

## **Inhalt**

	Seite
Vorwort.....	2
Einleitung .....	8
1 Anwendungsbereich .....	11
2 Normative Verweisungen .....	12
3 Begriffe .....	13
4 Übereinstimmung mit dieser Norm.....	29
5 FS-SPS Sicherheitslebenszyklus .....	29
5.1 Allgemeines .....	29
5.2 Anforderungen an die funktionale Sicherheit und das SIL-Vermögen einer FS-SPS.....	31
5.3 Qualitätsmanagementsystem .....	32
5.4 Management des Sicherheitslebenszyklus der FS-SPS .....	33
6 Spezifikation der FS-SPS-Sicherheitsanforderungen .....	38
6.1 Allgemein .....	38
6.2 Inhalte der Spezifikation der Sicherheitsanforderungen .....	38
6.3 Ziel Fehlerrate .....	39
7 Planung von Entwurf, Entwicklung und Validierung der FS-SPS .....	41
7.1 Allgemeines .....	41
7.2 Aufteilungen der Anforderungen .....	41
8 Architektur einer FS-SPS .....	42
8.1 Allgemeines .....	42
8.2 Architekturen und Teilsysteme .....	42
8.3 Datenkommunikation.....	42
9 Entwurf, Entwicklung und Validierung der FS-SPS-HW .....	43
9.1 Allgemeine HW-Anforderungen.....	43
9.2 Spezifikation der Anforderungen an die funktionale Sicherheit der HW .....	43
9.3 Planung der Validierung der Sicherheit der HW .....	43
9.4 Entwurf und Entwicklung der HW.....	43
9.5 Integration von Hardware und Embedded Software in eine FS-SPS .....	62
9.6 Hardware-Betriebs- und Instandhaltungsverfahren .....	63
9.7 Validierung der Sicherheit der HW .....	64
9.8 Verifikation der HW.....	65
10 Entwurf und Entwicklung der FS-SPS-SW.....	66
10.1 Allgemeines .....	66
10.2 Anforderungen.....	67
10.3 Klassifizierung von Engineering-Werkzeugen.....	67
10.4 Planung der Validierung der Sicherheit der SW.....	68
11 Validierung der Sicherheit der FS-SPS .....	68

	Seite
12	Typprüfung der FS-SPS ..... 68
12.1	Allgemeines ..... 68
12.2	Anforderungen an die Typprüfung ..... 69
12.3	Anforderungen an die Klimaprüfungen ..... 71
12.4	Anforderungen an die mechanischen Prüfungen ..... 71
12.5	EMV Prüfanforderungen ..... 71
13	Verifikation der FS-SPS ..... 75
13.1	Verifikationsplan ..... 75
13.2	Anforderungen an den Test durch Fehlereinbau ..... 76
13.3	Zustand bei der Prüfung und bei der Auslieferung ..... 77
14	Beurteilung der funktionalen Sicherheit ..... 78
14.1	Ziel ..... 78
14.2	Anforderung an die Beurteilung ..... 78
14.3	Informationen über die Beurteilung der FS-SPS ..... 80
14.4	Unabhängigkeit ..... 81
15	Verfahren zu Betrieb, Instandhaltung und Modifikation einer FS-SPS ..... 82
15.1	Ziel ..... 82
15.2	Modifikation einer FS-SPS ..... 82
16	Informationen, die der Hersteller der FS-SPS dem Anwender zur Verfügung stellen muss ..... 82
16.1	Allgemeines ..... 83
16.2	Angaben über die Übereinstimmung mit dieser Norm ..... 83
16.3	Angaben über Art und Inhalt der Dokumentation ..... 83
16.4	Angaben in Katalogen und/oder Datenblättern ..... 83
16.5	Sicherheitshandbuch ..... 83
Anhang A (informativ) Berechnungen der Zuverlässigkeit ..... 86	
A.1	Allgemeines ..... 86
A.2	Zuverlässigkeits-Blockdiagramm-Technik ..... 86
A.3	Fehlzustandsbaumanalyse-Technik ..... 86
A.4	Markov-Modellierungstechniken ..... 86
Anhang B (informativ) Typische Architekturen von FS-SPS ..... 87	
B.1	Beispiele für Architekturen von FS-SPS-Teilsystemen ..... 87
B.2	Einkanalige FS-SPS mit einkanaligen E/A und externem Watchdog (1oo1D) ..... 88
B.3	Zweikanalige Prozessoreinheit (PE) mit einkanaligen E/A und externen Watchdogs (1oo1D) ..... 88
B.4	Zweikanalige Prozessoreinheit mit zweikanaligen E/A, ohne Kommunikation zwischen den Prozessoren und einer 1oo2-Abschaltlogik ..... 89
B.5	Zweikanalige Prozessoreinheit mit zweikanaligen E/A, mit Kommunikation zwischen den Prozessoren und einer 1oo2D-Abschaltlogik ..... 90
B.6	Zweikanalige Prozessoreinheit mit zweikanaligen E/A, ohne Kommunikation zwischen den Prozessoren, externen Watchdogs und einer 2oo2-Abschaltlogik ..... 91
B.7	Zweikanalige Prozessoreinheit mit zweikanaligen E/A, mit Kommunikation zwischen den

