# Sicherheitskontroller XS/SC26-2 und SC10-2

## Bedienungsanleitung

Übersetzung der Orginalanweisungen
174868_DE Rev. V
2021-1-19
© Banner Engineering Corp. Alle Rechte vorbehalten

ПРОМЭЛЕКТРОНИКА/ sales@prom-elec.com

# Inhaltsverzeichnis


**1 Über dieses Dokument ..... 5**
1.1 Wichtig… Unbedingt lesen! ..... 5
1.2 Verwendung der Warnhinweise ..... 5
1.3 EU-Konformitätserklärung ..... 5
**2 Produktbeschreibung ..... 7**
2.1 In diesem Handbuch verwendete Fachbegriffe ..... 7
2.2 Software ..... 7
2.3 USB-Anschlüsse ..... 7
2.4 Ethernetverbindungen ..... 8
2.5 Interne Logik ..... 8
2.6 Passwort-Übersicht ..... 8
2.7 SC-XM2/3-Laufwerk und Programmierwerkzeug SC-XMP2 ..... 8
**3 XS/SC26-2 – Überblick ..... 10**
3.1 Ausführungen des XS/SC26-2 ..... 10
3.2 Funktionen und Anzeigen des XS/SC26-2 ..... 11
3.3 Verwendung von XS/SC26-2 Sicherheitskontrollern mit unterschiedlichen FIDs ..... 11
3.4 Ein- und Ausgangsanschlüsse ..... 12
3.4.1 XS/SC26-2 Sicherheitseingangsgeräte und nicht sicherheitsrelevante Eingangsgeräte ..... 12
3.4.2 Sicherheitsausgänge am XS/SC26-2 ..... 12
3.4.3 XS/SC26-2: Statusausgänge und virtuelle Statusausgänge ..... 13
3.5 Funktion des XS/SC26-2 für die automatische Optimierung von Anschlüssen deaktivieren ..... 14
**4 SC10-2 – Überblick ..... 16**
4.1 Ausführungen des SC10-2 ..... 16
4.2 Funktionen und Anzeigen des SC10-2 ..... 16
4.3 Verwendung von SC10-2 Sicherheitskontrollern mit verschiedenen FIDs ..... 17
4.4 Ein- und Ausgangsanschlüsse ..... 18
4.4.1 SC10-2 Sicherheitseingangsgeräte und nicht sicherheitsrelevante Eingangsgeräte ..... 18
4.4.2 Sicherheits-Relaisausgänge am SC10-2 ..... 18
4.4.3 Statusausgänge und virtuelle Statusausgänge am SC10-2 ..... 18
4.5 Funktion des SC10-2 für die automatische Optimierung von Anschlüssen (ATO) bei externen Klemmenblöcken (ETB) ..... 19
**5 Spezifikationen und Anforderungen ..... 20**
5.1 XS/SC26-2 – Spezifikationen ..... 20
5.2 Spezifikationen für den SC10-2 ..... 22
5.3 Abmessungen ..... 25
5.4 Systemvoraussetzungen für den PC ..... 25
**6 Systeminstallation ..... 27**
6.1 Installation der Software ..... 27
6.2 Installation des Sicherheitskontrollers ..... 27
6.2.1 Montageanleitung ..... 27
**7 Überlegungen vor der Installation ..... 28**
7.1 Geeignete Anwendung ..... 28
7.2 Anwendungen des XS/SC26-2 ..... 28
7.3 Anwendungen des SC10-2 ..... 29
7.4 Sicherheitseingangsgeräte ..... 29
7.4.1 Integrität der Sicherheitsschaltungen und Sicherheitsschaltungsprinzipien nach ISO 13849-1 ..... 30
7.4.2 Eigenschaften von Sicherheitseingangsgeräten ..... 31
7.5 Optionen für Sicherheitseingangsgeräte ..... 33
7.5.1 Sicherheitsstufen von Sicherheitsschaltungen ..... 34
7.5.2 Not-Aus-Schalter ..... 34
7.5.3 Seilzugschalter (Kabelzugschalter) ..... 35
7.5.4 Zustimmtaster ..... 36
7.5.5 Schutzhalt (Sicherheitsstopp) ..... 36
7.5.6 Verriegelte Schutzeinrichtung bzw. Schutztür ..... 36
7.5.7 Optosensor ..... 37
7.5.8 Zweihandsteuerung ..... 38
7.5.9 Sicherheitsmatte ..... 40
7.5.10 Muting-Sensor ..... 43
7.5.11 Überbrückungsschalter ..... 45
7.5.12 AVM-Funktion (Adjustable Valve Monitoring, einstellbare Ventilüberwachung) ..... 45
7.5.13 SC10-2: ISD-Eingänge ..... 46
7.5.14 XS/SC26-2: Zyklusinitiierung für Pressensteuerungs-Funktionsblock ..... 51
7.5.15 XS/SC26-2: SQS-Funktion (sequenzieller Stopp) der Pressensteuerung ..... 51
7.5.16 XS/SC26-2: Muting-Sensor der Pressesteuerung ..... 52
7.5.17 XS/SC26-2: Fußpedal ..... 53
7.6 Nicht sicherheitsrelevante Eingangsgeräte ..... 54
7.6.1 Manueller Reset-Eingang ..... 55
7.7 Virtuelle nicht sicherheitsrelevante Eingangsgeräte (XS/SC26-2 ab FID 2 und SC10-2) ..... 57
7.7.1 Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) ..... 57
7.7.2 Virtuelle Ein-/Ausschaltung und Muting-Aktivierung ..... 60
7.8 Sicherheitsausgänge ..... 60
7.8.1 XS/SC26-2 – Sicherheits-Transistorausgänge ..... 63
7.8.2 Sicherheits-Relaisausgänge ..... 66
7.8.3 EDM- und Endschaltgeräteanschluss ..... 67
7.9 Statusausgänge ..... 73
7.9.1 Signallogik für Statusausgänge ..... 73
7.9.2 Statusausgangsfunktion ..... 74
7.9.3 XS/SC26-2: Statusausgangsfunktion der Pressensteuerung ..... 75
7.10 Virtuelle Statusausgänge ..... 76

**8 Erste Schritte ..... 78**
8.1 Erstellen einer Konfiguration ..... 78
8.2 Hinzufügen von Eingängen und Statusausgängen ..... 78
8.2.1 Hinzufügen von Sicherheits- und nicht sicherheitsrelevanten Eingängen ..... 78
8.2.2 Hinzufügen von Statusausgängen ..... 81
8.3 Entwerfen der Steuerungslogik ..... 82
8.4 Speichern und Bestätigen einer Konfiguration ..... 83
8.4.1 Speichern einer Konfiguration ..... 83
8.4.2 Bestätigung einer Konfiguration ..... 83
8.4.3 Schreiben der bestätigten Konfiguration mithilfe des Programmierwerkzeugs auf einen SC-XM2/3 ..... 84
8.4.4 Hinweise zum Bestätigen oder Schreiben einer Konfiguration in einen konfigurierten SC10-2 oder XS/SC26-2 ab FID 3 ..... 84
8.5 Beispielkonfigurationen ..... 85
8.5.1 XS/SC26-2 Beispielkonfiguration ..... 85
8.5.2 XS/SC26-2: Beispielkonfiguration – einfache Pressensteuerung mit mutingfähigem Sicherheitseingang ..... 88
8.5.3 XS/SC26-2: Beispielkonfiguration der vollfunktionalen Pressensteuerung ..... 90
**9 Software ..... 95**
9.1 Abkürzungen ..... 95
9.2 Software-Übersicht ..... 97
9.3 Neues Projekt ..... 99
9.4 Projekteinstellungen ..... 99
9.5 Registerkarte Geräte ..... 100
9.6 Registerkarte Funktionsansicht ..... 101
9.6.1 Logikblöcke ..... 102
9.6.2 Funktionsblöcke ..... 105
9.7 Registerkarte Schaltplan ..... 105
9.8 Registerkarte Kontaktplan ..... 107
9.9 Registerkarte ISD ..... 108
9.10 Registerkarte Industrie-Ethernet ..... 110
9.10.1 Netzwerkeinstellungen ..... 112
9.10.2 Erstellen von SPS-Tags/Etiketten-Dateien ..... 113
9.10.3 Ethernet/IP-Gruppenobjekte ..... 115
9.11 Registerkarte Konfigurationsübersicht ..... 116
9.12 Druckoptionen ..... 116
9.13 XS/SC26-2 Passwort-Manager ..... 117
9.14 Passwort-Manager für SC10-2 ..... 118
9.15 Anzeigen und Importieren von Kontrollerdaten ..... 118
9.16 Livemodus ..... 120
9.17 Simulationsmodus ..... 123
9.17.1 Aktionszeitsteuerungsmodus ..... 126
9.18 Referenzsignale ..... 127
**10 Beschreibung der Funktionsblöcke ..... 128**
10.1 Überbrückungsblock ..... 128
10.1.1 Verriegeln/Kennzeichnen ..... 128
10.2 Verzögerungsblock (XS/SC26-2 ab FID 2 und SC10-2) ..... 129
10.3 Zustimmtaster-Block ..... 130
10.4 Latch-Reset-Block ..... 132
10.5 Muting-Block ..... 135
10.5.1 Optionale Muting-Attribute ..... 140
10.6 One-Shot-Block (XS/SC26-2 ab FID 4) ..... 143
10.7 Pressensteuerung (XS/SC26-2 ab FID 4) ..... 144
10.7.1 Modus-Funktionsblock ..... 146
10.7.2 Funktionsblock Pressensteuerungeingänge ..... 146
10.7.3 Beispiele für den Pressensteuerungs-Funktionsblock ..... 148
10.7.4 Regelkreis ..... 150
10.8 Zweihandsteuerungsblock (für XS/SC26-2 bis FID 3 und SC10-2 FID 1) ..... 151
10.9 Zweihandsteuerungsblock (XS/SC26-2 ab FID 4 sowie SC10-2 ab FID 2) ..... 154
**11 Bedienfeld am XS/SC26-2 ..... 155**
11.1 XS/SC26-2: Konfigurationsmodus ..... 155
**12 Industrie-Ethernet – Übersicht ..... 157**
12.1 Konfiguration des Sicherheitskontrollers ..... 157
12.2 Industrie-Ethernet – Definitionen ..... 158
12.3 Abrufen aktueller Fehlerinformationen ..... 159
12.4 EtherNet/IP™ ..... 159
12.4.1 Welche XS/SC26-2-EDS-Datei und -Dokumentation sollten Sie verwenden? ..... 159
12.4.2 Installation der EDS-Datei des Sicherheitskontroller von Banner in der ControlLogix-Software ..... 160
12.4.3 RSLogix5000-Konfiguration (implizite Nachrichten) ..... 167
12.4.4 Eingänge zum Sicherheitskontroller (Ausgänge von der SPS) ..... 172
12.4.5 Ausgänge vom Sicherheitskontroller (Eingänge zur SPS) ..... 174
12.4.6 Konfigurationsbaugruppenobjekt ..... 182
12.4.7 Fehlerbeispiele ..... 182
12.4.8 Flags ..... 184
12.4.9 Erweiterte Flags ..... 185
12.4.10 ISD-Systemstatuswörter ..... 185
12.4.11 RSLogix5000-Konfiguration (explizite Nachrichten) ..... 186
12.4.12 EIP in der Omron-SPS-Konfiguration ..... 194
12.5 Modbus/TCP ..... 206
12.5.1 Flags ..... 217
12.5.2 Erweiterte Flags ..... 218
12.6 SPS5, SLC500 und MicroLogix (PCCC) ..... 218
12.6.1 SPS-Konfiguration ..... 218
12.6.2 Ausgänge vom Sicherheitskontroller (Eingänge zur SPS) ..... 220
12.6.3 Eingänge zum Sicherheitskontroller (Ausgänge von der SPS) ..... 228
12.6.4 Flags ..... 229
12.6.5 Erweiterte Flags ..... 230
12.7 PROFINET® ..... 230
12.7.1 PROFINET und die Sicherheitskontroller ..... 230

12.7.2 GSD-Datei (General Station Description) ..... 230
12.7.3 PROFINET IO-Datenmodell ..... 230
12.7.4 Konfiguration des Sicherheitskontrollers für eine PROFINET IO-Verbindung ..... 231
12.7.5 Beschreibung der Module ..... 231
12.7.6 Konfigurationsanleitung ..... 241
12.8 ISD: Informationen zur Umwandlung von Temperatur, Spannung und Abstand ..... 248
12.8.1 ISD: Versorgungsspannung ..... 248
12.8.2 ISD: Innentemperatur ..... 248
12.8.3 ISD: Auslöserabstand ..... 249
**13 Systemüberprüfung ..... 251**
13.1 Zeitplan für vorgeschriebene Überprüfungen ..... 251
13.2 Inbetriebnahmeprüfung ..... 251
13.2.1 Überprüfung des Systembetriebs ..... 252
13.2.2 Setup vor der Inbetriebnahme, Inbetriebnahme und regelmäßige Prüfroutinen ..... 252
**14 Informationen zum Status und zum Betrieb ..... 259**
14.1 Status der LED-Anzeigen am XS/SC26-2 ..... 259
14.2 Statusanzeigen des Eingangsmoduls ..... 260
14.3 Ausgangsmodul (Transistor oder Relais) Statusanzeigen ..... 261
14.4 Status der LED-Anzeigen am SC10-2 ..... 261
14.5 Livemodus-Informationen: Software ..... 263
14.6 Informationen zum Livemodus: Bedienfeld am Kontroller ..... 263
14.7 Sperrzustände ..... 263
14.8 Nach einem Sperrzustand ..... 264
14.9 SC10-2: Automatische Optimierung von Anschlüssen ..... 264
14.10 Beispielkonfiguration für den SC10-2 ohne automatische Optimierung von Anschlüssen ..... 266
14.11 XS/SC26-2-Modelle ohne integrierte Schnittstelle: Verwendung des SC-XM2/3 ..... 270
14.12 XS/SC26-2-Modelle mit integrierter Schnittstelle: Verwendung des SC-XM2/3 ..... 271
14.13 SC10-2: Verwendung des SC-XM3 ..... 275
14.14 Setzen Sie den Sicherheitskontroller auf die Werkseinstellungen zurück. ..... 276
14.15 Werkseinstellungen ..... 277
**15 Fehlerbehebung ..... 278**
15.1 Software: Fehlerbehebung ..... 278
15.2 Software: Fehlercodes ..... 279
15.3 Überprüfen der Treiberinstallation ..... 281
15.4 Fehlersuche und -behebung ..... 283
15.4.1 Fehlercode-Tabelle für XS/SC26-2 ..... 283
15.4.2 SC10-2 Fehlercode-Tabelle ..... 288
**16 Komponenten und Zubehörteile ..... 292**
16.1 Ersatzteile und Zubehör ..... 292
16.2 Ethernet-Anschlussleitungen ..... 292
16.3 Interface-Module ..... 292
16.3.1 Mechanisch verbundene Kontaktgeber ..... 292
**17 Kundendienst und Wartung ..... 293**
17.1 Reinigung ..... 293
17.2 Reparaturen und Garantie ..... 293
17.3 Kontakt ..... 293
17.4 Beschränkte Garantie der Banner Engineering, Corp. ..... 293
17.5 Banner Engineering Corp. Urheberrechtsvermerk zur Software ..... 294
**18 Normen und Vorschriften ..... 295**
18.1 Geltende US-Normen ..... 295
18.2 Geltende OSHA-Vorschriften ..... 295
18.3 Geltende europäische und internationale Normen ..... 296
**19 Glossar ..... 297**

# 1 Über dieses Dokument

## 1.1 Wichtig… Unbedingt lesen!

Es liegt in der Verantwortlichkeit des Maschinenkonstrukteurs, des überwachenden Ingenieurs, des Maschinenbauers, des Maschinenbedieners und/oder des Wartungspersonals oder Wartungselektrikers, diese Vorrichtung in vollständiger Übereinstimmung mit allen geltenden Bestimmungen und Normen einzusetzen und zu warten. Die Vorrichtung kann die geforderte Schutzfunktion nur ausfüllen, wenn sie vorschriftsmäßig montiert, bedient und gewartet wird. In diesem Handbuch wird versucht, vollständige Anweisungen zu Montage, Bedienung und Wartung zu geben. *Es ist sehr zu empfehlen, das Handbuch vollständig durchzulesen.* Wenden Sie sich bei Fragen zur Anwendung oder zum Gebrauch der Vorrichtung bitte an Banner Engineering.

Weitere Informationen zu US- und internationalen Instituten für die Normierung der Leistung von Schutzanwendungen und Schutzeinrichtungen finden Sie unter Normen und Vorschriften auf Seite 295.

**WARNUNG:**

- Es liegt in der Verantwortung des Anwenders, diese Anweisungen zu befolgen.
- **Wenn diese Aufgaben nicht befolgt werden, kann möglicherweise eine Gefahrsituation entstehen, die zu schweren oder tödlichen Verletzungen führen kann.**
- Alle Anweisungen zu diesem Gerät sorgfältig durchzulesen, zu verstehen und zu beachten.
- Eine Risikobeurteilung durchzuführen, die die konkrete Maschinenschutzanwendung berücksichtigt. Informationen zur normgerechten Methodik sind ISO 12100 oder ANSI B11.0 zu entnehmen.
- Zu ermitteln, welche Schutzeinrichtungen und -methoden aufgrund der Ergebnisse der Risikobeurteilung geeignet sind, und diese unter Beachtung aller geltenden örtlichen, regionalen und nationalen Gesetze und Vorschriften zu implementieren. In diesem Zusammenhang wird auch auf ISO 13849-1, ANSI B11.19 und/oder weitere geeignete Normen verwiesen.
- Zu prüfen, ob das komplette Schutzsystem (einschließlich Ein- und Ausgangsgeräten und Steuerungen) sachgemäß konfiguriert und installiert ist, ob es funktionsfähig ist und wie beabsichtigt läuft.
- Nach Bedarf regelmäßig zu überprüfen, ob das gesamte Schutzsystem wie für die Anwendung beabsichtigt läuft.

## 1.2 Verwendung der Warnhinweise

Die Sicherheitshinweise und Erklärungen in diesem Dokument sind durch Warnsymbole gekennzeichnet und müssen für die sichere Verwendung des Sicherheitskontroller von Banner beachtet werden. Bei Nichtbeachtung aller Sicherheits- und Warnhinweise ist die sichere Bedienung bzw. der sichere Betrieb nicht mehr unbedingt gewährleistet. Die folgenden Signalwörter und Warnsymbole werden wie folgt definiert:

| Signalwort | Definition | Symbol |
|---|---|---|
| **WARNUNG** | **Warnhinweise vom Typ „Warnung“** beziehen sich auf potenzielle Gefahrensituationen, die, wenn sie nicht verhindert werden, zu schweren Verletzungen bis einschließlich zum Tod führen können. | |
| **VORSICHT** | **Warnhinweise vom Typ „Vorsicht“** beziehen sich auf potenzielle Gefahrensituationen, die, sofern sie nicht verhindert werden, zu leichten bis mäßigen Verletzungen oder potenziellen Sachschäden führen können. | |

Diese Hinweise sollen den Maschinenkonstrukteur und den Hersteller, den Endbenutzer und das Wartungspersonal darüber informieren, wie sie eine falsche Anwendung vermeiden und das Sicherheitskontroller von Banner so anwenden, dass die diversen Anforderungen für Schutzanwendungen erfüllt werden. Es liegt in der Verantwortung der genannten Personen, diese Hinweise zu lesen und zu beachten.

## 1.3 EU-Konformitätserklärung

Banner Engineering Corp. erklärt hiermit, dass diese Produkte die Bestimmungen der genannten Richtlinien sowie sämtliche wesentlichen Gesundheits- und Sicherheitsvorschriften erfüllen. Die vollständige Konformitätserklärung finden Sie unter www.bannerengineering.com.

| Produkt | Richtlinie |
| --- | --- |
| Programmierbarer Sicherheitskontroller SC26-2, programmierbarer Sicherheitskontrollers XS26-2, Sicherheits-Transistorausgangsmodule XS2so und XS4so, Sicherheitseingangsmodule XS8si und XS16si, Sicherheitsrelaismodule XS1ro und XS2ro und Sicherheitskontroller SC10-2: | 2006/42/EG und EMV-Richtlinie 2004/108/EG |

Vertreter in der EU: Peter Mertens, Geschäftsführer Banner Engineering BV. Adresse: Park Lane, Culliganlaan 2F, Bus 3, 1831 Diegem, Belgien.

# 2 Produktbeschreibung

Die Sicherheitssteuerung ist ein kritischer und unverzichtbarer Bestandteil eines jeden Sicherheitssystems. Das liegt daran, dass Sicherheitskontroller dafür sorgen, dass Ihre Sicherheitsmaßnahmen 1) entweder gar nicht oder 2) zumindest in berechenbarer, sicherer Weise versagen.

Ein Sicherheitskontroller ist oft eine ideale Lösung für die Sicherheitssteuerung, denn er bietet mehr Funktionen als ein Sicherheitsrelais und ist kostengünstiger als eine Sicherheits-SPS. Außerdem können Sie einen intelligenten, skalierbaren Sicherheitskontroller Ihrem Bedarf entsprechend erweitern und Ihre Maschinensicherheitssysteme damit fernüberwachen.

Die Sicherheitskontroller von Banner sind benutzerfreundliche, konfigurierbare und erweiterbare Module (Ausführungen XS26-2xx) für die Überwachung zahlreicher Sicherheits- und nicht sicherheitsrelevanter Eingangsgeräte und bieten sichere Stopp- und Startfunktionen für Maschinen mit gefährlichen Bewegungen. Der Sicherheitskontroller kann zahlreiche Sicherheitsrelais-Module in Anwendungen ersetzen, wie zum Beispiel Sicherheitseingangsgeräte wie Not-Aus-Schalter, Schutztürschalter mit Verriegelung, Sicherheits-Lichtvorhänge, Zweihandsteuerungen, Sicherheitsmatten und andere Schutzeinrichtungen. Die Sicherheitskontroller können außerdem mithilfe von zusätzlichen Eingangs- und/oder Ausgangserweiterungsmodulen anstelle von größeren und komplexeren Sicherheits-SPS verwendet werden.

Das Bedienfeld am Kontroller:

- Ermöglicht den Zugriff auf die Fehlerdiagnose.
- Ermöglicht das Lesen und Schreiben der Konfigurationsdatei von SC-XM2- und SC-XM3-Laufwerken und auf diese Laufwerke.
- XS/SC26-2: Zeigt die Konfigurationsübersicht an, einschließlich der Klemmenzuordnungen und der Netzwerkeinstellungen.

## 2.1 In diesem Handbuch verwendete Fachbegriffe

In diesem Handbuch werden die folgenden Fachbegriffe verwendet.

**Sicherheitskontroller**: Eine abgekürzte Version, die sich auf das gesamte XS/SC26-2-Sicherheitskontrollersystem sowie auf den SC10-2 bezieht, die beide in diesem Handbuch behandelt werden.

**Erweiterbarer Sicherheitskontroller**: Bezieht sich auf erweiterbare Ausführungen.

**Basiskontroller**: Bezieht sich auf das Hauptmodul im XS/SC26-2-Sicherheitskontrollersystem.

**Programmierbarer Sicherheitskontroller SC26-2, Programmierbarer Sicherheitskontroller XS26-2, Sicherheits-Transistorausgangsmodule XS2so und XS4so, Sicherheitseingangsmodule XS8si und XS16si, Sicherheitsrelaismodule XS1ro und XS2ro**: Der offizielle Name der XS/SC26-2 Produktreihe.

## 2.2 Software

Die Software für den Sicherheitskontroller von Banner ist eine Anwendung mit Echtzeit-Display und Diagnosewerkzeugen, über die Sie folgende Aufgaben ausführen können:

- Erstellen und Bearbeiten von Konfigurationen
- Testen einer Konfiguration im Simulationsmodus
- Schreiben einer Konfiguration auf den Sicherheitskontroller
- Lesen der aktuellen Konfiguration vom Sicherheitskontroller
- Anzeigen von Echtzeitinformationen, z. B. zum Gerätestatus
- Anzeigen von Fehlerinformationen

Die Software verwendet Symbole und Schaltungssymbole, mit denen Sie die geeigneten Eingangsgeräte und Eigenschaften auswählen können. Während die diversen Geräteeigenschaften und E/A-Steuerungsbeziehungen auf der Registerkarte **Funktionsansicht** konfiguriert werden, erstellt das Programm automatisch die entsprechenden Schalt- und Kontaktpläne.

Nähere Informationen finden Sie unter Software-Übersicht auf Seite 97.

## 2.3 USB-Anschlüsse

Der Micro-USB-Port am Basiskontroller und der SC10-2 dienen zum Anschließen an den PC (über das SC-USB2-Kabel) und das SC-XM2/3-Laufwerk zum Lesen und Schreiben der mit der Software erstellten Konfigurationen.

**VORSICHT: Mögliche unbeabsichtigte Masserückleitung**

Die USB-Schnittstelle wird nach Industriestandard implementiert und nicht von der 24-V-Versorgung isoliert.

Über das USB-Kabel können der Computer und der Sicherheitskontroller Teil einer unbeabsichtigten Masserückleitung für andere verbundene Geräte werden. Durch starke Ströme könnte der PC und/oder der Sicherheitskontroller beschädigt werden. Dies sollte möglichst vermieden werden. Banner empfiehlt hierzu, das USB-Kabel als einziges Kabel an den PC anzuschließen und den PC auf einer nicht leitenden Fläche aufzustellen. Hierzu sollte das Netzteil nach Möglichkeit vom Laptop getrennt werden.

Die USB-Schnittstelle ist zum Herunterladen von Konfigurationen und für die vorübergehende Überwachung oder Fehlerbehebung gedacht. Sie ist nicht für den Dauerbetrieb ausgelegt.

# 2.4 Ethernetverbindungen

Ethernetverbindungen werden mithilfe eines Ethernetkabels hergestellt, das vom Ethernetanschluss am Sicherheitskontroller der Basis (nur bei Ethernet-Ausführungen) oder vom Typ SC10-2 mit einem Netzwerkschalter oder mit dem Steuer- oder Überwachungsgerät verbunden wird. Der Sicherheitskontroller unterstützt entweder Standardkabel oder Kabel im Crossover-Stil. In Umgebungen mit starken Störungen ist eventuell ein geschirmtes Kabel erforderlich.

# 2.5 Interne Logik

Die interne Logik des Sicherheitskontrollers ist so ausgelegt, dass ein Sicherheitsausgang nur einschalten kann, wenn alle Sicherheitseingangs-Steuersignale und die selbstüberwachenden Signale des Sicherheitskontrollers im Ein-Zustand sind und melden, dass kein Fehlerzustand vorliegt.

Die Software für den Sicherheitskontroller von Banner verwendet sowohl Logik- als auch Sicherheitsfunktionsblöcke für allgemeine und erweiterte Anwendungen.

Logikblöcke basieren auf booleschen Logikgesetzen (wahr oder falsch). Die folgenden Logikblöcke sind verfügbar:

- NOT
- AND
- OR
- NAND
- NOR
- XOR
- Bistabile Kippschaltung (Set-Priorität und Reset-Priorität)

Weitere Informationen siehe Logikblöcke auf Seite 102.

Funktionsblöcke sind vorprogrammierte Blöcke mit integrierter Logik, die diverse Attributauswahlen enthalten, um den Anforderungen sowohl allgemeiner als auch komplexer Anwendungen gerecht zu werden. Die folgenden Funktionsblöcke sind verfügbar:

- Überbrückungsblock
- Zustimmtaster-Block
- Latch-Reset-Block
- Muting-Block
- Zweihandsteuerungsblock
- Verzögerungsblock (XS/SC26-2 ab FID 2 und SC10-2)
- One-Shot-Block (XS/SC26-2 ab FID 4)
- Pressensteuerungsblock (XS/SC26-2 ab FID 4)

Siehe Funktionsblöcke auf Seite 105 für weitergehende Informationen.

# 2.6 Passwort-Übersicht

Um die Konfiguration zu bestätigen und in den Sicherheitskontroller zu schreiben und um über die Software auf den Passwort-Manager zuzugreifen, ist ein Passwort erforderlich. Weitere Informationen finden Sie unter XS/SC26-2 Passwort-Manager auf Seite 117 und Passwort-Manager für SC10-2 auf Seite 118.

# 2.7 SC-XM2/3-Laufwerk und Programmierwerkzeug SC-XMP2

Die Laufwerke SC-XM2 und SC-XM3 dienen zum Speichern einer **bestätigten** Konfiguration.

**XS/SC26-2**: Die Konfiguration kann direkt durch den Sicherheitskontroller geschrieben werden, wenn das Laufwerk in den Mikro-USB-Anschluss eingesteckt wird (siehe XS/SC26-2: Konfigurationsmodus auf Seite 155). Eine andere Möglichkeit ist die Konfiguration über das Programmierwerkzeug SC-XMP2. Hierbei verwenden Sie nur die Software ohne Anschließen des Sicherheitskontrollers.

**Wichtig:** Überprüfen Sie (über die Software oder anhand der Aufschrift auf dem weißen Etikett am SC-XM2/3-Laufwerk), ob die auf den Sicherheitskontroller importierte Konfiguration korrekt ist.

Klicken Sie auf , um auf die Optionen für das Programmierwerkzeug zuzugreifen:

- **Lesen**: Liest die aktuelle Sicherheitskontrollerkonfiguration vom SC-XM2/3-Laufwerk und lädt sie in die Software.
- **Schreiben**: Schreibt eine bestätigte Konfiguration von der Software auf das SC-XM2/3-Laufwerk.
- **Sperre**: Sperrt das SC-XM2/3-Laufwerk und verhindert dadurch, dass Konfigurationen auf das Laufwerk geschrieben werden (ein leeres Laufwerk kann nicht gesperrt werden).

**Anmerkung:** Sie können die Sperre für das SC-XM2/3-Laufwerk nicht mehr aufheben, nachdem es gesperrt wurde.

# 3 XS/SC26-2 – Überblick

Mit der Möglichkeit, bis zu acht E/A-Erweiterungsmodule hinzuzufügen, bietet der erweiterbare Sicherheitskontroller XS26-2 die Fähigkeit, sich an unterschiedliche Maschinen anzupassen, einschließlich großer Maschinen mit mehreren Prozessen.




- Programmierung in wenigen Minuten mit intuitiver, benutzerfreundlicher Konfigurationssoftware
- Bis zu acht E/A-Erweiterungsmodule können bei wachsenden oder wechselnden Automatisierungsanforderungen hinzugefügt werden
- Erweiterungsmodule in sechs Ausführungen zur Auswahl
- Ausführungen der Erweiterungsmodule bieten verschiedene Sicherheitseingänge, Sicherheits-Transistorausgänge und Sicherheits-Relaisausgänge
- Innovative Live-Anzeige Funktion und Diagnostik ermöglichen eine aktive Überwachung der I/Os auf einem PC und helfen bei der Fehlersuche und Inbetriebnahme
- Sicherheitskontroller und Eingangsmodule ermöglichen die Umwandlung der Sicherheitseingänge in Statusausgänge zur effizienten Nutzung der Anschlüsse
- Ethernet-fähige Ausführungen können für bis zu 256 virtuelle Statusausgänge konfiguriert werden
- Optionales externes Laufwerk vom Typ SC-XM2/3 für schnellen Austausch und schnelle Konfiguration ohne PC

## 3.1 Ausführungen des XS/SC26-2

Alle erweiterbaren und nicht erweiterbaren Basismodule haben 18 Sicherheitseingänge, 8 konvertierbare Sicherheitsein-/-ausgänge und 2 Sicherheits-Transistorausgangspaare. Bis zu acht Erweiterungsmodule in einer beliebigen Kombination aus Eingangs- und Ausgangsmodulen können zu den erweiterbaren Ausführungen des Basiskontrollers hinzugefügt werden.

*Tabelle 1. Erweiterbare Basisausführungen*

| Typenbezeichnung | Anzeige | Ethernet-fähig |
|---|---|---|
| **XS26-2** | Nein | Nein |
| **XS26-2d** | Ja | Nein |
| **XS26-2e** | Nein | Ja |
| **XS26-2de** | Ja | Ja |

*Tabelle 2. Nicht erweiterbare Basisausführungen*

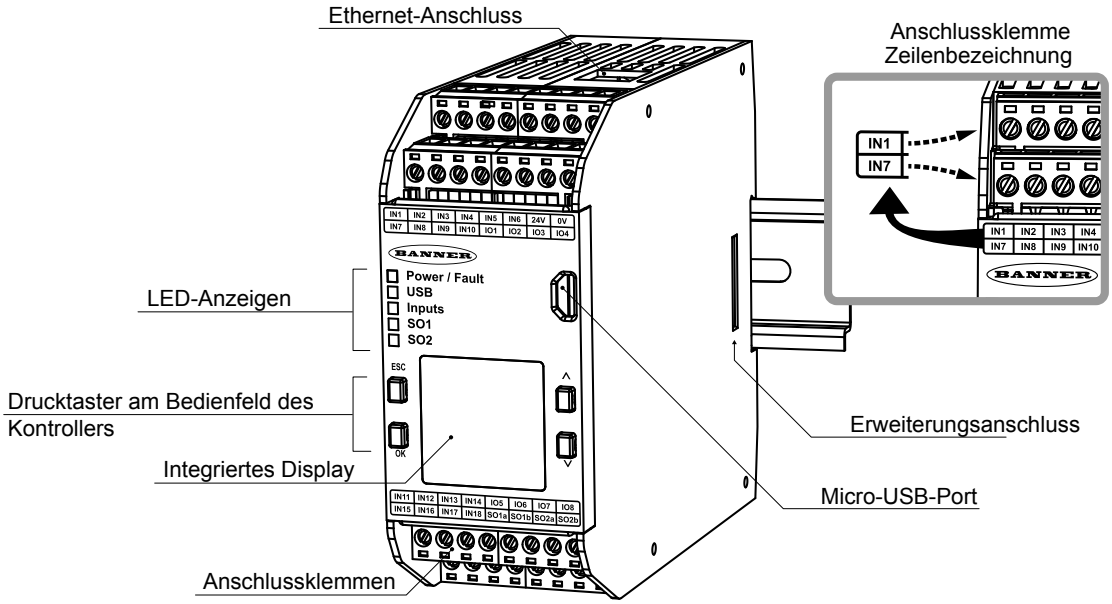
| Typenbezeichnung | Anzeige | Ethernet-fähig |
|---|---|---|
| **SC26-2** | Nein | Nein |
| **SC26-2d** | Ja | Nein |
| **SC26-2e** | Nein | Ja |
| **SC26-2de** | Ja | Ja |

*Tabelle 3. E/A-Erweiterungsmodule*

| Typenbezeichnung | Beschreibung |
|---|---|
| **XS16si** | Sicherheitseingangsmodul – 16 Eingänge (4 umrüstbar) |
| **XS8si** | Sicherheitseingangsmodul – 8 Eingänge (2 umrüstbar) |
| **XS2so** | Modul mit 2 zweikanaligen Sicherheits-Transistorausgängen |
| **XS4so** | Modul mit 4 zweikanaligen Sicherheits-Transistorausgängen |
| **XS1ro** | Modul mit 1 zweikanaligen Sicherheitsrelais |

| Typenbezeichnung | Beschreibung |
|---|---|
| XS2ro | Modul mit 2 zweikanaligen Sicherheitsrelais |

# 3.2 Funktionen und Anzeigen des XS/SC26-2




# 3.3 Verwendung von XS/SC26-2 Sicherheitskontrollern mit unterschiedlichen FIDs

Im Laufe der Zeit fügt Banner einigen Vorrichtungen neue Funktionen hinzu. Die Funktions-ID (FID) kennzeichnet die Merkmale und Funktionen, die in einem bestimmten Modell enthalten sind. Allgemein gilt, dass eine höhere FID-Nummer einem größeren Merkmalsatz entspricht. Eine Konfiguration mit einer höheren FID-Nummer wird von einem Sicherheitskontroller mit einer kleineren FID-Nummer nicht unterstützt. Funktions-IDs sind nur vorwärts kompatibel, nicht rückwärts.

XS/SC26-2-Basismodule, die unterschiedliche FIDs haben, können in derselben Anwendung verwendet werden, es müssen jedoch Schritte unternommen werden, um die Kompatibilität zu gewährleisten. Die FID-Zahl eines bestimmten Geräts kann am seitlichen Etikett auf dem Modul (Abbildung 1 auf Seite 11) abgelesen oder über die Modulinformationen des Basismoduls abgefragt werden. Damit eine Konfigurationsdatei für ein Gerät mit beliebiger FID-Zahl anwendbar ist, erstellen Sie Konfigurationen, ohne die in der folgenden Tabelle aufgeführten Funktionen zu verwenden. Überprüfen Sie alle Konfigurationen nach dem Laden auf ihre Richtigkeit.

*Abbildung 1. Beispiel für Etikett*

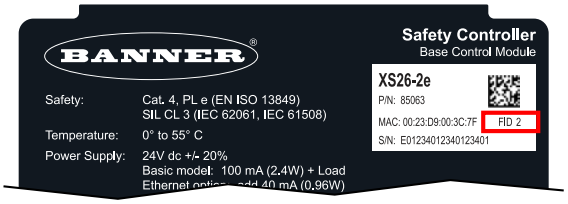


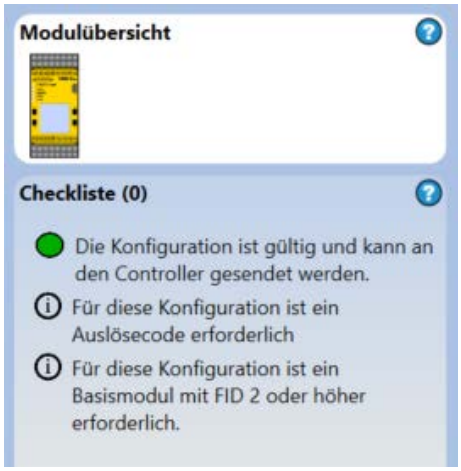

*Tabelle 4. FID-Beschreibungen*

| FID-Nummer | Zusätzliche Funktionen |
|---|---|
| FID 1 | Ursprüngliche Funktionen |
| FID 2 | PROFINET, virtuelle nicht sicherheitsrelevante Eingänge, Verzögerungsblöcke, Statusausgänge zur Verfolgung von Funktionsblöcken und eine Erweiterung von 64 auf 256 virtuelle Statusausgänge |

| FID-Nummer | Zusätzliche Funktionen |
|---|---|
| FID 3 | Funktionen gemäß Werkseinstellungen, SC-XM3-Übertragung |
| FID 4 | Hydraulischer/pneumatischer Pressensteuerungsblock, die Fähigkeit, ODER-Logik an Reset-Eingängen auszuführen, One-Shot-Zeitverlaufsblock und die Einstellung eines physischen Statusausgangs zum Ein- und Ausschalten |

Die Checkliste in der Software des Sicherheitskontroller von Banner zeigt eine Warnung an, wenn eine Funktion hinzugefügt wird, die einen Sicherheitskontroller mit einer anderen Firmware als der eines FID 1-Sicherheitskontrollers erfordert.

*Abbildung 2. Beispiel einer Checklisten-Warnung*




# 3.4 Ein- und Ausgangsanschlüsse

## 3.4.1 XS/SC26-2 Sicherheitseingangsgeräte und nicht sicherheitsrelevante Eingangsgeräte

Der Basiskontroller hat 26 Eingangsanschlüsse, die zur Überwachung entweder von Sicherheitsvorrichtungen oder von nicht sicherheitsrelevanten Vorrichtungen verwendet werden können. Diese Vorrichtungen können weitere Halbleiterausgänge oder kontaktbasierte Ausgänge enthalten. Einige der Eingangsanschlüsse können so konfiguriert werden, dass sie entweder 24 V DC für Überwachungskontakte liefern oder den Status eines Ein- oder Ausgangs signalisieren. Die Funktion der einzelnen Eingangsschaltungen hängt von der Art des angeschlossenen Geräts ab. Diese Funktion wird bei der Konfiguration des Kontrollers festgelegt.

Der Basiskontroller ab FID 2 unterstützt auch nicht sicherheitsrelevante virtuelle Eingänge.

Die Erweiterungsmodule XS8si und XS16si fügen weitere Eingänge zum Sicherheitskontroller-System hinzu.

Weitere Informationen zum Anschließen weiterer, nicht in diesem Handbuch beschriebener Geräte erhalten Sie bei Banner Engineering.

## 3.4.2 Sicherheitsausgänge am XS/SC26-2

Die Sicherheitsausgänge dienen der Ansteuerung von Endschaltgeräten (FSDs) und primären Steuerelementen der Maschine (MSPEs), bei denen es sich um die (zeitlich) letzten Komponenten in der Kette der Steuerelemente zur Steuerung der gefährlichen Maschinenbewegung handelt. Zu diesen Steuerelementen gehören Relais, Schütze, Magnetventile, Motorsteuerungen und andere Vorrichtungen, in der Regel mit zwangsgeführten (mechanisch verbundenen) Überwachungskontakten, oder für die externe Geräteüberwachung erforderlichen elektrischen Signalen.

Der Sicherheitskontroller hat zwei unabhängig gesteuerte und redundante Sicherheits-Transistorausgänge (Anschlüsse SO1a & SO1b sowie SO2a & SO2b). Der Selbstüberwachungs-Algorithmus des Sicherheitskontrollers sorgt dafür, dass die Ausgänge als Reaktion auf die zugewiesenen Eingangssignale und die Selbstüberwachungs-Testsignale des Systems zu den passenden Zeitpunkten ein- und ausschalten.

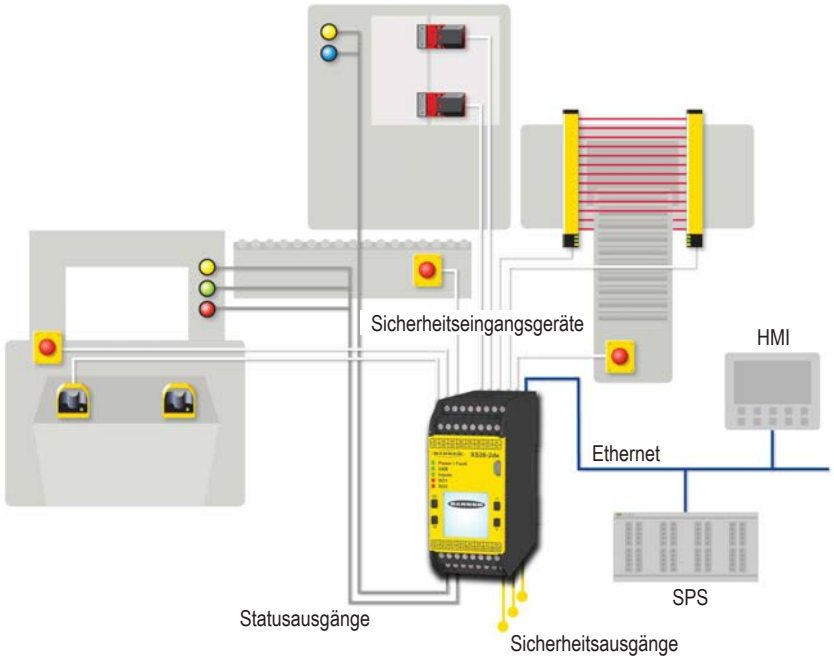
Jeder redundante Sicherheits-Transistorausgang ist so ausgelegt, dass er entweder in Paaren oder in Form von zwei einzelnen Ausgängen funktioniert. Bei der paarweisen Steuerung eignen sich die Sicherheitsausgänge für Anwendungen der Kategorie 4. Bei unabhängiger Funktion eignen sich sie sich für Anwendungen bis zur Kategorie 3, wenn ein geeigneter Fehlerausschluss durchgeführt wurde (siehe *Einkanalsteuerung* in Sicherheits-(Schutz-)Stoppschaltungen auf Seite 69 und Integrität der Sicherheitsschaltungen und Sicherheitsschaltungsprinzipien nach ISO 13849-1 auf Seite 30). Siehe Sicherheitsausgänge auf Seite 60 mit weiteren Informationen zu Anschlüssen, Sicherheits-Transis-

torausgängen und Sicherheits-Relaisausgängen, externer Geräteüberwachung, ein-/zweikanaligen Sicherheitsstoppschaltungen und zur Konfiguration von Sicherheitsausgängen.

Weitere Sicherheits-Transistorausgänge oder Sicherheits-Relaisausgänge können zu erweiterbaren Ausführungen (XS26-2xx) des Basiskontrollers durch Hinzufügen von Erweiterungs-Ausgangsmodulen (XS2so, XS4so, XS1ro und XS2ro) hinzugefügt werden. Bis zu acht Erweiterungsmodule können hinzugefügt werden, wobei beliebige Kombinationen von Eingangs- und Ausgangsmodulen möglich sind.

Die Sicherheitsausgänge können von Eingangsgeräten mit automatischem oder mit manuellem Reset gesteuert werden.

*Abbildung 3. Sicherheitsausgänge (Beispielanwendung)*




## Funktionsabschaltung gemäß IEC 60204-1 und ANSI NFPA79

Der Sicherheitskontroller kann für zwei verschiedene Arten von Funktionsabschaltungen konfiguriert werden:

- Kategorie 0: eine ungesteuerte Abschaltung mit unmittelbarer Unterbrechung der Versorgung zur überwachten Maschine
- Kategorie 1: eine gesteuerte Abschaltung mit einer Verzögerung, bevor die Versorgung zur überwachten Maschine unterbrochen wird

Abschaltungen mit Verzögerung können bei Anwendungen eingesetzt werden, bei denen Strom für einen Bremsmechanismus zum Stoppen der gefährlichen Maschinenbewegung erforderlich ist.

# 3.4.3 XS/SC26-2: Statusausgänge und virtuelle Statusausgänge

Der Basiskontroller verfügt über acht umrüstbare E/As (als IOx beschriftet), die als Statusausgänge verwendet werden können. Diese sind dann fähig, nicht sicherheitsrelevante Statussignale an Geräte wie programmierbare Steuerungen (SPS) oder Anzeigelampen zu senden. Darüber hinaus kann jeder nicht verwendete Sicherheitsausgangsanschluss so konfiguriert werden, dass er eine Statusausgangsfunktion ausführt. Dies hat den Vorteil einer höheren Stromkapazität (siehe XS/SC26-2 – Spezifikationen auf Seite 20 für weitere Informationen). Bei den Sicherheits-Transistorausgängen, die als Statusausgänge konfiguriert werden, bleiben die Sicherheitstestimpulse aktiviert, selbst wenn diese als Statusausgang designiert sind. Die Konvention des Statusausgangssignals kann so konfiguriert werden, dass sie 24 V DC, 0 V DC oder zyklisches Ein- und Ausschalten umfasst. Informationen zu den spezifischen Funktionen eines Statusausgangs finden Sie unter Signallogik für Statusausgänge auf Seite 73.

Ethernet-Ausführungen, die die Software verwenden, können für bis zu 64 virtuelle Statusausgänge auf FID 1-Basiskontrollern und für bis zu 256 virtuelle Statusausgänge auf FID 2-Basiskontrollern konfiguriert werden. Diese Ausgänge können über das Netzwerk dieselben Informationen übermitteln wie die Statusausgänge. Siehe Virtuelle Statusausgänge auf Seite 76 für weitergehende Informationen.

**WARNUNG:**

- **Die Statusausgänge und virtuellen Statusausgänge sind keine Sicherheitsausgänge und können sowohl im ein- als auch im ausgeschalteten Zustand Fehler aufweisen.**
- Wenn ein Statusausgang oder ein virtueller Statusausgang für die Steuerung einer sicherheitskritischen Anwendung verwendet wird, ist ein zu einem gefährlichen Zustand führender Ausfall möglich, der zu schweren oder tödlichen Verletzungen führen kann.
- Ein Statusausgang oder ein virtueller Statusausgang darf niemals zur Steuerung von sicherheitskritischen Anwendungen eingesetzt werden.

# 3.5 Funktion des XS/SC26-2 für die automatische Optimierung von Anschlüssen deaktivieren

Die Funktion für die automatische Optimierung von Anschlüssen (ATO) ist eine Standardfunktion bei allen XS/SC26-2-Modellen. Diese Funktion kombiniert automatisch bis zu zwei Ein-/Ausgangsanschlüsse für zwei Geräte, die +24-V-Testimpulse vom Sicherheitskontroller erfordern. Gegebenenfalls leistet die Software dies automatisch für jedes Gerätepaar, das hinzugefügt wird, bis keine Ein-/Ausgangsanschlüsse mehr verfügbar sind. Die gemeinsame Nutzung ist auf zwei Geräte begrenzt, da die verschraubbaren Anschlüsse bis zu zwei Leiter aufnehmen können.

Im Fenster „Geräteeigenschaften“ können die Anschlusszuweisungen bei Bedarf manuell geändert werden.

Die folgenden Abbildungen veranschaulichen die ATO-Funktion des XS/SC26-2 anhand der Optimierung von Anschlüssen für zwei Schutztürschalter. Insgesamt werden so sechs Anschlüsse genutzt, während ohne Verwendung der ATO-Funktion acht Anschlüsse benötigt werden. Der erste Schutztürschalter (GS1) wird hinzugefügt. Hierbei handelt es sich um einen zweikanaligen, vieradrigen Schutztürschalter, der zwei unabhängige +24-V-Impulsausgaben vom Sicherheitskontroller erfordert. IO1 wird als +24-V-Testimpuls 1 zugewiesen, der über Kanal 1 von GS1 zu IN1 übertragen wird. IO2 wird als +24-V-Testimpuls 2 zugewiesen, der über Kanal 2 von GS1 zu IN2 übertragen wird. Wenn der zweite Schutztürschalter GS2 hinzugefügt wird, verwendet dieser ebenfalls IO1 und IO2, aber die beiden Kanäle werden mit IN3 und IN4 überwacht.

*Abbildung 4. Gemeinsame Nutzung von IO1 und IO2 durch GS1 und GS2*

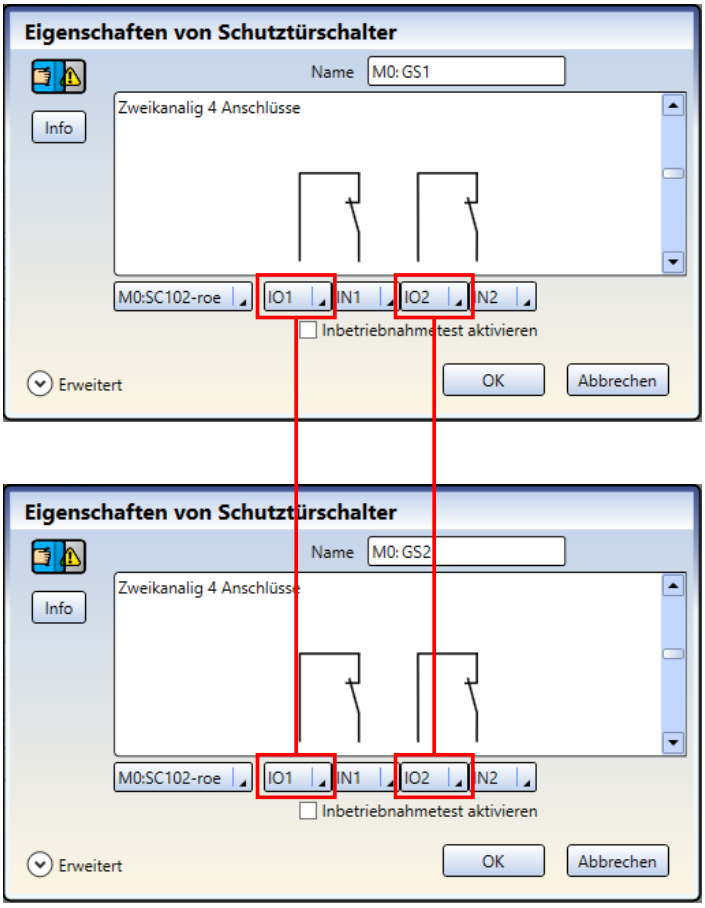
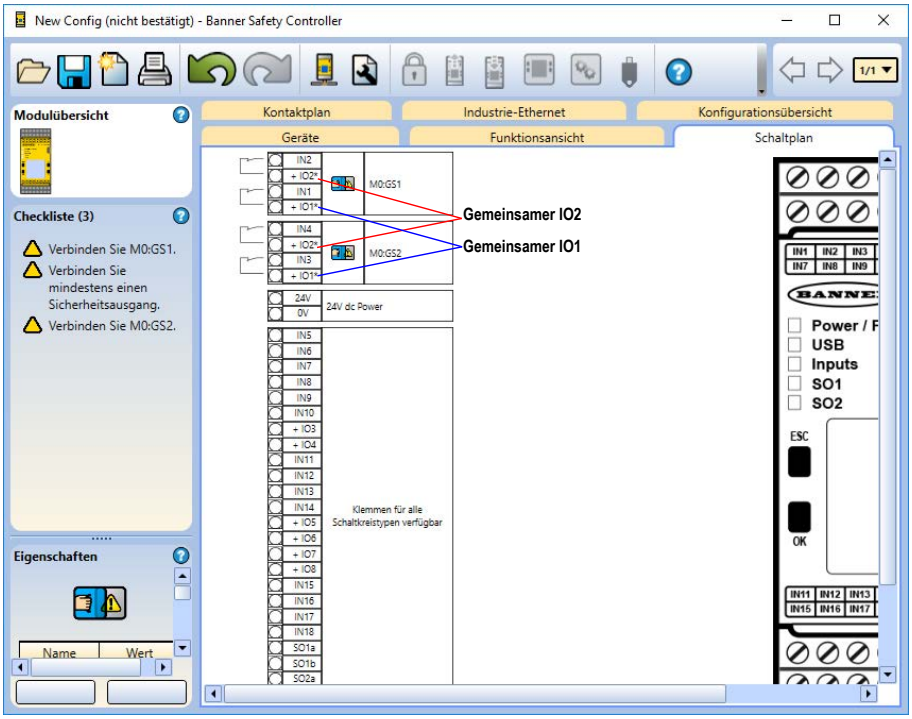


*Abbildung 5. Registerkarte **Schaltplan** – Ansicht gemeinsam genutzter Ein-/Ausgänge*



# 4 SC10-2 – Überblick

*Abbildung 6. SC10-2 – Sicherheitskontroller*



Der konfigurierbare Sicherheitsrelais-Kontroller SC10-2 ist eine einfach zu bedienende und kostengünstige Alternative zu Sicherheitsrelaismodulen. Er ersetzt die Funktionalität und die Kapazität von zwei unabhängigen Sicherheitsrelaismodulen, ist konfigurierbar, einfach in der Bedienung und bietet die erweiterten Diagnosefunktionen, die das Sicherheitskontroller-Sortiment von Banner ausmachen.

- In-Series Diagnostics (ISD) liefert detaillierte Status- und Leistungsdaten von jedem angeschlossenen Sicherheitsgerät, auf das mit einer HMI oder einem ähnlichen Gerät zugegriffen werden kann.
- Intuitive Programmierung auf Symbolbasis mit Konfiguration auf dem PC per Drag&Drop vereinfacht die Geräteeinrichtung und -verwaltung
- Unterstützt eine breite Palette von Sicherheitsvorrichtungen, wodurch der Kauf und die Bevorratung von Sicherheitsrelaismodulen für bestimmte Sicherheitsvorrichtungen überflüssig wird.
- Zwei 6-A-Sicherheitsrelaisausgänge mit je drei Schließerkontaktsätzen
- Zehn Eingänge, von denen vier als nicht sicherheitsrelevante Ausgänge verwendet werden können
- Automatische Optimierung von Anschlüssen (ATO) kann die Zahl der Eingänge von 10 auf 14 erweitern
- Bidirektionale Kommunikation über Industrie-Ethernet
  - 256 virtuelle nicht sicherheitsrelevante Statusausgänge
  - 80 virtuelle nicht sicherheitsrelevante Eingänge (Reset, Ein/Aus, Abbruch Ausschaltverzögerung, Muting-Aktivierung)
- Optionales externes Speicherlaufwerk vom Typ SC-XM3 für schnelles Austauschen und schnelle Konfiguration ohne PC (siehe SC10-2: Verwendung des SC-XM3 auf Seite 275)

## 4.1 Ausführungen des SC10-2

| Typenbezeichnung | Beschreibung |
|---|---|
| **SC10-2roe** | Konfigurierbarer Kontroller mit Sicherheitsrelais – 10 Eingänge (4 umrüstbar), 2 3-Kanal-Sicherheitsrelais-Ausgänge, Industrie-Ethernet |

## 4.2 Funktionen und Anzeigen des SC10-2

Anschlusspunkte sind Einsteckanschlüsse mit Federspanner.

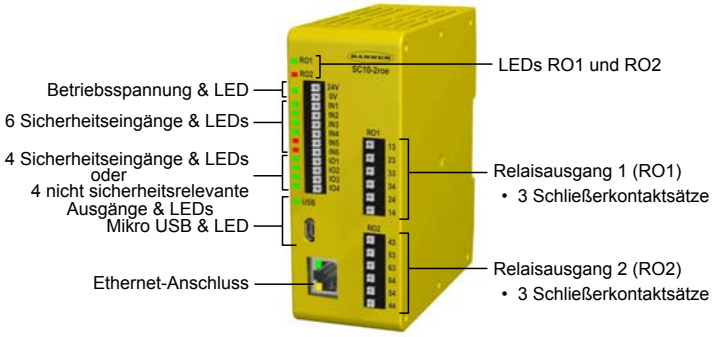
**Drahtgröße:** 24 bis 14 AWG, 0,2 mm² bis 2,08 mm²

**Wichtig:** Die Klemmenanschlüsse sind nur für 1 Leiter bestimmt. Wenn mehr als 1 Leitung an einem Anschluss verbunden wird, können sich Leitungen lockern oder vollständig lösen und Kurzschlüsse verursachen.

Verseilten Draht oder Draht mit Glatthülse verwenden. Verzinnte Drähte werden nicht empfohlen.

Nach dem Einlegen des Drahtes in den Anschluss am Draht ziehen, um zu prüfen, ob er fest sitzt. Löst sich der Draht, sollte eine andere Verdrahtungslösung in Betracht gezogen werden.

*Abbildung 7. Funktionen und Anzeigen*




# 4.3 Verwendung von SC10-2 Sicherheitskontrollern mit verschiedenen FIDs

Im Laufe der Zeit fügt Banner einigen Vorrichtungen neue Funktionen hinzu. Die Funktions-ID (FID) kennzeichnet die Merkmale und Funktionen, die in einem bestimmten Modell enthalten sind. Allgemein gilt, dass eine höhere FID-Nummer einem größeren Merkmalsatz entspricht. Eine Konfiguration mit einer höheren FID-Nummer wird von einem Sicherheitskontroller mit einer kleineren FID-Nummer nicht unterstützt. Funktions-IDs sind nur vorwärts kompatibel, nicht rückwärts.

*Abbildung 8. Beispiel für Etikett des SC10-2*

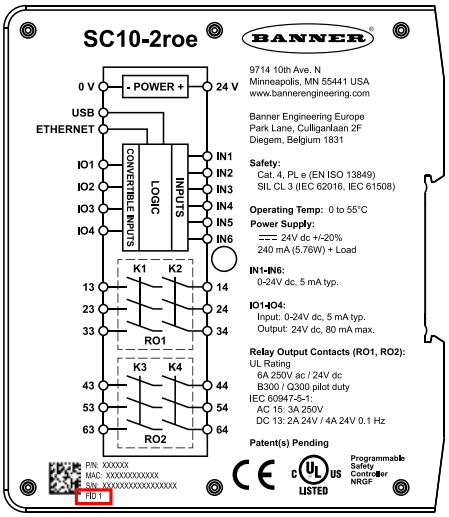
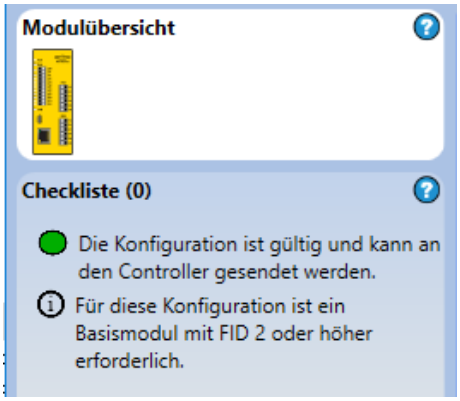



*Tabelle 5. FID-Beschreibungen*

| FID-Nummer | Zusätzliche Funktionen |
|---|---|
| FID 1 | Ursprüngliche Funktionen |
| FID 2 | Zusätzliche Fähigkeit, In-Series Diagnostic-Informationen direkt an USB- (über die Software) und Industrie-Ethernet-Protokolle zu konvertieren. |

Die Checkliste in der Software des Sicherheitskontroller von Banner zeigt eine Warnung an, wenn eine Funktion hinzugefügt wird, die einen Sicherheitskontroller mit einer anderen Firmware als der eines FID 1-Sicherheitskontrollers erfordert.

*Abbildung 9. Beispiel einer Checklisten-Warnung*




# 4.4 Ein- und Ausgangsanschlüsse

## 4.4.1 SC10-2 Sicherheitseingangsgeräte und nicht sicherheitsrelevante Eingangsgeräte

Der SC10-2 hat 10 Eingangsanschlüsse, die zur Überwachung entweder von Sicherheitsvorrichtungen oder von nicht sicherheitsrelevanten Vorrichtungen verwendet werden können. Diese Vorrichtungen können weitere Halbleiterausgänge oder kontaktbasierte Ausgänge enthalten.

Einige der Eingangsanschlüsse können so konfiguriert werden, dass sie entweder 24 V DC für Überwachungskontakte liefern oder den Status eines Ein- oder Ausgangs signalisieren. Die Funktion der einzelnen Eingangsschaltungen hängt von der Art des angeschlossenen Geräts ab. Diese Funktion wird bei der Konfiguration des Kontrollers festgelegt.

## 4.4.2 Sicherheits-Relaisausgänge am SC10-2

Der SC10-2 hat zwei dreikanalige Schließer-Sicherheitsrelaisausgänge.

Die Sicherheitsausgänge dienen der Ansteuerung von Endschaltgeräten (FSDs) und primären Steuerelementen der Maschine (MSPEs), bei denen es sich um die (zeitlich) letzten Komponenten in der Kette der Steuerelemente zur Steuerung der gefährlichen Maschinenbewegung handelt. Zu diesen Steuerelementen gehören Relais, Schütze, Magnetventile, Motorsteuerungen und andere Vorrichtungen, teils mit zwangsgeführten (mechanisch verbundenen) Überwachungskontakten, oder für die externe Geräteüberwachung (EDM) erforderlichen elektrischen Signalen.

### Funktionsabschaltung gemäß IEC 60204-1 und ANSI NFPA79

Der Sicherheitskontroller kann für zwei verschiedene Arten von Funktionsabschaltungen konfiguriert werden:

- Kategorie 0: eine ungesteuerte Abschaltung mit unmittelbarer Unterbrechung der Versorgung zur überwachten Maschine
- Kategorie 1: eine gesteuerte Abschaltung mit einer Verzögerung, bevor die Versorgung zur überwachten Maschine unterbrochen wird

Abschaltungen mit Verzögerung können bei Anwendungen eingesetzt werden, bei denen Strom für einen Bremsmechanismus zum Stoppen der gefährlichen Maschinenbewegung erforderlich ist.

## 4.4.3 Statusausgänge und virtuelle Statusausgänge am SC10-2

Mit der Software können für den SC10-2 bis zu 256 virtuelle Statusausgänge zur Übertragung von Informationen über das Netzwerk konfiguriert werden. Diese Ausgänge können nicht sicherheitsrelevante Statussignale an Geräte wie programmierbare Steuerungen (SPS) oder Mensch-Maschine-Schnittstellen (HMIs) senden. Siehe Virtuelle Statusausgänge auf Seite 76 für weitergehende Informationen.

Der SC10-2 hat vier umrüstbare E/As (als **IOx** beschriftet), die als Statusausgänge für die Direktsteuerung von Anzeigelampen oder die feste Verdrahtung mit SPS-Eingängen verwendet werden können. Diese Ausgänge kommunizieren die gleichen Informationen wie die virtuellen Statusausgänge.

**WARNUNG:**

- **Die Statusausgänge und virtuellen Statusausgänge sind keine Sicherheitsausgänge und können sowohl im ein- als auch im ausgeschalteten Zustand Fehler aufweisen.**
- Wenn ein Statusausgang oder ein virtueller Statusausgang für die Steuerung einer sicherheitskritischen Anwendung verwendet wird, ist ein zu einem gefährlichen Zustand führender Ausfall möglich, der zu schweren oder tödlichen Verletzungen führen kann.
- Ein Statusausgang oder ein virtueller Statusausgang darf niemals zur Steuerung von sicherheitskritischen Anwendungen eingesetzt werden.

Der SC10-2 ab FID 2 kann als Schnittstelle fungieren, um Daten von einer Reihe an Geräten mit integrierten ISD-Daten (In-Series Diagnostics) wie dem SI-RF-Sicherheitsschaltern über das Netzwerk zu senden.

# 4.5 Funktion des SC10-2 für die automatische Optimierung von Anschlüssen (ATO) bei externen Klemmenblöcken (ETB)

Die Funktion für die automatische Optimierung von Anschlüssen (ATO) bei externen Klemmenblöcken (ETB) ist eine Standardfunktion bei allen SC10-Modellen und ist standardmäßig aktiviert.

Die ATO-Funktion kann die 10 Anschlüsse auf dem SC10-2 so erweitern, dass dieser durch Optimierung der Anschlüsse und Verwendung von ETBs mit zusätzlichen Eingängen verwendet werden kann. Beim Hinzufügen, Löschen oder Bearbeiten von Geräten sorgt die Software automatisch für die optimale Zuweisung der Anschlüsse und ermöglicht dadurch eine minimale Verdrahtung bei maximaler Auslastung der Anschlüsse.

ATO ist eine intelligente Funktion, die beim Erstellen der Konfiguration alle verfügbaren Gerätetypen und Konfigurationsoptionen liefert. Wenn alle Eingangs- und Ein-/Ausgangsanschlüsse belegt sind und ein weiteres Gerät hinzugefügt wird, sucht ATO nach Geräten, die +24-V-Testimpulse vom Sicherheitskontroller erfordern. Diese Geräte werden über einen externen Klemmenblock (ETB) kombiniert, damit ein Ein-/Ausgangsanschluss frei wird. Jeder ETB ermöglicht es, dass bis zu drei verschiedene Geräte das +24-V-Signal eines einzelnen Eingangs/Ausgangs gemeinsam nutzen.

ATO kann auf Wunsch durch Bearbeitung der Moduleigenschaften des SC10 in der Software deaktiviert werden. ETBs sind dann weiterhin aktiv, aber Sie müssen die Ein-/Ausgangsanschlüsse nach Bedarf manuell neu zuweisen, um eine optimale Auslastung der Anschlüsse zu erzielen.

# 5 Spezifikationen und Anforderungen

## 5.1 XS/SC26-2 – Spezifikationen

### Basiskontroller und Erweiterungsmodule

**Mechanische Belastung**

**Stoßfestigkeit:** 15 *g* über 11 ms, Halbsinuswelle, 18 Stöße insgesamt (gemäß IEC 61131-2)
**Schwingungsfestigkeit:**3,5 mm gelegentlich/1,75 mm Dauerschwingungen bei 5 Hz bis 9 Hz, 1,0 *g* gelegentlich und 0,5 *g* Dauerschwingungen bei 9 Hz bis 150 Hz: alle bei 10 Durchlaufzyklen pro Achse (gemäß IEC 61131-2)

**Sicherheit**

Kategorie 4 PL e (EN ISO 13849)
SIL CL 3 (IEC 62061, IEC 61508)

**Produkt-Gütenormen**

Eine Liste der geltenden US- und internationalen Industrienormen finden Sie unter Normen und Vorschriften auf Seite 295.

**EMV**

Erfüllt oder übertrifft sämtliche EMV-Anforderungen in IEC 61131-2, IEC 62061 Anhang E, Tabelle E.1 (erhöhte Störfestigkeitsstufen), IEC 61326-1:2006 und IEC61326-3-1:2008

**Betriebsbedingungen**

**Temperatur:** 0 °C bis +55 °C (+32 °F bis +131 °F)
**Lagerungstemperatur:** –30 °C bis +65 °C (–22 °F bis +149 °F)
**Luftfeuchtigkeit:** 90 % bei +50 °C maximale relative Luftfeuchtigkeit (nicht kondensierend)
**Betriebshöhe:** maximal 2000 m (maximal 6562 ft) nach IEC 61010-1

**Schutzart**

NEMA 1 (IP20 nach IEC), für Einsatz in Gehäuse nach NEMA 3 (IP54 nach IEC) oder höher

**Abziehbare Schraubklemmen**

**Leitergröße:** 24 bis 12 AWG (0,2 bis 3,31 mm²)
**Abisolierlänge:** 7 bis 8 mm (0,275 in bis 0,315 in)
**Drehmoment:** 0,565 N·m (5,0 in-lb)

**Abziehbare Klemmenanschlüsse**

***Wichtig:*** *Die Klemmenanschlüsse sind nur für 1 Leiter bestimmt. Wenn mehr als 1 Leitung an einem Anschluss verbunden wird, können sich Leitungen lockern oder vollständig lösen und Kurzschlüsse verursachen. Wenn mehr als ein Leiter benötigt wird, sollte eine Glatthülse oder ein externer Klemmenblock verwendet werden.*
**Leitergröße:** 24 bis 16 AWG (0,20 bis 1,31 mm²)
**Abisolierlänge:** 8,00 mm (0,315 in)

**Wichtig:** Das Netzteil muss die Anforderungen für besonders niedrige Spannungen mit Schutztrennung (SELV, PELV) erfüllen.

### Sicherheitskontroller-Basismodule XS26-2 und SC26-2

**Leistung**

24 V DC ± 20 % (einschließlich Restwelligkeit), 100 mA lastfrei
**Ethernet-Ausführungen:** 40 mA aufschlagen
**Ausführungen mit Display:** 20 mA aufschlagen
**Erweiterbare Ausführungen:** maximale Bus-Last 3,6 A

**Netzwerkschnittstelle (nur Ethernet-Ausführungen)**

Ethernet 10/100 Base-T/TX, modularer RJ45-Anschluss
Wählbare automatische Aushandlung oder manuelle Rate und Duplex
Auto-MDI/MDIX (automatisches Crossover)
**Protokolle:** EtherNet/IP (mit PCCC), Modbus/TCP und PROFINET (ab FID 2)
**Daten**: 64 konfigurierbare virtuelle Statusausgänge auf FID 1-Basiskontrollern oder 256 virtuelle Statusausgänge auf Basiskontrollern ab FID 2; Fehlerdiagnosecodes und -meldungen; Zugriff auf das Fehlerprotokoll

**Umrüstbare E/A**

**Stromversorgung:** max. 80 mA (Überstromschutz)

**Funktion für die automatische Optimierung von Anschlüssen**

Bis zu 2 Geräte

**Testimpuls**

**Breite:** maximal 200 µs
**Rate:** 200 ms (typisch)

**Ausgangsschutz**

Alle Transistorausgänge (Sicherheits- und andere Ausgänge) sind gegen Kurzschlüsse zu 0 V oder +24 V geschützt, einschließlich Überstromzuständen.

**Sicherheitsklasse**

**PFH [1/h]:** 1,05 × $10^{-9}$
**Überlasttestintervall:** 20 Jahre

**Zertifizierungen**

IND. CONT. EQ. LISTED
Programmable Safety Controller 3NBN LISTED
PROFIBUS • PROFINET

**Sicherheitseingänge (und umrüstbare E/A bei Verwendung als Eingänge)**

**Eingang-EIN-Schwellenwert:** > 15 V DC (Einschaltung garantiert), max. 30 V DC
**Eingang-AUS-Schwellenwert:** < 5 V DC und < 2 mA, min. –3 V DC
**Eingang-EIN-Strom:** 5 mA typisch bei 24 V DC, 50 mA Kontaktreinigungs-Spitzenstrom bei 24 V DC
**Widerstand der Eingangsleitungen:** max. 300 Ohm (150 Ohm pro Leitung)
**Eingangsanforderungen für eine 4-adrige Sicherheitsmatte:**
- Max. Kapazität zwischen Platten: 0,22 µF
- Max. Kapazität zwischen unterer Platte und Erde: 0,22 µF
- Max. Widerstand zwischen den 2 Eingangsanschlüssen derselben Platte: 20 Ω

**Sicherheits-Transistorausgänge**

Max. 0,5 A bei 24 V DC (max. 1,0 V DC Abfall), max. 1 A Einschaltstrom
**Ausgang-AUS-Schwellenwert:** 1,7 V DC typisch (max. 2,0 V DC)
**Leckstrom im Aus-Zustand:** max. 50 µA bei 0 V offen
**Last:** max. 0,1 µF, max. 1 H, max. 10 Ω pro Last

**Ansprech- und Wiederbereitschaftszeiten**

**Ansprechzeit (vom Ende der Eingabe bis zum Ausschalten des Ausgangs):** siehe Konfigurationsübersicht in der Software, da diese variieren kann.
**Wiederbereitschaftszeit Eingang (Stopp bis Anlauf):** Einschaltverzögerung (falls eingestellt) plus 250 ms typisch (maximal 400 ms)
**Differential Einschaltung Ausgang xA zu Ausgang xB (als Paar verwendet, nicht geteilt):** max. 5 ms
**Differential Einschaltung Ausgang X zu Ausgang Y (gleicher Eingang, gleiche Verzögerung, beliebiges Modul):** 3 Scanzeiten +25 ms max.
**Zeitgeberfunktion für virtuellen Eingang (Muting-Aktivierung und Ein/Aus) (ab FID 2):** RPI + 200 ms typisch
**Zeitgeberfunktion für virtuellen Eingang (manueller Reset und Abbruchverzögerung) (ab FID 2):** Details finden Sie unter Virtuelle nicht sicherheitsrelevante Eingangsgeräte (XS/SC26-2 ab FID 2 und SC10-2) auf Seite 57.

**Ausschaltverzögerungstoleranz**

Die maximale Toleranz ist die in der Konfigurationszusammenfassung angegebene Ansprechzeit plus 0,02 %.
Die Mindesttoleranz ist die konfigurierte Ausschaltverzögerungszeit minus 0,02 % (vorausgesetzt, es liegen weder Stromausfall noch Fehler vor).

**Einschaltverzögerungstoleranz**

Die maximale Toleranz ist die konfigurierte Einschaltverzögerung plus 0,02 % plus 250 ms typisch (400 ms maximal).
Die Mindesttoleranz ist die konfigurierte Einschaltverzögerung minus 0,02 %.

## Sicherheits-Transistorausgangsmodule XS2so und XS4so

### Sicherheits-Transistorausgänge

**XS2so**: 0,75 A maximal bei 24 V DC (1,0 V DC maximaler Abfall)
**XS4so**: 0,5 A maximal bei 24 V DC (1,0 V DC maximaler Abfall)
**Einschaltstrom:** 2 A maximal
**Ausgang-AUS-Schwellenwert:** 1,7 V DC typisch (maximal 2,0 V DC)
**Leckstrom im Aus-Zustand:** maximal 50 µA bei 0 V offen
**Last:** max. 0,1 µF, max. 1 H, maximal 10 Ω je Eingangsleitung

### Sicherheitsklasse

**PFH [1/h]:** $5{,}8 \times 10^{-10}$
**Überlasttestintervall:** 20 Jahre

### Zertifizierungen

### Externe Stromversorgung

**XS2so:** 24 V DC ± 20 % (einschließlich Restwelligkeit), 0,075 A lastfrei, maximal 3,075 A unter Last
**XS4so:** 24 V DC ± 20 % (einschließlich Restwelligkeit), 0,1 A lastfrei, maximal 4,1 A unter Last
**Max. Einschaltverzögerung:** 5 Sekunden nach dem Basiskontroller
**Begrenzte Isolierung:** Maximal ±30 V DC in Bezug auf den 0-V-Anschluss des Basiskontrollers

### Bus-Versorgung

0.02 A

### Testimpuls

**Breite:** maximal 200 µs
**Rate:** 200 ms (typisch)

### Ausgangsschutz

Alle Transistorausgänge (Sicherheits- und andere Ausgänge) sind gegen Kurzschlüsse zu 0 V oder +24 V geschützt, einschließlich Überstromzuständen.

## Sicherheitsrelevante Eingangsmodule XS8si und XS16si

### Umrüstbare E/A

**Stromversorgung:** max. 80 mA bei 55 °C Umgebungstemperatur für Betrieb (mit Überstromschutz)

### Bus-Versorgung

**XS8si**: 0,07 A lastfrei, maximale Last 0,23 A
**XS16si**: 0,09 A lastfrei, maximale Last 0,41 A

### Sicherheitsklasse

**PFH [1/h]:** $4 \times 10^{-10}$
**Überlasttestintervall:** 20 Jahre

### Zertifizierungen

### Sicherheitseingänge (und umrüstbare E/A bei Verwendung als Eingänge)

**Eingang-EIN-Schwellenwert:** > 15 V DC (Einschaltung garantiert), maximal 30 V DC
**Eingang-AUS-Schwellenwert:** < 5 V DC und < 2 mA, mindestens –3 V DC
**Eingang-EIN-Strom:** 5 mA typisch bei 24 V DC, 50 mA Kontaktreinigungs-Spitzenstrom bei 24 V DC
**Widerstand der Eingangsleitungen:** max. 300 Ohm (150 Ohm pro Leitung)
**Eingangsanforderungen für eine 4-adrige Sicherheitsmatte:**
- Maximale Kapazität zwischen Platten: 0,22 µF
- Maximale Kapazität zwischen unterer Platte und Erde: 0,22 µF
- Max. Widerstand zwischen den 2 Eingangsanschlüssen derselben Platte: 20 Ω

### Ausgangsschutz

Die konvertierbaren Eingänge sind gegen Kurzschlüsse zu 0 V oder +24 V geschützt, einschließlich Überstromzuständen.

**Sicherheits-Relaismodule XS1ro und XS2ro**

**Bus-Versorgung**
**XS1ro:** 0,125 A (Ausgänge EIN)
**XS2ro:** 0,15 A (Ausgänge EIN)

**Maximale Leistung**
2000 VA, 240 W

**Lebensdauer der Elektrik**
50.000 Schaltspiele bei voller Widerstandslast

**Überspannungskategorie**
III

**Verschmutzungsgrad**
2

**Lebensdauer der Mechanik**
40.000.000 Zyklen

**Anmerkung:** Ein Überspannungsbegrenzer sollte zum Schalten induktiver Lasten integriert werden. Überspannungsbegrenzer lastübergreifend installieren. Überspannungsbegrenzer niemals ausgangskontaktübergreifend installieren.

**Sicherheitsklasse**
**PFH [1/h]:** $7{,}6 \times 10^{-10}$
**Überlasttestintervall:** 20 Jahre

**B10d-Werte**

| Spannung | Strom | B10d |
|---|---|---|
| 230 V AC | 3 A | 300,000 |
| 230 V AC | 1 A | 750,000 |
| 24 V DC | ≤ 2 A | 1,500,000 |

**Zertifizierungen**

**Nennwerte der Kontakte**
**UL/NEMA:**
- **Schließerkontakte:** 6 A 250 V AC/24 V DC ohmsch; B300/Q300 Steuerbetrieb
- **Öffnerkontakte:** 2,5 A 150 V AC/24 V DC ohmsch; Q300 Steuerbetrieb

**IEC 60947-5-1:**
- **Schließerkontakte:** 6 A 250 V AC/DC kontinuierlich; AC 15: 3 A 250 V; DC 13: 1 A 24 V/4 A 24 V 0,1 Hz
- **Öffnerkontakte:** 2,5 A 150 V AC/DC kontinuierlich; AC 15: 1 A 150 V; DC 13: 1 A 24 V/4 A 24 V 0,1 Hz

**Kontaktspannung zum Erhalt der 5-µm-AgNi-Vergoldung**

| | Minimum | Maximum |
|---|---|---|
| **Spannung** | 100 mV AC/DC | 60 V AC/DC |
| **Strom** | 1 mA | 300 mA |
| **Stromversorgung** | 1 mW (1 mVA) | 7 W (7 VA) |

**Erforderlicher Überstromschutz**

**WARNUNG:** Die elektrischen Anschlüsse müssen von qualifizierten Personen unter Beachtung der örtlichen und nationalen Gesetze und Vorschriften für elektrische Anschlüsse verbunden werden.

Überstromschutz ist erforderlich, dieser muss von der Anwendung des Endprodukts gemäß der angegebenen Tabelle bereitgestellt werden.
Der Überstromschutz kann mit externen Sicherungen oder über ein Netzteil der Klasse 2 mit Strombegrenzung bereitgestellt werden.
Stromversorgungsdrähte < 24 AWG dürfen nicht verbunden werden.
Weiteren Produktsupport erhalten Sie unter www.bannerengineering.com.

| Stromversorgungsdrähte (AWG) | Erforderlicher Überstromschutz (A) |
|---|---|
| 20 | 5,0 |
| 22 | 3.0 |
| 24 | 2.0 |
| 26 | 1.0 |
| 28 | 0.8 |
| 30 | 0.5 |

# 5.2 Spezifikationen für den SC10-2

**Leistung**
**Spannung:** 24 V DC ±20 % (SELV)
**Strom:**
Max. 240 mA, keine Last (Relais ein)
Max. 530 mA, volle Last (IO1 bis IO4 als Hilfsausgänge verwendet)

**Sicherheitseingänge (und umrüstbare E/A bei Verwendung als Eingänge)**
**Eingang-EIN-Schwellenwert:** > 15 V DC (Einschaltung garantiert), maximal 30 V DC
**Eingang-AUS-Schwellenwert:** < 5 V DC und < 2 mA, mindestens –3 V DC
**Eingang-EIN-Strom:** 5 mA typisch bei 24 V DC, 50 mA Kontaktreinigungs-Spitzenstrom bei 24 V DC
**Widerstand der Eingangsleitungen:** max. 300 Ohm (150 Ohm pro Leitung)
**Eingangsanforderungen für eine 4-adrige Sicherheitsmatte:**
- Maximale Kapazität zwischen Platten: 0,22 µF [2]
- Maximale Kapazität zwischen unterer Platte und Erde: 0,22 µF [2]
- Max. Widerstand zwischen den 2 Eingangsanschlüssen derselben Platte: 20 Ω

**Umrüstbare E/A**
**Stromversorgung:** max. 80 mA (Überstromschutz)
**Testimpulse:** ~1 ms alle 25 bis 75 ms

**Funktion für die automatische Optimierung von Anschlüssen**
Bis zu drei Geräte mit vom Anwender bereitgestellten Klemmenblöcken verbunden

**Netzwerkschnittstelle**
Ethernet 10/100 Base-T/TX, modularer RJ45-Anschluss
Wählbare automatische Aushandlung oder manuelle Rate und Duplex
Auto-MDI/MDIX (automatisches Crossover)
**Protokolle:** EtherNet/IP (mit PCCC), Modbus/TCP und PROFINET
**Daten**: 256 konfigurierbare virtuelle Statusausgänge; Fehlerdiagnosecodes und -meldungen; Zugriff auf Fehlerprotokoll

[2] Wenn die Sicherheitsmatten gemeinsam einen umrüstbaren E/A nutzen, ist dies die Gesamtkapazität aller Sicherheitsmatten, die den E/A gemeinsam nutzen.

### Ansprech- und Wiederbereitschaftszeiten

**Ansprechzeit (vom Ende der Eingabe bis zum Ausschalten des Ausgangs):** siehe Konfigurationsübersicht in der Software, da diese variieren kann.
**Wiederbereitschaftszeit Eingang (Stopp bis Anlauf):** Einschaltverzögerung (falls eingestellt) plus 250 ms typisch (maximal 400 ms)
**Zeitablauffunktion für virtuellen Eingang (Muting-Aktivierung und Ein/Aus):** RPI + 200 ms typisch
**Zeitgeberfunktion für virtuellen Eingang (manueller Reset und Abbruchverzögerung):** Details finden Sie unter Virtuelle nicht sicherheitsrelevante Eingangsgeräte (XS/SC26-2 ab FID 2 und SC10-2) auf Seite 57 .

### Ausschaltverzögerungstoleranz

Die maximale Toleranz ist die in der Konfigurationszusammenfassung angegebene Ansprechzeit plus 0,02 %.
Die Mindesttoleranz ist die konfigurierte Ausschaltverzögerungszeit minus 0,02 % (vorausgesetzt, es liegen weder Stromausfall noch Fehler vor).

### Einschaltverzögerungstoleranz

Die maximale Toleranz ist die konfigurierte Einschaltverzögerung plus 0,02 % plus 250 ms typisch (400 ms maximal).
Die Mindesttoleranz ist die konfigurierte Einschaltverzögerung minus 0,02 %.

### Sicherheitsausgänge

3 Schließerkontaktsätze für jeden Ausgangskanal (RO1 und RO2). Jeder Schließerausgang ist eine Reihenschaltung von Kontakten von zwei zwangsgeführten (mechanisch verbundenen) Relais. RO1 besteht aus Relais K1 und K2. RO2 besteht aus Relais K3 und K4.

### Kontakte

AgNi + 0,2 µm Gold

### Überspannungskategorie

Spannung von 1 V bis 150 V AC/DC am Ausgangsrelaiskontakt: Kategorie III Spannung von 151 V bis 250 V AC/DC am Ausgangsrelaiskontakt: Kategorie II (Kategorie III, wenn eine geeignete Überspannungsbegrenzung bereitgestellt wird, wie in diesem Dokument beschrieben)

### Nennstrom der einzelnen Kontakte

Bei Verwendung mehrerer Kontaktausgänge das Diagramm Temperaturabzug beachten.

| | Minimum | Maximum |
|---|---|---|
| Spannung | 10 V AC/DC | 250 V AC/24 V DC |
| Strom | 10 mA AC/DC | 6 A |
| Stromversorgung | 100 mW (100 mVA) | 200 W (2000 VA) |

### Schaltkapazität (IEC 60947-5-1)

| | |
|---|---|
| AC 15 | Schließer (NO): 250 V AC, 3 A |
| DC 13 | Schließer (NO): 24 V DC, 2 A |
| DC 13 bei 0,1 Hz | Schließer (NO): 24 V DC, 4 A |

### Betriebsbedingungen

**Temperatur:** 0 °C bis +55 °C (+32 °F bis +131 °F) (siehe Diagramm Temperaturabzug)
**Lagerungstemperatur:** –30 °C bis +65 °C (–22 °F bis +149 °F)
**Luftfeuchtigkeit:** 90 % bei +50 °C maximale relative Luftfeuchtigkeit (nicht kondensierend)
**Betriebshöhe:** maximal 2000 m (maximal 6562 ft) nach IEC 61010-1

### Schutzart

NEMA 1 (IP20 nach IEC), für Einsatz in Gehäuse nach NEMA 3 (IP54 nach IEC) oder höher

### Mechanische Belastung

**Stoßfestigkeit:** 15 g über 11 ms, Halbsinuswelle, 18 Stöße insgesamt (gemäß IEC 61131-2)
**Schwingungsfestigkeit**:3,5 mm gelegentlich/1,75 mm Dauerschwingungen bei 5 Hz bis 9 Hz, 1,0 g gelegentlich und 0,5 g Dauerschwingungen bei 9 Hz bis 150 Hz: alle bei 10 Durchlaufzyklen pro Achse (gemäß IEC 61131-2)

### Lebensdauer der Mechanik

20.000.000 Zyklen

### Lebensdauer der Elektrik

50.000 Schaltspiele bei voller Widerstandslast

### UL Hilfsnutzleistung

B300 Q300

### B10d-Werte

| Spannung | Strom | B10d |
|---|---|---|
| 230 V AC | 2 A | 350,000 |
| 230 V AC | 1 A | 1,000,000 |
| 24 V DC | ≤ 4 A | 10,000,000 |

### Einsteckanschlüsse mit Federspanner

**Drahtgröße:** 24 bis 14 AWG, 0,2 mm² bis 2,08 mm²

**Wichtig:** Die Klemmenanschlüsse sind nur für 1 Leiter bestimmt. Wenn mehr als 1 Leitung an einem Anschluss verbunden wird, können sich Leitungen lockern oder vollständig lösen und Kurzschlüsse verursachen.

Verseilten Draht oder Draht mit Glatthülse verwenden. Verzinnte Drähte werden nicht empfohlen.

Nach dem Einlegen des Drahtes in den Anschluss am Draht ziehen, um zu prüfen, ob er fest sitzt. Löst sich der Draht, sollte eine andere Verdrahtungslösung in Betracht gezogen werden.

### EMV

Erfüllt oder übertrifft sämtliche EMV-Anforderungen für Störfestigkeit nach IEC 61326-3-1:2012 und Emissionen nach CISPR 11:2004 für Geräte der Gruppe 1, Klasse A

**Anmerkung:** Ein Überspannungsbegrenzer sollte zum Schalten induktiver Lasten integriert werden. Überspannungsbegrenzer lastübergreifend installieren. Überspannungsbegrenzer niemals ausgangskontaktübergreifend installieren (siehe Warnhinweis).

### Sicherheit

Kategorie 4 PL e (EN ISO 13849)
SIL CL 3 (IEC 62061, IEC 61508)

### Sicherheitsklasse

**PFH [1/h]:** $5{,}01 \times 10^{-10}$
**Überlasttestintervall:** 20 Jahre

### Produkt-Gütenormen

Eine Liste der geltenden US- und internationalen Industrienormen finden Sie im Abschnitt Normen und Vorschriften auf Seite 295.

### Zertifizierungen

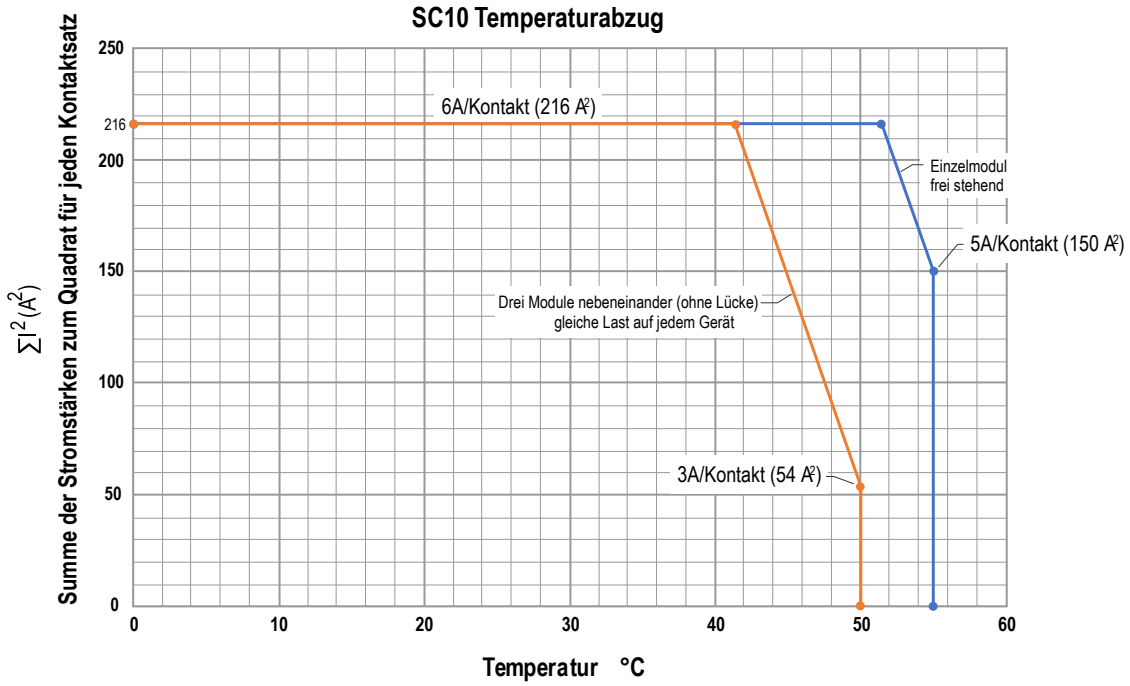
### Erforderlicher Überstromschutz

**WARNUNG:** Die elektrischen Anschlüsse müssen von qualifizierten Personen unter Beachtung der örtlichen und nationalen Gesetze und Vorschriften für elektrische Anschlüsse verbunden werden.

Überstromschutz ist erforderlich, dieser muss von der Anwendung des Endprodukts gemäß der angegebenen Tabelle bereitgestellt werden.
Der Überstromschutz kann mit externen Sicherungen oder über ein Netzteil der Klasse 2 mit Strombegrenzung bereitgestellt werden.
Stromversorgungsdrähte < 24 AWG dürfen nicht verbunden werden.
Weiteren Produktsupport erhalten Sie unter www.bannerengineering.com.

| Stromversorgungsdrähte (AWG) | Erforderlicher Überstromschutz (A) |
|---|---|
| 20 | 5,0 |
| 22 | 3.0 |
| 24 | 2.0 |
| 26 | 1.0 |
| 28 | 0.8 |
| 30 | 0.5 |

*Abbildung 10. SC10-2 Temperaturabweichung*




| Beispiel für die Berechnung des Temperaturabzugs | |
|---|---|
| **Einzelnes Gerät, frei stehend** | **Drei Module** |
| $\sum I^2 = I_1{}^2 + I_2{}^2 + I_3{}^2 + I_4{}^2 + I_5{}^2 + I_6{}^2$ | $\sum I^2 = I_1{}^2 + I_2{}^2 + I_3{}^2 + I_4{}^2 + I_5{}^2 + I_6{}^2$ (alle sechs Module) |
| $I_1$ = 4 A (Schließerausgang RO1 Kanal 1) | $I_1$ = 4 A |
| $I_2$ = 4 A (Schließerausgang RO1 Kanal 2) | $I_2$ = 4 A |
| $I_3$ = 4 A (Schließerausgang RO1 Kanal 3) | $I_3$ = 4 A |
| $I_4$ = 4 A (Schließerausgang RO2 Kanal 4) | $I_4$ = 4 A |
| $I_5$ = 4 A (Schließerausgang RO2 Kanal 5) | $I_5$ = 4 A |
| $I_6$ = 4 A (Schließerausgang RO2 Kanal 6) | $I_6$ = 4 A |

| Beispiel für die Berechnung des Temperaturabzugs | |
|---|---|
| **Einzelnes Gerät, frei stehend** | **Drei Module** |
| $\sum I^2 = 4^2 + 4^2 + 4^2 + 4^2 + 4^2 + 4^2 = 96\ A^2$ | $\sum I^2 = 4^2 + 4^2 + 4^2 + 4^2 + 4^2 + 4^2 = 96\ A^2$ |
| $T_{max} = 55\ °C$ | $T_{max} = 46\ °C$ |

# 5.3 Abmessungen

Alle Maße sind in Millimetern (Zoll) aufgeführt, sofern nichts anderes angegeben ist.

*Abbildung 11. XS/SC26-2 Basismodul – Abmessungen*

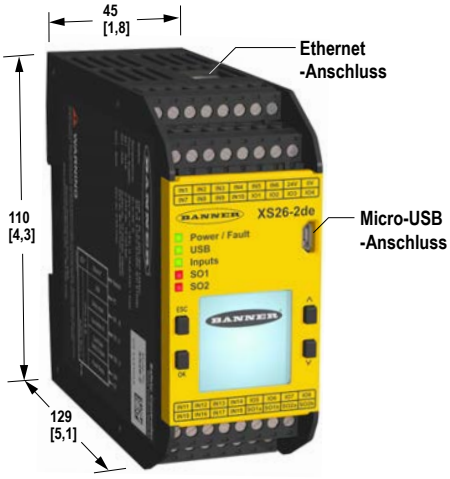



*Abbildung 12. Erweiterungsmodul – Abmessungen*

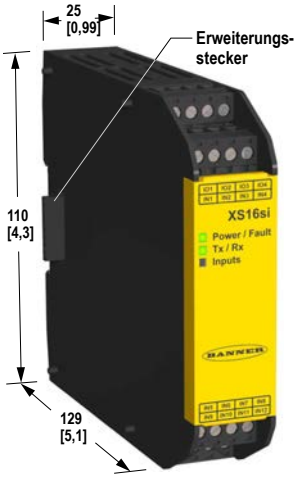
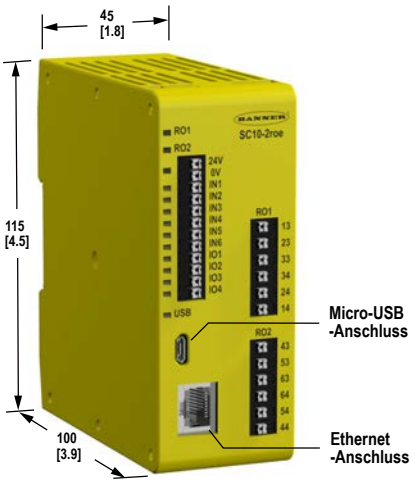



*Abbildung 13. Abmessungen des SC10-2*




# 5.4 Systemvoraussetzungen für den PC

**Wichtig:** Für die Treiberinstallation des Sicherheitskontrollers sind Administratorrechte erforderlich (für die Kommunikation mit dem Kontroller erforderlich).

**Betriebssystem:** Microsoft Windows 7, Windows 8 (außer Windows RT) oder Windows 10 [3]

**Systemverschlüsselungstyp:** 32-Bit, 64-Bit

[3] Microsoft und Windows sind eingetragene Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

| | |
|---|---|
| **Festplattenspeicher:** | 80 MB (plus bis zu 280 MB für Microsoft .NET 4.0, falls es nicht bereits installiert ist) |
| **Arbeitsspeicher (RAM):** | Mindestens 512 MB, mindestens 1 GB empfohlen |
| **Prozessor:** | Mindestens 1 GHz, 2 GHz+ empfohlen |
| **Bildschirmauflösung:** | Farbbildschirm mit mindestens 1024 × 768 Pixeln, Farbbildschirm mit 1650 × 1050 Pixeln empfohlen |
| **Drittanbietersoftware:** | Microsoft .NET 4.0 (im Installationsprogramm enthalten), PDF-Anzeigeprogramm (z. B. Adobe Acrobat) |
| **USB-Port:** | USB 2.0 (kein Konfigurationsaufwand erforderlich) |

# 6 Systeminstallation

## 6.1 Installation der Software

**Wichtig:** Für die Treiberinstallation des Sicherheitskontrollers sind Administratorrechte erforderlich (für die Kommunikation mit dem Kontroller erforderlich).

1. Laden Sie die neueste Version der Software hier herunter: www.bannerengineering.com/safetycontroller.
2. Navigieren Sie zu der heruntergeladenen Datei und öffnen Sie sie.
3. Klicken Sie auf **Weiter**, um den Installationsvorgang zu starten.
4. Bestätigen Sie den Zielspeicherort für die Software und die Verfügbarkeit für Benutzer und klicken Sie auf **Weiter**.
5. Klicken Sie auf **Weiter**, um die Software zu installieren.
6. Je nach den Systemeinstellungen wird möglicherweise ein Popup-Fenster eingeblendet, in dem Sie gefragt werden, ob Sie zulassen möchten, dass der Sicherheitskontroller von Banner Änderungen an Ihrem Computer vornimmt. Klicken Sie auf **Ja**.
7. Klicken Sie auf **Schließen**, um das Installationsprogramm zu beenden.

Öffnen Sie **Sicherheitskontroller von Banner** vom **Arbeitsplatz** oder vom **Start-Menü** aus.

## 6.2 Installation des Sicherheitskontrollers

Um einen zuverlässigen Betrieb zu gewährleisten, dürfen die Betriebsdaten nicht überschritten werden. Das Gehäuse muss eine entsprechende Wärmeabstrahlung ermöglichen, so dass die Temperatur der Luft rund um den Sicherheitskontroller die maximale Betriebstemperatur des Sicherheitskontrollers nicht überschreiten kann (siehe Spezifikationen und Anforderungen auf Seite 20).

**Wichtig:** Montieren Sie den Sicherheitskontroller an einem geeigneten Ort, d. h. dort, wo keine starken Erschütterungen auftreten.

**VORSICHT:** Elektrostatische Entladungen (ESD) können Schäden an elektronischen Geräten verursachen. Um dies zu verhindern, sollten Sie die geeigneten Praktiken für den Umgang mit elektrostatischen Entladungen beachten: Tragen Sie z. B. ein zugelassenes Erdungsarmband oder berühren Sie vor dem Umgang mit den Modulen einen geerdeten Gegenstand. Weitere Informationen über den Umgang mit elektromagnetischen Entladungen finden Sie in ANSI/ESD S20.20.

### 6.2.1 Montageanleitung

Der Sicherheitskontroller wird auf einer genormten 35-mm-DIN-Schiene montiert. Er muss in einem Gehäuse der Schutzart NEMA 3 (IEC IP54) oder besser untergebracht werden. Er sollte auf einer vertikalen Fläche mit den Belüftungsschlitzen auf der Unter- und Oberseite montiert werden, um die natürliche Konvektionskühlung zu ermöglichen.

Die Montageanleitung ist zu beachten, damit der Sicherheitskontroller nicht beschädigt wird.

**Montage** des Programmierbarer Sicherheitskontroller SC26-2, programmierbarer Sicherheitskontrollers XS26-2, Sicherheits-Transistorausgangsmodule XS2so und XS4so, Sicherheitseingangsmodule XS8si und XS16si, Sicherheitsrelaismodule XS1ro und XS2ro und Sicherheitskontroller SC10-2::

1. Kippen Sie die Oberseite des Moduls leicht rückwärts und setzen Sie das Modul auf die DIN-Schiene.
2. Richten Sie das Modul gerade über der Schiene aus.
3. Senken Sie das Modul auf die Schiene ab.

**Entfernen** des Programmierbarer Sicherheitskontroller SC26-2, programmierbarer Sicherheitskontrollers XS26-2, Sicherheits-Transistorausgangsmodule XS2so und XS4so, Sicherheitseingangsmodule XS8si und XS16si, Sicherheitsrelaismodule XS1ro und XS2ro und Sicherheitskontroller SC10-2::

1. Drücken Sie die Unterseite des Moduls nach oben.
2. Kippen Sie die Oberseite des Moduls leicht nach vorn.
3. Senken Sie das Modul ab, sobald sich die obere feste Klemme von der DIN-Schiene gelöst hat.

**Anmerkung:** Entfernen eines Erweiterungsmoduls: Ziehen Sie die anderen Module auf jeder Seite des gewünschten Moduls auseinander, um die Bus-Anschlüsse freizulegen.

# 7 Überlegungen vor der Installation

## 7.1 Geeignete Anwendung

Die korrekte Anwendung des Sicherheitskontrollers hängt von der Art der Maschine und den Schutzeinrichtungen ab, für die eine Schnittstelle mit dem Kontroller hergestellt werden muss. **Falls Bedenken bestehen, ob die Maschine mit diesem Kontroller kompatibel ist, wenden Sie sich bitte an Banner Engineering.**

**WARNUNG: Keine eigenständige Schutzeinrichtung**

Dieses Banner-Gerät gilt als Zusatzgerät und dient zur Verstärkung der Schutzeinrichtungen, mit denen Gefahrenquellen für Personen eingeschränkt oder beseitigt werden, ohne dass dafür eine Aktion durch eine Person erforderlich ist **Der Verzicht auf geeignete Schutzeinrichtungen für Gefahren aufgrund einer Risikobeurteilung, der lokalen Vorschriften und der entsprechenden Standards kann zu schweren bis tödlichen Verletzungen führen.**

**WARNUNG: Der Anwender ist für den sicheren Einsatz dieses Geräts verantwortlich**

Die in diesem Dokument beschriebenen Anwendungsbeispiele beziehen sich auf allgemeine Schutzsituationen. Jede Schutzanwendung stellt ihre eigenen, spezifischen Anforderungen.

Alle Sicherheitsanforderungen müssen erfüllt und alle Montageanweisungen befolgt werden. Bei Fragen zum Thema technische Schutzmaßnahmen stehen die Schutztechniker von Banner unter den Rufnummern bzw. Adressen zur Verfügung, die in diesem Dokument aufgeführt sind.

**WARNUNG: Lesen Sie vor Installation des Systems sorgfältig diesen Abschnitt durch**

Der Sicherheitscontroller von Banner ist ein Steuergerät, das normalerweise zusammen mit der Schutzeinrichtung einer Maschine verwendet wird. Wie gut er diese Funktion ausführen kann, hängt von der Eignung der Anwendung, der vorschriftsmäßigen mechanischen und elektrischen Installation des Sicherheitscontrollers und dem Anschluss an die zu überwachende Maschine ab.

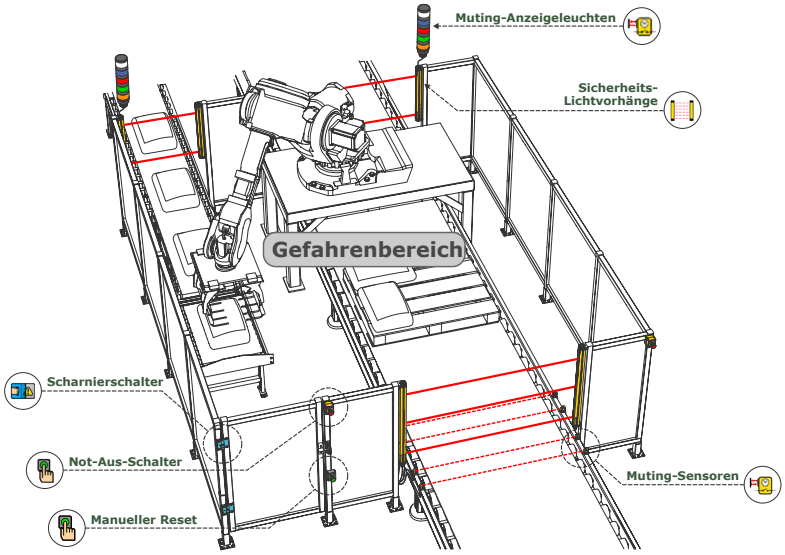
Werden nicht alle Verfahren bei der Montage, Installation, beim Anschließen und der Überprüfung vorschriftsmäßig eingehalten, so kann der Banner-Sicherheitscontroller nicht den Schutz bieten, für den er ausgelegt ist. Der Anwender ist für die Einhaltung aller lokalen und nationalen Gesetze, Vorschriften und Bestimmungen hinsichtlich der Installation und des Einsatzes dieses Steuersystems bei jeder individuellen Anwendung verantwortlich. Sämtliche Sicherheitsanforderungen müssen erfüllt und alle in diesem Dokument enthaltenen technischen Installations- und Wartungsanweisungen müssen befolgt werden.

## 7.2 Anwendungen des XS/SC26-2

Der Sicherheitskontroller kann überall dort verwendet werden, wo Sicherheitsmodule eingesetzt werden. Der Sicherheitskontroller eignet sich gut für vielfältige Arten von Anwendungen, insbesondere:

- Zweihandsteuerung mit Muting-Funktion
- Roboter-Schweiß-/Bearbeitungszellen mit Zweizonen-Muting
- Materialtransportanwendungen, bei denen mehrere Eingänge und Überbrückungsfunktionen erforderlich sind
- Drehbare Beladestationen mit manueller Beschickung
- Anwendungen mit mehreren Zweihandsteuerungsstationen
- Lean Manufacturing
- Dynamische Überwachung von Einzel- oder Doppelmagnetventilen oder Drucksicherheitsventilen

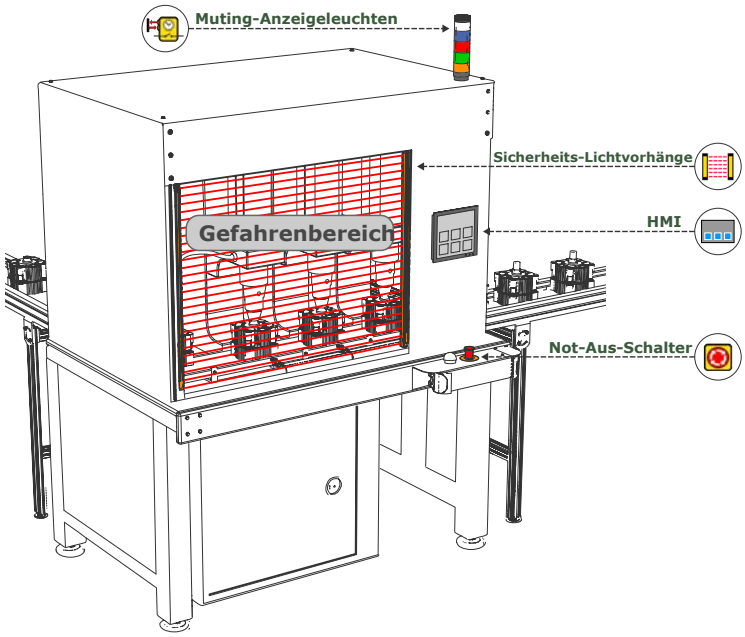
*Abbildung 14. Anwendungsbeipiel: Roboterzelle*



# 7.3 Anwendungen des SC10-2

Der Sicherheitskontroller SC10-2 ist ideal für alle Maschinen kleiner bis mittlerer Größe, die normalerweise zwei unabhängige Sicherheitsrelaismodule verwenden würden.

*Abbildung 15. Anwendungsbeispiel für den SC10-2*




# 7.4 Sicherheitseingangsgeräte

Der Sicherheitskontroller überwacht den Status der Sicherheitseingangsgeräte, die mit dem Kontroller verbunden sind. Generell schaltet sich der Sicherheitsausgang ein bzw. bleibt eingeschaltet, wenn alle Eingangsgeräte, die für die Steuerung eines bestimmten Sicherheitsausgangs konfiguriert wurden, im Ein-Zustand sind. Wenn mindestens eines der Sicherheitseingangsgeräte vom Ein-Zustand in den Aus-Zustand wechselt, schaltet sich der Sicherheitseingang aus. Einige spezielle Funktionen von Sicherheitseingangsgeräten können unter vordefinierten Umständen vorübergehend das Stoppsignal des Sicherheitseingangs aufheben, damit der Sicherheitsausgang eingeschaltet bleibt. Hierzu gehören beispielsweise Muting und Umgehung.

Der Sicherheitskontroller kann Eingangsfehler bei bestimmten Eingangsschaltungen erfassen, die anderenfalls zum Verlust der Steuerung der Sicherheitsfunktion führen würden. Wenn derartige Fehler erfasst werden, schaltet der Sicherheitskontroller die zugehörigen Ausgänge aus, bis die Fehler beseitigt wurden. Die in der Konfiguration verwendeten Funktionsblöcke wirken sich auf die Sicherheitsausgänge aus. Die Konfiguration muss beim Auftreten von Fehlern bei Eingangsgeräten sorgfältig überprüft werden.

Folgende Methoden können unter anderem verwendet werden, um die Wahrscheinlichkeit derartiger Fehler auszuschließen oder minimal zu halten:

- Physikalische Trennung der Anschlussleitungen voneinander und von sekundären Energiequellen.
- Verlegung der Anschlussleitungen in separaten Kabelwegen, -schutzrohren oder -kanälen
- Unterbringung aller Steuerungselemente (Sicherheitskontroller, Anschlussmodule, FSDs und MPSEs) nebeneinander auf einer Schalttafel und direkte Verbindung der Elemente untereinander mit kurzen Leitungen.
- Ordnungsgemäße Installation von mehradrigen Kabeln und mehreren Leitern, die durch Zugentlastungsklemmen verlegt werden. Zu starkes Anziehen einer Entlastungsklemme kann Kurzschluss an diesem Punkt verursachen.
- Verwendung von Komponenten mit Zwangsöffnung oder Direktantrieb gemäß der Beschreibung in IEC 60947-5-1, die im Zwangsführungsmodus installiert werden
- Regelmäßige Überprüfung der Funktionstüchtigkeit/Sicherheitsfunktion
- Schulung der Bedienpersonen, des Wartungspersonals und anderer Personen, die mit der Bedienung der Maschine und dem Schutz zu tun haben, damit diese sämtliche Störungen erfassen und unverzüglich beheben können

**Anmerkung:** Beachtung der Installations-, Bedienungs- und Wartungsanleitung des Herstellers sowie sämtlicher geltenden Vorschriften Bei Fragen zu den an den Sicherheitskontroller angeschlossenen Geräten wenden Sie sich an Banner Engineering.

*Abbildung 16. Position der Eingangs- und Ausgangsanschlüsse am XS/SC26-2*

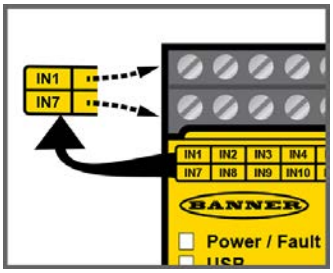
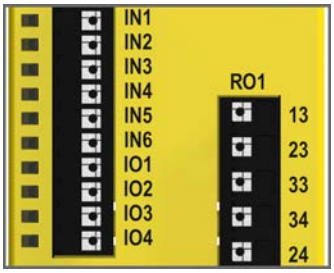



*Abbildung 17. Position der Eingangs- und Ausgangsanschlüsse am SC10-2*




**WARNUNG: Eingangsgerät und Sicherheitsstufe**

Der Sicherheitskontroller kann zahlreiche verschiedene Sicherheitseingangsgeräte überwachen. Der Benutzer muss eine Risikobeurteilung der Schutzanwendung durchführen, um zu ermitteln, welche Sicherheitsstufe erreicht werden muss und wie die Eingangsgeräte folglich korrekt an den Sicherheitskontroller angeschlossen werden müssen. Der Benutzer muss außerdem Maßnahmen ergreifen, um mögliche Eingangssignalfehler oder -störungen zu beseitigen oder zu minimieren, die zum Verlust der Sicherheitsfunktionen führen könnten.

# 7.4.1 Integrität der Sicherheitsschaltungen und Sicherheitsschaltungsprinzipien nach ISO 13849-1

Sicherheitsschaltungen umfassen die sicherheitsrelevanten Funktionen einer Maschine, die die Gefahrstufe minimieren. Diese sicherheitsrelevanten Funktionen können einen Maschinenanlauf verhindern, eine Maschinenbewegung anhalten oder eine Gefahr beseitigen. Das Versagen einer sicherheitsrelevanten Funktion oder ihrer zugehörigen Sicherheitsschaltung ergibt normalerweise eine erhöhte Gefahrstufe.

Die Integrität einer Sicherheitsschaltung hängt von mehreren Faktoren ab, u. a. Fehlertoleranz, Risikominderung, zuverlässigen und bewährten Komponenten, bewährten Sicherheitsprinzipien sowie anderen Konstruktionserwägungen.

Je nach der mit der Maschine oder ihrem Betrieb verbundenen Gefahrstufe muss ein geeignetes Maß an Integrität der Sicherheitsschaltungen (Leistung) in diese Konstruktion aufgenommen werden. Folgende Normen gehen näher auf Sicherheitsleistungsstufen ein: ANSI B11.19 Performance Criteria for Safeguarding (Leistungskriterien für Schutzeinrichtungen) und ISO 13849-1 Sicherheitsrelevante Teile eines Kontrollsystems.

## Sicherheitsstufen von Sicherheitsschaltungen

Sicherheitsschaltungen wurden in internationalen und europäischen Normen in Kategorien und Leistungsstufen unterteilt, je nach ihrer Fähigkeit, ihre Integrität im Falle eines Versagens zu bewahren, sowie der statistischen Wahrscheinlichkeit eines solchen Versagens. ISO 13849-1 geht näher auf die Integrität von Sicherheitsschaltungen ein und beschreibt die Schaltungsarchitektur bzw. -struktur (Kategorien) sowie die erforderliche Leistungsstufe (Performance Level, PL) von Sicherheitsfunktionen unter vorhersehbaren Bedingungen.

In den USA wird die normale Integritätsstufe von Sicherheitsschaltungen als „Steuerungszuverlässigkeit“ bezeichnet. Steuerungszuverlässigkeit umfasst normalerweise redundante Steuerungs- und selbstüberwachende Schaltkreise und wird in etwa mit ISO 13849-1, Kategorie 3 oder 4 und/oder der Leistungsstufe „d“ oder „e“ gleichgesetzt (siehe ANSI B11.19).

Führen Sie eine Risikobewertung durch, um die geeignete Anwendung, korrekte Anschlüsse und Risikominderung zu überprüfen (siehe ANSI B11.0 oder ISO 12100). Die Risikobewertung muss ausgeführt werden, um die geeignete Integrität der Sicherheitsschaltung zu ermitteln, mit der gewährleistet wird, dass die erwartete Risikominderung erreicht wird. Diese Risikobewertung muss alle örtlichen Vorschriften und einschlägigen Normen berücksichtigen, z. B. die US-Normen zur Steuerungszuverlässigkeit oder die europäischen Normen der Stufe „C“.

Die Eingänge des Sicherheitskontrollers sind für Anschlüsse bis einschließlich Kategorie 4 PL e (ISO 13849-1) und Sicherheitsstufe 3 (IEC 61508 und IEC 62061) ausgelegt. Die tatsächliche Sicherheitsstufe der Schaltungen hängt von der Konfiguration, der korrekten Installation der externen Schaltungen und Art und Installation der Sicherheitseingangsgeräte ab. Es liegt in der Verantwortung des Benutzers, die Schutzart(en) der Gesamtkonfiguration zu ermitteln und für die vollständige Konformität mit sämtlichen Vorschriften und Normen zu sorgen.

Die folgenden Abschnitte beziehen sich nur auf Anwendungen der Kategorien 2, 3 und 4 gemäß ISO 13849-1. Die Schaltungen der Eingangsgeräte in der nachfolgenden Tabelle werden häufig in Schutzanwendungen verwendet. Andere Lösungen sind jedoch je nach Fehlerausschluss und Risikobeurteilung ebenfalls möglich. Die nachfolgende Tabelle zeigt die Schaltungen der Eingangsgeräte und die jeweils mögliche Sicherheitsstufe, wenn sämtliche Anforderungen der Fehlererkennung und des Fehlerausschlusses erfüllt sind.

**WARNUNG: Risikobeurteilung**

Die Sicherheitsstufe von Sicherheitsschaltungen kann durch Gestaltung und Montage von Sicherheitsgeräten und Anschlussart dieser Geräte stark beeinflusst werden. **Um die passende Sicherheitsstufe der Sicherheitsschaltungen zu bestimmen, muss eine Risikobeurteilung vorgenommen werden. Dadurch soll sichergestellt werden, dass die erwartete Risikominderung erreicht und alle relevanten Vorschriften und Standards erfüllt werden.**

**WARNUNG:** Eingangsgeräte mit zwei Kontakteingängen und 2 oder 3 Anschlüssen

Erkennung eines Kurzschlusses zwischen zwei Eingangskanälen (Kontakteingänge, jedoch keine antivalenten Kontakte) ist nicht möglich, wenn beide Kontakte geschlossen sind. Ein Kurzschluss kann erfasst werden, wenn sich der Eingang mindestens 2 Sekunden lang im Aus-Zustand befindet (siehe Tipp zu **INx- und IOx-Eingangsanschlüssen** in Optionen für Sicherheitseingangsgeräte auf Seite 33).

**WARNUNG:**

- **Eingangskurzschlüsse der Kategorien 2 oder 3**
- Es ist nicht möglich, einen Kurzschluss zwischen zwei Eingangskanälen (Kontakteingänge, aber keine komplementären Kontakte) zu erfassen, wenn diese über dieselbe Quelle versorgt werden (z. B. dieselbe Klemme vom Sicherheitskontroller bei einem Zweikanalanschluss mit 3 Anschlussklemmen, oder von einer externen 24-V-Versorgung) und wenn beide Kontakte geschlossen sind.
- Ein derartiger Kurzschluss kann nur erfasst werden, wenn beide Kontakte offen sind und der Kurzschluss mindestens 2 Sekunden lang andauert.

## Fehlerausschluss

Ein wichtiger Begriff in den Anforderungen von ISO 13849-1 ist die Wahrscheinlichkeit des Auftretens eines Fehlers. Diese kann mit einer Methode verringert werden, die als „Fehlerausschluss“ bezeichnet wird. Dies basiert auf der Begründung, dass die Möglichkeit bestimmter genau definierter Fehler durch Konstruktion, Installation oder technische Möglichkeiten so weit gesenkt werden kann, dass die übrigen Fehler weitgehend vernachlässigbar sind – bzw. bei der Risikobeurteilung „ausgeschlossen“ werden können.

Der Fehlerausschluss ist ein Instrument, das Konstrukteure bei der Entwicklung der sicherheitsrelevanten Teile des Steuersystems und beim Risikobewertungsprozess verwenden können. Mit dem Fehlerausschluss kann der Konstrukteur die Möglichkeit mehrerer Fehler ausschließen und dies mit dem Risikobeurteilungsprozess begründen, um die gewünschte Sicherheitsleistung gemäß den Anforderungen von ISO 13849-1/-2 zu erzielen.

Die Anforderungen für die Sicherheit von Sicherheitsschaltungen in Schutzanwendungen (d. h. Steuerungszuverlässigkeit oder Kategorie/Leistungsstufe) gemäß ISO 13849-1 variieren erheblich. Banner Engineering empfiehlt für jede Anwendung immer das höchste Maß an Sicherheit. Dennoch liegt es in der Verantwortung des Benutzers, jedes Sicherheitssystem sicher zu installieren, zu betreiben und zu warten und alle geltenden Gesetze und Vorschriften zu beachten.

**WARNUNG: Risikobeurteilung**

Die Sicherheitsstufe von Sicherheitsschaltungen kann durch Gestaltung und Montage von Sicherheitsgeräten und Anschlussart dieser Geräte stark beeinflusst werden. **Um die passende Sicherheitsstufe der Sicherheitsschaltungen zu bestimmen, muss eine Risikobeurteilung vorgenommen werden. Dadurch soll sichergestellt werden, dass die erwartete Risikominderung erreicht und alle relevanten Vorschriften und Standards erfüllt werden.**

# 7.4.2 Eigenschaften von Sicherheitseingangsgeräten

Der Sicherheitskontroller wird über die Software konfiguriert, um viele Arten von Sicherheitseingangsgeräten zu unterstützen. Siehe Hinzufügen von Eingängen und Statusausgängen auf Seite 78 für weitere Informationen über die Konfiguration der Eingangsgeräte.

## Reset-Logik: Manueller oder automatischer Reset

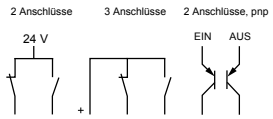
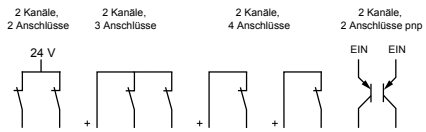
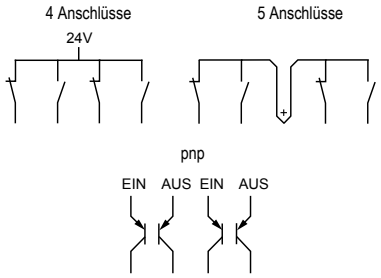
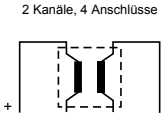
Ein manueller Reset kann für Sicherheitseingangsgeräte erforderlich sein, indem ein Latch-Reset-Block verwendet oder ein Sicherheitsausgang für einen Latch-Reset konfiguriert wird, damit die von ihnen gesteuerten Sicherheitsausgänge erst nach einem Latch-Reset wieder einschalten können. Dies wird gelegentlich als „Verriegelungsmodus“ bezeichnet, weil der Sicherheitsausgang im Aus-Zustand verriegelt wird, bis ein Reset ausgeführt wird. Wenn ein Sicherheitseingangsgerät für automatischen Reset-Modus (bzw. „Schaltmodus“) konfiguriert wird, schalten die von ihm gesteuerten Sicherheitsausgänge wieder ein, wenn das Eingangsgerät in den Ein-Zustand wechselt (vorausgesetzt, dass alle anderen Steuereingänge ebenfalls im Ein-Zustand sind).

## Anschluss von Eingangsgeräten

Der Sicherheitskontroller muss wissen, welche Gerätesignalleitungen an welche Anschlussklemmen angeschlossen werden, damit er die richtigen Signalüberwachungsmethoden, Ein - und Ausschaltregeln, Zeitregeln und Fehlerregeln anwenden kann. Die Anschlussklemmen werden während des Konfigurationsvorgangs automatisch zugewiesen und können über das die Software manuell geändert werden.

## Arten von Signalzustandsänderungen

Zwei Arten von Zustandsänderungen (COS) können bei der Überwachung der Signale von zweikanaligen Sicherheitseingangsgeräten verwendet werden: simultan oder nicht simultan.

| Eingangsschaltung | Zeitregelung für Zustandsänderung des Eingangssignals | |
|---|---|---|
| | **Aus-Zustand: Sicherheitsausgang schaltet sich aus, wenn [4]:** | **Ein-Zustand: Sicherheitsausgang schaltet sich ein, wenn [5]:** |
| **Zweikanalig A und B antivalent**<br> | Mindestens 1 Kanaleingang (A oder B) ist im Aus-Zustand. | **Simultan:** A und B sind beide im Aus-Zustand und schalten dann beide innerhalb von 3 s, bevor sich die Ausgänge einschalten, in den Ein-Zustand.<br>**Nicht simultan:** A und B schalten beide gleichzeitig in den Aus-Zustand und schalten dann beide nicht simultan in den Ein-Zustand, um die Ausgänge einzuschalten. |
| **Zweikanalig A und B**<br> | | |
| **Zweikanalig A und B 2x antivalent**<br> | Mindestens 1 Kanal (A oder B) eines Kontaktpaars im Aus-Zustand. | **Simultan:** A und B sind gleichzeitig im Aus-Zustand, dann schalten beide Kontakte in einem Kanal innerhalb von 400 ms (bei Zweihandsteuerung 150 ms) in den Ein-Zustand; beide Kanäle befinden sich innerhalb von 3 s (bei Zweihandsteuerung 0,5 s) im Ein-Zustand.<br>**Simultan:** A und B sind gleichzeitig im Aus-Zustand, dann schalten die Kontakte innerhalb eines Kanals innerhalb von 3 Sekunden in den Ein-Zustand. Die Schaltung von Kanal A und Kanal B muss nicht unbedingt simultan erfolgen. |
| **4-adrige Sicherheitsmatte**<br> | Eine der folgenden Bedingungen ist erfüllt:<br>• Eingangskanäle untereinander kurzgeschlossen (Normalbetrieb)<br>• Mindestens ein Kabel ist gelöst<br>• Einer der offenen Kanäle wird als geschlossen erfasst<br>• Einer der geschlossenen Kanäle wird als offen erfasst | Jeder Kanal ist mit seinen eigenspezifischen Impulsen behaftet. |

## Signal-Entprellzeiten

**Ausschaltentprellzeiten (von 6 ms bis 1000 ms in 1-ms-Intervallen, außer 6 ms bis 1500 ms bei Muting-Sensoren).** Die Ausschaltentprellzeit ist das erlaubte Zeitlimit für das Eingangssignal, um vom EIN- Zustand (24 VDC) in den endgültigen AUS- Zustand (0 VDC) überzugehen. Dieses Zeitlimit muss in Fällen, bei denen starke Gerätevibrationen, Aufprallstöße oder Schaltstörungen zu längeren Signalübergangszeiten führen, eventuell erhöht werden. Wenn die Entprellzeit unter diesen rauen Bedingungen zu kurz eingestellt ist, kann das System einen Signaldisparitätsfehler erkennen und in einen Sperrzustand eintreten. Die Standardeinstellung ist 6 ms.

[4] Sicherheitsausgänge schalten sich aus, wenn einer der steuernden Eingänge im Aus-Zustand ist.
[5] Sicherheitsausgänge schalten sich nur ein, wenn alle steuernden Eingänge im Ein-Zustand sind und nachdem ein manueller Reset ausgeführt worden ist (wenn mindestens einer dieser Sicherheitseingänge für manuellen Reset konfiguriert wurde und in seinem Aus-Zustand war).

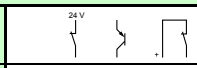
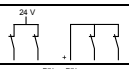
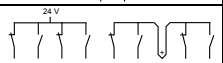
**VORSICHT: Entprellzeit und Ansprechzeit**

**Änderungen der Entprellzeit können die Ansprechzeit des Sicherheitsausgangs (um abzuschalten) beeinträchtigen.** Dieser Wert wird für jeden Sicherheitsausgang berechnet und dargestellt, wenn eine Konfiguration erstellt wird.

**Einschaltentprellzeiten (von 10 ms bis 1000 ms in 1-ms-Intervallen, außer 10 ms bis 1500 ms bei Muting-Sensoren).** Die Einschaltentprellzeit ist das erlaubte Zeitlimit für das Eingangssignal, um vom Aus- Zustand (0 V DC) in den endgültigen Ein-Zustand (24 V DC) überzugehen. Dieses Zeitlimit muss in Fällen, bei denen starke Gerätevibrationen, Aufprallstöße oder Schaltstörungen zu längeren Signalübergangszeiten führen, eventuell erhöht werden. Wenn die Entprellzeit unter diesen rauen Bedingungen zu kurz eingestellt ist, kann das System einen Signaldisparitätsfehler erkennen und in einen Sperrzustand eintreten. Die Standardeinstellung ist 50 ms.

# 7.5 Optionen für Sicherheitseingangsgeräte

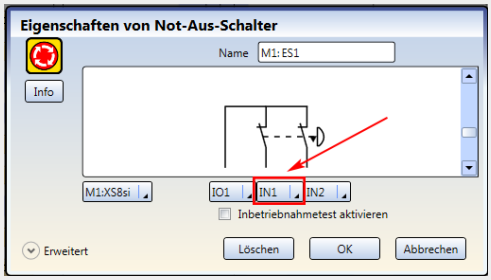
*Abbildung 18. Eingangsgeräteschaltungen – Sicherheitskategorien (Anleitung)*

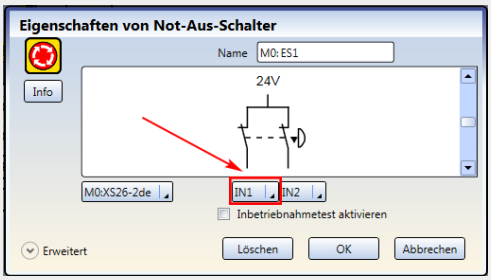
| Allgemeine Schaltungssymbole | | Schaltungen im Ein-Zustand abgebildet | | | | | | | Schaltungen im Stopp-Zustand abgebildet | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | ES | GS | OS | RP | PS | SM | ISD | THC | ED |
| **1 und 2 Anschlüsse 1 Kanal** (siehe Anmerkung 1) |   | Kat. 2 | Kat. 2 | Kat. 2 | Kat. 2 | Kat. 2 | | | | |
| **2 und 3 Anschlüsse 2 Kanäle** (siehe Anmerkung 2) |   | Kat. 3 | Kat. 3 | Kat. 3 | Kat. 3 | Kat. 3 | | | Typ IIIa Kat. 1<br>Typ IIIb Kat. 3 | Kat. 3 |
| **2 Anschlüsse 2 Kanäle PNP mit integrierter Überwachung** (siehe Anmerkung 3) |   | Kat. 4 | Kat. 4 | Kat. 4 | Kat. 4 | Kat. 4 | | Kat. 4 | Typ IIIa Kat. 1 | Kat. 4 |
| **3 und 4 Anschlüsse 2 Kanäle** (siehe Anmerkungen 2 und 4) |  | Kat. 4 | Kat. 4 | Kat. 4 | Kat. 4 | Kat. 4 | | | Typ IIIa Kat. 1<br>Typ IIIb Kat. 3 | Kat. 4 |
| **2 und 3 Anschlüsse 2 Kanäle Antivalent** |   | | Kat. 4 | Kat. 4 | Kat. 4 | Kat. 4 | | | | Kat. 4 |
| **2 Anschlüsse 2 Kanäle Antivalenter PNP-Ausgang** |   | | Kat. 4 | Kat. 4 | Kat. 4 | Kat. 4 | | | | Kat. 4 |
| **4 und 5 Anschlüsse 2 Kanäle Antivalent** |   | | Kat. 4 | | | | | | Typ IIIc Kat. 4 | Kat. 4 |
| **4 Anschlüsse, 2 Kanäle Antivalenter PNP-Ausgang** |   | | Kat. 4 | | | | | | Typ IIIc Kat. 4 | Kat. 4 |
| **Sicherheitsmatte mit 4 Anschlüssen** |  | | | | | | Kat. 3 | | | |

**WARNUNG: Unvollständige Informationen** – Viele Überlegungen im Zusammenhang mit der Installation sind für den sachgemäßen Einsatz von Eingabegeräten erforderlich, werden jedoch nicht in diesem Dokument behandelt. **Daher sind die entsprechenden Installationshinweise zum Gerät zu beachten, um einen sicheren Einsatz des Gerätes zu gewährleisten.**

**WARNUNG:** Diese Tabelle enthält eine Liste der höchstmöglichen Sicherheitskategorien für gängige sicherheitsrelevante Eingangsgeräteschaltungen. Sind die in den nachfolgenden Anmerkungen angegebenen zusätzlichen Anforderungen aufgrund von Beschränkungen der Sicherheitsvorrichtung oder der Installation nicht möglich, oder sind beispielsweise alle Anschlussklemmen des IOx-Eingangs am Sicherheitskontroller in Gebrauch, ist die höchste Sicherheitskategorie möglicherweise nicht möglich.

**Tipp: INx- und IOx-Eingangsanschlussklemmen**: Diese Schaltungen können manuell so konfiguriert werden, dass sie die Anforderungen für Schaltungen der Kategorie 4 erfüllen. Hierzu wird die erste Standardeingangsklemme (INx, am weitesten links) in eine beliebige verfügbare konvertierbare Klemme (IOx) geändert, siehe unten. Diese Schaltungen erfassen Kurzschlüsse zu anderen Stromquellen und zwischen Kanälen, wenn sich der Eingang seit mindestens 2 Sekunden im Aus-Zustand befindet.




**Anmerkungen:**

1. Die Schaltung erfüllt normalerweise die Anforderungen bis ISO 13849-1, Kategorie 2, wenn Eingangsgeräte sicherheitsrelevant sind und Verdrahtungspraktiken mit Fehlerausschluss Folgendes verhindern: a) Kurzschlüsse zwischen den Kontakten oder Transistorvorrichtungen und b) Kurzschlüsse zu anderen Stromquellen.
2. Schaltungen erfüllen normalerweise die Anforderungen für ISO 13849-1, Kategorie 3, wenn die Eingangsgeräte sicherheitsrelevant sind (siehe oben, **Tipp: INx- und IOx-Eingangsklemmen**).
   Die 2-Klemmen-Schaltung erfasst einen Einzelkanalkurzschluss zu anderen Stromquellen, wenn sich die Kontakte öffnen und wieder schließen (Gleichzeitigkeitsfehler).
   Die 3-Klemmen-Schaltung erfasst einen Kurzschluss zu anderen Stromquellen unabhängig davon, ob die Kontakte geöffnet oder geschlossen sind.
3. Die Schaltung erfüllt normalerweise die Anforderungen bis ISO 13849-1, Kategorie 4, wenn Eingangsgeräte sicherheitsrelevant sind und die interne Überwachung der pnp-Ausgänge leisten, um Folgendes zu erfassen: a) Kurzschlüsse zwischen Kanälen und b) Kurzschlüsse zu anderen Stromquellen.
4. Schaltungen erfüllen die Anforderungen für ISO 13849-1, Kategorie 4, wenn die Eingangsgeräte sicherheitsrelevant sind (siehe oben, **Tipp: INx- und IOx-Eingangsklemmen**). Diese Schaltungen können sowohl Kurzschlüsse zu anderen Stromquellen als auch Kurzschlüsse zwischen Kanälen erfassen.

## 7.5.1 Sicherheitsstufen von Sicherheitsschaltungen

Die Anforderungen an die Steuerungszuverlässigkeit oder Sicherheitskategorie per ISO 13849-1 bei der Anwendung von Verriegelungsvorrichtungen variieren stark. Während Banner Engineering bei jeder Anwendung immer die höchste Sicherheitsstufe empfiehlt, liegt es in der Verantwortung des Anwenders, jedes Sicherheitssystem sicher zu installieren, einzusetzen und zu warten und alle geltenden Gesetze und Bestimmungen zu erfüllen.

Die Sicherheitsleistung (Sicherheitsstufe) muss das Risiko der bei der Risikobeurteilung ermittelten Gefahren der Maschine mindern. Unter Integrität der Sicherheitsschaltungen und Sicherheitsschaltungsprinzipien nach ISO 13849-1 auf Seite 30 finden Sie eine Orientierung dazu, ob die Anforderungen gemäß ISO 13849-1 implementiert werden müssen.

## 7.5.2 Not-Aus-Schalter

Die Sicherheitseingänge des Sicherheitskontrollers können zur Überwachung von Nothaltschaltern verwendet werden.

**WARNUNG:**
- **Not-Aus-Geräte weder muten noch überbrücken**
- Bei Muting oder Überbrücken der Sicherheitsausgänge wird die Not-Aus-Funktion unwirksam.
- Gemäß ANSI B11.19, NFPA 79 und IEC/EN 60204-1 muss die Nothaltfunktion ständig aktiv bleiben.

**WARNUNG:**
- **Konfiguration entspricht den anwendbaren Normen**
- Wenn die Anwendung nicht entsprechend überprüft wird, können schwere oder tödliche Verletzungen die Folge sein.
- Die Software für den Sicherheitskontroller von Banner prüft primär die Logikkonfiguration auf Verbindungsfehler. Der Benutzer ist dafür verantwortlich, dass die Anwendung die Anforderungen an die Risikobewertung erfüllt und allen geltenden Normen entspricht.

**WARNUNG:**
- **Reset-Routine erforderlich**
- Wird ein Neuanlauf der Maschine ohne Betätigung des normalen Startbefehls bzw. der normalen Startvorrichtung nicht verhindert, so kann ein unsicherer Zustand entstehen. Die Folge könnten schwere Verletzungen oder Tod sein.
- Lassen Sie nicht einen Neuanlauf der Maschine ohne Betätigung des normalen Startbefehls bzw. der normalen Startvorrichtung nicht zu. Führen Sie die Reset-Routine aus, nachdem Sie die Ursache für einen Stoppzustand beseitigt haben. Beachten Sie dabei die US- und internationalen Normen.

Zusätzlich zu den in diesem Abschnitt aufgeführten Anforderungen müssen Konstruktion und Installation der Nothaltvorrichtung NFPA 79 oder ISO 13850 entsprechen. Die Stoppfunktion muss entweder ein Funktionsstopp der Kategorie 0 oder eine Funktion der Kategorie 1 sein (siehe NFPA 79).

## Anforderungen für Not-Aus-Schalter

Der Nothaltschalter muss einen oder zwei Sicherheitskontakte enthalten, die bei betriebsbereitem Schalter geschlossen sind. Bei der Aktivierung muss der Nothaltschalter alle seine sicherheitsrelevanten Kontakte öffnen, und für die Rückkehr in die betriebsbereite Position (Kontakte geschlossen) muss eine absichtliche Handlung erforderlich sein (z. B. Drehen, Ziehen oder Aufschließen). Der Schaltertyp muss ein Zwangsöffner (bzw. Direktöffner) gemäß IEC 60947-5-1 sein. Eine auf besagte Taste (oder besagten Schalter) angewandte mechanische Kraft wird direkt auf die Kontakte übertragen und erzwingt dadurch ihre Öffnung. Dadurch wird sichergestellt, dass sich die Schalterkontakte jedes Mal öffnen, wenn der Schalter aktiviert wird.

In den Normen NFPA 79, ANSI B11.19, IEC/EN 60204-1 und ISO 13850 werden zusätzliche Anforderungen an Nothalt-Schaltvorrichtungen spezifiziert, u. a.:
- Not-Aus-Schalter müssen an jedem Bedienstand und anderen Bedientafeln angebracht sein, wo eine Notabschaltung benötigt wird.
- Aus- und Not-Aus-Schalter müssen von jedem Bedienstand und jeder Bedientafel aus, an denen sie angebracht sind, jederzeit betätigt werden können. **Not-Aus-Schalter dürfen nicht gemutet oder überbrückt werden.**
- Auslöseschalter für Not-Aus-Vorrichtungen müssen die Farbe Rot aufweisen. Der Hintergrund in der unmittelbaren Umgebung des Auslöseschalters für die Vorrichtung muss die Farbe Gelb aufweisen. Durch Druck- oder Schlag ausgelöste Not-Aus-Schalter müssen als Pilz- oder Grobhandtaster ausgeführt sein.
- Der Nothaltschalter muss selbstverriegelnd sein.

**Anmerkung:** Bei manchen Anwendungen kann es notwendig sein, weitere Vorschriften zu beachten. Der Anwender ist für die Erfüllung sämtlicher relevanten Vorschriften verantwortlich.

**Anmerkung:** Für beleuchtete Nothalttaster mit ISD von Banner ist auch SC10-2: ISD-Eingänge auf Seite 46 zu beachten, da die Vorrichtung als vom ISD-Eingang ausgewählter Nothaltschalter hinzugefügt wird.

# 7.5.3 Seilzugschalter (Kabelzugschalter)

Für Seilzug-(Kabelzug)-Nothaltschalter werden Stahldrahtseile verwendet. Diese Schalter ermöglichen dauerhaft Nothaltbetätigungen über eine Distanz wie z. B. entlang eines Fließbands.

Für Seilzug-(Kabelzug)-Nothaltschalter gelten viele derselben Anforderungen wie für Nothalt-Drucktaster, wie zum Beispiel der direkte (zwangsgeführte) Betrieb entsprechend der Beschreibung in IEC 60947-5-1. Siehe Not-Aus-Schalter auf Seite 34 für weitere Informationen.

Bei Nothaltschalter-Anwendungen müssen die Seilzugschalter die Fähigkeit besitzen, nicht nur auf einen Seilzug in eine beliebige Richtung anzusprechen, sondern auch auf einen Durchhang oder Riss des Seils zu reagieren. Nothalt-Seilzugschalter müssen außerdem über eine Verriegelungsfunktion verfügen, die nach der Betätigung einen manuellen Reset erfordert.

## Richtlinien für die Installation von Seilzugschaltern (Kabelzugschaltern)

In den Normen ANSI NFPA 79, ANSI B11.19, IEC/EN 60204-1 und ISO 13850 werden die Anforderungen an Not-Aus-Schalter für Seilzugschalter- (Kabelzugschalter-) Installationen spezifiziert, u. a.:
- Seilzugschalter (Kabelzugschalter) müssen dort installiert werden, wo die Not-Ausschaltung benötigt wird.
- Seilzugschalter (Kabelzugschalter) müssen dauerhaft betriebsbereit, leicht sichtbar und gut zugänglich sein. Muting oder Überbrückung nicht zulässig
- Seilzugschalter (Kabelzugschalter) müssen eine konstante Spannung des Seil- bzw. Kabelzugs aufweisen.
- Der Seil- oder Kabelzugschalter sowie etwaige Kennzeichnungen, müssen die Farbe Rot aufweisen.
- Der Seil- bzw. Kabelzugschalter muss fähig sein, auf eine Kraft in einer beliebigen Richtung anzusprechen.
- Der Schalter muss folgende Bedingungen erfüllen:
  - Er muss eine Selbstverriegelungsfunktion aufweisen, die nach der Betätigung einen manuellen Reset erfordert.

- Er muss für den Direktöffnungsbetrieb ausgelegt sein.
- Er muss einen Durchhang oder Riss des Seils bzw. Kabels melden.

**Weitere Richtlinien für die Installation:**

- Der Seil- bzw. Kabelzugschalter muss gut zugänglich sein, für Not-Aus-Funktionen die Farbe Rot aufweisen und auf seiner gesamten Länge sichtbar sein. Kennzeichen dürfen am Seil bzw. Kabel befestigt werden, um dessen Sichtbarkeit zu erhöhen.
- Montagestellen, einschließlich Halterungen, müssen fest sein und um das Seil bzw. Kabel herum genügend Platz frei lassen, damit dieses gut zugänglich ist.
- Das Seil bzw. Kabel muss über alle Halterungen reibungsfrei laufen. Es werden Seilrollen empfohlen. Möglicherweise ist eine Schmierung erforderlich. Eine Kontamination des Systems, etwa durch Verschmutzung, Metallspäne oder Feilstaub usw., muss verhindert werden, da diese den Betrieb beeinträchtigen könnte.
- Verwenden Sie nur Seilrollen (keine Hebeösen), wenn das Seil um Ecken geführt wird oder wenn die Richtung geändert wird – auch bei geringfügigen Richtungsänderungen.
- Verlegen Sie das Seil bzw. Kabel niemals durch Rohre.
- Befestigen Sie niemals Gewichte am Seil
- Eine Anlagefeder wird empfohlen, um die Konformität mit der richtungsunabhängigen Betätigung des Seilzugs bzw. Kabelzugs zu gewährleisten. Diese muss auf der Lastträgerstruktur installiert werden (Maschinenrahmen, Wand usw.).
- Die Temperatur wirkt sich auf die Seilspannung aus. Das Seil bzw. Kabel dehnt sich aus (wird länger), wenn die Temperatur steigt, und zieht sich zusammen (wird kürzer), wenn die Temperatur sinkt. Bei signifikanten Temperaturschwankungen muss die Spannungseinstellung häufig überprüft werden.

**WARNUNG:** Bei Nichtbeachtung der Installationsanleitung und der Installationsverfahren wird die Funktion des Seil- bzw. Kabelzugschaltersystems möglicherweise unwirksam oder fällt aus. Dies könnte einen unsicheren Zustand mit schweren bis tödlichen Verletzungen als Folge bedingen.

## 7.5.4 Zustimmtaster

Ein Zustimmtaster ist ein manuell bedientes Steuergerät, das bei dauernder Betätigung zusammen mit einem Startschalter das Anlaufen eines Maschinenzyklus zulässt. Für die Konstruktion und Anwendung von Zustimmtastern gelten unter anderem die folgenden Normen: ISO 12100-1/-2, IEC 60204-1, ANSI/NFPA 79, ANSI/RIA R15.06 und ANSI B11.19.

Der Zustimmtaster steuert aktiv die Aufhebung eines Stoppsignals während eines Abschnitts des Maschinenbetriebs, bei dem eine Gefahrsituation eintreten kann. Der Zustimmtaster ermöglicht einem gefährlichen Maschinenteil zu laufen, darf ihn aber nicht starten. Ein Zustimmtaster kann einen oder mehrere Sicherheitsausgänge steuern. Wenn das Aktivierungssignal vom Aus-Zustand in den Ein-Zustand schaltet, wechselt der Sicherheitskontroller in den Freigabe-Modus. Zum Starten einer gefährlichen Maschinenbewegung ist ein separates Maschinenbefehlsignal von einer anderen Vorrichtung erforderlich. **Bei Verwendung muss dieser Zustimmtaster die letztendliche Befugnis zum Abschalten oder Stoppen der gefährlichen Maschinenbewegung haben.**

## 7.5.5 Schutzhalt (Sicherheitsstopp)

Ein Schutzhalt (Sicherheitsstopp) ist für den Anschluss unterschiedlicher Vorrichtungen vorgesehen, zu denen Schutzeinrichtungen und Zusatzeinrichtungen gehören können. Diese Stoppfunktion ist eine Art der Betriebsunterbrechung, die eine geregelte Bewegungseinstellung zu Schutzzwecken zulässt. Die Funktion kann automatisch oder manuell aktiviert und zurückgesetzt werden.

### Anforderungen für Schutzhalt (Sicherheitsstopp)

Die erforderliche Sicherheitsstufe von Sicherheitsschaltungen wird durch eine Risikobeurteilung ermittelt und ergibt die zulässige Sicherheitskategorie, z. B. Kategorie 4, Steuerungszuverlässigkeit (siehe Integrität der Sicherheitsschaltungen und Sicherheitsschaltungsprinzipien nach ISO 13849-1 auf Seite 30). Die Schutzhalt-Schaltung muss die gesicherte Gefahrstelle überwachen, indem sie gefährliche Maschinenbewegungen anhält und die Versorgung zu den Maschinenantrieben unterbricht. Hierbei handelt es sich gewöhnlich um eine funktionelle Abschaltung der Kategorie 0 oder Kategorie 1 entsprechend ANSI NFPA 79 und IEC 60204-1.

## 7.5.6 Verriegelte Schutzeinrichtung bzw. Schutztür

Die Sicherheitseingänge des Sicherheitskontrollers können zur Überwachung von elektrisch verriegelten Schutzeinrichtungen oder Schutztüren eingesetzt werden.

## Anforderungen an Sicherheitsschalter

Die folgenden allgemeinen Anforderungen und Erwägungen betreffen die Installation von Verriegelungsvorrichtungen und Schutztüren. Daneben sind die geltenden Vorschriften zu beachten, um sicherzustellen, dass alle Anforderungen erfüllt werden.

Gefährliche Maschinen, die durch die Schutzeinrichtung gesichert werden, müssen am Betrieb gehindert werden, solange die Schutzeinrichtung nicht geschlossen ist. Wenn die Schutzeinrichtung öffnet, während eine Gefahr vorliegt, muss ein Stoppbefehl an die überwachte Maschine geschickt werden. Durch das Schließen der Schutzeinrichtung allein darf die gefährliche Maschinenbewegung nicht initiiert werden. Dazu muss ein separater Vorgang erforderlich sein. Die Sicherheitsschalter dürfen nicht als mechanischer Anschlag oder für die Endlagen-Abschaltung verwendet werden.

Die Schutzeinrichtung muss in ausreichender Entfernung vom Gefahrenbereich aufgestellt werden (damit die gefährliche Maschinenbewegung anhalten kann, bevor die Schutzeinrichtung soweit öffnet, um Zugang zur Gefahrstelle zu ermöglichen). Sie muss sich entweder seitwärts oder von der Gefahrstelle weg öffnen und nicht in den überwachten Bereich hinein. Es sollte außerdem die Möglichkeit ausgeschlossen werden, dass sich die Schutzeinrichtung selbst schließt und den Verriegelungsschaltkreis aktiviert. Darüber hinaus muss die Installation verhindern, dass Personal über, unter, durch oder um die Schutzeinrichtung herum greifen und die überwachte Gefahrstelle erreichen kann. Öffnungen in der Schutzeinrichtung dürfen den Zugang zur Gefahrstelle nicht erlauben (siehe OSHA 29CFR1910.217 Tabelle O-10, ANSI B11.19, ISO 13857, ISO14120/EN953 oder die geeignete Norm). Die Schutzeinrichtung muss stark genug sein, um ein Austreten der Gefahren aus dem überwachten Bereich durch Auswerfen, Herunterfallen oder Ausgabe durch die Maschine zu verhindern.

Die Sicherheitsschalter, Auslöseschalter, Sensoren und Magneten müssen so gebaut und installiert werden, dass sie nicht leicht umgangen werden können. Sie müssen sicher befestigt werden, so dass sich ihre physische Position nicht verschieben kann. Hierzu sind zuverlässige Befestigungsmittel zu verwenden, die nicht ohne Werkzeug entfernt werden können. Die Montageschlitze in den Gehäusen dienen lediglich der ersten Einstellung. Die Endmontagebohrungen müssen für die permanente Befestigung verwendet werden.

**WARNUNG: Bereichssicherungsanwendungen**

Wenn die Anwendung eine Hintertretungsgefahr bewirken könnte (z. B. bei Bereichssicherung), müssen entweder die Schutzeinrichtung oder die Haupt-Stoppsteuerungen/MPSEs der überwachten Maschine infolge eines Stoppbefehls eine Verriegelung mit Wiederanlaufsperre bewirken (z. B. die Unterbrechung des Erfassungsfeldes eines Lichtvorhangs, oder die Öffnung eines durch einen Sicherheitsschalter geschützten Tors bzw. Schutzes). Die Zurücksetzung dieses Verriegelungszustands kann nur durch Betätigung eines Reset-Schalters erreicht werden, der von den normalen Vorrichtungen zur Initiierung des Maschinenzyklus getrennt ist. Der Schalter muss der Beschreibung in diesem Dokument entsprechend positioniert werden.

Es können Lockout/Tagout-Verfahren (Verriegeln/Kennzeichnen) gemäß ANSI Z244.1 erforderlich sein oder es muss eine zusätzliche Schutzeinrichtung gemäß den Sicherheitsanforderungen in ANSI B11 oder anderen geltenden Normen verwendet werden, wenn eine Hintertretungsgefahr nicht beseitigt oder auf ein Risiko von akzeptablem Ausmaß gesenkt werden kann. **Wenn diese Anweisungen nicht befolgt werden, können schwere oder tödliche Verletzungen die Folge sein.**

# 7.5.7 Optosensor

Die Sicherheitseingänge des Sicherheitskontrollers können verwendet werden, um die Vorrichtungen auf optischer Basis zu überwachen, bei denen die Erfassung mithilfe von Licht erfolgt.

## Anforderungen für Optosensoren

Für die Verwendung als Schutzeinrichtungen werden Optosensoren in der Norm IEC 61496-1/-2/-3 als aktive optoelektronische Schutzvorrichtungen (AOPD) und auf diffuse Reflexion ansprechende aktive optoelektronische Schutzvorrichtungen (AOPDDR) beschrieben.

AOPDs umfassen Sicherheits-Lichtvorhänge und Einstrahl- oder Mehrstrahl-Sicherheitslichtschranken. Diese Geräte erfüllen in der Regel die Anforderungen für Bauarten des Typs 2 oder des Typs 4. Eine Vorrichtung vom Typ 2 darf gemäß ISO 13849-1 in einer Anwendung der Kategorie 2 verwendet werden, und eine Vorrichtung vom Typ 4 darf in einer Anwendung der Kategorie 4 verwendet werden.

AOPDDRs umfassen Bereichs- oder Laserscanner. Diese Vorrichtungen werden vorwiegend als Typ 3 eingestuft und können entsprechend in Anwendungen der Kategorie 3 eingesetzt werden.

Außerdem müssen optische Sicherheitsgeräte entsprechend den geltenden Normen in einem angemessenen Mindestsicherheitsabstand angebracht werden. Für die geeigneten Berechnungen sind die geltenden Normen und die Dokumentation des Herstellers für Ihre Vorrichtung zu beachten. Die Ansprechzeit zwischen den Ausgängen des Sicherheitskontrollers und den einzelnen Sicherheitseingängen ist auf der Registerkarte **Konfigurationsübersicht** in der Software angegeben.

Umfasst die Anwendung eine Hintertretungsgefahr (die Gefahr, dass eine Person die Strahlen der optischen Vorrichtung passieren und auf der Gefahrseite stehen könnte, ohne erkannt zu werden), so können zusätzliche Schutzeinrichtungen erforderlich sein, und der manuelle Reset sollte gewählt werden (siehe Manueller Reset-Eingang auf Seite 55).

## 7.5.8 Zweihandsteuerung

Der Sicherheitskontroller kann als Steuergerät für die meisten angetriebenen Maschinen verwendet werden, bei denen der Maschinenzyklus von einer Bedienperson gesteuert wird.

Die Bedienelemente der Zweihandsteuerung (THC) müssen so angeordnet sein, dass die gefährliche Bewegung abgeschlossen ist oder gestoppt wird, bevor der Bediener einen oder beide Taster loslassen und den Gefahrenbereich erreichen kann (siehe Berechnung des Sicherheitsabstands (Mindestabstands) für Zweihandsteuerung auf Seite 39).

Die Sicherheitseingänge des Sicherheitskontrollers dienen zur Überwachung der Auslösung der Handsteuerungen und erfüllen damit die Funktionalitätsanforderungen der Sicherheitskategorie III entsprechend IEC 60204-1 und ISO 13851 und die Anforderungen entsprechend ANSI NFPA79 und ANSI B11.19 für Zweihandsteuerungen, die Folgendes umfassen:

- Gleichzeitige (simultane) Betätigung durch beide Hände in einem Zeitrahmen von 500 ms
- Wenn dieses Zeitlimit überschritten wird, müssen beide Zweihandschalter losgelassen werden, bevor ein neuer Arbeitsgang gestartet werden kann.
- Ununterbrochene Betätigung während eines Gefahrenzustands
- Beenden des Gefahrenzustands, wenn eine der Zweihandsteuerungen losgelassen wird
- Loslassen und erneute Betätigung beider Handsteuerungen, um die gefährliche Maschinenbewegung bzw. den Gefahrenzustand wieder zu initiieren
- Der passende Effektivitätsgrad der Sicherheitsfunktion (z. B. Steuerungszuverlässigkeit, Kategorie/Effektivitätsgrad, oder einschlägige Vorschrift bzw. Norm, oder Sicherheitsstufe), der durch eine Risikobeurteilung ermittelt wurde.

**WARNUNG: Überwachung des Bedienorts**

Bei ordnungsgemäßer Installation bietet ein zweihändiges Steuergerät nur Schutz für die Hände des Maschinenbedieners. **Darüber hinaus ist ggf. die Installation von zusätzlichen Schutzeinrichtungen erforderlich**, beispielsweise Sicherheits-Lichtvorhänge, zusätzliche Zweihandsteuerungen und/oder feste Schutzeinrichtungen, **um das Personal vor gefährlichen Maschinen zu schützen**.

**Das Fehlen geeigneter Schutzeinrichtungen an gefährlichen Maschinen kann zu Gefahrensituationen und in der Folge zu schweren oder tödlichen Verletzungen führen.**

**VORSICHT: Zweihandsteuerungen**

**Die Umgebung, in der die Zweihandsteuerungen installiert werden, darf die Auslösegeräte nicht negativ beeinträchtigen.** Starke Verschmutzung oder andere Umwelteinflüsse können lange Ansprechzeiten oder falsche Ein-Zustände von mechanischen Tasten oder ergonomischen Tastern zur Folge haben. **Dies kann zu einer Gefahrenquelle werden.**

Die erreichte Sicherheitsstufe (z. B. Kategorie nach ISO 13849-1) hängt teilweise vom gewählten Schaltungstyp ab.

