

Inhalt

	Seite
Europäisches Vorwort	2
0 Einleitung.....	8
0.1 Allgemeines.....	8
0.2 Übergang von Ausgabe 2 zu erweiterten Bewertungsmethoden in Ausgabe 3	10
0.3 Patentangaben.....	11
1 Anwendungsbereich.....	12
2 Normative Verweisungen	12
3 Begriffe, Symbole, Abkürzungen und Konventionen	14
3.1 Begriffe.....	14
3.2 Symbole und Abkürzungen.....	22
4 Konformität.....	23
5 Grundlagen von sicherheitsbezogenen Feldbussystemen	23
5.1 Struktur einer Sicherheitsfunktion	23
5.2 Kommunikationssystem	24
5.2.1 Allgemeines.....	24
5.2.2 Feldbusse der IEC 61158	24
5.2.3 Kommunikationskanaltypen	25
5.2.4 Reaktionszeit einer Sicherheitsfunktion.....	25
5.3 Kommunikationsfehler.....	26
5.3.1 Allgemeines.....	26
5.3.2 Verfälschung	26
5.3.3 Unbeabsichtigte Wiederholung.....	26
5.3.4 Falsche Abfolge	27
5.3.5 Verlust	27
5.3.6 Inakzeptable Verzögerung	27
5.3.7 Einfügung	27
5.3.8 Maskerade	27
5.3.9 Adressierung	27
5.4 Deterministische Abhilfemaßnahmen	27
5.4.1 Allgemeines.....	27
5.4.2 Laufende Nummer	28
5.4.3 Zeitstempel.....	28
5.4.4 Zeiterwartung	28
5.4.5 Verbindungsauthentizität.....	28
5.4.6 Rückmeldung	28
5.4.7 Datensicherung.....	28
5.4.8 Redundanz mit Kreuzvergleich	29
5.4.9 Unterschiedliche Sicherungssysteme für die Datenintegrität	29

	Seite
5.5	Typische Beziehungen zwischen Fehlern und Sicherheitsmaßnahmen..... 29
5.6	Kommunikationsphasen 30
5.7	FSCP-Implementierungsaspekte 31
5.8	Betrachtungen zur Datenintegrität..... 32
5.8.1	Berechnung der Restfehlerrate 32
5.8.2	Gesamtrestfehlerrate und SIL 33
5.9	Beziehungen zwischen funktionaler Sicherheit und IT-Sicherheit 34
5.10	Randbedingungen und Auflagen..... 35
5.10.1	Elektrische Sicherheit..... 35
5.10.2	Elektromagnetische Verträglichkeit (EMV)..... 35
5.11	Installationsleitfäden 36
5.12	Sicherheitshandbuch 36
5.13	Sicherheitsgrundsätze (Policy)..... 36
6	Kommunikationsprofilfamilie 1 (Foundation™ Fieldbus) – Profile für funktionale Sicherheit..... 37
7	Kommunikationsprofilfamilie 2 (CIP™) und Familie 16 (SERCOS®) – Profile für funktionale Sicherheit..... 37
8	Kommunikationsprofilfamilie 3 (PROFIBUS™, PROFINET™) – Profile für funktionale Sicherheit..... 37
9	Kommunikationsprofilfamilie 6 (INTERBUS®) – Profile für funktionale Sicherheit 38
10	Kommunikationsprofilfamilie 8 (CC-Link™) – Profile für funktionale Sicherheit 38
10.1	Funktional sicheres Kommunikationsprofil 8/1 38
10.2	Funktional sicheres Kommunikationsprofil 8/2 39
11	Kommunikationsprofilfamilie 12 (EtherCAT™) – Profile für funktionale Sicherheit..... 39
12	Kommunikationsprofilfamilie 13 (Ethernet POWERLINK™) – Profile für funktionale Sicherheit..... 39
13	Kommunikationsprofilfamilie 14 (EPA®) – Profile für funktionale Sicherheit 40
14	Kommunikationsprofilfamilie 17 (RAPIEnet™) – Profile für funktionale Sicherheit..... 40
15	Kommunikationsprofilfamilie 18 (SafetyNET p™) – Profile für funktionale Sicherheit..... 40
Anhang A (informativ) Beispiele für funktional sichere Kommunikationsmodelle 41	
A.1	Allgemeines 41
A.2	Modell A (Einzelnachricht, Kanal und FAL, redundante SCLs)..... 41
A.3	Modell B (vollständige Redundanz)..... 41
A.4	Modell C (redundante Nachrichten, FALs und SCLs, einkanalig)..... 42
A.5	Modell D (redundante Nachrichten und SCLs, einkanalig und FAL) 42
Anhang B (normativ) Kanalmodell für sichere Kommunikation unter Einsatz von CRC-basierten Fehlerprüfungen 44	
B.1	Übersicht 44
B.2	Kanalmodell für Berechnungen 44
B.3	Bitfehlerwahrscheinlichkeit P_e 45
B.4	CRC-Prüfung 45

