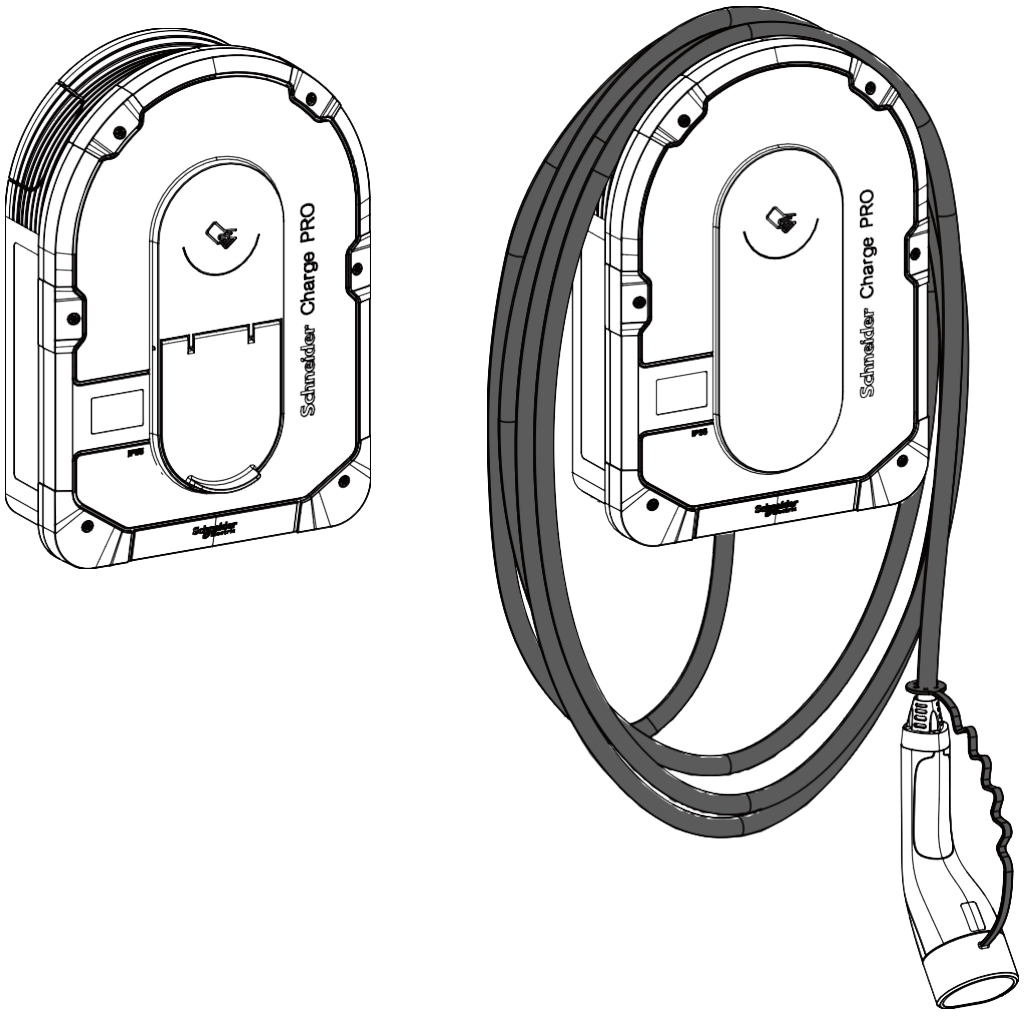
Schneider Charge Pro

Cybersecurity Guide

BRU5883000-02_EN

04/2025



www.se.com

Legal Information

The information provided in this document contains general descriptions, technical characteristics and/or recommendations related to products/solutions.

This document is not intended as a substitute for a detailed study or operational and site-specific development or schematic plan. It is not to be used for determining suitability or reliability of the products/solutions for specific user applications. It is the duty of any such user to perform or have any professional expert of its choice (integrator, specifier or the like) perform the appropriate and comprehensive risk analysis, evaluation and testing of the products/solutions with respect to the relevant specific application or use thereof.

The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this document are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owner.

Schneider Electric does not grant any right or license for commercial use of the document or its content, except for a non-exclusive and personal license to consult it on an «as is» basis.

Schneider Electric reserves the right to make changes or updates with respect to or in the content of this document or the format thereof, at any time without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this document, as well as any non-intended use or misuse of the content thereof.

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

Table of Content

Safety Information

Important Information

Read these instructions carefully and look at the equipment to become familiar with the device before trying to install, operate, service, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result** in death or serious injury.