	Seite
Prozessoren, externen Watchdogs und einer 2oo2D-Abschaltlogik.....	92
B.8 Dreikanalige Prozessoreinheit mit dreikanaligen E/A, mit Kommunikation zwischen den Prozessoren und einer 2oo3D-Abschaltlogik .....	93
Anhang C (informativ) Anwendung des Arbeitsstromprinzips bei FS-SPSsen .....	94
C.1 Allgemeines .....	94
C.2 Sicherer und angeforderter Zustand .....	94
C.3 Zusätzlich erforderliche Angaben bei Anwendung des Arbeitsstromprinzips .....	94
C.4 Besondere Betrachtungen.....	94
Anhang D (informativ) Verfügbare Ausfallraten-Datenbanken .....	96
D.1 Datenbanken .....	96
D.2 Hilfreiche Normen bezüglich des Ausfalls von Bauelementen.....	96
Anhang E (informativ) Methode zur Schätzung der Raten der Ausfälle infolge gemeinsamer Ursache in einer FS-SPS mit mehreren Kanälen.....	98
E.1 Allgemeines .....	98
E.2 Methodik .....	98
Literaturhinweise.....	100
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen .....	103
<b>Bilder</b>	
Bild 1 – FS-SPS in den Sicherheitslebenszyklus-Phasen eines sicherheitsbezogenen E/E/PE-Gesamtsystems.....	9
Bild 2 – Ausfallmodell .....	18
Bild 3 – FS-SPS Sicherheitslebenszyklus (in der Realisierungsphase).....	30
Bild 4 – Relevante Teile einer Sicherheitsfunktion .....	40
Bild 5 – Beziehung zwischen FS-SPS und Softwarewerkzeugen .....	42
Bild 6 – Aufteilung eines HW-Teilsystems .....	48
Bild 7 – Beispiel der Bestimmung des höchsten SIL für eine festgelegte Architektur.....	50
Bild 8 – Beispiel der Begrenzung der Sicherheitsintegrität der Hardware für eine mehrkanalige Sicherheitsfunktion .....	52
Bild 9 – Fehlerklassifizierung und Verhalten der FS-SPS .....	60
Bild 10 – ASIC-Entwicklungslebenszyklus (V-Modell).....	62
Bild 11 – Modell der Schichten einer FS-SPS und der Engineering-Werkzeuge .....	66
Bild B.1 – Einkanalige FS-SPS mit einkanaligen E/A und externem Watchdog (1oo1D) .....	88
Bild B.2 – Zweikanalige Prozessoreinheit (PE) mit einkanaligen E/A und externen Watchdogs (1oo1D).....	88
Bild B.3 – Zweikanalige Prozessoreinheit mit zweikanaligen E/A, ohne Kommunikation zwischen den Prozessoren und einer 1oo2-Abschaltlogik.....	89
Bild B.4 – Zweikanalige Prozessoreinheit mit zweikanaligen E/A, mit Kommunikation zwischen den Prozessoren und einer 1oo2D-Abschaltlogik .....	90
Bild B.5 – Zweikanalige Prozessoreinheit mit zweikanaligen E/A, ohne Kommunikation zwischen den Prozessoren, externen Watchdogs und einer 2oo2-Abschaltlogik .....	91
Bild B.6 – Zweikanalige Prozessoreinheit mit zweikanaligen E/A, mit Kommunikation zwischen den Prozessoren, externen Watchdogs und einer 2oo2D-Abschaltlogik.....	92

Bild B.7 – Dreikanalige Prozessoreinheit mit dreikanaligen E/A, mit Kommunikation zwischen den Prozessoren und einer 2oo3D-Abschaltlogik.....	93
<b>Tabellen</b>	
Tabelle 1 – Sicherheits-Integritätslevel für die Betriebsart mit niedriger Anforderungsrate.....	40
Tabelle 2 – Sicherheits-Integritätslevel für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung .....	40
Tabelle 3 – Fehler, die erkannt und dem Anwendungsprogramm (per Alarm) gemeldet werden .....	44
Tabelle 4 – Sicherheitsintegrität eines Hardware-Teilsystems mit niedriger Komplexität (Typ A).....	46
Tabelle 5 – Sicherheitsintegrität eines Hardware-Teilsystems mit hoher Komplexität (Typ B) .....	46
Tabelle 6 – Fehler oder Ausfälle, die bei der Bewertung der Auswirkung zufälliger HW-Ausfälle angenommen oder bei der Herleitung des Anteils sicherer Ausfälle in Betracht gezogen werden müssen.....	55
Tabelle 7 – Beispiele für die Klassifizierung von Werkzeugen.....	67
Tabelle 8 – Bewertungskriterien zum Betriebsverhalten .....	70
Tabelle 9 – Prüfwerte für die Prüfung der Störfestigkeit auf Gehäuseanschlüsse in allgemeiner EMV Umgebung.....	72
Tabelle 10 – Prüfwerte für die Störfestigkeit in allgemeiner EMV-Umgebung .....	73
Tabelle 11 – Prüfwerte für die Prüfung der Störfestigkeit auf Gehäuseanschlüsse in festgelegter EMV-Umgebung.....	74
Tabelle 12 – Prüfwerte für die Störfestigkeit in festgelegter EMV-Umgebung.....	75
Tabelle 13 – Test auf Fehlerunempfindlichkeit, erforderliche Wirksamkeit.....	77
Tabelle 14 – Informationen über die Beurteilung der funktionalen Sicherheit .....	80
Tabelle 15 – Minimale Unabhängigkeitsgrade derjenigen Personen, die die Beurteilung der funktionalen Sicherheit ausführen.....	82
Tabelle E.1 – Kriterien für die Bestimmung von Ausfällen mit gemeinsamer Ursache.....	98
Tabelle E.2 – Festlegung des $\beta$ -Faktors für Ausfälle mit gemeinsamer Ursache .....	99