halstrup walcher

Sicherheitshandbuch

PSx3xx mit STO Teilsicherheitsfunktion

halstrup-walcher GmbH
Stegener Straße 10
D-79199 Kirchzarten

Tel. +49 (0) 76 61/39 63-0
info@halstrup-walcher.de
www.halstrup-walcher.de

Versionsübersicht

Version	Datum	Autor	Inhalt
A	27.06.19	La	Entwurf für Musterlieferung
B	28.01.21	La	Initiale Version/Draft
C	11.02.21	PI	Ergänzung nach Review
D	08.04.21	PI	Korrekturen und Ergänzungen
		LA	Kapitel [1.3] „Transport, Montage, Anschluss und Inbetriebnahme“ hinzugefügt
E	26.04.21	Kö	Überarbeitung: Layout und Struktur

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Allgemeines

1.1 Zweck des Dokuments

In diesem Dokument sind die sicherheitstechnischen Grundlagen und erwarteten Kennzahlen bei der Verwendung der Positioniersysteme PSx3xx mit STO (Safe Torque Off) Teilsicherheitsfunktion beschrieben.

Dieses Sicherheitshandbuch ist ein Zusatz zur jeweiligen Betriebsanleitung:

Bus-Kommunikation	Betriebsanleitung	Dokumenten-Nummer
Ethernet IP	PSx3xxEIP-STO	7100.006334
PROFINET	PSx3xxPNET-STO	7100.006234
EtherCAT	PSx3xxECAT-STO	7100.006694

Tabelle 1: Mitgeltende Betriebsanleitungen

1.2 Abkürzungen und Begriffsdefinitionen

Im Dokument werden Abkürzungen und Begriffsdefinitionen verwendet, die nachfolgend erläutert werden.

1.2.1 Abkürzungen

Finden Sie hier die Beschreibung zu den verwendeten Abkürzungen in folgender Tabelle:

Abkürzung	Beschreibung
a, b, c, d, e	Bezeichnung für die Performance Level
DC	Diagnostic Coverage = Diagnose Deckungsgrad
DC_{avg}	Diagnostic Coverage Average = Durchschnittlicher Diagnose Deckungsgrad
EMV	Elektro-Magnetische Verträglichkeit
FIT	Failure in time = Ausfallrate
HFT	Hardware Fehler Toleranz
MTTFd	Mean Time To Failure = Mittlere Zeit bis zum gefahrenbringenden Ausfall
PFH	Probability of Failure per Hour = Ausfallwahrscheinlichkeit pro Betriebsstunde
PELV	Protective Extra Low Voltage = Funktionskleinspannung mit elektrisch sicherer Trennung
PSE, PSS, PSW	Positioniersystem-Familien der halstrup-walcher GmbH
PL	Performance Level, siehe auch [1] unter 1.2.3 Angewandte Normen

Abkürzung	Beschreibung
SELV	Safety Extra Low Voltage = Sicherheitskleinspannung
SIL	Sicherheits-Integritätslevel
SFF	Safe Failure Fraction = Anteil sicherer Ausfälle
STO	Safe Torque Off = eine Teilsicherheitsfunktion, bei der ein Antrieb kein aktives Drehmoment erzeugt und frei austrudelt
OSSD	Output Signal Switching Device = eine Fehlererkennungs-maßnahme, bei der die Quelle auf das Signal zusätzliche Testimpulse schaltet, um Fehler in der Verdrahtung zu erkennen

Tabelle 2: Beschreibung der Abkürzungen

1.2.2 Begriffsdefinitionen

Hier finden Sie Begriffsdefinitionen für spezifische, häufig verwendete Begriffe.

Begriff	Definition
austrudeln	Am Positioniersystem wird kein Drehmoment und kein Bremsmoment mehr erzeugt. Der Antrieb läuft momentfrei aus. Die Zeit bis zum vollständigen Auslaufen des Antriebs ist anwendungsabhängig und wird daher nicht angegeben. Dies wird als der sichere Zustand angenommen.
Positioniersysteme	Antriebe der halstrup-walcher GmbH für Positionieraufgaben in Maschinen.
Fahrauftrag	Befehl von der Maschinensteuerung an das Positioniersystem, eine gewisse Anzahl von Umdrehungen / Schritten zu fahren.
Selbsthemmung	Ein durch Reibung verursachter Widerstand gegen ein Verdrehen.
Fehlerreaktionszeit	Zeit vom Auftreten eines Fehlers bis zur Rückkehr in den sicheren Zustand.
Reaktionszeit	Zeit vom Aktivieren der Sicherheitsfunktion bis der sichere Zustand erreicht wird (es wird aktiv kein Drehmoment mehr erzeugt).

