

Inhalt

	Seite
Vorwort.....	2
Vorwort zu A1	3
Einleitung	7
1 Anwendungsbereich	10
2 Normative Verweisungen	11
3 Begriffe und Abkürzungen	12
3.1 Alphabetische Liste der Begriffe.....	12
3.2 Begriffe	14
3.3 Abkürzungen	24
4 Management der funktionalen Sicherheit.....	24
4.1 Ziel	24
4.2 Anforderungen.....	24
5 Anforderungen zur Spezifikation der sicherheitsbezogenen Steuerungsfunktionen (SRCFs)	26
5.1 Ziel	26
5.2 Spezifikation der Anforderungen für SRCFs	26
6 Entwurf und Integration des sicherheitsbezogenen elektrischen Steuerungssystems (SRECS).....	28
6.1 Ziel	28
6.2 Allgemeine Anforderungen	28
6.3 Anforderungen zum Verhalten (des SRECS) bei Erkennung eines Fehlers im SRECS	29
6.4 Anforderungen zur systematischen Sicherheitsintegrität des SRECS.....	30
6.5 Auswahl eines sicherheitsbezogenen elektrischen Steuerungssystems	32
6.6 Entwurf und Entwicklung eines sicherheitsbezogenen elektrischen Steuerungssystems (SRECS).....	32
6.7 Realisierung von Teilsystemen	38
6.8 Realisierung von Diagnosefunktionen.....	53
6.9 Hardware-Implementierung des SRECS.....	54
6.10 Spezifikation der Software-Sicherheitsanforderungen	54
6.11 Software-Entwurf und Entwicklung.....	56
6.12 Integration und Test des sicherheitsbezogenen elektrischen Steuerungssystems	63
6.13 Installation des SRECS	64
7 Benutzerinformationen des SRECS	64
7.1 Ziel	64
7.2 Dokumentation für Installation, Gebrauch und Instandhaltung	65
8 Validierung des sicherheitsbezogenen elektrischen Steuerungssystems	66
8.1 Ziel	66
8.2 Allgemeine Anforderungen	66
8.3 Validierung der systematischen Sicherheitsintegrität des SRECS	66
9 Modifikation	68

	Seite
9.1 Ziel.....	68
9.2 Modifikationsverfahren	68
9.3 Konfigurationsmanagementverfahren	68
10 Dokumentation	70
Anhang A (informativ) Festsetzung des SIL.....	72
Anhang B (informativ) Beispiel eines Entwurfs eines sicherheitsbezogenen elektrischen Steuerungssystems (SRECS) unter Anwendung der Konzepte und Anforderungen aus den Abschnitten 5 und 6	80
Anhang C (informativ) Hinweise zu Entwurf und Entwicklung von Embedded-Software	87
Anhang D (informativ) Ausfallarten elektrischer/elektronischer Bauteile	96
Anhang E (informativ) Elektromagnetische (EM) Phänomene und erhöhte Störfestigkeitsgrade für SRECS, die für den Gebrauch im Industriebereich nach IEC 61000-6-2 vorgesehen sind	97
Anhang F (informativ) Methodologie zur Abschätzung der Anfälligkeit gegenüber Ausfällen in Folge gemeinsamer Ursache (CCF)	98
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	100
Anhang ZZ (informativ) Zusammenhang mit grundlegenden Anforderungen von EU-Richtlinien.....	101

Bilder

Bild 1 – Verhältnis der IEC 62061 zu anderen relevanten Normen	8
Bild 2 – Ablauf des SRECS-Entwurfs- und Entwicklungsprozesses	35
Bild 3 – Zuordnung von Sicherheitsanforderungen der Funktionsblöcke zu Teilsystemen (siehe 6.6.2.1.1)	36
Bild 4 – Ablauf für Entwurf und Entwicklung eines Teilsystems (siehe Kästchen 6B von Bild 2)	41
Bild 5 – Aufteilung eines Funktionsblocks in redundante Funktionsblock-Elemente und ihre zugehörigen Teilsystem-Elemente.....	42
Bild 6 – Logische Darstellung Teilsystem A	48
Bild 7 – Logische Darstellung Teilsystem B	48
Bild 8 – Logische Darstellung Teilsystem C	49
Bild 9 – Logische Darstellung Teilsystem D	50
Bild A.1 – Ablauf des Prozesses der Festsetzung des SIL	73
Bild A.2 – Parameter der Risikoabschätzung.....	74
Bild A.3 – Beispiel-Formblatt für den Prozess der Bestimmung des SIL	79
Bild B.1 – Terminologie im Zusammenhang funktionaler Aufteilung	80
Bild B.2 – Beispiel einer Maschine	81
Bild B.3 – Spezifikation der Anforderungen für eine SRCF.....	81
Bild B.4 – Aufteilung in eine Struktur von Funktionsblöcken.....	82
Bild B.5 – Erstes Konzept für eine Architektur eines SRECS	83
Bild B.6 – SRECS-Architektur mit innerhalb jedes Teilsystems eingebetteten Diagnosefunktionen (TS1 bis TS4)	84
Bild B.7 – SRECS-Architektur mit innerhalb des Teilsystems TS3 eingebetteten Diagnosefunktionen.....	85
Bild B.8 – Abschätzung der PFH_D für ein SRECS	86

Tabellen

Tabelle 2 – Übersicht und Ziele der IEC 62061.....	11
Tabelle 3 – Sicherheits-Integritätslevels: Ausfallgrenzwerte für SRCFs	28
Tabelle 4 – Merkmale der in diesem Beispiel verwendeten Teilsysteme 1 und 2 (siehe 6.6.3.3, Anmerkung)	38
Tabelle 5 – Strukturelle Einschränkungen von Teilsystemen: maximal in Anspruch nehmbarer SIL für eine SRCF, die dieses Teilsystem verwendet	44
Tabelle 8 – Informationen und Dokumentationen eines SRECS	71
Tabelle A.1 – Klassifikation der Schwere (S)	74
Tabelle A.2 – Klassifikation der Häufigkeit und der Dauer der Exposition (F).....	75
Tabelle A.3 – Klassifikation der Wahrscheinlichkeit (W)	76
Tabelle A.4 – Klassifikation der Wahrscheinlichkeit der Vermeidung oder Begrenzung des Schadens (P).....	77
Tabelle A.5 – Parameter zur Festlegung der Klasse der Wahrscheinlichkeit des Schadens (K)	77
Tabelle A.6 – Matrix der Festlegung des SIL	78
Tabelle F.1 – Kriterien zur Bestimmung von CCF (1 von 2).....	98
Tabelle F.2 – Abschätzung des CCF-Faktors (β).....	99