

Anwendungsbereich

Anwendungsbereich dieser Norm ist ...

Inhalt

	Seite
Nationales Vorwort.....	4
1 Anwendungsbereich.....	15
1.1 Allgemeines.....	15
1.2 Anwendung.....	16
1.3 Rahmen.....	16
2 Normative Verweisungen.....	18
3 Begriffe.....	18
4 Formelzeichen und Abkürzungen.....	21
5 Erstellung und Management einer IT-Sicherheitsplanung für nukleare Leittechnik.....	22
5.1 Allgemeines.....	22
5.1.1 Kontext, Gesamtkonzepte und Ziele.....	22
5.1.2 Rollen und Verantwortlichkeiten.....	23
5.1.3 Vorgehensweisen und Prozeduren.....	24
5.1.4 Dokumentations-Anforderungen.....	25
5.2 Errichtung des IT-Sicherheitsplans.....	25
5.2.1 Definition der Vorgehensweise.....	25
5.2.2 Definition von Aufgabenbereich und Grenzen.....	26
5.2.3 Abgestuftes Vorgehen zu IT-Sicherheit und Risiko-Untersuchung der Leittechnik.....	26
5.2.4 Management-Genehmigung.....	31
5.3 Realisierung und Betrieb der IT-Sicherheitspläne.....	32
5.3.1 Allgemeine Realisierungs-Anforderungen.....	32
5.3.2 Definition der Effektivitätsmessung.....	32
5.3.3 Training und Sensibilisierung.....	32
5.4 Überwachung und Überprüfung des IT-Sicherheitsplans.....	33
5.5 Aufrechterhaltung und Verbesserung des IT-Sicherheitsplans.....	33
6 Lebenszyklus-Realisierung für die IT-Sicherheit des leittechnischen Systems.....	33
6.1 Allgemeines.....	33
6.2 Anforderungsphase.....	33
6.3 Planungsphase.....	34
6.3.1 Ermittlung und Klassifizierung von Einrichtungen der rechnerbasierten Leittechnik.....	34
6.4 Auslegungsphase.....	34
6.4.1 Allgemeines.....	34
6.4.2 Risiko-Untersuchung in der Auslegungsphase.....	34
6.4.3 Projekt-IT-Sicherheitsplan.....	34
6.4.4 Kommunikationswege.....	35
6.5 Realisierungsphase.....	35

	Seite
6.6 Validierungsphase.....	35
6.7 Errichtungs- und Abnahmetest-Phase.....	35
6.8 Betriebs- und Wartungsphase.....	35
6.9 Änderungs-Management.....	36
6.10 Außerbetriebsetzung.....	36
7 IT-Sicherheitskontrollen	36
7.1 Allgemeines.....	36
7.2 IT-Sicherheits-Themenfelder.....	37
7.2.1 IT-Sicherheitsstrategie	37
7.2.2 Organisation der IT-Sicherheit.....	37
7.2.3 Asset Management	37
7.2.4 IT-Sicherheit der menschlichen Ressourcen	38
7.2.5 Physikalische und Umgebungs-mit-Sicherheit.....	38
7.2.6 Kommunikations- und Betriebs-Management.....	39
7.2.7 Zugriffskontrolle.....	39
7.2.8 Akquisition, Entwicklung und Wartung leittechnischer Systeme.....	39
7.2.9 Störungsmanagement der leittechnischen IT-Sicherheit.....	40
7.2.10 Management der Betriebskontinuität	40
7.2.11 Übereinstimmung	40
Anhang A (informativ) Beispiele von abgestuften Vorgehensweisen zur leittechnischen IT-Sicherheit.....	41
A.1 Allgemeines.....	41
A.2 Beispiel Zonenarchitektur der abgestuften Vorgehensweise.....	41
A.3 Beispiel IT-Sicherheitsgrade und IT-Sicherheitszonenmodell	44
A.3.1 Allgemeines.....	44
A.3.2 Beispiel IT-Sicherheitsgrad	44
A.3.3 Beispiel IT-Sicherheitszonen.....	45
A.3.4 Zuordnung von erhöhten IT-Sicherheitsgraden	46
A.3.5 Partielle Erhöhung des IT-Sicherheitsgrades eines leittechnischen Teilsystems.....	47
Anhang B (informativ) Generische Überlegungen über IT-Sicherheitsgrade.....	48
B.1 Warum drei IT-Sicherheitsgrade	48
B.2 Was geschieht mit Werkzeugen für Online-Systeme.....	48
B.3 Praktische Auslegung und Implementierung	48
Anhang C (informativ) Vergleich mit ISO/IEC 27001	50
Anhang D (informativ) Übereinstimmung mit dem NIST IT-Sicherheitsrahmen	52
D.1 Aufgabenbereich	52
D.2 Korrelation zwischen IEC und NIST Cyber-Sicherheitsrahmen.....	52
Anhang E (informativ) Angreiferprofile und Angriffsszenarien	56
Literaturhinweise	57