

Carsten Pinnow, Stephan Schäfer



Industrie 4.0

Safety und Security - Mit Sicherheit gut vernetzt

Branchentreff der Berliner und Brandenburger
Wissenschaft und Industrie



Beuth

**Industrie 4.0 – Safety und Security –
Mit Sicherheit gut vernetzt**

(Leerseite)



Carsten Pinnow
Stephan Schäfer

Industrie 4.0 – Safety und Security – Mit Sicherheit gut vernetzt

**Branchentreff der Berliner und Brandenburger
Wissenschaft und Industrie**

1. Auflage 2017

Herausgeber:
DIN Deutsches Institut für Normung e. V.

Beuth Verlag GmbH · Berlin · Wien · Zürich

© 2017 Beuth Verlag GmbH

Berlin · Wien · Zürich

Am DIN-Platz

Burggrafenstraße 6

10787 Berlin

Telefon: +49 30 2601-0

Telefax: +49 30 2601-1260

Internet: www.beuth.de

E-Mail: kundenservice@beuth.de

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der Grenzen des Urheberrechts ist ohne schriftliche Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung in elektronischen Systemen.

© für DIN-Normen: DIN Deutsches Institut für Normung e. V., Berlin.

Die im Werk enthaltenen Inhalte wurden vom Verfasser und Verlag sorgfältig erarbeitet und geprüft. Eine Gewährleistung für die Richtigkeit des Inhalts wird gleichwohl nicht übernommen. Der Verlag haftet nur für Schäden, die auf Vorsatz oder grobe Fahrlässigkeit seitens des Verlages zurückzuführen sind. Im Übrigen ist die Haftung ausgeschlossen.

Titelbild: © Blue Island, Benutzung unter Lizenz von shutterstock.com

Satz: Meta Systems Publishing & Printservices GmbH,
Wustermark

Druck: Colonel, Kraków

Gedruckt auf säurefreiem, alterungsbeständigem Papier nach DIN EN ISO 9706

ISBN 978-3-410-26406-4

ISBN (E-Book) 978-3-410-26407-1

Inhalt

EchoRing™ – Wireless Safety durch Massive Kooperation	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 EchoRing™ – ein auf massiver Kooperation basierendes Kabellos- system	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
Sichere Drahtlos-Handbediengeräte	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

6	Produkte	24
6.1	Wireless Handheld Safety	24
6.2	Gateway	25
6.3	EchoRing-Modul	25
7	Ausblick	26
8	Zusammenfassung	26
9	Autor	26
10	Quellen	27

Modellbasiertes Systems Engineering – methodische Unterstützung zur Entwicklung Cyber-physischer Produktionssysteme 28

1	Einleitung	28
2	Automatisierungsgerechte Produktentwicklung mittels MBSE	29
3	PLM als offene IT-Plattform	31
4	ausgewählte Umsetzungsstrategien	34
4.1	Virtuelle Inbetriebnahme smarterer Produktionssysteme	34
4.2	Factory Cloud zur Produktionsoptimierung	36
5	Zusammenfassung und Ausblick	38
6	Literatur	39

Optische Raumüberwachungssysteme in wandelbaren Umgebungen der Smart Factory 41

1	Kurzfassung	41
2	Einleitung und Motivation	42
2.1	Industrielle Praxis in der Bildverarbeitung	42
3	Standards in Bereichen der Automatisierungstechnik	46
4	Anforderungen in wandelbaren Umgebungen	47
5	Konzeptvorschlag	51
6	Zusammenfassung und Ausblick	53
7	Quellen	54

Pragmatische Cyber Security in kritischen Infrastrukturen – zwei Fallbeispiele 57

1	IT Security und Cyber Security in kritischen Infrastrukturen	57
1.1	Informations- und Datensicherheit in vernetzten Infrastrukturen ..	57
1.2	SANS Critical Security Controls	58
1.3	NIST Cybersecurity Framework	59
2	Fallbeispiel Unternehmen 1	59
2.1	Pragmatische Positionierung mit SANS	59

2.2	Security Information and Event Management (SIEM)	61
2.3	Management-Paradoxien in einer komplexen systemischen Prozesskette	63
3	Fallbeispiel Unternehmen 2	64
3.1	IT Security due Diligence mit SANS	64
3.2	IT Security als Teil der Cyber Security	65
4	Lessons Learnt	65
4.1	Systemische Sicht auf den Cyber- und Informationsraum	65
4.2	HTW Berlin Digital Value Lab	66
5	Autorenporträts	67
6	Quellen	67
Industrie 4.0: Industrielle IT-Sicherheit im Wandel		69
Wie Big-Data-Ansätze helfen, die Betriebssicherheit von Energieversor- gungsanlagen zu verbessern.		74
1	Einleitung	74
2	Künstliche Intelligenz und Mustererkennung	76
3	Redundantes System	80
4	Zusammenfassung und Ausblick	81
5	Literaturverzeichnis	82
Plattform Industrie 4.0 – Ergebnisse der Arbeitsgruppe „Sicherheit vernetzter Systeme“		84
1	Ausgangslage	84
2	Von Bits und Bytes zu Information	84
3	Vertrauenswürdigkeit	84
4	Handlungsfelder	85
4.1	Sichere Kommunikation	85
4.2	Sichere Identitäten	85
4.3	Integrität und Vertrauenswürdigkeit	85
4.4	Sicherer Betrieb	86
4.5	Aus- und Weiterbildung	86
5	Ausblick	86
6	Literaturverzeichnis	86
RFTS – Remote Fiber Test System Optisches Monitoring der physika- lischen Leitung		88
1	Einleitung	88

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
Sicherheit durch autarke IoT-Netze mit minimalen Fern-Angriffsflächen ..		101
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
Das digitale Leben – Chancen und Risiken des vernetzten Mitarbeiters ..		113
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

