



Handbuch



Security-Optionen für MOVI-C® CONTROLLER ab Firmware V08.01 (MOVISUITE® V2.40)



Inhaltsverzeichnis

1	Allgemeine Hinweise	5
1.1	Gebrauch der Dokumentation	5
1.2	Inhalt der Dokumentation	5
1.3	Mitgeltende Unterlagen	5
1.4	Aufbau der Warnhinweise	5
1.4.1	Bedeutung der Signalworte	5
1.4.2	Aufbau der abschnittsbezogenen Warnhinweise	6
1.4.3	Aufbau der eingebetteten Warnhinweise	6
1.5	Dezimaltrennzeichen bei Zahlenwerten	6
1.6	Mängelhaftungsansprüche	6
1.7	Produktnamen und Marken	6
1.8	Urheberrechtsvermerk	6
2	Sicherheitshinweise	7
2.1	Vorbemerkungen	7
2.2	Zielgruppe	7
2.3	IT-Sicherheit	7
3	Überblick	8
3.1	Voraussetzungen	8
3.2	Verfügbare Security-Optionen	8
3.3	Security-Screen öffnen	9
4	Secure Channel	10
5	Gerätebenutzerverwaltung	12
5.1	Gerätebenutzerverwaltung einrichten	12
5.2	Benutzer und Gruppen verwalten	13
5.3	Passwort zurücksetzen	13
5.4	Benutzer deaktivieren	14
5.5	Benutzerverwaltung übertragen	14
5.6	Zugriffsrechte	14
6	Secure Web Visualization	16
6.1	Schlüssel und Werte	16
6.2	Beispiel einer Konfigurationsdatei	16
6.3	Warnung vor ungültigem Zertifikat	17
7	Zertifikate	18
7.1	Selbst signierte Zertifikate	18
7.1.1	Zertifikat erzeugen	18
7.1.2	Zertifikat erneuern	18
7.2	Zertifikate einer Zertifizierungsstelle	19
7.2.1	CSR-Dateien erzeugen	19
7.2.2	Zertifikat verwenden	20
8	Weiterführende Informationen	21
8.1	Verschlüsselte Kommunikation im IEC-Projekt erzwingen	21
8.2	Zertifikate in der NBS-Bibliothek	21

8.3 Konfigurationsdatei verwenden..... 21

8.4 MOVIKIT® OPC-UA 22

8.4.1 Verschlüsselung 22

8.4.2 Port 4840 22

8.5 MOVIKIT® Visualization 22

Stichwortverzeichnis 23

1 Allgemeine Hinweise

1.1 Gebrauch der Dokumentation

Diese Dokumentation ist Bestandteil des Produkts. Die Dokumentation wendet sich an alle Personen, die Arbeiten an dem Produkt ausführen.

Stellen Sie die Dokumentation in einem leserlichen Zustand zur Verfügung. Stellen Sie sicher, dass die Anlagen- und Betriebsverantwortlichen sowie Personen, die unter eigener Verantwortung mit dem Produkt arbeiten, die Dokumentation vollständig gelesen und verstanden haben. Bei Unklarheiten oder weiterem Informationsbedarf wenden Sie sich an SEW-EURODRIVE.

1.2 Inhalt der Dokumentation

Die Beschreibungen in dieser Dokumentation beziehen sich auf die Soft- und Firmware zum Zeitpunkt der Publikation. Wenn Sie neuere Soft- oder Firmware installieren, kann die Beschreibung abweichen. Kontaktieren Sie in diesem Fall SEW-EURODRIVE.

Die aktuelle Ausgabe der Dokumentation finden Sie auch immer im Online-Support auf der Webseite von SEW-EURODRIVE.

1.3 Mitgeltende Unterlagen

Für alle weiteren Komponenten gelten die dazugehörigen Dokumentationen.

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.

1.4 Aufbau der Warnhinweise

1.4.1 Bedeutung der Signalworte

Die folgende Tabelle zeigt die Abstufung und Bedeutung der Signalworte der Warnhinweise.

Signalwort	Bedeutung	Folgen bei Missachtung
▲ GEFAHR	unmittelbar drohende Gefahr	Tod oder schwere Verletzungen
▲ WARNUNG	mögliche gefährliche Situation	Tod oder schwere Verletzungen
▲ VORSICHT	mögliche gefährliche Situation	leichte Verletzungen
ACHTUNG	möglicher Sachschaden	Beschädigung des Produkts oder seiner Umgebung
HINWEIS	nützlicher Hinweis oder Tipp: Erleichtert die Handhabung des Produkts.	

1.4.2 Aufbau der abschnittsbezogenen Warnhinweise

Die abschnittsbezogenen Warnhinweise gelten nicht nur für eine spezielle Handlung, sondern für mehrere Handlungen innerhalb eines Themas. Die verwendeten Gefahrensymbole weisen entweder auf eine allgemeine oder spezifische Gefahr hin.

Hier sehen Sie den formalen Aufbau eines abschnittsbezogenen Warnhinweises:

**SIGNALWORT!**

Art der Gefahr und ihre Quelle.

Mögliche Folge(n) der Missachtung.

- Maßnahme(n) zur Abwendung der Gefahr.

1.4.3 Aufbau der eingebetteten Warnhinweise

Die eingebetteten Warnhinweise sind direkt in die Handlungsanleitung vor dem gefährlichen Handlungsschritt integriert.

Hier sehen Sie den formalen Aufbau eines eingebetteten Warnhinweises:

▲ SIGNALWORT! Art der Gefahr und ihre Quelle. Mögliche Folge(n) der Missachtung. Maßnahme(n) zur Abwendung der Gefahr.

1.5 Dezimaltrennzeichen bei Zahlenwerten

Diese Dokumentation verwendet den Punkt als Dezimaltrennzeichen.

Beispiel: 30.5 kg

1.6 Mängelhaftungsansprüche

Beachten Sie die Informationen in dieser Dokumentation. Dies ist die Voraussetzung für den störungsfreien Betrieb und die Erfüllung eventueller Mängelhaftungsansprüche. Lesen Sie zuerst die Dokumentation, bevor Sie mit dem Produkt arbeiten!

1.7 Produktnamen und Marken

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

1.8 Urheberrechtsvermerk

© 2024 SEW-EURODRIVE. Alle Rechte vorbehalten. Jegliche – auch auszugsweise – Vervielfältigung, Bearbeitung, Verbreitung und sonstige Verwertung ist verboten.

