

# Inhalt

<b>EchoRing™ – Wireless Safety durch Massive Kooperation</b> .....	1
1 Einführung .....	1
2 Kommunikation über den kabellosen Kanal .....	3
2.1 Gründe für Übertragungsfehler .....	3
2.2 Maßnahmen gegen Übertragungsfehler .....	4
3 Kooperation verschiedener Knoten eines kabellosen Systems ....	5
3.1 Kooperation durch Relaying .....	6
3.2 Massive Kooperation .....	8
4 <b>EchoRing™ – ein auf massiver Kooperation basierendes Kabellos- system</b> .....	8
4.1 Massive Kooperation durch instantane Relay-Wahl .....	9
4.2 Die Performance von EchoRing™ im Vergleich mit anderen Systemen .....	10
5 Zusammenfassung und Ausblick .....	11
6 Autoren .....	12
7 Quellen .....	12
<b>Sichere Drahtlos-Handbediengeräte</b> .....	14
1 Einführung .....	14
2 Das Problem .....	14
3 EchoRing .....	15
3.1 EchoRing erfüllt die Anforderungen .....	15
3.2 Lösung in Kooperation mit R3Communication .....	16
4 Anwendung in Handbediengeräten .....	16
4.1 Use Cases .....	17
4.2 Tablets und Smartphones .....	17
4.3 Sicherheitsgeräte .....	18
4.4 Smart und sicher .....	18
4.5 Übertragung von sicheren Daten .....	19
4.6 Das Handgerät mit EchoRing .....	20
4.7 Wechselnde Verbindungen .....	21
4.8 Security .....	23
4.8.1 Updates .....	23
5 Einsatz im Umfeld von Industrie 4.0 .....	24

2	Systemübersicht und Hardwarekomponenten .....	90
2.1	Konzept und Gesamtüberblick .....	90
3	lilix®-Reflektor .....	91
4	RTU / Multi Port OTDR .....	92
5	PIM – Parallel Interface Module – Detektion .....	93
6	SIM – Serial Interface Module – Detektion & Lokalisation .....	93
7	SDIM – Shut Down Interface Module .....	94
8	CAG – Connection Assembly Group .....	94
9	NMS (Network Management System) via Element Manager & Line Control Manager .....	94
10	Systemübersicht: In-Service, Dark Fiber, P2P & P2MP .....	96
11	Systemübersicht: Mess-PON in P2P Topologie .....	96
12	Sicherheits-Applikationen .....	98
12.1	OPTION: Abhörsicherheit – Optical Tapping & Non Touching .....	98
12.2	OPTION: Schachtdeckelüberwachung / Überwachung gegen Überflutung & Neigung .....	99
13	Der Autor .....	100
 <b>Sicherheit durch autarke IoT-Netze mit minimalen Fern-Angriffsflächen ..101</b>		
1	Das autarke IoT-Netz SAM-LAN .....	101
2	Anwendungsbeispiel: Nachrüstung eines Fernwärmenetzes .....	103
3	SAM-LAN zur Minimierung der Angriffsfläche für Fern-Angriffe .....	106
4	Schutz vor Nah-Angriffen .....	107
5	Der Einfluss minimierter Angriffsfläche .....	111
6	Fazit .....	112
 <b>Das digitale Leben – Chancen und Risiken des vernetzten Mitarbeiters ..113</b>		
1	Das Internet der Dinge als Fundament für höhere Mitarbeitersicherheit .....	114
2	Vernetzte Geräte als digitale Begleiter im privaten und beruflichen Umfeld .....	115
3	Datenerfassung und -übertragung bei Wearables .....	117
4	Höherer Mitarbeiterschutz durch intelligente Datenauswertung .....	121
5	Sicherheitslücken im Internet der Dinge .....	122
6	Technische Schwachstellen und Angriffspunkte .....	123
7	Best Practices zum Schutz vor Angriffen .....	124
8	Zusammenfassung .....	126
9	Quellen und Abbildungen .....	127

