



**We make
safety happen.**

Programmierbare Sicherheitsauswertungen **SCR P und SCx**



Inhalt

1.	Über dieses Dokument	6
1.1	Wichtig unbedingt lesen!	6
1.2	Verwendung der Warnhinweise	6
1.3	EU-Konformitätserklärungen	7
2.	Produktbeschreibung	9
2.1	In diesem Handbuch verwendete Fachbegriffe	9
2.2	Software	9
2.3	USB-Anschlüsse	9
2.4	Ethernet-Verbindung	9
2.5	Interne Logik	10
2.6	Passwort-Manager	10
2.7	Programmier-Stick SCR P-FPS und USB-Programmieradapter SCR P-PA	10
3.	SCx Übersicht	11
3.1	SCx-Modelle	11
3.2	SCx-Funktionen und -Anzeigen	12
3.3	Ein- und Ausgangsanschlüsse	12
3.3.1	SCx Sicherheits- und nicht sicherheitsrelevante Eingabegeräte	12
3.3.2	SCx Sicherheitsausgänge	12
3.3.3	SCx-Statusausgänge und virtuelle Statusausgänge	13
3.4	SCx Automatische Terminal-Optimierung (ATO) Funktion	14
4.	SCR P Übersicht	15
4.1	Ausführungen des SCR P	16
4.2	Funktionen und Anzeigen des SCR P	16
4.3	SCR P: FID	16
4.4	Ein- und Ausgangsanschlüsse	17
4.4.1	SCR P Sicherheitseingänge und nicht sicherheitsrelevante Eingänge	17
4.4.2	Sicherheits-Relaisausgänge am SCR P	17
4.4.3	Statusausgänge und virtuelle Statusausgänge am SCR P	17
4.5	Funktion des SCR P für die automatische Optimierung von Anschlüssen (ATO) bei externen Klemmenblöcken (ETB)	17
5.	Spezifikationen und Anforderungen	18
5.1	SCx Spezifikationen	18
5.2	Spezifikationen für das SCR P	23
5.3	Abmessungen	26
5.4	Systemvoraussetzungen für den PC	27
6.	Systeminstallation	28
6.1	Installation der Software	28
6.2	Installation der Sicherheitsauswertung	28
6.2.1	Montageanleitung	28
7.	Überlegungen vor der Installation	29
7.1	Geeignete Anwendung	29
7.2	SCx-Anwendungen	30
7.3	SCR P-Anwendungen	31
7.4	Sichere Eingangsfunktionen	32
7.4.1	Widerstandsfähigkeit gegen Fehler und Sicherheitsschaltungsprinzipien nach ISO 13849-1	33
7.4.2	Eigenschaften von Sicherheitseingängen	34
7.5	Optionen für Sicherheitseingangsgeräte	36
7.5.1	Sicherheitsstufen von Sicherheitsschaltungen	37
7.5.2	Zustimmtaster	37
7.5.3	Not-Halt-Schalter	37
7.5.4	Seilzugschalter	38
7.5.5	Schutzhalt (Sicherheitsstopp)	39
7.5.6	Verriegelte Schutzeinrichtung bzw. Schutztür	39
7.5.7	Optosensor	40
7.5.8	Zweihandsteuerung	40



7.5.9	Schaltmatte	43
7.5.10	Muting-Sensor	46
7.5.11	Überbrückungsschalter	47
7.5.12	AVM-Funktion (Adjustable Valve Monitoring, einstellbare Ventilüberwachung)	48
7.5.13	DCD-Eingänge	50
7.5.14	Zykluseinleitung für Funktionsblock Pressensteuerung	50
7.5.15	Pressensteuerung Sequentieller Stopp (SQS) Funktion	51
7.5.16	Presse Steuerung Stummschaltungssensor	52
7.5.17	Fußschalter	53
7.6	Nicht sicherheitsrelevante Eingangsgeräte	54
7.6.1	Manueller Reset-Eingang	55
7.7	Virtuelle nicht sicherheitsrelevante Eingangsgeräte	57
7.7.1	Virtueller manueller Reset und Abbrechen einer Zeitverzögerung (RCD)	57
7.7.2	Virtuelle Ein-/Ausschaltung und Muting-Aktivierung	60
7.8	Sicherheitsausgänge	60
7.8.1	Solid-State-Sicherheitsausgänge	64
7.8.2	Sicherheits-Relaisausgänge	66
7.8.3	EDM- und Abschaltgeräteanschluss	67
7.9	Statusausgänge	73
7.9.1	Signallogik für Statusausgänge	73
7.9.2	Statusausgangsfunktion	74
7.9.3	Pressesteuerung Statusausgabefunktionalität	75
7.10	Virtuelle Statusausgänge	76
8.	Erste Schritte	77
8.1	Erstellen einer Konfiguration	77
8.2	Hinzufügen von Eingängen und Statusausgängen	77
8.2.1	Hinzufügen von Sicherheits- und nicht sicherheitsrelevanten Eingängen	77
8.2.2	Hinzufügen von Statusausgängen	81
8.3	Entwerfen der Steuerungslogik	82
8.4	Speichern und Bestätigen einer Konfiguration	82
8.4.1	Schreiben einer bestätigten Konfiguration in einen SCR P-FPS mit dem Programmierwerkzeug	83
8.4.2	Hinweise zum Bestätigen oder Schreiben einer Konfiguration in ein konfiguriertes SCR P oder SCx	84
8.5	Beispiel-Konfigurationen	85
8.5.1	SCx: Einfache Pressensteuerung mit veränderbarem Sicherheitseingang Beispielkonfiguration	88
8.5.2	SCx: Beispielkonfiguration der Pressesteuerung mit allen Funktionen	90
9.	Software	94
9.1	Abkürzungen	94
9.2	Software-Übersicht	96
9.3	Neues Projekt	97
9.4	Projekteinstellungen	98
9.5	Registerkarte Geräte	99
9.6	Registerkarte Funktionsansicht	100
9.6.1	Logikblöcke	101
9.6.2	Funktionsblöcke	103
9.7	Registerkarte Schaltplan	104
9.8	Registerkarte Kontaktplan	105
9.9	Registerkarte DCD	106
9.10	Registerkarte Industrial-Ethernet	108
9.10.1	Netzwerkeinstellungen	109
9.10.2	Erstellung einer Datei mit SPS-Tags/-Labels	110
9.10.3	Ethernet/IP-Gruppenobjekte	112
9.11	Registerkarte Konfigurationsübersicht	113
9.12	Druckoptionen	114
9.13	SCx Passwort-Manager	115
9.14	SCR P Passwort-Manager	115
9.15	Anzeigen und Importieren von Daten	116
9.16	Livemodus	118
9.17	Simulationsmodus	121
9.17.1	Aktionszeitsteuerungsmodus	124
9.18	Referenzsignale	125



10.	Funktionsblöcke	126
10.1	One Shot Block	141
10.2	Steuerung der Presse	143
10.2.1	Modus Funktionsblock	145
10.2.2	Presse Steuereingänge Funktionsblock	146
10.2.3	Beispiele für Funktionsblöcke zur Pressensteuerung	147
10.3.1	Geschlossener Regelkreis	149
10.3	Zweihandsteuerungsblock	149
10.4	Zweihand-Bedienungsblock (SCx FID 4 und höher und SCR P FID 2 und höher)	152
11.	SCx Onboard-Schnittstelle	153
11.1	SCx-Konfigurationsmodus	155
12.	Industrial-Ethernet – Übersicht	156
12.1	Konfiguration der Sicherheitsauswertung	156
12.2	Industrial-Ethernet – Definitionen	157
12.3	Abrufen aktueller Fehlerinformationen	158
12.4	EtherNet/IP™	159
12.4.1	Eingänge Sicherheitsauswertung (Ausgänge von der SPS) O > T	159
12.4.2	Eingänge Sicherheitsauswertung (Ausgänge von der SPS) O > T	160
12.4.3	Eingänge Sicherheitsauswertung (Ausgänge von der SPS) O > T	160
12.4.4	Konfigurationsbaugruppenobjekt der Sicherheitsauswertung	162
12.4.5	Ausgänge Sicherheitsauswertung (Eingänge zur SPS) T > O	162
12.4.6	SPS-Eingang Baugruppeninstanz 100 (0x64) — 8 Register (VO-Status/Fehler)	162
12.4.7	SPS-Eingang Baugruppeninstanz 101 (0x65) - 104 Register	163
12.4.8	SPS-Eingang Baugruppeninstanz 102 (0x66) - 150 Register (nur Fehlerprotokoll)	165
12.4.9	SPS-Eingang Baugruppeninstanz 103 (0x67) — 35 Register (Reset-/Abbruchverzögerung)	167
12.4.10	SPS-Eingangsbaugruppeninstanz 104 (0x68) — 112 Register (Reset-/Abbruchverzögerung + DCD)	168
12.4.11	Fehlerbeispiele	170
12.4.12	Flags	172
12.4.13	Erweiterte Flags	173
12.5	Modbus/TCP	174
12.5.1	Die ersten 64 virtuellen Ausgänge und virtuellen Ausgangsfehler (Eingänge 10001–10128)	174
12.5.2	Alle 256 virtuellen Ausgänge und virtuellen Ausgangsfehler. (Eingänge 11001–11256, 12001–12256)	174
12.5.3	Virtuelle Eingänge, virtuelle Reset-/Abbruchverzögerung und Feedback (Spulen 3001–30064, 4001–4016, Eingänge 15001–15016)	174
12.5.4	Sicherheitsauswertung-Ausgangsregister (Modbus/TCP-Eingangs- oder Haltereister)	175
12.5.5	Leistungs- und Statusinformationen zu einem einzelnen Gerät über DCD anfordern	182
12.5.6	Flags	182
12.5.7	Erweiterte Flags	183
12.6	PROFINET®	184
12.6.1	PROFINET und die Sicherheitsauswertung	184
12.6.2	GSD-Datei (General Station Description)	184
12.6.3	PROFINET IO-Datenmodell	184
12.6.4	Konfiguration der Sicherheitsauswertung für eine PROFINET IO-Verbindung	185
12.6.5	Beschreibung der Module	186
12.6.6	Leistungs- und Statusinformationen zu einem einzelnen Gerät über DCD anfordern	194
12.6.7	Konfigurationsanleitung	194
12.7	EtherCAT®	200
12.7.1	EtherCAT® und die Sicherheitssteuerungen	200
12.7.2	EtherCAT® Slave Information (ESI) Datei	200
12.7.3	EtherCAT® IO-Datenmodell	201
12.7.4	Konfigurieren der Sicherheitssteuerung für EtherCAT® IOAnbindung	201
12.7.5	Erstellen eines PLCopenXML für EtherCAT® für TwinCAT® 3.0	202
12.7.6	Beschreibung von Prozessdatenobjekten	204
12.7.7	Anweisungen zur Konfiguration	211
12.7.8	EtherCAT® PDO-Änderung	212
12.8	Daisy Chain Diagnose - DCD	214
12.8.1	Leistungs- und Statusinformationen zu einem einzelnen Gerät über DCD anfordern	214
12.8.2	DCD-Reihe Systemstatus	214
12.8.3	Spezifische Daten einzelner DCD-Geräte	215
12.8.4	Informationen zur Temperatur-, Spannungs- und Abstandsum-wandlung	216



12.8.5	Versorgungsspannung	216
12.8.6	Innentemperatur	216
12.8.7	Abstand Betätiger	217
13.	Systemüberprüfung	218
13.1	Zeitplan für vorgeschriebene Überprüfungen	218
13.2	Inbetriebnahmeprüfung	218
13.2.1	Überprüfung des Systembetriebs	219
13.2.2	Setup vor der Inbetriebnahme, Inbetriebnahme und regelmäßige Prüfroutinen	219
14.	Informationen zum Status und zum Betrieb	224
14.1	Status der LED-Anzeigen am SCx	225
14.2	Statusanzeigen der Eingangsmodule	226
14.3	Ausgangsmodule (Solid-State oder Relais) Statusanzeigen	227
14.4	Status der LED-Anzeigen am SCR P	228
14.5	Livemodus-Informationen: Software	229
14.6	Informationen zum Livemodus: Onboard-Schnittstelle	229
14.7	Sperrzustände	230
14.8	Nach einem Sperrzustand	230
14.9	SCR P und SCx: Automatische Optimierung von Anschlüssen	231
14.10	Beispielkonfiguration für das SCR P und SCx ohne automatische Optimierung von Anschlüssen	232
14.11	SCx-Modelle mit integrierter Schnittstelle: Verwendung des SCR P-FPS	235
14.12	SCR P unter Verwendung des SCR P-FPS	235
14.13	SCx bzw. SCR P auf die Werkseinstellungen zurücksetzen	236
14.14	Werkseinstellungen	237
15.	Fehlerbehebung	238
15.1	Software: Fehlerbehebung	238
15.2	Software: Fehlercodes	239
15.3	Überprüfen der Treiberinstallation	241
15.4	Fehlersuche und -behebung	242
15.5	SCx-Fehlercode-Tabelle	243
15.6	SCR P-Fehlercode-Tabelle	249
16.	Komponenten und Zubehörteile	251
17.	Kundendienst und Wartung	252
17.1	Reinigung	252
17.2	Reparaturen und Garantie	252
17.3	Kontakt	252
17.4	Haftungsausschluss	252
18.	Normen und Vorschriften	253
18.1	Geltende europäische und internationale Normen	253
18.2	Geltende US-Normen	253
18.3	Geltende OSHA-Vorschriften	254
19.	Glossar	255



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 „18. Normen und Vorschriften“ auf Seite 253.



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 der Sicherheitsauswertung der BERNSTEIN AG beachtet werden. Bei Nichtbeachtung aller Sicherheits- und Warnhinweise ist die sichere Bedienung bzw. der sichere Betrieb nicht mehr unbedingt gewährleistet. Diese Signalwörter und Warnsymbole werden wie folgt definiert.

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

Diese Hinweise sollen den Maschinenkonstrukteur und -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-Konformitätserklärungen



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

<p>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.</p> <p>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.</p> <p>Cette déclaration de conformité correspond au Norme Européenne EN ISO/IEC 17050-1: Évaluation 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 la langue d’origine de la déclaration de conformité. Les autres langues ne sont qu’une traduction de la déclaration de conformité en langue allemande.</p>	<p style="text-align: center;">Wir / We / Nous</p> <hr/> <p style="text-align: center;">BERNSTEIN AG <small>(Name des Anbieters) / (Supplier’s name) / (Nom du fournisseur)</small></p> <hr/> <p style="text-align: center;">Hans-Bernstein-Straße 1 D-32457 Porta Westfalica</p> <hr/> <p style="text-align: center;"><small>(Anschrift) / (Address) / (Adresse)</small></p> <hr/> <p>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):</p> <p style="text-align: center;">Programmierbare Sicherheitsauswertung / Programmable Safety Controller Typ / Type: SCR-P...</p> <p>...(siehe Betriebs- und Montageanleitung / refer to Installation and Operating Instructions / voir Instructions de service et de montage)</p> <p><small>(Bezeichnung, Typ oder Modell, Los-, Chargen- oder Serien-Nr., möglichst Herkunft und Stückzahl) (Name, type or model, batch or serial number, possibly sources and number of items) (Nom, type ou modèle, n° de lot, d’échantillon ou de série, éventuellement les sources et le nombre d’exemplaires)</small></p> <p>mit folgenden Richtlinien übereinstimmt (übereinstimmen): is (are) in conformity with the following directives: est (sont) conforme(s) aux directives européennes:</p> <p style="text-align: center;">Maschinenrichtlinie / Machinery-Directive 2006/42/EC EMV-Richtlinie / EMC-Directive 2014/30/EU RoHSII Richtlinie / RoHSII Directive 2011/65/EU</p> <p style="text-align: center;">UK Richtlinien / UK Directives / UK Directives Supply of Machinery (Safety) Regulations 2008: 2008 No. 1597</p> <hr/> <p>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):</p> <p style="text-align: center;">IEC 62061:2015; EN ISO 13849-1:2015 IEC 61508 Parts 1-7:2010; IEC 61131-2:2017</p> <hr/> <p style="text-align: center;">Benannte Stelle / Notified Body / Organisme Notifié</p> <p style="text-align: center;">NB 0035 TÜV Rheinland Industrieservice GmbH, Am Grauen Stein, 51105 Köln EG-Baumusterprüfbescheinigung Reg.-No.: 01/205/5782.01/24</p> <hr/> <p>Name und Anschrift Bevollmächtigter Dokumentation: Name and address of authorized agent documentation: Nom et adresse de la documentation autorisée:</p> <p style="text-align: center;">Herr Wolfgang Vogt D-32457 Porta Westfalica, Hans-Bernstein-Straße 1</p> <div style="display: flex; justify-content: space-between; margin-top: 20px;"> <div style="width: 45%;"> <p style="text-align: center;">Porta Westfalica, 2024-07-22 <small>(Ort und Datum der Ausstellung) (Place and date of issue) (Date et lieu)</small></p> </div> <div style="width: 45%; text-align: center;">  i. V. Wolfgang Vogt Compliance Officer Product <hr/> <small>(Name, Position, Unterschrift) (Name, status, signature) (Nom, fonction, signature)</small> </div> </div>
---	---





EU/UK-Konformitätserklärung / EU/UK-Declaration of Conformity / UE/UK-Déclaration 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: Évaluation 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 la langue 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):

SCx-...

(Bezeichnung, Typ oder Modell, Los-, Chargen- oder Serien-Nr., möglichst Herkunft und Stückzahl)
 (Name, type or model, batch or serial number, possibly sources 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 Richtlinien übereinstimmt (übereinstimmen):
 is (are) in conformity with the following directives:
 est (sont) conforme(s) aux directives européennes:

EU Richtlinien / EU Directives / UE Diréctives
Maschinenrichtlinie / Safety-of-Machinery-Directive 2006/42/EC

UK Richtlinien / UK Directives / UK Diréctives
Supply of Machinery (Safety) Regulations 2008: 2008 No. 1597

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):

EN 62061:2015, EN 61508 Parts 1-7:2010
EN ISO 13849-1:2015, IEC 61131-2:2017

Benannte Stelle / Notified Body / Organisme Notifié

NB 0035
TÜV Rheinland Industrie Services GmbH, Am Grauen Stein, 51105 Köln
EG Baumusterprüfbescheinigung Reg.-No.: 01/205/5978/00/24

Name und Anschrift Bevollmächtigter Dokumentation:
 Name and address of authorized agent documentation:
 Nom et adresse de la documentation autorisée:

Herr Wolfgang Vogt
 D-32457 Porta Westfalica, Hans-Bernstein-Straße 1

W. Vogt
 i. V. Wolfgang Vogt
 Compliance Officer Product

Porta Westfalica, 2024-06-11

(Ort und Datum der Ausstellung)
 (Place and date of issue)
 (Date et lieu)

(Name, Position, Unterschrift)
 (Name, status, 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 viele weitere 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 programmierbaren Sicherheitsauswertungen SCR P und SCx beziehen.

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

Programmierbare Sicherheitssteuerung SCx: Der offizielle Name des SCx.

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 „9.2 Software-Übersicht“ auf Seite 96.

2.3 USB-Anschlüsse

Der Micro-USB-Port des SCR P und SCx dient zum Verbinden der Auswertungen 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 und auf das SCx.



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 Netzwerkwitich 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 „9.6.1 Logikblöcke“ auf Seite 101 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
- Zustimmungstaster-Block
- Latch-Reset-Block
- Muting-Block
- Zweihandsteuerungsblock
- Verzögerungsblock

Unter „9.6.2 Funktionsblöcke“ auf Seite 103 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 über die Software auf den Passwort-Manager zuzugreifen.

Unter „9.13 SCx Passwort-Manager“ auf Seite 115 und „9.14 SCR P Passwort-Manager“ auf Seite 115 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. SCx Übersicht

Mit der Option, bis zu acht E/A-Erweiterungsmodule hinzuzufügen, kann die erweiterbare Sicherheitssteuerung SCx an eine Vielzahl von Maschinen angepasst werden, einschließlich großer Maschinen mit mehreren Prozessen.



Abbildung 1: Sicherheitssteuerung SCx

- Programmierung in wenigen Minuten mit intuitiver, benutzerfreundlicher Software
- Bis zu acht E/A-Erweiterungsmodule können hinzugefügt werden, wenn die Automatisierungsanforderungen wachsen oder sich ändern
- Wählen Sie aus vier Erweiterungsmodulmodellen
- Die Modelle der Erweiterungsmodule verfügen über eine Vielzahl von Sicherheitseingängen, Halbleiter-Sicherheitsausgängen und Sicherheitsrelaisausgängen
- Innovative Live-Display-Funktion und Diagnose ermöglichen die aktive Überwachung der E/A auf einem PC und unterstützen die Fehlersuche und Inbetriebnahme
- Sicherheits-Controller und Eingangsmodule ermöglichen die Umwandlung von Sicherheitseingängen in Statusausgänge für eine effiziente Terminalnutzung
- Ethernet-fähige Modelle können für bis zu 256 virtuelle Statusausgänge konfiguriert werden
- Optionaler Programmier-Stick SCR P-FPS für schnelles Auswechseln und schnelle Konfiguration ohne PC
- Daisy Chain Diagnostic (DCD) liefert detaillierte Status- und Leistungsdaten von jedem angeschlossenen Sicherheitsgerät, auf die mit einem HMI oder einem ähnlichen Gerät zugegriffen werden kann.

3.1 SCx-Modelle

Alle erweiterbaren und nicht erweiterbaren Basissteuerungen verfügen über 18 Sicherheitseingänge, 8 konvertierbare Sicherheits-E/As und 2 Solid-State-Sicherheitsausgangspaare. Bis zu acht Erweiterungsmodule in beliebiger Kombination von Eingangs- und Ausgangsmodulen können zu den erweiterbaren Modellen der Basissteuerung hinzugefügt werden. Ein Kommunikationsgateway kann zu den erweiterbaren, Ethernet-fähigen Modellen der Basissteuerung FID 6 und höher hinzugefügt werden.

Modell	Anzeige	Ethernet-fähig	# Anzahl der DCD-Kanäle
SCx-B-26-2T-8	Nein	Nein	8
SCx-B-26-2T-7	Ja	Nein	8
SCx-B-26-2T-6	Nein	Ja	8
SCx-B-26-2T-5	Ja	Ja	8

Tabelle 1: Erweiterungsfähige Basismodelle

Modell	Beschreibung
SCx-I-16	Sicherheitseingangsmodul 16 Eingänge (4 konvertierbar)
SCx-I-8	Sicherheitseingangsmodul 8 Eingänge (2 konvertierbar)
SCx-O-2T	2 Zweikanal-Solid-State-Sicherheitsausgangsmodul
SCx-O-4T	4 Zweikanal-Solid-State-Sicherheitsausgangsmodul
SCx-O-1R	1 Zweikanal-Sicherheitsrelaismodul
SCx-O-2R	2 Zweikanal-Sicherheitsrelaismodul
SCx-N-Cat	EtherCAT-Kommunikations-Gateway

Tabelle 2: E/A-Erweiterungsmodule



3.2 SCx-Funktionen und -Anzeigen

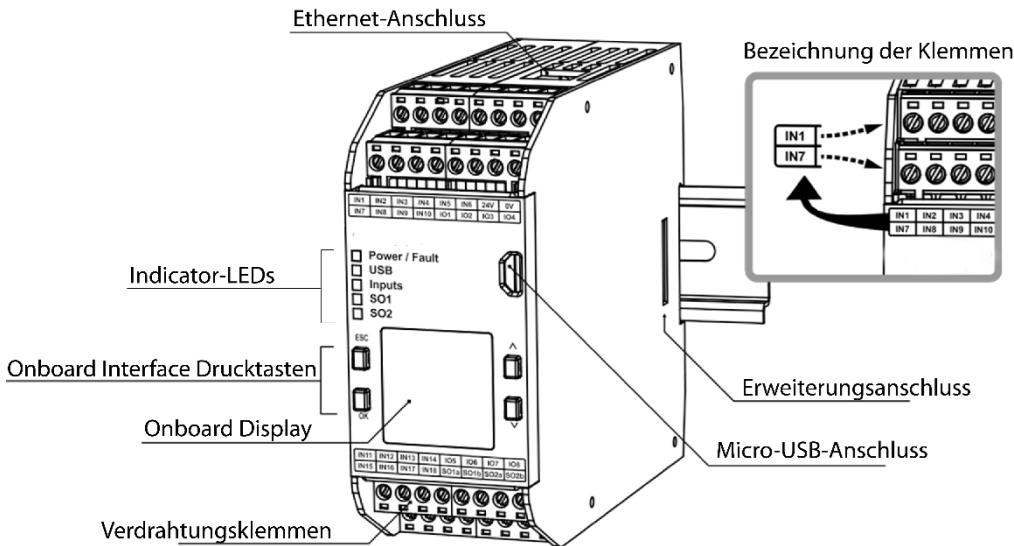


Abbildung 2: SCx-Merkmale und -Anzeigen

3.3 Ein- und Ausgangsanschlüsse

3.3.1 SCx Sicherheits- und nicht sicherheitsrelevante Eingabegeräte

Der Basis-Controller verfügt über 26 Eingangsklemmen, die zur Überwachung von Sicherheits- oder Nicht-Sicherheitsgeräten verwendet werden können; diese Geräte können entweder Halbleiter oder kontaktbasierte Ausgänge haben. Einige der Eingangsklemmen können so konfiguriert werden, dass sie entweder 24 V DC für Überwachungskontakte liefern oder den Status eines Eingangs oder eines Ausgangs signalisieren. Die Funktion jedes Eingangskreises hängt von der Art des angeschlossenen Geräts ab; diese Funktion wird bei der Konfiguration des Reglers festgelegt.

Einige der Eingangsklemmen des SCx-B-26-2T-5 können so konfiguriert werden, dass sie eine Kette von DCD-fähigen Geräten überwachen; diese Funktionalität wird während der Konfiguration der Steuerung eingerichtet.

Die Erweiterungsmodule SCx-I-8 und SCx-I-16 erweitern das Sicherheitssteuerungssystem um zusätzliche Eingänge. Wenden Sie sich an die BERNSTEIN AG, wenn Sie weitere Informationen über den Anschluss anderer, nicht in diesem Handbuch beschriebener Geräte benötigen.

3.3.2 SCx Sicherheitsausgänge

Die Sicherheitsausgänge sind für die Steuerung von Endschaltern (FSDs) und primären Maschinensteuerungselementen (MPCEs) vorgesehen, die die letzten Elemente (in der Zeit) zur Steuerung der gefährlichen Bewegung sind. Zu diesen Steuerelementen gehören Relais, Schütze, Magnetventile, Motorsteuerungen und andere Geräte, die typischerweise zwangsgeführte (mechanisch gekoppelte) Überwachungskontakte oder elektrische Signale enthalten, die für die externe Geräteüberwachung (EDM) benötigt werden.

Die Sicherheitssteuerung verfügt über zwei unabhängig gesteuerte und redundante Halbleiter-Sicherheitsausgänge (Klemmen SO1a & SO1b und SO2a & SO2b). Der Selbstprüfungsalgorithmus des Sicherheitscontrollers stellt sicher, dass die Ausgänge in Reaktion auf die zugewiesenen Eingangssignale zum richtigen Zeitpunkt ein- und ausgeschaltet werden. Jeder redundante Halbleiter-Sicherheitsausgang ist so ausgelegt, dass er entweder paarweise oder als zwei Einzelausgänge funktioniert. Wenn sie paarweise gesteuert werden, eignen sich die Sicherheitsausgänge für Anwendungen der Kategorie 4; wenn sie unabhängig voneinander arbeiten, eignen sie sich für Anwendungen bis zur Kategorie 3, wenn ein geeigneter Fehlerausschluss verwendet wurde (siehe „Sicherheitsabschaltungen“ auf Seite 70 und „7.4.1 Widerstandsfähigkeit gegen Fehler und Sicherheitsschaltungsprinzipien nach ISO 13849-1“ auf Seite 33). Weitere Informationen zum Anschluss, zu Halbleiter- und Sicherheitsrelaisausgängen, zur Überwachung externer Geräte, zu ein- oder zweikanaligen Sicherheits-Stopp-Schaltungen und zur Konfiguration von Sicherheitsausgängen finden Sie unter „7.8 Sicherheitsausgänge“ auf Seite 60.

Zusätzliche Halbleiter- oder Sicherheitsrelaisausgänge können zu der Basissteuerung hinzugefügt werden, indem Erweiterungsangangsmodule (SCx-O-2T, SCx-O-4T, SCx-O-1R und SCx-O-2R) eingebaut werden. Es können bis zu acht Erweiterungsmodule in beliebiger Kombination von Eingangs- oder Ausgangsmodulen hinzugefügt werden.

Die Sicherheitsausgänge können durch Eingangsgeräte gesteuert werden, die sowohl automatisch als auch manuell zurückgesetzt werden können.



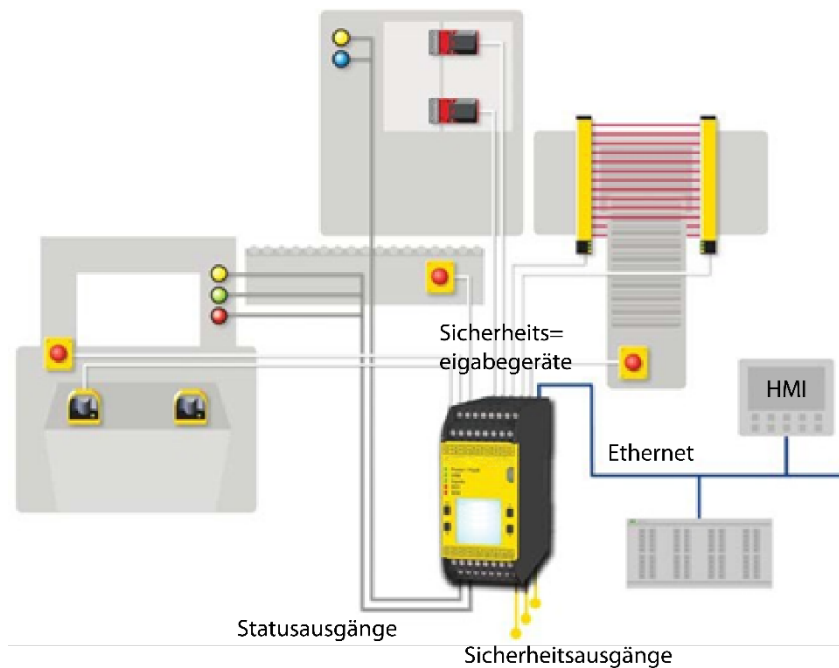


Abbildung 3: Sicherheitsausgänge (Anwendungsbeispiel)

Funktionssperren nach IEC 60204-1 und NFPA 79

Die Sicherheitssteuerung ist in der Lage zwei funktionale Stopptypen auszuführen:

- Kategorie 0: unkontrolliertes Anhalten mit sofortiger Unterbrechung der Energiezufuhr zur gesicherten Maschine
- Kategorie 1: ein kontrolliertes Anhalten mit einer Verzögerung, bevor der Strom von der geschützten Maschine abgeschaltet wird

Verzögerte Anschläge können in Anwendungen eingesetzt werden, bei denen Maschinen Energie für einen Bremsmechanismus benötigen, um die gefährliche Bewegung zu stoppen.

3.3.3 SCx-Statusausgänge und virtuelle Statusausgänge

Der Basis-Controller verfügt über acht konvertierbare E/As (mit der Bezeichnung IOx), die als Statusausgänge verwendet werden können, die in der Lage sind, nicht sicherheitsrelevante Statussignale an Geräte wie speicherprogrammierbare Steuerungen (SPS) oder Anzeigeleuchten zu senden. Darüber hinaus können alle nicht verwendeten Sicherheitsausgangsklemmen so konfiguriert werden, dass sie die Funktion eines Statusausgangs mit dem Vorteil einer höheren Stromkapazität erfüllen (weitere Informationen finden Sie unter SCx-Spezifikationen auf Seite 20). Bei den als Statusausgänge konfigurierten Halbleitersicherheitsausgängen bleiben die Sicherheitstestimpulse aktiviert, auch wenn sie als Statusausgang bestimmt sind. Die Signalkonvention des Statusausgangs kann als 24 V DC, 0 V DC oder als zyklisches Ein und Ausschalten konfiguriert werden. Informationen zu den spezifischen Funktionen eines Statusausgangs finden Sie unter „7.9.1 Signallogik für Statusausgänge“ auf Seite 73.

Ethernet-Modelle können mit Hilfe der Software für bis zu 256 virtuelle Statusausgänge an SCx-Sicherheits-Steuerungen konfiguriert werden. Diese Ausgänge können die gleichen Informationen wie die Statusausgänge über das Netzwerk übertragen.

Weitere Informationen finden Sie unter „7.10 Virtuelle Statusausgänge“ auf Seite 76.



WARNUNG:

- **Statusausgänge und virtuelle Statusausgänge sind keine Sicherheitsausgänge und können sowohl im Zustand Ein als auch im Zustand Aus ausfallen.**
- Wenn ein Statusausgang oder ein virtueller Statusausgang zur Steuerung einer sicherheitskritischen Anwendung verwendet wird, ist ein zu einem gefährlichen Zustand führender Ausfall möglich und kann zu schweren Verletzungen oder Tod führen.
- Verwenden Sie niemals einen Statusausgang oder virtuellen Statusausgang, um sicherheitskritische Anwendungen zu steuern.



3.4 SCx Automatische Terminal-Optimierung (ATO) Funktion

Die automatische Klemmenoptimierung (ATO) ist eine Standardfunktion bei allen SCx-Modellen. Diese Funktion kombiniert automatisch bis zu zwei E/A-Klemmen für zwei Geräte, die +24-V-Testimpulse von der Sicherheitssteuerung benötigen. Falls zutreffend, führt die Software dies automatisch für jedes hinzugefügte Gerätepaar durch, bis keine E/A-Klemmen mehr verfügbar sind. Die gemeinsame Nutzung ist auf zwei begrenzt, da die Schraubklemmen bis zu zwei Drähte aufnehmen können.

Falls gewünscht, können die Terminals im Fenster Geräteeigenschaften manuell neu zugewiesen werden.

Die folgenden Abbildungen zeigen, wie die ATO-Funktion des SCx die Klemmen für zwei Gate-Schalter optimiert.

Dies führt zu einer Gesamtklemmenbelegung von sechs gegenüber acht, wenn ATO nicht verwendet wird. Der erste Gate-Schalter (GS1) wird hinzugefügt. Es handelt sich um einen zweikanaligen, vieradrigen Torschalter, der zwei unabhängige +24-V-Impulsausgänge von der Sicherheitssteuerung benötigt. IO1 wird als +24-V-Testimpuls 1 zugewiesen, der durch Kanal 1 von GS1 zu IN1 läuft. IO2 wird als +24 V Testimpuls 2 zugewiesen, der über Kanal 2 von GS1 zu IN2 läuft. Wenn der zweite Torschalter GS2 hinzugefügt wird, verwendet er ebenfalls IO1 und IO2, aber IN3 und IN4 zur Überwachung seiner beiden Kanäle.

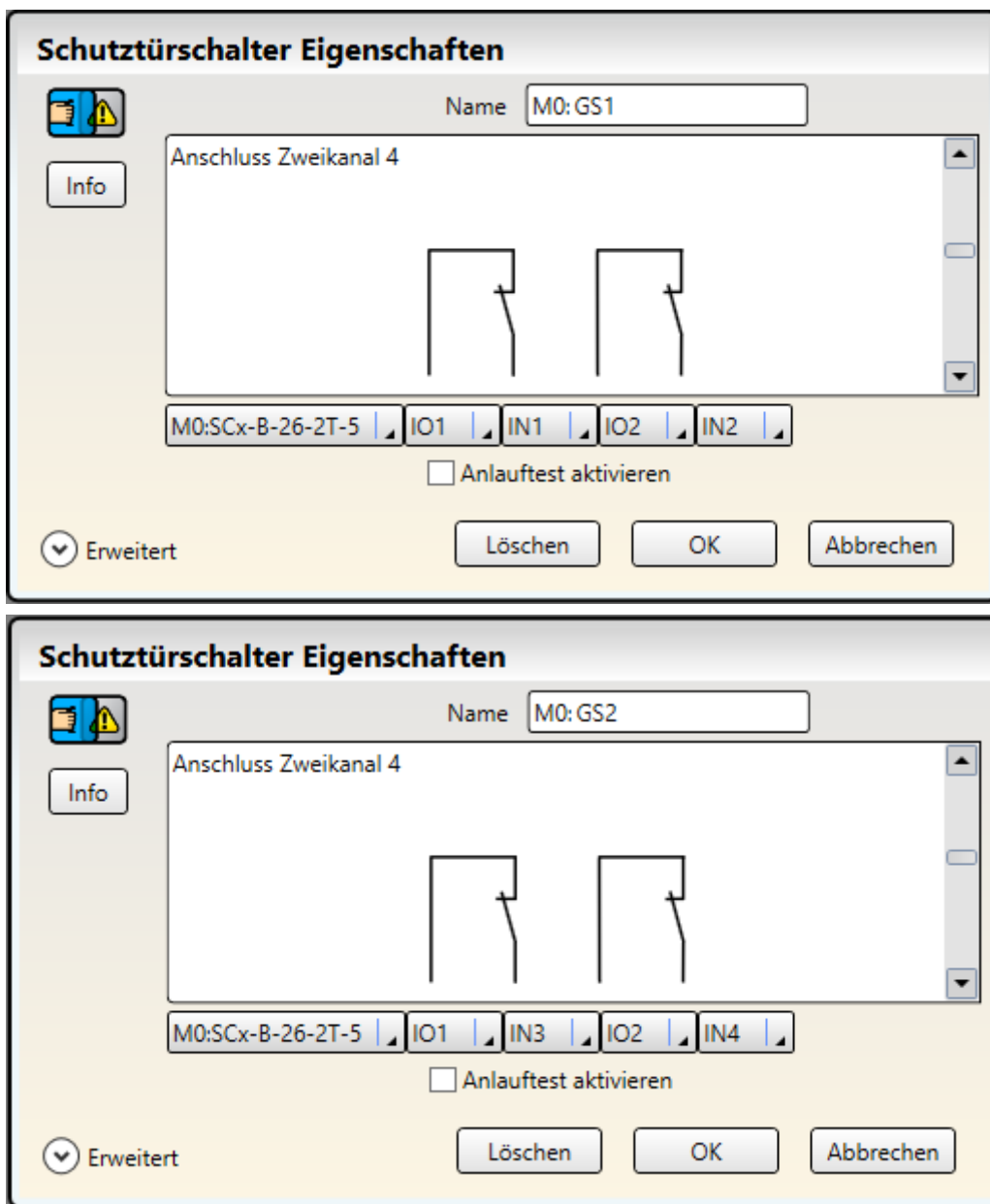


Abbildung 4: GS1 und GS2 Gemeinsame Nutzung von IO1 und IO2



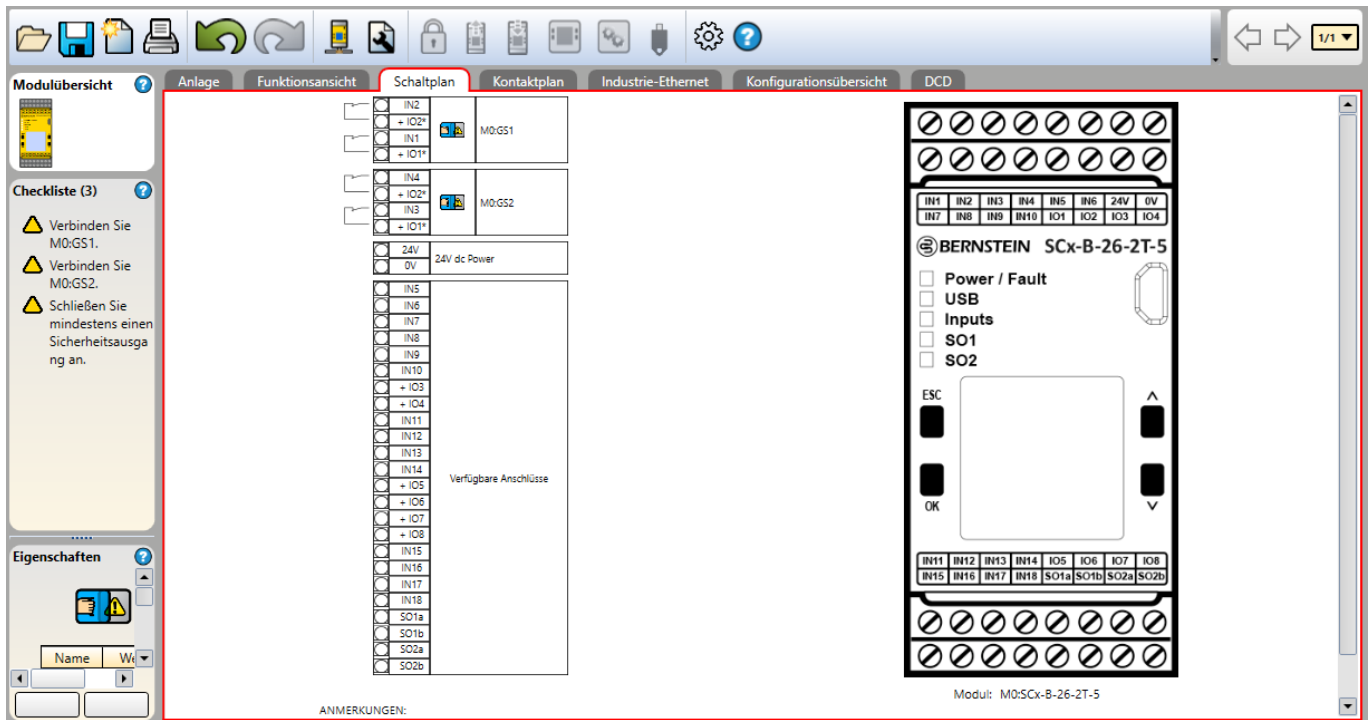


Abbildung 5: Schaltplan-Registerkartenansicht der gemeinsam genutzten E/As

4. SCR P Übersicht

Die programmierbare Sicherheitsauswertung SCR P von BERNSTEIN ist eine benutzerfreundliche und kostengünstige Alternative zu Sicherheitsrelaismodulen. Sie 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 und suche nach SCR P



Abbildung 6: Sicherheitssteuerung 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 Schließkontakten
- 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
 - 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 „14.12 SCR P unter Verwendung des SCR P-FPS“ auf Seite 235)



4.1 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

4.2 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. Verzinnete 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.

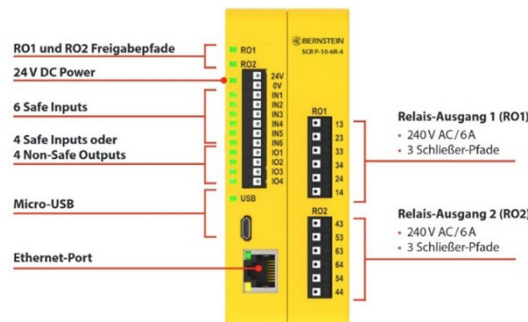


Abbildung 7: Funktionen und Anzeigen

4.3 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.

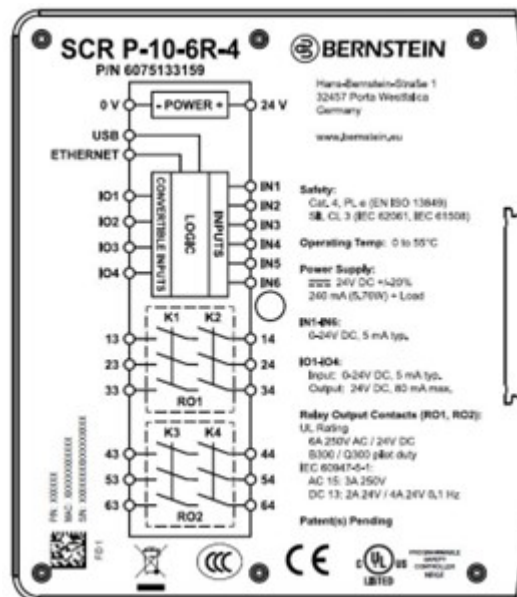


Abbildung 8: Beispiel für die Bedruckung des SCR P



4.4 Ein- und Ausgangsanschlüsse

4.4.1 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.

4.4.2 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.

4.4.3 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 „7.10 Virtuelle Statusausgänge“ auf Seite 76.

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.

4.5 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 dieses 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 unterschiedliche 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.



5. Spezifikationen und Anforderungen

5.1 SCx Spezifikationen

■ Basis-Controller und Erweiterungsmodule

Mechanische Belastung

Schock: 15 g für 11 ms, Halbsinuswelle, insgesamt 18 Schocks (gemäß IEC 61131-2)

Vibration: 3,5 mm gelegentlich / 1,75 mm kontinuierlich bei 5 Hz bis 9 Hz, 1,0 g gelegentlich und 0,5 g kontinuierlich bei 9 Hz bis 150 Hz: alle bei 10 Sweep-Zyklen pro Achse (gemäß IEC 611312)

Sicherheit

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

Normen für die Produktleistung

Siehe „18. Normen und Vorschriften“ auf Seite 253 für eine Liste der in der Branche geltenden US-amerikanischen und internationalen Normen.

EMC

Erfüllt oder übertrifft alle EMV-Anforderungen gemäß IEC 61131-2, IEC 62061 Anhang E, Tabelle E.1 (erhöhte Störfestigkeitswerte), IEC 61326-1:2006 und IEC61326-31:2008

Betriebsbedingungen

Temperatur: 0 °C bis +55 °C (+32 °F bis +131 °F)

Lagertemperatur: -30 °C bis +65 °C (-22 °F bis +149 °F)

Luftfeuchtigkeit: 90% bei +50 °C maximale relative Luftfeuchtigkeit (nicht kondensierend)

Betriebshöhe: maximal 2000 m (6562 ft) gemäß IEC 61010-1

Umweltbewertung

NEMA 1 (IEC IP20), zur Verwendung in NEMA 3 (IEC IP54) oder besseren Gehäusen

Abnehmbare Schraubklemmen

Drahtgröße: 24 bis 12 AWG (0,2 bis 3,31 mm²)

Drahtstreifenlänge: 7 bis 8 mm (0,275 in bis 0,315 in)

Anzugsdrehmoment: 0,565 Nm (5,0 lbf in)

Abnehmbare Klemmenanschlüsse

Wichtig: Die Klemmen sind nur für einen Draht ausgelegt. Wenn mehr als ein Draht an eine Klemme angeschlossen wird, kann sich ein Draht lösen oder vollständig von der Klemme abgetrennt werden, was einen Kurzschluss verursacht. Wenn mehr als ein Draht erforderlich ist, sollte eine Aderendhülse oder ein externer Klemmenblock verwendet werden.

Drahtgröße: 24 bis 16 AWG (0,20 bis 1,31 mm²)

Länge des Drahtstreifens: 8,00 mm (0,315 Zoll)



Wichtig: Die Stromversorgung muss den Anforderungen für Kleinstspannungen mit Schutztrennung (SELV, PELV) entsprechen.

■ SCx-B-26-2T-5, SCx-B-26-2T-8, SCx-B-26-2T-7 und SCx-B-26-2T-6 - Basis-Sicherheitssteuerungsmodule

Mechanische Belastung

Schock: 15 g für 11 ms, Halbsinuswelle, insgesamt 18 Schocks (gemäß IEC 61131-2)

Vibration: 3,5 mm gelegentlich / 1,75 mm kontinuierlich bei 5 Hz bis 9 Hz, 1,0 g gelegentlich und 0,5 g kontinuierlich bei 9 Hz bis 150 Hz: alle bei 10 Sweep-Zyklen pro Achse (gemäß IEC 611312)

Strom

24 V DC ± 20% (inkl. Restwelligkeit), 100 mA ohne Last

Ethernet-Modelle: 40 mA hinzufügen

Anzeigemodelle: 20 mA hinzufügen

Ausbaufähige Modelle: 3,6 A maximale Buslast

Netzwerkschnittstelle (nur Ethernet-Modelle)

Ethernet 10/100 Base-T/TX, modularer RJ45-Anschluss wählbare automatische Aushandlung oder manuelle Rate und Duplex Auto MDI/MDIX (Auto-Cross)

Protokolle: ⁴ EtherNet/IP™ (mit PCCC), Modbus® TCP, PROFINET® (FID 2 oder höher), und EtherCAT® (erfordert SCx-N-Cat-Gateway)

Daten: 64 konfigurierbare virtuelle Statusausgänge an Sicherheitssteuerungen SCx mit FID 1 oder 256 virtuelle Statusausgänge an SCx-Sicherheits-Steuerungen mit FID 2 oder höher; Fehlerdiagnosecodes und -meldungen; Zugang zum Fehlerprotokoll

⁴ EtherNet/IP™ ist ein Warenzeichen der ODVA, Inc.; Modbus® ist ein eingetragenes Warenzeichen der Schneider Electric USA, Inc.; PROFINET® ist ein eingetragenes Warenzeichen der PROFIBUS Nutzerorganisation e.V.; EtherCAT® ist ein eingetragenes Warenzeichen und patentierte Technologie, lizenziert von Beckhoff Automation GmbH, Deutschland.



Konvertierbare E/A

Ausgangsstrom: maximal 80 mA (überstromgeschützt) Prüfpulse: etwa 1 ms alle 25 ms bis 75 ms

Automatische Terminal-Optimierungsfunktion

Bis zu zwei Geräte

Prüfpuls

Breite: maximal 200 µs

Rate: 200 ms typisch

Schutz des Ausganges

Alle Halbleiterausgänge (Sicherheits- und Nicht-Sicherheitsausgänge) sind gegen Kurzschlüsse gegen 0 V oder +24 V geschützt, einschließlich Überstrombedingungen

Sicherheitsbewertungen

PFH [1/h]: 1.05 × 10⁻⁹

Proof-Test-Intervall: 20 Jahre

Sicherheitseingänge (und konvertierbare E/A bei Verwendung als Eingänge)

Eingangs-EIN-Schwelle: > 15 V DC (garantiert eingeschaltet), max. 30 V DC.

Eingangs-AUS-Schwelle: < 5 V DC und < 2 mA, -3 V DC min.

Eingangs-EIN-Strom: 5 mA typisch bei 24 V DC, 50 mA Spitzenstrom zur Kontaktreinigung bei 24 V DC

Widerstand der Eingangsleitung: 300 Ω max. (150 Ω pro Leitung)

Eingangsanforderungen für eine 4-Draht-Schaltmatte:

- Max. Kapazität zwischen den Platten: 0,22 µF
- Max. Kapazität zwischen Bodenplatte und Erde: 0,22 µF
- Max. Widerstand zwischen den 2 Eingangsklemmen einer Platte: 20 Ω

Solid-State-Sicherheitsausgänge

0,5 A max. bei 24 V DC (1,0 V DC max. Abfall), 1 A max. inrush

Schwelle Ausgang AUS: 1,7 V DC typisch (2,0 V DC max.)

Ausgangsleckstrom: 50 µA max. bei offenen 0 V

Belastung: max. 0,1 µF, max. 1 H, max. 10 Ω pro Leitung

Reaktions- und Wiederherstellungszeiten

Reaktionszeit zwischen Eingang und Ausgang (Eingangsstopp bis Ausgang aus): siehe die Konfigurationsübersicht in der Software, da sie variieren kann.

Wiederanlaufzeit: Einschaltverzögerung (falls eingestellt) plus 250 ms typisch (400 ms maximal)

Ausgang xA bis Ausgang xB schalten differenziell ein (als Paar verwendet, nicht geteilt): 5 ms max.

Ausgang X zu Ausgang Y einschalten Differential (gleicher Eingang, gleiche Verzögerung, beliebiges Modul): 3 Abtastzeiten + 25 ms maximal

Virtueller Eingang (Mute Enable und On/Off) Timing (FID 2 oder höher): RPI + 200 ms typisch

Virtuelle Eingabe (manuelle Rückstellung und Abbruchverzögerung) (FID 2 oder höher): siehe „7.7 Virtuelle nicht sicherheitsrelevante Eingangsgeräte“ auf Seite 57 für Details

AUS-Verzögerungstoleranz

Das Maximum ist die in der Konfigurationsübersicht angegebene Antwortzeit plus 0,02%.

Das Minimum ist die konfigurierte AUS-Verzögerungszeit minus 0,02% (unter der Annahme, dass kein Stromausfall oder Fehler vorliegt)

ON-Verzögerungstoleranz

Das Maximum ist die konfigurierte Einschaltverzögerung plus 0,02% plus 250 ms typisch (400 ms maximal)

Das Minimum ist die konfigurierte Einschaltverzögerung minus 0,02%.

Zertifizierungen



Programmierbare Sicherheitssteuerung 3NBN



Konformität

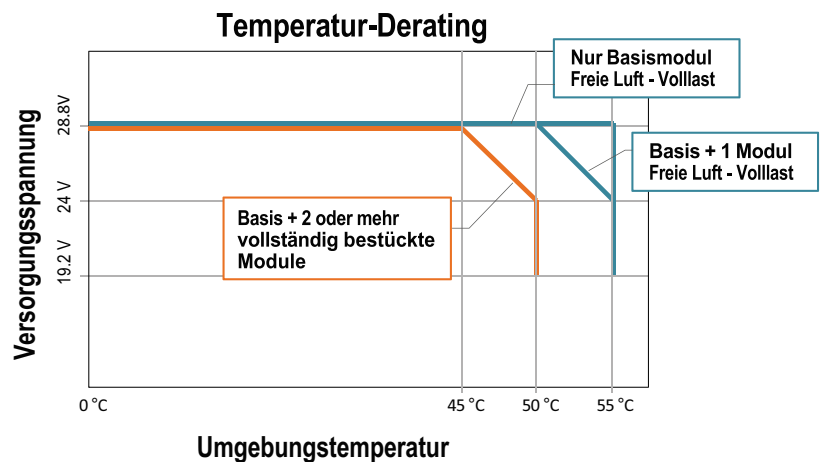


Abbildung 9: SCx-DCD Temperatur-Derating



■ SCx-O-2T und SCx-O-4T Solid-State-Sicherheitsausgangsmodule

Solid-State-Sicherheitsausgänge

SCx-O-2T: 0,75 A maximal bei 24 V DC (1,0 V DC maximaler Abfall)

SCx-O-4T/SCx-O-4T: 0,5 A maximal bei 24 V DC (1,0 V DC maximaler Abfall)

Einschaltstrom: 2 A maximal

Schwellenwert Ausgang aus: 1,7 V DC typisch (2,0 V DC maximal)

Ausgangsleckstrom: 50 µA maximal bei offenen 0 V Last; 0,1 µF max., 1 H max., 10 Ω maximal pro Leitung

Sicherheitsbewertungen

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

Proof-Test-Intervall: 20 Jahre

Externe Stromversorgung

SCx-O-2T: 24 V DC ± 20% (einschließlich Restwelligkeit); 0,075 A Leerlauf, 3,075 A Höchstlast

SCx-O-4T: 24 V DC ± 20% (einschließlich Restwelligkeit); 0,1 A Leerlauf, 4,1 A Höchstlast

Maximale Einschaltverzögerung: 5 Sekunden nach dem Basis-Controller

Begrenzte Isolierung: maximal ±30 V DC, bezogen auf 0 V am Basis-Controller

Bus-Strom

0,02 A

Prüfimpuls

Breite: maximal 200 µs

Rate: 200 ms typisch

Schutz des Ausganges

Alle Halbleiterausgänge (Sicherheits- und Nicht-Sicherheitsausgänge) sind gegen Kurzschlüsse gegen 0 V oder +24 V, einschließlich Überstrombedingungen

Zertifizierungen



Programmierbare
Sicherheitssteuerung
3NBN

Konformität



■ SCx-I-8 und SCx-I-16 Sicherheits-Eingangsmodule

Konvertierbare E/A

Stromaufnahme: maximal 80 mA bei 55 °C (131 °F) Betriebsumgebungstemperatur (überstromsicher)

Prüfimpulse: etwa 1 ms alle 25 ms bis 75 ms

Bus-Strom

SCx-I-8: 0,07 A ohne Last; 0,23 A maximale Last

SCx-I-16: 0,09 A ohne Last; 0,41 A maximale Last

Sicherheitsbewertungen

PFH [1/h]: 4×10^{-10}

Proof-Test-Intervall: 20 Jahre

Sicherheitseingänge (und konvertierbare E/A bei Verwendung als Eingänge)

Einschaltswelle: > 15 V DC (garantiert eingeschaltet), maximal 30 V DC

Eingang-Aus-Schwelle: < 5 V DC und < 2 mA, mindestens -3 V DC

Eingang Einschaltstrom: 5 mA typisch bei 24 V DC, 50 mA Spitzenstrom zur Kontaktreinigung bei 24 V DC

Widerstand der Eingangsleitung: 300 Ω max. (150 Ω pro Leitung)

Eingangsanforderungen für eine 4-Draht-Schaltmatte:

- Maximale Kapazität zwischen den Platten: 0,22 µF
- Maximale Kapazität zwischen Bodenplatte und Erde: 0,22 µF
- Maximaler Widerstand zwischen den 2 Eingangsklemmen einer Platte: 20 Ω

Schutz des Ausganges

Die konvertierbaren Eingänge sind gegen Kurzschlüsse gegen 0 V oder +24 V geschützt, einschließlich Überstrombedingungen

Zertifizierungen



Programmierbare
Sicherheitssteuerung
3NBN

Konformität



■ SCx-O-1R und SCx-O-2R Sicherheitsrelais-Module

Bus-Strom

SCx-O-1R: 0,125 A (Ausgänge eingeschaltet)

SCx-O-2R: 0,15 A (Ausgänge eingeschaltet)

Maximale Leistung

2000 VA, 240 W

Elektrische Lebensdauer

50.000 Zyklen bei voller Widerstandslast

Überspannungskategorie

III

Grad der Verschmutzung

2

Mechanische Lebensdauer

40.000.000 Zyklen

Schaltleistung UL/NEMA:

- **Schließer:** 6 A 250 V AC/24 V DC ohmsch; B300/Q300 Steuerbetrieb

- **Öffnerkontakte:** 2,5 A 150 V AC/24 V DC ohmsch; Q300 Pilotbetrieb

IEC 60947-5-1:

- **Schließer:** 6 A 250 V AC/DC kontinuierlich; AC 15: 3 A 250 V; DC13: 1

- A 24 V/4 A 24 V 0,1 Hz

- **Öffnerkontakte:** 2,5 A 150 V AC/DC kontinuierlich; AC 15: 1 A 150 V; DC13:

- 1 A 24 V/4 A 24 V 0,1 Hz

Kontaktwerte zur Erhaltung der 5 µm AgNi-Goldbeschichtung

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



Hinweis: Beim Schalten von induktiven Lasten wird eine Transientenunterdrückung empfohlen. Installieren Sie Entstörglieder über der Last. Installieren Sie niemals Entstörglieder über den Ausgangskontakten.

Sicherheitsbewertungen

PFH [1/h]: $7,6 \times 10^{-10}$

Proof-Test-Intervall: 20 Jahre

B10d Werte

Spannung	Strom	B10d
230 V AC	3 A	300.000
230 V AC	1 A	750.000
24 V DC	≤ 2 A	1.500.000



WARNUNG: Die elektrischen Anschlüsse müssen von qualifiziertem Personal in Übereinstimmung mit den örtlichen und nationalen elektrischen Vorschriften und Bestimmungen vorgenommen werden.



Der Überstromschutz muss je nach Endproduktanwendung gemäß der mitgelieferten Tabelle vorgesehen werden. Der Überstromschutz kann mit einer externen Sicherung oder über eine strombegrenzende Stromversorgung der Klasse 2 erfolgen.

Die Leitungen der Versorgungskabel < 24 AWG dürfen nicht gespleißt werden. Weitere Informationen zur Produktunterstützung finden Sie unter www.bernstein.eu.

Verdrahtung (AWG)	Erforderlicher Überstromschutz (Ampere)
20	5.0
22	3.0
24	2.0
26	1.0
28	0.8
30	0.5

Zertifizierungen



Programmierbare
Sicherheitssteuerung
3NBN



Konformität



■ SCx-N-Cat EtherCAT Kommunikations-Gateway-Modul

Netzwerk-Schnittstelle

EtherCAT® 5

Datenübertragungsrate: 100 Mbits/s, 100 Base-T Autosensing

Anschlussart: Zwei RJ-45-Buchsen

Mechanische Belastung

Schock: 15 g für 11 ms, Halbsinuswelle, insgesamt 18 Schocks (gemäß IEC 61131-2)

Vibration: 3,5 mm gelegentlich / 1,75 mm kontinuierlich bei 5 Hz bis 9 Hz, 1,0 g gelegentlich und 0,5 g kontinuierlich bei 9 Hz bis 150 Hz: alle bei 10 Sweep-Zyklen pro Achse (gemäß IEC 611312)

EMC

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

Bus-Strom

0,06 A

Betriebsbedingungen

Temperatur: 0 °C bis +55 °C (+32 °F bis +131 °F)

Lagertemperatur: -30 °C bis +65 °C (-22 °F bis +149 °F)

Luftfeuchtigkeit: 90% bei +50 °C maximale relative Luftfeuchtigkeit (nicht kondensierend)

Betriebshöhe: maximal 2000 m (6562 ft) gemäß IEC 61010-1

Umweltbewertung

NEMA 1 (IEC IP20), zur Verwendung in NEMA 3 (IEC IP54) oder besseren Gehäusen

Zertifizierungen



5.2 Spezifikationen für das SCR P

Stromversorgung

Strom:

- Max. 240 mA, keine Last (Relais ein)
- Max. 530 mA, volle Last (IO1 bis IO4 als Hilfsausgänge verwendet)

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

- Einschaltswellenwert für Eingang:** > 15 V DC (garantiert ein), max. 30 V DC
- Ausschaltswellenwert für Eingang:** < 5 V DC und < 2 mA, min. – 3 V DC mindestens
- Einschaltswellenwert für Eingang:** 5 mA typisch bei 24 V DC, 50 mA Kontaktreinigungs-Spitzenstrom bei 24 V DC
- Widerstand der Eingangsleitungen:** max. 300 Ohm (150 Ohm pro Leitung)
- Eingangsanforderungen für eine 4-adrige Schaltmatte:**
 - Max. Kapazität zwischen Platten: 0,22 µF¹
 - Max. Kapazität zwischen unterer Platte und Erde: 0,22 µF¹
 - Max. Widerstand zwischen den 2 Eingangsanschlüssen derselben Platte: 20 Ω

Konfigurierbare E/A

- Stromversorgung:** max. 80 mA (Überstromschutz)
- Testimpulse:** ~1 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 PROFI-NET
- Daten:** 256 konfigurierbare virtuelle Statusausgänge; Fehlerdiagnosecodes und -meldungen; Zugriff auf Fehlerprotokoll

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 „7.7 Virtuelle nicht sicherheitsrelevante Eingangsgeräte“ auf Seite 57.

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
Leistung	100 mW (100 mVA)	200 W (2000 VA)

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



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

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



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.

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)



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.



Sicherheitsklasse

PFH [1/h]: $5,01 \times 10$

Gebrauchsdauer: 20 Jahre

Stromversorgungsdrähte (mm ² / 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

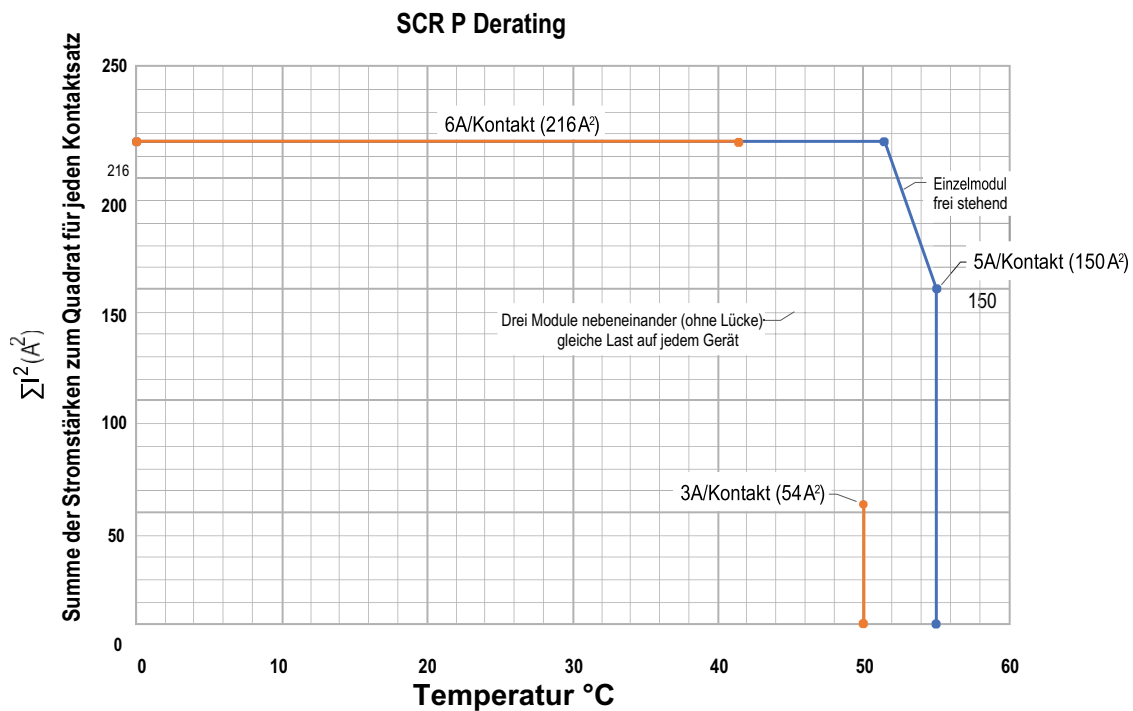
Produktnormen

Im Abschnitt „18. Normen und Vorschriften“ auf Seite 253 finden Sie eine Liste der geltenden internationalen und US-Industrienormen.

Zertifizierungen



Konformität



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)
$I_1 = 4 \text{ A}$ (Schließerausgang RO1 Kanal 1) →	$I_1 = 4 \text{ A}$
$I_2 = 4 \text{ A}$ (Schließerausgang RO1 Kanal 2) →	$I_2 = 4 \text{ A}$
$I_3 = 4 \text{ A}$ (Schließerausgang RO1 Kanal 3) →	$I_3 = 4 \text{ A}$
$I_4 = 4 \text{ A}$ (Schließerausgang RO2 Kanal 4) →	$I_4 = 4 \text{ A}$
$I_5 = 4 \text{ A}$ (Schließerausgang RO2 Kanal 5) →	$I_5 = 4 \text{ A}$
$I_6 = 4 \text{ A}$ (Schließerausgang RO2 Kanal 6) →	$I_6 = 4 \text{ A}$

Beispiel für die Berechnung des Temperaturabzugs

Einzelnes Gerät, frei stehend	Drei Module
$\Sigma I^2 = 4^2 + 4^2 + 4^2 + 4^2 + 4^2 + 4^2 = 96 \text{ A}^2$	→ $\Sigma I^2 = 4^2 + 4^2 + 4^2 + 4^2 + 4^2 + 4^2 = 96 \text{ A}^2$
$T_{\text{max}} = 55 \text{ °C}$	→ $T_{\text{max}} = 46 \text{ °C}$

5.3 Abmessungen

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

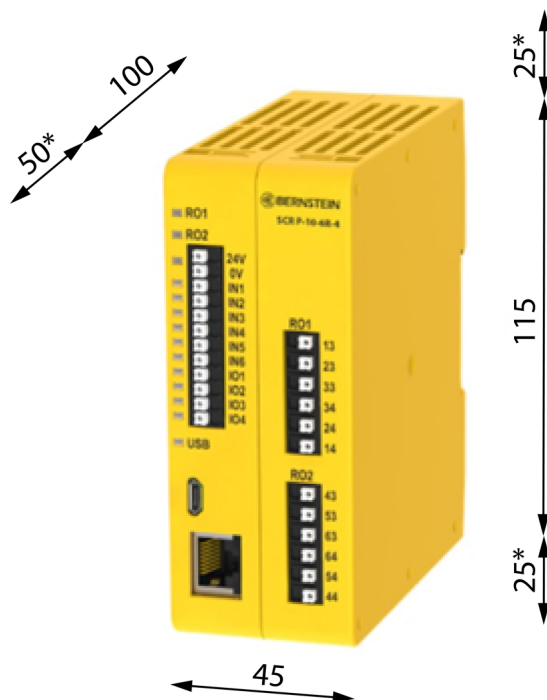


Abbildung 10: Abmessungen des SCR P

* kleinster Einbauabstand





Abbildung 11: Abmessungen der Basissteuerung

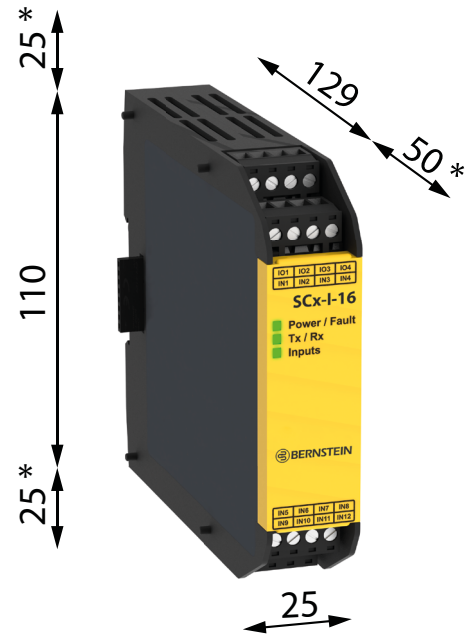


Abbildung 12: Abmessungen des Erweiterungsmoduls

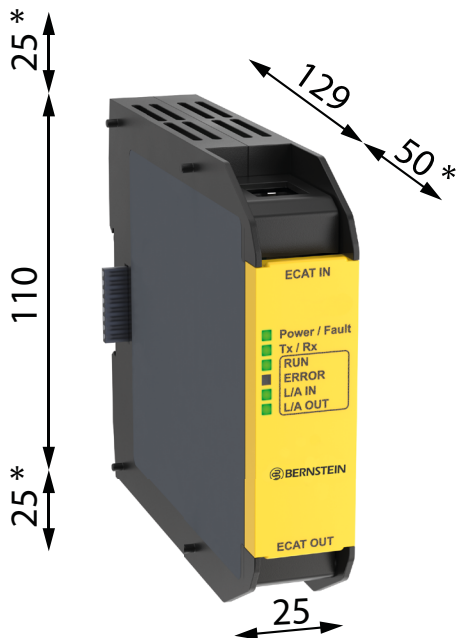


Abbildung 14: Abmessungen des EtherCat-Moduls

* kleinster Einbauabstand

5.4 Systemvoraussetzungen für den PC



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

Betriebssystem:	Microsoft Windows 7, Windows 8 (außer Windows RT) oder Windows 102
Systemverschlüsselungstyp:	32-Bit, 64-Bit
Festplattenspeicher:	80 MB (plus bis zu 280 MB für Microsoft .NET 4.0, falls es nicht bereits installiert ist)
Arbeitsspeicher (RAM):	Mindestens 512 MB, mindestens 1 GB empfohlen
Prozessor:	Mindestens 1 GHz, 2 GHz+ empfohlen
Bildschirmauflösung:	Farbbildschirm mit mindestens 1024 × 768 Pixeln, Farbbildschirm mit 1650 × 1050 Pixeln empfohlen
Drittanbietersoftware:	Microsoft .NET 4.0 (im Installationsprogramm enthalten), PDF-Anzeigeprogramm (z. B. Adobe Acrobat)
USB-Port:	USB 2.0 (kein Konfigurationsaufwand erforderlich)



6. Systeminstallation

6.1 Installation der Software



Wichtig: Für die Treiberinstallation 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.
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 die **Konfigurationssoftware** vom **Arbeitsplatz aus** oder über das **Start-Menü**.

6.2 Installation der Sicherheitsauswertung

Um einen zuverlässigen Betrieb zu gewährleisten, dürfen die Betriebsdaten nicht überschritten werden. Das Schaltschrankgehäuse muss eine entsprechende Wärmeabstrahlung ermöglichen, sodass die Temperatur der Luft rund um die Sicherheitsauswertung die maximale Betriebstemperatur nicht überschreiten kann (siehe „5. Spezifikationen und Anforderungen“ auf Seite 18).



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 Anwendungshinweise für den Umgang mit elektrostatischen Entladungen beachten: Tragen Sie z. B. ein zugelassenes Erdungsarmband oder berühren Sie vor dem Umgang mit den Modulen einen geerdeten Gegenstand. Weitere Informationen über den Umgang mit elektromagnetischen Entladungen finden Sie in ANSI/ESD S20.20.

6.2.1 Montageanleitung

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.



7. Überlegungen vor der Installation

7.1 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.



7.2 SCx-Anwendungen

Der Safety Controller kann überall dort eingesetzt werden, wo Sicherheitsmodule verwendet werden. Die Sicherheitssteuerung eignet sich für viele Arten von Anwendungen, einschließlich, aber nicht beschränkt auf:

- Zweihandbedienung mit Stummschaltfunktion
- Roboter-Schweiß-/Bearbeitungszellen mit Zwei-Zonen-Muting
- Materialhandhabungsvorgänge, die mehrere Eingänge und Bypass-Funktionen erfordern
- Manuell beschickte Rotationsladestationen
- Mehrere Anwendungen für Zweihandbedienungsstationen
- Stationen der schlanken Produktion
- Dynamische Überwachung von ein- oder zweipoligen Magnetventilen oder Pressensicherheitsventilen

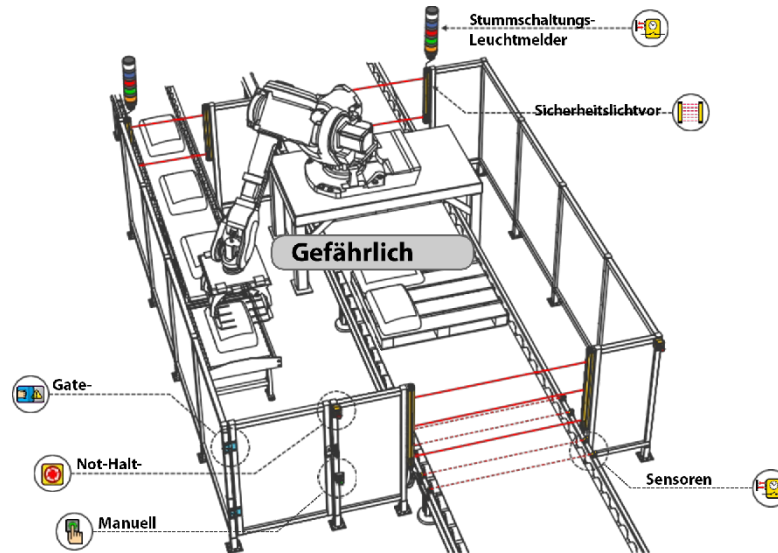


Abbildung 15: Anwendungsbeispiel Roboterzelle



7.3 SCR P-Anwendungen

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

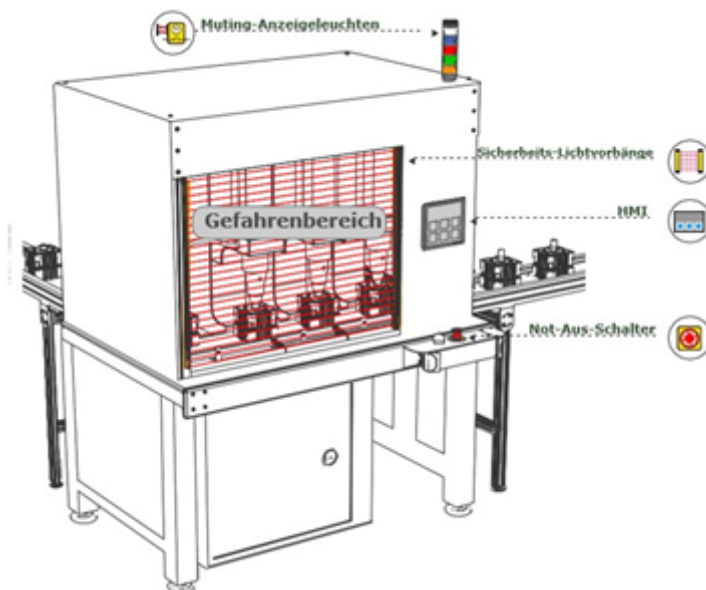


Abbildung 16: Anwendungsbeispiel 1 für das SCR P

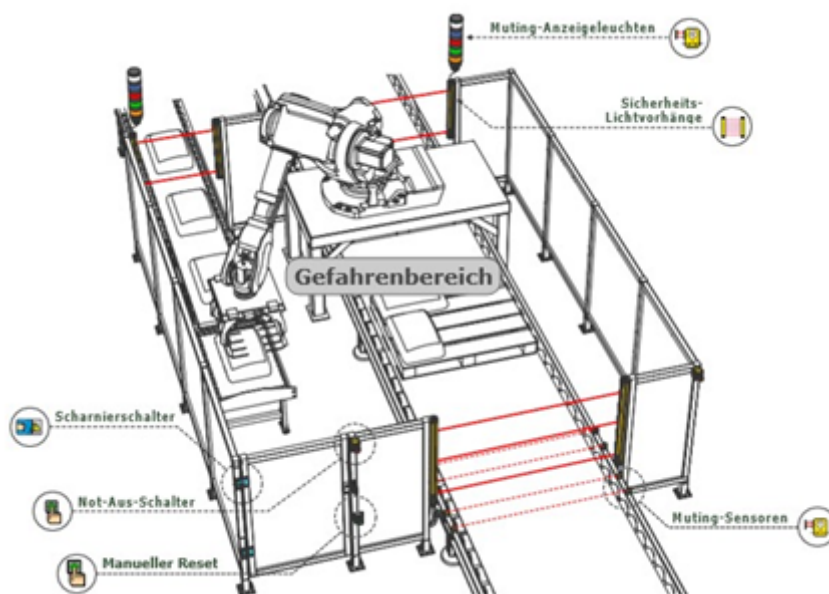


Abbildung 17: Anwendungsbeispiel 2 für das SCR P



7.4 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, Sicherheitssensoren und Abschaltetelemente) 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 einen 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 sämtliche Störungen erfassen und unverzüglich beheben können.



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

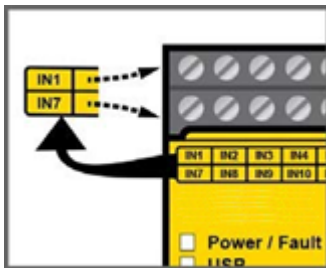


Abbildung 18: Lage der SCx Klemmen

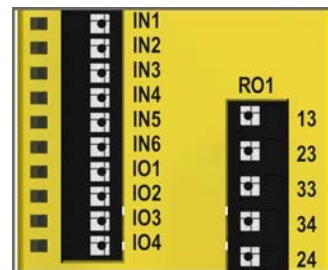


Abbildung 19: Position der Eingangs- und Ausgangsanschlüsse am SCR P



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.



7.4.1 Widerstandsfähigkeit gegen Fehler und Sicherheitsschaltungsprinzipien 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 „7.5 Optionen für Sicherheitseingangsgeräte“ auf Seite 36).



**WARNUNG:**

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

Fehlerausschluss

Ein wichtiger Begriff in den Anforderungen von ISO 13849-1 ist die Wahrscheinlichkeit des Auftretens eines Fehlers. Diese kann mit einer Methode verringert werden, die als „Fehlerausschluss“ bezeichnet wird. Dies basiert auf der 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 Fehlerausschluss ist ein Instrument, das Konstrukteure bei der Entwicklung der sicherheitsrelevanten Teile des Steuersystems und beim Risikobewertungsprozess verwenden können. Mit dem Fehlerausschluss kann der Konstrukteur die Möglichkeit mehrerer Fehler ausschließen und dies mit dem Risikobeurteilungsprozess begründen, um die gewünschte 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.

7.4.2 Eigenschaften von Sicherheitseingängen

Die Sicherheitsauswertung wird über die Software konfiguriert, um viele Arten von Sicherheitsschaltgeräten zu unterstützen. Siehe „8.2 Hinzufügen von Eingängen und Statusausgängen“ auf Seite 77 für weitere Informationen über die Konfiguration der Eingänge.

Reset-Logik: manueller oder automatischer Reset

Ein manueller Reset kann für Sicherheitseingänge erforderlich sein, indem ein LatchResetBlock verwendet oder ein Sicherheitsausgang für einen LatchReset 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 ³ :	Ein-Zustand: Sicherheitsausgang schaltet sich ein, wenn ⁴ :				
<p>Zweikanalig A und B antivalent</p> <p>2 Anschlüsse 24 V 3 Anschlüsse, 2 Anschlüsse pnp EIN AUS</p>	<p>Mindestens 1 Kanaleingang (A oder B) ist im Aus-Zustand.</p>	<p>Simultan: A und B sind beide im Aus-Zustand und schalten dann beide innerhalb von 3 s in den Ein-Zustand.</p> <p>Nicht simultan: A und B sind beide im Aus-Zustand und schalten dann beide ohne begrenztes Zeitfenster in den Ein-Zustand.</p>				
<p>Zweikanalig A und B</p> <p>2 Kanäle, 2 Anschlüsse 24 V 2 Kanäle, 3 Anschlüsse 2 Kanäle, 4 Anschlüsse 2 Kanäle, 2 Anschlüsse pnp EIN AUS</p>			<p>Zweikanalig A und B 2x antivalent</p> <p>4 Anschlüsse 24 V 5 Anschlüsse</p> <p>pnp EIN AUS EIN AUS</p>	<p>Mindestens 1 Kanal (A oder B) eines Kontaktpaars im Aus-Zustand.</p>	<p>Simultan: 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.</p> <p>Nicht simultan: 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.</p>	<p>4-adrige Sicherheitsmatte</p> <p>2 Kanäle, 4 Anschlüsse</p>
<p>Zweikanalig A und B 2x antivalent</p> <p>4 Anschlüsse 24 V 5 Anschlüsse</p> <p>pnp EIN AUS EIN AUS</p>	<p>Mindestens 1 Kanal (A oder B) eines Kontaktpaars im Aus-Zustand.</p>	<p>Simultan: 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.</p> <p>Nicht simultan: 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.</p>				
<p>4-adrige Sicherheitsmatte</p> <p>2 Kanäle, 4 Anschlüsse</p>	<p>Eine der folgenden Bedingungen ist erfüllt:</p> <ul style="list-style-type: none"> • Eingangskanäle untereinander kurzgeschlossen (Normalbetrieb) • Mindestens ein Kabel ist gelöst • Einer der offenen Kanäle wird als geschlossen erfasst • Einer der geschlossenen Kanäle wird als offen erfasst 	<p>Jeder Kanal ist mit seinen eigenspezifischen Impulsen behaftet.</p>				

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.

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

4 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.

