Product Release Brief

Sicherheitsmodul SE6 – Erweiterte Sicherheitstechnik für SD6

Frei, Markus

23.11.2018

Safe Motion Monitoring

STÖBER

Inhaltsverzeichnis

1. Vorwort 5
2. Dokumentenhistorie 6
   2.1. Autoren 6
   2.2. Änderungen 6
   2.3. Anmerkungen zur Dokumentenversion V 0.x 6
   2.4. Anmerkungen zur Dokumentenversion ab V 1.x 6
3. Projektüberblick 7
   3.1. ePEP-Projekt 7
   3.2. ePEP-Projektteam 7
   3.3. Entwicklungsziel 7
   3.4. Projekthistorie 8
   3.5. Einsatzgebiet 8
   3.6. Montage 8
   3.7. Firmware-Update 9
   3.8. Konfiguration/ Parametrierung 9
   3.9. Dokumentation 9
   3.10. Validierung und Verifikation 10
   3.11. Baumusterprüfung 10
   3.12. Vertriebsstart 10
4. Sicherheitsfunktionen 11
   4.1. Normative Sicherheitsfunktionen nach DIN EN 60204-1 11
   4.2. Normative Sicherheitsfunktionen nach DIN EN 61800-5-2 12
      4.2.1. Sichere Stopp-Funktionen 12
      4.2.2. Sichere Bewegungsfunktionen 12
      4.2.3. Sichere Bremsfunktionen 13

4.3. Normative Sicherheitsfunktionen nach DIN EN 14118 13
4.4. Nicht normativ beschriebene Sicherheitsfunktionen 14
5. Prinzipielle Funktionsweise 15
5.1. Verfügbaren Sicherheitsfunktionen 15
5.1.1. Sicher Stillsetzen 15
5.1.2. Sicher Begrenzen 15
5.1.3. Sicher Melden 15
5.1.4. Sicheres Bremsenmanagement 16
5.2. Reaktion auf Grenzwertverletzung 16
5.3. Sicherheitsfunktionen kurz erklärt 16
5.3.1. Sicherer Stopp 1 (Safe Stop 1; SS1) 16
5.3.2. Sicherer Stopp 2 (Safe Stop 2; SS2) 18
5.3.3. Sicher begrenzte Geschwindigkeit (Safely-Limited Speed, SLS) 19
5.3.4. Sicher begrenzter Geschwindigkeitsbereich (Safe Speed Range; SSR) 20
5.3.5. Sicher begrenzte Richtung (Safe Direction; SDI) 21
5.3.6. Sicherer Betriebshalt (Safe Operating Stop; SOS) 22
5.3.7. Sicher begrenztes Schrittmaß (Safely Limited Increment; SLI) 23
5.3.8. Sicher begrenzte Position (Safely Limited Position, SLP) 24
5.3.9. Sicheres Bremsenmanagement 25
6. Besonderheiten 26
6.1. Encoder-unabhängig 26
6.2. Betrieb von Synchron-Servomotoren 27
6.3. Betrieb von Asynchronmotoren 27
6.4. Absichern von schwerkraftbelasteten Achsen 27
6.4.1. Marktsituation 28
6.5. Herstellerneutrale Schnittstelle 28
6.6. Vermeiden von Fehlauslösungen 29
6.7. Multiinstanz-Fähigkeit 29

6.8. Reaktion auf Grenzwertverletzungen 30
6.8.1. Sicheres Melden 30
6.8.2. Sicheres Abschalten 30
6.9. Sicherheitsniveau 32
6.10. Worst-Case-Reaktionszeit 33
6.11. Service-Konzept 33
6.11.1. Motor 33
6.11.2. Antriebsregler 34
7. Marktvergleich 35
7.1. Antriebslösungen basierend „Failsafe-Encodern“ 35
7.2. Antriebslösungen basierend auf konventionellen Sin/Cos-Encodern 36
7.3. Antriebsregler-unabhängige Systeme 36
7.4. SE6-Produktvorteile gegenüber Antrieben mit Fail-Safe-Encodern 37
7.5. SE6-Produktvorteile gegenüber klassischen Sin/Cos-Lösungen 38
8. FAQ 39
8.1. Fragen zur Hardware 39
8.2. Fragen zur Software 39
8.3. Fragen zum Handling 39

1. Vorwort

Die 6. Antriebsreglergeneration von STÖBER umfasst unterschiedliche Gerätebaureihen mit unterschiedlichen Sicherheitsfunktionalitäten.

Dieser Product-Release-Brief beschreibt das optionale Sicherheitsmodul SE6 für die Antriebsreglerbaureihe SD6 und deren Funktionalität zum Marktstart.

Das Sicherheitsmodul SE6 ist zum Zeitpunkt des Marktstarts nicht kompatibel mit den Antriebsreglerbaureihen SI6 und SC6. Zum Zeitpunkt des Marktstarts von SE6 gibt es aufgrund der stark unterschiedlichen Gerätekonstruktionen keine Anstrengungen seitens des Produktmanagements und der Entwicklung, dies zu ändern.

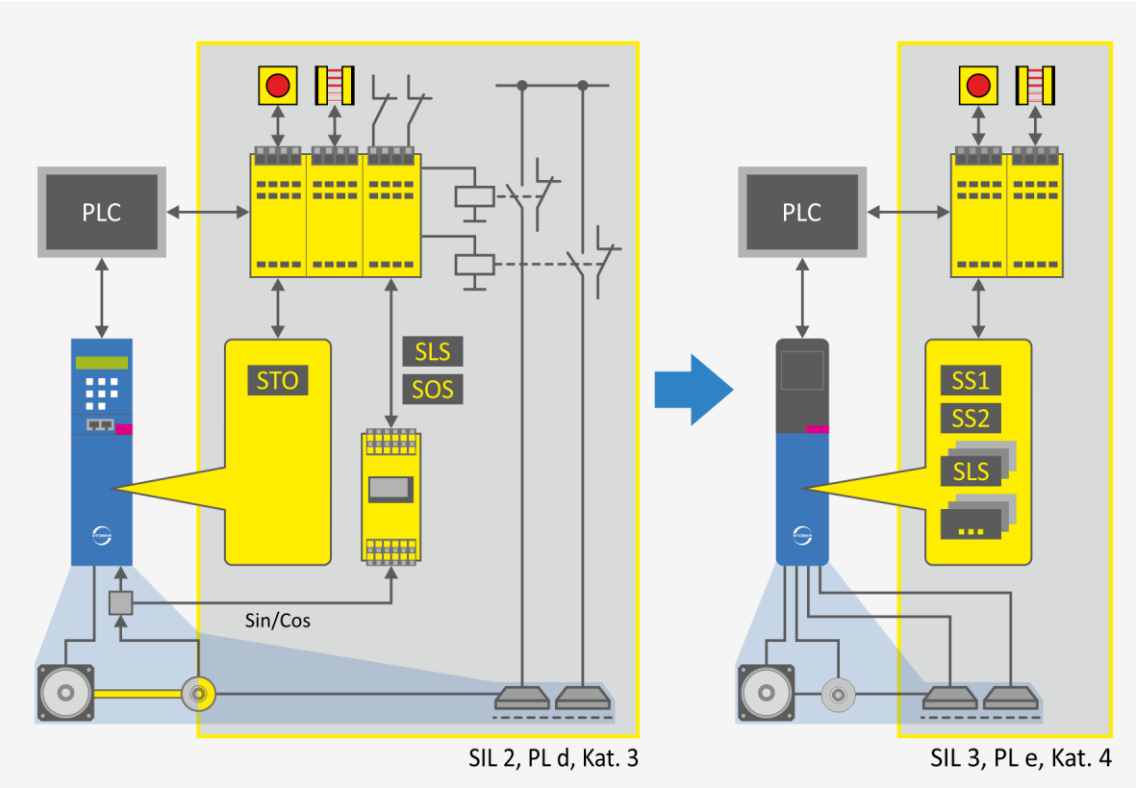

Abbildung 1- SE6 Grundkonzept

2. Dokumentenhistorie

2.1. Autoren

Abteilung	Name (Abkürzung)	E-Mail-Kontakt
SPE	Markus Frei (mf)	markus.frei@stoeber.de

2.2. Änderungen

Die in diesem Dokument gemachten Angaben wurden nach bestem Wissen und Gewissen recherchiert, zusammengestellt und dokumentiert.

Es kann jedoch nicht ausgeschlossen werden, dass sich der Fehlerteufel auch in diesem Dokument bemerkbar macht. Über Rückmeldungen zu hilfreichen oder notwendigen Ergänzungen oder Fehlern würden wir uns freuen. Hierzu senden sie bitte eine formlose E-Mail an einen der in Kapitel 2.1 benannten Autoren.

2.3. Anmerkungen zur Dokumentenversion V 0.x

Entwurfsversion, Änderungen im Dokument werden nicht dokumentiert

2.4. Anmerkungen zur Dokumentenversion ab V 1.x

Inhaltliche Änderungen und Ergänzungen im Dokument werden in diesem Kapitel dokumentiert. Nicht dokumentiert werden orthographische Verbesserungen und Korrekturen.

Datum	Name	Bemerkung

3. Projektüberblick

3.1. ePEP-Projekt

Das Sicherheitsmodul SE6 in der Version A wurde im Zuge des ePEP-Projekts „E1214 Sicherheitstechnik SD6 V2“ entwickelt.

3.2. ePEP-Projektteam

Entsprechend den Grundlagen des ePEP-Prozesses setzt sich das Projektteam aus den folgenden Rollen und Mitgliedern zusammen:

ePEP Projekt Rolle	Projektmitglied	eMail Kontakt
Marktverantwortlicher (MV)	Udo Cyrol (CY)	udo.cyrol@stoeber.de
Produktverantwortlicher (PV)	Markus Frei (mf)	markus.frei@stoeber.de
Entwicklungsverantwortlicher (EV)	Stephan Dilger (dlg)	stephan.dilger@stoeber.de
Projektmanager (PM)	Siehe PV	Siehe PV

Tabelle 1- Projektteam

Für eventuelle Rückfragen zum Produkt bzw. zum Projekt stehen die Projektmitglieder entsprechend Ihrer Rolle im ePEP-Prozess gerne zur Verfügung.

3.3. Entwicklungsziel

Erweiterte Sicherheitsfunktionalität für den Antriebsregler SD6 mit dem Schwerpunkt auf Synchron-Servomotoren.

Hinweis:
Asynchronmotoren wurden bei der Entwicklung nicht explizit berücksichtigt. Dennoch können Asynchronmotoren mittels eines zweiten Encoders sicher überwacht werden.

