EVlink Pro DC

Cybersecurity Guide

DOCA0310EN-01
03/2024

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.

Table of Contents

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

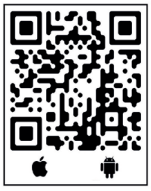
HAZARD OF ELECTRIC SHOCK

- 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

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).

Validity Note

This document applies to Schneider Electric EVlink Pro DC 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 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) with firmware signature verification (using asymmetric cryptography)
- Both TLS 1.2 & TLS1.3 supported for securing and authenticating OCCP 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 (TLS 1.2) + HTTPS	Communications with a remote Charging Station Management System **NOTE:** The OCPP protocol relies on additional HTTPS communications for supporting OCPP reporting and maintenance operations (firmware update)
HTTPS (TLS 1.2)	Configuration through configuration tools
Modbus RTU	Communications with power meters
DHCP	Networking IP address
DNS	Network name resolution

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	Modbus RTU, 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.

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.

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

DOCA0310EN-01