7.5 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 <small>(siehe Anmerkung 1)</small>		Kat.2	Kat.2	Kat.2	Kat.2	Kat.2				
2 und 3 Anschlüsse 2 Kanäle <small>(siehe Anmerkung 2)</small>		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 <small>(siehe Anmerkung 3)</small>		Kat.4	Kat.4	Kat.4	Kat.4	Kat.4		Kat.4	Typ IIIa Kat.1	Kat.4
3 und 4 Anschlüsse 2 Kanäle <small>(siehe Anmerkungen 2 und 4)</small>		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 Antivalenter PNP-Ausgang			Kat.4	Kat.4	Kat.4	Kat.4				Kat.4
4 und 5 Anschlüsse 2 Kanäle Antivalent			Kat.4						Typ IIIc Kat.4	Kat.4
4 Anschlüsse, 2 Kanäle Antivalenter PNP-Ausgang			Kat.4						Typ IIIc Kat.4	Kat.4
Sicherheitsmatte mit 4 Anschlüssen							Kat.3			

Abbildung14: 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 an der Sicherheitsauswertung 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) 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.



7.5.1 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.

7.5.2 Zustimmungstaster



Ein Zustimmungstaster ist ein manuell bedientes Steuergerät, das bei dauernder Betätigung zusammen mit einem Starttaster, die Initiierung eines Maschinenzyklus zulässt. Normen, die Gestaltung und Anwendung von Zustimmungstastern abdecken, umfassen: ISO 12100-1/-2, IEC 60204-1, ANSI/NFPA 79, ANSI/RIA R15.06 und ANSI B11.19.

Der Zustimmungstaster steuert aktiv die Aufhebung eines Stoppsignals während eines Abschnitts des Maschinenbetriebs, bei der eine Gefahrensituation eintreten kann. Der Zustimmungstaster ermöglicht es einem gefährlichen Maschinenteil zu laufen, darf es aber nicht starten. Ein Zustimmungstaster 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 Zustimmungstaster muss die letztendliche Möglichkeit zum Abschalten oder Stoppen der gefährlichen Maschinenbewegung haben.**

7.5.3 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..

7.5.4 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 „7.5.3 Not-Halt-Schalter“ auf Seite 37 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, Metallspäne oder Feilstaub usw., muss verhindert werden, da diese den Betrieb beeinträchtigen könnte.
- Verwenden Sie nur Seilrollen (keine Hebeösen), wenn das Seil um Ecken geführt wird oder wenn die Richtung geändert wird – auch bei geringfügigen Richtungsänderungen.



- Verlegen Sie das Seil bzw. Kabel niemals durch Rohre.
- Befestigen Sie niemals Gewichte am Seil
- Eine 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.

7.5.5 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 Sicherheitschaltungen wird durch eine Risikobeurteilung ermittelt und ergibt die zulässige Sicherheitskategorie (siehe „7.4.1 Widerstandsfähigkeit gegen Fehler und Sicherheitschaltungsprinzipien nach ISO 13849-1“ auf Seite 33). 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.

7.5.6 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 Abschalteteile 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 / Abschaltetelemente 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**

7.5.7 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 „7.6.1 Manueller Reset-Eingang“ auf Seite 55).

7.5.8 Zweihandsteuerung



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

Die Bedienelemente der Zweihandsteuerung (THC) müssen so angeordnet sein, dass die gefährliche Bewegung abgeschlossen ist oder gestoppt wird, bevor der Bediener einen oder beide Taster loslassen und den Gefahrenbereich erreichen kann (siehe „Berechnung des Sicherheitsabstands (Mindestabstands) für Zweihandsteuerungen“ auf Seite 41). 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 feststehendes 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 Wiederanlauf Sperre haben**

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

Dieses BERNSTEIN-Gerät kann zur Ausführung einer Wiederanlauf Sperre 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 USA

Die Formel für Sicherheitsabstand gemäß ANSI B11.19:

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

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

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

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

D_s

der Sicherheitsabstand (in Zoll)

K

die von OSHA/ANSI empfohlene Handgeschwindigkeitskonstante (in Zoll pro Sekunde); diese wird in den meisten Fällen bei 63 in/s berechnet, kann jedoch von 63 in/s bis 100 in/s variieren, je nach den Umständen der Anwendung; keine unumstößlichen Werte; bei der Bestimmung des Wertes von K sollten vom Arbeitgeber alle Faktoren einschließlich der körperlichen Fähigkeiten der Bedienungsperson berücksichtigt werden.

T_h

die Ansprechzeit der langsameren Zweihandsteuerung (vom Zeitpunkt, an dem ein Handschalter losgelassen wird, bis zum Öffnen des Schalters); T_h ist für rein mechanische Schalter gewöhnlich nicht von Bedeutung. T_h sollte jedoch zur Berechnung von Sicherheitsabständen in Betracht gezogen werden, wenn elektronische oder elektromechanische Handsteuerungen verwendet werden

T_m

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

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

N = Anzahl der Kupplungs-Einrückpunkte pro Umdrehung

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

T_r

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

T_s 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)

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.



7.5.9 Schaltmatte



Die Sicherheitsauswertung kann zur Überwachung von druckempfindlichen Sicherheitsschaltmatten und Sicherheitsschaltleisten 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 46).



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: Anordnung der Zweihandsteuerungen

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 Tippbetrieb 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 Dichtwirkung kann zum Eintreten von Flüssigkeit in die Matte führen und möglicherweise den Verlust der Sensorempfindlichkeit bewirken. Eventuell müssen die Endstücke der Anschlusskabel in einem Gehäuse mit einer geeigneten Schutzart untergebracht werden.

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

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

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

Installation von 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 Betriebsspezifikationen (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, manipulations sichere 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 Schutzeinrichtung 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-Schutzeinrichtung verwendet (siehe ANSI B11.19, ANSI/RIA R15.06 und ISO 13855).

Der für eine Anwendung erforderliche Sicherheitsabstand (Mindestabstand) hängt von mehreren Faktoren ab, u. a. von der Geschwindigkeit der Hand (oder Person), der Gesamt-Systemstopzeit (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.

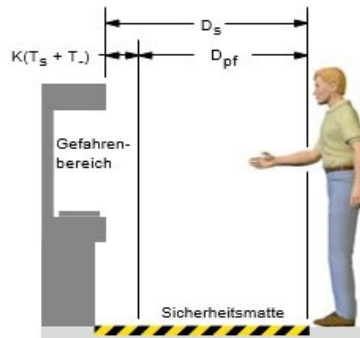


Abbildung 20: Ermittlung des Sicherheitsabstands für die Schaltmatte

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

T_s 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.

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
der Mindestabstand (in Millimeter)

C
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.

Anschlussoptionen für Schaltmatten

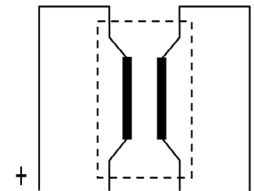
Druckempfindliche Matten und druckempfindliche Böden müssen die Anforderungen der Kategorie erfüllen, für die sie spezifiziert und gekennzeichnet sind. Diese Kategorien sind in ISO 13849-1 definiert.

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.



7.5.10 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 (nichtleitende) 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 (nichtleitend) sein.

Zwangöffnende 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 Schließkontakte, pnp-Ausgänge (die jeweils die in den „5. Spezifikationen und Anforderungen“ auf Seite 18 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).

7.5.11 Überbrückungsschalter



Bei der Überbrückung einer Schutzeinrichtung handelt es sich um eine manuell aktivierte und vorübergehende Aufhebung eines oder mehrerer Stoppsignale für die Sicherheitseingänge unter Aufsicht, wenn keine unmittelbare Gefahr besteht. Dazu wird gewöhnlich 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 Anforderungen⁵:

- 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 Gefahrensituation 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).

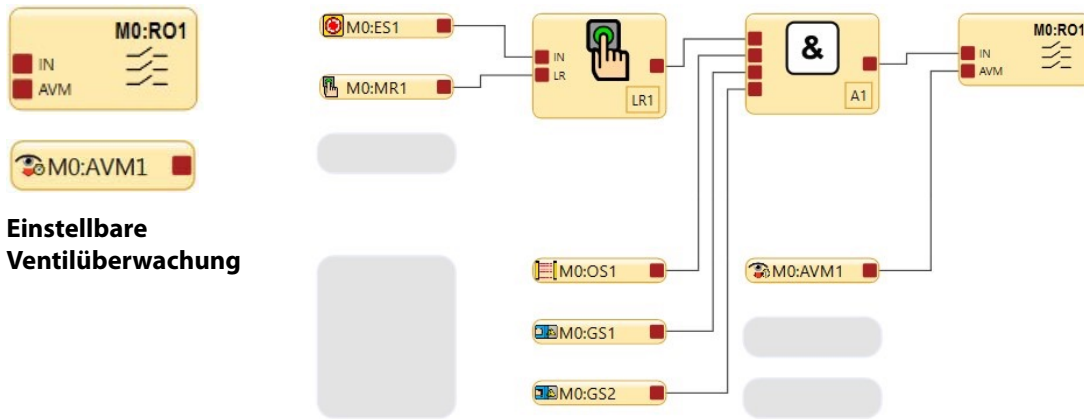
7.5.12 AVM-Funktion (Adjustable Valve Monitoring, einstellbare Ventilüberwachung)



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 67). Die AVM-Funktion überwacht den Status von Geräten, die von dem Sicherheitsausgang gesteuert werden, dem die Funktion zugeordnet ist. Wenn sich der Sicherheitsausgang ausschaltet, muss der AVM-Eingang 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.

⁵ 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.





Einstellbare Ventilüberwachung

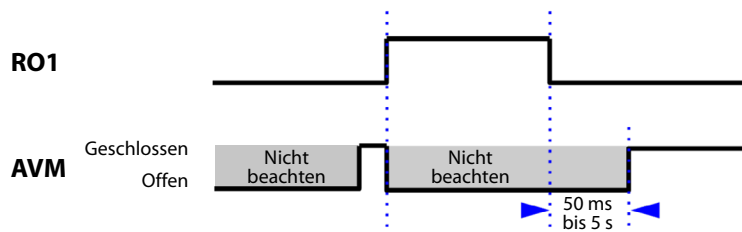


Abbildung 21: Zeitgeberlogik - AVM-Funktion

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.



7.5.13 DCD-Eingänge



Über die Sicherheitseingänge DCD-Eingänge

SCR P:

- IN3/IN4
- IN5/IN6

SCx:

- IN1/IN2
- IN3/IN4
- IN5/IN6
- IN7/IN8
- IN9/IN10
- IN11/IN12
- IN13/IN14
- IN15/IN16

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 „7.6.1 Manueller Reset-Eingang“ auf Seite 55.



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.

7.5.14 Zykluseinleitung für Funktionsblock Pressensteuerung

Diese Funktion ist bei SCx verfügbar.

Ein einzelner, momentaner Aktuator kann als Auslösevorrichtung für kleine hydraulische/pneumatische Pressen verwendet werden, wenn er mit dem Funktionsblock Pressensteuerung verwendet wird und für die Steuerung mit einem Aktuator konfiguriert ist. Es handelt sich dabei um einen Initiierungseingang zum Starten des Pressenzyklus. Wenn die Einzelantriebssteuerung ausgewählt ist, kann der Bediener den Zyklus mit diesem Eingang starten und dann loslassen und andere Aufgaben ausführen.



VORSICHT: Es müssen andere Vorkehrungen getroffen werden, um sicherzustellen, dass die Bediener vor den Gefahren geschützt sind, da ihre Hände nicht während der gesamten Bewegung der Presse in den Knopf eingreifen müssen.

Der Zugang zur Gefahrstelle muss mit anderen Mitteln als einer Einschalttaste gesichert werden, z. B. mit Lichtvorhängen, Toren usw. Diese Sicherheitseinrichtungen müssen ebenfalls an die Eingänge des Funktionsblocks Press Control angeschlossen werden.

Der Eingang für die Zykluseinleitung kann an den GO-Knoten des Press Control Function Blocks oder an den IN-Knoten eines Bypass-Blocks angeschlossen werden, der mit dem GO-Knoten des Press Control Function Blocks verbunden ist. Der Zyklusauslöser muss an einer Stelle montiert werden, die den folgenden Warnhinweisen entspricht.



**WARNUNG:**

- **Ordnungsgemäße Installation von Zyklusauslösern**
- Wenn die Zyklusauslöser nicht ordnungsgemäß installiert werden, kann dies zu schweren Verletzungen oder zum Tod führen.
- Installieren Sie die Zyklusauslöser so, dass sie nur von außerhalb des gesicherten Raums und in voller Sicht zugänglich sind. Zyklusauslöser dürfen nicht von innerhalb des gesicherten Raums zugänglich sein. Sichern Sie Zyklusauslöser gegen unbefugte oder versehentliche Betätigung (z. B. durch Ringe oder Schutzvorrichtungen). Falls es gefährliche Bereiche gibt, die von den Taktgebern aus nicht einsehbar sind, sind zusätzliche Sicherungen vorzusehen.

7.5.15 Pressensteuerung Sequentieller Stopp (SQS) Funktion

Diese Funktion ist bei SCx verfügbar.

Der Eingang Press Control Sequential Stop (SQS) signalisiert der Pressensteuerung, dass der Pressenstößel eine Position erreicht hat, in der keine Quetschgefahr mehr besteht (weniger als 6 mm Spalt). Die Abwärtsbewegung des Pressenstößels stoppt an diesem Punkt. Der Bediener kann seine Hände von der Zweihandsteuerung nehmen, um sich zu vergewissern, dass sich das Werkstück in der richtigen Position befindet (der Mutable Safety-Eingang ist zu diesem Zeitpunkt stummgeschaltet). Nachdem der Bediener sichergestellt hat, dass sich das Werkstück in der richtigen Position befindet, betätigt er den Fußschaltereingang, um den Abwärtshub zu beenden.

**Hinweis:**

Die oben beschriebene Methode ist eine Möglichkeit, den Prozess der Pressesteuerung zu steuern. Es gibt drei zulässige Prozesse:

1. Der Zweihand-Steuerzugang (TC1) schaltet den GO-Eingang ein, um die Ramme auf den SQS-Punkt zu fahren. Lassen Sie TC1 los und schalten Sie FS1 ein, um den Fußschalterzugang einzuschalten und die Ramme auf den unteren Hubpunkt (BOS) zu fahren, lassen Sie den Fußschalterzugang (FS1) los und schalten Sie TC1 ein, um die Ramme anzuheben.
2. FS1 schaltet den GO-Eingang ein, um den Stempel zum SQS-Punkt zu fahren, FS1 loslassen. Durch erneutes Einschalten von FS1 wird die Ramme auf den BOS-Punkt und dann wieder auf den TOS-Punkt (Top of Stroke) gefahren. (Der Eingang Ft Switch verschwindet, wenn FS1 mit dem GO-Knoten verbunden ist).
3. TC1 schaltet den GO-Eingang ein, um den Stößel zum SQS-Punkt zu fahren, TC1 freigeben. Beim erneuten Aktivieren von TC1 fährt der Stößel zum BOS-Punkt und dann wieder zurück zum TOS-Punkt (oberes Hubende). (Um das System für diese Methode einzurichten, wählen Sie NICHT den Fußpedal-Knoten im Funktionsblock für Pressesteuerungseingänge aus.)

Der Eingang „Sequential Stop“ wird normalerweise verwendet, wenn „Dual Pressure“ ausgewählt ist. Die Doppeldruckfunktion erfordert vier Sicherheitsausgänge (Auf, Ab, Niederdruck und Hochdruck). Aus diesem Grund ist der Eingang „Sequential Stop“ bei nicht erweiterbaren Modellen nicht verfügbar.

Der Eingang „Sequential Stop“ kann den Eingang „Mutable Safety“ direkt stummschalten oder zusammen mit dem Eingang „Press Control Mute Sensor“ arbeiten, um den Eingang „Mutable Safety“ des Pressensteuerungssystems stummzuschalten (zum Eingang „Press Control Mute Sensor“ siehe „Press Control Mute Sensor“ auf Seite 53).

Der Eingang für den sequenziellen Stopp kann ein- oder zweikanalig sein, je nach den Anforderungen des Systems. Die Eingabegeräte müssen so positioniert werden, dass der Pressenstößel in einer Position anhält, die keinen so großen Spalt aufweist, dass ein Finger eindringen kann (der Spalt muss weniger als 6 mm/0,25 Zoll betragen).



Hinweis: Wenn für den Eingang „Sequentieller Stopp“ eine einkanalige Konfiguration gewählt wird, muss er zusammen mit dem Eingang „Press Control Mute Sensor“ funktionieren, um den Eingang „Press Control Mutable Safety Stop“ stummzuschalten. Wenn eine Zweikanal-Konfiguration für den Eingang „Sequentieller Stopp“ gewählt wird, kann er den Eingang „Press Control Mutable Safety Stop“ direkt selbst stummschalten.

Die US-amerikanischen und internationalen Normen verlangen, dass der Benutzer das Sicherheitssystem so anordnet, installiert und betreibt, dass das Personal geschützt und die Möglichkeit der Umgehung des Schutzes minimiert wird.



**WARNUNG:**

- Vermeiden Sie gefährliche Installationen
- Ein einkanaliges SQS-Gerät ist nicht zulässig, es sei denn, es wird in Verbindung mit einem Press Control Mute Sensor (PCMS)-Eingangsggerät verwendet. Wenn ein zweikanaliger SQS-Eingang ohne PCMS verwendet wird, muss jeder SQS-Kanal ein unabhängiger Positionsschalter sein und ordnungsgemäß eingestellt oder positioniert werden, so dass er sich erst schließt, wenn die Gefahr nicht mehr besteht, und sich wieder öffnet, wenn der Zyklus abgeschlossen ist oder die Gefahr erneut besteht. Wenn die Schalter nicht richtig eingestellt oder positioniert sind, kann dies zu Verletzungen oder zum Tod führen.
- Der Benutzer ist dafür verantwortlich, dass alle lokalen, staatlichen und nationalen Gesetze, Regeln, Vorschriften und Bestimmungen in Bezug auf die Verwendung von Sicherheitsausrüstung in einer bestimmten Anwendung eingehalten werden. Stellen Sie sicher, dass alle entsprechenden behördlichen Anforderungen erfüllt sind und dass alle in den entsprechenden Handbüchern enthaltenen Installations- und Wartungsanweisungen befolgt werden.

SQS-Geräte müssen mindestens die folgenden Anforderungen erfüllen. Wenn das SQS-Gerät als Stummschalteingang mit dem Press Control Mute Sensor verwendet wird, muss das Paar die folgenden Anforderungen erfüllen.

1. Es müssen mindestens zwei unabhängige, fest verdrahtete Geräte vorhanden sein.
2. Die Geräte müssen über eine der folgenden Möglichkeiten verfügen: Schließerkontakte, PNP-Ausgänge (die beide die unter Spezifikationen und Anforderungen auf Seite 20 aufgeführten Eingangsanforderungen erfüllen müssen) oder ein komplementäres Schaltverhalten. Mindestens einer dieser Kontakte muss schließen, wenn der Schalter betätigt wird, und muss öffnen (oder nicht leiten), wenn der Schalter nicht betätigt wird oder sich im ausgeschalteten Zustand befindet.
3. Die Aktivierung der Eingänge dieser Stummschaltfunktion muss von separaten Quellen ausgehen. Diese Quellen müssen getrennt montiert werden, um einen unsicheren Zustand zu vermeiden, der durch eine falsche Einstellung, eine falsche Ausrichtung oder einen einzelnen Gleichtaktfehler, wie z. B. eine physische Beschädigung der Montagefläche, entsteht. Nur eine dieser Quellen darf durch eine SPS oder ein ähnliches Gerät geleitet oder von ihr beeinflusst werden.
4. Die Vorrichtungen müssen so installiert werden, dass sie nicht leicht überwunden oder umgangen werden können.
5. Die Geräte sind so zu montieren, dass ihre Lage und Ausrichtung nicht leicht verändert werden kann.
6. Es darf nicht möglich sein, dass Umgebungsbedingungen, wie z. B. extreme Luftverschmutzung, den Stummschaltzustand auslösen.
7. Die Geräte dürfen keine Verzögerungs- oder sonstigen Zeitfunktionen verwenden, es sei denn, diese Funktionen werden so ausgeführt, dass kein Ausfall eines einzelnen Bauteils die Beseitigung der Gefahr verhindert, nachfolgende Maschinenzyklen verhindert werden, bis der Fehler behoben ist, und keine Gefahr durch Verlängerung der Stummschaltzeit entsteht.

**7.5.16 Presse Steuerung Stummschaltungssensor**

Diese Funktion ist bei SCx verfügbar.

Bei der Stummschaltung von Sicherheitsvorrichtungen handelt es sich um eine automatisch gesteuerte Unterbrechung des Stummschalteingangs des Pressensteuerungs-Funktionsblocks während eines Teils des Pressenzyklus, wenn keine unmittelbare Gefahr besteht oder wenn der Zugang zur Gefahr durch andere Mittel geschützt ist. Ordnen Sie die Stummschaltungssensoren der Pressensteuerung dem M-Sensor-Eingang des Pressensteuerungs-Eingangsfunktionsblocks zu, um zusammen mit dem Eingang für den sequenziellen Stopp (SQS) eine oder mehrere der folgenden Sicherheitseingangsvorrichtungen stummzuschalten:

- Schalter für Sicherheitsschleusen (Verriegelung)
- Optische Sensoren
- Schalmatten
- Schützende Anschläge

Nach US-amerikanischen und internationalen Normen muss der Benutzer das Sicherheitssystem so einrichten, installieren und betreiben, dass das Personal geschützt ist und die Möglichkeit, die Schutzvorrichtungen zu überwinden, möglichst gering ist.



**WARNUNG:**

- Vermeiden Sie gefährliche Installationen
- Zwei (1 SQS und 1 Press Control Mute-Sensor) oder vier (2 SQS und 2 Press Control Mute-Sensoren) unabhängige Positionsschalter müssen richtig eingestellt oder positioniert werden, so dass sie sich erst schließen, wenn die Gefahr nicht mehr besteht, und sich wieder öffnen, wenn der Zyklus beendet ist oder die Gefahr wieder besteht. Wenn die Schalter nicht richtig eingestellt oder positioniert sind, kann dies zu Verletzungen oder zum Tod führen.
- Der Benutzer ist dafür verantwortlich, dass alle lokalen, staatlichen und nationalen Gesetze, Regeln, Vorschriften und Bestimmungen in Bezug auf die Verwendung von Sicherheitsausrüstungen in einer bestimmten Anwendung eingehalten werden. Stellen Sie sicher, dass alle entsprechenden behördlichen Anforderungen erfüllt sind und dass alle in den entsprechenden Handbüchern enthaltenen Installations- und Wartungsanweisungen befolgt werden.

Der Press Control Mute Sensor (mit dem SQS-Gerät) muss mindestens die folgenden Anforderungen erfüllen:

1. Es müssen mindestens zwei unabhängige, fest verdrahtete Geräte vorhanden sein.
2. Die Geräte müssen über eine der folgenden Möglichkeiten verfügen: Schließerkontakte, PNP-Ausgänge (die beide die unter „5. Spezifikationen und Anforderungen“ auf Seite 18 aufgeführten Eingangsanforderungen erfüllen müssen) oder ein komplementäres Schaltverhalten. Mindestens einer dieser Kontakte muss schließen, wenn der Schalter betätigt wird, und muss öffnen (oder nicht leiten), wenn der Schalter nicht betätigt wird oder sich im ausgeschalteten Zustand befindet.
3. Die Aktivierung der Eingänge dieser Stummschaltfunktion muss von separaten Quellen ausgehen. Diese Quellen müssen getrennt montiert werden, um einen unsicheren Zustand zu vermeiden, der durch eine falsche Einstellung, eine falsche Ausrichtung oder einen einzelnen Gleichtaktfehler, wie z. B. eine physische Beschädigung der Montagefläche, entsteht. Nur eine dieser Quellen darf durch eine SPS oder ein ähnliches Gerät geleitet oder von ihr beeinflusst werden.
4. Die Vorrichtungen müssen so installiert werden, dass sie nicht leicht überwunden oder umgangen werden können.
5. Die Geräte sind so zu montieren, dass ihre Lage und Ausrichtung nicht leicht verändert werden kann.
6. Es darf nicht möglich sein, dass Umgebungsbedingungen, wie z. B. extreme Luftverschmutzung, den Stummschaltzustand auslösen.
7. Die Geräte dürfen keine Verzögerungs- oder sonstigen Zeitfunktionen verwenden, es sei denn, diese Funktionen werden so ausgeführt, dass kein Ausfall eines einzelnen Bauteils die Beseitigung der Gefahr verhindert, nachfolgende Maschinentzyklen verhindert werden, bis der Fehler behoben ist, und keine Gefahr durch Verlängerung der Stummschaltzeit entsteht.

7.5.17 Fußschalter

Diese Funktion ist bei SCx verfügbar.

Der Fußschaltereingang (FS1) kann auf verschiedene Weise mit den Press Control-Funktionsblöcken verwendet werden:

- Er kann an den GO-Knoten des Funktionsblocks Pressensteuerung als Zyklusauslöser angeschlossen werden, wenn der Block auf Einzelaktuatorsteuerung eingestellt ist.
- Er kann an den GO-Knoten des Funktionsblocks Press Control angeschlossen werden, wenn er für die Einstellung Manueller Aufwärtshub konfiguriert und der SQS-Eingang aktiviert ist. (Das Aktivieren des FS1-Eingangs treibt den RAM zum SQS-Punkt. Zu diesem Zeitpunkt wird der FS1 freigegeben. Da der Mutable Safety Stop-Eingang jetzt stummgeschaltet ist, kann der Bediener das Werkstück einstellen. Durch erneutes Einschalten von FS1 wird der RAM auf den BOS-Punkt und dann wieder auf den TOS-Punkt gefahren).
- Sie kann wie im folgenden Abschnitt beschrieben verwendet werden.

Der Fußschaltereingang kann zum Funktionsblock Pressensteuerungseingang hinzugefügt und konfiguriert werden, wenn der SQS-Eingang konfiguriert ist. Die Presse hält am SQS-Eingang an, so dass der Bediener seine Hände vom Zweihand-Steuerungseingang nehmen kann. Der Bediener kann sich vergewissern, dass das Werkstück richtig positioniert ist, und muss das Werkstück manchmal in Position halten. Der Bediener kann dann das an den Fußschaltereingang angeschlossene Eingabegerät betätigen, um die Presse wieder in Gang zu setzen und den Prozess zu beenden.

Der Eingang des Fußschalters kann auch auf den Knoten Press GO konfiguriert werden. In diesem Fall kann der Fußschalter mit und ohne SQS-Konfiguration verwendet werden. Dies ermöglicht mehr Flexibilität bei den Anwendungsfällen.

Ein physischer Ein/Aus-Eingang oder ein Fußschaltereingang kann an den Fußschaltereingang des Funktionsblocks Press Control Input angeschlossen werden. Bei dem Gerät kann es sich um einen Fußschalter, aber auch um andere Auslösegeräte handeln.

Der Zugang zur Gefahr muss auf andere Weise als durch den veränderlichen Sicherheitsstopp-Eingang verhindert werden (z. B. muss die innere Öffnung fingersicher sein, d. h. weniger als 6 mm/0,25 Zoll). Der Schutz kann auch durch Sicherheitsvorrichtungen gewährleistet werden, die an den nicht veränderbaren Safety Stop-Eingang angeschlossen sind.



7.6 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 Funktions-block, 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 „7.7 Virtuelle nicht sicherheitsrelevante Eingangsgeräte“ auf Seite 57.



WARNUNG: Nicht überwachte Resets

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

Ein/Aus-Schalter: Sendet einen Ein- bzw. Ausschaltbefehl an die Maschine. Wenn alle steuernden Sicherheitseingänge im Ein-Zustand sind, kann der Sicherheitsausgang mit dieser Funktion ein- bzw. ausgeschaltet werden. Dies ist ein einkanaliges Signal; bei 24 V DC ergibt sich ein Ein-Zustand und bei 0 V DC ergibt sich ein Aus-Zustand. Ein Eingang für das Ein-/Ausschalten kann ohne Zuordnung zu einem Sicherheitsausgang hinzugefügt werden, wodurch dieser Eingang nur einen Statusausgang steuern kann. Ein Ein/Aus-Schalter kann auch mit einem virtuellen Eingang erstellt werden. Siehe „7.7 Virtuelle nicht sicherheitsrelevante Eingangsgeräte“ auf Seite 57.

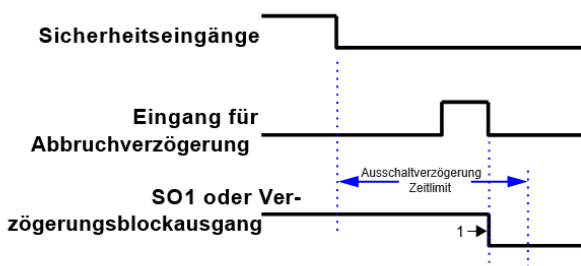
Muting-Aktivierungsschalter: signalisiert der Sicherheitsauswertung, ob es den Muting-Sensoren erlaubt ist, eine Muting-Funktion auszuführen. Wenn die Muting-Aktivierungsfunktion konfiguriert ist, werden die Muting-Sensoren nicht zum Muting aktiviert, solange das Muting-Aktivierungssignal nicht im Ein-Zustand 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 „7.7 Virtuelle nicht sicherheitsrelevante Eingangsgeräte“ auf Seite 57.

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 „7.7 Virtuelle nicht sicherheitsrelevante Eingangsgeräte“ auf Seite 57.

Zeitgeber für den Abbruch von Aus-Verzögerungen



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

Abbildung 22: Sicherheitseingang verbleibt im Stopp-Modus

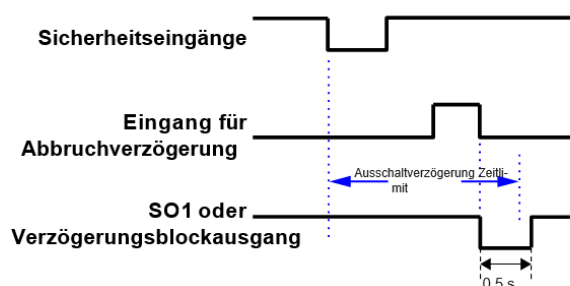


Abbildung 23: Ausgang schaltet sich aus



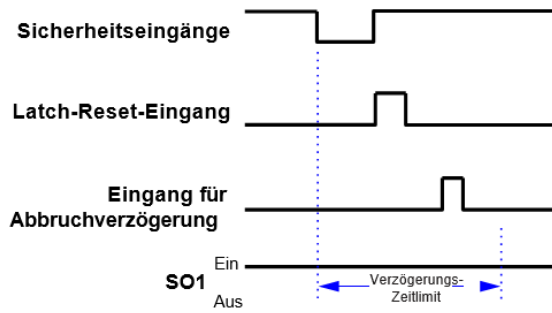


Abbildung 24: Ausgang bleibt für Sicherheitseingänge mit Latch-Reset eingeschaltet

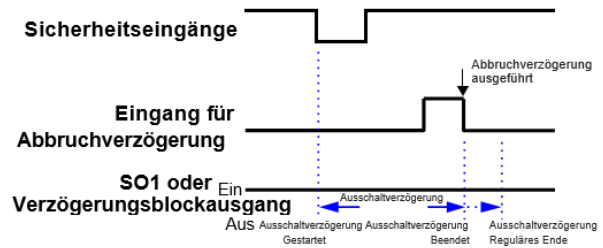


Abbildung 25: Ausgang bleibt für Sicherheitseingänge ohne Latch-Reset eingeschaltet

7.6.1 Manueller Reset-Eingang

Der manuelle Reset-Eingang kann so konfiguriert werden, dass eine beliebige Kombination der folgenden Funktionen ausgeführt wird (siehe „8.2 Hinzufügen von Eingängen und Statusausgängen“ auf Seite 77):

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 eingeschaltet 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 (Hintertrittungsgefahr) wird nicht verhindert.





WARNUNG: Reset-Schalterpositionen

Alle Reset-Schalter dürfen nur von außen zugänglich sein und müssen die uneingeschränkte Sicht auf den Gefahrenbereich ermöglichen. Reset-Schalter müssen sich zudem vom geschützten Bereich aus außer Reichweite befinden und vor unbefugter oder unbeabsichtigter Betätigung geschützt sein (z. B. durch den Einsatz von Ringen oder Schutzeinrichtungen). Können Bereiche von den Reset-Schaltern aus nicht eingesehen werden, so müssen zusätzliche 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 „10. Funktionsblöcke“ auf Seite 126).

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 Hintertretungsgefahren in Bereichssicherungen gemindert oder beseitigt werden können (siehe „7.4.2 Eigenschaften von Sicherheitseingängen“ auf Seite 34).

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:

Überwacher 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.



7.7 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.

7.7.1 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

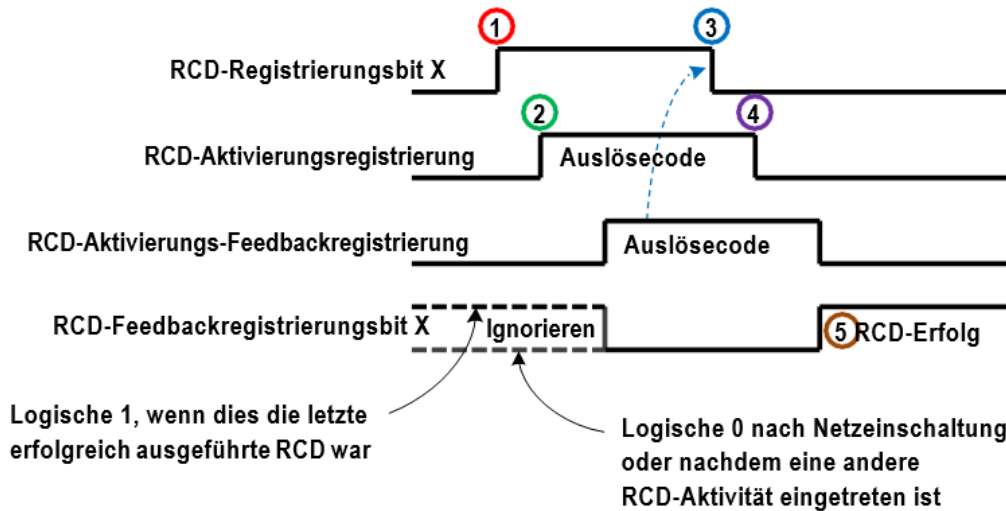


Abbildung 26: Virtuelle Resetsequenz oder Abbruchsequenz einer Zeitverzögerung (RCD) – Feedbackmethode

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

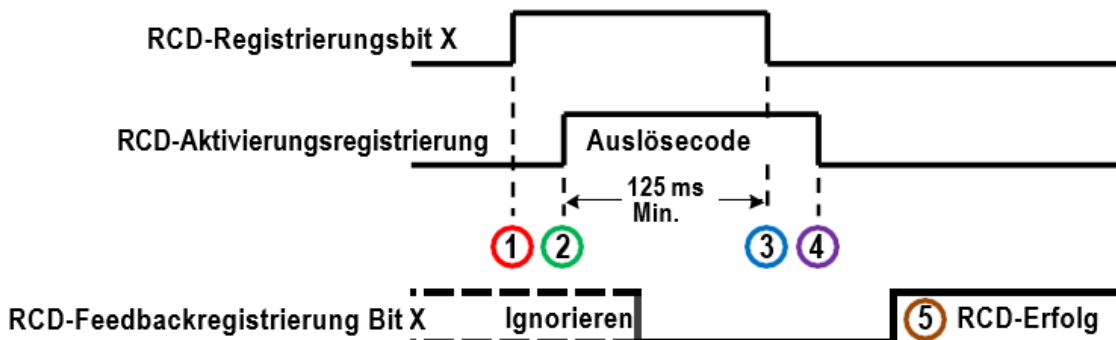


Abbildung 27: Virtuelle Resetsequenz oder Abbruchsequenz einer Zeitverzögerung (RCD) - zeitgeschaltete Methode

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 „7.6 Nicht sicherheitsrelevante Eingangsgeräte“ auf Seite 54.





WARNUNG: Virtueller manueller Reset

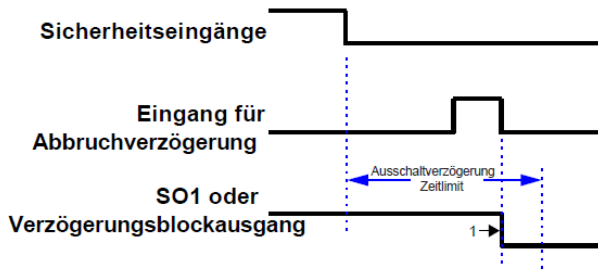
Ein virtueller manueller Reset, der zur Ausführung einer manuellen Netzeinschaltfunktion zusammen mit Geräten an diversen Standorten in demselben Netzwerk konfiguriert ist, sollte vermieden werden, außer wenn die Sicherheit aller Gefahrenbereiche bestätigt wurde.

Virtuelle Einrichtungen für den Abbruch von Ausschaltverzögerungen: Bieten die Möglichkeit, eine konfigurierte Ausschaltverzögerungszeit abzurechnen. 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 „7.6 Nicht sicherheitsrelevante Eingangsgeräte“ auf Seite 54.

Zeitablauffunktion für den virtuellen Abbruch einer Ausschaltverzögerung



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

Abbildung 28: Sicherheitseingang verbleibt im Stopp-Modus

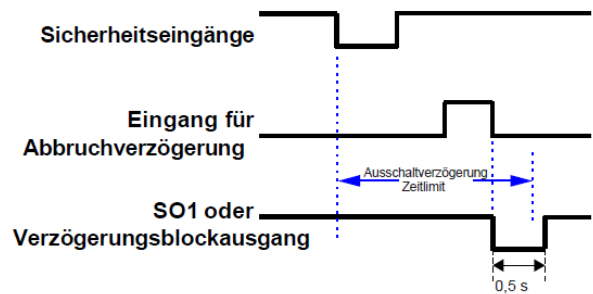


Abbildung 29: Ausgang schaltet sich aus

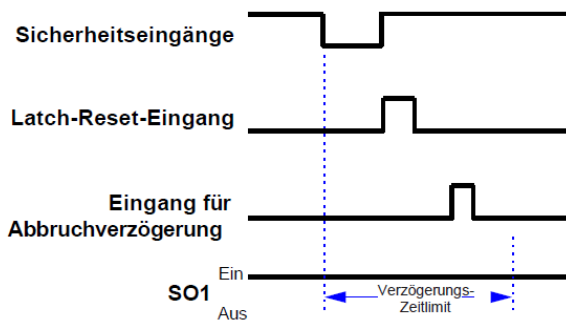


Abbildung 30: Ausgang bleibt für Sicherheitseingänge mit Latch-Reset eingeschaltet

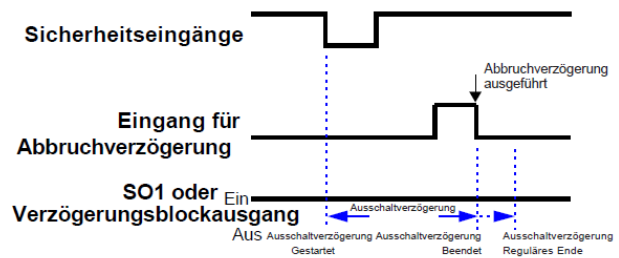


Abbildung 31: Ausgang bleibt für Sicherheitseingänge ohne Latch-Reset eingeschaltet



7.7.2 Virtuelle Ein-/Ausschaltung und Muting-Aktivierung

Virtuelle Ein-/Ausschaltung

Sendet einen Ein- bzw. 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 „7.6 Nicht sicherheitsrelevante Eingangsgeräte“ auf Seite 54.

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 Zu-stand (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 „7.6 Nicht sicherheitsrelevante Eingangsgeräte“ auf Seite 54.

7.8 Sicherheitsausgänge

SCx

Das Basismodul verfügt über zwei Paare von Halbleiter-Sicherheitsausgängen (Klemmen SO1a und b sowie SO2a und b). Diese Ausgänge liefern jeweils bis zu 500 mA bei 24 V DC. Jeder redundante Solid-State-Sicherheitsausgang kann so konfiguriert werden, dass er einzeln oder paarweise funktioniert, z. B. SO1a unabhängig von SO1b oder SO1 als zweikanaliger Ausgang.

Erweiterbare Modelle der Basissteuerung können durch den Einbau von E/A-Modulen um zusätzliche Sicherheitsausgänge ergänzt werden. Bei diesen zusätzlichen Sicherheitsausgängen kann es sich um galvanisch getrennte Relaisausgänge handeln, die zur Steuerung/Schaltung einer breiten Palette von Leistungsmerkmalen verwendet werden können (siehe „5.1 SCx Spezifikationen“ auf Seite 18).

SCR P

Das SCR P hat zwei galvanisch getrennte redundante Relaisausgänge. Jeder Relaisausgang verfügt über drei unabhängige Kontaktsätze. Siehe „5.2 Spezifikationen für das SCR P“ auf Seite 23 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 Abschaltelementen 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 „8.2 Hinzufügen von Eingängen und Statusausgängen“ auf Seite 77):

EDM (externe Geräteüberwachung)

Ermöglicht der Sicherheitsauswertung die Überwachung der angeschlossenen Geräte (Sicherheitssensoren und Abschaltelemente) 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 „7.8.3 EDM- und Abschaltgeräteanschluss“ auf Seite 67).

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 „7.5.12 AVM-Funktion (Adjustable Valve Monitoring, einstellbare Ventilüberwachung)“ auf Seite 48).

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 „7.6.1 Manueller Reset-Eingang“ auf Seite 55 erhalten Sie weitere Informationen.



RE (Reset aktivieren)

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

FR (Systemfehler-Reset)

Liefert eine manuelle Reset-Funktion, wenn Eingangsfehler auftreten. Der FR-Knoten muss mit dem manuellen Reset-Schalter bzw. -Signal verbunden werden. Diese Funktion dient dazu, den 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 „7.6.1 Manueller Reset-Eingang“ auf Seite 55 erhalten Sie weitere Informationen.

Anlaufmodus

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

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

Unter „7.6.1 Manueller Reset-Eingang“ auf Seite 55 erhalten Sie weitere Informationen.

Teilen (Sicherheitsausgänge) - nur SCx

Diese Option ist nur für Solid-State-Sicherheitsausgänge verfügbar. Jeder redundante Halbleitersicherheitsausgang kann so konfiguriert werden, dass er einzeln oder paarweise funktioniert (Standard).

Die Aufteilung eines Halbleiter-Sicherheitsausgangs erzeugt zwei unabhängige einkanalige Ausgänge (die Steuerung von SO1a ist unabhängig von SO1b). Um einen geteilten Sicherheitsausgang zu kombinieren, öffnen Sie das Fenster Mx:SOxA Eigenschaften und klicken Sie auf Verbinden.

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 55), wobei der Ausgang erst nach Ablauf des Zeitlimits ein- bzw. ausschaltet. Ein Ausgang kann nicht gleichzeitig eine Ein- und eine Ausschaltverzögerung haben. Das Zeitlimit für die Ein- und Ausschaltverzögerung kann in Stufen à 1 Millisekunde von 100 Millisekunden bis 5 Minuten eingestellt werden.

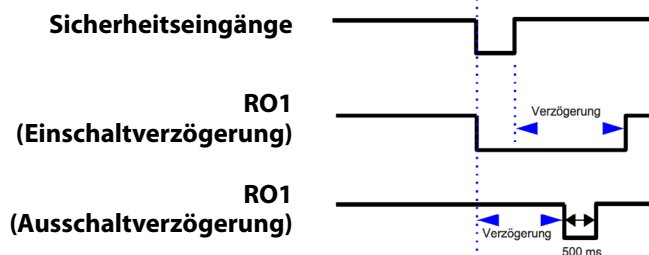


Abbildung 32: Zeitablauf-Diagramm: Ein- und Ausschaltverzögerung für Sicherheitsausgänge



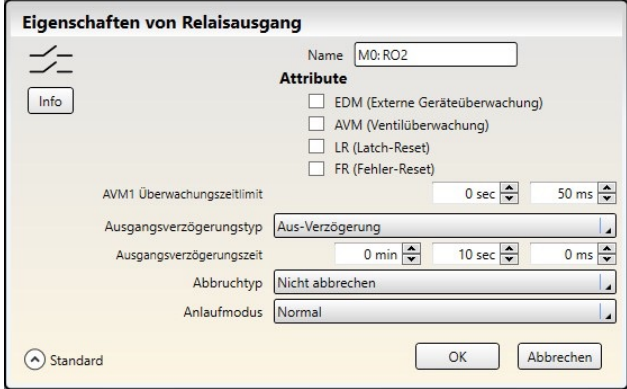
WARNUNG:

- **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 58 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.



Eigenschaften von Relaisausgang

Name: M0:RO2

Attribute

EDM (Externe Geräteüberwachung)

AVM (Ventilüberwachung)

LR (Latch-Reset)

FR (Fehler-Reset)

AVM1 Überwachungszeitlimit: 0 sec 50 ms

Ausgangsverzögerungstyp: Aus-Verzögerung

Ausgangsverzögerungszeit: 0 min 10 sec 0 ms

Abbruchtyp: Nicht abrechen

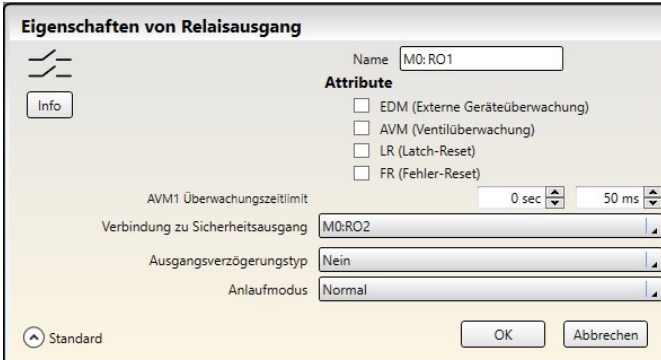
Anlaufmodus: Normal

Standard OK Abbrechen

Abbildung 33: Auswahlbeispiel für Sicherheitsausgangsverzögerung: Ausschaltverzögerung

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 58 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.
3. Legen Sie die gewünschte Ausschaltverzögerungszeit fest.
4. Klicken Sie auf **OK**.
5. Öffnen Sie das Fenster **Eigenschaften** für den Sicherheitsausgang, der mit dem Sicherheitsausgang mit Ausschaltverzögerung verkettet werden soll.
6. Wählen Sie aus der Dropdown-Liste Verbindung zu Sicherheitsausgang den Sicherheitsausgang mit Ausschaltverzögerung aus, mit dem Sie diesen Sicherheitsausgang verketteten möchten.



Eigenschaften von Relaisausgang

Name: M0:RO1

Attribute

EDM (Externe Geräteüberwachung)

AVM (Ventilüberwachung)

LR (Latch-Reset)

FR (Fehler-Reset)

AVM1 Überwachungszeitlimit: 0 sec 50 ms

Verbindung zu Sicherheitsausgang: M0:RO2

Ausgangsverzögerungstyp: Nein

Anlaufmodus: Normal

Standard OK Abbrechen

Abbildung 34: Auswahlbeispiel für Verkettung mit Sicherheitsausgang



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



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

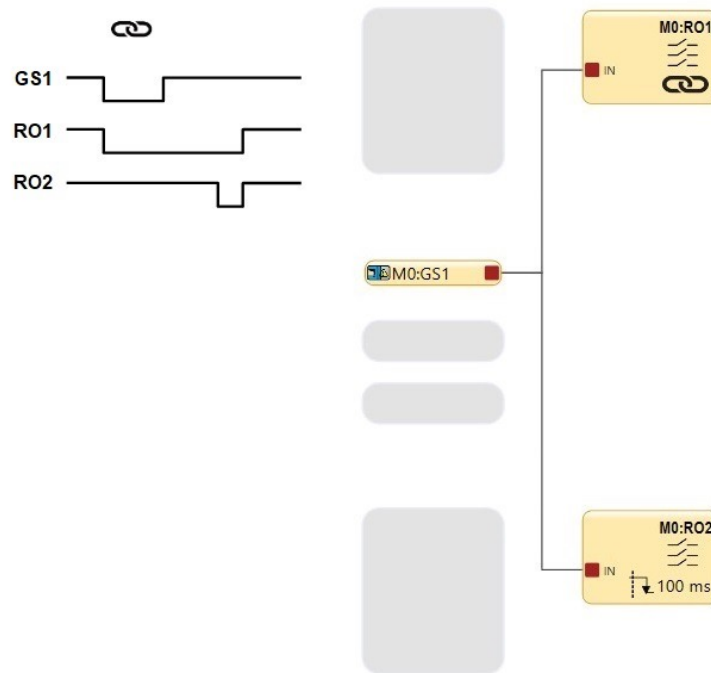


Abbildung 35: Zeitablauf-Diagramm: Verkettete Sicherheitsausgänge



7.8.1 Solid-State-Sicherheitsausgänge

Diese Funktion ist bei SCx verfügbar.

Die Halbleiter-Sicherheitsausgänge, z. B. SO1a und b sowie SO2a und b, werden aktiv überwacht, um Kurzschlüsse zur Versorgungsspannung, zueinander und zu anderen Spannungsquellen zu erkennen, und sind für Sicherheitsanwendungen der Kategorie 4 ausgelegt. Wird an einem Kanal eines Sicherheitsausgangspaars ein Fehler erkannt, versuchen beide Ausgänge, sich auszuschalten und gehen in einen Sperrzustand über. Der Ausgang ohne Fehler ist in der Lage, die gefährliche Bewegung abzuschalten.

Auch ein Sicherheitsausgang, der einzeln verwendet wird (Split), wird aktiv überwacht, um Kurzschlüsse zu anderen Spannungsquellen zu erkennen, kann aber keine Aktionen ausführen. Gehen Sie bei der Verdrahtung der Klemmen und der Verlegung der Drähte äußerst sorgfältig vor, um die Möglichkeit von Kurzschlüssen zu anderen Spannungsquellen, einschließlich anderer Sicherheitsausgänge, zu vermeiden. Jeder geteilte Sicherheitsausgang ist aufgrund einer internen Reihenschaltung zweier Schaltgeräte für Anwendungen der Kategorie 3 ausreichend, ein externer Kurzschluss muss jedoch verhindert werden.



Wichtig: Wenn Solid-State-Sicherheitsausgangsmodule (SCx-O-2T oder SCx-O-4T) verwendet werden, muss die Stromversorgung dieser Module entweder vor oder innerhalb von 5 Sekunden nach dem Anlegen der Stromversorgung an die Basissteuerung erfolgen, wenn separate Stromversorgungen verwendet werden.



Hinweis: Jedes Solid-State-Sicherheitsausgangsmodul (SCx-O-2T oder SCx-O-4T) hat zwei 24-V-Anschlüsse und zwei 0-V-Anschlüsse. Für die Stromversorgung des jeweiligen Moduls wird nur eine von beiden benötigt. Der zweite Satz kann zur Überbrückung der Stromversorgung des nächsten Moduls verwendet werden.



WARNUNG:

- **Einkanalige (geteilte) Ausgänge zur Verwendung in sicherheitskritischen Anwendungen**
- Werden bei der Verwendung von einkanaligen Ausgängen in sicherheitskritischen Anwendungen keine angemessenen Fehlerausschlussverfahren eingesetzt, kann dies zu einem Verlust der Sicherheitssteuerung und zu schweren Verletzungen oder zum Tod führen.
- Wenn ein einkanaliger Ausgang in einer sicherheitskritischen Anwendung verwendet wird, müssen die Prinzipien des Fehlerausschlusses berücksichtigt werden, um einen sicheren Betrieb der Kategorie 3 zu gewährleisten. Ein Beispiel für eine ordnungsgemäße Fehlerausschlussmethode ist die Verlegung und Verwaltung von einkanaligen Ausgangsdrähten, so dass Kurzschlüsse zu anderen Ausgängen oder anderen Spannungsquellen nicht möglich sind.

Wann immer es möglich ist, wird die Integration einer externen Geräteüberwachung (EDM) und/oder einer einstellbaren Ventilüberwachung (AVM) dringend empfohlen, um kontrollierte Geräte (Sicherheitssensoren und Abschaltetelemente) auf unsichere Ausfälle zu überwachen. Siehe Externe Geräteüberwachung (EDM) auf Seite 70 für weitere Informationen.

Beschaltung der Ausgänge

Die Sicherheitsausgänge müssen so an die Maschinensteuerung angeschlossen werden, dass das sicherheitsbezogene Steuersystem der Maschine den Stromkreis oder die Stromzufuhr zu dem/den primären Steuerelement(en) der Maschine (Abschaltetelemente) unterbricht, was zu einem nicht gefährlichen Zustand führt.

Bei Verwendung von Endschaltern (Sicherheitssensoren) wird dies in der Regel erreicht, wenn die Sicherheitsausgänge in den Aus-

Zustand gehen. Lesen Sie „5.1 SCx Spezifikationen“ auf Seite 18, bevor Sie Verbindungen herstellen und die Sicherheitssteuerung mit der Maschine verbinden.

Der Grad der Integrität des Sicherheitskreises muss durch eine Risikobewertung bestimmt werden; dieser Grad ist abhängig von der Konfiguration, der ordnungsgemäßen Installation der externen Schaltung und dem Typ und der Installation der gesteuerten Geräte (Sicherheitssensoren und Abschaltetelemente). Die Halbleiter-Sicherheitsausgänge eignen sich für Anwendungen

der Kategorie 4 PL e / SIL 3, wenn sie paarweise gesteuert werden (nicht geteilt), und für Anwendungen bis zu Kategorie 3 PL d / SIL 2, wenn sie unabhängig arbeiten (geteilt), wenn ein geeigneter Fehlerausschluss verwendet wurde. Siehe Abbildung 41 auf Seite 72 für Anschlussbeispiele.



**WARNUNG:**

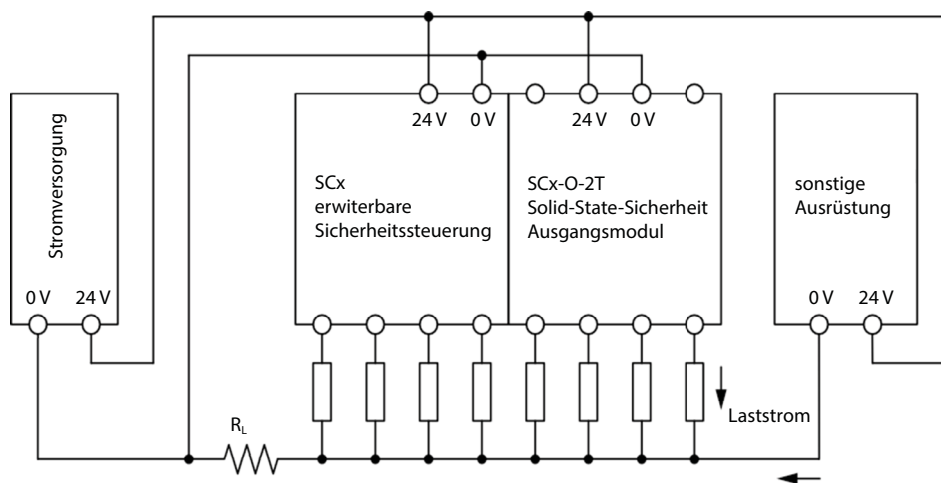
- **Sicherheitsausgang Leitungswiderstand**
- Ein Widerstand von mehr als 10 Ohm könnte einen Kurzschluss zwischen den zweikanaligen Sicherheitsausgängen verdecken und einen unsicheren Zustand verursachen, der zu schweren Verletzungen oder zum Tod führen kann.
- Der Widerstand der Leitungen darf 10 Ohm nicht überschreiten.

Gemeinsame Installation der Ausgänge

Berücksichtigen Sie den Leitungswiderstand der gemeinsamen 0-V-Leitung und die Ströme, die in dieser Leitung fließen, um unerwünschte Verriegelungen zu vermeiden. Beachten Sie die Position des Widerstandssymbols im folgenden Diagramm, das den Widerstand der 0-V-Leitung (R_L) darstellt.

Zu den Methoden zur Vermeidung dieser Situation gehören:

- Verwendung dickerer oder kürzerer Leitungen, um den Widerstand (R_L) des gemeinsamen 0-V-Drahtes zu verringern
- Trennen Sie die gemeinsame 0-V-Leitung von den an die Sicherheitssteuerung angeschlossenen Lasten und die gemeinsame 0-V-Leitung von anderen Geräten, die über die gemeinsame 24-V-Versorgung versorgt werden.



R_L = Gemeinsamer Zuleitung, der von mehreren Lasten oder Systemen genutzt wird.

Die gemeinsame Nutzung von Kabeln mit geringem Querschnitt kann zu Fehlern an Halbleiterausgängen führen.

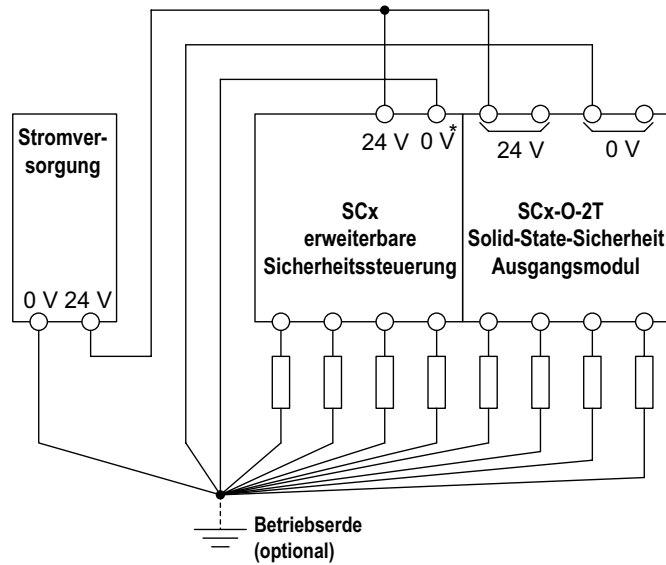
Abbildung 36: Gemeinsame Installation der Ausgänge



Hinweis: Wenn der Sicherheitsausgang ausgeschaltet wird, muss die Spannung an dieser Ausgangsklemme unter 1,7 V in Bezug auf die 0-V-Klemme an diesem Modul fallen. Wenn die Spannung höher als 1,7 V ist, entscheidet die Sicherheitssteuerung, dass der Ausgang noch eingeschaltet ist, was zu einer Verriegelung führt. Erwägen Sie die Verwendung von Leitern mit größerem Querschnitt, kürzeren Leitern oder die Verwendung eines Ein-Punkt-Erdungsschemas, ähnlich wie in den folgenden Diagrammen dargestellt.



Bevorzugter 0-V-Leitungsplan bei Verwendung eines einzigen Netzteils



* Die Spannung für alle Sicherheitseingangsgeräte (einschließlich aller Eingangserweiterungsmodule) sollte in Bezug auf die 0-V-Klemme der Basissteuerung gemessen werden.

Bevorzugter 0-V-Leitungsplan bei Verwendung getrennter Stromversorgungen

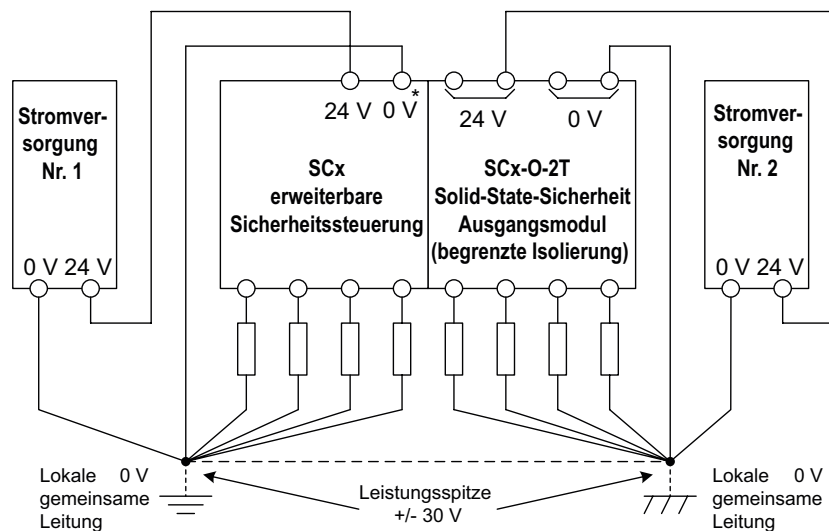


Abbildung 37: Schaltplan - Empfohlene Erdung

7.8.2 Sicherheits-Relaisausgänge

Das SCR P verfügt über galvanisch getrennte, redundante Relaisausgänge, mit denen ein breites Spektrum an elektrischen Geräten gesteuert/geschaltet werden kann („5.2 Spezifikationen für das SCR P“ auf Seite 23). 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 Fehlerrückmeldung 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 67 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 „5.2 Spezifikationen für das SCR P“ auf Seite 23, 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 (Sicherheitssensoren und Abschalteteile) ab. Die Sicherheits-Relaisausgänge sind für Kategorie 4 PL e/SIL 3 geeignet. Unter Abbildung 25 auf Seite 59 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 Bedienungsperson 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 Abzweigungen (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).

7.8.3 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 Abschalteteile.

Ein einzelner EDM-Eingang kann einem oder mehreren Sicherheitsausgängen zugeordnet werden. Öffnen Sie hier-zu 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 59.
- **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 62.
- **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 Abschaltelemente überwacht werden kann (siehe Abbildung). Dadurch wird der ordnungsgemäße Betrieb der Abschaltelemente überwacht. **Verwenden Sie die Überwachungskontakte der Abschaltelemente zur Erhaltung der Sicherheitsstufe.**

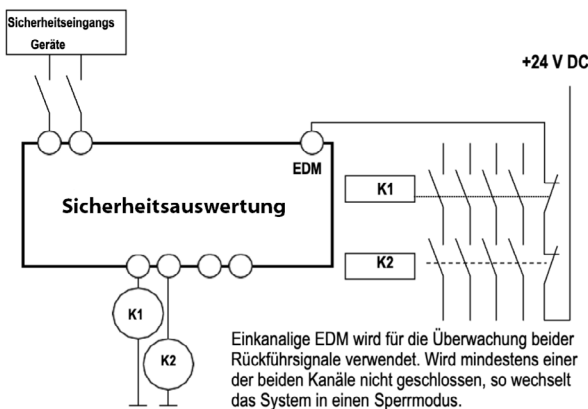


Abbildung 38: Anschluss der externen Zweikanal-Geräteüberwachung (Einkanal-EMD)

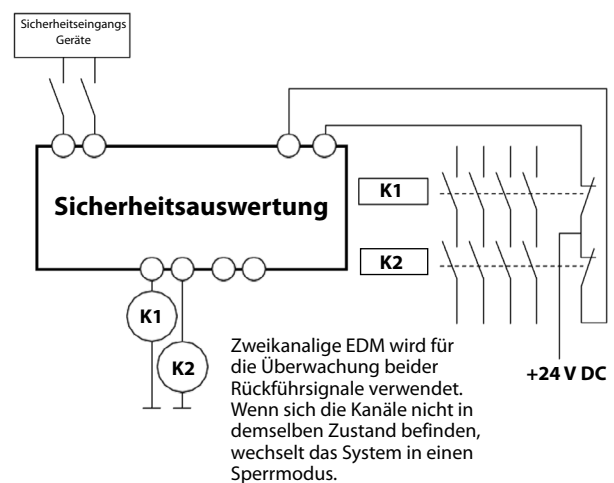
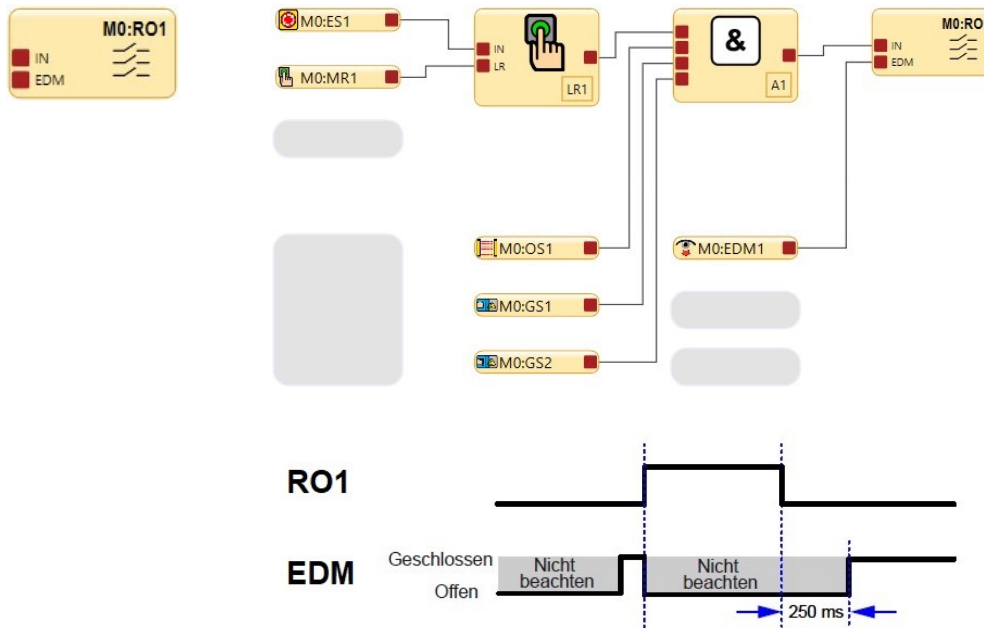


Abbildung 39: Anschluss der externen Zweikanal-Geräteüberwachung (Zweikanal-EDM)





Die externe Geräteüberwachung (EDM) ist eine Methode zur Überprüfung des Betriebs von zweikanaligen Abschaltgeräten. Die zwangsgeführten Öffner-Überwachungskontakte der Sicherheitssensoren und Abschalt Elemente dienen als Eingänge für die Erkennung eines verschweißten Ein-Zustands als Fehlerzustand und verhindern ein Einschalten der Ausgänge des Sicherheitsauswertung.

Abbildung 40: Zeitdiagramm: Status der einkanaligen 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.

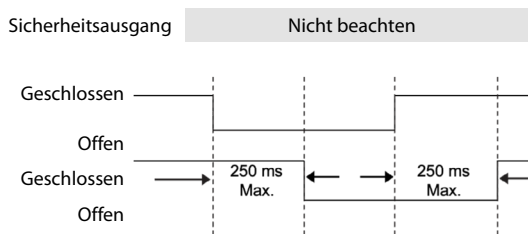


Abbildung 41: Zeitdiagramm: Zweikanalige EDM, zeitliche Abstimmung zwischen Kanälen

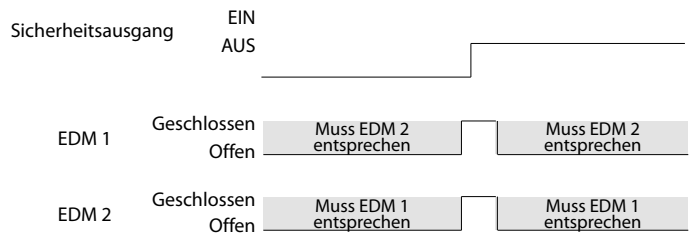


Abbildung 42: Zeitdiagramm: Status der zweikanaligen externen Geräteüberwachung in Bezug auf den Sicherheitsausgang



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 Schließerkontakte 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 Schließerkontakten, 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. 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: Anschluss der Sicherheitsausgänge

- **Das Gerät korrekt verdrahten**
- Wird der Sicherheitsauswertung 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.

Allgemeiner SCx-Anschluss: Sicherheitsausgang mit EDM

Die Solid-State-Sicherheitsausgänge SO2, SO3 und SO4 können auf ähnliche Weise verdrahtet werden.

Wenn ein Solid-State-Sicherheitsausgang in zwei Einzelausgänge aufgeteilt wurde, benötigt jeder Ausgang einen eigenen EDM- oder AVM-Eingang zur Überwachung.

Die DC-Masse (0 Vdc) muss zwischen der 0Vdc-Klemme des Moduls und der Masse der Last (z. B. FSD) liegen.

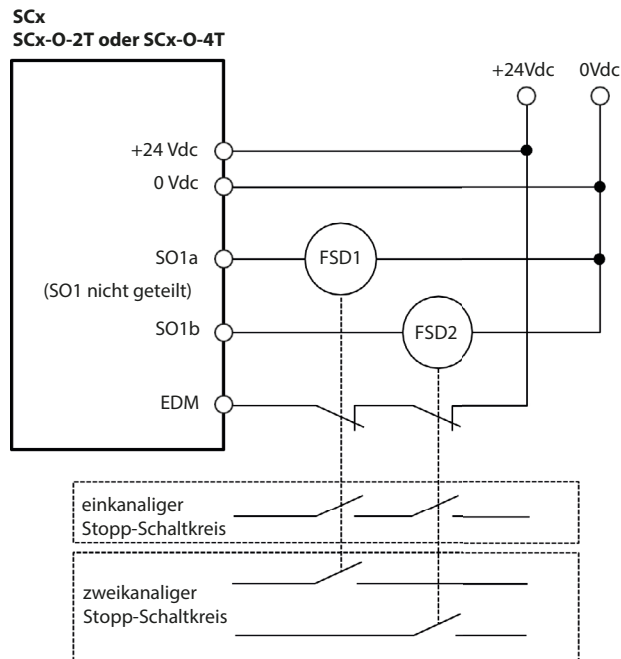


Abbildung 43: Generische SCx-Verbindung: Solid-State-Sicherheitsausgang mit EDM

Die Sicherheitsrelaisausgänge 43/44, 53/54 und 61/62 können in ähnlicher Weise verdrahtet werden, erfordern jedoch einen separaten EDM- oder AVMEingang zur Überwachung.

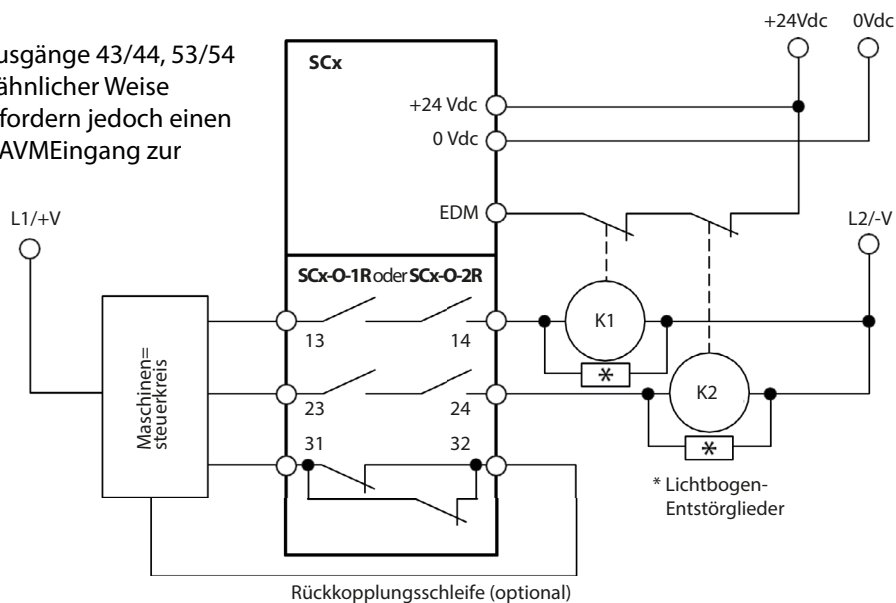


Abbildung 44: Allgemeiner SCx-Anschluss: Sicherheitsrelaisausgang (zweikanalig) mit EDM



**WARNUNG:**

- **Ordnungsgemäße Installation von Lichtbogen- oder Transientenunterdrückern**
- Die Nichtbeachtung dieser Anweisungen kann zu schweren Verletzungen oder zum Tod führen.
- Installieren Sie etwaige Schutzbeschaltungen wie gezeigt über den Spulen der primären Steuerelemente der Maschine. Installieren Sie keine Schutzbeschaltungen direkt über den Ausgangskontakten des Sicherheits- oder Schnittstellenmoduls. In einer solchen Konfiguration ist es möglich, dass Schutzbeschaltungen als Kurzschluss ausfallen.

Typischer Anschluss des SCR P: Sicherheitsausgang mit EDM

Die Sicherheitsrelaisausgänge 43/44, 53/54 und 63/64 können in ähnlicher Weise verdrahtet werden, erfordern jedoch einen separaten EDM- oder AVM-Eingang zur Überwachung.

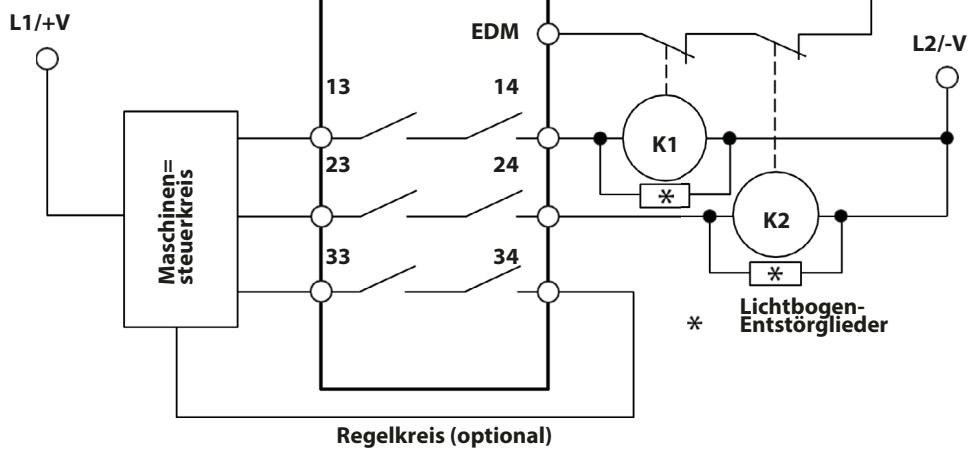


Abbildung 45: Typischer Anschluss des SCR P: Sicherheits-Relaisausgang (zweikanalig) mit EDM



7.9 Statusausgänge

7.9.1 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 3: Signallogik für Statusausgänge

Funktion	Signallogik			
	Aktiv = PNP ein		Aktiv = PNP aus	
	Statusausgangs-Status		Statusausgangs-Status	
	+24 V DC	+24 V DC	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	+24 V DC	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



7.9.2 Statusausgangsfunktion

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

SCx: Bis zu 8 konfigurierbare Eingänge können als Statusausgänge 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.

Einganggruppenanzeige

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.

Funktionsblock Presse-Tracking

Zeigt den Status einer Reihe von Pressenfunktionsereignissen an; siehe „7.9.3 Pressesteuerung Statusausgabefunktionalität“ auf Seite 75 für weitere Informationen.

Warten auf manuellen Reset

Gibt an, dass ein bestimmter konfigurierter Reset erforderlich ist.



Hinweis: Wenn der manuelle Rücksetzeingang mit einem Reset-OR-Block verbunden ist, kann dieser Statusausgang nicht verwendet werden.

Systemsperrung

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



7.9.3 Pressesteuerung Statusausgabefunktionalität

Der Funktionsblock Pressesteuerung hat mehrere Ein- und Ausgänge. Daraus ergibt sich eine Statusausgangsfunktion, die nicht nur ein einfaches Ein/Aus für ein einzelnes Element ist. Der Statusausgang des Pressesteuerung Blocks hat sieben verschiedene Ereignisse, die über den Statusausgang signalisiert werden können. Der Statusausgang des Pressesteuerung Blocks kann so konfiguriert werden, dass er ein, zwei oder drei Signale liefert. Jedes Signal vom Statusausgang des Pressesteuerung Blocks kann wie folgt sein:

- Massiv ein
- 2 Impulse pro Sekunde

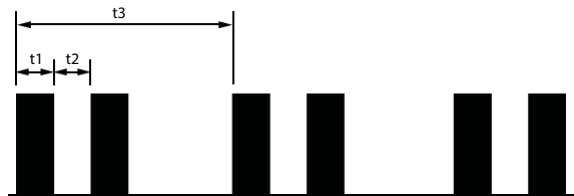


Abbildung 46: 2 Pulse pro Sekunde

$t1 = 100 \text{ ms}$, $t2 = 100 \text{ ms}$ und $t3 = 1 \text{ s}$

- 3 Impulse pro Sekunde

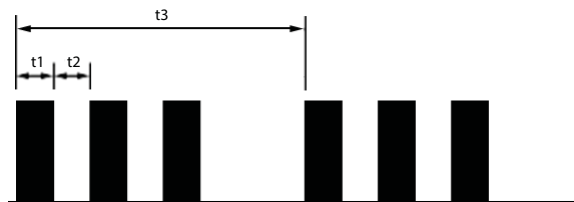


Abbildung 47: 3 Pulse pro Sekunde

$t1 = 100 \text{ ms}$, $t2 = 100 \text{ ms}$ und $t3 = 1 \text{ s}$

Der Statusausgang des Pressesteuerung Blocks ist nur als physikalischer Statusausgang verfügbar. Jeder physikalische Statusausgang kann zur Signalisierung von drei verschiedenen Ereignissen verwendet werden. Die folgende Abbildung zeigt die Standardeinstellungen für den Statusausgang des Funktionsblocks Pressesteuerung:

Funktionsblock Presse-Tracking Eigenschaften

Name: M0:STAT2

Info

Anschluss Statusausgang 3

M0:SCx-B-26-2T-5

Funktionsblock Presse: PC1

Anschlüsse auswählen: IO4, IO5, IO6

Name des Ereignisses	Wert für Farbe1	Wert für Farbe2	Wert für Farbe3
Reset erwartet	Zwei Impulse	Nicht verwen:	Nicht verwen:
Betriebsbereit/Betrieb	Ein	Nicht verwen:	Nicht verwen:
SQS-Stopp	Nicht verwen:	Zwei Impulse	Nicht verwen:
PIP zurück prüfen	Drei Impulse	Nicht verwen:	Nicht verwen:
Sicherheitsstopp	Nicht verwen:	Nicht verwen:	Zwei Impulse
Betriebsfehler	Nicht verwen:	Drei Impulse	Nicht verwen:
Systemfehler	Nicht verwen:	Nicht verwen:	Drei Impulse

OK Abbrechen

Abbildung 48: Track Press Funktionsblock Eigenschaften



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

Die Funktionen der einzelnen Ereignisse sind wie folgt:

- **Warten auf Reset - Schaltet sich** ein, wenn ein Reset-Eingang benötigt wird, nachdem die nicht veränderbaren und veränderbaren (falls konfiguriert) Sicherheitsstopp-Eingänge in den EIN-Zustand zurückkehren.
- **Ready to Run/Run** - Leuchtet immer dann, wenn die Presse betriebsbereit ist (veränderbare und nicht veränderbare Sicherheitsstopp-Eingänge sind eingeschaltet und werden zurückgesetzt) oder die Presse im Auf- oder Abwärtshub läuft.
- **SQS Stop - Schaltet sich** ein, wenn der Pressenstößel den Punkt „Sequence Stop“ erreicht
- **PIP-Rückprüfungsalarm - Schaltet sich** ein, wenn die Presse betriebsbereit ist und versucht wird, einen Pressenzyklus zu starten, und der PIP-Eingang (Part in Place), falls konfiguriert, ausgeschaltet ist oder sich nicht ausgeschaltet und dann wieder eingeschaltet hat (Teil nicht entfernt und ersetzt).
- **Sicherheitsstopp - Schaltet sich** ein, wenn entweder der veränderliche oder der nicht veränderliche Sicherheitsstopp-Eingang ausgeschaltet wird, der GO-Eingangsknoten auf Low geht (wenn für die manuelle Aufwärtshubeinstellung konfiguriert), bevor SQS, BOS oder TOS erreicht wird (abhängig von den Einstellungen und dem Teil des Prozesses).
- **Betriebsstörung - Schaltet sich** ein, wenn sich gegenseitig ausschließende Betriebseingänge eingeschaltet sind (z. B. TOS und BOS, TOS und SQS, TOS und PCMS, SQS und BOS usw.; wenn mehr als 3 Sekunden zwischen den Signalen SQS und PCMS vergehen, schalten sich beide ein, sofern konfiguriert).
- **Systemfehler - Schaltet sich** ein, wenn ein Systemfehler vorliegt.

7.10 Virtuelle Statusausgänge

Bis zu 256 virtuelle Statusausgänge können bei SCR P und SCx Sicherheitsauswertungen hinzugefügt werden. Diese Ausgänge können über das Netzwerk dieselben Informationen übermitteln wie die Statusausgänge. Siehe „7.9.2 Statusausgangsfunktion“ auf Seite 74 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 „9.10 Registerkarte Industrial-Ethernet“ auf Seite 108 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 und SCx 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 „12.4.12 Flags“ auf Seite 172.






8. Erste Schritte

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

8.1 Erstellen einer Konfiguration

Die folgenden Schritte sind erforderlich, um die Konfiguration abzuschließen und zu bestätigen (in 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 „6.1 Installation der Software“ auf Seite 28
3. Machen Sie sich mit den Optionen in der Software vertraut. Siehe „9.2 Software-Übersicht“ auf Seite 96.
4. Starten Sie ein neues Projekt mit einem Klick auf **Neues Projekt/ Zuletzt verwendete Dateien**.
5. Definieren Sie die **Projekteinstellungen**. Siehe „9.4  Projekteinstellungen“ auf Seite 98.
6. Fügen Sie Sicherheitseingänge, nicht sicherheitsrelevante Eingänge und Statusausgänge hinzu. Siehe „8.2 Hinzufügen von Eingängen und Statusausgängen“ auf Seite 77.
7. Entwerfen Sie die Steuerungslogik. Siehe „8.3 Entwerfen der Steuerungslogik“ auf Seite 82.
8. Stellen Sie optionale Ein- oder Ausschaltverzögerungszeiten für Sicherheitsausgänge ein.
9. Sofern verwendet, konfigurieren Sie die Netzwerkeinstellungen. Siehe „9.10.1.1 Netzwerkeinstellungen: Modbus/TCP, Ethernet/IP, PCCC “ auf Seite 109 oder „9.10.1.2 Netzwerkeinstellungen: PROFINET “ auf Seite 110.
10. Speichern und bestätigen Sie die Konfiguration. Siehe „8.4 Speichern und Bestätigen einer Konfiguration“ auf Seite 82.

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 „9.11 Registerkarte Konfigurationsübersicht“ auf Seite 113.
3. Drucken Sie die Konfigurationsansichten, einschließlich der **Konfigurationsübersicht** und der **Netzwerkeinstellungen**. Siehe „9.12 Druckoptionen“ auf Seite 114
4. Konfigurationstests mit dem Simulationsmodus. Siehe „9.17 Simulationsmodus“ auf Seite 121.

8.2 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.

