

Inhalt

	Seite
Europäisches Vorwort	2
Einleitung	8
1 Anwendungsbereich	11
2 Normative Verweisungen	11
3 Begriffe, Abkürzungen, Akronyme und Vereinbarungen	11
3.1 Begriffe	11
3.2 Abkürzungen und Akronyme	18
3.3 Vereinbarungen	18
4 Allgemeine Grundsätze	19
4.1 Ziele	19
4.2 Reifegradmodell	20
5 Ansatz 1 – Verwaltung der IT-Sicherheit	22
5.1 Zweck	22
5.2 SM-1: Entwicklungsprozess	22
5.2.1 Anforderung	22
5.3 Begründung und zusätzliche Leitfäden	22
5.4 SM-2: Kennzeichnung von Verantwortlichkeiten	23
5.4.1 Anforderung	23
5.4.2 Begründung und zusätzliche Leitfäden	23
5.5 SM-3: Kennzeichnung der Anwendbarkeit	23
5.5.1 Anforderung	23
5.5.2 Begründung und zusätzliche Leitfäden	23
5.6 SM-4: Fachkenntnisse im Hinblick auf die IT-Sicherheit	24
5.6.1 Anforderung	24
5.6.2 Begründung und zusätzliche Leitfäden	24
5.7 SM-5: Prozesseingrenzung	24
5.7.1 Anforderung	24
5.7.2 Begründung und zusätzliche Leitfäden	24
5.8 SM-6: Integrität von Dateien	24
5.8.1 Anforderung	24
5.8.2 Begründung und zusätzliche Leitfäden	25
5.9 SM-7: IT-Sicherheit der Entwicklungsumgebung	25
5.9.1 Anforderung	25
5.9.2 Begründung und zusätzliche Leitfäden	25
5.10 SM-8: Überwachung privater Schlüssel	25
5.10.1 Anforderung	25
5.10.2 Begründung und zusätzliche Leitfäden	25

	Seite
5.11 SM-9: Anforderungen an die IT-Sicherheit von extern bereitgestellten Komponenten.....	25
5.11.1 Anforderung.....	25
5.11.2 Begründung und zusätzliche Leitfäden	26
5.12 SM-10: Kundenspezifische Komponenten von Fremdanbietern.....	26
5.12.1 Anforderung.....	26
5.12.2 Begründung und zusätzliche Leitfäden	26
5.13 SM-11: Bewertung und Behandlung sicherheitsbezogener Probleme	27
5.13.1 Anforderung.....	27
5.13.2 Begründung und zusätzliche Leitfäden	27
5.14 SM-12: Prozessverifikation.....	27
5.14.1 Anforderung.....	27
5.14.2 Begründung und zusätzliche Leitfäden	27
5.15 SM-13: Ständige Verbesserung	27
5.15.1 Anforderung.....	27
5.15.2 Begründung und zusätzliche Leitfäden	27
6 Ansatz 2 – Spezifikation der IT-Sicherheitsanforderungen	29
6.1 Zweck	29
6.2 SR-1: IT-Sicherheitsumfeld des Produkts	29
6.2.1 Anforderung.....	29
6.2.2 Begründung und zusätzliche Leitfäden	29
6.3 SR-2: Bedrohungsmodell	30
6.3.1 Anforderung.....	30
6.3.2 Begründung und zusätzliche Leitfäden	30
6.4 SR-3: IT-Sicherheitsanforderungen für das Produkt	31
6.4.1 Anforderung.....	31
6.4.2 Begründung und zusätzliche Leitfäden	31
6.5 SR-4: Anforderungen an das IT-Sicherheitsumfeld des Produkts	31
6.5.1 Anforderung.....	31
6.5.2 Begründung und zusätzliche Leitfäden	31
6.6 SR-5: Überblick über IT-Sicherheitsanforderungen	32
6.6.1 Anforderung.....	32
6.6.2 Begründung und zusätzliche Leitfäden	32
7 Ansatz 3 – IT-Sicherheit durch den Entwurf.....	32
7.1 Zweck	32
7.2 SD-1: Grundsätze für einen gesicherten Entwurf.....	32
7.2.1 Anforderung.....	32
7.2.2 Begründung und zusätzliche Leitfäden	33
7.3 SD-2: Entwurf eines Defense-in-Depth-Konzepts	34
7.3.1 Anforderung.....	34

	Seite
7.3.2 Begründung und zusätzliche Leitfäden.....	34
7.4 SD-3: Entwurfsprüfung der IT-Sicherheit.....	34
7.4.1 Anforderung	34
7.4.2 Begründung und zusätzliche Leitfäden.....	35
7.5 SD-4: Bewährte Verfahren des gesicherten Entwurfs	35
7.5.1 Anforderung	35
7.5.2 Begründung und zusätzliche Leitfäden.....	35
8 Ansatz 4 – Gesicherte Implementierung.....	36
8.1 Zweck.....	36
8.2 Anwendbarkeit.....	36
8.3 SI-1: Überprüfung der gesicherten Implementierung.....	36
8.3.1 Anforderung	36
8.3.2 Begründung und zusätzliche Leitfäden.....	36
8.4 SI-2: Codierungsnormen für IT-Sicherheit	37
8.4.1 Anforderung	37
8.4.2 Begründung und zusätzliche Leitfäden.....	37
9 Ansatz 5 – Verifikations- und Validierungsprüfungen der IT-Sicherheit	37
9.1 Zweck.....	37
9.2 SVV-1: Prüfung der IT-Sicherheitsanforderungen	38
9.2.1 Anforderung	38
9.2.2 Begründung und zusätzliche Leitfäden.....	38
9.3 SVV-2: Prüfung der Bedrohungsabschwächung	38
9.3.1 Anforderung	38
9.3.2 Begründung und zusätzliche Leitfäden.....	38
9.4 SVV-3: Prüfung von Sicherheitslücken	39
9.4.1 Anforderung	39
9.4.2 Begründung und zusätzliche Leitfäden.....	39
9.5 SVV-4: Eindringprüfung	39
9.5.1 Anforderung	39
9.5.2 Begründung und zusätzliche Leitfäden.....	39
9.6 SVV-5: Unabhängigkeit der Prüfer.....	40
9.6.1 Anforderung	40
9.6.2 Begründung und zusätzliche Leitfäden.....	41
10 Ansatz 6 – Behandlung sicherheitsbezogener Probleme	41
10.1 Zweck.....	41
10.2 DM-1: Empfang von Meldungen über sicherheitsbezogene Probleme	41
10.2.1 Anforderung	41
10.2.2 Begründung und zusätzliche Leitfäden.....	41
10.3 DM-2: Überprüfung sicherheitsbezogener Probleme.....	42

