Tagungsband

17. Ilmenauer TK-Manager Workshop

Technische Universität Ilmenau
29. September 2023

Herausgegeben vom
Telekommunikations-Manager (TKM) e.V.

ilmedia

2023

Impressum

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Angaben sind im Internet über http://dnb.d-nb.de abrufbar.

Redaktion

Michael Heubach
Jochen Seitz
Wolfram Rink

Technische Universität Ilmenau/Universitätsbibliothek
ilmedia
Postfach 10 05 65
98684 Ilmenau
www.tu-ilmenau.de/ilmedia

DOI: 10.22032/dbt.57781
URN: urn:nbn:de:gbv:ilm1-2023200238

Inhaltsverzeichnis

Seite

Grußwort

von Dr.-Ing. Wolfram Rink

Dr.-Ing. Wolfram Rink gehörte zu den Gründungsgremien des weiterbildenden Studienganges „Telekommunikations-Manager" und des „TKM Telekommunikations-Manager e.V.". Er ist Absolvent des TKM-Jahrgangs 1997/98, betreute den Studiengang von seinen Anfängen 1993 bis 1999 organisatorisch und war langjährig als Dozent im Studiengang tätig. Seit 2003 ist Dr. Rink erster Vorstand des „TKM Telekommunikations-Manager e.V." Dr. Rink arbeitet seit 2011 bei der DB Systel GmbH.

Sehr geehrte Gäste, liebe TKMs,

wir können uns wieder persönlich treffen, was für eine Freude!

Aber die durch die Pandemie verursachten Veränderungen in der Art unserer Zusammenarbeit bleibt nachhaltig sichtbar. So ist es inzwischen selbstverständlich geworden, bei einer Vor-Ort-Veranstaltung zusätzlich auch eine virtuelle Beteiligung zu ermöglichen. Auch wir werden es in diesem Jahr so handhaben und freuen uns sehr darauf, dadurch weiteren Gästen die Möglichkeit zur Teilnahme zu geben.

Auf unserem diesjährigen und nunmehr 17. Ilmenauer TKM-Workshop wenden wir uns wieder stärker einem übergreifenden technischen Schwerpunkt zu:

„Moderne Mobilkommunikation und Künstliche Intelligenz"

Die moderne Mobilfunkkommunikation ist für uns ein Themenschwerpunkt per se und in den letzten Jahren ist das Thema Künstliche Intelligenz (KI) immer präsenter geworden. Und das nicht nur in der Fachpresse, sondern in den letzten Monaten auch zunehmend in den öffentlichen Medien.

Denn zunehmend ist das Interesse bei Wirtschaft und Politik, aber auch beim Bürger geweckt.

Einerseits eröffnen sich da große Chancen, denn Systeme mit Funktionen generativer KI könnten nach einer Studie zur Wertschöpfung der deutschen Wirtschaft in Zukunft rund 330 Mrd. EUR beitragen (Thüringer Allgemeine v. 26.09.2023).

Andererseits ergeben sich daraus auch mögliche Gefahren, wie z.B. Identitätsdiebstahl.

Neuerdings angewandt beim Enkeltrick mit der von KI generierten vermeintlichen Stimme eines bekannten Menschen aus der Familie (Brisant, 01.06.2023).

Oder - sehr prominent- bei Christian Sievers, der als ZDF-Moderator Opfer eine KI-Fakes wurde (Berliner Morgenpost, 21.09.2023).

Heute und hier konzentrieren wir uns aber auf unseren Beitrag als Wissenschaftler und Ingenieure, um die Welt wie immer „etwas besser zu machen".

Mein besonderer Dank gilt auch in diesem Jahr wieder allen Vortragenden. Ohne Sie/Dich wäre dieser Workshop undenkbar.

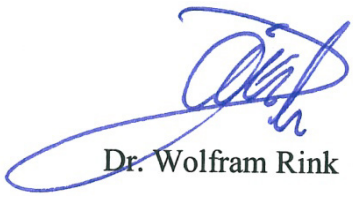
Ein ganz besonderes Dankeschön auch wieder an Michael Heubach als verantwortlichen Organisator. So manche Hürde war zu überwinden, aber Du hast das wieder hervorragend gemeistert. Danke!

Ich wünsche Ihnen/Euch und uns einen erfolgreichen Workshop und viel Erfolg!

