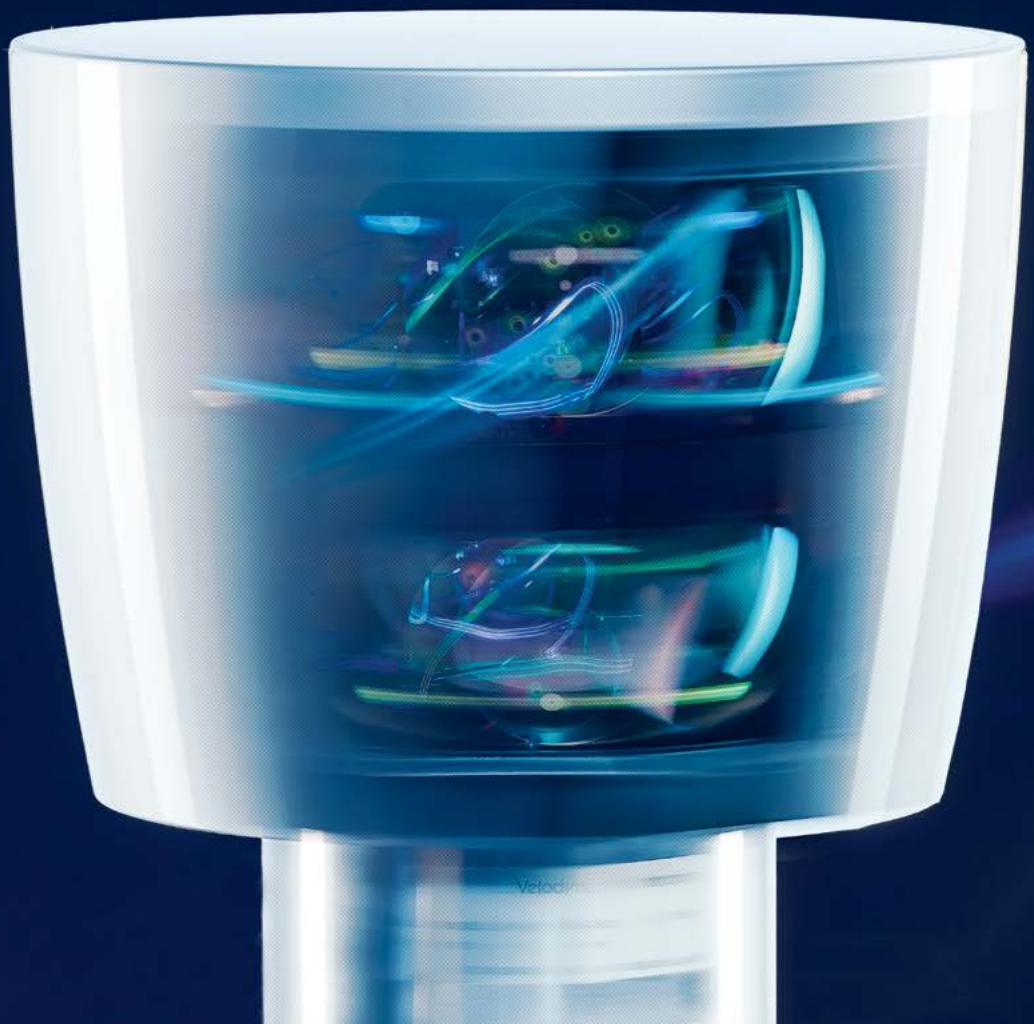
Fraunhofer
FKIE

FRAUNHOFER-INSTITUT FÜR KOMMUNIKATION, INFORMATIONSVERARBEITUNG UND ERGONOMIE FKIE

JAHRESBERICHT 2013/14



JAHRESBERICHT
2013/14

Titelbild:

3D Laserdistanzmesser

»Velodyne HDL-64E« der Firma Velodyne.

VORWORT

Liebe Leserinnen, lieber Leser,

es bedurfte nicht der Enthüllungen des Jahres 2013, um die Notwendigkeit der Forschung im Bereich Cyber Security zu erkennen. Heute wissen wir: Fast alles, was technisch möglich ist, wird tatsächlich auch zum Einsatz gebracht. Höchst professionelle Ansätze zum Ausspähen schutzbedürftiger Informationen sind Realität, in nahezu allen Lebensbereichen. Die zuverlässige Sicherung digitaler Daten ist nicht zuletzt deshalb eines der wichtigsten Themen unserer Gegenwart – ganz gleich, ob im staatlichen, industriellen oder privaten Bereich.

Im Bereich der »Cyber Security and Defense« sehen wir es als eine unserer zentralen Aufgaben an, möglichen Bedrohungen frühzeitig entgegenzuwirken, um so mehr Sicherheit zu gewährleisten. Unsere Experten forschen und entwickeln nicht erst seit den Enthüllungen von »Whistleblower« Edward Snowden im Bereich von Cybersicherheit. Ihre Arbeit ist auf der Höhe der Zeit und zukunftsweisend. Sie liefert uns bereits heute wertvolle Beiträge zur Sicherheit im virtuellen Raum. Und nicht nur dort: Auch das »Internet der Dinge« schreitet voran. IT-Sicherheit wird auch jenseits des klassischen Cyberspace eine immer wichtigere Rolle spielen. Das Thema Gebäudeautomation liefert hier ein anschauliches Beispiel. Umso mehr freuen wir uns, dass wir im letzten Jahr in diesem wichtigen Themenfeld die Vernetzung mit der Universität Bonn festigen und den Bereich der »Usable Security and Privacy« deutlich ausbauen konnten.

Es ist uns ein Anliegen, unsere Expertise auf dem Gebiet der IT-Sicherheit mit regionalen und starken Wissenschaftspartnern auszutauschen. Nicht zuletzt, um das Bewusstsein für das Thema Cybersicherheit in der Öffentlichkeit auszubauen, haben wir 2013 gemeinsam mit der Deutschen Telekom den »Bonner Dialog für Cybersicherheit« aufgenommen – inzwischen hat sich die Stadt Bonn als Mitveranstalter hinzu gesellt: Ein Gesprächsfaden, den wir so bald nicht abreißen lassen werden, denn die Veranstaltungsreihe verspricht viel spannenden Austausch zu aktuellen und brisanten Themen.

Neben unserer zivilen Forschung sehen wir uns weiterhin und zentral als zuverlässigen Partner in unserem Kerngebiet, dem wehrtechnisch ausgerichteten Aufgabenspektrum. Unsere Fachleute arbeiten hier an richtungsweisenden Projekten – allein oder im Verbund mit anderen.

Wir möchten Ihnen mit den folgenden Beiträgen unseres Jahresberichts Einblicke in ausgewählte Projekte am Institut gewähren. Sie finden einen Querschnitt durch die, wie wir ganz persönlich finden, beeindruckend vielfältigen Aktivitäten unseres Instituts, bei denen Sicherheit stets im Mittelpunkt steht. Um nur einige zu nennen: Spracherkennung im Hochfrequenzbereich, Entwicklung eines Passiv-Radars für den Gebrauch im maritimen Bereich, neue Techniken für die Mobilfunk-Ortung, spielend leicht steuerbare Roboterarme, u.v.m. Fortschritte auf diesen Gebieten können wir nur dank unserer Mitarbeiter erzielen, die uns ihren exzellenten Sachverstand auf unterschiedlichen Gebieten zugute kommen lassen. Ihrem Engagement gilt unser Dank!

Alle vorgestellten Projekte stehen überdies beispielhaft für unser FKIE-Motto, das unsere Mitarbeiterinnen und Mitarbeiter verinnerlicht haben: »Wo andere aufhören, gehen wir ein Stück weiter!«