2 Sicherheitshinweise

2.1 Vorbemerkungen

Die folgenden grundsätzlichen Sicherheitshinweise dienen dazu, Personen- und Sachschäden zu vermeiden und beziehen sich vorrangig auf den Einsatz der hier dokumentierten Produkte. Wenn Sie zusätzlich weitere Komponenten verwenden, beachten Sie auch deren Warn- und Sicherheitshinweise.

2.2 Zielgruppe

Fachkraft für Arbeiten mit Software

Alle Arbeiten mit der eingesetzten Software dürfen ausschließlich von einer Fachkraft mit geeigneter Ausbildung ausgeführt werden. Fachkraft im Sinne dieser Dokumentation sind Personen, die über folgende Qualifikationen verfügen:

- geeignete Unterweisung
- Kenntnis dieser Dokumentation und der mitgeltenden Dokumentationen
- Für die Nutzung dieser Software empfiehlt SEW-EURODRIVE zusätzlich Schulungen zu den Produkten.

2.3 IT-Sicherheit



Wenn Sie Unterstützung bei der Konfiguration benötigen, wenden Sie sich an den Service von SEW-EURODRIVE. Über aktuelle sicherheitsbezogene Probleme können Sie sich per E-Mail oder auf der Internetseite des Product Security Management informieren. Dort finden Sie verschiedene Kontaktmöglichkeiten, um sicherheitsbezogene Probleme zu melden.

Detaillierte Informationen zur IT-Sicherheit der verwendeten Produkte finden Sie in der jeweiligen Dokumentation.

3 Überblick

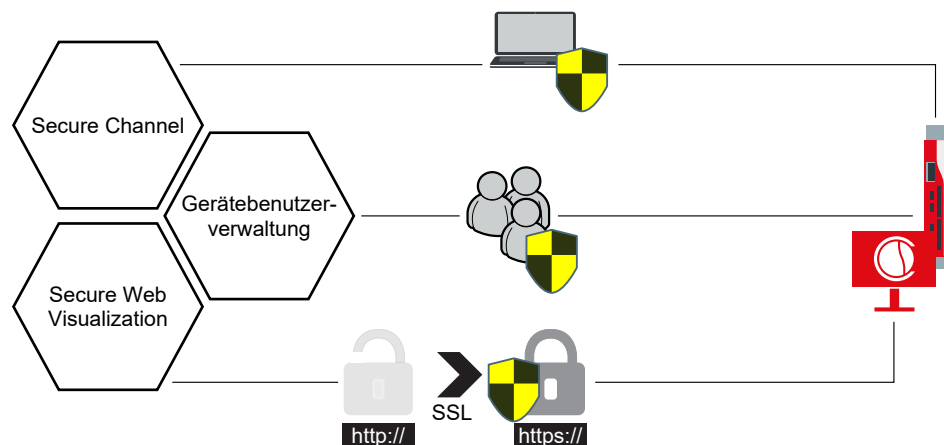
3.1 Voraussetzungen

Folgende Voraussetzungen müssen erfüllt sein, damit der Security-Screen verfügbar und der vollständige Zugriff auf die Security-Funktionen möglich ist:

- MOVI-C CONTROLLER® mit Firmware ab V08.01
- MOVISUITE® ab V2.40
- Zugriff auf das Verzeichnis `root/APP` des MOVI-C® CONTROLLER, beispielsweise über das Register "Dateien" des IEC-Editor.
- Um die Gültigkeit von Zertifikaten zu gewährleisten, müssen Zeit und Datum des MOVI-C® CONTROLLER aktuell und synchron sein. Klicken Sie dazu in der Konfiguration des MOVI-C® CONTROLLER in der Parametergruppe "Datum und Uhrzeit" auf die Schaltfläche [PC-Systemzeit übernehmen].

3.2 Verfügbare Security-Optionen

Folgende Grafik gibt einen Überblick über die zur Verfügung stehenden Security-Optionen:



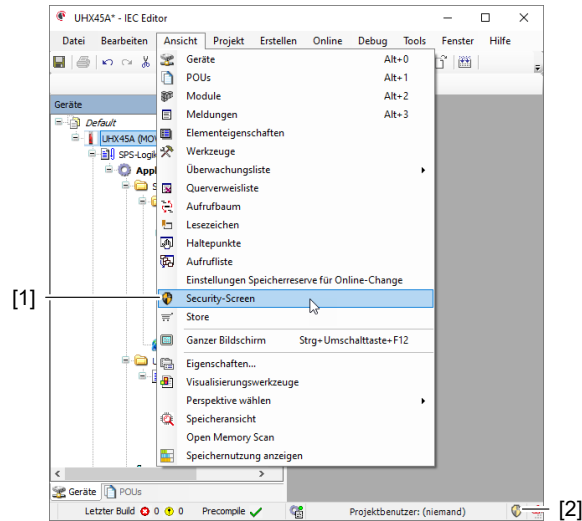
18014447434028555

Weitere Informationen finden Sie in den folgenden Kapiteln:

- "Secure Channel" (→ 10)
- "Gerätebenutzerverwaltung" (→ 12)
- "Secure Web Visualization" (→ 16)

3.3 Security-Screen öffnen

Um den Security-Screen zu öffnen, wählen Sie den Menübefehl "Ansicht" > "Security-Screen" [1] oder doppelklicken Sie auf das Symbol [2] in der Statusleiste des IEC-Editor.



