Funktionale Sicherheit in Automation und Leittechnik

H. Kloust, Berlin

Sicherheitstechnische Systeme (SIS) in der Prozessindustrie müssen numerischen Mindestanforderungen bezüglich der Ausfallwahrscheinlichkeit in Abhängigkeit von Schutzzielen und Leistungsstufen entsprechen. Sie sind über Genehmigungsverfahren von staatlichen Behörden bzw. unabhängigen Institutionen zu prüfen und zu genehmigen.

1 Gefährdungs- und Risikoanalyse

Sicherheitstechnische Systeme für die Prozessindustrie (SIS) können nach Schutzebenen gegliedert werden (Tafel 1). Diese Systeme (Anlagen) müssen in Umsetzung der EU-Richtlinie 96/82/EU und durch die Störfallverordnung im Bundesimmissionsschutzgesetz (12 BImSchV) sowie nach DIN EN 61511 (VDE 0810) Teil 1 bis 3 [1] bzw. für Einrichtungen und Geräte nach DIN EN 61508 (VDE 803) Teil 1 bis 7 [2] erstmals numerischen Mindestanforderungen bezüglich der Ausfallwahrscheinlichkeit in Abhängigkeit von Schutzzielen und Leistungsstufen entsprechen.

Die europäischen Normen fordern daher die Durchführung einer Gefährdungs- und Risikoanalyse, um daraus die Spezifikation der notwendigen sicherheitstechnischen Systeme bestimmen zu können. Hierbei umfasst das SIS alle zur Ausführung der sicherheitstechnischen Funktion (SIF) erforderlichen Komponenten und Teilsysteme vom Sensor bis zum Aktor. Die Normen beschreiben allgemeine Lösungswege für alle Tätigkeiten während des Sicherheitslebenszyklus und definieren die Sicherheits-Integritätslevel (SIL) für Systeme, die aus elektrischen und/oder elektronischen und/oder programmierbar elektronischen Bauteilen bestehen, um die notwendigen Sicherheitsfunktionen in den vier Sicherheitsstufen (SIL 1 bis 4) auszuführen. In den meisten Anwendungsbeispielen wird die Sicherheit eines Prozesses durch eine Anzahl von Schutzsystemen erreicht, die auf vielerlei Technologien (chemische, mechanische, hydraulische, pneumatische, elektrische, elektronische, programmierbare elektronische Einrichtungen) basieren. Um diese Ziele zu erreichen fordert [1] speziell für die Prozessindustrie nach Tafel 2

- die Durchführung einer Gefährdungs- und Risikobeurteilung, um die übergreifenden Sicherheitsanforderungen festzulegen,
- die Zuordnung der Sicherheitsanforderungen zu den einzelnen sicherheitstechnischen Systemen,
- einen Betrachtungsrahmen innerhalb des Sicherheitslebenszyklus, der alle sicherheitstechnischen Methoden, wie Planungs- und Nutzungsetappen (Konzeption, Entwurf, Ausführung, Betrieb, Instandhaltung in der Prozessindustrie) zur Erlangung funktionaler Sicherheit umfasst,
- den Gebrauch bestimmter Tätigkeiten, wie die Anwendung eines Sicherheits-Managements gemäß DIN EN 60300-3-1 [3],

und führt im Einzelnen auf, welche Methoden zur Erlangung der funktionalen Sicherheit angewendet werden können.

Der Anwendungsbereich der Vorschriften betrifft Anlagen, Einrichtungen, Geräte und die Anwendungssoftware, die in ein System der Prozessindustrie eingesetzt werden. Dazu gehören auch Anlagen der Chemieindustrie, Raffinerien, Öl- und Gasförderung, Papierherstellung, konventionelle Stromerzeugung u. a. Sie legen weiterhin die Anforderungen an die Systemarchitektur und Hardwarekonfiguration sowie Anwendungssoftware und Systemintegration fest. Dies betrifft:

- die Phasen und die Tätigkeiten des Sicherheitslebenszyklus nach Modell, die während der Planung und Erstellung der Anwendungssoftware festgelegt werden; dies schließt die Anwendung von Maßnahmen und Techniken ein, die Fehler in der Software vermeiden und Ausfälle beherrschen sollen
- Umfang der Dokumentation für die bestätigte Software, die an den Errichter des SIS übergeben wird
- Vorbereitung von Dokumentationen und Vorschriften für die Software, die der Anwender für den Betrieb und die Instandhaltung des SIS benötigt.