Bei der Installation von Handsteuerungen ist Folgendes zu berücksichtigen:

- Fehlermöglichkeiten, die zu Kurzschluss, gebrochenen Federn oder mechanischem Festfressen führen würden, aufgrund derer das Loslassen einer Zweihandsteuerung nicht erfasst würde.
- Starke Verunreinigungen oder andere Umwelteinflüsse, die beim Loslassen lange Ansprechzeiten bewirken, oder falsche Ein-Zustände der Zweihandsteuerungen, z. B. ein festsitzendes mechanisches Gestänge.
- Schutz vor versehentlicher oder unbeabsichtigter Betätigung (z. B. Montageposition, Ringe, Abdeckungen oder Blenden)
- Verminderung der Umgehungsmöglichkeit (z. B. müssen Zweihandschalter weit genug auseinander liegen, damit sie nicht mit einem einzigen Arm betätigt werden können – normalerweise mindestens 550 mm in gerader Linie entsprechend ISO 13851)
- Die funktionelle Zuverlässigkeit und Montage externer Logikelemente
- Sachgemäße elektrische Installation gemäß NEC und NFPA79 bzw. IEC 60204

**VORSICHT: Installation von Zweihandsteuerungen darf keine versehentliche Betätigung erlauben**

Ein absolut zuverlässiger Schutz der Zweihandsteuerung vor missbräuchlicher Verwendung ist nicht möglich. **Allerdings ist der Anlagenbetreiber gemäß den Vorschriften der USA und internationalen Vorschriften dazu verpflichtet, die Zweihandsteuerungen so anzuordnen und zu schützen, dass die Möglichkeit einer absichtlichen Umgehung oder versehentlichen Betätigung minimiert wird.**

**VORSICHT: Die Maschinensteuerung muss eine Wiederholsperre haben**

Gemäß US- und internationalen Normen für Einzelhub- oder Eintakt-Maschinen muss die Maschinensteuerung über eine geeignete Wiederholsperre verfügen.

Dieses Banner-Gerät kann zur Ausführung einer Wiederholsperre verwendet werden, wobei jedoch eine Risikoeinschätzung durchgeführt werden muss, um die Eignung für diese Verwendungsart zu bestimmen.

# Berechnung des Sicherheitsabstands (Mindestabstands) für Zweihandsteuerung

Der Bediener der Handsteuerungen darf nicht in der Lage sein, den Gefahrenbereich mit einer Hand oder einem anderen Körperteil zu erreichen, bevor die Maschinenbewegung zum Stillstand kommt. Berechnen Sie den Sicherheitsabstand (Mindestabstand) mit der nachstehenden Formel.

**WARNUNG: Anordnung der Berührungstastersteuerungen**

**Handsteuerungen müssen in sicherer Entfernung von beweglichen Maschinenteilen montiert werden. Dabei ist die jeweils geltende Norm zu beachten.** Für Maschinenbediener oder andere nicht qualifizierte Personen darf es nicht möglich sein, die Position der Vorrichtung zu verändern. **Bei Nichteinhaltung des erforderlichen Sicherheitsabstands können schwere bis tödliche Verletzungen die Folge sein.**

**Anwendungen in den USA**

Die Formel für Sicherheitsabstand gemäß ANSI B11.19:

***Kupplungsbetätigte Maschinen mit Teilumdrehung*** (die Maschine und ihre Steuerungen erlauben es der Maschine, die Bewegung während des gefährlichen Teils des Maschinenzyklus anzuhalten)

$$D_s = K \times (T_s + T_r) + D_{pf}$$

***Kupplungsbetätigte Maschinen mit Vollumdrehung*** (die Maschine und ihre Steuerungen sind so ausgelegt, dass ein Maschinenzyklus vollständig ausgeführt wird)

$$D_s = K \times (T_m + T_r + T_h)$$

**$D_s$**

der Sicherheitsabstand (in Zoll)

**K**

die von OSHA/ANSI empfohlene Handgeschwindigkeitskonstante (in Zoll pro Sekunde); diese wird in den meisten Fällen bei 63 in/s berechnet, kann jedoch von 63 in/s bis 100 in/s variieren, je nach den Umständen der Anwendung;

keine unumstößlichen Werte; bei der Bestimmung des Wertes von K sollten vom Arbeitgeber alle Faktoren einschließlich der körperlichen Fähigkeiten der Bedienungsperson berücksichtigt werden.

**$T_h$**

die Ansprechzeit der langsameren Zweihandsteuerung (vom Zeitpunkt, an dem ein Handschalter losgelassen wird, bis zum Öffnen des Schalters);

$T_h$ ist für rein mechanische Schalter gewöhnlich nicht von Bedeutung. $T_h$ sollte jedoch zur Berechnung von Sicherheitsabständen in Betracht gezogen werden, wenn elektronische oder elektromechanische Handsteuerungen verwendet werden. Für selbstüberwachende Berührungstaster (STB-Taster) von Banner beträgt die Ansprechzeit 0,02 Sekunden.

**$T_m$**

die maximale Zeit (in Sekunden), die die Maschine braucht, um alle Bewegungen einzustellen, nachdem sie ausgeschaltet wurde. Bei kupplungsbetätigten Pressen mit Vollumdrehung und nur einem Einrückpunkt ist $T_m$ gleich der benötigten Zeit für eineinhalb Umdrehungen der Kurbelwelle. Bei kupplungsbetätigten Pressen mit Vollumdrehung und mehreren Einrückpunkten wird $T_m$ wie folgt berechnet:

$$T_m = (1/2 + 1/N) \times T_{cy}$$

**N** = Anzahl der Kupplungs-Einrückpunkte pro Umdrehung

**$T_{cy}$** = benötigte Zeit (in Sekunden) für eine vollständige Umdrehung der Kurbelwelle

**$T_r$**

die Ansprechzeit des Sicherheitskontrollers gemessen ab dem Zeitpunkt, zu dem von einer der Handsteuerungen ein Stoppsignal erfolgt. Die Ansprechzeit des Sicherheitskontrollers ist der Registerkarte **Konfigurationsübersicht** in der Software zu entnehmen.

**$T_s$**

die Gesamtstoppzeit der Maschine (in Sekunden) vom ersten Stoppsignal bis zum vollständigen Stillstand, einschließlich der Stoppzeiten für alle betreffenden Steuerelemente, gemessen bei maximaler Maschinengeschwindigkeit

$T_s$ wird üblicherweise mit einem Stoppzeitmessgerät erfasst. Wird eine spezifizierte Maschinenstoppzeit bei der Berechnung von T angewendet, sollten mindestens 20 % als Sicherheitsfaktor hinzugefügt werden, um eine eventuelle Alterung des Bremssystems zu berücksichtigen. Wenn die Stoppzeit der beiden redundanten Bedienelemente der Maschine nicht gleich ist, muss zur Berechnung des Sicherheitsabstands die längere der beiden Zeiten verwendet werden.

**Anwendungen in Europa**

Die Formel für Mindestabstand gemäß EN 13855:

```
S = (K x T) + C
```

**S**

der Mindestabstand (in Millimeter)

**K**

die von EN 13855 empfohlene Handgeschwindigkeitskonstante (in Millimetern pro Sekunde); diese wird in den meisten Fällen bei 1600 mm/s berechnet, kann jedoch von 1600 bis 2500 mm/s variieren, je nach den Umständen der Anwendung;

keine unumstößlichen Werte; bei der Bestimmung des Wertes von K sollten vom Arbeitgeber alle Faktoren einschließlich der körperlichen Fähigkeiten der Bedienungsperson berücksichtigt werden.

**T**

die Gesamtansprechzeit bis zum Maschinenstillstand (in Sekunden), von der physikalischen Auslösung der Sicherheitsvorrichtung bis zum Stillstand der gesamten Maschine.

**C**

der addierte Abstand aufgrund des Eintrittstiefefaktors ist gleich 250 mm gemäß EN 13855. Der **C**-Faktor gemäß EN 13855 kann auf 0 gesenkt werden, wenn das Risiko des Eindringens beseitigt ist; der Sicherheitsabstand muss jedoch immer mindestens 100 mm betragen.

## 7.5.9 Sicherheitsmatte

Der Sicherheitskontroller kann zur Überwachung von druckempfindlichen Sicherheitsmatten und Sicherheitskanten verwendet werden.

Der Zweck des Sicherheitsmatten-Eingangs des Sicherheitskontrollers besteht darin, die korrekte Funktionsweise von 4-adrigen Sicherheitsmatten mit Anwesenheitserkennung zu überwachen. Es können mehrere Sicherheitsmatten in Reihe an einen Kontroller mit einem maximalen Widerstand von 150 Ohm pro Eingang angeschlossen werden (siehe Anschlussoptionen für Sicherheitsmatten auf Seite 43).

**Wichtig:** Der Sicherheitskontroller ist nicht zur Überwachung von 2-adrigen Matten, Puffern oder Kanten geeignet (mit oder ohne Messwiderstände).

Der Sicherheitskontroller überwacht die Kontakte (Kontaktplatten) und die Verdrahtung von einer oder mehreren Sicherheitsmatten auf Ausfälle und verhindert den Wiederanlauf der Maschine, wenn ein Ausfall erfasst wird. Der Sicherheitskontroller kann eine Reset-Routine ausführen, nachdem der Bediener die Sicherheitsmatte verlassen hat, oder falls der Sicherheitskontroller im Auto-Reset-Modus verwendet wird, muss die Reset-Funktion vom Maschinensteuersystem ausgeführt werden. Hierdurch wird verhindert, dass die gesteuerte Maschine automatisch wiederanläuft, nachdem die Matte verlassen wurde.

**WARNUNG:**

**Einsatz von Sicherheitsmatten**: Die Anforderungen für den Einsatz von Sicherheitsmatten variieren in Bezug auf die Steuerungszuverlässigkeit oder die Kategorie und den Effektivitätsgrad gemäß der Beschreibung in ISO 13849-1 und ISO 13856. Banner Engineering empfiehlt für jede Anwendung immer das höchste Maß an Sicherheit. Dennoch liegt es in der Verantwortung des Benutzers, jedes Sicherheitssystem den Herstellerempfehlungen entsprechend sicher zu installieren, zu betreiben und zu warten und alle geltenden Gesetze und Vorschriften zu beachten.

Verwenden Sie Sicherheitsmatten nicht als Trittschutzvorrichtungen bei der Initiierung der Maschinenbewegung (wie z. B. bei einer Anwendung mit automatischer Maschinenbetätigung), weil durch Fehler in der Matte und der Anschlussverkabelung die Möglichkeit unerwarteten Anlaufs oder Wiederanlaufs des Maschinenzyklus besteht.

Verwenden Sie eine Sicherheitsmatte nicht, wenn durch bloßes Stehen auf der Sicherheitsmatte bei der Maschinensteuerung eine gefährliche Bewegung ausgelöst werden kann (z. B. bei einer Kontrollstation). Diese Art der Anwendung verwendet eine umgekehrte/negative Logik und bestimmte Fehler (z. B. Unterbrechung der Stromversorgung für das Modul) können zu einem "falschen" Aktivierungssignal führen.

# Anforderungen für Sicherheitsmatten

Es folgen Mindestanforderungen für Gestaltung, Konstruktion und Montage von vieradrigen Sicherheitsmatten-Sensoren zum Anschluss an den Sicherheitskontroller. Diese Anforderungen sind eine Zusammenfassung der folgenden Normen: ISO 13856-1, ANSI/RIA R15.06 und ANSI B11.19. Der Anwender muss sich über alle relevanten Vorschriften und Normen informieren und dafür sorgen, dass alle einschlägigen Vorschriften und Normen erfüllt werden.

## Gestaltung und Konstruktion des Sicherheitsmattensystems

Der Sensor des Sicherheitsmattensystems, der Sicherheitskontroller und alle zusätzlichen Vorrichtungen müssen eine Ansprechzeit aufweisen, die schnell genug ist, um die Möglichkeit zu mindern, dass eine Person leicht und schnell über die Erfassungsfläche der Matte tritt (weniger als 100 bis 200 ms, je nach relevanter Norm).

Für ein Sicherheitsmattensystem muss die Mindest-Objektempfindlichkeit des Sensors so ausgelegt sein, dass der Sensor Objekte mit einem Gewicht von mindestens 30 kg auf einem runden, flachen Testobjekt mit 80 mm Durchmesser auf der Erfassungsfläche, der Matte einschließlich Fugen und Verbindungsstellen, erfasst. Die effektive Erfassungsfläche bzw. der effektive Erfassungsbereich muss erkennbar sein und kann einen oder mehrere Sensoren umfassen. Der Lieferant der Sicherheitsmatte sollte dieses Mindestgewicht und den Mindestdurchmesser als Mindest-Objektempfindlichkeit des Sensors angeben.

Einstellungen des Anwenders von Auslösekraft und Ansprechzeit sind nicht zulässig (ISO 13856-1). Der Sensor sollte so gefertigt sein, dass vorhersehbare Defekte (z. B. Oxidieren der Kontaktelemente), die die Erfassungsempfindlichkeit verringern könnten, verhindert werden.

Die Schutzart des Sensors muss mindestens IP54 entsprechen. Wenn der Sensor laut Spezifikationen zum Einsatz unter Wasser ausgelegt ist, muss die Gehäuseschutzart des Sensors mindestens IP67 entsprechen. Die Anschlusskabel können besondere Aufmerksamkeit erfordern. Eine Dochtwirkung kann zum Eintreten von Flüssigkeit in die Matte führen und möglicherweise den Verlust der Sensorempfindlichkeit bewirken. Eventuell müssen die Endstücke der Anschlusskabel in einem Gehäuse mit einer geeigneten Schutzart untergebracht werden.

Der Sensor darf durch die Umgebungsbedingungen, für die das System vorgesehen ist, nicht nachteilig beeinträchtigt werden; d. h. die Auswirkungen von Flüssigkeiten und anderen Verunreinigungen müssen berücksichtigt werden (z. B. kann langfristige Einwirkung einiger Flüssigkeiten eine Schwächung oder ein Anschwellen des Sensorgehäusematerials bewirken und zu einem gefährlichen Zustand führen).

Die Oberseite des Sensors sollte dauerhaft rutschfest sein oder auf andere Weise die Möglichkeit eines Ausrutschens unter den erwarteten Betriebsbedingungen minimieren.

Die vieradrige Verbindung zwischen den Anschlusskabeln und dem Sensor muss einem Ziehen oder dem Tragen des Sensors an seinem Kabel standhalten, ohne dass der Sensor ausfällt und einen gefährlichen Zustand verursacht (z. B. gerissene Verbindungen durch ruckartiges Ziehen, stetiges Ziehen oder dauerndes Biegen). Andernfalls müssen andere Mittel eingesetzt werden, um derartige Ausfälle zu vermeiden, z. B. ein Kabel, das sich ohne Beschädigung löst und einen sicheren Zustand herbeiführt.

# Installation von Sicherheitsmatten

Die Beschaffenheit der Montagefläche und die Vorbereitung für die Sicherheitsmatte müssen die vom Sensorhersteller angegebenen Anforderungen erfüllen. Unregelmäßigkeiten bei den Montageflächen können die Funktion des Sensors beeinträchtigen und müssen auf ein akzeptables Minimum reduziert werden. Die Montagefläche sollte eben und sauber sein. Eine Ansammlung von Flüssigkeiten unter dem Sensor oder um den Sensor herum ist zu vermeiden. Das Ausfallrisiko durch Schmutzablagerungen, Drehspäne oder andere Materialien unter dem Sensor oder den zugehörigen Befestigungsteilen muss verhindert werden. Besondere Aufmerksamkeit sollte den Fugen zwischen den Sensoren gewidmet werden, um sicherzustellen, dass keine Fremdkörper unter oder in den Sensor gelangen.

Alle Beschädigungen (z. B. Schnitte, Risse, Verschleiß oder durchgestoßene Stellen) am äußeren Isoliermantel des Anschlusskabels oder an äußeren Teilen der Sicherheitsmatte müssen sofort repariert oder die entsprechenden Teile ausgetauscht werden. Eindringen von Material (einschließlich Schmutzpartikel, Insekten, Flüssigkeit, Feuchtigkeit oder Drehspäne), das sich neben der Sicherheitsmatte befinden könnte, kann dazu führen, dass der Sensor rostet oder seine Empfindlichkeit verliert.

Jede Sicherheitsmatte ist gemäß den Empfehlungen des Herstellers routinemäßig zu überprüfen und zu testen. Die Betriebsspezifikationen (z. B. die Anzahl der Schaltvorgänge) dürfen nicht überschritten werden.

Jede Sicherheitsmatte muss sicher montiert werden, um unbeabsichtigte Bewegungen oder unbefugtes Entfernen zu verhindern. Zu den Methoden gehören u. a. sicheres Abkanten, manipulationssichere oder Einweg-Befestigungsteile sowie vertiefte Böden oder Montageflächen zusätzlich zur Verwendung großer und schwerer Matten.

Jede Sicherheitsmatte muss so montiert werden, dass Stolpergefahren minimiert werden (insbesondere in Richtung auf die gefährdende Maschine). Eine Stolpergefahr kann bestehen, wenn der Höhenunterschied einer angrenzenden horizontalen Oberfläche 4 mm oder mehr beträgt. Stolpergefahren müssen an Fugen, Verbindungsstellen und Kanten und bei Verwendung zusätzlicher Abdeckungen minimal gehalten werden. Zu den Methoden gehört eine mit dem Boden bündige Sensormontage (versenkt im Boden, damit er mit dem umgebenden Boden bündig ist) oder eine Rampe, die nicht mehr als 20° von der Horizontalen abweicht. Verwenden Sie kontrastreiche Farben oder Markierungen, um Rampen und Kanten zu kennzeichnen.

Das Sicherheitsmatten-System muss groß genug und so positioniert sein, dass niemand den Gefahrenbereich betreten kann, ohne erfasst zu werden, und dass niemand die Gefahrstelle erreichen kann, bevor die gefährliche Maschinenbewegung zum Stillstand gekommen ist. Um sicherzustellen, dass es nicht möglich ist, die Gefahrstelle durch Um-, Unter- oder Übergreifen der Erfassungsfläche der Vorrichtung zu erreichen, sind unter Umständen zusätzliche Schutzeinrichtungen erforderlich.

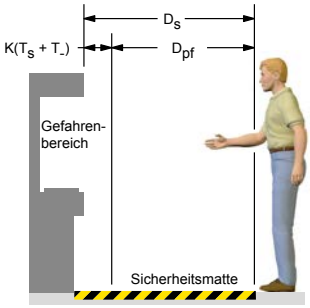
Bei einer Sicherheitsmatten-Installation muss die Möglichkeit berücksichtigt werden, dass jemand über die Erfassungsfläche tritt und nicht erfasst wird. In ANSI und in internationalen Normen wird je nach Anwendung und relevanter Norm eine Mindestentfernung der Sensoroberfläche (der kleinste Abstand zwischen der Mattenkante und der Gefahrstelle) von 750 mm bis 1200 mm gefordert. Die Möglichkeit, auf Maschinenstützen oder andere Gegenstände zu treten, um den Sensor zu umgehen oder darüber hinweg zu klettern, muss ebenfalls verhindert werden.

## Sicherheitsabstand (Mindestabstand) für Sicherheitsmatten

Als eigenständige Schutzeinrichtung muss die Sicherheitsmatte so im Sicherheitsabstand (Mindestabstand) montiert werden, dass sich die Außenkante der Erfassungsfläche am oder hinter dem Sicherheitsabstand befindet, es sei denn, die Sicherheitsmatte wird ausschließlich zur Verhinderung eines Anlaufs/Wiederanlaufs oder ausschließlich für eine Zwischenraum-Schutzeinrichtung verwendet (siehe ANSI B11.19, ANSI/RIA R15.06 und ISO 13855).

Der für eine Anwendung erforderliche Sicherheitsabstand (Mindestabstand) hängt von mehreren Faktoren ab, u. a. von der Geschwindigkeit der Hand (oder Person), der Gesamt-Systemstoppzeit (zu der mehrere Ansprechzeitkomponenten gehören) und dem Eintrittstiefefaktor. Der Anwender muss anhand der relevanten Norm den richtigen Abstand ermitteln oder sonstige Maßnahmen ergreifen, damit sichergestellt wird, dass niemand den Gefahren ausgesetzt werden kann.

*Abbildung 19. Ermittlung des Sicherheitsabstands für die Sicherheitsmatte*




### Anwendungen in den USA

Die Formel für Sicherheitsabstand gemäß ANSI B11.19:

$$D_s = K \times (T_s + T_r) + D_{pf}$$

**$D_s$**

der Sicherheitsabstand (in Zoll)

**$T_r$**

die Ansprechzeit des Sicherheitskontrollers gemessen ab dem Zeitpunkt, zu dem von einer der Handsteuerungen ein Stoppsignal erfolgt. Die Ansprechzeit des Sicherheitskontrollers ist der Registerkarte **Konfigurationsübersicht** in der Software zu entnehmen.

**K**

die von OSHA/ANSI empfohlene Handgeschwindigkeitskonstante (in Zoll pro Sekunde); diese wird in den meisten Fällen bei 63 in/s berechnet, kann jedoch von 63 in/s bis 100 in/s variieren, je nach den Umständen der Anwendung;

keine unumstößlichen Werte; bei der Bestimmung des Wertes von K sollten vom Arbeitgeber alle Faktoren einschließlich der körperlichen Fähigkeiten der Bedienungsperson berücksichtigt werden.

**$T_s$**

die Gesamtstoppzeit der Maschine (in Sekunden) vom ersten Stoppsignal bis zum vollständigen Stillstand, einschließlich der Stoppzeiten für alle betreffenden Steuerelemente, gemessen bei maximaler Maschinengeschwindigkeit

$T_S$ wird üblicherweise mit einem Stoppzeitmessgerät erfasst. Wird eine spezifizierte Maschinenstoppzeit bei der Berechnung von T angewendet, sollten mindestens 20 % als Sicherheitsfaktor hinzugefügt werden, um eine eventuelle Alterung des Bremssystems zu berücksichtigen. Wenn die Stoppzeit der beiden redundanten Bedienelemente der Maschine nicht gleich ist, muss zur Berechnung des Sicherheitsabstands die längere der beiden Zeiten verwendet werden.

**$D_{pf}$**

die zusätzliche Entfernung aufgrund des Eintrittstiefefaktors

gleich 48 in gemäß ANSI B11.19

| Anwendungen in Europa |
|---|

Die Formel für Mindestabstand gemäß EN 13855:

```
S = (K x T) + C
```

**S**

der Mindestabstand (in Millimeter)

**K**

die von EN 13855 empfohlene Handgeschwindigkeitskonstante (in Millimetern pro Sekunde); diese wird in den meisten Fällen bei 1600 mm/s berechnet, kann jedoch von 1600 bis 2500 mm/s variieren, je nach den Umständen der Anwendung;

keine unumstößlichen Werte; bei der Bestimmung des Wertes von K sollten vom Arbeitgeber alle Faktoren einschließlich der körperlichen Fähigkeiten der Bedienungsperson berücksichtigt werden.

**T**

die Gesamtansprechzeit bis zum Maschinenstillstand (in Sekunden), von der physikalischen Auslösung der Sicherheitsvorrichtung bis zum Stillstand der gesamten Maschine.

**C**

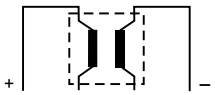
Der addierte Abstand aufgrund des Eintrittstiefefaktors ist gleich 1200 mm gemäß EN 13855.

## Anschlussoptionen für Sicherheitsmatten

Druckempfindliche Matten und druckempfindliche Böden müssen die Anforderungen der Kategorie erfüllen, für die sie spezifiziert und gekennzeichnet sind. Diese Kategorien sind in ISO 13849-1 definiert.

Die Sicherheitsmatte, ihr Sicherheitskontroller und alle Ausgangssignal-Schaltgeräte müssen mindestens die Sicherheitsanforderungen für Kategorie 1 erfüllen. Siehe ISO 13856-1 (EN 1760-1) und ISO 13849-1 für nähere Informationen zu den einschlägigen Anforderungen.

**Der Sicherheitskontroller wurde zur Überwachung von 4-adrigen Sicherheitsmatten entwickelt, ist jedoch mit zweiadrigen Vorrichtungen** (Matten, Messkanten usw. mit zwei Leitern und einem Messwiderstand) nicht kompatibel.

| 4-adrig | |
|---|---|
| Diese Schaltung erfüllt in der Regel die Anforderungen für Vorrichtungen der Kategorie 2 oder Kategorie 3 nach ISO 13849-1, je nach Schutzart und Installation der Matte(n). Der Sicherheitskontroller wechselt in einen Sperrmodus, wenn eine Leitungsunterbrechung, ein Kurzschluss zu 0 V oder ein Kurzschluss zu einer anderen Stromquelle erfasst wird. |  |

## 7.5.10 Muting-Sensor

Beim Muting von Sicherheitsgeräten handelt es sich um die automatisch gesteuerte Aufhebung eines oder mehrerer Sicherheitseingangs-Stoppsignale während eines Abschnitts des Maschinenbetriebs, wenn keine unmittelbare Gefahr besteht oder wenn der Zugang zur Gefahrstelle gesichert ist. Muting-Sensoren können einem oder mehreren der folgenden Sicherheitseingangsgeräte zugeordnet werden:

- Schutztürschalter (Verriegelungsschalter)
- Optosensoren
- Zweihandsteuerungen
- Sicherheitsmatten
- Schutzhaltvorrichtungen

US-Normen und internationale Normen schreiben vor, dass der Benutzer das Sicherheitssystem so anordnen, installieren und bedienen muss, dass das Personal geschützt ist und dass die Möglichkeit einer Umgehung der Schutzeinrichtung minimiert wird.

# Beispiele für Muting-Sensoren und -Schalter

**WARNUNG: Vermeidung gefährlicher Installationen**

**Zwei oder vier unabhängige Positionsschalter müssen richtig eingestellt bzw. positioniert werden, damit sie nur dann schließen, wenn die Gefahr nicht mehr besteht, und wieder öffnen, wenn der Maschinenzyklus abgeschlossen ist oder die Gefahr wieder vorhanden ist. Falsche Einstellung oder Stellung der Schalter kann zu Verletzungen oder Tod führen.**

Der Anwender ist für die Einhaltung sämtlicher örtlichen und nationalen Gesetze, Vorschriften und Bestimmungen über den Einsatz von Sicherheitsausrüstungen bei einer konkreten Anwendung verantwortlich. Achten Sie darauf, dass sämtliche Rechtsvorschriften eingehalten und sämtliche in dieser Anleitung enthaltenen Installations- und Wartungsanweisungen befolgt werden.

## Optoelektronische Sensoren (Einweglichtschranken)

Einweglichtschrankensensoren sollten für die Dunkelschaltung (DO) konfiguriert werden und offene (nicht leitende) Ausgangskontakte im ausgeschalteten Zustand aufweisen. Sender und Empfänger eines jeden Paares sollten jeweils von derselben Quelle versorgt werden, um Gleichtaktfehler möglichst zu vermeiden.

## Optoelektronische Sensoren (Reflexionslichtschranken mit Polarisationsfilter)

Der Benutzer muss sicherstellen, dass die irrtümliche Aktivierung aufgrund glänzender oder reflektierender Oberflächen nicht möglich ist. Banner Flachprofil-Sensoren mit linearer Polarisation können diesen Effekt enorm verringern oder ganz beseitigen.

Verwenden Sie einen als Hellschaltung (Hellschaltung oder Schließerausgang) konfigurierten Sensor, wenn bei Erfassung des reflektierenden Objekts oder des reflektierenden Bands ein Muting ausgelöst wird (Ausgangsposition). Verwenden Sie einen als Dunkelschaltung (Dunkelschaltung oder Öffnerausgang) konfigurierten Sensor, wenn ein blockierter Strahlenweg den Muting-Zustand auslöst (Eingang/Ausgang). In beiden Situationen müssen die Ausgangskontakte bei unterbrochener Stromzufuhr offen (nicht leitend) sein.

## Zwangsgeöffnete Sicherheitsschalter

Normalerweise werden zwei (oder vier) unabhängige Schalter mit mindestens je einem geschlossenen Sicherheitskontakt zum Auslösen des Muting-Zyklus verwendet. Bei einer Anwendung, die nur einen Schalter mit einem Bedienelement und zwei geschlossenen Kontakten verwendet, kann eine unsichere Situation entstehen.

## Induktive Näherungssensoren

Induktive Näherungssensoren werden gewöhnlich verwendet, um einen Muting-Zyklus auszulösen, wenn eine Metalloberfläche erfasst wird. Verwenden Sie keine zweiadrigen Sensoren, weil durch übermäßige Kriechströme falsche Ein-Zustände verursacht werden können. Verwenden Sie nur drei- oder vieradrige Sensoren mit pnp- oder fest verdrahteten Kontakt-Digitalausgängen, die vom Eingangsstrom unabhängig sind.

# Anforderungen an Muting-Vorrichtungen

Die Muting-Vorrichtungen müssen mindestens die folgenden Anforderungen erfüllen:

1. Es müssen mindestens zwei unabhängige fest verdrahtete Muting-Vorrichtungen verwendet werden.
2. Die Muting-Vorrichtungen müssen entweder Schließerkontakte, pnp-Ausgänge (die jeweils die in den Spezifikationen und Anforderungen auf Seite 20 aufgeführten Eingangsanforderungen erfüllen müssen) oder antivalentes Schaltverhalten aufweisen. Mindestens einer dieser Kontakte muss schließen, wenn der Schalter betätigt wird, und öffnen (bzw. nicht leiten), wenn der Schalter nicht betätigt wird oder wenn die Stromversorgung ausgeschaltet ist.
3. Die Aktivierung der Eingänge zur Muting-Funktion muss von separaten Vorrichtungen kommen. Diese Vorrichtungen müssen separat installiert werden, damit ein unsicherer Muting-Zustand verhindert wird, der aus falscher Einstellung, Fehlausrichtung oder einem einzelnen Gleichtaktfehler entstehen kann, z. B. durch physische Beschädigungen der Montagefläche. Nur eine dieser Vorrichtungen darf durch ein programmierbares Steuergerät (SPS) o. ä. gehen oder davon beeinflusst werden.
4. Die Muting-Vorrichtungen müssen so installiert werden, dass sie nicht leicht außer Kraft gesetzt oder umgangen werden können.
5. Die Muting-Vorrichtungen müssen so montiert werden, dass ihre Position und Ausrichtung nicht einfach geändert werden kann.
6. Es darf nicht möglich sein, dass Umweltbedingungen (z. B. extreme Luftverschmutzung) einen Muting-Zustand auslösen.
7. Die Muting-Vorrichtungen dürfen nicht für Verzögerungen oder andere Zeitfunktionen eingestellt werden (es sei denn, solche Funktionen werden so ausgeführt, dass der Ausfall einer einzelnen Komponente die Beseitigung der Gefahr nicht verhindert und weitere Maschinenzyklen ermöglicht, solange der Fehler nicht behoben wurde, und durch Verlängerung der Muting-Periode keine Gefahr erzeugt wird).

## 7.5.11  Überbrückungsschalter

Bei der Überbrückung einer Schutzeinrichtung handelt es sich um eine manuell aktivierte und vorübergehende Aufhebung eines oder mehrerer Stoppsignale für die Sicherheitseingänge unter Aufsicht, wenn keine unmittelbare Gefahr besteht. Dazu wird gewöhnlich ein Überbrückungsmodus mit einem Schlüsselschalter eingestellt, um Maschinen-Inbetriebnahme, Bandausrichtung/-einstellungen, Roboterprogrammierung und Prozessfehlersuche zu erleichtern.

Überbrückungsschalter können einem oder mehreren der folgenden Sicherheitseingangsgeräte zugeordnet werden:

- Schutztürschalter (Verriegelungsschalter)
- Optosensoren
- Zweihandsteuerungen
- Sicherheitsmatten
- Schutzhalt

### Anforderungen für die Umgehung von Schutzeinrichtungen

Für die Überbrückung einer Schutzeinrichtung gelten die folgenden Anforderungen [6]:

- Die Überbrückungsfunktion muss zeitlich begrenzt sein.
- Die Vorrichtung zur Einstellung bzw. Aktivierung der Überbrückung muss beaufsichtigt werden können.
- Automatischer Maschinenbetrieb muss durch Einschränkung von Bewegungsbereich, Geschwindigkeit oder Leistung verhindert werden (z. B. nur Einsatz im Tipp-Betrieb, bei Einzelhub oder bei niedriger Geschwindigkeit). Der Überbrückungsmodus darf nicht für die Produktion verwendet werden.
- Zusätzliche Schutzeinrichtungen müssen bereitgestellt werden. Das Personal darf keinen Gefahren ausgesetzt werden.
- Die Überbrückungsvorrichtung muss von der zu überbrückenden Schutzeinrichtung aus vollständig einsehbar sein.
- Die Bewegungsinitiierung darf nur durch einen Tippschalter möglich sein.
- Alle Not-Aus-Schalter müssen aktiv bleiben.
- Die Überbrückungsvorrichtung muss mit der gleichen Zuverlässigkeitsstufe verwendet werden wie die Schutzeinrichtung.
- Ein Überbrücken der Schutzeinrichtung muss vom Standort der Schutzeinrichtung aus deutlich erkennbar sein.
- Das Personal muss in der Verwendung der Schutzeinrichtung und der Überbrückung unterwiesen werden.
- Es müssen Risikobeurteilung und Risikoreduzierung (entsprechend der relevanten Norm) vorgenommen werden.
- Durch Rücksetzen, Betätigung, Freigabe oder Aktivierung der Schutzvorrichtung darf keine gefährliche Maschinenbewegung initiiert und keine Gefahrsituation erzeugt werden.

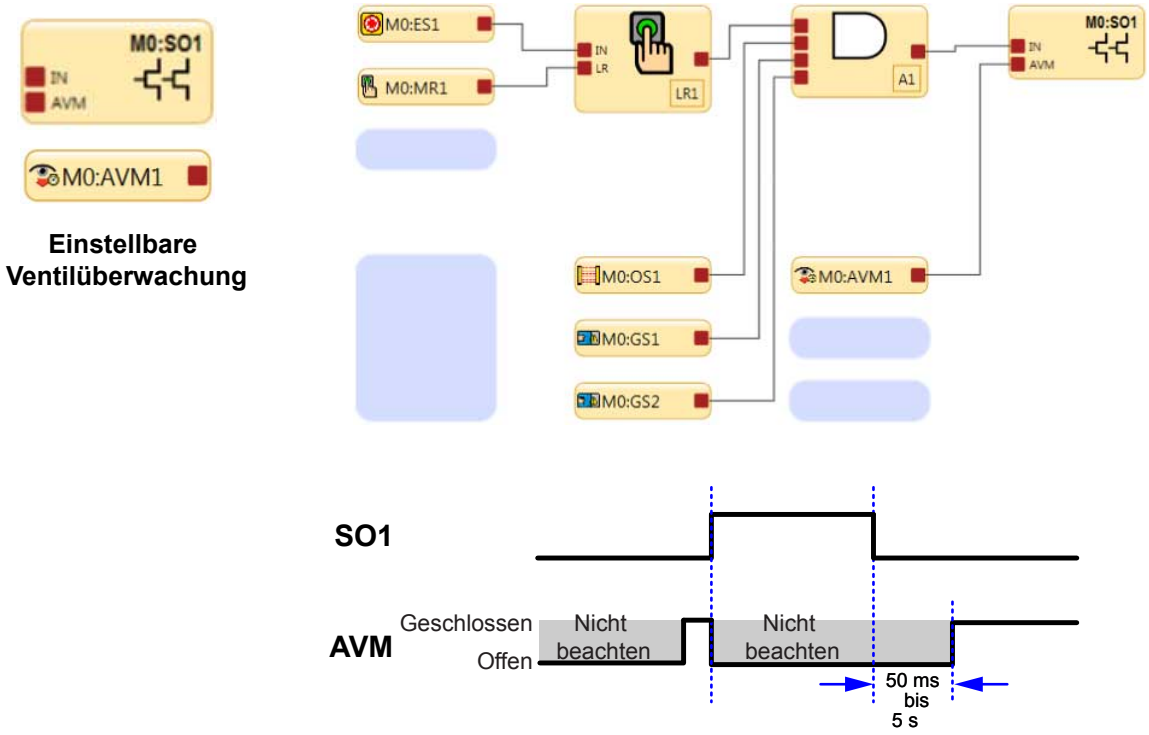
Die Überbrückung einer Schutzeinrichtung darf nicht mit *Muting* verwechselt werden, bei dem es sich um die vorübergehende automatische Aufhebung der Schutzfunktion einer Schutzeinrichtung während eines ungefährlichen Abschnitts des Maschinenzyklus handelt. Durch Muting kann einer Maschine oder einem Prozess manuell oder automatisch Material zugeführt werden, ohne dass ein Stoppbefehl initiiert werden muss. Ein weiterer, oft mit Überbrückung verwechselter Begriff ist *Ausblendung*. Bei der Ausblendung wird ein Teil des Erfassungsbereichs einer optischen Schutzeinrichtung desensibilisiert wird (z. B. Deaktivierung eines oder mehrerer Strahlen eines Sicherheits-Lichtvorhangs, damit eine spezifische Strahlunterbrechung ignoriert wird).

## 7.5.12  AVM-Funktion (Adjustable Valve Monitoring, einstellbare Ventilüberwachung)

Die AVM-Funktion (Adjustable Valve (Device) Monitoring) ist vergleichbar mit der einkanaligen externen Geräteüberwachungsfunktion EDM (One-Channel External Device Monitoring, siehe Externe Geräteüberwachung (EDM) auf Seite 67). Die AVM-Funktion überwacht den Status von Geräten, die von dem Sicherheitsausgang gesteuert werden, dem die Funktion zugeordnet ist. Wenn sich der Sicherheitsausgang ausschaltet, muss der AVM-Eingang die Einstellung Hoch/Ein aufweisen (mit einer anliegenden Spannung von +24 V DC), bevor der AVM-Zeitgeber abläuft; sonst tritt eine Sperre ein. Der AVM-Eingang muss auch die Einstellung Hoch/Ein aufweisen, wenn der Sicherheitsausgang einen Einschaltversuch unternimmt; sonst tritt eine Sperre ein.

[6] Diese Zusammenfassung wurde unter Einbeziehung der folgenden Normen erstellt: ANSI NFPA79, ANSI/RIA R15.06, ISO 13849-1 (EN954-1), IEC60204-1 und ANSI B11.19.

*Abbildung 20. Zeitgeberlogik – AVM-Funktion*




Die einstellbare Ventilüberwachung (AVM) ist eine Methode zur Überprüfung des Betriebs von 2-kanaligen Ventilen. Die zwangsgeführten Öffner-Überwachungskontakte der Ventile dienen als Eingänge für die Erkennung eines „verschweißten Ein-Zustands“ als Fehlerzustand und verhindern ein Einschalten der Ausgänge des Sicherheitskontrollers.

**Anmerkung:** Ein Zeitraum von 50 ms bis 5 s kann in 50-ms-Intervallen eingestellt werden (die Werkseinstellung lautet 50 ms).

Die AVM-Funktion ist nützlich für die dynamische Überwachung von Geräten, die vom Sicherheitsausgang gesteuert werden, die jedoch im aktivierten Zustand bzw. in aktivierter Position langsam reagieren, stagnieren oder ausfallen und deren Betrieb nach dem Eintreten eines Stoppsignals überprüft werden muss. Zu den Anwendungsmöglichkeiten gehören beispielsweise Einzel- oder Doppelmagnetventile zur Steuerung von Kupplung-Bremse-Mechanismen sowie Positionssensoren, die die Ausgangsposition eines linearen Antriebs überwachen.

Die Synchronisierung oder Überprüfung einer maximalen Zeitgebungsdifferenz zwischen mehreren Geräten, z. B. Doppelventilen, kann durch Zuordnung mehrerer AVM-Funktionen zu einem Sicherheitsausgang und Konfiguration des AVM-Timers mit denselben Werten erzielt werden. Eine beliebige Anzahl an AVM-Eingängen kann einem Sicherheitsausgang zugeordnet werden. Ein Eingangssignal kann von einem ständigen Kontakt bzw. Relaiskontakt oder einem pnp-Transistorausgang generiert werden.

**WARNUNG:**

- **AVM-Betrieb (Adjustable Valve Monitoring)**
- Wenn die AVM-Funktion verwendet wird, schalten sich die Sicherheitsausgänge erst EIN, wenn die Voraussetzungen für den AVM-Eingang erfüllt sind. Dies könnte zu einer Einschaltverzögerung bis zur konfigurierten AVM-Überwachungszeit führen.
- Der Anwender hat dafür Sorge zu tragen, dass die AVM-Überwachungszeit angemessen für die Anwendung konfiguriert ist und dass alle Personen, die mit der Maschine zu tun haben, über die Möglichkeit des Einschaltverzögerungseffekts informiert werden, da dieser für Maschinenbediener oder anderes Personal nicht unbedingt einfach zu erkennen ist.

## 7.5.13 SC10-2: ISD-Eingänge

Über die Sicherheitseingänge IN3/IN4 und IN5/IN6 des Sicherheitskontrollers können Gerätereihen mit eingebetteten ISD-Daten (In-Series Diagnostic) wie SI-RFD-Sicherheitsschalter von Banner, beleuchtete Nothalttaster mit ISD von Banner oder der ISD-Anschluss von Banner überwacht werden. Die SI-RFD Sicherheitsschalter von Banner verwenden die RFID-Technologie zur Erfassung.

ISD-Geräte wie SI-RFD-Sicherheitsschalter müssen gemäß den Anwendungsnormen mit einem entsprechenden Sicherheitsabstand (Mindestabstand) angebracht werden. Für die geeigneten Berechnungen sind die geltenden Normen und die spezifische Dokumentation für das Gerät zu beachten. Die Ansprechzeit zwischen den Ausgängen des Sicherheitskontrollers und den einzelnen Sicherheitseingängen ist auf der Registerkarte **Konfigurationsübersicht** in der Software angegeben. Diese Zeit muss zur Ansprechzeit der ISD-Geräteeihe hinzugefügt werden.

Die aktiven Transistorausgänge der ISD-Geräte können (und müssen) externe Kurzschlüsse zur Stromversorgung, zur Masse und untereinander erkennen. Die Geräte werden gesperrt, wenn ein solcher Kurzschluss erkannt wird.

Wenn die Anwendung eine Hintertretungsgefahr umfasst (eine Person könnte durch eine offene Schutztür treten und unerkannt auf der Gefahrenseite stehen), sind gegebenenfalls andere Schutzeinrichtungen erforderlich und es sollte der manuelle Reset ausgewählt werden. Siehe Manueller Reset-Eingang auf Seite 55.

**WARNUNG:**
- **Konfiguration entspricht den anwendbaren Normen**
- Wenn die Anwendung nicht entsprechend überprüft wird, können schwere oder tödliche Verletzungen die Folge sein.
- Die Software für den Sicherheitskontroller von Banner prüft primär die Logikkonfiguration auf Verbindungsfehler. Der Benutzer ist dafür verantwortlich, dass die Anwendung die Anforderungen an die Risikobewertung erfüllt und allen geltenden Normen entspricht.

**Anmerkung:** In einer langen Reihe bzw. in Reihen mit vielen ISD-Geräten muss die Spannung der ersten Einheit (am nächsten zum Anschlussstecker gelegen) über 19,5 Volt bleiben, damit die Reihe ordnungsgemäß funktioniert.

**Anmerkung:** Die Sicherheitskontroller von Banner Software wendet die Regeln für die Torschaltung auf die ISD-Eingänge an.

## Leistungs- und Statusinformationen zu einem einzelnen Gerät über ISD anfordern

1. Ändern Sie das Register "ISD-Reihe angefordert", sodass es mit der ISD-Reihennummer für das betreffende Gerät (1 oder 2) übereinstimmt.
2. Ändern Sie das Register "ISD-Gerät angefordert", sodass es mit der ISD-Gerätenummer für das betreffende Gerät (1 bis 32) übereinstimmt.
3. Ändern Sie das Register "ISD-Leseanforderung" von 0 zu 1, um einen einmaligen Lesevorgang durchzuführen.
4. Beachten Sie das Registerdatenfeld "Spezifische Daten einzelner ISD-Geräte", um die gewünschten Gerätedaten zu lesen.

## ISD-Reihe Systemstatus

Banner hat mehrere Wörter erstellt, auf die von der SPS schnell zugegriffen werden kann. Auf diese Weise kann die SPS angeben, ob Probleme mit der ISD-Reihe vorliegen.

Diese Informationen haben das folgende Format:

| Informationen | Typ | Datengröße |
|---|---|---|
| Zahl der ISD-Reihe stimmt nicht mit der Konfiguration überein | SC10-Warnung | 1 Bit |
| Reihenfolge der ISD-Reihe stimmt nicht mit der Konfiguration überein | SC10-Warnung | 1 Bit |
| In der konfigurierten ISD-Reihe wurden keine ISD-Daten gefunden | SC10-Warnung | 1 Bit |
| Ungültiges (Nicht-ISD)-Gerät in der ISD-Reihe | SC10-Warnung | 1 Bit |
| ISD-Gerät erkannt, aber nicht konfiguriert | Informativ | 1 Bit |
| Anschlussstecker der ISD-Reihe fehlt | ISD-Status | 1 Bit |
| SI-RF hoher oder einzelner Sensor ohne programmierten Auslöser | ISD-Fehler | 1 Bit |
| Falscher Auslöser in einem hohen oder einzelnen Sensor | ISD-Fehler | 1 Bit |
| Interner Fehler in einem ISD-Gerät in der Reihe | ISD-Fehler | 1 Bit |
| ISD-Ausgangsfehler erkannt, Ausgangsausschaltzähler gestartet | ISD-Fehler | 1 Bit |
| *Reserviert* | | 2 Bit |
| ISD-Reihe OSSD-Status | ISD-Status | 1 Bit |

## Spezifische Daten einzelner ISD-Geräte

| Informationen | Daten-größe | Gilt für Banner-Gerät (J/N/Reser-viert) | | |
|---|---|---|---|---|
| | | SI-RF | Not-Aus-Schaltung | ISD-Ans-chluss |
| Sicherheitseingangsfehler | 1-Bit | Y | Y | Y |
| *reserviert* | 1-Bit | *reserviert* | *reserviert* | *reserviert* |
| Sensor nicht gekoppelt | 1-Bit | Y | N | N |
| ISD-Datenfehler | 1-Bit | Y | Y | Y |
| Falscher Auslöser-/Tasterstatus/Eingangsstatus | 1-Bit | Y | Y | Y |
| Marginaler Bereich/Tasterstatus/Eingangsstatus | 1-Bit | Y | Y | Y |
| Auslöser erkannt | 1-Bit | Y | N | N |
| Ausgangsfehler | 1-Bit | Y | Y | Y |
| Eingang 2 | 1-Bit | Y | Y | Y |
| Eingang 1 | 1-Bit | Y | Y | Y |
| Lokaler Reset erwartet | 1-Bit | Y | Y | N |
| Warnung Betriebsspannung | 1-Bit | Y | Y | Y |
| Fehler bei Betriebsspannung | 1-Bit | Y | Y | Y |
| Ausgang 2 | 1-Bit | Y | Y | Y |
| Ausgang 1 | 1-Bit | Y | Y | Y |
| Aus- und Wiedereinschalten der Stromversorgung erforderlich | 1-Bit | Y | Y | Y |
| Fehlertolerante Ausgänge | 1-Bit | Y | Y | Y |
| Einheit für lokalen Reset | 1-Bit | Y | Y | N |
| Kaskadierbar | 1-Bit | Y | Y | Y |
| Hohe Codierstufe | 1-Bit | Y | N | N |
| Verbleibende Einlerninstanzen | 4-Bit | Y | N | N |
| Geräte-ID | 5-Bit | Y | Y | Y |
| Anzahl Bereichswarnungen | 6-Bit | Y | N | N |
| Ausschaltzeit für Ausgang | 5-Bit | Y | Y | Y |
| Anzahl der Spannungsfehler | 8-Bit | Y | Y | Y |
| Innentemperatur [7] | 8-Bit | Y | Y | Y |
| Auslöserabstand [7] | 8-Bit | Y | N | N |
| Versorgungsspannung [7] | 8-Bit | Y | Y | Y |
| Erwarteter Firmenname | 4-Bit | Y | N (immer "6") | N (immer "6") |
| Empfangener Firmenname | 4-Bit | Y | N | N |
| Erwarteter Code | 16-Bit | Y | N | N |
| Empfangener Code | 16-Bit | Y | N | N |
| Interner Fehler A | 16-Bit | Y | Y | Y |
| Interner Fehler B | 16-Bit | Y | Y | Y |

[7] Informationen zur Umrechnung von Innentemperatur, Auslöserabstand und Betriebsspannung finden Sie unter ISD: Informationen zur Umwandlung von Temperatur, Spannung und Abstand auf Seite 248.

## SI-RF-Gerät

Bei dem ISD-fähigen Schutztürschalter (SI-RF) haben die vom SI-RF-Gerät zurückkommenden spezifischen Daten einzelner ISD-Geräte das folgende Format:

| Informationen | Datengröße |
|---|---|
| Sicherheitseingangsfehler | 1 Bit |
| *reserviert* | 1 Bit |
| Sensor nicht gekoppelt | 1-bit |
| ISD-Datenfehler | 1-bit |
| Falscher Auslöser | 1-bit |
| Marginaler Bereich | 1-bit |
| Auslöser erkannt | 1-bit |
| Ausgangsfehler | 1-bit |
| Eingang 2 | 1-bit |
| Eingang 1 | 1-bit |
| Lokaler Reset erwartet | 1-bit |
| Warnung Betriebsspannung | 1-bit |
| Fehler bei Betriebsspannung | 1-bit |
| Ausgang 2 | 1-bit |
| Ausgang 1 | 1-bit |
| Aus- und Wiedereinschalten der Stromversorgung erforderlich | 1-bit |
| Fehlertolerante Ausgänge | 1-bit |
| Einheit für lokalen Reset | 1-bit |
| Kaskadierbar | 1-bit |
| Allgemeine Codierung | 1-bit |
| Verbleibende Einlerninstanzen | 4-bit |
| Geräte-ID | 5-bit |
| Anzahl Bereichswarnungen | 6-bit |
| Ausschaltzeit für Ausgang | 5-Bit<br>(Wert 31 bedeutet, dass der Zeitgeber ausgeschaltet ist) |
| Anzahl der Spannungsfehler | 8-bit |
| Innentemperatur [8] | 8-Bit |
| Auslöserabstand [8] | 8-bit |
| Versorgungsspannung [8] | 8-bit |
| Erwarteter Firmenname | 4-bit |
| Empfangener Firmenname | 4-bit |
| Erwarteter Code | 16-bit |
| Empfangener Code | 16-bit |
| Interner Fehler A | 16-bit |
| Interner Fehler B | 16-bit |

[8] Informationen zur Umrechnung von Innentemperatur, Auslöserabstand und Betriebsspannung finden Sie unter ISD: Informationen zur Umwandlung von Temperatur, Spannung und Abstand auf Seite 248.

## Nothaltvorrichtung und ISD-Anschluss

Bei dem ISD-fähigen Nothaltschalter oder ISD-Anschluss haben die von der Vorrichtung zurückkommenden gerätespezifischen Daten einzelner ISD-Geräte das folgende Format:

| Informationen | Datengröße |
|---|---|
| Sicherheitseingangsfehler | 1-bit |
| *reserviert* | 2-bit |
| ISD-Datenfehler | 1-bit |
| *reserviert* | 3-bit |
| Ausgangsfehler | 1-bit |
| Eingang 2 | 1-bit |
| Eingang 1 | 1-bit |
| Lokaler Reset erwartet | 1-Bit<br>(bei ISD-Anschluss nie zutreffend) |
| Warnung Betriebsspannung | 1-bit |
| Fehler bei Betriebsspannung | 1-bit |
| Ausgang 2 | 1-bit |
| Ausgang 1 | 1-bit |
| Aus- und Wiedereinschalten der Stromversorgung erforderlich | 1-bit |
| Fehlertolerante Ausgänge | 1-Bit<br>(bei ISD-Nothaltschalter und -Anschluss immer zutreffend) |
| Einheit für lokalen Reset | 1-Bit<br>(bei ISD-Anschluss nie zutreffend) |
| Kaskadierbar | 1-Bit<br>(bei ISD-Nothaltschalter und -Anschluss immer zutreffend) |
| *reserviert* | 5-bit |
| Geräte-ID | 5-Bit<br>(bei ISD-Nothaltschalter immer Wert 7)<br>(bei ISD-Anschluss immer Wert 9) |
| *reserviert* | 6-bit |
| Ausschaltzeit für Ausgang | 5-Bit<br>(Wert 31 bedeutet, dass der Zeitgeber ausgeschaltet ist) |
| Anzahl der Spannungsfehler | 8-bit |
| Innentemperatur [9] | 8-Bit |
| *reserviert* | 8-bit |
| Versorgungsspannung [9] | 8-bit |
| Erwarteter Firmenname | 4-Bit<br>(bei ISD-Nothaltschalter und -Anschluss immer Wert 6) |
| *reserviert* | 36-bit |
| Interner Fehler A | 16-bit |
| Interner Fehler B | 16-bit |

[9] Informationen zur Umrechnung von Innentemperatur, Auslöserabstand und Betriebsspannung finden Sie unter ISD: Informationen zur Umwandlung von Temperatur, Spannung und Abstand auf Seite 248.

## 7.5.14 XS/SC26-2: Zyklusinitiierung für Pressensteuerungs-Funktionsblock

Ein einzelner, momentaner Auslöser kann als Auslösevorrichtung für kleine hydraulische/pneumatische Pressen verwendet werden, wenn er zusammen mit dem Pressensteuerungs-Funktionsblock verwendet wird und dieser für die Einzelauslösersteuerung konfiguriert ist. Dies ist ein Initiierungseingang zum Starten des Pressenzyklus. Wenn Einzelauslösersteuerung gewählt ist, kann der Bediener den Zyklus über diesen Eingang starten und dann loslassen, um sich anderen Aufgaben zu widmen.

**VORSICHT:** Mithilfe zusätzlicher Vorkehrungen muss sichergestellt werden, dass die Bediener vor Gefahren geschützt sind, da ihre Hände den Knopf nicht während der gesamten Bewegung der Presse betätigen müssen.

Der Zugang zur Gefahr muss geschützt werden, z. B. mit Lichtvorhängen, Schutztüren usw. Ein Betätigungsschalter eignet sich in diesem Fall nicht. Diese Sicherheitsvorrichtungen müssen auch an die Eingänge des Funktionsblocks der Pressensteuerung angeschlossen werden.

Der Eingang für die Zyklusinitiierung kann mit dem GO-Knoten des Funktionsblocks der Pressensteuerung oder dem IN-Knoten eines Bypass-Blocks verbunden werden, der mit dem GO-Knoten des Funktionsblocks Pressensteuerung verbunden ist.

Die Vorrichtung zur Zyklusinitiierung muss an einer Stelle montiert werden, die dem folgenden Warnhinweis entspricht.

**WARNUNG:**

- **Sachgemäße Installation von Vorrichtungen zur Zyklusinitiierung**
- Die nicht sachgemäße Installation von Zyklusinitiierungsvorrichtungen kann zu schweren Verletzungen oder zum Tod führen.
- Installieren Sie Zyklusinitiierungsvorrichtungen so, dass sie nur von außen und unter voller Sicht auf den gesicherten Raum zugänglich sind. Zyklusinitiierungsvorrichtungen sind vom gesicherten Raum aus nicht zugänglich. Schützen Sie Zyklusinitiierungsvorrichtungen gegen unbefugte oder versehentliche Betätigung (z. B. durch Ringe oder Schutzeinrichtungen). Wenn es Gefahrenbereiche gibt, die von den Zyklusinitiierungsvorrichtungen aus nicht einsehbar sind, müssen zusätzliche Sicherheitsvorkehrungen getroffen werden.

## 7.5.15 XS/SC26-2: SQS-Funktion (sequenzieller Stopp) der Pressensteuerung

Der SQS-Eingang der Pressensteuerung (sequenzieller Stopp) signalisiert der Pressensteuerung, dass der Pressenstößel eine Position erreicht hat, in der keine Quetschgefahr mehr besteht (eine Lücke von weniger als 6 mm/0,25 Zoll). Die Abwärtsbewegung des Pressenstößels wird an diesem Punkt angehalten. Der Bediener kann die Hände von der Zweihandsteuerung nehmen, um sicherzustellen, dass sich das Werkstück in der richtigen Position befindet (der mutingfähige Sicherheitseingang ist zu diesem Zeitpunkt gemutet). Nachdem der Bediener sichergestellt hat, dass sich das Werkstück in der richtigen Position befindet, aktiviert er den Fußpedal-Eingang, um den Abwärtshub zu beenden.

**Anmerkung:** HINWEIS: Dies ist eine Methode zur Steuerung des Pressensteuerungsprozesses: Es gibt drei zulässige Verfahren:

1. TC1 schaltet den GO-Eingang ein, um den Stößel zum SQS-Punkt zu fahren. TC1 freigeben und FP1 aktivieren, um den Fußpedal-Eingang einzuschalten und den Stößel zum unteren Hubende (BOS) zu fahren, FP1 freigeben und TC1 aktivieren, um den Stößel anzuheben.
2. FP1 schaltet den GO-Eingang ein, um den Stößel zum SQS-Punkt zu fahren, FP1 freigeben. Beim erneuten Aktivieren von FP1 fährt der Stößel zum BOS-Punkt und dann wieder zurück zum TOS-Punkt (oberes Hubende). (Der Fußpedal-Eingang wird deaktiviert, wenn FP1 an den GO-Knoten angeschlossen wird).
3. TC1 schaltet den GO-Eingang ein, um den Stößel zum SQS-Punkt zu fahren, TC1 freigeben. Beim erneuten Aktivieren von TC1 fährt der Stößel zum BOS-Punkt und dann wieder zurück zum TOS-Punkt (oberes Hubende). (Um das System für diese Methode einzurichten, wählen Sie NICHT den Fußpedal-Knoten im Funktionsblock für Pressesteuerungseingänge aus.)

Der SQS-Eingang (sequenzieller Stopp) kann den mutingfähigen Sicherheitseingang direkt muten, oder er kann zusammen mit dem Muting-Sensoreingang der Pressensteuerung arbeiten, um den mutingfähigen Sicherheitseingang der Pressensteuerung zu muten (zum Muting-Sensoreingang der Pressensteuerung siehe XS/SC26-2: Muting-Sensor der Pressesteuerung auf Seite 52).

Bei dem SQS-Eingang (sequenzieller Stopp) kann es sich je nach den Anforderungen des Systems um einen ein- oder zweikanaligen Eingang handeln. Die Eingangsgeräte müssen so positioniert sein, dass der Pressenstößel in einer fingersicheren Position anhält. Das bedeutet, dass keine Lücke vorhanden sein darf, in die ein Finger eindringen könnte. Als fingersichere Lücke gilt eine Lücke von weniger als 6 mm/0,25 Zoll.

**Anmerkung:** Wenn eine einkanalige Konfiguration für den SQS-Eingang (sequenzieller Stopp) gewählt wird, muss diese zusammen mit dem Muting-Sensoreingang der Pressensteuerung funktionieren, um den mutingfähigen Sicherheitsstopp-Eingang der Pressensteuerung zu muten. Wenn eine zweikanalige Konfiguration für den SQS-Eingang (sequenzieller Stopp) gewählt wird, kann sie den mutingfähigen Sicherheitsstopp-Eingang der Pressensteuerung direkt selbst muten.

US-Normen und internationale Normen schreiben vor, dass der Benutzer das Sicherheitssystem so anordnen, installieren und bedienen muss, dass das Personal geschützt ist und dass die Möglichkeit einer Umgehung der Schutzeinrichtung minimiert wird.

**WARNUNG:**

- Vermeidung gefährlicher Installationen
- Ein einkanaliges SQS-Gerät ist nicht zulässig, es sei denn, es wird in Verbindung mit einem PCMS-Eingangsgerät (Muting-Sensor-Eingangsgerät der Pressensteuerung) verwendet. Wenn ein zweikanaliger SQS-Eingang ohne PCMS verwendet wird, muss jeder SQS-Kanal ein unabhängiger Positionsschalter sein und muss so eingestellt bzw. positioniert sein, dass er sich erst dann schließt, wenn die Gefahr nicht mehr besteht, und sich wieder öffnet, wenn der Zyklus abgeschlossen ist oder die Gefahr wieder vorhanden ist. Falsche Einstellung oder Stellung der Schalter kann zu Verletzungen oder Tod führen.
- Der Anwender ist für die Einhaltung sämtlicher örtlichen und nationalen Gesetze, Vorschriften und Bestimmungen über den Einsatz von Sicherheitsausrüstungen bei einer konkreten Anwendung verantwortlich. Achten Sie darauf, dass sämtliche Rechtsvorschriften eingehalten und sämtliche in dieser Anleitung enthaltenen Installations- und Wartungsanweisungen befolgt werden.

SQS-Geräte müssen mindestens die folgenden Anforderungen erfüllen. Wenn das SQS-Gerät als Muting-Eingang mit dem Muting-Sensor der Pressensteuerung verwendet wird, muss das Paar die folgenden Anforderungen erfüllen.

1. Es müssen mindestens zwei unabhängige fest verdrahtete Vorrichtungen verwendet werden.
2. Die Vorrichtungen müssen entweder Schließerkontakte, pnp-Ausgänge (die jeweils die in Spezifikationen und Anforderungen auf Seite 20 aufgeführten Eingangsanforderungen erfüllen müssen) oder antivalentes Schaltverhalten aufweisen. Mindestens einer dieser Kontakte muss schließen, wenn der Schalter betätigt wird, und öffnen (bzw. nicht leiten), wenn der Schalter nicht betätigt wird oder wenn die Stromversorgung ausgeschaltet ist.
3. Die Aktivierung der Eingänge dieser Muting-Funktion muss von separaten Vorrichtungen ausgehen. Diese Vorrichtungen müssen separat installiert werden, damit ein unsicherer Zustand verhindert wird, der aus falscher Einstellung, Fehlausrichtung oder einem einzelnen Gleichtaktfehler entstehen kann, z. B. durch physische Beschädigungen der Montagefläche. Nur eine dieser Vorrichtungen darf durch ein programmierbares Steuergerät (SPS) o. ä. gehen oder davon beeinflusst werden.
4. Die Vorrichtungen müssen so installiert werden, dass sie nicht leicht außer Kraft gesetzt oder umgangen werden können.
5. Die Vorrichtungen müssen so montiert werden, dass ihre physische Position und Ausrichtung nicht einfach geändert werden können.
6. Es darf nicht möglich sein, dass Umweltbedingungen (z. B. extreme Luftverschmutzung) den Muting-Zustand auslösen.
7. Die Vorrichtungen dürfen keine Verzögerungen oder anderen Zeitfunktionen verwenden (es sei denn, diese Funktionen werden so ausgeführt, dass der Ausfall einer einzelnen Komponente die Beseitigung der Gefahr nicht verhindert und weitere Maschinenzyklen ermöglicht, solange der Fehler nicht behoben wurde, und durch Verlängerung der Muting-Periode keine Gefahr erzeugt wird).

## 7.5.16 XS/SC26-2: Muting-Sensor der Pressesteuerung

Das Muting der Sicherheitsvorrichtung ist eine automatisch gesteuerte Aufhebung des mutingfähigen Sicherheitsstopp-Eingangs des Pressensteuerungs-Funktionsblocks während eines Teils des Pressenzyklus, wenn keine unmittelbare Gefahr besteht oder wenn der Zugang zur Gefahr durch andere Mittel geschützt ist. Ordnen Sie die Muting-Sensoren der Pressensteuerung dem M-Sensoreingang des Funktionsblocks Pressensteuerungseingang zu, damit das Muting von mindestens einem der folgenden Sicherheitseingangsgeräte mit dem SQS-Eingang (sequenzieller Stopp) funktioniert:

- Schutztürschalter (Verriegelungsschalter)
- Optosensoren
- Sicherheitsmatten

- Schutzhaltvorrichtungen

US-Normen und internationale Normen schreiben vor, dass der Benutzer das Sicherheitssystem so anordnen, installieren und bedienen muss, dass das Personal geschützt ist und dass die Möglichkeit einer Umgehung der Schutzeinrichtungen minimiert wird.

**WARNUNG:**

- Vermeidung gefährlicher Installationen
- Zwei (1 SQS und 1 Muting-Sensor der Pressensteuerung) oder vier (2 SQS und 2 Muting-Sensoren der Pressensteuerung) unabhängige Positionsschalter müssen richtig eingestellt oder positioniert werden, so dass sie sich erst schließen, wenn die Gefahr nicht mehr besteht, und sich wieder öffnen, wenn der Zyklus abgeschlossen ist oder die Gefahr wieder besteht. Falsche Einstellung oder Stellung der Schalter kann zu Verletzungen oder Tod führen.
- Der Anwender ist für die Einhaltung sämtlicher örtlichen und nationalen Gesetze, Vorschriften und Bestimmungen über den Einsatz von Sicherheitsausrüstungen bei einer konkreten Anwendung verantwortlich. Achten Sie darauf, dass sämtliche Rechtsvorschriften eingehalten und sämtliche in dieser Anleitung enthaltenen Installations- und Wartungsanweisungen befolgt werden.

Der Muting-Sensor der Pressensteuerung (mit dem SQS-Gerät) muss mindestens die folgenden Anforderungen erfüllen:

1. Es müssen mindestens zwei unabhängige fest verdrahtete Vorrichtungen verwendet werden.
2. Die Vorrichtungen müssen entweder Schließerkontakte, pnp-Ausgänge (die jeweils die in Spezifikationen und Anforderungen auf Seite 20 aufgeführten Eingangsanforderungen erfüllen müssen) oder antivalentes Schaltverhalten aufweisen. Mindestens einer dieser Kontakte muss schließen, wenn der Schalter betätigt wird, und öffnen (bzw. nicht leiten), wenn der Schalter nicht betätigt wird oder wenn die Stromversorgung ausgeschaltet ist.
3. Die Aktivierung der Eingänge dieser Muting-Funktion muss von separaten Vorrichtungen ausgehen. Diese Vorrichtungen müssen separat installiert werden, damit ein unsicherer Zustand verhindert wird, der aus falscher Einstellung, Fehlausrichtung oder einem einzelnen Gleichtaktfehler entstehen kann, z. B. durch physische Beschädigungen der Montagefläche. Nur eine dieser Vorrichtungen darf durch ein programmierbares Steuergerät (SPS) o. ä. gehen oder davon beeinflusst werden.
4. Die Vorrichtungen müssen so installiert werden, dass sie nicht leicht außer Kraft gesetzt oder umgangen werden können.
5. Die Vorrichtungen müssen so montiert werden, dass ihre physische Position und Ausrichtung nicht einfach geändert werden können.
6. Es darf nicht möglich sein, dass Umweltbedingungen (z. B. extreme Luftverschmutzung) den Muting-Zustand auslösen.
7. Die Vorrichtungen dürfen keine Verzögerungen oder anderen Zeitfunktionen verwenden (es sei denn, diese Funktionen werden so ausgeführt, dass der Ausfall einer einzelnen Komponente die Beseitigung der Gefahr nicht verhindert und weitere Maschinenzyklen ermöglicht, solange der Fehler nicht behoben wurde, und durch Verlängerung der Muting-Periode keine Gefahr erzeugt wird).

## 7.5.17 XS/SC26-2: Fußpedal

Der Fußpedal-Eingang kann auf verschiedene Weise mit den Funktionsblöcken der Pressensteuerung verwendet werden:

- Er kann mit dem GO-Knoten des Funktionsblocks der Pressensteuerung als Zyklusinitiierungsvorrichtung verbunden werden, wenn der Block auf Einzelauslösersteuerung eingestellt ist.
- Er kann mit dem GO-Knoten des Funktionsblocks der Pressensteuerung verbunden werden, wenn er für die manuelle Einstellung des Aufwärtshubs konfiguriert und der SQS-Eingang aktiviert ist. (Die Aktivierung des FP1-Eingangs treibt den Stößel zum SQS-Punkt. Zu diesem Zeitpunkt wird FP1 freigegeben. Da der Eingang für den mutingfähigen Sicherheitsstopp jetzt gemutet ist, kann der Bediener das Werkstück einstellen. Durch erneutes Aktivieren von FP1 fährt der Stößel zum BOS-Punkt und dann wieder zurück zum TOS-Punkt.)
- Er kann wie im folgenden Abschnitt beschrieben verwendet werden.

Der Fußpedal-Eingang kann dem Funktionsblock Pressensteuerungseingang hinzugefügt und konfiguriert werden, wenn der SQS-Eingang konfiguriert wird. Die Presse stoppt am SQS-Eingang, so dass der Bediener die Hände vom Eingang der Zweihandsteuerung nehmen kann. Der Bediener kann sicherstellen, dass das Werkstück richtig positioniert ist, und muss das Werkstück gelegentlich festhalten. Der Bediener kann dann das mit dem Fußpedal-Eingang verbundene Eingangsgerät aktivieren, um die Presse wieder zu aktivieren und den Prozess zu beenden.

Der Fußpedal-Eingang kann auch auf den GO-Knoten der Presse konfiguriert werden. In diesem Fall kann das Fußpedal mit und ohne SQS-Konfiguration verwendet werden. Dies ermöglicht mehr Flexibilität für verschiedene Anwendungen.

Ein physischer Ein/Aus-Eingang oder ein Fußpedal-Eingang kann an den Fußpedal-Eingang des Funktionsblocks Pressensteuerungseingang angeschlossen werden. Bei dem Gerät kann es sich um ein Fußpedal handeln, aber auch andere Auslösegeräte kommen in Frage.

Der Zugang zur Gefahr muss mit anderen Mitteln als dem Eingangsgerät des mutingfähigen Sicherheitsstopps verhindert werden (z. B. muss die innere Öffnung fingersicher sein, weniger als 6 mm/0,25 Zoll). Der Schutz kann auch durch Sicherheitsvorrichtungen gewährleistet werden, die an den nicht mutingfähigen Sicherheitsstopp-Eingang angeschlossen sind.

**VORSICHT:** Es müssen andere Mittel vorgesehen werden, um sicherzustellen, dass die Bediener vor den Gefahren geschützt sind, da ihre Hände bei dieser letzten Bewegung der Presse nicht den Knopf betätigen müssen.

Der Eingang kann ein- oder zweikanalig sein (2 Schließer oder 1 Schließer/1 Öffner).

# 7.6 Nicht sicherheitsrelevante Eingangsgeräte

Zu den nicht sicherheitsrelevanten Eingangsgeräten gehören manuelle Reset-Vorrichtungen, Ein-/Aus-Schalter, Muting-Freigabevorrichtungen und Abbruchverzögerungseingänge.

**Manuelle Reset-Vorrichtungen**: dienen zum Generieren eines Reset-Signals für einen Ausgang oder Funktionsblock, der für einen manuellen Reset konfiguriert wurde, wenn zum Einschalten des Ausgangs des betreffenden Blocks eine Aktion des Bedieners erforderlich ist. Resets können auch mit einem virtuellen Reset-Eingang erstellt werden. Siehe Virtuelle nicht sicherheitsrelevante Eingangsgeräte (XS/SC26-2 ab FID 2 und SC10-2) auf Seite 57.

**WARNUNG: Nicht überwachte Resets**

**Wenn ein Reset ohne Überwachung (entweder für einen verriegelten Ausgang oder ein System-Reset) konfiguriert ist** und alle anderen Bedingungen für einen Reset gegeben sind, **werden die Sicherheitsausgänge durch einen Kurzschluss vom Reset-Anschluss an +24 V sofort eingeschaltet**.

**Ein/Aus-Schalter**: sendet einen Ein- bzw. Ausschaltbefehl an die Maschine. Wenn alle steuernden Sicherheitseingänge im Ein-Zustand sind, kann der Sicherheitsausgang mit dieser Funktion ein- bzw. ausgeschaltet werden. Dies ist ein einkanaliges Signal; bei 24 V DC ergibt sich ein Ein-Zustand und bei 0 V DC ergibt sich ein Aus-Zustand. Ein Eingang für das Ein-/Ausschalten kann ohne Zuordnung zu einem Sicherheitsausgang hinzugefügt werden, wodurch dieser Eingang nur einen Statusausgang steuern kann. Ein Ein/Aus-Schalter kann auch mit einem virtuellen Eingang erstellt werden. Siehe Virtuelle nicht sicherheitsrelevante Eingangsgeräte (XS/SC26-2 ab FID 2 und SC10-2) auf Seite 57.

XS/SC26-2 ab FID 4: Die Eingänge zum Ein-/Ausschalten werden zur Moduswahl des Funktionsblocks Pressensteuerungsmodus verwendet. Drei separate Eingänge sind erforderlich, um diesen Block zu erfüllen. Der Block akzeptiert virtuelle Eingänge zum Ein-/Ausschalten.

**Muting-Freigabeschalter**: signalisiert dem Sicherheitskontroller, wenn die Muting-Sensoren eine Muting-Funktion ausführen dürfen. Wenn die Muting-Aktivierungsfunktion konfiguriert ist, werden die Muting-Sensoren erst für die Ausführung einer Muting-Funktion aktiviert, wenn das Muting-Freigabesignal im Ein-Zustand ist. Dies ist ein einkanaliges Signal; bei 24 V DC ergibt sich der Freigabezustand (Ein-Zustand) und bei 0 V DC ergibt sich der Aus-Zustand (Stoppzustand). Ein Muting-Freigabeschalter kann auch mit einem virtuellen Eingang erstellt werden. Siehe Virtuelle nicht sicherheitsrelevante Eingangsgeräte (XS/SC26-2 ab FID 2 und SC10-2) auf Seite 57.

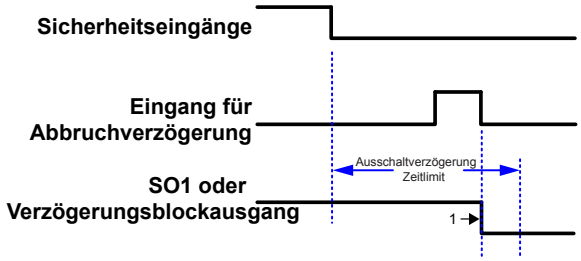
**Vorrichtungen für den Abbruch von Ausschaltverzögerungen**: bieten die Möglichkeit, eine konfigurierte Ausschaltverzögerungszeit eines Sicherheitsausgangs oder eines Verzögerungsblockausgangs zu stornieren oder eine konfigurierte One-Shot-Zeit eines One-Shot-Blockausgangs zu stornieren. Diese Funktion bewirkt Folgendes:

- Sie sorgt dafür, dass der Sicherheits- oder Verzögerungsblockausgang eingeschaltet bleibt.
- Sie schaltet den Sicherheits- oder Verzögerungsblockausgang oder den One-Shot-Blockausgang sofort aus, nachdem der Sicherheitskontroller ein Signal für den Abbruch der Ausschaltverzögerung empfängt.
- Wenn für **Cancel Type (Abbruchtyp)** die Einstellung „Control Input (Steuereingang)“ gewählt ist, bleibt der Sicherheits- oder Verzögerungsblockausgang eingeschaltet, wenn sich der Eingang vor dem Ende der Verzögerung wieder einschaltet. (Dies gilt nicht für einen One-Shot-Blockausgang.)

Eine Statusausgabefunktion (Ausgangsverzögerung läuft) gibt an, wenn ein Abbruchverzögerungseingang aktiviert werden kann, um den Sicherheitsausgang mit der Ausschaltverzögerung eingeschaltet zu lassen. Eine Vorrichtung für den Abbruch von Ausschaltverzögerungen kann auch mit einem virtuellen Eingang erstellt werden. Siehe Virtuelle nicht sicherheitsrelevante Eingangsgeräte (XS/SC26-2 ab FID 2 und SC10-2) auf Seite 57.

## Zeitgeber für den Abbruch von Aus-Verzögerungen

*Abbildung 21. Sicherheitseingang verbleibt im Stopp-Modus*




Anmerkung 1: Wenn die Funktion „Ausgang ausschalten“ gewählt ist

*Abbildung 22. Ausgang schaltet sich aus*

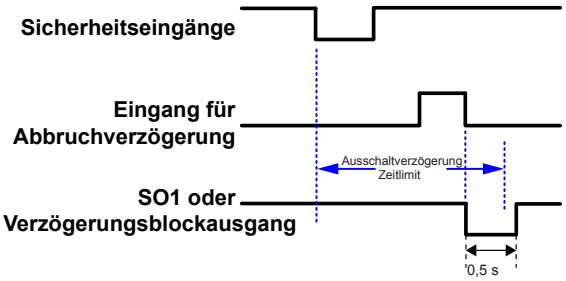



*Abbildung 23. Ausgang bleibt für Sicherheitseingänge mit Latch-Reset eingeschaltet*

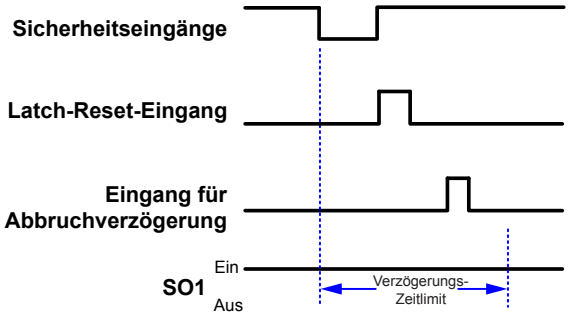
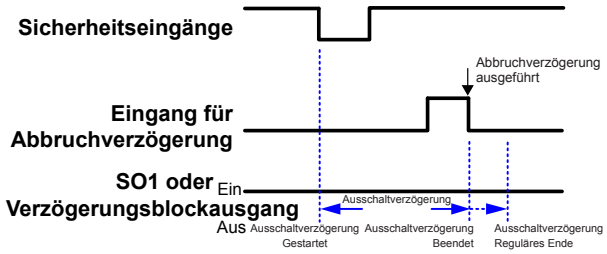



*Abbildung 24. Ausgang bleibt für Sicherheitseingänge ohne Latch-Reset eingeschaltet*




# 7.6.1 Manueller Reset-Eingang

Der manuelle Reset-Eingang kann so konfiguriert werden, dass eine beliebige Kombination der folgenden Funktionen ausgeführt wird (siehe Hinzufügen von Eingängen und Statusausgängen auf Seite 78):

**Reset von Sicherheitseingängen**

Versetzt den Ausgang der Latch-Reset-Blöcke vom Verriegelungszustand in den Ein-Zustand, wenn sich der IN-Knoten im Ein-Zustand befindet.

**Reset von Sicherheitsausgängen**

Schaltet den Ausgang ein, wenn der für den Latch-Reset konfigurierte Ausgangsblock EIN ist.

*Ausnahmen:*

Ein Sicherheitsausgang kann nicht für die Verwendung eines manuellen Reset konfiguriert werden, wenn dieser mit einem Zweihandsteuerungseingang oder einem Zustimmtaster-Funktionsblock verbunden ist.

**System-Reset**

Versetzt das System von einem durch einen Systemfehler verursachten Sperrzustand in den Ein-Zustand, wenn die Fehlerursache beseitigt wurde. Mögliche Szenarien, bei denen ein Systemreset erforderlich sein kann:

- Es werden Signale auf nicht verwendeten Anschlussstiften erfasst.
- Zeitüberschreitung bei Konfigurationsmodus
- Beenden des Konfigurationsmodus
- Interne Fehler
- Fehler in der Pressensteuerung

**Anmerkung:** Zum Abschließen der Bestätigung einer neuen Konfiguration kann ein manueller Reset als Systemreset ausgewählt und durchgeführt werden, damit das Gerät nicht aus- und wieder eingeschaltet werden muss.

**Ausgangsfehler-Reset**

Löscht den Fehler und ermöglicht es dem Ausgang, sich wieder einzuschalten, wenn die Ursache für den Fehler beseitigt wurde. Mögliche Szenarien, bei denen ein Ausgangsfehler-Reset erforderlich sein kann:

- Ausgangsfehler
- EDM- oder AVM-Fehler

**Manueller Reset bei Netzeinschaltung**

Ermöglicht es, diverse Latch-Reset-Blöcke und/oder Ausgangsblöcke nach der Netzeinschaltung durch einen einzelnen Reset-Eingang steuern zu lassen.

**Freigabe-Modus beenden**

Zum Beenden des Freigabe-Modus ist ein Reset erforderlich.

**Eingangsanzeigegruppen-Reset**

Setzt die Funktion **Eingangsgruppe verfolgen** des Statusausgangs und die Funktion des virtuellen Funktion **Eingangsgruppe verfolgen** des Statusausgangs zurück.

**Der Reset-Schalter muss an einer Position montiert werden, die die Anforderungen des nachstehenden Warnhinweises erfüllt.** Ein schlüsselbetätigter Reset-Schalter bietet eine gewisse Kontrolle durch den Bediener oder die Aufsicht, weil der Schlüssel aus dem Schalter entfernt und in den Schutzbereich mitgenommen werden kann. Allerdings werden unbefugte oder unbeabsichtigte Resets mit Ersatzschlüsseln im Besitz anderer dadurch nicht verhindert; auch das unbemerkte Eintreten weiterer Personen in das Schutzfeld (Hintertretungsgefahr) wird nicht verhindert.

**WARNUNG: Reset-Schalterpositionen**

**Alle Reset-Schalter dürfen nur von außen zugänglich sein und müssen die uneingeschränkte Sicht auf den Gefahrenbereich ermöglichen. Reset-Schalter müssen sich zudem vom geschützten Bereich aus außer Reichweite befinden und vor unbefugter oder unbeabsichtigter Betätigung** geschützt sein (z. B. durch den Einsatz von Ringen oder Schutzeinrichtungen). Können Bereiche von den Reset-Schaltern aus nicht eingesehen werden, so müssen zusätzliche Schutzeinrichtungen bereitgestellt werden. **Wenn diese Anweisungen nicht befolgt werden, können schwere oder tödliche Verletzungen die Folge sein.**

**Wichtig:** Durch Zurücksetzen einer Schutzeinrichtung darf keine gefährliche Maschinenbewegung in Gang gesetzt werden. Zur Gewährleistung sicherer Arbeitsverfahren muss ein sicheres Anlaufverfahren eingehalten werden, und die Person, die den Reset ausführt, muss **vor jedem Zurücksetzen einer Schutzeinrichtung prüfen**, ob der gesamte Gefahrenbereich frei von Personen ist. Wenn von dort, wo sich der Reset-Schalter befindet, ein Bereich nicht eingesehen werden kann, müssen zusätzliche Schutzeinrichtungen verwendet werden, mindestens visuelle und akustische Warnungen über den Maschinenanlauf.

**Anmerkung: Automatischer Reset** lässt ohne Eingreifen durch eine Person einen Ausgang zurück in den Ein-Zustand wechseln, sobald die Eingangsgeräte zum Ein-Zustand wechseln und sich alle anderen Logikblöcke im Ein-Zustand befinden. Der automatische Reset wird auch als „Schaltmodus“ bezeichnet. Er wird normalerweise in Anwendungen verwendet, in denen die Person ständig vom Sicherheitseingangsgerät erfasst wird.

**WARNUNG: Automatischer Anlauf**

Bei der Netzeinschaltung schalten die für automatische Netzeinschaltung konfigurierten Sicherheitsausgänge und Latch-Reset-Blöcke ihre Ausgänge ein, wenn sich alle zugehörigen Eingänge im Ein-Zustand befinden. Wenn ein manueller Reset erforderlich ist, müssen die Ausgänge für einen manuellen Netzeinschaltungsmodus konfiguriert werden.

## Automatische & manuelle Reset-Eingänge, die demselben Sicherheitsausgang zugeordnet sind

Standardmäßig sind die Sicherheitsausgänge für den automatischen Reset (Schaltmodus) konfiguriert. Sie können als Latch-Reset unter Verwendung des Attributs „Eigenschaften Halbleiterausgang“ des Sicherheitsausgangs konfiguriert werden (siehe Funktionsblöcke auf Seite 105).

Sicherheitseingangsgeräte funktionieren als automatischer Reset, sofern nicht ein Latch-Reset-Block hinzugefügt wird. Wird ein Latch-Reset-Block in Reihe mit einem für den Latch-Reset-Modus konfigurierten Ausgang hinzugefügt, können dieselben oder andere Eingangsgeräte für manuellen Reset zum Zurücksetzen des Latch-Reset-Blocks und der Sicherheitsausgangs-Verriegelung verwendet werden. Wird dasselbe Eingangsgerät für manuellen Reset für beide Zwecke verwendet und befinden sich alle Eingänge im Ein-Zustand, entriegelt eine einzelne Reset-Aktion den Funktionsblock und den Ausgangsblock. Bei Verwendung verschiedener Eingangsgeräte für manuellen Reset muss der mit dem Sicherheitsausgang verbundene Reset zuletzt aktiviert werden. Dies kann zum Erzwingen einer Reset-Sequenz dienen, mit der Hintertretungsgefahren in Bereichssicherungen gemindert oder beseitigt werden können (siehe Eigenschaften von Sicherheitseingangsgeräten auf Seite 31).

Wenn die steuernden Eingänge zu einem Latch-Reset-Block oder einem Sicherheitsausgangsblock nicht im Ein-Zustand sind, wird der Reset für den betreffenden Block ignoriert.

### Reset-Signalanforderungen

Reset-Eingangsgeräte zurücksetzen kann für den überwachten oder den nicht überwachten Betrieb konfiguriert werden:

**Überwachter Reset**: Das Reset-Signal muss von Aus (0 V DC) auf Ein (24 V DC) und dann wieder ausschalten (0 V DC). Die Dauer des Ein-Zustands muss 0,5 Sekunden bis 2 Sekunden betragen. Dies wird als abfallender Flankenreset bezeichnet.

**Nicht überwachter Reset**: Das Reset-Signal muss nur von Aus (0 V DC) auf Ein (24 V DC) umschalten und mindestens 0,5 Sekunden auf Ein bleiben. Nach dem Reset kann das Reset-Signal entweder Ein oder Aus sein. Dies wird als ansteigender Flankenreset bezeichnet.

## 7.7 Virtuelle nicht sicherheitsrelevante Eingangsgeräte (XS/SC26-2 ab FID 2 und SC10-2)

Für alle virtuellen Eingänge ist FID 2 oder höher für den XS/SC26-2 erforderlich. Die virtuellen nicht sicherheitsrelevanten Eingangsgeräte umfassen Geräte für manuellen Reset, Ein/Aus-Schaltung, Muting-Aktivierung und Abbruch der Ausschaltverzögerung.

**WARNUNG:** Virtuelle nicht sicherheitsrelevante Eingänge dürfen niemals für die Steuerung von sicherheitskritischen Anwendungen verwendet werden. Wenn ein virtueller nicht sicherheitsrelevanter Eingang für die Steuerung einer sicherheitskritischen Anwendung verwendet wird, ist ein gefährlicher Ausfall möglich, der zu schweren oder tödlichen Verletzungen führen kann.

**Wichtig:** Durch Zurücksetzen einer Schutzeinrichtung darf keine gefährliche Maschinenbewegung in Gang gesetzt werden. Zur Gewährleistung sicherer Arbeitsverfahren muss ein sicheres Anlaufverfahren eingehalten werden, und die Person, die den Reset ausführt, muss vor jedem Zurücksetzen einer Schutzeinrichtung prüfen, ob der gesamte Gefahrenbereich frei von Personen ist. Wenn von dort, wo sich der Reset-Schalter befindet, ein Bereich nicht eingesehen werden kann, müssen zusätzliche Schutzeinrichtungen verwendet werden, mindestens visuelle und akustische Warnungen über den Maschinenanlauf.

### 7.7.1 Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD)

Gemäß Abschnitt 5.2.2 der Norm EN ISO 13849-1:2015 ist eine "bewusste Handlung" durch den Maschinenbediener erforderlich, um eine Sicherheitsfunktion zurückzusetzen. Traditionell wird diese Anforderung erfüllt, indem ein mechanischer Schalter verwendet wird und die zugehörigen Leitungen an die angegebenen Anschlussklemmen am Sicherheitskontroller angeschlossen werden. Bei einem überwachten Reset müssen die Kontakte innerhalb des korrekten Zeitraums zuerst geöffnet, dann geschlossen und dann wieder geöffnet werden. Wenn der Zeitraum weder zu kurz noch zu lang ist, wird die Handlung als bewusst bewertet und der Reset wird ausgeführt.

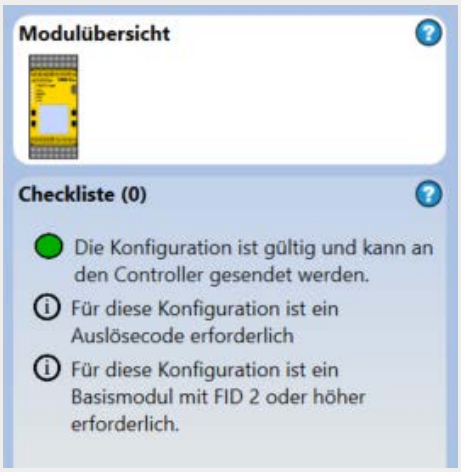
Banner Engineering hat eine virtuelle Reset-Lösung entwickelt, die eine bewusste Handlung erfordert. Zum Beispiel kann anstelle des mechanischen Schalters eine HMI verwendet werden. Anstelle der Leitungen wird ein eindeutiger Auslösecode für jeden Sicherheitskontroller im Netzwerk verwendet. Außerdem wird jeder virtuelle Reset innerhalb eines Sicherheitskontrollers einem bestimmten Bit in einem Register zugeordnet. Dieses Bit muss zusammen mit dem Auslösecode in koordinierter Weise geschrieben und gelöscht werden. Wenn die Schritte in der richtigen Abfolge und im richtigen Zeitrahmen ausgeführt werden, gilt die Handlung als bewusst und der Reset wird ausgeführt.

Die Standards verlangen zwar keine „bewusste Handlung“, um eine virtuelle Abbruchverzögerung auszuführen, aber um weitere Komplexität zu vermeiden, hat Banner Engineering diese Funktion in derselben Weise implementiert wie den virtuellen manuellen Reset.

Der Benutzer muss übereinstimmende Auslösecodes auf dem Sicherheitskontroller und dem steuernden Netzwerkgerät (SPS, HMI usw.) festlegen. Der Auslösecode gehört zu den Netzwerkeinstellungen und ist nicht in der CRC der Konfiguration enthalten. Es besteht keine Werksvoreinstellung für den Auslösecode. Der Benutzer muss auf dem Bildschirm **Netzwerkeinstellungen** einen einrichten. Der Auslösecode kann für bis zu 2 Sekunden aktiviert werden, um wirksam zu sein. Verschiedene Sicherheitskontroller im selben Netzwerk sollten verschiedene Auslösecodes haben.

**Anmerkung:** Wenn ein virtueller manueller Reset oder eine Abbruchverzögerung in der Funktionsansicht hinzugefügt wird, wird der Checkliste ein Hinweis hinzugefügt, dass unter **Netzwerkeinstellungen** ein Auslösecode eingegeben werden muss.

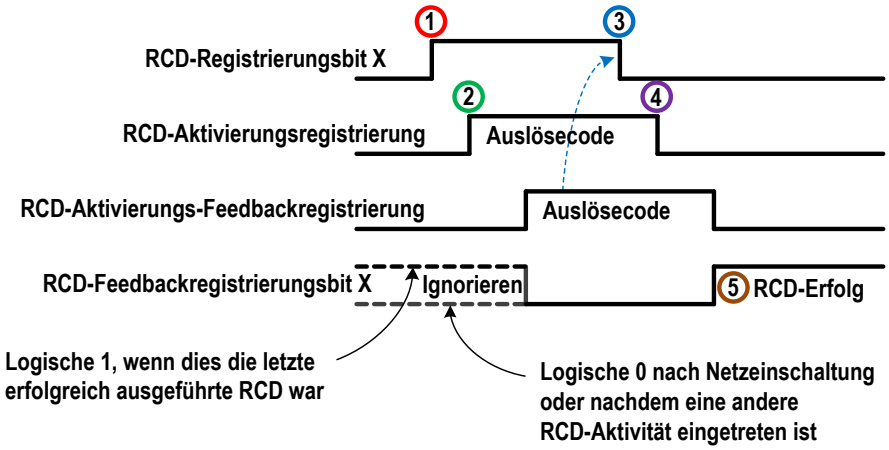
*Abbildung 25. Beispiel einer Checklisten-Warnung*




Der HMI/SPS-Programmierer kann je nach Präferenz zwischen zwei verschiedenen Methoden auswählen: einer Feedback-basierten Sequenz und einer zeitgeschalteten Sequenz. Diese Methoden werden in den folgenden Abbildungen beschrieben. Der tatsächliche Speicherort des Registers hängt davon ab, welches Protokoll verwendet wird.

### Virtuelle Reset- oder Abbruchverzögerungssequenz (RCD) – Feedbackmethode

*Abbildung 26. Virtuelle Reset- oder Abbruchverzögerungssequenz (RCD) - Feedbackmethode*



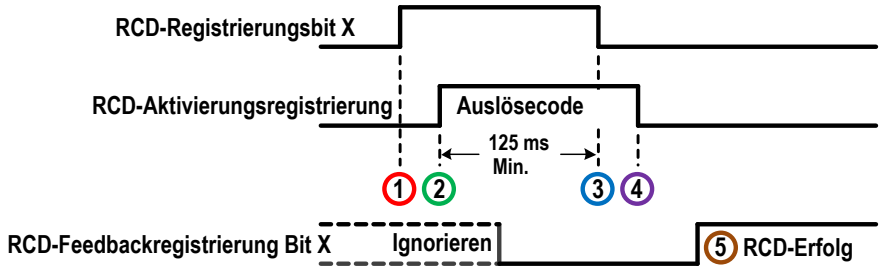

1. Schreiben Sie eine logische 1 in das oder die RCD-Registerbit(s), die der gewünschten virtuellen Reset- oder Abbruchverzögerung entsprechen.
2. Schreiben Sie zugleich oder irgendwann später den Betätigungscode in das RCD-Aktivierungsregister.
3. Überwachen Sie das RCD-Aktivierungs-Feedbackregister, damit der Betätigungscode angezeigt wird (125 ms typisch). Schreiben Sie dann eine logische 0 in das RCD-Registerbit.
4. Schreiben Sie zugleich oder irgendwann später den Betätigungscode in das RCD-Aktivierungsregister. Dieser Schritt muss innerhalb von 2 Sekunden ab dem ersten Schreiben des Codes (Schritt 2) abgeschlossen sein.
5. Überwachen Sie das RCD-Feedbackregister, sofern gewünscht, um festzustellen, ob die gewünschte Reset- oder Abbruchverzögerung akzeptiert wurde (175 ms typisch).

**Anmerkung:** Die verschiedenen benötigten Register-Bits finden Sie auf der Registerkarte „Industrial Ethernet“ in der grafischen Benutzeroberfläche, indem Sie die Auswahl „Virtual Status Output (Virtueller Statusausgang)“ in „Virtual Non-Safety Inputs (Virtuelle nicht sicherheitsrelevante Eingänge)“ ändern. Der Auslösecode wird vom Benutzer unter dem Symbol „Netzwerkeinstellungen“ in der Symbolleiste erstellt.

**Anmerkung:** Eine AOI und ein SPS-Funktionsblock sind unter www.bannerengineering.com auf der Produktseite des Sicherheitskontrollers verfügbar. Der AOI-Ordner enthält eine lesbare Datei zum Reset von Banner SC10 SC26 XS26 und zur Aktivierung der Abbruchverzögerung, die zur Erläuterung des Verfahrens beiträgt.

### Virtuelle Reset- oder Abbruchverzögerungssequenz (RCD) – zeitgeschaltete Methode

*Abbildung 27. Virtuelle Reset- oder Abbruchverzögerungssequenz (RCD) - zeitgeschaltete Methode*




1. Schreiben Sie eine logische 1 zu den RCD-Registerbit(s), die der gewünschten virtuellen Reset- oder Abbruchverzögerung entsprechen.
2. Schreiben Sie zugleich oder irgendwann später den Betätigungscode in das RCD-Aktivierungsregister.
3. Schreiben Sie mindestens 125 ms nach Schritt 2 eine logische 0 in das RCD-Registerbit.
4. Schreiben Sie zugleich oder irgendwann später den Betätigungscode (schreiben Sie eine logische 0 in das RCD-Aktivierungsregister). Dieser Schritt muss innerhalb von 2 Sekunden ab dem ersten Schreiben des Codes (Schritt 2) abgeschlossen sein.
5. Überwachen Sie das RCD-Feedbackregister, sofern gewünscht, um festzustellen, ob die gewünschte Reset- oder Abbruchverzögerung akzeptiert wurde (175 ms typisch).

**Virtuelle manuelle Reset-Vorrichtungen** dienen zum Generieren eines Reset-Signals für einen Ausgang oder Funktionsblock, der für einen manuellen Reset konfiguriert wurde, wenn zum Einschalten des Ausgangs des betreffenden Blocks eine Aktion des Bedieners erforderlich ist. Resets können auch mit einem physischen Reset-Eingang erstellt werden. Siehe Nicht sicherheitsrelevante Eingangsgeräte auf Seite 54.

**WARNUNG: Virtueller manueller Reset**

Ein virtueller manueller Reset, der zur Ausführung einer manuellen Netzeinschaltfunktion zusammen mit Geräten an diversen Standorten in demselben Netzwerk konfiguriert ist, sollte vermieden werden, außer wenn die Sicherheit aller Gefahrenbereiche bestätigt wurde.

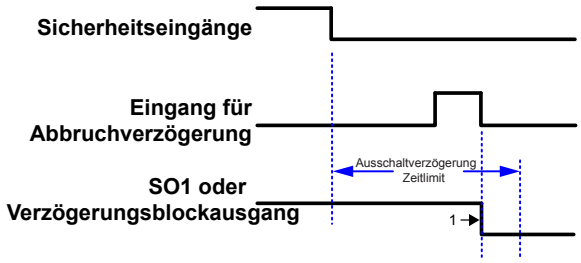
**Virtuelle Vorrichtungen für den Abbruch von Ausschaltverzögerungen:** bieten die Möglichkeit, eine konfigurierte Ausschaltverzögerungszeit zu stornieren. Diese Funktion bewirkt Folgendes:

- Sie sorgt dafür, dass der Sicherheits- oder Verzögerungsblockausgang eingeschaltet bleibt.
- Sie schaltet den Sicherheits- oder Verzögerungsblockausgang oder den One-Shot-Blockausgang sofort aus, nachdem der Sicherheitskontroller ein Signal für den Abbruch der Ausschaltverzögerung empfängt.
- Wenn für **Abbruchtyp** die Einstellung „Steuereingang“ gewählt ist, bleibt der Sicherheits- oder Verzögerungsblockausgang eingeschaltet, wenn sich der Eingang vor dem Ende der Verzögerung wieder einschaltet.

Eine Statusausgabefunktion (Ausgangsverzögerung läuft) gibt an, wenn ein Abbruchverzögerungseingang aktiviert werden kann, um den Sicherheitsausgang mit der Ausschaltverzögerung eingeschaltet zu lassen. Eine Vorrichtung für den Abbruch von Ausschaltverzögerungen kann auch mit einem physischen Eingang erstellt werden. Siehe Nicht sicherheitsrelevante Eingangsgeräte auf Seite 54.

## Zeitablauffunktion für den virtuellen Abbruch einer Ausschaltverzögerung

*Abbildung 28. Sicherheitseingang verbleibt im Stopp-Modus*




Anmerkung 1: Wenn die Funktion „Ausgang ausschalten“ gewählt ist

*Abbildung 29. Ausgang schaltet sich aus*

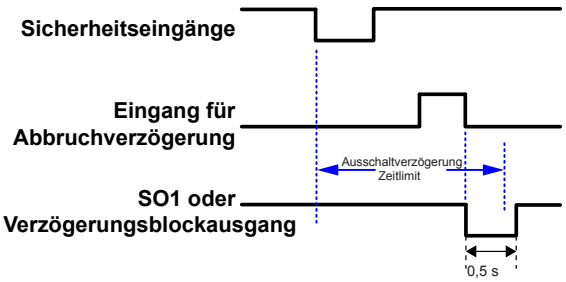


*Abbildung 30. Ausgang bleibt für Sicherheitseingänge mit Latch-Reset eingeschaltet*

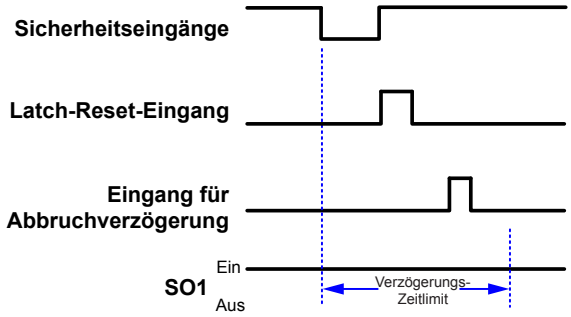
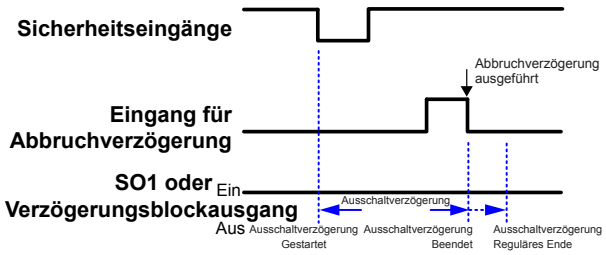



*Abbildung 31. Ausgang bleibt für Sicherheitseingänge ohne Latch-Reset eingeschaltet*




## 7.7.2 Virtuelle Ein-/Ausschaltung und Muting-Aktivierung

**Virtuelle Ein-/Ausschaltung**

Sendet einen EIN- bzw. AUS-Befehl an die Maschine. Wenn alle steuernden Sicherheitseingänge im Ein-Zustand sind, kann der Sicherheitsausgang mit dieser Funktion ein- bzw. ausgeschaltet werden. Der Ein-Zustand ist eine logische 1 und der Aus-Zustand ist eine logische 0. Ein virtueller Ein/Aus-Eingang kann ohne Zuordnung zu einem Sicherheitsausgang hinzugefügt werden, um einen nicht sicherheitsrelevanten Statusausgang zu steuern. Ein Ein/Aus-Schalter kann auch mit einem physischen Eingang erstellt werden. Siehe Nicht sicherheitsrelevante Eingangsgeräte auf Seite 54.

XS/SC26-2 ab FID4: Die virtuellen Ein/Aus-Eingänge werden zur Moduswahl des Pressensteuerungsmodus-Funktionsblocks verwendet. Drei separate Eingänge sind erforderlich, um diesen Block zu erfüllen. Der Block akzeptiert Ein/Aus-Eingänge.

**Virtuelle Muting-Aktivierung**

Signalisiert dem Sicherheitskontroller, wenn die Muting-Sensoren eine Muting-Funktion ausführen dürfen. Wenn die Muting-Aktivierungsfunktion konfiguriert ist, werden die Muting-Sensoren erst für die Ausführung einer Muting-Funktion aktiviert, wenn das Muting-Freigabesignal im Ein-Zustand ist. Der Aktivierungszustand (Ein-Zustand) ist eine logische 1 und der Deaktivierungszustand (Aus-Zustand) ist eine logische 0. Ein Muting-Freigabeschalter kann außerdem unter Verwendung eines physischen Eingangs erstellt werden. Siehe Nicht sicherheitsrelevante Eingangsgeräte auf Seite 54.

# 7.8 Sicherheitsausgänge

### XS/SC26-2

Der Basiskontroller verfügt über zwei Paare mit Sicherheits-Transistorausgängen (Anschlüsse SO1a und b sowie SO2a und b). Diese Ausgänge liefern bis zu je 500 mA bei 24 V DC. Jeder redundante Sicherheits-Transistorausgang kann so konfiguriert werden, dass die Ausgänge einzeln oder paarweise funktionieren. Beispielsweise kann der Ausgang für den unabhängigen Betrieb von SO1a und SO1b geteilt werden, oder SO1 kann als zweikanaliger Ausgang verwendet werden.

Weitere Sicherheitsausgänge können durch Integration von Eingangs-/Ausgangsmodulen zu erweiterbaren Ausführungen des Basiskontrollers hinzugefügt werden. Bei diesen weiteren Sicherheitsausgängen kann es sich um isolierte Relaisausgänge handeln, mit denen ein breites Spektrum an elektrischen Geräten gesteuert/geschaltet werden kann (siehe XS/SC26-2 – Spezifikationen auf Seite 20).

### SC10-2

Der SC10-2 hat zwei isolierte redundante Relaisausgänge. Jeder Relaisausgang verfügt über drei unabhängige Kontaktsätze. Siehe Spezifikationen für den SC10-2 auf Seite 22 für Überlegungen zu Nennwerten und Abzügen.

## XS/SC26-2 und SC10-2

**WARNUNG:** Die Sicherheitsausgänge müssen so an die Maschinensteuerung angeschlossen werden, dass das sicherheitsrelevante Steuersystem der Maschine den Schaltkreis zu den primären Steuerelementen der Maschine unterbricht, um einen sicheren Zustand herbeizuführen.

Schließen Sie Zwischengeräte (z. B. SPS, PES oder PC), die ausfallen könnten, nicht so an, dass es zu Verlust des Sicherheitsabschaltungsbefehls kommt, oder dass die Schutzfunktion aufgehoben, außer Kraft gesetzt oder umgangen werden kann, es sei denn, der Anschluss erfolgt mit demselben oder einem höheren Grad an Sicherheit.

Die folgende Liste enthält eine Beschreibung weiterer Knoten und Attribute, die im Fenster **Eigenschaften** für den Sicherheitsausgangs-Funktionsblock konfiguriert werden können (siehe Hinzufügen von Eingängen und Statusausgängen auf Seite 78):

**EDM (externe Geräteüberwachung)**

Ermöglicht dem Sicherheitskontroller die Überwachung der gesteuerten Geräte (FSDs und MPSEs) für eine geeignete Reaktion auf den Abschaltungsbefehl der Sicherheitsausgänge. **Es wird dringend empfohlen, EDM (oder AVM)** in die Maschinenkonstruktion und in die Konfiguration des Sicherheitskontrollers einzubeziehen, um eine angemessene Integrität der Sicherheitsschaltungen zu gewährleisten (siehe EDM- und Endschaltgeräteanschluss auf Seite 67).

**AVM (einstellbare Ventilüberwachung)**

Ermöglicht dem Sicherheitskontroller die Überwachung von Ventilen und anderen Vorrichtungen, die im aktivierten Zustand bzw. in aktivierter Position langsam reagieren, stagnieren oder ausfallen und deren Betrieb nach dem Eintreten eines Stoppsignals überprüft werden muss. Bis zu drei AVM-Eingänge können ausgewählt werden, wenn EDM nicht verwendet wird**. Es wird dringend empfohlen, AVM (oder EDM)** in die Maschinenkonstruktion und in die Konfiguration des Sicherheitskontrollers einzubeziehen, um eine angemessene Integrität der Sicherheitsschaltungen zu gewährleisten (siehe AVM-Funktion (Adjustable Valve Monitoring, einstellbare Ventilüberwachung) auf Seite 45).

**LR (Latch-Reset)**

Sorgt dafür, dass der SO- oder RO-Ausgang ausgeschaltet bleibt, bis der Eingang in den Ein-Zustand wechselt und ein manueller Reset ausgeführt wird. Unter Manueller Reset-Eingang auf Seite 55 erhalten Sie weitere Informationen.

**RE (Reset aktivieren)**

Diese Option wird nur angezeigt, wenn **LR (Latch-Reset)** aktiviert ist. Der **Latch-Reset** kann durch Auswahl von **Reset aktivieren** gesteuert werden, um das Zurücksetzen des Sicherheitsausgangs in den Ein-Zustand zu beschränken.

**FR (Systemfehler-Reset)**

Liefert eine manuelle Reset-Funktion, wenn Eingangsfehler auftreten. Der FR-Knoten muss mit dem manuellen Reset-Schalter bzw. -Signal verbunden werden. Diese Funktion dient dazu, den SO- oder RO-Ausgang ausgeschaltet zu lassen, bis der Fehler des Eingangsgeräts behoben ist, das fehlerhafte Gerät sich im Ein-Zustand befindet und ein manueller Reset ausgeführt wurde. Diese Funktion ersetzt die Methode der Stromaus- und -wiedereinschaltung zum Zurücksetzen des Zyklus. Unter Manueller Reset-Eingang auf Seite 55 erhalten Sie weitere Informationen.

**Anlaufmodus**

Der Sicherheitsausgang kann für drei Anlaufszenarien (Betriebseigenschaften beim Anlegen der Stromversorgung) konfiguriert werden:

- Normaler Anlaufmodus (Standard)
- Manuelle Netzeinschaltung
- Automatische Netzeinschaltung

Unter Manueller Reset-Eingang auf Seite 55 erhalten Sie weitere Informationen.

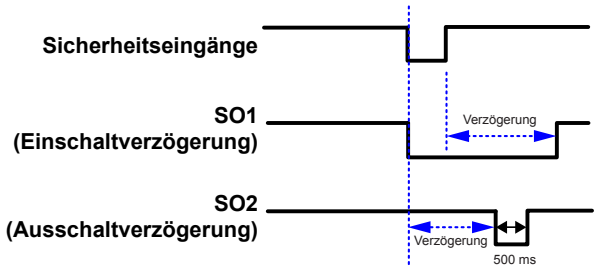
**Teilen (Sicherheitsausgänge): nur XS/SC26-2**

Diese Option ist nur für Sicherheits-Transistorausgänge verfügbar. Jeder redundante Sicherheits-Transistorausgang kann für den Einzel- oder Paarbetrieb (Standard) konfiguriert werden. Durch das Teilen eines Sicherheits- Transistorausgangs werden zwei unabhängige einkanalige Ausgänge erstellt (die Steuerung von SO1a ist unabhängig von der Steuerung von SO1b). Zum Vereinen eines geteilten Sicherheitsausgangs öffnen Sie das Fenster **Eigenschaften** für Mx:SOxA und klicken Sie auf **Vereinigen**.

### Einschalt- und Ausschaltverzögerungen

Jeder Sicherheitsausgang kann so konfiguriert werden, dass er entweder mit einer Einschaltverzögerung oder mit einer Ausschaltverzögerung funktioniert (siehe Abbildung 32 auf Seite 62), wobei der Ausgang erst nach Ablauf des Zeitlimits ein- bzw. ausschaltet. Ein Ausgang kann nicht gleichzeitig eine Ein- und eine Ausschaltverzögerung haben. Das Zeitlimit für die Ein- und Ausschaltverzögerung kann in Stufen à 1 Millisekunde von 100 Millisekunden bis 5 Minuten eingestellt werden.

*Abbildung 32. Zeitablauf-Diagramm: Ein- und Ausschaltverzögerung für Sicherheitsausgänge allgemein*



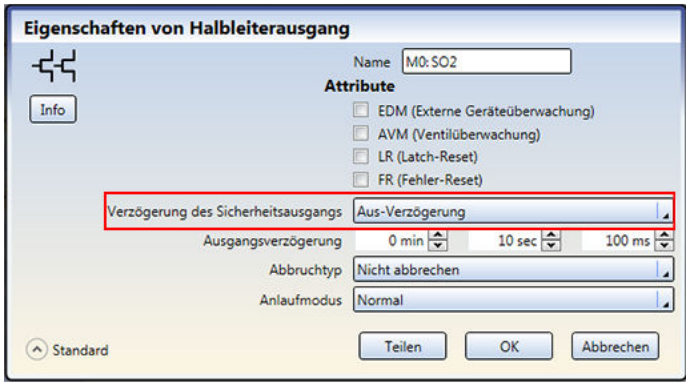

**WARNUNG:**

- **Bei einer Stromunterbrechung oder einem Stromausfall kann eine Ausschaltverzögerungszeit jedoch sofort enden.**
- Wenn diese Anweisungen nicht befolgt werden, können schwere oder tödliche Verletzungen die Folge sein.
- Die Ausschaltverzögerungszeit eines Sicherheitsausgangs wird auch dann eingehalten, wenn der Sicherheitseingang, der den Start des Zeitgebers für die Ausschaltverzögerung bewirkt hat, in den Ein-Zustand zurückschaltet, bevor die Verzögerungszeit abgelaufen ist. Wenn eine derartige sofortige Abschaltung einer Maschine eine mögliche Gefahr darstellen könnte, müssen zur Vermeidung von Verletzungen zusätzliche Schutzmaßnahmen getroffen werden.

Zwei Sicherheitsausgänge können miteinander verkettet werden, wenn einer der Sicherheitsausgänge für eine Ausschaltverzögerung konfiguriert ist und bei dem anderen Ausgang keine Verzögerung konfiguriert wurde. Nach der Verkettung schaltet sich der Ausgang ohne Verzögerung nicht sofort wieder ein, wenn der steuernde Eingang während einer Ausschaltverzögerung eingeschaltet wird, wie in Abbildung 35 auf Seite 63dargestellt. So verketten Sie zwei Sicherheitsausgänge:

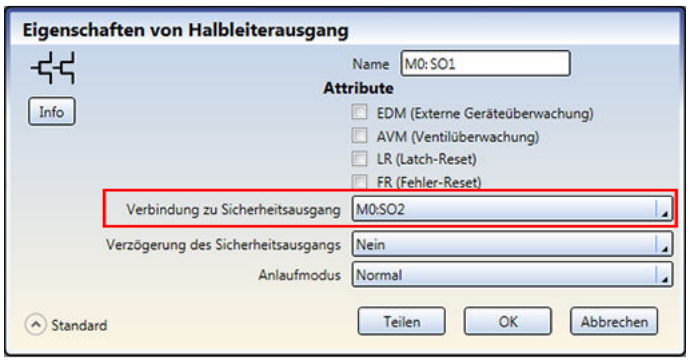
1. Öffnen Sie das Fenster **Eigenschaften** für den Sicherheitsausgang, der eine Ausschaltverzögerung benötigt.
2. Wählen Sie „Aus-Verzögerung“ aus der Dropdown-Liste *Verzögerung des Sicherheitsausgangs* aus.

*Abbildung 33. Auswahlbeispiel für Sicherheitsausgangsverzögerung: Ausschaltverzögerung*




3. Legen Sie die gewünschte Ausschaltverzögerungszeit fest.
4. Klicken Sie auf **OK**.
5. Öffnen Sie das Fenster **Eigenschaften** für den Sicherheitsausgang, der mit dem Sicherheitsausgang mit Ausschaltverzögerung verkettet werden soll.
6. Wählen Sie aus der Dropdown-Liste *Verbindung zu Sicherheitsausgang* den Sicherheitsausgang mit Ausschaltverzögerung aus, mit dem Sie diesen Sicherheitsausgang verketten möchten.

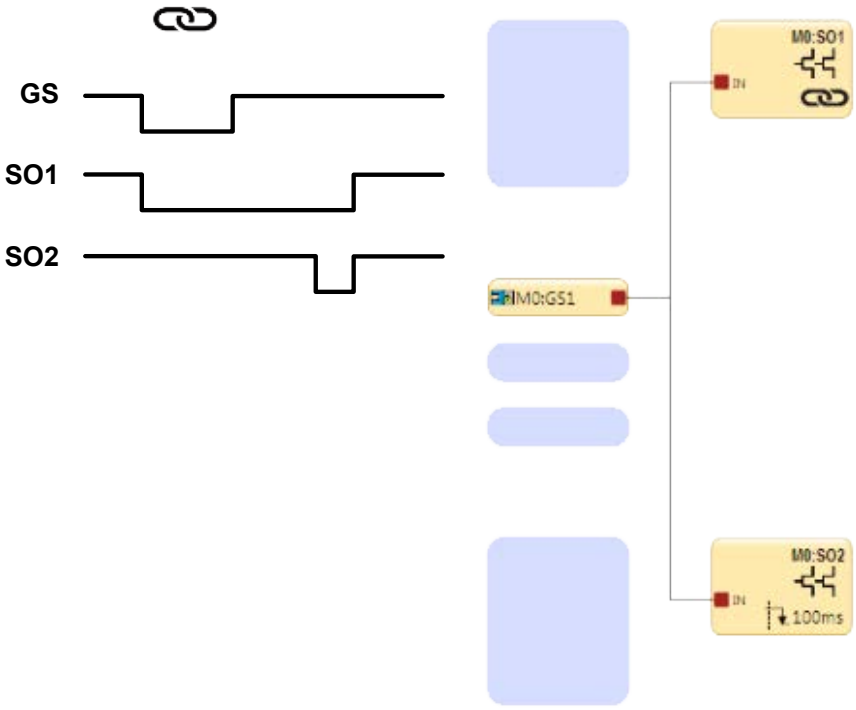
*Abbildung 34. Auswahlbeispiel für Verkettung mit Sicherheitsausgang*




**Anmerkung:** Die beiden Sicherheitsausgänge müssen mit demselben Eingang bzw. denselben Eingängen verbunden werden, damit sie als für die Verkettung verfügbar angezeigt werden.

7. Klicken Sie auf **OK**. Der verkettete Sicherheitsausgang ist mit einem Verkettungssymbol gekennzeichnet.

*Abbildung 35. Zeitablauf-Diagramm: Verkettete Sicherheitsausgänge*




## 7.8.1 XS/SC26-2 – Sicherheits-Transistorausgänge

Die Sicherheits-Transistorausgänge, z. B. SO1a und b sowie SO2a und b, werden aktiv überwacht, um Kurzschlüsse zur Spannungsversorgung, zueinander und zu anderen Spannungsquellen zu erfassen. Sie sind für Sicherheitsanwendungen entsprechend Kategorie 4 ausgelegt. Wenn eine Störung auf einem Kanal eines Sicherheitsausgangspaars erfasst wird, versuchen sich beide Ausgänge auszuschalten und wechseln in einen Sperrzustand. Der Ausgang, an dem kein Fehler vorliegt, kann die gefährliche Bewegung anhalten.

In ähnlicher Weise wird auch ein einzeln verwendeter (geteilter) Sicherheitsausgang aktiv überwacht, um Kurzschlüsse zu anderen Stromquellen zu erfassen. Dieser kann jedoch keine Aktionen ausführen. Beim Verbinden der Anschlüsse und beim Verlegen der Leitungen ist äußerste Vorsicht geboten. Die Möglichkeit von Kurzschlüssen zu anderen Spannungsquellen, einschließlich zu anderen Sicherheitsausgängen, ist zu vermeiden. Jeder geteilte Sicherheitsausgang ist aufgrund einer internen Reihenschaltung von zwei Schaltgeräten ausreichend für Anwendungen entsprechend Kategorie 3, aber ein externer Kurzschluss muss verhindert werden.

**Wichtig:** Wenn Sicherheits-Transistorausgangsmodule (XS2so oder XS4so) verwendet werden, muss die Stromversorgung für diese Module entweder vor dem Anlegen der Stromversorgung zum Basiskontroller angelegt werden oder innerhalb von 5 Sekunden danach, sofern separate Stromversorgungen verwendet werden.

**WARNUNG: Verwendung von einkanaligen (geteilten) Ausgängen in sicherheitskritischen Anwendungen**

Wenn ein einkanaliger Ausgang in einer sicherheitskritischen Anwendung verwendet wird, müssen Fehlerausschlussprinzipien integriert werden, um eine Sicherheitsstufe entsprechend Kategorie 3 zu gewährleisten. Ein Beispiel für eine geeignete Fehlerausschlussmethode ist die Verlegung und Handhabung der einkanaligen Ausgangsleitungen in einer Weise, durch die Kurzschlüsse zu anderen Ausgängen oder zu anderen Spannungsquellen nicht möglich sind. Wird bei Verwendung von einkanaligen Ausgängen in sicherheitskritischen Anwendungen auf die Einbeziehung geeigneter Fehlerausschlussmethoden verzichtet, kann es zum Verlust der Sicherheitssteuerung kommen und die Folge können schwere Verletzungen bis hin zum Tod sein.

Soweit möglich, wird die Einbeziehung einer externen Geräteüberwachung (EDM) und/oder einer einstellbaren Ventilüberwachung (AVM) dringend empfohlen, um die gesteuerten Geräte (FSDs und MPSEs) auf Störungen zu überwachen, die die Sicherheit gefährden. Unter Externe Geräteüberwachung (EDM) auf Seite 67 erhalten Sie weitere Informationen.

### Ausgangsanschlüsse

Die Sicherheitsausgänge müssen so an die Maschinensteuerung angeschlossen werden, dass das sicherheitsrelevante Steuerungssystem der Maschine den Stromkreis oder die Versorgung zu den primären Steuerelementen der Maschine (MPSEs) unterbricht und einen ungefährlichen Zustand herbeiführt.

Sofern sie verwendet werden, erfüllen Endschaltgeräte (FSDs) in der Regel diese Aufgabe, wenn die Sicherheitsausgänge in den Aus-Zustand wechseln. Siehe XS/SC26-2 – Spezifikationen auf Seite 20 , bevor Anschlüsse hergestellt werden und der Sicherheitskontroller an die Maschine angeschlossen wird.

Die Sicherheitsstufe muss durch die Risikobeurteilung ermittelt werden. Diese Stufe hängt von der Konfiguration, der sachgemäßen Installation der externen Schaltkreise und der Art und Installation der gesteuerten Geräte (FSDs und MPSEs) ab. Die Sicherheits-Relaisausgänge sind für Anwendungen entsprechend Kategorie 4 PL e/SIL 3 geeignet, wenn diese paarweise (nicht geteilt) gesteuert werden, sowie für Anwendungen entsprechend bis Kategorie 3 PL d/SIL 2, wenn diese unabhängig (geteilt) gesteuert werden und eine geeignete Fehlerausschlussmethode verwendet wurde. Unter Abbildung 36 auf Seite 65 finden Sie Anschlussbeispiele.

**WARNUNG:**

- **Widerstand der Sicherheitsausgangsleitungen**
- Ein Widerstand von mehr als 10 Ohm könnte einen Kurzschluss zwischen den zweikanaligen Sicherheitsausgängen verdecken. Dies könnte einen Gefahrenzustand erzeugen, der zu schweren oder tödlichen Verletzungen führen kann.
- Der Widerstand in den Leitern der Sicherheitsausgänge darf höchstens 10 Ohm betragen.

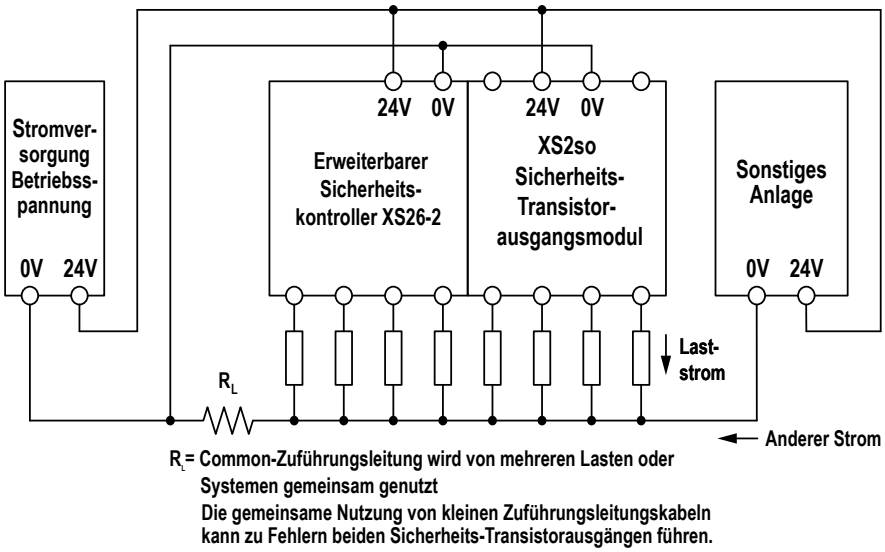
# Installation des Common-Leiters

*Abbildung 36. Installation des Common-Leiters*

Beachten Sie den Leiterwiderstand des 0 V-Common-Leiters und die Stromstärken in dem Leiter, um unnötige Sperrzustände zu vermeiden. Beachten Sie die Position des Widerstandssymbols in dem nachstehenden Schaltplan, das den Widerstand des 0 V-Common-Leiters (RL) darstellt.

Diese Situation kann mit folgenden Methoden verhindert werden:

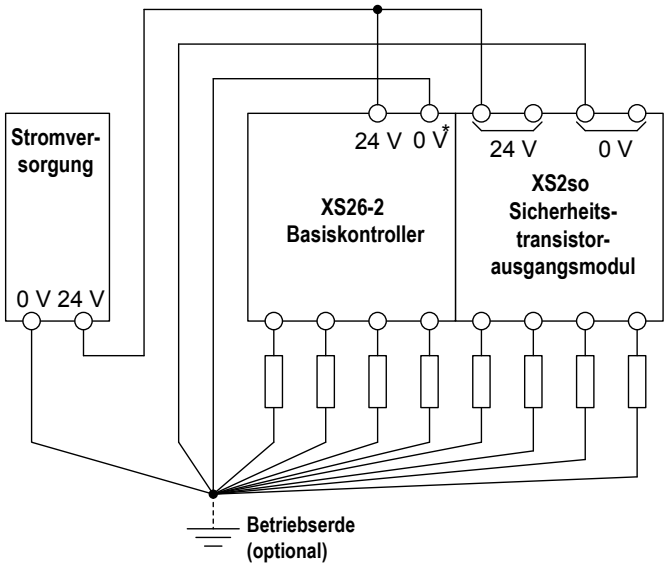
- Durch Verwendung dickerer oder kürzerer Leiter zur Verringerung des Widerstands ($R_L$) des 0 V-Common-Leiters
- Durch Trennung des 0 V-Common-Leiters von den an den Sicherheitskontroller angeschlossenen Lasten und des 0 V-Common-Leiters von anderen über die 24 V-Common-Stromversorgung versorgten Geräten




**Anmerkung:** Beim Ausschalten des Sicherheitsausgangs muss die Spannung am betreffenden Ausgangsanschluss unter 1,7 V in Bezug auf den 0-V-Anschluss am Modul sinken. Ist die Spannung höher als 1,7 V, geht der Kontroller davon aus, dass sich der Ausgang noch im Sperrzustand befindet. Ziehen Sie die Verwendung dünnerer oder kürzerer Kabel in Betracht, oder verwenden Sie einen Einzelpunkt-Erdungsplan, ähnlich wie in den folgenden Schaltplänen angezeigt.

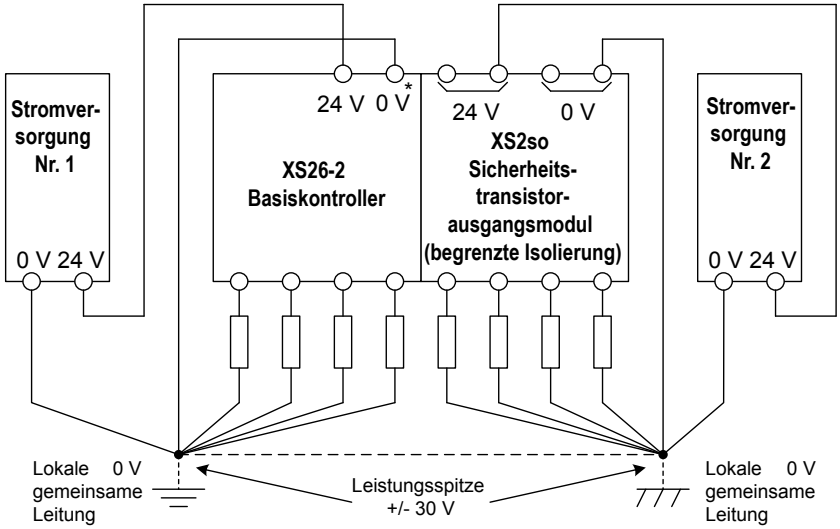
*Abbildung 37. Schaltplan – Empfohlene Erdung*

**Bevorzugter 0-V-Leitwegplan bei Verwendung einer einzelnen Stromversorgung**




*** Die Spannung für alle Sicherheitseingangsgeräte (einschließlich aller Eingangserweiterungsmodule) sollte in Bezug auf den 0-V-Anschluss des Basiskontrollers gemessen werden.**

**Bevorzugter 0-V-Leitwegplan bei Verwendung separater Stromversorgungen**




## 7.8.2 Sicherheits-Relaisausgänge

Sicherheitsrelais-Erweiterungsmodule für den XS/SC26-2 und der SC10-2 verfügen über isolierte redundante Relaisausgänge, mit denen ein breites Spektrum an elektrischen Geräten gesteuert/geschaltet werden kann (siehe XS/SC26-2 – Spezifikationen auf Seite 20 und Spezifikationen für den SC10-2 auf Seite 22). Im Gegensatz zu einem Sicherheits-Transistorausgang funktioniert ein einzelner Sicherheits-Relaisausgang (Mx:ROx) in einem Ausgangsmodul als Gruppe und kann nicht geteilt werden.

Die Sicherheits-Relaisausgänge werden vom Basiskontroller XS/SC26-2 oder dem SC10-2 gesteuert und überwacht. Hierzu sind keine zusätzlichen Leitungen erforderlich.

Für Schaltungen, die ein Höchstmaß an Sicherheit und Zuverlässigkeit erfordern, muss jeder Sicherheitsausgang bei paarweiser Verwendung (zwei Schließer) fähig sein, die Bewegung der durch einen Sicherheitsausgang geschützten Maschine im Notfall anzuhalten. Bei Einzelverwendung (ein einzelner Schließerausgang) muss mit dem Fehlerausschluss gewährleistet werden, dass keine Störungen auftreten können, die zu einem Verlust der Sicherheitsfunktion führen würden, beispielsweise ein Kurzschluss zu einem anderen Sicherheitsausgang oder eine sekundäre Strom- oder Spannungsquelle. Weitere Informationen erhalten Sie unter *Einkanalsteuerung* in Sicherheits-(Schutz-)Stoppschaltungen auf Seite 69 und Fehlerausschluss auf Seite 31.

Soweit möglich, wird die Einbeziehung einer externen Geräteüberwachung (EDM) und/oder einer einstellbaren Ventilüberwachung (AVM) dringend empfohlen, um die gesteuerten Geräte (FSDs und MPSEs) auf Störungen zu überwachen, die die Sicherheit gefährden. Unter Externe Geräteüberwachung (EDM) auf Seite 67 erhalten Sie weitere Informationen.

**Ausgangsanschlüsse**: Die Sicherheits-Relaisausgänge müssen so an die Maschinensteuerung angeschlossen werden, dass das sicherheitsrelevante Steuerungssystem der Maschine den Stromkreis oder die Versorgung zu den primären Steuerelementen der Maschine (MPSEs) unterbricht und einen ungefährlichen Zustand herbeiführt. Sofern sie verwendet werden, erfüllen Endschaltgeräte (FSDs) in der Regel diese Aufgabe, wenn die Sicherheitsausgänge in den Aus-Zustand wechseln.

Die Sicherheits-Relaisausgänge können als Endschaltgeräte (FSDs) verwendet werden, und sie können in einem zweikanaligen oder einkanaligen Schutzhalt-Schaltkreis angeschlossen werden (siehe FSD-Anschlüsse auf Seite 69). Beachten Sie XS/SC26-2 – Spezifikationen auf Seite 20 und Spezifikationen für den SC10-2 auf Seite 22, bevor Anschlüsse hergestellt werden und der Sicherheitskontroller an die Maschine angeschlossen wird.

Die Sicherheitsstufe muss durch die Risikobeurteilung ermittelt werden. Diese Stufe hängt von der Konfiguration, der sachgemäßen Installation der externen Schaltkreise und der Art und Installation der gesteuerten Geräte (FSDs und MPSEs) ab. Die Sicherheits-Relaisausgänge sind für Kategorie 4 PL e/SIL 3 geeignet. Unter Abbildung 36 auf Seite 65 finden Sie Anschlussbeispiele.

**Wichtig:** Es liegt in der Verantwortung des Benutzers, für alle Relaisausgänge einen Überstromschutz bereitzustellen.

## Installationen der Überspannungskategorien II und III (EN 50178 und IEC 60664-1)

Der XS/SC26-2 und der SC10-2 sind für die Überspannungskategorie III zugelassen, wenn Spannungen von 1 V bis 150 V AC/DC an den Ausgangsrelaiskontakten anliegen. Sie sind für die Überspannungskategorie II zugelassen, wenn Spannungen von 151 V bis 250 V AC/DC an den Ausgangsrelaiskontakten anliegen und keine weiteren Schutzmaßnahmen zur Begrenzung potenzieller Überspannungen in der Betriebsspannung vorhanden sind. Der XS/SC26-2 oder der SC10-2 kann in Umgebungen der Überspannungskategorie III (bei einer Spannung von 151 V bis 250 V AC/DC) eingesetzt werden, wenn durch Installation von Überspannungsschutzvorrichtungen (z. B. Lichtbogen-Entstörgliedern) dafür gesorgt ist, dass entweder die vom XS/SC26-2 bzw. dem SC10-2 zu schützenden elektrischen Störungen auf das Niveau der Überspannungskategorie II reduziert werden, oder wenn eine zusätzliche externe Isolierung installiert wurde, um sowohl den XS/SC26-2 bzw. den SC10-2 als auch die Bedienperson vor den höheren Spannungen einer Umgebung der Kategorie III zu schützen.

**Bei Installationen der Überspannungskategorie III mit an den Ausgangskontakten anliegenden Spannungen von 151 V bis 250 V AC/DC** darf der XS/SC26-2 oder der SC10-2 unter den Bedingungen einer höheren Überspannungskategorie eingesetzt werden, wenn ein ausreichender Überspannungsschutz vorhanden ist. Geeignete Methoden:

- eine Überspannungsschutzvorrichtung,
- ein Transformator mit isolierten Wicklungen,
- ein Verteilungssystem mit mehreren Abzweigleitungen (die die Energie von Spannungsspitzen ableiten können),
- eine ausreichende Kapazität, um die Energie von Spannungsspitzen aufzunehmen,
- ein Widerstand oder eine vergleichbare Dämpfungsvorrichtung zur Ableitung der Energie von Spannungsspitzen,

Beim Schalten von induktiven Wechselstromlasten sollten die Ausgänge des XS/SC26-2 bzw. des SC10-2 durch Installation entsprechender Lichtbogen-Entstörglieder geschützt werden. Werden Lichtbogen-Entstörglieder verwendet, müssen diese jedoch zwischen der zu schaltenden Last (z. B. zwischen den Spulen externer Sicherheitsrelais) und niemals zwischen den Ausgangskontakten des XS/SC26-2 bzw. des SC10-2 installiert werden (siehe WARNUNG, Lichtbogen-Entstörglieder).

# 7.8.3 EDM- und Endschaltgeräteanschluss

## Externe Geräteüberwachung (EDM)

Die Sicherheitsausgänge des Sicherheitskontrollers können externe Relais, Kontaktgeber oder andere Komponenten steuern, die einen Satz zwangsgeführter (mechanisch verbundener) Kontakte mit einem Öffnerkontakt haben, der zur Statusüberwachung der Stromkontakte der Maschine verwendet werden kann. Der Monitorkontakt ist im geschlossenen Zustand, wenn die Komponente ausgeschaltet wird. Dadurch kann der Sicherheitskontroller erfassen, ob die angeschlossenen Komponenten auf den Sicherheitsausgang ansprechen oder ob die Schließerkontakte möglicherweise im geschlossenen Zustand verschweißt oder im Ein-Zustand blockiert sind.

**Anmerkung:** Die internen Relais des XS1ro, XS2ro und SC10-2 werden immer von den Modulen überwacht. EDM ist nur für Geräte erforderlich, die sich außerhalb der Kontroller befinden.

Die EDM-Funktion bietet eine Methode zur Überwachung dieser Fehlerarten und zur Sicherstellung der Funktionsfähigkeit eines zweikanaligen Systems einschließlich der MPSEs und der FSDs.

Ein einzelner EDM-Eingang kann einem oder mehreren Sicherheitsausgängen zugeordnet werden. Öffnen Sie hierzu das Fenster **Properties (Eigenschaften)** für den Sicherheitsausgang und aktivieren Sie **EDM**. Fügen Sie dann **External Device Monitoring (Externe Geräteüberwachung)** von der Registerkarte **Safety Input (Sicherheitseingang)** im Fenster **Add Equipment (Geräte hinzufügen)** hinzu (dieses wird über die Ansicht **Equipment (Geräte)** oder über die Registerkarte **Functional View (Funktionsansicht)** aufgerufen), und verbinden Sie den Eingang für die **External Device Monitoring (Externe Geräteüberwachung)** mit dem **EDM**-Knoten des Sicherheitsausgangs.

Die EDM-Eingänge können für Einkanal- oder Zweikanalüberwachung konfiguriert werden. Einkanal-EDM-Eingänge werden verwendet, wenn die OSSD-Ausgänge die Deaktivierung der MPSEs oder der externen Vorrichtungen direkt steuern.

- **Einkanal-Überwachung**: Eine Reihenschaltung geschlossener zwangsgeführter Monitorkontakten, einer von jeweils einem der von den Sicherheitsausgängen des Kontrollers angesteuerten Geräten. Die Monitorkontakte müssen geschlossen sein, bevor an den Ausgängen des Sicherheitskontrollers ein System-Reset ausgeführt werden kann (entweder manuell oder automatisch). Nachdem ein Reset ausgeführt wurde und die Sicherheitsausgänge einschalten, wird der Status der Monitorkontakte nicht mehr überwacht und kann sich ändern. Die Monitorkontakte müssen jedoch innerhalb von 250 Millisekunden geschlossen werden, nachdem die Sicherheitsausgänge von Ein zu Aus wechseln. Siehe Abbildung 40 auf Seite 69.
- **Zweikanal-Überwachung**: Anschluss voneinander unabhängiger geschlossener Überwachungskontakte, die jeweils mit einem durch den Sicherheitskontroller gesteuerten Gerät mechanisch verbunden sind. Beide EDM-Eingänge müssen geschlossen werden, bevor am Sicherheitskontroller ein Reset durchgeführt und die OSSDs eingeschaltet werden können. Während die OSSDs eingeschaltet sind, können die Eingänge ihren Zustand ändern (entweder beide offen oder beide geschlossen). Wenn die Eingänge länger als 250 Millisekunden im entgegengesetzten Zustand bleiben, tritt ein Sperrzustand ein. Siehe Abbildung 42 auf Seite 69.
- **Keine Überwachung (Standard)**: Wenn keine Überwachung gewünscht wird, dürfen Sie den EDM-Knoten des Sicherheitsausgangs nicht aktivieren. Wenn der Sicherheitskontroller keinen Rückführkreis bei Anwendungen der Kategorie 3 oder 4 verwendet, muss der Anwender dafür sorgen, dass ein einzelner Ausfall oder eine Anhäufung von Ausfällen der externen Geräte nicht zu einem gefährlichen Zustand führt, und dass ein darauffolgender Maschinenzyklus verhindert wird.

**VORSICHT: EDM-Konfiguration**

Wenn die EDM-Funktion bei der Anwendung nicht benötigt wird, trägt der Anwender die Verantwortung dafür, dass dadurch keine gefährliche Situation entsteht.

**VORSICHT: Anschluss der externen Geräteüberwachung (EDM)**

Es wird empfohlen, mindestens einen zwangsgeführten Öffner-Überwachungskontakt von jedem primären Steuerelement der Maschine (MPSE) bzw. jeder externen Vorrichtung zu verdrahten, um den Zustand der MPSEs zu überwachen (siehe Abbildung). Danach werden die MPSEs auf den ordnungsgemäßen Betrieb überprüft. **Die Kontakte für die MPSE-Überwachung dienen dazu, die Steuerungszuverlässigkeit zu erhalten.**

*Abbildung 38. Anschluss der externen Einkanal-Geräteüberwachung (Einkanal-EDM)*

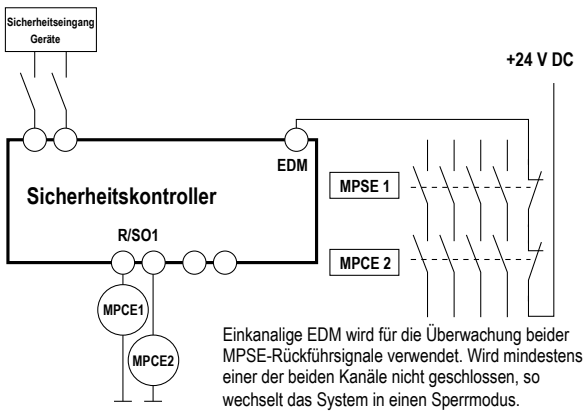



*Abbildung 39. Anschluss der externen Zweikanal-Geräteüberwachung (Zweikanal-EDM)*

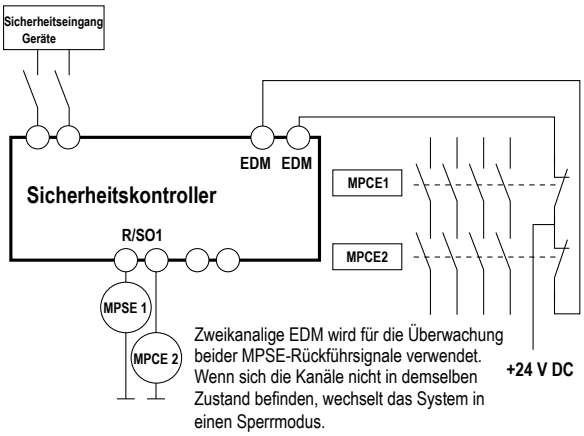
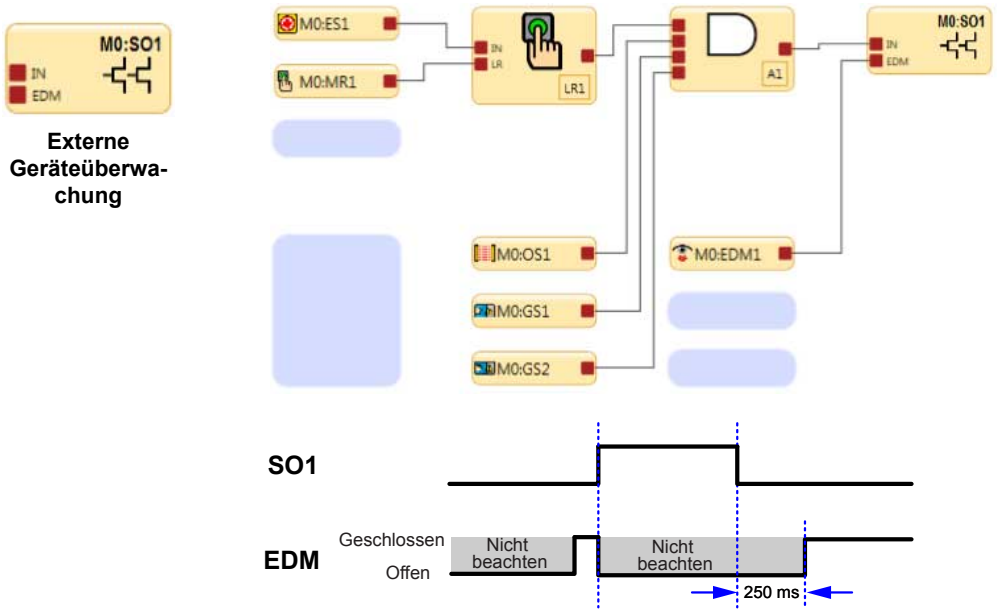


*Abbildung 40. Zeitgebungslogik: Status der einkanaligen externen Geräteüberwachung in Bezug auf den Sicherheitsausgang*




Die externe Geräteüberwachung (EDM) ist eine Methode zur Überprüfung des Betriebs von zweikanaligen Endschaltgeräten (FSDs) oder primären Steuerelementen der Maschine (MSPEs). Die zwangsgeführten Öffner-Überwachungskontakte der FSDs oder MSPEs dienen als Eingänge für die Erkennung eines verschweißten Ein-Zustands als Fehlerzustand und verhindern ein Einschalten der Ausgänge des Sicherheitskontrollers.

Bei der zweikanaligen externen Geräteüberwachung müssen, wie unten abgebildet, beide Kanäle geschlossen sein, bevor sich die entsprechenden Sicherheitsausgänge einschalten.

*Abbildung 41. Zeitgebungslogik: Zweikanalige EDM, zeitliche Abstimmung zwischen Kanälen*

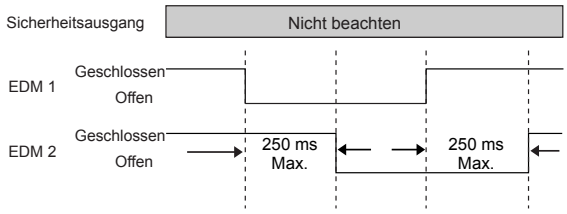
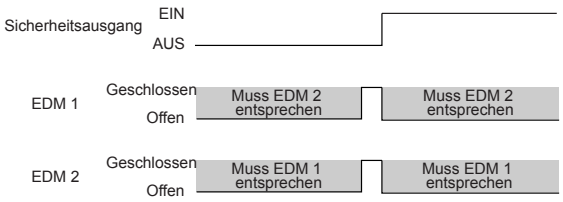



*Abbildung 42. Zeitgebungslogik: Status der zweikanaligen externen Geräteüberwachung in Bezug auf den Sicherheitsausgang*




# FSD-Anschlüsse

Endschaltgeräte (FSDs) unterbrechen die Stromversorgung im Schaltkreis zum primären Steuerelement der Maschine (MPSE), wenn die Sicherheitsausgänge in den Aus-Zustand schalten. FSDs können in vielen Formen auftreten. Die häufigsten sind zwangsgeführte, mechanisch verbundene Relais oder Interface-Module. Die mechanische Verbindung zwischen den Kontakten ermöglicht es, dass das Gerät von der externen Geräteüberwachung auf bestimmte Ausfälle hin überwacht wird.

Je nach Anwendung kann der Einsatz von FSDs die Regelung von Spannungs- und Stromwerten vereinfachen, die von den Sicherheitsausgängen des Sicherheitskontrollers abweichen. FSDs können auch zur Kontrolle zusätzlicher Gefahren benutzt werden, indem sie zur Bildung von mehrfachen Sicherheitsstoppschaltungen verwendet werden.

## Sicherheits-(Schutz-)Stoppschaltungen

Eine Sicherheitsabschaltung bewirkt einen definierten Bewegungsstopp und eine Unterbrechung der Versorgungsspannung von den s für Schutzzwecke (vorausgesetzt, es werden hierdurch keine zusätzlichen Gefahren erzeugt). Eine Sicherheitsstoppschaltung umfasst gewöhnlich mindestens zwei Schließerkontakte von zwangsgeführten (mechanisch verbundenen) Relais, die zur Erkennung bestimmter Störungen (über einen mechanisch verbundenen Öffnerkontakt) überwacht werden, damit der Verlust der Schutzfunktion verhindert wird. Eine solche Schaltung kann als „sicherer Schaltpunkt“ beschrieben werden.

Gewöhnlich sind Sicherheitsstoppschaltungen Reihenschaltungen von mindestens zwei Schließerkontakten, die von zwei separaten zwangsgeführten Relais kommen, die jeweils von einem separaten Sicherheitsausgang des Sicherheitskontrollers gesteuert werden. Die Sicherheitsfunktion beruht auf der Verwendung redundanter Kontakte zur Überwa-

chung einer einzelnen Gefahrenstelle, so dass bei Ausfall eines Kontakts im Ein-Zustand der zweite Kontakt die gefährliche Maschinenbewegung anhält und den Eintritt des nächsten Zyklus verhindert.

Der Anschluss der Sicherheitsstoppschaltungen muss so erfolgen, dass die Schutzfunktion weder aufgehoben, deaktiviert oder umgangen werden kann, es sei denn, dass der gleiche oder ein höherer Grad an Sicherheit erreicht wird wie der des Maschinen-Sicherheitssteuerungssystem, welches den Sicherheitskontroller mit einschließt.

Die Schließerausgänge eines Anschlussmoduls sind eine Reihenschaltung redundanter Kontakte, die Sicherheitsstoppschaltungen bilden und in Einkanal- oder Zweikanalsteuerungen eingesetzt werden können.

**Zweikanalsteuerung**: Bei Zweikanalsteuerung kann der sichere Schaltpunkt elektrisch über die FSD-Kontakte hinaus erweitert werden. Bei ordnungsgemäßer Überwachung (z. B. EDM) können mit dieser Anschlussmethode bestimmte Störungen in der Verdrahtung zwischen der Sicherheitsstoppschaltung und den MPSEs entdeckt werden. Zu diesen Störungen gehören Kurzschlüsse im Anschluss eines Kanals an eine sekundäre Energie- oder Spannungsquelle oder der Verlust der Schaltfähigkeit eines der FSD-Ausgänge. Solche Störungen könnten zum Verlust der Redundanz oder zum vollständigen Verlust der Schutzfunktion führen, wenn sie nicht erkannt und behoben werden.

Die Wahrscheinlichkeit einer Störung in der Verdrahtung erhöht sich mit zunehmendem Abstand zwischen den FSD-Sicherheitsstoppschaltungen und den MPSEs, mit zunehmender Länge der Anschlussleitungen oder bei Unterbringung der FSD-Sicherheitsstoppschaltungen und der MPSEs in unterschiedlichen Gehäusen. Aus diesem Grund sollte bei Installationen, bei denen die FSDs von den MPSEs weit entfernt sind, eine Zweikanalsteuerung mit EDM-Überwachung verwendet werden.

**Einkanalsteuerung**: Bei der Einkanalsteuerung wird eine Reihenschaltung von FSD -Kontakten zur Bildung eines sicheren Schaltpunkts verwendet. Hinter diesem Punkt im Sicherheitssteuerungssystem der Maschine können Störungen auftreten, die zu einem Verlust der Schutzfunktion führen, z. B. ein Kurzschluss im Anschluss an eine sekundäre Energie- oder Spannungsquelle.

Aus diesem Grund sollte diese Anschlussmethode nur bei Installationen verwendet werden, bei denen die FSD -Sicherheitsstoppschaltungen und die MPSEs nebeneinander in derselben Steuertafel montiert und direkt miteinander verbunden werden, oder bei denen die Möglichkeit einer derartigen Störung ausgeschlossen werden kann. Wenn sich das nicht erreichen lässt, muss eine Zweikanalsteuerung verwendet werden.

Folgende Methoden können unter anderem verwendet werden, um die Wahrscheinlichkeit derartiger Störungen auszuschließen:

- Trennung der Anschlussleitungen voneinander und von sekundären Energiequellen
- Verlegung der Anschlussleitungen in separaten Kabelwegen, -schutzrohren oder -kanälen
- Anschluss von Steuerleitungen mit niedriger Spannung oder neutral, so dass keine Gefahr erzeugt wird
- Unterbringung aller Elemente (Module, Schalter, gesteuerte Geräte usw.) nebeneinander im selben Schaltschrank und direkte Verbindung der Elemente untereinander mit kurzen Leitungen
- Ordnungsgemäße Installation von mehradrigen Kabeln und mehreren Leitern, die durch Zugentlastungsklemmen geführt werden. Zu starkes Anziehen einer Entlastungsklemme kann Kurzschluss an diesem Punkt verursachen.
- Verwendung von Komponenten mit Zwangsöffnung oder Direktantrieb, die im Zwangsführungsmodus installiert werden

**WARNUNG:**

- **Überspannungsbegrenzer oder Lichtbogen-Entstörglieder ordnungsgemäß installieren**
- Wenn diese Anweisungen nicht befolgt werden, können schwere oder tödliche Verletzungen die Folge sein.
- Installieren Sie Lichtbogen-Entstörglieder bzw. Überspannungsbegrenzer wie abgebildet über den Spulen der FSDs oder MPSEs. Installieren Sie diese nicht direkt auf den Kontakten der FSDs bzw. MSPEs. In einer solchen Konfiguration ist ein Ausfall der Lichtbogen-Entstörglieder bzw. Überspannungsbegrenzer in Form eines Kurzschlusses möglich.

**WARNUNG: Anschluss der Sicherheitsausgänge**

Zur Sicherstellung des ordnungsgemäßen Betriebs müssen die Ausgangsparameter des Banner-Produkts und die Eingangsparameter der Maschine beim Anschließen der Sicherheits-Transistorausgänge an die Maschineneingänge berücksichtigt werden. Die Steuerschaltung der Maschine muss so ausgelegt sein, dass folgende Anforderungen erfüllt sind:

- Der maximale Kabelwiderstandswert zwischen den Sicherheits-Transistorausgängen des Sicherheitscontrollers und den Maschineneingängen darf nicht überschritten werden.
- Die maximale Sperrspannung des Sicherheits-Transistorausgangs des Sicherheitscontrollers darf nicht zu einem eingeschalteten Zustand führen.
- Der maximale Leckstrom des Sicherheits-Transistorausgangs des Sicherheitscontrollers aufgrund des Verlusts der 0-V-Leitung darf nicht zu einem eingeschalteten Zustand führen.

**Wenn die Sicherheitsausgänge nicht richtig an die überwachte Maschine angeschlossen werden, kann es zu schweren oder tödlichen Verletzungen kommen.**

**WARNUNG: Gefahr eines elektrischen Schlages und gefährliche Energie**

**Trennen Sie immer die Stromversorgung vom Sicherheitssystem (z. B. Gerät, Modul, Anschlüssen usw.) und der überwachten Maschine, bevor Anschlüsse verbunden oder Komponenten ausgetauscht werden.**

Die elektrische Installation und Verdrahtung muss von qualifizierten Personen durchgeführt werden [10] Dabei sind die geltenden elektrischen Standards und Verdrahtungsvorschriften einzuhalten, wie zum Beispiel der NEC (National Electric Code), ANSI NFPA79 oder IEC/EN 60204-1, sowie sämtliche geltenden örtlichen Normen und Vorschriften.

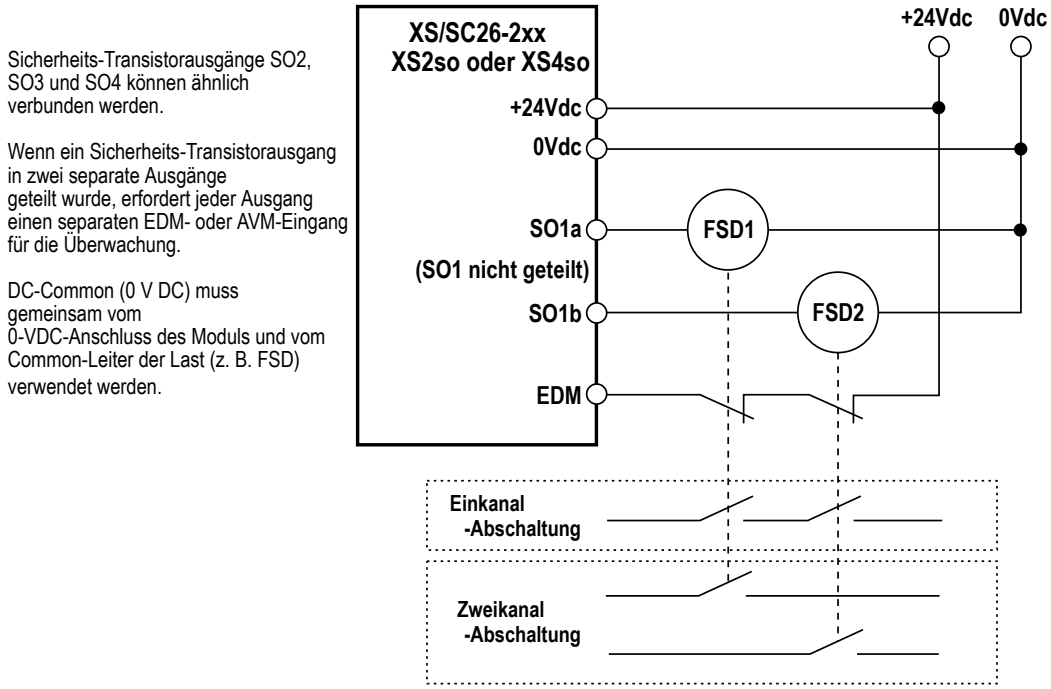
**Hierfür sind möglicherweise Lockout/Tagout-Verfahren (Verriegelung/Kennzeichnung) erforderlich.** Siehe OSHA 29CFR1910.147, ANSI Z244-1, ISO 14118 oder die entsprechende Norm zur Steuerung gefährlicher Energie.

**WARNUNG:**

- **Das Gerät korrekt verdrahten**
- Wird der Sicherheitskontroller mit der jeweiligen Maschine falsch verdrahtet, so könnte sich ein Gefahrenzustand ergeben, der schwere Verletzungen oder Tod zur Folge haben könnte.
- Eine ordnungsgemäße Verdrahtung des Sicherheitskontrollers liegt in der Verantwortung des Anwenders. Die Verdrahtungskonfigurationen gelten ganz allgemein und sollen lediglich veranschaulichen, wie wichtig eine sachgemäße Installation ist.

## Typischer Anschluss des XS/SC26-2: Sicherheitsausgang mit EDM

*Abbildung 43. Typischer Anschluss des XS/SC26-2: Sicherheits-Transistorausgang mit EDM*




[10] Eine Person, die durch ein anerkanntes Ausbildungs- oder Berufsabschlusszertifikat bzw. durch umfangreiche Kenntnisse und die entsprechende Ausbildung oder Erfahrung mit Erfolg nachweisen kann, dass sie in der Lage ist, Probleme bezüglich des in Frage stehenden Gegenstands und bei der Arbeit mit diesem zu lösen.