Digitale Hoheit über den Maschinenpark	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
„Prozess-Sensoren 4.0“ – Chancen für neue Automatisierungskonzepte und neue Geschäftsmodelle in der Prozessindustrie	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
Frühzeitige Prädiktion von Fehlverschraubungen mittels künstlicher Intelligenz	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

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	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
Steuerung in der Cloud – Sicherheitsanforderungen und praktische Grenzen	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

Entwicklung komplexer, derivativer Datenparameter für die Prognose von Störungen

	Entwicklung komplexer, derivativer Datenparameter für die Prognose von Störungen	210
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

Konzeption und prototypische Umsetzung einer Augmented-Reality-Lösung zur Unterstützung qualitätssichernder Maßnahmen in der industriellen Produktion

	Konzeption und prototypische Umsetzung einer Augmented-Reality-Lösung zur Unterstützung qualitätssichernder Maßnahmen in der industriellen Produktion	219
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
Industrie 4.0: Smarte Systeme brauchen smarte Security-Lösungen		235
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

OpenIoTfog: Eine anbieterunabhängige Verwaltungsschale für Industrie-4.0-Komponenten	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
Prozessindustrie 4.0 – Was bringt der digitale Zwilling?	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
Softwarequalität als grundlegende Eigenschaft für Technische Sicherheit ..	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

EchoRing™ – Wireless Safety durch Massive Kooperation

Christian Dombrowski und Dr. Mathias Bohge – R3 Reliable Realtime Radio Communications GmbH

Abstract

Kabellose Kommunikation ist die Basis aller IoT- (Internet-of-Things) und Industrie-4.0-Zukunftsszenarien. Die Vernetzung von vielen Milliarden Geräten durch Kabel ist nicht realisierbar. In vielen Bereichen ist heute der Verzicht auf Kabel nicht vorstellbar, da die kabellose Übertragungstechnik als grundlegend unzuverlässig wahrgenommen wird. Eine neue Generation Kabellos-Übertragungstechnik muss bezüglich Echtzeitfähigkeit und Zuverlässigkeit signifikante Verbesserungen mit sich bringen. Das EchoRing™-System ist eine neuartige Übertragungstechnik, die auf massiver Kooperation basiert. Dabei ist grundsätzlich jeder Knoten in der Lage, die Kommunikationsaufgaben benachbarter Knoten zu übernehmen. Die Zuverlässigkeit eines auf massiver Kooperation basierenden Systems steigt dadurch mit der Anzahl der im System existenten Kommunikationsknoten – im Gegensatz zu anderen Systemen, deren Zuverlässigkeit sich antiproportional zu der Anzahl kommunizierender Knoten verhält. In diesem Beitrag wird das Prinzip der massiven Kooperation vorgestellt, mit anderen Systemen verglichen, und es werden EchoRing™ Anwendungsszenarien aufgezeigt.

1 Einführung

In Fabriken spielt die Informations- und Kommunikationstechnik eine wichtige Rolle. Auch die Koordination von Fließbändern, Robotern und aktuellen Lager-systemen ist ohne netzwerkgebundenen Datenaustausch nicht denkbar. Ebenso läuft die Kommunikation unter den Mitarbeitern einer Fabrik inzwischen fast ausschließlich auf digitalem Wege. Allerdings basiert nur ein vergleichsweise geringer Anteil des Datenaustauschs in heutigen Fabrikhallen auf Basis drahtloser Kommunikationssysteme. Der Grund für die Vorherrschaft kabelgebundener Systeme liegt in deren vergleichsweise hohen Zuverlässigkeit, Ausfall- und Abhörsicherheit, sowie den geringen Verzögerungszeiten, die beim Zugriff auf das Übertragungsmedium entstehen. Insbesondere für die Steuerung und Regelung von Produktionsmitteln wie Robotern sind diese Eigenschaften unabdingbar, da verzögerte, verfälschte oder sogar fehlende Steuer- und Regelungssignale bei der Güterproduktion signifikanten Schaden anrichten können.

Im Kontext des Zukunftskonzepts Industrie 4.0 wird sich die Vernetzung unter den verschiedenen Einheiten in der Produktion signifikant erhöhen [1]. Der Grad der Vernetzung von Produktionsmitteln, -gütern, Maschinen und Mitarbeitern wird so hoch sein, dass sich eine kabelbasierte Vernetzung nicht mehr darstellen lassen wird. Gleichzeitig werden die Ansprüche an die Zuverlässigkeit der genutzten Netzwerke mindestens im gleichen Umfang bestehen bleiben. Da Standard-Kabellosysteme nicht in der Lage sind, Paketfehlerraten im Bereich von $P_{\text{Fehler}} < 10^{-6}$ in Echtzeit darzustellen, müssen auf Echtzeit und Zuverlässigkeit spezialisierte Systeme genutzt werden, die diesen Ansprüchen genügen.

R3 Communications' EchoRing™ System [2] ist eines dieser hochzuverlässigen und gleichzeitig echtzeitfähigen Kabellosysteme. Es ist das erste Kabellosystem, das auf massiver Kooperation basiert und es befindet sich derzeit in der Entwicklung zur Serienreife. In den folgenden Kapiteln werden die Herausforderungen der kabellosen Kommunikation dargestellt und das Prinzip der Kooperation näher erklärt.

