

IEC 61508 Funktionale Sicherheit

Sicherheitsnormen

Im Bereich der Sicherheitstechnik setzt sich international die IEC 61508 durch. Auch im Vergleich zu den weit verbreiteten TÜV Anforderungsklassen (TÜV AK) bietet sie den Vorteil der internationalen Akzeptanz. Sie ermöglicht eine weltweite Harmonisierung von Sicherheitsinstrumentierung und erlaubt so eine deutliche Kostenreduktion. Käufer und Behörden betrachten sie als Referenz zur Beurteilung von Systemen.

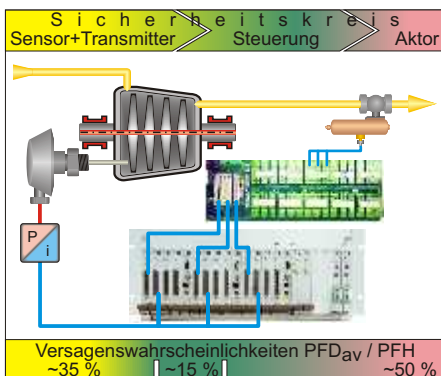
IEC 61508 Grundlagen

Die Aufgabe von Sicherheitsfunktionen (safety functions) ist es, das Risiko von Anlagen mit großem Gefahrenpotenzial für Menschen, Umwelt und Sachwerte zu minimieren. Die Normen IEC 61508/IEC 61511 definieren vier Sicherheitsstufen, SIL 1 bis SIL 4 (safety integrity level), die die Maßnahmen zur Risikoreduzierung auf ein vertretbares Niveau beschreiben.

Die IEC 61508 beschreibt sowohl die Art der Risikoabschätzung als auch die Anforderungen an Komponenten und Systeme für Sicherheitsfunktionen. Die IEC 61511 legt die Auswahlkriterien für Komponenten der Sicherheitsfunktionen fest, die u. a. auch die Betriebsbewährungen von Sensoren und Aktoren beinhaltet.

Die IEC 61508 gilt für alle Anwendungen, in denen elektrische, elektronische oder programmierbare elektronische sicherheitsgerichtete Systeme (PES Systeme) zur Ausführung von Sicherheitsfunktionen eingesetzt werden.

Bewertet wird bei der IEC 61508 immer der ganze Sicherheitskreis, vom Sensor und Transmitter über die Steuerung bis zum Aktor.



Vor der Auslegung der Sicherheitskreise steht dabei die Risikoabschätzung. Besonders wahrscheinliche oder gefährliche Störungen erfordern eine höhere Sicherheit der Steuerung.

Die Gesamtklassifizierung des Systems ergibt sich dabei nicht automatisch aus der SIL-Einstufung der einzelnen Komponenten, sondern muß gemäß der Berechnungsformeln neu berechnet werden.

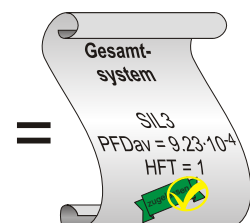
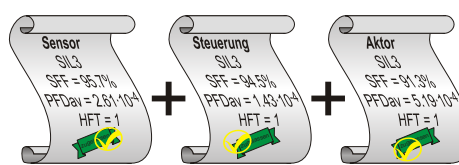
Wichtige Beurteilungskriterien sind ausserdem die Fehlertoleranz der Hardware (HFT = Hardware Fault Tolerance) und der Anteil ungefährlicher Ausfälle (SFF = Safe Fail Fraction). Eine HFT=0 bedeutet keinerlei Redundanz. Jeder Fehler verursacht ein Versagen der Steuerung, eventuell mit gefährlichen Folgen. Bei redundanten (HFT=1) oder dreifach redundanten (HFT=2) Systemen können einzelne Fehler ausgeglichen werden und verursachen so keinen Fehler der Steuerung.

Wenn es zum Fehler der Steuerung kommt ermöglicht die SFF eine Risikoabschätzung. Je höher der Wert ist, desto wahrscheinlicher ist im Fehlerfall ein sicheres Verhalten, das heißt eine Abschaltung. Um ein SIL 3 Gesamtsystem zu erhalten müssen die SFF und HFT Bewertungen der Einzelkomponenten den SIL 3 Anforderungen genügen. Zusätzlich muß die Ausfallwahrscheinlichkeit (PFDav oder PFH) des Gesamtsystems SIL 3 erfüllen.

