



Manual



Cybersecurity for generation B inverters



Table of contents

1	General information	4
1.1	How to use this documentation	4
1.2	Other applicable documentation	5
1.3	Product names and trademarks	5
1.4	Copyright notice	5
2	Safety notes	6
2.1	Target group	6
2.2	Contact.....	6
3	Fulfillment of the requirements from IEC 62443-4-2	7
3.1	Compensatory measures	7
3.2	Structure of the tables	7
3.3	FR1 – Identification and authentication (IAC)	8
3.4	FR2 – Use control (UC)	10
3.5	FR3 – System integrity (SI).....	12
3.6	FR4 – Data confidentiality (DC)	13
3.7	FR5 – Restricted data flow (RDF).....	14
3.8	FR6 – Timely response to events (TRE).....	14
3.9	FR7 – Availability of resources (RA)	15
4	Recommendations for safe operation.....	16
4.1	Recommendations for installation in a control cabinet.....	17
4.2	Recommendations for decentralized installation	18
5	Software and firmware updates	19
6	Ports and services	20
7	Contacting SEW-EURODRIVE.....	21

1 General information

1.1 How to use this documentation

As a system operator or integrator, you must ensure that your system meets the relevant cybersecurity requirements for the application. With this manual, SEW-EURODRIVE provides you with the information required for evaluation and provides recommendations regarding hardening measures and processes.

This documentation bundles security-related information for several SEW-EURODRIVE products. It supplements, but does not replace, the respective operating instructions and product manuals.

This documentation is aimed at the following groups within the system operator and system integrator: IT security officers, planners, project planners and programmers of automation systems, as well as persons authorized to start up, operate, and maintain the devices and systems.

Knowledge in the area of OT security and of the relevant security regulations is required.

The measures in this document are intended to increase cybersecurity in general and are based on the requirements for SL 1 at system level according to IEC 62443. However, SEW-EURODRIVE does not guarantee that SL 1 will be achieved. Higher Security Levels are not considered.

1.1.1 Referenced standards

This manual primarily refers to the following standards:

IEC 62443-3-3	The IEC 62443-3-3 standard is part of the international "Industrial communication networks – Network and system security" IEC 62443 series of standards. The standard defines the System Requirements (SR) that are associated with the Foundational Requirements (FR) from IEC 62443-1-1. Use the standard to assess the extent to which your products and services meet the requirements or whether the Target Security Level (SL-T) is achieved. Not every component of the system has to comply with all system requirements of the SL-T. You can implement compensatory measures and document them in order to still achieve the SL-T at the system level (SL-A).
IEC 62443-4-2	Similar to the IEC 62443-3-3 standard, standard 62443-4-2 defines requirements and security levels. However, it deals with the component level. The Foundational Requirements (FR) and System Requirements (SR) are assigned technical requirements for components (CR). As a component manufacturer, SEW-EURODRIVE provides information on the extent to which the products meet the requirements and, if necessary, recommends compensatory measures.

1.1.2 Products described

This documentation applies to the following generation B products:

- MOVIDRIVE® MDX60B/61B
- MOVITRAC® MC07B
- MOVITRAC® LTE-B⁺, MOVITRAC® LTP-B
- MOVIAxis®
- MOVIGEAR® B
- MOVIMOT® D
- MOVIFIT®
- MOVITRANS®
- MOVIPRO® SDC/ADC
- MOVI-DPS®
- DRC
- MFE

1.2 Other applicable documentation

This documentation supplements the operating instructions of the associated product. Use this document only in connection with the operating instructions.

Always use the latest edition of the documentation and the software.

The SEW-EURODRIVE website (www.sew-eurodrive.com) provides a wide selection of documents for download in various languages. If required, you can also order printed and bound copies of the documentation from SEW-EURODRIVE.

1.3 Product names and trademarks

The product names mentioned in this documentation are trademarks or registered trademarks of the respective titleholders.