3.4. Projekthistorie

Zeitraum	Aktion
4Q 2012	Projektstart
…	Marktanalyse und Produktdefinition
2Q 2015	Entwicklungsstart
2Q 2017	Start Feldtestphase
3Q 2017	TÜV Vorab-Zertifikat
1Q 2018	Entwicklungsende
2Q2018	Aufbau SE6 Lagerbestand (200 Stk.)
2Q 2018	Offizielles Zertifikat; SE6 wird auf Kundennachfrage angeboten und verkauft
01.11.2018	Offizielle Marktfreigabe bei SAT
SPS IPC Drives 2018	Offizielle Produktpräsentation

Tabelle 2-Projekthistorie

3.5. Einsatzgebiet

Das Sicherheitsmodul SE6 steht als optionales Zubehör für den Antriebsregler SD6 von Baugröße 0 (SD6A0x) bis Baugröße 3 (SD6A3x) zur Verfügung. Die Einsatzumgebung entspricht der des SD6-Grundgeräts.

Das Sicherheitsmodul ersetzt das in der Standardausführung im Antriebsregler SD6 integrierte Sicherheitsmodul ST6 mit der Sicherheitsfunktion STO (Safe Torque Off).

Hinweis:
Das Sicherheitsmodul SE6 kann nicht mit den anderen Antriebsreglerbaureihen von STÖBER (SI6, SC6, …) genutzt werden.

3.6. Montage

Das Sicherheitsmodul wird während der Geräte-Endfertigung bei STÖBER in den Antriebsregler eingebaut und beim Warenausgangstest auf Funktionsfähigkeit geprüft. Neben der Prüfung auf korrekte Integration wird hier auch zur lückenlosen Nachvollziehbarkeit des Verbleibs u. a. die Seriennummer von SE6 mit der des SD6-Grundgeräts verknüpft.

Ein nachträglicher Einbau des Sicherheitsmoduls SE6 im Feld ist aus organisatorischen Gründen nicht möglich! Weder durch einen Kunden noch durch einen STÖBER Mitarbeiter.

3.7. Firmware-Update

Ein Firmware-Update des Sicherheitsmoduls SE6 im Feld ist nicht möglich. An einer Lösung für ein Firmware-Update bei STÖBER und/oder PILZ wird im Zuge der Projektpflege gearbeitet. Ein Zieltermin kann zum jetzigen Zeitpunkt noch nicht benannt werden.

Ein Firmware- oder Applikations-Update des SD6-Grundgeräts ist unabhängig vom Sicherheitsmodul jederzeit möglich.

3.8. Konfiguration/ Parametrierung

Die Konfiguration/Parametrierung des Sicherheitsmoduls SE6 erfolgt mit der STÖBER DriveControlSuite (DS6). Hierzu wurde die DS6 um ein Plugin der Firma PILZ mit dem Namen PASmotion erweitert.

PASmotion nutzt zur Kommunikation mit dem Sicherheitsmodul SE6 im Antriebsregler die Kommunikationsschnittstelle der DS6, welche diese mit dem Antriebsregler aufbaut.

Die (Sicherheits-)Konfiguration in PASmotion und im Antriebsregler ist Checksummen- und Passwort-gesichert. Die Sicherheitskonfiguration wird im Antriebsregler sowohl auf SE6 als auch auf der µSD-Karte gespeichert. Dies ermöglicht ein problemloses Handling des Antriebsreglers im Servicefall. Ein Gerätetausch kann sicher erkannt werden.

In PASmotion kann ein Report für die Sicherheitskonfiguration in Form einer PDF-Datei erstellt werden, welche die Konfiguration und Parametrierung der SE6 enthält.

Hinweis:
Ein verlorenes oder vergessenes Passwort kann auch bei STÖBER nicht mehr wiederhergestellt werden.

3.9. Dokumentation

Für SE6 steht, wie bei STÖBER üblich, ein separates Handbuch zur Verfügung. Zum Marktstart ist das Handbuch in den Sprachen DE und EN verfügbar.

Die Übersetzung in weitere Sprachen erfolgt nach Bedarf.

3.10. Validierung und Verifikation

Vor der Auslieferung und nach Änderungen müssen unsere Kunden die korrekte Sicherheitsfunktionalität der Maschine überprüfen und dies dokumentieren. Dies beinhaltet auch die Validierung und Verifikation der Sicherheitsfunktionen, an denen SE6 beteiligt ist.

Die Sicherheitsfunktionalität von SE6 kann mittels der Scope-Funktion der DS6 überprüft werden. Die gemachten Scope-Aufnahmen können vom Kunden in die entsprechenden Unterlagen (Safety-Check, Safety-Abnahmeprotokoll, …) übernommen werden.

Hinweis:
Die Dokumente zur Validierung der Sicherheitsfunktionen haben erfahrungsgemäß bei unseren Kunden sehr unterschiedliche Bezeichnungen.

3.11. Baumusterprüfung

Komponenten aus dem Bereich Sicherheitstechnik unterliegen per Definition der Maschinenrichtlinie. So auch unsere Antriebsregler mit integrierter Sicherheitstechnik.

Daher benötigen wir, um unsere Antriebsregler ordnungsgemäß in Verkehr bringen zu können, eine Geräte-Baumusterprüfung. Diese wurde vom TÜV-Süd Anfang 2018 für den SD6 in Verbindung mit dem neuen Sicherheitsmodul SE6 ausgestellt und kann bei Bedarf aus dem Download-Bereich unserer Webseite heruntergeladen werden.

3.12. Vertriebsstart

Das Sicherheitsmodul ist ab dem 01.11.2018 bei STÖBER offiziell erhältlich. Zu diesem Zeitpunkt wird SE6 zum Brutto-VK von 595 € im SAP-System freigeschaltet und ist sofort ab Lager verfügbar.

SE6 wird offiziell auf der SPS IPC Drives 2018 in Nürnberg vorgestellt und ist dort eines der STÖBER Messe-Highlights.

4. Sicherheitsfunktionen

Im Anschluss an die Marktanalyse zu Projektbeginn wurde beschlossen, nicht alle in der DIN EN 61800-5-2 „Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl- Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit“ beschriebenen Sicherheitsfunktionen zu realisieren. Der Aufwand wäre nicht im Verhältnis zum geschätzten Nutzen gewesen.

Bei der Realisierung der Sicherheitsfunktionen und deren Schnittstellen wurde darauf geachtet, nicht nur die Anforderungen der 61800-5-2 zu erfüllen (SIL-Level), sondern diese auch so zu realisieren, dass unsere Kunden diese auch gemäß den Anforderungen der DIN EN ISO 13849-1 „Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze“ (Performance-Level (PL)) einsetzen können.

Bei korrekter Anwendung können alle auf SE6 verfügbaren Sicherheitsfunktionen das höchste im Maschinenbau benannte Sicherheitsniveau SIL 3/PL e/Kategorie 4 erreichen.

Hinweis:
In diesem Kapitel werden nur die im Projekt E1214 realisierten Sicherheitsfunktionen benannt.

Mit Hilfe der in SE6 implementierten Sicherheitsfunktionen können auch Anforderungen aus anderen, hier nicht explizit genannten Normen erfüllt werden, z. B. EN 13850 „Sicherheit von Maschinen-Not-Halt-Funktion – Gestaltungsleitsätze“.

4.1. Normative Sicherheitsfunktionen nach DIN EN 60204-1

Die DIN EN 60204-1 „Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen – Teil 1: Allgemein Anforderungen“ ist eine der grundlegendsten Normen im Maschinenbau. Sie beschreibt neben den Anforderungen zur grundlegenden elektrischen Sicherheit auch Stopp-Kategorien zum Stillsetzen von Bewegungen.

Achtung:
Viele unserer Kunden nutzen diese Begriffe, da sie die für Antriebsregler relevante Norm EN 61800-5-2 nicht kennen. Hier kommt es gelegentlich zu Missverständnissen mit dem Begriff „Kategorie“.

Sicherheitsfunktion	Beschreibung
Stopp-Kategorie 0	Entspricht der Sicherheitsfunktion STO der DIN EN 61800-5-2
Stopp-Kategorie 1	Entspricht der Sicherheitsfunktion SS1 der DIN EN 61800-5-2
Stopp-Kategorie 2	Entspricht der Sicherheitsfunktion SS2 der DIN EN 61800-5-2

Tabelle 3-Normative Sicherheitsfunktionen nach DIE EN 60204-1

4.2. Normative Sicherheitsfunktionen nach DIN EN 61800-5-2

Die DIN EN 61800-5-2 „Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit“ ist die Basisnorm für die Sicherheit von Antriebsreglern und Frequenzumrichtern. In dieser Norm werden neben den sicheren Stopp-Funktionen weitere Sicherheitsfunktionen zur Begrenzung und Überwachung von Bewegungen sowie Zusatzfunktionen wie die Sichere Bremsenansteuerung beschrieben.

4.2.1. Sichere Stopp-Funktionen

Sicherheitsfunktionen zum sicheren Stillsetzen von Bewegungen

Sicherheitsfunktion	Beschreibung	Reaktion bei erkannter Grenzwertverletzung
STO	Safe Toque Off	-
SS1	Safe Stop 1 Gesteuertes oder überwachtes Überführen in STO	STO
SS2	Safe Stop 2 Gesteuertes oder überwachtes Überführen in SOS	SS1

Tabelle 4- Sichere Stopp-Funktionen nach EN 61800-5-2

4.2.2. Sichere Bewegungsfunktionen

Sicherheitsfunktionen zum Überwachen von Bewegungen. Bei einer Grenzwertverletzung wird das Stillsetzen der Bewegung durch eine der Stopp-Funktionen STO oder SS1 eingeleitet.

Achtung:
Bei einer erkannten Grenzwertverletzung durch eine Bewegungsfunktion wird immer die Sicherheitsfunktion SS1 aktiviert. Diese kann bei Bedarf so parametriert werden, dass direkt ein STO auslöst wird. In der Regel macht dies jedoch keinen Sinn.

Sicherheitsfunktion	Beschreibung	Reaktion bei erkannter Grenzwertverletzung
SLS	Sicher begrenzte Drehzahl	SS1
SSR	Sicher begrenzter Drehzahlbereich	SS1
SDI	Sicher begrenzte Bewegungsrichtung	SS1
SOS	Sicher begrenzter Stillstand	SS1
SLI	Sicher begrenztes Schrittmaß	SS1
SLP	Sicher begrenzte Position	SS1

Tabelle 5- Sichere Bewegungsfunktionen nach EN 61800-5-2

4.2.3. Sichere Bremsfunktionen

Sicherheitsfunktion zur sicheren Ansteuerung von einer oder mehrerer Bremsen.