*Abbildung 44. Typischer Anschluss des XS/SC26-2: Sicherheits-Relaisausgang (zweikanalig) mit EDM*

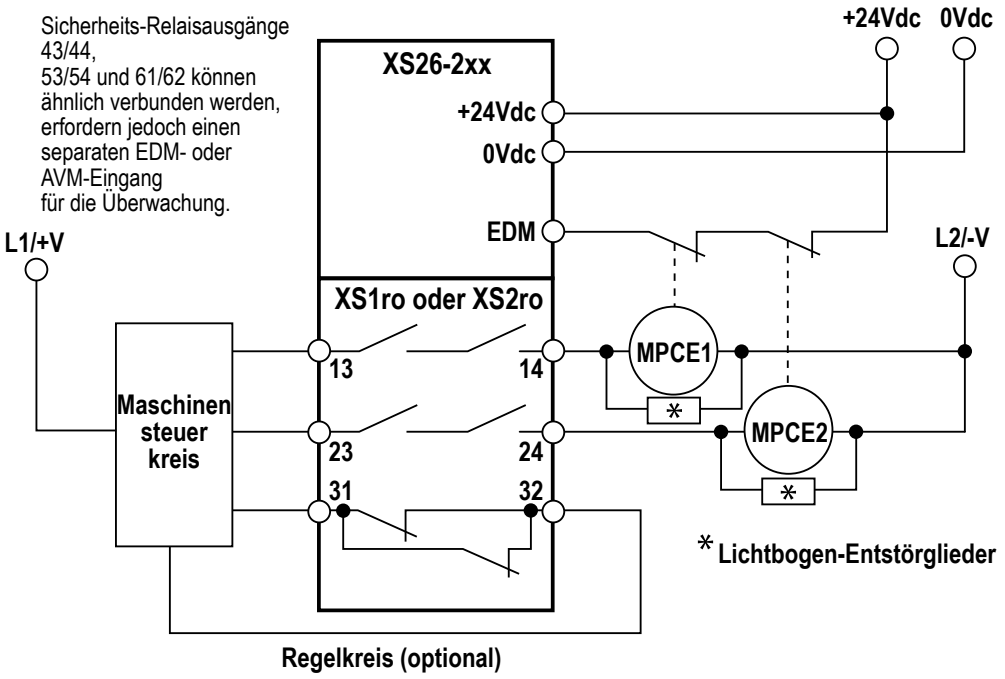
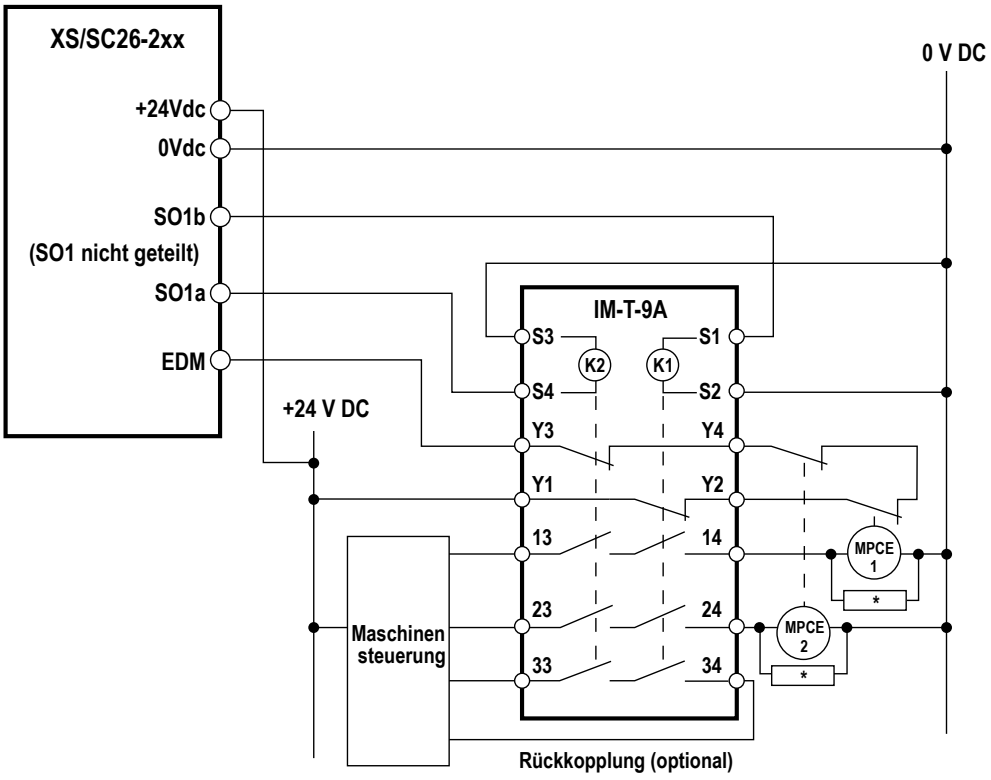


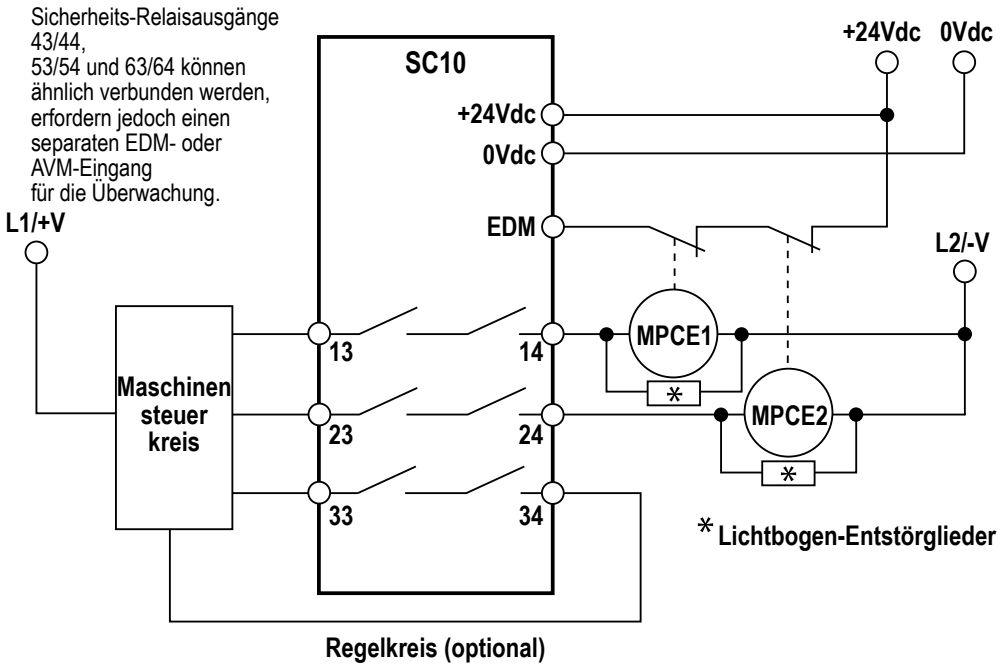

*Abbildung 45. Typischer Anschluss des XS/SC26-2: Sicherheits-Transistorausgang an IM-T-9A*




*** Es wird empfohlen, über den Spulen von MPSE1 und MPSE2 Überspannungsbegrenzer (Lichtbogen-Entstörglieder) zu installieren (siehe WARNUNG).**

### Typischer Anschluss des SC10-2: Sicherheitsausgang mit EDM

*Abbildung 46. Typischer Anschluss des SC10-2: Sicherheits-Relaisausgang (zweikanalig) mit EDM*




# 7.9 Statusausgänge

Anweisungen zum Hinzufügen eines Statusausgangs finden Sie unter Hinzufügen von Statusausgängen auf Seite 81.

## 7.9.1 Signallogik für Statusausgänge

**Anmerkung:** Sie dürfen die Sicherheitsausgänge am SC10-2 nicht als Statusausgänge verwenden.

Für jeden Statusausgang stehen zwei Signallogiken zur Auswahl: „PNP ein“ (liefert 24 V DC) oder „PNP aus“ (nicht leitend). Die Standardlogik ist „Aktiv = PNP ein“.

Für einen Statusausgang im Ein-Zustand kann auch eine Blinkrate konfiguriert werden. Die drei Optionen sind:

- Kein Blinken (für konstant leuchtend)
- Normal (abwechselnd 500 ms an und 500 ms aus)
- Schnell (abwechselnd 150 ms an und 150 ms aus)

Die Standard-Blinkrate ist „Kein Blinken“. Für einen Muting-Statusausgang kann keine Blinkrate konfiguriert werden (siehe Muting in Statusausgangsfunktion auf Seite 74).

*Tabelle 6. Signallogik für Statusausgänge*

| Funktion | Signallogik | | | |
|---|---|---|---|---|
| | Aktiv = PNP ein | | Aktiv = PNP aus | |
| | Statusausgangs-Status | | Statusausgangs-Status | |
| | +24 V DC | Aus | Aus | 24 V DC |
| **Überbrückung** | Überbrückt | Nicht überbrückt | Überbrückt | Nicht überbrückt |
| **Muting** | Gemutet | Nicht gemutet | Gemutet | Nicht gemutet |
| **Ausgangsverzögerung läuft** | Verzögerung | Keine Verzögerung | Verzögerung | Keine Verzögerung |
| **Eingangsstatus anzeigen** | Ein | Stopp | Ein | Stopp |
| **Eingangsfehler anzeigen** | Fehler | OK | Fehler | OK |
| **Beliebigen Eingangsfehler anzeigen** | Fehler | OK | Fehler | OK |
| **Eingangsanzeigegruppe** | Stopp initiiert | Anderer Eingang verursachte Stopp | Stopp initiiert | Anderer Eingang verursachte Stopp |

| Funktion | Signallogik | | | |
|---|---|---|---|---|
| | Aktiv = PNP ein | | Aktiv = PNP aus | |
| | Statusausgangs-Status | | Statusausgangs-Status | |
| | +24 V DC | Aus | Aus | 24 V DC |
| Ausgangsstatus anzeigen | SO ein | SO aus | SO ein | SO aus |
| Ausgangsfehler anzeigen | Fehler | OK | Fehler | OK |
| Ausgangsfehler anzeigen, alle | Fehler | OK | Fehler | OK |
| Logischen Ausgangsstatus anzeigen | Logisch ein | Logisch aus | Logisch ein | Logisch aus |
| Status des Funktionsblocks verfolgen (XS/SC26-2 ab FID 2 und SC10-2) | Ein | Stopp | Ein | Stopp |
| Pressen-Funktionsblock verfolgen (XS/SC26-2 ab FID 4) | Nähere Informationen finden Sie unter XS/SC26-2: Statusausgangsfunktion der Pressensteuerung auf Seite 75. | | | |
| Warten auf manuellen Reset | Reset erforderlich | Nicht erfüllt | Reset erforderlich | Nicht erfüllt |
| Systemsperre | Sperr- | RUN-Modus | Sperr- | RUN-Modus |

## 7.9.2 Statusausgangsfunktion

**SC10-2:** Bis zu 4 umrüstbare Eingänge können als Statusausgang verwendet werden.

**XS/SC26-2:** Bis zu 32 umrüstbare Eingänge oder Sicherheitsausgänge können als Statusausgang verwendet werden. Sicherheits-Transistorausgänge können geteilt und als Statusausgänge verwendet werden. Sicherheits-Relaisausgänge können nicht als Statusausgänge verwendet und nicht geteilt werden.

Statusausgänge können für die Ausführung der folgenden Funktionen konfiguriert werden:

**Überbrückung**
Zeigt an, wenn der Eingang zum Überbrückungs-Funktionsblock umgangen wird.

**Muting**
Zeigt einen Muting-Aktiv-Status für den Eingang des jeweiligen Muting-Funktionsblocks an:
- EIN, wenn ein mutingfähiger Eingang gemutet ist
- AUS, wenn ein mutingfähiger Eingang nicht gemutet ist
- Die Anzeige blinkt, wenn die Bedingungen zum Starten eines Muting-abhängigen Override gegeben sind (ein inaktiver Muting-Zyklus, der mutingfähige Sicherheitseingang befindet sich im Aus-Zustand und mindestens ein Muting-Sensor befindet sich im Aus-Zustand (Sperrzustand)). Nicht für virtuellen Statusausgang verfügbar.
- EIN während einer aktiven Muting-abhängigen Override-Funktion (keine Umgehungsfunktion) eines mutingfähigen Sicherheitseingangs

**Ausgangsverzögerung läuft**
Gibt an, wenn die Ein- oder Ausschaltverzögerung aktiv ist.

**Eingangsstatus anzeigen**
Gibt den Status eines bestimmten Sicherheitseingangs an.

**Eingangsfehler anzeigen**
Gibt an, wenn ein bestimmter Sicherheitseingang einen Fehler aufweist.

**Beliebigen Eingangsfehler anzeigen**
Gibt an, wenn irgendein Sicherheitseingang einen Fehler aufweist.

**Eingangsanzeigebaugruppe**
Gibt den Status einer Sicherheitseingangsbaugruppe an, zum Beispiel, welcher Sicherheitseingang zuerst ausgeschaltet wurde. Nachdem diese Funktion angezeigt wurde, kann sie durch einen konfigurierten Reset-Eingang erneut aktiviert werden. Bis zu drei Eingangsbaugruppen können angezeigt werden.

**Ausgangsstatus anzeigen**
Gibt den physikalischen Zustand (Ein oder Aus) eines bestimmten Sicherheitsausgangs an.

**Ausgangsfehler anzeigen**
Gibt an, wenn ein bestimmter Sicherheitsausgang einen Fehler aufweist.

**Ausgangsfehler anzeigen, alle**
Gibt an, wenn irgendein Sicherheitsausgang einen Fehler aufweist.

**Logischen Status des Ausgangs verfolgen**

Gibt den logischen Status eines bestimmten Sicherheitsausgangs an. Beispiel: Der logische Status ist Aus, aber der Sicherheitsausgang befindet sich in der Ausschaltverzögerung und ist physikalisch noch nicht ausgeschaltet.

**Status des Verzögerungsblocks verfolgen (XS/SC26-2 ab FID 2 und SC10-2)**

Gibt den Status eines bestimmten Funktionsblocks an.

**Pressen-Funktionsblock verfolgen (XS/SC26-2 ab FID 4)**

Zeigt den Status einer Reihe von Pressenfunktionsereignissen an; siehe XS/SC26-2: Statusausgangsfunktion der Pressensteuerung auf Seite 75 für Details.

**Warten auf manuellen Reset**

Gibt an, dass ein bestimmter konfigurierter Reset erforderlich ist.

**Anmerkung:** Wenn der manuelle Reset-Eingang mit einem Reset-ODER-Block verbunden ist, kann dieser Statusausgang nicht verwendet werden.

**Systemsperre**

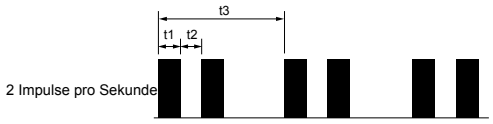
Gibt einen nicht funktionsfähigen Sperrzustand an, zum Beispiel einen nicht zugeordneten Eingang, der an die 24-V-Versorgung angeschlossen ist.

## 7.9.3 XS/SC26-2: Statusausgangsfunktion der Pressensteuerung

Der Pressensteuerungs-Funktionsblock hat mehrere Ein- und Ausgänge. Dies führt zu einer Statusausgangsfunktion, die kein einfaches Ein-/Ausschalten für eine einzelne Komponente ist. Der Statusausgang des Pressensteuerungsblocks verfügt über sieben verschiedene Ereignisse, die über den Statusausgang signalisiert werden können. Der Statusausgang des Pressensteuerungsblocks kann so konfiguriert werden, dass er ein, zwei oder drei Signale sendet. Jedes Signal vom Statusausgang des Pressensteuerungsblocks kann wie folgt aussehen:

- Konstant ein
- 2 Impulse pro Sekunde

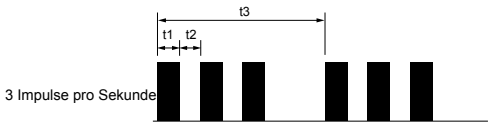
*Abbildung 47. 2 Impulse pro Sekunde*




t1 = 100 ms, t2 = 100 ms und t3 = 1 Sekunde

- 3 Impulse pro Sekunde

*Abbildung 48. 3 Impulse pro Sekunde*




t1 = 100 ms, t2 = 100 ms und t3 = 1 Sekunde

Der Statusausgang des Pressensteuerungsblocks ist nur als physischer Statusausgang verfügbar. Jeder physische Statusausgang kann drei verschiedene Ereignisse signalisieren.

Die folgende Abbildung zeigt die Standardeinstellungen des Statusausgangs des Pressensteuerungs-Funktionsblocks:

*Abbildung 49. Eigenschaften Pressen-Funktionsblock verfolgen*




Die Standardeinstellung des Funktionsblocks konfiguriert drei der IO-Pins als Statusausgänge. Wenn für eine bestimmte Anwendung nicht alle sieben Ereignisse angezeigt werden müssen, verwenden Sie den Schieberegler rechts neben der Abbildung, um weniger Pins auszuwählen. Durch Verschieben des Balkens um eine Position nach oben wird die Anzahl der Anschlüsse auf zwei reduziert, durch Verschieben des Balkens um zwei Positionen nach oben wird die Anzahl der Anschlüsse auf einen reduziert.

Die Funktionalität der einzelnen Ereignisse ist wie folgt:

- **Warten auf Reset**: Schaltet sich ein, wenn ein Reset-Eingang erforderlich ist, nachdem die nicht mutingfähigen und (sofern konfiguriert) mutingfähigen Sicherheitsstopp-Eingänge in den EIN-Zustand zurückgekehrt sind.
- **Betriebsbereit/Betrieb**: Ist immer dann eingeschaltet, wenn die Presse betriebsbereit ist (mutingfähige und nicht mutingfähige Sicherheitsstopp-Eingänge sind eingeschaltet und werden zurückgesetzt) oder wenn die Presse im Auf- oder Abwärtshub läuft.
- **SQS-Stopp**: Schaltet sich ein, wenn der Pressenstößel den SQS-Punkt (sequenzieller Stopp) erreicht.
- **PIP zurück Alarm prüfen**: Schaltet sich ein, wenn die Presse betriebsbereit ist und versucht wird, einen Pressenzyklus zu starten, und der PIP-Eingang (Part in Place), sofern konfiguriert, ausgeschaltet ist oder sich nicht ausgeschaltet hat und dann wieder eingeschaltet wird (Teil nicht entfernt und ausgetauscht).
- **Sicherheitsabschaltung**: Schaltet sich ein, wenn sich entweder der mutingfähige oder der nicht mutingfähige Eingang der Sicherheitsabschaltung ausschaltet und der GO-Eingangsknoten zu Tief wechselt (sofern für die Einstellung „Manueller Aufwärtshub“ konfiguriert), bevor SQS, BOS oder TOS erreicht wird (je nach Einstellungen und Teil des Prozesses).
- **Betriebsfehler**: Schaltet sich ein, wenn sich gegenseitig ausschließende Betriebseingänge eingeschaltet sind (z. B. TOS und BOS, TOS und SQS, TOS und PCMS, SQS und BOS usw.; wenn mehr als 3 Sekunden zwischen den Signalen von SQS und PCMS vergehen, schalten sich beide ein, falls konfiguriert).
- **Systemfehler**: Schaltet sich ein, wenn ein Systemfehler vorliegt.

# 7.10 Virtuelle Statusausgänge

Bis zu 64 virtuelle Statusausgänge können bei FID 1-Basiskontrollern für eine Konfiguration hinzugefügt werden, bei der die Modbus/TCP-, EtherNet/IP-Eingangsgruppen-, EtherNet/IP-explizite-Nachrichten- und PCCC-Protokolle verwendet werden, und bis zu 256 virtuelle Statusausgänge können bei FID 2-Basiskontrollern und SC10-2-Sicherheitskontrollern hinzugefügt werden. FID 2-Basiskontroller und SC10-2-Sicherheitskontroller können auch PROFINET verwenden. Diese Ausgänge können über das Netzwerk dieselben Informationen übermitteln wie die Statusausgänge. Siehe Statusausgangsfunktion auf Seite 74 für weitergehende Informationen. Die Funktion **Automatisch konfigurieren** auf der Registerkarte **Industrie-Ethernet** in der Software konfiguriert die virtuellen Statusausgänge auf Basis der aktuellen Konfiguration automatisch für eine Kombination häufig verwendeter Funktionen. Diese Funktion wird am besten verwendet, nachdem die Konfiguration festgelegt wurde. Die Konfiguration der virtuellen Statusausgänge kann nach der Verwendung der Funktion **Auto Configure (Automatisch konfigurieren)** manuell überarbeitet werden. Die über das Netzwerk verfügbaren Informationen entsprechen dem logischen Status der Ein- und Ausgänge innerhalb von 100 ms für die Tabellen der virtuellen Statusausgänge (diese können über die Software angezeigt werden) und innerhalb von 1 Sekunde für die anderen Tabellen. Der logische Status der Ein- und Ausgänge wird ermittelt, nachdem alle internen Entprellzeiten abgelaufen

und alle Tests abgeschlossen sind. Nähere Informationen zum Konfigurieren der virtuellen Statusausgänge finden Sie unter Registerkarte Industrie-Ethernet auf Seite 110.

ISD-Reihen sowie Leistung und Status einzelner Geräte können von SC10-2-Sicherheitskontrollern ab FID 2 abgerufen werden. Sechzehn Wörter (16 Bit) können zum Status der jeweiligen Reihe abgerufen werden. Drei administrative Wörter (16 Bit) und 18 Byte (je 8 Bit) der spezifischen Daten auf einem einzelnen Gerät einer Reihe können abgerufen werden. Nähere Informationen finden Sie unter Leistungs- und Statusinformationen zu einem einzelnen Gerät über ISD anfordern auf Seite 47.

# 8 Erste Schritte

Schalten Sie den Sicherheitskontroller ein und überprüfen Sie, ob die Betriebs-LED grün leuchtet (EIN).

## 8.1 Erstellen einer Konfiguration

Die folgenden Schritte sind erforderlich, um die Konfiguration abzuschließen und zu bestätigen (in den Kontroller zu schreiben):

1. Definition einer Schutzanwendung (Risikobeurteilung).
   - Bestimmung der erforderlichen Komponenten
   - Bestimmung der erforderlichen Sicherheitsstufe
2. Installieren Sie die Software für den Sicherheitskontroller von Banner. Siehe Installation der Software auf Seite 27.
3. Machen Sie sich mit den Optionen in der Software vertraut. Siehe Software-Übersicht auf Seite 97.
4. Starten Sie die Software und wählen Sie das gewünschte Gerät aus.
5. Starten Sie ein neues Projekt mit einem Klick auf **Neues Projekt/Zuletzt verwendete Dateien**.
6. Definieren Sie die **Projekteinstellungen**. Siehe Projekteinstellungen auf Seite 99.
7. XS/SC26-2: Passen Sie die Einstellungen des Basiskontrollers an und fügen Sie Erweiterungsmodule hinzu (sofern verwendet). Siehe Registerkarte Geräte auf Seite 100.
8. Fügen Sie Sicherheitseingangsgeräte, nicht sicherheitsrelevante Eingangsgeräte und Statusausgänge hinzu. Siehe Hinzufügen von Eingängen und Statusausgängen auf Seite 78.
9. Entwerfen Sie die Steuerungslogik. Siehe Entwerfen der Steuerungslogik auf Seite 82.
10. Stellen Sie optionale Ein- oder Ausschaltverzögerungszeiten für Sicherheitsausgänge ein.
11. Sofern verwendet, konfigurieren Sie die Netzwerkeinstellungen. Siehe Netzwerkeinstellungen: Modbus/TCP, Ethernet/IP, PCCC auf Seite 112 oder Netzwerkeinstellungen: PROFINET (XS/SC26-2 ab FID 2 und SC10-2) auf Seite 113.
12. Speichern und bestätigen Sie die Konfiguration. Siehe Speichern und Bestätigen einer Konfiguration auf Seite 83.

Die folgenden Schritte sind optional und können zur Unterstützung der Systeminstallation verwendet werden:

- Ändern Sie die Zugriffsrechte für die Konfiguration. Siehe XS/SC26-2 Passwort-Manager auf Seite 117 oder Passwort-Manager für SC10-2 auf Seite 118.
- Überprüfen Sie anhand der Registerkarte **Konfigurationsübersicht** die detaillierten Geräteinformationen und Ansprechzeiten. Siehe Registerkarte Konfigurationsübersicht auf Seite 116.
- Drucken Sie die Konfigurationsansichten, einschließlich der **Konfigurationsübersicht** und der **Netzwerkeinstellungen**. Siehe Druckoptionen auf Seite 116
- Konfigurationstests mit dem Simulationsmodus. Siehe Simulationsmodus auf Seite 123.

## 8.2 Hinzufügen von Eingängen und Statusausgängen

Sicherheits- und nicht sicherheitsrelevante Eingänge können entweder über die Registerkarte **Equipment (Geräte)** oder über die Registerkarte **Functional View (Funktionsansicht)** hinzugefügt werden. Statusausgänge können nur über die Registerkarte **Equipment (Geräte)** hinzugefügt werden. Virtuelle nicht sicherheitsrelevante Eingänge können nur über die Registerkarte **Functional View (Funktionsansicht)** hinzugefügt werden. Wenn Eingänge über die Registerkarte **Equipment (Geräte)** hinzugefügt werden, werden diese automatisch in die Registerkarte **Functional View (Funktionsansicht)** aufgenommen. Alle Eingänge, **Logik**- und **Funktionsblöcke** können auf der Registerkarte **Functional View (Funktionsansicht)** verschoben werden. Die **Sicherheitsausgänge** sind statisch auf der rechten Seite aufgeführt.

### 8.2.1 Hinzufügen von Sicherheits- und nicht sicherheitsrelevanten Eingängen

1. Klicken Sie in der Ansicht **Geräte** unter dem Modul, mit dem das Eingangsgerät verbunden werden soll, auf  (das Modul und die Klemmen können über das Fenster **Eigenschaften** für das Eingangsgerät geändert werden), oder auf einen Platzhalter auf der Registerkarte **Funktionsansicht**.

   **Anmerkung:** Virtuelle nicht sicherheitsrelevante Eingänge sind nur über die Registerkarte **Funktionsansicht** verfügbar.

2. Klicken Sie auf **Sicherheitseingang** oder **Nichtsicherheitsrelevanter Eingang**, um Eingangsgeräte hinzuzufügen:

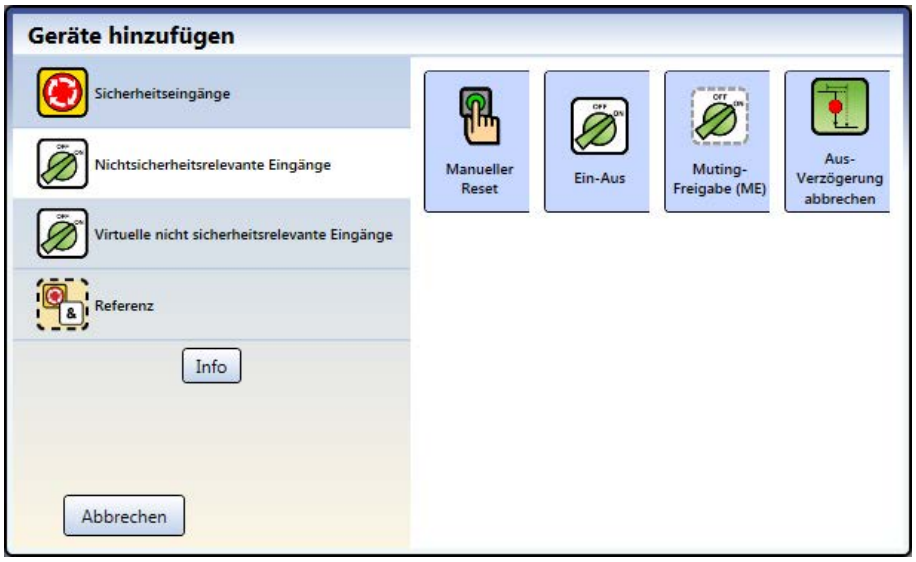
*Abbildung 50. XS/SC26-2: Hinzufügen von Eingängen aus der Funktionsansicht (virtuelle nicht sicherheitsrelevante Eingänge können nur aus dieser Ansicht hinzugefügt werden).*




*Abbildung 51. SC10-2: Hinzufügen von Eingängen aus der Geräteansicht (physischer Statusausgang kann nur aus dieser Ansicht hinzugefügt werden).*



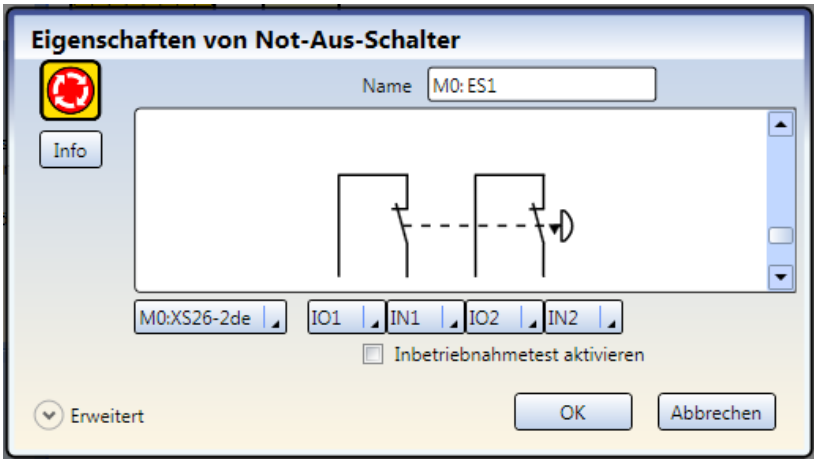

*Abbildung 52. Nicht sicherheitsrelevante Eingänge (virtuelle nicht sicherheitsrelevante Eingänge nur über die Registerkarte **Funktionsansicht** verfügbar)*




3. Wählen Sie die geeigneten Geräteeinstellungen aus:

### *Allgemeine Einstellungen:*

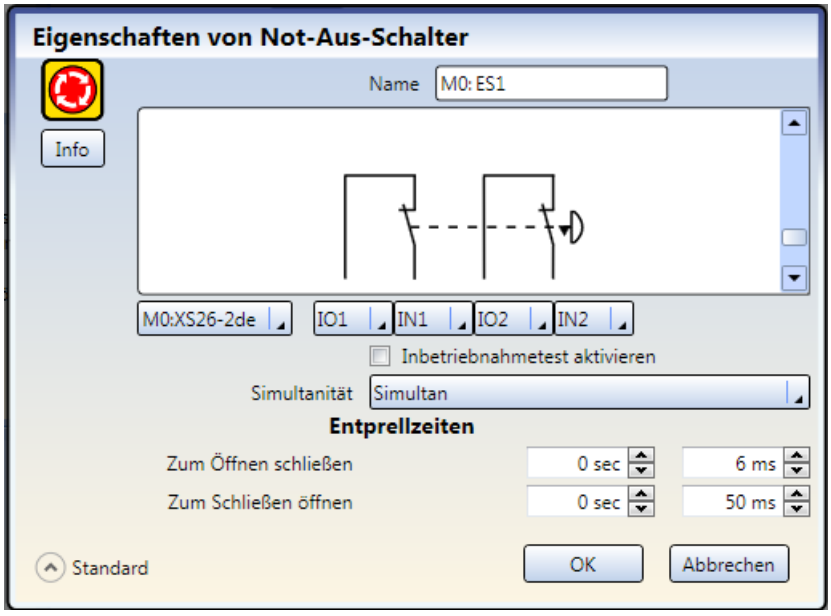
*Abbildung 53. Allgemeine Einstellungen für Sicherheitseingänge*




- *Name*: der Name des Eingangsgeräts. Dieser wird automatisch generiert und kann vom Benutzer geändert werden.
- *Schaltungstyp*: Die geeigneten Schaltungs- und Signalkonventionsoptionen für das ausgewählte Eingangsgerät; scrollen Sie zu der gewünschten Option und wählen Sie sie aus.
- *Modul*: Das Modul, an das das Eingabegerät angeschlossen ist (z. B. M0:XS26-2e).
- *Ein-/Ausgangsklemmen*: die Zuordnung der Eingangsklemmen für das ausgewählte Gerät an dem ausgewählten Modul.
- *Inbetriebnahmetest aktivieren* (sofern zutreffend): ein optionaler Test des Sicherheitseingangsgeräts als Vorsichtsmaßnahme, der nach jedem Anlauf erforderlich ist.
- *Reset-Optionen* (sofern zutreffend): diverse Optionen für den Reset, z. B. „Manueller Anlauf“, „System-Reset“ und „Reset Eingangsanzeigegruppe“.

### *Erweiterte Einstellungen (sofern zutreffend):*

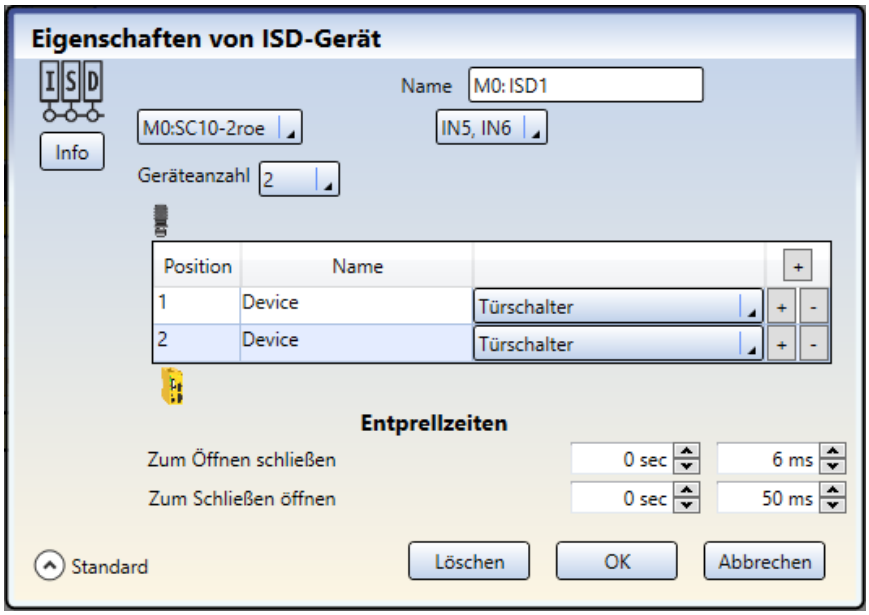
*Abbildung 54. Erweiterte Einstellungen für Sicherheitseingänge*




- *Simultanität* (sofern zutreffend): „Simultan“ oder „Nicht simultan“ (zu den Definitionen siehe Glossar auf Seite 297).
- *Entprellzeiten*: die Zeit für den Übergang des Signals in einen anderen Zustand.
- *Überwacht/Nicht überwacht* (sofern zutreffend): Siehe Reset-Signalanforderungen auf Seite 57

***ISD-Geräteeigenschaften (sofern zutreffend):***

*Abbildung 55. Erweiterte ISD-Geräteeinstellungen*



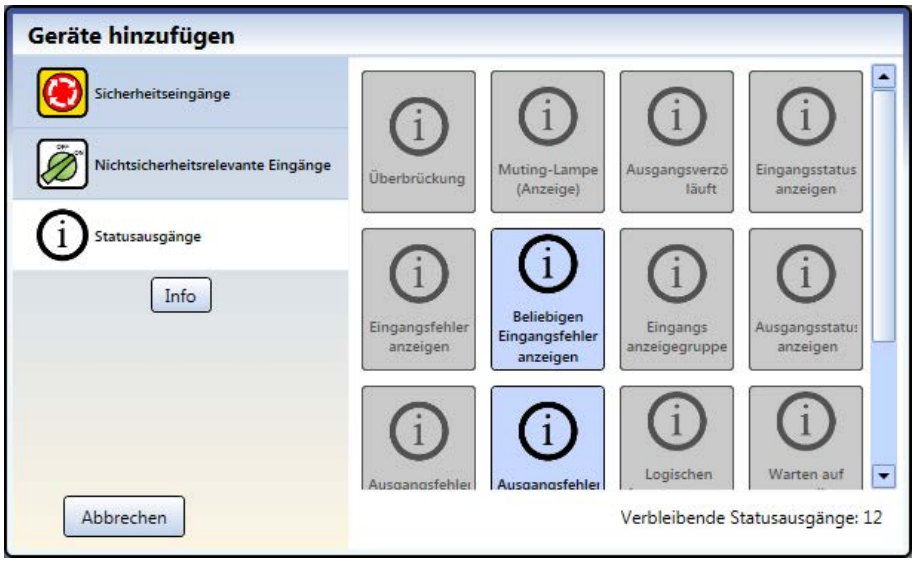

- *Name*: der Name des Eingangsgeräts. Dieser wird automatisch generiert und kann vom Benutzer geändert werden.
- *Ein-/Ausgangsklemmen*: die Zuordnung der Eingangsklemmen für das ausgewählte Gerät an dem ausgewählten Modul.
- *Anzahl an Geräten* (erforderlich): die in der Anwendung verwendete Anzahl an ISD-Sensoren
- *Position, Name und Typ*: Position, Name und Typ (Türschalter, Nothaltschalter, ISD-Anschluss) der in der Anwendung verwendeten ISD-Sensoren. Der **Name** wird automatisch generiert und kann vom Benutzer geändert werden. Der **Typ** kann vom Benutzer aus einem Menü ausgewählt werden.
- *Entprellzeiten*: die Zeit für den Übergang des Signals in einen anderen Zustand.

**Anmerkung:** Wenn die gesamte Reihe nur aus Türschaltern besteht, gelten die Konfigurationsregeln für einen Schutztürschalter. Handelt es sich bei einem Gerät im String um einen Nothaltschalter, gelten die Konfigurationsregeln für Nothaltschalter.

## 8.2.2 Hinzufügen von Statusausgängen

1. Klicken Sie auf der Registerkarte **Geräte** unter dem Modul, für das die Statusüberwachung durchgeführt werden soll, auf ✚.
2. Klicken Sie auf **Statusausgänge**, um die Statusüberwachung hinzuzufügen [11].

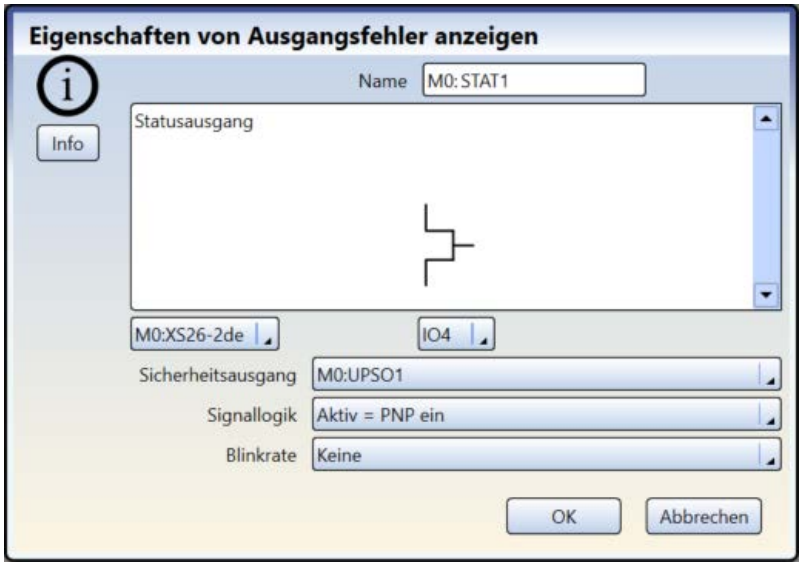
*Abbildung 56. Statusausgänge*




[11] Statusausgänge können konfiguriert werden, wenn der Status eines Eingangsgeräts oder eines Ausgangs kommuniziert werden muss. Die IOx-Klemmen werden für diese Statussignale verwendet.

3. Wählen Sie die geeigneten Einstellungen für Statusausgänge:

*Abbildung 57. Statusausgangs-Eigenschaften*




- *Name*
- *Modul*
- *E/A (sofern zutreffend)*
- *Klemme*
- *Eingang oder Ausgang (sofern zutreffend)*
- *Signallogik*
- *Blinkrate*

# 8.3 Entwerfen der Steuerungslogik

So **entwerfen Sie die Steuerungslogik**:

1. Fügen Sie die gewünschten **sicherheits**- und **nicht sicherheitsrelevanten Eingänge** hinzu:
   - Auf der Registerkarte **Geräte**: Klicken Sie auf unter dem Modul, mit dem der Eingang verbunden werden soll, auf ✣ (das Modul kann im Fenster **Eigenschaften** für den Eingang geändert werden).
   - Auf der Registerkarte **Funktionsansicht**: Klicken Sie auf einen leeren Platzhalter in der linken Spalte.

   Siehe Hinzufügen von Eingängen und Statusausgängen auf Seite 78 für weitere Informationen und Geräteeigenschaften.
2. Fügen Sie **Logik**- und/oder **Funktionsblöcke** hinzu (siehe Logikblöcke auf Seite 102 und Funktionsblöcke auf Seite 105), indem Sie auf einen beliebigen leeren Platzhalter im mittleren Bereich klicken.

**Anmerkung:** Die Ansprechzeit der Sicherheitsausgänge kann sich erhöhen, wenn eine große Anzahl von Blöcken zur Konfiguration hinzugefügt wird. Verwenden Sie die Funktions- und Logikblöcke effizient, um optimale Ansprechzeiten zu erzielen.

3. Stellen Sie die geeigneten Anschlüsse zwischen den hinzugefügten Eingängen, **Funktions-** und **Logikblöcken** und den Sicherheitsausgängen her.

**WARNUNG:**
- **Konfiguration entspricht den anwendbaren Normen**
- Wenn die Anwendung nicht entsprechend überprüft wird, können schwere oder tödliche Verletzungen die Folge sein.
- Die Software für den Sicherheitskontroller von Banner prüft primär die Logikkonfiguration auf Verbindungsfehler. Der Benutzer ist dafür verantwortlich, dass die Anwendung die Anforderungen an die Risikobewertung erfüllt und allen geltenden Normen entspricht.

**Anmerkung:** Die Checkliste auf der linken Seite enthält eine Anzeige der Anschlüsse, die für eine gültige Konfiguration erforderlich sind. Alle dort aufgeführten Anschlüsse müssen verbunden werden. Der Sicherheitskontroller akzeptiert keine ungültige Konfiguration.

**Anmerkung:** Der Ausgangsknoten eines beliebigen Elements kann mit mehreren Eingangsknoten verbunden werden. Ein Eingangsknoten kann nur mit einem Element verbunden sein.

**Tipp:** Zur Unterstützung beim Erstellen einer gültigen Konfiguration zeigt das Programm hilfreiche Quickinfos an, wenn Sie versuchen, einen ungültigen Anschluss zu verbinden.

# 8.4 Speichern und Bestätigen einer Konfiguration

Die Bestätigung ist ein Überprüfungsprozess, bei dem der Sicherheitskontroller die von der Software generierte Konfiguration auf ihre logische Integrität und Vollständigkeit überprüft. Der Benutzer muss das Ergebnis überprüfen und bestätigen, bevor die Konfiguration gespeichert und vom Sicherheitskontroller verwendet werden kann. Nachdem die Konfiguration bestätigt wurde, kann sie an einen Sicherheitskontroller gesendet oder auf einem PC oder einem SC-XM2/3-Laufwerk gespeichert werden.

**WARNUNG:**
- Inbetriebnahmeprüfung abschließen
- Wenn dieses Inbetriebnahmeprüfungsverfahren nicht eingehalten wird, können schwere oder tödliche Verletzungen die Folge sein.
- Nachdem die Konfiguration bestätigt wurde, muss der Betrieb des Sicherheitskontrollers vollständig getestet werden (Inbetriebnahmeprüfung), bevor er zur Steuerung von Gefahren verwendet werden kann.

## 8.4.1 Speichern einer Konfiguration

1. Klicken Sie auf **Projekt speichern**.
2. Wählen Sie **Save As (Speichern unter)**.
3. Navigieren Sie zu dem Ordner, in dem Sie die Konfiguration speichern möchten.
4. Benennen Sie die Datei (der Dateiname kann mit dem Konfigurationsnamen identisch oder von diesem verschieden sein).
5. Klicken Sie auf **Save (Speichern)**.

## 8.4.2 Bestätigung einer Konfiguration

Der Sicherheitskontroller muss eingeschaltet und mit dem SC-USB2-Kabel am PC angeschlossen sein.

1. Klicken Sie auf .
2. Klicken Sie auf **Konfiguration in den Kontroller schreiben**.
3. Geben Sie das Passwort ein, wenn Sie dazu aufgefordert werden (das Standardpasswort lautet 1901).
   Der Bildschirm **Wechsel in den Konfig.-Modus** wird geöffnet.
4. Klicken Sie auf **Weiter**, um in den Konfigurationsmodus zu wechseln.
   Nachdem der Vorgang **Konfiguration wird aus dem Kontroller gelesen** abgeschlossen ist, wird der Bildschirm **Bestätigung einer Konfiguration** geöffnet.
5. Überprüfen Sie, ob die Konfiguration korrekt ist.
6. **Führen Sie einen Bildlauf bis zum Ende der Konfiguration durch und klicken Sie auf Bestätigen.**
7. Klicken Sie auf **Schließen**, nachdem der Vorgang **Schreiben der Konfiguration in den Kontroller** abgeschlossen ist.

**Anmerkung:**
- Die Netzwerkeinstellungen werden separat von den Konfigurationseinstellungen gesendet. Klicken Sie im Fenster **Netzwerkeinstellungen** auf **Senden**, um die Netzwerkeinstellungen auf den Sicherheitskontroller zu schreiben.
- SC10-2 und XS/SC26-2 ab FID 3: Netzwerkeinstellungen werden nur dann automatisch gesendet, wenn es sich bei dem Sicherheitskontroller um einen werkseitig voreingestellten Sicherheitskontroller handelt. Andernfalls müssen Sie das Fenster **Netzwerkeinstellungen** verwenden.
- SC10-2 und XS/SC26-2 ab FID 3: Passwörter werden nur dann automatisch geschrieben, wenn es sich bei dem Sicherheitskontroller um einen werkseitig voreingestellten Sicherheitskontroller handelt oder wenn die Konfiguration bestätigt wurde. Andernfalls müssen Sie das Fenster **Password Manager (Passwort-Manager)** verwenden, um Passwörter auf den Sicherheitskontroller zu schreiben.

Beim Konfigurieren eines SC10-2 oder XS/SC26-2 ab FID 3 wird unter Umständen der Bildschirm **Do you want to change the passwords of the controller? (Möchten Sie die Passwörter des Kontrollers ändern?)** angezeigt.

8. SC10-2 und XS/SC26-2 ab FID 3: Ändern Sie die Passwörter, wenn Sie dazu aufgefordert werden und wenn gewünscht.
9. Schalten Sie den Sicherheitskontroller aus und wieder ein oder führen Sie einen System-Reset aus, damit die Änderungen wirksam werden.
10. Speichern Sie die bestätigte Konfiguration auf dem PC.

**Anmerkung:** Es wird empfohlen, die jetzt bestätigte Konfiguration zu speichern. Bestätigte Konfigurationen haben ein anderes Dateiformat (.xcc) als unbestätigte Dateien (.xsc). Für das Laden in ein SC-XM2/3-Laufwerk sind bestätigte Konfigurationen erforderlich. Klicken Sie auf **Speichern unter**.

## 8.4.3 Schreiben der bestätigten Konfiguration mithilfe des Programmierwerkzeugs auf einen SC-XM2/3

1. Fügen Sie den SC-XM2/3 in das SC-XMP2-Programmierwerkzeug ein.
2. Öffnen Sie die Banner-Software für den Sicherheitskontroller von Banner und stecken Sie das Programmierwerkzeug in einen USB-Port am Computer ein.
   Das Symbol SC-XM2/3 sollte live geschaltet werden (wird etwas dunkler als ausgegraut angezeigt).
3. Klicken Sie auf und wählen Sie **Write XM (XM schreiben)**.

**Anmerkung:** Wenn **Write XM (XM schreiben)** ausgegraut ist, handelt es sich bei der Konfiguration nicht um eine .xcc (bestätigte Version).

4. Überprüfen Sie die gewünschten Passwörter.
5. Klicken Sie auf **Send to XM (An XM senden)**.
   Das Fenster **Writing Configuration to SC-XM drive (Konfiguration wird auf SC-XM-Laufwerk geschrieben)** wird geöffnet.

**Anmerkung:** Bei diesem Vorgang werden alle Daten (Konfigurationsdaten, Netzwerkeinstellungen und Passwörter) auf das SC-XM2/3-Laufwerk kopiert.

6. Klicken Sie nach Abschluss des Vorgangs auf **Save Confirmed Configuration (Bestätigte Konfiguration speichern)** und dann auf **Close (Schließen)**, oder klicken Sie auf **Close (Schließen)**, wenn die Datei bereits auf dem PC gespeichert wurde.

## 8.4.4 Hinweise zum Bestätigen oder Schreiben einer Konfiguration in einen konfigurierten SC10-2 oder XS/SC26-2 ab FID 3

Benutzereinstellungen und Passwörter beeinflussen die Art und Weise, wie das System beim Bestätigen einer Konfiguration oder beim Schreiben einer bestätigten Konfiguration in einen konfigurierten Sicherheitskontroller SC10-2 oder XS/SC26-2 ab FID 3 reagiert.

### Benutzer1

1. Klicken Sie auf **Konfiguration in den Kontroller schreiben**, um eine Konfiguration zu bestätigen bzw. um eine bestätigte Konfiguration in einen konfigurierten Sicherheitskontroller zu schreiben.
2. Geben Sie das Passwort „Benutzer1“ ein.
3. Der Bestätigungs- bzw. Schreibvorgang beginnt.

Am Ende des Bestätigungs- bzw. Schreibvorgangs hat der Sicherheitskontroller folgende Daten empfangen:

- Neue Passwörter
- Neue Konfiguration

Die Netzwerkeinstellungen werden nicht geändert.

### Benutzer2 oder Benutzer3 – Bestätigen oder Schreiben der Konfiguration erfolgreich

Dieses Szenario setzt die folgenden Einstellungen für Benutzer2 oder Benutzer3 voraus:

- **Berechtigung zum Ändern der Konfiguration** = aktiviert
- **Berechtigung zum Ändern der Netzwerkeinstellungen** = aktiviert ODER deaktiviert

1. Klicken Sie auf **Konfiguration in den Kontroller schreiben**, um eine Konfiguration zu bestätigen bzw. um eine bestätigte Konfiguration in einen konfigurierten Sicherheitskontroller zu schreiben.

2. Geben Sie das Passwort für Benutzer2 oder Benutzer3 ein.
3. Der Bestätigungs- bzw. Schreibvorgang beginnt.

Am Ende des Bestätigungs- bzw. Schreibvorgangs hat der Sicherheitskontroller folgende Daten empfangen:

- Neue Konfiguration

Passwörter und Netzwerkeinstellungen werden nicht geändert.

### Benutzer2 oder Benutzer3 – Bestätigen oder Schreiben der Konfiguration nicht erfolgreich

Dieses Szenario setzt die folgenden Einstellungen für Benutzer2 oder Benutzer3 voraus:

- **Berechtigung zum Ändern der Konfiguration** = deaktiviert
- **Berechtigung zum Ändern der Netzwerkeinstellungen** = aktiviert ODER deaktiviert

1. Klicken Sie auf **Konfiguration in den Kontroller schreiben**, um eine Konfiguration zu bestätigen bzw. um eine bestätigte Konfiguration in einen konfigurierten Sicherheitskontroller zu schreiben.
2. Geben Sie das Passwort für Benutzer2 oder Benutzer3 ein.
3. Der Bestätigungs- bzw. Schreibvorgang wird abgebrochen.

## 8.5 Beispielkonfigurationen

Die Software enthält diverse Beispielkonfigurationen, die unterschiedliche Anwendungen des Sicherheitskontroller zeigen. Um auf die Konfigurationen zuzugreifen, gehen Sie zu **Projekte öffnen** > **Beispielprojekte** und wählen Sie das gewünschte Projekt aus.

Für den XS/SC26-2 gibt es drei Gruppen von Beispielkonfigurationen:

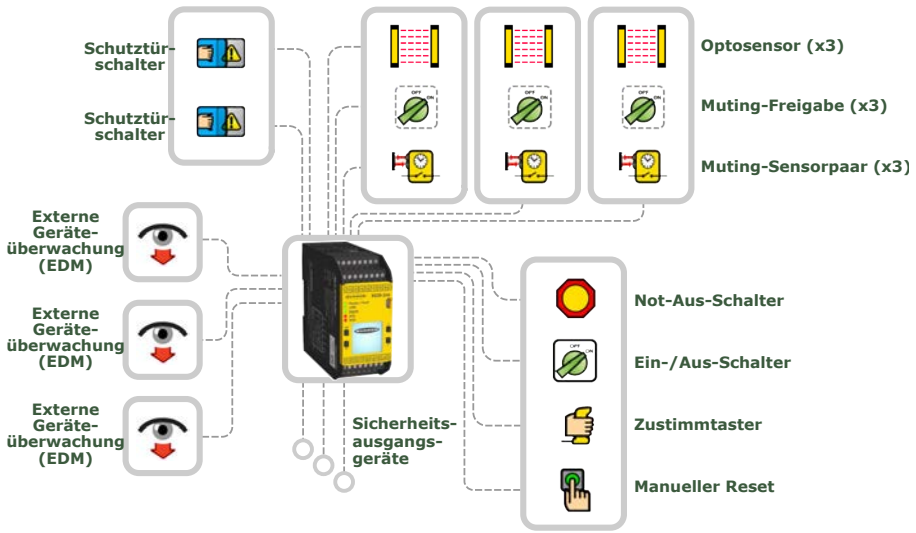
- **Anwendungen**: Hier befinden sich vier Beispiele einfacher möglicher Anwendungen des Kontrollers. Zwei der Beispiele beziehen sich auf den Austausch veralteter Module.
- **Dokumentation**: Enthält Beispiele. Die meisten der hier enthaltenen Beispiele werden in den folgenden Abschnitten beschrieben; eines davon ist in der (online verfügbaren) Kurzanleitung beschrieben.
- **Beispiele**: Diese enthalten die drei Bereiche: **Funktionsblöcke**, **Logikblöcke** und **Sicherheitsausgänge**. Diese Beispiele zeigen die Funktionen der jeweiligen Blöcke. Wenn Sie beispielsweise wissen möchten, wie ein Überbrückungsblock funktioniert, wählen Sie **Funktionsblöcke** > **Überbrückungsblock (alle Funktionen aktiviert)** aus und führen den Simulationsmodus aus.

Der SC10-2 hat acht Beispielkonfigurationen. Diese Beispiele umfassen typische Anwendungen des SC10-2-Modells. Verwenden Sie die Beispiele als Ausgangskonfiguration und ändern Sie sie entsprechend Ihren Anforderungen ab.

## 8.5.1 XS/SC26-2 Beispielkonfiguration

In diesem Abschnitt wird beschrieben, wie Sie die Beispielkonfiguration aus der „Anleitung zum Muting von 3 Zonen“ erstellen. Diese befindet sich unter den Beispielprogrammen des XS/SC26-2 im Abschnitt **Dokumentation**. Diese Beispielkonfiguration ist für eine Palettierroboter-Anwendung, die einen XS26-2-Sicherheitskontroller, ein sicherheitsrelevantes Eingangsmodul vom Typ XS8si, drei Optosensoren (Muting wird über die Software hinzugefügt), zwei Verriegelungsschalter, einen manuellen Reset-Schalter und einen Not-Aus-Schalter verwendet.

*Abbildung 58. Beispielkonfiguration (schematische Darstellung)*




So erstellen Sie die Konfiguration für diese Anwendung:

1. Klicken Sie auf **Neues Projekt**.

2. Definieren Sie die Projekteinstellungen. Siehe Projekteinstellungen auf Seite 99.
3. Wählen Sie die Basiskontroller-Ausführung aus. Siehe Registerkarte Geräte auf Seite 100 (bei dieser Konfiguration muss nur das Kontrollkästchen **Ist erweiterbar** markiert werden).
4. Fügen Sie das Erweiterungsmodul **XS8si** mit einem Klick auf ✚ rechts vom Basiskontroller hinzu.
    a. Klicken Sie auf **Eingangsmodule**.
    b. Wählen Sie **XS8si**.
5. Fügen Sie die folgenden Eingänge hinzu. Ändern Sie dabei nur den Schaltungstyp:

| Eingang | Anzahl | Typ | Modul | Anschlüsse | Schaltung |
|---|---|---|---|---|---|
| **Not-Aus-Schalter** | 1 | Sicherheitseingang | XS8si | IO1, IN1, IN2 | Zweikanalig, 3 Anschlüsse |
| **Zustimmtaster** | 1 | Sicherheitseingang | XS8si | IO1, IN3, IN4 | Zweikanalig, 3 Anschlüsse |
| **Externe Geräteüberwachung** | 3 | Sicherheitseingang | Sockel | 1. IO3<br>2. IO4<br>3. IO5 | Einkanalig 1 Anschluss |
| **Schutztürschalter** | 2 | Sicherheitseingang | Sockel | 1. IO1, IN15, IN16<br>2. IO2, IN17, IN18 | Zweikanalig, 3 Anschlüsse |
| **Manueller Reset** | 1 | Nicht sicherheitsrelevanter Eingang | XS8si | IN6 | Einkanalig 1 Anschluss |
| **Muting-Sensorpaar** | 3 | Sicherheitseingang | Sockel | 1. IN9, IN10<br>2. IN11, IN12<br>3. IN13, IN14 | Zweikanalig, 2 Anschlüsse |
| **Muting-Freigabe (ME)** | 3 | Nicht sicherheitsrelevanter Eingang | Sockel | 1. IN1<br>2. IN2<br>3. IO8 | Einkanalig, 1 Anschluss |
| **Ein-Aus** | 1 | Nicht sicherheitsrelevanter Eingang | XS8si | IN5 | Einkanalig, 1 Anschluss |
| **Optosensor** | 3 | Sicherheitseingang | Sockel | 1. IN3, IN4<br>2. IN5, IN6<br>3. IN7, IN8 | Zweikanalig PNP |

6. Öffnen Sie die Registerkarte **Funktionsansicht**.



**Tipp:** Sie sehen möglicherweise, dass nicht alle Eingänge auf Seite 1 aufgeführt sind. Es gibt zwei Lösungen, um die Konfiguration auf einer Seite aufzuführen. Führen Sie hierzu einen der folgenden Schritte aus:

1. Fügen Sie eine **Referenz** zu dem Block hinzu, der sich auf einer anderen Seite befindet. Klicken Sie hierzu auf einen leeren Platzhalter im mittleren Bereich, wählen Sie **Referenz** und wählen Sie den Block aus, der sich auf der nächsten Seite befindet. Nur Blöcke von anderen Seiten können als **Referenz** hinzugefügt werden.
2. Seite neu zuweisen: Standardmäßig werden alle Eingänge, die in der Ansicht **Geräte** hinzugefügt werden, in der **Funktionsansicht** auf den ersten verfügbaren Platzhalter in der linken Spalte gesetzt. Die Eingänge können jedoch an eine beliebige Stelle im mittleren Bereich verschoben werden. Verschieben Sie einen der Blöcke an einen beliebigen Platzhalter im mittleren Bereich. Rufen Sie die Seite aus, die den Block enthält, welcher verschoben werden soll. Wählen Sie den Block aus und ändern Sie die Seitenzuordnung unter der Tabelle **Eigenschaften**.

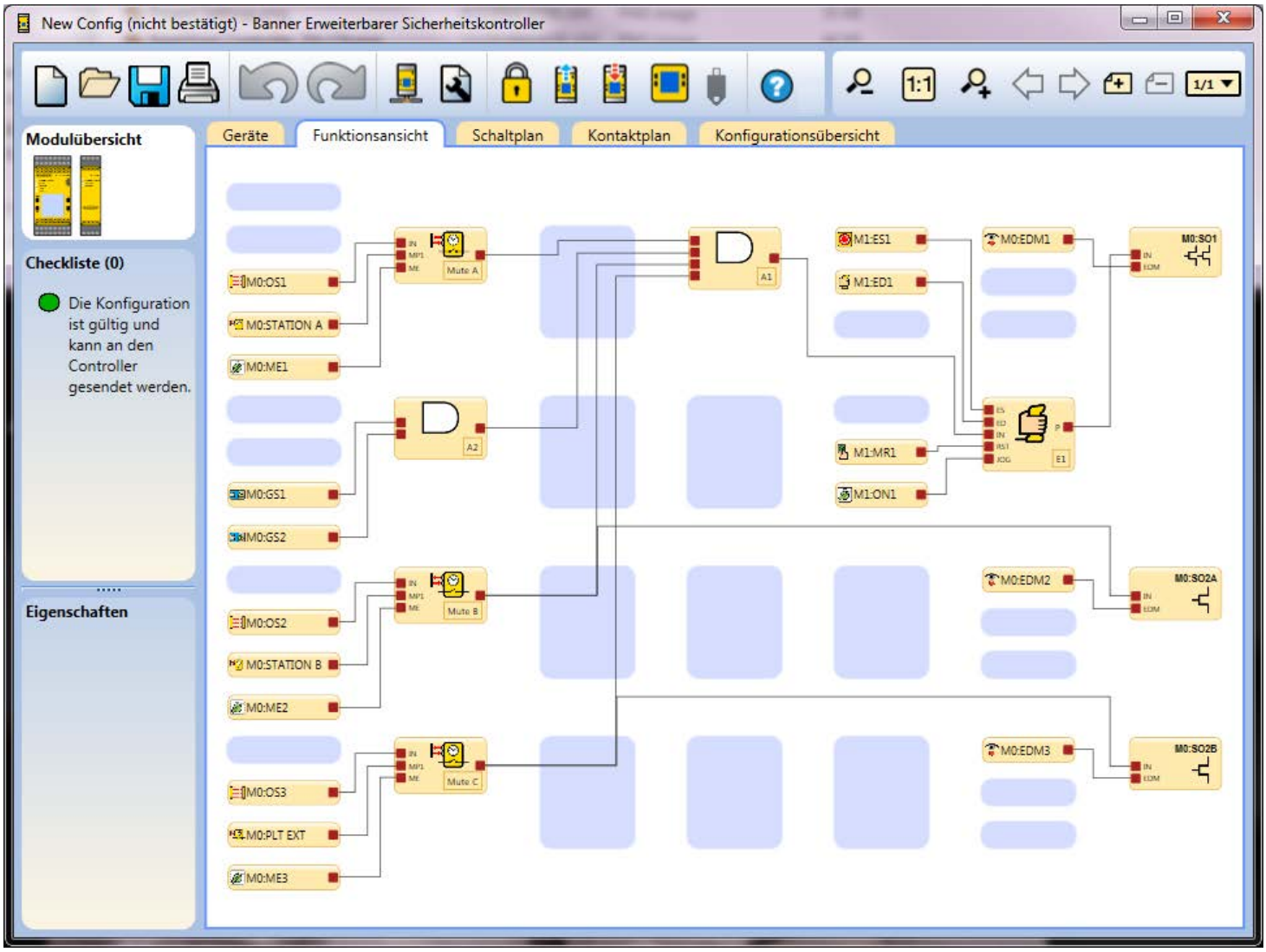
7. **M0:SO2** teilen:
    a. Doppelklicken Sie auf **M0:SO2** oder markieren Sie dieses Element und klicken Sie auf **Bearbeiten** unter der Tabelle **Eigenschaften**.
    b. Klicken Sie auf **Teilen.**
8. Fügen Sie die folgenden **Funktionsblöcke** hinzu, indem Sie im mittleren Bereich auf der Registerkarte **Funktionsansicht** auf einen leeren Platzhalter klicken (weitere Informationen finden Sie unter Funktionsblöcke auf Seite 105):
    - **Muting-Block** x **3** (**Muting-Mode**: 1 Paar, **ME (Muting-Aktivierung)**: aktiviert)
    - **Zustimmtaster-Block** (**ES**: aktiviert, **JOG (Weiterschalten)**: aktiviert)
9. Fügen Sie die folgenden **Logikblöcke** hinzu, indem Sie im mittleren Bereich auf der Registerkarte**Funktionsansicht** auf einen leeren Platzhalter klicken (weitere Informationen finden Sie unter Logikblöcke auf Seite 102):
    - **AND** mit 2 Eingangsknoten
    - **AND** mit 4 Eingangsknoten

10. Verbinden Sie folgende Vorrichtungen mit jedem **Muting-Block**:
    - 1 **Optosensor** (**IN**-Knoten)
    - 1 **Muting-Sensorpaar** (**MP1**-Knoten)
    - 1 **Muting-Freigabe** (**ME**-Knoten)
11. Verbinden Sie 2 **Schutztürschalter** mit dem **AND**-Block mit 2 Knoten.
12. Verbinden Sie 3 **Muting-Blöcke** und den **AND**-Block mit 2 Knoten mit dem **AND**-Block mit 4 Knoten.
13. Verbinden Sie einen der **Muting-Blöcke** mit einem der geteilten Sicherheitsausgänge (**M0:SO2A** oder **M0:SO2B**) und mit einem Anschluss des anderen geteilten Sicherheitsausgangs.
14. Verbinden Sie folgende Vorrichtungen mit dem **Zustimmtaster-Block**:
    - **Not-Aus-Schalter** (**ES**-Knoten)
    - **Zustimmtaster** (**ED**-Knoten)
    - **AND**-Block mit vier Eingangsknoten (**IN**-Knoten)
    - **Manueller Reset** (**RST**-Knoten)
    - **Ein-Aus** (**JOG**-Knoten)
15. Verbinden Sie den **Zustimmtaster-Block** mit dem verbleibenden Sicherheitsausgang (**M0:SO1**).
16. Aktivieren Sie *EDM (externe Geräteüberwachung)* für jeden Sicherheitsausgang in dem jeweiligen Fenster **Eigenschaften**.
17. Verbinden Sie je 1 Eingang für **externe Geräteüberwachung** mit den Sicherheitsausgängen.

Die Beispielkonfiguration ist abgeschlossen.

**Anmerkung:** An dieser Stelle können Sie die Blöcke auf der Registerkarte **Funktionsansicht** neu anordnen, um den Konfigurationsablauf zu optimieren (siehe Abbildung 59 auf Seite 87).

*Abbildung 59. Beispielkonfiguration – Registerkarte **Funktionsansicht***

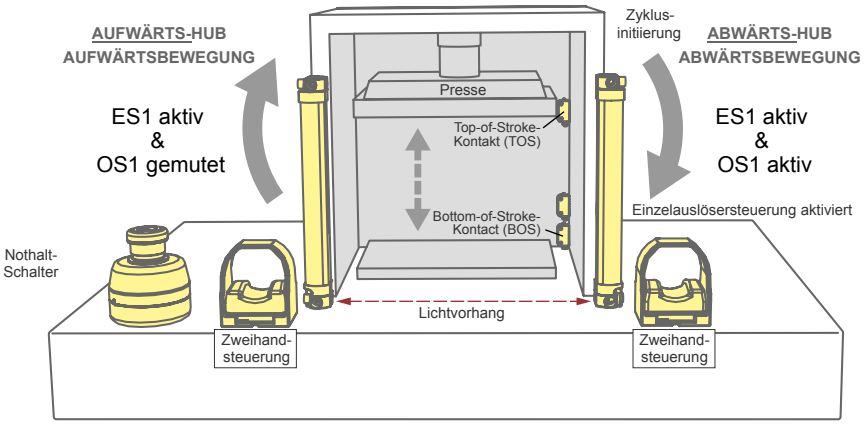


# 8.5.2 XS/SC26-2: Beispielkonfiguration – einfache Pressensteuerung mit mutingfähigem Sicherheitseingang

In diesem Abschnitt wird beschrieben, wie Sie ein einfaches Pressensteuerungssystem erstellen. Dieses befindet sich unter den Beispielprogrammen des XS/SC26-2 im Abschnitt „Dokumentation“.

Diese Beispielkonfiguration eignet sich für eine einfache hydraulische/pneumatische Pressenanwendung, die einen XS26-2 Sicherheitskontroller, Pressenstatuseingänge, eine Zyklusinitiierung, einen manuellen Reset, einen optischen Sicherheitssensor und einen Nothaltschalter verwendet.

*Abbildung 60. Beispielkonfiguration für eine einfache Pressensteuerung*




So erstellen Sie die Konfiguration für diese Anwendung:

1. Klicken Sie auf **Neues Projekt**.
2. Legen Sie die Projekteinstellungen fest.

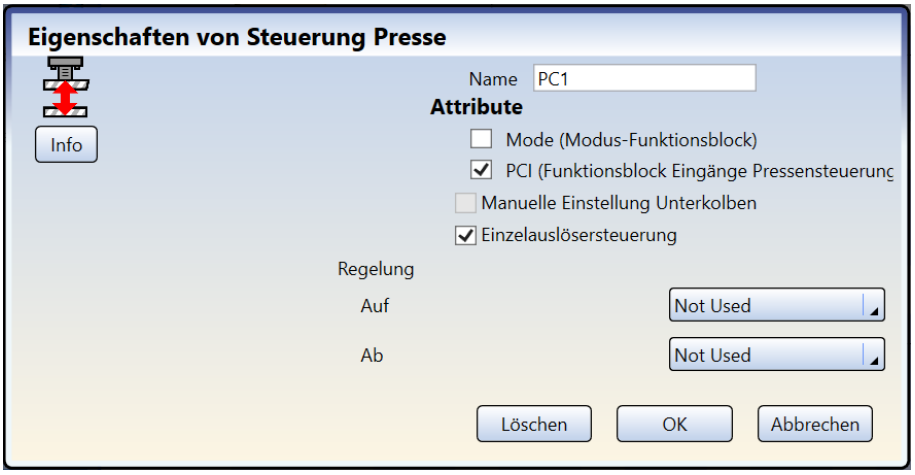
   Siehe Projekteinstellungen auf Seite 99.
3. Wählen Sie das gewünschte Basiskontroller-Modell aus.

   Siehe Registerkarte Geräte auf Seite 100.
4. Fügen Sie die folgenden Eingänge hinzu und ändern Sie bei Bedarf den Namen und den Schaltungstyp.

| Eingang | Anzahl | Typ | Anschlüsse | Schaltung |
|---|---|---|---|---|
| Zyklusinitiierung | 1 | Sicherheitseingang | IN1, IN2 | Zweikanalig, 2 Anschlüsse |
| TOS (ein/aus) | 1 | Nicht sicherheitsrelevant | IN5 | Einkanalig, 1 Anschluss |
| BOS (ein/aus) | 1 | Nicht sicherheitsrelevant | IN6 | Einkanalig, 1 Anschluss |
| Manueller Reset | 1 | Nicht sicherheitsrelevant | IN7 | Einkanalig, 1 Anschluss |
| Nothaltschalter | 1 | Sicherheitseingang | IN10, IN11 | Zweikanalig, 2 Anschlüsse |
| Optosensor | 1 | Sicherheitseingang | IN8, IN9 | Zweikanalig, pnp |

5. Öffnen Sie die Registerkarte **Funktionsansicht**.
6. Fügen Sie den Pressensteuerungs-Funktionsblock hinzu und konfigurieren Sie ihn.
   a) Klicken Sie im mittleren Bereich der Registerkarte **Functional View (Funktionsansicht)** auf einen leeren Platzhalter. Für weitere Informationen siehe Funktionsblöcke auf Seite 105.
   b) Wählen Sie **Function Blocks (Funktionsblöcke)** und dann **Press Control (Pressensteuerung)** aus.
   c) Wählen Sie im Fenster **Press Control Properties (Eigenschaften der Pressensteuerung)** die Optionen **PCI (Press Control Input Function Block) (PCI [Funktionsblock Pressensteuerungseingang])** und **Single Actuator Control (Einzelauslösersteuerung)** aus.

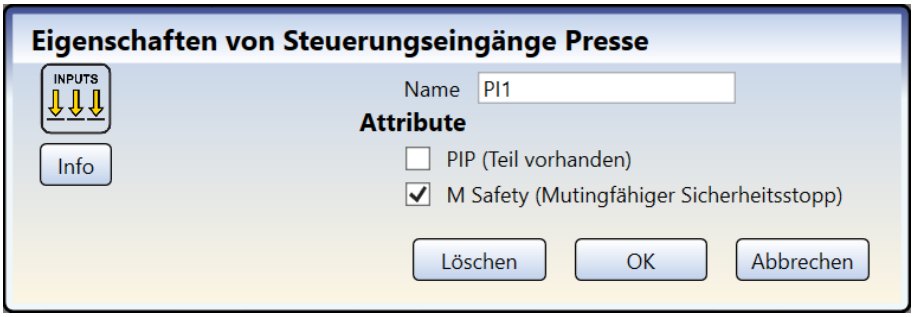
*Abbildung 61. **Eigenschaften der Pressensteuerung***




Das Häkchen im Kästchen **Manual Upstroke Setting (Manuelle Einstellung Aufwärtshub)** erlischt.

d) Auf **OK** klicken.
Das Fenster **Press Control Inputs Properties (Eigenschaften der Pressensteuerungseingänge)** wird geöffnet.

*Abbildung 62. **Eigenschaften der Pressensteuerungseingänge***




e) Wählen Sie **M Safety (Mutable Safety Stop) (M-Sicherheit [Mutingfähiger Sicherheitsstopp])**.

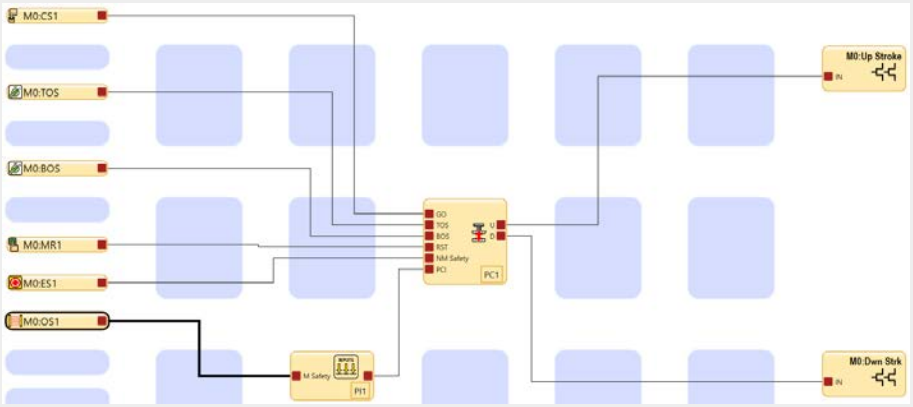
f) Auf **OK** klicken.

7. Verbinden Sie die folgenden Anschlüsse:
   - Zyklusinitiierungseingang mit dem GO-Knoten des Pressensteuerungs-Funktionsblocks
   - TOS mit dem TOS-Knoten des Pressensteuerungs-Funktionsblocks
   - BOS mit dem BOS-Knoten des Pressensteuerungs-Funktionsblocks
   - Manuellen Reset mit dem RST-Knoten des Pressensteuerungs-Funktionsblocks
   - Nothaltschalter mit dem NM-Sicherheitsknoten des Pressensteuerungs-Funktionsblocks
   - Optischen Sensor mit dem M-Sicherheitsknoten des Funktionsblocks Pressensteuerungseingang
8. Verbinden Sie den U-Ausgangsknoten des Pressensteuerungs-Funktionsblocks mit SO1 (ändern Sie den Namen von SO1 in „Aufwärtshub“).
9. Verbinden Sie den D-Ausgangsknoten des Pressensteuerungs-Funktionsblocks mit SO2 (ändern Sie den Namen von SO2 in „Abwärtshub“).

Die Beispielkonfiguration ist abgeschlossen.

**Anmerkung:** An diesem Punkt kann es hilfreich sein, die Blöcke in der Funktionsansicht für einen besseren Konfigurationsfluss neu zu positionieren, wie in der folgenden Abbildung dargestellt:

*Abbildung 63. **Funktionsblock-Position***




## XS/SC26-2: Simulieren Sie die Funktionalität der Konfiguration für die einfache Pressensteuerung

Im Folgenden wird beschrieben, wie die Funktionalität der Konfiguration für die einfache Pressensteuerung simuliert wird:

1. Klicken Sie auf , um den Simulationsmodus aufzurufen.
2. Klicken Sie auf **Play (Wiedergabe)**, um den Simulationstimer einzuschalten (ähnlich wie beim Einschalten der Maschine).
3. Klicken Sie auf die Eingänge für Nothaltschalter, optischen Sensor und TOS für den Ein-Zustand (grün).
4. Klicken Sie auf den MR1-Reset-Eingang.
   Der Pressensteuerungs-Funktionsblock sollte sich einschalten (grün).
5. Versetzen Sie den CS1-Eingang mit einem Klick in den Ein-Zustand (grün).
   Der Abwärtshub-Ausgang schaltet sich ein (grün).
6. Versetzen Sie den TOS-Eingang mit einem Klick in den Aus-Zustand (rot).
7. Versetzen Sie den BOS-Eingang mit einem Klick in den Ein-Zustand (grün).
   Der Abwärtshub-Ausgang schaltet sich aus (rot) und der Aufwärtshub-Ausgang schaltet sich ein (grün).
8. Schalten Sie den BOS-Eingang mit einem Klick aus (rot).
9. Versetzen Sie den TOS-Eingang mit einem Klick in den Ein-Zustand (grün).
   Der Aufwärtshub-Ausgang schaltet sich aus (rot).
10. Versetzen Sie den CS1-Eingang mit einem Klick in den Aus-Zustand (rot). Dies kann jederzeit nach dem Einschalten (grün) des Abwärtshub-Ausgangs erfolgen.
11. Versetzen Sie den optischen Sensoreingang mit einem Klick in den Aus- (rot) und dann zurück in den Ein-Zustand (grün).

Das System ist bereit, den nächsten Zyklus durch erneutes Einschalten des CS1-Eingangs zu starten.

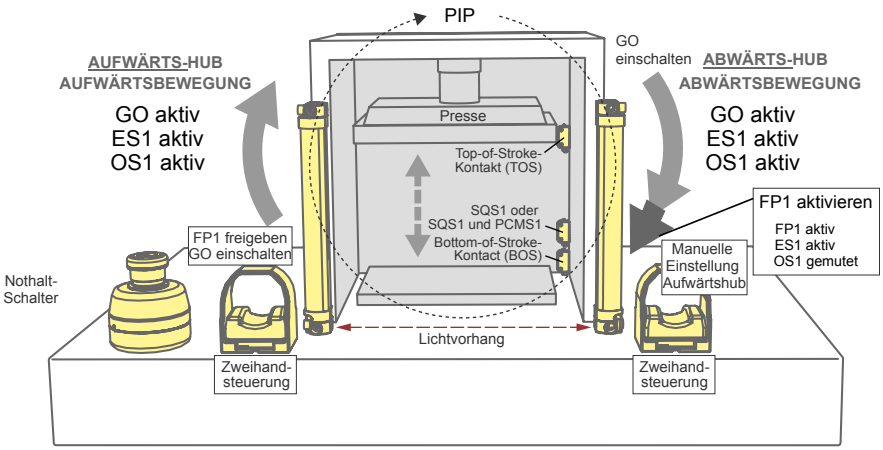
Wenn der optische Sensor oder der Nothaltschalter während des Aufwärts- oder Abwärtshubs ausgeschaltet wird, muss der MR1-Eingang durchgeschaltet werden, und durch die Aktivierung von CS1 schaltet sich dann der Aufwärtshub-Ausgang ein.

# 8.5.3 XS/SC26-2: Beispielkonfiguration der vollfunktionalen Pressensteuerung

In diesem Abschnitt wird die Konzeption eines Pressensteuerungssystems beschrieben, das die möglichen Funktionen vollständig verwendet (Ausnahme: AVM). Die Beispielkonfiguration befindet sich unter dem Abschnitt „Documentation (Dokumentation)“ der XS/SC26-2-Beispielprogramme.

Diese Beispielkonfiguration ist für eine komplexere hydraulische/pneumatische Pressenanwendung gedacht, bei der ein XS26-2 Sicherheitskontroller, ein XS2so Sicherheitsausgangsmodul, Pressenstatuseingänge, Zyklusstart, ein manueller Reset, ein optischer Sicherheitssensor, sequenzieller Stopp, Muting-Sensor, Fußpedal-Eingang und ein Nothaltschalter verwendet wird.

*Abbildung 64. Musterkonfiguration der Pressensteuerung mit vollem Funktionsumfang*



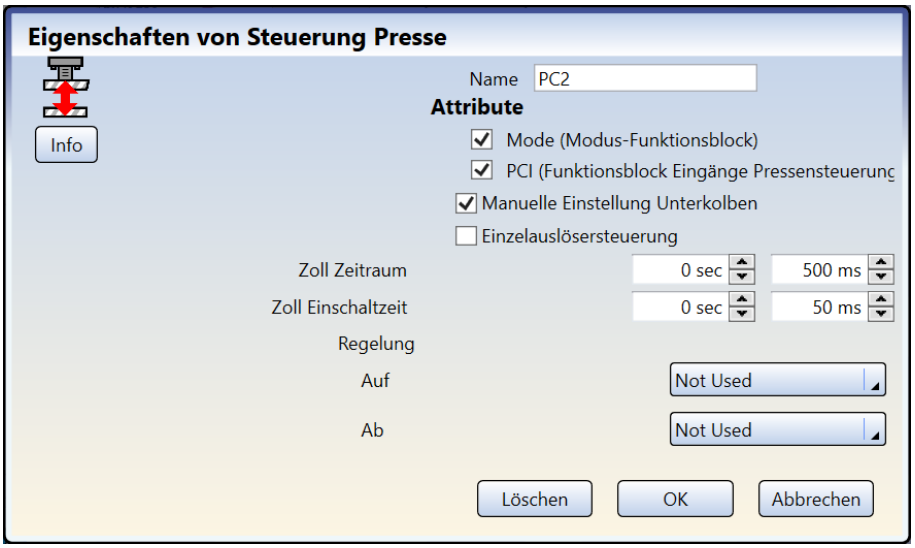

So erstellen Sie die Konfiguration für diese Anwendung:

1. Klicken Sie auf **Neues Projekt**.
2. Legen Sie die Projekteinstellungen fest.
   Siehe Projekteinstellungen auf Seite 99.
3. Wählen Sie das gewünschte Basiskontroller-Modell aus.
   Siehe Registerkarte Geräte auf Seite 100 (für diese Konfiguration muss nur **Is Expandable (Ist erweiterbar)** ausgewählt werden).
4. Erweiterungsmodul XS2so hinzufügen.
   a) Klicken Sie rechts neben dem Basiskontroller auf ✚.
   b) Klicken Sie auf **Output Modules (Ausgangsmodule)**.
   c) Wählen Sie XS2so.
5. Fügen Sie die folgenden Eingänge hinzu und ändern Sie bei Bedarf den Namen und den Schaltungstyp.

| Eingang | Anzahl | Typ | Anschlüsse | Schaltung |
|---|---|---|---|---|
| Zweihandsteuerung | 1 | Sicherheitseingang | IN9, IN10 | Zweikanalig, pnp |
| TOS (ein/aus) | 1 | Nicht sicherheitsrelevant | IN1 | Einkanalig, 1 Anschluss |
| BOS (ein/aus) | 1 | Nicht sicherheitsrelevant | IN2 | Einkanalig, 1 Anschluss |
| Manueller Reset | 1 | Nicht sicherheitsrelevant | IN11 | Einkanalig, 1 Anschluss |
| Nothaltschalter | 1 | Sicherheitseingang | IO1, IN3, IN4 | Zweikanalig, 3 Anschlüsse |
| Betrieb (ein/aus) | 1 | Nicht sicherheitsrelevant | IN12 | Einkanalig, 1 Anschluss |
| Aufwärts (ein/aus) | 1 | Nicht sicherheitsrelevant | IN13 | Einkanalig, 1 Anschluss |
| Abwärts (ein/aus) | 1 | Nicht sicherheitsrelevant | IN14 | Einkanalig, 1 Anschluss |
| PIP (ein/aus) | 1 | Nicht sicherheitsrelevant | IN5 | Einkanalig, 1 Anschluss |
| Steuerung SQS Presse | 1 | Sicherheitseingang | IN6 | Einkanalig, 1 Anschluss |
| Fußpedal | 1 | Sicherheitseingang | IO2 | Einkanalig, 1 Anschluss |
| Muting-Sensor der Pressensteuerung | 1 | Sicherheitseingang | IO3 | Einkanalig, 1 Anschluss |
| Optosensor | 1 | Sicherheitseingang | IN7, IN8 | Zweikanalig, pnp |

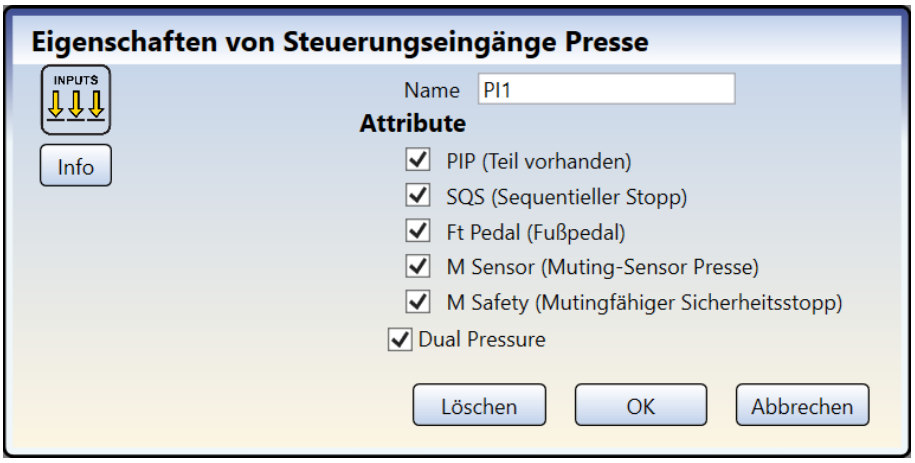
6. Öffnen Sie die Registerkarte **Funktionsansicht**.
7. Fügen Sie den Pressensteuerungs-Funktionsblock hinzu und konfigurieren Sie ihn.
   a) Klicken Sie im mittleren Bereich der Registerkarte **Functional View (Funktionsansicht)** auf einen leeren Platzhalter. Für weitere Informationen siehe Funktionsblöcke auf Seite 105.
   b) Wählen Sie **Function Blocks (Funktionsblöcke)** und dann **Press Control (Pressensteuerung)** aus.
   c) Wählen Sie im Fenster **Press Control Properties (Eigenschaften der Pressensteuerung)** die Option **Mode (Mode Function Block) (Modus [Modus-Funktionsblock])** und **PCI (Press Control Input Function Block) (PCI [Funktionsblock Pressensteuerungseingang])** aus. Lassen Sie das Kontrollkästchen **Manual Upstroke Setting (Manuelle Einstellung Aufwärtshub)** aktiviert.

*Abbildung 65. **Eigenschaften der Pressensteuerung***




   d) Auf **OK** klicken.
   Das Fenster **Press Control Inputs Properties (Eigenschaften der Pressensteuerungseingänge)** wird geöffnet.

*Abbildung 66. **Eigenschaften der Pressensteuerungseingänge***




   e) Markieren Sie alle Kontrollkästchen. Beachten Sie, dass bei Auswahl von **SQS** drei weitere Optionen angezeigt werden; wählen Sie diese ebenfalls aus (alle sechs Kästchen sollten aktiviert sein).
   f) Auf **OK** klicken.
   Das Fenster **Mode Properties (Modus-Eigenschaften)** wird angezeigt.
   g) Auf **OK** klicken.
8. Folgendes mit dem Moduswahlblock verbinden:
   - Eingang Betrieb mit dem Eingangsknoten Betrieb
   - Aufwärts-Eingang mit dem Schrittsteuerung-Aufwärts-Eingangsknoten
   - Abwärts-Eingang mit dem Schrittsteuerung-Abwärts-Eingangsknoten
9. Verbinden Sie Folgendes mit dem Pressensteuerungseingangsblock:
   - PIP-Eingang (Part-in-Place) mit dem PIP-Eingangsknoten
   - SQS-Eingang (sequenzieller Stopp) mit dem SQS-Eingangsknoten
   - Fußpedal-Eingang mit dem Fußpedal-Eingangsknoten
   - Muting-Sensor der Pressensteuerung (PCMS) mit dem M-Sensor-Eingangsknoten
   - Optischen Sensor mit dem M-Sicherheitseingangsknoten
10. Verbinden Sie Folgendes mit dem Pressensteuerungsblock:

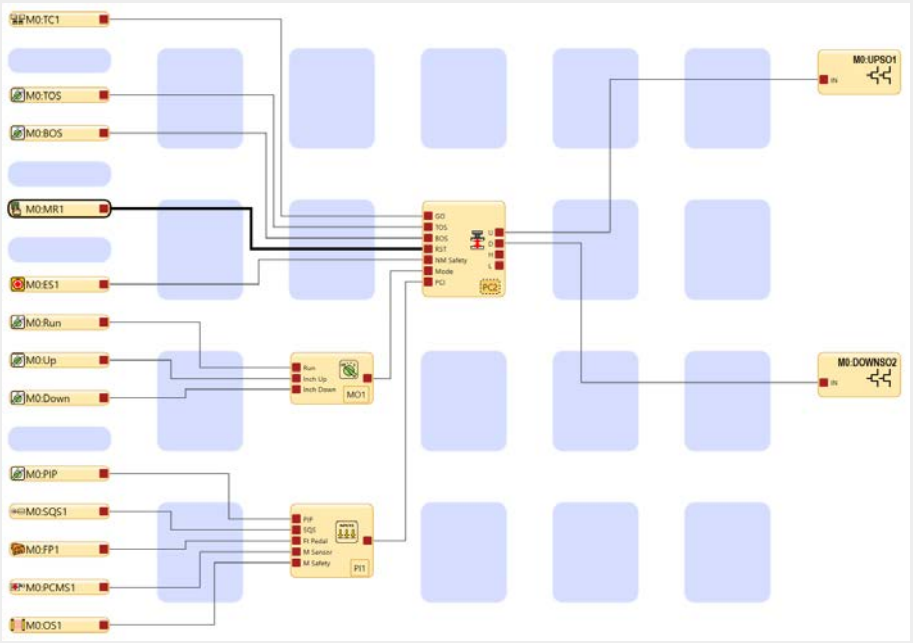
- Zweihandsteuerungseingang mit dem GO-Eingangsknoten
- TOS mit dem TOS-Eingangsknoten
- BOS mit dem BOS-Eingangsknoten
- Manuellen Reset mit dem RST-Eingangsknoten
- Nothaltschalter mit dem NM-Sicherheitseingangsknoten

11. Verbinden Sie den U-Ausgangsknoten des Funktionsblocks der Pressensteuerung mit SO1 (ändern Sie den Namen von SO1 in „UPSO1“).
12. Verbinden Sie den D-Ausgangsknoten des Funktionsblocks der Pressensteuerung mit SO2 (ändern Sie den Namen von SO2 in „DOWNSO2“).
13. Gehen Sie zu Seite 2 der Registerkarte „Funktionsansicht“ (verwenden Sie den Pfeil in der oberen rechten Ecke).
14. Legen Sie einen Referenzknoten für PCx-H und einen weiteren für PCx-L an.
15. Verbinden Sie PCx-H mit SO1 (ändern Sie den Namen von SO1 in „HIGHSO1“).
16. Verbinden Sie PCx-L mit SO2 (ändern Sie den Namen von SO2 in „LOWSO2“).

Die Beispielkonfiguration ist abgeschlossen.

**Anmerkung:** An diesem Punkt kann es hilfreich sein, die Blöcke in der **Funktionsansicht** für einen besseren Konfigurationsfluss neu zu positionieren, wie in der folgenden Abbildung dargestellt.

*Abbildung 67. **Funktionsblock-Position***




## XS/SC26-2: Simulieren der Funktionalität der Konfiguration für die vollfunktionale Pressensteuerung

Im Folgenden wird beschrieben, wie die Funktionalität dieser Pressensteuerungskonfiguration simuliert wird:

1. Klicken Sie auf , um den Simulationsmodus aufzurufen.
2. Klicken Sie auf **Play (Wiedergabe)**, um den Simulationstimer einzuschalten (ähnlich wie beim Einschalten der Maschine).
3. Klicken Sie auf die Eingänge für Nothaltschalter, optischen Sensor, TOS und Betrieb für den Ein-Zustand (grün).
4. Klicken Sie auf den MR1-Reset-Eingang.
   Der Pressensteuerungs-Funktionsblock und der LOWSO2-Ausgang sollten in den Ein-Zustand (grün) wechseln. Dies ist auf Seite 2; klicken Sie auf den Pfeil oben rechts, um die Seiten zu wechseln.
5. Versetzen Sie den PIP-Eingang mit einem Klick in den Ein-Zustand (grün).
6. Versetzen Sie den TC1-Eingang mit einem Klick in den Ein-Zustand (grün).
   Der DOWNSO2-Ausgang wird eingeschaltet (grün).
7. Versetzen Sie den TOS-Eingang mit einem Klick in den Aus-Zustand (rot).
8. Versetzen Sie den SQS1- und den PCMS1-Eingang mit einem Klick in den Ein-Zustand (grün).
   Der Ausgang DOWNSO2 schaltet sich aus (rot), der Ausgang LOWSO2 schaltet sich aus (rot) und der Ausgang HIGHSO1 (Seite 2) schaltet sich ein (grün).
9. Versetzen Sie den TC1-Eingang mit einem Klick in den Aus-Zustand (rot).

10. Versetzen Sie den FP1-Eingang mit einem Klick in den Ein-Zustand (grün).
    Der DOWNSO2-Ausgang wird eingeschaltet (grün).
11. Versetzen Sie den BOS-Eingang mit einem Klick in den Ein-Zustand (grün).
    Der Ausgang DOWNSO2 und der Ausgang HIGHSO1 (Seite 2) schalten sich aus (rot) und der Ausgang LOW-SO2 (Seite 2) schaltet sich ein (grün).
12. Versetzen Sie den FP1-Eingang mit einem Klick in den Aus-Zustand (rot).
13. Versetzen Sie den TC1-Eingang mit einem Klick in den Ein-Zustand (grün).
    Der UPSO1-Ausgang wird eingeschaltet (grün).
14. Versetzen Sie die Eingänge BOS, PCMS1 und SQS1 mit einem Klick in den Aus-Zustand (rot).
15. Versetzen Sie den TOS-Eingang mit einem Klick in den Ein-Zustand (grün).
    Der UPSO1-Ausgang schaltet sich aus (rot).
16. Versetzen Sie den TC1-Eingang mit einem Klick in den Aus-Zustand (rot).
17. Versetzen Sie den optischen Sensoreingang mit einem Klick in den Aus-Zustand (rot), versetzen Sie den PIP-Eingang mit einem Klick in den Aus-Zustand (rot) und dann zurück in den Ein-Zustand (grün) und versetzen Sie dann den optischen Sensoreingang mit einem Klick zurück in den Ein-Zustand (grün).

Das System ist bereit, den nächsten Zyklus zu starten, indem der TC1-Eingang wieder in den Ein-Zustand (grün) geschaltet wird.

Wenn der TC1-Eingang während des Abwärtshubs ausgeschaltet (rot) ist, wird der Abwärtshub durch erneutes Einschalten des Eingangs nicht verändert; die Presse fährt mit dem Abwärtshub fort. Um die Presse nach dem Ausschalten des TC1-Eingangs nach oben (statt nach unten) zu bewegen, klicken Sie auf den MR1-Eingang und schalten Sie dann den TC1-Eingang wieder ein. Wenn der optische Sensor oder der Nothaltschalter während des Aufwärts- oder Abwärtshubs ausgeschaltet wird, sollte der TC1-Eingang ausgeschaltet und der MR1-Eingang durchgeschaltet werden, und durch die Aktivierung von TC1 schaltet sich dann der UPSO1-Ausgang ein.

# 9 Software

Die Software für den Sicherheitskontroller von Banner ist eine Anwendung mit Echtzeit-Display und Diagnosewerkzeugen, über die Sie folgende Aufgaben ausführen können:

- Erstellen und Bearbeiten von Konfigurationen
- Testen einer Konfiguration im Simulationsmodus
- Schreiben einer Konfiguration auf den Sicherheitskontroller
- Lesen der aktuellen Konfiguration vom Sicherheitskontroller
- Anzeigen von Echtzeitinformationen, z. B. zum Gerätestatus
- Anzeigen von Fehlerinformationen

Die Software verwendet Symbole und Schaltungssymbole, mit denen Sie die geeigneten Eingangsgeräte und Eigenschaften auswählen können. Während die diversen Geräteeigenschaften und E/A-Steuerungsbeziehungen auf der Registerkarte **Funktionsansicht** konfiguriert werden, erstellt das Programm automatisch die entsprechenden Schalt- und Kontaktpläne.

Unter Erstellen einer Konfiguration auf Seite 78 finden Sie Informationen zum Konfigurationserstellungsprozess. Unter XS/SC26-2 Beispielkonfiguration auf Seite 85 finden Sie ein Beispiel für den Konfigurationserstellungsprozess.

Unter Registerkarte Schaltplan auf Seite 105 finden Sie Informationen zum Verbinden von Geräten sowie Registerkarte Kontaktplan auf Seite 107 die Darstellung der Kontaktpläne der Konfiguration.

Unter Livemodus auf Seite 120 finden Sie Laufzeitinformationen zum Sicherheitskontroller.

## 9.1 Abkürzungen

| Abkürzung [12] | Beschreibung |
|---|---|
| **AVM** | Eingangsknoten für einstellbare Ventilüberwachung der Sicherheitsausgänge |
| **AVMx** | Eingang für einstellbare Ventilüberwachung |
| **BP** | Eingangsknoten für Überbrückung bei den Überbrückungsblöcken und Muting-Blöcken |
| **BPx** | Überbrückungsschalter-Eingang |
| **BOS** | Bottom-of-Stroke-Eingangsknoten der Pressensteuerungsblöcke (nur XS/SC26-2) |
| **CD** | Eingangsknoten für Abbruchverzögerung der Sicherheitsausgänge, Verzögerungsblöcke und One-Shot-Blöcke |
| **CDx** | Eingang für Abbruchverzögerung |
| **CSx** | Eingang für Zyklusinitiierung |
| **ED** | Eingangsknoten für Zustimmtaster der Zustimmtaster-Blöcke |
| **EDx** | Zustimmtaster-Eingang |
| **EDM** | Eingangsknoten für externe Geräteüberwachung der Sicherheitsausgänge |
| **EDMx** | Eingang für externe Geräteüberwachung |
| **ES** | Eingangsknoten für Not-Aus-Schalter der Zustimmtaster-Blöcke |
| **ESx** | Eingang für Not-Aus-Schalter |
| **ETB** | Externer Klemmenblock (nur SC10-2) |
| **FID** | Merkmalkennzeichnung |
| **FPx** | Fußpedal-Eingang |
| **FR** | Eingangsknoten für Fehler-Reset der Sicherheitsausgänge |
| **Ft-Pedal** | Fußpedal-Eingangsknoten der Pressensteuerungsblöcke (nur XS/SC26-2) |
| **GO** | Zyklus-Start-Eingangsknoten der Pressensteuerungsblöcke (nur XS/SC26-2) |
| **GSx** | Schutztürschalter-Eingang |
| **Weiterschalten** | Eingangsknoten für Weiterschalten der Zustimmtaster-Blöcke |
| **IN** | Normaler Eingangsknoten der Funktionsblöcke und Sicherheitsausgangsblöcke |
| **ISD** | ISD (In-Series Diagnostics) |
| **LR** | Eingangsknoten für Latch-Reset des Latch-Reset-Blocks und der Sicherheitsausgänge |
| **ME** | Eingangsknoten für Muting-Freigabe der Muting-Blöcke und der Zweihandsteuerungsblöcke |

[12] Die Endung „x“ bezeichnet die automatisch zugewiesene Nummer.

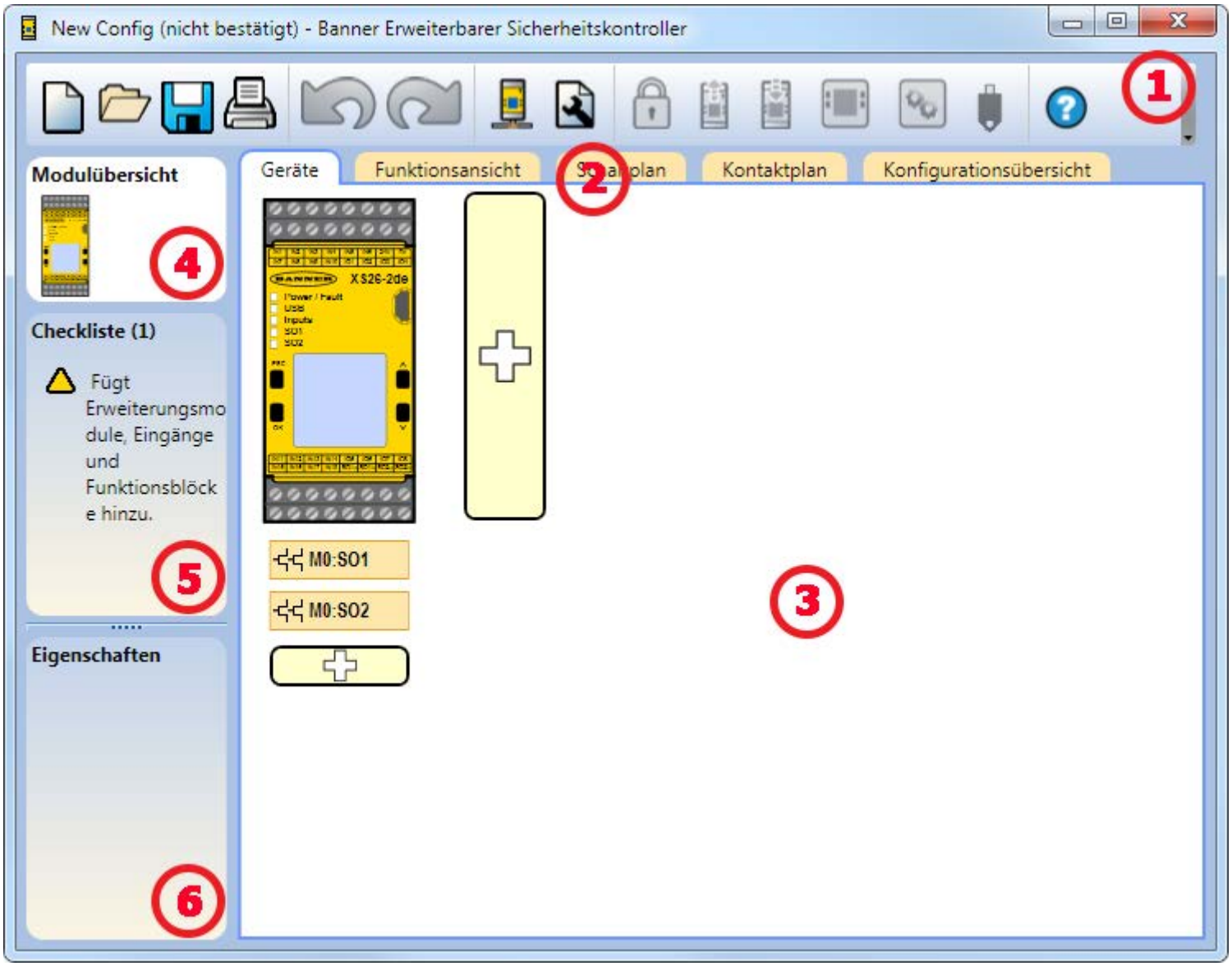
| Abkürzung [12] | Beschreibung |
|---|---|
| **MEx** | Eingang für Muting-Freigabe |
| **MP1** | Eingangsknoten für das erste Muting-Sensorpaar in Muting-Blöcken und Zweihandsteuerungsblöcken |
| **MP2** | Eingangsknoten für das zweite Muting-Sensorpaar (nur Muting-Blöcke) |
| **M-Sicherheit** | Mutingfähiger Sicherheitseingangsknoten der Pressensteuerungsblöcke (nur XS/SC26-2) |
| **M-Sensor** | Muting-Sensor-Eingangsknoten der Pressensteuerungsblöcke (nur XS/SC26-2) |
| **Mx** | Basiskontroller- und Erweiterungsmodule (in der Reihenfolge, in der sie auf der Registerkarte **Geräte** aufgeführt sind) |
| **MRx** | Manueller Reset-Eingang |
| **MSPx** | Muting-Sensorpaar-Eingang |
| **NM-Sicherheit** | Nicht mutingfähiger Sicherheitseingangsknoten der Pressensteuerungsblöcke (nur XS/SC26-2) |
| **ONx** | Eingang für EIN/AUS |
| **OSx** | Optosensor-Eingang |
| **PCMSx** | Muting-Sensor-Eingang der Pressensteuerung |
| **PIP** | Part-in-Place-Eingangsknoten der Pressensteuerungsblöcke (nur XS/SC26-2) |
| **PSx** | Schutzhalt-Eingang |
| **RE** | Eingangsknoten für Reset-Aktivierung der Latch-Reset-Blöcke und der Sicherheitsausgänge |
| **ROx** | Relaisausgang |
| **RPI** | Gefordertes Paketintervall |
| **RPx** | Seilzugschalter-Eingang |
| **RST** | Reset-Knoten für SR Flip-Flop, RS Flip-Flop, Latch-Reset-Blöcke, Pressensteuerungsblöcke und Zustimmtaster-Blöcke |
| **BETRIEB** | Eingangsknoten des Standardbetriebsmodus (RUN) der Blöcke für den Pressensteuerungsmodus (nur XS/SC26-2) |
| **SET** | Einstellknoten der SR- und RS-Flip-Flop-Blöcke |
| **SMx** | Eingang für Sicherheitsmatten |
| **SOx** | Sicherheitsausgang |
| **SQS** | Eingangsknoten für den sequenziellen Stopp der Pressensteuerungsblöcke (nur XS/SC26-2) |
| **SQSx** | Eingang für den sequenziellen Stopp (SQS) der Pressensteuerung |
| **STATx** | Statusausgang |
| **GE** | Eingangsknoten für Zweihandsteuerung der Zweihandsteuerungsblöcke |
| **TCx** | Zweihandsteuerungseingang |
| **TOS** | Top-of-Stroke-Eingangsknoten der Pressensteuerungsblöcke (nur XS/SC26-2) |

[12] Die Endung „x“ bezeichnet die automatisch zugewiesene Nummer.

# 9.2 Software-Übersicht

**Anmerkung:** In den folgenden Abschnitten wird der XS/SC26-2 als Beispiel verwendet. Die Benutzeroberfläche des SC10-2 ist ähnlich.

*Abbildung 68. Software für den Sicherheitskontroller von Banner*



### (1) Symbolleiste „Navigation“


Startet ein **Neues Projekt**


Öffnet ein bestehendes Projekt, öffnet eines der **Zuletzt bearbeitet**en Projekte oder öffnet **Beispielprojekte**


Speichert das Projekt unter dem benutzerdefinierten Pfad.


Druckt eine anpassbare Konfigurationsübersicht.


Macht bis zu zehn vorher ausgeführte Aktionen rückgängig.


Stellt bis zu zehn zuvor rückgängig gemachte Aktionen wieder her.


Zeigt die Netzwerkeinstellungen an und schreibt diese in den Sicherheitskontroller.


Zeigt Projekteinstellungen an.


Öffnet den Passwort-Manager.


Liest die Daten, wie z. B. Fehlerprotokoll, Konfigurationsdaten, Netzwerkeinstellungen und Geräteinformationen, vom Sicherheitskontroller.


Schreibt die Daten, wie z. B. Konfigurationsdaten Einstellungen, auf den Sicherheitskontroller.


Macht die Livemodus-Ansicht verfügbar.


Macht die Simulationsmodus-Ansicht verfügbar.


Gibt die SC-XM2- bzw. SC-XM3-Laufwerksverbindung an.


Öffnet die **Hilfe**-Optionen

- **Hilfe**: Öffnet die Hilfethemen.
- **Über**: Zeigt die Versionsnummer der Software und den Warnhinweis zu den Pflichten des Benutzers an.
- **Versionshinweise**: Zeigt die Versionshinweise für die einzelnen Softwareversionen an.
- **Symbole**: Schaltet zwischen den Symbolen im US-amerikanischen und europäischen Format hin und her.
- **Support-Informationen**: Beschreibt, wie Sie bei der Advanced Technical Support Group von Banner Hilfe anfordern können.
- **Sprache**: Dient zur Auswahl der Sprachoptionen für die Software.

### (2) Registerkarten für Arbeitsblätter und Diagramme

**Geräte**: Zeigt eine bearbeitbare Ansicht aller verbundenen Geräte an.

**Funktionsansicht**: Liefert die bearbeitbare Symboldarstellung der Steuerungslogik.

**Schaltplan**: Zeigt die Verdrahtungsdetails für das E/A-Gerät zur Verwendung durch den Installateur an.

**Kontaktplanlogik**: Zeigt eine symbolische Darstellung der Schutzlogik des Sicherheitskontrollers zur Verwendung durch den Maschinenkonstrukteur oder den Steuerungstechniker an.

**Industrie-Ethernet** (sofern aktiviert): Zeigt die bearbeitbaren Netzwerkkonfigurationsoptionen an.

**Konfigurationsübersicht**: Zeigt eine detaillierte Konfigurationsübersicht an.

**Livemodus** (sofern aktiviert): Zeigt die Livemodus-Daten an, einschließlich aktueller Fehler.

**Simulationsmodus** (sofern aktiviert): Zeigt die Daten des Simulationsmodus an.

**ISD** (SC10-2 ab FID 2): Zeigt die ISD-Reihe an.

### (3) Ausgewählte Ansicht

Zeigt die Ansicht an, die der ausgewählten Registerkarte entspricht (die Abbildung zeigt die Ansicht **Geräte**).

### (4) Modulübersicht

Zeigt den Basiskontroller und alle angeschlossenen Module an oder zeigt den SC10-2 an.

### (5) Checkliste

Enthält Aktionselemente für die Konfiguration des Systems und für die Behebung von Fehlern, um die Konfiguration erfolgreich abzuschließen.

### (6) Eigenschaften

Zeigt die Eigenschaften des ausgewählten Geräts, Funktionsblocks oder der ausgewählten Verbindung an (die Eigenschaften können in dieser Ansicht nicht bearbeitet werden; klicken Sie unten auf **Bearbeiten**, um Änderungen vorzunehmen).

**Löschen**: Löscht das markierte Element.

**Bearbeiten**: Zeigt die Konfigurationsoptionen für das ausgewählte Gerät oder den ausgewählten Funktionsblock an.

Informationen zu Problemen im Zusammenhang mit den Funktionen der Software finden Sie unter Software: Fehlerbehebung auf Seite 278.

# 9.3 Neues Projekt

Klicken Sie auf **New Project (Neues Projekt)**, um den gewünschten Kontroller auszuwählen und den Bildschirm **Start a New Project (Neues Projekt starten)** zu öffnen. Dieser Bildschirm enthält Projektinformationen, die nur beim erstmaligen Anlegen eines Projekts verfügbar sind. Diese sind nicht über den Bildschirm **Project Settings (Projekteinstellungen)** verfügbar.

## XS/SC26-2

Alle Ankreuzfelder sind standardmäßig markiert.

**Hat Display**
Aktivieren Sie dieses Kontrollkästchen, wenn Ihr Kontroller über ein integriertes Display verfügt.

**Verfügt über Industrie-Ethernet**
Aktivieren Sie dieses Kontrollkästchen, wenn Ihr Kontroller über Industrie-Ethernet verfügt.

**Ist erweiterbar**
Aktivieren Sie dieses Kontrollkästchen, wenn Ihr Kontroller ein XS26-2 ist. Deaktivieren Sie dieses Kontrollkästchen, wenn Ihr Kontroller ein SC26-2 ist.

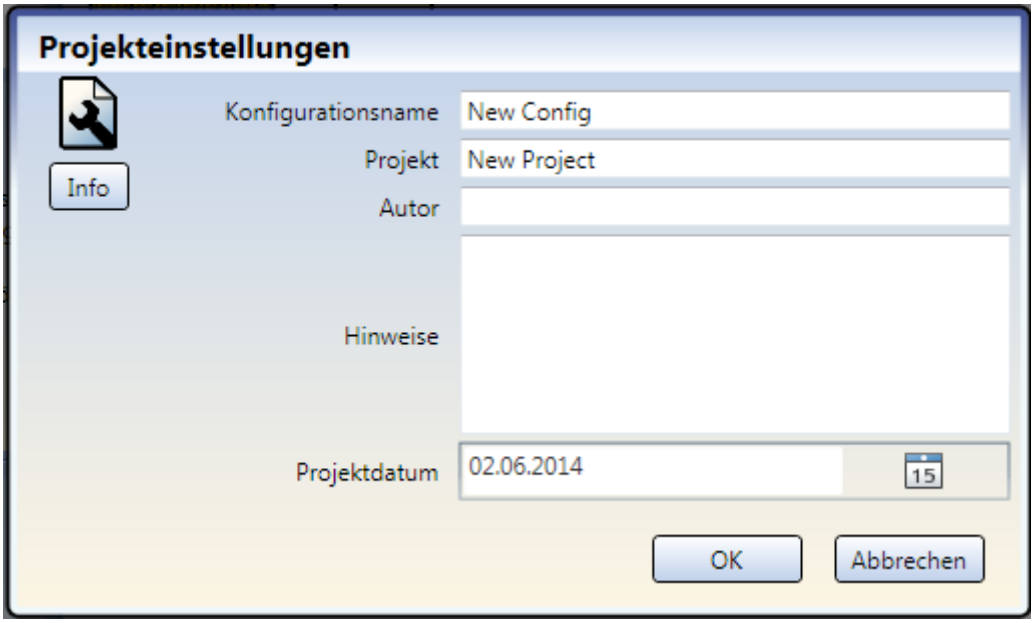
## SC10-2

**Funktion für die automatische Optimierung von Anschlüssen deaktivieren (nur SC10-2)**
Aktiviert bzw. deaktiviert die automatische Optimierung von Anschlüssen, mit der sich die Anzahl der Eingänge unter Verwendung eines externen Klemmenblocks (ETB) erweitern lässt.

**Anmerkung:** Die oben aufgeführten Projektinformationen sind in den **Project Settings (Projekteinstellungen)** nicht verfügbar, können jedoch über die Funktion **Edit (Bearbeiten)** der **Module Properties (Moduleigenschaften)** bearbeitet werden.

# 9.4 Projekteinstellungen

*Abbildung 69. Projekteinstellungen*




Jede Konfiguration hat eine Option für die Aufnahme weiterer Projektinformationen, damit einfacher zwischen mehreren Konfigurationen unterschieden werden kann. Klicken Sie zum Eingeben dieser Informationen auf **Project Settings (Projekteinstellungen)**.

**Konfigurationsname**
Der Name der Konfiguration. Dieser wird auf dem Sicherheitskontroller angezeigt (bei Ausführungen mit Display) und ist vom Dateinamen verschieden.

**Projekt**
Der Projektname. Dieser ist hilfreich für die Unterscheidung zwischen verschiedenen Anwendungsbereichen.

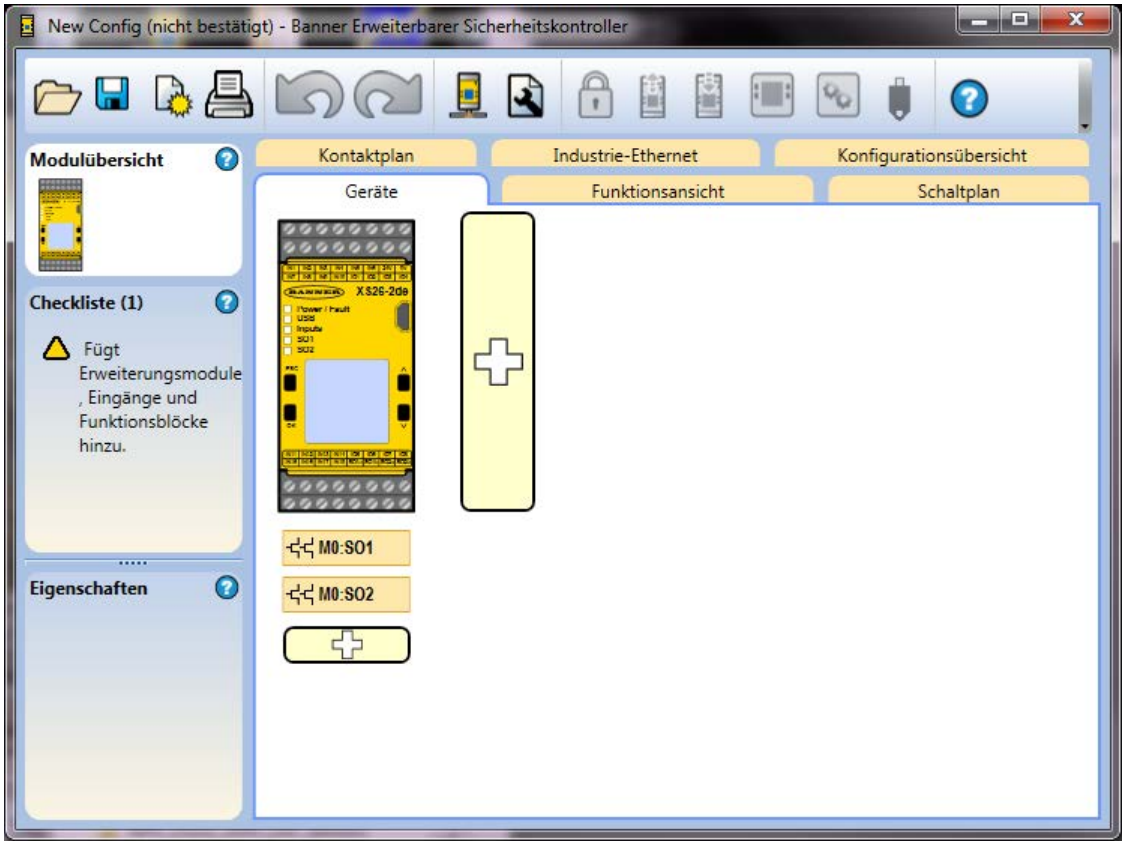
**Autor**
Die Person, die die Konfiguration erstellt.

**Anmerkungen**
Ergänzende Informationen zu dieser Konfiguration oder diesem Projekt.

**Projektdatum**
Das Datum des Projekts.

# 9.5 Registerkarte Geräte

*Abbildung 70. Beispiel: Registerkarte **Geräte** für den XS/SC26-2*




**XS/SC26-2:** Die Registerkarte **Geräte** dient zum Auswählen der Basisausführung, zum Hinzufügen von Erweiterungsmodulen (Eingangs- und Ausgangsmodule) sowie zum Hinzufügen von Eingangsgeräten und Statusausgängen. Fügen Sie die Erweiterungsmodule mit einem Klick auf ✚ rechts vom Basiskontroller-Modul hinzu.

**SC10-2:** Die Registerkarte **Geräte** dient zum Hinzufügen von Eingangsgeräten und Statusausgängen.

Passen Sie das Basiskontroller-Modul oder den SC10-2 an, indem Sie entweder auf das Modul doppelklicken oder es markieren und links unter der Tabelle **Eigenschaften** auf **Bearbeiten** klicken und anschließend die geeigneten Kontrollermerkmale auswählen (Anzeige, Ethernet, Erweiterbarkeit, automatische Optimierung von Anschlüssen). Die Eigenschaften von Sicherheits- und nicht sicherheitsrelevanten Eingängen, Statusausgängen, Logikblöcken und Funktionsblöcken werden ebenfalls konfiguriert, indem Sie entweder auf den betreffenden Block doppelklicken oder diesen markieren und unter der Tabelle **Eigenschaften** auf **Bearbeiten** klicken. Durch erneutes Klicken auf den Block wird die Markierung des Blocks wieder aufgehoben.

*Abbildung 71. Eigenschaften des Moduls XS/SC26-2*

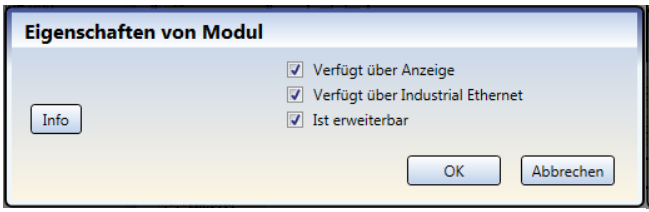
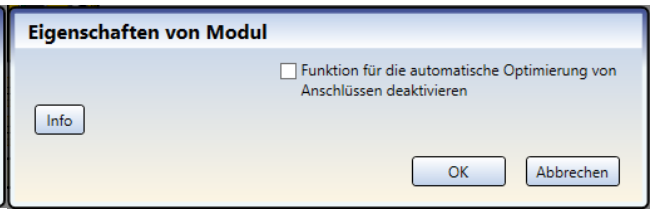
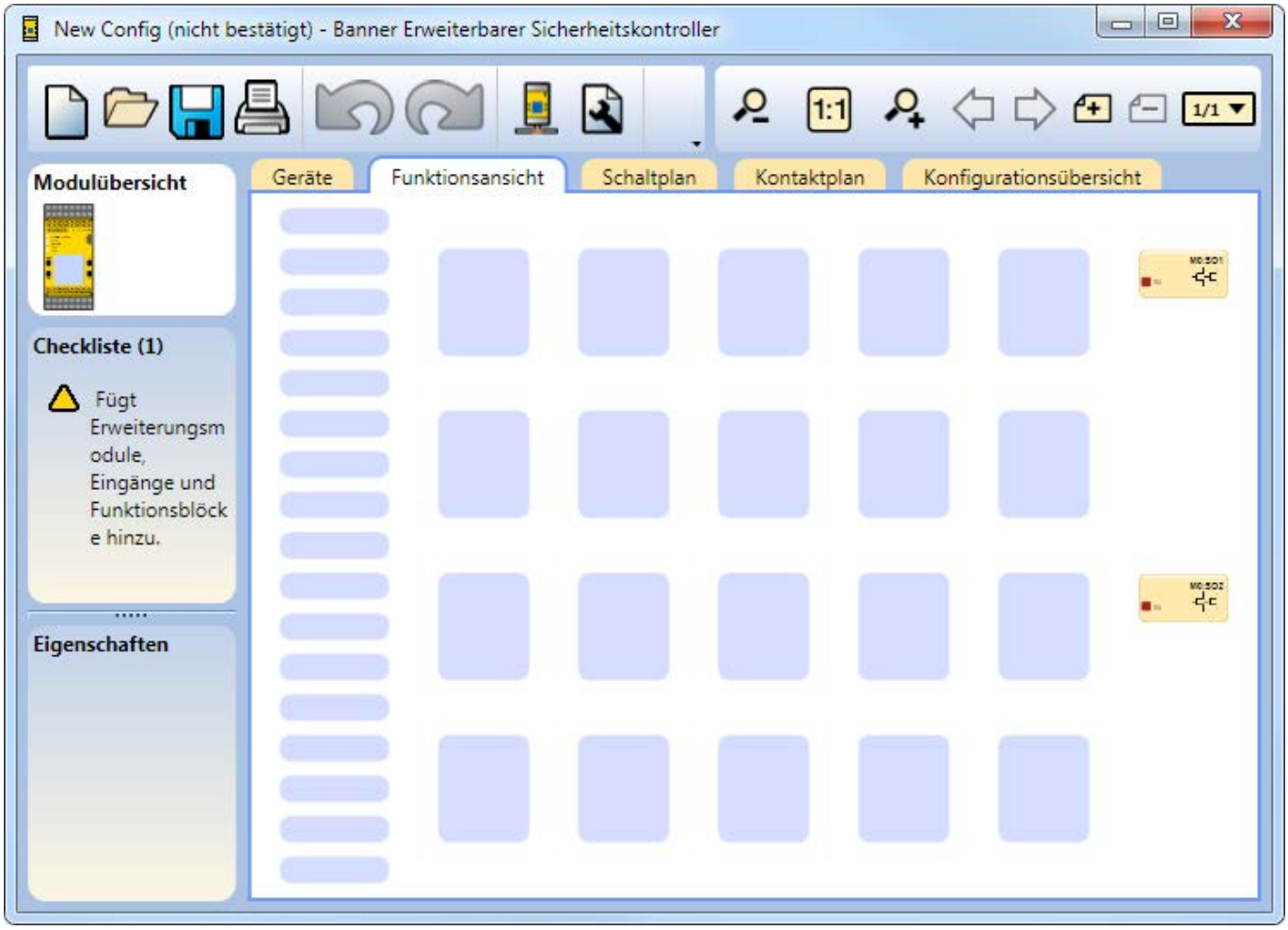



*Abbildung 72. Eigenschaften des Moduls SC10-2*



# 9.6 Registerkarte Funktionsansicht

*Abbildung 73. Registerkarte **Funktionsansicht***




Die Steuerungslogik wird über die Registerkarte **Functional View (Funktionsansicht)** erstellt. Die linke Spalte in der Registerkarte **Functional View (Funktionsansicht)** wird für sicherheits- und nicht sicherheitsrelevante Eingänge verwendet, der mittlere Bereich ist für die Logik- und Funktionsblöcke vorgesehen und die rechte Spalte ist für die Sicherheitsausgänge vorbehalten. Die Sicherheits- und nicht sicherheitsrelevanten Eingänge können zwischen dem linken und mittleren Bereich verschoben werden. Die Funktions- und Logikblöcke können nur innerhalb des mittleren Bereichs verschoben werden. Die Ausgänge werden vom Programm statisch eingefügt und können nicht verschoben werden. Referenzblöcke jeder Art können an einer beliebigen Stelle innerhalb des linken und mittleren Bereichs eingefügt werden.

**Wichtig:** Die Banner-Software für den Sicherheitskontroller von Banner hilft Anwendern beim Erstellen einer gültigen Konfiguration. Dabei ist der Anwender dafür zuständig, die Integrität, Sicherheit und Funktionalität der Konfiguration mithilfe des Inbetriebnahmeprüfung auf Seite 251 zu prüfen.

Auf der Registerkarte **Functional View (Funktionsansicht)** können Sie folgende Vorgänge ausführen:

- Die Darstellung des Diagramms durch Positionsverschiebung von Eingängen, Funktionsblöcken und Logikblöcken anpassen
- Die zuletzt ausgeführten (maximal 10) Aktionen **rückgängig** machen und **wiederherstellen**
- Weitere Seiten für größere Konfigurationen anhand der Werkzeugleiste „Seitennavigation“ hinzufügen (siehe Abbildung 74 auf Seite 101)
- Die Diagrammansicht mit der Zoom-Funktion vergrößern und verkleinern oder sie automatisch an das optimale Seitenverhältnis für die aktuelle Fenstergröße anpassen (siehe Abbildung 74 auf Seite 101)

*Abbildung 74. Werkzeugleiste „Seitennavigation“ und „Diagrammgröße“*




- Durch die Seiten navigieren, indem Sie oben rechts in der Software im Seitennavigationsbereich auf den Links- und Rechtspfeil klicken
- Eigenschaften aller Blöcke entweder durch Doppelklicken auf einen Block oder durch Auswahl eines Blocks und Klicken auf **Bearbeiten** unter der Tabelle **Eigenschaften** bearbeiten

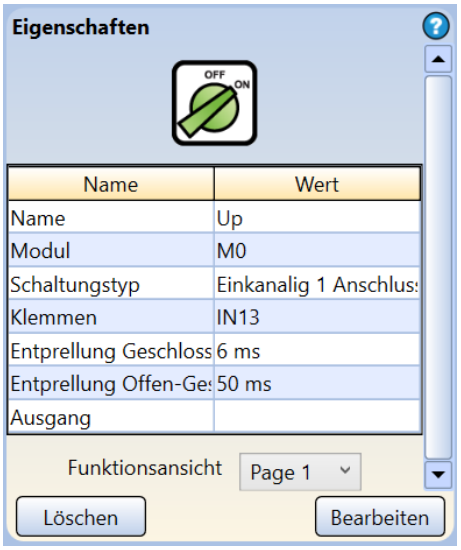
- Einen Block oder eine Verbindung löschen, indem Sie das Element markieren und dann entweder die **Entfernen-Taste** auf der Tastatur drücken oder in der Tabelle **Eigenschaften** auf **Löschen** klicken

**Anmerkung:** Die Löschung des Objekts wird nicht bestätigt. Sie können die Löschung mit einem Klick auf **Rückgängig** rückgängig machen.

Standardmäßig werden alle Eingänge, die über die Registerkarte **Equipment (Geräte)** hinzugefügt werden, in der Registerkarte **Functional View (Funktionsansicht)** auf den ersten verfügbaren Platzhalter in der linken Spalte gesetzt. Es gibt zwei Möglichkeiten, Signale zwischen verschiedenen Seiten zu verschieben. Führen Sie hierzu einen der folgenden Schritte aus:

1. Fügen Sie eine **Referenz** zu dem Block hinzu, der sich auf einer anderen Seite befindet. Klicken Sie hierzu auf einen leeren Platzhalter im mittleren Bereich, wählen Sie **Referenz** und wählen Sie den Block aus, der sich auf der nächsten Seite befindet. Nur Blöcke von anderen Seiten können als **Referenz** hinzugefügt werden.
2. Ordnen Sie die Seite neu zu: Auf der Seite, auf der Sie die Konfiguration beibehalten möchten, verschieben Sie einen der Blöcke an einen Platzhalter im mittleren Bereich. Rufen Sie die Seite aus, die den Block enthält, welcher verschoben werden soll. Wählen Sie den Block aus und ändern Sie die Seitenzuordnung unter der Tabelle **Eigenschaften**.

*Abbildung 75. Tabelle **Properties (Eigenschaften)***




## 9.6.1 Logikblöcke

Logikblöcke dienen zum Erstellen boolescher (wahr oder falsch) funktionaler Beziehungen zwischen Eingängen, Ausgängen und anderen Logik- und Funktionsblöcken. Logikblöcke akzeptieren geeignete Sicherheitseingänge, nicht sicherheitsrelevante Eingänge oder Sicherheitsausgänge als Eingang. Der Status des Ausgangs spiegelt das Ergebnis der booleschen Logik aus der Kombination der Status seiner Eingänge wider (**1** = Ein, **0** = Aus, **x** = Nicht beachten).

**VORSICHT: Invertierte Logik**

Es wird davon abgeraten, invertierte Logikkonfigurationen bei Sicherheitsanwendungen zu verwenden, bei denen eine Gefahrsituation eintreten kann.

Die Signalzustände können durch die Verwendung der Logikblöcke NOT, NAND und NOR umgekehrt werden, oder durch Markieren der Kontrollkästchen für „Ausgang invertieren“ oder „Eingangsquelle invertieren“ (sofern verfügbar). Bei einem Logikblock-Eingang behandelt die invertierte Logik einen Aus-Zustand (0 oder Aus) als „1“ (Wahr oder Ein) und führt dazu, dass sich ein Ausgang einschaltet. Dabei wird angenommen, dass alle Eingänge betätigt wurden. In ähnlicher Weise führt die invertierte Logik auch zu der umgekehrten Funktion eines Ausgangs, wenn der Block „wahr“ wird (der Ausgang schaltet von Ein zu Aus). Da bestimmte Fehlerzustände zum Verlust des Signals führen würden, z. B. unterbrochene Kabelleitungen, Masseschluss oder Kurzschluss zu 0 V, Unterbrechung der Stromzufuhr zur Schutzeinrichtung usw., wird die invertierte Logik in Sicherheitsanwendungen normalerweise nicht verwendet. Eine Gefahrsituation kann eintreten, wenn ein Stoppsignal an einem Sicherheitseingang unterbrochen wird. Dies kann dazu führen, dass sich ein Sicherheitsausgang einschaltet.

## AND


(USA)


(EU)

Der Ausgangswert basiert auf der logischen UND-Beziehung zwischen **2** bis **5** Eingängen.

Der Ausgang ist eingeschaltet, wenn alle Eingänge eingeschaltet sind.

| Eingang 1 | Eingang 2 | Ausgang |
|---|---|---|
| 0 | x | 0 |
| x | 0 | 0 |
| 1 | 1 | 1 |

## OR


(USA)


(EU)

Der Ausgangswert basiert auf der logischen ODER-Beziehung zwischen **2** bis **5** Eingängen.

Der Ausgang ist eingeschaltet, wenn mindestens ein Eingang eingeschaltet ist.

| Eingang 1 | Eingang 2 | Ausgang |
|---|---|---|
| 0 | 0 | 0 |
| 1 | x | 1 |
| x | 1 | 1 |

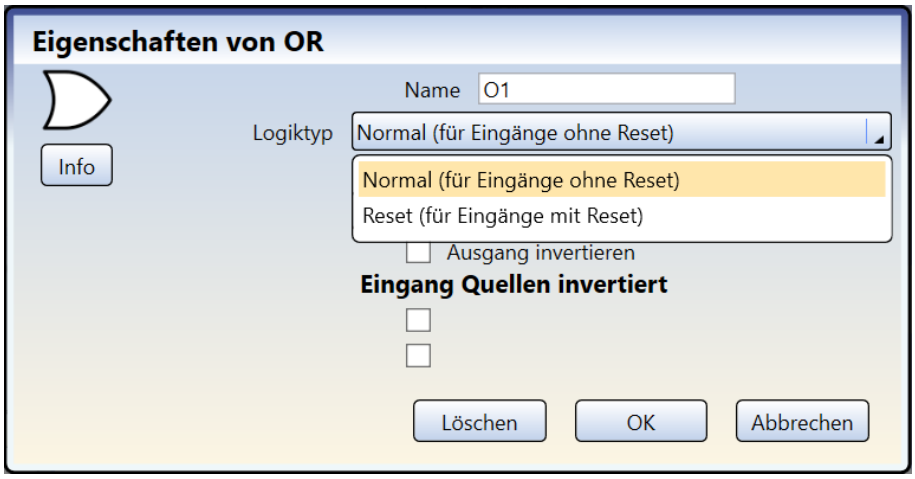
Es gibt zwei Arten von ODER-Logikblöcken: Regulär und Reset.

**ODER-Block vom Typ Reset** Damit mehr als ein Reset die gleiche Reset-Funktion ausführen kann (wie ein fest verdrahteter manueller Reset und ein virtueller manueller Reset), wurde eine Reset-ODER-Blockfunktion geschaffen. Dieser spezielle ODER-Blocktyp akzeptiert nur Reset-Eingänge und kann in der Logik nur wie ein manueller Reset-Eingang angeschlossen werden.

**ODER-Block vom Typ Regulär** Zur Durchführung der ODER-Logik für jede Funktion, die mit einem ODER-Block verbunden werden kann (außer Resets), sollte der Logiktyp Regulär gewählt werden. Dieser Typ ist die Standardeinstellung für den ODER-Logikblock.

Den gewünschten Logiktyp (Regulär oder Reset) wählen Sie über das Menü **Logic Type (Logiktyp)** in den **OR Properties (ODER-Eigenschaften)** aus.

*Abbildung 76. **ODER-Eigenschaften***



## NAND







Der Ausgangswert basiert auf der Umkehr der logischen UND-Beziehung zwischen 2 bis 5 Eingängen.

Der Ausgang ist ausgeschaltet, wenn alle Eingänge eingeschaltet sind.

| Eingang 1 | Eingang 2 | Ausgang |
|---|---|---|
| 0 | x | 1 |
| x | 0 | 1 |
| 1 | 1 | 0 |

## NOR







Der Ausgangswert basiert auf der Umkehr der logischen ODER-Beziehung zwischen 2 bis 5 Eingängen.

Der Ausgang ist eingeschaltet, wenn alle Eingänge ausgeschaltet sind.

| Eingang 1 | Eingang 2 | Ausgang |
|---|---|---|
| 0 | 0 | 1 |
| 1 | x | 0 |
| x | 1 | 0 |

## XOR







Der Ausgangswert ist eine ausschließliche ODER-Beziehung zwischen 2 bis 5 Eingängen.

Der Ausgang ist eingeschaltet, wenn nur ein Eingang (ausschließlich) eingeschaltet ist.

| Eingang 1 | Eingang 2 | Ausgang |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

## NOT







Der Ausgang befindet sich im gegensätzlichen Zustand zum Eingang.

| Eingang | Ausgang |
|---|---|
| 0 | 1 |
| 1 | 0 |

## RS Flip-Flop




Dieser Block ist rücksetzdominant (Reset hat Priorität, wenn beide Eingänge eingeschaltet sind).

| Eingang 1 (Set) | Eingang 2 (Reset) | Ausgang |
|---|---|---|
| 0 | 0 | Wert bleibt gleich |
| 0 | 1 | 0 (Reset) |
| 1 | 0 | 1 (Set) |
| 1 | 1 | 0 (Reset hat Priorität) |

## SR Flip-Flop




Dieser Block ist setzdominant (Set hat Priorität, wenn beide Eingänge eingeschaltet sind).

| Eingang 1 (Set) | Eingang 2 (Reset) | Ausgang |
|---|---|---|
| 0 | 0 | Wert bleibt gleich |
| 0 | 1 | 0 (Reset) |
| 1 | 0 | 1 (Set) |
| 1 | 1 | 1 (Set hat Priorität) |

## 9.6.2 Funktionsblöcke

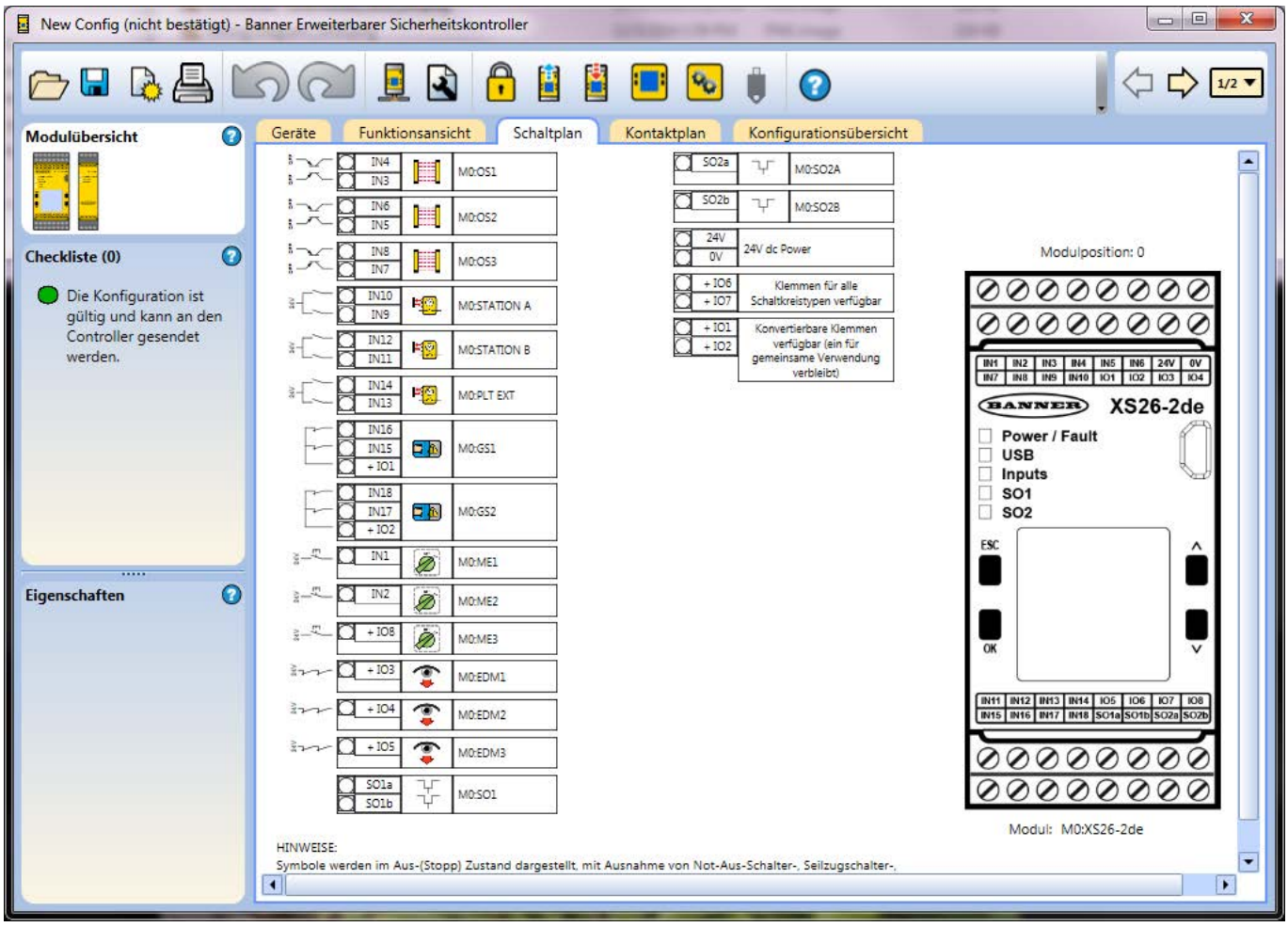
Funktionsblöcke enthalten integrierte Funktionen für die gängigsten Anwendungen in einem Block. Man kann zwar prinzipiell eine Konfiguration ohne Funktionsblöcke erstellen, aber die Verwendung von Funktionsblöcken bietet substanzielle Effizienzvorteile, ist benutzerfreundlicher und zeichnet sich durch höhere Funktionalität aus.

Bei den meisten Funktionsblöcken wird davon ausgegangen, dass das entsprechende Sicherheitseingangsgerät mit ihnen verbunden ist. Die **Checkliste** auf der linken Seite erstellt eine Benachrichtigung, wenn ein obligatorischer Anschluss nicht verbunden wurde. Je nach Anwendung können einige Funktionsblöcke mit anderen Funktionsblöcken und/oder Logikblöcken verbunden werden.

Zweikanalige Sicherheitseingänge haben zwei separate Signalleitungen. Bei manchen Komponenten sind beide zweikanaligen Signale positiv (+ 24 V DC), wenn das Sicherheitseingangsschaltgerät im EIN -Zustand ist. Andere Geräte haben möglicherweise eine antivalente Schaltungsstruktur, bei der ein Kanal 24 V DC und der andere 0 V DC hat, wenn das Eingangsschaltgerät im EIN -Zustand ist. Anstatt ein Sicherheitseingangsgerät als eingeschaltet (z. B. 24 V DC) oder ausgeschaltet (z. B. 0 V DC) zu bezeichnen, werden in diesem Handbuch die Begriffe Ein-Zustand und Aus-Zustand verwendet.

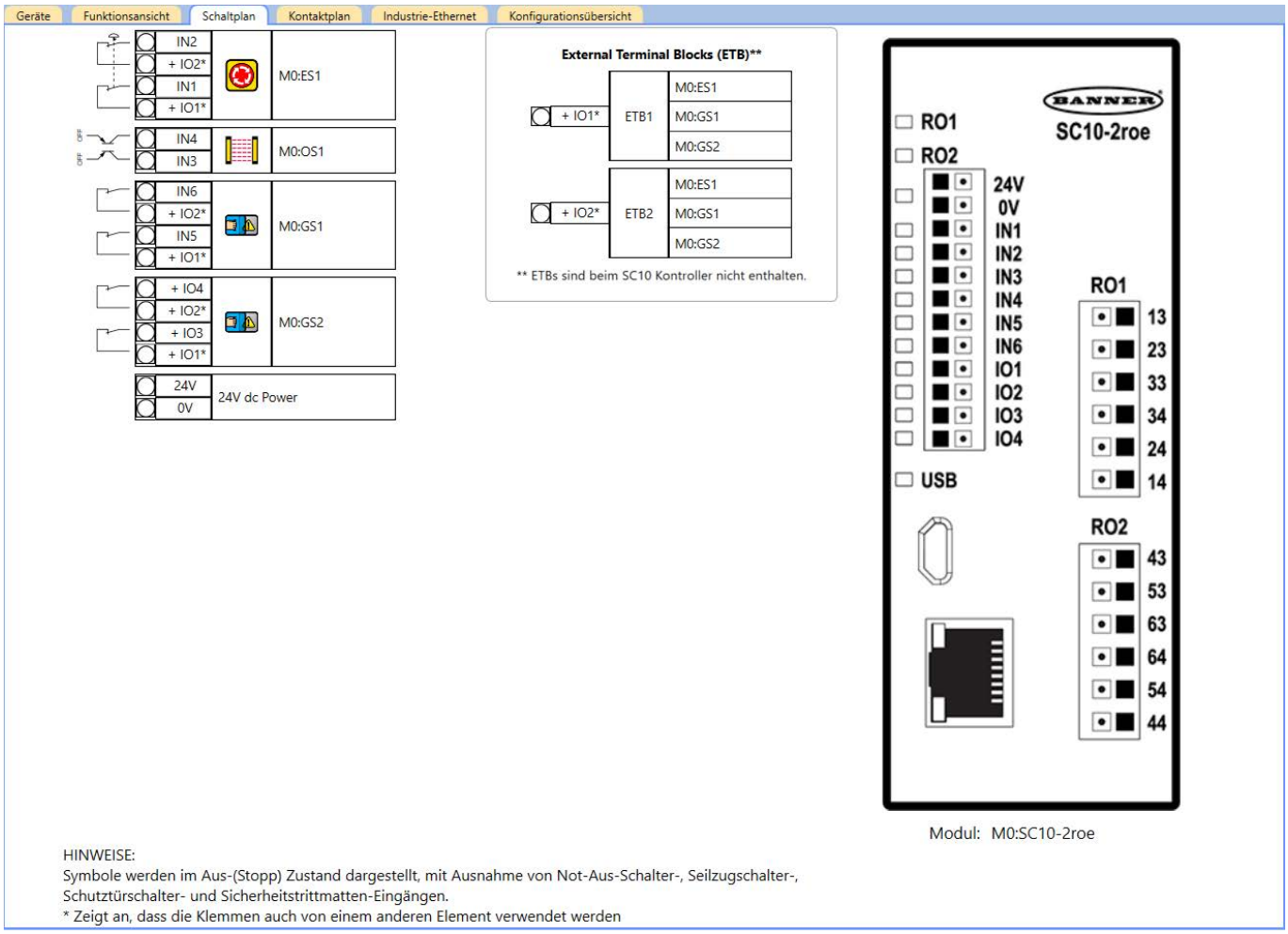
# 9.7 Registerkarte Schaltplan

*Abbildung 77. Registerkarte **Schaltplan**: XS26-2*



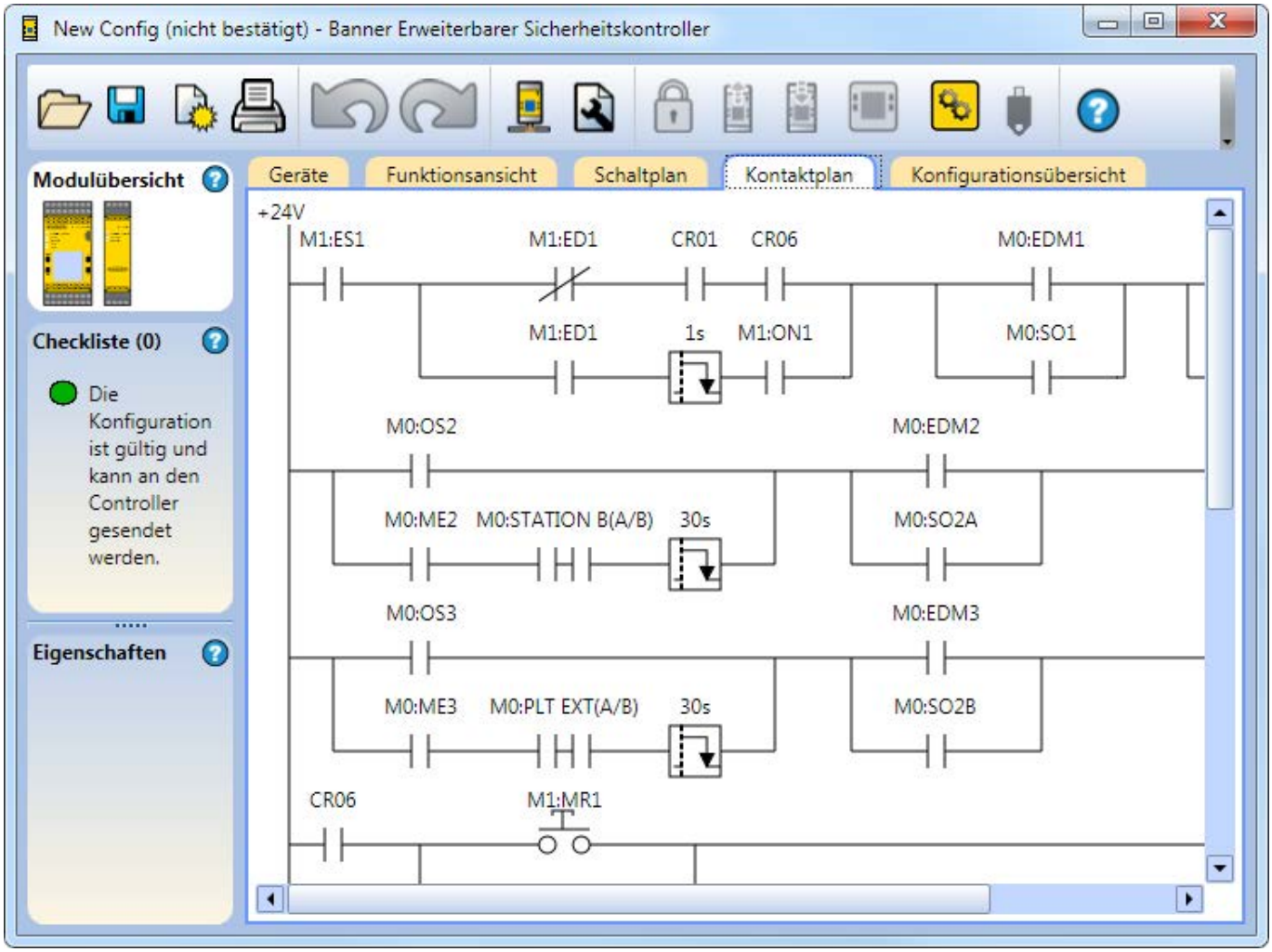

Die Registerkarte **Schaltplan** zeigt die Anschlussbelegungen und die elektrischen Schaltungen für die Sicherheits- und nicht sicherheitsrelevanten Eingänge, Sicherheitsausgänge und Statusausgänge sowie etwaige unbelegte Anschlüsse, die für das ausgewählte Modul zur Verfügung stehen. Verwenden Sie den Schaltplan als Anleitung für die physikalische Verbindung der Geräte. Navigieren Sie zwischen den Modulen anhand der Symbolleiste „Seitennavigation“ oben rechts in der Software.

*Abbildung 78. Registerkarte **Schaltplan**: SC10-2 mit externen Klemmenblöcken*



# 9.8 Registerkarte Kontaktplan

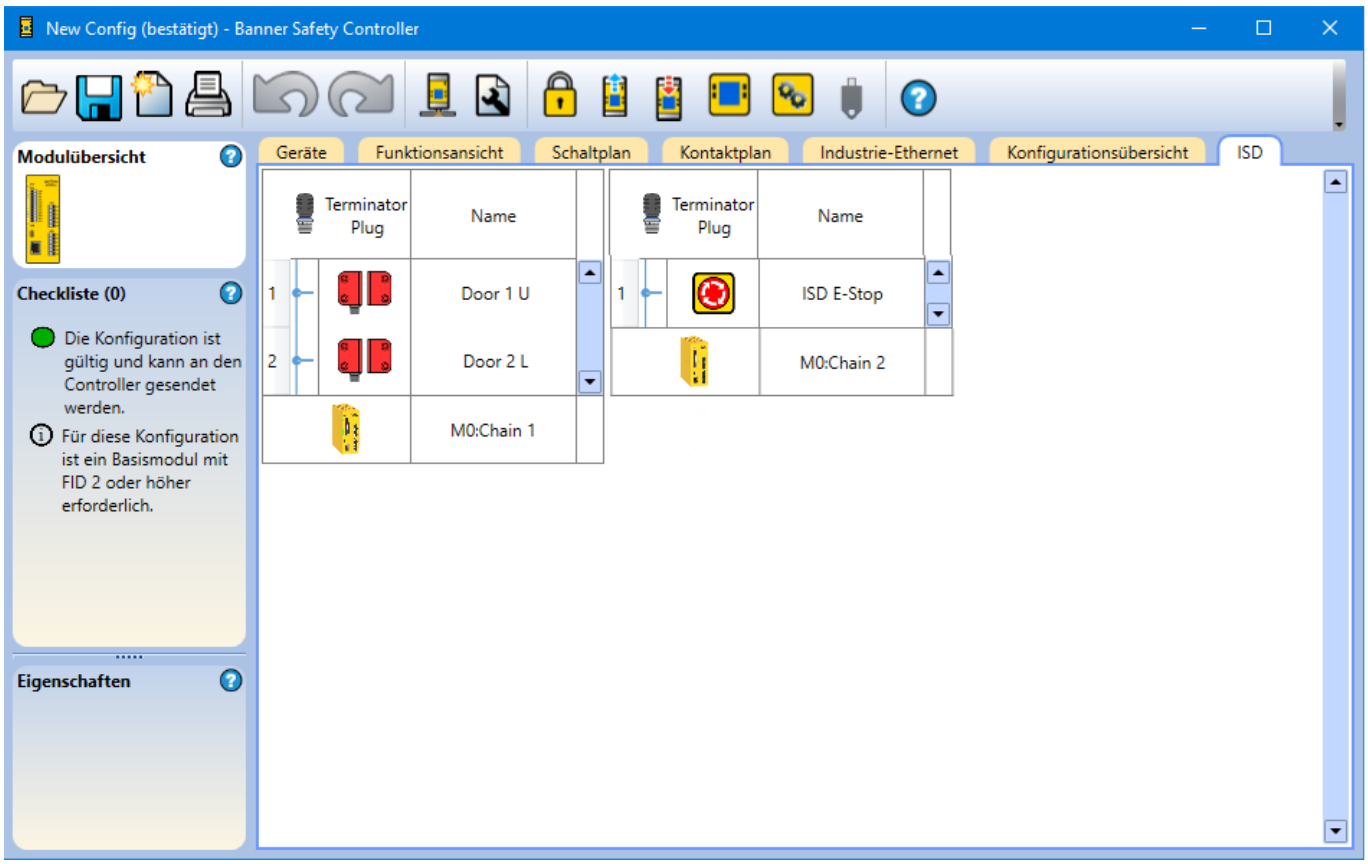
*Abbildung 79. Registerkarte **Kontaktplan***




Die Ansicht **Kontaktplan** zeigt eine vereinfachte Abbildung der Relais-Logik der Konfiguration.

# 9.9 Registerkarte ISD

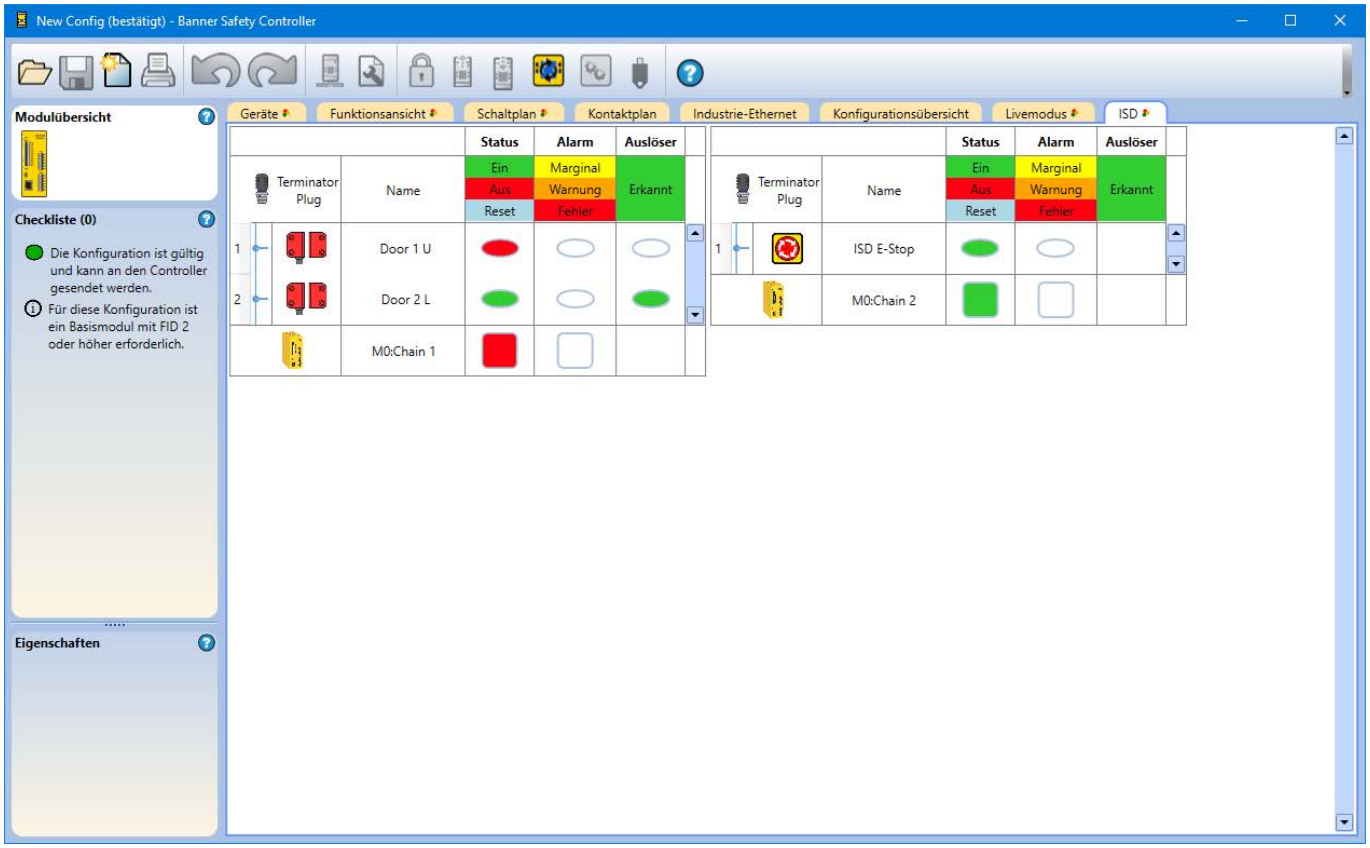
*Abbildung 80. Registerkarte **ISD***




Auf der Registerkarte **ISD** sind die Reihenfolge und die Gerätenamen der angeschlossenen ISD-Geräte in der jeweiligen ISD-Reihe angegeben.