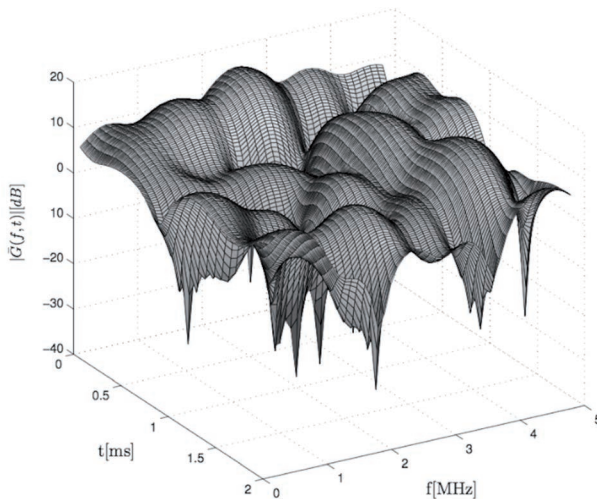


Bild 1: Zeit- (t) und Frequenz- (f) Selektivität des kabellosen Kanals an einer bestimmten Stelle im Raum

2 Kommunikation über den kabellosen Kanal

Der grundlegende Unterschied zwischen einer kabellosen und einer kabelgebundenen Datenübertragung ist die variierende Kanalqualität im kabellosen Fall. Der kabellose Kanal ist in den Dimensionen Zeit t , Frequenz f und Raum x, y, z selektiv. Das bedeutet, dass die Kanalgröße G in einem bestimmten Frequenzbereich an einem bestimmten Ort über die Zeit variiert (vgl. Bild 1). Ein Frequenzbereich, der zu einem bestimmten Zeitpunkt für eine Datenübertragung mit hohen Raten exzellent geeignet ist, kann kurze Zeit später für diese Übertragung völlig ungeeignet sein (Zeitselektivität). Ebenso kann die Kanalgröße eines zum Startzeitpunkt ungeeigneten Frequenzbereiches in diesem Moment eine wesentlich bessere Kanalgröße haben als der nun unbrauchbare erste Frequenzbereich (Frequenzselektivität). Außerdem können sich die Kanalgröße-Beobachtungen an verschiedenen Positionen im Raum signifikant voneinander unterscheiden (räumliche Selektivität). Neben den Positionen von Sender und Empfänger sind die Mehrwege-Ausbreitung des Signals und Hindernisse im Raum sowie sich im Raum bewegende Objekte für die Selektivität der Kanalgröße verantwortlich, wobei die für die Kanalgröße maßgeblich verantwortliche Signaldämpfung aus deterministischen (Pfadverlust) und zufälligen Komponenten (Shadowing, Fading) besteht [3].

2.1 Gründe für Übertragungsfehler

Eine direkte Folge hieraus ist die Tatsache, dass ein gesendetes Signal nicht zwangsläufig beim Empfänger ankommen muss. Befindet sich der Empfänger zum Übertragungszeitpunkt an einer ungünstigen Stelle im Raum, an der die Kanalgröße extrem niedrig ist (einem „Fadingloch“), ist der Empfang des Signals unmöglich. Doch selbst, wenn sich der Empfänger zum Übertragungszeitpunkt an einer besonders günstigen Position befindet, ist der korrekte Empfang des Signals nicht sichergestellt, da aufgrund der Broadcast-Natur des drahtlosen Kanals alle elektromagnetischen Schwingungen, inklusive aller Nutz- und Störsignale von der Antenne des Empfängers, als Interferenz oder Rauschen eingefangen werden und nicht ohne Weiteres vom eigentlich gewünschten Signal unterschieden werden können. Unterschreitet das Verhältnis von gewünschtem Signal und Rauschen plus Interferenz (Signal-to-Noise-plus-Interference Ratio – SNIR) einen bestimmten Wert, ist der Empfang mit anschließender Dekodierung des Signals nicht mehr möglich, was einen Übertragungsfehler zur Folge hat. In paketvermittelnden Netzwerken wird die Übertragungszuverlässigkeit darum oft in einer Paketfehlerwahrscheinlichkeit angegeben bzw. als Paketverlustrate gemessen.

2.2 Maßnahmen gegen Übertragungsfehler

Zu den wichtigsten Mitteln, um Übertragungsfehler zu vermeiden, gehören Kodierungs- und Wiederholungsmechanismen [4]. Im Falle der *Kodierung* wird die Übertragung durch zusätzliche Information (Redundanz) abgesichert. Im einfachsten Fall kann man sich vorstellen, dass jedes Bit nicht ein Mal, sondern in drei Kopien übertragen wird. Ein Bitfehler kann hierdurch durch eine einfache Mehrheitsentscheidung unter den Kopien korrigiert werden. Je nachdem, ob man die Kopien auf der gleichen Frequenz nacheinander oder über verschiedene Kanäle gleichzeitig überträgt, unterscheidet man zwischen Zeit- und Frequenzkodierung. Bei Mehrantennensystemen ist außerdem eine räumliche Kodierung möglich. Nachteilig an der Kodierung ist sowohl die Verringerung der Übertragungskapazität (bestimmt durch die Kodingrate=Nutzdaten/[Nutzdaten+Redundanzdaten]), als auch die erhöhte Komplexität, die Rechenleistung und -zeit benötigt.

Im Falle der *Wiederholung* wird ein Datenpaket so oft wiederholt gesendet, bis es fehlerfrei am Empfänger angekommen ist. Dazu ist es nötig, dass der Empfänger erstens erkennen kann, ob eine Übertragung geglückt ist, und zweitens in der Lage ist, den fehlerfreien Empfang dem Sender zu signalisieren. Hierzu sendet der Empfänger eine Empfangsbestätigung (engl. *acknowledgement* – ACK) an den Sender, indem er ihm den korrekten Empfang des Pakets bestätigt. Solche Mechanismen sind allgemein als Automatische-Wiederholungsanfrage-(engl. *automatic repeat request* – ARQ)Methoden bekannt. Üblicherweise wird die Wiederholung der Daten in der Zeitdomäne vorgenommen, d. h., die Wahrscheinlichkeit einer geglückten Wiederholung hängt davon ab, ob sich der Kanal aufgrund der Zeitselektivität in der Zeitspanne zwischen Versenden des Originalpakets und der Wiederholung in einem Maße gebessert hat. Einige Systeme nutzen außerdem die Frequenzselektivität des Kanals aus, indem sie die Wiederholung auf einer anderen Frequenz übertragen. Mehrantennensysteme können außerdem durch einen Wechsel der Antennenkonfiguration die räumliche Diversität ausnutzen. Zu den Nachteilen der ARQ-Mechanismen gehören der regelmäßige Overhead, der durch das Versenden der Bestätigungen zustande kommt, sowie der individuelle Overhead, den ggf. die Wiederholungen verursachen. Außerdem schränkt die Nutzung mehrfacher Wiederholungen die Echtzeitfähigkeit des Systems stark ein.

