

## **Inhalt**

	Seite
Europäisches Vorwort.....	2
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen .....	3
Einleitung .....	12
1 Anwendungsbereich .....	14
2 Normative Verweisungen .....	14
3 Begriffe und Abkürzungen .....	14
Anhang A (informativ) Anleitung für IEC 61511-1 .....	15
A.1 Anwendungsbereich .....	15
A.2 Normative Verweisungen .....	15
A.3 Begriffe und Abkürzungen .....	15
A.4 Übereinstimmung mit IEC 61511-1:– .....	15
A.5 Management der funktionalen Sicherheit.....	15
A.5.1 Ziel .....	15
A.5.2 Anleitung zu „Anforderungen“ .....	16
A.6 Anforderungen an den Sicherheitslebenszyklus .....	24
A.6.1 Ziele .....	24
A.6.2 Anleitung zu „Anforderungen“ .....	25
A.6.3 Anleitung zu Anforderungen an das „Anwendungsprogramm im PLT- Sicherheitseinrichtungs-Sicherheitslebenszyklus“ .....	25
A.7 Verifizierung.....	27
A.7.1 Ziel .....	27
A.7.2 Anleitung zu „Anforderungen“ .....	27
A.8 Gefährdungs- und Risikobeurteilung des Prozesses .....	29
A.8.1 Ziele .....	29
A.8.2 Anleitung zu „Anforderungen“ .....	29
A.9 Zuordnung der Sicherheitsfunktionen zu den Schutzebenen .....	32
A.9.1 Ziel .....	32
A.9.2 Anleitung zu „Anforderungen an den Prozess der Zuordnung“ .....	32
A.9.3 Anleitung zu „Anforderungen an das Prozessleitsystem als Schutzebene“ .....	35
A.9.4 Anleitung zu „Anforderungen zur Vermeidung von Ausfällen infolge gemeinsamer Ursache, gleichartigen Ausfällen und abhängigen Ausfällen“ .....	37
A.10 Spezifikation der Sicherheitsanforderungen an die PLT-Sicherheitseinrichtung .....	38
A.10.1 Ziel .....	38
A.10.2 Anleitung zu „Allgemeine Anforderungen“ .....	38
A.10.3 Anleitung zu „Sicherheitsanforderungen an die PLT-Sicherheitseinrichtung“ .....	38
A.11 Entwurf und Konstruktion der PLT-Sicherheitseinrichtung.....	43
A.11.1 Ziel .....	43

	Seite
A.11.2 Anleitung zu „Allgemeine Anforderungen“ .....	43
A.11.3 Anleitung zu „Anforderungen an das Systemverhalten bei Entdeckung eines Fehlers“ .....	51
A.11.4 Anleitung zu „Anforderungen an die Hardware-Fehlertoleranz“ .....	51
A.11.5 Anleitung zu „Anforderungen an die Geräteauswahl“ .....	55
A.11.6 Feldgeräte .....	58
A.11.7 Schnittstellen .....	58
A.11.8 Anleitung zu „Anforderungen an Instandhaltung oder Prüfdesign“ .....	60
A.11.9 Anleitung zu „Quantifizierung zufälliger Ausfälle“ .....	62
A.12 Entwicklung des PLT-Sicherheitseinrichtungs-Anwendungsprogramms.....	68
A.12.1 Ziel.....	68
A.12.2 Anleitung zu „Allgemeine Anforderungen“ .....	68
A.12.3 Anleitung zu „Entwurf des Anwendungsprogramms“ .....	69
A.12.4 Anleitung zu „Implementierung des Anwendungsprogramms“ .....	72
A.12.5 Anleitung zu „Anforderungen an die Verifizierung des Anwendungsprogramms (Review und Test)“ .....	73
A.12.6 Anleitung zu „Anforderungen hinsichtlich Methodik und Werkzeuge des AP“ .....	77
A.13 Werksabnahmeprüfungen (FAT).....	79
A.13.1 Ziele.....	79
A.13.2 Anleitung zu „Empfehlungen“ .....	79
A.14 PLT-Sicherheitseinrichtungs-Montage und Inbetriebnahme.....	79
A.14.1 Ziele.....	79
A.14.2 Anleitung zu „Anforderungen“ .....	79
A.15 Sicherheits-Validierung der PLT-Sicherheitseinrichtung .....	80
A.15.1 Ziel.....	80
A.15.2 Anleitung zu „Anforderungen“ .....	80
A.16 Betrieb und Instandhaltung der PLT-Sicherheitseinrichtung .....	81
A.16.1 Ziele.....	81
A.16.2 Anleitung zu „Anforderungen“ .....	81
A.16.3 Funktionsprüfung und Inspektion.....	82
A.17 Modifizierung der PLT-Sicherheitseinrichtung .....	85
A.17.1 Ziel.....	85
A.17.2 Anleitung zu „Anforderungen“ .....	85
A.18 Außerbetriebnahme der PLT-Sicherheitseinrichtung.....	86
A.18.1 Ziele.....	86
A.18.2 Anleitung zu „Anforderungen“ .....	86
A.19 Anforderungen an die Information und Dokumentation .....	86
A.19.1 Ziele.....	86
A.19.2 Anleitung zu „Anforderungen“ .....	86