8.2.1 Hinzufügen von Sicherheits- und nicht sicherheitsrelevanten Eingängen



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



1. Klicken Sie in der Ansicht **Geräte** unter dem Modul, mit dem das Schaltgerät verbunden werden soll, auf (das Modul



Abbildung 49: Sicherheitseingänge (virtuelle nicht sicherheitsrelevante Eingänge nur über die Registerkarte **Funktionsansicht** verfügbar)

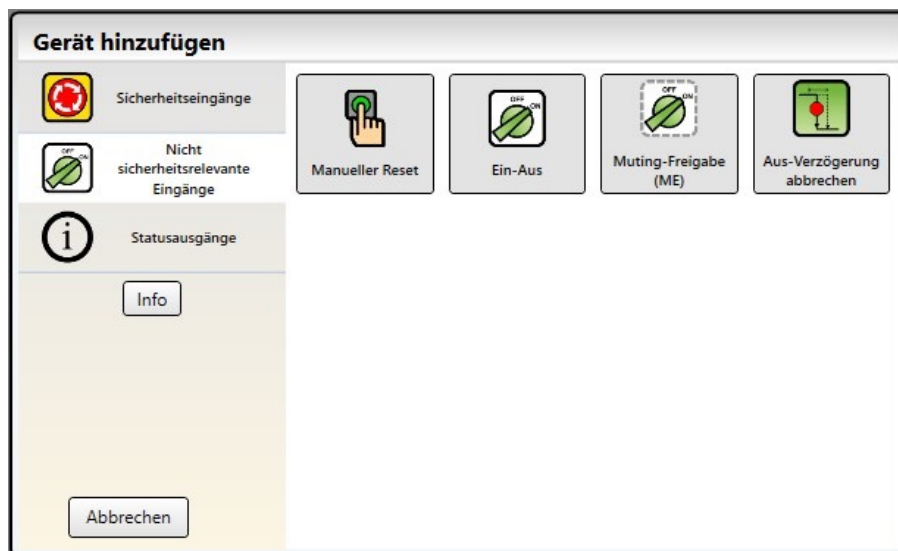


Abbildung 50: Nicht sicherheitsrelevante Eingänge (virtuelle nicht sicherheitsrelevante Eingänge nur über die Registerkarte **Funktionsansicht** verfügbar)



und die Klemmen können über das Fenster Eigenschaften für das **Eingangsgerät** geändert werden), oder auf einen Platzhalter auf der Registerkarte **Funktionsansicht**.

2. Klicken Sie auf **Sicherheitseingang oder Nichtsicherheitsrelevanter Eingang**, um Eingangsgeräte hinzuzufügen:
3. Wählen Sie die geeigneten Geräteeinstellungen aus:

Allgemeine Einstellungen

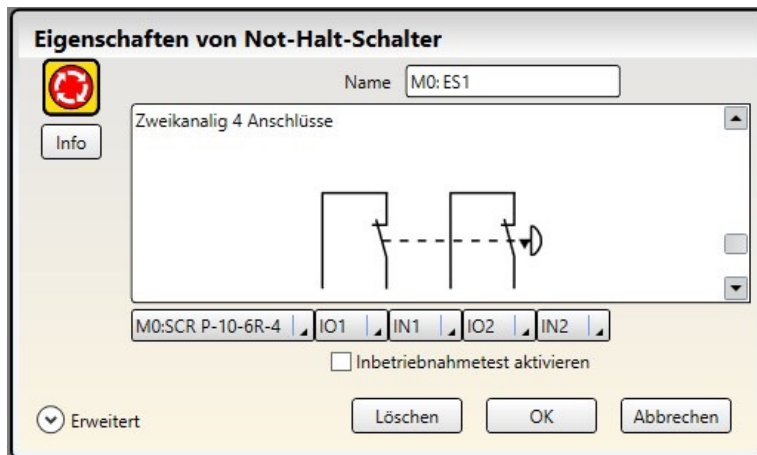


Abbildung 51: Allgemeine Einstellungen für Sicherheitseingänge

- 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):

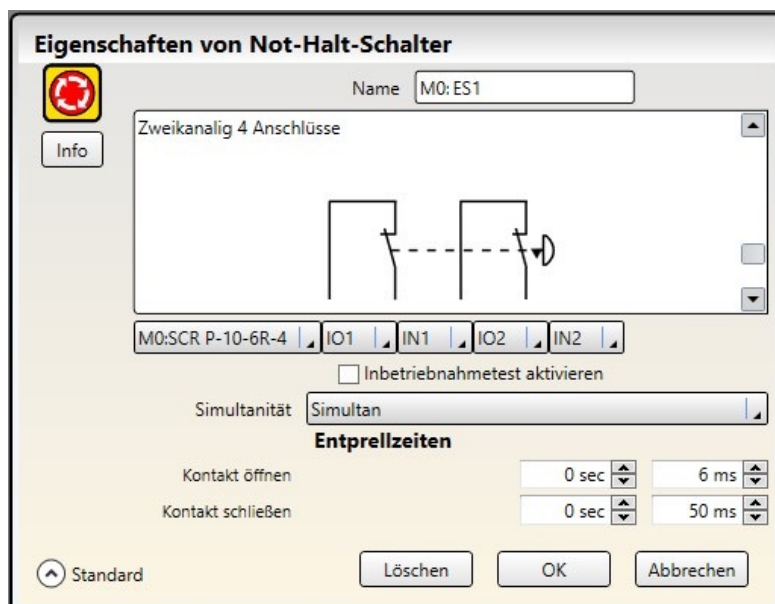




Abbildung 52: Erweiterte Einstellungen für Sicherheitseingänge

- Simultaneität (sofern zutreffend): „Simultan“ oder „Nicht simultan“ (zu den Definitionen siehe „19. Glossar“ auf Seite 255).
- 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

 Name:

 Geräteanzahl:

Position	Name	Typ		
1	Gerät 1	Türschalter	+	-
2	Gerät 2	Türschalter	+	-

Entprellzeiten

Kontakt öffnen:
 Kontakt schließen:

Abbildung 53: 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. Türschalter) 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 Schutztürschalter.



8.2.2 Hinzufügen von Statusausgängen

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

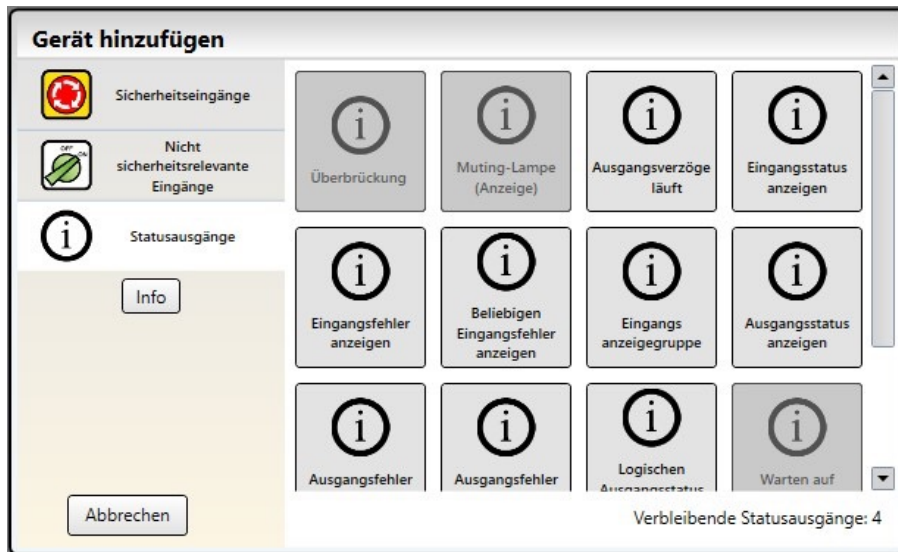


Abbildung 54: Statusausgänge

3. Wählen Sie die geeigneten Einstellungen für Statusausgänge:

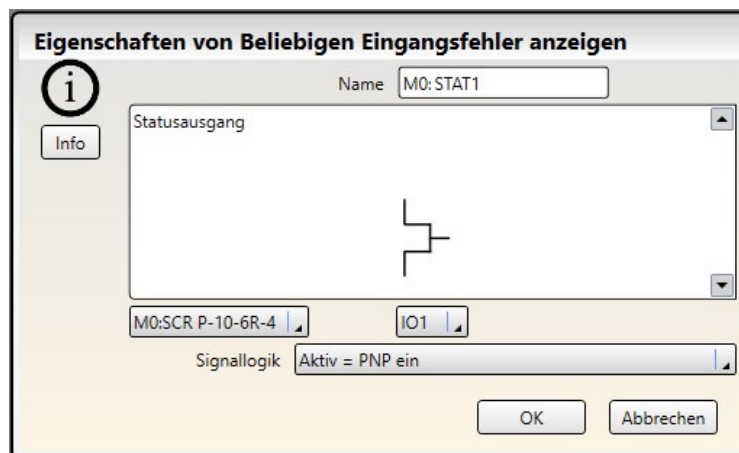



Abbildung 55: Statusausgangs-Eigenschaften

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



8.3 Entwerfen der Steuerungslogik

So entwerfen Sie die Steuerungslogik:

- 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 „8.2 Hinzufügen von Eingängen und Statusausgängen“ auf Seite 77 finden Sie weitere Informationen und Geräteeigenschaften.
- Fügen Sie **Logik-** und/oder **Funktionsblöcke** hinzu (siehe „9.6.1 Logikblöcke“ auf Seite 101 und „9.6.2 Funktionsblöcke“ auf Seite 103), 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

- 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



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

⁷ Statusausgänge können konfiguriert werden, wenn der Status eines Eingangsgeräts oder eines Ausgangs kommuniziert werden muss. Die IOx-Klemmen werden für diese Statussignale verwendet.

8.4 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:

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

8.4.1 Schreiben einer bestätigten Konfiguration in einen SCR P-FPS mit dem Programmierwerkzeug

1. Stecken Sie den SCR P-FPS in den Programmieradapter SCR P-PA.
2. Stecken Sie bei laufender BERNSTEIN Safety Controller Software den Programmieradapter in einen USB-Anschluss des PCs. Das SCR P-FPS Symbol sollte aktiv werden (etwas dunkler als ausgegraut werden).
3. Klicken Sie auf  und wählen Sie **SCR P-FPS schreiben**.



Hinweis: Wenn **Write SCR P-FPS** ausgegraut ist, handelt es sich bei der Konfiguration nicht um eine .xcc (bestätigte Version).

4. Überprüfen Sie die gewünschten Passwörter.
5. Klicken Sie auf **An SCR P-FPS senden**.
Das Fenster Konfiguration auf SCR P-FPS Laufwerk schreiben wird geöffnet.



Hinweis: Bei diesem Vorgang werden alle Daten (Konfiguration, Netzwerkeinstellungen und Kennwörter) auf das SCR P-FPS Laufwerk kopiert.

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



8.4.2 Hinweise zum Bestätigen oder Schreiben einer Konfiguration in ein konfiguriertes SCR P oder SCx

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

Benutzer1

1. Klicken Sie auf **Konfiguration in die Auswertung schreiben**, um eine Konfiguration zu bestätigen bzw. um eine bestätigte Konfiguration in eine konfigurierten 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.



8.5 Beispiel-Konfigurationen

Die Software enthält mehrere Beispielkonfigurationen, die verschiedene Funktionen oder Anwendungen der Sicherheitssteuerung demonstrieren. Um auf diese Konfigurationen zuzugreifen, gehen Sie zu  **Open Project** > **Sample Projects** und wählen Sie das gewünschte Projekt aus. Der SCx verfügt über drei Gruppierungen von Beispielkonfigurationen:

Anwendungen - **Enthält** Beispiele für einfache mögliche Anwendungen des Controllers. Zwei der Beispiele sind Ersatz für veraltete Module.

Dokumentation - **Enthält** Beispiele. Die meisten der hier enthaltenen Beispiele werden in den folgenden Abschnitten beschrieben, ein Beispiel ist in der Kurzanleitung (online verfügbar) beschrieben.

Beispiele - **Enthält** drei Abteilungen: **Funktionsblöcke**, **Logikblöcke** und **Sicherheitsausgänge**. Diese Beispiele zeigen die Funktionalität der verschiedenen Blöcke. Um beispielsweise zu sehen, wie ein Bypass-Block funktioniert, wählen Sie **Funktionsblöcke** > **Bypass-Block (alle Funktionen aktiviert)** und führen ihn im Simulationsmodus aus.

Für das SCR P-10-6R-4 gibt es mehrere Beispielkonfigurationen. Diese Beispiele umfassen typische Anwendungen des Modells SCR P-10-6R-4. Verwenden Sie die Beispiele als Ausgangspunkt und ändern Sie sie für Ihre spezifischen Anforderungen.

SCx Beispielkonfiguration

Dieser Abschnitt beschreibt den Entwurf der Beispielkonfiguration „3 Zone Muting Instruction Manual“, die sich im Abschnitt **Dokumentation** der SCx Beispielprogramme befindet. Diese Beispielkonfiguration ist für eine Palettierroboter-Anwendung, die eine SCx-Sicherheitssteuerung, ein SCx-I-8-Sicherheitseingangsmodul, drei optische Sensoren (Muting wird über die Software hinzugefügt), zwei Verriegelungsschalter, einen manuellen Reset und eine Not-Aus-Taste verwendet.

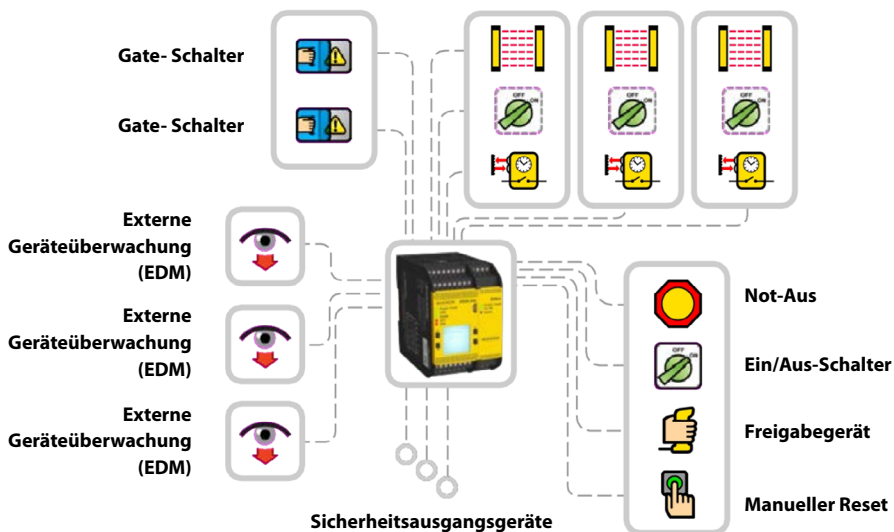



Abbildung 56: Schematische Darstellung einer Beispielkonfiguration



Um die Konfiguration für diese Anwendung zu entwerfen:

1. Klicken Sie auf **Neues Projekt**.
2. Definieren Sie Projekteinstellungen. Siehe „9.4  Projekteinstellungen“ auf Seite 98.
3. Wählen Sie das Base Controller-Modell aus. Siehe Registerkarte Ausrüstung auf Seite 106 (bei dieser Konfiguration muss nur das Feld **Ist erweiterbar** markiert sein).
4. Fügen Sie das Erweiterungsmodul SCx-I-16 hinzu, indem Sie auf rechts neben dem Base Controller klicken.
 - Klicken Sie auf **Eingangsmodule**.
 - Wählen Sie **SCx-I-16**.

Eingabe	Menge	Typ	Modul	Terminals	Schaltung
Not-Aus	1	Sicherheitseingang	SCx-I-16	IO1, IN1, IN2	Zweikanalige 3-Klemme
Freigabegerät	1	Sicherheitseingang	SCx-I-16	IO1, IN3, IN4	Zweikanalige 3-Klemme
Externe Geräteüberwachung	3	Sicherheitseingang	Basis	1. IO3 2. IO4 3. IO5	Einkanalig 1 Klemme
Gate-Schalter	2	Sicherheitseingang	Basis	1. IO1, IN15, IN16 2. IO2, IN17, IN18	Zweikanalige 3-Klemme
Manueller Reset	1	Nicht-Sicherheits-Eingang	SCx-I-16	IN6	Einkanalig 1 Klemme
Stummschaltung eines Sensorpaares	3	Sicherheitseingang	Basis	1. IN9, IN10 2. IN11, IN12 3. IN13, IN14	Zweikanaliges 2-Terminal
Stummschaltung Aktivieren	3	Nicht-Sicherheits-Eingang	Basis	1. IN1 2. IN2 3. IO8	Einkanalig 1 Klemme
Ein-Aus	1	Nicht-Sicherheits-Eingang	SCx-I-16	IN5	Einkanalig 1 Klemme
Optischer Sensor	3	Sicherheitseingang	Basis	1. IN3, IN4 2. IN5, IN6 3. IN7, IN8	Zweikanal-PNP

5. Fügen Sie die folgenden Eingänge hinzu und ändern Sie nur den Schaltkreistyp:



Tipp: Sie werden feststellen, dass nicht alle Eingaben auf Seite 1 platziert sind. Es gibt zwei Lösungen, um die Konfiguration auf einer Seite zu halten. Führen Sie einen der folgenden Schritte aus:

1. Fügen Sie einen **Verweis** zu einem Block auf einer anderen Seite hinzu - klicken Sie auf einen der leeren Platzhalter im mittleren Bereich, wählen Sie **Verweis** und wählen Sie den Block auf der nächsten Seite. Es können nur Blöcke von anderen Seiten als **Verweis** hinzugefügt werden.
2. Seite neu zuordnen - standardmäßig werden alle auf der Registerkarte **Ausrüstung** hinzugefügten Eingaben auf der Registerkarte **Funktionsansicht** auf dem ersten verfügbaren Platzhalter in der linken Spalte platziert. Die Eingänge können jedoch an eine beliebige Stelle im mittleren Bereich verschoben werden. Verschieben Sie einen der Blöcke auf einen der Platzhalter im mittleren Bereich. Wechseln Sie zu der Seite, die den zu verschiebenden Block enthält. Wählen Sie den Block aus und ändern Sie die Seitenzuordnung unterhalb der Tabelle **Eigenschaften**



6. Gehen Sie auf die Registerkarte **Funktionale Ansicht**.
 7. Split **M0:SO2**:
 - Doppelklicken Sie auf **M0:SO2** oder wählen Sie es aus und klicken Sie in der Tabelle **Eigenschaften** auf **Bearbeiten**.
 - Klicken Sie auf **Teilen**.
 8. Fügen Sie die folgenden **Funktionsblöcke** hinzu, indem Sie auf einen der leeren Platzhalter im mittleren Bereich der Registerkarte **Funktionsansicht** klicken (weitere Informationen finden Sie unter „9.6.2 Funktionsblöcke“ auf Seite 103):
 - **Muting-Block x 3 (Muting-Modus: One Pair, ME (Mute Enable):** Abgehakt)
 - **Aktivieren der Gerätesperre (ES: Angekreuzt, JOG (Jog):** Angekreuzt)
 9. Fügen Sie die folgenden **Logikblöcke** hinzu, indem Sie auf einen der leeren Platzhalter im mittleren Bereich der Registerkarte **Funktionsansicht** klicken (weitere Informationen finden Sie unter „9.6.1 Logikblöcke“ auf Seite 101):
 - **AND** mit 2 Eingangsknoten
 - **AND** mit 4 Eingangsknoten
 10. Schließen Sie Folgendes an jeden **Muting-Block** an:
 - 1 x **Optischer Sensor** (IN-Knoten)
 - 1 x **Stummschaltungssensor-Paar** (MP1-Knoten)
 - 1 x **Mute-Freigabe** (ME-Knoten)
 11. Verbinden Sie **Gate Switch** x 2 mit dem AND-Block mit 2 Knoten.
 12. Verbinden Sie den **Muting-Block** x 3 und den AND-Block mit 2 Knoten mit dem AND-Block mit 4 Knoten.
 13. Schließen Sie einen der **Muting-Blöcke** an einen der geteilten Sicherheitsausgänge (**M0:SO2A** oder **M0:SO2B**) und einen an den anderen geteilten Sicherheitsausgang an.
 14. Schließen Sie Folgendes an den **Enabling Device Block** an:
 - **Not-Aus** (ES-Knoten)
 - **Freigabegerät** (ED-Knoten)
 - AND-Block mit vier Eingangsknoten (IN-Knoten)
 - Manueller Reset (RST-Knoten)
 - **Ein-Aus** (JOG-Knoten)
 15. Schließen Sie den **Enabling Device Block** an den verbleibenden Sicherheitsausgang (**M0:SO1**) an.
 16. Aktivieren Sie EDM (External Device Monitoring) in jedem der Fenster der **Sicherheitsausgangseigenschaften**.
 17. Verbinden Sie 1x den Eingang **Externe Geräteüberwachung** mit jedem der Sicherheitsausgänge. Die Beispielkonfiguration ist abgeschlossen.
- Sicherheitsausgänge. Die Beispielkonfiguration ist abgeschlossen.



Hinweis: An dieser Stelle können Sie die Blöcke auf der Registerkarte **Funktionsansicht** neu positionieren, um einen besseren Konfigurationsfluss zu erreichen, wie in der folgenden Abbildung dargestellt:





Hinweis: An dieser Stelle können Sie die Blöcke auf der Registerkarte **Funktionsansicht** neu positionieren, um einen besseren Konfigurationsfluss zu erreichen, wie in der folgenden Abbildung dargestellt:

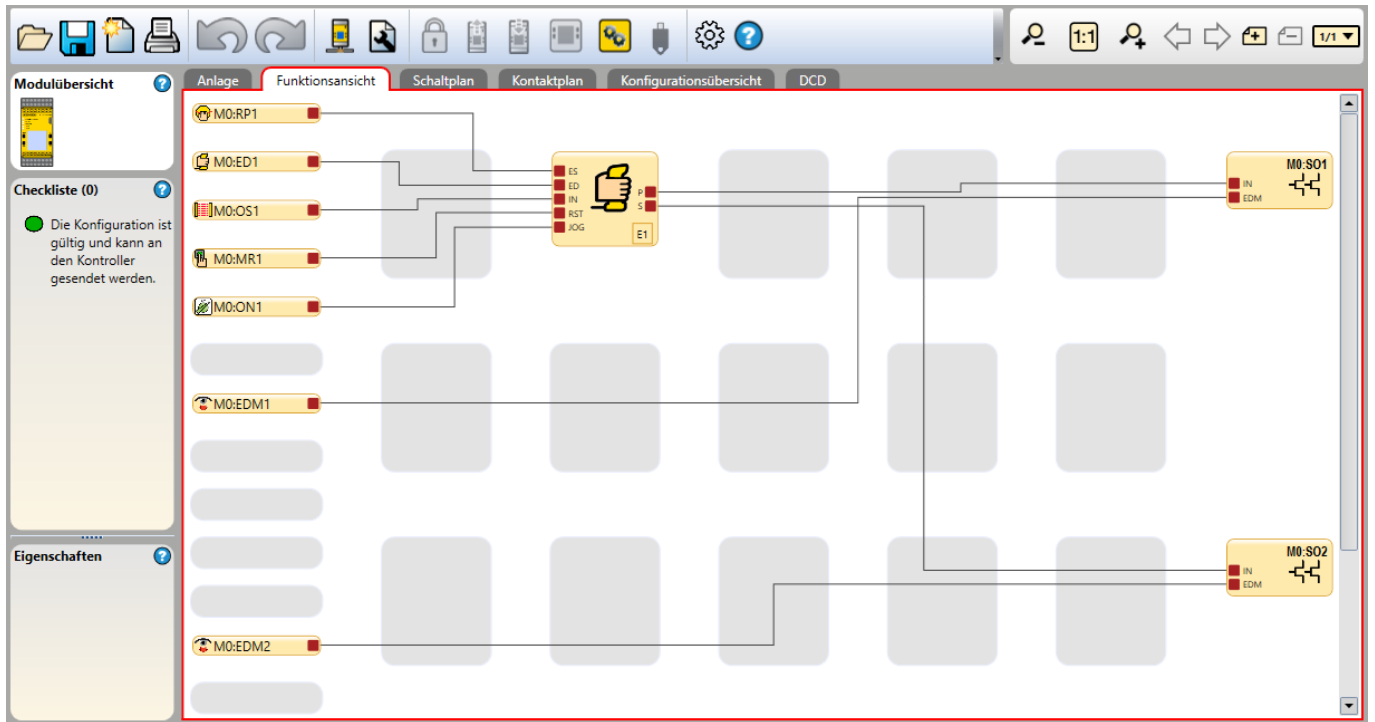


Abbildung 57: Abbildung 66: Beispielkonfiguration - Registerkarte **Funktionsansicht**

8.5.1 SCx: Einfache Pressensteuerung mit veränderbarem Sicherheitseingang Beispielkonfiguration

In diesem Abschnitt wird der Aufbau einer einfachen Pressensteuerung beschrieben, die sich unter dem Abschnitt Dokumentation der SCx-Beispielprogramme befindet.

Diese Beispielkonfiguration ist für eine einfache hydraulische/pneumatische Pressenanwendung, die eine SCx-Sicherheitssteuerung, Eingänge für den Pressenstatus, eine Zyklusauslösung, eine manuelle Rückstellung, einen optischen Sicherheitssensor und einen Notausschalter verwendet.

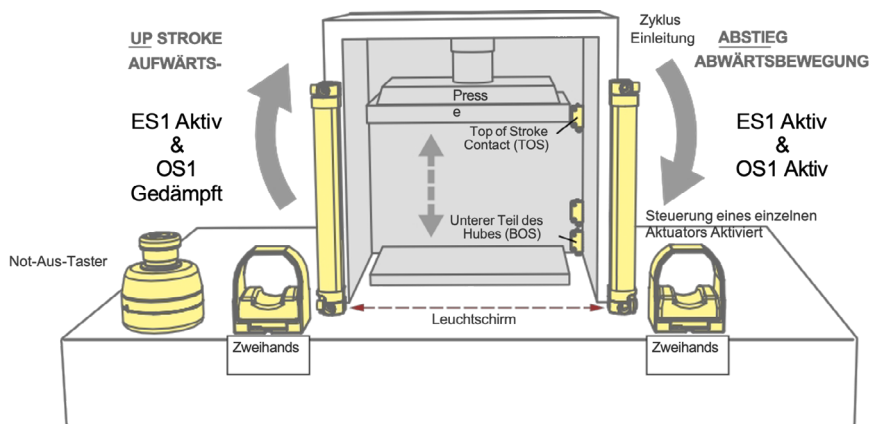



Abbildung 58: Abbildung 67. Einfache Beispielkonfiguration der Pressensteuerung



Um die Konfiguration für diese Anwendung zu entwerfen:

1. Klicken Sie auf **Neues Projekt**.
2. Definieren Sie die Projekteinstellungen. Siehe „9.4  Projekteinstellungen“ auf Seite 98.
3. Wählen Sie das gewünschte Base. Controller-Modell aus. Siehe Registerkarte Ausrüstung auf Seite 106.

Eingabe	Menge	Typ	Terminals	Schaltung
Einleitung des Zyklus	1	Sicherheitseingang	IN1, IN2	Zweikanaliges 2-Terminal
TOS (ein/aus)	1	Nicht-Sicherheit	IN5	Einkanalig 1 Klemme
BOS (ein/aus)	1	Nicht-Sicherheit	IN6	Einkanalig 1 Klemme
Manueller Reset	1	Nicht-Sicherheit	IN7	Einkanalig 1 Klemme
Not-Aus	1	Sicherheitseingang	IN10, IN11	Zweikanaliges 2-Terminal
Optischer Sensor	1	Sicherheitseingang	IN8, IN9	Zweikanal-PNP

4. Fügen Sie die folgenden Eingänge hinzu, indem Sie den Namen und den Schaltkreistyp nach Bedarf ändern.
5. Gehen Sie auf die Registerkarte **Funktionale Ansicht**.
6. Fügen Sie den Funktionsblock Pressensteuerung hinzu und konfigurieren Sie ihn.
 - a. Klicken Sie auf einen der leeren Platzhalter im mittleren Bereich der Registerkarte **Funktionsansicht**. Weitere Informationen finden Sie unter „9.6.2 Funktionsblöcke“ auf Seite 103.
 - b. Wählen Sie **Funktionsblöcke** und wählen Sie **Steuerung drücken**.
 - c. Wählen Sie im Fenster **Press Control Properties** die Option **PCI (Press Control Input Function Block)** und **Single**

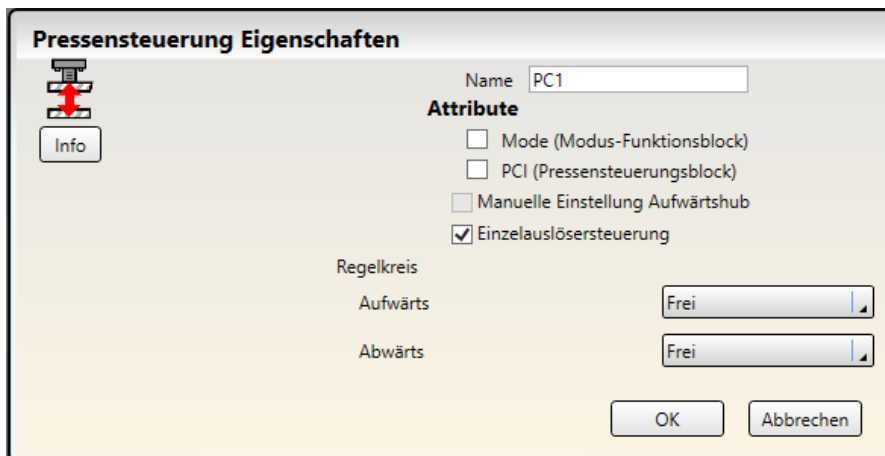


Abbildung 59: Eigenschaften der Pressesteuerung

Actuator Control.

Das Häkchen im Feld **Manuelle Aufwärtshubeinstellung** verschwindet.

- d. Klicken Sie auf **OK**.
- Das Fenster **Eigenschaften der Pressesteuereingänge** wird geöffnet.
- e. Abbildung 69. Eigenschaften der Pressesteuereingänge
- f. Wählen Sie **M Safety (Mutable Safety Stop)**.
- g. Klicken Sie auf **OK**.
7. Schließen Sie Folgendes an:
 - Eingang zur Zykluseinleitung an den GO-Knoten des Funktionsblocks Pressensteuerung
 - TOS an den TOS-Knoten des Funktionsblocks Press Control
 - BOS an den BOS-Knoten des Funktionsblocks Press Control
 - Manueller Reset auf den RST-Knoten des Funktionsblocks Press Control
 - Not-Aus an den NM-Sicherheitsknoten des Funktionsblocks Pressensteuerung
 - Optischer Sensor an den Sicherheitsknoten M des Funktionsblocks Press Control Input
8. Verbinden Sie den Ausgangsknoten U des Funktionsblocks Press Control mit SO1 (ändern Sie den Namen von SO1 in „Up Stroke“).
9. Verbinden Sie den Ausgangsknoten D des Funktionsblocks Press Control mit SO2 (ändern Sie den Namen von SO2 in „Dwn Strk“). Die Beispielkonfiguration ist abgeschlossen.





Hinweis: An dieser Stelle können Sie die Blöcke auf der Registerkarte **Funktionsansicht** neu positionieren, um einen besseren Konfigurationsfluss zu erreichen, wie in der folgenden Abbildung dargestellt:

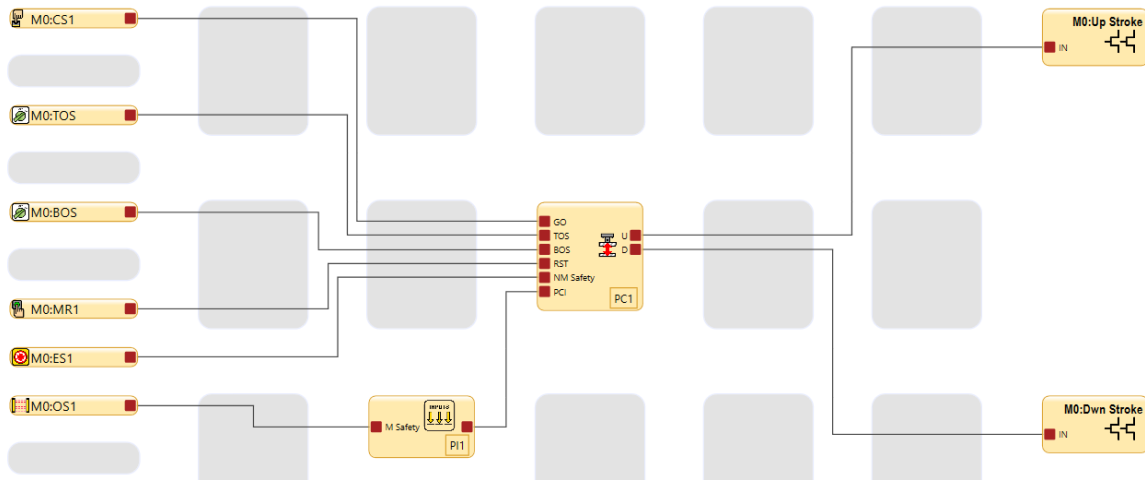



Abbildung 60: Abbildung 70. Funktionsblock Position

SCx: Simulieren Sie die Funktionsweise der einfachen Pressensteuerungskonfiguration

Im Folgenden wird die Funktionsweise der einfachen Konfiguration der Pressensteuerung simuliert:

1. Klicken Sie auf  um in den Simulationsmodus zu gelangen.
2. Klicken Sie auf **Abspielen**, um den Simulations-Timer einzuschalten (ähnlich wie beim Einschalten der Maschine).
3. Schalten Sie die Eingänge Not-Aus, optischer Sensor und TOS in den Zustand EIN (grün).
4. Klicken Sie auf den Rücksetzeingang MR1. Der Funktionsblock Pressensteuerung sollte auf EIN (grün) schalten.
5. Klicken Sie auf den Eingang CS1, um den Zustand EIN (grün) zu erreichen. Der SCx Ausgang Dwn Strk wird EIN (grün).
6. Klicken Sie den TOS-Eingang in den AUS-Zustand (rot).
7. Klicken Sie auf den BOS-Eingang, um ihn einzuschalten (grün). Der Ausgang „Dwn Strk“ wird ausgeschaltet (rot) und der Ausgang „Up Stroke“ wird eingeschaltet (grün).
8. Klicken Sie auf den BOS-Eingang AUS (rot).
9. Klicken Sie auf den TOS-Eingang, um ihn einzuschalten (grün). Der Aufwärts-hub- Ausgang wird ausgeschaltet (rot).
10. Schalten Sie den CS1-Eingang in den AUS-Zustand (rot). Dies kann jederzeit geschehen, nachdem der Ausgang Dwn Strk auf ON (grün) geschaltet wurde.
11. Klicken Sie den Eingang des optischen Sensors in den AUS-Zustand (rot) und dann wieder in den EIN-Zustand (grün). Das System ist bereit, den nächsten Zyklus zu starten, indem es den CS1-Eingang wieder einschaltet.

Wenn der optische Sensor oder der Not-Aus-Schalter während des Auf- oder Abwärtshubs ausgeschaltet werden, muss der MR1-Eingang umgeschaltet werden, dann muss der CS1 schaltet den Ausgang Up Stroke auf ON.

8.5.2 SCx: Beispielkonfiguration der Pressesteuerung mit allen Funktionen

Dieser Abschnitt beschreibt den Aufbau einer Pressensteuerung, die alle möglichen Funktionen (außer AVM) nutzt. Die Beispielkonfiguration befindet sich unter dem Abschnitt Dokumentation der SCx-Beispielprogramme.

Diese Beispielkonfiguration ist für eine komplexere hydraulische/pneumatische Pressenanwendung, die eine SCx-Sicherheitssteuerung, ein SCx-O-4T-Sicherheitsausgangsmodul, Pressestatuseingänge, einen Zyklusstart, einen manuellen Reset, einen optischen Sicherheitssensor, einen sequenziellen Stopp, einen Stummschaltungssensor, einen Fußschaltereingang und ein Not-Halt-Taster verwendet.



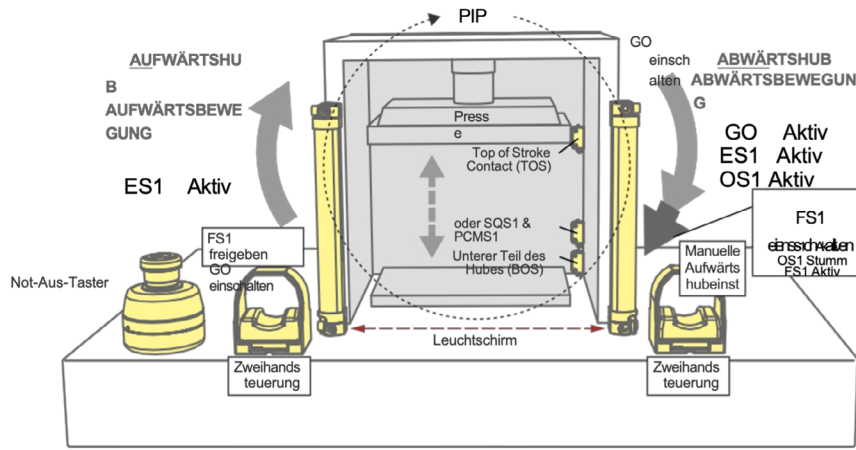


Abbildung 61: Beispiel für die Konfiguration der Pressesteuerung mit allen Funktionen

Um die Konfiguration für diese Anwendung zu entwerfen:

1. Klicken Sie auf **Neues Projekt**.
2. Definieren Sie die Projekteinstellungen. Siehe „9.4 Projekteinstellungen“ auf Seite 98.
3. Wählen Sie das gewünschte Base Controller-Modell aus. Siehe Registerkarte Ausrüstung auf Seite 106 (für diese Konfiguration muss nur die Option **Ist erweiterbar** ausgewählt werden).
4. Erweiterungsmodul SCx-O-4T hinzufügen.
 - a. Klicken Sie rechts neben dem Basiscontroller.
 - b. Klicken Sie auf **Ausgabemodule**.
 - c. Wählen Sie SCx-O-4T.
5. Fügen Sie die folgenden Eingänge hinzu, indem Sie den Namen und den Schaltkreistyp nach Bedarf ändern.

Eingabe	Anz ahl.	Typ	Terminals	Schaltung
Zweihandsteuerung	1	Sicherheitseingang	IN9, IN10	Zweikanal-PNP
TOS (EIN/AUS)	1	Nicht-Sicherheit	IN1	Einkanalig 1 Klemme
BOS (EIN/AUS)	1	Nicht-Sicherheit	IN2	Einkanalig 1 Klemme
Manueller Reset	1	Nicht-Sicherheit	IN11	Einkanalig 1 Klemme
Not-Aus	1	Sicherheitseingang	IO1, IN3, IN4	Zweikanalige 3-Klemme
Laufen (EIN/AUS)	1	Nicht-Sicherheit	IN12	Einkanalig 1 Klemme
Aufwärts (EIN/AUS)	1	Nicht-Sicherheit	IN13	Einkanalig 1 Klemme
Abwärts (ON/OFF)	1	Nicht-Sicherheit	IN14	Einkanalig 1 Klemme
PIP (EIN/AUS)	1	Nicht-Sicherheit	IN5	Einkanalig 1 Klemme
Pressensteuerung SQS	1	Sicherheitseingang	IN6	Einkanalig 1 Klemme
Fußschalter	1	Sicherheitseingang	IO2	Einkanalig 1 Klemme
Presse Steuerung Stummschaltungssensor	1	Sicherheitseingang	IO3	Einkanalig 1 Klemme
Optischer Sensor	1	Sicherheitseingang	IN7, IN8	Zweikanal-PNP



- 6.
7. Gehen Sie auf die Registerkarte **Funktionale Ansicht**.
8. Fügen Sie den Funktionsblock Pressensteuerung hinzu und konfigurieren Sie ihn.
 - a. Klicken Sie auf einen der leeren Platzhalter im mittleren Bereich der Registerkarte **Funktionsansicht**. Weitere Informationen finden Sie unter „9.6.2 Funktionsblöcke“ auf Seite 103.
 - b. Wählen Sie **Funktionsblöcke** und wählen Sie **Steuerung drücken**.
 - c. Wählen Sie im Fenster **Eigenschaften von Press Control** den **Modus (Mode Function Block)** und **PCI (Press**

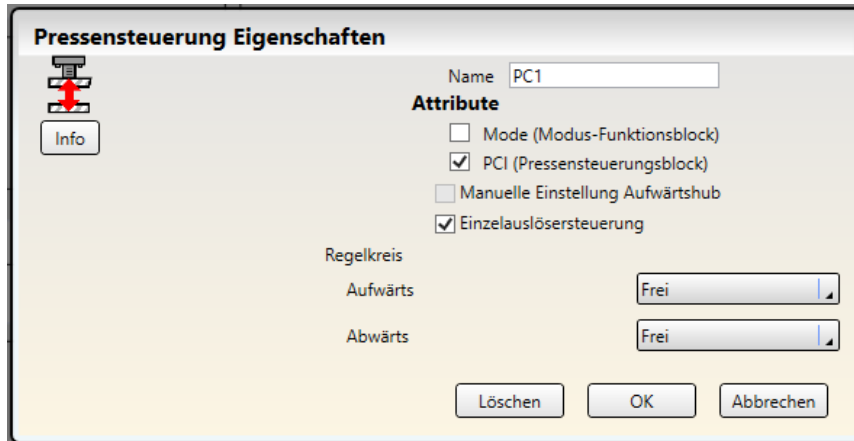


Abbildung 62: Eigenschaften der Pressesteuerung

Control Input Function Block). Lassen Sie das Kästchen **Manuelle Aufwärtshubeinstellung** markiert.

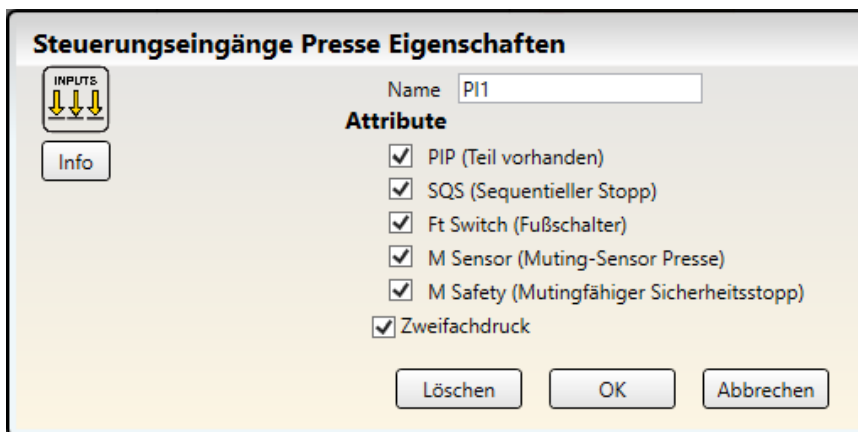


Abbildung 63: Eigenschaften der Pressesteuereingänge

- d. Klicken Sie auf **OK**. Das Fenster **Eigenschaften der Pressesteuereingänge** wird geöffnet.
- e. Aktivieren Sie alle Kontrollkästchen. Beachten Sie, dass bei Auswahl von **SQS** drei weitere Optionen angezeigt werden; wählen Sie diese ebenfalls aus (alle sechs Kästchen sollten markiert sein).
- f. Klicken Sie auf **OK**. Das Fenster **Modus-Eigenschaften** wird angezeigt.
- g. Klicken Sie auf **OK**.
9. Schließen Sie Folgendes an den Modusauswahlblock an:
 - Eingabe in den Knoten „Eingabe ausführen“ ausführen
 - Up-Eingang zum Inch Up-Eingangsknoten
 - Down-Eingang zum Inch Down-Eingangsknoten
10. Schließen Sie Folgendes an den Press Control Inputs Block an:
 - Part-In-Place (PIP)-Eingang zum PIP-Eingangsknoten
 - Sequentieller Stopp (SQS) Eingang zum SQS-Eingangsknoten
 - Fußschaltereingang zum Eingangsknoten Ft Switch
 - Drücken Sie Control Mute Sensor (PCMS) auf den Eingangsknoten M Sensor
 - Optischer Sensor an den M Safety Eingangsknoten
11. Schließen Sie Folgendes an den Pressesteuerblock an:
 - Two-Hand-Control-Eingang zum GO-Eingangsknoten
 - TOS an den TOS-Eingangsknoten
 - BOS an den BOS-Eingangsknoten
 - Manueller Reset auf den RST-Eingangsknoten



- Not-Aus an den NM Safety-Eingangsknoten
- 12. Verbinden Sie den Ausgangsknoten U des Funktionsblocks Press Control mit SO1 (ändern Sie den Namen von SO1 in „UPSO1“).
- 13. Verbinden Sie den Ausgangsknoten D des Funktionsblocks Press Control mit SO2 (ändern Sie den Namen von SO2 in „DOWNSO2“).
- 14. Gehen Sie auf Seite 2 der Registerkarte Funktionale Ansicht (verwenden Sie den Pfeil in der oberen rechten Ecke).
- 15. Legen Sie einen Referenzknoten für PCx-H und einen weiteren für PCx-L an.
- 16. Schließen Sie den PCx-H an SO1 an (ändern Sie den Namen von SO1 in „HIGHSO1“).
- 17. Schließen Sie das PCx-L an SO2 an (ändern Sie den Namen von SO2 in „LOWSO2“). Die Konfiguration der Probe ist abgeschlossen.



Hinweis: An dieser Stelle kann es hilfreich sein, die Blöcke in der **Funktionsansicht** neu zu positionieren, um den Konfigurationsfluss zu verbessern, wie in der folgenden Abbildung dargestellt.

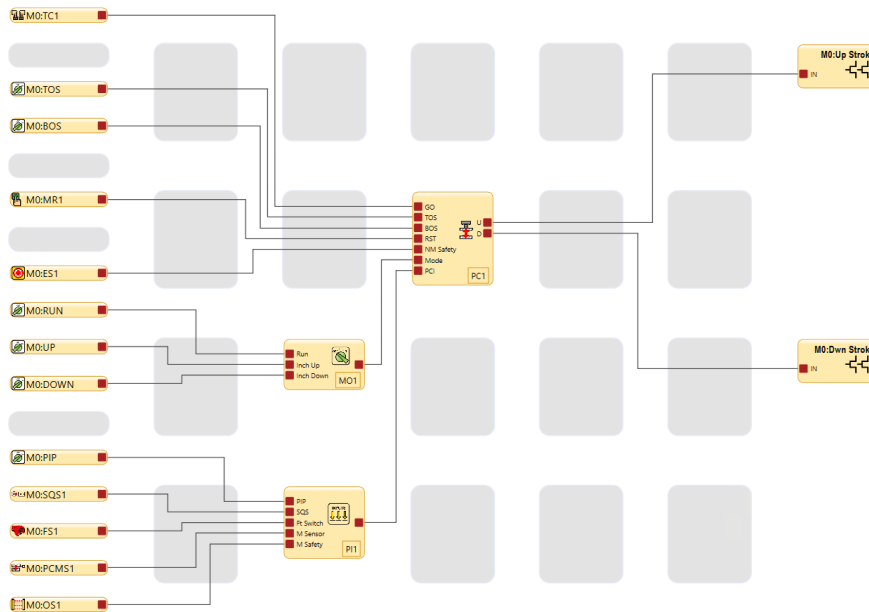



Abbildung 64: Funktionsblock Position

SCx: Simulieren Sie die Funktionalität der Konfiguration der Pressesteuerung mit allen Funktionen

Im Folgenden wird beschrieben, wie Sie die Funktionsweise dieser Pressesteuerungskonfiguration simulieren können:

1. Klicken Sie auf , um in den Simulationsmodus zu gelangen.
2. Klicken Sie auf Abspielen, um den Simulations-Timer einzuschalten (ähnlich wie beim Einschalten der Maschine).
3. Schalten Sie die Eingänge Not-Aus, optischer Sensor, TOS und Run auf den Zustand Ein (grün).
4. Klicken Sie auf den Rücksetzeingang MR1. Der Funktionsblock Press Control und der Ausgang LOWSO2 sollten in den Zustand On (grün) übergehen. Dies ist auf Seite 2; klicken Sie auf den Pfeil oben rechts, um die Seite zu wechseln.
5. Klicken Sie auf den PIP-Eingang, um ihn einzuschalten (grün).
6. Klicken Sie auf den Eingang TC1, um ihn einzuschalten (grün). Der Ausgang DOWNSO2 wird eingeschaltet (grün).
7. Klicken Sie den TOS-Eingang in den Zustand Aus (rot).
8. Klicken Sie die Eingänge SQS1 und PCMS1 an, um sie in den Zustand Ein (grün) zu versetzen. Der Ausgang DOWNSO2 wird ausgeschaltet (rot), der Ausgang LOWSO2 wird ausgeschaltet (rot) und der Ausgang HIGHSO1 (Seite 2) wird eingeschaltet (grün).
9. Klicken Sie den Eingang TC1 in den Aus-Zustand (rot).
10. Klicken Sie auf den Eingang FS1, um ihn einzuschalten (grün). Der Ausgang DOWNSO2 wird eingeschaltet (grün).
11. Klicken Sie den BOS-Eingang in den Zustand Ein (grün). Der Ausgang DOWNSO2 und der Ausgang HIGHSO1 (Seite 2) werden ausgeschaltet (rot) und der Ausgang LOWSO2 (Seite 2) wird eingeschaltet (grün).
12. Klicken Sie auf den Eingang FS1, um ihn in den Aus-Zustand (rot) zu versetzen.
13. Klicken Sie auf den Eingang TC1, um ihn einzuschalten (grün). Der Ausgang UPSO1 wird eingeschaltet (grün).
14. Klicken Sie die Eingänge BOS, PCMS1 und SQS1 in den Aus-Zustand (rot).
15. Klicken Sie den TOS-Eingang an, um ihn einzuschalten (grün). Der Ausgang UPSO1 wird ausgeschaltet (rot).
16. Klicken Sie den Eingang TC1 in den Aus-Zustand (rot).
17. Klicken Sie auf den Eingang des optischen Sensors, um ihn auszuschalten (rot), klicken Sie auf den PIP-Eingang, um ihn auszuschalten (rot), dann zurück in den Ein-Zustand (grün) und klicken Sie dann auf den Eingang des optischen Sensors, um ihn wieder einzuschalten (grün).



Das System ist bereit, den nächsten Zyklus zu starten, indem es den Eingang TC1 wieder in den Ein-Zustand (grün) versetzt. Wenn der TC1-Eingang während des Abwärtshubs ausgeschaltet ist (rot), wird der Abwärtshub durch das Wiedereinschalten nicht verändert; die Presse fährt mit dem Abwärtshub fort. Damit die Presse nach dem Ausschalten des TC1-Eingangs nach oben (statt nach unten) fährt, klicken Sie auf den MR1-Eingang und schalten dann den TC1-Eingang wieder ein. Wenn der optische Sensor oder der Not-Aus-Schalter während des Auf- oder Abwärtshubs ausgeschaltet sind, sollte der TC1-Eingang ausgeschaltet werden, dann sollte der MR1-Eingang betätigt werden, und dann schaltet das Einschalten von TC1 den UP-SO1-Ausgang ein.

9. 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 Echtzeitinformatoren, 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 „8.1 Erstellen einer Konfiguration“ auf Seite 77 finden Sie Informationen zum Konfigurationserstellungsprozess. Unter „9.7 Registerkarte Schaltplan“ auf Seite 104 finden Sie Informationen zum Verbinden von Geräten sowie „9.8 Registerkarte Kontaktplan“ auf Seite 105 die Darstellung der Kontaktpläne der Konfiguration.

Unter „9.16 Livemodus“ auf Seite 118 finden Sie Laufzeitinformationen der Sicherheitsauswertung.

9.1 Abkürzungen

Abkürzung ⁸	Beschreibung
AVM	Einstellbarer Ventilüberwachungs-Eingangsknoten der Sicherheitsausgänge
AVMx	Einstellbarer Ventilüberwachungseingang
BP	Bypass-Eingangsknoten der Bypass-Blöcke und Muting-Blöcke
BPx	Bypass Schaltereingang
BOS	Unterseite des Hub-Eingangsknotens der Press Control-Blöcke (nur SCx)
CD	Verzögerungs-Eingangsknoten der Sicherheitsausgänge, Verzögerungsblöcke und One-Shot-Blöcke abrechen
CDx	Abbrechen Verzögerungseingang
CSx	Eingang Zykluseinleitung
DCD	Daisy Chain Diagnose
ED	Freigabe-Eingangsknoten der Freigabeblocke
EDx	Aktivieren der Geräteeingabe
EDM	Externes Gerät Überwachungseingangsknoten der Sicherheitsausgänge
EDMx	Externes Gerät Überwachungseingang
ES	Not-Aus-Eingangsknoten der Freigabegeräteblöcke
ESx	Not-Aus-Eingang
ETB	Externe Klemmleiste (nur SCR P)
FID	Identifizierung von Merkmalen
FSx	Fußschalter-Eingang
FR	Fault Reset Eingangsknoten der Safety Outputs
Ft Schalter	Fußschalter-Eingangsknoten der Press Control Blocks (nur SCx)

⁸ Die Endung ‚x‘ bezeichnet die automatisch zugewiesene Nummer.



Abkürzung⁸	Beschreibung
GO	Zyklusstart-Eingangsknoten der Pressensteuerungsblöcke (nur SCx)
GSx	Gate Schaltereingang
JOG	Jog-Eingangsknoten der Freigabegeräteblöcke
IN	Normaler Eingangsknoten von Funktionsblöcken und Sicherheitsausgangsblöcken
LR	Latch-Reset-Eingangsknoten des Latch-Reset-Blocks und der Sicherheitsausgänge
ME	Mute-Enable-Eingangsknoten der Muting-Blöcke und Zweihand-Steuerblöcke
MEx	Stummschaltung Aktivierungseingang
MP1	Erster Muting-Sensorpaar-Eingangsknoten in Muting-Blöcken und Zweihand-Steuerblöcken
MP2	Zweiter Muting-Sensorpaareingangsknoten (nur Muting-Blöcke)
M Sicherheit	Mutable Safety Input Knoten der Press Control Blöcke (nur SCx)
M Sensor	Press Control Mute Sensor-Eingangsknoten der Press Control-Blöcke (nur SCx)
Mx	Basis-Controller und Erweiterungsmodule (in der auf der Registerkarte Ausrüstung angezeigten Reihenfolge)
MRx	Manueller Reset-Eingang
MSPx	Stummschaltung des Sensorpaareingangs
NM Sicherheit	Nicht veränderbarer Sicherheitseingangsknoten der Press Control-Blöcke (nur SCx)
ONx	Ein-Aus-Eingang
OSx	Optischer Sensoreingang
PCMSx	Presse Steuerung Stummschaltung Sensoreingang
PIP	Bauteil in Place-Eingangsknoten der Press Control-Blöcke (nur SCx)
PSx	Schutzeingang Stop
RE	Reset-Freigabe-Eingangsknoten der Latch-Reset-Blöcke und der Sicherheitsausgänge
ROx	Relaiskontakt
RPI	Gewünschtes Paketintervall
RPx	Seilzug-Eingang
RST	Reset-Knoten der SR-Flip-Flop-, RS-Flip-Flop-, Latch-Reset-Blöcke, Press Control-Blöcke und Enabling Device-Blöcke
LAUFEN	Eingangsknoten der Betriebsart Standardbetrieb (RUN) der Press Control Mode Blocks (nur SCx)
SETZEN	Knoten der SR- und RS-Flip-Flop-Bausteine setzen
SMx	Trittschaltereingang
SOx	Sicherheit Ausgang
SQS	Sequentieller Stop-Eingangsknoten der Press Control-Blöcke (nur SCx)
SQSx	Drücken Sie Steuerung SQS (Sequentieller Stopp) Eingang
STATx	Status Ausgabe
TC	Two-Hand-Control-Eingangsknoten der Two-Hand-Control-Blöcke
TCx	Zweihand-Steuerungseingang
TOS	Oberer Hub-Eingangsknoten der Press Control-Blöcke (nur SCx)

⁸ Die Endung ‚x‘ bezeichnet die automatisch zugewiesene Nummer.



9.2 Software-Übersicht

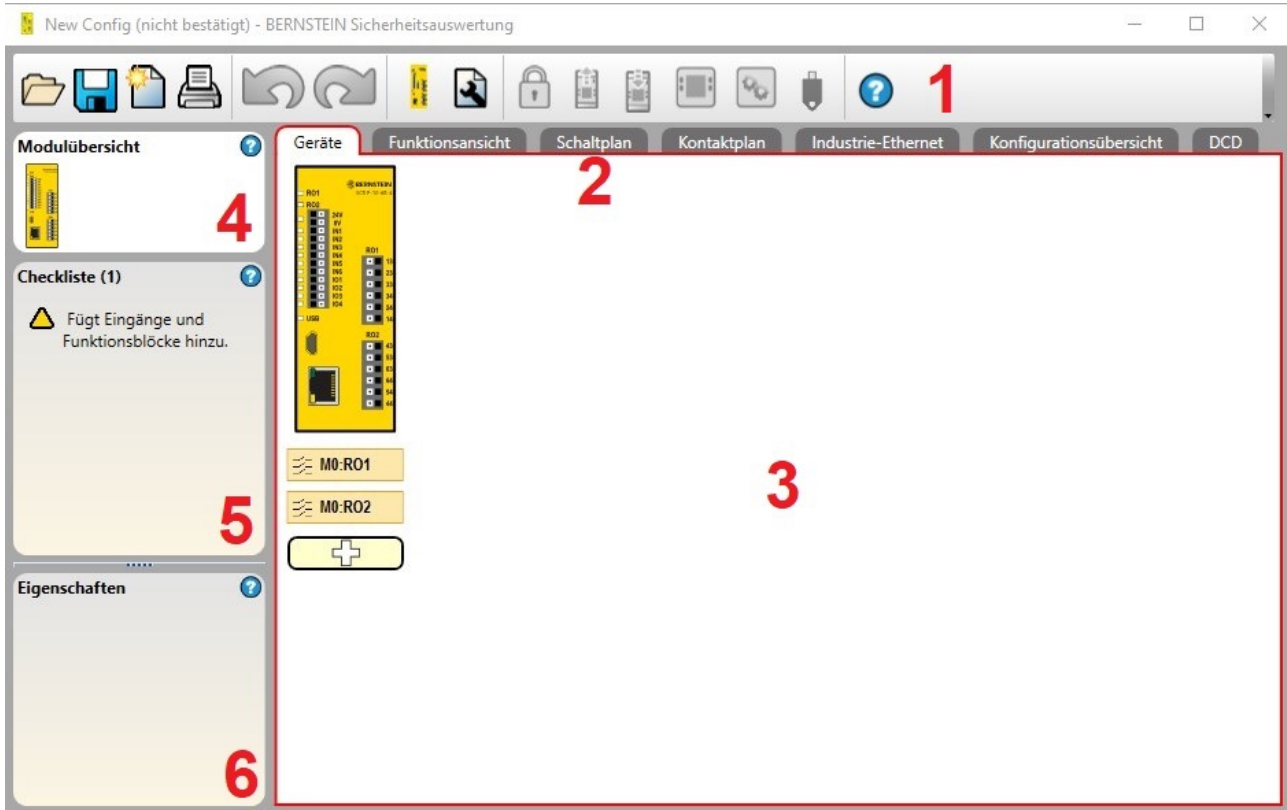


Abbildung 65: Software für die Sicherheitsauswertung von BERNSTEIN

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

(1) Symbolleiste „Navigation“

- | | | | |
|--|---|--|---|
| | Startet ein Neues Projekt | | Liest Daten aus der Sicherheitsauswertung (Upload), wie z.B. Fehlerprotokoll, Konfigurationsdaten, Netzwerkeinstellungen und Geräteinformationen. |
| | Öffnet ein bestehendes Projekt, öffnet eines der Zuletzt bearbeiteten Projekte oder öffnet Beispielprojekte | | 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 | | Öffnet die Hilfe-Optionen.
5. Hilfe: Öffnet die Hilfethemen.
6. Über: Zeigt die Versionsnummer der Software und den Warnhinweis zu den Pflichten des Benutzers. |
| | Zeigt die Netzwerkeinstellungen an und schreibt diese in die Sicherheitsauswertung. | | 7. Versionshinweise: Zeigt die Versionshinweise für alle Softwareversionen an.
8. Symbole: Umschaltung zwischen den Symbolen im US-amerikanischen und europäischen Format. |
| | Öffnet die Projekteinstellungen | | 9. Support-Informationen: Beschreibt, wie Sie bei BERNSTEIN Hilfe anfordern können. |
| | Öffnet den Passwort-Manager | | 10. Sprache: Auswahl der Sprachoptionen für die Software. |



(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 „15.1 Software: Fehlerbehebung“ auf Seite 238 erhalten Sie Informationen zu Problemlösungen im Zusammenhang mit den Funktionen der Software.

9.3 Neues Projekt

Klicken Sie auf **Neues Projekt**, um die gewünschte Steuerung auszuwählen und den Bildschirm **Neues Projekt starten zu öffnen**. Dieser Bildschirm enthält Projektinformationen, die nur bei der erstmaligen Erstellung eines Projekts zur Verfügung stehen und nicht über den Bildschirm **Projekteinstellungen verfügbar sind**.

SCx

Alle Kontrollkästchen sind standardmäßig aktiviert. Die folgenden Optionen sind verfügbar:

Hat Display

Aktivieren Sie dieses Kontrollkästchen, wenn Ihr Steuergerät über ein Display verfügt. Wenn es aktiviert ist, wird ein „d“ nach der „-2“ in der Modellnummer in der Software angezeigt.

Verfügt über Industrial Ethernet


Aktivieren Sie dieses Kontrollkästchen, wenn Ihre Steuerung über Industrial Ethernet verfügt. Wenn dieses Kontrollkästchen aktiviert ist, wird ein „e“ nach der „-2“ in der in der Software angezeigten Modellnummer angezeigt.

SCR P

Automatische Terminal-Optimierung deaktivieren (nur SCR P)

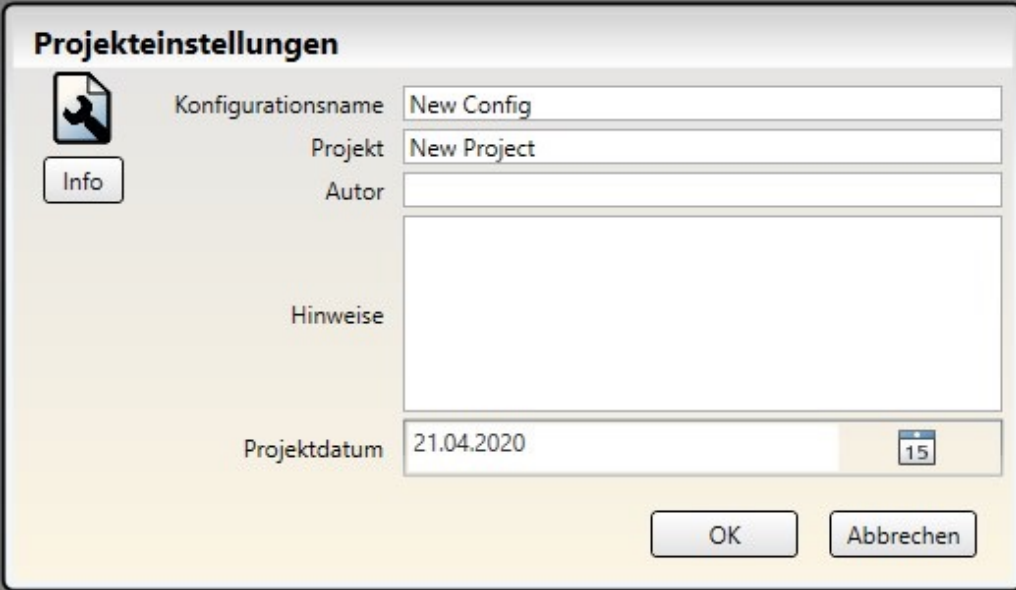
Aktivieren oder deaktivieren Sie die automatische Klemmenoptimierung, die eine Erweiterung der Anzahl der Eingänge über eine externe Klemmenleiste (ETB) ermöglicht.




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



9.4 Projekteinstellungen



Projekteinstellungen

 **Info**

Konfigurationsname

Projekt

Autor

Hinweise


Projektdatum 

Abbildung 66: 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.

9.5 Registerkarte Geräte

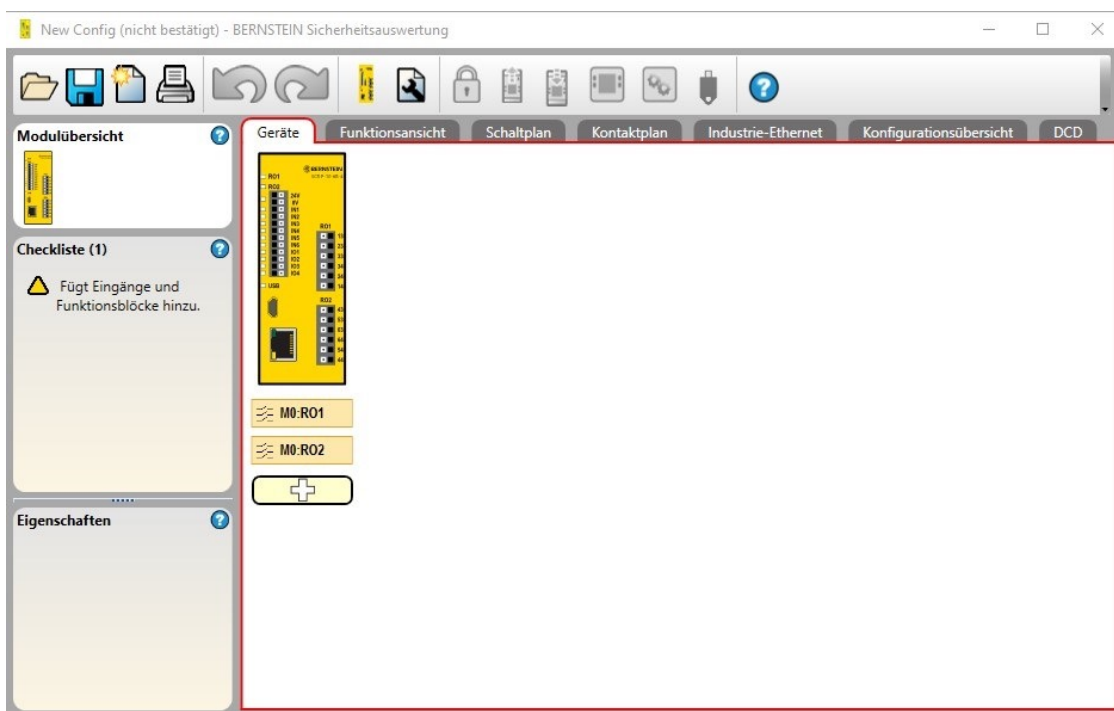


Abbildung 67: : Beispiel: Registerkarte Geräte

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.

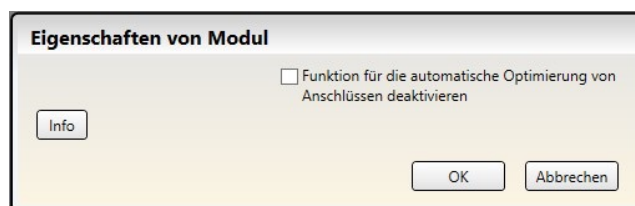


Abbildung 68: Eigenschaften des Moduls SCR P



9.6 Registerkarte Funktionsansicht

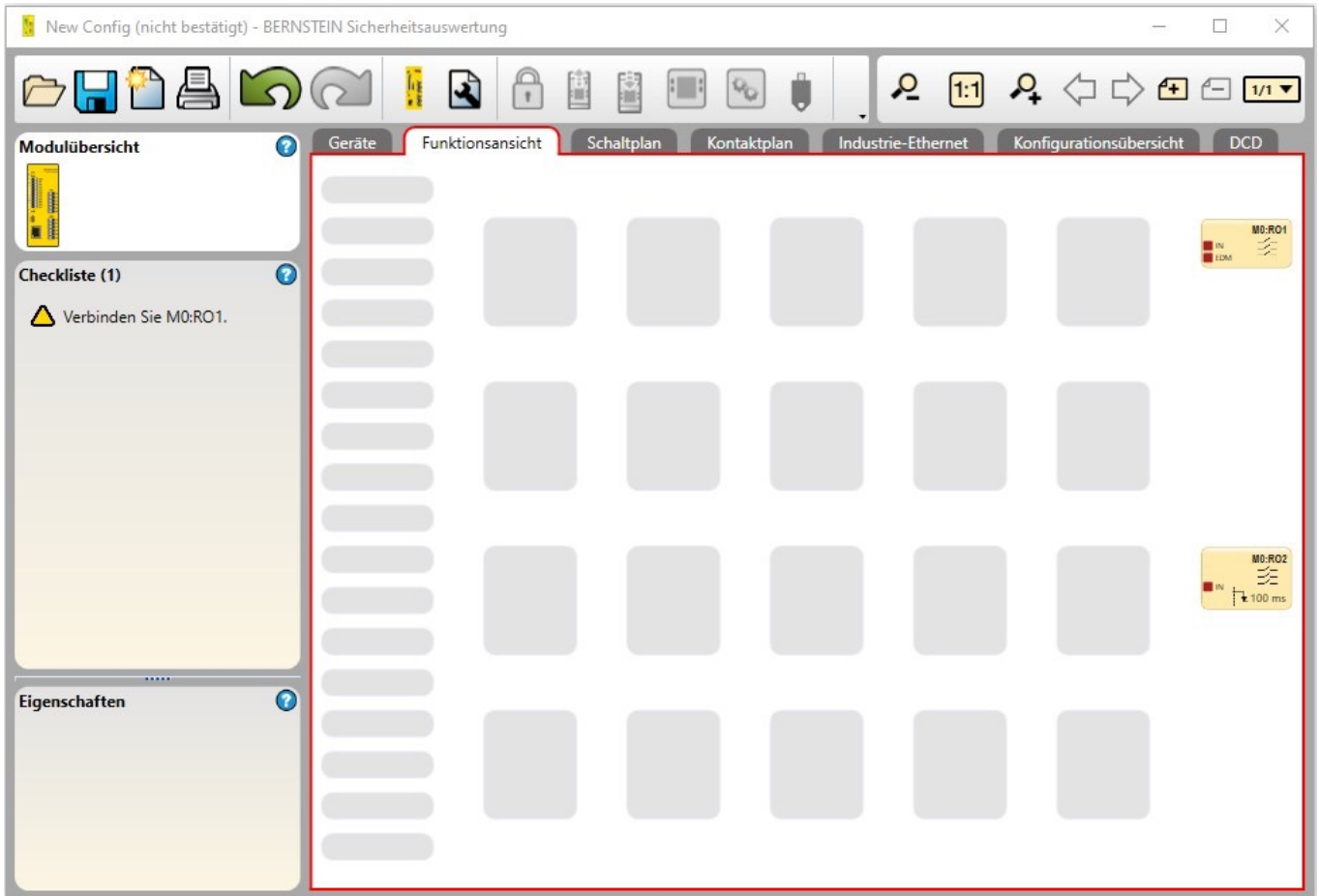


Abbildung 69: Registerkarte Funktionsansicht

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 „13.2 Inbetriebnahmeprüfung“ auf Seite 218

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 75)
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 75)



Abbildung 70: 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 hier-zu 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**.

9.6.1 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 Gefahrensituation 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 Gefahrensituation kann eintreten, wenn ein Stoppsignal an einem Sicherheitseingang unterbrochen wird. Dies kann dazu führen, dass sich ein Sicherheitsausgang einschaltet.

AND



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



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 logischen AND-Beziehung zwischen 2 bis 5 Eingängen.

Der Ausgang ist eingeschaltet, 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 logischen OR-Beziehung zwischen 2 bis 5 Eingängen.

Der Ausgang ist eingeschaltet, wenn alle Eingänge eingeschaltet sind

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

XOR



Der Ausgangswert basiert auf der logischen 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	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	0 (Reset hat Priorität)



9.6.2 Funktionsblöcke

Funktionsblöcke bieten integrierte Funktionen für die meisten gängigen Anwendungen in einem Block. Obwohl es möglich ist, eine Konfiguration ohne Funktionsblöcke zu entwerfen, bietet die Verwendung von Funktionsblöcken erhebliche Effizienz, Benutzerfreundlichkeit und verbesserte Funktionalität

Die meisten Funktionsblöcke erwarten, dass das entsprechende Sicherheitseingabegerät mit ihnen verbunden ist. Die Checkliste auf der linken Seite erzeugt eine Benachrichtigung, wenn die erforderlichen Verbindungen fehlen. Je nach Anwendung können einige Funktionsblöcke mit anderen Funktionsblöcken und/oder Logikblöcken verbunden sein.

Zweikanalige Sicherheitseingangsgeräte haben zwei getrennte Signalleitungen. Bei einigen Geräten sind beide Zweikanalsignale positiv (+24 V DC), wenn sich das Gerät im Run-Zustand befindet. Andere Geräte können eine komplementäre Schaltungsstruktur haben, bei der ein Kanal auf 24 V DC und der andere auf 0 V DC liegt, wenn sich das Gerät im Run-Zustand befindet. In diesem Handbuch wird die Konvention Run-Status/Stop-Status verwendet, anstatt sich auf ein Sicherheitseingabegerät als EIN (24 V DC) oder AUS (0 V DC) zu beziehen.



9.7 Registerkarte Schaltplan

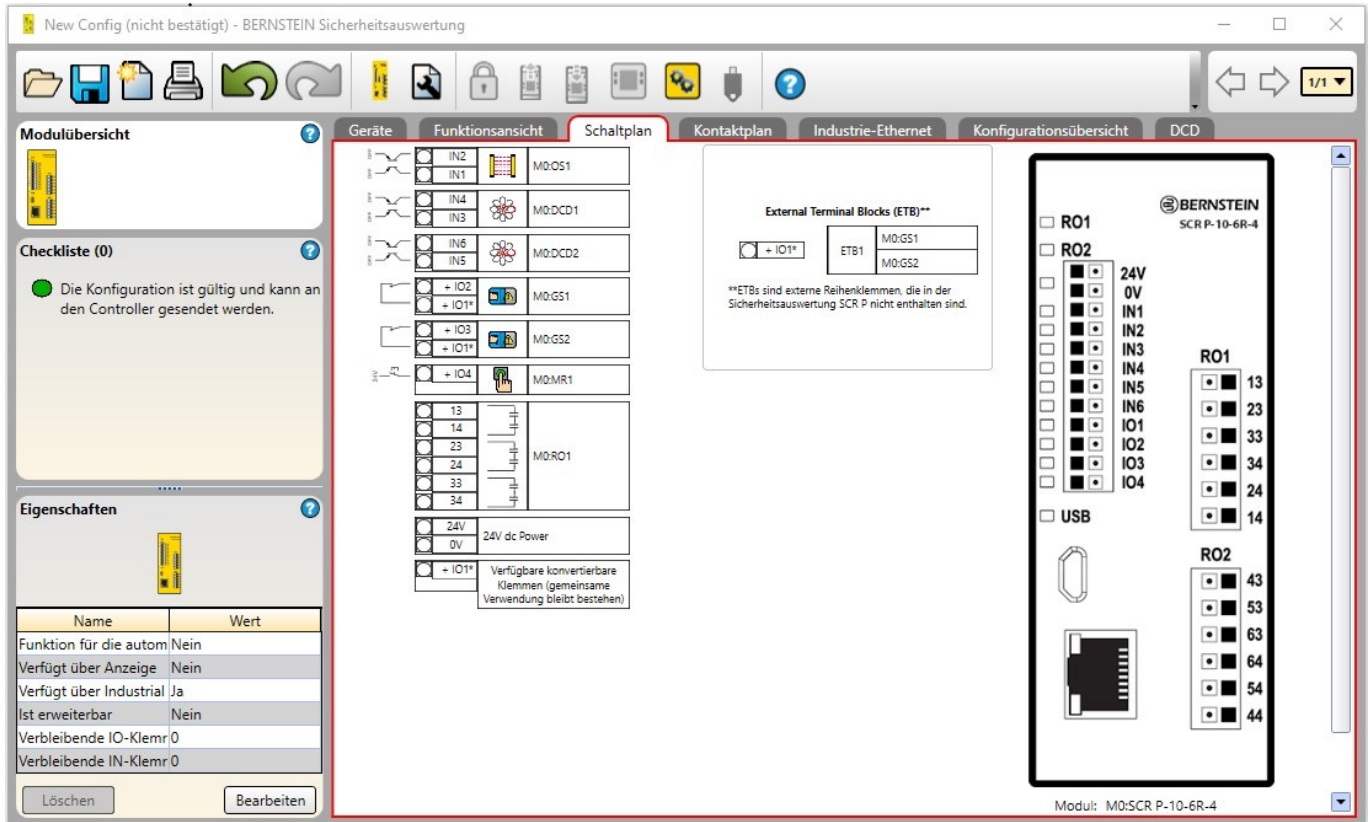


Abbildung 71: Registerkarte Schaltplan: SCR P mit externen Klemmenblöcken

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.



9.8 Registerkarte Kontaktplan

New Config (nicht bestätigt) - BERNSTEIN Sicherheitsauswertung

Geräte Funktionsansicht Schaltplan **Kontaktplan** Industrie-Ethernet Konfigurationsübersicht DCD

Modulübersicht

Checkliste (0)

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

Eigenschaften

Name	Wert
Funktion für die autom	Nein
Verfügt über Anzeige	Nein
Verfügt über Industrial	Ja
Ist erweiterbar	Nein
Verbleibende IO-Klemm	0
Verbleibende IN-Klemm	0

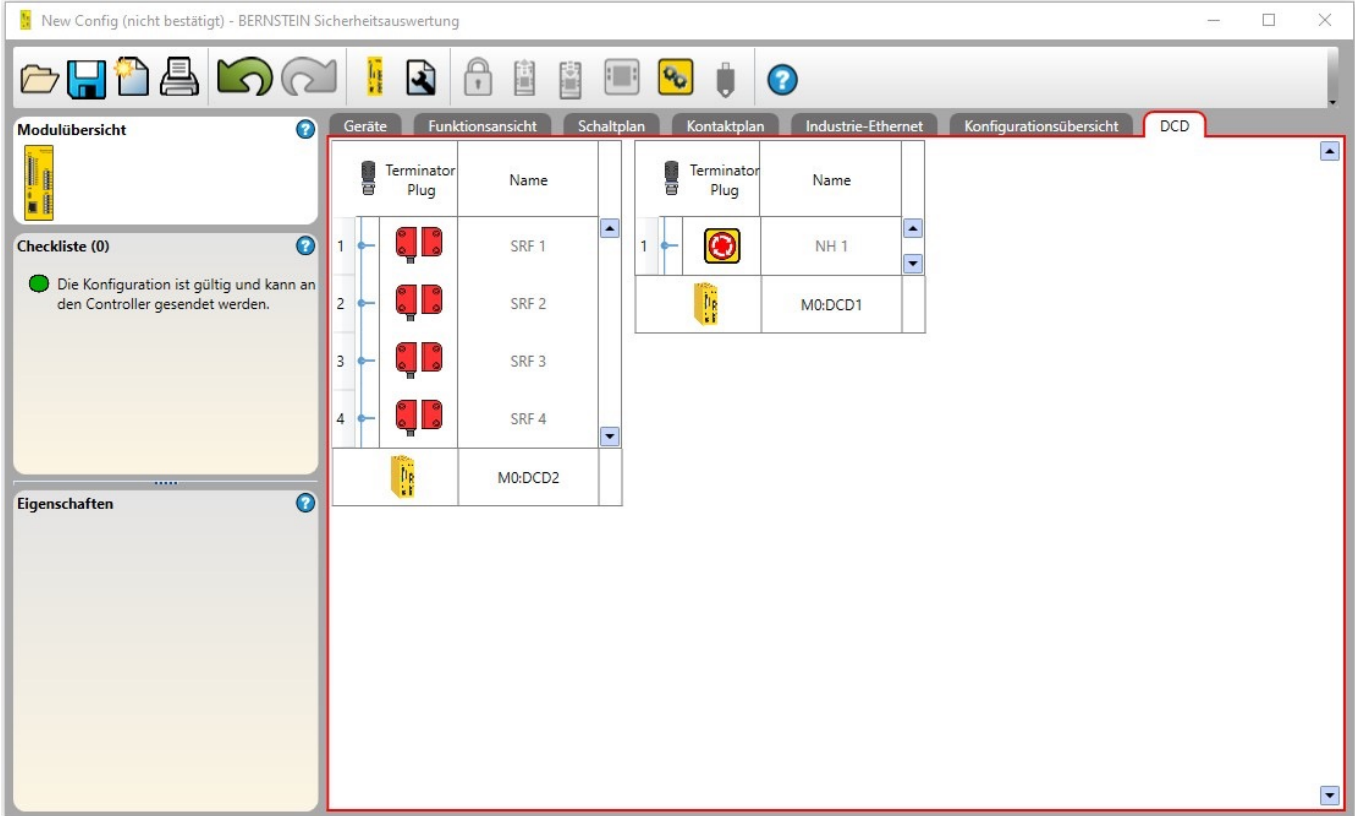
Löschen Bearbeiten

Abbildung 72: Registerkarte Kontaktplan






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



9.9 Registerkarte DCD



The screenshot displays the 'DCD' register configuration in the BERNSTEIN software. The main area is divided into two tables, each with columns for 'Terminator Plug' and 'Name'. The left table lists four SRF devices (SRF 1 to SRF 4) and one M0:DCD2 device. The right table lists one NH 1 device and one M0:DCD1 device. The 'Terminator Plug' column contains icons representing the device type, and the 'Name' column contains the device identifier.

Terminator Plug	Name
	SRF 1
	SRF 2
	SRF 3
	SRF 4
	M0:DCD2



Terminator Plug	Name
	NH 1
	M0:DCD1

Abbildung 73: 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.



