Inhalt

Vorwort 5

Hinweise und Hilfestellungen 13

1 Grundlagen 15
1.1 Gefahr, Risiko und Schaden 15
1.2 Klassifikation der Sicherheitsfunktionen 22
1.3 Beziehung zwischen DIN EN ISO 12100 und DIN EN IEC 62061 (**VDE 0113-50**), DIN EN ISO 13849-1 23

2 Umsetzung Schritt für Schritt 25
2.1 Projektinformationen 25
2.2 Risikobeurteilung und SRS 29
2.3 Sicherheitsfunktionen und funktionale Anforderungen 34
2.4 SCS- und SRP/CS-Methodik 35
2.5 Kategorien und Architekturen 37
2.5.1 Geräte-Typen 37
2.5.2 Vorgesehene Architekturen vs. Ein- und Zweikanaligkeit und *SFF* 41
2.6 Diagnose und Diagnosedeckungsgrad 53
2.7 Fehlerausschlüsse 62
2.8 *PFH* oder PFH_D 66
2.9 CCF und systematische Ausfälle 70
2.10 Validieren mit Verifizieren 76
2.11 Security-Aspekte 80

3 Liste der Sicherheitsfunktionen nach DIN EN ISO 12100 87
3.1 Sicherheitsfunktionen zum Schutz von Personen 92
3.2 Andere Sicherheitsfunktionen 92
3.3 Sicherheitsfunktionen zum Schutz der Maschine 92

4 Software erstellen und prüfen 97
4.1 Grundsätzliches 97
4.2 Anwendungssoftware 99
4.3 Softwareentwurf – SW-Level 1 101
4.4 Softwareentwurf – SW-Level 2 110
4.5 Programmierrichtlinien 119

4.6 Spezifikation der Software 121
4.7 Programmgestaltung 122
4.8 Verifizieren und Validieren 124

5 Validierung 127
5.1 Grundsätzliches 127
5.2 Relevante Informationen 128
5.3 Tests und Prüfungen. 134
5.4 Validierung jeder Sicherheitsfunktion 135

6 Dokumentation. 137
6.1 Muss und Kann 137
6.2 Struktur 138
6.3 Vorlagen zum kopieren 141

7 Hintergrundwissen zu *PFH* 145
7.1 Hilfreiche Tabellen. 145
7.2 *PFH*-Formeln im Überblick 149
7.3 Grundannahmen für die *PFH*-Ermittlung 153
7.3.1 Allgemein 153
7.3.2 Definitionen 153
7.4 Einkanalige Architektur, ohne Diagnose 159
7.4.1 Allgemein 159
7.4.2 *PFH* 160
7.5 Einkanalige Architektur, mit Diagnose 160
7.5.1 Allgemein 160
7.5.2 Fehlerreaktion durch ein anderes Teilsystem. 160
7.5.3 Im Teilsystem zu berücksichtigende Fehlerreaktion 162
7.5.4 Betrachtung von CCF 165
7.5.5 Einfluss von CCF. 166
7.6 Zweikanalige Architektur, ohne Diagnose. 169
7.6.1 Allgemein 169
7.6.2 *PFH* 170
7.6.3 Einfluss von CCF. 170
7.7 Zweikanalige Architektur, mit Diagnose 171
7.7.1 Allgemein 171
7.7.2 *PFH*-Ermittlung für den Term A 172
7.7.3 *PFH*-Ermittlung für den Term B 173
7.7.4 *PFH*-Ermittlung für den Term C 173
7.7.5 *PFH*-Ermittlung für den Term C und Term D 173

7.7.6 *PFH* aller Terme 173
7.7.7 Einfluss von CCF 174
7.8 Zweikanalige Architektur, mit Diagnose und mit zwei Betrachtungszeiträumen 174
7.8.1 Allgemein 174
7.8.2 *PFH*-Ermittlung für den Term A 175
7.8.3 *PFH*-Ermittlung für den Term B 175
7.8.4 *PFH*-Ermittlung für den Term C und Term D 175
7.8.5 *PFH* aller Terme 176
7.8.6 Einfluss von CCF 176

8 Risikobeurteilung 179
8.1 Detaillierte Vorgehensweise 179
8.2 Gefährdungen 185
8.3 Gefahren und die Ermittlung von SIL und PL 191
8.4 Risikominderung 194

9 Begriffe und Definitionen 199
9.1 Übersicht aller Abkürzungen und Begriffe 199
9.2 Begriffe kompakt – ergänzend erläutert 202
9.3 Fachwörterbuch Deutsch – Englisch 248

10 Normenlotse 257

11 Die Software „FSP“ 271
11.1 Quick Start (Portable und Start) 271
11.2 Projektinformation 283
11.3 Import 284
11.4 Risikobeurteilung 286
11.5 Basis-Maßnahmen 293
11.6 Funktionale Anforderungen (einer Sicherheitsfunktion) 296
11.7 SCS oder SRP/CS 298
11.8 Software 308
11.9 Validierung 309
11.10 Dokumentation 310
11.11 MeineTypicals (oder Vorlagen) 313