49227683083

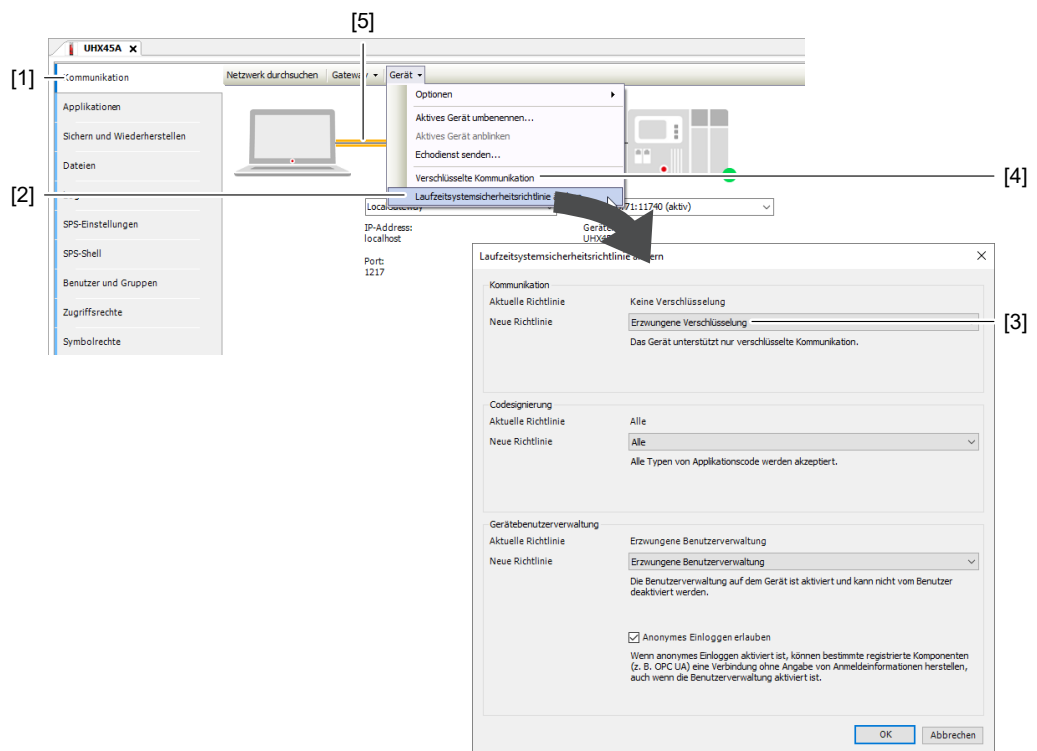
4 Secure Channel

Der Secure Channel erlaubt eine auf Zertifikaten basierende verschlüsselte Kommunikation. Dazu kann wahlweise ein externes Zertifikat importiert oder ein selbst signiertes Zertifikat vom MOVI-C® CONTROLLER generiert werden. Weitere Informationen finden Sie im Kapitel "Zertifikate" (→ 18).

HINWEIS



Wenn auf dem MOVI-C® CONTROLLER kein Zertifikat für die Kommunikation mit einer Komponente vorhanden ist, erzeugt er ein selbst signiertes Zertifikat mit Standardwerten und nutzt dieses für die verschlüsselte Kommunikation.



18014447442763531

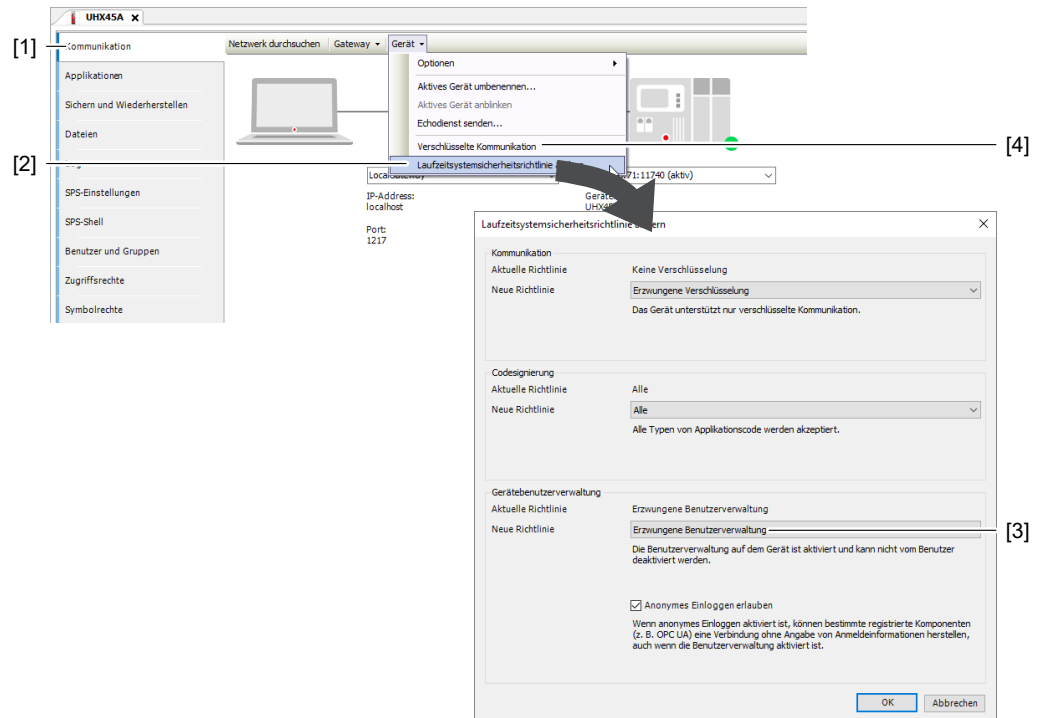
Um die verschlüsselte Kommunikation zu aktivieren, gehen Sie folgendermaßen vor:

- ✓ Der IEC-Editor ist geöffnet.
 - ✓ Die Verbindung zum MOVI-C® CONTROLLER ist hergestellt.
 - ✓ Der Gerätebaum ist geöffnet.
1. Doppelklicken Sie im Gerätebaum auf den MOVI-C® CONTROLLER.
 2. Wählen Sie auf der Registerkarte "Kommunikation" [1] den Menüpunkt [Gerät] > [Laufzeitsystemsicherheitsrichtlinie ändern...] [2].
 - ⇒ Das Fenster "Laufzeitsystemsicherheitseinstellungen ändern" wird angezeigt.
 3. Wählen Sie in der Gruppe "Kommunikation" im Auswahlfeld "Neue Richtlinie" den Eintrag [Erzwungene Verschlüsselung] [3].
 4. Klicken Sie auf die Schaltfläche [OK].
 - ⇒ Der MOVI-C® CONTROLLER unterstützt ab sofort ausschließlich verschlüsselte Kommunikation.

5. Wählen Sie auf der Registerkarte "Kommunikation" [1] den Menüpunkt [Gerät] > [Verschlüsselte Kommunikation] [4].
 - ⇒ Die verschlüsselte Kommunikation wird mit einer gelb hinterlegten Verbindungslinie [5] dargestellt.

