

## Anwendungsbeginn

Anwendungsbeginn dieser Norm ist ...

### Inhalt

	Seite
Nationales Vorwort.....	7
Nationaler Anhang NA (informativ) Zusammenhang mit Europäischen und Internationalen Normen.....	8
Nationaler Anhang NB (informativ) Literaturhinweise.....	9
0 Einleitung.....	11
0.1 Allgemeines.....	11
0.2 Übergang von Ausgabe 2 zu erweiterten Prüfmethode n in Ausgabe 3.....	13
0.3 Patentangaben.....	13
1 Anwendungsbereich.....	15
2 Normative Verweisungen.....	15
3 Begriffe, Symbole, Abkürzungen und Konventionen.....	17
3.1 Begriffe.....	17
3.2 Symbole und Abkürzungen.....	24
4 Konformität.....	25
5 Grundlagen von sicherheitsrelevanten Feldbussystemen.....	26
5.1 Struktur einer Sicherheitsfunktion.....	26
5.2 Kommunikationssystem.....	27
5.3 Kommunikationsfehler.....	28
5.4 Deterministische Abhilfemaßnahmen.....	30
5.5 Typische Beziehungen zwischen Fehlern und Sicherheitsmaßnahmen.....	32
5.6 Kommunikationsphasen.....	33
5.7 FSCP-Implementierungsaspekte.....	33
5.8 Betrachtungen zur Datenintegrität.....	34
5.9 Beziehungen zwischen funktionaler Sicherheit und IT-Sicherheit.....	36
5.10 Randbedingungen und Auflagen.....	37
5.9 Installationsleitfäden.....	38
5.10 Sicherheitshandbuch.....	38
5.11 Sicherheitsgrundsätze (Policy).....	38
6 Kommunikationsprofilfamilie 1 (FOUNDATION™ Fieldbus) – Profil für funktionale Sicherheit.....	39
7 Kommunikationsprofilfamilie 2 (CIP™) und Familie 16 (SERCOS™) – Profile für funktionale Sicherheit.....	39
8 Kommunikationsprofilfamilie 3 (PROFIBUS™, PROFINET™) – Profil für funktionale Sicherheit.....	40
9 Kommunikationsprofilfamilie 6 (INTERBUS®) – Profil für funktionale Sicherheit.....	40
10 Kommunikationsprofilfamilie 8 (CC-Link™) – Profile für funktionale Sicherheit.....	41
10.1 Funktional sicheres Kommunikationsprofil 8/1.....	41
10.2 Funktional sicheres Kommunikationsprofil 8/2.....	41

	Seite
11 Kommunikationsprofilfamilie 12 (EtherCAT™) – Profile für funktionale Sicherheit .....	41
12 Kommunikationsprofilfamilie 13 (Ethernet POWERLINK™) – Profile für funktionale Sicherheit .....	41
13 Kommunikationsprofilfamilie 14 (EPA®) – Profile für funktionale Sicherheit .....	42
14 Kommunikationsprofilfamilie 17 (RAPInet™) – Profile für funktionale Sicherheit.....	42
15 Kommunikationsprofilfamilie 18 (SafetyNET p™) – Profile für funktionale Sicherheit.....	42
Anhang A (informativ) Beispiele für funktional sichere Kommunikationsmodelle .....	43
A.1 Allgemeines.....	43
A.2 Modell A (Einzelnachricht, Kanal und FAL, redundante SCLs) .....	43
A.3 Modell B (Volle Redundanz) .....	43
A.4 Modell C (redundante Nachrichten, FALs und SCLs, ein Kanal).....	44
A.5 Modell D (redundante Nachrichten und SCLs, ein Kanal und FAL) .....	45
Anhang B (normativ) Ein Kanalmodell für sichere Kommunikation unter Einsatz von CRC-basierten Fehlerprüfungen.....	46
B.1 Übersicht .....	46
B.2 Kanalmodell für Berechnungen.....	46
B.3 Bitfehlerwahrscheinlichkeit $P_e$ .....	47
B.4 CRC-Prüfung.....	48
B.4.1 Allgemeines.....	48
B.4.2 Betrachtungen zu CRC-Polynomen.....	49
Anhang C (informativ) Struktur der technologiespezifischen Teile .....	51
Anhang D (informativ) Prüfungsleitfaden .....	54
D.1 Übersicht .....	54
D.2 Kanaltypen .....	54
D.2.1 Allgemeines.....	54
D.2.2 „Black Channel“ .....	54
D.2.3 „White Channel“ .....	54
D.3 Überlegungen zur Datensicherung bei „White Channel“-Ansätzen .....	55
D.3.1 Allgemeines.....	55
D.3.2 Modell B und Modell C .....	55
D.3.3 Modell A und Modell D .....	56
D.4 Verifikation der Sicherheitsmaßnahmen .....	57
D.4.1 Allgemeines.....	57
D.4.2 Implementierung.....	57
D.4.3 „Ruhestromprinzip“.....	57
D.4.4 Sicherer Zustand .....	57
D.4.5 Übertragungsfehler .....	57
D.4.6 Sicherheitsreaktions- und Antwortzeiten.....	57
D.4.7 Kombinierte Maßnahmen.....	57
D.4.8 Rückwirkungsfreiheit .....	58