Sicherheitsfunktion	Beschreibung	Reaktion bei erkannter Grenzwertverletzung
SBC	Sichere Bremsenansteuerung	SS1

Tabelle 6- Sichere Bremsfunktionen nach EN 61800-5-2

4.3. Normative Sicherheitsfunktionen nach DIN EN 14118

Die DIN EN ISO 14118 „Sicherheit von Maschinen – Vermeidung von unerwartetem Anlauf“ beschreibt die Anforderungen zur Verhinderung von unerwartetem Anlauf von Maschinen.

Hinweis:
Im Wesentlichen geht es darum sicherzustellen, nachdem der Antriebsregler in den sicheren Zustand STO geschaltet wurde, dass der sichere STO-Zustand erst nach erfolgter Quittierung wieder verlassen wird.

Sicherheitsfunktion	Beschreibung	Reaktion bei erkannter Grenzwertverletzung
SRL	Sichere Wiederanlaufsperre	STO

Tabelle 7- Sicherheitsfunktionen nach EN 14118

4.4. Nicht normativ beschriebene Sicherheitsfunktionen

Zur Erhöhung der Praxistauglichkeit von SE6 wurden einige der in der EN 61800-5-2 beschriebenen Sicherheitsfunktionen ohne direkte Störungsreaktion implementiert. Um diese leicht identifizieren zu können, wurde den Basis-Sicherheitsfunktionen das Kürzel „-M“ für Monitoring hinzugefügt.

Im Falle von SBT wurde die in der 61800-5-2 beschriebene Sicherheitsfunktion ergänzt, um die Normative Lücke zur 13849-1 im Bereich „Sicheres Bremsenmanagement“ entsprechend den Empfehlungen der „Deutschen Gesetzlichen Unfallversicherung (DGUV)“ zu schließen.

Sicherheitsfunktion	Beschreibung	Reaktion bei erkannter Grenzwertverletzung
SLS-M	Sicher begrenzte Drehzahl – Monitoring	Statusmeldung
SSR-M	Sicher begrenzter Drehzahlbereich – Monitoring	Statusmeldung
SDI-M	Sicher begrenzte Bewegungsrichtung – Monitoring	Statusmeldung
SOS-M	Sicher begrenzter Stillstand – Monitoring	Statusmeldung
SLI-M	Sicher begrenztes Schrittmaß – Monitoring	Statusmeldung
SLP-M	Sicher begrenzte Position – Monitoring	Statusmeldung
SBT	Sicherer Bremsentest	SS1

Tabelle 8- Nicht normativ beschriebene Sicherheitsfunktionen

5. Prinzipielle Funktionsweise

Das Sicherheitsmodul SE6 plausibilisiert den Motorencoder mit Hilfe eines gerechneten virtuellen Encoders und überwacht die Bewegung des Antriebs.

Es werden keine Begrenzungen im Antriebsregler vorgenommen. Einzig bei den Stopp-Funktionen SS1 und SS2 im optionalen Modus „Antriebsgeführt“ greift SE6 in den funktionalen Teil des Antriebsreglers SD6 ein.

5.1. Verfügbaren Sicherheitsfunktionen

Die einzelnen Sicherheitsfunktionen können in nachfolgend genannten Gruppen unterteilt werden.

5.1.1. Sicher Stillsetzen

- Sicherer Stopp 1 (Safe Stop 1; SS1)
- Sicherer Stopp 2 (Safe Stop 2; SS2)

5.1.2. Sicher Begrenzen

Die Begrenzung von Geschwindigkeit und Position erfolgt durch einen erzwungenen Stopp bei einer Grenzwertverletzung. Hierzu wird die Sicherheitsfunktion SS1 aktiviert)

- Sicher begrenzte Geschwindigkeit (Safely-Limited Speed, SLS)
- Sicher begrenzter Geschwindigkeitsbereich (Safe Speed Range; SSR)
- Sicher begrenzte Richtung (Safe Direction; SDI)
- Sicherer Betriebshalt (Safe Operating Stop; SOS)
- Sicher begrenztes Schrittmaß (Safely-Limited Increment; SLI)
- Sicher begrenzte Position (Safely Limited Position, SLP)

5.1.3. Sicher Melden

Alle Sicherheitsfunktionen, die zum Begrenzen von Geschwindigkeit und Position zur Verfügung stehen, werden auch als eine Variante angeboten, welche kein Stoppen erzwingt, sondern eine Grenzwertverletzung lediglich sicher meldet.

5.1.4. Sicheres Bremsenmanagement

Das sichere Bremsenmanagement (Safe Brake Management; SBM) setzt sich aus zwei Sicherheitsfunktionen zusammen:

- Sichere Bremsansteuerung (Safe Brake Control; SBC)
- Sicherer Bremsentest (Safe Brake Test; SBT)

5.2. Reaktion auf Grenzwertverletzung

Bei einer erkannten Grenzwertverletzung bietet SE6 unterschiedliche Reaktionsmöglichkeiten:

- Sicher Melden (-M Funktionen)
- Sicher Abschalten (SS1)
  - Antriebsbasiertes Stoppen
  - Steuerungsbasiertes Stoppen

5.3. Sicherheitsfunktionen kurz erklärt

Im Folgenden werden die wichtigsten verfügbaren Sicherheitsfunktionen kurz erklärt. Die detaillierte Funktionsweise kann bei Bedarf dem SE6-Handbuch entnommen werden.

5.3.1. Sicherer Stopp 1 (Safe Stop 1; SS1)

Nach dem Aktivieren der Sicherheitsfunktion durch das Steuersignal SS1_ACT (SS1_Activate) steuert und/oder überwacht die Sicherheitsfunktion das Stillsetzen des Antriebs. Hierzu stehen verschiedene Möglichkeiten und Optionen zur Verfügung. Nach Ablauf der parametrierten t_max Zeit wird das Leistungsteil im Antriebsregler abgeschaltet (STO).

Antriebsbasiertes Stillsetzen:
SE6 löst einen Halt-Befehl mit der festgelegten Bremsrampe aus. Die Bremsrampe und/oder der Stillstand können zusätzlich zur t_max Zeit überwacht werden und das Abschalten des Leistungsteils (STO) vor Ablauf der t_max Zeit aktivieren.

Steuerungsgeführtes Stillsetzen: Die überlagerte Steuerung bremst den Antrieb bis zum Stillstand ab. Die Bremsrampe und/oder der Stillstand können zusätzlich zur t_max Zeit überwacht werden und das Abschalten des Leistungsteils (STO) vor Ablauf der t_max Zeit aktivieren.

Hinweis:
Wird bei einem steuerungsgeführten SS1 und aktiver Bremsrampenüberwachung eine Grenzwertverletzung erkannt, z. B. aufgrund eines Fehlers in der funktionalen Steuerung, bietet SE6 eine weitere Rückfallebene. Für diesen Fall kann ein „Fallback“ aktiviert werden, sodass die SE6 ein antriebsbasiertes Stillsetzen auslöst.

Wird bei aktiver Bremsrampenüberwachung die parametrierte Bremsrampe nicht eingehalten oder nach Aktivierung der Stillstandsüberwachung eine unzulässige Bewegung erkannt, wird dies als Grenzwertverletzung erkannt.

Der Status der Sicherheitsfunktion wird über die Ausgänge SS1_ACK (Safe Stop 1_Acknowledge) und STO_ACK (Safe Torque Off_Acknowledge) dem Anwender bereitgestellt.

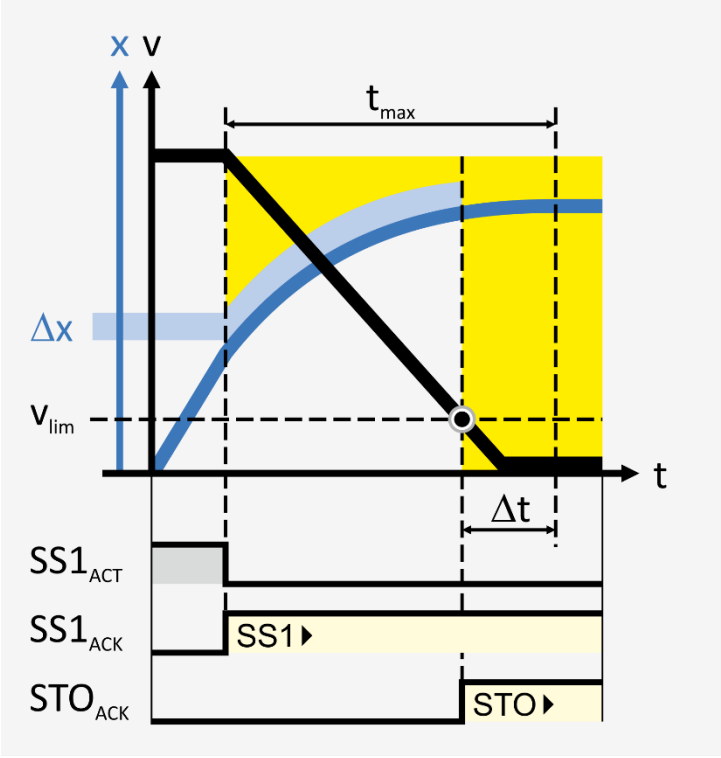

Abbildung 2- Sicherer Stopp 1 (SS1)

5.3.2. Sicherer Stopp 2 (Safe Stop 2; SS2)

Nach dem Aktivieren der Sicherheitsfunktion durch das Steuersignal SS2_ACT (SS2_Activate) steuert und/oder überwacht die Sicherheitsfunktion das Stillsetzen des Antriebs. Hierzu stehen verschiedene Möglichkeiten und Optionen zur Verfügung. Nach Ablauf der parametrierten t_max Zeit bleibt der Antrieb bestromt und wird auf Stillstand überwacht (SOS).

Antriebsbasiertes Stillsetzen:
SE6 löst einen Halt-Befehl mit der festgelegten Bremsrampe aus. Die Bremsrampe und/oder der Stillstand können zusätzlich zur t_max Zeit überwacht werden und die Stillstandsüberwachung (SOS) vor Ablauf der t_max Zeit aktivieren.

Steuerungsgeführtes Stillsetzen:
Die überlagerte Steuerung bremst den Antrieb bis zum Stillstand ab. Die Bremsrampe und/oder der Stillstand können zusätzlich zur t_max Zeit überwacht werden und die Stillstandsüberwachung (SOS) vor Ablauf der t_max Zeit aktivieren.

Wird bei aktiver Bremsrampenüberwachung die parametrierte Bremsrampe nicht eingehalten oder nach Aktivierung der Stillstandsüberwachung eine unzulässige Bewegung erkannt, wird dies als Grenzwertverletzung erkannt.