Tabelle 3: Begriffsdefinitionen

1.2.3 Angewandte Normen

Hier finden Sie eine Beschreibung und Dokumentidentifikation der angewandten Normen.

Ref.	Dokumentidentifikation	Beschreibung
	DIN EN ISO 13849	Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen
[1]	DIN EN ISO 13849-**1**:2016-06	Teil 1: Allgemeine Gestaltungsleitsätze
[2]	DIN EN ISO 13849-**2**:2013-02	Teil 2: Validierung
	DIN EN 61800-5	Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl. Anforderungen an die Sicherheit
[3]	DIN EN 61800-5-**1**:2017-11	Einschaltdauer, Definition siehe IEC 60034-1 bzw. VDE 0530-1
[4]	DIN EN 61800-5-**2**:2017-11	Teil 5-2: Funktionale Sicherheit
	DIN EN IEC 61800-3	Drehzahlveränderbare elektrische Antriebssysteme
[5]	DIN EN IEC 61800-3:2019-04	EMV-Anforderungen einschließlich spezieller Prüfverfahren für Antriebssysteme und Maschinen mit darin enthaltenen Antriebssystemen
	DIN EN 61508	Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/ programmierbarer elektronischer Systeme
[6]	DIN EN 61508-**1**:2011-02	Teil 1: Allgemeine Anforderungen
[7]	DIN EN 61508-**2**:2011-02	Teil 2: Anforderungen an sicherheitsbezogene elektrischer/elektronischer/programmierbarer elektronischer Systeme
[8]	DIN EN 61508-**3**:2011-02	Teil 3: Anforderungen an Software
[9]	DIN EN 61508-**4**:2011-02	Teil 4: Begriffe und Abkürzungen
[10]	DIN EN 61508-**5**:2011-02	Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (Safety Integrity Level)
[11]	DIN EN 61508-**6**:2011-02	Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3
[12]	DIN EN 61508-**7**:2011-02	Teil 7: Überblick über Verfahren und Maßnahmen

Ref.	Dokumentidentifikation	Beschreibung
	DIN EN 62061:2016	Sicherheit von Maschinen
[13]	DIN EN 62061:2016-**05**	Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme
[14]	**ZVEI Positionspapier CB24I**	Klassifizierung binärer 24V-Schnittstellen mit Testung im Bereich der Funktionalen Sicherheit

Tabelle 4: Beschreibung und Dokumentidentifikation der angewandten Normen

1.2.4 Bedeutung von Symbolen und Signalwörtern

Hier werden die verwendeten Symbole und Signalwörter erläutert.

GEFAHR

Bedeutung:	Unmittelbar drohende Gefahr
Folgen bei Missachtung:	Tod oder schwere Verletzungen

WARNUNG

Bedeutung:	Mögliche gefährliche Situation
Folgen bei Missachtung:	Tod oder schwere Verletzungen

VORSICHT

Bedeutung:	Mögliche gefährliche Situation
Folgen bei Missachtung:	Leichte Verletzungen

HINWEIS

Bedeutung:	Hinweise / Einschränkungen
Folgen bei Missachtung:	Fehlfunktion, unerwartetes Verhalten, mögliche Beschädigungen an Positioniersystem oder Maschine

INFO

Bedeutung:	Infos und Hinweis zur weiterführenden Doku
Folgen bei Missachtung:	Funktionen werden u.U. nicht vollständig genutzt oder Fehlanwendungen möglich

1.3 Transport , Montage, Anschluss und Inbetriebnahme

GEFAHR

Die Montage und der elektrische Anschluss des Geräts dürfen nur von Fachpersonal durchgeführt werden. Es muss dazu eingewiesen und vom Anlagenbetreiber beauftragt sein. Nur eingewiesene vom Anlagenbetreiber beauftragte Personen dürfen das Gerät bedienen

1.4 Haftungsansprüche

Das Positioniersystem PSx3xx stellt eine Teilsicherheitsfunktion für STO zur Verfügung. Für die Erfüllung der Sicherheitsfunktion sind weitere Komponenten und die Einhaltung der hier genannten Voraussetzungen erforderlich. Die Beurteilung und Bewertung der gesamten Sicherheitsfunktion liegt in der Verantwortung des Anwenders des Positioniersystems. Als Lieferant eines Teilsystems lehnt halstrup-walcher daher weitergehende Haftungsansprüche ab.

