively in European data centres.

Firmware updates are not carried out automatically but must first be confirmed by the user. The transmission of the signed software packages is encrypted. Compromising the cyber security of the SolBrid can therefore be ruled out in this way.

In addition to encrypted communication with verified certificates, the SolBrid uses the latest cryptographic methods for multiple protection in all security-relevant processes. SolBrid inverters are equipped with a security chip for this purpose, which is used for all essential security functions.

In addition, installers only have access to protected settings in the inverter once they have been registered and authorised. When accessing the inverter, they must also identify themselves with an individual security code. Here too, the level of security is well above the usual market standard.



kontron solar

The SolBrid Inverter's Cybersecurity

Whitepaper — 11 June 2025

Summary

Due to the security concept of the SolBrid inverter, cyber attacks are theoretically only possible via the internet connection. However, this connection is protected against manipulation in several ways. Thanks to strong encryption and the consistent use and verification of certificates, only a connection from or to authorised communication partners can be established. Incoming connections and thus direct attacks on the inverter are impossible.

Data is only transferred after authorisation by the system operator and only to Kontron's own SunCloud. Manipulation or control of the inverter from outside can therefore be ruled out. This level of cyber security is currently confirmed by an accredited body in accordance with EN 18031.

Irrespective of this, SolBrid inverters can be completely protected against all cyber threats by operating them offline.