Der Status der Sicherheitsfunktion wird über die Ausgänge SS2_ACK (Safe Stopp 2_Acknowledge) und SSA_ACK (Safe Standstill_Acknowledge) dem Anwender bereitgestellt.

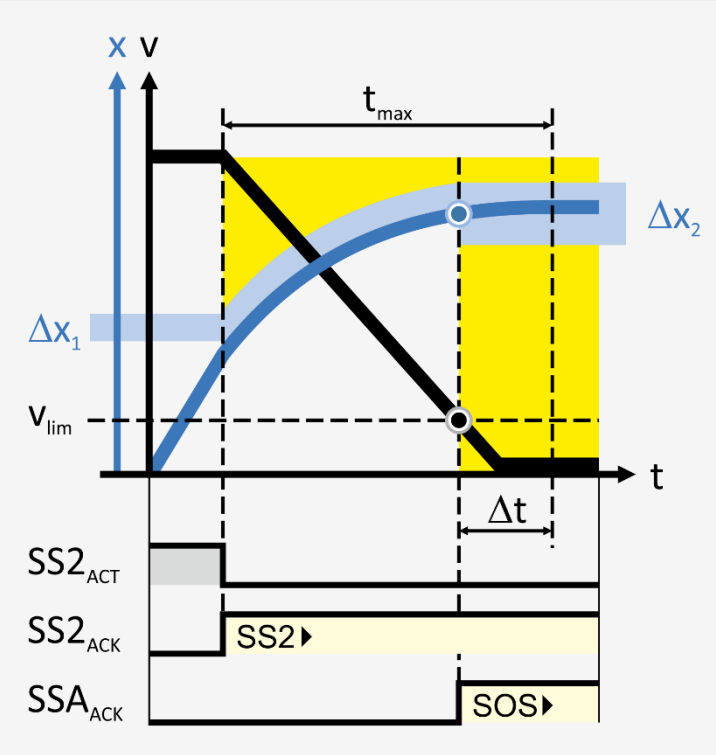

Abbildung 3- Sicherer Stopp 2 (SS2)

5.3.3. Sicher begrenzte Geschwindigkeit (Safely-Limited Speed, SLS)

Nach dem Aktivieren der Sicherheitsfunktion durch das Steuersignal SLS_ACT (SLS_Activate) und Ablauf der Verzögerungszeit t_delay überwacht die Sicherheitsfunktion, dass die konfigurierte Geschwindigkeit nicht überschritten wird. Wird der Betrag des Geschwindigkeitsgrenzwerts über- bzw. unterschritten, wird eine Grenzwertverletzung erkannt.

Der Status der Sicherheitsfunktion wird über den Ausgang SRA_ACK (Safe Range_Acknowledge) dem Anwender bereitgestellt.

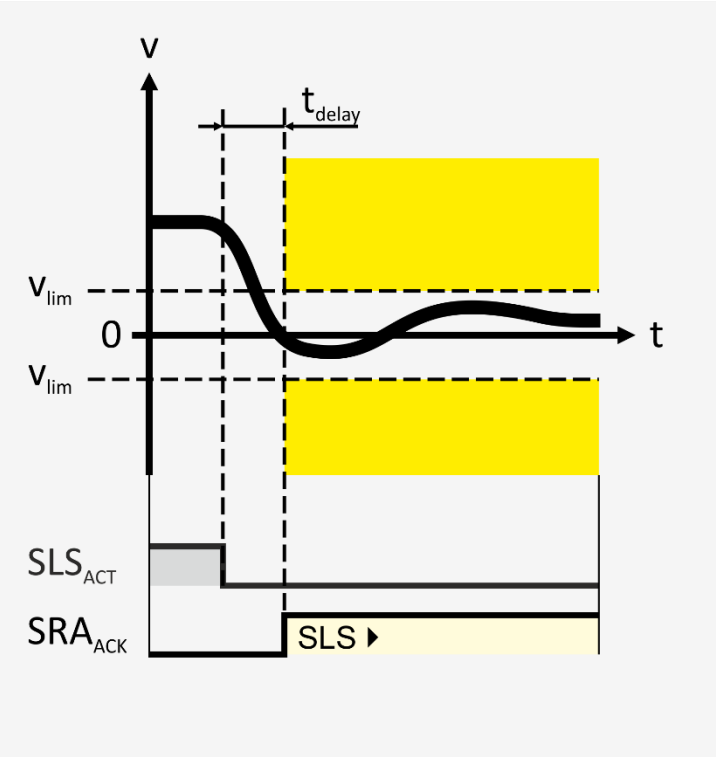

Abbildung 4- Sicher begrenzte Geschwindigkeit (SLS)

5.3.4. Sicher begrenzter Geschwindigkeitsbereich (Safe Speed Range; SSR)

Nach dem Aktivieren der Sicherheitsfunktion durch das Steuersignal SSR_ACT (SSR_Activate) und Ablauf der Verzögerungszeit t_delay überwacht die Sicherheitsfunktion, dass die konfigurierten Geschwindigkeiten nicht überschritten werden. Wird eine der beiden projektierten Geschwindigkeitsgrenzen über- bzw. unterschritten, wird eine Grenzwertverletzung erkannt.

Der Status der Sicherheitsfunktion wird über den Ausgang SRA_ACK (Safe Range_Acknowledge) dem Anwender bereitgestellt.

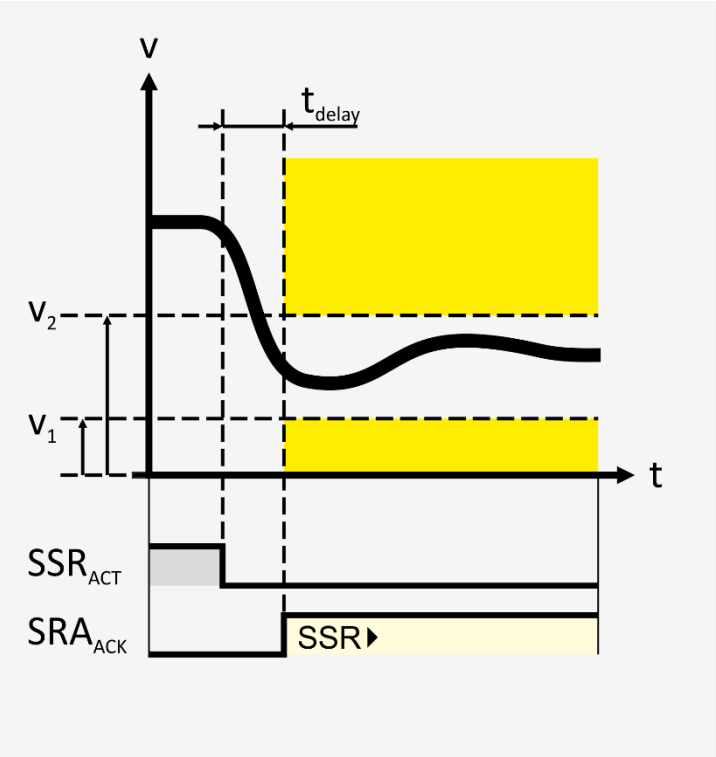

Abbildung 5- Sicherer Geschwindigkeitsbereich (SSR)

5.3.5. Sicher begrenzte Richtung (Safe Direction; SDI)

Nach dem Aktivieren der Sicherheitsfunktion durch das Steuersignal SDI_ACT (SDI_Activate) und Ablauf der Verzögerungszeit t_delay überwacht die Sicherheitsfunktion, dass die konfigurierten Bewegungsrichtung eingehalten wird.

Hierzu wird zum Zeitpunkt des Überwachungsstarts eine Überwachungsposition aus der Istposition der Motorwelle und dem parametrierten Toleranzbereich gebildet. Bewegt sich die Achse in die zulässige Richtung, wird die Überwachungsposition nachgeführt.

Bewegt sich die Achse in die gesperrte Drehrichtung und erreicht die Überwachungsposition, wird eine Grenzwertverletzung erkannt.

Der Status der Sicherheitsfunktion wird über den Ausgang SDA_ACK (Safe Direction_Acknowledge) dem Anwender bereitgestellt.

Hinweis: Mit Hilfe der positionsbasierten Überwachung wird die Sicherheitsfunktion SDI sehr unempfindlich gegenüber Drehzahlschwankungen aufgrund von Encoder-Rauschen.

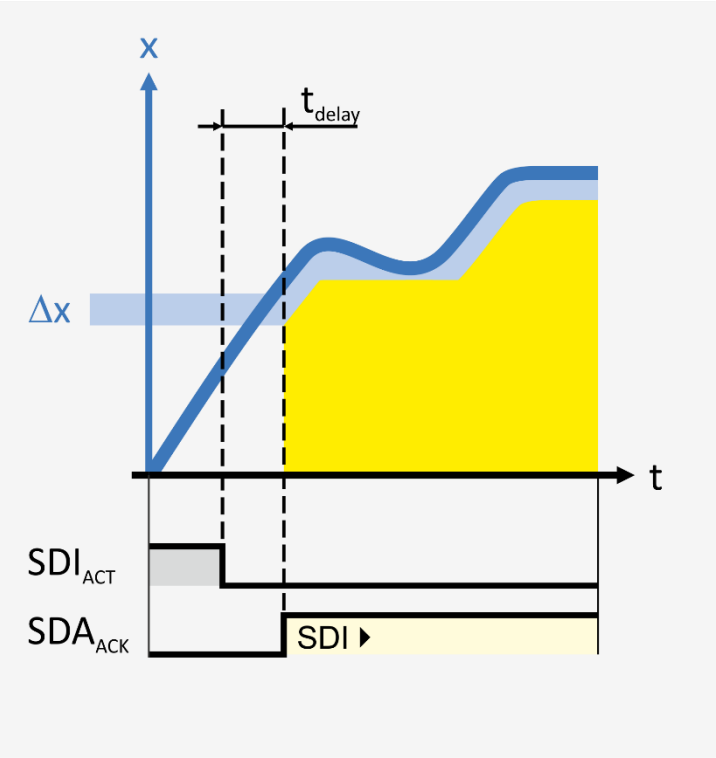

Abbildung 6- Sicher begrenzte Richtung (SDI)

5.3.6. Sicherer Betriebshalt (Safe Operating Stop; SOS)

Nach dem Aktivieren der Sicherheitsfunktion durch das Steuersignal SOS_ACT (SOS_Activate) und Ablauf der Verzögerungszeit t_max überwacht die Sicherheitsfunktion, dass sich der Antrieb nicht bewegt. Mit Hilfe einer optionalen Stillstandserkennung kann die Verzögerungszeit bis zur Aktivierung der Überwachung reduziert werden.