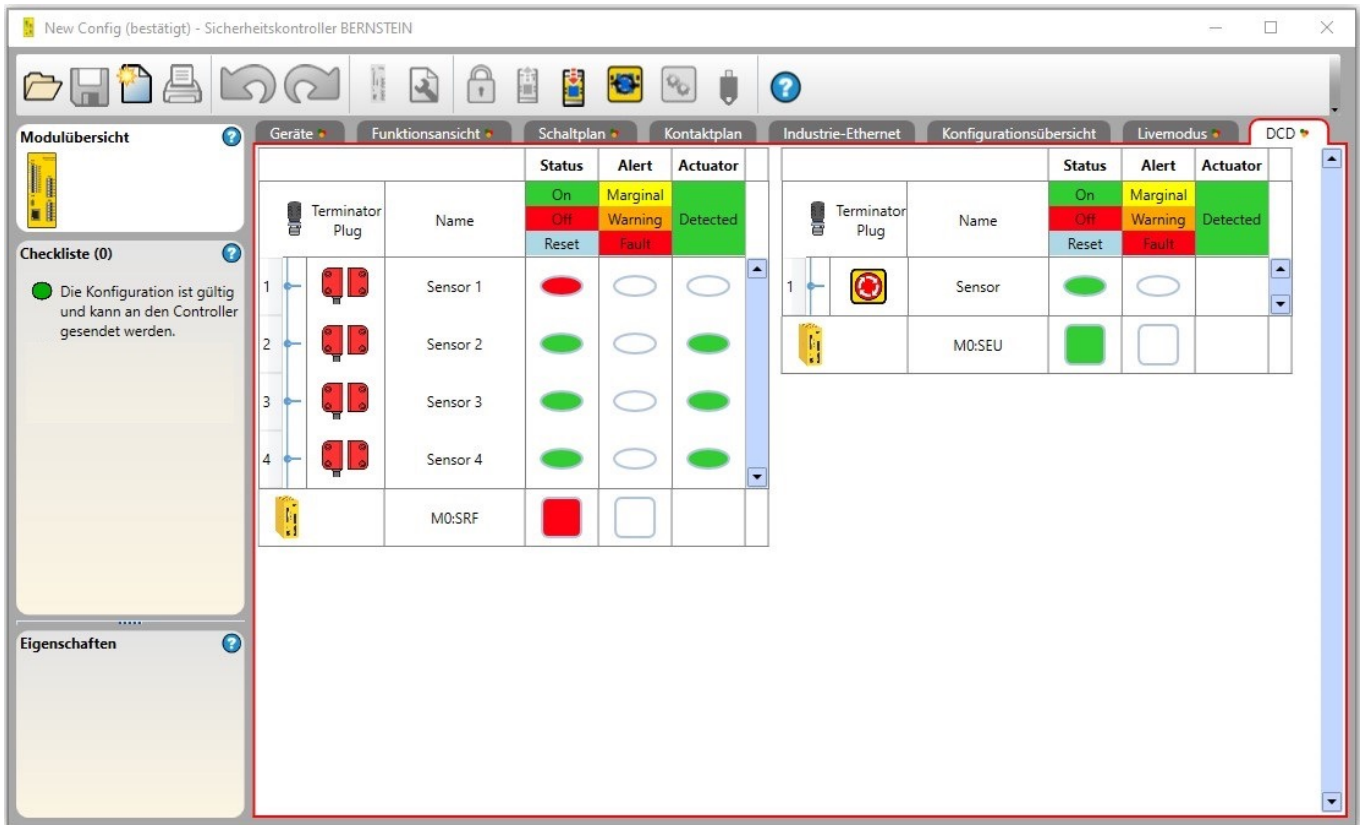


Abbildung 74: Registerkarte DCD im „Live“-Modus mit nicht betätigtem Sensor

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.

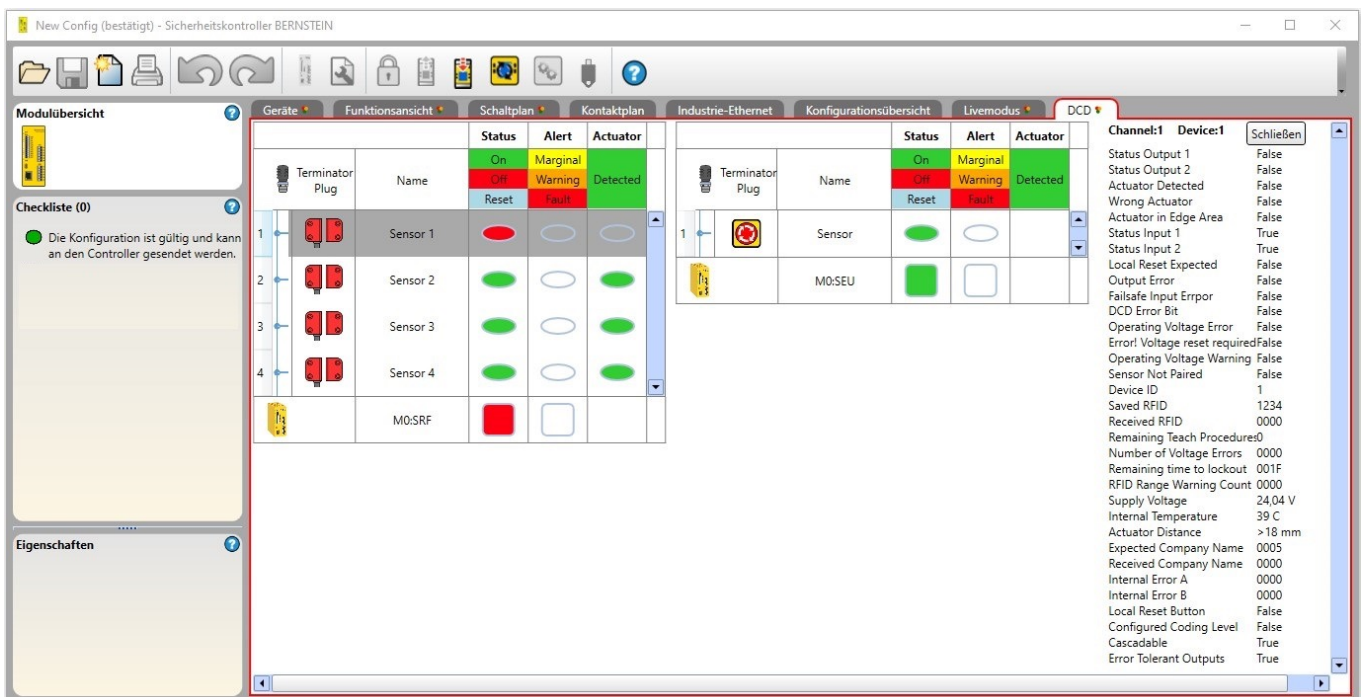
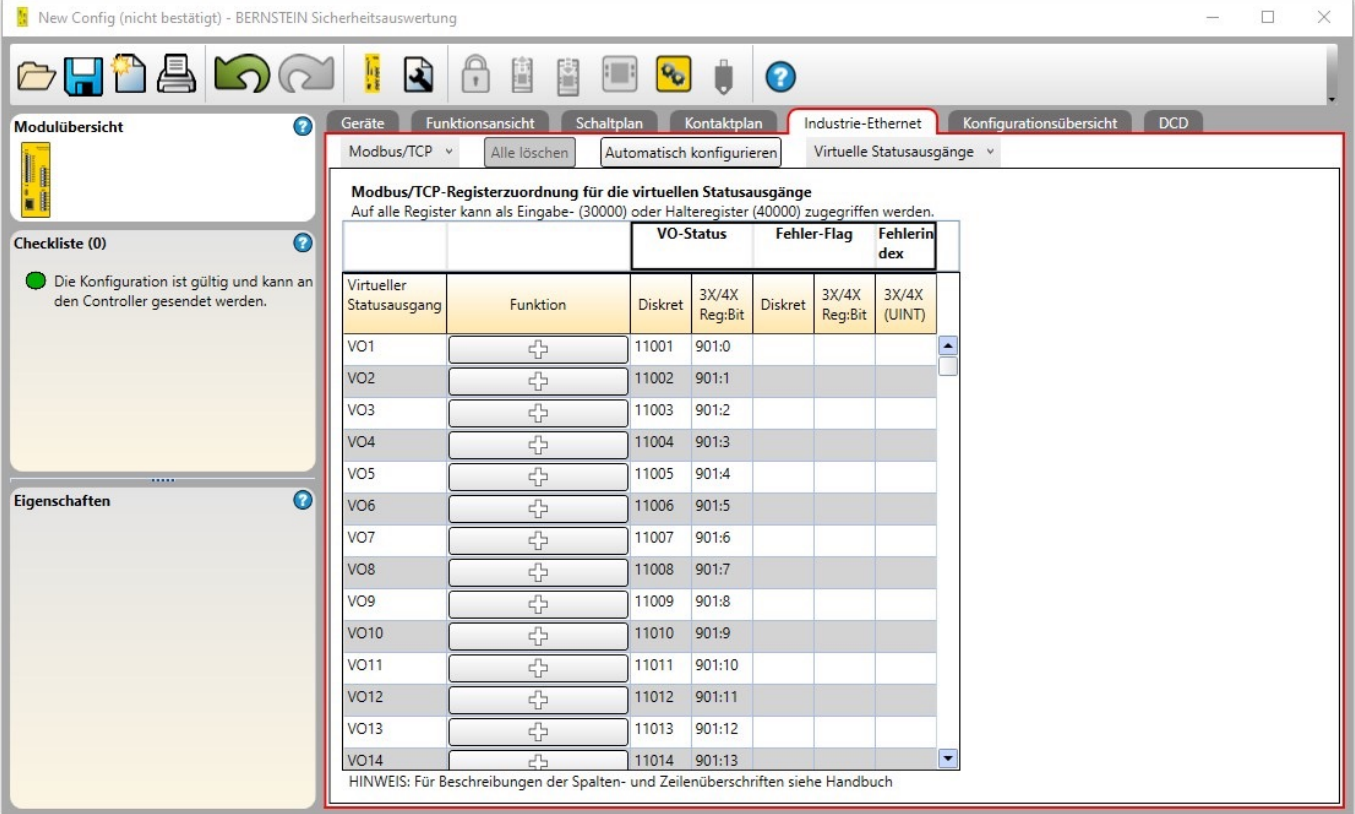


Abbildung 75: Registerkarte DCD im „Live“-Modus mit Diagnose Daten



9.10 Registerkarte Industrial-Ethernet



Modbus/TCP-Registerzuordnung für die virtuellen Statusausgänge
Auf alle Register kann als Eingabe- (30000) oder Halteregeister (40000) zugegriffen werden.

Virtueller Statusausgang	Funktion	VO-Status		Fehler-Flag		Fehlerindex
		Diskret	3X/4X Reg:Bit	Diskret	3X/4X Reg:Bit	
VO1	+	11001	901:0			
VO2	+	11002	901:1			
VO3	+	11003	901:2			
VO4	+	11004	901:3			
VO5	+	11005	901:4			
VO6	+	11006	901:5			
VO7	+	11007	901:6			
VO8	+	11008	901:7			
VO9	+	11009	901:8			
VO10	+	11010	901:9			
VO11	+	11011	901:10			
VO12	+	11012	901:11			
VO13	+	11013	901:12			
VO14	+	11014	901:13			

HINWEIS: Für Beschreibungen der Spalten- und Zeilenüberschriften siehe Handbuch

Abbildung 76: 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 „7.9.1 Signallogik für Statusausgänge“ auf Seite 73 und „7.9.2 Statusausgangsfunktion“ auf Seite 74 für detaillierte Informationen.) Die folgenden Industrial-Ethernet-Protokolle können ausgewählt und verwendet werden: PROFINET, Modbus/TCP, Ethernet/IP-Eingangsguppen, Ethernet/IP-explizite-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 „9.10.1.1 Netzwerkeinstellungen: Modbus/TCP, Ethernet/IP, PCCC “ auf

Seite 109 oder „9.10.1.2 Netzwerkeinstellungen: PROFINET “ auf Seite 110).

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.



9.10.1 Netzwerkeinstellungen

9.10.1.1 Netzwerkeinstellungen: Modbus/TCP, Ethernet/IP, PCCC

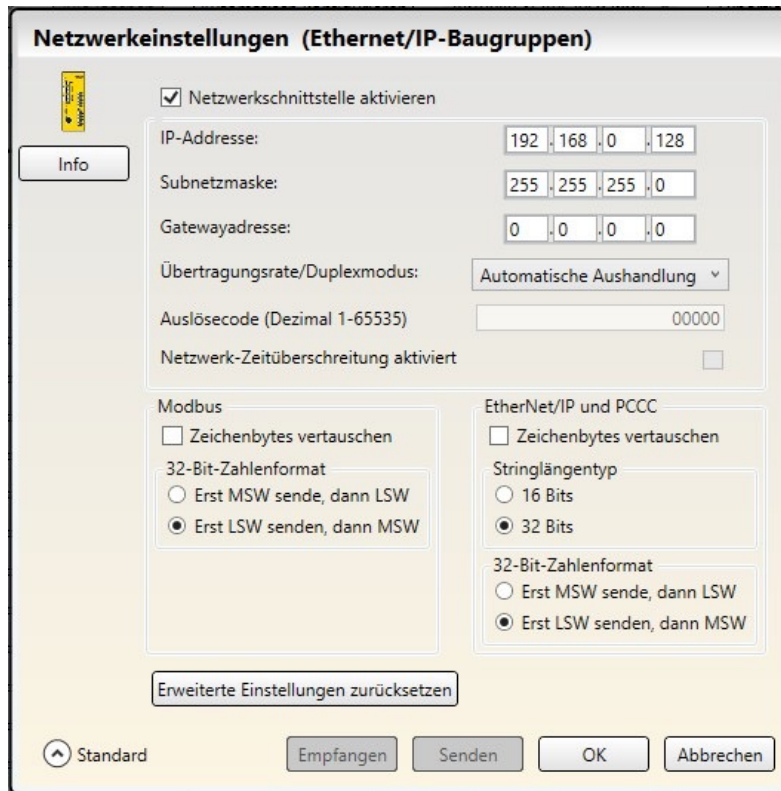


Abbildung 77: Netzwerkeinstellungen

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.


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

Die Option **Erweitert** ermöglicht die weitere Konfiguration der Modbus/TCP- und Ethernet/IP-Einstellungen, wie zum Beispiel „Zeichenbytes vertauschen“, „MSW- und LSW-Sendeprezedenz“ 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.



9.10.1.2 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

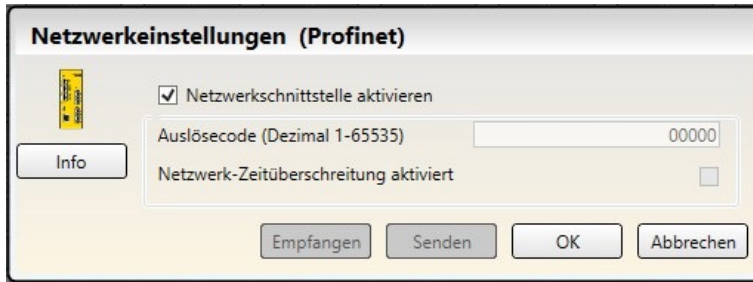


Abbildung 78: Netzwerkeinstellungen – PROFINET

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.

9.10.2 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 79: 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 DCD	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 80: 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 (Statusausgänge).

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).

9.10.3 Ethernet/IP-Gruppenobjekte



Anmerkung: Die EDS-Datei steht unter dem folgenden Link zum Download zur Verfügung:
www.bernstein.eu

Einganggruppenobjekte (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.



9.11 Registerkarte Konfigurationsübersicht

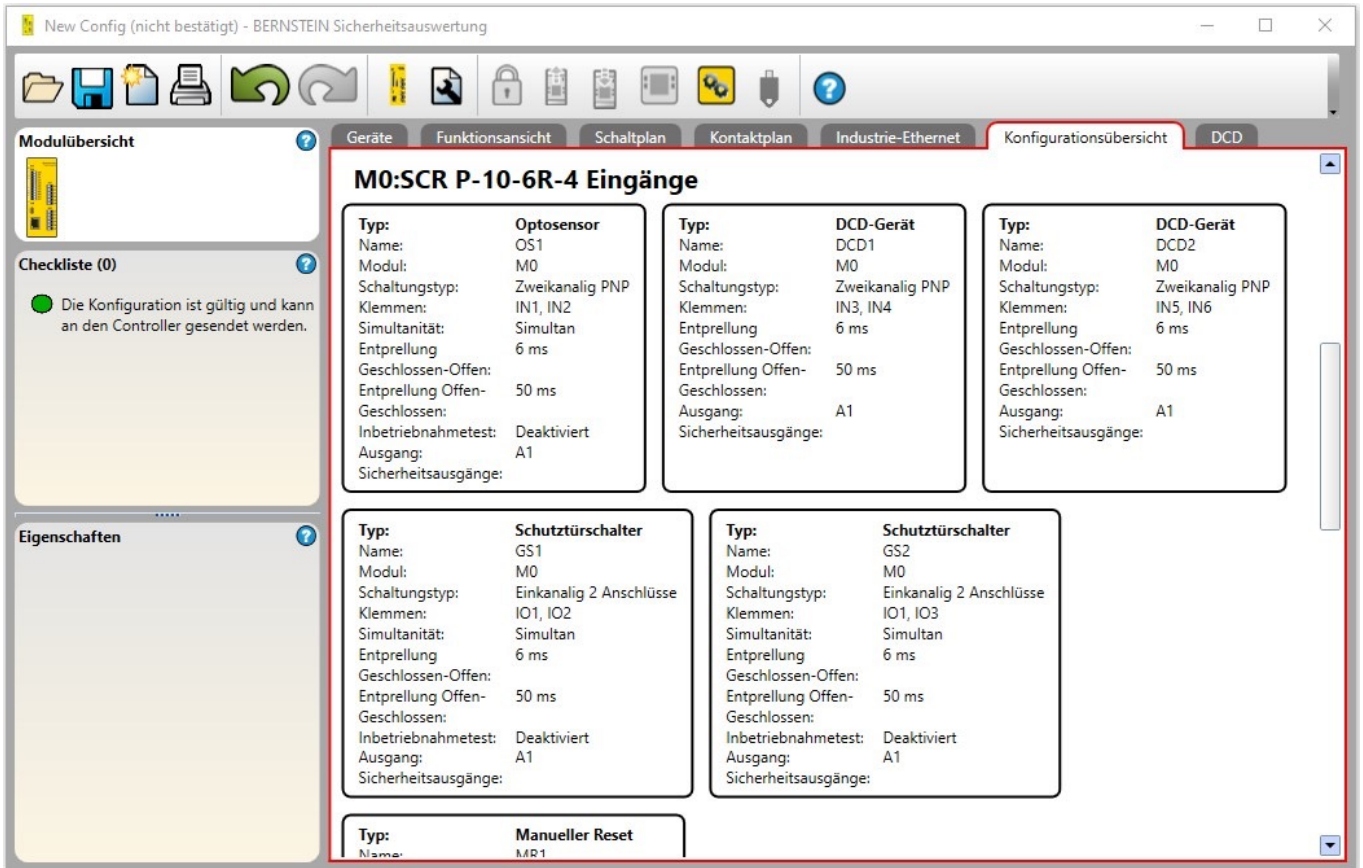


Abbildung 81: Registerkarte Konfigurationsübersicht

Auf der Registerkarte **Konfigurationsübersicht** werden die detaillierten Informationen über alle konfigurierten Eingänge, Funktions- und Logikblöcke, Sicherheitsausgänge, Statusausgänge und die zugehörigen Ansprechzeiten in einem Textformat angezeigt.



9.12 Druckoptionen

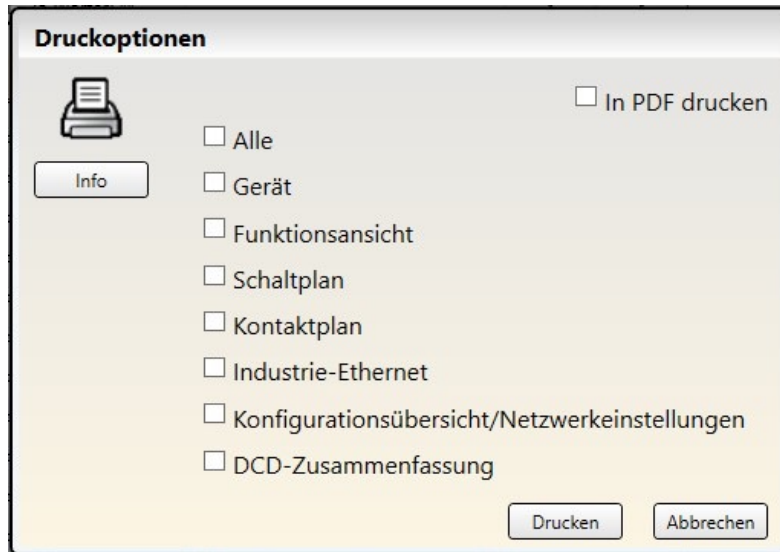


Abbildung 82: Druckoptionen



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.



9.13 SCx Passwort-Manager



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

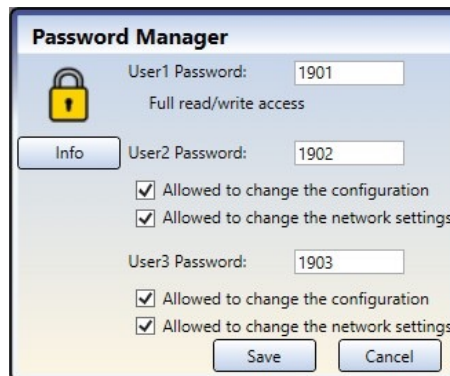



Abbildung 83: Passwort-Manager

Klicken Sie auf  **Passwort Manager** in der Software-Symboleiste, um die Zugriffsrechte für die Konfiguration zu bearbeiten. Die Sicherheitssteuerung speichert bis zu drei Benutzerkennwörter, um verschiedene Zugriffsebenen auf die Konfigurationseinstellungen zu verwalten. Das Passwort für Benutzer1 bietet vollen Lese-/Schreibzugriff und die Möglichkeit, Zugriffsebenen für Benutzer2 und Benutzer3 festzulegen (Benutzernamen können nicht geändert werden). Grundlegende Informationen, wie z. B. Netzwerkeinstellungen, Schaltpläne und Diagnoseinformationen, sind auch ohne Passwort zugänglich. Eine auf einem PC oder einem SCR P-FPS-Laufwerk gespeicherte Konfiguration ist nicht passwortgeschützt.

Benutzer2 oder Benutzer3 können die Konfiguration in die Sicherheitssteuerung schreiben, wenn die **Änderung der Konfiguration** erlaubt ist. Sie können die Netzwerkeinstellungen ändern, wenn die Option Erlaubt, **die Netzwerkeinstellungen zu ändern aktiviert ist**. Bei Softwareversion 4.1 oder früher ist die Option Konfiguration anzeigen für Benutzer2 und Benutzer3 verfügbar und kann aktiviert werden, wenn **Passwort zum Anzeigen der Konfiguration** für Benutzer1 **erforderlich** aktiviert ist. Die jeweiligen Passwörter sind erforderlich.

Klicken Sie auf **Speichern**, um die Passwortinformationen für die aktuelle Konfiguration in der Software zu übernehmen und sie in die Sicherheitssteuerung 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 SCx auf die Werkseinstellungen zurücksetzen.

9.14 SCR P 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 84: 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 Zugriffs-ebenen 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.

9.15 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.



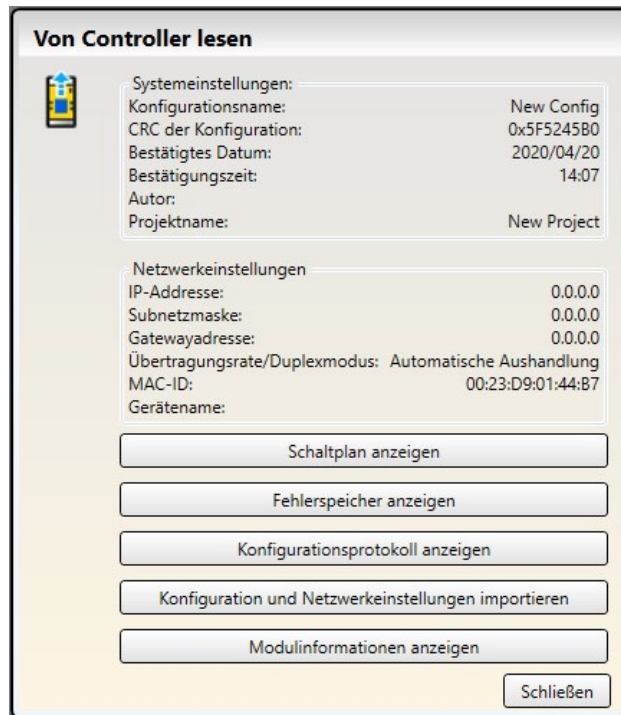
Von der Auswertung lesen ist verfügbar, wenn eine Sicherheitsauswertung über USB an den PC angeschlossen ist.

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
- Übertragungs-rate/Duplexmodus
- MAC-ID





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.



9.16 Livemodus



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

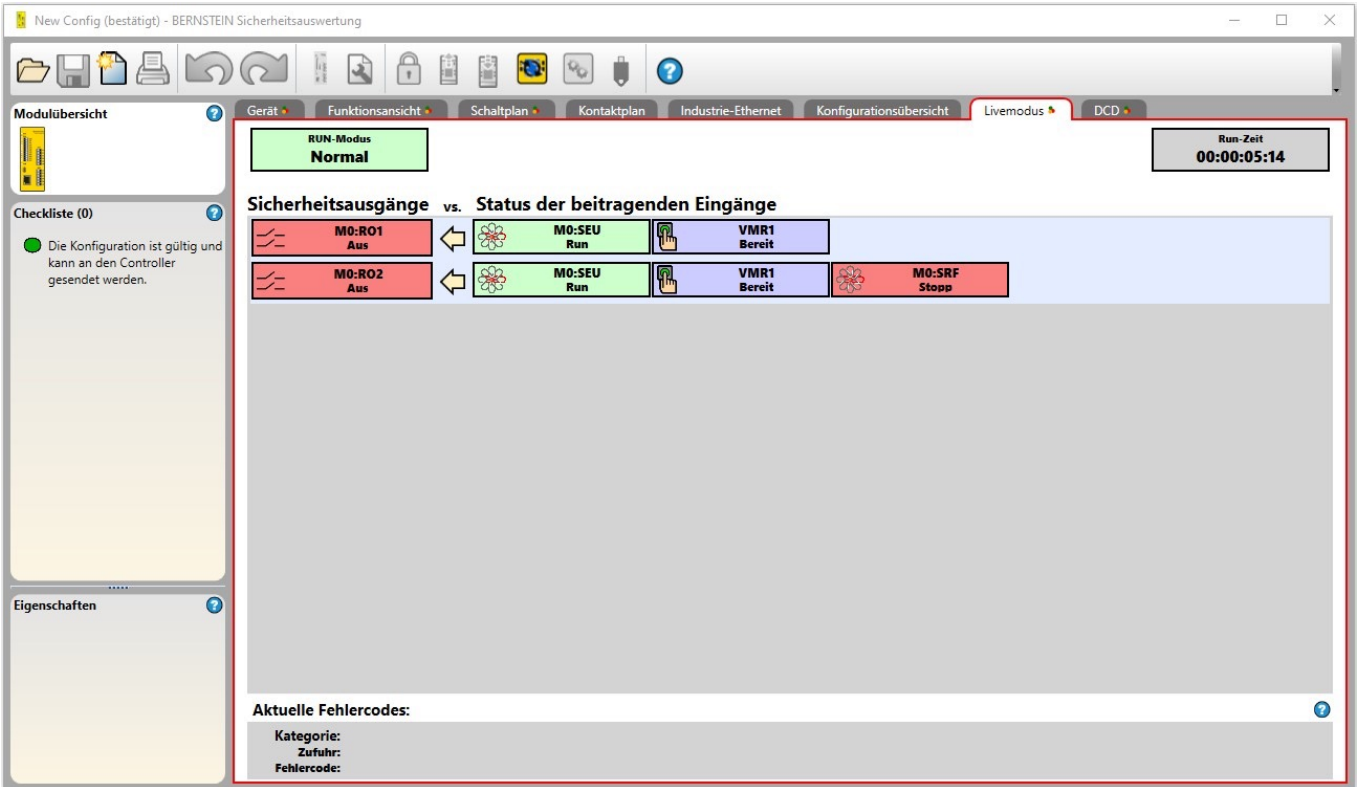


Abbildung 85: Laufzeit – Registerkarte Livemodus

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 ei-nen Fehlercode (siehe „15.6 SCR P-Fehlercode-Tabelle“ auf Seite 249 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.



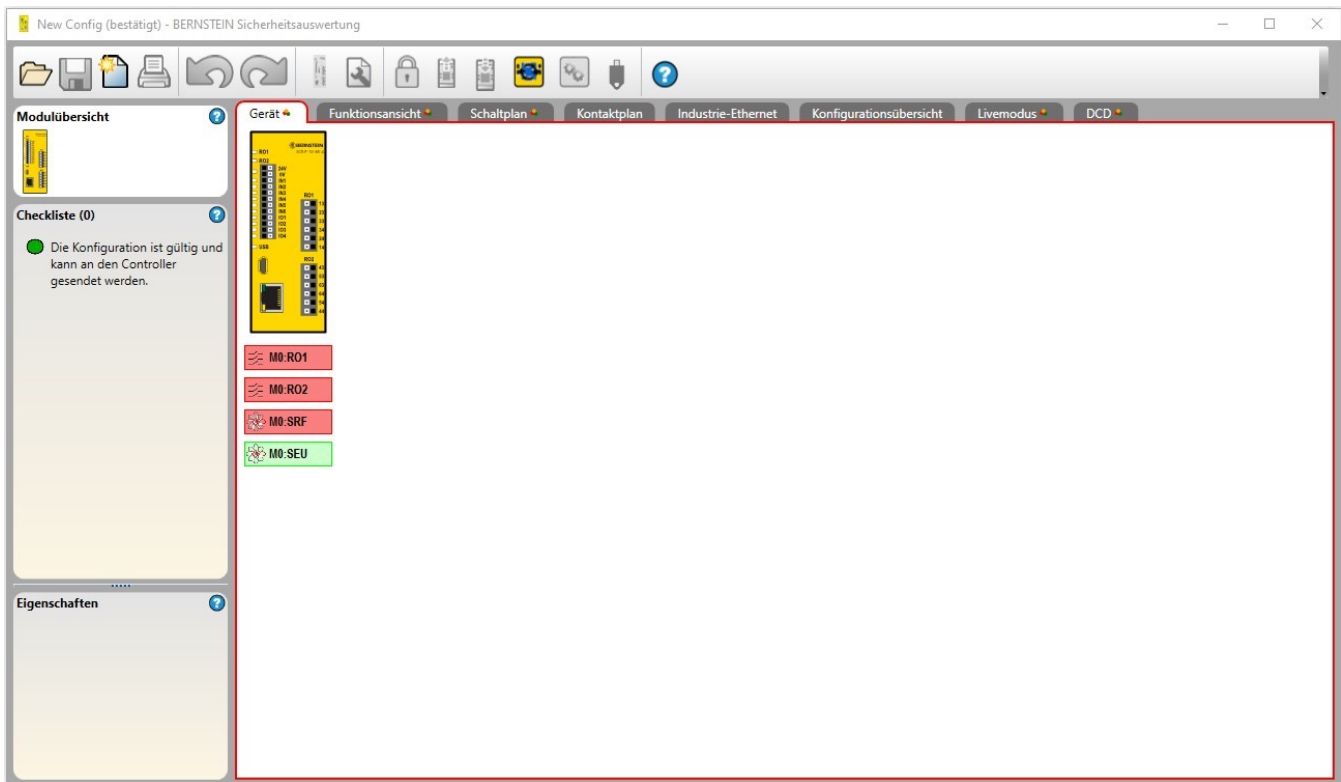


Abbildung 86: Registerkarte Geräte

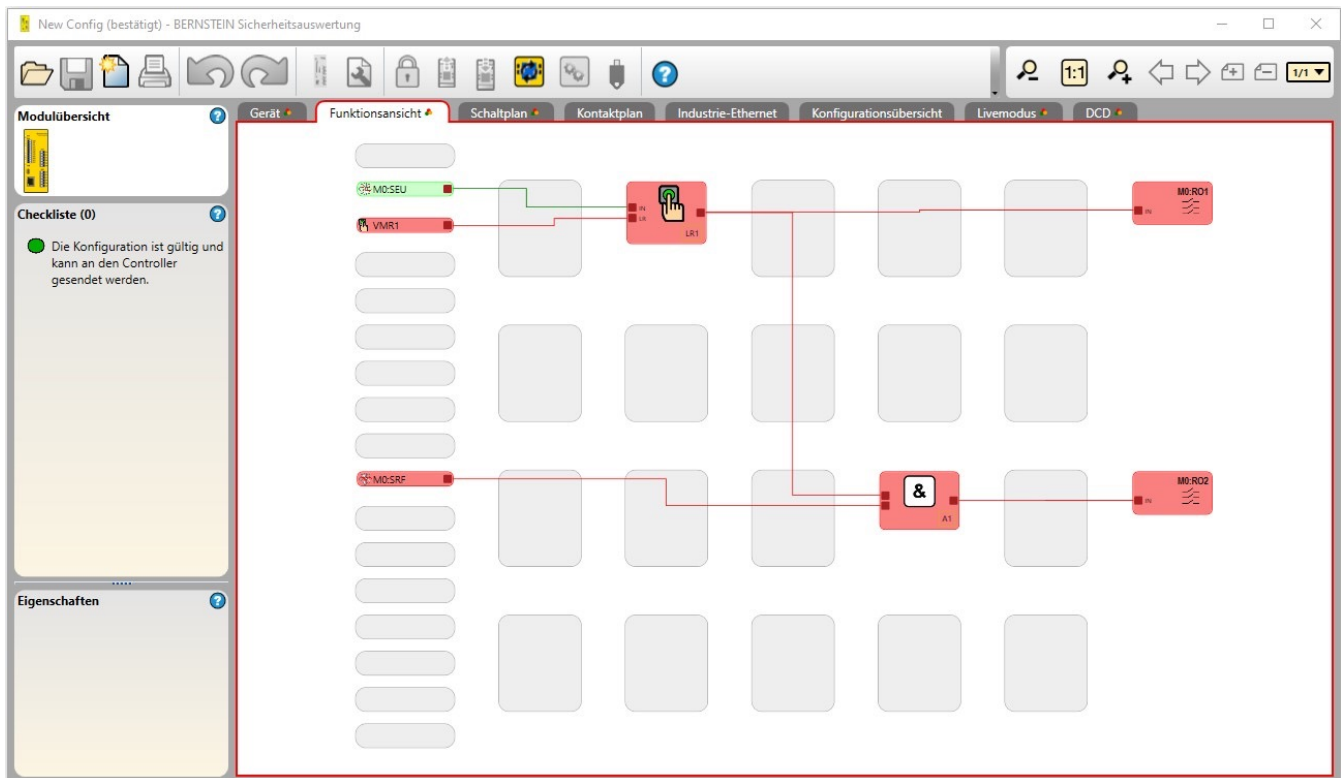


Abbildung 87: Laufzeit – Registerkarte Funktionsansicht



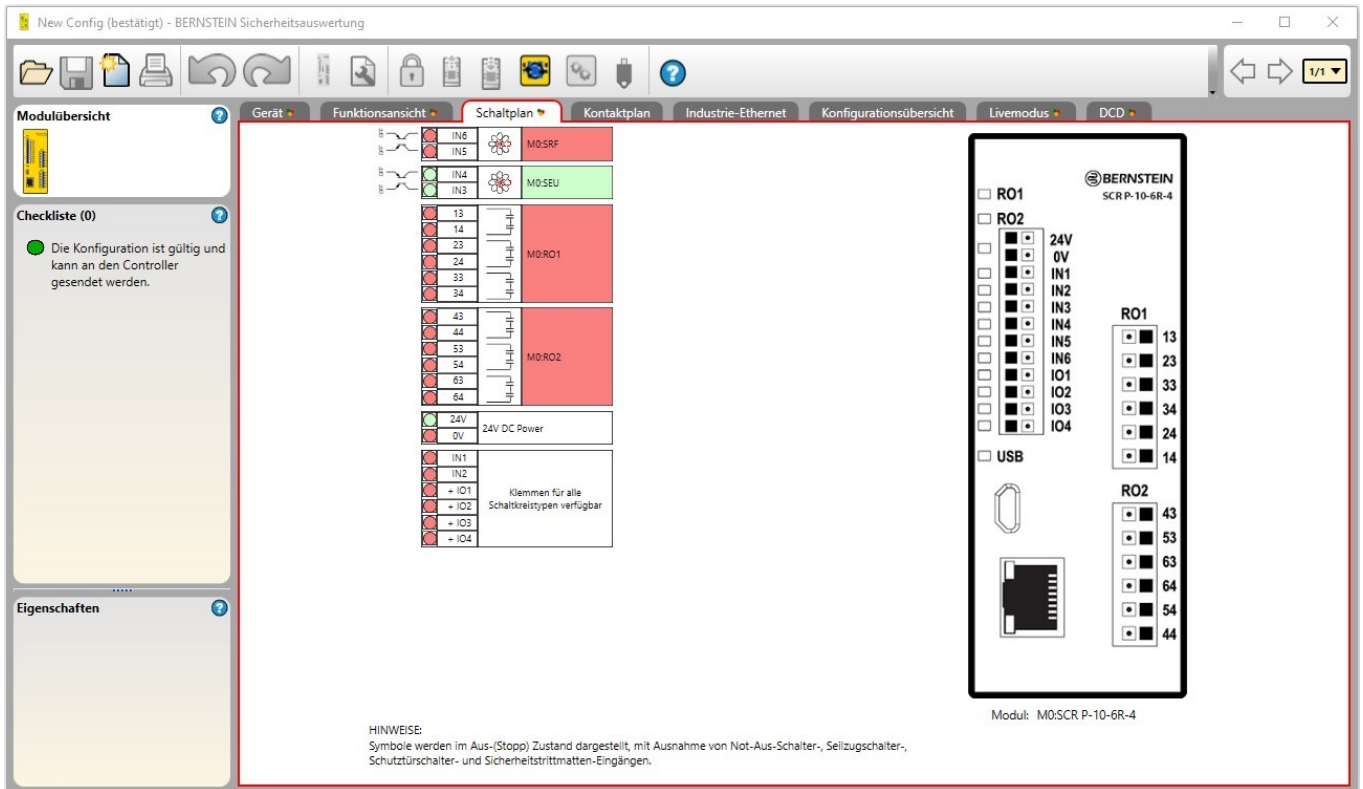


Abbildung 88: Laufzeit – Registerkarte Schaltplan

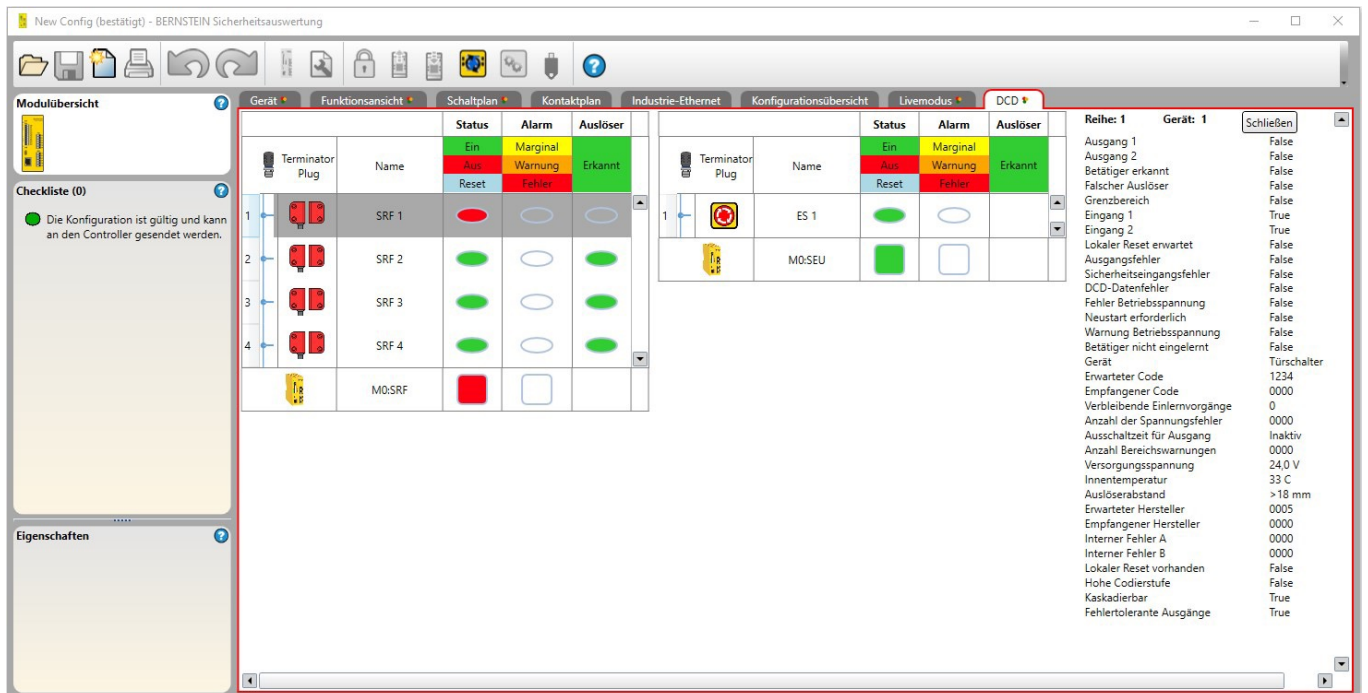
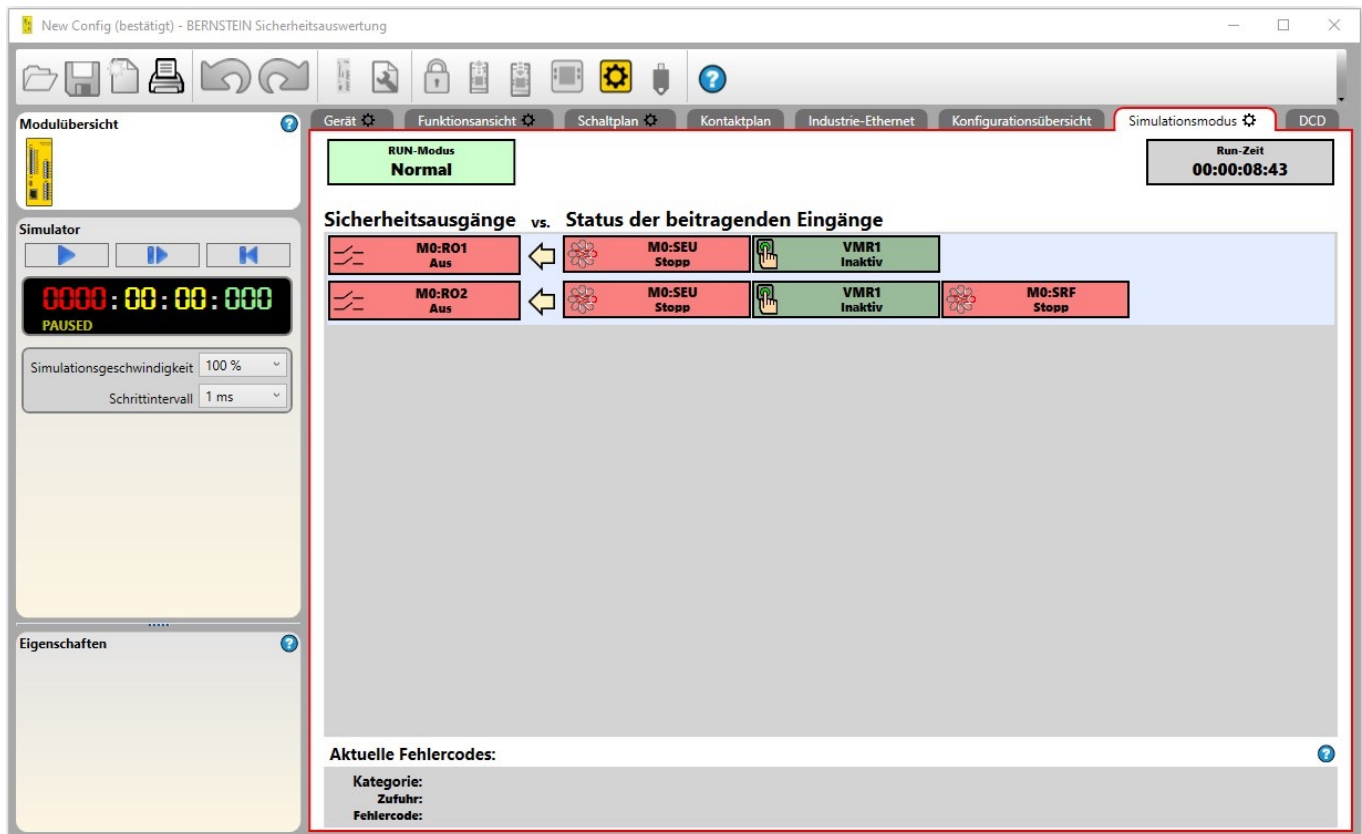




Abbildung 89: Laufzeit – Registerkarte DCD





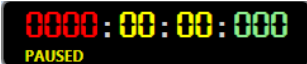


9.17 Simulationsmodus



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 %
- 10%
- 100 % (Standardgeschwindigkeit)
- 500 %
- 2.000 %



Schrittintervall: Legt fest, um welches Zeitintervall die Einzelschritt-Schaltfläche vorrückt, wenn sie betätigt wird. Die Größe des Intervalls richtet sich nach der Größe der Konfiguration.

Wählen Sie **Wiedergabe**, um die Simulation zu starten. Der Zeitgeber läuft und die sich drehenden Zahnräder zeigen an, dass die Simulation läuft. Die Registerkarten **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 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.

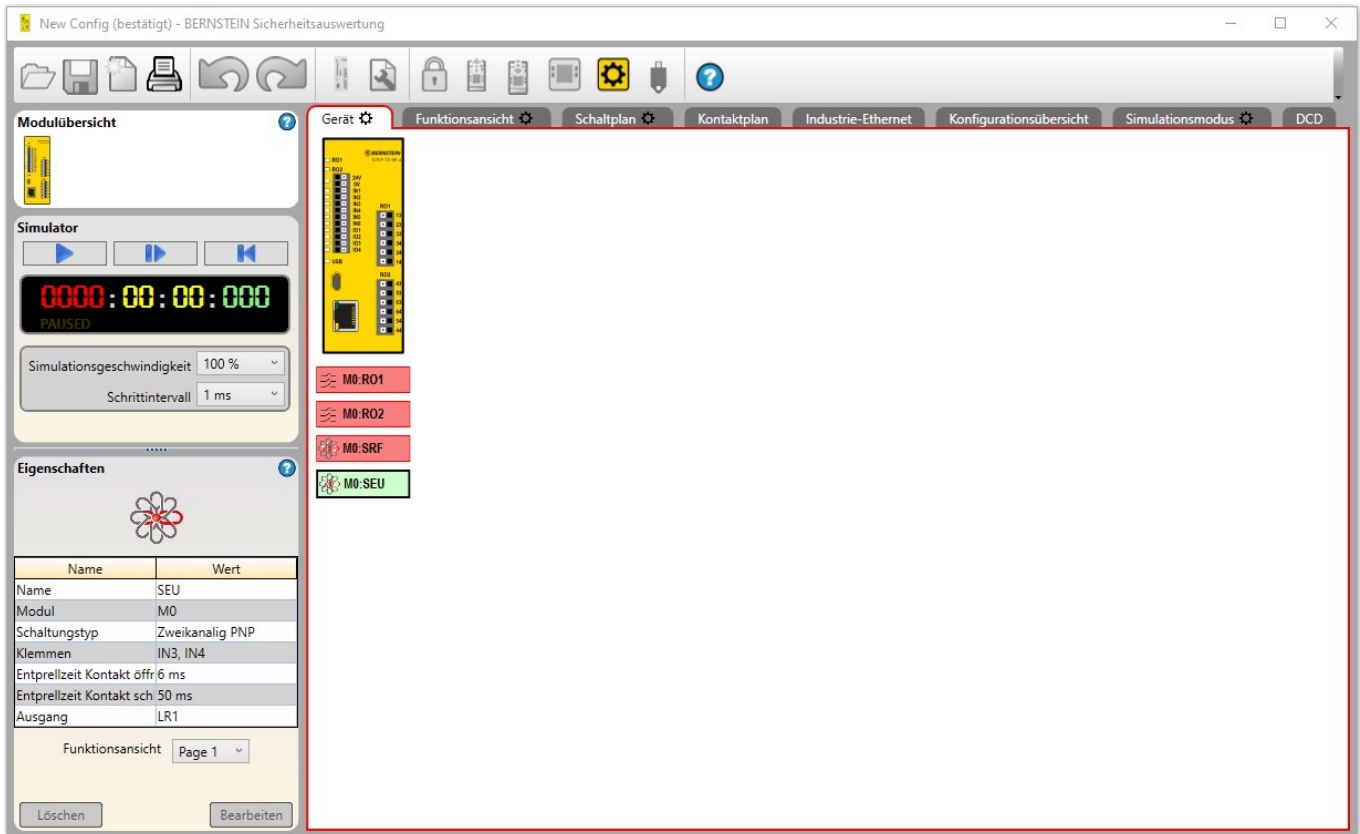


Abbildung 90: Simulationsmodus: Registerkarte Geräte



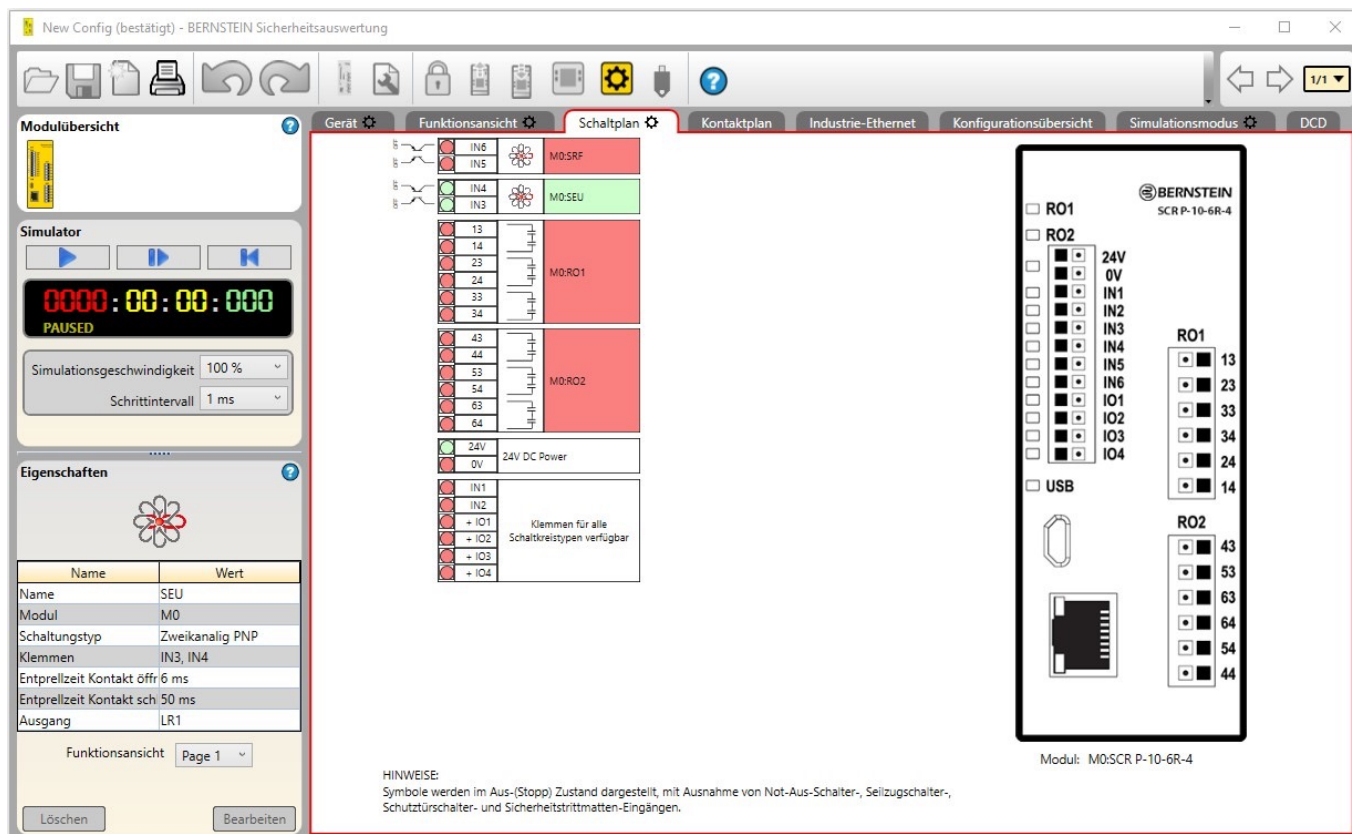


Abbildung 91: Simulationsmodus: Registerkarte Schaltplan



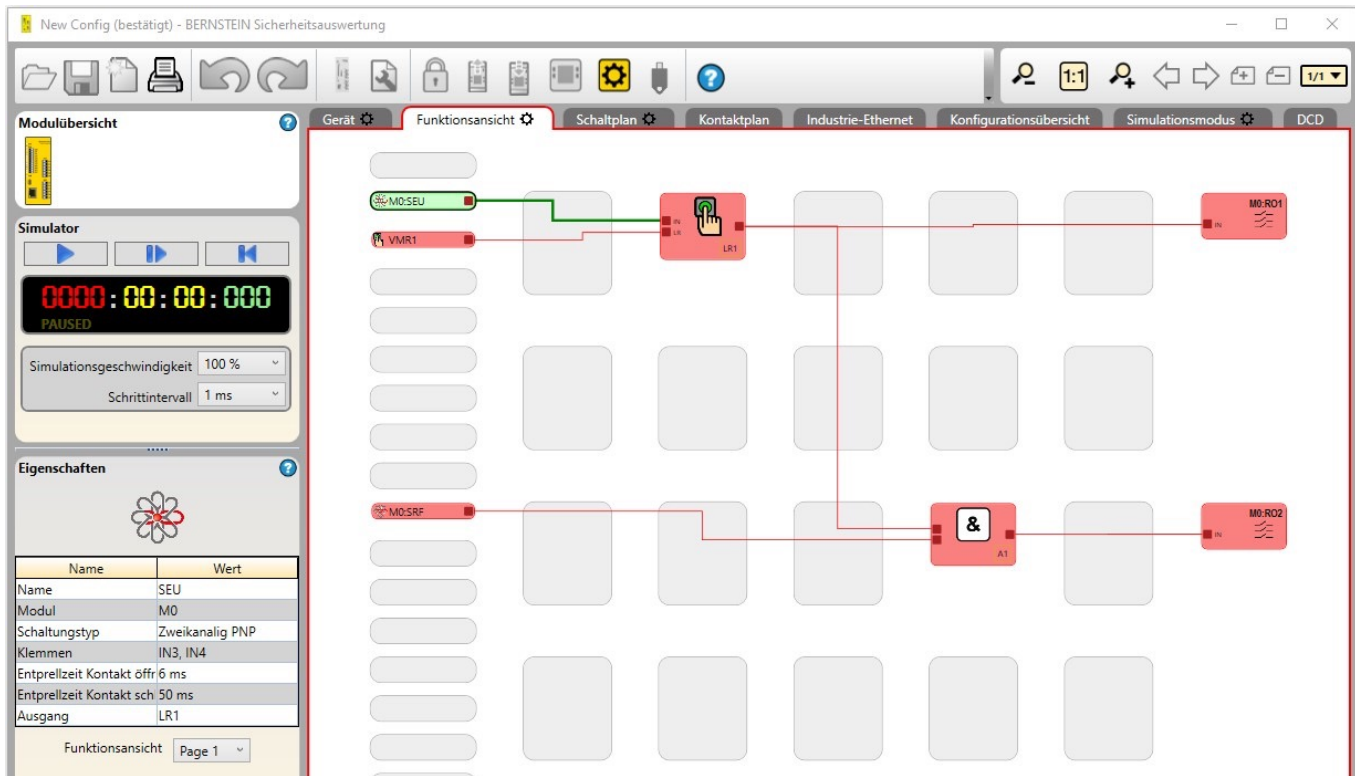


Abbildung 92: Simulationsmodus: Registerkarte Funktionsansicht

9.17.1 Aktionszeitsteuerungsmodus

Im Simulationsmodus und auf der Registerkarte **Funktionsansicht** werden bestimmte Elemente, die sich in Aktionsverzögerungsmodi befinden, lilafarben angezeigt. Die Statusleiste zeigt den Countdown des mit dem Element verbundenen Zeitgebers an.

Die folgenden Abbildungen zeigen die verschiedenen Elementzustände an:

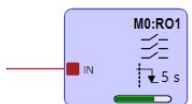


Abbildung 93: Sicherheitsausgang im Modus für zeitgesteuerte Ausschaltverzögerung

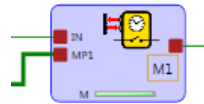


Abbildung 94: Muting-Block im Modus für zeitgesteuertes Muting



Abbildung 95: Überbrückungsblock im Modus für zeitgesteuerte Überbrückung

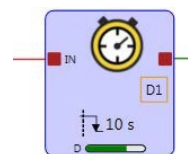


Abbildung 96: Verzögerungsblock



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



9.18 Referenzsignale



Wichtig: Anzeige für Muting-Status

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 128 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.

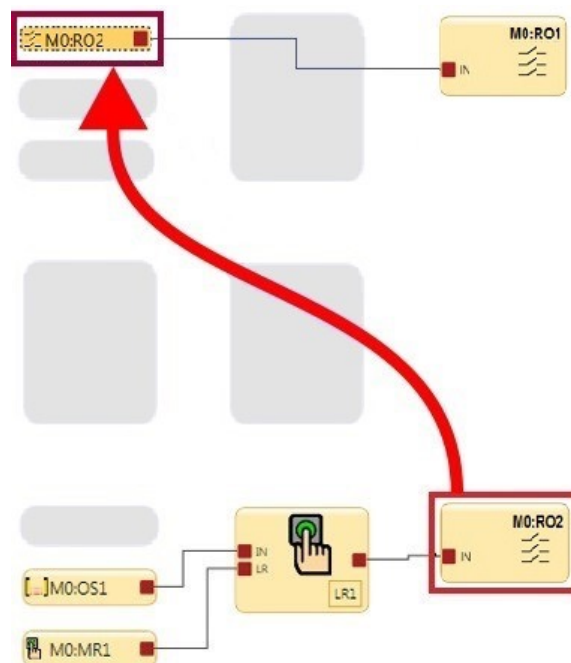


Abbildung 97: Von einem anderen Sicherheitsausgang gesteuerter Sicherheitsausgang



10. 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 Ausgang schaltet sich aus, wenn beide Eingänge (IN und BP) eingeschaltet sind deaktiviert ist). Der Ausgang des zugehörigen Überbrückungsblocks schaltet sich aus, wenn der Überbrückungs-Zeitgeber abläuft.

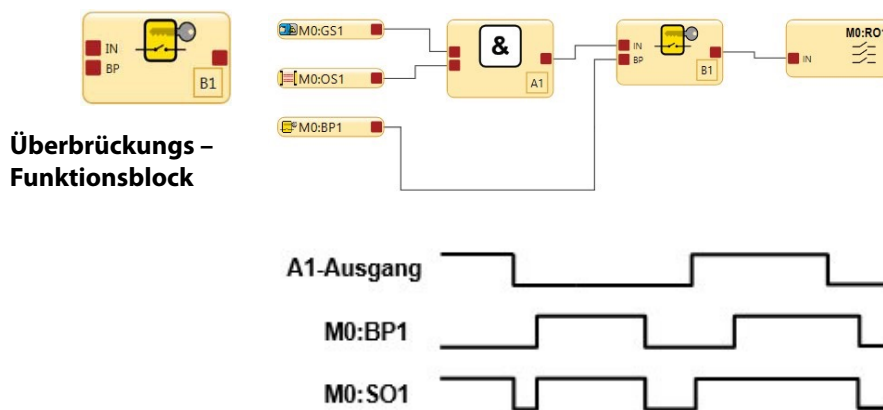


Abbildung 98: Zeitdiagramm: Überbrückungsblock

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.

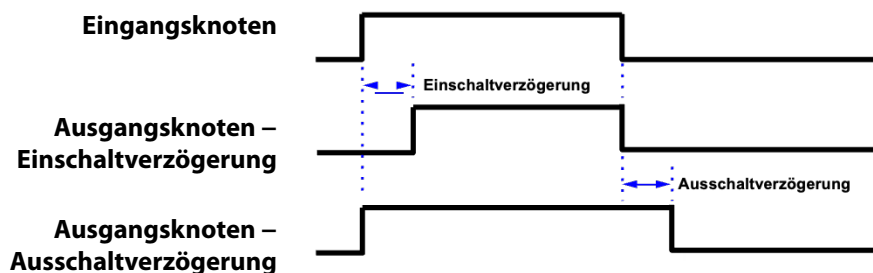


Abbildung 99: Zeitdiagramm für Verzögerungsblock



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

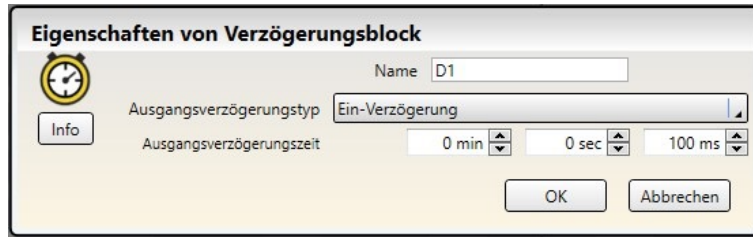


Abbildung 100: Verzögerungsblock-Eigenschaften

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.).



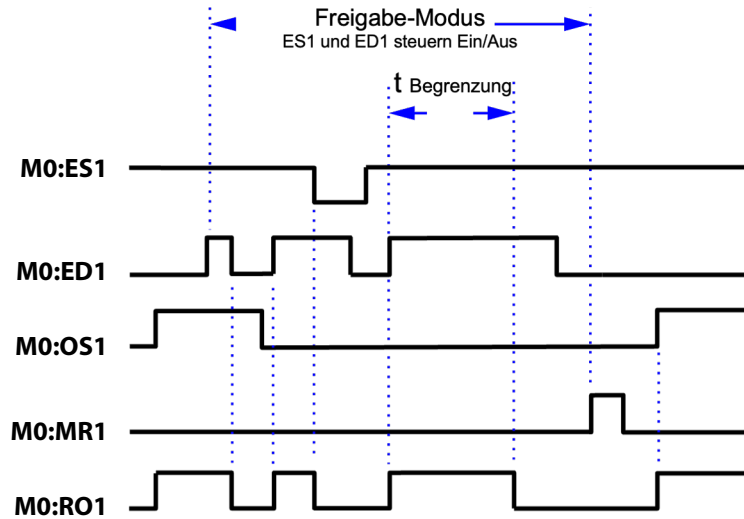
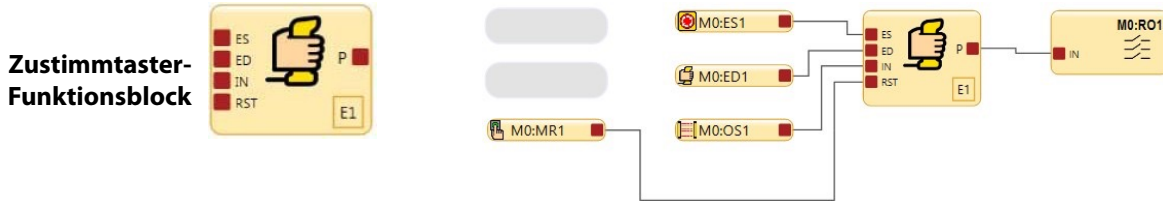


Abbildung 101: Zeitdiagramm: Zustimmtaster, einfache Konfiguration

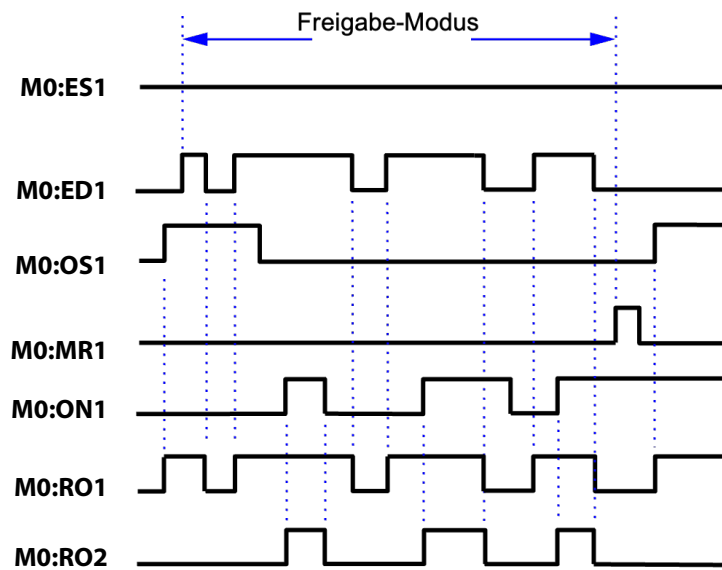


Abbildung 102: Zeitdiagramm: Zustimmtaster

1-Freigabemodus startet, wenn der Zustimmtaster ED1 in den Ein-Zustand geschaltet wird.

ED1- und ES-Eingangsgeräte haben im Freigabemodus die Ein-/Aus-Steuerungshoheit.

Wenn MR1 für die Durchführung eines Reset verwendet wird, wird der normale Ein-Zustand wiederhergestellt und OS1 und ES1 haben die Ein-/Aus-Steuerungshoheit.

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

Das Zeitlimit für den Zustimmtaster 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 Zustimmtaster von Ein auf Aus und wieder zurück auf Ein geschaltet werden.

Alle mit den Sicherheitsausgängen verbundenen Einschalt- und Ausschaltverzögerungszeiten, die durch die Zustimmtasterfunktion 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 Abbildung 48 auf Seite 79; das Referenzsignal RO2 ist dabei mit dem RE-Knoten verbunden.

Zustimmtaster-Funktionsblock

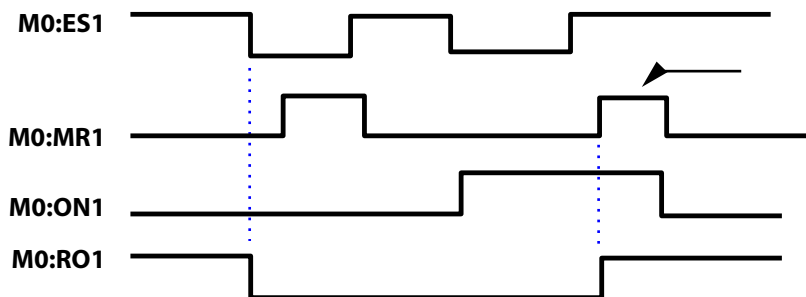
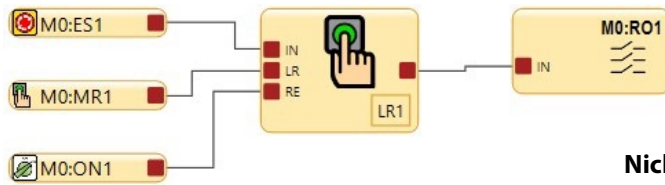
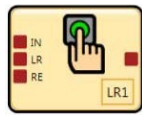


Abbildung 103: Zeitdiagramm: Latch-Reset-Block

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. Für die Durchführung des Reset wird MR1 verwendet.

Manueller Reset-Eingang

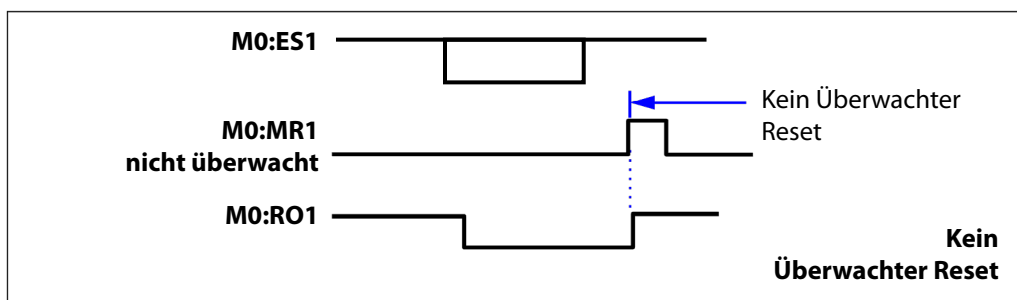
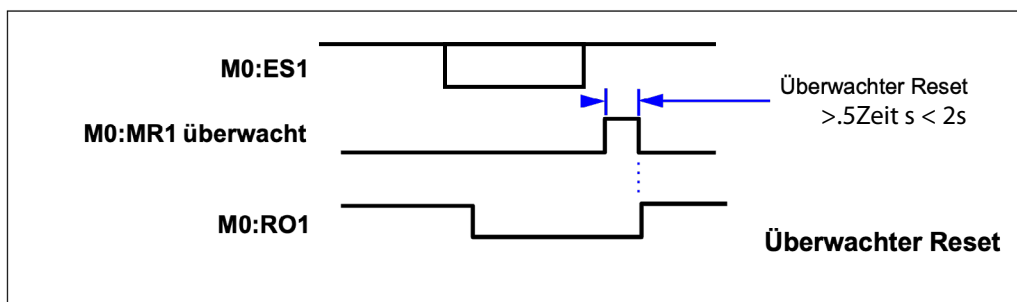
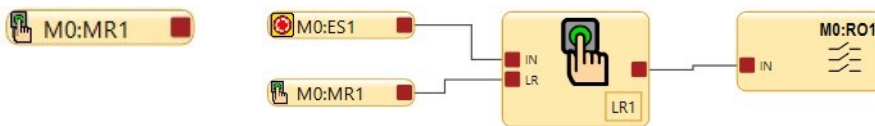
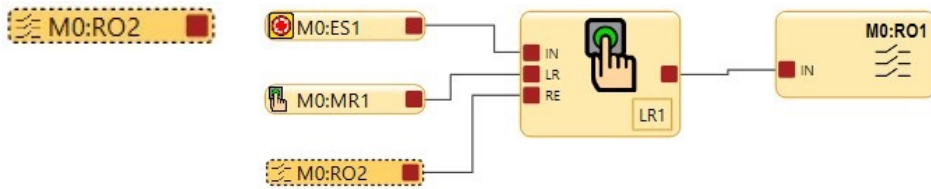


Abbildung 104: Zeitdiagramm: Latch-Reset-Block, überwachter/nicht überwachter Reset

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



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.

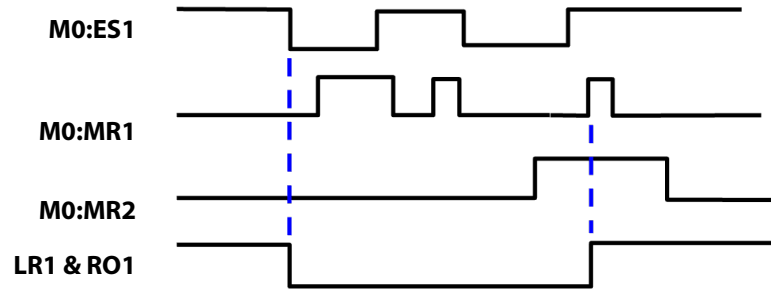


Abbildung 105: Zeitdiagramm: Latch-Reset-Block und referenzierter Sicherheitsausgang

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 „9.18 Referenzsignale“ auf Seite 125.

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.

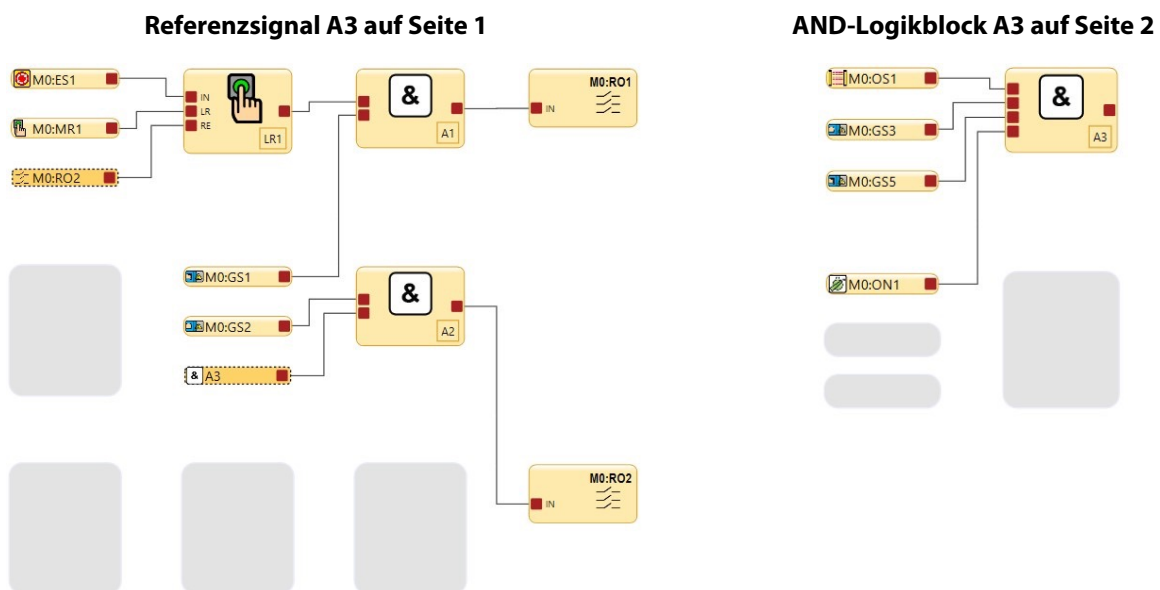


Abbildung 106: Latch-Reset und referenzierter Sicherheitsausgang und AND-Block



Latch-Reset Muting-Funktion

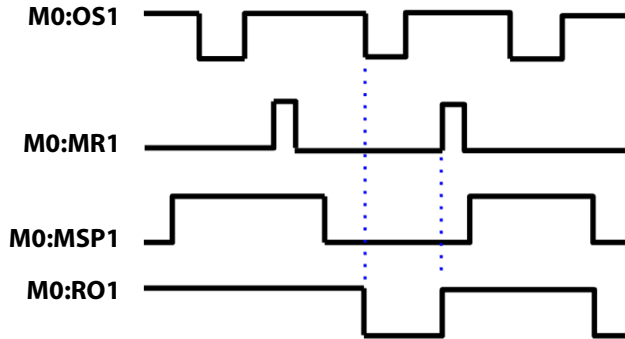
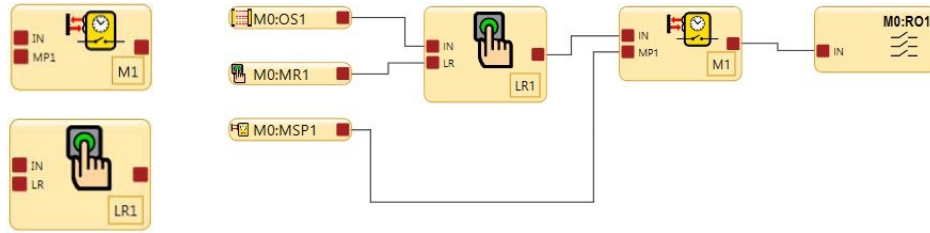


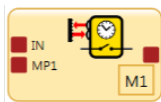
Abbildung 107: Zeitdiagramm: Latch-Reset-Block und Muting-Block

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.

Muting-Funktionsblock

Standardknoten	Zusätzliche Knoten	Anmerkungen
IN MP1	ME BP MP2	Die Eingangsblöcke für Muting-Sensorpaare müssen direkt mit dem Muting-Funktionsblock verbunden werden.

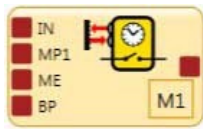


Unten sind fünf Muting-Funktionsarten aufgeführt. Die folgenden Zeitablauf-Diagramme zeigen das Funktionsdetail und die Reihenfolge der Statuswechsel der Sensoren/Schutzeinrichtungen für jede Muting-Funktionsart.

- 1- **Eine Richtung – 1 Muting-Sensorpaar**
- 2- **Zwei Richtungen – 1 Muting-Sensorpaar**
- 1- **Eine Richtung – 2 Muting-Sensorpaare**
- 2- **Zwei Richtungen – 2 Muting-Sensorpaare**
- 2- **Zwei Richtungen – 1 Muting-Sensorpaar**

Abbildung 108: 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 Schutzeinrichtung im Stoppzustand befindet.

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

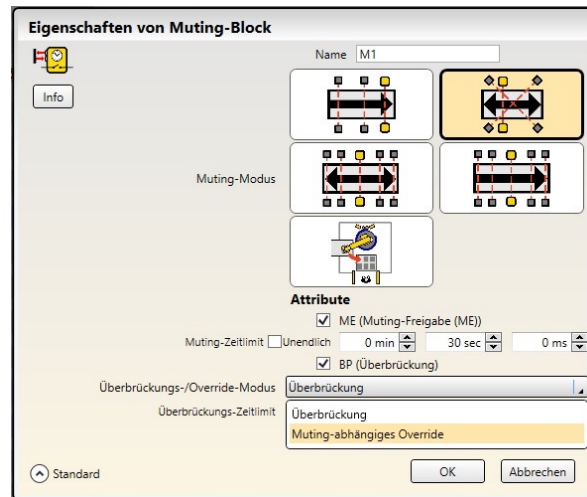


Abbildung 109: Muting-Block: Optionen für den Überbrückungs-/Override-Modus

Muting-abhängiges Override

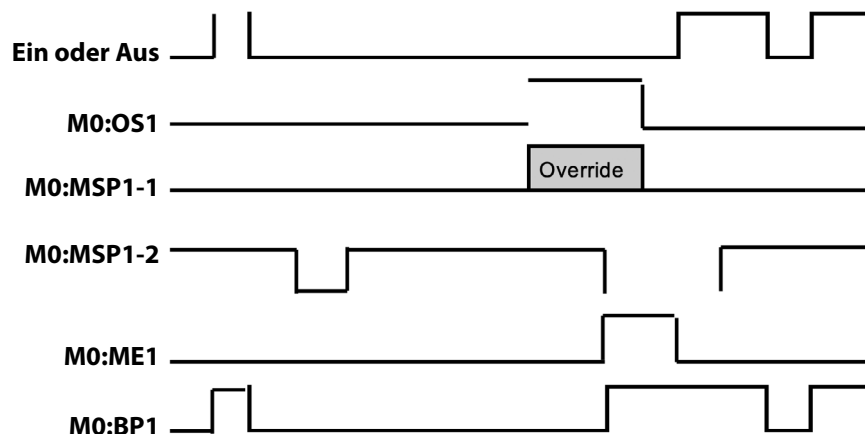
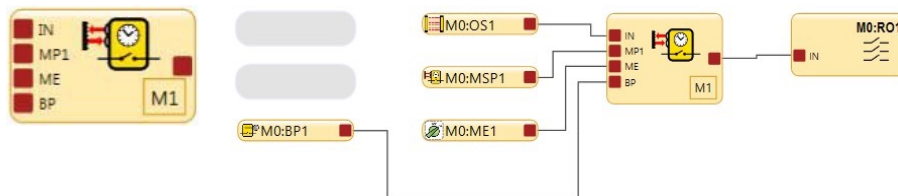


Abbildung 110: Muting-abhängiges Override



Muting-Überbrückung

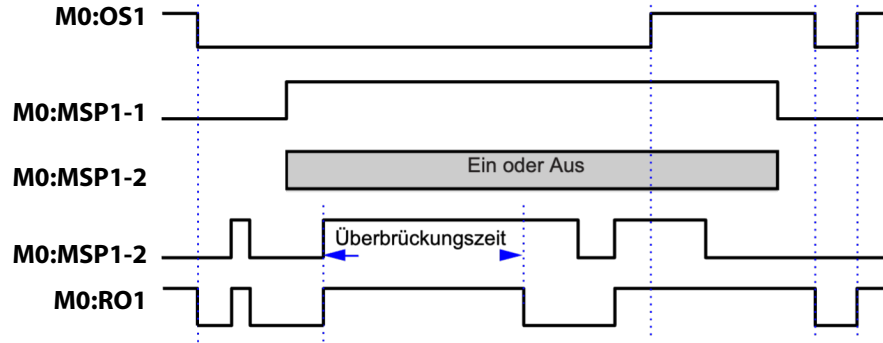
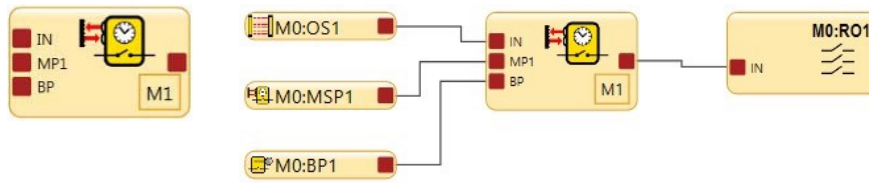


Abbildung 111: Muting-Überbrückung

**Muting-Funktion
1-Richtung – 1
Sensorpaar**

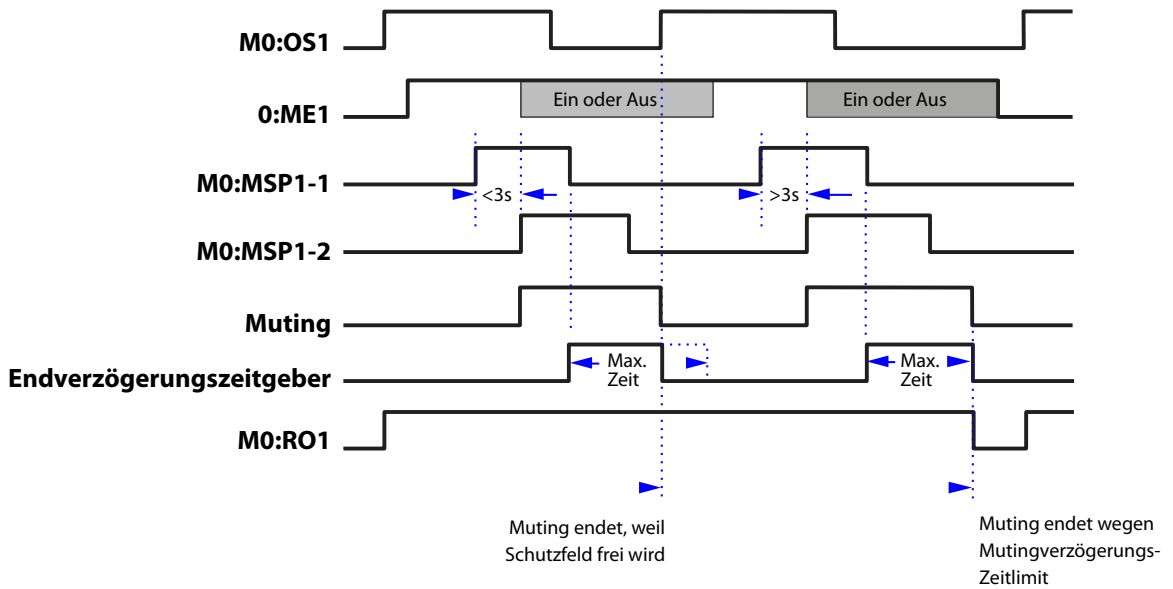
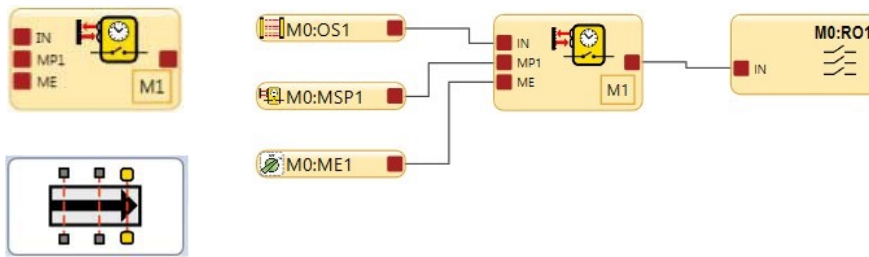


Abbildung 112: Zeitdiagramm: Unidirektionaler Muting-Block, ein Muting-Sensorpaar



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



**Muting-Funktion
1-Richtung – 2
Sensorpaare**

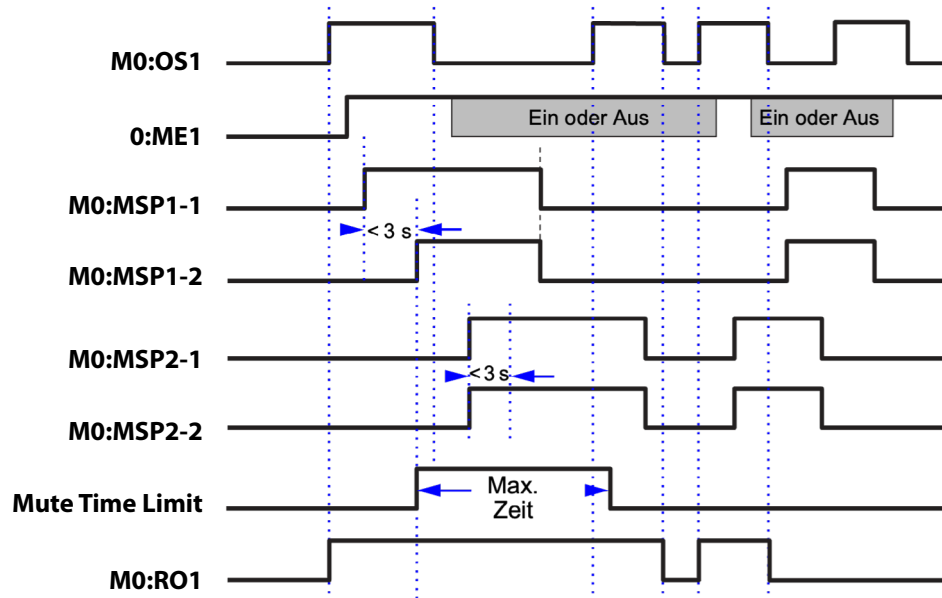
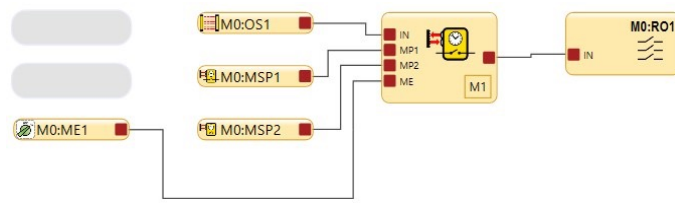
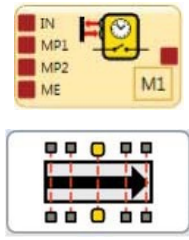


Abbildung 113: Zeitdiagramm: Unidirektionaler Muting-Block, zwei Muting-Sensorpaare

**Muting-Funktion
2-Richtungen – 1
Sensorpaar**

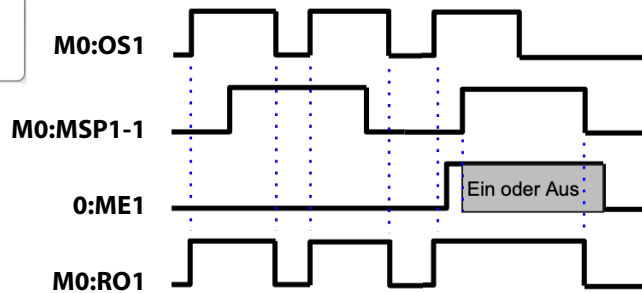
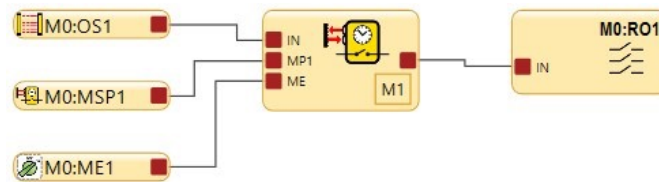
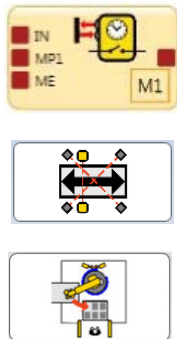


Abbildung 114: Zeitdiagramm: Bidirektionaler Muting-Block, ein Muting-Sensorpaar



**Muting-Funktion
2-Richtungen –
2 Sensorpaare**

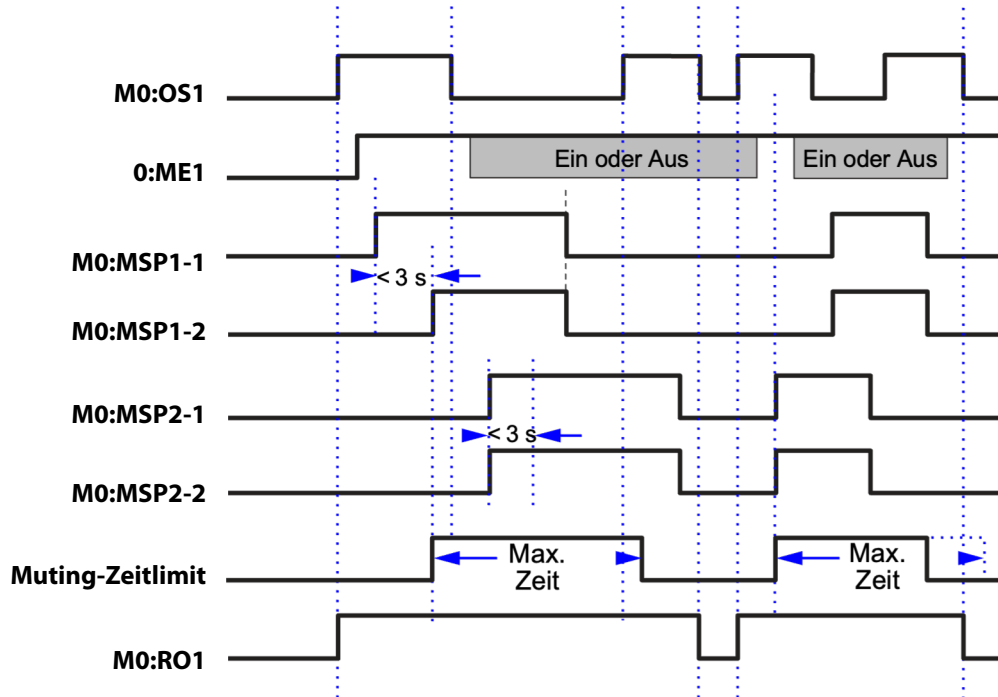
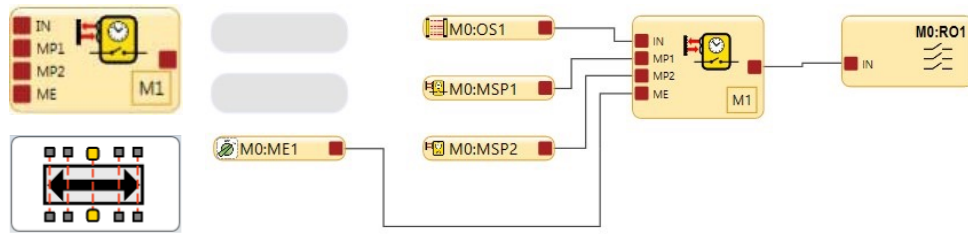


Abbildung 115: Zeitdiagramm: Bidirektionaler Muting-Block, zwei Muting-Sensorpaare

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 gemuted.