Ihr/Euer

Dr. Wolfram Rink

1. Vorstand „TKM Telekommunikations-Manager e. V."



Going private - a closer look at 5G/6G for AI/ML in industry automation

von Florian Spinty, Adtran Networks SE

Florian Spinty studierte Elektro- und Informationstechnik mit Fokus auf eingebettete Systeme an der Hochschule Schmalkalden. Derzeit arbeitet er bei Adtran Networks SE in Meiningen in der Forschung an Themen im Bereich Softwareentwicklung für Microcontroller und FPGA. Der Forschungsschwerpunkt liegt im Bereich Physical-Layer-Technologien für optische Übertragungsnetze.

Motivation und Zielstellung

Eine Schlüsselrolle bei der Effizienzsteigerung moderner Fertigungsanlagen kommt der Digitalisierung und den dafür benötigten Kommunikations-, Sensor- und Assistenztechnolgien zu. 5G und zukünftig 6G, künstliche Intelligenz bzw. maschinelles Lernen (KI/ML), Cloud- und Edge-Computing sowie innovative Robotik erlauben es im Industrie-4.0-Kontext, eine bisher ungekannte Automatisierungstiefe in der Produktion und eine partnerschaftliche Kollaboration zwischen Menschen und Maschinen zu erreichen.

Dank hoher Bandbreiten und insbesondere deterministischer und niedriger Latenzen der neuen 5G/6G Standards ist es nicht mehr nötig, Steuerungen für Industrieanlagen lokal zu implementieren. Stattdessen können dank Cloud/Edge-Lösungen Steuerungsaufgaben auf einem zentralen Rechner oder in der Cloud zur Erhöhung der Ausfallsicherheit bündeln und Entscheidungen nicht nur auf der Basis der Informationen getroffen werden, die der einzelnen Maschine lokal zur Verfügung stehen, sondern auf der Basis eines Gesamtlagebildes. Auch kann redundante Hardware eingespart werden, was sich wiederum positiv auf Wartungs- Anschaffungs- und Betriebskosten auswirkt. Künstliche Intelligenz und Bilderkennungsalgorithmen erweitern die Fähigkeiten der menschlichen Arbeitskräfte und erkennen und verhindern Fehler frühzeitig. Künstliche Intelligenz übernimmt Aufgaben zur Optimierung und Visualisierung von Produktionsprozessen.

Die Firma Adtran baut derzeit in Meiningen eine neue Produktionsstätte und etabliert dabei ein privates 5G-Campus-Netz zur Steuerung und Automatisierung von

Produktions- und Logistikaufgaben. 5G ist dabei mehr als nur ein Standard zum Datentransfer. Es ermöglicht Tracking und Positionierung von Waren, die Steuerung und Priorisierung von Produktionsaufgaben. Gleichzeitig bildet das Kommunikationsnetz die Grundlage für die Auswertung von beispielsweise Materialfluss-Wegen und damit die Optimierung von Prozessen. Mithilfe von künstlicher Intelligenz und Bilderkennungsverfahren wird der Mitarbeiter in der Produktionsumgebung unterstützt und die Fehlerquote wird durch automatische Kontrollen in Versand und Fertigung gesenkt.

Im Vortrag wird es um die Planung und Einrichtung eines Netzes sowie die Möglichkeiten der Nutzung gehen.

„Zero Trust 2023 – Buzzword oder Mythos? Ein Realitätscheck und mögliche Migrationswege“

von Dipl.-Phys. Christoph Schmidt, Controlware GmbH

Christoph Schmidt ist seit 2005 bei der Controlware GmbH als Lead Architect Information Security tätig. Nach dem Studium der Physik an der TH Darmstadt waren weitere Stationen im Beruf die Netzwerkadministration beim Hessischen Rundfunk in Frankfurt/M., sowie div. IT Dienstleister mit dem Schwerpunkt der IT Security. Neben den klassischen Themen wie z.B. Netzwerksecurity oder auch „Network Access Control“ beschäftigt sich Christoph Schmidt hauptsächlich mit dem „Re-Design“ von Netzwerkinfrastrukturen in Bezug auf Segmentierung und DMZ/Internet/Cloud-Übergängen. Themen wie SASE oder vor allem „Zero Trust“ bestimmen hierbei die strategischen Aspekte, die moderne Architekturen nicht nur beeinflussen, sondern sogar bestimmen.