Prof. Dr. Peter Martini
Institutsleiter

Prof. Dr. Christopher Schlick
Stellv. Institutsleiter

INHALT

KURZPORTRAIT

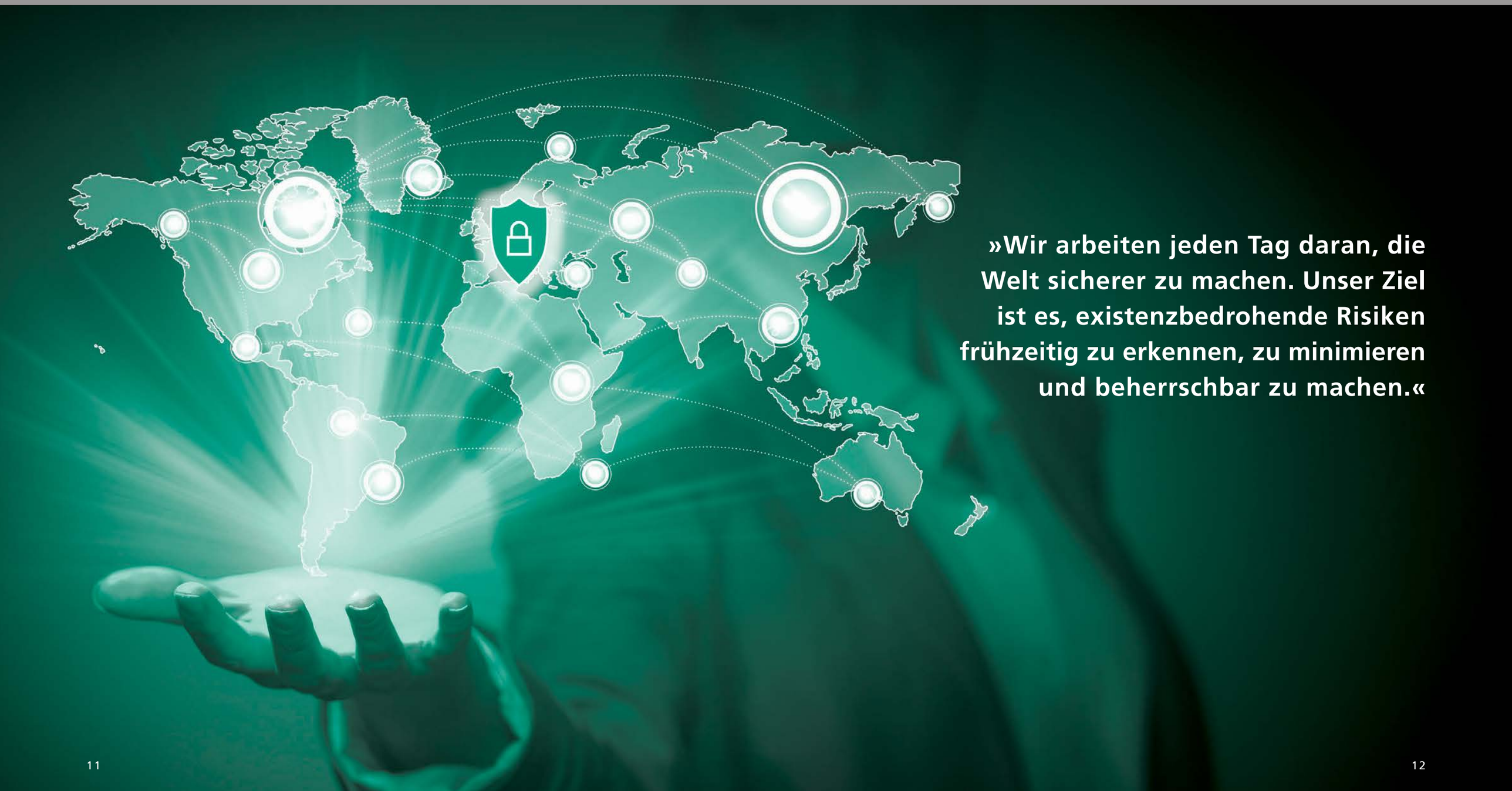
Das Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE stellt sich den aktuellen wissenschaftlich-technologischen Herausforderungen in sicherheitsbezogenen Fragestellungen im zivilen und wehrtechnischen Bereich. In der Wehrtechnik geht es in erster Linie um die Unterstützung der Bundeswehr getreu dem Motto »Vom Einsatz her denken«. Bei den zivilen Forschungsaktivitäten, mit denen das FKIE unmittelbar an seine traditionell wehrtechnisch ausgerichtete Forschung anschließt, liegt der Schwerpunkt auf Informations- und Telekommunikationstechnologie.

Die Ausrichtung des Instituts liegt auf der Forschung zur Verbesserung der Leistungsfähigkeit komplexer cyber-physischer Systeme. Dabei geht es um die Weiterentwicklung informationstechnischer Systeme hinsichtlich Datensicherheit, Interoperabilität und Vernetzung sowie um die Auswertung verfügbarer Informationen mit hoher Präzision und Zuverlässigkeit. Das FKIE arbeitet an der Unterstützung des Nutzers in allen Phasen strategischer, operativer und taktischer Führungsprozesse. Stärke unseres Instituts ist die vertiefte Auseinandersetzung mit der gesamten Komplexität der Fragestellungen, die durch das breite Spektrum wissenschaftlicher Kompetenzen möglich wird.

Die technische Umsetzung der Konzepte wird von Beginn an mitgedacht. Im Sinne anwendungsorientierter Wissenschaft werden am Institut erarbeitete Konzepte und Methoden experimentell verifiziert und mittels Prototypen evaluiert. Ein »proof of concept« gehört zum Standard. Die so gewonnenen Erkenntnisse können in enger Zusammenarbeit mit Kooperationspartnern aus Wissenschaft, Industrie und Behörden rasch zur Marktreife geführt werden: Dank der hervorragenden Vernetzung und sehr leistungsfähiger Ressourcen ist der Weg aus dem Versuchslabor zur praktischen Anwendung sehr kurz.

Das Fraunhofer FKIE betreibt Standorte in Wachtberg-Werthhoven und Bonn. Das Institut beschäftigt inzwischen mehr als 400 Mitarbeiterinnen und Mitarbeiter. Der Etat im Jahr 2013 betrug rund 28 Millionen Euro.

MISSION STATEMENT



»Wir arbeiten jeden Tag daran, die Welt sicherer zu machen. Unser Ziel ist es, existenzbedrohende Risiken frühzeitig zu erkennen, zu minimieren und beherrschbar zu machen.«

ANSPRECHPARTNER IM FRAUNHOFER FKIE

Institutsleiter
Prof. Dr. Peter Martini
Telefon 0228 9435-287
peter.martini@fkie.fraunhofer.de

Stellv. Institutsleiter
Prof. Dr. Christopher Schlick
Telefon 0228 9435-287
christopher.schlick@fkie.fraunhofer.de

Sensordaten- und Informationsfusion

Abteilungsleiter
Priv.-Doz. Dr. Wolfgang Koch
Telefon 0228 9435-373
wolfgang.koch@fkie.fraunhofer.de

- Datenfusion für Array-Sensoren
- Ortung und Navigation
- Weitbereichsüberwachung

Kommunikationssysteme

Abteilungsleiter
Dr. Markus Antweiler
Telefon 0228 9435-811
markus.antweiler@fkie.fraunhofer.de

- Aufklärung und Störung
- Software Defined Radio
- Robuste heterogene Netze

Informationstechnik für Führungssysteme

Abteilungsleiter
Dr. Michael Wunder
Telefon 0228 9435-511
michael.wunder@fkie.fraunhofer.de

- Interoperabilität verteilter Systeme
- Architekturen für Führungssysteme
- Informationsanalyse

Ergonomie und Mensch-Maschine-Systeme

Abteilungsleiter
Prof. Dr. Frank Flemisch
Telefon 0228 9435-573
frank.flemisch@fkie.fraunhofer.de

- Systemtechnik
- Human Factors

Cyber Security & Defense

Forschungsgruppenleiter
Dr. Jens Tölle
Telefon 0228 9435-513
jens.toelle@fkie.fraunhofer.de

Forschungsgruppenleiter
Prof. Dr. Michael Meier
Telefon 0228 73-54249
michael.meier@fkie.fraunhofer.de

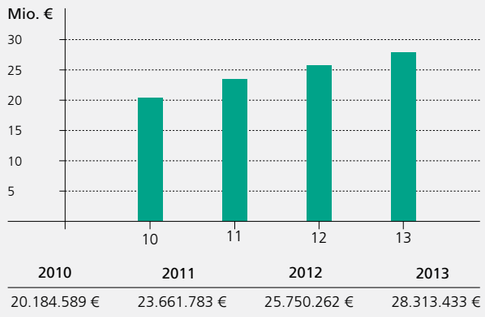
Unbemannte Systeme

Forschungsgruppenleiter
Dr. Dirk Schulz
Telefon 0228 9435-483
dirk.schulz@fkie.fraunhofer.de

ENTWICKLUNG IN ZAHLEN

Wachstum in allen Bereichen

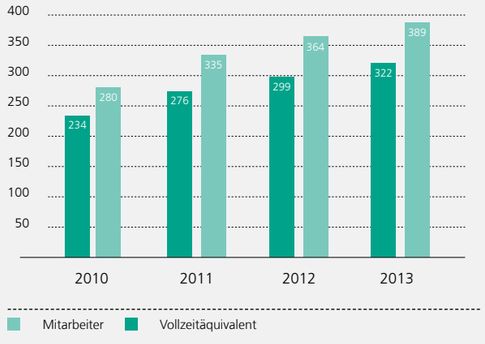
Budgetentwicklung 2010 - 2013



Das kontinuierliche Wachstum des Fraunhofer FKIE der vergangenen Jahre setzte sich auch im Jahr 2013 fort: Auf 28,3 Millionen Euro bezifferte sich das Gesamtbudget für 2013, das entspricht einer Steigerung um 10 Prozent gegenüber dem Vorjahr (2012: 25,8 Mio.).

Während die institutionelle Förderung auf ähnlichem Niveau blieb, stieg die Projektfinanzierung durch Bund und Länder an – sie machte 2013 erstmals den größten Anteil am Gesamtbudget aus. Auch die erzielten Wirtschaftserträge sind in den vergangenen Jahren deutlich gewachsen und am Jahresende von 2013 steht ein Rekordbetrag von über 37 Prozent des Budgets im zivilen Institutsteil.

Mitarbeiterentwicklung 2010 - 2013 (*)



Demgemäß ist auch die Zahl der Mitarbeiter stetig gestiegen: 389 Mitarbeiterinnen und Mitarbeiter beschäftigte das Fraunhofer FKIE Ende 2013 (2012: 364), und der Trend zur Expansion setzt sich auch im neuen Jahr deutlich fort: Im April 2014 sind es bereits mehr als 400. Damit hat sich die Zahl der Mitarbeiterinnen und Mitarbeiter seit 2005 annähernd verdoppelt.