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.

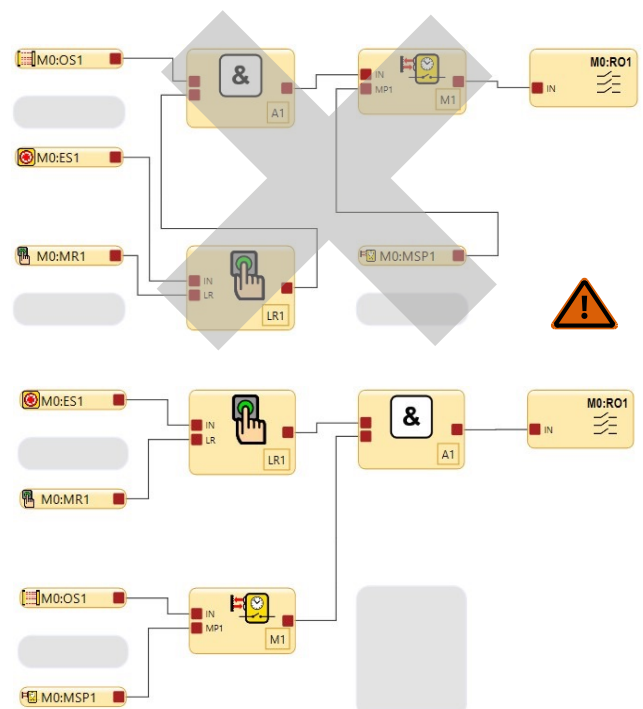


Abbildung 116: : Not-Aus-Schalter und Muting-Funktion



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 Maschinenzklus 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 Überbrückungsfunktionen.

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 Maschinenzklus 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 Schließkontakten für die Muting-Eingänge zu verwenden. Dieses einzelne Gerät mit mehreren Ausgängen könnte ausfallen und ein 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 Mutings 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.

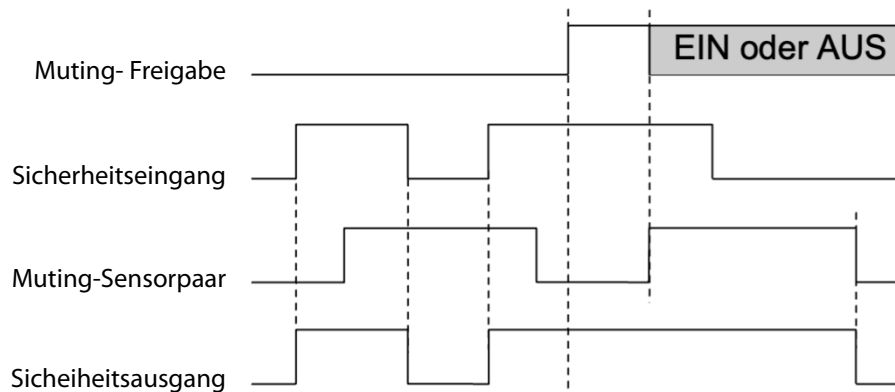


Abbildung 117: Zeitdiagramm: ein Muting-Sensorpaar mit Muting-Freigabe

Reset-Funktion für Gleichzeitigkeitsüberwachung

Der Eingang für die Muting-Aktivierung kann auch verwendet werden, um die Gleichzeitigkeitsüberwachung der Muting-Sensoreingänge zurückzusetzen. Wenn ein Eingang länger als 3 Sekunden aktiv ist, bevor der zweite Eingang aktiv wird, verhindert die 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 Overrides 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 der 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. Mehrstrahlsysteme bei reinen Arbeitszellen-Ausgangsanwendungen verwendet, bei denen sich die Muting-Sensoren nur auf einer Seite des Schutzfelds befinden. Der Muting-Blockausgang bleibt bis zu 5 Sekunden lang eingeschaltet, nachdem die erste Muting-Vorrichtung freigegeben wurde, oder bis das gemutete 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 Risikobeurteilung und für den Betrieb der jeweiligen Maschine erforderlich ist.



WARNUNG:

Die Funktion Muting bei Anlauf sollte nur bei Anwendungen verwendet werden, bei denen:

- Muting des Systems (M1 und M2 geschlossen) beim Anlauf erforderlich ist und dadurch unter keinen Umständen Gefahren für Personen entstehen.

Entprellzeiten für Muting-Sensorpaar

Anhand der Eingangs-Entprellzeiten, die unter den **Erweiterten Einstellungen** im Fenster mit Eigenschaften für das **Muting-Sensorpaar** konfiguriert werden können, kann ein Muting-Zyklus über das Entfernen des Muting-Sensorsignals hinaus verlängert werden. Durch die Konfiguration der Ausschaltentprellzeit kann der Muting-Zyklus um bis zu 1,5 Sekunden (1500 ms) verlängert werden, damit 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 Schaltungsoptionen für die Muting-Vorrichtung sind konfigurierbar und werden im Fenster **Eigenschaften** für das Muting-Sensorpaar angezeigt. Ein ordnungsgemäßes Muting-Signal kommt zustande, wenn beide Kanäle der Muting-Vorrichtung in den Muting-Aktiv-Zustand wechseln, während sich die gemutete 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: optoelektronische Sensoren, induktive Näherungssensoren, Grenzschalter, 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 Schutzfunktion auf allen Seiten aufgehoben. Es darf für Personen nicht möglich sein, unbemerkt und ohne Ausgabe eines Stoppbefehls an die Maschinensteuerung in das Schutzfeld einzudringen. Diese zusätzliche Sicherheitseinrichtung wird normalerweise 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 Erfassungsbereichen wird nicht empfohlen, wenn eine Person in den überwachten Bereich treten kann, ohne erfasst zu werden und ohne, dass ein Stoppbefehl an die Maschinensteuerung gesendet wird. Wenn wie bei der Verwendung von Umlenkspiegeln (siehe Umlenkspiegel, optische **Sicherheitssysteme und Muting auf Seite 145**) an mehreren Erfassungsbereichen ein Muting durchgeführt wird, besteht die Möglichkeit, dass Personen durch einen dem Muting unterliegenden Bereich oder Zugangspunkt in den geschützten Bereich treten können, ohne erfasst zu werden.

Wenn zum Beispiel bei einer Eintritts-/Austritts-Anwendung, in der durch eine in eine Zelle eintretende Palette der Muting-Zyklus initiiert wird, sowohl an den Eintritts- wie auch an den Austritts-PSSDs ein Muting durchgeführt wird, kann eine Person durch den „Austritt“ aus der Zelle in den überwachten Bereich treten. Eine geeignete Lösung des Problems wäre das Muting von Ein- und Austritt mit separaten 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.



10.1 One Shot Block

Der One-Shot-Block ermöglicht den vom Benutzer konfigurierbaren gepulsten Einschaltzustand von maximal 5 Minuten in 1 ms-Schritten.

Standardknoten	Zusätzliche Knoten	Anmerkungen
IN	CD	Eine Zustandsänderung des Eingangssignals von niedrig auf hoch führt dazu, dass der Ausgangsknoten für die konfigurierte Zeit auf hoch geht und dann ausgeschaltet wird.



Hinweis: Die tatsächliche Länge der One Shot-Zeit kann bis zu 1 Scan-Zeit länger sein als die eingestellte Zeit.

Der Knoten „Abbruchverzögerung“ ist ein konfigurierbarer Knoten für den One-Shot-Block. Der Eingang „Cancel Delay“ (Abbruchverzögerung) schaltet den Ausgangsknoten des One Shot-Blocks sofort ab, nachdem er erkannt wurde (aufgrund menschlicher und systembedingter Verzögerungen werden kürzere One Shots höchstwahrscheinlich beendet, bevor eine Abbruchverzögerung in Kraft treten kann).



VORSICHT: Die Verzögerungszeit eines Pulses wirkt sich auf die Reaktionszeit aus. Das One-Shot-Timing kann die Reaktionszeit der Sicherheitssteuerung erheblich verlängern. Dies wirkt sich auf die Positionierung von Schutzeinrichtungen aus, deren Installation durch die Formeln für den Sicherheitsabstand (Mindestabstand) bestimmt wird oder auf andere Weise durch die Zeitspanne bis zum Erreichen eines ungefährlichen Zustands beeinflusst wird. Bei der Installation von Schutzeinrichtungen muss die Verlängerung der Ansprechzeit berücksichtigt werden.



Hinweis: Die auf der Registerkarte „Konfigurationsübersicht“ angegebene Reaktionszeit ist eine Maximalzeit, die sich je nach Verwendung von Verzögerungsblöcken, One-Shot-Blöcken und anderen Logikblöcken (z. B. OR-Funktionen) ändern kann. Es liegt in der Verantwortung des Benutzers, die angemessene Reaktionszeit zu ermitteln, zu überprüfen und einzubauen.

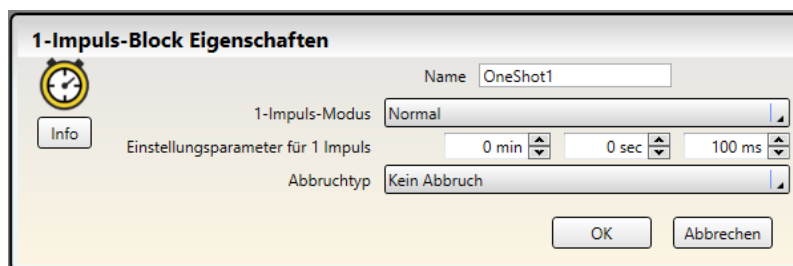


Abbildung 118: One-Shot-Eigenschaften

Im Fenster One Shot-Eigenschaften kann der Benutzer Folgendes konfigurieren:

Name

Erstellen Sie einen Namen mit bis zu 10 Zeichen für den Funktionsblock.

One-Shot-Modus

- Normal
- Heartbeat

One Shot Einstellung Parameter

Einmalige Aufnahmezeit: 1 ms bis 5 Minuten, in Schritten von 1 ms. Die Standardeinstellung ist 100 ms.

Abbrechen Typ

- Nicht abbrechen
- Abbrechen Verzögerung Knoten



One-Shot-Modus

Wenn der Modus „Normal“ ausgewählt ist, wird der Ausgangsknoten eingeschaltet, wenn der Eingangsknoten eingeschaltet wird. Der Ausgang bleibt für die in der One Shot-Einstellung festgelegte Zeit eingeschaltet, unabhängig von Zustandsänderungen am Eingang. (Siehe „Abbildung 119: Typische normale One-Shot-Zeitdiagramme“ auf Seite 142).

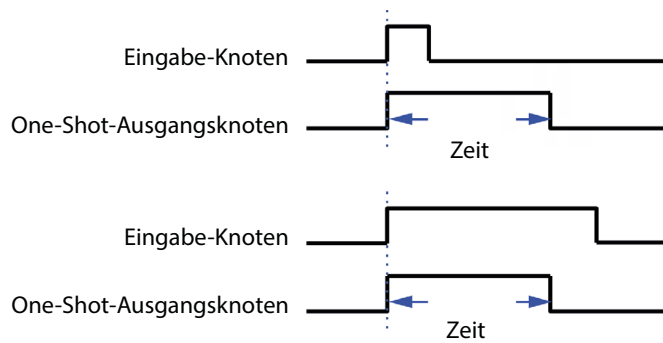


Abbildung 119: Typische normale One-Shot-Zeitdiagramme



Hinweis: Die Einschaltzeit des Sicherheitsausgangs wird um die Einschaltverzögerung des Sicherheitsausgangs (ca. 60 ms) reduziert. Je kürzer die Einschaltverzögerung, desto stärker ist die Reduzierung (größerer Prozentsatz des gewünschten Impulses).

Wenn der Heartbeat-Modus ausgewählt ist, wird der Ausgangsknoten eingeschaltet, wenn der Eingangsknoten eingeschaltet wird. Der Ausgang bleibt für die Zeit eingeschaltet, die für die One-Shot-Einstellung festgelegt wurde. Der für den One Shot eingestellte Timer wird zurückgesetzt, wenn der Eingangsknoten AUS und dann wieder EIN schaltet. (Siehe „Abbildung 120: Heartbeat One Shot Timing Diagramm“ auf Seite 142).

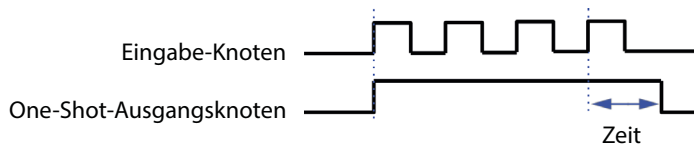


Abbildung 120: Heartbeat One Shot Timing Diagramm



10.2 Steuerung der Presse

Der Funktionsblock Press Control ist für die Verwendung mit einfachen hydraulischen/pneumatischen Pressen vorgesehen. Es gelten die folgenden Normen:

- B11.2-2013, Sicherheitsanforderungen für hydraulische und pneumatische Kraftpressen
- EN ISO 16092-1:2018, Sicherheit von Werkzeugmaschinen - Teil 1 - Allgemeine Sicherheitsanforderungen
- EN ISO 16092-3, Sicherheit von Werkzeugmaschinen - Teil 3 - Sicherheitsanforderungen für hydraulische Pressen
- EN ISO 16092-4, Allgemeine Sicherheitsanforderungen - Teil 4 - Sicherheitsanforderungen für pneumatische Pressen

Es liegt in der alleinigen Verantwortung des Nutzers, sicherzustellen, dass seine Anwendung diesen und allen anderen einschlägigen Normen (einschließlich anderer Pressestandards) entspricht.



WARNUNG:

- Der Funktionsblock Pressensteuerung enthält eine Startvorrichtung (löst eine gefährliche Bewegung aus).
- Die Nichtbeachtung dieser Anweisungen kann zu schweren Verletzungen oder zum Tod führen.
- Die qualifizierte Person muss sicherstellen, dass die Aktivierung (Übergang in den EIN-Zustand) einer angehaltenen Sicherheitseinrichtung (Not-Aus, Seilzug, optischer Sensor, Sicherheitsmatte, Schutzanschlag usw.) durch einen Benutzer keine gefährliche Bewegung auslöst, wenn sie mit einem bereits aktivierten Funktionsblock der Pressensteuerung (EIN-Zustand) verbunden ist.



WARNUNG:

- Installieren Sie dieses Gerät ordnungsgemäß.
- Der Benutzer trägt die alleinige Verantwortung dafür, dass dieses Gerät von BERNSTEIN von qualifizierten Personen gemäß dieser Anleitung und den geltenden Sicherheitsvorschriften installiert und mit der geschützten Maschine verbunden wird. Die Nichtbeachtung dieser Anweisungen kann zu schweren Verletzungen oder zum Tod führen.
- Wenn alle Montage-, Installations-, Anschluss- und Überprüfungsverfahren nicht ordnungsgemäß befolgt werden, kann das Gerät von BERNSTEIN nicht den Schutz bieten, für den es entwickelt wurde. Der Benutzer ist dafür verantwortlich, dass alle lokalen, staatlichen und nationalen Gesetze, Regeln, Codes oder Vorschriften in Bezug auf die Installation und Verwendung dieses Steuersystems in einer bestimmten Anwendung erfüllt werden. Stellen Sie sicher, dass alle gesetzlichen Anforderungen erfüllt sind und dass alle in diesem Handbuch enthaltenen technischen Installations- und Wartungsanweisungen befolgt werden.

Standardknoten	Zusätzliche Knoten	Anmerkungen
GO TOS BOS RST NM Sicherheit	Modus PCI	Wenn Sie die Eingänge Mode oder PCI (Press Control Input) auswählen, erzeugt jeder seinen eigenen Funktionsblock von Eingängen, die mit dem Funktionsblock Press Control verbunden sind. Weitere Informationen finden Sie unter „10.2.1 Modus Funktionsblock“ auf Seite 145 und „10.2.2 Presse Steuereingänge Funktionsblock“ auf Seite 146.

Der Funktionsblock Pressensteuerung enthält Attribute, die aktiviert oder deaktiviert werden können.



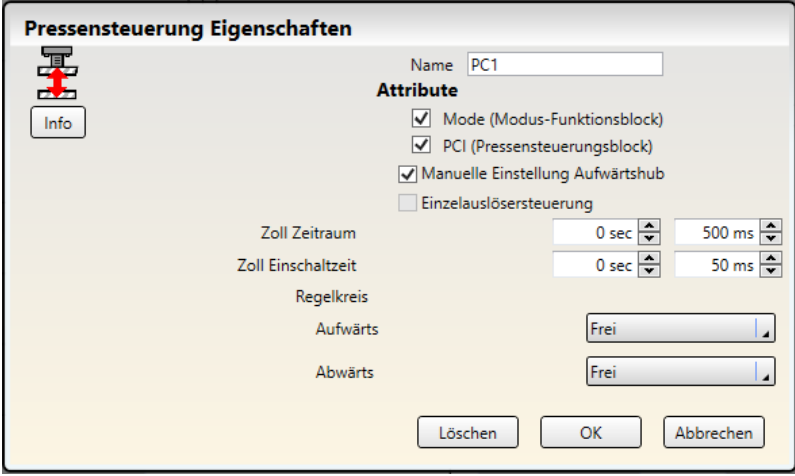


Abbildung 121: Eigenschaften der Pressesteuerung

Die zusätzlichen Knoten, die dem Funktionsblock Pressesteuerung hinzugefügt werden können, erzeugen eigene neue Funktionsblöcke. Der Modus-Funktionsblock wird hinzugefügt, wenn das Attribut Modus ausgewählt ist. Der Pressesteuerung Inputs Function Block wird hinzugefügt, wenn das PCI-Attributfeld ausgewählt ist. Die beiden anderen Attribute, Manuelle Aufwärtshubeinstellung und Einzelantriebsteuerung, können nicht beide ausgewählt werden.

Wenn die manuelle Aufwärtshubeinstellung konfiguriert ist, muss der GO-Eingang während des gesamten Zyklus (sowohl nach unten als auch nach oben) auf EIN gehalten werden. An den GO-Eingangsknoten kann nur ein Zweihandsteuereingang oder ein Fußschalteneingang angeschlossen werden.

Wenn die Einzelantriebsteuerung konfiguriert ist, wirkt der GO-Eingang wie eine Starttaste und muss nur lange genug eingeschaltet bleiben, um den Prozess zu starten. An den GO-Eingangsknoten kann nur ein Zykluseinleitungseingang, ein Fußschalteneingang oder ein Zweihand-Steuereneingang angeschlossen werden.

**WARNUNG:**

- Gefahrenhinweise für den Aufwärtshub drücken.
- Wenn während des Aufwärtshubs eine Gefahr besteht, kann die Nichtverwendung der manuellen Aufwärtshubeinstellung zu schweren Verletzungen oder zum Tod führen.
- Bei Single Actuator Control darf der Aufwärtshub der Presse keine Gefahr darstellen, da der veränderbare Sicherheitsstopp-Eingang während des Aufwärtshubs stummgeschaltet ist.

Die andere Funktion des Funktionsblocks Press Control ist Closed Loop Control. Durch die Aktivierung der Closed-Loop-Steuerung wird die Steuerung gezwungen, zu überprüfen, ob die an die notierten Ausgänge angeschlossenen Geräte ausgeschaltet wurden, wenn das Signal zum Ausschalten kam, bevor der nächste Ausgang eingeschaltet werden kann. Weitere Informationen finden Sie unter Steuerung mit geschlossenem Regelkreis auf Seite 158.



10.2.1 Modus Funktionsblock

Der Modus-Funktionsblock wird hinzugefügt, wenn das Attribut Modus in den Eigenschaften der Pressesteuerung ausgewählt ist.

Die Auswahl Mode Function Block ermöglicht das Hinzufügen eines Funktionswahlschalters. Die drei Eingänge für den Press Function Block sind Run, Inch Up und Inch Down.



Hinweis: Gemäß den Pressestandards sollte der Betriebsartenwahlschalter (oder das Menü) mindestens diese drei Positionen und eine Aus-Position haben. Die Aus-Stellung wäre kein Sicherheits-Aus-Zustand, sondern eine Presse in einem Nicht-Lauf-Zustandseingang (wird nicht mit der Steuerung verbunden, aber die drei Modus-Eingänge wären auch im Aus-Zustand). Wenn alle 3 Modus-Eingänge inaktiv/aus sind, dann bleibt der Press Mode FB aus (rot).



Abbildung 122: Eingänge des Funktionsblocks Pressensteuerung

Wenn der Modus-Funktionsblock im Pressensteuerungs-Funktionsblock ausgewählt wird, werden dem Pressensteuerungs-Funktionsblock die Parameter Inch Period und Inch On Time hinzugefügt. Bei diesen Parametern handelt es sich um benutzerdefinierte Werte für das System, um sicherzustellen, dass sich die Presse beim Tippen nicht zu schnell bewegt (typischerweise im Einrichtungsmodus verwendet).



Hinweis: In der Norm EN ISO 16092-3:2018 ist festgelegt, dass die Zollgeschwindigkeit im Zollmodus nicht höher als 10 mm/Sekunde sein darf.

- Ein Inch-Verfahren ist eine intermittierende Bewegung des Stößels, um ihn langsam auf- oder abwärts zu bewegen, typischerweise zur Wartung oder zum Einstellen von Werkzeugen.
- Die **Inch-Periode** ist die komplette Zykluszeit, Ein und Aus, einer intermittierenden Bewegung des Schiebers
- Die **Inch On Time** ist der On-Teil der Inch Period (das Einschalten der Ausgangsperiode zur Steuerung der Schlittenbewegung)
- Berücksichtigen Sie bei der Einstellung der Perioden- und Einschaltzeiten die Verzögerungen beim Einleiten der Bewegung und beim Anhalten der Bewegung, um die richtige Inch-Geschwindigkeit zu gewährleisten, wenn der GO-Eingang für mehrere Inch-Perioden geschlossen gehalten wird.



WARNUNG:

- Geschwindigkeit der Presse im Inch-Modus.
- Eine zu hohe Geschwindigkeit des Schlittens im Zollmodus kann zu schweren Verletzungen oder zum Tod führen.
- Bei der Einstellung von „Inch Period“ und „Inch On Time“ muss darauf geachtet werden, dass sich der Schlitten im Tipbetrieb mit einer sicheren Geschwindigkeit bewegt.



10.2.2 Presse Steuereingänge Funktionsblock

Der Funktionsblock Press Control Inputs wird hinzugefügt, wenn das PCI-Attributfeld in den Eigenschaften der Pressensteuerung ausgewählt ist. Wenn der PCI-Funktionsblock ausgewählt ist, können andere Pressensteuerungsattribute aktiviert werden.

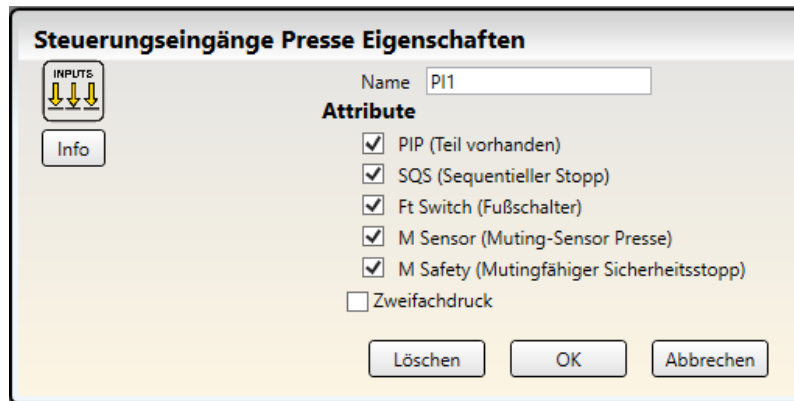


Abbildung 123: Eigenschaften der Pressesteuereingänge

Die Standardknoten des PCI-Blocks sind der PIP-Eingang (Part in Place), der SQS-Eingang (Sequential Stop) und der M Safety-Eingang (Mutable Safety Stop). Wenn SQS ausgewählt wird, sind die Eingänge Ft Switch (Fußschalter) und M Sensor (Press Mute Sensor) als Optionen verfügbar und das Attribut Dual Pressure wird verfügbar (dies ermöglicht das Hinzufügen von Hoch- und Niederdruckausgängen zu den Standardausgängen für Auf- und Abwärtsbewegung).

Verwenden Sie den PIP-Eingang in Pressensteuerungen, bei denen die Presse nicht laufen soll, wenn kein Teil vorhanden ist. Der PIP-Eingang muss High sein, damit der Pressenzyklus beginnt. Nachdem die Presse BOS verlassen hat, muss der PIP-Eingang auf Low und dann wieder auf High gehen, bevor der nächste Pressenzyklus gestartet werden kann; dies kann geschehen, bevor oder nachdem die Presse TOS erreicht.

Verwenden Sie den SQS-Eingang in Pressensteuerungen, bei denen der Pressenstößel auf einen fingersicheren Punkt abgesenkt wird. An diesem Punkt kann der Eingang Mutable Safety Stop stummgeschaltet werden, der Bediener kann den Zweihand-Steuereingang (TC1) (konfiguriert auf den GO-Eingang des Funktionsblocks Pressensteuerung) freigeben und das Werkstück bei Bedarf greifen. Wenn der Eingang Ft Switch (FS1) ausgelöst wird, fährt der Pressenstößel bis zum unteren Ende des Hubs, wo er anhält.



Hinweis: Das oben beschriebene Verfahren ist eine Methode zur Steuerung des Press Control-Prozesses mit konfigurierter SQS. Es gibt drei zulässige Prozesse:

1. TC1 schaltet den GO-Eingang ein, um die Ramme auf den SQS-Punkt zu fahren. Lassen Sie TC1 los und schalten Sie FS1 ein, um den Ft Switch-Eingang einzuschalten und die Ramme auf den BOS-Punkt zu fahren, lassen Sie FS1 los und schalten Sie TC1 ein, um die Ramme anzuheben.
2. FS1 schaltet den GO-Eingang ein, um den Ram zum SQS-Punkt zu fahren. Lassen Sie FS1 los. Durch erneutes Einschalten von FS1 wird der Ram auf den BOS-Punkt und dann wieder auf den TOS-Punkt gefahren. (Der Eingang Ft Switch verschwindet, wenn FS1 mit dem GOKnoten verbunden ist).
3. TC1 schaltet den GO-Eingang ein, um die Ramme auf den SQS-Punkt zu fahren, TC1 loslassen. Durch erneutes Einschalten von TC1 wird die Ramme auf den BOS-Punkt und dann wieder auf den TOS-Punkt gefahren. (Um das System für diese Methode einzurichten, wählen Sie NICHT den Knoten Ft Switch im Funktionsblock Press Control Inputs).

Der M-Sensor-Eingang kann in Verbindung mit dem SQS-Eingang verwendet werden, um den Mutable Safety Stop-Eingang stummzuschalten, wenn er eine fingersichere Position erreicht.

Wenn der SQS-Eingang und der Doppeldruck im Funktionsblock Pressensteuerung Eingang konfiguriert sind, werden dem Funktionsblock Pressensteuerung zwei neue Ausgänge hinzugefügt. Die Ausgangsknoten H (High) und L (Low) werden zusätzlich zu den Standardausgängen U (für Up, Auskuppeln oder Rückhub) und D (für Down, Einkuppeln oder Aushub) hinzugefügt. Der H-Knoten dient zum Einschalten des hohen Drucks, um den letzten Teil des Hubs zu beenden. Der L-Ausgang dient zum Einschalten des Standarddrucks (niedriger Druck), um den Schlitten zum SQS-Punkt zu bringen und in die Ausgangsposition zurückzukehren.



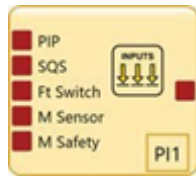


Abbildung 124: Press Control Input

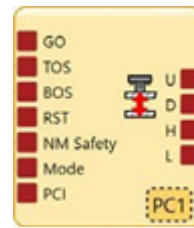


Abbildung 125: Press Control Funktionsblock

10.2.3 Beispiele für Funktionsblöcke zur Pressensteuerung

Dieser Abschnitt enthält zwei Beispielkonfigurationen.

Im Folgenden finden Sie ein Beispiel für eine einfache Konfiguration für eine kleine Presse.

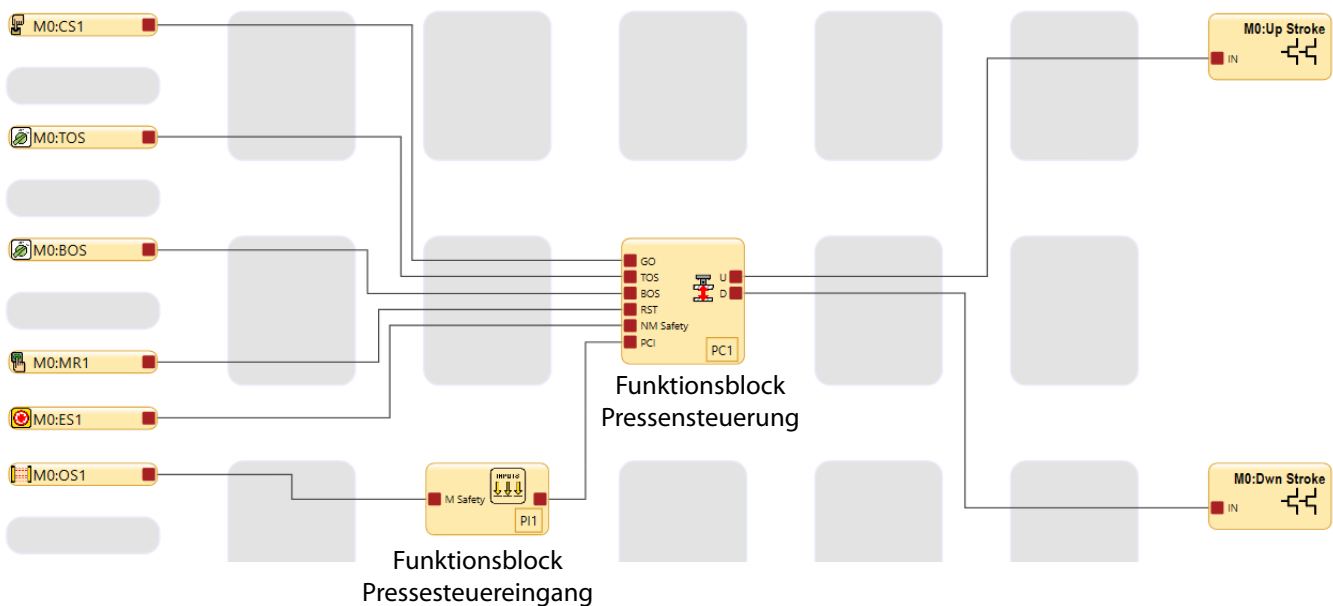


Abbildung 126: Beispielkonfiguration für eine kleine Presse

Der Funktionsblock Pressensteuerung erfordert für den ordnungsgemäßen Betrieb die korrekte Abfolge der Eingangssignale. ES1, OS1 und TOS müssen sich im Zustand „Run“ befinden (und zurückgesetzt worden sein), bevor der CS1-Eingang den entsprechenden Ausgang einschalten kann. Sobald der CS1-Eingang den Prozess gestartet hat, hat entweder der ES1- Eingang, der OS1-Eingang oder das Ende des Zyklus (TOS schaltet sich wieder ein) die Befugnis zum Ausschalten. Siehe das Zeitdiagramm unten oder die Simulationsbeschreibung in „8.5.1 SCx: Einfache Pressensteuerung mit veränderbarem Sicherheitseingang Beispielkonfiguration“ auf Seite 88.

Das folgende Zeitdiagramm zeigt die korrekte Abfolge der Eingänge des Funktionsblocks Pressensteuerung, die zu einem korrekten Betrieb der Ausgänge führt, wenn die Einzelantriebssteuerung aktiviert ist.

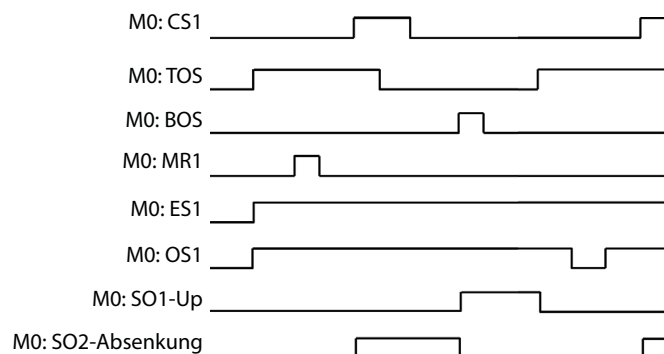


Abbildung 127: Zeitdiagramm für die Pressensteuerung, Steuerung mit einem Stellantrieb

Im Folgenden wird eine Konfiguration gezeigt, die die meisten Funktionen des Funktionsblocks Press Control nutzt.



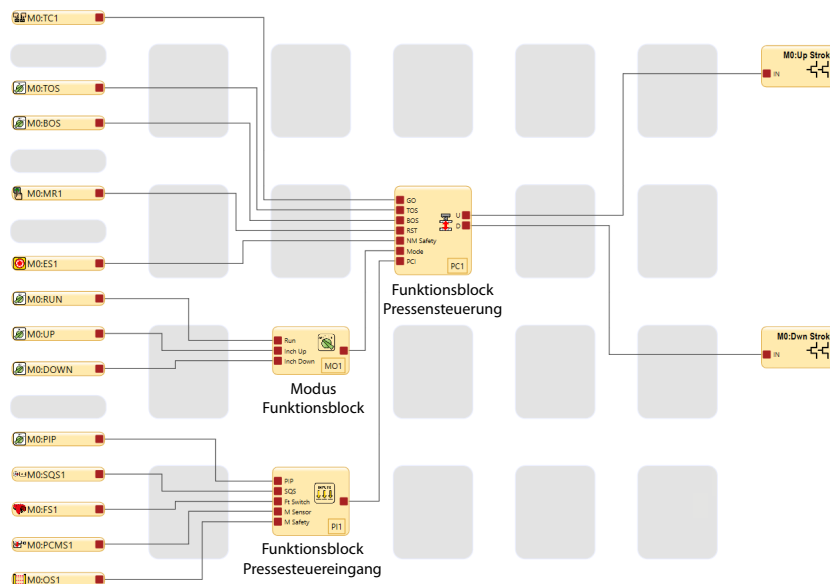


Abbildung 128: Pressesteuerung - Beispielkonfiguration

Der Funktionsblock Pressensteuerung erfordert für den ordnungsgemäßen Betrieb die richtige Abfolge der Eingangssignale. Diese Konfiguration verwendet die manuelle Aufwärtshubeinstellung. ES1, OS1, PIP und TOS müssen sich im Zustand Run befinden (und zurückgesetzt worden sein), bevor der TC1-Eingang den entsprechenden Ausgang einschalten kann.

Während des Abwärtshubs startet der TC1-Eingang den Prozess, und der ES1-Eingang, OS1-Eingang, TC1-Eingang oder das Erreichen des sequentiellen Stopp-Eingangs (SQS schaltet sich ein) hat die Befugnis zum Ausschalten. Wenn die Presse den SQS-Punkt erreicht (SQS und PCMS schalten sich ein), hält sie an und der OS1 wird stummgeschaltet. Der TC1 kann losgelassen werden. Um den Hub zu beenden, schalten Sie den Eingang FS1 ein. Während des restlichen Abwärtshubs hat der ES1-Eingang, der FS1-Eingang oder der BOS (Einschalten) die Befugnis zum Ausschalten. Wenn BOS erreicht ist, wird der FS1-Eingang freigegeben und TC1 verwendet, um die Presse in die TOS-Position zurückzubringen. Während des Aufwärtshubs haben der TC1-Eingang, der ES1-Eingang, der OS1-Eingang oder das Erreichen der TOS-Position die Ausschaltberechtigung. Siehe die Zeittabelle unten oder die Simulationsbeschreibung in SCx: „8.5.2 SCx: Beispielkonfiguration der Pressesteuerung mit allen Funktionen“ auf Seite 90.

Das folgende Zeitdiagramm zeigt die korrekte Abfolge der Eingänge des Funktionsblocks Pressensteuerung, was zu einem ordnungsgemäßen Betrieb der Ausgänge führt, wenn die manuelle Aufwärtshubeinstellung aktiviert ist.

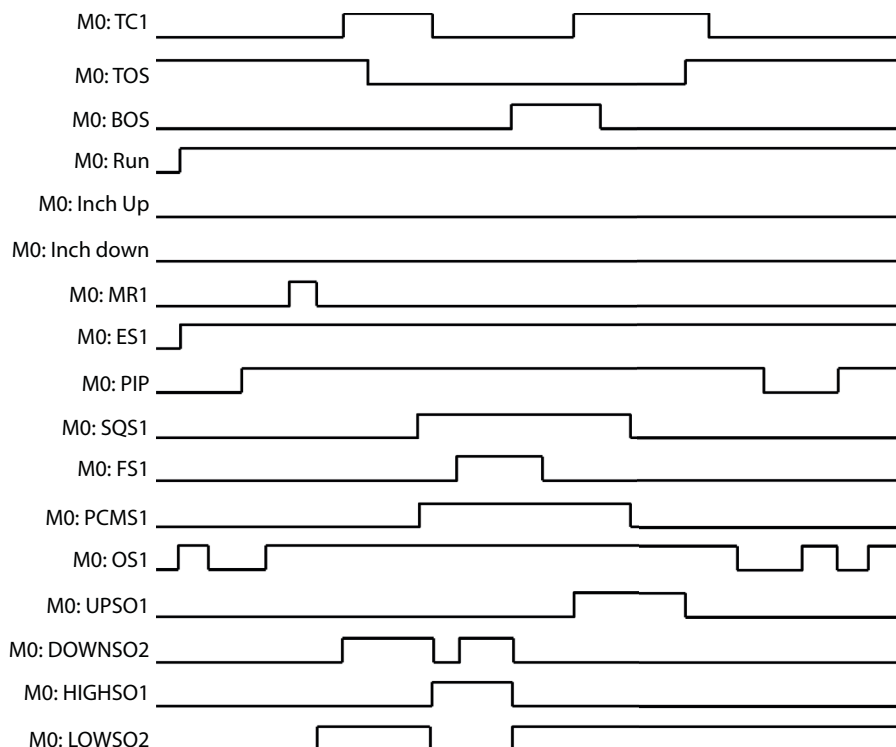


Abbildung 129: Press Control-Timing-Diagramm mit manueller Aufwärtshubeinstellung



10.3.1 Geschlossener Regelkreis

Der Funktionsblock Pressensteuerung bietet die Möglichkeit, die Closed-Loop-Steuerung zu aktivieren. Durch die Aktivierung der Closed-Loop-Steuerung wird der Controller gezwungen, zu überprüfen, ob die an den angegebenen Ausgängen angeschlossenen Geräte ausgeschaltet sind, wenn das Signal zum Ausschalten gegeben wird, bevor der nächste Ausgang zum Einschalten freigegeben wird.

Zur Verwendung des geschlossenen Regelkreises:

1. Dem gewünschten Sicherheitsausgang, der vom Funktionsblock Press Control angesteuert wird, muss ein AVM-Knoten hinzugefügt werden.
2. Der AVM-Eingang gibt Auskunft über den Zustand des jeweiligen Pressventils.
3. Der Funktionsblock Pressensteuerung muss für die Closed-Loop-Steuerung für jeden Ausgang konfiguriert werden. Siehe die Eigenschaften der Pressensteuerung in der folgenden Abbildung.

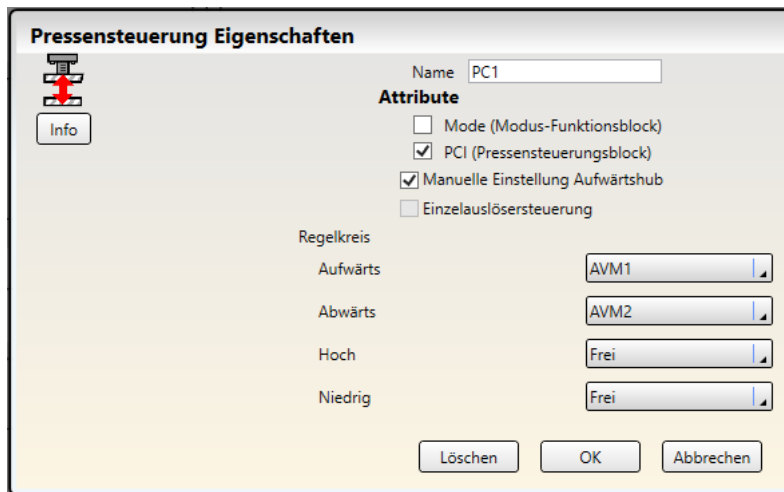


Abbildung 130: Geschlossener Regelkreis

In diesem Beispiel ist die Closed-Loop-Steuerung so eingestellt, dass sie sicherstellt, dass das Aufwärts-Ausgangsventil ausgeschaltet ist, bevor sie andere Funktionen zulässt. Es wird auch sichergestellt, dass das Ventil „Hoch“ geschlossen ist, bevor der Ausgang „Auf“ aktiviert wird.

10.3 Zweihandsteuerungsblock

Standardknoten	Zusätzliche Knoten	Anmerkungen
TC (bis zu 4 TC- Knoten)	IN MP ME	Die Eingänge für Zweihandsteuerungen müssen entweder direkt mit einem Zweihandsteuerungsblock oder indirekt über einen an einen Zweihandsteuerungsblock angeschlossenen Überbrückungsblock verbunden werden. Die Verwendung eines Eingangs für eine Zweihandsteuerung ohne Zweihandsteuerungsblock ist nicht möglich. Mit dem IN-Knoten lassen sich Eingangsgeräte verbinden, die erst eingeschaltet werden müssen, bevor die Zweihandsteuerung die Ausgänge einschalten kann.



Zweihandsteuerungs-Funktionsblock

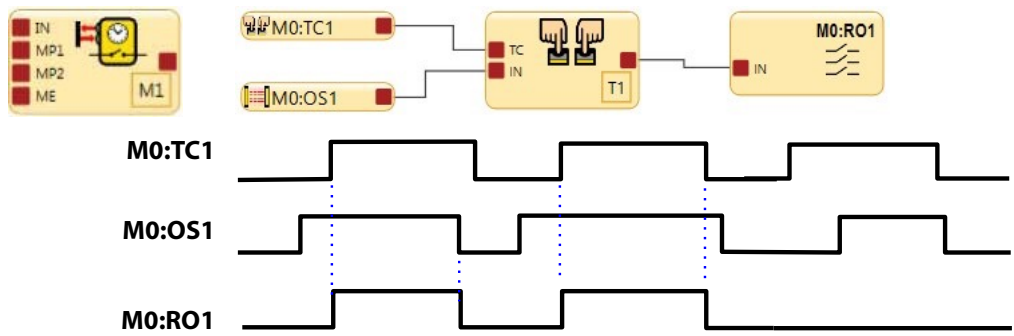


Abbildung 131: Zeitdiagramm: Zweihandsteuerungsblock

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.

Zweihandsteuerungs- und Überbrückungs-funktionsblöcke

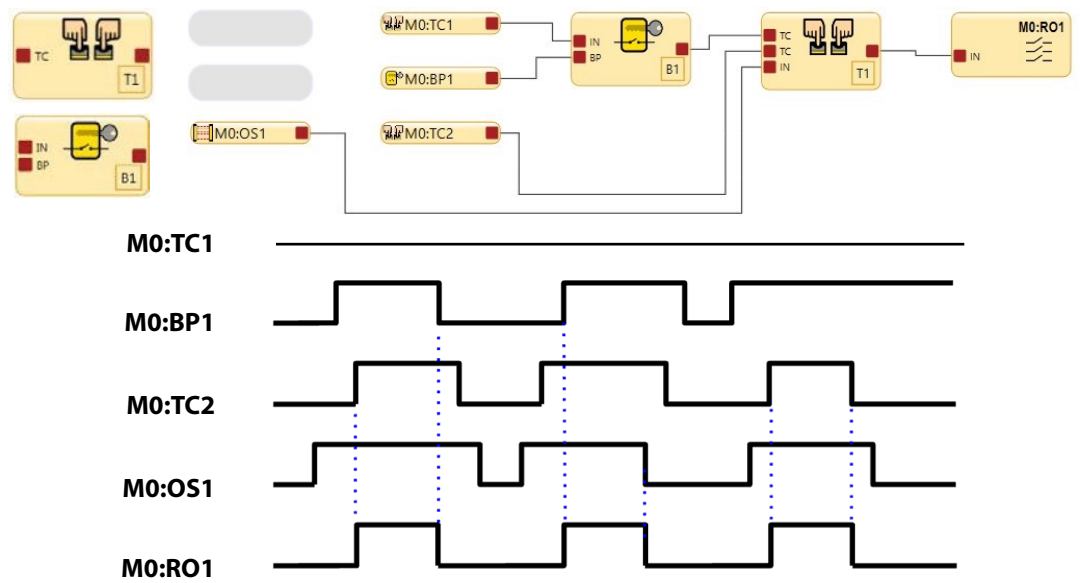


Abbildung 132: Zeitdiagramm: Zweihandsteuerungsblock und Überbrückungsblöcke

Die Zweihandsteuerungs-Bedienelemente TC2 und der Überbrückungsschalter BP1 müssen im Ein-Zustand sein und sie müssen die letzten Geräte im Zeitablauf sein, die in den Ein-Zustand übergehen, damit sich der TC1-Funktionsblock einschaltet.

Zweihandsteuerungs- und Überbrückungs-funktionsblöcke

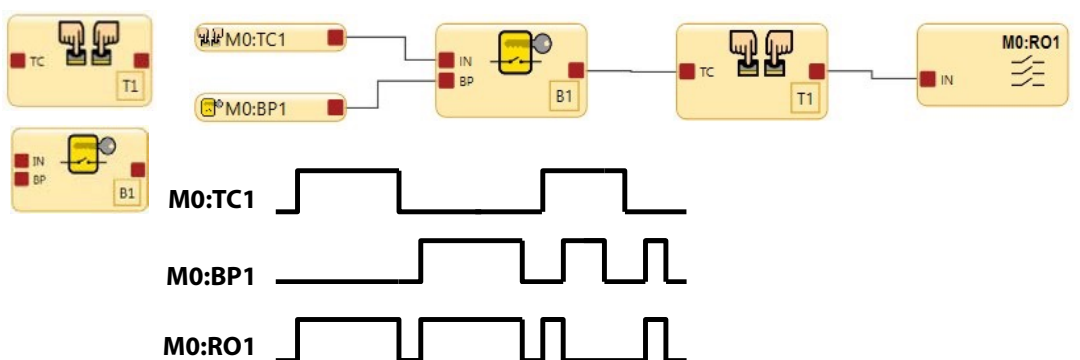


Abbildung 133: Zeitdiagramm: Zweihandsteuerungsblock und Überbrückungsblöcke mit 1 Eingang für Zweihandsteuerung

Wenn die TC1-Bedienelemente und der BP1-Überbrückungsschalter gleichzeitig aktiv sind, schalten sich der Ausgang des B1-Überbrückungsfunktionsblocks und der Ausgang des Zweihandsteuerungs-Funktionsblocks aus.

Die Ausgänge für B1 und T1 schalten sich nur ein, wenn entweder die TC1-Bedienelemente oder der BP1-Schalter im Ein-Zustand sind.



Zweihandsteuerungs- und Überbrückungs-funktionsblöcke

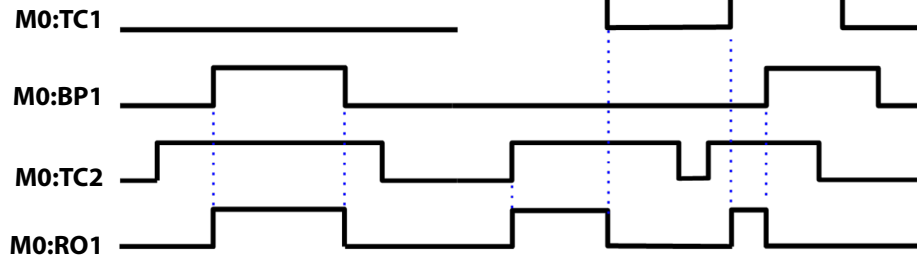
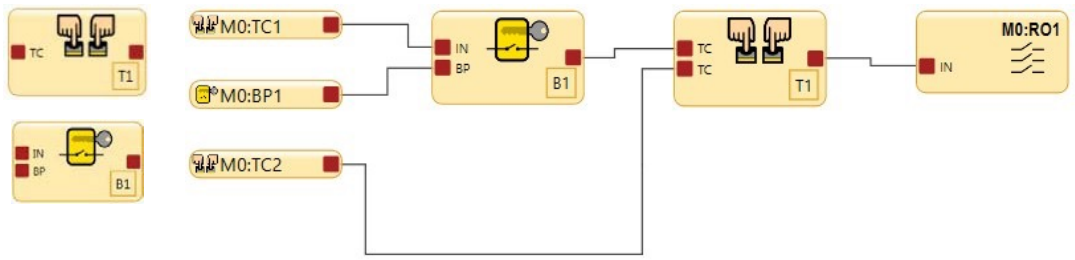


Abbildung 134: Zeitdiagramm: Zweihandsteuerungsblock und Überbrückungsblöcke mit 2 Eingängen für Zweihandsteuerung

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 TI und RO1 nicht eingeschaltet werden oder schalten sich aus.

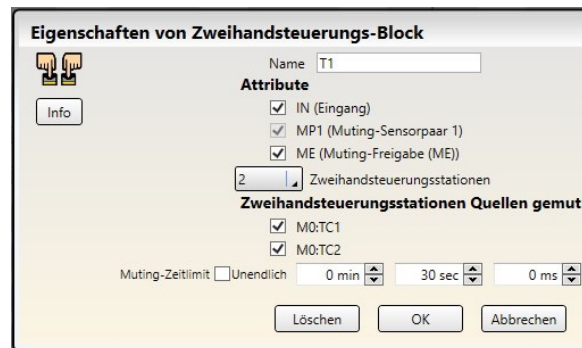


Abbildung 135: Muting-Optionen für Zweihandsteuerungen

Zum Konfigurieren der Muting-Option für die Zweihandsteuerung müssen die TC-Bedienelemente erst mit dem Zweihandsteuerungs-Funktionsblock in der Funktionsansicht verbunden werden. Die Kontrollkästchen (blaues Quadrat oben) im Menü Eigenschaften zeigen die Namen aller Eingangsgeräte für TC-Bedienelemente an. Nur die Stationsfelder der Zweihandsteuerung, deren Kontrollkästchen aktiviert sind, werden gemutet.



Zweihandsteuerung mit Muting:

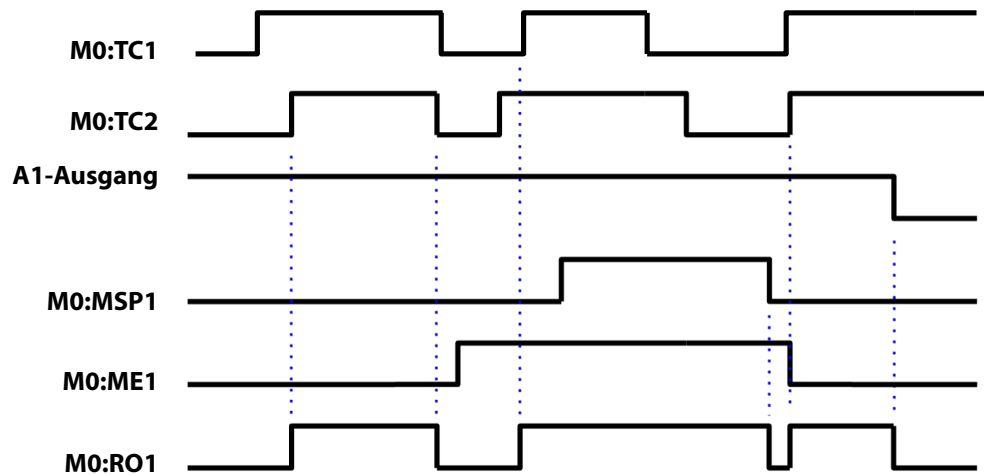
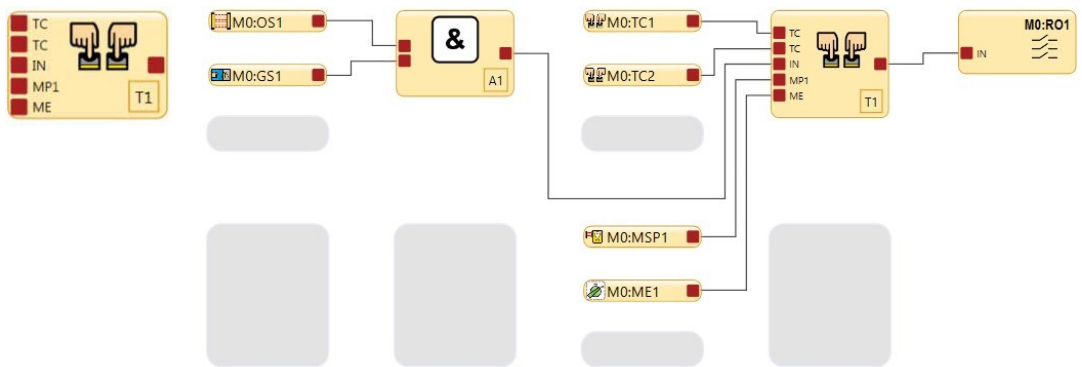


Abbildung 136: Zeitablauf-Diagramm: Zweihandsteuerungsblock mit Muting

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.

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.

10.4 Zweihand-Bedienungsblock (SCx FID 4 und höher und SCR P FID 2 und höher)

Bei SCx und SCR P kann der TC-Eingang direkt auf einen Ausgang oder einen Logikblock abgebildet werden. Der Two-Hand-Control-Funktionsblock kann direkt auf einem Ausgang oder einem Logikblock abgebildet werden. Wenn die Maschine mehrere Bediener hat und jeder Bediener seine Zweihandsteuerung betätigen muss, verwenden Sie den Funktionsblock Zweihandsteuerung, in dem mehrere TC-Eingänge ausgewählt werden können. Wenn das System über eine Haltefunktion verfügt (TC-Eingänge, die eine Aktion auslösen, die es sicher macht, dann können die Bediener ihre Hände entfernen, während der Prozess beendet wird), verwenden Sie den Funktionsblock Zweihandsteuerung mit der ausgewählten Muting-Funktion. Wenn die Maschine über bestimmte Sicherheitseinrichtungen verfügt, die erfüllt sein müssen (und dies auch bleiben müssen), damit der TC-Eingang den Betrieb der Maschine ermöglicht, verwenden Sie den Funktionsblock Zweihandsteuerung mit dem ausgewählten Knoten IN.

- Wenn der IN-Knoten ausgeschaltet ist, führt das Aktivieren des Zweihand-Eingangs zu keinen Aktionen.
- Wenn der Funktionsblock Two-Hand-Control eingeschaltet ist und der TC-Block ausgeschaltet wird, schaltet sich der Ausgang aus.
- Wenn der IN-Knoten wieder auf „High“ geht, bleibt der Ausgang ausgeschaltet, bis die TC-Eingänge auf „Off“ und wieder auf „High“ gehen.





WARNUNG:

- Zweihandschaltungen sind Startvorrichtungen (lösen eine gefährliche Bewegung aus).
- Die Nichtbeachtung dieser Anweisungen kann zu schweren Verletzungen oder zum Tod führen.
- Die sachkundige Person muss sicherstellen, dass die Aktivierung (Übergang in den EIN-Zustand) einer stoppenden Sicherheitseinrichtung (Not-Aus, Seilzug, optischer Sensor, Schaltmatte, Schutzanschlag usw.) durch einen Benutzer keine gefährliche Bewegung auslöst, wenn diese logisch mit einem bereits aktivierten TC-Eingang oder einem Zweihandsteuerungs-Funktionsblock verbunden ist (EIN-Zustand).

11. SCx Onboard-Schnittstelle

Mit Ausnahme spezieller Einstellungen zeigt die integrierte Schnittstelle der Sicherheitssteuerung SCx beim Einschalten den Bildschirm Systemstatus an

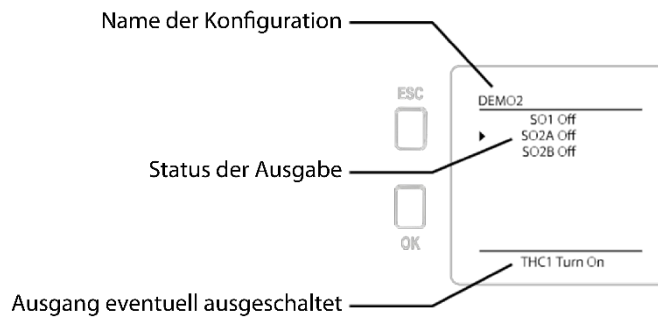


Abbildung 137: Onboard-Schnittstelle beim Start

Um auf andere Informationen über die integrierte Schnittstelle zuzugreifen, drücken Sie die Escape-Taste, um das **Systemmenü** aufzurufen.

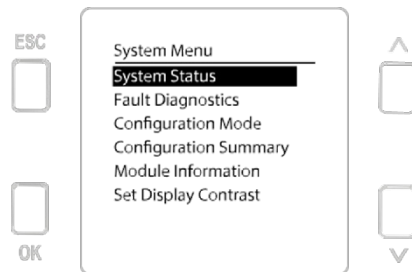


Abbildung 138: Onboard **Interface-System Menü**

Systemstatus

Zeigt den aktuellen Status der Sicherheitsausgänge und, wenn ausgewählt, die mit diesem Ausgang verbundenen Eingänge an (siehe Abbildung 156 auf Seite 163).

Störungsdiagnose

Zeigt die aktuellen Fehler, das Fehlerprotokoll und eine Option zum Löschen des Fehlerprotokolls an (siehe Suchen und Beheben von Fehlern auf Seite 334).



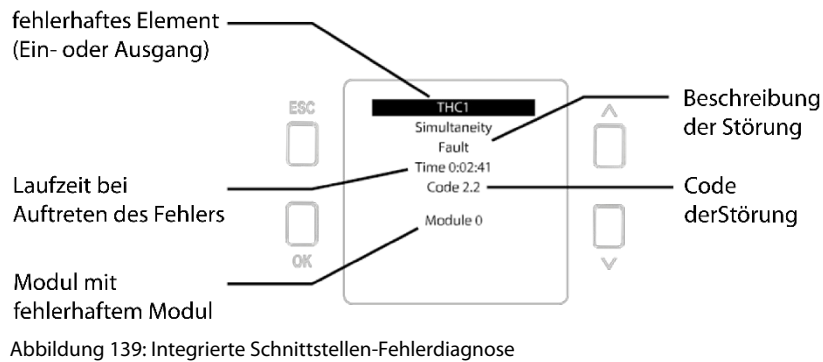


Abbildung 139: Integrierte Schnittstellen-Fehlerdiagnose

Verwenden Sie die Pfeiltasten, um zu anderen Fehlercodes zu gelangen.

Konfigurationsmodus

Ruft den Konfigurationsmodus auf (Kennwort erforderlich) und ermöglicht den Zugriff auf das Kopieren oder Schreiben der Konfiguration vom und zum SCR P-FPS-Laufwerk (siehe „11.1 SCx-Konfigurationsmodus“ auf Seite 155).

Zusammenfassung der Konfiguration

Ermöglicht den Zugriff auf Terminalzuweisungen, Netzwerkeinstellungen und die Konfiguration CRC.

Modell

Zeigt die aktuelle Modellnummer und die Versionen der einzelnen Mikrocontroller an.

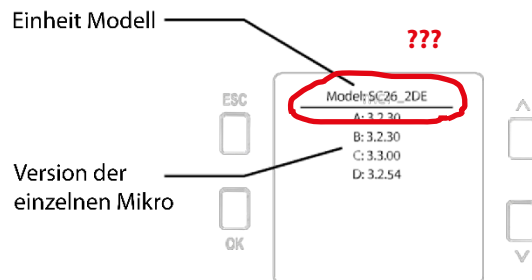


Abbildung 140: Bordseitige Schnittstelle - Modell #

Wenn Erweiterungsmodule an die Sicherheitssteuerung angeschlossen sind, verwenden Sie die Pfeiltasten, um die Versionen der Erweiterungsmodule anzuzeigen.

Display-Kontrast einstellen

Ermöglicht die Einstellung der Display-Helligkeit.



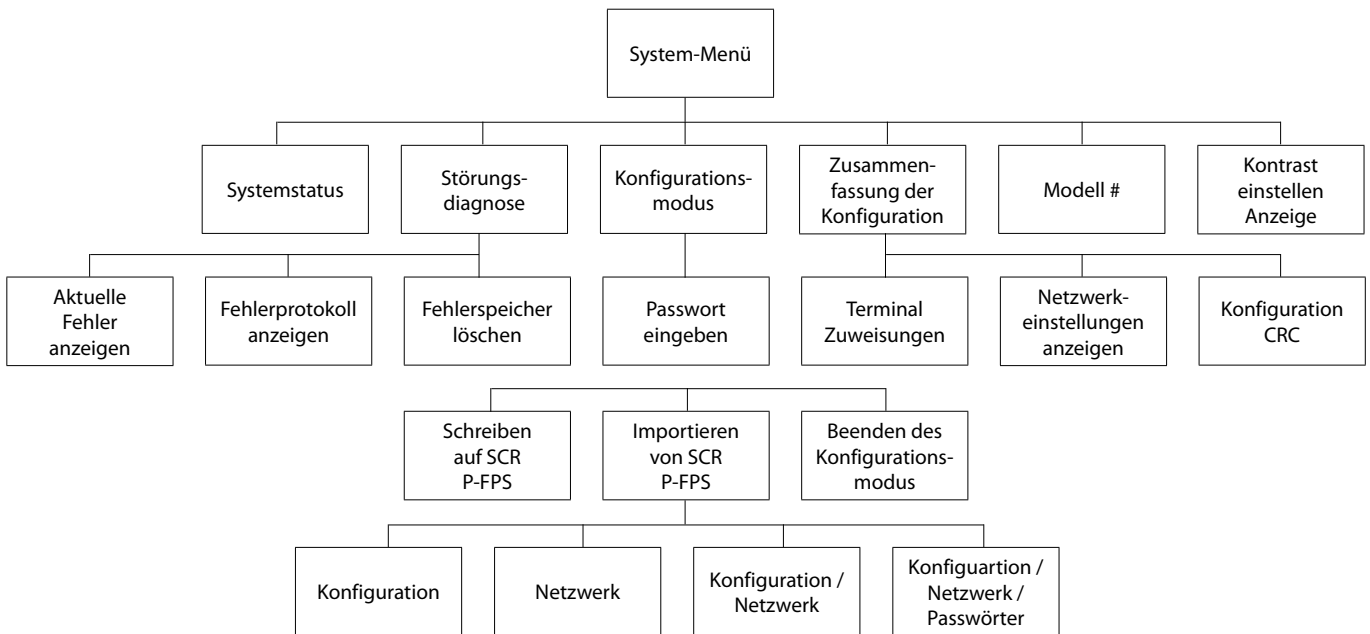


Abbildung 141: Karte der Onboard-Schnittstelle

11.1 SCx-Konfigurationsmodus

Der Konfigurationsmodus bietet Optionen zum Senden der aktuellen Konfiguration an einen SCR P-FPS-Laufwerk und zum Empfangen einer Konfiguration vom SCR P-FPS-Laufwerk.



Hinweis: Für den Zugriff auf das Menü „**Konfigurationsmodus**“ ist ein Passwort erforderlich



Wichtig: Beim Aufrufen des **Konfigurationsmodus** werden die Sicherheitsausgänge ausgeschaltet.

Zum Schreiben von Daten auf den SCR P-FPS -Laufwerk über die integrierte Schnittstelle:

1. Stecken Sie das SCR P-FPS in die Sicherheitssteuerung.
2. Wählen Sie im **Systemmenü** die Option **Konfigurationsmodus**.
3. Geben Sie das Passwort ein.
4. Halten Sie **OK** gedrückt, bis das Menü **Konfigurationsmodus** erscheint.
5. Wählen Sie Write to **SCR P-FPS**.



Hinweis: Beim Schreiben auf SCR P-FPS werden alle Daten (Konfiguration, Netzwerkeinstellungen und Kennwörter) auf das SCR P-FPS -Laufwerk kopiert.

6. Warten Sie, bis der Schreibvorgang abgeschlossen ist.
7. Setzen Sie das System zurück.

So importieren Sie Daten vom SCR P-FPS -Laufwerk über die integrierte Schnittstelle:


1. Stecken Sie den Antrieb SCR P-FPS in die Sicherheitssteuerung.
2. Wählen Sie im **Systemmenü** die Option **Konfigurationsmodus**.
3. Geben Sie das Passwort ein.
4. Halten Sie **OK** gedrückt, bis das Menü **Konfigurationsmodus** erscheint.
5. Wählen Sie **Import aus SCR P-FPS**:
 - Nur für die Konfiguration wählen Sie **Konfiguration**
 - Nur für die Netzwerkeinstellungen wählen Sie **Netzwerkeinstellungen**
 - Für Konfigurations- und Netzwerkeinstellungen wählen Sie **Konfiguration/Netzwerk**
 - Für alle Daten, d. h. Konfiguration, Netzwerkeinstellungen und Benutzerkennwörter, wählen Sie **Konfiguration/Netzwerk/Kennwörter**
6. Warten Sie, bis der Importvorgang abgeschlossen ist.
7. Setzen Sie das System zurück.



12. Industrial-Ethernet – Übersicht

12.1 Konfiguration der Sicherheitsauswertung

Vergewissern Sie sich, dass die Option **Netzwerkschnittstelle aktivieren** markiert ist und die Netzwerkeinstellungen entsprechend dem ausgewählten Protokoll konfiguriert sind.


1. Verbinden Sie die Sicherheitsauswertung über das USB-Kabel mit dem PC.
2. Öffnen Sie die Konfigurationssoftware der Sicherheitsauswertung von BERNSTEIN.
3. Klicken Sie auf  **Netzwerkeinstellungen**.
4. Markieren Sie das Kontrollkästchen **Netzwerkschnittstelle aktivieren**.
5. Konfigurieren Sie entsprechend Ihrem Netzwerk die IP-Adresse und die Subnetzmaske.



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

6. Klicken Sie auf **Senden**.
7. Klicken Sie auf den Pfeil **Erweitert**, um gegebenenfalls die erweiterten Netzwerkeinstellungen zu konfigurieren. Nachfolgend sind die Standardwerte für den Ethernet-Port und das Industrial-Ethernet der Sicherheitsauswertung angegeben.

Netzwerkeinstellungen (Ethernet/IP-Baugruppen)


 Info

Netzwerkschnittstelle aktivieren

IP-Adresse:

Subnetzmaske:

Gatewayadresse:

Übertragungsrate/Duplexmodus: Automatische Aushandlung

Auslösecode (Dezimal 1-65535)

Netzwerk-Zeitüberschreitung aktiviert

Modbus

Zeichenbytes vertauschen

32-Bit-Zahlenformat

Erst MSW sende, dann LSW

Erst LSW senden, dann MSW

EtherNet/IP und PCCC

Zeichenbytes vertauschen

Stringlängentyp

16 Bits

32 Bits

32-Bit-Zahlenformat

Erst MSW sende, dann LSW

Erst LSW senden, dann MSW

8. Geben Sie das entsprechende Passwort ein, um die Konfigurations- und Netzwerkeinstellungen für die Sicherheitsauswertung zu ändern.
9. Vergewissern Sie sich, dass die Sicherheitsauswertung eine gültige und bestätigte Konfigurationsdatei hat.

Der Ethernet-Port ist aktiviert.



12.2 Industrial-Ethernet – Definitionen

Es folgen Beschreibungen der Tabellenzeilen und -spalten (in alphabetischer Reihenfolge) für die Registerkarten der Ansicht **Industrial-Ethernet** in der Software.

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

Tabelle 4: Datentypen

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 („15.6 SCR P-Fehlercode-Tabelle“ auf Seite 249 erhalten Sie weitere Informationen).

Funktion

Die Funktion, die den Zustand des betreffenden virtuellen Ausganges ermittelt.

Betriebsart

Betriebsart

Wert für Betriebsart	Beschreibung
1 (0x01)	Normalbetrieb (einschließlich E/A-Fehlern, sofern vorhanden)
2 (0x02)	Konfigurationsmodus
4 (0x04)	Systemsperrung
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

12.3 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 „15.6 SCR P-Fehlercode-Tabelle“ auf Seite 249, um eine Fehlerbeschreibung und Schritte für die Behebung des Fehlers aufzurufen.



12.4 EtherNet/IP™

In diesem Kontext bezieht sich EtherNet/IP™ speziell auf die EtherNet/IP-Transportklasse 1. Diese wird gelegentlich auch als zyklische EtherNet/IP-E/A-Datenübertragung oder implizite Nachrichtenübertragung bezeichnet. Die Verbindung liefert eine echtzeitnahe Datenübertragung zu und von der SPS sowie dem Zielgerät.

VO-Status/Fehler (100):

- O>T SPS-Ausgang/Sicherheitsauswertung-Eingang Baugruppe 112 (0x70), Größe 2 16-Bit-Register
- T>O SPS-Eingang/Sicherheitsauswertung-Ausgang Baugruppe 100 (0x64), Größe 8 16-Bit-Register

Fehlerindexwörter (101):

- O>T SPS-Ausgang/ Sicherheitsauswertung-Eingang Baugruppe 112 (0x70), Größe 2 16-Bit-Register
- T>O SPS-Eingang/ Sicherheitsauswertung-Ausgang Baugruppe 101 (0x65), Größe 104 16-Bit-Register

Nur Fehlerprotokoll (102):

- O>T SPS-Ausgang/ Sicherheitsauswertung-Eingang Baugruppe 112 (0x70), Größe 2 16-Bit-Register
- T>O SPS-Eingang/ Sicherheitsauswertung-Ausgang Baugruppe 102 (0x66), Größe 150 16-Bit-Register

Reset-/Abbruchverzögerung (103):

- O>T SPS-Ausgang/ Sicherheitsauswertung-Eingang Baugruppe 112 (0x70), Größe 2 16-Bit-Register
- T>O SPS-Eingang/ Sicherheitsauswertung-Ausgang Baugruppe 103 (0x67), Größe 35 16-Bit-Register

VI-Status/Fehler (100):¹⁵

- O>T SPS-Ausgang/ Sicherheitsauswertung-Eingang Baugruppe 113 (0x71), Größe 11 16-Bit-Register
- T>O SPS-Eingang/ Sicherheitsauswertung-Ausgang Baugruppe 100 (0x64), Größe 8 16-Bit-Register

Fehlerindexwörter (101):¹⁵

- O>T SPS-Ausgang/ Sicherheitsauswertung-Eingang Baugruppe 113 (0x71), Größe 11 16-Bit-Register
- T>O SPS-Eingang/ Sicherheitsauswertung-Ausgang Baugruppe 101 (0x65), Größe 104 16-Bit-Register

VI-Reset-/Abbruchverzögerung (103):¹⁵

- O>T SPS-Ausgang/ Sicherheitsauswertung-Eingang Baugruppe 113 (0x71), Größe 11 16-Bit-Register
- T>O SPS-Eingang/ Sicherheitsauswertung-Ausgang Baugruppe 103 (0x67), Größe 35 16-Bit-Register

VRCD Plus DCD (104):¹⁵

- O>T SPS-Ausgang/ Sicherheitsauswertung-Eingang Baugruppe 114 (0x72), Größe 14 16-Bit-Register
- T>O SPS-Eingang/ Sicherheitsauswertung-Ausgang Baugruppe 104 (0x68), Größe 112 16-Bit-Registers

12.4.1 Eingänge Sicherheitsauswertung (Ausgänge von der SPS) O > T

Die Sicherheitsauswertung kann die Instanz 112 (0x70) mit einer Größe von zwei Registern (16-Bit) zum Senden der virtuellen Eingänge 1–32 verwenden.

WORD #	WORD NAME	DATENTYP
0	Virtueller Eingang Ein/Aus (1–16)	16-Bit-Ganzzahl
1	Virtueller Eingang Ein/Aus (17–32)	16-Bit-Ganzzahl

Tabelle 5: Tabelle 2: SPS-Ausgang Baugruppeninstanz 112 (0x70) — Sicherheitsauswertung-Eingänge O > T

¹⁵ Wählen Sie eine der Verbindungen O > T Baugruppeninstanz 113 (0x71) oder 114 (0x72) aus, um die virtuelle Eingangs-/Abbruchverzögerung zu verwenden



12.4.2 Eingänge Sicherheitsauswertung (Ausgänge von der SPS) O > T

Die Sicherheitsauswertung verwendet Instanz 113 (0x71) mit einer Größe von elf Registern (16-Bit) für die Eingangsbaugruppe (SPS-Ausgang) beim Senden virtueller Eingänge, Resets und Abbruchverzögerungen.

WORD #	WORD NAME	DATENTYP
0	Virtueller Eingang Ein/Aus (1–16)	16-Bit-Ganzzahl
1	Virtueller Eingang Ein/Aus (17–32)	16-Bit-Ganzzahl
2	Virtueller Eingang Ein/Aus (33–48)	16-Bit-Ganzzahl
3	Virtueller Eingang Ein/Aus (49–64)	16-Bit-Ganzzahl
4	reserviert	16-Bit-Ganzzahl
5	reserviert	16-Bit-Ganzzahl
6	reserviert	16-Bit-Ganzzahl
7	reserviert	16-Bit-Ganzzahl
8	Virtuelle Reset-/Abbruchverzögerung (1–16) [RCD-Registerbits] (siehe „7.7.1 Virtueller manueller Reset und Abbrechen einer Zeitverzögerung (RCD)“ auf Seite 57)	16-Bit-Ganzzahl
9	reserviert	16-Bit-Ganzzahl
10	RCD-Auslösecode [RCD-Aktivierung Register] (siehe „7.7.1 Virtueller manueller Reset und Abbrechen einer Zeitverzögerung (RCD)“ auf Seite 57)	16-Bit-Ganzzahl

Tabelle 6: SPS-Ausgang Baugruppeninstanz 113 (0x71) — Sicherheitsauswertung-Eingänge O > T

12.4.3 Eingänge Sicherheitsauswertung (Ausgänge von der SPS) O > T

Die Sicherheitsauswertung verwendet die Instanz 114 (0x72) mit einer Größe von 14 Registern (16-Bit) als ihre Eingangsgruppe (SPS-Ausgang), wenn sie virtuelle Eingänge, Resets und Abbruchverzögerungen abrufen und um Leistungs- und Statusinformationen zu den DCD-Geräten abzurufen.



WORD #	WORD NAME	DATENTYP
0	Virtueller Eingang Ein/Aus (1–16)	16-Bit-Ganzzahl
1	Virtueller Eingang Ein/Aus (17–32)	16-Bit-Ganzzahl
2	Virtueller Eingang Ein/Aus (33–48)	16-Bit-Ganzzahl
3	Virtueller Eingang Ein/Aus (49–64)	16-Bit-Ganzzahl
4	reserviert	16-Bit-Ganzzahl
5	reserviert	16-Bit-Ganzzahl
6	reserviert	16-Bit-Ganzzahl
7	reserviert	16-Bit-Ganzzahl
8	Virtuelle Reset-/Abbruchverzögerung (1–16) [RCD-Registerbits] (siehe „7.7.1 Virtueller manueller Reset und Abbrechen einer Zeitverzögerung (RCD)“ auf Seite 57)	16-Bit-Ganzzahl
9	reserviert	16-Bit-Ganzzahl
10	RCD-Auslösecode [RCD-Aktivierung Register] (siehe „7.7.1 Virtueller manueller Reset und Abbrechen einer Zeitverzögerung (RCD)“ auf Seite 57)	16-Bit-Ganzzahl
11	DCD-Leseanfrage	16-Bit-Ganzzahl
12	DCD-Reihe angefordert	16-Bit-Ganzzahl
13	DCD-Gerät angefordert	16-Bit-Ganzzahl

Tabelle 7: SPS-Ausgang Baugruppeninstanz 114 (0x72) — Sicherheitsauswertung-Eingänge O > T



10.4.3.1 Leistungs- und Statusinformationen zu einem einzelnen Gerät über DCD anfordern

1. Word 12: DCD-Reihenschaltung, in der das betreffende Gerät angeschlossen ist (1 oder 2), auswählen.
2. Word 13: DCD-Gerätenummer (1 bis 32) auswählen.
3. Word 11: Wechseln von 0 zu 1, um einen einmaligen Lesevorgang durchzuführen.
4. Gehen Sie zur SPS-Eingangsbaugruppeninstanz 104 (0x68), Wörter 103–112, um die gerätespezifische Datenantwort zu lesen.