2 Beschreibung der Teilsicherheitsfunktion

WARNUNG

Für die Bewertung nach SIL1 und PL c sind nur Einzelfehler relevant. In der Ansteuerung des Motors kann es durch die Brückenschaltung jedoch in seltenen Fehlerfällen zu einem gleichzeitigen Kurzschluss von zwei der Ausgangshalbleiter kommen. Hierdurch ergibt sich das Restrisiko einer plötzlichen kurzzeitigen und ruckartigen Bewegung, auch wenn sich der Antrieb im sicheren Zustand befindet.

HINWEIS

Die Sicherheitsfunktion STO (Safe Torque Off) entspricht einer Not-Halt Funktion. Bei Aktivierung von STO erzeugt das Positioniersystem aktiv kein Drehmoment mehr und trudelt frei aus. Die Höhe des Haltemoments durch die inhärente Selbsthemmung hängt von der jeweiligen Ausführung ab. Von dieser Selbsthemmung und der Belastung hängt die Zeit ab, die der Antrieb zum Austrudeln braucht.

WARNUNG

Die STO Teilsicherheitsfunktion ist völlig in Hardware realisiert. Die Firmware des Positioniersystems erfüllt keine Sicherheitsfunktion! Funktionen der Firmware, z. B. Status-Bits oder Messwerte, dienen lediglich der zusätzlichen Information, Indikation und Überwachung. Sie dürfen jedoch nicht für Sicherheitsfunktionen verwendet werden!

INFO

Es gibt keine Selbsthaltung für das STO-Signal von Seiten des Positioniersystems, eine eventuelle Wideranlaufsperre nach aktivem STO muss in der Steuerung implementiert werden.

WARNUNG

Für die Aktivierung des STO-Teilsicherheitssystem besitzt das Positioniersystem einen eigenen Eingang, der durch eine Sicherheits-Steuerung oder ein Sicherheits-Relais angesteuert werden muss. Die Sicherheitsfunktion ist nur gewährleistet, wenn auch die anderen Komponenten in der Kette entsprechend sicherheitstechnisch bewertet wurden.

WARNUNG

Die Bewertung der Sicherheitskette muss auch die Verkabelung umfassen. Das Positioniersystem bietet optional die Auswertung von Testimpulsen (OSSD) in Fällen, in denen kein Fehlerausschluss für die Verkabelung in Anspruch genommen werden kann. In allen anderen Fällen muss der Anwender für eine sichere Verdrahtung sorgen.

Fehlerausschlüsse bezüglich Kurzschlüssen zwischen zwei beliebigen Leitern können nach DIN EN ISO 13849-2 [2] (siehe auch 1.2.3 Angewandte Normen) in Anspruch genommen werden

- bei dauerhafter fester und geschützter Verlegung, z. B. in Kabelkanal oder Panzerrohr,
- innerhalb eines elektrischen Einbauraums,
- bei einzelnem Schutz durch eine Erdverbindung, z. B. durch Verwendung von Leitungen mit einzeln geschirmten Adern.

Für weitere Informationen siehe Kapitel 3 Verdrahtung des Positioniersystems.

2.1 Definition der Pegel des STO-Signals

Die Pegel des STO Signals sind folgendermaßen definiert:

STO low	< 5 V	STO ist ausgelöst, Antrieb trudelt aus
STO high	> 15 V	STO ist nicht ausgelöst, Antrieb ist freigegeben
STO Signal	≥ 5 V und ≤ 15 V	undefiniert

Im Normalbetrieb liegt das STO-Signal auf der Betriebsspannung des Positioniersystems von nominal + 24 V. Um STO auszulösen wird es auf 0V (Masse, GND) gelegt.

Während STO aktiv ist, nimmt das Positioniersystem keine Fahrbefehle an. Achten Sie daher bei einer Wiederinbetriebnahme darauf, dass zuerst das STO-Signal zurückgenommen wird und erst anschließend Fahrbefehle von der Steuerung an das Positioniersystem übermittelt werden.