	Seite
Anhang B (informativ) Beispiel für die Entwicklung eines Anwendungsprogramms für ein PLT-Sicherheitseinrichtungs-Logiksystem mittels Funktionsblockdiagramm .....	88
B.1 Allgemeines .....	88
B.2 Entwicklung des Anwendungsprogramms und Validierungsphilosophie .....	88
B.3 Anwendungsbeschreibung .....	89
B.3.1 Allgemeines .....	89
B.3.2 Prozessbeschreibung .....	90
B.3.3 Sicherheitstechnische Funktionen.....	90
B.3.4 Risikominderung und Dominoeffekte .....	91
B.4 Ausführung des Sicherheitslebenszyklus für das Anwendungsprogramm .....	91
B.4.1 Allgemeines .....	91
B.4.2 Eingabedaten für die Erstellung der SRS des Anwendungsprogramms .....	91
B.4.3 Entwurf und Erstellung des Anwendungsprogramms .....	95
B.4.4 Erzeugung des Anwendungsprogramms .....	109
B.4.5 Verifizierung und Prüfung des Anwendungsprogramms.....	109
B.4.6 Validierung.....	109
Anhang C (informativ) Überlegungen beim Umwandeln von NP-Technologien zu PE-Technologien.....	110
Anhang D (informativ) Beispiel für die Erstellung eines Anwendungsprogramms aus einem Rohrleitungs- und Instrumentierungsdiagramm (P&ID) .....	112
Anhang E (informativ) Methoden und Werkzeuge für die Erstellung eines Anwendungsprogramms .....	115
E.1 Werkzeugsatz für die Anwendungsprogrammierung .....	115
E.2 Regeln und Einschränkungen für die Gestaltung des Anwendungsprogramms.....	116
E.3 Regeln und Einschränkungen für die Anwendungsprogrammierung.....	117
Anhang F (informativ) Beispiel eines PLT-Sicherheitseinrichtungs-Projekts für jede Phase des Sicherheitslebenszyklus mit Entwicklung eines Anwendungsprogramms unter Anwendung der Relaisleitersprache.....	119
F.1 Überblick.....	119
F.2 Projektdefinition .....	120
F.2.1 Allgemeines .....	120
F.2.2 Konzeptionelle Planung.....	120
F.2.3 Prozessgefahrenanalyse .....	120
F.3 Vereinfachte Prozessbeschreibung.....	120
F.4 Vorläufiger Entwurf .....	122
F.5 Anwendung von IEC 61511.....	122
F.5.1 Allgemeines .....	122
F.5.2 Schritt F.1: Gefährdungs- und Risikobewertung .....	125
F.5.3 Erkennung der Gefährdungen.....	126
F.5.4 Vorläufige Gefährdungsbewertung.....	126
F.5.5 Unfallhistorie.....	126
F.6 Sicherheitsbetrachtungen des vorläufigen Prozessentwurfs .....	128