5 Gerätebenutzerverwaltung

5.1 Gerätebenutzerverwaltung einrichten



49230031755

Um die Gerätebenutzerverwaltung des MOVI-C® CONTROLLER einzurichten, gehen Sie folgendermaßen vor:

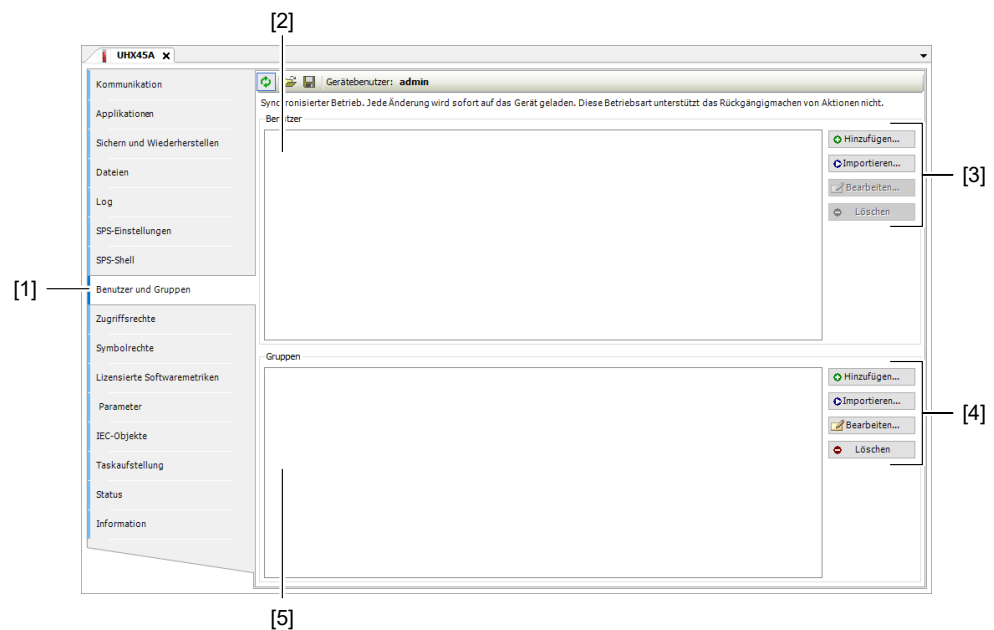
- ✓ Der IEC-Editor ist geöffnet.
- ✓ Die Verbindung zum MOVI-C® CONTROLLER ist hergestellt.
- 1. Doppelklicken Sie im Gerätebaum auf den MOVI-C® CONTROLLER.
- 2. Wählen Sie auf der Registerkarte "Kommunikation" [1] den Menüpunkt "Gerät" > "Laufzeitsystemsicherheitsrichtlinie ändern..." [2].
- 3. Das Fenster "Laufzeitsystemsicherheitseinstellungen ändern" wird angezeigt.
- 4. Wählen Sie in der Gruppe "Gerätebenutzerverwaltung" im Auswahlfeld "Neue Richtlinie" den Eintrag "Erzwungene Benutzerverwaltung" [3].
- 5. Klicken Sie auf die Schaltfläche [OK].
 - ⇒ Der MOVI-C® CONTROLLER erfordert ab sofort beim Verbindungsaufbau eine Benutzeranmeldung.
- 6. Verbinden Sie sich mit dem Gerät.
 - ⇒ Die Abfrage "Gerätebenutzerverwaltung aktivieren" wird angezeigt.
- 7. Bestätigen Sie die Abfrage, ob Sie die Gerätebenutzerverwaltung auf dem Gerät aktivieren möchten.
 - ⇒ Beim ersten Einrichten werden Sie aufgefordert, einen Administratorbenutzer anzulegen: Das Fenster "Gerätebenutzer hinzufügen" wird angezeigt.

8. Legen Sie den Administratorbenutzer an.

⇒ Die Gerätebenutzerverwaltung ist aktiv und ein Administratorbenutzer ist eingerichtet.

5.2 Benutzer und Gruppen verwalten

Um Benutzer und Gruppen zu bearbeiten, müssen Sie über entsprechende Berechtigungen verfügen. Verwenden Sie zum Bearbeiten die entsprechenden Schaltflächen der Registerkarte "Benutzer und Gruppen". Benutzer können nur bereits vorhandenen Gruppen zugeordnet werden.



48596892043

- [1] Registerkarte "Benutzer und Gruppen"
- [2] Liste der Benutzer
- [3] Schaltflächen zum Bearbeiten der Benutzer
- [4] Schaltflächen zum Bearbeiten der Gruppen
- [5] Liste der Gruppen

5.3 Passwort zurücksetzen

Um das Passwort eines Benutzers zurückzusetzen, gehen Sie folgendermaßen vor:

✓ Sie verfügen über entsprechende Berechtigungen.

1. Doppelklicken Sie auf den Benutzer, dessen Passwort Sie zurücksetzen möchten.

⇒ Das Fenster "Benutzer ... bearbeiten" wird geöffnet.

2. Tragen Sie in die Eingabefelder "Passwort" und "Passwort bestätigen" ein neues Passwort ein.

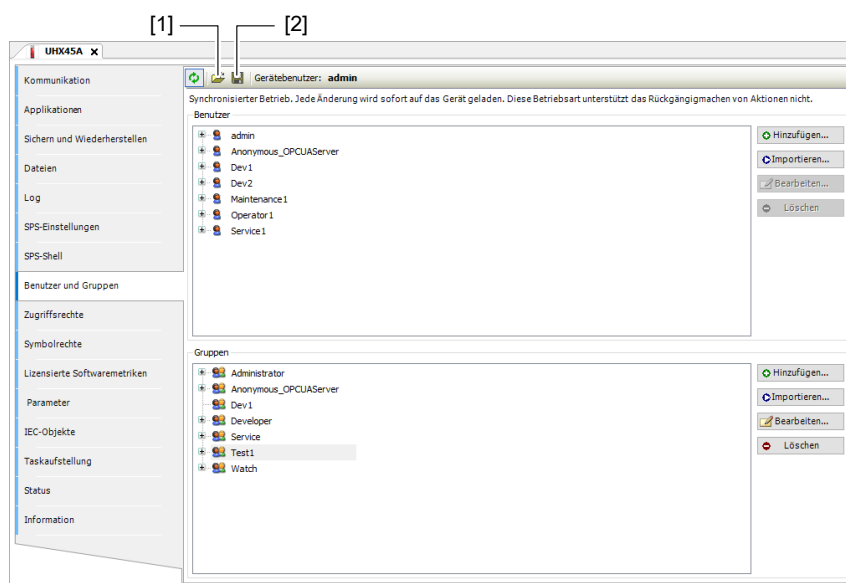
3. Klicken Sie auf die Schaltfläche [OK].

5.4 Benutzer deaktivieren

Um einen Benutzer zu deaktivieren, müssen Sie über entsprechende Berechtigungen verfügen. Entfernen Sie ihn aus allen verfügbaren Gruppen. Ohne zugewiesene Gruppe erfüllt ein Benutzer keine Rolle und verliert alle zugehörigen Zugriffsrechte.