	Seite
D.4.9 Weitere Fehlerfälle („White Channel“)	58
D.4.10 Referenztestanlagen und Betriebsbedingungen	58
D.4.11 Konformitäts-Tester	58
Anhang E (informativ) Beispiele für implizite FSCP-Mechanismen	59
E.1 Allgemeines	59
E.2 Beispiel für Feldbus-Nachricht mit Sicherheits-PDUs	59
E.3 Modell mit vollständig expliziten Sicherungsmechanismen	59
E.4 Modell mit expliziten A-Code- und impliziten T-Code-Sicherungsmechanismen	60
E.5 Modell mit expliziten T-Code- und impliziten A-Code-Sicherungsmechanismen	61
E.6 Modell mit gemischt expliziten und impliziten Sicherungsmechanismen	62
E.7 Modell mit vollständig impliziten Sicherungsmechanismen	63
E.8 Ergänzung zu Anhang B – Einfluss der impliziten Daten auf die „Properness“	64
Anhang F (informativ) Erweiterte Modelle für die Abschätzung der gesamten Restfehlerrate	65
F.1 Geltungsbereich	65
F.2 Allgemeine Modelle für die „Black-Channel“-Kommunikation	65
F.3 Die Grund-Sicherheitseigenschaften	66
F.4 Annahmen für die Berechnung der Restfehler	66
F.5 Restfehlerraten	67
F.5.1 Explizite und implizite Mechanismen	67
F.5.2 Berechnungen der Restfehlerraten	67
F.6 Datenintegrität	68
F.6.1 Probabilistische Betrachtungen	68
F.6.2 Deterministische Betrachtungen	68
F.7 Authentizität	68
F.7.1 Allgemeines	68
F.7.2 Restfehlerrate für Authentizität ( $RR_A$ )	70
F.8 Aktualität (Timeliness)	71
F.8.1 Allgemeines	71
F.8.2 Restfehlerrate für Aktualität ( $RR_T$ )	73
F.9 Maskerade	74
F.9.1 Allgemeines	74
F.9.2 Restfehlerrate für die Abweisung von Maskerade ( $RR_M$ )	74
F.10 Berechnung der Gesamtrestfehlerrate für den SCL	74
F.10.1 Auf Basis der Summe der Restfehlerraten	74
F.10.2 Auf Basis anderer quantitativer Nachweise	76
F.11 Gesamtfehlerrate und SIL	76
F.12 Konfiguration und Parametrierung eines FSCP	77
F.12.1 Allgemeines	77
F.12.2 Änderungsrate der Konfiguration und Parametrierung	78