Zum Zeitpunkt des Überwachungsstarts wird ein Positionsfenster um die Istposition der Motorwelle mit dem parametrierten Toleranzbereich gebildet. Überschreitet die Achse eine der Positionsgrenzen, wird eine Grenzwertverletzung erkannt.

Der Status der Sicherheitsfunktion wird über den Ausgang SSA_ACK (Safe Standstill_Acknowledge) dem Anwender bereitgestellt.

Hinweis:
Mit Hilfe der positionsbasierten Überwachung wird die Sicherheitsfunktion SOS sehr unempfindlich gegenüber Drehzahlschwankungen aufgrund von Encoder-Rauschen.

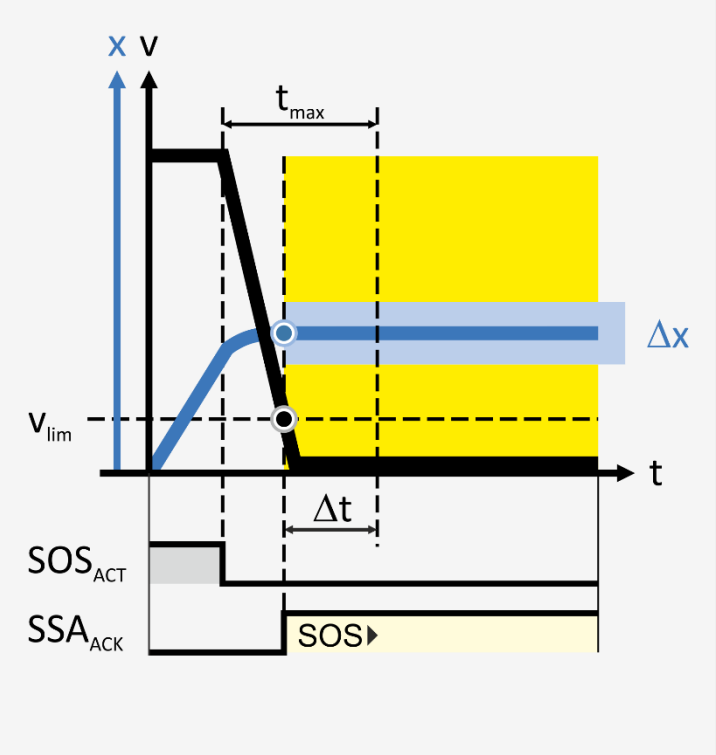

Abbildung 7- Sicherer Betriebshalt (SOS)

5.3.7. Sicher begrenztes Schrittmaß (Safely Limited Increment; SLI)

Nach dem Aktivieren der Sicherheitsfunktion durch das Steuersignal SLI_ACT (SLI_Activate) und Ablauf der Verzögerungszeit t_delay überwacht die Sicherheitsfunktion, dass sich der Antrieb nur im zulässigen Bereich bewegt.

Zum Zeitpunkt des Überwachungsstarts wird ein Positionsfenster um die Istposition der Motorwelle mit dem parametrierten Grenzen gebildet. Überschreitet die Achse eine der Positionsgrenzen, wird eine Grenzwertverletzung erkannt.

Der Status der Sicherheitsfunktion wird über den Ausgang SRA_ACK (Safe Range_Acknowledge) dem Anwender bereitgestellt.

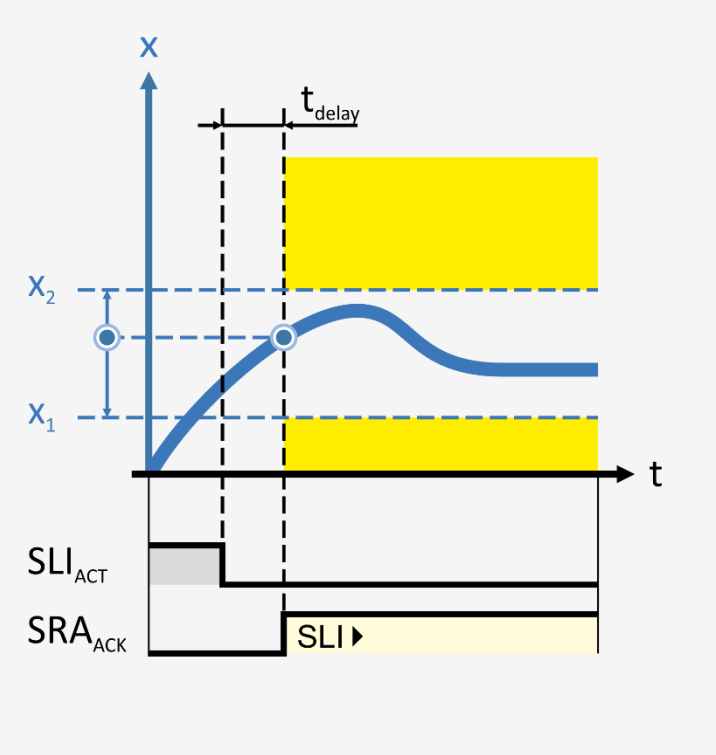

Abbildung 8- Sicher begrenztes Schrittmaß (SLI)

5.3.8. Sicher begrenzte Position (Safely Limited Position, SLP)

Nach dem Aktivieren der Sicherheitsfunktion durch das Steuersignal SLP_ACT (SLP_Activate) und Ablauf der Verzögerungszeit t_delay überwacht die Sicherheitsfunktion, dass sich der Antrieb nur im parametrierten Positionsbereich bewegt. Überschreitet die Achse eine der Positionsgrenzen wird eine Grenzwertverletzung erkannt.

Der Status der Sicherheitsfunktion wird über den Ausgang SRA_ACK (Safe Range_Acknowledge) dem Anwender bereitgestellt.

> Hinweis:
> Die Sicherheitsfunktion SLP benötigt einen zweiten Multiturn-Encoder zur Plausibilisierung des Motorencoders. Die beiden Encoder müssen während der Inbetriebnahme zueinander abgeglichen und referenziert werden.

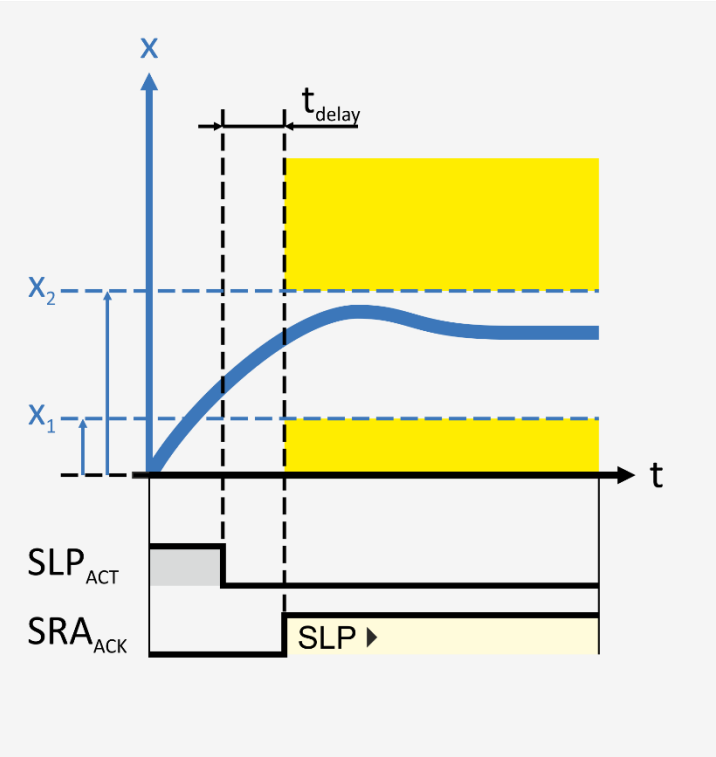

Abbildung 9- Sicher begrenzte Position (SLP)

5.3.9. Sicheres Bremsenmanagement

Das sichere Bremsenmanagement besteht aus zwei Komponenten:

- Sicherem Ansteuern (Safe Brake Control; SBC)
- Sicherem Überwachen (Safe Brake Test; SBT)

Das sichere Ansteuern der Bremsen wird mittels der SE6-Hardware und für den Anwender unsichtbaren Tests während des Betriebs sichergestellt.

Nach dem Aktivieren der Sicherheitsfunktion durch das Steuersignal SBT_ACT (SBT_Activate) und Ablauf der Verzögerungszeit t_delay überwacht die Sicherheitsfunktion den zuvor für den Bremsentest definierten Ablauf. Während des Ablaufs der einzelnen Testschritte wird der Antrieb auf Stillstand überwacht. Nach dem Geräteanlauf und nach Ablauf der Zeit des definierten Testzyklus meldet die SBC-Funktion, dass ein Bremsentest benötigt wird und startet eine Toleranzzeit innerhalb derer ein Bremsentest zwingend erfolgen muss. Dies muss vom Kunden beim Maschinenkonzept berücksichtigt werden.

Der Status der Sicherheitsfunktion wird über die Ausgänge SBA_ACK (Safe Brake_Acknowledge) und SSA (Safe Standstill_Acknowledge) dem Anwender bereitgestellt.

Hinweis: Der Bremsentest ist nicht in jeder Position einer Achse möglich bzw. sinnvoll. Vor dem Bremsentest muss der Anwender die Achse in eine definierte Position fahren.

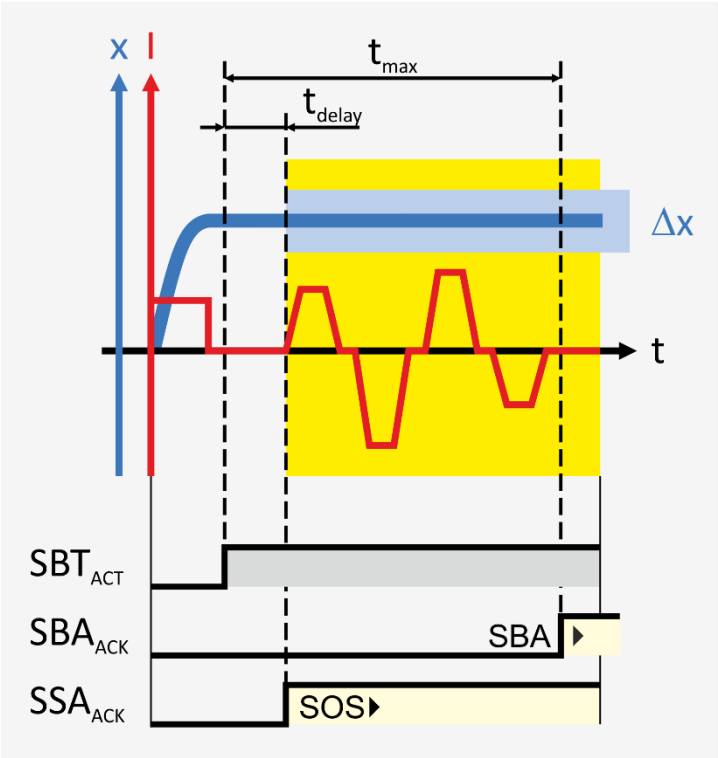

Abbildung 10- Sicherer Bremsentest (SBT)

6. Besonderheiten

Der Antriebsregler SD6 mit dem Sicherheitsmodul SE6 stellt für den Kunden einige Besonderheiten zur Verfügung, welche am Markt nicht alltäglich sind.