2.2 STO-Diagnosefunktion

Das Positioniersystem besitzt eine Diagnosefunktion für die STO-Funktion. Wenn STO ausgelöst wurde und der Motor weiterhin mit Strom versorgt wird, liegt ein Fehler vor. Dieser Fehler wird erkannt und das Positioniersystem über einen zweiten Abschaltweg abgeschaltet.

Dieser Zustand wird auch am Bus durch Bit 9 im Statuswort signalisiert. Eine detailliertere Beschreibung des Statusworts befindet sich in der jeweiligen Betriebsanleitung (siehe Tabelle 1: Mitgeltende Betriebsanleitungen).

Dieser Fehler ist ein Zeichen für einen möglichen Defekt der Hardware. Die Abschaltung lässt sich nur aufheben, indem das Positioniersystem kurzzeitig vollständig von der Versorgungsspannung getrennt wird, z. B. durch Lösen des Steckers der Versorgungsspannung.

VORSICHT

Nehmen Sie das Positioniersystem umgehend außer Betrieb und senden Sie es zur Überprüfung und/oder Reparatur ein und/oder ersetzen es durch ein gleichartiges Positioniersystem.

Achten Sie beim Austausch von Komponenten in der Sicherheitskette darauf, dass Sie diese nur gegen solche mit gleichen Eigenschaften und Kenndaten austauschen. Andernfalls müssen Sie eine Bewertung der gesamten Sicherheitskette erneut vornehmen. Nach dem Austausch von Komponenten ist die Inbetriebnahmeprüfung (siehe 2.4) zu wiederholen und zu dokumentieren.

2.3 Spannungsversorgung der STO-Funktion

WARNUNG

Zur Versorgung des Positioniersystems muss ein SELV / PELV Netzteil verwendet werden, welches garantiert, dass die maximale Spannung von 60 V auch im Fehlerfall nicht überschritten wird.

Bei Spannungen über 60 V können Beschädigungen auftreten, die auch zum Verlust der Sicherheitsfunktion führen könnten.

VORSICHT

Die verwendeten Stecker und Verbindungsleitungen sind häufig nur für Spannungen bis 30 V zugelassen. Damit überhöhte Spannungen nicht zur Beeinträchtigung der STO Teilsicherheits- oder Diagnosefunktion führen, wird die Versorgungsspannung intern überwacht. Bei einer dauerhaften Versorgungsspannung von > 31,4 V (± 0,5 V) wird das Positioniersystem intern von der Anschlüssen der Versorgungsspannung getrennt.

HINWEIS

Dieser Zustand kann nur wieder verlassen werden, indem die äußere Versorgungsspannung kurzzeitig unterbrochen wird, z. B. durch Abschaltung im Schaltschrank oder Lösen des Steckers der Versorgungsspannung!

Kurze Störungen, z. B. EMV-Störungen, werden gefiltert und führen nicht zu einer Abschaltung.

Achten Sie darauf, dass die Versorgungsspannung unterhalb der Abschaltgrenze bleibt! Versorgungsspannung getrennt

2.4 Inbetriebnahmeprüfung

Bei der Inbetriebnahme eines Positioniersystems mit STO Teilsicherheitsfunktion muss eine Inbetriebnahmeprüfung wie folgt durchgeführt und dokumentiert werden. Hierbei ist darauf zu achten, dass dies im sicheren Zustand der Maschine / Anlage stattfindet und Gefährdungen, z. B. durch manuelles Verfahren eines einzelnen Antriebs, unbedingt vermieden werden. Gehen Sie wie folgt vor:

WARNUNG

1. Das Positioniersystem gemäß der Herstellerdokumentation und den einschlägigen örtlichen Vorschriften anschließen.
2. Die softwaremäßige Einrichtung abschließen und mit der Ausführung eines Fahrbefehls testen. Dabei darauf achten, dass hierdurch keine Beschädigungen verursacht werden können.
3. Während der Ausführung eines Fahrbefehls STO auslösen. → Kontrollieren, dass das Positioniersystem austrudelt.
4. Alternativ, falls das Ausführen von Fahrbefehlen nicht möglich ist, kann STO ausgelöst werden und dann ein Fahrbefehl abgesetzt werden. → Kontrollieren, dass das Positioniersystem den Fahrbefehl nicht ausführt.

Nach Austausch von Komponenten ist diese Inbetriebnahme Prüfung erneut durchzuführen und zu dokumentieren.

3 Verdrahtung des Positioniersystems

Die Sicherheitsfunktion ist nur gewährleistet, wenn alle Komponenten in der Abschaltkette entsprechende Bedingungen erfüllen. Dies umfasst auch die Verdrahtung des Positioniersystems.

