



Manual



Cybersecurity best practice for UHX..A and FHX..A type controllers (MOVI-C®)

MOVI-C® CONTROLLER and MOVI-C® FIELD CONTROLLER



Table of contents

1	General information	6
1.1	Contents of this documentation	6
1.2	Other applicable documentation	6
1.3	Additional information	6
1.4	Product names and trademarks	7
1.4.1	Trademark of Beckhoff Automation GmbH	7
1.5	Copyright notice	7
1.6	Products described	7
1.7	Note on additional components	7
1.8	Short designation	7
2	Safety notes	8
2.1	Target group	8
2.2	Contact	8
2.3	Software and firmware updates	8
3	Introduction to cybersecurity	9
3.1	Motivation	9
3.2	Differentiation between safety and security	9
3.3	Measures to maintain security	10
3.3.1	Awareness	10
3.3.2	Good engineering practice	10
3.3.3	Set up trusted zones	11
3.4	Security as a process	11
3.4.1	Identify	12
3.4.2	Protect	12
3.4.3	Detect	13
3.4.4	Respond	13
3.4.5	Recover	13
4	Recommendations for safe operation	14
4.1	General recommendations	14
4.1.1	Network security concepts	14
4.1.2	Access control concepts (use of access control systems)	15
4.2	Requirements for the operating environment	15
4.3	Requirements for the location of use	16
4.4	Compensatory measures	16
4.4.1	M1: Restrict physical access to the product	16
4.4.2	M2: Remove and safely store operator panels	16
4.4.3	M3: Set up access control at system level	16
4.4.4	M4: Introduce password policy at system level	16
4.4.5	M5: Only establish connections to trusted networks	17
4.4.6	M6: Segment the network	17
4.4.7	M7: Treat event data sets at system level	17
4.4.8	M8: Check safety configurations regularly for unwanted changes	17
4.4.9	M9: Protection of unused interfaces	17

4.4.10	M10: Secure remote maintenance systems	17
4.4.11	M11: Use of approved software	18
4.4.12	M12: Backup and restore process	18
4.4.13	M13: Audit log	18
4.4.14	M14: Physical detection of manipulation on the storage medium	18
4.5	Network security and access protection	18
4.5.1	Recommendations for remote access	19
5	UHX..A / FHX..A as motion controller.....	20
5.1	Area of application	20
5.2	Data classification	20
5.3	Protection requirement analysis.....	21
5.4	Network segmentation	21
5.4.1	Motion control application case	22
5.4.2	Conduit	23
5.5	Time synchronization	26
6	Hardening measures.....	27
6.1	External measures – physically secure the device	27
6.2	Basic settings.....	27
6.3	Setting up device user management	27
6.4	Secure communication channels	28
6.5	Controller services and options for protection.....	28
6.6	Encrypt project files.....	31
6.7	Logging	31
6.8	Time synchronization	31
6.9	GPOS – second operating system of the controller	32
7	Configuring the engineering PC	33
7.1	Configuring UEFI/BIOS settings	33
7.2	Securing interfaces	33
7.3	Reducing privileges (principle of least privilege).....	33
7.4	Apply patches in a controlled manner	34
7.5	Using antivirus software	34
7.6	Configuring application whitelisting.....	34
7.7	Ports to be enabled	35
8	Backup and restore.....	36
8.1	Backup	36
8.2	Disaster recovery	36
9	Shutdown and waste disposal	37
9.1	Deleting data on SD/CFast cards	37
9.2	Deleting NVRAM data	37
10	Cybersecurity requirements from the EU Machinery Regulation.....	38
10.1	EU Machinery Regulation	38
10.2	Measures	38
10.2.1	Available technical measures	38
10.2.2	Risk assessment in accordance with ISO 12100.....	38

10.2.3	Physical access protection	39
10.2.4	Digital access protection.....	39
10.2.5	Protect hardware interfaces.....	40
10.2.6	Transparency about installed safety-relevant software	40
10.2.7	Proof of intervention in the software	40
11	Cybersecurity requirements from the EU Data Act	41
11.1	EU Data Act	41
12	Example of motion control user management	42
12.1	Creating a role concept.....	42
12.2	Assets of the controller	43
12.3	User roles.....	44
12.4	Suggested user roles	45
12.5	Suggested access rights for IEC Editor	47
12.5.1	R01 – R07 access rights.....	47
12.5.2	R08 – R013 access rights.....	48
13	Appendix	49
13.1	Assignment of assets/roles	49
	Glossary	51
14	Contacting SEW-EURODRIVE.....	52

1 General information

1.1 Contents of this documentation

This manual describes basic requirements for protecting data and systems from common cyber threats. The measures described are based on established standards and proven recommendations.

At the same time, the manual does not claim to be complete. Depending on the company size, IT infrastructure, regulatory requirements or individual risk situation, additional or alternative security measures may be required.

Cybersecurity measures should be reviewed regularly and adapted to current developments. Specific company-internal specifications must also be observed if necessary.

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

The recommended security measures and best practices apply to the use of MOVI-C® CONTROLLER and MOVI-C® FIELD CONTROLLER as motion controllers in combination with subcomponents of SEW-EURODRIVE below a 3rd-party PLC. The measures serve as guidelines and can be transferred to other application cases involving the MOVI-C® CONTROLLER and MOVI-C® FIELD CONTROLLER and adapted accordingly. SEW-EURODRIVE recommends reviewing further measures on a project-specific basis to achieve a high level of security.

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.

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 Additional information

Observe the following other applicable documentation:

- "MOVI-C® CONTROLLER UHX25A" operating instructions
- "MOVI-C® CONTROLLER UHX45A" operating instructions
- "MOVI-C® CONTROLLER UHX65A" operating instructions
- "MOVI-C® CONTROLLER UHX85A" operating instructions
- "MOVI-C® FIELD CONTROLLER" operating instructions
- "Security options for MOVI-C® CONTROLLER" manual
- "Ports and services for Wi-Fi- and Ethernet-based communication" manual

1.4 Product names and trademarks

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

1.4.1 Trademark of Beckhoff Automation GmbH

EtherCAT® is a registered trademark and patented technology, licensed by Beckhoff Automation GmbH, Germany.



1.5 Copyright notice

© 2026 SEW-EURODRIVE. All rights reserved. Copyright law prohibits the unauthorized reproduction, modification, distribution, and use of this document – in whole or in part.

1.6 Products described

This documentation applies to the following controllers of the MOVI-C® modular automation system:

- MOVI-C® CONTROLLER type UHX86A
- MOVI-C® CONTROLLER type UHX65A
- MOVI-C® CONTROLLER type UHX45A
- MOVI-C® CONTROLLER type UHX25A
- MOVI-C® CONTROLLER type UHX15A
- MOVI-C® FIELD CONTROLLER type FHX25A
- MOVI-C® FIELD CONTROLLER type FHX45A

1.7 Note on additional components

The additional components described in this manual, such as firewalls, virus protection programs, or other IT infrastructure elements, serve exclusively as general technical recommendations for increasing cybersecurity. These components are not included in the scope of delivery of the product.

1.8 Short designation

The following short designations are used in this document.

Type designation	Short designation
Controllers of the MOVI-C® modular automation system (MOVI-C® CONTROLLER and MOVI-C® FIELD CONTROLLER)	Controllers

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.

2.3 Software and firmware updates

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

Observe the following information:

- The contents of the update are published via the corresponding release notes.
- The respective product documentation provides information about the product-specific support period.
- Software updates are not imported automatically. As soon as an update is available, the updates/patches are notified and made available in the respective engineering software.

3 Introduction to cybersecurity

3.1 Motivation

Motivated by the backup of collected and processed data and an increasing number of legal requirements, the need for data security and thus the importance of cybersecurity in the industrial environment (OT) is increasing.

Industrial cybersecurity protection objectives include protection against:

- Loss or manipulation of data or software (e.g. program code)
- Sabotage or standstill of production systems
- Data espionage or resulting consequences

3.2 Differentiation between safety and security

Safety describes the state of freedom from unacceptable risks. In addition to the technical measures for risk reduction, organizational measures must always also be taken into account.

Safety or functional safety

Safety or functional safety refers to the part of the safety of a system that depends on the correct functioning of the safety-related system and other risk-reducing measures. This involves avoiding systematic errors (functional safety management) and reducing and controlling random errors (e.g. component faults that can be reduced or controlled through fail-safe design, the creation of hardware fault tolerances and the use of diagnostics).

Security

Security describes the security with regard to the confidentiality of data, its integrity and availability. In contrast to safety, security usually involves targeted external influences (e.g. hackers). Safety can only be ensured on the basis of correct data. This means that the conditions for safety can only be guaranteed if appropriate security measures have been implemented.

The priority of the above-mentioned protection objectives confidentiality, integrity, and availability depends on the application. In information technology (IT), data confidentiality is usually the top priority; in automation technology (OT), data availability and integrity are usually the top priority.

Data integrity is usually of the utmost importance for meeting the safety requirements.

Technical and organizational measures

Additional (secondary) protection objectives are authentication, authorization, and non-repudiation. Organizational protective measures are supported by technical measures (TOM). Individual consideration is required for all systems to be protected.

3.3 Measures to maintain security

3.3.1 Awareness

Technical measures only work reliably if the workforce has an awareness of security. Standards and publications on security cover this topic in detail. This awareness must be present in all phases, from planning and startup to operation and shutdown.

3.3.2 Good engineering practice

The security principles defined by Viega and McGraw in 2002 are still valid today. The principles presented do not provide 100% protection, but are intended to help achieve 80% of the possible risk reduction with 20% of the effort.

1. **Secure the weakest link.**

Identify and strengthen the weakest link.

Attackers look for easy ways to influence a system and therefore look for the weakest possible point. Secure this weakest link first.

2. **Practice defense in depth.**

Address software risks with layered security solutions.

If a vulnerability is exploited, not the entire system but only a part of it can be affected. The risk for the attacker to be detected increases. In safety engineering, this concept is also referred to as "layers of protection".

3. **Fail securely.**

Make sure that the system will fail in a "secure" manner in the event of a failure.

4. **Follow the principle of least privilege.**

Ensure that only the minimum necessary privileges are granted for the minimum necessary period of time.

What is not explicitly permitted is considered prohibited. If only read access is required, grant only that access.

5. **Compartmentalize.**

Try to limit faults on one part of the system so that they do not affect the rest of the system.

6. **Keep it simple & stupid.**

"KISS" should be balanced with the defense in depth strategy: Transparency, re-use of well-tested components, and the creation of individual controllable data channels ("conduits").

Practice "security by design": Talk to users and take their requirements into account.

7. **Promote privacy.**

Do not disclose unnecessary information. Handle data sensitively.

8. **Remember that hiding secrets is hard.**

Obfuscation through a non-obvious format, such as a binary file, does not provide security. This approach is called "security by obscurity" and is not considered effective.

9. **Be reluctant to trust.**

Manufacturers of security software are not infallible. Even one's own organization should not be trusted unconditionally. If necessary, consult independent third parties.

10. Use your community resources.

Document the measures you implement to meet safety requirements.

If your products and processes withstand independent review, you can assume that they are largely secure.

3.3.3 Set up trusted zones

The formation of zones and the associated separation of networks form the basis of the defense-in-the-depth concept, which is recognized as a central security principle. The degree and specific design of the segmentation into zones should be based on the security risk analysis to be performed and the specific framework conditions of the system.