Die genannten Nachteile der oben beschriebenen Fehlerkorrekturmechanismen lassen den Schluss zu, dass Zuverlässigkeit und Latenzperformance eines Systems in einem antiproportionalen Verhältnis zueinander stehen. Das bedeutet, dass es relativ leicht ist, ein sehr zuverlässiges System mit großen Latenzen oder ein echtzeitfähiges System mit großer Fehleranfälligkeit zu designen, es

aber schwierig ist, die Echtzeitfähigkeit und Hochzuverlässigkeit eines Systems gleichzeitig zu optimieren. Aus diesem Grund wird derzeit mit Hochdruck an verschiedenen neuen Architektur-Prinzipien für hochzuverlässige Echtzeit-Kabellosysteme gearbeitet. Eines dieser Prinzipien ist die Kooperation zwischen Kommunikationsknoten. Sie wird im nächsten Abschnitt näher erklärt.

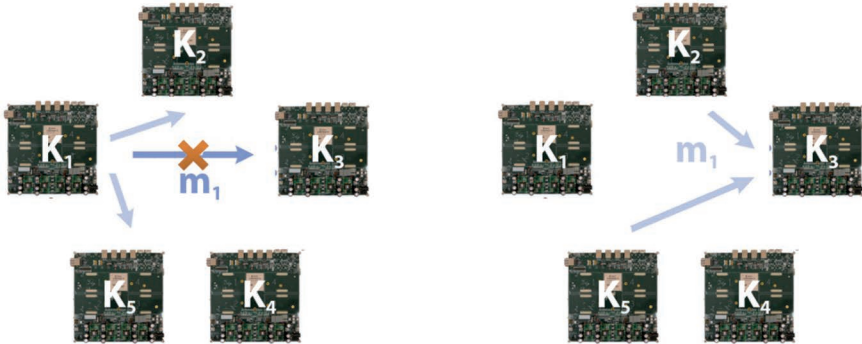


Bild 2: Prinzip der expliziten Kooperation im Fall von Relaying bei Übertragung von K_1 zu K_3

3 Kooperation verschiedener Knoten eines kabellosen Systems

Das Wort Kooperation (lat. *cooperatio*) beschreibt das zweckgerichtete Zusammenwirken von Handlungen mehrerer Einheiten, um ein gemeinsames Ziel zu erreichen. Wichtig hierbei ist die Zweckbindung, da ein zufälliges Zusammenwirken keine Kooperation, sondern eine Interaktion beschreibt.

Im Falle von Kooperation von Kommunikationsknoten eines Systems kann zwischen (1) sozialer, (2) operationaler und (3) kommunikativer Kooperation unterschieden werden [5]. Während die soziale Kooperation vor allem die individuelle Freiheit jedes Einzelnen berücksichtigt, Teil eines größeren Systems zu sein, oder sich dagegen zu entscheiden (z. B. durch Ein- und Ausschalten des Geräts ohne Rücksicht auf die Performance anderer Nutzer), beschreibt die operationale Kooperation zumeist die Ende-zu-Ende-Funktion eines Systems mit heterogenen Technologien (z. B. Anruf eines Festnetztelefons aus dem Mobilfunknetz). In unserem Fall geht es um die kommunikative Kooperation, die wiederum in (a) implizite und (b) explizite kommunikative Kooperation unter-

teilt werden kann. Bei der impliziten Kooperation wird ein Zustand von Fairness und Respekt auf passive Weise erhalten, d. h., die Methodik jedes einzelnen Nutzers basiert auf Prinzipien, die ein kooperatives/fares Verhalten implizit sicherstellen. Ein Beispiel ist das Transport Control Protocol (TCP): Jeder Nutzer evaluiert eigenständig, ob der Kanal überlastet ist, und reagiert nach einer vorgegebenen Gesetzmäßigkeit auf einen solchen Kanal durch Reduktion des eigenen Datenflusses. Im Gegensatz dazu sorgt bei der expliziten Kooperation ein gemeinsames Framework für den nötigen aktiven Datenaustausch zwischen den Knoten des Systems, sodass gemeinsam eine beste Lösung bezüglich des Kooperationsziels gefunden werden kann.

3.1 Kooperation durch Relaying

Eines der wichtigsten Kooperations-Frameworks in kabellosen Systemen ist das Relaying. Beim Relaying werden grundsätzlich Daten eines Senders, der außerhalb des Empfangsgebiets eines angestrebten Empfängers liegt, durch einen dritten Kommunikationsknoten, dem Relay, der durch seine Position dazu in der Lage ist, empfangen und an den eigentlichen Empfängerknoten weitergeleitet. Hierdurch entsteht dem Relay kein unmittelbarer Vorteil, er kann als Knoten eines explizit kooperativen Frameworks aber davon ausgehen, dass auch seine Pakete an potenzielle Empfänger weitergeleitet werden, in deren Empfangsgebieten er sich nicht befindet.