(*) Stichtag: 01. Dezember

KURATORIUM

VORSITZENDER DES KURATORIUMS
Prof. Dr.-Ing. Gerd Ascheid
RWTH Aachen, Aachen

STELLVERTRETENDER VORSITZENDER DES KURATORIUMS
Dr. Uwe Wacker
CASSIDIAN EADS – Deutschland GmbH, Ulm

Prof. Dr. Armin B. Cremers
Rheinische Friedrich-Wilhelms-Universität Bonn, Bonn

MinDirig Dr. Dietmar Theis
BMVg – Bundesministerium der Verteidigung, Bonn

Dipl.-Ing. Thomas Dittler, MBA
Dittler & Associates International
Management Consultants GmbH, Schondorf

Dipl.-Ing. (FH) Thomas Tschersich
Deutsche Telekom AG, Bonn

Prof. Dr.-Ing. Axel Schulte
Universität der Bundeswehr München, Neubiberg

Prof. Dr. Stefan Fischer
Universität zu Lübeck, Lübeck

Prof. Dr.-Ing. Uwe Hanebeck
Karlsruher Institut für Technologie KIT, Karlsruhe

MinR Dipl.-Ing. Norbert Michael Weber
BMVg – Bundesministerium der Verteidigung, Bonn

Dr.-Ing. Hans-Joachim Kolb
MEDAV GmbH, Uttenreuth

Prof. Dr.-Ing. Klaus Wehrle
RWTH Aachen, Aachen

Dipl.-Ing. Herbert Rewitzer
ROHDE & SCHWARZ GmbH & Co. KG, München

Dr. Thomas H. G. G. Weise
Rheinmetall AG, Düsseldorf

Leitung:
Priv.-Doz. Dr. Wolfgang Koch
Telefon +49 228 9435-373
wolfgang.koch@fkie.fraunhofer.de

SENSORDATEN- UND INFORMATIONSFUSION (SDF)

Ausrichtung der Abteilung

Große Datenströme unterschiedlichster Sensoren lassen sich nicht mehr ohne Unterstützung durch den Computer auswerten. Daher befasst sich die Abteilung Sensordaten und Informationsfusion (SDF) mit der Erforschung anspruchsvoller mathematischer Algorithmen, mit denen heterogene Sensordaten und nicht-sensorielle Informationen verknüpft werden. Ziel ist es aus nackten Daten unterschiedlicher Art, Signale, nahe am physikalisch-technischen Gewinnungsprozess, lokal vorverarbeitete Messungen oder nicht-sensorielle Datenbankeinträge, semantisch gehaltvolle Informationen zu gewinnen, die Grundlage für situationsadäquate Entscheidungen sind.

Dazu werden Methoden der statistischen Signal- und Schätztheorie angewendet, um aus unscharfen Daten Zustandsschätzungen abzuleiten, Methoden der kombinatorischen Optimierung, um die anfallenden Zuordnungsprobleme zu lösen, Methoden der statistischen Entscheidungstheorie, um Anomalien zu detektieren, und schließlich Methoden des Ressourcen-Managements zur Optimierung der Freiheitsgrade von Sensorsystemen, der verwendeten Plattformen oder der Kommunikationsverbindungen.

Charakteristisch für die Forschungsarbeiten ist der Aufbau von Experimentalsystemen und Demonstratoren, durch die nach den Phasen der mathematischen Algorithmenentwicklung und ihrer Evaluation in Simulationen die Praxistauglichkeit der erforschten Ansätze nachgewiesen wird. Der so erreichte »proof of concept« schlägt die Brücke zur Realisierung, die gemeinsam mit industriellen Partnern beschritten wird.

Forschungs- / Entwicklungsbereiche

- Passive multisensorielle Aufklärung
- Sensor- und Ressourcen-Management
- Sensordatenfusion für Selbstschutzsysteme
- Multisensorielle Multi-UAS-Systeme
- Multisensorielle Weitbereichsüberwachung

Schwerpunkte / Kernkompetenzen

- Adaptive Array-Signalverarbeitung
- Steuerung multifunktionaler Sensorik
- Lokalisierung, Tracking, Klassifikation
- Fusion heterogener Sensordaten / Kontext

Projekte

- Überwachung durch Mobilfunk-Beleuchtung
- Emitter-Lokalisierung und -Tracking
- Management von Multifunktionssensorik
- Optimierung von Plattform-Trajektorien
- Stör- und täuschrobuste Navigation
- Selbstschutz fahrender / fliegender Plattformen
- Einsatz multisensorieller Multi-UAS-Systeme

NÜTZLICHER ELEKTROSMOG FÜR DEN KÜSTENSCHUTZ

Mathematikerin Dr. Martina Brötje forscht für die FKIE-Abteilung Sensordaten- und Informationsfusion (SDF) an Algorithmen für ein Passiv-Radar, mit dem Schiffe mithilfe der Abstrahlungen von Mobilfunk-Basisstationen geortet werden können. Mit ausgeklügelten Tracking-Algorithmen macht sie sich den Elektrosmog zunutze.

Immer wenn sie Mobilfunk-Basisstationen auf dem Weg zu ihrem Büro in der FKIE-Abteilung Sensordaten- und Informationsfusion (SDF) sieht, freut sich Dr. Martina Brötje. Jede einzelne Station sendet ein schwaches, aber kontinuierliches Radarsignal aus – wie eine bei Tag und Nacht leuchtende, auch Nebel und Wolken durchdringende 10-Watt-Glühbirne. Was andere für einen längeren Chat nutzen, »beleuchtet« für Brötje die Umgebung und macht Flugzeuge, Schiffe und Fahrzeuge sichtbar. Möglich macht sie dies durch pfiffige Mathematik und leistungsfähige Computer, die geduldig große Datenmengen mit hoher Geschwindigkeit verarbeiten und aus endlosen Zahlenkolonnen wertvolle Information werden lassen. Auf ihrem Bildschirm fügt sich das alles zu einem anschaulichen Lagebild zusammen.

Prinzip eines Passiv-Radars: Über einen Empfänger, links dargestellt das FKIE-Experimental System GAMMA, werden die Signale von vorhandenen Sendern, hier Mobilfunkstationen, aufgezeichnet. Neben dem direkten Signal werden dabei auch zahlreiche Reflexionen ausgewertet. Diese können zur Lokalisierung bewegter Objekte (z.B. Boote) ausgenutzt werden.

Die Bucht von Eckernförde. Beliebtes Ferienziel und Standort der Wehrtechnischen Dienststelle für Schiffe und Marinewaffen der Bundeswehr, Maritime Technologie und Forschung. 2013 wird hier mit einem am FKIE gebauten Demonstrator eine Theorie in der Praxis erprobt: Mit einer auf einer Hebebühne einige Meter in die Höhe gehobenen Empfangsantenne wird die Bewegung von Schiffen in der Bucht beobachtet, die im Dunst verschwimmen oder verschwinden. »Multistatisches Tracking« heißt das Verfahren, mit dem ermittelt wird, was vor der Küste umherschippert. Neuartig daran ist: Es handelt sich um ein Passiv-Radar, das keine eigenen Strahlen aussendet. Genutzt werden Funkwellen, die ohnehin da sind – der Elektrosmog also – und von den Schiffen zurückgeworfen werden. In diesem Fall stammen die Funkwellen von Mobilfunkmasten in Ufernähe, die an den Ufern fast aller Küsten der Welt zu finden sind. Ein entsprechendes System hat SDF in einem Demonstrator-System umgesetzt.

Der Einsatz eines Passiv-Radars in der zivilen Nutzung bietet den klaren Vorteil, dass keine zusätzliche Strahlung emittiert wird, für die überdies eine Erlaubnis vonnöten wäre. Auch im militärischen Bereich bietet diese Art maritimer Aufklärung strategische Vorteile: Das Gegenüber bemerkt keine Radarstrahlen, fühlt sich also unbeobachtet und wiegt sich in Sicherheit. Brötje: »Ein Mobilfunknetz ist an vielen Standorten ausreichend dicht, um gute Ergebnisse zu liefern.« Trotz aller ausgeklügelten Technik kommt es dennoch immer mal zu Fehlmessungen, etwa durch vom Wasser zurückgeworfene Funkwellen oder andere Störfaktoren. Die Ingenieure, Physiker und Mathematiker, die an diesem System arbeiten, nennen sie »Geister«. Aber Martina Brötje kann sie vertreiben: »Die Geisterproblematik ist eines der Hauptthemen meiner Dissertation gewesen.«

Seit einigen Jahren beschäftigt sie sich mit Tracking-Algorithmen für weitere Passiv-Radar Anwendungen, bei denen digitale Fernseh- und Radiosender zur Luftraumüberwachung genutzt werden. In diesem Projekt arbeitet sie mit dem Fraunhofer FHR zusammen, das sich um die Sensorkonfiguration und Signalverarbeitung kümmert.

Martina Brötjes Aufgabe ist es jeweils, an den Tracking-Algorithmen zu schrauben. Das Ziel: Die Fehlerquote – und damit das Auftauchen von Geistern – bei dem hier angewendeten Multi-Hypothesen-Tracking möglichst niedrig zu halten. Das ist keine leichte Aufgabe, besonders dann nicht, wenn viel los ist, zum Beispiel auf See. Brötje: »Es wird beliebig kompliziert, je mehr Schiffe in dem Bereich herumfahren.« Große Schiffe können in einem Radius von bis zu 40 Kilometern erfasst werden, kleinere Schnellboote immerhin noch auf eine Distanz von bis zu sechs Kilometern, das zeigte der Test in der Bucht. Und das ganze mit einer Genauigkeit von rund 50 bis 400 Metern. Die Qualität der Ergebnisse hänge immer auch entscheidend vom Standort der Sendemasten ab, erklärt Brötje: »Wir müssen damit eine gute Geometrie erreichen.«

Das Radar-Projekt, an dem neben Brötje noch fünf weitere Kollegen arbeiten, hat noch ein Schwesterprojekt, das sie derzeit zusammen mit einem Doktoranden bearbeitet: Es geht dabei um die Entwicklung von Tracking-Algorithmen für Sonar zur Aufklärung unter Wasser. Hier sind Fischschwärme, Felsen, Wracks und die Eigenarten des Wassers potenzielle Kandidaten, um »Geistererscheinungen« und damit Falschalarme auszulösen. Auch die Unter-Wasser-Geister wird Brötje vertreiben.

