Funktionale Sicherheit: Sicherheitsrelevante Temperaturmessung nach IEC 61508

WIKA Datenblatt IN 00.19

Einführung

Elektrische Thermometer können unter bestimmten Voraussetzungen in einem sicherheitsbezogenen System nach IEC 61508 eingesetzt werden. Für die Bewertung des sicherheitsbezogenen Systems sind insbesondere die Ausführung des elektrischen Thermometers als Widerstandsthermometer oder als Thermoelement sowie die technischen Eigenschaften des verwendeten Temperatur-Transmitters zu berücksichtigen.

Diese technische Information beschreibt die Grundlagen der Funktionalen Sicherheit nach IEC 61508 und gibt Hinweise zur sicherheitstechnischen Auslegung einer Temperaturmessstelle.

Notwendigkeit der Risikoreduzierung

Aufgrund steigender gesellschaftlicher Erwartungen an die Sicherheit von technischen Anlagen, sind die von technischen Systemen ausgehenden Risiken im Laufe der Zeit immer weiter reduziert worden. Es sind Normen und Richtlinien entstanden, die dem Anlagenbetreiber helfen, seine Anlage auf höchstem Sicherheitsniveau zu betreiben. Grundlage hierfür ist die Durchführung von Störfallanalysen und Risikobetrachtungen. Ziel ist es, das von einem technischen System ausgehende Risiko durch Sicherheitsmaßnahmen auf ein nach gesellschaftlichen Wertvorstellungen akzeptierbares Risiko zu reduzieren.

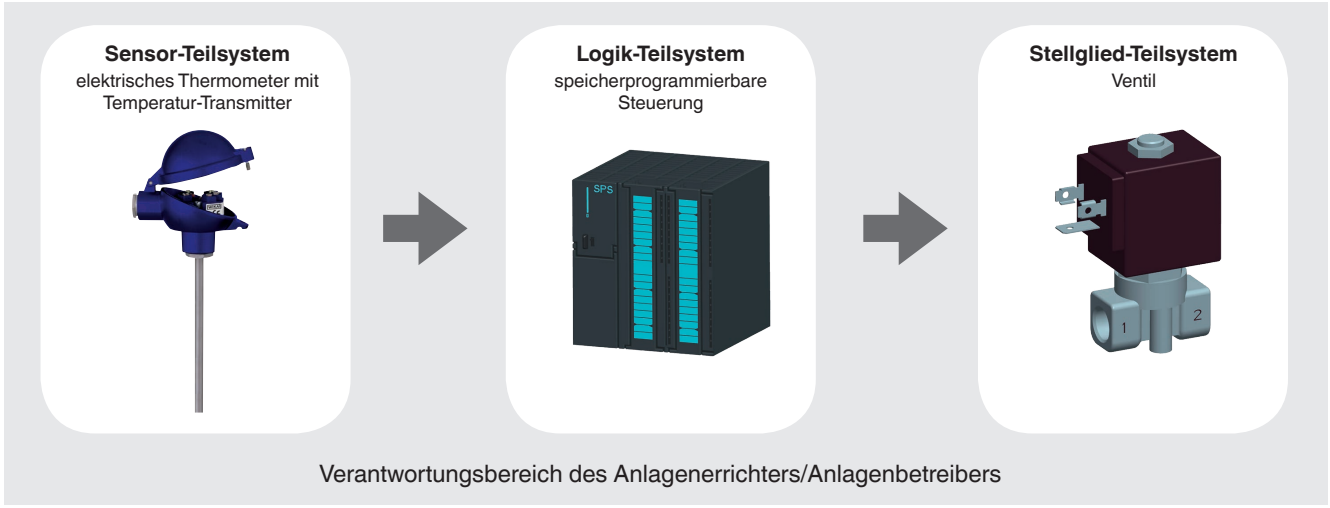
Zur Vermeidung eines gefahrbringenden Ausfalls einer Anlage kommen elektrische/elektronische/programmierbare elektronische Systeme (E/E/PE-Systeme) zum Einsatz. Die Gesamtheit aller erforderlichen Sicherheitsfunktionen, die zur Aufrechterhaltung des sicheren Zustandes einer Anlage dienen, wird als sicherheitstechnisches System SIS (Safety Instrumented System) oder sicherheitsbezogenes System bezeichnet.

Ein Beispiel für ein solches Sicherheitssystem ist eine Temperaturüberwachung, die bei Überschreiten der Temperaturgrenzwerte zuverlässig die Energiezufuhr einer Anlage abschaltet, diese in den sicheren Zustand versetzt und somit ein gefahrbringendes Ereignis verhindert.

Architektur eines sicherheitsbezogenen Systems

Ein elektrisches/elektronisches/programmierbar elektronisches System besteht grundsätzlich aus den Elementen Sensor, Steuerung und Aktor. In diesem Fall spricht man von einer einkanaligen Architektur des Sicherheitssystems (1oo1-System). Die Architektur beschreibt die spezifische Konfiguration von Hardware- und Softwareelementen in einem System. Ein 1oo1-System (1 out of 1) besteht aus einem Kanal, welcher sicher arbeiten muss, damit die Sicherheitsfunktion ausgeführt werden kann. Bei Sicherheitssystemen mit mehrkanaliger Architektur werden Hardware- oder Softwareelemente redundant ausgeführt (siehe „Redundante Systeme“).

Beispiel einer einkanaligen Architektur eines sicherheitstechnischen Systems



Ein elektrisches Thermometer mit Temperatur-Transmitter Typen T32.1S (Kopfversion) und T32.3S (Schienenversion) kann vom Anlagenbetreiber als Sensor-Teilsystem eines sicherheitstechnischen Systems verwendet werden.

