

# **Programmierbare Sicherheitsauswertung SCR P**

## **Bedienungsanleitung**

# Inhaltsverzeichnis

<b>1.Über dieses Dokument .....</b>	<b>4</b>
1.1 Wichtig - Unbedingt lesen! .....	4
1.2 Verwendung der Warnhinweise .....	4
1.3 EU-Konformitätserklärung .....	4
<b>2.Produktbeschreibung .....</b>	<b>6</b>
2.1 In diesem Handbuch verwendete Fachbegriffe .....	6
2.2 Software .....	6
2.3 USB-Anschlüsse .....	6
2.4 Ethernet-Verbindung .....	6
2.5 Interne Logik .....	7
2.6 Passwort-Manager .....	7
2.7 Programmier-Stick SCR P-FPS und USB-Programmieradapter SCR P-PA .....	7
<b>3.Überblick über das SCR P .....</b>	<b>8</b>
3.1 Ausführungen des SCR P .....	8
3.2 Funktionen und Anzeigen des SCR P .....	8
3.3 SCR P: FID .....	9
3.4 Ein- und Ausgangsanschlüsse .....	9
3.4.1 SCR P Sicherheitseingänge und nicht sicherheitsrelevante Eingänge .....	9
3.4.2 Sicherheits-Relaisausgänge am SCR P .....	9
3.4.3 Statusausgänge und virtuelle Statusausgänge am .....	10
3.5 Funktion des SCR P für die automatische Optimierung von Anschlüssen (ATO) bei externen Klemmenblöcken(ETB) .....	10
<b>4.Spezifikationen und Anforderungen .....</b>	<b>11</b>
4.1 Spezifikationen für das SCR P .....	11
4.2 Abmessungen .....	14
4.3 Systemvoraussetzungen für den PC .....	14
<b>5.Systeminstallation .....</b>	<b>15</b>
5.1 Installation der Software .....	15
5.2 Installation der Sicherheitsauswertung .....	15
5.2.1 Montageanleitung .....	15
<b>6.Überlegungen vor der Installation .....</b>	<b>16</b>
6.1 Geeignete Anwendung .....	16
6.2 Anwendungen des SCR P .....	16
6.3 Sichere Eingangsfunktionen .....	17
6.3.1 Widerstandsfähigkeit gegen Fehler und Sicherheits- schaltungsprinzipien nach ISO 13849-1 .....	18
6.3.2 Eigenschaften von Sicherheitseingängen .....	19
6.4 Optionen für Sicherheitseingangsgeräte .....	21
6.4.1 Sicherheitsstufen von Sicherheitsschaltungen .....	22
6.4.2 Zustimmtaster .....	22
6.4.3 Not-Halt-Schalter .....	22
6.4.4 Seilzugschalter .....	23
6.4.5 Schutzhalt (Sicherheitsstopp) .....	24
6.4.6 Verriegelte Schutteinrichtung bzw. Schutztür .....	24
6.4.7 Optosensor .....	25
6.4.8 Zweihandsteuerung .....	25
6.4.9 Schaltmatte .....	28
6.4.10 Muting-Sensor .....	31
6.4.11 Überbrückungsschalter .....	32
6.4.12 AVM-Funktion (Adjustable Valve Monitoring, einstellbare Ventilüberwachung) .....	33
6.4.13 DCD-Eingänge .....	35
6.5 Nicht sicherheitsrelevante Eingangsgeräte .....	36
6.5.1 Manueller Reset-Eingang .....	37
6.6 Virtuelle nicht sicherheitsrelevante Eingangsgeräte .....	39
6.6.1 Virtueller manueller Reset und Abbrechen einer Zeitverzögerung (RCD) .....	39
6.6.2 Virtuelle Ein-/Ausschaltung und Muting-Aktivierung .....	42
6.7 Sicherheitsausgänge .....	42
6.7.1 Sicherheits-Relaisausgänge .....	44
6.7.2 EDM- und Abschaltgeräteanschluss .....	45
6.8 Statusausgänge .....	50
6.8.1 Signallogik für Statusausgänge .....	50
6.8.2 Statusausgangsfunktion .....	51
6.9 Virtuelle Statusausgänge .....	52
<b>7.Erste Schritte .....</b>	<b>53</b>
7.1 Erstellen einer Konfiguration .....	53
7.2 Hinzufügen von Eingängen und Statusausgängen .....	53
7.2.1 Hinzufügen von Sicherheits- und nicht sicherheitsrelevanten Eingängen .....	53
7.2.2 Hinzufügen von Statusausgängen .....	57
7.3 Entwerfen der Steuerungslogik .....	58
7.4 Speichern und Bestätigen einer Konfiguration .....	58
7.4.1 Hinweise zum Bestätigen oder Schreiben einer Konfiguration in ein konfiguriertes SCR P .....	59
<b>8.Software .....</b>	<b>60</b>
8.1 Abkürzungen .....	60

8.2 Software-Übersicht .....	62
8.3 Projekteinstellungen .....	64
8.4 Registerkarte <b>Geräte</b> .....	65
8.5 Registerkarte <b>Funktionsansicht</b> .....	66
8.5.1 Logikblöcke .....	67
8.5.2 Funktionsblöcke .....	69
8.6 Registerkarte <b>Schaltplan</b> .....	88
8.7 Registerkarte <b>Kontaktplan</b> .....	89
8.8 Registerkarte <b>DCD</b> .....	90
8.9 Registerkarte <b>Industrial-Ethernet</b> .....	93
8.9.1 Netzwerkeinstellungen .....	94
8.9.2 Erstellung einer Datei mit SPS-Tags/-Labels .....	95
8.9.3 Ethernet/IP-Gruppenobjekte .....	97
8.9.4 Industrial-Ethernet: Beschreibung der Tabellenzeilen und -spalten .....	98
8.9.5 Tabellen mit unterstützten Fehlerprotokollen .....	99
8.10 Registerkarte Konfigurationsübersicht .....	103
8.11 Druckoptionen .....	104
8.12 Passwort-Manager .....	105
8.13 Anzeigen und Importieren von Daten .....	105
8.14 Livemodus .....	107
8.15 Simulationsmodus .....	110
8.15.1 Aktionszeitsteuerungsmodus .....	113
8.16 Referenzsignale .....	114
<b>9. Systemüberprüfung .....</b>	<b>115</b>
9.1 Zeitplan für vorgeschriebene Überprüfungen .....	115
9.2 Inbetriebnahmeprüfung .....	115
9.2.1 Überprüfung des Systembetriebs .....	116
9.2.2 Setup vor der Inbetriebnahme, Inbetriebnahme und regelmäßige Prüfroutinen .....	116
<b>10. Informationen zum Status und zum Betrieb .....</b>	<b>122</b>
10.1 Status der LED-Anzeigen am SCR P .....	122
10.2 Livemodus-Informationen: Software .....	123
10.3 Sperrzustände .....	124
10.4 Nach einem Sperrzustand .....	124
10.5 SCR P: Automatische Optimierung von Anschlüssen .....	125
10.6 Beispielkonfiguration für das SCR P ohne automatische Optimierung von Anschlüssen .....	126
10.7 SCR P unter Verwendung des SCR P-FPS .....	130
10.8 SCR P Sicherheitsauswertung auf die Werkseinstellungen zurücksetzen .....	131
10.9 Werkseinstellungen .....	131
<b>11. Fehlerbehebung .....</b>	<b>133</b>
11.1 Software: Fehlerbehebung .....	133
11.2 Software: Fehlercodes .....	134
11.3 Überprüfen der Treiberinstallation .....	135
11.4 Fehlersuche und -behebung .....	137
11.4.1 Fehlercode-Tabelle für SCR P .....	137
<b>12. Komponenten und Zubehörteile .....</b>	<b>141</b>
<b>13. Kundendienst und Wartung .....</b>	<b>142</b>
13.1 Reinigung .....	142
13.2 Reparaturen und Garantie .....	142
13.3 Kontakt .....	142
13.4 Haftungsausschluss .....	142
<b>14. Normen und Vorschriften .....</b>	<b>143</b>
14.1 Geltende europäische und internationale Normen .....	143
<b>15. Glossar .....</b>	<b>145</b>

# 1. Über dieses Dokument

## 1.1 Wichtig - Unbedingt lesen!

Es liegt in der Verantwortlichkeit des überwachenden Ingenieurs, des Maschinenbauers, des Maschinenbedieners und/oder des Wartungspersonals oder Wartungselektrikers, dieses Gerät in vollständiger Übereinstimmung mit allen geltenden Bestimmungen und Normen einzusetzen und zu warten. Das Gerät kann die geforderte Sicherheitsfunktion nur erfüllen, wenn es 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 des Gerätes bitte an die BERNSTEIN AG.

Weitere Informationen zu internationalen Instituten für die Normierung der Leistung von Sicherheitsanwendungen und Sicherheitseinrichtungen finden Sie unter [Normen und Vorschriften](#) auf Seite 143.



### WARNUNG: Pflichten des Anwenders





In der Verantwortung des Anwenders liegt es:

- Alle Anweisungen zu diesem Gerät sorgfältig durchzulesen, zu verstehen und zu beachten.
- Eine Risikobeurteilung durchzuführen, die die konkrete Sicherheitsanwendung berücksichtigt. Informationen zur normgerechten Methodik sind der ISO 12100 zu entnehmen.
- Zu ermitteln, welche Sicherheitseinrichtungen und -prinzipien 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, und/oder weitere geeignete Normen verwiesen.
- Zu prüfen, ob das komplette Sicherheitssystem (einschließlich Ein- und Ausgangsgeräte 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.

**Wenn diese Aufgaben nicht befolgt werden, kann möglicherweise eine Gefahrensituation entstehen, die zu schweren oder tödlichen Verletzungen führen kann.**

## 1.2 Verwendung der Warnhinweise

Die Sicherheitshinweise und Erklärungen in diesem Dokument sind durch Warnsymbole gekennzeichnet und müssen für die sichere Verwendung des Sicherheitsauswertung der BERNSTEIN AG 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
 <b>WICHTIG</b>	<b>Warnhinweise vom Typ „Warnung“</b> beziehen sich auf potenzielle Gefahrensituationen, die, wenn sie nicht verhindert werden, zu schweren Verletzungen bis einschließlich zum Tod führen können.	
 <b>VORSICHT</b>	<b>Warnhinweise vom Typ „Achtung“</b> beziehen sich auf potenzielle Gefahrensituationen, die, sofern sie nicht verhindert werden, zu leichten bis mäßige Verletzungen oder potenziellen Sachschäden führen können.	

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

## 1.3 EU-Konformitätserklärung



## EU-Konformitätserklärung / EU Declaration of Conformity / Déclaration UE de conformité

Diese Konformitätserklärung entspricht der europäischen Norm DIN EN ISO/IEC 17050-1: Konformitätsbewertung – Konformitätserklärung von Anbietern – Teil 1: Allgemeine Anforderungen. Die Grundlage der Kriterien sind internationale Dokumente, insbesondere ISO/IEC-Leitfaden 22, 1982, Informations on manufacturer's declaration of conformity with standards or other technical specifications. Die deutsche Sprachfassung ist die Originalkonformitätserklärung. Bei anderen Sprachen handelt es sich um die Übersetzung der Originalkonformitätserklärung.

This Declaration of Conformity is suitable to the European Standard EN ISO/IEC 17050-1: Conformity assessment – Supplier's declaration of conformity – Part 1: General requirements. The basis for the criteria has been found in international documentation, particularly in: ISO/IEC Guide 22, 1982, Informations on manufacturer's declaration of conformity with standards or other technical specifications. The original Declaration of Conformity is the German language version. Other languages are a translation of the original Declaration of Conformity.

Cette déclaration de conformité correspond au Norme Européenne EN ISO/IEC 17050-1 : Evaluation de la conformité – Déclaration de conformité du fournisseur – Partie 1 : Exigences générales. La base des directives sont des documents internationaux répondant à ISO/IEC-Guide 22, 1982, Informations on manufacturer's declaration of conformity with standards or other technical specifications. La version allemande est le langage d'origine de la déclaration de conformité. Les autres langues ne sont qu'une traduction de la déclaration de conformité en langue allemande.

Wir / We / Nous

**BERNSTEIN AG**

(Name des Anbieters) / (Supplier's name) / (Nom du fournisseur)

**Hans-Bernstein-Straße 1**

**D-32457 Porta Westfalica**

(Anschrift) / (Address) / (Adresse)

erklären in alleiniger Verantwortung, dass das (die) Produkt(e):  
declare under our sole responsibility that the product(s):  
déclarons sous notre seule responsabilité que le(s) produit(s):

**Programmierbare Sicherheitsauswertung / Programmable Safety Controller**  
**Typ / Type: SCR P...**

... (siehe Betriebs- und Montageanleitung / refer to Installation and Operating Instructions / voir Instructions de service et de montage)

(Bezeichnung, Typ oder Modell, Los-, Chargen- oder Serien-Nr., möglichst Herkunft und Stückzahl)  
(Name, type or model, batch or serial number, possibly source and number of items)  
(Nom, type ou modèle, n° de lot, d'échantillon ou de série, éventuellement les sources et le nombre d'exemplaires)

mit folgenden Europäischen Richtlinien übereinstimmt (übereinstimmen):  
is (are) in conformity with the following directives:  
est (sont) conforme(s) aux directives européennes :

**Maschinenrichtlinie / Machinery-Directive 2006/42/EC**

**EMV-Richtlinie / EMC-Directive 2014/30/EU**

**RoHSII Richtlinie / RoHSII Directive 2011/65/EU**

Dies wird nachgewiesen durch die Einhaltung folgender Norm(en):  
This is documented by the accordance with the following standard(s):  
Notre justification est l'observation de la (des) norme(s) suivante(s):

**IEC 62061-2:2015; EN ISO 13849-1:2015**

**IEC 61508 Parts 1-7:2010; IEC 61326-3-1:2017**

**IEC 61131-2:2017**

Benannte Stelle / Notified Body / Organisme Notifié

**NB 0035**

**TÜV Rheinland Industrieservice GmbH, Am Grauen Stein, 51105 Köln**

**EG-Baumusterprüfbescheinigung Reg.-No.: 01/205/5782.00/20**

Name und Anschrift Bevollmächtigter Dokumentation:

Name and address of authorized agent documentation:

Nom et adresse de la documentation autorisée :

**Herr Roland Mönnings D-32457 Porta Westfalica, Hans-Bernstein-Straße 1**

*W. Vogt*

i.V. Wolfgang Vogt

**Compliance Officer Product**

**Porta Westfalica, 09.07.2020**

(Ort und Datum der Ausstellung):

(place and date of issue):

(date et lieu d'établissement):

(Name, Funktion) (Unterschrift):

(name, function) (signature):

(nom, fonction) (signature):

## 2. Produktbeschreibung

Die Sicherheitssteuerung ist ein kritischer und unverzichtbarer Bestandteil eines jeden Sicherheitssystems. Das liegt daran, dass Sicherheitssteuerungen dafür sorgen, dass Ihre Sicherheitsfunktionen korrekt ausgeführt werden.

Eine programmierbare Sicherheitsauswertung ist oft eine ideale Lösung für die Sicherheitssteuerung, denn diese bietet mehr Funktionen als ein herkömmliches Sicherheitsrelais und ist kostengünstiger als eine Sicherheits-SPS.

Die Sicherheitsauswertung von BERNSTEIN ist eine benutzerfreundliche und einfach konfigurierbare Auswertung, entwickelt zur Überwachung von diversen sicherheits- und nicht sicherheitsrelevanten Eingangsfunktionen und zur Bereitstellung von sicheren Start- und Stoppfunktionen für Maschinen mit Gefährdungen. Die Sicherheitsauswertung ersetzt zahlreiche anwendungsbezogene Sicherheitsrelais-Module für Sicherheitseingangsgeräte wie Not-Halt-Schalter, Schutztürschalter mit Verriegelung, Sicherheits-Lichtvorhänge, Zweihandsteuerungen, Sicherheitsmatten und vielen weiteren Schutzeinrichtungen.

### 2.1 In diesem Handbuch verwendete Fachbegriffe

In diesem Handbuch werden die folgenden Fachbegriffe verwendet.

**Sicherheitsauswertung; Auswertung:** Eine abgekürzte Version, die sich auf die programmierbare Sicherheitsauswertung SCR P bezieht.

**Programmierbare Sicherheitsauswertung SCR P:** Der offizielle Name des SCR P.

### 2.2 Software

Die Software für die Sicherheitsauswertung von BERNSTEIN 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 die Sicherheitsauswertung
- Lesen der aktuellen Konfiguration aus der Sicherheitsauswertung
- Anzeigen von Echtzeitinformationen, z. B. zum Gerätestatus, Diagnosedaten
- Anzeigen von Fehlerinformationen

Die Software verwendet simple Schaltungs- und Logiksymbole, mit denen Sie intuitiv die geeigneten Eingangsfunktionen und deren Eigenschaften festlegen können. Nachdem die benötigte Konfiguration, inkl. Geräteeigenschaften und E/A-Steuerungsbeziehungen auf der Registerkarte **Funktionsansicht** erstellt wurde, erstellt das Programm automatisch die entsprechenden Schalt- und Kontaktpläne.

Nähere Informationen finden Sie unter [Software-Übersicht](#) auf Seite 62.

### 2.3 USB-Anschlüsse

Der Micro-USB-Port des SCR P dient zum Verbinden der Auswertung mit dem PC (über das USB-Kabel). Zudem kann hier der Programmier-Stick SCR P-FPS angeschlossen werden. Der Programmier-Stick dient zum Übertragen einer auf dem PC erstellten Konfigurationen auf das SCR P.



#### **VORSICHT: Mögliche unbeabsichtigte Masserückleitung**

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

Über das USB-Kabel können der Computer und die Sicherheitsauswertung Teil einer unbeabsichtigten Masserückleitung für andere verbundene Geräte werden. Durch große Ströme könnte der PC und/oder die Sicherheitsauswertung beschädigt werden. Dies sollte möglichst vermieden werden. BERNSTEIN empfiehlt deshalb, das USB-Kabel als einziges Kabel an den PC anzuschließen. Das Netzteil sollte nach Möglichkeit vom Laptop getrennt werden.

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

### 2.4 Ethernet-Verbindung

Die Sicherheitsauswertung kann über eine Ethernet-Verbindung mit einem Steuer- oder Überwachungsgerät (z.B. eine übergeordnete Maschinensteuerung) verbunden werden. Die Verbindung wird mit Hilfe eines Ethernet-Kabels hergestellt und kann auch über einen Netzwerkschalter erfolgen. Unterstützt werden Standard- und Crossover-Kabel. In Umgebungen mit starken Störeinflüssen ist eventuell ein geschirmtes Kabel erforderlich.

## 2.5 Interne Logik

Die interne Logik der Sicherheitsauswertung ist so ausgelegt, dass ein Sicherheitsausgang nur eingeschaltet werden kann, wenn alle Sicherheitseingangssignale und die selbstüberwachenden Signale der Sicherheitsauswertung im „Ein“-Zustand sind und melden, dass kein Fehlerzustand vorliegt.

Die Software für die Sicherheitsauswertung von BERNSTEIN verwendet sowohl Logik- als auch Sicherheitsfunktionsblöcke für die Konfiguration von allgemeinen und erweiterten 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)

Unter [Logikblöcke](#) auf Seite 67 erhalten Sie weitere Informationen.



Funktionsblöcke sind vorprogrammierte Blöcke mit integrierter Logik, die unterschiedliche Steuerungselemente 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

Unter [Funktionsblöcke](#) auf Seite 69 erhalten Sie weitere Informationen.

## 2.6 Passwort-Manager

Ein Passwort wird benötigt, um eine Konfiguration zu bestätigen, eine Konfiguration auf die Sicherheitsauswertung zu schreiben und um über die Software auf den Passwort-Manager zuzugreifen.


Unter [Passwort-Manager SCR P](#) auf Seite 105 erhalten Sie weitere Informationen.

## 2.7 Programmier-Stick SCR P-FPS und USB-Programmieradapter SCR P-PA

Der Programmier-Stick SCR P-FPS dient zum Speichern einer **bestätigten** Konfiguration.



**Wichtig:** Überprüfen Sie (über die Software oder anhand der Aufschrift auf dem weißen Etikett am Programmier-Stick), ob die auf den Sicherheitskontroller übertragene Konfiguration korrekt ist.

Klicken Sie auf , um auf die Optionen für den Programmieradapter zuzugreifen:

- **Lesen:** Liest die aktuelle Konfiguration vom Programmier-Stick und lädt diese in die Konfigurations-Software.
- **Schreiben:** Schreibt eine bestätigte Konfiguration von der Konfigurations-Software auf den Programmier-Stick.
- **Sperre:** Sperrt den Programmier-Stick und verhindert so, dass Konfigurationen auf den Stick geschrieben werden können (ein leeres Laufwerk kann nicht gesperrt werden).



**Anmerkung:** Sie können die Sperre für den Programmier-Stick nicht wieder aufheben, nachdem dieser gesperrt wurde. Ein erneutes Beschreiben des Sticks ist somit nicht möglich.

### 3. Überblick über das SCR P

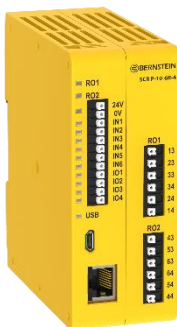


Abbildung 1: Sicherheitsauswertung SCR P

Die programmierbare Sicherheitsauswertung SCR P von BERNSTEIN ist eine benutzerfreundliche und kostengünstige Alternative zu Sicherheitsrelaismodulen. Er ersetzt die Funktionalität und den Leistungsumfang von zwei unabhängigen Sicherheitsrelaismodulen, ist konfigurierbar, einfach in der Handhabung und bietet erweiterte Diagnosefunktionen.

Für vollständige technische Informationen über dieses Produkt, einschließlich Installationsanweisungen, Anwendungsanforderungen und Richtlinien, EU-Konformitätserklärung, technische Spezifikationen und Zubehör, siehe [www.bernstein.eu](http://www.bernstein.eu) und Suche nach SCR P.

- Intuitive Programmierung auf Symbolbasis mit Konfiguration auf dem PC per Drag&Drop vereinfacht die Geräteeinrichtung und -verwaltung
- Zwei 6-A-Sicherheitsrelaisausgänge mit je drei Schließerkontakten
- Zehn Eingänge, von denen vier als nicht sicherheitsrelevante Ausgänge konfiguriert werden können
- Innovative Daisy Chain Diagnose (DCD)
- Automatische Optimierung von Anschlüssen (ATO) kann die Zahl der Eingänge von 10 auf 14 erweitern
- Bidirektionale Kommunikation über Industrial Ethernet basierten Protokollen
  - 256 virtuelle nicht sicherheitsrelevante Statusausgänge
  - 80 virtuelle nicht sicherheitsrelevante Eingänge (Reset, Ein/Aus, Abbruch Ausschaltverzögerung, Muting-Aktivierung)
  - Bereitstellen der DCD-Diagnosedaten
- Programmier-Stick vom Typ SCR P-FPS für schnelles Austauschen und schnelle Konfiguration ohne PC (siehe [SCR P unter Verwendung des SCR P-FPS](#) auf Seite 130)

#### 3.1 Ausführungen des SCR P

Typenbezeichnung	Beschreibung
SCR P-10-6R-4	Programmierbare Sicherheitsauswertung – 10 Eingänge (4 konfigurierbare Ausgänge), 2x 3 polige Sicherheitsrelais-Ausgänge, Daisy Chain Diagnose, Industrie-Ethernet basierte Protokolle

#### 3.2 Funktionen und Anzeigen des SCR P

Die Anschlusspunkte sind als Federzugklemmen ausgeführt.

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



**Wichtig:** Die Anschlussklemmen sind nur für ein Kabel bestimmt. Wenn mehr als ein Kabel an einem Anschluss angebracht wird, können sich Kabel lockern oder vollständig lösen und Kurzschlüsse verursachen.

Draht mit Aderendhülsen oder Aderendclips verwenden. Verzinnte Drähte werden nicht empfohlen.

Nach dem Einlegen des Drahtes in die Anschlussklemme festen Sitz durch Ziehen am Draht prüfen. Löst sich der Draht, sollte eine andere Verdrahtungslösung in Betracht gezogen werden.

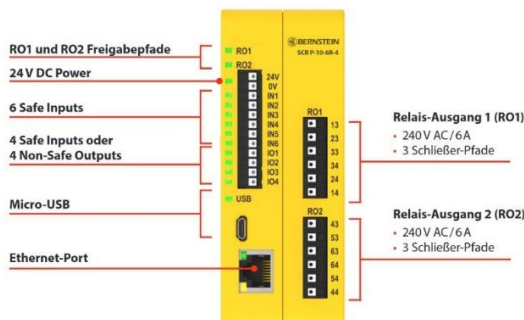


Abbildung 2: Funktionen und Anzeigen



### 3.3 SCR P: FID

Im Laufe der Zeit fügt BERNSTEIN einigen Geräten 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. Konfigurationen mit einer höheren FID werden von einer Sicherheitsauswertung mit niedrigerer FID nicht unterstützt.

Die Sicherheitsauswertungen des Typs SCR P sind FID2-Geräte.

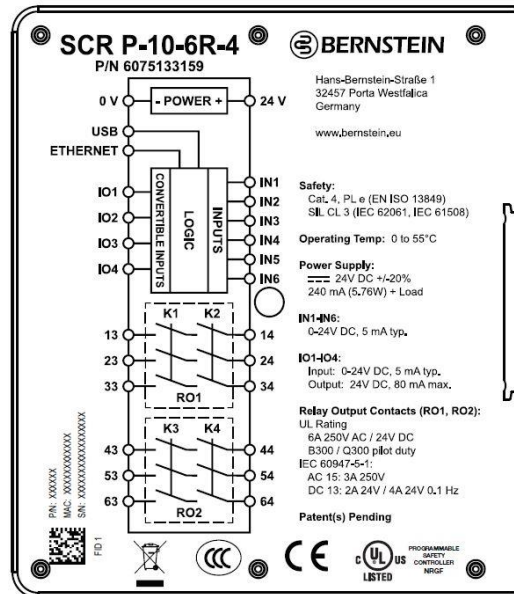


Abbildung 3: Beispiel für die Bedruckung des SCR P

### 3.4 Ein- und Ausgangsanschlüsse

#### 3.4.1 SCR P Sicherheitseingänge und nicht sicherheitsrelevante Eingänge

Das SCR P hat 10 Eingangsanschlüsse, die zur Überwachung von sicherheitsrelevanten oder nicht sicherheitsrelevanten Geräten verwendet werden können. Diese Geräte können Halbleiterausgänge oder kontaktbehaftete Ausgänge enthalten.

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

#### 3.4.2 Sicherheits-Relaisausgänge am SCR P

Das SCR P hat zwei unabhängige Relaisausgänge mit je drei Freigabepfaden.

Die Sicherheitsausgänge dienen der Ansteuerung von Leistungssteuerungselementen, bei denen es sich um die letzten Komponenten in der Kette der sicherheitsbezogenen Teile zur Steuerung der gefährlichen Maschinenbewegung handelt. Zu diesen Steuerelementen gehören Relais, Schütze, Magnetventile, Motorsteuerungen und andere Bauteile, teils mit zwangsgeführten (mechanisch verbundenen) Sicherheitskontakten, oder für die Überwachung eines Rückführkreises (EDM) erforderlichen elektrischen Signalen.

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

Die Sicherheitsauswertung kann für zwei verschiedene Arten von Stop-Kategorien 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 Statusausgänge und virtuelle Statusausgänge am SCR P

Über die Software können bis zu 256 virtuelle Statusausgänge konfiguriert werden, um Informationen über das Netzwerk zu kommunizieren. Über diese Ausgänge können nicht sicherheitsrelevante Statussignale an Geräte wie programmierbare Steuerungen (SPS) oder Mensch-Maschine-Schnittstellen (HMIs) gesendet werden. Weitere Informationen erhalten Sie unter [Virtuelle Statusausgänge](#) auf Seite 52.

Das SCR P hat vier konfigurierbare E/As (als **IOx** beschriftet), die als Statusausgänge für die Direktansteuerung von Anzeigelampen oder die feste Verdrahtung mit SPS-Eingängen verwendet werden können. Diese Ausgänge können zur Übertragung nicht sicherheitsrelevanter Signale verwendet werden.



**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 SCR P 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 SCR P-Modellen und ist standardmäßig aktiviert.

Die ATO-Funktion kann die 10 Anschlüsse auf dem SCR P 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 von der Sicherheitsauswertung erfordern. Diese Geräte werden über einen externen Klemmenblock (ETB) kombiniert, damit ein Ein-/Ausgangsanschluss frei wird. Jeder ETB ermöglicht es, dass bis zu drei unterschiedlichen Geräten das +24-V-Signal eines einzelnen Eingangs/Ausgangs gemeinsam nutzen.

ATO kann auf Wunsch durch Bearbeitung der Moduleigenschaften des SCR P 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.

## 4. Spezifikationen und Anforderungen

### 4.1 Spezifikationen für das SCR P

#### Stromversorgung

**Spannung:** 24 V dc  $\pm 20\%$  (SELV/PELV)

**Strom:**

Max. 240 mA, keine Last (Relais ein)

Max. 530 mA, volle Last (IO1 bis IO4 als Hilfsausgänge verwenden- det)

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

**Einschaltsschwellenwert für Eingang:**  $> 15\text{ V DC}$  (garantiert ein), max.  $30\text{ V DC}$

**Ausschaltsschwellenwert für Eingang:**  $< 5\text{ V DC}$  und  $< 2\text{ mA}$ , min.  $- 3\text{ V DC}$  mindestens

**Einschaltsschwellenwert für Eingang:**  $5\text{ mA}$  typisch bei  $24\text{ V DC}$ ,  $50\text{ mA}$  Kontaktreinigungs-Spitzenstrom bei  $24\text{ V DC}$

**Widerstand der Eingangsleitungen:** max.  $300\text{ Ohm}$  ( $150\text{ Ohm}$  pro Leitung)

**Eingangsanforderungen für eine 4-adrige Schaltmatte:**

- Max. Kapazität zwischen Platten:  $0,22\text{ }\mu\text{F}$ <sup>1</sup>
- Max. Kapazität zwischen unterer Platte und Erde:  $0,22\text{ }\mu\text{F}$ <sup>1</sup>
- Max. Widerstand zwischen den 2 Eingangsanschlüssen derselben Platte:  $20\text{ }\Omega$

#### Konfigurierbare E/A

**Stromversorgung:** max.  $80\text{ mA}$  (Überstromschutz)

**Testimpulse:**  $\sim 1\text{ ms}$  alle 25 bis 75 ms

#### Daisy Chain Diagnose

Bis zu zwei Diagnosekreise anschließbar (IN3+4 und IN5+6)

Bis zu 32 DCD-Teilnehmer pro Diagnosekreis

#### Funktion für die automatische Optimierung von Anschlüssen

Bis zu drei Geräte können mit vom Anwender bereitgestellten Klemmenblöcken verbunden werden

#### 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

<sup>1</sup> Wenn die Schaltmatten gemeinsam an einem konfigurierbaren E/A verwendet wird, ist dies die Gesamtkapazität aller Sicherheitsmatten, die verwendet werden darf.

#### 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):** 250 ms typisch, 400 ms max.

**Zeitablauffunktion für virtuellen Eingang (Muting-Aktivierung und Ein/Aus):** RPI + 200 ms typisch

**Zeitablauffunktion für virtuellen Eingang (manueller Reset und Abbruchverzögerung):** Details finden Sie unter [Virtuelle nicht sicherheitsrelevante Eingangsgeräte \(SCR P\)](#) auf Seite 39

#### Verzögerungstoleranz

±(0,02 % + 2 Scan-Zeiten)

#### Sicherheitsausgänge

3 Schließer pro Ausgangskanal (RO1 und RO2). Jeder Schließer ist eine Reihenschaltung von zwei 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 Ausgangsrelaiskontakt von 151 V bis 250 V AC/DC: Kategorie II (Kategorie III, wenn ein geeigneter Überspannungsschutz vorhanden ist, 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: 250 V AC, 3 A
DC 13	Schließer: 24 V DC, 2 A
DC 13 bei 0,1 Hz	Schließer: 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 % maximale relative Luftfeuchtigkeit bei +50 °C (nicht kondensierend)

**Betriebshöhe:** max. 2000 m (max. 6562 ft.)

#### Schutzart

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

#### Mechanische Belastung

**Stoßfestigkeit:** 15 g für 11 ms, Halbsinus, 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

50.00 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

#### Federzugklemmen



**Wichtig:** Die Klemmanschlüsse sind nur für ein Kabel bestimmt. Wenn mehr als ein Kabel an einem Anschluss angebracht wird, können sich Kabel lockern oder vollständig lösen und Kurzschlüsse verursachen.

Draht mit Aderendhülse oder Aderendclips verwenden. Verzinnete Drähte werden nicht empfohlen.

Nach dem Einlegen des Drahtes in den Anschluss am Draht ziehen und auf festen Sitz prüfen. Löst sich der Draht, sollte eine andere Verdrahtungslösung in Betracht gezogen werden.

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

**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 Warnung).

**Sicherheit**

Kategorie 4 PL e (EN ISO 13849-1)  
SIL CL 3 (IEC 62061, IEC 61508)

**Sicherheitsklasse**

–

PFH [1/h]: 5,01 × 10  
Gebrauchsdauer: 20 Jahre

**Produktnormen**

Im Abschnitt [Normen und Vorschriften](#) auf Seite 143 finden Sie eine Liste der geltenden internationalen- und US-Industrienormen.

**Zertifizierungen**

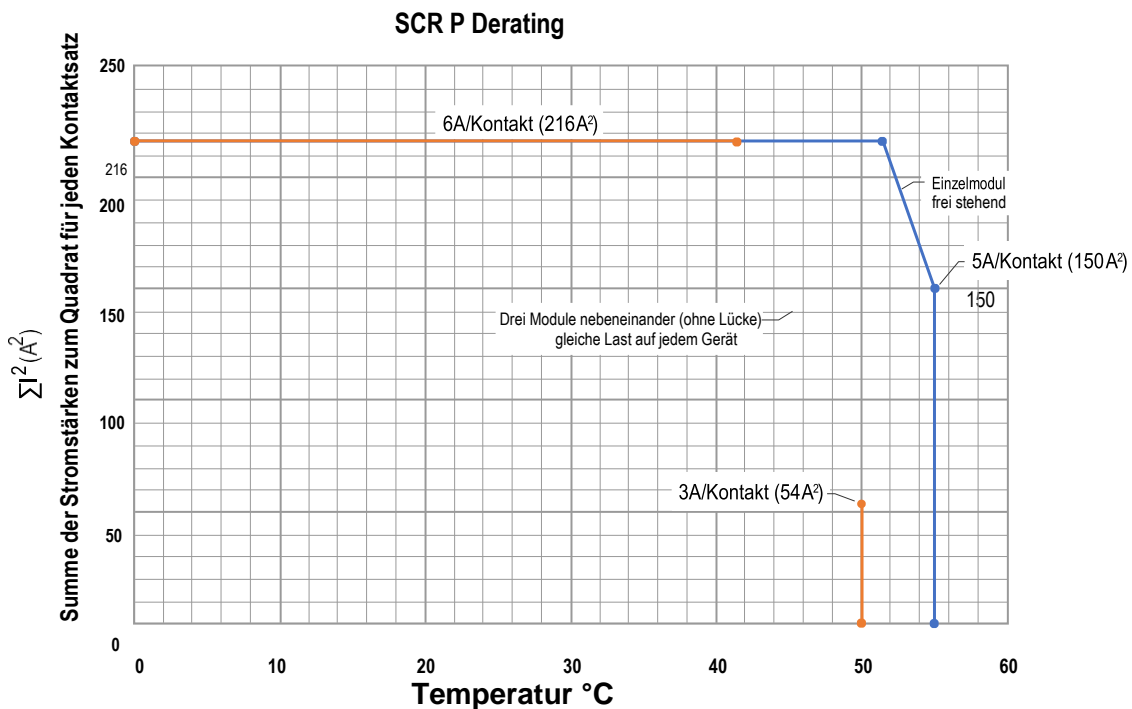
**Erforderlicher Überstromschutz**


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

Ein Überstromschutz ist erforderlich, dieser muss von der Anwendung des Endprodukts gemäß der angegebenen Tabelle bereitgestellt werden.

Der Überstromschutz kann durch externe Sicherungen oder über ein Netzteil der Klasse 2 mit Strombegrenzung bereitgestellt werden. Stromversorgungsdrähte < 0,20mm² (24 AWG) dürfen nicht verbunden werden. Weiteren Produktsupport erhalten Sie unter [www.bernstein.eu](http://www.bernstein.eu)

Stromversorgungsdrähte (mm² / AWG)	Erforderlicher Überstromschutz (A)
0,50 / 20	5,0
0,32 / 22	3,0
0,20 / 24	2,0
0,13 / 26	1,0
0,08 / 28	0,8
0,05 / 30	0,5


**Beispiel für die Berechnung des Temperaturabzugs**

Einzelnes Gerät, frei stehend	Drei Module
$\Sigma I^2 = I_1^2 + I_2^2 + I_3^2 + I_4^2 + I_5^2 + I_6^2$	$\Sigma I^2 = I_1^2 + I_2^2 + I_3^2 + I_4^2 + I_5^2 + I_6^2$ (alle sechs Module)
$I_1 = 4 \text{ A}$ (Schließer Ausgang RO1 Kanal 1)	$I_1 = 4 \text{ A}$
$I_2 = 4 \text{ A}$ (Schließer Ausgang RO1 Kanal 2)	$I_2 = 4 \text{ A}$
$I_3 = 4 \text{ A}$ (Schließer Ausgang RO1 Kanal 3)	$I_3 = 4 \text{ A}$
$I_4 = 4 \text{ A}$ (Schließer Ausgang RO2 Kanal 4)	$I_4 = 4 \text{ A}$
$I_5 = 4 \text{ A}$ (Schließer Ausgang RO2 Kanal 5)	$I_5 = 4 \text{ A}$
$I_6 = 4 \text{ A}$ (Schließer Ausgang RO2 Kanal 6)	$I_6 = 4 \text{ A}$

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

## 4.2 Abmessungen

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

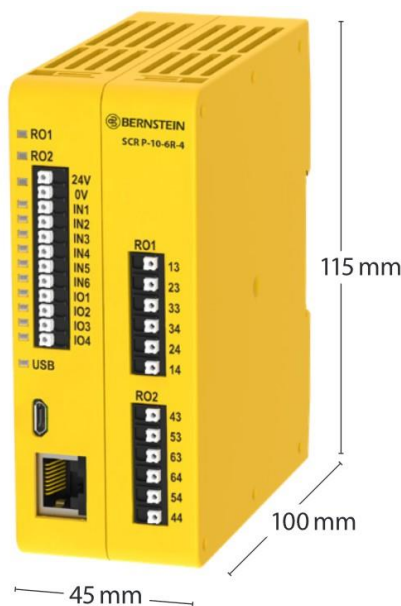


Abbildung 4: Abmessungen des SCR P

## 4.3 Systemvoraussetzungen für den PC



**Wichtig:** Für die Treiberinstallation der Sicherheitsauswertung sind Administratorrechte erforderlich (Treiber für die Kommunikation mit der Sicherheitsauswertung erforderlich).

<b>Betriebssystem:</b>	Microsoft Windows 7, Windows 8 (außer Windows RT) oder Windows 10 <sup>2</sup>
<b>Systemverschlüsselungstyp:</b>	32-Bit, 64-Bit
<b>Festplattenspeicher:</b>	80 MB (plus bis zu 280 MB für Microsoft .NET 4.0, falls es nicht bereits installiert ist)
<b>Arbeitsspeicher (RAM):</b>	Mindestens 512 MB, mindestens 1 GB empfohlen
<b>Prozessor:</b>	Mindestens 1 GHz, 2 GHz+ empfohlen
<b>Bildschirmauflösung:</b>	Farbbildschirm mit mindestens 1024 x 768 Pixeln, Farbbildschirm mit 1650 x 1050 Pixeln empfohlen
<b>Drittanbietersoftware:</b>	Microsoft .NET 4.0 (im Installationsprogramm enthalten), PDF-Anzeigeprogramm (z. B. Adobe Acrobat)
<b>USB-Port:</b>	USB 2.0 (kein Konfigurationsaufwand erforderlich)

<sup>2</sup> Microsoft und Windows sind eingetragene Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

# 5. Systeminstallation

## 5.1 Installation der Software



**Wichtig:** Für die Treiberinstallation der Sicherheitsauswertung sind Administratorrechte erforderlich (Treiber für die Kommunikation mit der Sicherheitsauswertung erforderlich).

1. Laden Sie die neueste Version der Software hier herunter: [www.bernstein.eu/downloads](http://www.bernstein.eu/downloads).
2. Navigieren Sie zu der heruntergeladenen Datei und öffnen Sie diese.
3. Klicken Sie auf **Weiter**, um den Installationsvorgang zu starten.
4. Bestätigen Sie den Zielspeicherort für die Software, die Verfügbarkeit für Benutzer und klicken Sie auf **Weiter**.
5. Klicken Sie auf **Weiter**, um die Installation zu starten.
6. Je nach den Systemeinstellungen wird möglicherweise ein Popup-Fenster eingeblendet, in dem Sie gefragt werden, ob Sie zulassen möchten, dass die Software von BERNSTEIN Änderungen an Ihrem Computer vornimmt. Klicken Sie auf **Ja**.
7. Klicken Sie auf **Schließen**, um das Installationsprogramm zu beenden.

Öffnen Sie **Konfigurationssoftware** vom **Arbeitsplatz aus** oder über das **Start-Menü**.

## 5.2 Installation der Sicherheitsauswertung

Um einen zuverlässigen Betrieb zu gewährleisten, dürfen die Betriebsdaten nicht überschritten werden. Das Schaltschrankgehäuse muss eine entsprechende Wärmeabstrahlung ermöglichen, so dass die Temperatur der Luft rund um die Sicherheitsauswertung die maximale Betriebstemperatur nicht überschreiten kann (siehe [Spezifikationen und Anforderungen](#) auf Seite 11).



**Wichtig:** Montieren Sie die Sicherheitsauswertung an einem geeigneten Ort, der keine starken Erschütterungen aufweist.



**VORSICHT:** Elektrostatische Entladungen (ESD) können Schäden an elektronischen Geräten verursachen. Um dies zu verhindern, sollten Sie die geeigneten Anwendungshinweisen 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.

### 5.2.1 Montageanleitung

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

Die Montageanleitung ist zu beachten, damit die Sicherheitsauswertung nicht beschädigt wird.

**Montage** der programmierbaren Sicherheitsauswertung SCR P:

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

**Entfernen** der programmierbaren Sicherheitsauswertung SCR P:

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.



## 6. Überlegungen vor der Installation

### 6.1 Geeignete Anwendung

Die korrekte Anwendung der Sicherheitsauswertung hängt von der Art der Maschine und den Schutzeinrichtungen ab, für die eine Schnittstelle mit der Sicherheitsauswertung hergestellt werden muss. **Falls Bedenken bestehen, ob die Maschine mit dieser Auswertung kompatibel ist, wenden Sie sich bitte an die BERNSTEIN AG.**



#### **WARNUNG: Keine eigenständige Schutzeinrichtung**

Dieses 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 Sicherheitsanwendungen. Jede dieser Anwendungen stellt ihre eigenen, spezifischen Anforderungen.

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



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

Die Sicherheitsauswertung der Bernstein AG ist ein Steuergerät, das normalerweise zusammen mit der Schutzeinrichtung einer Maschine verwendet wird. Wie gut es diese Funktion ausführen kann, hängt von der Eignung der Anwendung, der vorschriftsmäßigen mechanischen und elektrischen Installation der Sicherheitsauswertung 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 die Sicherheitsauswertung nicht den Schutz bieten, für den sie ausgelegt ist. Der Anwender ist für die Einhaltung aller lokalen und nationalen Gesetze, Vorschriften und Bestimmungen hinsichtlich der Installation und des Einsatzes dieses Gerätes bei jeder individuellen Anwendung verantwortlich. Sämtliche Sicherheitsanforderungen müssen erfüllt und alle in diesem Dokument enthaltenen technischen Installations- und Wartungsanweisungen müssen befolgt werden.

### 6.2 Anwendungen des SCR P

Die Sicherheitsauswertung SCR P ist ideal für alle Maschinen kleinerer bis mittlerer Größe, die normalerweise zwei unabhängige Sicherheitsrelaismodule verwenden würden.

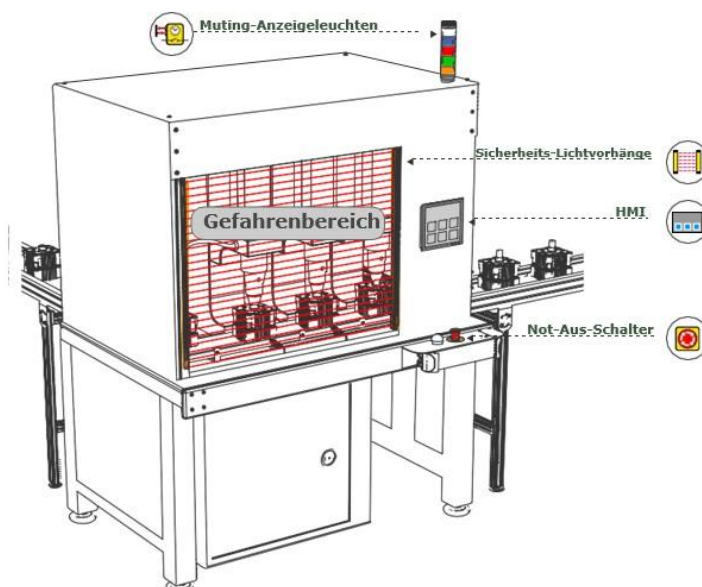


Abbildung 5: Anwendungsbeispiel 1 für das SCR P



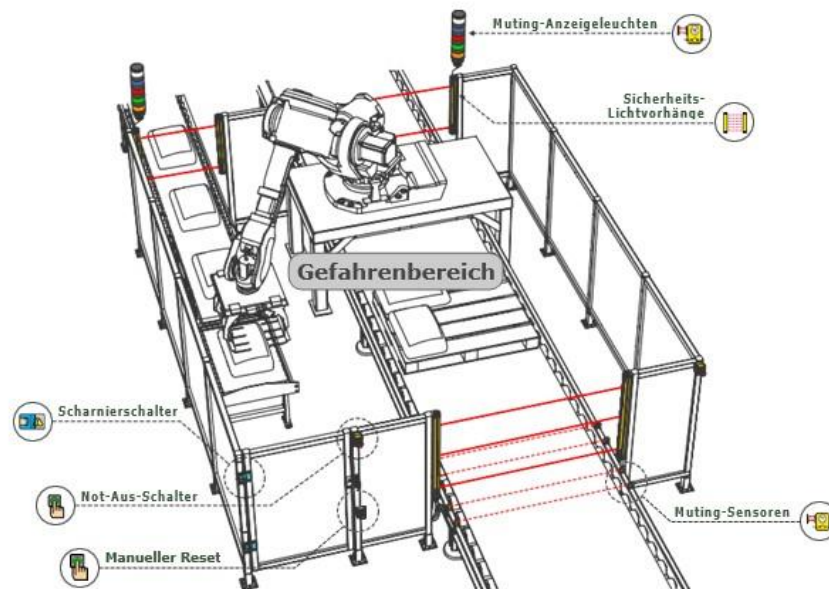


Abbildung 6: Anwendungsbeispiel 2 für das SCR P

## 6.3 Sichere Eingangsfunktionen

Die Sicherheitsauswertung überwacht den Status der Sicherheitsschaltgeräte, die mit ihr 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 können den sicheren Eingängen zugeordnet werden, um das Stoppsignal unter vordefinierten Umständen vorübergehend aufheben, damit der Sicherheitsausgang eingeschaltet bleibt. Hierzu gehören beispielsweise Muting und Umgehung.

Die Sicherheitsauswertung kann Eingangsfehler bei bestimmten Eingangsschaltungen erfassen, die anderenfalls zum Verlust der Sicherheitsfunktion führen würden. Wenn derartige Fehler erfasst werden, schaltet die Sicherheitsauswertung 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 Kabelkanälen oder Schutzrohren.
- Unterbringung aller Steuerungselemente (Sicherheitsauswertung, 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 mit Zugentlastungen verlegt werden. Zu starkes Anziehen einer klemmenden Zugentlastung kann Kurzschluss an diesem Punkt verursachen.
- Verwendung von Komponenten mit Zwangsöffnung gemäß der Beschreibung in IEC 60947-5-1, die nach IEC 14119 installiert werden.
- Regelmäßige Überprüfung der Funktion der Sicherheitsfunktion.
- Schulung der Bedienpersonen, des Wartungspersonals und anderer Personen, die mit der Bedienung der Maschine und deren Wartung zu tun haben, damit diese sämtlichen Störungen erfassen und unverzüglich beheben können.