Beispiel

Ein Gesamtsystem bestehend aus einem Sensor, der Steuerung und einem Aktor, alle mit vorliegender SIL 3 Zertifizierung, soll eine sicherheitskritische

SFF	HFT		
	0	1	2
< 60%	---	SIL 1	SIL 2
60-90%	SIL 1	SIL 2	SIL 3
90-99%	SIL 2	SIL 3	SIL 4
>99%	SIL 3	SIL 4	SIL 4



Risikoabschätzung nach IEC 61508

	S1	S2		S3		S4		
		A1	A2	A1	A2			
		G1	G2	G1	G2			
—	SIL 1	SIL 1	SIL 2	SIL 3	SIL 3	SIL 4	SIL 4	W3
—	—	SIL 1	SIL 1	SIL 2	SIL 3	SIL 3	SIL 4	W2
—	—	—	SIL 1	SIL 1	SIL 2	SIL 3	SIL 3	W1

Schadensausmaß

- S1: leichte Verletzung einer Person; kleinere schädliche Umwelteinflüsse
- S2: schwere irreversible Verletzung einer oder mehrerer Personen oder Tod einer Person; vorübergehende größere schädliche Umwelteinflüsse
- S3: Tod mehrerer Personen; langandauernde größere schädliche Umwelteinflüsse
- S4: katastrophale Auswirkungen, sehr viele Tote

Aufenthaltsdauer von Personen

- A1: selten bis öfter
- A2: häufig bis dauernd

Eintrittswahrscheinlichkeit

- W1: sehr gering
- W2: gering
- W3: relativ hoch

Gefahrenabwendung

- G1: möglich unter bestimmten Bedingungen
- G2: kaum möglich

Die Versagenswahrscheinlichkeiten (PFDav = Probability of dangerous Failure on Demand, average or PFH = Probability of dangerous Failure per Hour) aller Komponenten müssen beispielsweise addiert und entsprechend neu bewertet werden. Die SIL-Einstufung des Gesamtsystems erfolgt aufgrund der Gesamtausfallwahrscheinlichkeit anhand der PFDav / PFH Tabelle.

SIL	PFDav	PFH
1	$\geq 10^{-2} \dots < 10^{-1}$	$\geq 10^{-6} \dots < 10^{-5}$
2	$\geq 10^{-3} \dots < 10^{-2}$	$\geq 10^{-7} \dots < 10^{-6}$
3	$\geq 10^{-4} \dots < 10^{-3}$	$\geq 10^{-8} \dots < 10^{-7}$
4	$\geq 10^{-5} \dots < 10^{-4}$	$\geq 10^{-9} \dots < 10^{-8}$

Steuerung mit SIL 3 Anforderung ausführen.

Da die Einzelkomponenten für SIL 3 geeignet sind muss noch kontrolliert werden ob die Ausfallwahrscheinlichkeit des Gesamtsystems für SIL 3 akzeptabel ist.

Die Berechnung ergibt:

$$PFD_{av,gesamt} = \sum PFD_{av} = (2,61 + 1,43 + 5,19) \cdot 10^{-4} = 9,23 \cdot 10^{-4}$$

Der Wert liegt im Bereich zwischen 10^{-4} und 10^{-3} , erfüllt also die Anforderung für SIL 3.

IEC 61508 bei Gebhardt automation

Um die für SIL 3 erforderlichen hohen Sicherheitsanforderungen zu erfüllen, werden unterschiedliche Maßnahmen kombiniert. Neben einer geringen Ausfallwahrscheinlichkeit der Baugruppen wird durch eine Vielzahl so genannter Build in Tests eine hohe Fehleraufdeckung erreicht. Diese Selbsttests werden auf den intelligenten E/A-Karten zyklisch durchgeführt.

Weitere signifikante Massnahmen:

- Einsatz von redundanter Signalerfassung, auch auf SIMPLEX Systemen. Damit kann ein fehlerhaftes Einlesen der Eingangssignale erkannt (SIMPLEX, DUPLEX) oder auch korrigiert (TMR) werden.
- Digitaleingänge werden analog eingelesen. Damit können neben den Signalzuständen High / Low eindeutig auch die Fehler Kabelbruch / Kurzschluß erkannt werden.
- Redundante Digitalausgänge auch in SIMPLEX-Systemen.
- Rücklesbarkeit der Digitalausgänge, kombiniert mit einem zweiten, unabhängigen Abschaltweg der Stromversorgung der Ausgänge.
- Externe, im Betrieb testbare Hardware-Voter für Digitalausgänge.

- Redundante Steuerungsprogramme direkt auf der digitalen Ausgangskarte, auch im SIMPLEX-System.
- Trennung in Sicherheitskern und nicht sichere Komponenten. Dies erlaubt die kostengünstige Kombination von sicherem SIL 3 Maschinenschutz und normalen Steuerungsfunktionen rückwirkungsfrei in einem System.
- Einsatz qualitativ hochwertiger Bauteile mit sehr hoher MTBF
- Sicherheitskonzept für interne Kommunikation und Datenbuskommunikation.
- umfangreiche Selbsttests der Hard- und Software.