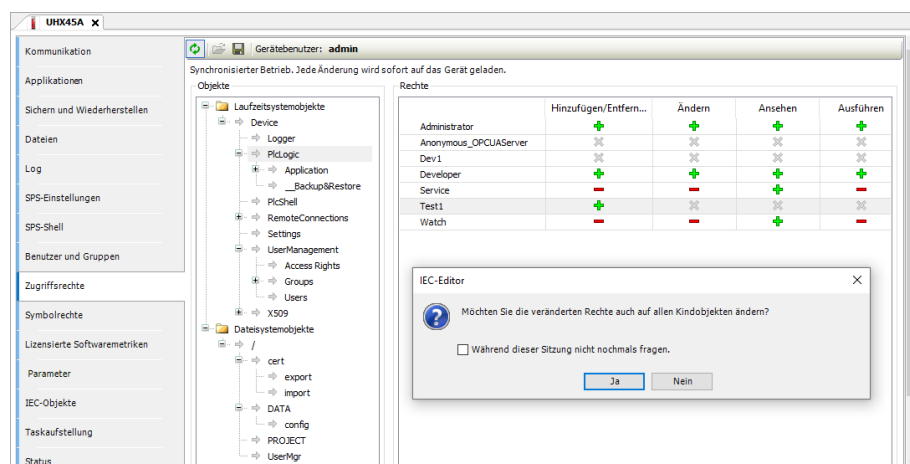
5.5 Benutzerverwaltung übertragen

Das Übertragen der Benutzerverwaltung erfolgt mit einer .dum2-Datei. Damit können Benutzer und Gruppen gesichert, wiederhergestellt und auf weitere MOVI-C® CONTROLLER übertragen werden. Verwenden Sie die entsprechenden Schaltflächen für Import [1] und Export [2] und vergeben Sie optional ein Passwort für die Datei.



49230292747

5.6 Zugriffsrechte








9007248620625163

Um die Zugriffsrechte auf ein Objekt zu ändern, gehen Sie folgendermaßen vor:

- ✓ Sie verfügen über entsprechende Berechtigungen.

1. Klicken Sie auf das Objekt, auf das Sie die Zugriffsrechte ändern möchten.
2. Doppelklicken Sie auf das Zugriffsrecht.
 - ⇒ Eine Abfrage wird angezeigt, ob die neuen Rechte vererbt werden sollen.
3. Klicken Sie auf die entsprechende Schaltfläche.
 - ⇒ Das Zugriffsrecht wurde geändert.

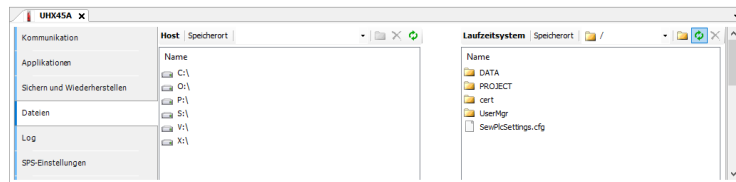
Mögliche Zugriffsrechte

Symbol	Bedeutung
	Zugriffsrecht explizit erteilt
	Zugriffsrecht explizit verweigert
	Zugriffsrecht neutral, vererbt erteilt
	Zugriffsrecht neutral, vererbt verweigert
	Das Zugriffsrecht wurde nicht explizit gesetzt oder verweigert, auch nicht im Vaterobjekt. Ein Zugriff ist nicht möglich.
keines	Es sind mehrere Objekte ausgewählt, die keine einheitlichen Zugriffsrechte haben.

6 Secure Web Visualization

SEW-EURODRIVE empfiehlt, die Kommunikation mit der browserbasierten Web Visualization zu verschlüsseln. Je nach eingestellten Optionen ist der Parallelbetrieb von verschlüsselter und unverschlüsselter Kommunikation möglich.

Die Einrichtung erfolgt über die Konfigurationsdatei `SewPlcSettings.cfg` im Verzeichnis `root/APP/` des MOVI-C® CONTROLLER. Erstellen Sie sie bei der Erstinbetriebnahme mit einem Texteditor und legen Sie sie dort ab. Verwenden Sie dazu die Registerkarte "Dateien" des MOVI-C® CONTROLLER:



49289758347

6.1 Schlüssel und Werte

SECURITY.CommunicationMode	
Bedeutung	mögliche Werte
Mit diesem Schlüssel legen Sie die Verbindungsart zwischen Browser und Web Visualization fest.	<ul style="list-style-type: none"> HTTPS REDIRECT_HTTP_TO_HTTPS HTTP, HTTPS HTTP
SECURITY.CreateSelfSignedCert	
Bedeutung	mögliche Werte
Mit diesem Schlüssel legen Sie fest, ob der MOVI-C® CONTROLLER ein selbst signiertes Zertifikat erzeugt falls keines hinterlegt ist.	<ul style="list-style-type: none"> Yes No
WebServerSecurePortNr	
Bedeutung	
Mit diesem Schlüssel legen Sie den Port fest, über den Browser und Web Visualization kommunizieren.	

6.2 Beispiel einer Konfigurationsdatei

```
[CmpWebServer]
SECURITY.CommunicationMode=REDIRECT_HTTP_TO_HTTPS
SECURITY.CreateSelfSignedCert=YES
WebServerSecurePortNr=8443
```

Damit wird der URL `http://<eigene_ip>:8080/webvisu.htm` weitergeleitet auf `https://<eigene_ip>:8443/webvisu.htm`.

6.3 Warnung vor ungültigem Zertifikat

Beim Aufruf der Web Visualization im Browser kann eine Warnung angezeigt werden, dass das verwendete Zertifikat ungültig ist. Folgende Fälle sind möglich:

- selbst signierte Zertifikate

Es kann eine Warnung beim Aufruf der Web Visualization auftreten. In diesem Fall kann im Browser eine Ausnahmeregelung hinterlegt werden, um keine weiteren Warnungen zu erhalten.

- Zertifikate einer Zertifizierungsstelle

Um keine Warnungen zu erhalten, installieren Sie das Root-Zertifikat der Zertifizierungsstelle auf dem Gerät, mit dem die Web Visualization aufgerufen wird.