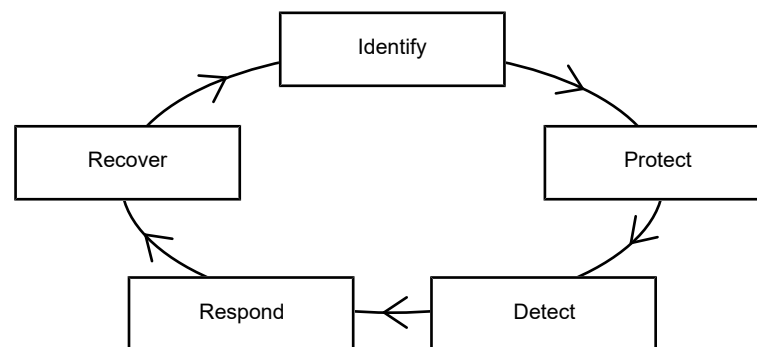
A zone can include several assets and separate certain systems or system parts from each other. IEC 62443 specifies this concept explicitly. If possible, the individual "trusted zones" should only allow transitions (so-called "conduits") to the other zones at one explicitly defined point. These transitions are clearly defined and can be protected accordingly.

For an example, refer to chapter "Network segmentation" (→ 21).

3.4 Security as a process

Constant changes in the security risk require a continuous process to achieve and maintain the required security level. Similar to the continuous improvement process in quality management or functional safety management, security must be actively and continuously maintained. This is best supported by a management system.

The process for reducing security risk can, for example, be divided into the following 5 functions of the "NIST Framework for Improving Critical Infrastructure Cybersecurity":



9007257909354507

After a defined period of time, the disclosure of a threat, or the detection of an incident, the process starts again from the beginning. In addition to maintaining the targeted security level, this also serves to increase the maturity of the process.

Change management must take into account not only the safety properties of the system, but also the security properties of the system.

The cycle shown is an example. You can find more information, for example, in the standards ISO 27000 (ff.), IEC 62443-2-1 and VDI 2182.

For a complete description of the cycle, refer to: <https://www.nist.gov/cyberframework>. In order to simplify the reference to the original, the English terms are also listed below for key terms.

3.4.1 Identify

Which processes and assets need to be protected?

Development of an organizational understanding for managing security risks to systems, people, assets, data, and capabilities.

The activities within the “Identify” function provide the foundation for effective use of the framework.

Organizations must understand the business context and the resources used to deliver critical functions. This understanding helps identify security risks and enables targeted and prioritized implementation of measures in alignment with the organization’s risk management strategy and business requirements.

This results in the following categories:

- Asset management
- Governance
- Risk assessment
- Risk management strategy
- Supply chain risk management

The risk analysis is described in several standards. Helpful references include, for example, IEC 62443-3-2, NA163, ISO 27005, and BSI 200-3.

3.4.2 Protect

What protection mechanisms are available?

Development and implementation of appropriate protective measures to ensure the provision of critical services.

The protection function supports the capability to limit or contain the impact of a potential security event.

This results in the following categories:

- Identity management, authentication, and access control
- Awareness and training
- Data security
- Processes and procedures for information protection (information)
- Maintenance
- Protective technology

Organizational measures

Security measures are not necessarily associated with high investments in security technology or the employment of highly qualified personnel.

The key success factors are well-designed organizational rules and reliable employees who are sensitized to the topic of industrial cybersecurity.

Technical measures

Technical measures support the organizational measures. Multi-layered defense systems (defense-in-depth strategy) are currently recognized as the most efficient measure for risk reduction. Industrial automation systems should have multiple layers of protection.

3.4.3 Detect

What technologies are available to detect incidents?

Development and implementation of appropriate activities to detect the occurrence of a security event.

The Detect function enables the timely detection of security events.

This results in the following categories:

- Anomalies and events
- Security continuous monitoring
- Detection processes

3.4.4 Respond

Which techniques can contain the effects of incidents?

Development and implementation of appropriate activities to take measures in the event of a security incident.

The Respond function supports the capability to contain the impact of a security incident.

This results in the following categories:

- Response planning
- Communications
- Analysis
- Mitigation
- Improvements

3.4.5 Recover

Which techniques can restore operations and capabilities?

Development and implementation of appropriate activities to maintain and restore capabilities or services that have been impaired by a security incident.

The "Recover" function supports the timely restoration of normal operations to reduce the impact of a security incident.

This results in the following categories:

- Recovery planning
- Improvements
- Communications

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.

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 controllers of the MOVI-C® modular automation system differ in their installation location, degree of protection and scope of services:

- The scalable design of the MOVI-C® CONTROLLER allows you to adapt your control to the conditions on site. They comply with degree of protection IP20 and are intended for installation in a lockable control cabinet in dry environments.
- MOVI-C® FIELD CONTROLLER are designed for control applications in factory automation, especially for mechanical and plant engineering. Thanks to their housing with high degree of protection, the controllers can be used flexibly in the field without the need for an additional control cabinet. Refer to the nameplate for the exact degree of protection.

4.1 General recommendations

Employees must regularly be sensitized and trained to the topic of information security. This can prevent, for example, organizational defects or human errors. Recommendations from the Federal Office for Information Security (BSI) can serve as a framework for a concept. For more information, go to <https://www.bsi.bund.de>.

A threat and risk assessment as part of the security management of the systems in which the components described here are used is required to identify the necessary measures for protecting the systems and components. These can go beyond the measures described in this document.

In this context, concepts for network security as well as access control must be evaluated and implemented if necessary. An example list can be found below.

4.1.1 Network security concepts

The following network security concepts are used:

- Network segmentation
- Asset and network management
- Network protection
- Remote access

4.1.2 Access control concepts (use of access control systems)

Establish physical protection by shutting off and monitoring control cabinets and systems. Secure critical components in lockable or alarm-protected areas, supplemented by clear guidelines on the use of third-party data carriers and IT devices. The company premises must be clearly delineated and secured by access controls and binding accompanying regulations for persons outside the company.

4.2 Requirements for the operating environment

The following requirements apply to the environment of the automation system:

- The premises are fenced and closed. A corresponding access concept is available. Information can be obtained from the Federal Office for Information Security (BSI) (INF.1.A7 Site Access Regulations and Control).
- The control cabinet components of the automation solution must be housed in lockable control cabinets. Only authorized personnel may gain access to these components.
- Decentralized components of the automation solution must be accommodated in lockable rooms or fenced areas of the system/machine. Only appropriately authorized personnel may be allowed access to the machines.
- If the decentralized components are not located in lockable areas, access to the components and the associated cabling should be ensured by suitable organizational measures, such as seals, safety screws or locks.

The IT and network infrastructure includes, among other things, PC workstations and server systems that provide administrative functions. For example, the following requirements are placed on the local IT and network infrastructure:

- NTP server for retrieving the system time is provided
- Logging server for storing the event log provided by the components
- If necessary, server for patch and update management
- Maintenance computer with engineering software and central user management, Active Directory with network policy server (NPS)

Maintenance computer

If a maintenance computer is used, SEW-EURODRIVE recommends the following measures:

- Observe the company's internal IT and cybersecurity guidelines.
- When using virus scanners on the maintenance computer, consider the required configuration for operating the engineering software. If this is not the case, check the need for alternative protection methods as part of a risk analysis.
- If virus scanners are used, they must be supplied with the latest virus signatures. An update strategy regarding virus signatures, update cycle, roll-out procedure and corresponding distribution service should be defined and implemented.
- Use multi-factor authentication on the maintenance computer.
- Set up session locks. For example, under [Windows] > [Security Options], activate the "Interactive logon: Machine inactivity limit" check box and enter the required value.

Quarantine PC

A quarantined PC can check storage media for malicious programs as a proxy for the automation solution. For this purpose, employees must be instructed to use storage media (e.g. USB sticks) using the quarantine PC to check for malicious programs before inserting the storage media into the ICS network.

The quarantine PC must have a current patch status of the virus protection programs and must be loaded with the latest malware signatures. In addition to an automated check of the storage media by the quarantine PC, a manual scan for the data medium is also recommended.

4.3 Requirements for the location of use

Rooms and buildings of the automation system must be included in object protection, which ensures monitoring even outside employee attendance hours.

An uninterruptible power supply (UPS) must be installed to bridge a brief power failure or to maintain the power supply until an orderly shutdown of connected systems is possible.

Control cabinets and EDP cabinets containing components of the automation solution must be locked.

4.4 Compensatory measures

The following chapter lists compensation measures that are used for SEW-EURODRIVE devices. Measures that do not apply to controllers, for example because they are only relevant for inverters, are listed but marked as "not relevant".

4.4.1 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, 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.
- Regularly train affected personnel in the use of restricted devices.

4.4.2 M2: Remove and safely store operator panels

This measure is not relevant for MOVI-C® CONTROLLER and MOVI-C® FIELD CONTROLLER.

4.4.3 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.

4.4.4 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.

4.4.5 M5: Only establish connections to trusted networks

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

4.4.6 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.
- Define suitable, controlled transition points between zones (so-called conduits) to create a transparent data flow.

4.4.7 M7: Treat event data sets at system level

This measure is not relevant for MOVI-C® CONTROLLER and MOVI-C® FIELD CONTROLLER.

4.4.8 M8: Check safety configurations regularly for unwanted changes

This measure is not relevant for MOVI-C® CONTROLLER and MOVI-C® FIELD CONTROLLER.

4.4.9 M9: Protection of unused interfaces

- To prevent use, block unused hardware interfaces with physical protection, e.g. a port blocker, port lock or at least with lockable closing plugs or cover caps.
- Only open ports that are required in your firewall. Close all other ports (Principle of Least Privilege).

4.4.10 M10: Secure remote maintenance systems

- Perform a careful risk analysis and adhere to the resulting measures if you use a remote maintenance system.
- Define requirements for trusted networks in advance. Only allow connections to networks that meet the specified requirements. When using an unprotected network or a radio link, measures should be taken as necessary (TOM based on a TRA) to ensure adequate protection.

4.4.11 M11: Use of approved software

- Only use software approved by SEW-EURODRIVE. Obtain the MOVISUITE® engineering software and the MOVIRUN® open Editor installer from Online Support. Check the integrity using the associated hash value¹⁾. Firmware packages and security updates are provided via MOVISUITE® or the MOVIRUN® open Editor installer.
- Only use MOVIKIT® from SEW-EURODRIVE provided in the Online Support.

1) Available in the release notes or via the link from the "Program information" in MOVISUITE®

4.4.12 M12: Backup and restore process

- Establish a backup and restore process to act as quickly as possible in an emergency. Use the backup and restore function of MOVISUITE® for this purpose. Note that not all security settings are saved. For more information, refer to the "Security options for controllers type UHX.. and FHX.. (MOVI-C®)" manual.

4.4.13 M13: Audit log

MOVI-C® CONTROLLER of type UHX..A and MOVI-C® FIELD CONTROLLER of type FHX..A do not have an audit log. If the results of the risk analysis require access logging to these controllers, this must be implemented via external technical or organizational measures.

The controllers support the routing of syslog messages from MR-compliant MOVI-C® inverters in conjunction with the corresponding software from SEW-EURODRIVE, which will be published in a subsequent release. This software allows you to read log data of the inverters.

The operator must ensure the following:

- Provision of a syslog server
- Execution environment of the SEW app/software

4.4.14 M14: Physical detection of manipulation on the storage medium

- Attach your own seals to the device cover or directly to the storage medium or its slot to reliably detect tampering.