Kunden, die diese Funktionalitäten benötigen, haben am Markt nur eine sehr begrenzte alternative Auswahl.

Hinweis:
Das ePEP-Projektteam ist über Rückmeldungen zu Marktbegleitern, die vergleichbare Funktionalität bieten, sehr interessiert und hofft hierzu auf Feedback aus dem Feld.

6.1. Encoder-unabhängig

Zum Betrieb von SE6 werden keine speziellen Fail-Safe-Encoder benötigt. Auch werden keine speziellen Anforderungen an den Encoder-Anbau gestellt. Dadurch kann SD6 auch problemlos Motoren mit Hohlwelle, Linearmotoren, Motoren mit Resolvern oder induktiven Encodern sicher überwachen.

Hinweis:
Der sichere Encoder-Anbau an den Motor hat bei STÖBER die Bezeichnung FMA (Fehlerausschluss für die mechanische Ankopplung).

Das „Institut für Arbeitssicherheit“ (IFA) der „Deutschen gesetzlichen Unfallversicherung“ (DGUV) hat zu diesem Thema „Brauchen sichere Antriebssteuerungen auch sichere Positionsgeber“ zuletzt im Jahr 2017 publiziert. Nahezu alle am Markt bekannten Hersteller von Antriebsreglern halten sich an die dort zusammengefassten (normativen) Anforderungen.

Die von STÖBER und PILZ gemeinsam entwickelte Lösung wird in diesem Dokument nur indirekt beschrieben. Die Lösung basiert darauf, dass der Motorencoder durch den Antriebsregler plausibilisiert wird. Hierzu errechnet SE6 aus den Daten des Leistungsteils einen „virtuellen Encoder“. Mit dessen Hilfe kann auch das grundsätzliche Problem „Lösen des Encoders von der Motorwelle“ gelöst werden, welches eine der Grundprobleme in der Publikation der IFA ist.

Einzig bei der Sicherheitsfunktion SLP (Safe Limited Position) wird zur Plausibilisierung der Multiturn-Stufe des Motorencoders ein zusätzlicher (SSI-)Multiturn-Encoder an der SE6-Schnittstelle X50 benötigt.

6.2. Betrieb von Synchron-Servomotoren

Das Sicherheitsmodul SE6 ist primär zur Überwachung von Synchron-Servomotoren entwickelt worden. Bei Synchron-Servomotoren wird der Motorencoder während des Betriebs mit Hilfe eines auf Basis des Leistungsteils berechneten virtuellen Encoders berechnet. Dieser ersetzt einen zweiten Encoder.

Mit Hilfe eines externen Encoders an der X50 Schnittstelle können auch Asynchronmotoren überwacht werden.

6.3. Betrieb von Asynchronmotoren

Soll die Geschwindigkeit oder Position eines Asynchronmotors überwacht werden, wird ein zweiter Encoder an der Schnittstelle X50 benötigt (TTL oder SSI). Für Asynchronmotoren kann kein virtueller Encoder berechnet werden.

An den X50-Encoder und dessen Anbau werden keine speziellen Anforderungen gestellt.

Einzig eine Diversität des X50-Encoders zum Motorencoder wird benötigt, und es muss darauf geachtet werden, dass die Montage der beiden Encoder unabhängig voneinander ist, um die Anforderungen an Fehler gemeinsamer Ursache zu erfüllen.

6.4. Absichern von schwerkraftbelasteten Achsen

Zum Zeitpunkt der Markteinführung von SE6 ist keine in der EU harmonisierte Norm bekannt, welche das Thema „Schwerkraftbelastete Achsen“ behandelt.

Die „DIN EN 16090-1:2016-02 Entwurf – Werkzeugmaschinen Sicherheit – Fräsmaschinen, Bearbeitungszentren, Transfermaschinen – Teil 1: Sicherheitsanforderungen“ befindet sich noch in Bearbeitung und ist nicht harmonisiert.

Der Teil des 16090-1-Entwurfs, in welchem die Absicherung von schwerkraftbelasteten Achsen behandelt wird, basiert auf den Empfehlungen des DGUV-Fachbereich Holz und Metall aus dem Fachbereichsinformationsblatt Nr. 005 Ausgabe 09/2012.

Dieses Dokument war eine der Vorgaben zum sicheren Bremsenmanagement im SE6-Entwicklungsprojekt.

Das Fachbereichsinformationsblatt 005-09/2012 der DGUV mit dem Titel „Schwerkraftbelastete Achsen“ kann von unseren Kunden und Interessenten bei Interesse kostenlos über STÖBER „Sales & Product Management Electronics“ (SPE) bezogen werden. Alternativ kann es vom Server der DGUV/IFA heruntergeladen werden.

Mit Hilfe von SE6 können unsere Kunden die im Fachbereichsinformationsblatt zusammengestellten Empfehlungen erfüllen. SE6 erfüllt dabei die Empfehlungen bezüglich der beschriebenen Lösungen, basierend auf einer als auch auf zwei Bremsen.

Hinweis:
Das Thema „Absichern von schwerkraftbelasteten Achsen“ wird oftmals mehr oder weniger kompetent durch Artikel in Fachzeitschriften beschrieben. Hierzu gibt es auch eine Publikation von STÖBER zu SE6, welche im Herbst 2018 an diverse Agenturen verteilt wurde.

6.4.1. Marktsituation

Die Sicherheitsfunktion SBC findet sich bei vielen Marktbegleitern mit unterschiedlichen Sicherheitsklassifizierungen und wird auch dort aktiv beworben.

In der Regel erfüllen diese Systeme jedoch lediglich die Anforderungen aus der EN 61800-5-2 an Antriebsregler. D. h., sie stellen einen sicheren Ausgang zur Ansteuerung einer Bremse zur Verfügung. Die erweiterten Anforderungen der DGUV an Test und Testüberwachung werden nicht erfüllt.

Eine bekannte Ausnahme ist die Firma PILZ, die für den Servostar 700 direkt (Brandlabeling Servostar Grundgerät als Protego) und indirekt über Kollmorgen eine Lösung anbietet. Diese birgt jedoch einige Praxisprobleme. Z. B. kann der Servostar keine zwei Bremsen verwalten und benötigt dazu kostspieliges Zubehör.

Bosch bewirbt seit Mitte 2018 eine mit STÖBER vergleichbare Lösung, nachdem jahrelang ein funktionaler Bremsentest ohne belastbare Sicherheitskennzahlen zum Einsatz gekommen ist. Diese Lösung stufen wir als direkten Wettbewerb ein.

Mayr-Bremsen aus Kaufbeuren bewirbt eine zusammen mit PILZ entwickelte antriebsunabhängige Lösung, welche auf einem speziellen Sicherheitsschaltgerät realisiert wurde. Diese ist kritisch zu bewerten, da auch diese Lösung keinen Bremsentest zur Verfügung stellt.

6.5. Herstellerneutrale Schnittstelle

Das Sicherheitsmodul SE6 stellt 8 sichere Eingänge zur Verfügung. Diese können mittels Kontakten oder sicheren (überwachten) Halbleiterausgängen (sog. OSSD-Signalen) angesteuert werden. Zusätzlich zu den Eingängen stellt das Sicherheitsmodul 5 sichere (Halbleiter-)Ausgänge für Statusmeldungen zur Verfügung. Die Ein- und Ausgänge können den projektierten Sicherheitsfunktionen flexibel zugeordnet werden.

Damit kann SE6 herstellerunabhängig an die bekannten am Markt befindlichen Sicherheitssteuerungen angeschlossen werden.

Ein interessantes Feature von SE6 besteht darin, dass die Basis-Sicherheitsfunktion SS1 einen zusätzlichen Eingang zur direkten Anwahl von STO zur Verfügung stellt. Alle anderen Sicherheitsfunktionen benötigen nur eine Anschlussleitung zur Aktivierung.

Auf diese Weise konnte die benötigte Gesamtverdrahtung minimiert werden.

Hinweis:
Das ePEP-Projektteam ist auf der Suche nach potenziellen Interessenten für eine FSoE und/oder PROFIsafe-Anbindung. Hierzu nehmen wir gerne Feedback aus dem Markt entgegen.

6.6. Vermeiden von Fehlauslösungen

Die Ermittlung der Motorgeschwindigkeit basiert auf der Positionsmessung des Motorencoders. Messtoleranzen und ungünstige Abtast-Timings führen aufgrund der Auflösung zu Fehlern bei der Berechnung der Motordrehzahl.

Wird beispielsweise ein Absolut-Encoder mit 12 Bit Auflösung alle 250 µS abgetastet, beträgt die Geschwindigkeits-Auflösung, wenn ein Bit zu viel oder zu wenig gemessen wurde, ca. +/- 60 U/min. Bedingt durch mechanische Effekte wie z. B. Ketten, können weitere Störimpulse auf die gemessene Geschwindigkeit Einfluss haben.

Um Fehlauslösungen bei der Motorüberwachung zu vermeiden, bietet SE6 die Möglichkeit, Störimpulse gezielt auszublenden. Normativ vorgegebene Grenzwerte können auf diese Weise mit geringem Sicherheitsabstand angefahren werden.

6.7. Multiinstanz-Fähigkeit

SE6 kann zusätzlich zur Basis-Sicherheitsfunktion SS1 bis zu 10 Sicherheitsfunktionen gleichzeitig überwachen. Der Anwender kann diese Sicherheitsfunktionen nach Belieben zusammenstellen.

Der Anwender kann beispielsweise gleichzeitig bis zu 10 Geschwindigkeiten (SLS) oder 10 Bewegungsbereiche (SLI) sicher überwachen.

Hinweis:
Die von uns angebotene Multiinstanz-Fähigkeit der Sicherheitsfunktionen konnten wir bisher in dieser Form bei keinem Marktbegleiter beobachten.