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

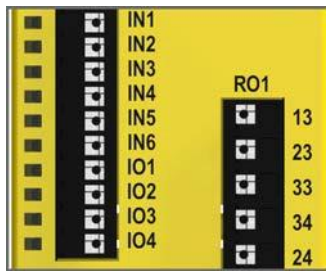


Abbildung 7: Position der Eingangs- und Ausgangsanschlüsse am SCR P



#### **WARNUNG: Eingangsgerät und Sicherheitsstufe**

Die Sicherheitsauswertung kann zahlreiche unterschiedliche sichere Eingangsgeräte überwachen. Der Benutzer muss eine Risikobeurteilung der Sicherheitsanwendung durchführen, um zu ermitteln, welche Sicherheitsstufe erreicht werden muss und wie die Eingangsgeräte folglich korrekt an die Sicherheitsauswertung 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.

## 6.3.1 Widerstandsfähigkeit gegen Fehler und Sicherheits-schaltungsprinzipien nach ISO 13849-1

Sicherheitsschaltungen umfassen die sicherheitsrelevanten Funktionen einer Maschine, die das Risiko mindern. Diese sicherheitsrelevanten Funktionen können einen Maschinenanlauf verhindern oder eine Maschinenbewegung stoppen. Das Versagen einer sicherheitsrelevanten Funktion oder ihrer zugehörigen Sicherheitsschaltung führt normalerweise zu einem erhöhten Risiko.

Die Widerstandsfähigkeit einer Sicherheitsschaltung gegen Fehler hängt von mehreren Faktoren ab, u. a. Fehlertoleranz, Risikominderung, zuverlässigen und bewährten Komponenten, bewährten Sicherheitsprinzipien sowie anderen Konstruktionsmerkmalen.

Je nach dem mit der Maschine oder ihrem Betrieb verbundenen Risiko muss ein geeignetes Maß an Widerstandsfähigkeit der Sicherheitsschaltungen gegen Fehler (Performance) in diese Konstruktion aufgenommen werden. Folgende Normen gehen näher auf Sicherheitsstufen ein: ISO 13849-1 Sicherheitsbezogene Teile von Steuerungen.

### **Sicherheitsstufen von Sicherheitsschaltungen**

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

Die Widerstandsfähigkeit gegen Fehler umfasst normalerweise redundante Steuerungs- und selbstüberwachende Schaltkreise und wird in etwa mit ISO 13849-1, Kategorie 3 oder 4 und/oder Performance Level „d“ oder „e“ gleichgesetzt (siehe ANSI B11.19).

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

Die Eingänge der Sicherheitsauswertung sind für Anwendungen bis einschließlich Kategorie 4 PL e (ISO 13849-1) und SIL 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 Sicherheitsschaltgeräte ab. Es liegt in der Verantwortung des Benutzers, eine Sicherheitseinstufung der Gesamtkonfiguration zu durchzuführen 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 Sicherheitsanwendungen 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: Zweikanalige kontaktbehaftete Eingänge mit nur 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 21).


**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.

## Fehlerrückmeldung

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 „Fehlerrückmeldung“ bezeichnet wird. Dies basiert auf der Annahme, 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 Fehlerrückmeldung ist ein Instrument, das Konstrukteure bei der Entwicklung der sicherheitsrelevanten Teile des Steuersystems und beim Risikobewertungsprozess verwenden können. Mit dem Fehlerrückmeldung kann der Konstrukteur die Möglichkeit mehrerer Fehler ausschließen und dies mit dem Risikobewertungsprozess begründen, um die gewünschte Fehlersicherheit gemäß den Anforderungen von ISO 13849-1/2 zu erzielen.

Die Anforderungen für die Fehlersicherheit von Sicherheitsschaltungen (Kategorie/Performance Level) gemäß ISO 13849-1 variieren in unterschiedlichen Anwendungen erheblich. Die BERNSTEIN AG 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.**

## 6.3.2 Eigenschaften von Sicherheitseingängen

Die Sicherheitsauswertung wird über die Software konfiguriert, um viele Arten von Sicherheitsschaltgeräten zu unterstützen. Siehe [Hinzufügen von Eingängen und Statusausgängen](#) auf Seite 53 für weitere Informationen über die Konfiguration der Eingänge.

### Reset-Logik: Manueller oder automatischer Reset

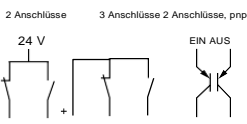
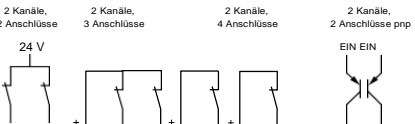
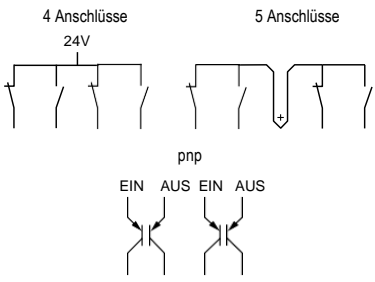
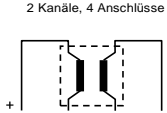
Ein manueller Reset kann für Sicherheitseingänge erforderlich sein, indem ein Latch-Reset-Block verwendet oder ein Sicherheitsausgang für einen Latch-Reset konfiguriert wird, damit die von ihnen gesteuerten Sicherheitsausgänge erst nach einer Quittierung wieder einschalten können. Dies wird gelegentlich als „Verriegelungsmodus“ bezeichnet, weil der Sicherheitsausgang im Aus-Zustand verriegelt wird, bis ein Reset ausgeführt wird. Wenn ein Sicherheitseingang für automatischen Reset-Modus 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

Die Sicherheitsauswertung muss wissen, welche Gerätesignalleitungen an welche Anschlussklemmen angeschlossen werden, damit sie die richtigen Signalüberwachungsmethoden, Ein - und Ausschaltfunktionen, Zeitfunktionen und Fehlerfunktionen anwenden kann. Die Anschlussklemmen werden während des Konfigurationsvorgangs automatisch zugewiesen und können über die Software manuell geändert werden.

## Arten von Signalzustandsänderungen

Zwei Arten von Zustandsänderungen können bei der Überwachung der Signale von zweikanaligen Sicherheitseingängen verwendet werden: simultan oder nicht simultan.

Eingangsschaltung	Zeitregelung für Zustandsänderung des Eingangssignals	
	Aus-Zustand: Sicherheitsausgang schaltet sich aus, wenn <sup>3</sup> :	Ein-Zustand: Sicherheitsausgang schaltet sich ein, wenn <sup>4</sup> :
<b>Zweikanalig A und B antivalent</b>  	Mindestens 1 Kanaleingang (A oder B) ist im Aus-Zustand.	<b>Simultan:</b> A und B sind beide im Aus-Zustand und schalten dann beide innerhalb von 3 s in den Ein-Zustand.  <b>Nicht simultan:</b> A und B sind beide im Aus-Zustand und schalten dann beide ohne begrenztes Zeitfenster in den Ein-Zustand.
<b>Zweikanalig A und B</b>  		
<b>Zweikanalig A und B 2x antivalent</b>  	Mindestens 1 Kanal (A oder B) eines Kontaktpaars im Aus-Zustand.	<b>Simultan:</b> A und B sind im Aus-Zustand, dann schalten beide Kontaktpaare jeweils 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.  <b>Nicht simultan:</b> A und B sind gleichzeitig im Aus-Zustand, dann schalten beide Kontaktpaare jeweils innerhalb von 3 Sekunden in den Ein-Zustand. Kanal A und Kanal B schalten ohne begrenztes Zeitfenster in den Ein-Zustand.
<b>4-adrige Sicherheitsmatte</b>  	Eine der folgenden Bedingungen ist erfüllt: <ul style="list-style-type: none"> <li>Eingangskanäle untereinander kurzgeschlossen (Normalbetrieb)</li> <li>Mindestens ein Kabel ist gelöst</li> <li>Einer der offenen Kanäle wird als geschlossen erfasst</li> <li>Einer der geschlossenen Kanäle wird als offen erfasst</li> </ul>	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, mechanischen Schocks oder andere Störungen zu längeren Signalübergangszeiten führen, eventuell erhöht werden. Wenn die Entprellzeit unter diesen rauen Bedingungen zu kurz eingestellt ist, kann das System einen Fehler erkennen und in einen Sperrzustand eintreten. Die Standardeinstellung ist 6 ms.

<sup>3</sup> Sicherheitsausgänge schalten sich aus, wenn einer der steuernden Eingänge im Aus-Zustand ist.

<sup>4</sup> 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, mechanischen Schocks oder andere Störungen zu längeren Signalübergangszeiten führen, eventuell erhöht werden. Wenn die Entprellzeit unter diesen rauen Bedingungen zu kurz eingestellt ist, kann das System einen Fehler erkennen und in einen Sperrzustand eintreten. Die Standardeinstellung ist 50 ms.

## 6.4 Optionen für Sicherheitseingangsgeräte

Allgemeine Schaltungssymbole		Schaltungen im Ein-Zustand abgebildet							Schaltungen im Stopp-Zustand abgebildet	
		ES	GS	OS	RP	PS	SM	DCD	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 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 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 An- tivalenter 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 An- tivalenter PNP-Ausgang			Kat. 4						Typ IIIc Kat. 4	Kat. 4
Sicherheitsmatte mit 4 Anschlüssen							Kat. 3			

Abbildung 8: Eingangsschaltungen – Kategorien (Anleitung)



**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.**

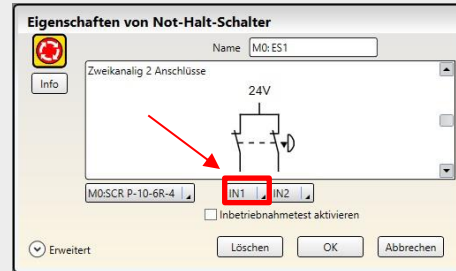
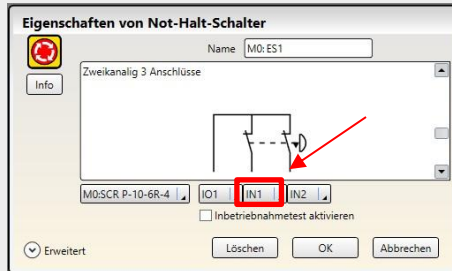


**WARNUNG:** Diese Tabelle enthält eine Liste der höchstmöglichen Sicherheitskategorien für gängige sicherheitsrelevante Eingangsgeräteschaltungen. Sind die in den nachfolgenden Anmerkungen angegebenen zusätzlichen Anforderungen aufgrund von Beschränkungen der Sicherheitsvorrichtung oder der Installation 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 Stromkreisen und zwischen Kanälen, wenn sich der Eingang seit mindestens 2 Sekunden im Aus-Zustand befindet.



## 6.4.1 Sicherheitsstufen von Sicherheitsschaltungen

Die Anforderungen an die Sicherheitsstufe bzw. das Performance Level gemäß ISO 13849-1 bei der Anwendung von Verriegelungseinrichtungen variieren stark. Während die BERNSTEIN AG 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 Sicherheitsstufe muss das Risiko der bei der Risikobeurteilung ermittelten Gefahren der Maschine ausreichend mindern.

## 6.4.2 Zustimmtaster



Ein Zustimmtaster ist ein manuell bedientes Steuergerät, das bei dauernder Betätigung zusammen mit einem Starttaster, die Initiierung eines Maschinenzyklus zulässt. Normen, die Gestaltung und Anwendung von Zustimmtastern abdecken, umfassen: 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 der eine Gefahrensituation eintreten kann. Der Zustimmtaster ermöglicht es einem gefährlichen Maschinenteil zu laufen, darf es aber nicht starten. Ein Zustimmtaster kann einen oder mehrere Sicherheitsausgänge steuern. Wenn das Aktivierungssignal vom Aus-Zustand in den Ein-Zustand schaltet, wechselt die Sicherheitsauswertung in den Freigabe-Modus. Zum Start einer gefährlichen Maschinenbewegung ist ein separates Maschinenbefehlssignal von einer anderen Vorrichtung erforderlich. **Der Zustimmtaster muss die letztendliche Möglichkeit zum Abschalten oder Stoppen der gefährlichen Maschinenbewegung haben.**

## 6.4.3 Not-Halt-Schalter



Die Sicherheitseingänge der Sicherheitsauswertung können zur Überwachung von Not-Halt-Schaltern verwendet werden.



### WARNUNG:

- **Not-Halt-Geräte weder muten noch überbrücken**
- Bei Muting oder Überbrücken der Sicherheitsausgänge wird die Not-Halt-Funktion unwirksam.
- Gemäß ANSI B11.19, ANSI NFPA79 und IEC/EN 60204-1 muss die Not-Halt-Funktion ständig aktiv bleiben.



**WARNUNG:** Die Not-Halt-Konfiguration der Sicherheitsauswertung verhindert ein Muten oder Überbrücken der Not-Halt-Schaltereingänge. Der Anwender muss jedoch immer noch dafür sorgen, dass der Not-Halt-Schalter jederzeit aktiv bleibt.



### WARNUNG: Reset-Funktion erforderlich

Internationale Normen schreiben vor, dass nach der Beseitigung der Ursache für einen Stopp-Zustand (z. B. Auslösen einer Not-Halt-Taste, Schließen einer verriegelten Schutzeinrichtung usw.) eine Reset-Routine durchgeführt wird. **Wird ein Neuanlauf der Maschine ohne Betätigung des normalen Startbefehls bzw. der normalen Startvorrichtung zugelassen, so kann ein unsicherer Zustand entstehen. Die Folge könnten schwere Verletzungen oder Tod sein.**

Zusätzlich zu den in diesem Abschnitt aufgeführten Anforderungen müssen Konstruktion und Installation der Not-Halt-Vorrichtung ANSI NFPA 79 oder ISO 13850 entsprechen. Die Stoppfunktion muss entweder ein Funktionsstopp der Kategorie 0 oder eine Funktion der Kategorie 1 sein (siehe ANSI NFPA79).

## Anforderungen für Not-Halt-Schalter

Not-Halt-Schalter müssen einen oder zwei Sicherheitskontakte haben, die geschlossen sind, wenn der Schalter in betriebsbereiter Stellung ist. Sobald er aktiviert ist, muss der Not-Halt-Schalter alle seine sicherheitsrelevanten Kontakte öffnen, und es muss eine bewusst ausgeführte Handlung notwendig sein (Drehen, Ziehen oder Entriegeln), um den Schalter in die betriebsbereite Stellung mit geschlossenen Kontakten zurückzubringen. Der Schalter muss entsprechend IEC 60947-5-1 Zwangsöffnung haben. Eine mechanische Kraft, die auf so einen Schalter ausgeübt wird, wird direkt auf die Kontakte übertragen und zwingt diese zur Öffnung. Dadurch wird sichergestellt, dass die Schalterkontakte jedes Mal öffnen, wenn der Schalter aktiviert wird.

In den Normen ANSI NFPA 79, ANSI B11.19, IEC/EN 60204-1 und ISO 13850 werden zusätzliche Anforderungen an Not-Halt-Schalter spezifiziert, u. a.:

- Not-Halt-Schalter müssen an jedem Bedienstand und anderen Bedientafeln angebracht sein, wo eine Notabschaltung benötigt wird.
- Aus- und Not-Halt-Schalter müssen von jedem Bedienstand und jeder Bedientafel aus, an denen sie angebracht sind, jederzeit betätigt werden können. **Not-Halt-Schalter dürfen nicht gemutet oder überbrückt werden.**
- Auslösevorrichtungen von Not-Halt-Schaltern müssen rot auf gelbem Hintergrund sein. Durch Druck oder Schlag ausgelöste Not-Halt-Schalter müssen als Pilz- oder Grobhandtaster ausgeführt sein
- Der Not-Halt-Schalter muss nach Betätigung in der Aus-Stellung verbleiben.



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

## 6.4.4 Seilzugschalter



Für Seilzugschalter mit Not-Halt Funktion (Sicherheitsseilzugschalter) werden Stahldrahtseile verwendet. Diese Schalter ermöglichen Not-Halt-Betätigungen über eine Distanz wie z. B. entlang eines Förderbands.

Für Sicherheitsseilzugschalter gelten viele derselben Anforderungen wie für Not-Halt-Drucktaster, wie zum Beispiel der direkte (zwangsgeführte) Betrieb entsprechend der Beschreibung in IEC 60947-5-1. Siehe [Not-Halt-Schalter](#) auf Seite 22 für weitere Informationen.

Sicherheitsseilzugschalter müssen die Fähigkeit besitzen, nicht nur auf einen Seilzug anzusprechen, sondern auch auf einen Durchhang oder Riss des Seils zu reagieren. Sicherheitsseilzugschalter müssen außerdem über eine Verriegelungsfunktion verfügen, die nach der Betätigung einen manuellen Reset erfordert.

### Richtlinien für die Installation von Sicherheitsseilzugschaltern

In den Normen ANSI NFPA 79, ANSI B11.19, IEC/EN 60204-1 und ISO 13850 werden die Anforderungen an die Installation von Sicherheitsseilzugschaltern spezifiziert, u. a.:

- Sicherheitsseilzugschalter müssen dort installiert werden, wo die Not-Halt Funktion benötigt wird.
- Sicherheitsseilzugschalter müssen dauerhaft betriebsbereit, leicht sichtbar und gut zugänglich sein. Muting oder Überbrückung nicht zulässig.
- Sicherheitsseilzugschalter müssen das Seil gleichmäßig spannen.
- Seile und Stellteile müssen die Farbe Rot aufweisen.
- Der Sicherheitsseilzugschalter muss in der Lage 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 zwangsöffnend ausgelegt sein.
  - Er muss einen Durchhang oder Riss des Seils bzw. Kabels melden.

#### Weitere Richtlinien für die Installation:

- Das Seil muss gut zugänglich sein, für Not-Halt-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, Metalispäne 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 Gegenfeder 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 Sicherheitsseilzugschaltersystems möglicherweise unwirksam oder fällt aus. Dies könnte einen unsicheren Zustand mit schweren bis tödliche Verletzungen als Folge bedingen.

## 6.4.5 Schutzhalt (Sicherheitsstopp)



Ein Schutzhalt ist für den Anschluss unterschiedlicher Vorrichtungen vorgesehen, zu denen Schutzeinrichtungen und ergänzende Einrichtungen gehören können. Diese Stoppfunktion ist eine Art der Betriebsunterbrechung, die eine geregeltes Herunterfahren zu Sicherheitszwecken 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 (siehe [Widerstandsfähigkeit gegen Fehler und Sicherheitsschaltungsprinzipien nach ISO 13849](#) auf Seite 18). 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 einen Stopp der Kategorie 0 oder Kategorie 1 entsprechend ANSI NFPA 79 und IEC 60204-1.

## 6.4.6 Verriegelte Schutzeinrichtung bzw. Schutztür



Die Sicherheitseingänge der Sicherheitsauswertung können zur Überwachung von elektrisch verriegelten Schutzeinrichtungen oder Schutztüren eingesetzt werden.

### Anforderungen an Sicherheitsschalter

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

Gefährliche Maschinen, die durch die Verriegelungseinrichtung 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 Abschalt Elemente der 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 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 die Schutzeinrichtung selbstständig schließt und den Verriegelungsschaltkreis aktiviert. Darüber hinaus muss die Installation verhindern, dass Personal über, unter, durch oder an der Schutzeinrichtung vorbei 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 eine weitere 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 verändern 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 Wiederanlaufsperrung 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.**

## 6.4.7 Optosensor



Die Sicherheitseingänge der Sicherheitsauswertung 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 der Sicherheitsauswertung 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 37).

## 6.4.8 Zweihandsteuerung



Die Sicherheitsauswertung kann als Steuergerät für die meisten angetriebenen Maschinen verwendet werden, bei denen der Maschinenzyklus von einer Bedierson 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 26).

Die Sicherheitseingänge der Sicherheitsauswertung dienen zur Überwachung der Auslösung der Handsteuerungen und erfüllen damit die Funktionalitätsanforderungen der Sicherheitskategorie III entsprechend IEC60204-1 und ISO 13851 (EN 574) 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 eine Zweihandsteuerung 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 falscher Ein-Zustand 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 Zweihandsteuerungen 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 falscher Ein-Zustand 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 Wiederanlaufsperrung haben**

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

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

## **Berechnung des Sicherheitsabstands (Mindestabstands) für Zweihandsteuerungen**

Der Bediener der Zweihandsteuerungen 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 Zweihandsteuerungen

**Zweihandsteuerungen 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 Sicherheitseinrichtung 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<sub>S</sub>**

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<sub>h</sub>**

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

T<sub>h</sub> ist für rein mechanische Schalter gewöhnlich nicht von Bedeutung. T<sub>h</sub> sollte jedoch zur Berechnung von Sicherheitsabständen in Betracht gezogen werden, wenn elektronische oder elektromechanische Handsteuerungen verwendet werden

**T<sub>m</sub>**

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<sub>m</sub> gleich der benötigten Zeit für eineinhalb Umdrehungen der Kurbelwelle. Bei kupplungsbetätigten Pressen mit Vollumdrehung und mehreren Einrückpunkten wird T<sub>m</sub> wie folgt berechnet:

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

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

**T<sub>cy</sub>** = benötigte Zeit (in Sekunden) für eine vollständige Umdrehung der Kurbelwelle

**T<sub>r</sub>**

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

**T<sub>s</sub>**

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

T<sub>s</sub> wird üblicherweise mit einem Stoppzeitmessgerät erfasst. Wird eine spezifizierte Maschinenstopzeit bei der Berechnung von T angewendet, sollten mindestens 20 % als Sicherheitsfaktor hinzugefügt werden, um eine eventuelle Alterung des Bremssystems zu berücksichtigen. Wenn die Stopzeit 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:

$$S = (K \times T) + C$$

**S**

der Mindestabstand (in Millimeter)

## Anwendungen in Europa

### 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 Eintrittstiefenfaktors 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.

## 6.4.9 Schaltmatte



Die Sicherheitsauswertung kann zur Überwachung von druckempfindlichen Sicherheitsschaltmatten und Sicherheitschaltleisten verwendet werden.

Der Schaltmatten-Eingang an der Sicherheitsauswertung dient zur Überwachung der korrekten Funktionsweise von 4-adrigen Sicherheitsschaltmatten mit Anwesenheitserkennung (Sensoren). Es können mehrere Sicherheitsschaltmatten in Reihe an einer Sicherheitsauswertung angeschlossen werden. Der maximale Widerstand je Eingang beträgt dabei 150 Ohm (siehe [Anschlussoptionen für Schaltmatten](#) auf Seite 31).



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

Die Sicherheitsauswertung überwacht die Kontakte (Kontaktplatten) und die Verdrahtung von einer oder mehreren Schaltmatten auf Fehler und verhindert den Wiederanlauf der Maschine, wenn ein Fehler erfasst wird. Die Sicherheitsauswertung kann eine Reset-Routine ausführen, nachdem der Bediener die Sicherheitsmatte verlassen hat, oder falls die Sicherheitsauswertung im Auto-Reset-Modus verwendet wird, muss die Reset-Funktion von der Maschinensteuerung ausgeführt werden. Hierdurch wird verhindert, dass die Maschine automatisch wiederanläuft, nachdem die Matte verlassen wurde.



### WARNUNG:

**Anwendung von Schaltmatten:** Die Anforderungen für den Einsatz von Sicherheitsschaltmatten variieren in Bezug auf das Performance Level gemäß der Beschreibung in ISO 13849-1 und ISO 13856. Die BERNSTEIN AG 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.

Verwenden Sie Schaltmatten nicht für den Tipbetrieb zur 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 Sicherheitsschaltmatten nicht, um die gefährliche Maschinenbewegung zu aktivieren oder der Maschinensteuerung nur durch Betreten der Matte einen Startbefehl zu geben (z. B. an einer Bedienerstation). Bei dieser Anwendungsart wird Umkehrlogik/negative Logik verwendet, und bestimmte Ausfälle (z. B. Stromausfall am Modul) können zu einem fehlerhaften Aktivierungssignal führen.

## Anforderungen für Schaltmatten

Es folgen Mindestanforderungen für Gestaltung, Konstruktion und Montage von vieradrigen Sicherheitsschaltmatten zum Anschluss an die Sicherheitsauswertung. 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 Schaltmattensystems

Der Sensor des Schaltmattensystems, die Sicherheitsauswertung 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 Schaltmattensystem 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 Schaltmatte sollte dieses Mindestgewicht und den Mindestdurchmesser als Mindest-Objektempfindlichkeit des Sensors angeben.

Änderungen 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 Sensorgehäusmaterials 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 Schaltmatten

Die Beschaffenheit der Montagefläche und die Vorbereitung für die Schaltmatte 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 Schaltmatte 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 korrodiert oder seine Empfindlichkeit verliert.

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

Jede Schaltmatte 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 Schaltmatte muss so montiert werden, dass Stolpergefahren minimiert werden (insbesondere in Richtung auf die gefährlichen Maschinenteile). 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 Schaltmatten-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 Sicherheitseinrichtung zu erreichen, sind unter Umständen zusätzliche Sicherheitseinrichtungen erforderlich.

Bei einer Sicherheitsschaltmatten-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 Schaltmatten

Als eigenständige Schutteinrichtung muss die Schaltmatte mit einem solchen 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-Schutteinrichtung 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 Eintrittstiefenfaktor. 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.

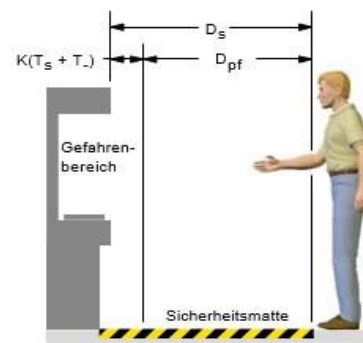


Abbildung 9: Ermittlung des Sicherheitsabstands für die Schaltmatte

### 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 der Sicherheitsauswertung gemessen ab dem Zeitpunkt, zu dem von einer der Handsteuerungen ein Stoppsignal erfolgt. Die Ansprechzeit der Sicherheitsauswertung 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.

#### $K$

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.

#### $D_{pf}$

die zusätzliche Entfernung aufgrund des Eintrittstiefenfaktors

gleich 48 in gemäß ANSI B11.19

### Anwendungen in Europa

Die Formel für Mindestabstand gemäß EN 13855:

$$S = (K \times T) + C$$

#### $S$

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.



## Anwendungen in Europa

T

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

C

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

## Anschlussoptionen für Schaltmatten

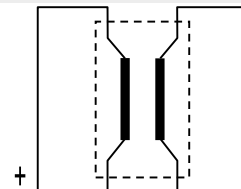
Druckempfindliche Matten und druckempfindliche Böden müssen die Anforderungen der Kategorie erfüllen, für die sie spezifiziert und gekennzeichnet sind. Diese Kategorien sind in ISO 13849-1 definiert.

Die Schaltmatte, ihre Sicherheitsauswertung 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.

**Die Sicherheitsauswertung 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). Die Sicherheitsauswertung wechselt in einen Sperrmodus, wenn eine Leitungsunterbrechung, ein Kurzschluss zu 0 V oder ein Kurzschluss zu einem anderen Stromkreis erfasst wird.



## 6.4.10 Muting-Sensor



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

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

US-Normen und internationale Normen schreiben vor, dass der Benutzer das Sicherheitssystem so auslegen, installieren und bedienen muss, dass das Personal geschützt ist und dass die Möglichkeit einer Umgehung der Sicherheitseinrichtung 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)

Einweglichtschranken 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.

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.

## Zwangsöffnende 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-Ausgängen oder kontaktbehafteten Ausgängen, die von der Spannungsversorgung unabhängig sind.

## Anforderungen an Muting-Einrichtungen

Die Muting-Vorrichtungen müssen mindestens die folgenden Anforderungen erfüllen:

- Es müssen mindestens zwei unabhängige fest verdrahtete Muting-Einrichtungen verwendet werden.
- Die Muting-Einrichtungen müssen entweder Schließerkontakte, pnp-Ausgänge (die jeweils die in den [Spezifikationen und Anforderungen](#) auf Seite 11 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 Spannungsversorgung ausgeschaltet ist.
- Die Aktivierung der Eingänge zur Muting-Funktion muss von getrennten Einrichtungen kommen. Diese Einrichtungen müssen separat installiert werden, damit ein unsicherer Muting-Zustand verhindert wird, der aus falscher Einstellung, Fehlausrichtung oder zwei Fehlern gleicher Ursache entstehen kann, z. B. durch physische Beschädigungen der Montagefläche. Nur eine dieser Einrichtungen darf auf einem programmierbaren Steuergerät (SPS) basieren.
- Die Muting-Einrichtungen müssen so installiert werden, dass sie nicht leicht außer Kraft gesetzt oder umgangen werden können.
- Die Muting-Einrichtungen müssen so montiert werden, dass ihre Position und Ausrichtung nicht einfach geändert werden kann.
- Es darf nicht möglich sein, dass Umweltbedingungen (z. B. extreme Luftverschmutzung) einen Muting-Zustand auslösen.
- Die Muting-Einrichtungen 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).

## 6.4.11 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 eine Überbrückungs-Betriebsart 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<sup>5</sup>:

- Die Überbrückungsfunktion muss zeitlich begrenzt sein.
- Die Einrichtung 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 Überbrückungseinrichtung muss von der zu überbrückenden Sicherheitseinrichtung aus vollständig einsehbar sein.
- Die Bewegungsinitiierung darf nur durch einen Tippschalter möglich sein.
- Alle Not-Halt-Schalter müssen aktiv bleiben.
- Die Überbrückungseinrichtung muss mit der gleichen Sicherheitsstufe verwendet werden wie die Sicherheitseinrichtung.
- Ein Überbrücken der Sicherheitseinrichtung muss vom Standort der Sicherheitseinrichtung aus deutlich erkennbar sein.
- Das Personal muss in der Verwendung der Sicherheitseinrichtung und der Überbrückung unterwiesen werden.
- Es müssen Risikobeurteilung und Risikominderung (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 Sicherheitseinrichtung darf nicht mit *Muting* verwechselt werden, bei dem es sich um die vorübergehende automatische Aufhebung der Sicherheitsfunktion einer Sicherheitseinrichtung 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 *Blanking*. Beim Blanking wird ein Teil des Erfassungsbereichs einer optischen Sicherheitseinrichtung deaktiviert (z. B. Deaktivierung eines oder mehrerer Strahlen eines Sicherheits-Lichtvorhangs, damit eine spezifische Strahlunterbrechung ignoriert wird).

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



Die AVM-Funktion (Adjustable Valve (Device) Monitoring) ist vergleichbar mit der einkanaligen Überwachung externer Geräte EDM (One-Channel External Device Monitoring, siehe [Externe Geräteüberwachung \(EDM\)](#) auf Seite 45). 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 den Zustand „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 den „Ein“ aufweisen, wenn der Sicherheitsausgang einen Einschaltversuch unternimmt; sonst tritt eine Sperre ein.

<sup>5</sup> 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.

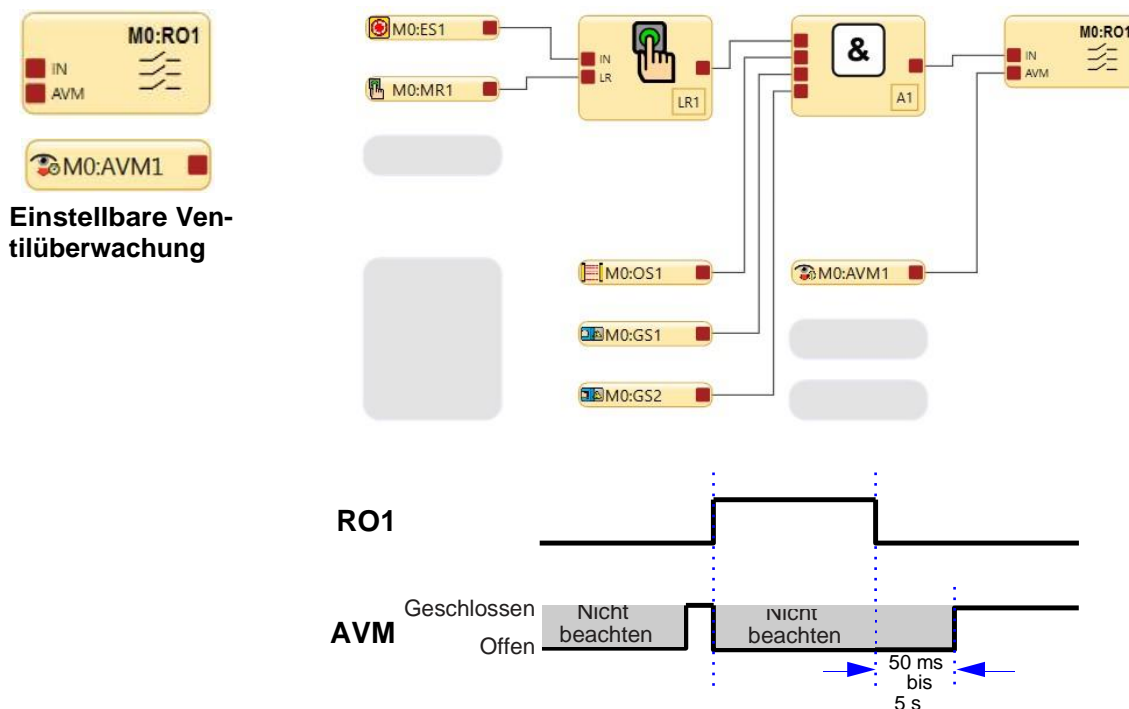


Abbildung 10: Zeitgeberlogik – AVM-Funktion

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 der Sicherheitsauswertung.



**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 Zeitdifferenz zwischen mehreren Geräten, z. B. Doppelventilen, kann durch Zuordnung mehrerer AVM-Funktionen zu einem Sicherheitsausgang und Konfiguration des AVM-Timers mit denselben Werten erreicht werden. Eine beliebige Anzahl an AVM-Eingängen kann einem Sicherheitsausgang zugeordnet werden. Ein Eingangssignal kann von einem Relaiskontakt oder einem 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.

## 6.4.13 DCD-Eingänge



Über die Sicherheitseingänge IN3/IN4 und IN5/IN6 des Sicherheitsauswertung können Geräte mit DCD-Daten (Daisy Chain Diagnostic) – auch in einer Reihenschaltung – wie SRF-Sicherheitssensoren von BERNSTEIN überwacht werden. Die SRF- Sicherheitssensoren von BERNSTEIN nutzen zur Erkennung RFID-Technologie.

DCD-Geräte wie SRF-Sicherheitssensoren 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 der Sicherheitsauswertung und den einzelnen Sicherheitseingängen ist auf der Registerkarte **Konfigurationsübersicht** in der Software angegeben. Diese Zeit muss zur Ansprechzeit der DCD-Reihenschaltung hinzugefügt werden.

Die aktiven Transistorausgänge der DCD-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 37.



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



**Anmerkung:** Wenn die gesamte Reihe nur aus Türschaltern besteht, gelten die Konfigurationsregeln für einen Schutztürschalter.

## 6.5 Nicht sicherheitsrelevante Eingangsgeräte

Zu den nicht sicherheitsrelevanten Eingangsgeräten gehören manuelle Reset-Vorrichtungen, Ein-/Aus-Schalter, Muting- und Freigabeeinrichtungen und Eingänge zum Abbruch von Zeitverzögerungen.

**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](#) auf Seite 39.



### 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](#) auf Seite 39.

**Muting-Aktivierungsschalter:** signalisiert der Sicherheitsauswertung, ob es den Muting-Sensoren erlaubt ist, eine Muting-Funktion auszuführen. Wenn die Muting-Aktivierungsfunktion konfiguriert ist, werden die Muting-Sensoren nicht zum Muting aktiviert, solange das Muting-Aktivierungssignal nicht im Ein-Zustand ist. Dies ist ein einkanaliges Signal; für die Aktivierung (EIN) sind 24 V DC, für die Deaktivierung (Stopp) sind 0 V DC erforderlich. Ein Muting-Aktivierungsschalter kann auch mit einem virtuellen Eingang erstellt werden. Siehe [Virtuelle nicht sicherheitsrelevante Eingangsgeräte](#) auf Seite 39.

**Einrichtungen für den Abbruch von Ausschaltverzögerungen:** Bieten die Möglichkeit, eine konfigurierte Ausschaltverzögerungszeit zu abbrechen. Diese Funktion bewirkt Folgendes:

- Sie sorgt dafür, dass der Sicherheits- oder Verzögerungsblockausgang eingeschaltet bleibt.
- Sie schaltet den Sicherheits- oder Verzögerungsblockausgang sofort aus, nachdem die Sicherheitsauswertung ein Signal für den Abbruch der Aus-Verzögerung 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 virtuellen Eingang erstellt werden. Siehe [Virtuelle nicht sicherheitsrelevante Eingangsgeräte](#) auf Seite 39.

**Zeitgeber für den Abbruch von Aus-Verzögerungen**

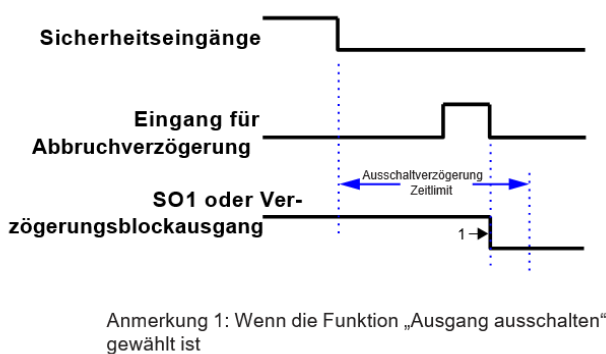


Abbildung 11: Sicherheitseingang verbleibt im Stopp-Modus

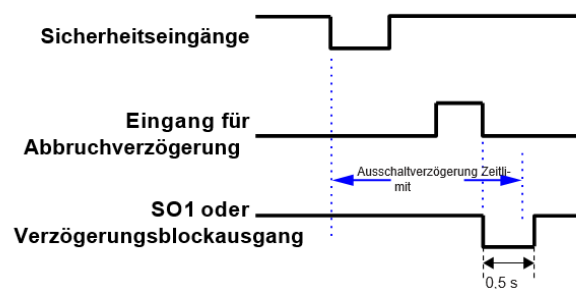


Abbildung 12: Ausgang schaltet sich aus

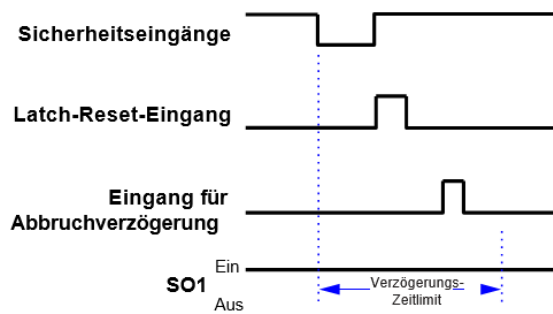


Abbildung 13: Ausgang bleibt für Sicherheitseingänge mit Latch-Reset eingeschaltet

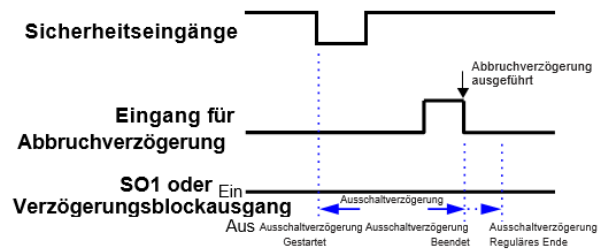


Abbildung 14: Ausgang bleibt für Sicherheitseingänge ohne Latch-Reset eingeschaltet

## 6.5.1 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 53):

### Reset von Sicherheitseingängen

Versetzt den Ausgang der Latch-Reset-Blöcke vom Verriegelungszustand in den Ein-Zustand, wenn sich der IN-Knoten in 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 Zustimmungstaster-Funktionsblock verbunden ist.

### System-Reset

Versetzt das System von einem durch einen Systemfehler verursachten Verriegelungszustand in den Ein-Zustand. Mögliche Szenarien, bei denen ein System-Reset erforderlich sein kann:

- Es werden Signale auf nicht verwendeten Anschlüssen erfasst.
- Zeitüberschreitung bei Konfigurationsmodus
- Beenden des Konfigurationsmodus
- Interne Fehler

### 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 der nachstehenden Warnhinweise 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 versehentliche Resets mit Ersatzschlüsseln im Besitz anderer dadurch nicht verhindert; auch das unbemerkte Eintreten weiterer Personen in den überwachten Bereich (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 Schutzvorrichtungen). Können Bereiche von den Reset-Schaltern aus nicht eingesehen werden, so müssen zusätzliche Sicherheitseinrichtungen bereitgestellt werden. Wenn diese Anweisungen nicht befolgt werden, können schwere oder tödliche Verletzungen die Folge sein.**



**Wichtig:** Durch Zurücksetzen einer Sicherheitseinrichtung 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 Sicherheitseinrichtung** 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 Sicherheitseinrichtungen 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 normalerweise in Anwendungen verwendet, in denen die Person ständig von der Sicherheitssensorik 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 von Relaisausgang“ des Sicherheitsausgangs konfiguriert werden (siehe [Funktionsblöcke](#) auf Seite 69).

Sicherheitseingänge arbeiten 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 Verriegelung des Sicherheitsausganges 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 Hintergrundgefahren in Bereichssicherungen gemindert oder beseitigt werden können (siehe [Eigenschaften von Sicherheitseingängen](#) auf Seite 19).

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 Reset mit abfallender Flanke 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 Reset mit ansteigender Flanke bezeichnet.

## 6.6 Virtuelle nicht sicherheitsrelevante Eingangsgeräte

Die virtuellen nicht sicherheitsrelevanten Eingangsgeräte umfassen Geräte für manuellen Reset, Ein/Aus-Schaltung, Muting-Aktivierung und Abbruch einer 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 Sicherheitseinrichtung 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 Sicherheitseinrichtungen verwendet werden, mindestens visuelle und akustische Warnungen über den Maschinenanlauf.

### 6.6.1 Virtueller manueller Reset und Abbrechen einer Zeitverzögerung (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 Sicherheitsauswertung 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.

Die BERNSTEIN AG 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 Betätigungscode für jede Sicherheitsauswertung im Netzwerk verwendet. Außerdem wird jeder virtuelle Reset innerhalb einer Auswertung einem bestimmten Bit in einem Register zugeordnet. Dieses Bit muss zusammen mit dem Betätigungscode 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 Normen verlangen zwar keine "bewusste Handlung", um ein virtuelles Abbrechen einer Zeitverzögerung auszuführen, aber um weitere Komplexität zu vermeiden, hat die BERNSTEIN AG diese Funktion in derselben Weise implementiert wie den virtuellen manuellen Reset.

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

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 Resetsequenz oder Abbruchsequenz einer Zeitverzögerung (RCD) – Feedbackmethode

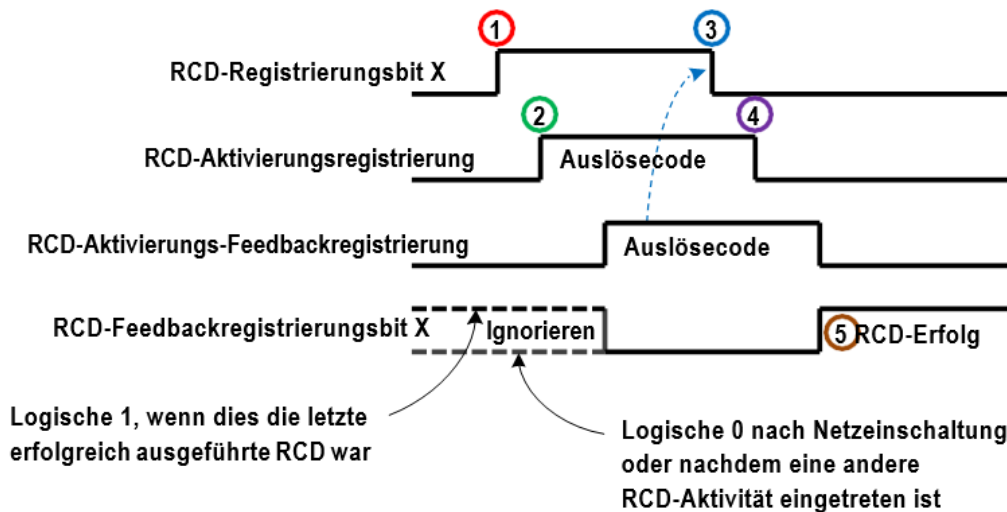


Abbildung 15: Virtuelle Resetsequenz oder Abbruchsequenz einer Zeitverzögerung (RCD) – Feedbackmethode

1. Schreiben Sie eine logische 1 in das oder die RCD-Registerbit(s), die der gewünschten virtuellen Reset- oder Abbruchfunktion 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 Abbruchfunktion akzeptiert wurde (175 ms typisch).

### Virtuelle Resetsequenz oder Abbruchsequenz einer Zeitverzögerung (RCD) – zeitgeschaltete Methode

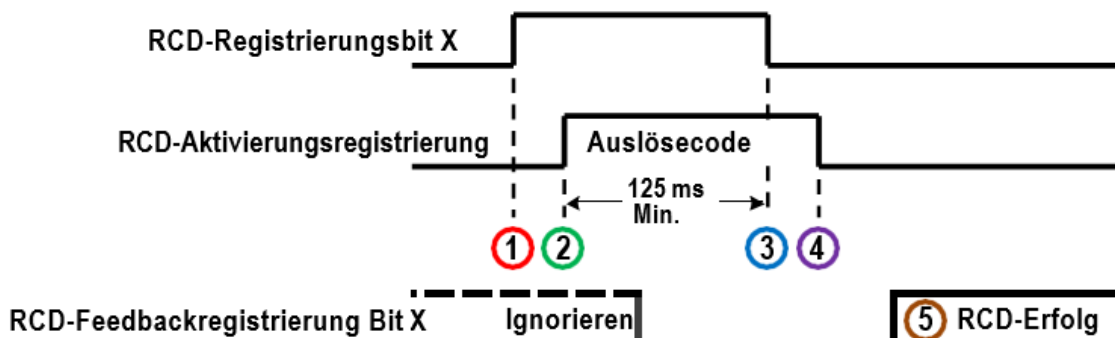


Abbildung 16: Virtuelle Resetsequenz oder Abbruchsequenz einer Zeitverzögerung (RCD) - zeitgeschaltete Methode

1. Schreiben Sie eine logische 1 zu den RCD-Registerbit(s), die der gewünschten virtuellen Reset- oder Abbruchfunktion 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 Abbruchfunktion akzeptiert wurde (175 ms typisch).

**Virtuelle manuelle Reset-Einrichtungen:** 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 36.




**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 Einrichtungen für den Abbruch von Ausschaltverzögerungen:** Bieten die Möglichkeit, eine konfigurierte Ausschaltverzögerungszeit abubrechen. Diese Funktion bewirkt Folgendes:

- Sie sorgt dafür, dass der Sicherheits- oder Verzögerungsblockausgang eingeschaltet bleibt.
- Sie schaltet den Sicherheits- oder Verzögerungsblockausgang sofort aus, nachdem die Sicherheitsauswertung ein Signal für den Abbruch der Aus-Verzögerung 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 Eingang aktiviert werden kann, um den Sicherheitsausgang mit der Ausschaltverzögerung eingeschaltet zu lassen. Eine Einrichtung für den Abbruch von Ausschaltverzögerungen kann auch mit einem physischen Eingang erstellt werden. Siehe *Nicht sicherheitsrelevante Eingangsgeräte* auf Seite 36.