4.5 Network security and access protection

A bus system can be used to adapt electronic drive components to the system conditions within wide limits. This entails the danger of a parameter change that is not visible externally resulting in unexpected system behavior, which in turn may impact negatively on operational safety and reliability, system availability, or data security.

Ensure that unauthorized access is prevented, particularly with Ethernet-based networked systems and engineering interfaces.

The use of IT-specific security standards complements access protection to ports and services that are not permanently required.

You can find a port overview in the Online Support in the following documents:

- Manual of the respective device, in chapter "Technical data"
- "Ports and services for Wi-Fi- and Ethernet-based communication - hardware and software" manual

4.5.1 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 is possible via fieldbus interfaces such as PROFINET.

- 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.
- Avoid communication via untrustworthy networks. Ensure sufficient protection when using an unprotected network or a radio link.

5 UHX..A / FHX..A as motion controller

5.1 Area of application

Areas of application of a MOVI-C® CONTROLLER are, for example, the control of a machine or a motion sequence within a system. In this chapter, a MOVI-C® CONTROLLER of type UHX25A with the following properties is used as an example:

- RTOS real-time operating system
- FW08.xx or later

The specifications apply to all MOVI-C® CONTROLLER and MOVI-C® FIELD CONTROLLER with the above-mentioned properties.

5.2 Data classification

Data is collected, processed and exchanged for operating the MOVI-C® CONTROLLER in the motion control role. This data is classified as follows:

Data class	Abbreviation	Description
Configuration Data onBoard	CDO	Configuration data is located on the device.
Configuration Data System	CDS	Configuration data of the inverters is also located on the device.
Log Data Central	LDC	Log data is stored on an external, central log server.
Log Data onBoard	LDO	Log data is only available on the device.
Application Data	AD	Application data is located on the device.
Process Data	PD	Process data is transferred between devices and processed there.
System Data	SD	System data (access data, keys, certificates) is located on the device.
Parameter Data	PAD	Parameter data are changeable values (e.g. minimum, maximum).

Do not save personal data

Observe the following information:

- Personal data is not required for the operation of the system.
- The system is not designed for storing or managing personal data in terms of safety. This does not include access data such as user name and password, see "Setting up device user management" (→ 27).
- Do not use the system in conjunction with personal data. Make sure that no personal data is stored on the device.

5.3 Protection requirement analysis

Different protection objectives are assigned to each data class (→ 20). The protection objectives are classified as follows:

- C = Confidentiality
- I = Integrity
- A = Availability

Integrity and availability of the data in the OT are essential.

In the "motion control" application case, the following protection objectives for the respective data class have been identified:

Data class	Protection objectives	Description
CDO	I, A	Own configuration data is located on the device and is available if required.
CDS	I, A	Configuration data of system components, e.g. inverters, are also located on the device and are available if required.
LDC	C, I, A	Log data can contain confidential information and provide information about (critical) system functions.
LDO		
AD	C, I, A	Applicative characteristic values and application data can contain confidential information (e.g. recipes) and are required for operation.
PD	I, A	Process data is transferred between the devices and processed there and is required for operation.
SD	C, I, A	System data (access data, keys, certificates) is located on the device and is required for operation and communication.
PAD	I, A	Changeable values (e.g. minimum, maximum).

5.4 Network segmentation

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.

Zones can be implemented using routers and VLAN. A zone combines components with common functional, logical, and physical relationships. Communication between components within a zone is already evaluated and, if necessary, secured. Trust limits usually define a zone and thus identify a protected or safe area.

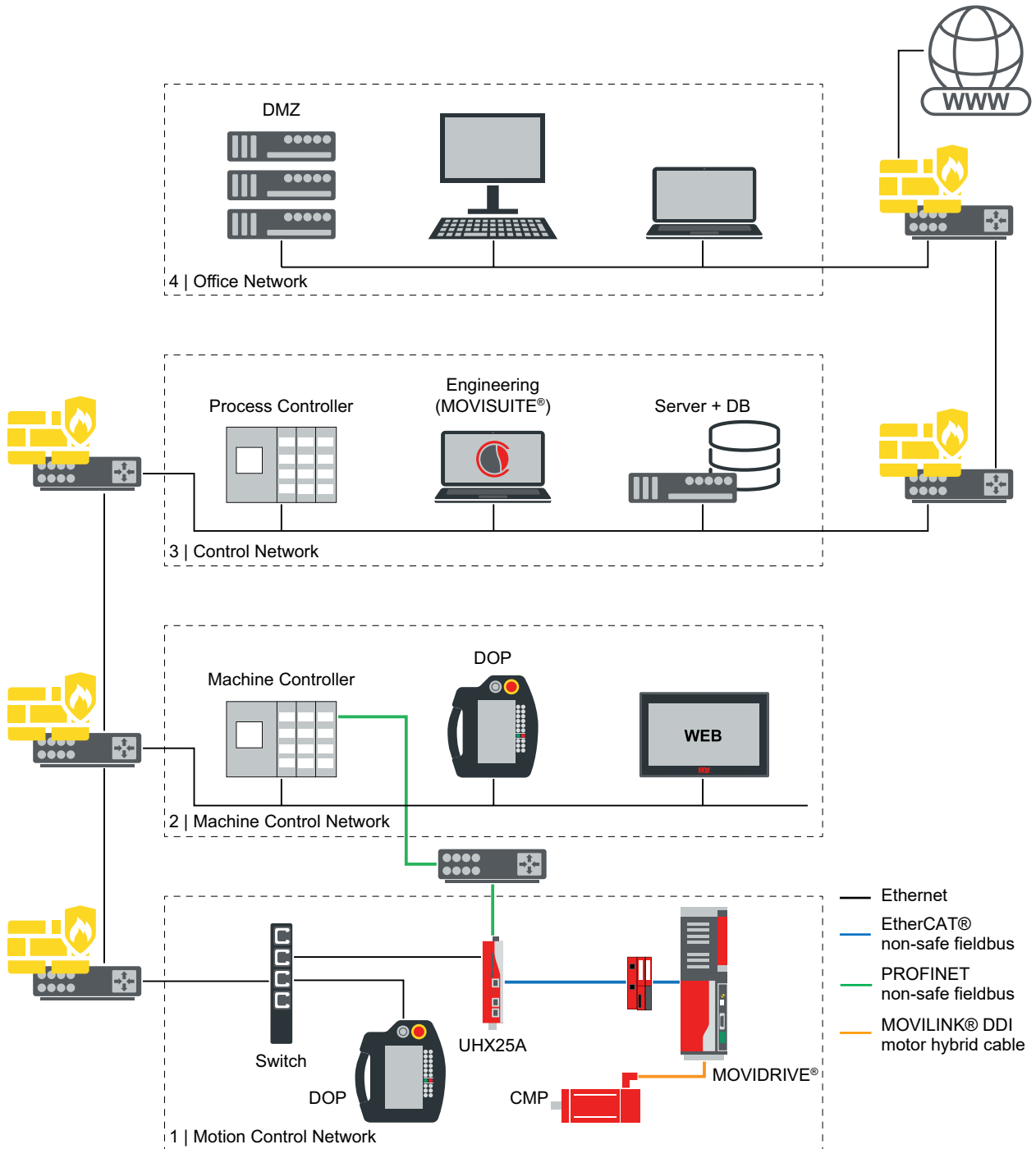
A logical grouping of communication channels with common security requirements that connect 2 or more zones with each other is referred to as "Conduit" (→ 23). Conduits can also be set up in a situation-specific manner (e.g. in case of maintenance).

IEC 62443-4-1/3.1.41 defines zones as a collection of units that depicts the division of a system taking into account the basic functional, logical and physical (including location) relationship.

5.4.1 Motion control application case

In motion control application cases, the MOVI-C® CONTROLLER is used in the machine network as a motion controller for controlling the drives. The overall process is managed and controlled by a higher-level (third-party) controller.

The following figure shows an example of a possible network setup/network segmentation. This must be adjusted based on the respective local conditions, specifications and guidelines.



61538515339

33350418/EN – 04/2026

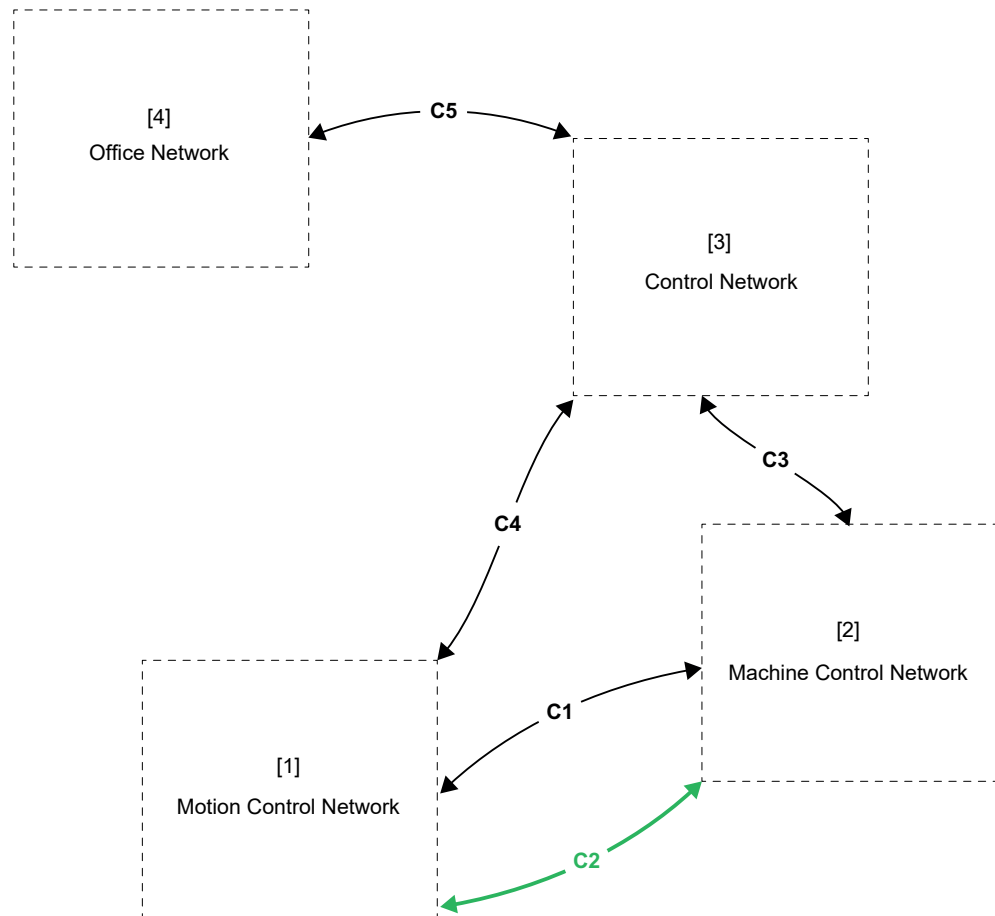
No.	Network level	Description
[1]	Motion Control Network	The motion control level includes all the stations required for the motion control functions as well as directly connected components for system monitoring and control, e.g. web panel for visualization or handheld for teach-in. Tasks for motion control with the MOVI-C® CONTROLLER: • Receiving, processing, and sending process data • Provision of device user management and certificate management • Engineering for motion control (incl. updates and patches)
[2]	Machine Control Network	The control level includes all components for machine control (incl. higher-level control of the machine). Tasks: • Control and monitoring of the overall process of the machine • Providing and sending motion control and process-relevant data for MOVI-C® CONTROLLER • Connection to databases, if necessary
[3]	Control Network	The control and process control level comprises all components for controlling the overall process, connected components for data storage, backup and provision of data to higher-level systems (e.g. SCADA). Tasks: • Control and monitoring of the overall process of a system and adjacent machines • Provision of time synchronization • Connection of databases, if necessary • Control and monitoring of remote access • Provision of maintenance windows and files (updates)
[4]	Office Network	The office network comprises members of the corporate network that require system or process-relevant data (information). Tasks: • Data access/storage on servers within a DMZ: The DMZ can usually be found between the process control level and the office network. • Connection to cloud services, if necessary • System management

5.4.2 Conduit

Data is transferred across zone limits for configuration, startup, diagnostics, maintenance and operation. A logical grouping of communication channels with common security requirements that connect 2 or more zones with each other is referred to as conduit.

