

Beginn der Gültigkeit

Diese Norm gilt ab ...

Inhalt

	Seite
Nationales Vorwort	6
Einleitung	11
1 Anwendungsbereich	12
1.1 Allgemeines	12
1.2 Rahmen dieses Teils	13
2 Normative Verweisungen	15
3 Begriffe und Abkürzungen	17
4 Übereinstimmung mit dieser Norm	31
5 FS-PLC Sicherheitslebenszyklus	31
5.1 Allgemeines	31
5.2 Anforderungen an die funktionale Sicherheit einer FS-PLC	33
5.3 Qualitätsmanagementsystem	33
5.4 Management des Sicherheitslebenszyklus der FS-PLC	34
6 Spezifikation der FS-PLC-Sicherheitsanforderungen	36
6.1 Inhalte der Spezifikation der Sicherheitsanforderungen	37
6.2 Bestimmung des SIL-Vermögens	38
7 Planung von Entwurf, Entwicklung und Validierung der FS-PLC	40
7.1 Allgemeines	40
7.2 Datenkommunikation	40
8 Architektur einer FS-PLC	41
8.1 Allgemeines	41
8.2 Architekturen und Teilsysteme	42
8.3 HW für IT-Sicherheit von Daten	43
9 Entwurf und Entwicklung der FS-PLC-HW	44
9.1 Allgemeine HW-Anforderungen	44
9.2 Spezifikation der Anforderungen an die funktionale Sicherheit der HW	44
9.3 Planung der Validierung der Sicherheit der HW	44
9.4 Entwurf und Entwicklung der HW	45
9.5 Integration von Hardware und Embedded Software einer FS-PLC	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-PLC-SW	66
10.1 Allgemeines	66

	Seite
10.2 Anforderungen.....	67
10.3 Sicherheits-Kritikalität von SW	68
10.4 Planung der Validierung der Sicherheit der SW	70
11 Planung der Validierung der Sicherheit der FS-PLC	70
11.1 Allgemeines	70
12 Typprüfung der FS-PLC	70
12.1 Allgemeines	70
12.2 Anforderungen an die Typprüfung	71
12.3 Anforderungen an die Klimaprüfungen	73
12.4 Anforderungen an die mechanischen Prüfungen.....	73
12.5 EMV Prüfanforderungen	74
13 Verifikation der FS-PLC.....	78
13.1 Verifikationsplan	78
13.2 Anforderungen an die Prüfung der Fehlertoleranz.....	79
13.3 Zustand bei der Prüfung und bei der Auslieferung	80
14 Unabhängige Beurteilung der Sicherheit	81
14.1 Ziel.....	81
14.2 Anforderung an die Beurteilung	81
14.3 Informationen über die Beurteilung der FS-PLC	83
15 Verfahren zu Betrieb, Instandhaltung und Modifikation einer FS-PLC	84
15.1 Ziel.....	84
15.2 Modifikation einer FS-PLC	84
16 Informationen die der Hersteller der FS-PLC dem Anwender zur Verfügung stellen muss	85
16.1 Allgemeines	85
16.2 Angaben über die Übereinstimmung mit dieser Norm	85
16.3 Angaben über Art und Inhalt der Dokumentation.....	85
16.4 Angaben in Katalogen und/oder Datenblättern	85
16.5 Sicherheitshandbuch.....	85
Anhang A (informativ) Berechnungen der Zuverlässigkeit.....	87
A.1 Allgemeines	87
A.2 Zuverlässigkeits-Blockdiagramm-Technik.....	87
A.3 Fehlzustandsbaumanalyse-Technik.....	87
A.4 Markov-Modellierungstechniken	87
Anhang B (informativ) Typische Architekturen von FS-PLCs	88
B.1 Beispiele für Architekturen von FS-PLC-Teilsystemen	88
B.2 Einkanalige FS-PLC mit einkanaligen E/A und externem Watchdog	89
B.3 Zweikanalige Prozessoreinheit (PE) mit einkanaligen E/A und externem Watchdog.....	89
B.4 Zweikanalige Prozessoreinheit mit zweikanaligen E/A, ohne Kommunikation zwischen den Prozessoren und einer 1oo2-Abschaltlogik	90

