# Anforderungen für Antriebe und die Auswirkung der europäischen Maschinenrichtlinie

Wenn Sicherheitsfunktionen gleich im Antrieb integriert sind, wirkt sich das unmittelbar auf die Kosten einer Anlage oder Maschine aus. Die Sicherheitsfunktion „*Safe-Torque-Off (STO)*“ ist häufig schon Standard. Weitere gebräuchliche Funktionen sind „*Safe-Operating-Stop*“ (SOS) und „*Safe-Stop*“(SS1/ SS2).

In den letzten Jahren hat es bedeutende Entwicklungen für Antriebsanwendungen innerhalb der Industrie gegeben. Diese Entwicklungen fordern mehr als je zuvor von Antrieben die Übernahme von sicherheitsrelevanten Funktionen. Dabei müssen Antriebe vor allem im Hinblick auf die Erfüllung der Norm EN 61800-5-2 bestimmten Anforderungen genügen.

Und so wirkt sich die Richtlinie 2006/42/EG auf Antriebe mit integrierten Sicherheits-funktionen aus: Gemäß den harmonisierten Sicherheitsstandards der europäischen Maschinenrichtlinie 2006/42/EG muss für die Realisierung von Sicherheitsfunktionen in Maschinenanwendungen immer die gesamte Sicherheitskette betrachtet werden.

Eine typische Sicherheitskette besteht aus Sensor, Logik und Aktorik. Eine Sicherheitskette kann somit aus einem Lichtgitter als Sensor, einer sicheren SPS als Logik und einem Antrieb mit integrierter Sicherheit als Aktorik (als Teil der Sicherheitsfunktion, welches zum Beispiel die gefährliche Bewegung eines Roboters verhindert) bestehen. Anstatt diese Sicherheits-funktionalität durch Verwendung elektromechanischer Komponenten zur Unterbrechung der Energieversorgung zum Motor zu realisieren, bieten immer mehr Antriebe diese Funktionalität als zertifizierte integrierte elektronische Lösung an. Diese elektronisch realisierte Abschaltung bietet selbstredend verschiedene Vorteile, wie kurze Reaktionszeiten, weniger Verschleiß durch Wegfall mechanischer Komponenten sowie kleinere Abmaße der Realisierung. Dies alles wirkt sich unmittelbar auf die Verfügbarkeit und die Kosten einer Anlage aus.

## Der Standard definiert die Anforderungen

Der harmonisierte anzuwendende Produktstandard für Antriebe mit integrierter Sicherheit ist die EN 61800-5-2. Dieser Standard definiert die Anforderungen der **F**unktionalen **S**icherheit für Antriebe und nennt die in der Industrie üblichen verwendeten Sicherheitsfunktionen. Die wichtigste und am häufigsten angewendete Sicherheitsfunktion ist „*Safe-Torque-Off (STO)“*. Bei dieser Sicherheitsfunktion wird der angeschlossene Motor momentenfrei geschaltet. Dies wird erreicht durch die sichere Abschaltung der PWM Signale, z.B. durch die sichere Unterbrechung der Energie zur Ansteuerung der Leistungsschalter, um den Motor momentenfrei zu schalten. Zu beachten: Hier wird der Motor momentenfrei geschaltet, so dass dieser aufgrund der Massenträgheit weiterlaufen und austrudeln kann. Im Falle, dass äußere Kräfte anliegen kann es sogar zu einer Beschleunigung kommen. Dies muss bei der Gefährdungsanalyse berücksichtigt werden und gegebenenfalls sind zusätzliche Maßnahmen erforderlich wie z.B. Bremsen.

Alle anderen in der EN 61800-5-2 beschriebenen Sicherheitsfunktionen, wie zum Beispiel

„*Safe-Stop-1(SS1)*“ und „*Safety-Limited-Speed (SLS)*“, nutzen letztendlich die Sicherheits-funktion STO als den sicheren Zustand. Entsprechend der EN 61800-5-2 muss bei Auftreten eines sicherheitsrelevanten Fehlers der sichere Zustand eingenommen werden. Dieser muss klar definiert werden und ist in der Regel der „STO“.

**Standard definiert Anforderungen für sichere Überwachungsfunktionen**

Des Weiteren definiert der Standard Anforderungen für sichere Überwachungsfunktionen, wie z.B. Überwachung der Geschwindigkeit, der Position usw.

Heutzutage sind die meisten Hersteller von Antrieben bestrebt, die Sicherheitsfunktion STO als Standard in ihren Antrieben zu integrieren. Diese Sicherheitsfunktion wird gewöhnlich mittels diskreter Hardware ohne Involvierung von Software realisiert. Wenn erforderlich, wird der nicht sicherheitsrelevante Drive-Controller lediglich zur Diagnose der Hardware verwendet. Für die Sicherheitsfunktion „*Safe Operating Stop (SOS)*“ ist es erforderlich, ein spezifiziertes Positionsfenster während des Stillstandes zu überwachen. Jedoch wird im Falle eines Fehlers während der SOS Funktion, z.B. Verlassen des spezifizierten Positionsfensters, der sichere Zustand STO in Kombination mit einer Bremse eingenommen, um die Last im zulässigen Positionsfenster zu halten. Die Funktion STO ist hierbei die sichere Fehlerreaktion der SOS Funktion. Somit ist die Funktion STO eine der Voraussetzungen für die Realisierung dieser Funktion.

**SIL 2/PL reicht oft aus**

Es wird empfohlen, die STO Funktion für den höchsten Sicherheitsintegritätslevel 3 (SIL 3) entsprechend EN 62061 und Performance Level e (PL e) entsprechend EN ISO 13849-1 auszulegen, da diese Funktion von allen anderen Sicherheitsfunktionen im Fehlerfall angefordert wird um den sicheren Zustand einzunehmen. Darüber hinaus nutzen diverse Sicherheitsfunktionen, wie sichere Stopfunktionen und sichere Überwachungsfunktionen, die STO Funktion als sicheren Zustand und die Sicherheitsintegrität dieser Funktionen ist somit abhängig von der Sicherheitsintegrität der STO Funktion. Man kann somit die Sicherheitsfunktion STO auch als Flaschenhals der Sicherheitskette bezeichnen. Für die meisten Anwendungen mit sicheren Überwachungsfunktionen ist jedoch in der Regel SIL2/PLd ausreichend.

Andere wichtige Sicherheitsfunktionen für Antriebe sind „*Safe-Stop-1 (SS1)*“ und „*Safe-Stop-2 (SS2)*“. Für SS1 und auch SS2 hat die EN 61800-5-2 drei verschiedene Varianten definiert. Die am häufigsten verwendete Variante basiert auf eine feste vordefinierte Zeitverzögerung für die Einnahme der Sicherheitsfunktion STO oder SOS.

**Überwachungsfunktionen für Geschwindigkeit und Position**

Für die Realisierung der sicheren Überwachungsfunktionen für Geschwindigkeit und Position müssen zusätzlich die erforderlichen Geber zur Erfassung berücksichtig werden.

Die eingesetzten Geber müssen denselben Sicherheitsintegritätslevel und/ oder Performance Level erfüllen wie die sichere Überwachungsfunktion selbst, da der Geber ein Teil der Sicherheitskette ist. Aus diesem Grund streben immer mehr Hersteller von Gebern die Zertifizierung ihrer Geber nach SIL 2 oder SIL 3 an.

Die EN 61800-5-2 listet eine Anzahl von sicheren Überwachungsfunktionen auf, für die es in der Industrie eine häufige Anwendung gibt. Die Liste der Norm ist nicht vollständig. Sicherheitsfunktionen, welche in der Industrie benötigt werden und hier nicht gelistet sind, können vom Anwender selbst spezifiziert werden. Wichtig für jede selbstspezifizierte Sicherheitsfunktion ist es, dass die Eigenschaften eindeutig beschrieben werden und der sichere Zustand bei Anforderung und im Fehlerfall eindeutig definiert ist.

**Sicherheit beim Einrichten von Robotern**

Eine häufig verwendete Sicherheitsfunktion in der Industrie ist die *„Safely-limited speed (SLS)“*. Diese Sicherheitsfunktion wird häufig für den „Einrichtbetrieb“ bei Robotern verwendet. Die Eigenschaft dieser Sicherheitsfunktion ist die Überwachung der Geschwindigkeit hinsichtlich der Nichtüberschreitung einer spezifizierten oberen Grenze. Die Realisierung dieser Sicherheitsfunktion erfolgt in der Regel durch eine parametrierbare integrierte sichere Überwachungsfunktion in Kombination mit einen oder zwei sicheren Gebern zur Geschwindigkeitserfassung. Im Fehlerfall wird entweder die Sicherheitsfunktion SOS oder STO ausgeführt, um den sicheren Zustand herbeizuführen.

Weitere in der EN 61800-5-2 genannte verwendete Sicherheitsfunktionen sind unter anderem:

- SLP (Safely-Limited-Position),
- SLI (Safely-Limited-Increment),
- SDI (Safe-Direction),
- SBC (Safe-Brake-Control)
- SSM (Safe-Speed-Monitoring).

Um die Konformität zur Maschinenrichtlinie sicher zu stellen, müssen neben dem Produktstandard auch die harmonisierten Standards für die Maschinensicherheit EN ISO 13849-1 und/ oder EN 62061 sowie EN 60204-1 und weitere in Abhängigkeit der Anwendung berücksichtigt werden. Neben der Benennung von Sicherheitsfunktionen werden in der EN 61800-5-2 auch Aspekte der systematischen Integrität z.B. die Anwendung von Maßnahmen zur Fehlervermeidung und Aspekte der Sicherheitsintegrität wie z. B. die Berücksichtigung von Maßnahmen zur Erkennung und Kontrollierung von gefährlichen Fehlern genannt.

Für die Erreichung der erforderlichen systematischen Integrität definiert die EN 61800-5-2 Anforderungen zum Management der Funktionalen Sicherheit, für die Beurteilung der Funktionalen Sicherheit, sowie an die Dokumentation bezüglich aller Lebenszyklusphasen einer Produktentwicklung. Systematische Fehler, die während der Entwicklung übersehen werden, können die Konsequenzen von kostspieligen Änderungen sowie einer verspäteten Markteinführung nach sich ziehen. Daher ist eine detaillierte Dokumentation jeder Entwicklungsphase erforderlich, um eine Reproduzierbarkeit des Entwicklungsprozesses zu erreichen. Maßnahmen zur Vermeidung von Fehlern müssen während jeder Lebens-zyklusphase angewendet werden. Die anzuwendenden Maßnahmen sind abhängig vom angestrebten Sicherheitsintegritätslevel.

**Prooftest erkennt Ausfälle**

Des Weiteren fordert die EN 61800-5-2 die Bestimmung der gefährlichen Versagensrate pro Stunde (PFH). Der erforderliche Wert für die PFH hängt wiederum vom angestrebten Sicherheitsintegritätslevel ab und muss für die gesamte Sicherheitsfunktion eingehalten werden. Aufgrund der Tatsache, dass die integrierte Sicherheitsfunktion im Antrieb nur ein Teil der Sicherheitskette darstellt, sollte der PFH Wert ausreichend kleiner sein als der durch Sicherheitsintegritätslevel definierte Wert.

Die PFH ist hauptsächlich abhängig von der gewählten Hardwarearchitektur, der abgeschätzten Ausfallrate, die Anfälligkeit bezüglich Fehler gemeinsamer Ursache sowie dem Diagnosedeckungsgrad der implementierten Tests zur Fehlererkennung. Auch das gewählte Intervall für den „Prooftest“, der unternommen werden muss, um Fehler zu erkennen, welche nicht durch die interne Diagnose erkannt werden, hat einen beträchtlichen Einfluss

auf die PFH. Der Prooftest dient der Erkennung von Ausfällen, welche nicht durch die interne Diagnose erkannt werden. Diese Ausfälle gehen direkt in die PFH ein. Da die Durchführung eines Prooftests für programmierbare elektronische Komponenten sich durchaus schwierig gestalten kann, wird empfohlen, ein Prooftestinterval von 20 Jahren anzustreben, so dass innerhalb der Lebenszeit (Missiontime) des Produktes kein Prooftest erforderlich ist.

Ferner muss in Abhängigkeit der beabsichtigten Anwendung entsprechend EN 61800-5-2 die integrierte Sicherheitstechnik mit erhöhten EMV -Prüfschärfegraden getestet werden. Erhöhte Prüfschärfegrade sind bereits in der neuen Ausgabe der IEC 61800-5-2 normativ genannt und werden in die zukünftigen Ausgaben der EN 61800-5-2 übernommen werden.

---

Dieser Beitrag wurde uns freundlicherweise von Herrn Dipl.-Ing. Thomas Steffens zur Verfügung gestellt. Herr Steffens ist Geschäftsfeldleiter für den Bereich Functional Safety and Security beim TÜV Rheinland Industrie Service und ist Mitglied des Arbeitskreises AK 226.0.3 "Sicherheitsgerichtete Funktionen elektrischer Antriebssysteme in Maschinen".

Wir bedanken uns bei Herrn Steffens und dem TÜV Rheinland für die freundliche Unterstützung.