6.8. Reaktion auf Grenzwertverletzungen

SE6 bietet verschiedene Möglichkeiten um auf erkannte Grenzwertverletzungen zu reagieren

6.8.1. Sicheres Melden

SE6 bietet für die Sicherheitsfunktionen zur Bewegungsüberwachung jeweils eine Monitoring-Variante an. Erkennt eine aktivierte Monitoring-Funktion eine Grenzwertverletzung, wird diese lediglich an die überlagerte Sicherheitssteuerung gemeldet, ohne direkte Reaktion im Antriebsregler.

Applikationsabhängig kann die überlagerte Sicherheitssteuerung entscheiden, ob und wie auf die Statusmeldung vom Antriebsregler reagiert wird.

Hinweis: Die Monitoring-Funktionen sind im Projektierungstool mit dem Zusatz -M gekennzeichnet, z. B. SLS-M.

6.8.2. Sicheres Abschalten

Erkennt eine der sicheren Bewegungsfunktionen (z. B. SLS) eine Grenzwertverletzung, wird im Antriebsregler die Sicherheitsfunktion Safe Stop 1 (SS1) aktiv. In diesem Fall muss der Antrieb stillgesetzt werden. Hierzu stehen passend zum Anwendungsfall zwei unterschiedliche Varianten zur Verfügung.

6.8.2.1. Antriebsbasiertes Stoppen

Bei Aktivierung der Sicherheitsfunktion SS1 wird auf dem Antriebsreger ein Halt-Befehl mit der projektierten Bremsrampe aktiviert. Die Zeit zwischen erkannter Grenzwertverletzung und Start der Bremsrampe beträgt in diesem Fall nur wenige Millisekunden. SE6 stellt zur Überwachung auf korrekte Funktion und möglichst schnellem Abschalten des Leistungsteils unterschiedliche Möglichkeiten zur Verfügung

- Bremsrampenüberwachung
- Stillstandserkennung
- Maximalzeit

Spätestens nach Ablauf der Maximalzeit wird das Leistungsteil des Antriebsreglers sicher abgeschaltet.

6.8.2.2. Steuerungsbasiertes Stoppen

Bei Aktivierung der Sicherheitsfunktion SS1 wird auf dem Antriebsregler kein Halt-Befehl ausgelöst. Diese Funktion wird der überlagerten Steuerung überlassen, welche somit die Kontrolle über den Antriebsregler behält. Dies ist insbesondere bei Verbundantrieben mit zentraler Bewegungssteuerung von Vorteil da dies ein koordiniertes abbremsen der Maschine ermöglicht. SE6 stellt zur Überwachung auf korrekte Funktion und möglichst schnellem Abschalten des Leistungsteils unterschiedliche Möglichkeiten zur Verfügung

- Bremsrampenüberwachung
- Stillstandserkennung
- Maximalzeit

Erkennt SE6, dass die Bremsrampe nicht den projektierten Vorgaben entspricht, kann als „Fallback“ wie beim antriebsbasierten SS1 von SE6 ein Halt-Befehl aktiviert werden.

Spätestens nach Ablauf der Maximalzeit wird das Leistungsteil des Antriebsreglers sicher abgeschaltet.

6.9. Sicherheitsniveau

SE6 erfüllt für alle Sicherheitsfunktionen die Anforderungen an SIL 3/ PL e (Kat. 4)

Die SIL-Klassifizierung basiert auf unserer Produktnorm für Antriebsregler DIN EN 61800-5-2. SIL 3 ist darin die höchstmögliche Klassifizierung.

Die PL-Klassifizierung entstammt der für 99,9 % unserer Kunden anzuwendenden DIN EN ISO 13849-1. PL e ist das höchste darin beschriebene Sicherheitsniveau.

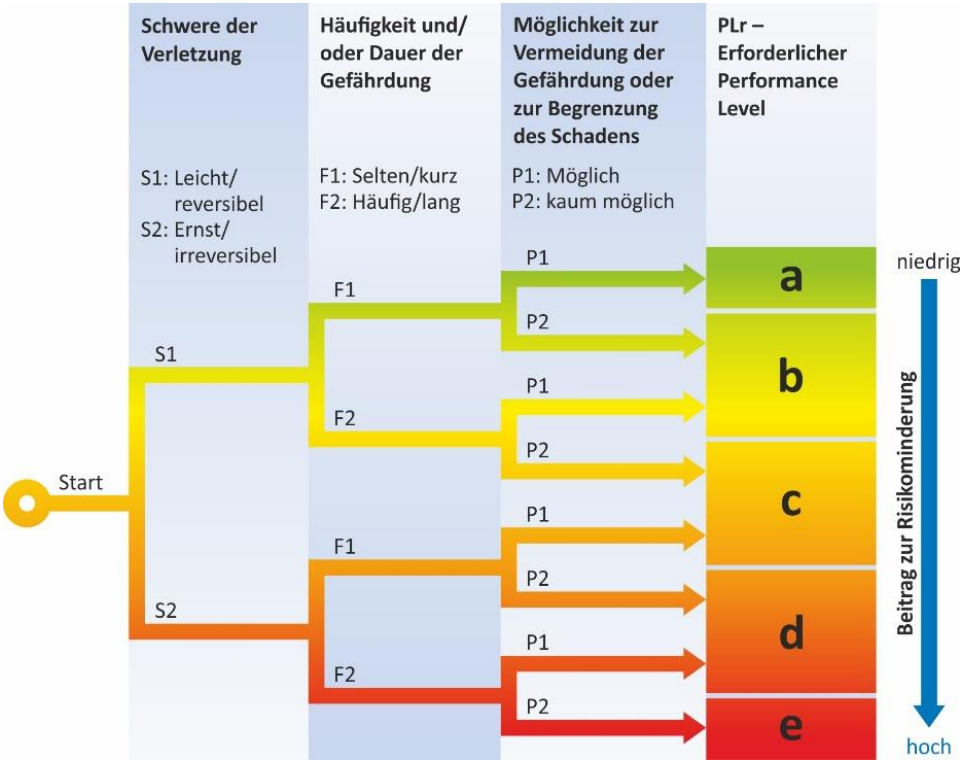

Abbildung 11- Risikograph der DIN EN ISO 13849-1

6.10. Worst-Case-Reaktionszeit

Die Zeit vom Auslösen einer Sicherheitsfunktion an einer Maschine bis zum Abschalten der Antriebe untergliedert sich in mehrere Phasen.

Die Phasen vom Auslösen eines Sensors (z. B. Not-Halt Taster), dessen Erkennen und Verarbeiten der Information in der Sicherheitssteuerung ist unabhängig von SE6.

Abhängig vom Ausgangstyp der Sicherheitssteuerung und dessen Realisierung müssen die Eingänge von SE6 verzögert werden, um keine Fehlauslösungen aufgrund von Testimpulsen zu erzeugen. Hierzu können die Eingänge von SE6 mit Filterzeiten von bis zu 10 ms parametriert werden (Typisch 1 ms).

Nach Ablauf dieser von SE6 unabhängigen Verzögerungszeit erkennt SE6 die Aktivierung einer Sicherheitsfunktion nach spätestens einem Programmzyklus. Zur Erkennung einer Grenzwertverletzung wird ein zusätzlicher Zyklus benötigt. Ein weiterer Zyklus wird zum Aktivieren der Reaktion auf die Grenzwertverletzung (in der Regel SS1) benötigt.

Die Zeit für das Stoppen des Antriebs ist wieder applikationsabhängig. Diese hängt von der Antriebsmechanik, deren Belastung und den möglichen Bremsrampen ab. Typische Werte hierfür liegen in der Praxis zwischen 100 ms und mehreren Sekunden.

Für den applikationsunabhängigen Teil vom Erkennen der Aktivierung der Sicherheitsfunktion bis zum Einleiten der Störungsreaktion werden von SE6 maximal 3 Zyklen benötigt. Die Zykluszeit von SE6 beträgt 3 ms. Was zu der von uns beworbenen Worst-Case-Reaktionszeit von 10 ms führt.

Hinweis:
Am Markt werden sehr unterschiedliche Zeiten beworben. Beckhoff bewirbt beispielsweise 31,25 µs. Dies sind in der Regel Best-Case-Zeiten.
Die FSoE-Watchdog-Überwachungszeit im Beckhoff-System beträgt z. B. im Default 100 ms. Werte unter 50 ms können zu Problemen im System bei Telegrammausfällen führen.

6.11. Service-Konzept

Das STÖBER Service-Konzept ist denkbar einfach. Sowohl für den Motor als auch für den Antriebsregler.

6.11.1. Motor

Da das SE6-Sicherheitskonzept keinerlei spezielle Anforderungen an den Motor, den Encoder und den Encoder-Anbau hat, kann dieser bei Bedarf einfach 1:1 im spannungslosen Zustand gegen

einen Motor vom gleichen Typ getauscht werden. Auch die Reparatur des Motors vor Ort ist problemlos möglich.

Einschränkungen, basierend auf dem branchenüblichen „Fehlerausschluss für den Encoder-Anbau“, entfallen.

- Lösen des „fehlersicher“ montierten Encoders.
  Bricht die Encoder-Halteschraube beim Versuch, die Verbindung zu lösen, muss die Motorwelle aufgebohrt und nachbearbeitet werden.
- Notwendige Ruhezeit zum Aushärten der Klebeverbindung.
  Die entsprechend der bestimmungsgemäßen Verwendung von Heidenhain zu verwendende Klebeverbindung hat eine Aushärtezeit von 6 h bis 12 h. In der Praxis „über Nacht“.
- Überprüfung der Encodermontage.
- Dokumentation zur Nachweisführung.

Hinweis:
In der Regel müssen Motoren, bei denen der Encoder „fehlersicher“ montiert werden muss, im Service-Fall zurück zum Hersteller!

6.11.2. Antriebsregler

Die Safety-Projektierung ist sowohl auf SE6 als auch auf der SD-Karte gespeichert. Wird der Antriebsregler wegen eines Defekts getauscht und die SD-Karte des „alten“ Geräts in den „Neuen“ gesteckt, erkennt dieser den Tausch. Um die Safety-Applikation auf den „neuen“ Antriebsregler zu übernehmen, wird eine bewusste Handlung benötigt. Diese kann direkt am Bedienfeld des Antriebsreglers durchgeführt werden.

Nach dem Gerätestart erfolgt eine Meldung im Display, welche durch einen 2 s langen Tastendruck innerhalb eines Zeitfensters an den Bedientasten quittiert werden muss.
Nach dem 2 s-Tastendruck zeigt der Antriebsregler die Checksumme der Safety-Konfiguration an, welche vom Bediener überprüft werden muss. Damit wird ausgeschlossen, dass der Antriebsregler beim Tausch verwechselt wird.

