



Handbuch



Cybersecurity für Umrichter des Automatisierungsbaukastens MOVI-C®

Gültig für Firmwareversionen vor V20.00



Inhaltsverzeichnis

1	Allgemeine Hinweise	4
1.1	Inhalt der Dokumentation	4
1.2	Mitgeltende Unterlagen	5
1.3	Produktnamen und Marken	5
1.4	Urheberrechtsvermerk	5
2	Sicherheitshinweise	6
2.1	Zielgruppe	6
2.2	Kontakt	6
3	Empfehlungen zum sicheren Betrieb	7
3.1	Ausgleichsmaßnahmen	7
3.2	Empfehlungen nach Installationsart	10
4	Erfüllung der Cybersecurity-Anforderungen der EU-Maschinenverordnung (MVO)	13
4.1	Betroffene Geräte	13
4.2	Maßnahmen	13
5	Erfüllung der Anforderungen aus IEC 62443-4-2	15
5.1	Aufbau der Tabellen	15
5.2	FR1 – Identifizierung und Authentifikation (IAC)	15
5.3	FR2 – Nutzungskontrolle (UC)	17
5.4	FR3 – Systemintegrität (SI)	19
5.5	FR4 – Vertraulichkeit der Daten (DC)	20
5.6	FR5 – Eingeschränkter Datenfluss (RDF)	21
5.7	FR6 – Rechtzeitige Reaktion auf Ereignisse (TRE)	21
5.8	FR7 – Verfügbarkeit der Ressourcen (RA)	22
6	Erfüllung der Anforderungen der EU-Datenverordnung	23
7	Software- und Firmware-Updates	24
8	Ports und Services	25
8.1	MOVI-C®: MOVIMOT®, MOVIGEAR®, MOVIPRO®, MOVIDRIVE®, MOVITRAC®	25
9	Ihr Kontakt zu SEW-EURODRIVE	28

1 Allgemeine Hinweise

1.1 Inhalt der Dokumentation

Als Systembetreiber oder -Integrator müssen Sie sicherstellen, dass Ihr System die für den Anwendungsfall relevanten Anforderungen an die Cybersicherheit erfüllt. Mit diesem Handbuch stellt SEW-EURODRIVE Ihnen die zur Bewertung benötigten Informationen zur Verfügung und gibt Empfehlungen zu Härtingsmaßnahmen und Prozessen.

Die vorliegende Dokumentation bündelt security-bezogene Informationen für mehrere Produkte von SEW-EURODRIVE. Sie ergänzt dabei die jeweiligen Betriebsanleitungen und Produkthandbücher, aber ersetzt diese nicht.

Zielgruppe der Dokumentation sind folgende Personengruppen bei Systembetreiber und Systemintegrator: IT-Sicherheitsbeauftragte, Planer, Projektierer und Programmierer von Automatisierungsanlagen sowie Personen, die zu Inbetriebnahme, Betrieb und Wartung der Geräte und Systeme berechtigt sind.

Kenntnisse im Bereich OT-Security und über die relevanten Security-Vorschriften werden vorausgesetzt.

Die Maßnahmen in diesem Dokument dienen der generellen Erhöhung der Cybersecurity und orientieren sich an den Anforderungen für SL 1 auf Systemebene nach IEC 62443. SEW-EURODRIVE garantiert das Erreichen von SL 1 jedoch nicht. Höhere Security Level werden nicht betrachtet.

1.1.1 Beschriebene Produkte

Die vorliegende Dokumentation gilt für folgende Umrichter des MOVI-C® Automatisierungsbaukastens einschließlich der jeweiligen Kommunikationsschnittstellen:

- MOVIDRIVE® modular
- MOVIDRIVE® system
- MOVIDRIVE® technology
- MOVITRAC® advanced
- MOVITRAC® classic
- MOVITRAC® basic
- MOVTRAC® advanced Netzurückspeisung
- MOVIMOT® flexible
- MOVIMOT® advanced
- MOVIMOT® performance
- MOVIMOT® performance ELV
- MOVIDYN®
- MOVIONE®
- MOVIGEAR® performance
- MOVIPRO® technology

1.2 Mitgeltende Unterlagen

Diese Dokumentation ergänzt die Betriebsanleitung des dazugehörigen Produkts. Sie dürfen diese Dokumentation nur in Verbindung mit der Betriebsanleitung verwenden.

Verwenden Sie immer die aktuelle Ausgabe der Dokumentationen und Software.

Auf der Webseite von SEW-EURODRIVE (www.sew-eurodrive.com) finden Sie eine große Auswahl an Dokumentationen in verschiedenen Sprachen zum Herunterladen. Bei Bedarf können Sie die Dokumentationen in gedruckter und gebundener Form bei SEW-EURODRIVE bestellen.

1.3 Produktnamen und Marken

Die in dieser Dokumentation genannten Produktnamen sind Marken oder eingetragene Marken der jeweiligen Titelführer.

1.4 Urheberrechtsvermerk

© 2026 SEW-EURODRIVE. Alle Rechte vorbehalten. Jegliche – auch auszugsweise – Vervielfältigung, Bearbeitung, Verbreitung und sonstige Verwertung ist verboten.

2 Sicherheitshinweise

2.1 Zielgruppe

Angaben zu den Zielgruppen der Produkte entnehmen Sie den jeweiligen Produktdokumentationen.

2.2 Kontakt



SEW-EURODRIVE bietet zum Thema IT-Sicherheit folgende Kommunikationskanäle an:

- Melden Sie Zwischenfälle, die die Cybersecurity betreffen, per E-Mail an cert@sew-eurodrive.com oder über das Kontaktformular auf der Internetseite des Product Security Management (<http://go.sew/psm>).
- Security Advisories finden Sie im Online Support von SEW-EURODRIVE.
 - Um sich über neue und geänderte Security Advisories automatisch informieren zu lassen, abonnieren Sie den Newsletter über die Seite des Product Security Management (<http://go.sew/psm>).
- Wenn Sie Unterstützung bei der Konfiguration benötigen, wenden Sie sich an den Service von SEW-EURODRIVE.

3 Empfehlungen zum sicheren Betrieb

Unberechtigten Zugriffen auf die Produkte kann je nach Systemumgebung auf verschiedene Weise vorgebeugt werden. Der Systemintegrator entscheidet auf Grundlage einer Risiko- und Bedrohungsbewertung, welche Vorkehrungen im konkreten Fall getroffen werden müssen. Die folgenden Kapitel zeigen verschiedene Möglichkeiten auf, die Produkte abzusichern. Mit den Maßnahmen kann in den meisten Fällen ein Sicherheitsniveau in Anlehnung an SL 1 im System erreicht werden.

Generell gilt:

- Reduzieren Sie die Angriffsfläche.
 - Öffnen Sie in Ihrer Firewall ausschließlich Ports, die benötigt werden. Schließen Sie alle anderen Ports (Least-Privilege-Prinzip).
 - Aktivieren Sie während des Betriebs nur die für den Betrieb erforderlichen Dienste.
- Beschränken Sie den Zugang zu Räumen, Schaltschränken und Gehäusen.