Bei der Verwendung von konventionellen Leitungen können Fehlerausschlüsse für Kurzschluss zwischen zwei beliebigen Leitern unter gewissen Umständen in Anspruch genommen werden:

- Feste Verlegung und Schutz gegen äußere Beschädigungen
- STO-Signal wird in einer separaten Mantelleitung geführt
- Die Leitungen befinden sich innerhalb eines elektrischen Einbauraums gemäß IEC 60204-1.
- Bei einzelnem Schutz durch eine Erdverbindung (in der Regel einzeln geschirmte Adern, wobei der Schirm mit Erde verbunden ist).

In allen Fällen, in denen ein solcher Fehlerausschluss nicht in Anspruch genommen werden kann, können Sie das Positioniersystem mit Auswertung von Testimpulsen auf der STO-Signalleitung bestellen. Die Auswertung der Testimpulse bietet eine zusätzliche Diagnosemöglichkeit für die Verdrahtung. Die Ansteuerung durch eine Sicherheits-SPS oder ein Sicherheitsrelais muss diese Möglichkeit ebenfalls unterstützen (OSSD).

Bei Verwendung des Hybridsteckers (Bus, Versorgung und STO in einen Stecker und damit auch in einer Leitung) sind in der Regel zwingend Testimpulse auf der STO-Signalleitung zu verwenden, weil handelsübliche Hybridleitungen die Bedingungen für einen Fehlerausschluss in der Regel nicht erfüllen.

4 Zeitverhalten der STO-Teilsicherheitsfunktion

In den folgenden Abbildungen werden die grundlegenden Anforderungen an das Zeitverhalten des STO-Signals erläutert. Dabei ist das STO-Eingangssignal stets schwarz dargestellt, das interne Abschaltsignal rot.

4.1 Normalbetrieb ohne Testimpulse

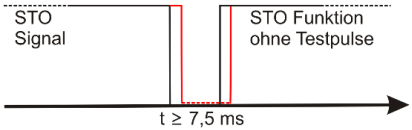


Bild 1: Normalbetrieb ohne Testimpulse

Bild 1 zeigt den Normalbetrieb ohne Testimpulse für die Verkabelung. Um STO auszulösen, muss der STO Eingang für mindestens 7,5 ms auf Low gezogen werden. Dies ist die minimale Zeit unter Berücksichtigung der ungünstigsten Bedingungen. Die Zeit setzt sich zusammen aus der Zeit für die zuverlässige Erkennung des STO-Eingangssignals und der Zeit für die Durchführung der Diagnose.

Die eigentliche Abschaltung des Motors erfolgt dabei schon unmittelbar nach der Erkennung des STO-Eingangssignals nach maximal 3,5 ms, während in der restlichen Zeit die Diagnosefunktion ihre Auswertung vornimmt. Die Erkennung des STO Eingangssignals dauert auch beim Deaktivieren maximal 3,5 ms, der Antrieb ist erst nach dieser Verzögerung für neue Fahrbefehle bereit!

4.2 Fehlersituation ohne Testimpulse

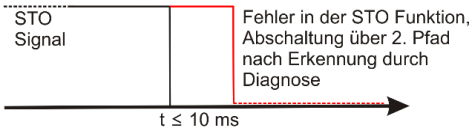


Bild 2: Fehlersituation: Testimpulse für die Verkabelung fehlen

Bild 2 zeigt eine Fehlersituation, wieder ohne Testimpulse für die Verkabelung, bei der aufgrund eines Defekts in der Hardware der Motorstrom nicht unterbrochen wird. Die Diagnosefunktion erkennt diesen Zustand und schaltet den Motor über einen zweiten Abschaltpfad ab. Die Abschaltung erfolgt unmittelbar nach Durchführung der Diagnose, eine Reaktionszeit von ≤ 10 ms wird unter allen Bedingungen eingehalten. Da ein Hardware-Defekt angenommen werden muss, kann der Zustand nur verlassen werden, wenn die äußere Versorgungsspannung kurzzeitig unterbrochen wird! Es wird deshalb dringend empfohlen, das Positioniersystem gegen ein gleichartiges auszutauschen.