12.4.4 Konfigurationsbaugruppenobjekt der Sicherheitsauswertung

Die Sicherheitsauswertung verwendet kein Konfigurationsbaugruppenobjekt.

Da einige EtherNet/IP-Clients dieses Objekt erfordern, verwenden Sie die Instanz 128 (0x80) mit einer Größe von null Registern (16-Bit).

12.4.5 Ausgänge Sicherheitsauswertung (Eingänge zur SPS) T > O

Es stehen fünf Optionen für Baugruppenobjekte der Ausgänge der Sicherheitsauswertung zur Verfügung.

- Die erste und kleinste Option umfasst Informationen zu den virtuellen Ausgängen und ob dort Fehler vorliegen.
- Die zweite Option enthält zusätzlich erweiterte Daten wie den Grund, warum die jeweiligen Sicherheitsausgänge inaktiv sind, sowie weitere beschreibende Fehlerinformationen für die virtuellen Ausgänge.
- Die dritte Option dient ausschließlich dem Zugriff auf das Fehlerprotokoll der Sicherheitsauswertung.
- Die vierte Option wird für das Feedback der virtuellen manuellen Resets und dem Abbruch einer Ausschaltverzögerung verwendet.
- Die fünfte Option erlaubt Zugriff auf Feedback- und DCD-Informationen, zum virtuellen manuellen Reset und den Abbruchverzögerungen.

Alle fünf Optionen sind in den folgenden Abschnitten dargestellt.

12.4.6 SPS-Eingang Baugruppeninstanz 100 (0x64) — 8 Register (VO-Status/Fehler)

Diese Baugruppeninstanz umfasst nur allgemeine Informationen zum Status der ersten 64 virtuellen Ausgänge.

WORD #	WORD NAME	DATENTYP
0	VO1–VO16 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
1	VO17–VO32 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
2	VO33–VO48 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
3	VO49–VO64 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
4	Fehlerbits für VO1–VO16 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
5	Fehlerbits für VO17–VO32 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
6	Fehlerbits für VO33–VO48 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
7	Fehlerbits für VO49–VO64 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl

Tabelle 8: SPS-Eingang Baugruppeninstanz 100 (0x64) — Sicherheitsauswertung-Ausgänge T > O



12.4.7 SPS-Eingang Baugruppeninstanz 101 (0x65) - 104 Register

(Fehlerindexwörter)

Die Baugruppeninstanz enthält den Status der ersten 64 virtuellen Ausgänge sowie erweiterte Informationen zu möglichen Fehlercodes und den Status der 2 Sicherheitsausgänge.

WORD #	WORD NAME	DATENTYP
0	VO1–VO16 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
1	VO17–VO32 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
2	VO33–VO48 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
3	VO49–VO64 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
4	Fehlerbits für VO1–VO16 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
5	Fehlerbits für VO17–VO32 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
6	Fehlerbits für VO33–VO48 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
7	Fehlerbits für VO49–VO64 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
8–39	reserviert	16-Bit-Ganzzahl
40	VO1-Fehlerindex	16-Bit-Ganzzahl
41	VO2-Fehlerindex	16-Bit-Ganzzahl
42	VO3-Fehlerindex	16-Bit-Ganzzahl
43	VO4-Fehlerindex	16-Bit-Ganzzahl
44	VO5-Fehlerindex	16-Bit-Ganzzahl
45	VO6-Fehlerindex	16-Bit-Ganzzahl
46	VO7-Fehlerindex	16-Bit-Ganzzahl
47	VO8-Fehlerindex	16-Bit-Ganzzahl
48	VO9-Fehlerindex	16-Bit-Ganzzahl
49	VO10-Fehlerindex	16-Bit-Ganzzahl
50	VO11-Fehlerindex	16-Bit-Ganzzahl
51	VO12-Fehlerindex	16-Bit-Ganzzahl
52	VO13-Fehlerindex	16-Bit-Ganzzahl
53	VO14-Fehlerindex	16-Bit-Ganzzahl
54	VO15-Fehlerindex	16-Bit-Ganzzahl
55	VO16-Fehlerindex	16-Bit-Ganzzahl
56	VO17-Fehlerindex	16-Bit-Ganzzahl
57	VO18-Fehlerindex	16-Bit-Ganzzahl
58	VO19-Fehlerindex	16-Bit-Ganzzahl
59	VO20-Fehlerindex	16-Bit-Ganzzahl
60	VO21-Fehlerindex	16-Bit-Ganzzahl
61	VO22-Fehlerindex	16-Bit-Ganzzahl
62	VO23-Fehlerindex	16-Bit-Ganzzahl
63	VO24-Fehlerindex	16-Bit-Ganzzahl
64	VO25-Fehlerindex	16-Bit-Ganzzahl
65	VO26-Fehlerindex	16-Bit-Ganzzahl
66	VO27-Fehlerindex	16-Bit-Ganzzahl
67	VO28-Fehlerindex	16-Bit-Ganzzahl
68	VO29-Fehlerindex	16-Bit-Ganzzahl
69	VO30-Fehlerindex	16-Bit-Ganzzahl
70	VO31-Fehlerindex	16-Bit-Ganzzahl
71	VO32-Fehlerindex	16-Bit-Ganzzahl
72	VO33-Fehlerindex	16-Bit-Ganzzahl
73	VO34-Fehlerindex	16-Bit-Ganzzahl
74	VO35-Fehlerindex	16-Bit-Ganzzahl



WORD #	WORD NAME	DATENTYP
75	VO36-Fehlerindex	16-Bit-Ganzzahl
76	VO37-Fehlerindex	16-Bit-Ganzzahl
77	VO38-Fehlerindex	16-Bit-Ganzzahl
78	VO39-Fehlerindex	16-Bit-Ganzzahl
79	VO40-Fehlerindex	16-Bit-Ganzzahl
80	VO41-Fehlerindex	16-Bit-Ganzzahl
81	VO42-Fehlerindex	16-Bit-Ganzzahl
82	VO43-Fehlerindex	16-Bit-Ganzzahl
83	VO44-Fehlerindex	16-Bit-Ganzzahl
84	VO45-Fehlerindex	16-Bit-Ganzzahl
85	VO46-Fehlerindex	16-Bit-Ganzzahl
86	VO47-Fehlerindex	16-Bit-Ganzzahl
87	VO48-Fehlerindex	16-Bit-Ganzzahl
88	VO49-Fehlerindex	16-Bit-Ganzzahl
89	VO50-Fehlerindex	16-Bit-Ganzzahl
90	VO51-Fehlerindex	16-Bit-Ganzzahl
91	VO52-Fehlerindex	16-Bit-Ganzzahl
92	VO53-Fehlerindex	16-Bit-Ganzzahl
93	VO54-Fehlerindex	16-Bit-Ganzzahl
94	VO55-Fehlerindex	16-Bit-Ganzzahl
95	VO56-Fehlerindex	16-Bit-Ganzzahl
96	VO57-Fehlerindex	16-Bit-Ganzzahl
97	VO58-Fehlerindex	16-Bit-Ganzzahl
98	VO59-Fehlerindex	16-Bit-Ganzzahl
99	VO60-Fehlerindex	16-Bit-Ganzzahl
100	VO61-Fehlerindex	16-Bit-Ganzzahl
101	VO62-Fehlerindex	16-Bit-Ganzzahl
102	VO63-Fehlerindex	16-Bit-Ganzzahl
103	VO64-Fehlerindex	16-Bit-Ganzzahl

SPS-Eingang Baugruppeninstanz 101 (0x65) — Sicherheitsauswertung-Ausgänge T > O

Fehlerindex-Wörter eines virtuellen Ausgangs (VO)

Mit der Fehlerindexnummer eines virtuellen Ausgangs kann der mit einem bestimmten virtuellen Ausgang verknüpfte Fehlercode als einzelne 16-Bit-Ganzzahl dargestellt werden. Dieser Wert entspricht dem Wert des Fehlermeldungsindex für einen bestimmten virtuellen Ausgang. Siehe „15.6 SCR P-Fehlercode-Tabelle“ auf Seite 249 und „15.5 SCx-Fehlercode-Tabelle“ auf Seite 243. Hinweis: Nicht jeder virtuelle Ausgang hat einen verknüpften Fehlerindex.



12.4.8 SPS-Eingang Baugruppeninstanz 102 (0x66) - 150 Register (nur Fehlerprotokoll)

Mit dieser Baugruppeninstanz wird ausschließlich auf die Fehlerprotokollinformationen auf der Sicherheitsauswertung zugegriffen.



Hinweis: Diese Baugruppeninstanz umfasst nur Informationen zum Status der virtuellen Ausgänge.

Die Sicherheitsauswertung kann 10 Fehler im Protokoll speichern. Fehler Nr. 1 ist der neueste Fehler. Je höher die Nummer, desto älter die Fehler.

WORD #	WORD NAME	DATENTYP
0–1	Fehler Nr. 1 Zeitstempel	32-Bit-Ganzzahl
2–9	Fehler Nr. 1 E/A- oder Systemname	Doppelwortlänge + 12-ASCII-Zeichen
10	Fehler Nr. 1 Fehlercode	16-Bit-Ganzzahl
11	Fehler Nr. 1 Erweiterter Fehlercode	16-Bit-Ganzzahl
12	Fehler Nr. 1 Fehlermeldungsindex	16-Bit-Ganzzahl
13–14	reserviert	16-Bit-Ganzzahl
15–16	Fehler Nr. 2 Zeitstempel	32-Bit-Ganzzahl
17–24	Fehler Nr. 2 E/A- oder Systemname	Doppelwortlänge + 12-ASCII-Zeichen
25	Fehler Nr. 2 Fehlercode	16-Bit-Ganzzahl
26	Fehler Nr. 2 Erweiterter Fehlercode	16-Bit-Ganzzahl
27	Fehler Nr. 2 Fehlermeldungsindex	16-Bit-Ganzzahl
28–29	reserviert	16-Bit-Ganzzahl
30–31	Fehler Nr. 3 Zeitstempel	32-Bit-Ganzzahl
32–39	Fehler Nr. 3 E/A- oder Systemname	Doppelwortlänge + 12-ASCII-Zeichen
40	Fehler Nr. 3 Fehlercode	16-Bit-Ganzzahl
41	Fehler Nr. 3 Erweiterter Fehlercode	16-Bit-Ganzzahl
42	Fehler Nr. 3 Fehlermeldungsindex	16-Bit-Ganzzahl
43–44	reserviert	16-Bit-Ganzzahl
45–46	Fehler Nr. 4 Zeitstempel	32-Bit-Ganzzahl
47–54	Fehler Nr. 4 E/A- oder Systemname	Doppelwortlänge + 12-ASCII-Zeichen
55	Fehler Nr. 4 Fehlercode	16-Bit-Ganzzahl
56	Fehler Nr. 4 Erweiterter Fehlercode	16-Bit-Ganzzahl
57	Fehler Nr. 4 Fehlermeldungsindex	16-Bit-Ganzzahl
58–59	reserviert	16-Bit-Ganzzahl
60–61	Fehler Nr. 5 Zeitstempel	32-Bit-Ganzzahl
62–69	Fehler Nr. 5 E/A- oder Systemname	Doppelwortlänge + 12-ASCII-Zeichen
70	Fehler Nr. 5 Fehlercode	16-Bit-Ganzzahl
71	Fehler Nr. 5 Erweiterter Fehlercode	16-Bit-Ganzzahl
72	Fehler Nr. 5 Fehlermeldungsindex	16-Bit-Ganzzahl
73–74	reserviert	16-Bit-Ganzzahl
75–76	Fehler Nr. 6 Zeitstempel	32-Bit-Ganzzahl
77–84	Fehler Nr. 6 E/A- oder Systemname	Doppelwortlänge + 12-ASCII-Zeichen
85	Fehler Nr. 6 Fehlercode	16-Bit-Ganzzahl
86	Fehler Nr. 6 Erweiterter Fehlercode	16-Bit-Ganzzahl
87	Fehler Nr. 6 Fehlermeldungsindex	16-Bit-Ganzzahl
88–89	reserviert	16-Bit-Ganzzahl
90–91	Fehler Nr. 7 Zeitstempel	32-Bit-Ganzzahl
92–99	Fehler Nr. 7 E/A- oder Systemname	Doppelwortlänge + 12-ASCII-Zeichen



WORD #	WORD NAME	DATENTYP
100	Fehler Nr. 7 Fehlercode	16-Bit-Ganzzahl
101	Fehler Nr. 7 Erweiterter Fehlercode	16-Bit-Ganzzahl
102	Fehler Nr. 7 Fehlermeldungsindex	16-Bit-Ganzzahl
103–104	reserviert	16-Bit-Ganzzahl
105–106	Fehler Nr. 8 Zeitstempel	32-Bit-Ganzzahl
107–114	Fehler Nr. 8 E/A- oder Systemname	Doppelwortlänge + 12-ASCII-Zeichen
115	Fehler Nr. 8 Fehlercode	16-Bit-Ganzzahl
116	Fehler Nr. 8 Erweiterter Fehlercode	16-Bit-Ganzzahl
117	Fehler Nr. 8 Fehlermeldungsindex	16-Bit-Ganzzahl
118–119	reserviert	16-Bit-Ganzzahl
120–121	Fehler Nr. 9 Zeitstempel	32-Bit-Ganzzahl
122–129	Fehler Nr. 9 E/A- oder Systemname	Doppelwortlänge + 12-ASCII-Zeichen
130	Fehler Nr. 9 Fehlercode	16-Bit-Ganzzahl
131	Fehler Nr. 9 Erweiterter Fehlercode	16-Bit-Ganzzahl
132	Fehler Nr. 9 Fehlermeldungsindex	16-Bit-Ganzzahl
133–134	reserviert	16-Bit-Ganzzahl
135–136	Fehler Nr. 10 Zeitstempel	32-Bit-Ganzzahl
137–144	Fehler Nr. 10 E/A- oder Systemname	Doppelwortlänge + 12-ASCII-Zeichen
145	Fehler Nr. 10 Fehlercode	16-Bit-Ganzzahl
146	Fehler Nr. 10 Erweiterter Fehlercode	16-Bit-Ganzzahl
147	Fehler Nr. 10 Fehlermeldungsindex	16-Bit-Ganzzahl
148–149	reserviert	16-Bit-Ganzzahl

Tabelle 9: : SPS-Eingang Baugruppeninstanz 102 (0–66) — Sicherheitsauswertung-Ausgänge T > O

Falscher Zeitstempel

Die relative Zeit in Sekunden, nachdem der Fehler aufgetreten ist. Gemessen ab Zeitpunkt 0, also dem letzten Zeitpunkt, an dem die Sicherheitsauswertung eingeschaltet wurde.

E/A- oder Systemname

Dies ist ein ASCII-String, der den Ursprung des Fehlers beschreibt.

Fehlercode, erweiterter Fehlercode, Fehlerindexmeldung

Der Sicherheitsauswertungs-Fehlercode setzt sich aus dem Fehlercode und dem erweiterten Fehlercode zusammen. Das Format des Fehlercodes ist Fehlercode„Punkt“ erweiterter Fehlercode. Der Sicherheitsauswertungs-Fehlercode 2.1 wird beispielsweise vom Fehlercode 2 und dem erweiterten Fehlercode 1 angegeben. Der Indexwert der Fehlermeldung ist der Fehlercode und der erweiterte Fehlercode zusammen und umfasst eine führende Null mit dem erweiterten Fehlercode, falls erforderlich. Der Sicherheitsauswertungs-Fehlercode 2.1 wird beispielsweise vom Fehlermeldungsindex 201 angegeben. Mit dem Indexwert der Fehlermeldung kann der vollständige Fehlercode bequem nur anhand eines einzigen 16-Bit-Registerwerts abgerufen werden.



12.4.9 SPS-Eingang Baugruppeninstanz 103 (0x67) — 35 Register (Reset-/Abbruchverzögerung)

Diese Baugruppeninstanz übermittelt den Status aller 256 virtuellen Ausgänge und Fehler und stellt die erforderlichen Feedback-Informationen für die Ausführung virtueller Reset- und Abbruchverzögerungen zur Verfügung.

WORD #	WORD NAME	DATENTYP
0	VO1–VO16 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
1	VO17–VO32 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
2	VO33–VO48 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
3	VO49–VO64 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
4	VO65–VO80 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
5	VO81–VO96 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
6	VO97–VO112 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
7	VO113–VO128 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
8	VO129–VO144 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
9	VO145–VO160 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
10	VO161–VO176 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
11	VO177–VO192 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
12	VO193–VO208 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
13	VO209–VO224 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
14	VO225–VO240 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
15	VO241–VO256 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
16	Fehlerbits für VO1–VO16 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
17	Fehlerbits für VO17–VO32 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
18	Fehlerbits für VO33–VO48 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
19	Fehlerbits für VO49–VO64 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
20	Fehlerbits für VO65–VO80 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
21	Fehlerbits für VO81–VO96 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
22	Fehlerbits für VO97–VO112 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
23	Fehlerbits für VO113–VO128 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
24	Fehlerbits für VO129–VO144 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
25	Fehlerbits für VO145–VO160 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
26	Fehlerbits für VO161–VO176 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
27	Fehlerbits für VO177–VO192 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
28	Fehlerbits für VO193–VO208 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
29	Fehlerbits für VO209–VO224 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
30	Fehlerbits für VO225–VO240 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
31	Fehlerbits für VO241–VO256 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl



WORD #	WORD NAME	DATENTYP
32	Virtuelle Reset-/Abbruchverzögerung (1–16) Feedback [RCD-Feedback Registerbits] (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 52)	16-Bit-Ganzzahl
33	reserviert	16-Bit-Ganzzahl
34	RCD-Auslösecode Feedback [RCD-Aktivierung Feedbackregister] (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 52.	16-Bit-Ganzzahl

Tabelle 10: SPS-Eingang Baugruppeninstanz 103 (0–67) — Sicherheitsauswertung-Ausgänge T > O

12.4.10 SPS-Eingangsbaugruppeninstanz 104 (0x68) — 112 Register (Reset-/Abbruchverzögerung + DCD)

Diese Baugruppeninstanz übermittelt den Status aller 256 virtuellen Ausgänge und Fehler und stellt die erforderlichen Feedback-Informationen für die Ausführung virtueller Reset- und Abbruchverzögerungen zur Verfügung. Des Weiteren übermittelt Sie die Leistungs- und Statusinformationen zu DCD-Geräten.

WORD #	WORD NAME	DATENTYP
0	VO1–VO16 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
1	VO17–VO32 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
2	VO33–VO48 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
3	VO49–VO64 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
4	VO65–VO80 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
5	VO81–VO96 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
6	VO97–VO112 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
7	VO113–VO128 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
8	VO129–VO144 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
9	VO145–VO160 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
10	VO161–VO176 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
11	VO177–VO192 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
12	VO193–VO208 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
13	VO209–VO224 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
14	VO225–VO240 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
15	VO241–VO256 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
16	Fehlerbits für VO1–VO16 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
17	Fehlerbits für VO17–VO32 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
18	Fehlerbits für VO33–VO48 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
19	Fehlerbits für VO49–VO64 (siehe Flags auf Seite 188)	16-Bit-Ganzzahl
20	Fehlerbits für VO65–VO80 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
21	Fehlerbits für VO81–VO96 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
22	Fehlerbits für VO97–VO112 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
23	Fehlerbits für VO113–VO128 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
24	Fehlerbits für VO129–VO144 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
25	Fehlerbits für VO145–VO160 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
26	Fehlerbits für VO161–VO176 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
27	Fehlerbits für VO177–VO192 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl



WORD #	WORD NAME	DATENTYP
28	Fehlerbits für VO193–VO208 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
29	Fehlerbits für VO209–VO224 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
30	Fehlerbits für VO225–VO240 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
31	Fehlerbits für VO241–VO256 (siehe Erweiterte Flags auf Seite 189)	16-Bit-Ganzzahl
32	Virtuelle Reset-/Abbruchverzögerung (1–16) Feedback [RCD- Feedback Registerbits] (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 52)	16-Bit-Ganzzahl
33	reserviert	16-Bit-Ganzzahl
34	RCD-Auslösecode Feedback [RCD-Aktivierung Feedbackregister] (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 52)	16-Bit-Ganzzahl
35–36	DCD-Systemstatus – Reihe 1 Geräteanzahl	32-Bit-Ganzzahl
37–38	DCD-Systemstatus – Reihe 2 Geräteanzahl	32-Bit-Ganzzahl
39–40	DCD-Systemstatus – Reihe 1 Gerät-Ein/Aus-Status	32-Bit-Ganzzahl
41–42	DCD-Systemstatus – Reihe 2 Gerät-Ein/Aus-Status	32-Bit-Ganzzahl
43–44	DCD-Systemstatus – Reihe 1 Fehlerstatus	32-Bit-Ganzzahl
45–46	DCD-Systemstatus – Reihe 2 Fehlerstatus	32-Bit-Ganzzahl
47–48	DCD-Systemstatus – Reihe 1 Betätiger im Randbereich	32-Bit-Ganzzahl
49–50	DCD-Systemstatus – Reihe 2 Betätiger im Randbereich	32-Bit-Ganzzahl
51–52	DCD-Systemstatus – Reihe 1 Warnstatus	32-Bit-Ganzzahl
53–54	DCD-Systemstatus – Reihe 2 Warnstatus	32-Bit-Ganzzahl
55–56	DCD-Systemstatus – Reihe 1 Resetstatus	32-Bit-Ganzzahl
57–58	DCD-Systemstatus – Reihe 2 Resetstatus	32-Bit-Ganzzahl
59–60	DCD-Systemstatus – Reihe 1 Auslöser erkannt	32-Bit-Ganzzahl
61–62	DCD-Systemstatus – Reihe 2 Auslöser erkannt	32-Bit-Ganzzahl
63–64	DCD-Systemstatus – Reihe 1 Systemstatus	32-Bit-Ganzzahl
65–66	DCD-Systemstatus – Reihe 2 Systemstatus	32-Bit-Ganzzahl
67–99	reserviert	16-Bit-Ganzzahl
100	DCD-Leseanfrage Bestätigung	16-Bit-Ganzzahl
101	DCD-Reihe (angefragt) Bestätigung	16-Bit-Ganzzahl
102	DCD-Gerät (angefragt) Bestätigung	16-Bit-Ganzzahl
103–112	Spezifische Daten einzelner DCD-Geräte (siehe Spezifische Daten einzelner DCD-Geräte auf Seite 219)	16-Bit-Ganzzahl

Abbildung 142: SPS-Eingang Baugruppeninstanz 104 (0–68) — Sicherheitsauswertung-Ausgänge T > O



12.4.11 Fehlerbeispiele

Die folgende Abbildung zeigt einen Fehler aus dem Fehlerprotokoll der Konfigurationssoftware der Sicherheitsauswertung.

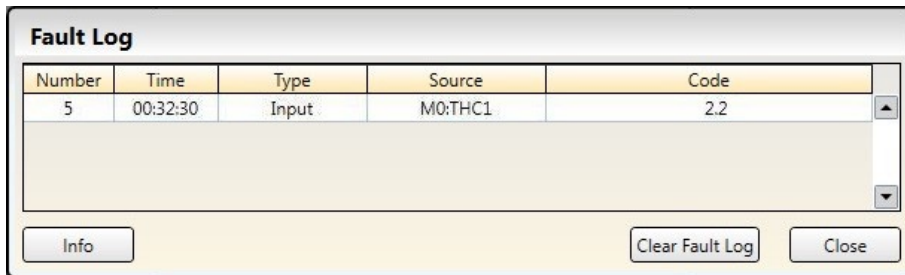


Abbildung 143: Fehlerprotokoll mit 1 Fehler

Die folgende Abbildung zeigt denselben Fehler, wie in den Ethernet/IP-Registern zu sehen ist.

-	SCx oder SCR P: I	{...}	{...}		AB:ETHER
-	SCx oder SCR P: I.Data	{...}	{...}	Dezimal	INT[150]
+	SCx oder SCR P: I.Data[0]	1950		Dezimal	INT
+	SCx oder SCR P: I.Data[1]	0		Dezimal	INT
+	SCx oder SCR P: I.Data[2]	4		Dezimal	INT
+	SCx oder SCR P: I.Data[3]	0		Dezimal	INT
+	SCx oder SCR P: I.Data[4]	'HT'		ASCII	INT
+	SCx oder SCR P: I.Data[5]	'1C'		ASCII	INT
+	SCx oder SCR P: I.Data[6]	0		Dezimal	INT
+	SCx oder SCR P: I.Data[7]	0		Dezimal	INT
+	SCx oder SCR P: I.Data[8]	0		Dezimal	INT
+	SCx oder SCR P: I.Data[9]	0		Dezimal	INT
+	SCx oder SCR P: I.Data[10]	2		Dezimal	INT
+	SCx oder SCR P: I.Data[11]	2		Dezimal	INT
+	SCx oder SCR P: I.Data[12]	202		Dezimal	INT
+	SCx oder SCR P: I.Data[13]	34		Dezimal	INT
+	SCx oder SCR P: I.Data[14]	1		Dezimal	INT

Abbildung 144: EtherNet/IP-Register mit 1 Fehler

Beachten Sie das ControllLogix-Stringformat, in dem die ASCII-Zeichen angegeben sind: zwei pro Register, abwärts. „THC1“ wird „HT“ in Register 4, gefolgt von „1C“ in Register 5.

Fehler-Nummer 202 = Fehlercode 2.2 (Simultanitätsfehler). Weitere Informationen zu Fehlern finden Sie unter „15.5 SCx-Fehlercode-Tabelle“ auf Seite 243.

Die folgende Abbildung zeigt zwei Fehler im Fehlerprotokoll der SCR P-Software.

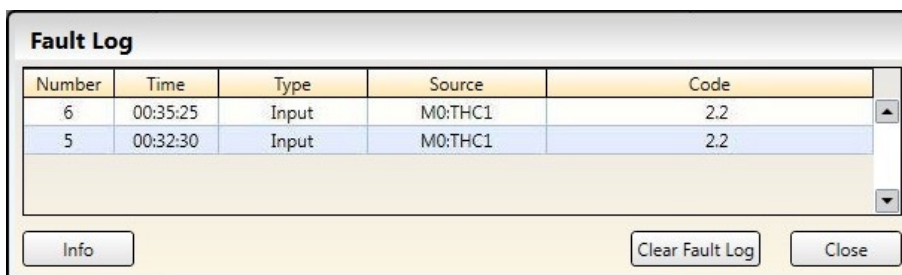


Abbildung 145: Fehlerprotokoll mit zwei Fehlern



Die folgende Abbildung zeigt die beiden gleichen Fehler in den SPS-Registern. Dabei wird der neuere Fehler Nr. 2 in der Liste vor dem Fehler Nr. 1 angezeigt

[-] SCx: I		{...}	{...}		AB:ETHER_...
[-] SCx: I.Data		{...}	{...}	Dezimal	INT[150]
[+] SCx: I.Data[0]	Zeitstempel	2125	Fehler Nr. 2	Dezimal	INT
[+] SCx: I.Data[1]		0		Dezimal	INT
[+] SCx: I.Data[2]	E/A oder Systemlänge	4		Dezimal	INT
[+] SCx: I.Data[3]	(Anzahl der ASCII-Zeichen	0		Dezimal	INT
[+] SCx: I.Data[4]	E/A oder Systemlänge (Leerzeichen für 12 der ASCII-Zeichen	'HT'		ASCII	INT
[+] SCx: I.Data[5]		'1C'		ASCII	INT
[+] SCx: I.Data[6]		0		Dezimal	INT
[+] SCx: I.Data[7]		0		Dezimal	INT
[+] SCx: I.Data[8]		0		Dezimal	INT
[+] SCx: I.Data[9]		0		Dezimal	INT
[+] SCx: I.Data[10]	Fehlercode	2		Dezimal	INT
[+] SCx: I.Data[11]	Erweiterter Fehlercode Falscher	2		Dezimal	INT
[+] SCx: I.Data[12]	Fehlermeldungsindex	202		Dezimal	INT
[+] SCx: I.Data[13]	Reserviert	34		Dezimal	INT
[+] SCx: I.Data[14]		1	Dezimal	INT	
[+] SCx: I.Data[15]	Zeitstempel	1950	Fehler Nr. 1	Dezimal	INT
[+] SCx: I.Data[16]		0		Dezimal	INT
[+] SCx: I.Data[17]	E/A oder Systemlänge	4		Dezimal	INT
[+] SCx: I.Data[18]	(Anzahl der ASCII-Zeichen	0		Dezimal	INT
[+] SCx: I.Data[19]	E/A oder Systemlänge (Leerzeichen für 12 der ASCII-Zeichen	'HT'		ASCII	INT
[+] SCx: I.Data[20]		'1C'		ASCII	INT
[+] SCx: I.Data[21]		0		Dezimal	INT
[+] SCx: I.Data[22]		0		Dezimal	INT
[+] SCx: I.Data[23]		0		Dezimal	INT
[+] SCx: I.Data[24]		0		Dezimal	INT
[+] SCx: I.Data[25]	Fehlercode	2		Dezimal	INT
[+] SCx: I.Data[26]	Erweiterter Fehlercode Falscher	2		Dezimal	INT
[+] SCx: I.Data[27]	Fehlermeldungsindex	202		Dezimal	INT
[+] SCx: I.Data[28]	Reserviert	34		Dezimal	INT
[+] SCx: I.Data[29]		1	Dezimal	INT	

Tabelle 11: EtherNet/IP-Register mit zwei Fehlern



12.4.12 Flags

Die unten definierten Wörter 0 bis 7 werden in den Baugruppeninstanzen 100, 101 und 103 als die ersten 8 Wörter angezeigt.

Bit-Position															
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
VO16	VO15	VO14	VO13	VO12	VO11	VO10	VO9	VO8	VO7	VO6	VO5	VO4	VO3	VO2	VO1

Tabelle 12: Word Nr. 0, Virtueller Ausgang 1–16

Bit-Position															
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
VO32	VO31	VO30	VO29	VO28	VO27	VO26	VO25	VO24	VO23	VO22	VO21	VO20	VO19	VO18	VO17

Tabelle 13: Word Nr. 1, Virtueller Ausgang 17–32

Bit-Position															
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
VO48	VO47	VO46	VO45	VO44	VO43	VO42	VO41	VO40	VO39	VO38	VO37	VO36	VO35	VO34	VO33

Tabelle 14: Word Nr. 2, Virtueller Ausgang 33–48

Bit-Position															
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
VO64	VO63	VO62	VO61	VO60	VO59	VO58	VO57	VO56	VO55	VO54	VO53	VO52	VO51	VO50	VO49

Tabelle 15: Word Nr. 3, Virtueller Ausgang 49–64

Hinweis: Nicht jeder virtuelle Ausgang hat ein definiertes Fehlerflag.

Bit-Position															
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
VO16	VO15	VO14	VO13	VO12	VO11	VO10	VO9	VO8	VO7	VO6	VO5	VO4	VO3	VO2	VO1

Tabelle 16: Word Nr. 4, Fehlerflagbits für virtuellen Ausgang 1–16

Hinweis: Nicht jeder virtuelle Ausgang hat ein definiertes Fehlerflag.

Bit-Position															
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
VO32	VO31	VO30	VO29	VO28	VO27	VO26	VO25	VO24	VO23	VO22	VO21	VO20	VO19	VO18	VO17

Tabelle 17: Word Nr. 5, Fehlerflagbits für virtuellen Ausgang 17–32

Hinweis: Nicht jeder virtuelle Ausgang hat ein definiertes Fehlerflag.

Bit-Position															
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
VO48	VO47	VO46	VO45	VO44	VO43	VO42	VO41	VO40	VO39	VO38	VO37	VO36	VO35	VO34	VO33

Tabelle 18: Word Nr. 6, Fehlerflagbits für virtuellen Ausgang 33–48



Bit-Position															
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
VO64	VO63	VO62	VO61	VO60	VO59	VO58	VO57	VO56	VO55	VO54	VO53	VO52	VO51	VO50	VO49

Tabelle 19: Word Nr. 7, Fehlerflagbits für virtuellen Ausgang 49–64



Hinweis: Nicht jeder virtuelle Ausgang hat ein definiertes Fehlerflag.

12.4.13 Erweiterte Flags

Zusätzlich zu den oben aufgeführten ersten 64 virtuellen Ausgängen, wurden für die Baugruppeninstanz 103 weitere 192 virtuelle Ausgänge hinzugefügt (insgesamt 256). Die Fehlerflagbits verschieben sich nach unten, um alle 256 Ausgänge gesammelt hintereinander zu übertragen.

Die Wörter 0 bis 3 sind wie unter Flags auf Seite 188 abgebildet identisch. Im Falle der Baugruppeninstanz 103 werden die folgenden Änderungen gemacht:

- Word Nr. 4 – Virtuelle Ausgänge 65 bis 80 mit VO65 in Bit 0 und VO80 in Bit 15
- Word Nr. 5 – Virtuelle Ausgänge 81 bis 96 mit VO81 in Bit 0 und VO96 in Bit 15
- Word Nr. 6 – Virtuelle Ausgänge 97 bis 112 mit VO97 in Bit 0 und VO112 in Bit 15
- Word Nr. 7 – Virtuelle Ausgänge 113 bis 128 mit VO113 in Bit 0 und VO128 in Bit 15
- Word Nr. 8 – Virtuelle Ausgänge 129 bis 144 mit VO129 in Bit 0 und VO144 in Bit 15
- Word Nr. 9 – Virtuelle Ausgänge 145 bis 160 mit VO145 in Bit 0 und VO160 in Bit 15
- Word Nr. 10 – Virtuelle Ausgänge 161 bis 176 mit VO161 in Bit 0 und VO176 in Bit 15
- Word Nr. 11 – Virtuelle Ausgänge 177 bis 192 mit VO177 in Bit 0 und VO192 in Bit 15
- Word Nr. 12 – Virtuelle Ausgänge 193 bis 208 mit VO193 in Bit 0 und VO208 in Bit 15
- Word Nr. 13 – Virtuelle Ausgänge 209 bis 224 mit VO209 in Bit 0 und VO224 in Bit 15
- Word Nr. 14 – Virtuelle Ausgänge 225 bis 240 mit VO225 in Bit 0 und VO240 in Bit 15
- Word Nr. 15 – Virtuelle Ausgänge 241 bis 256 mit VO241 in Bit 0 und VO256 in Bit 15
- Word Nr. 16 bis Nr. 19 sind wie unter Flags auf Seite 188 dargestellt die gleichen wie Word Nr. 4 bis Nr. 7
- Word Nr. 20 – Fehlerbits für VO65 bis VO80 mit Fehler VO65 in Bit 0 und VO80 in Bit 15
- ...
- Word Nr. 31 – Fehlerbits für VO241 bis VO256 mit Fehler VO241 in Bit 0 und VO256 in Bit 15



12.5 Modbus/TCP

Das Modbus/TCP-Protokoll bietet die Möglichkeit, Geräteinformationen anhand von Registern und Spulenblöcken, welche vom Slave-Gerät definiert werden, zu übertragen.

In diesem Abschnitt werden Register und Spulenblöcke der Sicherheitsauswertung definiert. Gemäß Spezifikation verwendet Modbus/TCP den TCP-Port 502.

Anhand der folgenden Register werden Ausgangswerte von der Sicherheitsauswertung an die SPS gesendet.

Die Informationen in diesen Registern können als Eingangsregister (30000) mit dem Modbus-Funktionscode 04 (Eingangsregister lesen) gelesen werden. Dieselben Werte können auch als Haltereister (40000) mit dem Modbus-Funktionscode 03 (Haltereister lesen) gelesen werden. Die Statusinformationen für alle virtuellen Ausgänge und den entsprechenden Fehlerflags, die in den ersten 8 Registern enthalten sind, können auch als Eingänge (10000) mit dem Modbus-Funktionscode 02 (Eingangsstatus lesen) gelesen werden.

12.5.1 Die ersten 64 virtuellen Ausgänge und virtuellen Ausgangsfehler (Eingänge 10001–10128)

Eingang Nr.	NAME	Eingang Nr.	NAME
10001	VO1	10065	VO1-Fehlerbit
10002	VO2	10066	VO2-Fehlerbit
10003	VO3	10067	VO3-Fehlerbit
...
10063	VO63	10127	VO63-Fehlerbit
10064	VO64	10128	VO64-Fehlerbit

Tabelle 20: : 02: Eingangsstatus lesen

12.5.2 Alle 256 virtuellen Ausgänge und virtuellen Ausgangsfehler. (Eingänge 11001–11256, 12001–12256)

Eingang Nr.	NAME	Eingang Nr.	NAME
11001	VO1	12001	VO1-Fehlerbit
11002	VO2	12002	VO2-Fehlerbit
11003	VO3	12003	VO3-Fehlerbit
...
11255	VO255	12255	VO255-Fehlerbit
11256	VO256	12256	VO256-Fehlerbit

Tabelle 21: 02: Eingangsstatus lesen

12.5.3 Virtuelle Eingänge, virtuelle Reset-/Abbruchverzögerung und Feedback (Spulen 3001–30064, 4001–4016, Eingänge 15001–15016)

Siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 52.

Eingang Nr.	NAME	Eingang Nr.	NAME
3001	VI1 ein/aus	15001	VRCD1 Feedback
3002	VI2 ein/aus	15002	VRCD2 Feedback
...
3064	VI 64 ein/aus	15016	VRCD16 Feedback
4001	VRCD1 ein/aus		
4002	VRCD2 ein/aus		
...	...		
4016	VRCD16 ein/aus		

Tabelle 22: 05: Einzelspule schreiben; 02: Eingangsstatus lesen



12.5.4 Sicherheitsauswertung-Ausgangsregister (Modbus/TCP-Eingangs- oder Halteregeister)

Eingangsreg. Nr.	Haltereg. Nr.	WORTNAME	DATENTYP
1	1	VO1–VO16 (siehe Flags auf Seite 198)	16-Bit-Ganzzahl
2	2	VO17–VO32 (siehe Flags auf Seite 198)	16-Bit-Ganzzahl
3	3	VO33–VO48 (siehe Flags auf Seite 198)	16-Bit-Ganzzahl
4	4	VO49–VO64 (siehe Flags auf Seite 198)	16-Bit-Ganzzahl
5	5	Fehlerbits für VO1–VO16 (siehe Flags auf Seite 198)	16-Bit-Ganzzahl
6	6	Fehlerbits für VO17–VO32 (siehe Flags auf Seite 198)	16-Bit-Ganzzahl
7	7	Fehlerbits für VO33–VO48 (siehe Flags auf Seite 198)	16-Bit-Ganzzahl
8	8	Fehlerbits für VO49–VO64 (siehe Flags auf Seite 198)	16-Bit-Ganzzahl
	9	Virtueller Eingang Ein/Aus (1–16)	16-Bit-Ganzzahl
	10	Virtueller Eingang Ein/Aus (17–32)	16-Bit-Ganzzahl
	11	Virtueller Eingang Ein/Aus (33–48)	16-Bit-Ganzzahl
	12	Virtueller Eingang Ein/Aus (49–64)	16-Bit-Ganzzahl
13–16	13–16	reserviert	16-Bit-Ganzzahl
	17	Virtuelle Reset-/Abbruchverzögerung (1–16) [RCD-Registerbits] (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 52)	16-Bit-Ganzzahl
18	18	reserviert	16-Bit-Ganzzahl
	19	RCD-Auslösecode [RCD-Aktivierung Register] (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 52)	16-Bit-Ganzzahl
20	20	Virtuelle Reset-/Abbruchverzögerung (1–16) Feedback [RCD-Feedback Registerbits] (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 52)	16-Bit-Ganzzahl
21	21	reserviert	16-Bit-Ganzzahl
22	22	RCD-Auslösecode Feedback [RCD-Aktivierung Feedbackregister] (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 52)	16-Bit-Ganzzahl
23–40	23–40	reserviert	16-Bit-Ganzzahl
41	41	VO1-Fehlerindex	16-Bit-Ganzzahl
42	42	VO2-Fehlerindex	16-Bit-Ganzzahl
43	43	VO3-Fehlerindex	16-Bit-Ganzzahl
44	44	VO4-Fehlerindex	16-Bit-Ganzzahl
45	45	VO5-Fehlerindex	16-Bit-Ganzzahl
46	46	VO6-Fehlerindex	16-Bit-Ganzzahl
47	47	VO7-Fehlerindex	16-Bit-Ganzzahl
48	48	VO8-Fehlerindex	16-Bit-Ganzzahl
49	49	VO9-Fehlerindex	16-Bit-Ganzzahl
50	50	VO10-Fehlerindex	16-Bit-Ganzzahl
51	51	VO11-Fehlerindex	16-Bit-Ganzzahl



Eingangsreg. Nr.	Halteleg. Nr.	WORTNAME	DATENTYP
52	52	VO12-Fehlerindex	16-Bit-Ganzzahl
53	53	VO13-Fehlerindex	16-Bit-Ganzzahl
54	54	VO14-Fehlerindex	16-Bit-Ganzzahl
55	55	VO15-Fehlerindex	16-Bit-Ganzzahl
56	56	VO16-Fehlerindex	16-Bit-Ganzzahl
57	57	VO17-Fehlerindex	16-Bit-Ganzzahl
58	58	VO18-Fehlerindex	16-Bit-Ganzzahl
59	59	VO19-Fehlerindex	16-Bit-Ganzzahl
60	60	VO20-Fehlerindex	16-Bit-Ganzzahl
61	61	VO21-Fehlerindex	16-Bit-Ganzzahl
62	62	VO22-Fehlerindex	16-Bit-Ganzzahl
63	63	VO23-Fehlerindex	16-Bit-Ganzzahl
64	64	VO24-Fehlerindex	16-Bit-Ganzzahl
65	65	VO25-Fehlerindex	16-Bit-Ganzzahl
66	66	VO26-Fehlerindex	16-Bit-Ganzzahl
67	67	VO27-Fehlerindex	16-Bit-Ganzzahl
68	68	VO28-Fehlerindex	16-Bit-Ganzzahl
69	69	VO29-Fehlerindex	16-Bit-Ganzzahl
70	70	VO30-Fehlerindex	16-Bit-Ganzzahl
71	71	VO31-Fehlerindex	16-Bit-Ganzzahl
72	72	VO32-Fehlerindex	16-Bit-Ganzzahl
73	73	VO33-Fehlerindex	16-Bit-Ganzzahl
74	74	VO34-Fehlerindex	16-Bit-Ganzzahl
75	75	VO35-Fehlerindex	16-Bit-Ganzzahl
76	76	VO36-Fehlerindex	16-Bit-Ganzzahl
77	77	VO37-Fehlerindex	16-Bit-Ganzzahl
78	78	VO38-Fehlerindex	16-Bit-Ganzzahl
79	79	VO39-Fehlerindex	16-Bit-Ganzzahl
80	80	VO40-Fehlerindex	16-Bit-Ganzzahl
81	81	VO41-Fehlerindex	16-Bit-Ganzzahl
82	82	VO42-Fehlerindex	16-Bit-Ganzzahl
83	83	VO43-Fehlerindex	16-Bit-Ganzzahl
84	84	VO44-Fehlerindex	16-Bit-Ganzzahl
85	85	VO45-Fehlerindex	16-Bit-Ganzzahl
86	86	VO46-Fehlerindex	16-Bit-Ganzzahl
87	87	VO47-Fehlerindex	16-Bit-Ganzzahl
88	88	VO48-Fehlerindex	16-Bit-Ganzzahl
89	89	VO49-Fehlerindex	16-Bit-Ganzzahl
90	90	VO50-Fehlerindex	16-Bit-Ganzzahl
91	91	VO51-Fehlerindex	16-Bit-Ganzzahl
92	92	VO52-Fehlerindex	16-Bit-Ganzzahl
93	93	VO53-Fehlerindex	16-Bit-Ganzzahl
94	94	VO54-Fehlerindex	16-Bit-Ganzzahl



Eingangsreg. Nr.	Haltereg. Nr.	WORTNAME	DATENTYP
95	95	VO55-Fehlerindex	16-Bit-Ganzzahl
96	96	VO56-Fehlerindex	16-Bit-Ganzzahl
97	97	VO57-Fehlerindex	16-Bit-Ganzzahl
98	98	VO58-Fehlerindex	16-Bit-Ganzzahl
99	99	VO59-Fehlerindex	16-Bit-Ganzzahl
100	100	VO60-Fehlerindex	16-Bit-Ganzzahl
101	101	VO61-Fehlerindex	16-Bit-Ganzzahl
102	102	VO62-Fehlerindex	16-Bit-Ganzzahl
103	103	VO63-Fehlerindex	16-Bit-Ganzzahl
104	104	VO64-Fehlerindex	16-Bit-Ganzzahl
105-106	105-106	Vollständiger VO1-Fehlercode	32-Bit-Ganzzahl
107-108	107-108	Vollständiger VO2-Fehlercode	32-Bit-Ganzzahl
109-110	109-110	Vollständiger VO3-Fehlercode	32-Bit-Ganzzahl
111-112	111-112	Vollständiger VO4-Fehlercode	32-Bit-Ganzzahl
113-114	113-114	Vollständiger VO5-Fehlercode	32-Bit-Ganzzahl
115-116	115-116	Vollständiger VO6-Fehlercode	32-Bit-Ganzzahl
117-118	117-118	Vollständiger VO7-Fehlercode	32-Bit-Ganzzahl
119-120	119-120	Vollständiger VO8-Fehlercode	32-Bit-Ganzzahl
121-122	121-122	Vollständiger VO9-Fehlercode	32-Bit-Ganzzahl
123-124	123-124	Vollständiger VO10-Fehlercode	32-Bit-Ganzzahl
125-126	125-126	Vollständiger VO11-Fehlercode	32-Bit-Ganzzahl
127-128	127-128	Vollständiger VO12-Fehlercode	32-Bit-Ganzzahl
129-130	129-130	Vollständiger VO13-Fehlercode	32-Bit-Ganzzahl
131-132	131-132	Vollständiger VO14-Fehlercode	32-Bit-Ganzzahl
133-134	133-134	Vollständiger VO15-Fehlercode	32-Bit-Ganzzahl
135-136	135-136	Vollständiger VO16-Fehlercode	32-Bit-Ganzzahl
137-138	137-138	Vollständiger VO17-Fehlercode	32-Bit-Ganzzahl
139-140	139-140	Vollständiger VO18-Fehlercode	32-Bit-Ganzzahl
141-142	141-142	Vollständiger VO19-Fehlercode	32-Bit-Ganzzahl
143-144	143-144	Vollständiger VO20-Fehlercode	32-Bit-Ganzzahl
145-146	145-146	Vollständiger VO21-Fehlercode	32-Bit-Ganzzahl
147-148	147-148	Vollständiger VO22-Fehlercode	32-Bit-Ganzzahl
149-150	149-150	Vollständiger VO23-Fehlercode	32-Bit-Ganzzahl
151-152	151-152	Vollständiger VO24-Fehlercode	32-Bit-Ganzzahl
153-154	153-154	Vollständiger VO25-Fehlercode	32-Bit-Ganzzahl
155-156	155-156	Vollständiger VO26-Fehlercode	32-Bit-Ganzzahl
157-158	157-158	Vollständiger VO27-Fehlercode	32-Bit-Ganzzahl
159-160	159-160	Vollständiger VO28-Fehlercode	32-Bit-Ganzzahl
161-162	161-162	Vollständiger VO29-Fehlercode	32-Bit-Ganzzahl
163-164	163-164	Vollständiger VO30-Fehlercode	32-Bit-Ganzzahl
165-166	165-166	Vollständiger VO31-Fehlercode	32-Bit-Ganzzahl
167-168	167-168	Vollständiger VO32-Fehlercode	32-Bit-Ganzzahl
169-170	169-170	Vollständiger VO33-Fehlercode	32-Bit-Ganzzahl
171-172	171-172	Vollständiger VO34-Fehlercode	32-Bit-Ganzzahl



Eingangsreg. Nr.	Haltereg. Nr.	WORTNAME	DATENTYP
173–174	173–174	Vollständiger VO35-Fehlercode	32-Bit-Ganzzahl
175–176	175–176	Vollständiger VO36-Fehlercode	32-Bit-Ganzzahl
177–178	177–178	Vollständiger VO37-Fehlercode	32-Bit-Ganzzahl
179–180	179–180	Vollständiger VO38-Fehlercode	32-Bit-Ganzzahl
181–182	181–182	Vollständiger VO39-Fehlercode	32-Bit-Ganzzahl
183–184	183–184	Vollständiger VO40-Fehlercode	32-Bit-Ganzzahl
185–186	185–186	Vollständiger VO41-Fehlercode	32-Bit-Ganzzahl
187–188	187–188	Vollständiger VO42-Fehlercode	32-Bit-Ganzzahl
189–190	189–190	Vollständiger VO43-Fehlercode	32-Bit-Ganzzahl
191–192	191–192	Vollständiger VO44-Fehlercode	32-Bit-Ganzzahl
193–194	193–194	Vollständiger VO45-Fehlercode	32-Bit-Ganzzahl
195–196	195–196	Vollständiger VO46-Fehlercode	32-Bit-Ganzzahl
197–198	197–198	Vollständiger VO47-Fehlercode	32-Bit-Ganzzahl
199–200	199–200	Vollständiger VO48-Fehlercode	32-Bit-Ganzzahl
201–202	201–202	Vollständiger VO49-Fehlercode	32-Bit-Ganzzahl
203–204	203–204	Vollständiger VO50-Fehlercode	32-Bit-Ganzzahl
205–206	205–206	Vollständiger VO51-Fehlercode	32-Bit-Ganzzahl
207–208	207–208	Vollständiger VO52-Fehlercode	32-Bit-Ganzzahl
209–210	209–210	Vollständiger VO53-Fehlercode	32-Bit-Ganzzahl
211–212	211–212	Vollständiger VO54-Fehlercode	32-Bit-Ganzzahl
213–214	213–214	Vollständiger VO55-Fehlercode	32-Bit-Ganzzahl
215–216	215–216	Vollständiger VO56-Fehlercode	32-Bit-Ganzzahl
217–218	217–218	Vollständiger VO57-Fehlercode	32-Bit-Ganzzahl
219–220	219–220	Vollständiger VO58-Fehlercode	32-Bit-Ganzzahl
221–222	221–222	Vollständiger VO59-Fehlercode	32-Bit-Ganzzahl
223–224	223–224	Vollständiger VO60-Fehlercode	32-Bit-Ganzzahl
225–226	225–226	Vollständiger VO61-Fehlercode	32-Bit-Ganzzahl
227–228	227–228	Vollständiger VO62-Fehlercode	32-Bit-Ganzzahl
229–230	229–230	Vollständiger VO63-Fehlercode	32-Bit-Ganzzahl
231–232	231–232	Vollständiger VO64-Fehlercode	32-Bit-Ganzzahl
233–234	233–234	Fehler Nr. 1 Zeitstempel	32-Bit-Ganzzahl
235–242	235–242	Fehler Nr. 1 E/A- oder Systemname	Doppelwortlänge + 12-ASCII-Zeichen
243	243	Fehler Nr. 1 Fehlercode	16-Bit-Ganzzahl
244	244	Fehler Nr. 1 Erweiterter Fehlercode	16-Bit-Ganzzahl
245	245	Fehler Nr. 1 Fehlermeldungsindex	16-Bit-Ganzzahl
246–247	246–247	reserviert	16-Bit-Ganzzahl
248–249	248–249	Fehler Nr. 2 Zeitstempel	32-Bit-Ganzzahl
250–257	250–257	Fehler Nr. 2 E/A- oder Systemname	Doppelwortlänge + 12-ASCII-Zeichen
258	258	Fehler Nr. 2 Fehlercode	16-Bit-Ganzzahl
259	259	Fehler Nr. 2 Erweiterter Fehlercode	16-Bit-Ganzzahl
260	260	Fehler Nr. 2 Fehlermeldungsindex	16-Bit-Ganzzahl
261–262	261–262	reserviert	16-Bit-Ganzzahl
263–264	263–264	Fehler Nr. 3 Zeitstempel	32-Bit-Ganzzahl



Eingangsreg. Nr.	Haltereg. Nr.	WORTNAME	DATENTYP
265–272	265–272	Fehler Nr. 3 E/A- oder Systemname	Doppelwortlänge + 12-ASCII-Zeichen
273	273	Fehler Nr. 3 Fehlercode	16-Bit-Ganzzahl
274	274	Fehler Nr. 3 Erweiterter Fehlercode	16-Bit-Ganzzahl
275	275	Fehler Nr. 3 Fehlermeldungsindex	16-Bit-Ganzzahl
276–277	276–277	reserviert	16-Bit-Ganzzahl
278–279	278–279	Fehler Nr. 4 Zeitstempel	32-Bit-Ganzzahl
280–287	280–287	Fehler Nr. 4 E/A- oder Systemname	Doppelwortlänge + 12-ASCII-Zeichen
288	288	Fehler Nr. 4 Fehlercode	16-Bit-Ganzzahl
289	289	Fehler Nr. 4 Erweiterter Fehlercode	16-Bit-Ganzzahl
290	290	Fehler Nr. 4 Fehlermeldungsindex	16-Bit-Ganzzahl
291–292	291–292	reserviert	16-Bit-Ganzzahl
293–294	293–294	Fehler Nr. 5 Zeitstempel	32-Bit-Ganzzahl
295–302	295–302	Fehler Nr. 5 E/A- oder Systemname	Doppelwortlänge + 12-ASCII-Zeichen
303	303	Fehler Nr. 5 Fehlercode	16-Bit-Ganzzahl
304	304	Fehler Nr. 5 Erweiterter Fehlercode	16-Bit-Ganzzahl
305	305	Fehler Nr. 5 Fehlermeldungsindex	16-Bit-Ganzzahl
306–307	306–307	reserviert	16-Bit-Ganzzahl
308–309	308–309	Fehler Nr. 6 Zeitstempel	32-Bit-Ganzzahl
310–317	310–317	Fehler Nr. 6 E/A- oder Systemname	Doppelwortlänge + 12-ASCII-Zeichen
318	318	Fehler Nr. 6 Fehlercode	16-Bit-Ganzzahl
319	319	Fehler Nr. 6 Erweiterter Fehlercode	16-Bit-Ganzzahl
320	320	Fehler Nr. 6 Fehlermeldungsindex	16-Bit-Ganzzahl
321–322	321–322	reserviert	16-Bit-Ganzzahl
323–324	323–324	Fehler Nr. 7 Zeitstempel	32-Bit-Ganzzahl
325–332	325–332	Fehler Nr. 7 E/A- oder Systemname	Doppelwortlänge + 12-ASCII-Zeichen
333	333	Fehler Nr. 7 Fehlercode	16-Bit-Ganzzahl
334	334	Fehler Nr. 7 Erweiterter Fehlercode	16-Bit-Ganzzahl
335	335	Fehler Nr. 7 Fehlermeldungsindex	16-Bit-Ganzzahl
336–337	336–337	reserviert	16-Bit-Ganzzahl
338–339	338–339	Fehler Nr. 8 Zeitstempel	32-Bit-Ganzzahl
340–347	340–347	Fehler Nr. 8 E/A- oder Systemname	Doppelwortlänge + 12-ASCII-Zeichen
348	348	Fehler Nr. 8 Fehlercode	16-Bit-Ganzzahl
349	349	Fehler Nr. 8 Erweiterter Fehlercode	16-Bit-Ganzzahl
350	350	Fehler Nr. 8 Fehlermeldungsindex	16-Bit-Ganzzahl
351–352	351–352	reserviert	16-Bit-Ganzzahl
353–354	353–354	Fehler Nr. 9 Zeitstempel	32-Bit-Ganzzahl
355–362	355–362	Fehler Nr. 9 E/A- oder Systemname	Doppelwortlänge + 12-ASCII-Zeichen
363	363	Fehler Nr. 9 Fehlercode	16-Bit-Ganzzahl
364	364	Fehler Nr. 9 Erweiterter Fehlercode	16-Bit-Ganzzahl
365	365	Fehler Nr. 9 Fehlermeldungsindex	16-Bit-Ganzzahl
366–367	366–367	reserviert	16-Bit-Ganzzahl
368–369	368–369	Fehler Nr. 10 Zeitstempel	32-Bit-Ganzzahl



Eingangsreg. Nr.	Haltereg. Nr.	WORTNAME	DATENTYP
370–377	370–377	Fehler Nr. 10 E/A- oder Systemname	Doppelwortlänge + 12-ASCII-Zeichen
378	378	Fehler Nr. 10 Fehlercode	16-Bit-Ganzzahl
379	379	Fehler Nr. 10 Erweiterter Fehlercode	16-Bit-Ganzzahl
380	380	Fehler Nr. 10 Fehlermeldungsindex	16-Bit-Ganzzahl
381–382	381–382	reserviert	16-Bit-Ganzzahl
383–384	383–384	Sekunden seit Systemstart	32-Bit-Ganzzahl
385	385	Betriebsart	16-Bit-Ganzzahl
386–395	386–395	ConfigName	Doppelwortlänge + 16-ASCII-Zeichen
396–397	396–397	Konfig. CRC	32-Bit-Ganzzahl
398–900	398–900	reserviert	16-Bit-Ganzzahl
901	901	VO1–VO16 (siehe Flags auf Seite 198)	16-Bit-Ganzzahl
902	902	VO17–VO32 (siehe Flags auf Seite 198)	16-Bit-Ganzzahl
903	903	VO33–VO48 (siehe Flags auf Seite 198)	16-Bit-Ganzzahl
904	904	VO49–VO64 (siehe Flags auf Seite 198)	16-Bit-Ganzzahl
905	905	VO65–VO80 (siehe Erweiterte Flags auf Seite 199)	16-Bit-Ganzzahl
906	906	VO81–VO96 (siehe Erweiterte Flags auf Seite 199)	16-Bit-Ganzzahl
907	907	VO97–VO112 (siehe Erweiterte Flags auf Seite 199)	16-Bit-Ganzzahl
908	908	VO113–VO128 (siehe Erweiterte Flags auf Seite 199)	16-Bit-Ganzzahl
909	909	VO129–VO144 (siehe Erweiterte Flags auf Seite 199)	16-Bit-Ganzzahl
910	910	VO145–VO160 (siehe Erweiterte Flags auf Seite 199)	16-Bit-Ganzzahl
911	911	VO161–VO176 (siehe Erweiterte Flags auf Seite 199)	16-Bit-Ganzzahl
912	912	VO177–VO192 (siehe Erweiterte Flags auf Seite 199)	16-Bit-Ganzzahl
913	913	VO193–VO208 (siehe Erweiterte Flags auf Seite 199)	16-Bit-Ganzzahl
914	914	VO209–VO224 (siehe Erweiterte Flags auf Seite 199)	16-Bit-Ganzzahl
915	915	VO225–VO240 (siehe Erweiterte Flags auf Seite 199)	16-Bit-Ganzzahl
916	916	VO241–VO256 (siehe Erweiterte Flags auf Seite 199)	16-Bit-Ganzzahl
917	917	Fehlerbits für VO1–VO16 (siehe Flags auf Seite 198)	16-Bit-Ganzzahl
918	918	Fehlerbits für VO17–VO32 (siehe Flags auf Seite 198)	16-Bit-Ganzzahl
919	919	Fehlerbits für VO33–VO48 (siehe Flags auf Seite 198)	16-Bit-Ganzzahl
920	920	Fehlerbits für VO49–VO64 (siehe Flags auf Seite 198)	16-Bit-Ganzzahl
921	921	Fehlerbits für VO65–VO80 (siehe Erweiterte Flags auf Seite 199)	16-Bit-Ganzzahl



Eingangsreg. Nr.	Haltereg. Nr.	WORTNAME	DATENTYP
922	922	Fehlerbits für VO81–VO96 (siehe Erweiterte Flags auf Seite 199)	16-Bit-Ganzzahl
923	923	Fehlerbits für VO97–VO112 (siehe Erweiterte Flags auf Seite 199)	16-Bit-Ganzzahl
924	924	Fehlerbits für VO113–VO128 (siehe Erweiterte Flags auf Seite 199)	16-Bit-Ganzzahl
925	925	Fehlerbits für VO129–VO144 (siehe Erweiterte Flags auf Seite 199)	16-Bit-Ganzzahl
926	926	Fehlerbits für VO145–VO160 (siehe Erweiterte Flags auf Seite 199)	16-Bit-Ganzzahl
926	926	Fehlerbits für VO161–VO176 (siehe Erweiterte Flags auf Seite 199)	16-Bit-Ganzzahl
928	928	Fehlerbits für VO177–VO192 (siehe Erweiterte Flags auf Seite 199)	16-Bit-Ganzzahl
929	929	Fehlerbits für VO193–VO208 (siehe Erweiterte Flags auf Seite 199)	16-Bit-Ganzzahl
930	930	Fehlerbits für VO209–VO224 (siehe Erweiterte Flags auf Seite 199)	16-Bit-Ganzzahl
931	931	Fehlerbits für VO225–VO240 (siehe Erweiterte Flags auf Seite 199)	16-Bit-Ganzzahl
932	932	Fehlerbits für VO241–VO256 (siehe Erweiterte Flags auf Seite 199)	16-Bit-Ganzzahl
933–934	933–934	RCD-Bits Feedback (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 52)	32-Bit-Ganzzahl
935	935	RCD-Aktivierung Feedback (siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 52)	16-Bit-Ganzzahl
936	936	VO1-Fehlerindex	16-Bit-Ganzzahl
937	937	VO2-Fehlerindex	16-Bit-Ganzzahl
938	938	VO3-Fehlerindex	16-Bit-Ganzzahl
...
1190	1190	VO256-Fehlerindex	16-Bit-Ganzzahl
1191–1192	1191–1192	Vollständiger VO1-Fehlercode	32-Bit-Ganzzahl
1193–1194	1193–1194	Vollständiger VO2-Fehlercode	32-Bit-Ganzzahl
1195–1196	1195–1196	Vollständiger VO3-Fehlercode	32-Bit-Ganzzahl
1197–1198	1197–1198	Vollständiger VO4-Fehlercode	32-Bit-Ganzzahl
...
1702–1703	1702–1703	Vollständiger VO256-Fehlercode	32-Bit-Ganzzahl
1704–1705	1704–1705	DCD-Systemstatus – Reihe 1 Geräteanzahl	32-Bit-Ganzzahl
1706–1707	1706–1707	DCD-Systemstatus – Reihe 2 Geräteanzahl	32-Bit-Ganzzahl
1708–1709	1708–1709	DCD-Systemstatus – Reihe 1 Gerät-Ein/Aus-Status	32-Bit-Ganzzahl
1710–1711	1710–1711	DCD-Systemstatus – Reihe 2 Gerät-Ein/Aus-Status	32-Bit-Ganzzahl
1712–1713	1712–1713	DCD-Systemstatus – Reihe 1 Fehlerstatus	32-Bit-Ganzzahl
1714–1715	1714–1715	DCD-Systemstatus – Reihe 2 Fehlerstatus	32-Bit-Ganzzahl
1716–1717	1716–1717	DCD-Systemstatus – Reihe 1 Betätiger im Randbereich	32-Bit-Ganzzahl
1718–1719	1718–1719	DCD-Systemstatus – Reihe 2 Betätiger im Randbereich	32-Bit-Ganzzahl



Eingangsreg. Nr.	Haltereg. Nr.	WORTNAME	DATENTYP
1720-1721	1720-1721	DCD-Systemstatus – Reihe 1 Warnstatus	32-Bit-Ganzzahl
1722-1723	1722-1723	DCD-Systemstatus – Reihe 2 Warnstatus	32-Bit-Ganzzahl
1724-1725	1724-1725	DCD-Systemstatus – Reihe 1 Resetstatus	32-Bit-Ganzzahl
1726-1727	1726-1727	DCD-Systemstatus – Reihe 2 Resetstatus	32-Bit-Ganzzahl
1728-1729	1728-1729	DCD-Systemstatus – Reihe 1 Auslöser erkannt	32-Bit-Ganzzahl
1730-1731	1730-1731	DCD-Systemstatus – Reihe 2 Auslöser erkannt	32-Bit-Ganzzahl
1732-1733	1732-1733	DCD-Systemstatus – Reihe 1 Systemstatus	32-Bit-Ganzzahl
1734-1735	1734-1735	DCD-Systemstatus – Reihe 2 Systemstatus	32-Bit-Ganzzahl
1736-1768	1736-1768	reserviert	16-Bit-Ganzzahl
1769	1769	DCD-Leseanfrage Bestätigung	16-Bit-Ganzzahl
1770	1770	DCD-Reihe angefragte Bestätigung	16-Bit-Ganzzahl
1771	1771	DCD-Gerät angefragte Bestätigung	16-Bit-Ganzzahl
1772-1780	1772-1780	Spezifische Daten einzelner DCD-Geräte ²⁶	16-Bit-Ganzzahl
	1781	DCD-Leseanfrage	16-Bit-Ganzzahl
	1782	DCD-Reihe angefordert	16-Bit-Ganzzahl
	1783	DCD-Gerät angefordert	16-Bit-Ganzzahl

Tabelle 25: Ausgangsregister

12.5.5 Leistungs- und Statusinformationen zu einem einzelnen Gerät über DCD anfordern

1. Haltereister 1782: DCD-Reihenschaltung, in der das betreffende Gerät angeschlossen ist (1 oder 2) auswählen.
2. Haltereister 1783: DCD-Gerätenummer (1 bis 32) auswählen.
3. Haltereister 1781: Wechseln von 0 zu 1, um einen einmaligen Lesevorgang durchzuführen.
4. Haltereister 1772-1780: Angeforderte gerätespezifische Daten des Gerätes.

12.5.6 Flags

Die unten definierten Register 1 bis 8 werden in der Registerzuordnung als die ersten 8 Wörter angezeigt.

Dies stellt die ersten 64 virtuellen Ausgänge und die zugehörigen Fehlerflags dar. Die Informationen in diesen Registern können als Eingangsregister (30000) mit dem Modbus-Funktionscode 04 (Eingangsregister lesen) gelesen werden. Dieselben Werte können auch als Haltereister (40000) mit dem Modbus-Funktionscode 03 (Haltereister lesen) gelesen werden.

Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
VO16	VO15	VO14	VO13	VO12	VO11	VO10	VO9	VO8	VO7	VO6	VO5	VO4	VO3	VO2	VO1

Tabelle 23: Virtueller Ausgang 1-16

Eingangsregister 30001 oder Haltereister 40001 der SPS, auch Eingänge 10001-16 oder Spulen 00001-16

Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
VO32	VO31	VO30	VO29	VO28	VO27	VO26	VO25	VO24	VO23	VO22	VO21	VO20	VO19	VO18	VO17

Tabelle 24: Virtueller Ausgang 17-32

Eingangsregister 30002 oder Haltereister 40002 der SPS, auch Eingänge 10017-32 oder Spulen 00017-32



Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
VO48	VO47	VO46	VO45	VO44	VO43	VO42	VO41	VO40	VO39	VO38	VO37	VO36	VO35	VO34	VO33

Tabelle 26: Virtueller Ausgang 33–48

Eingangsregister 30003 oder Halteregeister 40003 der SPS, auch Eingänge 10033–48 oder Spulen 00033–48

Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
VO64	VO63	VO62	VO61	VO60	VO59	VO58	VO57	VO56	VO55	VO54	VO53	VO52	VO51	VO50	VO49

Tabelle 27: Virtueller Ausgang 49–64

Eingangsregister 30004 oder Halteregeister 40004 der SPS, auch Eingänge 10049–64 oder Spulen 00049–64

Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
VO16-Fehler	VO15-Fehler	VO14-Fehler	VO13-Fehler	VO12-Fehler	VO11-Fehler	VO10-Fehler	VO9-Fehler	VO8-Fehler	VO7-Fehler	VO6-Fehler	VO5-Fehler	VO4-Fehler	VO3-Fehler	VO2-Fehler	VO1-Fehler

Tabelle 31: Virtueller Ausgangsfehler 1–16

Eingangsregister 30005 oder Halteregeister 40005 der SPS, auch Eingänge 10033–48 oder Spulen 00033–48

Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
VO32-Fehler	VO31-Fehler	VO30-Fehler	VO29-Fehler	VO28-Fehler	VO27-Fehler	VO26-Fehler	VO25-Fehler	VO24-Fehler	VO23-Fehler	VO22-Fehler	VO21-Fehler	VO20-Fehler	VO19-Fehler	VO18-Fehler	VO17-Fehler

Tabelle 28: Virtueller Ausgangsfehler 17–32

Eingangsregister 30006 oder Halteregeister 40006 der SPS, auch Eingänge 10049–64 oder Spulen 00049–64

Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
VO48-Fehler	VO47-Fehler	VO46-Fehler	VO45-Fehler	VO44-Fehler	VO43-Fehler	VO42-Fehler	VO41-Fehler	VO40-Fehler	VO39-Fehler	VO38-Fehler	VO37-Fehler	VO36-Fehler	VO35-Fehler	VO34-Fehler	VO33-Fehler

Tabelle 29: Virtueller Ausgangsfehler 33–48

Eingangsregister 30007 oder Halteregeister 40007 der SPS, auch Eingänge 10033–48 oder Spulen 00033–48

Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
VO64-Fehler	VO63-Fehler	VO62-Fehler	VO61-Fehler	VO60-Fehler	VO59-Fehler	VO58-Fehler	VO57-Fehler	VO56-Fehler	VO55-Fehler	VO54-Fehler	VO53-Fehler	VO52-Fehler	VO51-Fehler	VO50-Fehler	VO49-Fehler

Tabelle 30: Tabelle 29: Virtueller Ausgangsfehler 49–64

Eingangsregister 30008 oder Halteregeister 40008 der SPS, auch Eingänge 10049–64 oder Spulen 00049–64

12.5.7 Erweiterte Flags

Auf alle 256 virtuellen Ausgänge kann, ähnlich wie unter Flags auf Seite 198 abgebildet, zugegriffen werden.

Die Eingänge 11001 bis 11256 stellen alle 256 möglichen virtuellen Ausgänge dar. Diese virtuellen Ausgänge können auch als Eingangsregister 901–916 oder Halteregeister 901–916 gelesen werden.

Die Eingänge 12001 bis 12256 sind alle 256 virtuelle Ausgangsfehler. Diese virtuellen Ausgangsfehler können auch als Eingangsregister 917–932 oder Halteregeister 917–932 gelesen werden.



12.6 PROFINET®

PROFINET®28 ist ein Datenkommunikationsprotokoll für Industrieautomatisierung und -prozesse. PROFINET IO definiert, wie Controller (E/A-Controller) und Peripheriegeräte (E/A-Geräte) Daten in Echtzeit austauschen. Die Sicherheitsauswertung von BERNSTEIN unterstützt PROFINET IO. Das Datenkommunikationsprotokoll ist TCP/IP; das Datenübertragungsmedium ist Kupferdraht; die Konformitätsklasse von PROFINET ist CC-A.29



Anmerkung: In diesem Dokument werden Ausgänge von der Sicherheitsauswertung zum Controller (SPS) als „Eingänge“ bezeichnet. Ausgänge vom Controller (SPS) zur Sicherheitsauswertung werden als „Ausgänge“ bezeichnet

12.6.1 PROFINET und die Sicherheitsauswertung

PROFINET-Echtzeitdaten werden über Steckplätze gesendet und empfangen.



Anmerkung: Die GSDML-Datei steht unter <http://www.bernstein.eu/downloads> zum Download zur Verfügung.

12.6.2 GSD-Datei (General Station Description)

Die GSD-Datei (General Station Description) enthält alle Modulinformationen, wie:

- Konfigurationsdaten
- Dateninformationen (Durchlaufzähler, Inspektionsstatus usw.)
- Diagnose

12.6.3 PROFINET IO-Datenmodell

Das PROFINET IO-Datenmodell basiert auf dem typischen, erweiterbaren Feldgerät mit einer Rückwandplatine und mit mehreren Steckplätzen. Module und Submodule können für unterschiedliche Funktionen eingefügt werden. Module werden in Steckplätze eingesteckt, Submodule in Substeckplätze. Im PROFINET IO-Datenmodell ist Steckplatz 0 Substeckplatz 1 für den Device Access Point (DAP) bzw. die Netzwerkschnittstelle reserviert. Module wie auch Submodule werden zur Steuerung des Typs und des Volumens der Daten verwendet, die an den Controller (SPS) gesendet werden.


- Ein Submodul ist in der Regel als Eingangstyp, Ausgangstyp oder kombinierter Eingangs-/Ausgangstyp ausgewiesen.
- Ein Eingangssubmodul wird zum Senden von Daten an den Controller (SPS) verwendet.
- Ein Ausgangssubmodul wird zum Empfangen von Daten vom Controller (SPS) verwendet.
- Das kombinierte Eingangs-/Ausgangssubmodul empfängt und sendet Daten in beide Richtungen.

²⁶ PROFINET® ist eine eingetragene Marke des PROFIBUS Nutzerorganisation e.V.

²⁷CC-A gewährleistet, dass das Gerät die Mindestanforderungen an Funktionalität und Interoperabilität erfüllt



12.6.4 Konfiguration der Sicherheitsauswertung für eine PROFINET IO-Verbindung

1. Verbinden Sie die Sicherheitsauswertung über ein USB-Kabel mit dem PC.
2. Öffnen Sie die Konfigurationssoftware der Sicherheitsauswertung von BERNSTEIN und klicken Sie auf die Registerkarte **Industrial- Ethernet**.
3. Wählen Sie aus der Dropdown-Liste links **Profinet** aus.
4. Klicken Sie auf , um den PROFINET-Submodulen Informationen hinzuzufügen. Tipp: Bei dieser Aufgabe kann **automatisches Konfigurieren** hilfreich sein.
5. Geben Sie das entsprechende Passwort ein, um die Konfigurations- und Netzwerkeinstellungen für die Sicherheitsauswertung zu ändern.
6. Vergewissern Sie sich, dass die Sicherheitsauswertung eine gültige und bestätigte Konfigurationsdatei hat.



Anmerkung: Wenn eine virtuelle Reset- oder Abbruchverzögerung verwendet wird, muss der Auslösecode in den **Netzwerkeinstellungen** erstellt werden. Der Code muss dann über **Senden** in den **Netzwerkeinstellungen** an den Sicherheitscontroller gesendet werden.



12.6.5 Beschreibung der Module

In dieser Tabelle ist die E/A-Richtung vom Standpunkt der SPS aus genannt.

Steckplatz	Modulfunktion	E/A	Modulname	Modulgröße (Byte)
1	Benutzerdefinierte Statusbits (0–31)	Eingehend	4 Statusbytes, Bits 0..31_1	4
2	Benutzerdefinierte Statusbits (32–63)	Eingehend	4 Statusbytes, Bits 0..31_2	4
3	Sicherheitsauswertung Fehlerbits (0–31)	Eingehend	4 Statusbytes, Bits 0..31_3	4
4	Sicherheitsauswertung Fehlerbits (32–63)	Eingehend	4 Statusbytes, Bits 0..31_4	4
5	Sicherheitsauswertung Eingangstatusbits (0–31)	Eingehend	4 Statusbytes, Bits 0..31_5	4
6	Sicherheitsauswertung Eingangstatusbits (32–63)	Eingehend	4 Statusbytes, Bits 0..31_6	4
7	Sicherheitsauswertung Eingangstatusbits (64–95)	Eingehend	4 Statusbytes, Bits 0..31_7	4
8	Sicherheitsauswertung Eingangstatusbits (96–127)	Eingehend	4 Statusbytes, Bits 0..31_8	4
9	Sicherheitsauswertung Eingangstatusbits (128–159)	Eingehend	4 Statusbytes, Bits 0..31_9	4
10	Sicherheitsauswertung Ausgangstatusbits (0–31)	Eingehend	4 Statusbytes, Bits 0..31_10	4
11	Sicherheitsauswertung Ausgangstatusbits (32–63)	Eingehend	4 Statusbytes, Bits 0..31_11	4
12	Sicherheitsauswertung Ausgangstatusbits (64–95)	Eingehend	4 Statusbytes, Bits 0..31_12	4
13	Virtueller E/A (Ein/Aus/Muting-Aktivierung) Bits (0–63)	Ausgehend	8 Byte Virtuell Ein/AUS/MA Data_1	8
14	Virtuelle Reset-/Abbruchverzögerung Bits (0–16)	Ausgehend	2 Byte RCD Data_1	2
15	Auslösecode für Reset-/Abbruchverzögerung	Ausgehend	2 Byte RCD Auslösung Code_1	2
16	Virtuelle Reset-/Abbruchverzögerung Bits (0–16) Feedback	Eingehend	RCD Data Feedback Register_1	2
17	Auslösecode für Reset-/Abbruchverzögerung Feedback	Eingehend	RCD Passcode Feedback Register_1	2
18 ³⁰	Fehlerprotokoll	Eingehend	Fehlerprotokollpuffermodul	300
19 ³⁰	Systeminformationen	Eingehend	Systeminformationsmodul	30
20	DCD-Status	Eingehend	DCD-Statusinformationsmodul	128
21	Informationen zu einzelnen DCD-Geräten	Ein-/Ausgehend	DCD-Einzelstatusinformationsmodul	24 eingehend 6 ausgehend

Tabelle 32: Zuweisung von Steckplätzen

²⁶ Das Fehlerprotokoll- und das Systeminformationsmodul werden nicht von der Standardverbindung verwendet.



12.6.5.1 Benutzerdefinierte Statusbits

Die Steckplätze 1 und 2 (64 Bits) sind immer von den benutzerdefinierten Statusbit-Modulen belegt. Diese Module umfassen beliebige Informationen der virtuellen Statusausgänge.

Die zu übertragene Informationen der Bits werden im **Industrie-Ethernet** Tab der Konfigurationssoftware festgelegt.

SPS-Eingangsdatenname	Eingangsdatentyp	SPS-Ausgangsdatenname	Ausgangsdatentyp
Benutzerdefinierte Statusbits 0–7	Byte	Entfällt	Entfällt
Benutzerdefinierte Statusbits 8–15	Byte		
Benutzerdefinierte Statusbits 16–23	Byte		
Benutzerdefinierte Statusbits 24–31	Byte		

Tabelle 33: Benutzerdefinierte Statusbits (0–31) Modul (Ident 0x100) [fest in Steckplatz 1]

SPS-Eingangsdatenname	Eingangsdatentyp	SPS-Ausgangsdatenname	Ausgangsdatentyp
Benutzerdefinierte Statusbits 32–39	Byte	Entfällt	Entfällt
Benutzerdefinierte Statusbits 40–47	Byte		
Benutzerdefinierte Statusbits 48–55	Byte		
Benutzerdefinierte Statusbits 56–63	Byte		

Tabelle 34: Benutzerdefinierte Statusbits (32–63) Modul (Ident 0x100) [fest in Steckplatz 2]

12.6.5.2 Fehlerbits

Über die Steckplätze 3 und 4 (64 Bits) werden Informationen über Fehler in der Sicherheitsauswertung übertragen.

Die zu übertragene Informationen der Bits werden im **Industrie-Ethernet** Tab der Konfigurationssoftware festgelegt.

SPS-Eingangsdatenname	Eingangsdatentyp
Fehlerbits 0–7	Byte
Fehlerbits 8–15	Byte
Fehlerbits 16–23	Byte
Fehlerbits 24–31	Byte

Tabelle 35: Sicherheitsauswertung Fehlerbits (0–31) Modul (Ident 0x100) [fest in Steckplatz 3]

SPS-Eingangsdatenname	Eingangsdatentyp	SPS-Ausgangsdatenname	Ausgangsdatentyp
Fehlerbits 32–39	Byte	Entfällt	Entfällt
Fehlerbits 40–47	Byte		
Fehlerbits 48–55	Byte		
Fehlerbits 56–63	Byte		

Tabelle 36: Sicherheitsauswertung Fehlerbits (32–63) Modul (Ident 0x100) [fest in Steckplatz 4]



12.6.5.3 Eingangstatusbits

Die Steckplätze 5 bis 9 (160 Bits) sind immer für die Eingangstatus-Informationen der Sicherheitseingänge reserviert. Die zu übertragene Informationen der Bits werden im **Industrie-Ethernet** Tab der Konfigurationssoftware festgelegt.

SPS-Eingangsdatenname	Eingangsdatentyp	SPS-Ausgangsdatenname	Ausgangsdatentyp
Eingangstatusbits 0–7	Byte	Entfällt	Entfällt
Eingangstatusbits 8–15	Byte		
Eingangstatusbits 16–23	Byte		
Eingangstatusbits 24–31	Byte		

Tabelle 37: Sicherheitsauswertung Eingangstatusbits (0–31) Modul (Ident 0x100) [fest in Steckplatz 5]

SPS-Eingangsdatenname	Eingangsdatentyp	SPS-Ausgangsdatenname	Ausgangsdatentyp
Eingangstatusbits 32–39	Byte	Entfällt	Entfällt
Eingangstatusbits 40–47	Byte		
Eingangstatusbits 48–55	Byte		
Eingangstatusbits 56–63	Byte		

Tabelle 38: Sicherheitsauswertung Eingangstatusbits (32–63) Modul (Ident 0x100) [fest in Steckplatz 6]

SPS-Eingangsdatenname	Eingangsdatentyp	SPS-Ausgangsdatenname	Ausgangsdatentyp
Eingangstatusbits 64–71	Byte	Entfällt	Entfällt
Eingangstatusbits 72–79	Byte		
Eingangstatusbits 80–87	Byte		
Eingangstatusbits 88–95	Byte		

Tabelle 39: Sicherheitsauswertung Eingangstatusbits (64–95) Modul (Ident 0x100) [fest in Steckplatz 7]

SPS-Eingangsdatenname	Eingangsdatentyp	SPS-Ausgangsdatenname	Ausgangsdatentyp
Eingangstatusbits 96–103	Byte	Entfällt	Entfällt
Eingangstatusbits 104–111	Byte		
Eingangstatusbits 112–119	Byte		
Eingangstatusbits 120–127	Byte		

Tabelle 40: Sicherheitsauswertung Eingangstatusbits (96–127) Modul (Ident 0x100) [fest in Steckplatz 8]

SPS-Eingangsdatenname	Eingangsdatentyp	SPS-Ausgangsdatenname	Ausgangsdatentyp
Eingangstatusbits 128–135	Byte	Entfällt	Entfällt
Eingangstatusbits 136–143	Byte		
Eingangstatusbits 144–151	Byte		
Eingangstatusbits 152–159	Byte		

Tabelle 41: Sicherheitsauswertung Eingangstatusbits (128–159) Modul (Ident 0x100) [fest in Steckplatz 9]



12.6.5.4 Ausgangsstatusbits

Die Steckplätze 10 bis 12 (96 Bits) sind immer für die Ausgangsstatus-Informationen der Sicherheitsausgänge reserviert. Die zu übertragene Informationen der Bits werden im **Industrie-Ethernet** Tab der Konfigurationssoftware festgelegt.