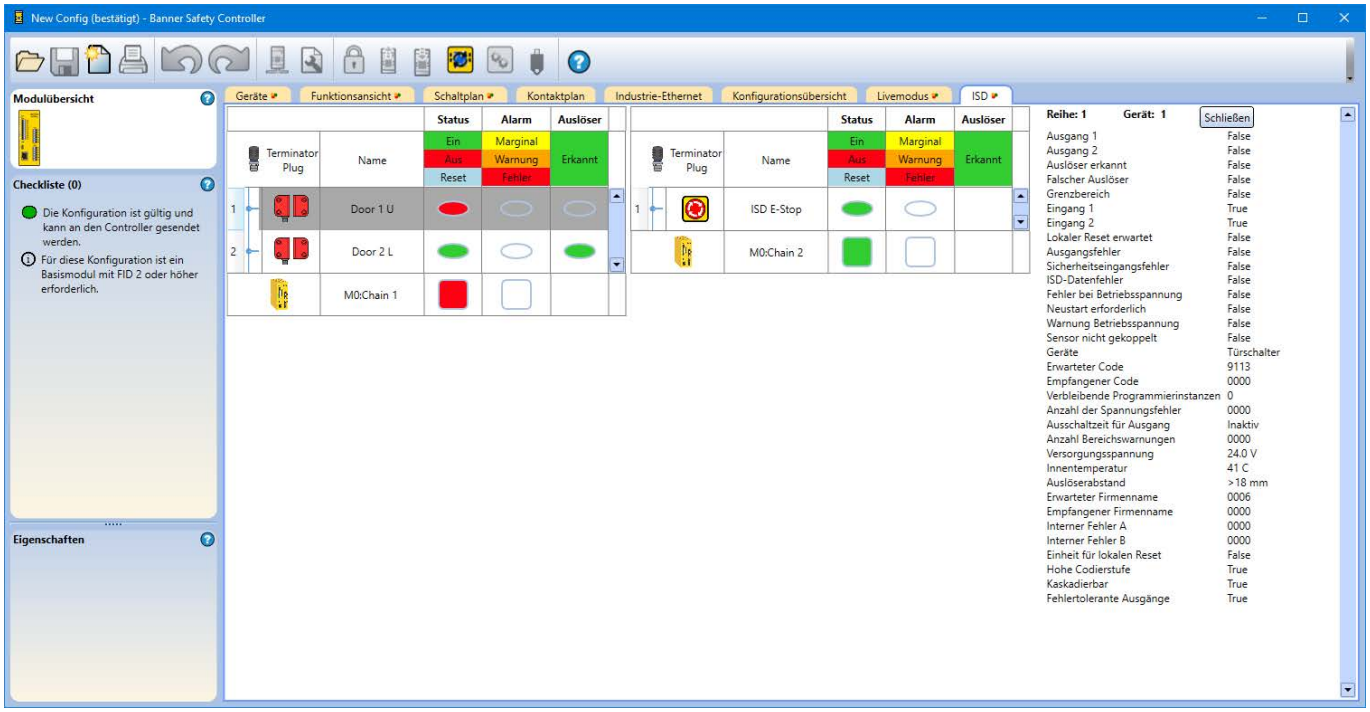
Im Livemodus enthält die Registerkarte **ISD** Echtzeitinformationen, die ca. einmal pro Sekunde aktualisiert werden, zu den angeschlossenen Geräten. Im folgenden Beispiel ist ein Schutztürschalter offen, wie durch die rote Anzeige oder den ausgeschalteten Zustand und eine leere Anzeige unter „Auslöser“ angegeben.

*Abbildung 81. Registerkarte **ISD** im Livemodus mit offenem Schalter*




Klicken Sie im Livemodus auf ein Gerät, um die zugehörigen Diagnosedaten anzuzeigen. Die Daten umfassen Ausgang, Eingang und ob der Auslöser erkannt wird.

*Abbildung 82. Registerkarte **ISD** im Livemodus mit Diagnosedaten*



# 9.10 Registerkarte Industrie-Ethernet

*Abbildung 83. XS/SC26-2 Registerkarte **Industrie-Ethernet***

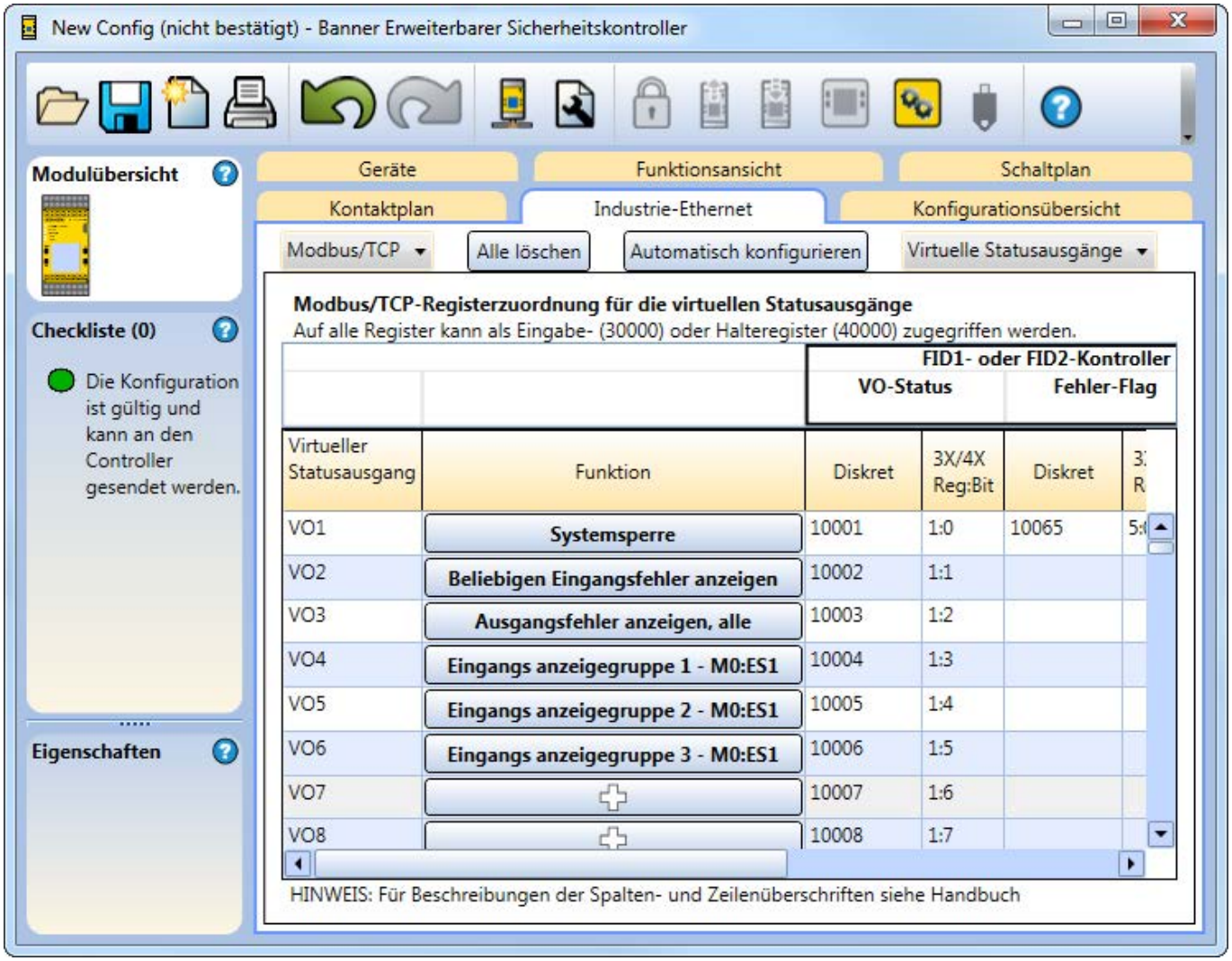
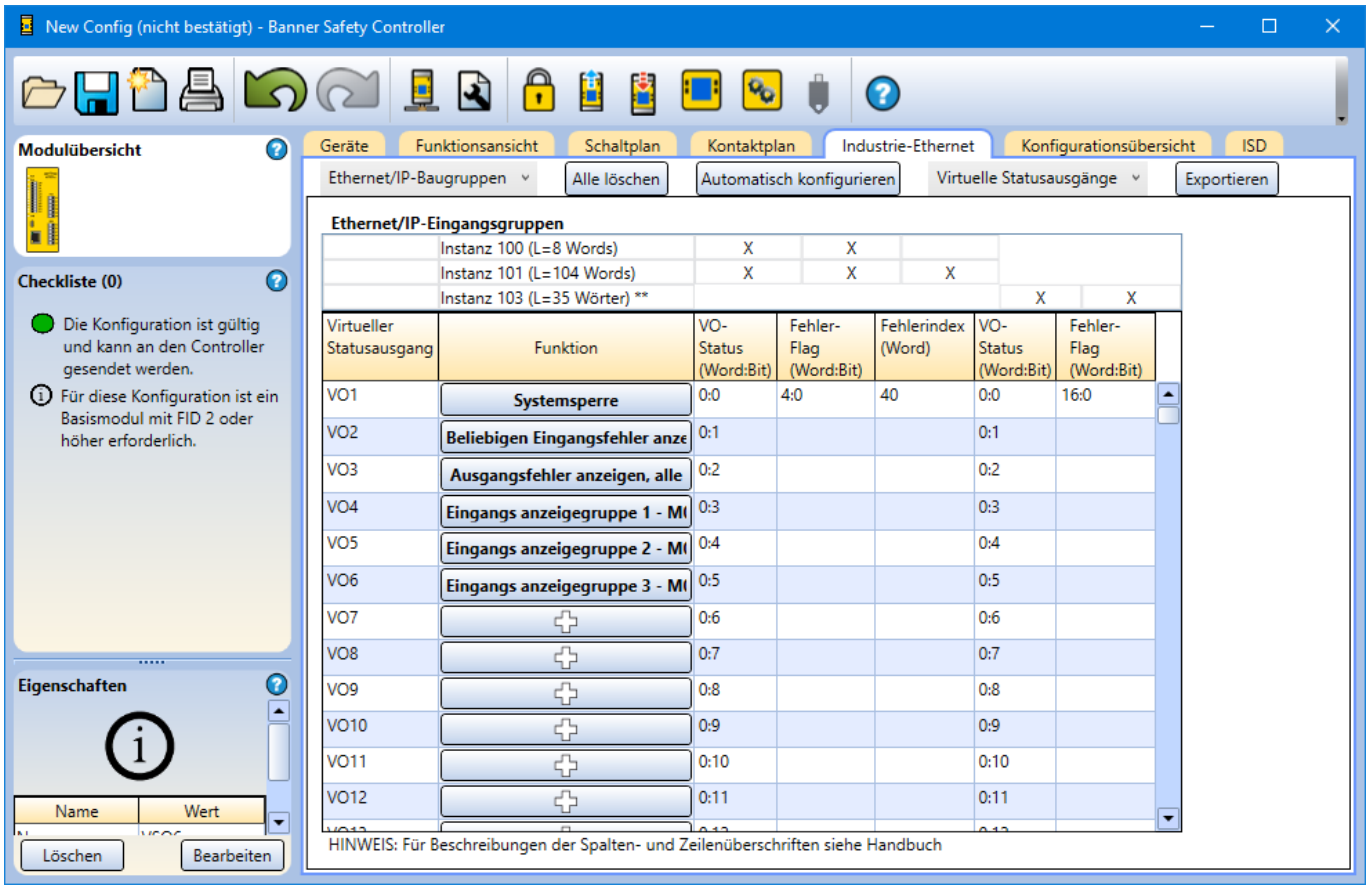


*Abbildung 84. SC10-2 Registerkarte **Industrie-Ethernet***




Auf der Registerkarte **Industrie-Ethernet** in der Software können die virtuellen Statusausgänge über das Netzwerk konfiguriert werden. Diese Ansicht enthält die gleichen Funktionen wie die Option **Statusausgänge** (in der Ansicht **Geräte** hinzugefügt) (weitere Informationen siehe Signallogik für Statusausgänge auf Seite 73 und Statusausgangsfunktion auf Seite 74). Bis zu 64 virtuelle Statusausgänge können bei FID 1-Basiskontrollern für eine Konfiguration hinzugefügt werden, bei der die Modbus/TCP-, EtherNet/IP-Eingangsgruppen-, EtherNet/IP-explizite-Nachrichten- und PCCC-Protokolle verwendet werden, und bis zu 256 virtuelle Statusausgänge können bei FID 2-Basiskontrollern und SC10-2-Sicherheitskontrollern hinzugefügt werden. FID 2-Basiskontroller und SC10-2-Sicherheitskontroller können auch PROFINET verwenden.

Zugriff auf die Registerkarte **Industrie-Ethernet**:

1. Klicken Sie auf **Netzwerkeinstellungen**.
2. Wählen Sie **Netzwerkschnittstelle aktivieren**.
3. Passen Sie die Einstellungen ggf. an. Siehe Netzwerkeinstellungen: Modbus/TCP, Ethernet/IP, PCCC auf Seite 112 oder Netzwerkeinstellungen: PROFINET (XS/SC26-2 ab FID 2 und SC10-2) auf Seite 113.
4. Klicken Sie auf **OK**.

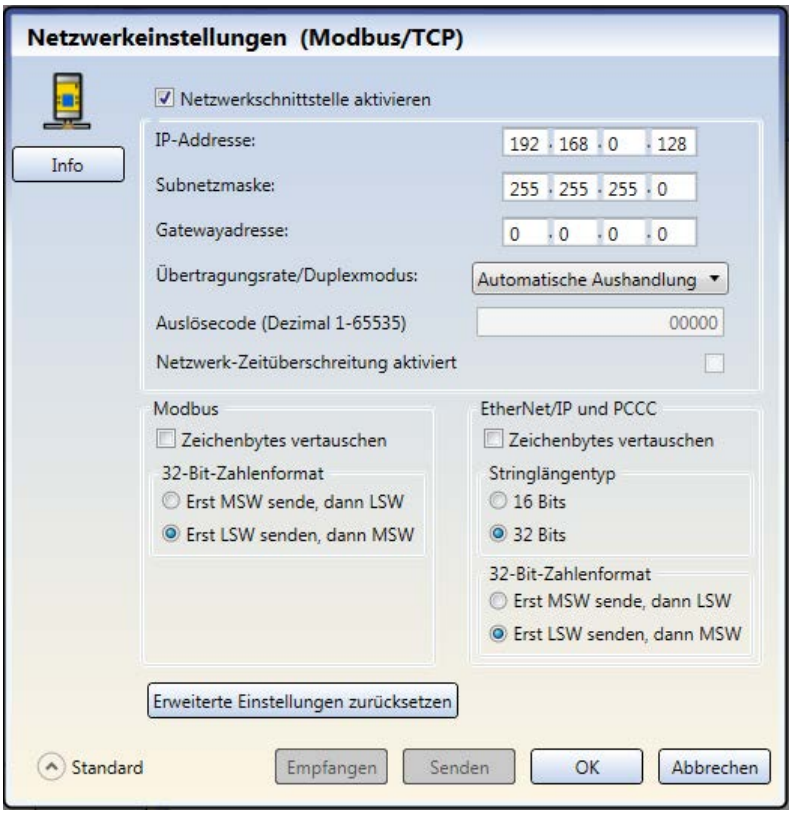
Verwenden Sie die Funktion **Automatisch konfigurieren** auf der Registerkarte **Industrie-Ethernet** der Software, um die virtuellen Statusausgänge auf Basis der aktuellen Konfiguration automatisch für eine Kombination häufig verwendeter

Funktionen zu konfigurieren. Klicken Sie in der Spalte **Funktion** neben einer der **VOx**-Zellen auf ✚, um einen virtuellen Statusausgang manuell hinzuzufügen. Funktionen aller virtuellen Statusausgänge können geändert werden, indem Sie auf die Schaltfläche klicken, die den Namen der Funktion des virtuellen Statusausgangs enthält, oder durch einen Klick auf **Bearbeiten** unter der Tabelle **Eigenschaften**, wenn „VOx“ gewählt ist.

# 9.10.1 Netzwerkeinstellungen

## Netzwerkeinstellungen: Modbus/TCP, Ethernet/IP, PCCC

*Abbildung 85. Netzwerkeinstellungen*




Klicken Sie in der Software auf **Netzwerkeinstellungen**, um das Fenster **Netzwerkeinstellungen** zu öffnen. Im Falle einer Modbus/TCP-Verbindung wird spezifikationsgemäß Port 502 als Standard-TCP-Port verwendet. Dieser Wert wird im Fenster **Netzwerkeinstellungen** nicht angezeigt.

*Tabelle 7. Netzwerk-Standardeinstellungen*

| Name der Einstellung | Im Werk voreingestellter Wert |
|---|---|
| **IP-Adresse** | 192.168.0.128 |
| **Subnetzmaske** | 255.255.255.0 |
| **Gatewayadresse** | 0.0.0.0 |
| **Übertragungsrate/Duplexmodus** | Automatische Aushandlung |

Für Konfigurationen mit einem manuellem Reset- oder Abbruchverzögerungseingang ist ein **Auslösecode** erforderlich.

Die Option **Erweitert** ermöglicht die weitere Konfiguration der Modbus/TCP- und Ethernet/IP-Einstellungen, wie zum Beispiel „Zeichenbytes vertauschen“, „MSW- und LSW-Sendepräzedenz“ und „Stringlängentyp“ (EtherNet/IP und PCCC).

Klicken Sie auf **Senden**, um die Netzwerkeinstellungen auf den Sicherheitskontroller zu schreiben. Die Netzwerkeinstellungen werden separat von den Konfigurationseinstellungen gesendet.

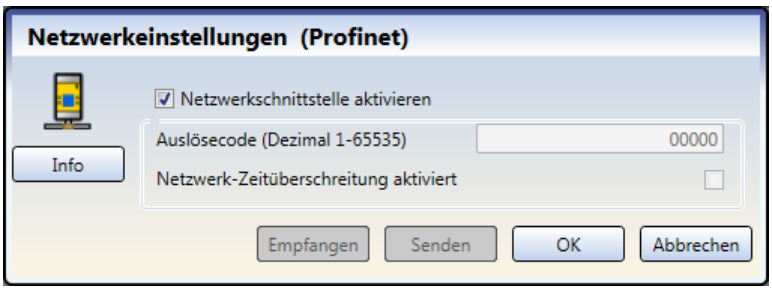
Klicken Sie auf **Netzwerk-Zeitüberschreitung aktiviert**, damit die konfigurierten virtuellen Ein-/Ausschaltungen bzw. virtuellen Muting-Aktivierungen im Falle einer Netzwerk-Zeitüberschreitung deaktiviert werden. Als Netzwerk-Zeitüberschreitung wurden 5 Sekunden festgelegt.

**Anmerkung:** Aktivieren oder deaktivieren Sie mit dem **Passwort-Manager** die Berechtigung zum Ändern der Netzwerkeinstellung für Benutzer2 und Benutzer3.

### Netzwerkeinstellungen: PROFINET (XS/SC26-2 ab FID 2 und SC10-2)

Klicken Sie nach der Auswahl des PROFINET-Protokolls in der Software auf der Registerkarte **Industrie-Ethernet** auf **Netzwerkeinstellungen**, um das Fenster **Netzwerkeinstellungen** zu öffnen.

*Abbildung 86. **Netzwerkeinstellungen** – PROFINET*




Klicken Sie auf **Senden**, um die Netzwerkeinstellungen auf den Sicherheitskontroller zu schreiben. Die Netzwerkeinstellungen werden separat von den Konfigurationseinstellungen gesendet.

Klicken Sie auf **Netzwerk-Zeitüberschreitung aktiviert**, damit alle konfigurierten virtuellen Ein-/Ausschaltungen bzw. virtuellen Muting-Aktivierungen im Falle einer Netzwerk-Zeitüberschreitung deaktiviert werden. Als Netzwerk-Zeitüberschreitung wurden 5 Sekunden festgelegt.

**Anmerkung:** Aktivieren oder deaktivieren Sie mit dem **Passwort-Manager** die Berechtigung zum Ändern der Netzwerkeinstellung für Benutzer2 und Benutzer3.

## 9.10.2 Erstellen von SPS-Tags/Etiketten-Dateien

Verwenden Sie die Software des Sicherheitskontroller von Banner, um eine .csv- oder .xml-Datei mit den Namen aller virtuellen Statusausgänge und -eingänge zu generieren.

Wenn Sie die in der Software des Sicherheitskontroller von Banner erstellten Namen als SPS-Tags/Labels verwenden möchten, importieren Sie die .csv- bzw. .xml-Datei in die SPS-Software über Ethernet/IP-Baugruppen oder PROFINET.

Erstellen Sie zuerst alle Statusausgänge und -eingänge, die Sie in der Software des Sicherheitskontroller von Banner haben möchten. Weisen Sie gegebenenfalls unter **Netzwerkeinstellungen** einen Auslösecode zu. Vergewissern Sie sich dann, dass das gewünschte Protokoll ausgewählt ist (entweder Ethernet/IP-Baugruppen oder PROFINET).

### Erstellen einer CSV-Datei für Ethernet/IP-Baugruppen

Zwei Elemente müssen bekannt sein:

- Der Name, der dem Sicherheitskontroller in der SPS zugewiesen ist. Dieser ist erforderlich, um die Datei zu generieren, die in die SPS-Software der Ethernet/IP-Baugruppe importiert werden soll.
- Welche Eingangs- und Ausgangsbaugruppeninstanzen angefordert werden sollen.

1. Vergewissern Sie sich, dass auf der Registerkarte **Industrie-Ethernet** in der Liste links **Ethernet/IP-Baugruppen** ausgewählt ist.
2. Klicken Sie auf **Exportieren**.
   Das Fenster **Als CSV exportieren** wird geöffnet.

*Abbildung 87. **Als CSV exportieren***




3. Geben Sie im Feld **Kontrollername** den Namen ein, der dem Sicherheitskontroller in der SPS-Software zugewiesen ist.
4. Wählen Sie die gewünschte Instanz aus der Liste **Instanz auswählen** aus.

   Die Auswahl der Instanz ist davon abhängig, welche Instanzen angefordert werden.

| Instanzname | Ausgangsbaugruppe | Eingangsbaugruppe |
|---|---|---|
| Status/Fehler | 112 | 100 |
| Fehlerindexwörter | 112 | 101 |
| Reset-/Abbruchverzögerung | 112 | 103 |
| VI-Status/Fehler | 113 | 100 |
| VI-Fehlerindexwörter | 113 | 101 |
| VI-Reset-/Abbruchverzögerung | 113 | 103 |
| VRCD Plus ISD | 114 | 104 |

Bei Verwendung virtueller Eingänge (VI) muss für die Ausgangsbaugruppe der SPS 113 oder 114 festgelegt sein. Dies ist erforderlich, damit die SPS die virtuellen Eingangswörter an den Sicherheitskontroller senden kann. Wenn Informationen an den ISD-Eingängen für Kontroller ab SC10 FID 2 gewünscht sind, muss eine mit 114 festgelegte Ausgangsbaugruppe verwendet werden, damit die virtuellen Eingänge (sofern verwendet) und die zusätzlichen Wörter zur Anfrage der ISD-Informationen gesendet werden können (VRCD steht für virtuelle Reset-/Abbruchverzögerung).

5. Klicken Sie auf **Exportieren**.
6. Speichern Sie die .csv-Datei am gewünschten Speicherort.

Die .csv-Datei kann direkt in die SPS-Software der Ethernet/IP-Baugruppe importiert werden. Sie kann aber auch mit beliebiger Software geöffnet werden, die .csv-Dateien lesen kann (z. B. Microsoft Excel).

## Erstellen einer XML-Datei für PROFINET

Drei Elemente müssen bekannt sein:

- Der Name, der dem Sicherheitskontroller in der SPS zugewiesen ist. Dieser ist erforderlich, um die Datei zu generieren, die in die PROFINET-SPS-Software importiert werden soll.
- Adresspfad zum SPS-Steckplatz 1
- Adresspfad zum SPS-Steckplatz 13
- Adresspfad zum SPS-Steckplatz 20
- Adresspfad zum SPS-Steckplatz 21

**Anmerkung:** Die Steckplätze 20 und 21 sind für ISD-Informationen vorgesehen und stehen erst zur Verfügung, nachdem ISD-Eingänge konfiguriert wurden (SC10-2 ab FID 2).

1. Vergewissern Sie sich, dass auf der Registerkarte **Industrie-Ethernet** in der Liste links **Profinet** ausgewählt ist.
2. Klicken Sie auf **Exportieren**.
   Das Fenster **An Excel exportieren** wird geöffnet.

*Abbildung 88. **An Excel exportieren***




3. Geben Sie im Feld **Kontrollername** den Namen ein, der dem Sicherheitskontroller in der SPS-Software zugewiesen ist.
4. Geben Sie im Feld **Adresspfad zum SPS-Steckplatz 1** den Anfang des Adresspfads zum Steckplatz 1 ein (Statusausgänge).
5. Geben Sie im Feld **Adresspfad zum SPS-Steckplatz 13** den Anfang des Adresspfads zum Steckplatz 13 ein (virtuelle Eingänge).
6. Geben Sie im Feld **Adresspfad zum SPS-Steckplatz 20** den Anfang des Adresspfads zum Steckplatz 20 ein (ISD-Statusinformationsmodul).

7. Geben Sie im Feld **Adresspfad zum SPS-Steckplatz 21** den Anfang des Adresspfads zum Steckplatz 21 ein (Modul für Informationen einzelner ISD-Geräte).
8. Klicken Sie auf **Exportieren**.
9. Speichern Sie die .xml-Datei am gewünschten Speicherort.

Die .csv-Datei kann direkt in die PROFINET-SPS-Software importiert werden. Sie kann aber auch mit beliebiger Software geöffnet werden, die .csv-Dateien lesen kann (z. B. Microsoft Excel).

## 9.10.3 Ethernet/IP-Gruppenobjekte

**Anmerkung:** Die EDS-Datei steht unter www.bannerengineering.com zum Download zur Verfügung. Weitere Informationen finden Sie unter Industrie-Ethernet – Übersicht auf Seite 157.

### Eingangsbaugruppenobjekte (T>O)

| Instanz-ID | Datenlänge (16-Bit-Wörter) | Beschreibung |
|---|---|---|
| **100 (0×64)** | 8 | Dient für den Zugriff auf die Basisinformationen über die virtuellen Statusausgänge 1–64. |
| **101 (0×65)** | 104 | Dient für den Zugriff auf die erweiterten Informationen (außer Basisinformationen) über die virtuellen Statusausgänge. |
| **102 (0×66)** | 150 | Dient für den Zugriff auf die Fehlerprotokollinformationen und enthält keine Informationen zu den virtuellen Statusausgängen. |
| **103 (0×67)** | 35 | Dient für den Zugriff auf die allgemeinen Informationen über die virtuellen Statusausgänge 1–256 und auf Feedback-Informationen über virtuelle Reset- und virtuelle Abbruchverzögerungseingänge. Auf Basiskontrollern ab FID 2 und SC10-2 verfügbar. |
| **104 (0×68)** | 112 | Dient für den Zugriff auf die allgemeinen Informationen über die virtuellen Statusausgänge 1–256, auf Feedback-Informationen über virtuelle Reset- und virtuelle Abbruchverzögerungseingänge sowie zur Unterstützung der Kommunikation mit ISD-fähigen Geräten. |

### Ausgangsbaugruppenobjekt (O>T)

| Instanz-ID | Datenlänge (16-Bit-Wörter) | Beschreibung |
|---|---|---|
| **112 (0×70)** | 2 | *Reserviert* |
| **113 (0×71)** | 11 | Dient zur Steuerung von virtuellen Eingängen (Ein/Aus, Muting-Aktivierung, Reset, Abbruchverzögerung). Auf Basiskontrollern ab FID 2 und SC10-2 verfügbar. |
| **114 (0×72)** | 14 | Dient zur Steuerung von virtuellen Eingängen (Ein/Aus, Muting-Aktivierung, Reset, Abbruchverzögerung) sowie zur Unterstützung der Kommunikation mit ISD-fähigen Geräten. |

### Konfigurationsbaugruppenobjekt

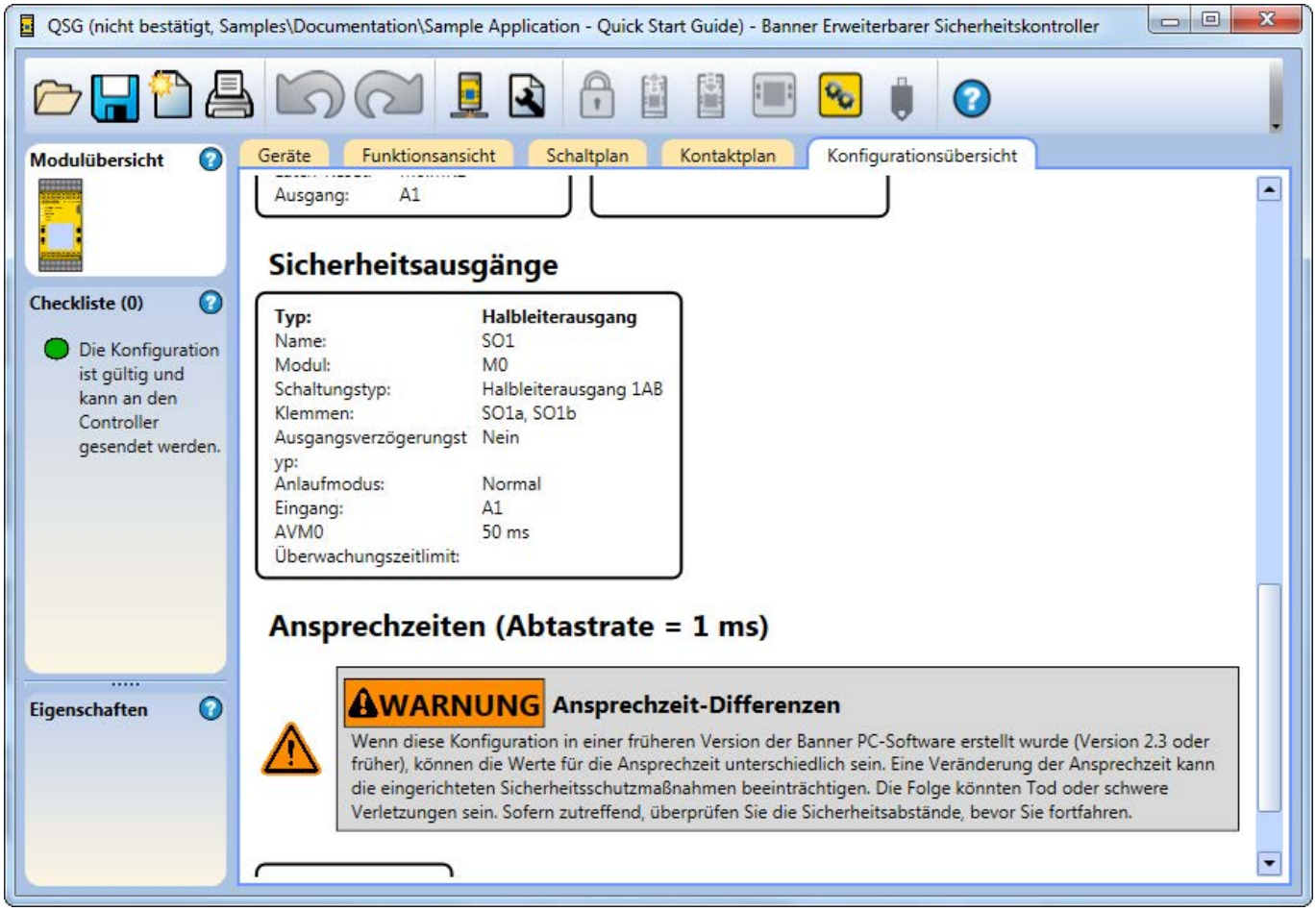
Das Konfigurationsbaugruppenobjekt ist nicht implementiert. Allerdings erfordern einige EtherNet-/IP-Clients ein solches Objekt. In diesem Fall wird Instanz-ID 128 (0×80) mit einer Datenlänge von 0 verwendet.

Legen Sie als Datentyp des Kommunikationsformats INT fest.

Legen Sie als gefordertes Paketintervall (RPI) mindestens den Wert 150 fest.

# 9.11 Registerkarte Konfigurationsübersicht

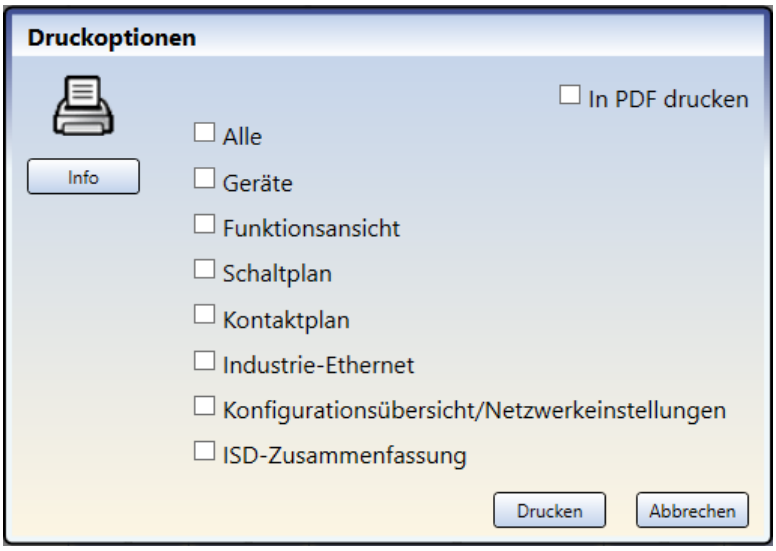
*Abbildung 89. Registerkarte **Konfigurationsübersicht***




Auf der Registerkarte **Konfigurationsübersicht** werden die detaillierten Informationen über alle konfigurierten Eingänge, Funktions- und Logikblöcke, Sicherheitsausgänge, Statusausgänge und die zugehörigen Ansprechzeiten in einem Textformat angezeigt.

# 9.12 Druckoptionen

*Abbildung 90. Druckoptionen*



Die Software enthält diverse Optionen zum Drucken der Konfiguration. Klicken Sie in der Symbolleiste auf **Drucken**, um das Fenster **Druckoptionen** aufzurufen.

Die folgenden Druckoptionen sind verfügbar:

- **Alles**: Druckt alle Ansichten, einschließlich der **Netzwerkeinstellungen** (bei Ethernet-fähigen Versionen).
- **Geräte**: Druckt die Registerkarte **Geräte**.
- **Funktionsansicht**: Druckt die Registerkarte **Funktionsansicht**.
- **Schaltplan**: Druckt die Registerkarte **Schaltplan**.
- **Kontaktplan**: Druckt die Registerkarte **Kontaktplan**.
- **Industrie-Ethernet**: Druckt die Registerkarte **Industrie-Ethernet**.
- **Konfigurationsübersicht/Netzwerkeinstellungen**: Druckt die **Konfigurationsübersicht** und die **Netzwerkeinstellungen** (sofern zutreffend).
- **ISD-Zusammenfassung**: Druckt die Registerkarte **ISD** (verfügbar auf SC10-2-Geräten ab FID 2)

Druckoptionen:

- **In PDF drucken**: Druckt die Auswahl in einer PDF-Datei, die an einem benutzerdefinierten Speicherort gespeichert wird.
- **Drucken**: Öffnet den Windows-Standarddialog für Drucken und sendet die Auswahl an den benutzerdefinierten Drucker.

## 9.13 XS/SC26-2 Passwort-Manager

**Passwort-Manager** ist verfügbar, wenn ein Sicherheitskontroller über einen USB-Anschluss mit dem PC verbunden ist. Die im **Passwort-Manager** angezeigten Informationen stammen vom Sicherheitskontroller.

*Abbildung 91. XS/SC26-2 **Passwort-Manager** (Version 4.2 angezeigt)*




Klicken Sie in der Symbolleiste der Software auf **Passwort-Manager**, um die Zugriffsrechte für die Konfiguration zu bearbeiten. Der Sicherheitskontroller speichert bis zu drei Benutzerpasswörter, um verschiedene Zugriffsebenen auf die Konfigurationseinstellungen zu verwalten. Das Passwort für Benutzer1 ermöglicht den uneingeschränkten Lese- und Schreibzugriff und die Möglichkeit zum Festlegen von Zugriffsebenen für Benutzer2 und Benutzer3 (Benutzernamen können nicht geändert werden). Auf allgemeine Informationen wie Netzwerkeinstellungen, Schaltpläne und Diagnoseinformationen kann ohne Passwort zugegriffen werden. Auf einem PC oder SC-XM2/3-Laufwerk gespeicherte Konfigurationen sind nicht passwortgeschützt.

Benutzer2 oder Benutzer3 kann die Konfiguration auf den Sicherheitskontroller schreiben, wenn **Allowed to change the configuration (Berechtigung zum Ändern der Konfiguration)** aktiviert ist. Die Netzwerkeinstellungen können geändert werden, wenn **Allowed to change the network settings (Berechtigung zum Ändern der Netzwerkeinstellungen)** aktiviert ist. Bis zur Softwareversion 4.1. ist die Option **Anzeige der Konfiguration zulassen** für Benutzer2 und Benutzer3 verfügbar und kann aktiviert werden, wenn für Benutzer1 **Zum Anzeigen der Konfiguration ist das Passwort erforderlich** markiert ist. Dazu sind die jeweiligen Passwörter erforderlich.

Klicken Sie auf **Speichern**, um die Passwort-Informationen in den Sicherheitskontroller zu schreiben.

Nur Benutzer1 kann den XS/SC26-2 auf die Werkseinstellungen zurücksetzen.

**Anmerkung:** Die Standardpasswörter für Benutzer1, Benutzer2 und Benutzer3 lauten jeweils 1901, 1902 und 1903. Die Standardpasswörter sollten unbedingt auf neue Werte geändert werden.

# 9.14 Passwort-Manager für SC10-2

**Passwort-Manager** ist verfügbar, wenn ein Sicherheitskontroller über einen USB-Anschluss mit dem PC verbunden ist. Die im **Passwort-Manager** angezeigten Informationen stammen vom Sicherheitskontroller.

*Abbildung 92. SC10-2 **Passwort-Manager***




Klicken Sie in der Symbolleiste der Software auf **Passwort-Manager**, um die Zugriffsrechte für die Konfiguration zu bearbeiten. Der Sicherheitskontroller speichert bis zu drei Benutzerpasswörter, um verschiedene Zugriffsebenen auf die Konfigurationseinstellungen zu verwalten. Das Passwort für Benutzer1 ermöglicht den uneingeschränkten Lese- und Schreibzugriff und die Möglichkeit zum Festlegen von Zugriffsebenen für Benutzer2 und Benutzer3 (Benutzernamen können nicht geändert werden). Konfiguration, Netzwerkeinstellungen, Schaltpläne und Diagnoseinformationen können ohne Passwort aufgerufen werden. Auf einem PC oder SC-XM2/3-Laufwerk gespeicherte Konfigurationen sind nicht passwortgeschützt.

Benutzer2 oder Benutzer3 kann die Konfiguration auf den Sicherheitskontroller schreiben, wenn **Berechtigung zum Ändern der Konfiguration** aktiviert ist. Die Netzwerkeinstellungen können geändert werden, wenn **Berechtigung zum Ändern der Netzwerkeinstellungen** aktiviert ist. Dazu sind die jeweiligen Passwörter erforderlich.

Klicken Sie auf **Speichern**, um die Passwortinformationen für die aktuelle Konfiguration in der Software zu übernehmen und sie in den Sicherheitskontroller zu schreiben.

**Anmerkung:** Die Standardpasswörter für Benutzer1, Benutzer2 und Benutzer3 lauten jeweils 1901, 1902 und 1903. Die Standardpasswörter sollten unbedingt auf neue Werte geändert werden.

Nur Benutzer1 kann den SC10-2 auf die Werkseinstellungen zurücksetzen.

# 9.15 Anzeigen und Importieren von Kontrollerdaten

Über die Software für den Sicherheitskontroller von Banner können aktuelle Sicherheitskontrollerdaten (z. B. Modellnummer und Firmware-Version, Konfigurations- und Netzwerkeinstellungen sowie Schaltplan) angezeigt oder kopiert werden.

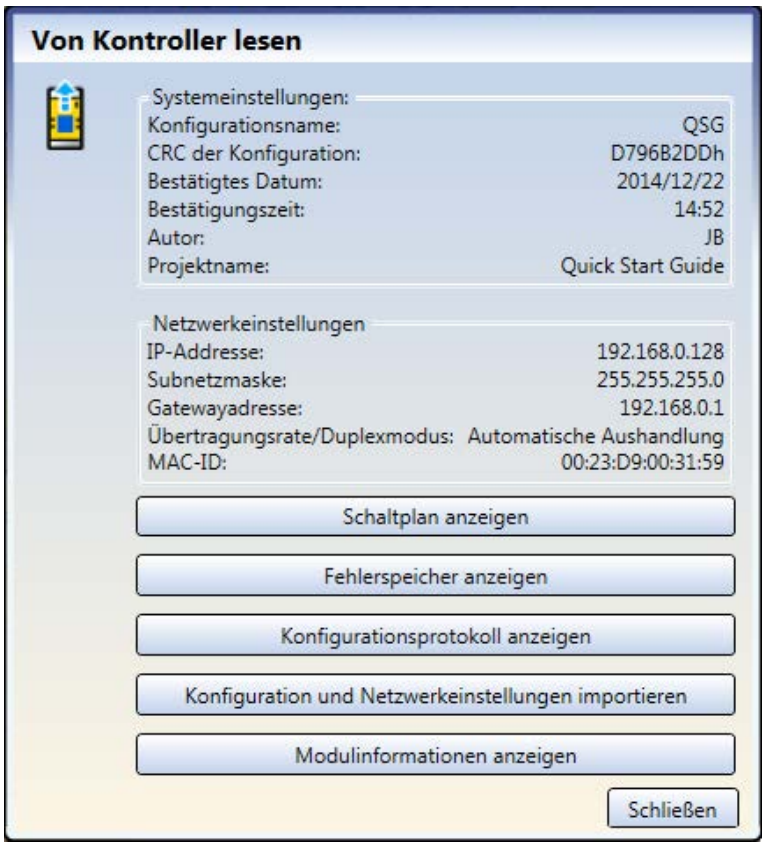
**Von Kontroller lesen** ist verfügbar, wenn ein Sicherheitskontroller über USB an den PC angeschlossen ist.

## Anzeigen einer Momentaufnahme von den System- und Netzwerkeinstellungen

Klicken Sie in der Symbolleiste der Software auf **Von Kontroller lesen**. Die aktuellen Einstellungen für den Sicherheitskontroller werden angezeigt:

- Konfigurationsname
- CRC der Konfiguration
- Datum der Bestätigung
- Uhrzeit der Bestätigung
- Autor
- Projektname
- IP-Adresse
- Subnetzmaske
- Gatewayadresse
- Übertragungsrate/Duplexmodus
- MAC-ID

*Abbildung 93. Anzeigen einer Momentaufnahme von den System- und Netzwerkeinstellungen*




## Anzeigen und Importieren von Kontrollerdaten

Klicken Sie auf **Von Kontroller lesen**, um folgende Informationen anzuzeigen:

- **Schaltplan**: Entfernt alle anderen Registerkarten und Arbeitsblätter von der Software und zeigt nur die Ansichten **Schaltplan** und **Geräte** an.
- **Fehlerprotokoll**: Der Verlauf der letzten 10 Fehler.

**Anmerkung:** Die Nummerierung der Fehlerprotokolle steigt bis maximal 4.294.967.295, sofern der Sicherheitskontroller nicht aus- und wieder eingeschaltet wird. Nach dem Aus- und Wiedereinschalten des Sicherheitskontrollers beginnt die Nummerierung der Fehlerprotokolle wieder bei 1. Durch Löschen des Fehlerprotokolls (über die Software oder über das Bedienfeld am Kontroller) wird der Protokollverlauf entfernt; die Nummerierung wird jedoch beibehalten.

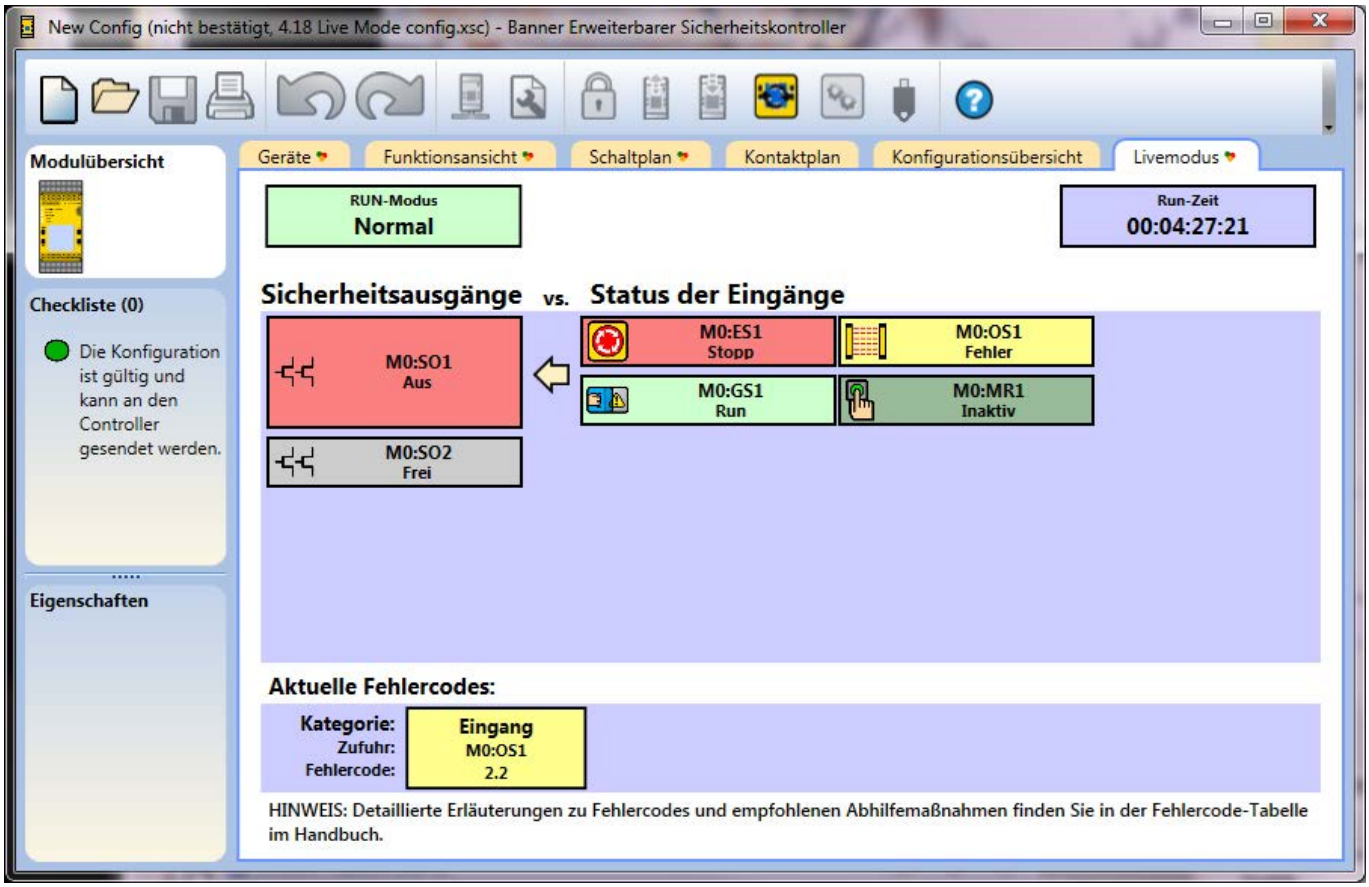
- **Konfigurationsprotokoll**: Verlauf von bis zu 10 zuletzt verwendeten Konfigurationen (nur die aktuelle Konfiguration kann angezeigt oder importiert werden)
- **Modulinformationen**

Klicken Sie auf **Konfiguration und Netzwerkeinstellungen importieren**, um die aktuelle Konfiguration und die aktuellen Netzwerkeinstellungen des Sicherheitskontrollers aufzurufen (dies hängt jeweils von den Benutzerzugriffsrechten ab, siehe XS/SC26-2 Passwort-Manager auf Seite 117 oder Passwort-Manager für SC10-2 auf Seite 118).

# 9.16 Livemodus

**Livemodus** ist verfügbar, wenn ein Sicherheitskontroller über USB an den PC angeschlossen ist.

*Abbildung 94. Laufzeit – XS/SC26-2 Registerkarte **Livemodus***




Die Registerkarte **Livemodus** kann mit einem Klick auf **Livemodus** in der Symbolleiste aufgerufen werden. Mit der Aktivierung des **Livemodus** werden Konfigurationsbearbeitungen auf allen anderen Registerkarten deaktiviert. Die Registerkarte **Livemodus** enthält zusätzliche Geräte- und Fehlerinformationen, einschließlich von Fehlercodes (siehe Fehlercode-Tabelle für XS/SC26-2 auf Seite 283 und SC10-2 Fehlercode-Tabelle auf Seite 288 für eine Beschreibung und mögliche Abhilfemaßnahmen). Die Laufzeitdaten werden ebenfalls auf den Registerkarten **Funktionsansicht**, **Geräte** und **Schaltplan** aktualisiert, die eine visuelle Darstellung des jeweiligen Gerätezustands liefern.

*Abbildung 95. Laufzeit – Registerkarte **Geräte***

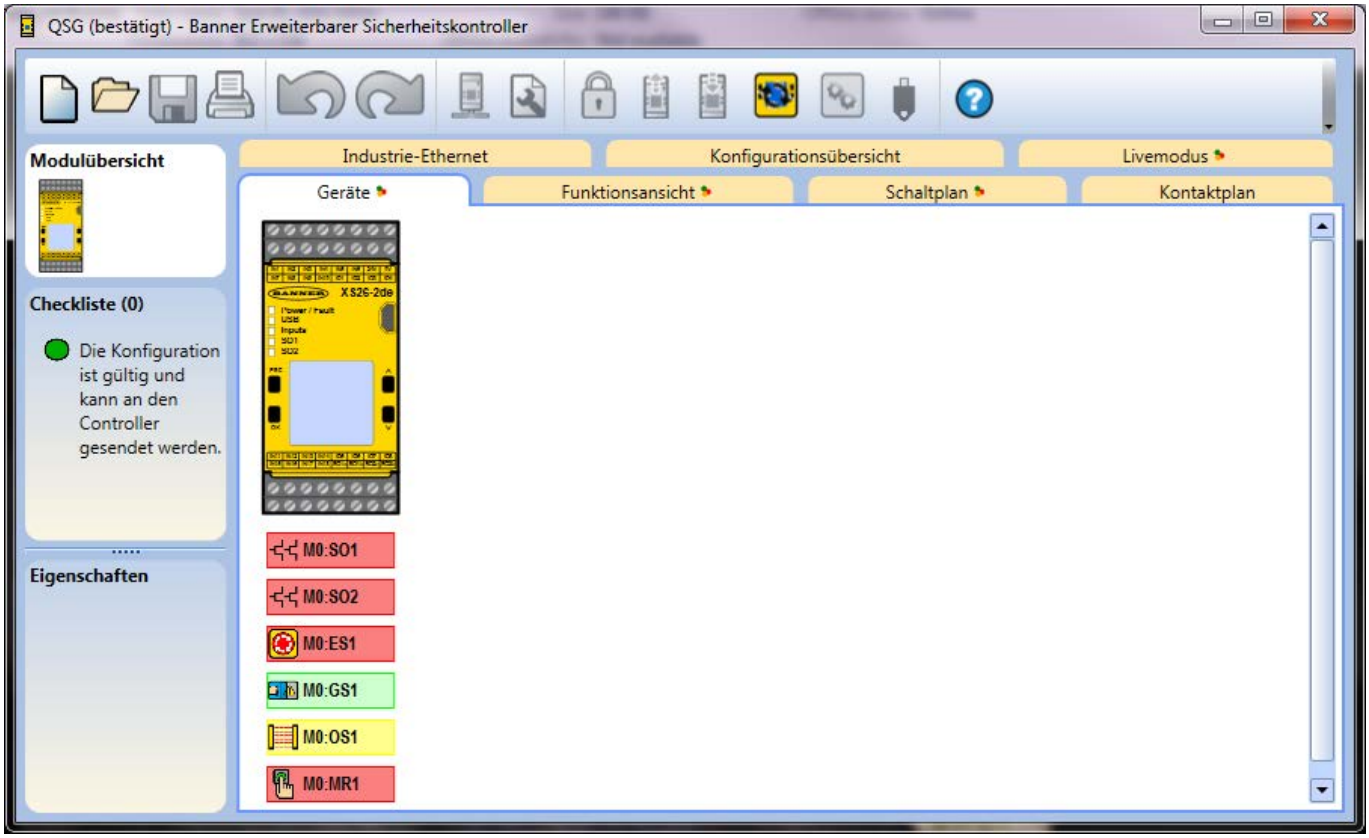



*Abbildung 96. Laufzeit – Registerkarte **Funktionsansicht***

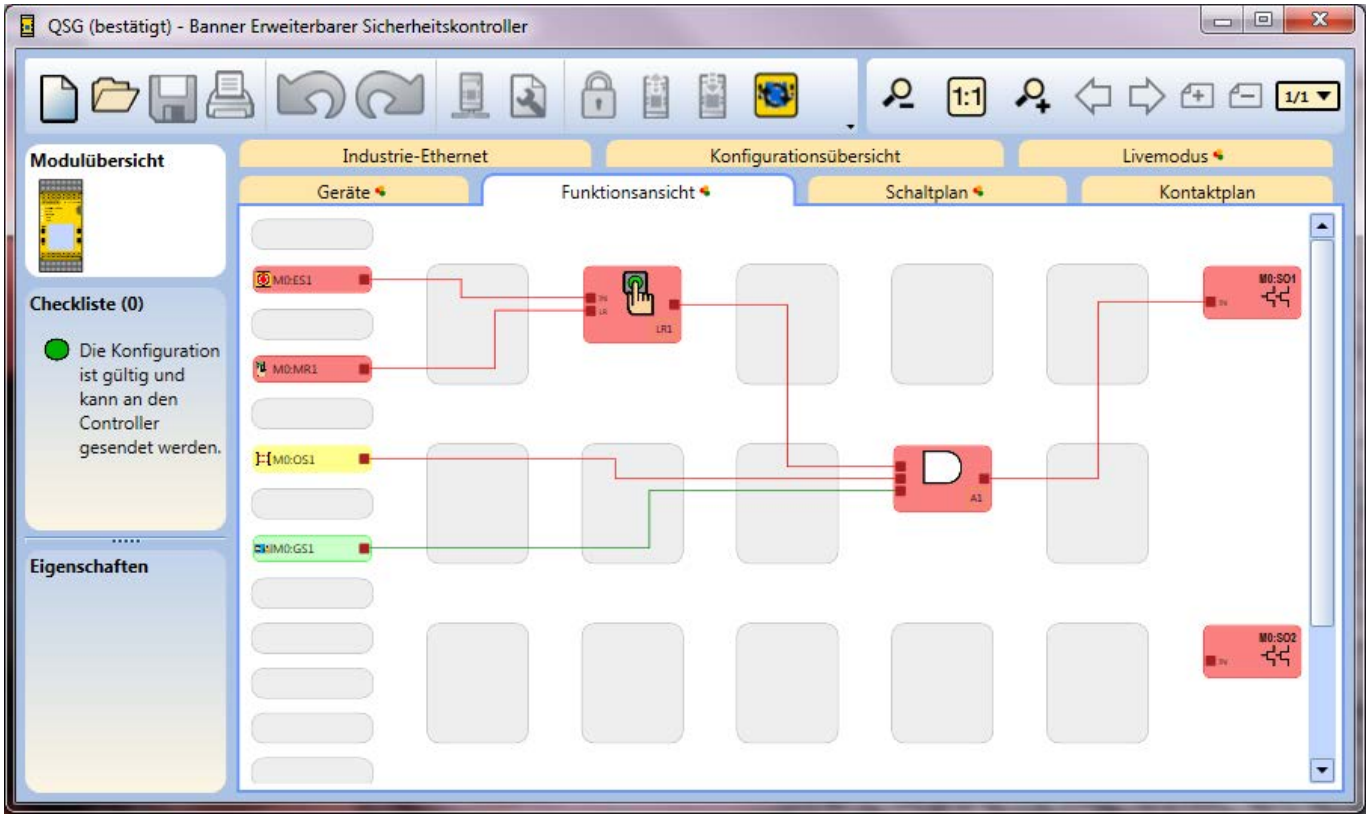


*Abbildung 97. Laufzeit – Registerkarte **Schaltplan***

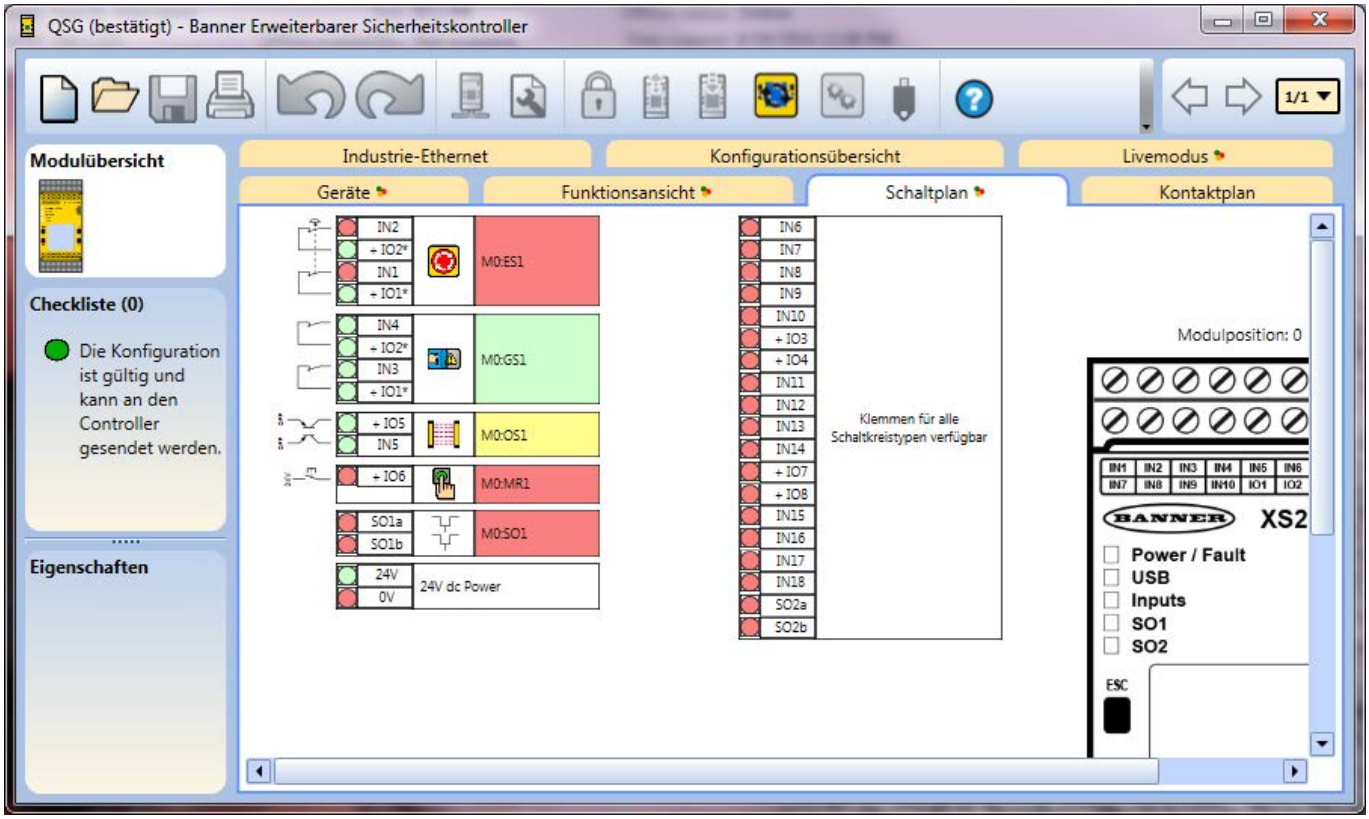
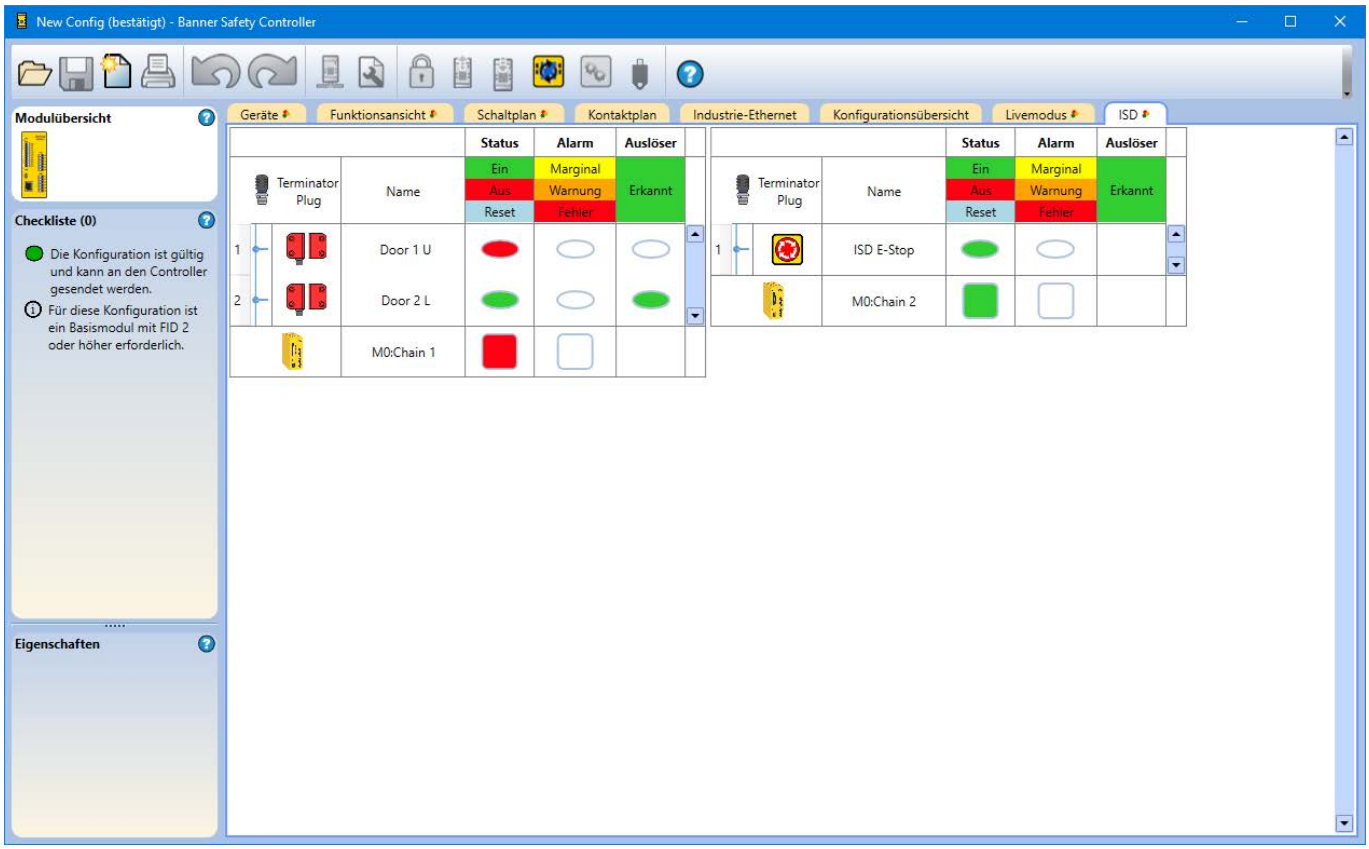
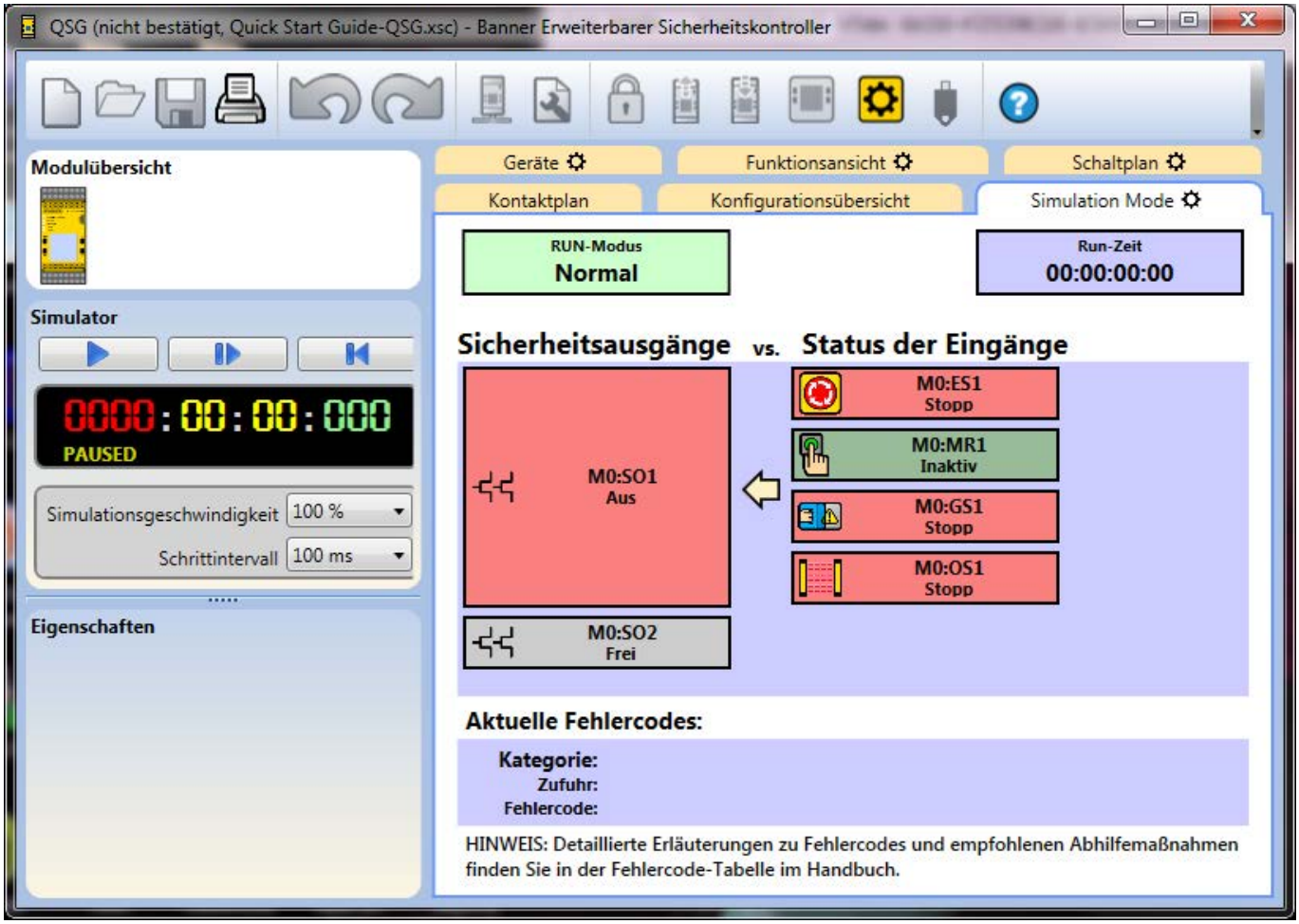



*Abbildung 98. Laufzeit — SC10-2 Registerkarte **ISD***



# 9.17 Simulationsmodus

*Abbildung 99. Simulationsmodus*




Die Registerkarte **Simulationsmodus** kann mit einem Klick auf **Simulationsmodus** in der Symbolleiste aufgerufen werden. Die Optionen für den Simulationsmodus werden auf der linken Bildschirmseite verfügbar. Die Registerkarte **Simulationsmodus** enthält Informationen, die nur zur Anzeige bestimmt sind. In dieser Ansicht können Sie nicht auf die Ein- oder Ausgabeelemente klicken.

**Anmerkung:** Für ISD-Eingänge werden keine einzelnen Geräte simuliert, sondern nur der letzte Ausgang, der an die Eingangsklemmen des SC10-2 angeschlossen ist (ein oder aus).



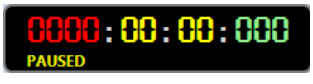
[Wiedergabe/Pause] Startet die Simulationszeit, die mit der angegebenen Simulationsgeschwindigkeit läuft, oder hält die Simulationszeit vorübergehend an.



[Einzelschritt] Rückt die Simulationszeit um einen Schritt zum angegebenen Schrittintervall vor.



[Reset] Setzt den Zeitgeber auf null und die Ausrüstung auf den anfänglichen Aus-Zustand zurück.




[Zeitgeber] Zeigt die abgelaufene Zeit in Stunden, Minuten, Sekunden und tausendstel Sekunden an.

**Simulationsgeschwindigkeit**: Legt die Geschwindigkeit der Simulation fest.

- 1 %
- 10 %
- 100 % (Standardgeschwindigkeit)
- 500 %
- 2.000 %

**Schrittintervall**: Legt fest, um welches Zeitintervall die Einzelschritt-Schaltfläche vorrückt, wenn sie betätigt wird. Die Größe des Intervalls richtet sich nach der Größe der Konfiguration.

Wählen Sie **Wiedergabe**, um die Simulation zu starten. Der Zeitgeber läuft und die sich drehenden Zahnräder zeigen an, dass die Simulation läuft. Die Registerkarten **Funktionen**, **Geräte** und **Schaltplan** werden aktualisiert, sodass die simulierten Gerätezustände visuell dargestellt werden. Die Konfiguration kann so getestet werden. Klicken Sie auf die Elemente, die getestet werden sollen. Ihre Farbe und ihr Zustand ändern sich entsprechend. Rot gibt den Stopp- oder ausgeschalteten Zustand an. Grün gibt den RUN- oder eingeschalteten Zustand an. Gelb gibt einen Fehlerzustand an. Orange zeigt an, dass der Eingang vor der Inbetriebnahme der Simulation eingeschaltet wurde. Wegen eines notwendigen Anlauf-Ausschalttests muss der Ausgang erst als ausgeschaltet gesehen werden, bevor er als eingeschaltet erkannt werden kann.

*Abbildung 100. Simulationsmodus: Registerkarte **Geräte***

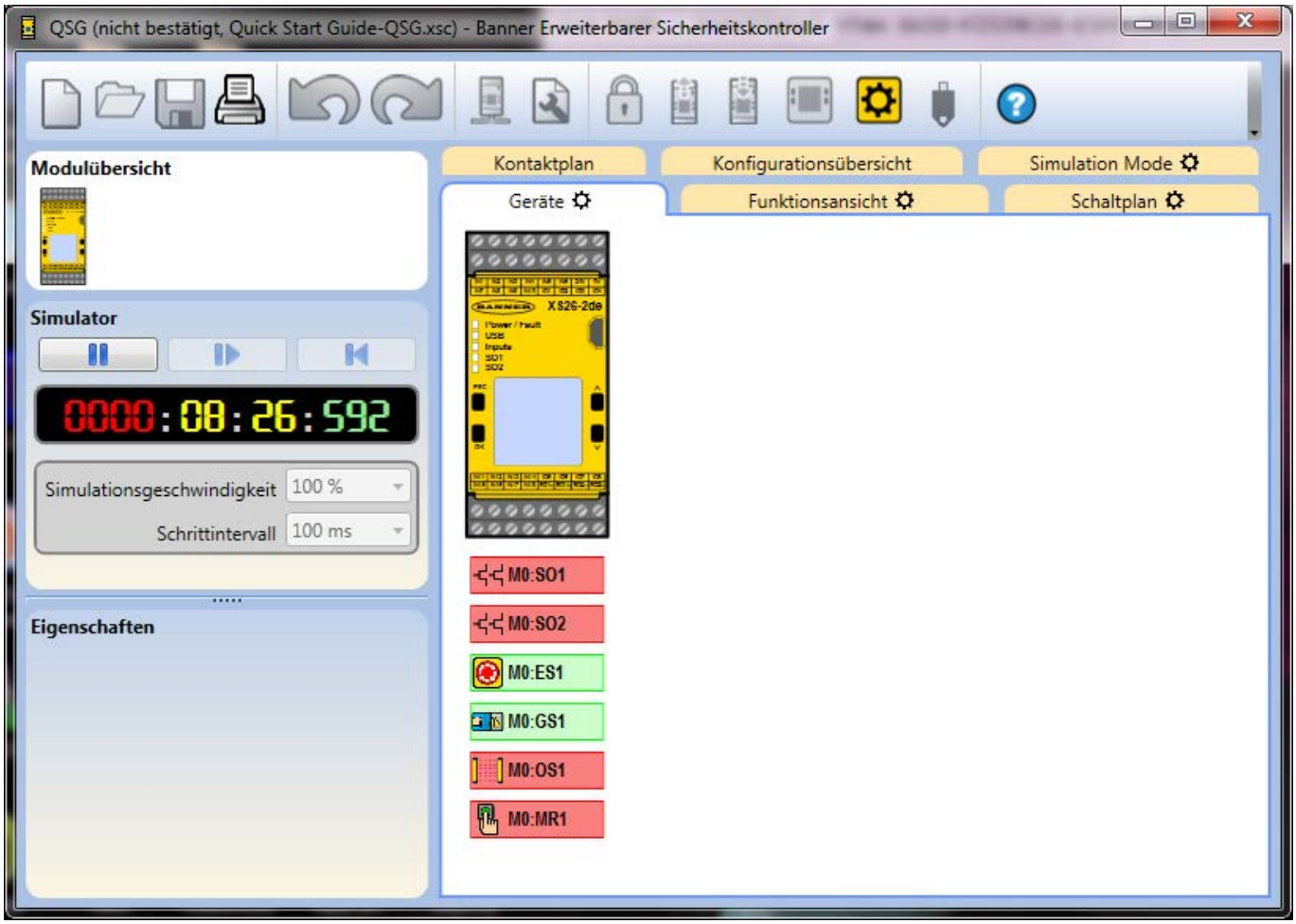


*Abbildung 101. Simulationsmodus: Registerkarte **Schaltplan***

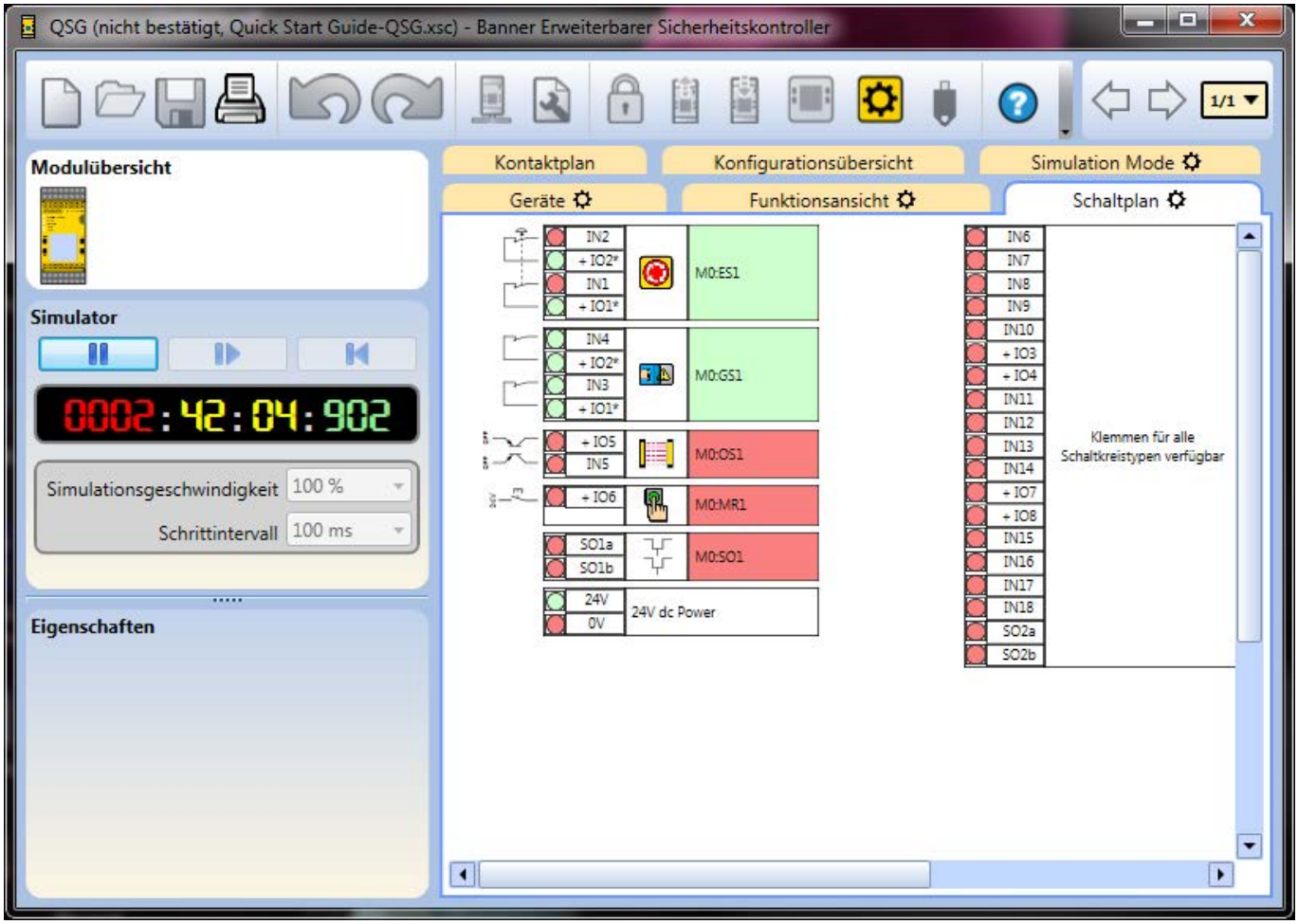
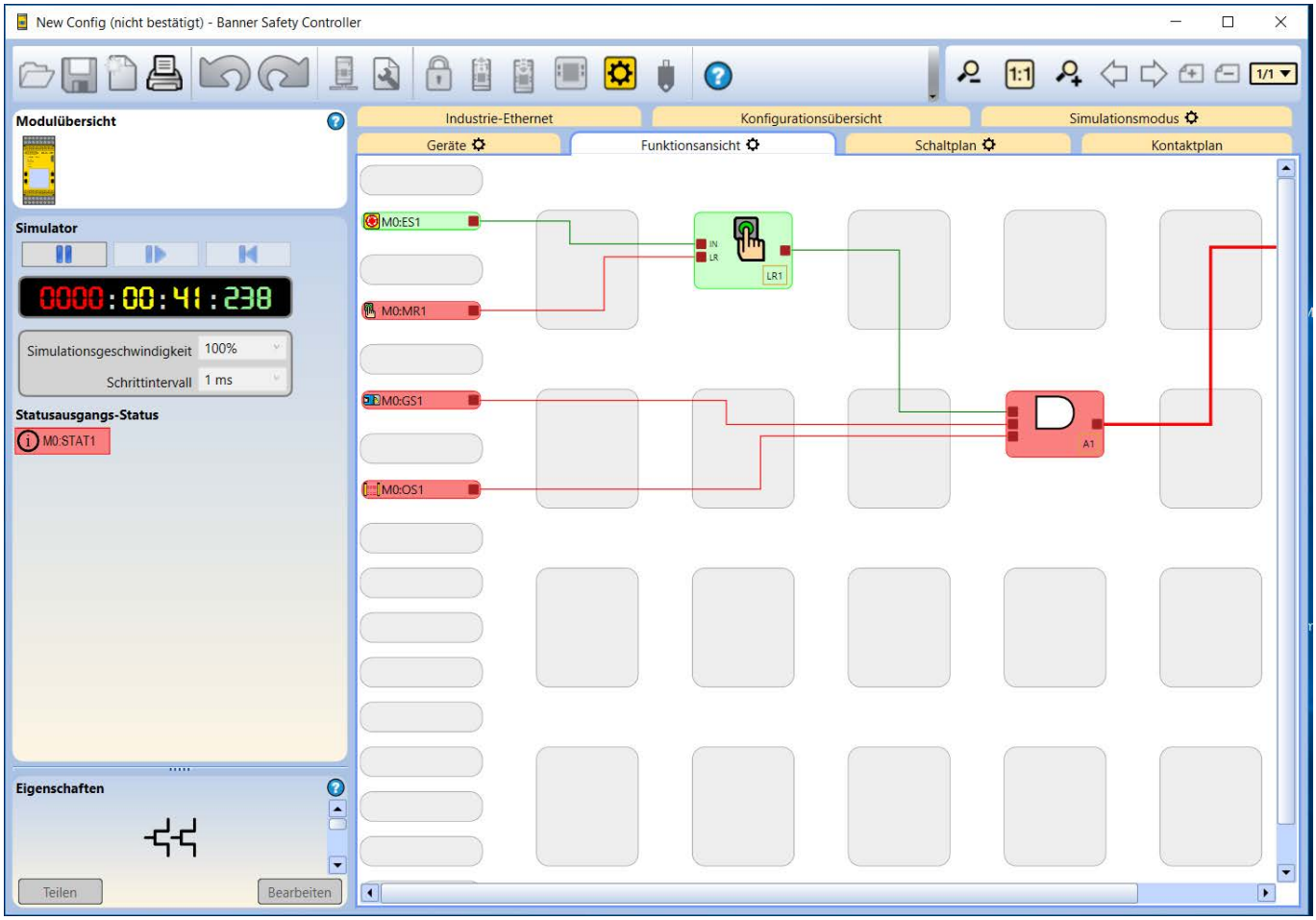


*Abbildung 102. Simulationsmodus: Registerkarte **Funktionsansicht***




## 9.17.1 Aktionszeitsteuerungsmodus

Im Simulationsmodus und auf der Registerkarte **Funktionsansicht** werden bestimmte Elemente, die sich in Aktionsverzögerungsmodi befinden, lilafarben angezeigt. Die Statusleiste zeigt den Countdown des mit dem Element verbundenen Zeitgebers an.

Die folgenden Abbildungen zeigen die verschiedenen Elementzustände an:

*Abbildung 103. Sicherheitsausgang im Modus für zeitgesteuerte Ausschaltverzögerung.*

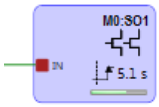



*Abbildung 104. Muting-Block im Modus für zeitgesteuertes Muting*

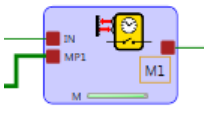
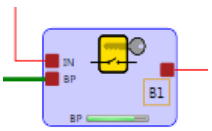



*Abbildung 105. Überbrückungsblock im Modus für zeitgesteuerte Überbrückung*




**Anmerkung:** Das M neben der Statusleiste gibt das zeitgesteuerte Muting an.

*Abbildung 106. Verzögerungsblock: XS/SC26-2 nur Basiskontroller ab FID 2 und SC10-2*

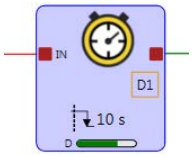
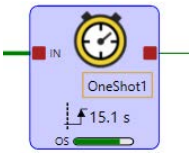



*Abbildung 107. One-Shot-Block: nur Basiskontroller vom Typ XS/SC26-2 ab FID 4*

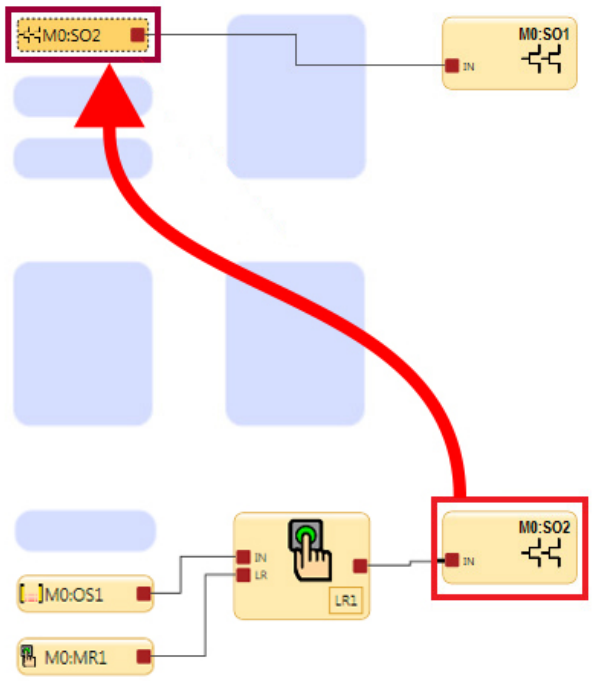


# 9.18 Referenzsignale

**Wichtig:** Die Konfigurationssoftware enthält Referenzsignale, die den Zustand der Kontrollerausgänge, Eingangsgeräte und sowohl der Funktions- als auch der Logikblöcke darstellen. Ein Referenzsignal für einen Sicherheitsausgang kann zur Steuerung eines anderen Sicherheitsausgangs dienen. Bei dieser Art der Konfiguration ist der physikalische Ein-Zustand des steuernden Sicherheitsausgangs nicht bekannt. Ist der Ein-Zustand des Sicherheitsausgangs kritisch für die Anwendungssicherheit, ist ein externer Rückkopplungsmechanismus erforderlich. Beachten Sie, dass sich dieser Kontroller im sicheren Zustand befindet, wenn die Ausgänge ausgeschaltet sind. Wenn es von kritischer Bedeutung ist, dass der Sicherheitsausgang 1 eingeschaltet ist, bevor sich der Sicherheitsausgang 2 einschaltet, muss die vom Sicherheitsausgang 1 gesteuerte Vorrichtung überwacht werden, damit ein Eingangssignal erzeugt wird, mit dem Sicherheitsausgang 2 gesteuert werden kann. Das Referenzsignal für Sicherheitsausgang 1 ist in diesem Fall möglicherweise nicht geeignet.

Abbildung 108 auf Seite 127 zeigt, wie ein Sicherheitsausgang einen anderen Sicherheitsausgang steuern kann. Wenn manueller Reset **M0:MR1** gewählt wird, wird dadurch Sicherheitsausgang **M0:SO2** eingeschaltet. Dieser schaltet daraufhin Sicherheitsausgang **M0:SO1** ein.

*Abbildung 108. Von einem anderen Sicherheitsausgang gesteuerter Sicherheitsausgang*



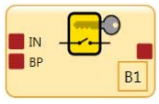
# 10 Beschreibung der Funktionsblöcke

In den folgenden Abschnitten werden die verfügbaren Funktionsblöcke im Detail beschrieben.

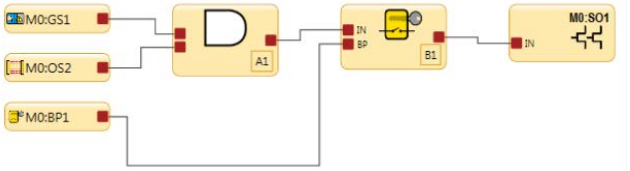
## 10.1 Überbrückungsblock

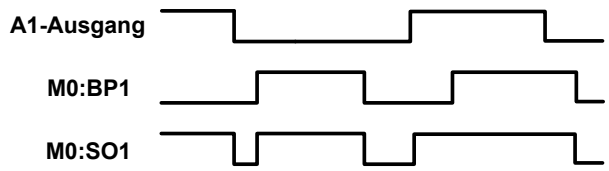
*Abbildung 109. Zeitablauf-Diagramm: Überbrückungsblock*

| Standardknoten | Zusätzliche Knoten | Anmerkungen |
|---|---|---|
| IN BP | - | Wenn der BP-Knoten inaktiv ist, durchläuft das Sicherheitssignal einfach den Überbrückungsblock. Wenn der BP-Knoten aktiv ist, ist der Ausgang des Blocks unabhängig vom Status des IN-Knotens eingeschaltet (wenn das Kontrollkästchen **Ausgang schaltet sich aus, wenn beide Eingänge (IN und BP) eingeschaltet sind** deaktiviert ist). Der Ausgang des zugehörigen Überbrückungsblocks schaltet sich aus, wenn der Überbrückungs-Zeitgeber abläuft. |




**Überbrückungs - Funktionsblock**




**Überbrückungs-Zeitlimit**: Ein Zeitlimit für die Überbrückungsfunktion muss festgelegt werden, um die Aktivitätsdauer der Überbrückung für das Sicherheitseingangsgerät zu begrenzen. Es kann ein Zeitlimit von 1 Sekunde (Standard) bis 12 Stunden eingestellt werden. Dieses kann nicht deaktiviert werden. Es kann nur ein Zeitlimit festgelegt werden. Dieses Zeitlimit gilt dann für alle überbrückten Sicherheitsvorrichtungen. Am Ende des Zeitlimits wird die Steuerungsbefugnis für den Sicherheitsausgang wieder zurück auf die überbrückten Sicherheitseingangsgeräte übertragen.

**Überbrückung für Zweihandsteuerung**: Der Sicherheitskontroller gibt ein Stoppsignal aus, wenn ein Zweihandsteuerungseingang betätigt wird, während der Eingang überbrückt wird. Hierdurch wird sichergestellt, dass der Bediener nicht irrtümlich annimmt, dass die Zweihandsteuerung funktional ist, ohne zu wissen, das die Zweihandsteuerung überbrückt wurde und ihre Schutzfunktion nicht mehr erfüllt.

### 10.1.1 Verriegeln/Kennzeichnen

Gefährliche Energie (Verriegeln/Kennzeichnen) muss bei der Maschinenwartung und -reparatur kontrolliert werden, wenn die unerwartete Stromzufuhr, ein unerwarteter Maschinenanlauf oder die Freisetzung der gespeicherten Energie Verletzungen verursachen könnte. Sorgen Sie anhand von OSHA 29CFR 1910.147, ANSI 2244.1, ISO 14118, ISO 12100 oder anderen einschlägigen Normen, dass eine Umgehung einer Schutzeinrichtung den in den Normen enthaltenen Anforderungen nicht widerspricht.

**WARNUNG: Eingeschränkte Anwendung der Überbrückungsfunktion**

**Die Überbrückungsfunktion ist nicht für Produktionszwecke gedacht. Sie wird ausschließlich für vorübergehende oder aussetzende Maßnahmen verwendet, beispielsweise zur Bereinigung des definierten Bereichs von einem Sicherheits-Lichtvorhang, wenn ein Materialstau entstanden ist.** Bei Anwendung der Überbrückungsfunktion hat der Anwender dafür Sorge zu tragen, die Funktion normkonform (z. B. gemäß ANSI NFPA79 oder IEC/EN60204-1) zu installieren und zu verwenden.

#### Sichere Arbeitsmethoden und Einweisungen

Sichere Arbeitsverfahren bieten den Personen die Möglichkeit, ihre Gefahrenexposition durch die Nutzung schriftlicher Verfahren für bestimmte Aufgaben und die damit verbundenen Gefahren zu kontrollieren. Es muss auch die Möglichkeit in Betracht gezogen werden, dass eine Person die Schutzeinrichtung umgehen könnte und sie dann entweder nicht wieder in Betrieb nimmt oder anderes Personal nicht auf die bestehende Umgehung aufmerksam macht. In beiden Fällen kann eine Gefahrsituation entstehen. Um das zu verhindern, kann zum Beispiel ein sicherer Arbeitsablauf entwickelt

werden. Im Weiteren ist sicherzustellen, dass das Personal entsprechend eingewiesen wird und diesen Arbeitsablauf korrekt befolgt.

# 10.2 Verzögerungsblock (XS/SC26-2 ab FID 2 und SC10-2)

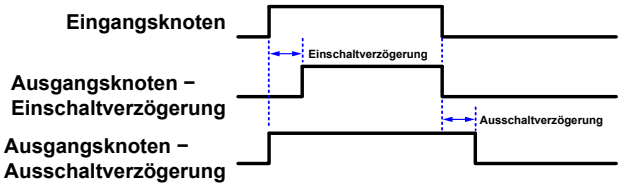
Mit dem Verzögerungsblock können Benutzer eine Ein- oder Ausschaltverzögerung von bis zu 5 Minuten in 1-ms-Schritten konfigurieren.

| Standardknoten | Zusätzliche Knoten | Anmerkungen |
|---|---|---|
| IN | CD | Je nach Auswahl wird ein Übergang des Signals in einen anderen Zustand am Eingangsknoten um die Ausgangsverzögerungszeit verzögert, indem entweder der Ausgang ausgeschaltet bleibt (Einschaltverzögerung) oder der Ausgang eingeschaltet bleibt (Ausschaltverzögerung). |

**Anmerkung:** Die tatsächliche Verzögerungszeit eines Verzögerungsfunktionsblocks oder eines Sicherheitsausgangs mit Verzögerung kann bis zu 1 Scan-Zeit länger sein als die Verzögerungszeiteinstellung. Mehrere Verzögerungsblöcke oder Verzögerungsausgänge in Reihe erhöhen die Gesamtverzögerungszeit um bis zu 1 Scan pro Verzögerungsfunktion. Beispiel: 3 Funktionsblöcke für die Ausschaltverzögerung à 100 ms in Reihe und eine Scan-Zeit von 15 ms können zu einer tatsächlichen Verzögerungszeit von bis zu 345 ms führen (300 ms + 45 ms).

Der Abbruchverzögerungsknoten ist ein konfigurierbarer Knoten, wenn die Ausschaltverzögerung ausgewählt wurde.

*Abbildung 110. Zeitablaufdiagramm für Verzögerungsblock*

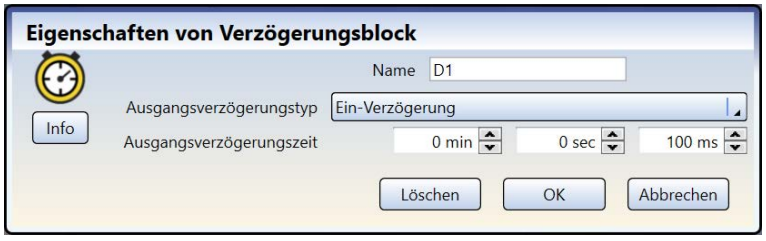



**VORSICHT: Auf die Ansprechzeit wirkende Verzögerungszeit**

Die Ausschaltverzögerungszeit kann die Ansprechzeit der Sicherheitssteuerung erheblich erhöhen. Dies wirkt sich auf die Stellung der Schutzeinrichtungen aus, deren Installation sich nach den Formeln für (Mindest-)Sicherheitsabstand richtet oder anderweitig von der Zeitberechnung für das Erreichen eines nicht gefährlichen Zustands beeinflusst wird. Bei der Installation der Schutzeinrichtungen muss der Anstieg der Ansprechzeit berücksichtigt werden.

**Anmerkung:** Die auf der Registerkarte **Konfigurationsübersicht** angegebene Ansprechzeit ist eine maximale Zeit. Diese kann sich je nach der Verwendung der Verzögerungsblöcke oder anderer logischer Blöcke (z. B. ODER-Funktionen) ändern. Es liegt in der Verantwortung des Anwenders, die korrekte Ansprechzeit zu ermitteln, zu überprüfen und einzurechnen.

*Abbildung 111. Verzögerungsblock-Eigenschaften*




Im Fenster **Verzögerungsblock-Eigenschaften** kann der Benutzer Folgendes konfigurieren:

**Name**

Die Bezeichnung des Eingangs.

**Ausgangsverzögerungstyp**

Dies ist der Ausgangsverzögerungstyp

- Keine
- Ausschaltverzögerung
- Einschaltverzögerung

**Ausgangsverzögerungszeit**

Verfügbar, wenn als Einstellung für die Verzögerung des Sicherheitsausgangs entweder Ausschaltverzögerung oder Einschaltverzögerung gewählt wurde.

Verzögerungszeit: 1 ms bis 5 Minuten, in 1-ms-Schritten. Standardeinstellung ist 100 ms.

**Abbruchtyp**

Verfügbar, wenn als Einstellung für die Verzögerung des Sicherheitsausgangs die Ausschaltverzögerung gewählt wurde.

- Kein Abbruch
- Steuerungseingang (Der Ausgang des Verzögerungsblocks bleibt eingeschaltet, wenn der Eingang vor dem Ende der Verzögerung wieder eingeschaltet wird.)
- Abbruchverzögerungsknoten

**Endlogik**

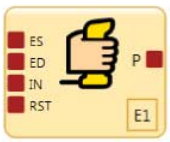
Verfügbar, wenn als Einstellung für den Abbruchtyp Abbruchverzögerungsknoten gewählt wurde.

- Ausgang eingeschaltet lassen
- Ausgang ausschalten

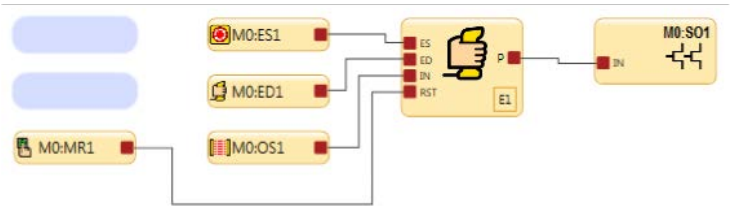
# 10.3 Zustimmtaster-Block

*Abbildung 112. Zeitablauf-Diagramm: Zustimmtaster, einfache Konfiguration*

| Standardknoten | Zusätzliche Knoten | Anmerkungen |
|---|---|---|
| ED IN RST | ES JOG | Ein Zustimmtaster-Block muss direkt mit einem Ausgangsblock verbunden werden. Durch diese Methode wird sichergestellt, dass die Endkontrolle des Ausgangs beim Bediener liegt, die den Zustimmtaster hält. Der ES-Knoten ist für Sicherheitssignale zu verwenden, die nicht vom ED-Knoten überbrückt werden sollten. Falls keine weiteren Eingänge des Funktionsblocks konfiguriert werden, ist die Verwendung eines Funktionsblocks für Zustimmtaster nicht erforderlich. |




**Zustimmtaster-Funktionsblock**



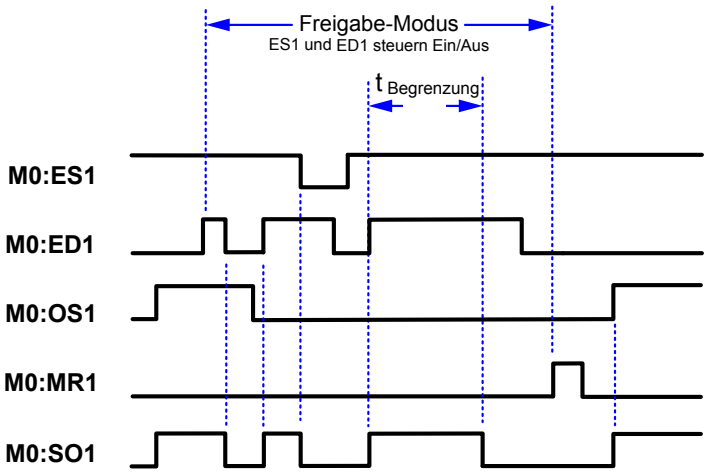
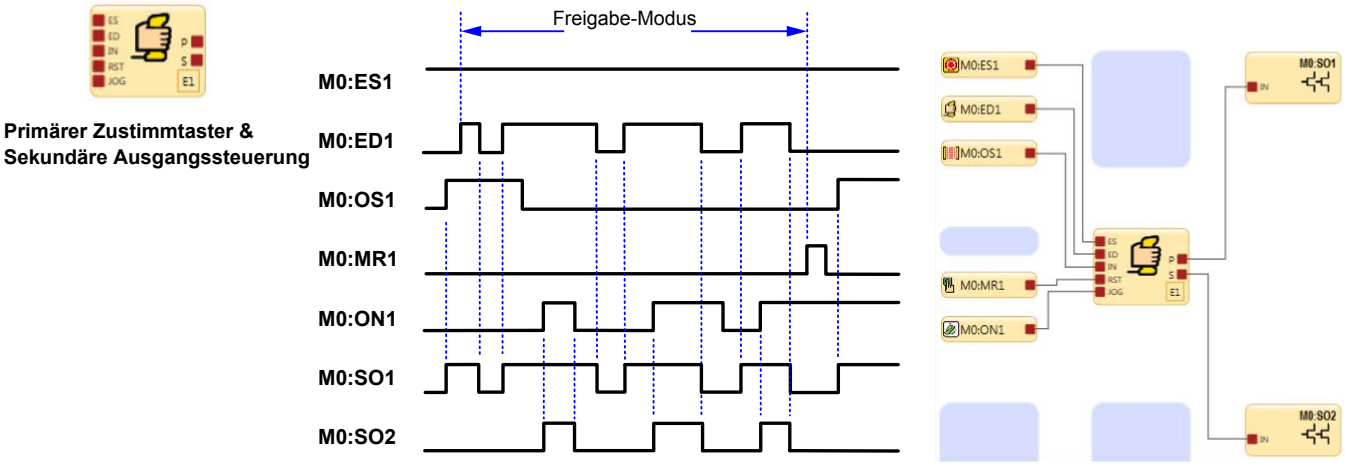



*Abbildung 113. Zeitablauf-Diagramm: Zustimmtaster*




E1-Freigabemodus startet, wenn der Zustimmtaster ED1 in den Ein-Zustand geschaltet wird.
ED1- und ES-Eingangsgeräte haben im Freigabemodus die Ein-/Aus-Steuerungshoheit.
Wenn MR1 für die Durchführung eines Reset verwendet wird, wird der normale Ein-Zustand wiederhergestellt und OS1 und ES1 haben die Ein-/Aus-Steuerungshoheit.

**Zum Beenden des Freigabe-Modus** muss sich der Zustimmtaster im Aus-Zustand befinden, und ein Zustimmtaster-Block-Reset muss durchgeführt werden.

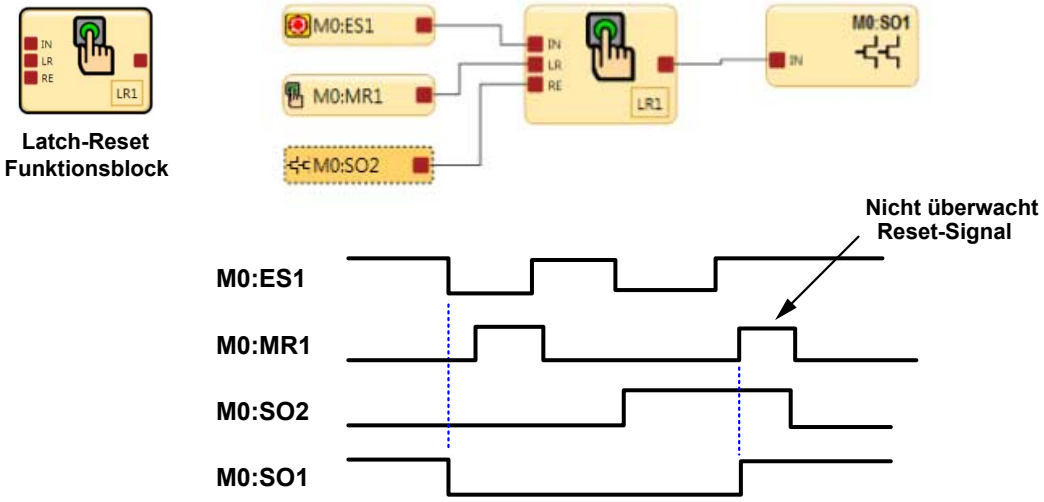
Als **Zeitlimit für den Zustimmtaster** kann ein Wert von 1 Sekunde (Standard) bis 30 Minuten eingestellt werden. Dieses kann nicht deaktiviert werden. Bei Ablauf des Zeitlimit schalten sich die zugehörigen Sicherheitsausgänge aus. Zum Starten eines neuen Zyklus des Freigabe-Modus bei einem Zeitlimit, das auf den Originalwert zurückgesetzt ist, muss sich der Zustimmtaster ein-, aus- und wieder einschalten.

Alle mit den Sicherheitsausgängen verbundenen Einschalt- und Ausschaltverzögerungszeiten, die durch die Zustimmtasterfunktion gesteuert werden, werden während des Freigabe-Modus berücksichtigt.

# 10.4 Latch-Reset-Block

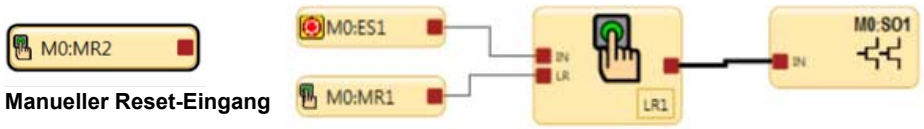
*Abbildung 114. Zeitablauf-Diagramm: Latch-Reset-Block*

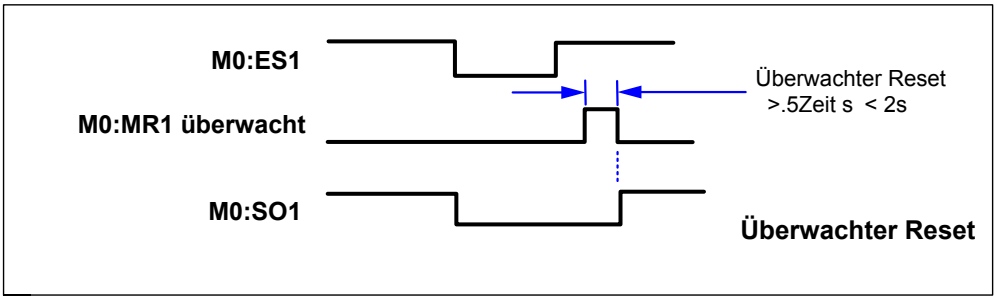
| Standardknoten | Zusätzliche Knoten | Anmerkungen |
|---|---|---|
| IN LR | RE | Der RE-Knoten (Reset aktivieren) kann zum Aktivieren oder Deaktivieren der Latch-Reset-Funktion verwendet werden. Befinden sich alle mit dem IN-Knoten verbundenen Eingangsgeräte im Ein-Zustand und ist das RE-Eingangssignal in Ein-Zustand, kann der LR-Funktionsblock manuell zurückgesetzt werden, damit sich sein Ausgang einschaltet. Siehe Abbildung 114 auf Seite 132; das Referenzsignal SO2 ist dabei mit dem RE-Knoten verbunden. |

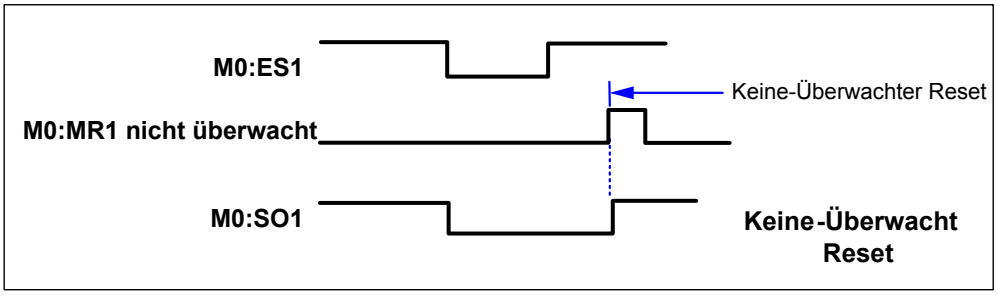



Der Latch-Reset-Funktionsblock LR1 schaltet seinen Ausgang und den Sicherheitsausgang SO1 aus, wenn der Not-Aus-Schalter in den Stoppzustand wechselt.
Der Verriegelung-aus-Zustand kann zurückgesetzt werden, wenn die Reset-Aktivierung RE von LR1 erfasst, dass sich das SO2-Referenzsignal im Ein-Zustand befindet, und für die Durchführung des Reset wird MR1 verwendet.

*Abbildung 115. Zeitablauf-Diagramm: Latch-Reset-Block, überwachter/nicht überwachter Reset*



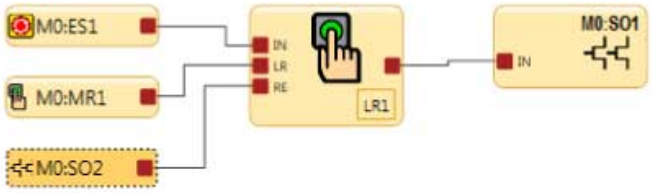

Das Eingangsgerät für manuellen Reset kann für eine oder zwei Arten von Reset-Signalen konfiguriert werden: Überwacht und Nicht überwacht

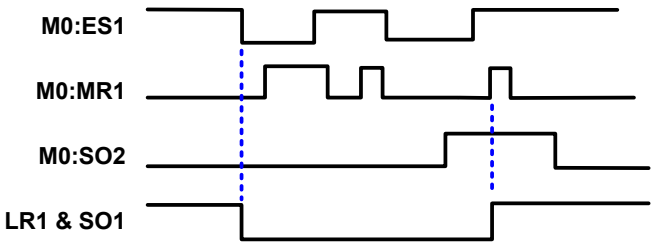
*Abbildung 116. Zeitablauf-Diagramm: Latch-Reset-Block und referenzierter Sicherheitsausgang*




**Referenzsignale**

Ein Referenzsignal dient zum:
- Steuern eines Ausgangs anhand des Status eines anderen Ausgangs
- Darstellen des Status eines Ausgangs, Eingangs, einer Sicherheitsfunktion oder eines Logikblocks auf einer anderen Seite.




Wenn Ausgang SO2 eingeschaltet ist, ist der Status des Referenzsignals SO2 Ein oder Hoch. Bei dem oben abgebildeten Funktionsblock ist das Referenzsignal SO2 mit dem Reset-Aktivierungsknoten RE von Latch-Reset-Block LR1 verbunden.

Ein Reset (Einschalten) von LR1 ist nur möglich, wenn sich ES1 im Ein-Zustand befindet und SO2 eingeschaltet ist.

Zur Verwendung der referenzierten Sicherheitsausgänge siehe Referenzsignale auf Seite 127.

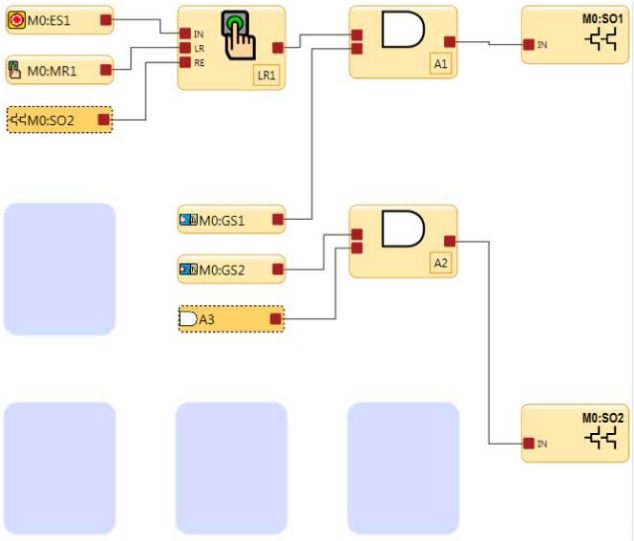
*Abbildung 117. Latch-Reset und referenzierter Sicherheitsausgang und AND-Block*




**Referenzsignale**

In der nachfolgenden Abbildung befindet sich das Referenzsignal A3 auf Seite 1 des Funktionsblockdiagramms, und der A3 AND-Block befindet sich auf Seite 2. Der Ausgangsknoten auf dem A3 AND-Block kann auch auf Seite 2 für eine andere Sicherheitssteuerungslogik verwendet werden.

**Referenzsignal A3 auf Seite 1**




**AND-Logikblock A3 auf Seite 2**

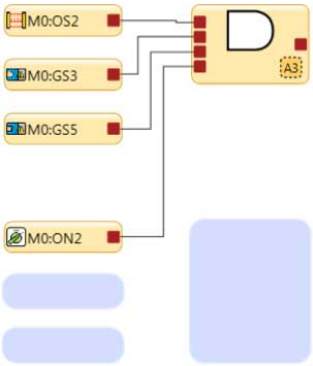
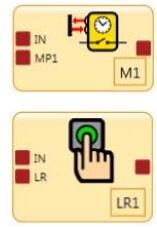
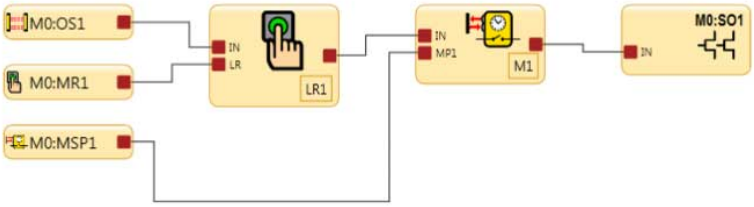
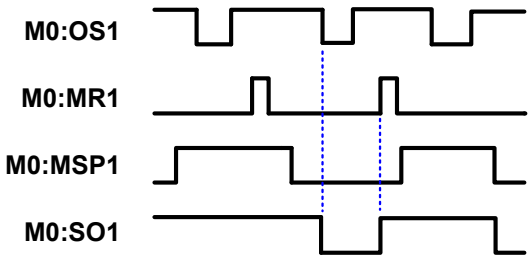


*Abbildung 118. Zeitablauf-Diagramm: Latch-Reset-Block und Muting-Block*




**Latch-Reset Muting-Funktion**



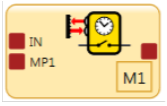




Wenn OS1 für eine Schutzeinrichtung in einem gültigen Muting-Zyklus in einen Stoppzustand übergeht, wird der Latch-Reset-Funktionsblock verriegelt, und ein Reset-Signal ist erforderlich, damit SO1 nach dem Ende des Mutings eingeschaltet bleibt.
Wenn OS1 in einem gültigen Muting-Zyklus in den Stoppzustand schaltet und kein Reset-Signal erfasst wird, schaltet sich SO1 nach dem Ende des Mutings aus.

## 10.5 Muting-Block

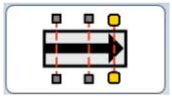
*Abbildung 119. Muting-Block: Funktionsarten*

| Standardknoten | Zusätzliche Knoten | Anmerkungen |
|---|---|---|
| IN MP1 | ME BP MP2 | Die Eingangsblöcke für Muting-Sensorpaare müssen direkt mit dem Muting-Funktionsblock verbunden werden. |

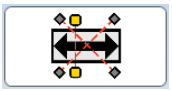



**Muting-Funktionsblock**

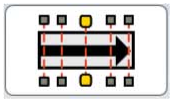
Unten sind fünf Muting-Funktionsarten aufgeführt. Die folgenden Zeitablauf-Diagramme zeigen das Funktionsdetail und die Reihenfolge der Statuswechsel der Sensoren/Schutzeinrichtungen für jede Muting-Funktionsart.



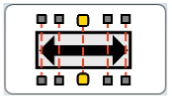
**1-Weg – 1 Muting-Sensorpaar**



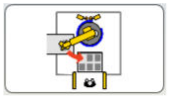
**2-Wege – 1 Muting-Sensorpaar**



**1-Weg – 2 Muting-Sensorpaare**

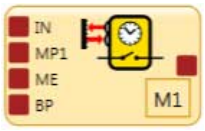


**2-Wege – 2 Muting-Sensorpaare**



**2-Wege – 1 Muting-Sensorpaar**

*Abbildung 120. Muting-Block: Optionen für den Überbrückungs-/Override-Modus*




Es gibt zwei Arten von Muting-Überbrückungen:
- Muting-abhängiges Override
- Überbrückung (normal)

Im Menü Muting-Block-Eigenschaften in den Erweiterten Einstellungen ist bei aktiviertem Kontrollkästchen für Überbrückung die Option zum Auswählen einer Überbrückung oder eines Muting-abhängigen Override möglich.

Das Muting-abhängige Override dient zum vorübergehenden Neustarten eines unvollständigen Muting-Zyklus (z. B. nachdem das Muting-Zeitlimit abgelaufen ist). In diesem Fall muss mindestens ein Muting-Sensor aktiviert werden, während sich die Schutzeinrichtung im Stoppzustand befindet.

Die normale Überbrückung dient der vorübergehenden Umgehung der Schutzeinrichtung, um den Ausgang des Funktionsblocks einzuschalten oder damit dieser eingeschaltet bleibt.

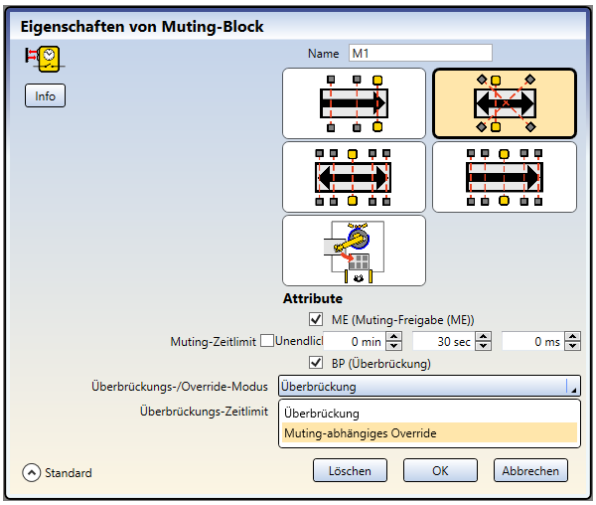



*Abbildung 121. Muting-abhängiges Override*

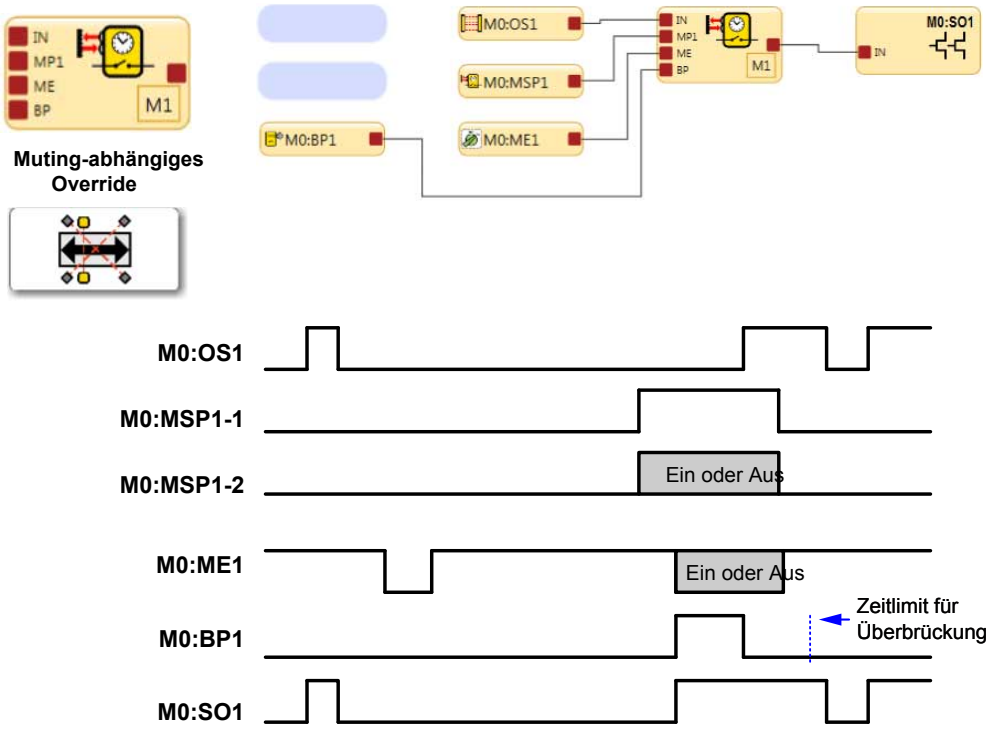


*Abbildung 122. Muting-Überbrückung*

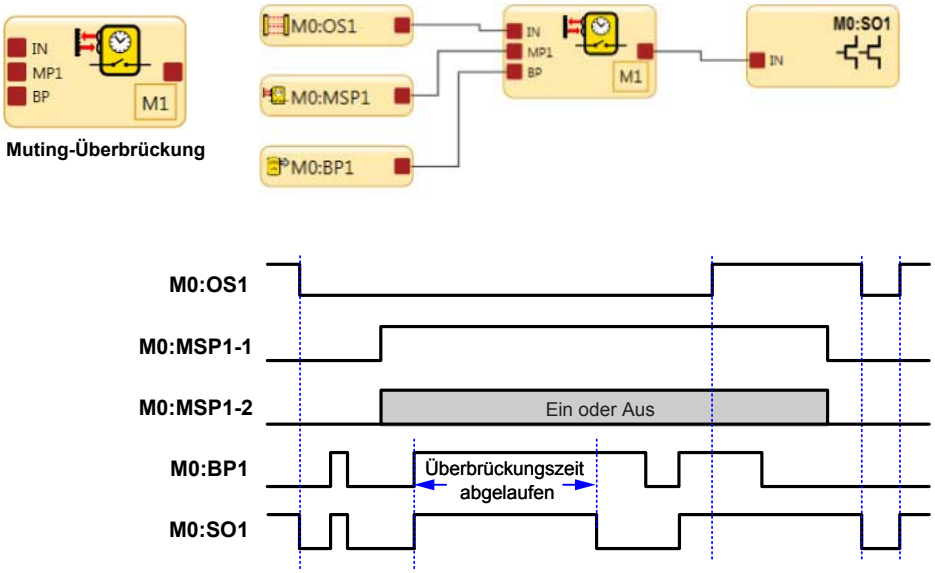
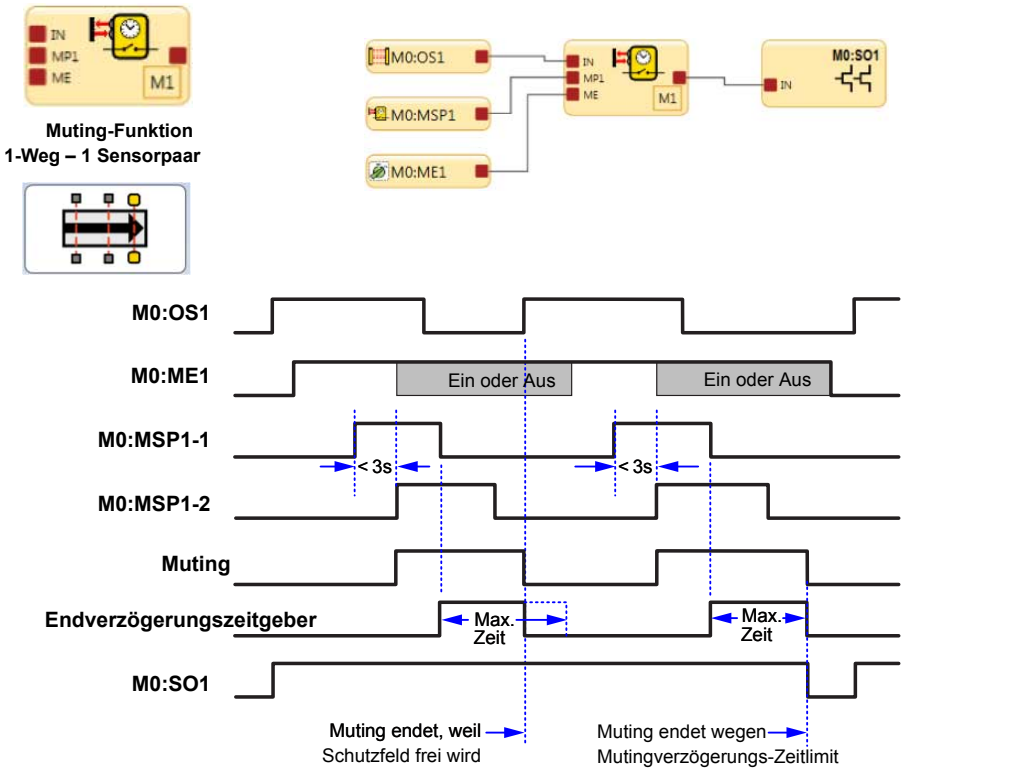



*Abbildung 123. Zeitablauf-Diagramm: Unidirektionaler Muting-Block, ein Muting-Sensorpaar*




**Hinweis:** MO:OS1 muss blockiert werden, bevor entweder MSP1-1 oder MSP1-2 frei wird.

*Abbildung 124. Zeitablauf-Diagramm: Unidirektionaler Muting-Block, zwei Muting-Sensorpaare*

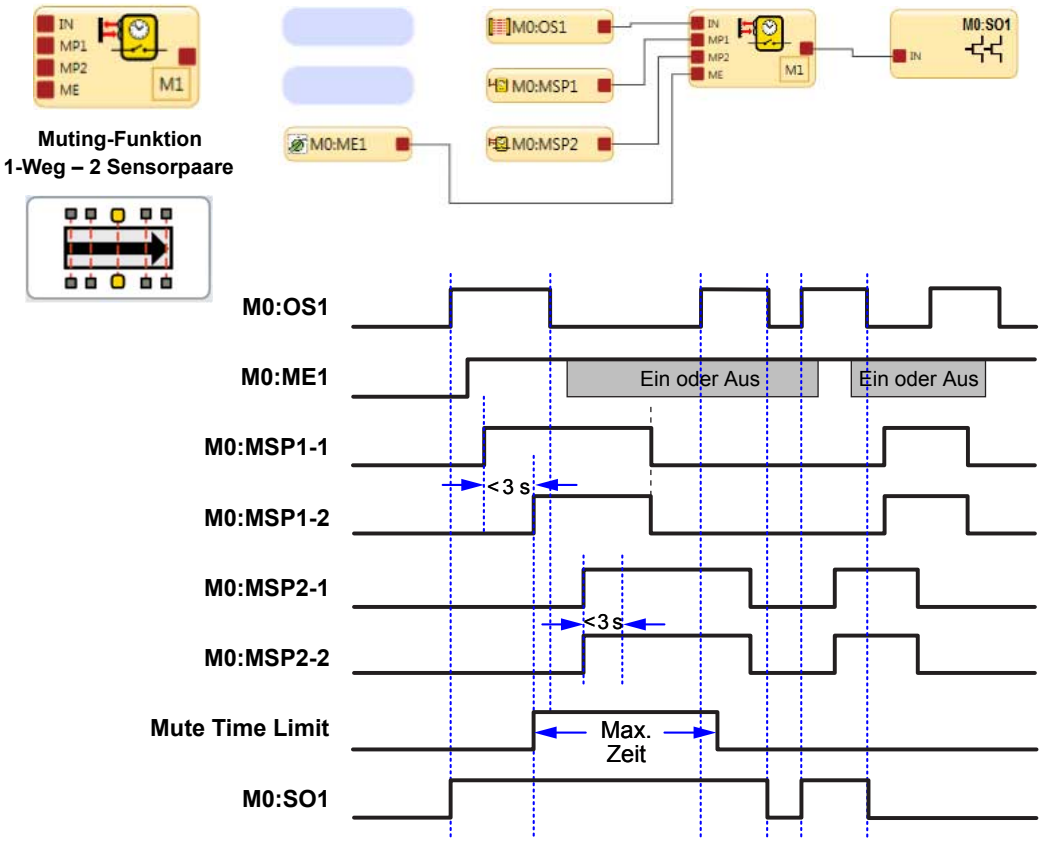



*Abbildung 125. Zeitablauf-Diagramm: Bidirektionaler Muting-Block, ein Muting-Sensorpaar*

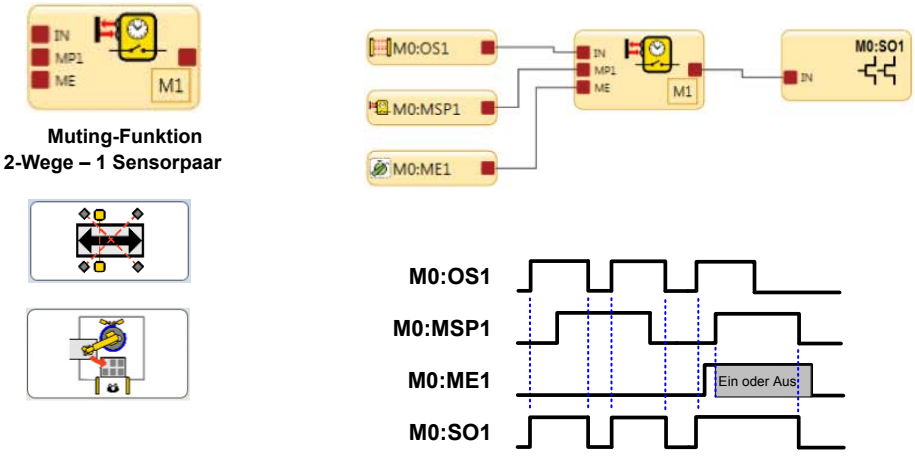


*Abbildung 126. Zeitablauf-Diagramm: Bidirektionaler Muting-Block, zwei Muting-Sensorpaare*

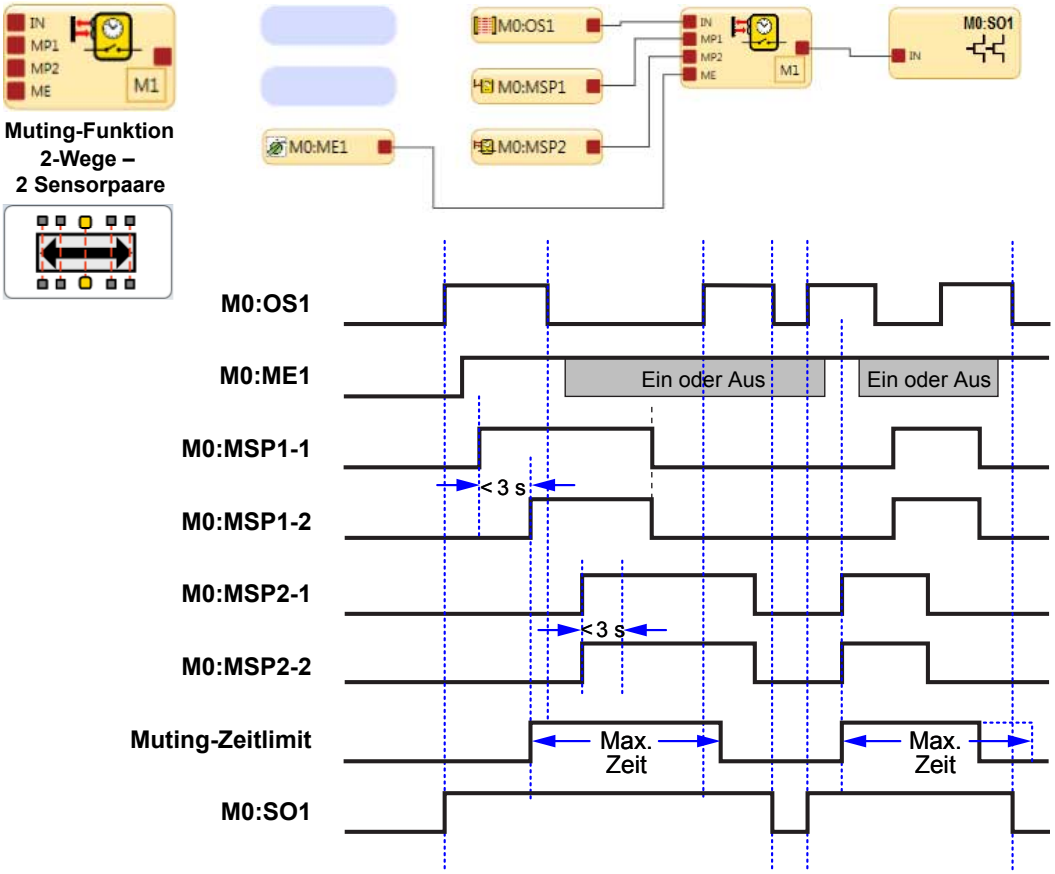
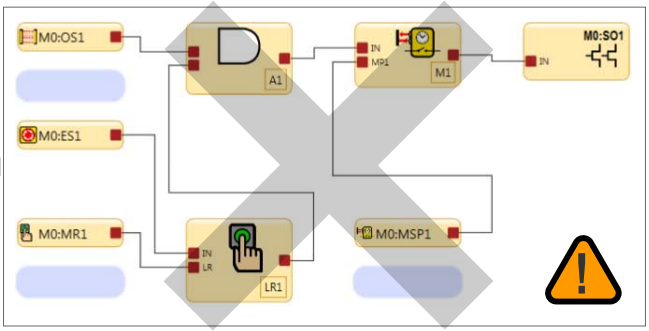



*Abbildung 127. Not-Aus-Schalter und Muting-Funktion*

## WICHTIG Not-Aus-Steuerungshoheit bei Verwendung der Muting-Funktion

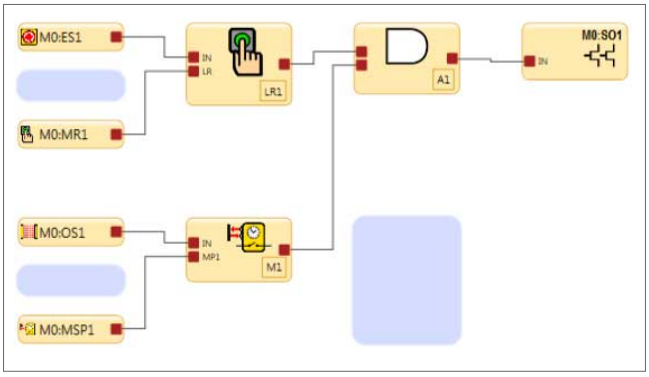
**Falsche Not-Aus-Steuerung**
**NICHT EMPFOHLEN**
Die Konfiguration oben rechts zeigt OS1 und den Not-Aus-Schalter ES1 mit einem Latch-Reset LR1, der über die AND-Funktion mit einer Muting-Funktion verbunden ist. In diesem Fall werden ES1 und OS1 beide gemutet.

Wenn ein aktiver Muting-Zyklus läuft und der Not-Aus-Schalter betätigt (in den Stoppzustand geschaltet) wird, schaltet sich SO1 nicht aus. Dies führt zu einem Verlust der Sicherheitssteuerung und kann eine potenzielle Gefahrsituation bewirken.




**Richtige Not-Aus-Steuerung**
Bei der Konfiguration rechts ist OS1 direkt mit dem Muting-Block M1 verbunden. M1 und ES1 sind beide Eingänge für AND A1. In diesem Fall steuern M1 und ES1 beide SO1.

Wenn ein aktiver Muting-Zyklus läuft und der Not-Aus-Schalter betätigt (in den Stoppzustand geschaltet) wird, schaltet sich SO1 aus.



Nothaltschalter, Seilzugschalter, Zustimmtaster, externe Geräteüberwachung und Überbrückungsschalter sind keine mutingfähigen Vorrichtungen bzw. Funktionen.

Zum Muting der primären Schutzeinrichtung muss ein Muting-System:

1. den ungefährlichen Teil des Maschinenzyklus erkennen,
2. die Auswahl der richtigen Muting-Vorrichtungen einbeziehen,
3. die richtige Montage und Installation solcher Vorrichtungen einschließen,

**WARNUNG:**

- **Muting und Überbrückungen so verwenden, dass das Risiko für das Personal minimal gehalten wird.**
- Wenn diese Regeln nicht befolgt werden, kann ein gefährlicher Zustand entstehen, der zu schweren oder tödlichen Verletzungen führen könnte.
- Schutz gegen unbeabsichtigte Aufhebung von Stoppsignalen durch Verwendung eines oder mehrerer divers-redundanter Muting-Sensorpaare oder eines zweikanaligen Überbrückungsschalters mit Sicherheitsschlüssel.
- Konfigurieren angemessener Zeitlimits für die Muting- und Überbrückungsfunktion.

Der Sicherheitskontroller kann redundante Signale überwachen, die das Muting initiieren, und darauf reagieren. Das Muting unterbricht dann die Schutzfunktion, indem der Zustand des Eingangsgeräts, dem die Muting-Funktion zugeordnet ist, ignoriert wird. Hierdurch ist es möglich, dass ein Objekt oder eine Person das Schutzfeld eines Sicherheits-Lichtvorhangs passieren kann, ohne einen Stopp-Befehl auszulösen. Dies ist nicht mit Ausblendung zu verwechseln, bei der Strahlen in einem Sicherheits-Lichtvorhang deaktiviert werden, sodass die Auflösung vergrößert wird.

Die Muting-Funktion kann durch diverse externe Geräte ausgelöst werden. Diese Funktion bietet diverse Optionen für die genaue Abstimmung des Systems auf die Anforderungen einer spezifischen Anwendung.

Ein Muting-Vorrichtungspaar muss gleichzeitig ausgelöst werden (im Abstand von maximal 3 Sekunden). Dadurch verringert sich die Wahrscheinlichkeit eines Gleichtaktfehlers oder einer absichtlichen Umgehung. Direktionales Muting, bei dem das Sensorpaar 1 zuerst gesperrt werden muss, kann ebenfalls die Möglichkeit einer Umgehung reduzieren.

Mindestens zwei Muting-Sensoren sind für jeden Muting-Vorgang erforderlich. Das Muting tritt in der Regel 100 ms nach der Betätigung des zweiten Muting-Sensoreingangs ein. Ein oder zwei Muting-Sensorpaare können einem oder mehreren Sicherheitseingangsgeräten zugeordnet werden. Dadurch können die zugehörigen Sicherheitsausgänge eingeschaltet bleiben, um den Vorgang abzuschließen.

**WARNUNG: Einschränkungen hinsichtlich der Muting-Funktion**

Muting ist nur während des ungefährlichen Teils des Maschinenzyklus zugelassen.

Eine Muting-Anwendung muss so ausgelegt werden, dass der Ausfall einer einzelnen Komponente den Stoppbefehl nicht verhindert oder weitere Maschinenzyklen ermöglicht, solange der Fehler nicht behoben wurde.

**WARNUNG: Muting-Eingänge müssen redundant sein**

**Es ist nicht zulässig, einen einzelnen Schalter, ein einzelnes Gerät oder ein einzelnes Relais mit zwei Schließerkontakten für die Muting-Eingänge zu verwenden.** Dieses einzelne Gerät mit mehreren Ausgängen könnte ausfallen und Muting des Systems zu einem falschen Zeitpunkt verursachen. **Dadurch kann eine gefährliche Situation entstehen.**

## 10.5.1 Optionale Muting-Attribute

Der Eingang für das Muting-Sensorpaar und der Muting-Block haben diverse optionale Funktionen, mit denen die Möglichkeit einer unbefugten Manipulation und eines unbeabsichtigten Muting-Zyklus minimiert werden kann.

### Muting-Freigabe (ME)

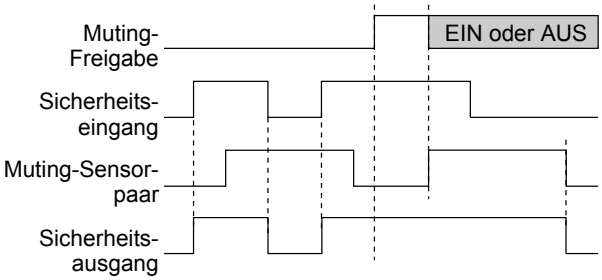
Der Eingang für die Muting-Aktivierung ist als nicht sicherheitsrelevant spezifiziert. Wenn der Eingang geschlossen oder für einen virtuellen Eingang aktiviert ist, lässt der Kontroller ein Muting zu. Öffnen des Eingangs während eines Mutings hat keine Auswirkung.

Typische Anwendungen für die Muting-Aktivierung sind unter anderem:

- Um der Maschinensteuerungslogik zu ermöglichen, einen Zeitraum für den Beginn des Muting zu erzeugen
- Um zu verhindern, dass Muting eintreten kann
- Um die Wahrscheinlichkeit unbefugter oder unbeabsichtigter Umgehung des Sicherheitssystems zu mindern

Die optionale Muting-Aktivierungsfunktion (ME) kann konfiguriert werden, um sicherzustellen, dass eine Muting-Funktion nur zum passenden Zeitpunkt zugelassen wird. Wenn ein ME-Eingangsgerät einem mutingfähigen Sicherheitseingang zugeordnet wurde, kann dieser Sicherheitseingang nur gemutet werden, wenn sich der ME-Schalter zum Zeitpunkt des Anlaufs des Muting-Zyklus im aktivierten Zustand (24 V DC) befindet (bzw. im Falle eines virtuellen Eingangs im aktiven Zustand). Ein ME-Eingangsgerät kann einem oder mehreren Mutingblöcken zugeordnet werden.

*Abbildung 128. Zeitgebungslogik: ein Muting-Sensorpaar mit Muting-Freigabe*




### Reset-Funktion für Simultanitäts-Zeitgeber

Der Eingang für die Muting-Aktivierung kann auch verwendet werden, um den Gleichzeitigkeits-Zeitgeber der Muting-Sensoreingänge zurückzusetzen. Wenn ein Eingang länger als 3 Sekunden aktiv ist, bevor der zweite Eingang aktiv wird, verhindert der Gleichzeitigkeits-Zeitgeber, dass ein Muting-Zyklus eintreten kann. Das kann durch das normale Anhalten eines Montagebands bedingt sein, wodurch eine Muting-Vorrichtung blockiert und die Zeit des Gleichzeitigkeits-Zeitgebers abläuft.

Wenn der ME-Eingang schaltet (geschlossen-offen-geschlossen bzw. im Falle eines virtuellen Eingangs aktiviert-deaktiviert-aktiviert), während ein Muting-Eingang aktiv ist, wird der Simultanitäts-Zeitgeber zurückgesetzt, und wenn der zweite Muting-Eingang innerhalb von 3 Sekunden aktiv wird, beginnt ein normaler Muting-Zyklus. Die Funktion kann den Zeitgeber nur einmal pro Muting-Zyklus zurücksetzen (das heißt, alle Muting-Eingänge M1–M4 müssen öffnen, bevor ein weiterer Reset erfolgen kann).

## Überbrückung

Ein optionaler **Überbrückungs-/Override-Modus** kann aktiviert werden. Hierzu wird das Feld **Überbrückung** im Fenster mit Eigenschaften für **Muting-Block** aktiviert. Zwei Überbrückungs-/Override-Modi stehen zur Verfügung: **Überbrückung** und **mutingabhängiges Override**. Der **Überbrückungsmodus** dient zur vorübergehenden Überbrückung der Schutzeinrichtung, damit der Ausgang des Funktionsblocks eingeschaltet bleibt oder eingeschaltet werden kann. Der **mutingabhängige Override-Modus** dient dazu, einen unvollständigen Muting-Zyklus manuell außer Kraft zu setzen (z. B. nachdem das Muting-Zeitlimit abgelaufen ist). In diesem Fall müssen zum Initiieren des Override Muting-Sensoren aktiviert werden, während sich die Schutzeinrichtung im Aus-Zustand befindet.

## Muting-Lampenausgang (ML)

Je nach der Risikobeurteilung und den geltenden Normen ist es für einige Anwendungen erforderlich, dass eine Leuchte (oder ein anderes Mittel) anzeigt, wenn die Sicherheitsvorrichtung (z. B. ein Lichtvorhang) gemutet ist. Der Sicherheitskontroller gibt über den Muting-Statusausgang ein Signal aus, welches besagt, dass die Schutzfunktion vorübergehend aufgehoben ist.

**Wichtig: Anzeige für Muting-Status**

Eine Anzeige für den gemuteten Status der Sicherheitsvorrichtung muss eingerichtet werden und vom Standort der gemuteten Sicherheitsvorrichtung gut sichtbar sein. Der Betrieb der Anzeige muss möglicherweise in geeigneten Intervallen vom Bediener überprüft werden.

## Muting-Zeitlimit

Das Muting-Zeitlimit ermöglicht die Einstellung einer maximalen Zeitspanne, während der das Muting zugelassen sein soll. Diese Funktion verhindert die absichtliche Umgehung der Mute-Sensoren zur Initiierung eines unangebrachten Mutings. Sie ist auch sinnvoll zur Erkennung eines Gleichtaktfehlers, der alle Mute-Sensoren der Anwendung beeinträchtigen würde. Es kann ein Zeitlimit von 1 s bis 30 min in 100-Millisekunden-Schritten eingestellt werden (Die Werkseinstellung beträgt 30 s). Für das Muting-Zeitlimit kann auch die Einstellung **Unendlich** (deaktiviert) gewählt werden.

Die Überwachungszeit wird gestartet, wenn das zweite Mute-Sensor Paar die Gleichzeitigkeitsanforderung erfüllt (innerhalb von 3 Sekunden nach Betätigung des ersten Sensorpaares). Wenn die Zeit abgelaufen ist, endet das Muting ungeachtet der Signale von den Mute-Sensoren. Wenn das gemutete Eingangsgerät im Aus-Zustand ist, schaltet der zugehörige Muting-Block aus.

**WARNUNG: Muting-Zeitlimit**. Für das Muting-Zeitlimit sollte nur dann eine endliche Zeit gewählt werden (deaktiviert), wenn die Möglichkeit eines fehlerhaften oder ungewollten Muting-Zyklus entsprechend der Risikobeurteilung der Maschine minimal gehalten wird. Der Anwender trägt die Verantwortung dafür, dass hierdurch keine gefährliche Situation erzeugt wird.

## Muting-Ausschaltverzögerungszeit

Eine Verzögerungszeit kann konfiguriert werden, um den Muting-Zustand bis zur gewählten Zeit zu verlängern (1, 2, 3, 4 oder 5 Sekunden), nachdem das Muting-Sensorpaar keinen Muting-Zustand mehr signalisiert. Die Ausschaltverzögerung wird normalerweise für Sicherheits-Lichtvorhänge bzw. Mehrstrahlsysteme bei reinen Arbeitszellen-Ausgangsanwendungen verwendet, bei denen sich die Muting-Sensoren nur auf einer Seite des Schutzfelds befinden. Der Muting-Blockausgang bleibt bis zu 5 Sekunden lang eingeschaltet, nachdem die erste Muting-Vorrichtung freigegeben wurde, oder bis das gemutete Sicherheitseingangsgerät (Muting-Block-Eingang) wieder in den Ein-Zustand wechselt, wobei das jeweils erste Ereignis ausschlaggebend ist.

## Muting bei Anlauf

Diese Funktion initiiert einen Muting-Zyklus, nachdem die Stromzufuhr zum Sicherheitskontroller verbunden wurde. Ist die Muting-bei-Anlauf-Funktion gewählt, wird unter folgenden Bedingungen ein Muting initiiert:

- Wenn der Muting-Aktivierungseingang eingeschaltet ist (sofern konfiguriert)
- Wenn die Eingänge der Sicherheitsvorrichtung aktiviert sind (im Ein-Zustand)
- Wenn die Muting-Sensoren M1-M2 (bzw. M3-M4, sofern verwendet, aber nicht alle vier) geschlossen sind

Wenn **automatische Netzeinschaltung** konfiguriert ist, lässt der Sicherheitskontroller den Eingangsgeräten ca. 2 Sekunden Zeit zur Aktivierung, damit Systeme unterstützt werden, die nicht unmittelbar beim Anlauf aktiv sind.

Wenn **manuelle Netzeinschaltung** konfiguriert ist und alle anderen Bedingungen erfüllt sind, führt der erste gültige Anlauf-Reset, nachdem die gemuteten Sicherheitseingänge aktiviert wurden (Ein-Zustand oder geschlossen), zu einem Muting-Zyklus. Die Funktion Muting bei Anlauf sollte nur verwendet werden, wenn die Sicherheit des Systems bei erwartetem Muting-Zyklus garantiert werden kann, und wenn die Verwendung dieser Funktion das Ergebnis einer Risikobeurteilung und für den Betrieb der jeweiligen Maschine erforderlich ist.

**WARNUNG:** Die Funktion Muting bei Anlauf sollte nur bei Anwendungen verwendet werden, bei denen:

- Muting des Systems (M1 und M2 geschlossen) beim Anlauf erforderlich ist und
- dadurch unter keinen Umständen Gefahren für Personen entstehen.

## Entprellzeiten für Muting-Sensorpaar

Anhand der Eingangs-Entprellzeiten, die unter den **Erweiterten** Einstellungen im Fenster mit Eigenschaften für das **Muting-Sensorpaar** konfiguriert werden können, kann ein Muting-Zyklus über das Entfernen des Muting-Sensorsignals hinaus verlängert werden. Durch die Konfiguration der Ausschaltentprellzeit kann der Muting-Zyklus um bis zu 1,5 Sekunden (1500 ms) verlängert werden, damit sich das Sicherheitseingangsgerät einschalten kann. Ebenso kann auch der Start des Muting-Zyklus durch Konfigurieren der Einschaltverzögerungszeit verzögert werden.

### Anforderungen an die Muting-Funktion

Anfang und Ende eines Muting-Zyklus werden durch Signale von einem Muting-Vorrichtungspaar ausgelöst. Die Schaltungsoptionen für die Muting-Vorrichtung sind konfigurierbar und werden im Fenster **Eigenschaften** für das Muting-Sensorpaar angezeigt. Ein ordnungsgemäßes Muting-Signal kommt zustande, wenn beide Kanäle der Muting-Vorrichtung in den Muting-Aktiv-Zustand wechseln, während sich die gemutete Schutzeinrichtung im Ein-Zustand befindet.

Der Sicherheitskontroller überwacht die Muting-Vorrichtungen um sicherzustellen, dass ihre Ausgänge innerhalb von 3 Sekunden einschalten. Wenn die Eingänge diese Simultanitätsanforderung nicht erfüllen, kann kein Muting erfolgen.

Es können verschiedene Arten und Kombinationen von Muting-Vorrichtungen verwendet werden, unter anderem: optoelektronische Sensoren, induktive Näherungssensoren, Grenzschalter, zwangsgeführte Sicherheitsschalter und Whisker-Schalter.

### Umlenkspiegel, optische Sicherheitssysteme und Muting

Spiegel werden gewöhnlich mit Sicherheits-Lichtvorhängen und Einzel-/Mehrstrahl-Sicherheitssystemen eingesetzt, um das Schutzfeld von mehreren Seiten zu schützen. Wenn der Sicherheits-Lichtvorhang gemutet ist, wird die Schutzfunktion auf allen Seiten aufgehoben. Es darf für Personen nicht möglich sein, unbemerkt und ohne Ausgabe eines Stoppbefehls an die Maschinensteuerung in das Schutzfeld einzudringen. Diese zusätzliche Schutzeinrichtung wird normalerweise durch Zusatzvorrichtungen bereitgestellt, die während des Mutings der primären Schutzeinrichtung aktiv bleiben. Daher sind Spiegel für Anwendungen mit Muting gewöhnlich nicht zulässig.

### Mehrere Sicherheitsvorrichtungen mit Anwesenheitserkennung

Muting von mehreren Sicherheitsvorrichtungen mit Anwesenheitserkennung (PSSDs) oder eines PSSD mit mehreren Erfassungsbereichen wird nicht empfohlen, wenn eine Person in den überwachten Bereich treten kann, ohne erfasst zu werden und ohne dass ein Stoppbefehl an die Maschinensteuerung gesendet wird. Wenn wie bei der Verwendung von Umlenkspiegeln (siehe Umlenkspiegel, optische Sicherheitssysteme und Muting auf Seite 142) an mehreren Erfassungsbereichen ein Muting durchgeführt wird, besteht die Möglichkeit, dass Personen durch einen dem Muting unterliegenden Bereich oder Zugangspunkt in den geschützten Bereich treten können, ohne erfasst zu werden.

Wenn zum Beispiel bei einer Eintritts-/Austritts-Anwendung, in der durch eine in eine Zelle eintretende Palette der Muting-Zyklus initiiert wird, sowohl an den Eintritts- wie auch an den Austritts-PSSDs ein Muting durchgeführt wird, kann eine Person durch den „Austritt“ aus der Zelle in den überwachten Bereich treten. Eine geeignete Lösung des Problems wäre das Muting von Ein- und Austritt mit separaten Schutzeinrichtungen.

**WARNUNG: Sicherung mehrerer Bereiche**

**Es ist nicht zulässig, mehrere Bereiche mit Spiegeln oder durch mehrere Erfassungsfelder zu sichern, wenn das Personal während eines System-Mutings in den gefährlichen Bereich eintreten kann und nicht durch eine zusätzliche Schutzeinrichtung erfasst wird, die einen Stoppbefehl an die Maschine schickt.**

## 10.6 One-Shot-Block (XS/SC26-2 ab FID 4)

Mit dem One-Shot-Block können Benutzer einen impulsgesteuerten Ein-Zustand von bis zu 5 Minuten in 1-ms-Schritten konfigurieren.

| Standardknoten | Zusätzliche Knoten | Anmerkungen |
|---|---|---|
| IN | CD | Ein Statuswechsel des Eingangssignals von Niedrig zu Hoch bewirkt, dass der Ausgangsknoten für die konfigurierte Zeit zu Hoch wechselt und sich dann ausschaltet. |

**Anmerkung:** Die tatsächliche One-Shot-Dauer kann bis zu 1 Scanzeit länger als die eingestellte Zeit sein.

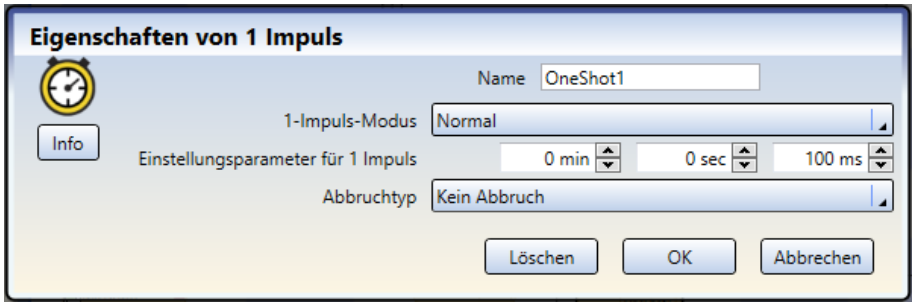
Der Abbruchverzögerungsknoten ist ein konfigurierbarer Knoten für den One-Shot-Funktionsblock. Der Abbruchverzögerungseingang schaltet den Ausgangsknoten des One-Shot-Funktionsblocks sofort ab, nachdem er erkannt wurde (aufgrund menschlicher und systembedingter Verzögerungen werden kürzere One-Shots höchstwahrscheinlich beendet, bevor eine Abbruchverzögerung in Kraft treten kann).

**VORSICHT:** Auswirkung der One-Shot-Verzögerungszeit auf die Ansprechzeit

Der One-Shot-Zeitverlauf kann die Ansprechzeit der Sicherheitssteuerung erheblich verlangsamen. Dies wirkt sich auf die Stellung der Schutzeinrichtungen aus, deren Installation sich nach den Formeln für (Mindest-)Sicherheitsabstand richtet oder anderweitig von der Zeitberechnung für das Erreichen eines nicht gefährlichen Zustands beeinflusst wird. Bei der Installation der Schutzeinrichtungen muss der Anstieg der Ansprechzeit berücksichtigt werden.

**Anmerkung:** Die auf der Registerkarte „Configuration Summary (Konfigurationsübersicht)“ angegebene Ansprechzeit ist eine maximale Zeit. Diese kann sich je nach der Verwendung der Verzögerungsblöcke, One-Shot-Blöcke oder anderer logischer Blöcke (z. B. ODER-Funktionen) ändern. Es liegt in der Verantwortung des Anwenders, die korrekte Ansprechzeit zu ermitteln, zu überprüfen und einzurechnen.

*Abbildung 129. **One-Shot-Eigenschaften***




Über das Fenster „One Shot Properties (One-Shot-Eigenschaften)“ kann der Anwender folgende Einstellungen konfigurieren:

**Name**

Einen bis zu 10 Zeichen langen Namen für den Funktionsblock erstellen

**1-Impuls-Modus**

- Normal
- Puls

**Einstellungsparameter für One-Shot**

One Shot Time (One-Shot-Zeit): 1 ms bis 5 Minuten, in 1-ms-Schritten

Standardeinstellung ist 100 ms.

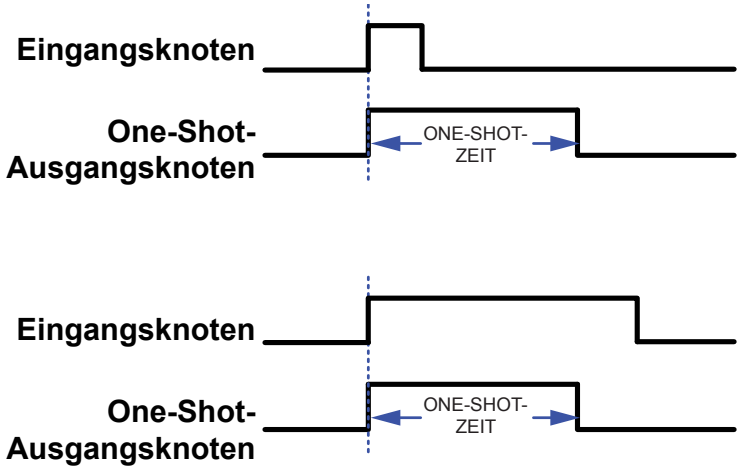
**Abbruchtyp**

- Kein Abbruch
- Abbruchverzögerungsknoten

### 1-Impuls-Modus

Wenn der Normal-Modus gewählt ist, wird der Ausgangsknoten eingeschaltet, wenn der Eingangsknoten eingeschaltet wird. Der Ausgang bleibt für die für die One-Shot-Einstellung eingestellte Zeit eingeschaltet, unabhängig von Zustandsänderungen des Eingangs. (Zeitverlaufsdiagramme mit typischen One-Shot-Zeiten im Normal-Modus finden Sie unter Abbildung 130 auf Seite 144.)

