

Anwendungsbeginn

Anwendungsbeginn dieser Norm ist ...

Inhalt

	Seite
0 Einleitung	9
0.1 Allgemeines	9
0.2 Anwendung von erweiterten Bewertungsmethoden in Ausgabe 4	13
0.3 Patentangaben	15
1 Anwendungsbereich	16
2 Normative Verweisungen	16
3 Begriffe, Symbole, Abkürzungen und Konventionen.....	18
3.1 Begriffe	18
3.2 Symbole und Abkürzungen	26
3.2.1 Abkürzungen	26
3.2.2 Symbole.....	28
4 Konformität	28
5 Grundlagen von sicherheitsbezogenen Feldbussystemen	29
5.1 Struktur einer Sicherheitsfunktion	29
5.2 Kommunikationssystem.....	30
5.2.1 Allgemeines	30
5.2.2 Feldbusse der IEC 61158.....	30
5.2.3 Kommunikationskanaltypen	31
5.2.4 Reaktionszeit einer Sicherheitsfunktion	31
5.3 Kommunikationsfehler	32
5.3.1 Allgemeines	32
5.3.2 Verfälschung.....	32
5.3.3 Unbeabsichtigte Wiederholung	33
5.3.4 Falsche Reihenfolge.....	33
5.3.5 Verlust	33
5.3.6 Unzulässige Verzögerung	33
5.3.7 Einfügung	33
5.3.8 Maskerade.....	34
5.3.9 Adressierung	34
5.4 Deterministische Abhilfemaßnahmen.....	34
5.4.1 Allgemeines	34
5.4.2 Laufende Nummer.....	34
5.4.3 Zeitstempel	34
5.4.4 Zeiterwartung.....	34
5.4.5 Verbindungsauthentifizierung.....	35

	Seite
5.4.6	Rückmeldung 35
5.4.7	Sicherung der Datenintegrität 35
5.4.8	Redundanz mit Kreuzvergleich 35
5.4.9	Unterschiedliche Sicherungssysteme für die Datenintegrität 35
5.5	Typische Beziehungen zwischen Fehlern und Sicherheitsmaßnahmen 36
5.6	Kommunikationsphasen 37
5.7	FSCP-Implementierungsaspekte 38
5.8	Modelle für die Abschätzung der Gesamt-Restfehlerrate 39
5.8.1	Geltungsbereich 39
5.8.2	Allgemeine Modelle für die Black-Channel-Kommunikation 39
5.8.3	Beschreibung der Grund-Sicherheitseigenschaften 41
5.8.4	Annahmen für die Berechnung der Restfehler 41
5.8.5	Restfehlerraten 42
5.8.6	Datenintegrität 44
5.8.7	Authentizität 44
5.8.8	Aktualität 47
5.8.9	Maskerade 50
5.8.10	Berechnung der Gesamt-Restfehlerraten 50
5.8.11	Gesamt-Restfehlerrate und SIL 52
5.8.12	Konfiguration und Parametrierung eines FSCP 53
5.9	Beziehungen zwischen funktionaler Sicherheit und IT-Sicherheit 55
5.10	Randbedingungen und Auflagen 56
5.10.1	Elektrische Sicherheit 56
5.10.2	Elektromagnetische Verträglichkeit (EMV) 56
5.11	Installationsleitfäden 56
5.12	Sicherheitshandbuch 56
5.13	Sicherheitsgrundsätze (Policy) 57
6	Kommunikationsprofilfamilie 1 (Foundation™ Fieldbus) – Profile für funktionale Sicherheit 57
7	Kommunikationsprofilfamilie 2 (CIP™) und Familie 16 (SERCOS®) – Profile für funktionale Sicherheit 58
8	Kommunikationsprofilfamilie 3 (PROFIBUS™, PROFINET™) – Profile für funktionale Sicherheit 58
9	Kommunikationsprofilfamilie 6 (INTERBUS®) – Profile für funktionale Sicherheit 58
10	Kommunikationsprofilfamilie 8 (CC-Link™) – Profile für funktionale Sicherheit 59
10.1	Funktional sicheres Kommunikationsprofil 8/1 59
10.2	Funktional sicheres Kommunikationsprofil 8/2 59
11	Kommunikationsprofilfamilie 12 (EtherCAT™) – Profile für funktionale Sicherheit 60
12	Kommunikationsprofilfamilie 13 (Ethernet POWERLINK™) – Profile für funktionale Sicherheit 60
13	Kommunikationsprofilfamilie 14 (EPA®) – Profile für funktionale Sicherheit 60