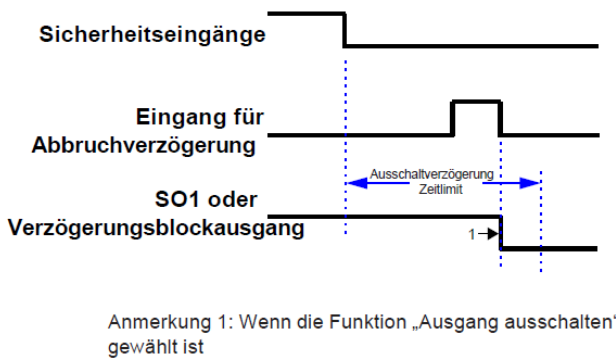
**Zeitablauffunktion für den virtuellen Abbruch einer Ausschaltverzögerung**


Abbildung 17: Sicherheitseingang verbleibt im Stopp-Modus

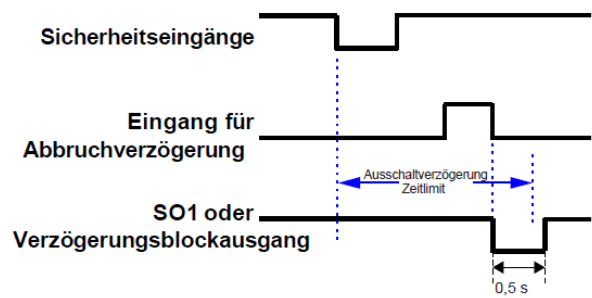


Abbildung 18: Ausgang schaltet sich aus

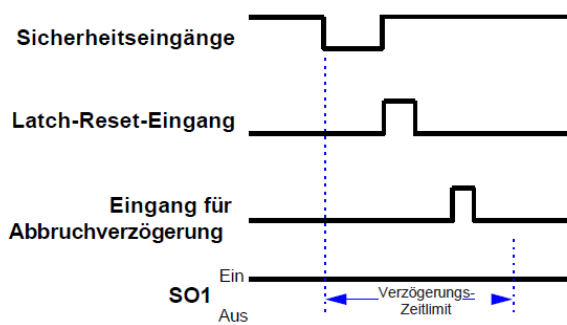


Abbildung 19: Ausgang bleibt für Sicherheitseingänge mit Latch-Reset eingeschaltet

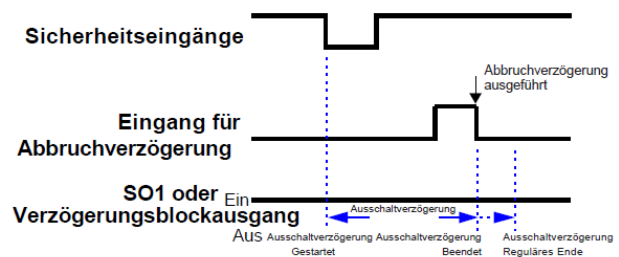


Abbildung 20: Ausgang bleibt für Sicherheitseingänge ohne Latch-Reset eingeschaltet

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

### Virtuelle Ein-/Ausschaltung

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. 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 36.

### Virtuelle Muting-Aktivierung

Signalisiert der Sicherheitsauswertung, wann es den Muting-Sensoren erlaubt ist, eine Muting-Funktion auszuführen. Wenn die Muting-Aktivierungsfunktion konfiguriert ist, werden die Muting-Sensoren nicht zum Muting aktiviert, solange das Muting-Aktivierungssignal nicht im Ein-Zustand ist. Der aktivierte Zustand (Ein-Zustand) ist eine logische 1 und der deaktivierte Zustand (Stoppzustand) ist eine logische 0. Ein Muting-Aktivierungsschalter kann auch mit einem physischen Eingang erstellt werden. Siehe [Nicht sicherheitsrelevante Eingangsgeräte](#) auf Seite 36.

## 6.7 Sicherheitsausgänge

Das SCR P hat zwei isolierte redundante Relaisausgänge. Jeder Relaisausgang verfügt über drei unabhängige Kontaktsätze. Siehe [Spezifikationen für das SCR P](#) auf Seite 11 zu Angaben über Nennwerten und Deratings.



**WARNUNG:** Die Sicherheitsausgänge müssen so an die Maschinensteuerung angeschlossen werden, dass der sicherheitsrelevante Teil der Maschinensteuerung den Freigabepfad zu den Abschalt-elementen der Maschine unterbricht, um einen sicheren Zustand herbeizuführen.

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

Die folgende Liste enthält eine Beschreibung weiterer Funktionen und Attribute, die im Fenster **Eigenschaften** für den Sicherheitsausgangs-Funktionsblock konfiguriert werden können (siehe [Hinzufügen von Eingängen und Statusausgängen](#) auf Seite 53):

### EDM (externe Geräteüberwachung)

Ermöglicht der Sicherheitsauswertung die Überwachung der angeschlossenen Geräte (FSDs und MPSEs) auf die richtige Reaktion auf den Abschaltbefehl der Sicherheitsausgänge. **Es wird dringend empfohlen, EDM (oder AVM)** in die Maschinenkonstruktion und in die Konfiguration der Sicherheitsauswertung einzubeziehen, um eine angemessene Fehlersicherheit der Sicherheitsschaltungen zu gewährleisten (siehe [EDM- und Abschaltgeräteanschluss](#) auf Seite 45).

### AVM (einstellbare Ventilüberwachung)

Ermöglicht der Sicherheitsauswertung 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 der Sicherheitsauswertung einzubeziehen, um eine angemessene Fehlersicherheit der Sicherheitsschaltungen zu gewährleisten (siehe [AVM-Funktion \(Adjustable Valve Monitoring, einstellbare Ventilüberwachung\)](#) auf Seite 33).

### LR (Latch-Reset)

Sorgt dafür, dass der RO-Ausgang ausgeschaltet bleibt, bis der Eingang in den Ein-Zustand wechselt und ein manueller Reset ausgeführt wird. Unter [Manueller Reset-Eingang](#) auf Seite 37 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 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 der Sicherheitsauswertung. Unter [Manueller Reset-Eingang](#) auf Seite 37 erhalten Sie weitere Informationen.

## Anlaufmodus

Der Sicherheitsausgang kann für drei Anlaufszenarien (Betriebs-eigenschaften beim Anlegen der Stromversorgung) konfiguriert werden:

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

Unter **Manueller Reset-Eingang** auf Seite 37 erhalten Sie weitere Informationen.

## Einschalt- und Ausschaltverzögerungen

Jeder Sicherheitsausgang kann so konfiguriert werden, dass er entweder mit einer Einschaltverzögerung oder mit einer Ausschaltverzögerung arbeitet (siehe **Abbildung 21** auf Seite 43), 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.

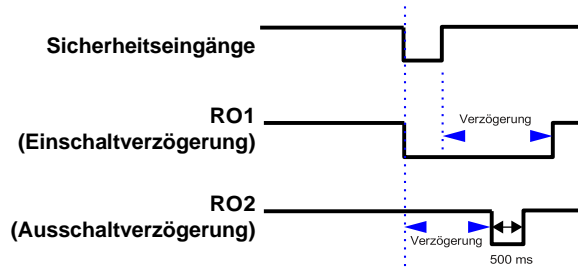


Abbildung 21: Zeitablauf-Diagramm: Ein- und Ausschaltverzögerung für Sicherheitsausgänge



### 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 Sicherheitsmaßnahmen 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 22** auf Seite 43 dargestellt. So verketteten 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.

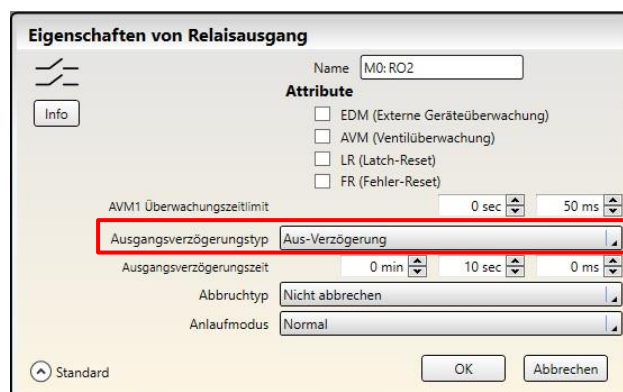


Abbildung 22: Auswahlbeispiel für Sicherheitsausgangsverzögerung: Ausschaltverzögerung

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 Aus- schaltverzögerung verkettet werden soll.
6. Wählen Sie aus der Dropdown-Liste *Verbindung zu Sicherheitsausgang* den Sicherheitsausgang mit Aus- schaltverzögerung aus, mit dem Sie diesen Sicherheitsausgang verketteten möchten.

Abbildung 23: 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.

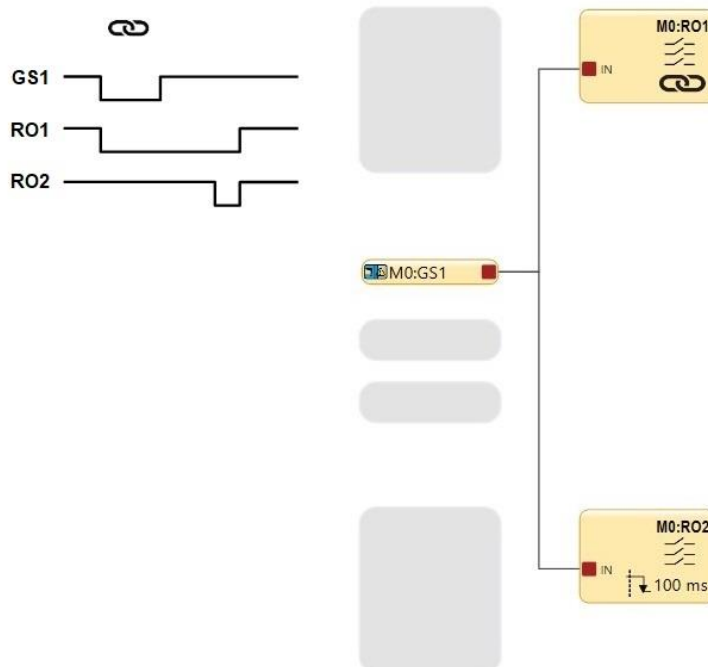


Abbildung 24: Zeitablauf-Diagramm: Verkettete Sicherheitsausgänge

## 6.7.1 Sicherheits-Relaisausgänge

Das SCR P verfügt über isolierte redundante Relaisausgänge, mit denen ein breites Spektrum an elektrischen Geräten gesteuert/geschaltet werden kann ([Spezifikationen für das SCR P](#) auf Seite 11). 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 SCR P 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 Schließer) 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 einem anderen Schaltkreis.

Soweit möglich, wird die Einbeziehung einer externen Geräteüberwachung (EDM) und/oder einer einstellbaren Ventilüberwachung (AVM) dringend empfohlen, um die angeschlossenen Geräte auf Störungen zu überwachen, die die Sicherheit gefährden. Unter [Externe Geräteüberwachung \(EDM\)](#) auf Seite 45 erhalten Sie weitere Informationen.

**Ausgangsanschlüsse:** Die Sicherheits-Relaisausgänge müssen so an die Maschinensteuerung angeschlossen werden, dass der sicherheitsrelevante Teil der Maschinensteuerung den Stromkreis oder die Versorgung zu den Abschaltenteilen der Maschine unterbricht und einen ungefährlichen Zustand herbeiführt.

Beachten Sie [Spezifikationen für das SCR P](#) auf Seite 11, bevor die Sicherheitsauswertung an die Maschine angeschlossen wird.

Das Sicherheitslevel 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 25](#) auf Seite 46 finden Sie Anschlussbeispiele.



**Wichtig:** Es liegt in der Verantwortung des Benutzers, alle Relaisausgänge mit einem geeigneten Kurzschlusschutz abzusichern.

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

Das SCR P ist 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. Das SCR P 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 SCR P zu schützenden elektrischen Störungen auf das Niveau der Überspannungskategorie II reduziert werden, oder wenn eine zusätzliche externe Isolierung installiert wurde, um sowohl das SCR P als auch die Bedienerperson 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 das SCR P unter den Bedingungen einer höheren Überspannungskategorie eingesetzt werden, wenn ein ausreichender Überspannungsschutz vorhanden ist. Geeignete Methoden:

- eine Überspannungsschutzeinrichtung,
- ein Transformator mit isolierten Wicklungen,
- ein Verteilungssystem mit mehreren Abzwegleitungen (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 SCR P 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 SCR P installiert werden (siehe WARNUNG, Lichtbogen-Entstörglieder).

### 6.7.2 EDM- und Abschaltgeräteanschluss Externe Geräteüberwachung (EDM)

Die Sicherheitsausgänge der Sicherheitsauswertung können externe Relais, Schütze oder andere Komponenten ansteuern, die einen Satz zwangsgeführter (mechanisch verbundener) Kontakte mit einem Öffnerkontakt haben, der zur Statusüberwachung der Schließerkontakte der Abschaltgeräte verwendet werden kann. Der Überwachungskontakt ist im geschlossenen Zustand, wenn die Komponente ausgeschaltet ist. Dadurch kann die Sicherheitsauswertung erkennen, ob die angeschlossenen Komponenten auf den Sicherheitsausgang ansprechen oder ob die Schließerkontakte möglicherweise verschweißt oder im Ein-Zustand blockiert sind.

Die EDM-Funktion bietet eine Methode zur Überwachung dieser Fehler und zur Sicherstellung der Funktionsfähigkeit eines zweikanaligen Systems einschließlich der Abschalt Elemente.

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

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

- **Einkanal-Überwachung:** Es handelt sich um eine Reihenschaltung geschlossener zwangsgeführter Überwachungskontakte, die zu den von jeweils einem der von den Sicherheitsausgängen der Auswertung angesteuerten Geräten gehören. Die Überwachungskontakte müssen geschlossen sein, bevor an den Ausgängen der Sicherheitsauswertung ein System-Reset ausgeführt werden kann (entweder manuell oder automatisch). Nachdem ein Reset ausgeführt wurde und die Sicherheitsausgänge einschalten, wird der Status der Überwachungskontakte 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 27](#) auf Seite 47.
- **Zweikanal-Überwachung:** Es handelt sich um den Anschluss voneinander unabhängiger geschlossener Überwachungskontakte, die jeweils mit einem durch die Sicherheitsauswertung gesteuerten Gerät mechanisch verbunden sind. Beide EDM-Eingänge müssen geschlossen werden, bevor am Sicherheitsauswertung 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 29](#) auf Seite 47.
- **Keine Überwachung (Standard):** Wenn keine Überwachung gewünscht wird, dürfen Sie den EDM-Knoten des Sicherheitsausgangs nicht aktivieren. Wenn die Sicherheitsauswertung 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 Maschinenstart 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)

Schließen Sie mindestens einen zwangsgeführten Überwachungs-Öffnerkontakt jedes externen Gerätes so an, dass der Status der einzelnen MPSEs überwacht werden kann (siehe Abbildung). Dadurch wird der ordnungsgemäße Betrieb der MPSEs überwacht. **Verwenden Sie die Überwachungskontakte der Abschalteteile zur Erhaltung der Sicherheitsstufe.**

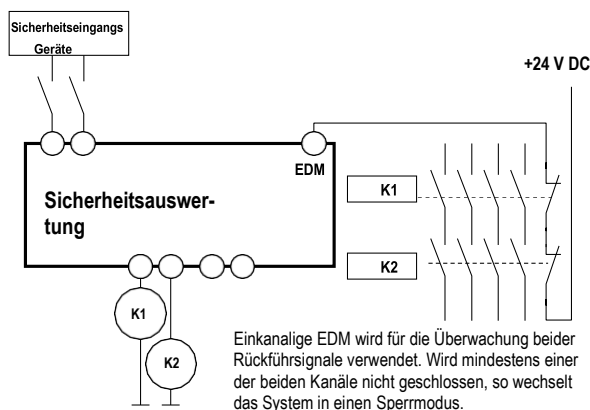


Abbildung 25: Anschluss der externen Zweikanal-Geräteüberwachung (Einkanal-EDM)

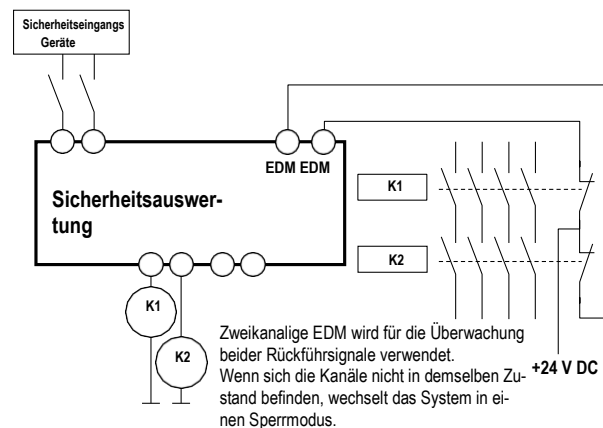
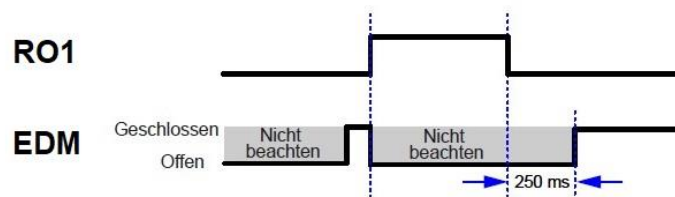
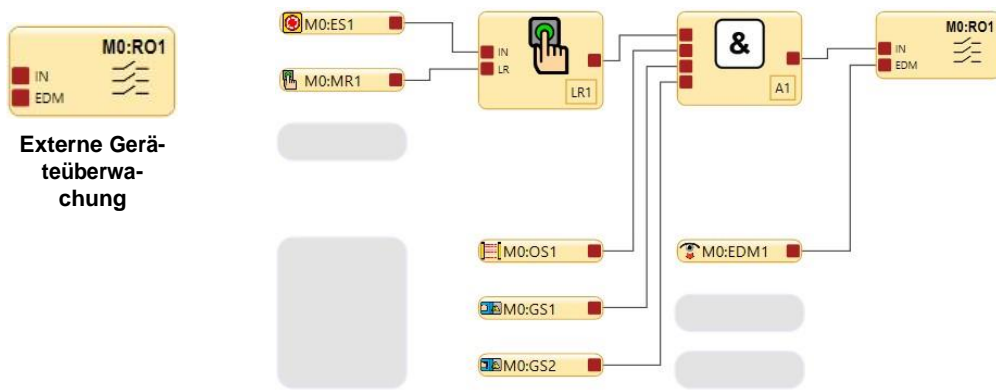


Abbildung 26: Anschluss der externen Zweikanal-Geräteüberwachung (Zweikanal-EDM)





Die externe Geräteüberwachung (EDM) ist eine Methode zur Überprüfung des Betriebs von zweikanaligen Abschaltgeräten. 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 Sicherheitsauswertung.

Abbildung 27: Zeitdiagramm: Status der einkanalen externen Geräteüberwachung in Bezug auf den Sicherheitsausgang

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

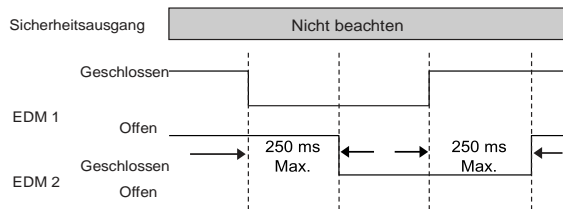


Abbildung 28: Zeitdiagramm: Zweikanalige EDM, zeitliche Abstimmung zwischen Kanälen

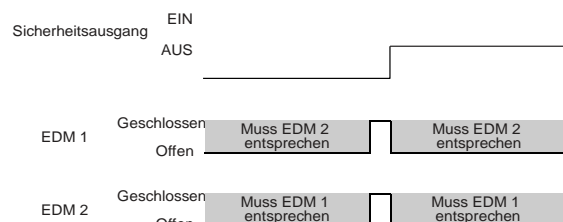


Abbildung 29: Zeitdiagramm: Status der zweikanaligen externen Geräteüberwachung in Bezug auf den Sicherheitsausgang

## Sicherheitsabschaltungen

Eine Sicherheitsabschaltung bewirkt einen definierten Stopp der Maschinenbewegung und eine Unterbrechung der Versorgungsspannung von den Antrieben (vorausgesetzt, es werden hierdurch keine zusätzlichen Gefahren erzeugt). Eine Sicherheitsabschaltung umfasst gewöhnlich mindestens zwei Schließkontakte von zwangsgeführten (mechanisch verbundenen) Relais, die zur Erkennung bestimmter Störungen (über einen mechanisch verbundenen Öffnerkontakt) überwacht werden, damit der Verlust der Sicherheitsfunktion verhindert wird.

Gewöhnlich sind Sicherheitsabschaltungen Reihenschaltungen von mindestens zwei Schließkontakten, die von zwei separaten zwangsgeführten Relais kommen, die jeweils von einem separaten Sicherheitsausgang der Sicherheitsauswertung angesteuert werden. Die Sicherheitsfunktion beruht auf der Verwendung redundanter Kontakte zur Überwachung einer einzelnen Gefahrenstelle, so dass bei Ausfall eines Kontakts im Ein-Zustand der zweite Kontakt die gefährliche Maschinenbewegung anhält und den Eintritt des nächsten Maschinenstarts verhindert.

Der Anschluss der Sicherheitsabschaltungen 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 Sicherheitssystems, zu dem die Sicherheitsauswertung gehört.



### **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 Abschaltetelemente. Installieren Sie diese nicht direkt auf den Kontakten der Abschaltetelemente. 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 der Sicherheitsauswertung und die Eingangsparameter der Maschine beim Anschließen der Sicherheitsausgänge 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 der Sicherheitsauswertung 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<sup>6</sup>. Dabei sind die geltenden elektrischen Standards und Verdrahtungsvorschriften einzuhalten, wie zum Beispiel der IEC/EN 60204-, NEC (National Electric Code), oder ANSI NFPA79, sowie sämtliche geltenden örtlichen Normen und Vorschriften.

Hierfür sind möglicherweise Lockout/Tagout-Verfahren (Verriegelung/Kennzeichnung) erforderlich. Siehe ISO 14118, OSHA 29CFR1910.147, ANSI Z244-1, 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 der Sicherheitsauswertung liegt in der Verantwortung des Anwenders. Die Verdrahtungskonfigurationen gelten allgemein und sollen lediglich veranschaulichen, wie wichtig eine sachgemäße Installation ist.

## Typischer Anschluss des SCR P: Sicherheitsausgang mit EDM

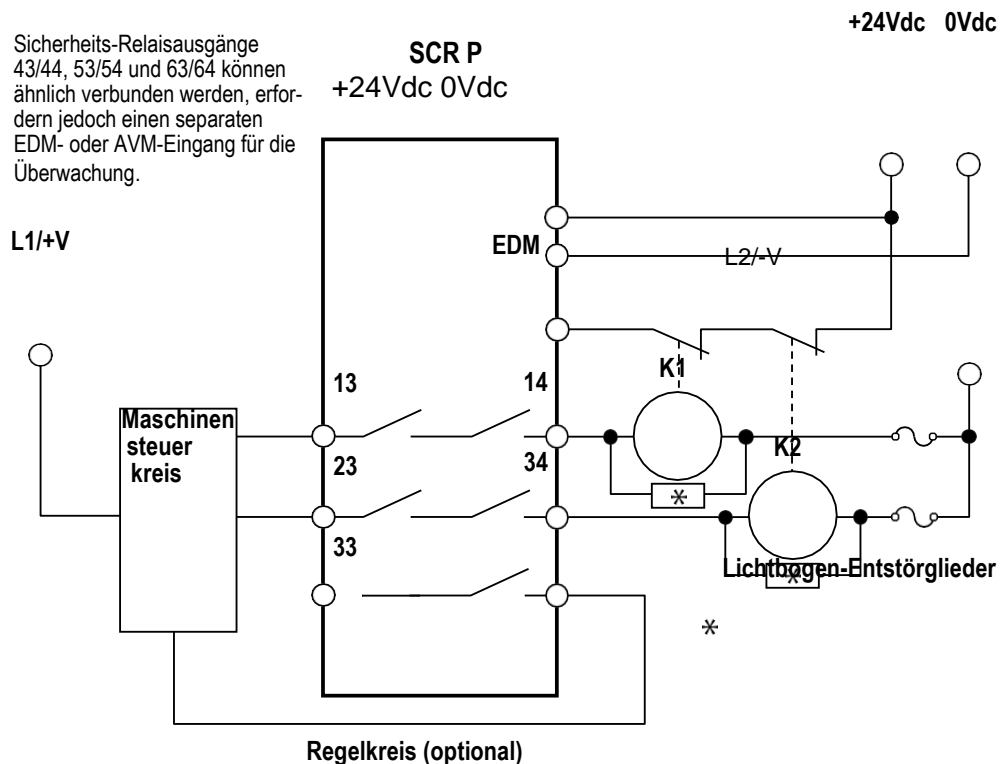


Abbildung 30: Typischer Anschluss des SCR P: Sicherheits-Relaisausgang (zweikanalig) mit EDM

## 6.8 Statusausgänge

### 6.8.1 Signallogik für Statusausgänge



**Anmerkung:** Sie dürfen die Sicherheitsausgänge am SCR P 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“.

Tabelle 4. 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
Eingangstatus 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
Ausgangsstatus anzeigen	RO ein	RO aus	RO ein	RO 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

Funktion	Signallogik			
	Aktiv = PNP ein		Aktiv = PNP aus	
	Statusausgangs-Status		Statusausgangs-Status	
	+24 V DC	Aus	Aus	24 V DC
Status des Verzögerungsblocks verfolgen	Ein	Stopp	Ein	Stopp
Warten auf manuellen Reset	Reset erforderlich	Nicht erfüllt	Reset erforderlich	Nicht erfüllt
Systemsperr	Gesperrt	RUN-Modus	Gesperrt	RUN-Modus

## 6.8.2 Statusausgangsfunktion

**SCR P:** Bis zu 4 konfigurierbare Eingänge können als Statusausgang verwendet werden.

Statusausgänge können für die Ausführung der folgenden Funktionen konfiguriert werden:

### Überbrückung

Gibt an, wenn ein bestimmter Sicherheitseingang überbrückt wird.

### Muting

Gibt einen Muting-Freigabestatus für einen bestimmten mutingfähigen Sicherheitseingang an:

- EIN, wenn ein mutingfähiger Eingang gemutet ist
- AUS, wenn ein mutingfähiger Eingang nicht gemutet ist
- Die Anzeige blinkt, wenn die Bedingungen zum Starten für das Muting der Sicherheitseinrichtung 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 des aktiven Mutings (keine Umgehungsfunktion) eines mutingfähigen Sicherheitseingangs

### Ausgangsverzögerung läuft

Gibt an, dass die Ein- oder Ausschaltverzögerung aktiv ist.

### Eingangstatus anzeigen

Gibt den Status eines bestimmten Sicherheitseingangs an.

### Eingangsfehler anzeigen

Gibt an, dass ein bestimmter Sicherheitseingang einen Fehler aufweist.

### Beliebigen Eingangsfehler anzeigen

Gibt an, dass irgendein Sicherheitseingang einen Fehler aufweist.

### Eingangsgruppenanzeige

Gibt den Status einer Gruppe von Sicherheitseingängen 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 Eingangsgruppen können nachverfolgt werden.

### Ausgangsstatus anzeigen

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

### Ausgangsfehler anzeigen

Gibt an, dass ein bestimmter Sicherheitsausgang einen Fehler aufweist.

### Ausgangsfehler anzeigen, alle

Gibt an, dass irgendein Sicherheitsausgang einen Fehler aufweist.

### Logischen Ausgangsstatus anzeigen

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

Gibt den Status eines bestimmten Funktionsblocks an.

### Warten auf manuellen Reset

Gibt an, dass ein bestimmter konfigurierter Reset erforderlich ist.

### Systemsperrung

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

## 6.9 Virtuelle Statusausgänge

---

Bis zu 256 virtuelle Statusausgänge können bei SCR P Sicherheitsauswertungen hinzugefügt werden. Diese Ausgänge können über das Netzwerk dieselben Informationen übermitteln wie die Statusausgänge. Siehe [Statusausgangsfunktion](#) auf Seite [Statusausgangsfunktion51](#) für weitere Informationen. Die Funktion **Automatisch konfigurieren** auf der Registerkarte **Industrial 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 **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. Siehe [Registerkarte Industrial-Ethernet](#) auf Seite 93 für nähere Informationen zum Konfigurieren der virtuellen Statusausgänge.

Leistungs- und Statusinformationen der angeschlossenen DCD-Reihenschaltungen und der einzelnen Geräte innerhalb der Reihenschaltung können über die Sicherheitsauswertung SCR P abgerufen werden.

Für den Status jeder angeschlossenen Reihenschaltung stehen 16 Word (16 Bit) Daten zur Verfügung.

Für jedes Gerät innerhalb der Reihenschaltung stehen 3 Word (16 Bit) administrative und 18 Byte (8 Bit) spezifische Daten zur Verfügung (1 Word = 16 Bit; 1 Byte = 8 Bit).

Weitere Informationen finden Sie in Kapitel [Baugruppenobjekte](#) auf Seite 97.



## 7. Erste Schritte

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

### 7.1 Erstellen einer Konfiguration

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

1. Definition einer Sicherheitsanwendung (Risikobeurteilung)
  - Bestimmung der erforderlichen Komponenten
  - Bestimmung der erforderlichen Sicherheitsstufe
2. Installieren Sie die Software für die Sicherheitsauswertung der BERNSTEIN AG. Siehe [Installation der Software](#) auf Seite 15.
3. Machen Sie sich mit den Optionen in der Software vertraut. Siehe [Software-Übersicht](#) auf Seite 62.
4. Starten Sie ein neues Projekt mit einem Klick auf **Neues Projekt/ Zuletzt verwendete Dateien**.
5. Definieren Sie die **Projekteinstellungen**. Siehe [Projekteinstellungen](#) auf Seite 64.
6. Fügen Sie Sicherheitseingänge, nicht sicherheitsrelevante Eingänge und Statusausgänge hinzu. Siehe [Hinzufügen von Eingängen und Statusausgängen](#) auf Seite 53.
7. Entwerfen Sie die Steuerungslogik. Siehe [Entwerfen der Steuerungslogik](#) auf Seite 58.
8. Stellen Sie optionale Ein- oder Ausschaltverzögerungszeiten für Sicherheitsausgänge ein.
9. Sofern verwendet, konfigurieren Sie die Netzwerkeinstellungen. Siehe [Netzwerkeinstellungen: Modbus/TCP, Ethernet/IP, PCCC](#) auf Seite 94 oder [Netzwerkeinstellungen: PROFINET](#) auf Seite 95.
10. Speichern und bestätigen Sie die Konfiguration. Siehe [Speichern und Bestätigen einer Konfiguration](#) auf Seite 70.


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

1. Ändern Sie die Zugriffsrechte für die Konfiguration.
2. Überprüfen Sie anhand der Registerkarte **Konfigurationsübersicht** die detaillierten Geräteinformationen und Ansprechzeiten. Siehe [Registerkarte Konfigurationsübersicht](#) auf Seite 103.
3. Drucken Sie die Konfigurationsansichten, einschließlich der **Konfigurationsübersicht** und der **Netzwerkeinstellungen**. Siehe [Druckoptionen](#) auf Seite 104
4. Konfigurationstests mit dem Simulationsmodus. Siehe [Simulationsmodus](#) auf Seite 110.

### 7.2 Hinzufügen von Eingängen und Statusausgängen

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

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

1. Klicken Sie in der Ansicht **Geräte** unter dem Modul, mit dem das Schaltgerät 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.

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



Abbildung 31: Sicherheitseingänge (virtuelle nicht sicherheitsrelevante Eingänge nur über die Registerkarte **Funktionsansicht** verfügbar)



Abbildung 32: Nicht sicherheitsrelevante Eingänge (virtuelle nicht sicherheitsrelevante Eingänge nur über die Registerkarte **Funktionsansicht** verfügbar)

3. Wählen Sie die geeigneten Geräteeinstellungen aus:

**Allgemeine Einstellungen:**

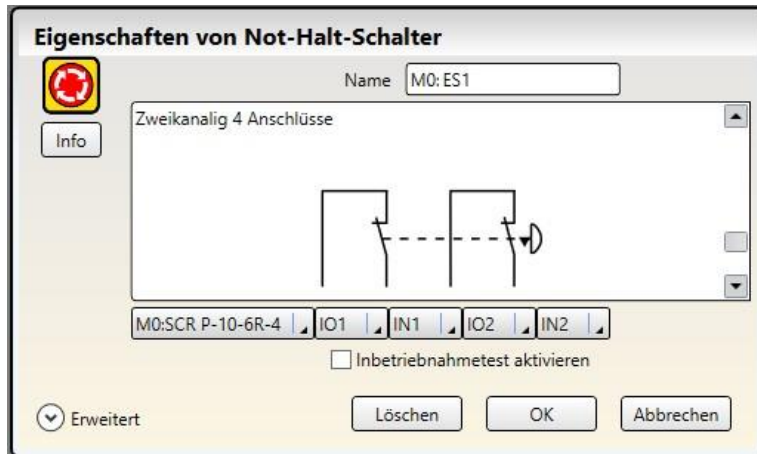


Abbildung 33: Allgemeine Einstellungen für Sicherheitseingänge

- **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.
- **Modul:** das Modul, mit dem das Eingangsgerät verbunden ist.
- **Ein-/Ausgangsklemmen:** die Zuordnung der Eingangsklemmen für das ausgewählte Gerät an dem ausgewählten Modul.
- **Inbetriebnahmetest aktivieren** (sofern zutreffend): ein optionaler Test des Sicherheitsschaltgeräts 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):**

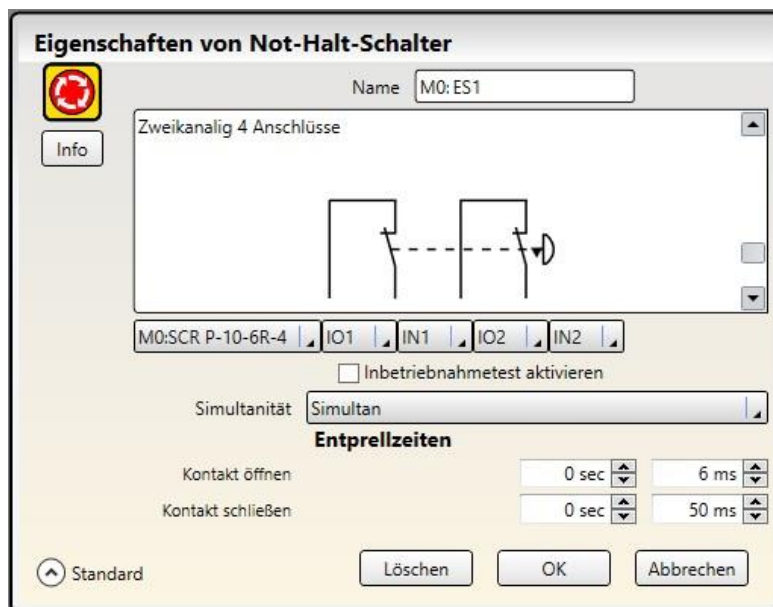


Abbildung 34: Erweiterte Einstellungen für Sicherheitseingänge

- **Simultanität** (sofern zutreffend): „Simultan“ oder „Nicht simultan“ (zu den Definitionen siehe [Glossar](#) auf Seite 145).
- **Entprellzeiten:** die Zeit für den Übergang des Signals in einen anderen Zustand.
- **Überwacht/Nicht überwacht** (sofern zutreffend).

**DCD Geräteeigenschaften (sofern zutreffend):**

**Eigenschaften von DCD-Gerät**

Info

Name: M0: DCD1

Module: M0:SCR P-10-6R-4

Terminals: IN3, IN4

Geräteanzahl: 2

Position	Name	Typ
1	Gerät 1	Türschalter
2	Gerät 2	Türschalter

**Entprellzeiten**

Kontakt öffnen: 0 sec, 6 ms

Kontakt schließen: 0 sec, 50 ms

Standard Löschen OK Abbrechen


Abbildung 35: DCD Geräteeigenschaften für Sicherheitseingänge

- **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 Geräte (Notwendig):** Die Anzahl der in Reihe geschalteten DCD - Geräte in der Applikation
- **Position, Name und Typ:** Die Position, relativ zum SCR P, der Name und der Typ (z.B. Türsensor) des DCD Gerätes in der Applikation
- **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 Schutz Türschalter.

## 7.2.2 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.<sup>7</sup>

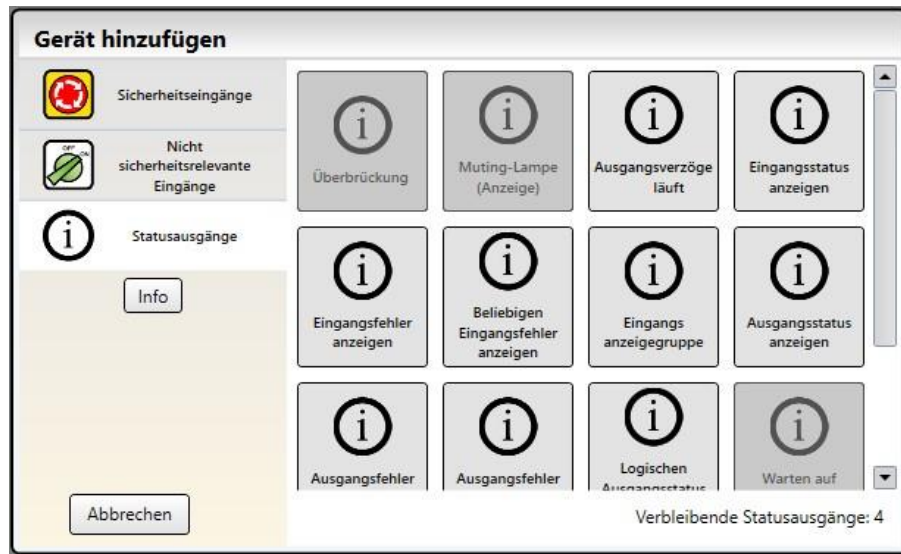


Abbildung 36: Statusausgänge

3. Wählen Sie die geeigneten Einstellungen für Statusausgänge:

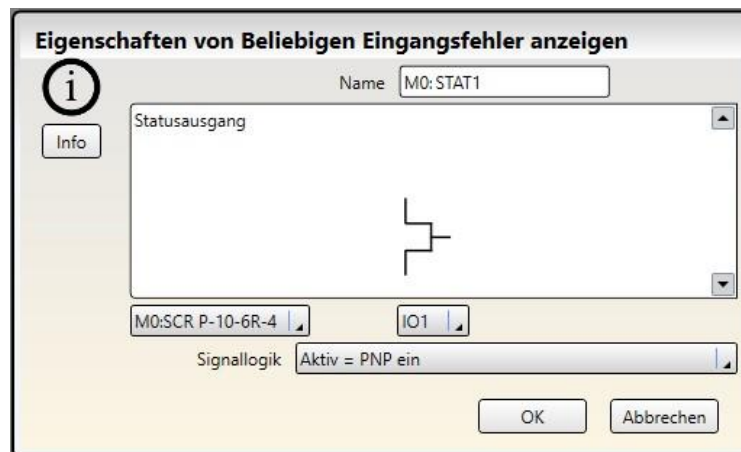



Abbildung 37: Statusausgangs-Eigenschaften

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

## 7.3 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.

Unter [Hinzufügen von Eingängen und Statusausgängen](#) auf Seite 53 finden Sie weitere Informationen und Geräteeigenschaften.

2. Fügen Sie **Logik-** und/oder **Funktionsblöcke** hinzu (siehe [Logikblöcke](#) auf Seite 67 und [Funktionsblöcke](#) auf Seite 69), 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.



**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 Sicherheitsauswertung akzeptiert keine ungültige Konfiguration.



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

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

## 7.4 Speichern und Bestätigen einer Konfiguration


Die Bestätigung ist ein Überprüfungsprozess, bei dem die Sicherheitsauswertung 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 von dem Gerät verwendet werden kann. Nachdem die Konfiguration bestätigt wurde, kann sie an eine Sicherheitsauswertung gesendet oder auf einem PC oder SCR P-FPS-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 der Sicherheitsauswertung vollständig getestet werden (Inbetriebnahmeprüfung), bevor er zur Steuerung von Gefahren verwendet werden kann.

### Speichern einer Konfiguration:

1. Klicken Sie auf  **Projekt speichern**.
2. Wählen Sie **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 **Speichern**.

**Bestätigen einer Konfiguration** (die Sicherheitsauswertung muss eingeschaltet und über das USB-Kabel mit dem PC verbunden sein):

1. Klicken Sie auf .
2. Klicken Sie auf **Konfiguration in die Auswertung 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 der Auswertung 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 die Auswertung** abgeschlossen ist.



**Anmerkung:**

- Die Netzwerkeinstellungen werden von den Konfigurationseinstellungen getrennt gesendet. Klicken Sie im Fenster **Netzwerkeinstellungen** auf **Senden**, um die Netzwerkeinstellungen in die Sicherheitsauswertung zu schreiben.
- SCR P: Die Netzwerkeinstellungen werden nur dann automatisch gesendet, wenn auf dem SCR P die Werkseinstellungen für die Sicherheitsauswertung konfiguriert sind. Andernfalls müssen Sie das Fenster **Netzwerkeinstellungen** verwenden.
- SCR P: Die Passwörter werden nur dann automatisch geschrieben, wenn auf dem SCR P die Werkseinstellungen für die Sicherheitsauswertung konfiguriert sind und die Konfiguration bestätigt wurde. Verwenden Sie andernfalls zum Schreiben von Passwörtern in einen SCR P das Fenster **Passwort-Manager**.

Beim Konfigurieren eines SCR P wird unter Umständen der Bildschirm „*Möchten Sie die Passwörter der Auswertung ändern?*“ angezeigt.

8. Ändern Sie die Passwörter für das SCR P bei Bedarf oder wenn Sie dazu aufgefordert werden.
9. Schalten Sie die Sicherheitsauswertung aus und wieder ein oder führen Sie einen System-Reset aus, damit die Änderungen wirksam werden.



**Anmerkung:** Es empfiehlt sich, die soeben bestätigte Konfiguration zu speichern. Bestätigte Konfigurationen haben ein anderes Dateiformat (.xcc) als unbestätigte (.xsc). Bestätigte Konfigurationen sind zum Laden der jeweiligen Konfiguration in ein SCR P-FPS-Laufwerk erforderlich. Klicken Sie auf **Speichern unter**, um die Konfiguration zu speichern.

## 7.4.1 Hinweise zum Bestätigen oder Schreiben einer Konfiguration in ein konfiguriertes SCR P

Benutzereinstellungen und Passwörter beeinflussen, wie das System beim Bestätigen einer Konfiguration oder beim Schreiben einer bestätigten Konfiguration in ein konfiguriertes SCR P reagiert.

### Benutzer1

1. Klicken Sie auf **Konfiguration in die Auswertung schreiben**, um eine Konfiguration zu bestätigen bzw. um eine bestätigte Konfiguration in eine konfigurierte Sicherheitsauswertung zu schreiben.
2. Geben Sie das Passwort „Benutzer1“ ein.
3. Der Bestätigungs- bzw. Schreibvorgang beginnt.

Am Ende des Bestätigungs- bzw. Schreibvorgangs hat die Sicherheitsauswertung 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 die Auswertung schreiben**, um eine Konfiguration zu bestätigen bzw. um eine bestätigte Konfiguration in eine konfigurierte Sicherheitsauswertung 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 die Sicherheitsauswertung 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 die Auswertung schreiben**, um eine Konfiguration zu bestätigen bzw. um eine bestätigte Konfiguration in eine konfigurierte Sicherheitsauswertung zu schreiben.
2. Geben Sie das Passwort für Benutzer2 oder Benutzer3 ein.
3. Der Bestätigungs- bzw. Schreibvorgang wird abgebrochen.

## 8. Software

Die Software für die Sicherheitsauswertung von BERNSTEIN 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 die Sicherheitsauswertung
- Lesen der aktuellen Konfiguration aus der Sicherheitsauswertung
- Anzeigen von Echtzeitinformationen, z. B. zum Gerätestatus, Diagnosedaten
- Anzeigen von Fehlerinformationen

Die Software verwendet simple Schaltungs- und Logiksymbole, mit denen Sie intuitiv die geeigneten Eingangsfunktionen und deren Eigenschaften festlegen können. Nachdem die benötigte Konfiguration, inkl. Geräteeigenschaften und E/A-Steuerungsbeziehungen auf der Registerkarte **Funktionsansicht** erstellt wurde, erstellt das Programm automatisch die entsprechenden Schalt- und Kontaktpläne.

Unter [Erstellen einer Konfiguration](#) auf Seite 53 finden Sie Informationen zum Konfigurationserstellungsprozess.

Unter [Registerkarte Schaltplan](#) auf Seite 88 finden Sie Informationen zum Verbinden von Geräten sowie [Registerkarte Kontaktplan](#) auf Seite 89 die Darstellung der Kontaktpläne der Konfiguration.

Unter [Livemodus](#) auf Seite 107 finden Sie Laufzeitinformationen der Sicherheitsauswertung.

### 8.1 Abkürzungen

Abkürzung <sup>8</sup>	Beschreibung
<b>AVM</b>	Eingangsknoten für einstellbare Ventilüberwachung der Sicherheitsausgänge
<b>AVMx</b>	Eingang für einstellbare Ventilüberwachung
<b>BP</b>	Eingangsknoten für Überbrückung bei den Überbrückungsblöcken und Muting-Blöcken
<b>BPx</b>	Überbrückungsschalter-Eingang
<b>CD</b>	Eingangsknoten für Abbruchverzögerung der Sicherheitsausgänge
<b>CDx</b>	Eingang für Abbruchverzögerung
<b>DCD</b>	Daisy Chain Diagnose
<b>ED</b>	Eingangsknoten für Zustimmungstaster der Zustimmungstaster-Blöcke
<b>EDx</b>	Zustimmungstaster-Eingang
<b>EDM</b>	Eingangsknoten für externe Geräteüberwachung der Sicherheitsausgänge
<b>EDMx</b>	Eingang für externe Geräteüberwachung
<b>ES</b>	Eingangsknoten für Not-Aus-Schalter der Zustimmungstaster-Blöcke
<b>ESx</b>	Eingang für Not-Halt-Schalter
<b>ETB</b>	Externer Klemmenblock
<b>FID</b>	Merkmalkennzeichnung
<b>FR</b>	Eingangsknoten für Fehler-Reset der Sicherheitsausgänge
<b>GSx</b>	Schutztürschalter-Eingang
<b>Weiterschalten</b>	Eingangsknoten für Weiterschalten der Zustimmungstaster-Blöcke
<b>IN</b>	Normaler Eingangsknoten der Funktionsblöcke und Sicherheitsausgangsblöcke
<b>LR</b>	Eingangsknoten für Latch-Reset des Latch-Reset-Blocks und der Sicherheitsausgänge
<b>ME</b>	Eingangsknoten für Muting-Freigabe der Muting-Blöcke und der Zweihandsteuerungsblöcke
<b>MEx</b>	Eingang für Muting-Freigabe
<b>MP1</b>	Eingangsknoten für das erste Muting-Sensorpaar in Muting-Blöcken und Zweihandsteuerungsblöcken
<b>MP2</b>	Eingangsknoten für das zweite Muting-Sensorpaar (nur Muting-Blöcke)
<b>Mx</b>	Sicherheitsauswertung
<b>MRx</b>	Manueller Reset-Eingang

<sup>8</sup> Die Endung „x“ bezeichnet die automatisch zugewiesene Nummer.

<b>Abkürzung<sup>8</sup></b>	<b>Beschreibung</b>
<b>MSPx</b>	Muting-Sensorpaar-Eingang
<b>ONx</b>	Eingang für EIN/AUS
<b>OSx</b>	Optosensor-Eingang
<b>PSx</b>	Schutzhalt-Eingang
<b>RE</b>	Eingangsknoten für Reset-Aktivierung der Latch-Reset-Blöcke und der Sicherheitsausgänge
<b>ROx</b>	Relaisausgang
<b>RPI</b>	Gefordertes Paketintervall
<b>RPx</b>	Seilzugschalter-Eingang
<b>RST</b>	Reset-Knoten für SR Flip-Flop, RS Flip-Flop, Latch-Reset-Blöcke und Zustimmungstaster-Blöcke
<b>SET</b>	Einstellknoten der SR- und RS-Flip-Flop-Blöcke
<b>SMx</b>	Eingang für Sicherheitsmatten
<b>ROx</b>	Sicherheitsausgang
<b>STATx</b>	Statusausgang
<b>GE</b>	Eingangsknoten für Zweihandsteuerung der Zweihandsteuerungsblöcke
<b>TCx</b>	Zweihandsteuerungseingang

<sup>8</sup> Die Endung „x“ bezeichnet die automatisch zugewiesene Nummer.