SPS-Eingangsdatenname	Eingangsdatentyp	SPS-Ausgangsdatenname	Ausgangsdatentyp
Ausgangsstatusbits 0–7	Byte	Entfällt	Entfällt
Ausgangsstatusbits 8–15	Byte		
Ausgangsstatusbits 16–23	Byte		
Ausgangsstatusbits 24–31	Byte		

Tabelle 42: Sicherheitsauswertung Ausgangsstatusbits (0–31) Modul (Ident 0x100) [fest in Steckplatz 10]

SPS-Eingangsdatenname	Eingangsdatentyp	SPS-Ausgangsdatenname	Ausgangsdatentyp
Ausgangsstatusbits 32–39	Byte	Entfällt	Entfällt
Ausgangsstatusbits 40–47	Byte		
Ausgangsstatusbits 48–55	Byte		
Ausgangsstatusbits 56–63	Byte		

Tabelle 43: Sicherheitsauswertung Ausgangsstatusbits (32–63) Modul (Ident 0x100) [fest in Steckplatz 11]

SPS-Eingangsdatenname	Eingangsdatentyp	SPS-Ausgangsdatenname	Ausgangsdatentyp
Ausgangsstatusbits 64–71	Byte	Entfällt	Entfällt
Ausgangsstatusbits 72–79	Byte		
Ausgangsstatusbits 80–87	Byte		
Ausgangsstatusbits 88–95	Byte		

Tabelle 44: Sicherheitsauswertung Ausgangsstatusbits (64–95) Modul (Ident 0x100) [fest in Steckplatz 12]



12.6.5.5 Ausgangsstatusbits

Die Steckplätze 10 bis 12 (96 Bits) sind immer für die Ausgangsstatus-Informationen der Sicherheitsausgänge reserviert. Die zu übertragenden Informationen der Bits werden im **Industrie-Ethernet** Tab der Konfigurationssoftware festgelegt.

SPS-Eingangsdatenname	Eingangsdatentyp	SPS-Ausgangsdatenname	Ausgangsdatentyp
Entfällt	Entfällt	Virtuelle Ein-/Ausschaltung/MA Bits 0–7	Byte
		Virtuelle Ein-/Ausschaltung/MA Bits 8–15	Byte
		Virtuelle Ein-/Ausschaltung/MA Bits 16–23	Byte
		Virtuelle Ein-/Ausschaltung/MA Bits 24–31	Byte
		Virtuelle Ein-/Ausschaltung/MA Bits 32–39	Byte
		Virtuelle Ein-/Ausschaltung/MA Bits 40–47	Byte
		Virtuelle Ein-/Ausschaltung/MA Bits 48–55	Byte
		Virtuelle Ein-/Ausschaltung/MA Bits 56–63	Byte

Tabelle 45: Virtuelle Ein-/Ausschaltung und Muting-Aktivierung Bits (0–63) Modul (Ident 0x200) [fest in Steckplatz 13]

12.6.5.6 Reset-/Abbruchverzögerungsbits (VRCD)

Steckplatz 14 (16 Bits) umfasst alle virtuellen, nicht sicherheitsrelevanten Eingänge, die für die virtuellen Reset- und Abbruchverzögerung verwendet werden können.

Siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 52.

SPS-Eingangsdatenname	Eingangsdatentyp	SPS-Ausgangsdatenname	Ausgangsdatentyp
Entfällt	Entfällt	VRCD-Bits 0–7	Byte
		VRCD-Bits 8–15	Byte

Tabelle 46: Virtuelle Reset-/Abbruchverzögerung Bits (0–63) Modul (Ident 0x300) [fest in Steckplatz 14]

12.6.5.7 Reset-/Abbruchverzögerung Auslösecode (RCD)

Steckplatz 15 (1 Word) enthält den RCD-Auslösecode, welcher für die virtuellen Reset-/ Abbruchverzögerung verwendet wird

Siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 52.

SPS-Eingangsdatenname	Eingangsdatentyp	SPS-Ausgangsdatenname	Ausgangsdatentyp
Entfällt	Entfällt	Auslösecode für Reset-/ Abbruchverzögerung	Ohne Vorzeichen 16

Tabelle 47: Modul für den Auslösecode für die Reset- und Abbruchverzögerung (Ident 0x301) [fest in Steckplatz 15]



12.6.5.8 Virtuelle Reset-/Abbruchverzögerung Feedbackbits

Steckplatz 16 (16 Bits) umfasst die Feedbackbits für die 16 Reset-/Abbruchverzögerungsbits in Steckplatz 14. Diese dienen zur Empfangsbestätigung und spiegeln das entsprechende Bit aus Steckplatz 14 für einen vollständigen Handshake zurück.

Siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 52.

SPS-Eingangsdatenname	Eingangsdatentyp	SPS-Ausgangsdatenname	Ausgangsdatentyp
VRCD-Feedbackbits 0–7	Byte	Entfällt	Entfällt
VRCD-Feedbackbits 8–15	Byte		

Tabelle 48: Virtuelle Reset-/Abbruchverzögerung Feedbackbits (0–63) Modul (Ident 0x400) [fest in Steckplatz 16]

12.6.5.9 Reset-/Abbruchverzögerung Auslösecode Feedback

Steckplatz 17 (1 Word) enthält den Feedback-Wert des RCD-Auslösecodes aus Steckplatz 15. Dieser Wert dient zur Empfangsbestätigung und spiegelt den Wert aus Steckplatz 15 für einen vollständigen Handshake zurück.

Siehe Virtueller manueller Reset und Abbruchverzögerungssequenz (RCD) auf Seite 52.

SPS-Eingangsdatenname	Eingangsdatentyp	SPS-Ausgangsdatenname	Ausgangsdatentyp
Auslösecode für Reset-/Abbruchverzögerung Feedback	Ohne Vorzeichen 16	Entfällt	Entfällt

Tabelle 49: Modul für den Auslösecode für die Reset-/Abbruchverzögerung (Ident 0x401) [fest in Steckplatz 17]

12.6.5.10 Fehlerprotokolleinträge

In Steckplatz 18 kann das optionale Fehlerprotokollpuffermodul eingesteckt werden.

SPS-Eingangsdatenname	Eingangsdatentyp	SPS-Ausgangsdatenname	Ausgangsdatentyp
Fehlerprotokolleintrag 1 (neuester)	15 Wörter	Entfällt	Entfällt
Fehlerprotokolleintrag 2	15 Wörter		
Fehlerprotokolleintrag 3	15 Wörter		
Fehlerprotokolleintrag 4	15 Wörter		
Fehlerprotokolleintrag 5	15 Wörter		
Fehlerprotokolleintrag 6	15 Wörter		
Fehlerprotokolleintrag 7	15 Wörter		
Fehlerprotokolleintrag 8	15 Wörter		
Fehlerprotokolleintrag 9	15 Wörter		
Fehlerprotokolleintrag 10 (ältester)	15 Wörter		

Tabelle 50: Sicherheitsauswertung Fehlerprotokollpuffermodul (Ident 0x500) [optional; fest in Steckplatz 18, wenn verwendet]

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

Tabelle 51: Aufbau Fehlerprotokoll-Eintrag



12.6.5.11 Puffer für Systeminformationen

In Steckplatz 19 kann das optionale Systeminformationspuffermodul eingesteckt werden.

SPS-Eingangsdatenname	Eingangsdatentyp	SPS-Ausgangsdatenname	Ausgangsdatentyp
Puffer für Systeminformationen	30 Wörter	Entfällt	Entfällt

Tabelle 52: Sicherheitsauswertung Systeminformationspuffermodul (Ident 0x600) [optional; fest in Steckplatz 19, wenn verwendet]

Puffer für Systeminformationen	Typ	Länge (Wörter)
Sekunden seit Systemstart	UDINT	2
Betriebsart	WORD	1
Länge des Konfigurationsnamens	DWORD	2
Konfigurationsname	String	8
Konfig. CRC	WORD	2

Tabelle 53: : Aufbau Systeminformations-Eintrag

Sekunden seit Systemstart

Die 32-Bit-Ganzzahldarstellung der Anzahl an Sekunden seit dem Einschalten der Sicherheitsauswertung.

Betriebsart

Der aktuelle Betriebsstatus der Sicherheitsauswertung.

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

Länge des Konfigurationsnamens

Die Anzahl an ASCII-Zeichen im „Konfigurationsnamen“.

Konfigurationsname

Ein ASCII-String, der den Ursprung des Fehlers beschreibt.

Konfig. CRC

Der Wert der zyklischen Redundanzprüfung (CRC) für die aktuelle Konfiguration der Sicherheitsauswertung



12.6.5.12 DCD-Statusinformationsmodul

In Steckplatz 20 kann das optionale DCD-Statusinformationsmodul eingesteckt werden.

SPS-Eingangsdatenname	Eingangsdatentyp	SPS-Ausgangsdatenname	Ausgangsdatentyp
DCD-Systemstatus – Reihe 1 Geräteanzahl	Ohne Vorzeichen 32	Entfällt	Ohne Vorzeichen 16
DCD-Systemstatus – Reihe 2 Geräteanzahl	Ohne Vorzeichen 32		
DCD-Systemstatus – Reihe 1 Gerät-Ein/Aus-Status	Ohne Vorzeichen 32		
DCD-Systemstatus – Reihe 2 Gerät-Ein/Aus-Status	Ohne Vorzeichen 32		
DCD-Systemstatus – Reihe 1 Fehlerstatus	Ohne Vorzeichen 32		
DCD-Systemstatus – Reihe 2 Fehlerstatus	Ohne Vorzeichen 32		
DCD-Systemstatus – Reihe 1 Betätiger im Randbereich	Ohne Vorzeichen 32		
DCD-Systemstatus – Reihe 2 Betätiger im Randbereich	Ohne Vorzeichen 32		
DCD-Systemstatus – Reihe 1 Warnstatus	Ohne Vorzeichen 32		
DCD-Systemstatus – Reihe 2 Warnstatus	Ohne Vorzeichen 32		
DCD-Systemstatus – Reihe 1 Resetstatus	Ohne Vorzeichen 32		
DCD-Systemstatus – Reihe 2 Resetstatus	Ohne Vorzeichen 32		
DCD-Systemstatus – Reihe 1 Auslöser erkannt	Ohne Vorzeichen 32		
DCD-Systemstatus – Reihe 2 Auslöser erkannt	Ohne Vorzeichen 32		
DCD-Systemstatus – Reihe 1 Systemstatus	Ohne Vorzeichen 32		
DCD-Systemstatus – Reihe 2 Systemstatus	Ohne Vorzeichen 32		
64 Byte reserviert	Byte		

Tabelle 54: Sicherheitsauswertung DCD-Statusinformationsmodul [optional]; fest in Steckplatz 20, wenn verwendet

12.6.5.13 Modul für Informationen einzelner DCD-Geräte

In Steckplatz 21 kann das optionale Modul für Informationen einzelner DCD-Geräte eingesteckt werden..

SPS-Eingangsdatenname	Eingangsdatentyp	SPS-Ausgangsdatenname	Ausgangsdatentyp
DCD-Leseanfrage Bestätigung	Ohne Vorzeichen 16	DCD-Leseanfrage	Ohne Vorzeichen 16
DCD-Reihe angeforderte Bestätigung	Ohne Vorzeichen 16	DCD-Reihe angefordert	Ohne Vorzeichen 16
DCD-Gerät angeforderte Bestätigung	Ohne Vorzeichen 16	DCD-Gerät angefordert	Ohne Vorzeichen 16
DCD-Daten des angeforderten Gerätes (18 Byte)	Byte		

Tabelle 55: Sicherheitsauswertung DCD-Einzelinformationsmodul [optional]; fest in Steckplatz 21, wenn verwendet



12.6.6 Leistungs- und Statusinformationen zu einem einzelnen Gerät über DCD anfordern

1. DCD-Reihe angefordert: DCD-Reihenschaltung, in der das betreffende Gerät angeschlossen ist (1 oder 2) auswählen.
2. DCD-Gerät angefordert: DCD-Gerätenummer (1 bis 32) auswählen.
3. DCD-Leseanfrage: Wechseln von 0 zu 1, um einen einmaligen Lesevorgang durchzuführen.
4. DCD-Daten des angeforderten Gerätes: Angeforderte gerätespezifische Daten des Gerätes.

12.6.7 Konfigurationsanleitung

Installation der GSD-Datei

Installieren Sie die GSD-Datei entsprechend dieser Anleitung im TIA Portal von Siemens. Diese Anleitung können Sie auch als Grundlage für die Installation der GSD-Datei in einem anderen Controller (SPS) verwenden.

1. Laden Sie die GSD-Datei von <http://www.bernstein.eu/downloads> herunter.
2. Rufen Sie die Software im TIA Portal von Siemens auf.
3. Klicken Sie auf **Vorhandenes Projekt öffnen**.
4. Wählen Sie ein Projekt aus und öffnen Sie es.
5. Klicken Sie auf **Geräte und Netzwerke**, nachdem das Projekt hochgeladen wurde.

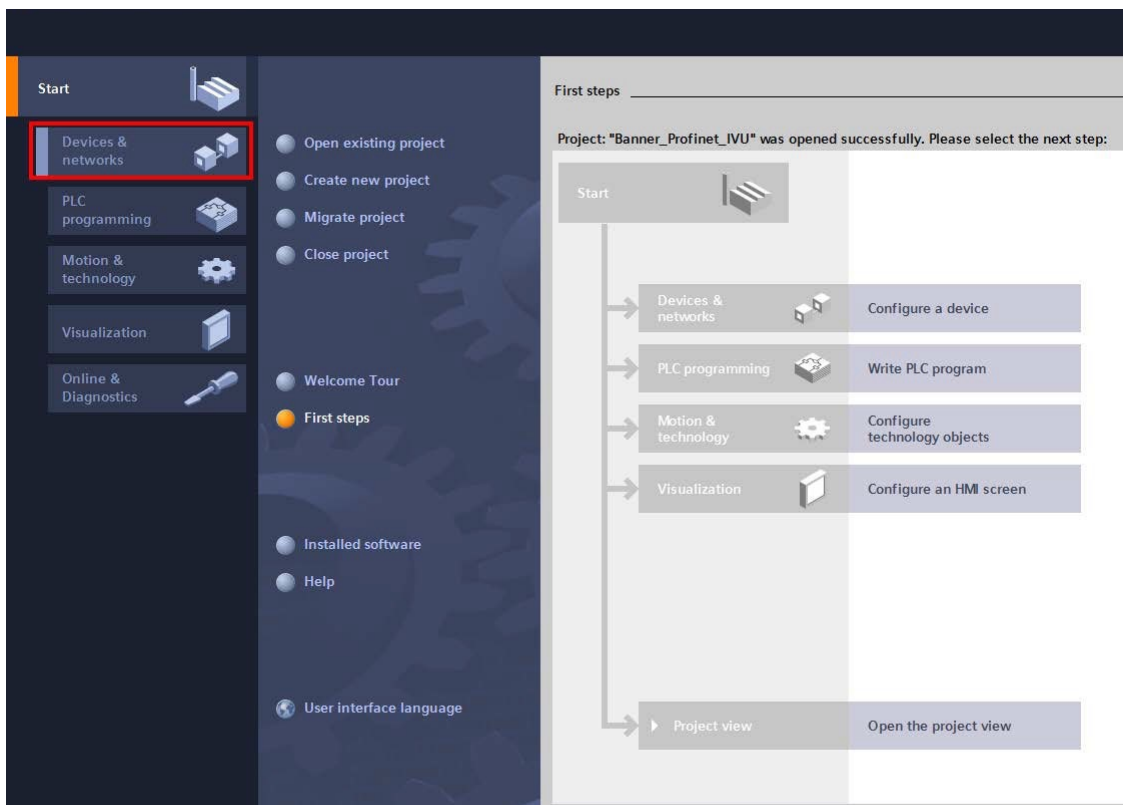


Abbildung 146: Geräte und Netzwerke

6. Klicken Sie auf **Netzwerke konfigurieren**





Abbildung 147: Netzwerke konfigurieren

Die Netzwerkansicht wird angezeigt.

7. Klicken Sie auf **Optionen** und wählen Sie **GSD-Datei (General Station Description) verwalten**

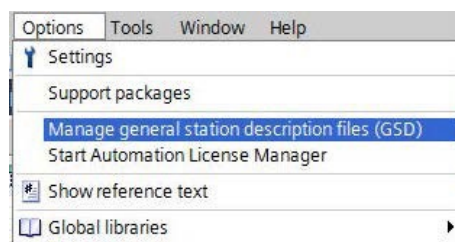


Abbildung 148: Optionen — GSD-Datei installieren

aus. Das Fenster **GSD-Datei (General Station Description) installieren** wird geöffnet.

8. Klicken Sie auf die Durchsuchen-Schaltfläche (...) rechts neben dem Pfeil **Quellpfad**.

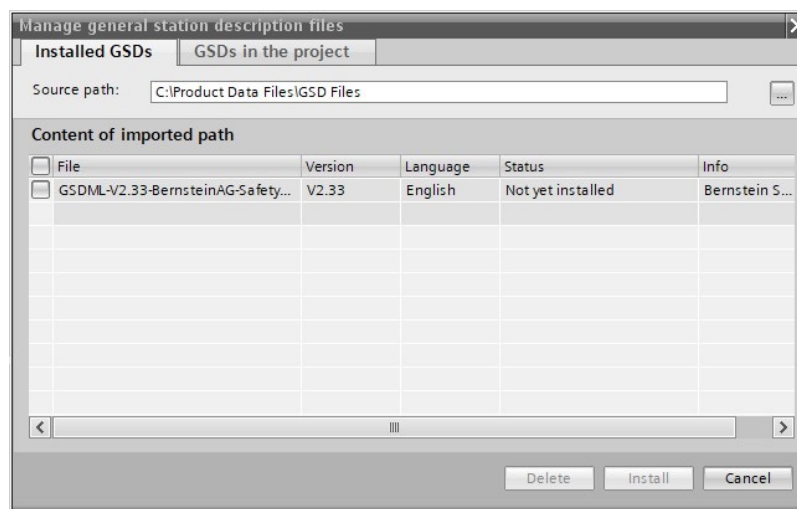


Abbildung 149: : GSD-Dateien verwalten

9. Navigieren Sie zum Speicherort, in den Sie die GSD-Datei der Sicherheitsauswertung heruntergeladen haben.

10. Wählen Sie die GSD-Datei der Sicherheitsauswertung.

11. Auf **Installieren** klicken



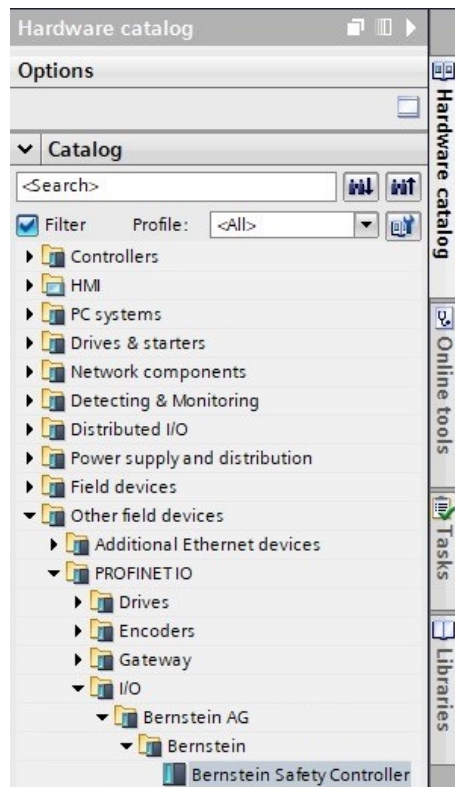


Abbildung 150: Hardware-Katalog

Die GSD-Datei der Sicherheitsauswertung wird vom System installiert und im **Hardware-Katalog** abgelegt. Im obigen Beispiel befindet sich die GSD-Datei der Sicherheitsauswertung unter **Andere Feldgeräte > PROFINET IO > E/A > BERNSTEIN AG > BERNSTEIN**.



Anmerkung: Wenn die GSD-Datei der Sicherheitsauswertung nicht richtig installiert wird, speichern Sie das Protokoll und kontaktieren Sie die BERNSTEIN AG

Ändern der IP-Adresse von Geräten

Ändern Sie die IP-Adresse der Sicherheitsauswertung entsprechend dieser Anleitung über die Software im TIA Portal von Siemens. Diese Anleitung können Sie auch als Grundlage verwenden, wenn Sie einen anderen Controller (SPS) verwenden.

1. Rufen Sie die Software im TIA Portal von Siemens auf.
2. Klicken Sie auf **Vorhandenes Projekt öffnen**.
3. Wählen Sie ein Projekt aus und öffnen Sie es.
4. Klicken Sie auf **Geräte und Netzwerke**, nachdem das Projekt hochgeladen wurde, um die **Netzwerkansicht** aufzurufen. Die Netzwerkansicht wird angezeigt.
5. Doppelklicken Sie auf die Sicherheitsauswertung, um die **Geräteansicht** zu öffnen.

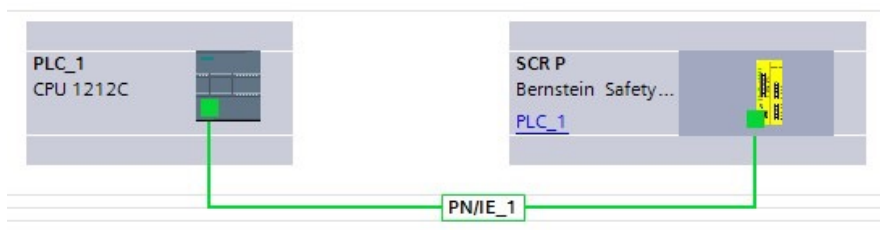


Abbildung 151: Abbildung 115: Netzwerkansicht

6. Klicken in der **Geräteansicht** im Grafikbereich auf die Sicherheitsauswertung, um das Fenster **Moduleigenschaften** zu öffnen. Sie können das Modul jetzt konfigurieren.
7. Klicken Sie auf **Eigenschaften**.
8. Klicken Sie auf **Allgemein**.
9. Auswählen **PROFINET-Schnittstelle > Ethernet-Adressen**.
10. Wählen Sie **IP-Adresse im Projekt festlegen** aus.



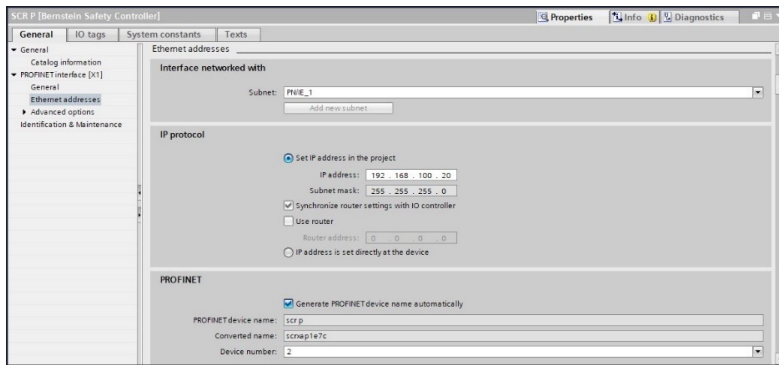


Abbildung 152: Ethernet-Adressen

Das Projekt legt die IP-Adresse des Geräts fest.

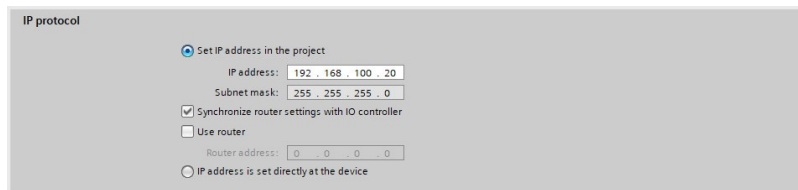


Abbildung 153: IP-Adresse festlegen

11. Geben Sie die IP-Adresse ein.
12. Klicken Sie mit der rechten Maustaste auf das Gerätesymbol und wählen Sie **Online** und **Diagnosen** aus. Das Fenster **Online und Diagnosen** wird angezeigt.

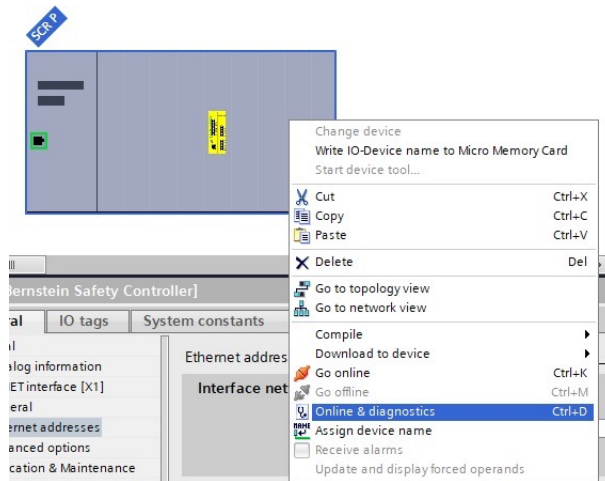


Abbildung 154: Online und Diagnosen“ auswählen

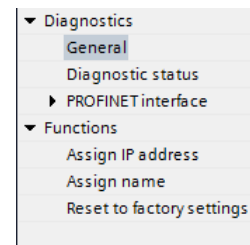


Abbildung 155: Online und Diagnosen

13. Wählen Sie **IP-Adresse** zuweisen unter **Funktionen** aus
14. Klicken Sie auf **Zugängliche Geräte**. Im Fenster **Gerät auswählen** wird nach dem Netzwerk für verfügbare Geräte gesucht.

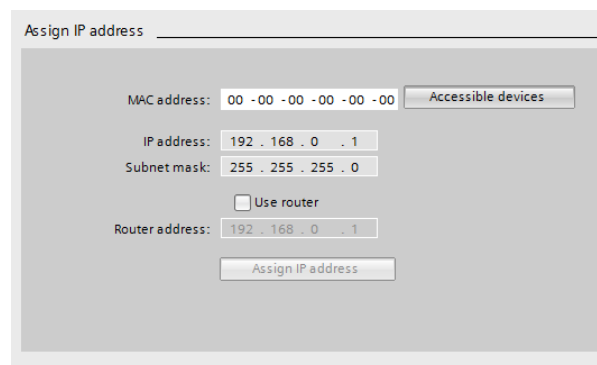


Abbildung 156: IP-Adresse zuweisen — Zugängliche Geräte

15. Ermitteln Sie das Gerät, das Sie anpassen möchten, anhand der MAC-Adresse und wählen Sie es aus.
16. Klicken Sie auf **Anwenden**.



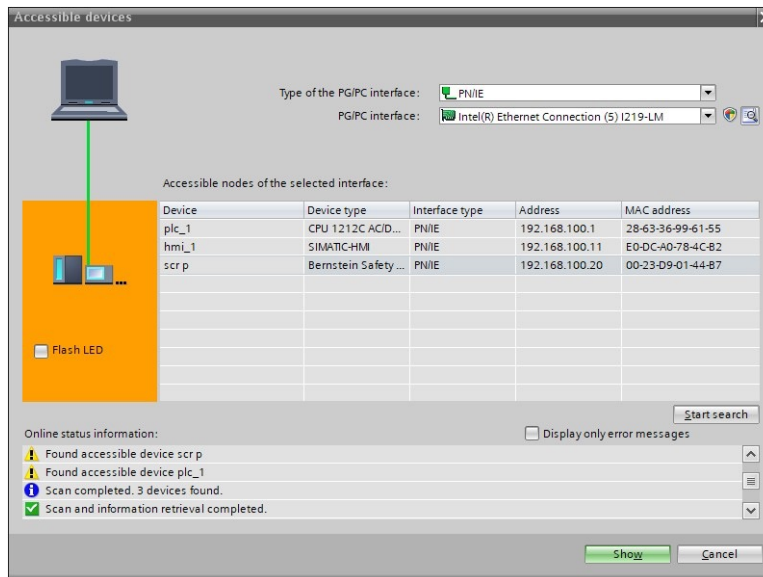


Abbildung 157: Gerät auswählen und Änderungen übernehmen

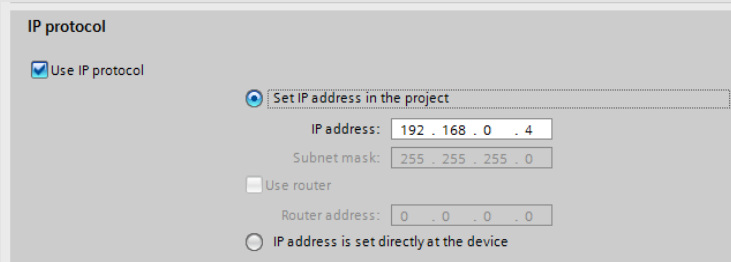
Die IP-Adresse für das Gerät wird aktualisiert.

17. Klicken Sie auf **IP-Adresse zuweisen**, um den Schritt abzuschließen.

Dieser Schritt wird für alle Geräte abgeschlossen.



Anmerkung: PROFINET-Geräte haben beim Starten in der Regel keine IP-Adresse (IP-Adresse = alles Nullen). Controller (SPS) benötigen jedoch generell eine IP-Adresse, um sich mit der Sicherheitsauswertung SCR P von BERNSTEIN zu verbinden und die Gerätekonfiguration festzulegen. Standardmäßig ist jeder Sicherheitsauswertung bei Auslieferung ab Werk die IP-Adresse 192.168.0.128 zugewiesen. Die Standardadresse kann mit der Konfigurationssoftware von BERNSTEIN geändert werden. Die Sicherheitsauswertung ruft ihre IP-Adresse unmittelbar nach Aktivierung des PROFINET-Protokolls in der Sicherheitsauswertung ab, aber bevor die SPS die Sicherheitsauswertung erkennt und sich damit verbunden hat. Nachdem die SPS die Sicherheitsauswertung erkennt und sich mit ihr verbunden hat, hängt das Verhalten der IP-Adresse davon ab, wie die SPS zum Zuweisen der IP-Adresse der Sicherheitsauswertung konfiguriert wurde. Es sind zwei Konfigurationsoptionen verfügbar.



- Die IP-Adresse wird im Projekt festgelegt: Wenn die SPS angewiesen wird, die IP-Adresse der Sicherheitsauswertung zuzuweisen (z. B. anhand der Option **IP-Adresse im Projekt festlegen** im TIA Portal von Siemens) empfängt die Sicherheitsauswertung die spezifische Adresse. Dazu muss allerdings erst das Programm in die SPS geladen und ausgeführt werden. Wird die Sicherheitsauswertung neu gestartet, nachdem sie von der SPS erkannt und konfiguriert wurde, hat sie die IP-Adresse 0.0.0.0, bis die SPS die Sicherheitsauswertung erkannt hat und ihr die festgelegte Adresse erneut zugewiesen hat. Wenn der Sicherheitsauswertung keine IP-Adresse zugewiesen ist, kann sie dennoch mit der Konfigurationssoftware von BERNSTEIN zugewiesen werden. Wenn sich diese Adresse jedoch von der in der SPS angegebenen unterscheidet, verwendet die Sicherheitsauswertung wieder die in der SPS angegebene Adresse, sobald die SPS erneut aktiv wird.
- Die IP-Adresse wird im Gerät festgelegt: Wenn die SPS angewiesen wird, dass die IP-Adresse der Sicherheitsauswertung im Gerät konfiguriert ist (z. B. anhand der Option **IP-Adresse ist direkt im Gerät festgelegt** im TIA Portal von Siemens) ruft die Sicherheitsauswertung immer die über Konfigurationssoftware von BERNSTEIN zugewiesene IP-Adresse ab.

Diese Konfigurationsoptionen entsprechen der PROFINET-Norm.



Ändern des Gerätenamens

Ändern Sie den Namen der Sicherheitsauswertung entsprechend dieser Anleitung im TIA Portal von Siemens. Diese Anleitung können Sie auch als Grundlage verwenden, wenn Sie einen anderen Controller (SPS) verwenden.

1. Öffnen Sie das Projekt und klicken Sie auf **Geräte und Netzwerke**, um die **Netzwerkansicht** aufzurufen.

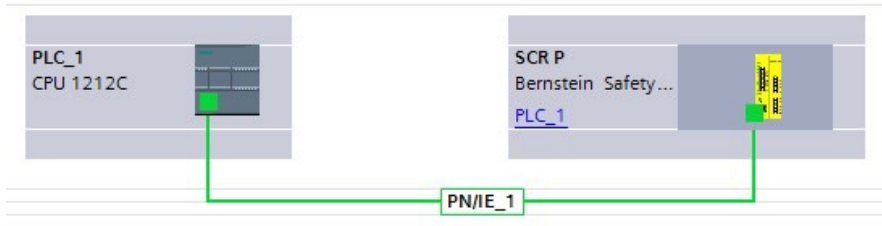


Abbildung 158: Netzwerkansicht

Die **Netzwerkansicht** wird angezeigt.

2. Klicken Sie mit der rechten Maustaste auf die Sicherheitsauswertung und wählen Sie **Gerätename zuweisen** aus.

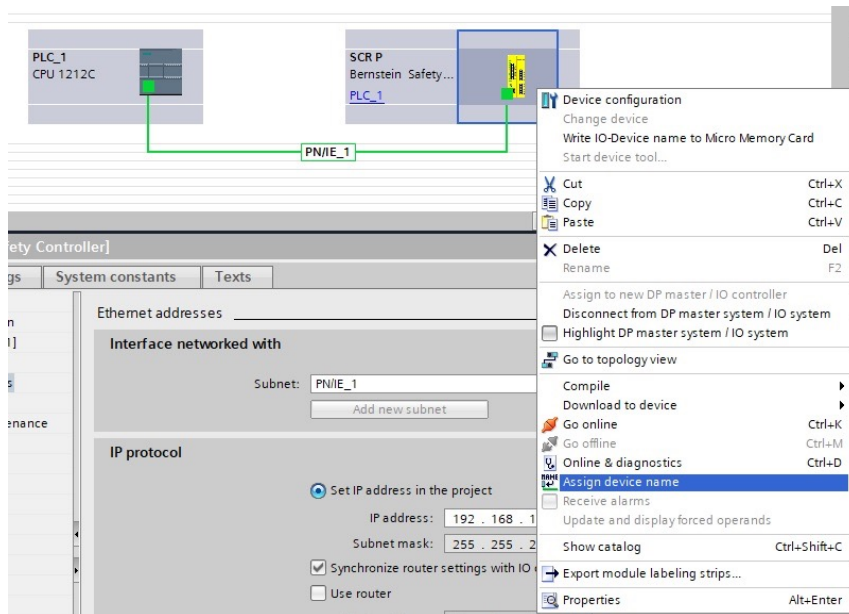


Abbildung 159: Ethernet-Adressen

Das Fenster **PROFINET-Gerätename zuweisen** wird angezeigt und die Software sucht nach Geräten des gleichen Typs

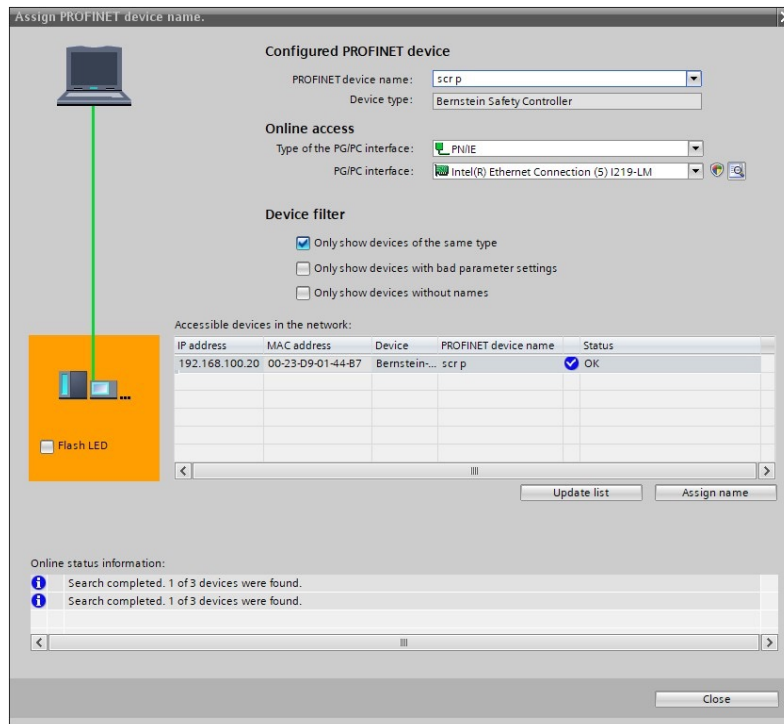


Abbildung 160: Ethernet-Adressen



3. Geben Sie den gewünschten Namen in das Feld PROFINET-Gerätenamen ein.



Anmerkung: Jeder Name darf nur einmal verwendet werden

4. Klicken Sie auf **Name zuweisen**.

Das Gerät hat jetzt einen PROFINET-Namen.

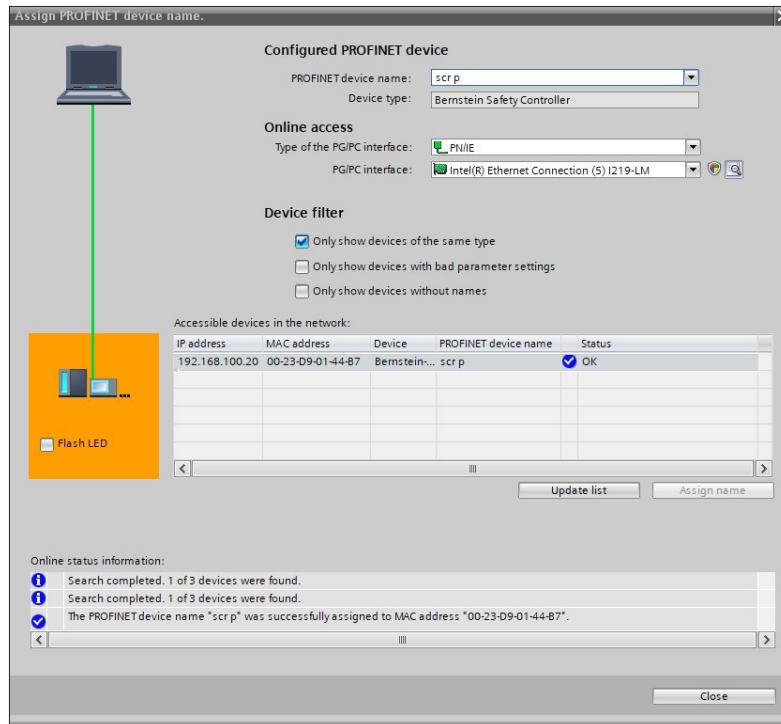


Abbildung 161: Ethernet-Adressen

12.7 EtherCAT®

EtherCAT® 57 ist ein Datenkommunikationsprotokoll für industrielle Automatisierungsprozesse. EtherCAT IO definiert, wie Steuerungen (IO-Controller) und Peripheriegeräte (IO-Devices) Daten in Echtzeit austauschen.

Der BERNSTEIN Safety Controller unterstützt EtherCAT IO. Das EtherCAT-Protokoll folgt der Norm IEC 61158; das Datenübertragungsmedium ist Kupferdraht.



Hinweis: In diesem Dokument werden die Ausgänge der Sicherheitssteuerung als „Eingänge“ für die Steuerung (SPS) bezeichnet. Die Ausgänge der Steuerung (SPS) werden als „Eingänge“ für die Sicherheitssteuerung bezeichnet.

12.7.1 EtherCAT® und die Sicherheitssteuerungen

Dieser Abschnitt enthält Anweisungen für SCx Sicherheits-Steuerungen mit der Bezeichnung FID 6 auf dem Produktetikett. Auf der Sicherheitssteuerung muss das EtherCAT-Kommunikationsgateway XSeCAT installiert sein.

EtherCAT-Echtzeitdaten werden über Prozessdaten-Objekte (PDO) gesendet und empfangen.



Hinweis: Die ESI-Datei steht unter www.bernstein.eu zum Download bereit.

12.7.2 EtherCAT® Slave Information (ESI) Datei

Die EtherCAT-Slave-Informationsdatei (ESI) enthält Modulinformationen, wie z. B.:

- Daten zur Konfiguration
- Dateninformationen (Anzahl der Durchgänge, Prüfstatus usw.)
- Diagnostik



12.7.3 EtherCAT® IO-Datenmodell

Das Datenmodell von EtherCAT IO basiert auf dem typischen, erweiterbaren Feldgerät, das über eine Backplane mit Steckplätzen verfügt.

Jeder Slot ist entweder ein Tx-PDO (Transmit Process Data Object) oder ein Rx-PDO (Received Process Data Object). Das Tx-PDO oder Rx-PDO ist in Datenstrukturen aufgeteilt. Der Großteil der SCx-Daten wird in PDOs mit 4 Byte Daten aufgeteilt. Die PDOs DCD, RCD, Fault Log und System Information haben eigene Strukturen.

- Ein PDO wird entweder als Tx (Transmit) oder als Rx (Received) bezeichnet.
- Ein Transmit PDO wird verwendet, um Daten an die Steuerung (SPS) zu senden.
- Ein Received PDO wird verwendet, um Daten von der Steuerung (SPS) zu empfangen

12.7.4 Konfigurieren der Sicherheitssteuerung für EtherCAT® IOAnbindung

1. Verbinden Sie die Sicherheitssteuerung über das USB-Kabel SC-USB2 mit dem PC.
2. Öffnen Sie die BERNSTEIN Safety Controller Software, und klicken Sie auf die Registerkarte Industrial Ethernet.
3. Vergewissern Sie sich, dass das EtherCAT Communication Gateway auf der Registerkarte Equipment der Projektdatei hinzugefügt wurde.
Die Registerkarte EtherCAT sollte automatisch angezeigt werden, da sich das EtherCAT Communication Gateway in Equipment tab.
4. Klicken Sie auf , um dem EtherCAT-Prozessdatenobjekt (PDO) Informationen hinzuzufügen. Auto Configure kann Sie bei dieser Aufgabe unterstützen.
5. Geben Sie das entsprechende Passwort ein, um die Konfigurations- und Netzwerkeinstellungen für die Sicherheitssteuerung zu ändern.
6. Stellen Sie sicher, dass die Sicherheitssteuerung über eine gültige und bestätigte Konfigurationsdatei verfügt.



Hinweis: Wenn ein virtueller Reset oder eine Abbruchverzögerung verwendet wird, muss in den **Netzwerkeinstellungen** ein Aktivierungscode erstellt werden. Anschließend muss der Code mit **Senden** in den **Netzwerkeinstellungen** an die Sicherheitssteuerung gesendet werden.



Hinweis: ClickSet IP ist nicht für EtherCAT verfügbar.



12.7.5 Erstellen eines PLCopenXML für EtherCAT® für TwinCAT® 3.0

Zwei Punkte müssen bekannt sein:

- Der Name des Projekts in TwinCAT ⁶²
- Der Name der Sicherheitssteuerung im System

Diese Informationen sind in der SPS-Software verfügbar. Die folgende Abbildung ist ein Beispiel aus der Beckhoff TwinCAT 3.0 Software.

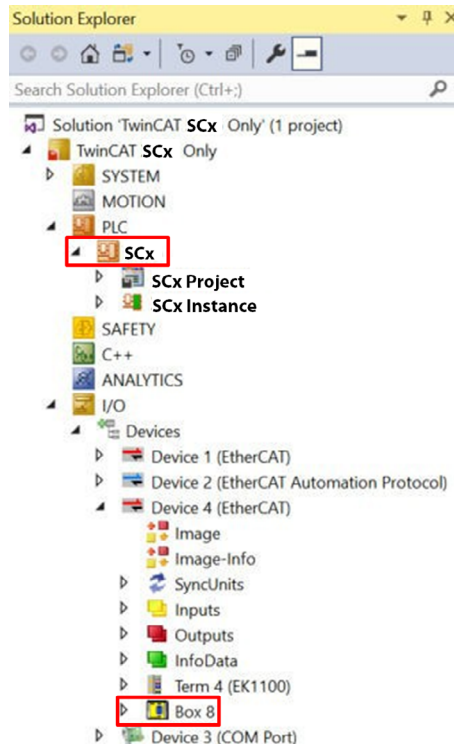


Abbildung 162: Lösungs-Explorer

1. Vergewissern Sie sich in der Software BERNSTEIN Safety Controller auf der Registerkarte **Industrial Ethernet**, dass **EtherCAT** in der Liste auf der linken Seite ausgewählt ist.
2. Klicken Sie auf **Exportieren**.
Das Fenster **In XML exportieren** wird geöffnet.



Abbildung 163: Exportieren nach XML - keine DCD-Kette

⁶² TwinCAT® ist ein eingetragenes Warenzeichen der Beckhoff Automation GmbH, Deutschland, und wird von dieser lizenziert.



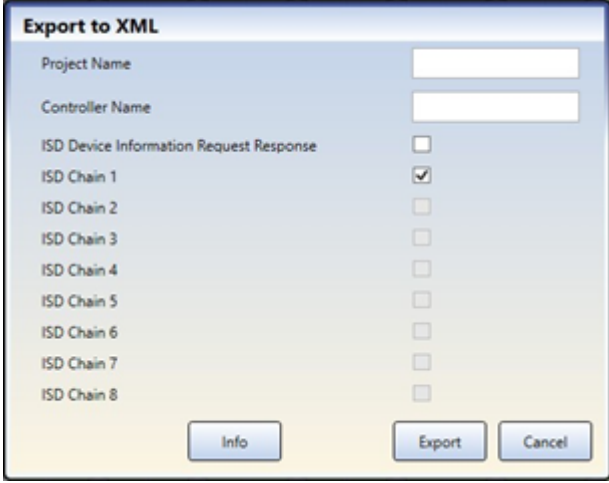


Abbildung 164: Exportieren nach XML - mit DCD-Ketten

3. Geben Sie die Informationen in das Fenster ein.
 - a. Geben Sie in das Feld **Projektname** den Namen des Projekts in der SPS-Software ein. Siehe Punkt 1 in Abbildung 159 auf Seite 202. In diesem Beispiel ist es SCx.
 - b. Geben Sie in das Feld **Steuerungsname** den Namen der Sicherheitssteuerung in der SPS-Software ein. Siehe Punkt 2 in Abbildung 159 auf Seite 202. In diesem Beispiel ist es Box 8.
 4. Klicken Sie auf **Exportieren**.
 5. Speichern Sie die PLCopenXML-Datei an dem gewünschten Ort.
- Die PLCopenXML-Datei kann direkt in die Beckhoff TwinCAT-Software importiert oder mit jeder Software, die eine .xml-Datei lesen kann, geöffnet werden.



12.7.6 Beschreibung von Prozessdatenobjekten

In dieser Tabelle ist die E/A-Richtung vom Standpunkt der SPS aus gesehen.

PDO	Name	IO	Größe (Bytes)
1A00	Benutzerdefinierte VS TxPDO [1] 0x1A00	Unter	4
1A01	Benutzerdefinierte VS TxPDO [2] 0x1A01	Unter	4
1A02	Fehler VS TxPDO [1] 0x1A02	Unter	4
1A03	Fehler VS TxPDO [2] 0x1A03	Unter	4
1A04	Eingänge VS TxPDO[1] 0x1A04	Unter	4
1A05	Eingänge VS TxPDO[2] 0x1A05	Unter	4
1A06	Eingänge VS TxPDO[3] 0x1A06	Unter	4
1A07	Eingänge VS TxPDO[4] 0x1A07	Unter	4
1A08	Eingänge VS TxPDO[5] 0x1A08	Unter	4
1A09	Ausgänge VS TxPDO[1] 0x1A09	Unter	4
1A0A	Ausgänge VS TxPDO[2] 0x1A0A	Unter	4
1A0B	Ausgänge VS TxPDO[3] 0x1A0B	Unter	4
1A0C	Zurücksetzen, Verzögerungsrückmeldung abbrechen TxPDO 0x1A0C	Unter	4
1A10	DCD Geräteinformation Antwort 0x1A10 ⁶⁴	Unter	56
1A20	Systemstatus der DCD-Kette 1 TxPDO 0x1A20 ⁶⁴	Unter	32
1A3A	ECAT-Modul Status TxPDO 0x1A3A	Unter	4
1600	Ein/Aus, Stummschaltung VI RxPDO [1] 0x1600	Aus	4
1601	Ein/Aus, Stummschaltung VI RxPDO [2] 0x1601	Aus	4
1602	Reset, Abbruch Verzögerungssteuerung RxPDO 0x1610	Aus	4
1610	DCD Anforderung von Geräteinformationen RxPDO 0x1610 ⁶⁴	Aus	6

Tabelle 56: PDO-Zuordnung



Benutzerdefinierte Statusbits

PDO 1 und PDO 2 werden mit benutzerdefinierten Statusbit-Prozessdatenobjekten (PDO) gefüllt. Diese PDO enthalten 64 Bit virtuelle Statusausgangsinformationen beliebigen Typs.

PLC-Eingangsdaten Name	Eingangsdaten Typ
Benutzerdefinierte VS TxPDO [1] 0x1A00 Byte 0	BYTE
Benutzerdefinierte VS TxPDO [1] 0x1A00 Byte 1	BYTE
Benutzerdefinierte VS TxPDO [1] 0x1A00 Byte 2	BYTE
Benutzerdefinierte VS TxPDO [1] 0x1A00 Byte 3	BYTE

Tabelle 57: Benutzerdefinierte VS TxPDO [1] 0x1A00

PLC-Eingangsdaten Name	Eingangsdaten Typ
Benutzerdefinierte VS TxPDO [2] 0x1A00 Byte 0	BYTE
Benutzerdefinierte VS TxPDO [2] 0x1A00 Byte 1	BYTE
Benutzerdefinierte VS TxPDO [2] 0x1A00 Byte 2	BYTE
Benutzerdefinierte VS TxPDO [2] 0x1A00 Byte 3	BYTE

Tabelle 58: Benutzerdefinierte VS TxPDO [2] 0x1A01

Störungs-Bits

PDO 3 und PDO 4 werden mit 64 Bits virtueller Status-Ausgangsinformationen der Sicherheitssteuerung gefüllt.

PLC-Eingangsdaten Name	Eingangsdaten Typ
Störungen VS TxPDO [1] 0x1A02 Byte 0	BYTE
Störungen VS TxPDO [1] 0x1A02 Byte 1	BYTE
Fehler VS TxPDO [1] 0x1A02 Byte 2	BYTE
Fehler VS TxPDO [1] 0x1A02 Byte 3	BYTE

Tabelle 59: Fehler VS TxPDO [1] 0x1A02

PLC-Eingangsdaten Name	Eingangsdaten Typ
Fehler VS TxPDO [2] 0x1A03 Byte 0	BYTE
Störungen VS TxPDO [2] 0x1A03 Byte 1	BYTE
Fehler VS TxPDO [2] 0x1A03 Byte 2	BYTE
Fehler VS TxPDO [2] 0x1A03 Byte 3	BYTE

Tabelle 60: Fehler VS TxPDO [1] 0x1A02

⁶⁴ Diese PDO-Zuweisung ist standardmäßig ausgeschaltet.



Eingangsstatus-Bits

PDO 5 bis PDO 9 sind für 160 Bits der Eingangsinformationen der Sicherheitssteuerung reserviert. Eine erweiterbare Sicherheitssteuerung kann bis zu 154 Eingänge haben, wenn alle acht möglichen Erweiterungskarten als 16-Kanal-Eingänge verwendet werden (zusätzlich zu den 26 in der Basissteuerung eingebauten Eingängen).

PLC-Eingangsdaten Name	Eingangsdaten Typ
Eingänge VS TxPDO [1] 0x1A04 Byte 0	BYTE
Eingänge VS TxPDO [1] 0x1A04 Byte 1	BYTE
Eingänge VS TxPDO [1] 0x1A04 Byte 2	BYTE
Eingänge VS TxPDO [1] 0x1A04 Byte 3	BYTE

Tabelle 61: Eingänge VS TxPDO [1] 0x1A04

PLC-Eingangsdaten Name	Eingangsdaten Typ
Eingänge VS TxPDO [2] 0x1A05 Byte 0	BYTE
Eingänge VS TxPDO [2] 0x1A05 Byte 1	BYTE
Eingänge VS TxPDO [2] 0x1A05 Byte 2	BYTE
Eingänge VS TxPDO [2] 0x1A05 Byte 3	BYTE

Tabelle 62: Eingänge VS TxPDO [2] 0x1A05

PLC-Eingangsdaten Name	Eingangsdaten Typ
Eingänge VS TxPDO [3] 0x1A06 Byte 0	BYTE
Eingänge VS TxPDO [3] 0x1A06 Byte 1	BYTE
Eingänge VS TxPDO [3] 0x1A06 Byte 2	BYTE
Eingänge VS TxPDO [3] 0x1A06 Byte 3	BYTE

Tabelle 63: Eingänge VS TxPDO [3] 0x1A06

PLC-Eingangsdaten Name	Eingangsdaten Typ
Eingänge VS TxPDO [4] 0x1A07 Byte 0	BYTE
Eingänge VS TxPDO [4] 0x1A07 Byte 1	BYTE
Eingänge VS TxPDO [4] 0x1A07 Byte 2	BYTE
Eingänge VS TxPDO [4] 0x1A07 Byte 3	BYTE

Tabelle 64: Eingänge VS TxPDO [4] 0x1A07



PLC-Eingangsdaten Name	Eingangsdaten Typ
Eingänge VS TxPDO [5] 0x1A08 Byte 0	BYTE
Eingänge VS TxPDO [5] 0x1A08 Byte 1	BYTE
Eingänge VS TxPDO [5] 0x1A08 Byte 2	BYTE
Eingänge VS TxPDO [5] 0x1A08 Byte 3	BYTE

Tabelle 65: Eingänge VS TxPDO [5] 0x1A08

Ausgangsstatus-Bits

PDO 10 bis PDO 12 sind für 96 virtuelle Status-Ausgangsbits des Typs Sicherheitssteuerung reserviert.

PLC-Eingangsdaten Name	Eingangsdaten Typ
Ausgänge VS TxPDO [1] 0x1A09 Byte 0	BYTE
Ausgänge VS TxPDO [1] 0x1A09 Byte 1	BYTE
Ausgänge VS TxPDO [1] 0x1A09 Byte 2	BYTE
Ausgänge VS TxPDO [1] 0x1A09 Byte 3	BYTE

Tabelle 66: Ausgänge VS TxPDO [1] 0x1A09

PLC-Eingangsdaten Name	Eingangsdaten Typ
Ausgänge VS TxPDO [2] 0x1A0A Byte 0	BYTE
Ausgänge VS TxPDO [2] 0x1A0A Byte 1	BYTE
Ausgänge VS TxPDO [2] 0x1A0A Byte 2	BYTE
Ausgänge VS TxPDO [2] 0x1A0A Byte 3	BYTE

Tabelle 67: Ausgänge VS TxPDO [2] 0x1A0A

PLC-Eingangsdaten Name	Eingangsdaten Typ
Ausgänge VS TxPDO [3] 0x1A0B Byte 0	BYTE
Ausgänge VS TxPDO [3] 0x1A0B Byte 1	BYTE
Ausgänge VS TxPDO [3] 0x1A0B Byte 2	BYTE
Ausgänge VS TxPDO [3] 0x1A0B Byte 3	BYTE

Tabelle 68: Ausgänge VS TxPDO [3] 0x1A0B



Virtueller Reset, Abbruchverzögerung (RCD) Rückmeldung

PDO 13 enthält die Rückmeldung des RCD-Betätigungscode sowie 16 virtuelle nicht sicherheitsrelevante Eingänge. Sie werden in der virtuellen Reset-, Cancel-Delay-Sequenz verwendet.

Siehe „7.7.1 Virtueller manueller Reset und Abbrechen einer Zeitverzögerung (RCD)“ auf Seite 57.

PLC-Eingangsdaten Name	Eingangsdaten Typ
RCD-Betätigungscode Rückmeldung	BYTE
Rücksetzen, Verzögerungsrückmeldung abbrechen TxPDO [1] 0x1A0C Byte 0	BYTE
Rücksetzen, Verzögerungsrückmeldung abbrechen TxPDO [1] 0x1A0C Byte 1	BYTE

Tabelle 69: Virtueller Reset, Abbruchverzögerung

DCD Geräteinformationen Antwort

PDO 14 enthält die Antwortdaten für die Kommunikation mit einem einzelnen DCD-Gerät.

Siehe auch Abfrage von Leistungs- und Statusinformationen zu einem einzelnen Gerät über DCD auf Seite 50 und DCD Individuelle gerätespezifische Daten - detaillierte Beschreibung auf Seite 202.

PLC-Eingangsdaten Name	Eingangsdaten Typ
DCD-Anfrage-Bestätigung	UINT
DCD-Ketten-Bestätigung	UINT
DCD-Geräte-Bestätigung	UINT
DCD-Geräteinformationen ⁶⁶	ARRAY[0..17] aus BYTE
Erkanntes Gerät [0-15] in einer Kette	ARRAY[0..15] aus BYTE
Erkanntes Gerät [16-31] in einer Kette	ARRAY[0..15] aus BYTE

Tabelle 70: Virtueller Reset, Abbruchverzögerung

DCD Individuelle Geräteinformationsspezifische Daten Detaillierte Beschreibung

Gibt das Datenformat für PLC Input Data Name an: DCDGeräteinformationen.

Siehe Antwort auf DCD-Geräteinformationen auf Seite 291.

Informationen	Byte.Wort	Daten Größe
Fehler am Sicherheitseingang	0.0	1-Bit
Reserviert	0.1	1-Bit
Sensor nicht gepaart	0.2	1-Bit
DCD-Datenfehler	0.3	1-Bit
Falscher Aktor/Tastenstatus/Eingangsstatus	0.4	1-Bit
Randbereich/Tastenstatus/Eingangsstatus	0.5	1-Bit
Aktuator erkannt	0.6	1-Bit
Ausgang Fehler	0.7	1-Bit



Informationen	Byte.Wort	Daten Größe
Eingabe 2	1.0	1-Bit
Eingang 1	1.1	1-Bit
Lokaler Reset Erwartet	1.2	1-Bit
Warnung zur Betriebsspannung	1.3	1-Bit
Betriebsspannung Fehler	1.4	1-Bit
Ausgang 2	1.5	1-Bit
Ausgang 1	1.6	1-Bit
Power Cycle erforderlich	1.7	1-Bit
Fehlertolerante Ausgänge	2.0	1-Bit
Lokale Reset-Einheit	2.1	1-Bit
Kaskadierbar	2.2	1-Bit
Hohe Codierungsebene	2.3	1-Bit
Verbleibende Teach-ins	2,7 bis 2,4	4-Bit
Geräte-ID	3,4 bis 3,0	5-Bit
Bereich Anzahl der Warnungen	4,2 bis 3,5	6-Bit
Ausgang Abschaltzeit	4,7 bis 4,3	5-Bit
Anzahl von Spannungsfehlern	5	8-Bit
Innentemperatur	6	8-Bit
Betätigungselement Abstand	7	8-Bit
Versorgungsspannung	8	8-Bit
Erwarteter Name des Unternehmens	9,3 bis 9,0	4-Bit
Empfangener Firmenname	9.7 bis 9.4	4-Bit
Erwarteter Code	11 zu 10	16-Bit
Empfangener Code	13 zu 12	16-Bit
Interner Fehler A	15 zu 14	16-Bit
Interner Fehler B	17 zu 16	16-Bit

Tabelle 71: DCD Einzelne Gerätedaten

⁶⁶ Für das Datenformat siehe DCD Individuelle Geräteinformationen - Spezifische Daten - Detaillierte Beschreibung auf Seite 292.



Systemstatus der DCD-Kette - 8 Ketten

PDO 15 bis PDO 22 umfassen die spezifischen Daten einer einzelnen DCD-Kette. Jede Kette hat ihre eigenen Daten.

PLC-Eingangsdaten Name	Eingangsdaten Typ
Anzahl der Eingänge in der Kette #	UDINT
Kette Status der Kette # ⁶⁷	ARRAY[0..27] aus BYTE

Tabelle 72: Einzelne DCD-Ketten Status

Status der Kette #-spezifische Daten Detaillierte Beschreibung

Gibt das Datenformat für PLC Input Data Name an: Kettenstatus der Kette #. Siehe Systemstatus der DCD-Kette - 8 Ketten auf Seite 293.

Informationen	Daten Größe
Kette # Geräteanzahl	32-Bit
Kette # Gerät ein/aus (siehe DCD System Status Words auf Seite 206)	32-Bit
Kette # Fault Status (siehe DCD System Status Words auf Seite 206)	32-Bit
Kette # Marginal Status (siehe DCD System Status Words auf Seite 206)	32-Bit
Kette # Alert Status (siehe DCD System Status Words auf Seite 206)	32-Bit
Kette # Reset Status (siehe DCD System Status Words auf Seite 206)	32-Bit
Kette # Actuator Recognized (siehe DCD System Status Words auf Seite 206)	32-Bit
Kette # Systemstatus (siehe DCD Kette Systemstatus auf Seite 50)	32-Bit

Tabelle 73: DCD Einzelne Kettendaten

EtherCAT-Modul-Status

PLC-Eingangsdaten Name	Eingangsdaten Typ
ECAT-Modul-Status	UINT
Betriebsart	UINT

Virtuell Ein, Aus, Stummschaltung Aktivierungsbits

PDO 25 ist mit 64 virtuellen nicht-sicherheitsgerichteten Eingängen gefüllt, die als virtuelle Ein-/Ausgänge (zum Sicherheits-Controller) oder virtuelle Stummschalteingänge (zum Sicherheits-Controller) verwendet werden können.

PLC-Ausgangsdaten Name	Ausgabe-Datentyp
Ein/Aus, Mute-Freigabe VI RxPDO [1] 0x1600 Byte 0	BYTE
Ein/Aus, Mute-Freigabe VI RxPDO [1] 0x1600 Byte 1	BYTE
Ein/Aus, Mute-Freigabe VI RxPDO [1] 0x1600 Byte 2	BYTE
Ein/Aus, Mute-Freigabe VI RxPDO [1] 0x1600 Byte 3	BYTE

Tabelle 74: Virtuell Ein, Aus, Stummschaltung Aktivierungsbits Bits 0x1600



PLC-Ausgangsdaten Name	Ausgabe-Datentyp
Ein/Aus, Mute-Freigabe VI RxPDO [2] 0x1601 Byte 0	BYTE
Ein/Aus, Mute-Freigabe VI RxPDO [2] 0x1601 Byte 1	BYTE
Ein/Aus, Mute-Freigabe VI RxPDO [2] 0x1601 Byte 2	BYTE
Ein/Aus, Mute-Freigabe VI RxPDO [2] 0x1601 Byte 3	BYTE

Tabelle 75: Virtuell Ein, Aus, Stummschaltung Aktivierungsbits Bits 0x1601

Virtueller Reset, Abbruchverzögerung (RCD) Steuerung

PDO 26 enthält den RCD Actuation Code, ein wichtiges Codewort, das in der virtuellen Reset-, Cancel Delay-Sequenz verwendet wird.

Siehe Virtuelle manuelle Rückstell- und Abbruchverzögerungssequenz (RCD) auf Seite 61. Dieses PDO enthält auch sechzehn virtuelle nicht sicherheitsrelevante Eingänge, die in der virtuellen Rücksetz- und Abbruchverzögerungssequenz verwendet werden können.

PLC-Eingangsdaten Name	Eingangsdaten Typ
RCD-Betätigungscode	UDINT
Reset, Abbruch der Dealy Control RxPDO [1] 0x1602 Byte 0	BYTE
Reset, Dealy Control abbrechen RxPDO [1] 0x1602 Byte 1	BYTE

Tabelle 76: RCD-Steuerung

DCD Informationsanfrage für einzelne Geräte

PDO 27 enthält die Antwortdaten für die Kommunikation mit einem einzelnen DCD-Gerät.

Siehe auch Abfrage von Leistungs- und Statusinformationen zu einem einzelnen Gerät über DCD auf Seite 50 und DCD Individuelle gerätespezifische Daten - detaillierte Beschreibung auf Seite 202.

PLC-Eingangsdaten Name	Eingangsdaten Typ
DCD Leseanforderung	UINT
DCD-Kette angefordert	UINT
DCD-Gerät angefordert	UINT

Tabelle 77: DCD-Anfrage für individuelle Geräteinformationen

12.7.7 Anweisungen zur Konfiguration

Installieren der ESI-Datei

Verwenden Sie diese Anleitung, um die ESI-Datei in der Beckhoff TwinCAT 3 Software zu installieren.

1. Laden Sie die ESI-Datei von www.bernstein.eu herunter.
2. Navigieren Sie zum Ordner `TwinCAT/3.1/Config/IO/EtherCAT`.
3. Verschieben Sie die ESI-Datei in diesen Ordner.

Die ESI wird beim nächsten Programmstart in TwinCAT verfügbar sein.

Hinzufügen der Sicherheitssteuerung zu einem Projekt

Verwenden Sie diese Anweisungen, um ein SCx-Gerät zu einem TwinCAT-Projekt hinzuzufügen.

1. Starten Sie die TwinCAT 3 Software.
2. Öffnen Sie ein Projekt.
3. Erweitern Sie die E/A-Auswahl.
4. Klicken Sie mit der rechten Maustaste auf das Gerät, zu dem der BERNSTEIN Safety Controller gehören soll.



Hinzufügen der Sicherheitssteuerung zu einem Projekt

Verwenden Sie diese Anweisungen, um ein SCx-Gerät zu einem TwinCAT-Projekt hinzuzufügen.

1. Starten Sie die TwinCAT 3 Software.
2. Öffnen Sie ein Projekt.
3. Erweitern Sie die E/A-Auswahl.
4. Klicken Sie mit der rechten Maustaste auf das Gerät, zu dem der BERNSTEIN Safety Controller gehören soll.
5. Wählen Sie die Option **Neuen Artikel hinzufügen**.
„BERNSTEIN AG“ wird aufgelistet. Optional können Sie die Suche verwenden und SCx eingeben, um die ESI schnell auszuwählen.
6. Wählen Sie das **SCx EtherCAT-Modul**.
7. Ändern Sie den **Namen** nach Bedarf für Ihr System.
8. Klicken Sie auf **OK**, um die Sicherheitssteuerung dem System hinzuzufügen.

12.7.8 EtherCAT® PDO-Änderung

Das EtherCAT-PDO kann geändert werden. Standardmäßig ist nur ein bestimmter Satz von Daten aktiviert.

Es ist möglich, PDO einzuschalten, die gerade ausgeschaltet sind, und gleichzeitig PDO auszuschalten, die gerade eingeschaltet sind. Durch die Anpassung der PDOs können nur die für die Anwendung benötigten Daten gesendet und empfangen werden.

Je kleiner das PDO ist, desto leichter lässt es sich in die zugewiesene Paketgröße für EtherCAT einpassen. Verwenden Sie die folgenden Anweisungen, um PDO je nach Bedarf ein- und auszuschalten.

Zugriff auf das PDO-Menü

1. Doppelklicken Sie im TwinCAT Solution Explorer auf den BERNSTEIN Safety Controller in der E/A-Struktur. Es öffnet sich ein Fenster. Die Registerkarte **Allgemein** ist standardmäßig aktiv.
2. Klicken Sie auf die Registerkarte **Prozessdaten**.
Dies ist die Registerkarte, die das Ein- und Ausschalten von PDO ermöglicht.
3. Notieren Sie sich die Ausgänge und Eingänge im **Sync Manager**-Fenster.

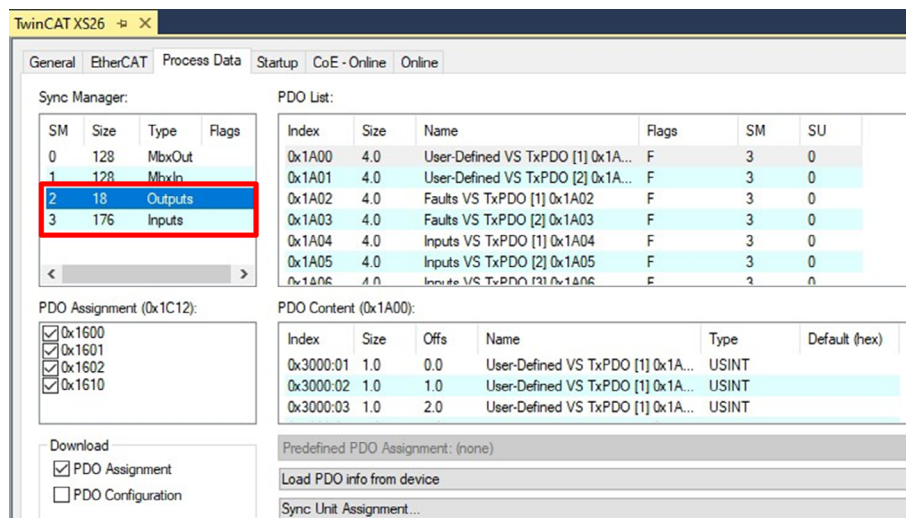


Abbildung 165: Ausgang und Eingänge im Sync Manager

PDO ausschalten

Diese Beispielprozedur schaltet ein Ausgangs-PDO aus.

1. Wählen Sie im Fenster **Sync Manager** in TwinCAT entweder **Ausgänge** oder **Eingänge** aus.
2. Untersuchen Sie den Bereich **PDO-Zuordnung** für Ausgänge.
3. Deaktivieren Sie das Kontrollkästchen für das Element, das Sie ausschalten möchten.
In diesem Beispiel wird PDO 0x1610 (DCD Device Information Request) ausgeschaltet.



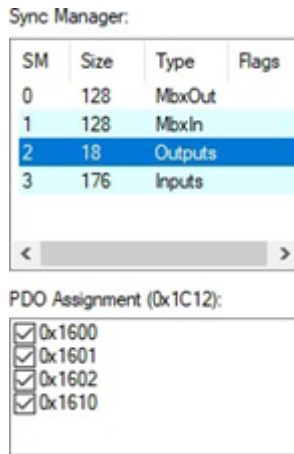


Abbildung 166: PDO-Zuweisung - Alle Ausgänge

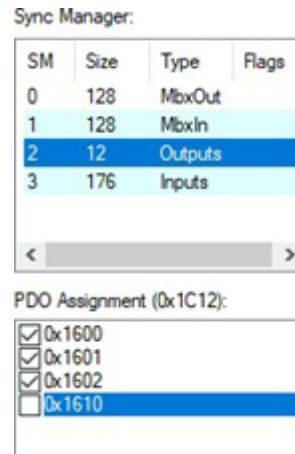


Abbildung 167: PDO-Zuweisung - 0x1610

4. Wiederholen Sie diesen Vorgang nach Bedarf für alle Elemente, die ausgeschaltet werden müssen.

Einschalten eines PDO

Diese Beispielprozedur schaltet ein Eingangs-PDO ein.

1. Wählen Sie im Fenster **Sync Manager** in TwinCAT entweder **Ausgänge** oder **Eingänge** aus.
2. Untersuchen Sie den Bereich **PDO-Zuordnung** für Eingaben.
3. Aktivieren Sie das Kontrollkästchen für das Element oder die Elemente, die Sie einschalten möchten.
In diesem Beispiel werden die PDO 0x1A20 und 0x1A21 (DCD Status Chain 1 und DCD Status Chain 2) eingeschaltet.

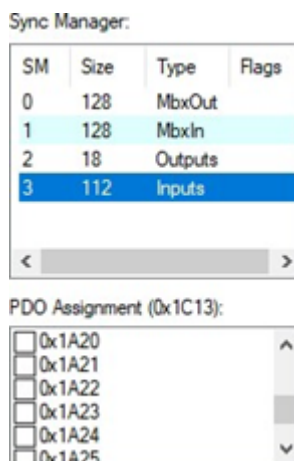


Abbildung 168: PDO-Zuweisung - Alle Eingänge

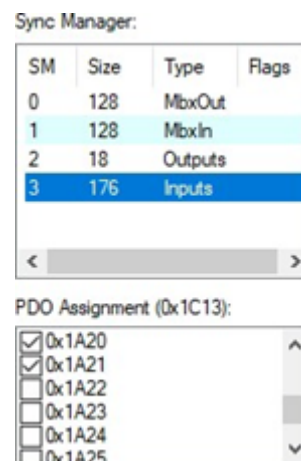


Abbildung 169: PDO-Zuweisung - zwei Eingänge ausgewählt



12.8 Daisy Chain Diagnose - DCD

12.8.1 Leistungs- und Statusinformationen zu einem einzelnen Gerät über DCD anfordern

Sehen Sie hierfür bitte in den jeweiligen Kapiteln der des verwendeten Industrial-Ethernets nach.

12.8.2 DCD-Reihe Systemstatus

Der Systemstatus der DCD-Reihe besteht aus mehreren Wörtern, auf die von der SPS schnell zugegriffen werden kann, ohne dass vorab eine Anforderung an die Sicherheitsauswertung gesendet werden muss. Auf diese Weise kann über die SPS schnell ausgewertet werden, ob Probleme mit der DCD-Reihenschaltung vorliegen.

Diese Informationen haben das folgende Format:

Informationen	Typ	Datengröße
Zahl der Geräte in der DCD-Reihe stimmt nicht mit der Konfiguration überein	SCR P-Warnung	1 Bit
Reihenfolge der Geräte in der DCD-Reihe stimmt nicht mit der Konfiguration überein	SCR P- und SCx-Warnung	1 Bit
Von der konfigurierten DCD-Reihe wurden keine DCD-Daten empfangen	SCR P-Warnung	1 Bit
Ungültiges (nicht DCD-fähiges) Gerät in der DCD-Reihe gefunden	SCR P-Warnung	1 Bit
Reserviert		1 Bit
Abschlussstecker der DCD-Reihe fehlt	DCD-Status	1 Bit
SRF-Betätiger nicht eingelernt (hoch- oder unique-codiert)	DCD-Fehler	1 Bit
Falscher SRF-Betätiger erkannt (hoch- oder unique-codiert)	DCD-Fehler	1 Bit
Interner Fehler in einem DCD-Gerät	DCD-Fehler	1 Bit
Ausgangsfehler in einem DCD-Gerät erkannt, Timer (20Min.) zum Ausschalten der Ausgänge gestartet	DCD-Fehler	1 Bit
Reserviert		2 Bit
DCD-Reihe OSSD-Status	DCD-Status	1 Bit

Tabelle 78: DCD-Reihe Systemstatus



12.8.3 Spezifische Daten einzelner DCD-Geräte

Bei DCD-fähigen Geräten haben die spezifischen Daten einzelner Geräte das folgende Format:

Informationen	Abkürzung	Datengröße
Eingangsfehlerquittierung nötig	EF	1 Bit
reserviert	--	1 Bit
Betätiger nicht eingelernt (SRF)	BE	1-bit
DCD-Datenfehler	CE	1-bit
Falscher Betätiger (SRF) / Zustand Sicherheitskontakt 2 (SEU)	FB	1-bit
Betätiger im Randbereich (SRF) / Zustand Sicherheitskontakt 1 (SEU)	BB	1-bit
Betätiger erkannt (SRF)	RB	1-bit
Ausgangsfehler: Querschluss erkannt	QS	1-bit
Zustand Sicherheitseingang 2	E2	1-bit
Zustand Sicherheitseingang 1	E1	1-bit
Lokaler Reset erwartet	LS	1-bit
Betriebsspannung Warnung	UW	1-bit
Betriebsspannung Fehler	UF	1-bit
Zustand Sicherheitsausgang 2	Q2	1-bit
Zustand Sicherheitsausgang 1	Q1	1-bit
Stopp-Modus: Neustart der Komponente erforderlich	MF	1-bit
Mit fehlertolerantem Ausgang	MQ	1-bit
Mit Lokalem Reset	MS	1-bit
Reihenschaltbar	RS	1-bit
Mit hoher (oder unique) Codierung	HC	1-bit
Anzahl verbleibender Teach-Vorgänge (hoch- oder unique-codiert)	RTP	4-bit
Geräte-ID	--	5-bit
Zähler Betätiger im Randbereich (SRF)	--	6-bit
Ausgangsfehler: Timer Querschluss (20 Min.)	--	5-bit
Zähler Betriebsspannungswarnung	--	8-bit
Temperatur	--	8-bit
Abstand Betätiger	--	8-bit
Betriebsspannung	--	8-bit
Erwarteter Herstellercode	--	4-bit
Empfangener Herstellercode	--	4-bit
Erwartete Betätiger-ID	--	16-bit
Empfangene Betätiger-ID	--	16-bit
Interner Fehler A	--	16-bit
Interner Fehler B	--	16-bit

Tabelle 79: Spezifische Daten einzelner DCD-Geräte

20 Informationen zur Umrechnung von Innentemperatur, Auslöserabstand und Betriebsspannung finden Sie unter „12.8.4 Informationen zur Temperatur-, Spannungs- und Abstandsum-wandlung“ auf Seite 216



12.8.4 Informationen zur Temperatur-, Spannungs- und Abstandsum-wandlung

Laden Sie eine AOI (Add-on-Anweisung) von <http://www.bernstein.eu> herunter, die Sie in das SPS-Programm einbinden können, um die abgerufenen Werte in echte Werte umzuwandeln.

12.8.5 Versorgungsspannung

Der tatsächliche Spannungswert berechnet sich aus dem an die SPS gesendeten ADC-Wert multipliziert mit 0,1835.

Betriebsspannung = ADC-Wert × 0,1835

12.8.6 Innentemperatur

Verschieben Sie zuerst den verbliebenen ADC-Wert um 2 Bit. Wandeln Sie dann den binären Messwert in eine Zahl um. Wenn die Zahl dem ADC-Wert der folgenden Tabelle entspricht, lesen Sie die Temperatur einfach ab. Liegt die Zahl zwischen den Messwerten in der Tabelle, berechnen Sie die tatsächliche Temperatur anhand der folgenden Formel.

$$\text{Internal Temperature} = ((A-L) / (H-L)) \times 5 + T$$

- A**
der von der Sicherheitsauswertung bezogene ADC-Wert
- L**
der ADC-Wert in der Nachschlagetabelle kleiner oder gleich A
- H**
der ADC-Wert in der Nachschlagetabelle größer A
- T**
die mit dem L-Wert verbundene Temperatur

ADC-Messwert	Temperatur (°C)
41	-40
54	-35
69	-30
88	-25
110	-20
136	-15
165	-10
199	-5
237	0
278	5
321	10
367	15
414	20
461	25
508	30
554	35
598	40
640	45
679	50
715	55
748	60
778	65
804	70
829	75
850	80
869	85
886	90
901	95
914	100
926	105
936	110

Tabelle 80: Temperatur



12.8.7 Abstand Betätiger

Wandeln Sie den binären Messwert in eine Zahl um. Wenn die Zahl dem ADC-Wert der folgenden Tabelle entspricht, lesen Sie den Abstand einfach ab. Liegt die Zahl zwischen den Messwerten in der Tabelle, berechnen Sie den tatsächlichen Abstand anhand der folgenden Formel.

$$\text{Actuator Distance} = ((A-L) / (H-L)) + D$$

- A**
der von der Sicherheitsauswertung bezogene ADC-Wert
- L**
der ADC-Wert in der Nachschlagetabelle kleiner oder gleich A
- H**
der ADC-Wert in der Nachschlagetabelle größer A
- D**
der Abstand im Zusammenhang mit dem L-Wert

ADC-Messwert	Abstand (mm)
<62	<7
62	7
65	8
77	9
110	10
133	11
148	12
158	13
163	14
169	15
172	16
176	17
180	18
>180	>18

Tabelle 81: Abstand Betätiger



13. Systemüberprüfung

13.1 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. „13.2.2 Setup vor der Inbetriebnahme, Inbetriebnahme und regelmäßige Prüfroutinen“ auf Seite 219 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) 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 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 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 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.**

13.2 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.



13.2.1 Überprüfung des Systembetriebs

Die Inbetriebnahmeprüfung muss von einer qualifizierten Person durchgeführt werden. 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 „7.5 Optionen für Sicherheitseingangsgeräte“ auf Seite 36 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 „13.1 Zeitplan für vorgeschriebene Überprüfungen“ auf Seite 218).

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 galvanisch getrennt** (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 67 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.

13.2.2 Setup vor der Inbetriebnahme, Inbetriebnahme und regelmäßige Prüfroutinen

In der Phase der ersten Konfigurationsüberprüfung gibt es zwei Möglichkeiten der Überprüfung, dass die Sicherheitsausgänge den Status zu den vorgesehenen Zeiten wechseln (öffnen Sie die Registerkarte **Konfigurationsübersicht** in der Software, um den Anlauftest und die Konfigurationseinstellungen für Netzeinschaltung anzuzeigen):

- Beobachten Sie die den Ein- und Ausgängen zugeordneten LEDs. Leuchtet die Eingangs-LED grün, ist der Eingang eingeschaltet (bzw. 24 V). Leuchtet die Eingangs-LED rot, ist der Eingang ausgeschaltet (bzw. 0 V). Analog leuchtet die entsprechende LED grün, wenn die RO1- und RO2-Ausgangskontakte geschlossen sind. Sind die Kontakte hingegen geöffnet, leuchtet die LED rot.
- Starten Sie den **Livemodus** 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 Zustimmtasterfunktionen verbundenen Ausgänge nicht ein. Nach der Netzeinschaltung müssen diese Vorrichtungen in den Aus-Zustand und wieder in den Ein-Zustand geschaltet werden, damit sich ihre zugehörigen Ausgänge einschalten.

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).

¹⁰ Für Definitionen siehe „19. Glossar“ auf Seite 255.



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.



Hinweis: Blinkt die Anzeige für einen Ein- oder Ausgang rot, siehe „15. Fehlerbehebung“ auf Seite 238

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, über-springen 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.

