

Cybersecurity

Information for REO AG Electronic Devices



Change History

Version	Date	Change
1.0	October 2, 2026	First Edition

Table of Contents

Change History	2
1.0 Purpose and Scope	4
2.0 General Information for Secure Integration.....	4
2.1 Internal Interfaces and Physical Access.....	4
3.0 Industrial Ethernet Interfaces.....	5
3.1 General Safety Instructions	5
3.2 Protocol-Specific Features	5
PROFINET and EtherNet/IP	5
EtherCAT.....	5
Modbus TCP	5
OPC UA.....	5
3.3 Additional Network Services and Functions	5
4.0 Fieldbuses—CAN, DeviceNet, and PROFIBUS.....	6
5.0 Security Updates and Revisions.....	6
6.0 Vulnerability Reporting	6
7.0 Permanent Decommissioning	6
8.0 Applicable Documentation	6

1.0 Purpose and Scope

This document describes general cybersecurity guidelines for the secure use of electronic devices from REO AG that fall within the scope of the Cyber Resilience Act (CRA) and supplements the product-specific Operating Instructions and Interface Manuals.

REO AG electronic devices, such as control units for vibratory feeders or power supplies, may be equipped with one or more communication interfaces, depending on the device version. These include, in particular, Industrial Ethernet interfaces such as PROFINET, EtherNet/IP, EtherCAT, Modbus TCP, and OPC UA, as well as conventional fieldbus interfaces such as PROFIBUS, DeviceNet, and CAN.

Depending on the device version, the communication interfaces may be integrated directly into the device or connected via communication modules or gateways. The corresponding connections may be accessible from the outside or located inside the device housing or behind covers. In addition, internal programming or service interfaces may be present, for example, for the microcontroller or for internal communication purposes.

2.0 General Information for Secure Integration

The following measures apply regardless of the communication protocol used and must be implemented in accordance with the respective system and network architecture:

- Restrict access to communication interfaces to authorized personnel and systems required for operation, control, commissioning, and service.
- Protect devices, communication interfaces, cables, and accessible connections against unauthorized physical access.
- Changes to security-relevant device and communication settings may only be made by authorized personnel.
- Use only the files, parameter lists, and documentation approved by REO that are intended for the specific product version and corresponding revision status.

2.1 Internal Interfaces and Physical Access

Depending on the device version, programming or communication interfaces may be located inside the closed device housing or behind covers. This restricts physical access to these interfaces and reduces the risk of unauthorized access.

For device versions with an internal microcontroller programming interface, this is typically located inside the closed device housing. Where provided for the respective microcontroller version, additional technical access protection mechanisms—such as lock bits—are used to restrict unauthorized access to program memory and firmware.

3.0 Industrial Ethernet Interfaces

3.1 General Safety Instructions

Network-enabled communication interfaces are intended for operation within controlled industrial network environments. Direct, unprotected accessibility from the Internet or from untrusted networks is not intended.

- Segment Industrial Ethernet networks from office, third-party, and public networks in accordance with the system architecture
- Restrict communication between network segments—to the extent required by the system architecture—using firewalls or comparable access controls.
- Allow configuration, parameterization, engineering, and diagnostic access only by authorized persons or systems and from the designated network segments.
- Avoid or limit unnecessary connections between the automation network and other networks.

3.2 Protocol-Specific Features

The general security measures from Section 3.1 apply regardless of the protocol used. Protocol-specific information is included in this document only if it results in an additional measure for secure operation. Technical integration and compatibility information, such as that regarding GSDML, EDS, or ESI files, is part of the respective interface manual. Only files approved by REO for the respective product and communication configuration may be used.

PROFINET and EtherNet/IP

The current REO device versions support PROFINET RT and EtherNet/IP, respectively, and do not include the additional protocol-specific security functions PROFINET Security and CIP Security, respectively. Secure integration must therefore be implemented in accordance with Section 3.1.

EtherCAT

For typical EtherCAT system configurations, external assessments in accordance with IEC 62443-3-3 are available up to Security Level 2. The EtherCAT system architecture can thus help limit the attack surface. The general protective measures outlined in Section 3.1 apply to the secure integration of the REO EtherCAT interface.

Modbus TCP

Classic Modbus TCP does not provide integrated user authentication or encryption. Secure integration must therefore be implemented in accordance with the general protective measures outlined in Section 3.1.

OPC UA

For OPC UA, only the security policies, certificate, and authentication mechanisms approved for the specific product configuration may be used. The supported functions can be found in the product-specific OPC UA documentation.

3.3 Additional Network Services and Functions

Depending on the communication interface, additional network services or functions may be available, such as web, diagnostic, or configuration functions. Access to such services must be restricted to the designated network segments as well as to authorized persons and systems. Which services are available in the specific implementation and how they are to be used securely is described in the respective interface or product documentation.