	Seite
F.7	Anerkannte Prozessgefahren..... 129
F.8	Strategie für den Prozessentwurf..... 130
F.9	Vorläufige Gefährdungsbewertung ..... 133
F.9.1	Allgemeines..... 133
F.9.2	Schritt F.2: Zuordnung von Sicherheitsfunktionen ..... 137
F.10	Bestimmung des PLT-Sicherheitsfunktions-Sicherheitsintegritätslevels ..... 138
F.11	Anwendung von LOPA auf das Beispiel ..... 138
F.12	Kriterien für das tolerierbare Risiko..... 140
F.13	Schritt F.3: Spezifikationen der PLT-Sicherheitseinrichtungs-Sicherheitsanforderungen ..... 143
F.13.1	Überblick ..... 143
F.13.2	Eingabeanforderungen..... 143
F.13.3	Funktionale Sicherheitsanforderungen ..... 144
F.13.4	Anforderungen an die Sicherheitsintegrität..... 146
F.14	Funktionale Beschreibung und konzeptioneller Entwurf..... 146
F.14.1	Beschreibung einer Beispiellogik für das Reaktorsystem..... 147
F.15	Berechnungen der SIL-Verifizierung..... 148
F.16	Anforderungen an das AP..... 155
F.17	Schritt F.4: PLT-Sicherheitseinrichtungs-Sicherheitslebenszyklus..... 162
F.18	Auswahl von Verfahren und Komponenten ..... 162
F.18.1	Allgemeines..... 162
F.18.2	Logiksystem ..... 162
F.18.3	Sensoren..... 163
F.18.4	Aktoren..... 163
F.18.5	Magnetventile..... 163
F.18.6	Notentgasungsventile..... 164
F.18.7	Modulierende Ventile ..... 164
F.18.8	Umgehungsventile ..... 164
F.18.9	Mensch-Maschine-Schnittstellen (HMIs) ..... 164
F.18.10	Trennung..... 166
F.19	Ausfälle infolge gemeinsamer Ursache und systematischer Ausfälle ..... 166
F.19.1	Allgemeines..... 166
F.19.2	Diversität ..... 167
F.19.3	Spezifikationsfehler ..... 167
F.19.4	Fehler des Hardwareentwurfs ..... 167
F.19.5	Fehler des Softwareentwurfs ..... 167
F.19.6	Überlastung durch die Umwelt..... 168
F.19.7	Temperatur..... 168
F.19.8	Luftfeuchte..... 168
F.19.9	Verunreinigungen..... 168

	Seite
F.19.10 Schwingungen .....	168
F.19.11 Erdung .....	169
F.19.12 Verbesserung der Stromversorgungsqualität .....	169
F.19.13 Elektromagnetische Verträglichkeit (EMV) .....	169
F.19.14 Versorgungsquellen .....	170
F.19.15 Sensoren .....	170
F.19.16 Prozesskorrosion oder Schmutzablagerung .....	170
F.19.17 Instandhaltung .....	171
F.19.18 Anfälligkeit für Fehlbedienung .....	171
F.19.19 PLT-Sicherheitseinrichtungs-Architektur .....	171
F.20 Entwurfsmerkmale des PLT-Sicherheitseinrichtungs-Anwendungsprogramms .....	173
F.21 Installationstechnik .....	173
F.22 Sicherheit .....	173
F.23 Schritt F.5: Installation, Inbetriebnahme und Validierung der PLT-Sicherheitseinrichtung .....	174
F.24 Installation .....	175
F.25 Inbetriebnahme .....	176
F.26 Dokumentation .....	176
F.27 Validierung .....	177
F.28 Prüfung .....	178
F.29 Schritt F.6: Betrieb und Instandhaltung der PLT-Sicherheitseinrichtung .....	191
F.30 Schritt F.7: PLT-Sicherheitseinrichtungs-Modifikation .....	194
F.31 Schritt F.8: PLT-Sicherheitseinrichtungs-Außerbetriebnahme .....	194
F.32 Schritt F.9: PLT-Sicherheitseinrichtungs-Verifizierung .....	195
F.33 Schritt F.10: Management der funktionalen Sicherheit und Bewertung der funktionalen Sicherheit der PLT-Sicherheitseinrichtung .....	196
F.34 Management der funktionalen Sicherheit .....	196
F.34.1 Allgemeines .....	196
F.34.2 Befähigung des Personals .....	196
F.35 Bewertung der funktionalen Sicherheit .....	197
Anhang G (informativ) Leitfaden für die Entwicklung von Anwendungsprogrammierverfahren .....	198
G.1 Zweck dieses Leitfadens .....	198
G.2 Eigenschaften einer generisch sicheren Anwendungssoftware .....	198
G.3 Zuverlässigkeit .....	199
G.3.1 Allgemeines .....	199
G.3.2 Vorhersagbarkeit der Speicherausnutzung .....	199
G.3.3 Vorhersagbarkeit des Steuerflusses .....	200
G.3.4 Beachtung der Genauigkeit und Fehlerfreiheit .....	202
G.3.5 Vorhersagbarkeit des Zeitablaufs .....	204
G.4 Vorhersagbarkeit des mathematischen oder logischen Ergebnisses .....	205