3.1 Ausgleichsmaßnahmen

Auf die nachfolgenden Ausgleichsmaßnahmen wird im weiteren Verlauf des Dokuments Bezug genommen, z. B. zur Erfüllung der Anforderungen aus IEC 62443-4-2.

Die Maßnahmen sind nummeriert. Die Nummerierung wird produktübergreifend einheitlich verwendet. Da jedoch nicht alle Maßnahmen für die betrachteten Produkte relevant sind, wurden einzelne Maßnahmen ausgelassen.

3.1.1 M1: Physischen Zugriff auf das Produkt einschränken

- Richten Sie eine physische Zugangskontrolle für den Raum oder Schaltschrank ein, in dem sich das Produkt befindet.
 - Nutzen Sie dazu z. B. robuste Gehäuse, Schlösser oder Sicherheitsschrauben.
- Nur qualifiziertem Personal darf der Zugriff möglich sein, z. B. über Schlüssel, Schlüsselkarten, biometrische Merkmale oder Spezialwerkzeug.

3.1.2 M2: Bediengeräte entfernen und sicher verwahren

- Entfernen Sie Bediengeräte nach der Verwendung vom Produkt.
- Bewahren Sie Bediengeräte getrennt vom Produkt sicher auf.
- Nur befugte Personen, z. B. Instandhaltungspersonal, dürfen Zugang zu Bediengeräten haben.

3.1.3 M3: Zugriffskontrolle auf Systemebene einrichten

- Richten Sie auf Systemebene Zugriffskontrollen ein. Schützen Sie z. B. Engineering-PC und Bedienoberflächen mit Passwörtern.

3.1.4 M4: Passwortrichtlinie auf Systemebene einführen

- Führen Sie eine Passwortrichtlinie ein, die z. B. die Passwortstärke und die Häufigkeit der Passwortänderungen vorgibt.

- Ändern Sie Passwörter gemäß Ihrer Passwortrichtlinie, spätestens jedoch beim Ausscheiden von Mitarbeitenden.
- Vergeben Sie individuelle Passwörter. Verwenden Sie nicht dasselbe Passwort für mehrere Konten.

3.1.5 M5: Verbindungen ausschließlich zu vertrauenswürdigen Netzwerken herstellen

- Definieren Sie vorab Anforderungen für vertrauenswürdige Netzwerke. Lassen Sie ausschließlich Verbindungen zu Netzwerken zu, die die festgelegten Anforderungen erfüllen.

3.1.6 M6: Netzwerk segmentieren

Die Zonenbildung und die damit verbundene Netzwerktrennung bilden die Basis für eine Defense-in-Depth-Strategie. Segmentieren Sie in Zonen auf Grundlage der Ergebnisse der Bedrohungs- und Risikoanalyse und der Anlagengegebenheiten.

- Unterteilen Sie das Netzwerk in kleinere Zonen.

3.1.7 M7: Ereignisdatensätze auf Systemebene behandeln

- Behandeln Sie Ereignisdatensätze zur IT-Sicherheit auf Systemebene.
- Erstellen Sie Ereignisdatensätze beispielsweise in Übereinstimmung mit IEC 62443-4-2. Die Norm fordert folgende Kategorien und Angaben:
 - Geforderte Kategorien: Zugriffskontrolle, fehlerhafte Anfragen, Ereignisse im Automatisierungssystem, Ereignisse bei Sicherung und Wiederherstellung, Konfigurationsänderungen, Ereignisse, die aus dem Ereignisprotokoll hervorgehen
 - Geforderte Angaben: Zeitstempel, Quelle, Kategorie, Art, Ereigniskennung, Ergebnis des Ereignisses

3.1.8 M8: Safety-Konfigurationen regelmäßig auf unerwünschte Änderungen prüfen

- Prüfen Sie die Safety-Konfigurationen in regelmäßigen Abständen auf ungewollte Änderungen. Die Prüfintervalle ergeben sich z. B. aus der Bewertung Ihrer Bedrohungs- und Risikoanalyse (TRA).
 - Änderungen erkennen Sie z. B. daran, dass sich Prüfsummen in den Menüs der jeweiligen Parametrierungssoftware ändern.
 - Änderungen der Daten von Sicherheits-Teilfunktionen (FS-Konfiguration) werden über einen Zähler protokolliert. Dieser Zähler kann ausgelesen und überwacht werden.
 - Jede Änderung von Daten für Sicherheits-Teilfunktionen löscht die "Abnahme"-Markierung im Gerät. Diese Information kann ausgelesen (Parameterdienst und Prozessdaten) und überwacht werden.
- Lesen Sie über MOVISUITE® in regelmäßigen Abständen den Fehlerspeicher des Geräts aus. Im Fehlerspeicher werden u. a. folgende Ereignisse protokolliert:
 - Änderung der Daten für Sicherheits-Teilfunktionen durch einen Download
 - Änderung der Daten für Sicherheits-Teilfunktionen durch einen Restore
 - Änderung der Daten für Sicherheits-Teilfunktionen durch Zurücksetzen auf den Auslieferungszustand/Grundinitialisierung (Decommissioning)
 - Änderung der Software für Sicherheits-Teilfunktionen (Update, Reorganisation)

3.1.9 M11: Nur freigegebene Software einsetzen

- Setzen Sie nur Software ein, die SEW-EURODRIVE freigegeben hat.
- Laden Sie die Software ausschließlich über die offizielle Webseite von SEW-EURODRIVE herunter.
- Achten Sie darauf, dass der Download über eine HTTPS-gesicherte Verbindung erfolgt.

3.1.10 M15: Netzwerkverkehr kontinuierlich überwachen

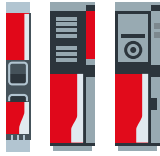
- Überwachen Sie den Netzwerkverkehr kontinuierlich.
- Untersuchen Sie den Netzwerkverkehr auf security-relevante Anomalien.

3.1.11 M16: Hardware- und Softwarestand über ein Asset Management auf unerwünschte Änderungen prüfen

- Stellen Sie durch ein Asset Management sicher, dass die Gerätekonfiguration dem vorgesehenen Hardware- und Softwarestand entspricht.

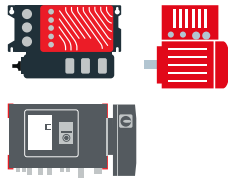
3.2 Empfehlungen nach Installationsart

Spezifische Informationen für die verschiedenen Installationsarten finden Sie in den folgenden Kapiteln:



**Produkte zur Schaltschrank-
installation (Schutzart IP1. oder IP2.)**

Siehe "Empfehlungen bei Installation im Schaltschrank" (→ 10).



**Produkte zur dezentralen Installation
(Schutzart IP5. oder IP6.)**

Siehe "Empfehlungen bei dezentraler Installation" (→ 12).

3.2.1 Empfehlungen bei Installation im Schaltschrank

Die Produkte zur Schaltschrankmontage sind für den Einbau in abschließbare Gehäuse oder Räume vorgesehen.

Prüfen Sie, ob beim Einsatz in Ihrem System die nachfolgenden Richtlinien berücksichtigt werden müssen.