Autor
Dipl.-Ing. *Heinz Kloust,* Ingenieurbüro für Normung, Zertifizierung und Planung von elektro- und leittechnischen Anlagen, Berlin

2 DIN EN 61511 (VDE 0810)

Desgleichen gibt DIN EN 61511 (VDE 0810) [1] an:

- Festlegungen einer Reihe von Tätigkeiten, die notwendig sind, um die funktionalen Anforderungen und die erforderliche Sicherheitsintegrität für die SIS zu erreichen.
- Durchführung einer Gefährdungs- und Risikoanalyse. Eine Übersicht über Methoden zur Risikominderung zeigt Tafel 1.
- Definition der mittleren Ausfallwahrscheinlichkeit bei Anforderungsbetriebsart und die Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (PFD), den verschiedenen Sicherheits-Integritätslevel gemäß den Tafeln 3 und 4 sowie deren Maßnahmen bei Erreichung der geforderten Integritätslevel
- Definition der höchsten bzw. niedrigsten Sicherheitslevel (SIL 4 bis SIL 1), welche eine sicherheitstechnische Funktion (SIF) erreichen kann, die nach diesen Normen ausgeführt wurde bzw. unterhalb dessen diese Normen nicht mehr gültig sind
- Festlegungen über den notwendigen Rahmen von Integritätsleveln (SIL) im speziellen Anwendungsfall und Anforderungen für alle Teile des SIS von den Sensoren bis zu den Aktoren sowie der notwendigen Dokumentation, welche während des Sicherheitslebenszyklus benötigt wird.

Tafel 1 Typische Methoden der Risikominderung in prozesstechnischen Anlagen nach DIN EN 61511 (VDE 0810-1):2005-05

Öffentliche Maßnahmen in Notfällen • Rundfunkinformationen im Notfall
Anlagenbezogene Maßnahmen in Notfällen • Evakuierungsmaßnahmen
Schadensbegrenzung • Mechanische Systeme • Sicherheitstechnische Regeleinrichtungen • Sicherheitstechnische Schadensbegrenzungseinrichtungen • Betriebliche Überwachung
Schutz • Mechanische Systeme • Prozessalarme mit Bedienereingriff • Sicherheitstechnische Regeleinrichtungen • Sicherheitstechnische Schutzeinrichtungen
Regelung und Überwachung • Betriebs- und Überwachungseinrichtungen (BPCS) • Überwachungseinrichtungen (Prozessalarme)

3 Spezielle Sicherheitsanforderungen

Als spezielle Sicherheitsanforderungen an das konkrete SIS müssen in der Planungsphase Spezifikationen z. B. folgendermaßen festgelegt und beschrieben werden:

- Beschreibung aller für die funktionelle Sicherheit notwendigen sicherheitstechnischen Funktionen (SIF) und eine Aufstellung derjenigen sicheren Prozesszustände, die – sofern sie gemeinsam auftreten – eine Gefährdung darstellen (z. B. bei Überlastung eines Notbehälters, mehrfache Notent-

spannung über eine Fackel) sowie die zu erwartenden Auslöser und Raten von Anforderungen sowie maximal zulässige Häufigkeit aktiver Fehler z. B. nach Tafel ❺;
- Definition des sicheren Zustands für jede einzelne SIF und Anforderungen, um Fehler gemeinsamer Ursache herauszufinden und auszuschalten. Definition, wie gefahrbringende Kombinationen von Ausgangszuständen des SIS vermieden werden können, und Festlegung aller Maßnahmen, um im Fall eines bekannten Fehlers in der SIS den sicheren Zustand zu erreichen oder beizubehalten
- Beschreibung der Betriebsarten und der normalen als auch anormalen Betriebszustände der Gesamtanlage und Anlagenteile sowie eine Aufstellung der SIS, die zum Betreiben der Anlage in jeder Betriebsart benötigt werden
- Beschreibung der Ausfallarten und deren gewünschte Reaktion der SIS (z. B. Alarme, automatische Abschaltungen) sowie Angabe aller Schnittstellen zwischen dem SIS und anderen Systemen (einschließlich der Betriebseinrichtungen und der Bediener)
- Sicherheits-Integritätslevel (SIL 1 bis 4) und die Betriebsart (auf Anforderung oder kontinuierlich) jeder Sicherheitsfunktion in Übereinstimmung mit Tafel ❸ bzw. ❹.
- Beschreibung der Messsignale und deren Grenzwerte
- durch Signal-Ausgänge der SIS ausgelöste Maßnahmen im Prozess sowie Kriterien für eine erfolgreiche Arbeitsweise (z. B. auf Anforderung hinsichtlich des dichten Schließens von Stellventilen)
- funktioneller Zusammenhang zwischen Signaleingängen und -ausgängen, einschließlich logischer Verknüpfungen, mathematischer Funktionen und erforderlicher Freigaben sowie Anforderungen für Über-

Tafel ❷ Übersicht über den Sicherheitslebenszyklus eines SIS nach DIN EN 61511 (VDE 0810-1:2005-05)