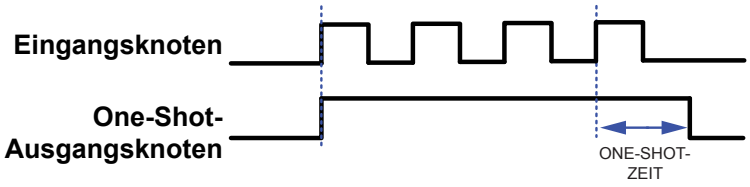
*Abbildung 130. Zeitverlaufsdiagramme mit typischen One-Shot-Zeiten im Normal-Modus*




**Anmerkung:** Die Einschaltzeit des Sicherheitsausgangs wird durch die Einschaltverzögerung des Sicherheitsausgangs reduziert (ca. 60 ms). Je kürzer die One-Shot-Zeit, desto ausgeprägter ist die Reduktion (größerer Prozentsatz des gewünschten Impulses).

Wenn der Heartbeat-Modus ausgewählt ist, wird der Ausgangsknoten eingeschaltet, wenn der Eingangsknoten eingeschaltet wird. Der Ausgang bleibt für die für die One-Shot-Einstellung festgelegte Zeit eingeschaltet. Beim Aus- und Wiedereinschalten des Eingangsknotens wird der für den One-Shot eingestellte Timer zurückgesetzt. (Ein Zeitverlaufsdiagramm mit typischen One-Shot-Zeiten im Heartbeat-Modus finden Sie unter Abbildung 131 auf Seite 144.)

*Abbildung 131. Zeitverlaufsdiagramm mit One-Shot-Zeiten im Heartbeat-Modus*




## 10.7 Pressensteuerung (XS/SC26-2 ab FID 4)

Der Pressensteuerungs-Funktionsblock ist für den Einsatz mit einfachen hydraulischen/pneumatischen motorgetriebenen Pressen konzipiert.

Es gelten die folgenden Standards:

B11.2-2013, Safety Requirements for Hydraulic and Pneumatic Power Presses (Sicherheitsanforderungen für hydraulische und pneumatische Pressen)
DIN EN ISO 16092-1:2018, Werkzeugmaschinen-Sicherheit – Pressen – Teil 1: Allgemeine Sicherheitsanforderungen
DIN EN ISO 16092-3, Werkzeugmaschinen-Sicherheit – Pressen – Teil 3: Sicherheitsanforderungen für hydraulische Pressen
EN ISO 16092-4, Werkzeugmaschinen – Sicherheit von Pressen – Teil 4: Pneumatische Pressen

Es liegt in der alleinigen Verantwortung des Anwenders, sicherzustellen, dass die Anwendung mit diesen und allen anderen geeigneten Standards (einschließlich weiterer Standards für Pressen) übereinstimmt.

**WARNUNG:**

- Der Pressensteuerungs-Funktionsblock enthält eine Startvorrichtung (initiiert eine gefährliche Bewegung).
- Wenn diese Anweisungen nicht befolgt werden, können schwere oder tödliche Verletzungen die Folge sein.
- Die sachkundige Person muss sicherstellen, dass die Aktivierung (Wechsel in einen eingeschalteten Zustand) einer Sicherheitsstoppvorrichtung (Nothaltschalter, Seilzugschalter, optischer Sensor, Sicherheitsmatte, Schutzhalt usw.) durch einen Anwender keine gefährliche Bewegung initiiert, wenn diese mit einem Pressensteuerungs-Funktionsblock verbunden ist, der bereits aktiviert ist (eingeschalteter Zustand).

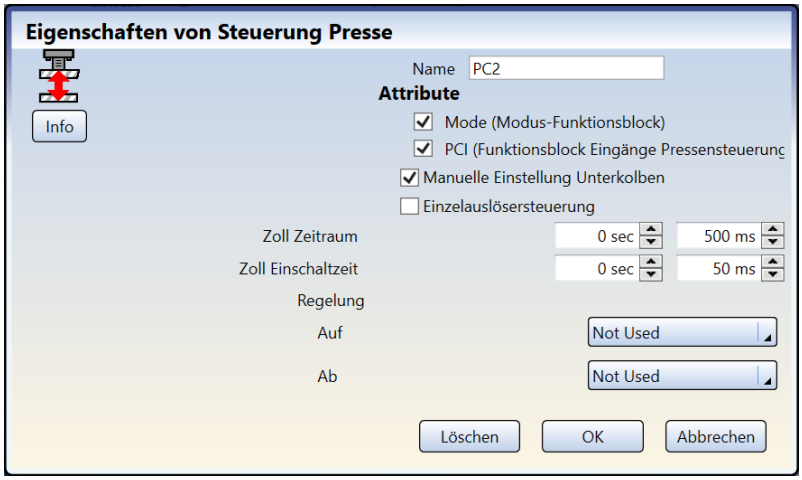
**WARNUNG:**

- Das Gerät korrekt installieren.
- Es liegt in der alleinigen Verantwortung des Anwenders, dafür zu sorgen, dass dieses Gerät der Banner Engineering von sachkundigen Personen installiert und an die zu überwachte Maschine angeschlossen wird und dass dabei die Anweisungen in diesem Handbuch und alle geltenden Sicherheitsvorschriften beachtet werden. Wenn diese Anweisungen nicht befolgt werden, können schwere oder tödliche Verletzungen die Folge sein.
- Werden nicht alle Verfahren bei der Montage, Installation, beim Anschließen und der Überprüfung vorschriftsmäßig eingehalten, so kann das Gerät der Banner Engineering nicht den Schutz bieten, für den es ausgelegt ist. Der Anwender ist für die Einhaltung aller lokalen und nationalen Gesetze, Vorschriften und Bestimmungen hinsichtlich der Installation und des Einsatzes dieses Steuersystems bei jeder individuellen Anwendung verantwortlich. Sämtliche rechtlichen Anforderungen müssen erfüllt und alle in dieser Anleitung enthaltenen technischen Installations- und Wartungsanweisungen müssen befolgt werden.

| Standardknoten | Zusätzliche Knoten | Anmerkungen |
|---|---|---|
| GO TOS BOS RST NM Sicherheit | Modus PCI | Bei der Auswahl des Modus- oder des PCI-Eingangs (Pressensteuerungseingang) erzeugt jeder Eingang einen eigenen Funktionsblock von Eingängen, die mit dem Pressensteuerungs-Funktionsblock verbunden sind. Weitere Informationen finden Sie unter Modus-Funktionsblock auf Seite 146 und Funktionsblock Pressensteuerungeingänge auf Seite 146. |

Der Pressensteuerungs-Funktionsblock enthält Attribute, die aktiviert oder deaktiviert werden können.

*Abbildung 132. **Eigenschaften der Pressensteuerung***




Die zusätzlichen Knoten, die dem Pressensteuerungs-Funktionsblock hinzugefügt werden können, erzeugen eigene neue Funktionsblöcke. Der Modus-Funktionsblock wird hinzugefügt, wenn das Modus-Attribut ausgewählt ist. Der Funktionsblock Pressensteuerungseingänge wird hinzugefügt, wenn das Feld „PCI-Attribut“ ausgewählt ist. Die beiden anderen Attribute, „Manual Upstroke Setting (Manuelle Einstellung Aufwärtshub)“ und „Single Actuator Control (Einzelauslösersteuerung)“, können nicht beide ausgewählt werden.

Wenn das Attribut „Manual Upstroke Setting (Manuelle Einstellung Aufwärtshub)“ konfiguriert ist, muss der GO-Eingang während des gesamten Zyklus (Abwärts- und Aufwärtsbewegung) eingeschaltet bleiben. An den GO-Eingangsknoten kann nur ein Zweihandsteuerungseingang oder ein Fußpedal-Eingang angeschlossen werden.

Wenn das Attribut „Single Actuator Control (Einzelauslösersteuerung)“ konfiguriert ist, verhält sich der GO-Eingang wie eine Starttaste, so dass er nur lange genug eingeschaltet bleiben muss, um den Prozess zu starten. An den GO-Eingangsknoten kann nur ein Zyklusinitiierungseingang, ein Fußpedal-Eingang oder ein Zweihandsteuerungseingang angeschlossen werden.

**WARNUNG:**
- Überlegungen zur Gefahr beim Aufwärtshub der Presse.
- Wenn während des Aufwärtshubs eine Gefahr besteht, kann die Nichtbeachtung der manuellen Aufwärtshub-Einstellung schwere bis tödliche Verletzungen zur Folge haben.
- Bei der Einzelauslösersteuerung darf der Aufwärtshub der Presse keine Gefährdung darstellen, da der mutingfähige Sicherheitsstopp-Eingang während des Aufwärtshubs gemutet wird.

Die andere Funktion im Pressensteuerungs-Funktionsblock ist der **Regelkreis**. Wenn der **Regelkreis** aktiviert wird, wird der Kontroller dadurch gezwungen, vor dem Einschalten des nächsten Ausgangs erst zu überprüfen, ob sich die an die angegebenen Ausgänge angeschlossenen Geräte ausgeschaltet haben, wenn sie das entsprechende Signal empfangen haben. Weitere Informationen finden Sie unter Regelkreis auf Seite 150.

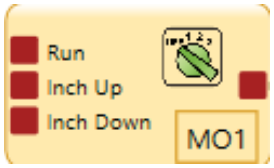
## 10.7.1 Modus-Funktionsblock

Der Modus-Funktionsblock wird hinzugefügt, wenn das Attribut „Modus“ in den **Press Control Properties (Pressensteuerungseigenschaften)** ausgewählt ist.

Die Auswahl des Modus-Funktionsblocks ermöglicht das Hinzufügen eines Funktionswahlschalters. Die drei Eingänge am Funktionsblock der Presse sind Run, Schrittsteuerung aufwärts und Schrittsteuerung abwärts.

**Anmerkung:** Gemäß den Pressenstandards sollte der Moduswahlschalter (oder das Menü) mindestens diese drei Positionen und eine Aus-Position aufweisen. Die Aus-Position wäre kein Sicherheitsabschaltungszustand, sondern eine Presse in einem Eingang für den Zustand „Kein Betrieb“ (wird nicht mit dem Kontroller verbunden, sondern hätte auch die drei Modus-Eingänge im Aus-Zustand). Wenn alle 3 Modus-Eingänge inaktiv/aus sind, bleibt der Funktionsblock für den Pressenmodus ausgeschaltet (rot).

*Abbildung 133. Eingänge am Pressensteuerungs-Funktionsblock*




Wenn der Modus-Funktionsblock im Pressensteuerungs-Funktionsblock ausgewählt wird, werden dem Pressensteuerungs-Funktionsblock die Dauer und Einschaltzeit der Schrittsteuerung hinzugefügt. Bei diesen Parametern handelt es sich um benutzerdefinierte Werte für ihr System, um sicherzustellen, dass sich die Presse bei der Schrittsteuerung nicht zu schnell bewegt (typischerweise während der Einrichtungsmodi verwendet).

**Anmerkung:** Gemäß DIN EN ISO 16092-3:2018 darf die Schrittgeschwindigkeit im Schrittsteuerungsmodus maximal 10 mm/Sekunde betragen.

- Ein Schrittsteuerungsprozess ist eine intermittierende Bewegung des Stößels, um ihn langsam aufwärts oder abwärts zu bewegen, typischerweise zur Wartung oder zum Setzen der Stanzform.
- Die **Schrittsteuerungsperiode** ist die Dauer des vollständigen Zyklus (Ein- und Ausschaltung) einer intermittierenden Bewegung des Stößels.
- Die **Einschaltzeit der Schrittsteuerung** ist der eingeschaltete Teil der Schrittsteuerungsperiode (der Zeitraum, in dem der Ausgang eingeschaltet ist, um die Stößelbewegung anzutreiben).
- Berücksichtigen Sie beim Einstellen der Einschaltzeit und -dauer Verzögerungen bei der Initiierung und beim Anhalten der Bewegung, um die richtige Schrittgeschwindigkeit zu gewährleisten, wenn der GO-Eingang für mehrere Schrittsteuerungsperioden geschlossen gehalten wird.

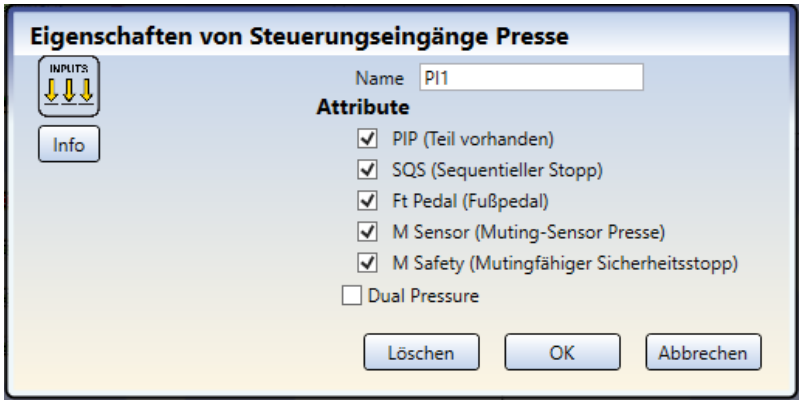
**WARNUNG:**
- Pressengeschwindigkeit während des Schrittsteuerungsmodus.
- Eine zu hohe Geschwindigkeit des Stößels im Schrittsteuerungsmodus kann schwere bis tödliche Verletzungen zur Folge haben.
- Bei der Einstellung der Einschaltzeit und -dauer der Schrittsteuerung ist darauf zu achten, dass sich der Stößel im Schrittsteuerungsmodus mit einer sicheren Geschwindigkeit bewegt.

## 10.7.2 Funktionsblock Pressensteuerungeingänge

Der Funktionsblock Pressensteuerungseingänge wird hinzugefügt, wenn das Feld für das PCI-Attribut in den **Press Control Properties (Pressensteuerungseigenschaften)** aktiviert ist.

Wenn der Funktionsblock PCI ausgewählt ist, können weitere Pressensteuerungsattribute aktiviert werden.

*Abbildung 134. **Eigenschaften der Pressensteuerungseingänge***




Die Standardknoten des PCI-Blocks sind der **PIP**-Eingang (Part in Place), der **SQS**-Eingang (sequenzieller Stopp) und der **M Safety**-Eingang (Eingang für mutingfähigen Sicherheitsstopp). Wenn **SQS** ausgewählt ist, sind die Eingänge **Ft Pedal** (Fußpedal) und **M Sensor** (Muting-Sensor der Presse) als Optionen verfügbar und die Doppeldruck-Attribute werden verfügbar (dies ermöglicht das Hinzufügen von Hoch- und Niederdruckausgängen zu den standardmäßigen Aufwärts- und Abwärts-Ausgängen).

Verwenden Sie den PIP-Eingang in Pressensteuerungen, wo die Presse nicht laufen soll, wenn kein Teil vorhanden ist. Der PIP-Eingang muss hoch sein, damit der Pressenzyklus beginnen kann. Nachdem die Presse das BOS verlassen hat, muss der PIP-Eingang aus- und wiedereingeschaltet werden, bevor der nächste Pressenzyklus eingeleitet werden kann; dies kann geschehen, bevor oder nachdem die Presse das TOS erreicht hat.

Verwenden Sie den SQS-Eingang in Pressensteuerungen, bei denen der Pressenstößel auf einen fingersicheren Punkt abgesenkt wird. An diesem Punkt kann der mutingfähige Sicherheitsstopp-Eingang gemutet werden, der Bediener kann den Zweihand-Steuerungseingang freigeben (konfiguriert auf den GO-Eingang des Funktionsblocks der Pressensteuerung) und das Werkstück bei Bedarf greifen. Durch die Initiierung des Ft Pedal-Eingangs fährt der Pressenstößel zum unteren Ende des Hubs und bleibt dort stehen.

**Anmerkung:** Dies ist eine Methode zur Steuerung des Pressensteuerungsprozesses bei konfiguriertem SQS. Es gibt drei zulässige Verfahren:

1. TC1 schaltet den GO-Eingang ein, um den Stößel zum SQS-Punkt zu fahren. TC1 freigeben und FP1 aktivieren, um den Fußpedal-Eingang einzuschalten und den Stößel zum unteren Hubende (BOS) zu fahren, FP1 freigeben und TC1 aktivieren, um den Stößel anzuheben.
2. FP1 schaltet den GO-Eingang ein, um den Stößel zum SQS-Punkt zu fahren. FP1 freigeben. Beim erneuten Aktivieren von FP1 fährt der Stößel zum BOS-Punkt und dann wieder zurück zum TOS-Punkt (oberes Hubende). (Der Ft Pedal-Eingang wird deaktiviert, wenn FP1 an den GO-Knoten angeschlossen wird).
3. TC1 schaltet den GO-Eingang ein, um den Stößel zum SQS-Punkt zu fahren, TC1 freigeben. Beim erneuten Aktivieren von TC1 fährt der Stößel zum BOS-Punkt und dann wieder zurück zum TOS-Punkt (oberes Hubende). (Um das System für diese Methode einzurichten, wählen Sie NICHT den Ft Pedal-Knoten im Funktionsblock für Pressesteuerungseingänge aus.)

Der M-Sensor-Eingang kann in Verbindung mit dem SQS-Eingang verwendet werden, um den Eingang für die Muting-Sicherheitsabschaltung zu muten, wenn er eine fingersichere Position erreicht.

Wenn der SQS-Eingang und Doppeldruck im Eingang des Pressensteuerungs-Funktionsblocks konfiguriert sind, werden dem Pressensteuerungs-Funktionsblock zwei neue Ausgänge hinzugefügt. **H** (Hoch)- und **L** (Niedrig)-Ausgangsknoten werden zusätzlich zu den Standardausgängen **U** (für Aufwärts, Ausrücken oder Rückhub) und **D** (für Abwärts, Einrücken oder Ausrückhub) hinzugefügt. H dient zum Einrücken des hohen Drucks, um den letzten Teil des Hubs zu beenden. L dient zum Einrücken des Standarddrucks (Niedrigdrucks), um den Schlitten auf den SQS-Punkt herunterfahren zu lassen und ihn dann in die Ausgangsposition zurückzubringen.

*Abbildung 135. Eingangsblock der Pressensteuerung*

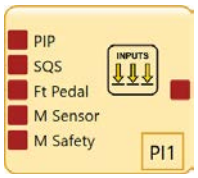
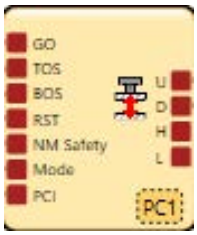



*Abbildung 136. Pressensteuerungs-Funktionsblock*

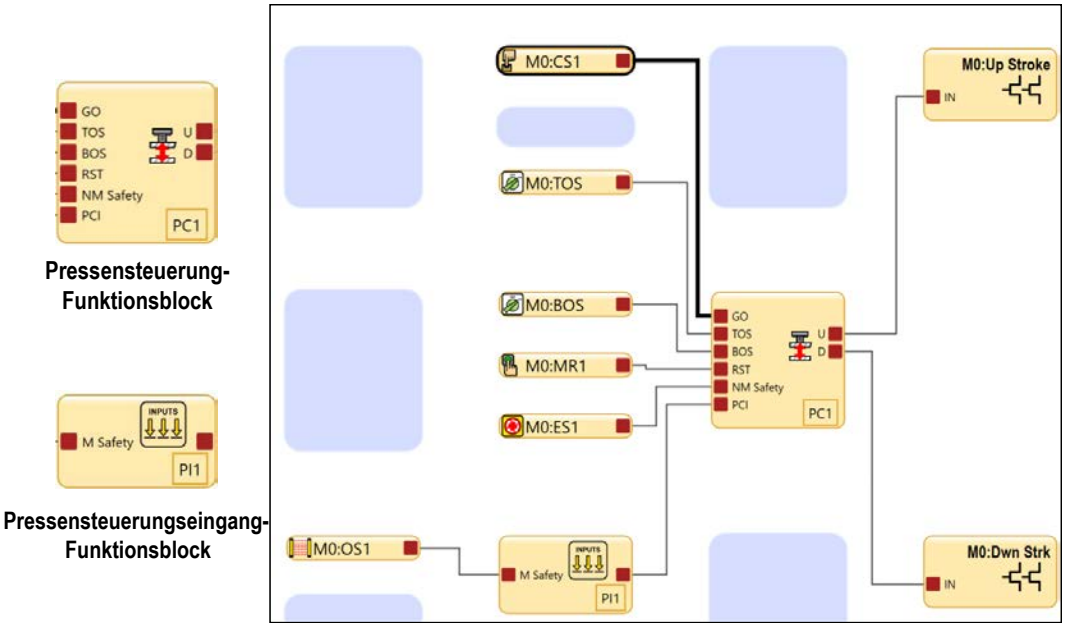


# 10.7.3 Beispiele für den Pressensteuerungs-Funktionsblock

Dieser Abschnitt enthält zwei Beispielkonfigurationen.

Es folgt ein Beispiel für eine einfache Konfiguration für eine kleine Presse.

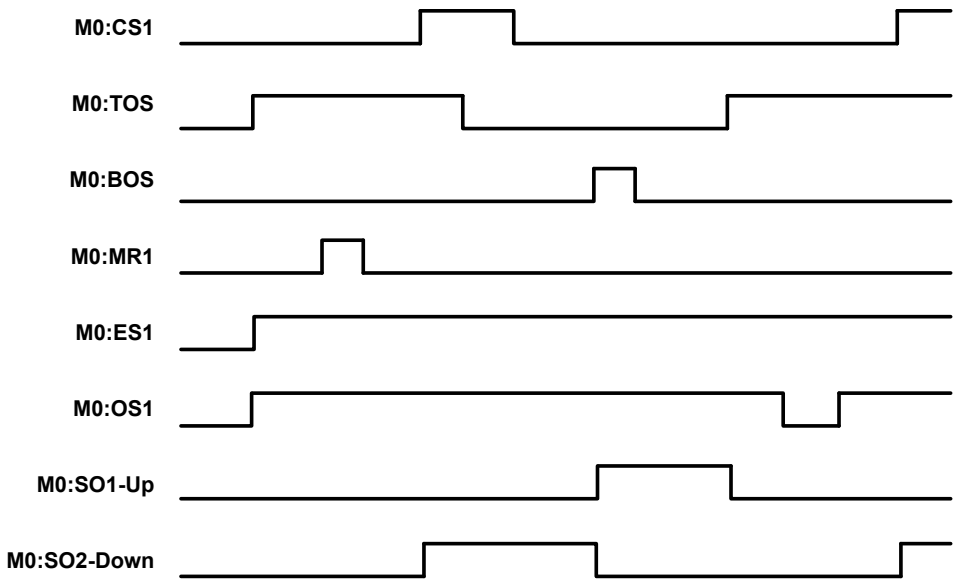
*Abbildung 137. Beispielkonfiguration für eine kleine Presse*




Der Pressensteuerungs-Funktionsblock erfordert für den ordnungsgemäßen Betrieb die korrekte Reihenfolge der Eingangssignale. ES1, OS1 und TOS müssen sich im Ein-Zustand befinden (und zurückgesetzt worden sein), bevor der CS1-Eingang den entsprechenden Ausgang einschalten kann. Bei dieser Konfiguration wird die Einzelauslösersteuerung verwendet, d. h. sobald der CS1-Eingang den Prozess gestartet hat, hat entweder der ES1-Eingang, der OS1-Eingang oder das Ende des Zyklus (TOS schaltet sich wieder ein) die Berechtigung zum Ausschalten. Siehe das nachfolgende Zeitverlaufsdiagramm oder die Simulationsbeschreibung in XS/SC26-2: Beispielkonfiguration – einfache Pressensteuerung mit mutingfähigem Sicherheitseingang auf Seite 88.

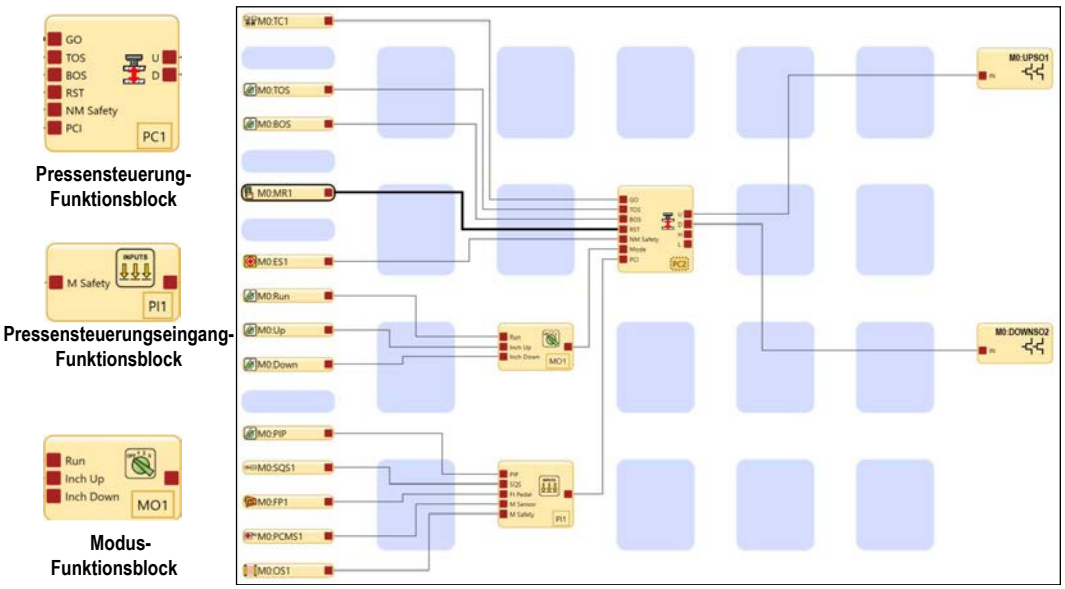
Das folgende Zeitverlaufsdiagramm zeigt die korrekte Abfolge der Eingänge zum Pressensteuerungs-Funktionsblock, die bei aktivierter Einzelauslösersteuerung zum ordnungsgemäßen Betrieb der Ausgänge führt.

*Abbildung 138. Pressensteuerung – Zeitverlaufsdiagramm, Einzelauslösersteuerung*




Im Folgenden sehen Sie eine Konfiguration, die die meisten Funktionen des Funktionsblocks der Pressensteuerung verwendet.

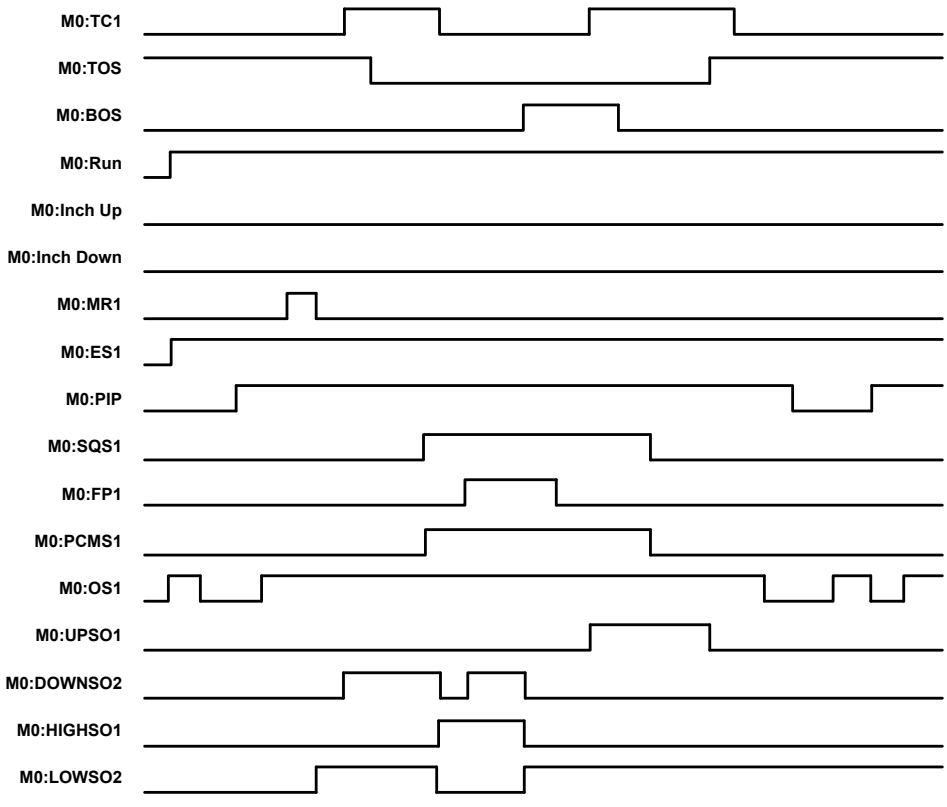
*Abbildung 139. Pressensteuerung – Beispielkonfiguration*




Der Pressensteuerungs-Funktionsblock erfordert für den ordnungsgemäßen Betrieb die korrekte Reihenfolge der Eingangssignale. Diese Konfiguration verwendet die manuelle Aufwärtshubeinstellung. ES1, OS1, PIP und TOS müssen sich im Ein-Zustand befinden (und zurückgesetzt worden sein), bevor der TC1-Eingang den entsprechenden Ausgang einschalten kann. Während des Abwärtshubs startet der TC1-Eingang den Prozess, und der ES1-Eingang, der OS1-Eingang, der TC1-Eingang oder das Erreichen des SQS-Eingangs (sequenzieller Stopp, SQS schaltet sich ein) hat die Berechtigung zum Ausschalten. Wenn die Presse den SQS-Punkt erreicht (SQS und PCMS schalten sich ein), stoppt sie und OS1 wird gemutet. TC1 kann freigegeben werden. Um den Hub zu beenden, schalten Sie den FP1-Eingang ein. Während des restlichen Abwärtshubs haben der ES1-Eingang, der FP1-Eingang oder BOS (Einschalten) die Berechtigung zum Ausschalten. Wenn BOS erreicht ist, wird FP1 freigegeben und TC1 wird verwendet, um die Presse in die TOS-Position zurückzubringen. Während des Aufwärtshubs haben der TC1-Eingang, der ES1-Eingang, der OS1-Eingang oder das Erreichen der TOS-Position die Berechtigung zum Ausschalten. Siehe das nachfolgende Zeitverlaufsdiagramm oder die Simulationsbeschreibung in XS/SC26-2: Beispielkonfiguration der vollfunktionalen Pressensteuerung auf Seite 90.

Das folgende Zeitverlaufsdiagramm zeigt die korrekte Abfolge der Eingänge zum Pressensteuerungs-Funktionsblock, die bei aktivierter manueller Aufwärtshubeinstellung zum ordnungsgemäßen Betrieb der Ausgänge führt.

*Abbildung 140. Pressensteuerung – Zeitverlaufsdiagramm mit manueller Aufwärtshubeinstellung*



## 10.7.4 Regelkreis

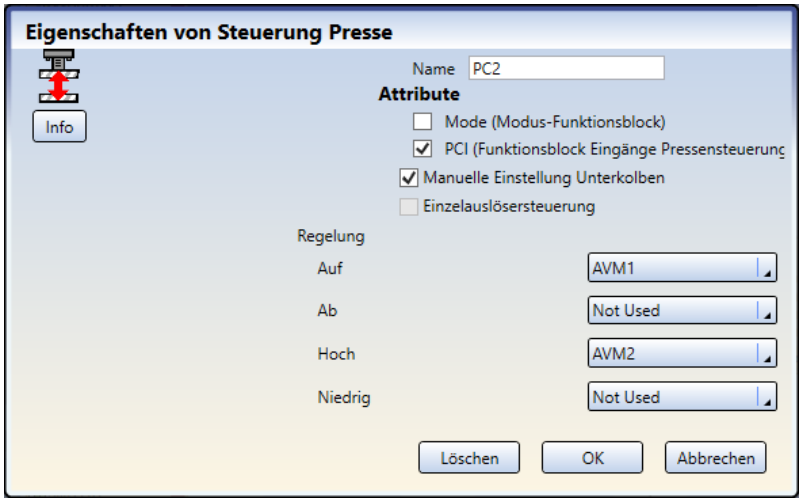
Über den Pressensteuerungs-Funktionsblock lässt sich der Regelkreis aktivieren.

Wenn der Regelkreis aktiviert wird, wird der Kontroller dadurch gezwungen, vor dem Einschalten des nächsten Ausgangs erst zu überprüfen, ob sich die an die angegebenen Ausgänge angeschlossenen Geräte ausgeschaltet haben.

So verwenden Sie einen Regelkreis:

1. Ein AVM-Knoten muss zu dem gewünschten Sicherheitsausgang hinzugefügt werden, der vom FB Presse angetrieben wird.
2. Der AVM-Eingang liefert einen Hinweis auf den Zustand dieses Pressenventils.
3. Der FB Presse muss so konfiguriert werden, dass jeder Ausgang einzeln geregelt wird. Siehe die **Pressensteuerungseigenschaften** in der folgenden Abbildung.

*Abbildung 141. Regelkreis*




In diesem Beispiel wird der Regelkreis so eingerichtet, dass sich das Aufwärts-Ausgangsventil erst abgeschaltet haben muss, bevor andere Funktionen zugelassen werden. Außerdem wird sichergestellt, dass sich das Hoch-Ventil erst schließen muss, bevor der Aufwärts-Ausgang aktiviert wird.

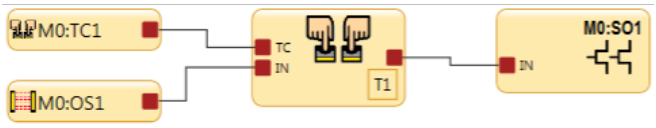
# 10.8 Zweihandsteuerungsblock (für XS/SC26-2 bis FID 3 und SC10-2 FID 1)

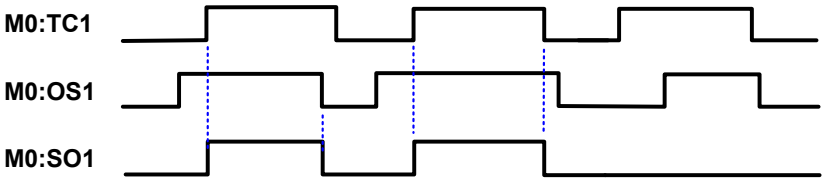
*Abbildung 142. Zeitablauf-Diagramm: Zweihandsteuerungsblock*

| Standardknoten | Zusätzliche Knoten | Anmerkungen |
|---|---|---|
| TC (bis zu 4 TC-Knoten) | IN MP1 ME | Die Eingänge für Zweihandsteuerungen müssen entweder direkt mit einem Zweihandsteuerungsblock oder indirekt über einen an einen Zweihandsteuerungsblock angeschlossenen Überbrückungsblock verbunden werden. Die Verwendung eines Eingangs für eine Zweihandsteuerung ohne Zweihand-steuerungsblock ist nicht möglich.<br>Mit dem IN-Knoten lassen sich Eingangsgeräte verbinden, die erst eingeschaltet werden müssen, bev-or die Zweihandsteuerung die Ausgänge einschalten kann. |



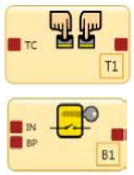

**Zweihandsteuerungs-Funktionsblock**



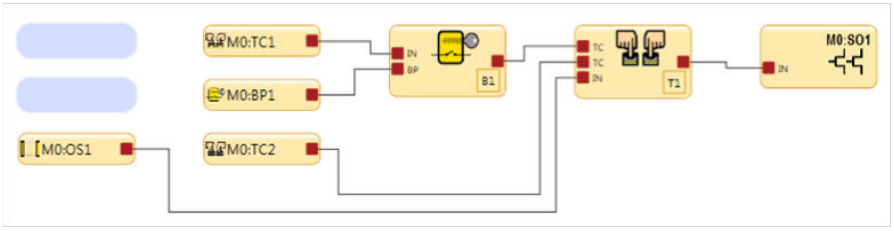



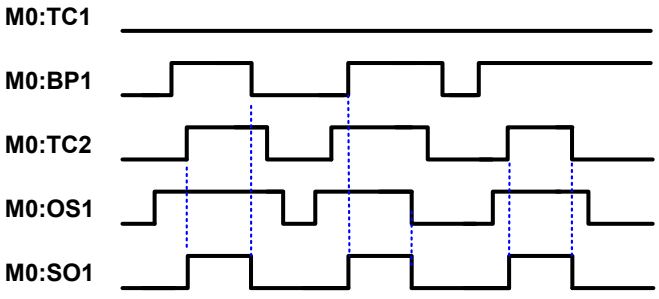

Entweder der TC1-Eingang oder der OS1-Eingang hat die Ausschalthoheit. OS1 muss im Ein-Zustand sein, bevor TC1 den Ausgang von T1 und SO1 einschalten kann.

*Abbildung 143. Zeitablauf-Diagramm: Zweihandsteuerungsblock und Überbrückungsblöcke*



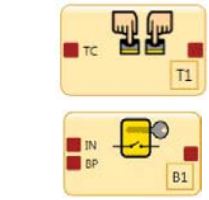

**2-Handsteuerung & Funktionsblöcke überbrücken**



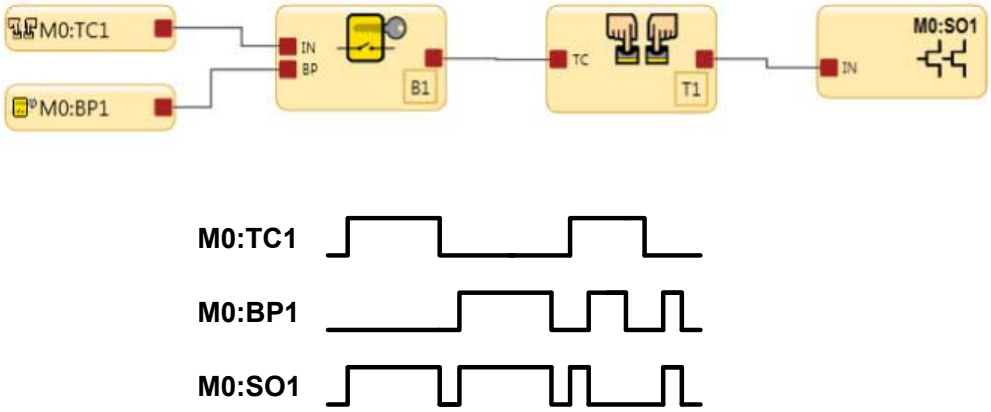




OS1 muss in den Ein-Zustand übergehen, bevor TC2 in den Ein-Zustand übergeht. BP1 kann vor oder nach OS1 in den Ein-Zustand übergehen. Wenn sich OS1 im Ein-Zustand befindet, spielt die Reihenfolge, in der TC2 oder BP1 in den Ein-Zustand übergehen, keine Rolle. Der Auslöser, der zuletzt in den Ein-Zustand übergeht, löst den Übergang des Funktionsblocks T1 in den Ein-Zustand aus.

*Abbildung 144. Zeitablauf-Diagramm: Zweihandsteuerungsblock und Überbrückungsblöcke mit 1 Eingang für Zweihandsteuerung*

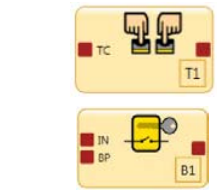



**Zweihandsteuerungs- und Überbrückungs-funktionsblöcke**

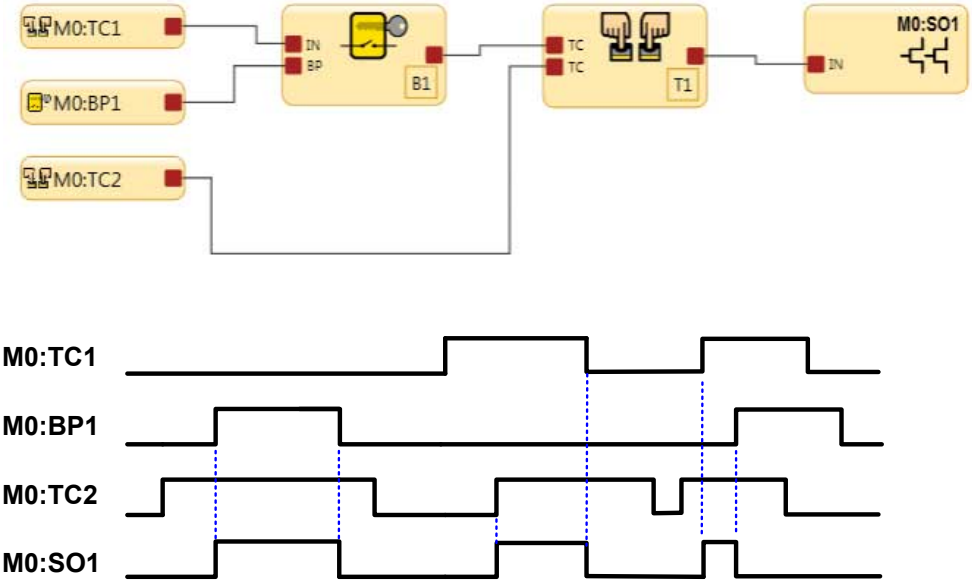



Wenn die TC1-Bedienelemente und der BP1-Überbrückungsschalter gleichzeitig aktiv sind, schalten sich der Ausgang des B1-Überbrückungsfunktionsblocks und der Ausgang des Zweihandsteuerungs-Funktionsblocks aus.
Die Ausgänge für B1 und T1 schalten sich nur ein, wenn entweder die TC1-Bedienelemente oder der BP1-Schalter im Ein-Zustand sind.

*Abbildung 145. Zeitablauf-Diagramm: Zweihandsteuerungsblock und Überbrückungsblöcke mit 2 Eingängen für Zweihandsteuerung*



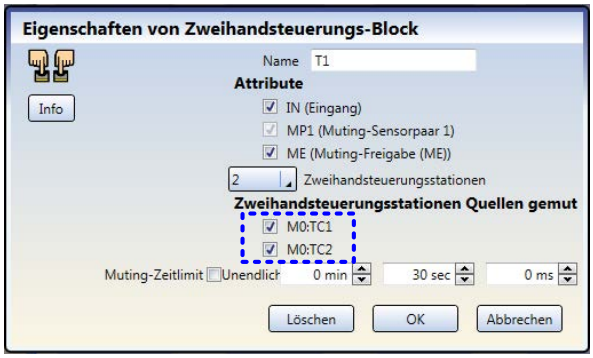

**Zweihandsteuerungs- und Überbrückungsfunk-tionsblöcke**




Die Überbrückungsfunktion kann mit den TC2-Bedienelementen verwendet werden, um den Sicherheitsausgang einzuschalten.

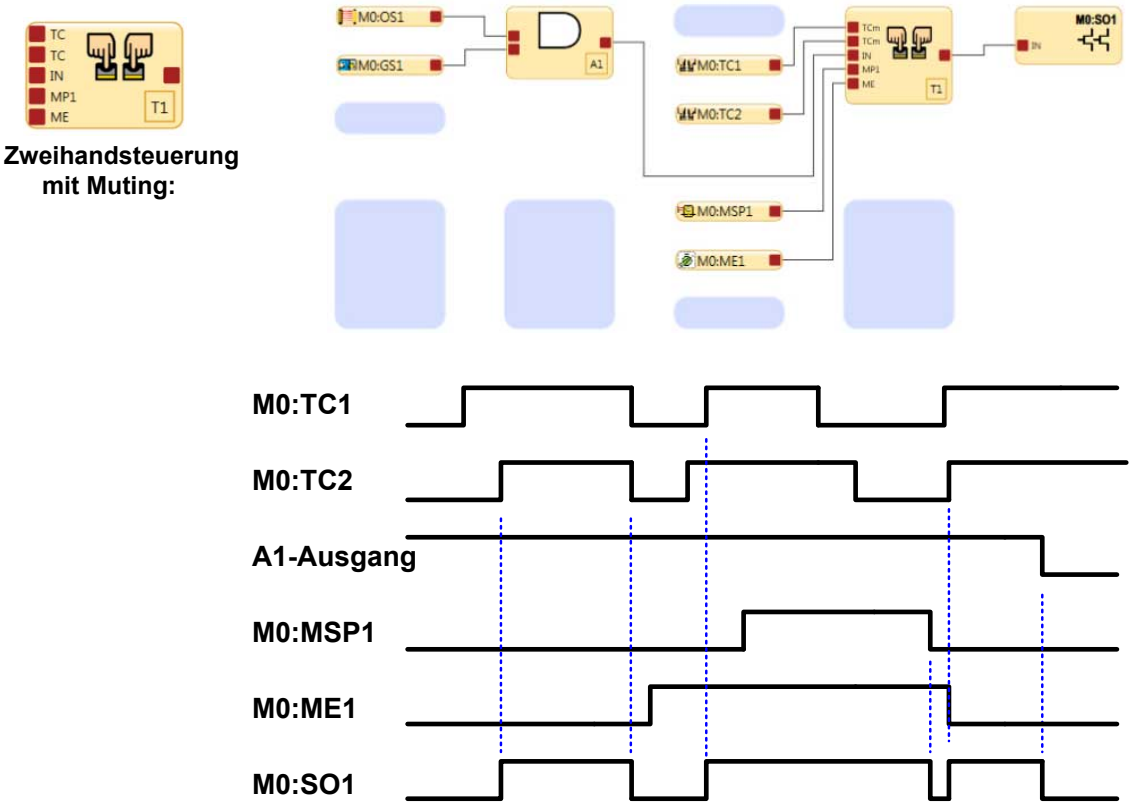
Wenn die TC1-Bedienelemente nicht überbrückt werden, müssen sie zusammen mit den TC2-Bedienelementen verwendet werden, um den Sicherheitsausgang einzuschalten. Wenn die TC1-Bedienelemente und der Überbrückungsschalter beide im Ein-Zustand sind, können TI und SO1 nicht eingeschaltet werden oder schalten sich aus.

*Abbildung 146. Muting-Optionen für Zweihandsteuerungen*




Zum Konfigurieren der Muting-Option für die Zweihandsteuerung müssen die TC-Bedienelemente erst mit dem Zweihandsteuerungs-Funktionsblock in der Funktionsansicht verbunden werden. Die Kontrollkästchen (blaues Quadrat oben) im Menü Eigenschaften zeigen die Namen aller Eingangsgeräte für TC-Bedienelemente an. Nur die Stations felder der Zweihandsteuerung, deren Kontrollkästchen aktiviert sind, werden gemutet.

*Abbildung 147. Zeitablauf-Diagramm: Zweihandsteuerungsblock mit Muting*




Die Auslöser TC1 und TC2 können unabhängig vom Zustand des Eingangs für die Muting-Freigabe (ME1) − ein- oder ausgeschaltet − einen Zweihandzyklus auslösen. ME1 muss aktiv sein, damit die MSP1-Muting-Sensoren SO eingeschaltet lassen, nachdem die Auslöser TC1 und TC2 in den Stoppzustand geschaltet haben.

**Schutz der Zweihandsteuerung gegen Aktivierung bei Anlauf** Die Zweihandsteuerungslogik des Sicherheitskontrollers lässt es nicht zu, dass sich der zugeordnete Sicherheitsausgang einschaltet, wenn die Spannung angelegt wird, während sich die Bedienelemente der Zweihandsteuerung noch im Ein-Zustand befinden. Die Bedienelemente der Zweihandsteuerung müssen in den Aus-Zustand wechseln und dann wieder in den Ein-Zustand, bevor sich der Sicherheitsausgang einschalten kann. Sicherheitsausgänge, die einer Zweihandsteuerungsvorrichtung zugeordnet sind, haben keine Option für manuellen Reset.

# 10.9 Zweihandsteuerungsblock (XS/SC26-2 ab FID 4 sowie SC10-2 ab FID 2)

Bei XS/SC26-2-Geräten ab FID 4 und SC10-2-Geräten ab FID 2 kann der TC-Eingang direkt einem Ausgang oder einem Logikblock zugeordnet werden. Der Zweihandsteuerungs-Funktionsblock kann direkt einem Ausgang oder einem Logikblock zugeordnet werden.

Wenn mehrere Bediener die Maschine verwenden und jeder Bediener die Zweihandsteuerung aktivieren muss, verwenden Sie den Zweihandsteuerungs-Funktionsblock, bei dem mehrere TC-Eingänge ausgewählt werden können.

Wenn das System eine Haltefunktion hat (TC-Eingänge, die eine Aktion auslösen, die sie sicher macht, sodass der Bediener dann seine Hände beim Abschließen des Prozesses wegnehmen kann), verwenden Sie den Zweihandsteuerungs-Funktionsblock mit ausgewählter Muting-Funktion.

Wenn die Maschine bestimmte Sicherheitsvorrichtungen hat, die für den TC-Eingang funktionsfähig sein sollten (und bleiben müssen), damit der Maschinenbetrieb möglich ist, verwenden Sie den Zweihandsteuerungs-Funktionsblock mit ausgewähltem IN-Knoten.

- Wenn der IN-Knoten ausgeschaltet ist, bewirkt die Betätigung des Zweihandeingangs keine Aktionen.
- Wenn der Zweihandsteuerungs-Funktionsblock eingeschaltet ist und der TC-Block ausschaltet, schaltet auch der Ausgang aus.
- Wenn der IN-Knoten wieder einschaltet, bleibt der Ausgang ausgeschaltet, bis die TC-Eingänge aus- und wieder einschalten.

**WARNUNG:**

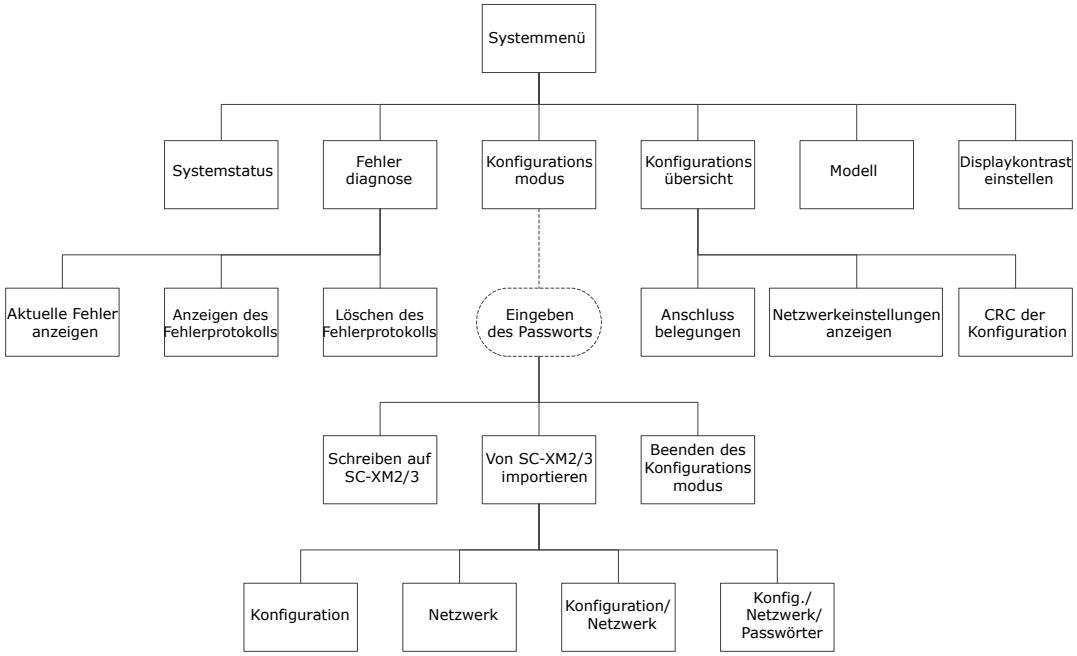
- Zweihandsteuerungen sind Startvorrichtungen (Initiierung einer gefährlichen Bewegung).
- Wenn diese Anweisungen nicht befolgt werden, können schwere oder tödliche Verletzungen die Folge sein.
- Die qualifizierte Person muss sicherstellen, dass die Aktivierung (Wechsel in einen eingeschalteten Zustand) einer Sicherheitsstoppvorrichtung (Not-Aus-Schalter, Seilzugschalter, optische Sensoren, Sicherheitsmatten, Schutzhalt usw.) durch einen Anwender keine gefährliche Bewegung initiiert, wenn diese logisch mit einem TC-Eingang oder einem Zweihandsteuerungs-Funktionsblock verbunden ist, der bereits aktiviert ist (EINGESCHALTETER Zustand).

# 11 Bedienfeld am XS/SC26-2

Über das Bedienfeld am Sicherheitskontroller XS/SC26-2 können Sie folgende Funktionen aufrufen:

- **Systemstatus**: zeigt den aktuellen Status der Sicherheitsausgänge und, sofern gewählt, der mit dem betreffenden Sicherheitsausgang verbundenen Eingänge an.
- **Fehlerdiagnose**: zeigt die aktuellen Fehler, das Fehlerprotokoll und eine Option zum Löschen des Fehlerprotokolls an (siehe Fehlersuche und -behebung auf Seite 283).
- **Configuration Mode (Konfigurationsmodus)**: wechselt in den Konfigurationsmodus (Passwort erforderlich) und ermöglicht den Zugriff auf die Funktionen zum Kopieren oder Schreiben der Konfiguration vom SC-XM2/3-Laufwerk und auf das Laufwerk (siehe XS/SC26-2: Konfigurationsmodus auf Seite 155).
- **Konfigurationsübersicht**: ermöglicht den Zugriff auf die Klemmenzuordnungen, Netzwerkeinstellungen und CRC der Konfiguration.
- **Model # (Typenbezeichnung)**: zeigt jeweils die aktuelle Typenbezeichnung und die Softwareversion an.
- **Einstellung Bildschirmkontrast**: ermöglicht die Einstellung der Display-Helligkeit mit den Bedienelementen.

*Abbildung 148. Bedienfeld am Kontroller: Zuordnung*




## 11.1 XS/SC26-2: Konfigurationsmodus

Der **Konfigurationsmodus** enthält Möglichkeiten zum Senden der aktuellen Konfiguration an ein SC-XM2/3-Laufwerk und zum Empfangen einer Konfiguration vom SC-XM2/3-Laufwerk.

**Anmerkung:** Für den Zugriff auf das Menü **Konfigurationsmodus** ist ein Passwort erforderlich.

**Wichtig:** Beim Wechsel in den **Konfigurationsmodus** werden die Sicherheitsausgänge ausgeschaltet.

### So *schreiben* Sie Daten über das Bedienfeld am Kontroller auf ein SC-XM2/3-Laufwerk:

1. Legen Sie das SC-XM2/3-Laufwerk in den Sicherheitskontroller ein.
2. Wählen Sie im **System-Menü** den Befehl **Konfigurationsmodus**.
3. Geben Sie das Passwort ein.
4. Halten Sie **OK** gedrückt, bis das Menü **Konfigurationsmodus** angezeigt wird.
5. Wählen Sie **Auf XM schreiben**.

   **Anmerkung:** Beim Schreibvorgang auf XM werden alle Daten (Konfigurationsdaten, Netzwerkeinstellungen und Passwörter) auf das SC-XM2/3-Laufwerk kopiert.
6. Warten Sie, bis der Schreibvorgang abgeschlossen ist.

7. Führen Sie einen System-Reset durch.

### So *importieren* Sie Daten über das Bedienfeld am Kontroller von einem SC-XM2/3-Laufwerk:

1. Legen Sie das SC-XM2/3-Laufwerk in den Sicherheitskontroller ein.
2. Wählen Sie im **System-Menü** den Befehl **Konfigurationsmodus**.
3. Geben Sie das Passwort ein.
4. Halten Sie **OK** gedrückt, bis das Menü **Konfigurationsmodus** angezeigt wird.
5. Klicken Sie auf **Import from XM (Von XM importieren)**:
    - Wenn Sie nur Konfigurationsdaten importieren möchten, wählen Sie **Konfiguration.**
    - Wenn Sie nur Netzwerkeinstellungen importieren möchten, wählen Sie **Netzwerkeinstellungen.**
    - Wählen Sie zum Importieren der Konfigurationsdaten und Netzwerkeinstellungen die Option **Konfiguration/Netzwerk.**
    - Wählen Sie zum Importieren aller Daten (Konfigurationsdaten, Netzwerkeinstellungen und Benutzerpasswörter) die Option **Konfig/Netzwerk/Passwörter.**
6. Warten Sie, bis der Importvorgang abgeschlossen ist.
7. Führen Sie einen System-Reset durch.

# 12 Industrie-Ethernet – Übersicht

Eine Hilfe beim Aufbau der Ethernet-Kommunikation zwischen dem Sicherheitskontroller und einer SPS oder HMI.

Die folgenden Abschnitte enthalten die Anleitung für Sicherheitskontroller mit der Bezeichnung FID 2 auf dem Typenschild und den Datumcodes 1717 oder später sowie für Sicherheitskontroller ab FID 3.

Für FID 2-Sicherheitskontroller mit Datumcodes 1716 oder früher siehe *Benutzerhandbuch zum Industrie-Ethernet XS26/SC26-2E (FID 2 1716-)*. Für FID 1-Sicherheitskontroller mit Datumcodes 1547 oder später siehe *Benutzerhandbuch zum Industrie-Ethernet XS/SC26-2E (FID 1)*. Für ältere Versionen der FID 1-Sicherheitskontroller siehe *Benutzerhandbuch zum Industrie-Ethernet XS/SC26-2E (ALT)*. Für Informationen, wo Sie diese Dokumente finden, siehe Welche XS/SC26-2-EDS-Datei und -Dokumentation sollten Sie verwenden? auf Seite 159.

Für PROFINET-Verbindungen auf SC10-2-Kontrollern und XS/SC26-2-Kontrollern ab FID 2 siehe PROFINET auf Seite 230.

## 12.1 Konfiguration des Sicherheitskontrollers

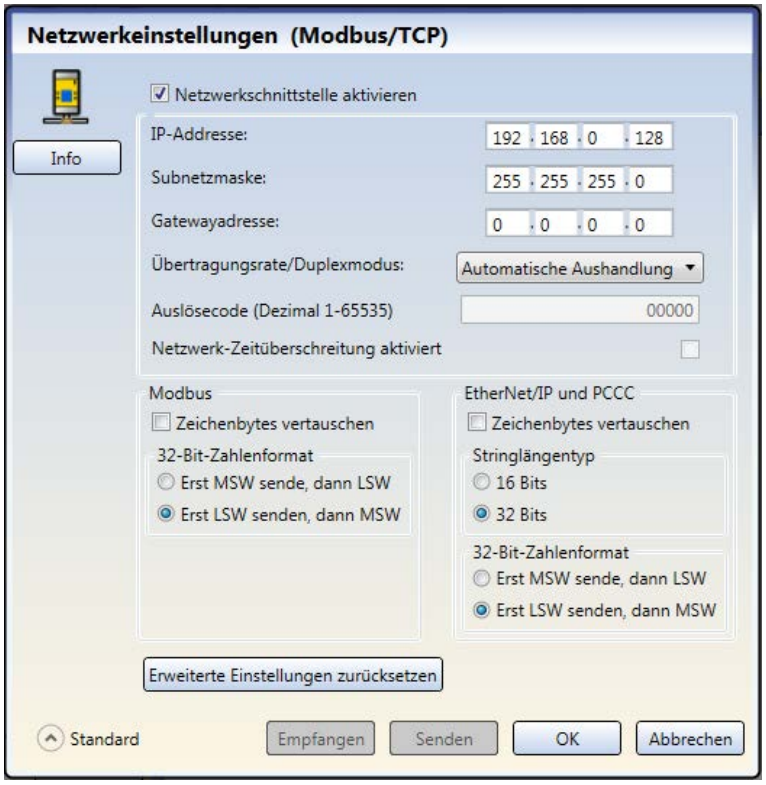
Vergewissern Sie sich, dass die Option **Netzwerkschnittstelle aktivieren** markiert ist und die Netzwerkeinstellungen entsprechend dem ausgewählten Protokoll konfiguriert sind.

1. Verbinden Sie den Sicherheitskontroller über das SC-USB2-USB-Kabel mit dem PC, um den Port zu aktivieren.
2. Öffnen Sie die Software des Sicherheitskontroller von Banner.
3. Klicken Sie auf **Netzwerkeinstellungen**.
4. Markieren Sie das Kontrollkästchen **Netzwerkschnittstelle aktivieren**.
5. Konfigurieren Sie entsprechend Ihrem Netzwerk die IP-Adresse und die Subnetzmaske.

> **Anmerkung:** Wenn eine virtuelle Reset- oder Abbruchverzögerung verwendet wird, muss ein Auslösecode definiert und an den Sicherheitskontroller gesendet werden.

6. Klicken Sie auf **Senden**.
7. Klicken Sie auf den Pfeil **Erweitert**, um gegebenenfalls die erweiterten Netzwerkeinstellungen zu konfigurieren. Nachfolgend sind die Standardwerte für den Ethernet-Port und das Industrie-Ethernet des Sicherheitskontrollers angegeben.

*Abbildung 149. Standardwerte*




8. Geben Sie das entsprechende Passwort ein, um die Konfigurations- und Netzwerkeinstellungen für den Sicherheitskontroller zu ändern.
9. Vergewissern Sie sich, dass der Sicherheitskontroller eine gültige und bestätigte Konfigurationsdatei hat.

Der Ethernet-Port ist aktiviert.

# 12.2 Industrie-Ethernet – Definitionen

Es folgen Beschreibungen der Tabellenzeilen und -spalten (in alphabetischer Reihenfolge) für die Registerzuordnungen auf der Registerkarte **Industrie-Ethernet** in der Software.

*Tabelle 8. Datentypen*

| Datentyp | Beschreibung |
|---|---|
| **UINT** | Unsigned integer (vorzeichenlose ganze Zahl) – 16 Bit |
| **UDINT** | Unsigned double integer (vorzeichenlose doppelte ganze Zahl) – 32 Bit |
| **Word (Wort)** | Bit string (Bit-Zeichenfolge) – 16 Bit |
| **Dword (Datenwort)** | Bit string (Bit-Zeichenfolge) – 32 Bit |
| **String (Zeichenfolge)** | Zwei ASCII-Zeichen pro Wort (siehe protokollbasierte String-Informationen unten) |
| **Octet (Oktett)** | Stellt jedes Byte als Dezimalzahl, getrennt durch einen Punkt, dar |
| **Hex (Hexadezimalzahl)** | Stellt jedes Halbbyte als Hexadezimalzahl in Paaren und durch Leerzeichen getrennt dar |
| **Byte** | Bit string (Bit-Zeichenfolge) – 8 Bit |

### Byte:Bit

Gibt den Byte-Versatz gefolgt vom spezifischen Bit an.

### Fehler-Flag

Wenn ein bestimmter nachverfolgter Ein- oder Ausgang einen Sperrzustand verursacht, wird ein mit dem betreffenden virtuellen Ausgang verbundenes Kennzeichen auf **1** gesetzt. In Modbus/TCP kann dies als diskretes Eingangssignal, Eingaberegister oder das Ein- und Ausgaberegister gelesen werden.

### Fehlerindex

Wenn das Fehler-Flag-Bit für einen virtuellen Ausgang gesetzt ist, enthält der Fehlerindex eine Nummer, die in einen Fehlercode übersetzt wird. Beispiel: Ein Fehlerindex 41 kann eine Nummer 201 enthalten, die in den Fehlercode 2.1 übersetzt wird; die Nummer 412 würde in den Fehlercode 4.12 übersetzt (weitere Informationen siehe Fehlercode-Tabelle für XS/SC26-2 auf Seite 283 und SC10-2 Fehlercode-Tabelle auf Seite 288).

### Funktion

Die Funktion, die den Zustand des betreffenden virtuellen Ausgangs ermittelt.

### Betriebsart

| Wert für Betriebsart | Beschreibung |
|---|---|
| 1 (0x01) | Normalbetrieb (einschließlich E/A-Fehlern, sofern vorhanden) |
| 2 (0x02) | Konfigurationsmodus |
| 4 (0x04) | Systemsperre |
| 65 (0x41) | Warten auf System-Reset/Beenden des Konfigurationsmodus |
| 129 (0x81) | Aufruf des Konfigurationsmodus |

### Reg:Bit

Gibt den Versatz von 30000 oder 40000, gefolgt von dem spezifischen Bit im Register an.

### Reserviert

Register, die zur internen Verwendung reserviert sind.

### Sekunden seit Systemstart

Die Zeit in Sekunden seit der Netzeinschaltung des Sicherheitskontrollers. Kann in Verbindung mit dem Zeitstempel im Fehlerprotokoll und einer Echtzeituhr-Referenz verwendet werden, um den Zeitpunkt festzustellen, zu dem ein Fehler aufgetreten ist.

### String (Ethernet/IP und PCCC-Protokoll)

Das Standardformat für das Ethernet/IP-Zeichenfolgenformat hat eine Länge von 32 Bit, die der Zeichenfolge vorausgeht (geeignet für ControlLogix). Beim Konfigurieren der **Netzwerkeinstellungen** über die Software können Sie diese Einstellung in eine Länge von 16 Bit ändern. Dies entspricht dem standardmäßigen CIP-„String“ im Menü **Erweitert**. Beim Lesen einer Eingangsbaugruppe, die einen String mit einer Länge von 16 Bit enthält, wird der Stringlänge jedoch ein zusätzliches 16-Bit-Wort (0x0000) vorangestellt.

Der String selbst ist ein gepackter ASCII-Ausdruck (2 Zeichen pro Wort). In einigen Systemen kann die Zeichenreihenfolge umgekehrt oder durcheinander erscheinen. Das Wort „System“ kann beispielsweise als „yStsme“ dargestellt sein. Sie können die Zeichen so umstellen, dass die Wörter korrekt lesbar sind. Wählen Sie hierzu die Option „*Zeichenbytes vertauschen*“ im Menü **Erweitert** im Fenster **Netzwerkeinstellungen**.

**String (Modbus/TCP-Protokoll)**

Das String-Format selbst ist ein gepackter ASCII-Ausdruck (2 Zeichen pro Wort). In einigen Systemen kann die Zeichenreihenfolge umgekehrt oder durcheinander erscheinen. Das Wort „System“ kann beispielsweise als „yStsme“ dargestellt sein. Sie können die Zeichen so umstellen, dass die Wörter korrekt lesbar sind. Wählen Sie hierzu die Option „*Zeichenbytes vertauschen*“ im Menü **Erweitert** im Fenster **Netzwerkeinstellungen**.

Die Stringlänge ist zwar angegeben, aber dies ist für Modbus/TCP-Systeme in der Regel nicht erforderlich. Wenn die Zeichenfolgenlänge für Modbus/TCP verwendet wird, entspricht das Längenformat den für Ethernet/IP verwendeten Einstellungen.

**Zeitstempel**

Die Zeit in Sekunden nach der Netzeinschaltung, zu der der Fehler aufgetreten ist.

**Virtueller Statusausgang**

Der Referenzkennwert, der mit einem bestimmten virtuellen Statusausgang verbunden ist, zum Beispiel bezeichnet VO10 den virtuellen Statusausgang 10.

**VO-Status**

Gibt den Speicherort eines Bits an, das den Status eines virtuellen Statusausgangs angibt. Im Falle von Modbus/TCP kann der Status des virtuellen Statusausgangs als diskretes Eingangssignal, als Teil eines Eingaberegisters oder eines Ein- und Ausgaberegisters gelesen werden. Das angegebene Register ist der Versatz von 30000 oder 40000, gefolgt von der spezifischen Bit-Stelle im Register.

# 12.3 Abrufen aktueller Fehlerinformationen

Befolgen Sie die nachstehend beschriebenen Schritte, um Informationen über Netzwerkkommunikationen zu einem gegenwärtig vorhandenen Fehler abzurufen:

1. Lesen Sie den Speicherort *Fehlerindex*, um den Fehlerindexwert abzurufen.
2. Suchen Sie den Indexwert in der Fehlercode-Tabelle für XS/SC26-2 auf Seite 283 oder SC10-2 Fehlercode-Tabelle auf Seite 288, um eine Fehlerbeschreibung und Schritte für die Behebung des Fehlers aufzurufen.

# 12.4 EtherNet/IP™

In diesem Kontext bezieht sich EtherNet/IP™ [14] speziell auf die EtherNet/IP-Transportklasse 1. Diese wird gelegentlich auch als zyklische EtherNet/IP-E/A-Datenübertragung oder implizite Nachrichtenübertragung bezeichnet. Die Verbindung liefert eine echtzeitnahe Datenübertragung zu und von der SPS sowie dem Zielgerät.

Die CompactLogix- und ControlLogix-SPS-Serien von Allen-Bradley verwenden dieses Kommunikationsprotokoll. Die von den SPS verwendete Programmiersoftware ist RSLogix5000 oder Studio 5000 Logix Designer.

## 12.4.1 Welche XS/SC26-2-EDS-Datei und -Dokumentation sollten Sie verwenden?

*Abbildung 150. FID-Nummer*

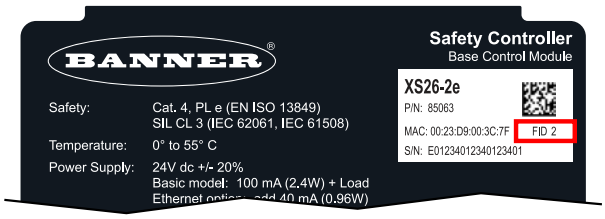
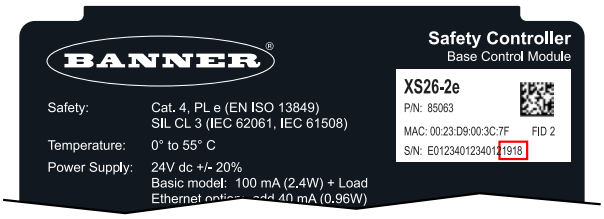



*Abbildung 151. Seriennummer*




1. Notieren Sie sich die FID-Nummer und den Datumscode vom Schild mit der Typenbezeichnung.

   Der Datumscode sind die letzten 4 Ziffern der Seriennummer des Sicherheitskontrollers. In dem gezeigten Beispiel steht „19“ für 2019 und „18“ für die 18. Woche.
2. Anhand der FID-Nummer und des Datumscodes finden Sie in der nachfolgenden Tabelle die richtigen EIP-Parameter, die EDS-Datei und das Benutzerhandbuch zum Industrie-Ethernet (sofern zutreffend).

[14] EtherNet/IP™ist eine Marke von ODVA, Inc.

| Modell und FID | Datumscode | EIP-Prod-Code | O>T — Größe | T>O — Größe | Zu verwendende Dateien |
|---|---|---|---|---|---|
| XS26<br>SC26<br>1 | 1546 oder niedriger | 8193 | 112 (0×70) – 2 | 100 (0×64) – 8<br>101 (0×65) – 104<br>102 (0×66) – 150 | **Produktname (Hauptversion.Nebenversion):** Banner XS26 (8193) [2.22]<br>**EDS-Datei:** BannerXS_SC26_2E_8193_1_4_08102017.eds<br>**Benutzerhandbuch zum Industrie-Ethernet:** Benutzerhandbuch zum Industrie-Ethernet XS/SC26-2E (ALT) |
| XS26<br>SC26<br>1 | 1547 bis 1705 | 300 [15] | 112 (0×70) - 2 | 100 (0×64) - 8<br>101 (0×65) - 104<br>102 (0×66) - 150 | **Produktname (Hauptversion.Nebenversion):** Banner XS26 1547 (300) [2.002]<br>**EDS-Datei:** BannerXS_SC26_2E_300_1547_1_6_08102017.eds [15]<br>**Benutzerhandbuch zum Industrie-Ethernet:** Benutzerhandbuch zum Industrie-Ethernet XS/SC26-2E (FID 1) |
| XS26<br>SC26<br>2 | 1706 bis 1716 | 301 | 112 (0×70) – 11 | 100 (0×64) – 8<br>101 (0×65) – 104<br>102 (0×66) – 150<br>103 (0×67) – 35 | **Produktname [Hauptversion.Nebenversion]:** Banner XS26 FID2 (301) [2.050]<br>**EDS-Datei:** BannerXS_SC26_2E_301_FID2_1_2_08102017.eds<br>**Benutzerhandbuch zum Industrie-Ethernet:** Benutzerhandbuch zum Industrie-Ethernet XS/SC26-2E (FID 2 1716-) |
| XS26<br>SC26<br>2 und 3 | 1717 oder höher | 300 [15] | 112 (0×70) – 2<br>113 (0×70) – 11 | 100 (0×64) – 8<br>101 (0×65) – 104<br>102 (0×66) – 150<br>103 (0×67) – 35 | **Produktname [Hauptversion.Nebenversion]:** Banner XS26 FID 1/2 (300) [2.064]<br>**EDS-Datei:** BannerXS_SC26_2E_300_1_8_11102017.eds [15]<br>**Benutzerhandbuch zum Industrie-Ethernet:** Benutzerhandbuch zum Industrie-Ethernet XS/SC26-2E (FID 2 1717+) |
| XS26<br>SC26<br>2, 3 und 4<br>SC10 beliebig | 1717 oder höher | 300 [15] | 112 (0×70) - 2<br>113 (0×70) - 11<br>114 (0×72) - 14 | 100 (0×64) - 8<br>101 (0×65) - 104<br>102 (0×66) - 150<br>103 (0×67) - 35<br>104 (0×68) - 112 | **Produktname [Hauptversion.Nebenversion]:** Banner XS26 SC26 SC10 (300) [2.090]<br>**EDS-Datei:** Banner_XS26_SC26_SC10_300_2_1_03032020.eds [15]<br>**Bedienungshandbuch für XS/SC26-2 und SC10-2:** Rev R und höher |

**Anmerkung:** Seit dem 1. Oktober 2019 enthält das *Bedienungshandbuch zum XS/SC26-2 und SC10-2* die aktuellen Informationen zum Industrie-Ethernet. Das *Benutzerhandbuch zum Industrie-Ethernet* für die älteren Systeme ist in den EDS-Ordner eingebettet, der unter www.bannerengineering.com/safetycontroller zur Verfügung steht.

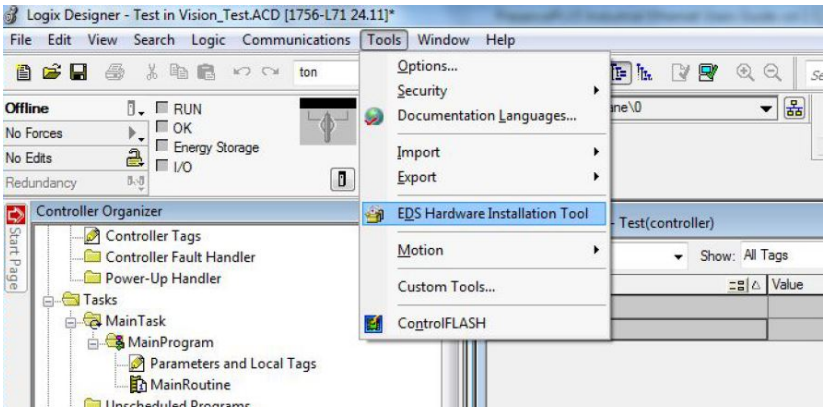
## 12.4.2 Installation der EDS-Datei des Sicherheitskontroller von Banner in der ControlLogix-Software

Registrieren Sie die EDS-Datei (elektronisches Datenblatt) mithilfe des **EDS-Hardwareinstallationstools**.

1. Klicken Sie dazu im Menü **Tools** auf **EDS-Hardwareinstallationstools**.
   Daraufhin wird der **EDS-Assistent von Rockwell Automation** angezeigt.

[15] Banner_XS26_SC26_SC10_300_2_1_03032020.eds ist abwärtskompatibel mit allen ProdCode 300-Steuerungen (XS26, SC26, SC10)

*Abbildung 152. Tools – EDS-Hardwareinstallationstool*




2. Auf **Weiter** klicken.
3. Wählen Sie die Option **EDS-Datei(en) registrieren** aus.

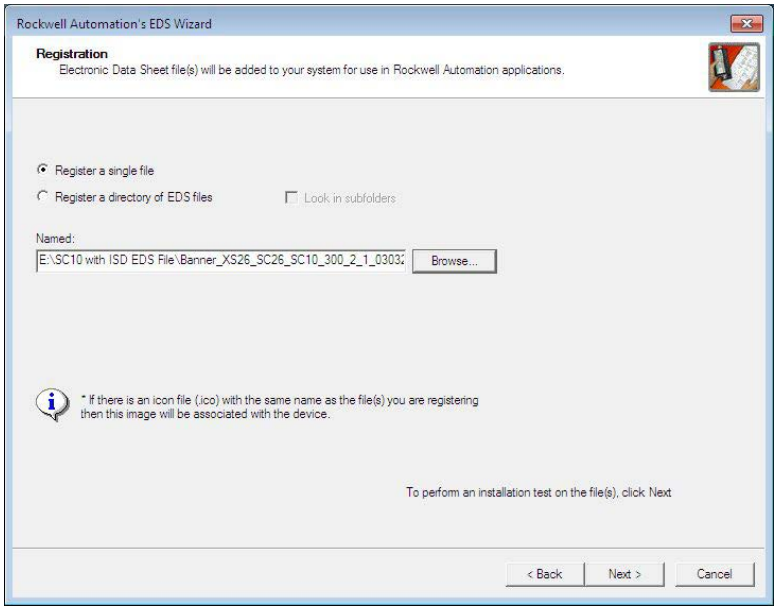
*Abbildung 153. EDS-Assistent von Rockwell Automation — Optionen*




4. Geben Sie den Speicherort der EDS-Datei an und klicken Sie auf **Weiter**.

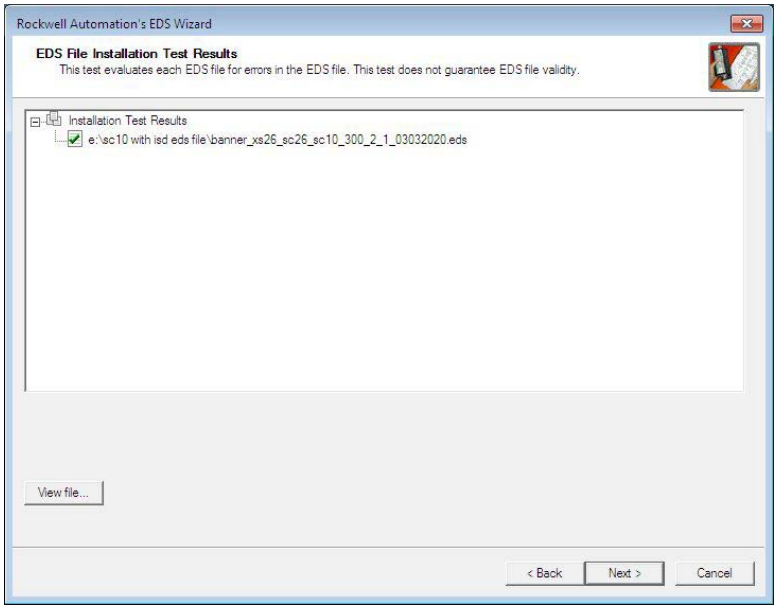
   Siehe Welche XS/SC26-2-EDS-Datei und -Dokumentation sollten Sie verwenden? auf Seite 159 für weitergehende Informationen.

*Abbildung 154. Auswahl der zu registrierenden Datei*



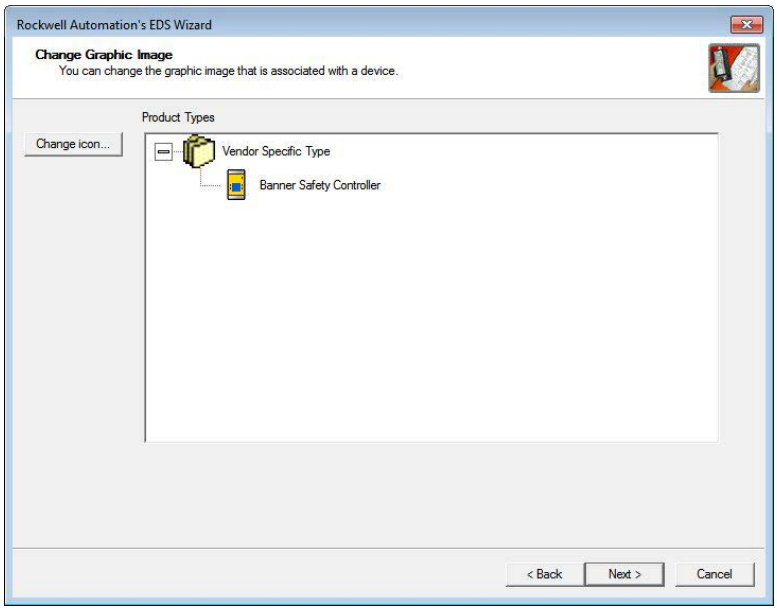
5. Klicken Sie auf **Weiter**, um die geprüfte Datei zu registrieren.

*Abbildung 155. Registrieren der geprüften Datei*



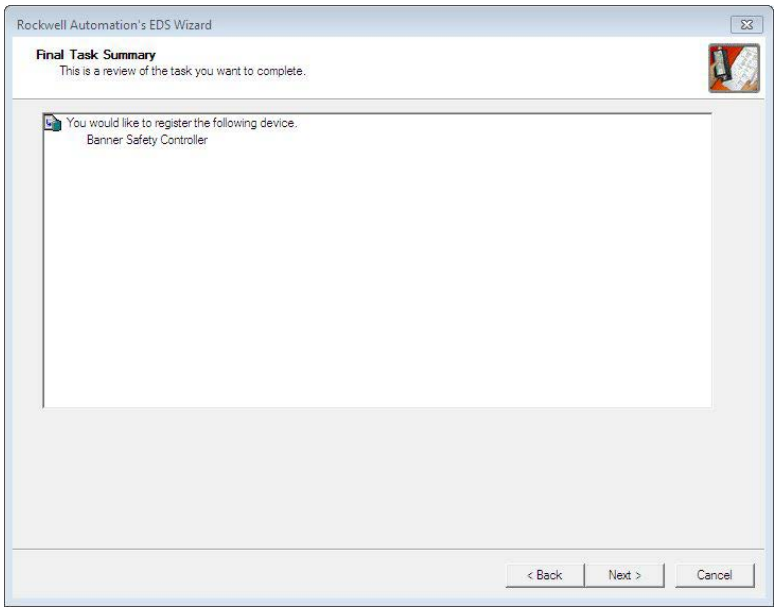

6. Klicken Sie auf **Weiter**, wenn Sie das Symbol für die EDS-Datei sehen.

*Abbildung 156. EDS-Assistent von Rockwell Automation*



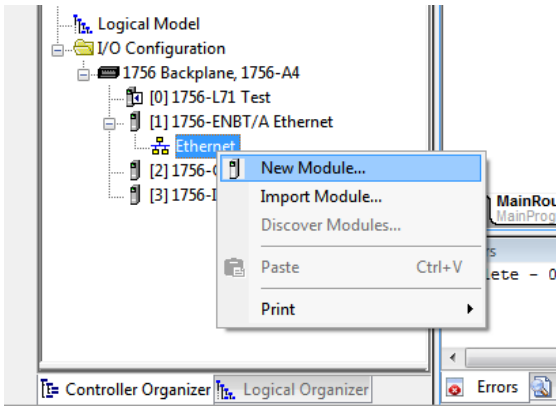

7. Klicken Sie auf **Weiter**, um die EDS-Datei zu registrieren.

*Abbildung 157. Registrieren der EDS-Datei*



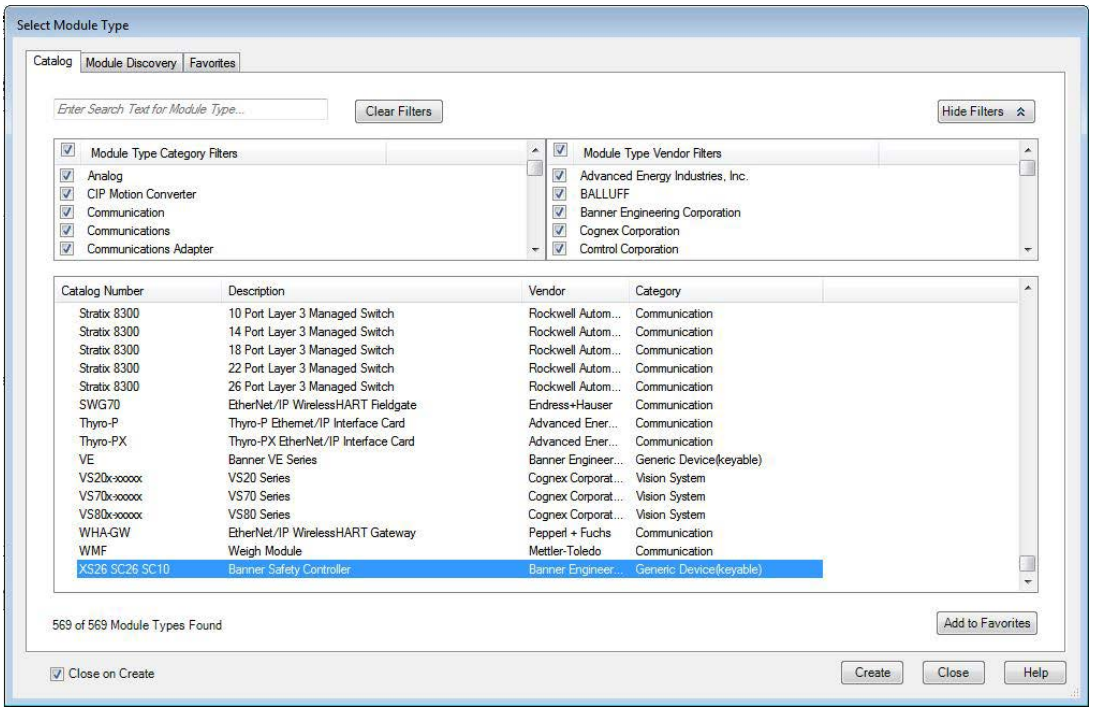

8. Klicken Sie auf **Beenden**, um den **EDS-Assistenten** zu schließen.
9. Klicken Sie mit der rechten Maustaste auf den Ethernet-Adapter der SPS und wählen Sie **Neues Modul...** aus.

*Abbildung 158. Neues Modul*



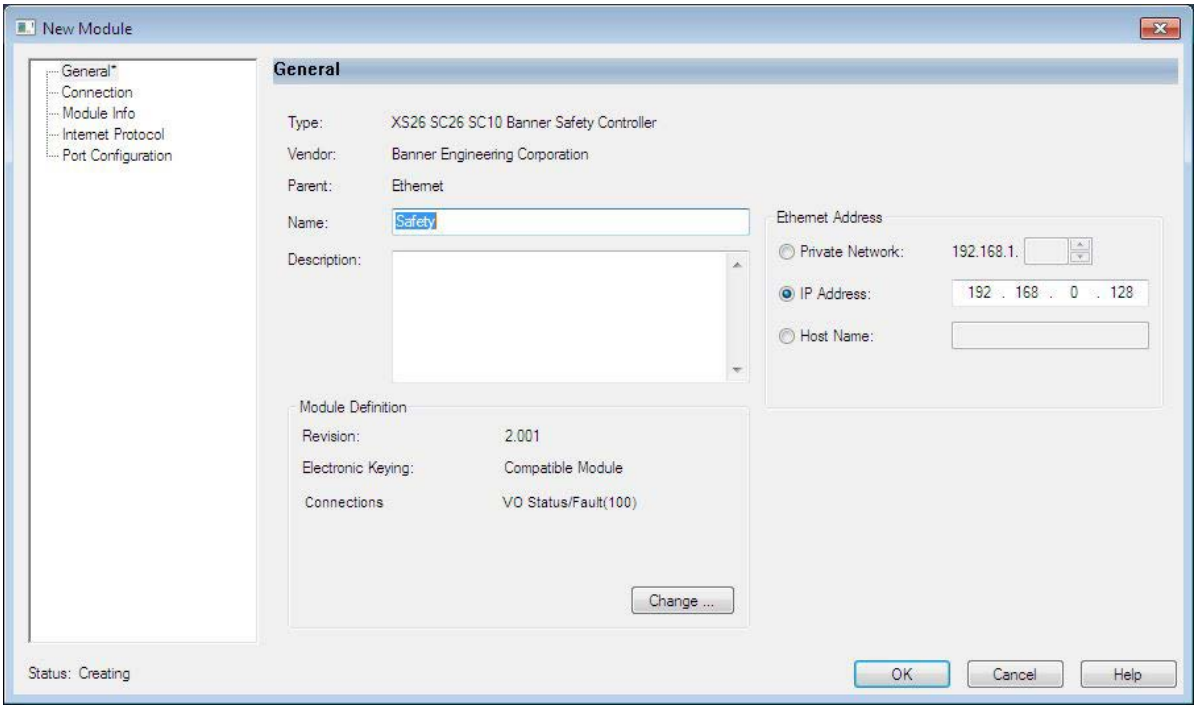

10. Suchen Sie das Gerät im Katalog und klicken Sie auf **Erstellen**.

*Abbildung 159. Auswahl des Modultyps*



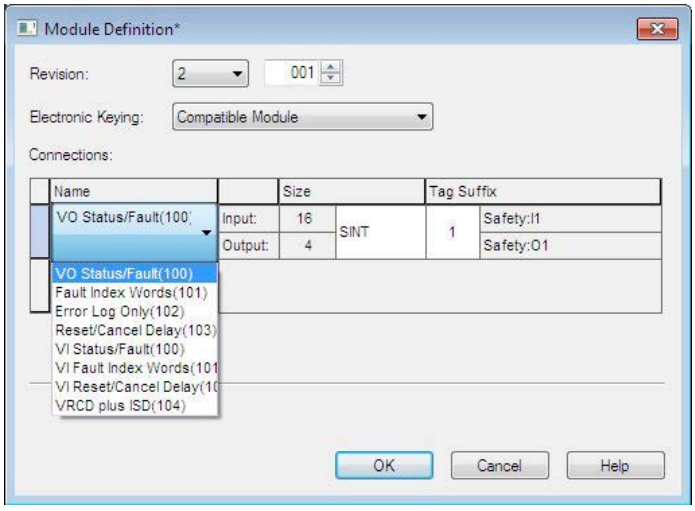
11. Geben Sie einen Namen, eine Beschreibung (optional) und die IP-Adresse für das Gerät ein.

*Abbildung 160. Neues Modul*




12. Klicken Sie im Feld **Moduldefinition** auf **Ändern**.

*Abbildung 161. Moduldefinition*




13. Wählen Sie im Fenster **Moduldefinition** die gewünschte Verbindung. Jedes Element in der Liste **Name** bezeichnet eine feste Gruppierung von Eingangs- und Ausgangsbaugruppeninstanzen:

**Anmerkung:** Nicht alle Verbindungsoptionen gelten für alle Sicherheitskontroller.

**VO-Status/Fehler (100):**

- O>T SPS-Ausgang/Sicherheitskontrollereingang Baugruppe 112 (0×70), Größe 2 16-Bit-Register
- T>O SPS-Eingang/Sicherheitskontrollerausgang Baugruppe 100 (0×64), Größe 8 16-Bit-Register

**Fehlerindexwörter (101):**

- O>T SPS-Ausgang/Sicherheitskontrollereingang Baugruppe 112 (0×70), Größe 2 16-Bit-Register
- T>O SPS-Eingang/Sicherheitskontrollerausgang Baugruppe 101 (0×65), Größe 104 16-Bit-Register

**Nur Fehlerprotokoll (102):**

- O>T SPS-Ausgang/Sicherheitskontrollereingang Baugruppe 112 (0×70), Größe 2 16-Bit-Register
- T>O SPS-Eingang/Sicherheitskontrollerausgang Baugruppe 102 (0×66), Größe 150 16-Bit-Register

**Reset-/Abbruchverzögerung (103):**

- O>T SPS-Ausgang/Sicherheitskontrollereingang Baugruppe 112 (0×70), Größe 2 16-Bit-Register
- T>O SPS-Eingang/Sicherheitskontrollerausgang Baugruppe 103 (0×67), Größe 35 16-Bit-Register

**VI-Status/Fehler (100):** [17]

- O>T SPS-Ausgang/Sicherheitskontrollereingang Baugruppe 113 (0×71), Größe 11 16-Bit-Register
- T>O SPS-Eingang/Sicherheitskontrollerausgang Baugruppe 100 (0×64), Größe 8 16-Bit-Register

**Fehlerindexwörter (101):** [17]

- O>T SPS-Ausgang/Sicherheitskontrollereingang Baugruppe 113 (0×71), Größe 11 16-Bit-Register
- T>O SPS-Eingang/Sicherheitskontrollerausgang Baugruppe 101 (0×65), Größe 104 16-Bit-Register

**VI-Reset-/Abbruchverzögerung(103):** [17]

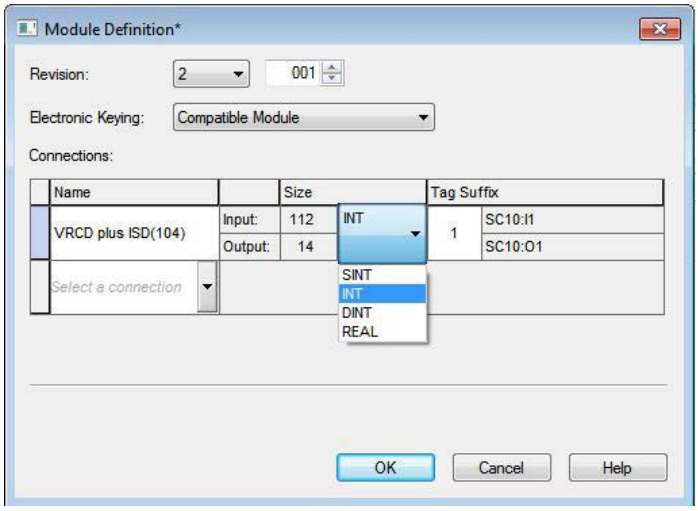
- O>T SPS-Ausgang/Sicherheitskontrollereingang Baugruppe 113 (0×71), Größe 11 16-Bit-Register
- T>O SPS-Eingang/Sicherheitskontrollerausgang Baugruppe 103 (0×67), Größe 35 16-Bit-Register

**VRCD Plus ISD (104):** [17]

- O>T SPS-Ausgang/Sicherheitskontrollereingang Baugruppe 114 (0×72), Größe 14 16-Bit-Register
- T>O SPS-Eingang/Sicherheitskontrollerausgang Baugruppe 104 (0×68), Größe 112 16-Bit-Registers

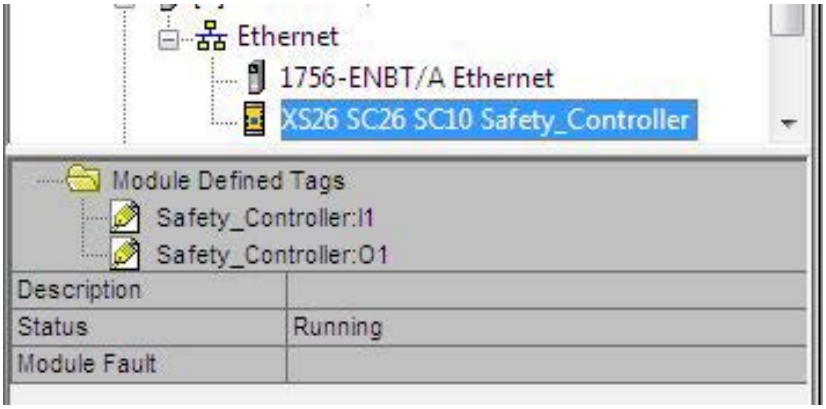
14. Wählen Sie als Datentyp **INT** aus.

*Abbildung 162. Moduldefinition – Datentyp*




15. Klicken Sie zweimal auf **OK** und laden Sie das Programm auf die SPS herunter.

*Abbildung 163. Auf SPS herunterladen*




Die Verbindung sieht wie die in Abbildung 163 auf Seite 165 aus.

[17] Wählen Sie eine der Verbindungen O > T Baugruppeninstanz 113 (0×71) oder 114 (0×72) aus, um die virtuelle Eingangs-/Abbruchverzögerung zu verwenden.

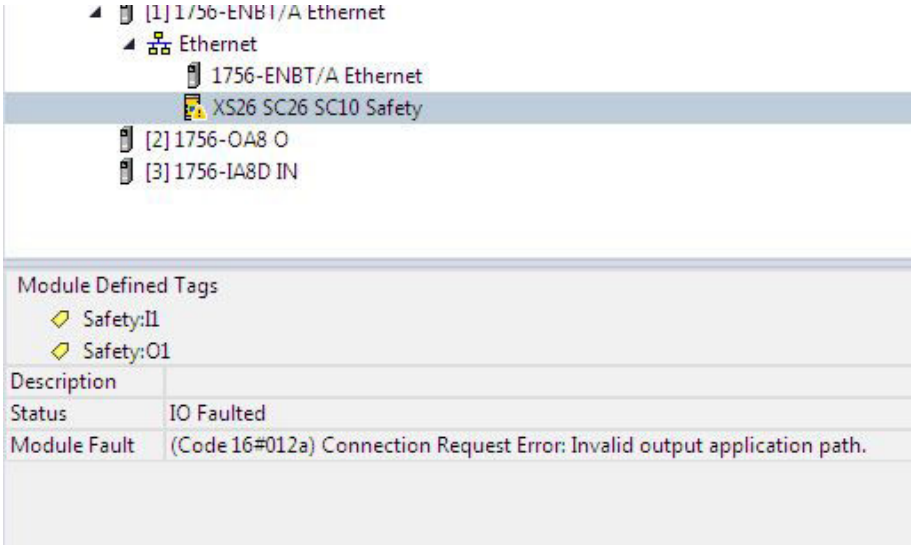
# Beispiele für fehlerhafte Verbindungsoptionen

Im Folgenden finden Sie Beispiele für die Auswahl einer falschen Verbindung aus der EDS-Datei.

## Beispiel 1

Versuch, eine "VI Status/Fehler (100)"-Verbindung auf einem Sicherheitskontroller zu verwenden, der keine virtuellen Eingänge unterstützt; O>T Baugruppeninstanz 113 existiert für diese Hardware nicht.

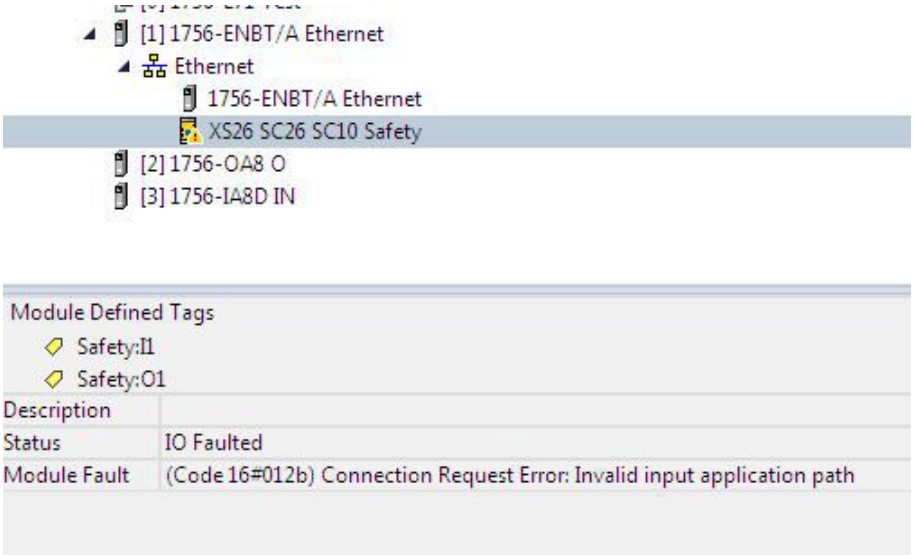
*Abbildung 164. Falsch: Verwendung von VI/Status-Fehlern auf einem Sicherheitskontroller, der diese Funktion nicht unterstützt*




## Beispiel 2

Versuch, die "Reset/Abbruchverzögerung (103)"-Verbindung auf einem Sicherheitskontroller zu verwenden, der keine virtuellen Eingänge unterstützt; T>O Baugruppeninstanz 103 existiert für diese Hardware nicht.

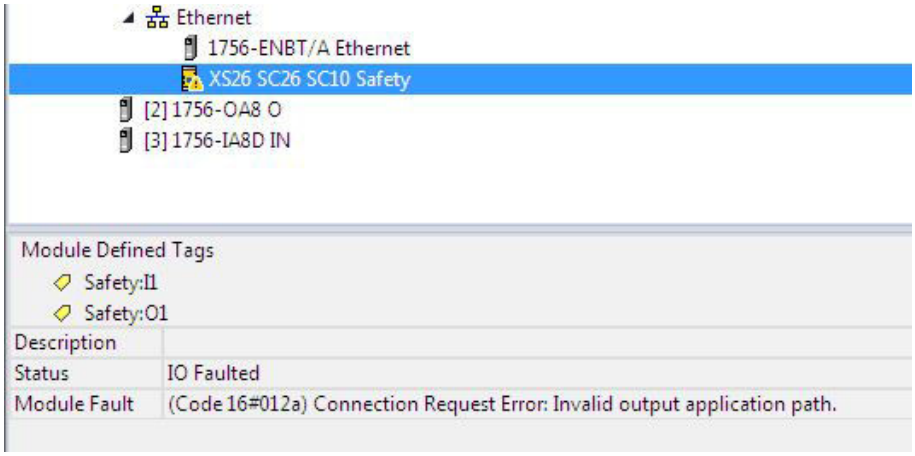
*Abbildung 165. Falsch: Reset/Abbruchverzögerung auf einem Sicherheitskontroller, der diese Funktion nicht unterstützt*




## Beispiel 3

Versuch, eine "VRCD plus ISD (104)"-Verbindung auf einem Sicherheitskontroller zu verwenden, der ISD nicht unterstützt; T>O Baugruppeninstanz 104 existiert für diese Hardware nicht.

*Abbildung 166. Falsch: VRCD plus ISD auf einem Sicherheitskontroller, der diese Funktion nicht unterstützt*



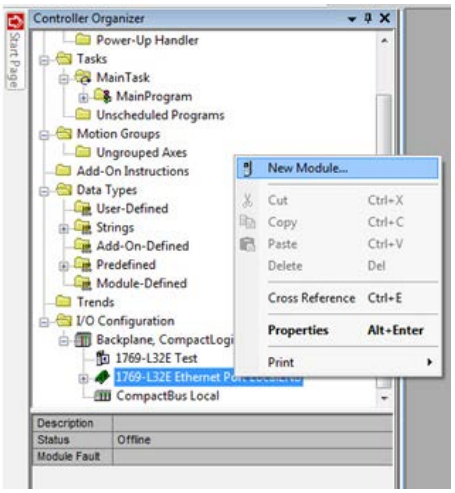

## 12.4.3 RSLogix5000-Konfiguration (implizite Nachrichten)

Um eine implizite Konfiguration der Klasse 1 für den Sicherheitskontroller mittels EtherNet/IP bei Verwendung einer SPS der ControlLogix-Serie zu erstellen, konfigurieren Sie den Sicherheitskontroller als "Allgemeines Ethernet-Modul". Die nachfolgenden Schritte beschreiben eine Beispielkonfiguration eines Banner-Geräts.

**Anmerkung:** Dieses ist eine Beispielkonfiguration.

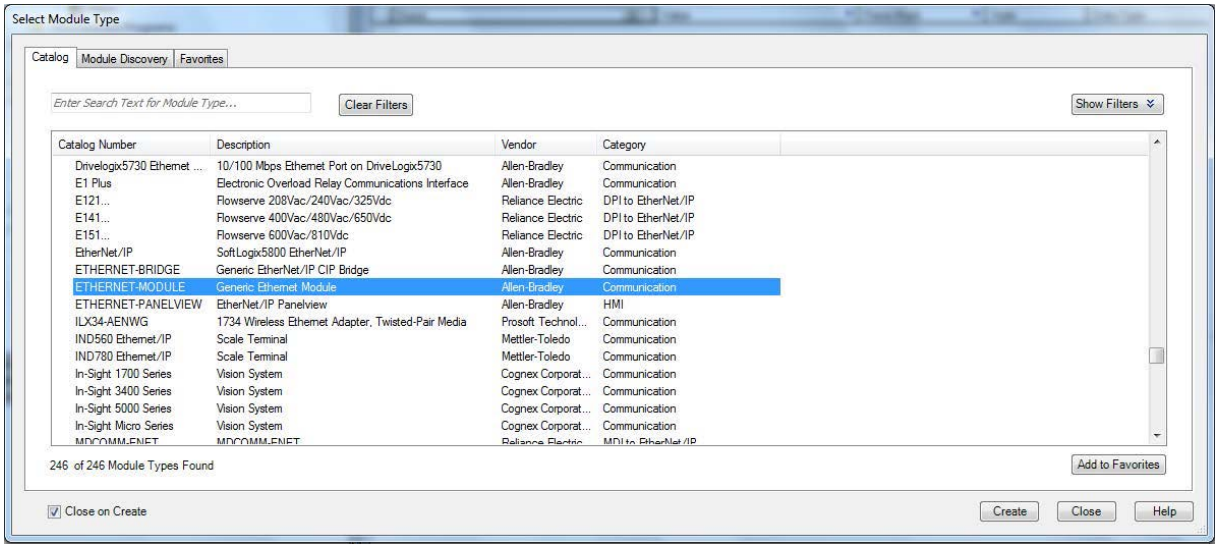
1. Fügen Sie der Ethernetkarte der SPS ein allgemeines Ethernet-Modul hinzu.
   a) Klicken Sie auf **Neues Modul**.

*Abbildung 167. Hinzufügen eines Ethernet-Moduls*



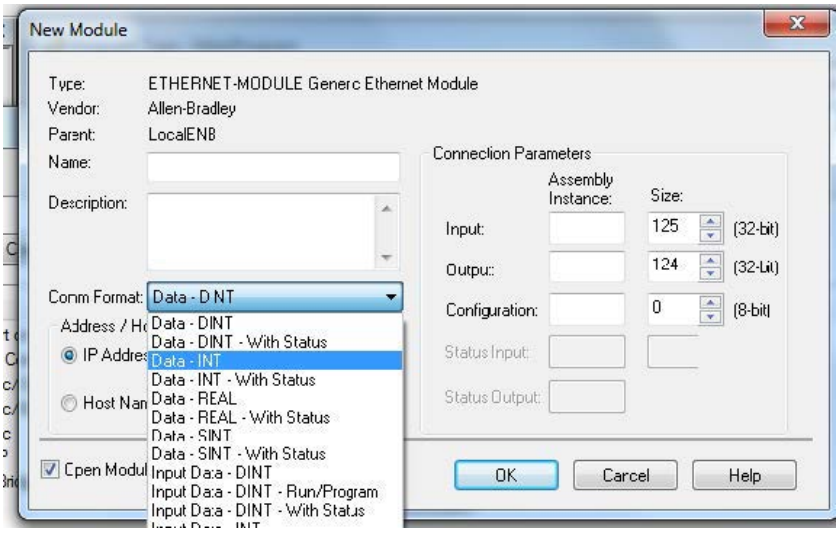

   b) Wählen Sie aus dem Katalog **Allgemeines Ethernet-Modul** aus.

*Abbildung 168. Auswahl des Moduls*



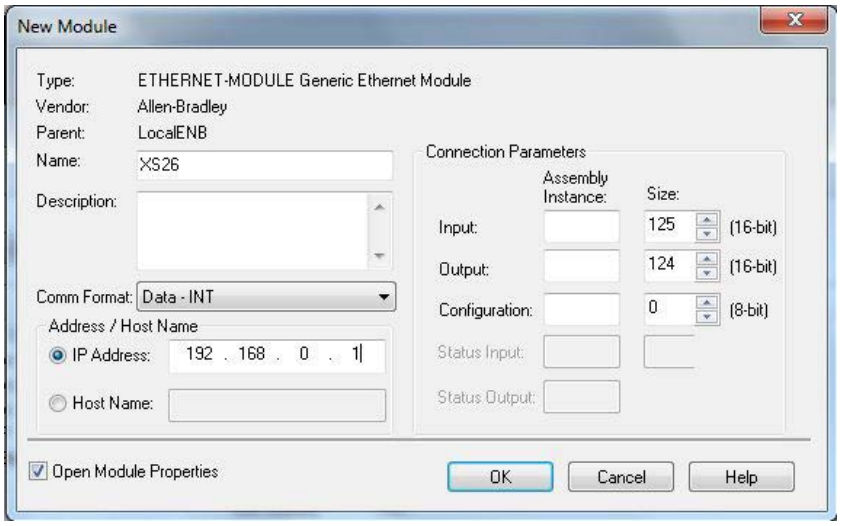

2. Konfigurieren Sie die Moduleigenschaften.
   a) Wählen Sie **INT** aus der Liste **Kommunikationsformat** aus (Standardeinstellung ist DINT).

*Abbildung 169. Festlegen des Kommunikationsformats*




   b) Geben Sie einen **Modulnamen** und die **IP-Adresse** des Sicherheitskontrollers ein.
   Die Standard-IP-Adresse des Sicherheitskontrollers ist 192.168.0.128 mit der Subnetzmaske 255.255.255.0.

*Abbildung 170. Hinzufügen von Name und IP-Adresse*



c) Wählen Sie unter "Connection Parameters (Verbindungsparameter)" eine der verschiedenen Baugruppenobjektkonfigurationen aus, die möglich sind. Weitere Informationen zu der jeweiligen Auswahl finden Sie unter Eingänge zum Sicherheitskontroller (Ausgänge von der SPS) auf Seite 172 und Ausgänge vom Sicherheitskontroller (Eingänge zur SPS) auf Seite 174.

**Anmerkung:** Wählen Sie eine der Verbindungen O > T Baugruppeninstanz 113 (0×71) aus, um den virtuellen Eingang/Abbruchverzögerung zu verwenden.

*Abbildung 171. SPS-Eingang Baugruppe 100 (0x64), Größe 8 Wörter (VO-Status/Fehler)*

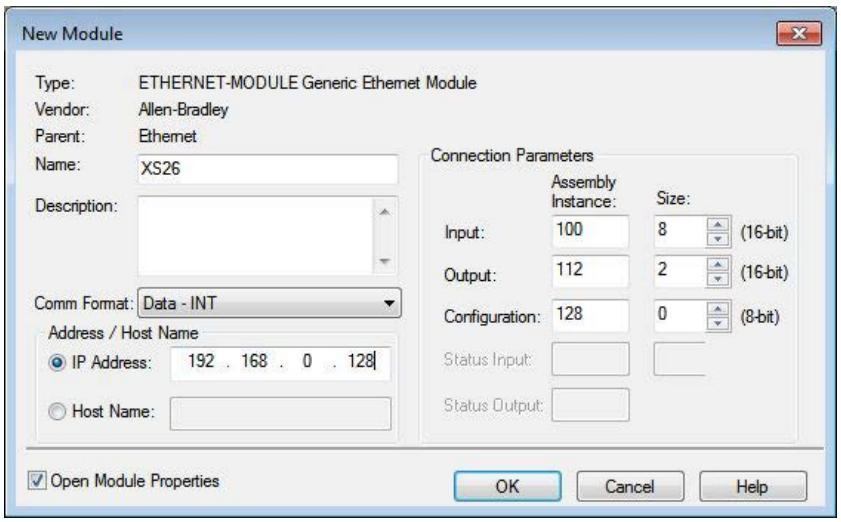



*Abbildung 172. SPS-Eingang Baugruppe 101 (0x65), Größe 104 Wörter (Fehlerindexwörter)*

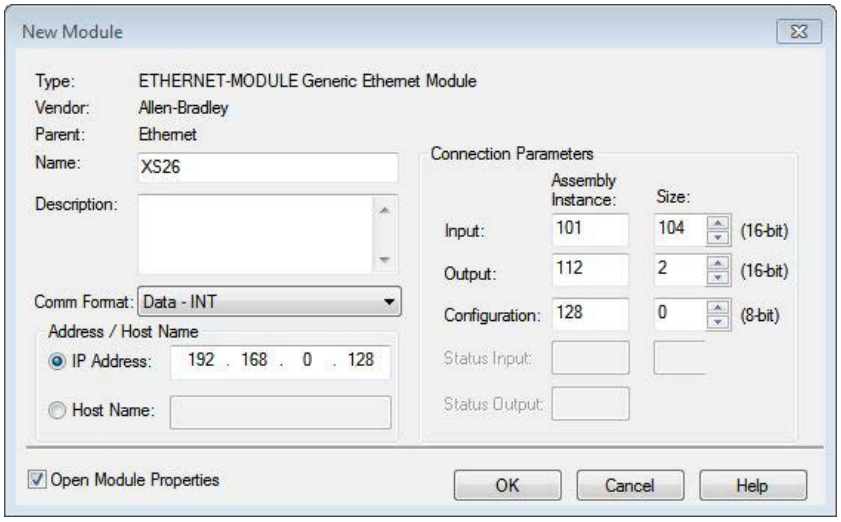



*Abbildung 173. SPS-Eingang Baugruppe 102 (0x66), Größe 150 Wörter (nur Fehlerprotokoll des Sicherheitskontrollers)*

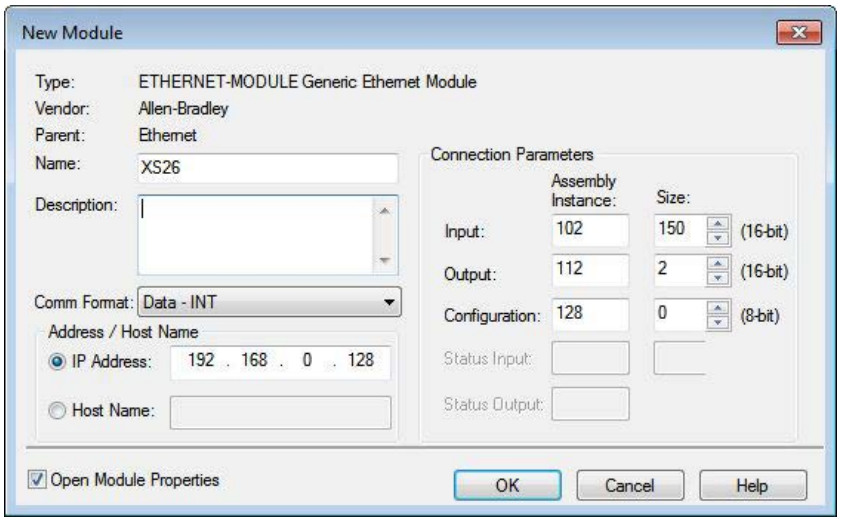


*Abbildung 174. SPS-Eingang Baugruppe 103 (0x67), Größe 35 Wörter (Reset-/Abbruchverzögerung)*

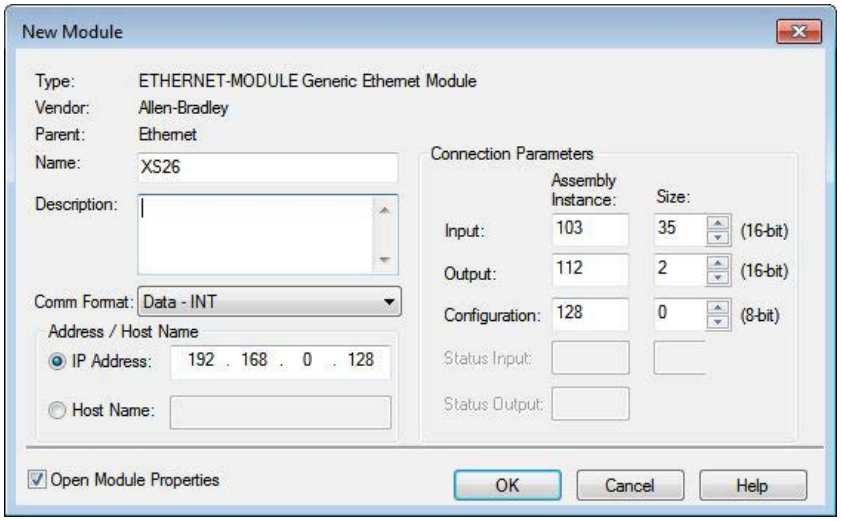



*Abbildung 175. SPS-Eingang Baugruppe 100 (0x64), Größe 8 Wörter (VI-Status/Fehler)*

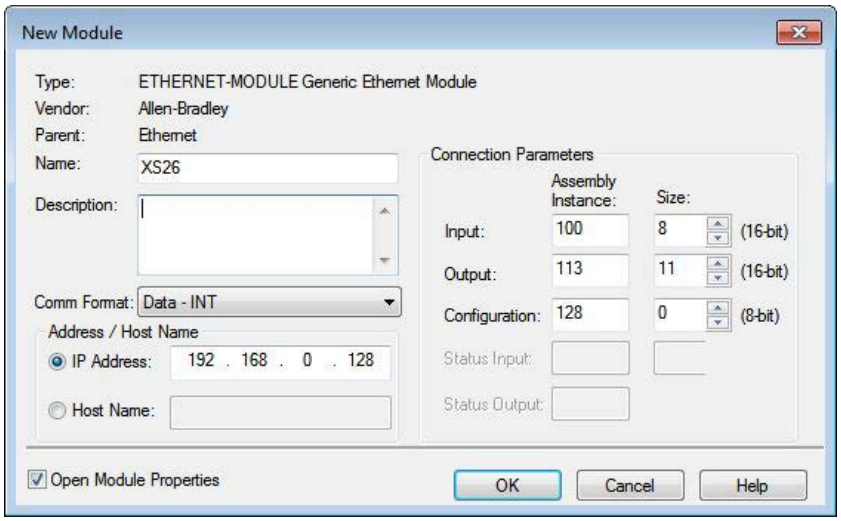



*Abbildung 176. SPS-Eingang Baugruppe 101 (0x65), Größe 104 Wörter (VI-Fehlerindexwörter)*

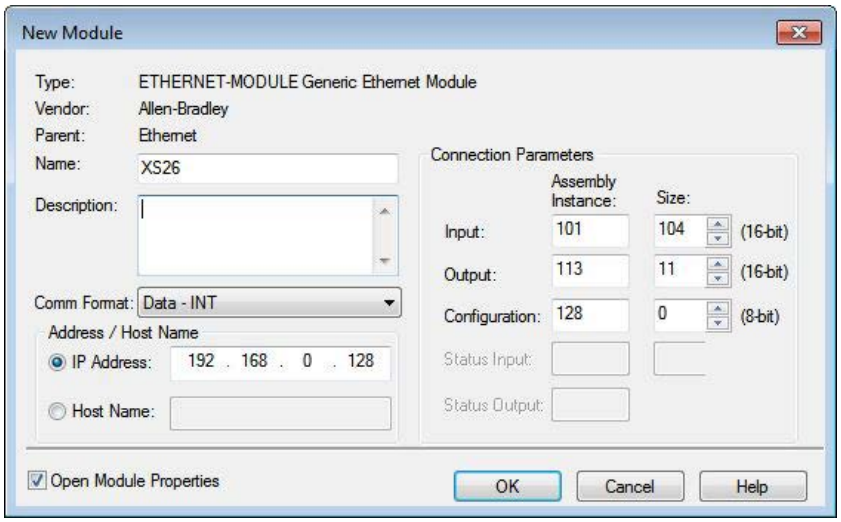


*Abbildung 177. SPS-Eingang Baugruppe 103 (0×67), Größe 35 Wörter (VI-Reset-/Abbruchverzögerung)*

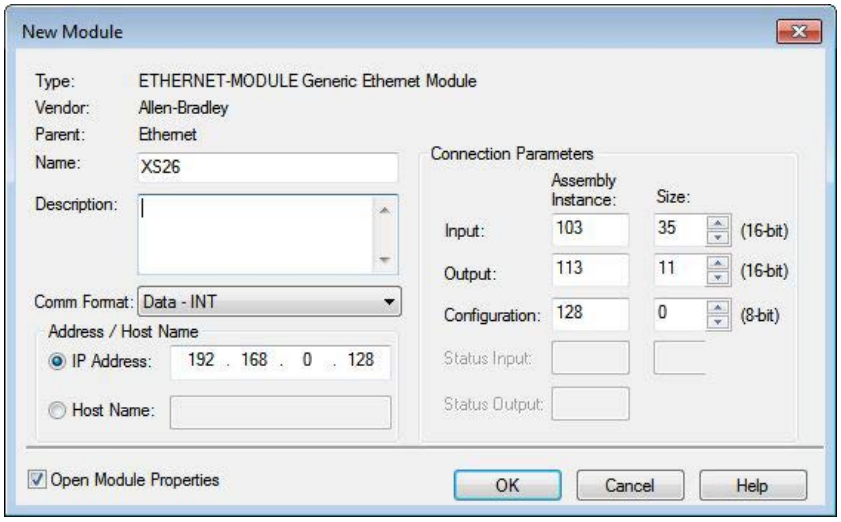
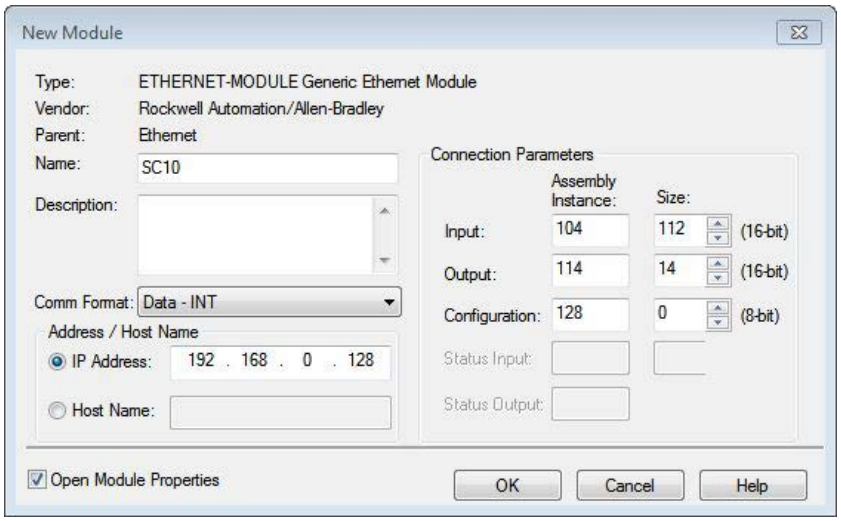


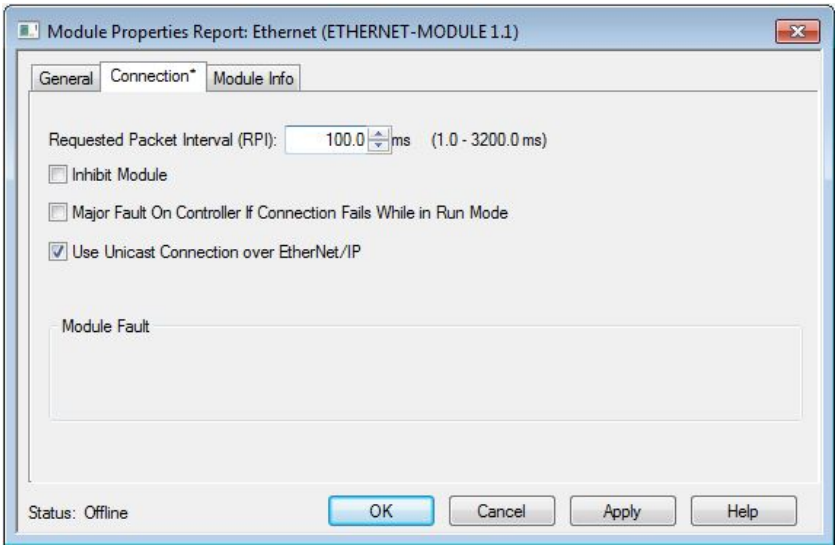

*Abbildung 178. SPS-Eingang Baugruppe 104 (0×68), Größe 112 Wörter (VRCD plus ISD)*




d) Gehen Sie zur Registerkarte **Verbindung** und legen Sie die Parameter fest:
   - Geben Sie das **angeforderte Paketintervall (RPI)** ein.
   - Aktivieren oder deaktivieren Sie das Kontrollkästchen **Unicast-Verbindung über Ethernet/IP verwenden**.

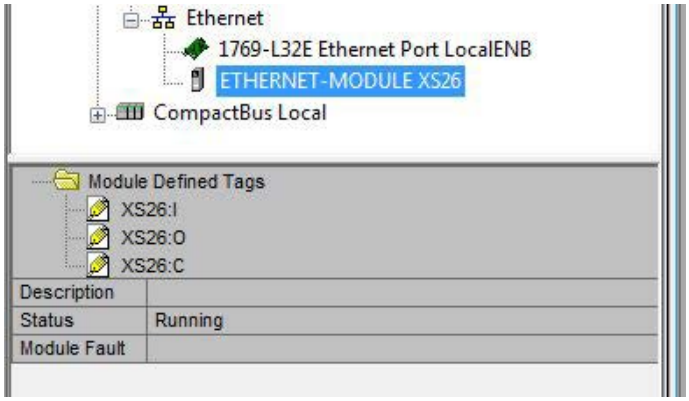
**Anmerkung:** Das empfohlene Mindest-RPI beträgt 100 ms.

*Abbildung 179. Verbindungsparameter*



Wenn die Konfiguration des Moduls erfolgreich war, werden folgende Informationen angezeigt:

*Abbildung 180. Erfolgreiche Konfiguration*




I = Eingänge zur SPS (Ausgänge vom Sicherheitskontroller)

O = Ausgänge von der SPS (Eingänge zum Sicherheitskontroller – nicht verwendet)

C = Konfiguration (nicht verwendet)

3. Suchen Sie in der Liste **Kontroller-Tags** die Speicherzuordnung. Die 8 Eingangswörter von der Baugruppeninstanz 100 sind nachfolgend als Beispiel gezeigt.

*Abbildung 181. Speicherzuordnung*

| | | | | |
|---|---|---|---|---|
| XS26:I | {...} | {...} | | AB:ETHERNET_MODULE_ |
| XS26:I.Data | {...} | {...} | Decimal | INT[8] |
| XS26:I.Data[0] | 1 | | Decimal | INT |
| XS26:I.Data[1] | 128 | | Decimal | INT |
| XS26:I.Data[2] | 0 | | Decimal | INT |
| XS26:I.Data[3] | 8 | | Decimal | INT |
| XS26:I.Data[4] | 0 | | Decimal | INT |
| XS26:I.Data[5] | 0 | | Decimal | INT |
| XS26:I.Data[6] | 0 | | Decimal | INT |
| XS26:I.Data[7] | 0 | | Decimal | INT |

In dem obigen Beispiel sind die virtuellen Ausgänge 1, 24 und 52 eingeschaltet.

VO1 ist Wort 0, Bit 0 > 2^0 = 1
VO24 ist Wort 1, Bit 7 > 2^7 = 128
VO52 ist Wort 3, Bit 3 > 2^3 = 8

# 12.4.4 Eingänge zum Sicherheitskontroller (Ausgänge von der SPS)

## SPS-Ausgangsbaugruppeninstanz 112 (0×70) – 2 Register (Einfacher VI)

Der Sicherheitskontroller kann die Instanz 112 (0×70) mit einer Größe von zwei Registern (16-Bit) zum Senden der virtuellen Eingänge 1–32 an den Sicherheitskontroller verwenden.

*Tabelle 9. SPS-Ausgang Baugruppeninstanz 112 (0×70) — Sicherheitskontrollereingänge O > T*

| WORD # | WORD NAME | DATENTYP |
|---|---|---|
| 0 | Virtueller Eingang Ein/Aus (1–16) | 16-Bit-Ganzzahl |
| 1 | Virtueller Eingang Ein/Aus (17–32) | 16-Bit-Ganzzahl |

## SPS-Ausgangsbaugruppeninstanz 113 (0×71) – 11 Register (Erweiterter VI plus VRCD)

Der Sicherheitskontroller verwendet Instanz 113 (0×71) [21] mit einer Größe von elf Registern (16-Bit) als Eingangsbaugruppe (SPS-Ausgang) beim Senden von virtuellen Eingängen, Resets und Abbruchverzögerungen an den Sicherheitskontroller.

[21] Diese Baugruppe mit 11 Wörtern nennt sich 112 (0x70) für FID 2-Sicherheitskontroller mit Datumcodes vor und einschließlich "1716". Siehe Welche XS/SC26-2-EDS-Datei und -Dokumentation sollten Sie verwenden? auf Seite 159 für weitergehende Informationen.

*Tabelle 10. SPS-Ausgang Baugruppeninstanz 113 (0x71) — Sicherheitskontrollereingänge O > T*

| WORD # | WORD NAME | DATENTYP |
|---|---|---|
| 0 | Virtueller Eingang Ein/Aus (1–16) | 16-Bit-Ganzzahl |
| 1 | Virtueller Eingang Ein/Aus (17–32) | 16-Bit-Ganzzahl |
| 2 | Virtueller Eingang Ein/Aus (33–48) | 16-Bit-Ganzzahl |
| 3 | Virtueller Eingang Ein/Aus (49–64) | 16-Bit-Ganzzahl |
| 4 | *reserviert* | 16-Bit-Ganzzahl |
| 5 | *reserviert* | 16-Bit-Ganzzahl |
| 6 | *reserviert* | 16-Bit-Ganzzahl |
| 7 | *reserviert* | 16-Bit-Ganzzahl |
| 8 | Virtuelle Reset-/Abbruchverzögerung (1–16) [RCD-Registerbits] (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 57) | 16-Bit-Ganzzahl |
| 9 | *reserviert* | 16-Bit-Ganzzahl |
| 10 | RCD-Auslösecode [RCD-Aktivierung Register] (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 57) | 16-Bit-Ganzzahl |

## SPS-Ausgabebaugruppen-Instanz 114 (0×72) – 14 Register (Erweiterter VI, VRCD, plus ISD)

Der Sicherheitskontroller verwendet Instanz 114 (0×72) mit einer Größe von 14 Registern (16-Bit) als Eingangsbaugruppe (SPS-Ausgang) beim Senden von virtuellen Eingängen, Resets und Abbruchverzögerungen an den Sicherheitskontroller und zum Abrufen der Leistungs- und Statusinformationen über ISD-Geräte.

*Tabelle 11. SPS-Ausgang Baugruppeninstanz 114 (0×72) — Sicherheitskontrollereingänge O > T*

| WORD # | WORD NAME | DATENTYP |
|---|---|---|
| 0 | Virtueller Eingang Ein/Aus (1–16) | 16-Bit-Ganzzahl |
| 1 | Virtueller Eingang Ein/Aus (17–32) | 16-Bit-Ganzzahl |
| 2 | Virtueller Eingang Ein/Aus (33–48) | 16-Bit-Ganzzahl |
| 3 | Virtueller Eingang Ein/Aus (49–64) | 16-Bit-Ganzzahl |
| 4 | *reserviert* | 16-Bit-Ganzzahl |
| 5 | *reserviert* | 16-Bit-Ganzzahl |
| 6 | *reserviert* | 16-Bit-Ganzzahl |
| 7 | *reserviert* | 16-Bit-Ganzzahl |
| 8 | Virtuelle Reset-/Abbruchverzögerung (1–16) [RCD-Registerbits] (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 57) | 16-Bit-Ganzzahl |
| 9 | *reserviert* | 16-Bit-Ganzzahl |
| 10 | RCD-Auslösecode [RCD-Aktivierung Register] (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 57) | 16-Bit-Ganzzahl |
| 11 | ISD-Leseanforderung (siehe Leistungs- und Statusinformationen zu einem einzelnen Gerät über ISD anfordern auf Seite 47) | 16-Bit-Ganzzahl |
| 12 | ISD-Reihe angefordert (siehe Leistungs- und Statusinformationen zu einem einzelnen Gerät über ISD anfordern auf Seite 47) | 16-Bit-Ganzzahl |
| 13 | ISD-Gerät angefordert (siehe Leistungs- und Statusinformationen zu einem einzelnen Gerät über ISD anfordern auf Seite 47) | 16-Bit-Ganzzahl |

# 12.4.5 Ausgänge vom Sicherheitskontroller (Eingänge zur SPS)

Es stehen fünf Optionen für Baugruppenobjekte der Sicherheitskontrollerausgänge zur Verfügung.

Die erste und kleinste Option umfasst Informationen zu den virtuellen Ausgängen und dazu, ob dort Fehler vorliegen. Die zweite Option enthält zusätzlich erweiterte Daten wie den Grund, warum die jeweiligen Sicherheitsausgänge inaktiv sind, sowie weitere beschreibende Fehlerinformationen für die virtuellen Ausgänge. Die dritte Option dient ausschließlich dem Zugriff auf das Fehlerprotokoll des Sicherheitskontrollers. Die vierte Option wird für die Rückmeldung virtueller manueller Reset und Abbruch Ausschaltverzögerung verwendet. Die fünfte Option erlaubt Zugriff auf Feedback- und ISD-Informationen zum virtuellen manuellen Reset und die Abbruchverzögerung. Alle fünf Optionen sind in den folgenden Abschnitten dargestellt.

## SPS-Eingang Baugruppeninstanz 100 (0×64) — 8 Register (VO-Status/Fehler)

Diese Baugruppeninstanz umfasst nur allgemeine Informationen zum Status der ersten 64 virtuellen Ausgänge.

*Tabelle 12. SPS-Eingang Baugruppeninstanz 100 (0×64) — Sicherheitskontrollerausgänge T > O*

| WORD # | WORD NAME | DATENTYP |
|---|---|---|
| 0 | VO1–VO16 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 1 | VO17–VO32 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 2 | VO33–VO48 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 3 | VO49–VO64 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 4 | Fehlerbits für VO1–VO16 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 5 | Fehlerbits für VO17–VO32 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 6 | Fehlerbits für VO33–VO48 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 7 | Fehlerbits für VO49–VO64 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |

## SPS-Eingang Baugruppeninstanz 101 (0×65) — 104 Register (Fehlerindexwörter)

Die Baugruppeninstanz enthält den Status der ersten 64 virtuellen Ausgänge sowie erweiterte Informationen zu möglichen Fehlercodes und den Status der 2 Sicherheitsausgänge.

*Tabelle 13. SPS-Eingang Baugruppeninstanz 101 (0×65) — Sicherheitskontrollerausgänge T > O*

| WORD # | WORD NAME | DATENTYP |
|---|---|---|
| 0 | VO1–VO16 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 1 | VO17–VO32 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 2 | VO33–VO48 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 3 | VO49–VO64 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 4 | Fehlerbits für VO1–VO16 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 5 | Fehlerbits für VO17–VO32 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 6 | Fehlerbits für VO33–VO48 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 7 | Fehlerbits für VO49–VO64 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 8–39 | *reserviert* | 16-Bit-Ganzzahl |
| 40 | VO1-Fehlerindex | 16-Bit-Ganzzahl |
| 41 | VO2-Fehlerindex | 16-Bit-Ganzzahl |
| 42 | VO3-Fehlerindex | 16-Bit-Ganzzahl |
| 43 | VO4-Fehlerindex | 16-Bit-Ganzzahl |
| 44 | VO5-Fehlerindex | 16-Bit-Ganzzahl |
| 45 | VO6-Fehlerindex | 16-Bit-Ganzzahl |

| WORD # | WORD NAME | DATENTYP |
|---|---|---|
| 46 | VO7-Fehlerindex | 16-Bit-Ganzzahl |
| 47 | VO8-Fehlerindex | 16-Bit-Ganzzahl |
| 48 | VO9-Fehlerindex | 16-Bit-Ganzzahl |
| 49 | VO10-Fehlerindex | 16-Bit-Ganzzahl |
| 50 | VO11-Fehlerindex | 16-Bit-Ganzzahl |
| 51 | VO12-Fehlerindex | 16-Bit-Ganzzahl |
| 52 | VO13-Fehlerindex | 16-Bit-Ganzzahl |
| 53 | VO14-Fehlerindex | 16-Bit-Ganzzahl |
| 54 | VO15-Fehlerindex | 16-Bit-Ganzzahl |
| 55 | VO16-Fehlerindex | 16-Bit-Ganzzahl |
| 56 | VO17-Fehlerindex | 16-Bit-Ganzzahl |
| 57 | VO18-Fehlerindex | 16-Bit-Ganzzahl |
| 58 | VO19-Fehlerindex | 16-Bit-Ganzzahl |
| 59 | VO20-Fehlerindex | 16-Bit-Ganzzahl |
| 60 | VO21-Fehlerindex | 16-Bit-Ganzzahl |
| 61 | VO22-Fehlerindex | 16-Bit-Ganzzahl |
| 62 | VO23-Fehlerindex | 16-Bit-Ganzzahl |
| 63 | VO24-Fehlerindex | 16-Bit-Ganzzahl |
| 64 | VO25-Fehlerindex | 16-Bit-Ganzzahl |
| 65 | VO26-Fehlerindex | 16-Bit-Ganzzahl |
| 66 | VO27-Fehlerindex | 16-Bit-Ganzzahl |
| 67 | VO28-Fehlerindex | 16-Bit-Ganzzahl |
| 68 | VO29-Fehlerindex | 16-Bit-Ganzzahl |
| 69 | VO30-Fehlerindex | 16-Bit-Ganzzahl |
| 70 | VO31-Fehlerindex | 16-Bit-Ganzzahl |
| 71 | VO32-Fehlerindex | 16-Bit-Ganzzahl |
| 72 | VO33-Fehlerindex | 16-Bit-Ganzzahl |
| 73 | VO34-Fehlerindex | 16-Bit-Ganzzahl |
| 74 | VO35-Fehlerindex | 16-Bit-Ganzzahl |
| 75 | VO36-Fehlerindex | 16-Bit-Ganzzahl |
| 76 | VO37-Fehlerindex | 16-Bit-Ganzzahl |
| 77 | VO38-Fehlerindex | 16-Bit-Ganzzahl |
| 78 | VO39-Fehlerindex | 16-Bit-Ganzzahl |
| 79 | VO40-Fehlerindex | 16-Bit-Ganzzahl |
| 80 | VO41-Fehlerindex | 16-Bit-Ganzzahl |
| 81 | VO42-Fehlerindex | 16-Bit-Ganzzahl |
| 82 | VO43-Fehlerindex | 16-Bit-Ganzzahl |
| 83 | VO44-Fehlerindex | 16-Bit-Ganzzahl |
| 84 | VO45-Fehlerindex | 16-Bit-Ganzzahl |
| 85 | VO46-Fehlerindex | 16-Bit-Ganzzahl |
| 86 | VO47-Fehlerindex | 16-Bit-Ganzzahl |
| 87 | VO48-Fehlerindex | 16-Bit-Ganzzahl |
| 88 | VO49-Fehlerindex | 16-Bit-Ganzzahl |

| WORD # | WORD NAME | DATENTYP |
|---|---|---|
| 89 | VO50-Fehlerindex | 16-Bit-Ganzzahl |
| 90 | VO51-Fehlerindex | 16-Bit-Ganzzahl |
| 91 | VO52-Fehlerindex | 16-Bit-Ganzzahl |
| 92 | VO53-Fehlerindex | 16-Bit-Ganzzahl |
| 93 | VO54-Fehlerindex | 16-Bit-Ganzzahl |
| 94 | VO55-Fehlerindex | 16-Bit-Ganzzahl |
| 95 | VO56-Fehlerindex | 16-Bit-Ganzzahl |
| 96 | VO57-Fehlerindex | 16-Bit-Ganzzahl |
| 97 | VO58-Fehlerindex | 16-Bit-Ganzzahl |
| 98 | VO59-Fehlerindex | 16-Bit-Ganzzahl |
| 99 | VO60-Fehlerindex | 16-Bit-Ganzzahl |
| 100 | VO61-Fehlerindex | 16-Bit-Ganzzahl |
| 101 | VO62-Fehlerindex | 16-Bit-Ganzzahl |
| 102 | VO63-Fehlerindex | 16-Bit-Ganzzahl |
| 103 | VO64-Fehlerindex | 16-Bit-Ganzzahl |

**Fehlerindex-Wörter eines virtuellen Ausgangs (VO)**

Mit der Fehlerindexnummer eines virtuellen Ausgangs kann der mit einem bestimmten virtuellen Ausgang verknüpfte Fehlercode als einzelne 16-Bit-Ganzzahl dargestellt werden. Dieser Wert entspricht dem Wert des Fehlermeldungsindex für einen bestimmten virtuellen Ausgang. Siehe Fehlercode-Tabelle für XS/SC26-2 auf Seite 283 und SC10-2 Fehlercode-Tabelle auf Seite 288. Hinweis: Nicht jeder virtuelle Ausgang hat einen verknüpften Fehlerindex.

## SPS-Eingang Baugruppeninstanz 102 (0×66) — 150 Register (nur Fehlerprotokoll)

Mit dieser Baugruppeninstanz wird ausschließlich auf die Fehlerprotokollinformationen auf dem Sicherheitskontroller zugegriffen.

Hinweis: Diese Baugruppeninstanz umfasst nur Informationen zum Status der virtuellen Ausgänge.

Der Sicherheitskontroller kann 10 Fehler im Protokoll speichern. Fehler Nr. 1 ist der neueste Fehler. Je höher die Nummer, desto älter die Fehler.

*Tabelle 14. SPS-Eingang Baugruppeninstanz 102 (0–66) — Sicherheitskontrollerausgänge T > O*

| WORD # | WORD NAME | DATENTYP |
|---|---|---|
| 0–1 | Fehler Nr. 1 Zeitstempel | 32-Bit-Ganzzahl |
| 2–9 | Fehler Nr. 1 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 10 | Fehler Nr. 1 Fehlercode | 16-Bit-Ganzzahl |
| 11 | Fehler Nr. 1 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 12 | Fehler Nr. 1 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 13–14 | *reserviert* | 16-Bit-Ganzzahl |
| 15–16 | Fehler Nr. 2 Zeitstempel | 32-Bit-Ganzzahl |
| 17–24 | Fehler Nr. 2 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 25 | Fehler Nr. 2 Fehlercode | 16-Bit-Ganzzahl |
| 26 | Fehler Nr. 2 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 27 | Fehler Nr. 2 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 28–29 | *reserviert* | 16-Bit-Ganzzahl |
| 30–31 | Fehler Nr. 3 Zeitstempel | 32-Bit-Ganzzahl |
| 32–39 | Fehler Nr. 3 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |

| WORD # | WORD NAME | DATENTYP |
|---|---|---|
| 40 | Fehler Nr. 3 Fehlercode | 16-Bit-Ganzzahl |
| 41 | Fehler Nr. 3 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 42 | Fehler Nr. 3 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 43–44 | *reserviert* | 16-Bit-Ganzzahl |
| 45–46 | Fehler Nr. 4 Zeitstempel | 32-Bit-Ganzzahl |
| 47–54 | Fehler Nr. 4 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 55 | Fehler Nr. 4 Fehlercode | 16-Bit-Ganzzahl |
| 56 | Fehler Nr. 4 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 57 | Fehler Nr. 4 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 58–59 | *reserviert* | 16-Bit-Ganzzahl |
| 60–61 | Fehler Nr. 5 Zeitstempel | 32-Bit-Ganzzahl |
| 62–69 | Fehler Nr. 5 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 70 | Fehler Nr. 5 Fehlercode | 16-Bit-Ganzzahl |
| 71 | Fehler Nr. 5 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 72 | Fehler Nr. 5 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 73–74 | *reserviert* | 16-Bit-Ganzzahl |
| 75–76 | Fehler Nr. 6 Zeitstempel | 32-Bit-Ganzzahl |
| 77–84 | Fehler Nr. 6 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 85 | Fehler Nr. 6 Fehlercode | 16-Bit-Ganzzahl |
| 86 | Fehler Nr. 6 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 87 | Fehler Nr. 6 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 88–89 | *reserviert* | 16-Bit-Ganzzahl |
| 90–91 | Fehler Nr. 7 Zeitstempel | 32-Bit-Ganzzahl |
| 92–99 | Fehler Nr. 7 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 100 | Fehler Nr. 7 Fehlercode | 16-Bit-Ganzzahl |
| 101 | Fehler Nr. 7 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 102 | Fehler Nr. 7 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 103–104 | *reserviert* | 16-Bit-Ganzzahl |
| 105–106 | Fehler Nr. 8 Zeitstempel | 32-Bit-Ganzzahl |
| 107–114 | Fehler Nr. 8 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 115 | Fehler Nr. 8 Fehlercode | 16-Bit-Ganzzahl |
| 116 | Fehler Nr. 8 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 117 | Fehler Nr. 8 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 118–119 | *reserviert* | 16-Bit-Ganzzahl |
| 120–121 | Fehler Nr. 9 Zeitstempel | 32-Bit-Ganzzahl |
| 122–129 | Fehler Nr. 9 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 130 | Fehler Nr. 9 Fehlercode | 16-Bit-Ganzzahl |
| 131 | Fehler Nr. 9 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 132 | Fehler Nr. 9 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 133–134 | *reserviert* | 16-Bit-Ganzzahl |
| 135–136 | Fehler Nr. 10 Zeitstempel | 32-Bit-Ganzzahl |
| 137–144 | Fehler Nr. 10 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 145 | Fehler Nr. 10 Fehlercode | 16-Bit-Ganzzahl |

| WORD # | WORD NAME | DATENTYP |
|---|---|---|
| 146 | Fehler Nr. 10 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 147 | Fehler Nr. 10 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 148–149 | *reserviert* | 16-Bit-Ganzzahl |

**Falscher Zeitstempel**

Die relative Zeit in Sekunden, nachdem der Fehler aufgetreten ist. Gemessen ab Zeitpunkt 0, also dem letzten Zeitpunkt, an dem der Sicherheitskontroller eingeschaltet wurde.

**E/A- oder Systemname**

Dies ist ein ASCII--String, der den Ursprung des Fehlers beschreibt.

**Fehlercode, erweiterter Fehlercode, Fehlerindexmeldung**

Der Sicherheitskontroller-Fehlercode setzt sich aus dem Fehlercode und dem erweiterten Fehlercode zusammen. Das Format des Fehlercodes ist `Fehlercode "Punkt" erweiterter Fehlercode` . Der Sicherheitskontroller-Fehlercode 2.1 wird beispielsweise vom Fehlercode `2` und dem erweiterten Fehlercode `1` angegeben. Der Indexwert der Fehlermeldung ist der Fehlercode und der erweiterte Fehlercode zusammen und umfasst eine führende Null mit dem erweiterten Fehlercode, falls erforderlich. Der Sicherheitskontroller-Fehlercode 2.1 wird beispielsweise vom Fehlermeldungsindex `201` angegeben. Mit dem Indexwert der Fehlermeldung kann der vollständige Fehlercode bequem nur anhand eines einzigen 16-Bit-Registerwerts abgerufen werden.

## SPS-Eingang Baugruppeninstanz 103 (0×67) — 35 Register (Reset-/Abbruchverzögerung)

Diese Baugruppeninstanz übermittelt den Status aller 256 virtuellen Ausgänge und Fehler und stellt die erforderlichen Feedback-Informationen für die Ausführung virtueller Reset- und Abbruchverzögerungen zur Verfügung.

| WORD # | WORD NAME | DATENTYP |
|---|---|---|
| 0 | VO1–VO16 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 1 | VO17–VO32 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 2 | VO33–VO48 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 3 | VO49–VO64 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 4 | VO65–VO80 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 5 | VO81–VO96 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 6 | VO97–VO112 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 7 | VO113–VO128 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 8 | VO129–VO144 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 9 | VO145–VO160 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 10 | VO161–VO176 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 11 | VO177–VO192 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 12 | VO193–VO208 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 13 | VO209–VO224 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 14 | VO225–VO240 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 15 | VO241–VO256 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 16 | Fehlerbits für VO1–VO16 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 17 | Fehlerbits für VO17–VO32 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 18 | Fehlerbits für VO33–VO48 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 19 | Fehlerbits für VO49–VO64 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 20 | Fehlerbits für VO65–VO80 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 21 | Fehlerbits für VO81–VO96 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |

| WORD # | WORD NAME | DATENTYP |
|---|---|---|
| 22 | Fehlerbits für VO97–VO112 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 23 | Fehlerbits für VO113–VO128 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 24 | Fehlerbits für VO129–VO144 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 25 | Fehlerbits für VO145–VO160 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 26 | Fehlerbits für VO161–VO176 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 27 | Fehlerbits für VO177–VO192 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 28 | Fehlerbits für VO193–VO208 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 29 | Fehlerbits für VO209–VO224 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 30 | Fehlerbits für VO225–VO240 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 31 | Fehlerbits für VO241–VO256 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 32 | Virtuelle Reset-/Abbruchverzögerung (1–16) Feedback [RCD-Feedback Registerbits] (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 57) | 16-Bit-Ganzzahl |
| 33 | *reserviert* | 16-Bit-Ganzzahl |
| 34 | RCD-Auslösecode Feedback [RCD-Aktivierung Feedbackregister] (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 57) | 16-Bit-Ganzzahl |

## SPS-Eingangsbaugruppeninstanz 104 (0×68) — 112 Register (Reset-/Abbruchverzögerung plus ISD)

Diese Baugruppeninstanz übermittelt den Status aller 256 virtuellen Ausgänge und Fehler und stellt die erforderlichen Feedback-Informationen für die Ausführung virtueller Reset- und Abbruchverzögerungen zur Verfügung. Des Weiteren übermittelt Sie die Leistungs- und Statusinformationen zu ISD-Geräten.

| WORD # | WORD NAME | DATENTYP |
|---|---|---|
| 0 | VO1–VO16 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 1 | VO17–VO32 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 2 | VO33–VO48 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 3 | VO49–VO64 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 4 | VO65–VO80 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 5 | VO81–VO96 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 6 | VO97–VO112 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 7 | VO113–VO128 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 8 | VO129–VO144 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 9 | VO145–VO160 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 10 | VO161–VO176 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 11 | VO177–VO192 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 12 | VO193–VO208 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 13 | VO209–VO224 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 14 | VO225–VO240 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |

| WORD # | WORD NAME | DATENTYP |
|---|---|---|
| 15 | VO241–VO256 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 16 | Fehlerbits für VO1–VO16 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 17 | Fehlerbits für VO17–VO32 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 18 | Fehlerbits für VO33–VO48 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 19 | Fehlerbits für VO49–VO64 (siehe Flags auf Seite 184) | 16-Bit-Ganzzahl |
| 20 | Fehlerbits für VO65–VO80 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 21 | Fehlerbits für VO81–VO96 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 22 | Fehlerbits für VO97–VO112 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 23 | Fehlerbits für VO113–VO128 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 24 | Fehlerbits für VO129–VO144 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 25 | Fehlerbits für VO145–VO160 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 26 | Fehlerbits für VO161–VO176 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 27 | Fehlerbits für VO177–VO192 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 28 | Fehlerbits für VO193–VO208 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 29 | Fehlerbits für VO209–VO224 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 30 | Fehlerbits für VO225–VO240 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 31 | Fehlerbits für VO241–VO256 (siehe Erweiterte Flags auf Seite 185) | 16-Bit-Ganzzahl |
| 32 | Virtuelle Reset-/Abbruchverzögerung (1–16) Feedback [RCD-Feedback Registerbits] (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 57) | 16-Bit-Ganzzahl |
| 33 | *reserviert* | 16-Bit-Ganzzahl |
| 34 | RCD-Auslösecode Feedback [RCD-Aktivierung Feedbackregister] (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 57) | 16-Bit-Ganzzahl |
| 35–36 | ISD-Systemstatus – Reihe 1 Geräteanzahl | 32-Bit-Ganzzahl |
| 37–38 | ISD-Systemstatus – Reihe 2 Geräteanzahl | 32-Bit-Ganzzahl |
| 39–40 | ISD-Systemstatus – Reihe 1 Gerätestatus Ein/Aus (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 41–42 | ISD-Systemstatus – Reihe 2 Gerätestatus Ein/Aus (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 43–44 | ISD-Systemstatus – Reihe 1 Fehlerstatus (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 45–46 | ISD-Systemstatus – Reihe 2 Fehlerstatus (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 47–48 | ISD-Systemstatus – Reihe 1 marginaler Status (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 49–50 | ISD-Systemstatus – Reihe 2 marginaler Status (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 51–52 | ISD-Systemstatus – Reihe 1 Alarmstatus (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |

| WORD # | WORD NAME | DATENTYP |
|---|---|---|
| 53–54 | ISD-Systemstatus – Reihe 2 Alarmstatus (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 55–56 | ISD-Systemstatus – Reihe 1 Reset-Status (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 57–58 | ISD-Systemstatus – Reihe 2 Reset-Status (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 59–60 | ISD-Systemstatus – Reihe 1 Auslöser erkannt (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 61–62 | ISD-Systemstatus – Reihe 2 Auslöser erkannt (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 63–64 | ISD-Systemstatus – Reihe 1 Systemstatus (siehe ISD-Reihe Systemstatus auf Seite 47) | 32-Bit-Ganzzahl |
| 65–66 | ISD-Systemstatus – Reihe 2 Systemstatus (siehe ISD-Reihe Systemstatus auf Seite 47) | 32-Bit-Ganzzahl |
| 67–99 | *reserviert* | 16-Bit-Ganzzahl |
| 100 | ISD-Leseanforderung Bestätigung (siehe Leistungs- und Statusinformationen zu einem einzelnen Gerät über ISD anfordern auf Seite 47) | 16-Bit-Ganzzahl |
| 101 | Von ISD-Reihe angeforderte Bestätigung (siehe Leistungs- und Statusinformationen zu einem einzelnen Gerät über ISD anfordern auf Seite 47) | 16-Bit-Ganzzahl |
| 102 | Von ISD-Gerät angeforderte Bestätigung (siehe Leistungs- und Statusinformationen zu einem einzelnen Gerät über ISD anfordern auf Seite 47) | 16-Bit-Ganzzahl |
| 103–111 | Spezifische Daten einzelner ISD-Geräte (siehe Detaillierte Beschreibung spezifischer Daten einzelner ISD-Geräte auf Seite 181) | 16-Bit-Ganzzahl |

## Detaillierte Beschreibung spezifischer Daten einzelner ISD-Geräte

Die folgende Tabelle beschreibt Baugruppeninstanz 104 (0×68) WORT Nr. 103–111 oder explizite Nachricht ISD-Antwort lesen WORT Nr. 68–76.

*Tabelle 15. Detaillierte Beschreibung spezifischer Daten einzelner ISD-Geräte*

| WORD.BIT # | Informationen | Datengröße |
|---|---|---|
| 103.0 | Sicherheitseingangsfehler | 1 Bit |
| 103.1 | *reserviert* | 1 Bit |
| 103.2 | Sensor nicht gekoppelt | 1-Bit |
| 103.3 | ISD-Datenfehler | 1-Bit |
| 103.4 | Falscher Auslöser-/Tasterstatus/Eingangsstatus | 1-Bit |
| 103.5 | Marginaler Bereich/Tasterstatus/Eingangsstatus | 1-Bit |
| 103.6 | Auslöser erkannt | 1-Bit |
| 103.7 | Ausgangsfehler | 1-Bit |
| 103.8 | Eingang 2 | 1-Bit |
| 103.9 | Eingang 1 | 1-Bit |
| 103.10 | Lokaler Reset erwartet | 1-Bit |
| 103.11 | Warnung Betriebsspannung | 1-Bit |
| 103.12 | Fehler bei Betriebsspannung | 1-Bit |
| 103.13 | Ausgang 2 | 1-Bit |
| 103.14 | Ausgang 1 | 1-Bit |
| 103.15 | Aus- und Wiedereinschalten der Stromversorgung erforderlich | 1-Bit |

| WORD.BIT # | Informationen | Datengröße |
|---|---|---|
| 104.0 | Fehlertolerante Ausgänge | 1-Bit |
| 104.1 | Einheit für lokalen Reset | 1-Bit |
| 104.2 | Kaskadierbar | 1-Bit |
| 104.3 | Hohe Codierstufe | 1-Bit |
| 104.4 bis 104.7 | Verbleibende Einlerninstanzen | 4-Bit |
| 104.8 bis 104.12 | Geräte-ID | 5-Bit |
| 104.13 bis 105.2 | Anzahl Bereichswarnungen | 6-Bit |
| 105.3 bis 105.7 | Ausschaltzeit für Ausgang | 5-Bit |
| 105.8 bis 105.15 | Anzahl der Spannungsfehler | 8-Bit |
| 106.0 bis 106.7 | Innentemperatur [23] | 8-Bit |
| 106.8 bis 106.15 | Auslöserabstand [23] | 8-Bit |
| 107.0 bis 107.7 | Versorgungsspannung [23] | 8-Bit |
| 107.8 bis 107.11 | Erwarteter Firmenname | 4-Bit |
| 107.12 bis 107.15 | Empfangener Firmenname | 4-Bit |
| 108 | Erwarteter Code | 16-Bit |
| 109 | Empfangener Code | 16-Bit |
| 110 | Interner Fehler A | 16-Bit |
| 111 | Interner Fehler B | 16-Bit |

## 12.4.6 Konfigurationsbaugruppenobjekt

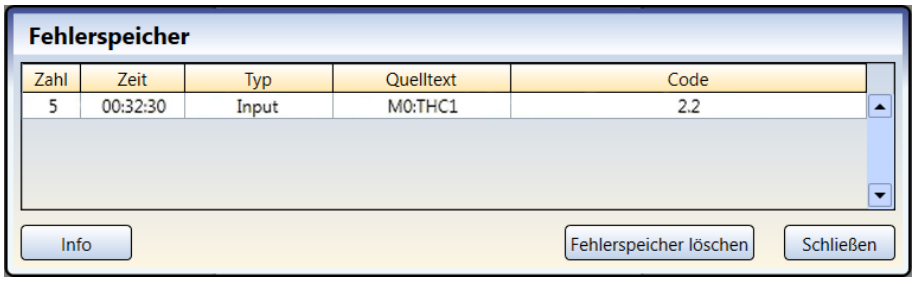
Der Sicherheitskontroller verwendet kein Konfigurationsbaugruppenobjekt.

