

**Speicherprogrammierbare Steuerungen –  
Teil 6: Funktionale Sicherheit**

**Inhalt**

	Seite
Einleitung .....	5
1 Anwendungsbereich .....	6
1.1 Allgemeines .....	6
1.2 Rahmen dieses Teils .....	7
2 Normative Verweisungen .....	9
3 Begriffe und Abkürzungen .....	11
4 Übereinstimmung mit dieser Norm .....	25
5 FS-SPS Sicherheitslebenszyklus .....	25
5.1 Allgemeines .....	25
5.2 Anforderungen an die funktionale Sicherheit und das SIL-Vermögen einer FS-SPS .....	27
5.3 Qualitätsmanagementsystem .....	29
5.4 Management des Sicherheitslebenszyklus der FS-SPS .....	29
6 Spezifikation der FS-SPS-Sicherheitsanforderungen .....	33
6.1 Allgemein .....	33
6.2 Inhalte der Spezifikation der Sicherheitsanforderungen .....	33
6.3 Zuordnung der Sicherheitsfunktion .....	35
6.4 Bestimmung des SIL-Vermögens .....	35
7 Planung von Entwurf, Entwicklung und Validierung der FS-SPS .....	36
7.1 Allgemeines .....	36
7.2 Datenkommunikation .....	37
8 Architektur einer FS-SPS .....	37
8.1 Allgemeines .....	37
8.2 Architekturen und Teilsysteme .....	38
9 Entwurf und Entwicklung der FS-SPS-HW .....	38
9.1 Allgemeine HW-Anforderungen .....	38
9.2 Spezifikation der Anforderungen an die funktionale Sicherheit der HW .....	38
9.3 Planung der Validierung der Sicherheit der HW .....	39
9.4 Entwurf und Entwicklung der HW .....	39
9.5 Integration von Hardware und Embedded Software einer FS-SPS .....	58
9.6 Hardware-Betriebs- und Instandhaltungsverfahren .....	59
9.7 Validierung der Sicherheit der HW .....	60
9.8 Verifikation der HW .....	62
10 Entwurf und Entwicklung der FS-SPS-SW .....	62
10.1 Allgemeines .....	62
10.2 Anforderungen .....	63

	Seite
10.3	Klassifizierung von Engineering-Werkzeugen..... 63
10.4	Planung der Validierung der Sicherheit der SW..... 64
11	Validierung der Sicherheit der FS-SPS..... 64
11.1	Allgemeines..... 64
12	Typprüfung der FS-SPS..... 65
12.1	Allgemeines..... 65
12.2	Anforderungen an die Typprüfung..... 65
12.3	Anforderungen an die Klimaprüfungen..... 67
12.4	Anforderungen an die mechanischen Prüfungen..... 68
12.5	EMV Prüfanforderungen..... 68
13	Verifikation der FS-SPS..... 72
13.1	Verifikationsplan..... 72
13.2	Anforderungen an den Test durch Fehlereinbau..... 73
13.3	Zustand bei der Prüfung und bei der Auslieferung..... 74
14	Beurteilung der funktionalen Sicherheit..... 75
14.1	Ziel..... 75
14.2	Anforderung an die Beurteilung..... 75
14.3	Informationen über die Beurteilung der FS-SPS..... 77
14.4	Unabhängigkeit..... 78
15	Verfahren zu Betrieb, Instandhaltung und Modifikation einer FS-SPS..... 79
15.1	Ziel..... 79
15.2	Modifikation einer FS-SPS..... 79
16	Informationen die der Hersteller der FS-SPS dem Anwender zur Verfügung stellen muss..... 80
16.1	Allgemeines..... 80
16.2	Angaben über die Übereinstimmung mit dieser Norm..... 80
16.3	Angaben über Art und Inhalt der Dokumentation..... 80
16.4	Angaben in Katalogen und/oder Datenblättern..... 80
16.5	Sicherheitshandbuch..... 80
Anhang A (informativ)	Berechnungen der Zuverlässigkeit..... 83
A.1	Allgemeines..... 83
A.2	Zuverlässigkeits-Blockdiagramm-Technik..... 83
A.3	Fehlzustandsbaumanalyse-Technik..... 83
A.4	Markov-Modellierungstechniken..... 83
Anhang B (informativ)	Typische Architekturen von FS-SPS..... 84
B.1	Beispiele für Architekturen von FS-SPS-Teilsystemen..... 84
B.2	Einkanalige FS-SPS mit einkanaligen E/A und externem Watchdog (1oo1D)..... 85
B.3	Zweikanalige Prozessoreinheit (PE) mit einkanaligen E/A und externen Watchdogs (1oo1D)..... 85
B.4	Zweikanalige Prozessoreinheit mit zweikanaligen E/A, ohne Kommunikation zwischen den Prozessoren und einer 1oo2-Abschaltlogik..... 86