Temperatur-Transmitter, Typ T32.xS

Normative Grundlagen

Die Normenreihe IEC 61508 „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbare elektronischer Systeme“ wird als Sicherheitsgrundnorm bezeichnet. Sie beschreibt Maßnahmen zur Vermeidung und Beherrschung von Fehlern in Geräten und Anlagen und ist unabhängig vom Industriebereich anwendbar.

Die IEC 61508 ist insbesondere dann anzuwenden, wenn
- die Sicherheitsfunktion durch ein E/E/PE-System ausgeführt wird
- ein Ausfall des sicherheitstechnischen Systems zur Gefahr für Mensch und Umwelt führt
- keine anwendungsbezogene Norm zur Auslegung von Sicherheitssystemen existiert

Die IEC 61508 stellt den Stand der Technik in Bezug auf die Auslegung von sicherheitstechnischen Systemen dar. Bei der Auslegung von Sicherheitssystemen ist der Stand der Technik und somit die IEC 61508 unbedingt zu berücksichtigen.

Für Planer, Errichter und Betreiber des Sicherheitssystems gibt es auch anwendungsspezifische Normen. Diese sind beispielsweise die IEC 61511 „Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie“ für die Prozessindustrie und die EN 62061 „Sicherheit von Maschinen - Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme“ für den Maschinenbau.

Ein elektrisches Thermometer kann in einem sicherheitstechnischen System entsprechend der Norm IEC 61508 eingesetzt werden, wenn das Thermometer zusammen mit einem für sicherheitsrelevante Applikationen zertifiziertem Temperatur-Transmitter verwendet wird. Der Temperatur-Transmitter Typ T32.xS von WIKA ist unter Berücksichtigung der IEC 61508 für den Einsatz in der Prozessindustrie entwickelt und vom TÜV Rheinland für diese Anwendung zertifiziert worden.

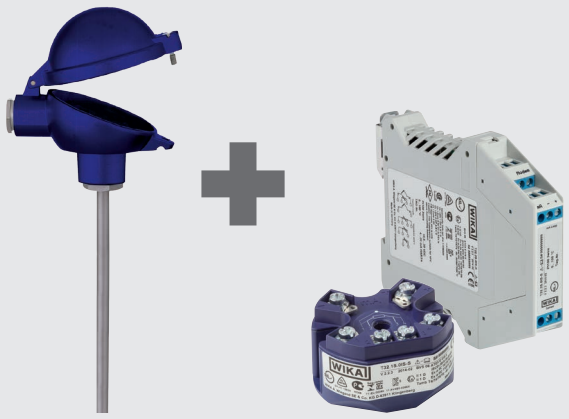
Ein elektrisches Thermometer ohne Temperatur-Transmitter, wie beispielsweise ein Widerstandsthermometer oder ein Thermoelement, fällt nicht unter die IEC 61508, da z. B. ein Messwiderstand ein einfaches elektrisches Bauteil ist, das keine Selbstdiagnose durchführen und Fehler aufdecken kann.

Für elektrische Thermometer ohne einen nach IEC 61508 zertifizierten Temperatur-Transmitter können lediglich Ausfallraten angegeben werden. Denn es hängt immer von der verwendeten Auswerteeinheit des Anwenders ab, welche Fehlerarten am elektrischen Thermometer aufgedeckt und sicher erkannt werden können.

Bei der Zertifizierung des Temperatur-Transmitters Typ T32.xS wurde der Temperatur-Transmitter in Verbindung mit einem elektrischen Thermometer betrachtet. Im Sicherheitshandbuch „Hinweise zur Funktionalen Sicherheit für Temperatur-Transmitter Typ T32.xS“ werden sicherheitsrelevante Kennwerte für den Temperatur-Transmitter, die angeschlossenen Temperatursensoren und den gesamten Aufbau angegeben.

Das Sensor-Teilsystem wird für die Bewertung in die Elemente „elektrisches Thermometer (Temperatursensor)“ und „Temperatur-Transmitter“ aufgeteilt. Die Temperatursensoren werden als Typ A-Komponenten (elementares Bauteil) und der Temperatur-Transmitter als Typ B-Komponenten (komplexes Bauteil) eingestuft.

Sensor-Teilsystem bestehend aus Temperatur-Transmitter und Temperatursensor



Thermoelement oder Widerstandsthermometer | **Temperatur-Transmitter Typ T32.xS**

Bewertung von sicherheitsbezogenen Systemen

Die Wahrscheinlichkeit, dass eine Sicherheitsfunktion bei Anforderung (d. h. beim Auftreten eines Fehlers im System) ausgeführt wird, wird durch die Sicherheitsintegrität definiert. Um ein Maß für die Anforderungen an die Sicherheitsintegrität zu erhalten, wird diese in vier Sicherheitsintegritätslevel (Safety Integrity Level, SIL) unterteilt. Wird der SIL 4 erreicht, ist die Wahrscheinlichkeit, dass die Sicherheitsfunktion ausgeführt wird, am größten und gewährleistet damit die maximal erreichbare Risikoreduzierung.

Stufen der Sicherheitsintegrität

Der Begriff „SIL“ ist also eine wesentliche Kenngröße des Sicherheitssystems, wird aber häufig gleichbedeutend für „Funktionale Sicherheit“ benutzt.