Empfehlungen für den lokalen Zugriff

- Richten Sie eine physische Zugangskontrolle für den Raum oder Schaltschrank ein, in dem sich das Produkt befindet.
- Nur qualifiziertem Personal darf der Zugriff möglich sein, z. B. über Schlüssel, Schlüsselkarten, biometrische Merkmale oder Spezialwerkzeug.
- Entfernen Sie Bediengeräte nach der Verwendung vom Produkt.
- Bewahren Sie Bediengeräte getrennt vom Produkt sicher auf.
- Nur befugte Personen, z. B. Instandhaltungspersonal, dürfen Zugang zu Bediengeräten haben.
- Um das Risiko von unbeabsichtigten Änderungen an Parametern zu verringern, aktivieren Sie die Parametersperre, wenn im Gerät vorhanden.

Empfehlungen für den Fernzugriff

Die Zonenbildung und die damit verbundene Netzwerktrennung bilden die Basis für eine Defense-in-Depth-Strategie. Segmentieren Sie in Zonen auf Grundlage der Ergebnisse der Bedrohungs- und Risikoanalyse und der Anlagegegebenheiten.

Ein Fernzugriff kann z. B. über Feldbus-Schnittstellen wie PROFINET, EtherNet/IP™, EtherCAT®, Modbus TCP oder über andere Kommunikationsverbindungen wie z. B. RS485 oder CAN erfolgen.

- Führen Sie eine Bedrohungs- und Risikoanalyse durch. Entwickeln und implementieren Sie darauf basierend ein Fernzugriffskonzept nach Stand der Technik. Bedrohungen müssen berücksichtigt und unautorisierter Zugriff verhindert werden.
- Um das Risiko von unbeabsichtigten Änderungen an Parametern zu verringern, aktivieren Sie die Parametersperre, wenn im Gerät vorhanden.

- Definieren Sie vorab Anforderungen für vertrauenswürdige Netzwerke. Lassen Sie ausschließlich Verbindungen zu Netzwerken zu, die die festgelegten Anforderungen erfüllen.
- Beachten Sie die Maßnahme "M15" (→  9) Netzwerkverkehr überwachen.

3.2.2 Empfehlungen bei dezentraler Installation

Die Produkte zur dezentralen Installation sind für den Einsatz direkt an verteilten Maschinenteilen oder Anlagenteilen ohne einen explizit geschützten umgebenden Raum vorgesehen.

Prüfen Sie, ob beim Einsatz in Ihrem System die nachfolgenden Richtlinien berücksichtigt werden müssen.

Empfehlungen für den lokalen Zugriff

- Der Bereich, in dem die Geräte betrieben werden, muss ausreichend gegen Zutritt durch nicht autorisiertes Personal geschützt sein.
 - Prüfen Sie, ob Ihre bestehenden Maßnahmen (z. B. Sicherheitszäune) ausreichend sind.
- Die Geräte selbst können durch zusätzliche zugriffsbeschränkende Einhausungen geschützt werden. Beachten Sie dabei die Installationsvorgaben der einzelnen Geräte.
- Nur qualifiziertem Personal darf der Zugriff möglich sein, z. B. über Schlüssel, Schlüsselkarten, biometrische Merkmale oder Spezialwerkzeug.
- Entfernen Sie Bediengeräte nach der Verwendung vom Produkt.
- Bewahren Sie Bediengeräte getrennt vom Produkt sicher auf.
- Nur befugte Personen, z. B. Instandhaltungspersonal, dürfen Zugang zu Bediengeräten haben.
- Um das Risiko von unbeabsichtigten Änderungen an Parametern zu verringern, aktivieren Sie die Parametersperre, wenn im Gerät vorhanden.

Empfehlungen für den Fernzugriff

Die Zonenbildung und die damit verbundene Netzwerktrennung bilden die Basis für eine Defense-in-Depth-Strategie. Segmentieren Sie in Zonen auf Grundlage der Ergebnisse der Bedrohungs- und Risikoanalyse und der Anlagengegebenheiten.

Ein Fernzugriff kann z. B. über Feldbus-Schnittstellen wie PROFINET, EtherNet/IP™, EtherCAT®, Modbus TCP oder über andere Kommunikationsverbindungen wie z. B. RS485 oder CAN erfolgen.

- Führen Sie eine Bedrohungs- und Risikoanalyse durch. Entwickeln und implementieren Sie darauf basierend ein Fernzugriffskonzept nach Stand der Technik. Bedrohungen müssen berücksichtigt und unautorisierter Zugriff verhindert werden.
- Um das Risiko von unbeabsichtigten Änderungen an Parametern zu verringern, aktivieren Sie die Parametersperre, wenn im Gerät vorhanden.
- Definieren Sie vorab Anforderungen für vertrauenswürdige Netzwerke. Lassen Sie ausschließlich Verbindungen zu Netzwerken zu, die die festgelegten Anforderungen erfüllen.
- Beachten Sie die Maßnahme "M15" (→ 9) Netzwerkverkehr überwachen.

4 Erfüllung der Cybersecurity-Anforderungen der EU-Maschinenverordnung (MVO)

Beachten Sie zur Umsetzung der Cybersecurity-Anforderungen aus der EU-Maschinenverordnung (Verordnung 2023/1230, "MVO") die nachfolgenden Informationen. Alle weiteren Anforderungen der MVO gelten zusätzlich und sind hier nicht beschrieben.

4.1 Betroffene Geräte

Betroffene Produkte	Die Cybersecurity-Anforderungen der MVO gelten für Produkte, die nach Inkrafttreten der MVO am 20.01.2027 innerhalb der Europäischen Union in Betrieb genommen oder in Verkehr gebracht werden, sofern mindestens eines der folgenden Kriterien erfüllt ist: - Die Produkte integrieren Funktionen der funktionalen Sicherheit. - Die Produkte verarbeiten oder übertragen mittelbar oder unmittelbar Daten der funktionalen Sicherheit.
Nicht betroffene Gerätetypen	Nicht betroffen von den Cybersecurity-Anforderungen der MVO sind Produkte, bei denen die Sicherheitsfunktionen ausschließlich elektronisch, ohne den Einsatz von Software, realisiert sind. Die Sicherheitsbauteile dieser Produkte sind in ihrer Funktionalität nicht per Software korrumpierbar. Dies gilt z. B. für Produkte mit STO über Klemme.

4.2 Maßnahmen

Um die Cybersecurity-Anforderungen der MVO zu erfüllen, wird die Umsetzung folgender organisatorischer Maßnahmen zum Schutz der Komponenten an den Maschinenbauer und den Betreiber übertragen:

- Führen Sie eine Risikobeurteilung und Risikominimierung der Maschine gemäß ISO 12100 durch.
- Implementieren Sie geeignete technische und organisatorische Maßnahmen, um jeglichen unbefugten Zugriff auf sicherheitsrelevante sowie nicht-sicherheitsrelevante Funktionen zu verhindern, sofern deren Manipulation gemäß Risikobeurteilung zu einer Gefährdung führen kann. Folgende Checklisten zeigen Maßnahmen, die Sie dazu in Betracht ziehen können.