## 8.2 Software-Übersicht

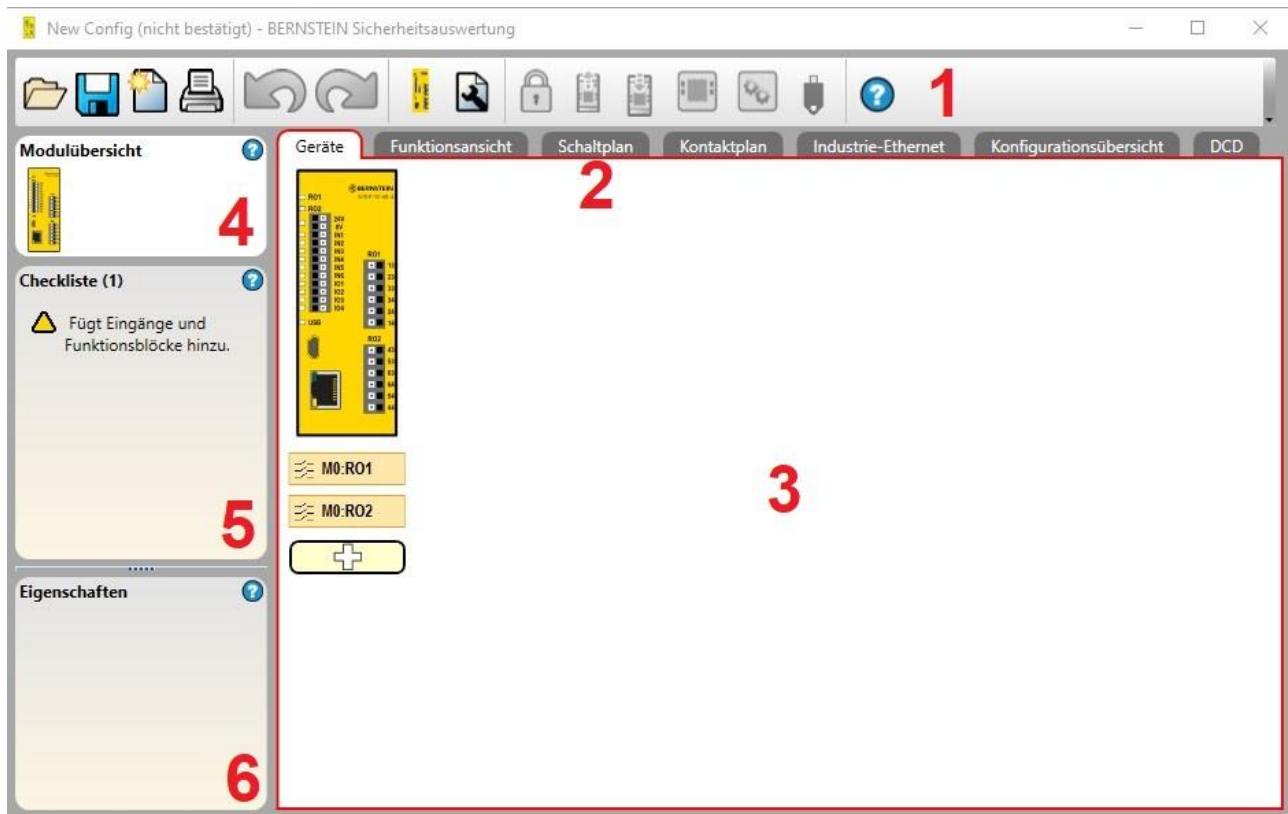


Abbildung 38: Software für die Sicherheitsauswertung von BERNSTEIN

- (1) Symbolleiste „Navigation“
- (2) Registerkarten für Arbeitsblätter und Diagramme
- (3) Ausgewählte Ansicht
- (4) Modulübersicht
- (5) Checkliste
- (6) Eigenschaften

## (1) Symbolleiste „Navigation“

	Startet ein <b>Neues Projekt</b>		Liest Daten aus der Sicherheitsauswertung (Upload), wie z.B. Fehlerprotokoll, Konfigurationsdaten, Netzwerkeinstellungen und Geräteinformationen.
	Öffnet ein bestehendes Projekt, öffnet eines der <b>Zuletzt bearbeiteten</b> Projekte oder öffnet <b>Beispielprojekte</b>		Schreibt Daten auf die Sicherheitsauswertung (Download), wie z.B. Konfigurationsdaten und Einstellungen.
	Speichert das Projekt unter dem benutzerdefinierten Pfad.		Startet den Livemodus.
	Druckt eine anpassbare Konfigurationsübersicht.		Startet den Simulationsmodus.
	Macht bis zu 10 vorher ausgeführte Aktionen rückgängig.		Status der Laufwerksverbindung zum SCR P-PA bzw. SCR P-FPS.
	Stellt bis zu 10 zuvor rückgängig gemachte Aktionen wieder her.	<p>Öffnet die <b>Hilfe</b>-Optionen.</p> <ol style="list-style-type: none"> <li>5. <b>Hilfe</b>: Öffnet die Hilfethemen.</li> <li>6. <b>Über</b>: Zeigt die Versionsnummer der Software und den Warnhinweis zu den Pflichten des Benutzers.</li> <li>7. <b>Versionshinweise</b>: Zeigt die Versionshinweise für alle Softwareversionen an.</li> <li>8. <b>Symbole</b>: Umschaltung zwischen den Symbolen im US-amerikanischen und europäischen Format.</li> <li>9. <b>Support-Informationen</b>: Beschreibt, wie Sie bei BERNSTEN Hilfe anfordern können.</li> <li>10. <b>Sprache</b>: Auswahl der Sprachoptionen für die Software.</li> </ol>	
	Zeigt die Netzwerkeinstellungen an und schreibt diese in die Sicherheitsauswertung.		
	Öffnet die Projekteinstellungen.		
	Öffnet den Passwort-Manager.		

## (2) Registerkarten für Arbeitsblätter und Diagramme

**Geräte**: Zeigt eine editierbare Übersicht aller verbundenen Geräte.

**Funktionsansicht**: Zeigt die konfigurierte Steuerungslogik.

**Schaltplan**: Zeigt einen Anschlussplan für das SCR P (z.B. für den Elektorinstallateur).

**Kontaktplan**: Zeigt eine symbolische Darstellung der konfigurierten Schutzlogik (z.B. für den Maschinenkonstrukteur oder den Steuerungstechniker).

**Industrial-Ethernet** (sofern aktiviert): Zeigt die aktuelle Netzwerkkonfiguration.

**Konfigurationsübersicht**: Zeigt eine detaillierte Konfigurationsübersicht des SCR P.

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

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

**DCD**: Zeigt die aktuelle Konfiguration der DCD-Diagnosereihen.

## (3) Ausgewählte Ansicht

Zeigt die ausgewählte Registerkarte (die Abbildung zeigt die Ansicht **Geräte**).

## (4) Modulübersicht

Zeigt die konfigurierbare Sicherheitsauswertung SCR P.

## (5) Checkliste

Zeigt notwendige Aktionen zur Erstellung der Konfiguration und für die Behebung von anstehenden Fehlern.

## (6) Eigenschaften

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

**Löschen**: Löscht das markierte Element.

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

Unter [Software: Fehlerbehebung](#) auf Seite 133 erhalten Sie Informationen zu Problemlösungen im Zusammenhang mit den Funktionen der Software.

## 8.3 Projekteinstellungen



Abbildung 39: Projekteinstellungen

Für jedes Projekt und jede Konfiguration können zusätzliche Informationen hinterlegt werden, damit die erstellte Konfiguration im Nachhinein besser identifiziert werden kann. Klicken Sie zum Eingeben dieser Informationen auf **Projekteinstellungen**.

### Konfigurationsname

Der Name der Konfiguration (z.B. innerhalb eines Projektes). Der Konfiguration ist vom Dateinamen unterschiedlich.

### Projekt

Der Projektname. Dieser ist hilfreich für die Unterscheidung zwischen unterschiedlichen Anwendungsbereichen.

### Autor

Die Person, die die Konfiguration erstellt.

### Hinweise

Ergänzende Informationen zu dieser Konfiguration oder diesem Projekt.

### Projektdatum

Das Datum, an dem das Projekt bzw. die Konfiguration erstellt wurde.



## 8.4 Registerkarte **Geräte**

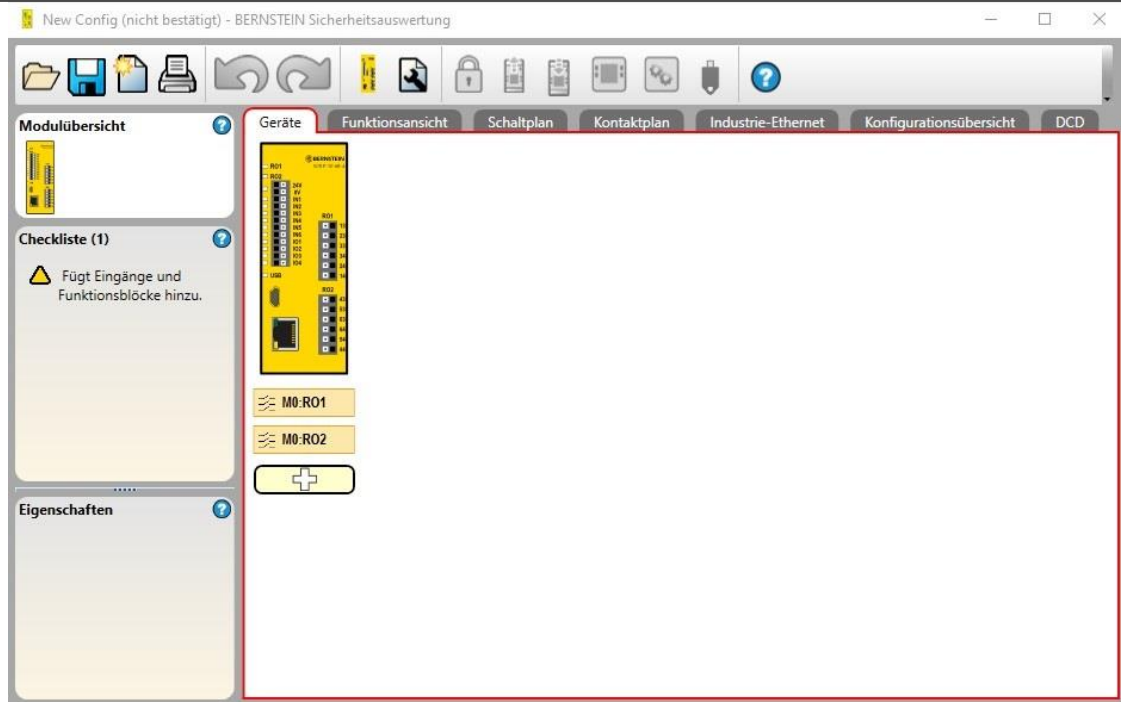


Abbildung 40: Beispiel: Registerkarte **Geräte**

Die Registerkarte **Geräte** dient zum Hinzufügen von Sicherheitseingängen und Statusausgängen.

Passen Sie das SCR P an, indem Sie entweder auf das Modul doppelklicken oder es markieren und links unter der Tabelle **Eigenschaften** auf **Bearbeiten** klicken und anschließend die geeigneten Merkmale auswählen (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.

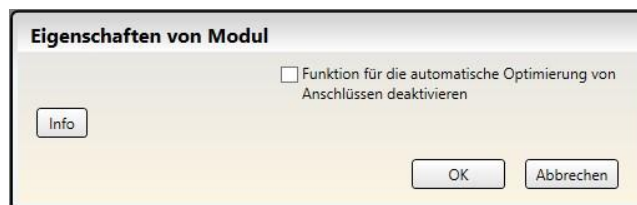


Abbildung 41: Eigenschaften des Moduls SCR P

## 8.5 Registerkarte Funktionsansicht

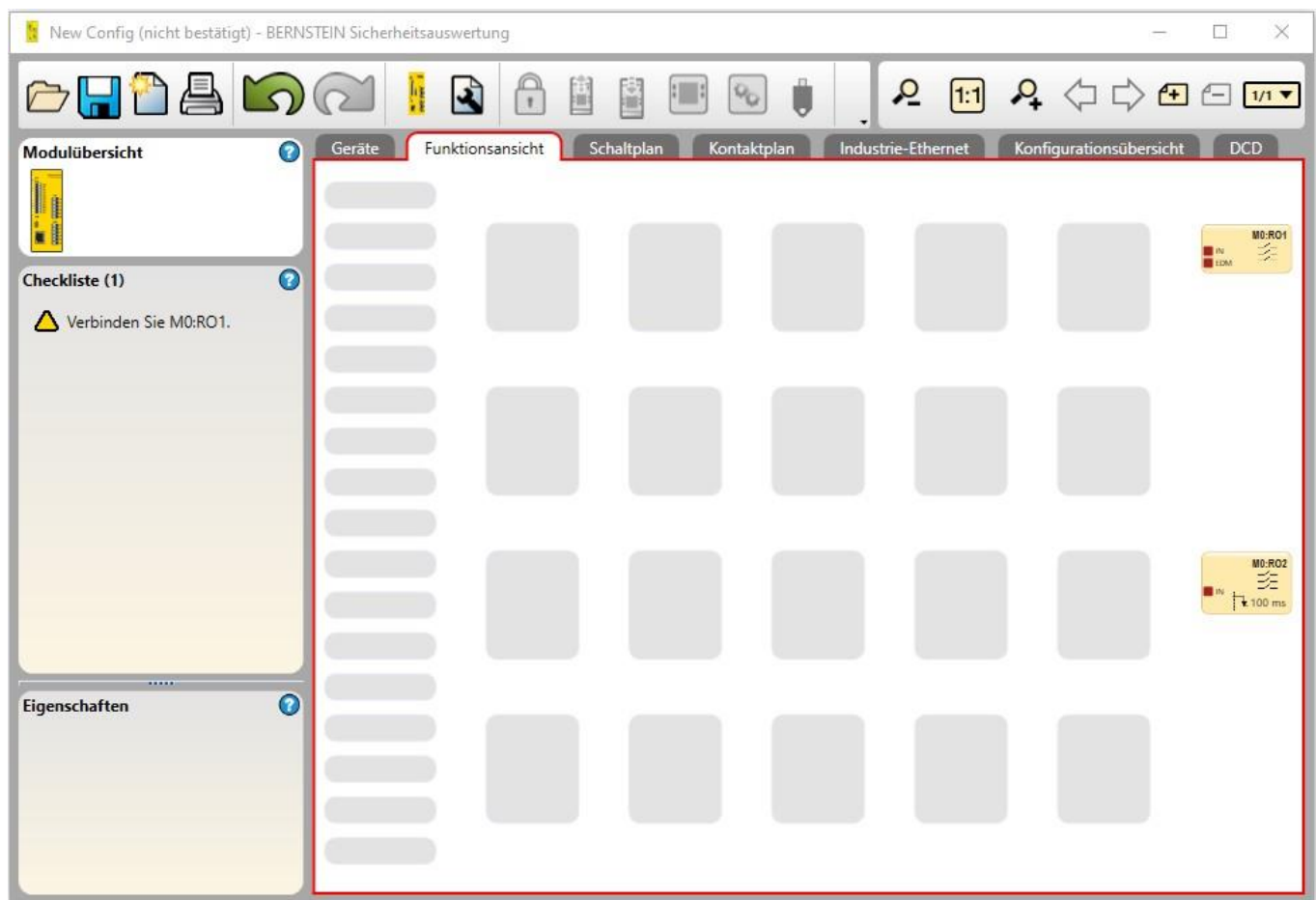


Abbildung 42: Registerkarte Funktionsansicht

Über die Registerkarte **Funktionsansicht** wird die Steuerungslogik erstellt. Die linke Spalte der Registerkarte **Funktionsansicht** wird für Sicherheitseingänge und nicht sicherheitsrelevante Eingänge verwendet, der mittlere Bereich wird für Logik- und Funktionsblöcke verwendet und die rechte Spalte ist für Sicherheitsausgänge vorbehalten. Sicherheitseingänge und nicht sicherheitsrelevante Eingänge lassen sich vom linken in den mittleren Bereich verschieben und umgekehrt. Funktions- und Logikblöcke lassen sich nur innerhalb des mittleren Bereichs verschieben. Ausgänge werden vom Programm statisch platziert und sind nicht verschiebbar. Referenzblöcke jeglicher Art können an einer beliebigen Stelle im linken und mittleren Bereich platziert werden.



**Wichtig:** Die Software zur Sicherheitsauswertung von BERNSTEIN soll dabei helfen, eine gültige Konfiguration zu erstellen. Es liegt jedoch in der Verantwortung des Benutzers, die Integrität, Sicherheit und Funktionalität der Konfiguration anhand der [Inbetriebnahmeprüfung](#) auf Seite 115.

Auf der Registerkarte **Funktionsansicht** können Sie folgende Vorgänge ausführen:



1. Die Darstellung der Steuerungslogik durch Positionsverschiebung von Eingängen, Funktionsblöcken und Logikblöcken anpassen
2. Die zuletzt ausgeführten (maximal 10) Aktionen  **rückgängig** machen und  **wiederherstellen**
3. Weitere Seiten für größere Konfigurationen anhand der Werkzeugleiste „Seitennavigation“ hinzufügen (siehe [Abbildung 43](#) auf Seite 66)
4. Die Diagrammansicht mit der Zoom-Funktion vergrößern und verkleinern oder sie automatisch an das optimale Seitenverhältnis für die aktuelle Fenstergröße anpassen (siehe [Abbildung 43](#) auf Seite 66)



Abbildung 43: Werkzeugleiste „Seitennavigation“ und „Diagrammgröße“

5. Durch die Seiten navigieren, indem Sie oben rechts in der Software im Seitennavigationsbereich auf den Links- und Rechtspfeil klicken
6. Eigenschaften aller Blöcke entweder durch Doppelklicken auf einen Block oder durch Auswahl eines Blocks und Klicken auf **Bearbeiten** unter der Tabelle **Eigenschaften** bearbeiten

7. 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 auf der Registerkarte **Geräte** hinzugefügt werden, auf der Registerkarte **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**.

## 8.5.1 Logikblöcke

Logikblöcke dienen zum Erstellen boolescher (wahr oder falsch) funktionaler Beziehungen zwischen Eingängen, Ausgängen und weiteren Logik- und Funktionsblöcken. Logikblöcke akzeptieren geeignete Sicherheitseingänge, nicht sicherheitsrelevante Eingänge oder Sicherheitsausgänge als Eingangsbedingungen. 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

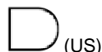
Es wird davon abgeraten, invertierte Logikkonfigurationen bei Sicherheitsanwendungen zu verwenden, bei denen eine Gefahrsituation eintreten kann.

Die Signalzustände können durch die Verwendung der Logikblöcke NOT, NAND und NOR, oder durch Markieren der Kontrollkästchen für „Ausgang invertieren“ oder „Eingangsquelle invertieren“ (sofern verfügbar), umgekehrt werden. 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



(EU)



(US)

Der Ausgangswert basiert auf der logischen AND-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



(EU)



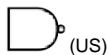
(US)

Der Ausgangswert basiert auf der logischen OR-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

## NAND

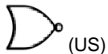


Der Ausgangswert basiert auf der Umkehr der logischen AND-Beziehung zwischen 2 bis 5 Eingängen.

Der Ausgang ist ausgeschaltet, wenn alle Eingänge eingeschaltet sind.

Eingang 1	Eingang 2	Ausgang
0	x	1
x	0	1
1	1	0

## NOR

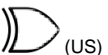


Der Ausgangswert basiert auf der Umkehr der logischen OR-Beziehung zwischen 2 bis 5 Eingängen.

Der Ausgang ist eingeschaltet, wenn alle Eingänge ausgeschaltet sind.

Eingang 1	Eingang 2	Ausgang
0	0	1
1	x	0
x	1	0

## XOR

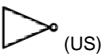


Der Ausgangswert ist eine ausschließliche OR-Beziehung zwischen 2 bis 5 Eingängen.

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)

## 8.5.2 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 substantielle Effizienzvorteile, ist benutzerfreundlicher und zeichnet sich durch höhere Funktionalität aus.

Bei den meisten Funktionsblöcken wird davon ausgegangen, dass das entsprechende Sicherheitsschaltgerät 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 vielen Komponenten sind beide Signale positiv (+ 24 V DC), wenn das Sicherheitsschaltgerät 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 Sicherheitsschaltgerät im EIN-Zustand ist. Anstatt ein Sicherheitsschaltgerät 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.

### Überbrückungsblock

Standardknoten	Zusätzliche Knoten	Anmerkungen
IN BP	-	Wenn der BP-Knoten inaktiv ist, durchläuft das Sicherheitssignal den Überbrückungsblock. Wenn der BP-Knoten aktiv ist, ist der Ausgang des Blocks unabhängig vom Status des IN-Knotens eingeschaltet (wenn das Kontrollkästchen <b>Ausgang schaltet sich aus, wenn beide Eingänge (IN und BP) eingeschaltet sind</b> deaktiviert ist). Der Ausgang des zugehörigen Überbrückungsblocks schaltet sich aus, wenn der Überbrückungs-Zeitgeber abläuft.

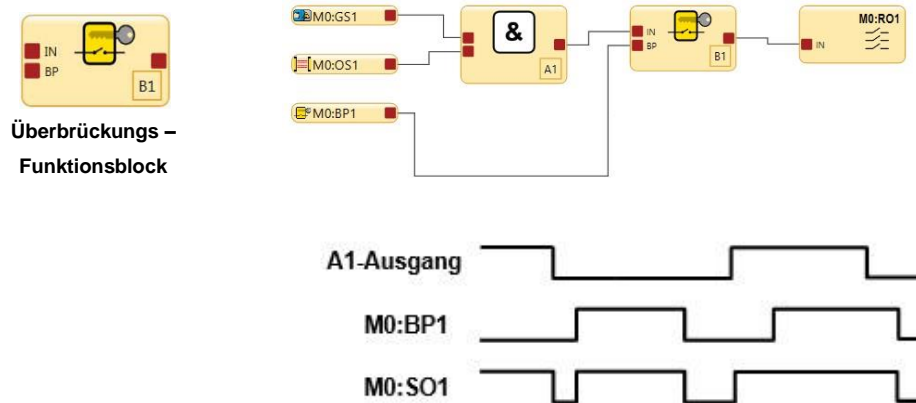



Abbildung 44: Zeitdiagramm: Überbrückungsblock

**Zeitlimit für Überbrückung** – Um den Zeitraum zu begrenzen, in dem die Überbrückung der Sicherheitsschaltgeräte aktiv sein soll, muss ein Zeitlimit für die Überbrückungsfunktion festgelegt werden. Das Zeitlimit kann von 1 Sekunde (Werkseinstellung) bis 12 Stunden eingestellt werden und lässt sich nicht deaktivieren. Es kann nur ein Zeitlimit festgelegt werden, dass die Überbrückung aller Sicherheitsvorrichtungen betrifft. Nach Ablauf des Zeitlimits wird die Überbrückung gestoppt und die Steuerung der Sicherheitsausgänge wieder an die entsprechenden Sicherheitseingänge zurückgegeben.

**Überbrückung für Zweihandsteuerung** – Die Sicherheitsauswertung gibt ein Stoppsignal aus, wenn die Sicherheitseingänge einer Zweihandsteuerung überbrückt werden und gleichzeitig einer der Eingänge betätigt wird. Hierdurch wird sichergestellt, dass der Bediener nicht irrtümlich annimmt, dass die Zweihandsteuerung funktional ist, ohne zu wissen, dass die Zweihandsteuerung überbrückt wurde und ihre Schutzfunktion nicht mehr erfüllt.

### Verriegeln/Kennzeichnen

 Beachten Sie gemäß ISO 14118, ISO 12100, OSHA 29CFR 1910.147, ANSI 2244.1 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 IEC/EN60204-1 oder ANSI NFPA79) 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.

## Verzögerungsblock

Mit dem Verzögerungsblock können Benutzer eine Ein- oder Ausschaltverzögerung von bis zu 5 Minuten (in 1-ms-Schritten) konfigurieren.

Standardknoten	Zusätzliche Knoten	Anmerkungen
IN	-	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 Knoten zum Abbruch einer Zeitverzögerung ist ein konfigurierbarer Knoten, der nur für eine Ausschaltverzögerung ausgewählt werden kann.

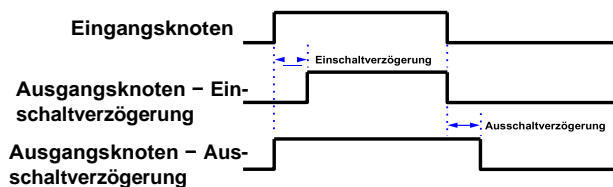


Abbildung 45: Zeitdiagramm für Verzögerungsblock



### 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. OR-Funktionen) ändern. Es liegt in der Verantwortung des Anwenders, die korrekte Ansprechzeit zu ermitteln, zu überprüfen und einzurechnen.



Abbildung 46: Verzögerungsblock-Eigenschaften

Im Fenster **Verzögerungsblock-Eigenschaften** kann der Benutzer Folgendes konfigurieren:

#### **Name**

Die Bezeichnung des Eingangs.

#### **Verzögerung des Sicherheitsausgangs**

- Keine
- Ausschaltverzögerung
- Einschaltverzögerung

#### **Ausgangsverzögerungszeit**

Verfügbar, wenn als Einstellung für die Verzögerung des Sicherheitsausgangs entweder Ausschaltverzögerung oder Einschaltverzögerung ausgewählt wurde.

Verzögerungszeit: 1 ms bis 5 min, in 1-ms-Schritten. Die Werkseinstellung beträgt 100 ms.

#### **Abbruchtyp**

Verfügbar, wenn als Einstellung für die Verzögerung des Sicherheitsausgangs die Ausschaltverzögerung gewählt wurde.

- Kein Abbruch
- Steuereingang
- Abbruchverzögerungsknoten

#### **Endlogik**

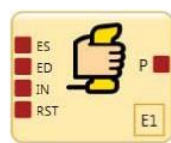
Verfügbar, wenn als Einstellung für den Abbruchtyp Abbruchverzögerungsknoten gewählt wurde.

- Ausgang eingeschaltet lassen
- Ausgang ausschalten



## Zustimmtaster-Block

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

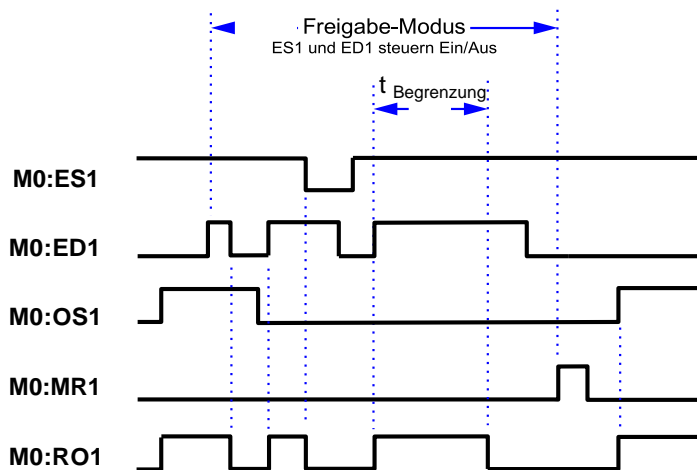
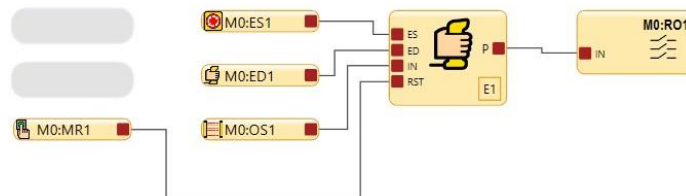
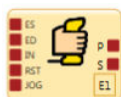
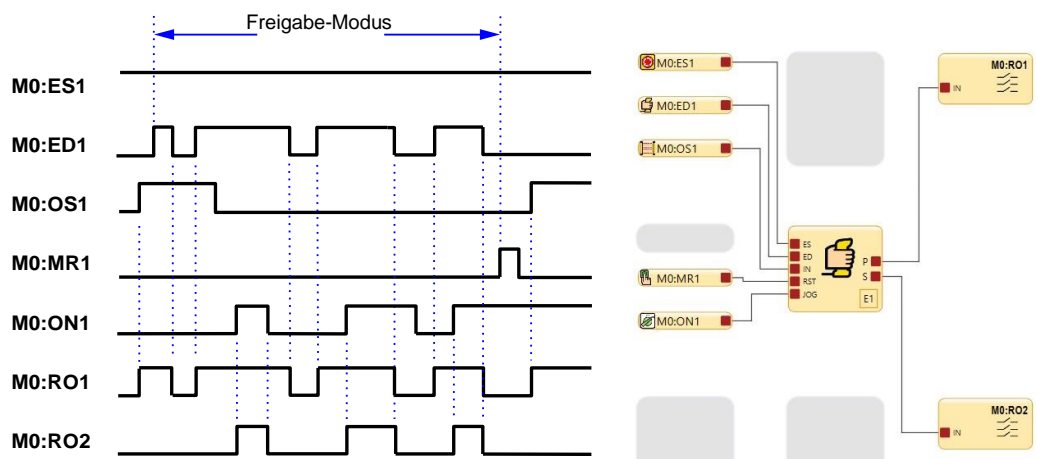


Abbildung 47: Zeitdiagramm: Zustimmtaster, einfache Konfiguration



Primärer Zustimmtaster & Sekundäre Ausgangssteuerung



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.

Abbildung 48: Zeitdiagramm: Zustimmtaster

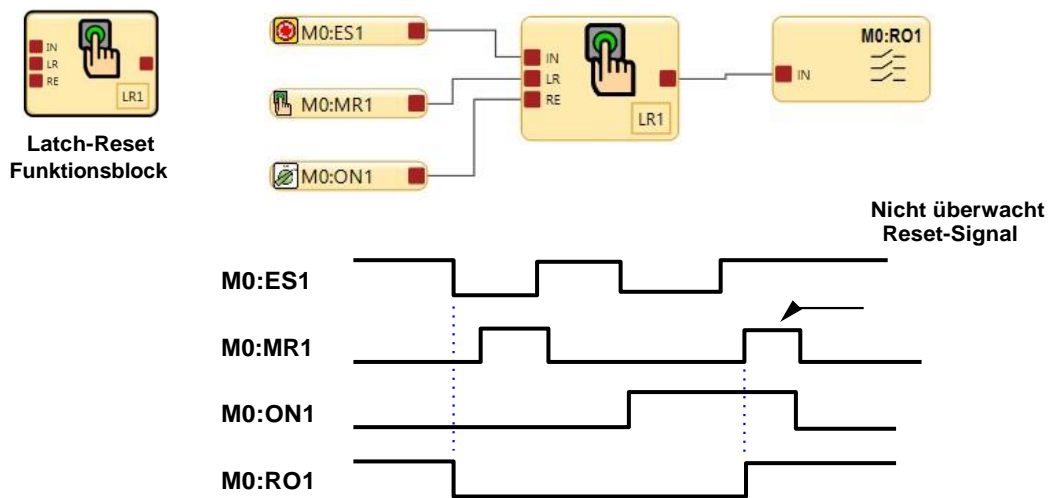
**Zum Beenden des Freigabe-Modus** muss sich der Zustimmtaster im Aus-Zustand befinden, und ein Zustimmtaster-Block-Reset muss durchgeführt werden.

Das **Zeitlimit für den Zustimmungstaster** kann zwischen 1 Sekunde (Werkseinstellung) und 30 Minuten eingestellt werden und lässt sich nicht abschalten. Wenn das Zeitlimit abgelaufen ist, schalten die zugehörigen Sicherheitsausgänge ab. Um einen neuen Freigabe-Modus-Zyklus mit dem ursprünglichen Zeitlimitwert für den manuellen Reset zu starten, muss der Zustimmungstaster von Ein auf Aus und wieder zurück auf Ein geschaltet werden.

Alle mit den Sicherheitsausgängen verbundenen Einschalt- und Ausschaltverzögerungszeiten, die durch die Zustimmungstasterfunktion gesteuert werden, werden während des Freigabe-Modus berücksichtigt.

## Latch-Reset-Block

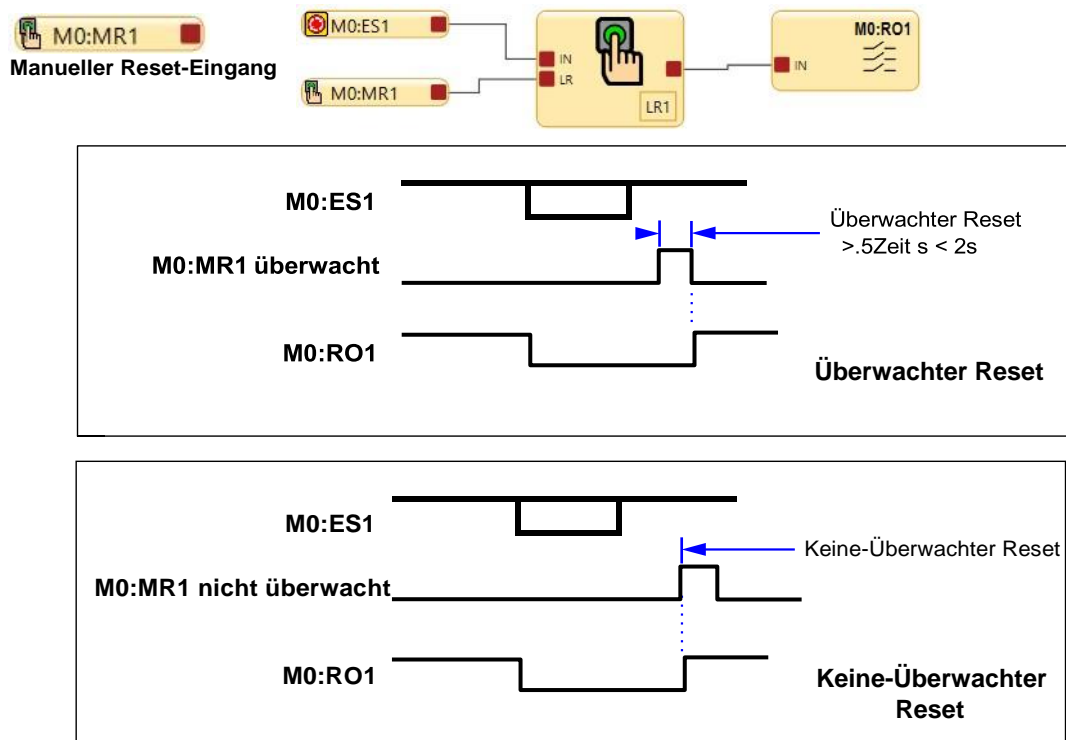
Standardknoten	Zusätzliche Knoten	Anmerkungen
IN LR	RE	Der RE-Knoten (Reset aktivieren) kann zum Aktivieren oder Deaktivieren der Latch-Reset-Funktion verwendet werden. Befinden sich alle mit dem IN-Knoten verbundenen Eingangsgeräte im Ein-Zustand und ist das RE-Eingangssignal im Ein-Zustand, kann der LR-Funktionsblock manuell zurückgesetzt werden, damit sich sein Ausgang einschaltet. Siehe <a href="#">Abbildung 48</a> auf Seite 73; das Referenzsignal RO2 ist dabei mit dem RE-Knoten verbunden.



Der Latch-Reset-Funktionsblock LR1 schaltet seinen Ausgang und den Sicherheitsausgang RO1 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 RO2-Referenzsignal im Ein-Zustand befindet, und für die Durchführung des Reset wird MR1 verwendet.

Abbildung 49: Zeitdiagramm: Latch-Reset-Block



Das Eingangsgerät für manuellen Reset kann für eine oder zwei Arten von Reset-Signalen konfiguriert werden: Überwacht und Nicht überwacht

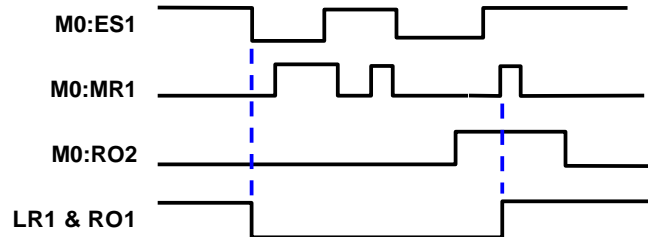
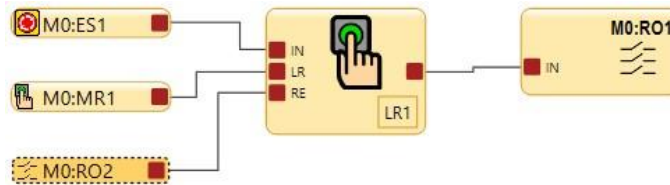
Abbildung 50: Zeitdiagramm: Latch-Reset-Block, überwachter/nicht überwachter Reset



## 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 RO2 eingeschaltet ist, ist der Status des Referenzsignals RO2 Ein. Bei dem oben abgebildeten Funktionsblock ist das Referenzsignal RO2 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 RO2 eingeschaltet ist.

Zur Verwendung der referenzierten Sicherheitsausgänge siehe [Referenzsignale](#) auf Seite 114.

Abbildung 51: Zeitdiagramm: Latch-Reset-Block und referenzierter Sicherheitsausgang



## 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 Sicherheitsfunktion verwendet werden.

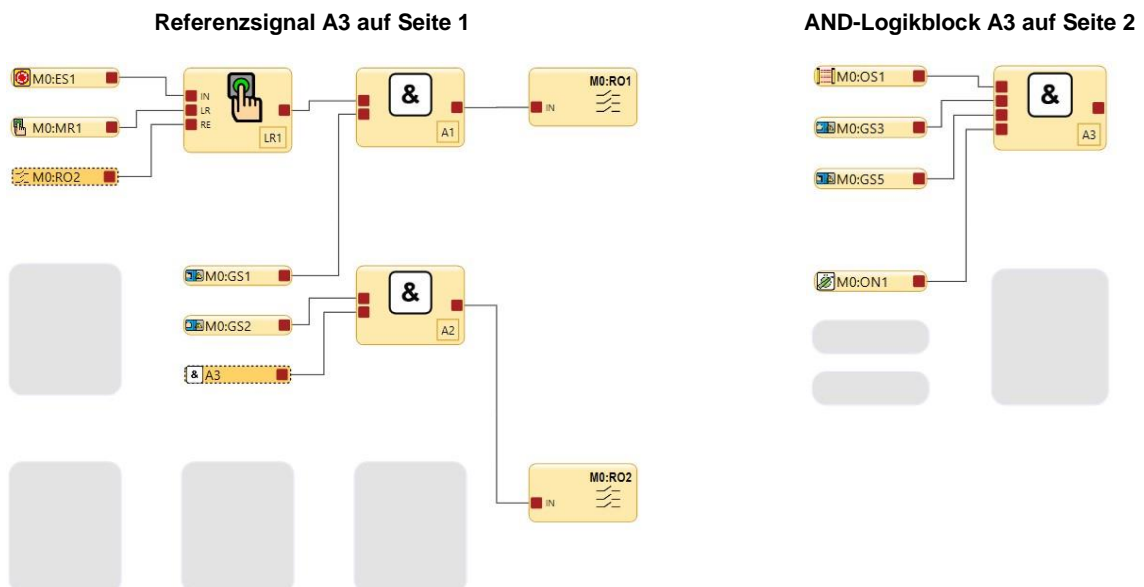
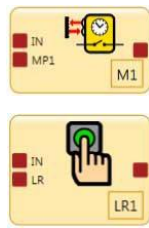
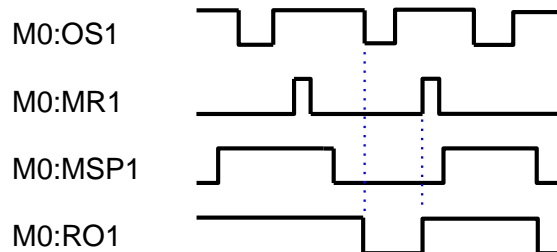
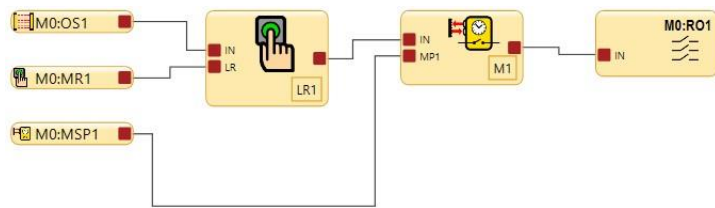


Abbildung 52: Latch-Reset und referenzierter Sicherheitsausgang und AND-Block



**Latch-Reset  
Muting-Funktion**



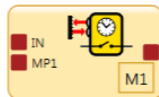
Wenn OS1 für eine Schutzeinrichtung in einem gültigen Muting-Zyklus in einen Stoppzustand übergeht, wird der Latch-Reset-Funktionsblock verriegelt, und ein Reset-Signal ist erforderlich, damit RO1 nach dem Ende des Mutings eingeschaltet bleibt.

Wenn OS1 in einem gültigen Muting-Zyklus in den Stoppzustand schaltet und kein Reset-Signal erfasst wird, schaltet sich RO1 nach dem Ende des Mutings aus.

Abbildung 53: Zeitdiagramm: Latch-Reset-Block und Muting-Block

## Muting-Block

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.

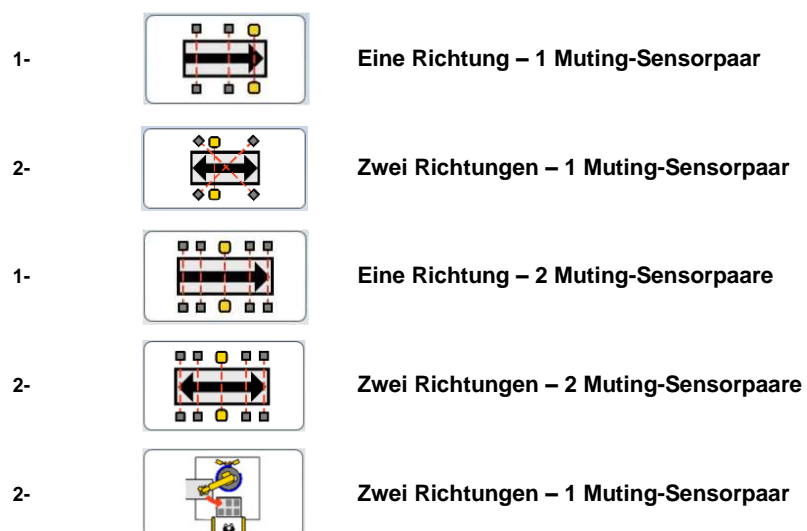
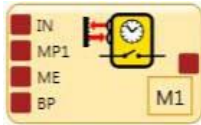


Abbildung 54: Muting-Block: Funktionsarten



- 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 Schutz-einrichtung im Stoppzustand befindet.

Die normale Überbrückung dient der vorübergehenden Umgehung der Schutz-einrichtung, um den Ausgang des Funktionsblocks einzuschalten oder damit dieser eingeschaltet bleibt.

