

Inhalt

| | Seite |
|---|-------|
| Vorwort..... | 2 |
| Einleitung | 9 |
| 1 Anwendungsbereich | 11 |
| 2 Normative Verweisungen | 11 |
| 3 Begriffe und Abkürzungen | 12 |
| 3.1 Begriffe | 12 |
| 3.2 Abkürzungen | 23 |
| 4 Festlegung von Sicherheitsfunktionen innerhalb von IMD und IFLS | 25 |
| 4.1 Allgemeines | 25 |
| 4.2 Festlegung der Sicherheitsfunktionen | 25 |
| 4.2.1 Lokale Isolationsfehlermeldung (LIW, en: local insulation warning) | 25 |
| 4.2.2 Externe Isolationsfehlermeldung (RIW, en: remote insulation warning) | 25 |
| 4.2.3 Lokale Lokalisierungsmeldung (LLW, en: local location warning) | 26 |
| 4.2.4 Externe Lokalisierungsmeldung (RLW, en: remote location warning) | 26 |
| 4.2.5 Externes Freigabe-/Sperrsignal (REDC, remote enabling / disabling command)..... | 26 |
| 4.2.6 Lokale Transformator-Überwachungsmeldung (LTMW, en: local transformer monitoring warning)..... | 27 |
| 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 |
| 5.2.1 Allgemeines | 27 |
| 5.2.2 Zusätzliche Leistungsanforderungen für IMD, die SIL 1 oder SIL 2 entsprechen | 28 |
| 5.2.3 Zusätzliche Leistungsanforderungen für IFLS, die SIL 1 oder SIL 2 entsprechen | 28 |
| 6 Management der funktionalen Sicherheit während des Entwicklungslebenszyklus | 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 Sicherheitslebenszyklus von IMD und IFLS in der Realisierungsphase | 29 |
| 7 Management der funktionalen Sicherheit während des Realisierungslebenszyklus von IMD und IFLS | 30 |
| 7.1 Allgemeines | 30 |
| 7.2 Spezifikation der Anforderungen für die IMD- und IFLS-Entwicklung (Phase 10.1) | 31 |
| 7.2.1 Spezifikation der Anforderungen zur funktionalen Sicherheit | 31 |
| 7.2.2 Maßnahmen zur Entwicklung der Sicherheitsfunktionen | 31 |
| 7.2.3 Plan zur Verifikation der Entwicklung der Sicherheitsfunktionen | 32 |
| 7.2.4 Plan zur Validation der Entwicklung der Sicherheitsfunktionen | 32 |
| 7.2.5 Planung von Inbetriebnahme, Installation und Inbetriebsetzung | 32 |
| 7.2.6 Planung der Benutzerdokumentation | 33 |

| | Seite |
|--|-------|
| 7.3 Planung der Sicherheitsvalidierung für IMD und IFLS (Phase 10.2) | 33 |
| 7.3.1 Allgemeines | 33 |
| 7.3.2 Plan zur funktionalen Sicherheit | 33 |
| 7.4 Entwurf und Entwicklung von IMD und IFLS (Phase 10.3) | 34 |
| 7.4.1 Allgemeines | 34 |
| 7.4.2 Normen für die Entwicklung | 34 |
| 7.4.3 Realisierung | 34 |
| 7.4.4 Sicherheitsintegrität und Fehleraufdeckung | 34 |
| 7.4.5 Zuordnung eines Sicherheitsintegritätslevels (SIL) | 35 |
| 7.4.6 Anforderungen an die Hardware | 35 |
| 7.4.7 Anforderungen an die Software | 35 |
| 7.4.8 Überprüfung der Anforderungen | 35 |
| 7.4.9 Anforderungen für die Wahrscheinlichkeit gefahrbringender Ausfälle bei Anforderung (PFD) | 36 |
| 7.4.10 Daten für Ausfallraten | 37 |
| 7.4.11 Diagnose-Testintervall | 37 |
| 7.4.12 Einschränkungen hinsichtlich der Architektur | 38 |
| 7.4.13 Beurteilung des Anteils sicherer Ausfälle (SFF, en: safe failure fraction) | 39 |
| 7.4.14 Anforderungen zur systematischen Sicherheitsintegrität | 40 |
| 7.5 IMD- und IFLS-Integration (Phase 10.4) | 42 |
| 7.5.1 Hardware Integration | 42 |
| 7.5.2 Software Integration | 43 |
| 7.5.3 Modifikationen während der Integration | 43 |
| 7.5.4 Integrationsprüfungen | 43 |
| 7.6 Dokumentation für Installation, Inbetriebnahme, Betrieb und Wartung von IMD und IFLS (Phase 10.5) | 43 |
| 7.6.1 Allgemeines | 43 |
| 7.6.2 Funktionsbeschreibung | 43 |
| 7.6.3 Information zur Übereinstimmung | 43 |
| 7.6.4 Informationen für die Inbetriebnahme, die Installation, das Inbetriebsetzen, den Betrieb und die Wartung | 44 |
| 7.7 Phase zur Validierung der Sicherheit für IMD und IFLS (Phase 10.6) | 45 |
| 7.7.1 Allgemeines | 45 |
| 7.7.2 Prüfungen | 45 |
| 7.7.3 Verifikation | 45 |
| 7.7.4 Validierung | 45 |
| 7.7.5 EMV-Anforderungen | 45 |
| 8 Anforderungen an Modifikationen | 46 |
| 8.1 Allgemeines | 46 |
| 8.2 Anforderung der Modifikation | 46 |