Im Anschluss ist der „neue“ Antriebsregler betriebsbereit, und die Maschinenfunktionalität kann getestet werden.

Hinweis:
Das Thema Service-Konzept wird von unseren Marktbegleitern oftmals in den Hintergrund gestellt, da das Ersetzen eines Motors oder Antriebsreglers nicht ohne Zutun vom Hersteller oder eines hochqualifizierten Mitarbeiters möglich ist.

7. Marktvergleich

Die am Markt verfügbaren Lösungen für erweiterte antriebsbasierte Sicherheitstechnik sind stark unterschiedlich. Die angebotenen Konzepte hängen teilweise auch vom Prüfinstitut ab.

Im Wesentlichen kann man den Markt in folgende Gruppen einteilen:

1. Antriebslösungen basierend auf Failsafe-Encodern
2. Antriebslösungen basierend auf konventionellen Sin/Cos-Encodern
3. Antriebsregler-unabhängige Systeme

7.1. Antriebslösungen basierend „Failsafe-Encodern“

Heidenhain als auch Sick-Stegmann bieten Encoder zum Einbau in Servomotoren mit Sicherheitszertifizierung an.

Heidenhain bietet mit den EnDat 2.2-FS-Encodern volldigitale Failsafe-Encoder an. Diese sind sowohl optisch als auch induktiv erhältlich. Für die Auswertung der Encoder wird ein spezieller Stack benötigt. Die Anzahl der Antriebsregler, welche die Anforderungen an die Encoder-Auswertung erfüllen, ist überschaubar. Bekanntester Marktteilnehmer ist B&R.

Sick Stegmann bietet sowohl klassische Sin/Cos-basierende (Hiperface-Safety) als auch volldigitale Failsafe-Encoder (Hiperface-DSL-Safety) an. Kunden sind beispielsweise die Firma SEW oder KEB, welche die Sin/Cos-basierenden Varianten einsetzt.

Allen Lösungen gemeinsam ist, dass diese auf einem Fehlerausschluss für den mechanischen Anbau des Encoders am Motor basieren. Da diese Encoder basierend auf dem FMA-Anbau nur über eine SIL 2-Zertifizierung verfügen, beschränkt dies das Gesamtsystem in der Regel auch auf SIL 2.

Hinweis:
In der Ausgabe 2017 des IFA-Positionspapiers zu sicheren Antriebssteuerungen und Encodern gab es eine interessante Ergänzung. Es wurde beschrieben, dass der FMA-Anbau nicht zwangsläufig zu einer Reduzierung des Sicherheitsniveaus auf SIL 2 führt. Abhängig vom Zertifizierungsinstitut und Zertifizierungsdatum wurden daher unterschiedliche Maßstäbe bei der Bewertung angewandt.

7.2. Antriebslösungen basierend auf konventionellen Sin/Cos-Encodern

Der größte Teil unserer Marktbegleiter setzt auf konventionelle Sin/Cos-Encoder, welche durch den Antriebsregler überwacht werden. An den kritischen Stellen wird mittels Fehlerausschluss argumentiert, was in Summe in der Regel zu einer SIL 2-Einstufung führt.

Die Systeme sind daran zu erkennen, dass die von Heidenhain angebotenen optischen EnDat 2.1-Sin/Cos-Encoder zum Einsatz kommen.

7.3. Antriebsregler-unabhängige Systeme

Antriebsregler-unabhängige Systeme basieren in der Regel auf den Sin/Cos-Spuren der Motorencoder. In den Handbüchern werden die Anforderungen an diese Systeme beschrieben. Die Systeme sind meist flexibel und bieten unterschiedliche Möglichkeiten zur Encoder-Plausibilisierung. Nahezu alle namhaften und bekannten Hersteller von Sicherheitsschaltgeräten haben entsprechende Baugruppen im Programm. Beispielsweise PILZ, Siemens, BBH, DINA, Phoenix Contakt, Dold, Schmersal, Motrona, …

Bei Lösungen mit einem Encoder wird ein Fehlerausschluss für den Encoder-Anbau benötigt. Bei Plausibilisierung des Motorencoders durch einen zweiten Encoder wird diese nicht benötigt.

Hinweis:
Bei der Überwachung des Antriebs mittels eines konventionellen Sin/Cos-Encoders finden sich in der Regel Anforderungen an den Aufbau des Encoders. Dadurch scheiden induktive Encoder in der Regel aus.

7.4. SE6-Produktvorteile gegenüber Antrieben mit Fail-Safe-Encodern

Lf.Nr.:	Schlagwort	Bemerkung
1	Freie Motorenauswahl	Nicht für alle Motoren sind passende Sin/Cos-Encoder erhältlich
2	Kein FMA-Encoder-Anbau	Preisvorteil und Vorteile beim Service
3	Freie Encoderwahl	Keine Einschränkungen bei Performance, Robustheit oder Wirtschaftlichkeit
4	-	-
5	-	-
6	-	-
7	Service-Konzept	SD-Karte tauschen und gut!
8	Wirtschaftlichkeit	Projektierung über DS6, wirtschaftlich attraktive Gesamtlösung
9	Sicheres Bremsenmanagemet	Fast ohne Wettbewerb am Markt
10	Sicherheitsniveau	SIL 3/PL e/ Kat. 4 für alle Sicherheitsfunktionen
11	Retrofit	Antriebsregler tauschen und gut!

Tabelle 9- Produktvorteile gegenüber Systemen mit Fail-Safe Encodern

7.5. SE6-Produktvorteile gegenüber klassischen Sin/Cos-Lösungen

Lf.Nr.:	Schlagwort	Bemerkung
1	Freie Motorenauswahl	Nicht für alle Motoren sind passende Sin/Cos-Encoder erhältlich
2	Kein FMA-Encoder-Anbau	Preisvorteil und Vorteile beim Service
3	Freie Encoderwahl	Keine Einschränkungen bei Performance, Robustheit oder Wirtschaftlichkeit
4	Einfache Encoderkabel	Preisvorteil: Es werden keine hochwertig geschirmten Kabel benötigt
5	Keine Sin/Cos-Adapter	Es werden keine Adapter zum Herausführen der Sin/Cos-Spuren für ein externes Überwachungsgerät benötigt
6	Reaktionszeit	Die Reaktion auf Grenzwertverletzungen erfolgt direkt im Antriebsregler innerhalb weniger Millisekunden; Laufzeiten externer Komponenten bis zum Abschalten des Antriebsreglers entfallen
7	Service-Konzept	SD-Karte tauschen und gut!
8	Wirtschaftlichkeit	Projektierung über DS6, wirtschaftlich attraktive Gesamtlösung
9	Sicheres Bremsenmanagemet	Fast ohne Wettbewerb am Markt
10	Sicherheitsniveau	SIL 3/PL e/ Kat. 4 für alle Sicherheitsfunktionen
11	Retrofit	Antriebsregler tauschen und gut!

Tabelle 10- Produktvorteile gegenüber klassischen Sin/Cos Lösungen

8. FAQ

Bei den Gesprächen mit unseren Kunden bekommen wir wiederkehrende Fragen gestellt, auf welche in diesem Kapitel eingegangen wird.

Hinweis:
Gerne nehmen wir Rückmeldungen zu „Häufig gestellten Fragen“ entgegen, um unsere Unterlagen zu verbessern.

8.1. Fragen zur Hardware

Warum benötigt das SE6-System keinen sicheren Encoder?

SD6 mit SE6 benötigt keinen sicheren Encoder, da der Motorencoder von SE6 plausibilisiert wird.

Warum benötigt das SE6-System keinen Fehlerausschluss beim Encoder-Anbau am Motor?

Die Encoder-Plausibilisierung erkennt auch Fehler im mechanischen Encoder-Anbau.

Warum erreicht das SE6-System für die Sicherheitsfunktionen SIL 3/PL e/Kategorie 4, während Marktbegleiter trotz sicherem Encoder nur SIL 2/PL d erreichen?

Durch die Encoder-Plausibilisierung entsteht ein durchgängiges zweikanaliges System im Bereich der Sensorik. Es gibt keine strukturellen Einschränkungen z. B. auf Basis von Fehlerausschlüssen.

8.2. Fragen zur Software

Warum kann man mit dem „nicht sicheren“ Scope der DS6 die Sicherheitsfunktionen der verifizieren?

Mit dem DS6-Scope wird eine Erwartungshaltung des Anwenders überprüft. Bei einer Fehlfunktion des Scopes würde die Erwartungshaltung nicht erfüllt werden.

8.3. Fragen zum Handling

Warum benötigt SE6 so lange (ca. 5 s), um von STO nach RUN zu wechseln?

Nach dem Deaktivieren des STO-Zustands von SE6 erfolgt ein Systemtest, bevor SE6 in den Betriebsmodus wechselt. Aufgrund dieser Systemtests sind beim Endkunden keine

zyklischen Funktionstests notwendig. SE6 wird vor jeder gefahrbringenden Funktion (Anrieb bewegt sich) getestet.

Wie kann ich die lange Systemdiagnose beim Deaktivieren von STO umgehen?

Müssen Bewegungen nur kurzfristig verhindert werden, kann alternativ zum SS1 auch die Sicherheitsfunktion SS2 genutzt werden. Wird diese dann wieder deaktiviert, gibt es keine nennenswerte Verzögerungszeit im System.

Wann benötigt man einen SS1?

Die DIN EN ISO 13850 beschreibt die Anforderungen bei Not-Halt. Dort werden lediglich SS1 und STO als mögliche Funktionen zum Stillsetzen beschrieben.

Wann benötigt man einen STO?

Die DIN EN ISO 13850 beschreibt die Anforderungen bei Not-Halt. Dort werden lediglich SS1 und STO als mögliche Funktionen zum Stillsetzen beschrieben.

Der STO kann zusätzlich als Basis für eine Wiedereinschaltsperre nach 14118 zum Schutz vor unerwartetem Anlauf benutzt werden.

Welche Vorteile bringt ein SS2?

Bei einem SS2 bleibt der Antriebsregler in Regelung und kann sofort nach Abwahl der Sicherheitsfunktion den Antrieb verfahren.

Insbesondere bei zentralen Bewegungssteuerungen kann die überlagerte Steuerung in Regelung bleiben und muss nicht neu referenziert werden.

STÖBER Antriebstechnik GmbH + Co. KG
Kieselbronner Straße 12
75177 Pforzheim
Deutschland
Tel. +49 7231 582-0
mail@stoeber.de
www.stober.com

24h Service Hotline
+49 7231 582-3000

STÖBER