4.2.1 Risikobeurteilung nach ISO 12100

Exemplarische Maßnahme	Beschreibung	Durchgeführt
Risikobeurteilung und Risikominimierung gemäß ISO 12100 durchführen.	–	

4.2.2 Physischer Zugriffsschutz

Exemplarische Maßnahme	Beschreibung	Durchgeführt
Betriebsgelände sichern, z. B. mit Zäunen und Werkschutz.	"M1" (→ 7)	

4 Erfüllung der Cybersecurity-Anforderungen der EU-Maschinenverordnung (MVO) Maßnahmen

Exemplarische Maßnahme	Beschreibung	Durchgeführt
Räume und Gebäude der Automatisierungsanlage in einen Objektschutz einbeziehen, der die Überwachung auch außerhalb der Präsenzzeit von Mitarbeitenden gewährleistet.	–	
Schaltschrankkomponenten in verschließbaren Schaltschränken sichern.	"Empfehlungen bei Installation im Schaltschrank" (→ 10)	
Dezentrale Komponenten in verschließbaren Räumen oder eingezäunten Bereichen sichern.	"Empfehlungen bei dezentraler Installation" (→ 12)	
Zutrittsberechtigte Personen auf mögliche Gefahren schulen und Bewusstsein für die Auswirkungen manueller Eingriffe schaffen.	–	
Bei Geräten mit tauschbarem Speicher, z. B. MOVIDRIVE® technology, MOVIPRO®: Zur Erkennung von Manipulation Siegel auf Blende oder Speicher anbringen.	–	
Bediengeräte entfernen und sicher verwahren.	"M2" (→ 7)	

4.2.3 Digitaler Zugriffsschutz

Exemplarische Maßnahme	Beschreibung	Durchgeführt
Netzwerk segmentieren und Defense-in-Depth-Strategie anwenden.	"M6" (→ 8)	
Netzwerk überwachen. Verbindungen ausschließlich zu vertrauenswürdigen Netzwerken herstellen.	"M5" (→ 8), "M15" (→ 9)	
Zugriffskontrolle auf Systemebene einrichten.	"M3" (→ 7)	
Passwortrichtlinie auf Systemebene einführen.	"M4" (→ 7)	

4.2.4 Weitere Maßnahmen

Exemplarische Maßnahme	Beschreibung	Durchgeführt
Safety-Konfigurationen regelmäßig auf unerwünschte Änderungen prüfen.	"M8" (→ 8) - jeweilige Dokumentation zur funktionalen Sicherheit	
Nur freigegebene Software aus sicheren Bezugsquellen verwenden.	"M11" (→ 9)	

33355924/DE – 05/2026

5 Erfüllung der Anforderungen aus IEC 62443-4-2

Im Folgenden wird angegeben, inwieweit die Produkte die Anforderungen aus IEC 62443-4-2 erfüllen. Außerdem werden Ausgleichsmaßnahmen empfohlen, mit denen bei Integration in ein System ein Sicherheitsniveau angelehnt an SL 1 erreicht werden kann.

Diese Ausgabe des Handbuchs berücksichtigt die Normenfassung von 2019.

5.1 Aufbau der Tabellen

Spalte "Anforderung"

Die angegebenen Anforderungen sind der IEC 62443-4-2 entnommen.

- FR: Grundanforderungen
- CR: technische Anforderungen an die Komponenten
- RE: weitergehende Anforderungen
- EDR: Anforderungen an eingebettete Geräte

Spalte "SL 1"

Gibt an, inwieweit die Anforderungen von Security Level 1 auf Komponentenebene erfüllt werden und ob Ausgleichsmaßnahmen empfohlen werden.

- "✓": Die Anforderung ist erfüllt.
- "+": Die Anforderung ist mit entsprechender Parametrierung erfüllt.
- "o": Die Anforderung wird für das Security-Level nicht gefordert oder ist für das Produkt nicht relevant.
- "–": Die Anforderung wird nicht erfüllt.

Spalte "Empfohlene Ausgleichsmaßnahmen auf Systemebene"

Verweist auf Ausgleichsmaßnahmen, die SEW-EURODRIVE empfiehlt, um die Security auf Systemebene zu verbessern. Das angestrebte Sicherheitsniveau ist an SL 1 nach IEC 62443-3-3 angelehnt.

- "–": Nicht erforderlich.

5.2 FR1 – Identifizierung und Authentifikation (IAC)

5.2.1 Bedeutung der Sicherheitslevel

Die Norm IEC 62443-4-2 definiert Security Level 1 folgendermaßen:

Security Level	Beschreibung
SL 1	Identifizieren und Authentifizieren aller Nutzer (menschliche Nutzer, Softwareprozesse und Geräte) durch Verfahren, die gegen gelegentlichen oder zufälligen Zugriff von nicht authentifizierten Stellen schützen.

5.2.2 Erfüllung der Anforderungen (FR1)

Anforderung	SL 1	Empfohlene Ausgleichsmaßnahmen auf Systemebene
CR 1.1 – Identifizierung und Authentifikation von menschlichen Nutzern	–	"M1" (→ 7), "M2" (→ 7), "M3" (→ 7), "M5" (→ 8), "M6" (→ 8), "M15" (→ 9)

Anforderung	SL 1	Empfohlene Ausgleichsmaßnahmen auf Systemebene
CR 1.1 RE (1) – Eindeutige Identifizierung und Authentifikation	o	–
CR 1.1 RE (2) – Multifaktor-Authentifikation über alle Schnittstellen	o	–
CR 1.2 – Identifizierung und Authentifikation von Softwareprozessen und Geräten	o	–
CR 1.2 RE (1) – Eindeutige Identifizierung und Authentifikation	o	–
CR 1.3 – Nutzerkontenverwaltung	–	"M1" (→ 7), "M2" (→ 7), "M3" (→ 7)
CR 1.4 – Verwaltung der Kennungen	–	"M1" (→ 7), "M2" (→ 7), "M3" (→ 7)
CR 1.5 – Verwaltung der Authentifizierer	–	"M1" (→ 7), "M2" (→ 7), "M3" (→ 7)
CR 1.5 RE (1) – Hardwaresicherheit für Authentifizierer	o	–
CR 1.7 – Stärke der Authentifikation durch Passwörter	–	"M4" (→ 7)
CR 1.7 RE (1) Erzeugung und Lebensdauerbeschränkungen von Passwörtern für menschliche Nutzer	o	–
CR 1.7 RE (2) – Lebensdauerbeschränkungen von Passwörtern für alle Nutzer (menschliche Nutzer, Softwareprozess oder Gerät)	o	–
CR 1.8 – PKI-Zertifikate	o	–
CR 1.9 – Stärke der Authentifikation durch öffentliche Schlüssel	o	–
CR 1.10 – Rückmeldung vom Authentifizierer	–	"M3" (→ 7)
CR 1.11 – Erfolgreiche Anmeldeversuche	–	"M3" (→ 7)
CR 1.12 – Nutzungshinweis des Systems	–	"M1" (→ 7), "M3" (→ 7)
CR 1.14 – Stärke der Authentifikation durch symmetrische Schlüssel	o	–
RE (1) – Hardwaresicherheit für eine Authentifikation durch symmetrische Schlüssel	o	–

5.3 FR2 – Nutzungskontrolle (UC)

5.3.1 Bedeutung der Sicherheitslevel

Die Norm IEC 62443-4-2 definiert Security Level 1 folgendermaßen:

Security Level	Beschreibung
SL 1	Beschränken der Nutzung des IACS (Industrial Automation and Control System) entsprechend den festgelegten Berechtigungen, um vor gelegentlichem oder zufälligem Missbrauch zu schützen.