SENSORDATEN- UND INFORMATIONSFUSION

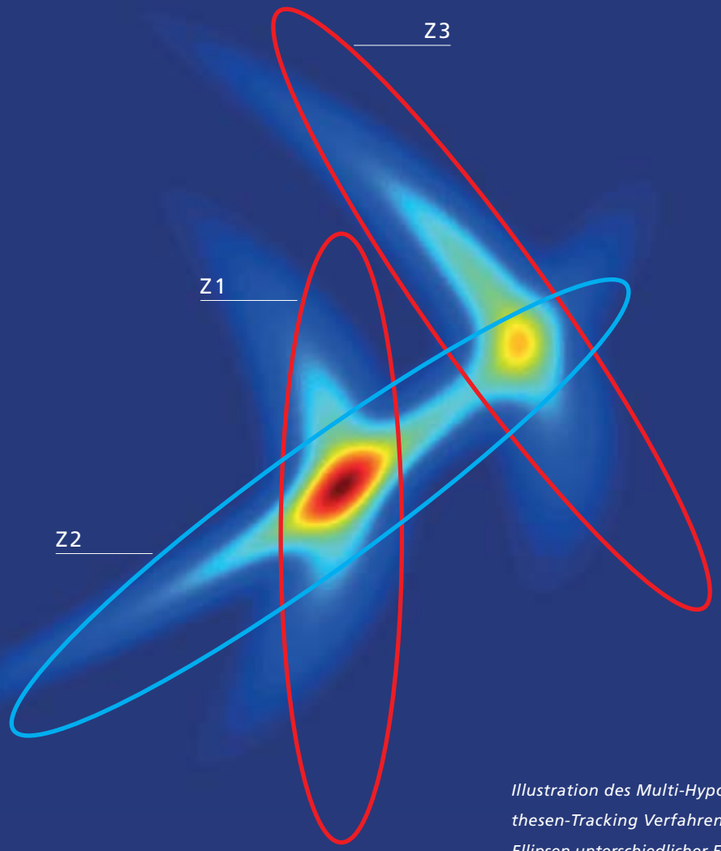


Illustration des Multi-Hypothesen-Tracking Verfahrens: Ellipsen unterschiedlicher Farbe repräsentieren die Beiträge der verschiedenen Beleuchter. Die Schnittbereiche markieren die Bereiche hoher Wahrscheinlichkeit und damit die Position der potenziellen Ziele.

MEHRWEGE FÜR EINE GENAUE LOKALISIERUNG NUTZEN

Handy-Ortung ist ein effektives Mittel – sei es, um Kriminelle zu ermitteln oder hilflose Personen zu finden. Ist ein Handy aber nicht via GPS zu orten, sondern nur via Funknetz, ist die Lokalisierung schwierig. In einem Projekt entwickelt ein Team der Abteilung Sensordaten- und Informationsfusion (SDF) ein völlig neues Verfahren zur Lokalisierung von Emittern auch in der Stadt.

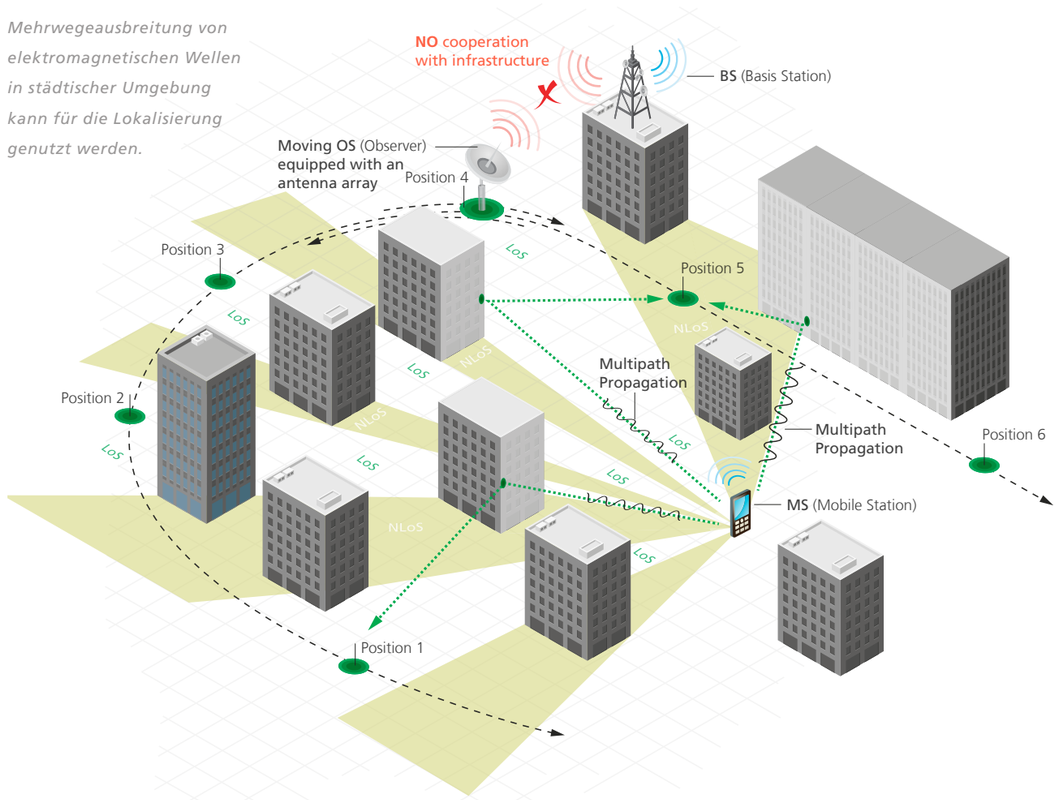
Gute Gründe vorlegen muss die Polizei, möchte sie mit richterlicher Erlaubnis ein Handy orten. Aber auch mit der Erlaubnis in der Tasche ist es dann oft immer noch kein Kinderspiel, das gesuchte Handy nebst Besitzer zu lokalisieren. Zumal dann nicht, wenn sich das Handy nicht »freiwillig« via GPS metergenau orten lässt. Und Kriminelle oder solche, die Böses im Schilde führen, werden sich dazu kaum überreden lassen, ebenso sind hilflose Personen, die vermisst werden, in der Regel nicht mehr dazu aufzufordern, ihr Handy entsprechend zu aktivieren. Die Lokalisierung eines Handys oder eines anderen Senders gestaltet sich also in all jenen Fällen schwierig, in denen der Besitzer nicht kooperiert. Und das gilt, wenn die Polizei im Spiel ist, in den allermeisten Fällen.

Ein dichtes Funknetz, viele Handynutzer, Funkwellen, die von Häuserwänden und Metallen reflektiert oder abgeschattet werden – ein gewöhnlicher Funkpeilsender muss auf der Suche nach einem Handy in der Stadt zwangsläufig in die Knie gehen. Mathematiker Dr. Felix Govaers aus der Abteilung Sensordaten- und Informationsfusion (SDF) beschäftigt sich mit diesem Problem: »Auf dem Land funktioniert ein Peilsender gut, aber innerstädtisch ist das ein Problem, wenn die Funkwellen von Gebäuden reflektiert oder gebeugt werden.« Durch diese Reflexionen entstehen sogenannte Mehrwege. Die erschweren die einfache Peilung, können aber durchaus zur Lokalisierung genutzt werden – vorausgesetzt, der Empfänger ist in der Lage, die Reflexionen voneinander zu unterscheiden.

Mit dem Projekt, an dem neben dem Team der Abteilung Sensordaten- und Informationsfusion (SDF) am Fraunhofer FKIE vier weitere Partner beteiligt sind, soll für einen Demonstrator eine von MEDAV entwickelte Antenne mit funktionsfähiger Software gekoppelt werden, die dazu in der Lage ist und die Handys oder andere Sender auch unter den besonderen Bedingungen in einer Stadt lokalisieren kann. Im April 2014 forscht das Team seit zwei Jahren an dem Versuch, von der Theorie den Weg in die Praxis zu finden: Eine an der TU Ilmenau eingereichte Dissertation hat nämlich bereits gezeigt, dass das Prinzip in der Theorie funktioniert. Govaers zeigt sich von der Idee angetan: »Die Umsetzung hat einen großen Innovationswert, es handelt sich um ein völlig neues Verfahren, um die Mehrwege-Ausbreitung zu nutzen.« Ein Algorithmus vergleicht hierfür Antennenmessungen mit den Vorhersagen einer Simulation für elektromagnetische Wellen der Firma AWE Communications.

Die Fachleute vom FKIE besorgen die Sensordatenfusion, die bei dem Projekt eine wichtige Rolle spielt: Denn bewegen sich entweder der Beobachter oder das zu beobachtende Ziel (oder beide), fällt eine Vielfalt von Daten an, die so kombiniert, statistisch bewertet und verdichtet werden muss, dass schließlich ein brauchbares Ergebnis dabei herauskommt. Dazu entwickelt das Team neue Tracking-Algorithmen, mit denen die Zielbewegung erfasst werden kann und die in die neue Antenne implementiert werden. Die Adaption und Entwicklung von Algorithmen ist die neue Herausforderung, der sich die Forscher stellen. Am Fraunhofer FKIE fließt das Know-how von Mathematikern, Informatikern, Elektrotechnikern und Physikern zusammen – Christoph Degen ist für das Implementieren der Daten zuständig. Govaers schätzt diese Vielfalt an Expertise: »Man muss die Physik verstehen, möchte man die mathematisch gewonnen Erkenntnisse effizient implementieren.«

Mehrwegeausbreitung von elektromagnetischen Wellen in städtischer Umgebung kann für die Lokalisierung genutzt werden.