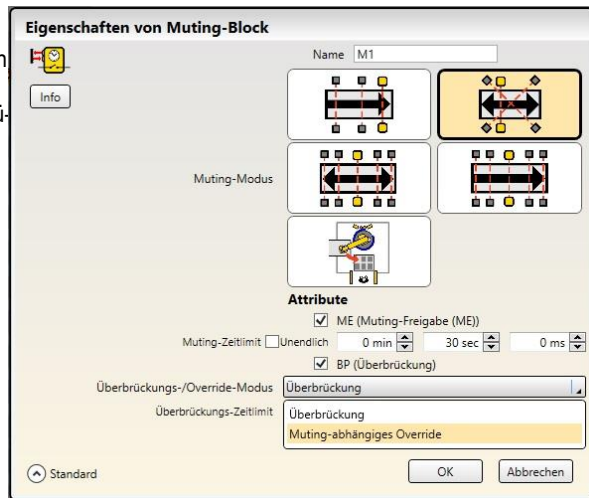
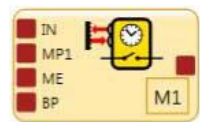


Abbildung 55: Muting-Block: Optionen für den Überbrückungs-/Override-Modus



Muting-abhängiges

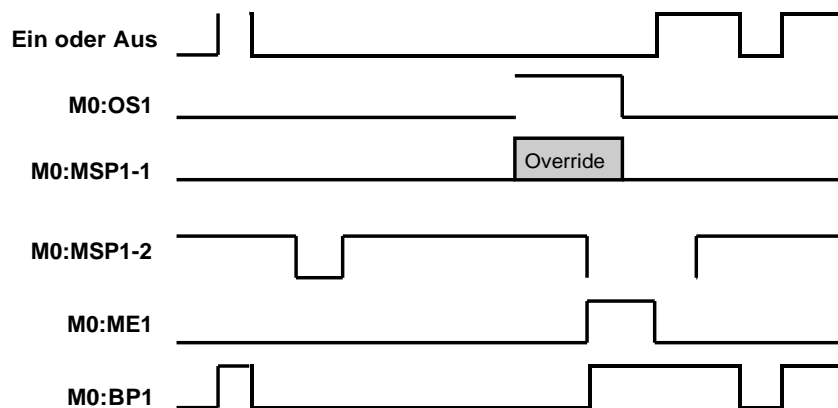
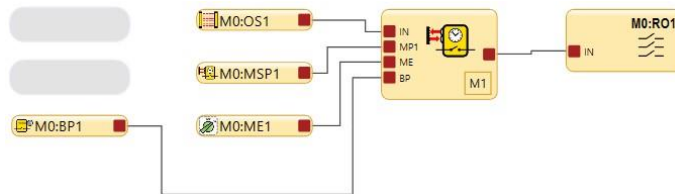


Abbildung 56: Muting-abhängiges Override

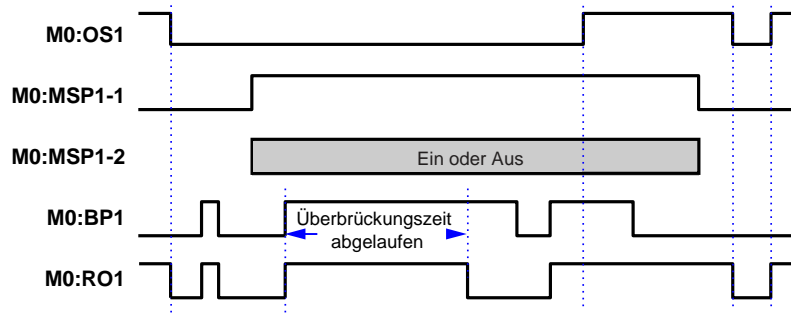
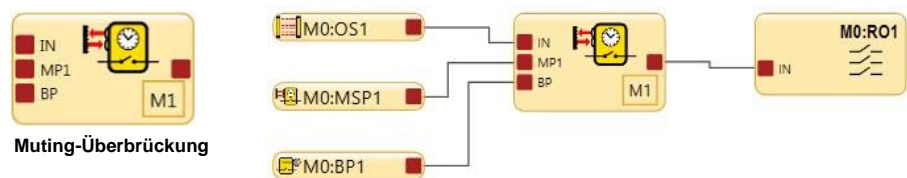
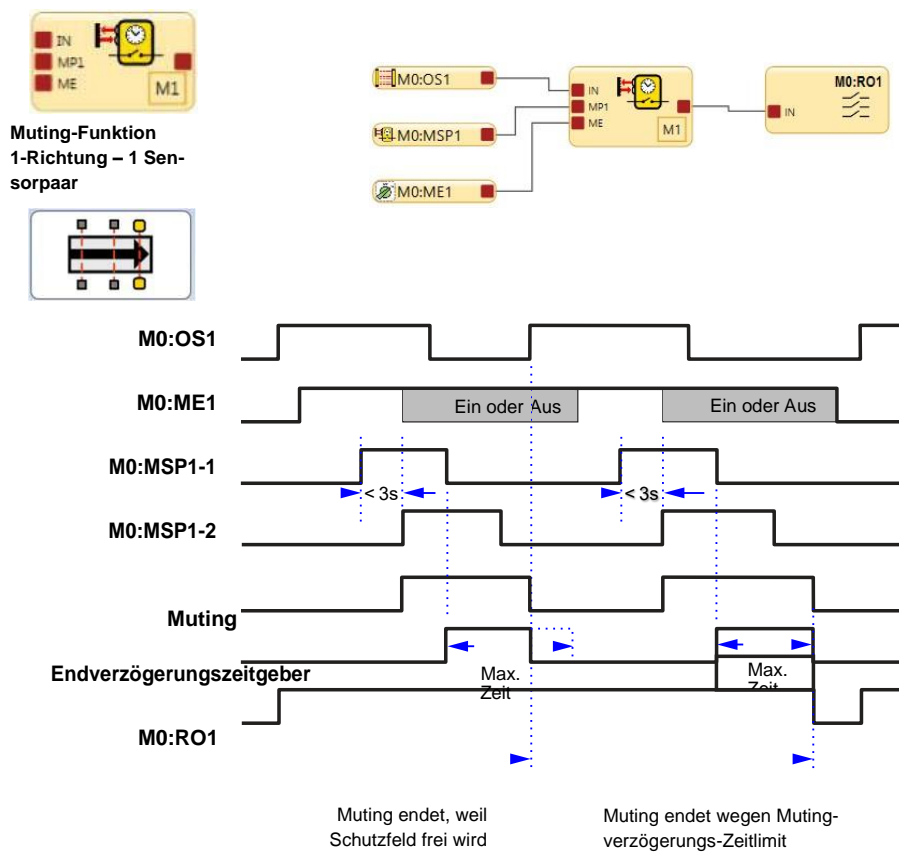


Abbildung 57: Muting-Überbrückung



**Hinweis:** M0:OS1 muss blockiert werden, bevor entweder MSP1-1 oder MSP1-2 frei wird.

Abbildung 58: Zeitdiagramm: Unidirektionaler Muting-Block, ein Muting-Sensorpaar



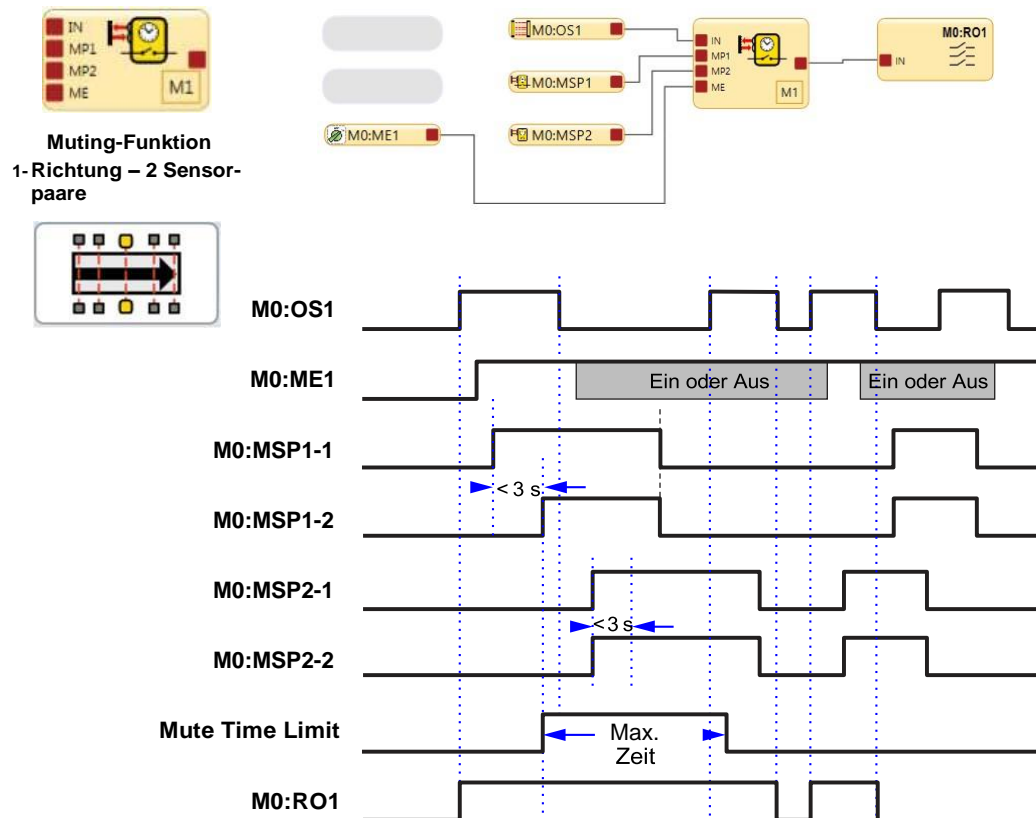


Abbildung 59: Zeitdiagramm: Unidirektionaler Muting-Block, zwei Muting-Sensorpaare

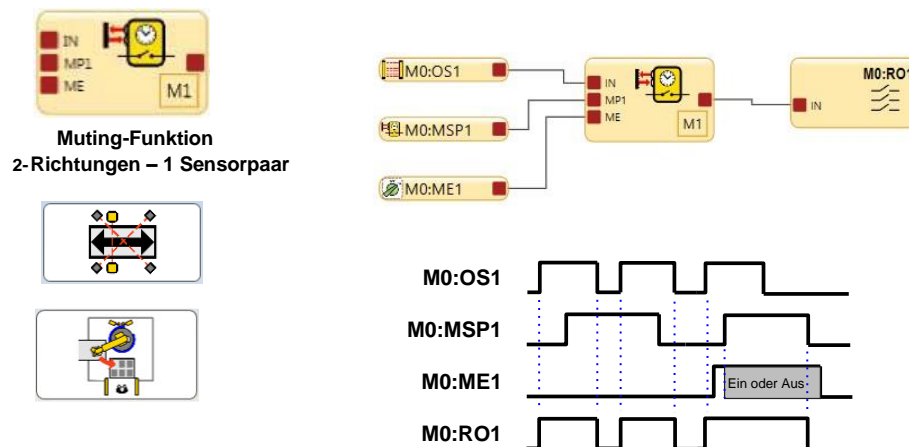


Abbildung 60: Zeitdiagramm: Bidirektionaler Muting-Block, ein Muting-Sensorpaar

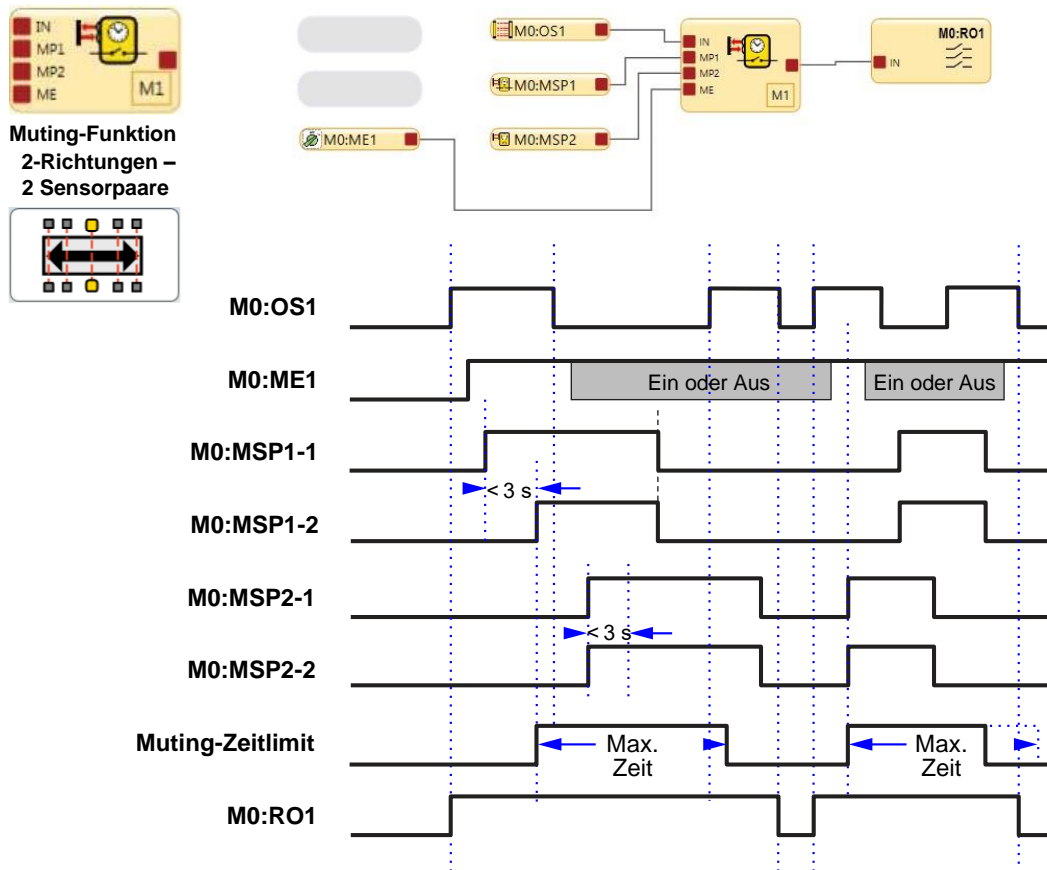


Abbildung 61: Zeitdiagramm: Bidirektionaler Muting-Block, zwei Muting-Sensorpaare

## WICHTIG

### Not-Halt-Vorrang bei Verwendung der Muting-Funktion

#### Falsche Not-Halt-Steuerung

##### NICHT EMPFOHLEN

Die Konfiguration oben rechts zeigt OS1 und den Not-Halt-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-Halt-Schalter betätigt (in den Stoppzustand geschaltet) wird, schaltet sich RO1 nicht aus. Dies führt zu einem Verlust der Sicherheitsfunktion und kann eine potenzielle Gefahrensituation bewirken.

#### Richtige Not-Halt-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 RO1.

Wenn ein aktiver Muting-Zyklus läuft und der Not-Halt-Schalter betätigt (in den Stoppzustand geschaltet) wird, schaltet sich RO1 aus.

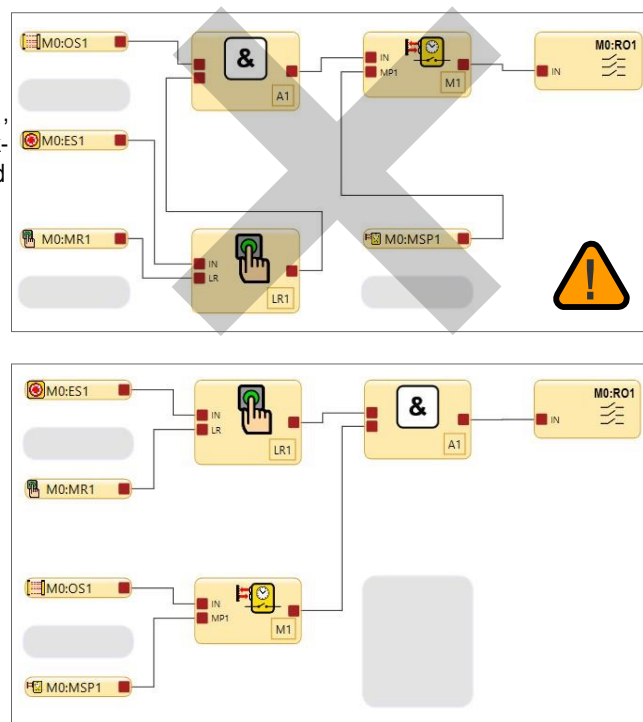


Abbildung 62: Not-Aus-Schalter und Muting-Funktion

Not-Halt-Schalter, Seilzugschalter, Zustimmungstaster, 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-Einrichtungen einbeziehen,
3. die richtige Montage und Installation solcher Einrichtungen 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 Sicherheitsauswertung kann redundante Signale, die das Muting initiieren, überwachen und darauf reagieren. Das Muting hebt dann die Schutzfunktion auf, indem der Zustand des Eingangsgeräts, dem die Muting-Funktion zugewiesen wurde, ignoriert wird. Dadurch wird z. B. einem Objekt oder einer Person ermöglicht, den definierten Bereich eines Sicherheits-Lichtvorhangs zu passieren, ohne einen Stoppbefehl zu erzeugen. Dies ist nicht mit Blanking zu verwechseln, bei der einer oder mehrere Strahlen in einem Sicherheits-Lichtvorhang deaktiviert werden, was zu einer größeren Auflösung führt.

Das Muting kann von einer Reihe externer Einrichtungen ausgelöst werden. Diese Funktion bietet eine Reihe von Optionen, damit das System auf die Anforderungen einer speziellen Anwendung zugeschnitten werden kann.

Ein Muting-Sensorpaar muss gleichzeitig ausgelöst werden (im Abstand von maximal 3 Sekunden). Dadurch verringert sich die Wahrscheinlichkeit eines Fehlers gemeinsamer Ursache oder einer absichtlichen Umgehung. Direktionales Muting, bei dem das Sensorpaar 1 zuerst gesperrt werden muss, kann ebenfalls die Möglichkeit einer Umgehung reduzieren.

Für jeden Muting-Vorgang sind mindestens zwei Muting-Sensoren 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 Sicherheitseingängen zugeordnet werden, damit ihre zugewiesenen Sicherheitsausgänge eingeschaltet bleiben können, um den Arbeitsgang 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.**

## 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 die Auswertung ein Muting zu. Öffnen des Eingangs während eines Mutings hat keine Auswirkung.

Typische Anwendungen für die Muting-Aktivierung sind unter anderem:

- Um der Maschinensteuerung 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.

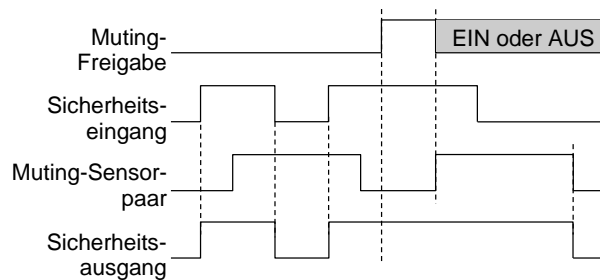


Abbildung 63: Zeitdiagramm: ein Muting-Sensorpaar mit Muting-Freigabe

### Reset-Funktion für Gleichzeitigkeitsüberwachung

Der Eingang für die Muting-Aktivierung kann auch verwendet werden, um den Gleichzeitigkeitsüberwachung der Muting- Sensoreingänge zurückzusetzen. Wenn ein Eingang länger als 3 Sekunden aktiv ist, bevor der zweite Eingang aktiv wird, verhindert der Gleichzeitigkeitsüberwachung, dass ein Muting-Zyklus eintreten kann. Das kann durch das normale Anhalten eines Montagebands bedingt sein, wodurch eine Muting-Vorrichtung blockiert und die Zeit der Gleichzeitigkeitsüberwachung 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 die Gleichzeitigkeitsüberwachung zurückgesetzt, und wenn der zweite Muting-Eingang innerhalb von 3 Sekunden aktiv wird, beginnt ein normaler Muting-Zyklus. Die Funktion kann die Überwachung 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 Sicherheitseinrichtung, 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 Sicherheitseinrichtung 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 Sicherheitseinrichtung (z. B. ein Lichtvorhang) gemutet ist. Die Sicherheitsauswertung gibt über den Muting-Statusausgang ein Signal aus, welches besagt, dass die Sicherheitsfunktion vorübergehend aufgehoben ist.



#### Wichtig: Anzeige für Muting-Status

Eine Anzeige für den gemuteten Status der Sicherheitseinrichtung muss eingerichtet werden und vom Standort der gemuteten Sicherheitseinrichtung 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 Fehlers gemeinsamer Ursache, 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 unendliche 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. Mehrstrahlssysteme bei reinen Arbeitszellen-Ausgangs- anwendungen 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 Sicherheitsschaltgerät (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 Spannungsversorgung der Sicherheitsauswertung eingeschaltet 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 die Sicherheitsauswertung 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 Risiko- beurteilung 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 das Sicherheitsschaltgerät 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-Sensorpaar ausgelöst. Die Schal- tungs- optionen für die Muting-Vorrichtung sind konfigurierbar und werden im Fenster **Eigenschaften** für das Muting-Sen- sor- paar angezeigt. Ein ordnungsgemäßes Muting-Signal kommt zustande, wenn beide Kanäle der Muting-Vorrichtung in den Muting-Aktiv-Zustand wechseln, während sich die gemutete Sicherheitseinrichtung im Ein-Zustand befindet.

Die Sicherheitsauswertung überwacht die Muting-Einrichtungen, 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-Einrichtungen verwendet werden, unter anderem: opto- elektronische Sensoren, induktive Näherungssensoren, Grenzscharter, zwangsgeführte Sicherheitsschalter und Fühler- 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 Schutzfunk- tion auf allen Seiten aufgehoben. Es darf für Personen nicht möglich sein, unbemerkt und ohne Ausgabe eines Stopp- befehls an die Maschinensteuerung in das Schutzfeld einzudringen. Diese zusätzliche Sicherheitseinrichtung wird norma- lerweise durch Zusatzvorrichtungen bereitgestellt, die während des Mutings der primären Sicherheitseinrichtung aktiv bleiben. Daher sind Spiegel für Anwendungen mit Muting gewöhnlich nicht zulässig.

## Mehrere Sicherheitseinrichtungen mit Anwesenheitserkennung

Muting von mehreren Sicherheitsvorrichtungen mit Anwesenheitserkennung (PSSDs) oder eines PSSD mit mehreren Er- fassungsbereichen 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 83) an mehreren Erfas- sungsbereichen ein Muting durchgeführt wird, besteht die Möglichkeit, dass Personen durch einen dem Muting unterlie- genden 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 Mu- ting-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 Sicherheitseinrichtungen.

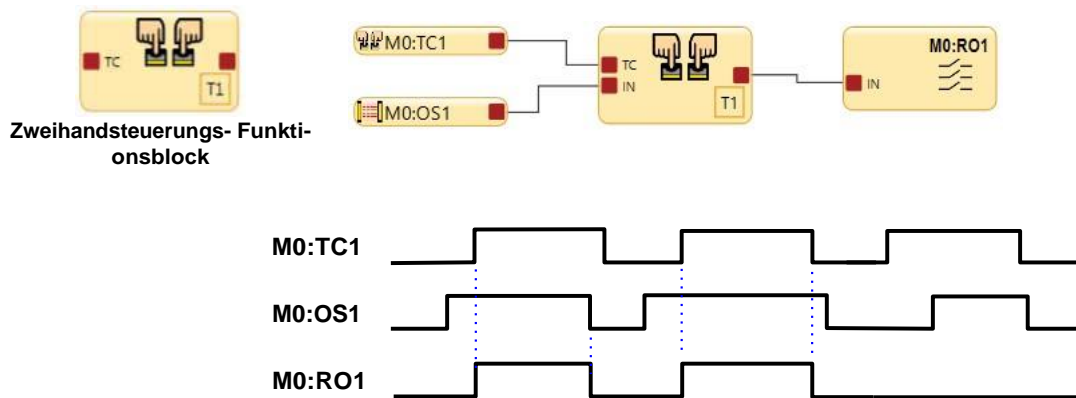


### WARNUNG: Sicherung mehrerer Bereiche

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 Sicherheitseinrichtung erfasst wird, die einen Stoppbefehl an die Maschine schickt.

## Zweihandsteuerungsblock

Standardknoten	Zusätzliche Knoten	Anmerkungen
TC (bis zu 4 TC-Knoten)	IN MP1 ME	<p>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 Zweihandsteuerungsblock ist nicht möglich.</p> <p>Mit dem IN-Knoten lassen sich Eingangsgeräte verbinden, die erst eingeschaltet werden müssen, bevor die Zweihandsteuerung die Ausgänge einschalten kann.</p>



Entweder der TC1-Eingang oder der OS1-Eingang hat die Ausschalthoheit. OS1 muss im Ein-Zustand sein, bevor TC1 den Ausgang von T1 und RO1 einschalten kann.

Abbildung 64: Zeitdiagramm: Zweihandsteuerungsblock

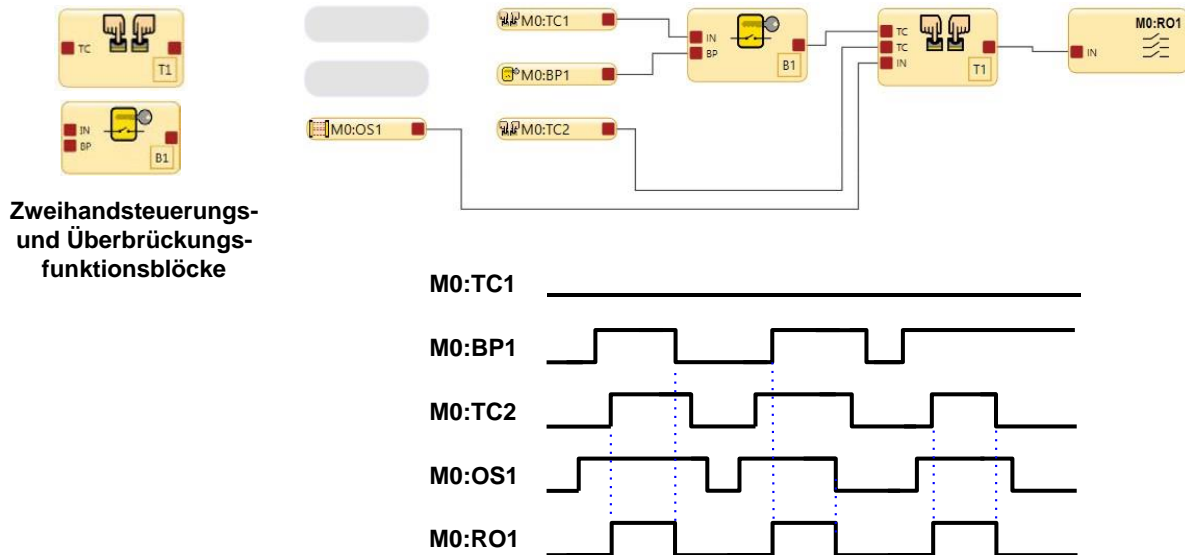


Abbildung 65: Zeitdiagramm: Zweihandsteuerungsblock und Überbrückungsblöcke

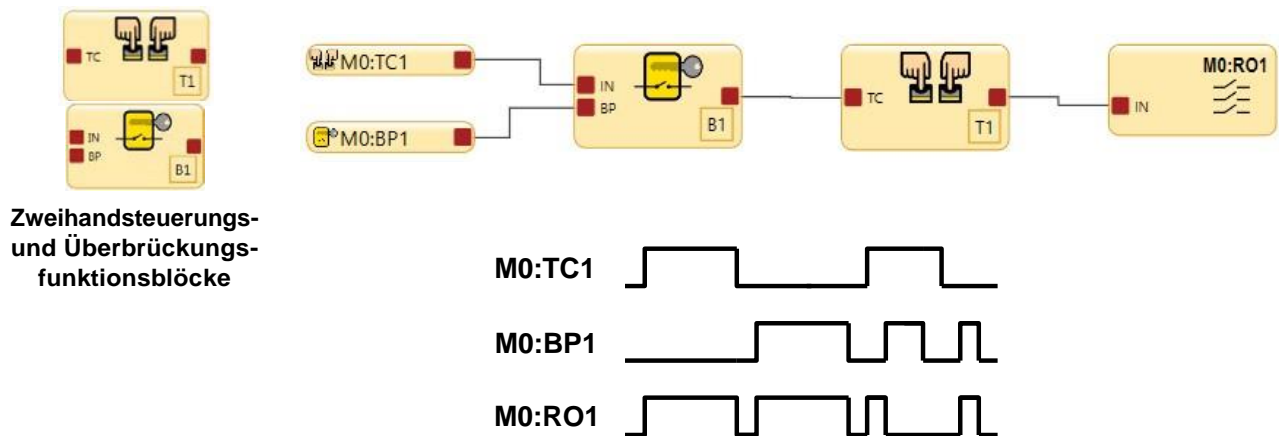
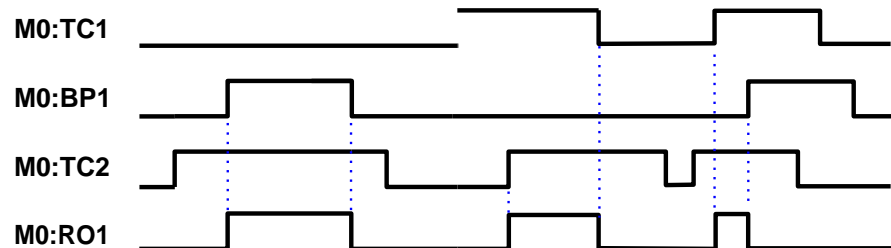
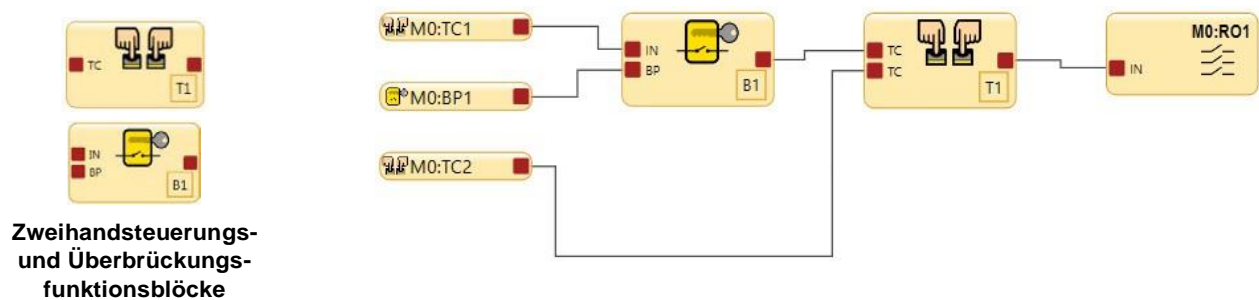


Abbildung 66: Zeitdiagramm: Zweihandsteuerungsblock und Überbrückungsblöcke mit 1 Eingang für Zweihandsteuerung





Die Überbrückungsfunktion kann mit den TC2-Bedienelementen verwendet werden, um den Sicherheitsausgang einzuschalten.

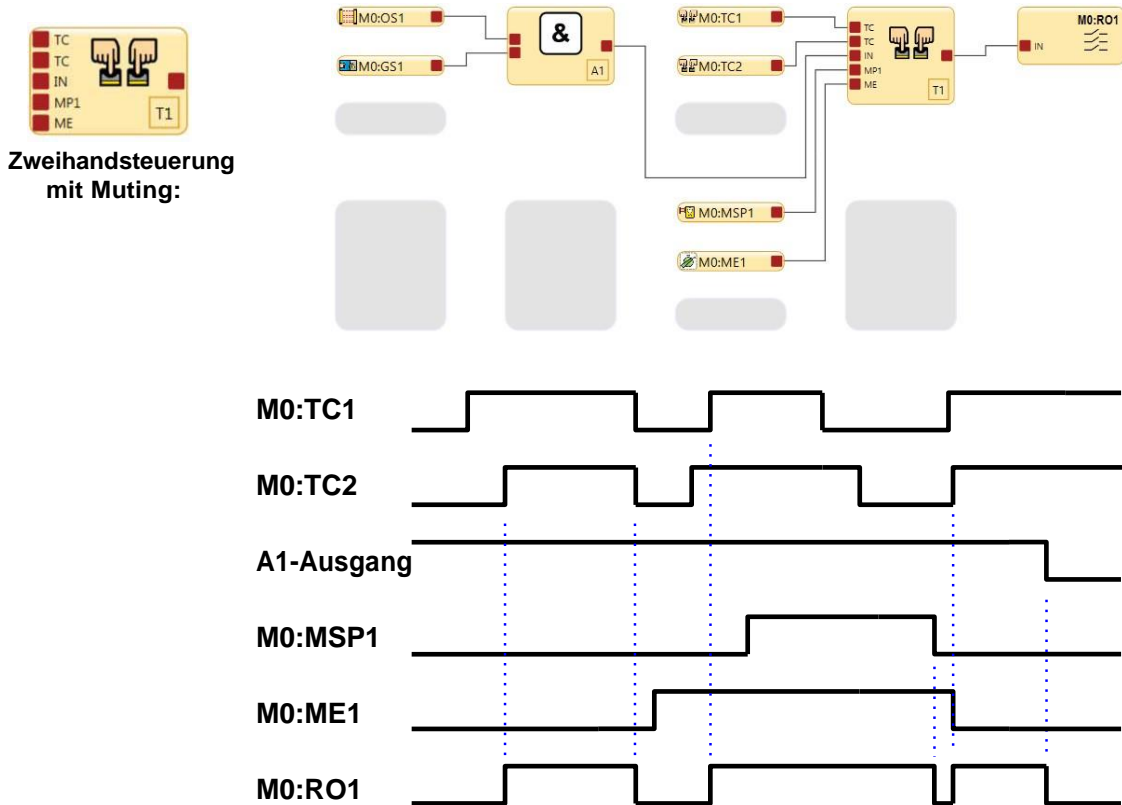
Wenn die TC1-Bedienelemente nicht überbrückt werden, müssen sie zusammen mit den TC2-Bedienelementen verwendet werden, um den Sicherheitsausgang einzuschalten. Wenn die TC1-Bedienelemente und der Überbrückungsschalter beide im Ein-Zustand sind, können T1 und RO1 nicht eingeschaltet werden oder schalten sich aus.

Abbildung 67: Zeitdiagramm: Zweihandsteuerungsblock und Überbrückungsblöcke mit 2 Eingängen für Zweihandsteuerung



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 Stationsfelder der Zweihandsteuerung, deren Kontrollkästchen aktiviert sind, werden gemutet.

Abbildung 68: Muting-Optionen für Zweihandsteuerungen



Die Bedienelemente C1 und TC2 können einen Zweihandzyklus initiieren, wenn die Muting-Freigabe ME1 nicht aktiv ist. ME1 muss aktiv sein, damit die MSP1-Muting-Sensoren SO eingeschaltet lassen, nachdem die TC1- und TC2-Bedienelemente in den Stoppzustand geschaltet haben.

Abbildung 69: Zeitablauf-Diagramm: Zweihandsteuerungsblock mit Muting

**Schutz der Zweihandsteuerung gegen Aktivierung bei Anlauf.** Die Logik der Zweihandsteuerung der Sicherheitsauswertung lässt nicht zu, dass der zugewiesene Sicherheitsausgang beim Anlegen der Betriebsspannung einschaltet, solange sich die Bedienelemente der Zweihandsteuerung im Ein-Zustand befinden. Die Bedienelemente der Zweihandsteuerung müssen in den Aus-Zustand und wieder in den Ein-Zustand wechseln, bevor der Sicherheitsausgang einschalten kann. Sicherheitsausgänge, die einer Zweihandsteuerungsvorrichtung zugeordnet sind, haben keine Option für manuellen Reset.

## 8.6 Registerkarte **Schaltplan**

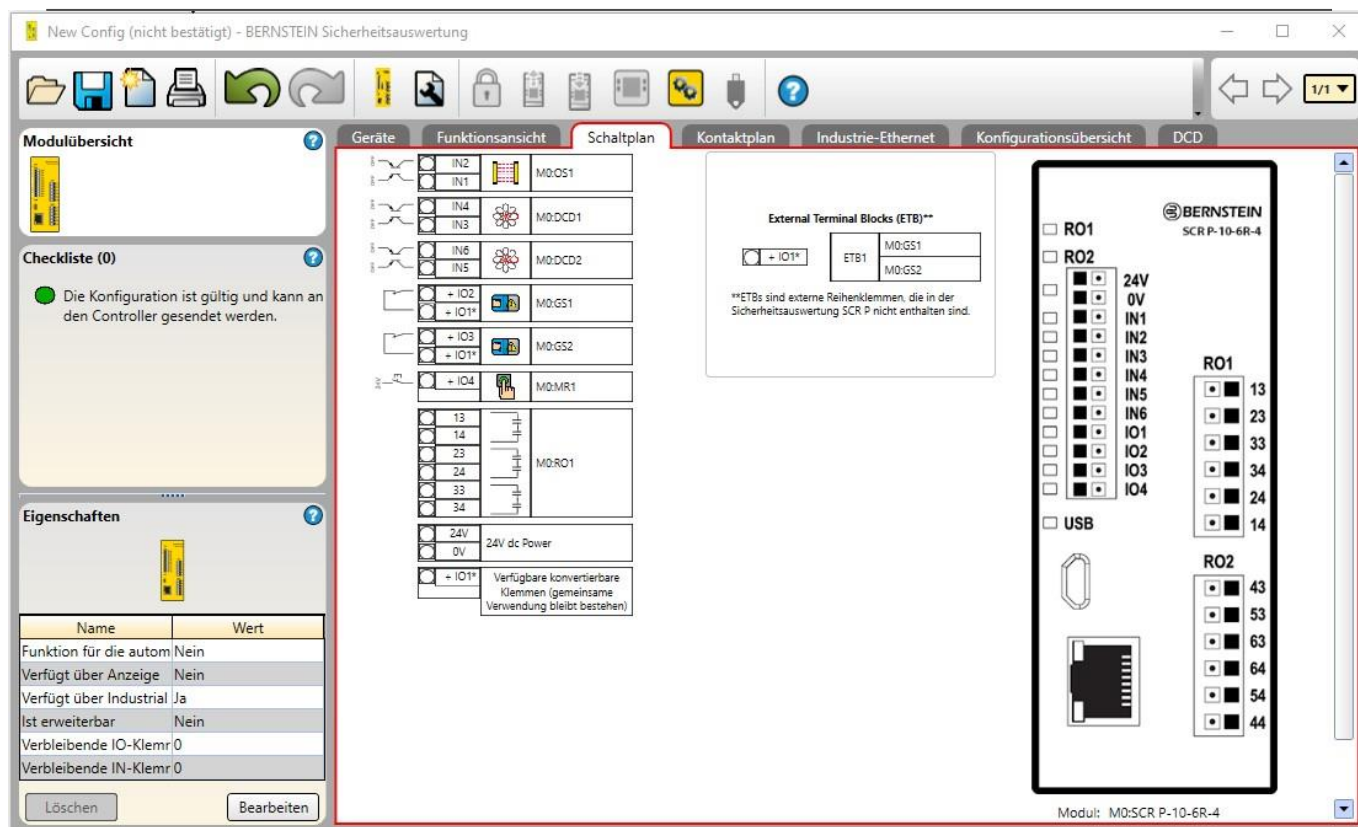


Abbildung 70: Registerkarte **Schaltplan**: SCR P mit externen Klemmenblöcken

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.

## 8.7 Registerkarte **Kontaktplan**

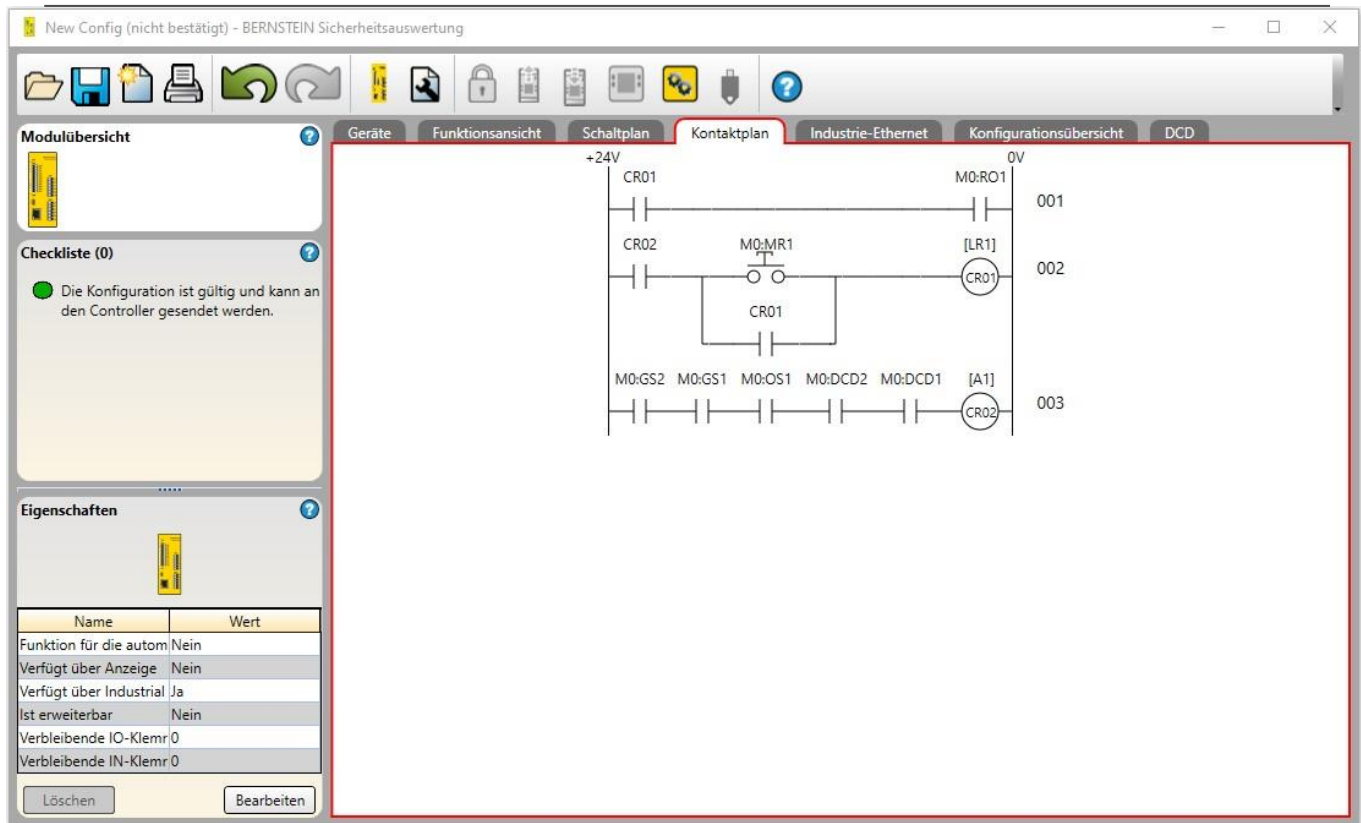


Abbildung 71: Registerkarte **Kontaktplan**

Die Ansicht **Kontaktplan** zeigt eine vereinfachte Abbildung der Relais-Logik der Konfiguration

## 8.8 Registerkarte DCD

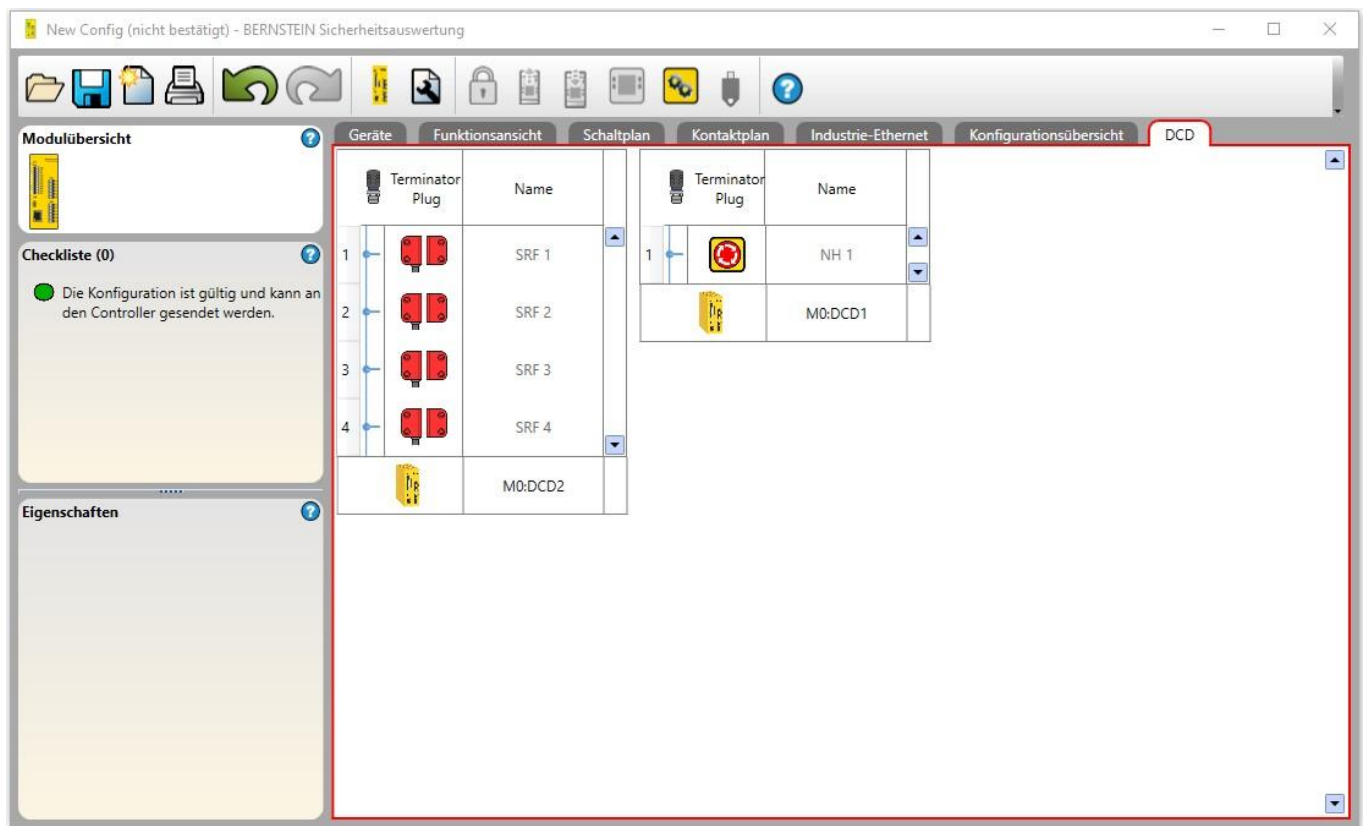


Abbildung 72: Registerkarte DCD

Das DCD-Register zeigt die Anordnung und Namen der angeschlossenen DCD-Geräte jeder DCD-Reihe.

Im "Live"-Modus zeigt das DCD-Register aktuelle Informationen über das angeschlossene Gerät (Aktualisierung ca. jede Sekunde). Im folgenden Beispiel ist ein Türsensor nicht betätigt, wie die rote Farbe in der Spalte "Status" zeigt. Zusätzlich ist der zugehörige Betätiger in der Spalte "Betätiger" weiß dargestellt.

New Config (bestätigt) - Sicherheitskontroller BERNSTEIN

Geräte Funktionsansicht Schaltplan Kontaktplan Industrie-Ethernet Konfigurationsübersicht Livemodus DCD

**Modulübersicht**

**Checkliste (0)**

Die Konfiguration ist gültig und kann an den Controller gesendet werden.

**Eigenschaften**

		Status	Alert	Actuator
Terminator Plug	Name	On Off Reset	Marginal Warning Fault	Detected
1	Sensor 1	Red circle	White circle	White circle
2	Sensor 2	Green circle	White circle	Green circle
3	Sensor 3	Green circle	White circle	Green circle
4	Sensor 4	Green circle	White circle	Green circle
	M0:SRF	Red square	White square	

		Status	Alert	Actuator
Terminator Plug	Name	On Off Reset	Marginal Warning Fault	Detected
1	Sensor	Green circle	White circle	
	M0:SEU	Green square	White square	

Abbildung 73: Registerkarte DCD im "Live"-Modus mit nicht betätigtem Sensor

Im "Live"-Modus werden durch Anklicken eines DCD-Gerätes dessen Diagnosedaten angezeigt. Diese beinhalten Eingangs- und Ausgangsdaten und ob der zugehörige Betätiger erkannt wurde falls zutreffend.

New Config (bestätigt) - Sicherheitskontrollern BERNSTEIN

Geräte Funktionsansicht Schaltplan Kontaktplan Industrie-Ethernet Konfigurationsübersicht Livemodus DCD

**Modulübersicht**

**Checkliste (0)**

Die Konfiguration ist gültig und kann an den Controller gesendet werden.

**Eigenschaften**

Terminator Plug	Name	Status	Alert	Actuator
		On Off Reset	Marginal Warning Fault	Detected
1	Sensor 1	Off	Warning	Detected
2	Sensor 2	On	Warning	Detected
3	Sensor 3	On	Warning	Detected
4	Sensor 4	On	Warning	Detected
	MO:SRF	Off	Warning	Detected

Terminator Plug	Name	Status	Alert	Actuator
		On Off Reset	Marginal Warning Fault	Detected
1	Sensor	On	Warning	Detected
	MO:SEU	On	Warning	Detected

**Channel:1 Device:1** Schließen

- Status Output 1: False
- Status Output 2: False
- Actuator Detected: False
- Wrong Actuator: False
- Actuator in Edge Area: False
- Status Input 1: True
- Status Input 2: True
- Local Reset Expected: False
- Output Error: False
- Failsafe Input Error: False
- DCD Error Bit: False
- Operating Voltage Error: False
- Error! Voltage reset required: False
- Operating Voltage Warning: False
- Sensor Not Paired: False
- Device ID: 1
- Saved RFID: 1234
- Received RFID: 0000
- Remaining Teach Procedures: 0
- Number of Voltage Errors: 0000
- Remaining time to lockout: 001F
- RFID Range Warning Count: 0000
- Supply Voltage: 24,04 V
- Internal Temperature: 39 C
- Actuator Distance: >18 mm
- Expected Company Name: 0005
- Received Company Name: 0000
- Internal Error A: 0000
- Internal Error B: 0000
- Local Reset Button: False
- Configured Coding Level: False
- Cascadable: True
- Error Tolerant Outputs: True

Abbildung 74: Registerkarte DCD im "Live"-Modus mit Diagnose Daten



## 8.9 Registerkarte **Industrial-Ethernet**

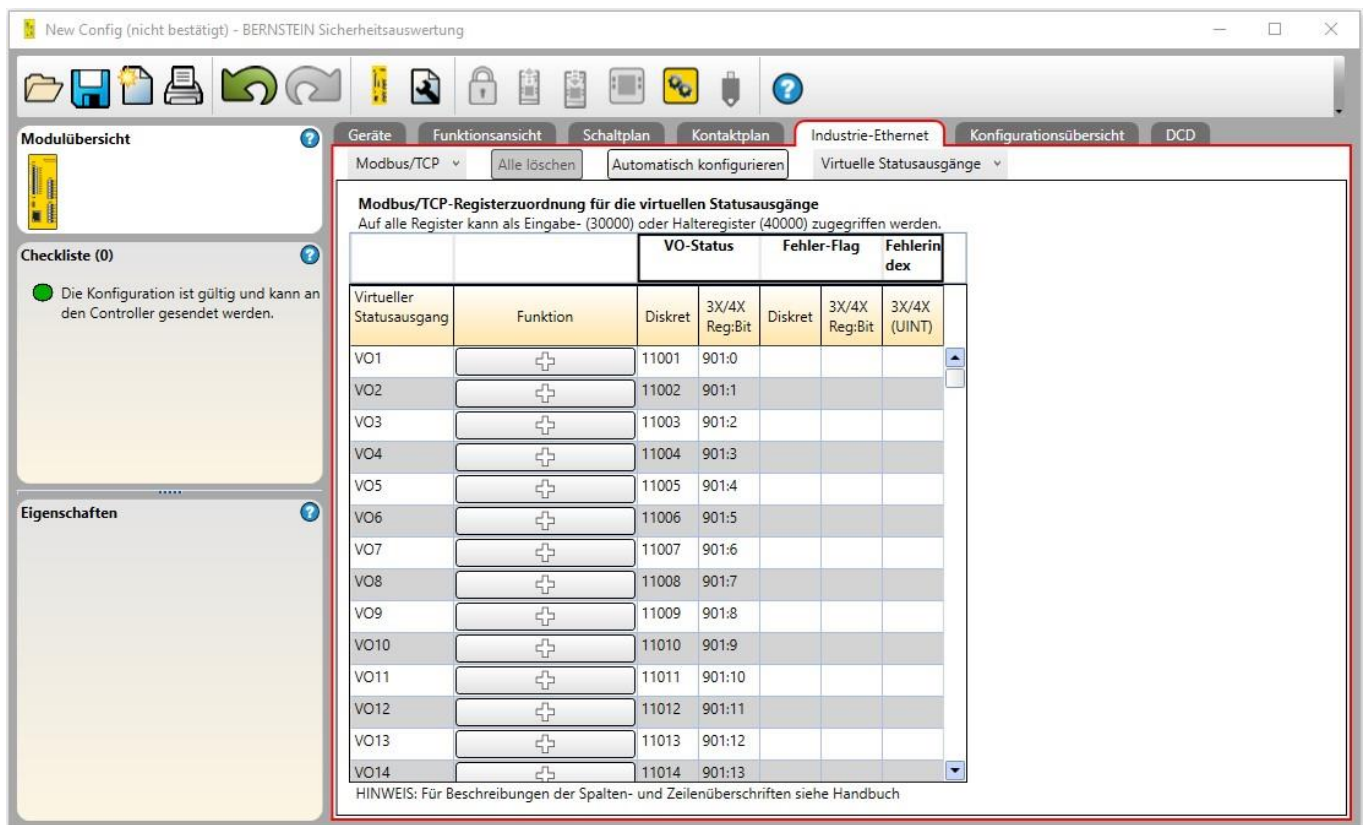



Abbildung 75: Registerkarte **Industrial-Ethernet**

Auf der Registerkarte **Industrial-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) (siehe [Signallogik für Statusausgänge](#) auf Seite 50 und [Statusausgangsfunktion](#) auf Seite 51 für detaillierte Informationen.) Die folgenden Industrial-Ethernet-Protokolle können ausgewählt und verwendet werden: PROFINET, Modbus/TCP, Ethernet/IP-Eingangsguppen, Ethernet/IP-explicite-Nachrichten und PCCC-Protokolle. Es können bis zu 256 virtuelle Statusausgänge hinzugefügt werden.