Neben dem Nutzen von Relays zur Erweiterung der Sende- und Empfangsradien in einem System, können Relays auch genutzt werden, um die Zuverlässigkeit eines Systems zu erhöhen. Nutzt man die Relays, wie in [6] beschrieben, um ARQ-Wiederholungen für den eigentlichen Sender zu übernehmen. Hierdurch wird neben der zeitlichen auch die räumliche Diversität des kabellosen Kanals ausgenutzt, um die erfolgreiche Übertragung der Daten sicherzustellen. Die grundsätzliche Funktionsweise kann gut an Bild 2 erklärt werden: Bei der Übertragung der Nachricht m_1 von K_1 zu K_3 befindet sich der kabellose Kanal zwischen den beiden Knoten in einem Zustand, der den korrekten Empfang von Nachricht m_1 nicht zulässt. Im Gegensatz dazu können aber Knoten K_2 und K_5 Nachricht m_1 fehlerfrei empfangen. Sie haben also potenziell die Möglichkeit, m_1 zu speichern und bei Bedarf weiterzuschicken. Wenn nun K_3 den Empfang von m_1 nicht bestätigt, kann die ARQ-Wiederholung je nach Bedarf und Positionierung von K_2 und/oder K_5 vorgenommen werden.

Der positive Effekt, der durch den Nutzen von Relays im ARQ-Mechanismus entsteht, ist von den Graphen in Bild 3 ablesbar: Mit jedem Knoten der als Relay-Kooperationspartner im ARQ Prozess zur Verfügung steht, sinken die Paketfehlerraten um mehrere Größenordnungen. Konkret sinkt die Wahrscheinlichkeit in einem vier

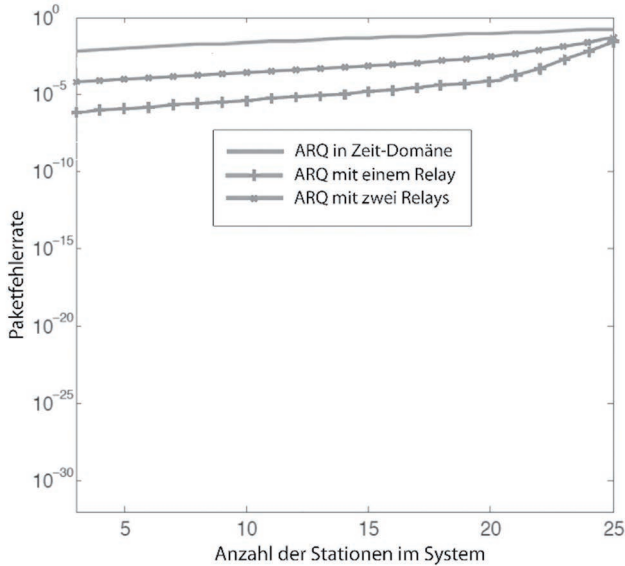


Bild 3: Der Nutzen von Relays in Automatic-Repeat-Request- (ARQ) Protokollen

Knoten umfassenden System, wenn einer der beiden nicht beteiligten Knoten als Relay fungiert von etwa $P = 10^{-2}$ auf etwa $P = 10^{-4}$. Wenn sogar beide eigentlich nicht beteiligten Knoten als Relay zur Verfügung stehen, sinkt die Wahrscheinlichkeit sogar auf etwa $P = 10^{-6}$. Durch die volle Ausnutzung der räumlichen Diversität in Kombination mit der zeitlichen Diversität im ARQ-Prozess kann das System also 10.000-fach zuverlässiger betrieben werden, als durch Nutzen der einfachen ARQ-Methodik.

Ein anderer Effekt, der in Bild 3 abgelesen werden kann, ist, dass der individuelle Übertragungserfolg mit der Anzahl von Stationen im System abnimmt. Dies liegt daran, dass die in jedem realen System zur Verfügung stehenden Ressourcen begrenzt sind. Jedem einzelnen Teilnehmer steht dadurch weniger Kapazität für seine eigene Datenübertragung zu, was unter anderem zur Folge hat, dass die Kodierate, also das Verhältnis von Nutzdaten zu Redundanzdaten kleiner werden muss (vgl. Kapitel 2.2). Somit können Fehler auf der Empfängerseite weniger gut korrigiert werden.

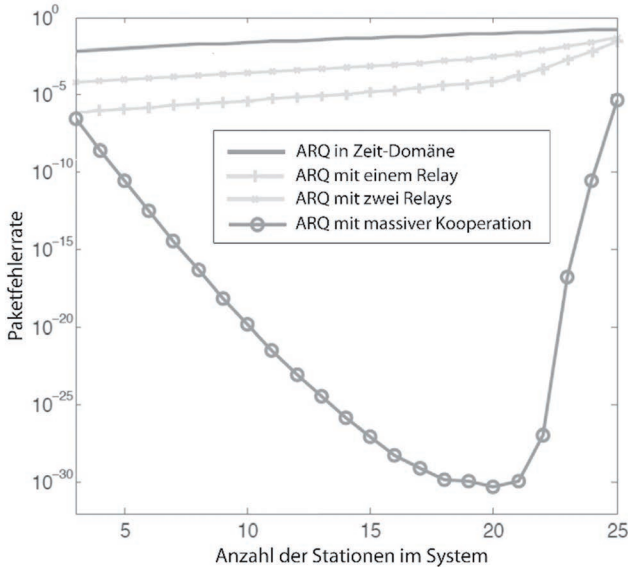


Bild 4: Der Nutzen von massiver Kooperation in ARQ-Protokollen

3.2 Massive Kooperation

Stehen nicht nur ein oder zwei, sondern alle Knoten des Systems als potenzielles ARQ Relay zur Verfügung, ist es das Prinzip der massiven Kooperation. Der positive Effekt massiver Kooperation ist in Bild 4 dargestellt: die Untersuchung des Konzepts unter Verwendung endlicher Blocklängen (engl. *finite block lengths*) aus [6] zeigt, dass der positive Effekt durch Ausnutzung der räumlichen Diversität, den negativen Effekt durch endliche Ressourcen im System bis zu einer bestimmten Anzahl an Knoten im System (in diesem Fall 20) mehr als aufwiegt. Es werden theoretische Paketfehlerraten erzielt, die in realen Systemen nicht mehr messbar sind und damit den Paketfehlerraten einer kabelgebundenen Kommunikation ähneln.