Der Sicherheitsintegritätslevel bezieht sich immer auf das gesamte Sicherheitssystem. Ein Element hat keinen SIL, sondern kann lediglich für eine SIL-Anwendung geeignet sein. Beispielsweise bildet der Temperatur-Transmitter Typ T32.xS alleine kein sicherheitstechnisches System. Für die Festlegung und die Einhaltung des geforderten Sicherheitsintegritätslevels sowohl des gesamten Sicherheitssystems als auch der einzelnen Elemente ist der Anwender verantwortlich!

WIKA als Hersteller von elektrischen Thermometern unterstützt den Anwender hierbei. Zum einen, indem bestätigt wird, dass die Anforderungen der Norm IEC 61508 eingehalten werden, wie zum Beispiel während der Entwicklung des T32.xS. Zum anderen können dem Anwender entsprechende sicherheitstechnische Kenndaten für die Anlagenprojektierung und die Bewertung der Sicherheitsfunktion zur Verfügung gestellt werden.

Anforderungen an ein Sicherheitssystem

Um eine Temperaturmessstelle optimal für ein sicherheitsbezogenes System auszulegen, sind folgende Aspekte zu beachten:

- Der sichere Zustand der Anlage und die Sicherheitsfunktion jedes Elements ist vom Anlagenbetreiber zu definieren.
- Der benötigte Sicherheitsintegritätslevel ist vom Betreiber des Sicherheitssystems durch eine Risikobewertung z. B. mit dem Risikographen zu ermitteln.
- Die Einsatzbedingungen (Prozessmedium, Umwelteinflüsse) des Thermometers sind genau zu spezifizieren, damit in Zusammenarbeit mit WIKA die Temperaturmessstelle optimal ausgelegt werden kann.
- Die Angaben in der WIKA-Dokumentation des verwendeten Thermometers sind einzuhalten.
- Sicherstellen, dass messstoffberührte Teile für das Messmedium geeignet sind.

Grundlegend für eine optimale Sicherheit an der Temperaturmessstelle ist die korrekte Auslegung des elektrischen Thermometers, entsprechend den Anforderungen im Prozess. Erst im nächsten Schritt wird ein für Sicherheitssysteme geeigneter Temperatur-Transmitter ausgewählt, der möglichst viele Fehlerarten des elektrischen Thermometers und des Transmitters selbst aufdeckt.

Ermittlung des maximal erreichbaren Sicherheitsintegritätslevels am Beispiel des Temperatur-Transmitters Typ T32.xS

Zur Bestimmung des Sicherheitsintegritätslevels eines sicherheitsbezogenen Systems sind sowohl die Anforderungen an die systematische Sicherheitsintegrität als auch an die Sicherheitsintegrität der Hardware zu bestimmen.

Systematische Sicherheitsintegrität

Um die Anforderungen an die systematische Sicherheitsintegrität zu erfüllen, sind systematische Fehler zu berücksichtigen. Systematische Fehler sind Konstruktionsfehler, Produktionsfehler oder Bedienungsfehler. Um diese zu verringern, gibt die IEC 61508 Sicherheitsmaßnahmen vor, die während der gesamten Lebensdauer (Product-Lifecycle) eines technischen Systems eingehalten werden müssen. Der Sicherheitslebenszyklus von Sicherheitssystemen beginnt bei der Konzeptionierung und endet mit der Außerbetriebnahme.
Im Rahmen des Sicherheitsmanagements während der Entwicklung des T32.xS sind beispielsweise durch Validierungs- und Verifikationstätigkeiten sowie durch Planung und sorgfältige Dokumentation systematische Fehler verhindert worden. Dadurch erfüllt die Software des Temperatur-Transmitters Typ T32.xS sogar die Kriterien für SIL 3 im Bezug auf die systematische Sicherheitsintegrität.

Sicherheitsintegrität der Hardware

Zufällige Fehler
Um die Sicherheitsintegrität der Hardware zu bewerten, sind zufällige Fehler zu betrachten. Diese entstehen durch zufällige Veränderungen eines Bauteilverhaltens, z. B. durch Unterbrechung, Kurzschluss oder zufällige Wertänderung eines Kondensators in einer elektrischen Schaltung. Zufällige Fehler können nicht vermieden werden. Lediglich die Wahrscheinlichkeit des Auftretens eines solchen Fehlers kann berechnet werden. Die Ausfallrate wird in der Einheit FIT (Failures in Time) angegeben.

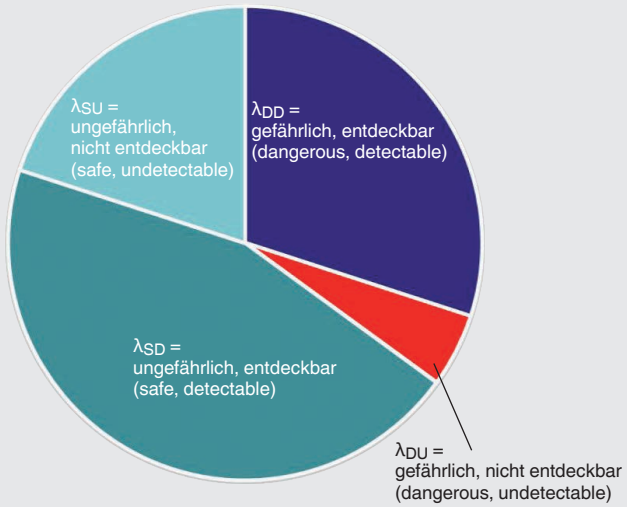
Es gilt: $$1\ FIT = 10^{-9}\ \frac{1}{h}$$

Die Gesamtheit aller Ausfälle in einem Zeitintervall mit konstanter Ausfallrate wird als Basisausfallrate λ_B bezeichnet. Die Basisausfallrate setzt sich zusammen aus gefährlichen Fehlern λ_D = dangerous und ungefährlichen Fehlern λ_S = safe, die einen Einfluss auf die Sicherheitsfunktion haben.

$$\lambda = \lambda_S + \lambda_D$$

Abhängig davon, ob ein Fehler zum Beispiel durch eine Diagnosefunktion in der Elektronik des Sicherheitssystems aufgedeckt werden kann oder unerkannt bleibt, werden die gefährlichen und ungefährlichen Fehler weiter unterteilt.