Zugriff auf die Registerkarte **Industrial-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 94 oder [Netzwerkeinstellungen: PROFINET](#) auf Seite 95).
4. Klicken Sie auf **OK**.

Verwenden Sie die Funktion **Automatisch konfigurieren** auf der Registerkarte **Industrial-Ethernet** in 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.

## 8.9.1 Netzwerkeinstellungen

### 8.9.1.1 Netzwerkeinstellungen: Modbus/TCP, Ethernet/IP, PCCC

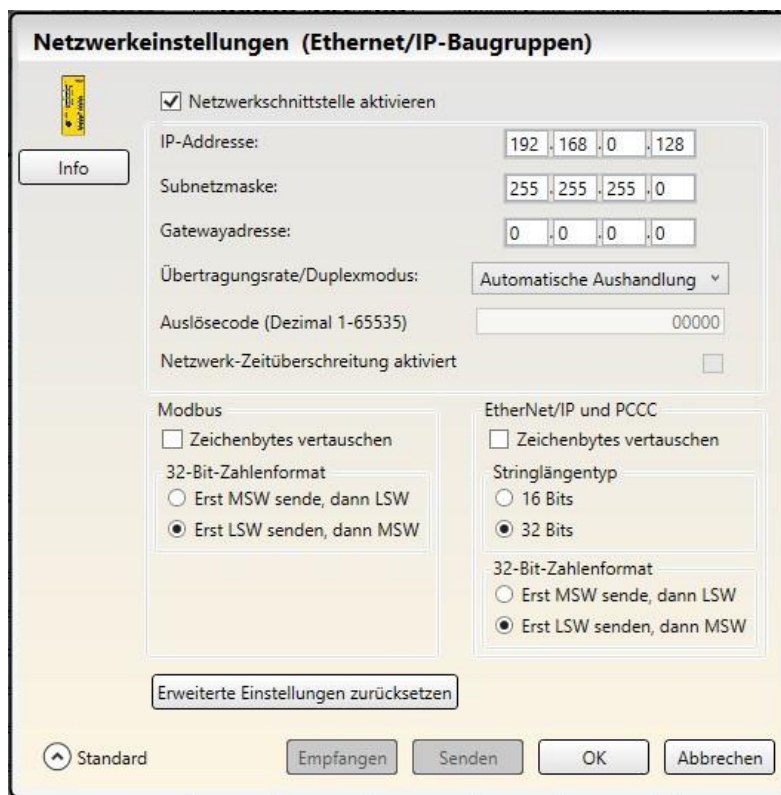


Abbildung 76: Netzwerkeinstellungen


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 5. Netzwerk-Standard-einstellungen

Name der Einstellung	Im Werk voreingestellter Wert
<b>IP-Adresse</b>	192.168.0.128
<b>Subnetzmaske</b>	255.255.255.0
<b>Gatewayadresse</b>	0.0.0.0
<b>Übertragungsrate/Duplexmodus</b>	Automatische Aushandlung

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 in die Sicherheitsauswertung zu schreiben. Die Netzwerkeinstellungen werden separat von den Konfigurationseinstellungen gesendet.

Klicken Sie auf **Netzwerk-Zeitüberschreitung aktiviert**, damit konfigurierten virtuelle 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.

### 8.9.1.2 Netzwerkeinstellungen: PROFINET


Klicken Sie nach der Auswahl des PROFINET-Protokolls in der Software auf der Registerkarte **Industrial-Ethernet** auf  **Netzwerkeinstellungen**, um das Fenster **Netzwerkeinstellungen** zu öffnen.



Abbildung 77: Netzwerkeinstellungen – PROFINET

Klicken Sie auf **Senden**, um die Netzwerkeinstellungen in die Sicherheitsauswertung 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.

## 8.9.2 Erstellung einer Datei mit SPS-Tags/-Labels

Verwenden Sie die Software der Sicherheitsauswertung von BERNSTEIN, um eine .csv- oder .xml-Datei mit den Namen aller virtuellen Statusausgänge und -eingänge zu generieren.

Wenn Sie die in der Software der Sicherheitsauswertung erstellten Namen als SPS-Tags/Labels verwenden möchten, importieren Sie die .csv- bzw. .xml-Datei in die verwendete SPS-Software im Bereich Ethernet/IP-Baugruppen oder PROFINET.

Erstellen Sie zuerst alle Statusausgänge und -eingänge, die Sie in der Software der Sicherheitsauswertung nutzen möchten. Weisen Sie gegebenenfalls unter **Netzwerkeinstellungen** einen Auslösecode zu. Vergewissern Sie sich anschließend, dass das gewünschte Protokoll ausgewählt ist (entweder Ethernet/IP-Baugruppen oder PROFINET).

### CSV-Datei für Ethernet/IP-Baugruppen erstellen

Zwei Elemente müssen bekannt sein:

- Der Name, der der Sicherheitsauswertung 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 Auswahlliste **Ethernet/IP-Baugruppen** ausgewählt ist.
2. Klicken Sie auf **Exportieren**.

Das Fenster **Als CSV exportieren** wird geöffnet.



Abbildung 78: Als CSV exportieren

3. Geben Sie im Feld **Name der Auswertung** den Namen ein, der der Sicherheitsauswertung 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 die Sicherheitsauswertung senden kann. Wenn Informationen an den DCD-Eingängen gewünscht sind, muss eine mit 114 festgelegte Ausgangsbaugruppe verwendet werden, damit die virtuellen Eingänge (sofern verwendet) und die zusätzlichen Wörter zur Anfrage der DCD-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).

## XML-Datei für PROFINET erstellen

Drei Elemente müssen bekannt sein:

- Der Name, der der Sicherheitsauswertung 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-Slot 1
  - Adresspfad zum SPS-Slot 13
  - Adresspfad zum SPS-Slot 20
  - Adresspfad zum SPS-Slot 21
1. Vergewissern Sie sich, dass auf der Registerkarte **Industrie-Ethernet** in der Auswahlliste **Profinet** ausgewählt ist.
  2. Klicken Sie auf **Exportieren**.  
Das Fenster **Als XML exportieren** wird geöffnet.

Abbildung 79: Als XML exportieren

3. Geben Sie im Feld **Name der Auswertung** den Namen ein, der der Sicherheitsauswertung in der SPS-Software zugewiesen ist.
4. Geben Sie im Feld **Adresspfad zum SPS-Slot 1** den Anfang des Adresspfads zum Slot 1 ein (Stausgänge).
5. Geben Sie im Feld **Adresspfad zum SPS-Slot 13** den Anfang des Adresspfads zum Slot 13 ein (virtuelle Eingänge).
6. Geben Sie im Feld **Adresspfad zum SPS-Slot 20** den Anfang des Adresspfads zum Slot 20 ein (DCD-Statusinformationsmodul).
7. Geben Sie im Feld **Adresspfad zum SPS-Slot 21** den Anfang des Adresspfads zum Slot 21 ein (Modul für Informationen einzelner DCD-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).

## 8.9.3 Ethernet/IP-Gruppenobjekte



**Anmerkung:** Die EDS-Datei steht unter dem folgenden Link zum Download zur Verfügung:  
[www.bernstein.eu](http://www.bernstein.eu).

### Eingangsgruppenobjekte (T->O)

Instanz-ID	Datenlänge (16-Bit-Wörter)	Beschreibung
100 (0x64)	8	Dient für den Zugriff auf die Basisinformationen über die virtuellen Statusausgänge 1–64.
101 (0x65)	104	Dient für den Zugriff auf die erweiterten Informationen (außer Basisinformationen) über die virtuellen Statusausgänge.
102 (0x66)	150	Dient für den Zugriff auf die Fehlerprotokollinformationen und enthält keine Informationen zu den virtuellen Statusausgängen.
103 (0x67)	35	Dient für den Zugriff auf die allgemeinen Informationen über die virtuellen Statusausgänge 1–256 und auf Feedback-Informationen über virtuelle Reset- und virtuelle Eingänge zum Abbruch einer Zeitverzögerung.
104 (0x68)	111	Dient für den Zugriff auf die allgemeinen Informationen über die virtuellen Statusausgänge 1–256 und auf Feedback-Informationen über virtuelle Reset- und virtuelle Eingänge zum Abbruch einer Zeitverzögerung und zur Unterstützung der Kommunikation mit DCD-Geräten.

### Ausgangsgruppenobjekt (O->T)

Instanz-ID	Datenlänge (16-Bit-Wörter)	Beschreibung
112 (0x70)	2	Reserviert
113 (0x71)	11	Dient zur Steuerung von virtuellen Eingängen (Ein/Aus, Muting-Aktivierung, Reset, Abbruch einer Zeitverzögerung).
114 (0x72)	16	Dient zur Steuerung von virtuellen Eingängen (Ein/Aus, Muting-Aktivierung, Reset, Abbruch einer Zeitverzögerung) und zur Unterstützung der Kommunikation mit DCD-Geräten.

### Konfigurationsgruppenobjekt

Das Konfigurationsgruppenobjekt ist nicht implementiert. Allerdings erfordern einige Ethernet-/IP-Clients ein solches Objekt. In diesem Fall wird Instanz-ID 128 (0x80) mit einer Datenlänge von 0 verwendet.

Legen Sie als Datentyp des Kommunikationsformat INT fest.

Legen Sie als gefordertes Paketintervall (RPI) mindestens den Wert 150 fest.

## 8.9.4 Industrial-Ethernet: Beschreibung der Tabellenzeilen und -spalten

Es folgen Beschreibungen der Tabellenzeilen und -spalten (in alphabetischer Reihenfolge) für die Registerkarten der Ansicht **Industrial-Ethernet** in der Software und in den *Tabellen mit unterstützten Fehlerprotokollen* auf Seite 99.

Tabelle 6. 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 (*Fehlercode-Tabelle für SCR P* auf Seite 137 erhalten Sie weitere Informationen).

### 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)	Systemsperr
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 der Sicherheitsauswertung. 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 Eingangsgruppe, 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 im Fenster **Netzwerkeinstellungen** im Menü **Erweitert** die Option „*Zeichenbytes vertauschen*“.

### String (Modbus/TCP-Protokoll)

Das String-Format 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 im Fenster **Netzwerkeinstellungen** im Menü **Erweitert** die Option „*Zeichenbytes vertauschen*“.

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.

## 8.9.5 Tabellen mit unterstützten Fehlerprotokollen

### Modbus/TCP 3X/4X

Fehlerprotokoll	Typ	Länge (Wörter)	Anfangsregister
Fehlerprotokolleintrag 1 (zuletzt erstellt)	Siehe unten in der Tabelle der <b>Fehlerprotokolleinträge</b>	15	233
Fehlerprotokolleintrag 2		15	248
Fehlerprotokolleintrag 3		15	263
Fehlerprotokolleintrag 4		15	278
Fehlerprotokolleintrag 5		15	293
Fehlerprotokolleintrag 6		15	308
Fehlerprotokolleintrag 7		15	323
Fehlerprotokolleintrag 8		15	338
Fehlerprotokolleintrag 9		15	353
Fehlerprotokolleintrag 10 (zuerst erstellt)		15	368

Fehlerprotokolleintrag	Typ	Länge (Wörter)
Zeitstempel	UDINT	2
Name Länge	DWORD	2
Namensstring	String	6
Fehlercode	WORD	1
Erweiterter Fehlercode	WORD	1
Fehlermeldungsindex	WORD	1
Reserviert	WORD	2



Systeminformationen	Typ	Länge (Wörter)	Anfangsregister
Sekunden seit Systemstart	UDINT	2	383
Betriebsart	WORD	1	385
Länge ConfigName	DWORD	2	386
ConfigName	String	8	388
Konfig. CRC	WORD	2	396

## PCCC

Fehlerprotokoll	Typ	Länge (Wörter)	Anfangsregister
Fehlerprotokolleintrag 1 (zuletzt erstellt)	Siehe unten in der Tabelle der Fehlerprotokolleinträge	15	232
Fehlerprotokolleintrag 2		15	247
Fehlerprotokolleintrag 3		15	262
Fehlerprotokolleintrag 4		15	277
Fehlerprotokolleintrag 5		15	292
Fehlerprotokolleintrag 6		15	307
Fehlerprotokolleintrag 7		15	322
Fehlerprotokolleintrag 8		15	337
Fehlerprotokolleintrag 9		15	352
Fehlerprotokolleintrag 10 (zuerst erstellt)		15	367

Fehlerprotokolleintrag	Typ	Länge (Wörter)	Anfangsregister
Zeitstempel	UDINT	2	Versatz: 0
Name Länge	DWORD	2	Versatz: 2
Namensstring	String	6	Versatz: 4
Fehlercode	WORD	1	Versatz: 10
Erweiterter Fehlercode	WORD	1	Versatz: 11
Fehlermeldungsindex	WORD	1	Versatz: 12
Reserviert	WORD	2	Versatz: 13

Systeminformationen	Typ	Länge (Wörter)	Anfangsregister
Sekunden seit Systemstart	UDINT	2	382
Betriebsart	WORD	1	384
Länge ConfigName	DWORD	2	385
ConfigName	String	8	387
Konfig. CRC	WORD	2	395

## Ethernet/IP Explizite Nachrichten

Fehlerprotokoll	Typ	Länge (Wörter)	Klasse 0x71 Instanz 1 Attribut
Fehlerprotokolleintrag 1 (zuletzt erstellt)	Siehe unten in der Tabelle der Fehlerprotokolleinträge	15	1
Fehlerprotokolleintrag 2		15	2
Fehlerprotokolleintrag 3		15	3
Fehlerprotokolleintrag 4		15	4
Fehlerprotokolleintrag 5		15	5
Fehlerprotokolleintrag 6		15	6
Fehlerprotokolleintrag 7		15	7

Fehlerprotokoll	Typ	Länge (Wörter)	Klasse 0x71 Instanz 1 Attribut
Fehlerprotokolleintrag 8		15	8
Fehlerprotokolleintrag 9		15	9
Fehlerprotokolleintrag 10 (zuerst erstellt)		15	10

Fehlerprotokolleintrag	Typ	Länge (Wörter)
Zeitstempel	UDINT	2
Name Länge	DWORD	2
Namensstring	String	6
Fehlercode	WORD	1
Erweiterter Fehlercode	WORD	1
Fehlermeldungsindex	WORD	1
Reserviert	WORD	2

Systeminformationen	Typ	Länge (Wörter)	Klasse 0x72 Instanz 1 Attribut
Sekunden seit Systemstart	UDINT	2	1
Betriebsart	WORD	1	2
Länge ConfigName	DWORD	2	3
ConfigName	String	8	3
Konfig. CRC	WORD	2	4

## Ethernet/IP-Eingangsgruppen

Klasse 4, Instanz 102, Attribut 3

Fehlerprotokoll	Zeitstempel	Name Länge	Namensstring	Fehlercode	Erw. Fehlercode	Fehlermeldung Index	Reserviert
Fehlerprotokolleintrag 1 (zuletzt erstellt)	0	2	4	10	11	12	13
Fehlerprotokolleintrag 2	15	17	19	25	26	27	28
Fehlerprotokolleintrag 3	30	32	34	40	41	42	43
Fehlerprotokolleintrag 4	45	47	49	55	56	57	58
Fehlerprotokolleintrag 5	60	62	64	70	71	72	73
Fehlerprotokolleintrag 6	75	77	79	85	86	87	88
Fehlerprotokolleintrag 7	90	92	94	100	101	102	103
Fehlerprotokolleintrag 8	105	107	109	115	116	117	118
Fehlerprotokolleintrag 9	120	122	124	130	131	132	133
Fehlerprotokolleintrag 10 (zuerst erstellt)	135	137	139	145	146	147	148
	UDINT	DWORD	String	WORD	WORD	WORD	WORD

## Abrufen aktueller Fehlerinformationen

Befolgen Sie die nachstehend beschriebenen Schritte, um Informationen über Netzwerkkommunikationen zu einem gegenwärtig vorhandenen Fehler abzurufen:

- Lesen Sie den Speicherort *Fehlerindex*, um den Fehlerindexwert abzurufen.

Suchen Sie den Indexwert in der [Fehlercode-Tabelle für SCR P](#) auf Seite 137, um eine Fehlerbeschreibung und Schritte für die Behebung des Fehlers aufzurufen.

## PROFINET-Steckplätze

PROFINET-Echtzeitdaten werden über Steckplätze gesendet und empfangen.



**Anmerkung:** Die GSDML-Datei steht unter dem folgenden Link zum Download zur Verfügung:  
[www.bernstein.eu](http://www.bernstein.eu)

Die Funktion der Steckplätze 1 bis 17 ist festgelegt und immer aktiv. Die vom Benutzer auswählbaren Daten sind 4 Byte. Die Steckplätze 1 bis 12 sind für virtuelle Statusausgänge bestimmt. Die Steckplätze 13 bis 17 sind für virtuelle nicht sicherheitsrelevante Eingänge bestimmt. Die Steckplätze 18 und 19 haben auswählbare Moduldaten. Aktivieren Sie die Steckplätze 18 und 19 über das TIA-Portal.

### Slot 18: Fehlerprotokollpuffer

Fehlerprotokoll	Typ	Länge (Wörter)
Fehlerprotokolleintrag 1 (zuletzt erstellt)	Siehe unten in der Tabelle der <b>Fehlerprotokolleinträge</b>	15
Fehlerprotokolleintrag 2		15
Fehlerprotokolleintrag 3		15
Fehlerprotokolleintrag 4		15
Fehlerprotokolleintrag 5		15
Fehlerprotokolleintrag 6		15
Fehlerprotokolleintrag 7		15
Fehlerprotokolleintrag 8		15
Fehlerprotokolleintrag 9		15
Fehlerprotokolleintrag 10 (zuerst erstellt)		15

Fehlerprotokolleintrag	Typ	Länge (Wörter)
Zeitstempel	UDINT	2
Name Länge	DWORD	2
Namensstring	String	6
Fehlercode	WORD	1
Erweiterter Fehlercode	WORD	1
Fehlermeldungsindex	WORD	1
Reserviert	WORD	2

### Slot 19: Puffer für Systeminformationen

Systeminformationen	Typ	Länge (Wörter)
Sekunden seit Systemstart	UDINT	2
Betriebsart	WORD	1
Länge ConfigName	DWORD	2
ConfigName	String	8
Konfig. CRC	WORD	2

## 8.10 Registerkarte Konfigurationsübersicht

**M0:SCR P-10-6R-4 Eingänge**

Typ:	Optosensor	Typ:	DCD-Gerät	Typ:	DCD-Gerät
Name:	OS1	Name:	DCD1	Name:	DCD2
Modul:	M0	Modul:	M0	Modul:	M0
Schaltungstyp:	Zweikanalig PNP	Schaltungstyp:	Zweikanalig PNP	Schaltungstyp:	Zweikanalig PNP
Klemmen:	IN1, IN2	Klemmen:	IN3, IN4	Klemmen:	IN5, IN6
Simultanität:	Simultan	Entprellung:	6 ms	Entprellung:	6 ms
Entprellung:	6 ms	Geschlossen-Offen:	50 ms	Geschlossen-Offen:	50 ms
Geschlossen-Offen:	50 ms	Entprellung Offen:	50 ms	Entprellung Offen:	50 ms
Entprellung Offen:	50 ms	Geschlossen:	A1	Geschlossen:	A1
Geschlossen:		Ausgang:		Ausgang:	A1
Inbetriebnahmetest:	Deaktiviert	Sicherheitsausgänge:		Sicherheitsausgänge:	
Ausgang:	A1				
Sicherheitsausgänge:					

Typ:	Schutztürschalter	Typ:	Schutztürschalter
Name:	GS1	Name:	GS2
Modul:	M0	Modul:	M0
Schaltungstyp:	Einkanalig 2 Anschlüsse	Schaltungstyp:	Einkanalig 2 Anschlüsse
Klemmen:	IO1, IO2	Klemmen:	IO1, IO3
Simultanität:	Simultan	Simultanität:	Simultan
Entprellung:	6 ms	Entprellung:	6 ms
Geschlossen-Offen:	50 ms	Geschlossen-Offen:	50 ms
Entprellung Offen:	50 ms	Entprellung Offen:	50 ms
Geschlossen:		Geschlossen:	
Inbetriebnahmetest:	Deaktiviert	Inbetriebnahmetest:	Deaktiviert
Ausgang:	A1	Ausgang:	A1
Sicherheitsausgänge:		Sicherheitsausgänge:	

Typ:	Manueller Reset
Name:	MR1

 Abbildung 80: 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.

## 8.11 Druckoptionen

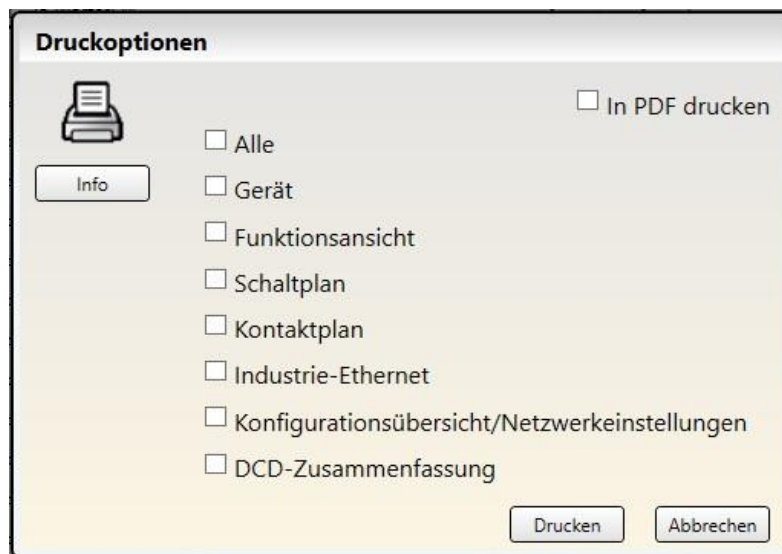


Abbildung 81: Druckoptionen



Die Software bietet mehrere Möglichkeiten 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**.
- **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).
- **DCD Zusammenfassung:** Druckt die DCD-Registerkarte.

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.

## 8.12 Passwort-Manager



**Passwort-Manager** ist verfügbar, wenn eine Sicherheitsauswertung über einen USB-Anschluss mit dem PC verbunden ist. Die im **Passwort-Manager** angezeigten Informationen stammen von der Sicherheitsauswertung.

Abbildung 82: Passwort-Manager

Klicken Sie in der Symbolleiste der Software auf **Passwort-Manager**, um die Zugriffsrechte für die Konfiguration zu bearbeiten. Die Sicherheitsauswertung 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 die Konfiguration, Netzwerkeinstellungen, Schaltpläne und Diagnoseinformationen kann ohne Passwort zugegriffen werden. Auf einem PC oder SCR P-FPS-Laufwerk gespeicherte Konfigurationen sind nicht passwortgeschützt.

Benutzer2 oder Benutzer3 kann die Konfiguration in die Sicherheitsauswertung schreiben, wenn **Berechtigung zum Ändern der Konfiguration** aktiviert ist. Diese Benutzer können die Netzwerkeinstellungen ändern, wenn **Berechtigung zum Ändern der Netzwerkeinstellungen** aktiviert ist. Die jeweiligen Passwörter müssen eingegeben werden.

Klicken Sie auf **Speichern**, um die Passwortinformationen für die aktuelle Konfiguration in der Software zu übernehmen und sie in die Sicherheitsauswertung zu schreiben.



**Anmerkung:** Die im Werk voreingestellten Passwörter für Benutzer1, Benutzer2 und Benutzer3 lauten jeweils 1901, 1902 und 1903. Es wird dringend empfohlen, die im Werk voreingestellten Passwörter zu ändern.

Nur Benutzer1 kann das SCR P auf die Werkseinstellungen zurücksetzen.

## 8.13 Anzeigen und Importieren von Daten



Über die Software für die Sicherheitsauswertung der BERNSTEIN AG können aktuelle Daten (z. B. Modellnummer und Firmware-Version, Konfigurations- und Netzwerkeinstellungen sowie Schaltplan) angezeigt oder kopiert werden.

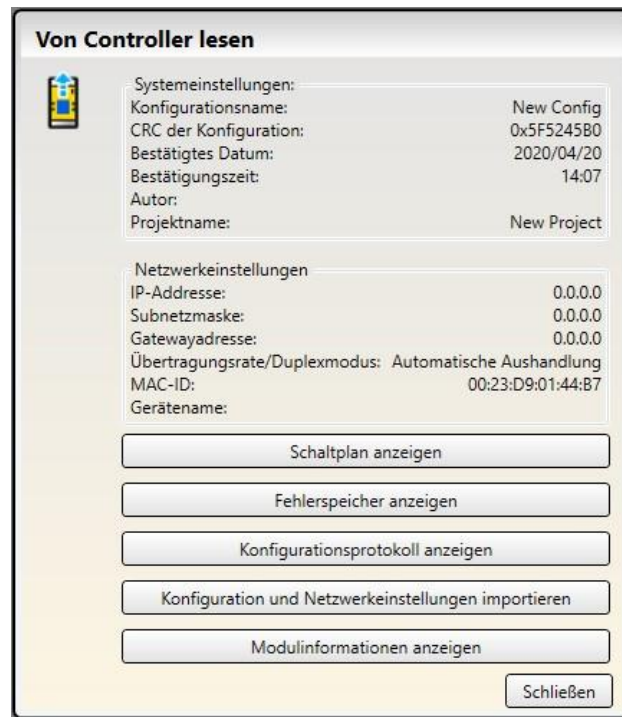


**Von der Auswertung lesen** ist verfügbar, wenn eine Sicherheitsauswertung über USB an den PC angeschlossen ist.

### Anzeigen einer Momentaufnahme der System- und Netzwerkeinstellungen

Klicken Sie in der Symbolleiste der Software auf **Von der Auswertung lesen**. Die aktuellen Einstellungen für die Sicherheitsauswertung werden angezeigt:

- Konfigurationsname
- CRC der Konfiguration
- Datum der Bestätigung
- Uhrzeit der Bestätigung
- Autor
- Projektname
- IP-Adresse
- Subnetzmaske
- Gatewayadresse
- Übertragungsrate/Duplexmodus
- MAC-ID



**Von Controller lesen**

Systemeinstellungen:

Konfigurationsname:	New Config
CRC der Konfiguration:	0x5F5245B0
Bestätigtes Datum:	2020/04/20
Bestätigungszeit:	14:07
Autor:	
Projektname:	New Project

Netzwerkeinstellungen

IP-Adresse:	0.0.0.0
Subnetzmaske:	0.0.0.0
Gatewayadresse:	0.0.0.0
Übertragungsrate/Duplexmodus:	Automatische Aushandlung
MAC-ID:	00:23:D9:01:44:B7
Geräteiname:	

Schaltplan anzeigen

Fehlerspeicher anzeigen

Konfigurationsprotokoll anzeigen

Konfiguration und Netzwerkeinstellungen importieren

Modulinformationen anzeigen

Schließen

Abbildung 83: Anzeigen einer Momentaufnahme der System- und Netzwerkeinstellungen

## Anzeigen und Importieren von Daten

Klicken Sie auf  **Von der Auswertung 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 die Sicherheitsauswertung nicht aus- und wieder eingeschaltet wird. Nach dem Aus- und Wiedereinschalten der Sicherheitsauswertung beginnt die Nummerierung der Fehlerprotokolle wieder bei 1. Durch Löschen des Fehlerprotokolls (über die Software der Sicherheitsauswertung) 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 der Sicherheitsauswertung aufzurufen.



## 8.14 Livemodus



**Livemodus** ist verfügbar, wenn eine Sicherheitsauswertung über USB an den PC angeschlossen ist.

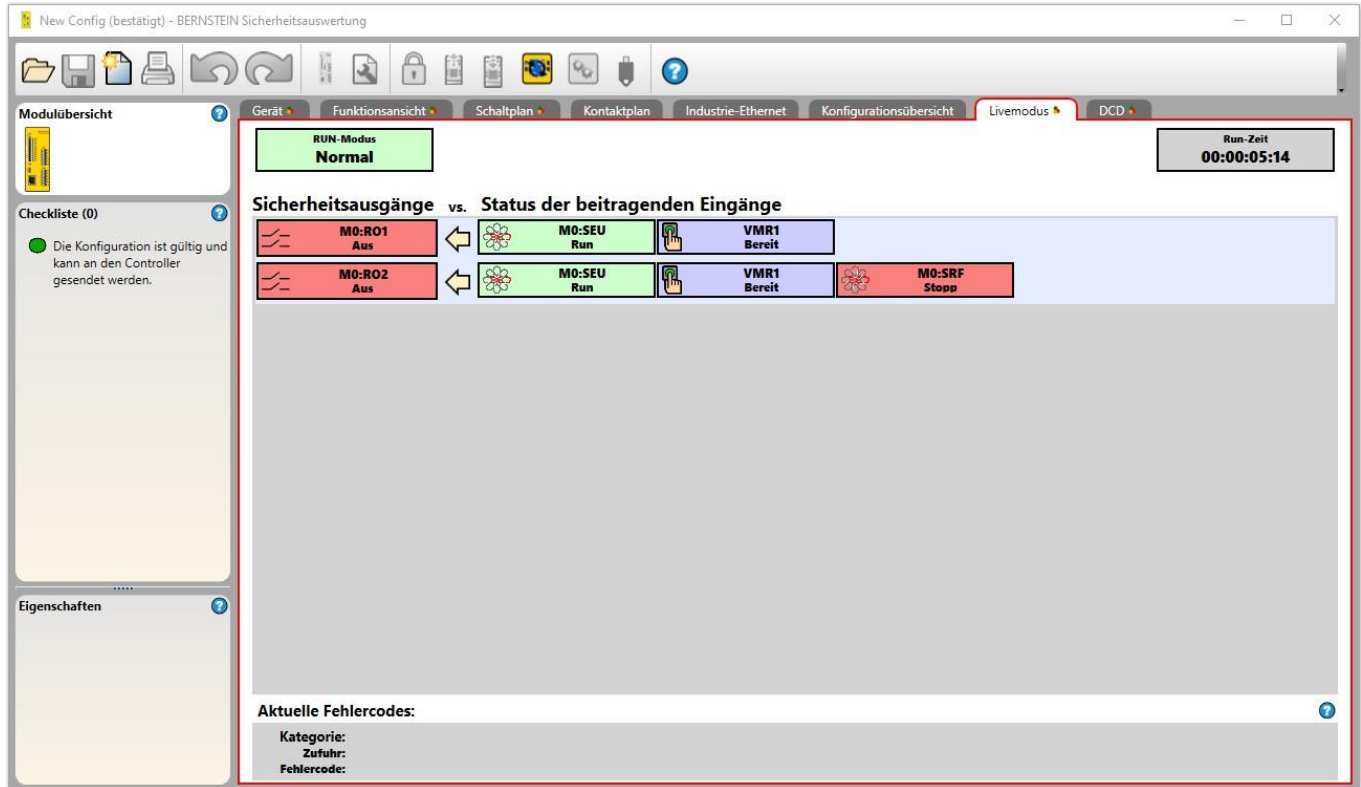



Abbildung 84: Laufzeit – Registerkarte *Livemodus*

Auf die Registerkarte **Livemodus** kann zugegriffen werden, nachdem in der Symbolleiste auf  **Livemodus** geklickt wurde. Wenn der **Livemodus** aktiviert werden die Änderungen an der Konfiguration auf allen Registerkarten deaktiviert. Die Registerkarte **Livemodus** enthält zusätzliche Informationen zu Geräten und Fehlern, darunter einen Fehlercode (siehe [Fehlercode-Tabelle für SCR P](#) auf Seite 137 für die Beschreibung und möglichen Abhilfemaßnahmen). Die Laufzeitdaten werden ebenfalls in der **Funktionsansicht**, in den Ansichten **Geräte** und **Schaltplan** aktualisiert, die eine visuelle Darstellung des jeweiligen Gerätezustands liefern.

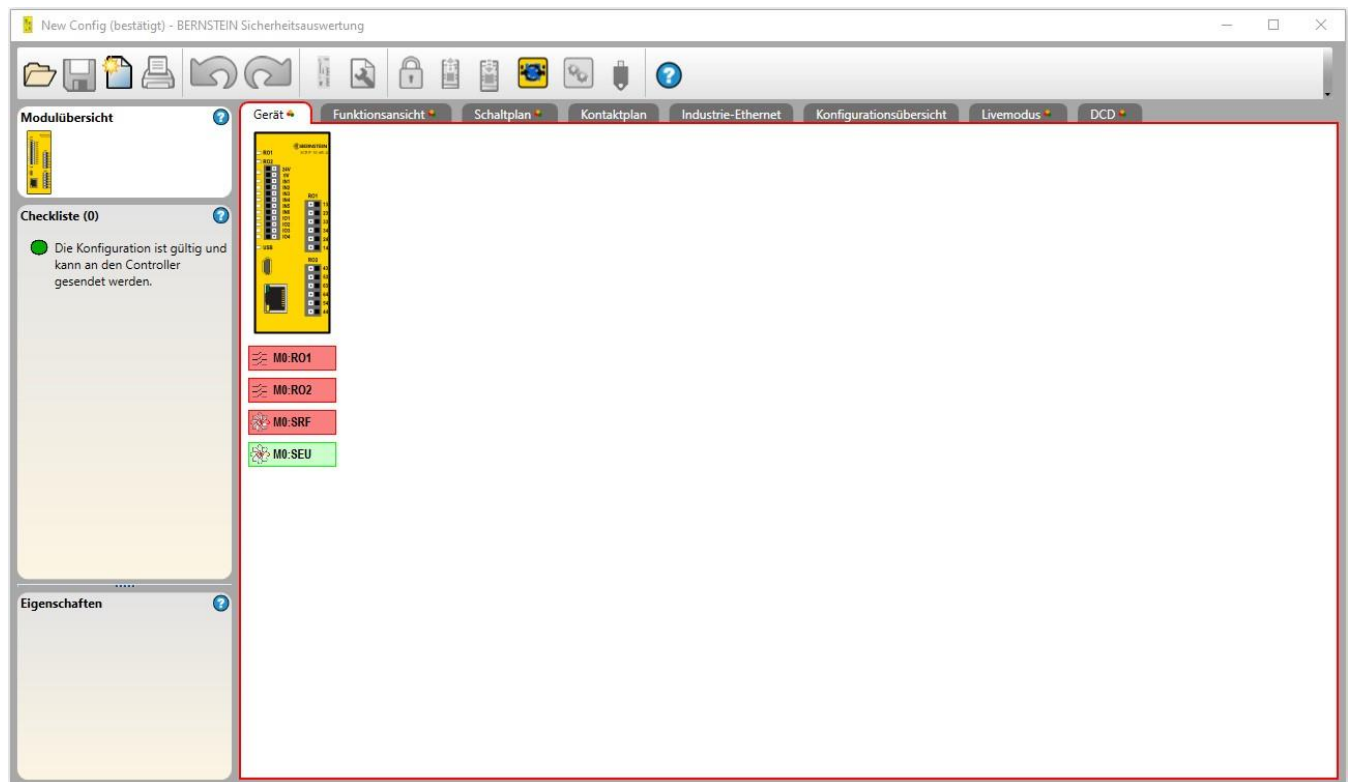


Abbildung 85: Laufzeit – Registerkarte **Geräte**

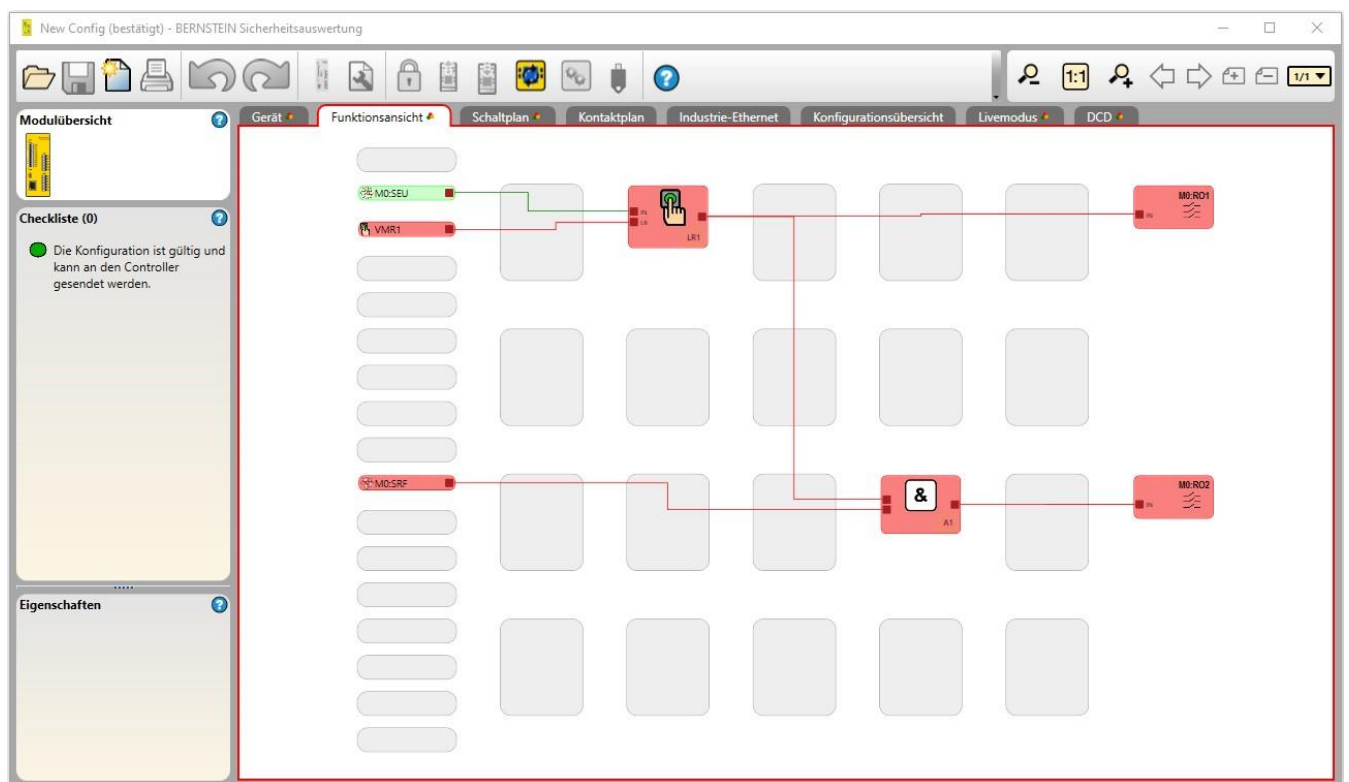
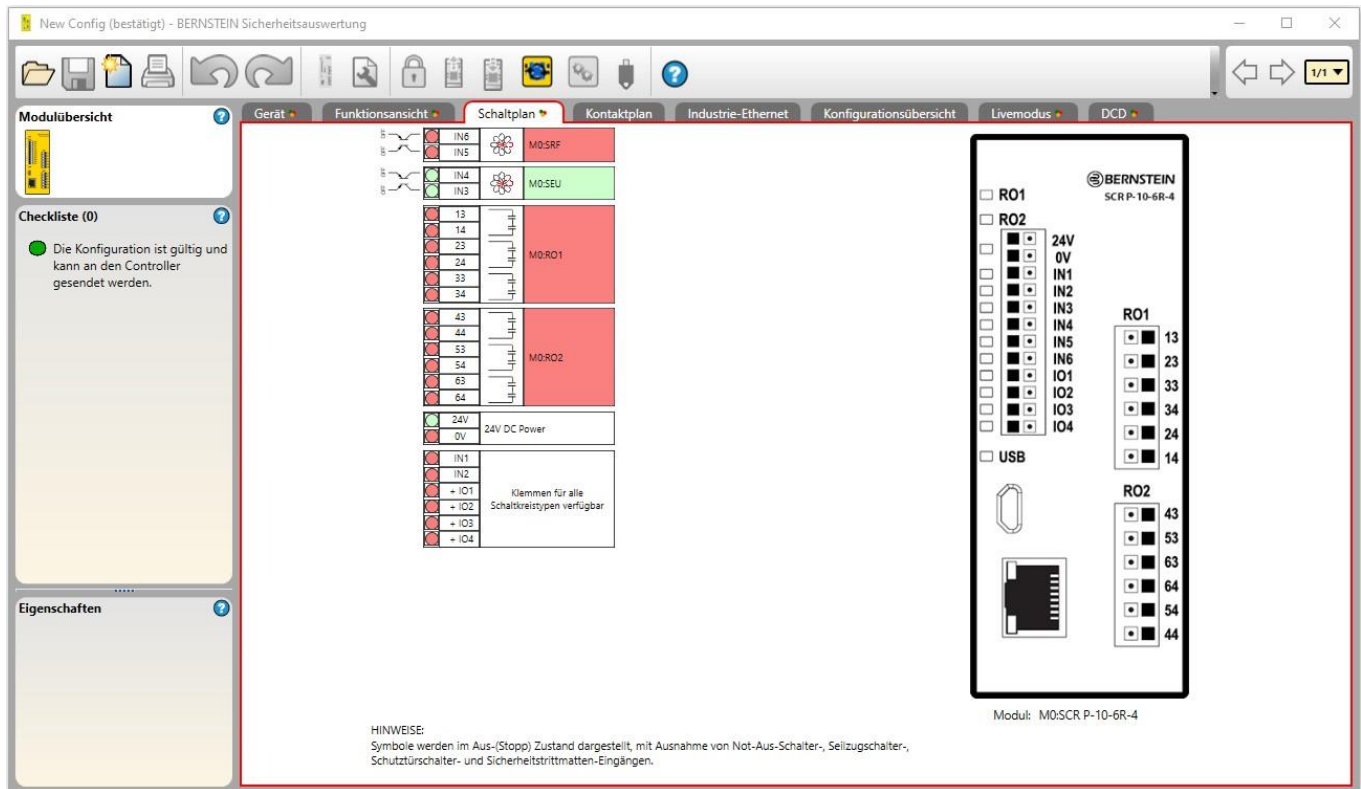


Abbildung 86: Laufzeit – Registerkarte **Funktionsansicht**


 Abbildung 87: Laufzeit – Registerkarte **Schaltplan**

New Config (bestätigt) - BERNSTEIN Sicherheitsauswertung

Modulübersicht

Checkliste (0)

Die Konfiguration ist gültig und kann an den Controller gesendet werden.

Eigenschaften

Gerät

Funktionsansicht

Schaltplan

Kontaktplan

Industrie-Ethernet

Konfigurationsübersicht

Livemodus

DCD

Terminator	Plug	Name	Status	Alarm	Auslöser
1	SRF 1	Ein	Marginal	Erkannt	
2	SRF 2	Aus	Warnung		
3	SRF 3	Reset	Fehler		
4	SRF 4				
	M0:SRF				

Terminator	Plug	Name	Status	Alarm	Auslöser
1	ES 1	Ein	Marginal	Erkannt	
	M0:SEU				

Reihe: 1	Gerät: 1	Schließen
Ausgang 1	False	
Ausgang 2	False	
Betätigter erkannt	False	
Falscher Auslöser	False	
Grenzbereich	False	
Eingang 1	True	
Eingang 2	True	
Lokaler Reset erwartet	False	
Ausgangsfehler	False	
Sicherheitseingangsfehler	False	
DCD-Datenfehler	False	
Fehler Betriebsspannung	False	
Neustart erforderlich	False	
Warnung Betriebsspannung	False	
Betätigter nicht eingelesen	False	
Gerät	Türschalter	
Erwarteter Code	1234	
Empfangener Code	0000	
Verbleibende Einlernvorgänge	0	
Anzahl der Spannungsfehler	0000	
Ausschaltzeit für Ausgang	Inaktiv	
Anzahl Bereichswarnungen	0000	
Versorgungsspannung	24.0 V	
Innentemperatur	33 C	
Auslöserabstand	>18 mm	
Erwarteter Hersteller	0005	
Empfangener Hersteller	0000	
Interner Fehler A	0000	
Interner Fehler B	0000	
Lokaler Reset vorhanden	False	
Hohe Codierstufe	False	
Kaskadierbar	True	
Fehlertolerante Ausgänge	True	

 Abbildung 88: Laufzeit – Registerkarte **DCD**

## 8.15 Simulationsmodus

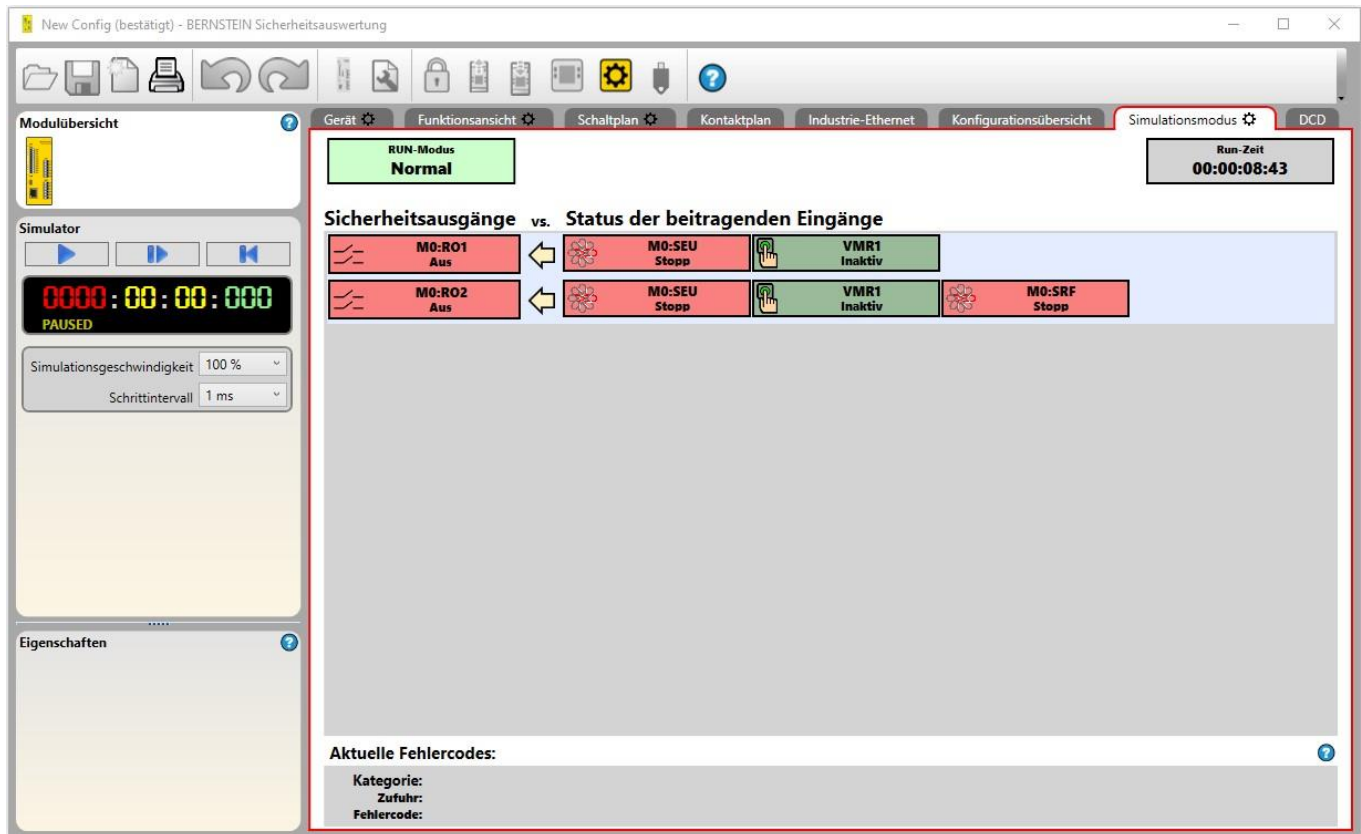



Abbildung 89: Simulationsmodus

Auf die Registerkarte **Simulationsmodus** kann durch einen Klick auf  **Simulationsmodus** in der Symbolleiste zugegriffen werden. Die Optionen für den Simulationsmodus werden links auf dem Bildschirm verfügbar. Die Registerkarte **Simulationsmodus** enthält Informationen, die nur zur Ansicht verfügbar sind. In dieser Ansicht können Sie nicht auf die Elemente „Ausgang“ und „Eingang“ klicken.



**Anmerkung:** Bei Verwendung von DCD-Geräten wird nur das Gesamtausgangssignal der Reihe/Kette simuliert, nicht das der einzelnen Geräte.



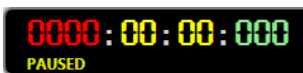
[Wiedergabe/Pause] Startet die Simulationszeit, die mit der angegebenen Simulationsgeschwindigkeit läuft, oder hält die Simulationszeit vorübergehend an.



[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 %
- %
- 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 **Funktionsansicht**, **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 ausgeschaltet werden, bevor er als eingeschaltet erkannt werden kann.

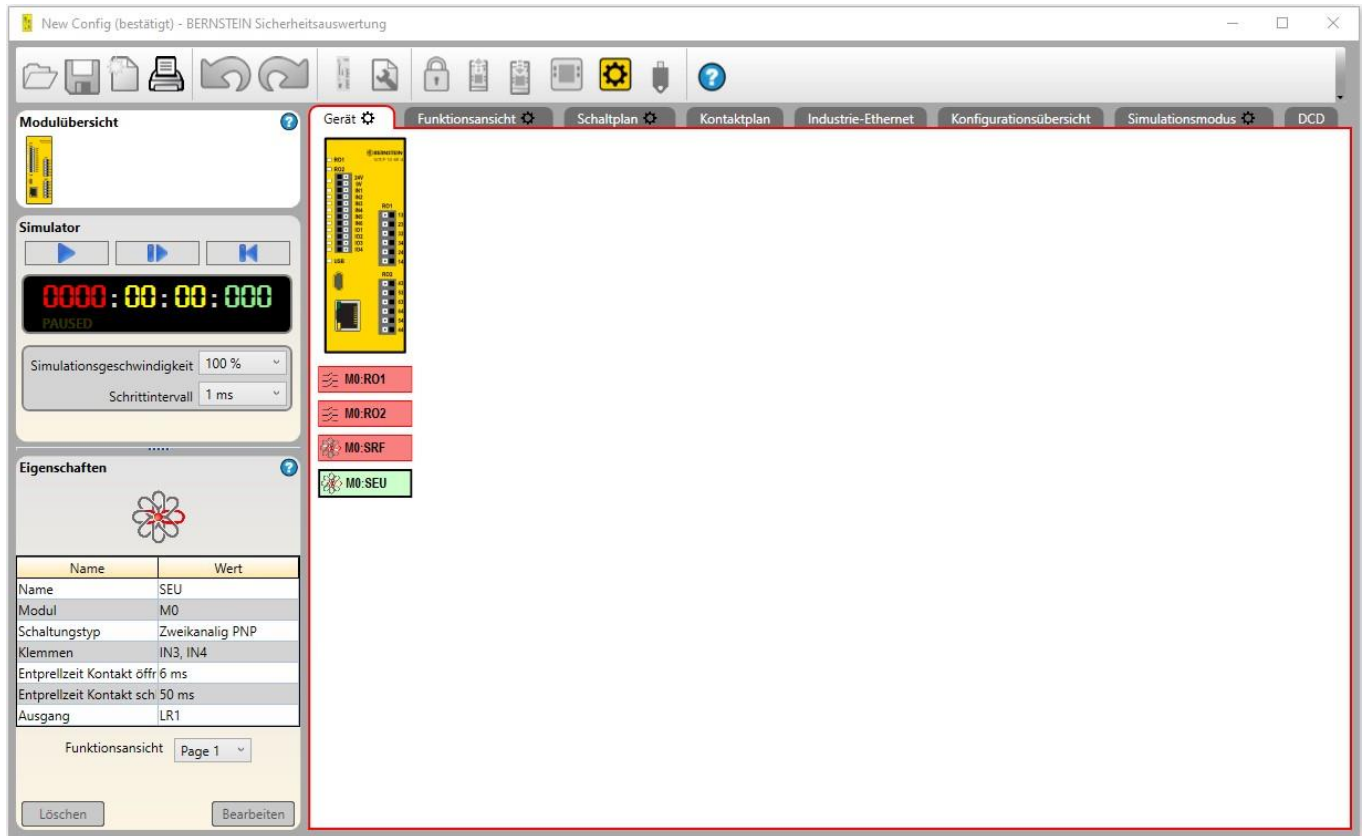


Abbildung 90: Simulationsmodus: Registerkarte **Geräte**

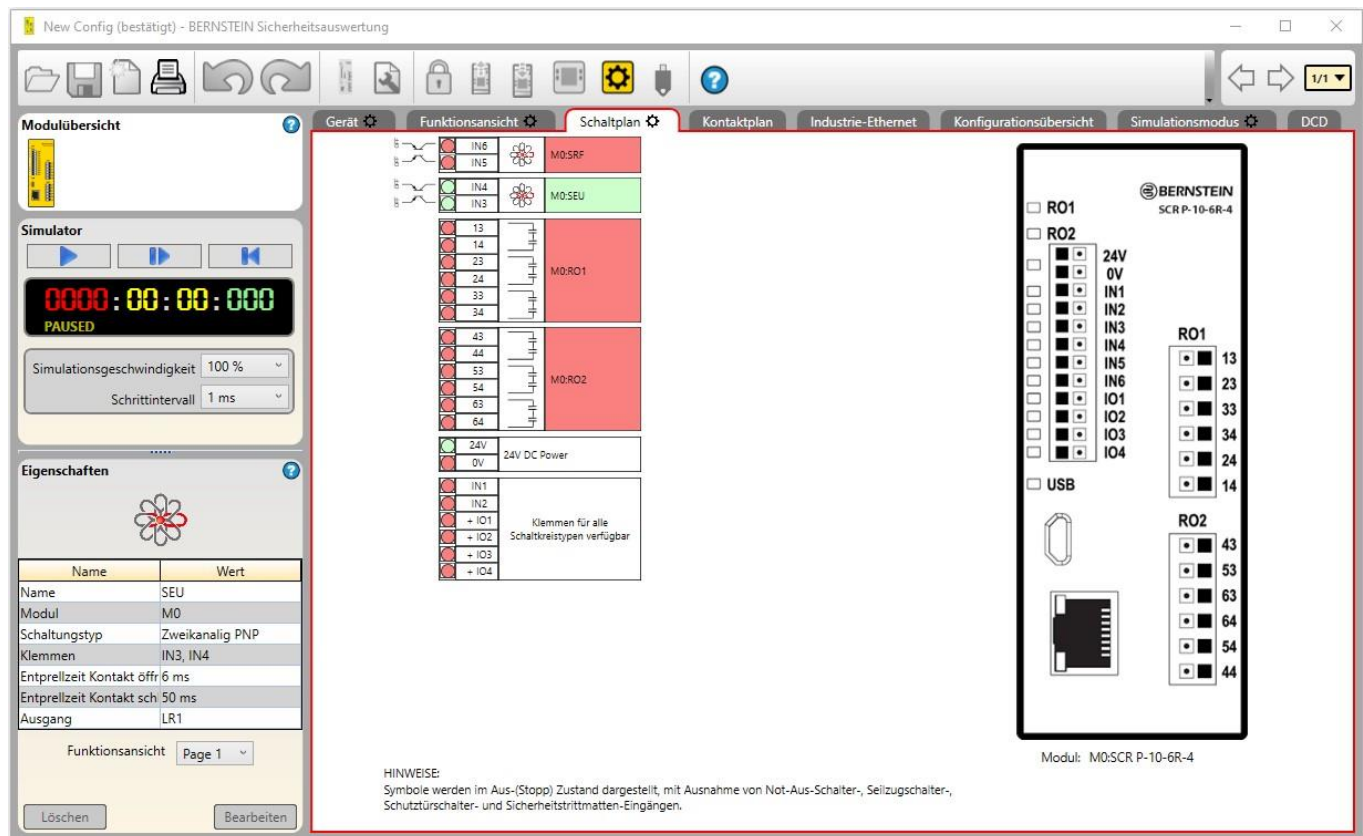


Abbildung 91: Simulationsmodus: Registerkarte **Schaltplan**

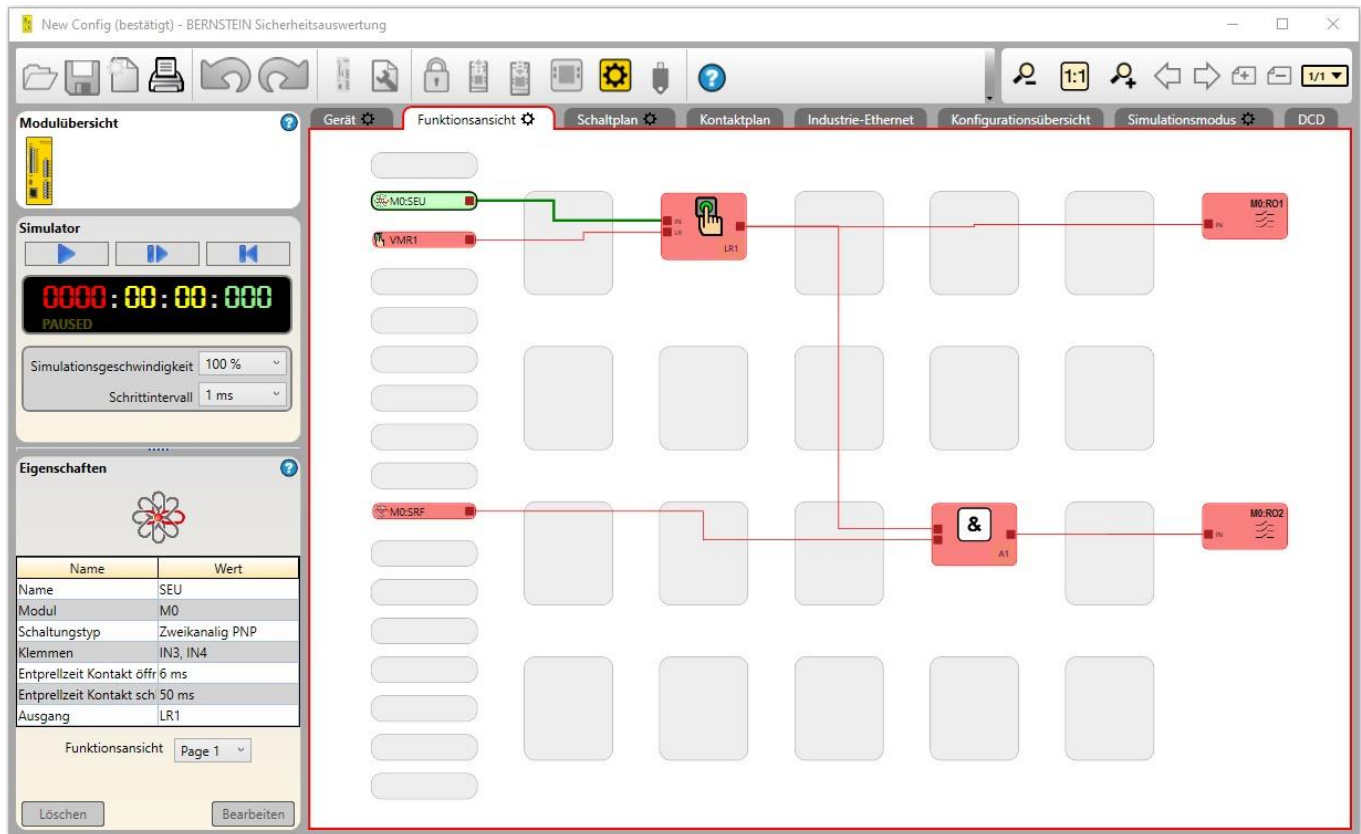


Abbildung 92: Simulationsmodus: Registerkarte Funktionsansicht

## 8.15.1 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:

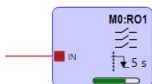


Abbildung 93: Sicherheitsausgang im Modus für zeitgesteuerte Ausschaltverzögerung

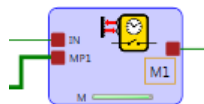


Abbildung 94: Muting-Block im Modus für zeitgesteuertes Muting

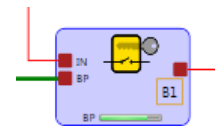


Abbildung 95: Überbrückungsblock im Modus für zeitgesteuerte Überbrückung

**Anmerkung:** Das Mneben der Statusleiste gibt das zeitgesteuerte Muting an.

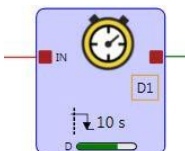


Abbildung 96: Verzögerungsblock



## 8.16 Referenzsignale



**Wichtig:** Die Konfigurationssoftware enthält Referenzsignale, die den Zustand der Ausgänge, Eingänge 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 diese Auswertung 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 96** auf Seite 114 zeigt, wie ein Sicherheitsausgang einen anderen Sicherheitsausgang steuern kann. Wenn manueller Reset **M0:MR1** gewählt wird, wird dadurch Sicherheitsausgang **M0:RO2** eingeschaltet. Dieser schaltet daraufhin Sicherheitsausgang **M0:RO1** ein.

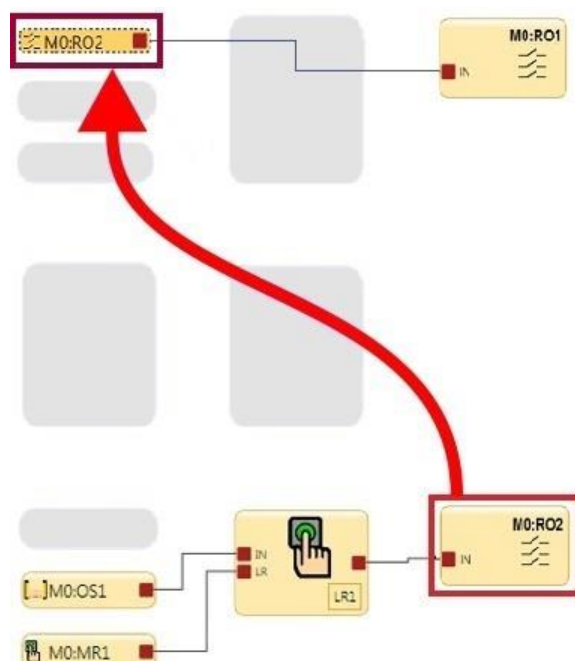


Abbildung 97: Von einem anderen Sicherheitsausgang gesteuerter Sicherheitsausgang

## 9. Systemüberprüfung

### 9.1 Zeitplan für vorgeschriebene Überprüfungen

Zur Überprüfung der Konfiguration und der Funktionsfähigkeit der Sicherheitsauswertung gehört die Prüfung 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.



**WARNUNG: Die Maschine nicht einsetzen, solange das System nicht richtig funktioniert.**

**Wenn nicht alle diese Prüfungen durchgeführt werden können, ist von der Benutzung der sicheren Maschinensteuerung abzusehen, dass dieses Gerät der BERNSTEIN AG enthält, bis der Defekt bzw. das Problem behoben wurde. Der Versuch, die sichere Maschinensteuerung unter derartigen Bedingungen zu benutzen, kann schwere oder tödliche Verletzungen zur Folge haben.**

Zur Überprüfung des Betriebs der Sicherheitsauswertung und der Funktionalität der vorgesehenen Konfiguration muss ein umfassender Test durchgeführt werden. [Setup vor der Inbetriebnahme](#), [Inbetriebnahme](#) und [regelmäßige Prüf-routinen](#) auf Seite 116 soll bei der Aufstellung einer konfigurationsspezifischen Checkliste für jede Anwendung helfen. Diese spezifische Checkliste muss dem Wartungspersonal für die Inbetriebnahmeprüfung und regelmäßigen Funktionstests zur Verfügung gestellt werden. Eine ähnliche, vereinfachte Checkliste für die tägliche Überprüfungsroutine sollte für den Bediener (bzw. für die autorisierte Person<sup>9</sup>) 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 qualifizierte Person<sup>9</sup> 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 der Sicherheitsauswertung.

**Regelmäßige (halbjährliche) Überprüfung:** Eine qualifizierte Person<sup>9</sup> 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 autorisierte Person<sup>9</sup> 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 Spannungsversorgung zur überwachten Maschine eingeschaltet wird. **Wenn diese Anweisungen nicht befolgt werden, können schwere oder tödliche Verletzungen die Folge sein.**

### 9.2 Inbetriebnahmeprüfung

**Überprüfen Sie vor der Durchführung des Verfahrens Folgendes:**

1. Keiner der Relaisausgangsanschlüsse des gesamten Sicherheitsauswertungssystems darf mit der Maschine verbunden sein.
2. 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.

<sup>9</sup> Unter [Glossar](#) auf Seite 164 finden Sie Definitionen.

## 9.2.1 Überprüfung des Systembetriebs

Die Inbetriebnahmeprüfung muss von einer qualifizierten Person durchgeführt werden.<sup>10</sup> Sie darf erst nach der Konfiguration der Sicherheitsauswertung und nach der sachgemäßen Installation und Konfiguration der mit den Eingängen der Auswertung verbundenen Sicherheitssysteme und Schutzeinrichtungen ausgeführt werden (siehe [Optionen für Sicherheitseingänge](#) auf Seite 21 und die einschlägigen Normen).

Die Inbetriebnahmeprüfung muss in den folgenden beiden Fällen durchgeführt werden:

1. Wenn die Sicherheitsauswertung 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 der Sicherheitsauswertung dauerhaft gewährleistet wird (siehe [Zeitplan für vorgeschriebene Überprüfungen](#) auf Seite 115).

**Während des ersten Teils der Inbetriebnahmeprüfung müssen die Sicherheitsauswertung und angeschlossene Sicherheitssysteme überprüft werden, ohne dass die Spannungsversorgung zum Maschinenantrieb hergestellt wurde.** Die endgültigen Anschlüsse an den Maschinenantrieb dürfen erst vorgenommen werden, nachdem diese Systeme überprüft worden sind.

**Folgendes überprüfen:**

- **Die Leitungen der Sicherheitsausgänge sind isoliert** (d. h. nicht untereinander und nicht zu anderen Stromkreisen 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 45 und in den Schaltplänen angegeben.
- Die korrekte Konfigurationsdatei für Ihre Anwendung wurde in der Sicherheitsauswertung installiert.
- Alle Ein- und Ausgangsklemmen wurden gemäß den entsprechenden Abschnitten verbunden und erfüllen die NEC-Vorschriften sowie die örtlichen Vorschriften für elektrische Anschlüsse.

Dadurch wird ermöglicht, dass die Sicherheitsauswertung und die angeschlossenen Sicherheitssysteme separat überprüft werden können, bevor die Spannungsversorgung zum Maschinenantrieb hergestellt wird.

## 9.2.2 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 (die Sicherheitsauswertung muss eingeschaltet und mit einem USB-Kabel an den PC angeschlossen sein).

### Hochlaufkonfiguration

Bei der Netzeinschaltung schalten sich die mit Zweihandsteuerungs-, Überbrückungs- oder Zustimmungsfunktionen 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.

#### 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. 5 Sekunden eingeschaltet werden (Ausgänge mit aktivierter Einschaltverzögerung schalten sich möglicherweise später ein).

<sup>10</sup> Für Definitionen siehe [Glossar](#) auf Seite 164.

### Bei Konfiguration für manuelle Netzeinschaltung

Überprüfen Sie, ob alle Sicherheitsausgänge nach der Netzeinschaltung AUS bleiben.

Warten 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 Sicherheitsauswertungen muss sorgfältig beurteilt und getestet werden, um sicherzustellen, dass eine Unterbrechung der Spannungsversorgung für ein Sicherheitsschaltgerät, die Sicherheitsauswertung oder das invertierte Eingangssignal von einem Sicherheitsschaltgerät 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 133.

## Betrieb der Sicherheitsschaltgeräte (Not-Aus-Schalter, Seilzugschalter, Optosensor, Sicherheitsmatte, Schutzhalt)

1. Betätigen Sie bei eingeschalteten zugehörigen Sicherheitsausgängen jedes Sicherheitsschaltgerät einzeln jeweils ein Mal.
2. Stellen Sie sicher, dass sich jeder zugehörige Sicherheitsausgang mit der richtigen Ausschaltverzögerung, so weit zutreffend, ausschaltet.
3. Während sich die Sicherheitseinrichtung im Ein-Zustand befindet:
  - **Falls ein Sicherheitsschaltgerät 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 Sicherheitseinrichtungen immer unter Beachtung der Empfehlungen des Herstellers der jeweiligen Einrichtung.

Bei der nachfolgenden Abfolge der Schritte gilt: Gehört eine bestimmte Funktion oder Einrichtung 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 Sicherheitseinrichtung 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 Sicherheitseinrichtung 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 Spannungsversorgung der Sicherheitsauswertung 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 Sicherheitseinrichtungen im Ein-Zustand befinden.
5. Schalten Sie die Spannungsversorgung zur Sicherheitsauswertung ein.
6. Überprüfen Sie, dass sich der Sicherheitsausgang einschaltet und dass ein Muting-Zyklus beginnt.
7. Wiederholen Sie diesen Test mit der mutingfähigen Sicherheitseinrichtung 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.

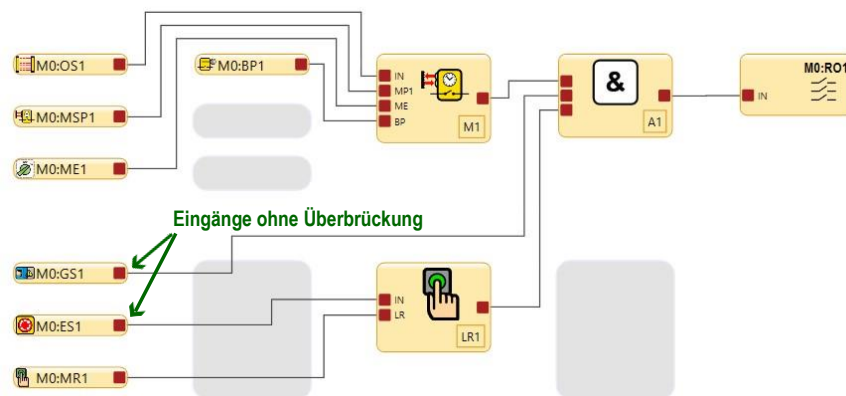


Abbildung 98: Setup: Eingänge ohne Überbrückung

## 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 aktiver Ausschaltverzögerungszeit den Eingang in den Ein-Zustand und prüfen Sie, ob der Sicherheitsausgang eingeschaltet ist und bleibt.



## Ausschaltverzögerungsfunktion für Sicherheitsausgänge – Eingang zum Abbruch einer Zeitverzögerung

Aktivieren Sie den Eingang zum Abbruch der Zeitverzögerung, während sich die zugehörigen Eingänge im Aus-Zustand befinden und während die Ausschaltverzögerung des Sicherheitsausgangs aktiv ist, 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

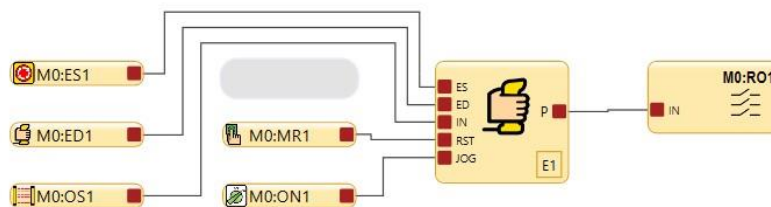


Abbildung 99: Setup: Zustimmtasterfunktion ohne sekundären Weiterschaltausgang

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-Halt- 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

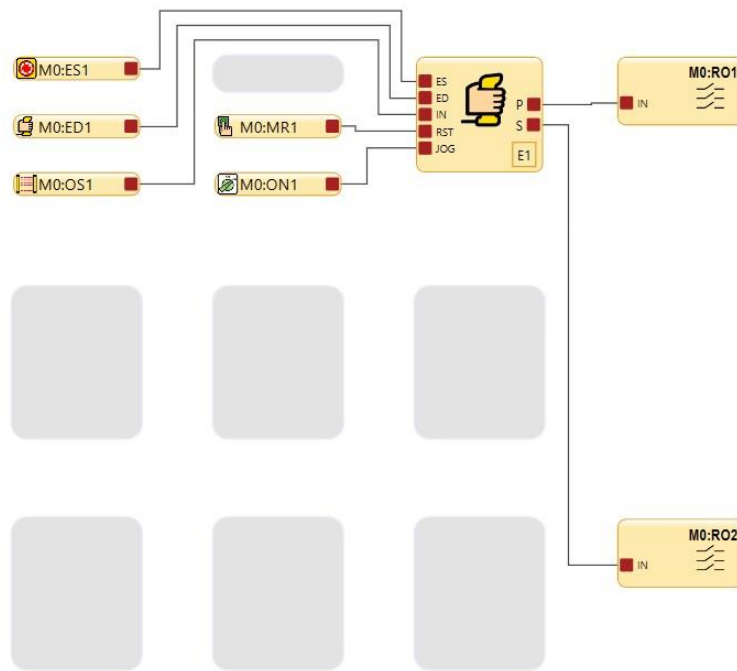


Abbildung 100: Setup: Zustimmtasterfunktion - mit Weiterschaltfunktion am Sekundärausgang

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.

# 10. Informationen zum Status und zum Betrieb

Die Sicherheitsauswertung SCR P kann über die Software beobachtet werden, um den Status dauerhaft zu überwachen.

## 10.1 Status der LED-Anzeigen am SCR P

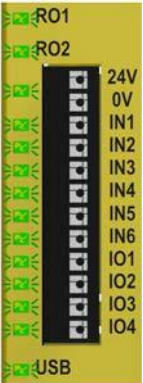
Anhand der folgenden Tabelle lässt sich der Status der Sicherheitsauswertung feststellen. Solange die Sicherheitsauswertung nicht ausgeschaltet wird, sind die LEDs immer eingeschaltet.

LED	Status	Bedeutung
Alle	Aus	Initialisierungs-Modus
	<b>Abfolge:</b> Grün EIN für 0,5 s Rot EIN für 0,5 s Aus für min. 0,5 s	Eingeschaltet
Versorgung/Fehler (1)	Grün konstant	24 V DC verbunden
	Grün blinkend	Konfigurations- oder manueller Netzeinschaltungsmodus Konfiguration über SCR P-FPS: Spannungsversorgung aus- und wiedereinschalten
	Rot blinkend	Sperrzustand
USB (1)	Grün konstant	USB-Kabel verbunden oder SCR P-FPS eingesteckt
	Grün blinkend	Sicherheitsauswertung im Werkszustand; weder USB-Kabel angeschlossen noch SCR P-FPS eingesteckt
	Grün schnell blinkend für 3 s, dann konstant	Konfiguriertes (gesperrtes oder entsperrtes) SCR P-FPS in eine Sicherheitsauswertung im Werkszustand eingesteckt; Konfiguration, Netzwerkeinstellungen und Passwörter werden vom SCR P-FPS auf die Sicherheitsauswertung übertragen
	Grün blinkend für 3 s, dann konstant	Konfiguriertes und entsperrtes SCR P-FPS in eine konfigurierte Sicherheitsauswertung mit übereinstimmender Konfiguration und übereinstimmenden Passwörtern eingesteckt  <b>Anmerkung:</b> Wenn die Netzwerkeinstellungen nicht übereinstimmen, werden die Netzwerkeinstellungen von der Sicherheitsauswertung auf ein entsperrtes SCR P-FPS übertragen. Auf ein gesperrtes SCR P-FPS werden keine Netzwerkeinstellungen übertragen.
	Grün schnell blinkend für 3 s, dann rot blinkend	Konfiguriertes und verriegeltes SCR P-FPS in eine konfigurierte Sicherheitsauswertung mit übereinstimmender Konfiguration und übereinstimmenden Passwörtern, aber nicht übereinstimmenden Netzwerkstellungen eingesteckt
	Rot konstant	Konfigurierte Sicherheitsauswertung; weder USB-Kabel angeschlossen noch SCR P-FPS eingesteckt
	Rot blinkend	Konfiguriertes (verriegeltes oder unverriegeltes) SCR P-FPS in eine konfigurierte Sicherheitsauswertung mit nicht übereinstimmender Konfiguration und nicht übereinstimmendem Passwort oder leeres SCR P-FPS in eine Sicherheitsauswertung eingesteckt
Eingänge (10)	Grün konstant	24 V DC und kein Fehler


LED	Status	Bedeutung
	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	Blinkt bei Datenübertragung	Verbindung hergestellt/Normalbetrieb
Aus	Aus	Hardwarefehler

Gelbe und grüne LED blinken synchron	Beschreibung
5-maliges Blinken und danach mehrmaliges kurzes Blinken.	Normaler Hochlauf
1 Blinken alle 3 Sekunden	BERNSTEIN AG 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	BERNSTEIN AG kontaktieren

PROFINET-Blinkbefehl	Bedeutung
<p>Alle LEDs blinken 4 Sekunden lang zweimal pro Sekunde.</p> 	<p>Die blinkenden LEDs geben an, dass das SCR P verbunden ist. Das ist das Ergebnis des Befehls „LED blinken“ vom PROFINET-Netzwerk.</p>

## 10.2 Livemodus-Informationen: Software

Um Echtzeitinformationen über den Run-Modus auf einem PC anzuzeigen, muss die Sicherheitsauswertung mit dem USB-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 107 erhalten Sie weitere Informationen.

## 10.3 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 Fehler/Reset (FR) Eingang am Sicherheitsausgang angeschlossene Reset-Eingang durchgeschaltet wird.

Systemfehler, wie zum Beispiel niedrige Versorgungsspannung, Übertemperatur oder an nicht zugewiesenen Eingängen erfasste Spannung, 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.

Ein System-Reset wird ausgeführt, um Sperrzustände zu beheben, die nicht mit Sicherheitseingängen oder -ausgängen in Verbindung stehen. Bei einem Sperrzustand handelt es sich um eine Reaktion der Sicherheitsauswertung, bei der er alle betroffenen Sicherheitsausgänge ausschaltet, wenn ein sicherheitsrelevanter Fehler erkannt wird. Zur Behebung dieses Zustands müssen alle Fehler beseitigt und ein System-Reset ausgeführt werden. Solange der Fehler, der den Sperrzustand verursacht hat, nicht behoben wurde, tritt der Sperrzustand nach dem System-Reset erneut ein.

Ein System-Reset ist unter den folgenden Bedingungen erforderlich:

1. Für den Wiederanlauf nach einem System-Sperrzustand
2. Zum Starten der Sicherheitsauswertung, nachdem eine neue Konfiguration heruntergeladen wurde

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. Wenn diese Anweisungen nicht befolgt werden, können schwere oder tödliche Verletzungen die Folge sein.**

## 10.4 Nach einem Sperrzustand

Zur Behebung eines Sperrzustands:

1. Befolgen Sie die empfohlenen Schritte und Überprüfungen in der [Fehlercode-Tabelle für SCR P](#) auf Seite 137
2. System-Reset durchführen
3. 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 BERNSTEIN AG (siehe [Reparaturen und Garantie](#) auf Seite 142).

## 10.5 SCR P: 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. 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.

3. Klicken Sie auf der Registerkarte **Geräte** unter der Sicherheitsauswertung auf . Das Fenster **Gerät hinzufügen** wird geöffnet.
4. Fügen Sie einen Not-Halt-Schalter hinzu und klicken Sie auf **OK**, um die Standardeinstellungen zu akzeptieren.
5. Klicken Sie auf .
6. Fügen Sie einen optischen Sensor hinzu und klicken Sie auf **OK**, um die Standardeinstellungen zu akzeptieren.
7. Klicken Sie auf .
8. Fügen Sie einen Schutztürschalter hinzu und klicken Sie auf **OK**, um die Standardeinstellungen zu akzeptieren.
9. Wechseln Sie zur Registerkarte **Schaltplan** und lesen Sie dort ab, welche Anschlüsse belegt sind.

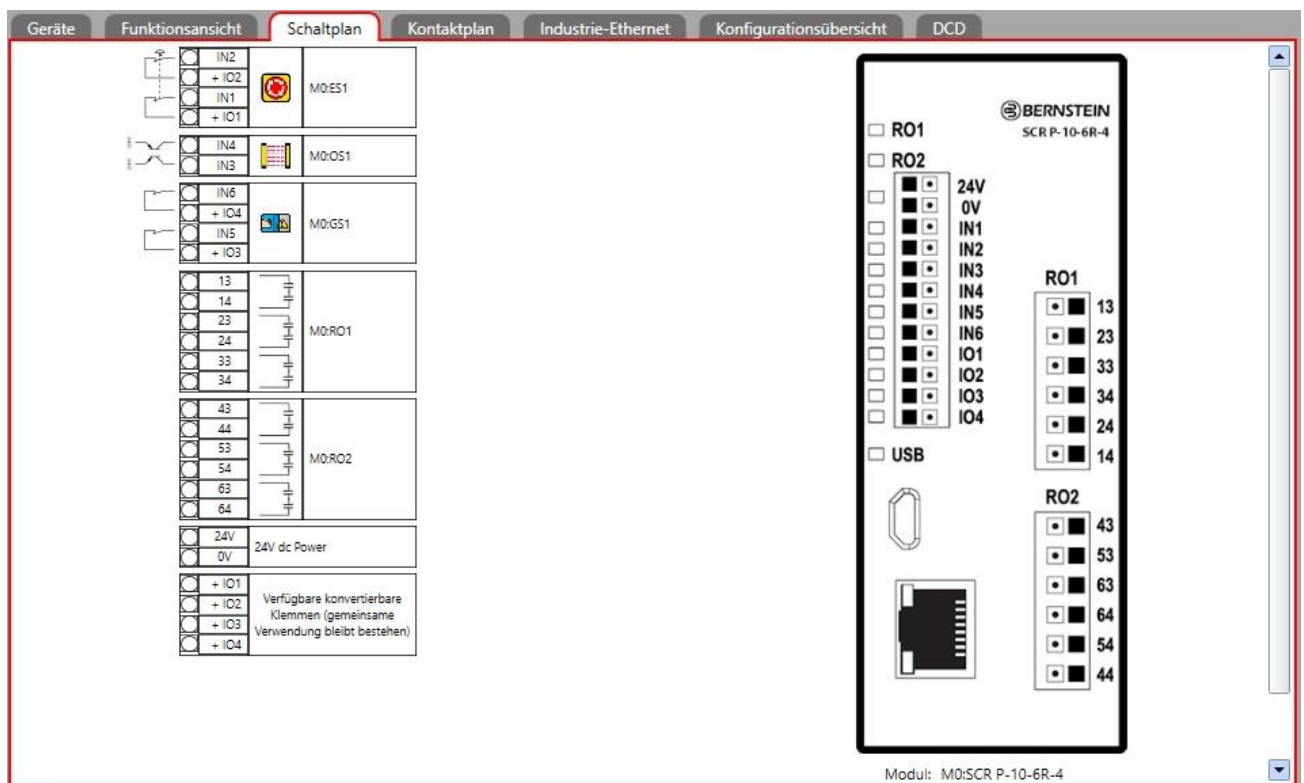


Abbildung 101: Registerkarte **Schaltplan** mit einem Not-Aus-Schalter, optischen Sensor und Schutztürschalter

10. Wechseln Sie zur Registerkarte **Geräte** und klicken Sie auf .
11. Fügen Sie einen zweiten Schutztürschalter hinzu und klicken Sie auf **OK**, um die Standardeinstellungen zu akzeptieren.

12. 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.

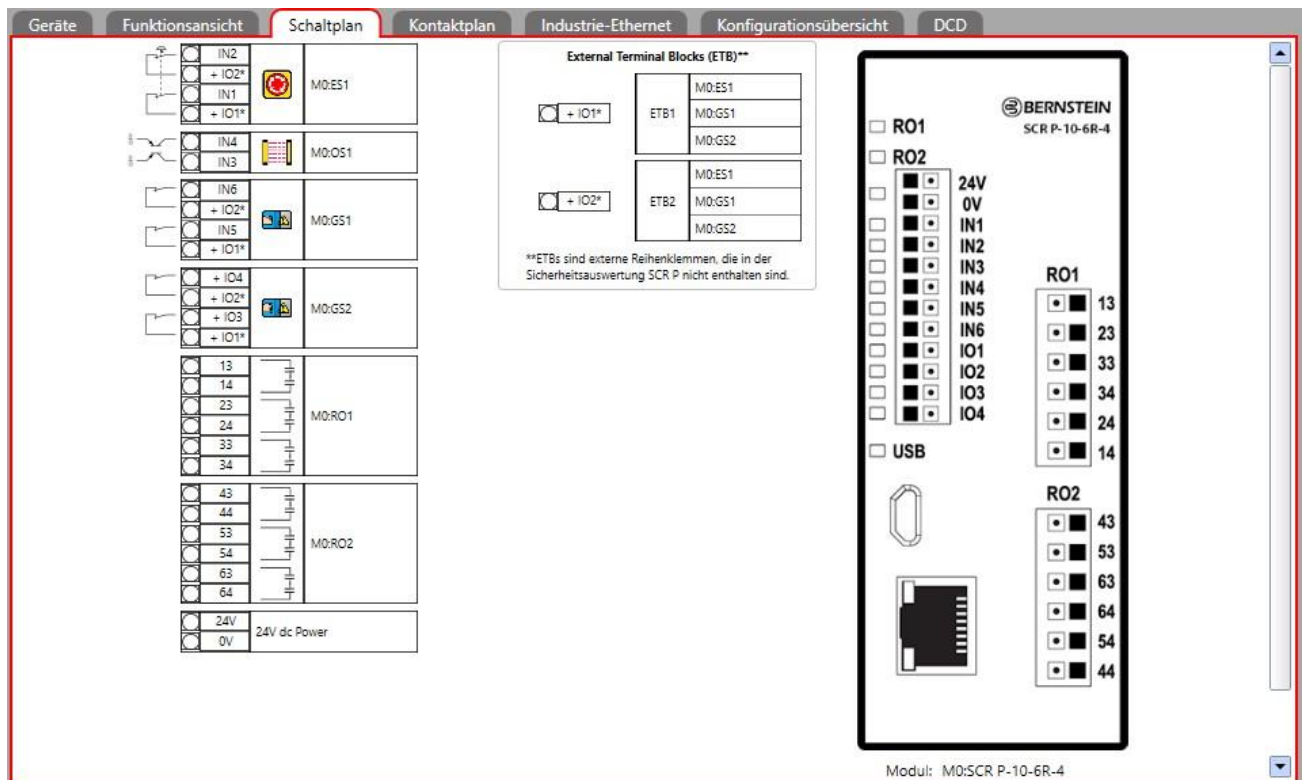


Abbildung 102: Registerkarte **Schaltplan** mit drei Not-Aus-Tastern und ETBs

## 10.6 Beispielkonfiguration für das SCR P 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. 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.

**Neues SCR P-Projekt beginnen**

Info

Konfigurationsname: New Config

Projekt: New Project

Autor:

Hinweise

Projektdatum: 21.04.2020

☒ Funktion für die automatische Optimierung von Anschlüssen deaktivieren

OK Abbrechen

Abbildung 103: Funktion für die automatische Optimierung von Anschlüssen deaktivieren ausgewählt

Das Projekt wird erstellt.

3. Klicken Sie auf der Registerkarte **Geräte** unter dem Sicherheitsauswertung auf . Das Fenster **Gerät hinzufügen** wird geöffnet.
4. Fügen Sie einen Not-Aus-Schalter hinzu und klicken Sie auf **OK**, um die Standardeinstellungen zu akzeptieren.
5. Klicken Sie auf .
6. Fügen Sie einen optischen Sensor hinzu und klicken Sie auf **OK**, um die Standardeinstellungen zu akzeptieren.
7. Klicken Sie auf .
8. Fügen Sie einen Schutztürschalter hinzu und klicken Sie auf **OK**, um die Standardeinstellungen zu akzeptieren.



9. Wechseln Sie zur Registerkarte **Schaltplan** und lesen Sie dort ab, welche Anschlüsse belegt sind.

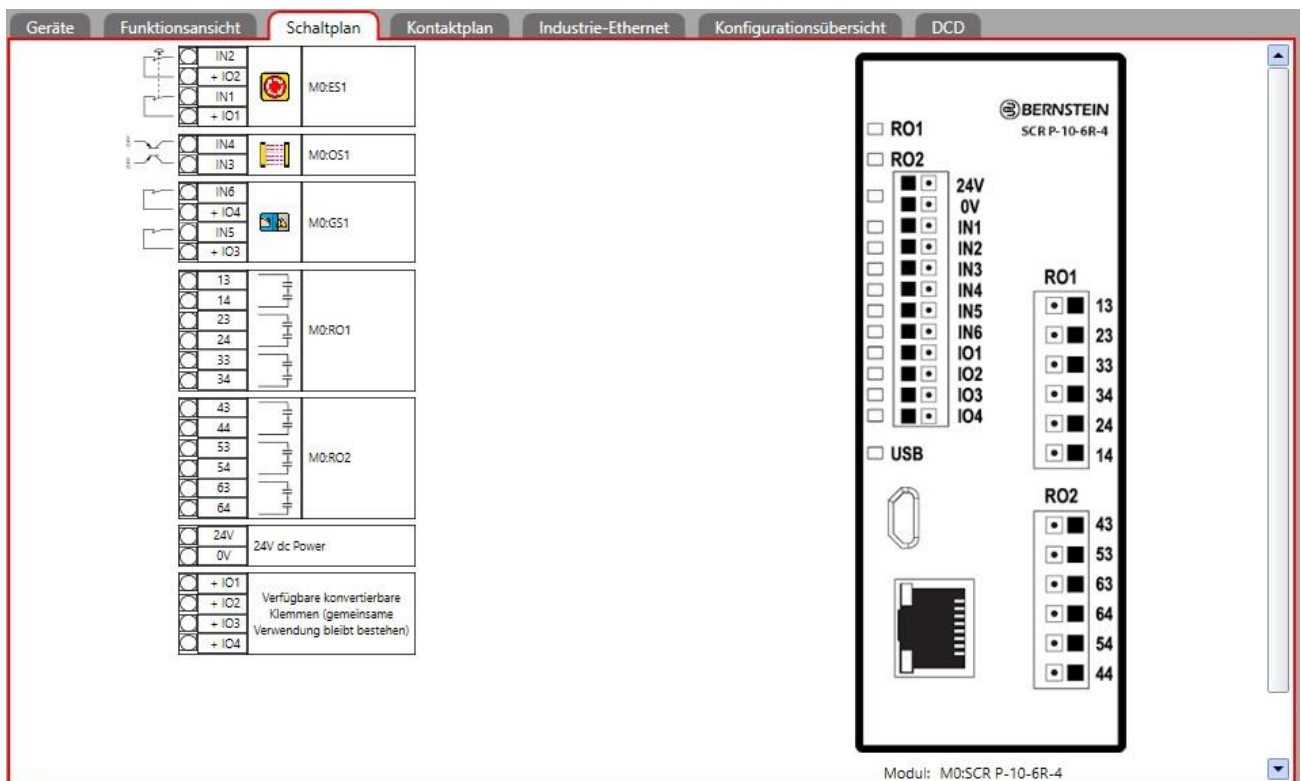


Abbildung 104: Registerkarte **Schaltplan** mit einem Not-Halt-Schalter, optischen Sensor und Schutztürschalter

10. 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.
11. 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.
12. Klicken Sie auf **Abbrechen**.
13. 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.

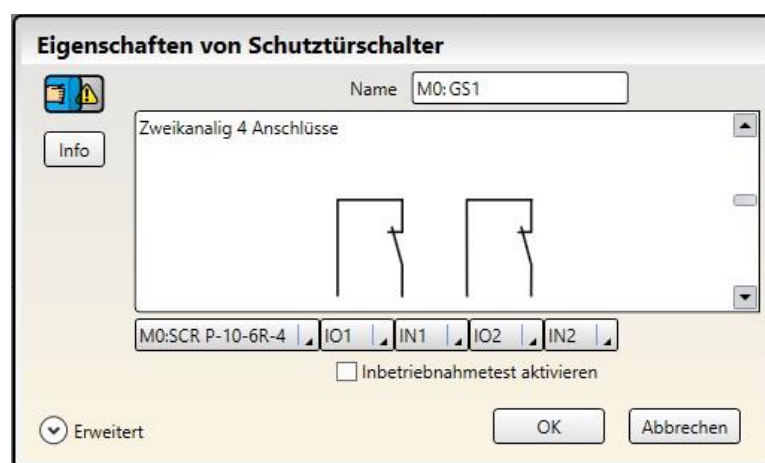


Abbildung 105: Schutztürschaltereigenschaften

- b) Klicken Sie auf **OK**.

14. 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.

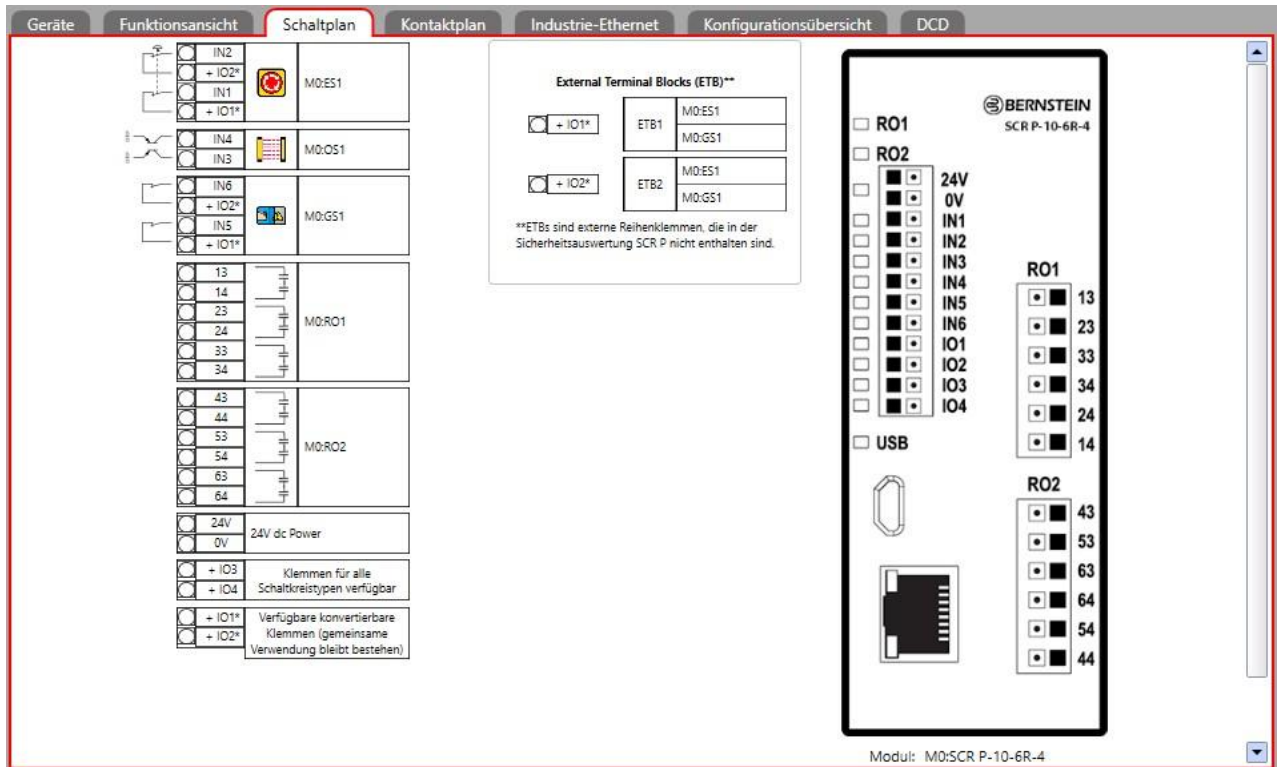


Abbildung 106: Registerkarte **Schaltplan** mit einem Not-Halt-Schalter, optischen Sensor, Schutztürschalter und ETBs

15. 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.
16. Fügen Sie einen zweiten Schutztürschalter hinzu und klicken Sie auf **OK**, um die Standardeinstellungen zu akzeptieren.

