

Anwendungsbereich

Anwendungsbereich dieser Norm ist ...

Inhalt

	Seite
Einleitung	8
1 Anwendungsbereich	11
2 Normative Verweisungen	12
3 Begriffe und Abkürzungen	13
3.1 Begriffe	13
3.2 Abkürzungen	24
4 Festlegung von Sicherheitsfunktionen innerhalb von IMD und IFLS	24
4.1 Allgemeines	24
4.2 Festlegung der Sicherheitsfunktionen	25
5 Anforderungen an Produkte die sicherheitsbezogene Funktionen beinhalten.....	27
5.1 Anforderungen an nicht sicherheitsbezogene Funktionen	27
5.2 Zusätzliche Leistungsanforderungen für Produkte die Sicherheitsfunktionen beinhalten	27
6 Management der funktionalen Sicherheit während des Entwicklungs-Lebenszyklus.....	28
6.1 Management der funktionalen Sicherheit für das IT-System	28
6.2 Einsatz von IMD und IFLS in IT-Systemen	29
6.3 Sicherheits-Lebenszyklus von IMD und IFLS in der Realisierungsphase.....	29
7 Management der funktionalen Sicherheit während des Realisierungs-Lebenszyklus von IMD und IFLS	30
7.1 Allgemeines	30
7.2 Spezifikation der Anforderungen für die IMD- und IFLS-Entwicklung (Phase 10.1).....	31
7.3 Planung der Sicherheitsvalidierung für IMD und IFLS (Phase 10.2)	33
7.4 Entwurf und Entwicklung von IMD und IFLS (Phase 10.3)	34
7.5 IMD- und IFLS-Integration (Phase 10.4)	42
7.6 Dokumentation für Installation, Inbetriebnahme, Betrieb und Wartung von IMD und IFLS (Phase 10.5)	43
7.7 Phase zur Validierung der Sicherheit für IMD und IFLS (Phase 10.6).....	45
8 Anforderungen an Modifikationen	46
8.1 Allgemeines	46
8.2 Anforderung der Modifikation	46
8.3 Analyse der Auswirkungen	47
8.4 Genehmigung	47
9 Vorgehensweise bei Betriebsbewährung	47
Anhang A (informativ) Risikoanalyse und SIL-Festlegung für IMD und IFLS	48
A.1 Allgemeines	48
A.2 Festlegung des SIL für IMD und IFLS	48

	Seite
A.3 Beispiel einer Risikografik	49
A.4 Alternative Methode zur Bestimmung des SIL: Quantitative Methode	50
Anhang B (informativ) Beispiele zur Bestimmung von PFD, DC und SFF	51
B.1 Allgemeines	51
B.2 Beispiele für IMD- und IFLS-Architekturen	51
Anhang C (informativ) Datenbanken für Ausfallraten	52
C.1 Allgemeines	52
C.2 Referenzen für Ausfallraten in aktuellen Normen	52
Anhang D (informativ) Leitfaden für Entwurf und Entwicklung von embedded Software	53
D.1 Allgemeines	53
D.2 Leitfaden für Softwareelemente	53
D.3 Richtlinien für den Software-Entwicklungsprozess	55
D.4 Entwicklungswerkzeuge	57
D.5 Reproduzierbarkeit, Übergabe	57
D.6 Software Verifikation und Validierung	57
D.7 Allgemeine Richtlinien zur Verifikation und Validierung	58
D.8 Überprüfung der Verifikation und der Validierung	58
D.9 Software Prüfungen	58
Anhang E (informativ) Information zur Bewertung von Sicherheitsfunktionen	61
E.1 Allgemeines	61
E.2 Dokumentenmanagement	61
E.3 Dokumentation, die für die Bewertung der Konformität bereitzustellen ist	61
E.4 Dokumentation des Entwicklungs-Lebenszyklus	64
E.5 Entwicklungsdokumentation	64
E.6 Dokumentation der Verifikation und der Validierung	64
E.7 Dokumentation der Prüfungen	64
E.8 Dokumentation von Modifikationen	64
E.9 Benutzerinformationen	64
Anhang F (informativ) Beispiele für Anwendungen	65
F.1 Einleitung	65
F.2 Einschränkung der Anwendungen	65
F.3 Typische Anwendungen, die durch IEC 61557-15 abgedeckt sind	65
Literaturhinweise	74
Bild 1 – Funktionale Teile eines IT-Systems und ihre Beziehung zu den Begriffen und Abkürzungen der Normenreihe IEC 61508	8
Bild 2 – Zusammenhang zwischen der IEC 61557-15 und den verbundenen Normen	10
Bild 3 – Gesamter, für ein IT-System anzuwendender Lebenszyklus	29
Bild 4 – Sicherheitslebenszyklus von IMD und IFLS (in der Realisierungsphase)	30
Bild A.1 – Beispiel eines Risikographen	49

	Seite
Bild B.1 – Ablaufdiagramm für die Bestimmung von PFD, DC, SFF	51
Bild F.1 – Lokale Warnung basierend auf der systematischen Anwesenheit einer Person sowie auf einem genau definierten Managementprozess für die Meldung	66
Bild F.2 – Lokale Transformator-Überwachungsmeldung basierend auf der systematischen Anwesenheit einer Fachkraft sowie auf einem genau definierten Managementprozess für die Meldungen	67
Bild F.3 Meldung und Weiterverarbeitung der externen Isolationsfehlermeldung und / oder der externen Lokalisierungsmeldung in einem Überwachungs- und Steuerungssystem	68
Bild F.4 – Abschaltung des gesamten IT-Systems bei Erfassung eines Isolationsfehlers	69
Bild F.5 – Ansprechwert 1 mit Meldung und Ansprechwert 2 mit Abschaltung des gesamten IT-Systems bei Erfassung eines Isolationsfehlers	70
Bild F.6 – Automatische Abschaltung eines fehlerhaften Abganges über die direkte Ansteuerung vom IFLS	70
Bild F.7 – Automatische Abschaltung eines fehlerbehafteten Abganges über eine SPS	71
Bild F.8 – Steuerung von zwei Einspeisungen oder von einer Einspeisung plus Generator	72
Bild F.9 – Steuerung von zwei Einspeisungen oder von einer Einspeisung plus Generator mit Lastmanagement	73
Tabelle 1 – IT-System Risikoanalyse	9
Tabelle 2 – Abkürzungen mit Verweis	24
Tabelle 3 – Sicherheits-Integritätslevel (SIL) und Wahrscheinlichkeit eines gefährlichen Ausfalls bei Anforderung für IMD und IFLS	31
Tabelle 4 – Sicherheitsintegrität der Hardware: Einschränkungen hinsichtlich der Architektur auf sicherheitsbezogene Typ A und Typ B Teilsysteme	39
Tabelle A.1 – SIL-Festlegung für IMD und IFLS	48
Tabelle A.2 – Verbindung zwischen der mindestens erforderlichen Risikoreduzierung und dem SIL	49
Tabelle A.3 – Beispiel von Klassifikationen nach dem Risikographen in Bild A	50
Tabelle E.1 – Bereitzustellende Dokumentation	62