In the motion controller application case, the zones of the system network can be connected via the conduits illustrated below.

Furthermore, situation-specific conduits must also be taken into account, e.g. only the ones active in the event of maintenance.



62359509771

The following table shows the transfer of data in the conduits using the example of the motion control application case. Depending on the system, the data may also be transmitted via other channels or fieldbuses.

Con-duit	Data	Description
C1	Configuration Data on-Board (CDO)	• Transfer of the configuration data of the controller via service and maintenance access
	Configuration Data System (CDS)	• Transfer of the configuration data of the inverters via service and maintenance access
	Log Data Onboard (LDO)	• Retrieving saved log information via the IEC Editor or service and maintenance access
	Application data (AD)	• Transfer of the application data to the motion controller via service and maintenance access • Feedback of applicative characteristic values via web visualization
	System data (SD)	• Certificates are updated and retrieved via service and maintenance access
	Parameter data (PAD)	• Applicative parameter data is exchanged during startup and during operation in order to respond to dynamic processes (e.g. adjustment of the tension of the conveyor belt). This is done via service and maintenance access or web visualization.

33350418/EN – 04/2026

Con-duit	Data	Description
C2	Configuration Data on-Board (CDO)	Transfer of the controller configuration data via PROFINET engineering.
	Configuration Data System (CDS)	Transfer of the configuration data of the inverters, for example if a device replacement is automatically loaded onto the subcomponent via PROFINET engineering.
	Log Data Onboard (LDO)	Retrieving saved log information via the IEC Editor via PROFINET engineering.
	Application data (AD)	- Application data is transferred to the motion controller via PROFINET engineering. - Feedback of applicative characteristic values
	Process data (PD)	Process-relevant data and information are exchanged between the motion controller and the higher-level controller
	System data (SD)	Certificates are updated and retrieved via PROFINET engineering
	Parameter data (PAD)	- Transfer of parameter values via one of the following options: - Web visualization - MOVISUITE® (PROFINET routing) - Parameter channel of the process data
C3 ¹⁾	Configuration Data on-Board (CDO)	Transfer of the controller configuration data via PROFINET engineering
	Configuration Data System (CDS)	Transferring the configuration data of the inverters
	Log Data Onboard (LDO)	Retrieving saved log information via the IEC Editor
	Application data (AD)	- Application data is transferred to the motion controller - Feedback of applicative characteristic values
	System data (SD)	Certificates are updated and retrieved
	Parameter data (PAD)	- Transfer of parameter values via one of the following options: - Via web visualization - MOVISUITE® (PROFINET routing) - Parameter channel of the process data

Con-duit	Data	Description
C4	Configuration Data on-Board (CDO)	• Transfer of the controller configuration data via MOVISUITE® engineering PC
	Configuration Data System (CDS)	• Transferring the configuration data of the inverters via MOVISUITE®
	Log Data Onboard (LDO):	• Retrieving saved log information via the IEC Editor
	Log Data Central (LDC)	• Log data is sent to a syslog server
	Application data (AD)	• Application data is transferred to the motion controller • Feedback of applicative characteristic values
	System data (SD)	• Certificates are updated and retrieved
	Parameter data (PAD)	• Transfer of parameter values via one of the following options: – Via web visualization – MOVISUITE®
C5	System data (SD)	• Certificates are updated and retrieved
	Application data (AD)	• Application data is transferred to or returned to the motion controller (e.g. remote maintenance or evaluations of production)

1) This conduit uses PROFINET for engineering purposes.

For information about securing the conduits, refer to chapter "Controller services and options for protection" (→ 28).

5.5 Time synchronization

To use certificate-based encrypted communication, the time of the MOVI-C® CONTROLLER must be correct.

Observe the following information:

- SEW-EURODRIVE recommends operating the time server in the same machine network as the MOVI-C® CONTROLLER.
- If the time server is located outside of the machine network, the port in the firewall may need to be enabled. Incoming port 123 is used by default.
- If the MOVI-C® CONTROLLER also serves as a time server for other network stations, the user-specific port must also be enabled in the firewall.

6 Hardening measures

Observe the following information:

- No local encryption is performed at the operating system level of the UHX..A or FHX..A controller.
- Appropriate measures must be taken to physically access the device, see chapter "External measures – physically secure the device" (→ 27).
- Access to the device via the network must be protected by authentication mechanisms. Functions integrated on the controller can be used for this purpose.

6.1 External measures – physically secure the device

MOVI-C® CONTROLLER and MOVI-C® FIELD CONTROLLER have hardware interfaces (RJ45 and USB). USB ports are only available for the MOVI-C® CONTROLLER, type UHX65A and UHX86A. The MOVI-C® FIELD CONTROLLER also has M12 plug connectors and M16 and M25 cable glands.

Observe the following:

- To prevent use, block unused hardware interfaces with physical protection, e.g. a port blocker, port lock or at least with lockable closing plugs or cover caps.
- Set up a physical access control for the room or control cabinet where the product is located. For example, use robust housings, locks, or safety screws for this purpose.

6.2 Basic settings

You can use the runtime system safety guidelines of the device to make system-wide security basic settings. You have the following options to take device security requirements into account directly during initial startup of the controller:

- Activate encrypted communication. (→ 27)
- Activate the device user management. (→ 28)

Both options can be set up in such a way that they are mandatory for the user. This is called "forced" in the settings.

For a detailed description, refer to the "Security options for controllers type UHX.. and FHX.. (MOVI-C®) firmware V08.01 or later" manual.

6.3 Setting up device user management

Security option: Device user management

Local device user management can be activated on the controller and managed via the engineering tool. Created device users receive defined access permissions and execution permissions for interaction with the device based on assigned roles.

The asset owner (e.g. system operator or system administrator) must be informed about the following changes:

- Device users that are no longer required must be removed by the administrator.

- Passwords that are known to the service provider, no longer secret or at risk must be changed.
- Passwords (e.g. system users) that are no longer required must be changed. This will indirectly delete system access.

For a detailed description, refer to the "Security options for controllers type UHX.. and FHX.. (MOVI-C®) firmware V08.01 or later" manual.

For the motion control application case, possible user roles (groups) were identified and analyzed based on the functions and task areas of these users so that the controller assets could be assigned to these groups. This configuration serves as an extension and finer structure of the user management created as standard. For the tables for the motion control example, refer to chapter "Example of motion control user management" (→ 42).

6.4 Secure communication channels

Security option: Secure channel

As of firmware version 08.01, controllers support encrypted connections to the engineering tool as well as via provided services (OPC UA, MQTT, ..).

Observe the following information:

- Only open the communication interfaces used.
- Secure the communication channels using suitable measures. The controllers offer certificate-based encryption for provided services for example.
- Activate encrypted communication.

Security option: Secure web visualization

Encrypt the communication to the web server (HTTPS) and only allow secure connections to the provided web visualization.

For a detailed description, refer to the "Security options for controllers type UHX.. and FHX.. (MOVI-C®) firmware V08.01 or later" manual.

6.5 Controller services and options for protection

A description of the data classes can be found in chapter "Data classification" (→ 20).

Service/ [port]	Data class	Recommended measures
FTP [X80/X81]	CDO, CDS, AD, SD, PAD	FTP access is deactivated by default: • Use the default setting. • Deactivate FTP after the startup phase at the latest.
Telnet [X80/X81]	CDO, AD, SD	Telnet access is deactivated by default: • Use the default setting. • Deactivate Telnet after the startup phase at the latest. • Implement time synchronization via IEC SNTP libraries.

Service/ [port]	Data class	Recommended measures
Fieldbus [X40]	CDO, CDS, AD, PD, SD, PAD	Operator measures: - Access from external networks or higher-level controllers (e.g. 3rd-party head PLC) must not take place directly on the fieldbus (e.g. separation by firewall) - Physical access protection to the system bus exists. - Secure local hardware fieldbus ports (e.g. via deactivation or use of closable protection covers of unused ports). - The 3rd-party head PLC should check the devices in the fieldbus.
EtherCAT® /SBus ^{plus} [X30]	CDS, LDO, PD, PAD	Operator measures: - External networks must not access the system bus (EtherCAT / SBus^{PLUS}) directly (e.g. separated by firewall or physically with the OT network) - Physical access protection to the system bus exists (e.g. ports in closed control cabinets). - Perform the restart of the system bus as follows: After changing the EtherCAT® structure, the startup must require a check and approval of the appropriately authorized operator. Do not restart automatically. The application developer is responsible for setup.
3S engineering stack [X80/X81], [X40] ¹⁾	CDO, LDO, AD, SD, PAD	Activate device security settings (via IEC Editor): - Activate encryption of communication via the secure channel. - Activate the device user management. Define groups, users, symbol rights, and access rights.
Service data communication (data streaming) [X80/X81] or [X40] ¹⁾	CDO, CDS, LDC, AD, PD, SD, PAD	The following measure only applies to MOVI-C® CONTROLLER types UHX65A and UHX86A: - Only for a VPN connection via GPOS. The motion control example only takes RTOS into account. Operator measure: - Only allow access via data streaming within the trust limits. - Use a firewall to delineate the external trust range. - Operate a permanently installed maintenance computer with MOVISUITE® within the trust range. Only allow access by authorized persons.
Firmware [SD/CFast card]	SD	The following measure only applies to MOVI-C® CONTROLLER types UHX65A and UHX86A. - Only for a VPN connection via GPOS. The motion control example only takes RTOS into account. Operator measures: - Set up a physical access control for the room or control cabinet where the product is located. For example, use robust housings, locks, or safety screws for this purpose. - Only allow authorized and qualified persons to physically access the SD/CFast card.

Service/ [port]	Data class	Recommended measures
IEC application [SD/CFast card]	AD	Activate device security settings (via IEC Editor): • Activate encrypted communication. • Activate the device user management. Define groups, users, symbol rights, and access rights. • Use password-protected and certificate-based project encryption if the project is stored on the memory card. Operator measures: • Set up a physical access control for the room or control cabinet where the product is located. For example, use robust housings, locks, or safety screws for this purpose. • Only allow authorized and qualified persons to physically access the SD/CFast card.
Parameter set on disk [SD/CFast card]	PAD	Activate device security settings (via IEC Editor): • Activate the device user management. Define groups, users, symbol rights, and access rights. Operator measures: • Set up a physical access control for the room or control cabinet where the product is located. For example, use robust housings, locks, or safety screws for this purpose. • Only allow authorized and qualified persons to physically access the SD/CFast card.
CAN stack [X85/X9] ²⁾ A	User-specific	CAN stack access is deactivated by default. By configuring and assigning the telegram, you specify which data (process, parameter, or configuration data) is sent via the telegram. Operator measures: • If the controller is operated in an unsecured network, this must only be done in a safe environment and according to a risk analysis. • Physically protect access to the CAN bus.
SysSock Communication [X80/X81]	LDC, LDS, PD, PAD	Activate device security settings (via IEC Editor): • Use the <code>NetBaseServices</code> CODESYS library for data encryption of TCP/UDP telegrams. The implementation takes place in the IEC program code.
Web server [X80]	PAD	Activate device security settings (via IEC Editor): • Use secure web visualization to communicate certificate-based via HTTPS. • Activate the device user management. Define groups, users, symbol rights, and access rights.
OPC UA server [X80]	LDC, LDS, PD, PAD	Activate device security settings (via IEC Editor): • Activate certificate-based, encrypted communication via OPC UA (currently deactivated by default). • Activate the device user management. Define groups, users, symbol rights, and access rights. • Create a role and a user for OPC UA.

Service/ [port]	Data class	Recommended measures
OPC UA client [X80]	LDC, LDS, PD, PAD	Activate device security settings (via IEC Editor): • Activate certificate-based, encrypted communication via OPC UA (currently deactivated by default). The function is available as of controller firmware 10.x and MOVISUITE® V2.70.2.

1) for fieldbus engineering

2) Only controller type UHX15A, UHX25A, UHX45A or FHX25A, FHX45

6.6 Encrypt project files

Security option: Project encryption

MOVI-C® CONTROLLER and MOVI-C® FIELD CONTROLLER offer the option of storing the IEC project on the controller. The saved project can be encrypted for additional protection.

For a detailed description, refer to the "Security options for controllers type UHX.. and FHX.. (MOVI-C®) firmware V08.01 or later" manual.

6.7 Logging

Access to the controller should be logged. Some components (e.g. WebVisu) generate an entry in the system log of the controller when establishing a connection. You can view the log data from the device in the connected state via the IEC Editor. Alternatively, accesses with higher-level systems can be logged.

For a detailed description, refer to the "Security options for controllers type UHX.. and FHX.. (MOVI-C®) firmware V08.01 or later" manual.

6.8 Time synchronization

Correct time synchronization is required for using the following functions:

- Validation of certificates because their validity periods must be checked.
- Precise timestamps are important in log files in order to clearly assign events, to limit errors and to document safety-relevant processes in a comprehensible manner.

Ideally, the time server is located in the same network zone as the controller to enable direct communication. If the time server is located in another network zone, a corresponding conduit must exist between the zones and the firewall must enable the incoming UDP port 123.

The technical implementation can be carried out, for example, via the CODESYS library "SNTP_Service_SL" from the IoT Libraries SL package. Package V1.5.0.0 or later is integrated in the IEC Editor as of MOVISUITE® V2.30 and MOVI-C® CONTROLLER firmware V07.00.

As of MOVI-C® CONTROLLER firmware version 07.x, the required license is already integrated as standard.

The system time and time zone of the MOVI-C® CONTROLLER and MOVI-C® FIELD CONTROLLER can be set via MOVISUITE®.

For a detailed description, refer to the "Security options for controllers type UHX.. and FHX.. (MOVI-C®) firmware V08.01 or later" manual.

6.9 GPOS – second operating system of the controller

The MOVI-C® CONTROLLER UHX65A and UHX86A can host a 2nd operating system via the RTS hypervisor, which is executed independently of the real-time system for the motion control part. This 2nd operating system can be configured and used for customer-specific application programs and services that are usually run on industrial PCs. The internal virtual LAN interface can be used to communicate between GPOS and RTOS. The following IP addresses are used:

- 192.168.2.1 (RTOS)
- 192.168.2.2 (GPOS)

The following Ethernet ports are available for physically connecting the GPO to networks:

- UHX65A-04
 - X90
- UHX86A
 - X90
 - X91

Deactivate, lock or uninstall all unnecessary services, services and OS components after startup of the Windows part of the controller.

For example, the measures suggested by Microsoft can be performed according to the CIS benchmark to harden the Windows part. Hardening according to level 1 (L1) + BitLocker (BL) was successfully tested without restricting the functionality of the MOVIKIT® Visualization and PLCNode products. For engineering access to MOVIKIT® Visualization, port 11740 must be opened in the Local Group Policy.

SEW-EURODRIVE recommends installing and operating only signed drivers and signed apps from trusted sources on the GPOS. Only establish a connection of the controller outside the local production network after performing a risk analysis of the entire system. The configuration, management and exact settings of the GPOS are the responsibility of the user.

Engineering connection via GPOS

To prevent direct engineering access to the RTOS part, engineering access can be implemented via the Windows part (GPOS) and the internal VNET interface via port forwarding.

The routing and activation of the required ports can be implemented by the user. More detailed information about required ports can be determined via the port list and should only be opened for the duration of engineering access.

7 Configuring the engineering PC

PCs used in automation technology typically cannot be modified during operation, and updates and additional software are difficult to install. Daily updates of virus signatures are rarely possible.

Therefore, the following chapters provide guidance on the secure configuration of a PC using a multi-layered protection concept. Since Windows systems rarely have identical configurations, only typical characteristics can be described.

If your IT organization has established specifications for setting up PC systems, the specifications of your organization must be followed and the information in this chapter must only be considered as advice.

Observe the following information:

- Set up a multi-layered protection concept.
- Secure PCs at regular intervals in accordance with the state-of-the-art.

7.1 Configuring UEFI/BIOS settings

Observe the following information:

- Secure the base software as thoroughly as possible in accordance with the principle of least privilege. Allow only access and functions that are required by the applications.
- Configure the boot order so that the internal hard drive is used first, followed by additional required media.
- Disable all unused interfaces in the UEFI/BIOS, for example wireless, USB, Bluetooth.
- Use UEFI/BIOS passwords where possible.

7.2 Securing interfaces

If interfaces cannot be disabled in the UEFI/BIOS, they must be blocked in the operating system using appropriate measures, for example:

- Enable and configure the Windows Firewall. Access to external media must only be possible with administrator privileges.
- Check all media with a current virus scanner before connecting.
- Only allow the use of approved USB devices and prevent other use by e.g. USB blockers.

7.3 Reducing privileges (principle of least privilege)

One basic idea of protection is to reduce the attack area as much as possible. The rights offered by Windows for the device user must be kept to a minimum by the system administrator.

Observe the following information:

- Enable the Windows screen lock with password protection. Configure the screen lock so that it switches on automatically after a defined time.

- Operate Windows with standard user privileges during daily use. Administrator privileges are only required for installation.
- Since any software can represent a potential vulnerability, SEW-EURODRIVE recommends using only mandatory software on the PC.

7.4 Apply patches in a controlled manner

SEW-EURODRIVE provides updates to the MOVISUITE® engineering software at regular intervals. These include both function updates and security patches.

To ensure smooth transition from the maintenance phase to the operating phase, security patches must be planned within an automation system after successful qualification (compatibility check).

Observe the following information:

- Preferably apply patches, software updates, and signature updates in non-critical situations. Interactions that affect availability and changes in behavior, such as reduced performance, cannot be completely ruled out in advance.
- Carefully check whether connecting the PC to the Internet is actually necessary for patches or updates. Perform a full virus scan after connecting the PC to the Internet.
- Obtain the update only from a trusted source. You can find updates to the MOVISUITE® engineering software in the [SEW-EURODRIVE OnlineSupport](#).
- Check compatibility with the system before applying the update. You can use release notes to identify dependencies that are already required in advance and take any necessary measures.
- If the update is downloaded directly to the engineering PC, protect the connection to the Internet via a firewall and use other suitable protection mechanisms (e.g. website whitelisting, deep packet inspection).

7.5 Using antivirus software

SEW-EURODRIVE recommends using antivirus software that detects malware using signatures and heuristic methods. SEW-EURODRIVE does not recommend any specific antivirus software.

Observe the following information:

- Use security software, such as antivirus programs, and update their signatures regularly.
- Use antivirus software in accordance with your own security policy.

7.6 Configuring application whitelisting

Application whitelisting is a security measure that prevents the execution of unauthorized software. Particularly in environments where regular updates are not possible or not appropriate, application whitelisting provides a complement or an alternative to traditional antivirus software. Application whitelisting is now recognized as equivalent to the use of antivirus software.

Observe the following information:

- Check whether application whitelisting can be used in your environment.
- Use application whitelisting in addition to the operating system's access restrictions.
- Check whether all necessary programs are qualified in application whitelisting to avoid problems in everyday work.

For information on the interfaces and protocols used, refer to the documentation of the respective software so that they are also known to IT network administration.

7.7 Ports to be enabled

In the "Ports and services for Wi-Fi- and Ethernet-based communication - hardware and software" manual, chapter MOVISUITE® lists the ports that must be explicitly enabled for the UHX/FHX engineering software. Additional ports should remain closed or only be enabled depending on the respective intended use of the engineering PC.

8 Backup and restore

8.1 Backup

Save system-relevant data to a separate storage medium. You can save the application program and all controller-relevant data using the MOVISUITE® "Data Backup and Restore" function.

SEW-EURODRIVE recommends using the 3-2-1 strategy for backing up and retaining data. This strategy relates to the creation of 3 backups on 2 different storage media. One backup should be located outside the site to provide maximum protection.

You can export the following data via the IEC Editor:

- Security settings
- Device user management
- Access rights and symbol rights

Installed certificates can be transferred from the controller to the engineering PC via the security screen.

Note that certificates contain device-specific information, such as the device name. If the device name is changed, the affected certificates can no longer be used and must be issued again.

8.2 Disaster recovery

Based on the risk analysis carried out, the system integrator creates a restore process together with the operator. The required process steps are tested and practiced with the persons involved.

To restart the system as quickly as possible in the event of damage, you can trigger the "Data Backup and Restore" function via MOVISUITE® and restore a previously saved data set version.

The device user management and access rights created in the IEC Editor can be imported from a previous backup. If certificates were used but not saved separately, these certificates must be created or issued again based on the system information contained.

If new security patches have been provided since your last backup, check whether an update is required and update your project if necessary before transferring the files back to the controller.

For a detailed description, refer to the "Security options for controllers type UHX.. and FHX.. (MOVI-C®) firmware V08.01 or later" manual.

9 Shutdown and waste disposal

The data on the device must be securely deleted before the device is disposed of or sent to a recycling process. Select a safe deletion procedure for data classified as relevant for IT security.

For a detailed description, refer to the product manual of the respective controller.

9.1 Deleting data on SD/CFast cards

To delete saved data on the SD or CFast card without destroying it, a low-level formatting (LLF) can be performed. This type of formatting completely deletes the map and creates new sectors on it. LLF creates a physical format that determines where your data is stored on the hard disk to be formatted. Unlike high-level formatting, this type of formatting is performed directly on your hard disk sectors.

When formatting a storage medium low-level, the storage areas are highlighted and the start of a recording block and other information are displayed. The internal controller later uses this meta data for all read and write operations.

Suitable tools are available on the Internet, partly as freeware.

Note that after low-level formatting, the SD card can no longer be used with a MOVI-C® CONTROLLER or MOVI-C® FIELD CONTROLLER.

9.2 Deleting NVRAM data

In order to delete stored data in the NVRAM of the controller non-destructively without hardware intervention, the user must ensure that both the retain and retain-persistent memory areas are fully allocated up to the specified maximum capacity and then overwritten with a defined overwrite pattern.

This process reliably makes all data previously stored in NVRAM inaccessible.

10 Cybersecurity requirements from the EU Machinery Regulation

Observe the following information regarding the implementation of the cybersecurity requirements from the EU Machinery Regulation (Regulation 2023/1230, "MR"). All other requirements of the MR apply additionally and are not described here.

10.1 EU Machinery Regulation

The EU Machinery Regulation (Regulation 2023/1230, "MR") sets special requirements on safety components and machines to protect them from corruption.

The described device does not integrate a safety component. MOVI-C® CONTROLLER and MOVI-C® FIELD CONTROLLER do not have integrated safety subfunctions. In their task as e.g. motion controllers, they forward unprocessed functional safety data from a higher-level fieldbus protocol to a lower-level inverter or I/O module.

The devices provide cybersecurity functions for protecting the software and data. These functions make it easier for you to integrate the devices into MR-compliant systems. Depending on the results of the risk assessment, you must take additional organizational measures to protect the systems.

10.2 Measures

The following chapter supports you in fulfilling MR-relevant requirements for your system based on organizational measures and technically available functions of the controllers. In order to meet the cybersecurity requirements of the MR, the implementation of technical and organizational measures to protect the components is transferred to the machine manufacturer.

Observe the following:

- Perform a risk assessment and risk minimization of the machine according to ISO 12100. Take into account the mentioned functionality and the possibility of corrupting the transferred data.

10.2.1 Available technical measures

MOVI-C® CONTROLLER and MOVI-C® FIELD CONTROLLER support security functions that you can activate as of firmware version V08.01.

- Set up certificate-based encrypted communication (e.g. engineering, OPC UA, ...).
- Activate device user management.
- Set up project encryption (certificate/password).
- Set up secure web visualization to web server (HTTPS).

10.2.2 Risk assessment in accordance with ISO 12100

Sample measure	Description	Completed
Perform risk assessment and risk minimization according to ISO 12100.	–	

10.2.3 Physical access protection

Sample measure	Description	Completed
Secure the company premises, e.g. with fences and plant protection.	"M1" (→ 16)	
Include rooms and buildings of the automation system in object protection, which ensures monitoring even outside employee attendance hours.	–	
Secure control cabinet components in lockable control cabinets.	"Requirements for the location of use" (→ 16)	
Secure decentralized components in lockable rooms or fenced areas.	"Requirements for the operating environment" (→ 15)	
Train authorized persons for possible hazards and raise awareness of the effects of manual intervention.	–	

10.2.4 Digital access protection

The following technical and organizational measures support protection against corruption of your system.

Organizational measures

Sample measure	Description	Completed
Set up access control at system level	"M3" (→ 16)	
Introduce password policy at system level	"M4" (→ 16)	
Monitor the network. Only establish connections to trusted networks.	"M5" (→ 17)	
Segment the network and apply a defense-in-depth strategy.	"M6" (→ 17)	
Secure remote maintenance systems	"M10" (→ 17)	
Use of approved software	"M11" (→ 18)	
Backup and restore process	"M12" (→ 18)	
Audit log	"M13" (→ 18)	
Physical detection of manipulation on the storage medium	"M14" (→ 18)	

Available technical measures on the controller (via the IEC Editor)

Sample measure	Description	Completed
Set up certificate-based encrypted communication (e.g. engineering, OPC UA, ..)	"Secure communication channels" (→ 28)	
Activate device user management.	"Setting up device user management" (→ 27)	
Set up project encryption (certificate/password)	"Encrypt project files" (→ 31)	

Sample measure	Description	Completed
Set up secure web visualization to web server (HTTPS)	"Secure communication channels" (→ 28)	

10.2.5 Protect hardware interfaces

Sample measure	Description	Completed
Restrict physical access to the product	"M1" (→ 16)	
Physical protection of unused interfaces	"M9" (→ 17)	
Create audit log	"M13" (→ 18)	
Physical detection of manipulation on the storage medium	"M14" (→ 18)	

10.2.6 Transparency about installed safety-relevant software

Sample measure	Description	Completed
Only use approved software	"M11" (→ 18)	
Set up project encryption (certificate/password)	"Encrypt project files" (→ 31)	

10.2.7 Proof of intervention in the software

Sample measure	Description	Completed
Audit log	"M13" (→ 18)	

11 Cybersecurity requirements from the EU Data Act

MOVI-C® CONTROLLER and MOVI-C® FIELD CONTROLLER are not designed and developed for transporting, storing and processing personal data.

No personal data is required to operate applications on a MOVI-C® CONTROLLER or MOVI-C® FIELD CONTROLLER. If processing of personal data is still required in exceptional cases, the data must be secured by the application developer and the operator using additional external and organizational protective measures.

By default, MOVI-C® CONTROLLER and MOVI-C® FIELD CONTROLLER do not provide device-relevant and application-relevant data outside of MOVISUITE® or the IEC Editor. If you activate and use standardized interfaces such as OPC UA or the web server, these interfaces and provided data must be managed, protected and checked.

The interfaces and the respective data accesses must be activated and configured. SEW-EURODRIVE recommends implementing the latest security measures for access protection when using these interfaces and services.

11.1 EU Data Act

The product offers "Access by Design" for all data generated by the product and thus meets the requirements of the EU Data Act (Regulation 2023/2851):

Storing data	• Data in the product is stored until it is actively deleted or overwritten. • Log and trace data is automatically overwritten in the designated ring buffers as soon as they are full. • Trace data is collected as soon as a trace has been configured and added to the active application. Trace data is stored in memory at runtime and can be exported by the user and saved as a TRACE file on the engineering PC. Depending on the configuration and selected trace duration, collected data is overwritten if the buffer memory is full.
Accessing data	• All data can be read from the product using freely available engineering software from SEW-EURODRIVE or via local interfaces or network connections. HMI systems and external controllers can also access product data according to the active device configuration.
Deleting data	• For information on deleting data, refer to "Shutdown and waste disposal" (→ 37).
Data transmission	• In delivery state, the product does not automatically transfer data to devices in its environment. Depending on the firmware version, you can configure an independent data transmission.
Quality of service	• The device has different qualities of service for data communication: – Cyclic communication to control the device. A few bytes are transferred real-time capably and cyclically. – Acyclic access to all idle data stored on the device. • The response time depends on the communication interface used. • The cycle time is determined by the controlling or requesting device, and is usually between 1 ms and 100 ms. • The quality of service of additionally configured, independent data transmissions depends on their respective configuration.

12 Example of motion control user management

12.1 Creating a role concept

Access rights of a group are assigned based on runtime system objects or file system objects and are inherited from the parent object to the child object below. All members of a group have the same rights.

The following tables show the recommended structural structure of a role concept using the example of motion control:

Table	Description
"Assets of the controller" (→ 43)	This table lists the assets used by the controller. Some of these assets can be protected by access protection settings using the user rights in the IEC Editor.
"User roles" (→ 44)	Various user roles are suggested in this table. You can use these as a basis for creating your own user roles in the IEC Editor.
"Assignment of assets/roles" (→ 49)	The table assigns the roles to the respective required assets. These assets are required for the assigned role to perform its respective tasks.
"Suggested access rights for IEC Editor" (→ 47)	This table shows the relationship between the user rights and the settings in the IEC Editor.

You can use this information to create your own user concept.

12.2 Assets of the controller

The following assets of the MOVI-C® CONTROLLER and MOVI-C® FIELD CONTROLLER are available.

ID	Asset (protocol/function)	Interface	Task
A01	Telnet	X80/X81	Time synchronization without IEC
A02	FTP	X80/X81	(Full) access to the file system of the MOVI-C® CONTROLLER
A03	Fieldbus	X40	Fieldbus and fieldbus engineering
A04	System bus stack	X30	MOVISUITE® access to MOVI-C® CONTROLLER and MOVIDRIVE®
A05	3S engineering stack	X80/X81 X40/X41 X90/X91 ¹⁾	Device user management, diagnostics, debugging and programming, IEC program in general
A06	Service data communication (data streaming)	X80/X81 X40/X41 X90/X91 ¹⁾	Data streaming (currently only unprotected communication is supported)
A07	FW on disk	X80/X81 X40 CFast/SD card	Backup and restore, firmware upgrade/downgrade
A08	IEC application	X80/X81 X40 CFast/SD card	IEC application and code
A09	ParamSet on disk	X80/X81 X40 CFast/SD card	Parameterization of the MOVI-C® CONTROLLER
A10	CAN stack	X85 (UHX..) X9 (FHX..)	Available for UHX15A, UHX25A, UHX45A, FHX25A and FHX45A. The interface is deactivated by default and can only be used after implementation.
A11	Cmp web	X80/X81 X90/X91	Web server and WebVisualization
A12	SysSock	X80/X81 X40	Depending on the IEC implementation
A13	OPC UA	X80/X81	OPC UA communication
A14	Time sync	X80/X81	Time synchronization to a time server via IEC SNTP library functions

1) for MOVIKIT® Visualization

12.3 User roles

The following possible user roles have been defined for the use case of a MOVI-C® CONTROLLER or MOVI-C® FIELD CONTROLLER as motion controller.

ID	Phase	Role/user profile	Description
R01	Operation	Observer (monitoring)	Monitoring of information via an HMI interface
R02	Operation	Operator (operation)	- Operator of a software module, machine or system - Intervention via start, stop of the system - Acknowledgment of known error situations
R03	Operation	Expert operation	- Error correction - Maintenance - Application-specific parameterization - Application-specific optimization
R04	Engineering	Exception to operation	- System intervention - Parameterization with MOVISUITE® and IEC Editor - Error correction
R05	Engineering	IT administration device	- Management of security properties - Device user management setup (users, groups, authorization concepts, certificates) - Network configuration (optional)
R06	Engineering	IT agreements and definition of security measures	- Risk assessment module, machine and systems - Assignment of safety zones (trusted zone) - Remote maintenance concept
R07	Operation	Performance and condition statistics	Statistics on the performance and condition of the modules, machines and systems
R08	Engineering	Startup on-site service	- First startup - Service on site
R09	Engineering	Remote maintenance	- First startup - Service on site
R10	Engineering	Neighboring devices	Establishing communication between "certified" devices and the SEW controller
R11	Operation	DriveRadar®	- Collecting and forwarding data that is relevant to DriveRadar® - Supporting DriveRadar® functions
R12	Engineering	Firmware updates	Standard firmware via MOVISUITE®
R13	Engineering	Product service/repair	Repair of a defective product by an employee of SEW-EURODRIVE