Anwendungsbeispiele für eine solche Antenne finden sich im militärischen Bereich, aber auch in der Verbrechensbekämpfung, für Anti-Terrormaßnahmen oder in Notfall- bzw. Ausnahmesituationen. Auch die Bundesnetzagentur ist interessiert daran, mögliche Störsender rasch ausfindig machen zu können. In 2014 gilt es, mit dem Demonstrator möglichst viele Daten zu sammeln und damit Erfahrungen zu machen. In Bezug auf die Genauigkeit ist Govaers nach verschiedenen Versuchen vorsichtig optimistisch: »Es wäre sinnlos, wenn wir hinterher eine Genauigkeit von nur unter 100 Metern erreichen. Wenn wir eine Genauigkeit von unter 20 Metern schaffen, sind wir zufrieden!«

In dem Projekt stecken »jede Menge spannende theoretische Fragen«, die bei Govaers offenkundig Pioniergeist wecken: »Die zu lösen erfordert Kreativität von allen Teilnehmern.« Und das sei noch nicht alles, ergänzt er: Das ganze Vorhaben wirke zwar zunächst sehr theoretisch, »aber hinterher ein Produkt, eine Antenne, die man anfassen kann, vor sich zu haben – das treibt einen schon an!« Der Schritt von der Theorie in die Praxis gehört also zum motivierenden Bestandteil bei diesem Projekt mit Innovationscharakter, gleichwohl stecke hier »der Teufel sprichwörtlich im Detail.« Es sei ein wenig wie Kreuzworträtseln: »Man muss ein wenig knobeln, aber es gibt ein befriedigendes Gefühl, wenn man die Lösung gefunden hat.«

Leitung:
Dr. Markus Antweiler
Telefon +49 228 9435-811
markus.antweiler@fkie.fraunhofer.de

KOMMUNIKATIONSSYSTEME (KOM)

Ausrichtung der Abteilung

Unser Leitbild ist die Erforschung und Entwicklung innovativer Lösungen für Kommunikationssysteme und Kommunikationsaufklärung in den Bereichen Verteidigung und Sicherheit. Aus einem profunden Verständnis der Anforderungen realer Einsatzszenarien entstehen Konzepte, Methoden und Prototypen, die wir zusammen mit einem Netzwerk nationaler und internationaler Partner bis zu praxisgerechten Lösungen umsetzen. In unseren Forschungsfeldern Aufklärung und Störung, Robuste heterogene Netze sowie Software Defined Radio unterstützen wir die Bundeswehr und Behörden für die zivile Sicherheit bei der Wahrnehmung hoheitlicher Aufgaben.

Unsere Expertise erlaubt es, Kommunikationssysteme bezüglich Sicherheit, Zuverlässigkeit und Mobilität über alle Schichten der Netzwerkprotokollarchitektur hinweg zu untersuchen. Diese ermöglicht den Entwurf rasch einsetzbarer Kommunikations- und Aufklärungssysteme, die zu einer informationstechnischen Überlegenheit und zu gesteigerten Fähigkeiten führen.

Forschungs- / Entwicklungsbereiche

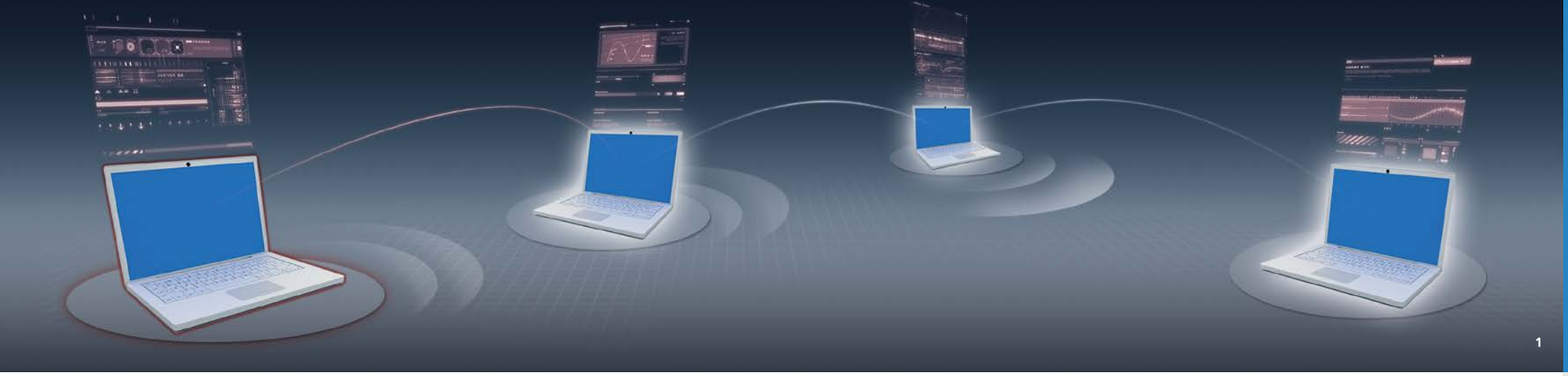
- Aufklärung und Störung
- Robuste heterogene Netze
- Software Defined Radio

Schwerpunkte / Kernkompetenzen

- Breitbandige Signalerfassung und hochauflösende Peilverfahren
- Effiziente Algorithmen zur Funksignaldetektion und -klassifikation
- Erschließung von Sprach- und Audiosignalen
- Störfestigkeit von Funkkommunikation
- Quality of Service, Routing und Sicherheit für heterogene Netze
- Sensor- und Effektornetze
- Mobile Adhoc- und Mesh-Netze, auch akustische
- Entwurfsmethodik und Wellenformen für SDR
- Dynamischer Spektrumszugriff mit kognitiven Radios
- Systemintegration von taktischen Datenlinks
- Erstellung von Funktionsmustern und praktische Validierung
- Internationale Gremien- und Standardisierungsarbeiten

Projekte

- Verdeckte akustische Kommunikationsnetze
- Robuste Sprachdetektion für komplexe Signalszenarien
- Optimierung des LINK-22 Network Managements



HORCH, WAS KOMMT VON DRINNEN RAUS?

Während rund um die Welt die Sicherheit von Daten diskutiert wird, macht diese Entdeckung Schlagzeilen: Computer können abgehorcht werden. Die Informatiker Michael Hanspach und Michael Goetz vom Fraunhofer FKIE beweisen, wie selbst aufwändig geschützte Geräte über einen verdeckten Kanal, an den bisher noch niemand dachte, ausspioniert werden können.

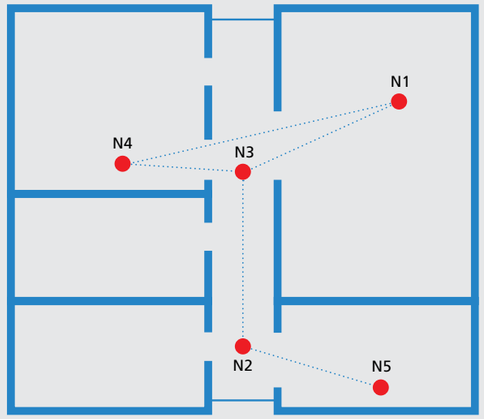
Still! Auf den Schwellen Ihres Computers, jenseits vertrauter Schnittstellen, lispeln still Ihre vertraulichsten Geheimnisse! Mögen Sie nicht glauben? Das könnte ein Fehler sein. Ihr Computer könnte gerade jetzt damit beschäftigt sein, Ihre Geheimnisse im Ultraschallbereich sprichwörtlich auszuplaudern. Den beeindruckenden Beweis führten die Informatiker Michael Hanspach und Michael Goetz aus der FKIE-Abteilung Kommunikationssysteme (KOM). Mit der Veröffentlichung ihres ungewöhnlichen Experiments im »Journal of Communications« im November 2013 sorgten die beiden Forscher weltweit für Aufsehen: Computer, die nicht auf herkömmliche Weise miteinander verbunden waren, tauschten in einem für Menschen nicht hörbaren akustischen Mesh-Netzwerk Daten aus. Mit ihren standardmäßig eingebauten Lautsprechern und Mikrofonen konnten die Computer auf eine Reichweite von bis zu 20 Metern miteinander kommunizieren. Auf diese Weise, erläutert Hanspach, sei es möglich, Daten auch bis ins Internet zu verbreiten. Hanspach: »Das funktioniert alles über Software und nutzt nur die internen Lautsprecher.« Während alle Welt über Datensicherheit debattiert, zeigen die beiden FKIE-Informatiker, wie Daten geradezu spielerisch an sämtlichen herkömmlichen Sicherungssystemen vorbei abgehorcht werden können. »Multi-Hop-Audio Kommunikation« nennen die Wissenschaftler die »Methode«.

Universell einsetzbar seien solche Methoden nicht, aber selbst ein so besonders geschütztes Gerät wie das Kanzlerinnen-Handy wäre auf ähnliche Weise prinzipiell angreifbar, erläutert Hanspach: Über einen so genannten »verdeckten Kanal« können auch Informationen aus einem speziell geschützten Bereich auf einen ungeschützten Bereich des selben Geräts übermittelt werden. Grundlagen bezüglich dieser Art von verdeckten Kanälen hat Hanspach bereits gemeinsam mit dem Betreuer seines Promotionsprojekts, Prof. Dr. Jörg Keller von der FernUniversität Hagen, in internationalem Rahmen vorgestellt. Durch weiterführende Versuche konnte gezeigt werden, dass selbst streng isolierte Bereiche eines Computersystems auf diesem Weg miteinander verbunden werden können. »Der Computer spricht im Prinzip mit sich selbst«, erläutert Hanspach.

»Man muss sich in den Angreifer hineindenken!«

Allein: Warum denken sich Wissenschaftler so etwas aus? Die Antwort ist ganz einfach, erklärt Hanspach: »Man muss sich in den Angreifer hineindenken!« Nur so könne man dem Gegenüber stets einen Schritt voraus sein. Will man sich vor Cyber-Terroristen schützen, müsse man deren Methoden kennen, und dort werde gewiss ein großer Aufwand betrieben: »Wir müssen wissen, was überhaupt möglich ist«, befindet Hanspach.