Unterteilung von Fehlerraten



Fehlerarten am elektrischen Thermometer

An einem elektrischen Thermometer können folgende Fehler auftreten:

- Kabelbruch - der Messkreis wird unterbrochen
- Kurzschluss - zwei Anschlussleitungen werden ungewollt verbunden
- Drift durch Änderungen im Widerstandsmaterial bzw. Drift der Thermospannung
- Änderung des Leitungswiderstandes, z. B. durch Temperaturwechsel

Abhängig von den Fehleraufdeckungsfunktionen des verwendeten Temperatur-Transmitters ist die Art des Ausfalls (λ_{SD}, λ_{SU}, λ_{DD}, λ_{DU}) für verschiedene Fehlerfälle am elektrischen Thermometer zu definieren.

Tabelle 1: Fehlererkennung durch den Temperatur-Transmitter Typ T32.xS

Mögliche Fehlerfälle am elektrischen Thermometer	Widerstandsthermometer 2-Leiter-Schaltung	Widerstandsthermometer 3-Leiter-Schaltung	Widerstandsthermometer 4-Leiter-Schaltung	Thermo-element
Kabelbruch	λ_{DD}	λ_{DD}	λ_{DD}	λ_{DD}
Kurzschluss	λ_{DD}	λ_{DD}	λ_{DD}	**λ_{DU}**
Drift	**λ_{DU}**	**λ_{DU}**	**λ_{DU}**	**λ_{DU}**
Änderung des Leitungswiderstandes	**λ_{DU}**	λ_{DD} 1)	λ_{DD}	λ_{DD}

1) Eine Änderung des Leitungswiderstandes in 3-Leiter-Schaltung kann nur bedingt unter der Voraussetzung, dass die Anschlussleitungen zwischen Messwiderstand und Transmitter die gleiche Länge sowie den gleichen Leitungsquerschnitt haben, aufgedeckt werden.

In der Literatur werden Ausfallraten für Thermoelemente und Widerstandsthermometer in verschiedenen Anwendungen und Bauformen angegeben. Die Ausfallraten beziehen sich auf den „Worst Case“ eines Thermometerausfalls und dienen als Orientierung bei der Auslegung von sicherheitstechnischen Systemen. Die Ausfallraten können unter Berücksichtigung der Einsatzbedingungen sowie der Anschlussleitung zwischen Messstelle und Transmitter herangezogen werden. Sie werden nach den Vibrationsanforderungen am Einsatzort (low stress/high stress) und nach der Art der Verbindung zwischen Messstelle und Temperatur-Transmitter (close coupled/extension wire) unterschieden (siehe „Definitionen und Abkürzungen“).

Tabelle 2: Ausfallraten für Thermoelemente ohne Temperatur-Transmitter 2)

Fehlerart	Close coupled		Extension wire	
	Low stress	High stress	Low stress	High stress
Kabelbruch	95 FIT	1.900 FIT	900 FIT	18.000 FIT
Kurzschluss	4 FIT	80 FIT	50 FIT	1.000 FIT
Drift	1 FIT	20 FIT	50 FIT	1.000 FIT

2) Die angegebenen Ausfallraten basieren auf Berechnungen seitens WIKA unter Einbeziehung von Basiskennzahlen der Firma exida.com L.L.C. (siehe Seite 12 „Literatur- und Quellenverzeichnis“, „Exida“)

Tabelle 3: Ausfallraten für Widerstandsthermometer in 4-Leiter-Schaltung ohne Temperatur-Transmitter 2)

Fehlerart	Close coupled		Extension wire	
	Low stress	High stress	Low stress	High stress
Kabelbruch	42 FIT	830 FIT	410 FIT	8.200 FIT
Kurzschluss	3 FIT	50 FIT	20 FIT	400 FIT
Drift	6 FIT	120 FIT	70 FIT	1.400 FIT

Tabelle 4: Ausfallraten für Widerstandsthermometer in 2- oder 3-Leiterschaltung ohne Temperatur-Transmitter 2)

Fehlerart	Close coupled		Extension wire	
	Low stress	High stress	Low stress	High stress
Kabelbruch	38 FIT	758 FIT	371 FIT	7.410 FIT
Kurzschluss	1 FIT	29 FIT	10 FIT	190 FIT
Drift	9 FIT	173 FIT	95 FIT	1.900 FIT

2) Die angegebenen Ausfallraten basieren auf Berechnungen seitens WIKA unter Einbeziehung von Basiskennzahlen der Firma exida.com L.L.C. (siehe Seite 12 „Literatur- und Quellenverzeichnis“, „Exida“)

Begrenzung des Sicherheitsintegritätslevels eines Elements

Der maximal erreichbare SIL eines Elements des Sicherheitssystems wird durch folgende Faktoren begrenzt:

- Anteil sicherer Ausfälle eines Hardwareelements (Safe Failure Fraction, SFF)
- Hardware-Fehlertoleranz (HFT)
  Die Hardware-Fehlertoleranz stellt ein Maß für den Redundanzgrad des Sicherheitssystems dar. Bei einer Hardwarefehlertoleranz von N, ist N+1 die minimale Anzahl von Fehlern, die zum Verlust einer Sicherheitsfunktion führen können. Ein sicherheitstechnisches System mit einkanaliger Architektur hat eine Hardware-Fehlertoleranz von 0.
- Komplexität der Komponenten (Typ A und B Komponenten)
  - Typ A-Komponenten sind elementare Bauteile, deren Ausfallverhalten vollständig definiert und deren Fehlverhalten bestimmt ist. Typ A-Komponenten sind beispielsweise Widerstandstemperatursensoren und Thermoelemente.
  - Bei komplexen Komponenten des Typs B ist das Ausfallverhalten mindestens einer Komponente nicht oder nicht vollständig definiert. Eine Typ B-Komponente ist beispielsweise eine elektronische Schaltung, die einen Mikroprozessor enthält. Der Temperatur-Transmitter T32.xS ist als Typ B-Komponente definiert (siehe Tabelle 5).

Um den SFF-Wert von Widerstandstemperatursensoren und Thermoelementen, die an den Temperatur-Transmitter T32.xS angeschlossen sind, zu berechnen, sind zunächst die Ausfallraten der Temperatursensoren unter Berücksichtigung der Diagnosefunktion des Transmitters in die Kategorien (λ_S, λ_{DD}, λ_{DU}) zu unterteilen. Daraus lässt sich der SFF-Wert entsprechend nachfolgender Formel berechnen:

$$SFF = \frac{\lambda_{DD} + \lambda_S}{\lambda_{DU} + \lambda_{DD} + \lambda_S}$$

Damit die als Typ A-Komponenten definierten Temperatursensoren in einkanaliger Architektur (HFT = 0) in sicherheitstechnischen Systemen bis SIL 2 eingesetzt werden dürfen, ist entsprechend Tabelle 5 ein SFF ≥ 60 % einzuhalten. Für die gleiche Applikation ist für den Temperatur-Transmitter T32.xS als Typ B-Komponente ein SFF ≥ 90 % notwendig.

Tabelle 5: Maximaler Sicherheitsintegritätslevel einer Komponente abhängig von der Hardware-Fehlertoleranz, der Komplexität der Komponenten und des Anteils sicherer Ausfälle

SFF	Hardware-Fehlertoleranz					
	0		1		2	
	Typ A	Typ B	Typ A	Typ B	Typ A	Typ B
< 60 %	SIL 1	nicht erlaubt	SIL 2	SIL 1	SIL 3	SIL 2
60 … < 90 %	SIL 2	SIL 1	SIL 3	SIL 2	SIL 4	SIL 3
90 … < 99 %	SIL 3	SIL 2	SIL 4	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 3	SIL 4	SIL 4	SIL 4	SIL 4

Nur wenn der SFF-Wert sowohl des Temperatur-Transmitters als auch des Temperatursensors die jeweils angegebene Grenze einhält, sind diese Elemente für sicherheitstechnische Systeme mit entsprechendem SIL zulässig. Zusätzlich muss der PFD-Wert der gesamten Sicherheitsfunktion den Anforderungen nach Tabelle 6 genügen.

Begrenzung des SIL des gesamten Sicherheitssystems

Die Norm IEC 61508 gibt Werte an, die den Sicherheitsintegritätslevel des gesamten Sicherheitssystems begrenzen. Je nachdem wie häufig das Sicherheitssystem angefordert wird, werden zwei Kennwerte unterschieden:

- **PFH** (Probability of dangerous failure per hour)

Mittlere Häufigkeit eines gefahrbringenden Ausfalls der Sicherheitsfunktion für eine Betriebsart mit hoher oder kontinuierlicher Anforderungsrate (High Demand). Diese Betriebsarten sind vor allem für den Maschinenbau relevant.

- **PFD_{avg}** (Probability of failure on demand)

Mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung der Sicherheitsfunktion für eine Betriebsart mit niedriger Anforderungsrate (Low Demand).

T_{proof} bezeichnet das Intervall der Wiederholungsprüfung. Nach diesem Intervall wird durch eine geeignete Prüfung („proof test") das System fast in einen „Wie-Neu-Zustand" innerhalb der vorgesehenen Gebrauchsdauer gebracht. Bei dieser Prüfung können auch gefährliche, nicht entdeckbare Fehler erkannt werden. Bei einem elektrischen Thermometer wird durch eine regelmäßige Kalibirierung sichergestellt, dass der Messwert noch innerhalb der geforderten Genauigkeit liegt. Damit wird also ein unzulässig hoher Drift ausgeschlossen.

Bei einem Wiederholungsprüfungsintervall von einem Jahr (T_{proof} = 8.760 h) resultiert folgender PFD_{avg}-Wert für ein Widerstandsthermometer in 4-Leiter-Schaltung und angeschlossenem Temperatur-Transmitter Typ T32.xS:
- Umgebungsbedingung: low stress
- Verbindung zwischen Messstelle und Transmitter: close coupled
- Ausfallrate λ_{DU} = 16 FIT 3)

$$PFD_{avg} = 0{,}5 * \lambda_{DU} * T_{proof}$$
$$= 0{,}5 * 16\ FIT * 8760\ h = 7{,}15 * 10^{-5}$$

Damit ist diese Kombination bezüglich der Anforderungen an den PFD_{avg}-Wert für Sicherheitssysteme mit höherem Sicherheitsintegritätslevel als SIL 2 geeignet, jedoch aufgrund der einkanaligen Struktur und der SFF auf SIL 2 begrenzt (siehe „Begrenzung des Sicherheitsintegritätslevels eines Elements").