5.3.2 Erfüllung der Anforderungen (FR2)

Anforderung	SL 1	Empfohlene Ausgleichsmaßnahmen auf Systemebene
CR 2.1 – Durchsetzung der Autorisierung	–	"M1" (→ 7), "M3" (→ 7), "M5" (→ 8), "M6" (→ 8)
CR 2.1 RE (1) – Durchsetzung der Autorisierung für alle Nutzer (menschliche Nutzer, Softwareprozesse und Geräte)	o	–
CR 2.1 RE (2) – Abbildung der Berechtigung auf Rollen	o	–
CR 2.1 RE (3) – Eingriff des Aufsichtspersonals	o	–
CR 2.1 RE (4) – Doppelte Zustimmung	o	–
CR 2.2 – Nutzungskontrolle von Funkverbindungen	o	–
CR 2.3 – Nutzungskontrolle von tragbaren und mobilen Geräten	o ^{1) 2)}	–
EDR 2.4 – Mobiler Code	o ¹⁾	–
EDR 2.4 RE (1) – Authentizitätsprüfung von mobilen Codes	o	–
CR 2.5 – Sitzungssperrung	–	"M3" (→ 7)
CR 2.6 – Beendigung einer Fernzugriffssitzung	o	–
CR 2.7 – Kontrolle gleichzeitiger Sitzungen	o	–
CR 2.8 – Prüfbare Ereignisse	–	"M7" (→ 8)
CR 2.9 – Speicherkapazität für Ereignisdatensätze	–	"M7" (→ 8)
CR 2.9 RE (1) – Warnung, wenn die Speicherkapazität für Ereignisdatensätze erreicht ist	o	–
CR 2.10 – Verhalten bei Verarbeitungsfehlern von Ereignisdaten	–	"M7" (→ 8)
CR 2.11 – Zeitstempel	–	"M7" (→ 8)

Anforderung	SL 1	Empfohlene Ausgleichsmaßnahmen auf Systemebene
CR 2.12 – Nichtabstreitbarkeit	–	"M1" (→ 7), "M3" (→ 7), "M5" (→ 8), "M6" (→ 8)
CR 2.12 RE (1) – Nichtabstreitbarkeit für alle Nutzer	o	–
EDR 2.13 – Nutzung von physikalischen Diagnose- und Prüfschnittstellen	o	–

1) Das Produkt verwendet keinen mobilen Code.

2) Für IEC 62443-3-3 SR 2.3 gibt es keine Anforderungen auf Komponentenebene.

5.4 FR3 – Systemintegrität (SI)

5.4.1 Bedeutung der Sicherheitslevel

Die Norm IEC 62443-4-2 definiert Security Level 1 folgendermaßen:

Security Level	Beschreibung
SL 1	Schützen der Integrität des IACS gegen gelegentliche oder zufällige Manipulation.

5.4.2 Erfüllung der Anforderungen (FR3)

Anforderung	SL 1	Empfohlene Ausgleichsmaßnahmen auf Systemebene
CR 3.1 – Kommunikationsintegrität	– ¹⁾	"M1" (→ 7), "M3" (→ 7), "M5" (→ 8), "M6" (→ 8), "M15" (→ 9)
CR 3.1 RE (1) – Authentifikation der Kommunikation	o	–
EDR 3.2 – Schutz vor Schadcodes	–	"M1" (→ 7), "M3" (→ 7), "M5" (→ 8), "M6" (→ 8), "M11" (→ 9)
CR 3.3 – Verifikation der IT-Sicherheitsfunktionalität	–	Der Systemintegrator muss dem Betreiber Anleitungen zur Prüfung der erforderlichen IT-Sicherheitsmaßnahmen bereitstellen.
CR 3.3 RE (1) – Verifikation der IT-Sicherheitsfunktionalität im laufenden Betrieb	o	–
CR 3.4 – Software- und Informationsintegrität	– ¹⁾	"M1" (→ 7), "M3" (→ 7), "M5" (→ 8), "M6" (→ 8), "M11" (→ 9), "M16" (→ 9)
CR 3.4 RE (1) – Authentizität der Software und der Informationen	o	–
CR 3.4 RE (2) – Automatisierte Meldung von IT-Sicherheitsverstößen	o	–
CR 3.5 – Eingabevalidierung	✓	–
CR 3.6 – Vorbestimmte Zustände der Ausgänge	✓ ²⁾	–
CR 3.7 – Fehlerbehandlung	✓	–
CR 3.8 – Sitzungsintegrität	o	–
CR 3.9 – Schutz von Prüfinformationen	o	–
CR 3.9 RE (1) – Ereignisdatensätze auf nur einmal beschreibbaren Speichermedien	o	–
EDR 3.10 – Unterstützung von Updates	✓	"M1" (→ 7), "M3" (→ 7)
EDR 3.10 RE (1) – Authentizität und Integrität von Updates	o	–
EDR 3.11 – Physikalische Manipulationsicherheit und -erkennung	o	–

Anforderung	SL 1	Empfohlene Ausgleichsmaßnahmen auf Systemebene
EDR 3.11 RE (1) – Meldung eines Manipulationsversuchs	o	–
EDR 3.12 – Bereitstellung von Hersteller-Vertrauensankern	o	–
EDR 3.13 – Bereitstellung von Betreiber-Vertrauensankern	o	–
EDR 3.14 – Integrität von Boot-Prozessen	✓ ¹⁾	–
EDR 3.14 RE (1) – Authentizität des Boot-Prozesses	o	–

1) Die Integrität gegenüber Bit- und Speicherfehlern wird durch eine CRC32-Prüfsumme gewährleistet.

2) Reaktionen auf Fehler wie Netzwerk-Zeitüberschreitung oder -Überlastung sind definiert.

5.5 FR4 – Vertraulichkeit der Daten (DC)

5.5.1 Bedeutung der Sicherheitslevel

Die Norm IEC 62443-4-2 definiert Security Level 1 folgendermaßen:

Security Level	Beschreibung
SL 1	Verhindern der nicht autorisierten Offenlegung von Informationen durch Abhören oder zufälliges Aufdecken.

5.5.2 Erfüllung der Anforderungen (FR4)

Anforderung	SL 1	Empfohlene Ausgleichsmaßnahmen auf Systemebene
CR 4.1 – Vertraulichkeit von Informationen	o ¹⁾	–
CR 4.2 – Dauerhaftigkeit von Informationen	o	–
CR 4.2 RE (1) – Löschen gemeinsam genutzter Speicherressourcen	o	–
CR 4.2 RE (2) – Verifikation der Löschung	o	–
CR 4.3 – Verwendung von Verschlüsselung	o ²⁾	–

1) Nicht anwendbar, da es keine Daten mit explizitem Leseschutz gibt.