Da einige EtherNet/IP-Clients dieses Objekt erfordern, verwenden Sie die Instanz 128 (0×80) mit einer Größe von null Registern (16-Bit).

## 12.4.7 Fehlerbeispiele

Die folgende Abbildung zeigt einen Fehler aus dem Fehlerprotokoll der Software des Sicherheitskontroller von Banner.

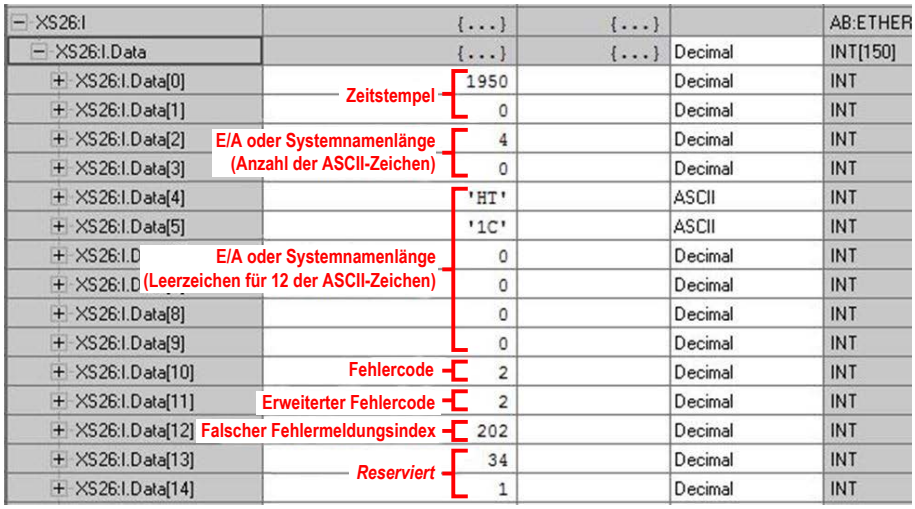
*Abbildung 182. Fehlerprotokoll mit 1 Fehler*




Die folgende Abbildung zeigt denselben Fehler, wie in den Ethernet/IP-Registern zu sehen ist.

[23] Informationen zur Umrechnung von Innentemperatur, Auslöserabstand und Betriebsspannung finden Sie unter ISD: Informationen zur Umwandlung von Temperatur, Spannung und Abstand auf Seite 248.

*Abbildung 183. EtherNet/IP-Register mit 1 Fehler*

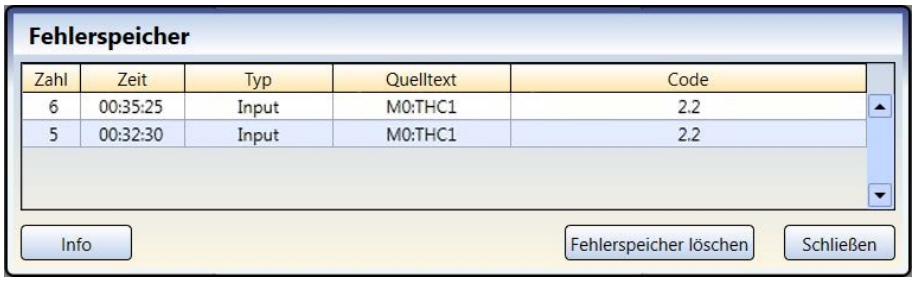



Beachten Sie das ControlLogix-Stringformat, in dem die ASCII-Zeichen angegeben sind, zwei pro Register, abwärts. "THC1" wird "HT" in Register 4, gefolgt von "1C" in Register 5.

Fehler-Nummerierungsfehler 202 = Fehlercode 2.2 (Simulatinitätsfehler). Weitere Informationen zu Fehlern finden Sie unter Fehlercode-Tabelle für XS/SC26-2 auf Seite 283 oder SC10-2 Fehlercode-Tabelle auf Seite 288.

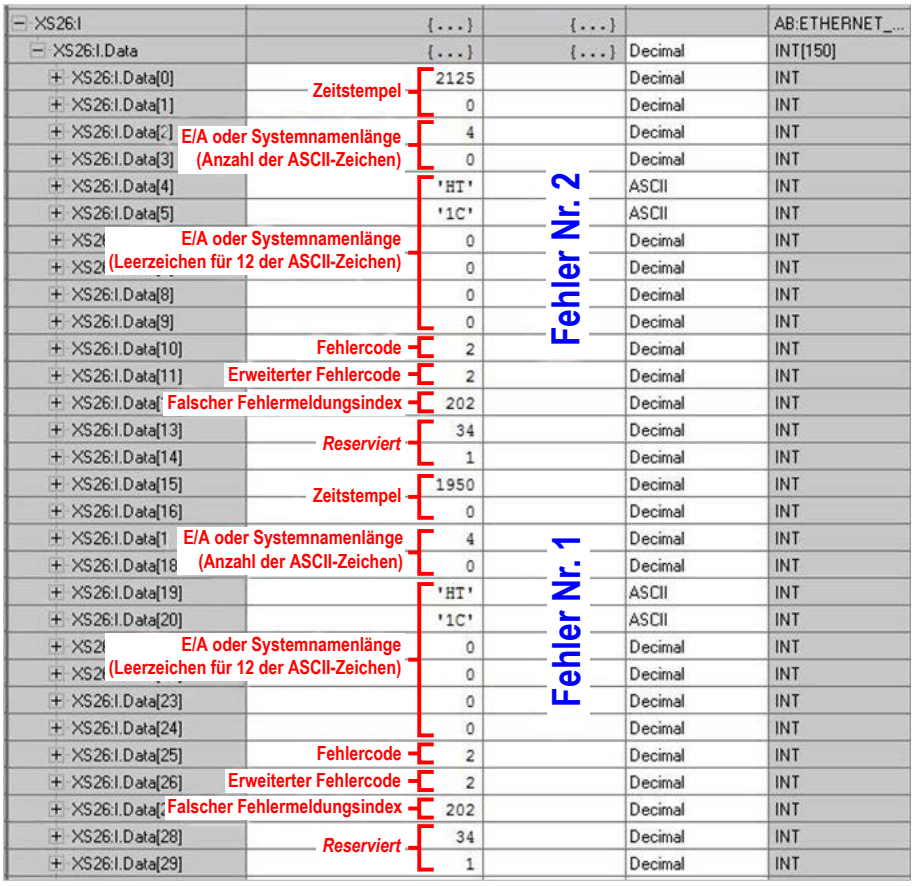
Die folgende Abbildung zeigt zwei Fehler im Fehlerprotokoll der XS26-2E-Software.

*Abbildung 184. Fehlerprotokoll mit zwei Fehlern*




Die folgende Abbildung zeigt die beiden gleichen Fehler in den SPS-Registern. Dabei wird der neuere Fehler Nr. 2 in der Liste vor dem Fehler Nr. 1 angezeigt.

*Abbildung 185. EtherNet/IP-Register mit zwei Fehlern*




# 12.4.8 Flags

Die unten definierten Wörter 0 bis 7 werden in den Baugruppeninstanzen 100, 101 und 103 als die ersten 8 Wörter angezeigt.

*Tabelle 16. Wort Nr. 0, Virtueller Ausgang 1–16*

| Bit-Position | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **15** | **14** | **13** | **12** | **11** | **10** | **9** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** | **0** |
| VO16 | VO15 | VO14 | VO13 | VO12 | VO11 | VO10 | VO9 | VO8 | VO7 | VO6 | VO5 | VO4 | VO3 | VO2 | VO1 |

*Tabelle 17. Wort Nr. 1, Virtueller Ausgang 17–32*

| Bit-Position | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **15** | **14** | **13** | **12** | **11** | **10** | **9** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** | **0** |
| VO32 | VO31 | VO30 | VO29 | VO28 | VO27 | VO26 | VO25 | VO24 | VO23 | VO22 | VO21 | VO20 | VO19 | VO18 | VO17 |

*Tabelle 18. Wort Nr. 2, Virtueller Ausgang 33–48*

| Bit-Position | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **15** | **14** | **13** | **12** | **11** | **10** | **9** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** | **0** |
| VO48 | VO47 | VO46 | VO45 | VO44 | VO43 | VO42 | VO41 | VO40 | VO39 | VO38 | VO37 | VO36 | VO35 | VO34 | VO33 |

*Tabelle 19. Wort Nr. 3, Virtueller Ausgang 49–64*

| Bit-Position | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **15** | **14** | **13** | **12** | **11** | **10** | **9** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** | **0** |
| VO64 | VO63 | VO62 | VO61 | VO60 | VO59 | VO58 | VO57 | VO56 | VO55 | VO54 | VO53 | VO52 | VO51 | VO50 | VO49 |

*Tabelle 20. Wort Nr. 4, Fehlerflagbits für virtuellen Ausgang 1–16*

Hinweis: Nicht jeder virtuelle Ausgang hat ein definiertes Fehlerflag.

| Bit-Position | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| VO16 | VO15 | VO14 | VO13 | VO12 | VO11 | VO10 | VO9 | VO8 | VO7 | VO6 | VO5 | VO4 | VO3 | VO2 | VO1 |

*Tabelle 21. Wort Nr. 5, Fehlerflagbits für virtuellen Ausgang 17–32*

Hinweis: Nicht jeder virtuelle Ausgang hat ein definiertes Fehlerflag.

| Bit-Position | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| VO32 | VO31 | VO30 | VO29 | VO28 | VO27 | VO26 | VO25 | VO24 | VO23 | VO22 | VO21 | VO20 | VO19 | VO18 | VO17 |

*Tabelle 22. Wort Nr. 6, Fehlerflagbits für virtuellen Ausgang 33–48*

Hinweis: Nicht jeder virtuelle Ausgang hat ein definiertes Fehlerflag.

| Bit-Position | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| VO48 | VO47 | VO46 | VO45 | VO44 | VO43 | VO42 | VO41 | VO40 | VO39 | VO38 | VO37 | VO36 | VO35 | VO34 | VO33 |

*Tabelle 23. Wort Nr. 7, Fehlerflagbits für vituellen Ausgang 49–64*

Hinweis: Nicht jeder virtuelle Ausgang hat ein definiertes Fehlerflag.

| Bit-Position | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| VO64 | VO63 | VO62 | VO61 | VO60 | VO59 | VO58 | VO57 | VO56 | VO55 | VO54 | VO53 | VO52 | VO51 | VO50 | VO49 |

## 12.4.9 Erweiterte Flags

Zusätzlich zu den oben aufgeführten ersten 64 virtuellen Ausgängen fügt die Baugruppeninstanz 103 weitere 192 hinzu (insgesamt dann 256). Die Fehlerflagbits verschieben sich nach unten, damit Platz für alle 256 virtuellen Ausgänge zusammen ist.

Die Wörter 0 bis 3 sind wie in Flags auf Seite 184 abgebildet gleich. Im Falle der Baugruppeninstanz 103 werden die folgenden Änderungen gemacht:

- Wort Nr. 4 – Virtuelle Ausgänge 65 bis 80 mit VO65 in Bit 0 und VO80 in Bit 15
- Wort Nr. 5 – Virtuelle Ausgänge 81 bis 96 mit VO81 in Bit 0 und VO96 in Bit 15
- Wort Nr. 6 – Virtuelle Ausgänge 97 bis 112 mit VO97 in Bit 0 und VO112 in Bit 15
- Wort Nr. 7 – Virtuelle Ausgänge 113 bis 128 mit VO113 in Bit 0 und VO128 in Bit 15
- Wort Nr. 8 – Virtuelle Ausgänge 129 bis 144 mit VO129 in Bit 0 und VO144 in Bit 15
- Wort Nr. 9 – Virtuelle Ausgänge 145 bis 160 mit VO145 in Bit 0 und VO160 in Bit 15
- Wort Nr. 10 – Virtuelle Ausgänge 161 bis 176 mit VO161 in Bit 0 und VO176 in Bit 15
- Wort Nr. 11 – Virtuelle Ausgänge 177 bis 192 mit VO177 in Bit 0 und VO192 in Bit 15
- Wort Nr. 12 – Virtuelle Ausgänge 193 bis 208 mit VO193 in Bit 0 und VO208 in Bit 15
- Wort Nr. 13 – Virtuelle Ausgänge 209 bis 224 mit VO209 in Bit 0 und VO224 in Bit 15
- Wort Nr. 14 – Virtuelle Ausgänge 225 bis 240 mit VO225 in Bit 0 und VO240 in Bit 15
- Wort Nr. 15 – Virtuelle Ausgänge 241 bis 256 mit VO241 in Bit 0 und VO256 in Bit 15
- Wort Nr. 16 bis Nr. 19 sind wie unter Flags auf Seite 184 dargestellt die gleichen wie Wort Nr. 4 bis Nr. 7. Gruppeninstanz 103 umfasst ebenfalls mehr Fehlerflagbits, wie nachfolgend gezeigt.
- Wort Nr. 20 – Fehlerbits für VO65 bis VO80 mit Fehler VO65 in Bit 0 und VO80 in Bit 15

Dieses Muster setzt sich fort für Wort Nr. 21 bis Nr. 31 für die restlichen Fehlerbits für die insgesamt 256 virtuellen Ausgänge.

## 12.4.10 ISD-Systemstatuswörter

Die ISD-Systemstatuswörter, wie sie in der SPS-Eingangsbaugruppeninstanz 104 (0×68), Wörter 39–62, zu finden sind, sind nachstehend definiert.

Jedes dieser Systemstatuswörter ist nicht als eine einzelne 32-Bit-Ganzzahl zu verstehen, sondern vielmehr als ein Datenfeld aus 32 einzelnen ISD-Gerätestatusbits, wobei Bit 0 dem ISD-Gerät 1 zugeordnet ist, Bit 1 dem ISD-Gerät 2 usw., bis Bit 31, das dem ISD-Gerät 32 in dieser Reihe zugeordnet ist.

- Wort Nr. 39–40 Reihe 1 Gerätestatus Ein/Aus – Reihe 1, ISD-Gerät 1 ein/aus ist Wort 39, Bit 0; Reihe 1, ISD-Gerät 32 ein/aus ist Wort 40, Bit 15
- Wort Nr. 41–42 Reihe 2 Gerätestatus Ein/Aus – Reihe 2, ISD-Gerät 1 ein/aus ist Wort 41, Bit 0; Reihe 2, ISD-Gerät 32 ein/aus ist Wort 42, Bit 15

- Wort Nr. 43–44 Reihe 1 Fehlerstatus – Reihe 1, ISD-Gerät 1 Fehlerstatus ist Wort 43, Bit 0; Reihe 1, ISD-Gerät 32 Fehlerstatus ist Wort 44, Bit 15
- Wort Nr. 45–46 Reihe 2 Fehlerstatus – Reihe 2, ISD-Gerät 1 Fehlerstatus ist Wort 45, Bit 0; Reihe 2, ISD-Gerät 32 Fehlerstatus ist Wort 46, Bit 15
- Wort Nr. 47–48 Reihe 1 marginaler Status – Reihe 1, ISD-Gerät 1 marginaler Status ist Wort 47, Bit 0; Reihe 1, ISD-Gerät 32 marginaler Status ist Wort 48, Bit 15
- Wort Nr. 49–50 Reihe 2 marginaler Status – Reihe 2, ISD-Gerät 1 marginaler Status ist Wort 49, Bit 0; Reihe 2, ISD-Gerät 32 marginaler Status ist Wort 50, Bit 15
- Wort Nr. 51–52 Reihe 1 Alarmstatus – Reihe 1, ISD-Gerät 1 Alarmstatus ist Wort 51, Bit 0; Reihe 1, ISD-Gerät 32 Alarmstatus ist Wort 52, Bit 15
- Wort Nr. 53–54 Reihe 2 Alarmstatus – Reihe 2, ISD-Gerät 1 Alarmstatus ist Wort 53, Bit 0; Reihe 2, ISD-Gerät 32 Alarmstatus ist Wort 54, Bit 15
- Wort Nr. 55–56 Reihe 1 Reset-Status – Reihe 1, ISD-Gerät 1 Reset-Status ist Wort 55, Bit 0; Reihe 1, ISD-Gerät 32 Reset-Status ist Wort 56, Bit 15
- Wort Nr. 57–58 Reihe 2 Reset-Status – Reihe 2, ISD-Gerät 1 Reset-Status ist Wort 57, Bit 0; Reihe 2, ISD-Gerät 32 Reset-Status ist Wort 58, Bit 15
- Wort Nr. 59–60 Reihe 1 Auslöser erkannt – Reihe 1, ISD-Gerät 1 Auslöser erkannt ist Wort 59, Bit 0; Reihe 1, ISD-Gerät 32 Auslöser erkannt ist Wort 60, Bit 15
- Wort Nr. 61–62 Reihe 2 Auslöser erkannt – Reihe 2, ISD-Gerät 1 Auslöser erkannt ist Wort 61, Bit 0; Reihe 2, ISD-Gerät 32 Auslöser erkannt ist Wort 62, Bit 15

# 12.4.11 RSLogix5000-Konfiguration (explizite Nachrichten)

Der Sicherheitskontroller unterstützt verschiedene explizite Nachrichtenverbindungen. Zusätzlich zu den Baugruppeninstanzen aus dem vorherigen Abschnitt gibt es noch weitere Baugruppeninstanzen, auf die nur über explizite Nachrichten zugegriffen werden kann.

## Auswahl für explizite Nachrichtenverbindungen

### Sicherheitskontrollerausgänge lesen

Zum Ausführen eines einmaligen Lesevorgangs einer der T>O Sicherheitskontrollerausgangs-/SPS-Eingangsbaugruppeninstanzen von Ausgänge vom Sicherheitskontroller (Eingänge zur SPS) auf Seite 174 verwenden Sie den Servicetyp 14 (einzelnes Attribut abrufen, hex 0E), Klasse 4, Instanz 100 (0×64) oder 101 (0×65) oder 102 (0×66) oder 103 (0×67) oder 104 (0×68), Attribut 3. Eine erfolgreiche explizite Nachricht dieses Typs gibt die entsprechende Baugruppeninstanz wie in Ausgänge vom Sicherheitskontroller (Eingänge zur SPS) auf Seite 174 dargestellt zurück.

Ein Beispiel dieses Verbindungstyps finden Sie unter Beispiel für das Lesen von Sicherheitskontrollerausgängen auf Seite 189.

### Sicherheitskontrollerausgänge schreiben

Einen einmaligen Schreibvorgang der Daten in die Eingangsbaugruppeninstanzen des Sicherheitskontrollers (SPS-Ausgangsbaugruppeninstanzen) von Eingänge zum Sicherheitskontroller (Ausgänge von der SPS) auf Seite 172 führen Sie mit Servicetyp 16 aus (einzelnes Attribut festlegen, hex 10), Klasse 4, Instanz 112 (0×70) oder 113 (0×71) oder 114 (0×72), Attribut 3. Die Größe des MSG-Quellelements (eines benutzerdefinierten Tag-Datenfelds) wird von dem fraglichen Baugruppenobjekt angegeben. Eine erfolgreiche explizite Nachricht dieses Typs schreibt die relevanten Daten in den Sicherheitskontroller; siehe Eingänge zum Sicherheitskontroller (Ausgänge von der SPS) auf Seite 172.

Ein Beispiel dieses Verbindungstyps finden Sie unter Beispiel für das Schreiben von Sicherheitskontrollerausgängen auf Seite 191.

**Anmerkung:** Nicht alle Sicherheitskontroller unterstützen virtuelle Eingänge.

### Status virtueller Ausgänge

Den aktuellen Status von den ersten 64 virtuellen Ausgängen rufen Sie mit dem Servicetyp 14 ab (einzelnes Attribut abrufen, hex 0E), Klasse 0×64, Instanz 1, Attribut 1. Eine erfolgreiche explizite Nachricht dieses Typs gibt zwei 32-Bit-Ganzzahlen zurück, die den Status von VO1 bis VO64 angeben. Ein Beispiel dieses Verbindungstyps finden Sie unter Beispiel für das Lesen des Status virtueller Ausgänge auf Seite 192.

### Erweiterten Status der virtuellen Ausgänge lesen

Den aktuellen Status von allen 256 virtuellen Ausgängen rufen Sie mit dem Servicetyp 14 ab (einzelnes Attribut abrufen, hex 0E), Klasse 0×75, Instanz 1, Attribut 1. Eine erfolgreiche explizite Nachricht dieses Typs gibt zwei 32-Bit-Ganzzahlen zurück, die die Statusbits der virtuellen Ausgänge VO1 bis VO256 angeben.

## Fehlerbits der virtuellen Ausgänge

Den aktuellen Status der Fehlerbits von den ersten 64 virtuellen Ausgängen rufen Sie mit dem Servicetyp 14 ab (einzelnes Attribut abrufen, hex 0E), Klasse 0×65, Instanz 1, Attribut 1. Eine erfolgreiche explizite Nachricht dieses Typs gibt zwei 32-Bit-Ganzzahlen zurück, die den Status der Fehlerbits für VO1 bis VO64 angeben.

## Fehlerbits der erweiterten virtuellen Ausgänge lesen

Den aktuellen Status der Fehlerbits von allen 256 virtuellen Ausgängen rufen Sie mit dem Servicetyp 14 ab (einzelnes Attribut abrufen, hex 0E), Klasse 0×76, Instanz 1, Attribut 1. Eine erfolgreiche explizite Nachricht dieses Typs gibt zwei 32-Bit-Ganzzahlen zurück, die die Fehlerbits der virtuellen Ausgänge VO1 Fehler bis VO256 Fehler angeben.

## Einzelne Fehlerindexwerte

Den spezifischen Fehlerindexwert für einen der ersten 64 virtuellen Ausgänge rufen Sie mit dem Servicetyp 14 ab (einzelnes Attribut abrufen, hex 0E), Klasse 0×6F, Instanz 1–64 (eine auswählen), Attribut 1. Eine erfolgreiche explizite Nachricht dieses Typs gibt ein einzelnes 16-Bit-Register zurück, das den Fehlerindexwert für einen der virtuellen Ausgänge angibt.

## Erweiterte einzelne Fehlerindexwerte lesen

Den spezifischen Fehlerindexwert für einen der 256 virtuellen Ausgänge rufen Sie mit dem Servicetyp 14 ab (einzelnes Attribut abrufen, hex 0E), Klasse 0×7A, Instanz 1–255 (eine auswählen), Attribut 1. Eine erfolgreiche explizite Nachricht dieses Typs gibt ein einzelnes 16-Bit-Register zurück, das den Fehlerindexwert für einen der virtuellen Ausgänge angibt.

## Virtuelle Eingänge schreiben (virtueller manueller Reset und Abbruch Ausschaltverzögerung)

Um Bits für virtuellen Reset/Abbruchverzögerung in den Sicherheitskontroller zu schreiben, verwenden Sie den Servicetyp 16 (einzelnes Attribut festlegen, hex 10), Klasse 0×78, Instanz 1, Attribut 1. Die Länge der zu schreibenden Daten beträgt zwei 32-Bit-Ganzzahlen (8 Byte). Eine erfolgreiche explizite Nachricht dieses Typs schreibt die Bits für virtuellen Reset/Abbruchverzögerung VRCD1 bis VRCD16 und den RCD-Auslösecode.

**Anmerkung:** Nicht alle Sicherheitskontroller unterstützen virtuelle Eingänge.

| Wort Nr. | Wortname | Datentyp |
|---|---|---|
| 0 | VRCD (VRCD1–16) (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 57) | 16-Bit-Ganzzahl |
| 1 | *reserviert* | 16-Bit-Ganzzahl |
| 2 | RCD-Auslösecode [RCD-Aktivierung] (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 57) | 16-Bit-Ganzzahl |
| 3 | *reserviert* | 16-Bit-Ganzzahl |

## Virtuelle Ausgänge lesen (Rückmeldung virtueller manueller Reset und Abbruch Ausschaltverzögerung)

Um die Statusbits der virtuellen Ausgänge in Bezug auf die Rückmeldung virtueller manueller Reset und Abbruch Ausschaltverzögerung vom Sicherheitskontroller zu lesen, verwenden Sie den Servicetyp 14 (einzelnes Attribut abrufen, hex 0E), Klasse 0×79, Instanz 1, Attribut 1. Eine erfolgreiche explizite Nachricht dieses Typs gibt zwei 32-Bit-Ganzzahlen zurück, die die Bits für die Rückmeldung virtueller manueller Reset und Abbruch Ausschaltverzögerung "VRCD Feedback 1" bis "VRCD Feedback 16" und die Rückmeldung des RCD-Auslösecodes enthalten.

**Anmerkung:** Nicht alle Sicherheitskontroller unterstützen virtuelle Eingänge.

| Wort Nr. | Wortname | Datentyp |
|---|---|---|
| 0 | VRCD-Rückmeldung (VRCD1–16) (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 57) | 16-Bit-Ganzzahl |
| 1 | *reserviert* | 16-Bit-Ganzzahl |
| 2 | RCD-Auslösecode Rückmeldung [RCD-Aktivierung Rückmeldung] (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 57) | 16-Bit-Ganzzahl |

| Wort Nr. | Wortname | Datentyp |
|---|---|---|
| 3 | *reserviert* | 16-Bit-Ganzzahl |

## ISD-Anforderung schreiben

Um eine Anforderung für ISD-Geräteinformationen in den Sicherheitskontroller zu schreiben, verwenden Sie Servicetyp 16 (einzelnes Attribut festlegen, hex 10), Klasse 0×81, Instanz 1, Attribut 1. Die Länge der zu schreibenden Daten beträgt drei 16-Bit-Ganzzahlen (6 Byte). Eine erfolgreiche explizite Nachricht dieses Typs schreibt die ISD-Anforderung an den Sicherheitskontroller.

**Anmerkung:** Nicht alle Sicherheitskontroller unterstützen ISD.

| Wort Nr. | Wortname | Datentyp |
|---|---|---|
| 0 | ISD-Leseanforderung (siehe Leistungs- und Statusinformationen zu einem einzelnen Gerät über ISD anfordern auf Seite 47) | 16-Bit-Ganzzahl |
| 1 | ISD-Reihe angefordert (siehe Leistungs- und Statusinformationen zu einem einzelnen Gerät über ISD anfordern auf Seite 47) | 16-Bit-Ganzzahl |
| 2 | ISD-Gerät angefordert (siehe Leistungs- und Statusinformationen zu einem einzelnen Gerät über ISD anfordern auf Seite 47) | 16-Bit-Ganzzahl |

## ISD-Antwort lesen

Die Antwort des Sicherheitskontrollers auf eine ISD-Anforderung (siehe ISD-Anforderung schreiben auf Seite 188) lesen Sie mit dem Servicetyp 14 (einzelnes Attribut abrufen, hex 0E), Klasse 0×80, Instanz 1, Attribut 1. Eine erfolgreiche explizite Nachricht dieses Typs gibt 77 Wörter zurück, die die unten angezeigten Informationen angeben.

**Anmerkung:** Nicht alle Sicherheitskontroller unterstützen ISD.

| Wort Nr. | Wortname | Datentyp |
|---|---|---|
| 0–1 | ISD-Systemstatus – Reihe 1 Geräteanzahl | 32-Bit-Ganzzahl |
| 2–3 | ISD-Systemstatus – Reihe 2 Geräteanzahl | 32-Bit-Ganzzahl |
| 4–5 | ISD-Systemstatus – Reihe 1 Gerätestatus Ein/Aus (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 6–7 | ISD-Systemstatus – Reihe 2 Gerätestatus Ein/Aus (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 8–9 | ISD-Systemstatus – Reihe 1 Fehlerstatus (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 10–11 | ISD-Systemstatus – Reihe 2 Fehlerstatus (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 12–13 | ISD-Systemstatus – Reihe 1 marginaler Status (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 14–15 | ISD-Systemstatus – Reihe 2 marginaler Status (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 16–17 | ISD-Systemstatus – Reihe 1 Alarmstatus (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 18–19 | ISD-Systemstatus – Reihe 2 Alarmstatus (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 20–21 | ISD-Systemstatus – Reihe 1 Reset-Status (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 22–23 | ISD-Systemstatus – Reihe 2 Reset-Status (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 24–25 | ISD-Systemstatus – Reihe 1 Auslöser erkannt (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 26–27 | ISD-Systemstatus – Reihe 2 Auslöser erkannt (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |

| Wort Nr. | Wortname | Datentyp |
|---|---|---|
| 28–29 | ISD-Systemstatus – Reihe 1 Systemstatus (siehe ISD-Reihe Systemstatus auf Seite 47) | 32-Bit-Ganzzahl |
| 30–31 | ISD-Systemstatus – Reihe 2 Systemstatus (siehe ISD-Reihe Systemstatus auf Seite 47) | 32-Bit-Ganzzahl |
| 32–64 | *reserviert* | 16-Bit-Ganzzahl |
| 65 | ISD-Leseanforderung Bestätigung (siehe Leistungs- und Statusinformationen zu einem einzelnen Gerät über ISD anfordern auf Seite 47) | 16-Bit-Ganzzahl |
| 66 | Von ISD-Reihe angeforderte Bestätigung (siehe Leistungs- und Statusinformationen zu einem einzelnen Gerät über ISD anfordern auf Seite 47) | 16-Bit-Ganzzahl |
| 67 | Von ISD-Gerät angeforderte Bestätigung (siehe Leistungs- und Statusinformationen zu einem einzelnen Gerät über ISD anfordern auf Seite 47) | 16-Bit-Ganzzahl |
| 68–76 | Spezifische Daten einzelner ISD-Geräte (siehe Detaillierte Beschreibung spezifischer Daten einzelner ISD-Geräte auf Seite 181) | 16-Bit-Ganzzahl |

### Einzelner Fehlerprotokolleintrag

Den speziellen Eintrag aus den 10 Eintragsfehlerprotokollen rufen Sie mit dem Servicetyp 14 ab (einzelnes Attribut abrufen, hex 0E), Klasse 0×71, Instanz 1, Attribut 1–10 (eines ist auszuwählen). Eine erfolgreiche explizite Nachricht dieses Typs gibt einen einzelnen 15-Register-Eintrag aus dem Fehlerprotokoll zurück, das wie nachfolgend definiert den Fehlerindexwert für einen der virtuellen Ausgänge angibt. Hinweis: Attribut = 1 bezieht sich auf den neuesten Eintrag im Fehlerlog und Attribut = 10 auf den ältesten.

| Wort Nr. | Wortname | Datentyp |
|---|---|---|
| 0–1 | Fehler Nr. 1 Zeitstempel | 32-Bit-Ganzzahl |
| 2–9 | Fehler Nr. 1 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 10 | Fehler Nr. 1 Fehlercode | 16-Bit-Ganzzahl |
| 11 | Fehler Nr. 1 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 12 | Fehler Nr. 1 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 13–14 | *reserviert* | 16-Bit-Ganzzahl |

### Systeminformationen

Einige Systeminformationen können mittels Servicetyp 14 abgerufen werden (einzelnes Attribut abrufen, hex 0E), Klasse 0×72, Instanz 1, Attribut 1–4 (eines ist auszuwählen, siehe nachfolgende Tabelle). Eine erfolgreiche explizite Nachricht dieses Typs gibt die nachfolgend gezeigten Systeminformationen zurück (Größe und Datentyp variieren). Ein Beispiel dieses Verbindungstyps finden Sie unter Beispiel für das Lesen von Systeminformationen auf Seite 193.

| Attribut | Systemwert | Datentyp |
|---|---|---|
| 1 | Sekunden seit Systemstart | 32-Bit-Ganzzahl |
| 2 | Betriebsart | 16-Bit-Ganzzahl |
| 3 | ConfigName | Doppelwortlänge + 16-ASCII-Zeichen |
| 4 | Konfig. CRC | 32-Bit-Ganzzahl |

## Beispiele der expliziten Nachrichtenverbindungen

### Beispiel für das Lesen von Sicherheitskontrollerausgängen

Zum Ausführen eines einmaligen Lesevorgangs der Baugruppeninstanz 100 (0×64) verwenden Sie den Servicetyp 14 (einzelnes Attribut abrufen, hex 0E), Klasse 4, Instanz 100, Attribut 3. Eine erfolgreiche explizite Nachricht dieses Typs gibt alle 8 Register der Baugruppeninstanz 100 (0×64) zurück, wie in Konfigurationsbaugruppenobjekt auf Seite 182 definiert.

Die folgende Abbildung zeigt den MSG-Befehl für diese explizite Nachricht.

*Abbildung 186. MSG-Befehl — Registerkarte **Konfiguration***

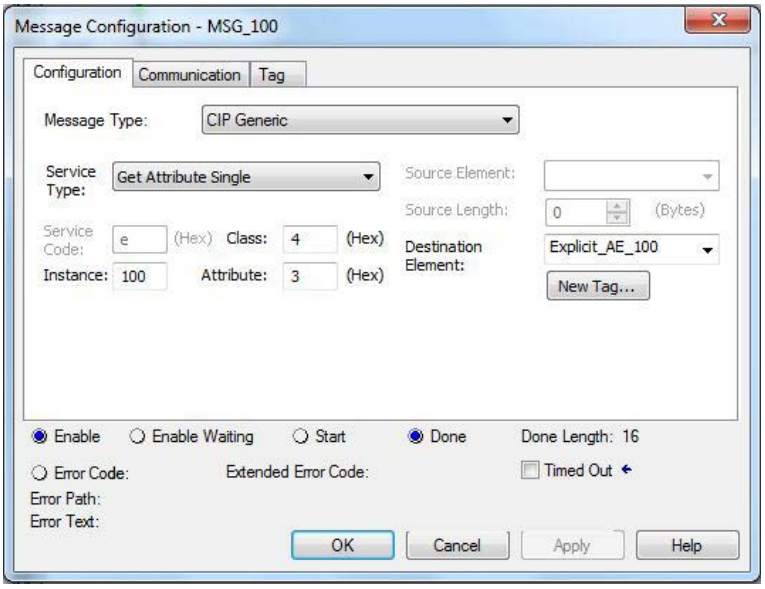
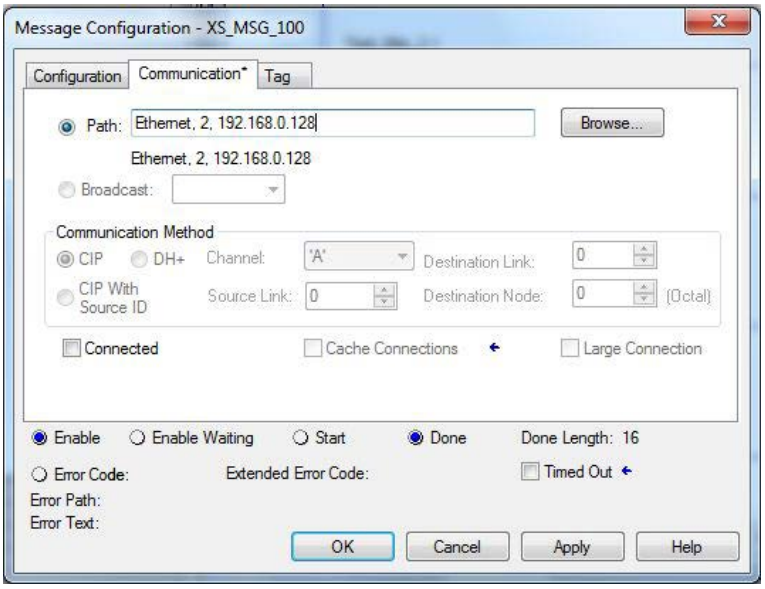



*Abbildung 187. MSG-Befehl — Registerkarte **Kommunikation***




Die folgende Abbildung zeigt das benutzerdefinierte Datenfeld (mit der Bezeichnung XS_Explicit_AE_100) mit allen 8 Registern.

*Abbildung 188. Benutzerdefiniertes Datenfeld*

| | | | | |
|---|---|---|---|---|
| XS_Explicit_AE_100 | {...} | {...} | Decimal | INT[8] |
| XS_Explicit_AE_100[0] | 2 | | Decimal | INT |
| XS_Explicit_AE_100[1] | 0 | | Decimal | INT |
| XS_Explicit_AE_100[2] | 0 | | Decimal | INT |
| XS_Explicit_AE_100[3] | 0 | | Decimal | INT |
| XS_Explicit_AE_100[4] | 0 | | Decimal | INT |
| XS_Explicit_AE_100[5] | 0 | | Decimal | INT |
| XS_Explicit_AE_100[6] | 0 | | Decimal | INT |
| XS_Explicit_AE_100[7] | 0 | | Decimal | INT |

In diesen Beispieldaten ist ersichtlich, dass VO2 aktuell AKTIVIERT ist. VO2 ist Wort 0, Bit 1 > 2^1 = 2

## Beispiel für das Schreiben von Sicherheitskontrollerausgängen

Zum Ausführen eines einmaligen Schreibvorgangs der Daten in die Eingangsbaugruppeninstanz 112 (0×70) des Sicherheitskontrollers (SPS-Ausgangsbaugruppeninstanz) verwenden Sie den Servicetyp 16 (einzelnes Attribut festlegen, hex 10), Klasse 4, Instanz 112 (0×70), Attribut 3. Die Größe des MSG-Quellelements (ein benutzerdefiniertes Tag-Datenfeld) beträgt in diesem Fall 4 Byte.

Die folgende Abbildung zeigt das benutzerdefinierte Datenfeld (genannt AE112), das in den Sicherheitskontroller geschrieben werden soll.

*Abbildung 189. Benutzerdefiniertes Datenfeld, das in den Sicherheitskontroller geschrieben werden soll*

| | | | | |
|---|---|---|---|---|
| ◢ AE112 | {...} | {...} | Decimal | INT[2] |
| ▶ AE112[0] | 7 | | Decimal | INT |
| ▶ AE112[1] | 0 | | Decimal | INT |

Die folgende Abbildung zeigt den MSG-Befehl für diese explizite Nachricht.

*Abbildung 190. MSG-Befehl — Registerkarte **Configuration (Konfiguration)***

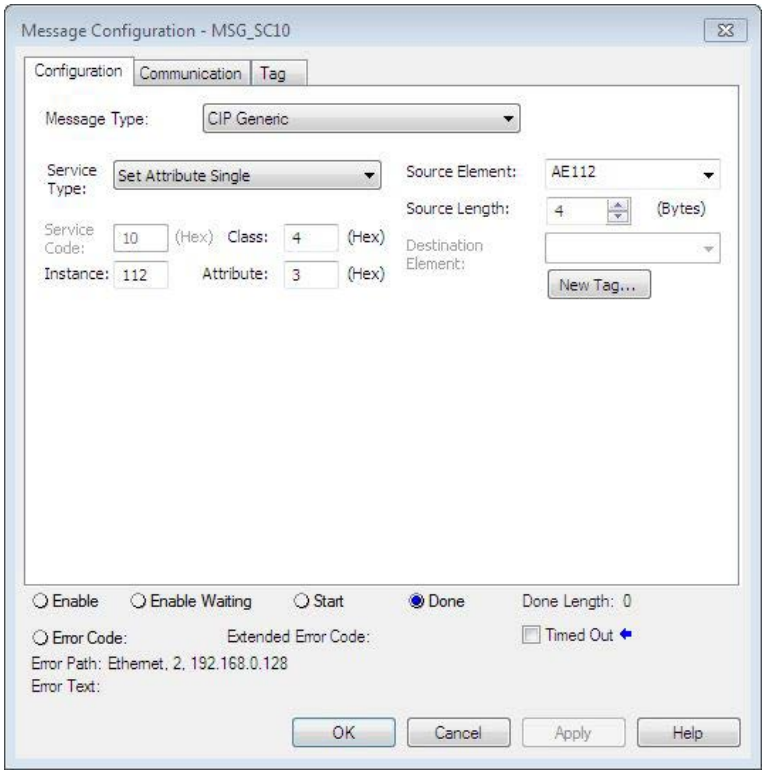
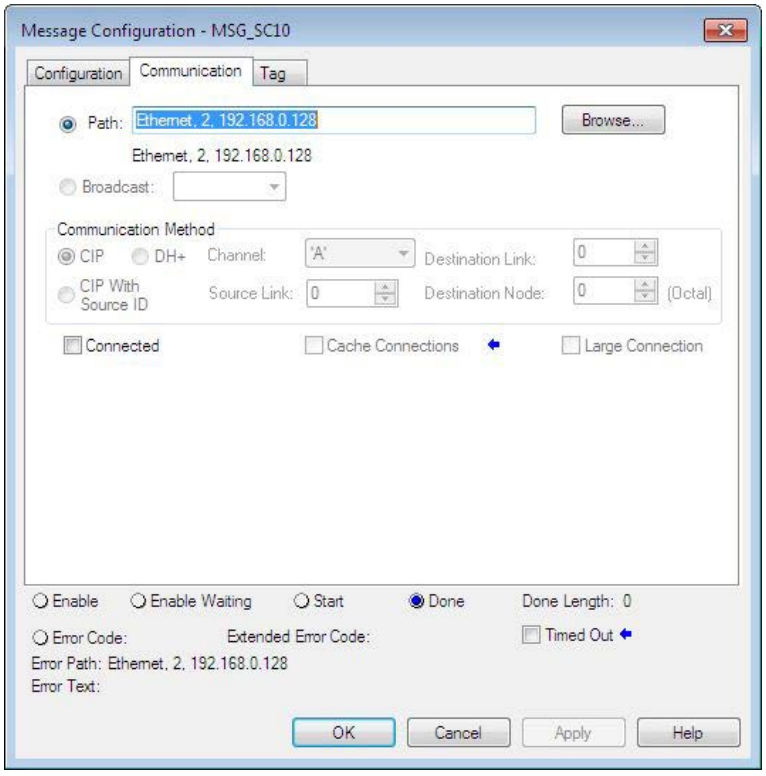


*Abbildung 191. MSG-Befehl — Registerkarte **Communication (Kommunikation)***




## Beispiel für das Lesen des Status virtueller Ausgänge

Zum Ausführen eines einmaligen Lesevorgangs des aktuellen Status der ersten 64 virtuellen Ausgänge verwenden Sie den Servicetyp 14 (einzelnes Attribut abrufen, hex 0E), Klasse 0×64, Instanz 1, Attribut 1. Eine erfolgreiche explizite Nachricht dieses Typs gibt zwei 32-Bit-Ganzzahlen zurück, die den Status von VO1 bis VO64 angeben.

Die folgende Abbildung zeigt den MSG-Befehl für diese explizite Nachricht.

*Abbildung 192. MSG-Befehl — Registerkarte **Konfiguration***

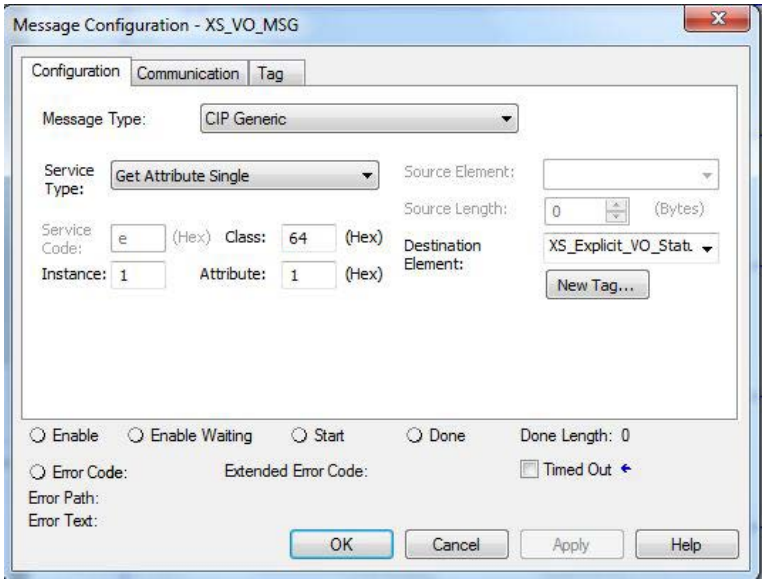


*Abbildung 193. MSG-Befehl — Registerkarte **Kommunikation***




Die folgende Abbildung zeigt das benutzerdefinierte Datenfeld (genannt XS_Explicit_VO_Status) mit zwei 32-Bit-Ganzzahlen.

*Abbildung 194. Benutzerdefiniertes Datenfeld*

| | | | | |
|---|---|---|---|---|
| XS_Explicit_VO_Status | {...} | {...} | Decimal | DINT[2] |
| XS_Explicit_VO_Status[0] | 1 | | Decimal | DINT |
| XS_Explicit_VO_Status[1] | 0 | | Decimal | DINT |

In diesen Beispieldaten können wir sehen, dass VO1 derzeit eingeschaltet ist. VO1 ist Wort 1, Bit 0 > 2^0 = 1

## Beispiel für das Lesen von Systeminformationen

Einige Systeminformationen können anhand der expliziten EtherNet/IP-Nachrichten aufgerufen werden. Dazu gehört beispielsweise der Konfigurationsname vom Sicherheitskontroller. Zum Abrufen dieser Informationen verwenden Sie den Servicetyp 14 (einzelnes Attribut abrufen, hex 0E), Klasse 0×72, Instanz 1, Attribut 3. Eine erfolgreiche explizite Nachricht dieses Typs gibt die 32-Bit-Länge und den ASCII-String zurück und umfasst auch den Konfigurationsnamen des Sicherheitskontrollers.

Die folgende Abbildung zeigt den MSG-Befehl für diese explizite Nachricht.

*Abbildung 195. MSG-Befehl — Registerkarte **Konfiguration***

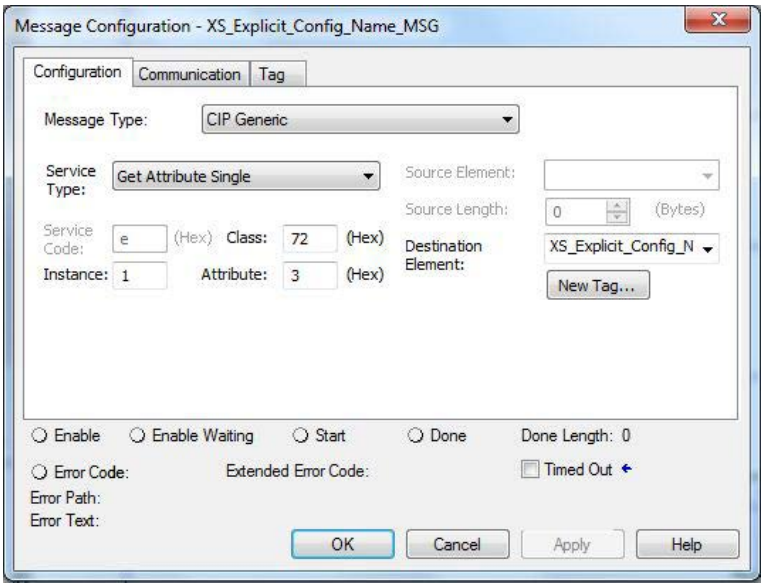
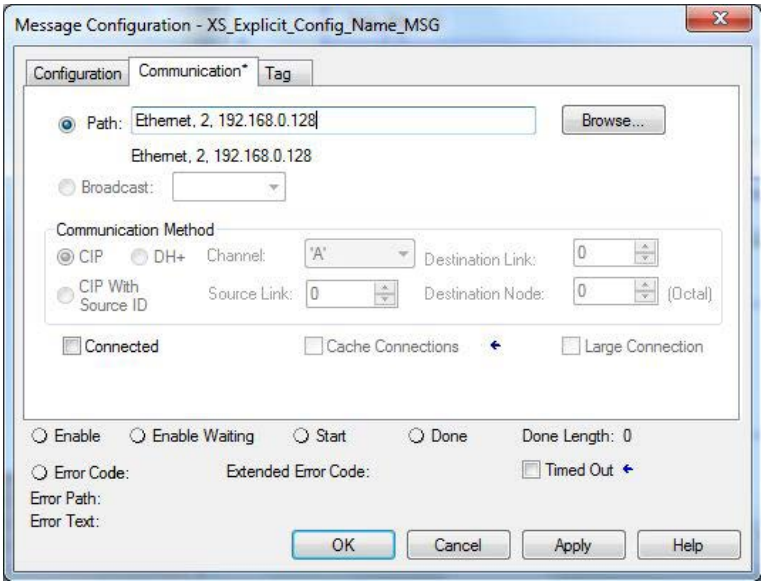


*Abbildung 196. MSG-Befehl — Registerkarte **Kommunikation***




Die folgende Abbildung zeigt das benutzerdefinierte Datenfeld (mit der Bezeichnung XS_Explicit_Config_Name) mit allen 8 Registern.

*Abbildung 197. Benutzerdefiniertes Datenfeld*

| XS_Explicit_Config_Name | {...} | {...} | Decimal | INT[10] |
|---|---|---|---|---|
| XS_Explicit_Config_Name[0] | 12 | | Decimal | INT |
| XS_Explicit_Config_Name[1] | 0 | | Decimal | INT |
| XS_Explicit_Config_Name[2] | '1B' | | ASCII | INT |
| XS_Explicit_Config_Name[3] | 'na' | | ASCII | INT |
| XS_Explicit_Config_Name[4] | ' k' | | ASCII | INT |
| XS_Explicit_Config_Name[5] | 'oC' | | ASCII | INT |
| XS_Explicit_Config_Name[6] | 'fn' | | ASCII | INT |
| XS_Explicit_Config_Name[7] | 'gi' | | ASCII | INT |
| XS_Explicit_Config_Name[8] | 0 | | Decimal | INT |
| XS_Explicit_Config_Name[9] | 0 | | Decimal | INT |

Die ersten zwei Register sind 32-Bit-Ganzzahlen und beschreiben, wie viele ASCII-Zeichen im Konfigurationsnamen vorkommen. Hier ist der Wert *12*. ASCII-Zeichen sind mit jeweils zwei Zeichen pro Register im sogenannten ControlLogix-Stringformat gepackt. Der Konfigurationsname hier ist *Blank Config (Leere Konfiguration)*, aber das ControlLogix-Stringformat zeigt diese Zeichen mit zwei Zeichen pro Zeile in umgekehrter Reihenfolge an.

### Explizite Schritt-für-Schritt-Nachrichten

Um eine explizite Nachrichtenverbindung komplett neu zu erstellen, müssen Sie in Allen-Bradley-SPS-Programmen folgende Schritte ausführen:

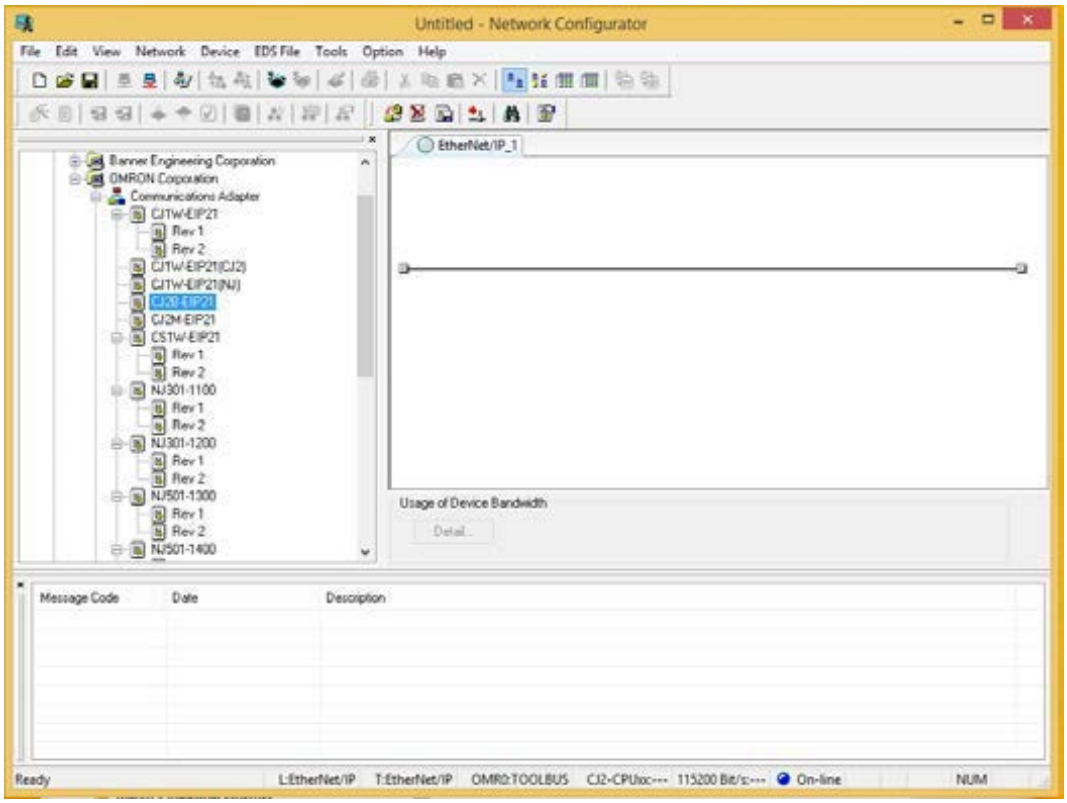
1. Erstellen Sie ein neues Tag mit dem Datentyp „Nachricht“.
2. Erstellen Sie ein neues Tag, der als Zielelement fungiert (ein 16-Bit-Array, das groß genug ist, die angeforderten Daten aufzunehmen).
3. Fügen Sie einen MSG-Befehl zum Kontaktplan hinzu (mit dem Nachrichten-Tag von Schritt 1 und dem Zielelement von Schritt 2). Die Klassen-, Instanz- und Attributwerte hängen von den gewünschten Daten ab.
4. Geben Sie auf der Registerkarte "Kommunikation" des MSG-Befehls den Pfad zum Sicherheitskontroller ein: z. B. `Ethernet, 2, 192.168.0.128`, wobei *2* für EtherNet/IP-Verbindungen in der SPS verwendet wird und die angezeigte Adresse die des Sicherheitskontrollers ist.

## 12.4.12 EIP in der Omron-SPS-Konfiguration

Die folgende Abbildung zeigt eine EtherNet/IP-Verbindung zwischen einem Sicherheitskontroller und einer Omron CJ2H-SPS.

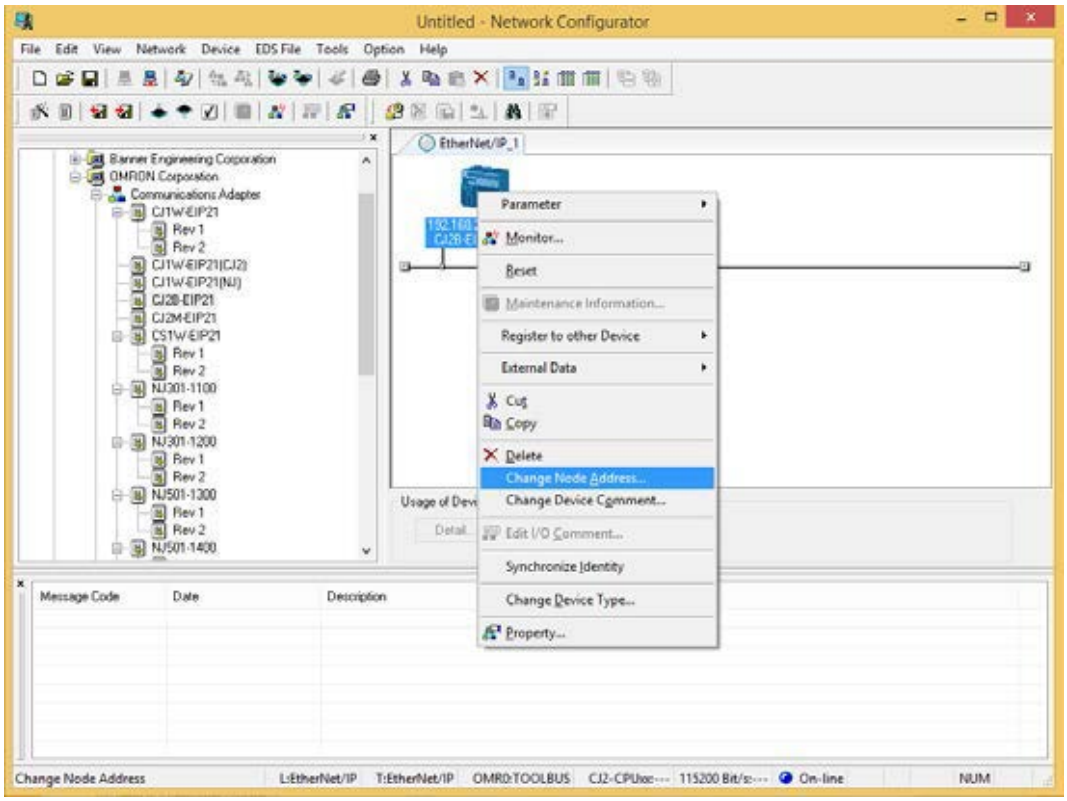
1. Öffnen Sie die Omron-Netzwerkkonfiguratorsoftware.

*Abbildung 198. Omron-Netzwerkkonfiguratorsoftware*



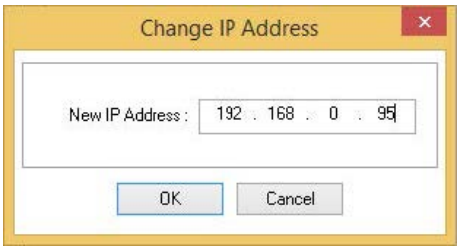

2. Fügen Sie dem Netzwerk die richtige SPS hinzu.
3. Klicken Sie mit der rechten Maustaste auf die SPS und klicken Sie dann auf **Knotenadresse ändern**, um die IP-Adresse zu ändern.

*Abbildung 199. Rechtsklick-Menü*



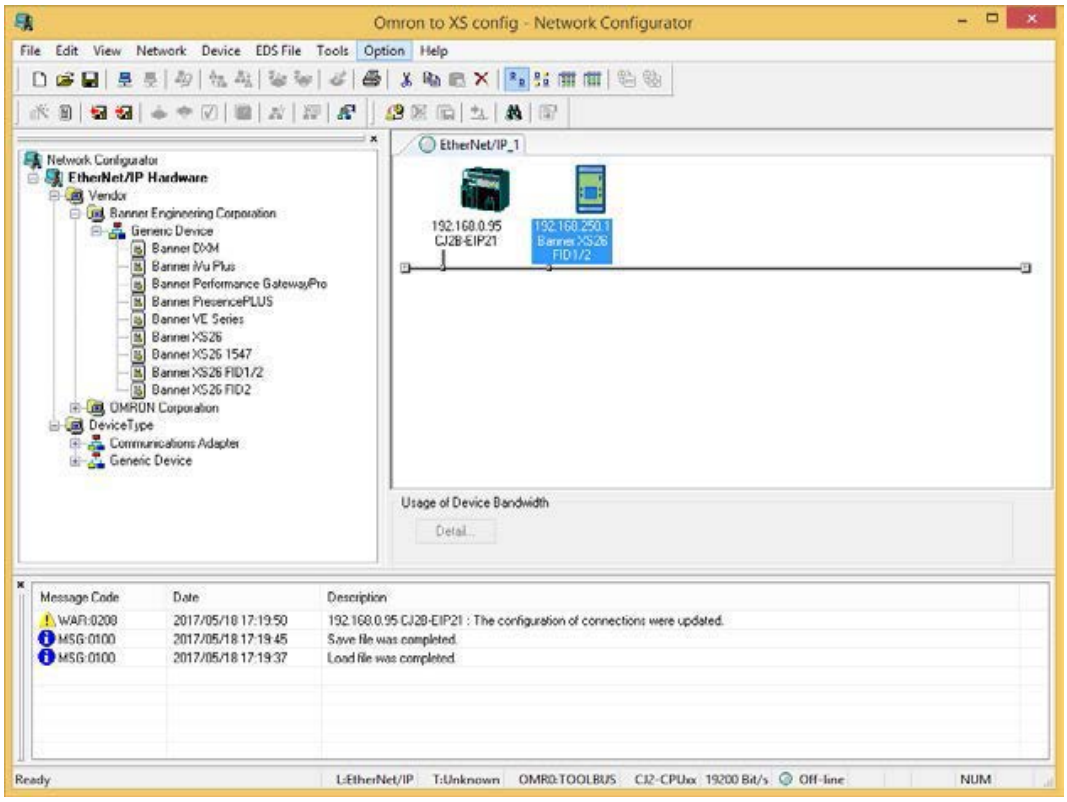

Hier die IP-Adresse der SPS:

*Abbildung 200. SPS-IP-Adresse*



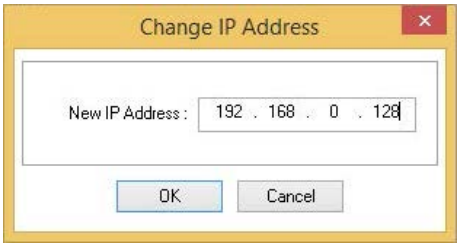

4. Installieren Sie die EDS-Datei des Sicherheitskontrollers.
   a) Siehe unter **EDS_File** > **Installieren**.
   b) Gehen Sie zur EDS-Datei und wählen Sie sie aus.
   c) Doppelklicken Sie in der Liste links auf das neue Element, um es zum Netzwerk hinzuzufügen.

*Abbildung 201. Hinzufügen des Sicherheitskontrollers*



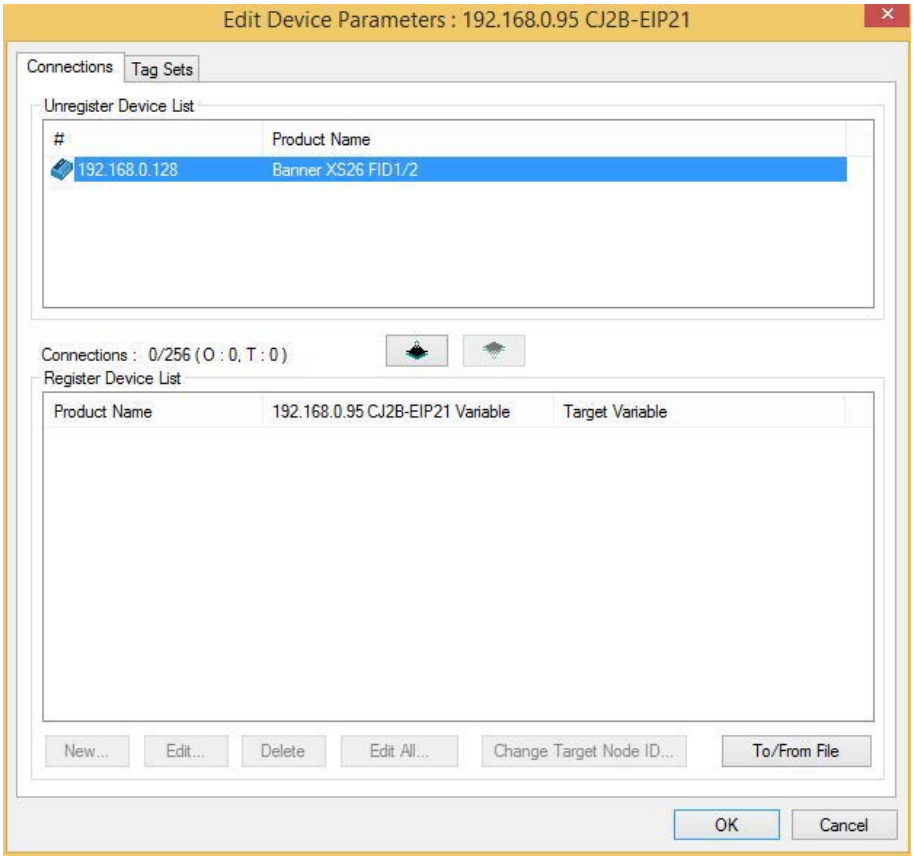

5. Klicken Sie mit der rechten Maustaste auf den Sicherheitskontroller und klicken Sie dann auf **Knotenadresse ändern**, um die IP-Adresse zu ändern.
6. Geben Sie die IP-Adresse des Sicherheitskontrollers ein.

*Abbildung 202. IP-Adresse des Sicherheitskontrollers*



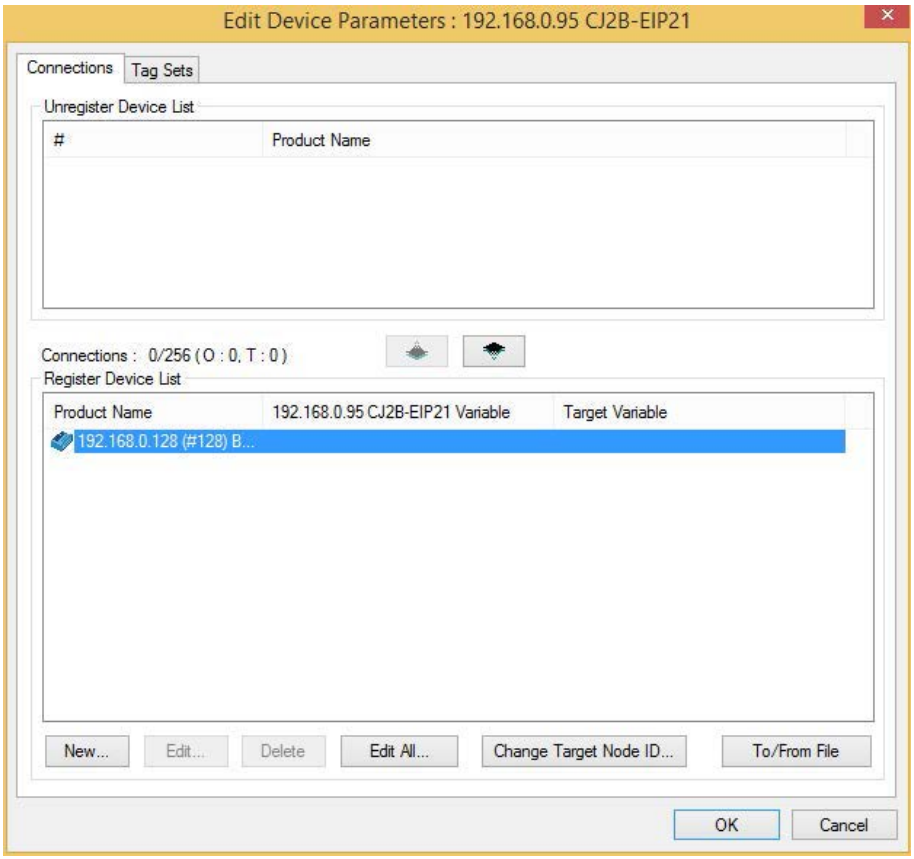

7. Doppelklicken Sie auf das SPS-Symbol, um die Geräteparameter zu bearbeiten.
   a) Wählen Sie den Sicherheitskontroller aus der **Liste "Registrierung von Gerät aufheben"**.

*Abbildung 203. **Liste "Registrierung von Gerät aufheben"***



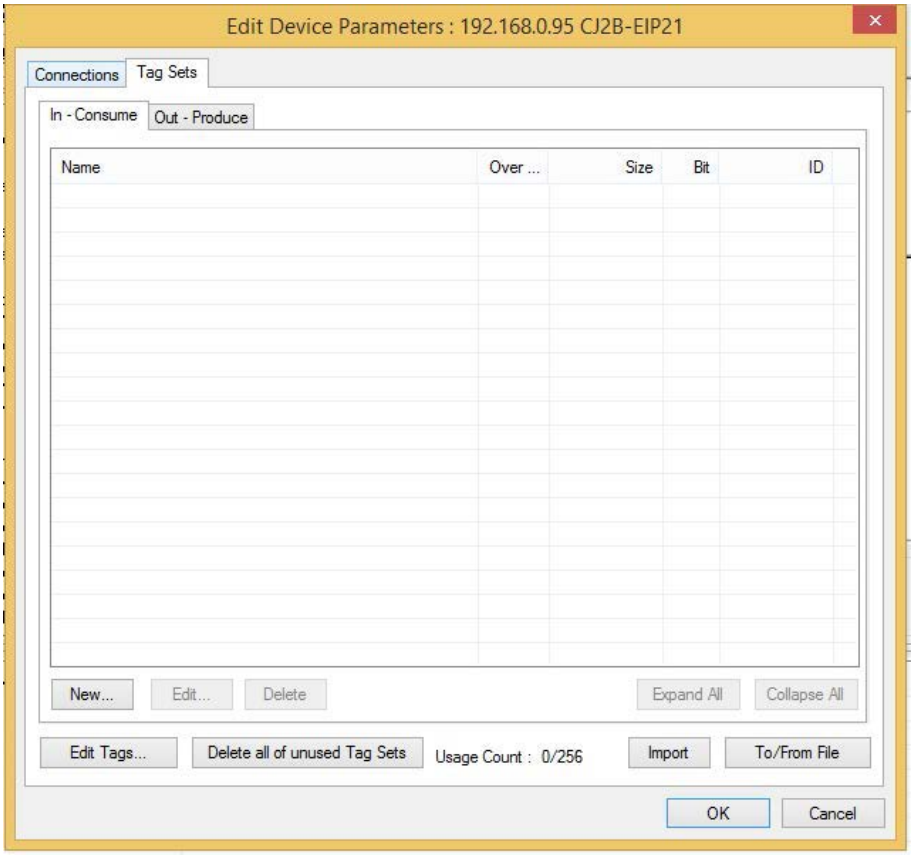

b) Klicken Sie auf den Pfeil nach unten, um ihn an die **Liste "Gerät registrieren"** zu senden.

*Abbildung 204. **Liste "Gerät registrieren"***




c) Klicken Sie auf die Registerkarte **Tag-Sets** (siehe nachfolgendes Fenster).

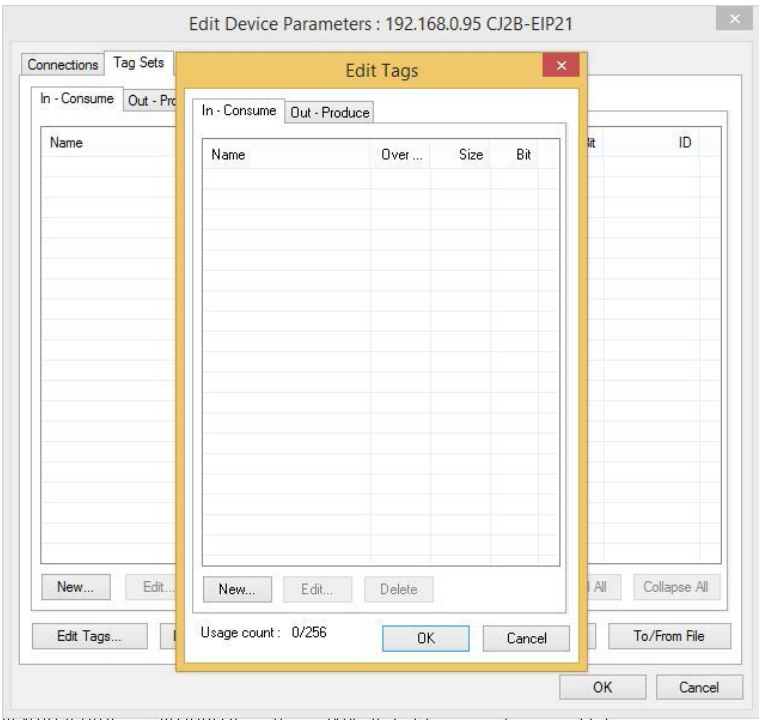
*Abbildung 205. Registerkarte **Tag-Sets***




d) Klicken Sie auf **Tags bearbeiten…**.
Das Fenster **Tags bearbeiten** wird angezeigt.

e) Klicken Sie auf **Eingehend - Verarbeiten**.

*Abbildung 206. Fenster **Tag bearbeiten** — Registerkarte **Eingehend - Verarbeiten***



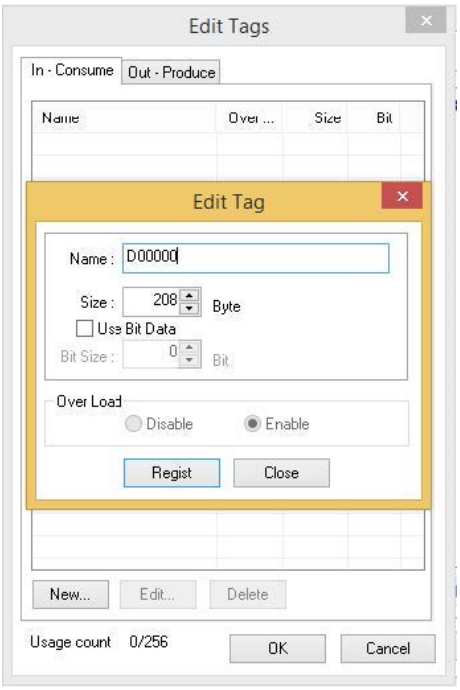

f) Klicken Sie auf **Neu**.
Das Fenster **Tag bearbeiten** wird angezeigt.

g) Wählen Sie einen entsprechenden Typ und eine entsprechende Größe für den CPU-Datenbereich aus.
In diesem Beispiel sendet der Sicherheitskontroller ausgehend 16-Bit-Wörter, sodass der DM-Bereich funktioniert. Wählen Sie eine **Size (Größe)** (Anzahl an Byte), die gleich der gewünschten EIP-Baugruppeninstanz ist. Hier geht es um *In - Consume (Eingehend – Verarbeiten)* (aus Sicht der SPS), also die T > O-Baugruppen. Weitere Informationen zu den Baugruppenobjekten finden Sie unter Eingänge zum Sicherheitskontroller

(Ausgänge von der SPS) auf Seite 172 und Ausgänge vom Sicherheitskontroller (Eingänge zur SPS) auf Seite 174. Die Auswahlmöglichkeiten sind:

- VO-Status/Fehler: 100 (0×64), Größe 16 Byte
- Fehlerindexwörter: 101 (0×65), Größe 208 Byte
- Nur Fehlerprotokoll: 102 (0×66), Größe 300 Byte
- Reset-/Abbruchverzögerung: 103 (0×67), Größe 70 Byte
- VRCD plus ISD: 104 (0×68), Größe 224 Byte

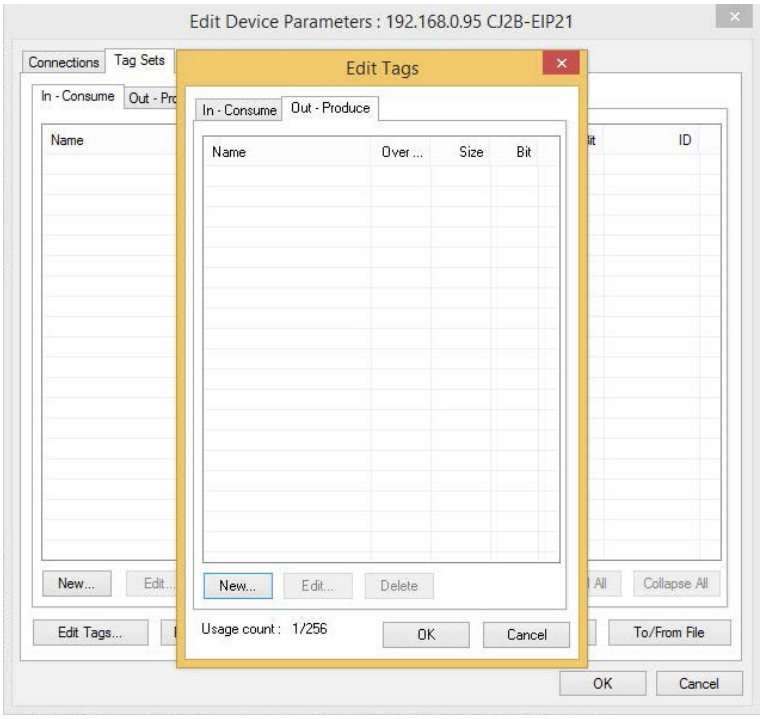
*Abbildung 207. Fenster **Tag bearbeiten***




h) Nachdem Sie den **Namen** (beachten Sie, dass sich dieser auf einen CPU-Datenbereich auf der CPU der SPS bezieht) und die **Größe** in Byte eingegeben haben, klicken Sie auf **Registrieren** und anschließend auf **Schließen**.

i) Klicken Sie auf die Registerkarte **Ausgehend - Erzeugen**.

*Abbildung 208. Registerkarte **Ausgehend – Erzeugen***



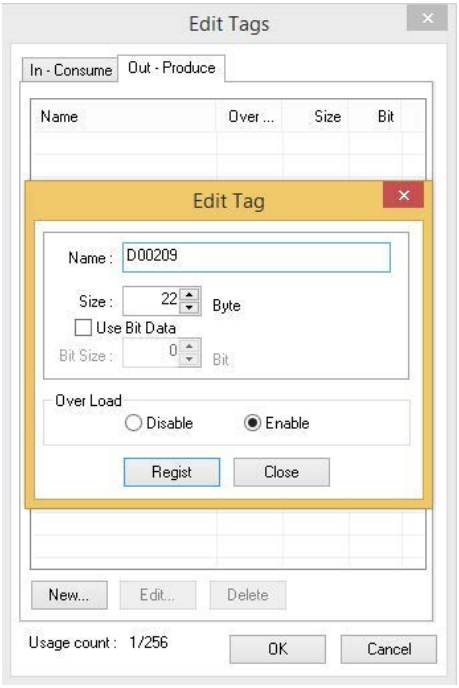

j) Klicken Sie auf **Neu**.

k) Wählen Sie einen entsprechenden Typ und eine entsprechende Größe für den CPU-Datenbereich aus.

Die Auswahlmöglichkeiten sind:

- 112 (0×70), Größe 2 Byte (keine Daten in diesen Registern)
- 113 (0×71), Größe 22 Byte (virtuelle Reset-/Abbruchverzögerung Bits)

*Abbildung 209. Fenster **Tag bearbeiten***




l) Nachdem Sie den **Namen** (beachten Sie, dass sich dieser auf einen CPU-Datenbereich auf der CPU der SPS bezieht) und die **Größe** in Byte eingegeben haben, klicken Sie auf **Registrieren** und anschließend auf **Schließen**.

m) Klicken Sie im Fenster **Tags bearbeiten** auf **OK**.
Daraufhin wird die Meldung "Die neuen Tags werden als Tag-Sets registriert" angezeigt.

n) Klicken Sie auf **Ja**.

8. Überprüfen Sie die Tags, indem Sie jeweils auf die Registerkarte **In-Consume (Eingehend - Verarbeiten)** und **Out - Produce (Ausgehend - Erzeugen)** doppelklicken.

*Abbildung 210. Registerkarte **Eingehend - Verarbeiten***

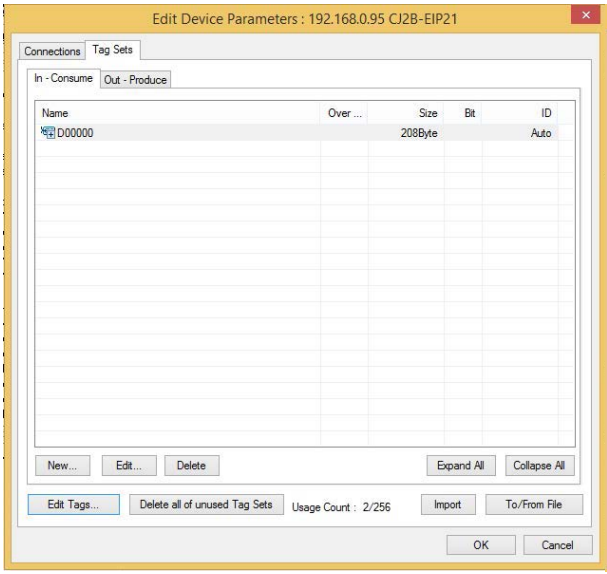
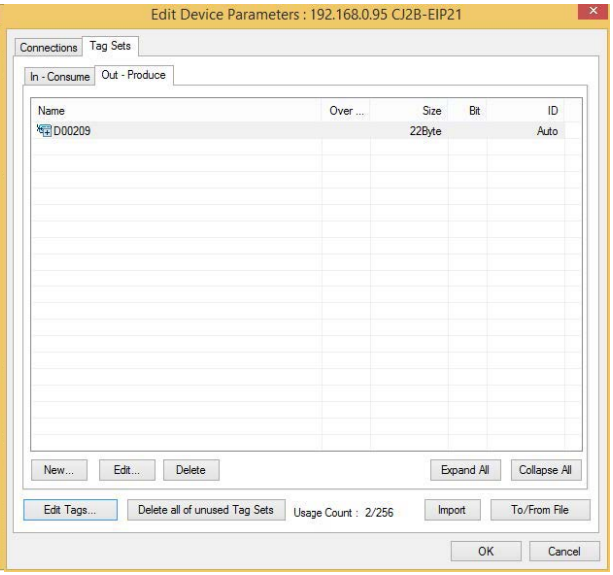
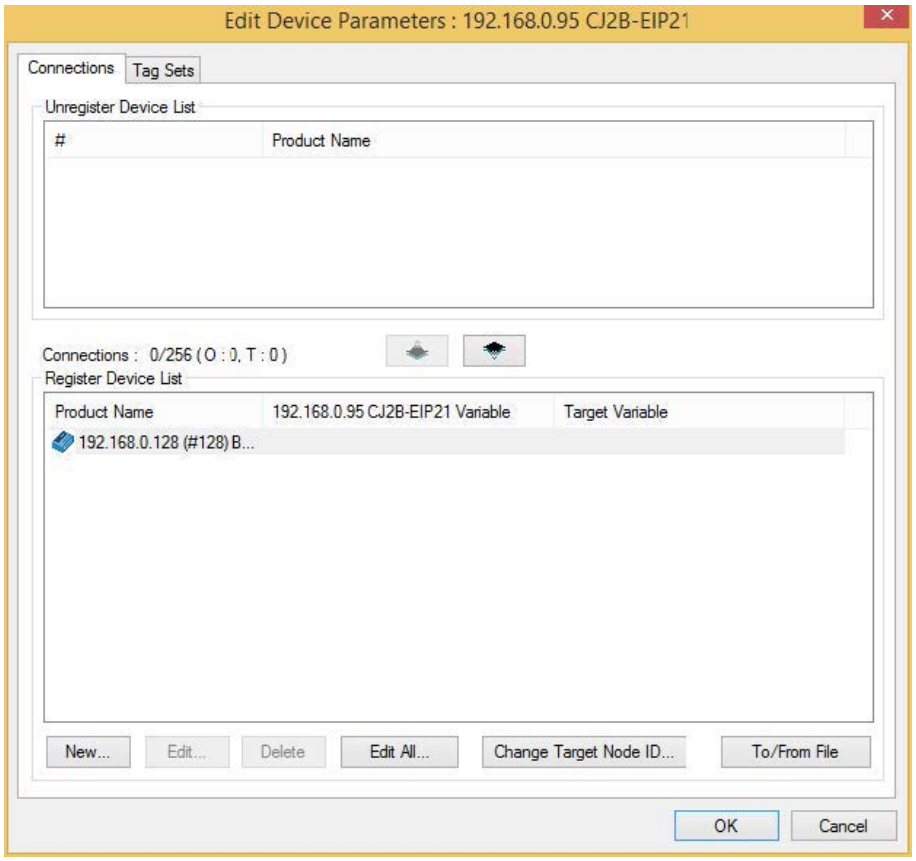



*Abbildung 211. Registerkarte **Ausgehend – Erzeugen***



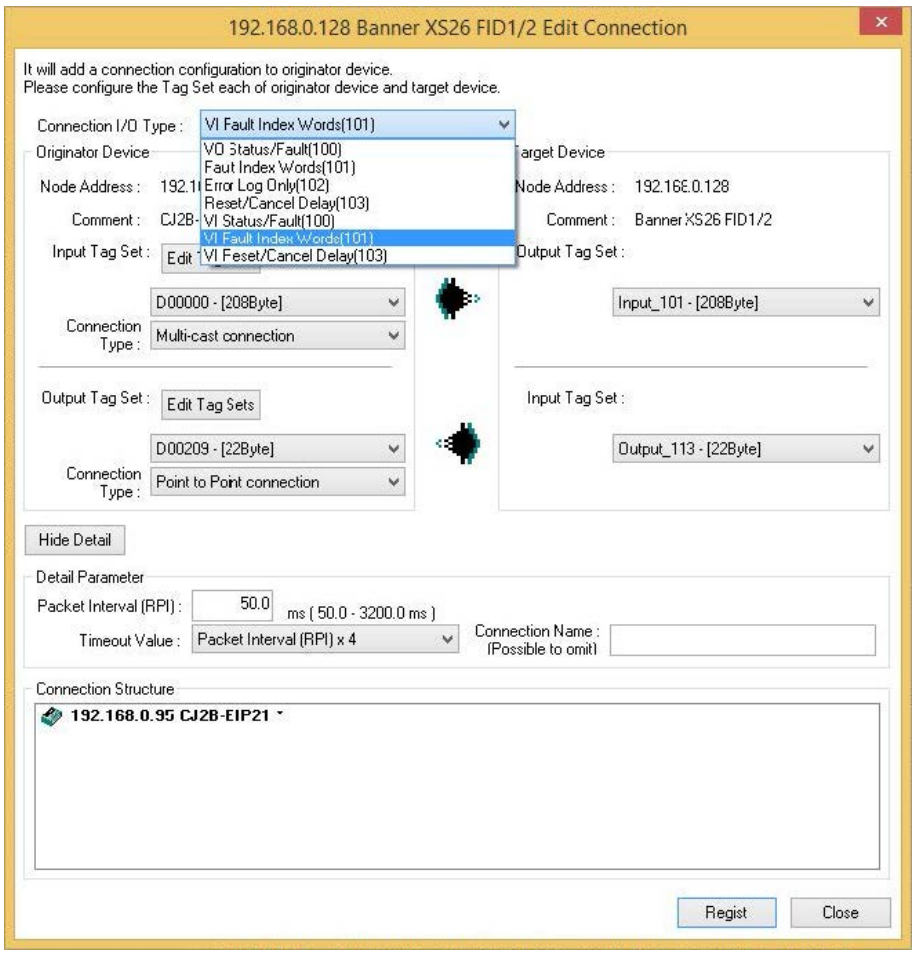

9. Gehen Sie zurück zur Registerkarte **Verbindungen**, um das nachfolgende Fenster aufzurufen.

*Abbildung 212. Fenster **Geräteparameter bearbeiten** — Registerkarte **Verbindungen***



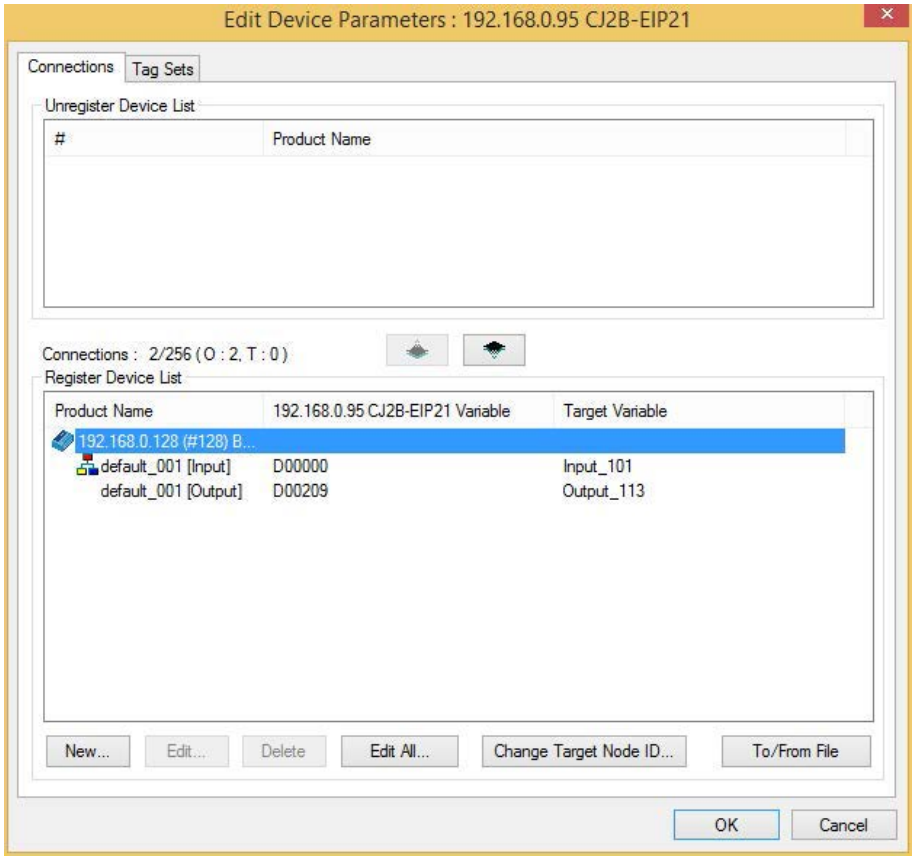

10. Doppelklicken Sie auf den in der **Liste "Gerät registrieren"** zu sehenden Sicherheitskontroller. Das Fenster **Verbindung bearbeiten** wird geöffnet.
11. Wählen Sie die entsprechenden **Verbindungen** und **RPI** aus.

*Abbildung 213. Verbindungen bearbeiten*



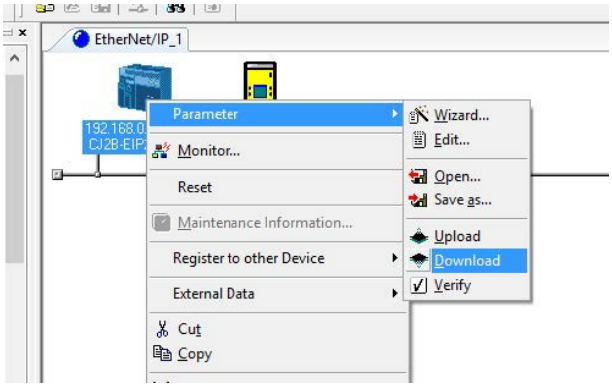

12. Klicken Sie auf **Registrieren** und dann auf **Schließen**.
13. Klicken Sie im Fenster **Edit Parameters (Parameter bearbeiten)** auf **OK**.

*Abbildung 214. Fenster **Parameter bearbeiten***



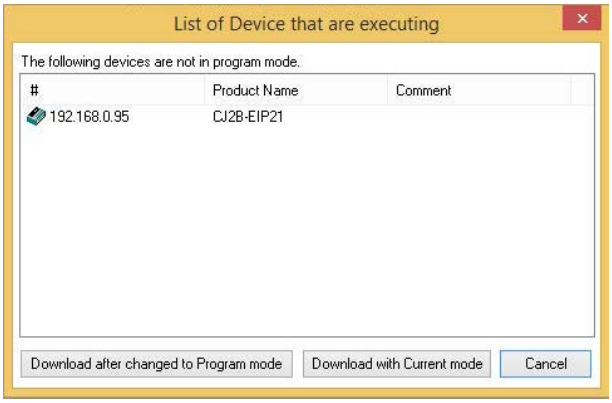
14. Gehen Sie online und laden Sie die Konfiguration auf die SPS herunter.

*Abbildung 215. Herunterladen der Konfiguration*




15. Klicken Sie bei der Meldung "Herunterladen der Parameter auf die ausgewählten Geräte starten" auf **Ja**.
16. Wählen Sie die Download-Option aus.

*Abbildung 216. Download-Optionen*



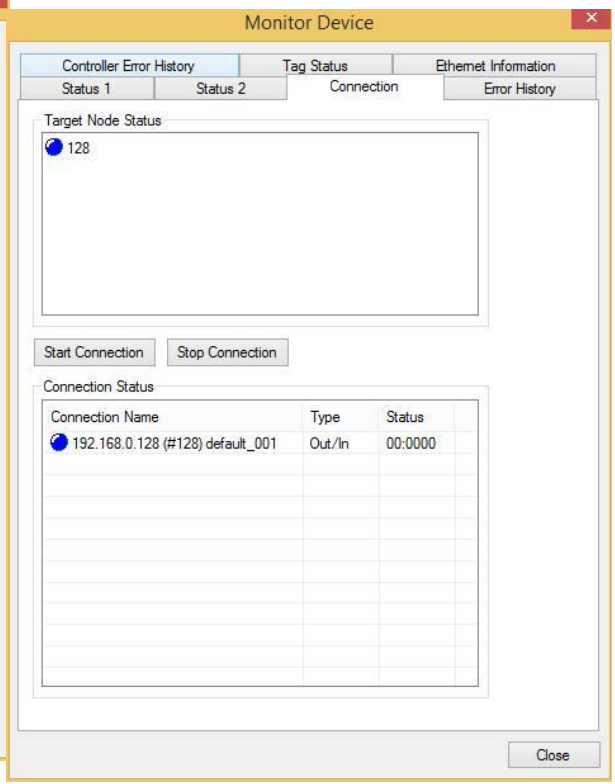

17. Klicken Sie für die Meldung "Rückkehr zum Status des Kontrollermodus wie vor Beginn des Downloads" auf **Ja**. Klicken Sie anschließend für die Meldung "Die Geräteparameter wurden heruntergeladen" auf **OK**.
18. Klicken Sie mit der rechten Maustaste auf das SPS-Symbol und wählen Sie **Monitor (Überwachen)** aus.

    In diesem Fenster können Sie erkennen, ob die Verbindung in Ordnung ist. Blaue Symbole weisen auf eine fehlerfrei ausgeführte Verbindung hin.

*Abbildung 217. Fenster **Gerät überwachen** — Registerkarte **Status 1***

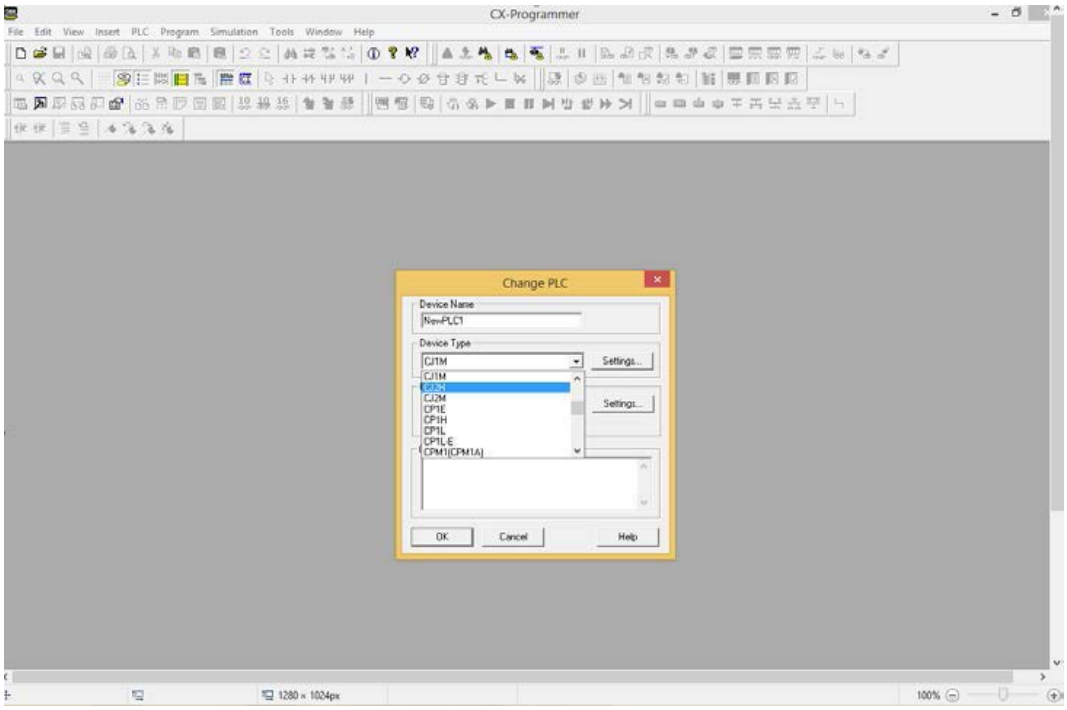



*Abbildung 218. Fenster **Gerät überwachen** — Registerkarte **Verbindung***



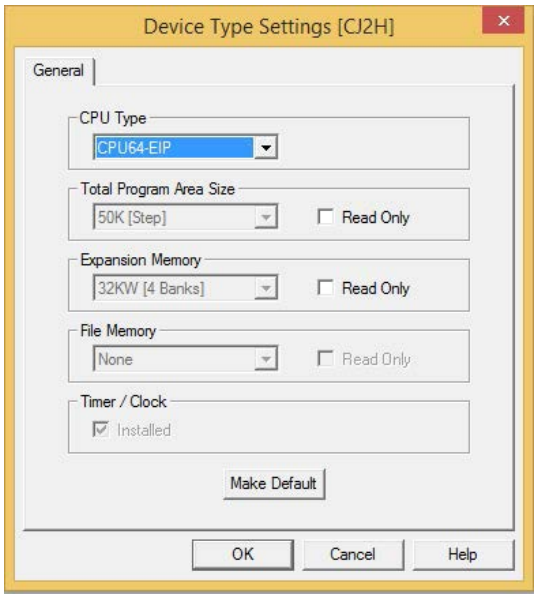

19. Öffnen Sie die CX-Programmiersoftware.
20. Siehe unter **Datei** > **Neu**.
    Das Fenster **SPS ändern** wird angezeigt.
21. Wählen Sie ein SPS-Modell aus und klicken Sie dann auf **Einstellungen**.

*Abbildung 219. Fenster **SPS ändern***



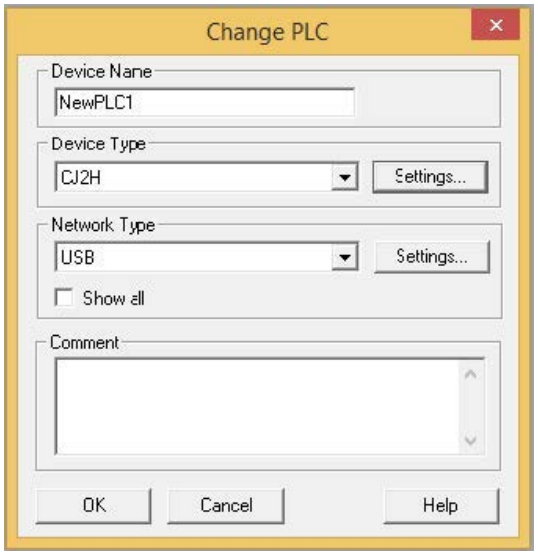

22. Wählen Sie einen **CPU-Typ** aus und klicken Sie auf **OK**.

*Abbildung 220. Fenster **Gerätetypeinstellungen***



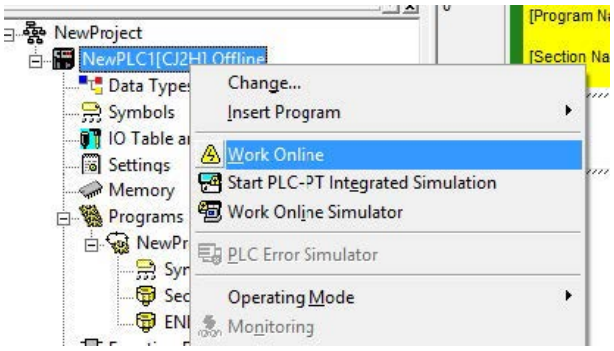

23. Wählen Sie einen **Netzwerktyp** aus und klicken Sie auf **OK**.

*Abbildung 221. Fenster **SPS ändern***



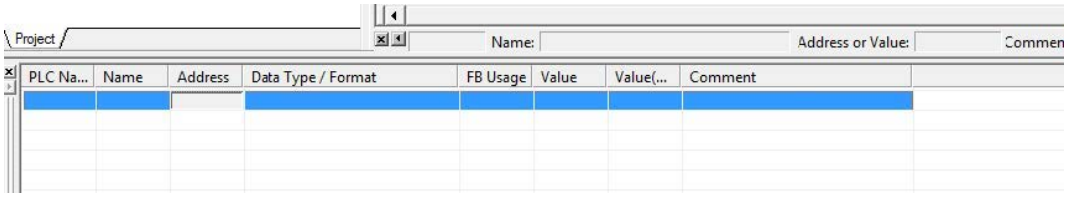

24. Gehen Sie mit der SPS online; klicken Sie dazu auf **Online arbeiten**.

*Abbildung 222. Online arbeiten*




25. Klicken Sie auf **Ja**, um eine Verbindung mit der SPS herzustellen.
26. Siehe unter **Ansicht** > **Fenster** > **Beobachten**.
27. Klicken Sie im Fenster **Beobachten** auf die obere Zeile.
    Das Fenster **Dialog bearbeiten** wird geöffnet.

*Abbildung 223. Fenster **Beobachten***

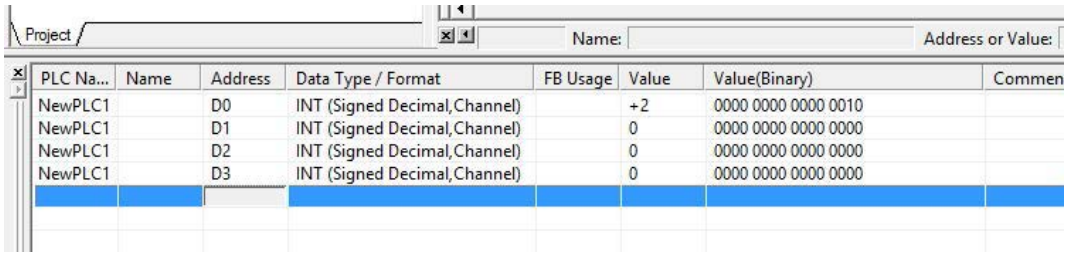



28. Fügen Sie im Fenster **Beobachten** einige Register hinzu.

*Abbildung 224. **Dialog bearbeiten***




*Abbildung 225. Fenster **Beobachten** — Vier Register*




Im Fenster **Beobachten** in der vorherigen Abbildung sind vier Register der Daten des Sicherheitskontrollerausgangs (SPS-Eingang) zu sehen. Beachten Sie, wie der virtuelle Ausgang Nr. 2 aktuell aktiviert ist (D0-Register, Bit 1).

# 12.5 Modbus/TCP

Das Modbus/TCP-Protokoll bietet Geräteinformationen anhand von Registern und Spulenblöcken, die vom Slave-Gerät definiert sind.

In diesem Abschnitt werden Register und Spulenblöcke definiert. Gemäß Spezifikation verwendet Modbus/TCP den TCP-Port 502. Der Sicherheitskontroller unterstützt keine Einheiten-ID von 0 (gelegentlich auch als Slave-ID oder Geräte-ID bezeichnet).

Anhand der folgenden Register werden Ausgangswerte vom Sicherheitskontroller an die SPS gesendet. Die Informationen in diesen Registern können als Eingangsregister (30000) mit dem Modbus-Funktionscode 04 (Eingangsregister lesen) gelesen werden. Dieselben Werte können auch als Halteregister (40000) mit dem Modbus-Funktionscode 03 (Halteregister lesen) gelesen werden. Die Statusinformationen für alle virtuellen Ausgänge und ihre Fehlerflags, die in den ersten acht Registern enthalten sind, können auch als Eingänge (10000) mit dem Modbus-Funktionscode 02 (Eingangsstatus lesen) gelesen werden.

**Anmerkung:** XS/SC26-2 Sicherheitskontroller ab FID 2 unterscheiden sich von den FID 1-Modellen des XS/SC26-2 insofern, als Modelle ab FID 2 keinen Zugriff mehr auf die ersten 64 virtuellen Ausgänge über Modbus/TCP-Spulen 0001–00064 sowie auf die ersten 64 virtuellen Ausgangsfehlerbits über Modbus/TCP-Spulen 00065–00128 zulassen.

### Die ersten 64 virtuellen Ausgänge und virtuellen Ausgangsfehler (Eingänge 10001–10128).

*Tabelle 24. 02: Eingangsstatus lesen*

| Eingang Nr. | NAME |
|---|---|
| 10001 | VO1 |
| 10002 | VO2 |
| 10003 | VO3 |
| … | … |
| 10063 | VO63 |
| 10064 | VO64 |

| Eingang Nr. | NAME |
|---|---|
| 10065 | VO1-Fehlerbit |
| 10066 | VO2-Fehlerbit |
| 10067 | VO3-Fehlerbit |
| … | … |
| 10127 | VO63-Fehlerbit |
| 10128 | VO64-Fehlerbit |

### Alle 256 virtuellen Ausgänge und virtuellen Ausgangsfehler (Eingänge 11001–11256, 12001–12256).

*Tabelle 25. 02: Eingangsstatus lesen*

| Eingang Nr. | NAME |
|---|---|
| 11001 | VO1 |
| 11002 | VO2 |
| 11003 | VO3 |
| … | … |
| 11255 | VO255 |
| 11256 | VO256 |

| Eingang Nr. | NAME |
|---|---|
| 12001 | VO1-Fehlerbit |
| 12002 | VO2-Fehlerbit |
| 12003 | VO3-Fehlerbit |
| … | … |
| 12255 | VO255-Fehlerbit |
| 12256 | VO256-Fehlerbit |

### Steuerung und Rückkopplung für virtuelle Eingänge, virtuellen Reset/Abbruchverzögerung (Spulen 3001–3064, 4001–4016, Eingänge 15001–15016).

Siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 57.

*Tabelle 26. 05: Einzelspule schreiben; 02: Eingangsstatus lesen*

| Eingang Nr. | NAME |
|---|---|
| 3001 | VI1 ein/aus |
| 3002 | VI2 ein/aus |
| … | … |
| 3064 | VI 64 ein/aus |
| 4001 | VRCD1 ein/aus |
| 4002 | VRCD2 ein/aus |
| … | |
| 4016 | VRCD16 ein/aus |

| Eingang Nr. | NAME |
|---|---|
| 15001 | VRCD1 Feedback |
| 15002 | VRCD2 Feedback |
| … | … |
| 15016 | VRCD16 Feedback |

### Sicherheitskontroller-Ausgangsregister (Modbus/TCP-Eingangs- oder Halteregister)

| Eingangs-reg. Nr. | Haltereg. Nr. | WORTNAME | DATENTYP |
|---|---|---|---|
| 1 | 1 | VO1–VO16 (siehe Flags auf Seite 217) | 16-Bit-Ganzzahl |
| 2 | 2 | VO17–VO32 (siehe Flags auf Seite 217) | 16-Bit-Ganzzahl |

| Eingangs-reg. Nr. | Haltereg. Nr. | WORTNAME | DATENTYP |
|---|---|---|---|
| 3 | 3 | VO33–VO48 (siehe Flags auf Seite 217) | 16-Bit-Ganzzahl |
| 4 | 4 | VO49–VO64 (siehe Flags auf Seite 217) | 16-Bit-Ganzzahl |
| 5 | 5 | Fehlerbits für VO1–VO16 (siehe Flags auf Seite 217) | 16-Bit-Ganzzahl |
| 6 | 6 | Fehlerbits für VO17–VO32 (siehe Flags auf Seite 217) | 16-Bit-Ganzzahl |
| 7 | 7 | Fehlerbits für VO33–VO48 (siehe Flags auf Seite 217) | 16-Bit-Ganzzahl |
| 8 | 8 | Fehlerbits für VO49–VO64 (siehe Flags auf Seite 217) | 16-Bit-Ganzzahl |
| | 9 | Virtueller Eingang Ein/Aus (1–16) | 16-Bit-Ganzzahl |
| | 10 | Virtueller Eingang Ein/Aus (17–32) | 16-Bit-Ganzzahl |
| | 11 | Virtueller Eingang Ein/Aus (33–48) | 16-Bit-Ganzzahl |
| | 12 | Virtueller Eingang Ein/Aus (49–64) | 16-Bit-Ganzzahl |
| 13–16 | 13–16 | *reserviert* | 16-Bit-Ganzzahl |
| | 17 | Virtuelle Reset-/Abbruchverzögerung (1–16) [RCD-Registerbits] (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 57) | 16-Bit-Ganzzahl |
| 18 | 18 | reserviert | 16-Bit-Ganzzahl |
| | 19 | RCD-Auslösecode [RCD-Aktivierung Register] (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 57) | 16-Bit-Ganzzahl |
| 20 | 20 | Virtuelle Reset-/Abbruchverzögerung (1–16) Feedback [RCD-Feedback Registerbits] (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 57) | 16-Bit-Ganzzahl |
| 21 | 21 | *reserviert* | 16-Bit-Ganzzahl |
| 22 | 22 | RCD-Auslösecode Feedback [RCD-Aktivierung Feedbackregister] (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 57) | 16-Bit-Ganzzahl |
| 23–40 | 23–40 | reserviert | 16-Bit-Ganzzahl |
| 41 | 41 | VO1-Fehlerindex | 16-Bit-Ganzzahl |
| 42 | 42 | VO2-Fehlerindex | 16-Bit-Ganzzahl |
| 43 | 43 | VO3-Fehlerindex | 16-Bit-Ganzzahl |
| 44 | 44 | VO4-Fehlerindex | 16-Bit-Ganzzahl |
| 45 | 45 | VO5-Fehlerindex | 16-Bit-Ganzzahl |
| 46 | 46 | VO6-Fehlerindex | 16-Bit-Ganzzahl |
| 47 | 47 | VO7-Fehlerindex | 16-Bit-Ganzzahl |
| 48 | 48 | VO8-Fehlerindex | 16-Bit-Ganzzahl |
| 49 | 49 | VO9-Fehlerindex | 16-Bit-Ganzzahl |
| 50 | 50 | VO10-Fehlerindex | 16-Bit-Ganzzahl |
| 51 | 51 | VO11-Fehlerindex | 16-Bit-Ganzzahl |
| 52 | 52 | VO12-Fehlerindex | 16-Bit-Ganzzahl |
| 53 | 53 | VO13-Fehlerindex | 16-Bit-Ganzzahl |
| 54 | 54 | VO14-Fehlerindex | 16-Bit-Ganzzahl |
| 55 | 55 | VO15-Fehlerindex | 16-Bit-Ganzzahl |

| Eingangs-reg. Nr. | Haltereg. Nr. | WORTNAME | DATENTYP |
|---|---|---|---|
| 56 | 56 | VO16-Fehlerindex | 16-Bit-Ganzzahl |
| 57 | 57 | VO17-Fehlerindex | 16-Bit-Ganzzahl |
| 58 | 58 | VO18-Fehlerindex | 16-Bit-Ganzzahl |
| 59 | 59 | VO19-Fehlerindex | 16-Bit-Ganzzahl |
| 60 | 60 | VO20-Fehlerindex | 16-Bit-Ganzzahl |
| 61 | 61 | VO21-Fehlerindex | 16-Bit-Ganzzahl |
| 62 | 62 | VO22-Fehlerindex | 16-Bit-Ganzzahl |
| 63 | 63 | VO23-Fehlerindex | 16-Bit-Ganzzahl |
| 64 | 64 | VO24-Fehlerindex | 16-Bit-Ganzzahl |
| 65 | 65 | VO25-Fehlerindex | 16-Bit-Ganzzahl |
| 66 | 66 | VO26-Fehlerindex | 16-Bit-Ganzzahl |
| 67 | 67 | VO27-Fehlerindex | 16-Bit-Ganzzahl |
| 68 | 68 | VO28-Fehlerindex | 16-Bit-Ganzzahl |
| 69 | 69 | VO29-Fehlerindex | 16-Bit-Ganzzahl |
| 70 | 70 | VO30-Fehlerindex | 16-Bit-Ganzzahl |
| 71 | 71 | VO31-Fehlerindex | 16-Bit-Ganzzahl |
| 72 | 72 | VO32-Fehlerindex | 16-Bit-Ganzzahl |
| 73 | 73 | VO33-Fehlerindex | 16-Bit-Ganzzahl |
| 74 | 74 | VO34-Fehlerindex | 16-Bit-Ganzzahl |
| 75 | 75 | VO35-Fehlerindex | 16-Bit-Ganzzahl |
| 76 | 76 | VO36-Fehlerindex | 16-Bit-Ganzzahl |
| 77 | 77 | VO37-Fehlerindex | 16-Bit-Ganzzahl |
| 78 | 78 | VO38-Fehlerindex | 16-Bit-Ganzzahl |
| 79 | 79 | VO39-Fehlerindex | 16-Bit-Ganzzahl |
| 80 | 80 | VO40-Fehlerindex | 16-Bit-Ganzzahl |
| 81 | 81 | VO41-Fehlerindex | 16-Bit-Ganzzahl |
| 82 | 82 | VO42-Fehlerindex | 16-Bit-Ganzzahl |
| 83 | 83 | VO43-Fehlerindex | 16-Bit-Ganzzahl |
| 84 | 84 | VO44-Fehlerindex | 16-Bit-Ganzzahl |
| 85 | 85 | VO45-Fehlerindex | 16-Bit-Ganzzahl |
| 86 | 86 | VO46-Fehlerindex | 16-Bit-Ganzzahl |
| 87 | 87 | VO47-Fehlerindex | 16-Bit-Ganzzahl |
| 88 | 88 | VO48-Fehlerindex | 16-Bit-Ganzzahl |
| 89 | 89 | VO49-Fehlerindex | 16-Bit-Ganzzahl |
| 90 | 90 | VO50-Fehlerindex | 16-Bit-Ganzzahl |
| 91 | 91 | VO51-Fehlerindex | 16-Bit-Ganzzahl |
| 92 | 92 | VO52-Fehlerindex | 16-Bit-Ganzzahl |
| 93 | 93 | VO53-Fehlerindex | 16-Bit-Ganzzahl |
| 94 | 94 | VO54-Fehlerindex | 16-Bit-Ganzzahl |
| 95 | 95 | VO55-Fehlerindex | 16-Bit-Ganzzahl |
| 96 | 96 | VO56-Fehlerindex | 16-Bit-Ganzzahl |
| 97 | 97 | VO57-Fehlerindex | 16-Bit-Ganzzahl |

| Eingangs-reg. Nr. | Haltereg. Nr. | WORTNAME | DATENTYP |
|---|---|---|---|
| 98 | 98 | VO58-Fehlerindex | 16-Bit-Ganzzahl |
| 99 | 99 | VO59-Fehlerindex | 16-Bit-Ganzzahl |
| 100 | 100 | VO60-Fehlerindex | 16-Bit-Ganzzahl |
| 101 | 101 | VO61-Fehlerindex | 16-Bit-Ganzzahl |
| 102 | 102 | VO62-Fehlerindex | 16-Bit-Ganzzahl |
| 103 | 103 | VO63-Fehlerindex | 16-Bit-Ganzzahl |
| 104 | 104 | VO64-Fehlerindex | 16-Bit-Ganzzahl |
| 105–106 | 105–106 | Vollständiger VO1-Fehlercode | 32-Bit-Ganzzahl |
| 107–108 | 107–108 | Vollständiger VO2-Fehlercode | 32-Bit-Ganzzahl |
| 109–110 | 109–110 | Vollständiger VO3-Fehlercode | 32-Bit-Ganzzahl |
| 111–112 | 111–112 | Vollständiger VO4-Fehlercode | 32-Bit-Ganzzahl |
| 113–114 | 113–114 | Vollständiger VO5-Fehlercode | 32-Bit-Ganzzahl |
| 115–116 | 115–116 | Vollständiger VO6-Fehlercode | 32-Bit-Ganzzahl |
| 117–118 | 117–118 | Vollständiger VO7-Fehlercode | 32-Bit-Ganzzahl |
| 119–120 | 119–120 | Vollständiger VO8-Fehlercode | 32-Bit-Ganzzahl |
| 121–122 | 121–122 | Vollständiger VO9-Fehlercode | 32-Bit-Ganzzahl |
| 123–124 | 123–124 | Vollständiger VO10-Fehlercode | 32-Bit-Ganzzahl |
| 125–126 | 125–126 | Vollständiger VO11-Fehlercode | 32-Bit-Ganzzahl |
| 127–128 | 127–128 | Vollständiger VO12-Fehlercode | 32-Bit-Ganzzahl |
| 129–130 | 129–130 | Vollständiger VO13-Fehlercode | 32-Bit-Ganzzahl |
| 131–132 | 131–132 | Vollständiger VO14-Fehlercode | 32-Bit-Ganzzahl |
| 133–134 | 133–134 | Vollständiger VO15-Fehlercode | 32-Bit-Ganzzahl |
| 135–136 | 135–136 | Vollständiger VO16-Fehlercode | 32-Bit-Ganzzahl |
| 137–138 | 137–138 | Vollständiger VO17-Fehlercode | 32-Bit-Ganzzahl |
| 139–140 | 139–140 | Vollständiger VO18-Fehlercode | 32-Bit-Ganzzahl |
| 141–142 | 141–142 | Vollständiger VO19-Fehlercode | 32-Bit-Ganzzahl |
| 143–144 | 143–144 | Vollständiger VO20-Fehlercode | 32-Bit-Ganzzahl |
| 145–146 | 145–146 | Vollständiger VO21-Fehlercode | 32-Bit-Ganzzahl |
| 147–148 | 147–148 | Vollständiger VO22-Fehlercode | 32-Bit-Ganzzahl |
| 149–150 | 149–150 | Vollständiger VO23-Fehlercode | 32-Bit-Ganzzahl |
| 151–152 | 151–152 | Vollständiger VO24-Fehlercode | 32-Bit-Ganzzahl |
| 153–154 | 153–154 | Vollständiger VO25-Fehlercode | 32-Bit-Ganzzahl |
| 155–156 | 155–156 | Vollständiger VO26-Fehlercode | 32-Bit-Ganzzahl |
| 157–158 | 157–158 | Vollständiger VO27-Fehlercode | 32-Bit-Ganzzahl |
| 159–160 | 159–160 | Vollständiger VO28-Fehlercode | 32-Bit-Ganzzahl |
| 161–162 | 161–162 | Vollständiger VO29-Fehlercode | 32-Bit-Ganzzahl |
| 163–164 | 163–164 | Vollständiger VO30-Fehlercode | 32-Bit-Ganzzahl |
| 165–166 | 165–166 | Vollständiger VO31-Fehlercode | 32-Bit-Ganzzahl |
| 167–168 | 167–168 | Vollständiger VO32-Fehlercode | 32-Bit-Ganzzahl |
| 169–170 | 169–170 | Vollständiger VO33-Fehlercode | 32-Bit-Ganzzahl |
| 171–172 | 171–172 | Vollständiger VO34-Fehlercode | 32-Bit-Ganzzahl |
| 173–174 | 173–174 | Vollständiger VO35-Fehlercode | 32-Bit-Ganzzahl |

| Eingangs-reg. Nr. | Haltereg. Nr. | WORTNAME | DATENTYP |
|---|---|---|---|
| 175–176 | 175–176 | Vollständiger VO36-Fehlercode | 32-Bit-Ganzzahl |
| 177–178 | 177–178 | Vollständiger VO37-Fehlercode | 32-Bit-Ganzzahl |
| 179–180 | 179–180 | Vollständiger VO38-Fehlercode | 32-Bit-Ganzzahl |
| 181–182 | 181–182 | Vollständiger VO39-Fehlercode | 32-Bit-Ganzzahl |
| 183–184 | 183–184 | Vollständiger VO40-Fehlercode | 32-Bit-Ganzzahl |
| 185–186 | 185–186 | Vollständiger VO41-Fehlercode | 32-Bit-Ganzzahl |
| 187–188 | 187–188 | Vollständiger VO42-Fehlercode | 32-Bit-Ganzzahl |
| 189–190 | 189–190 | Vollständiger VO43-Fehlercode | 32-Bit-Ganzzahl |
| 191–192 | 191–192 | Vollständiger VO44-Fehlercode | 32-Bit-Ganzzahl |
| 193–194 | 193–194 | Vollständiger VO45-Fehlercode | 32-Bit-Ganzzahl |
| 195–196 | 195–196 | Vollständiger VO46-Fehlercode | 32-Bit-Ganzzahl |
| 197–198 | 197–198 | Vollständiger VO47-Fehlercode | 32-Bit-Ganzzahl |
| 199–200 | 199–200 | Vollständiger VO48-Fehlercode | 32-Bit-Ganzzahl |
| 201–202 | 201–202 | Vollständiger VO49-Fehlercode | 32-Bit-Ganzzahl |
| 203–204 | 203–204 | Vollständiger VO50-Fehlercode | 32-Bit-Ganzzahl |
| 205–206 | 205–206 | Vollständiger VO51-Fehlercode | 32-Bit-Ganzzahl |
| 207–208 | 207–208 | Vollständiger VO52-Fehlercode | 32-Bit-Ganzzahl |
| 209–210 | 209–210 | Vollständiger VO53-Fehlercode | 32-Bit-Ganzzahl |
| 211–212 | 211–212 | Vollständiger VO54-Fehlercode | 32-Bit-Ganzzahl |
| 213–214 | 213–214 | Vollständiger VO55-Fehlercode | 32-Bit-Ganzzahl |
| 215–216 | 215–216 | Vollständiger VO56-Fehlercode | 32-Bit-Ganzzahl |
| 217–218 | 217–218 | Vollständiger VO57-Fehlercode | 32-Bit-Ganzzahl |
| 219–220 | 219–220 | Vollständiger VO58-Fehlercode | 32-Bit-Ganzzahl |
| 221–222 | 221–222 | Vollständiger VO59-Fehlercode | 32-Bit-Ganzzahl |
| 223–224 | 223–224 | Vollständiger VO60-Fehlercode | 32-Bit-Ganzzahl |
| 225–226 | 225–226 | Vollständiger VO61-Fehlercode | 32-Bit-Ganzzahl |
| 227–228 | 227–228 | Vollständiger VO62-Fehlercode | 32-Bit-Ganzzahl |
| 229–230 | 229–230 | Vollständiger VO63-Fehlercode | 32-Bit-Ganzzahl |
| 231–232 | 231–232 | Vollständiger VO64-Fehlercode | 32-Bit-Ganzzahl |
| 233–234 | 233–234 | Fehler Nr. 1 Zeitstempel | 32-Bit-Ganzzahl |
| 235–242 | 235–242 | Fehler Nr. 1 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 243 | 243 | Fehler Nr. 1 Fehlercode | 16-Bit-Ganzzahl |
| 244 | 244 | Fehler Nr. 1 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 245 | 245 | Fehler Nr. 1 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 246–247 | 246–247 | *reserviert* | 16-Bit-Ganzzahl |
| 248–249 | 248–249 | Fehler Nr. 2 Zeitstempel | 32-Bit-Ganzzahl |
| 250–257 | 250–257 | Fehler Nr. 2 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 258 | 258 | Fehler Nr. 2 Fehlercode | 16-Bit-Ganzzahl |
| 259 | 259 | Fehler Nr. 2 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 260 | 260 | Fehler Nr. 2 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 261–262 | 261–262 | *reserviert* | 16-Bit-Ganzzahl |
| 263–264 | 263–264 | Fehler Nr. 3 Zeitstempel | 32-Bit-Ganzzahl |

| Eingangs-reg. Nr. | Haltereg. Nr. | WORTNAME | DATENTYP |
|---|---|---|---|
| 265–272 | 265–272 | Fehler Nr. 3 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 273 | 273 | Fehler Nr. 3 Fehlercode | 16-Bit-Ganzzahl |
| 274 | 274 | Fehler Nr. 3 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 275 | 275 | Fehler Nr. 3 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 276–277 | 276–277 | *reserviert* | 16-Bit-Ganzzahl |
| 278–279 | 278–279 | Fehler Nr. 4 Zeitstempel | 32-Bit-Ganzzahl |
| 280–287 | 280–287 | Fehler Nr. 4 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 288 | 288 | Fehler Nr. 4 Fehlercode | 16-Bit-Ganzzahl |
| 289 | 289 | Fehler Nr. 4 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 290 | 290 | Fehler Nr. 4 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 291–292 | 291–292 | *reserviert* | 16-Bit-Ganzzahl |
| 293–294 | 293–294 | Fehler Nr. 5 Zeitstempel | 32-Bit-Ganzzahl |
| 295–302 | 295–302 | Fehler Nr. 5 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 303 | 303 | Fehler Nr. 5 Fehlercode | 16-Bit-Ganzzahl |
| 304 | 304 | Fehler Nr. 5 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 305 | 305 | Fehler Nr. 5 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 306–307 | 306–307 | *reserviert* | 16-Bit-Ganzzahl |
| 308–309 | 308–309 | Fehler Nr. 6 Zeitstempel | 32-Bit-Ganzzahl |
| 310–317 | 310–317 | Fehler Nr. 6 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 318 | 318 | Fehler Nr. 6 Fehlercode | 16-Bit-Ganzzahl |
| 319 | 319 | Fehler Nr. 6 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 320 | 320 | Fehler Nr. 6 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 321–322 | 321–322 | *reserviert* | 16-Bit-Ganzzahl |
| 323–324 | 323–324 | Fehler Nr. 7 Zeitstempel | 32-Bit-Ganzzahl |
| 325–332 | 325–332 | Fehler Nr. 7 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 333 | 333 | Fehler Nr. 7 Fehlercode | 16-Bit-Ganzzahl |
| 334 | 334 | Fehler Nr. 7 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 335 | 335 | Fehler Nr. 7 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 336–337 | 336–337 | *reserviert* | 16-Bit-Ganzzahl |
| 338–339 | 338–339 | Fehler Nr. 8 Zeitstempel | 32-Bit-Ganzzahl |
| 340–347 | 340–347 | Fehler Nr. 8 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 348 | 348 | Fehler Nr. 8 Fehlercode | 16-Bit-Ganzzahl |
| 349 | 349 | Fehler Nr. 8 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 350 | 350 | Fehler Nr. 8 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 351–352 | 351–352 | *reserviert* | 16-Bit-Ganzzahl |
| 353–354 | 353–354 | Fehler Nr. 9 Zeitstempel | 32-Bit-Ganzzahl |
| 355–362 | 355–362 | Fehler Nr. 9 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 363 | 363 | Fehler Nr. 9 Fehlercode | 16-Bit-Ganzzahl |
| 364 | 364 | Fehler Nr. 9 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 365 | 365 | Fehler Nr. 9 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 366–367 | 366–367 | *reserviert* | 16-Bit-Ganzzahl |
| 368–369 | 368–369 | Fehler Nr. 10 Zeitstempel | 32-Bit-Ganzzahl |

| Eingangs-reg. Nr. | Haltereg. Nr. | WORTNAME | DATENTYP |
|---|---|---|---|
| 370–377 | 370–377 | Fehler Nr. 10 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 378 | 378 | Fehler Nr. 10 Fehlercode | 16-Bit-Ganzzahl |
| 379 | 379 | Fehler Nr. 10 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 380 | 380 | Fehler Nr. 10 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 381–382 | 381–382 | *reserviert* | 16-Bit-Ganzzahl |
| 383–384 | 383–384 | Sekunden seit Systemstart | 32-Bit-Ganzzahl |
| 385 | 385 | Betriebsart | 16-Bit-Ganzzahl |
| 386–395 | 386–395 | ConfigName | Doppelwortlänge + 16-ASCII-Zeichen |
| 396–397 | 396–397 | Konfig. CRC | 32-Bit-Ganzzahl |
| 398–900 | 398–900 | *reserviert* | 16-Bit-Ganzzahl |
| 901 | 901 | VO1–VO16 (siehe Flags auf Seite 217) | 16-Bit-Ganzzahl |
| 902 | 902 | VO17–VO32 (siehe Flags auf Seite 217) | 16-Bit-Ganzzahl |
| 903 | 903 | VO33–VO48 (siehe Flags auf Seite 217) | 16-Bit-Ganzzahl |
| 904 | 904 | VO49–VO64 (siehe Flags auf Seite 217) | 16-Bit-Ganzzahl |
| 905 | 905 | VO65–VO80 (siehe Erweiterte Flags auf Seite 218) | 16-Bit-Ganzzahl |
| 906 | 906 | VO81–VO96 (siehe Erweiterte Flags auf Seite 218) | 16-Bit-Ganzzahl |
| 907 | 907 | VO97–VO112 (siehe Erweiterte Flags auf Seite 218) | 16-Bit-Ganzzahl |
| 908 | 908 | VO113–VO128 (siehe Erweiterte Flags auf Seite 218) | 16-Bit-Ganzzahl |
| 909 | 909 | VO129–VO144 (siehe Erweiterte Flags auf Seite 218) | 16-Bit-Ganzzahl |
| 910 | 910 | VO145–VO160 (siehe Erweiterte Flags auf Seite 218) | 16-Bit-Ganzzahl |
| 911 | 911 | VO161–VO176 (siehe Erweiterte Flags auf Seite 218) | 16-Bit-Ganzzahl |
| 912 | 912 | VO177–VO192 (siehe Erweiterte Flags auf Seite 218) | 16-Bit-Ganzzahl |
| 913 | 913 | VO193–VO208 (siehe Erweiterte Flags auf Seite 218) | 16-Bit-Ganzzahl |
| 914 | 914 | VO209–VO224 (siehe Erweiterte Flags auf Seite 218) | 16-Bit-Ganzzahl |
| 915 | 915 | VO225–VO240 (siehe Erweiterte Flags auf Seite 218) | 16-Bit-Ganzzahl |
| 916 | 916 | VO241–VO256 (siehe Erweiterte Flags auf Seite 218) | 16-Bit-Ganzzahl |
| 917 | 917 | Fehlerbits für VO1–VO16 (siehe Flags auf Seite 217) | 16-Bit-Ganzzahl |
| 918 | 918 | Fehlerbits für VO17–VO32 (siehe Flags auf Seite 217) | 16-Bit-Ganzzahl |
| 919 | 919 | Fehlerbits für VO33–VO48 (siehe Flags auf Seite 217) | 16-Bit-Ganzzahl |
| 920 | 920 | Fehlerbits für VO49–VO64 (siehe Flags auf Seite 217) | 16-Bit-Ganzzahl |
| 921 | 921 | Fehlerbits für VO65–VO80 (siehe Erweiterte Flags auf Seite 218) | 16-Bit-Ganzzahl |

| Eingangs-reg. Nr. | Haltereg. Nr. | WORTNAME | DATENTYP |
|---|---|---|---|
| 922 | 922 | Fehlerbits für VO81–VO96 (siehe Erweiterte Flags auf Seite 218) | 16-Bit-Ganzzahl |
| 923 | 923 | Fehlerbits für VO97–VO112 (siehe Erweiterte Flags auf Seite 218) | 16-Bit-Ganzzahl |
| 924 | 924 | Fehlerbits für VO113–VO128 (siehe Erweiterte Flags auf Seite 218) | 16-Bit-Ganzzahl |
| 925 | 925 | Fehlerbits für VO129–VO144 (siehe Erweiterte Flags auf Seite 218) | 16-Bit-Ganzzahl |
| 926 | 926 | Fehlerbits für VO145–VO160 (siehe Erweiterte Flags auf Seite 218) | 16-Bit-Ganzzahl |
| 926 | 926 | Fehlerbits für VO161–VO176 (siehe Erweiterte Flags auf Seite 218) | 16-Bit-Ganzzahl |
| 928 | 928 | Fehlerbits für VO177–VO192 (siehe Erweiterte Flags auf Seite 218) | 16-Bit-Ganzzahl |
| 929 | 929 | Fehlerbits für VO193–VO208 (siehe Erweiterte Flags auf Seite 218) | 16-Bit-Ganzzahl |
| 930 | 930 | Fehlerbits für VO209–VO224 (siehe Erweiterte Flags auf Seite 218) | 16-Bit-Ganzzahl |
| 931 | 931 | Fehlerbits für VO225–VO240 (siehe Erweiterte Flags auf Seite 218) | 16-Bit-Ganzzahl |
| 932 | 932 | Fehlerbits für VO241–VO256 (siehe Erweiterte Flags auf Seite 218) | 16-Bit-Ganzzahl |
| 933–934 | 933–934 | RCD-Bits Feedback (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 57) | 32-Bit-Ganzzahl |
| 935 | 935 | RCD-Aktivierung Feedback (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 57) | 16-Bit-Ganzzahl |
| 936 | 936 | VO1-Fehlerindex | 16-Bit-Ganzzahl |
| 937 | 937 | VO2-Fehlerindex | 16-Bit-Ganzzahl |
| 938 | 938 | VO3-Fehlerindex | 16-Bit-Ganzzahl |
| … | … | … | … |
| 1190 | 1190 | VO256-Fehlerindex | 16-Bit-Ganzzahl |
| 1191–1192 | 1191–1192 | Vollständiger VO1-Fehlercode | 32-Bit-Ganzzahl |
| 1193–1194 | 1193–1194 | Vollständiger VO2-Fehlercode | 32-Bit-Ganzzahl |
| 1195–1196 | 1195–1196 | Vollständiger VO3-Fehlercode | 32-Bit-Ganzzahl |
| 1197–1198 | 1197–1198 | Vollständiger VO4-Fehlercode | 32-Bit-Ganzzahl |
| … | … | … | … |
| 1702–1703 | 1702–1703 | Vollständiger VO256-Fehlercode | 32-Bit-Ganzzahl |
| 1704–1705 | 1704–1705 | ISD-Systemstatus – Reihe 1 Geräteanzahl | 32-Bit-Ganzzahl |
| 1706–1707 | 1706–1707 | ISD-Systemstatus – Reihe 2 Geräteanzahl | 32-Bit-Ganzzahl |
| 1708–1709 | 1708–1709 | ISD-Systemstatus – Reihe 1 Gerätestatus Ein/Aus (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 1710–1711 | 1710–1711 | ISD-Systemstatus – Reihe 2 Gerätestatus Ein/Aus (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 1712–1713 | 1712–1713 | ISD-Systemstatus – Reihe 1 Fehlerstatus (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 1714–1715 | 1714–1715 | ISD-Systemstatus – Reihe 2 Fehlerstatus (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |

| Eingangs-reg. Nr. | Haltereg. Nr. | WORTNAME | DATENTYP |
|---|---|---|---|
| 1716–1717 | 1716–1717 | ISD-Systemstatus – Reihe 1 marginaler Status (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 1718–1719 | 1718–1719 | ISD-Systemstatus – Reihe 2 marginaler Status (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 1720–1721 | 1720–1721 | ISD-Systemstatus – Reihe 1 Alarmstatus (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 1722–1723 | 1722–1723 | ISD-Systemstatus – Reihe 2 Alarmstatus (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 1724–1725 | 1724–1725 | ISD-Systemstatus – Reihe 1 Reset-Status (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 1726–1727 | 1726–1727 | ISD-Systemstatus – Reihe 2 Reset-Status (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 1728–1729 | 1728–1729 | ISD-Systemstatus – Reihe 1 Auslöser erkannt (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 1730–1731 | 1730–1731 | ISD-Systemstatus – Reihe 2 Auslöser erkannt (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 1732–1733 | 1732–1733 | ISD-Systemstatus – Reihe 1 Systemstatus (siehe ISD-Reihe Systemstatus auf Seite 47) | 32-Bit-Ganzzahl |
| 1734–1735 | 1734–1735 | ISD-Systemstatus – Reihe 2 Systemstatus (siehe ISD-Reihe Systemstatus auf Seite 47) | 32-Bit-Ganzzahl |
| 1736–1768 | 1736–1768 | *reserviert* | 16-Bit-Ganzzahl |
| 1769 | 1769 | ISD-Leseanforderung Bestätigung (siehe Leistungs- und Statusinformationen zu einem einzelnen Gerät über ISD anfordern auf Seite 47) | 16-Bit-Ganzzahl |
| 1770 | 1770 | Von ISD-Reihe angeforderte Bestätigung (siehe Leistungs- und Statusinformationen zu einem einzelnen Gerät über ISD anfordern auf Seite 47) | 16-Bit-Ganzzahl |
| 1771 | 1771 | Von ISD-Gerät angeforderte Bestätigung (siehe Leistungs- und Statusinformationen zu einem einzelnen Gerät über ISD anfordern auf Seite 47) | 16-Bit-Ganzzahl |
| 1772–1780 | 1772–1780 | Spezifische Daten einzelner ISD-Geräte [31] (siehe Detaillierte Beschreibung spezifischer Daten einzelner ISD-Geräte auf Seite 215) | 16-Bit-Ganzzahl |
| | 1781 | ISD-Leseanforderung (siehe Leistungs- und Statusinformationen zu einem einzelnen Gerät über ISD anfordern auf Seite 47) | 16-Bit-Ganzzahl |
| | 1782 | ISD-Reihe angefordert (siehe Leistungs- und Statusinformationen zu einem einzelnen Gerät über ISD anfordern auf Seite 47) | 16-Bit-Ganzzahl |
| | 1783 | ISD-Gerät angefordert (siehe Leistungs- und Statusinformationen zu einem einzelnen Gerät über ISD anfordern auf Seite 47) | 16-Bit-Ganzzahl |

## Detaillierte Beschreibung spezifischer Daten einzelner ISD-Geräte

Die folgende Tabelle beschreibt die Dateneingabe- und Datenhalteregister 1772–1780.

*Tabelle 27. Detaillierte Beschreibung spezifischer Daten einzelner ISD-Geräte*

| Eingangs-REG Nr. | Halte-REG Nr. | Informationen | Datengröße |
|---|---|---|---|
| 1772.0 | 1772.0 | Sicherheitseingangsfehler | 1 Bit |

[31] Informationen zur Umrechnung von Innentemperatur, Auslöserabstand und Betriebsspannung finden Sie unter ISD: Informationen zur Umwandlung von Temperatur, Spannung und Abstand auf Seite 248.

| Eingangs-REG Nr. | Halte-REG Nr. | Informationen | Datengröße |
|---|---|---|---|
| 1772.1 | 1772.1 | *reserviert* | 1 Bit |
| 1772.2 | 1772.2 | Sensor nicht gekoppelt | 1-Bit |
| 1772.3 | 1772.3 | ISD-Datenfehler | 1-Bit |
| 1772.4 | 1772.4 | Falscher Auslöser-/Tasterstatus/Eingangsstatus | 1-Bit |
| 1772.5 | 1772.5 | Marginaler Bereich/Tasterstatus/Eingangsstatus | 1-Bit |
| 1772.6 | 1772.6 | Auslöser erkannt | 1-Bit |
| 1772.7 | 1772.7 | Ausgangsfehler | 1-Bit |
| 1772.8 | 1772.8 | Eingang 2 | 1-Bit |
| 1772.9 | 1772.9 | Eingang 1 | 1-Bit |
| 1772.10 | 1772.10 | Lokaler Reset erwartet | 1-Bit |
| 1772.11 | 1772.11 | Warnung Betriebsspannung | 1-Bit |
| 1772.12 | 1772.12 | Fehler bei Betriebsspannung | 1-Bit |
| 1772.13 | 1772.13 | Ausgang 2 | 1-Bit |
| 1772.14 | 1772.14 | Ausgang 1 | 1-Bit |
| 1772.15 | 1772.15 | Aus- und Wiedereinschalten der Stromversorgung erforderlich | 1-Bit |
| 1773.0 | 1773.0 | Fehlertolerante Ausgänge | 1-Bit |
| 1773.1 | 1773.1 | Einheit für lokalen Reset | 1-Bit |
| 1773.2 | 1773.2 | Kaskadierbar | 1-Bit |
| 1773.3 | 1773.3 | Hohe Codierstufe | 1-Bit |
| 1773.4 bis 1773.7 | 1773.4 bis 1773.7 | Verbleibende Einlerninstanzen | 4-Bit |
| 1773.8 bis 1773.12 | 1773.8 bis 1773.12 | Geräte-ID | 5-Bit |
| 1773.13 bis 1774.2 | 1773.13 bis 1774.2 | Anzahl Bereichswarnungen | 6-Bit |
| 1774.3 bis 1774.7 | 1774.3 bis 1774.7 | Ausschaltzeit für Ausgang | 5-Bit |
| 1774.8 bis 1774.15 | 1774.8 bis 1774.15 | Anzahl der Spannungsfehler | 8-Bit |
| 1775.0 bis 1775.7 | 1775.0 bis 1775.7 | Innentemperatur [32] | 8-Bit |
| 1775.8 bis 1775.15 | 1775.8 bis 1775.15 | Auslöserabstand [32] | 8-Bit |
| 1776.0 bis 1776.7 | 1776.0 bis 1776.7 | Versorgungsspannung [32] | 8-Bit |
| 1776.8 bis 1776.11 | 1776.8 bis 1776.11 | Erwarteter Firmenname | 4-Bit |
| 1776.12 bis 1776.15 | 1776.12 bis 1776.15 | Empfangener Firmenname | 4-Bit |
| 1777 | 1777 | Erwarteter Code | 16-Bit |
| 1778 | 1778 | Empfangener Code | 16-Bit |
| 1779 | 1779 | Interner Fehler A | 16-Bit |
| 1780 | 1780 | Interner Fehler B | 16-Bit |

[32] Informationen zur Umrechnung von Innentemperatur, Auslöserabstand und Betriebsspannung finden Sie unter ISD: Informationen zur Umwandlung von Temperatur, Spannung und Abstand auf Seite 248.

**Anmerkung:** Siehe Spezifische Daten einzelner ISD-Geräte auf Seite 48 für weitere Informationen über die Struktur der ISD-Daten.

## 12.5.1 Flags

Die unten definierten Register 1 bis 8 werden in der Registerzuordnung als die ersten 8 Wörter angezeigt.

Dies stellt die ersten 64 virtuellen Ausgänge und die zugehörigen Fehlerflags dar. Die Informationen in diesen Registern können als Eingangsregister (30000) mit dem Modbus-Funktionscode 04 (Eingangsregister lesen) gelesen werden. Dieselben Werte können auch als Halteregister (40000) mit dem Modbus-Funktionscode 03 (Halteregister lesen) gelesen werden.

*Tabelle 28. Virtueller Ausgang 1–16*

Eingangsregister 30001 oder Halteregister 40001 der SPS, auch Eingänge 10001–16 oder Spulen 00001–16

| Bit 15 | Bit 14 | Bit 13 | Bit 12 | Bit 11 | Bit 10 | Bit 9 | Bit 8 | Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 | Bit 0 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| VO16 | VO15 | VO14 | VO13 | VO12 | VO11 | VO10 | VO9 | VO8 | VO7 | VO6 | VO5 | VO4 | VO3 | VO2 | VO1 |

*Tabelle 29. Virtueller Ausgang 17–32*

Eingangsregister 30002 oder Halteregister 40002 der SPS, auch Eingänge 10017–32 oder Spulen 00017–32

| Bit 15 | Bit 14 | Bit 13 | Bit 12 | Bit 11 | Bit 10 | Bit 9 | Bit 8 | Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 | Bit 0 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| VO32 | VO31 | VO30 | VO29 | VO28 | VO27 | VO26 | VO25 | VO24 | VO23 | VO22 | VO21 | VO20 | VO19 | VO18 | VO17 |

*Tabelle 30. Virtueller Ausgang 33–48*

Eingangsregister 30003 oder Halteregister 40003 der SPS, auch Eingänge 10033–48 oder Spulen 00033–48

| Bit 15 | Bit 14 | Bit 13 | Bit 12 | Bit 11 | Bit 10 | Bit 9 | Bit 8 | Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 | Bit 0 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| VO48 | VO47 | VO46 | VO45 | VO44 | VO43 | VO42 | VO41 | VO40 | VO39 | VO38 | VO37 | VO36 | VO35 | VO34 | VO33 |

*Tabelle 31. Virtueller Ausgang 49–64*

Eingangsregister 30004 oder Halteregister 40004 der SPS, auch Eingänge 10049–64 oder Spulen 00049–64

| Bit 15 | Bit 14 | Bit 13 | Bit 12 | Bit 11 | Bit 10 | Bit 9 | Bit 8 | Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 | Bit 0 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| VO64 | VO63 | VO62 | VO61 | VO60 | VO59 | VO58 | VO57 | VO56 | VO55 | VO54 | VO53 | VO52 | VO51 | VO50 | VO49 |

*Tabelle 32. Virtueller Ausgangsfehler 1–16*

Eingangsregister 30005 oder Halteregister 40005 der SPS, auch Eingänge 10033–48 oder Spulen 00033–48

| Bit 15 | Bit 14 | Bit 13 | Bit 12 | Bit 11 | Bit 10 | Bit 9 | Bit 8 | Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 | Bit 0 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| VO16-Fehler | VO15-Fehler | VO14-Fehler | VO13-Fehler | VO12-Fehler | VO11-Fehler | VO10-Fehler | VO9-Fehler | VO8-Fehler | VO7-Fehler | VO6-Fehler | VO5-Fehler | VO4-Fehler | VO3-Fehler | VO2-Fehler | VO1-Fehler |

*Tabelle 33. Virtueller Ausgangsfehler 17–32*

Eingangsregister 30006 oder Halteregister 40006 der SPS, auch Eingänge 10049–64 oder Spulen 00049–64

| Bit 15 | Bit 14 | Bit 13 | Bit 12 | Bit 11 | Bit 10 | Bit 9 | Bit 8 | Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 | Bit 0 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| VO32-Fehler | VO31-Fehler | VO30-Fehler | VO29-Fehler | VO28-Fehler | VO27-Fehler | VO26-Fehler | VO25-Fehler | VO24-Fehler | VO23-Fehler | VO22-Fehler | VO21-Fehler | VO20-Fehler | VO19-Fehler | VO18-Fehler | VO17-Fehler |

*Tabelle 34. Virtueller Ausgangsfehler 33–48*

Eingangsregister 30007 oder Halteregister 40007 der SPS, auch Eingänge 10033–48 oder Spulen 00033–48

| Bit 15 | Bit 14 | Bit 13 | Bit 12 | Bit 11 | Bit 10 | Bit 9 | Bit 8 | Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 | Bit 0 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| VO48-Fehler | VO47-Fehler | VO46-Fehler | VO45-Fehler | VO44-Fehler | VO43-Fehler | VO42-Fehler | VO41-Fehler | VO40-Fehler | VO39-Fehler | VO38-Fehler | VO37-Fehler | VO36-Fehler | VO35-Fehler | VO34-Fehler | VO33-Fehler |

*Tabelle 35. Virtueller Ausgangsfehler 49–64*

Eingangsregister 30008 oder Halteregister 40008 der SPS, auch Eingänge 10049–64 oder Spulen 00049–64

| Bit 15 | Bit 14 | Bit 13 | Bit 12 | Bit 11 | Bit 10 | Bit 9 | Bit 8 | Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 | Bit 0 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| VO64-Fehler | VO63-Fehler | VO62-Fehler | VO61-Fehler | VO60-Fehler | VO59-Fehler | VO58-Fehler | VO57-Fehler | VO56-Fehler | VO55-Fehler | VO54-Fehler | VO53-Fehler | VO52-Fehler | VO51-Fehler | VO50-Fehler | VO49-Fehler |

### 12.5.2 Erweiterte Flags

Auf alle 256 virtuellen Ausgänge kann ähnlich wie unter Flags auf Seite 217 abgebildet zugegriffen werden.

Die Eingänge 11001 bis 11256 stellen alle 256 möglichen virtuellen Ausgänge dar. Diese virtuellen Ausgänge können auch als Eingangsregister 901–916 oder Halteregister 901–916 gelesen werden.

Die Eingänge 12001 bis 12256 sind alle 256 virtuelle Ausgangsfehler. Diese virtuellen Ausgangsfehler können auch als Eingangsregister 917–932 oder Halteregister 917–932 gelesen werden.

## 12.6 SPS5, SLC500 und MicroLogix (PCCC)

Die SPS5-, SLC 500- und MicroLogix-Geräteserie von Allen-Bradley verwendet das Kommunicationprotokoll PCCC.

PCCC ist auch als EtherNet/IP-Transportklasse 3 bekannt und verwendet explizite Lese- und Schreibnachrichtenbefehle bzw. EIP-Messaging. Die Befehle werden im Kontaktplanprogramm als Schnittstelle zum Sicherheitskontroller gespeichert.

Diese SPS unterstützen keine zyklische EtherNet/IP-E/A-Datenübertragung (in diesem Handbuch als EtherNet/IP bezeichnet). Die von diesen SPS verwendete Programmiersoftware ist RSLogix 5 (SPS5) oder RSLogix 500 (SLC500- und MicroLogix-Serie).

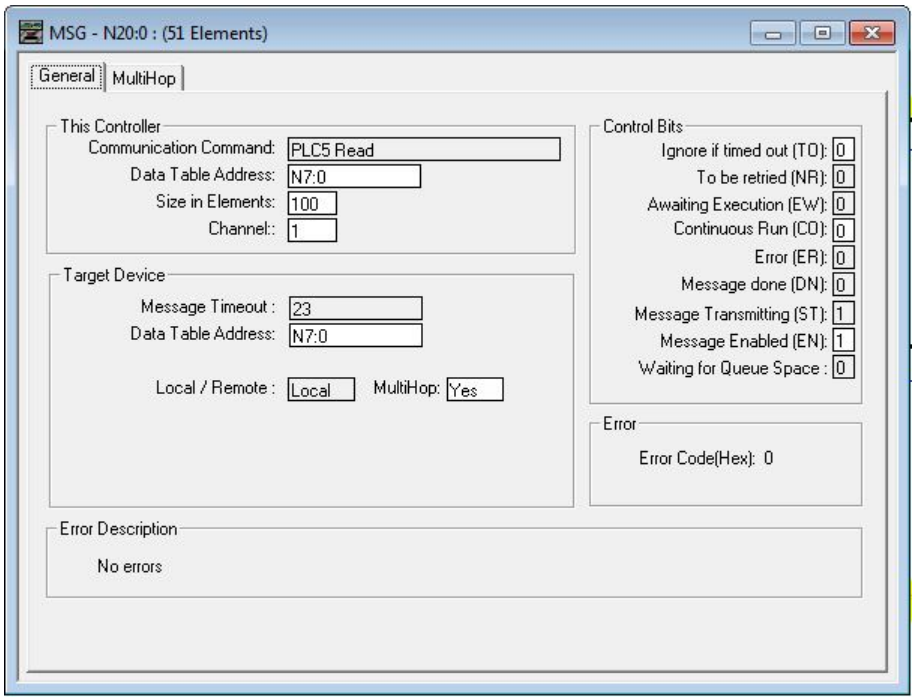
Der Sicherheitskontroller unterstützt diese SPS durch ein Eingangsregister-Array Der Begriff *Eingang* wird hier vom Standpunkt der SPS verwendet.

### 12.6.1 SPS-Konfiguration

Die nachfolgenden Abbildungen zeigen eine typische Konfiguration.

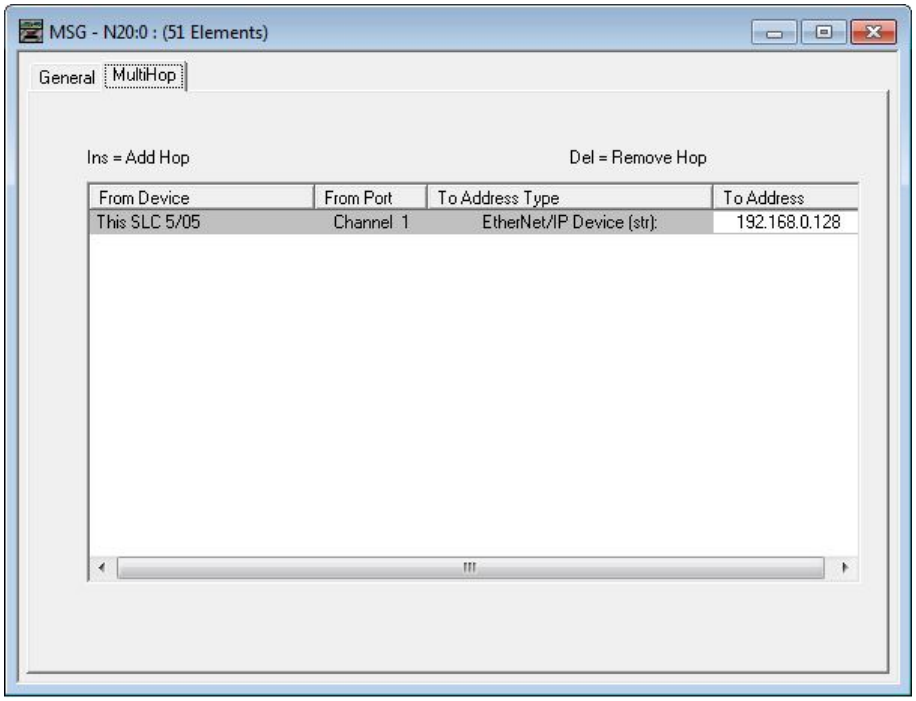
1. Lesen. Nachrichtenbefehl, der aus der N7-Tabelle auf dem Sicherheitskontroller liest.

*Abbildung 226. Fenster **MSG - N20:0 (51 Elemente)** — Registerkarte **Allgemein***



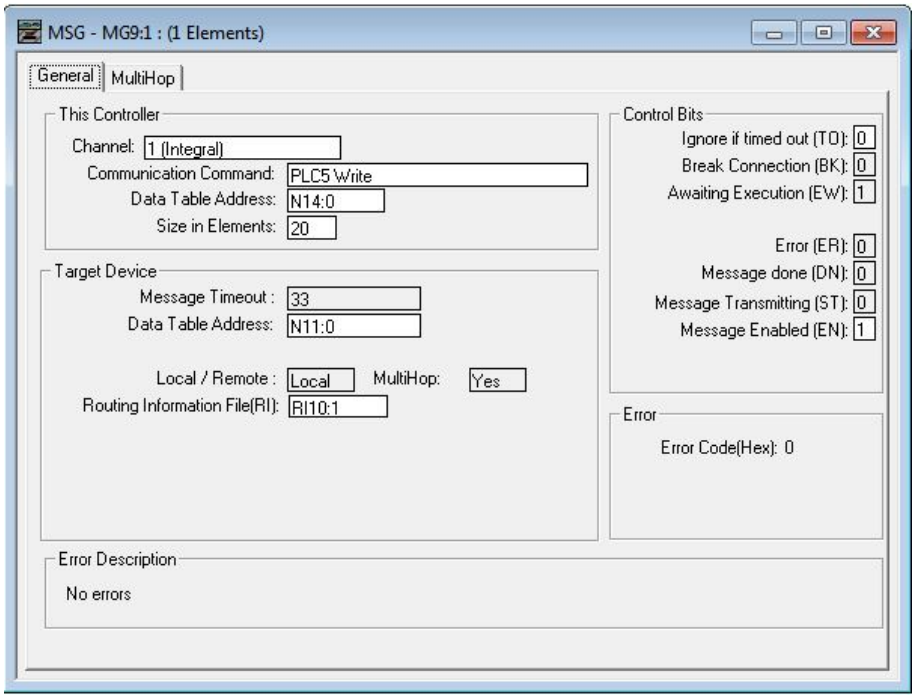

2. Lesen. Die IP-Adresse des Sicherheitskontrollers wird hier eingegeben.

*Abbildung 227. Fenster **MSG - N20:0 (51 Elemente)** — Registerkarte **MultiHop***



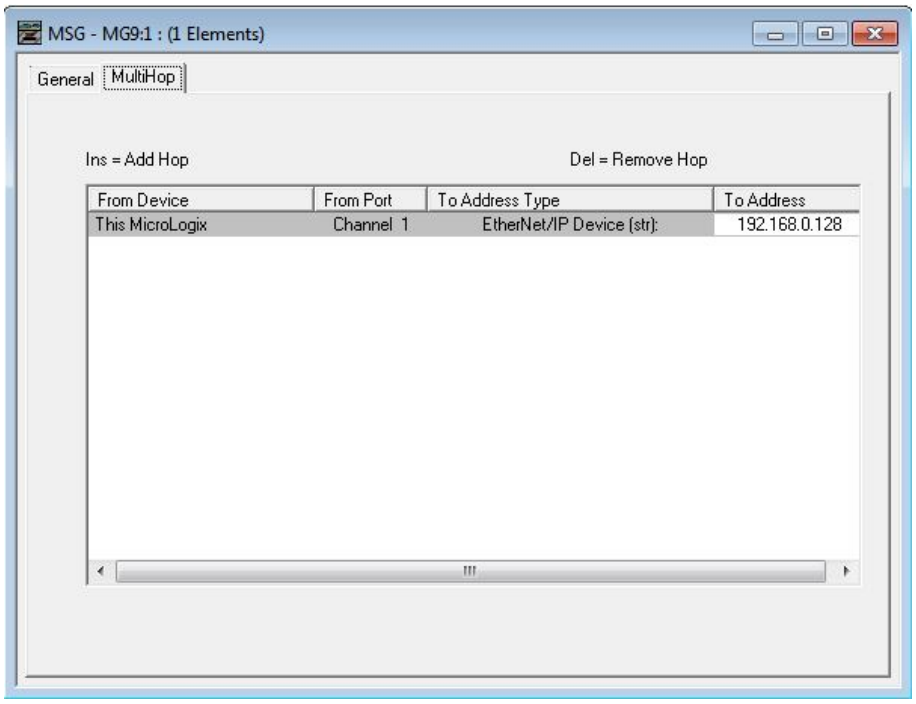

3. Schreiben. Nachrichtenbefehl, der in die N11-Tabelle auf dem Sicherheitskontroller schreibt.

*Abbildung 228. Fenster **MSG - MG9:1 (1 Element)** — Registerkarte **Allgemein***




4. Schreiben. Die IP-Adresse des Sicherheitskontrollers wird hier eingegeben.

*Abbildung 229. Fenster **MSG - MG9:1 (1 Element)** — Registerkarte **MultiHop***




## 12.6.2 Ausgänge vom Sicherheitskontroller (Eingänge zur SPS)

Anhand der Ausgangsregister werden Ausgangswerte vom Sicherheitskontroller an die SPS weitergeleitet. MSG(Nachrichten)-Befehle werden zum Lesen (N7) vom Sicherheitskontroller verwendet.

