Security Advisory 2023-001

As of: Sep 19, 2023

Important Information

System Solutions with MOVI-C® CONTROLLER

in Combination with CODESYS

Edition 09/2023

31554008/EN

Table of Contents

1 Security vulnerabilities in CODESYS products

1.1 Problem

CODESYS GmbH has identified a number of weak points in CODESYS products and published corresponding advisories. Products and system solutions from SEW-EURODRIVE use CODESYS software components and are partially affected by these vulnerabilities.

SEW-EURODRIVE is currently examining with high priority to what extent our products, components, and systems are affected by these vulnerabilities. In the meantime, our customers should immediately ensure that they have implemented the best practices for cyber security in their areas to protect themselves from vulnerabilities. These include, for example, securing all systems with remote access using firewalls. Ensure that unauthorized access is prevented, particularly with Ethernet-based networked systems and engineering interfaces. Use IT-specific safety standards to complement access protection.

1.2 Details

The following table contains the relevant CODESYS Security Advisories. Further information on these vulnerabilities is available in English at the following link: Security Reports (codesys.com). The owners of this website are responsible for the contents and the presentation of the topic.

Advisory-Nummer	Advisory
2023-10	CODESYS Security Advisory 2023-10
2023-09	CODESYS Security Advisory 2023-09
2023-08	CODESYS Development System V3 CODESYS Security Advisory 2023-08
2023-07	CODESYS Development System V3 CODESYS Security Advisory 2023-07
2023-06	CODESYS Development System V3 CODESYS Security Advisory 2023-06
2023-05	CODESYS Control V3 CODESYS Security Advisory 2023-05
2023-04	CODESYS Control V3 CODESYS Security Advisory 2023-04
2023-03	Security update for CODESYS runtime system V3 communication server
2023-02	Security update for CODESYS Control V3
2023-01	Security update for CODESYS Control V3 file access
2022-16	Security update for CODESYS Control V3 communication server
2022-15	Security update for CODESYS V3 boot application encryption
2022-14	Security update for CODESYS V3 Visualization
2022-13	Security update for CODESYS Gateway V2
2022-12	Security update for CODESYS V2 password transport
2022-11	Security update for CODESYS Control V2
2022-10	Security update for CODESYS OPC DA Server V3
2022-09	Security update for CODESYS V3 products containing a CODESYS communication server
2022-08	Security Note: Framework for attacks on ICS and SCADA systems (INCONTROLLER / PIPEDREAM)

Advisory-Nummer	Advisory
2022-07	Security update for CODESYS V3 web server
2022-06	Security update for several CODESYS V3 products containing a CODESYS communication server
2022-05	Security update for CODESYS Control V3 online user management
2022-04	Security update for various CODESYS V3 products using the CODESYS communication protocol
2022-03	Security update for SysDrv3S
2022-02	Security update for CODESYS Control V3 configuration file access
2022-01	Security update for CODESYS PROFINET
2021-18	Security update for CODESYS Git
2021-15	Security update for CODESYS V2 web server
2021-13	Security update for CODESYS Development System V3 including CODESYS Installer and CODESYS SVN
2018-04	Security update for CODESYS V2 and V3 runtime systems

