

Inhaltsverzeichnis

1	Einleitung	9
2	Cybersecurity wird durch Technologie, Prozesse und Menschen bestimmt ...	11
3	Rollen in der IEC 62443	15
4	Struktur der IEC 62443	17
5	Konzepte der IEC 62443	21
5.1	Tiefgestaffelte Verteidigung (Defense-in-Depth)	21
5.2	Die Norm IEC 62443 in Produkt- und IACS-Lebenszyklen	24
5.3	Risikobewertung nach VDI/VDE 2182	27
5.4	Security-Levels	33
6	Security-Programm (SP) und Security Protection Scheme (SPS)	37
6.1	Zusammenhang zwischen Security-Programm (SP) und Security Protection Scheme (SPS)	37
6.2	Entwicklung und Betrieb eines Schutzschemas	38
7	Security Protection Ratings (SPR)	43
7.1	Definition und Methode	43
7.2	Anwendung von SPR in der Risikoreduzierung	47
7.3	SPR- und SL-Ausprägungen	48
7.4	Gruppierung der System-Securityanforderungen	50
8	Kombination von ISO/IEC 27001/2 und IEC 62443	57
9	Rollenbasierte Aktivitäten und Beiträge für die Implementierung eines ganzheitlichen Schutzkonzepts	65
9.1	Spezifikation	66
9.2	Design	70
9.3	Implementierung	76
9.4	Verifikation und Validierung	77
9.5	Betrieb und Wartung	79
9.6	Update	80
9.7	Abbau	81
10	Vorgehensweise zum Aufbau eines Schutzkonzepts	83
10.1	Überblick	83
10.2	Anlagensicherheit	84
10.3	Netzwerksicherheit	85

10.4	Systemintegrität.....	89
10.5	Nutzerrollen und Rechtekonzepte.....	90
Anhang A Wesentliche Dokumente zur Erstellung und Pflege eines Schutzkonzepts ..		93
Anhang B Weitere Dokumente der IEC 62443.....		121
Anhang C Zuordnung der Securityanforderungen zu den Elementen des Security- Programms (SP) des Betreibers		129
Abkürzungen		153
Literaturverzeichnis.....		155
Stichwortverzeichnis		157