
Inhaltsverzeichnis

1	UNECE-Regulierung 155	1
1.1	Interpretation	3
1.2	Mapping der Anforderungen auf Prozessgruppen	4
1.3	Prozesshierarchie und Schnittstellen	4
2	Aufbau eines Cybersecurity Management Systems	7
2.1	Engineering-Prozesse	8
2.1.1	Cybersecurity Project Management Process	8
2.1.2	Risk Assessment und Risk Assessment Verification (TARA)	12
2.1.3	Requirement Specification und Implementation	16
2.1.4	Verification and Validation	19
2.1.5	Problem and Change Management	21
2.1.6	Release for Post Development	22
2.1.7	Production Control Verification	22
2.1.8	Quotation	23
2.1.9	Supplier Selection	23
2.2	CSMS Policy/Kernprozesse	25
2.2.1	Tool Management	26
2.2.2	Information Sharing	26
2.2.3	Configuration Management	27
2.2.4	Vulnerability Assessment & Management	28
2.2.5	Continuous Improvement	29

2.2.6	Supplier Monitoring	30
2.3	Vehicle Security Operation Center	31
2.3.1	Monitoring	33
2.3.2	Event Classification und Clearing	34
2.3.3	Forensics	35
2.3.4	Incident Response	35
2.3.5	Supplier Management	36
2.3.6	Reporting	36
2.3.7	End of Cybersecurity Support	36
3	Rollenkonzept	39
3.1	Cybersecurity Manager Projekt	39
3.2	Cybersecurity Engineer	40
3.3	Cybersecurity Manager Organisation	40
4	Kennzahlen (KPIs)	41
5	Audit eines Cybersecurity Management Systems	43
5.1	Arten von Audits	43
5.2	Auditdurchführung	44
6	Lessons learned	47
6.1	Schwierige Prozesse	47
6.2	Audits in der Lieferkette	47
7	Schnittstellen/Randthemen	49
	Was Sie aus diesem <i>essential</i> mitnehmen können	51
	Literatur	53