4 EchoRing™ – ein auf massiver Kooperation basierendes Kabellosssystem

Der EchoRing™-Ansatz basiert auf einem logischen Token-Ring-Verfahren [7]. Hierbei wird der Token nicht nur als Sendeerlaubnis, sondern auch als Austauschplattform für Kanalzustände genutzt. Da der Token jeden Knoten des Netzwerks durchläuft, ist es möglich, in ihm die Kanalzustände aller möglichen

Übertragungsstrecken des Systems zu transportieren. Jeder Knoten liest dazu die im Token enthaltenen Kanaldaten aus und schreibt seine aktuell gemessenen Daten vor dem Weiterversenden des Tokens hinein. Somit existiert nach einer Tokenzirkulation volle Kanalkennntnis innerhalb des gesamten Systems. Sollte der Token z. B. aufgrund von Kanalproblemen verlorengehen, sorgt eine optimierte ARQ-State-Machine für einen schnellen Ersatz.

4.1 Massive Kooperation durch instantane Relay-Wahl

Durch die verteilte vollständige Kanalkennntnis ist jeder Knoten in der Lage, die für ihn am besten situierten Systemknoten zu bestimmen, und er kann unter ihnen einen Partner für anstehende Nutzdatenübertragungen wählen. Zusätzlich zur Sender- und Empfängeradresse enthält der Header eines jedes Nutzdatenpakets die Adresse des Partnerknotens.

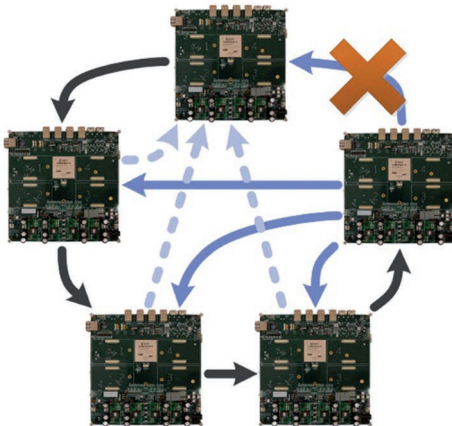


Bild 5: EchoRing™ – Kooperativer logischer Token-Ring im Broadcast-Medium

Während des Sendevorgangs versuchen nun Empfänger und Partnerknoten das Paket zu dekodieren. Der Partnerknoten wartet nach vollendeter Datenübertragung auf das Acknowledgement des adressierten Empfängers. Misslingt dem Empfänger die Dekodierung des Nutzdatenpakets und sendet er kein Acknowledgement, wiederholt der Partnerknoten das soeben vom Sender erhaltene Nutzdatenpaket, während dieser still bleibt. Bild 5 zeigt die grundsätzliche Funktionalität eines EchoRings™: Sollte ein Link nicht nutzbar werden, stehen

in dem gezeigten Szenario drei alternative Relay-Wege zur Verfügung. Aufgrund der vollständigen Kanalkennntnis an jedem Knoten des Systems kann der am besten geeignete Alternativpfad vom Sender vor der Nutzdatenübertragung bestimmt werden.

Ein weiterer Vorteil kontinuierlicher Beobachtung aller Übertragungstrecken im System ist die Tatsache, dass Kanalqualitätseinbrüche schnell erkannt und sogar prädiktiv vorausbestimmt werden.

4.2 Die Performance von EchoRing™ im Vergleich mit anderen Systemen

Heutige Standard-Drahtlossysteme sind für den Einsatz zur kritischen Kommunikation im industriellen Kontext ungeeignet. Für einige wenige spezielle Szenarien existieren proprietäre Drahtloskommunikationssysteme, die in ihren individuellen Eigenschaften den Standardsystemen überlegen sind. Zu den bekanntesten Vertretern dieser Kommunikationsnetze gehören das Siemens *Industrial Wireless Local Area Network* (IWLAN) [8] und das ABB *Wireless Sensor and Actuator* (WISA) System [9]. Dabei setzt IWLAN auf einer modifizierten Standard-WLAN-Architektur, der *industrial point coordination function* (iPCF), auf, bei der in einem *polling*-Verfahren ein zentraler Knoten (Basisstation) alle teilnehmenden Knoten nacheinander abfragt und diesen bei Bedarf Übertragungsslots zuteilt. Hierdurch können insbesondere die Verzögerung bei Zugriff auf den Kanal sowie die Handover-Performance maßgeblich gegenüber Standard-WLAN-Systemen verbessert werden. Zur Fehlerbehebung wird vornehmlich die Diversität des Kanals in der zeitlichen Domäne ausgenutzt. Das WISA-System setzt hingegen auf einem Frequenzsprungverfahren – vergleichbar mit Standard-Bluetooth-Systemen – auf. Ebenfalls wie bei Bluetooth arbeitet das System in einer Master-Slave-Architektur, in der der Master alle notwendigen Entscheidungen über die Übertragungsparameter trifft. Die Systembandbreite ist dabei auf 5 MHz Bandbreite beschränkt. Dadurch sind die erzielbaren Datenraten relativ gering.

Wiederholungen können bei WISA jedoch auf unterschiedlichen Frequenzbändern vorgenommen werden, wodurch neben der zeitlichen Diversität auch die Frequenzselektivität des kabellosen Kanals ausgenutzt werden kann. Zum Vergleich dieser beiden Systeme mit unserem EchoRing™-System wurden alle drei entsprechend den Vorgaben in [7]–[9] modelliert und analytisch untersucht.