	Seite
G.5 Robustheit .....	205
G.5.1 Allgemeines .....	205
G.5.2 Lenkung der Diversität .....	205
G.5.3 Lenkung der Ausnahmebehandlung .....	207
G.5.4 Prüfung der Eingabe- und Ausgabedaten .....	208
G.6 Rückverfolgbarkeit .....	208
G.6.1 Allgemeines .....	208
G.6.2 Lenkung von integrierten Funktionen .....	209
G.6.3 Lenkung von kompilierten Bibliotheken .....	209
G.7 Pflegbarkeit .....	209
G.7.1 Allgemeines .....	209
G.7.2 Lesbarkeit .....	209
G.7.3 Datenabstraktion .....	213
G.7.4 Funktionaler Zusammenhalt .....	213
G.7.5 Formbarkeit .....	214
G.7.6 Übertragbarkeit .....	214
Literaturhinweise .....	215
<b>Bilder</b>	
Bild 1 – Gesamtrahmen der Reihe IEC 61511 .....	13
Bild A.1 – Anwendungsprogramm des V-Modells .....	27
Bild A.2 – Unabhängigkeit einer PLT-Betriebseinrichtungsschutzebene und einer auslösenden Quelle ii der PLT-Betriebseinrichtung .....	36
Bild A.3 – Unabhängigkeit von zwei der PLT-Betriebseinrichtung zugeordneten Schutzebenen .....	37
Bild A.4 – Beziehung zwischen System, PLT-Sicherheitseinrichtungs-Hardware und PLT- Sicherheitseinrichtungs-Anwendungsprogramm .....	42
Bild A.5 – Darstellung der Unsicherheiten einer Zuverlässigkeitskenngröße .....	65
Bild A.6 – Darstellung der oberen 70%-Vertrauensgrenze .....	66
Bild A.7 – Typische probabilistische Verteilung der Zielergebnisse aus einer Monte-Carlo-Simulation .....	67
Bild B.1 – Prozessablaufdiagramm für PLT-Sicherheitsfunktion 02.01 .....	90
Bild B.2 – Prozessablaufdiagramm für PLT-Sicherheitsfunktion 06.02 .....	91
Bild B.3 – Funktionale Spezifikation von PLT-Sicherheitsfunktion 02.01 und PLT-Sicherheitsfunktion 06.02 .....	92
Bild B.4 – Funktionale Hardwarearchitektur von PLT-Sicherheitsfunktion 02.01 .....	93
Bild B.5 – Funktionale Hardwarearchitektur von PLT-Sicherheitsfunktion 06.02 .....	93
Bild B.6 – Aus dem Rohrleitungs- und Instrumentierungsdiagramm abgeleitete Hardwarespezifikation für ein SOV .....	94
Bild B.7 – Physikalische Hardwarearchitektur von PLT-Sicherheitsfunktion 02.01 .....	95
Bild B.8 – Physikalische Hardwarearchitektur von PLT-Sicherheitsfunktion 06.02 .....	95
Bild B.9 – Hierarchische Struktur der Modellintegration .....	99