	Seite
B.5 Zweikanalige Prozessoreinheit mit zweikanaligen E/A, mit Kommunikation zwischen den Prozessoren und einer 1oo2D-Abschaltlogik.....	87
B.6 Zweikanalige Prozessoreinheit mit zweikanaligen E/A, ohne Kommunikation zwischen den Prozessoren, externen Watchdogs und einer 2oo2-Abschaltlogik .....	88
B.7 Zweikanalige Prozessoreinheit mit zweikanaligen E/A, mit Kommunikation zwischen den Prozessoren, externen Watchdogs und einer 2oo2D-Abschaltlogik.....	89
B.8 Dreikanalige Prozessoreinheit mit dreikanaligen E/A, mit Kommunikation zwischen den Prozessoren und einer 2oo3D-Abschaltlogik.....	90
Anhang C (informativ) Anwendung des Prinzips „Strom fließt bei Auslösung“ .....	91
C.1 Allgemeines.....	91
C.2 Ungefährlicher Zustand und angeforderter Zustand.....	91
C.3 Zusätzlich erforderliche Angaben für die Verwendung von „Prinzip Strom fließt bei Auslösung“-Anwendungen .....	91
C.4 Besondere Betrachtungen .....	92
Anhang D (informativ) Verfügbare Ausfallraten-Datenbanken.....	93
D.1 Datenbanken.....	93
D.2 Hilfreiche Normen bezüglich des Ausfalls von Bauelementen .....	93
Anhang E (informativ) Methodiken zur Bestimmung von Ausfallraten infolge gemeinsamer Ursache in einer FS-SPS mit mehreren Kanälen.....	95
E.1 Allgemeines.....	95
E.2 Methodik.....	95
Anhang F (informativ) Literaturhinweise.....	97
<b><u>Bilder</u></b>	
Bild 1 – FS-SPS in den Sicherheitslebenszyklus-Phasen eines sicherheitsbezogenen E/E/PE-Gesamtsystems.....	8
Bild 2 – Ausfallmodell .....	24
Bild 3 – FS-SPS Sicherheitslebenszyklus (in der Realisierungsphase).....	26
Bild 4 – Relevante Teile einer Sicherheitsfunktion .....	35
Bild 5 – Beziehung zwischen FS-SPS und Engineering-Werkzeugen.....	38
Bild 6 – Aufteilung eines HW-Teilsystems.....	43
Bild 7 – Beispiel der Bestimmung des maximalen SIL für eine festgelegte Architektur.....	45
Bild 8 – Beispiel der Begrenzung der Sicherheitsintegrität der Hardware für eine mehrkanalige Sicherheitsfunktion .....	48
Bild 9 – Fehlerklassifizierung und Verhalten der FS-SPS.....	56
Bild 10 – ASIC-Entwicklungslebenszyklus (V-Modell) .....	58
Bild 11 – Modell der Schichten einer FS-SPS und der Engineering-Werkzeuge.....	63
Bild 12 – Einkanalige FS-SPS mit einkanaligen E/A und externem Watchdog (1oo1D) .....	85
Bild 13 – Zweikanalige Prozessoreinheit (PE) mit einkanaligen E/A und externen Watchdogs (1oo1D) .....	85
Bild 14 – Zweikanalige Prozessoreinheit mit zweikanaligen E/A, ohne Kommunikation zwischen den Prozessoren und einer 1oo2-Abschaltlogik .....	86
Bild 15 – Zweikanalige Prozessoreinheit mit zweikanaligen E/A, mit Kommunikation zwischen den	

	Seite
Prozessoren und einer 1oo2D-Abschaltlogik .....	87
Bild 16 – Zweikanalige Prozessoreinheit mit zweikanaligen E/A, ohne Kommunikation zwischen den Prozessoren, externen Watchdogs und einer 2oo2-Abschaltlogik .....	88
Bild 17 – Zweikanalige Prozessoreinheit mit zweikanaligen E/A, mit Kommunikation zwischen den Prozessoren, externen Watchdogs und einer 2oo2D-Abschaltlogik .....	89
Bild 18 – Dreikanalige Prozessoreinheit mit dreikanaligen E/A, mit Kommunikation zwischen den Prozessoren und einer 2oo3D-Abschaltlogik .....	90
<b><u>Tabellen</u></b>	
Tabelle 1 – Sicherheits-Integritätslevel – für Betriebsart mit niedriger Anforderungsrate .....	35
Tabelle 2 – Sicherheits-Integritätslevel – für Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung .....	36
Tabelle 3 – Fehler, die erkannt und dem Anwendungsprogramm (per Alarm) gemeldet werden .....	40
Tabelle 4 – Sicherheitsintegrität eines Hardware-Teilsystems mit niedriger Komplexität (Typ A) .....	44
Tabelle 5 – Sicherheitsintegrität eines Hardware-Teilsystems mit hoher Komplexität (Typ B) .....	45
Tabelle 6 – Fehler oder Ausfälle, die bei der Bewertung des Effekts von zufälligen HW-Ausfällen angenommen werden oder bei der Ableitung des Anteils sicherer Ausfälle in Betracht gezogen werden müssen .....	51
Tabelle 7 – Beispiele für die Klassifizierung von Werkzeugen .....	64
Tabelle 8 – Bewertungskriterien zum Betriebsverhalten .....	67
Tabelle 9 – Anforderungen an die Klimaprüfung, Langzeiteinwirkung .....	68
Tabelle 10 – Anforderungen an die mechanischen Prüfungen, Langzeitwirkung .....	68
Tabelle 11 – Prüfwerte für die Prüfung der Störfestigkeit auf Gehäuseanschlüsse .....	69
Tabelle 12 – Prüfwerte für die Störfestigkeit in allgemeiner EMV-Umgebung .....	70
Tabelle 13 – Prüfwerte für die Prüfung der Störfestigkeit auf Gehäuseanschlüsse in festgelegter EMV-Umgebung .....	71
Tabelle 14 – Prüfwerte für die Störfestigkeit in festgelegter EMV-Umgebung .....	72
Tabelle 15 – Test auf Fehlerunempfindlichkeit erforderliche Wirksamkeit .....	74
Tabelle 16 – Informationen über die Beurteilung der funktionalen Sicherheit .....	78
Tabelle 17 – Minimale Unabhängigkeitsgrade derjenigen Personen, die die Beurteilung der funktionalen Sicherheit ausführen .....	79
Tabelle 18 – Kriterien für die Bestimmung von Ausfällen mit gemeinsamer Ursache .....	95
Tabelle 19 – Festlegung des $\beta$ -Faktors für Ausfälle mit gemeinsamer Ursache .....	96