Bild 6 zeigt die Ergebnisse des Performancevergleichs zwischen dem Downlink der zentralen/Master-Slave Architekturen von IWLAN und WISA auf der einen Seite und dem vollständig verteilten EchoRing™-Ansatz andererseits: in einem

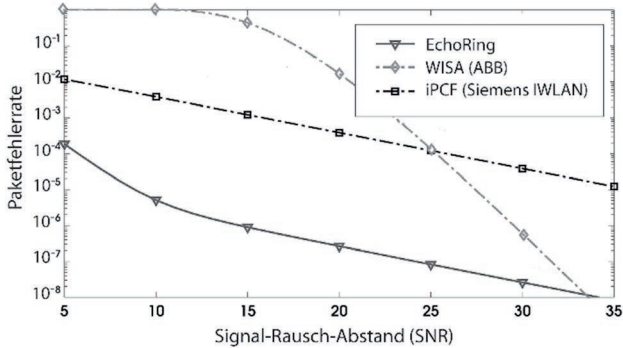


Bild 6: Paketfehlerraten von EchoRingTM im Vergleich zu dem Downlink von IWLAN- und WISA-Systemen

System mit fünf Knoten, einer maximal zugelassenen Verzögerung von 10 ms und Paketlängen von 100 Byte (EchoRingTM und IWLAN) bzw. 1 Byte (WISA) ist der Zugewinn an Zuverlässigkeit durch die Nutzung von massiver Kooperation deutlich erkennbar. Insbesondere in Szenarien mit schlechter bis mäßiger Kanalqualität ist das EchoRingTM-System deutlich überlegen. Je besser der Kanal, desto zuverlässiger werden die anderen zwei Systeme, ohne jedoch, dass das IWLAN-System die EchoRingTM-Performance erreicht. Im Gegensatz dazu steigt die Performance des WISA-Systems aufgrund der Ausnutzung der Frequenzselektivität des kabellosen Kanals bei sehr guten Kanälen in gleiche Regionen, wie das EchoRingTM-System.

5 Zusammenfassung und Ausblick

Kabellose Kommunikation ist die Basis aller IoT- und Industrie-4.0-Anwendungen. Die Vernetzung durch Kabel ist in den meisten Szenarien aufgrund unzureichender Flexibilität nicht realisierbar. Da die Fehlerperformance heutiger kabelloser Standardsysteme nicht ausreicht, müssen neuartige Kabellosysteme zum Einsatz kommen. Das EchoRingTM-System ermöglicht mit seiner auf massiver Kooperation basierenden Architektur zuverlässige kabellose Kommunikation auch bei schlechten bis mittelguten Kanalzuständen und eignet sich daher hervorragend für den Einsatz im industriellen Kontext.

Das EchoRingTM-System befindet sich derzeit in der Weiterentwicklung zur Serienreife. Der Prototyp wurde mit IEEE/VDE Awards sowie dem Deep Tech Award 2015 der Stadt Berlin ausgezeichnet. Ein erstes marktreifes Produkt wird in

Kooperation mit der Firma Scheicher Elektronik Berlin GmbH Ende dieses, Anfang des nächsten Jahres erwartet.

6 Autoren

Dipl.-Ing. Christian Dombrowski

Herr Christian Dombrowski ist Leiter der Entwicklung der R3 – Reliable Realtime Radio Communications GmbH. Nach seinem Abschluss an der TU Berlin im Bereich der Kommunikationsnetze ist er als Doktorand an das UMIC Exzellenz Cluster der RWTH Aachen gewechselt, wo er sich im Rahmen seiner Forschungstätigkeiten mit zentralisierten und dezentralisierten Ansätzen der zuverlässigen, drahtlosen Kommunikation beschäftigt hat. Einen Schwerpunkt bildet dabei sowohl die Modellgestützte als auch die experimentelle Evaluation der entwickelten Protokolle.



Dr.-Ing. Mathias Bohge

Herr Dr.-Ing. Mathias Bohge ist Geschäftsführer der R3 – Reliable Realtime Radio Communications GmbH. Seine Dissertationsschrift mit Auszeichnung hat Herr Dr. Bohge an der TU Berlin verfasst, nachdem er das Studium der Elektrotechnik in Berlin und am WinLab der Rutgers University, NJ, USA, beendet hatte. Seine professionelle Laufbahn führte ihn u. a. zu Siemens in Berlin und Ericsson in Kista, Schweden. Zuletzt arbeitete Herr Dr. Bohge als Berater für die Boston Consulting Group mit Schwerpunkt IT in Telekommunikationsunternehmen.



7 Quellen

- [1] Kagermann, H. et al (Hrsg.) 2013: Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0: Abschlussbericht des Arbeitskreises Industrie 4.0, April 2013.
- [2] Bohge, M.: Hochzuverlässige Drahtlose Kommunikation für Industrie-4.0-Anwendungen, Industrie 4.0 – Grundlagen und Anwendungen, Seiten 163–174, Beuth Verlag, 2015.
- [3] Cavers, J.: Mobile Channel Characteristics, Kluwer Academic, 2000.

- [4] Halsall, Data Communications, Computer Networks and Open Systems, 4th Edition, Addison-Wesley Publishing Company, 1995.
- [5] Fitzek, F. & Katz, M. (Hrsg.): Cooperation in Wireless Networks: Principles and Applications, Ed. Springer, ISBN 978-1-4020-4710-7, The Netherlands, 2006.
- [6] Hu, Y. et al., Finite Blocklength Performance of Multi-Terminal Wireless Industrial Networks, Cornell University Library, retrieved on April 6th, 2017, 15:25h via <https://arxiv.org/abs/1606.08646>, June 2016.
- [7] Dombrowski, C. & Gross, J.: EchoRing: A Low-Latency, Reliable Token-Passing MAC Protocol for Wireless Industrial Networks; Proceedings of the 21th European Wireless Conference (EW 2015); Seiten 1–8, Mai 2015.
- [8] Sisinni, E. et al: Simple interference detection and classification for industrial Wireless Sensor Networks, in IEEE Int'l Instrum. and Meas. Technology Conf. (I2MTC), Seiten 2106–2110, 2015.
- [9] Scheible, G. et al: Unplugged butConnected – Design and Implementation of a Truly Wireless Real-Time Sensor/Actuator Interface, IEEE Industrial Electronics Magazine, vol. 1, no. 2, Seiten 25–34, 2007.