	Seite
Bild B.10 – Hierarchische Struktur der Modellintegration einschließlich von Modellen der Sicherheitseigenschaften und der PLT-Betriebseinrichtungs-Logik .....	101
Bild B.11 – Diagramm der Zustandslogik .....	102
Bild B.12 – SOV-Typical-Logikdiagramm .....	103
Bild B.13 – SOV-Typical-Logikmodellldiagramm.....	104
Bild B.14 – Implementierung des Typical-Modell-Logikdiagramms – PLT-Betriebseinrichtungs-Teil.....	106
Bild B.15 – Implementierung des Typical-Modells des SOV-Anwendungsprogramms – PLT-Sicherheitseinrichtungs-Teil .....	107
Bild B.16 – Vollständiges Modell für die Überprüfung des endgültigen Implementierungsmodells .....	109
Bild D.1 – Beispiel eines P&ID für einen Öl- und Gas-Trenner (Abscheider) .....	112
Bild D.2 – Beispiel für ein (einen Teil eines) Ursache-Wirkung-Diagramm(s) (C&E) für die Notabschaltung (ESD).....	113
Bild D.3 – Beispiel für ein (einen Teil eines) Anwendungsprogramm(s) in einer Sicherheits-SPS-Programmierung mit der Funktionsbausteinsprache .....	114
Bild F.1 – Vereinfachtes Flussdiagramm: PVC-Herstellung.....	121
Bild F.2 – Phasen des PLT-Sicherheitseinrichtungs-Sicherheitslebenszyklus und FSA-Stufen.....	123
Bild F.3 – Beispiel für ein vorläufiges P&ID für eine PVC-Reaktoreinheit.....	132
Bild F.4 – Blasendiagramm für PLT-Sicherheitsfunktion S-1 mit der $PFD_{avg}$ für jede PLT-Sicherheitseinrichtungs-Komponente.....	150
Bild F.5 – S-1-Fehlerbaum.....	151
Bild F.6 – Blasendiagramm mit der PFD für jede PLT-Sicherheitseinrichtungs-Komponente .....	152
Bild F.7 – PLT-Sicherheitsfunktion-S-2-Fehlerbaum .....	153
Bild F.8 – Blasendiagramm für PLT-Sicherheitsfunktion S-3 mit der PFD für jede PLT-Sicherheitseinrichtungs-Komponente.....	154
Bild F.9 – PLT-Sicherheitsfunktion-S-3-Fehlerbaum .....	155
Bild F.10 – P&ID für die PLT-Sicherheitsfunktion einer PVC-Reaktoreinheit.....	156
Bild F.11 – Legende.....	157
Bild F.12 – Sicherheitstechnisches System für den VCM-Reaktor .....	172
<b>Tabellen</b>	
Tabelle B.1 – Spezifikation der Betriebsarten .....	96
Tabelle B.2 – Tabelle der Zustandsübergänge .....	102
Tabelle F.1 – Überblick über den PLT-Sicherheitseinrichtungs-Sicherheitslebenszyklus .....	124
Tabelle F.2 – PLT-Sicherheitseinrichtungs-Sicherheitslebenszyklus – Kasten 1 .....	126
Tabelle F.3 – Einige physikalische Eigenschaften von Vinylchlorid .....	128
Tabelle F.4 – Was-wäre-wenn/Checkliste .....	134
Tabelle F.5 – HAZOP .....	135
Tabelle F.6 – Teilzusammenfassung der Informationen der Gefährdungsbewertung für die Entwicklung der Strategie für PLT-Sicherheitsfunktion .....	136
Tabelle F.7 – PLT-Sicherheitseinrichtungs-Sicherheitslebenszyklus – Kasten 2 .....	138
Tabelle F.8 – Kriterien für das tolerierbare Risiko .....	140
Tabelle F.9 – Beispiel eines VCM-Reaktors: LOPA-basierter Integritätslevel .....	141

	Seite
Tabelle F.10 – 3 PLT-Sicherheitseinrichtungs-Sicherheitslebenszyklus – Kasten 3 .....	143
Tabelle F.11 – Sicherheitstechnische Funktionen und SIL .....	143
Tabelle F.12 – Funktionale Beziehung der E/A für die PLT-Sicherheitsfunktion .....	144
Tabelle F.13 – PLT-Sicherheitseinrichtungs-Sensoren, normaler Betriebsbereich und Auslösepunkte .....	144
Tabelle F.14 – Ursache-Wirkung-Diagramm .....	147
Tabelle F.15 – MTTF <sub>d</sub> -Zahlen der PLT-Sicherheitseinrichtungs-Komponenten .....	148
Tabelle F.16 – PLT-Sicherheitseinrichtungs-Sicherheitslebenszyklus – Kasten 4 .....	162
Tabelle F.17 – PLT-Sicherheitseinrichtungs-Sicherheitslebenszyklus – Kasten 5 .....	174
Tabelle F.18 – Liste der angewendeten Instrumententypen und Prüfverfahren .....	179
Tabelle F.19 – Überbrückungs-/Simulationsprüfblatt für das Prüfverfahren zur Prüfung der Verriegelungen .....	191
Tabelle F.20 – PLT-Sicherheitseinrichtungs-Sicherheitslebenszyklus – Kasten 6 .....	191
Tabelle F.21 – PLT-Sicherheitseinrichtungs-Auslöseprotokoll .....	192
Tabelle F.22 – Ausfallprotokoll für PLT-Sicherheitseinrichtungs-Komponenten .....	193
Tabelle F.23 – PLT-Sicherheitseinrichtungs-Sicherheitslebenszyklus – Kasten 7 .....	194
Tabelle F.24 – PLT-Sicherheitseinrichtungs-Sicherheitslebenszyklus – Kasten 8 .....	195
Tabelle F.25 – PLT-Sicherheitseinrichtungs-Sicherheitslebenszyklus – Kasten 9 .....	195
Tabelle F.26 – PLT-Sicherheitseinrichtungs-Sicherheitslebenszyklus – Kasten 10 .....	196