2 Affected products

2.1 Overview of affected products

CODESYS Advisory	Control cabinet controllers					Decentralized controllers		Software[1]		Measure (→ 🗎 9)
	UHX25A	UHX45A	UHX65A	UHX85A	UHX86A	FHX25A	FHX45A	Visualization	IEC-Editor	
2023-10	–	–	–	–	–	–	–	x	x	M16
2023-09	–	–	–	–	–	–	–	x	x	M15
2023-08	x	x	x	x	x	x	x	x	x	M11
2023-07	–	–	–	–	–	–	–	x	x	M12
2023-06	–	–	–	–	–	–	–	x	x	M13
2023-05	x	x	x	x	x	x	x	x	x	M11
2023-04	x	x	x	x	x	x	x	x	x	M11
2023-03	x	x	x	x	x	x	x	x	x	M12
2023-02	x	x	x	x	x	x	x	x	x	M11
2023-01	–	–	–	–	–	–	–	–	–	–
2022-16	x	x	x	x	x	x	x	x	–	M14
2022-15	–	–	–	–	–	–	–	–	–	–
2022-14	x	x	x	–	–	x	x	x	x	M10
2022-13	–	–	–	–	–	–	–	–	–	–
2022-12	x	x	x	x	x	x	x	x	–	M9
2022-11	–	–	–	–	–	–	–	–	–	–
2022-10	–	–	–	–	–	–	–	–	–	M2
2022-09	x	x	x	x	–	x	x	x	x	M7
2022-08	x	x	x	x	x	x	x	x	–	M11
2022-07	x	x	–	x	–	x	x	x	x	M8
2022-06	x	x	x	x	–	x	x	x	x	M7
2022-05	–	–	–	–	–	–	–	–	–	–
2022-04	x	x	x	x	–	x	x	x	x	M7
2022-03	–	–	–	–	–	–	–	–	–	–
2022-02	x	x	x	x	–	x	x	x	x	M6
2022-01	–	–	–	–	–	–	–	–	–	–
2021-18	–	–	–	–	–	–	–	–	–	M2
2021-15	–	–	–	–	–	–	–	–	–	–
2021-13	x	x	x	x	–	x	x	x	x	M5

CODESYS Advisory	Control cabinet controllers					Decentralized controllers		Software[1]		Measure (→ 🗎 9)
	UHX25A	UHX45A	UHX65A	UHX85A	UHX86A	FHX25A	FHX45A	Visualization	IEC-Editor	
2018-04	x	x	–	x	–	–	–	–	x	M3

[1] The IEC Editor is part of MOVISUITE® standard. You cannot download or install the IEC Editor individually. The IEC Editor is only available as part of MOVISUITE® standard. The IEC Editor is not included in MOVISUITE® compact.

2.2 Affected MAXOLUTION® system solutions

- All MAXOLUTION® AGV and mobile assistance systems with VDA5050 interface to the fleet controller also contain a CODESYS control. Depending on the delivery time and update status, the vehicles may be affected by the vulnerabilities listed in chapter "Details" (→ 🗎 4). Chapter "Mobile assistance systems with VDA5050 interface" (→ 🗎 11) provides detailed information and a recommendation for safe operation of the system solution.
- The stationary log controller "Operator terminal PA10005586 18.5 OEM" (part number 28274334) also has a CODESYS control section, which, however, cannot be accessed via a network interface accessible from outside if used according to the documentation. It is not possible to exploit existing weak points in the CODESYS SW components without further ado.
- The "AGV-Basic" automation package and the floor conveyor vehicles created with it and the associated logistics controller (LC) also use a CODESYS control, which, like all other components of the modular automation system, are sold as individual components. For existing CODESYS weak points of the MOVI-C® CONTROLLER, you must therefore proceed according to chapter "Overview of affected products" (→ 🗎 6) and the notes referenced therein in chapter "Product-specific information and measures" (→ 🗎 9).
- MOVIVISION® EMS and skillet applications usually do not contain a CODESYS-based controller and are therefore not affected by the vulnerabilities mentioned in chapter "Details" (→ 🗎 4).

3 General corrective measures

- Unused active network connections generally increase the security risk. Limit network access to the devices to minimize the risk of attacks.
- Unless absolutely necessary, devices/systems should be disconnected from the higher-level network.
- Prevent unauthorized people or devices from gaining access to affected devices and network segments in which affected devices are being operated.
- If you access the devices with a laptop, use a point-to-point Ethernet connection. The laptops should not be connected to the network.

3.1 Network security and access protection

A bus system can be used to adapt electronic drive components to the system conditions within a wide range. This entails the risk of a parameter change not being visible externally, resulting in unexpected – but not uncontrolled – system behavior, and this may impact negatively on operational safety and reliability, system availability or data security.

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

Use IT-specific safety standards to increase access protection to the ports. For a port overview, refer to the respective technical data of the device in use.

3.2 Check the firmware version used

The MOVISUITE® version, the firmware version of the MOVI-C® CONTROLLER and the MOVI-C® FIELD CONTROLLER must always be up to date. You can download the latest MOVISUITE® version free of charge from the SEW-EURODRIVE website. The latest MOVISUITE® version also includes the latest approved firmware versions of the MOVI-C® CONTROLLER and the MOVI-C® FIELD CONTROLLER. For a detailed description of the firmware update process, refer to the operating instructions of the corresponding product.