Horch! Der Akkord der Daten lischt, denn selbstverständlich haben die Wissenschaftler bereits das Gegenmittel zur Hand: »Wir haben am Institut bereits ein Intrusion-Detection-System, das sich für die Analyse von Schallwellen nutzen lässt.« Man entwickele zu diesem Zweck Signaturen wie bei einem Virenscanner. »Wir können das zur Marktreife bringen«, blickt Hanspach in die Zukunft: »Hochsicherheitsbereiche wird man zukünftig vielleicht auch mit einem speziellen Suchgerät in Verbindung mit einem Mikrofon auf die Anwesenheit dieser verdeckten Netzwerke prüfen.« Die Gefahr, die von einem Audio-Botnetz ausginge, wäre immens: »Die meisten Menschen glauben gar nicht, was alles möglich ist«, weiß Hanspach. Daher gelte es, neue Angriffsmethoden zu erforschen und aufzuzeigen. Das ist ihm und Goetz auf bemerkenswerte Weise gelungen. Mit verdeckten Kanälen wird Hanspach sich auch weiterhin beschäftigen. Schall betrachtet er jedoch nur als ein Beispiel für die Gefahren, die von verdeckten Kommunikationstechnologien ausgehen. Ihn reizen auch andere verdeckte Kanäle, mit denen er sich zukünftig beschäftigen möchte: »In Protokollen, in Algorithmen und auch in anderen physikalischen Bereichen.«



2

1 *Vom Netzwerk getrennte Computer etablieren ein verdecktes Mesh-Netzwerk, bei dem Daten über Ultraschall miteinander ausgetauscht werden.*

2 *Mittels Multi-Hop-Kommunikation können Angreifer ganze Gebäude unerkannt miteinander vernetzen.*

Die Vernetzung der Teilstreitkräfte der NATO mit Hilfe des taktischen Datenlinksystems Link-22.

GUTES MANAGEMENT FÜR EIN KOMPLEXES KOMMUNIKATIONSSYSTEM

Mit Hilfe des taktischen Datenlinksystems »Link-22« tauschen Schiffe, Flugzeuge und Landfahrzeuge mehrerer NATO-Partner ihre einsatzbezogenen Daten über Funk aus. Link-22 ist das Nachfolgesystem zu Link-11 und wird derzeit überwiegend von Marinekräften genutzt. Die Entwicklung begann in den 1990er Jahren, seit 2013 sind die Fachleute vom Fraunhofer FKIE mit der Optimierung des Netzwerkmanagements befasst.

Ein funktionierender Datenaustausch zwischen verschiedenen Verteidigungskräften mehrerer Nationen ist insbesondere bei gemeinsamen Einsätzen unverzichtbar. Um den Austausch von taktischen Einsatzdaten möglichst komplikationsfrei zu gewährleisten, begann die NATO bereits Mitte der 1950er Jahre, den Link-11-Standard zu entwickeln: ein taktisches Datenlinksystem, über das Marine- und Lufteinheiten verschiedener Nationen miteinander automatisiert Daten austauschen können. Mit der Entwicklung von Link-16 seit Mitte der 1970er Jahre und mit Link-22 seit den 1990er Jahren werden bis heute die taktischen Datenlinksysteme stetig verbessert. Die Entwicklung von Link-22 war bereits Ende der 1980er Jahre gemeinsam von Deutschland, Frankreich, Großbritannien, Italien, Kanada, den Niederlanden und den USA initiiert worden. Im Kreis der offiziell an der Systementwicklung und deren Finanzierung teilnehmenden Nationen hat Spanien die Niederlande inzwischen abgelöst. An der Entwicklung sind eine Reihe von Industriefirmen und Institutionen beteiligt. Derzeit befindet sich Link-22 in der »In-Service-Support«-Phase, seit Mai 2013 sind auch Experten der Abteilung Kommunikationssysteme (KOM) in der Weiterentwicklung des Netzwerkmanagements involviert.

Übung auf der Nordsee. Mehrere Fregatten und Jets im Manöver. Der Operator auf der Brücke der neuesten Bundeswehr-Fregatte hat auf seinem Bildschirm alle detaillierten Lagedaten im Blick, im unteren Bildschirm-Fenster technische Netzwerk-Details, im oberen Bildschirm-Fenster die taktischen Nachrichten. Dank Link-22 mit seinem Mensch-Maschine-Interface erhält er einen Überblick über die Gesamtlage, die Positionen der Schiffe sowie den Status von wichtigen Subsystemen und kann vordefinierte Informationen mit einem Knopfdruck automatisiert an die anderen Beteiligten weiterleiten. Über 1500 sowohl taktische, als auch netzwerkrelevante Meldungen können mit Link-22 übermittelt werden. Bei ungünstigen oder gestörten Funkübertragungen kann der Operator den Wechsel von Übertragungsparametern initiieren, so dass der Datenaustausch weiterhin möglich ist. Durch all die angezeigten Informationen und die daraus resultierenden Aufgaben ist der Operator hoch belastet. Mithilfe eines optimierten Netzwerkmanagements soll er entlastet werden, so dass er sich noch mehr auf seine taktisch-operationellen Aufgaben konzentrieren kann. Hierzu tragen die FKIE-Experten bei.

FKIE bringt sein Know-how projektbegleitend ein

Die an diesem Projekt beteiligen FKIE-Experten helfen mit, das Link-22-Netzwerkmanagement zu optimieren. Zum Team gehören Dr. Marc Adrat als Gesamtverantwortlicher, Dr. Ferdinand Liedtke und Marco Sieberath. »Wir bringen unser Know-how in das Projekt mit ein und bieten technisch-wissenschaftliche Beratung«, erläutert Liedtke die projektbegleitenden Aufgaben des FKIE-Teams. Liedtke weiter: »Zur Mitarbeit gehört es, das System zu verstehen und die als notwendig erkannten Anpassungen und Ergänzungen zu konzipieren und einzubringen.« Ziel des derzeitigen Arbeitsabschnittes ist die Mitwirkung bei internationalen Tests und Demonstrationen sowie der Aufbau und die Nutzung eines Demonstrationsgerätes, mit dem wichtige Module des Datenlinksystems bearbeitet und verifiziert werden sollen.

Link-22 arbeitet in verschiedenen Frequenzbereichen und nutzt dabei ein Time-Division-Multiple-Access-Zugriffsverfahren. Bei diesem Verfahren werden den verbundenen Netzwerkknoten systematisch Zeitschlitze für einen kollisionsfreien Datenaustausch zugeteilt. Treten bei der Datenübertragung Probleme durch Störungen auf den Übertragungskanälen auf, so können diese durch Zuteilung und Nutzung von weniger gestörten Frequenzkanälen umgangen werden. Speziell in Bezug auf Signalverarbeitung und -analyse können die FKIE-Experten ihr Know-how einsetzen. Marco Sieberath beschäftigt sich mit der Frage, wo in dem System das größte Optimierungspotenzial stecken könnte. »Das steckt ganz eindeutig in der auswertenden Signalvorverarbeitung für die Bildschirm-Darstellung«, erklärt er, »dort, wo der Operator sitzt.« Sieberaths klar definiertes Ziel: einfacher und übersichtlicher soll es werden! Aus einer Real-Life-Messkampagne im Frühjahr 2013, an der vier Nationen beteiligt waren, gilt es, die richtigen Rückschlüsse zu ziehen. Sieberath: »Das Link-22-System besteht aus zahlreichen Komponenten, deren Statusdaten dem Operator gemeldet werden. Diese Statusdaten sind so aufzubereiten und kompakt darzustellen, dass der Operator den Betrieb des Systems überwachen und steuern kann, ohne dass er Einschränkungen bei seiner taktisch-operationellen Hauptaufgabe hinnehmen muss.« Mit Hilfe einer verbesserten Signalvorverarbeitung soll der Operator merklich entlastet werden. Sieberath: »Bei der Aufbereitung der Meldungen gilt es zu unterscheiden, welche sinnvoll und wichtig und welche redundant sind.«

Bei der Übermittlung von Daten, die beispielsweise zwischen einer Gruppe von Schiffen auf bestimmten Frequenzen funktionieren soll, ist wieder das Know-how der FKIE-Experten gefragt. Das gilt insbesondere auch für die Auswertung und Beurteilung von solchen Daten, die systematisch zu Testzwecken übertragen werden. Für das FKIE-KOM-Team gibt es somit zahlreiche Herausforderungen, die von den Experten für Nachrichtentechnik und Informationsverarbeitung zu meistern sind. Das Team erstellt zu diesem Zweck Szenarien und Auswertesoftware und testet damit das Netzwerk unter Belastung, um die Praktikabilität der erweiterten Netzwerk-Managementfunktionen zu prüfen. Damit trägt das FKIE zum Erfolg des taktischen Datenlinksystems Link-22 bei.

SPRACHSUCHE IN »BIG-AUDIO-DATA«

Zuverlässige Sprachdetektion – wesentlich in vielen Einsatzszenarien.

Auf allen Kanälen kreucht und fleucht und rauscht es: YouTube, DropBox, die eigene Festplatte – technisch wird es immer leichter, Audiodateien aufzuzeichnen – und Speicherplatz ist immer günstiger verfügbar. Das Team um Professor Frank Kurth von der Abteilung Kommunikationssysteme (KOM) hat eine Technologie entwickelt, die Sprache auch im größten Big-Data-Haufen findet.

160 Stunden Rauschen. Mehr ist auf den Audiodateien nicht zu hören. Vermutlich. Oder doch? Das Problem: niemand wird sich die Mühe machen, das ernsthaft zu überprüfen. Denn wer sich endloses Rauschen oder Hintergrundgeräusche anhört, wird daran auch auf Dauer keinen Spaß entwickeln. »Solche Datenmengen sind manuell nicht handhabbar«, weiß Prof. Dr. Frank Kurth von der Abteilung Kommunikationssysteme (KOM) am FKIE, »daraus ergibt sich unsere Aufgabenstellung. Wir spezialisieren uns deshalb auf die Verarbeitung von Massendaten.« Und das bedeutet: In Big Data nach der Nadel im Heuhaufen suchen!