4.3 Normalbetrieb mit Testimpulsen

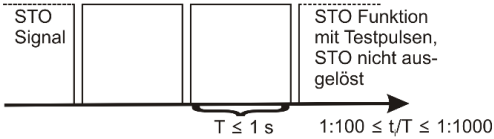


Bild 3: Normalbetrieb mit Testimpulsen

Bild 3 zeigt den Normalbetrieb mit Testimpulsen (OSSD) für die Verkabelung.

- Die Testimpulse müssen eine Dauer von t_i mindestens 100 µs haben und dürfen maximal 1 ms lang sein.
- Die Intervallzeit T zwischen zwei aufeinanderfolgenden Testimpulsen darf nicht mehr als 1 s betragen.

Von Bedeutung ist auch das Verhältnis der Zeiten t_i/T. Dieses Verhältnis sollte bevorzugt im Bereich 1:100 bis 1:1000 liegen. Für die Unterstützung gängiger Steuerungen wird eine Überschreitung dieses Verhältnisses von + 25 % toleriert. Unterstützt werden die Klassen C1 bis C3 nach ZVEI Positionspapier [14] (siehe 1.2.3 Angewandte Normen).

HINWEIS

Im Gegensatz zu der Beschreibung im Positionspapier wertet das Positioniersystem die Testimpulse aus. Andernfalls kann die Quelle (Steuerung) zwar Fehler in der Verdrahtung ebenfalls erkennen, eine sichere Abschaltung ist bei einer einkanaligen Ausführung aber dann nicht mehr gewährleistet!

Für solche Verdrahtungsfehler, die die Quelle (Steuerung) erkennt, ist daher ggf. ein zweiter Abschaltpfad in der Steuerung, z. B. durch Ausschalten der Versorgungsspannung für das Positioniersystem, vorzusehen.

4.4 Fehlersituation mit Testimpulsen

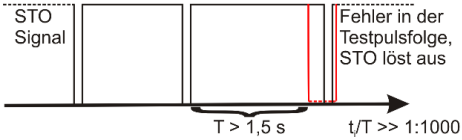


Bild 4: Fehlersituation mit Testimpulsen

Bild 4 zeigt den Fehlerfall in der Folge der Testimpulse für die Verkabelung.

Wenn die Intervallzeit ***T*** von einem zum nächsten Testimpuls den Wert von 1,5 s (1,25 s ± 20 %) übersteigt, wird STO ausgelöst und der Motor abgeschaltet.

Die Abschaltung erfolgt auch, wenn das Verhältnis der Zeiten ***ti/T*** den Wert von 1:1000 extrem überschreitet. Die Angabe einer exakten Grenze ist nicht möglich, da diese auch von der absoluten Dauer ***ti*** der Testimpulse abhängt.

4.5 Nutzung einer Wiedereinschaltsperre

Das Positioniersystem besitzt nur Selbsthaltungen für definitiv erkannte Fehler wie oben beschrieben. In allen Fällen, in denen kein eindeutiger Fehler erkannt wird, kann das Positioniersystem unmittelbar nach Verlassen des aktiven STO-Zustands wieder in Betrieb gehen!

Wenn dies nicht gewünscht ist, muss eine Wiedereinschaltsperre in der Steuerung vorgesehen werden. Dies betrifft auch die Fälle, in denen Testimpulse für die Verkabelung (OSSD) verwendet werden und fehlerhafte Testpulsfolgen erkannt werden. Vergleichbar dem Verhalten, wenn das STO-Signal aktiviert / deaktiviert wird, bleibt das Positioniersystem im sicheren Zustand, solange eine ungültige Testpulsfolge erkannt wird und nimmt bei einer gültigen Testpulsfolge den Normalbetrieb wieder auf, falls keine solche Wiedereinschaltsperre implementiert wird.

Daher wird dringend empfohlen, die Statusinformationen regelmäßig in der Steuerung auszuwerten, um solche ggf. kurzzeitigen Zustände zu erfassen und entsprechende Maßnahmen einzuleiten. Die Testimpulse dienen der Überwachung der externen Verkabelung. Bei Fehlern in der Testimpulsfolge ist es unwahrscheinlich, dass die Sicherheitsfunktion davon betroffen ist und die Sicherheitsfunktion steht weiter zur Verfügung.