12.4 Suggested user roles

	R01	R02	R03	R04	R05	R06	R07	R08	R09	R10	R11	R12	R13
Device	–	–	–	–	–	–	–	✓	✓	✓	–	–	–
Logger	–	–	✓	–	✓	–	✓	✓	✓	✓	–	✓	–
PlcLogic	–	–	–	✓	–	–	–	✓	–	✓	–	–	–
Application	–	–	✓	✓	–	–	–	✓	✓	✓	–	–	–
__Backup&Re-store__	–	–	–	✓	–	–	–	✓	✓	✓	–	–	–
PlcShell	–	–	–	–	–	–	–	✓	✓	✓	–	–	–
RemoteConnections	–	–	–	–	✓	–	–	✓	✓	✓	–	–	–
OPCUAServer	–	–	–	–	–	–	✓	✓	✓	✓	✓	–	–
Settings	–	–	–	✓	✓	–	–	✓	–	✓	–	–	–
SecuritySettings	–	–	–	–	✓	–	–	✓	–	✓	–	–	–
UserManagement	–	–	–	–	✓	–	–	✓	–	✓	–	–	–
Access Rights	–	–	–	–	✓	–	–	✓	–	✓	–	–	–
Groups	–	–	–	–	✓	–	–	✓	–	✓	–	–	–
Users	–	–	–	–	✓	–	–	✓	–	✓	–	–	–
X509	–	–	–	–	✓	–	–	✓	–	–	–	–	–
CreateCertificateSigningRequest	–	–	–	–	✓	–	✓	✓	–	–	–	–	–
CreateSelfSignedCertificate	–	–	–	–	✓	–	✓	✓	–	–	–	–	–
DeleteCertificate	–	–	–	–	✓	–	–	✓	–	–	–	–	–
ExportCertificate	–	–	–	–	✓	–	–	✓	–	–	–	–	–
ExportPkcs12Key-store	–	–	–	–	✓	–	–	✓	–	–	–	–	–
GetStatus	–	–	–	–	✓	–	✓	✓	✓	–	–	–	–
ImportCertificate	–	–	–	–	✓	–	–	✓	✓	–	–	–	–
ImportPkcs12Key-store	–	–	–	–	✓	–	–	✓	✓	–	–	–	–
ListCertificates	–	–	–	–	✓	–	–	✓	✓	–	–	–	–
ListUseCases	–	–	–	–	✓	–	–	✓	✓	–	–	–	–
MoveCertificate	–	–	–	–	✓	–	–	✓	–	–	–	–	–
/	–	–	–	–	–	–	–	✓	–	–	–	–	–
cert	–	–	–	–	–	–	–	✓	–	–	–	–	–
export	–	–	–	–	–	–	–	✓	–	–	–	–	–
import	–	–	–	–	–	–	–	✓	–	–	–	–	–
DATA	–	–	–	–	–	–	–	✓	–	–	–	–	–

12

Example of motion control user management

Suggested user roles

	R01	R02	R03	R04	R05	R06	R07	R08	R09	R10	R11	R12	R13
Blueprint	–	–	–	–	–	–	–	✓	–	–	–	–	–
config	–	–	–	–	–	–	–	✓	–	–	–	–	–
OPCUAServer	–	–	–	–	–	–	–	✓	–	–	–	–	–
Intermediate	–	–	–	–	–	–	–	✓	–	–	–	–	–
PROJECT	–	–	–	–	–	–	–	✓	–	–	–	–	–
UserMgr	–	–	–	–	–	–	–	✓	–	–	–	–	–

33350418/EN – 04/2026

12.5 Suggested access rights for IEC Editor

Key

Symbol	Meaning
	Access right explicitly granted
	Access right explicitly denied
	Access right neutral, granted through inheritance
	Access right neutral, denied through inheritance
	The access right was not explicitly set or denied, not even in the parent object. Access is not possible.
None	Several objects are selected that do not have uniform access rights.

12.5.1 R01 – R07 access rights

Component/access right	R01	R02	R03	R04	R05, R06	R07
CmpDevice Device	 All	 All	 All	 View  Modify  Other	 All	 View  Other
CmpUserMgr Device.UserManagement	 All	 All	 All	 All	 All	 All
CmpPlcShell Device.PlcShell	 All	 All	 All	 All	 All	 All
CmpApp Device.PlcLogic	 All	 All	 All	 All	 All	 View  Other
Device.PlcLogic .__Backup&Restore	 All	 All	 All	 All	 All	 All
CmpSettings Device.Settings	 All	 All	 All	 All	 All	 All
Device.Settings .SecuritySettings	 All	 All	 All	 All	 All	 All
CmpX509Cert Device.X509	 All	 All	 All	 All	 All	 All
Dateisystem /	 All	 All	 All	 All	 All	 All

Observe the following information:

- R03: Expert operation is used for parameterization via MOVISUITE® and uses the Data Streaming protocol. R03 does not run via a CODESYS device user, but via a system user for automatic code generation of MOVISUITE®.
- R05/R06: The IT administration device user corresponds to the administrator for OT and is also used for IT agreements and the definition of security measures (e.g. TRA, network zone boundaries, remote maintenance concept).

12.5.2 R08 – R013 access rights

Component/access right	R08	R09	R10	R11	R12	R13
CmpDevice Device	 All	 All	 View  Other	 View  Other	 All	 All
CmpUserMgr Device.UserManagement	 View  Modify  Other	 View  Modify  Other	 All	 All	 View  Other	 All
CmpPlcShell Device.PlcShell	 All	 All	 All	 All	 All	 All
CmpApp Device.PlcLogic	 All	 All	 All	 View  Other	 All	 All
Device.PlcLogic .__Backup&Restore	 All	 All	 All	 All	 All	 All
CmpSettings Device.Settings	 All	 All	 All	 All	 All	 All
Device.Settings .SecuritySettings	 All	 All	 All	 All	 All	 All
CmpX509Cert Device.X509	 View  Add_Remove  Other	 View  Add_Remove  Other	 View  Add_Remove  Other	 All	 All	 All
Dateisystem /	 View  Other	 View  Other	 All	 All	 All	 All

13 Appendix

13.1 Assignment of assets/roles

	Telnet	FTP		System bus stack	3S-Engineering-Stack	Data-Streaming	FW on Disc	IEC Application	ParamSet on Disc	CAN Stack	Cmp Web	SysSock	OPC UA	Time Sync
R01 Observer (monitoring)	4	4	2	2	4	2	2	2	2	2	1	2	2	2
R02 Operator (operation)	4	4	2	2	4	2	2	2	2	2	1	2	2	2
R03 Expert operation	4	4	2	2	4	1	2	2	1	2	1	2	2	2
R04 Exception to operation	4	4	2	2	1	1	2	2	1	1	2	2	4	2
R05 IT administration device	4	4	2	4	1	1	1	3	4	4	4	2	1	1
R06 IT agreements and definition of security measures	4	4	4	4	1	3	1	2	4	4	1	4	4	2
R07 Performance and condition statistics	4	4	3	2	2	4	2	2	2	4	4	3	1	2
R08 Startup & on-site service	4	4	1	1	1	1	1	1	1	1	1	1	1	1
R09 Remote maintenance	4	4	1	1	1	1	1	1	1	4	1	1	1	1
R10 Adjacent devices	4	4	1	1	2	2	2	2	3	4	3	1	1	2
R11 DriveRadar®	4	4	3	1	4	1	2	2	2	4	4	4	4	4
R12 Firmware updates	4	4	2	4	1	1	1	4	4	4	4	4	4	4

	Telnet	FTP		System bus stack	3S-Engineering-Stack	Data-Streaming	FW on Disc	IEC Application	ParamSet on Disc	CAN Stack	Cmp Web	SysSock	OPC UA	Time Sync
R13 Product service/re- pair	4	4	1	1	1	1	1	1	1	4	4	4	4	4

Key:

No.	Meaning
1	The asset is actively used and changed by the role.
2	The asset must be active. The asset is only used indirectly by the role. It is not changed. Example: OPC UA data is received and visualized. The role does not access the OPC UA asset directly.
3	The asset can be active. The asset is only used indirectly by the role. Example: The IEC program is always active, even if no role actively accesses it.
4	The asset is not required by the role and is not used.

Glossary

Conduit

Logical grouping of communication channels with common security requirements that connect at least 2 zones.

DMZ

Demilitarized zone. Logically or physically delimited network segment (safety zone) between an internal network and an external network for the isolated provision of services.

Firmware

Software that is embedded into electronic devices and closely coupled with the hardware in terms of functionality. The firmware provides basic control functions and allows the device to start correctly, function correctly, and communicate with other devices.

GPOS (general-purpose operating system)

Windows part of the MOVI-C® CONTROLLER

IT (information technology)

Generic term for all technologies in the context of electronic data processing. It includes, among other things, the use of computers and software for managing, storing, processing, and transferring data.

LLF

Low-level formatting. Process that permanently and irrevocably deletes all data.

NTP server

Server that uses the Network Time Protocol (NTP) to synchronize the clocks of computers and other devices in a network. For this purpose, the server provides the devices with a synchronized timestamp.

OT

Generic term for hardware and software used in industrial and technical environments to control and monitor devices, systems, physical processes, and events

OT network

Network that is configured and optimized for monitoring and controlling certain industrial processes or applications. The network consists of control and monitoring systems and devices (e.g. controllers, sensors, actuators) that are connected to each other by means of communication devices, either via cable or via radio technology, exchange information and share resources.

RTOS (real-time operating system)

Control section of the MOVI-C® CONTROLLER with control program

SCADA system

System for data acquisition, monitoring and control of processes and machines in industrial plants

TOM

Technical and organizational measures. Technical and organizational measures to minimize risk and damage.

TRA

Threat and Risk Analysis. A threat and risk analysis is used to identify, collect and evaluate potential dangers and resulting risks (damage) to a system or component.

VLAN

Virtual Local Area Network. Logical subnetwork.

14 Contacting SEW-EURODRIVE

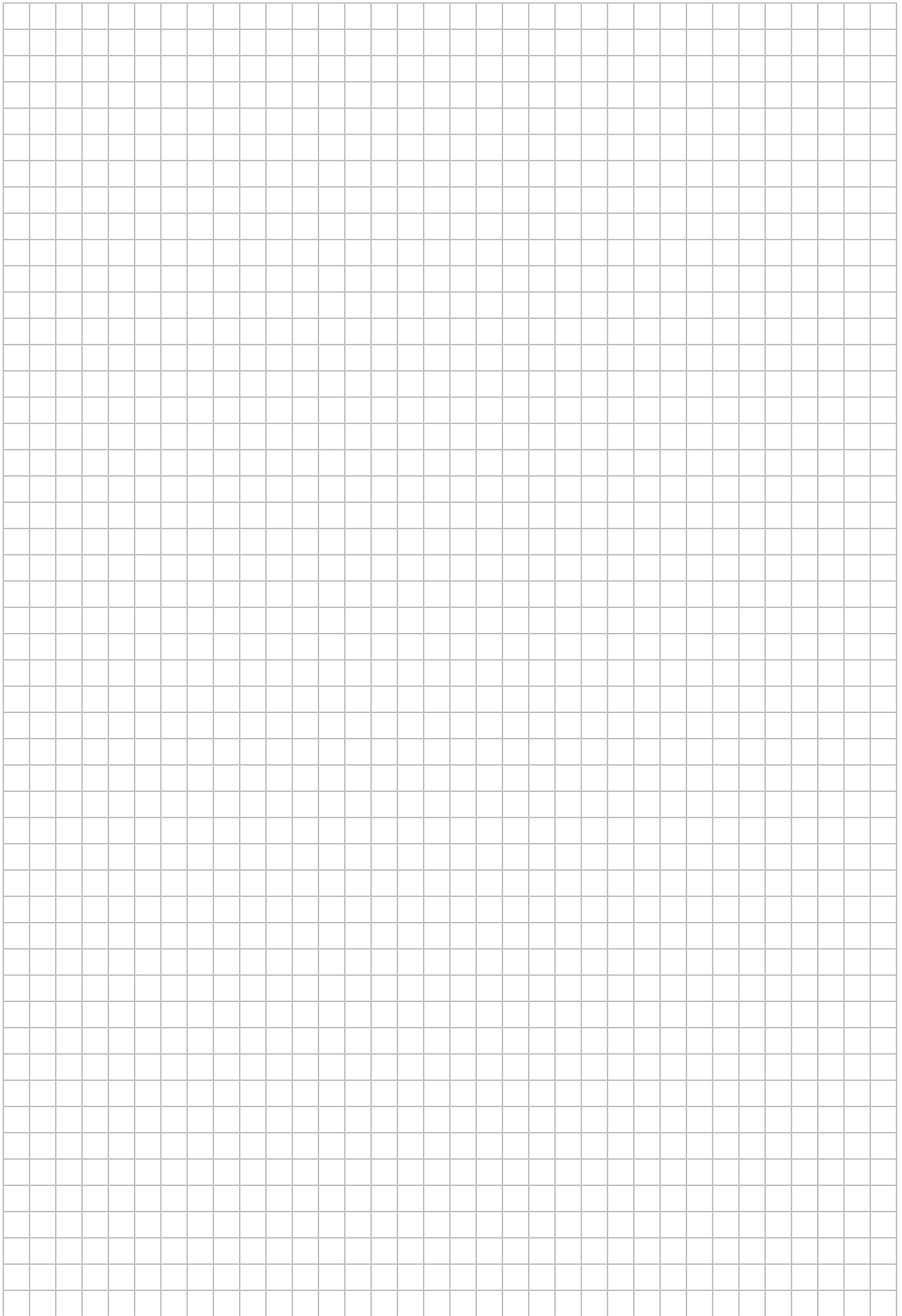
You can find the worldwide contact data and locations on the **SEW-EURODRIVE website** via the following link or the QR code shown below.

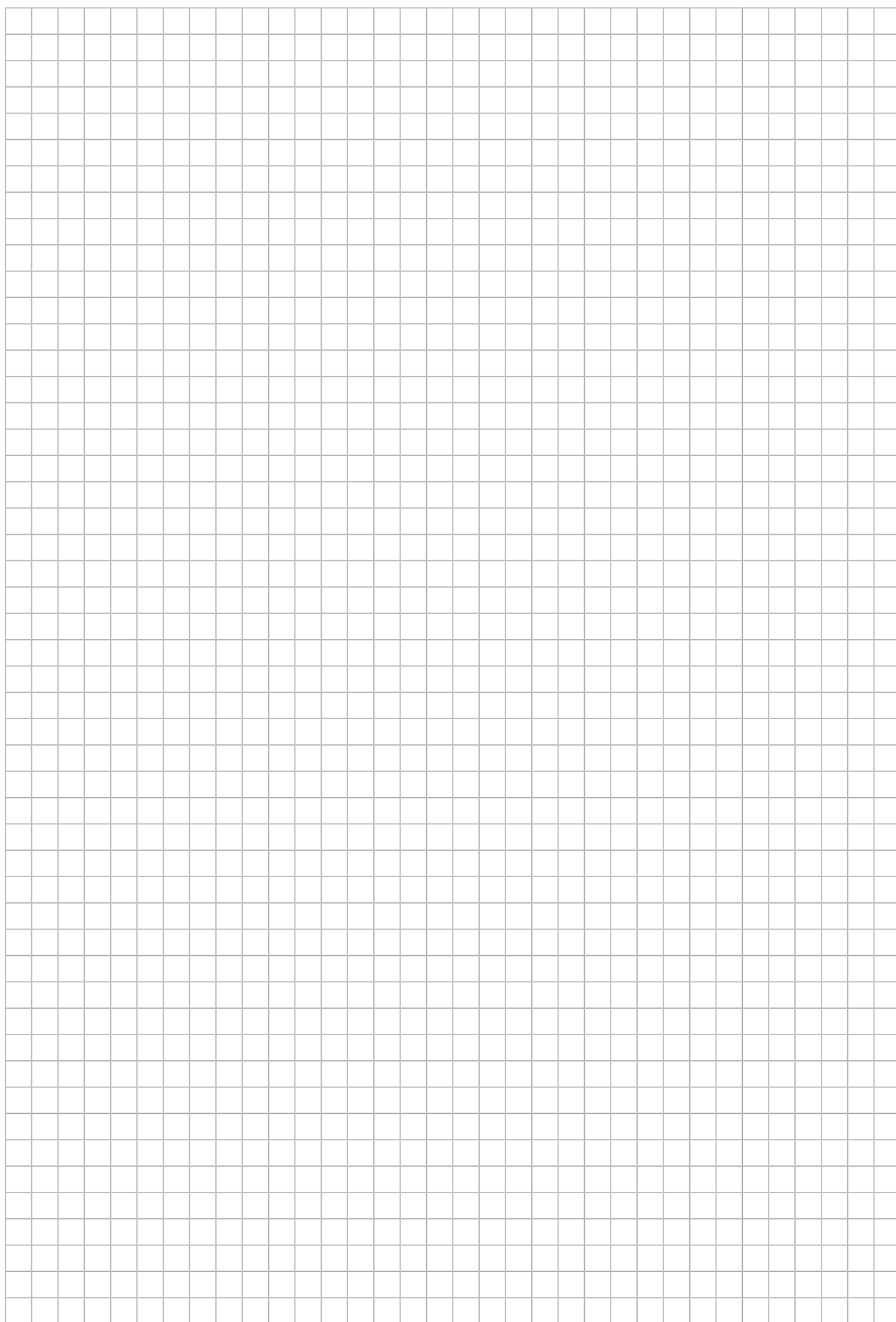
<https://www.sew-eurodrive.de/contacts-worldwide>

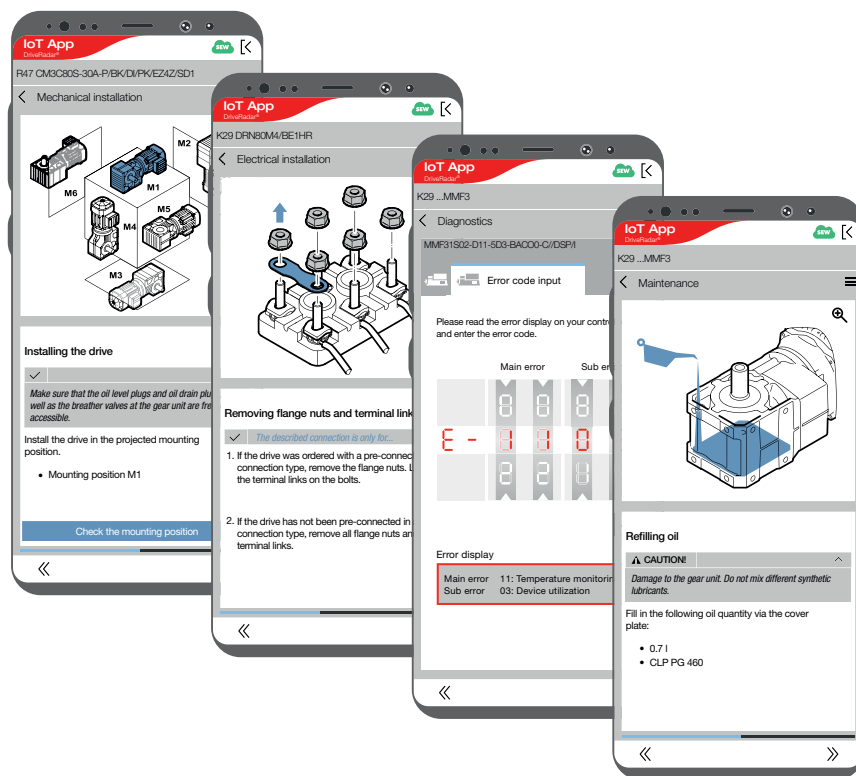


SEW
EURODRIVE







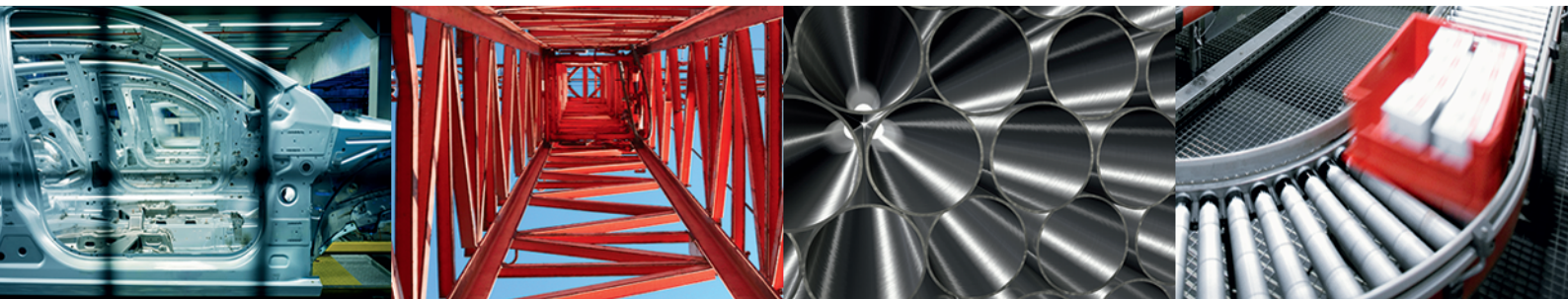


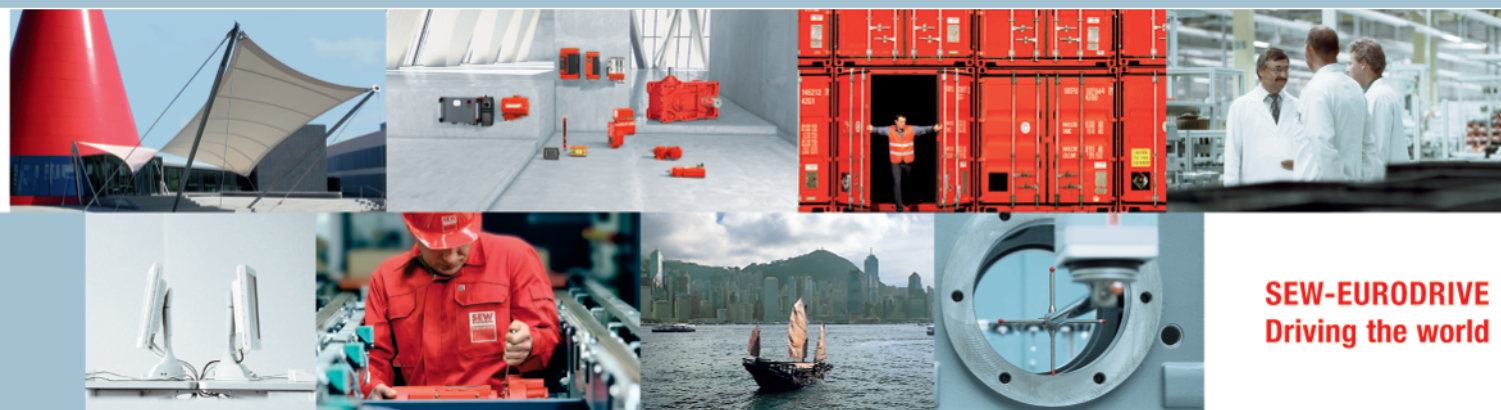
<https://iotapp.io>



**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