<b>Digitale Hoheit über den Maschinenpark</b>	128
1	Reichen Firewall und VPN? .....128
2	Herausforderung Sicherheitsmanagement .....129
3	Schutz auf mehreren Ebenen .....129
4	Fernzugriff externer Servicedienstleister .....130
5	Weitere Dienste .....132
6	Einsatz in der Praxis .....133
7	Checkliste .....133

<b>„Prozess-Sensoren 4.0“ – Chancen für neue Automatisierungskonzepte und neue Geschäftsmodelle in der Prozessindustrie</b>	135
1	Prozess-Sensoren 4.0 .....138
1.1	Konnektivität und Kommunikationsfähigkeit .....138
1.2	Instandhaltungs- und Betriebsfunktionen .....139
1.3	Traceability und Compliance .....140
1.4	Virtuelle Beschreibung .....140
1.5	Interaktionsfähigkeit und Bidirektionalität .....140
2	Eine „Weltsprache“ für Industrie 4.0 in der Prozessindustrie .....141
2.1	OPC Unified Architecture (OPC-UA) .....142
3	Von der heutigen Welt der Automation zum smarten Sensor .....143
4	Beispiel: Smarter Online-NMR-Sensor .....145
5	Zusammenfassung und Ausblick .....148
6	Danksagung .....149
7	Referenzen .....149

<b>Frühzeitige Prädiktion von Fehlverschraubungen mittels künstlicher Intelligenz</b>	152
1	Einleitung .....152
2	Daten .....152
3	Methodik .....153
4	Ergebnisse .....155
4.1	Technische Ergebnisse .....155
4.1.1	Klassifikatoren .....156
4.1.2	Neuronales Netzwerk .....157
4.1.3	Künstliche Intelligenz .....157
4.2	Wirtschaftliche Ergebnisse .....158
4.2.1	Fertigungskosten einer Wiederholverschraubung .....158
4.2.2	Austausch der Schraube bei Drehwinkelanzug .....159

4.2.3	Austausch von Bauteilen nach Fehlverschraubung .....	159
4.2.4	Fertigstellung an einem Standardarbeitsplatz .....	159
4.2.5	Gesamtbetrachtung .....	160
5	Ausblick .....	160
6	Quellen .....	161

**Sensordaten cloudbasiert sammeln und auswerten .....** 162

1	Einleitung .....	162
2	Fachliche Analyse .....	162
2.1	Anwendungsfall .....	163
2.2	Funktionale Anforderungen .....	165
2.3	Nichtfunktionale Anforderungen .....	166
2.4	MoSCoW-Analyse der Anforderungen .....	166
2.5	Struktur der Anwendung .....	168
3	Technische Analyse .....	168
3.1	Architektur des Systems .....	168
3.2	Datenflussmodell .....	170
3.3	Zentrales Datenmodell .....	171
4	Implementierung .....	172
4.1	Klassenmodell .....	172
4.2	Datenmodell .....	172
4.3	Umsetzung in der Cloud .....	172
4.4	Umsetzung des Power BI Webservice .....	173
5	Versuchsanwendungen .....	173
6	Schlussfolgerungen .....	174
7	Literaturverzeichnis .....	175

**Sicherung von IoT-Geräten durch kryptographisch verstärktes Port-Knocking – Ein Konzept zur langfristigen Sicherung ungewarteter Geräte in offenen Netzwerken .....** 176

1	Einführung .....	176
2	Was ist Port-Knocking? .....	177
3	Analyse der Bedrohungslage .....	178
4	Sicherheit durch Unsichtbarkeit .....	179
5	Traditionelles Port-Knocking kryptographisch verstärken .....	180
6	SYN-Knocking und TCP Stealth .....	182
7	Zusammenfassung .....	183
8	Literatur und Quellenverzeichnis .....	184

<b>Innovationen durch das Leuchtturmprojekt IC4F – Industrial Communication for Factories: Baukasten für eine vertrauenswürdige industrielle Kommunikations- und Computing-Infrastruktur als Grundlage für die Digitalisierung in der verarbeitenden Industrie</b> .....	186
1 Zusammenfassung .....	186
2 Einführung .....	187
3 Anwendungsfälle, Szenarien und Referenzarchitektur .....	188
4 Neue Technologien und Infrastruktur – Baukasten für die industrielle Kommunikation .....	190
4.1 Zugangs-Subsysteme .....	191
4.2 Kommunikations- und Computing-Infrastruktur .....	191
4.3 Anwendungs-Ebene .....	192
4.4 Sicherheit industrieller Lösungen .....	192
5 Demonstrationen und Evaluierung des Technologiebaukastens ..	193
6 Fazit .....	194
7 Danksagung .....	194
8 Referenzen .....	194
<b>Steuerung in der Cloud – Sicherheitsanforderungen und praktische Grenzen</b> .....	195
1 Einleitung .....	195
1.1 Maschinensteuerung .....	195
1.2 Betriebs- und Funktionssicherheit (Safety) .....	196
1.3 Informationssicherheit (Security) .....	197
2 Schutzziele .....	198
2.1 Verfügbarkeit .....	198
2.2 Integrität .....	199
2.3 Vertraulichkeit .....	199
2.4 Authentizität .....	199
2.5 Zurechenbarkeit und Nichtabstreitbarkeit .....	200
3 Angriffe auf industrielle Steuerungssysteme .....	200
3.1 Ausspähen von Zugangsdaten .....	200
3.2 Manipulation der Konfigurations- und Programmierwerkzeuge ..	201
3.3 Verbreitung über die Maschinensteuerung selbst .....	201
4 Spannungsfelder .....	202
4.1 Steuerung in der Cloud: Cloud versus Edge-Computing .....	202
4.2 Lebensdauer von Maschine und IT-Sicherheitsfunktionen .....	202
4.3 Firmware-Updates – Verfügbarkeit und Zertifizierung .....	203

4.4	Sicherheit – Bedienerfreundlichkeit und Kosten .....	204
5	Entwicklung sicherer Automatisierungskomponenten .....	204
6	Zusammenfassung und Fazit .....	207
7	Autorenporträt .....	208
8	Literaturverzeichnis .....	208

<b>Entwicklung komplexer, derivativer Datenparameter für die Prognose von Störungen .....</b>		<b>210</b>
1	Einleitung .....	210
2	Datenbasierte Strategie für Instandhaltung .....	211
2.1	Arten der Instandhaltung .....	211
2.2	Datenquellen .....	212
2.3	Erkennung von Störungen mithilfe derivativer Datenparameter ..	213
3	Anwendung der Prognoseberichte .....	215
3.1	Fallbeispiel: Anwendung der datenbasierten Prognosen in einem Wasserkraftwerk .....	216
4	Fazit .....	217
5	Autorenporträt .....	218

<b>Konzeption und prototypische Umsetzung einer Augmented-Reality-Lösung zur Unterstützung qualitätssichernder Maßnahmen in der industriellen Produktion .....</b>		<b>219</b>
1	Einleitung .....	219
1.1	Motivation .....	219
2	Theoretische Grundlagen zur Erweiterten Realität .....	220
2.1	Begriffsbestimmung .....	220
2.2	Historische Entwicklung .....	221
2.2.1	Ivan E. Sutherland .....	221
2.3	Architektonische Komponenten eines AR-Systems .....	223
2.3.1	Tracking .....	223
2.3.1.1	Optisches Tracking .....	223
2.3.1.2	Markerbasiertes Tracking .....	224
2.3.1.3	Merkmalbasiertes Tracking .....	225
2.3.1.4	Nicht optisches Tracking .....	226
3	Analyse und Anforderung .....	226
3.1	Ist-Analyse .....	226
3.2	Funktionale Anforderungen .....	228
3.2.1	Verwalten der Motorpräsentation .....	228

3.2.2	Pflege der Adressdaten .....	228
3.2.3	Kommunikation zur SPS .....	228
3.2.4	Wiedergabe der Motorpräsentation .....	228
3.3	Nicht funktionale Anforderungen .....	229
3.3.1	Stabilität der Anwendung .....	229
3.3.2	Zugriffszeit / Time to Content .....	229
3.3.3	Schutz der Daten .....	229
3.3.4	Bedienbarkeit .....	229
3.3.5	Nachhaltigkeit .....	229
3.4	Architektonische Konzeption .....	230
4	Prototypische Umsetzung .....	230
4.1	Phase 1 – Räumliche Entkopplung des Sichtprüfers .....	230
4.2	Erstellung einer Windows-Anwendung zur Generierung der Arbeitsanweisungen .....	231
4.3	Oberfläche zur Adressverwaltung der Stationen und Datenbrillen .	232
4.4	Anwendung auf der Datenbrille .....	232
5	Ergebnisbetrachtung .....	232
5.1	Ausblick .....	233
5.1.1	Unterstützung bei der Montage von Motorleitungssätzen .....	234
5.1.2	Finger Tracking .....	234
5.1.3	Eye-Tracking .....	234
<b>Industrie 4.0: Smarte Systeme brauchen smarte Security-Lösungen .....</b>		<b>235</b>
1	Potenziale durch Industrie 4.0 .....	235
1.1	Aktuelles Gefahrenpotenzial und NSA-Skandal .....	236
1.2	Stuxnet – was hat sich bis heute getan .....	238
1.3	Warum ist es so schwierig, ICS zu schützen? .....	240
2	Neue Herausforderungen für Security-Lösungen .....	241
2.1	Industrie 4.0 ist ohne Security nicht möglich .....	242
3	Symmetrisches Schlüsselmanagement für mehr Sicherheit .....	244
3.1	Warum symmetrische Verschlüsselungsverfahren in Zukunft sicherer sind .....	244
4	Problemlose Einbindung von Zulieferern im Ausland .....	246
5	Glossar .....	247
6	Abkürzungsverzeichnis .....	249
7	Autorenporträt .....	250
8	Quellenverzeichnis .....	250

<b>OpenIoTfog: Eine anbieterunabhängige Verwaltungsschale für Industrie-4.0-Komponenten</b>	252
1 Einleitung	252
2 Verwandte Arbeiten	254
3 Eigener Ansatz	259
4 Zusammenfassung und Ausblick	261
5 Literaturverzeichnis	261
6 Abkürzungsverzeichnis	263
7 Autoren	265
<b>Prozessindustrie 4.0 – Was bringt der digitale Zwilling?</b>	266
1 Stand der Dinge	266
2 Neue Geschäftsmodelle in anderen Branchen	267
3 Neue Geschäftsmodelle in der Prozessindustrie	269
4 Rahmenbedingungen neuer Geschäftsmodelle	271
4.1 Anlagenkomponenten werden intelligent	271
4.2 Datenanalysen zur Optimierung der Instandhaltung	271
4.3 Daten	271
4.4 Vertragswerk	272
5 Zusammenfassung und Ausblick	272
<b>Softwarequalität als grundlegende Eigenschaft für Technische Sicherheit</b>	274
1 Einführung	274
2 Sicherheit – Safety und Security	275
2.1 Sicherheit als erfolgskritischer Faktor in Zeiten des Digitalen Wandels	275
2.2 Begriff „Qualität“	277
2.3 Softwarequalität	277
2.4 Produktqualität und Prozessqualität	277
2.5 Softwarequalität ISO/IEC 9126	278
3 Komplexität von Software	278
4 Ursachen von Software-Schwachstellen	280
5 Fazit	280
6 Quellen	281