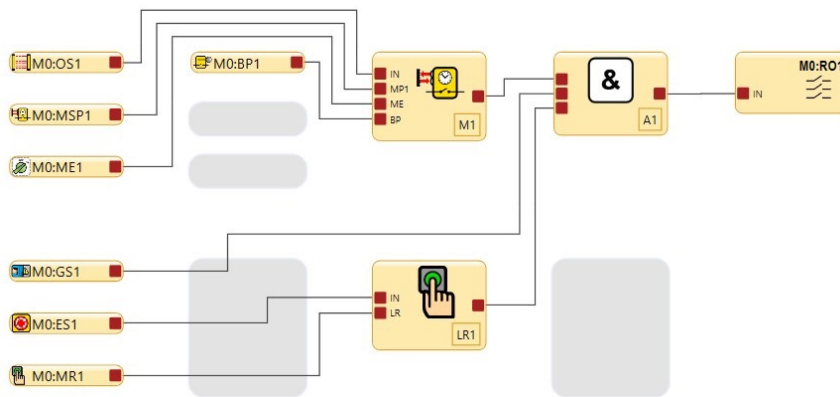


Abbildung 170: Setup: Eingänge ohne Überbrückung

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

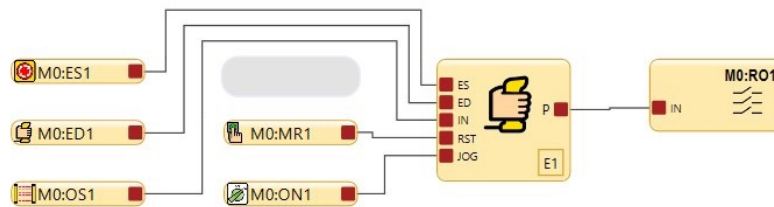


Abbildung 171: Setup: Zustimmtasterfunktion ohne sekundären Weiterschaltausgang

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 Weberschaltfunktion am Sekundärausgang

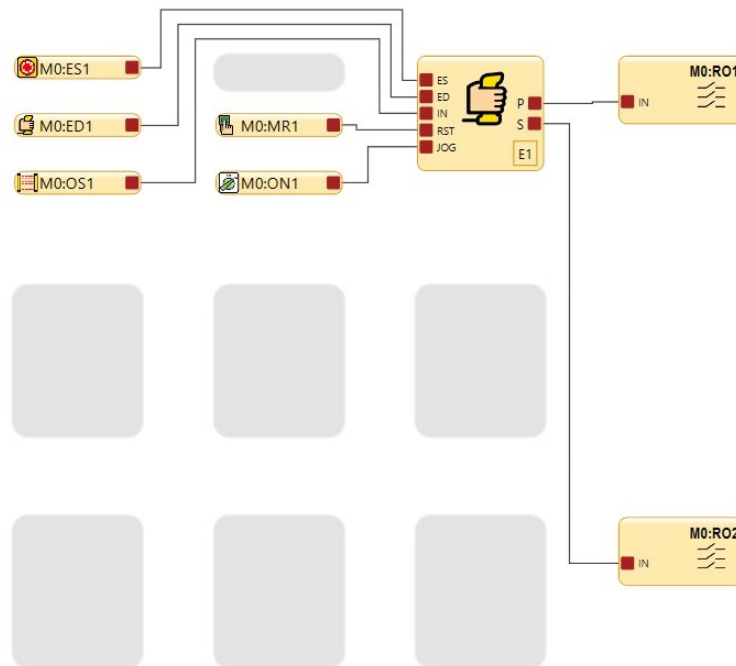


Abbildung 172: Setup: Zustimmtasterfunktion - mit Weberschaltfunktion am Sekundärausgang

1. Prüfen Sie, während sich der Zustimmtaster und die Weberschalttaste im Ein-Zustand befinden und den primären Sicherheitsausgang steuern, ob sich der Ausgang ausschaltet, wenn entweder der Zustimmtaster oder die Weberschalttaste in den Aus-Zustand geschaltet werden.
2. Prüfen Sie, während der Zustimmtaster den primären Sicherheitsausgang steuert und die Weberschalttaste 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 Weberschalttaste 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 Weberschalttaste im Ein-Zustand befindet.
4. Prüfen Sie, ob der Sekundärausgang folgende Schaltungen ausführt:
 - a. Einschaltung, wenn sich der Zustimmtaster und die Weberschalttaste im Ein-Zustand befinden.
 - b. Ausschaltung, wenn sich der Zustimmtaster oder die Weberschalttaste im Aus-Zustand befindet.

14. Informationen zum Status und zum Betrieb

Bedienen Sie die Sicherheitssteuerung SCx entweder über die integrierte Schnittstelle oder über die Software, um den aktuellen Status zu überwachen.

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



14.1 Status der LED-Anzeigen am SCx

LED	Status	Bedeutung
Alle	Aus	Initialisierungsmodus
	Abfolge: Grün EIN für 0,5 s Rot EIN für 0,5 s Aus für min. 0,5 s	Angewandte Leistung
Leistung/ Störung	AUS	Ausschalten
	Grün: EIN	Betriebsmodus
	Grün: Blinkend	Konfigurationsmodus ODER Manueller Einschaltmodus
	Rot: Blinkend	Manueller Einschaltmodus
USB (FID 2 oder früherer Basis- Controller)	AUS	Keine Verbindung zum PC hergestellt
	Grün: EIN	Verbindung zum PC hergestellt
	Grün: Blinken für 5 s, dann AUS	Übereinstimmung der SCR P-FPS-Konfiguration
	Rot: Blinken für 5 s, dann AUS	SCR P-FPS-Konfiguration stimmt nicht überein
USB (FID 3 oder höherer Basis- Controller)	AUS	Keine Verbindung hergestellt und konfiguriert Sicherheitssteuerung
	Grün: EIN	USB-Kabel, angeschlossen an eine konfigurierte Sicherheitssteuerung
	Grün: Blinkend	Keine Verbindung hergestellt und Werkseinstellung Sicherheitssteuerung ODER USB-Kabel angeschlossen und Werkseinstellung Safety Controller
	Grün: Blinken für 4 s, dann Grün EIN	Konfigurierter neuer SCR P-FPS ⁷² (verriegelt oder unverriegelt), der an eine werkseitig eingestellte Sicherheitssteuerung angeschlossen ist
	Grün: Blinken für 5 s, dann AUS	Konfigurierter und entsperrter neuer SCx ⁷² , der an eine konfigurierte Sicherheitssteuerung mit übereinstimmender Konfiguration, übereinstimmenden Passwörtern und übereinstimmenden oder nicht übereinstimmenden Netzwerkeinstellungen angeschlossen ist OR Der alte SCR P-FPS ⁷³ wird in den FID 3 oder einen neueren Controller eingesetzt (konfiguriert oder werkseitig voreingestellt) und hat eine passende Konfiguration
	Grün: Blinken für 5 s, dann Rot blinkend	Konfigurierter und gesperrter neuer SCR P-FPS ⁷² , der an eine konfigurierte Sicherheitssteuerung mit übereinstimmender Konfiguration und übereinstimmenden Kennwörtern, aber nicht übereinstimmenden Netzwerkeinstellungen angeschlossen ist
	Rot: Blinkend	Konfigurierter neuer SCR P-FPS ⁷² (verriegelt oder nicht verriegelt), der in eine konfigurierte Sicherheitssteuerung mit einer nicht übereinstimmenden Konfiguration, einem nicht übereinstimmenden Passwort oder einem leeren SCR P-FPS eingesteckt ist OR Leerer SCR P-FPS, angeschlossen an eine werkseitig voreingestellte Sicherheitssteuerung oder eine konfigurierte Sicherheitssteuerung
	Rot: Blinken für 5 s, dann AUS	Alter SCR P-FPS ⁷³ wird in FID 3 oder spätere Steuergeräte eingesetzt (konfiguriert oder werkseitig eingestellt) und hat eine nicht übereinstimmende Konfiguration
Eingaben	Grün: EIN	Keine Eingangsfehler
	Rot: Blinkend	Ein oder mehrere Eingänge befinden sich im Zustand „Sperr“.

⁷² „Neuer SCR P-FPS“: ein SCR P-FPS, der Informationen enthält, die mit der BERNSTEIN Safety Controller Software Version 4.2 oder höher erstellt wurden, oder der von einem FID 3 oder höher Safety Controller erstellt wurde.

⁷³ „Alter SCR P-FPS“: ein SCR P-FPS, der Informationen enthält, die mit der BERNSTEIN Safety Controller Software Version 4.1 oder früher erstellt wurden, oder der von einer Sicherheitssteuerung FID 2 oder früher erstellt wurde.



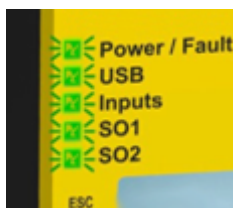
LED	Status	Bedeutung
SO1, SO2	AUS	Ausgang nicht konfiguriert
	Grün: EIN	Sicherheitsausgang ON
	Rot: EIN	Sicherheitsausgang AUS
	Rot: Blinkend	Fehler am Sicherheitsausgang erkannt oder EDM-Fehler erkannt oder AVM-Fehler erkannt

LED-Status für Split-Ausgänge	Bedeutung
Grün: EIN	Beide Ausgänge sind EIN
Rot: EIN	SOxa und/oder SOxb ist AUS
Rot: Blinkend	SOxa- und/oder SOxb-Fehler erkannt

Ethernet-Diagnose-LEDs		
Gelbe LED	Grüne LED	Beschreibung
EIN	Variiert je nach Datenverkehr	Verbindung hergestellt/Normalbetrieb
AUS	AUS	Hardware-Ausfall

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 Flash-Befehl	Bedeutung
Die LEDs des Basis-Controllers blinken 4 Sekunden lang	Die blinkenden LEDs zeigen an, dass der Base Controller angeschlossen ist. Dies ist das Ergebnis des Befehls „Flash LED“ aus dem PROFINET-Netzwerk.



14.2 Statusanzeigen der Eingangsmodule

Die folgenden Informationen beziehen sich auf die Modelle SCx-I-8 und SCx-I-16

LED	Status	Bedeutung
Alle	Sequenz: Grün EIN für 0,5 s Rot EIN für 0,5 s AUS für mindestens 0,5 s	Angewandte Leistung
	AUS	Initialisierungsmodus



14.3 Ausgangsmodul (Solid-State oder Relais) Statusanzeigen

Die folgenden Informationen beziehen sich auf die Modelle SCx-O-2T, SCx-O-4T, SCx-O-1R und SCx-O-1R.

LED	Status	Bedeutung
Alle	Sequenz: Grün EIN für 0,5 s Rot EIN für 0,5 s AUS für mindestens 0,5 s	Angewandte Leistung
	AUS	Initialisierungsmodus
Energie- Anzeige	AUS	Ausschalten
	Grün: EIN	Strom einschalten
	Rot: Blinkend	Verriegelungszustand bei Nichtbetrieb
Senden/ Empfangen- Anzeige	Grün: EIN	Übermittlung oder Empfang von Daten
	Rot: EIN	Keine Kommunikation
	Rot: Blinkend	Kommunikationsfehler erkannt ODER Sicherheitsbus-Kommunikationsproblem
Indikatoren für die Sicher- heitsleistung	AUS	Ausgang nicht konfiguriert
	Grün: EIN	Zwei einkanalige Sicherheitsausgänge (beide EIN) ODER Zweikanaliger oder ein einkanaliger Sicherheitsausgang ON
	Rot: EIN	Zwei einkanalige Sicherheitsausgänge (1 EIN und 1 AUS)
	Rot: EIN	Zwei einkanalige Sicherheitsausgänge (beide AUS) ODER Zweikanaliger oder ein einkanaliger Sicherheitsausgang AUS (anderer Kanal nicht verwendet)
	Rot: Blinkend	Sicherheit Fehler am Ausgang erkannt



14.4 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
	Abfolge: 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 Werkzustand; 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 Werkzustand 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 Anmerkung: 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 und verriegeltes SCR P-FPS in eine konfigurierte Sicherheitsauswertung mit übereinstimmender Konfiguration und übereinstimmenden Passwörtern, aber nicht übereinstimmenden Netzwerkstellungen eingesteckt
Eingänge (10)	Grün konstant	24 V DC und kein Fehler 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>

14.5 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 165 erhalten Sie weitere Informationen.

Die Registerkarte „Livemodus“ enthält dieselben Informationen, die auch auf dem Display der Sicherheitssteuerung SCx angezeigt werden können.

14.6 Informationen zum Livemodus: Onboard-Schnittstelle

Zur Anzeige von Echtzeit-Betriebsmodus-Informationen auf dem Display der Sicherheitssteuerung (Modelle mit Display) wählen Sie Systemstatus 74 aus dem Systemmenü (siehe SCx Onboard Interface auf Seite 163 für eine Navigationskarte). Der Systemstatus zeigt die Zustände des Eingangsgeräts und des Sicherheitsausgangs an; die Fehlerdiagnose zeigt aktuelle Fehlerinformationen (eine kurze Beschreibung, Abhilfemaßnahmen und den Fehlercode) und bietet Zugriff auf das Fehlerprotokoll. Weitere Informationen finden Sie unter SCx Onboard Interface auf Seite 163.

Das Display des Sicherheits-Controllers liefert dieselben Informationen, die auch über die Livemodus-Funktion der Software angezeigt werden können.



14.7 Sperrzustände

Sperrzustände von Eingängen werden in der Regel behoben, indem der Fehler repariert wird und der Eingang aus- und wieder eingeschaltet wird.

Sperrzustände an den Ausgängen (einschließlich EDM- und AVM-Fehlern) werden behoben, indem der Fehler repariert wird und anschließend der an den 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.**

14.8 Nach einem Sperrzustand

Zur Behebung eines Sperrzustands:

- Folgen Sie der Empfehlung in der Fehleranzeige (Modelle mit Display)
- Befolgen Sie die empfohlenen Schritte und Prüfungen, die in der „15.5 SCx-Fehlercode-Tabelle“ auf Seite 243 oder der „15.6 SCR P-Fehlercode-Tabelle“ auf Seite 249 aufgeführt sind.
- System-Reset durchführen
- Schalten Sie die Stromversorgung aus und wieder ein und führen Sie bei Bedarf einen System-Reset durch.

Wenn diese Schritte den Sperrzustand nicht beheben, wenden Sie sich die BERNSTEIN AG (siehe „17.2 Reparaturen und Garantie“ auf Seite 252).



14.9 SCR P und SCx: Automatische Optimierung von Anschlüssen

Mit den folgenden Schritten erstellen Sie eine Beispielkonfiguration, die die Funktion für die automatische Optimierung von Anschlüssen (ATO) verwendet.






Hinweis: 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.

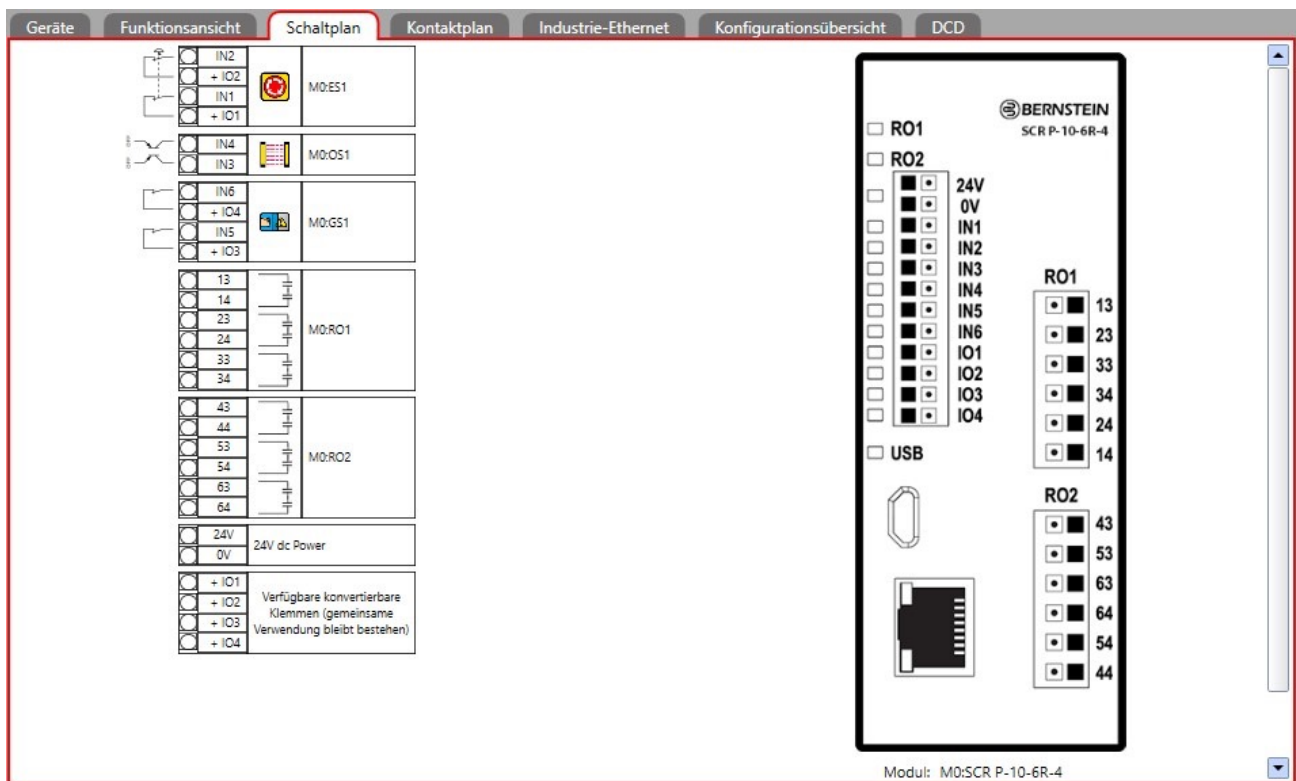



Abbildung 173: Registerkarte Schaltplan mit einem Not-Halt-Schalter, optischen Sensor und Schutztürschalter

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.

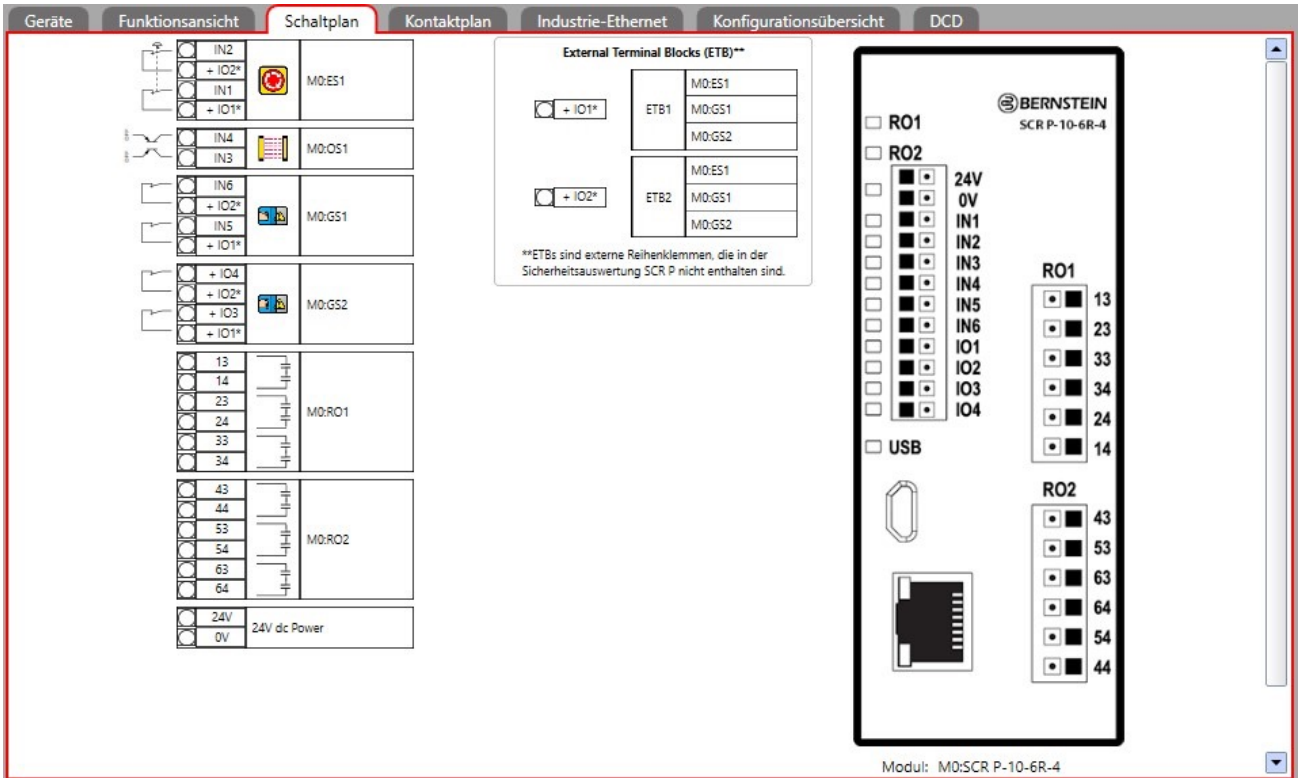


Abbildung 174: Registerkarte **Schaltplan** mit drei Not-Aus-Tastern und ETBs

14.10 Beispielkonfiguration für das SCR P und SCx 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

Konfigurationsname:

Projekt:

Autor:

Hinweise:

Projektdatum:

Funktion für die automatische Optimierung von Anschlüssen deaktivieren

Abbildung 175: 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

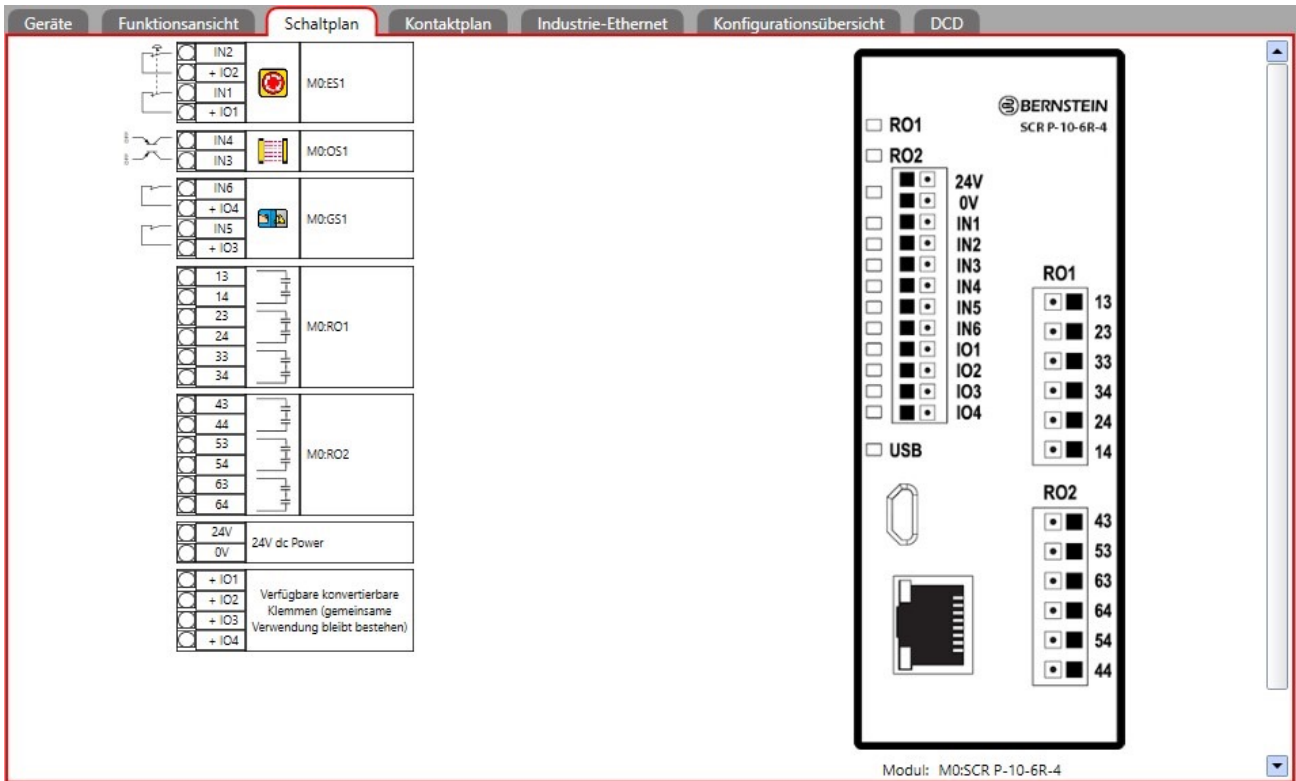


Abbildung 176: Registerkarte Schaltplan mit einem Not-Halt-Schalter, optischen Sensor und Schutztürschalter

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.

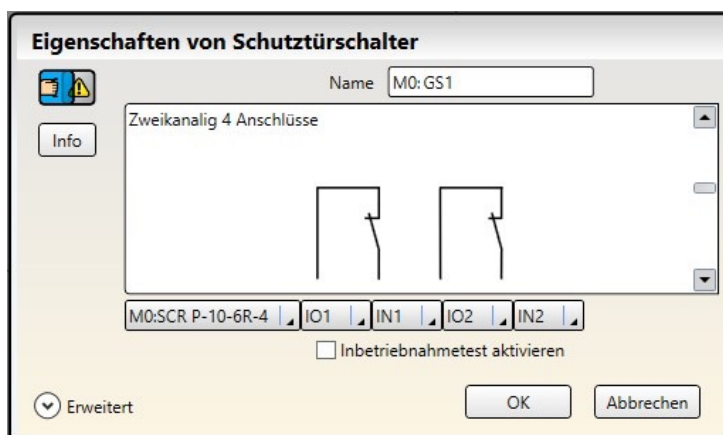


Abbildung 177: Schutztürschaltereigenschaften

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

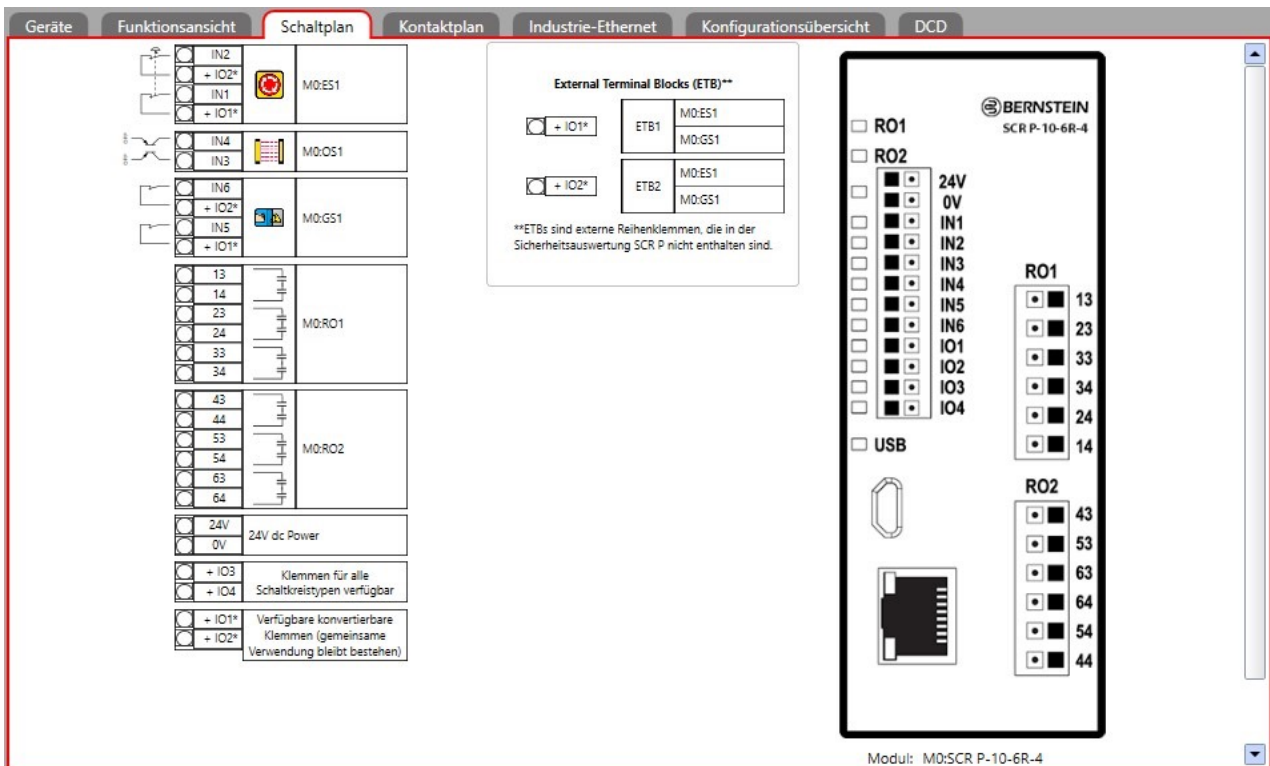


Abbildung 178: Registerkarte Schaltplan mit einem Not-Halt-Schalter, optischen Sensor, Schutztürschalter und ETBs

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.

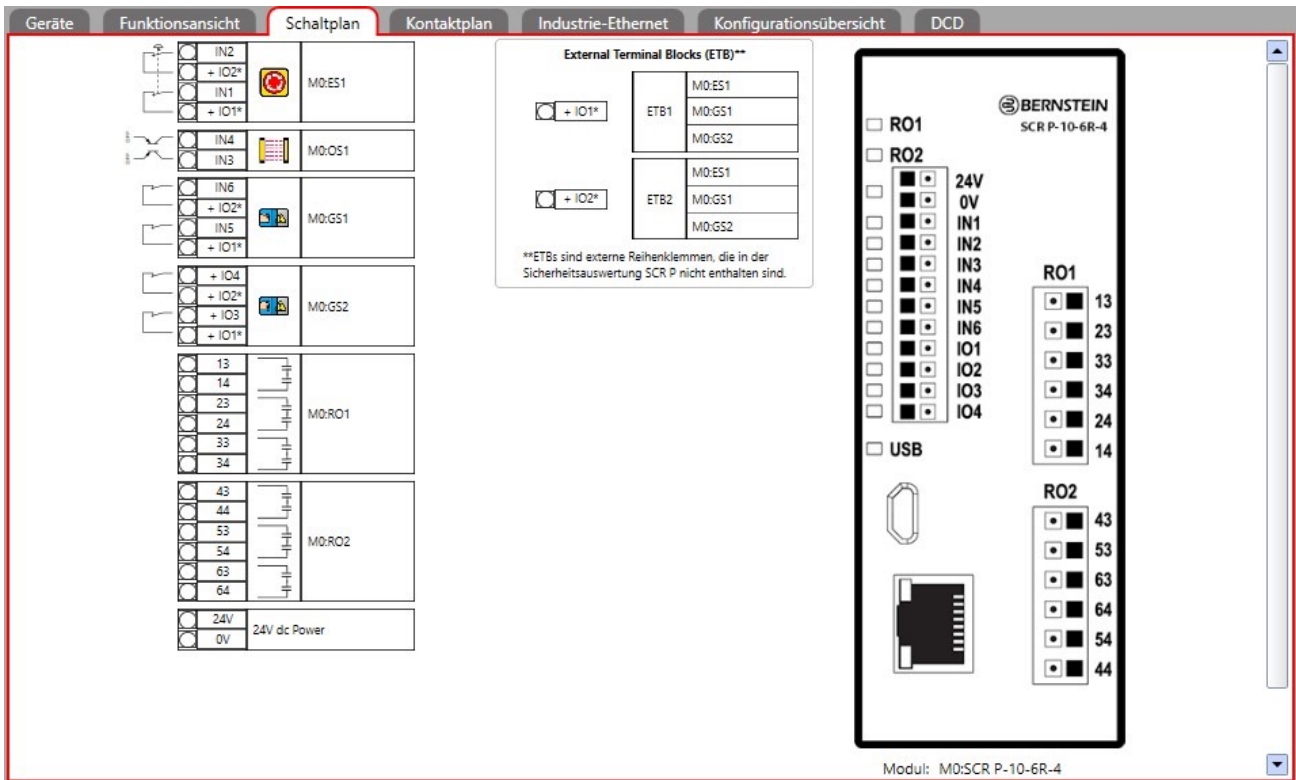


Abbildung 179: Registerkarte **Schaltplan** mit Not-Halt-Schalter, optischen Sensor, Schutztürschaltern und ETBs

14.11 SCx-Modelle mit integrierter Schnittstelle: Verwendung des SCR P-FPS

Verwenden Sie einen SCR P-FPS, um:

- Speichern einer bestätigten Konfiguration
- Schnelle Konfiguration mehrerer SCx-Sicherheitssteuerungen mit der gleichen Konfiguration
- Ersetzen einer SCx-Sicherheitssteuerung durch eine andere mit SCR P-FPS (FID 3 oder höher)

Hinweis: Das BERNSTEIN Programmieradapter (SCR P-PA) und die BERNSTEIN Safety Controller Software sind erforderlich, um eine bestätigte Konfiguration in einen SCR P-FPS zu schreiben. Dies beschränkt den Zugang auf autorisiertes Personal. Eine Konfiguration kann auch mit Hilfe eines Sicherheits-Controllers mit integrierter Schnittstelle in einen SCR P-FPS geschrieben werden.

Hinweis: Die LEDs verhalten sich mit oder ohne Onboard-Schnittstelle gleich (weitere Informationen finden Sie unter SCx-Modelle ohne Onboard-Schnittstelle: Verwendung des SCR P-FPS auf Seite 321), das folgende Verfahren konzentriert sich jedoch auf das, was auf dem Display geschieht.

14.12 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 „13.2 Inbetriebnahmeprüfung“ auf Seite 218.

14.13 SCx bzw. SCR P auf die Werkseinstellungen zurücksetzen

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

SCx bzw. 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 zurück-gesetzt werden.
3. Klicken Sie auf **Weiter**.
Der Bildschirm **Passwort eingeben** wird geöffnet.
4. Geben Sie das Passwort Benutzer1 ein und klicken Sie auf **OK**.
SCx bzw. SCR P wird auf die Werkseinstellungen zurückgesetzt und ein Bestätigungsfenster wird angezeigt.
5. Klicken Sie auf **OK**.
6. **Das Gerät aus- und wiedereinschalten.**
Die Werkseinstellungen sind damit wiederhergestellt..



14.14 Werkseinstellungen

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

Einstellung	Werkseinstellung	Produkt
AVM-Funktion	50 ms	SCx, SCR P
Ausschaltentprellzeit	6 ms	SCx, SCR P
EDM	Keine EDM-Überwachung	SCx, SCR P
Funktionsblock: Überbrückungsblock – Standardknoten	IN, BP	SCx, SCR P
Funktionsblock: Überbrückungs-Zeitlimit	1 s	SCx, SCR P
Funktionsblock: Verzögerungsblock – Standardknoten	IN	SCx, SCR P
Funktionsblock: Verzögerungsblock – Ausschaltverzögerung	100 ms	SCx, SCR P
Funktionsblock: Zustimmungstasterblock – Standardknoten	ED, IN, RST	SCx, SCR P
Funktionsblock: Zustimmungstasterblock – Zeitlimit	1 s	SCx, SCR P
Funktionsblock: Latch-Reset-Block – Standardknoten	IN, LR	SCx, SCR P
Funktionsblock: Mutingblock – Standardknoten	IN, MP1	SCx, SCR P
Funktionsblock: Mutingblock – Zeitlimit	30 s	SCx, SCR P
Funktionsblock: Zweihandsteuerungsblock – Standardknoten	TC	SCx, SCR P
Funktionsblock: One Shot Block-Default Nodes	IN	SCx
Funktion Block: One Shot Block-Time Limit	100 ms	SCx
Industrie-Ethernet: Zeichenfolge (EtherNet/IP und PCCC-Protokoll)	32 Bit	SCx, SCR P
Netzwerkeinstellungen: Gateway-Adresse	0.0.0.0	SCx, SCR P
Netzwerkeinstellungen: IP-Adresse	192.168.0.128	SCx, SCR P
Netzwerkeinstellungen: Verbindungsgeschwindigkeit und Duplexmodus	Automatische Aushandlung	SCx, SCR P
Netzwerkeinstellungen: Subnetzmaske	255.255.255.0	SCx, SCR P
Netzwerkeinstellungen: TCP-Port	502	SCx, SCR P
Einschaltentprellzeit	50 ms	SCx, SCR P
Passwort Benutzer1	1901	SCx, SCR P
Passwort Benutzer2	1902	SCx, SCR P
Passwort Benutzer3	1903	SCx, SCR P
Anlaufmodus	Normal	SCR P
Sicherheitsausgänge	Automatischer Reset (Schaltmodus)	SCx, SCR P
Sicherheitsausgänge: Anlaufmodus	Normal	SCx
Sicherheitsausgänge: Teilen (Sicherheitsausgänge)	Paarweise Funktion	SCx
Simulationsmodus: Simulationsgeschwindigkeit	1	SCx, SCR P
Automatische Optimierung von Anschlüssen	Aktiviert	SCR P
Signallogik für Statusausgänge	Aktiv = PNP ein	SCx, SCR P
Blinkfrequenz Statusausgang	Nein	SCx



15. 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 „5. Spezifikationen und Anforderungen“ auf Seite 18)

15.1 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: 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.

2. Überprüfen Sie, ob die Sicherheitsauswertung korrekt installiert ist; siehe „15.3 Überprüfen der Treiberinstallation“ auf Seite 241
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 „15.3 Überprüfen der Treiberinstallation“ auf Seite 241.
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.

1. **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.
2. Die **Sicherheits-** und nicht **sicherheitsrelevanten Eingänge** können an eine beliebige Stelle im linken und mittleren Bereich verschoben werden.
3. Die **Funktions-** und **Logikblöcke** können nur innerhalb des mittleren Bereichs verschoben werden.



15.2 Software: Fehlercodes

Die folgende Tabelle enthält eine Liste der Fehlercodes, die bei dem Versuch einer ungültigen Verbindung zwischen den Blöcken auf der Registerkarte Funktionsansicht ausgegeben werden.

Softwarecode	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 IN-Knoten nur einen Zweihandsteuerungseingang verbinden.
B.3	Dieser Überbrückungsblock ist bereits mit einem anderen Block verbunden.
B.4	Dieser Überbrückungsblock ist mit dem TC-Knoten eines Zweihandsteuerungsblocks verbunden und kann nicht mit anderen Blöcken verbunden werden.
B.5	Der Zweihandsteuerungsblock kann nicht mit dem IN-Knoten von diesem Überbrückungsblock verbunden werden, weil bei ihm die Option „Ausgang schaltet aus, wenn beide Eingänge (IN und BP) ein sind“ aktiviert ist.
B.6	Der IN-Knoten eines Überbrückungsblocks kann nicht mit Eingängen für Not-Halt-Schalter und Seilzugschalter verbunden werden.
B.7	Der IN-Knoten eines Überbrückungsblocks kann nicht über andere Blöcke mit Eingängen für Not-Halt-Schalter und Seilzugschalter verbunden werden.
C.1	Mit dem CD-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 CD-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 EDM-Knoten eines Sicherheitsausgangs verbunden werden.
E1	Die Ausgangsknoten für einen Zustimmungstaster-Block (P oder S) können nur mit dem IN-Knoten eines Sicherheitsausgangs verbunden werden.
E.2	Der IN-Knoten eines Zustimmungstaster-Blocks kann nicht mit Eingängen für Not-Aus-Schalter und Seilzugschalter verbunden werden.
E.3	Der ED-Knoten eines Zustimmungstaster-Blocks kann nur mit dem Eingang für einen Zustimmungstaster verbunden werden.
E.4	Der ED-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 IN-Knoten verbunden ist, kann nicht mit einem Sicherheitsausgang verbunden werden, bei dem als Verzögerung des Sicherheitsausgangs die Einstellung „Aus-Verzögerung“ gewählt ist.
E.6	Der sekundäre Ausgangsknoten S eines Zustimmungstaster-Blocks kann nur mit dem IN-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.



Softwarecode	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 FR-Knoten eines Sicherheitsausgangs verbunden werden.
G.2	Nur ein manueller Reset-Eingang kann mit dem LR-Knoten eines Latch-Reset-Blocks oder eines Sicherheitsausgangs verbunden werden.
G.3	Nur ein manueller Reset-Eingang kann mit dem RST-Knoten eines Zustimmungstaster-Blocks verbunden werden.
G.4	Ein manueller Reset-Eingang kann nur mit dem LR- und dem FR-Knoten eines Sicherheitsausgangs, dem LR-Knoten eines Latch-Reset-Blocks, dem RST-Knoten eines Zustimmungstaster-Blocks und dem SET- und RST-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 Schutzhaltsschalter können, mit dem MP1- und dem MP2-Knoten eines Muting-Blocks oder mit dem MP1-Knoten eines Zweihandsteuerungsblocks verbunden werden.
I.2	Der MP1- und der MP2-Knoten eines Muting-Blocks und der MP1-Knoten eines Zweihandsteuerungsblocks können mit Eingängen verbunden werden, die nur zweikanalige Schaltungen verwenden.
I.3	Der Eingang für Muting-Sensorpaar kann nur mit dem MP1- und dem MP2-Knoten eines Muting-Blocks oder mit dem MP1-Knoten eines Zweihandsteuerungsblocks verbunden werden.
J.1	Ein Zweihandsteuerungsblock kann nur mit einem Zustimmungstaster-Block (IN-Knoten) oder einem Sicherheitsausgang (IN-Knoten) verbunden werden.
J.3	Nur Zweihandsteuerungseingänge oder Überbrückungsblöcke mit daran angeschlossenen Zweihandsteuerungseingängen können mit dem TC-Knoten eines Zweihandsteuerungsblocks verbunden werden.
K.1	Ein Zweihandsteuerungseingang kann nur mit einem Zweihandsteuerungsblock (TC-Knoten) oder einem Überbrückungsblock (IN-Knoten) verbunden werden.
K.2	Ein Sicherheitsausgang, bei dem für die Verzögerung des Sicherheitsausgangs die Einstellung „Aus-Verzögerung“ gewählt ist, kann nicht mit einem Zweihandsteuerungsblock verbunden werden.
K.3	Ein Sicherheitsausgang, bei dem für die Verzögerung des Sicherheitsausgangs 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 IN-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 LR- (Latch-Reset-) Funktion aktiviert ist, kann nicht mit Zweihandsteuerungsblöcken oder Zustimmungstaster-Blöcken verbunden werden.
L.4	Ein Sicherheitsausgangsblock, bei dem für den Anlaufmodus die Einstellung „Manueller Reset“ gewählt ist, kann nicht mit Zweihandsteuerungsblöcken oder Zustimmungstaster-Blöcken verbunden werden.



15.3 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.

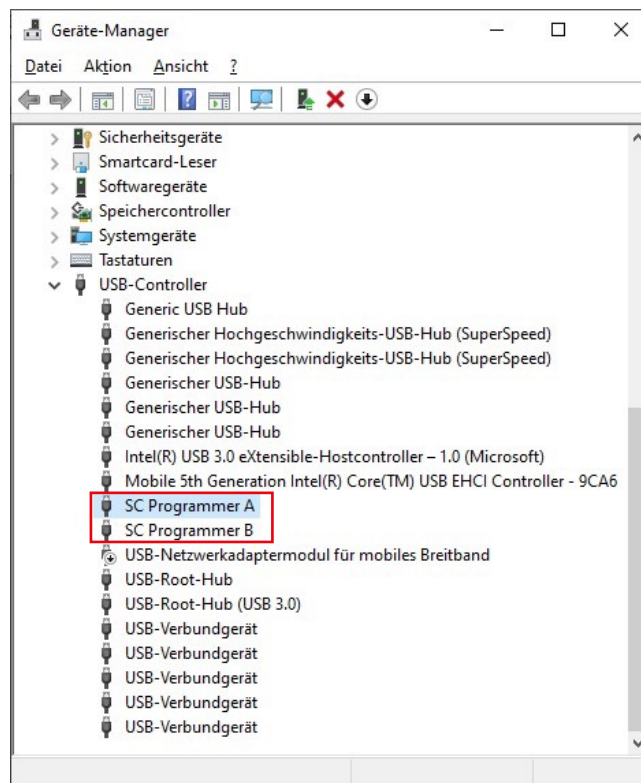


Abbildung 180: SCR P-FPS -Treiber korrekt installiert



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.

15.4 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.



15.5 SCx-Fehlercode-Tabelle

In der folgenden Tabelle sind der Fehlercode der Sicherheitssteuerung, die angezeigte Meldung, etwaige zusätzliche Meldungen sowie die Schritte zur Behebung des Fehlers aufgeführt.

Der Fehlercode und der erweiterte Fehlercode bilden zusammen den Fehlercode der Sicherheitssteuerung. Das Format für den Fehlercode ist Fehlercode, 'Punkt' Erweiterter Fehlercode. So wird z. B. ein Sicherheitssteuerungs- Fehlercode von 2.1 durch einen Fehlercode von 2 und einen erweiterten Fehlercode von 1 dargestellt. Der Fehlermeldungsindexwert ist der Fehlercode und der erweiterte Fehlercode zusammen und enthält ggf. eine führende Null mit dem erweiterten Fehlercode. Zum Beispiel wird ein Sicherheitssteuerungs-Fehlercode von 2.1 durch einen Fehlermeldungsindex von 201 dargestellt. Der Fehlermeldungs-Indexwert ist eine bequeme Methode, um den vollständigen Fehlercode zu erhalten, während nur ein einziges 16-Bit-Register gelesen wird.



Hinweis: Ein Fehlercode von 1,1 unterscheidet sich von einem Fehlercode von 1,10 (die Null ist signifikant).

Störung Code	Angezeigte Nachricht	Zusätzliche Nachricht	Schritte zur Behebung
1.1	Ausgang Störung	Basis-Controller oder Solid-State- Modul Auf kurze Hosen prüfen Relaismodul k.A.	<p>Basis-Controller oder Solid-State-Modul Ein Sicherheitsausgang erscheint EIN, obwohl er AUS sein sollte:</p> <ul style="list-style-type: none"> • Prüfen Sie, ob ein Kurzschluss mit der externen Spannungsquelle vorliegt. • Überprüfen Sie die Größe des gemeinsamen Gleichstromkabels, das an die Lasten des Sicherheitsausgangs angeschlossen ist. Die Leitung muss aus einem dicken Draht bestehen oder so kurz wie möglich sein, um Widerstand und Spannungsabfall zu minimieren. Verwenden Sie ggf. für jedes Ausgangspaar einen separaten DC-Gemeinschaftsleiter und/oder vermeiden Sie die gemeinsame Nutzung dieses DC- Gemeinschaftsrückkanals mit anderen Geräten (siehe Installation des gemeinsamen Leiters auf Seite 67). <p>Relaismodul</p> <ul style="list-style-type: none"> • Relaismodul austauschen
1.2	Ausgang Störung	Basis-Controller oder Solid-State- Modul Auf Kurzschlüsse prüfen Relaismodul n/	<p>Basis-Controller oder Solid-State-Modul Ein Sicherheitsausgang erkennt einen Fehler an einer anderen Spannungsquelle, während der Ausgang eingeschaltet ist:</p> <ul style="list-style-type: none"> • Prüfen Sie auf einen Kurzschluss zwischen den Sicherheitsausgängen • Prüfen Sie, ob ein Kurzschluss mit der externen Spannungsquelle vorliegt. • Kompatibilität der Ladegeräte prüfen • Überprüfen Sie die Größe des gemeinsamen Gleichstromkabels, das an die Lasten des Sicherheitsausgangs angeschlossen ist. Die Leitung muss aus einem dicken Draht bestehen oder so kurz wie möglich sein, um Widerstand und Spannungsabfall zu minimieren. Verwenden Sie ggf. für jedes Ausgangspaar einen separaten DC-Gemeinschaftsleiter und/oder vermeiden Sie die gemeinsame Nutzung dieses DC- Gemeinschaftsrückkanals mit anderen Geräten (siehe Installation des gemeinsamen Leiters auf Seite 67). <p>Relaismodul</p> <ul style="list-style-type: none"> • Relaismodul austauschen
1.3 - 1.8	Interne Störung	-	Interner Fehler - Wenden Sie sich an die BERNSTEIN AG (siehe „17.2 Reparaturen und Garantie“ auf Seite 252).
1.9	Ausgang Störung	Interner Relais-Ausfall	<ul style="list-style-type: none"> • Relaismodul austauschen
1.10	Ausgang Störung	Eingangszeitpunkt prüfen	<p>Sequenz-Timing-Fehler: SCR P-10-6R-4</p> <ul style="list-style-type: none"> • Führen Sie einen System-Reset durch, um den Fehler zu löschen.



Störung Code	Angezeigte Nachricht	Zusätzliche Nachricht	Schritte zur Behebung
2.1	Gleichzeitigkeitsfehler	Zyklus-Eingang	Bei einem Zweikanaleingang oder einem Komplementäreingang, bei dem sich beide Eingänge im Zustand „Run“ befinden, geht ein Eingang in den Zustand „Stop“ und dann zurück in den Zustand „Run“. Bei einem dualen Komplementäreingang, bei dem sich beide Eingangspaare im Zustand „Run“ befanden, ging ein Eingangspaar in den Zustand „Stop“ und dann zurück in den Zustand „Run“. <ul style="list-style-type: none"> • Prüfen Sie die Verkabelung • Prüfen Sie die Eingangssignale • Erwägen Sie die Anpassung der Entprellungszeiten
2.2	Störung der Gleichzeitigkeit	Zyklus-Eingang	Bei einem Zweikanaleingang oder einem Komplementäreingang ging ein Eingang in den Betriebszustand über, aber der andere Eingang folgte der Änderung nicht innerhalb von 3 Sekunden. Bei einem dualen komplementären Eingang ging ein Eingangspaar in den Zustand „Run“ über, aber das andere Eingangspaar folgte dem Wechsel nicht innerhalb von 3 Sekunden. <ul style="list-style-type: none"> • Prüfen Sie die Verkabelung • Prüfen Sie das Timing des Eingangssignals
2,3 oder 2,5	Gleichzeitigkeitsfehler	Zyklus-Eingang	Bei einem dualen Komplementäreingang, bei dem sich beide Eingänge eines Komplementärpaares im Run-Zustand befinden, wechselt ein Eingang dieses Komplementärpaares in den Stop-Zustand und dann zurück in den Run-Zustand: <ul style="list-style-type: none"> • Prüfen Sie die Verkabelung • Prüfen Sie die Eingangssignale • Überprüfen Sie die Stromversorgung, die Eingangssignale liefert • Erwägen Sie die Anpassung der Entprellungszeiten
2.4 oder 2.6	Störung der Gleichzeitigkeit	Zyklus-Eingang	Bei einem dual-komplementären Eingang ging ein Eingang eines komplementären Paares in den Run-Zustand über, aber der andere Eingang desselben komplementären Paares folgte dem Wechsel nicht innerhalb des Zeitlimits: <ul style="list-style-type: none"> • Prüfen Sie die Verkabelung • Prüfen Sie das Timing des Eingangssignals
2.7	Interne Störung		Interner Fehler - Wenden Sie sich an die BERNSTEIN AG (siehe „17.2 Reparaturen und Garantie“ auf Seite 252).
2.8 - 2.9	Eingangsstörung	Terminal xx prüfen	Der Eingang ist hoch: <ul style="list-style-type: none"> • Auf Kurzschlüsse zu anderen Eingängen oder anderen Spannungsquellen prüfen • Prüfen Sie die Kompatibilität der Eingabegeräte • Auf falsch verdrahtete Klemmen prüfen (Ausgangsklemme mit falscher Eingangsklemme verdrahtet)
2.10	Eingangsstörung	Terminal xx prüfen	<ul style="list-style-type: none"> • Prüfen Sie auf einen Kurzschluss zwischen den Eingängen
2.11 - 2.12	Eingangsstörung	Terminal xx prüfen	<ul style="list-style-type: none"> • Auf Kurzschluss zur Erde prüfen
2.13	Eingangsstörung	Terminal xx prüfen	Eingang steckt fest <ul style="list-style-type: none"> • Auf Kurzschluss zur Erde prüfen
2.14	Eingangsstörung	Terminal xx prüfen	Fehlende Prüfimpulse: <ul style="list-style-type: none"> • Prüfen Sie auf einen Kurzschluss zu anderen Eingängen oder anderen Spannungsquellen
2.15	Offene Leitung	Terminal xx prüfen	<ul style="list-style-type: none"> • Prüfen Sie auf eine offene Leitung
2.16 - 2.18	Eingangsstörung	Terminal xx prüfen	Fehlende Prüfimpulse: <ul style="list-style-type: none"> • Prüfen Sie auf einen Kurzschluss zu anderen Eingängen oder anderen Spannungsquellen
2.19	Offene Leitung	Terminal xx prüfen	<ul style="list-style-type: none"> • Prüfen Sie auf eine offene Leitung
2.20	Eingangsstörung	Terminal xx prüfen	Fehlende Prüfimpulse: <ul style="list-style-type: none"> • Auf Kurzschluss zur Erde prüfen
2.21	Offene Leitung	Terminal xx prüfen	<ul style="list-style-type: none"> • Prüfen Sie auf eine offene Leitung
2.22 - 2.23	Eingangsstörung	Terminal xx prüfen	<ul style="list-style-type: none"> • Prüfen Sie auf ein instabiles Signal am Eingang
2.24	Aktivierter Eingang bei Umgehung	System-Reset durchführen	Ein Two-Hand-Control-Eingang wurde aktiviert (eingeschaltet), während er überbrückt war.



Störung Code	Angezeigte Nachricht	Zusätzliche Nachricht	Schritte zur Behebung
2.25	Eingangsstörung	Überwachungs Timer ist abgelaufen, bevor AVM geschlossen wurde	Nachdem der zugehörige Sicherheitsausgang ausgeschaltet wurde, hat sich der AVM-Eingang nicht geschlossen, bevor die AVM-Überwachungszeit abgelaufen ist: <ul style="list-style-type: none"> • Das AVM ist möglicherweise nicht angeschlossen; überprüfen Sie die Verkabelung zum AVM • Entweder ist der AVM nicht angeschlossen, oder seine Reaktion auf das Ausschalten des Sicherheitsausgangs ist zu langsam • Prüfen Sie die Verkabelung zum AVM • Prüfen Sie die Einstellung der Steuerzeiten; erhöhen Sie die Einstellung, falls erforderlich. • Kontakt zu BERNSTEIN AG
2.26	Eingangsstörung	AVM nicht geschlossen, wenn der Ausgang eingeschaltet ist	Der AVM-Eingang war offen, hätte aber geschlossen sein müssen, als der zugehörige Sicherheitsausgang den Befehl EIN erhielt: <ul style="list-style-type: none"> • Das AVM ist möglicherweise nicht angeschlossen; überprüfen Sie die Verkabelung zum AVM
3.1	EDMxx-Fehler	Terminal xx prüfen	Der EDM-Kontakt wurde vor dem Einschalten der Sicherheitsgänge geöffnet: <ul style="list-style-type: none"> • Prüfen Sie, ob ein Schütz oder Relais festsetzt. • Auf einen offenen Draht prüfen
3.2	EDMxx-Fehler	Terminal xx prüfen	EDM-Kontakt(e) haben sich nicht innerhalb von 250 ms nach dem Ausschalten der Sicherheitsgänge geschlossen: <ul style="list-style-type: none"> • Prüfen Sie, ob das Schütz oder das Relais langsam ist oder festsetzt. • Auf einen offenen Draht prüfen
3.4	EDMxx-Fehler	Terminal xx prüfen	EDM-Kontaktpaar ist länger als 250 ms nicht korrekt eingestellt: <ul style="list-style-type: none"> • Prüfen Sie, ob das Schütz oder das Relais langsam ist oder festsetzt. • Auf einen offenen Draht prüfen
3.5	EDMxx-Fehler	Terminal xx prüfen	<ul style="list-style-type: none"> • Prüfen Sie auf ein instabiles Signal am Eingang
3.6	EDMxx-Fehler	Terminal xx prüfen	<ul style="list-style-type: none"> • Auf Kurzschluss zur Erde prüfen
3.7	EDMxx-Fehler	Terminal xx prüfen	<ul style="list-style-type: none"> • Prüfen Sie auf einen Kurzschluss zwischen den Eingängen
3.8	AVMxx-Fehler	System-Reset durchführen	Nachdem dieser Sicherheitsausgang ausgeschaltet wurde, hat sich ein mit diesem Ausgang verbundener AVM-Eingang nicht geschlossen, bevor seine AVM-Überwachungszeit abgelaufen ist: <ul style="list-style-type: none"> • Der AVM ist möglicherweise nicht angeschlossen oder seine Reaktion auf das Ausschalten des Sicherheitsausgangs ist zu langsam • Überprüfen Sie den AVM-Eingang und führen Sie dann einen System-Reset durch, um den Fehler zu löschen.
3.9	Eingangsstörung	AVM nicht geschlossen, wenn der Ausgang eingeschaltet ist	Der AVM-Eingang war offen, hätte aber geschlossen sein müssen, als der zugehörige Sicherheitsausgang den Befehl Ein erhielt: <ul style="list-style-type: none"> • Das AVM ist möglicherweise nicht angeschlossen; überprüfen Sie die Verkabelung zum AVM
3.10	Interne Störung	-	Interner Fehler - Wenden Sie sich an die BERNSTEIN AG (siehe „17.2 Reparaturen und Garantie“ auf Seite 252).
4.x	-	-	Siehe die folgende Tabelle.
5.1 - 5.3	Interne Störung	-	Interner Fehler - Wenden Sie sich an die BERNSTEIN AG (siehe „17.2 Reparaturen und Garantie“ auf Seite 252).
6.xx	Interne Störung	-	Ungültige Konfigurationsdaten. Möglicher interner Fehler: <ul style="list-style-type: none"> • Versuchen Sie, eine neue Konfiguration in die Sicherheitssteuerung zu schreiben
7.1	Fehler in der Pressensteuerung	TOS und BOS prüfen	TOS- und BOS-Eingänge gleichzeitig eingeschaltet <ul style="list-style-type: none"> • Auf Kurzschlüsse an den TOS- und BOS-Eingängen prüfen • Überprüfen Sie die Funktionsfähigkeit der TOS- und BOS-Gerät7.17



Störung Code	Angezeigte Nachricht	Zusätzliche Nachricht	Schritte zur Behebung
7.2	Fehler in der Pressensteuerung	TOS und SQS prüfen	TOS- und SQS-Eingänge gleichzeitig eingeschaltet <ul style="list-style-type: none"> • Auf Kurzschlüsse an den Eingängen TOS und SQS prüfen • Prüfen Sie, ob die TOS- und SQS-Geräte funktionieren.
7.3	Fehler in der Pressensteuerung	TOS und PCMS prüfen	TOS- und PCMS-Eingänge gleichzeitig eingeschaltet <ul style="list-style-type: none"> • Prüfen Sie auf Kurzschlüsse an den Eingängen TOS und PCMS • Prüfen Sie, ob die TOS- und PCMS-Geräte funktionieren.
SCR P-10-6R-4 7.4	Fehler in der Pressensteuerung	SQS und BOS prüfen	Fehler bei der Abfolge von SQS und BOS (BOS wurde vor SQS eingeschaltet) <ul style="list-style-type: none"> • Verdrahtung der SQS- und BOS-Sensoren prüfen • Überprüfung der Platzierung und Funktion der SQS- und BOS-Sensoren
7.5	Fehler in der Pressensteuerung	TOS prüfen	TOS-Timeout-Fehler (Beim automatischen Aufwärtshub wurde das interne Zeitlimit von 30 Sekunden überschritten) <ul style="list-style-type: none"> • Überprüfen Sie die Verkabelung des TOS-Systems • Überprüfung der Platzierung und der Funktion des TOS-Sensors
7.6	Fehler in der Pressensteuerung	BOS prüfen	BOS-Timeout-Fehler (Beim automatischen Abwärtshub wurde das interne Zeitlimit von 30 Sekunden überschritten) <ul style="list-style-type: none"> • Überprüfen Sie die Verkabelung des BOS-Systems • Prüfen Sie, ob der BOS-Sensor richtig platziert ist und funktioniert.
7.7	Fehler in der Pressensteuerung	Eingänge zur Auswahl des Prüfmodus	Moduswahlfehler (mehr als ein Moduswahleingang gleichzeitig eingeschaltet) <ul style="list-style-type: none"> • Überprüfen Sie die Verdrahtung der Eingänge für den Betriebszustand • Prüfen Sie den Betriebswahlschalter auf Fehler
7.8	Fehler in der Pressensteuerung	-	Indexfehler (interner Konfigurationsfehler) Wenden Sie sich an die BERNSTEIN AG (siehe „17.2 Reparaturen und Garantie“ auf Seite 252).
7.9	Fehler in der Pressensteuerung	Fußschaltereingang prüfen	Fußschalter Fehler (bei Konfiguration mit einer SQS wurde der Eingangsknoten Ft Switch anstelle des Eingangsknotens GO eingeschaltet) <ul style="list-style-type: none"> • Sequenzierungsfehler • Wenn das Problem weiterhin besteht, überprüfen Sie die Verkabelung der THC- und Fußschaltereingänge.
7.10	Fehler in der Pressensteuerung	Zylinder prüfen	Abwärts-AVM-Fehler (Abwärts-AVM befindet sich in einem falschen Zustand im Vergleich zum erwarteten Zustand) <ul style="list-style-type: none"> • AVM-Verkabelung prüfen • AVM-Sensor und Down Stroke-System überprüfen
7.11	Fehler in der Pressensteuerung	Prüfen von Zylindern	Aufwärts-AVM-Fehler (Aufwärts-AVM befindet sich in einem falschen Zustand im Vergleich zum erwarteten Zustand) <ul style="list-style-type: none"> • Überprüfung der AVM-Verkabelung • Überprüfen Sie den AVM-Sensor und das Up Stroke-System
7.12	Fehler in der Pressensteuerung	Hoher Zylinder prüfen	Hoher AVM-Fehler (Hoher AVM ist in einem falschen Zustand im Vergleich zum erwarteten Zustand) <ul style="list-style-type: none"> • Hohe AVM-Verkabelung prüfen • Hoch-AVM-Sensor und Hochhubsystem prüfen
7.13	Fehler in der Pressensteuerung	Niedrigen Zylinder prüfen	Low AVM Error (Low AVM ist im Vergleich zum erwarteten Zustand im falschen Zustand) <ul style="list-style-type: none"> • Niedrige AVM-Verkabelung prüfen • Low AVM-Sensor und Low Stroke-System prüfen
7.14	Fehler in der Pressensteuerung	Von SQS zu PCMS Gleichzeitigkeit	Gleichzeitigkeitsfehler zwischen SQS und PCMS (3-Sekunden-Grenze zwischen den Eingängen überschritten) <ul style="list-style-type: none"> • Überprüfung der Verkabelung von SQS und PCMS • Prüfen Sie die Platzierung von SQS und PCMS unter Berücksichtigung der Ladegeschwindigkeit
7.15	Fehler in der Pressensteuerung	SQS-Status prüfen	SQS-Statusfehler (SQS-Statusniveau nicht wie erwartet während des Pressenzyklus) <ul style="list-style-type: none"> • Verdrahtung des SQS-Eingangs prüfen • Überprüfen Sie die Platzierung des SQS-Sensors und seine Funktionalität
7.16	Fehler in der Pressensteuerung	PCMS-Status prüfen	PCMS-Statusfehler (PCMS-Statusniveau nicht wie erwartet während des Pressenzyklus) <ul style="list-style-type: none"> • Verdrahtung des PCMS-Eingangs prüfen • Überprüfen Sie die Platzierung des PCMS-Sensors und seine Funktionalität



Störung Code	Angezeigte Nachricht	Zusätzliche Nachricht	Schritte zur Behebung
7.17	Fehler in der Pressensteuerung	TOS-Status prüfen	TOS-Statusfehler (TOS-Statusniveau nicht wie erwartet während des Pressenzyklus) <ul style="list-style-type: none"> • Verdrahtung des TOS-Eingangs prüfen • Überprüfen Sie die Platzierung des TOS-Sensors und seine Funktionalität
7.18	Fehler in der Pressensteuerung	BOS-Status prüfen	BOS-Statusfehler (BOS-Statusniveau nicht wie erwartet während des Pressenzyklus) <ul style="list-style-type: none"> • Verdrahtung des BOS-Eingangs prüfen • Überprüfen Sie die Platzierung des BOS-Sensors und seine Funktionalität
10.xx	Interne Störung	-	Interner Fehler - Wenden Sie sich an die BERNSTEIN AG (siehe „17.2 Reparaturen und Garantie“ auf Seite 252).

Prüfen Sie bei Fehlercodes 4.x das Fehlerprotokoll auf zusätzliche Fehler, um das spezifische Modul zu ermitteln, in dem der ursprüngliche Fehler aufgetreten ist.

Störung Code	Angezeigte Nachricht	Zusätzliche Nachricht	Schritte zur Behebung
4.1	Versorgungsspannung niedrig	Prüfen Sie die Stromzufuhr	Die Versorgungsspannung ist für länger als 6 ms unter die Nennspannung gefallen: <ul style="list-style-type: none"> • Überprüfen Sie die Spannung und Stromstärke des Netzteils • Prüfen Sie, ob eine Überlast an den Ausgängen vorliegt, die dazu führen könnte, dass das Netzteil den Strom begrenzt.
4.2	Interne Störung		Ein Konfigurationsparameter ist beschädigt worden. Um die Konfiguration zu reparieren: <ul style="list-style-type: none"> • Ersetzen Sie die Konfiguration mit Hilfe einer Sicherungskopie der Konfiguration • Erstellen Sie die Konfiguration mit Hilfe der Software neu und schreiben Sie sie in die Sicherheitssteuerung.
4.3 - 4.11	Interne Störung	-	Interner Fehler: Wenden Sie sich an die BERNSTEIN AG (siehe „17.2 Reparaturen und Garantie“ auf Seite 252).
4.12	Konfiguration Zeitüberschreitung	Konfiguration prüfen	Die Sicherheitssteuerung wurde länger als eine Stunde im Konfigurationsmodus belassen, ohne dass eine Taste gedrückt wurde. <ul style="list-style-type: none"> • Schalten Sie den Strom ein • Durchführen eines System-Resets
4.13	Konfiguration Zeitüberschreitung	Bestätigen Sie die Konfiguration	Die Sicherheitssteuerung wurde länger als eine Stunde im Konfigurationsmodus belassen, ohne Befehle von der Software zu erhalten. <ul style="list-style-type: none"> • Schalten Sie den Strom ein • Durchführen eines System-Resets
4.14	Konfiguration Unbestätigt	Bestätigen Sie die Konfiguration	Die Konfiguration wurde nach der Bearbeitung nicht bestätigt: <ul style="list-style-type: none"> • Bestätigen Sie die Konfiguration über die Software
4.15 - 4.19	Interne Störung	-	Interner Fehler: Wenden Sie sich an die BERNSTEIN AG (siehe „17.2 Reparaturen und Garantie“ auf Seite 252).
4.20	Nicht zugewiesenes Terminal in Verwendung	Terminal xx prüfen	Diese Klemme ist in der vorliegenden Konfiguration keinem Gerät zugeordnet und sollte nicht aktiv sein: <ul style="list-style-type: none"> • Prüfen Sie die Verkabelung
4.21 - 4.34	Interne Störung	-	Interner Fehler: Wenden Sie sich an die BERNSTEIN AG (siehe „17.2 Reparaturen und Garantie“ auf Seite 252).
4.35	Übertemperatur	-	Ein interner Übertemperaturzustand ist aufgetreten. Überprüfen Sie, ob die Umgebungs- und Ausgangsbelastungsbedingungen den Spezifikationen der Sicherheitssteuerung entsprechen.
4.36 - 4.39	Interne Störung	-	Interner Fehler: Wenden Sie sich an die BERNSTEIN AG (siehe „17.2 Reparaturen und Garantie“ auf Seite 252).
4.40 - 4.41	Fehler in der Modulkommunikation	Modulleistung prüfen	Ein Ausgangserweiterungsmodul hat den Kontakt zur Basissteuerung verloren.
4.42	Modulfehlanpassung	-	Das erkannte Modul bzw. die erkannten Module stimmen nicht mit der Konfiguration der Sicherheitssteuerung überein.



Störung Code	Angezeigte Nachricht	Zusätzliche Nachricht	Schritte zur Behebung
4.43	Fehler in der Modulkommunikation	Modulleistung prüfen	Ein Erweiterungsmodul hat den Kontakt mit dem Base Controller verloren.
4.44 - 4.45	Interne Störung	-	Interner Fehler: Wenden Sie sich an die BERNSTEIN AG (siehe „17.2 Reparaturen und Garantie“ auf Seite 252).
4.46 - 4.47	Interne Störung	-	Interner Fehler: Wenden Sie sich an die BERNSTEIN AG (siehe „17.2 Reparaturen und Garantie“ auf Seite 252).
4.48	Unbenutzter Ausgang	Ausgangsverdrahtung prüfen	An einer unbestätigten Klemme wurde eine Spannung festgestellt.
4.49 - 4.55	Interne Störung	-	Interner Fehler - Wenden Sie sich an die BERNSTEIN AG (siehe „17.2 Reparaturen und Garantie“ auf Seite 252).
4.56	Display Comm Failure	-	Display (Onboard Interface) Kommunikationsfehler: <ul style="list-style-type: none"> • Schalten Sie die Stromzufuhr zur Sicherheitssteuerung aus. Wenn der Fehlercode weiterhin besteht, wenden Sie sich an die BERNSTEIN AG (siehe „17.2 Reparaturen und Garantie“ auf Seite 252).
4.57 - 4.59	Interne Störung	-	Interner Fehler: Wenden Sie sich an die BERNSTEIN AG (siehe „17.2 Reparaturen und Garantie“ auf Seite 252).
4.60	Ausgang Störung	Auf kurze Hosen prüfen	Eine Ausgangsklemme hat einen Kurzschluss festgestellt. Prüfen Sie den Ausgangsfehler für Details.
4.61	Unstimmigkeiten in der Konfiguration	-	Ein in der geladenen Konfiguration enthaltenes Merkmal (z. B. DCD-Eingänge, virtuelle Eingänge, Erweiterungsmodule) wird von diesem Steuerungsmodell nicht unterstützt. Die Konfiguration ist nun bestätigt und kann als bestätigte Konfiguration gespeichert und/oder auf einen SCR P-FPS geschrieben werden. Die Konfiguration wird auf diesem Modell nicht ausgeführt. <ul style="list-style-type: none"> • Entfernen Sie die von diesem Modell nicht unterstützten Funktionen. • Laden Sie die Konfiguration auf ein Modell, das die ausgewählten Funktionen unterstützt.



15.6 SCR P-Fehlercode-Tabelle

In der folgenden Tabelle sind der Fehlercode der Sicherheitssteuerung, die angezeigte Meldung, etwaige zusätzliche Meldungen sowie die Schritte zur Behebung des Fehlers aufgeführt.

Der Fehlercode und der erweiterte Fehlercode bilden zusammen den Fehlercode der Sicherheitssteuerung. Das Format für den Fehlercode ist Fehlercode, 'Punkt' Erweiterter Fehlercode. So wird z. B. ein Sicherheitssteuerungs-Fehlercode von 2.1 durch einen Fehlercode von 2 und einen erweiterten Fehlercode von 1 dargestellt. Der Fehlermeldungsindexwert ist der Fehlercode und der erweiterte Fehlercode zusammen und enthält ggf. eine führende Null mit dem erweiterten Fehlercode. Zum Beispiel wird ein Sicherheitssteuerungs-Fehlercode von 2.1 durch einen Fehlermeldungsindexwert von 201 dargestellt. Der Fehlermeldungs-Indexwert ist eine bequeme Möglichkeit, den vollständigen Fehlercode zu erhalten, während nur ein einziges 16-Bit-Register gelesen wird.



Hinweis: Ein Fehlercode von 1,1 unterscheidet sich von einem Fehlercode von 1,10 (die Null ist signifikant).

Fehlercode	Fehlerbeschreibung	Lösungsschritte
1.1 – 1.2	Ausgangsfehler	Sicherheitsauswertung austauschen
1.3 – 1.8	Interner Fehler	Interner Fehler: BERNSTEIN AG kontaktieren (siehe „17.2 Reparaturen und Garantie“ auf Seite 252)
1.9	Ausgangsfehler	Sicherheitsauswertung austauschen
1.10	Ausgangsfehler	Fehler beim Sequenz-Zeitverhalten: <ul style="list-style-type: none"> Zur Löschung des Fehlers einen System-Reset durchführen
2.1	Gleichzeitigkeitsfehler	An einem zweikanaligen Eingang oder einem antivalenten Eingang mit beiden Eingängen im Ein-Zustand ging ein Eingang in den Aus-Zustand und wieder zurück in den Ein-Zustand. 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"> Verdrahtung überprüfen Eingangssignale überprüfen Gegebenenfalls die Entprellzeiten anpassen Eingang schalten
2.2	Gleichzeitigkeitsfehler	An einem zweifach-antivalenten Eingang mit beiden Eingängen eines antivalenten Paares im Ein-Zustand ging ein Eingang dieses antivalenten Paares in den Aus-Zustand und wieder zurück in den Ein-Zustand. <ul style="list-style-type: none"> Verdrahtung überprüfen Eingangssignale überprüfen Überprüfen, ob die Stromversorgung Eingangssignale liefert Gegebenenfalls die Entprellzeiten anpassen Eingang schalten
2.4 oder 2.6	Gleichzeitigkeitsfehler	An einem zweifach-antivalenten Eingang ging ein Eingang von einem antivalenten Paar in den Ein-Zustand, aber der andere Eingang desselben antivalenten Paares folgte nicht innerhalb des Zeitlimits. <ul style="list-style-type: none"> Verdrahtung überprüfen Zeitverhalten der Eingangssignale kontrollieren Eingang schalten
2.7	Interner Fehler	Interner Fehler: BERNSTEIN AG kontaktieren (siehe „17.2 Reparaturen und Garantie“ auf Seite 252)
2.8 – 2.9	Eingangsfehler	Eingang im Ein-Zustand blockiert: <ul style="list-style-type: none"> Überprüfen, ob Kurzschlüsse zu anderen Eingängen oder zu einer anderen Spannungsquelle vorliegen Kompatibilität des Eingangsgeräts überprüfen



Fehlercode	Fehlerbeschreibung	Lösungsschritte
2.10	Eingangsfehler	<ul style="list-style-type: none"> Überprüfen, ob zwischen den Eingängen ein Kurzschluss vorliegt
2.11 – 2.12	Eingangsfehler	<ul style="list-style-type: none"> Überprüfen, ob Erdschluss vorliegt
2.13	Eingangsfehler	<p>Eingang im Aus-Zustand blockiert</p> <ul style="list-style-type: none"> Überprüfen, ob Erdschluss vorliegt
2.14	Eingangsfehler	<p>Fehlende Testimpulse:</p> <ul style="list-style-type: none"> Überprüfen, ob ein Kurzschluss zu anderen Eingängen oder zu einer anderen Spannungsquelle vorliegt
2.15	Leitungsunterbrechung	<ul style="list-style-type: none"> Überprüfen, ob eine Leitungsunterbrechung vorliegt
2.16 – 2.18	Eingangsfehler	<p>Fehlende Testimpulse:</p> <ul style="list-style-type: none"> Überprüfen, ob ein Kurzschluss zu anderen Eingängen oder zu einer anderen Spannungsquelle vorliegt
2.19	Leitungsunterbrechung	<ul style="list-style-type: none"> Überprüfen, ob eine Leitungsunterbrechung vorliegt
2.20	Eingangsfehler	<p>Fehlende Testimpulse:</p> <ul style="list-style-type: none"> Überprüfen, ob Erdschluss vorliegt
2.21	Leitungsunterbrechung	<ul style="list-style-type: none"> Überprüfen, ob eine Leitungsunterbrechung vorliegt
2.22 – 2.23	Eingangsfehler	<ul style="list-style-type: none"> Überprüfen, ob am Eingang ein instabiles Signal vorliegt
2.24	Eingang während Überbrückung aktiviert	Eine Zweihandsteuerung wurde aktiviert (eingeschaltet), während sie überbrückt wurde
2.25	Eingangsfehler	<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"> Die AVM ist möglicherweise getrennt. Verdrahtung zur AVM prüfen. Entweder die AVM ist getrennt, oder sie reagiert zu langsam auf das Ausschalten des Sicherheitsausgangs. Kabelanschlüsse zur AVM überprüfen Zeitgebereinstellung überprüfen und bei Bedarf erhöhen BERNSTEIN AG kontaktieren
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"> Die AVM ist möglicherweise getrennt. Verdrahtung zur AVM prüfen.
3.1	EDMxx-Fehler	<p>EDM-Kontakt wurde geöffnet, bevor sich die Sicherheitsausgänge einschalteten:</p> <ul style="list-style-type: none"> Überprüfen, ob Kontaktgeber oder Relais im Ein-Zustand verschweißt sind Auf Leitungsunterbrechungen überprüfen
3.2	EDMxx-Fehler	<p>EDM-Kontakte wurden nach dem Abschalten der Sicherheitsausgänge nicht innerhalb von 250 ms geschlossen:</p> <ul style="list-style-type: none"> Überprüfen, ob Kontaktgeber oder Relais zu langsam abfallen oder im Ein-Zustand verschweißt sind. Auf Leitungsunterbrechungen überprüfen
3.3	EDMxx-Fehler	<p>EDM-Kontakte wurden vor dem Einschalten der Sicherheitsausgänge geöffnet:</p> <ul style="list-style-type: none"> Überprüfen, ob Kontaktgeber oder Relais im Ein-Zustand verschweißt sind Auf Leitungsunterbrechungen überprüfen
3.4	EDMxx-Fehler	<p>Kontakte der beiden Rückführkreise (EDM-Kontaktpaar) länger als 250 ms in unterschiedlichem Zustand.</p> <ul style="list-style-type: none"> Überprüfen, ob Kontaktgeber oder Relais zu langsam abfallen oder im Ein-Zustand verschweißt sind. Auf Leitungsunterbrechungen überprüfen
3.5	EDMxx-Fehler	<ul style="list-style-type: none"> Überprüfen, ob am Eingang ein instabiles Signal vorliegt
3.6	EDMxx-Fehler	<ul style="list-style-type: none"> Überprüfen, ob Erdschluss vorliegt
3.7	EDMxx-Fehler	<ul style="list-style-type: none"> Überprüfen, ob zwischen den Eingängen ein Kurzschluss vorliegt
3.8	AVMxx-Fehler	<p>Nachdem sich der zugehörige Sicherheitsausgang ausgeschaltet hat, wurde ein mit diesem Ausgang verbundener AVM-Eingang nicht vor Ablauf seiner AVM-Überwachungszeit geschlossen:</p> <ul style="list-style-type: none"> Entweder die AVM ist getrennt, oder sie reagiert zu langsam auf das Ausschalten des Sicherheitsausgangs. Den AVM-Eingang überprüfen und dann zur Löschung des Fehlers einen System-Reset ausführen



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"> Die AVM ist möglicherweise getrennt. Verdrahtung zur AVM prüfen.
3.10	Interner Fehler	Interner Fehler: BERNSTEIN AG kontaktieren (siehe „17.2 Reparaturen und Garantie“ auf Seite 252)
4.1	Betriebsspannung zu niedrig	Betriebsspannung länger als 6 ms unter der Mindestversorgungsspannung: <ul style="list-style-type: none"> Betriebsspannungs- und Stromwerte der Versorgungsspannungsquelle überprüfen Überprüfen, ob an den Ausgängen Überlast vorliegt, die die Stromversorgung veranlassen könnte, den Strom zu begrenzen
4.2	Interner Fehler	Ein Konfigurationsparameter wurde beschädigt. Zur Behebung des Zustands: <ul style="list-style-type: none"> Die Konfiguration unter Verwendung einer Sicherungskopie von der Konfiguration ersetzen Die Konfiguration über die Software erneut erstellen und in die Sicherheitsauswertung schreiben
4.3–4.12	Interner Fehler	Interner Fehler: BERNSTEIN AG kontaktieren (siehe „17.2 Reparaturen und Garantie“ auf Seite 252).
4.13	Konfigurations-Zeitabschaltung	Die Sicherheitsauswertung blieb länger als eine Stunde ohne Empfang von Befehlen von der Software im Konfigurationsmodus.
4.14	Interner Fehler	Konfiguration wurde nach der Bearbeitung nicht bestätigt: <ul style="list-style-type: none"> Konfiguration über die Software bestätigen
4.15–4.19	Konfigurations-Zeitabschaltung	Interner Fehler: BERNSTEIN AG kontaktieren (siehe „17.2 Reparaturen und Garantie“ auf Seite 252).
4.20	Konfiguration unbestätigt	Dieser Anschluss ist keinem Gerät in der vorliegenden Konfiguration zugeordnet und sollte nicht aktiv sein: <ul style="list-style-type: none"> Verdrahtung überprüfen
4.21–4.34	Interner Fehler	Interner Fehler: BERNSTEIN AG kontaktieren (siehe „17.2 Reparaturen und Garantie“ auf Seite 252).
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 „17.2 Reparaturen und Garantie“ auf Seite 252).
4.48	Nicht verwendeter Ausgang	An einer unbekanntenen Klemme wurde Spannung festgestellt.
4.49–4.59	Interner Fehler	Interner Fehler: BERNSTEIN AG kontaktieren (siehe „17.2 Reparaturen und Garantie“ auf Seite 252).
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 „17.2 Reparaturen und Garantie“ auf Seite 252).
6.xx	Interner Fehler	Ungültige Konfigurationsdaten. Möglicher interner Fehler: <ul style="list-style-type: none"> Neue Konfiguration in die Sicherheitsauswertung zu schreiben versuchen
10.xx	Interner Fehler	Interner Fehler: BERNSTEIN AG kontaktieren (siehe „17.2 Reparaturen und Garantie“ auf Seite 252).

16. Komponenten und Zubehörteile

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



17. Kundendienst und Wartung

17.1 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.

17.2 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 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.

17.3 Kontakt

Sitz der Zentrale der BERNSTEIN AG:
Hans-Bernstein-Str. 1, 32457 Porta Westfalica, Deutschland
Website: www.bernstein.eu
Telefon: + 49 571/793-0

Weltweite Standorte und lokale Vertretungen finden Sie unter www.bernstein.eu

UK CA Representative:
BERNSTEIN Ltd.
Mr. Paul Sharp
Tintagel Way, Westgate, Aldridge, WS9 AER
+441922 744999
p.sharp@bernstein-ltd.co.uk

17.4 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 so-wie 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.

Die deutsche Sprachfassung ist die Originalbetriebs- und Montageanleitung. Bei anderen Sprachen handelt es sich um die Übersetzung der Originalbetriebs- und Montageanleitung.



18. 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.

18.1 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

18.2 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 (Kaltanstaucher 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)	



18.3 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)



19. 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 Maschinenabschalt einrichtung 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. Ist diese Bedingung nicht erfüllt, so befindet sich der Eingang in einem Fehlerzustand.

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 wiedereinschalten dürfen. Sind beide Bedingungen nicht erfüllt, so befindet sich der Eingang in einem

H**Hindertretungsgefahr**

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**

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

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. Sicherheits- Lichtvorhängen oder Absperrtoren, kann es von Vorteil sein, die Einrichtung beim Anlauf mindestens ein Mal auf den einwandfreien Funktionsbetrieb zu testen.



**DETECT****We make
safety happen.****PROTECT****We keep safe
your visions.**

Kontakt

**International Headquarters
BERNSTEIN AG**
Hans-Bernstein-Str. 1
32457 Porta Westfalica
Tel. +49 571 793-0
info@bernstein.eu
www.bernstein.eu

**China
BERNSTEIN Safe Solutions
(Taicang) Co., Ltd.**
Tel. +86 512 81608180
info@bernstein.asia
www.bernstein.asia

**Dänemark
BERNSTEIN A/S**
Tel. +45 7020 0522
info.denmark@bernstein.eu
www.bernstein.dk

**Italien
BERNSTEIN S.r.l.**
Tel. +39 035 4549037
sales@bernstein.it
www.bernstein.it

**Frankreich
BERNSTEIN S.A.R.L.**
Tel. +33 1 64 66 32 50
info.france@bernstein.eu
www.bernstein.fr

**Österreich
BERNSTEIN GmbH**
Tel. +43 2256 62070-0
office@bernstein.at
www.bernstein.at

**Großbritannien
BERNSTEIN Ltd**
Tel. +44 1922 744999
sales@bernstein-ltd.co.uk
www.bernstein-ltd.co.uk

**Schweiz
BERNSTEIN (Schweiz) AG**
Tel. +41 44 775 71-71
info.schweiz@bernstein.eu
www.bernstein-schweiz.ch

www.bernstein.eu