2) Nicht anwendbar, da keine kryptografischen Verfahren verwendet werden.

5.6 FR5 – Eingeschränkter Datenfluss (RDF)

5.6.1 Bedeutung der Sicherheitslevel

Die Norm IEC 62443-4-2 definiert Security Level 1 folgendermaßen:

Security Level	Beschreibung
SL 1	Verhindern der gelegentlichen oder zufälligen Umgehung der Aufteilung in Zonen und Conduits.

5.6.2 Erfüllung der Anforderungen (FR5)

Anforderung	SL 1	Empfohlene Ausgleichsmaßnahmen auf Systemebene
CR 5.1 – Netzaufteilung	✓	"M5" (→ 8), "M6" (→ 8), "M15" (→ 9)

5.7 FR6 – Rechtzeitige Reaktion auf Ereignisse (TRE)

5.7.1 Bedeutung der Sicherheitslevel

Die Norm IEC 62443-4-2 definiert Security Level 1 folgendermaßen:

Security Level	Beschreibung
SL 1	Überwachen des Betriebs der Komponente des IACS und Reagieren auf Vorfälle, sobald diese entdeckt worden sind, durch die Erfassung und Weitergabe forensischer Beweise auf Nachfrage.

5.7.2 Erfüllung der Anforderungen (FR6)

Anforderung	SL 1	Empfohlene Ausgleichsmaßnahmen auf Systemebene
CR 6.1 – Zugriffsmöglichkeit auf Ereignisprotokolle	o	"M7" (→ 8)
CR 6.1 RE (1) – Programmgesteuerter Zugriff auf Ereignisprotokolle	o	–
CR 6.2 – Kontinuierliche Überwachung	o	–

5.8 FR7 – Verfügbarkeit der Ressourcen (RA)

5.8.1 Bedeutung der Sicherheitslevel

Die Norm IEC 62443-4-2 definiert Security Level 1 folgendermaßen:

Security Level	Beschreibung
SL 1	Sicherstellen, dass die Komponente unter normalen Produktionsbedingungen zuverlässig arbeitet und DoS-Situationen (Denial of Service) verhindert, die eine Einheit durch gelegentliche oder zufällige Handlungen verursacht hat.

5.8.2 Erfüllung der Anforderungen (FR7)

Anforderung	SL 1	Empfohlene Ausgleichsmaßnahmen auf Systemebene
CR 7.1 – Schutz vor Denial-of-Service-Ereignissen	✓	SEW-EURODRIVE empfiehlt folgende Maßnahmen, um den Schutz zusätzlich zu erhöhen: "M1" (→ 7), "M3" (→ 7), "M5" (→ 8), "M6" (→ 8)
CR 7.1 RE (1) – Verwaltung der Kommunikationslast durch eine Komponente	o	–
CR 7.2 – Ressourcenmanagement	✓	–
CR 7.3 – Datensicherung im Automatisierungssystem (Backup)	✓ ¹⁾	–
CR 7.4 – Wiederherstellung des Automatisierungssystems	✓	–
CR 7.5 – Notstromversorgung	o	–
CR 7.6 – Netzwerk- und IT-Sicherheitseinstellungen	o ²⁾	–
CR 7.6 RE (1) – Maschinenlesbare Berichte über die momentanen IT-Sicherheitseinstellungen	o	–
CR 7.7 – Geringste Funktionalität	–	"M1" (→ 7), "M3" (→ 7), "M5" (→ 8), "M6" (→ 8), "M15" (→ 9)
CR 7.8 – Verzeichnis der Komponenten eines Automatisierungssystems	o	–

1) Die Datensicherung ist nur möglich, während der Umrichter nicht freigegeben ist.

2) Die Produkte haben keine IT-Security-Einstellungen. Informationen zu Netzwerkeinstellungen finden Sie in den Dokumentationen der Produkte.

6 Erfüllung der Anforderungen der EU-Datenverordnung

Die Produkte bieten "Access by Design" für alle von den Produkten erzeugten Daten und entsprechen damit den Anforderungen aus der EU-Datenverordnung (Verordnung 2023/2854, "EU Data Act"):

Der Zugriff auf die Produkte erfolgt unter Verwendung entsprechender Kommunikationsdienste in der Regel über folgende Wege:

- Engineering-Software, wie MOVITOOLS® MotionStudio oder MOVISUITE®
- verwendete Kommunikationsverbindungen

Sie können über diese Kommunikationsdienste z. B. folgende Aktionen durchführen:

- Parameter einsehen und ändern
- Parametersätze und Scope-Dateien auf externen Geräten speichern, z. B. auf Geräteoptionen oder sonstigen Speichermedien

Die Produkte verarbeiten und speichern keine personenbezogenen Daten.

Produktspezifische Details zum Datenzugriff, Speicherung, Löschung sowie der Art der Daten entnehmen Sie der jeweiligen Produktdokumentation.

7 Software- und Firmware-Updates

Software und Firmware werden über verschiedene Tools wie z. B. MOVISUITE® aktualisiert. Halten Sie bei Bedarf Rücksprache mit dem Service von SEW-EURODRIVE.

8 Ports und Services



Im Folgenden finden Sie zur sicheren Konfiguration von Routern und Firewalls die Ports und Services des Produkts.

Eine Erläuterung zur Bedeutung der Tabellenspalten sowie Informationen zu weiterer Hard- und Software von SEW-EURODRIVE finden Sie in folgender Dokumentation: Handbuch "Ports und Services bei WLAN- und ethernetbasierter Kommunikation".

8.1 MOVI-C®: MOVIMOT®, MOVIGEAR®, MOVIPRO®, MOVIDRIVE®, MOVITRAC®

Die folgende Tabelle bezieht sich auf die Produkte:

- MOVIMOT® advanced/performance/flexible
- MOVIGEAR® performance
- MOVIPRO® technology
- MOVIDRIVE® system/technology/modular
- MOVITRAC® classic/basic/advanced
- MOVIMOT® performance ELV

8.1.1 Zugriff über PROFINET-Schnittstelle

Geräte mit folgender Typenbezeichnung oder Geräteausführung:

- DFC2..
- MPX..DFC2
- MDX../CFN..
- MCX../CFN/..
- MCC../CFX11A-N
- MCB../CFX11A-N

Dienst/Funktion	Port	Protokoll	Werkseinstellung	Authentifizierung	Betrieb	Engineering	Berechtigung/ Beschreibung
PROFINET	EtherType 8892 _{hex}		aktiv	nein	ja	nein	Prozessdatenaustausch
MOVI-C AdressEditor	EtherType 88B5 _{hex}		aktiv	nein	ja	ja	Lesen und Schreiben auf die Adressparameter der Ethernet-Schnittstelle
PROFINET MRP Test Telegram	EtherType 88E3 _{hex}		aktiv	nein	ja	nein	Testtelegramm zum Erken- nen von Unterbrechungen im Kommunikationsring
PROFINET DCE/RPC	Dyn.	UDP	aktiv	nein	ja	ja	Lesen und Schreiben Zugriff auf alle indizierten Größen

Dienst/Funktion	Port	Protokoll	Werkseinstellung	Authentifizierung	Betrieb	Engineering	Berechtigung/ Beschreibung
Webserver ¹⁾	80	TCP	deaktivierbar	nein	nein	ja	Lesend auf indizierte Größen Schreibender Zugriff: Rücksetzen eines Fehlers, Aktivieren Blinkfunktion
SNMP (V1)	161	UDP	aktiv	ja	ja	ja	Lesen und Schreiben Zugriff auf MIBs, siehe "Anhang"
Engineering Protocol (SEW Datastream)	310	UDP	aktiv	nein	nein	ja	Scannen von allen Datastream-Teilnehmern
Engineering Protocol (SEW Datastream)	310	TCP	aktiv ²⁾	nein	nein	ja	Vollzugriff auf alle Daten und Funktionen

1) Der Dienst ist nicht in den Gateways CFX11A-... implementiert.