„Zero Trust 2023 – Buzzword oder Mythos? Ein Realitätscheck und mögliche Migrationswege“

In diesem Vortrag wird der Begriff „Zero Trust“ hinsichtlich Marketing-Hype und Machbarkeit gegenübergestellt.

Ist Zero Trust jetzt gerade nur irgendwie alter Wein in neuen Schläuchen oder „transformiert“ diese Methode Sicherheitsinfrastrukturen wie es seitens der Öffentlichkeit suggeriert wird?

Entstanden 2008 durch den Forrester Analysten John Kindervag beschreibt Zero Trust ein Sicherheitskonzept, das in der Informationstechnologie eingesetzt wird, um Netzwerke und Systeme vor Bedrohungen zu schützen. Im Gegensatz zu traditionellen Sicherheitsansätzen, die darauf abzielen, einen sicheren Perimeter um das Netzwerk zu errichten, geht Zero Trust von der Annahme aus, dass kein Benutzer oder keine Ressource innerhalb oder außerhalb des Netzwerks automatisch vertrauenswürdig ist.

Der Grundgedanke von Zero Trust besteht darin, dass jeder Zugriffsversuch auf Ressourcen oder Daten überprüft und autorisiert werden muss, unabhängig von der Netzwerkumgebung oder dem

Standort des Benutzers. Dies wird durch eine Kombination von Sicherheitsmechanismen wie Identitäts- und Zugriffsmanagement, mehrstufiger Authentifizierung, kontextbasierter Zugriffskontrolle, Verschlüsselung und fortgeschrittenen Bedrohungserkennungstechniken erreicht.

Fazit

Zero Trust hat sich zu einem wichtigen Konzept in der Cybersicherheit entwickelt, da traditionelle Sicherheitsansätze aufgrund der zunehmenden Komplexität und Verbreitung von Bedrohungen immer weniger effektiv werden. Unternehmen und Organisationen, die Zero Trust implementieren, können ihre Sicherheitslage verbessern und proaktiv auf potenzielle Sicherheitsverletzungen reagieren, um ihre sensiblen Daten und Systeme zu schützen

Privatsphäre-garantierendes Intrusion-Detection im Internet der Dinge

von Prof. Ralf C. Staudemeyer, Ph.D., Tobias Tefke, Hochschule Schmalkalden

Ralf C. Staudemeyer ist Professor mit Schwerpunkt IT-Sicherheit an der Fakultät für Informatik der Hochschule Schmalkalden. Seine Interessengebiete liegen in den Bereichen IT-Sicherheit und Privatheit, Rechnernetze und Künstliche Intelligenz. Herr Staudemeyer lehrte an zahlreichen akademischen Institutionen in Deutschland, Südafrika und Fidschi.

Tobias Tefke studiert seit 2018 Informatik an der Hochschule Schmalkalden. 2022 erwarb er den Bachelorgrad, seitdem studiert er im Masterprogramm „Applied Computer Science". Er interessiert sich für Softwareentwicklung sowie IT-Sicherheit und Privatheit, v.a. Im Bereich mobiler Geräte und Kleinstrechner (Internet of Things). Hier wirkte er maßgeblich an mehreren Publikationen mit.

Motivation und Zielstellung

Durch fortschreitende Digitalisierung nehmen Kleinstrechner immer weiter Einzug in unseren persönlichen Lebensbereich. Bei Anwendungsfällen im Bereich des Internet-der-Dinge (IoT), wie beispielsweise dem SmartHome, werden private Daten in hohem Maße und hoher Qualität erhoben, ausgetauscht und ausgewertet. Dies geschieht in Netzwerken, in denen Microcontroller mittels angeschlossener Sensoren Umgebungsdaten erheben und mit anderen Rechnern austauschen. Gateways sammeln diese Daten und ermöglichen es, auf Veränderungen in der Umgebung zu reagieren [3]. Dies kann beispielsweise das Einschalten eines Lichts bei der Erkennung von Bewegung sein.

Im Rahmen dieses Austausches ist sicherzustellen, dass Authentizität und Vertraulichkeit versandter Daten gewährleistet sind. Zur Abwehr entsprechender Angriffe können kryptografische Algorithmen eingesetzt werden. Gelingt einem Angreifer der Diebstahl genutzter kryptografischer Schlüssel, wird dieser Schutz jedoch nutzlos.

Intrusion-Detection-Systeme (IDS) können verwendet werden, um von Angreifern übernommene Geräte zu erkennen und aus Netzwerken auszuschließen [2, 6]. IDS können hierzu beispielsweise auf die Nutzung von Deep-Learning-Algorithmen zurückgreifen [1, 5]. Entsprechende neuronale Netze werden mit einem zuvor erstellten Datensatz darauf trainiert, Anomalien im Netzwerkverkehr zu erkennen. So ist eine Erkennung von durch Angreifer gesteuerten Geräten möglich. Sobald ein Gerät als nicht vertrauenswürdig identifiziert wird, können Administratoren gewarnt und das betroffene Gerät von der Netzwerkkommunikation ausgeschlossen werden. Allerdings muss hierbei der Schutz persönlicher Daten berücksichtigt werden. Verwendete Deep- Learning-Algorithmen müssen eine Privatsphäre-garantierende Erkennung von Anomalien ermöglichen [4].

Im Rahmen dieses Vortrags soll skizziert werden, wie ein entsprechendes System im Rahmen eines SmartHome-Anwendungsfalles aufgebaut sein könnte. In diesem Kontext wird auch darauf eingegangen, welche Deep-Learning-Algorithmen zur Erkennung von Anomalien im Netzwerkverkehr geeignet sind.

Literaturverzeichnis:

[1] Bulusu, S., Kailkhura, B., Li, B., Varshney, P. K. & Song, D. (2020). Anomalous Example Detection in Deep Learning: A Survey. *IEEE Access*, *8*, 132330–132347. https://doi.org/10.1109/access.2020.3010274

[2] Hajiheidari, S., Wakil, K., Badri, M. & Navimipour, N. J. (2019). Intrusion detection systems in the Internet of things: A comprehensive investigation. *Computer Networks*, *160*, 165–191. https://doi.org/10.1016/j.comnet.2019.05.014

[3] Li, S., Da Xu, L. & Zhao, S. (2015). The internet of things: a survey. *Information Systems Frontiers*, *17*(2), 243–259. https://doi.org/10.1007/s10796-014-9492-7

[4] Ruzafa-Alcazar, P., Fernandez-Saura, P., Marmol-Campos, E., González-Vidal, A., Ramos, J. G.

L., Bernal, J. & Skarmeta, A. F. (2021). Intrusion Detection Based on Privacy-Preserving Federated Learning for the Industrial IoT. *IEEE Transactions on Industrial Informatics*, *19*(2), 1145–1154. https://doi.org/10.1109/tii.2021.3126728

[5] Wang, S., Balarezo, J. F., Kandeepan, S., Al-Hourani, A., Gomez, K. & Rubinstein, B. I. P. (2021). Machine Learning in Network Anomaly Detection: A Survey. *IEEE Access*, *9*, 152379–152396. https://doi.org/10.1109/access.2021.3126834

[6] Zarpelo, B. B., Miani, R. S., Kawakani, C. T. & De Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications*, *84*, 25–37. https://doi.org/10.1016/j.jnca.2017.02.009

5G Sidelink für Positionsbestimmung und Verbesserung der Objektklassifikation in Fahrzeugen

von Thomas Kleinhenz, Elektrobit Automotive GmbH

Thomas Kleinhenz ist seit drei Jahren bei Elektrobit im Bereich Connect Mobility Solutions und leitet dort die Aktivitäten für System Engineering und Architektur mit etwa 40 Mitarbeitern. Ein Schwerpunkt liegt hier auf Lösungen und Anwendungen für ADAS sowie AI. Vor seiner Zeit bei Elektrobit war Thomas Kleinhenz in verschiedenen Funktionen bei der Entwicklung von 4G und 5G Systemen beteiligt und hat unter anderen für Intel und Ericsson als System Experte und Manager gearbeitet.

Motivation und Zielstellung

Eine der wichtigsten Grundlagen für das assistierte, automatisierte sowie zukünftig autonome Fahren ist die genaue Bestimmung der eigenen Fahrzeugposition sowie eine genaue Kenntnis der Positionen und Typen der anderen Verkehrsteilnehmer wie Fahrzeug, Fußgänger oder Radfahrer. Derzeit versucht man dies mit GNSS (Global Navigation Satellite Systems), einer Anbindung von Fahrzeugen an das globale Datennetz per WLAN IEEE 802.11p mit DSRC (Dynamic Short Range Communication) oder mit 4G-Mobilfunk bzw. C-V2X (Cellular Vehicle-to-Everything) zu lösen. Diese Technologien weisen jedoch Schwächen und Funktionslücken auf, die durch die nachfolgenden Generationen mobiler Netze überwunden werden sollen. So funktioniert die Lokalisierung per GNSS nur bei direkter Sichtverbindung zu den Satelliten, also z.B. nicht bei Verdeckung durch Gebäude oder in Tunneln. Einschränkungen ergeben sich auch, wenn zu viele Signalreflexionen wie in „Urban Street Canyons“ vorliegen oder die Signale gestört oder verfälscht werden (Jamming und Spoofing).

Mit 5G können erstmals zellulare Signale des Mobilfunknetzes auch zur Ortbestimmung des Fahrzeugs mit einer hohen Genauigkeit bis kleiner 1 m herangezogen werden. In den Releases 16 und 17 von 5G wurden bereits Messungen zur Ortsbestimmung auf den Up- und Downlink-Verbindungen zu den Basisstationen (z.B. DL-TDOA oder UL-TDOA auf der Uu-Schnittstelle) definiert.

Ab Release 18 sind auch genaue Device-to-Device-basierte Abstandsmessungen (V2X: Vehicle-to-Everything, z.B. Vehicle-to-Vehicle, Vehicle-to-Pedestrian) im 3GPP-Standard verankert. Die Device-To-Device-Verbindung wird als 5G-Sidelink oder als PC5-Schnittstelle bezeichnet. Damit werden Lücken im Lokalisierungskonzept für ADAS-Anwendungen / autonomes Fahren geschlossen.

Mit 5G-Advanced (ab 3GPP Release 18) werden beispielsweise hochpräzise Positionierungs- und Lokalisierungsmethoden mit dem gemeinsamen Performance Target von einer Genauigkeit bis zu 0,2 m eingeführt. Darüber hinaus unterstützt der 5G-Sidelink eine direkte Kommunikation auch ohne die Notwendigkeit der Funkabdeckung durch ein Mobilfunknetz in „Out-of-Coverage"-Szenarien. Damit werden völlig neue Anwendungsfälle und Funktionen für jede Art von Mobilität unterstützt. Im Vortrag wird ein Überblick über Möglichkeiten des 5G-Sidelinks und denkbare Lösungsansätze aus der Automotive-Perspektive gegeben.

Kommunikationsnetze und -technik an der Technischen Universität Ilmenau

von Jochen Seitz, TU Ilmenau

Prof. Dr. rer. nat. Jochen Seitz studierte Informatik an der Universität Karlsruhe (TH). Dort promovierte und habilitierte er am Institut für Telematik bei Prof. Gerhard Krüger. Nach einem Post-Doc-Aufenthalt an der Lancaster University (Großbritannien) und einer Vertretungsprofessur an der Technischen Universität Braunschweig nahm er 2001 einen Ruf auf die Professur „Kommunikationsnetze" an der Technischen Universität Ilmenau an. Dort war er als wissenschaftlicher Leiter für das Weiterbildungsstudium „Telekommunikations-Manager" verantwortlich und engagiert heute noch sich als Mitglied im „TKM Telekommunikations-Manager e.V.".

Ausgangslage

Aktuelle Schlagzeilen verkünden unisono einen kaum behebbaren Fachkräftemangel, gleichzeitig scheint das Niveau an deutschen Schulen immer mehr zu sinken und die Schüler und Schülerinnen haben offensichtlich kein Interesse mehr an einem technischen Studienfach. Ihnen wird das grundlegende Rüstzeug für ein technisches Studium nicht mehr vermittelt, weil die dazu notwendigen engagierten Lehrerinnen und Lehrer fehlen, gleichzeitig leidet auch das Berufsbild eines Ingenieurs. Die Abiturient*innen haben keine Vorstellung mehr davon, was einen Ingenieur ausmacht und welchen Aufgaben und Herausforderungen er sich stellen muss.

Kommunikationstechnik in Lehre und Forschung

Dabei ist gerade die Informationstechnik an der Technischen Universität Ilmenau sehr breit aufgestellt. In allen Fakultäten gibt es Fachgebiete, die sich mit unterschiedlichen Aspekten der Informationstechnik auseinandersetzen. Hierzu seien nur drei Beispiele genannt.