⚠ WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result** in death or serious injury.

⚠ CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result** in minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

Please Note

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation and has received safety training to recognize and avoid the hazards involved.

Safety Instructions

⚠ DANGER

HAZARD OF ELECTRIC SHOCK
- Do not open the product.
- Product to be serviced by qualified personnel only.

Failure to follow these instructions will result in death or serious injury.

NOTE: All instructions applicable to the enclosed product and all safety precautions must be observed.

For more information, you can download the app of the Customer Care Center by using the following QR code:

About the Book

Purpose of this Document

The Schneider Charge Pro Charging Station supports to be connected to Ethernet/ WIFI networks, however this networking capability is not designed to withstand the direct exposure to the public Internet.

The Schneider Charge Pro Charging Station is intended to be used in a trusted network environment, for instance, behind firewalls, and/or within the boundaries of an isolated OT network (separated from the IT network).

Validity Note

This document applies to Schneider Charge Pro charging stations.

Terminology

Acronym	Designation
OCPP	Open Charge Point Protocol (communication protocol used between the charging stations and a central system)

Cybersecurity Information

Important Information

⚠ WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Change default passwords at first step to help prevent unauthorized access to device settings, controls, and information.
- Disable unused ports/services and default accounts to help minimize pathways for malicious attackers.
- Place networked devices behind multiple layers of cyber defenses (such as firewalls, network segmentation, and network intrusion detection and protection).
- Use cybersecurity best practices (for example, least privilege, separation of duties) to help prevent unauthorized exposure, loss, modification of data and logs, or interruption of services.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Cybersecurity in Schneider Electric

Cybersecurity is integral to Schneider Electric's business strategy, and it follows a cybersecurity posture that covers many aspects:

- Securing internal activities
- Providing elevated levels of protection of strategic IT systems and assets
- Leading the digital transformation within a cybersecure framework
- Designing and developing new products and solutions with end-to-end cybersecurity measures and protection

Cybersecurity Policies

To support the development and maintenance of products, Schneider Electric follows a Secure Development Lifecycle (SDL) compliant with the IEC 62443-4-1 Security Standard for Industrial Automation and Control systems.

It consists in implementing a process, relying on security best practices and dedicated tools, that covers:

- Security training for teams involved in the product design, development, and testing.
- Threat modeling analysis and security design reviews
- Static code analysis and code security reviews
- Penetration testing and periodic vulnerability testing
- Stringent vulnerability management process

Cybersecurity Resources

Cybersecurity Solutions

For recommendations and guidance on how to help secure the environment and infrastructure in which Schneider Charge Pro charging station is deployed, Schneider Electric publishes guidelines, white papers, and best practices that can be consulted in the Cybersecurity Solutions page of Schneider Electric global website.

Cybersecurity Support Portal

In addition, other resources can be found in Schneider Electric Cybersecurity Support Portal, including:

- Schneider Electric vulnerability management policy
- Security notifications about vulnerabilities in products and systems

The Schneider Electric's vulnerability management policy addresses cybersecurity vulnerabilities affecting Schneider Electric products in order to support the security and safety of our customers.

Schneider Electric works cooperatively with researchers, Cyber Emergency Response Team (CERT), and asset owners to help ensure that accurate information is provided in a timely fashion to adequately protect customer installations.

Schneider Electric's Corporate Product CERT (CPCERT) is responsible for managing and alerting on vulnerabilities and mitigations affecting products.

The Cybersecurity Support Portal also provides interfaces to report cybersecurity vulnerabilities and to register for the security notification updates mailing list to stay informed via email on newly released or updated Security Notifications.

Security Features

Security features have been built into Schneider Charge Pro charging station to ensure that product operates according to its intended purpose.

These features provide security capabilities which are expected to protect the product from potential security threats that could allow disrupting the product operation (availability), modifying the product configuration (integrity) or disclosing information (confidentiality).

The key features are:

- Firmware authenticity verification at product startup (secure boot)
- Firmware update mechanism with firmware signature verification (using asymmetric cryptography)
- TLS 1.2 for securing and authenticating OCPP communications with a remote charging station management system (CSMS)
- Common Criteria EAL6+ certified security chip for storing the product private key and certificate.
- Deactivation of internal debug and test interfaces

These security capability features are aimed at mitigating the threats related to the usage of Schneider Charge Pro charging stations in their intended environments.

However, the effectiveness of these capabilities depends on the adoption and application of the recommendations provided in this guide to cover the commissioning, operation and maintenance of Schneider Charge Pro charging stations, as well as Recommended Cybersecurity Best Practices.

Supported Protocols

The following protocols are supported by Schneider Charge Pro charging stations:

Protocol	Usage
OCPP (TLS 1.2) + HTTPS/FTPS	Communications with a remote Charging Station Management System **NOTE:** The OCPP protocol relies on additional HTTPS/FTPS communications for supporting OCPP reporting and maintenance operations (firmware update)
HTTPS (TLS 1.2)	Configuration through configuration tools
Modbus RTU	Communications with powermeters
DHCP	Networking IP address
DNS	Network name resolution
ISO/IEC 14443A/B ISO/IEC 15693	User authentication with RFID badges
SSDP	Simple Service Discovery Protocol

Potential Risks and Compensating Controls

Area	Issue	Risk	Compensating controls
Physical access	A charging station may be subject to tampering attempts.	If the charging station is accessed by a malicious user and its content is altered, malfunctions or possible damages may occur.	Periodically inspect the charging station for evidence of tampering attempts (scratches, tears, rips…). Install the charging station in a controlled environment or install security cameras.
Communication protocols	Modbus RTU, DHCP, DNS and SSDP are unsecure.	If a malicious user has gained access to the network, it is possible to intercept and eavesdrop communications.	For transmitting data over an internal network, consider physically or logically segmenting the network. For transmitting data over an external network, consider encapsulating communications in an encrypted tunnel, a TLS wrapper, or a similar solution.
Maintenance user account	Default credentials are often the source of unauthorized access by malicious users.	If the charging station has not been commissioned and the default PIN code is left unchanged, unauthorized access can occur.	Update the default PIN code using the commissioning app. Also consider renewing the PIN code on a regular basis.
	Same user account PIN codes are used in different charging stations.	If the PIN code is known by a malicious user, he could also access to all other charging stations configured with the same PIN code.	When installing several charging stations, configure different PIN codes in each charging station.
RFID badges	A badge may be forged or duplicated.	If a malicious user gets his hands on an RFID badge, he may be able to duplicate it and spoof the identity of a legitimate charging station user.	Do not leave RFID badges unattended. In case of suspicion of potential badge duplication or forgery, revoke and renew badges.

Security Recommendations

Recommendations for Commissioning

Default PIN Code

A default user account is provisioned in Schneider Charge Pro Charging Station for supporting the initial connection to the product with commission app during the installation.

The PIN code for this account is described in the user documentation. It is thus recommended to replace it with a new PIN code using the commissioning app.

The new PIN code should follow security best practices such as using a minimum of 8 digits and avoiding easily guessable patterns (blocks of similar digits or sequential increments of digits).

OCPP Communication Security

When configuring Schneider Charge Pro charging stations to connect to a remote Charging Station Management System with OCPP, it is recommended to always use WSS or HTTPS to secure the communication.

Communications relying on plain HTTP or plain Web Sockets are unsecure and subject to Man-In-The-Middle attacks.

SSDP security

SSDP should only be enabled when necessary.

For network security, follow these best practices when enabling SSDP:

Network Environment

- Restrict SSDP to internal network. Ensure the network is isolated from the internet to prevent public exposure.

Block External Access

- Disable UPnP in your router to block external discovery requests.
- Configure firewall rules to limit SSDP port access (default: UDP 1900) to internal traffic only.

Enhanced Security Recommendations

- For stricter isolation, use VLANs or network segmentation to separate devices with SSDP enabled.
- Regularly review router and network device configurations to ensure no port-forwarding rules expose SSDP to the internet.

Important: Failure to implement these measures may leave devices vulnerable to external attacks or unauthorized scans. Strict compliance is required.

Configuration of Services

Most Schneider Charge Pro charging station services are disabled by default to reduce the attack surface and exposure to a minimum.

Consequently, it is recommended to only enable the services that are strictly required. Unused services should be kept disabled.

Similarly, when a service is no longer needed or used, it is advised to disable it.

Security Recommendations for Maintenance

Firmware Update

Schneider Charge Pro charging station is embedding a digital firmware that may require the application of security patches to maintain an optimum level of security.

Consequently, it is recommended to periodically verify that the installed firmware is the latest one available.

Firmware updates and release notes can be downloaded from our website at https://www.se.com/ww/en/download/.

Audit Log

Schneider Charge Pro charging station maintains an audit log tracking security related events such as reboots, firmware updates, invalid login attempts.

It is recommended to consult the audit logs on a regular basis to detect potential unexpected or incorrect behaviors.

Security Recommendations for Decommissioning

Reset to Factory Settings

Schneider Charge Pro charging station can be configured with sensitive user information, which may include user account identifiers, passwords, RFID badge identifiers and charge operations history.

When disposing of the product, it is required to perform a reset to factory settings of the product to erase all sensitive or confidential user information and to make sure it will not be disclosed or reused.

Annex A

Open Source Software Used in Schneider Charge Pro

The **Schneider Charge Pro** (“the Product”) contains, among other things, Open Source Software (“OSS”) components, as specified below, developed by third parties and licensed under an Open Source Software license. These OSS components are protected by copyright and other forms of intellectual property. Your right to use the OSS is governed by the relevant applicable OSS license conditions.

Warranty regarding use of the Open Source Software:

The following disclaimer applies to the GPL and LGPL components in relation to the rights holders:

“These programs are distributed by the copyright holders in the hope that these will be useful, but WITHOUT ANY WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE”. See the GNU General Public License or the GNU Lesser General Public License for more details.

For the remaining open source components, the liability exclusions of the rights holders apply as per the respective license.

Schneider Electric SE and all of its subsidiaries (“Schneider Electric Group”) provide no warranty for the OSS contained in the Product, if such OSS is used in any manner other than intended by Schneider Electric Group. The licenses listed below define the warranty, if any, from the rights holders of the OSS. Schneider Electric Group specifically disclaims any warranty for defects caused by altering any OSS or the Product’s configuration. Any warranty claims against Schneider Electric Group in the event that the OSS contained in the Product infringes the intellectual property rights of a third party are excluded.

Technical support, if any, will only be provided for unmodified software.

Further use of OSS:

Your compliance with those license conditions will entitle you to use the OSS as foreseen in the relevant license. In the event of conflicts between other Schneider Electric license conditions applicable to the Product and the OSS license conditions, the OSS conditions shall prevail. The OSS is provided royalty-free (i.e. no fees are charged for exercising the licensed rights). The following OSS is contained in this Product:

OSS Name	License	Source Link	URL to License Text
busybox	GPL-2.0	https://www.busybox.net/downlo ads/ busybox-1.36.1.tar.bz2	https://www.busybox.net/license.html
cgic	AFL-2.1 or GPL-2.0+ (library, tools), GPL-2.0+ (tools)	https://github.com/FastCGI-Archives/ fcgi2/archive/refs/tags/ 2.4.1.tar.gz	https://spdx.org/licenses/preview/OML. html
dbus	AFL-2.1 or GPL-2.0+ (library, tools), GPL-2.0+ (tools)	https://dbus.freedesktop.org/rele ases/dbus/dbus-1.14.10.tar.xz	https://spdx.org/licenses/AFL-2.1.html GNU General Public License version 2
e2fsprogs	GPL-2.0 (as a whole) LGPL-2.0 (lib/ext2fs and lib/e2p libraries) BSD-style license (lib/uuid library) MIT-like with advertising clause (libss and libet)	https://cdn.kernel.org/pub/linux/k ernel/people/tytso/e2fsprogs/v1. 47.0/ e2fsprogs-1.47.0.tar.xz	https://www.gnu.org/licenses/old-licenses/gpl-2.0.en.html https://www.gnu.org/licenses/old-licenses/lgpl-2.0.en.html
glibc	GPL-2.0+ (programs) LGPL-2.1+(as a whole) BSD-3-Clause MIT (library)	https://github.com/bminor/ glibc/a rchive/2.39-74-g198632a05f6c7b9ab67d3331d 8caace9ceabb685/glibc-2.39-74-g198632a05f6c7b9ab67d3331d 8caace9ceabb685.tar.gz	https://www.gnu.org/licenses/old-licenses/gpl-2.0.en.html https://www.gnu.org/licenses/old-licenses/lgpl-2.1.en.html https://spdx.org/licenses/BSD-3-Clause.html
iptables	GPL-2.0	https://netfilter.org/projects/iptabl es/ files/iptables-1.8.10.tar.xz	https://www.gnu.org/licenses/old-licenses/gpl-2.0.en.html
kmod	LGPL-2.1+ (library)	https://cdn.kernel.org/pub/linux/u tils/ kernel/kmod/kmod-31.tar.xz	https://www.gnu.org/licenses/old-licenses/lgpl-2.1.en.html
libatomic	GPL-3.0 with gcc exception	https://github.com/gcc-mirror/gcc/ tree/releases/gcc-12.3.0/libatomic	https://www.gnu.org/licenses/gpl-3.0.html
libnl	MIT with exceptions BSD-2 BSD-3 Apache 2.0 ZLIB CC-zero	https://github.com/warmcat/ libw ebsockets/archive/refs/tags/ v4.3.3.tar.gz	https://opensource.org/licenses/MIT https://opensource.org/license/bsd-2-clause/ https://opensource.org/license/bsd-3-clause/ https://www.apache.org/licenses/ LICENSE-2.0.html https://www.apache.org/licenses/ LICENSE-2.0.html https://creativecommons.org/pu blicdomain/zero/1.0/
libwebsockets	MIT with exceptions BSD-2 BSD-3 Apache 2.0 ZLIB CC-zero	https://github.com/warmcat/ libw ebsockets/archive/refs/tags/ v4.3.3.tar.gz	https://opensource.org/licenses/MIT https://opensource.org/license/bsd-2-clause/ https://opensource.org/license/bsd-3-clause/ https://www.apache.org/licenses/ LICENSE-2.0.html https://www.apache.org/licenses/ LICENSE-2.0.html https://creativecommons.org/ publicdomain/zero/1.0/
linux_kernel	GPL-2.0 WITH Linux-syscall-note and GCC exception GFDL 1.1 GFDL 1.2 GPL 1.0 ISCX Linux-OpenIB X11 zlib Apache-2.0 CDDL 1.0 cc-by-4.0 mpl 1.1	https://www.st.com/content/ccc/ resource/technical/software/firmware/ group1/87/b0/dd/40/30/7e/43/be/ stm32mp1dev/files/SOURCES-stm32mp1-openstlinux-5.15-yocto-kirkstone-mp1-v22.11.23. tar.gz/jcr:content/translations/ en.SOURCES-stm32mp1-openstlinux-5.15-yocto-kirkstone-mp1-v22.11.23.tar.gz	https://www.gnu.org/licenses/old-licenses/gpl-2.0.en.html

tdb	LGPL-2.0	https://cdn.kernel.org/pub/linux/kernel/people/tytso/e2fsprogs/v1.47.0/e2fsprogs-1.47.0.tar.xz	https://www.gnu.org/licenses/old-licenses/lgpl-2.0.en.html
u-boot	GPL-2.0+	https://github.com/u-boot/u-boot/archive/refs/tags/v2021.10.tar.gz	https://www.gnu.org/licenses/old-licenses/gpl-2.0.en.html
util-linux	GPL-2.0 GPL-2.0+ GPL-3.0+ LGPL-2.1+ (libblkid, libfdisk, libmount) BSD-2-Clause BSD-3-Clause (libuuid) BSD-4-Clause (xxhash) ISC (rfkill)	https://cdn.kernel.org/pub/linux/utils/util-linux/v2.39/util-linux-2.39.3.tar.gz	https://www.gnu.org/licenses/old-licenses/lgpl-2.1.en.html https://opensource.org/license/BSD-3-clause
wireless-tools	GPL-2.0	https://hewlettpackard.github.io/wireless-tools/wireless_tools.30.pre9.tar.gz	https://www.gnu.org/licenses/old-licenses/gpl-2.0.en.html
zeromq	MPL v2	https://github.com/zeromq/libzmq/archive/refs/tags/v4.3.5.tar.gz	https://www.gnu.org/licenses/gpl-3.0.en.html https://www.gnu.org/licenses/lgpl-3.0.en.html https://www.mozilla.org/en-US/MPL/2.0
libxcrypt	LGPL-2.1+	https://github.com/besser82/libxcrypt/releases/download/v4.4.36/libxcrypt-4.4.36.tar.xz	https://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
mmc-utils	GPL-2.0	https://git.kernel.org/pub/scm/utils/mmc/mmc-utils.git	https://www.gnu.org/licenses/old-licenses/gpl-2.0.html

If any OSS contained in this Product is licensed under GNU General Public License (GPL), GNU Lesser General Public License (LGPL), Mozilla Public License (MPL) or any other OSS license, which requires that source code is to be made available, you can download the corresponding source code of the OSS from the aforementioned link.

Schneider Electric Industries SAS

35, rue Joseph Monier
CS 30323
F - 92500 Rueil Malmaison Cedex

www.se.com

As standards, specifications, and design change from time to time, please ask for confirmation of the information given in this publication.

BRU5883000-02_EN