Kayser K.H. **Germany**
Esslingen

Hochschule Esslingen

INTEGRATION SICHERER ANTRIEBSFUNKTIONEN NACH NORM IEC 62061

Die Sicherheit technischer Systeme und Anlagen bezüglich der Gefährdung von Personen und Umwelt, war in der Vergangenheit geprägt durch eine Vielzahl branchenspezifischer und firmeneigener Standards sowie durch nationale Gesetze und Normen. 1998 wurde erstmals die internationale Sicherheits-Norm IEC 61508 mit dem Titel: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme veröffentlicht [1]. Aus dieser Grundnorm sind zwischenzeitlich eine Vielzahl internationaler, anwendungsspezifischer Normen entstanden bzw. befinden sich derzeit in der Entstehung. Zum Beispiel: IEC 61511: Prozessindustrie; EN 50128: Bahnanwendungen, Signaltechnik; IEC 62061: Sicherheit von Maschinen; IEC 60601-1: Medizinische elektrische Geräte; ISO 26262: Fahrzeugtechnik.

Der Geltungsbereich der Norm erstreckt sich über Konzept, Planung, Entwicklung, Realisierung, Inbetriebnahme, Instandhaltung, Modifikation bis hin zur Außerbetriebnahme und Deinstallation sowohl des gefahrverursachenden Systems als auch der sicherheitsbezogenen (risikomindernden) Systeme. Die Norm beschreibt Methoden und Verfahren zur Beherrschung systematischer und zufälliger Fehler. Die Anforderungen an die Sicherheitsintegrität ist abhängig vom Gefahrenrisiko des jeweiligen technischen Systems, und wird gemäß [1] in die "Safety Integrity Level" SIL1 (niedrig)…SIL4 (hoch) unterteilt. Anmerkung: Für Maschinen und Anlagen mit einem Risiko bleibender Verletzungen oder dem Tod einzelner Personen ist i.A. ein SIL3 erforderlich. Systematische Fehler werden in allen Produktlebensphasen durch entsprechende Vorgehensmodelle beherrscht.

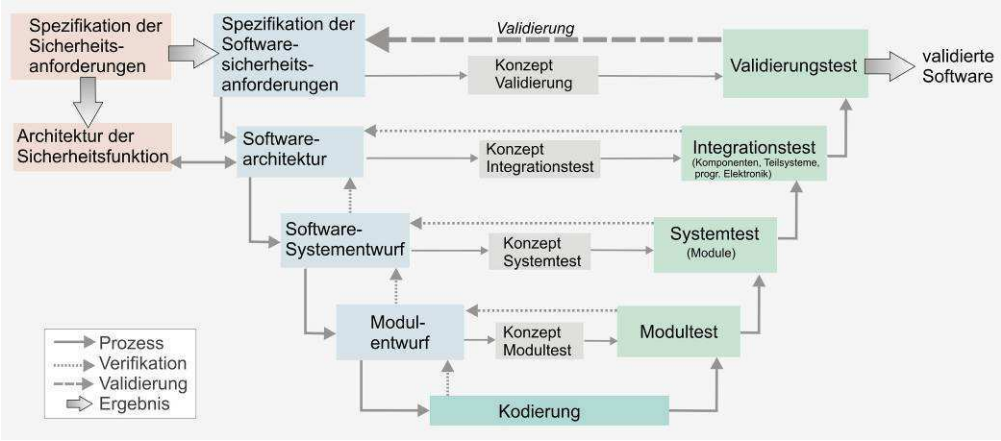


Abb. 1: IEC 61508 Vorgehensmodell am Beispiel Software-Entwicklung [1]