Sichere Drahtlos-Handbediengeräte

Peter Brinkmann – Schleicher Electronic Engineering GmbH

1 Einführung

Im täglichen Leben benutzen wir selbstverständlich drahtlose Technologien für die Kommunikation. Laptops, Tablets und vor allem das Telefon/Smartphone. Den Fernseher steuern wir mit der Fernbedienung, viele Geräte lassen sich inzwischen per APP bedienen. Kaum jemand weint der Zeit hinterher, als man zu Hause das Telefonkabel hinter sich herzog und doch angebunden war. Kabelsalat, verdrehte und ab und zu auch abgerissene Kabel waren ärgerlich.

Es gibt heute in der Industrie einen Bereich, in dem Kabel nach wie vor Stand der Technik sind: Die Bedienung von Maschinen und Anlagen erfolgt häufig mit tragbaren Bediengeräten, die per Kabel an die Maschine angebunden sind. Hier findet man besonders dicke, sperrige Kabel vor, die ein mächtiges Bündel von Kupferlitzen in sich tragen. Warum ist das so? Verschläft die deutsche Vorzeigeindustrie, der Maschinen- und Anlagenbau, hier die Zeit? Denkt denn nicht auch der Maschinenbau an Usability, an Nutzerfreundlichkeit? Dabei kommt doch der Begriff HMI (Human Machine Interface) aus dem Maschinenbau. Lehrstühle und Institute setzen sich mit der Optimierung der Maschinenbedienung auseinander.

2 Das Problem

In der industriellen Automatisierung befassen sich viele Hersteller von Automatisierungsgeräten seit vielen Jahren mit drahtlosen Kommunikationstechniken. Es gibt bereits seit Langem funkbasierte Lösungen zur Übertragung von Sensordaten, zur Ansteuerung von Anlagenteilen etc. Selbstverständlich werden bei der Benutzung von Maschinen mobile drahtlose Geräte wie Tablets und Smartphones eingesetzt. Dennoch hat sich die funkbasierte Technik kaum durchsetzen können. Die von den Herstellern angepeilten Marktanteile sind weit hinter denen der kabelgebundenen Kommunikation zurückgeblieben. Dabei liegen die Vorteile der Funktechnik so nahe: mehr Flexibilität, weniger Verdrahtung mit ihren Problemen.

Das Problem der Drahtlostechnik ist die Störanfälligkeit. Knistern und Rauschen stören z. B. beim Telefonieren. Wenn die Verbindung ganz abbricht, dann ist das ärgerlich, aber man hat sich damit arrangiert. Man ruft den Kommunikationspartner noch einmal an.

In der industriellen Automation ist dies nicht akzeptabel. Maschinen sollen nahezu 100 % verfügbar sein. Ein Maschinen- oder Anlagenstillstand wegen schlechter Funkverbindung ist tabu. Maschinen stellen hohe Ansprüche an die Qualität der Signale und Daten, die zwischen Maschinenteilen kommuniziert werden müssen. So muss z. B. ein Sensorsignal (z. B. das Signal einer Lichtschranke) innerhalb einer fest definierten Zeit von der Maschinensteuerung ausgewertet werden und eine Reaktion auslösen können. Diese Zeitgarantie ist die oft genannte Echtzeit innerhalb der Maschinenprozesse. Es gibt einige Signale innerhalb von Maschinen, die darüber hinaus Sicherheitssignale sind. Beispiele hierfür: Eine Lichtschranke erkennt, wenn sich ein Mensch in den Gefahrenbereich der Maschine hineinbewegt, und sendet dieses Signal sofort an die Sicherheitssteuerung der Maschine. Ebenso: wenn ein Benutzer den Notaus-Taster betätigt, dann überträgt die Elektronik das Signal an die Sicherheitssteuerung.

Für diese Sicherheitssignale gelten sehr hohe Ansprüche an die Signalqualität, sie dürfen nicht verfälscht oder unterbrochen werden. In der Technologie der Maschinensicherheit gibt es viele Mechanismen, die Signalfehler erkennen. Die einzig zulässige Reaktion darauf ist: anhalten, abschalten. Aber so ist die gewünschte Verfügbarkeit nicht zu erreichen.

Für Sicherheitssignale werden erstens eine hohe Signalqualität und zweitens garantierte kurze Übertragungszeiten benötigt.

Brauchen wir dies auch bei mobilen Maschinenbediengeräten? Nicht immer, deshalb sind bereits Tablets im Einsatz. Aber: häufig muss der Maschinenbenutzer einige wenige Sicherheitsfunktionen einsetzen: z. B. den Notastaster.

3 EchoRing

Ein neues Verfahren der drahtlosen Übertragungstechnik ist EchoRing. EchoRing arbeitet mit der Physik von WLAN, benutzt WLAN-Komponenten und ist deshalb kostengünstig zu realisieren. EchoRing wurde von Mitarbeitern mehrerer Forschungseinrichtungen in Stockholm, Aachen und Berlin erfunden und wird derzeit mit diesem Team in dem Startup-Unternehmen R3Communication zur Produktreife weiterentwickelt.

3.1 EchoRing erfüllt die Anforderungen

EchoRing bringt genau die Eigenschaften mit sich, die für den Betrieb von sicheren Handbediengeräten notwendig sind und von Standard-Funklösungen bis jetzt nicht erfüllt werden: