

## Inhalt

	Seite
Vorwort.....	2
Einleitung .....	7
1 Anwendungsbereich .....	9
2 Normative Verweisungen .....	9
3 Begriffe und Abkürzungen .....	9
4 Übereinstimmung mit dieser Internationalen Norm .....	9
5 Management der funktionalen Sicherheit.....	9
5.1 Ziel .....	9
5.2 Anforderungen .....	9
6 Anforderungen an den Sicherheitslebenszyklus .....	15
6.1 Ziele .....	15
6.2 Anforderungen .....	16
7 Verifikation .....	16
7.1 Ziel .....	16
8 Beurteilung des Risikos und der Gefährdung aus dem Prozess.....	17
8.1 Ziele .....	17
8.2 Anforderungen .....	17
9 Zuordnung der Sicherheitsfunktionen zu den Schutzebenen .....	19
9.1 Ziel .....	19
9.2 Anforderungen an den Prozess der Zuordnung .....	19
9.3 Zusätzliche Anforderungen für Sicherheits-Integritätslevel 4 .....	22
9.4 Anforderungen an Betriebseinrichtungen, die als Schutzebene eingesetzt werden.....	22
9.5 Anforderungen zur Vermeidung von Ausfällen infolge gemeinsamer Ursache, gleichartigen Ausfällen und abhängigen Ausfällen .....	22
10 Spezifikation der Sicherheitsanforderungen an das SIS .....	23
10.1 Ziel .....	23
10.2 Allgemeine Anforderungen .....	23
10.3 Sicherheitsanforderungen an das SIS.....	24
11 Entwurf und Planung des SIS.....	25
11.1 Ziel .....	25
11.2 Allgemeine Anforderungen .....	25
11.3 Anforderungen an das Systemverhalten bei Entdeckung eines Fehlers .....	29
11.4 Anforderungen an die Hardware-Fehlertoleranz .....	29
11.5 Anforderungen an die Auswahl von Komponenten und Teilsystemen .....	31
11.6 Feldgeräte.....	33
11.7 Schnittstellen .....	33
11.8 Anforderungen an Instandhaltungs- oder Testeinrichtungen .....	35
11.9 Ausfallwahrscheinlichkeit sicherheitstechnischer Funktionen .....	36
12 Anforderungen an die Anwendungssoftware und Auswahlkriterien für Software-Hilfsmittel .....	38

	Seite
12.1 Anforderungen an den Sicherheitslebenszyklus der Anwendungssoftware.....	38
12.2 Spezifikation der Sicherheitsanforderungen an die Anwendersoftware.....	41
12.3 Validierungsplanung für die Sicherheit der Anwendungssoftware .....	43
12.4 Entwurf und Erstellung der Anwendungssoftware.....	43
12.5 Integration der Anwendungs-Software in das SIS-Teilsystem .....	50
12.6 Vorgehen bei Modifikation einer FPL- und LVL-Software .....	50
12.7 Verifikation der Anwendungssoftware .....	51
13 Werksendprüfungen (FAT = Factory Acceptance Test).....	52
13.1 Ziele .....	52
13.2 Empfehlungen.....	53
14 SIS-Montage und Inbetriebnahme.....	53
14.1 Ziele .....	53
14.2 Anforderungen .....	53
15 SIS-Sicherheits-Validierung.....	53
15.1 Ziel .....	53
15.2 Anforderungen .....	54
16 Betrieb und Instandhaltung des SIS .....	54
16.1 Ziele .....	54
16.2 Anforderungen .....	54
16.3 Wiederholungsprüfungen und Inspektionen .....	55
17 Modifikationen am SIS.....	56
17.1 Ziele .....	56
17.2 Anforderungen .....	56
18 Außerbetriebnahme des SIS .....	56
18.1 Ziele .....	56
18.2 Anforderungen .....	56
19 Anforderungen an die Information und Dokumentation.....	57
19.1 Ziele .....	57
19.2 Anforderungen .....	57
Anhang A (informativ) Beispielhafte Methoden zur Berechnung der Wahrscheinlichkeit eines Ausfalles bei Anforderung einer sicherheitstechnischen Funktion .....	58
A.1 Allgemeines .....	58
A.2 Methode des Zuverlässigkeitsblockdiagramms.....	58
A.3 Methode der vereinfachten Gleichungen.....	58
A.4 Methode der Fehlerbaumanalyse .....	58
A.5 Methode der Markov-Modelle .....	58
Anhang B (informativ) Erstellung einer typischen SIS-Architektur.....	59
B.1 Hintergrund .....	59
B.1.1 Einführung.....	59
B.1.2 Anleitungen und Praktiken.....	59

	Seite
B.1.3 Instrumentierung.....	59
B.1.4 Logiksystem.....	59
B.2 Arbeitsablauf.....	59
B.2.1 Einführung .....	59
B.2.2 Typische Schritte im SIS-Lebenszyklus .....	59
B.2.3 Zuordnung der Sicherheitsanforderung.....	60
B.2.4 Zuordnung der Sicherheitsanforderungen innerhalb des SIS .....	60
B.2.5 Architekturbezogene Anforderungen an die Software .....	61
B.2.6 Erstellung der Anwendungssoftware.....	61
B.3 Beispiel 1 .....	61
B.3.1 Einführung .....	61
B.3.2 Gefährdungsszenario .....	61
B.3.3 Spezifikation der Sicherheitsanforderungen und SIL .....	61
B.3.4 Systemarchitektur .....	61
B.3.5 Zusätzliche auf die Architektur bezogene Sicherheitssoftware.....	62
B.4 Beispiel 2 .....	62
B.4.1 Einführung .....	62
B.4.2 Gefährliches Szenario .....	62
B.4.3 Spezifikation der Sicherheitsanforderungen und SIL .....	62
B.4.4 Systemarchitektur.....	62
B.4.5 Zusätzliche architekturbezogene Sicherheitssoftware .....	63
Anhang C (informativ) Anwendungseigenschaften einer Sicherheits-SPS .....	64
C.1 System.....	64
C.2 Arbeitsablauf.....	64
Anhang D (informativ) Beispiel für eine Methode zur Erstellung der Anwendungssoftware für ein SIS-Logiksystem.....	66
D.1 Zusammenfassung des gesamten Integrationsprozesses für ein System.....	66
D.2 Erstellung der Anwendungssoftware für SIS-Logiksysteme .....	67
D.3 Programmierstandards für den Anwendungsprogrammierer .....	68
D.4 Weitere Anforderungen für die Konfiguration/die Programmerstellung und Laufzeitsysteme für Sicherheitsanwendungen.....	68
D.5 Annahmen .....	69
Anhang E (informativ) Beispiel für die Entwicklung extern aufgebauter Diagnosen für eine programmierbare Sicherheitssteuerung .....	70
E.1 Intern aufgebaute Diagnosen .....	70
E.2 Extern aufgebaute Diagnosen.....	70
E.3 Literaturhinweis .....	72
<b>Bilder</b>	
Bild 1 – Gesamtrahmen dieser Norm .....	8
Bild 2 – Unabhängigkeit von BPCS-Funktion und auslösender Ursache.....	22
Bild 3 – Software-Entwicklungsprozess (das „V-Modell“).....	39

	Seite
Bild C.1 – Logiksystem.....	64
Bild E.1 – Zeitdiagramm eines externen Watchdog.....	71
<b>Tabellen</b>	
Tabelle 1 – Typischer Aufbau und Inhalt eines Sicherheitshandbuchs .....	48