*Tabelle 36. N7 Register*

| Reg. Nr. | WORTNAME | DATENTYP |
|---|---|---|
| 0 | VO1–VO16 (siehe Flags auf Seite 229) | 16-Bit-Ganzzahl |
| 1 | VO17–VO32 (siehe Flags auf Seite 229) | 16-Bit-Ganzzahl |
| 2 | VO33–VO48 (siehe Flags auf Seite 229) | 16-Bit-Ganzzahl |
| 3 | VO49–VO64 (siehe Flags auf Seite 229) | 16-Bit-Ganzzahl |
| 4 | Fehlerbits für VO1–VO16 (siehe Flags auf Seite 229) | 16-Bit-Ganzzahl |
| 5 | Fehlerbits für VO17–VO32 (siehe Flags auf Seite 229) | 16-Bit-Ganzzahl |
| 6 | Fehlerbits für VO33–VO48 (siehe Flags auf Seite 229) | 16-Bit-Ganzzahl |
| 7 | Fehlerbits für VO49–VO64 (siehe Flags auf Seite 229) | 16-Bit-Ganzzahl |
| 8–18 | *reserviert* | 16-Bit-Ganzzahl |
| 19 | Virtuelle Reset-/Abbruchverzögerung (1–16) Feedback [RCD-Feedback Registerbits] (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 57) | 16-Bit-Ganzzahl |
| 20 | *reserviert* | 16-Bit-Ganzzahl |
| 21 | RCD-Auslösecode Feedback [RCD-Aktivierung Feedbackregister] (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 57) | 16-Bit-Ganzzahl |
| 22–39 | *reserviert* | 16-Bit-Ganzzahl |
| 40 | VO1-Fehlerindex | 16-Bit-Ganzzahl |
| 41 | VO2-Fehlerindex | 16-Bit-Ganzzahl |
| 42 | VO3-Fehlerindex | 16-Bit-Ganzzahl |
| 43 | VO4-Fehlerindex | 16-Bit-Ganzzahl |

| Reg. Nr. | WORTNAME | DATENTYP |
|---|---|---|
| 44 | VO5-Fehlerindex | 16-Bit-Ganzzahl |
| 45 | VO6-Fehlerindex | 16-Bit-Ganzzahl |
| 46 | VO7-Fehlerindex | 16-Bit-Ganzzahl |
| 47 | VO8-Fehlerindex | 16-Bit-Ganzzahl |
| 48 | VO9-Fehlerindex | 16-Bit-Ganzzahl |
| 49 | VO10-Fehlerindex | 16-Bit-Ganzzahl |
| 50 | VO11-Fehlerindex | 16-Bit-Ganzzahl |
| 51 | VO12-Fehlerindex | 16-Bit-Ganzzahl |
| 52 | VO13-Fehlerindex | 16-Bit-Ganzzahl |
| 53 | VO14-Fehlerindex | 16-Bit-Ganzzahl |
| 54 | VO15-Fehlerindex | 16-Bit-Ganzzahl |
| 55 | VO16-Fehlerindex | 16-Bit-Ganzzahl |
| 56 | VO17-Fehlerindex | 16-Bit-Ganzzahl |
| 57 | VO18-Fehlerindex | 16-Bit-Ganzzahl |
| 58 | VO19-Fehlerindex | 16-Bit-Ganzzahl |
| 59 | VO20-Fehlerindex | 16-Bit-Ganzzahl |
| 60 | VO21-Fehlerindex | 16-Bit-Ganzzahl |
| 61 | VO22-Fehlerindex | 16-Bit-Ganzzahl |
| 62 | VO23-Fehlerindex | 16-Bit-Ganzzahl |
| 63 | VO24-Fehlerindex | 16-Bit-Ganzzahl |
| 64 | VO25-Fehlerindex | 16-Bit-Ganzzahl |
| 65 | VO26-Fehlerindex | 16-Bit-Ganzzahl |
| 66 | VO27-Fehlerindex | 16-Bit-Ganzzahl |
| 67 | VO28-Fehlerindex | 16-Bit-Ganzzahl |
| 68 | VO29-Fehlerindex | 16-Bit-Ganzzahl |
| 69 | VO30-Fehlerindex | 16-Bit-Ganzzahl |
| 70 | VO31-Fehlerindex | 16-Bit-Ganzzahl |
| 71 | VO32-Fehlerindex | 16-Bit-Ganzzahl |
| 72 | VO33-Fehlerindex | 16-Bit-Ganzzahl |
| 73 | VO34-Fehlerindex | 16-Bit-Ganzzahl |
| 74 | VO35-Fehlerindex | 16-Bit-Ganzzahl |
| 75 | VO36-Fehlerindex | 16-Bit-Ganzzahl |
| 76 | VO37-Fehlerindex | 16-Bit-Ganzzahl |
| 77 | VO38-Fehlerindex | 16-Bit-Ganzzahl |
| 78 | VO39-Fehlerindex | 16-Bit-Ganzzahl |
| 79 | VO40-Fehlerindex | 16-Bit-Ganzzahl |
| 80 | VO41-Fehlerindex | 16-Bit-Ganzzahl |
| 81 | VO42-Fehlerindex | 16-Bit-Ganzzahl |
| 82 | VO43-Fehlerindex | 16-Bit-Ganzzahl |
| 83 | VO44-Fehlerindex | 16-Bit-Ganzzahl |
| 84 | VO45-Fehlerindex | 16-Bit-Ganzzahl |
| 85 | VO46-Fehlerindex | 16-Bit-Ganzzahl |
| 86 | VO47-Fehlerindex | 16-Bit-Ganzzahl |

| Reg. Nr. | WORTNAME | DATENTYP |
|---|---|---|
| 87 | VO48-Fehlerindex | 16-Bit-Ganzzahl |
| 88 | VO49-Fehlerindex | 16-Bit-Ganzzahl |
| 89 | VO50-Fehlerindex | 16-Bit-Ganzzahl |
| 90 | VO51-Fehlerindex | 16-Bit-Ganzzahl |
| 91 | VO52-Fehlerindex | 16-Bit-Ganzzahl |
| 92 | VO53-Fehlerindex | 16-Bit-Ganzzahl |
| 93 | VO54-Fehlerindex | 16-Bit-Ganzzahl |
| 94 | VO55-Fehlerindex | 16-Bit-Ganzzahl |
| 95 | VO56-Fehlerindex | 16-Bit-Ganzzahl |
| 96 | VO57-Fehlerindex | 16-Bit-Ganzzahl |
| 97 | VO58-Fehlerindex | 16-Bit-Ganzzahl |
| 98 | VO59-Fehlerindex | 16-Bit-Ganzzahl |
| 99 | VO60-Fehlerindex | 16-Bit-Ganzzahl |
| 100 | VO61-Fehlerindex | 16-Bit-Ganzzahl |
| 101 | VO62-Fehlerindex | 16-Bit-Ganzzahl |
| 102 | VO63-Fehlerindex | 16-Bit-Ganzzahl |
| 103 | VO64-Fehlerindex | 16-Bit-Ganzzahl |
| 104–105 | Vollständiger VO1-Fehlercode | 32-Bit-Ganzzahl |
| 106–107 | Vollständiger VO2-Fehlercode | 32-Bit-Ganzzahl |
| 108–109 | Vollständiger VO3-Fehlercode | 32-Bit-Ganzzahl |
| 110–111 | Vollständiger VO4-Fehlercode | 32-Bit-Ganzzahl |
| 112–113 | Vollständiger VO5-Fehlercode | 32-Bit-Ganzzahl |
| 114–115 | Vollständiger VO6-Fehlercode | 32-Bit-Ganzzahl |
| 116–117 | Vollständiger VO7-Fehlercode | 32-Bit-Ganzzahl |
| 118–119 | Vollständiger VO8-Fehlercode | 32-Bit-Ganzzahl |
| 120–121 | Vollständiger VO9-Fehlercode | 32-Bit-Ganzzahl |
| 122–123 | Vollständiger VO10-Fehlercode | 32-Bit-Ganzzahl |
| 124–125 | Vollständiger VO11-Fehlercode | 32-Bit-Ganzzahl |
| 126–127 | Vollständiger VO12-Fehlercode | 32-Bit-Ganzzahl |
| 128–129 | Vollständiger VO13-Fehlercode | 32-Bit-Ganzzahl |
| 130–131 | Vollständiger VO14-Fehlercode | 32-Bit-Ganzzahl |
| 132–133 | Vollständiger VO15-Fehlercode | 32-Bit-Ganzzahl |
| 134–135 | Vollständiger VO16-Fehlercode | 32-Bit-Ganzzahl |
| 136–137 | Vollständiger VO17-Fehlercode | 32-Bit-Ganzzahl |
| 138–139 | Vollständiger VO18-Fehlercode | 32-Bit-Ganzzahl |
| 140–141 | Vollständiger VO19-Fehlercode | 32-Bit-Ganzzahl |
| 142–143 | Vollständiger VO20-Fehlercode | 32-Bit-Ganzzahl |
| 144–145 | Vollständiger VO21-Fehlercode | 32-Bit-Ganzzahl |
| 146–147 | Vollständiger VO22-Fehlercode | 32-Bit-Ganzzahl |
| 148–149 | Vollständiger VO23-Fehlercode | 32-Bit-Ganzzahl |
| 150–151 | Vollständiger VO24-Fehlercode | 32-Bit-Ganzzahl |
| 152–153 | Vollständiger VO25-Fehlercode | 32-Bit-Ganzzahl |
| 154–155 | Vollständiger VO26-Fehlercode | 32-Bit-Ganzzahl |

| Reg. Nr. | WORTNAME | DATENTYP |
|---|---|---|
| 156–157 | Vollständiger VO27-Fehlercode | 32-Bit-Ganzzahl |
| 158–159 | Vollständiger VO28-Fehlercode | 32-Bit-Ganzzahl |
| 160–161 | Vollständiger VO29-Fehlercode | 32-Bit-Ganzzahl |
| 162–163 | Vollständiger VO30-Fehlercode | 32-Bit-Ganzzahl |
| 164–165 | Vollständiger VO31-Fehlercode | 32-Bit-Ganzzahl |
| 166–167 | Vollständiger VO32-Fehlercode | 32-Bit-Ganzzahl |
| 168–169 | Vollständiger VO33-Fehlercode | 32-Bit-Ganzzahl |
| 170–171 | Vollständiger VO34-Fehlercode | 32-Bit-Ganzzahl |
| 172–173 | Vollständiger VO35-Fehlercode | 32-Bit-Ganzzahl |
| 174–175 | Vollständiger VO36-Fehlercode | 32-Bit-Ganzzahl |
| 176–177 | Vollständiger VO37-Fehlercode | 32-Bit-Ganzzahl |
| 178–179 | Vollständiger VO38-Fehlercode | 32-Bit-Ganzzahl |
| 180–181 | Vollständiger VO39-Fehlercode | 32-Bit-Ganzzahl |
| 182–183 | Vollständiger VO40-Fehlercode | 32-Bit-Ganzzahl |
| 184–185 | Vollständiger VO41-Fehlercode | 32-Bit-Ganzzahl |
| 186–187 | Vollständiger VO42-Fehlercode | 32-Bit-Ganzzahl |
| 188–189 | Vollständiger VO43-Fehlercode | 32-Bit-Ganzzahl |
| 190–191 | Vollständiger VO44-Fehlercode | 32-Bit-Ganzzahl |
| 192–193 | Vollständiger VO45-Fehlercode | 32-Bit-Ganzzahl |
| 194–195 | Vollständiger VO46-Fehlercode | 32-Bit-Ganzzahl |
| 196–197 | Vollständiger VO47-Fehlercode | 32-Bit-Ganzzahl |
| 198–199 | Vollständiger VO48-Fehlercode | 32-Bit-Ganzzahl |
| 200–201 | Vollständiger VO49-Fehlercode | 32-Bit-Ganzzahl |
| 202–203 | Vollständiger VO50-Fehlercode | 32-Bit-Ganzzahl |
| 204–205 | Vollständiger VO51-Fehlercode | 32-Bit-Ganzzahl |
| 206–207 | Vollständiger VO52-Fehlercode | 32-Bit-Ganzzahl |
| 208–209 | Vollständiger VO53-Fehlercode | 32-Bit-Ganzzahl |
| 210–211 | Vollständiger VO54-Fehlercode | 32-Bit-Ganzzahl |
| 212–213 | Vollständiger VO55-Fehlercode | 32-Bit-Ganzzahl |
| 214–215 | Vollständiger VO56-Fehlercode | 32-Bit-Ganzzahl |
| 216–217 | Vollständiger VO57-Fehlercode | 32-Bit-Ganzzahl |
| 218–219 | Vollständiger VO58-Fehlercode | 32-Bit-Ganzzahl |
| 220–221 | Vollständiger VO59-Fehlercode | 32-Bit-Ganzzahl |
| 222–223 | Vollständiger VO60-Fehlercode | 32-Bit-Ganzzahl |
| 224–225 | Vollständiger VO61-Fehlercode | 32-Bit-Ganzzahl |
| 226–227 | Vollständiger VO62-Fehlercode | 32-Bit-Ganzzahl |
| 228-229 | Vollständiger VO63-Fehlercode | 32-Bit-Ganzzahl |
| 230–231 | Vollständiger VO64-Fehlercode | 32-Bit-Ganzzahl |
| 232-233 | Fehler Nr. 1 Zeitstempel | 32-Bit-Ganzzahl |
| 234–241 | Fehler Nr. 1 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 242 | Fehler Nr. 1 Fehlercode | 16-Bit-Ganzzahl |
| 243 | Fehler Nr. 1 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 244 | Fehler Nr. 1 Fehlermeldungsindex | 16-Bit-Ganzzahl |

| Reg. Nr. | WORTNAME | DATENTYP |
|---|---|---|
| 245–246 | *reserviert* | 16-Bit-Ganzzahl |
| 247–248 | Fehler Nr. 2 Zeitstempel | 32-Bit-Ganzzahl |
| 249–256 | Fehler Nr. 2 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 257 | Fehler Nr. 2 Fehlercode | 16-Bit-Ganzzahl |
| 258 | Fehler Nr. 2 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 259 | Fehler Nr. 2 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 260–261 | *reserviert* | 16-Bit-Ganzzahl |
| 262–263 | Fehler Nr. 3 Zeitstempel | 32-Bit-Ganzzahl |
| 264–271 | Fehler Nr. 3 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 272 | Fehler Nr. 3 Fehlercode | 16-Bit-Ganzzahl |
| 273 | Fehler Nr. 3 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 274 | Fehler Nr. 3 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 275–276 | *reserviert* | 16-Bit-Ganzzahl |
| 277–278 | Fehler Nr. 4 Zeitstempel | 32-Bit-Ganzzahl |
| 279–286 | Fehler Nr. 4 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 287 | Fehler Nr. 4 Fehlercode | 16-Bit-Ganzzahl |
| 288 | Fehler Nr. 4 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 289 | Fehler Nr. 4 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 290–291 | *reserviert* | 16-Bit-Ganzzahl |
| 292–293 | Fehler Nr. 5 Zeitstempel | 32-Bit-Ganzzahl |
| 294–301 | Fehler Nr. 5 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 302 | Fehler Nr. 5 Fehlercode | 16-Bit-Ganzzahl |
| 303 | Fehler Nr. 5 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 304 | Fehler Nr. 5 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 305–306 | *reserviert* | 16-Bit-Ganzzahl |
| 307–308 | Fehler Nr. 6 Zeitstempel | 32-Bit-Ganzzahl |
| 309–316 | Fehler Nr. 6 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 317 | Fehler Nr. 6 Fehlercode | 16-Bit-Ganzzahl |
| 318 | Fehler Nr. 6 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 319 | Fehler Nr. 6 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 320–321 | *reserviert* | 16-Bit-Ganzzahl |
| 322–323 | Fehler Nr. 7 Zeitstempel | 32-Bit-Ganzzahl |
| 324–331 | Fehler Nr. 7 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 332 | Fehler Nr. 7 Fehlercode | 16-Bit-Ganzzahl |
| 333 | Fehler Nr. 7 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 334 | Fehler Nr. 7 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 335–336 | *reserviert* | 16-Bit-Ganzzahl |
| 337–338 | Fehler Nr. 8 Zeitstempel | 32-Bit-Ganzzahl |
| 339–346 | Fehler Nr. 8 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 347 | Fehler Nr. 8 Fehlercode | 16-Bit-Ganzzahl |
| 348 | Fehler Nr. 8 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 349 | Fehler Nr. 8 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 350–351 | *reserviert* | 16-Bit-Ganzzahl |

| Reg. Nr. | WORTNAME | DATENTYP |
|---|---|---|
| 352–353 | Fehler Nr. 9 Zeitstempel | 32-Bit-Ganzzahl |
| 354–361 | Fehler Nr. 9 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 362 | Fehler Nr. 9 Fehlercode | 16-Bit-Ganzzahl |
| 363 | Fehler Nr. 9 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 364 | Fehler Nr. 9 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 365–366 | reserviert | 16-Bit-Ganzzahl |
| 367–368 | Fehler Nr. 10 Zeitstempel | 32-Bit-Ganzzahl |
| 369–376 | Fehler Nr. 10 E/A- oder Systemname | Doppelwortlänge + 12-ASCII-Zeichen |
| 377 | Fehler Nr. 10 Fehlercode | 16-Bit-Ganzzahl |
| 378 | Fehler Nr. 10 Erweiterter Fehlercode | 16-Bit-Ganzzahl |
| 379 | Fehler Nr. 10 Fehlermeldungsindex | 16-Bit-Ganzzahl |
| 380–381 | *reserviert* | 16-Bit-Ganzzahl |
| 382–383 | Sekunden seit Systemstart | 32-Bit-Ganzzahl |
| 384 | Betriebsart | 16-Bit-Ganzzahl |
| 385–394 | ConfigName | Doppelwortlänge + 16-ASCII-Zeichen |
| 395–396 | Konfig. CRC | 32-Bit-Ganzzahl |
| 397–899 | *reserviert* | 16-Bit-Ganzzahl |
| 900 | VO1–VO16 (siehe Flags auf Seite 229) | 16-Bit-Ganzzahl |
| 901 | VO17–VO32 (siehe Flags auf Seite 229) | 16-Bit-Ganzzahl |
| 902 | VO33–VO48 (siehe Flags auf Seite 229) | 16-Bit-Ganzzahl |
| 903 | VO49–VO64 (siehe Flags auf Seite 229) | 16-Bit-Ganzzahl |
| 904 | VO65–VO80 (siehe Erweiterte Flags auf Seite 230) | 16-Bit-Ganzzahl |
| 905 | VO81–VO96 (siehe Erweiterte Flags auf Seite 230) | 16-Bit-Ganzzahl |
| 906 | VO97–VO112 (siehe Erweiterte Flags auf Seite 230) | 16-Bit-Ganzzahl |
| 907 | VO113–VO128 (siehe Erweiterte Flags auf Seite 230) | 16-Bit-Ganzzahl |
| 908 | VO129–VO144 (siehe Erweiterte Flags auf Seite 230) | 16-Bit-Ganzzahl |
| 909 | VO145–VO160 (siehe Erweiterte Flags auf Seite 230) | 16-Bit-Ganzzahl |
| 910 | VO161–VO176 (siehe Erweiterte Flags auf Seite 230) | 16-Bit-Ganzzahl |
| 911 | VO177–VO192 (siehe Erweiterte Flags auf Seite 230) | 16-Bit-Ganzzahl |
| 912 | VO193–VO208 (siehe Erweiterte Flags auf Seite 230) | 16-Bit-Ganzzahl |
| 913 | VO209–VO224 (siehe Erweiterte Flags auf Seite 230) | 16-Bit-Ganzzahl |
| 914 | VO225–VO240 (siehe Erweiterte Flags auf Seite 230) | 16-Bit-Ganzzahl |
| 915 | VO241–VO256 (siehe Erweiterte Flags auf Seite 230) | 16-Bit-Ganzzahl |
| 916 | Fehlerbits für VO1–VO16 (siehe Flags auf Seite 229) | 16-Bit-Ganzzahl |
| 917 | Fehlerbits für VO17–VO32 (siehe Flags auf Seite 229) | 16-Bit-Ganzzahl |
| 918 | Fehlerbits für VO33–VO48 (siehe Flags auf Seite 229) | 16-Bit-Ganzzahl |
| 919 | Fehlerbits für VO49–VO64 (siehe Flags auf Seite 229) | 16-Bit-Ganzzahl |
| 920 | Fehlerbits für VO65–VO80 (siehe Erweiterte Flags auf Seite 230) | 16-Bit-Ganzzahl |
| 921 | Fehlerbits für VO81–VO96 (siehe Erweiterte Flags auf Seite 230) | 16-Bit-Ganzzahl |
| 922 | Fehlerbits für VO97–VO112 (siehe Erweiterte Flags auf Seite 230) | 16-Bit-Ganzzahl |

| Reg. Nr. | WORTNAME | DATENTYP |
|---|---|---|
| 923 | Fehlerbits für VO113–VO128 (siehe Erweiterte Flags auf Seite 230) | 16-Bit-Ganzzahl |
| 924 | Fehlerbits für VO129–VO144 (siehe Erweiterte Flags auf Seite 230) | 16-Bit-Ganzzahl |
| 925 | Fehlerbits für VO145–VO160 (siehe Erweiterte Flags auf Seite 230) | 16-Bit-Ganzzahl |
| 926 | Fehlerbits für VO161–VO176 (siehe Erweiterte Flags auf Seite 230) | 16-Bit-Ganzzahl |
| 927 | Fehlerbits für VO177–VO192 (siehe Erweiterte Flags auf Seite 230) | 16-Bit-Ganzzahl |
| 928 | Fehlerbits für VO193–VO208 (siehe Erweiterte Flags auf Seite 230) | 16-Bit-Ganzzahl |
| 929 | Fehlerbits für VO209–VO224 (siehe Erweiterte Flags auf Seite 230) | 16-Bit-Ganzzahl |
| 930 | Fehlerbits für VO225–VO240 (siehe Erweiterte Flags auf Seite 230) | 16-Bit-Ganzzahl |
| 931 | Fehlerbits für VO241–VO256 (siehe Erweiterte Flags auf Seite 230) | 16-Bit-Ganzzahl |
| 932 | Virtuelle Reset-/Abbruchverzögerung (1–16) Feedback [RCD-Feedback Registerbits] (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 57) | 16-Bit-Ganzzahl |
| 933 | *reserviert* | 16-Bit-Ganzzahl |
| 934 | RCD-Auslösecode Feedback [RCD-Aktivierung Feedbackregister] (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 57) | 16-Bit-Ganzzahl |
| 935 | VO1-Fehlerindex | 16-Bit-Ganzzahl |
| 936 | VO2-Fehlerindex | 16-Bit-Ganzzahl |
| 937 | VO3-Fehlerindex | 16-Bit-Ganzzahl |
| … | … | … |
| 1190 | VO256-Fehlerindex | 16-Bit-Ganzzahl |
| 1191–1192 | Vollständiger VO1-Fehlercode | 32-Bit-Ganzzahl |
| 1193–1194 | Vollständiger VO2-Fehlercode | 32-Bit-Ganzzahl |
| 1195–1196 | Vollständiger VO3-Fehlercode | 32-Bit-Ganzzahl |
| 1197–1198 | Vollständiger VO4-Fehlercode | 32-Bit-Ganzzahl |
| … | … | … |
| 1701–1702 | Vollständiger VO256-Fehlercode | 32-Bit-Ganzzahl |
| 1703–1704 | ISD-Systemstatus – Reihe 1 Geräteanzahl | 32-Bit-Ganzzahl |
| 1705–1706 | ISD-Systemstatus – Reihe 2 Geräteanzahl | 32-Bit-Ganzzahl |
| 1707–1708 | ISD-Systemstatus – Reihe 1 Gerätestatus Ein/Aus (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 1709–1710 | ISD-Systemstatus – Reihe 2 Gerätestatus Ein/Aus (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 1711–1712 | ISD-Systemstatus – Reihe 1 Fehlerstatus (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 1713–1714 | ISD-Systemstatus – Reihe 2 Fehlerstatus (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 1715–1716 | ISD-Systemstatus – Reihe 1 marginaler Status (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 1717–1718 | ISD-Systemstatus – Reihe 2 marginaler Status (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |

| Reg. Nr. | WORTNAME | DATENTYP |
|---|---|---|
| 1719–1720 | ISD-Systemstatus – Reihe 1 Alarmstatus (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 1721–1722 | ISD-Systemstatus – Reihe 2 Alarmstatus (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 1723–1724 | ISD-Systemstatus – Reihe 1 Reset-Status (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 1725–1726 | ISD-Systemstatus – Reihe 2 Reset-Status (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 1727–1728 | ISD-Systemstatus – Reihe 1 Auslöser erkannt (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 1728–1730 | ISD-Systemstatus – Reihe 2 Auslöser erkannt (siehe ISD-Systemstatuswörter auf Seite 185) | 32-Bit-Ganzzahl |
| 1731–1732 | ISD-Systemstatus – Reihe 1 Systemstatus (siehe ISD-Reihe Systemstatus auf Seite 47) | 32-Bit-Ganzzahl |
| 1733–1734 | ISD-Systemstatus – Reihe 2 Systemstatus (siehe ISD-Reihe Systemstatus auf Seite 47) | 32-Bit-Ganzzahl |
| 1735–1766 | *reserviert* | 16-Bit-Ganzzahl |
| 1768 | ISD-Leseanforderung Bestätigung (siehe Leistungs- und Statusinformationen zu einem einzelnen Gerät über ISD anfordern auf Seite 47) | 16-Bit-Ganzzahl |
| 1769 | Von ISD-Reihe angeforderte Bestätigung (siehe Leistungs- und Statusinformationen zu einem einzelnen Gerät über ISD anfordern auf Seite 47) | 16-Bit-Ganzzahl |
| 1770 | Von ISD-Gerät angeforderte Bestätigung (siehe Leistungs- und Statusinformationen zu einem einzelnen Gerät über ISD anfordern auf Seite 47) | 16-Bit-Ganzzahl |
| 1771–1779 | Spezifische Daten einzelner ISD-Geräte[33] (siehe Detaillierte Beschreibung spezifischer Daten einzelner ISD-Geräte auf Seite 227) | 16-Bit-Ganzzahl |

**Anmerkung:** Siehe Spezifische Daten einzelner ISD-Geräte auf Seite 48 für weitere Informationen über die Struktur der ISD-Daten.

## Detaillierte Beschreibung spezifischer Daten einzelner ISD-Geräte

Die folgende Tabelle beschreibt N7 REG Nr. 1771–1779.

*Tabelle 37. Detaillierte Beschreibung spezifischer Daten einzelner ISD-Geräte*

| REG Nr. | Informationen | Datengröße |
|---|---|---|
| 1771.0 | Sicherheitseingangsfehler | 1 Bit |
| 1771.1 | *reserviert* | 1 Bit |
| 1771.2 | Sensor nicht gekoppelt | 1-Bit |
| 1771.3 | ISD-Datenfehler | 1-Bit |
| 1771.4 | Falscher Auslöser-/Tasterstatus/Eingangsstatus | 1-Bit |
| 1771.5 | Marginaler Bereich/Tasterstatus/Eingangsstatus | 1-Bit |
| 1771.6 | Auslöser erkannt | 1-Bit |
| 1771.7 | Ausgangsfehler | 1-Bit |
| 1771.8 | Eingang 2 | 1-Bit |
| 1771.9 | Eingang 1 | 1-Bit |
| 1771.10 | Lokaler Reset erwartet | 1-Bit |

[33] Informationen zur Umrechnung von Innentemperatur, Auslöserabstand und Betriebsspannung finden Sie unter ISD: Informationen zur Umwandlung von Temperatur, Spannung und Abstand auf Seite 248.

| REG Nr. | Informationen | Datengröße |
|---|---|---|
| 1771.11 | Warnung Betriebsspannung | 1-Bit |
| 1771.12 | Fehler bei Betriebsspannung | 1-Bit |
| 1771.13 | Ausgang 2 | 1-Bit |
| 1771.14 | Ausgang 1 | 1-Bit |
| 1771.15 | Aus- und Wiedereinschalten der Stromversorgung erforderlich | 1-Bit |
| 1772.0 | Fehlertolerante Ausgänge | 1-Bit |
| 1772.1 | Einheit für lokalen Reset | 1-Bit |
| 1772.2 | Kaskadierbar | 1-Bit |
| 1772.3 | Hohe Codierstufe | 1-Bit |
| 1772.4 bis 1772.7 | Verbleibende Einlerninstanzen | 4-Bit |
| 1772.8 bis 1772.12 | Geräte-ID | 5-Bit |
| 1772.13 bis 1773.2 | Anzahl Bereichswarnungen | 6-Bit |
| 1773.3 bis 1773.7 | Ausschaltzeit für Ausgang | 5-Bit |
| 1773.8 bis 1773.15 | Anzahl der Spannungsfehler | 8-Bit |
| 1774.0 bis 1774.7 | Innentemperatur [34] | 8-Bit |
| 1774.8 bis 1774.15 | Auslöserabstand [34] | 8-Bit |
| 1775.0 bis 1775.7 | Versorgungsspannung [34] | 8-Bit |
| 1775.8 bis 1775.11 | Erwarteter Firmenname | 4-Bit |
| 1775.12 bis 1775.15 | Empfangener Firmenname | 4-Bit |
| 1776 | Erwarteter Code | 16-Bit |
| 1777 | Empfangener Code | 16-Bit |
| 1778 | Interner Fehler A | 16-Bit |
| 1779 | Interner Fehler B | 16-Bit |

**Anmerkung:** Siehe Spezifische Daten einzelner ISD-Geräte auf Seite 48 für weitere Informationen über die Struktur der ISD-Daten.

## 12.6.3 Eingänge zum Sicherheitskontroller (Ausgänge von der SPS)

Die Eingangsregister senden Informationen an den Sicherheitskontroller von der SPS. MSG(Nachrichten)-Befehle werden zum Schreiben (N11) auf den Sicherheitskontroller verwendet.

*Tabelle 38. N11 Register*

| Reg. Nr. | WORTNAME | DATENTYP |
|---|---|---|
| 0–7 | *reserviert* | 16-Bit-Ganzzahl |
| 8 | Virtueller Eingang Ein/Aus (1–16) | 16-Bit-Ganzzahl |
| 9 | Virtueller Eingang Ein/Aus (17–32) | 16-Bit-Ganzzahl |
| 10 | Virtueller Eingang Ein/Aus (33–48) | 16-Bit-Ganzzahl |
| 11 | Virtueller Eingang Ein/Aus (49–64) | 16-Bit-Ganzzahl |
| 12–15 | *reserviert* | 16-Bit-Ganzzahl |
| 16 | Virtuelle Reset-/Abbruchverzögerung (1–16) [RCD-Registerbits] (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 57) | 16-Bit-Ganzzahl |

[34] Informationen zur Umrechnung von Innentemperatur, Auslöserabstand und Betriebsspannung finden Sie unter ISD: Informationen zur Umwandlung von Temperatur, Spannung und Abstand auf Seite 248.

| Reg. Nr. | WORTNAME | DATENTYP |
|---|---|---|
| 17 | *reserviert* | 16-Bit-Ganzzahl |
| 18 | RCD-Auslösecode [RCD-Aktivierung Register] (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 57) | 16-Bit-Ganzzahl |
| 19 | ISD-Leseanforderung (siehe Leistungs- und Statusinformationen zu einem einzelnen Gerät über ISD anfordern auf Seite 47) | 16-Bit-Ganzzahl |
| 20 | ISD-Reihe angefordert (siehe Leistungs- und Statusinformationen zu einem einzelnen Gerät über ISD anfordern auf Seite 47) | 16-Bit-Ganzzahl |
| 21 | ISD-Gerät angefordert (siehe Leistungs- und Statusinformationen zu einem einzelnen Gerät über ISD anfordern auf Seite 47) | 16-Bit-Ganzzahl |

## 12.6.4 Flags

Die unten definierten Register 0 bis 7 werden in der N7-Registerzuordnung als die ersten 8 Wörter angezeigt.

*Tabelle 39. Register Nr. 0, virtueller Ausgang 1–16, Bitposition*

| Bit-Position | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **15** | **14** | **13** | **12** | **11** | **10** | **9** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** | **0** |
| VO16 | VO15 | VO14 | VO13 | VO12 | VO11 | VO10 | VO9 | VO8 | VO7 | VO6 | VO5 | VO4 | VO3 | VO2 | VO1 |

*Tabelle 40. Register Nr. 1, virtueller Ausgang 17–32, Bitposition*

| Bit-Position | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **15** | **14** | **13** | **12** | **11** | **10** | **9** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** | **0** |
| VO32 | VO31 | VO30 | VO29 | VO28 | VO27 | VO26 | VO25 | VO24 | VO23 | VO22 | VO21 | VO20 | VO19 | VO18 | VO17 |

*Tabelle 41. Register Nr. 2, virtueller Ausgang 33–48, Bitposition*

| Bit-Position | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **15** | **14** | **13** | **12** | **11** | **10** | **9** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** | **0** |
| VO48 | VO47 | VO46 | VO45 | VO44 | VO43 | VO42 | VO41 | VO40 | VO39 | VO38 | VO37 | VO36 | VO35 | VO34 | VO33 |

*Tabelle 42. Register Nr. 3, virtueller Ausgang 49–64, Bitposition*

| Bit-Position | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **15** | **14** | **13** | **12** | **11** | **10** | **9** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** | **0** |
| VO64 | VO63 | VO62 | VO61 | VO60 | VO59 | VO58 | VO57 | VO56 | VO55 | VO54 | VO53 | VO52 | VO51 | VO50 | VO49 |

*Tabelle 43. Register Nr. 4, Fehlerflagbits für virtuellen Ausgang 1–16, Bitposition*

Hinweis: Nicht jeder virtuelle Ausgang hat ein definiertes Fehlerflag.

| Bit-Position | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **15** | **14** | **13** | **12** | **11** | **10** | **9** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** | **0** |
| VO16 | VO15 | VO14 | VO13 | VO12 | VO11 | VO10 | VO9 | VO8 | VO7 | VO6 | VO5 | VO4 | VO3 | VO2 | VO1 |

*Tabelle 44. Register Nr. 5, Fehlerflagbits für virtuellen Ausgang 17–32, Bitposition*

Hinweis: Nicht jeder virtuelle Ausgang hat ein definiertes Fehlerflag.

| Bit-Position | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **15** | **14** | **13** | **12** | **11** | **10** | **9** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** | **0** |
| VO32 | VO31 | VO30 | VO29 | VO28 | VO27 | VO26 | VO25 | VO24 | VO23 | VO22 | VO21 | VO20 | VO19 | VO18 | VO17 |

*Tabelle 45. Register Nr. 6, Fehlerflagbits für virtuellen Ausgang 33–48, Bitposition*

Hinweis: Nicht jeder virtuelle Ausgang hat ein definiertes Fehlerflag.

| Bit-Position | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| VO48 | VO47 | VO46 | VO45 | VO44 | VO43 | VO42 | VO41 | VO40 | VO39 | VO38 | VO37 | VO36 | VO35 | VO34 | VO33 |

*Tabelle 46. Register Nr. 7, Fehlerflagbits für virtuellen Ausgang 49–64, Bitposition*

Hinweis: Nicht jeder virtuelle Ausgang hat ein definiertes Fehlerflag.

| Bit-Position | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| VO64 | VO63 | VO62 | VO61 | VO60 | VO59 | VO58 | VO57 | VO56 | VO55 | VO54 | VO53 | VO52 | VO51 | VO50 | VO49 |

### 12.6.5 Erweiterte Flags

Auf alle 256 virtuellen Ausgänge kann ähnlich wie unter Flags auf Seite 229 abgebildet zugegriffen werden.

Alle 256 virtuellen Ausgänge können als Register 900–915 gelesen werden.

Alle 256 virtuellen Ausgangsfehler können als Register 916–931 gelesen werden.

## 12.7 PROFINET®

PROFINET® [35] ist ein Datenkommunikationsprotokoll für Industrieautomatisierung und -prozesse. PROFINET IO definiert, wie Kontroller (E/A-Kontroller) und Peripheriegeräte (E/A-Geräte) Daten in Echtzeit austauschen.

Sicherheitskontroller von Banner unterstützt PROFINET IO. Das Datenkommunikationsprotokoll ist TCP/IP; das Datenübertragungsmedium ist Kupferdraht; die Konformitätsklasse von PROFINET ist CC-A. [36]

**Anmerkung:** In diesem Dokument werden Ausgänge vom Sicherheitskontroller als „Eingänge“ zum Kontroller (SPS) bezeichnet. Ausgänge vom Kontroller (SPS) werden als „Eingänge“ zum Sicherheitskontroller bezeichnet.

### 12.7.1 PROFINET und die Sicherheitskontroller

Dieser Abschnitt enthält die Anleitung für XS/SC26-2-Sicherheitskontroller mit der Bezeichnung FID 2 auf dem Typenschild und den Datumcodes 1706 oder höher sowie für XS/SC26-2-Sicherheitskontroller ab FID 3.

Dieser Abschnitt behandelt den SC10-2.

PROFINET-Echtzeitdaten werden über Steckplätze gesendet und empfangen.

**Anmerkung:** Die GSDML-Datei steht unter http://www.bannerengineering.com zum Download zur Verfügung.

### 12.7.2 GSD-Datei (General Station Description)

Die GSD-Datei (General Station Description) enhält Modulinformationen wie:

- Konfigurationsdaten
- Dateninformationen (Durchlaufzähler, Inspektionsstatus usw.)
- Diagnose

### 12.7.3 PROFINET IO-Datenmodell

Das PROFINET IO-Datenmodell basiert auf dem typischen, erweiterbaren Feldgerät mit einer Rückwandplatine mit Steckplätzen. Module und Submodule haben unterschiedliche Funktionen.

Module werden in Steckplätze eingesteckt, Submodule in Substeckplätze. Im PROFINET IO-Datenmodel ist Steckplatz 0 Substeckplatz 1 für den Device Access Point (DAP) bzw. die Netzwerkschnittstelle reserviert.

Module wie auch Submodule werden zur Steuerung des Typs und des Volumens der Daten verwendet, die an den Kontroller (SPS) gesendet werden.

- Ein Submodul ist in der Regel als Eingangstyp, Ausgangstyp oder kombinierter Eingangs-/Ausgangstyp ausgewiesen.

35 PROFINET® ist eine eingetragene Marke des PROFIBUS Nutzerorganisation e.V.
36 CC-A gewährleistet, dass das Gerät die Mindestanforderungen an Funktionalität und Interoperabilität erfüllt.

- Ein Eingangssubmodul wird zum Senden von Daten an den Kontroller (SPS) verwendet.
- Ein Ausgangssubmodul wird zum Empfangen von Daten an den Kontroller (SPS) verwendet.
- Das kombinierte Eingangs-/Ausgangssubmodul empfängt und sendet Daten in beide Richtungen.

## 12.7.4 Konfiguration des Sicherheitskontrollers für eine PROFINET IO-Verbindung

1. Verbinden Sie den Sicherheitskontroller über das SC-USB2-USB-Kabel mit dem PC.
2. Öffnen Sie die Software des Sicherheitskontroller von Banner und klicken Sie auf die Registerkarte **Industrie-Ethernet**.
3. Wählen Sie aus der Dropdown-Liste links **Profinet** aus.
4. Klicken Sie auf , um den PROFINET-Submodulen Informationen hinzuzufügen.

   Bei dieser Aufgabe kann **automatisches Konfigurieren** hilfreich sein.
5. Geben Sie das entsprechende Passwort ein, um die Konfigurations- und Netzwerkeinstellungen für den Sicherheitskontroller zu ändern.
6. Vergewissern Sie sich, dass der Sicherheitskontroller eine gültige und bestätigte Konfigurationsdatei hat.

**Anmerkung:** Wenn eine virtuelle Reset- oder Abbruchverzögerung verwendet wird, muss der Auslösecode in den **Netzwerkeinstellungen** erstellt werden. Der Code muss dann über **Senden** in den **Netzwerkeinstellungen** an den Sicherheitskontroller gesendet werden.

## 12.7.5 Beschreibung der Module

*Tabelle 47. Zuweisung von Steckplätzen*

In dieser Tabelle ist die E/A-Richtung vom Standpunkt der SPS aus genannt.

| Steckplatz | Modulfunktion | E/A | Modulname | Modulgröße (Byte) |
|---|---|---|---|---|
| 1 | Benutzerdefinierte Statusbits (0–31) | Eingehend | 4 Statusbytes, Bits 0..31_1 | 4 |
| 2 | Benutzerdefinierte Statusbits (32–63) | Eingehend | 4 Statusbytes, Bits 0..31_2 | 4 |
| 3 | Sicherheitskontroller Fehlerbits (0–31) | Eingehend | 4 Statusbytes, Bits 0..31_3 | 4 |
| 4 | Sicherheitskontroller Fehlerbits (32–63) | Eingehend | 4 Statusbytes, Bits 0..31_4 | 4 |
| 5 | Sicherheitskontroller Eingangsstatusbits (0–31) | Eingehend | 4 Statusbytes, Bits 0..31_5 | 4 |
| 6 | Sicherheitskontroller Eingangsstatusbits (32–63) | Eingehend | 4 Statusbytes, Bits 0..31_6 | 4 |
| 7 | Sicherheitskontroller Eingangsstatusbits (64–95) | Eingehend | 4 Statusbytes, Bits 0..31_7 | 4 |
| 8 | Sicherheitskontroller Eingangsstatusbits (96–127) | Eingehend | 4 Statusbytes, Bits 0..31_8 | 4 |
| 9 | Sicherheitskontroller Eingangsstatusbits (128–159) | Eingehend | 4 Statusbytes, Bits 0..31_9 | 4 |
| 10 | Sicherheitskontroller Ausgangsstatusbits (0–31) | Eingehend | 4 Statusbytes, Bits 0..31_10 | 4 |
| 11 | Sicherheitskontroller Ausgangsstatusbits (32–63) | Eingehend | 4 Statusbytes, Bits 0..31_11 | 4 |
| 12 | Sicherheitskontroller Ausgangsstatusbits (64–95) | Eingehend | 4 Statusbytes, Bits 0..31_12 | 4 |
| 13 | Virtueller E/A (Ein/Aus/Muting-Aktivierung) Bits (0–63) | Ausgehend | 8 Byte Virtuell Ein/AUS/MA Data_1 | 8 |

| Steckplatz | Modulfunktion | E/A | Modulname | Modulgröße (Byte) |
|---|---|---|---|---|
| 14 | Virtuelle Reset-/Abbruchverzögerung Bits (0–16) | Ausgehend | 2 Byte RCD Data_1 | 2 |
| 15 | Auslösecode für Reset-/Abbruchverzögerung | Ausgehend | 2 Byte RCD Auslösung Code_1 | 2 |
| 16 | Virtuelle Reset-/Abbruchverzögerung Bits (0–16) Feedback | Eingehend | RCD Data Feedback Register_1 | 2 |
| 17 | Auslösecode für Reset-/Abbruchverzögerung Feedback | Eingehend | RCD Passcode Feedback Register_1 | 2 |
| 18 [37] | Fehlerprotokoll | E | Fehlerprotokollpuffermodul | 300 |
| 19 [37] | Systeminformationen | Eingehend | Systeminformationsmodul | 30 |
| 20 | ISD-Status | Eingehend | ISD-Statusinformationsmodul | 128 |
| 21 | Informationen zu einzelnen ISD-Geräten | Ein-/Ausgang | ISD-Einzelstatusinformationsmodul | 24 eingehend/6 ausgehend |

**Anmerkung:** Siehe Spezifische Daten einzelner ISD-Geräte auf Seite 48 für weitere Informationen über die Struktur der ISD-Daten.

## Benutzerdefinierte Statusbits

Die ersten zwei Steckplätze sind immer von den benutzerdefinierten Statusbit-Modulen belegt. Diese Module umfassen beliebige 64-Bit-Informationen des virtuellen Statusausgangs.

*Tabelle 48. Benutzerdefinierte Statusbits (0–31) Modul (Ident 0×100) [fest in Steckplatz 1]*

| SPS-Eingangsdatenname | Eingangsdatentyp |
|---|---|
| Benutzerdefinierte Statusbits 0–7 | Byte |
| Benutzerdefinierte Statusbits 8–15 | Byte |
| Benutzerdefinierte Statusbits 16–23 | Byte |
| Benutzerdefinierte Statusbits 24–31 | Byte |

| SPS-Ausgangsdatenname | Ausgangsdatentyp |
|---|---|
| Entfällt | Entfällt |

[37] Das Fehlerprotokoll- und das Systeminformationsmodul werden nicht von der Standardverbindung verwendet.

*Tabelle 49. Benutzerdefinierte Statusbits (32–63) Modul (Ident 0×100) [fest in Steckplatz 2]*

| SPS-Eingangsdatenname | Eingangsdatentyp |
|---|---|
| Benutzerdefinierte Statusbits 32–39 | Byte |
| Benutzerdefinierte Statusbits 40–47 | Byte |
| Benutzerdefinierte Statusbits 48–55 | Byte |
| Benutzerdefinierte Statusbits 56–63 | Byte |

| SPS-Ausgangsdatenname | Ausgangsdatentyp |
|---|---|
| Entfällt | Entfällt |

## Fehlerbits

Die Steckplätze 3 und 4 empfangen immer 64-Bit-Informationen von virtuellen Statusausgangsfehlern vom Sicherheitskontroller.

*Tabelle 50. Sicherheitskontroller Fehlerbits (0–31) Modul (Ident 0×100) [fest in Steckplatz 3]*

| SPS-Eingangsdatenname | Eingangsdatentyp |
|---|---|
| Fehlerbits 0–7 | Byte |
| Fehlerbits 8–15 | Byte |
| Fehlerbits 16–23 | Byte |
| Fehlerbits 24–31 | Byte |

| SPS-Ausgangsdatenname | Ausgangsdatentyp |
|---|---|
| Entfällt | Entfällt |

*Tabelle 51. Sicherheitskontroller Fehlerbits (32–63) Modul (Ident 0×100) [fest in Steckplatz 4]*

| SPS-Eingangsdatenname | Eingangsdatentyp |
|---|---|
| Fehlerbits 32–39 | Byte |
| Fehlerbits 40–47 | Byte |
| Fehlerbits 48–55 | Byte |
| Fehlerbits 56–63 | Byte |

| SPS-Ausgangsdatenname | Ausgangsdatentyp |
|---|---|
| Entfällt | Entfällt |

## Eingangsstatusbits

Die Steckplätze 5 bis 9 sind immer für 160 Bit an Sicherheitskontroller-Eingangsinformationen reserviert. Ein erweiterbarer (XS26) Sicherheitskontroller kann bis zu 154 Eingänge haben, wenn alle möglichen 8 Erweiterungskarten als 16-Kanal-Eingänge verwendet werden (zusätzlich zu den im Basiskontroller integrierten 26 Eingängen).

*Tabelle 52. Sicherheitskontroller Eingangsstatusbits (0–31) Modul (Ident 0×100) [fest in Steckplatz 5]*

| SPS-Eingangsdatenname | Eingangsdatentyp |
|---|---|
| Eingangsstatusbits 0–7 | Byte |
| Eingangsstatusbits 8–15 | Byte |
| Eingangsstatusbits 16–23 | Byte |
| Eingangsstatusbits 24–31 | Byte |

| SPS-Ausgangsdatenname | Ausgangsdatentyp |
|---|---|
| Entfällt | Entfällt |

*Tabelle 53. Sicherheitskontroller Eingangsstatusbits (32–63) Modul (Ident 0×100) [fest in Steckplatz 6]*

| SPS-Eingangsdatenname | Eingangsdatentyp |
|---|---|
| Eingangsstatusbits 32–39 | Byte |
| Eingangsstatusbits 40–47 | Byte |
| Eingangsstatusbits 48–55 | Byte |
| Eingangsstatusbits 56–63 | Byte |

| SPS-Ausgangsdatenname | Ausgangsdatentyp |
|---|---|
| Entfällt | Entfällt |

*Tabelle 54. Sicherheitskontroller Eingangsstatusbits (64–95) Modul (Ident 0×100) [fest in Steckplatz 7]*

| SPS-Eingangsdatenname | Eingangsdatentyp |
|---|---|
| Eingangsstatusbits 64–71 | Byte |
| Eingangsstatusbits 72–79 | Byte |
| Eingangsstatusbits 80–87 | Byte |
| Eingangsstatusbits 88–95 | Byte |

| SPS-Ausgangsdatenname | Ausgangsdatentyp |
|---|---|
| Entfällt | Entfällt |

*Tabelle 55. Sicherheitskontroller Eingangsstatusbits (96–127) Modul (Ident 0×100) [fest in Steckplatz 8]*

| SPS-Eingangsdatenname | Eingangsdatentyp |
|---|---|
| Eingangsstatusbits 96–103 | Byte |
| Eingangsstatusbits 104–111 | Byte |
| Eingangsstatusbits 112–119 | Byte |
| Eingangsstatusbits 120–127 | Byte |

| SPS-Ausgangsdatenname | Ausgangsdatentyp |
|---|---|
| Entfällt | Entfällt |

*Tabelle 56. Sicherheitskontroller Eingangsstatusbits (128–159) Modul (Ident 0×100) [fest in Steckplatz 9]*

| SPS-Eingangsdatenname | Eingangsdatentyp |
|---|---|
| Eingangsstatusbits 128–135 | Byte |
| Eingangsstatusbits 136–143 | Byte |
| Eingangsstatusbits 144–151 | Byte |
| Eingangsstatusbits 152–159 | Byte |

| SPS-Ausgangsdatenname | Ausgangsdatentyp |
|---|---|
| Entfällt | Entfällt |

## Ausgangsstatusbits

Die Steckplätze 10 bis 12 sind für 96 Sicherheitskontrollerausgänge vom Typ virtuelle Statusausgangsbits reserviert.

*Tabelle 57. Sicherheitskontroller Ausgangsstatusbits (0–31) Modul (Ident 0×100) [fest in Steckplatz 10]*

| SPS-Eingangsdatenname | Eingangsdatentyp |
|---|---|
| Ausgangsstatusbits 0–7 | Byte |
| Ausgangsstatusbits 8–15 | Byte |
| Ausgangsstatusbits 16–23 | Byte |
| Ausgangsstatusbits 24–31 | Byte |

| SPS-Ausgangsdatenname | Ausgangsdatentyp |
|---|---|
| Entfällt | Entfällt |

*Tabelle 58. Sicherheitskontroller Ausgangsstatusbits (32–63) Modul (Ident 0×100) [fest in Steckplatz 11]*

| SPS-Eingangsdatenname | Eingangsdatentyp |
|---|---|
| Ausgangsstatusbits 32–39 | Byte |
| Ausgangsstatusbits 40–47 | Byte |
| Ausgangsstatusbits 48–55 | Byte |
| Ausgangsstatusbits 56–63 | Byte |

| SPS-Ausgangsdatenname | Ausgangsdatentyp |
|---|---|
| Entfällt | Entfällt |

*Tabelle 59. Sicherheitskontroller Ausgangsstatusbits (64–95) Modul (Ident 0×100) [fest in Steckplatz 12]*

| SPS-Eingangsdatenname | Eingangsdatentyp |
|---|---|
| Ausgangsstatusbits 64–71 | Byte |
| Ausgangsstatusbits 72–79 | Byte |
| Ausgangsstatusbits 80–87 | Byte |
| Ausgangsstatusbits 88–95 | Byte |

| SPS-Ausgangsdatenname | Ausgangsdatentyp |
|---|---|
| Entfällt | Entfällt |

## Virtuelle Einschalt-, Ausschalt-, Muting-Aktivierungsbits

Steckplatz 13 ist mit 64 virtuellen nicht sicherheitsrelevanten Eingängen belegt, die als virtuelle Ein-/Ausschaltungseingänge (zum Sicherheitskontroller) oder als virtuelle Muting-Aktivierungseingänge (zum Sicherheitskontroller) verwendet werden.

*Tabelle 60. Virtuelle Ein-/Ausschaltung und Muting-Aktivierung Bits (0–63) Modul (Ident 0×200) [fest in Steckplatz 13]*

| SPS-Eingangsdatenname | Eingangsdatentyp |
|---|---|
| Entfällt | Entfällt |

| SPS-Ausgangsdatenname | Ausgangsdatentyp |
|---|---|
| Virtuelle Ein-/Ausschaltung/MA Bits 0–7 | Byte |
| Virtuelle Ein-/Ausschaltung/MA Bits 8–15 | Byte |
| Virtuelle Ein-/Ausschaltung/MA Bits 16–23 | Byte |
| Virtuelle Ein-/Ausschaltung/MA Bits 24–31 | Byte |
| Virtuelle Ein-/Ausschaltung/MA Bits 32–39 | Byte |
| Virtuelle Ein-/Ausschaltung/MA Bits 40–47 | Byte |
| Virtuelle Ein-/Ausschaltung/MA Bits 48–55 | Byte |
| Virtuelle Ein-/Ausschaltung/MA Bits 56–63 | Byte |

## Virtuelle Reset-/Abbruchverzögerungsbits (VRCD)

16 virtuelle nicht sicherheitsrelevante Eingängen können in Steckplatz 14 vorhanden sein und für die Abfolge der virtuellen Reset-/Abbruchverzögerung verwendet werden.

Siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 57.

*Tabelle 61. Virtuelle Reset-/Abbruchverzögerung Bits (0–63) Modul (Ident 0×300) [fest in Steckplatz 14]*

| SPS-Eingangsdatenname | Eingangsdatentyp |
|---|---|
| Entfällt | Entfällt |

| SPS-Ausgangsdatenname | Ausgangsdatentyp |
|---|---|
| VRCD-Bits 0–7 | Byte |
| VRCD-Bits 8–15 | Byte |

## Reset-/Abbruchverzögerung (RCD) 16-Bit-Auslösecode

Steckplatz 15 enthält den RCD-Auslösecodes, eines wichtigen Codeworts für die Abfolge der virtuellen Reset-/Abbruchverzögerung.

Siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 57.

*Tabelle 62. Modul für den Auslösecode für die Reset- und Abbruchverzögerung (Ident 0×301) [fest in Steckplatz 15]*

| SPS-Eingangsdatenname | Eingangsdatentyp |
|---|---|
| Entfällt | Entfällt |

| SPS-Ausgangsdatenname | Ausgangsdatentyp |
|---|---|
| Auslösecode für Reset-/Abbruchverzögerung | Ohne Vorzeichen 16 |

## Virtuelle Reset-/Abbruchverzögerung Feedbackbits

Steckplatz 16 umfasst Feedbackbits für die 16 virtuellen nicht sicherheitsrelevanten Eingänge in Steckplatz 14. Sie werden in der Abfolge der virtuellen Reset-/Abbruchverzögerung verwendet.

Siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 57.

*Tabelle 63. Virtuelle Reset-/Abbruchverzögerung Bits (0–63) Modul (Ident 0×400) [fest in Steckplatz 16]*

| SPS-Eingangsdatenname | Eingangsdatentyp |
|---|---|
| VRCD-Feedbackbits 0–7 | Byte |
| VRCD-Feedbackbits 8–15 | Byte |

| SPS-Ausgangsdatenname | Ausgangsdatentyp |
|---|---|
| Entfällt | Entfällt |

## Reset-/Abbruchverzögerung 16-bit-Auslösecode Feedback

Steckplatz 17 enthält den Feedback-Wert des RCD-Auslösecodes, eines wichtigen Codeworts für die Abfolge der virtuellen Reset-/Abbruchverzögerung.

Siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 57.

*Tabelle 64. Modul für den Auslösecode für die Reset-/Abbruchverzögerung (Ident 0×401) [fest in Steckplatz 17]*

| SPS-Eingangsdatenname | Eingangsdatentyp |
|---|---|
| Auslösecode für Reset-/ Abbruchverzögerung Feedback | Ohne Vorzeichen 16 |

| SPS-Ausgangsdatenname | Ausgangsdatentyp |
|---|---|
| Entfällt | Entfällt |

## Fehlerprotokolleinträge

In Steckplatz 18 kann das optionale Fehlerprotollpuffermodul eingesteckt werden.

*Tabelle 65. Sicherheitskontroller Fehlerprotokollpuffermodul (Ident 0×500) [optional; fest in Steckplatz 18, wenn verwendet]*

| SPS-Eingangsdatenname | Eingangsdatentyp |
|---|---|
| Fehlerprotokolleintrag 1 (neuester) | 15 Wörter |
| Fehlerprotokolleintrag 2 | 15 Wörter |
| Fehlerprotokolleintrag 3 | 15 Wörter |
| Fehlerprotokolleintrag 4 | 15 Wörter |
| Fehlerprotokolleintrag 5 | 15 Wörter |
| Fehlerprotokolleintrag 6 | 15 Wörter |
| Fehlerprotokolleintrag 7 | 15 Wörter |
| Fehlerprotokolleintrag 8 | 15 Wörter |
| Fehlerprotokolleintrag 9 | 15 Wörter |
| Fehlerprotokolleintrag 10 (ältester) | 15 Wörter |

| SPS-Ausgangsdatenname | Ausgangsdatentyp |
|---|---|
| Entfällt | Entfällt |

| Fehlerprotokolleintrag | Typ | Länge (Wörter) |
|---|---|---|
| Zeitstempel | UDINT | 2 |
| Name Länge | DWORD | 2 |
| Namensstring | String | 6 |

| Fehlerprotokolleintrag | Typ | Länge (Wörter) |
|---|---|---|
| Fehlercode | WORD | 1 |
| Erweiterter Fehlercode | WORD | 1 |
| Fehlerindexmeldung | WORD | 1 |
| *reserviert* | WORD | 2 |

**Falscher Zeitstempel**

Die relative Zeit in Sekunden, nachdem der Fehler aufgetreten ist. Gemessen ab Zeitpunkt 0, also dem letzten Zeitpunkt, an dem der Sicherheitskontroller eingeschaltet wurde.

**Name Länge**

Die Anzahl an ASCII-Zeichen im „Namensstring“.

**Namensstring**

Ein ASCII-String, der den Ursprung des Fehlers beschreibt.

**Fehlercode, erweiterter Fehlercode, Fehlerindexmeldung**

Der Sicherheitskontroller-Fehlercode setzt sich aus dem Fehlercode und dem erweiterten Fehlercode zusammen. Das Format des Fehlercodes ist `Fehlercode "Punkt" erweiterter Fehlercode` . Der Sicherheitskontroller-Fehlercode 2.1 wird beispielsweise vom Fehlercode `2` und dem erweiterten Fehlercode `1` angegeben. Der Indexwert der Fehlermeldung ist der Fehlercode und der erweiterte Fehlercode zusammen und umfasst eine führende Null mit dem erweiterten Fehlercode, falls erforderlich. Der Sicherheitskontroller-Fehlercode 2.1 wird beispielsweise vom Fehlermeldungsindex `201` angegeben. Mit dem Indexwert der Fehlermeldung kann der vollständige Fehlercode bequem nur anhand eines einzigen 16-Bit-Registerwerts abgerufen werden.

## Puffer für Systeminformationen

In Steckplatz 19 kann das optionale Systeminformationspuffermodul eingesteckt werden.

*Tabelle 66. Sicherheitskontroller Systminformationspuffermodul (Ident 0×600) [optional; fest in Steckplatz 19, wenn verwendet]*

| SPS-Eingangsdatenname | Eingangsdatentyp |
|---|---|
| Puffer für Systeminformationen | 30 Wörter |

| SPS-Ausgangsdatenname | Ausgangsdatentyp |
|---|---|
| Entfällt | Entfällt |

| Puffer für Systeminformationen | Typ | Länge (Wörter) |
|---|---|---|
| Sekunden seit Systemstart | UDINT | 2 |
| Betriebsart | WORD | 1 |
| Länge des Konfigurationsnamens | DWORD | 2 |
| Konfigurationsname | String | 8 |
| Konfig. CRC | WORD | 2 |

**Sekunden seit Systemstart**

Die 32-Bit-Ganzzahldarstellung der Anzahl an Sekunden seit dem Einschalten des Sicherheitskontrollers.

**Betriebsart**

Der aktuelle Betriebsstatus des Sicherheitskontrollers.

| Wert für Betriebsart | Beschreibung |
|---|---|
| 1 (0×01) | Normalbetrieb (einschließlich E/A-Fehlern, sofern vorhanden) |
| 2 (0×02) | Konfigurationsmodus |
| 4 (0×04) | Systemsperre |
| 65 (0×41) | Warten auf System-Reset/Beenden des Konfigurationsmodus |
| 129 (0×81) | Aufruf des Konfigurationsmodus |

**Länge des Konfigurationsnamens**
Die Anzahl an ASCII-Zeichen im „Konfigurationsnamen“.

**Konfigurationsname**
Ein ASCII-String, der den Ursprung des Fehlers beschreibt.

**Konfig. CRC**
Der Wert der zyklischen Redundanzprüfung (CRC) für die aktuelle Konfiguration des Sicherheitskontrollers.

## ISD-Statusinformationsmodul

In Steckplatz 20 kann das optionale ISD-Statusinformationsmodul eingesteckt werden.

Siehe auch ISD-Systemstatuswörter auf Seite 185 und ISD-Reihe Systemstatus auf Seite 47.

| SPS-Eingangsdatenname | Eingangsdatentyp |
|---|---|
| ISD-Systemstatus – Reihe 1 Geräteanzahl | Ohne Vorzeichen 32 |
| ISD-Systemstatus – Reihe 2 Geräteanzahl | Ohne Vorzeichen 32 |
| ISD-Systemstatus – Reihe 1 Gerät-Ein/Aus-Status | Ohne Vorzeichen 32 |
| ISD-Systemstatus – Reihe 2 Gerät-Ein/Aus-Status | Ohne Vorzeichen 32 |
| ISD-Systemstatus – Reihe 1 Fehlerstatus | Ohne Vorzeichen 32 |
| ISD-Systemstatus – Reihe 2 Fehlerstatus | Ohne Vorzeichen 32 |
| ISD-Systemstatus – Reihe 1 marginaler Status | Ohne Vorzeichen 32 |
| ISD-Systemstatus – Reihe 2 marginaler Status | Ohne Vorzeichen 32 |
| ISD-Systemstatus – Reihe 1 Warnstatus | Ohne Vorzeichen 32 |
| ISD-Systemstatus – Reihe 2 Warnstatus | Ohne Vorzeichen 32 |
| ISD-Systemstatus – Reihe 1 Resetstatus | Ohne Vorzeichen 32 |
| ISD-Systemstatus – Reihe 2 Resetstatus | Ohne Vorzeichen 32 |
| ISD-Systemstatus – Reihe 1 Auslöser erkannt | Ohne Vorzeichen 32 |
| ISD-Systemstatus – Reihe 2 Auslöser erkannt | Ohne Vorzeichen 32 |
| ISD-Systemstatus – Reihe 1 Systemstatus | Ohne Vorzeichen 32 |
| ISD-Systemstatus – Reihe 2 Systemstatus | Ohne Vorzeichen 32 |
| *64 Byte reserviert* | Byte |

| SPS-Ausgangsdatenname | Ausgangsdatentyp |
|---|---|
| Entfällt | Ohne Vorzeichen 16 |

## Modul für Informationen einzelner ISD-Geräte

In Steckplatz 21 kann das optionale Modul für Informationen einzelner ISD-Geräte eingesteckt werden.

Siehe auch Leistungs- und Statusinformationen zu einem einzelnen Gerät über ISD anfordern auf Seite 47 und Detaillierte Beschreibung spezifischer Daten einzelner ISD-Geräte auf Seite 240.

| SPS-Eingangsdatenname | Eingangsdatentyp |
|---|---|
| ISD-Leseanfrage Bestätigung | Ohne Vorzeichen 16 |
| ISD-Reihe angefragte Bestätigung | Ohne Vorzeichen 16 |
| ISD-Gerät angefragte Bestätigung | Ohne Vorzeichen 16 |
| Spezifische Daten einzelner ISD-Geräte (18 Byte) [38] | Byte |

| SPS-Ausgangsdatenname | Ausgangsdatentyp |
|---|---|
| ISD-Leseanfrage | Ohne Vorzeichen 16 |
| ISD-Reihe angefordert | Ohne Vorzeichen 16 |
| ISD-Gerät angefordert | Ohne Vorzeichen 16 |

## Detaillierte Beschreibung spezifischer Daten einzelner ISD-Geräte

Die folgende Tabelle beschreibt Slot 21 [39].

*Tabelle 67. Detaillierte Beschreibung spezifischer Daten einzelner ISD-Geräte*

| Moduleingang | Informationen | Datengröße |
|---|---|---|
| 206.0F4:F20 | Sicherheitseingangsfehler | 1 Bit |
| 206.1 | *reserviert* | 1 Bit |
| 206.2 | Sensor nicht gekoppelt | 1-Bit |
| 206.3 | ISD-Datenfehler | 1-Bit |
| 206.4 | Falscher Auslöser-/Tasterstatus/Eingangsstatus | 1-Bit |
| 206.5 | Marginaler Bereich/Tasterstatus/Eingangsstatus | 1-Bit |
| 206.6 | Auslöser erkannt | 1-Bit |
| 206.7 | Ausgangsfehler | 1-Bit |
| 207.0 | Eingang 2 | 1-Bit |
| 207.1 | Eingang 1 | 1-Bit |
| 207.2 | Lokaler Reset erwartet | 1-Bit |
| 207.3 | Warnung Betriebsspannung | 1-Bit |
| 207.4 | Fehler bei Betriebsspannung | 1-Bit |
| 207.5 | Ausgang 2 | 1-Bit |
| 207.6 | Ausgang 1 | 1-Bit |
| 207.7 | Aus- und Wiedereinschalten der Stromversorgung erforderlich | 1-Bit |
| 208.0 | Fehlertolerante Ausgänge | 1-Bit |
| 208.1 | Einheit für lokalen Reset | 1-Bit |
| 208.2 | Kaskadierbar | 1-Bit |
| 208.3 | Hohe Codierstufe | 1-Bit |
| 208.7 bis 208.4 | Verbleibende Einlerninstanzen | 4-Bit |
| 209.4 bis 209.0 | Geräte-ID | 5-Bit |
| 210.2 bis 209.5 | Anzahl Bereichswarnungen | 6-Bit |
| 210.7 bis 210.3 | Ausschaltzeit für Ausgang | 5-Bit |
| 211 | Anzahl der Spannungsfehler | 8-Bit |
| 212 | Innentemperatur [40] | 8-Bit |

[38] Informationen zur Umrechnung von Innentemperatur, Auslöserabstand und Betriebsspannung finden Sie unter ISD: Informationen zur Umwandlung von Temperatur, Spannung und Abstand auf Seite 248.

[39] Das Beispiel für Steckplatz 21 basiert auf der Annahme, dass der Steckplatz mit einem %I200 für seinen Standort beginnt. Vor den eigentlichen Daten befindet sich ein Kopfzeilenteil. Das Beispiel basiert außerdem auf der Annahme, dass die Daten im Byte-Format vorliegen.

[40] Informationen zur Umrechnung von Innentemperatur, Auslöserabstand und Betriebsspannung finden Sie unter ISD: Informationen zur Umwandlung von Temperatur, Spannung und Abstand auf Seite 248.

| Moduleingang | Informationen | Datengröße |
|---|---|---|
| 213 | Auslöserabstand [40] | 8-Bit |
| 214 | Versorgungsspannung [40] | 8-Bit |
| 215.3 bis 215.0 | Erwarteter Firmenname | 4-Bit |
| 215.7 bis 215.4 | Empfangener Firmenname | 4-Bit |
| 217 bis 216 | Erwarteter Code | 16-Bit |
| 219 bis 218 | Empfangener Code | 16-Bit |
| 221 bis 220 | Interner Fehler A | 16-Bit |
| 223 bis 222 | Interner Fehler B | 16-Bit |

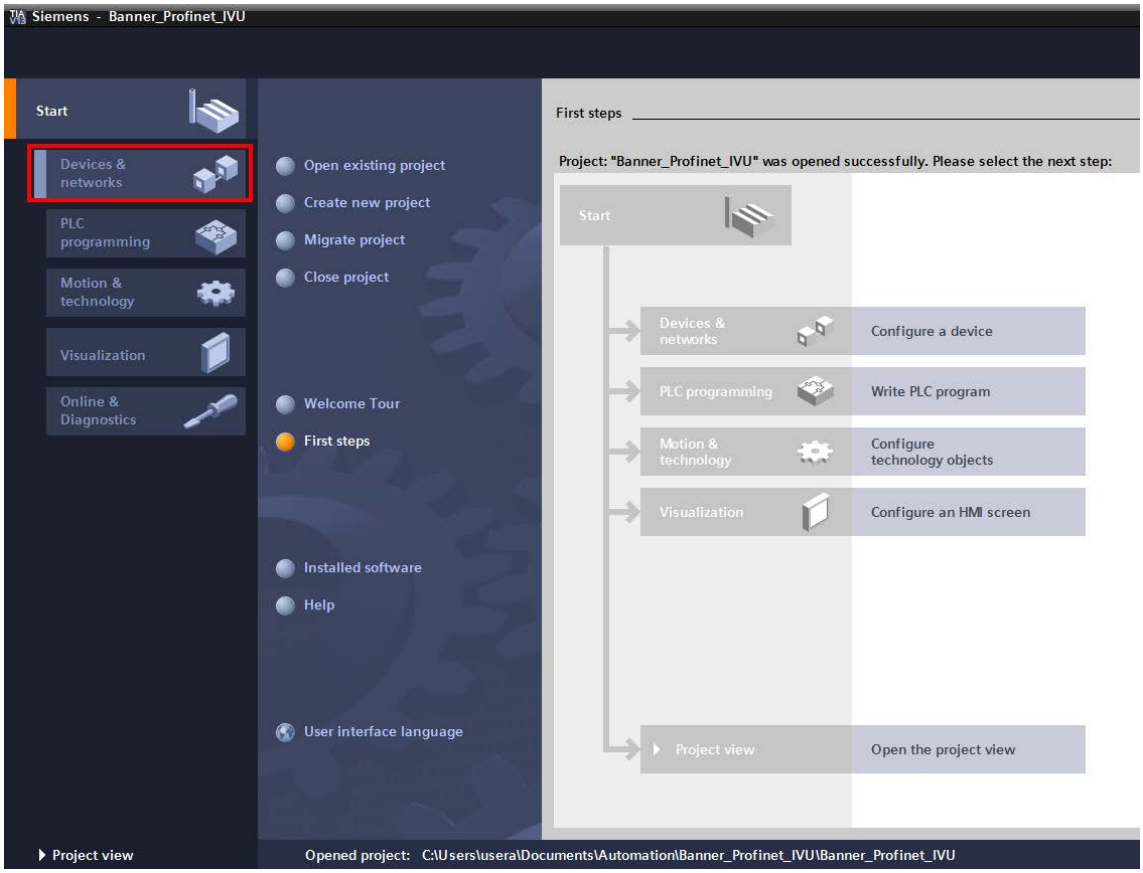
# 12.7.6 Konfigurationsanleitung

## Installation der GSD-Datei

Installieren Sie die GSD-Datei entsprechend der Anleitung in der Software im TIA Portal (v13) von Siemens. Diese Anleitung können Sie als Grundlage für die Installation der GSD-Datei in einem anderen Kontroller (SPS) verwenden.

1. Laden Sie die GSD-Datei von www.bannerengineering.com herunter.
2. Rufen Sie die Software im TIA Portal (v13) von Siemens auf.
3. Klicken Sie auf **Vorhandenes Projekt öffnen**.
4. Wählen Sie ein Projekt aus und öffnen Sie es.
5. Klicken Sie auf **Geräte und Netzwerke**, nachdem das Projekt hochgeladen wurde.

*Abbildung 230. Geräte und Netzwerke*




6. Klicken Sie auf **Netzwerke konfigurieren**.

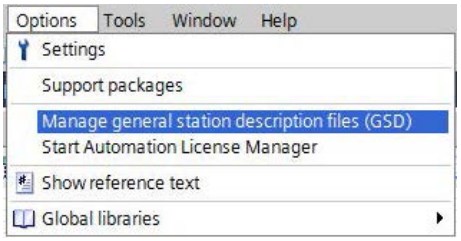
*Abbildung 231. Netzwerke konfigurieren*




Die **Netzwerkansicht** wird angezeigt.

7. Klicken Sie auf **Optionen** und wählen Sie **GSD-Datei (General Station Description) verwalten** aus.

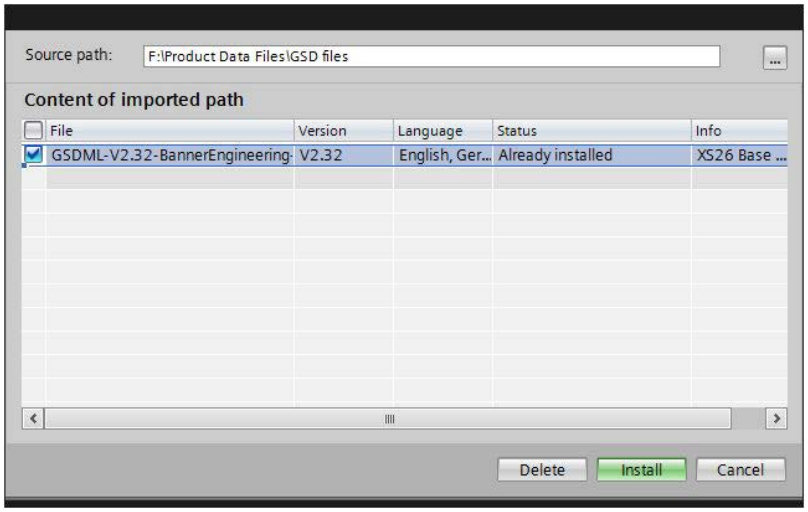
*Abbildung 232. Optionen — GSD-Datei installieren*




Das Fenster **GSD-Datei (General Station Description) installieren** wird geöffnet.

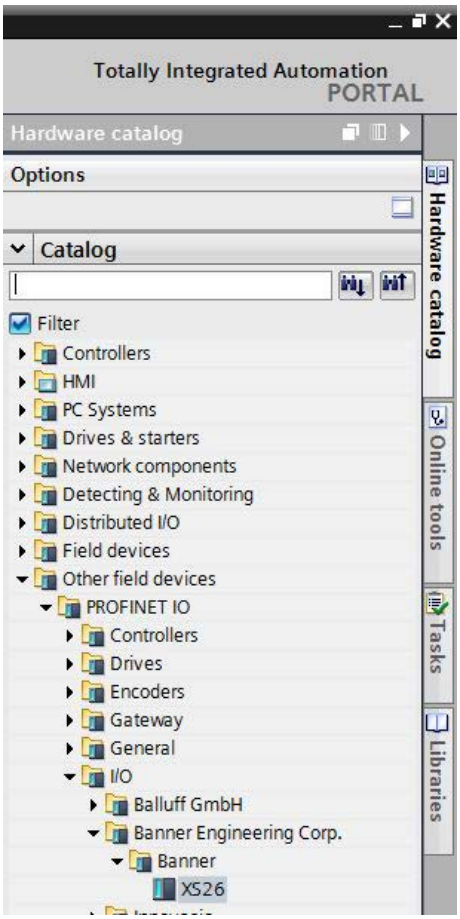
8. Klicken Sie auf die Durchsuchen-Schaltfläche **(...)** rechts neben dem Pfeil **Quellpfad**.

*Abbildung 233. GSD-Dateien verwalten*




9. Navigieren Sie zum Speicherort, in den Sie die GSD-Datei des Sicherheitskontroller heruntergeladen haben.
10. Wählen Sie die GDS-Datei des Sicherheitskontrolleraus.
11. Auf **Installieren** klicken.

*Abbildung 234. Hardware-Katalog*




Die GSD-Datei des Sicherheitskontroller wird vom System installiert und im **Hardware-Katalog** abgelegt. Im obigen Beispiel befindet sich die GSD-Datei des Sicherheitskontroller unter **Andere Feldgeräte** > **PROFINET IO** > **E/A** > **Banner Engineering Corp.** > **Banner**.

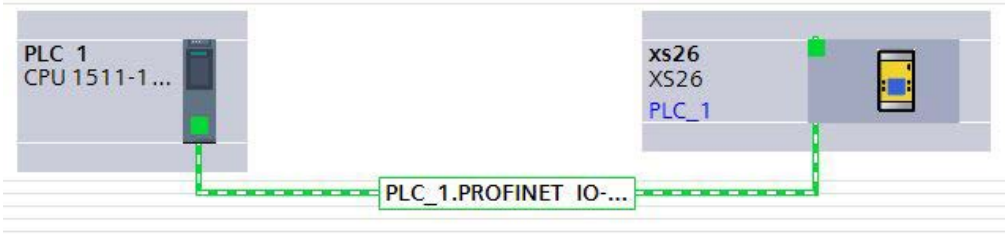
**Anmerkung:** Wenn die GSD-Datei des Sicherheitskontroller nicht richtig installiert wird, speichern Sie das Protokoll und kontaktieren Sie die Banner Engineering Corp.

## Ändern der IP-Adresse von Geräten

Ändern Sie die IP-Adresse des Sicherheitskontroller-Geräts entsprechend dieser Anleitung über die Software im TIA Portal (v13) von Siemens. Diese Anleitung können Sie als Grundlage verwenden, wenn Sie einen anderen Kontroller (SPS) verwenden.

1. Rufen Sie die Software im TIA Portal (v13) von Siemens auf.
2. Klicken Sie auf **Vorhandenes Projekt öffnen**.
3. Wählen Sie ein Projekt aus und öffnen Sie es.
4. Klicken Sie auf **Geräte und Netzwerke**, nachdem das Projekt hochgeladen wurde, um die **Netzwerkansicht** aufzurufen.

*Abbildung 235. Netzwerkansicht*

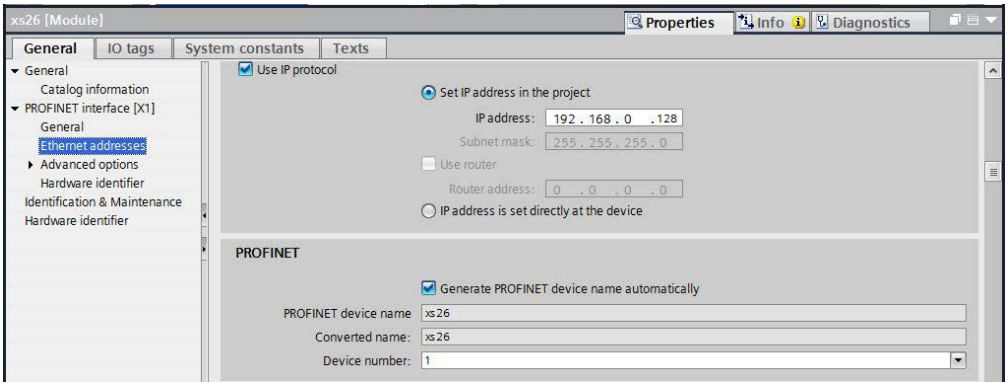



Die **Netzwerkansicht** wird angezeigt.

5. Doppelklicken Sie auf das Sicherheitskontroller, um die **Geräteansicht** zu öffnen.
6. Klicken in der **Geräteansicht** im Grafikbereich auf das Sicherheitskontroller, um das Fenster **Moduleigenschaften** zu öffnen.
   Sie können das Modul jetzt konfigurieren.

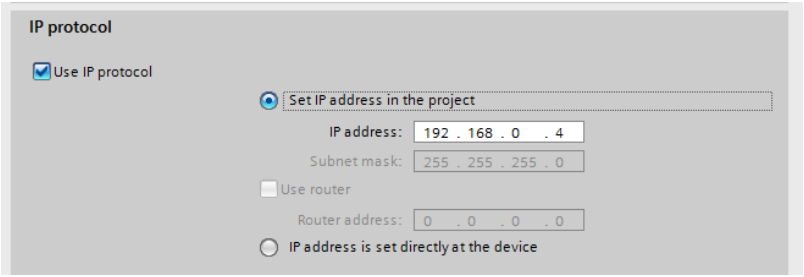
7. Klicken Sie auf **Eigenschaften**.
8. Klicken Sie auf **Allgemein**.
9. Auswählen **PROFINET-Schnittstelle** > **Ethernet-Adressen**.

*Abbildung 236. Ethernet-Adressen*




10. Wählen Sie **IP-Adresse im Projekt festlegen** aus.

*Abbildung 237. IP-Adresse festlegen*




Das Projekt legt die IP-Adresse des Geräts fest.

11. Geben Sie die IP-Adresse ein.
12. Klicken Sie mit der rechten Maustaste auf das Gerätesymbol und wählen Sie **Online und Diagnosen** aus.

*Abbildung 238. „Online und Diagnosen“ auswählen*

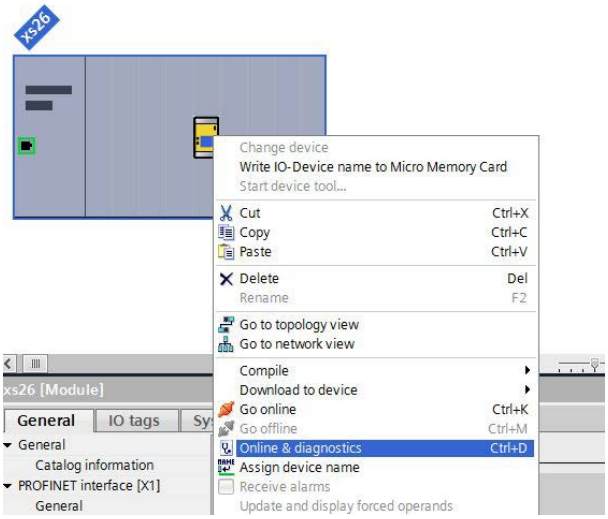
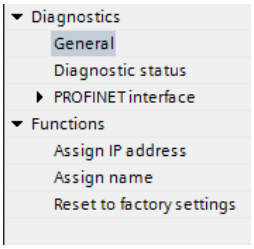


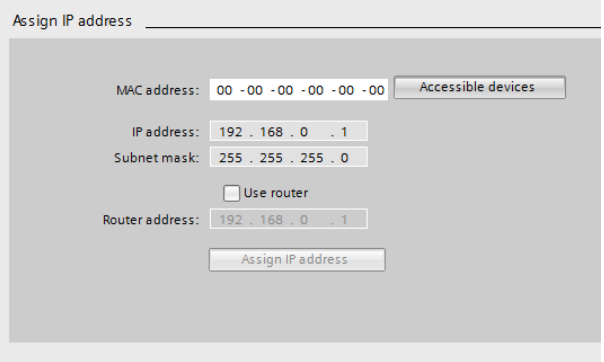

*Abbildung 239. Online und Diagnosen*




Das Fenster **Online und Diagnosen** wird angezeigt.

13. Wählen Sie **IP-Adresse zuweisen** unter **Funktionen** aus.
14. Klicken Sie auf **Zugängliche Geräte**.

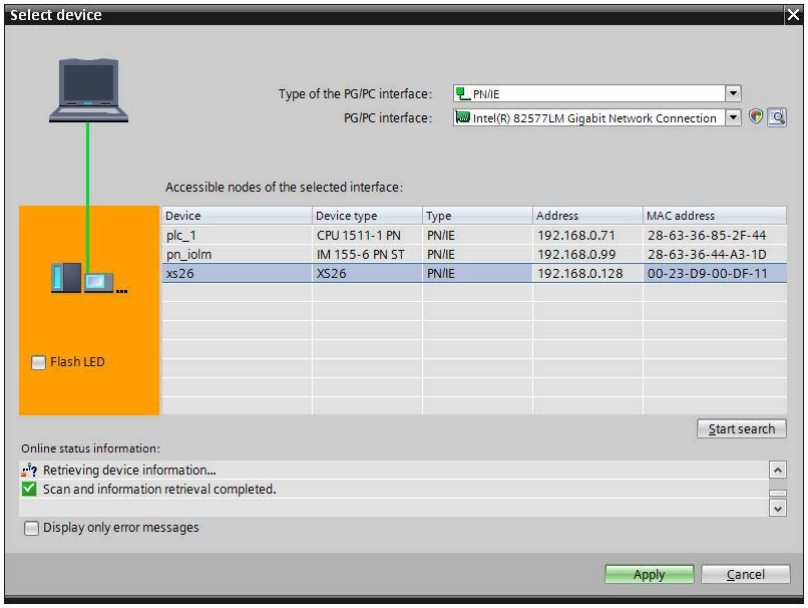
*Abbildung 240. IP-Adresse zuweisen — Zugängliche Geräte*




Im Fenster **Gerät auswählen** wird nach dem Netzwerk für verfügbare Geräte gesucht.

15. Ermitteln Sie das Gerät, das Sie anpassen möchten, anhand der MAC-Adresse und wählen Sie es aus.
16. Klicken Sie auf **Anwenden**.

*Abbildung 241. Gerät auswählen und Änderungen übernehmen*




Die IP-Adresse für das Gerät wird aktualisiert.

17. Klicken Sie auf **IP-Adresse zuweisen**, um den Schritt abzuschließen.

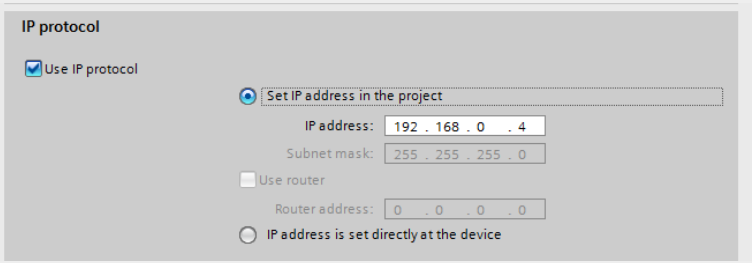
    Dieser Schritt wird für alle Geräte abgeschlossen.

**Anmerkung:** PROFINET-Geräte haben beim Starten in der Regel keine IP-Adresse (IP-Adresse = alles Nullen). Sicherheitskontroller benötigen jedoch eine IP-Adresse, um sich mit dem Sicherheitskontroller von Banner zu verbinden und die Gerätekonfiguration festzulegen.

Standardmäßig ist jeder Kamera bei Auslieferung ab Werk die IP-Adresse 192.168.0.128 zugewiesen. Die Standardadresse kann mit Sicherheitskontroller von Banner geändert werden.

Die Kamera ruft ihre IP-Adresse unmittelbar nach Aktivierung des PROFINET-Protokolls in der Kamera ab, aber bevor die SPS die Kamera erkannt und sich damit verbunden hat. Nachdem die SPS die Kamera erkannt und sich mit ihr verbunden hat, hängt das Verhalten der IP-Adresse davon ab, wie die SPS zum Zuweisen der IP-Adresse der Kamera konfiguriert wurde. Es sind zwei Konfigurationsoptionen verfügbar.

*Abbildung 242. TIA Portal (v13) von Siemens: IP-Protokoll-Optionen*




- Die IP-Adresse wird im Projekt festgelegt: Wenn die SPS angewiesen wird, die IP-Adresse der Kamera zuzuweisen (z. B. anhand der Option **IP-Adresse im Projekt festlegen** im TIA Portal von Siemens) empfängt die Kamera die spezifische Adresse. Dazu muss allerdings erst das Programm in die SPS geladen und ausgeführt werden.

  Wird die Kamera neu gestartet, nachdem sie von der SPS erkannt und konfiguriert wurde, hat sie die IP-Adresse 0.0.0.0, bis die SPS die Kamera erkannt hat und ihr die festgelegte Adresse erneut zugewiesen hat.

  Wenn der Kamera keine IP-Adresse zugewiesen ist, kann sie noch mit Sicherheitskontroller von Banner zugewiesen werden. Wenn sich diese Adresse jedoch von der in der SPS angegebenen unterscheidet, verwendet die Kamera wieder die in der SPS angegebene Adresse, sowie die SPS erneut aktiv wird.
- Die IP-Adresse wird im Gerät festgelegt: Wenn die SPS angewiesen wird, dass die IP-Adresse der Kamera im Gerät konfiguriert ist (z. B. anhand der Option **IP-Adresse ist direkt im Gerät festgelegt** im TIA Portal von Siemens) ruft die Kamera immer die über Sicherheitskontroller von Banner zugewiesene IP-Adresse ab.

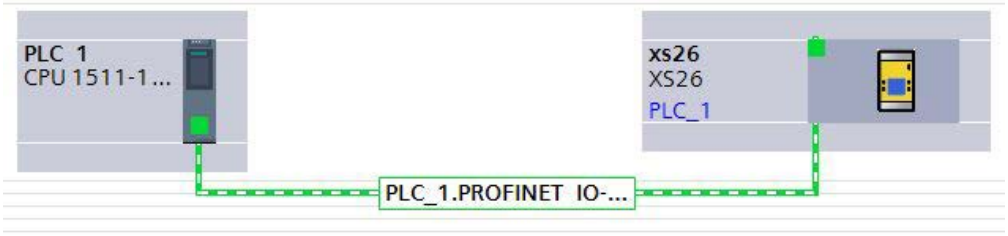
Diese Konfigurationsoptionen entsprechen der PROFINET-Norm.

## Ändern des Gerätenamens

Ändern Sie den Namen des Sicherheitskontroller-Geräts entsprechend dieser Anleitung über die Software im TIA Portal (v13) von Siemens. Diese Anleitung können Sie als Grundlage verwenden, wenn Sie einen anderen Kontroller (SPS) verwenden.

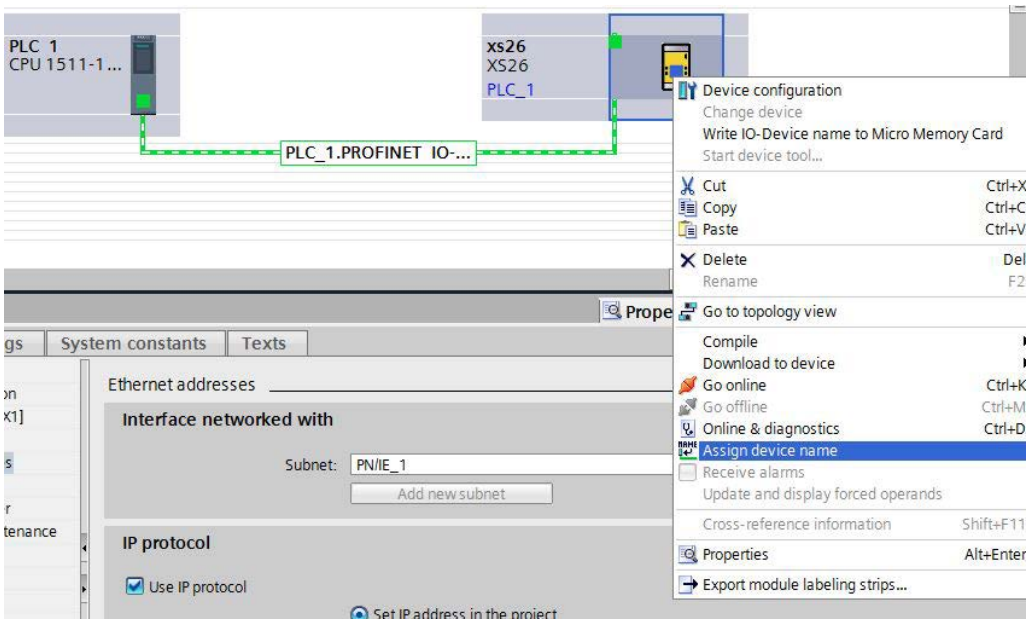
1. Öffnen Sie das Projekt und klicken Sie auf **Geräte und Netzwerke**, um die **Netzwerkansicht** aufzurufen.

   *Abbildung 243. Netzwerkansicht*

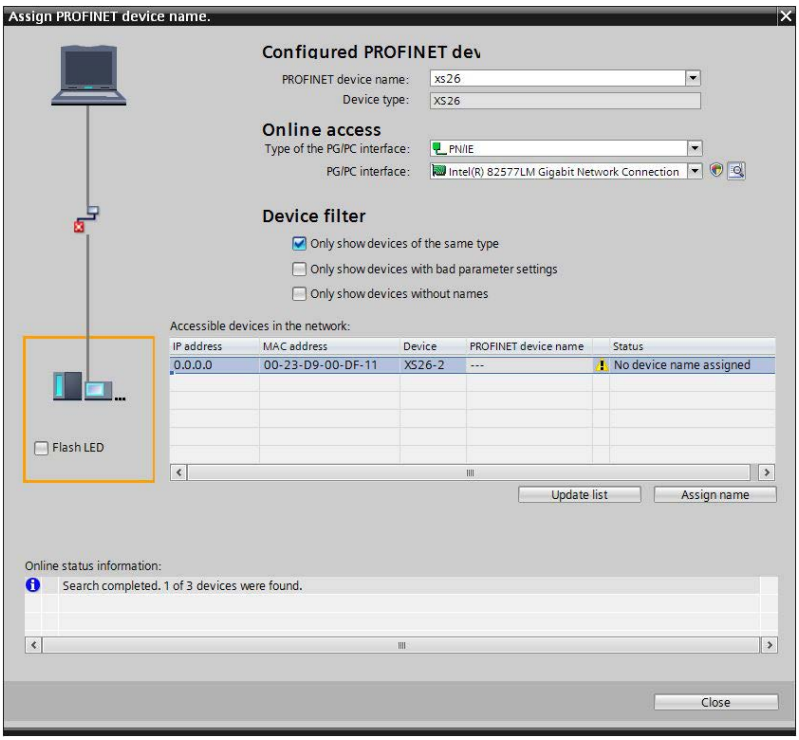
   Die **Netzwerkansicht** wird angezeigt.
2. Klicken Sie mit der rechten Maustaste auf das Sicherheitskontroller und wählen Sie **Gerätename zuweisen** aus.

*Abbildung 244. Ethernet-Adressen*




Das Fenster **PROFINET-Gerätename zuweisen** wird angezeigt und die Software sucht nach Geräten des gleichen Typs.

*Abbildung 245. Ethernet-Adressen*

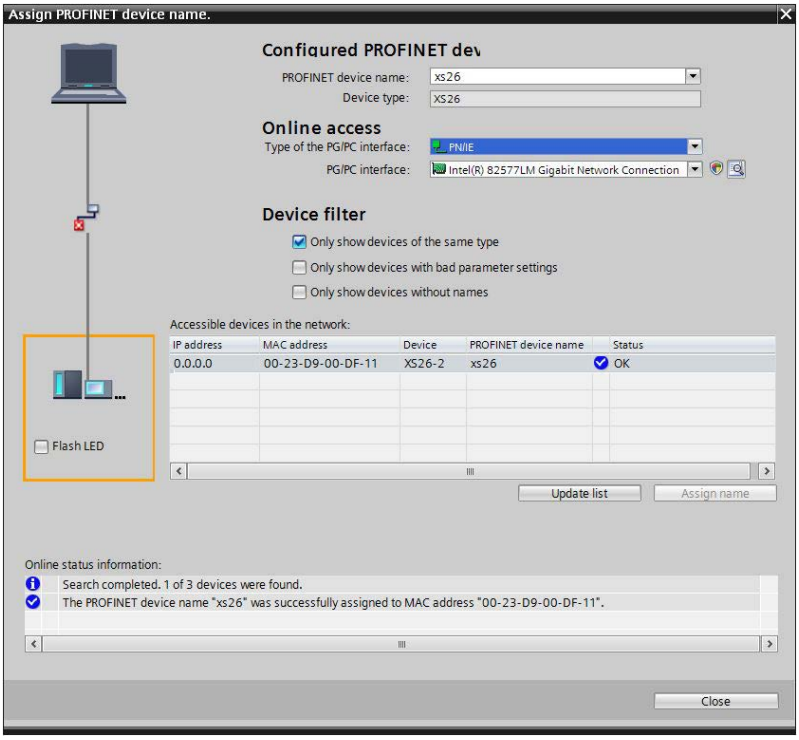



3. Geben Sie den gewünschten Namen in das Feld **PROFINET-Gerätename** ein.

**Anmerkung:** Jeder Name darf nur einmal verwendet werden.

4. Klicken Sie auf **Name zuweisen**.
   Das Gerät hat jetzt einen PROFINET-Namen.

*Abbildung 246. Ethernet-Adressen*




# 12.8 ISD: Informationen zur Umwandlung von Temperatur, Spannung und Abstand

Laden Sie eine AOI (Add-on-Anweisung) von www.bannerengineering.com herunter, die Sie in das SPS-Programm einbinden können, um die abgerufenen Werte in die echten Werte umzuwandeln.

## 12.8.1 ISD: Versorgungsspannung

Der tatsächliche Spannungswert berechnet sich aus dem an die SPS gesendeten ADC-Wert multipliziert mit 0,1835.

Betriebsspannung = ADC-Wert × 0,1835

## 12.8.2 ISD: Innentemperatur

Verschieben Sie zuerst den verbliebenen ADC-Wert um 2 Bit. Wandeln Sie dann den binären Messwert in eine Zahl um. Wenn die Zahl dem ADC-Wert der folgenden Tabelle entspricht, lesen Sie die Temperatur einfach ab. Liegt die Zahl zwischen den Messwerten in der Tabelle, berechnen Sie die tatsächliche Temperatur anhand der folgenden Formel.

```
Internal Temperature = ((A–L) / (H–L)) × 5 + T
```

**A**

der vom Kontroller bezogene ADC-Wert

**L**

der ADC-Wert in der Nachschlagetabelle kleiner oder gleich A

**H**

der ADC-Wert in der Nachschlagetabelle größer A

**T**

die mit dem L-Wert verbundene Temperatur

*Tabelle 68. Temperatur*

| ADC-Messwert | Temperatur (°C) |
|---|---|
| 41 | -40 |
| 54 | -35 |
| 69 | -30 |
| 88 | -25 |
| 110 | -20 |
| 136 | -15 |
| 165 | -10 |
| 199 | -5 |
| 237 | 0 |
| 278 | 5 |
| 321 | 10 |
| 367 | 15 |
| 414 | 20 |
| 461 | 25 |
| 508 | 30 |
| 554 | 35 |
| 598 | 40 |
| 640 | 45 |
| 679 | 50 |
| 715 | 55 |
| 748 | 60 |
| 778 | 65 |
| 804 | 70 |
| 829 | 75 |
| 850 | 80 |
| 869 | 85 |
| 886 | 90 |
| 901 | 95 |
| 914 | 100 |
| 926 | 105 |
| 936 | 110 |

## 12.8.3 ISD: Auslöserabstand

Wandeln Sie den binären Messwert in eine Zahl um. Wenn die Zahl dem ADC-Wert der folgenden Tabelle entspricht, lesen Sie den Abstand einfach ab. Liegt die Zahl zwischen den Messwerten in der Tabelle, berechnen Sie den tatsächlichen Abstand anhand der folgenden Formel.

```
Actuator Distance = ((A-L) / (H-L)) + D
```

**A**

der vom Kontroller bezogene ADC-Wert

**L**

der ADC-Wert in der Nachschlagetabelle kleiner oder gleich A

**H**

der ADC-Wert in der Nachschlagetabelle größer A

**D**

der Abstand im Zusammenhang mit dem L-Wert

*Tabelle 69. Abstand*

| ADC-Messwert | Abstand (mm) |
|---|---|
| <62 | <7 |
| 62 | 7 |
| 65 | 8 |
| 77 | 9 |
| 110 | 10 |
| 133 | 11 |
| 148 | 12 |
| 158 | 13 |
| 163 | 14 |
| 169 | 15 |
| 172 | 16 |
| 176 | 17 |
| 180 | 18 |
| >180 | >18 |

# 13 Systemüberprüfung

## 13.1 Zeitplan für vorgeschriebene Überprüfungen

Zur Überprüfung der Konfiguration und der Funktionsfähigkeit des Sicherheitskontrollers gehört die Kontrolle jedes Sicherheits- und nicht sicherheitsrelevanten Eingangsgeräts zusammen mit jedem Ausgangsgerät. Während die Eingänge einzeln vom Ein-Zustand in den Aus-Zustand geschaltet werden, muss überprüft werden, ob die Sicherheitsausgänge wie erwartet ein- und ausschalten.

Banner Engineering empfiehlt dringend, die Überprüfungen wie beschrieben durchzuführen. Eine Fachkraft (oder ein Team aus Fachkräften) sollte jedoch diese allgemeinen Empfehlungen im Hinblick auf die konkrete Anwendung überprüfen und über die geeignete Häufigkeit der Überprüfungen entscheiden. Dies ergibt sich in der Regel aus einer Risikobewertung, wie z. B. der in ANSI B11.0 beschriebenen. Aus dem Ergebnis der Risikobewertung ergibt sich die Häufigkeit und der Inhalt der regelmäßigen Überprüfungsroutinen, die einzuhalten sind.

**WARNUNG: Die Maschine nicht einsetzen, solange das System nicht richtig funktioniert.**

**Wenn nicht alle diese Kontrollen durchgeführt werden können, ist von der Benutzung des Sicherheitssystems abzusehen**, das die Banner-Vorrichtung und die überwachte Maschine enthält, bis der Defekt bzw. das Problem behoben wurde. **Der Versuch, die überwachte Maschine unter derartigen Bedingungen zu benutzen, kann schwere oder tödliche Verletzungen zur Folge haben.**

Der Betrieb des Sicherheitskontrollers und die Funktionalität der vorgesehenen Konfiguration müssen eingehend getestet werden. Setup vor der Inbetriebnahme, Inbetriebnahme und regelmäßige Prüfroutinen auf Seite 252 soll bei der Entwicklung einer maßgeschneiderten (konfigurationsspezifischen) Checkliste für jede Anwendung helfen. Diese spezifische Checkliste muss dem Wartungspersonal für die Inbetriebnahmeprüfung und regelmäßige Funktionstests zur Verfügung gestellt werden. Eine ähnliche, vereinfachte Checkliste für die tägliche Überprüfungsroutine sollte für den Bediener (bzw. für die autorisierte Person [41]) angefertigt werden. Es wird dringend empfohlen, für die Prüfungsverfahren Kopien der Anschlussdiagramme, der Schaltpläne und der Konfigurationszusammenfassung bereitzuhalten.

**WARNUNG:**

- **Regelmäßige Überprüfungen durchführen**
- Wenn diese Überprüfungen nicht durchgeführt werden, kann eine Gefahrensituation verursacht werden, die zu schweren oder tödlichen Verletzungen führen könnte.
- Die Inbetriebnahmeprüfung sowie regelmäßige und tägliche Überprüfungen am Sicherheitssystem müssen zu den vorgesehenen Zeitpunkten von qualifiziertem Personal durchgeführt werden, um sicherzustellen, dass das Sicherheitssystem bestimmungsgemäß funktioniert.

**Inbetriebnahmeprüfung:** Eine sachkundige Person [41] muss eine Inbetriebnahmeprüfung am Sicherheitssystem durchführen, bevor die Sicherheitsstromkreise der überwachten Maschine in Betrieb genommen werden können, sowie nach jeder Einrichtung oder Änderung der Konfiguration des Sicherheitskontrollers.

**Regelmäßige (halbjährliche) Überprüfung:** Eine sachkundige Person [41] muss auch halbjährlich (alle 6 Monate) oder in regelmäßigen Zeitabständen entsprechend den geltenden örtlichen bzw. nationalen Vorschriften eine erneute Inbetriebnahmeprüfung am Sicherheitssystem durchführen.

**Tägliche Funktionstests:** Eine befähigte Person [41] muss auch an jedem Einsatztag der überwachten Maschine die korrekte Funktion der Risikominderungsmaßnahmen entsprechend den Herstellerempfehlungen überprüfen.

**WARNUNG: Bevor die Maschine eingeschaltet wird**

Stellen Sie sicher, dass sich im überwachten Bereich kein Personal und keine unerwünschten Materialien befinden (z. B. Werkzeuge), bevor die Stromversorgung zur überwachten Maschine eingeschaltet wird. **Wenn diese Anweisungen nicht befolgt werden, können schwere oder tödliche Verletzungen die Folge sein.**

## 13.2 Inbetriebnahmeprüfung

**Überprüfen Sie vor der Durchführung des Verfahrens Folgendes:**

- Keiner der Transistor- und Relaisausgangsanschlüsse des gesamten Sicherheitskontrollersystems darf mit der Maschine verbunden sein. Es ist ratsam, alle steckbaren Anschlüsse am Sicherheitsausgang des Sicherheitskontrollers zu trennen.
- Die Stromversorgung muss von der Maschine getrennt worden sein, und es darf keine Stromverbindung zu den Bedienelementen oder Antrieben der Maschine bestehen.

Die permanenten Anschlüsse werden zu einem späteren Zeitpunkt verbunden.

[41] Unter Glossar auf Seite 297 finden Sie Definitionen.

## 13.2.1 Überprüfung des Systembetriebs

**Die Inbetriebnahmeprüfung muss von einer qualifizierten Person durchgeführt werden.** [42] **Sie darf erst nach der Konfiguration des Sicherheitskontrollers und nach der sachgemäßen Installation und Konfiguration** der mit den Eingängen des Kontrollers verbundenen Sicherheitssysteme und Schutzeinrichtungen ausgeführt werden (siehe Optionen für Sicherheitseingangsgeräte auf Seite 33 und die einschlägigen Normen).

Die Inbetriebnahmeprüfung muss in den folgenden beiden Fällen durchgeführt werden:

1. Wenn der Sicherheitskontroller zum ersten Mal installiert wird, um die korrekte Installation sicherzustellen.
2. Jedes Mal, wenn Wartungsarbeiten oder Änderungen am System oder an der durch das System überwachten Maschine vorgenommen werden, damit die korrekte Funktion des Sicherheitskontrollers dauerhaft gewährleistet wird (siehe Zeitplan für vorgeschriebene Überprüfungen auf Seite 251).

**Während des ersten Teils der Inbetriebnahmeprüfung müssen der Sicherheitskontroller und angeschlossene Sicherheitssysteme überprüft werden, ohne dass die Stromversorgung zur überwachten Maschine hergestellt wurde.** Die endgültigen Anschlüsse an die überwachte Maschine dürfen erst vorgenommen werden, nachdem diese Systeme überprüft worden sind.

**Folgendes überprüfen:**

- **Die Sicherheitsausgangsleitungen sind isoliert** (d. h. nicht untereinander und nicht zu stromführenden Leitungen oder zu Erde kurzgeschlossen).
- Sofern sie verwendet werden, müssen die Anschlüsse der externen Geräteüberwachung (EDM) über die Öffner-Überwachungskontakte der mit den Sicherheitsausgängen verbundenen Geräte an +24 V DC angeschlossen sein, wie in der Beschreibung in Externe Geräteüberwachung (EDM) auf Seite 67 und in den Schaltplänen angegeben.
- Die korrekte Sicherheitskontroller-Konfigurationsdatei für Ihre Anwendung wurde im Sicherheitskontroller installiert.
- Alle Anschlüsse wurden gemäß den entsprechenden Abschnitten verbunden und erfüllen die NEC-Vorschriften sowie die örtlichen Vorschriften für elektrische Anschlüsse.

Dadurch wird ermöglicht, dass der Sicherheitskontroller und die angeschlossenen Sicherheitssysteme separat überprüft werden können, bevor permanente Anschlüsse mit der überwachten Maschine verbunden werden.

## 13.2.2 Setup vor der Inbetriebnahme, Inbetriebnahme und regelmäßige Prüfroutinen

In der Phase der ersten Konfigurationsüberprüfung gibt es zwei Möglichkeiten der Überprüfung, dass die Sicherheitsausgänge den Status zu den vorgesehenen Zeiten wechseln (öffnen Sie die Registerkarte **Konfigurationsübersicht** in der Software, um den Anlauftest und die Konfigurationseinstellungen für Netzeinschaltung anzuzeigen):

- Beobachten Sie die den Ein- und Ausgängen zugeordneten LEDs. Leuchtet die Eingangs-LED grün, ist der Eingang eingeschaltet (bzw. 24 V). Leuchtet die Eingangs-LED rot, ist der Eingang ausgeschaltet (bzw. 0 V). Analog leuchtet die entsprechende LED grün, wenn die RO1- und RO2-Ausgangskontakte geschlossen sind. Sind die Kontakte hingegen geöffnet, leuchtet die LED rot.
- Starten Sie den **Live-Modus** in der Software (der Sicherheitskontroller muss eingeschaltet und mit einem SC-USB2-Kabel an den PC angeschlossen sein).

### Hochlaufkonfiguration

Bei der Netzeinschaltung schalten sich die mit Zweihandsteuerungs-, Überbrückungs-, Pressensteuerungs- oder Zustimmtasterfunktionen verbundenen Ausgänge nicht ein. Nach der Netzeinschaltung müssen diese Vorrichtungen in den Aus-Zustand und wieder in den Ein-Zustand geschaltet werden, damit sich ihre zugehörigen Ausgänge einschalten.

Für die Pressesteuerungsfunktion führen Sie das in Pressensteuerung (XS/SC26-2 ab FID 4) auf Seite 144 erörterte Verfahren durch.

**Bei Konfiguration für normale Netzeinschaltung**

Wenn die Verriegelungsfunktion nicht verwendet wird: Überprüfen Sie, dass sich die Sicherheitsausgänge nach der Netzeinschaltung einschalten.

Wenn ein Eingangsgerät oder ein Ausgang die Verriegelungsfunktion verwendet: Überprüfen Sie, dass die Sicherheitsausgänge nach der Netzeinschaltung erst eingeschaltet werden, wenn die spezifischen manuellen Latch-Reset-Vorgänge ausgeführt wurden.

**Bei Konfiguration für automatische Netzeinschaltung**

Überprüfen Sie, dass alle Sicherheitsausgänge innerhalb von ca. 7 Sekunden eingeschaltet werden (Ausgänge mit aktivierter Einschaltverzögerung schalten sich möglicherweise später ein).

[42] Für Definitionen siehe Glossar auf Seite 297.

**Bei Konfiguration für manuelle Netzeinschaltung**

Überprüfen Sie, ob alle Sicherheitsausgänge nach der Netzeinschaltung AUS bleiben.

Waren Sie mindestens 10 Sekunden nach der Netzeinschaltung und führen Sie den Reset für manuelle Netzeinschaltung aus.

Überprüfen Sie, dass die Sicherheitsausgänge eingeschaltet werden (Ausgänge mit aktivierter Einschaltverzögerung schalten sich möglicherweise später ein).

**VORSICHT: Überprüfung der Funktion der Eingänge und Ausgänge**

Die qualifizierte Person ist dafür verantwortlich, die Eingangsgeräte durchzuschalten (Ein-Zustand und Aus-Zustand), um zu überprüfen, dass sich die Sicherheitsausgänge ein- und ausschalten, um die beabsichtigten Schutzfunktionen unter normalen Betriebsbedingungen und vorhersehbaren Fehlerbedingungen auszuführen. Die Konfiguration der einzelnen Sicherheitskontroller muss sorgfältig beurteilt und getestet werden, um sicherzustellen, dass eine Unterbrechung der Stromversorgung für ein Schutzeingangsgerät, den Sicherheitskontroller oder das invertierte Eingangssignal von einem Schutzeingangsgerät keinen unbeabsichtigten Ein-Zustand, Muting-Zustand oder Überbrückungszustand der Sicherheitsausgänge verursachen.

**Anmerkung:** Blinkt die Anzeige für einen Ein- oder Ausgang rot, siehe Fehlerbehebung auf Seite 278.

## Betrieb der Sicherheitseingangsgeräte (Not-Aus-Schalter, Seilzugschalter, Optosensor, Sicherheitsmatte, Schutzhalt)

1. Betätigen Sie bei eingeschalteten zugehörigen Sicherheitsausgängen jedes Sicherheitseingangsgerät einzeln jeweils ein Mal.
2. Stellen Sie sicher, dass sich jeder zugehörige Sicherheitsausgang mit der richtigen Ausschaltverzögerung, soweit zutreffend, ausschaltet.
3. Während sich die Sicherheitsvorrichtung im Ein-Zustand befindet:
   - **Falls ein Sicherheitseingangsgerät mit einer Latch-Reset-Funktion konfiguriert ist:**
     1. Prüfen Sie, ob alle Sicherheitsausgänge ausgeschaltet bleiben.
     2. Führen Sie einen Latch-Reset durch, um die Ausgänge einzuschalten.
     3. Prüfen Sie, ob sich die einzelnen Sicherheitsausgänge einschalten.
   - **Wenn keine Latch-Reset-Funktionen verwendet werden**: Prüfen Sie, ob sich der Sicherheitsausgang einschaltet.

**Wichtig:** Testen Sie die Schutzeinrichtungen immer unter Beachtung der Empfehlungen des Herstellers der jeweiligen Einrichtung.

**Bei der nachfolgenden Abfolge der Schritte gilt: Gehört eine bestimmte Funktion oder Vorrichtung nicht zu der Anwendung, überspringen Sie den Schritt und gehen Sie weiter zum nächsten Punkt auf der Checkliste oder zum letzten Inbetriebnahmeschritt.**

## Zweihandsteuerungsfunktion ohne Muting

1. Achten Sie darauf, dass sich die Bedienelemente der Zweihandsteuerung im Aus-Zustand befinden.
2. Achten Sie darauf, dass sich alle anderen mit der Zweihandsteuerungsfunktion verbundenen Eingänge im Ein-Zustand befinden, und aktivieren Sie die Bedienelemente der Zweihandsteuerung, um den verbundenen Sicherheitseingang einzuschalten.
3. Überprüfen Sie, dass der verbundene Sicherheitsausgang ausgeschaltet bleibt, sofern nicht beide Bedienelemente im Abstand von 0,5 Sekunden aktiviert werden.
4. Überprüfen Sie, dass sich der Sicherheitsausgang ausschaltet und ausgeschaltet bleibt, wenn eine Hand entfernt und wieder aufgelegt wird (während das andere Bedienelement im Ein-Zustand verbleibt).
5. Überprüfen Sie, dass das Schalten eines Sicherheitseingangs (kein Bedienelement der Zweihandsteuerung) in den Aus-Zustand dazu führt, dass der verbundene Sicherheitsausgang ausgeschaltet wird bzw. ausgeschaltet bleibt.
6. Werden mehrere Bedienelementepaare von Zweihandsteuerungen verwendet, müssen die zusätzlichen Bedienelemente aktiviert werden, bevor sich der Sicherheitsausgang einschaltet. Überprüfen Sie, dass sich der Sicherheitsausgang ausschaltet und ausgeschaltet bleibt, wenn eine Hand entfernt und wieder aufgelegt wird (während das andere Bedienelement im Ein-Zustand verbleibt).

## Zweihandsteuerungsfunktion mit Muting

1. Führen Sie die oben beschriebenen Überprüfungsschritte für die Zweihandsteuerungsfunktion aus.
2. Aktivieren Sie die beiden Bedienelemente der Zweihandsteuerung und aktivieren Sie dann die MP1-Sensoren.
3. Entfernen Sie bei aktivierten MSP1-Sensoren die Hände von der Zweihandsteuerung und überprüfen Sie, ob der Sicherheitsausgang eingeschaltet bleibt.

4. Prüfen Sie, ob alle Sicherheitsausgänge ausgeschaltet bleiben, wenn eine der folgenden Bedingungen eintritt:
   - Die MSP1-Sensoren werden in den Aus-Zustand geschaltet.
   - Das Muting-Zeitlimit läuft ab.
5. Bei mehreren Bedienelementen für Zweihandsteuerungen mit mindestens einem Paar nicht mutingfähiger Bedienelemente: Vergewissern Sie sich, dass sich die Sicherheitsausgänge beim Entfernen von einer oder beiden Händen von den einzelnen nicht gemuteten Bedienelementen während eines aktiven Muting-Zyklus ausschalten.

## Bidirektionale (2-Wege-)Muting-Funktion (gilt auch für Muting-Funktion von Bereichssteuerungen)

1. Aktivieren Sie bei gemuteter Schutzeinrichtung im Ein-Zustand den Muting-Aktivierungseingang (sofern verwendet), und aktivieren Sie dann jeden Muting-Sensor der Reihe nach innerhalb von 3 Sekunden.
2. Generieren Sie einen Stoppbefehl von der gemuteten Schutzeinrichtung:
   a) Prüfen Sie, ob die zugehörigen Sicherheitsausgänge eingeschaltet bleiben.
   b) Falls ein Muting-Zeitlimit konfiguriert wurde, überprüfen Sie, ob die zugehörigen Sicherheitsausgänge ausgeschaltet werden, wenn der Muting-Zeitgeber abläuft.
   c) Wiederholen Sie die oben genannten Schritte für jedes Muting-Sensorpaar.
   d) Überprüfen Sie die einzelnen gemuteten Schutzeinrichtungen auf den ordnungsgemäßen Funktionsbetrieb.
   e) Generieren Sie jeweils einzeln einen Stoppbefehl von den nicht gemuteten Schutzeinrichtungen, während sich die Einrichtungen im Muting-Zyklus befinden, und überprüfen Sie, ob sich die zugehörigen Sicherheitsausgänge ausschalten.
   f) Überprüfen Sie den Muting-Vorgang in umgekehrter Richtung, indem Sie den oben beschriebenen Prozess wiederholen, die Muting-Sensoren jedoch in umgekehrter Reihenfolge aktivieren.

## Unidirektionale (1-Weg-)Muting-Funktion

1. Bei nicht aktivierten Muting-Sensoren, gemuteten Schutzeinrichtungen im Ein-Zustand und eingeschalteten Sicherheitsausgängen:
   a) Aktivieren Sie das Muting-Sensorpaar 1.
   b) Schalten Sie die gemutete Schutzeinrichtung in den Aus-Zustand.
   c) Aktivieren Sie das Muting-Sensorpaar 2.
   d) Deaktivieren Sie das Muting-Sensorpaar 1.
2. Überprüfen Sie, dass der zugehörige Sicherheitsausgang während des gesamten Prozesses im Aus-Zustand verbleibt.
3. Wiederholen Sie den Test in die *falsche Richtung* (Muting-Sensorpaar 2, dann Schutzeinrichtung, dann Muting-Sensorpaar 1).
4. Überprüfen Sie, dass sich der Ausgang ausschaltet, wenn die Schutzeinrichtung in den Aus-Zustand wechselt.

## Wenn ein Muting-Zeitlimit konfiguriert wurde

Überprüfen Sie, dass sich die zugehörigen Sicherheitsausgänge ausschalten, wenn der Muting-Zeitgeber abläuft.

## Muting-Funktion mit Netzeinschaltungsbetrieb (gilt nicht für Zweihandsteuerung)

1. Schalten Sie die Netzstromzufuhr des Sicherheitskontrollers aus.
2. Aktivieren Sie den Muting-Aktivierungseingang (soweit verwendet).
3. Aktivieren Sie ein geeignetes Muting-Sensorpaar zum Starten eines Muting-Zyklus.
4. Achten Sie darauf, dass sich alle mutingfähigen Schutzeinrichtungen im Ein-Zustand befinden.
5. Schalten Sie die Spannungsversorgung zum Sicherheitskontroller ein.
6. Überprüfen Sie, das sich der Sicherheitsausgang einschaltet und dass ein Muting-Zyklus beginnt.
7. Wiederholen Sie diesen Test mit der mutingfähigen Schutzeinrichtung im Aus-Zustand.
8. Prüfen Sie, ob der Sicherheitsausgang ausgeschaltet bleibt.

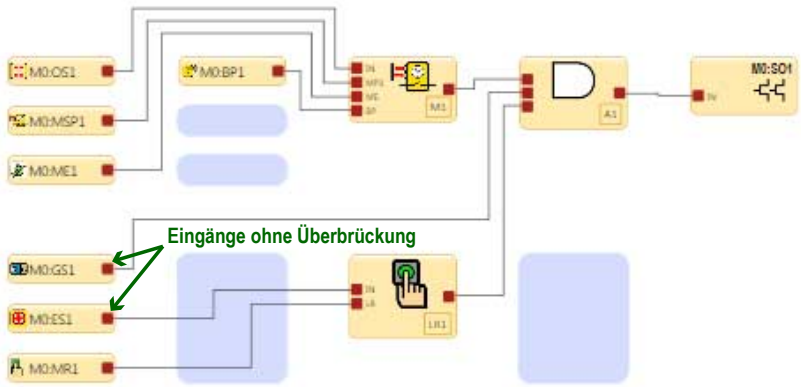
## Muting-Funktion mit mutingabhängigem Override

1. Achten Sie darauf, dass die Muting-Sensoren nicht aktiviert sind und dass sich die Muting-Schutzeinrichtungen im Ein-Zustand befinden.
2. Prüfen Sie, ob die zugehörigen Sicherheitsausgänge eingeschaltet sind.
3. Schalten Sie die Schutzeinrichtung in den Aus-Zustand.
4. Prüfen Sie, ob der Sicherheitsausgang ausgeschaltet wird.

5. Aktivieren Sie einen der Muting-Sensoren.
6. Überprüfen Sie, ob die optionale Muting-Leuchte blinkt.
7. Starten Sie das mutingabhängige Override durch Aktivieren des Überbrückungsschalters.
8. Prüfen Sie, ob der Sicherheitsausgang eingeschaltet wird.
9. Prüfen Sie, ob der Sicherheitsausgang ausgeschaltet wird, wenn eine der folgenden Bedingungen gegeben ist:
   - Zeitlimit für Überbrückung (Override) läuft ab
   - Die Muting-Sensoren werden deaktiviert.
   - Die Überbrückungsvorrichtung wird deaktiviert.

## Muting-Funktion mit Überbrückung

1. Prüfen Sie, ob sich jeder Sicherheitseingang, der gemutet oder überbrückt werden kann, im Aus-Zustand befindet.
2. Wenn der Überbrückungsschalter im Ein-Zustand ist, prüfen Sie Folgendes:
   a) Ob sich die zugehörigen Sicherheitsausgänge einschalten.
   b) Ob sich die zugehörigen Sicherheitsausgänge ausschalten, wenn der Überbrückungs-Zeitgeber abläuft.
3. Schalten Sie den Überbrückungsschalter in den Ein-Zustand und prüfen Sie, ob sich die zugehörigen Sicherheitsausgänge einschalten.
4. Schalten Sie die zugehörigen nicht überbrückten Eingangsgeräte (jeweils einzeln) in den Aus-Zustand und prüfen Sie, ob sich die zugehörigen Sicherheitsausgänge ausschalten, während sich der Überbrückungsschalter im Ein-Zustand befindet.




## Überbrückungsfunktion

1. Prüfen Sie, ob die zugehörigen Sicherheitsausgänge ausgeschaltet sind, wenn sich die zu überbrückenden Sicherheitseingänge im Aus-Zustand befinden.
2. Wenn der Überbrückungsschalter im Ein-Zustand ist, prüfen Sie Folgendes:
   a) Ob sich die zugehörigen Sicherheitsausgänge einschalten.
   b) Ob sich die zugehörigen Sicherheitsausgänge ausschalten, wenn der Überbrückungs-Zeitgeber abläuft.
3. Schalten Sie den Überbrückungsschalter in den Ein-Zustand und prüfen Sie, ob sich die zugehörigen Sicherheitsausgänge einschalten.
4. Schalten Sie die nicht überbrückten Eingangsgeräte einzeln der Reihe nach in den Aus-Zustand und prüfen Sie, ob sich die zugehörigen Sicherheitsausgänge ausschalten, während sich der Überbrückungsschalter im Ein-Zustand befindet.

## Ausschaltverzögerungsfunktion für Sicherheitsausgänge

1. Prüfen Sie bei einem der Steuereingänge im Aus-Zustand und beim verzögerten Sicherheitsausgang im Ausschaltverzögerungszustand, ob sich der Sicherheitsausgang ausschaltet, nachdem die Zeitverzögerung abgelaufen ist.
2. Schalten Sie bei einem der Steuereingänge im Aus-Zustand und aktivem Ausschaltverzögerungszeitgeber den Eingang in den Ein-Zustand und prüfen Sie, ob der Sicherheitsausgang eingeschaltet ist und bleibt.

## Ausschaltverzögerungsfunktion für Sicherheitsausgänge – Abbruchverzögerungseingang

Aktivieren Sie den Abbruchverzögerungseingang, während sich die zugehörigen Eingänge im Aus-Zustand befinden und während sich der verzögerte Sicherheitsausgang im Ausschaltverzögerungszustand befindet, und prüfen Sie, ob sich der Sicherheitsausgang sofort ausschaltet.

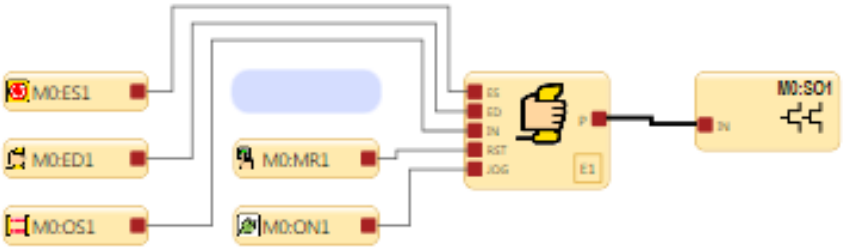
## Ausschaltverzögerungsfunktion für Sicherheitsausgänge – Steuereingänge

1. Schalten Sie bei einem der Steuereingänge im Aus-Zustand und während sich der verzögerte Sicherheitsausgang im Ausschaltverzögerungszustand befindet, den Eingang in den Ein-Zustand.
2. Prüfen Sie, ob der Sicherheitsausgang eingeschaltet wird und eingeschaltet bleibt.

## Ausschaltverzögerungsfunktion für Sicherheitsausgänge und Latch-Reset

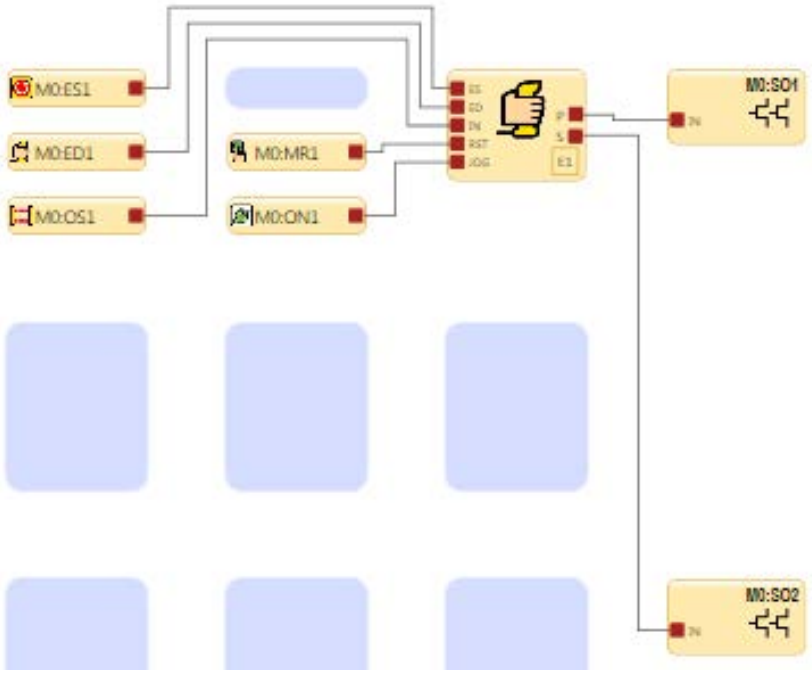
1. Achten Sie darauf, dass sich die zugehörigen Eingangsgeräte im Ein-Zustand befinden, so dass der verzögerte Sicherheitsausgang eingeschaltet ist.
2. Starten Sie die Ausschaltverzögerungszeit, indem Sie ein Eingangsgerät in den Aus-Zustand schalten.
3. Schalten Sie das Eingangsgerät während der Ausschaltverzögerungszeit erneut in den Ein-Zustand und drücken Sie die Reset-Taste.
4. Prüfen Sie, ob sich der verzögerte Ausgang am Ende der Verzögerung ausschaltet und ob er ausgeschaltet bleibt (ein Latch-Reset-Signal während der Verzögerungszeit wird ignoriert).

## Zustimmtasterfunktion ohne sekundären Weiterschaltausgang




1. Prüfen Sie, während sich die zugehörigen Eingänge im Ein-Zustand befinden und sich der Zustimmtaster im Aus-Zustand befindet, ob der Sicherheitsausgang eingeschaltet ist.
2. Prüfen Sie, während sich der Zustimmtaster noch im Ein-Zustand befindet und der zugehörige Sicherheitsausgang eingeschaltet ist, ob sich der Sicherheitsausgang bei Ablauf des Zustimmtaster-Zeitgebers ausschaltet.
3. Schalten Sie den Zustimmtaster zurück in den Aus-Zustand und dann wieder in den Ein-Zustand und prüfen Sie, ob sich die Sicherheitsausgänge einschalten.
4. Schalten Sie den Zustimmtaster in den Aus-Zustand und prüfen Sie, ob sich die zugehörigen Sicherheitsausgänge ausschalten.
5. Schalten Sie die einzelnen mit der Zustimmtasterfunktion verbundenen Not-Aus- und Seilzugschalter in den Aus-Zustand und prüfen Sie jeweils der Reihe nach, ob die zugehörigen Sicherheitsausgänge eingeschaltet sind und sich im Freigabe-Modus befinden.
6. Führen Sie einen Reset durch, während sich der Zustimmtaster im Aus-Zustand befindet.
7. Überprüfen Sie, ob die Steuerung jetzt auf den zugehörigen Eingangsgeräten der Zustimmtasterfunktion basiert:
   a) Wenn sich ein oder mehrere Eingangsgeräte im Aus-Zustand befinden, prüfen Sie, ob der Ausgang ausgeschaltet ist.
   b) Wenn sich alle Eingangsgeräte im Ein-Zustand befinden, prüfen Sie, ob der Ausgang eingeschaltet ist.

## Zustimmtasterfunktion – Mit Weiterschaltfunktion am Sekundärausgang




1. Prüfen Sie, während sich der Zustimmtaster und die Weiterschalttaste im Ein-Zustand befinden und den primären Sicherheitsausgang steuern, ob sich der Ausgang ausschaltet, wenn entweder der Zustimmtaster oder die Weiterschalttaste in den Aus-Zustand geschaltet werden.
2. Prüfen Sie, während der Zustimmtaster den primären Sicherheitsausgang steuert und die Weiterschalttaste den Sekundärausgang steuert, ob der primäre Ausgang folgende Schaltungen vornimmt:
   a) Einschaltung, wenn sich der Zustimmtaster im Ein-Zustand befindet.
   b) Ausschaltung, wenn sich der Zustimmtaster im Aus-Zustand die Weiterschalttaste im Ein-Zustand befindet.
3. Prüfen Sie, ob sich der Ausgang nur dann einschaltet, wenn sich der Zustimmtaster im Ein-Zustand befindet und sich die Weiterschalttaste im Ein-Zustand befindet.
4. Prüfen Sie, ob der Sekundärausgang folgende Schaltungen ausführt:
   a) Einschaltung, wenn sich der Zustimmtaster und die Weiterschalttaste im Ein-Zustand befinden.
   b) Ausschaltung, wenn sich der Zustimmtaster oder die Weiterschalttaste im Aus-Zustand befindet.

## Pressensteuerungs-Funktionsblock mit konfigurierter Einzelauslösersteuerung

1. Vergewissern Sie sich, dass der nicht mutingfähige Sicherheitseingang, der mutingfähige Sicherheitsstopp-Eingang (sofern konfiguriert) und TOS eingeschaltet sind.
2. Führen Sie einen Reset-Zyklus durch.
3. Schalten Sie den GO-Eingang vorübergehend ein. Überprüfen Sie, ob die Abwärtsbewegung beginnt.
4. Blockieren Sie den Eingang für den mutingfähigen Sicherheitsstopp mit einem Testobjekt. Überprüfen Sie, ob die Abwärtsbewegung angehalten wird.
5. Löschen Sie den Eingang für den mutingfähigen Sicherheitsstopp und führen Sie einen Reset-Zyklus durch.
6. Schalten Sie den GO-Eingang vorübergehend ein. Überprüfen Sie, ob der Stößel auf die TOS-Position angehoben wird und dort stehenbleibt.
7. Schalten Sie den GO-Eingang vorübergehend ein. Überprüfen Sie, ob sich der Stößel nach unten bewegt.
8. Wenn der Stößel den BOS-Punkt erreicht und seine Aufwärtsbewegung beginnt, blockieren Sie den Eingang für den mutingfähigen Sicherheitsstopp mit dem Testobjekt. Prüfen Sie, ob sich der Stößel weiter nach oben bis zur TOS-Position bewegt.

## Pressensteuerungs-Funktionsblock mit konfigurierter Einstellung für den manuellen Aufwärtshub

1. Vergewissern Sie sich, dass der nicht mutingfähige Sicherheitseingang, der mutingfähige Sicherheitseingang und TOS eingeschaltet sind.
2. Führen Sie einen Reset-Zyklus durch, schalten Sie PIP ein (falls verwendet) und aktivieren Sie dann den GO-Eingang. Überprüfen Sie, ob der Abwärts-Ausgang eingeschaltet ist.
3. Deaktivieren Sie den GO-Eingang. Überprüfen Sie, ob der Abwärts-Ausgang ausgeschaltet ist.
4. Aktivieren Sie den GO-Eingang. Der Abwärts-Ausgang sollte wieder eingeschaltet werden.

5. Blockieren Sie den Eingang für den mutingfähigen Sicherheitsstopp mit einem Testobjekt. Überprüfen Sie, ob die Abwärtsbewegung angehalten wird.
6. Löschen Sie den Eingang für den mutingfähigen Sicherheitsstopp und führen Sie einen Reset-Zyklus durch.
7. Aktivieren Sie den GO-Eingang. Überprüfen Sie, ob der Stößel auf die TOS-Position angehoben wird und dort stehenbleibt.
8. Aktivieren Sie den GO-Eingang. Nachdem der STÖSSEL den BOS-Punkt erreicht hat, überprüfen Sie, ob sich der Abwärts-Ausgang aus- und der Aufwärts-Ausgang einschaltet.
9. Blockieren Sie mit dem Teststück den Eingang für den mutingfähigen Sicherheitsstopp. Überprüfen Sie, ob die Aufwärtsbewegung angehalten wird.
10. Geben Sie den GO-Eingang frei.
11. Löschen Sie den Eingang für den mutingfähigen Sicherheitsstopp.
12. Führen Sie einen Reset-Zyklus durch.
13. Aktivieren Sie den GO-Eingang, um den Stößel in die TOS-Position zurückzufahren.

## Prüfungen des Funktionsblocks Pressensteuerungsmodus

Wenn die Einstellung „Doppeldruck“ gewählt ist, überprüfen Sie, ob alle Ausgänge korrekt funktionieren. Der Hochdruck-Ausgang sollte nur im RUN-Modus eingeschaltet werden.

1. Vergewissern Sie sich, dass der nicht mutingfähige Sicherheitseingang, der mutingfähige Sicherheitseingang und TOS eingeschaltet sind (alle Modus-Eingänge müssen jedoch ausgeschaltet sein).
2. Führen Sie einen Reset-Zyklus durch, schalten Sie PIP ein (falls verwendet) und aktivieren Sie dann den GO-Eingang. Prüfen Sie nach, dass sich kein Ausgang einschaltet.
3. Schalten Sie den GO-Eingang aus.
4. Wählen Sie den Ein-Zustand, führen Sie einen Reset-Zyklus durch und aktivieren Sie dann den GO-Eingang. Der Abwärts-Ausgang sollte sich einschalten. (Führen Sie einen kompletten Zyklus durch und stoppen Sie dann, einschließlich Durchschalten des PIP-Eingangs.)
5. Schalten Sie den Betriebs-Eingang aus und schalten Sie den Schrittsteuerung-Abwärts-Eingang ein.
6. Führen Sie einen Reset-Zyklus durch und aktivieren Sie dann den GO-Eingang. Überprüfen Sie den Ein- und Ausschaltzyklus des Abwärts-Ausgangs (und prüfen Sie, ob die Stößelgeschwindigkeit innerhalb der Spezifikationen für die Schrittsteuerung liegt).
7. Schalten Sie am BOS-Punkt des Prozesses den Schrittsteuerung-Abwärts-Eingang aus und den Schrittsteuerung-Aufwärts-Eingang ein.
8. Führen Sie einen Reset-Zyklus durch und aktivieren Sie dann den GO-Eingang. Überprüfen Sie den Ein- und Ausschaltzyklus des Aufwärts-Ausgangs (und prüfen Sie, ob die Stößelgeschwindigkeit innerhalb der Spezifikationen für die Schrittsteuerung liegt).

## Prüfungen der SQS- (oder SQS- und PCMS-)Funktion der Pressensteuerung

Wenn die Einstellung „Doppeldruck“ gewählt ist, überprüfen Sie, ob der Hochdruck-Ausgang nur dann eingeschaltet wird, wenn der Kolben von SQS zu BOS herunterfährt.

Spezifische GO-, SQS- und Fußpedal-Konfigurationen und -Verhalten finden Sie unter Funktionsblock Pressensteuerungeingänge auf Seite 146.

1. Vergewissern Sie sich, dass der nicht mutingfähige Sicherheitseingang, der mutingfähige Sicherheitseingang und TOS eingeschaltet sind.
2. Führen Sie einen Reset-Zyklus durch, schalten Sie PIP ein (falls verwendet) und aktivieren Sie dann den GO-Eingang. Überprüfen Sie, ob der Abwärts-Ausgang eingeschaltet ist.
3. Prüfen Sie, ob der Stößel beim SQS-Sensor (bzw. bei den SQS- und PCMS-Sensoren) anhält.
4. Geben Sie den GO-Eingang frei (schalten Sie ihn aus). Stellen Sie sicher, dass der Abstand der Werkzeuge weniger als 6 mm beträgt (fingersicher). Vergewissern Sie sich, dass der mutingfähige Sicherheitsstopp-Eingang jetzt gemutet ist.
5. Aktivieren Sie den Fußpedal-Eingang. Prüfen Sie, ob sich der Stößel vom SQS-Punkt zum BOS-Punkt bewegt und dort anhält.
6. Geben Sie den Fußpedal-Eingang frei.
7. Aktivieren Sie den GO-Eingang. Überprüfen Sie, ob der STÖSSEL zum TOS-Punkt zurückkehrt und dort anhält.
8. Geben Sie den GO-Eingang frei.

# 14 Informationen zum Status und zum Betrieb

Der Sicherheitskontroller XS/SC26-2 kann entweder über die Benutzeroberfläche am Gerät oder über die Software bedient werden, um den Status dauerhaft zu überwachen.

Der Sicherheitskontroller SC10-2 kann über die Software bedient werden, um den Status dauerhaft zu überwachen.

## 14.1 Status der LED-Anzeigen am XS/SC26-2

| LED | Status | Bedeutung |
|---|---|---|
| **Alle** | Aus | Initialisierungs-Modus |
| | **Abfolge:**<br>Grün EIN für 0,5 s<br>Rot EIN für 0,5 s<br>Aus für min. 0,5 s | Eingeschaltet |
| **Versorgung/Fehler** | Aus | Netzausschaltung |
| | Grün: Konstant | Run-Modus |
| | Grün blinkend | Konfigurationsmodus<br>ODER<br>Manuelle Netzeinschaltung |
| | Rot: Blinkend | Sperrzustand |
| **USB**<br>**(Basiskontroller bis FID 2)** | Aus | Keine Verbindung zum PC hergestellt |
| | Grün: Konstant | Verbindung zum PC hergestellt |
| | Grün blinkend für 5 s, dann aus | Übereinstimmung der SC-XM2/3-Konfiguration |
| | Rot blinkend für 5 s, dann aus | Keine Übereinstimmung der SC-XM2/3-Konfiguration |
| **USB**<br>**(Basiskontroller ab FID 3)** | Aus | Keine Verbindung hergestellt und konfigurierter Sicherheitskontroller |
| | Grün konstant | USB-Kabel an einen konfigurierten Sicherheitskontroller angeschlossen |
| | Grün blinkend | Keine Verbindung hergestellt und Sicherheitskontroller mit Werkseinstellungen<br>ODER<br>USB-Kabel angeschlossen und Sicherheitskontroller mit Werkseinstellungen |
| | Grün blinkend für 4 s, dann Grün EIN | Konfiguriertes neues SC-XM2/3 [43] (verriegelt oder unverriegelt) eingesteckt in einen Sicherheitskontroller mit Werkseinstellungen |
| | Grün blinkend für 5 s, dann aus | Konfiguriertes und unverriegeltes neues SC-XM2/3 [43] eingesteckt in einen konfigurierten Sicherheitskontroller mit übereinstimmender Konfiguration und übereinstimmenden Passwörtern sowie übereinstimmenden oder nicht übereinstimmenden Netzwerkstellungen<br>ODER<br>Altes SC-XM2/3 [44] ist in einen Kontroller ab FID 3 eingesteckt (konfiguriert oder Werkseinstellungen) und hat eine übereinstimmende Konfiguration |
| | Grün blinkend für 5 s, dann rot blinkend | Konfiguriertes und verriegeltes neues SC-XM2/3 [43] eingesteckt in einen konfigurierten Sicherheitskontroller mit übereinstimmender Konfiguration und übereinstimmenden Passwörtern, aber nicht übereinstimmenden Netzwerkstellungen |
| | Rot blinkend | Konfiguriertes (verriegeltes oder unverriegeltes) neues SC-XM2/3 [43] eingesteckt in einen konfigurierten Sicherheitskontroller mit nicht übereinstimmender Konfiguration und nicht übereinstimmendem Passwort oder leeres SC-XM2/3 eingesteckt<br>ODER<br>Leeres SC-XM2/3 eingesteckt in einem Sicherheitskontroller mit Werkseinstellungen oder einen konfigurierten Sicherheitskontroller |
| | Rot blinkend für 5 s, dann aus | Altes SC-XM2/3 [44] ist in einen Kontroller ab FID 3 eingesteckt (konfiguriert oder Werkseinstellungen) und hat keine übereinstimmende Konfiguration |
| **Eingänge** | Grün konstant | Keine Eingangsfehler |

[43] „Neues SC-XM2/3“: Ein SC-XM2/3 mit Informationen, die von der Software ab Version 4.2 des Sicherheitskontroller von Banner oder von einem Sicherheitskontroller ab FID 3 erstellt wurden.

[44] „Altes SC-XM2/3“: Ein SC-XM2/3 mit Informationen, die von der Software bis Version 4.1 des Sicherheitskontroller von Banner oder von einem Sicherheitskontroller bis FID 2 erstellt wurden.

| LED | Status | Bedeutung |
|---|---|---|
| | Rot: Blinkend | Einer oder mehrere Eingänge befinden sich im Aus-Zustand. |
| SO1, SO2 | Aus | Ausgang nicht konfiguriert |
| | Grün: Konstant | Sicherheitsausgang EIN |
| | Rot: Konstant | Sicherheitsausgang AUS |
| | Rot blinkend | Fehler bei Sicherheitsausgang erkannt oder EDM-Fehler erkannt oder AVM-Fehler erkannt |

| LED-Status für Spaltausgänge | Bedeutung |
|---|---|
| **Grün konstant** | Beide Ausgänge sind eingeschaltet. |
| **Rot konstant** | SO1 und/oder SO2 AUS |
| **Rot blinkend** | Fehler bei SO1 und/oder SO2 festgestellt |

| Ethernet-Diagnose-LEDs | | |
|---|---|---|
| **Gelbe LED** | **Grüne LED** | **Beschreibung** |
| Ein | Variiert je nach Verkehr | Verbindung hergestellt/Normalbetrieb |
| Aus | Aus | Hardwarefehler |

| Gelbe und grüne LED blinken synchron | Beschreibung |
|---|---|
| 5-maliges Blinken und danach mehrmaliges kurzes Blinken. | Normaler Anlauf |
| 1 Blinken alle 3 Sekunden | Banner Engineering kontaktieren |
| Wiederholte Sequenz aus zweimaligem Blinken | In den letzten 60 Sekunden wurde ein Kabel im aktiven Zustand getrennt. |
| Wiederholte Sequenz aus dreimaligem Blinken | Ein Kabel ist getrennt. |
| Wiederholte Sequenz aus viermaligem Blinken | Netzwerk in der Konfiguration nicht aktiviert. |
| Wiederholte Sequenz aus fünfmaligem oder häufigerem Blinken | Banner Engineering kontaktieren |

| PROFINET-Blinkbefehl | Bedeutung |
|---|---|
| Die Basiskontroller-LEDs blinken 4 Sekunden lang<br> | Die blinkenden LEDs geben an, dass der Basiskontroller verbunden ist. Das ist das Ergebnis des "LED blinken"-Befehls vom PROFINET-Netzwerk. |

# 14.2 Statusanzeigen des Eingangsmoduls

Die folgenden Informationen gelten für die Modelle XS8si und XS16si.

| LED | Status | Bedeutung |
|---|---|---|
| Alle | Abfolge:<br>Grün EIN für 0,5 s<br>Rot EIN für 0,5 s<br>AUS für min. 0,5 s | Eingeschaltet |
| | Aus | Initialisierungs-Modus |

| LED | Status | Bedeutung |
|---|---|---|
| Betriebsspannungsanzeige | Grün: Ein | Betriebsspannung Ein |
| | Aus | Netzausschaltung |
| | Rot blinkend | Sperrzustand |
| Anzeige Übertragung/ Empfang | Grün: EIN | Daten werden gesendet oder empfangen |
| | Rot: Ein | Keine Kommunikation |
| | Rot blinkend | Kommunikationsfehler erkannt<br>ODER<br>Fehler bei Sicherheits-Bus-Kommunikation |
| Eingangsanzeige | Grün: Ein | Keine Eingangsfehler |
| | Rot blinkend | Eingangsfehler erkannt |

## 14.3 Ausgangsmodul (Transistor oder Relais) Statusanzeigen

Die folgenden Informationen gelten für die Modelle XS2so, XS4so, XS1ro und XS2ro.

| LED | Status | Bedeutung |
|---|---|---|
| Alle | Abfolge:<br>Grün EIN für 0,5 s<br>Rot EIN für 0,5 s<br>AUS für min. 0,5 s | Eingeschaltet |
| | Aus | Initialisierungs-Modus |
| Betriebsspannungsanzeige | Aus | Netzausschaltung |
| | Grün: Ein | Betriebsspannung Ein |
| | Rot blinkend | Sperrzustand |
| Anzeige Übertragung/ Empfang | Grün: Ein | Daten werden gesendet oder empfangen |
| | Rot: Ein | Keine Kommunikation |
| | Rot blinkend | Kommunikationsfehler erkannt<br>ODER<br>Fehler bei Sicherheits-Bus-Kommunikation |
| Sicherheitsausgangsanzeigen | Aus | Ausgang nicht konfiguriert |
| | Grün: Ein | Zwei einkanalige Sicherheitsausgänge (beide Ein)<br>ODER<br>Zweikanaliger oder 1 einkanaliger Sicherheitsausgang Ein |
| | Rot: Ein | Zwei einkanalige Sicherheitsausgänge (1 Ein und 1 Aus) |
| | Rot: Ein | Zwei einkanalige Sicherheitsausgänge (beide Aus)<br>ODER<br>Zweikanaliger oder 1 einkanaliger Sicherheitsausgang Aus (anderer Kanal nicht verwendet) |
| | Rot blinkend | Sicherheitsausgangsfehler festgestellt |

## 14.4 Status der LED-Anzeigen am SC10-2

Anhand der folgenden Tabelle lässt sich der Status des Sicherheitskontrollers feststellen.

Solange der Sicherheitskontroller nicht ausgeschaltet wird, sind die LEDs immer eingeschaltet.

| LED | Status | Bedeutung |
|---|---|---|
| **Alle** | Aus | Initialisierungs-Modus |
| | **Abfolge:**<br>Grün EIN für 0,5 s<br>Rot EIN für 0,5 s<br>Aus für min. 0,5 s | Eingeschaltet |
| **Versorgung/Fehler** (1) | Grün konstant | 24 V DC verbunden |
| | Grün blinkend | Konfigurations- oder manueller Netzeinschaltungsmodus<br>Konfiguration über SC-XM3: Spannungsversorgung aus- und wiedereinschalten |
| | Rot blinkend | Sperrzustand |
| **USB** (1) | Grün konstant | USB-Kabel verbunden oder SC-XM3 eingesteckt |
| | Grün blinkend | Sicherheitskontroller im Werkszustand; weder USB-Kabel angeschlossen noch SC-XM3 eingesteckt |
| | Grün schnell blinkend für 3 s, dann konstant | Konfiguriertes (verriegeltes oder unverriegeltes) SC-XM3 in einen Sicherheitskontroller im Werkszustand eingesteckt; Konfiguration, Netzwerkeinstellungen und Passwörter werden vom SC-XM3 auf den Sicherheitskontroller übertragen |
| | Grün blinkend für 3 s, dann konstant | Konfiguriertes und unverriegeltes SC-XM3 in einen konfigurierten Sicherheitskontroller mit übereinstimmender Konfiguration und übereinstimmenden Passwörtern eingesteckt<br>**Anmerkung:** Wenn die Netzwerkeinstellungen nicht übereinstimmen, werden die Netzwerkeinstellungen vom Sicherheitskontroller auf ein unverriegeltes SC-XM3 übertragen. Auf ein verriegeltes SC-XM3 werden keine Netzwerkeinstellungen übertragen. |
| | Grün schnell blinkend für 3 s, dann rot blinkend | Konfiguriertes und verriegeltes SC-XM3 in einen konfigurierten Sicherheitskontroller mit übereinstimmender Konfiguration und übereinstimmenden Passwörtern, aber nicht übereinstimmenden Netzwerkstellungen eingesteckt |
| | Rot konstant | Konfigurierter Sicherheitskontroller; weder USB-Kabel angeschlossen noch SC-XM3 eingesteckt |
| | Rot blinkend | Konfiguriertes (verriegeltes oder unverriegeltes) SC-XM3 in einen konfigurierten Sicherheitskontroller mit nicht übereinstimmender Konfiguration und nicht übereinstimmendem Passwort oder leeres SC-XM3 in einen Sicherheitskontroller eingesteckt |
| **Eingänge** (10) | Grün konstant | 24 V DC und kein Fehler |
| | Grün konstant | Eingang als Statusausgang konfiguriert und aktiv |
| | Rot konstant | 0 V DC und kein Fehler |
| | Rot konstant | Eingang als Statusausgang konfiguriert und inaktiv |
| | Rot blinkend | Alle Anschlüsse eines fehlerhaften Eingangs (einschließlich gemeinsam genutzter Anschlüsse) |
| **RO1, RO2** (2) | Grün konstant | Ein (Kontakte geschlossen) |
| | Rot konstant | Aus (Kontakte geöffnet) oder nicht konfiguriert |
| | Rot blinkend | Fehler bei Sicherheitsausgang erkannt oder EDM-Fehler erkannt oder AVM-Fehler erkannt |

| **Ethernet-Diagnose-LEDs** | | |
|---|---|---|
| **Gelbe LED** | **Grüne LED** | **Beschreibung** |
| Ein | Variiert je nach Verkehr | Verbindung hergestellt/Normalbetrieb |
| Aus | Aus | Hardwarefehler |

| **Gelbe und grüne LED blinken synchron** | **Beschreibung** |
|---|---|
| 5-maliges Blinken und danach mehrmaliges kurzes Blinken. | Normaler Anlauf |
| 1 Blinken alle 3 Sekunden | Banner Engineering kontaktieren |
| Wiederholte Sequenz aus zweimaligem Blinken | In den letzten 60 Sekunden wurde ein Kabel im aktiven Zustand getrennt. |

| Gelbe und grüne LED blinken synchron | Beschreibung |
|---|---|
| Wiederholte Sequenz aus dreimaligem Blinken | Ein Kabel ist getrennt. |
| Wiederholte Sequenz aus viermaligem Blinken | Netzwerk in der Konfiguration nicht aktiviert. |
| Wiederholte Sequenz aus fünfmaligem oder häufigerem Blinken | Banner Engineering kontaktieren |

| PROFINET-Blinkbefehl | Bedeutung |
|---|---|
| Alle LEDs blinken 4 Sekunden lang   | Die blinkenden LEDs geben an, dass der SC10-2 verbunden ist. Das ist das Ergebnis des "LED blinken"-Befehls vom PROFINET-Netzwerk. |

# 14.5 Livemodus-Informationen: Software

Um Echtzeitinformationen über den Run-Modus auf einem PC anzuzeigen, muss der Sicherheitskontroller mit dem SC-USB2-Kabel an den Computer angeschlossen werden. Klicken Sie auf **Livemodus**, um die Registerkarte **Livemodus** aufzurufen. Diese Funktion aktualisiert laufend Daten und zeigt diese an, einschließlich Daten zu den Ein-, Stopp- und Fehlerzuständen aller Ein- und Ausgänge, sowie die Fehlercode-Tabelle. Die Registerkarten **Geräte** und **Funktionsansicht** enthalten ebenfalls eine gerätespezifische visuelle Darstellung der Daten. Unter Livemodus auf Seite 120 erhalten Sie weitere Informationen.

Die Registerkarte **Livemodus** enthält die gleichen Informationen, die auch auf dem integrierten Display des Sicherheitskontrollers zu sehen sind (gilt nur für Ausführungen des XS/SC26-2 mit Display).

# 14.6 Informationen zum Livemodus: Bedienfeld am Kontroller

Wählen Sie zum Anzeigen von Echtzeitinformationen zum RUN-Modus auf dem integrierten Display am Sicherheitskontroller (nur bei Ausführungen mit Display) **Systemstatus** [45] im **Systemmenü** (siehe Bedienfeld am XS/SC26-2 auf Seite 155 für eine Navigationsübersicht). Unter **Systemstatus** wird der Status der Eingangsgeräte und Sicherheitsausgänge angezeigt; unter **Fehlerdiagnose** werden aktuelle Fehlerinformationen angezeigt (eine kurze Beschreibung, Abhilfemaßnahmen und der Fehlercode); von dort können Sie auf das **Fehlerprotokoll** zugreifen.

Das Sicherheitskontroller-Display enthält dieselben Informationen, die über die Funktion **Livemodus** in der Software angezeigt werden können.

# 14.7 Sperrzustände

Sperrzustände von Eingängen werden in der Regel behoben, indem der Fehler repariert wird und der Eingang aus- und wieder eingeschaltet wird.

Sperrzustände an den Ausgängen (einschließlich EDM- und AVM-Fehlern) werden behoben, indem der Fehler repariert wird und anschließend der an den FR-Knoten am Sicherheitsausgang angeschlossene Reset-Eingang durchgeschaltet wird.

Systemfehler, wie zum Beispiel niedrige Versorgungsspannung, Übertemperatur oder an nicht zugewiesenen Eingängen erfasste Spannung, oder Fehler in der Pressensteuerung können gelöscht werden, indem der System-Reset-Eingang durchgeschaltet wird (für den System-Reset kann ein beliebiger Reset-Eingang zugewiesen werden). Nur eine physische oder virtuelle Reset-Taste kann für die Ausführung dieses Vorgangs konfiguriert werden.

[45] **Systemstatus** ist der erste Bildschirm, der angezeigt wird, wenn sich der Sicherheitskontroller nach einem Reset einschaltet. Klicken Sie auf **ESC**, um das **Systemmenü** anzuzeigen.

Ein System-Reset dient zum Beheben von Sperrzuständen, die nicht mit den Sicherheitseingängen oder -ausgängen zusammenhängen. Ein Sperrzustand ist eine Reaktion, bei der der Sicherheitskontroller alle betroffenen Sicherheitsausgänge ausschaltet, wenn ein sicherheitskritischer Fehler erfasst wird. Für den Wiederanlauf nach diesem Zustand müssen alle Fehler behoben worden sein, und es muss ein System-Reset durchgeführt werden. Ein Sperrzustand tritt nach einem System-Reset erneut ein, wenn der den Sperrzustand verursachende Fehler nicht behoben wurde.

Ein System-Reset ist unter den folgenden Bedingungen erforderlich:

- Für den Wiederanlauf nach einem System-Sperrzustand
- Zum Starten des Sicherheitskontrollers, nachdem eine neue Konfiguration heruntergeladen wurde
- Wiederherstellen nach einem Fehler in der Pressensteuerung

Bei internen Fehlern funktioniert der System-Reset wahrscheinlich nicht. Damit das System den Betrieb wieder aufnehmen kann, muss die Netzstromzufuhr aus- und wiedereingeschaltet werden.

**WARNUNG: Nicht überwachte Resets**

**Wenn ein Reset ohne Überwachung (entweder für einen verriegelten Ausgang oder ein System-Reset) konfiguriert ist** und alle anderen Bedingungen für einen Reset gegeben sind, **werden die Sicherheitsausgänge durch einen Kurzschluss vom Reset-Anschluss an +24 V sofort eingeschaltet**.

**WARNUNG: Kontrolle vor dem Reset**

Bei der Ausführung eines System-Reset-Vorgangs hat der Anwender dafür Sorge zu tragen, dass alle potenziellen Gefahrenzonen frei sind und sich darin keine Personen und unerwünschten Materialien (z. B. Werkzeuge) befinden, die der Gefahr ausgesetzt werden könnten. **Wenn diese Anweisungen nicht befolgt werden, können schwere oder tödliche Verletzungen die Folge sein.**

## 14.8 Nach einem Sperrzustand

Zur Behebung eines Sperrzustands:

- Empfehlung in der Fehleranzeige beachten (LCD-Ausführungen)
- Befolgen Sie die empfohlenen Schritte und Überprüfungen in der Fehlercode-Tabelle für XS/SC26-2 auf Seite 283 oder SC10-2 Fehlercode-Tabelle auf Seite 288
- System-Reset durchführen
- Schalten Sie das Gerät aus und wieder ein und führen Sie bei Bedarf einen System-Reset durch.

Wenn der Sperrzustand durch diese Schritte nicht behoben wird, wenden Sie sich an Banner Engineering (siehe Reparaturen und Garantie auf Seite 293).

## 14.9 SC10-2: Automatische Optimierung von Anschlüssen

Mit den folgenden Schritten erstellen Sie eine Beispielkonfiguration, die die Funktion für die automatische Optimierung von Anschlüssen (ATO) verwendet.