Phase des Sicherheitslebenszyklus oder Tätigkeit Lfd. Nr./Titel		Ziele	Abschnitt der Anforderungen gem. Norm	Eingaben	Ergebnisse
1.	Gefährdungs- und Risikobeurteilung	Festlegung von Gefährdungen und gefahrbringenden Ereignissen durch den Prozess bzw. die zugehörigen Einrichtungen, der Ereignisketten, die zu gefahrbringenden Ereignissen führen können, des damit verbundenen verfahrenstechnischen Risikos, der Anforderungen zur Risikominderung und der sicherheitstechnischen Funktionen, die zur notwendigen Risikominderung benötigt werden	8	Verfahrenstechnischer Entwurf, Auslegung, personelle Maßnahmen, Sicherheitsziele	Beschreibung der Gefährdungen, der benötigten Sicherheitsfunktionen und der jeweiligen Risikominderung
2.	Zuordnung der Sicherheitsfunktionen zu den Schutzebenen	Zuordnung der Sicherheitsfunktionen zu den entsprechenden Schutzebenen und für jede sicherheitstechnische Funktion; Zuordnung des zugehörigen Sicherheits-Integritätslevels (SIL)	9	Beschreibung der benötigten sicherheitstechnischen Funktion einschl. der Anforderungen an die Sicherheitsintegrität	Beschreibung der Zuordnung von Sicherheitsanforderungen
3.	Spezifikation der Sicherheitsanforderungen an das SIS	Festlegung der Anforderungen an jedes SIS in Form der notwendigen sicherheitstechnischen Funktionen und der zugehörigen Sicherheits-Integritätslevel zur Erreichung der erforderlichen funktionalen Sicherheit	10	Beschreibung der Zuordnung der Sicherheitsanforderungen nach Abschnitt 9 der Norm	Anforderungen an das sicherheitstechnische System und an die Software-Sicherheit
4.	Entwurf und Planung des SIS	Entwurf eines SIS, das den Anforderungen bezüglich der sicherheitstechnischen Funktionen und der Sicherheitsintegrität genügt	11 und 12.4	Sicherheitsanforderungen an das SIS und an die Software	Entwurf des SIS in Übereinstimmung mit den Sicherheitsanforderungen; Planung des SIS-Integrationstests
5.	SIS-Montage, Inbetriebnahme und Validierung	Integration und Prüfung des SIS; Validierung, dass das SIS mit seinen einzelnen sicherheitstechnischen Funktionen und deren Sicherheitsintegrität in jeder Hinsicht die gestellten Sicherheitsanforderungen erfüllt	12.3 14 15	SIS-Entwurf; Planung des SIS-Integrationstests; SIS-Sicherheitsanforderungen; Planung der Sicherheits-Validierung	Voll funktionierendes, der Planung entsprechendes SIS Ergebnisse der Integrationstests des SIS; Ergebnisse der Montage-, Inbetriebnahme- und der Validierungstätigkeiten
6.	SIS-Betrieb und Instandhaltung	Sicherstellen, dass die funktionale Sicherheit des SIS während des Betriebs und bei Instandhaltungssarbeiten erhalten bleibt	16	SIS-Anforderungen; SIS-Auslegung, Planung für SIS-Betrieb und Instandhaltung	Ergebnisse der Tätigkeiten im Rahmen des SIS-Betriebs und der Instandhaltung
7.	Modifikationen am SIS	Durchführung von Korrekturen, Verbesserungen oder Anpassungen des SIS so, dass der erforderliche Sicherheits-Integritätslevel erreicht und erhalten wird	17	Revidierte SIS-Sicherheitsanforderungen	Ergebnisse der SIS-Modifikationen
8.	Außerbetriebnahme	Durch geeignete Prüfung und Beachtung der Anlagenstruktur sicherstellen, dass nicht betroffene Funktionen in Betrieb bleiben	18	Sicherheitsanforderungen und Anlagendokumentation („as built“)	Sicherheitstechnische Funktion außer Betrieb
9.	SIS-Verifikation	Prüfung und Bewertung der Ergebnisse einer Phase auf Richtigkeit und Konsistenz bezüglich der Produkte und Normen, die als Vorgaben dieser Phase vorliegen	7 12.7	Phasenspezifische Planvorgaben zur Verifikation des SIS	Ergebnisse der SIS-Verifikation für jede Phase
10.	Beurteilung der funktionalen Sicherheit des SIS	Untersuchung und Bewertung der funktionalen Sicherheit des SIS	5	Plan zur Beurteilung der funktionalen Sicherheit des SIS	Ergebnis der Beurteilung der funktionalen Sicherheit des SIS

Tafel ❸ Sicherheits-Integritätslevel: Ausfallwahrscheinlichkeit bei Anforderung nach DIN EN 61511 (VDE 0810-1):2005-05

Anforderungsbetriebsart		
Sicherheits-Integritätslevel (SIL)	**Zielwert für die mittlere Ausfallwahrscheinlichkeit (Ausfallgrenzwert) bei Anforderung**	**Zielwert für die Risikominderung**
4	$\geq 10^{-5}$ bis $< 10^{-4}$	> 10000 bis ≤ 100000
3	$\geq 10^{-4}$ bis $< 10^{-3}$	> 1000 bis ≤ 10000
2	$\geq 10^{-3}$ bis $< 10^{-2}$	> 100 bis ≤ 1000
1	$\geq 10^{-2}$ bis $< 10^{-1}$	> 10 bis ≤ 100

Tafel ❹ Sicherheits-Integritätslevel: Häufigkeit gefahrbringender Ausfälle der sicherheitstechnischen Funktion nach DIN EN 61511-1 (VDE 0810-1) 2005-05

Betriebsart mit kontinuierlicher Anforderung	
SIL	**Zielwert für die Häufigkeit gefahrbringender Ausfälle der sicherheitstechnischen Funktion pro Stunde**
4	$\geq 10^{-9}$ bis $< 10^{-8}$
3	$\geq 10^{-8}$ bis $< 10^{-7}$
2	$\geq 10^{-7}$ bis $< 10^{-6}$
1	$\geq 10^{-6}$ bis $< 10^{-5}$

