

Inhalt

Vorwort	3
Danksagung	4
Kontakt	5
1 Einleitung	8
2 Sicherheitslebenszyklus	9
3 Prozessübersicht	12
3.1 Management der funktionalen Sicherheit	13
3.2 Konzeptphase	16
3.3 Produktentwicklung auf System-Ebene	21
3.4 Produktentwicklung auf Hardware-Ebene	29
3.5 Produktentwicklung auf Software-Ebene	36
3.6 Produktion und Betrieb	49
3.7 Unterstützungsprozesse	53
3.8 Automotive Sicherheitsintegritätslevel (ASIL)- und Sicherheitsanalysen	62
4 Beziehungen zu CMMI®, Automotive SPICE®, Agile	68
4.1 Capability Maturity Model Integration (CMMI®)	70
4.2 Automotive SPICE®	71
4.3 Agile Entwicklungsmethoden	72
5 Rollenübersicht	76
6 Beschreibung der Prozessergebnisse	78
6.1 Analyse von Verletzungen der Sicherheitsziele aufgrund zufälliger Hardware-Ausfälle	78
6.2 Assessment der funktionalen Sicherheit	79
6.3 Audit der funktionalen Sicherheit	81
6.4 Funktionales Sicherheitskonzept	81
6.5 Hardware-Architekturmetriken	83
6.6 Spezifikation des Hardware-Designs	84
6.7 Spezifikation der Hardware-Sicherheitsanforderungen	85
6.8 Hardware-Software-Schnittstelle (HSI)	86
6.9 Gefährdungs- und Risikoanalyse (G&R)	87
6.10 Item-Integrations- und -testplan	90
6.11 Nachweis der Betriebsbewährtheit	91
6.12 Qualifizierung von Hardware-Komponenten	92
6.13 Qualifizierung von Software-Komponenten	93
6.14 Sicherheitsanalysen	94
6.15 Sicherheitsnachweis	95
6.16 Sicherheitsziel	96
6.17 Sicherheitsplan	97
6.18 Spezifikation der Sicherheitsanforderungen	99
6.19 Software-Architekturentwurf	100

6.20 Spezifikation der Software-Sicherheitsanforderungen	101
6.21 Bericht zur Qualifizierung von Software-Werkzeugen/Bericht	103
zur Bewertung von Software-Werkzeugkriterien	
6.22 Spezifikation des Designs der Software-Einheiten	104
6.23 Implementierung der Software-Einheit	105
6.24 Spezifikation des System-Designs	106
6.25 Spezifikation der technischen Sicherheitsanforderungen	107
6.26 Validierungsplan	108
7 Beispiel	110
7.1 Management der funktionalen Sicherheit	110
7.2 Konzeptphase	110
7.3 Produktentwicklung auf System-Ebene (Linke Seite des V-Modells)	112
7.4 Produktentwicklung auf Hardware-Ebene	114
7.5 Produktentwicklung auf Software-Ebene	117
7.6 Produktentwicklung auf System-Ebene (Rechte Seite des V-Modells)	124
7.7 Produktion und Betrieb	125
7.8 Unterstützungsprozesse	125
7.9 Automotive Sicherheitsintegritätslevel (ASIL)- und Sicherheitsanalysen	126
Die Autoren	128
Glossar und Stichwortverzeichnis	130
Literatur	140
Fußnoten	141