5 Sicherheitstechnische Kennzahlen

5.1 Sicherheitsfunktion

Sicherheitsfunktion: sicherer Zustand und unterstützte Sicherheitsfunktionen
Ungesteuertes Stillsetzen nach DIN EN 60204-1
Stopp-Kategorie 0 nach DIN EN 60204-1
Sicher abgeschaltetes Drehmoment nach Kap.4.2.3.2 in DIN EN 61800-5-2
Reaktionszeit < 10 ms[1]
Fehlerreaktionszeit < 5 ms[1]

Tabelle 5: Sicherheitsfunktion

5.2 Sicherheits-Integritätslevel (SIL) (DIN EN 61508, DIN EN 62061, DIN EN 61800-5-2)

Sicherheitskennzahlen: Sicherheitsfunktion		
λ_S	440 FIT	Fehlerrate – sicher
λD	244 FIT	Fehlerrate – gefährlich
λDD	147 FIT	Fehlerrate – gefährlich, entdeckt
λDU	97 FIT	Fehlerrate – gefährlich, unentdeckt

Tabelle 6: SIL Sicherheitskennzahlen: Sicherheitsfunktion

Sicherheitskennzahlen: Diagnose/Testkanal		
λ_S	551 FIT	Fehlerrate – sicher
λD	576 FIT	Fehlerrate – gefährlich
λDD	5 FIT	Fehlerrate – gefährlich, entdeckt
λDU	571 FIT	Fehlerrate – gefährlich, unentdeckt

Tabelle 7: Sicherheitskennzahlen: Diagnose/Testkanal

[1] Werte für Anwendungen ohne Testpulse (OSSD) auf dem STO Signal, sonst abhängig vom Timing der Testpulse.

Gerätetyp	Typ A	Diskreter Aufbau der Sicherheitsfunktion
Betriebsrat	High Demand	Anforderung > 1/Jahr
HFT	0	Hardwarefehlertoleranz
SFF	85,5 %	Anteil der ungefährlichen Ausfälle
SIL	SIL 1	Erreichbarer Safety Integrity Level
Einsatzdauer	20 Jahre	Dauer, für die die Kennzahlen bei bestimmungsgemäßen Gebrauch gelten
PFH	$9{,}7*10^{-8}$ 1/h	Wahrscheinlichkeit einer Fehlfunktion je Stunde

Tabelle 8: Gerätebeschreibung

5.3 Performance Level (PL) (DIN EN ISO 13849-1)

MTTFd	100 Jahre – hoch	Mittlere Zeit bis zu einem gefahrbringendem Ausfall
DC_{avg}	60,2 % – niedrig	Mittlerer Diagnosedeckungsgrad
PL	c	Erreichbarer Performance Level
Kategorie	2	Eiskanalige Abschaltung, Testeinrichtung mit Ausgang (Diagnose mit 2.Abschaltpfad), Test der Sicherheitsfunktion bei jedem Ansprechen

Tabelle 9: Performance Level (PL)

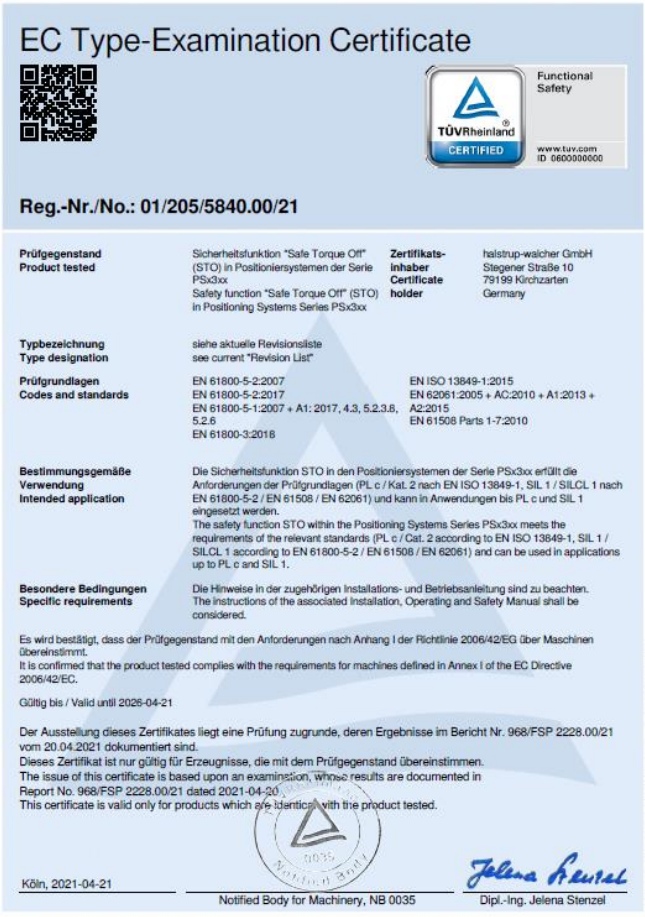
5.4 Testimpulse (OSSD)