Das Team am FKIE entwickelt seit einigen Jahren eine Technologie zur Erschließung von Audiosignalen. Besonderes Augenmerk legen die Experten dabei auf die Detektion von Sprachanteilen in Schmal- und Breitbandsignalen. Kurth: »Wir versuchen relevante Signale aus Signalmassendaten herauszufiltern, das bedeutet: Sprachanteile auffinden und herausschneiden.« Big Data ist der Begriff für Datenmassen, die kein Mensch ohne Hilfsmittel je überblicken kann: stundenlange Video- oder Audioaufzeichnungen ebenso wie alle anderen heutzutage sensoriell aufgenommenen Datenströme. Die gesuchte Nadel, das können zum Beispiel die entscheidenden fünf Sekunden eines ausführlichen Gesprächs unter Kriminellen, gewonnen aus umfangreichem sichergestelltem Audiodatenmaterial, sein.

Die Entwicklung der zum Patent angemeldeten »Shift-Methode« des FKIE ist inzwischen so weit fortgeschritten, dass selbst in Dateien mit schlechter Qualität und vielen Störgeräuschen die Sprachanteile gut herausgefiltert werden können. Zwei Testszenarien in 2013 konnten die verbesserte Leistung der Shift-Methode beweisen. Dies funktioniert unabhängig von der Frequenzlage. Kurth: »Wir können mit dieser Software auch Sprache in ganz anderen Frequenzbändern, zum Beispiel im Funksignalspektrum, detektieren.« Aber auch gewöhnlichere Hindernisse gilt es aus dem Weg zu räumen: So ist die Software in der Lage, Maschinengeräusche oder Straßenlärm herauszufiltern. »Robust gegen Störgeräusche«, nennt Kurth das. In der Fachsprache heißt das Projekt daher »Robuste Sprachdetektion für komplexe Signalszenarien«.

Die Shift-Methode ist in der Lage, im Kurzzeitspektrum menschlicher Sprache typische Strukturen zu erkennen, zum Beispiel stimmhafte Anteile. »So können wir kleinste klangliche Bestandteile detektieren und so herausfinden, dass und wo gesprochen wird«, erklärt Kurth. Kurth studierte Informatik und Mathematik und schloss sein Studium mit einer Diplomarbeit über Audiosignalverarbeitung ab. Mit seiner Doktorarbeit sorgte Kurth 1999 für Aufsehen, indem er dort das Problem mit Qualitätsverlusten bei wiederholter Audiocodierung löste. 2013 wurde er zum außerplanmäßigen Professor an der Universität Bonn ernannt.

Mit der Entwicklung der Software ist Kurth sehr zufrieden, der Nutzen sowohl im zivilen Bereich als auch im Bundeswehrumfeld liegt auf der Hand. Kurth erkennt aber weiterhin Ausbaupotenzial: »Die von uns entwickelte Technologie ist noch wesentlich universeller einsetzbar«, ist er überzeugt. Und man merkt ihm an, dass er sich unvermindert für dieses Thema begeistert, wie sein Ausblick beweist: »Mit den neuen Methoden zur Sprachsuche könnten wir eine robuste Art der Schlüsselworterkennung, also zum Keyword-Spotting realisieren. Dann hätte man mit einem Schlag neue, leistungsfähige Lösungen für eine Vielzahl von Problemen – das ist ein faszinierender Aspekt!«

Audiomassendaten bilden einen großen Teil von »Big Data«.

KOMMUNIKATIONSSYSTEME

Leitung:
Dr.-Ing. Michael Wunder
Telefon +49 228 9435-511
michael.wunder@fkie.fraunhofer.de

INFORMATIONSTECHNIK FÜR FÜHRUNGSSYSTEME (ITF)

Ausrichtung der Abteilung

Komplexe, dynamische Führungs- und Entscheidungsprozesse sind häufig gekennzeichnet durch hohen Zeitdruck in Verbindung mit hohem Risiko für Fehlentscheidungen, viele kooperierende Akteure, Wechselwirkungen zwischen simultanen Aktivitäten, Ressourcenkonflikte sowie teilredundante, fehlende oder unscharfe bis falsche Informationen. Die eingesetzten IT-Systeme sind oft heterogen, komplex, unflexibel und untereinander nicht interoperabel.

Die Abteilung entwickelt Architekturen und Interoperabilitätslösungen für Führungs- und Assistenzsysteme zur Unterstützung einer vernetzten Operations- bzw. Unternehmensführung.

Die Erzeugung eines unternehmensweiten, konsistenten Lagebildes ist die Voraussetzung für zielgerichtete Entscheidungen und abgestimmtes Handeln.

Abläufe werden analysiert, modelliert, optimiert, Konzepte und Architekturen für interoperable Systeme und Systemverbünde entwickelt, prototypisch implementiert sowie verifiziert. Zur Beherrschung der Informationsflut werden außerdem Verfahren zur automatischen Informationsanalyse und Fusion entwickelt.

Forschungs- / Entwicklungsbereiche

- Interoperabilität
- Architekturen von IuK-Systemen
- Informationsanalyse

Schwerpunkte / Kernkompetenzen

- Prozessanalyse, Modellierung, Ablaufoptimierung
- Harmonisierung komplexer IT-Systeme, Migration
- Qualitätssicherung
- Wissens- und Workflow-Management
- Sprachverarbeitung, Computerlinguistik
- Grafische Lagekarten
- Generierung und Nutzung von Ontologien

Projekte

- Meldewesen und Unternehmenskommunikation
- Informationsextraktion, intelligente Suche
- Aktuelle Lagesituation in Unternehmungen
- Harmonisierung von Führungsinformationssystemen

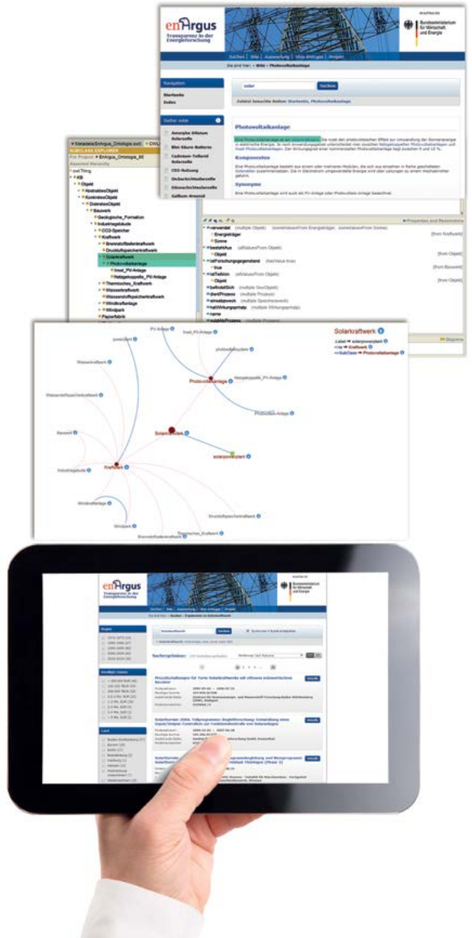
ENERGIEFORSCHUNG AUF EINEN BLICK

Nicht alles, was Energietechnik-Experten zu Papier bringen, ist leicht verständlich. Da die Energiewende aber auf unterschiedliche Weise jeden angeht, gilt es, das Wissen auch für jedermann zugänglich zu machen. Mit dem Gemeinschaftsprojekt EnArgus® öffnen die findigen Wissenschaftler am FKIE mit gut durchdachter Wissensrepräsentation Augen.

Wenn ein ganzes Land es sich zum Vorsatz macht, neue Technologien zur Energiegewinnung konsequent zu fördern, dann sind alle gefragt: Wissenschaft, Politik, Gesellschaft. Wenn aber jeder seinen Teil zum Gelingen beitragen können soll, muss auch die Kommunikation untereinander funktionieren. Mit dem Projekt EnArgus®, an dem sich unter Koordination des Fraunhofer-Instituts für Angewandte Informationstechnik FIT neben dem FKIE weitere sieben Partner aus Energieforschung und Informatik beteiligen, soll daher im Auftrag des Bundesministerium für Wirtschaft und Energie Transparenz in die Energieforschungsförderung und in die Bewertung technologischer Entwicklungen gebracht werden.

Wissenschaftler formulieren gern in Fachbegriffen

Die Transparenz wird dadurch hergestellt, dass EnArgus® ein Gesamtsystem bereitstellt, mit dem in den Forschungsförderungsdatenbanken gesucht werden kann. Im Vergleich dazu sucht eine Suchmaschine wie Google im gesamten Internet. EnArgus® arbeitet aber nicht nur mit genau spezifizierten Daten, sondern verwendet auch ein anderes Suchprinzip: Wird ein Datenbestand über Forschungsvorhaben mit einer stichwortartigen Suche wie bei Google ausgewertet, findet der Laie nur wenige der gesuchten Vorhaben, nicht zuletzt weil Wissenschaftler gern in Fachbegriffen formulieren, die der Laie weder kennt noch für seine Suche nutzt. Dabei wäre es gerade im Bereich der Energietechnik wichtig, zum Beispiel potenzielle Projektträger, aber auch Politiker oder Journalisten in die Lage zu versetzen, zu recherchieren, was möglich ist und was bereits gemacht wird. EnArgus® überwindet das Problem der nur wenigen bekannten Fachbegriffe, indem Wissen über Energieforschung mit in die Suche einbezogen wird. Dazu benötigt man eine Ontologie, in der dieses Wissen repräsentiert ist, so dass dem Suchenden zu einem eingegebenen Begriff auch weitere Fachbegriffe vorgeschlagen werden, die so in die Suche mit einbezogen werden können. Diese Fachontologie entwickelt das FKIE-Team um Professor Ulrich Schade in Zusammenarbeit mit den Energieexperten in dem Projekt. So wird die Lücke zwischen Fachartikeln auf der einen und nachvollziehbarer Repräsentation von Wissen auf der anderen Seite geschlossen und die Transparenz im Bereich der Energieforschungsförderung deutlich erhöht. Die von den Informatikern entwickelte Ontologie reichert jeden Suchbegriff an, stellt semantische Relationen her, findet Ober- und Unterbegriffe sowie Synonyme und Abkürzungen. »Das Wissen, das in Texten steht«, erklärt Schade, »muss in den Computer hinein.« Und anschließend natürlich auch wieder heraus. Was wie eine Selbstverständlichkeit erscheint, ist in Wirklichkeit die Herausforderung. Und mit ihrer Arbeit werden die Projektmitglieder von EnArgus® zugleich zu Streitern wider das Fachchinesisch, frei nach dem Motto: »Wir müssen das ja auch lesen und verstehen.«