	Seite
B.5 Zweikanalige Prozessoreinheit mit zweikanaligen E/A, mit Kommunikation zwischen den Prozessoren und einer 1oo2-Abschaltlogik.....	91
B.6 Zweikanalige Prozessoreinheit mit zweikanaligen E/A, ohne Kommunikation zwischen den Prozessoren, externen Watchdogs und einer 2oo2-Abschaltlogik.....	92
B.7 Zweikanalige Prozessoreinheit mit zweikanaligen E/A, mit Kommunikation zwischen den Prozessoren, externen Watchdogs und einer 2oo2-Abschaltlogik.....	93
B.8 Dreikanalige Prozessoreinheit mit dreikanaligen E/A, mit Kommunikation zwischen den Prozessoren und einer 2oo3-Abschaltlogik.....	94
Anhang C (informativ) Anwendung des Prinzips „Strom fließt bei Auslösung“	95
C.1 Allgemeines	95
C.2 Ungefährlicher Zustand und angeforderter Zustand	95
C.3 Zusätzlich erforderliche Angaben für die Verwendung von „Prinzip Strom fließt bei Auslösung“-Anwendungen	95
C.4 Besondere Betrachtungen.....	96
Anhang D (informativ) Verfügbare Ausfallraten-Datenbanken	97
D.1 Datenbanken	97
D.2 Hilfreiche Normen bezüglich des Ausfalls von Bauelementen.....	97
Anhang E (informativ) Methodiken zur Bestimmung von Ausfallraten infolge gemeinsamer Ursache in einer FS-PLC mit mehreren Kanälen	99
E.1 Allgemeines	99
E.2 Methodik	99
Literaturhinweise.....	101
Bilder	
Bild 1 – FS-PLC in den Sicherheitslebenszyklus-Phasen eines sicherheitsbezogenen E/E/PE-Gesamtsystems.....	14
Bild 2 – Ausfallmodell	29
Bild 3 – FS-PLC Sicherheitslebenszyklus (in der Realisierungsphase)	32
Bild 4 – Relevante Teile einer Sicherheitsfunktion	39
Bild 5 – Beziehung zwischen HW- und SW-Architekturen von programmierbarer Elektronik, FS-PLC.....	41
Bild 6 – Beziehung zwischen FS-PLC und Engineering-Werkzeugen	42
Bild 7 – Beispiel der Begrenzung der Sicherheitsintegrität der Hardware für eine einkanalige Sicherheitsfunktion	49
Bild 8 – Beispiel der Begrenzung der Sicherheitsintegrität der Hardware für eine mehrkanalige Sicherheitsfunktion	51
Bild 9 – Aufteilung eines HW-Teilsystems	52
Bild 10 – Fehlerklassifizierung und Verhalten der FS-PLC	60
Bild 11 – Modell der Schichten einer FS-PLC und der Engineering-Werkzeuge	67
Bild 12 – Einkanalige FS-PLC mit einkanaligen E/A und externem Watchdog	89
Bild 13 – Zweikanalige Prozessoreinheit (PE) mit einkanaligen E/A und externem Watchdog	89
Bild 14 – Zweikanalige Prozessoreinheit mit zweikanaligen E/A, ohne Kommunikation zwischen den Prozessoren und einer 1oo2-Abschaltlogik.....	90
Bild 15 – Zweikanalige Prozessoreinheit mit zweikanaligen E/A, mit Kommunikation zwischen den Prozessoren und einer 1oo2-Abschaltlogik.....	91

	Seite
Bild 16 – Zweikanalige Prozessoreinheit mit zweikanaligen E/A, ohne Kommunikation zwischen den Prozessoren, externen Watchdogs und einer 2oo2-Abschaltlogik	92
Bild 17 – Zweikanalige Prozessoreinheit mit zweikanaligen E/A, mit Kommunikation zwischen den Prozessoren, externen Watchdogs und einer 2oo2-Abschaltlogik	93
Bild 18 – Dreikanalige Prozessoreinheit mit dreikanaligen E/A, mit Kommunikation zwischen den Prozessoren und einer 2oo3-Abschaltlogik	94
 Tabellen	
Tabelle 1 – Sicherheits-Integritätslevel – für Betriebsart mit niedriger Anforderungsrate	39
Tabelle 2 – Sicherheits-Integritätslevel – für Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung	39
Tabelle 3 – Architekturelle Beziehungen	42
Tabelle 4 – Fehler, die erkannt und dem Anwendungsprogramm (per Alarm) gemeldet werden	46
Tabelle 5 – Sicherheitsintegrität eines Hardware-Teilsystems mit niedriger Komplexität (Typ A)	48
Tabelle 6 – Sicherheitsintegrität eines Hardware-Teilsystems mit hoher Komplexität (Typ B)	48
Tabelle 7 – Fehler oder Ausfälle, die während des Betriebs erkannt oder zur Bestimmung des Anteils sicherer Ausfälle analysiert werden müssen	55
Tabelle 8 – Beispiele für die Klassifizierung der Kritikalität von Werkzeugen	68
Tabelle 9 – Verhältnis des Sicherheits-Integritätslevels der Sicherheitsfunktion einer FS-PLC zur Kritikalität des Elements und der erforderlichen SIL-Erreichung des Elements	69
Tabelle 10 – Bewertungskriterien zum Betriebsverhalten	72
Tabelle 11 – Anforderungen an die Klimaprüfung, Langzeiteinwirkung	73
Tabelle 12 – Anforderungen an die mechanischen Prüfungen, Langzeitwirkung	74
Tabelle 13 – Prüfwerte für die Prüfung der Störfestigkeit auf Gehäuseanschlüsse	74
Tabelle 14 Prüfwerte für die Störfestigkeit in allgemeiner EMV-Umgebung	75
Tabelle 15 – Prüfwerte für die Prüfung der Störfestigkeit auf Gehäuseanschlüsse in festgelegter EMV-Umgebung	77
Tabelle 16 – Prüfwerte für die Störfestigkeit in festgelegter EMV-Umgebung	78
Tabelle 17 – Anforderungen an die Prüfung der Fehlertoleranz	79
Tabelle 18 – Anforderungen an die Prüfung der Fehlertoleranz bei hoher Verfügbarkeit	80
Tabelle 19 – Informationen über die Beurteilung der funktionalen Sicherheit	84
Tabelle 20 – Kriterien für die Bestimmung von Ausfällen mit gemeinsamer Ursache	99
Tabelle 21 – Festlegung des β -Faktors für Ausfälle mit gemeinsamer Ursache	100