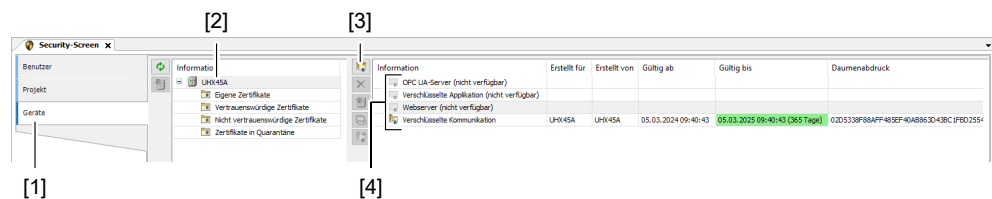
7 Zertifikate

7.1 Selbst signierte Zertifikate

7.1.1 Zertifikat erzeugen

Selbst signierte Zertifikate können Sie direkt auf dem MOVI-C® CONTROLLER für die folgenden Komponenten erzeugen:

- OPC-UA-Server
- Webserver
- verschlüsselte Kommunikation

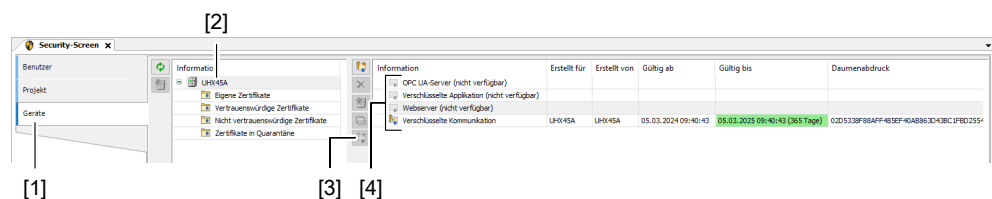


49184615947

Gehen Sie dazu folgendermaßen vor:

- ✓ Der IEC-Editor ist geöffnet.
 - ✓ Die Verbindung zum MOVI-C® CONTROLLER ist hergestellt.
 - ✓ Der Security-Screen ist geöffnet.
1. Öffnen Sie das Register "Geräte" [1].
 2. Klicken Sie auf den MOVI-C® CONTROLLER [2].
 3. Klicken Sie auf die Komponente [4], für die Sie ein Zertifikat erstellen wollen.
 4. Klicken Sie auf die Schaltfläche [Neues Zertifikat auf dem Gerät erzeugen] [3].
 - ⇒ Das Fenster "Zertifikatseinstellungen" wird angezeigt.
 5. Wählen Sie in der Auswahlliste "Schlüssellänge (Bit)" die Schlüssellänge aus.
 6. Geben Sie im Eingabefeld "Gültigkeitsdauer (Tage)" die Laufzeit des Zertifikats ein.
 7. Klicken Sie auf die Schaltfläche [OK].
 - ⇒ Das Zertifikat wird erzeugt.

7.1.2 Zertifikat erneuern



49725424395

Um ein Zertifikat zu erneuern, gehen Sie dazu folgendermaßen vor:

- ✓ Der IEC-Editor ist geöffnet.
 - ✓ Die Verbindung zum MOVI-C® CONTROLLER ist hergestellt.
 - ✓ Der Security-Screen ist geöffnet.
1. Öffnen Sie das Register "Geräte" [1].

2. Klicken Sie auf den MOVI-C® CONTROLLER [2].
3. Klicken Sie auf die Komponente [4], deren Zertifikat Sie erneuern wollen.
4. Klicken Sie auf die Schaltfläche [Erneuern des selektierten Zertifikats] [3].
⇒ Das Fenster "Zertifikateinstellungen" wird angezeigt.
5. Wählen Sie in der Auswahlliste "Schlüssellänge (Bit)" die Schlüssellänge aus.
6. Geben Sie im Eingabefeld "Gültigkeitsdauer (Tage)" die Laufzeit des Zertifikats ein.
7. Klicken Sie auf die Schaltfläche [OK].
⇒ Das Zertifikat wird erzeugt.

7.2 Zertifikate einer Zertifizierungsstelle

7.2.1 CSR-Dateien erzeugen

Für alle Komponenten

Um für alle Komponenten die CSR-Dateien zu erzeugen, gehen Sie folgendermaßen vor:

- ✓ Der IEC-Editor ist geöffnet.
 - ✓ Die Verbindung zum MOVI-C® CONTROLLER ist hergestellt.
1. Öffnen Sie im IEC-Editor die Registerkarte "SPS-Shell".
 2. Geben Sie in die Befehlszeile den Befehl `cert-createcsr` ein.
 3. Drücken Sie die Eingabetaste.
⇒ Die CSR-Dateien für alle Komponenten werden erzeugt und im Dateisystem des MOVI-C® CONTROLLER im Verzeichnis `root/APP/cert/export` abgelegt.
 4. Um die CSR-Dateien vom MOVI-C® CONTROLLER auf den Engineering-PC zu kopieren, verwenden Sie die Registerkarte "Dateien".

Für eine Komponente

Um für eine bestimmte Komponente die CSR-Datei zu erzeugen, gehen Sie folgendermaßen vor:

- ✓ Der IEC-Editor ist geöffnet.
 - ✓ Die Verbindung zum MOVI-C® CONTROLLER ist hergestellt.
1. Öffnen Sie im IEC-Editor die Registerkarte "SPS-Shell".
 2. Geben Sie in die Befehlszeile den Befehl `cert-getapplist` ein.
 3. Drücken Sie die Eingabetaste.
⇒ Die verfügbaren Komponenten werden aufgelistet.
 4. Geben Sie in die Befehlszeile den Befehl `cert-createcsr` gefolgt von der Nummer der Komponente ein.

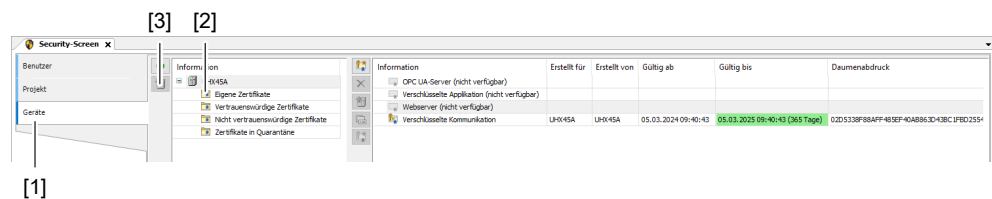
5. Drücken Sie die Eingabetaste.
 - ⇒ Die CSR-Datei für die gewählte Komponente wird erzeugt und im Dateisystem des MOVI-C® CONTROLLER im Verzeichnis `root/APP/cert/export` abgelegt.
6. Um die CSR-Datei vom MOVI-C® CONTROLLER auf den Engineering-PC zu kopieren, verwenden Sie die Registerkarte "Dateien".

7.2.2 Zertifikat verwenden

HINWEIS



Löschen Sie bereits vorhandene Zertifikate einer Komponente, bevor Sie ein neues Zertifikat verwenden.