	Seite
10.3.1	Anforderung..... 42
10.3.2	Begründung und zusätzliche Leitfäden 42
10.4	DM-3: Bewertung sicherheitsbezogener Probleme..... 42
10.4.1	Anforderung..... 42
10.4.2	Begründung und zusätzliche Leitfäden 43
10.5	DM-4: Behandlung sicherheitsbezogener Probleme..... 43
10.5.1	Anforderung..... 43
10.5.2	Begründung und zusätzliche Leitfäden 44
10.6	DM-5: Offenlegung sicherheitsbezogener Probleme 44
10.6.1	Anforderung..... 44
10.6.2	Begründung und zusätzliche Leitfäden 45
10.7	DM-6: Periodische Überprüfung der Behandlungsverfahren für Mängel der IT-Sicherheit 45
10.7.1	Anforderung..... 45
10.7.2	Begründung und zusätzliche Leitfäden 45
11	Ansatz 7 – Verwaltung von IT-Sicherheits-Updates..... 45
11.1	Zweck 45
11.2	SUM-1: Eignung von IT-Sicherheits-Updates 46
11.2.1	Anforderung..... 46
11.2.2	Begründung und zusätzliche Leitfäden 46
11.3	SUM-2: Dokumentation von IT-Sicherheits-Updates 46
11.3.1	Anforderung..... 46
11.3.2	Begründung und zusätzliche Leitfäden 46
11.4	SUM-3: Dokumentation der IT-Sicherheits-Updates für abhängige Komponenten oder Betriebssysteme 47
11.4.1	Anforderung..... 47
11.4.2	Begründung und zusätzliche Leitfäden 47
11.5	SUM-4: Auslieferung von IT-Sicherheits-Updates 47
11.5.1	Anforderung..... 47
11.5.2	Begründung und zusätzliche Leitfäden 47
11.6	SUM-5: Rechtzeitige Auslieferung von IT-Sicherheitspatches..... 47
11.6.1	Anforderung..... 47
11.6.2	Begründung und zusätzliche Leitfäden 48
12	Ansatz 8 – IT-Sicherheitsrichtlinien 48
12.1	Zweck 48
12.2	SG-1: Defense-in-Depth-Strategie für das Produkt..... 48
12.2.1	Anforderung..... 48
12.2.2	Begründung und zusätzliche Leitfäden 48
12.3	SG-2: Maßnahmen des Defense-in-Depth-Konzepts, die von der Umgebung zu erwarten sind 49

	Seite
12.3.1 Anforderung	49
12.3.2 Begründung und zusätzliche Leitfäden.....	49
12.4 SG-3: Richtlinien für die Härtung der IT-Sicherheit.....	49
12.4.1 Anforderung	49
12.4.2 Begründung und zusätzliche Leitfäden.....	50
12.5 SG-4: Richtlinien für eine gesicherte Entsorgung	50
12.5.1 Anforderung	50
12.5.2 Begründung und zusätzliche Leitfäden.....	50
12.6 SG-5: Richtlinien für einen gesicherten Betrieb	50
12.6.1 Anforderung	50
12.6.2 Begründung und zusätzliche Leitfäden.....	50
12.7 SG-6: Richtlinien für die Nutzerkontoverwaltung	51
12.7.1 Anforderung	51
12.7.2 Begründung und zusätzliche Leitfäden.....	51
12.8 SG-7: Überprüfung der Dokumentation	51
12.8.1 Anforderung	51
12.8.2 Begründung und zusätzliche Leitfäden.....	51
Anhang A (informativ) Mögliche Maßgrößen.....	52
Anhang B (informativ) Tabelle der Anforderungen.....	54
Literaturhinweise	56
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen.....	59
 Bilder	
Bild 1 – Teile der Normenreihe IEC 62443.....	9
Bild 2 – Beispiel für den Anwendungsbereich eines Produktlebenszyklus	10
Bild 3 – Eine Defense-in-Depth-Strategie ist ein Kerngedanke des gesicherten Produktlebenszyklus.....	20
 Tabellen	
Tabelle 1 – Reifegrade	21
Tabelle 2 – Beispiele für Aktivitäten der ständigen Verbesserung von SDL.....	28
Tabelle 3 – Geforderter Grad der Unabhängigkeit der Prüfer von den Entwicklern	40
Tabelle B.1 – Zusammenfassung aller Anforderungen.....	54