4.0 Fieldbuses—CAN, DeviceNet, and PROFIBUS

Fieldbus interfaces are intended for use in a controlled industrial environment. Access to the fieldbus must be restricted to the intended participants. The general protective measures from Section 2 apply to physical access as well as to configuration and parameterization.

5.0 Security Updates and Revisions

Security updates and update information are provided by REO as required for the respective product configuration.

For communication modules designed for this purpose, the customer may install approved updates themselves. Only updates and installation procedures that have been expressly approved by REO for the respective communication module may be used.

Firmware updates for REO device firmware, as well as for parts of the communication modules not approved for customer updates, are not intended for independent installation by the customer. Necessary revisions to these components are performed by REO. To this end, the device must generally be returned to REO.

6.0 Vulnerability Reporting

REO provides up-to-date information on the reporting of potential vulnerabilities centrally on the security page.

REO Security Information: <https://reo-ag.com/safety/>

7.0 Permanent Decommissioning

For device versions that store security-relevant user, certificate, network, or configuration data, this data must be securely removed or reset before the device is permanently taken out of service. This applies in particular to OPC UA versions equipped with these features.

The procedure for doing so can be found in the respective product or interface documentation.

For device versions that do not store such data, no additional measures for data erasure are required.

8.0 Applicable Documentation

- Operating Instructions for the respective REO device
- Interface manual for the communication interface used
- Device description files approved for the respective version

Notes:



■ REO AG

Brühler Straße 100 · D-42657 Solingen
Tel.: +49 (0)212 8804 0 · Fax: +49 (0)212 8804 188

E-Mail: info@reo.de
Internet: www.reo.de

Divisions:

REO Vibratory Feeding and Power Electronics Division

REO Vibratory Feeding and Power Electronics Division
Brühler Straße 100 · D-42657 Solingen
Tel.: +49 (0)212 8804 0 · Fax: +49 (0)212 8804 188
E-Mail: info@reo.de

REO Train Technologies Division

REO Train Technologies Division
Erasmusstraße 14 · D-10553 Berlin
Tel.: +49 (0)30 3670236 0 · Fax: +49 (0)30 3670236 10
E-Mail: zentrale.berlin@reo.de

REO Drives Division

REO Drives Division
Holzhausener Straße 52
D-16866 Kyritz
Tel.: +49 (0)33971 485 0 · Fax: +49 (0)33971 485 90
E-Mail: zentrale.kyritz@reo.de

REO Medical and Current Transformer Division

REO Medical and Current Transformer Division
Schuldhölzinger Weg 7 · D-84347 Pfarrkirchen
Tel.: +49 (0)8561 9886 0 · Fax: +49 (0)8561 9886 40
E-Mail: zentrale.pfarrkirchen@reo.de

REO Test and PowerQuality Division

REO Test and PowerQuality Division
Brühler Straße 100 · D-42657 Solingen
Tel.: +49 (0)212 8804 0 · Fax: +49 (0)212 8804 188
E-Mail: info@reo.de

PRODUCTION+SALES:

■ India

REO GPD INDUCTIVE COMPONENTS PVT. LTD
E-Mail: info@reogpd.com · Internet: www.reo-ag.in

■ USA

REO-USA, Inc.
E-Mail: info@reo-usa.com · Internet: www.reo-usa.com

SALES:

■ France

REO VARIAC S.A.R.L.
E-Mail: reovariac@reo.fr · Internet: www.reo.fr

■ Great Britain

REO (UK) Ltd.
E-Mail: main@reo.co.uk · Internet: www.reo.co.uk

■ Italy

REO ITALIA S.r.l.
E-Mail: info@reitalia.it · Internet: www.reoitalia.it

■ Poland

REO CROMA Sp.zo.o
E-Mail: croma@croma.com.pl · Internet: www.croma.com.pl

■ Spain

REO ESPAÑA 2002 S.A.
E-Mail: info@reospain.com · Internet: www.reospain.com

■ Switzerland

REO ELEKTRONIK AG
E-Mail: info@reo.ch · Internet: www.reo.ch

■ Turkey

REOTURKEY ELEKTRONİK San. ve Tic. Ltd. Şti.
E-Mail: info@reo-turkey.com · Internet: www.reo-turkey.com

■ China

REO Shanghai Inductive Components Co., Ltd
E-Mail: info@reo.cn · Internet: www.reo.cn

■ United Arab Emirates

REO INDUCTIVE COMPONENTS FZCO
E-Mail: info@reo-middle-east.com · Internet: www.reo-middle-east.com