49219074059

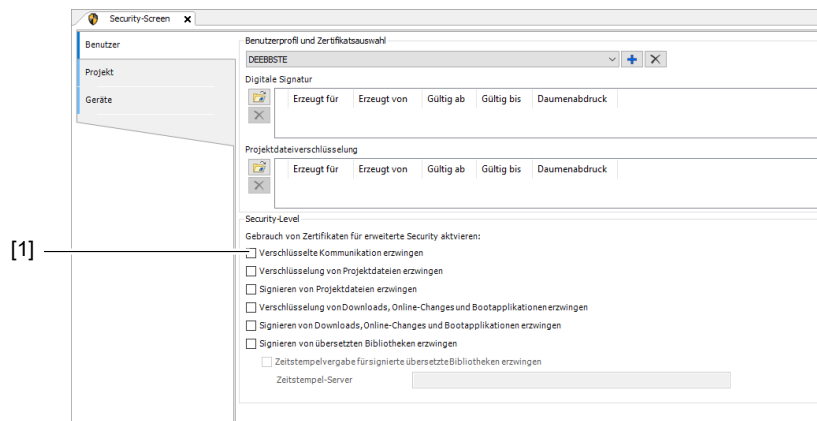
Um ein Zertifikat einer Zertifizierungsstelle zu verwenden, gehen Sie folgendermaßen vor:

- ✓ Sie verfügen über ein digitales Zertifikat einer Zertifizierungsstelle für eine Komponente des MOVI-C® CONTROLLER auf dem Engineering-PC.
 - ✓ Der IEC-Editor ist geöffnet.
 - ✓ Die Verbindung zum MOVI-C® CONTROLLER ist hergestellt.
1. Öffnen Sie das Register "Geräte" [1].
 2. Klicken Sie auf den Zertifikatsspeicher "Eigene Zertifikate" [2].
 3. Klicken Sie auf die Schaltfläche [Download] [3].
 4. Wählen Sie das digitale Zertifikat auf Ihrem Engineering-PC aus.
 5. Klicken Sie auf die Schaltfläche [Öffnen].
 - ⇒ Das importierte Zertifikat zur zugehörigen Komponente wird in der Liste angezeigt.
 6. Führen Sie einen Neustart des MOVI-C® CONTROLLER durch.

8 Weiterführende Informationen

8.1 Verschlüsselte Kommunikation im IEC-Projekt erzwingen

Die Option "verschlüsselte Kommunikation erzwingen" gilt für das gesamte IEC-Projekt. Eine Kommunikation ist dann nur mit Geräten möglich, die verschlüsselt kommunizieren.



48605803915

Um die verschlüsselte Kommunikation zu erzwingen, gehen Sie folgendermaßen vor:

- ✓ Der IEC-Editor ist geöffnet.
 - ✓ Die Verbindung zum MOVI-C® CONTROLLER ist hergestellt.
 - ✓ Der Security-Screen ist geöffnet.
1. Öffnen Sie die Registerkarte "Benutzer".
 2. Aktivieren Sie das Kontrollfeld "Verschlüsselte Kommunikation erzwingen" [1].

8.2 Zertifikate in der NBS-Bibliothek

Wenn Sie die NBS-Bibliothek nutzen, tauschen Sie die Zertifikate der Kommunikationspartner gegenseitig aus.

8.3 Konfigurationsdatei verwenden

Sie können die Konfiguration wahlweise über den IEC-Editor oder mit der Konfigurationsdatei `SewPlcSettings.cfg` vornehmen. Die Konfigurationsdatei wird beim Start des MOVI-C® CONTROLLER geladen. Wenn Sie im IEC-Editor securityrelevante Geräteoptionen eingestellt haben, die ebenfalls in der Konfigurationsdatei enthalten sind, werden diese überschrieben.

8.4 MOVIKIT® OPC-UA

8.4.1 Verschlüsselung

Das Softwaremodul MOVIKIT® OPC-UA unterstützt die zertifikatbasierte Verschlüsselung. Weitere Informationen finden Sie im Handbuch "MOVIKIT® OPC-UA, MOVIKIT® OPC-UA add-on SensorInterface".

8.4.2 Port 4840

permanent
schließen

Port 4840 ist geschlossen, wenn auf dem MOVI-C® CONTROLLER keine Lizenz für das Softwaremodul MOVIKIT® OPC-UA aktiviert ist (Testlizenz oder Vollversion), da der OPC-UA-Server nicht gestartet ist. Bei aktiver Lizenz startet der OPC-UA-Server zusammen mit dem MOVI-C® CONTROLLER automatisch, und Port 4840 ist geöffnet.

Über die Konfigurationsdatei `SewPlcSettings.cfg` können Sie den Port permanent schließen. Ist diese Einstellung aktiv, wird der OPC-UA-Server beim Hochfahren des Controllers trotz aktiver Lizenz nicht gestartet und lässt sich auch nicht nachträglich zur Laufzeit aktivieren. Verwenden Sie dazu folgenden Eintrag in der Konfigurationsdatei:

```
[CmpOPCUAServer]  
SECURITY.Activation=DEACTIVATED
```

8.5 MOVIKIT® Visualization

Das Softwaremodul MOVIKIT® Visualization unterstützt die Funktion `SecureChannel` derzeit nicht.