Probabilistische Methoden kommen zur Anwendung um das Risiko zufälliger Fehler abzuschätzen. Je nach gefordertem SIL sind Grenzwerte probabilistischer Kenngrößen wie: ***SFF*** - Safe Failure Fraction und $\boldsymbol{PF_D}$ - Probabilty of dangereous Failure, einzuhalten. Diese bestimmen sich wiederum aus den Fehlerraten $\boldsymbol{\lambda}$ ***[1/h], [FIT=10-9/h]*** des Systems und ***DC*** - Diagnostic Coverage. Fehlerraten von Komponenten bzw. Systemen werden unterteilt in: Sichere (Safe) Fehler $\boldsymbol{\lambda_S}$; Gefährliche Fehler (Dangereous) $\boldsymbol{\lambda_D}$; bei vorhandenen Diagnoseeinrichtungen können Fehler ggf. rechtzeitig entdeckt und gefährliche Situationen abgewendet werden; $\boldsymbol{\lambda_D}$ kann deshalb weiter unterteilt werden in Gefährliche unentdeckte Fehler (Dangereous Undetected) $\boldsymbol{\lambda_{DU}}$ und Gefährliche entdeckte Fehler (Dangereous Detected) $\boldsymbol{\lambda_{DD}}$. Ausgangsbasis zur Bestimmung von System- oder Gerätefehlerraten sind etablierte Datenbestände zu den Ausfallraten von Komponenten wie z.B. [2]. Zwischen den genannten Größen bestehen folgende Zusammenhänge:

$$\lambda = \lambda_S + \lambda_D = \lambda_S + \lambda_{DD} + \lambda_{DU} \qquad PF_D(t) = 1 - e^{-\lambda_{DU} t} \qquad SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_{DD} + \sum \lambda_{DU}} \qquad DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{DD} + \sum \lambda_{DU}} = \frac{\sum \lambda_{DD}}{\sum \lambda_D}$$

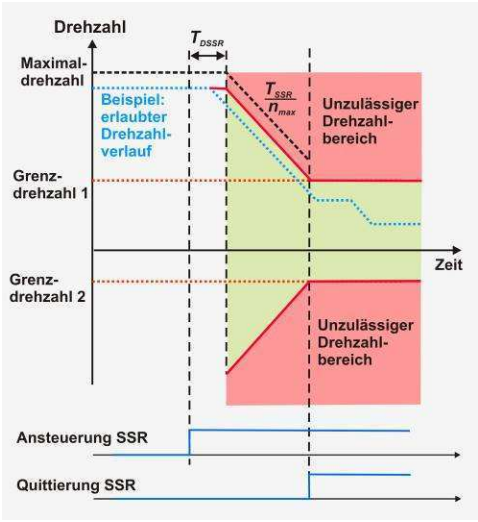
Diese Grenzwerte können ihrerseits durch Systemarchitekturmerkmale wie Ein- oder Mehrkanaligkeit (HFT-Hardware Fault Tolerance HFT=0 - Ein-kanalig; HFT=1 Zwei-kanalig), durch den Einsatz von Diagnosetechniken (Diagnostic Coverage DC) und ggf. durch die Wahl und Festlegung von Wartungsintervallen beeinflusst werden. Zur Berechnung der Kenngrößen SFF und PFD kommen je nach Komplexität unterschiedliche Methoden wie z.B. FMEDA-Failure Mode Effect an Diagnostic Analysis (FMEDA) ; FTA – Fehlerbaumanalyse, Fault Tree Analysis oder Markov-Modellierung zum Einsatz.

Aus industrieller Sichtweise hat die Norm u.a. folgende Vorteile:

- Durch den Einsatz von Mikroprozessor und Software für sichere Funktionen können diese kostengünstiger umgesetzt werden, und es können neue, komplexere Sicherheitsfunktionen realisiert werden.
- Die internationale Akzeptanz der Norm erleichtert die Erschließung internationaler Märkte.

Elektrische und elektronisch geregelte Servo-Antriebssysteme sind in Anwendungen bei Maschinen, Fertigungseinrichtungen, Werkzeugmaschinen, Robotern etc. seit jeher Bestandteil sicherheitstechnischer Betrachtungen. Die Sicherheit dieser Geräte konnte in der Vergangenheit nur durch aufwändige, kostenintensive und zusätzliche Überwachungsschaltungen gewährleistet werden. Mit der Grundnorm IEC 61508 und der anwendungsspezifischen Norm IEC 62061 ist es für die Hersteller dieser Geräte möglich, sichere Funktionen direkt in das Antriebssystem zu integrieren. So sind in jüngster Vergangenheit von Herstellern von Servo-Antriebssystemen unter dem Stichwort: „Safety Integrated“ [3], etablierte, aber auch neuartige Sicherheitsfunktionen in die Servo-Antriebssysteme integriert worden. Beispiele für sichere Antriebsfunktionen sind [4,5,6]:

Sicher abgeschaltetes Moment; safe torque off	**STO**	Sicherer Betriebshalt; safe operation stop	**SOS**
Sicherer Stopp 1; safe stop 1	**SS1**	Sicher begrenzte Geschwindigkeit; safely-limited speed	**SLS**
Sicherer Stopp 2; safe stop 2	**SS2**	Sicherer Geschwindigkeitsbereich; safe speed range	**SSR**
		Sichere Bewegungsrichtung; safe direction	**SDI**



Beispiel: Sichere Antriebsfunktion SSR

Bei Vorgabe des Ansteuersignals SSR von einer sicheren Steuerung über z.B. einen sicheren Feldbus, leitet der Antrieb die SSR-Funktion (Sicherer Geschwindigkeits-bereich) ein. Die Funktion SSR überwacht, dass die Istdrehzahl die eingestellten Grenzen nicht überschreitet. Nach Ablauf der parametrierbaren Zeit T_{DSSR} Überwacht der Antrieb den Verlauf der Bremsrampe, die durch den Parameter T_{SSR} und der maximal möglichen Drehzahl (Geschwindigkeit) n_{max} bestimmt wird. Nach dem Erreichen des Drehzahlbereichs wird die Einhaltung des Drehzahlbereichs überwacht. Wird der Bereich verlassen, wird in eine Stoppfunktion gewechselt z.B. STO. Es ist dabei parametrierbar, ob bei einer Verletzung der Grenzen die Stoppfunktion STO, SS1 oder SS2 eingenommen wird.

Abb. 2: Beispiel für sichere Antriebsfunktion: „Sicherer Geschwindigkeitsbereich“ [4,5,6]

Obwohl in den Anhängen der Norm auf viele technisch, praktische Aspekte eingegangen wird, stellt sie in keinster Weise eine „Standard-Bauanleitung“ für sicherheitsrelevante Systeme dar. Dies gibt den Entwicklern genügend Freiräume zur innovativen und wettbewerbsfähigen Produktumsetzung. Im nachfolgenden Bild ist beispielhaft eine geeignete Systemarchitektur für die Integration sicherer Funktionen in einen elektronisch geregelten Antrieb skizziert.

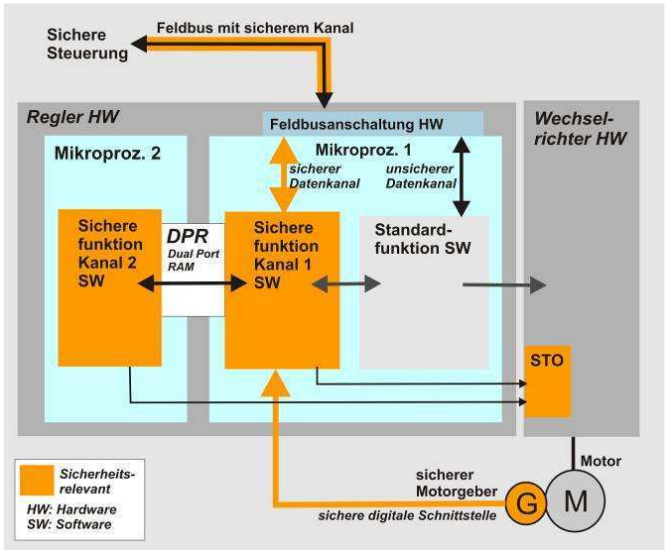


Abb. 3: Beispiel Systemarchitektur für sichere Antriebsfunktionen

Literatur:

[1] DIN EN61508-1…7: Funktionale Sicherheit sicherheitsbezogener elektrischer / elektronischer / programmierbarere elektronischer Systeme – Teil 1…7. VDE Verlag Berlin und Beuth Verlag Berlin.

[2] Siemens Norm SN 29500-1…14: Ausfallraten Bauelemente – Erwartungswerte. Siemens AG.

[3] Fehlersichere Steuerungen – SIMATIC Safety Integrated for Factory Automation – Funktionsbeispiel: AS-FE-I-013-V11-DE. Siemens AG 2007.

[4] Sichere Bewegungssteuerung / Safe Motion: Fa. Pilz GmbH & Co.KG 2008.

[5] Stefan Staudt: Funktionale Sicherheit nach IEC61800-5-2 und ISO 13849 im Antriebsbereich. Tagungsband 8. AALE Fachkonferenz 2011, S.67, München, Oldenbourg Industrieverlag GmbH 2011.

[6] IEC 61800-5-2: Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl. Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit. VDE Verlag Berlin und Beuth Verlag Berlin.