Mit den Grundlagen der **Künstlichen Intelligenz** befasst sich die Fakultät für Informatik und Automatisierung, wobei einige Fachgebiete im Thüringer Zentrum für Lernende Systeme und Robotik (https://tzlr.de) engagiert sind. Mit der Anwendung von KI-Methoden dagegen befassen sich Fachgebiete der Elektrotechnik und Informationstechnik, des Maschinenbaus und der Mathematik/Naturwissenschaften. Am

Fachgebiet Kommunikationsnetze wurde beispielsweise ein KI-basiertes Intrusion Detection System in einer Dissertation entwickelt.

Im Bereich „**Autonomes und vernetztes Fahren**“ sind ebenfalls verschiedene Fachgebiete vertreten. So sind insbesondere zwei erst kürzlich berufene Juniorprofessuren zu nennen: Prof. Dallmann für das Fachgebiet „Funktechnologien für Automatisierte und Vernetzte Fahrzeuge“ und Prof. Klingler für das Fachgebiet „Entwicklung von Systemen für das Internet-of-Things (IoT-Engineering)“. Im Thüringer Innovationszentrum Mobilität (ThIMo, https://www.mobilitaet-thueringen.de) erarbeiten die beteiligten Fachgebiete mit ihren Partnern wissenschaftlich hochwertige und zugleich innovationsrelevante Lösungen für nachhaltige Mobilitätstechnologien, wobei insbesondere informationstechnische Aspekte einen immer höheren Stellenwert einnehmen. Gerade die Vernetzung von Verkehrsteilnehmern unterschiedlicher Art ist Gegenstand der Forschung am Fachgebiet Kommunikationsnetze.

Schließlich hat die Technische Universität im letzten Jahr mit Hilfe des Thüringer Wissenschaftsministeriums im Rahmen des Programms „PROF-IT 25“ drei neue Professuren im Bereich der **Digitalisierung** eingerichtet. Dies sind die Professur „Medizinische Informatik“, die Professur „Mathematics of Data Science“ und die Professur „Digitale Werkstoffwissenschaft“. Hierbei geht es im Grunde um das Sammeln, Verdichten und Auswerten von großen Mengen digitaler Daten, was nur durch eine angepasste und optimierte Informations- und Kommunikationstechnik möglich ist. Eng damit zusammen hängt das Internet der Dinge, dessen Aspekte ebenfalls am Fachgebiet Kommunikationsnetze erforscht werden.

Schließlich rückt an der Fakultät für Elektrotechnik und Informationstechnik aktuell ein anderes Thema in den Fokus: **Quantum Engineering**. Hier steht die ingenieurwissenschaftliche Nutzbarmachung von Quanteneigenschaften im Mittelpunkt, wobei in der Kommunikationstechnik die darauf aufbauende Quantenkryptographie von großem Interesse ist. Im Master „Elektrotechnik und Informationstechnik“ der Technischen Universität können interessierte Studierende seit diesem Semester die Vertiefung „Quantum Engineering“ belegen.

Zusammenfassung

Zusammengefasst deckt die Technische Universität Ilmenau in Lehre und Forschung alle aktuell relevanten Facetten der Kommunikationsnetze und -technik ab. Interdisziplinäre Projekte und internationale Kooperationen erweitern den Blick und sensibilisieren für andere Gesichtspunkte. Jetzt müssen nur noch neue Studierende kommen und diese Gelegenheiten nutzen.

Autorenverzeichnis

Referent	Seite
Rink, Wolfram [Dr.] wolfram.rink@deutschebahn.com Operativer Chefarchitekt (IT) DB Systel GmbH Schlachthofstrasse 80 99085 Erfurt	4
Spinty , Florian FSpinty@adva.com Engineer Advanced Technology Adtran Networks SE Märzenquelle 1-3 98617 Meiningen	6
Schmidt, Christoph [Dipl.-Phys.] Christoph.Schmidt@controlware.de Controlware GmbH Waldstraße 92 63128 Dietzenbach	8
Staudemeyer, Ralf C. [Prof., PhD], Tefke, Tobias [B.Sc.] r.staudemeyer@hs-sm.de t.tefke@stud.fh-sm.de IT-Sicherheit und Betriebssysteme Hochschule Schmalkalden Blechhammer 9 98574 Schmalkalden	10
Kleinhenz, Thomas Thomas.Kleinhenz@elektrobit.com Elektrobit Automotiv GmbH Am Wolfsmantel 46 91058 Erlangen	13
Seitz, Jochen [Prof.] Jochen.Seitz@tu-ilmenau.de TU Ilmenau FG Kommunikationsnetze Helmholtzplatz 2 98693 Ilmenau	15