Die oben beschriebene Formel ist aus der IEC 61508 abgeleitet. Es wird angenommen, dass die Zeitdauer von 8 h, die für die Wiederherstellung des Systems benötigt wird, vernachlässigbar klein gegenüber dem Wiederholungsprüfungsintervall von 8.760 h ist.

Der PFD_{avg}-Wert verhält sich annähernd linear zum Intervall der Wiederholungsprüfung T_{proof}. Je kürzer das Intervall der Wiederholungsprüfung desto besser der erreichbare PFD_{avg}-Wert. Analog kann das Intervall der Wiederholungsprüfung verlängert werden, wenn der PFD_{avg}-Wert des Gesamtsystems geringer als der zulässige Grenzwert ist. Wird das Intervall der Wiederholungsprüfung auf 0,5 Jahre verkürzt oder auf 2 Jahr verlängert, halbiert bzw. verdoppelt sich der PFD_{avg}-Wert.

Je kleiner der PFD_{avg}- bzw. PFH-Wert, umso größer der erreichbare SIL des Gesamtsystems. In Tabelle 6 werden den PFD_{avg}- bzw. PFH-Kennwerten Sicherheitsintegritätslevel zugeordnet.

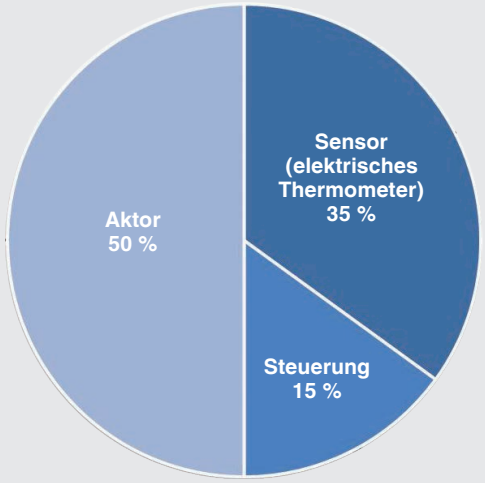
Tabelle 6: Einschränkung des SIL des Sicherheitssystems durch PFD_{avg}- und PFH-Werte

Sicherheits-integritätslevel (SIL)	Mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung der Sicherheitsfunktion (PFD_{avg})	Mittlere Häufigkeit eines gefahrbringenden Ausfalls je Stunde (PFH)
4	≥ 10^{-5} bis < 10^{-4}	≥ 10^{-9} bis < 10^{-8} h^{-1}
3	≥ 10^{-4} bis < 10^{-3}	≥ 10^{-8} bis < 10^{-7} h^{-1}
2	≥ 10^{-3} bis < 10^{-2}	≥ 10^{-7} bis < 10^{-6} h^{-1}
1	≥ 10^{-2} bis < 10^{-1}	≥ 10^{-6} bis < 10^{-5} h^{-1}

3) siehe Seite 12 „Literatur- und Quellenverzeichnis" und Seite 18-20 im Sicherheitshandbuch „Hinweise zur Funktionalen Sicherheit für Temperatur-Transmitter Typ T32.xS"

Für den Anwender ist immer der PFD_{avg}-Wert des gesamten Sicherheitssystems und nicht der Wert eines Elements relevant. Zur Bewertung hat sich als Richtwert folgende Aufteilung des PFD_{avg}-Wertes auf das Sicherheitssystem etabliert:

Anteile von Sensor, Steuerung, Aktor am gesamten PFD-Wert des SIS



Eine abweichende Verteilung auf die Komponenten kann vom Anlagenbetreiber festgelegt werden.

Nutzt der Sensor weniger als 35 % des maximal erlaubten PFD_{avg}-Wertes des Sicherheitssystems, wie z. B. ein elektrisches Thermometer mit Temperatur-Transmitter Typ T32.xS, so kann der Anwender eine Steuerung und einen Aktor mit entsprechend schlechteren PFD_{avg}-Werten einsetzen.

Strukturelle Einschränkungen

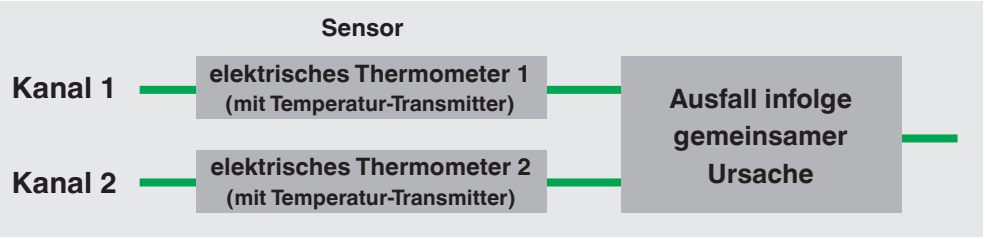
Strukturelle Eigenschaften des sicherheitstechnischen Systems können den maximal erreichbaren SIL einschränken. In einer einkanaligen Architektur wird der maximale SIL vom schwächsten Glied bestimmt. Im abgebildeten Sicherheitssystem sind die Teilsysteme „Sensor“ und „Logik“ für SIL 2, das Teilsystem „Stellglied“ lediglich für SIL 1 geeignet. Das gesamte Sicherheitssystem kann daher maximal SIL 1 erreichen.

Komponenten eines sicherheitsbezogenen Systems

Redundante Systeme

Werden zwei elektrische Thermometer mit Temperatur-Transmitter Typ T32.xS parallel aufgebaut, sind Ausfälle infolge gemeinsamer Ursache zu berücksichtigten. Ausfälle infolge gemeinsamer Ursache können beispielsweise auftreten, wenn Umweltbedingungen oder EMV-Störungen mehrere Kanäle gleichzeitig beeinflussen. Diese Fehler wirken sich gleichermaßen auf alle Kanäle eines redundanten Systems aus.