| | Seite |
|---|-------|
| 8.3 Analyse der Auswirkungen | 47 |
| 8.4 Genehmigung | 47 |
| 9 Vorgehensweise bei Betriebsbewahrung | 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 | 50 |
| A.3 Beispiel einer Risikografik | 51 |
| A.4 Alternative Methode zur Bestimmung des SIL: Quantitative Methode..... | 52 |
| Anhang B (informativ) Beispiele zur Bestimmung von PFD, DC und SFF | 53 |
| B.1 Allgemeines | 53 |
| B.2 Beispiele für IMD- und IFLS-Architekturen..... | 53 |
| Anhang C (informativ) Datenbanken für Ausfallraten | 54 |
| C.1 Allgemeines | 54 |
| C.2 Referenzen für Ausfallraten in aktuellen Normen | 54 |
| Anhang D (informativ) Leitfaden für Entwurf und Entwicklung von embedded Software | 55 |
| D.1 Allgemeines | 55 |
| D.2 Leitfaden für Softwareelemente | 55 |
| D.2.1 Allgemeines | 55 |
| D.2.2 Schnittstelle zur Systemarchitektur | 55 |
| D.2.3 Software Spezifikationen | 55 |
| D.2.4 Bestehende Software | 56 |
| D.2.5 Softwareentwicklung..... | 57 |
| D.2.6 Kodierung | 57 |
| D.3 Richtlinien für den Software-Entwicklungsprozess | 57 |
| D.3.1 Entwicklungsprozess: Software-Lebenszyklus | 57 |
| D.3.2 Dokumente: Dokumentenmanagement..... | 58 |
| D.3.3 Management von Konfiguration und von Softwaremodifikation | 58 |
| D.3.4 Management von Konfiguration und Archivierung | 58 |
| D.3.5 Management von Software-Modifikationen | 59 |
| D.4 Entwicklungswerkzeuge | 59 |
| D.5 Reproduzierbarkeit der Erzeugung von ausführbarem Code..... | 59 |
| D.6 Software Verifikation und Validierung | 59 |
| D.7 Allgemeine Richtlinien zur Verifikation und Validierung | 60 |
| D.8 Überprüfung der Verifikation und der Validierung | 60 |
| D.9 Software Prüfungen | 60 |
| D.9.1 Allgemeines zur Validierung | 60 |
| D.9.2 Verifikation der Software nach den Anforderungen: Validierungsprüfungen | 61 |
| D.9.3 Verifikation des Software Design: Software-Integrationsprüfungen..... | 62 |
| D.9.4 Detaillierte Designverifikation: Modulprüfungen | 62 |