17. Wechseln Sie zur Registerkarte **Schaltplan**. Sie sehen jetzt, dass der zweite Schutztürschalter hinzugefügt wurde und dass kein weiterer ETB hinzugefügt wurde.

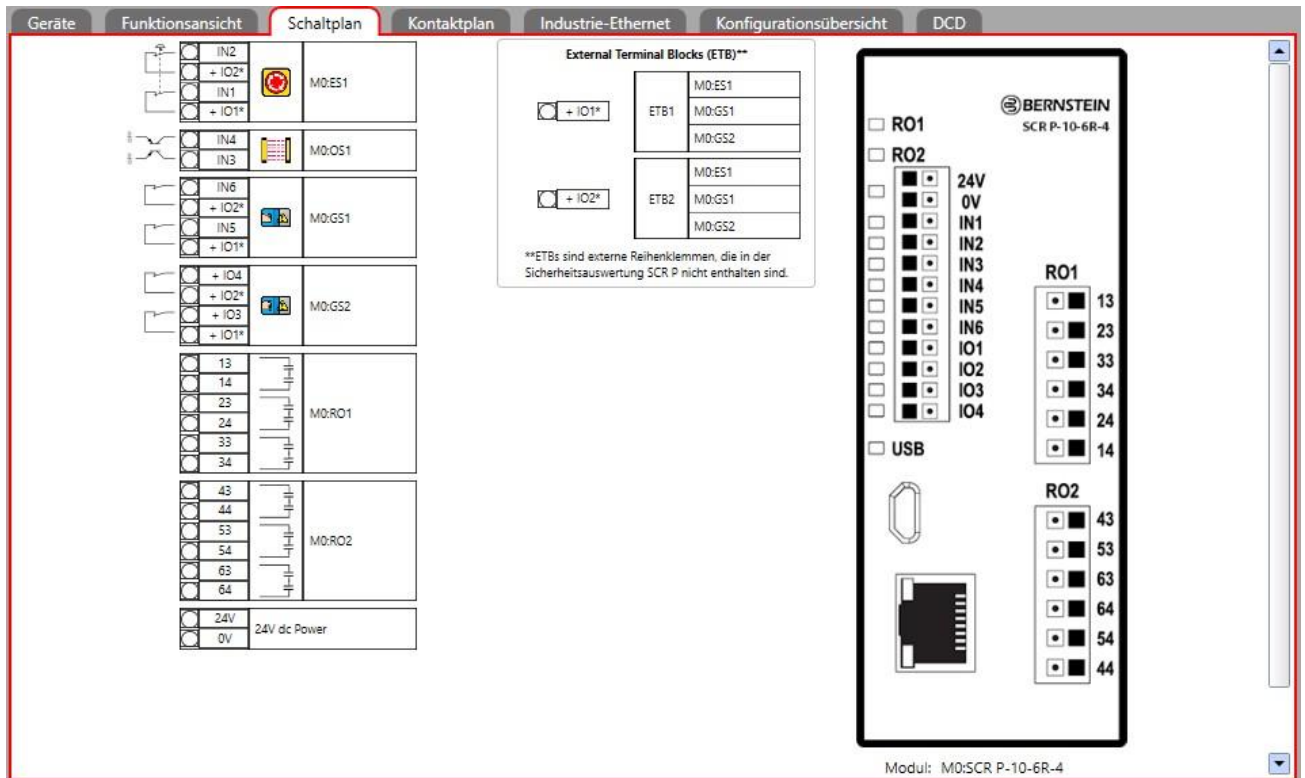


Abbildung 107: Registerkarte **Schaltplan** mit Not-Halt-Schalter, optischen Sensor, Schutztürschaltern und ETBs

## 10.7 SCR P unter Verwendung des SCR P-FPS

Mit einem SCR P-FPS haben Sie folgende Möglichkeiten:

1. Mehrere SCR P Sicherheitsauswertungen mit der gleichen Konfiguration schnell konfigurieren
2. Eine SCR P Sicherheitsauswertung gegen eine andere auswechseln (wobei das SCR P-FPS von der alten Sicherheitsauswertung verwendet wird)



**Anmerkung:** Zum Schreiben einer bestätigten Konfiguration in ein SCR P-FPS benötigen Sie das Programmierwerkzeug (SCR P-PA) und die Software von der BERNSTEIN AG. Dadurch ist der Zugriff auf befugtes Personal beschränkt.

1. Erstellen Sie die gewünschte Konfiguration in der Software.
2. Bestätigen Sie die Konfiguration, indem Sie sie auf ein SCR P hochladen.
3. Überprüfen und bestätigen Sie die Ergebnisse.  
Nach der Überprüfung und Bestätigung kann die Konfiguration gespeichert und vom SCR P verwendet werden.
4. Schreiben Sie die bestätigte Konfiguration mithilfe des Programmierwerkzeugs in das SCR P-FPS.



**Anmerkung:** Auf dem SCR P-FPS können nur bestätigte Konfigurationen gespeichert werden.

5. Beschriften Sie die Konfiguration, die Sie auf dem SCR P-FPS speichern.
6. Verbinden Sie die Spannungsquelle mit dem gewünschten SCR P (neue Sicherheitsauswertung oder Ersatz-Sicherheitsauswertung).
  - Gemäß den Werkseinstellungen weist eine grün leuchtende Betriebs-/Fehler-LED an der Sicherheitsauswertung SCR P zusammen mit einer grün blinkenden USB-LED darauf hin, dass das SCR P auf eine Konfiguration wartet.
  - Wurde das SCR P konfiguriert, leuchtet die Betriebs-/Fehler-LED grün und die USB-LED leuchtet rot.

7. Stecken Sie das SCR P-FPS in den Micro-USB-Port am SCR P ein.

#### Sicherheitsauswertung mit Werkseinstellungen

- Die USB-LED blinkt 3 Sekunden lang und leuchtet dann konstant. Die Konfiguration, die Netzwerkeinstellungen und die Passwörter werden dann automatisch auf die Sicherheitsauswertung heruntergeladen. Danach blinkt die Betriebs-/Fehler-LED grün, um darauf hinzuweisen, dass die Sicherheitsauswertung darauf wartet, aus- und wiedereingeschaltet zu werden.

#### Konfigurierte Sicherheitsauswertung


- Wenn die Konfiguration und die Passwörter an der Sicherheitsauswertung und am SCR P-FPS 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 SCR P-FPS übertragen, sofern das SCR P-FPS nicht gesperrt ist. Ist das SCR P-FPS gesperrt, wechselt das SCR P in einen Sperrzustand.
  - Wenn die Konfiguration oder die Passwörter an der Sicherheitsauswertung und am SCR P-FPS nicht übereinstimmen, blinkt die USB-LED rot. Wird das SCR P-FPS nicht innerhalb von 3 Sekunden von der Sicherheitsauswertung getrennt, blinken die Betriebs-/Fehler- und die USB-LED rot und das SCR P wechselt wegen der Unstimmigkeit in einen Sperrzustand.
8. Das Gerät aus- und wiedereinschalten.  
Die Betriebs-/Fehler-LED leuchtet grün, die USB-LED leuchtet grün (wenn das SCR P-FPS weiterhin verbunden ist) oder rot (wenn kein SCR P-FPS oder kein USB-Kabel angeschlossen ist), und die Eingangs- und Ausgangs-LEDs zeigen den tatsächlichen Eingangsstatus an.

Die Sicherheitsauswertung ist für die Inbetriebnahme bereit. Siehe [Inbetriebnahmeprüfung](#) auf Seite 115.

## 10.8 SCR P Sicherheitsauswertung auf die Werkseinstellungen zurücksetzen

Mit dem folgenden Verfahren können Sie die Sicherheitsauswertung SCR P wieder auf die Werkseinstellungen zurücksetzen.

Die Sicherheitsauswertung SCR P muss eingeschaltet und über das USB-Kabel mit dem PC verbunden sein.

1. Klicken Sie auf .
2. Klicken Sie auf **Werkseinstellungen wiederherstellen**.  
Daraufhin wird eine Warnmeldung 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 SCR P wird auf die Werkseinstellungen zurückgesetzt und ein Bestätigungsfenster wird angezeigt.
5. Klicken Sie auf **OK**.  
Die Werkseinstellungen sind damit wiederhergestellt.

## 10.9 Werkseinstellungen

In der folgenden Tabelle sind einige der Werkseinstellungen für den Sicherheitsauswertung und die Software aufgeführt.

Einstellung	Werkseinstellung	Produkt
AVM-Funktion	50 ms	SCR P
Ausschaltentprellzeit	6 ms	SCR P
EDM	Keine EDM-Überwachung	SCR P
Funktionsblock: Überbrückungsblock – Standardknoten	IN, BP	SCR P
Funktionsblock: Überbrückungs-Zeitlimit	1 s	SCR P
Funktionsblock: Verzögerungsblock – Standardknoten	IN	SCR P
Funktionsblock: Verzögerungsblock – Ausschaltverzögerung	100 ms	SCR P
Funktionsblock: Zustimmungstasterblock – Standardknoten	ED, IN, RST	SCR P
Funktionsblock: Zustimmungstasterblock – Zeitlimit	1 s	SCR P

Funktionsblock: Latch-Reset-Block – Standardknoten	IN, LR	SCR P
Funktionsblock: Mutingblock – Standardknoten	IN, MP1	SCR P
Funktionsblock: Mutingblock – Zeitlimit	30 s	SCR P

Einstellung	Werkseinstellung	Produkt
Funktionsblock: Zweihandsteuerungsblock – Standardknoten	TC	SCR P
Industrie-Ethernet: Zeichenfolge (EtherNet/IP und PCCC-Protokoll)	32 Bit	SCR P
Netzwerkeinstellungen: Gateway-Adresse	0.0.0.0	SCR P
Netzwerkeinstellungen: IP-Adresse	192.168.0.128	SCR P
Netzwerkeinstellungen: Verbindungsgeschwindigkeit und Duplexmodus	Automatische Aushandlung	SCR P
Netzwerkeinstellungen: Subnetzmaske	255.255.255.0	SCR P
Netzwerkeinstellungen: TCP-Port	502	SCR P
Einschaltentprellzeit	50 ms	SCR P
Anlaufmodus	Normal	SCR P
Sicherheitsausgänge	Automatischer Reset (Schaltmodus)	SCR P
Sicherheitsausgänge: Anlaufmodus	Normal	SCR P
Sicherheitsausgänge: Teilen (Sicherheitsausgänge)	Paarweise Funktion	SCR P
Simulationsmodus: Simulationsgeschwindigkeit	1	SCR P
Automatische Optimierung von Anschlüssen	Aktiviert	SCR P
Signallogik für Statusausgänge	Aktiv = PNP ein	SCR P

# 11. Fehlerbehebung

Die Sicherheitsauswertung wurde für hohe Beständigkeit gegen eine Vielzahl von elektrischen Störquellen, die in industriellen Umgebungen anzutreffen sind, entwickelt und entsprechend getestet. Starke elektrische Störquellen, die elektromagnetische und hochfrequente Störsignale jenseits 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 Kabel an jedem einzelnen Anschluss sicher befestigt sind
- Ob sich neben der Sicherheitsauswertung oder entlang von Leitungen, die an der Auswertung angeschlossen sind, Hochspannungs-Störquellen, Hochfrequenz-Störquellen oder Hochspannungsleitungen befinden
- Geeignete Überspannungsbegrenzer an den Ausgangslasten angebracht sind
- Ob die Umgebungstemperatur der Sicherheitsauswertung innerhalb des Nennbereichs für Umgebungstemperatur liegt (siehe [Spezifikationen und Anforderungen](#) auf Seite 11)

## 11.1 Software: Fehlerbehebung

### Schaltfläche Livemodus ist nicht verfügbar (grau abgeblendet)

1. Achten Sie darauf, dass das USB-Kabel sowohl mit dem Computer als auch mit der Sicherheitsauswertung verbunden ist.



**Anmerkung:** Die Verwendung des BERNSTEIN USB-Kabels ist vorzuziehen. Bei der Verwendung anderer USB-Kabel müssen Sie darauf achten, dass das Kabel einen Datenleiter enthält. Viele Handyaufgeladegeräte haben keinen Datenleiter.

2. Überprüfen Sie, ob die Sicherheitsauswertung korrekt installiert ist; siehe [Überprüfen der Treiberinstallation](#) auf Seite 135.
3. Beenden Sie die Software.
4. Trennen Sie die Sicherheitsauswertung und verbinden Sie sie erneut.
5. Starten Sie die Software.

### Die Konfiguration kann nicht von der Sicherheitsauswertung gelesen oder nicht an die Sicherheitsauswertung gesendet werden (Schaltflächen grau abgeblendet).

1. Achten Sie darauf, dass der **Livemodus** deaktiviert ist.
2. Achten Sie darauf, dass das USB-Kabel sowohl mit dem Computer als auch mit der Sicherheitsauswertung verbunden ist.



**Anmerkung:** Die Verwendung des BERNSTEIN USB-Kabels ist vorzuziehen. Bei der Verwendung anderer USB-Kabel müssen Sie darauf achten, dass das Kabel einen Datenleiter enthält. Viele Ladekabel für Mobiltelefone haben keinen Datenleiter.

3. Überprüfen Sie, ob die Sicherheitsauswertung korrekt installiert ist; siehe [Überprüfen der Treiberinstallation](#) auf Seite 135.
4. Beenden Sie die Software.
5. Trennen Sie die Sicherheitsauswertung und verbinden Sie sie 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.

3. **Sicherheitsausgänge** werden statisch eingefügt und lassen sich nicht verschieben. Wenn man eine **Referenz auf einen Sicherheitsausgang** erstellt, kann diese an eine beliebige Stelle im linken und mittleren Bereich verschoben werden.
4. Die **Sicherheits-** und **nicht sicherheitsrelevanten Eingänge** können an eine beliebige Stelle im linken und mittleren Bereich verschoben werden.
5. Die **Funktions-** und **Logikblöcke** können nur innerhalb des mittleren Bereichs verschoben werden.

## 11.2 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.

Software-code	Fehler
A.1	Durch diese Verbindung entsteht eine Schleife in der Verarbeitung der Sicherheitssignale.
A.2	Von diesem Block ist bereits eine Verbindung vorhanden.
A.3	Ein Block darf nicht mit sich selbst verbunden werden.
B.2	Dieser Überbrückungsblock ist mit dem Zweihandsteuerungsblock verbunden. Sie können mit dem <b>IN</b> -Knoten nur einen Zwei-handsteuerungseingang verbinden.
B.3	Dieser Überbrückungsblock ist bereits mit einem anderen Block verbunden.
B.4	Dieser Überbrückungsblock ist mit dem <b>TC</b> -Knoten eines Zweihandsteuerungsblocks verbunden und kann nicht mit anderen Blöcken verbunden werden.
B.5	Der Zweihandsteuerungsblock kann nicht mit dem <b>IN</b> -Knoten von diesem Überbrückungsblock verbunden werden, weil bei ihm die Option „Ausgang schaltet aus, wenn beide Eingänge (IN und BP) ein sind“ aktiviert ist.
B.6	Der <b>IN</b> -Knoten eines Überbrückungsblocks kann nicht mit Eingängen für Not-Halt-Schalter und Seilzugschalter verbunden werden.
B.7	Der <b>IN</b> -Knoten eines Überbrückungsblocks kann nicht über andere Blöcke mit Eingängen für Not-Halt-Schalter und Seilzugschalter verbunden werden.
C.1	Mit dem <b>CD</b> -Knoten kann nur ein Eingang zum Abbruch einer Aus-Verzögerung verbunden werden.
C.2	Ein Eingang zum Abbruch einer Aus-Verzögerung kann nur mit dem <b>CD</b> -Knoten eines Sicherheitsausgangs verbunden werden.
D.1	Dieser Eingang für die externe Geräteüberwachung ist für eine zweikanalige 2-Klemmen-Schaltung konfiguriert und kann nur mit dem <b>EDM</b> -Knoten eines Sicherheitsausgangs verbunden werden.
E1	Die Ausgangsknoten für einen Zustimmungstaster-Block ( <b>P</b> oder <b>S</b> ) können nur mit dem <b>IN</b> -Knoten eines Sicherheitsausgangs verbunden werden.
E.2	Der <b>IN</b> -Knoten eines Zustimmungstaster-Blocks kann nicht mit Eingängen für Not-Aus-Schalter und Seilzugschalter verbunden werden.
E.3	Der <b>ED</b> -Knoten eines Zustimmungstaster-Blocks kann nur mit dem Eingang für einen Zustimmungstaster verbunden werden.
E.4	Der <b>ED</b> -Knoten eines Zustimmungstaster-Blocks kann nicht über andere Blöcke mit Eingängen für Not-Aus-Schalter und Seilzugschalter verbunden werden.
E.5	Ein Zustimmungstaster-Block, bei dem ein Eingang für eine Zweihandsteuerung mit dem <b>IN</b> -Knoten verbunden ist, kann nicht mit einem Sicherheitsausgang verbunden werden, bei dem als <i>Verzögerung des Sicherheitsausgangs</i> die Einstellung „Aus-Verzögerung“ gewählt ist.
E.6	Der sekundäre Ausgangsknoten <b>S</b> eines Zustimmungstaster-Blocks kann nur mit dem <b>IN</b> -Knoten eines Sicherheitsausgangs verbunden werden.
F.1	Not-Halt- und Seilzugschaltereingänge können nicht gemutet werden.
F.2	Not-Halt- und Seilzugschaltereingänge können nicht mit einem Latch-Reset-Block verbunden werden, der an einen Muting-Block angeschlossen ist.



Software-code	Fehler
F.3	Ein Latch-Reset-Block, der mit einem Eingang für einen Not-Halt- oder Seilzugschalter verbunden ist, kann nicht an einen Muting-Block angeschlossen werden.
G.1	Nur ein manueller Reset-Eingang kann mit dem <b>FR</b> -Knoten eines Sicherheitsausgangs verbunden werden.
G.2	Nur ein manueller Reset-Eingang kann mit dem <b>LR</b> -Knoten eines Latch-Reset-Blocks oder eines Sicherheitsausgangs verbunden werden.
G.3	Nur ein manueller Reset-Eingang kann mit dem <b>RST</b> -Knoten eines Zustimmungstaster-Blocks verbunden werden.
G.4	Ein manueller Reset-Eingang kann nur mit dem <b>LR</b> - und dem <b>FR</b> -Knoten eines Sicherheitsausgangs, dem <b>LR</b> -Knoten eines Latch-Reset-Blocks, dem <b>RST</b> -Knoten eines Zustimmungstaster-Blocks und dem <b>SET</b> - und <b>RST</b> -Knoten des Flip-Flop-Blocks verbunden werden.
H.1	Dieser Latch-Reset-Block ist bereits mit einem anderen Funktionsblock verbunden.
H.2	Der Latch-Reset-Block kann nicht mit anderen Eingangsknoten verbunden werden.
I.1	Nur die Eingänge für Muting-Sensorpaar, Optosensor, Schutztürschalter, Schaltmatte oder Schutzhaltschalter können, mit dem <b>MP1</b> - und dem <b>MP2</b> -Knoten eines Muting-Blocks oder mit dem <b>MP1</b> -Knoten eines Zweihandsteuerungsblocks verbunden werden.
I.2	Der <b>MP1</b> - und der <b>MP2</b> -Knoten eines Muting-Blocks und der <b>MP1</b> -Knoten eines Zweihandsteuerungsblocks können mit Eingängen verbunden werden, die nur zweikanalige Schaltungen verwenden.
I.3	Der Eingang für Muting-Sensorpaar kann nur mit dem <b>MP1</b> - und dem <b>MP2</b> -Knoten eines Muting-Blocks oder mit dem <b>MP1</b> -Knoten eines Zweihandsteuerungsblocks verbunden werden.
J.1	Ein Zweihandsteuerungsblock kann nur mit einem Zustimmungstaster-Block ( <b>IN</b> -Knoten) oder einem Sicherheitsausgang ( <b>IN</b> -Knoten) verbunden werden.
J.3	Nur Zweihandsteuerungseingänge oder Überbrückungsblöcke mit daran angeschlossenen Zweihandsteuerungseingängen können mit dem <b>TC</b> -Knoten eines Zweihandsteuerungsblocks verbunden werden.
K.1	Ein Zweihandsteuerungseingang kann nur mit einem Zweihandsteuerungsblock ( <b>TC</b> -Knoten) oder einem Überbrückungsblock ( <b>IN</b> -Knoten) verbunden werden.
K.2	Ein Sicherheitsausgang, bei dem für die <i>Verzögerung des Sicherheitsausgangs</i> die Einstellung „Aus-Verzögerung“ gewählt ist, kann nicht mit einem Zweihandsteuerungsblock verbunden werden.
K.3	Ein Sicherheitsausgang, bei dem für die <i>Verzögerung des Sicherheitsausgangs</i> die Einstellung „Aus-Verzögerung“ gewählt ist, kann nicht über einen Zustimmungstaster-Block mit einem Zweihandsteuerungsblock verbunden werden.
L.1	Dieser Sicherheitsausgang ist aufgrund eines Statusausgangs deaktiviert, der seine Klemmen verwendet.
L.2	Der <b>IN</b> -Knoten eines Sicherheitsausgangs kann nicht mit den Eingängen für externe Geräteüberwachung, einstellbare Ventilüberwachung, Muting-Sensorpaar, Überbrückungsschalter, manuellen Reset, Muting-Freigabe oder Abbruch der Aus-Verzögerung verbunden werden.
L.3	Ein Sicherheitsausgangsblock, bei dem die <i>LR- (Latch-Reset-)</i> Funktion aktiviert ist, kann nicht mit Zweihandsteuerungsblöcken oder Zustimmungstaster-Blöcken verbunden werden.
L.4	Ein Sicherheitsausgangsblock, bei dem für den <i>Anlaufmodus</i> die Einstellung „Manueller Reset“ gewählt ist, kann nicht mit Zweihandsteuerungsblöcken oder Zustimmungstaster-Blöcken verbunden werden.

## 11.3 Überprüfen der Treiberinstallation

### 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 **Safety Controller**, gefolgt von einer COM-Anschlussnummer (z. B. COM3). Der Eintrag darf weder ein Ausrufezeichen noch ein rotes x 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

### SCR P-FPS Treiber

1. Erweitern Sie das Dropdown-Menü **USB-Controller**.
2. Suchen Sie **SC Programmier A** und **SC Programmier B**. Keiner dieser beiden Einträge darf ein Ausrufezeichen, ein rotes x 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.

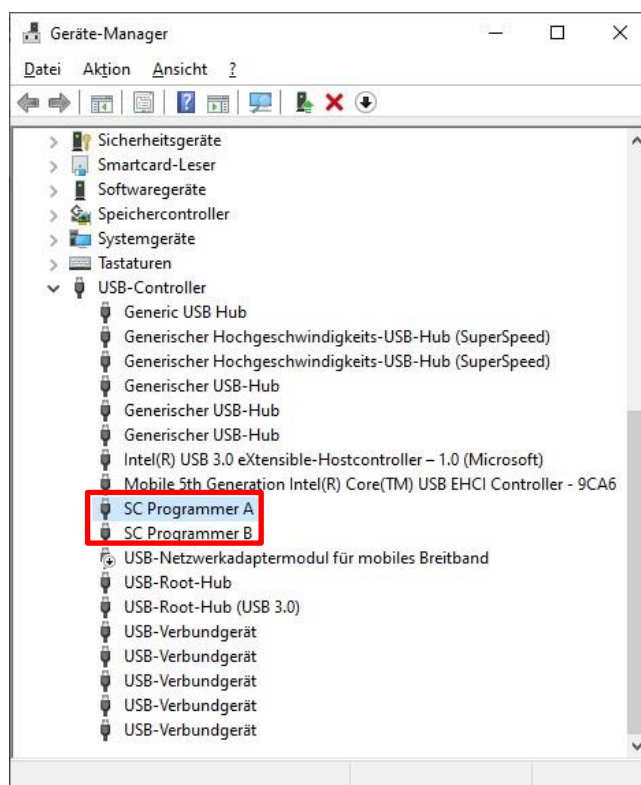


Abbildung 108: SCR P-FPS -Treiber korrekt installiert

**So beheben Sie die durch ein Ausrufezeichen, ein rotes x 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 der weiteren Fehlerbehebung 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 von der Sicherheitsauswertung 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 die Sicherheitsauswertung 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 der BERNSTEIN AG.

## 11.4 Fehlersuche und -behebung

Je nach Konfiguration kann die Sicherheitsauswertung unterschiedliche Eingangs-, Ausgangs- und Systemfehler erkennen, einschließlich:

1. Einen verschweißten Kontakt
2. Einen offenen Kontakt
3. Einen Kurzschluss zwischen Kanälen
4. Einen Erdschluss
5. Einen Kurzschluss zu einer Spannungsquelle
6. Einen Kurzschluss zu einem anderen Eingang
7. Eine lose oder offene Verbindung
8. Ein überschrittenes Betriebszeitlimit
9. Einen Spannungseinbruch
10. Einen Übertemperaturzustand

Verwenden Sie die Registerkarte **Livemodus** in der Software auf einem PC, der über das USB-Kabel mit der Sicherheitsauswertung 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 die Sicherheitsauswertung aus- und wiedereingeschaltet wird.

### 11.4.1 Fehlercode-Tabelle für SCR P

Fehlercode	Fehlerbeschreibung	Lösungsschritte
1.1 – 1.2	Ausgangsfehler	Sicherheitsauswertung austauschen
1.3 – 1.8	Interner Fehler	Interner Fehler: BERNSTEIN AG kontaktieren (siehe <a href="#">Reparaturen und Garantie</a> auf Seite 142)
1.9	Ausgangsfehler	Sicherheitsauswertung austauschen
1.10	Ausgangsfehler	Fehler beim Sequenz-Zeitverhalten: <ul style="list-style-type: none"> <li>• Zur Löschung des Fehlers einen System-Reset durchführen</li> </ul>
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.  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. <ul style="list-style-type: none"> <li>• Verdrahtung überprüfen</li> <li>• Eingangssignale überprüfen</li> <li>• Gegebenenfalls die Entprellzeiten anpassen</li> <li>• Eingang schalten</li> </ul>

2.2	Gleichzeitigkeitsfehler	<p>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.</p> <p>An einem zweifach-antivalenten Eingang ging ein Eingangspaar in den Ein-Zustand, aber das andere Eingangspaar folgte nicht innerhalb von 3 Sekunden.</p> <ul style="list-style-type: none"> <li>• Verdrahtung überprüfen</li> <li>• Zeitverhalten der Eingangssignale kontrollieren</li> <li>• Eingang schalten</li> </ul>
2.3 oder 2.5	Gleichzeitigkeitsfehler	<p>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.</p> <ul style="list-style-type: none"> <li>• Verdrahtung überprüfen</li> <li>• Eingangssignale überprüfen</li> <li>• Überprüfen, ob die Stromversorgung Eingangssignale liefert</li> <li>• Gegebenenfalls die Entprellzeiten anpassen</li> <li>• Eingang schalten</li> </ul>
2.4 oder 2.6	Gleichzeitigkeitsfehler	<p>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.</p> <ul style="list-style-type: none"> <li>• Verdrahtung überprüfen</li> <li>• Zeitverhalten der Eingangssignale kontrollieren</li> <li>• Eingang schalten</li> </ul>
2.7	Interner Fehler	Interner Fehler: BERNSTEIN AG kontaktieren (siehe <a href="#">Reparaturen und Garantie</a> auf Seite 142)
2.8 – 2.9	Eingangsfehler	<p>Eingang im Ein-Zustand blockiert:</p> <ul style="list-style-type: none"> <li>• Überprüfen, ob Kurzschlüsse zu anderen Eingängen oder zu einer anderen Spannungsquelle vorliegen</li> <li>• Kompatibilität des Eingangsgeräts überprüfen</li> </ul>

Fehlercode	Fehlerbeschreibung	Lösungsschritte
2.10	Eingangsfehler	<ul style="list-style-type: none"> <li>• Überprüfen, ob zwischen den Eingängen ein Kurzschluss vorliegt</li> </ul>
2.11 – 2.12	Eingangsfehler	<ul style="list-style-type: none"> <li>• Überprüfen, ob Erdschluss vorliegt</li> </ul>
2.13	Eingangsfehler	<p>Eingang im Aus-Zustand blockiert</p> <ul style="list-style-type: none"> <li>• Überprüfen, ob Erdschluss vorliegt</li> </ul>
2.14	Eingangsfehler	<p>Fehlende Testimpulse:</p> <ul style="list-style-type: none"> <li>• Überprüfen, ob ein Kurzschluss zu anderen Eingängen oder zu einer anderen Spannungsquelle vorliegt</li> </ul>
2.15	Leitungsunterbrechung	<ul style="list-style-type: none"> <li>• Überprüfen, ob eine Leitungsunterbrechung vorliegt</li> </ul>
2.16 – 2.18	Eingangsfehler	<p>Fehlende Testimpulse:</p> <ul style="list-style-type: none"> <li>• Überprüfen, ob ein Kurzschluss zu anderen Eingängen oder zu einer anderen Spannungsquelle vorliegt</li> </ul>
2.19	Leitungsunterbrechung	<ul style="list-style-type: none"> <li>• Überprüfen, ob eine Leitungsunterbrechung vorliegt</li> </ul>
2.20	Eingangsfehler	<p>Fehlende Testimpulse:</p> <ul style="list-style-type: none"> <li>• Überprüfen, ob Erdschluss vorliegt</li> </ul>
2.21	Leitungsunterbrechung	<ul style="list-style-type: none"> <li>• Überprüfen, ob eine Leitungsunterbrechung vorliegt</li> </ul>
2.22 – 2.23	Eingangsfehler	<ul style="list-style-type: none"> <li>• Überprüfen, ob am Eingang ein instabiles Signal vorliegt</li> </ul>
2.24	Eingang während Überbrückung aktiviert	Eine Zweihandsteuerung wurde aktiviert (eingeschaltet), während sie überbrückt wurde.
2.25	Eingangsfehler	<p>Nachdem sich der zugehörige Sicherheitsausgang ausgeschaltet hat, wurde der AVM-Eingang nicht vor Ablauf seiner AVM-Überwachungszeit geschlossen:</p> <ul style="list-style-type: none"> <li>• Die AVM ist möglicherweise getrennt. Verdrahtung zur AVM prüfen.</li> <li>• Entweder die AVM ist getrennt, oder sie reagiert zu langsam auf das Ausschalten des Sicherheitsausgangs.</li> <li>• Kabelanschlüsse zur AVM überprüfen</li> <li>• Zeitgebereinstellung überprüfen und bei Bedarf erhöhen</li> <li>• BERNSTEIN AG kontaktieren</li> </ul>
2.26	Eingangsfehler	<p>Der AVM-Eingang war offen, sollte sich aber beim Einschaltbefehl an den verbundenen Sicherheitsausgang geschlossen haben:</p> <ul style="list-style-type: none"> <li>• Die AVM ist möglicherweise getrennt. Verdrahtung zur AVM prüfen.</li> </ul>

3.1	EDMxx-Fehler	EDM-Kontakt wurde geöffnet, bevor sich die Sicherheitsausgänge einschalteten: <ul style="list-style-type: none"> <li>Überprüfen, ob Kontaktgeber oder Relais im Ein-Zustand verschweißt sind</li> <li>Auf Leitungsunterbrechungen überprüfen</li> </ul>
3.2	EDMxx-Fehler	EDM-Kontakte wurden nach dem Abschalten der Sicherheitsausgänge nicht innerhalb von 250 ms geschlossen: <ul style="list-style-type: none"> <li>Überprüfen, ob Kontaktgeber oder Relais zu langsam abfallen oder im Ein-Zustand verschweißt sind.</li> <li>Auf Leitungsunterbrechungen überprüfen</li> </ul>
3.3	EDMxx-Fehler	EDM-Kontakte wurden vor dem Einschalten der Sicherheitsausgänge geöffnet: <ul style="list-style-type: none"> <li>Überprüfen, ob Kontaktgeber oder Relais im Ein-Zustand verschweißt sind</li> <li>Auf Leitungsunterbrechungen überprüfen</li> </ul>
3.4	EDMxx-Fehler	Kontakte der beiden Rückführkreise (EDM-Kontaktpaar) länger als 250 ms in unterschiedlichem Zustand. <ul style="list-style-type: none"> <li>Überprüfen, ob Kontaktgeber oder Relais zu langsam abfallen oder im Ein-Zustand verschweißt sind.</li> <li>Auf Leitungsunterbrechungen überprüfen</li> </ul>
3.5	EDMxx-Fehler	<ul style="list-style-type: none"> <li>Überprüfen, ob am Eingang ein instabiles Signal vorliegt</li> </ul>
3.6	EDMxx-Fehler	<ul style="list-style-type: none"> <li>Überprüfen, ob Erdschluss vorliegt</li> </ul>
3.7	EDMxx-Fehler	<ul style="list-style-type: none"> <li>Überprüfen, ob zwischen den Eingängen ein Kurzschluss vorliegt</li> </ul>
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: <ul style="list-style-type: none"> <li>Entweder die AVM ist getrennt, oder sie reagiert zu langsam auf das Ausschalten des Sicherheitsausgangs.</li> <li>Den AVM-Eingang überprüfen und dann zur Löschung des Fehlers einen System-Reset ausführen</li> </ul>

Fehlercode	Fehlerbeschreibung	Lösungsschritte
3.9	Eingangsfehler	Der AVM-Eingang war offen, sollte sich aber beim Einschaltbefehl an den verbundenen Sicherheitsausgang geschlossen haben: <ul style="list-style-type: none"> <li>Die AVM ist möglicherweise getrennt. Verdrahtung zur AVM prüfen.</li> </ul>
3.10	Interner Fehler	Interner Fehler: BERNSTEIN AG kontaktieren (siehe <a href="#">Reparaturen und Garantie</a> auf Seite 142)
4.1	Betriebsspannung zu niedrig	Betriebsspannung länger als 6 ms unter der Mindestversorgungsspannung: <ul style="list-style-type: none"> <li>Betriebsspannungs- und Stromwerte der Versorgungsspannungsquelle überprüfen</li> <li>Überprüfen, ob an den Ausgängen Überlast vorliegt, die die Stromversorgung veranlassen könnte, den Strom zu begrenzen</li> </ul>
4.2	Interner Fehler	Ein Konfigurationsparameter wurde beschädigt. Zur Behebung des Zustands: <ul style="list-style-type: none"> <li>Die Konfiguration unter Verwendung einer Sicherungskopie von der Konfiguration ersetzen</li> <li>Die Konfiguration über die Software erneut erstellen und in die Sicherheitsauswertung schreiben</li> </ul>
4.3–4.12	Interner Fehler	Interner Fehler: BERNSTEIN AG kontaktieren (siehe <a href="#">Reparaturen und Garantie</a> auf Seite 142).
4.13	Konfigurations-Zeitabschaltung	Die Sicherheitsauswertung 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: <ul style="list-style-type: none"> <li>Konfiguration über die Software bestätigen</li> </ul>
4.15–4.19	Interner Fehler	Interner Fehler: BERNSTEIN AG kontaktieren (siehe <a href="#">Reparaturen und Garantie</a> auf Seite 142).
4.20	Nicht zugewiesener Anschluss belegt	Dieser Anschluss ist keinem Gerät in der vorliegenden Konfiguration zugeordnet und sollte nicht aktiv sein: <ul style="list-style-type: none"> <li>Verdrahtung überprüfen</li> </ul>
4.21–4.34	Interner Fehler	Interner Fehler: BERNSTEIN AG kontaktieren (siehe <a href="#">Reparaturen und Garantie</a> auf Seite 142).
4.35	Übertemperatur	Ein interner Übertemperaturzustand ist aufgetreten. Überprüfen Sie, ob die Umgebungs- und Ausgangslastbedingungen den Spezifikationen für die Sicherheitsauswertung entsprechen.
4.36–4.47	Interner Fehler	Interner Fehler: BERNSTEIN AG kontaktieren (siehe <a href="#">Reparaturen und Garantie</a> auf Seite 142).

4.48	Nicht verwendeter Ausgang	An einer unbekannten Klemme wurde Spannung festgestellt.
4.49–4.59	Interner Fehler	Interner Fehler: BERNSTEIN AG kontaktieren (siehe <a href="#">Reparaturen und Garantie</a> auf Seite 142).
4.60	Ausgangsfehler	Ein Ausgangsanschluss hat einen Kurzschluss erkannt. Überprüfen Sie den Ausgangsfehler für nähere Informationen.
5.1–5.3	Interner Fehler	Interner Fehler: BERNSTEIN AG kontaktieren (siehe <a href="#">Reparaturen und Garantie</a> auf Seite 142).
6.xx	Interner Fehler	Ungültige Konfigurationsdaten. Möglicher interner Fehler: <ul style="list-style-type: none"> <li>• Neue Konfiguration in die Sicherheitsauswertung zu schreiben versuchen</li> </ul>
10.xx	Interner Fehler	Interner Fehler: BERNSTEIN AG kontaktieren (siehe <a href="#">Reparaturen und Garantie</a> auf Seite 142).

## 12. Komponenten und Zubehörteile

Typenbezeichnung	Beschreibung	Produkt
USB-Kabel A/Mikro-B	USB-Kabel	SCR P
SCR P-PA	Programmieradapter	SCR P
SCR P-FPS	Programmier-Stick	SCR P



## 13. Kundendienst und Wartung

### 13.1 Reinigung

---

1. **Trennen Sie die Versorgungsspannung von der Sicherheitsauswertung.**
2. Wischen Sie das Polycarbonatgehäuse mit einem weichen, mit einer Lösung aus einem schonenden Reinigungsmittel und warmem Wasser befeuchteten Tuch ab.

### 13.2 Reparaturen und Garantie

---

Wenden Sie sich zur Fehlerbehebung dieses Gerätes an die BERNSTEIN AG. **Versuchen Sie nicht, Reparaturen an diesem Gerät vorzunehmen. Es enthält keine am Einsatzort auszuwechselnden Teile oder Komponenten.** Wenn ein BERNSTEIN-Anwendungstechniker zu dem Schluss kommt, dass dieses Gerät, ein Teil oder eine Komponente davon defekt ist, erhalten Sie von dem Techniker Erläuterungen zum RMA-Verfahren (Return Merchandise Authorization) der Bernstein AG für die Warenrückgabe.



**Wichtig:** Wenn Sie der Techniker anweist, das Gerät zurückzusenden, verpacken Sie sie bitte sorgfältig. Transportschäden bei der Rücksendung werden von der Garantie nicht abgedeckt.

Damit die BERNSTEIN AG Probleme beheben kann, während der PC mit der Sicherheitsauswertung verbunden ist, rufen Sie in der Software die Hilfe auf und klicken Sie auf „Support-Informationen“. Klicken Sie auf **SCR P-Diagnose speichern** (unter **Hilfe > Supportinformationen**), um eine Datei mit Statusinformationen zu generieren. Diese Informationen können für das Supportteam bei der BERNSTEIN AG von Nutzen sein. Senden Sie die Datei an die BERNSTEIN AG und beachten Sie dabei die Anweisungen auf dem Bildschirm.

### 13.3 Kontakt

---

Sitz der Zentrale der BERNSTEIN AG:

Hans-Bernstein-Str. 1, 32457 Porta Westfalica, Deutschland

Website: [www.bernstein.eu](http://www.bernstein.eu)

Telefon: + 49 571/793-0

Weltweite Standorte und lokale Vertretungen finden Sie unter [www.bernstein.eu](http://www.bernstein.eu)

### 13.4 Haftungsausschluss

---

BERNSTEIN gewährleistet nicht die Anwendbarkeit und Kompatibilität der Software-Komponenten mit der vom Kunden genutzten Hard- und Software. Unsere Haftung für die Verwendbarkeit und eine fehlerfreie und dauerhafte Funktionsfähigkeit der zum Download bereitgestellten Software sowie durch sie verursachte unmittelbar und mittelbare Schäden ist ausgeschlossen; ausgeschlossen ist insbesondere die Haftung für Systemausfälle, Datenverluste und andere Schäden an Soft- und Hardware sowie für entgangenen Gewinn, Betriebsunterbrechung, Produktionsausfall und Kosten der Ersatzbeschaffung. Ausgenommen vom Haftungsausschluss ist die Haftung für Schäden, die BERNSTEIN vorsätzlich oder grob fahrlässig verursacht hat sowie die Haftung für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit aufgrund einer von BERNSTEIN zu vertretenden Pflichtverletzung sowie die Haftung für vorsätzlich verschwiegene Mängel. Sofern die Haftung nicht ausgeschlossen ist, weil sie auf einem Verstoß gegen eine wesentliche Vertragspflicht beruht, beschränkt sich unsere Haftung auf den vorhersehbaren und vertragstypischen Schaden, sofern nicht Vorsatz oder grobe Fahrlässigkeit vorliegt.

# 14. Normen und Vorschriften

*Es folgt eine Liste mit Normen zu diesem BERNSTEIN-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.*

## 14.1 Geltende europäische und internationale Normen

EN ISO 12100: Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikoreduzierung  
 ISO 13857 Sicherheit von Maschinen - Sicherheitsabstände gegen das Erreichen von Gefährdungsbereichen mit den oberen und unteren Gliedmaßen  
 ISO 13850 (EN 418): Not-Ausschaltgeräte, Funktionelle Aspekte – Gestaltungsleitsätze EN 574: Zweihandschaltungen – 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

## 14.2 Geltende US-Normen

ANSI B11.0: Safety of Machinery, General Requirements, and Risk Assessment (Sicherheit von Maschinen, Allgemeine Anforderungen und Risikobewertung)	ANSI B11.15: Pipe, Tube, and Shape Bending Machines (Rohr-, Schlauch- und Formbiegemaschinen)
ANSI B11.1: Mechanical Power Presses (Mechanische Pressen)	ANSI B11.16: Metal Powder Compacting Presses (Metallpulver-Kompaktierungspressen)
ANSI B11.2: Hydraulic Power Presses (Hydraulische Pressen)	ANSI B11.17: Horizontal Extrusion Presses (Horizontale Strangpressen)
ANSI B11.3: Power Press Brakes (Bremsen von mechanischen Pressen)	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 B11.4: Shears (Abtrenner)	ANSI B11.19: Performance Criteria for Safeguarding
ANSI B11.5: Iron Workers (Stahlbauarbeiter) ANSI B11.6: Lathes (Drehmaschinen)	ANSI B11.20: Manufacturing Systems (Fabrikationssysteme)
ANSI B11.7: Cold Headers and Cold Formers (Kaltstauher und Kaltumformer)	ANSI B11.21: Machine Tools Using Lasers (Maschinenwerkzeuge mit Lasern)
ANSI B11.8: Drilling, Milling, and Boring (Bohren, Mahlen und Fräsen)	ANSI B11.22: Numerically Controlled Turning Machines (Digital gesteuerte Drehmaschinen)
ANSI B11.9: Grinding Machines (Schleifmaschinen)	ANSI B11.23: Machining Centers (Zentren für maschinelle Bearbeitung)
ANSI B11.10: Metal Sawing Machines (Metallsägemaschinen)	ANSI B11.24: Transfer Machines (Übertragungsmaschinen)
ANSI B11.11: Gear Cutting Machines (Verzahnungsmaschinen)	ANSI/RIA R15.06: Safety Requirements for Industrial Robots and Robot Systems (Sicherheitsanforderungen für Industrieroboter und Roboter-Systeme)
ANSI B11.12: Roll Forming and Roll Bending Machines (Rollenformungs- und Rollenbiegemaschinen)	ANSI NFPA 79: Electrical Standard for Industrial Machinery (Elektrische Norm für Industriemaschinen)
ANSI B11.13: Single- and Multiple-Spindle Automatic Bar and Chucking Machines (Automatische Stab- und Futtermaschinen mit einer oder mehreren Spindeln)	ANSI/PMMA B155.1: Package Machinery and Packaging-Related Converting Machinery – Safety Requirements (Verpackungsmaschinen und verpackungsbezogene Verarbeitungsmaschinen – Sicherheitsanforderungen)
ANSI B11.14: Coil Slitting Machines (Spulenlängsschneidemaschinen)	

## 14.3 Geltende OSHA-Vorschriften

---

Die genannten OSHA-Dokumente stammen von 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)

# 15. Glossar

## A

### Automatischer Reset

Die Einstellung zur Steuerung des Sicherheitseingangs, bei der der zugewiesene Sicherheitsausgang automatisch einschaltet, wenn alle seine ihm zugeordneten Eingänge im Ein-Zustand sind.

### 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.

### Ausschaltentprellzeit

Die erforderliche Zeit zur Überbrückung eines flackernden Eingangssignals oder von Eingangskontakt-Prellen, um störende Auslösungen der Sicherheitsauswertung zu verhindern. Einstellbar von 6 ms bis 100 ms. Standardeinstellung ist 50 ms für Muting-Sensoren, 6 ms für andere Vorrichtungen.

### Ansprechzeit der Maschine

Die Zeit zwischen der Aktivierung einer Maschinenabschalteneinrichtung und der Herstellung eines sicheren Zustands durch das Anhalten der gefährlichen Maschinenbewegung.

### Ausschaltsignal

Das Signal des Sicherheitsausgangs, das sich ergibt, wenn mindestens eines seiner zugehörigen Eingangsgerätsignale in den Aus-Zustand wechselt. In diesem Handbuch wird der Sicherheitsausgang als ausgeschaltet oder im Aus-Zustand befindlich bezeichnet, wenn das Signal nominell 0 V DC beträgt.

## 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.

### 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

### DCD

Daisy Chain Diagnose ermöglicht die Übermittlung von umfangreichen Diagnosedaten eines jedes DCD-Gerätes, auch bei einer Reihenschaltung solcher Geräte (s. jeweilige Bedienungsanleitung für eine detaillierte Beschreibung der Diagnosedaten, die ein bestimmtes DCD-Gerät zur Verfügung stellt.)

### 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 Fehlern gemeinsamer Ursache.

## E

### Zweikanalig

Die Verwendung redundanter Signalleitungen für jeden Sicherheitseingang bzw. Sicherheitsausgang.

### Einschaltsignal

Das Signal des Sicherheitsausgangs, das sich ergibt, wenn alle seine zugehörigen Eingangsgerätsignale in den Ein-Zustand wechseln. In diesem Handbuch wird der Sicherheitsausgang als eingeschaltet 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 Werkseinstellung beträgt 50 ms.

### Einkanalig

Die Verwendung nur einer Signalleitung 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.

### 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, wie z. B. ISO 13857

## G

### Gleichzeitig (auch "simultan" oder "Gleichzeitigkeit")

Die Einstellung, bei der beide Kanäle gleichzeitig ausgeschaltet sein müssen UND sich im Abstand von höchstens 3 Sekunden voneinander wieder einschalten dürfen. Sind beide Bedingungen nicht erfüllt, so befindet sich der Eingang in einem

## H

### Hintertretungsgefahr

Gefahren durch Hintertreten des Vorhangs entstehen bei Anwendungen, bei denen Personen durch eine Sicherheitseinrichtung (die einen Stoppbefehl ausgibt, um die Gefahr zu beseitigen) treten und dann weiter in den überwachten Bereich eindringen können, z. B. im Rahmen einer Bereichssicherung. Ihre Anwesenheit wird daraufhin nicht mehr erfasst, und es kommt zu einer Gefahr durch unerwarteten Anlauf bzw. Wiederanlauf der Maschine, während sich noch Personen im überwachten Bereich aufhalten.

## M

### Manueller Reset

Konfiguration zur Steuerung des Sicherheitsschaltgeräts, bei der der zugewiesene Sicherheitsausgang erst einschaltet, nachdem ein manueller Reset ausgeführt wurde, vorausgesetzt die anderen zugehörigen Eingänge sind im Ein-Zustand.

## Q

### Qualifizierte Person

ine 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.

## 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 Erdungsfehler in anderen Schaltkreisen, Kleinspannungen (25 V AC QMW oder 60 V DC welligkeitsfrei) nicht überschreiten darf.“

### Stoppsignal

Das von der Sicherheitsauswertung überwachte Eingangssignal, das – wenn es erfasst wird – bewirkt, dass einer oder mehrere Sicherheitsausgänge abschalten. In diesem Handbuch wird entweder 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 der Sicherheitsauswertung wieder eingeschaltet werden.

## T

### Test bei Anlauf

Bei bestimmten Sicherheitseinrichtungen, wie z. B. Sicherheitslichtvorhängen oder Absperrtoren, kann es von Vorteil sein, die Einrichtung beim Anlauf mindestens ein Mal auf den einwandfreien Funktionsbetrieb zu testen.