	Seite
B.4.1 Allgemeines	45
B.4.2 Betrachtungen zu CRC-Polynomen	47
Anhang C (informativ) Struktur der technologiespezifischen Teile	49
Anhang D (informativ) Bewertungsleitfaden	51
D.1 Übersicht	51
D.2 Kanaltypen	51
D.2.1 Allgemeines	51
D.2.2 „Black Channel“	51
D.2.3 „White Channel“	51
D.3 Überlegungen zur Datensicherung bei „White Channel“-Ansätzen	52
D.3.1 Allgemeines	52
D.3.2 Modell B und Modell C	52
D.3.3 Modell A und Modell D	53
D.4 Verifikation der Sicherheitsmaßnahmen	54
D.4.1 Allgemeines	54
D.4.2 Implementierung	54
D.4.3 „Ruhestromprinzip“	54
D.4.4 Sicherer Zustand	54
D.4.5 Übertragungsfehler	54
D.4.6 Sicherheitsreaktions- und Antwortzeiten	54
D.4.7 Kombinierte Maßnahmen	55
D.4.8 Rückwirkungsfreiheit	55
D.4.9 Weitere Fehlerfälle („White Channel“)	55
D.4.10 Referenztestanlagen und Betriebsbedingungen	55
D.4.11 Konformitäts-Tester	55
Anhang E (informativ) Beispiele für implizite FSCP-Mechanismen	56
E.1 Allgemeines	56
E.2 Beispiel für Feldbus-Nachricht mit Sicherheits-PDUs	56
E.3 Modell mit ausschließlich expliziten Sicherungsmechanismen	56
E.4 Modell mit explizitem A-Code- und implizitem T-Code-Sicherungsmechanismus	57
E.5 Modell mit explizitem T-Code- und implizitem A-Code-Sicherungsmechanismus	57
E.6 Modell mit teilweise expliziten und teilweise impliziten Sicherungsmechanismen	58
E.7 Modell mit ausschließlich impliziten Sicherungsmechanismen	59
E.8 Ergänzung zu Anhang B – Einfluss der impliziten Daten auf die „Properness“	59
Anhang F (informativ) Erweiterte Modelle für die Abschätzung der gesamten Restfehlerrate	60
F.1 Geltungsbereich	60
F.2 Allgemeine Modelle für die „Black-Channel“-Kommunikation	60
F.3 Die Grund-Sicherheitseigenschaften	61
F.4 Annahmen für die Berechnung der Restfehler	61

	Seite
F.5 Restfehlerraten	62
F.5.1 Explizite und implizite Mechanismen.....	62
F.5.2 Berechnungen der Restfehlerraten	62
F.5.2.1 Allgemeines	62
F.5.2.2 Beitrag von Datenintegritätsfehlern (RR_I)	63
F.5.2.3 Beitrag von Authentizitätsfehlern (RR_A).....	63
F.5.2.4 Beitrag von Aktualitätsfehlern (RR_T)	63
F.5.2.5 Beitrag von Maskeradefehlern (RR_M)	64
F.6 Datenintegrität	64
F.6.1 Probabilistische Betrachtungen.....	64
F.6.2 Deterministische Betrachtungen	64
F.7 Authentizität.....	65
F.7.1 Allgemeines	65
F.7.2 Restfehlerrate für Authentizität (RR_A)	66
F.8 Aktualität (en: Timeliness).....	67
F.8.1 Allgemeines	67
F.8.2 Restfehlerrate für Aktualität (RR_T)	69
F.9 Maskerade	70
F.9.1 Allgemeines	70
F.9.2 Restfehlerrate für die Abweisung von Maskerade (RR_M)	70
F.10 Berechnung der Gesamtrestfehlerrate für die SCL.....	70
F.10.1 Auf Basis der Summe der Restfehlerraten.....	70
F.10.2 Auf Basis anderer quantitativer Nachweise.....	71
F.11 Gesamtfehlerrate und SIL	72
F.12 Konfiguration und Parametrierung eines FSCP	72
F.12.1 Allgemeines	72
F.12.2 Änderungsrate der Konfiguration und Parametrierung	74
F.12.3 Restfehlerrate für die Konfiguration und Parametrierung.....	74
Literaturhinweise.....	75
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	78
Bilder	
Bild 1 – Beziehungen der IEC 61784-3 zu anderen Normen (Fertigung).....	8
Bild 2 – Beziehungen der IEC 61784-3 zu anderen Normen (Prozess).....	9
Bild 3 – Übergang von den Bewertungsmethoden der Ausgabe 2 zu denen der Ausgabe 3.....	10
Bild 4 – Sichere Kommunikation als Teil einer Sicherheitsfunktion.....	24
Bild 5 – Modellbeispiel für ein funktional sicheres Kommunikationssystem.....	25
Bild 6 – Beispiel für die Reaktionszeitkette einer Sicherheitsfunktion	26