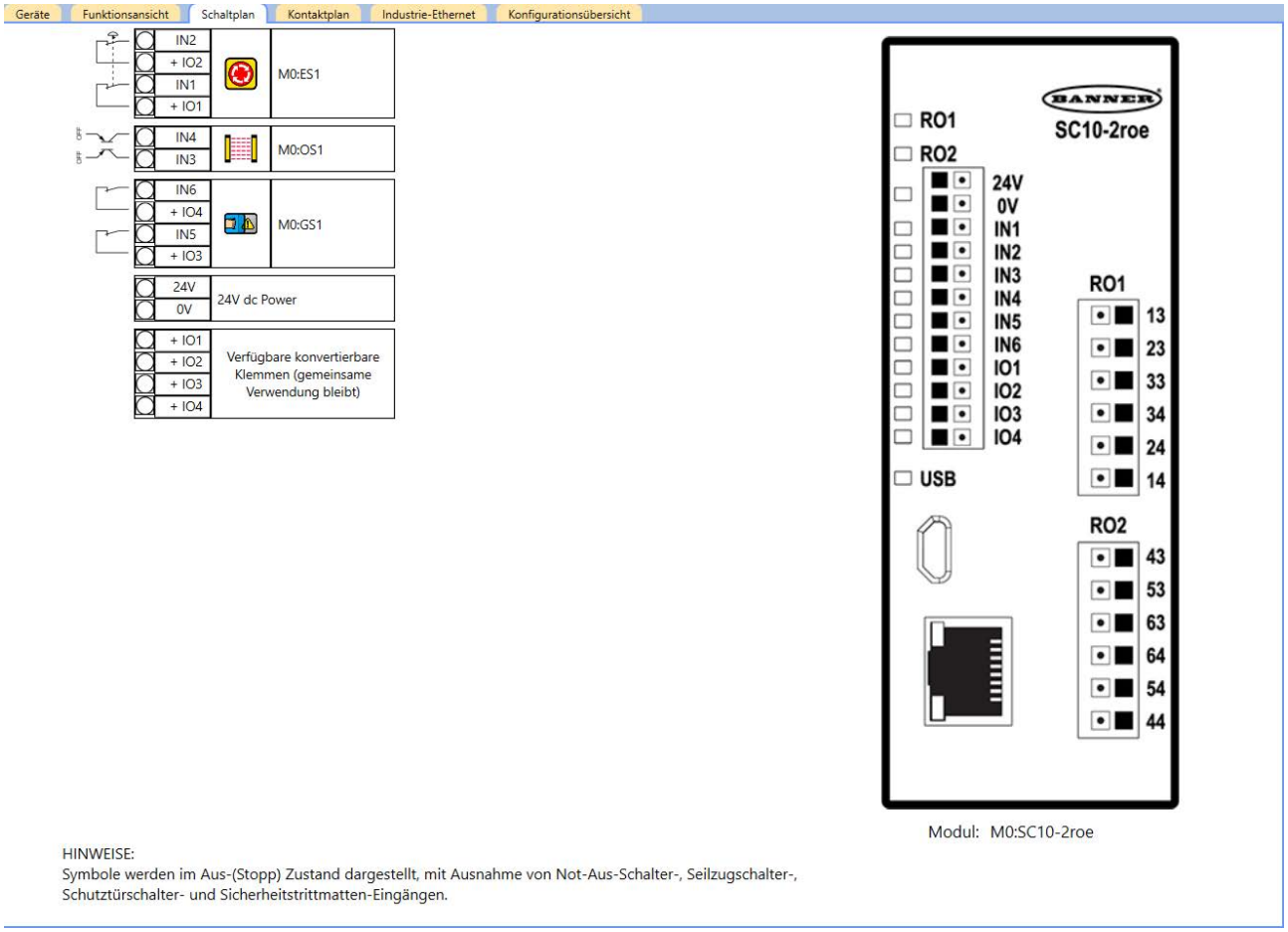
**Anmerkung:** Dieses Verfahren dient nur als Beispiel.

1. Klicken Sie auf **Neues Projekt**, um ein neues Projekt zu starten.
2. Wählen Sie die **Bauform** SC10-2 aus.
3. Definieren Sie die Projekteinstellungen und klicken Sie auf **OK**.

   **Anmerkung:** Achten Sie darauf, dass das Kontrollkästchen **Funktion für die automatische Optimierung von Anschlüssen deaktivieren** deaktiviert ist.

   Das Projekt wird erstellt.
4. Klicken Sie auf der Registerkarte **Geräte** unter dem Sicherheitskontroller auf ✙.
   Das Fenster **Gerät hinzufügen** wird geöffnet.
5. Fügen Sie einen Not-Aus-Schalter hinzu und klicken Sie auf **OK**, um die Standardeinstellungen zu akzeptieren.
6. Klicken Sie auf ✙.
7. Fügen Sie einen optischen Sensor hinzu und klicken Sie auf **OK**, um die Standardeinstellungen zu akzeptieren.
8. Klicken Sie auf ✙.
9. Fügen Sie einen Schutztürschalter hinzu und klicken Sie auf **OK**, um die Standardeinstellungen zu akzeptieren.
10. Wechseln Sie zur Registerkarte **Schaltplan** und lesen Sie dort ab, welche Anschlüsse belegt sind.

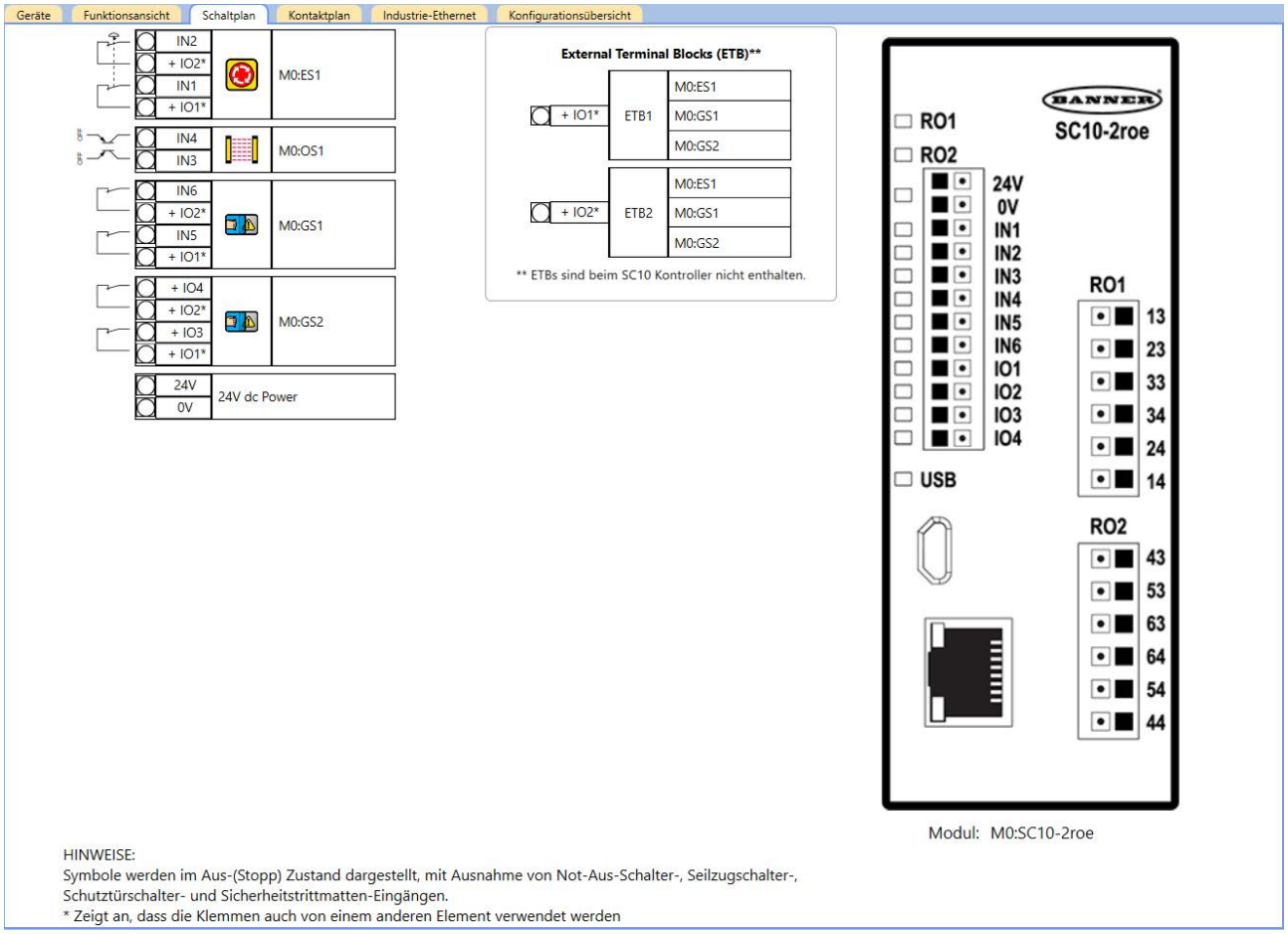
*Abbildung 247. Registerkarte **Schaltplan** mit einem Not-Aus-Schalter, optischen Sensor und Schutztürschalter*




11. Wechseln Sie zur Registerkarte **Geräte** und klicken Sie auf ✚.
12. Fügen Sie einen zweiten Schutztürschalter hinzu und klicken Sie auf **OK**, um die Standardeinstellungen zu akzeptieren.
13. Wechseln Sie zur Registerkarte **Schaltplan** und beachten Sie, dass externe Klemmenblöcke (ETB) für den zweiten Schutztürschalter hinzugefügt wurden.

**Anmerkung:** Die externen Klemmenblöcke werden vom Anwender bereitgestellt.

*Abbildung 248. Registerkarte **Schaltplan** mit drei Not-Aus-Tastern und ETBs*




# 14.10 Beispielkonfiguration für den SC10-2 ohne automatische Optimierung von Anschlüssen

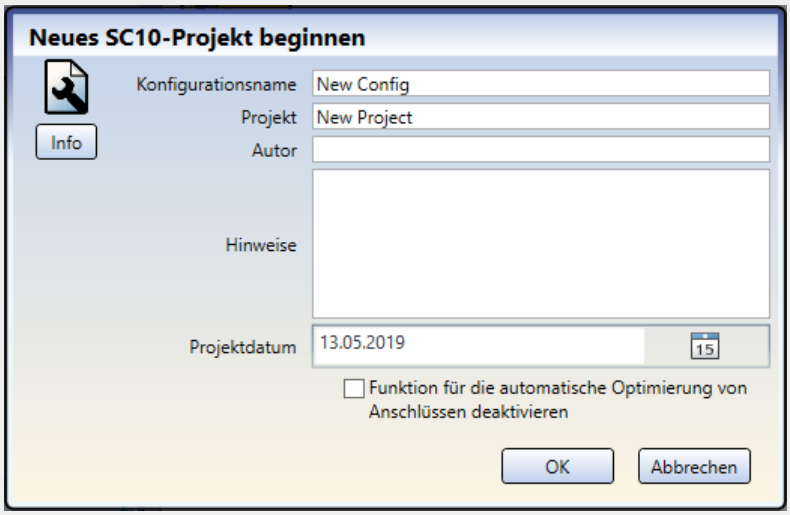
Mit den folgenden Schritten erstellen Sie eine Beispielkonfiguration, bei der die Funktion für die automatische Optimierung von Anschlüssen (ATO) deaktiviert ist.

**Anmerkung:** Dieses Verfahren dient nur als Beispiel.

1. Klicken Sie auf **Neues Projekt**, um ein neues Projekt zu starten.
2. Wählen Sie die **Bauform** SC10-2 aus.
3. Legen Sie die Projekteinstellungen fest, aktivieren Sie das Kontrollkästchen **Funktion für die automatische Optimierung von Anschlüssen deaktivieren** und klicken Sie auf **OK**.

**Anmerkung:** Achten Sie darauf, dass das Kontrollkästchen **Funktion für die automatische Optimierung von Anschlüssen deaktivieren** aktiviert ist.

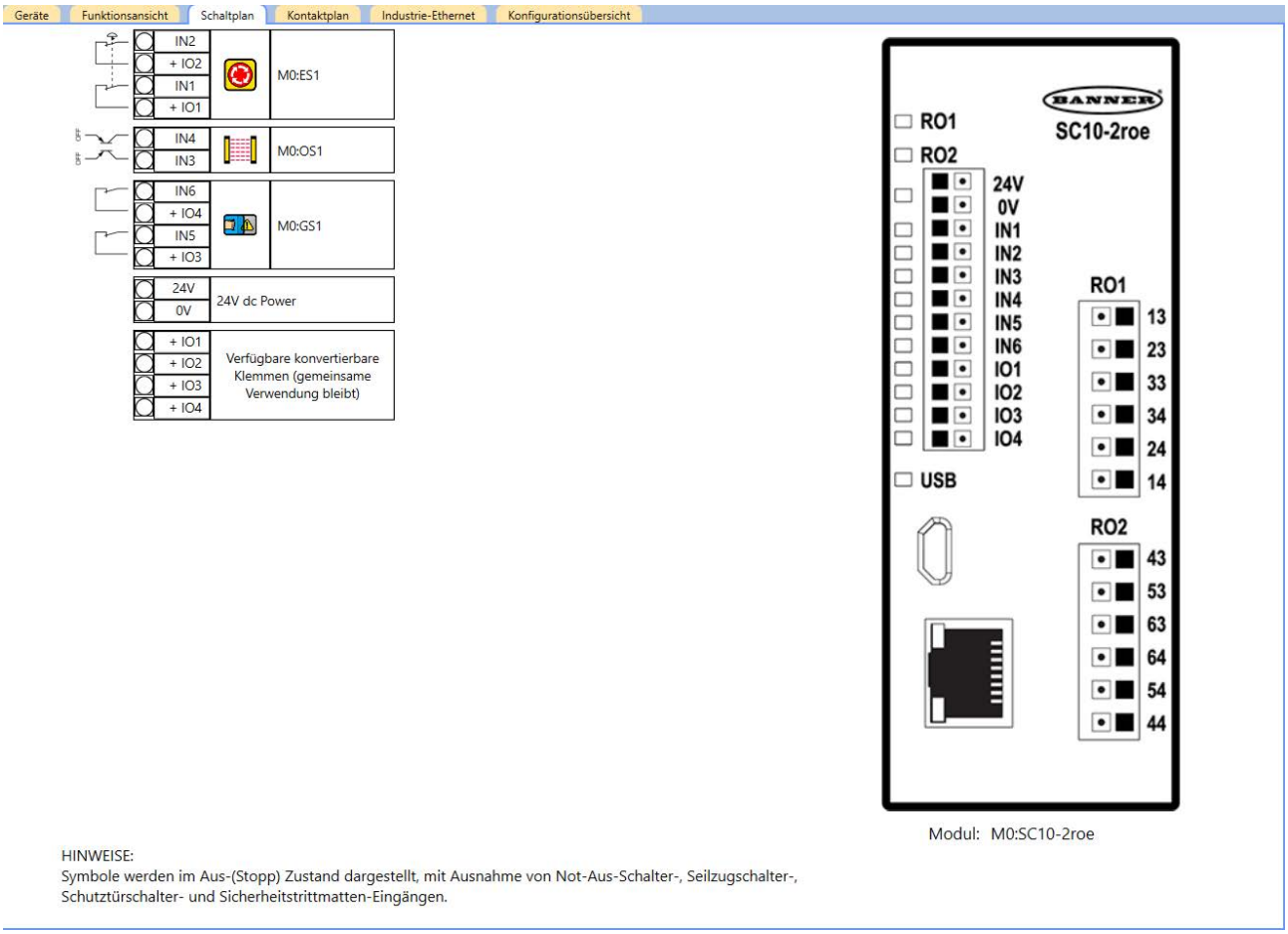
*Abbildung 249. **Funktion für die automatische Optimierung von Anschlüssen deaktivieren** ausgewählt*




Das Projekt wird erstellt.

4. Klicken Sie auf der Registerkarte **Geräte** unter dem Sicherheitskontroller auf ✚.
   Das Fenster **Gerät hinzufügen** wird geöffnet.
5. Fügen Sie einen Not-Aus-Schalter hinzu und klicken Sie auf **OK**, um die Standardeinstellungen zu akzeptieren.
6. Klicken Sie auf ✚.
7. Fügen Sie einen optischen Sensor hinzu und klicken Sie auf **OK**, um die Standardeinstellungen zu akzeptieren.
8. Klicken Sie auf ✚.
9. Fügen Sie einen Schutztürschalter hinzu und klicken Sie auf **OK**, um die Standardeinstellungen zu akzeptieren.
10. Wechseln Sie zur Registerkarte **Schaltplan** und lesen Sie dort ab, welche Anschlüsse belegt sind.

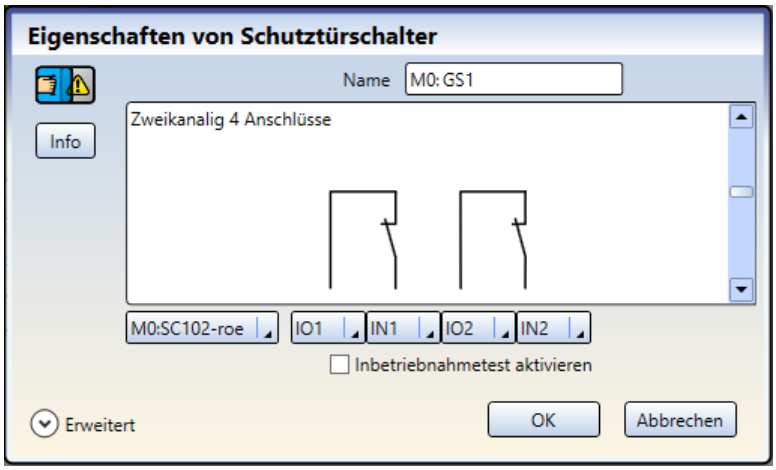
*Abbildung 250. Registerkarte **Schaltplan** mit einem Not-Aus-Schalter, optischen Sensor und Schutztürschalter*




11. Wechseln Sie zur Registerkarte **Geräte** und versuchen Sie einen weiteren Schutztürschalter hinzuzufügen.

    Es können keine weiteren Geräte hinzugefügt werden (✚ wird nicht angezeigt), da die ATO-Funktion deaktiviert ist und die Anschlüsse nicht ausreichen, um weitere Geräte zu unterstützen.
12. Wechseln Sie zur Registerkarte **Funktionsansicht** und versuchen Sie einen weiteren Schutztürschalter hinzuzufügen.
    Hier können ebenfalls keine weiteren Geräte hinzugefügt werden, da die ATO-Funktion deaktiviert ist.
13. Klicken Sie auf **Abbrechen**.
14. Klicken Sie auf der Registerkarte **Funktionsansicht** auf den Schutztürschalter und anschließend auf **Bearbeiten**, um die Eigenschaften zu ändern.
    a) Ändern Sie die Anschlüsse IO3 und IO4 jeweils in IO1 und IO2.

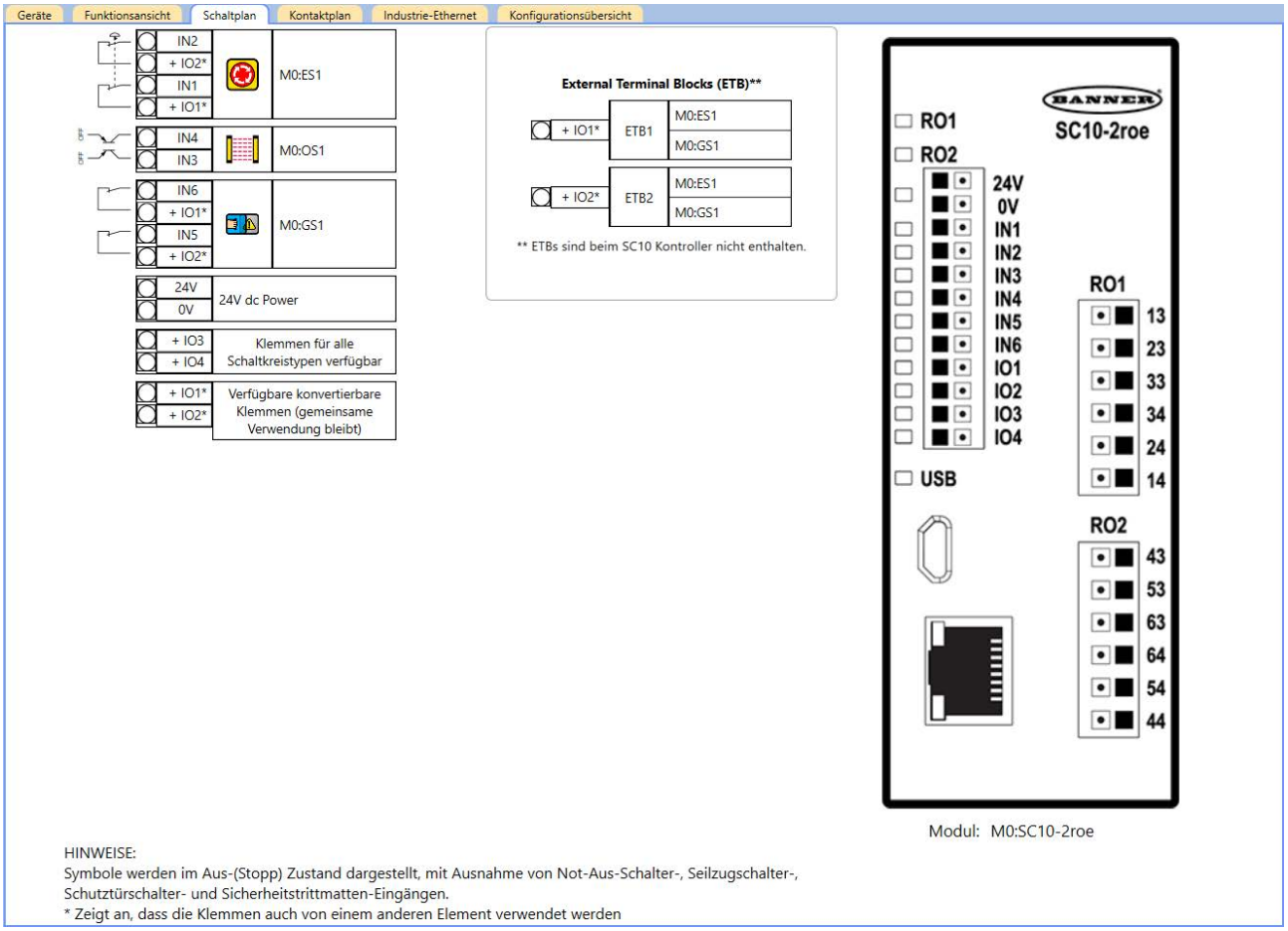
*Abbildung 251. Schutztürschaltereigenschaften*




    b) Klicken Sie auf **OK**.
15. Wechseln Sie zur Registerkarte **Schaltplan** und beachten Sie, dass externe Klemmenblöcke (ETB) der Änderung der Anschlusszuweisungen des Schutztürschalters entsprechend hinzugefügt wurden.

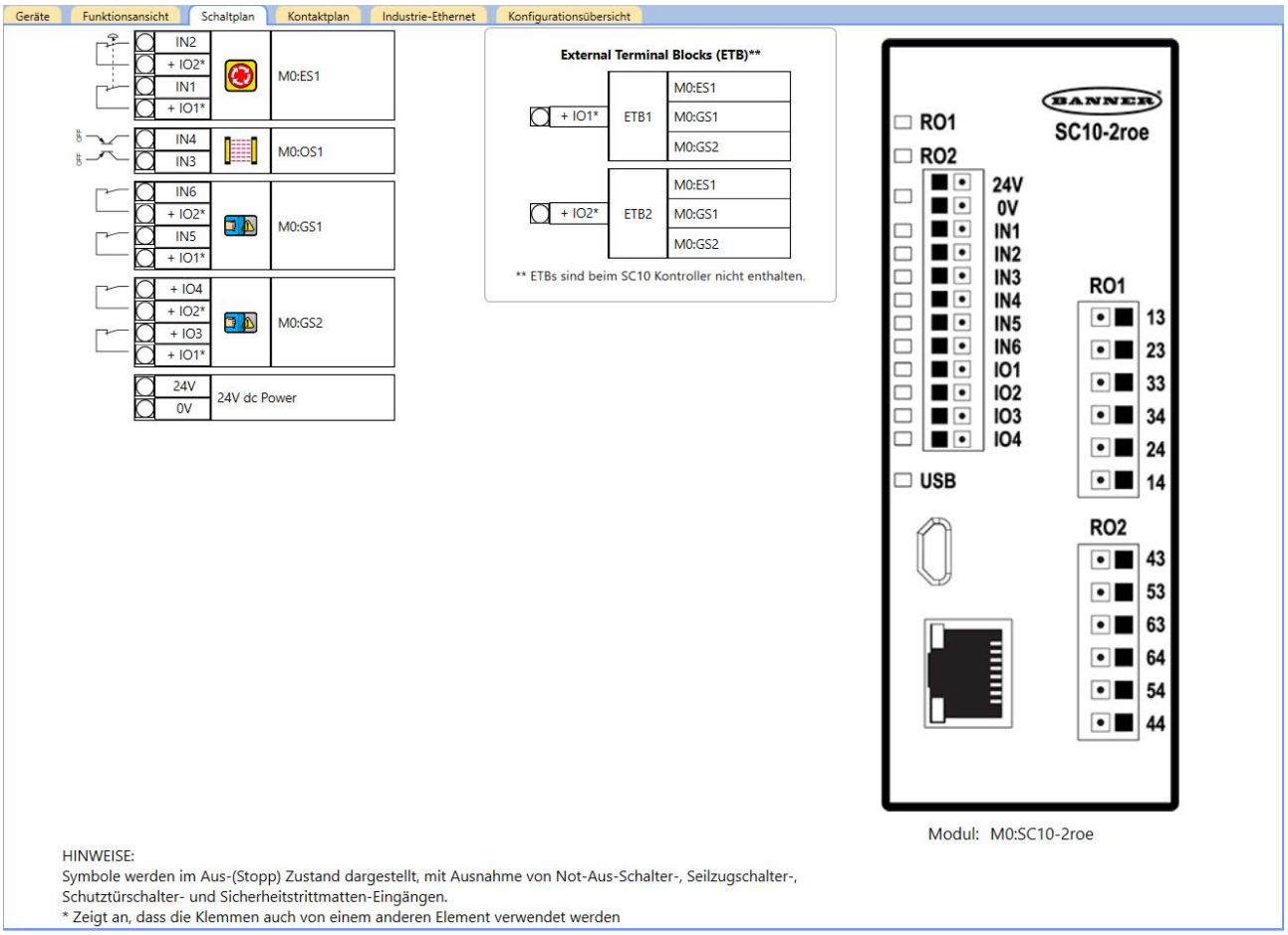
**Anmerkung:** Die externen Klemmenblöcke werden vom Anwender bereitgestellt.

*Abbildung 252. Registerkarte **Schaltplan** mit einem Not-Aus-Schalter, optischen Sensor, Schutztürschalter und ETBs*




16. Wechseln Sie zur Registerkarte **Funktionsansicht** und versuchen Sie einen weiteren Schutztürschalter hinzuzufügen.
    Ein weiterer Schutztürschalter kann jetzt hinzugefügt werden, da die Anschlussoptimierung manuell durchgeführt wurde.
17. Fügen Sie einen zweiten Schutztürschalter hinzu und klicken Sie auf **OK**, um die Standardeinstellungen zu akzeptieren.
18. Wechseln Sie zur Registerkarte **Schaltplan**. Sie sehen jetzt, dass der zweite Schutztürschalter hinzugefügt wurde und dass kein weiterer ETB hinzugefügt wurde.

*Abbildung 253. Registerkarte **Schaltplan** mit Not-Aus-Schalter, optischen Sensor, Schutztürschaltern und ETBs*




# 14.11 XS/SC26-2-Modelle ohne integrierte Schnittstelle: Verwendung des SC-XM2/3

Dieses Verfahren eignet sich für XS/SC26-2- und XS/SC26-2e-Modelle.

Verwenden Sie ein SC-XM2 oder SC-XM3 für folgende Vorgänge:

- Bestätigte Konfiguration speichern
- Mehrere XS/SC26-2-Sicherheitskontroller mit der gleichen Konfiguration schnell konfigurieren (ab FID 3)
- Austauschen eines XS/SC26-2 Sicherheitskontrollers durch einen anderen mithilfe des SC-XM2/3 (ab FID 3)

**Anmerkung:** Zum Schreiben einer bestätigten Konfiguration auf ein SC-XM2/3 sind das Programmiertool von Banner Engineering (SC-XMP2) und die Software des Sicherheitskontroller von Banner erforderlich. Dabei ist der Zugriff auf autorisierte Mitarbeiter beschränkt.

1. Erstellen Sie die gewünschte Konfiguration in der Software.

   Es wird empfohlen, die neuste Version der Software zu verwenden, auch wenn einige Funktionen in älteren Sicherheitskontrollern nicht verfügbar sind. Beziehen Sie sich beim Erstellen der Konfiguration auf die Checkliste auf der linken Seite des Softwarebildschirm mit weiterführenden Informationen.
2. Prüfen und bestätigen Sie die Konfiguration, indem Sie sie auf einen XS/SC26-2 hochladen.
   Nach der Überprüfung und Genehmigung kann die Konfiguration gespeichert und vom Sicherheitskontroller verwendet werden.
3. Schreiben Sie die bestätigte Konfiguration mithilfe des Programmierwerkzeugs auf das SC-XM2/3.

**Anmerkung:** Auf dem SC-XM2/3 kann nur eine bestätigte Konfiguration gespeichert werden. Siehe Schreiben der bestätigten Konfiguration mithilfe des Programmierwerkzeugs auf einen SC-XM2/3 auf Seite 84.

4. Beschriften Sie die Konfiguration, die Sie auf dem SC-XM2/3 speichern.
5. Installieren und/oder verbinden Sie die Spannungsquelle mit dem gewünschten XS/SC26-2 (Sicherheitskontroller mit Werkseinstellungen oder konfigurierter Sicherheitskontroller).

- **FID 1- oder FID 2-Kontroller:** Die USB-LED leuchtet nicht.
- **Kontroller ab FID 3:** Die USB-LED blinkt grün, wenn es sich bei dem XS/SC26-2 um einen Sicherheitskontroller mit Werkseinstellungen handelt. Die USB-LED leuchtet nicht, wenn es sich um einen konfigurierten Sicherheitskontroller handelt.

6. Legen Sie das SC-XM2/3 in den Micro-USB-Port am XS/SC26-2 ein.

**Anmerkung:** Weitere Informationen zu den LEDs finden Sie unter Status der LED-Anzeigen am XS/SC26-2 auf Seite 259.

**FID-1- oder FID-2-Sicherheitskontroller**

- Wenn die USB-LED 5 Sekunden lang grün blinkt, stimmt die Konfiguration auf dem Sicherheitskontroller mit dem SC-XM2/3 überein.
- Wenn die USB-LED 5 Sekunden lang rot blinkt, stimmt die Konfiguration auf dem Sicherheitskontroller nicht mit dem SC-XM2/3 überein.

**Sicherheitskontroller ab FID 3 mit Werkseinstellungen**

- Wenn die USB-LED 4 Sekunden lang grün blinkt und dann durchgehend leuchtet, werden die Konfiguration, die Netzwerkeinstellungen und die Passwörter automatisch auf den Sicherheitskontroller heruntergeladen.
- Wenn die USB-LED 5 Sekunden lang rot blinkt, wurde die Konfiguration auf dem SC-XM2/3 mit einer älteren Version der Software (bis 4.1) oder einem Sicherheitskontroller bis FID 2 erstellt und in einen Sicherheitskontroller ab FID 3 eingesteckt. Dies bedeutet, dass die Konfiguration nicht automatisch geladen werden kann. Dies ist nur möglich, wenn die SC-XM2/3-Konfiguration mit einer Softwareversion ab 4.2 oder einem Sicherheitskontroller ab FID 3 mit Display neu erstellt wird.

**Konfigurierter Sicherheitskontroller ab FID 3**

- Wenn ein altes [46] SC-XM2/3 eingesteckt ist und die USB-LED 5 Sekunden lang grün blinkt, stimmt die Konfiguration auf dem Sicherheitskontroller und dem SC-XM2/3 überein.
- Wenn ein altes [46] SC-XM2/3 eingesteckt ist und die USB-LED 5 Sekunden lang rot blinkt, stimmt die Konfiguration auf dem SC-XM2/3 nicht überein.
- Wenn ein neues [47] SC-XM2/3 eingesteckt ist und die USB-LED 5 Sekunden lang grün blinkt, stimmen die Konfiguration und die Passwörter auf dem Sicherheitskontroller und dem SC-XM2/3 überein. Und wenn die Netzwerkeinstellungen nicht übereinstimmen (XS/SC26-2e-Modelle), werden die Netzwerkeinstellungen des Sicherheitskontrollers auf das SC-XM2/3 übertragen, sofern das SC-XM2/3 nicht gesperrt ist. Wenn das SC-XM2/3 gesperrt ist, die USB-LED 5 Sekunden lang rot blinkt und das SC-XM2/3 nicht innerhalb dieser 5 Sekunden abgezogen wird, wechselt der Sicherheitskontroller in einen Sperrzustand.
- Wenn ein neues [47] SC-XM2/3 eingesteckt wird und die USB-LED rot blinkt, stimmen die Konfiguration oder die Passwörter auf dem Sicherheitskontroller und dem SC-XM2/3 nicht überein. Wird das SC-XM2/3 nicht innerhalb von 5 Sekunden abgezogen, blinkt die Betriebs-/Fehler-LED rot und der Sicherheitskontroller wechselt in einen Sperrzustand.

7. Wenn der Sicherheitskontroller in einen Sperrzustand gewechselt hat, entnehmen Sie das SC-XM2/3 und schalten Sie den Kontroller aus und wieder ein oder führen Sie einen Systemreset durch.
8. Für Sicherheitskontroller ab FID 3 mit Werkseinstellungen: Wenn die USB-LED nicht mehr schnell blinkt, schalten Sie aus und wieder ein oder führen Sie einen Systemreset durch.

Der Sicherheitskontroller kann jetzt in Betrieb genommen werden. Siehe Inbetriebnahmeprüfung auf Seite 251.

# 14.12 XS/SC26-2-Modelle mit integrierter Schnittstelle: Verwendung des SC-XM2/3

Dieses Verfahren gilt für XS/SC26-2d- und XS/SC26-2de-Modelle.

Verwenden Sie ein SC-XM2 oder SC-XM3 für folgenden Vorgang:

- Bestätigte Konfiguration speichern
- Schnelle Konfiguration mehrerer XS/SC26-2-Sicherheitskontroller mit den gleichen Konfigurationseinstellungen
- Ersetzen eines XS/SC26-2-Sicherheitskontrollers durch einen anderen mit dem SC-XM2/3 (Funktionen ab FID 3)

**Anmerkung:** Das Programmiertool von Banner Engineering (SC-XMP2) und die Sicherheitskontroller von Banner-Software sind erforderlich, um eine bestätigte Konfiguration auf ein SC-XM2/3 zu schreiben. Dabei ist der Zugriff auf autorisierte Mitarbeiter beschränkt. Eine Konfiguration kann auch mit einem Sicherheitskontroller mit integrierter Schnittstelle (Modelle XS/SC26-2d und -2de) auf ein SC-XM2/3 geschrieben werden.

[46] „Altes SC-XM2/3“: Ein SC-XM2/3 mit Informationen, die von der Software bis Version 4.1 des Sicherheitskontroller von Banner oder von einem Sicherheitskontroller bis FID 2 erstellt wurden.

[47] „Neues SC-XM2/3“: Ein SC-XM2/3 mit Informationen, die von der Software ab Version 4.2 des Sicherheitskontroller von Banner oder von einem Sicherheitskontroller ab FID 3 erstellt wurden.

**Anmerkung:** Die LEDs zeigen dasselbe Verhalten, ob mit oder ohne integrierte Schnittstelle (weitere Details siehe XS/SC26-2-Modelle ohne integrierte Schnittstelle: Verwendung des SC-XM2/3 auf Seite 270); das folgende Verfahren zeigt jedoch, was auf dem Display passiert.

1. Erstellen Sie die gewünschte Konfiguration in der Software.

   Es wird empfohlen, die neuste Version der Software zu verwenden, auch wenn einige Funktionen in älteren Sicherheitskontrollern nicht verfügbar sind. Beziehen Sie sich beim Erstellen der Konfiguration auf die Checkliste auf der linken Seite des Softwarebildschirm mit weiterführenden Informationen.
2. Überprüfen und bestätigen Sie die Konfiguration, indem Sie sie auf einen XS/SC26-2 laden.
   Nach der Überprüfung und Genehmigung kann die Konfiguration gespeichert und vom Sicherheitskontroller verwendet werden.
3. Schreiben Sie die bestätigte Konfiguration mithilfe des Programmierwerkzeugs oder der integrierten Schnittstelle (Modelle XS/SC26-2d und -2de) auf das SC-XM2/3.

   **Anmerkung:** Nur eine bestätigte Konfiguration kann auf dem SC-XM2/3 gespeichert werden.
4. Beschriften Sie die Konfiguration, die Sie auf dem SC-XM2/3 speichern.
5. Installieren und/oder verbinden Sie die Spannungsquelle mit dem gewünschten XS/SC26-2 (Sicherheitskontroller mit Werkseinstellungen oder konfigurierter Sicherheitskontroller).
   - **FID 1- oder FID 2-Kontroller:** Die USB-LED leuchtet nicht.
   - **Kontroller ab FID 3:** Die USB-LED blinkt grün, wenn es sich bei dem XS/SC26-2 um einen Sicherheitskontroller mit Werkseinstellungen handelt. Die USB-LED leuchtet nicht, wenn es sich um einen konfigurierten Sicherheitskontroller handelt.
6. Stecken Sie das SC-XM2/3 in den Mikro-USB-Anschluss am XS/SC26-2.

**FID-1- oder FID-2-Sicherheitskontroller**

- Wenn ein altes [48] oder neues [49] SC-XM2/3 in einen konfigurierten FID-1- oder FID-2-Sicherheitskontroller eingesteckt wird, wird einer der folgenden Bildschirme angezeigt, je nachdem, ob die Konfiguration des Sicherheitskontrollers übereinstimmt oder nicht:

*Abbildung 254. Muster*




*Abbildung 255. Keine Übereinstimmung*




Eine Anleitung zum Importieren von Daten aus dem SC-XM2/3 finden Sie unter XS/SC26-2: Konfigurationsmodus auf Seite 155.

- Wenn ein leeres SC-XM2/3 in einen konfigurierten FID-1- oder FID-2-Sicherheitskontroller eingesteckt wird, wird auf dem Display auf folgendes Problem hingewiesen:

*Abbildung 256. SC-XM2/3 leer*




**Sicherheitskontroller ab FID 3 mit Werkseinstellungen**

- Wenn ein altes [48] SC-XM2/3 in einen Sicherheitskontroller ab FID 3 mit Werkseinstellungen eingesteckt wird, stimmt die Konfiguration nicht überein:

[48] „Altes SC-XM2/3“: Ein SC-XM2/3 mit Informationen, die von der Sicherheitskontroller von Banner-Software bis Version 4.1 oder von einem Sicherheitskontroller bis FID 2 erstellt wurden.

[49] „Neues SC-XM2/3“: Ein SC-XM2/3 mit Informationen, die von der Sicherheitskontroller von Banner-Software ab Version 4.2 oder von einem Sicherheitskontroller ab FID 3 erstellt wurden.

*Abbildung 257. Keine Übereinstimmung*




- Wenn eine neues [49] SC-XM2/3 in einen Sicherheitskontroller ab FID 3 mit Werkseinstellungen eingesteckt wird, werden die Konfiguration, die Netzwerkeinstellungen und die Passwörter automatisch auf den Sicherheitskontroller heruntergeladen. Auf dem Display wird der automatische Upload angezeigt:

*Abbildung 258. Automatischer Upload*




Nach dem automatischen Upload wird auf dem Display: „Konfiguration empfangen, bitte aus- und wieder einschalten oder Systemreset durchführen“ angezeigt.

- Wenn ein leeres SC-XM2/3 in einen Sicherheitskontroller ab FID 3 mit Werkseinstellungen eingesteckt wird, weist das Display auf das Problem hin und zählt bis zu einer Systemsperre herunter:

*Abbildung 259. SC-XM2/3-Fehler*




Wird das SC-XM2/3 nicht innerhalb von 3 Sekunden vom Sicherheitskontroller getrennt, geht der Sicherheitskontroller in einen Sperrzustand über:

*Abbildung 260. Systemsperre*




### Konfigurierter Sicherheitskontroller ab FID 3

- Wenn ein altes [48] SC-XM2/3 in einen konfigurierten Sicherheitskontroller ab FID 3 eingesteckt wird, wird einer der folgenden Bildschirme angezeigt, je nachdem, ob die Konfiguration des Sicherheitskontrollers übereinstimmt oder nicht:

*Abbildung 261. Muster*




*Abbildung 262. Keine Übereinstimmung*




Eine Anleitung zum Importieren von Daten aus dem SC-XM2/3 finden Sie unter XS/SC26-2: Konfigurationsmodus auf Seite 155.

- Wenn ein neues [49] SC-XM2/3 in einen konfigurierten Sicherheitskontroller ab FID 3 eingesteckt wird und die Konfiguration und das Passwort übereinstimmen, erscheint eine der folgenden Anzeigen:

*Abbildung 263. XS/SC26-2d-Modelle: Netzwerkeinstellungen ignoriert*




*Abbildung 264. XS/SC26-2de-Modelle: Display zeigt eine Übereinstimmung an*




Wenn die Netzwerkeinstellungen nicht übereinstimmen (Modelle XS/SC26-2de), werden die Netzwerkeinstellungen des Sicherheitskontrollers auf das SC-XM2/3 übertragen. Wenn dies abgeschlossen ist, zeigt das Display Folgendes an:

*Abbildung 265. Netzwerkaktualisierung*




Auf **OK** klicken. Schlägt die Aktualisierung fehl (z. B. weil das SC-XM2/3 gesperrt ist), wird auf dem Display der Grund für den Fehler angezeigt und bis zu einer Systemsperre heruntergezählt:

*Abbildung 266. Netzwerkaktualisierung fehlgeschlagen*




Wird das SC-XM2/3 nicht innerhalb von 3 Sekunden vom Sicherheitskontroller getrennt, geht der Sicherheitskontroller in einen Sperrzustand über:

*Abbildung 267. Systemsperre*




- Wenn ein neues [49] SC-XM2/3 in einen konfigurierten Sicherheitskontroller ab FID 3 eingesteckt wird, die Konfiguration und/oder das Passwort jedoch nicht übereinstimmt, wird das Problem auf dem Display angezeigt und der Countdown bis zur Systemsperre beginnt:

*Abbildung 268. XS/SC26-2d-Modelle: Keine Übereinstimmung*




*Abbildung 269. XS/SC26-2de-Modelle: Keine Übereinstimmung*




Wenn das SC-XM2/3 nicht innerhalb von 3 Sekunden vom Sicherheitskontroller getrennt wird, geht der Sicherheitskontroller in einen Sperrzustand über:

*Abbildung 270. XS/SC26-2d-Modelle: Systemsperre*




*Abbildung 271. XS/SC26-2de-Modelle: Systemsperre*




Eine Anleitung zum Importieren von Daten aus dem SC-XM2/3 finden Sie unter XS/SC26-2: Konfigurationsmodus auf Seite 155.

- Wenn ein leeres SC-XM2/3 in einen konfigurierten Sicherheitskontroller ab FID 3 eingesteckt wird, wird das Problem auf dem Display angezeigt und der Countdown bis zur Systemsperre beginnt:

*Abbildung 272. SC-XM2/3-Fehler*




Wird das SC-XM2/3 nicht innerhalb von 3 Sekunden vom Sicherheitskontroller getrennt, geht der Sicherheitskontroller in einen Sperrzustand über:

*Abbildung 273. Systemsperre*




7. Wenn der Sicherheitskontroller in einen Sperrzustand gewechselt hat, entnehmen Sie das SC-XM2/3 und schalten Sie den Kontroller aus und wieder ein oder führen Sie einen Systemreset durch.
8. Sicherheitskontroller mit Werkseinstellungen: Wenn die USB-LED nicht mehr schnell blinkt, schalten Sie den Kontroller aus und wieder ein oder führen Sie einen Systemreset durch.

Der Sicherheitskontroller kann jetzt in Betrieb genommen werden. Siehe Inbetriebnahmeprüfung auf Seite 251.

# 14.13 SC10-2: Verwendung des SC-XM3

Mit einem SC-XM3 haben Sie folgende Möglichkeiten:

- Mehrere SC10-2 Sicherheitskontroller mit der gleichen Konfiguration schnell konfigurieren
- Einen SC10-2 Sicherheitskontroller gegen einen anderen Sicherheitskontroller auswechseln (wobei das SC-XM3 vom alten Sicherheitskontroller verwendet wird)

**Anmerkung:** Zum Schreiben einer bestätigten Konfiguration in ein SC-XM3 benötigen Sie das Programmierwerkzeug (SC-XMP2) und die Software von Banner. Dabei ist der Zugriff auf autorisierte Mitarbeiter beschränkt.

1. Erstellen Sie die gewünschte Konfiguration in der Software.
2. Prüfen und bestätigen Sie die Konfiguration, indem Sie sie auf einen SC10-2 hochladen.
   Nach der Überprüfung und Genehmigung kann die Konfiguration gespeichert und vom Sicherheitskontroller verwendet werden.
3. Schreiben Sie die bestätigte Konfiguration mithilfe des Programmierwerkzeugs in das SC-XM3.

   **Anmerkung:** Auf dem SC-XM3 können nur bestätigte Konfigurationen gespeichert werden. Siehe Schreiben der bestätigten Konfiguration mithilfe des Programmierwerkzeugs auf einen SC-XM2/3 auf Seite 84.
4. Beschriften Sie die Konfiguration, die Sie auf dem SC-XM3 speichern.
5. Installieren und/oder verbinden Sie die Spannungsquelle mit dem gewünschten SC10-2 (Sicherheitskontroller mit Werkseinstellungen oder konfigurierter Sicherheitskontroller).
   - Gemäß den Werkseinstellungen weist eine grün leuchtende Betriebs-/Fehler-LED am Sicherheitskontroller SC10-2 zusammen mit einer grün blinkenden USB-LED darauf hin, dass der Sicherheitskontroller auf eine Konfiguration wartet.
   - Wurde der Sicherheitskontroller SC10-2 konfiguriert, leuchtet die Betriebs-/Fehler-LED grün und die USB-LED leuchtet rot.
6. Stecken Sie das SC-XM3 in den Micro-USB-Port am SC10-2 ein.

   **Sicherheitskontroller mit Werkseinstellungen**
   - Die USB-LED blinkt 3 Sekunden lang und leuchtet dann konstant. Die Konfiguration, die Netzwerkeinstellungen und Passwörter werden dann automatisch auf den Sicherheitskontroller heruntergeladen. Danach blinkt die Betriebs-/Fehler-LED grün, um darauf hinzuweisen, dass der Sicherheitskontroller darauf wartet, aus- und wiedereingeschaltet zu werden.

   **Konfigurierter Sicherheitskontroller**
   - Wenn die Konfiguration und die Passwörter am Sicherheitskontroller und am SC-XM3 übereinstimmen, blinkt die USB-LED für 3 Sekunden und leuchtet dann konstant. Stimmen die Netzwerkeinstellungen nicht überein, werden die Netzwerkeinstellungen nach 3 Sekunden an das SC-XM3 übertragen, sofern das SC-XM3 nicht gesperrt ist. Ist das SC-XM3 gesperrt, wechselt der Kontroller in einen Sperrzustand.
   - Wenn die Konfiguration oder die Passwörter am Sicherheitskontroller und am SC-XM3 nicht übereinstimmen, blinkt die USB-LED rot. Wird das SC-XM3 nicht innerhalb von 3 Sekunden vom Sicherheitskontroller getrennt, blinken die Betriebs-/Fehler- und die USB-LED rot und der Sicherheitskontroller wechselt wegen der Unstimmigkeit in einen Sperrzustand.
7. Das Gerät aus- und wiedereinschalten.
   Die Betriebs-/Fehler-LED leuchtet grün, die USB-LED leuchtet grün (wenn das SC-XM3 weiterhin verbunden ist) oder rot (wenn kein SC-XM3 oder kein USB-Kabel angeschlossen ist), und die Eingangs- und Ausgangs-LEDs zeigen den tatsächlichen Eingangsstatus an.

Der Sicherheitskontroller kann jetzt in Betrieb genommen werden. Siehe Inbetriebnahmeprüfung auf Seite 251.

# 14.14 Setzen Sie den Sicherheitskontroller auf die Werkseinstellungen zurück.

Setzen Sie den XS/SC26-2 ab FID 3 oder den SC10-2-Sicherheitskontroller anhand der folgenden Schritte zurück.

**Anmerkung:** Beim XS/SC26-2 mit FID 1 oder FID 2 und Softwareversion ab 4.2 wird die Option **Auf Werkseinstellungen zurücksetzen** grau dargestellt.

Der Sicherheitskontroller muss eingeschaltet und mit dem SC-USB2-Kabel am PC angeschlossen sein.

1. Klicken Sie auf  .
2. Klicken Sie auf **Werkseinstellungen wiederherstellen**.
   Daraufhin wird eine Warnmeldung darüber eingeblendet, dass alle Einstellungen auf die Werkseinstellungen zurückgesetzt werden.
3. Klicken Sie auf **Weiter**.
   Der Bildschirm **Passwort eingeben** wird geöffnet.
4. Geben Sie das Passwort Benutzer1 ein und klicken Sie auf **OK**.
   Der Sicherheitskontroller wird auf die Werkseinstellungen zurückgesetzt und ein Bestätigungsfenster wird angezeigt.
5. Auf **OK** klicken.
6. Das Gerät aus- und wiedereinschalten.
   Die Werkseinstellungen sind damit wiederhergestellt.

# 14.15 Werkseinstellungen

In der folgenden Tabelle sind einige der Werkseinstellungen für den Sicherheitskontroller und die Software aufgeführt.

| Einstellung | Werkseinstellung | Produkt |
|---|---|---|
| AVM-Funktion | 50 ms | XS/SC26-2, SC10-2 |
| Ausschaltentprellzeit | 6 ms | XS/SC26-2, SC10-2 |
| EDM | Keine Überwachung | XS/SC26-2, SC10-2 |
| Funktionsblock: Überbrückungsblock – Standardknoten | IN, BP | XS/SC26-2, SC10-2 |
| Funktionsblock: Überbrückung – Zeitlimit | 1 s | XS/SC26-2, SC10-2 |
| Funktionsblock: Verzögerungsblock – Standardknoten | IN | XS/SC26-2, SC10-2 |
| Funktionsblock: Verzögerungsblock – Ausschaltverzögerung | 100 ms | XS/SC26-2, SC10-2 |
| Funktionsblock: Zustimmtasterblock – Standardknoten | ED, IN, RST | XS/SC26-2, SC10-2 |
| Funktionsblock: Zustimmtasterblock – Zeitlimit | 1 s | XS/SC26-2, SC10-2 |
| Funktionsblock: Latch-Reset-Block – Standardknoten | IN, LR | XS/SC26-2, SC10-2 |
| Funktionsblock: Mutingblock – Standardknoten | IN, MP1 | XS/SC26-2, SC10-2 |
| Funktionsblock: Mutingblock – Zeitlimit | 30 s | XS/SC26-2, SC10-2 |
| Funktionsblock: Zweihandsteuerungsblock – Standardknoten | TC | XS/SC26-2, SC10-2 |
| Funktionsblock: One-Shot-Block - Standardknoten | IN | XS/SC26-2 |
| Funktionsblock: One-Shot-Block – Zeitlimit | 100 ms | XS/SC26-2 |
| Industrial Ethernet: String (EtherNet/IP und PCCC-Protokoll) | 32 Bit | XS/SC26-2, SC10-2 |
| Netzwerkeinstellungen: Gateway-Adresse | 0.0.0.0 | XS/SC26-2, SC10-2 |
| Netzwerkeinstellungen: IP-Adresse | 192.168.0.128 | XS/SC26-2, SC10-2 |
| Netzwerkeinstellungen: Verbindungsgeschwindigkeit und Duplexmodus | Automatische Aushandlung | XS/SC26-2, SC10-2 |
| Netzwerkeinstellungen: Subnetzmaske | 255.255.255.0 | XS/SC26-2, SC10-2 |
| Netzwerkeinstellungen: TCP-Port | 502 | XS/SC26-2, SC10-2 |
| Einschaltentprellzeit | 50 ms | XS/SC26-2, SC10-2 |
| Passwort Benutzer1 | 1901 | XS/SC26-2, SC10-2 |
| Passwort für Benutzer2 | 1902 | XS/SC26-2, SC10-2 |
| Passwort für Benutzer3 | 1903 | XS/SC26-2, SC10-2 |
| Anlaufmodus | Normal | SC10-2 |
| Sicherheitsausgänge | Automatischer Reset (Schaltmodus) | XS/SC26-2, SC10-2 |
| Sicherheitsausgänge: Anlaufmodus | Normal | XS/SC26-2 |
| Sicherheitsausgänge: Teilen (Sicherheitsausgänge) | Paarweise Funktion | XS/SC26-2 |
| Simulationsmodus: Simulationsgeschwindigkeit | 1 | XS/SC26-2, SC10-2 |
| Automatische Optimierung von Anschlüssen | Aktiviert | SC10-2 |
| Signallogik für Statusausgänge | Aktiv = PNP ein | XS/SC26-2, SC10-2 |
| Blinkfrequenz Statusausgang | Nein | XS/SC26-2 |

# 15 Fehlerbehebung

Der Sicherheitskontroller wurde für hohe Beständigkeit gegen eine Vielzahl von elektrischen Störungsquellen, die in industriellen Umgebungen anzutreffen sind, entwickelt und entsprechend getestet. Starke elektrische Störquellen, die elektromagnetische und hochfrequente Störsignale oberhalb dieser Grenzwerte erzeugen, können jedoch willkürliche Schalt- oder Sperrzustände verursachen. Wenn willkürliche Schalt- oder Sperrzustände auftreten, prüfen Sie Folgendes:

- Die Betriebsspannung bei 24 V DC +/- 20 % liegt
- Die steckbaren Klemmenleisten des Sicherheitskontrollers richtig fest sitzen
- Die Kabel an jedem einzelnen Anschluss sicher befestigt sind
- Ob sich neben dem Sicherheitskontroller oder entlang von Leitungen, die am Kontroller angeschlossen sind, irgendwelche Hochspannungs-Störquellen, Hochfrequenz-Störquellen oder Hochspannungsleitungen befinden
- Geeignete Überspannungsbegrenzer an den Ausgangslasten angebracht sind
- Ob die Umgebungstemperatur des Sicherheitskontrollers innerhalb des Nennbereichs für Umgebungstemperatur liegt (siehe Spezifikationen und Anforderungen auf Seite 20)

## 15.1 Software: Fehlerbehebung

### Schaltfläche Livemodus ist nicht verfügbar (grau abgeblendet)

1. Achten Sie darauf, dass das SC-USB2-Kabel sowohl mit dem Computer als auch mit dem Sicherheitskontroller verbunden ist.

   **Anmerkung:** Die Verwendung des SC-USB2-Kabels von Banner ist vorzuziehen. Bei der Verwendung anderer USB-Kabel müssen Sie darauf achten, dass das Kabel einen Datenleiter enthält. Viele Handyaufladegeräte verfügen nicht über einen Datenleiter.
2. Überprüfen Sie, ob der Sicherheitskontroller korrekt installiert ist; siehe Überprüfen der Treiberinstallation auf Seite 281.
3. Beenden Sie die Software.
4. Trennen Sie den Sicherheitskontroller und verbinden Sie ihn erneut.
5. Starten Sie die Software.

### Die Konfiguration kann nicht vom Sicherheitskontroller gelesen oder nicht an den Sicherheitskontroller gesendet werden (Schaltflächen grau abgeblendet).

1. Achten Sie darauf, dass der **Livemodus** deaktiviert ist.
2. Achten Sie darauf, dass das SC-USB2-Kabel sowohl mit dem Computer als auch mit dem Sicherheitskontroller verbunden ist.

   **Anmerkung:** Die Verwendung des SC-USB2-Kabels von Banner ist vorzuziehen. Bei der Verwendung anderer USB-Kabel müssen Sie darauf achten, dass das Kabel einen Datenleiter enthält. Viele Handyaufladegeräte verfügen nicht über einen Datenleiter.
3. Überprüfen Sie, ob der Sicherheitskontroller korrekt installiert ist; siehe Überprüfen der Treiberinstallation auf Seite 281.
4. Beenden Sie die Software.
5. Trennen Sie den Sicherheitskontroller und verbinden Sie ihn erneut.
6. Starten Sie die Software.

### Ein Block lässt sich nicht an eine andere Position verschieben

Nicht alle Blöcke können verschoben werden. Einige Blöcke können nur innerhalb bestimmter Bereiche verschoben werden.

- **Sicherheitsausgänge** werden statisch eingefügt und lassen sich nicht verschieben. **Referenzierte Sicherheitsausgänge** können an eine beliebige Stelle im linken und mittleren Bereich verschoben werden.
- Die **Sicherheits-** und **nicht sicherheitsrelevanten Eingänge** können an eine beliebige Stelle im linken und mittleren Bereich verschoben werden.
- Die **Funktions-** und **Logikblöcke** können nur innerhalb des mittleren Bereichs verschoben werden.

**Die SC-XM2/3-Schaltfläche ist nicht verfügbar (grau abgeblendet)**

1. Achten Sie darauf, dass alle Anschlüsse fest verbunden sind: sowohl der Anschluss des SC-XMP2 an den USB-Anschluss des Computers als auch an das SC-XM2- oder SC-XM3-Laufwerk.
2. Überprüfen Sie, ob das SC-XMP2-Programmierwerkzeug korrekt installiert ist (siehe Überprüfen der Treiberinstallation auf Seite 281).
3. Beenden Sie die Software.
4. Trennen Sie alle Anschlüsse und verbinden Sie sie erneut: das SC-XMP2-Kabel mit dem USB-Anschluss am Computer und mit dem SC-XM2- bzw. SC-XM3-Laufwerk.
5. Starten Sie die Software.



**Anmerkung:** Wenden Sie sich an einen Anwendungstechniker von Banner, falls Sie weitere Hilfe benötigen.

# 15.2 Software: Fehlercodes

Die folgende Tabelle enthält eine Liste der Fehlercodes, die bei dem Versuch einer ungültigen Verbindung zwischen den Blöcken auf der Registerkarte **Funktionsansicht** ausgegeben werden.



**WARNUNG:**

- **Konfiguration entspricht den anwendbaren Normen**
- Wenn die Anwendung nicht entsprechend überprüft wird, können schwere oder tödliche Verletzungen die Folge sein.
- Die Software für den Sicherheitskontroller von Banner prüft primär die Logikkonfiguration auf Verbindungsfehler. Der Benutzer ist dafür verantwortlich, dass die Anwendung die Anforderungen an die Risikobewertung erfüllt und allen geltenden Normen entspricht.

| Softwarecode | Fehler |
|---|---|
| A.1 | Durch diese Verbindung entsteht ein geschlossener Stromkreis. |
| A.2 | Von diesem Block ist bereits eine Verbindung vorhanden. |
| A.3 | Ein Block darf nicht mit sich selbst verbunden werden. |
| B.2 | Dieser Bypass-Block ist mit dem **TC**-Knoten eines Zweihandsteuerungsblocks verbunden. An den **IN**-Knoten dieses Bypass-Blocks können Sie nur einen Zweihandsteuerungseingang anschließen. |
| B.3 | Dieser Überbrückungsblock ist bereits mit einem anderen Block verbunden. |
| B.4 | Dieser Überbrückungsblock ist mit dem **TC**-Knoten eines Zweihandsteuerungsblocks verbunden und kann nicht mit anderen Blöcken verbunden werden. |
| B.5 | Der Zweihandsteuerungsblock kann nicht mit dem **IN**-Knoten von diesem Überbrückungsblock verbunden werden, da bei ihm die Option „Ausgang schaltet aus, wenn beide Eingänge (**IN** und **BP**) eingeschaltet sind“ aktiviert ist. |
| B.6 | Der **IN**-Knoten eines Überbrückungsblocks kann nicht mit Eingängen für Nothaltschalter und Seilzugschalter verbunden werden. |
| B.7 | Der **IN**-Knoten eines Überbrückungsblocks kann nicht über andere Blöcke mit Eingängen für Nothaltschalter und Seilzugschalter verbunden werden. |
| C.1 | Mit dem **CD**-Knoten kann nur ein Eingang zum Abbruch einer Ausschaltverzögerung verbunden werden. |
| C.2 | Ein Eingang zum Abbruch einer Ausschaltverzögerung kann nur mit dem **CD**-Knoten eines Sicherheitsausgangs, eines Einzelimpuls-Funktionsblocks oder eines Verzögerungsfunktionsblocks verbunden werden. |
| D.1 | Dieser Eingang für die externe Geräteüberwachung ist für eine zweikanalige 2-Klemmen-Schaltung konfiguriert und kann nur mit dem **EDM**-Knoten eines Sicherheitsausgangs verbunden werden. |
| E.1 | Die Ausgangsknoten für einen Zustimmtaster-Block (**P** oder **S**) können nur mit dem **IN**-Knoten eines Sicherheitsausgangs verbunden werden. |
| E.2 | Der **IN**-Knoten eines Zustimmtaster-Blocks kann nicht mit Eingängen für Not-Aus-Schalter und Seilzugschalter verbunden werden. |
| E.3 | Der **ED**-Knoten eines Zustimmtaster-Blocks kann nur mit dem Eingang für einen Zustimmtaster verbunden werden. |
| E.4 | Der **ED**-Knoten eines Zustimmtaster-Blocks kann nicht über andere Blöcke mit Eingängen für Not-Aus-Schalter und Seilzugschalter verbunden werden. |
| E.5 | Ein Zustimmtaster-Block, bei dem ein Eingang für eine Zweihandsteuerung mit dem **IN**-Knoten verbunden ist, kann nicht mit einem Sicherheitsausgang verbunden werden, bei dem als *Verzögerung des Sicherheitsausgangs* die Einstellung „Aus-Verzögerung“ gewählt ist. |

| Softwarecode | Fehler |
|---|---|
| F.1 | Die Eingänge für einen Nothaltschalter und einen Seilzugschalter können nicht gemutet werden. Somit können sie auch nicht mit dem **IN**-Knoten eines Muting-Funktionsblocks oder dem **M-Sicherheitseingang** der Funktionsblocks Pressensteuerungseingänge verbunden werden. |
| F.2 | Not-Aus- und Seilzugschaltereingänge können nicht mit einem Latch-Reset-Block verbunden werden, der an einen Muting-Block angeschlossen ist. |
| F.3 | Ein Latch-Reset-Block, der mit einem Eingang für einen Not-Aus- oder Seilzugschalter verbunden ist, kann nicht an einen Muting-Block angeschlossen werden. |
| G.1 | **XS/SC26-2 FID 1, 2 und 3 und SC10:** Mit dem **FR**-Knoten eines Sicherheitsausgangs kann nur ein manueller Reset-Ausgang verbunden werden.<br>**XS/SC26-2 FID 4 oder höher:** Mit dem **FR**-Knoten eines Sicherheitsausgangs kann nur ein Eingang für manuellen Reset oder ein Ausgangsknoten eines speziellen Reset-ODER-Blocks verbunden werden. |
| G.2 | **XS/SC26-2 FID 1, 2 und 3 und SC10:** Nur ein manueller Reset-Eingang kann mit dem **LR**-Knoten eines Latch-Reset-Blocks oder eines Sicherheitsausgangs verbunden werden.<br>**XS/SC26-2 FID 4 oder höher:** Mit dem **LR**-Knoten eines Latch-Reset-Blocks oder Sicherheitsausgangs kann nur ein Eingang für manuellen Reset oder der Ausgangsknoten eines speziellen Reset-ODER-Blocks verbunden werden. |
| G.3 | **XS/SC26-2 FID 1, 2 und 3 und SC10:** Mit dem **RST**-Knoten eines Zustimmtaster-Blocks kann nur ein Ausgang für manuellen Reset verbunden werden.<br>**XS/SC26-2 FID 4 oder höher:** Mit dem **RST**-Knoten eines Zustimmtaster-Blocks kann nur ein Eingang für manuellen Reset oder ein Ausgangsknoten eines speziellen Reset-ODER-Blocks verbunden werden. |
| G.4 | **XS/SC26-2 FID 1, 2 und 3 und SC10:** Ein manueller Reset-Eingang kann nur mit dem **LR**- und dem **FR**-Knoten eines Sicherheitsausgangs, dem **LR**-Knoten eines Latch-Reset-Blocks, dem **RST**-Knoten eines Zustimmtaster-Blocks und dem **SET**- und **RST**-Knoten des Flip-Flop-Blocks verbunden werden.<br>**XS/SC26-2 FID 4 oder höher:** Ein Eingang für manuellen Reset kann nur mit einem **LR**- und einem **FR**-Knoten eines Sicherheitsausgangs, einem **LR**-Knoten eines Latch-Reset-Blocks, einem **RST**-Knoten eines Zustimmtaster-Blocks, **SET**- und **RST**-Knoten der Flip-Flop-Blöcke, einem **RST**-Knoten eines Pressensteuerungsblocks und einem Eingangsknoten eines speziellen Reset-ODER-Blocks verbunden werden. |
| G.5 | Der Eingangsknoten eines speziellen Reset-ODER-Blocks kann nur mit einem Eingang für manuellen Reset, einem virtuellen Eingang für manuellen Reset und dem Ausgangsknoten eines speziellen Reset-ODER-Blocks verbunden werden. |
| G.6 | Der Ausgangsknoten eines speziellen Reset-ODER-Blocks kann nur mit **LR**- und **FR**-Knoten eines Sicherheitsausgangs, einem **LR**-Knoten eines Latch-Reset-Blocks, einem **RST**-Knoten eines Zustimmtaster-Blocks, **SET**- und **RST**-Knoten der Flip-Flop-Blöcke und einem Eingangsknoten eines speziellen Reset-ODER-Blocks verbunden werden. |
| H.1 | Ein Latch-Reset-Block, der bereits mit einem Funktionsblock verbunden ist, kann nicht mit einem Muting-Block verbunden werden. |
| H.2 | Ein Latch-Reset-Block, der bereits mit einem Muting-Block verbunden ist, kann nicht mit einem anderen Funktionsblock verbunden werden. |
| I.1 | Nur die Eingänge für Muting-Sensorpaar, Optosensor, Schutztürschalter, Sicherheitsmatte oder Schutzhaltschalter können mit dem **MP1**- und dem **MP2**-Knoten eines Muting-Blocks oder mit dem **MP1**-Knoten eines Zweihandsteuerungsblocks verbunden werden. |
| I.2 | Der **MP1**- und der **MP2**-Knoten eines Muting-Blocks und der **MP1**-Knoten eines Zweihandsteuerungsblocks können mit Eingängen verbunden werden, die nur zweikanalige Schaltungen verwenden. |
| I.3 | Der Eingang für Muting-Sensorpaar kann nur mit dem **MP1**- und dem **MP2**-Knoten eines Muting-Blocks oder mit dem **MP1**-Knoten eines Zweihandsteuerungsblocks verbunden werden. |
| J.1 | **XS/SC26-2 FID 1, 2 und 3 und SC10 FID 1:** Ein Zweihandsteuerungsblock kann nur mit dem **IN**-Knoten eines Zustimmtaster-Blocks oder dem **IN**-Knoten eines Sicherheitsausgangs verbunden werden.<br>**XS/SC26-2 ab FID 4 oder SC10 ab FID 2:** Ein Zweihandsteuerungsblock kann nur mit einem Logikblock (ausgenommen Flip-Flop-Blöcke), dem **IN**-Knoten eines Zustimmtaster-Blocks oder dem **IN**-Knoten eines Sicherheitsausgangs verbunden werden. |
| J.3 | Nur Zweihandsteuerungseingänge oder Überbrückungsblöcke mit daran angeschlossenen Zweihandsteuerungseingängen können mit dem **TC**-Knoten eines Zweihandsteuerungsblocks verbunden werden. Ein Überbrückungsblock, mit dessen **IN**-Knoten ein Eingang für eine Zweihandsteuerung verbunden ist, kann nur an einen **TC**-Knoten eines Zweihandsteuerungsblocks angeschlossen werden. |
| K.1 | **XS/SC26-2 FID 1, 2 und 3 und SC10 FID 1:** Ein Zweihandsteuerungseingang kann nur mit einem Zweihandsteuerungsblock (**TC**-Knoten) oder einem Überbrückungsblock (**IN**-Knoten) verbunden werden.<br>**XS/SC26-2 FID 4 oder höher oder SC10 FID 2 oder höher:** Ein Eingang für eine Zweihandsteuerung kann nur mit einem Zweihandsteuerungsblock (**TC**-Knoten), einem Überbrückungsblock (**IN**-Knoten), Logikblöcken (außer Flip-Flop-Blöcken), einem Pressensteuerungsblock (**GO**-Knoten) oder einem Ausgang ohne Ausschaltverzögerung verbunden werden. |
| K.2 | **XS/SC26-2 FID 1, 2 und 3 und SC10 FID 1:** Ein Sicherheitsausgang, bei dem für die *Verzögerung des Sicherheitsausgangs* die Einstellung „Ausschaltverzögerung“ gewählt ist, kann nicht mit einem Zweihandsteuerungsblock verbunden werden.<br>**XS/SC26-2 FID 4 oder höher oder SC10 FID 2 oder höher:** Ein Sicherheitsausgang, bei dem für die *Verzögerung des Sicherheitsausgangs* die Einstellung „Ausschaltverzögerung“ gewählt ist, kann nicht direkt mit einem Zweihandsteuerungsblock verbunden werden. |
| K.3 | Ein Sicherheitsausgang, bei dem für die *Verzögerung des Sicherheitsausgangs* die Einstellung „Ausschaltverzögerung“ gewählt ist, kann nicht über einen Zustimmtaster-Block mit einem Zweihandsteuerungsblock verbunden werden. |

| Softwarecode | Fehler |
|---|---|
| L.1 | Dieser Sicherheitsausgang ist aufgrund eines Statusausgangs deaktiviert, der seine Klemmen verwendet. |
| L.2 | Der **IN**-Knoten eines Sicherheitsausgangs kann nicht mit den Eingängen für externe Geräteüberwachung, einstellbare Ventilüberwachung, Muting-Sensorpaar, Überbrückungsschalter, manuellen Reset, Muting-Freigabe oder Abbruch der Ausschaltverzögerung verbunden werden. |
| L.3 | Ein Sicherheitsausgangsblock, bei dem die *LR- (Latch-Reset-)* Funktion aktiviert ist, kann nicht mit Zweihandsteuerungsblöcken oder Zustimmtaster-Blöcken verbunden werden. |
| L.4 | **XS/SC26-2 FID 1, 2 und 3 und SC10 FID 1:** Ein Sicherheitsausgangsblock, bei dem für den *Power up Mode (Anlaufmodus)* die Einstellung „Manual Reset (Manueller Reset)“ gewählt ist, kann nicht mit Zweihandsteuerungsblöcken oder Zustimmtaster-Blöcken verbunden werden.<br>**XS/SC26-2 ab FID 4 oder SC10 ab FID 2:** Ein Sicherheitsausgangsblock, bei dem für den *Power up Mode (Anlaufmodus)* die Einstellung „Manual Reset (Manueller Reset)" gewählt ist, kann nicht mit Zweihandsteuerungseingängen, Zweihandsteuerungsblöcken oder Zustimmtaster-Blöcken verbunden werden. |
| P.1 | Nur physische oder virtuelle EIN/AUS-Eingänge können an die **RUN-**, **SCHRITTSTEUERUNG-AUFWÄRTS-** und **SCHRITTSTEUERUNG-ABWÄRTS-Knoten** des Funktionsblocks des Pressensteuerungsmodus angeschlossen werden. |
| P.2 | Nur ein physikalischer EIN/AUS-Eingang kann mit den **TOS**- und **BOS**-Knoten des Pressensteuerungs-Funktionsblocks und dem **PIP**-Knoten des Funktionsblocks Pressensteuerungseingänge verbunden werden. |
| P.3 | Mit dem **SQS**-Eingangsknoten des Funktionsblocks Pressensteuerungseingang kann nur ein **SQS**-Eingang verbunden werden. |
| P.4 | Der einzige Eingang, der an den **M-Sensor**-Eingang des Funktionsblocks Pressensteuerungseingang angeschlossen werden kann, ist ein Muting-Sensor-Eingangsgerät der Pressensteuerung. |
| P.5 | Wenn der Pressensteuerungsblock für die Einzelauslösersteuerung konfiguriert ist, kann der **GO**-Eingangsknoten nur mit einem Zyklusinitiierungseingang, einem Fußpedaleingang oder einem Zweihandsteuerungseingang verbunden werden. Wenn der Pressensteuerungsblock für die manuelle Aufwärtshub-Einstellung konfiguriert ist, kann der **GO**-Eingangsknoten nur mit einem Fußpedal-Eingang oder einem Zweihandsteuerungseingang verbunden werden. |
| P.6 | Wenn im Pressensteuerungs-Funktionsblock die Einzelauslösersteuerung ausgewählt ist, sind sequenzieller Stopp (**SQS**) und manueller Aufwärtshub nicht zulässig. |
| P.7 | An den **Ft Pedal**-Eingang des Funktionsblocks Pressensteuerungseingänge kann nur ein physischer Eingang zum Ein-/Ausschalten oder ein Fußpedal-Eingang angeschlossen werden. |
| P.8 | Die Ausgangsknoten des Pressensteuerungs-Funktionsblocks (**U**, **D**, **H** und **L**) können nur mit dem **IN**-Knoten eines Sicherheitsausgangs verbunden werden. |
| P.9 | Wenn der Muting-Sensor-Eingang der Pressensteuerung nicht ausgewählt ist, kann nur ein zweikanaliger SQS-Eingang mit dem **SQS**-Eingangsknoten des Funktionsblocks Pressensteuerungseingang verbunden werden. |

# 15.3 Überprüfen der Treiberinstallation

Dieser Abschnitt gilt sowohl für den XS/SC26-2 als auch für den SC10-2.

**Windows 7, 8 und 10**

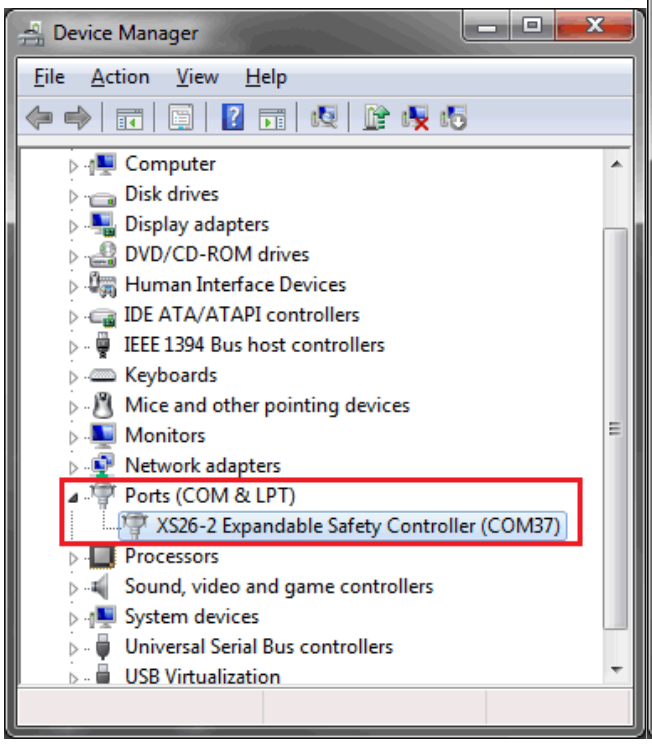
1. Klicken Sie auf **Start**.
2. Geben Sie „Geräte-Manager“ in das Feld *Programme/Dateien durchsuchen* unten im Menü ein und klicken Sie auf **Geräte-Manager**, wenn Windows dieses Programm gefunden hat.
3. Erweitern Sie das Dropdown-Menü **Anschlüsse (COM & LPT)**.
4. Suchen Sie **XS26-2 Erweiterbarer Sicherheitskontroller**, gefolgt von einer COM-Anschlussnummer (z. B. COM3). Der Eintrag darf weder ein Ausrufezeichen noch ein rotes × oder einen Abwärtspfeil enthalten. Falls Sie keines dieser Kennzeichen sehen, ist Ihr Gerät korrekt installiert. Wird eines dieser Kennzeichen angezeigt, beheben Sie die Probleme anhand der Hinweise, die dieser Tabelle folgen.

## Windows 7, 8 und 10

### Treiber für den Sicherheitskontroller XS/SC26-2

1. Erweitern Sie das Dropdown-Menü **Anschlüsse (COM & LPT)**.
2. Suchen Sie **XS26-2 Erweiterbarer Sicherheitskontroller**, gefolgt von einer COM-Anschlussnummer (z. B. COM3). Der Eintrag darf weder ein Ausrufezeichen noch ein rotes × oder einen Abwärtspfeil enthalten. Falls Sie keines dieser Kennzeichen sehen, ist Ihr Gerät korrekt installiert. Wird eines dieser Kennzeichen angezeigt, beheben Sie die Probleme anhand der Hinweise, die dieser Tabelle folgen.

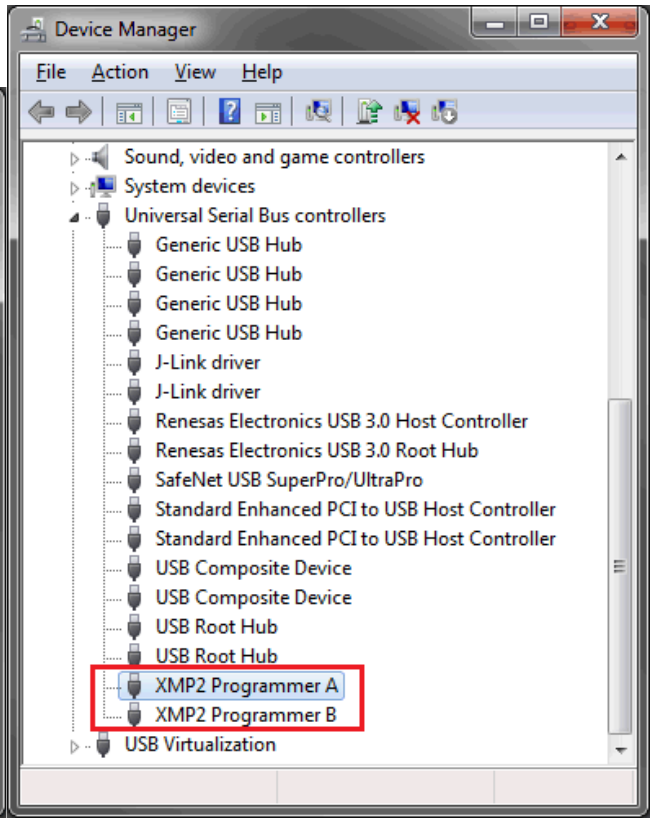
*Abbildung 274. Treiber für Sicherheitskontroller XS/SC26-2 korrekt installiert*




### SC-XMP2-Treiber

1. Erweitern Sie das Dropdown-Menü **USB-Controller**.
2. Suchen Sie **XMP2 Programmer A** und**XMP2 Programmer B**. Keiner dieser beiden Einträge darf ein Ausrufezeichen, ein rotes × oder einen Abwärtspfeil enthalten. Falls Sie keines dieser Kennzeichen sehen, ist Ihr Gerät korrekt installiert. Wird eines dieser Kennzeichen angezeigt, beheben Sie die Probleme anhand der Hinweise, die dieser Tabelle folgen.

*Abbildung 275. SC-XMP2-Treiber korrekt installiert*



**So beheben Sie die durch ein Ausrufezeichen, ein rotes × oder einen Abwärtspfeil gekennzeichneten Probleme:**

1. Achten Sie darauf, dass Ihr Gerät aktiviert ist:
    a. Klicken Sie mit der rechten Maustaste auf den Eintrag, der mit dem Kennzeichen versehen ist.
    b. Wenn Sie **Deaktivieren** sehen, ist das Gerät aktiviert. Wenn Sie **Aktivieren** sehen, ist das Gerät deaktiviert.
        - Wenn das Gerät aktiviert ist, fahren Sie mit den Fehlerbehebungsschritten fort.
        - Wenn das Gerät deaktiviert ist, klicken Sie auf **Aktivieren**. Wird das Kennzeichen hierdurch nicht entfernt, fahren Sie mit dem nächsten Schritt fort.
2. Trennen Sie das USB-Kabel entweder vom Sicherheitskontroller oder vom Computer, warten Sie einige Sekunden und verbinden Sie das Kabel dann erneut. Wenn das Kennzeichen hierdurch nicht entfernt wird, fahren Sie mit dem nächsten Schritt fort.
3. Verbinden Sie den Sicherheitskontroller mit einem anderen USB-Anschluss. Wird das Kennzeichen hierdurch nicht entfernt, fahren Sie mit dem nächsten Schritt fort.
4. Starten Sie Ihren Computer neu. Wird das Kennzeichen hierdurch nicht entfernt, fahren Sie mit dem nächsten Schritt fort.
5. Deinstallieren Sie die Software unter **Programme hinzufügen/entfernen** oder **Programme und Funktionen** in der **Systemsteuerung**, und installieren Sie sie dann erneut. Wird das Kennzeichen hierdurch nicht entfernt, fahren Sie mit dem nächsten Schritt fort.
6. Wenden Sie sich an einen Anwendungstechniker von Banner.

**Führen Sie diese Schritte aus, um den im Geräte-Manager aufgeführten Sicherheitskontroller als „Allgemeines USB-Gerät“ anzuzeigen.**

1. Klicken Sie mit der rechten Maustaste auf den Port „Allgemeines USB-Gerät“, der zum Banner-Sicherheitskontroller gehört.
2. Klicken Sie auf **Treiber aktualisieren**.
3. Wählen Sie **Auf dem Computer nach Treibersoftware suchen** aus.
4. Klicken Sie rechts neben dem Feld **Diesen Speicherplatz durchsuchen** auf **Durchsuchen**. Ein neues Fenster wird geöffnet.
5. Auswählen **Lokaler Datenträger (C:)** > **Programme (x86)** > **Banner Engineering** > **Banner Safety Controller** > **Treiber**.
6. Klicken Sie auf **OK**, um das Fenster zu schließen.
7. Klicken Sie im Feld zum Aktualisieren des Treibers auf **Weiter**. Der Treiber sollte jetzt aktualisiert worden sein.

Möglicherweise müssen Sie die Software des Sicherheitskontroller von Banner schließen und wieder öffnen. Der USB-Port sollte jetzt die Banner-Sicherheitskontroller mit der Software verknüpfen.

## 15.4 Fehlersuche und -behebung

Je nach Konfiguration kann der Sicherheitskontroller unterschiedliche Eingangs-, Ausgangs- und Systemfehler erkennen, einschließlich:

- Einen verschweißten Kontakt
- Einen offenen Kontakt
- Einen Kurzschluss zwischen Kanälen
- Einen Erdschluss
- Einen Kurzschluss zu einer Spannungsquelle
- Einen Kurzschluss zu einem anderen Eingang
- Eine lose oder offene Verbindung
- Ein überschrittenes Betriebszeitlimit
- Einen Spannungseinbruch
- Einen Übertemperaturzustand

Bei Erkennung eines Fehlers wird eine Meldung mit einer Fehlerbeschreibung im Menü **Fehlerdiagnose** angezeigt (Ausführungen mit LCD-Anzeige). Verwenden Sie für Ausführungen, die nicht mit einer LCD-Anzeige ausgestattet sind, die Registerkarte **Livemodus** in der Software auf einem PC, der über das SC-USB2-Kabel mit dem Sicherheitskontroller verbunden ist. Fehlerdiagnosen sind auch über das Netzwerk verfügbar. Unter Umständen wird eine weitere Meldung mit Angaben dazu angezeigt, wie der Fehler behoben werden kann.



**Anmerkung:** Das Fehlerprotokoll wird gelöscht, wenn die Spannungsversorgung für den Sicherheitskontroller aus- und wiedereingeschaltet wird.

### 15.4.1 Fehlercode-Tabelle für XS/SC26-2

Die folgende Tabelle enthält den Sicherheitskontroller-Fehlercode, die angezeigte Nachricht, alle weiteren Nachrichten sowie die Schritte zur Behebung des Fehlers.

Der Sicherheitskontroller-Fehlercode setzt sich aus dem Fehlercode und dem erweiterten Fehlercode zusammen. Das Format des Fehlercodes ist `Fehlercode "Punkt" erweiterter Fehlercode` . Der Sicherheitskontroller-Fehlercode 2.1 wird beispielsweise vom Fehlercode `2` und dem erweiterten Fehlercode `1` angegeben. Der Indexwert der Fehlermeldung ist der Fehlercode und der erweiterte Fehlercode zusammen und umfasst eine führende Null mit dem erweiterten Fehlercode, falls erforderlich. Der Sicherheitskontroller-Fehlercode 2.1 wird beispielsweise vom Fehlermeldungsindex `201` angegeben. Mit dem Indexwert der Fehlermeldung kann der vollständige Fehlercode bequem nur anhand eines einzigen 16-Bit-Registerwerts abgerufen werden.

| Fehlercode | Dargestellte Meldung | Zusätzliche Meldung | Lösungsschritte |
|---|---|---|---|
| 1.1 | Ausgangsfehler | **Basismodul oder Transistormodul**<br>Überprüfen, ob Kurzschlüsse vorliegen<br>**Relaismodul**<br>– | **Basismodul oder Transistormodul**<br>Ein Sicherheitsausgang erscheint als EIN, wenn er AUS sein sollte:<br>• Überprüfen, ob Kurzschluss zur externen Spannungsquelle vorliegt<br>• Die Größe des DC-Common-Leiters, der mit den Sicherheitsausgangslasten verbunden ist, überprüfen Als Leiter muss ein dicker oder möglichst kurzer Draht verwendet werden, um Widerstand und Spannungsabfall zu minimieren. Bei Bedarf kann ein separater DC-Common-Leiter für jedes Ausgangspaar verwendet werden, und/oder dieser DC-Common-Rückleitung darf nicht gemeinsam mit anderen Geräten verwendet werden (siehe Installation des Common-Leiters auf Seite 65).<br>**Relaismodul**<br>• Relais-Modul auswechseln |
| 1.2 | Ausgangsfehler | **Basismodul oder Transistormodul**<br>Überprüfen, ob Kurzschlüsse vorliegen<br>**Relaismodul**<br>– | **Basismodul oder Transistormodul**<br>Ein eingeschalteter Sicherheitsausgang erfasst eine fehlerhafte Verbindung zu einer anderen Spannungsquelle:<br>• Überprüfen, ob zwischen Sicherheitsausgängen ein Kurzschluss vorliegt<br>• Überprüfen, ob Kurzschluss zur externen Spannungsquelle vorliegt<br>• Kompatibilität des Lastgeräts überprüfen<br>• Die Größe des DC-Common-Leiters, der mit den Sicherheitsausgangslasten verbunden ist, überprüfen Als Leiter muss ein dicker oder möglichst kurzer Draht verwendet werden, um Widerstand und Spannungsabfall zu minimieren. Bei Bedarf kann ein separater DC-Common-Leiter für jedes Ausgangspaar verwendet werden, und/oder dieser DC-Common-Rückleitung darf nicht gemeinsam mit anderen Geräten verwendet werden (siehe Installation des Common-Leiters auf Seite 65).<br>**Relaismodul**<br>• Relais-Modul auswechseln |
| 1.3 – 1.8 | Interner Fehler | - | Interner Fehler: Banner Engineering kontaktieren (siehe Reparaturen und Garantie auf Seite 293) |
| 1.9 | Ausgangsfehler | Interner Relais-Fehler | • Relais-Modul auswechseln |
| 1.10 | Ausgangsfehler | Eingangszeitverhalten überprüfen | Fehler beim Sequenz-Zeitverhalten:<br>• Zur Löschung des Fehlers einen System-Reset durchführen |
| 2.1 | Gleichzeitigkeitsfehler | Eingang schalten | An einem zweikanaligen Eingang oder einem antivalenten Eingang mit beiden Eingängen im Ein-Zustand ging ein Eingang in den Aus-Zustand und wieder zurück in den Ein-Zustand.<br>An einem zweifach-antivalenten Eingang mit beiden Eingangspaaren im Ein-Zustand ging ein Eingangspaar in den Aus-Zustand und wieder zurück in den Ein-Zustand.<br>• Verdrahtung überprüfen<br>• Eingangssignale überprüfen<br>• Gegebenenfalls die Entprellzeiten anpassen |
| 2.2 | Gleichzeitigkeitsfehler | Eingang schalten | An einem zweikanaligen Eingang oder einem antivalenten Eingang ging ein Eingang in den Ein-Zustand, aber der andere Eingang folgte nicht innerhalb von 3 Sekunden.<br>An einem zweifach-antivalenten Eingang ging ein Eingangspaar in den Ein-Zustand, aber das andere Eingangspaar folgte nicht innerhalb von 3 Sekunden.<br>• Verdrahtung überprüfen<br>• Zeitverhalten der Eingangssignale kontrollieren |
| 2.3 oder 2.5 | Gleichzeitigkeitsfehler | Eingang schalten | An einem zweifach-antivalenten Eingang mit beiden Eingängen eines antivalenten Paares im Ein-Zustand ging ein Eingang dieses antivalenten Paares in den Aus-Zustand und wieder zurück in den Ein-Zustand:<br>• Verdrahtung überprüfen<br>• Eingangssignale überprüfen<br>• Überprüfen, ob die Stromversorgung Eingangssignale liefert<br>• Gegebenenfalls die Entprellzeiten anpassen |

| Fehlercode | Dargestellte Meldung | Zusätzliche Meldung | Lösungsschritte |
|---|---|---|---|
| 2.4 oder 2.6 | Gleichzeitigkeitsfehler | Eingang schalten | An einem zweifach-antivalenten Eingang ging ein Eingang von einem antivalenten Paar in den Ein-Zustand, aber der andere Eingang desselben antivalenten Paares folgte nicht innerhalb des Zeitlimits.<br>• Verdrahtung überprüfen<br>• Zeitverhalten der Eingangssignale kontrollieren |
| 2.7 | Interner Fehler | | Interner Fehler: Banner Engineering kontaktieren (siehe Reparaturen und Garantie auf Seite 293) |
| 2.8 – 2.9 | Eingangsfehler | Anschluss xx überprüfen | Eingang im Ein-Zustand blockiert:<br>• Überprüfen, ob Kurzschlüsse zu anderen Eingängen oder zu einer anderen Spannungsquelle vorliegen<br>• Kompatibilität des Eingangsgeräts überprüfen |
| 2.10 | Eingangsfehler | Anschluss xx überprüfen | • Überprüfen, ob zwischen den Eingängen ein Kurzschluss vorliegt |
| 2.11 – 2.12 | Eingangsfehler | Anschluss xx überprüfen | • Überprüfen, ob Erdschluss vorliegt |
| 2.13 | Eingangsfehler | Anschluss xx überprüfen | Eingang im Aus-Zustand blockiert<br>• Überprüfen, ob Erdschluss vorliegt |
| 2.14 | Eingangsfehler | Anschluss xx überprüfen | Fehlende Testimpulse:<br>• Überprüfen, ob ein Kurzschluss zu anderen Eingängen oder zu einer anderen Spannungsquelle vorliegt |
| 2.15 | Leitungsunterbrechung | Anschluss xx überprüfen | • Überprüfen, ob eine Leitungsunterbrechung vorliegt |
| 2.16 – 2.18 | Eingangsfehler | Anschluss xx überprüfen | Fehlende Testimpulse:<br>• Überprüfen, ob ein Kurzschluss zu anderen Eingängen oder zu einer anderen Spannungsquelle vorliegt |
| 2.19 | Leitungsunterbrechung | Anschluss xx überprüfen | • Überprüfen, ob eine Leitungsunterbrechung vorliegt |
| 2.20 | Eingangsfehler | Anschluss xx überprüfen | Fehlende Testimpulse:<br>• Überprüfen, ob Erdschluss vorliegt |
| 2.21 | Leitungsunterbrechung | Anschluss xx überprüfen | • Überprüfen, ob eine Leitungsunterbrechung vorliegt |
| 2.22 – 2.23 | Eingangsfehler | Anschluss xx überprüfen | • Überprüfen, ob am Eingang ein instabiles Signal vorliegt |
| 2.24 | Eingang während Überbrückung aktiviert | System-Reset ausführen | Eine Zweihandsteuerung wurde aktiviert (eingeschaltet), während sie überbrückt wurde. |
| 2.25 | Eingangsfehler | Überwachungstimer abgelaufen, bevor AVM geschlossen wurde | Nachdem sich der zugehörige Sicherheitsausgang ausgeschaltet hat, wurde der AVM-Eingang nicht vor Ablauf seiner AVM-Überwachungszeit geschlossen:<br>• Die AVM ist möglicherweise getrennt. Kabelanschlüsse zur AVM überprüfen<br>• Entweder die AVM ist getrennt, oder sie reagiert zu langsam auf das Ausschalten des Sicherheitsausgangs.<br>• Kabelanschlüsse zur AVM überprüfen<br>• Zeitgebereinstellung überprüfen und bei Bedarf erhöhen<br>• Banner Engineering kontaktieren |
| 2.26 | Eingangsfehler | AVM beim Einschalten des Ausgangs nicht geschlossen | Der AVM-Eingang war offen, sollte sich aber beim Einschaltbefehl an den verbundenen Sicherheitsausgang geschlossen haben:<br>• Die AVM ist möglicherweise getrennt. Kabelanschlüsse zur AVM überprüfen |
| 3.1 | EDMxx-Fehler | Anschluss xx überprüfen | EDM-Kontakt wurde geöffnet, bevor sich die Sicherheitsausgänge einschalteten:<br>• Überprüfen, ob Kontaktgeber oder Relais im Ein-Zustand verschweißt sind<br>• Auf Leitungsunterbrechungen überprüfen |
| 3.2 | EDMxx-Fehler | Anschluss xx überprüfen | EDM-Kontakte wurden nach dem Abschalten der Sicherheitsausgänge nicht innerhalb von 250 ms geschlossen:<br>• Überprüfen, ob Kontaktgeber oder Relais zu langsam abfallen oder im Ein-Zustand verschweißt sind.<br>• Auf Leitungsunterbrechungen überprüfen |
| 3.4 | EDMxx-Fehler | Anschluss xx überprüfen | Kontakte der beiden Rückführkreise (EDM-Kontaktpaar) länger als 250 ms in unterschiedlichem Zustand.<br>• Überprüfen, ob Kontaktgeber oder Relais zu langsam abfallen oder im Ein-Zustand verschweißt sind.<br>• Auf Leitungsunterbrechungen überprüfen |

| Fehlercode | Dargestellte Meldung | Zusätzliche Meldung | Lösungsschritte |
|---|---|---|---|
| 3.5 | EDMxx-Fehler | Anschluss xx überprüfen | • Überprüfen, ob am Eingang ein instabiles Signal vorliegt |
| 3.6 | EDMxx-Fehler | Anschluss xx überprüfen | • Überprüfen, ob Erdschluss vorliegt |
| 3.7 | EDMxx-Fehler | Anschluss xx überprüfen | • Überprüfen, ob zwischen den Eingängen ein Kurzschluss vorliegt |
| 3.8 | AVMxx-Fehler | System-Reset ausführen | Nachdem sich der zugehörige Sicherheitsausgang ausgeschaltet hat, wurde ein mit diesem Ausgang verbundener AVM-Eingang nicht vor Ablauf seiner AVM-Überwachungszeit geschlossen:<br>• Entweder die AVM ist getrennt, oder sie reagiert zu langsam auf das Ausschalten des Sicherheitsausgangs.<br>• Den AVM-Eingang überprüfen und dann zur Löschung des Fehlers einen System-Reset ausführen |
| 3.9 | Eingangsfehler | AVM beim Einschalten des Ausgangs nicht geschlossen | Der AVM-Eingang war offen, sollte sich aber beim Einschaltbefehl an den verbundenen Sicherheitsausgang geschlossen haben:<br>• Die AVM ist möglicherweise getrennt. Kabelanschlüsse zur AVM überprüfen |
| 3.10 | Interner Fehler | - | Interner Fehler: Banner Engineering kontaktieren (siehe Reparaturen und Garantie auf Seite 293) |
| 4.x | - | - | Siehe in der folgenden Tabelle. |
| 5.1 – 5.3 | Interner Fehler | - | Interner Fehler: Banner Engineering kontaktieren (siehe Reparaturen und Garantie auf Seite 293) |
| 6.xx | Interner Fehler | - | Ungültige Konfigurationsdaten. Möglicher interner Fehler:<br>• Neue Konfiguration in den Sicherheitskontroller zu schreiben versuchen |
| 7.1 | Press Control Fault (Fehler in der Pressensteuerung) | TOS und BOS prüfen | TOS- und BOS-Eingänge gleichzeitig eingeschaltet<br>• Prüfung auf Kurzschlüsse an TOS- und BOS-Eingängen<br>• Auf Funktionsstörungen bei den TOS- und BOS-Geräten prüfen |
| 7.2 | Press Control Fault (Fehler in der Pressensteuerung) | TOS und SQS überprüfen | TOS- und SQS-Eingänge gleichzeitig eingeschaltet<br>• Prüfung auf Kurzschlüsse an TOS- und SQS-Eingängen<br>• Auf Funktionsstörungen bei den TOS- und SQS-Geräten prüfen |
| 7.3 | Press Control Fault (Fehler in der Pressensteuerung) | TOS und PCMS überprüfen | TOS- und PCMS-Eingänge gleichzeitig eingeschaltet<br>• Prüfung auf Kurzschlüsse an TOS- und PCMS-Eingängen<br>• Auf Funktionsstörungen bei den TOS- und PCMS-Geräten prüfen |
| 7.4 | Press Control Fault (Fehler in der Pressensteuerung) | SQS und BOS prüfen | SQS-BOS-Sequenzierungsfehler (BOS wurde vor SQS eingeschaltet)<br>• Verdrahtung von SQS- und BOS-Sensoren überprüfen<br>• Auf Platzierungs- und Funktionsprobleme von SQS- und BOS-Sensoren prüfen |
| 7.5 | Press Control Fault (Fehler in der Pressensteuerung) | TOS überprüfen | TOS-Timeout-Fehler (Beim automatischen Anlauf wurde das interne Zeitlimit von 30 Sekunden überschritten.)<br>• Verdrahtung des TOS-Systems prüfen<br>• Auf Platzierungs- und Funktionsprobleme des TOS-Sensors prüfen |
| 7.6 | Press Control Fault (Fehler in der Pressensteuerung) | BOS prüfen | BOS-Timeout-Fehler (Beim automatischen Abwärtshub wurde das interne Zeitlimit von 30 Sekunden überschritten.)<br>• Verdrahtung des BOS-Systems prüfen<br>• Auf Platzierungs- und Funktionsprobleme des BOS-Sensors prüfen |
| 7.7 | Press Control Fault (Fehler in der Pressensteuerung) | Moduswahleingänge prüfen | Moduswahlfehler (mehr als ein Moduswahleingang gleichzeitig eingeschaltet)<br>• Verdrahtung von den Modus-Statuseingängen überprüfen<br>• Moduswahlschalter auf Fehler überprüfen |
| 7.8 | Press Control Fault (Fehler in der Pressensteuerung) | - | Index-Fehler (interner Konfigurationsfehler)<br>Banner Engineering kontaktieren (siehe Reparaturen und Garantie auf Seite 293) |
| 7.9 | Press Control Fault (Fehler in der Pressensteuerung) | Fußpedal-Eingang prüfen | Fußpedal-Fehler (Bei Konfiguration mit einem SQS wurde der Fußpedal-Eingangsknoten anstelle des GO-Eingangsknotens eingeschaltet.)<br>• Sequenzierungsfehler<br>• Wenn der Fehler weiterhin besteht, die Verdrahtung der THC- und Fußpedal-Eingänge prüfen |
| 7.10 | Press Control Fault (Fehler in der Pressensteuerung) | Abwärts-Zylinder prüfen | Abwärts-AVM-Fehler (Abwärts-AVM befindet sich im falschen Zustand im Vergleich zum erwarteten Zustand)<br>• AVM-Verdrahtung überprüfen<br>• AVM-Sensor und Abwärts-Hubsystem prüfen |

| Fehlercode | Dargestellte Meldung | Zusätzliche Meldung | Lösungsschritte |
|---|---|---|---|
| 7.11 | Press Control Fault (Fehler in der Pressensteuerung) | Aufwärts-Zylinder überprüfen | Aufwärts-AVM-Fehler (Aufwärts-AVM befindet sich im falschen Zustand im Vergleich zum erwarteten Zustand)<br>• Aufwärts-AVM-Verdrahtung überprüfen<br>• Aufwärts-AVM-Sensor und Aufwärts-Hubsystem überprüfen |
| 7.12 | Press Control Fault (Fehler in der Pressensteuerung) | Hoch-Zylinder prüfen | Hoch-AVM-Fehler (Hoch-AVM ist im falschen Zustand im Vergleich zum erwarteten Zustand)<br>• Verdrahtung von Hoch-AVM überprüfen<br>• Hoch-AVM-Sensor und Hoch-Hubsystem prüfen |
| 7.13 | Press Control Fault (Fehler in der Pressensteuerung) | Tief-Zylinder prüfen | Tief-AVM-Fehler (Tief-AVM ist im falschen Zustand im Vergleich zum erwarteten Zustand)<br>• Tief-AVM-Verdrahtung überprüfen<br>• Tief-AVM-Sensor und Tief-Hubsystem überprüfen |
| 7.14 | Press Control Fault (Fehler in der Pressensteuerung) | Gleichzeitigkeit von SQS und PCMS | SQS-PCMS-Gleichzeitigkeitsfehler (3-Sekunden-Zeitgrenze zwischen Eingaben überschritten)<br>• Verdrahtung von SQS und PCMS prüfen<br>• Platzierung von SQS und PCMS unter Berücksichtigung der Stößelgeschwindigkeit prüfen |
| 7.15 | Press Control Fault (Fehler in der Pressensteuerung) | SQS-Status prüfen | SQS-Zustandsfehler (SQS-Zustandsstufe während des Pressenzyklus nicht wie erwartet)<br>• Verdrahtung des SQS-Eingangs prüfen<br>• Platzierung des SQS-Sensors und seine Funktionsfähigkeit prüfen |
| 7.16 | Press Control Fault (Fehler in der Pressensteuerung) | PCMS-Status prüfen | PCMS-Zustandsfehler (PCMS-Zustandsstufe während des Pressenzyklus nicht wie erwartet)<br>• Verdrahtung des PCMS-Eingangs prüfen<br>• Platzierung des PCMS-Sensors und seine Funktionsfähigkeit prüfen |
| 7.17 | Press Control Fault (Fehler in der Pressensteuerung) | TOS-Status prüfen | TOS-Zustandsfehler (TOS-Zustandsstufe während des Pressenzyklus nicht wie erwartet)<br>• Verdrahtung des TOS-Eingangs prüfen<br>• Platzierung des TOS-Sensors und seine Funktionsfähigkeit prüfen |
| 7.18 | Press Control Fault (Fehler in der Pressensteuerung) | BOS-Status prüfen | BOS-Zustandsfehler (BOS-Zustandsstufe während des Pressenzyklus nicht wie erwartet)<br>• Verdrahtung des BOS-Eingangs prüfen<br>• Platzierung des BOS-Sensors und seine Funktionsfähigkeit prüfen |
| 10.xx | Interner Fehler | - | Interner Fehler: Banner Engineering kontaktieren (siehe Reparaturen und Garantie auf Seite 293) |

Überprüfen Sie für Fehlercodes 4.x das Fehlerprotokoll auf weitere Fehler, um festzustellen, in welchem spezifischen Modul der ursprüngliche Fehler aufgetreten ist.

| Fehlercode | Dargestellte Meldung | Zusätzliche Meldung | Lösungsschritte |
|---|---|---|---|
| 4.1 | Betriebsspannung zu niedrig | Die Spannungsversorgung überprüfen | Betriebsspannung länger als 6 ms unter der Mindestversorgungsspannung:<br>• Betriebsspannungs- und Stromwerte der Versorgungsspannungsquelle überprüfen<br>• Überprüfen, ob an den Ausgängen Überlast vorliegt, die die Stromversorgung veranlassen könnte, den Strom zu begrenzen |
| 4.2 | Interner Fehler | | Ein Konfigurationsparameter wurde beschädigt. Zur Behebung des Zustands:<br>• Die Konfiguration unter Verwendung einer Sicherungskopie von der Konfiguration ersetzen<br>• Die Konfiguration über die Software erneut erstellen und in den Sicherheitskontroller schreiben |
| 4.3 – 4.11 | Interner Fehler | - | Interner Fehler: Banner Engineering kontaktieren (siehe Reparaturen und Garantie auf Seite 293) |
| 4.12 | Konfigurations-Zeitabschaltung | Konfiguration überprüfen | Der Sicherheitskontroller blieb länger als eine Stunde ohne Tastendruck im Konfigurationsmodus. |
| 4.13 | Konfigurations-Zeitabschaltung | Konfiguration überprüfen | Der Sicherheitskontroller blieb länger als eine Stunde ohne Empfang von Befehlen von der Software im Konfigurationsmodus. |
| 4.14 | Konfiguration unbestätigt | Bestätigung einer Konfiguration | Konfiguration wurde nach der Bearbeitung nicht bestätigt:<br>• Konfiguration über die Software bestätigen |
| 4.15 – 4.19 | Interner Fehler | - | Interner Fehler: Banner Engineering kontaktieren (siehe Reparaturen und Garantie auf Seite 293) |
| 4.20 | Nicht zugewiesener Anschluss belegt | Anschluss xx überprüfen | Dieser Anschluss ist keinem Gerät in der vorliegenden Konfiguration zugeordnet und sollte nicht aktiv sein:<br>• Verdrahtung überprüfen |

| Fehlercode | Dargestellte Meldung | Zusätzliche Meldung | Lösungsschritte |
|---|---|---|---|
| 4.21 – 4.34 | Interner Fehler | - | Interner Fehler: Banner Engineering kontaktieren (siehe Reparaturen und Garantie auf Seite 293) |
| 4.35 | Übertemperatur | - | Ein interner Übertemperaturzustand ist aufgetreten. Überprüfen Sie, ob die Umgebungs- und Ausgangslastbedingungen den Spezifikationen für den Sicherheitskontroller entsprechen. |
| 4.36 – 4.39 | Interner Fehler | - | Interner Fehler: Banner Engineering kontaktieren (siehe Reparaturen und Garantie auf Seite 293) |
| 4.40–4.41 | Modul-Kommunikationsfehler | Modul-Stromzufuhr überprüfen | Ein Ausgangserweiterungsmodul hat den Kontakt zum Basiskontroller verloren. |
| 4.42 | Module stimmen nicht überein | - | Das erfasste Modul bzw. die erfassten Module stimmen nicht mit der Konfiguration des Sicherheitskontrollers überein. |
| 4.43 | Modul-Kommunikationsfehler | Modul-Stromzufuhr überprüfen | Ein Ausgangsmodul hat den Kontakt zum Basiskontroller verloren. |
| 4.44 – 4.45 | Interner Fehler | - | Interner Fehler: Banner Engineering kontaktieren (siehe Reparaturen und Garantie auf Seite 293) |
| 4.46 – 4.47 | Interner Fehler | - | Interner Fehler: Banner Engineering kontaktieren (siehe Reparaturen und Garantie auf Seite 293) |
| 4.48 | Nicht verwendeter Ausgang | Ausgangsverdrahtung überprüfen | An einer unbekannten Klemme wurde Spannung festgestellt. |
| 4.49 – 4.55 | Interner Fehler | - | Interner Fehler: Banner Engineering kontaktieren (siehe Reparaturen und Garantie auf Seite 293) |
| 4.56 | Anzeige-Kommunikationsfehler | - | Anzeige-Kommunikationsfehler:<br>• Schalten Sie den Sicherheitskontroller aus und wieder ein. Falls der Fehlercode weiter angezeigt wird, Banner Engineering kontaktieren (siehe Reparaturen und Garantie auf Seite 293). |
| 4.57 – 4.59 | Interner Fehler | - | Interner Fehler: Banner Engineering kontaktieren (siehe Reparaturen und Garantie auf Seite 293) |
| 4.60 | Ausgangsfehler | Überprüfen, ob Kurzschlüsse vorliegen | Ein Ausgangsanschluss hat einen Kurzschluss erkannt. Überprüfen Sie den Ausgangsfehler für nähere Informationen. |

## 15.4.2 SC10-2 Fehlercode-Tabelle

Die folgende Tabelle enthält den Sicherheitskontroller-Fehlercode, die angezeigte Nachricht, alle weiteren Nachrichten sowie die Schritte zur Behebung des Fehlers.

Der Sicherheitskontroller-Fehlercode setzt sich aus dem Fehlercode und dem erweiterten Fehlercode zusammen. Das Format des Fehlercodes ist `Fehlercode "Punkt" erweiterter Fehlercode` . Der Sicherheitskontroller-Fehlercode 2.1 wird beispielsweise vom Fehlercode `2` und dem erweiterten Fehlercode `1` angegeben. Der Indexwert der Fehlermeldung ist der Fehlercode und der erweiterte Fehlercode zusammen und umfasst eine führende Null mit dem erweiterten Fehlercode, falls erforderlich. Der Sicherheitskontroller-Fehlercode 2.1 wird beispielsweise vom Fehlermeldungsindex `201` angegeben. Mit dem Indexwert der Fehlermeldung kann der vollständige Fehlercode bequem nur anhand eines einzigen 16-Bit-Registerwerts abgerufen werden.

| Fehlercode | Fehlerbeschreibung | Lösungsschritte |
|---|---|---|
| 1.1 – 1.2 | Ausgangsfehler | Sicherheitskontroller austauschen |
| 1.3 – 1.8 | Interner Fehler | Interner Fehler: Banner Engineering kontaktieren (siehe Reparaturen und Garantie auf Seite 293) |
| 1.9 | Ausgangsfehler | Sicherheitskontroller austauschen |
| 1.10 | Ausgangsfehler | Fehler beim Sequenz-Zeitverhalten:<br>• Zur Löschung des Fehlers einen System-Reset durchführen |
| 2.1 | Gleichzeitigkeitsfehler | An einem zweikanaligen Eingang oder einem antivalenten Eingang mit beiden Eingängen im Ein-Zustand ging ein Eingang in den Aus-Zustand und wieder zurück in den Ein-Zustand.<br>An einem zweifach-antivalenten Eingang mit beiden Eingangspaaren im Ein-Zustand ging ein Eingangspaar in den Aus-Zustand und wieder zurück in den Ein-Zustand.<br>• Verdrahtung überprüfen<br>• Eingangssignale überprüfen<br>• Gegebenenfalls die Entprellzeiten anpassen<br>• Eingang schalten |

| Fehlercode | Fehlerbeschreibung | Lösungsschritte |
|---|---|---|
| 2.2 | Gleichzeitigkeitsfehler | An einem zweikanaligen Eingang oder einem antivalenten Eingang ging ein Eingang in den Ein-Zustand, aber der andere Eingang folgte nicht innerhalb von 3 Sekunden.<br>An einem zweifach-antivalenten Eingang ging ein Eingangspaar in den Ein-Zustand, aber das andere Eingangspaar folgte nicht innerhalb von 3 Sekunden.<br>• Verdrahtung überprüfen<br>• Zeitverhalten der Eingangssignale kontrollieren<br>• Eingang schalten |
| 2.3 oder 2.5 | Gleichzeitigkeitsfehler | An einem zweifach-antivalenten Eingang mit beiden Eingängen eines antivalenten Paares im Ein-Zustand ging ein Eingang dieses antivalenten Paares in den Aus-Zustand und wieder zurück in den Ein-Zustand.<br>• Verdrahtung überprüfen<br>• Eingangssignale überprüfen<br>• Überprüfen, ob die Stromversorgung Eingangssignale liefert<br>• Gegebenenfalls die Entprellzeiten anpassen<br>• Eingang schalten |
| 2.4 oder 2.6 | Gleichzeitigkeitsfehler | An einem zweifach-antivalenten Eingang ging ein Eingang von einem antivalenten Paar in den Ein-Zustand, aber der andere Eingang desselben antivalenten Paares folgte nicht innerhalb des Zeitlimits.<br>• Verdrahtung überprüfen<br>• Zeitverhalten der Eingangssignale kontrollieren<br>• Eingang schalten |
| 2.7 | Interner Fehler | Interner Fehler: Banner Engineering kontaktieren (siehe Reparaturen und Garantie auf Seite 293) |
| 2.8 – 2.9 | Eingangsfehler | Eingang im Ein-Zustand blockiert:<br>• Überprüfen, ob Kurzschlüsse zu anderen Eingängen oder zu einer anderen Spannungsquelle vorliegen<br>• Kompatibilität des Eingangsgeräts überprüfen |
| 2.10 | Eingangsfehler | • Überprüfen, ob zwischen den Eingängen ein Kurzschluss vorliegt |
| 2.11 – 2.12 | Eingangsfehler | • Überprüfen, ob Erdschluss vorliegt |
| 2.13 | Eingangsfehler | Eingang im Aus-Zustand blockiert<br>• Überprüfen, ob Erdschluss vorliegt |
| 2.14 | Eingangsfehler | Fehlende Testimpulse:<br>• Überprüfen, ob ein Kurzschluss zu anderen Eingängen oder zu einer anderen Spannungsquelle vorliegt |
| 2.15 | Leitungsunterbrechung | • Überprüfen, ob eine Leitungsunterbrechung vorliegt |
| 2.16 – 2.18 | Eingangsfehler | Fehlende Testimpulse:<br>• Überprüfen, ob ein Kurzschluss zu anderen Eingängen oder zu einer anderen Spannungsquelle vorliegt |
| 2.19 | Leitungsunterbrechung | • Überprüfen, ob eine Leitungsunterbrechung vorliegt |
| 2.20 | Eingangsfehler | Fehlende Testimpulse:<br>• Überprüfen, ob Erdschluss vorliegt |
| 2.21 | Leitungsunterbrechung | • Überprüfen, ob eine Leitungsunterbrechung vorliegt |
| 2.22 – 2.23 | Eingangsfehler | • Überprüfen, ob am Eingang ein instabiles Signal vorliegt |
| 2.24 | Eingang während Überbrückung aktiviert | Eine Zweihandsteuerung wurde aktiviert (eingeschaltet), während sie überbrückt wurde. |
| 2.25 | Eingangsfehler | Nachdem sich der zugehörige Sicherheitsausgang ausgeschaltet hat, wurde der AVM-Eingang nicht vor Ablauf seiner AVM-Überwachungszeit geschlossen:<br>• Die AVM ist möglicherweise getrennt. Verdrahtung zur AVM prüfen.<br>• Entweder die AVM ist getrennt, oder sie reagiert zu langsam auf das Ausschalten des Sicherheitsausgangs.<br>• Kabelanschlüsse zur AVM überprüfen<br>• Zeitgebereinstellung überprüfen und bei Bedarf erhöhen<br>• Banner Engineering kontaktieren |
| 2.26 | Eingangsfehler | Der AVM-Eingang war offen, sollte sich aber beim Einschaltbefehl an den verbundenen Sicherheitsausgang geschlossen haben:<br>• Die AVM ist möglicherweise getrennt. Verdrahtung zur AVM prüfen. |

| Fehlercode | Fehlerbeschreibung | Lösungsschritte |
|---|---|---|
| 3.1 | EDMxx-Fehler | EDM-Kontakt wurde geöffnet, bevor sich die Sicherheitsausgänge einschalteten:<br>• Überprüfen, ob Kontaktgeber oder Relais im Ein-Zustand verschweißt sind<br>• Auf Leitungsunterbrechungen überprüfen |
| 3.2 | EDMxx-Fehler | EDM-Kontakte wurden nach dem Abschalten der Sicherheitsausgänge nicht innerhalb von 250 ms geschlossen:<br>• Überprüfen, ob Kontaktgeber oder Relais zu langsam abfallen oder im Ein-Zustand verschweißt sind.<br>• Auf Leitungsunterbrechungen überprüfen |
| 3.4 | EDMxx-Fehler | Kontakte der beiden Rückführkreise (EDM-Kontaktpaar) länger als 250 ms in unterschiedlichem Zustand.<br>• Überprüfen, ob Kontaktgeber oder Relais zu langsam abfallen oder im Ein-Zustand verschweißt sind.<br>• Auf Leitungsunterbrechungen überprüfen |
| 3.5 | EDMxx-Fehler | • Überprüfen, ob am Eingang ein instabiles Signal vorliegt |
| 3.6 | EDMxx-Fehler | • Überprüfen, ob Erdschluss vorliegt |
| 3.7 | EDMxx-Fehler | • Überprüfen, ob zwischen den Eingängen ein Kurzschluss vorliegt |
| 3.8 | AVMxx-Fehler | Nachdem sich der zugehörige Sicherheitsausgang ausgeschaltet hat, wurde ein mit diesem Ausgang verbundener AVM-Eingang nicht vor Ablauf seiner AVM-Überwachungszeit geschlossen:<br>• Entweder die AVM ist getrennt, oder sie reagiert zu langsam auf das Ausschalten des Sicherheitsausgangs.<br>• Den AVM-Eingang überprüfen und dann zur Löschung des Fehlers einen System-Reset ausführen |
| 3.9 | Eingangsfehler | Der AVM-Eingang war offen, sollte sich aber beim Einschaltbefehl an den verbundenen Sicherheitsausgang geschlossen haben:<br>• Die AVM ist möglicherweise getrennt. Verdrahtung zur AVM prüfen. |
| 3.10 | Interner Fehler | Interner Fehler: Banner Engineering kontaktieren (siehe Reparaturen und Garantie auf Seite 293) |
| 4.1 | Betriebsspannung zu niedrig | Betriebsspannung länger als 6 ms unter der Mindestversorgungsspannung:<br>• Betriebsspannungs- und Stromwerte der Versorgungsspannungsquelle überprüfen<br>• Überprüfen, ob an den Ausgängen Überlast vorliegt, die die Stromversorgung veranlassen könnte, den Strom zu begrenzen |
| 4.2 | Interner Fehler | Ein Konfigurationsparameter wurde beschädigt. Zur Behebung des Zustands:<br>• Die Konfiguration unter Verwendung einer Sicherungskopie von der Konfiguration ersetzen<br>• Die Konfiguration über die Software erneut erstellen und in den Sicherheitskontroller schreiben |
| 4.3–4.12 | Interner Fehler | Interner Fehler: Banner Engineering kontaktieren (siehe Reparaturen und Garantie auf Seite 293). |
| 4.13 | Konfigurations-Zeitabschaltung | Der Sicherheitskontroller blieb länger als eine Stunde ohne Empfang von Befehlen von der Software im Konfigurationsmodus. |
| 4.14 | Konfiguration unbestätigt | Konfiguration wurde nach der Bearbeitung nicht bestätigt:<br>• Konfiguration über die Software bestätigen |
| 4.15–4.19 | Interner Fehler | Interner Fehler: Banner Engineering kontaktieren (siehe Reparaturen und Garantie auf Seite 293). |
| 4.20 | Nicht zugewiesener Anschluss belegt | Dieser Anschluss ist keinem Gerät in der vorliegenden Konfiguration zugeordnet und sollte nicht aktiv sein:<br>• Verdrahtung überprüfen |
| 4.21–4.34 | Interner Fehler | Interner Fehler: Banner Engineering kontaktieren (siehe Reparaturen und Garantie auf Seite 293). |
| 4.35 | Übertemperatur | Ein interner Übertemperaturzustand ist aufgetreten. Überprüfen Sie, ob die Umgebungs- und Ausgangslastbedingungen den Spezifikationen für den Sicherheitskontroller entsprechen. |
| 4.36–4.47 | Interner Fehler | Interner Fehler: Banner Engineering kontaktieren (siehe Reparaturen und Garantie auf Seite 293). |
| 4.48 | Nicht verwendeter Ausgang | An einer unbekannten Klemme wurde Spannung festgestellt. |

| Fehlercode | Fehlerbeschreibung | Lösungsschritte |
|---|---|---|
| 4.49–4.59 | Interner Fehler | Interner Fehler: Banner Engineering kontaktieren (siehe Reparaturen und Garantie auf Seite 293). |
| 4.60 | Ausgangsfehler | Ein Ausgangsanschluss hat einen Kurzschluss erkannt. Überprüfen Sie den Ausgangsfehler für nähere Informationen. |
| 5.1–5.3 | Interner Fehler | Interner Fehler: Banner Engineering kontaktieren (siehe Reparaturen und Garantie auf Seite 293) |
| 6.xx | Interner Fehler | Ungültige Konfigurationsdaten. Möglicher interner Fehler:<br>• Neue Konfiguration in den Sicherheitskontroller zu schreiben versuchen |
| 10.xx | Interner Fehler | Interner Fehler: Banner Engineering kontaktieren (siehe Reparaturen und Garantie auf Seite 293) |

# 16 Komponenten und Zubehörteile

## 16.1 Ersatzteile und Zubehör

| Typenbezeichnung | Beschreibung | Produkt |
|---|---|---|
| **SC-USB2** | USB-Kabel | XS/SC26-2, SC10-2 |
| **SC-XMP2** | Programmierwerkzeug für SC-XM2/3 | XS/SC26-2, SC10-2 |
| **DIN-SC** | DIN-Anschlussklemme | XS/SC26-2, SC10-2 |
| **SC-XM2** | Externes Speicherlaufwerk für den XS/SC26-2 | XS/SC26-2 |
| **SC-XM3** | Externes Speicherlaufwerk für den SC10-2 | XS/SC26-2, SC10-2 |
| **SC-TS2** | Schraubanschlussblöcke für Sicherheitskontroller | XS/SC26-2 |
| **SC-TS3** | Schraubanschlussblöcke für Erweiterungsmodul | XS/SC26-2 |
| **SC-TC2** | Federgehäuse-Anschlussblöcke für Kontroller | XS/SC26-2 |
| **SC-TC3** | Federgehäuse-Anschlussblöcke für Erweiterungsmodul | XS/SC26-2 |

## 16.2 Ethernet-Anschlussleitungen

| Geschirmte Cat5e-Anschlussleitungen | Geschirmte Cat5e-Crossover-Anschlussleitungen | Länge |
|---|---|---|
| **STP07** | **STPX07** | 2,1 m |
| **STP25** | **STPX25** | 7,62 m |
| **STP50** | **STPX50** | 15,2 m |
| **STP75** | **STPX75** | 22,9 m |

## 16.3 Interface-Module

Für weitere Informationen wird auf das Datenblatt mit der Ident.-Nr. 62822 und 208873 und EDM- und Endschaltgeräteanschluss auf Seite 67 verwiesen.

| Typenbezeichnung | Eingangsspannung | Eingänge | Sicherheitsausgänge | Hilfsausgänge | Ausgangsleistung (Nennwert) | EDM-Kontakte |
|---|---|---|---|---|---|---|
| **IM-T-9A** | 24 V DC | 2 (zweikanaliger Anschluss) | 3 Schließerkontakte | — | 6 A | 2 Öffnerkontakte |
| **IM-T-11A** | | | 2 Schließer | 1 Öffnerausgang | | |
| **SR-IM-9A** | | | 3 Schließerkontakte | — | Spezifikationen sind dem Datenblatt zu entnehmen | |
| **SR-IM-11A** | | | 2 Schließer | 1 Öffnerausgang | | |

### 16.3.1 Mechanisch verbundene Kontaktgeber

Mechanisch verbundene Kontaktgeber liefern zusätzliche 10-A- oder 18-A-Kapazitäten zur Führung der Signale für jedes Sicherheitssystem. Bei Verwendung sind für Kategorie 4 zwei Kontaktgeber pro Sicherheitsausgang erforderlich. Mit einem einzigen OSSD-Ausgang mit 2 Kontaktgebern lässt sich Kategorie 3 erfüllen. Die Öffnerkontakte müssen an einen externen Geräteüberwachungskreis (EDM-Kreis) angeschlossen werden.

Unter EDM- und Endschaltgeräteanschluss auf Seite 67 erhalten Sie weitere Informationen.

| Typenbezeichnung | Versorgungsspannung | Eingänge | Ausgänge | Ausgangsleistung (Nennwert) |
|---|---|---|---|---|
| **11-BG00-31-D-024** | 24 V DC | 2 (zweikanaliger Anschluss) | 3 Schließer und 1 Öffner | 10 A |
| **BF1801L-024** | | | | 18 A |

# 17 Kundendienst und Wartung

## 17.1 Reinigung

1. **Trennen Sie die Versorgungsspannung vom Sicherheitskontroller.**
2. Wischen Sie das Polycarbonatgehäuse und das Display (bei Ausführungen mit Display) mit einem weichen, mit einer Lösung aus einem schonenden Reinigungsmittel und warmem Wasser befeuchteten Tuch ab.

## 17.2 Reparaturen und Garantie

Wenden Sie sich zur Fehlerbehebung dieses Geräts an Banner Engineering. **Versuchen Sie nicht, Reparaturen an diesem Banner-Gerät vorzunehmen. Das Gerät enthält keine am Einsatzort auszuwechselnden Teile oder Komponenten.** Wenn ein Banner-Anwendungstechniker zu dem Schluss kommt, dass dieses Gerät, ein Teil oder eine Komponente davon defekt ist, erhalten Sie von dem Techniker Erläuterungen zu Banners RMA-Verfahren (Return Merchandise Authorization) für die Warenrückgabe.

**Wichtig:** Wenn Sie der Techniker anweist, das Gerät zurückzusenden, verpacken Sie es bitte sorgfältig. Transportschäden bei der Rücksendung werden von der Garantie nicht abgedeckt.

Damit Banner Engineering Probleme beheben kann, während der PC mit dem Sicherheitskontroller verbunden ist, rufen Sie in der Software die Hilfe auf und klicken Sie auf „Support-Informationen“. Klicken Sie auf **Kontrollerdiagnose speichern** (unter **Hilfe** > **Supportinformationen**), um eine Datei mit Statusinformationen zu generieren. Diese Informationen können für das Supportteam bei Banner von Nutzen sein. Senden Sie die Datei an Banner und beachten Sie dabei die Anweisungen auf dem Bildschirm.

## 17.3 Kontakt

Sitz der Zentrale von Banner Engineering Corp.:

9714 Tenth Avenue North, Minneapolis, MN 55441, USA Telefon: +1 888 373 6767

Weltweite Standorte und lokale Vertretungen finden Sie unter www.bannerengineering.com.

## 17.4 Beschränkte Garantie der Banner Engineering, Corp.

Die Banner Engineering Corp. gewährt auf ihre Produkte ein Jahr Garantie ab Versanddatum für Material- und Herstellungsfehler. Innerhalb dieser Garantiezeit wird die Banner Engineering Corp. alle Produkte aus der eigenen Herstellung, die zum Zeitpunkt der Rücksendung an den Hersteller innerhalb der Garantiedauer defekt sind, kostenlos reparieren oder austauschen. Diese Garantie gilt nicht für Schäden oder Verbindlichkeiten aufgrund von Missbrauch, unsachgemäßem Gebrauch oder unsachgemäßer Anwendung oder Installation des Banner-Produkts.

**DIESE BESCHRÄNKTE GARANTIE IST AUSSCHLIESSLICH UND ERSETZT SÄMTLICHE ANDEREN AUSDRÜCKLICHEN UND STILLSCHWEIGENDEN GARANTIEN (INSBESONDERE GARANTIEN ÜBER DIE MARKTTAUGLICHKEIT ODER DIE EIGNUNG FÜR EINEN BESTIMMTEN ZWECK), WOBEI NICHT MASSGEBLICH IST, OB DIESE IM ZUGE DES KAUFABSCHLUSSES, DER VERHANDLUNGEN ODER DES HANDELS AUSGESPROCHEN WURDEN.**

Diese Garantie ist ausschließlich und auf die Reparatur oder – im Ermessen von Banner Engineering Corp. – den Ersatz beschränkt. **IN KEINEM FALL HAFTET DIE BANNER ENGINEERING CORP. GEGENÜBER DEM KÄUFER ODER EINER ANDEREN NATÜRLICHEN ODER JURISTISCHEN PERSON FÜR ZUSATZKOSTEN, AUFWENDUNGEN, VERLUSTE, GEWINNEINBUSSEN ODER BEILÄUFIG ENTSTANDENE SCHÄDEN, FOLGESCHÄDEN ODER BESONDERE SCHÄDEN, DIE SICH AUS PRODUKTMÄNGELN ODER AUS DEM GEBRAUCH ODER DER UNFÄHIGKEIT ZUM GEBRAUCH DES PRODUKTS ERGEBEN. DABEI IST NICHT MASSGEBLICH, OB DIESE IM RAHMEN DES VERTRAGS, DER GARANTIE, DER GESETZE, DURCH ZUWIDERHANDLUNG, STRENGE HAFTUNG, FAHRLÄSSIGKEIT ODER AUF ANDERE WEISE ENTSTANDEN SIND.**

Die Banner Engineering Corp. behält sich das Recht vor, das Produktmodell zu verändern, zu modifizieren oder zu verbessern, und übernimmt dabei keinerlei Verpflichtungen oder Haftung bezüglich eines zuvor von der Banner Engineering Corp. gefertigten Produkts. Der Missbrauch, unsachgemäße Gebrauch oder die unsachgemäße Anwendung oder Installation dieses Produkts oder der Gebrauch dieses Produkts für Personenschutzanwendungen, wenn das Produkt als für besagte Zwecke nicht beabsichtigt gekennzeichnet ist, führt zum Verlust der Produktgarantie. Jegliche Modifizierungen dieses Produkts ohne vorherige ausdrückliche Genehmigung von Banner Engineering Corp führen zum Verlust der Produktgarantien. Alle in diesem Dokument veröffentlichten Spezifikationen können sich jederzeit ändern. Banner behält sich das Recht vor, die Produktspezifikationen jederzeit zu ändern oder die Dokumentation zu aktualisieren. Die Spezifikationen und Produktinformationen in englischer Sprache sind gegenüber den entsprechenden Angaben in einer anderen Sprache maßgeblich. Die neuesten Versionen aller Dokumentationen finden Sie unter: www.bannerengineering.com.

Informationen zu Patenten finden Sie unter www.bannerengineering.com/patents.

# 17.5 Banner Engineering Corp. Urheberrechtsvermerk zur Software

Diese Software ist urheberrechtlich und, durch das Betriebsgeheimnis und durch geistiges Eigentumsrecht geschützt. Sie erhalten nur das Recht auf Benutzung der Software zu den von Banner beschriebenen Zwecken. Banner behält sich alle anderen Rechte an dieser Software vor. Solange Sie eine autorisierte Kopie dieser Software direkt von Banner erhalten haben, gewährt Ihnen Banner ein beschränktes, nicht ausschließliches, nicht übertragbares Lizenzrecht zur Benutzung dieser Software.

Sie verpflichten sich, diese Software oder ihre Inhalte nicht in einer Weise zu benutzen, die gegen geltendes Recht, geltende Vorschriften oder die Benutzungsbedingungen gemäß diesem Vertrag verstößt, und dies auch Dritten nicht zu erlauben. Sie verpflichten sich, diese Software weder zu reproduzieren, zu modifizieren, zu kopieren, zu zerlegen, zu verkaufen, zu handeln oder weiterzuverkaufen noch für einen Dateifreigabe- oder Anwendungshostingdienst verfügbar zu machen.

**Gewährleistungsausschluss**. Sie benutzen diese Software vollständig auf Ihr eigenes Risiko, außer soweit in dieser Vereinbarung beschrieben. Diese Software wird ohne Mängelgewähr zur Verfügung gestellt. Im Rahmen des gesetzlich Zulässigen schließen Banner, die mit Banner verbunden Unternehmen und Personen und die Vertriebspartner von Banner sämtliche ausdrücklichen und stillschweigenden Gewährleistungen aus. Dies gilt einschließlich für Gewährleistungen über die Eignung der Software für einen bestimmten Zweck, Besitzrechte, die Marktgängigkeit, Datenverluste, die Nichtverletzung von geistigen Eigentumsrechten oder die Richtigkeit, Zuverlässigkeit, Qualität oder die Inhalte, die in den Diensten enthalten oder mit diesen verknüpft sind. Banner und die mit Banner verbundenen Unternehmen und Vertriebspartner geben keine Gewähr dafür, dass die Dienste sicher, frei von Fehlern, Viren, Unterbrechungen, Diebstahl oder Zerstörung sind. Falls die Ausschlüsse von stillschweigenden Gewährleistungen für Sie nicht gelten, sind alle stillschweigenden Gewährleistungen auf 60 Tage ab dem Tag der ersten Nutzung dieser Software beschränkt.

**Haftungsbeschränkung und Haftungsfreistellung**. Banner, die mit Banner verbundenen Unternehmen und Personen und die Vertriebspartner von Banner haften nicht für indirekte, besondere, beiläufig entstandene, Strafe einschließende oder Folgeschäden, Schäden bezüglich der Beschädigung, Sicherheit, des Verlusts oder Diebstahl von Daten, Viren, Spyware, entgangenen Geschäften, Umsätzen, Gewinnen oder Investitionen oder der Nutzung von Software oder Hardware, die die von Banner angegebenen Systemvoraussetzungen nicht erfüllt. Die vorgenannten Beschränkungen gelten auch, wenn Banner und den mit Banner verbundenen Unternehmen und Personen sowie den Vertriebspartnern von Banner die Möglichkeit solcher Schäden bekannt war. Diese Vereinbarung legt die gesamte Haftung von Banner und den mit Banner verbundenen Unternehmen und Personen dar und somit Ihr ausschließliches Rechtsmittel in Bezug auf die Nutzung der Software. Sie verpflichten sich, Banner, die mit Banner verbundenen Unternehmen und Personen sowie die Vertriebspartner von Banner von der Haftung freizustellen und zu entschädigen für sämtliche Ansprüche, Verbindlichkeiten und Aufwendungen, einschließlich angemessener Rechtsanwaltshonorare und -kosten, die sich aus Ihrer Nutzung der Dienste oder Ihrer Verletzung dieser Vereinbarung (zusammen als die "Ansprüche" bezeichnet) ergeben. Banner behält sich das Recht vor, nach alleinigem Ermessen und auf eigene Kosten von Banner die ausschließliche Verteidigung und Kontrolle von Ansprüchen zu übernehmen. Sie verpflichten sich, bei der Verteidigung gegen Ansprüche angemessen und auf Verlangen mit Banner zu kooperieren.

# 18 Normen und Vorschriften

*Es folgt eine Liste mit Normen zu diesem Banner-Gerät; diese dient zur Information für Anwender dieses Geräts. Die Angabe dieser Normen bedeutet nicht, dass das Gerät jede Norm erfüllt. Die erfüllten Normen sind unter den Spezifikationen in diesem Handbuch aufgeführt.*

## 18.1 Geltende US-Normen

ANSI B11.0: Safety of Machinery, General Requirements, and Risk Assessment (Sicherheit von Maschinen, Allgemeine Anforderungen und Risikobewertung)

ANSI B11.1: Mechanical Power Presses (Mechanische Pressen)

ANSI B11.2: Hydraulic Power Presses (Hydraulische Pressen)

ANSI B11.3: Power Press Brakes (Bremsen von mechanischen Pressen)

ANSI B11.4: Shears (Abtrenner)

ANSI B11.5: Iron Workers (Stahlbauarbeiter)

ANSI B11.6: Lathes (Drehmaschinen)

ANSI B11.7: Cold Headers and Cold Formers (Kaltanstaucher und Kaltumformer)

ANSI B11.8: Drilling, Milling, and Boring (Bohren, Mahlen und Fräsen)

ANSI B11.9: Grinding Machines (Schleifmaschinen)

ANSI B11.10: Metal Sawing Machines (Metallsägemaschinen)

ANSI B11.11: Gear Cutting Machines (Verzahnungsmaschinen)

ANSI B11.12: Roll Forming and Roll Bending Machines (Rollenformungs- und Rollenbiegemaschinen)

ANSI B11.13: Single- and Multiple-Spindle Automatic Bar and Chucking Machines (Automatische Stab- und Futtermaschinen mit einer oder mehreren Spindeln)

ANSI B11.14: Coil Slitting Machines (Spulenlängsschneidemaschinen)

ANSI B11.15: Pipe, Tube, and Shape Bending Machines (Rohr-, Schlauch- und Formbiegemaschinen)

ANSI B11.16: Metal Powder Compacting Presses (Metallpulver-Kompaktierungspressen)

ANSI B11.17: Horizontal Extrusion Presses (Horizontale Strangpressen)

ANSI B11.18: Machinery and Machine Systems for the Processing of Coiled Strip, Sheet, and Plate (Maschinen und Maschinenanlagen für die Verarbeitung von aufgerollten Streifen, Blättern und Platten)

ANSI B11.19: Performance Criteria for Safeguarding

ANSI B11.20: Manufacturing Systems (Fabrikationssysteme)

ANSI B11.21: Machine Tools Using Lasers (Maschinenwerkzeuge mit Lasern)

ANSI B11.22: Numerically Controlled Turning Machines (Digital gesteuerte Drehmaschinen)

ANSI B11.23: Machining Centers (Zentren für maschinelle Bearbeitung)

ANSI B11.24: Transfer Machines (Übertragungsmaschinen)

ANSI/RIA R15.06: Safety Requirements for Industrial Robots and Robot Systems (Sicherheitsanforderungen für Industrieroboter und Roboter-Systeme)

ANSI NFPA 79: Electrical Standard for Industrial Machinery (Elektrische Norm für Industriemaschinen)

ANSI/PMMI B155.1: Package Machinery and Packaging-Related Converting Machinery – Safety Requirements (Verpackungsmaschinen und verpackungsbezogene Verarbeitungsmaschinen – Sicherheitsanforderungen)

## 18.2 Geltende OSHA-Vorschriften

Die genannten OSHA-Dokumente stammen aus folgenden Quellen: Code of Federal Regulations, Title 29, Teile 1900 bis 1910

OSHA 29 CFR 1910.212: General Requirements for (Guarding of) All Machines (Allgemeine (Schutz-)Anforderungen für alle Maschinen)

OSHA 29 CFR 1910.147: The Control of Hazardous Energy (lockout/tagout) (Kontrolle gefährlicher Energie (Lockout/Tagout))

OSHA 29 CFR 1910.217: (Guarding of) Mechanical Power Presses ((Schutz von) mechanischen Pressen)

# 18.3 Geltende europäische und internationale Normen

EN ISO 12100: Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikoreduzierung

ISO 13857: Sicherheit von Maschinen – Sicherheitsabstände zur Verhinderung des Erreichens von Gefahrenzonen

ISO 13850 (EN 418): Not-Ausschaltgeräte, Funktionelle Aspekte – Gestaltungsleitsätze

ISO 13851: Zweihandsteuerungen – Funktionelle Aspekte; Gestaltungsleitsätze

IEC 62061: Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer Steuerungssysteme

EN ISO 13849-1: Sicherheitsbezogene Teile von Steuerungen

ISO 13855 (EN 999): Sicherheit von Maschinen – Anordnung von Schutzeinrichtungen im Hinblick auf Annäherungsgeschwindigkeiten von Körperteilen

ISO 14119 (EN 1088): Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen – Leitsätze für Gestaltung und Auswahl

EN 60204-1: Elektrische Ausrüstung von Maschinen – Teil 1: Allgemeine Anforderungen

IEC 61496: Berührungslos wirkende Schutzeinrichtungen

IEC 60529: Schutzarten durch Gehäuse

IEC 60947-1: Niederspannungsschaltgeräte – Allgemeine Festlegungen

IEC 60947-5-1: Niederspannungsschaltgeräte – Steuergeräte und Schaltelemente; Elektromechanische Steuergeräte

IEC 60947-5-5: Niederspannungsschaltgeräte – Elektrisches Not-Aus Schaltgerät mit mechanischer Verriegelungsfunktion

IEC 61508: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme

IEC 62046 Sicherheit von Maschinen – Anwendung von Schutzeinrichtungen zur Anwesenheitserkennung von Personen

ISO 16092-1: Werkzeugmaschinen-Sicherheit – Pressen – Teil 1: Allgemeine Sicherheitsanforderungen

ISO 16092-3: Werkzeugmaschinen-Sicherheit – Pressen – Teil 3: Sicherheitsanforderungen für hydraulische Pressen

ISO 16092-4: Werkzeugmaschinen – Sicherheit von Pressen – Teil 4: Pneumatische Pressen

ISO 4413: Fluidtechnik - Allgemeine Regeln und sicherheitstechnische Anforderungen an Hydraulikanlagen und deren Bauteile

ISO 4414: Fluidtechnik - Allgemeine Regeln und sicherheitstechnische Anforderungen an Pneumatikanlagen und deren Bauteile

# 19 Glossar

## A

**Automatischer Reset**

Die Einstellung zur Steuerung des Sicherheitseingangsgeräts, bei der der zugewiesene Sicherheitsausgang automatisch einschaltet, wenn alle seine ihm zugeordneten Eingänge im Ein-Zustand sind.

## C

**Zustandsänderung (COS)**

Zustandsänderung, d. h. die Änderung eines Eingangssignals, wenn es vom Ein- in den Aus- oder vom Aus- in den Ein-Zustand wechselt.

**Ausschaltentprellzeit**

Die erforderliche Zeit zur Überbrückung eines flackernden Eingangssignals oder von Eingangskontakt-Prellen, um störende Auslösungen des Kontrollers zu verhindern. Einstellbar von 6 ms bis 100 ms. Werksvoreinstellung ist 6 ms (50 ms für Muting-Sensoren).

**Komplementärkontakte**

Zwei Kontaktsätze, die sich jeweils im gegensätzlichen Zustand befinden.

**Simultan (auch "gleichzeitig" oder "Gleichzeitigkeit")**

Die Einstellung, bei der beide Kanäle gleichzeitig ausgeschaltet werden müssen, bevor sie wieder eingeschaltet werden. Ist diese Bedingung nicht erfüllt, so befindet sich der Eingang in einem Fehlerzustand.

## D

**Autorisierte Person**

Eine Person, die aufgrund einer angemessenen Schulung und Eignung schriftlich vom Arbeitgeber für die Durchführung einer spezifischen Prüfroutine ermächtigt und somit autorisiert worden ist.

**Diversitäre Redundanz**

Die Praxis der Verwendung von Komponenten, Schaltungen oder dem Betrieb verschiedener Konstruktionen, Architekturen oder Funktionen zur Erzielung von Redundanz und zur Reduzierung der Möglichkeit von Gleichtaktfehlern.

**Zweikanalig**

Die Verwendung redundanter Signalleitungen für jeden Sicherheitseingang bzw. Sicherheitsausgang.

## F

**Fehler**

Ein Gerätezustand, der durch die Unfähigkeit zur Ausführung einer bestimmten Funktion gekennzeichnet ist. Hierzu gehört jedoch nicht die Unfähigkeit während der vorbeugenden Wartung oder anderer geplanter Aktionen oder aufgrund mangelnder externer Ressourcen. Ein Fehler ergibt sich oft durch andere Fehler des Geräts selbst, kann jedoch auch ohne vorherigen Fehler auftreten.

## H

**Feste Schutzeinrichtung**

Gitter, Schranken oder andere mechanische Absperrungen, die am Rahmen der Maschine befestigt sind und den Eintritt von Personal in den Gefahrenbereich einer Maschine verhindern sollen, ohne die Sicht auf den Bedienort einzuschränken. Die maximale Größe der Öffnungen wird durch die jeweils zutreffende Norm bestimmt, zum Beispiel Tabelle O-10 der OSHA-Norm 29CFR1910.217. Feste Schutzeinrichtungen werden auch als „feste Schutzbarrieren“ bezeichnet.

## I

**ISD**

Das Kommunikationsprotokoll von In-Series Diagnostics (ISD) bietet Leistungs- und Statusinformationen von jedem Gerät in der Reihe an die SPS und/oder HMI. Benachrichtigungen werden beim Öffnen oder Schließen einer Tür, nicht übereinstimmenden oder falsch ausgerichteten Sensoren und Auslösern sowie einer Reihe weiterer Systemdiagnoseattribute gesendet.

## M

**Ansprechzeit der Maschine**

Die Zeit zwischen der Aktivierung einer Maschinenabschaltvorrichtung und der Herstellung eines sicheren Zustands durch das Anhalten der gefährlichen Maschinenbewegung.

**Manueller Reset**

Konfiguration zur Steuerung des Sicherheitseingangsgeräts, bei der der zugewiesene Sicherheitsausgang erst einschaltet, nachdem ein manueller Reset ausgeführt wurde, vorausgesetzt die anderen zugehörigen Eingänge sind im Ein-Zustand.

## O

**Ausschaltsignal**

Das Signal des Sicherheitsausgangs, das eintritt, wenn mindestens eines seiner zugehörigen Eingangsgerätesignale in den Aus-Zustand wechselt. In diesem Handbuch wird der Sicherheitsausgang als AUS oder im Aus-Zustand befindlich bezeichnet, wenn das Signal nominell 0 V DC beträgt.

**Einschaltsignal**

Das Signal des Sicherheitsausgangs, das eintritt, wenn alle seine zugehörigen Eingangsgerätesignale in den Ein-Zustand wechseln. In diesem Handbuch wird der Sicherheitsausgang als EIN oder im Ein-Zustand befindlich bezeichnet, wenn das Signal nominell 24 V DC beträgt.

**Einschaltentprellzeit**

Die erforderliche Zeit zur Überbrückung eines flackernden Eingangssignals oder von Eingangskontakt-Prellen, um einen unerwünschten Maschinenanlauf zu verhindern. Einstellbar von 10 ms bis 500 ms. Die Werksvoreinstellung beträgt 50 ms.

## P

**Hintertretungsgefahr**

Eine Hintertretungsgefahr ist mit Anwendungen verbunden, bei denen Personen eine Schutzeinrichtung passieren (wodurch ein Stoppbefehl ausgegeben wird, um die Gefahr zu beseitigen) und in das Schutzfeld eintreten können, zum Beispiel Bereichssicherungen. Folglich wird ihre Präsenz nicht mehr erfasst, und es besteht die Gefahr, dass die Maschine anläuft bzw. wiederanläuft, während sich die Person noch im Schutzfeld befindet.

**Schützende Kleinspannung (PELV)**

Schützende, besonders niedrige Spannungsversorgung, für geerdete Schaltkreise. Gemäß IEC 61140: „Ein PELV-System ist ein elektrisches System, dessen Spannung unter normalen Bedingungen und unter einzelnen Fehlern, ausgenommen Erdungsfehler in anderen Schaltkreisen, Kleinspannungen (25 V AC QMW oder 60 V DC welligkeitsfrei) nicht überschreiten darf.“

## Q

**Qualifizierte Person**

Eine Person, die durch ein anerkanntes Ausbildungs- oder Berufsabschlusszertifikat, bzw. durch umfangreiche Kenntnisse und die entsprechende Ausbildung oder Erfahrung mit Erfolg nachweisen kann, dass sie in der Lage ist, Probleme bezüglich des in Frage stehenden Gegenstands und bei der Arbeit mit diesem zu lösen.

## R

**Einschaltsignal**

Das vom Kontroller überwachte Eingangssignal, das – wenn es erfasst wird – bewirkt, dass einer oder mehrere Sicherheitsausgänge einschalten, wenn ihre anderen zugehörigen Eingangssignale auch im Ein-Zustand sind.

## S

**Schutzkleinspannung (SELV)**

Besonders niedrige separate bzw. Schutzspannungsversorgung, für geerdete Schaltkreise. Gemäß IEC 61140: „Ein SELV-System ist ein elektrisches System, dessen Spannung unter normalen Bedingungen und unter einzelnen Fehlern, einschließlich Erdschlüssen in anderen Stromkreisen, Kleinspannungen (25 V AC effektiv oder 60 V DC welligkeitsfrei) nicht überschreiten darf.“

**Gleichzeitig (auch "simultan" oder "Gleichzeitigkeit")**

Die Einstellung, bei der beide Kanäle gleichzeitig ausgeschaltet sein müssen UND sich im Abstand von höchstens 3 Sekunden voneinander wiedereinschalten dürfen. Sind beide Bedingungen nicht erfüllt, so befindet sich der Eingang in einem Fehlerzustand.

**Einkanalig**

Die Verwendung nur einer Signalleitung für jeden Sicherheitseingang bzw. Sicherheitsausgang.

**Test bei Anlauf**

Bei bestimmten Sicherheitsvorrichtungen, wie z. B. Sicherheits-Lichtvorhängen oder Absperrtoren, kann es von Vorteil sein, die Vorrichtung beim Anlauf mindestens ein Mal auf den einwandfreien Funktionsbetrieb zu testen.

**Stoppsignal**

Das vom Kontroller überwachte Eingangssignal, bei dessen Erfassung mindestens ein Sicherheitsausgang ausgeschaltet wird. In diesem Handbuch wird das Eingangsgerät oder das Gerätesignal als im Aus-Zustand befindlich bezeichnet.

**System-Reset**

Ein konfigurierbarer Reset eines oder mehrerer Sicherheitsausgänge, mit dem diese (bei Konfiguration für manuellen Anlauf oder nach einem Verriegelungszustand aufgrund einer Fehlererkennung) nach der Netzeinschaltung des Kontrollers wieder eingeschaltet werden.

# Index


(EDM) 67
(In-Series Diagnostics) 18
(ME) 140, 141

## A

Abbruchverzögerung 57, 256
Abkürzungen 95
Abmessungen 25
Aktuelle Informationen zum Kontroller abrufen 118
AND 103
Anschluss
  integriert 155
Anzeige
  Status 259–261
Anzeigen 261
ATO 14, 19, 264, 266
Ausführungen
  SC10-2 16
  XS/SC26-2 10
Ausgang
  Muting-Lampe 141
Ausgang weiterschalten 256
Ausgangsfunktion 75
Ausschaltverzögerung 255, 256
automatisch konfigurieren 110, 112–115
automatische Optimierung von Anschlüssen 14, 19, 264, 266
AVM 45

## B

Bedienfeld am Kontroller 155, 263
Beispielkonfiguration 85, 88, 90, 93
Benutzeroberfläche
  PC 95, 97, 99–105, 107, 108, 110, 112–118, 120, 123, 126, 127
Bestätigen einer Konfiguration 83, 84
Betrieb der Sicherheitseingangsgeräte 253
Betriebsbedingungen 20, 22
bidirektionales Muting 254
Bildschirmkontrast 155
Byte 158

## C

Common-Leiter 65
CSV-Datei 113, 114

## D

DAP 230
Datenmodell 230
Device Access Point
  , Siehe DAP
Diagnose
  Sicherheitskontroller speichern 293
drucken 116
Drucken der Konfiguration 116
DWORD 158

## E

Ein-Weg-Muting 254
Eingangsgeräte
  nicht sicherheitsrelevant 54–57
einstellbare Ventilüberwachung 45
Einstellung Bildschirmkontrast 155
Einstellungen
  Projekt 99
Ersatzteile
  SC10-2 292
  XS/SC26-2 292
Erweiterungsmodule
  XS/SC26-2 10
Ethernet 8
externe Geräteüberwachung 67

## F

Fehler 283, 288
Fehlercodes
  SC10-2 288
  XS/SC26-2 283
Fehlerdiagnose 155, 283, 288
FID 11, 17
Funktion
  SQS 51
Funktionsabschaltungen 13, 18
Funktionsblock
  Pressensteuerung 51
Funktionsblöcke 8, 105, 128–130, 132, 135, 140–144, 146, 148, 150, 151, 154
Fußpedal 53

## G

Garantie 293
Generic Station Description
  , Siehe GSD
Gruppenobjekte 115
GSD
  Installieren 241

## H

halbjährliche Überprüfung 251
Hex 158
Hochlaufkonfiguration 252

## I

Inbetriebnahmeprüfung 251–258
interne Logik 8
ISD 18, 46–50, 113, 114
ISD-gerätespezifische Daten 48–50, 181, 215, 227, 240
ISD-Systemstatus 47

## K

Kabelzugschalter 35
Kante, Sicherheit 40–43
Konfiguration
  Beispiel 85
  Modus 155
  Übersicht 155
Konfiguration speichern 83, 84
Konfigurationsmodus 155
Kontrollerdaten
  Ansicht 118
  anzeigen 118
  lesen 118
Kontrollerdaten anzeigen 118
Kontrollerdaten lesen 118
Kontrollerdatenansicht 118

## L

Latch-Reset 256
Latch-Reset-Block 132
LED 259–261
LED-Status 259–261
Livemodus 120, 263, 278
Logikblöcke 8, 102–104

## M

Matte, Sicherheit 40–43
Mindestabstand
  Sicherheitsmatte 42
  Zweihandsteuerung 39
Montage des Sicherheitskontrollers 27
Muting
  bidirektional 254
  Ein-Weg 254
  Überbrückung 255
  unidirektional 254
Muting-Aktivierung 140, 141
Muting-Block 135, 140–142
Muting-Lampenausgang 141
Muting-Sensor 43, 44, 52
Muting-Sensor der Pressensteuerung 52
Muting-Zeitlimit 141, 254
mutingabhängiges Override 254

## N

NAND 104
Netzwerkeinstellungen
  Modbus/TCP, Ethernet/IP, PCCC 112
  PROFINET 113
neue Konfiguration 82
neues Projekt 99
nicht sicherheitsrelevante Eingangsgeräte 54–57
NOR 104
NOT 104
Not-Aus-Schalter 34, 35
Nothalttaster 253

## O

Octet 158
One-Shot-Block 143
Optosensor 37, 253
OR 103
Override
  mutingabhängig 254

## P

Passwort 8, 117
Passwort-Manager 8, 117
Pressensteuerung 75, 88, 90
Pressensteuerungs-Funktionsblock 51
Pressensteuerungsblock 144, 146, 148, 150
PROFINET 230–233, 235–241, 243, 246

Programmierwerkzeug 8
Programmierwerkzeug für SC-XMP2 8
Projekt speichern 83, 84
Projekteinstellungen 99

## R

RCD 57
regelmäßige Überprüfung 251
Registerkarte
  Funktionsansicht 101–105
  Geräte 100
  Industrie-Ethernet 110, 112–115
  ISD 108
  Kontaktplan 107
  Livemodus 120
  Schaltplan 105
  Simulationsmodus 123, 126
Registerkarte „ISD“ 108
Registerkarte Funktionsansicht 101–105
Registerkarte Geräte 100
Registerkarte Industrie-Ethernet 110, 112–115
Registerkarte Konfigurationsübersicht 116
Registerkarte Kontaktplan 107
Registerkarte Schaltplan 105
Registerkarte Simulationsmodus 123, 126
Reinigung 293
Reparatur 293
RS Flip-Flop 104

## S

SC-USB2 7
SC-XM2 7, 8, 270, 271
SC-XM3 8, 270, 271, 275
Schalter
  Überbrückung 45
Schutzeinrichtung, verriegelt 36, 37
Schutzhalt 36, 253
Schutzhaltschaltungen 69
Schutztür, verriegelt 36, 37
Seilzugschalter 35, 253
sekundärer Ausgang 256
sequenzieller Stopp 51
Sicherheits-Relaisausgänge 18
Sicherheitsabstand
  Sicherheitsmatte 42
  Zweihandsteuerung 39
Sicherheitsausgang
  Ausschaltverzögerung 255, 256
Sicherheitsausgänge 12, 13
Sicherheitseingangsgerät 29–32
Sicherheitskante 40–43
Sicherheitskontroller-Daten anzeigen 118
Sicherheitskontrollerdiagnose speichern 293
Sicherheitsmatte 40–43, 253
Sicherheitsstopp 36
Sicherheitsstoppschaltungen 69
Sicherheitsstufen von Sicherheitsschaltungen 34
Simulationsmodus 123, 126
Software 27, 95, 97, 99–105, 107, 108, 110, 112–118, 120, 123, 126, 127
Sperre 264
Sperrzustand 263
Spezifikationen
  SC10-2 22
  XS/SC26-2 20
Sprache
  Auswahl 97
SQS 51
SR Flip-Flop 104
Standardeinstellungen 277
Status-Anzeige 260, 261
Statusanzeige 259
Statusausgang 73, 74, 81
Statusausgänge
  SC10-2 18
  XS/SC26-2 13
Statusausgänge, virtuell 76
Steuereingänge 256
Steuerungslogik 82
String 158
System-Reset 263
Systemstatus 155
Systemüberprüfung 251
Systemvoraussetzungen für den PC 25

## T

tab
  Konfigurationszusammenfassung 116
tägliche Überprüfung 251
Testimpuls 19, 264
THC
  , Siehe Zweihandsteuerung
Treiberinstallation
  Überprüfen 281
Typenbezeichnung 155

## U

Überbrückung 141, 255
Überbrückungsblock 128
Überbrückungsschalter 45
Überprüfen der Treiberinstallation 281
Überprüfung 251–258
UDINT 158
UINT 158
unidirektionales Muting 254
USB 7

## V

verriegelte Schutztür 36, 37
Verriegelungsvorrichtung 36, 37
Verzögerung
  Abbruch 256
Verzögerungsblock 129
virtuelle nicht sicherheitsrelevante Eingangsgeräte 57, 60
virtuelle Statusausgänge
  SC10-2 18
  XS/SC26-2 13
Virtueller manueller Reset 57

## W

weiterschalten 256
Werksvoreinstellungen 277
Word 158

## X

XM2
  , Siehe SC-XM2
XM3
  , Siehe SC-XM3
XML-Datei 113, 114
XOR 104

## Z

Zeitlimit
  Muting 254
Zeitlimit, Muting 141
Zubehör
  SC10-2 292
  XS/SC26-2 292
Zustimmtaster 36, 256
Zustimmtaster-Block 130
Zwei-Wege 254
Zwei-Wege-Muting 254
Zweihandsteuerung
  mit Muting 253
  ohne Muting 253
Zweihandsteuerungsblock 151, 154
Zyklusinitiierung 51