Zuverlässigkeitsblockdiagramm: elektrisches Thermometer in redundantem Aufbau



Die elektrischen Thermometer aus der vorherigen Abbildung stellen in diesem Fall eine zweikanalige Architektur (1oo2-System) dar. Solch eine Struktur wird als MooN-System bezeichnet. Ein MooN-System (M out of N) besteht aus N unabhängigen Kanälen, wovon M Kanale sicher funktionieren müssen, so dass das Gesamtsystem die sicherheitstechnische Funktion ausführen kann.

Das Auftreten von Ausfällen infolge gemeinsamer Ursache ist weniger wahrscheinlich, wenn die beiden verwendeten elektrischen Thermometer mit Temperatur-Transmitter hinsichtlich Aufbau, Messprinzip und Software möglichst diversitär sind. So kann beispielsweise ein Widerstandsthermometer für einen Kanal und ein Thermoelement für den anderen Kanal verwendet werden. Zur Messung kann sowohl je ein Schutzrohr für Widerstandsthermometer und Thermoelement als auch ein gemeinsames Schutzrohr verwendet werden. Bei Verwendung eines gemeinsamen Schutzrohres sind die Ausfälle infolge gemeinsamer Ursache entsprechend wahrscheinlicher. Eine höhere Diversität wird außerdem erreicht, wenn die verwendeten Temperatur-Transmitter von unterschiedlichen Herstellern sind und sich in ihrem Aufbau sowie der Software unterscheiden.

Speziell der WIKA-Temperatur-Transmitter Typ T32.xS hat den Vorteil, dass er in homogen redundanten Systemen bis SIL 3 verwendet werden kann. D.h. ein elektrisches Thermometer mit Temperatur-Transmitter Typ T32.xS wird parallel zu einem zweiten Thermometer mit baugleichem Transmitter geschaltet. In einkanaliger Architektur ist der Transmitter bis SIL 2 geeignet. Aufgrund der vollständigen Entwicklung und Zertifizierung des Temperatur-Transmitters Typ T32.xS nach allen Teilen der Norm IEC 61508 (Full-Assessment-Entwicklung) ist der Transmitter auch in homogen redundantem Aufbau für SIL 3-Applikationen geeignet. Bereits bei der Entwicklung wurden die fehlervermeidenden Maßnahmen der Software für SIL 3-Anwendungen ausgelegt. Damit unterscheidet sich der Temperatur-Transmitter Typ T32.xS von betriebsbewährten Geräten, die lediglich auf Basis einer früheren Verwendung für SIL-Anwendungen geeignet sind.

Betriebsbewährte Geräte erreichen in zweikanaligen Architekturen maximal den SIL des einzelnen Gerätes. Systematische Fehler werden bei diesen Geräten im Gegensatz zum Temperatur-Transmitter Typ T32.xS nicht von vornherein, z. B. während der Entwicklung des Gerätes, verhindert bzw. reduziert.

Um die Auswirkung der Ausfälle infolge gemeinsamer Ursache zu berücksichtigen, wird zur Berechnung des PFD-Wertes redundanter Systeme ein sogenannter β-Faktor benötigt. Der β-Faktor bezeichnet den Anteil unerkannter Ausfälle infolge gemeinsamer Ursache. Nach IEC 61508-6 und unter Berücksichtigung, dass die Zeitdauer von 8 h, die für die Wiederherstellung des Systems benötigt wird, vernachlässigbar klein gegenüber dem Wiederholungsprüfungsintervall von 8.760 h ist, wird der PFD-Wert für eine 1oo2-Struktur mit zwei identischen Kanälen durch folgende vereinfachte Formel berechnet:

$$PFD_{1oo2} = \frac{\lambda_{DU}^2 * T_{proof}^2}{3} + 0{,}5 * \lambda_{DU} * T_{proof} * \beta$$

Um den β-Faktor zu ermitteln, sind zunächst Maßnahmen zu definieren, die das Auftreten von Ausfällen infolge gemeinsamer Ursache verringern. Durch ingenieurmäßige Abschätzungen ist in Zusammenarbeit mit WIKA zu definieren, inwieweit jede Maßnahme das Auftreten von Ausfällen infolge gemeinsamer Ursache reduziert.

Zusammenfassende Empfehlungen

Zur optimalen Auslegung einer Temperaturmessstelle für sicherheitsgerichtete Anwendungen sind unbedingt die Anforderungen in Kapitel „Anforderungen an ein Sicherheitssystem“ zu berücksichtigen.

Weiterhin empfiehlt es sich, in Sicherheitsanwendungen den Temperatur-Transmitter Typ T32.xS (Kopf- oder Schienenversion) in Verbindung mit einem Widerstandsthermometer in 4-Leiter-Schaltung oder mit einem Thermoelement einzusetzen. Durch die umfangreichen Diagnoseeigenschaften des T32.xS und die Vorteile der 4-Leiter-Schaltung wird eine hohe Sicherheit bei der Temperaturmessung gewährleistet.

Um den Messeinsatz vor dem Prozessmedium zu schützen und um eine schnelle und einfache Kalibrierung des elektrischen Thermometers zu ermöglichen, sind Thermometer-Schutzarmaturen mit auswechselbarem Messeinsatz zu verwenden. Dabei ist insbesondere auf eine passende Auslegung des Schutzrohrs entsprechend der Anforderungen des Prozesses zu achten.