Tafel ❺ Mindest-Hardware-Fehlertoleranz von Sensoren, Aktoren und nichtprogrammierbaren Logiksystemen nach DIN EN 61511-1 (VDE 0810-1): 2005-05

SIL	Mindest-Hardware-Fehlertoleranz-Gruppe
1	0
2	1
3	2
4	Es gelten besondere Anforderungen; siehe IEC 61508

brückungen/Signalunterdrückungen/Umgänge einschließlich ihrer Aufhebung
- Anforderungen zum Abfahren der Anlage im Handbetrieb, der Verwendung des Arbeits- oder Ruhestromprinzips bei Steuerungen sowie die erforderlichen Antwortzeiten für die SIS, um den Prozess in den sicheren Zustand zu bringen und zum Zurücksetzen des SIS nach Abschaltung der Anlage
- Anforderungen zur Inbetriebnahme und Wiederinbetriebnahme und deren Intervalle der SIS, der erreichbaren mittlere Reparaturzeit unter Berücksichtigung von Reisezeiten, Örtlichkeiten, Verfügbarkeit von Ersatzteilen, Serviceverträgen, zulässige Umgebungsbedingungen.

Desgleichen sind die Extremwerte aller Umgebungsbedingungen zu ermitteln, die im Betrieb des SIS auftreten können. Dabei sind zu berücksichtigen: Temperatur, Feuchtigkeit, Verschmutzung, Erdung, elektromagnetische Verträglichkeit (EMV), Erschütterungen, Schwingungen, elektrostatische Entladungen, Ex-Zonen-Einteilung, Überschwemmung, Blitzschlag und andere zugehörige Faktoren. Beim Eintreten von größeren Schadensereignissen können darüber hinaus zusätzliche Anforderungen für alle Sicherheitsfunktionen notwendig werden (z. B. erforderliche Betriebszeit eines Ventils im Brandfall).

Beispiele der Anwendung der Normen aus der Praxis sind im Teil 3 von DIN EN 61511 (VDE 0810) [1] aufgeführt, so z. B. zur Regelung von Druckbehältern mit Betrachtung der Eintrittshäufigkeit von gefährlichen Ereignissen, die zur Überschreitung der Sicherheitsgrenzwerte im Behälter führt und schädliche Stoffe häufig in die Umwelt abgeben kann.

Eine Risikominderung zur Abwendung gefährlicher Ereignisse wird durch Einführung einer redundanten Schutzebene bzw. einer SIS-Sicherheitsfunktion (SIL2-Funktion) untersucht. Dabei konnte festgestellt werden, dass durch die Einführung der SIL2-Funktion die Häufigkeit der Freisetzungen aufgrund von Überdruck im Druckbehälter verringert wurde.

Eine weitere Möglichkeit zur Risikominimierung für Schutzeinrichtungen, z. B. in der chemischen Industrie oder der Kerntechnik – und wo ein rechnerischer Nachweis nicht oder nur schwer möglich ist, da keine gesicherte Daten über individuelle Ausfallraten vorliegen – ist ein Nachweis der sicherheitstechnischen Zuverlässigkeit nach NAMUR NE 93 [4]. Nach dieser in der Praxis erprobten Methode werden summarisch statistisch belastbare Aussagen für das abzudeckende Risiko der erforderlichen sicherheitsbezogenen Verfügbarkeit der sicherheitstechnischen Einrichtungen getroffen.

Literatur

[1] DIN EN 61511 (VDE 0810) Teil 1-3 Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie.

[2] DIN EN 61508 (VDE 0803) Teil 1-7 Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme.

[3] DIN EN 60300-3-1 Zuverlässigkeitsmanagement; Teil 3-1: Anwendungsleitfaden – Verfahren zur Analyse der Zuverlässigkeit – Leitfaden zur Methodik.

[4] NAMUR NE 93 Nachweis der technischen Zuverlässigkeit von PLT-Schutzeinrichtungen.