	Seite
14	Kommunikationsprofilfamilie 17 (RAPIEnet™) – Profile für funktionale Sicherheit..... 60
15	Kommunikationsprofilfamilie 18 (SafetyNET p™ Fieldbus) – Profile für funktionale Sicherheit 61
	Anhang A (informativ) Beispiele für funktional sichere Kommunikationsmodelle 62
A.1	Allgemeines 62
A.2	Modell A (Einzelnachricht, Kanal und FAL, redundante SCLs)..... 62
A.3	Modell B (vollständige Redundanz)..... 62
A.4	Modell C (redundante Nachrichten, FALs und SCLs, einkanalig)..... 63
A.5	Modell D (redundante Nachrichten und SCLs, einkanalig und FAL) 64
	Anhang B (normativ) Kanalmodell für sichere Kommunikation unter Einsatz von CRC-basierten Fehlerprüfungen 65
B.1	Übersicht 65
B.2	Kanalmodell für Berechnungen 65
B.3	Bitfehlerwahrscheinlichkeit P_e 67
B.4	Zyklische Redundanzprüfung 67
B.4.1	Allgemeines 67
B.4.2	Anforderungen an die Methoden für die Berechnung von R_{CRC} 69
	Anhang C (informativ) Struktur der technologiespezifischen Teile..... 71
	Anhang D (informativ) Bewertungsleitfaden 73
D.1	Übersicht 73
D.2	Kanaltypen..... 73
D.2.1	Allgemeines 73
D.2.2	Black Channel 73
D.2.3	White Channel 73
D.3	Überlegungen zur Datenintegrität bei „White Channel“-Ansätzen 74
D.3.1	Allgemeines 74
D.3.2	Modell B und Modell C 74
D.3.3	Modell A und Modell D 75
D.4	Verifikation der Sicherheitsmaßnahmen 76
D.4.1	Allgemeines 76
D.4.2	Implementierung..... 76
D.4.3	„Ruhestromprinzip“ 76
D.4.4	Sicherer Zustand 76
D.4.5	Übertragungsfehler..... 76
D.4.6	Sicherheitsreaktions- und Antwortzeiten 76
D.4.7	Kombinierte Maßnahmen 77
D.4.8	Rückwirkungsfreiheit 77
D.4.9	Weitere Fehlerfälle (White Channel) 77
D.4.10	Referenzprüfanlagen und Betriebsbedingungen..... 77
D.4.11	Konformitätsprüfer 77

	Seite
Anhang E (informativ) Beispiele für implizite FSCP-Sicherheitsmaßnahmen gegenüber expliziten FSCP-Sicherheitsmaßnahmen	78
E.1 Allgemeines	78
E.2 Beispiel für eine Feldbusnachricht mit Sicherheits-PDUs	78
E.3 Modell mit ausschließlich expliziten Sicherheitsmaßnahmen	78
E.4 Modell mit explizitem A-Code und implizitem T-Code als Sicherheitsmaßnahmen	80
E.5 Modell mit explizitem T-Code und implizitem A-Code als Sicherheitsmaßnahmen	80
E.6 Modell mit teilweise expliziten und teilweise impliziten Sicherheitsmaßnahmen	81
E.7 Modell mit ausschließlich impliziten Sicherheitsmaßnahmen	82
E.8 Ergänzung zu Anhang B – Einfluss der impliziten Daten auf die „Properness“	83
Anhang F (informativ) Vorgängermodelle für die Abschätzung der Gesamt-Restfehlerrate	84
F.1 Allgemeines	84
F.2 Berechnung der Restfehlerrate	84
F.3 Gesamt-Restfehlerrate und SIL	86
Anhang G (informativ) Implizite Datensicherungsmechanismen für funktional sichere Kommunikationsprofile (FSCPs) nach IEC 61784-3	88
G.1 Übersicht	88
G.2 Grundprinzipien	88
G.3 Problemstellung: konstante Werte für implizite Daten	90
G.4 RP für FSCPs mit einer zufälligen, gleichverteilten Variable err_{impl}	92
G.4.1 Allgemeines	92
G.4.2 Gleichverteilung innerhalb des Intervalls $[0;2^i-1]$, $i \geq r$	93
G.4.3 Gleichverteilung innerhalb des Intervalls $[1;2^r-1]$, $i \geq r$	95
G.5 Allgemeiner Fall	97
G.6 Berechnung von P_{ID}	98
Literaturhinweise	100
Bilder	
Bild 1 – Beziehungen der IEC 61784-3 zu anderen Normen (Fertigung)	11
Bild 2 – Beziehungen von IEC 61784-3 zu anderen Normen (Prozess)	12
Bild 3 – Übergänge von den Bewertungsmethoden der Ausgabe 2 zu Bewertungsmethoden der Ausgabe 4	14
Bild 4 – Sichere Kommunikation als Teil einer Sicherheitsfunktion	29
Bild 5 – Modellbeispiel für ein funktional sicheres Kommunikationssystem	31
Bild 6 – Beispiel für die Reaktionszeitkette einer Sicherheitsfunktion	32
Bild 7 – Konzeptionelles FSCP-Protokollmodell	38
Bild 8 – Implementierungsaspekte eines FSCP	39
Bild 9 – Black Channel aus der Sicht des FSCP	40
Bild 10 – Modell für die Betrachtung der Authentifizierung	45
Bild 11 – Feldbus- und interne Adressfehler	46