Parameter	**Min.**	**Typ.**	**Max.**
Klasse	Interface Typ C, Klasse 1, 2 und 3		
Testimpulsdauer t_i	100 µs	500 µs	1000 µs
Testimpulsintervall T	10 ms	300 ms	1000 ms
Eingangswiderstand R	3000 Ω	3300 Ω	3600 Ω
Eingangskapazität C_L	8nF	10nF	15nF
Induktivität L_L	bei Frequenzen unterhalb 1 MHz vernachlässigbar		

Tabelle 10: Testimpulse (OSSD)

6 Anhang

6.1 Zertifikat Baumusterprüfung



EC Type-Examination Certificate

Functional Safety

TÜVRheinland CERTIFIED

www.tuv.com
ID 0600000000

Reg.-Nr./No.: 01/205/5840.00/21

Prüfgegenstand **Product tested**	Sicherheitsfunktion "Safe Torque Off" (STO) in Positioniersystemen der Serie PSx3xx Safety function "Safe Torque Off" (STO) in Positioning Systems Series PSx3xx	**Zertifikats-inhaber** **Certificate holder**	halstrup-walcher GmbH Stegener Straße 10 79199 Kirchzarten Germany
Typbezeichnung **Type designation**	siehe aktuelle Revisionsliste see current "Revision List"		
Prüfgrundlagen **Codes and standards**	EN 61800-5-2:2007 EN 61800-5-2:2017 EN 61800-5-1:2007 + A1: 2017, 4.3, 5.2.3.8, 5.2.6 EN 61800-3:2018		EN ISO 13849-1:2015 EN 62061:2005 + AC:2010 + A1:2013 + A2:2015 EN 61508 Parts 1-7:2010
Bestimmungsgemäße Verwendung **Intended application**	Die Sicherheitsfunktion STO in den Positioniersystemen der Serie PSx3xx erfüllt die Anforderungen der Prüfgrundlagen (PL c / Kat. 2 nach EN ISO 13849-1, SIL 1 / SILCL 1 nach EN 61800-5-2 / EN 61508 / EN 62061) und kann in Anwendungen bis PL c und SIL 1 eingesetzt werden. The safety function STO within the Positioning Systems Series PSx3xx meets the requirements of the relevant standards (PL c / Cat. 2 according to EN ISO 13849-1, SIL 1 / SILCL 1 according to EN 61800-5-2 / EN 61508 / EN 62061) and can be used in applications up to PL c and SIL 1.		
Besondere Bedingungen **Specific requirements**	Die Hinweise in der zugehörigen Installations- und Betriebsanleitung sind zu beachten. The instructions of the associated Installation, Operating and Safety Manual shall be considered.		

Es wird bestätigt, dass der Prüfgegenstand mit den Anforderungen nach Anhang I der Richtlinie 2006/42/EG über Maschinen übereinstimmt.
It is confirmed that the product tested complies with the requirements for machines defined in Annex I of the EC Directive 2006/42/EC.

Gültig bis / Valid until 2026-04-21

Der Ausstellung dieses Zertifikates liegt eine Prüfung zugrunde, deren Ergebnisse im Bericht Nr. 968/FSP 2228.00/21 vom 20.04.2021 dokumentiert sind.
Dieses Zertifikat ist nur gültig für Erzeugnisse, die mit dem Prüfgegenstand übereinstimmen.
The issue of this certificate is based upon an examination, whose results are documented in Report No. 968/FSP 2228.00/21 dated 2021-04-20.
This certificate is valid only for products which are identical with the product tested.

Köln, 2021-04-21

Notified Body for Machinery, NB 0035

Dipl.-Ing. Jelena Stenzel

TÜV Rheinland Industrie Service GmbH, Am Grauen Stein, 51105 Köln / Germany
Tel. +49 221 806-2454, Fax: +49 221 806-1354, E-Mail: industrie-service@de.tuv.com

10/22 12 12 E A4 © TÜV, TUEV and TUV are registered trademarks. Utilisation and application requires prior approval.

www.fs-products.com
www.tuv.com

TÜVRheinland®
Precisely Right.