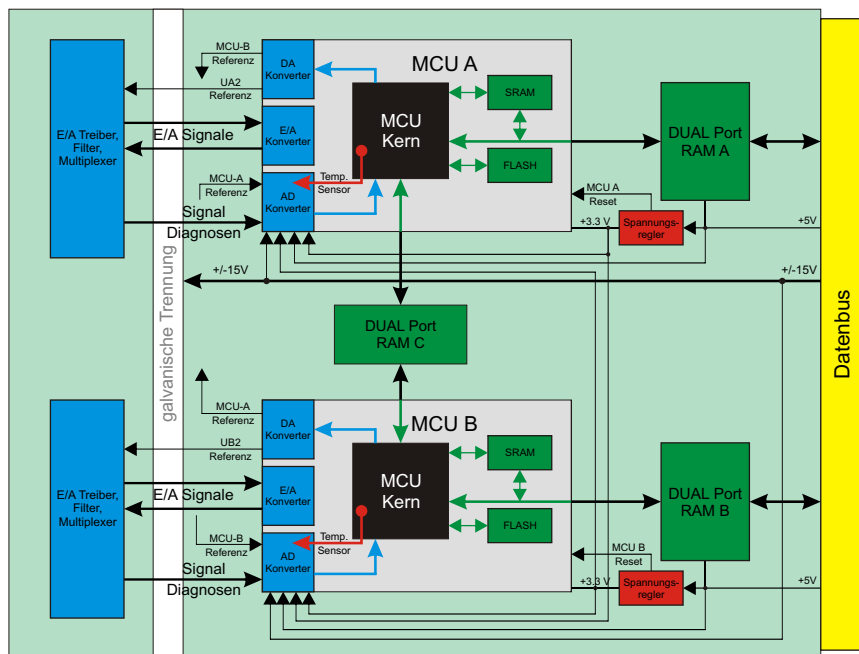
Einschalttests

Grundlegende Tests der Hardware erfolgen beim Einschalten der Karte. Die Power-On Selbst-Tests (POST) kontrollieren die gesamte Funktionalität der Karte und werden von beiden redundanten MCUs nach dem Einschalten durchgeführt:

Beispiele:

- Funktionalität der Mikrocontroller
- interner Analog-zu-Digital Konverter
- FLASH- und SRAM-Speicher
- Versorgungsspannung und Temperatur
- Prüfsummenvergleich von Firmware und Anwendungssoftware.

Erst nachdem alle Tests von beiden MCUs erfolgreich durchgeführt und gegenseitig kontrolliert wurden meldet sich die Karte im System als funktionsfähig an.



Sichere Kommunikation

Die MCU-Karten verwenden nur gesicherte Kommunikation. Sowohl für die interne Kommunikation zwischen den beiden MCUs auf einer Karte als auch für die externe Kommunikation der Karten untereinander werden alle Daten über Sicherheitspakete ausgetauscht. Dabei überprüft der Empfänger der Daten anhand von Prüfsummen alle empfangenen Pakete. Bei Fehlern kann entsprechend reagiert werden.

Zyklische Basistests

Im laufenden Betrieb werden von jeder MCU im Hintergrund Funktionstests durchgeführt. Diese Tests führen bei evtl. Fehlern auf unterschiedliche Fehlerreaktionen (Deaktivierung der Karte oder einzelner Kanäle etc.). Der Status der Tests kann jeder Zeit abgefragt und angezeigt werden. Ausserdem wird auf den Karten eine Fehlertest-Statistik geführt und im FLASH-Speicher hinterlegt:

Beispiele von Basistests:

- Online-Test SRAM- und FLASH-Speichertests
- Überwachung aller internen Spannungen und Temperaturen
- Gegenseitige Überwachung des internen AD-Konverters mittels Rampensignalen.
- Gegenseitige Programmablaufkontrolle
- Gegenseitige Fenster-Watchdogfunktionen
- Gegenseitige Erwartungswertkontrolle für Kommunikation

Zyklische Signaltests

Die analogen und digitalen Eingangssignale der Karten werden analog erfasst. Um die Qualität der Signalerfassung zu kontrollieren werden die AD-Wandler dabei mittels Referenzsignale bzw. Funktionen getestet. Diese Referenzsignale werden zyklisch eingangsseitig über Mikroschalter auf den zu testenden Signaleingang aufgeschaltet und der gewandelte Wert mit einem Erwartungswert verglichen.

Eingangs- und ausgangsseitig werden eine Vielzahl von Tests durchgeführt:

- Walking-Zero Test
- Rampentest
- NAMUR-Beschaltung für Kabelbruch und Kurzschlusserkennung.
- Digitalausgänge werden bis zum Ausgang des Sicherheitsrelais analog zurückgelesen und auf Signalabweichung kontrolliert.