	Seite
Bild 12 – Beispiel einer allmählich ansteigenden Nachrichten-Latenzzeit	48
Bild 13 – Beispiel für das Versagen eines aktiven Netzelements	49
Bild 14 – Anwendungsbeispiel 1 ($m = 4$).....	51
Bild 15 – Anwendungsbeispiel 2 ($m = 2$).....	52
Bild 16 – Beispiel mit Konfigurier- und Parametriervorgängen für FSCP	54
Bild A.1 – Modell A.....	62
Bild A.2 – Modell B.....	63
Bild A.3 – Modell C	63
Bild A.4 – Modell D	64
Bild B.1 – Kommunikationskanal mit Störungen.....	66
Bild B.2 – Binärsymmetrischer Kanal (BSC)	66
Bild B.3 – Beispiel eines Blocks mit Nachrichtenteil und CRC-Signatur	68
Bild B.4 – Blockcodes zur Fehlererkennung.....	68
Bild B.5 – Propere und nicht propere CRC-Polynome	70
Bild D.1 – Grundlegendes Markov-Modell.....	75
Bild E.1 – Beispiel von Sicherheits-PDUs in einer Feldbusnachricht	78
Bild E.2 – Modell mit ausschließlich expliziten Sicherheitsmaßnahmen	79
Bild E.3 – Modell mit explizitem A-Code und implizitem T-Code als Sicherheitsmaßnahmen.....	80
Bild E.4 – Modell mit explizitem T-Code und implizitem A-Code als Sicherheitsmaßnahmen.....	81
Bild E.5 – Modell mit teilweise expliziten und teilweise impliziten Sicherheitsmaßnahmen.....	82
Bild E.6 – Modell mit ausschließlich impliziten Sicherheitsmaßnahmen	83
Bild F.1 – Anwendungsbeispiel 1 ($m = 4$)	85
Bild F.2 – Anwendungsbeispiel 2 ($m = 2$)	86
Bild G.1 – FSCP mit der impliziten Übertragung des Authentizitätscodes und/oder des Aktualitätscodes	89
Bild G.2 – Beispiel für eine falsche Übertragung mit mehreren Fehlerfällen	90
Bild G.3 – Auswirkung von Fehlern in impliziten Daten auf die Restfehlerwahrscheinlichkeit.....	91
Tabellen	
Tabelle 1 – Überblick über die Wirksamkeit von Maßnahmen gegen mögliche Fehler	37
Tabelle 2 – Typische Beziehung zwischen Restfehlerrate und SIL	53
Tabelle 3 – Typische Beziehung zwischen Restfehler auf Anforderung und SIL.....	53
Tabelle 4 – Übersicht über Profilkennungen für FSCP 6/7	59
Tabelle B.1 – Beispiel für die Abhängigkeit von d_{\min} und Blockbitlänge n	69
Tabelle C.1 – Gemeinsame Gliederung der technologiespezifischen Teile.....	71
Tabelle F.1 – Definition der Größen für die Berechnung der Restfehlerraten.....	85
Tabelle F.2 – Typische Beziehung zwischen Restfehlerrate und SIL	86
Tabelle F.3 – Typische Beziehung zwischen tfehler auf Anforderung und SIL	87