Stichwortverzeichnis

A

Abschnittsbezogene Warnhinweise 6

D

Dezimaltrennzeichen 6

dum2-Datei 14

E

Eingebettete Warnhinweise 6

Einstellungen werden nicht übernommen 21

F

Firmware-Version 8

H

Hinweise

Kennzeichnung in der Dokumentation 5

K

keine Verbindung möglich 21

Konfigurationsdatei 16, 22

M

Mängelhaftungsansprüche 6

Marken 6

mitgeltende Unterlagen 5

P

Produktnamen 6

S

SewPlcSettings.cfg 16, 22

Sicherheitshinweise

Vorbemerkungen 7

Signalworte in Warnhinweisen 5

Systemvoraussetzungen 8

U

Unterlagen, mitgeltende 5

Urheberrechtsvermerk 6

W

Warnhinweise

Aufbau der abschnittsbezogenen 6

Aufbau der eingebetteten 6

Kennzeichnung in der Dokumentation 5

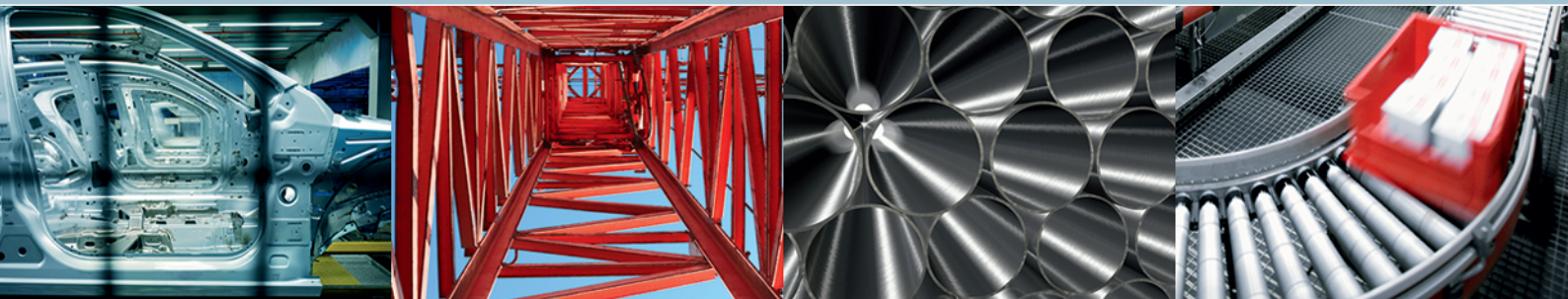
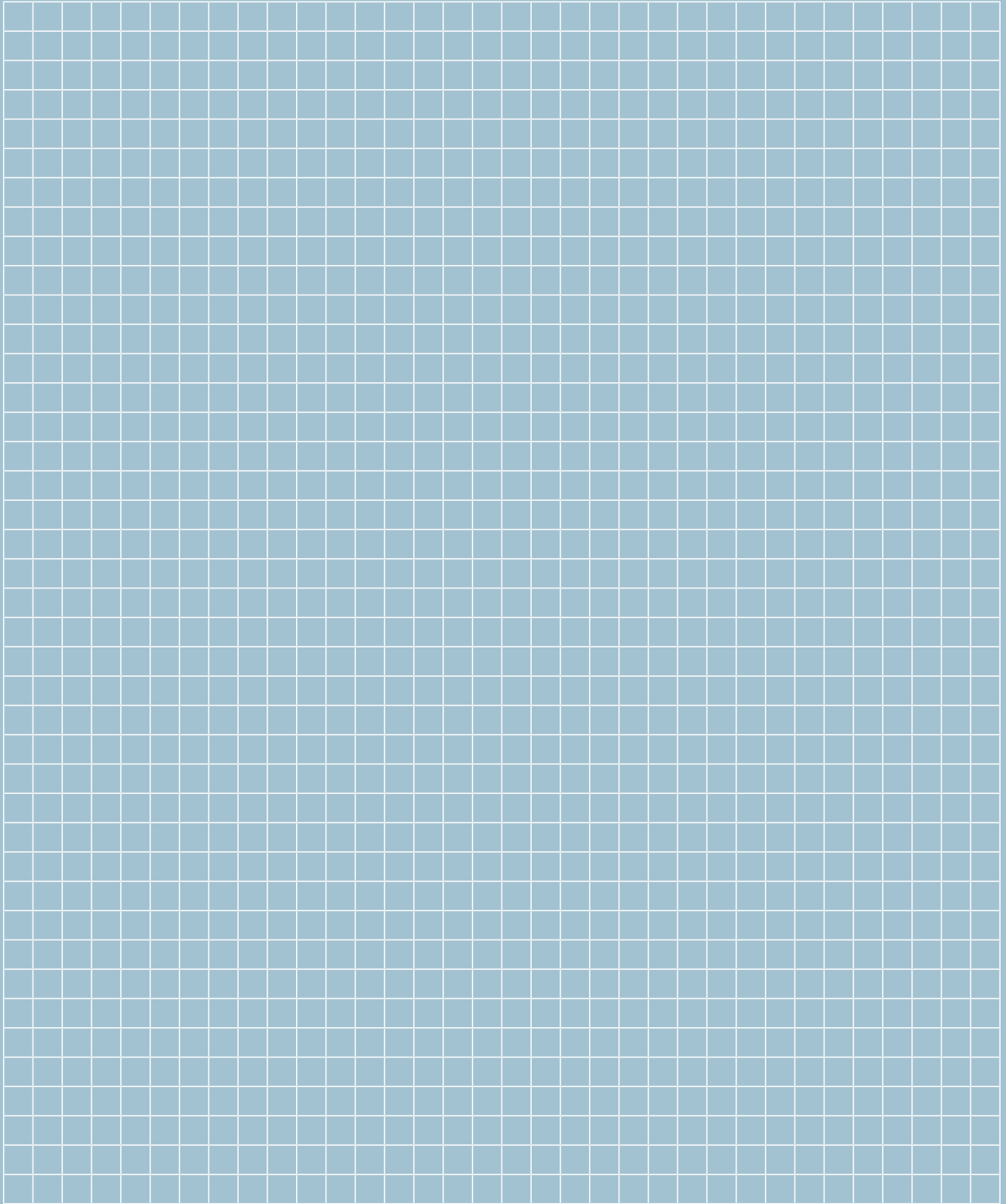
Z

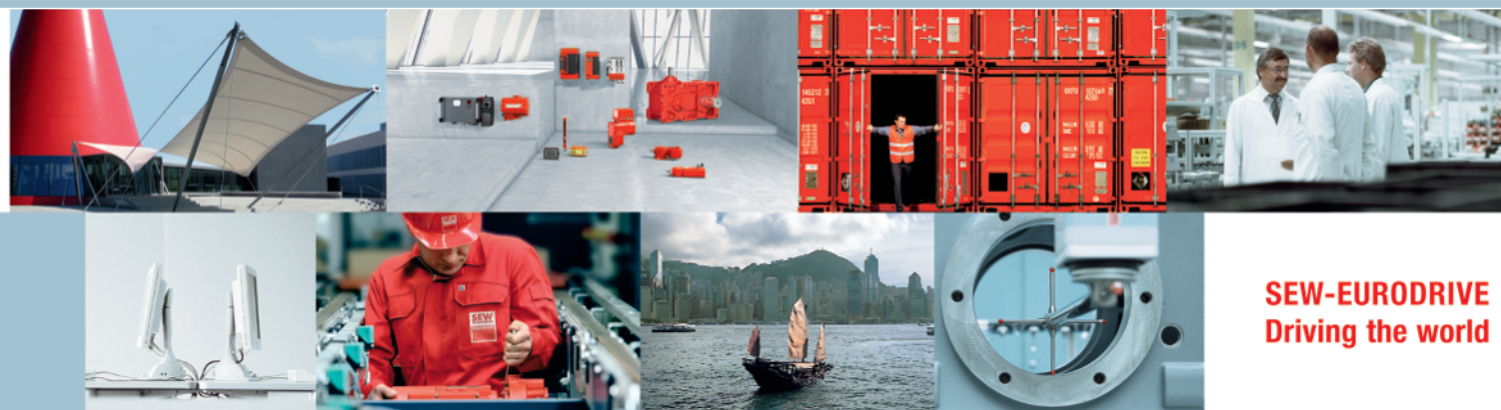
Zielgruppe 7











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