| | Seite |
|---|-------|
| Anhang E (informativ) Information zur Bewertung von Sicherheitsfunktionen..... | 63 |
| E.1 Allgemeines..... | 63 |
| E.2 Dokumentenmanagement..... | 63 |
| E.3 Dokumentation für die Bewertung der Konformität..... | 63 |
| E.4 Dokumentation des Entwicklungslebenszyklus..... | 66 |
| E.5 Entwicklungsdokumentation..... | 66 |
| E.6 Dokumentation der Verifikation und der Validierung..... | 66 |
| E.7 Dokumentation der Prüfungen..... | 66 |
| E.8 Dokumentation von Modifikationen..... | 66 |
| E.9 Benutzerinformationen..... | 66 |
| Anhang F (informativ) Beispiele für Anwendungen..... | 67 |
| F.1 Einleitung..... | 67 |
| F.2 Einschränkung der Anwendungen..... | 67 |
| F.3 Typische Anwendungen, die durch IEC 61557-15 abgedeckt sind..... | 67 |
| F.3.1 Allgemeines..... | 67 |
| F.3.2 Lokale Meldung..... | 67 |
| F.3.3 Lokale Transformator-Überwachungsmeldung..... | 68 |
| F.3.4 Meldung und Weiterverarbeitung von externer Isolationsfehlermeldung und/oder externer Lokalisierungsmeldung..... | 70 |
| F.3.5 Automatische Abschaltung des gesamten IT-Systems bei einem ersten Isolationsfehler..... | 71 |
| F.3.6 Automatische Abschaltung von Abgängen eines IT-Systems..... | 72 |
| F.3.7 Steuerungen eines Systems mit mehreren Einspeisungen (von zwei Einspeisungen oder einer Einspeisung plus Generator)..... | 74 |
| F.3.8 Steuerung von Systemen mit mehreren Einspeisungen (von zwei Einspeisungen oder von einer Einspeisung plus Generator mit Lastmanagement)..... | 74 |
| Literaturhinweise..... | 76 |
| Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen..... | 78 |
| <u>Bilder</u> | |
| Bild 1 – Zusammenhang zwischen der IEC 61557-15 und den verbundenen Normen..... | 9 |
| Bild 2 – Gesamter, für ein IT-System anzuwendender Lebenszyklus..... | 29 |
| Bild 3 – Sicherheitslebenszyklus von IMD und IFLS (in der Realisierungsphase)..... | 30 |
| Bild A.1 – Funktionale Teile eines IT-Systems und ihre Beziehung zu den Begriffen und Abkürzungen der Normenreihe IEC 61508..... | 48 |
| Bild A.2 – Beispiel eines Risikographen..... | 51 |
| Bild B.1 – Ablaufdiagramm für die Bestimmung von PFD, DC, SFF..... | 53 |
| Bild F.1 – Lokale Warnung basierend auf der systematischen Anwesenheit einer Person sowie auf einem genau definierten Managementprozess für die Meldung..... | 68 |
| Bild F.2 – Lokale Transformator-Überwachungsmeldung basierend auf der systematischen Anwesenheit einer Fachkraft sowie auf einem genau definierten Managementprozess für die Meldungen..... | 69 |
| Bild F.3 – Meldung und Weiterverarbeitung der externen Isolationsfehlermeldung und/oder der | |

| | Seite |
|---|-------|
| externen Lokalisierungsmeldung in einem Überwachungs- und Steuerungssystem | 70 |
| Bild F.4 – Abschaltung des gesamten IT-Systems bei Erfassung eines Isolationsfehlers | 71 |
| Bild F.5 – Ansprechwert 1 mit Meldung und Ansprechwert 2 mit Abschaltung des gesamten IT-Systems bei Erfassung eines Isolationsfehlers | 72 |
| Bild F.6 – Automatische Abschaltung eines fehlerhaften Abganges über die direkte Ansteuerung vom IFLS | 72 |
| Bild F.7 – Automatische Abschaltung eines fehlerbehafteten Abgangs über eine SPS | 73 |
| Bild F.8 – Steuerung eines Systems mit mehreren (von zwei Einspeisungen oder von einer Einspeisung plus Generator) | 74 |
| Bild F.9 – Steuerung eines Systems mit mehreren Einspeisungen (von zwei Einspeisungen oder von einer Einspeisung plus Generator mit Lastmanagement) | 75 |
| <u>Tabellen</u> | |
| Tabelle 1 – Abkürzungen mit Verweisung | 24 |
| Tabelle 2 – Sicherheitsintegritätslevel (SIL) und Wahrscheinlichkeit eines gefährlichen Ausfalls bei Anforderung (PFD) für IMD und IFLS | 31 |
| Tabelle 3 – Sicherheitsintegrität der Hardware: Einschränkungen hinsichtlich der Architektur auf sicherheitsbezogene Typ A und Typ B Teilsysteme | 39 |
| Tabelle A.1 – IT-System Risikoanalyse | 49 |
| Tabelle A.2 – SIL-Festlegung für IMD und IFLS | 50 |
| Tabelle A.3 – Verbindung zwischen der mindestens erforderlichen Risikoreduzierung und dem SIL | 51 |
| Tabelle A.4 – Beispiel von Klassifikationen nach dem Risikographen in Bild A | 52 |
| Tabelle E.1 – Bereitzustellende Dokumentation | 64 |