	Seite
F.12.3 Restfehlerrate für die Konfiguration und Parametrierung .....	79
Literaturhinweise .....	80
<b><u>Bilder</u></b>	
Bild 1 – Beziehungen der IEC 61784-3 mit anderen Normen (Fertigung) .....	11
Bild 2 – Beziehungen der IEC 61784-3 zu anderen Normen (Prozess) .....	12
Bild 3 – Übergang von den Prüfmethode der Ausgabe 2 zur Ausgabe 3 .....	13
Bild 4 – Sichere Kommunikation als Teil einer Sicherheitsfunktion .....	26
Bild 5 – Modellbeispiel für ein funktional sicheres Kommunikationssystem .....	27
Bild 6 – Beispiel für die Reaktionszeitkette einer Sicherheitsfunktion.....	28
Bild 7 – Konzeptionelles FSCP Protokollmodell.....	33
Bild 8 – Implementierungsaspekte eines FSCP .....	34
Bild 9 – Anwendungsbeispiel 1 (m=4).....	35
Bild 10 – Anwendungsbeispiel 2 (m=2).....	36
Bild 11 – Zonen und Durchleitungskonzept für IT-Sicherheit gemäß IEC 62443 .....	37
Bild A.1 – Modell A .....	43
Bild A.2 – Modell B .....	44
Bild A.3 – Modell C .....	44
Bild A.4 – Modell D .....	45
Bild B.1 – Kommunikationskanal mit Störungen .....	46
Bild B.2 – Binärsymmetrischer Kanal (BSC) .....	47
Bild B.3 – Beispiel eines Blocks mit Nachricht und CRC-Bits (redundanter Code) .....	48
Bild B.4 – Blockcodes zur Fehleraufdeckung.....	49
Bild B.5 – Propere und nicht propere CRC-Polynome .....	50
Bild D.1 – Grundlegendes Markov-Modell.....	56
Bild E.1 – Sicherheits-PDU-Beispiele in einer Feldbusnachricht .....	59
Bild E.2 – Modell mit vollständig expliziten Sicherungsmechanismen.....	60
Bild E.3 – Modell mit explizitem A-Code- und implizitem T-Code-Sicherungsmechanismus .....	61
Bild E.4 – Modell mit explizitem T-Code- und implizitem A-Code-Sicherungsmechanismus .....	62
Bild E.5 – Modell mit gemischtem explizitem und implizitem Sicherungsmechanismus .....	63
Bild E.6 – Modell mit vollständig impliziten Sicherungsmechanismen .....	63
Bild F.1 – „Black Channel“ aus der Sicht des FSCP .....	65
Bild F.2 – Modell für die Authentizitäts-Betrachtung .....	69
Bild F.3 – Feldbus- und interne Adressfehler .....	70
Bild F.4 – Beispiel einer allmählich ansteigenden Nachrichten-Latenzzeit.....	72
Bild F.5 – Beispiel für das Versagen eines aktiven Netzwerkelements .....	73
Bild F.6 – Anwendungsbeispiel 1 (m=4).....	76
Bild F.7 – Anwendungsbeispiel 2 (m=2).....	76
Bild F.8 – Beispiel mit Konfigurier- und Parametriervorgängen für FSCPs .....	77
<b><u>Tabellen</u></b>	
Tabelle 1 – Überblick über die Wirksamkeit von Maßnahmen gegen mögliche Fehler .....	32

	Seite
Tabelle 2 – Definition der Größen für die Berechnung der Restfehlerrate .....	35
Tabelle 3 – Typische Beziehung zwischen Restfehlerrate und SIL .....	36
Tabelle 4 – Übersicht über Profilkennungen für FSCP 6/7 .....	40
Tabelle B.1 – Beispiel für die Abhängigkeit von $d_{\min}$ und Blocklänge $n$ .....	49
Tabelle C.1 – Gemeinsame Gliederung der technologiespezifischen Teile (1 von 3) .....	51
Tabelle F.1 – Restfehlerraten für die FSCP-Kategorie „explizit“ (Beispiele) .....	67
Tabelle F.2 – Definition der Elemente für die Berechnung von $RR_1$ .....	75
Tabelle F.3 – Definition der Elemente für die Berechnung der Restfehlerrate.....	75
Tabelle F.4 – Typische Beziehung zwischen Restfehlerrate und SIL .....	77