2) Interne Dienste werden durch ein unveränderbares Passwort gesichert.

8.1.2 Zugriff über EtherNet/IP™, Modbus TCP-Schnittstelle

Geräte mit folgender Typenbezeichnung oder Geräteausführung:

- DFC3..
- MPX..DFC3
- MDX../CFE..
- MCX../CFE/..
- MCC../CFX11A-E
- MCB../CFX11A-E

Dienst/Funktion	Port	Protokoll	Werkseinstellung	Authentifizierung	Betrieb	Engineering	Berechtigung/ Beschreibung
ODVA® Ethernet DLR	EtherType 80E1 _{hex}		aktiv	nein	ja	ja	Lesen und Schreiben (Ringredundanzparameter)
DHCP-Client	67/68	UDP	aktiv	nein	ja	nein	Lesen und Schreiben auf Adressparameter
Webserver ¹⁾	80	TCP	deaktivierbar	nein	nein	ja	Lesend auf indizierte Größen Schreibender Zugriff: Rücksetzen eines Fehlers, Aktivieren Blinkfunktion

33355924/DE – 05/2026

Dienst/Funktion	Port	Protokoll	Werkseinstellung	Authentifizierung	Betrieb	Engineering	Berechtigung/ Beschreibung
SNMP (bis FW-Version 2.xx) ²⁾	161	UDP	aktiv	nein	ja	nein	Nur Lesen Zugriff auf MIBs
Engineering Protocol (SEW Datastream)	310	UDP	aktiv	nein	nein	ja	Scannen von allen Datastream-Teilnehmern
Engineering Protocol (SEW Datastream)	310	TCP	aktiv ³⁾	nein	nein	ja	Vollzugriff auf alle Daten und Funktionen
Modbus TCP	502	TCP	aktiv	nein	ja	nein	Prozessdatenaustausch, Lesen und Schreiben auf alle indizierten Parameter
EtherNet/IP™: Implicit Message	2222	UDP	aktiv	nein	ja	nein	Prozessdatenaustausch
EtherNet/IP™: Explicit Message	44818	TCP	aktiv	nein	ja	nein	Parameter-Service, Lesen und Schreiben auf alle indizierten Parameter

1) Der Dienst ist nicht in den Gateways CFX11A... implementiert.

2) Die Antriebe unterstützen MIB-II nur bis zur Firmware-Version 2.xx. In neueren Firmware-Versionen wird SNMP nicht mehr unterstützt.

3) Interne Dienste werden durch ein unveränderbares Passwort gesichert.

8.1.3 CFL21A, MCX../CFL..., Zugriff über POWERLINK-Schnittstelle

Dienst/Funktion	Port	Protokoll	Werkseinstellung	Authentifizierung	Betrieb	Engineering	Berechtigung/ Beschreibung
Engineering Protocol (SEW Datastream)	310	TCP	aktiv ¹⁾	nein	nein	ja	Vollzugriff auf alle Daten und Funktionen
POWERLINK specific	3819	UDP	siehe POWERLINK Spezifikation				

1) Interne Dienste werden durch ein unveränderbares Passwort gesichert.

9 Ihr Kontakt zu SEW-EURODRIVE

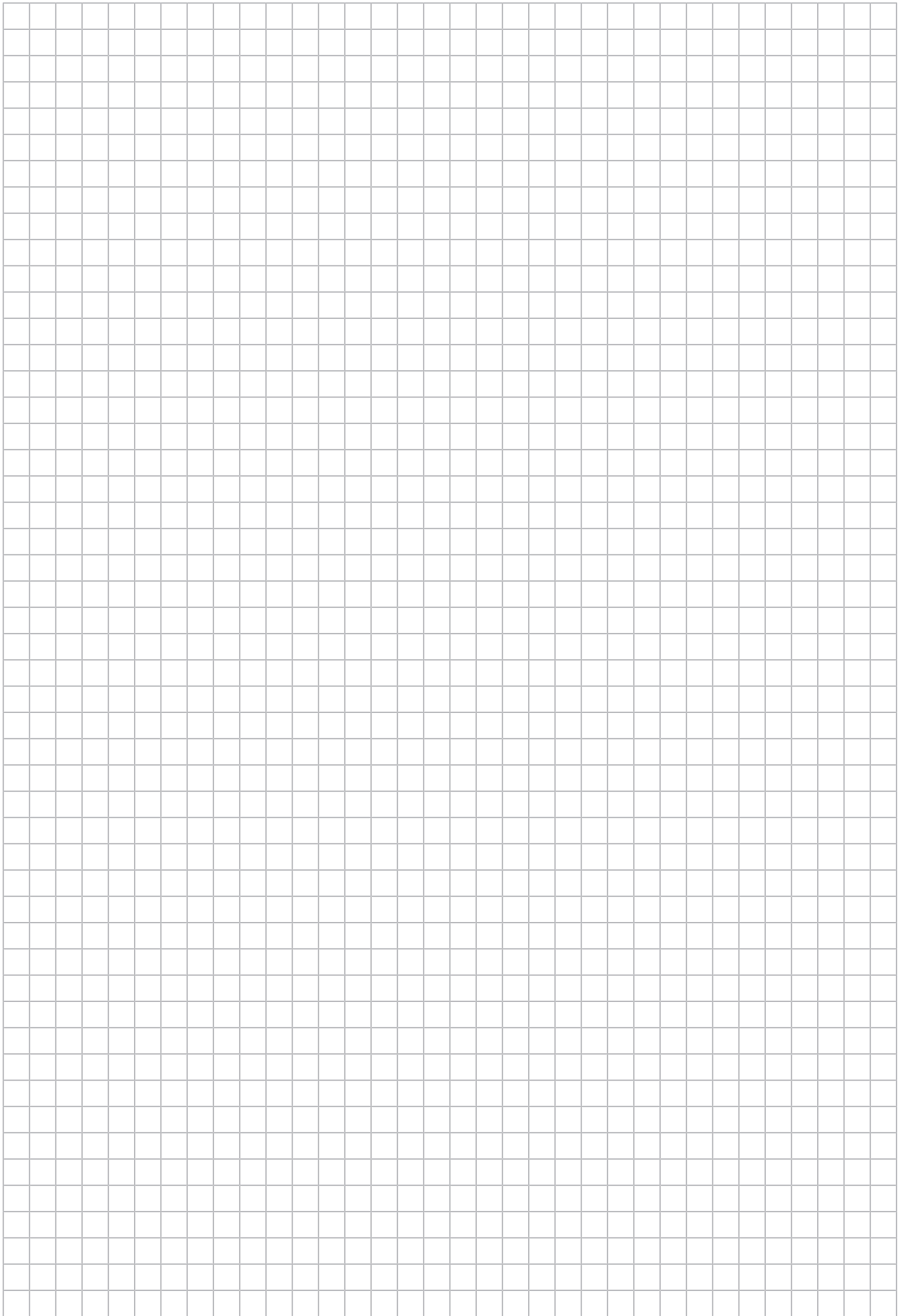
Die weltweiten Kontaktdaten und Standorte finden Sie auf der **Webseite von SEW-EURODRIVE** über folgenden Link oder den abgebildeten QR-Code.