When starting up new systems, make sure that the latest firmware version is always used. Check the firmware version of the MOVI-C® CONTROLLER and the MOVI-C® FIELD CONTROLLER via MOVISUITE®. If the latest firmware version is not used, update the firmware version.

3.3 Access protection and user management

SEW-EURODRIVE recommends activating and permanently using user management and secure engineering from the security features as of MOVISUITE® version V2.40.

4 Product-specific information and measures

4.1 Components

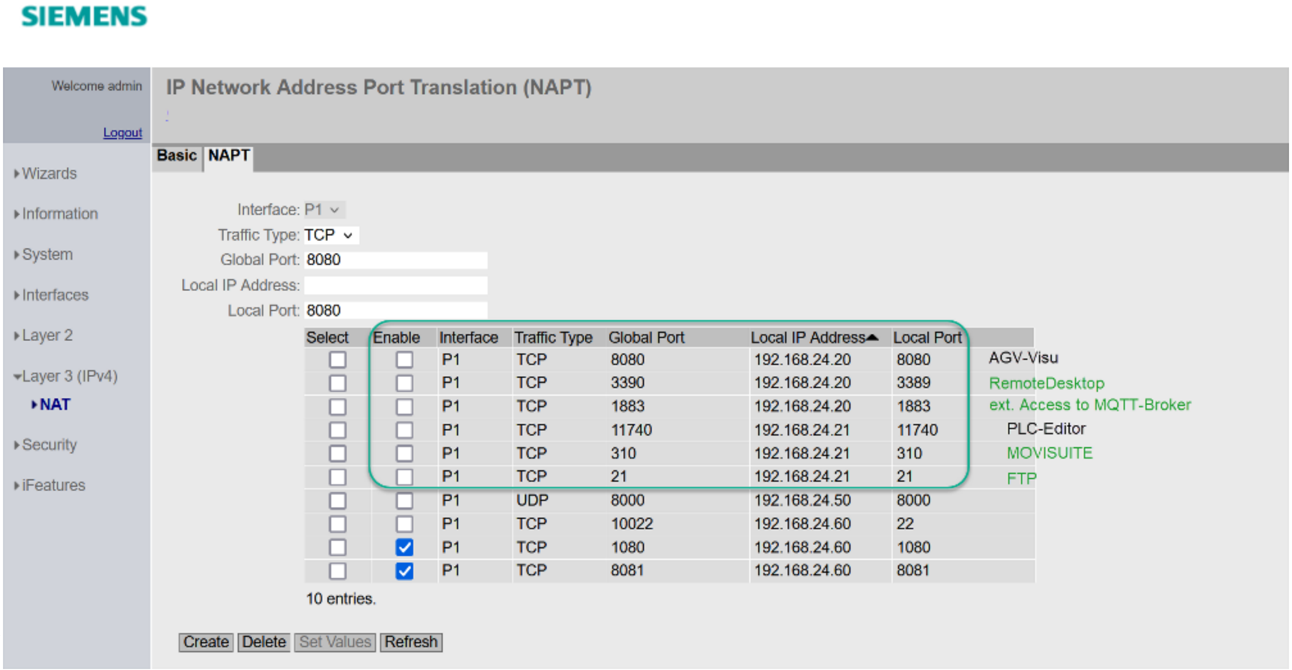
M2	Affected Codesys software components • For Advisory 2022-10: CODESYS OPC DA Server SL • For Advisory 2021-18: CODESYS Git The specified CODESYS software components are not included in the scope of delivery of SEW-EURODRIVE but can be installed as an optional package. In this case, please observe the information in the CODESYS advisory
M3	This only affects the following components: • MOVI-C® CONTROLLER UHX25A, UHX45A with firmware < V02.00 • MOVI-C® CONTROLLER UHX85A with firmware < V03.00 • MOVISUITE® < V2.0.114.100 • IEC-Editor < 3.5.12.3 Check your version of MOVISUITE® and the firmware versions of the MOVI-C® CONTROLLER. Update them, if necessary.
M5	Check your version of MOVISUITE®: • MOVISUITE® < V2.30: Update to MOVISUITE® V2.40 or later. • MOVISUITE® V2.30: A manual update of the CODESYS installer to V1.3.0 is required from the CODESYS website. Alternatively, install MOVISUITE® V2.40 or later.
M6	This only affects the following components: • MOVI-C® CONTROLLER UHX25A, UHX45A, UHX65A, UHX85A with firmware < V08.00 • MOVI-C® FIELD CONTROLLER FHX25A, FHX45A with firmware < V08.00 • MOVISUITE® < V2.40 • IEC-Editor < V3.5.18.20 • Visualization < 1.4 Steps for rectification: • Update MOVISUITE® to V2.40 or later. • Update the MOVI-C® CONTROLLER firmware to V08.00 or later. • Activate the security features that are available as of V2.40. • If you are using the MOVIKIT® Visualization software module, update the IEC Editor to V3.5.18.20 or later and activate the security features. • Set up the appropriate rights for accessing the file system in the "Access rights" tab of the MOVI-C® CONTROLLER in the IEC Editor.