1.4 Copyright notice

© 2025 SEW-EURODRIVE. All rights reserved. Copyright law prohibits the unauthorized reproduction, modification, distribution and use of this document – in whole or in part.

2 Safety notes

2.1 Target group

For information on the target groups of the products, refer to the respective product documentation.

2.2 Contact



SEW-EURODRIVE offers the following communication channels for IT security:

- Report incidents regarding cybersecurity by e-mail to cert@sew-eurodrive.com or via the contact form on the Product Security Management website (<http://go.sew/psm>).
- Security advisories can be found in the SEW-EURODRIVE Online Support.
 - For automatic updates on new and changed security advisories, subscribe to the newsletter on the Product Security Management page (<http://go.sew/psm>).
- If you need support with the configuration, contact SEW-EURODRIVE Service.

3 Fulfillment of the requirements from IEC 62443-4-2

The following information indicates to what extent the products meet the requirements of IEC 62443-4-2. In addition, compensatory measures are recommended that can be used to achieve a security level comparable to SL 1 when integrated into a system.

3.1 Compensatory measures

3.1.1 M1: Restrict physical access to the product

- Set up a physical access control for the room or control cabinet where the product is located. For example, use robust housings, locks, envelopes, or safety screws for this purpose.
- Access must only be possible for qualified personnel, for example via keys, key cards, biometric features, or special tools for access.

3.1.2 M2: Remove and safely store operator panels

- Remove operator panels from the product after use.
- Safely store operator panels separately from the product.
- Access to operator panels must only be granted to authorized persons, e.g. maintenance personnel.

3.1.3 M3: Set up access control at system level

- Set up access controls at the system level. For example, you can use passwords to protect engineering PCs and user interfaces.

3.1.4 M4: Introduce password policy at system level

- Implement a password policy that, for example, specifies the required password strength and how often passwords must be changed.
- Change passwords according to your password policy, but at the latest when employees leave the company.
- Assign individual passwords. Do not use the same password for multiple roles.

3.1.5 M5: Only establish connections to trusted networks

- Define requirements for trusted networks in advance. Only allow connections to networks that meet the specified requirements.

3.1.6 M6: Segment the network

The creation of zones and the associated network segmentation form the basis for a defense-in-depth strategy. Segment into zones based on the results of the threat and risk analysis and the system conditions.

- Divide the network into smaller zones.

3.2 Structure of the tables

Column "Requirement"

The specified requirements are taken from the IEC 62443-4-2 standard.

- FR: Foundational Requirements
- CR: Technical requirements for the components
- RE: Extended requirements
- EDR: Requirements for embedded devices

Column "SL 1"

Indicates the extent to which the requirements of Security Level 1 are met at the component level and whether compensatory measures are recommended.

- "✓": The requirement is met.
- "+": The requirement is met with appropriate parameterization.
- "o": The requirement is not required for the Security Level or is not relevant for the product.
- "-": The requirement is not met.

Column "Recommended compensatory measures at system level"

Refers to compensatory measures recommended by SEW-EURODRIVE to improve security at the system level. The intended security level corresponds to SL 1 according to IEC 62443-3-3.

- "-": Not required.

3.3 FR1 – Identification and authentication (IAC)

3.3.1 Meaning of the security level

The IEC 62443-4-2 standard defines Security Level 1 as follows:

Security Level	Description
SL 1	Identify and authenticate all users (human users, software processes, and devices) using mechanisms that protect against casual or accidental access by unauthenticated entities.

3.3.2 Fulfillment of the requirements (FR1)

Requirement	SL 1	Recommended compensatory measures at system level
CR 1.1 – Human user identification and authentication	–	"M1" (→ 7), "M2" (→ 7), "M3" (→ 7)
CR 1.1 RE (1) – Unique identification and authentication	o	–
CR 1.1 RE (2) – Multi-factor authentication via all interfaces	o	–
CR 1.2 – Identification and authentication of software processes and devices	o	–
CR 1.2 RE (1) – Unique identification and authentication	o	–
CR 1.3 – Account management	–	"M1" (→ 7), "M2" (→ 7), "M3" (→ 7)
CR 1.4 – Identifier management	–	"M1" (→ 7), "M2" (→ 7), "M3" (→ 7)

Requirement	SL 1	Recommended compensatory measures at system level
CR 1.5 – Authenticator management	–	"M1" (→ 7), "M2" (→ 7), "M3" (→ 7)
CR 1.5 RE (1) – Hardware security for authenticators	o	–
CR 1.7 – Strength of password-based authentication	–	"M4" (→ 7)
CR 1.7 RE (1) Generation and lifetime restrictions of passwords for human users	o	–
CR 1.7 RE (2) – Password lifetime restrictions for all users (human users, software processes, or devices)	o	–
CR 1.8 – PKI certificates	o	–
CR 1.9 – Strength of public key-based authentication	o	–
CR 1.10 – Authenticator feedback	–	"M3" (→ 7)
CR 1.11 – Unsuccessful login attempts	–	"M3" (→ 7)
CR 1.12 – System usage note	–	"M1" (→ 7), "M3" (→ 7)
CR 1.14 – Strength of symmetric key-based authentication	o	–
RE (1) – Hardware security for authentication using symmetrical keys	o	–

3.4 FR2 – Use control (UC)

3.4.1 Meaning of the security level

The IEC 62443-4-2 standard defines Security Level 1 as follows:

Security Level	Description
SL 1	Restricting the use of the IACS (Industrial Automation and Control System) according to defined permissions to protect against casual or accidental misuse.

3.4.2 Fulfillment of the requirements (FR2)

Requirement	SL 1	Recommended compensatory measures at system level
CR 2.1 – Authorization enforcement	–	"M1" (→ 7), "M3" (→ 7)
CR 2.1 RE (1) – Enforcement of authorization for all users (human users, software processes, and devices)	o	–
CR 2.1 RE (2) – Mapping permissions to roles	o	–
CR 2.1 RE (3) – Intervention by supervisory personnel	o	–
CR 2.1 RE (4) – Double consent	o	–
CR 2.2 – Wireless use control	o	–
CR 2.3 – Portable and mobile device use control	o ^{1) 2)}	–
EDR 2.4 – Mobile code	o ¹⁾	–
EDR 2.4 RE (1) – Authenticity check of mobile codes	o	–
CR 2.5 – Session lock	–	"M3" (→ 7)
CR 2.6 – Remote session termination	o	–
CR 2.7 – Concurrent session control	o	–
CR 2.8 – Auditable events	–	Handle IT security event records at the system level. - Required categories: Access control, faulty requests, events in the automation system, events during backup and restore, configuration changes, events visible in the event log - Required information: Timestamp, source, category, type, event ID, result of the event
CR 2.9 – Audit storage capacity	–	Handle IT security event records at the system level.
CR 2.9 RE (1) – Warning when the storage capacity for event records is reached	o	–
CR 2.10 – Response to audit processing failures	–	Handle IT security event records at the system level.
CR 2.11 – Timestamp	–	Handle IT security event records at the system level.
CR 2.12 – Non-repudiation	–	"M1" (→ 7), "M3" (→ 7)

Requirement	SL 1	Recommended compensatory measures at system level
CR 2.12 RE (1) – Non-repudiation for all users	o	–
EDR 2.13 – Use of physical diagnostic and test interfaces	o	–

- 1) The product does not use a mobile code.
2) There are no component-level requirements for IEC 62443-3-3 SR 2.3.

3.5 FR3 – System integrity (SI)

3.5.1 Meaning of the security levels

The IEC 62443-4-2 standard defines Security Level 1 as follows:

Security Level	Description
SL 1	Protecting the integrity of the IACS against occasional or accidental tampering

3.5.2 Fulfillment of the requirements (FR3)

Requirement	SL 1	Recommended compensatory measures at system level
CR 3.1 – Communication integrity	— ¹⁾	"M1" (→ 7), "M3" (→ 7), "M5" (→ 7), "M6" (→ 7)
CR 3.1 RE (1) – Authentication of communication	o	—
EDR 3.2 – Protection against malicious codes	—	"M1" (→ 7), "M3" (→ 7)
CR 3.3 – Verification of the IT security functionality	—	The system integrator must provide the operator with instructions for checking the required IT security measures.
CR 3.3 RE (1) – Verification of IT security functionality during ongoing operation	o	—
CR 3.4 – Software and information integrity	—	"M1" (→ 7), "M3" (→ 7)
CR 3.4 RE (1) – Authenticity of the software and information	o	—
CR 3.4 RE (2) – Automated notification of IT security violations	o	—
CR 3.5 – Input validation	✓	—
CR 3.6 – Predetermined output states	✓ ²⁾	—
CR 3.7 – Troubleshooting	✓	—
CR 3.8 – Session integrity	o	—
CR 3.9 – Protection of audit information	o	—
CR 3.9 RE (1) – Event records on write-once storage media	o	—
EDR 3.10 – Support for updates	✓	"M1" (→ 7), "M3" (→ 7)
EDR 3.10 RE (1) – Authenticity and integrity of updates	o	—
EDR 3.11 – Protection against and detection of physical tampering	o	—
EDR 3.11 RE (1) – Notification of a tampering attempt	o	—
EDR 3.12 – Provision of manufacturer trust anchors	o	—

Requirement	SL 1	Recommended compensatory measures at system level
EDR 3.13 – Provision of operator trust anchors	o	–
EDR 3.14 – Integrity of boot processes	— ³⁾	"M1" (→ 7), "M3" (→ 7)
EDR 3.14 RE (1) – Authenticity of the boot process	o	–

1) Communication is protected by a cyclic redundancy check (CRC).

2) Responses to errors such as network timeout or network overload are defined.

3) Integrity is protected by a cyclic redundancy check (CRC).

3.6 FR4 – Data confidentiality (DC)

3.6.1 Meaning of the security levels

The IEC 62443-4-2 standard defines Security Level 1 as follows:

Security Level	Description
SL 1	Prevention of unauthorized disclosure of information through eavesdropping or accidental exposure.

3.6.2 Fulfillment of the requirements (FR4)

Requirement	SL 1	Recommended compensatory measures at system level
CR 4.1 – Confidentiality of information	o ¹⁾	–
CR 4.2 – Durability of information	o	–
CR 4.2 RE (1) – Deleting shared storage resources	o	–
CR 4.2 RE (2) – Verification of deletion	o	–
CR 4.3 – Use of data encryption	o ²⁾	–

1) Not applicable since there is no data with explicit read protection.

2) Not applicable since no cryptographic methods are used.

3.7 FR5 – Restricted data flow (RDF)

3.7.1 Meaning of the security levels

The IEC 62443-4-2 standard defines Security Level 1 as follows:

Security Level	Description
SL 1	Preventing occasional or accidental bypass of zone and conduit separation.

3.7.2 Fulfillment of the requirements (FR5)

Requirement	SL 1	Recommended compensatory measures at system level
CR 5.1 – Network segmentation	✓	"M5" (→ 7), "M6" (→ 7)

3.8 FR6 – Timely response to events (TRE)

3.8.1 Meaning of the security levels

The IEC 62443-4-2 standard defines Security Level 1 as follows:

Security Level	Description
SL 1	Monitoring the operation of the IACS component and responding to incidents as soon as they are detected by collecting and providing forensic evidence upon request.

3.8.2 Fulfillment of the requirements (FR6)

Requirement	SL 1	Recommended compensatory measures at system level
CR 6.1 – Audit log accessibility	o	Handle IT security event records at the system level.
CR 6.1 RE (1) – Programmatic access to event logs	o	–
CR 6.2 – Continuous monitoring	o	–

3.9 FR7 – Availability of resources (RA)

3.9.1 Meaning of the security levels

The IEC 62443-4-2 standard defines Security Level 1 as follows:

Security Level	Description
SL 1	Ensure that the component operates reliably under normal production conditions and prevents Denial-of-Service (DoS) situations caused by occasional or accidental actions of an entity.

3.9.2 Fulfillment of the requirements (FR7)

Requirement	SL 1	Recommended compensatory measures at system level
CR 7.1 – Denial of service protection	✓	SEW-EURODRIVE recommends the following measures to further strengthen security: "M1" (→ 7), "M3" (→ 7), "M5" (→ 7), "M6" (→ 7)
CR 7.1 RE (1) – Management of the communication load by a component	o	–
CR 7.2 – Resource management	✓	–
CR 7.3 – Data backup in the automation system (backup)	✓ ¹⁾	–
CR 7.4 – Recovery of the automation system	✓	–
CR 7.5 – Emergency power supply	o	–
CR 7.6 – Network and IT security settings	o ²⁾	–
CR 7.6 RE (1) – Machine-readable reports about the current IT security settings	o	–
CR 7.7 – Least functionality	–	"M1" (→ 7), "M3" (→ 7), "M5" (→ 7), "M6" (→ 7)
CR 7.8 – Directory of the components of an automation system	o	–

1) Data backup is only possible while the inverter is not enabled.

2) The products do not have any IT security settings. For information on network settings, refer to the documentation of the products.

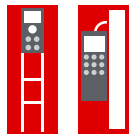
4 Recommendations for safe operation

There are various ways to prevent unauthorized access to the products depending on the system environment. Based on a risk and threat assessment, the system integrator decides which precautions must be taken in each specific case. The following chapters present various options for securing the products. With these measures, a security level comparable to SL 1 can be achieved within the system in most cases.

The following applies as a general rule:

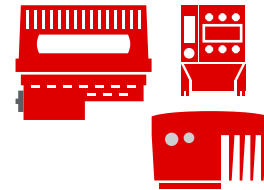
- Reduce the attack surface.
 - Only open ports that are required in your firewall. Close all other ports (Principle of Least Privilege).
 - During operation, activate only the services that are required for operation.
- Limit access to rooms, control cabinets, and housings.

The implementation largely depends on whether the product is operated in a control cabinet or in a decentralized setup:



Products for installation in a control cabinet (degree of protection IP1. or IP2.)

See "Recommendations for installation in a control cabinet" (→ 17).



Products for decentralized installation (degree of protection IP5. or IP6.)

See "Recommendations for decentralized installation" (→ 18).

4.1 Recommendations for installation in a control cabinet

The products for mounting in a control cabinet are intended for installation in lockable housings or rooms.

Check whether the following guidelines must be taken into account when the products are used in your system.

4.1.1 Recommendations for local access

- Set up a physical access control for the room or control cabinet where the product is located. For example, use robust housings, locks, envelopes, or safety screws for this purpose.
- Access must only be possible for qualified personnel, for example via keys, key cards, biometric features, or special tools for access.
- Remove operator panels from the product after use.
- Safely store operator panels separately from the product.
- Access to operator panels must only be granted to authorized persons, e.g. maintenance personnel.
- To reduce the risk of unintentional changes to parameters, activate the parameter lock if available on the device.

4.1.2 Recommendations for remote access

The creation of zones and the associated network segmentation form the basis for a defense-in-depth strategy. Segment into zones based on the results of the threat and risk analysis and the system conditions.

Remote access can be established, for example, via fieldbus interfaces such as PROFINET, EtherNet/IP™, or EtherCAT®.

- Perform a threat and risk analysis. Develop and implement a state-of-the-art remote access concept based on it. Threats must be taken into account, and unauthorized access must be prevented.
- To reduce the risk of unintentional changes to parameters, activate the parameter lock if available on the device.

4.2 Recommendations for decentralized installation

The products for decentralized installation are intended for use in the field.

Check whether the following guidelines must be taken into account when the products are used in your system.

4.2.1 Recommendations for local access

- The room in which the devices are operated must be adequately protected against access by unauthorized personnel.
 - Check whether your existing measures (e.g., safety fences) are sufficient.
- The devices themselves can be protected by additional access-restricting housings. Observe the installation specifications for the individual devices.
- Access must only be possible for qualified personnel, for example via keys, key cards, biometric features, or special tools for access.
- Remove operator panels from the product after use.
- Safely store operator panels separately from the product.
- Access to operator panels must only be granted to authorized persons, e.g. maintenance personnel.
- To reduce the risk of unintentional changes to parameters, activate the parameter lock if available on the device.

4.2.2 Recommendations for remote access

The creation of zones and the associated network segmentation form the basis for a defense-in-depth strategy. Segment into zones based on the results of the threat and risk analysis and the system conditions.

Remote access can be established, for example, via fieldbus interfaces such as PROFINET, EtherNet/IP™, or EtherCAT®.

- Perform a threat and risk analysis. Develop and implement a state-of-the-art remote access concept based on it. Threats must be taken into account, and unauthorized access must be prevented.
- To reduce the risk of unintentional changes to parameters, activate the parameter lock if available on the device.

5 Software and firmware updates

Software and firmware are updated via various tools such as MOVITOOLS® MotionStudio. If necessary, contact SEW-EURODRIVE Service.

6 Ports and services



For information on the available ports and services of the product, refer to the following documentation: "Ports and services for Wi-Fi- and Ethernet-based communication" manual.

7 Contacting SEW-EURODRIVE

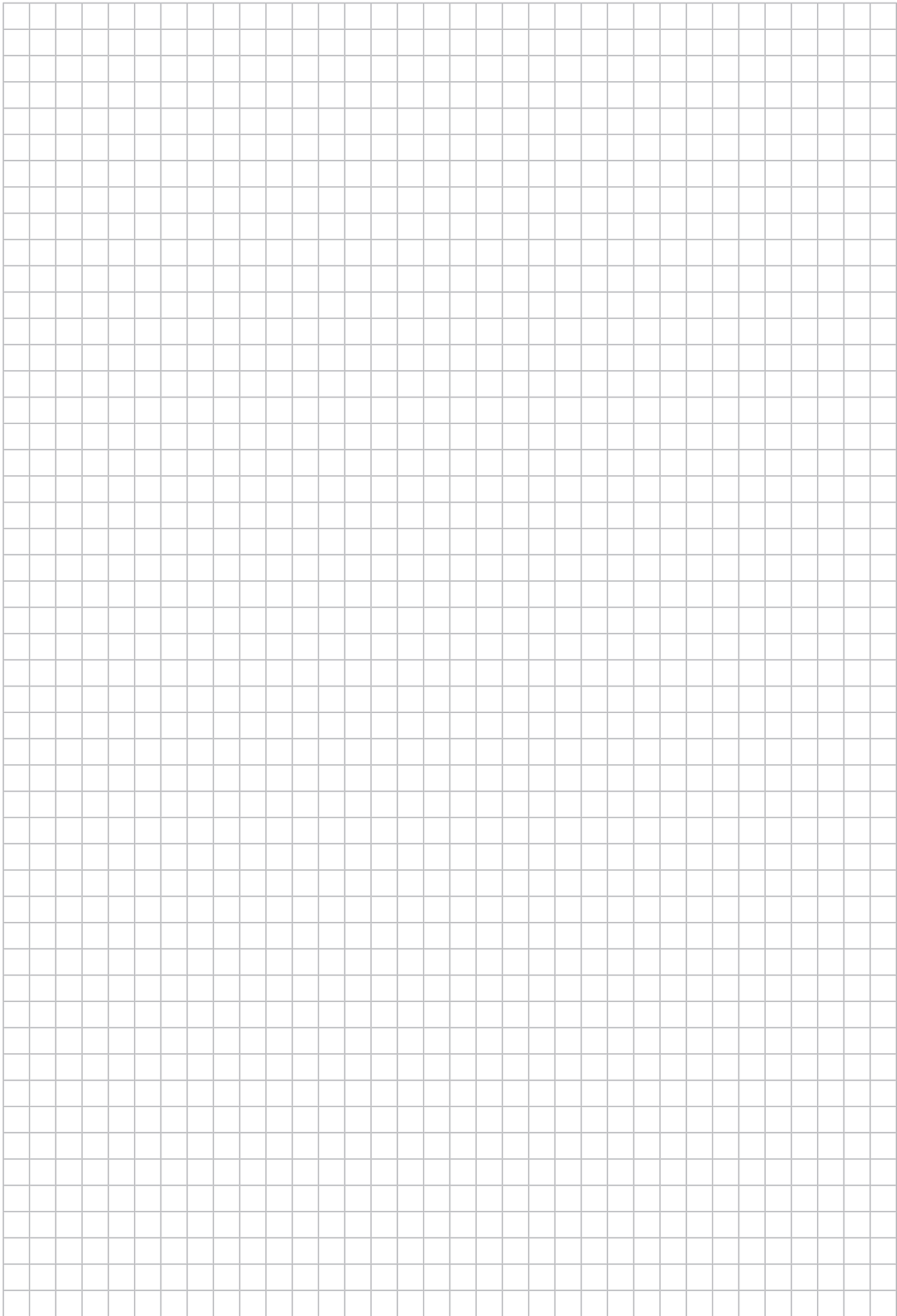
You can find the worldwide contact data and locations on the **SEW-EURODRIVE website** via the following link or the QR code shown below.

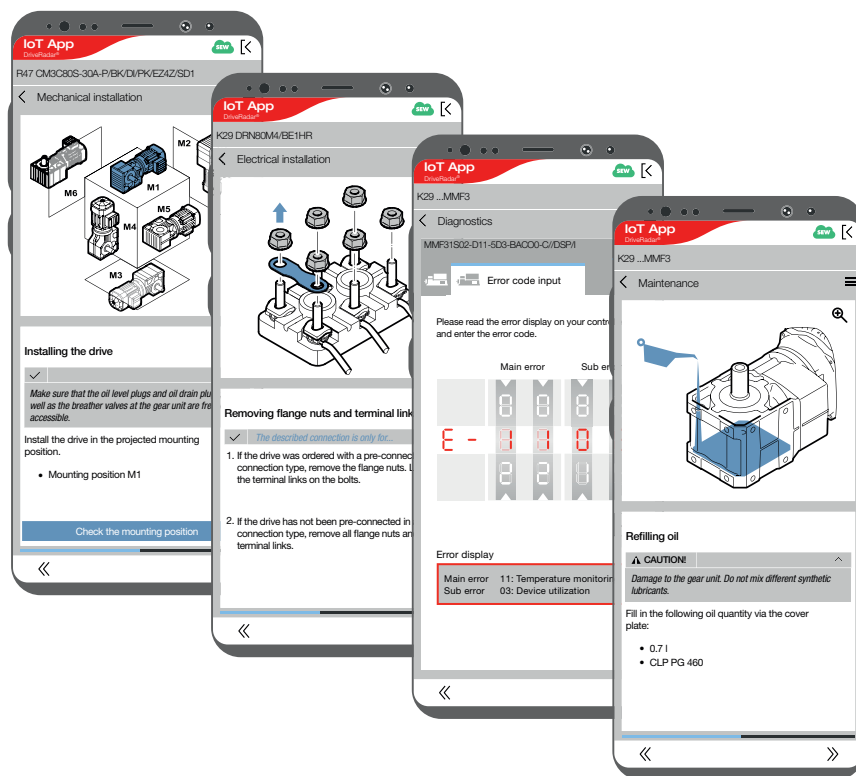
<https://www.sew-eurodrive.de/contacts-worldwide>



SEW
EURODRIVE





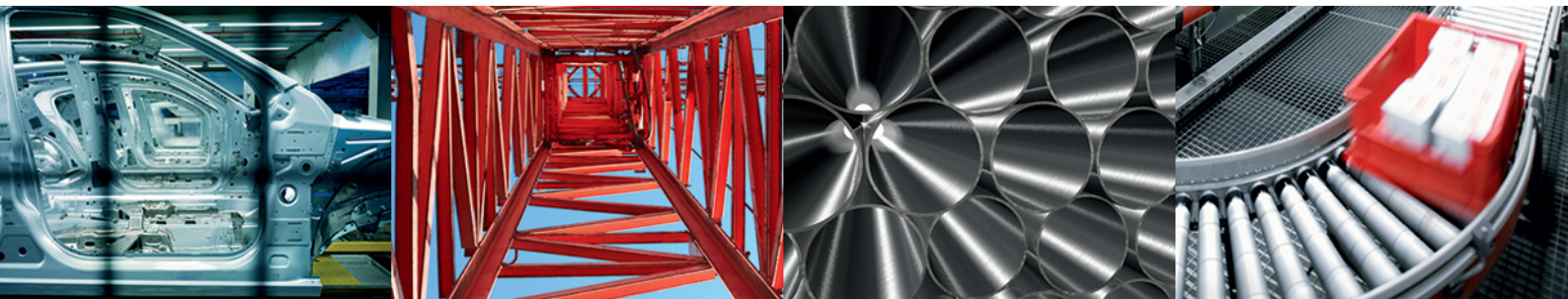


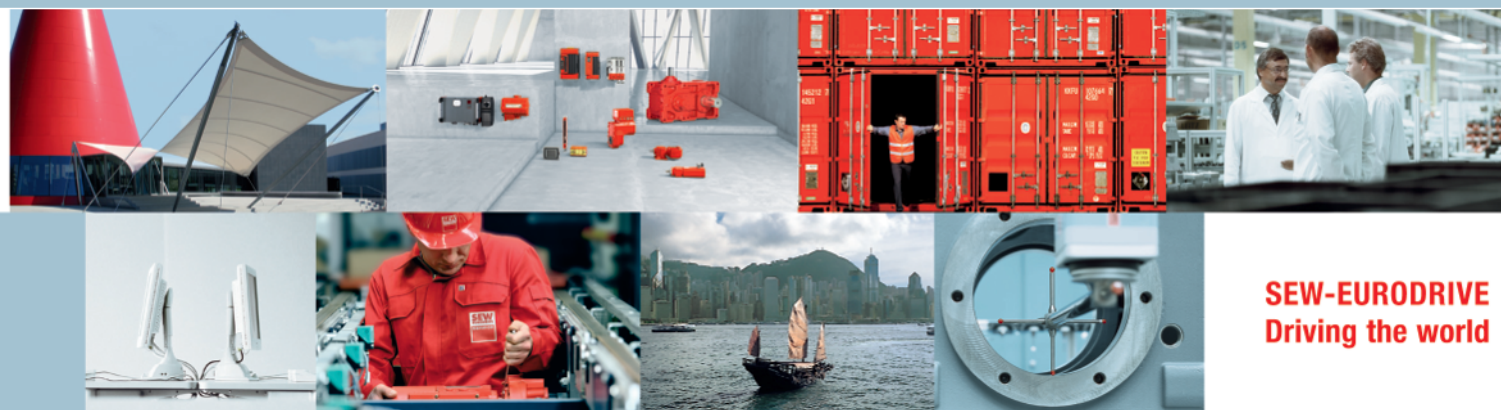
<https://iotapp.io>



THE GREEN SIDE OF DRIVE

Documentation and technical information on your smartphone –
paperless and always available





SEW-EURODRIVE
Driving the world

SEW
EURODRIVE

SEW-EURODRIVE GmbH & Co KG
Ernst-Blickle-Str. 42
76646 BRUCHSAL
GERMANY
Tel. +49 7251 75-0
Fax +49 7251 75-1970
sew@sew-eurodrive.com

→ www.sew-eurodrive.com