

Inhaltsverzeichnis

INHALTSVERZEICHNIS	III
ABBILDUNGSVERZEICHNIS	IX
ZUSAMMENFASSUNG	X
DANKSAGUNG	XI
VORWORT	XII
1 EINFÜHRUNG IN DIE INDUSTRIE 4.0	1
1.1 INDUSTRIE IM WANDEL	1
1.2 TECHNOLOGIEFELDER DER INDUSTRIE 4.0	4
1.3 CHANCEN UND RISIKEN IN DER INDUSTRIE 4.0	6
2 SECURITY & SAFETY	9
2.1 SECURITY (INFORMATIONSSICHERHEIT)	9
2.2 SAFETY (BETRIEBSSICHERHEIT)	9
3 INFORMATIONS- UND BETRIEBSSICHERHEIT IN SMART FACTORIES.....	11
3.1 NORMUNGSINSTITUTIONEN UND DEREN GREMIEN.....	11
3.1.1 ISO/IEC.....	11
3.1.2 ISA.....	12
3.1.3 NIST	12
3.1.4 US-DHS/ICS-CERT.....	12
3.1.5 CEN/CENELEC/ETSI	13
3.1.6 NATIONALE NORMUNGSINSTITUTIONEN	13
3.1.7 VDI/VDE	14
3.1.8 BSI	14

3.1.9	PLATTFORM INDUSTRIE 4.0.....	14
3.2	NORMEN UND RICHTLINIEN	15
3.2.1	IEC 62443.....	15
3.2.2	IEC 61508.....	20
3.2.3	NIST SP 800-53 & NIST SP 800-82R2	21
3.2.4	US-DHS/ICS-CERT PUBLIKATIONEN	22
3.2.5	RICHTLINIE VDI/VDE 2182	23
3.2.6	ICS-SECURITY-KOMPENDIUM.....	24
3.2.7	PLATTFORM-INDUSTRIE-4.0-ARBEITEN	25
4	INDUSTRIEPROTOKOLLE.....	27
4.1	SICHERHEIT VON INDUSTRIEPROTOKOLLEN	27
4.2	MODBUS	27
4.3	PROFIBUS	29
4.3.1	ANGRIFFE	32
4.4	PROFINET	32
4.5	CC-LINK (CONTROL AND COMMUNICATION LINK)	34
4.6	ETHERNET/IP	35
4.7	CAN (CONTROLLER AREA NETWORK)	36
4.7.1	CAN REMOTE FRAMES	37
4.8	DNP3 (DISTRIBUTED NETWORK PROTOCOL)	37
4.8.1	ANGRIFFE AUF DNP3	40
4.8.2	OPENDNP3	43
4.8.3	RESILIENTES DNP3-PARSING	43
4.9	OPC-UA (UNIFIED ARCHITECTURE).....	43
4.9.1	SICHERHEITSANALYSE DES BSI.....	45
4.9.2	EMPFEHLUNGEN	46
5	INTERNET OF THINGS.....	47
5.1	DEFINITIONEN IM INTERNET OF THINGS.....	47

5.1.1	INTERNET	47
5.1.2	THINGS.....	48
5.2	GESCHICHTE	49
5.3	LAYER IM INTERNET OF THINGS.....	49
5.3.1	PERCEPTION LAYER	49
5.3.2	NETWORK LAYER.....	50
5.3.3	APPLICATION LAYER	50
5.4	KOMMUNIKATIONSARTEN	51
5.4.1	DEVICE TO DEVICE	51
5.4.2	DEVICE TO GATEWAY	52
5.4.3	DEVICE TO CLOUD	52
5.4.4	BACK END DATA SHARING MODEL	53
5.5	KATEGORISIERUNG DER DEVICES	53
5.5.1	SMART WEARABLE	53
5.5.2	SMART HOME.....	53
5.5.3	SMART CITY	54
5.5.4	SMART ENVIRONMENT	54
5.5.5	SMART ENTERPRISE	54
5.6	REGULIERUNG	55
5.7	DAS POTENTIAL DES IoT	55
5.7.1	ANWENDUNGSFÄLLE FÜR PRIVATPERSONEN	56
5.7.2	ANWENDUNGSFÄLLE FÜR UNTERNEHMEN	56
5.8	HERAUSFORDERUNGEN IM IoT	57
5.9	IoT IN DER EU	58
6	SICHERHEIT UND PRIVATSPHÄRE IM INTERNET OF THINGS.....	59
6.1	SICHERHEIT UND PRIVATSPHÄRE	59
6.2	BEDROHUNGEN IM IoT.....	61
6.2.1	DENIAL OF SERVICE	61
6.2.2	SPOOFING	62

6.2.3	INFORMATION DISCLOSURE.....	63
6.2.4	INFORMATION TAMPERING	63
6.2.5	ELEVATION OF PRIVILEGES	63
6.3	ANFORDERUNGEN	64
6.3.1	MONITORING UND FILTERING.....	65
6.3.2	ZUGRIFFSKONTROLLE	65
6.3.3	VERSCHLÜSSELUNG.....	67
6.3.4	PHYSISCHE SICHERHEIT.....	68
6.3.5	SICHERE INTERFACES.....	69
6.4	DISKUSSION DER RISIKEN	70
7	CYBER-PHYSISCHE SYSTEME	71
7.1	GESCHICHTE UND DEFINITION.....	71
7.2	TERMINOLOGIE UND ABGRENZUNG.....	73
7.3	ANWENDUNGSGEBIETE	74
7.3.1	MEDIZIN	74
7.3.2	PRODUKTION	75
7.3.3	SMART BUILDINGS	75
7.3.4	VERKEHR.....	76
7.3.5	KRITISCHE INFRASTRUKTUR	77
7.4	HERAUSFORDERUNGEN VON CYBER-PHYSISCHEN SYSTEMEN	79
7.4.1	INTEROPERABILITÄT (INTEROPERABILITY)	80
7.4.2	VORHERSEHBARKEIT (PREDICTABILITY).....	81
7.4.3	ZUVERLÄSSIGKEIT (RELIABILITY)	82
7.4.4	VERLÄSSLICHKEIT (DEPENDABILITY).....	83
7.4.5	NACHHALTIGKEIT (SUSTAINABILITY)	84
7.4.6	SICHERHEIT (SECURITY)	85
8	SICHERHEIT VON CYBER-PHYSISCHEN SYSTEMEN	87
8.1	UNTERSCHIEDUNG ZU REIN VIRTUELLEN SYSTEMEN UND DARAUS RESULTIERENDE ANFORDERUNGEN	87

8.1.1	INPUT UND FEEDBACK VON PHYSIKALISCHER UMGEBUNG	87
8.1.2	ECHTZEITANFORDERUNG	87
8.1.3	UMGANG MIT PAKETEN	87
8.1.4	MESSSICHERHEIT	88
8.1.5	OBFUSKIERUNG VON METADATEN	88
8.1.6	SICHERE AGGREGATION	88
8.1.7	OBFUSKIERUNG DER TOPOLOGIE	88
8.1.8	ANONYMITÄT BEI AGGREGATION	89
8.1.9	VERTRAUENSMANAGEMENT	89
8.1.10	STEUERUNG UND VERWALTUNG	89
8.1.11	BETRIEBSSICHERHEIT	90
8.1.12	ZUSAMMENFASSUNG	90
8.2	BEKANNTE ANGRIFFSMETHODEN IN BEZUG AUF CPS.....	90
8.2.1	EAVESDROPPING	90
8.2.2	COMPROMISED-KEY.....	90
8.2.3	MAN IN THE MIDDLE	91
8.2.4	DENIAL OF SERVICE	91
8.2.5	MANIPULATION ODER ZERSTÖRUNG VON GERÄTEN ODER ZUBEHÖR.....	91
8.2.6	PHYSISCHER EINGRIFF IN EIN EINGEBETTETES SYSTEM	91
8.2.7	AUSWIRKUNGEN AUF BETRIEBSSICHERHEIT	92
8.3	ANGRIFFSERKENNUNG UND CPS-SPEZIFISCHE GEGENMAßNAHMEN	92
8.3.1	VERTRAUENSMANAGEMENT	92
8.3.2	ANOMALIEERKENNUNG	93
8.4	HERAUSFORDERUNGEN UND MAßNAHMEN	93
8.4.1	HERAUSFORDERUNGEN UND MAßNAHMEN AUS DER SICHT DER INFORMATIONSSICHERHEIT	93
8.4.2	HERAUSFORDERUNGEN UND MAßNAHMEN AUS DER SICHT DER BETRIEBSSICHERHEIT	96
9	SMART CONTRACTS.....	99
9.1	HERAUSFORDERUNGEN BEI DER NUTZUNG DEZENTRALER SYSTEME	99
9.1.1	ARCHITEKTUR VON ZENTRALEN UND DEZENTRALEN SYSTEMEN.....	99

9.1.2	DURCHSETZBARKEIT VON INTERESSEN IN AUTONOMEN TEILSYSTEMEN	100
9.2	BLOCKCHAIN-TECHNOLOGIE	101
9.3	EINFÜHRUNG IN SMART CONTRACTS	104
9.3.1	SMART-CONTRACTS-PROGRAMMIERUNG	106
9.4	RECHTLICHE ASPEKTE	108
9.4.1	EINFÜHRUNG UND PROBLEMAUFRISS	108
9.4.2	EINSATZ VON MDL-SYSTEMEN IM VERTRAGSMANAGEMENT	110
9.4.3	EINSATZ VON MDL-SYSTEMEN IN DER VERTRAGSERSTELLUNG UND -DURCHSETZUNG	110
10	CLOUD-COMPUTING	117
10.1	CLOUD-CHARAKTERISTIKEN	117
10.2	SERVICEMODELLE	118
10.2.1	INFRASTRUCTURE-AS-A-SERVICE	119
10.2.2	PLATFORM-AS-A-SERVICE	119
10.2.3	SOFTWARE-AS-A-SERVICE	120
10.2.4	EVERYTHING-AS-A-SERVICE	120
10.3	BETRIEBSMODELLE	120
10.4	CLOUD-SICHERHEIT	121
10.4.1	LOCK-IN-EFFEKT	121
10.4.2	SERVICE-LEVEL-AGREEMENTS	121
10.4.3	DATENSCHUTZ	121
10.4.4	BEDROHUNGEN	122
10.4.5	MAßNAHMEN	122
11	LITERATURVERZEICHNIS	125
INDEX		144