M7	This only affects the following components: • MOVI-C® CONTROLLER UHX25A, UHX45A, UHX65A, UHX85A with firmware < V08.00 • MOVI-C® FIELD CONTROLLER FHX25A, FHX45A with firmware < V08.00 • MOVISUITE® < V2.40 • IEC-Editor < V3.5.18.20 • Visualization < 1.4 Steps for rectification: • Update MOVISUITE® to V2.40 or later. • Update the MOVI-C® CONTROLLER firmware to V08.00 or later. • Activate the security features that are available as of V2.40.
M8	This only affects the following components: • MOVI-C® CONTROLLER UHX25A, UHX45A, UHX85A with firmware < V08.00 • MOVI-C® FIELD CONTROLLER FHX25A, FHX45A with firmware < V08.00 • MOVISUITE® < V2.40 • IEC-Editor < V3.5.18.20 • Visualization < 1.4 The threat exists when web visualization is activated on the MOVI-C® CONTROLLER and in the MOVIKIT® Visualization software module. If you do not need web visualization, please deactivate it. As an alternative, carry out the following steps: • Update MOVISUITE® to V2.40 or later. • Update the MOVI-C® CONTROLLER firmware to V08.00 or later. • Activate the security features that are available as of V2.40. • Update the IEC Editor to V3.5.18.20 or later and activate the security features.
M9	The threat exists in the case of Generation B mixed operation with MOVI-C® CONTROLLER and MOVI-C® FIELD CONTROLLER or when using CODESYS V2.3 legacy products with MOVI-C® CONTROLLER. SEW-EURODRIVE recommends avoiding such mixed operations. If this is unavoidable, observe chapter "General corrective measures" to reduce the risks.
M10	This only affects the following components: • MOVI-C® CONTROLLER UHX25A, UHX45A, UHX65A with firmware < V08.00 • MOVI-C® FIELD CONTROLLER FHX25A, FHX45A with firmware < V08.00 • MOVISUITE® < V2.40 • IEC-Editor < V3.5.18.20 • Visualization < 1.4 The threat exists when web visualization is activated on the MOVI-C® CONTROLLER and in the MOVIKIT® Visualization software module. If you do not need web visualization, please deactivate it. If you use MOVISUITE® V2.30 or V2.31 (IEC Editor 3.5.17.2, MOVI-C® CONTROLLER firmware V07.00 or V07.01), you can manually reinstall CODESYS Visualization V4.2.0.0 in the IEC Editor. As an alternative, carry out the following steps: • Update MOVISUITE® to V2.40 or later. • Update the MOVI-C® CONTROLLER firmware to V08.00 or later. • Activate the security features that are available as of V2.40. • Update the IEC Editor to V3.5.18.20 or later and activate the security features.

M11	Currently under review. To exploit this vulnerability, a successful login must take place on the affected product. User management with strong passwords and secure engineering, which are available as of MOVISUITE® V2.40 for MOVI-C® CONTROLLER and MOVI-C® FIELD CONTROLLER with firmware V08.00 or later, protect against exploiting these vulnerabilities. Also observe the chapter "General corrective measures".
M12	Observe chapter "General corrective measures".
M13	To exploit this vulnerability, the project, project archive or library file must be opened outside of MOVISUITE® or via the standard CODESYS. MOVISUITE® is not affected by the vulnerability because the affected CODESYS plug-in is not used in the MOVISUITE® IEC Editor. Installing MOVISUITE® standard installs a standard CODESYS with a corresponding link for opening project, project archive and library files by double-clicking. Steps for rectification: • Install CODESYS V3.5 SP19 Patch 2 or later. • Do not use CODESYS V3.5 SP18 Patch 2 anymore. • CODESYS V3.5 SP18 Patch 2 must still be installed for MOVISUITE® to function correctly.
M14	If you are working exclusively with MOVISUITE® and code generation: MOVISUITE® generates codesys projects that connect to the MOVI-C® CONTROLLER and MOVI-C® FIELD CONTROLLER via IP addresses. Thus, the node name is irrelevant. The general case of the connection to the controller via the CODESYS IEC Editor as stand-alone is still being processed. To exploit this vulnerability, a successful login must take place on the affected product. User management with strong passwords and secure engineering, which are available as of MOVISUITE® V2.40 for MOVI-C® CONTROLLER and MOVI-C® FIELD CONTROLLER with firmware V08.00 or later, protect against exploiting these vulnerabilities. If the node name has been changed, you can still connect to the controller via the device address or the IP address. After successful authentication, you can set the node name back to the original value.
M15	Currently under review. You can fix the vulnerability manually by updating the CODESYS scripting to version 4.1.0.0 or later using the CODESYS installer. You can find the package on the CODESYS download page.
M16	Currently under review. You can fix the vulnerability manually by downloading and installing the WIBU CodeMeter User Runtime for Windows version V7.60c or later from the company's page. By default, CodeMeter is not configured as a network server if it is installed via MOVISUITE® or the IEC Editor.

4.2 Mobile assistance systems with VDA5050 interface

The vulnerabilities listed in chapters "Security vulnerabilities in CODESYS products" (→ 🗎 4) and "Affected products" (→ 🗎 6) affect the motion controller and the central data transfer controller in the AGV. Both controllers only have to be accessible for engineering access via WLAN and the WLAN client of the assistance system. For the vehicle controller itself, the AGV independently establishes a connection to the stationary MQTT broker via the WLAN client; incoming connections via NATP are not required in normal operation. SEW-EURODRIVE therefore recommends deactivating the entered NATP connections in the WLAN client at least to the two above-mentioned controllers after completion of the engineering work according to the following screenshot.



IP Network Address Port Translation (NAPT)

Interface: P1
Traffic Type: TCP
Global Port: 8080
Local IP Address:
Local Port: 8080

Select	Enable	Interface	Traffic Type	Global Port	Local IP Address▲	Local Port	
□	□	P1	TCP	8080	192.168.24.20	8080	AGV-Visu
□	□	P1	TCP	3390	192.168.24.20	3389	RemoteDesktop
□	□	P1	TCP	1883	192.168.24.20	1883	ext. Access to MQTT-Broker
□	□	P1	TCP	11740	192.168.24.21	11740	PLC-Editor
□	□	P1	TCP	310	192.168.24.21	310	MOVISUITE
□	□	P1	TCP	21	192.168.24.21	21	FTP
□	□	P1	UDP	8000	192.168.24.50	8000	
□	□	P1	TCP	10022	192.168.24.60	22	
□	☑	P1	TCP	1080	192.168.24.60	1080	
□	☑	P1	TCP	8081	192.168.24.60	8081	

10 entries.

9007242587830667

This ensures that the existing weak points cannot be exploited via the (WLAN) network during normal operation of the vehicles. If engineering activities are required, individually required NATP releases can easily be temporarily activated via the web interface in the WLAN client. Since all affected mobile assistance systems are intended for operation in production or assembly halls with limited access, an accidental or even malicious connection to the AGV's LAN connection for downloading malicious software into the vehicles that exploits given weak points is unlikely.

5 General information

5.1 Disclaimer

This document is intended solely to provide information to our customers. The contents have been created with the greatest care, and efforts are made to ensure that they are as up to date as possible. However, SEW-EURODRIVE accepts no liability for the information provided being correct, complete, or up to date. It is published without recognition of any legal obligation.

The proposed corrective measures are for general informational purposes. Whether or to what extent these are applicable to your application environment is subject to your review of the specific conditions on site.

5.2 Product names and trademarks

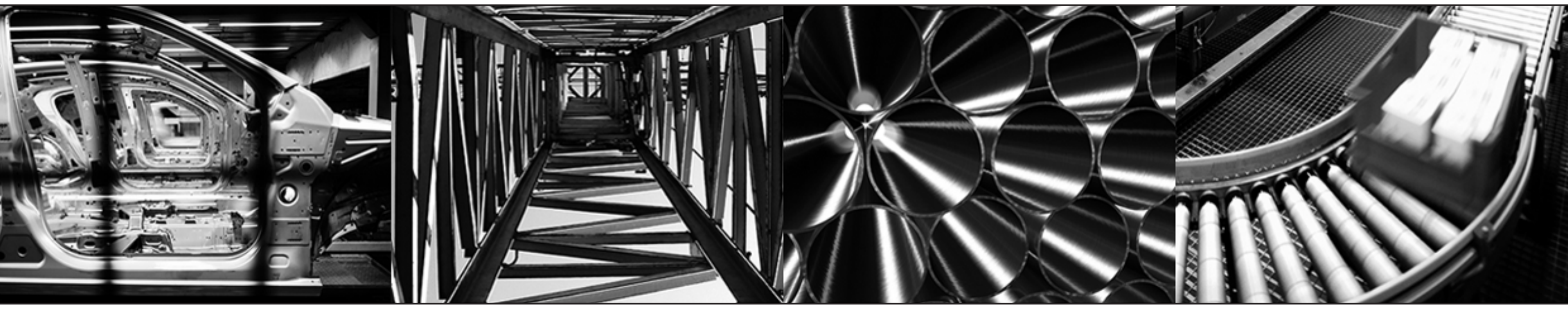
The product names mentioned in this documentation are trademarks or registered trademarks of the respective titleholders.

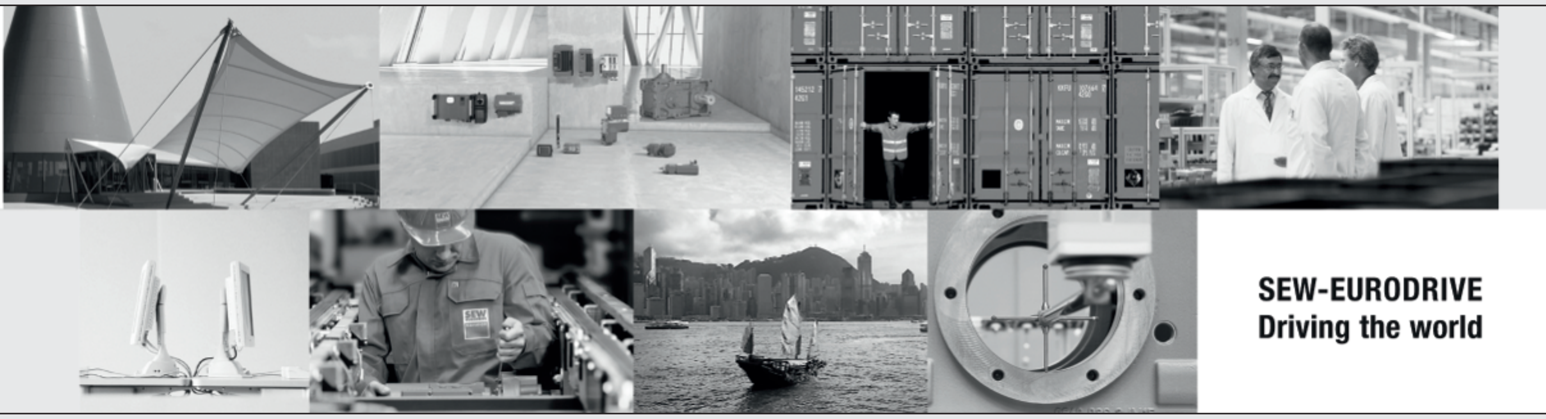
5.3 Copyright notice

5.4 Document history

This customer information is continually updated as new information becomes available, and the most recent version can be found at www.sew.eurodrive.de.

Version	Date of publication	Changes
1	September 19, 2023	Initial document





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**