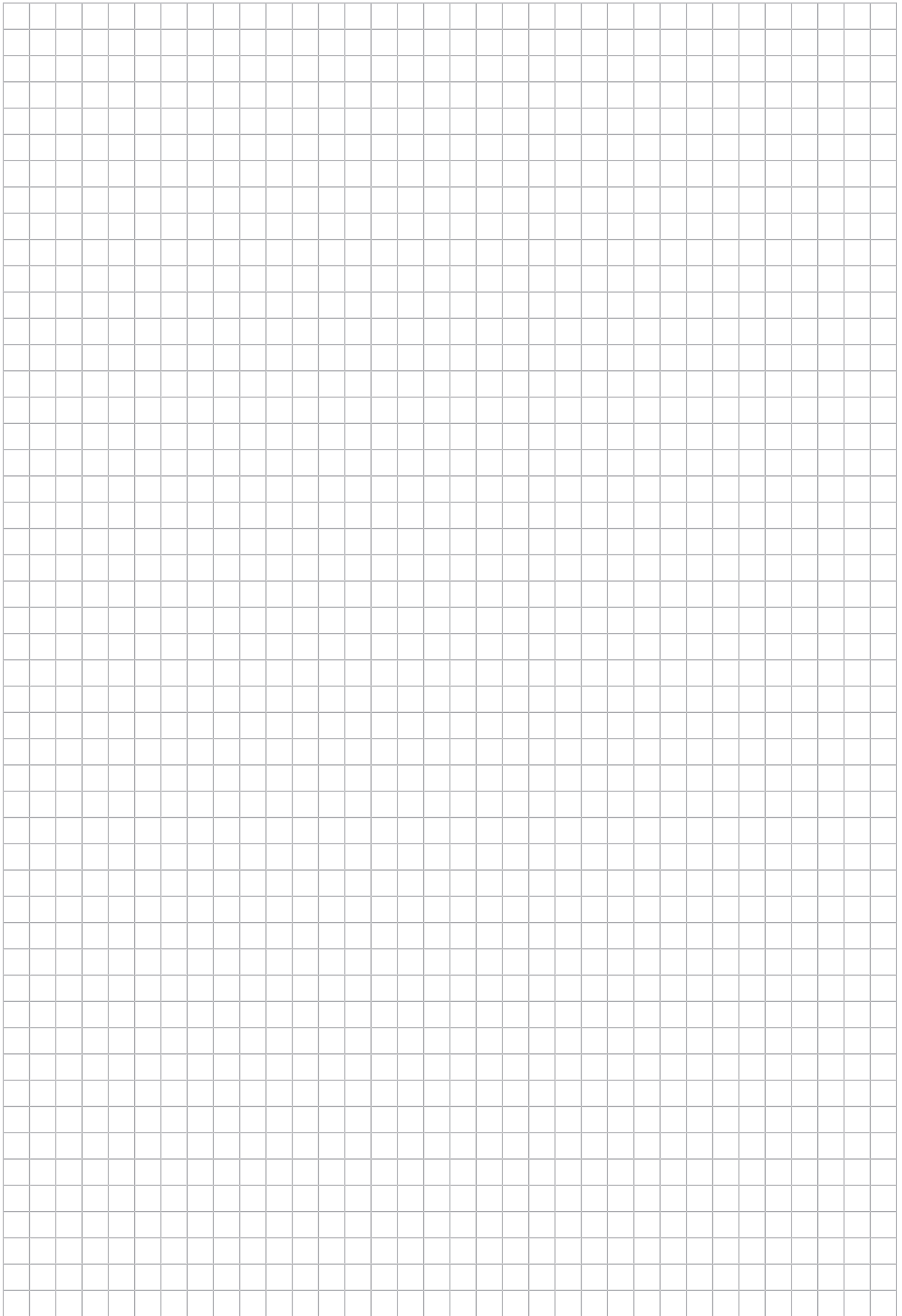
<https://www.sew-eurodrive.de/contacts-worldwide>

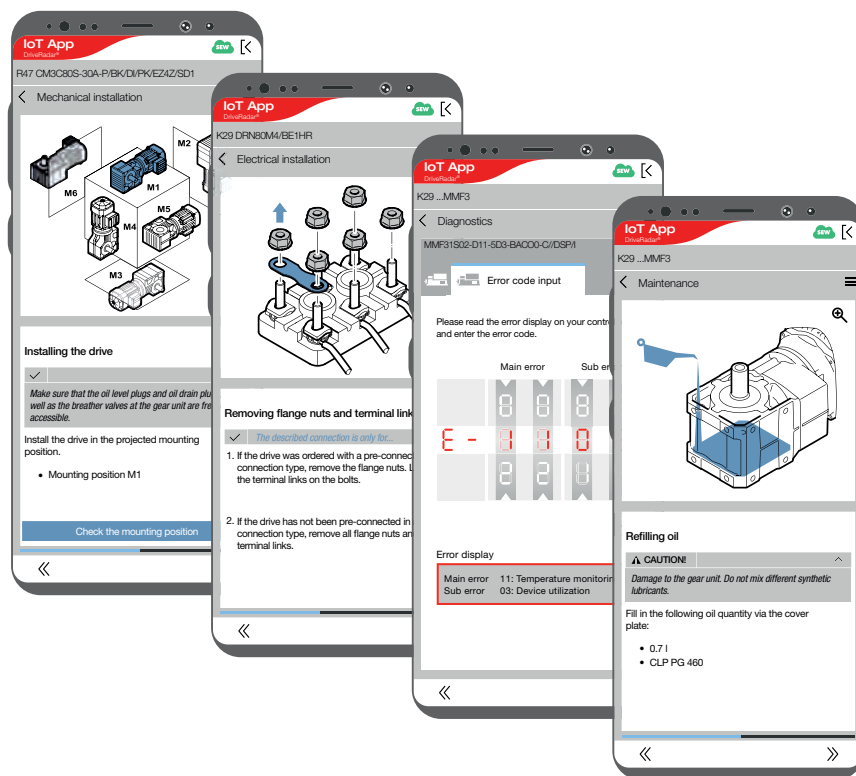


SEW
EURODRIVE









<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