Literatur- und Quellenverzeichnis

1.) IEC 61508:2010:
Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme
Beuth Verlag GmbH, 10772 Berlin

2.) Exida:
Safety Equipment Reliability Handbook - 3rd Edition, 2012, exida.com L.L.C.

3.) WIKA Alexander Wiegand SE & Co. KG:
Sicherheitshandbuch „Hinweise zur Funktionalen Sicherheit für Temperatur-Transmitter Typ T32.xS“ (ab Firmware Revision 2.2.3)

Abkürzungen und Definitionen

Abkürzung	Definition
Close coupled	Der Temperatur-Transmitter befindet sich im Anschlussskopf des elektrischen Thermometers (head-mounted).
DC	Diagnosedeckungsgrad
Extension wire	Der Temperatur-Transmitter befindet sich außerhalb des Anschlusskopfes des elektrischen Thermometers, zum Beispiel in einem Schaltschrank entfernt von der Messstelle (remote-mounted).
FIT	Ausfälle pro Zeiteinheit, engl. Failures in time
HFT	Hardwarefehlertoleranz
High Stress	Anwendungen mit Vibration (≥ 67 % der maximalen Vibrationsfestigkeit des elektrischen Thermometers)
Low stress	Geringe Vibration (< 67 % der maximalen Vibrationsfestigkeit des elektrischen Thermometers)
PFD_{avg}	Mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung der Sicherheitsfunktion
PFH	Mittlere Häufigkeit eines gefahrbringenden Ausfalls der Sicherheitsfunktion
RTD	englisch: “**R**esistance **t**emperature **d**etector”; Widerstandsthermometer
SFF	Anteil sicherer Ausfälle eines Hardware-Elements
SIS	Sicherheitstechnisches System, engl. Safety Instrumented System
TC	englisch: „**T**hermo**c**ouple“; Thermoelement
TR	englisch: „**T**emperature **R**esistance“; Widerstandsthermometer

Auswirkung der Neubewertung des Temperatur-Transmitters Typ T32.xS (ab Firmware Revision 2.2.3) auf die sicherheitsrelevanten Kennwerte

Im Rahmen der Neubewertung wurden keine sicherheitstechnischen Änderungen am Temperatur-Transmitter durchgeführt. Die Diagnoseaufdeckung des Transmitters bleibt unverändert. Lediglich der neue Bewertungsansatz führt zu einer Änderung der sicherheitsrelevanten Kennwerte.

Neuer Normenstand IEC 61508
Seit der Erstbewertung des Temperatur-Transmitters Typ T32.xS wurde die Basisnorm der Funktionalen Sicherheit IEC 61508 „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbare elektronischer Systeme“ auf den Stand IEC 61508:2010 aktualisiert. Ab Firmware-Revision 2.2.3 wird der T32.xS nach diesem Normenstand bewertet.

Aktualisierte Ausfallraten
In diesem Zusammenhang wurden auch die FMEDA (Failure Modes, Effects and Diagnostic Analysis) mit aktuellen Bauteil-Ausfallraten wiederholt. Den Berechnungen werden Baulemente-Ausfallraten nach SN29500 zugrunde gelegt. Für die am Temperatur-Transmitter angeschlossenen Temperaturwiderstandssensoren und Thermoelemente werden von der Firma exida.com LLC ermittelten Ausfallraten herangezogen.

Elementbetrachtung Teilsystem „Sensor“
Mit der Einführung des Begriffs „Element“ in der IEC 61508-4:2010 Abschnitt 3.4.5 wird die Zusammenschaltung Temperatur-Transmitter und elektrisches Thermometer als Teilsystem „Sensor“ wie folgt betrachtet und bewertet:

Element 1	**Element 2**
Elektrisches Thermometer ohne Transmitter (Thermoelement oder Widerstandsthermometer) Typ A / SFF ≥ 60 % für HFT = 0 und SIL 2	Temperatur-Transmitter Typ T32.xS (ohne Thermoelement oder Widerstandsthermometer) Typ B / SFF ≥ 90 % für HFT = 0 und SIL 2

Diese getrennte Betrachtung wirkt sich auf die Bewertung des SFF-Wertes aus. So sinkt beispielsweise der für SIL 2 notwendige SFF-Wert für Thermoelemente oder Widerstandsthermometer auf 60 %.

Anwendungsspezifische Ausfallraten
Mit der Neubewertung des T32.xS werden die Ausfallraten je nach Vibrationsbelastung am Einsatzort des elektrischen Thermometers und je nach Anschluss des Thermometers an den Transmitter anwendungsspezifisch angegeben. Weiterhin werden Ausfallraten für den Temperatur-Transmitter „stand alone“ für verschiedene Konfigurationen berechnet.

Tendenziell verbesserte Ausfallraten
Die Ausfallraten des Transmitters T32.xS mit angeschlossenem Thermoelement oder Widerstandssensor haben sich tendenziell verbessert. Insbesondere für die Anwendungsbedingungen „low stress, close coupled“ hat sich die Ausfallrate für gefährliche, nicht entdeckbare Fehler verringert.

Auswirkungen auf den PFD_{avg}-Wert
Vor allem für die Anwendungsbedingung „low stress, close coupled“ hat sich der PFD_{avg} -Wert verbessert. Dies erlaubt dem Anwender ggf. im sicherheitstechnischen System Logik- oder Stellglied-Teilsysteme mit entsprechend größeren PFD_{avg}-Werten zu verwenden oder das Intervall der Wiederholungsprüfung zu verlängern.

WIKA Alexander Wiegand SE & Co. KG
Alexander-Wiegand-Straße 30
63911 Klingenberg/Germany
Tel. +49 9372 132-0
Fax +49 9372 132-406
info@wika.de
www.wika.de