

# Cybersecurity Guide

DOCA0310EN\_IEC-01  
10/2025



# 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.

This document and its content are protected under applicable copyright laws and provided for informative use only. No part of this document may be reproduced or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), for any purpose, without the prior written permission of Schneider Electric.

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.**

---

# Table of Contents

Safety Information.....	4
Safety Instructions.....	4
About the Book.....	6
Cybersecurity Information.....	7
Cybersecurity in Schneider Electric.....	8
Cybersecurity Policies .....	8
Cybersecurity Resources .....	8
Security Features .....	9
Supported Protocols.....	10
Potential Risks and Compensating Controls.....	10
Security Recommendations .....	11
Recommendations for Commissioning.....	11
Security Recommendations for Maintenance .....	11
Security Recommendations for Decommissioning.....	12

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

### **WARNING**

**WARNING** indicates a hazardous situation which, if not avoided, **could result in death or serious injury.**  
**Failure to follow these instructions can result in death, serious injury, or equipment damage.**

### **CAUTION**

**CAUTION** indicates a hazardous situation which, if not avoided, **could result in minor or moderate injury.**  
**Failure to follow these instructions can result in injury or equipment damage.**

### **NOTICE**

**NOTICE** is used to address practices not related to physical injury. The safety alert symbol shall not be used with this signal word.  
**Failure to follow these instructions can result in equipment damage.**

## 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

This manual provides information about using EVlink Pro DC charging stations in a trusted network environment, for instance, behind firewalls, and/or within the boundaries of an isolated OT network (separated from the IT network).

## Document Version History

Document reference version	Release date	Evolution
2.1	08/30/2025	Added Modbus TCP support
2.0	06/10/2025	Added Schneider StarCharge Fast 60 support.
1.0	03/15/2025	Initial build

## Validity Note

This document applies to Schneider Electric EVlink Pro DC charging stations.

## Terminology

Acronym	Designation
OCP	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 business strategy, which 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

EVlink Pro DC charging stations support to be connected to Ethernet/Wi-Fi networks. However, this networking capability is not designed to withstand the direct exposure to the public Internet.

## 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
- Periodic penetration and 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 EVlink Pro DC charging stations are 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 vulnerability management policy addresses cybersecurity vulnerabilities affecting Schneider Electric products in order to help secure customers.

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

Schneider Electric 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 EVlink Pro DC charging stations to help ensure that products operate according to the intended purpose.

These features provide security capabilities which help to protect the products from potential security threats that could disrupt the product operation (availability), modify the product configuration (integrity) or disclose information (confidentiality).

The key features are:

- Firmware authenticity verification at product startup (secure boot)
- Firmware update mechanism (via the device webpage and remote via OCPP/OMC) with firmware signature verification (using asymmetric cryptography)
- Both TLS 1.2 & TLS1.3 supported for securing and authenticating OCPP communications with a remote charging station management system (CSMS) and local webpage configuration
- Common Criteria EAL6+ certified security chip for storing the product private key and certificate
- Deactivation of internal debug and test interfaces
- Unsuccessful login attempt management:

The webpage login interface is locked for 30 minutes after the user enters the wrong username or password for six consecutive times. After 30 minutes, the login interface is automatically unlocked

- Password enhancement:

Webpage default password is forced to be changed at first login. The password length must be 8 to 31 characters, and must include at least one number, one uppercase, one lowercase, one special character (-;,\$&@,.,?!)

- Auto log out after an inactivity period:

User logs in to the web page. The account automatically logs out after 30 minutes without any operation (no mouse click or movement, no keyboard operation)

These security capability features are aimed at mitigating the threats related to the usage of the EVlink Pro DC 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 EVlink Pro DC charging stations, as well as Recommended Cybersecurity Best Practices.

## Supported Protocols

The following protocols are supported by EVlink Pro DC charging stations:

Protocol	Usage
OCPP + HTTPS	Communications with a remote Charging Station Management System <b>NOTE:</b> The OCPP protocol relies on additional HTTPS communications for supporting OCPP reporting and maintenance operations (firmware update)
HTTPS	Configuration through configuration tools
DHCP	Networking IP address
DNS	Network name resolution
Secure / Unsecure Modbus TCP	Communication with Energy Management System

## 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 damage 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	DHCP, DNS 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.
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.
Unsecure Modbus TCP communication	Modbus TCP lacks built-in security features: • No encryption No authentication	<ul style="list-style-type: none"> <li>• Data leakage: All traffic is in plaintext</li> <li>• Unauthorized control: Attackers can send fake commands</li> <li>• MITM attacks: Messages can be intercepted and altered</li> </ul> DoS: Flooding can crash devices	Recommendation: Use Modbus TLS for Secure Communication, otherwise: <ul style="list-style-type: none"> <li>• Isolate Modbus devices in secure networks</li> <li>• Restrict access to port 502 via firewall/ACL</li> <li>• Monitor traffic with IDS/IPS</li> <li>• Use VPN or IPsec tunnels for encryption</li> </ul> Log and audit all Modbus activity

# Security Recommendations

## Recommendations for Commissioning

### OCPP Communication Security

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

Communications relying on plain HTTP or plain Web Sockets are unsecure and are subject to man-in-the-middle attacks.

### Configuration of Services

Most EVlink Pro DC 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

Digital firmware is embedded in the EVlink Pro DC charging stations. The digital firmware may require an application of security patches to maintain an optimum level of security.

Consequently, it is recommended to periodically check that the installed firmware is updated to the latest version available.

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

### Audit Log

EVlink Pro DC charging stations maintain audit logs 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.

### WIFI Usage

When using WIFI, it is recommended to manually disable WIFI after the process.

### Payment Terminal (If Supported)

Inspect the terminal on a regular basis, looking for scratches, marks, or damage that may indicate an attempt at tampering.

# Security Recommendations for Decommissioning

## Reset to Factory Settings

The EVlink Pro DC charging stations can be configured with sensitive user information, which may include user account identifiers and 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.

## INFORMATION

### Open Source Software Used in EVlink Pro DC charging stations

The EVlink Pro DC charging stations contain, 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	Distributed under	Source Link	URL to License Text
busybox	GPL-2.0	GPL-2.0	<a href="https://www.busybox.net/downloads/busybox-1.36.1.tar.bz2">https://www.busybox.net/downloads/busybox-1.36.1.tar.bz2</a>	<a href="https://www.gnu.org/licenses/old-licenses/gpl-2.0.en.html">https://www.gnu.org/licenses/old-licenses/gpl-2.0.en.html</a>
dbus	AFL-2.1/GPL-2.0	GPL-2.0(programs) AFL-2.1 (libraries)	<a href="https://dbus.freedesktop.org/releases/dbus/">https://dbus.freedesktop.org/releases/dbus/</a>	<a href="https://gitlab.freedesktop.org/dbus/dbus/-/blob/dbus-1.14.10/COPYING">https://gitlab.freedesktop.org/dbus/dbus/-/blob/dbus-1.14.10/COPYING</a>
e2fsprogs	GPL-2.0	GPL-2.0	<a href="https://git.kernel.org/pub/scm/fs/ext2/e2fsprogs.git">https://git.kernel.org/pub/scm/fs/ext2/e2fsprogs.git</a>	<a href="https://www.gnu.org/licenses/old-licenses/gpl-2.0.html">https://www.gnu.org/licenses/old-licenses/gpl-2.0.html</a>
eudev	GPL-2.0+ (programs)	GPL-2.0(programs) LGPL-2.1(libraries)	<a href="https://github.com/eudev-project/eudev/releases/tag/v3.2.14">https://github.com/eudev-project/eudev/releases/tag/v3.2.14</a>	<a href="https://www.gnu.org/licenses/old-licenses/gpl-2.0.html">https://www.gnu.org/licenses/old-licenses/gpl-2.0.html</a>
freetype	FTL or GPL-2.0+	FTL	<a href="https://github.com/freetype/freetype/tree/VER-2-13-2">https://github.com/freetype/freetype/tree/VER-2-13-2</a>	<a href="https://github.com/freetype/freetype/blob/VER-2-13-2/LICENSE.TXT">https://github.com/freetype/freetype/blob/VER-2-13-2/LICENSE.TXT</a>
glibc	LGPL-2.1	LGPL-2.1	<a href="https://sourceware.org/git/glibc.git">https://sourceware.org/git/glibc.git</a>	<a href="https://www.gnu.org/licenses/old-licenses/lgpl-2.1.html">https://www.gnu.org/licenses/old-licenses/lgpl-2.1.html</a>
htop	GPL-2.0+	GPL-2.0	<a href="https://github.com/htop-dev/htop/tree/3.3.0">https://github.com/htop-dev/htop/tree/3.3.0</a>	<a href="https://github.com/htop-dev/htop/blob/main/COPYING">https://github.com/htop-dev/htop/blob/main/COPYING</a>
imx-kobs	GPL-2.0+	GPL-2.0	<a href="https://github.com/nxp-imx/imx-kobs">https://github.com/nxp-imx/imx-kobs</a>	<a href="https://spdx.org/licenses/GPL-2.0.html">https://spdx.org/licenses/GPL-2.0.html</a>
iproute2	GPL-2.0+	GPL-2.0	<a href="https://git.kernel.org/pub/scm/network/iproute2/iproute2.git">https://git.kernel.org/pub/scm/network/iproute2/iproute2.git</a>	<a href="https://www.gnu.org/licenses/old-licenses/gpl-2.0.html">https://www.gnu.org/licenses/old-licenses/gpl-2.0.html</a>
iptables	GPL-2.0	GPL-2.0	<a href="https://git.netfilter.org/iptables/">https://git.netfilter.org/iptables/</a>	<a href="https://www.gnu.org/licenses/old-licenses/gpl-2.0.html">https://www.gnu.org/licenses/old-licenses/gpl-2.0.html</a>
kmod	LGPL-2.1+ (library)	LGPL-2.1 (library)	<a href="https://github.com/kmod-project/kmod/releases/tag/v31">https://github.com/kmod-project/kmod/releases/tag/v31</a>	<a href="https://www.gnu.org/licenses/old-licenses/gpl-2.0.html">https://www.gnu.org/licenses/old-licenses/gpl-2.0.html</a>
libatomic1	GPL-3.0-with-GCC-exception	GPL-3.0-with-GCC-exception	<a href="https://gcc.gnu.org/releases.html">https://gcc.gnu.org/releases.html</a>	<a href="https://gcc.gnu.org/onlinedocs/gcc-12.3.0/gcc/Copying.html">https://gcc.gnu.org/onlinedocs/gcc-12.3.0/gcc/Copying.html</a>
libestr	LGPL-2.1+	LGPL-2.1	<a href="https://github.com/rsyslog/libestr/releases/tag/v0.1.11">https://github.com/rsyslog/libestr/releases/tag/v0.1.11</a>	<a href="https://spdx.org/licenses/LGPL-2.1.html">https://spdx.org/licenses/LGPL-2.1.html</a>
libmodbus	LGPL-2.1+	LGPL-2.1	<a href="https://github.com/stephane/libmodbus/releases">https://github.com/stephane/libmodbus/releases</a>	<a href="https://spdx.org/licenses/LGPL-2.1.html">https://spdx.org/licenses/LGPL-2.1.html</a>
libnl	LGPL-2.1+	LGPL-2.1	<a href="https://github.com/thom311/libnl/releases/tag/libnl3_9_0">https://github.com/thom311/libnl/releases/tag/libnl3_9_0</a>	<a href="https://github.com/thom311/libnl/blob/libnl3_9_0/COPYING">https://github.com/thom311/libnl/blob/libnl3_9_0/COPYING</a>
libqrencode	LGPL-2.1+	LGPL-2.1	<a href="https://github.com/fukuchi/libqrencode/tree/v4.1.1">https://github.com/fukuchi/libqrencode/tree/v4.1.1</a>	<a href="https://github.com/fukuchi/libqrencode/blob/master/COPYING">https://github.com/fukuchi/libqrencode/blob/master/COPYING</a>
libts	LGPL-2.1	LGPL-2.1	<a href="https://github.com/libts/tslib/tree/1.23">https://github.com/libts/tslib/tree/1.23</a>	<a href="https://github.com/libts/tslib/blob/master/COPYING">https://github.com/libts/tslib/blob/master/COPYING</a>
libxcrypt	LGPL-2.1+	LGPL-2.1	<a href="https://github.com/bes">https://github.com/bes</a>	<a href="https://spdx.org/licenses/">https://spdx.org/licenses/</a>

			ser82/libxcrypt/releases	GPL-2.0.html
linux_kernel	GPL-2.0	GPL-2.0	<a href="https://www.kernel.org/pub/linux/kernel/v4.x/linux-4.14.98.tar.gz">https://www.kernel.org/pub/linux/kernel/v4.x/linux-4.14.98.tar.gz</a> For the code of the modifications made to this component, please refer to SOP of OSS Application on how to obtain a copy.	<a href="https://www.kernel.org/doc/html/v6.14-rc3/process/license-rules.html">https://www.kernel.org/doc/html/v6.14-rc3/process/license-rules.html</a>
mtd	GPL-2.0	GPL-2.0	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/mtd/linux.git">https://git.kernel.org/pub/scm/linux/kernel/git/mtd/linux.git</a>	<a href="https://www.gnu.org/licenses/old-licenses/gpl-2.0.html">https://www.gnu.org/licenses/old-licenses/gpl-2.0.html</a>
tzdata	Public domain	Public domain	<a href="https://www.iana.org/time-zones">https://www.iana.org/time-zones</a>	<a href="https://spdx.org/licenses/">https://spdx.org/licenses/</a>
u-boot	GPL-2.0	GPL-2.0	<a href="https://github.com/u-boot/u-boot/releases/tag/v2015.04">https://github.com/u-boot/u-boot/releases/tag/v2015.04</a> For the code of the modifications made to this component, please refer to SOP of OSS Application on how to obtain a copy.	<a href="https://www.gnu.org/licenses/old-licenses/gpl-2.0.html">https://www.gnu.org/licenses/old-licenses/gpl-2.0.html</a>
uboot-tools	GPL-2.0	GPL-2.0	<a href="https://github.com/u-boot/u-boot/releases/tag/v2021.07">https://github.com/u-boot/u-boot/releases/tag/v2021.07</a>	<a href="https://www.gnu.org/licenses/old-licenses/gpl-2.0.html">https://www.gnu.org/licenses/old-licenses/gpl-2.0.html</a>
util-linux	GPL-2.0	GPL-2.0	<a href="https://github.com/util-linux/util-linux/releases/tag/v2.39.3">https://github.com/util-linux/util-linux/releases/tag/v2.39.3</a>	<a href="https://www.gnu.org/licenses/old-licenses/gpl-2.0.html">https://www.gnu.org/licenses/old-licenses/gpl-2.0.html</a>
zeromq	MPL-2.0	MPL-2.0	<a href="https://github.com/zeromq/libzmq/releases/tag/v4.3.5">https://github.com/zeromq/libzmq/releases/tag/v4.3.5</a>	<a href="https://spdx.org/licenses/LGPL-3.0.html">https://spdx.org/licenses/LGPL-3.0.html</a>

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  
35 rue Joseph Monier  
92500 Rueil Malmaison  
France

+ 33 (0) 1 41 29 70 00

[www.se.com](http://www.se.com)

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

© 2024 – 2025 Schneider Electric. All rights reserved.

DOCA0310EN\_IEC-01