	Seite
Bild 7 – Konzeptionelles FSCP-Protokollmodell	31
Bild 8 – Implementierungsaspekte eines FSCP	31
Bild 9 – Anwendungsbeispiel 1 (m = 4)	33
Bild 10 – Anwendungsbeispiel 2 (m = 2)	33
Bild 11 – Zonen und Durchleitungskonzept für IT-Sicherheit nach IEC 62443	35
Bild A.1 – Modell A	41
Bild A.2 – Modell B	42
Bild A.3 – Modell C	42
Bild A.4 – Modell D	43
Bild B.1 – Kommunikationskanal mit Störungen	44
Bild B.2 – Binärsymmetrischer Kanal (BSC)	45
Bild B.3 – Beispiel eines Blocks mit Nachrichtteil und CRC-Signatur	46
Bild B.4 – Blockcodes zur Fehleraufdeckung	47
Bild B.5 – Propere und nicht propere CRC-Polynome	48
Bild D.1 – Grundlegendes Markov-Modell	53
Bild E.1 – Beispiel von Sicherheits-PDUs in einer Feldbusnachricht	56
Bild E.2 – Modell mit ausschließlich expliziten Sicherungsmechanismen	56
Bild E.3 – Modell mit explizitem A-Code- und implizitem T-Code-Sicherungsmechanismus	57
Bild E.4 – Modell mit explizitem T-Code- und implizitem A-Code-Sicherungsmechanismus	58
Bild E.5 – Modell mit teilweise explizitem und teilweise implizitem Sicherungsmechanismus für die Aktualität und implizitem Sicherungsmechanismus für die Authentizität	58
Bild E.6 – Modell mit ausschließlich impliziten Sicherungsmechanismen	59
Bild F.1 – „Black Channel“ aus der Sicht des FSCP	60
Bild F.2 – Modell für die Authentizitäts-Betrachtung	65
Bild F.3 – Feldbus- und interne Adressfehler	66
Bild F.4 – Beispiel einer allmählich ansteigenden Nachrichten-Latenzzeit	68
Bild F.5 – Beispiel für das Versagen eines aktiven Netzwerkelements	69
Bild F.6 – Anwendungsbeispiel 1 (m = 4)	71
Bild F.7 – Anwendungsbeispiel 2 (m = 2)	71
Bild F.8 – Beispiel mit Konfigurier- und Parametervorgängen für FSCPs	73
Tabellen	
Tabelle 1 – Überblick über die Wirksamkeit von Maßnahmen gegen mögliche Fehler	30
Tabelle 2 – Definition der Größen für die Berechnung der Restfehlerraten	32
Tabelle 3 – Typische Beziehung zwischen Restfehlerrate und SIL	34
Tabelle 4 – Typische Beziehung zwischen Restfehler auf Anforderung und SIL	34
Tabelle 5 – Übersicht über Profilkennungen für FSCP 6/7	38
Tabelle B.1 – Beispiel für die Abhängigkeit von d_{\min} und Blockbitlänge n	47
Tabelle C.1 – Gemeinsame Gliederung der technologiespezifischen Teile	49
Tabelle F.1 – Typische Beziehung zwischen Restfehlerrate und SIL	72
Tabelle F.2 – Typische Beziehung zwischen Restfehler auf Anforderung und SIL	72