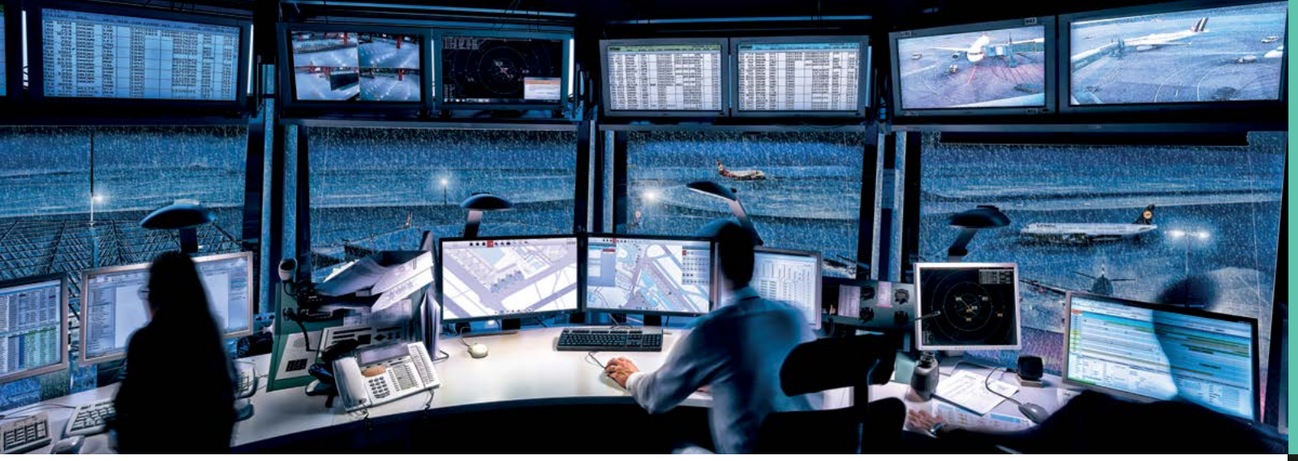
Aus dem EnArgus®-Energieforschungswiki (oben) wird das Wissen extrahiert und in der Ontologie (Mitte) repräsentiert. Damit steht es für das Suchsystem (unten) zur Verfügung.

Phase 2 des Projekts startete im Juli 2013

In Phase 1 hatte man sich in dem 2011 gestarteten Projekt auf vier Kernbereiche – Wind, Batterie, CO2-Abscheidung und -speicherung, Energieeffizienz in der Industrie – beschränkt. Mit Phase 2, die im Juli 2013 gestartet wurde, wird das Themenspektrum der Suchmaschine nun erweitert. »Das Projekt ist schon an einem Punkt, an dem man mit dem bislang entwickelten Informationssystem bereits sehr gut arbeiten kann«, befindet Schade. Mitarbeiter Lukas Sikorski demonstriert das gern an ein einigen Beispielen: Der Suchbegriff »Solarkraftwerk« beispielsweise fördert lediglich 38 Forschungsvorhaben aus unterschiedlichen Datenbanken zutage. Ergänzt um die vom System vorgeschlagenen Begriffe »Solaranlage« und »solar power plant« sind es schon 219. Eine Autocomplete-Funktion bietet überdies vorab bereits automatisch Vorschläge, während man den Begriff eintippt. Und filtern kann man die Ergebnisse anschließend nach Zeitraum, Bundesland, Fördersumme oder Zuwendungsgeber.

Bald für jedermann zugänglich

Projektträger im Auftrag des Ministeriums ist das Forschungszentrum Jülich. Ein Ziel ist, das Informationssystem bis 2016 mit allen öffentlichen Datenbanken zu bestücken und die Abfrage, ausgenommen datenschutzrelevanter Angaben, mit der intuitiven Suchfunktion noch in diesem Jahr für jedermann verfügbar zu machen. In einer Experten-Version erhalten zudem Projektträger, Ministerien und gegebenenfalls Forscher Vollzugriff auch auf sensible Daten. Mit dem dann vorliegenden Gesamtsystem können auch vermeidbare Doppelförderungen besser erkannt und Anfragen von Journalisten und der interessierten Öffentlichkeit leichter beantwortet werden. Bis dahin wird das Team um Professor Schade noch manchen Beitrag zur Energieforschung auf seine Verständlichkeit abklopfen, das enthaltene Wissen aufbereiten und für die Suche verfügbar machen.



EISFREIE LANDEBAHN DANK PERFEKTER VERNETZUNG

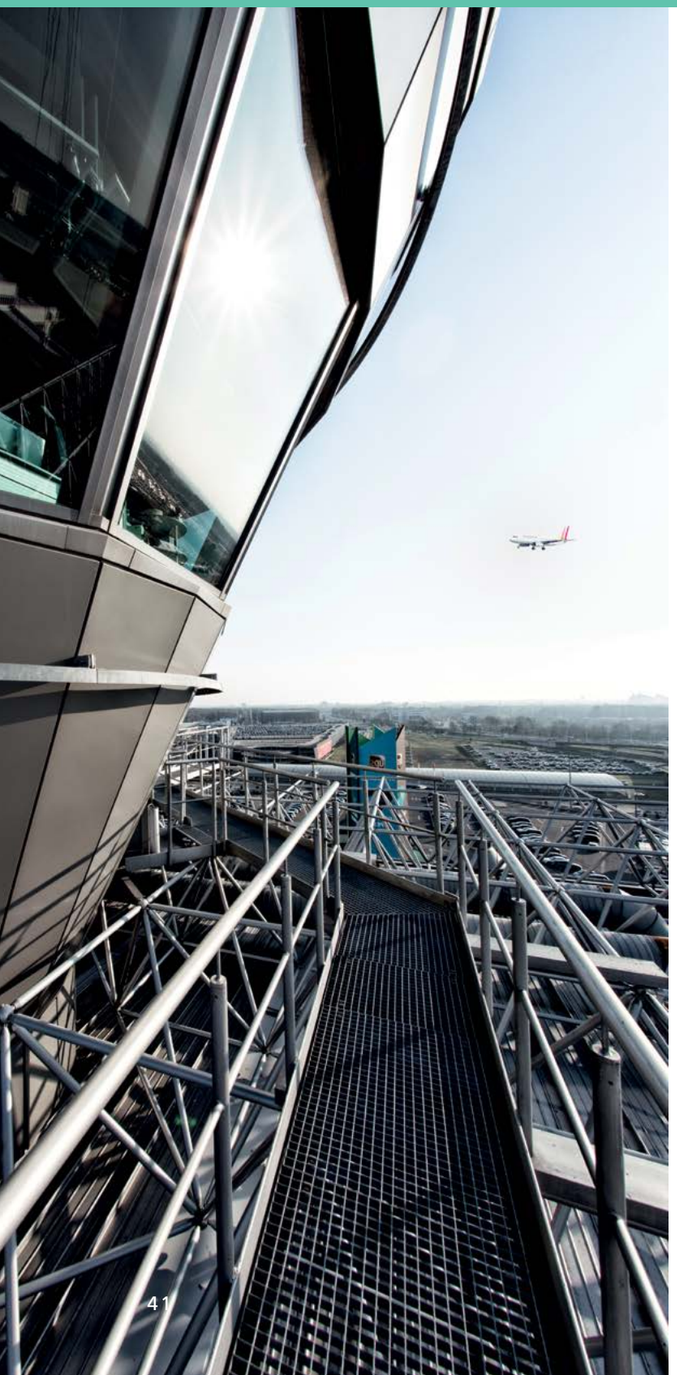
Am Flughafen Köln/Bonn stellt sich ein abteilungsübergreifendes Team des Fraunhofer FKIE in einem Pilotprojekt mit intelligenter Vernetzung und elektronischem Lagesystem den Unbilden des Wetters entgegen – und sorgt mit »Intelsys« nicht nur für eine eisfreie Landebahn.

An Sensoren mangelt es am Flughafen Köln/Bonn nicht: Die Fühler messen über das Gelände verteilt Luftfeuchtigkeit, Temperatur, Niederschlag oder Windrichtung. Das hilft den Flughafen-Mitarbeitern zuverlässig bei der Einschätzung der Wetterlage. Und es gibt Sensoren in den Tanks, die verraten, ob noch ausreichend Enteisungsflüssigkeit vorhanden ist. Doch wie können all diese Informationen sinnvoll vernetzt in die Arbeit des Flughafens einfließen?

Hier kommt das Know-how der Abteilungen Ergonomie und Mensch-Maschine-Systeme (EMS) und Informationstechnik für Führungssysteme (ITF) des Fraunhofer FKIE ins Spiel. Mit dem »**Int**egrierten **E**ntscheidungsunterstützungs- und **L**agedarstellungs**sys**tem«, kurz: »Intelsys«, hat das Team ein innovatives System entwickelt und im operativen Netzwerk des Flughafens Köln/Bonn in der Praxis getestet. Das System vereint sämtliche Sensordaten in einem einheitlichen Lagebild und macht potenzielle Probleme im Voraus erkennbar. Dazu dienen direkt aus den Sensoren abgeleitete Warnungen wie bei Schnee und Eis auf der Start- und Landebahn sowie beim Ausgehen des Enteisungsmittelvorrates – sehr wohl aber auch Hinweise, die erst aus der Kombination verschiedener Datenquellen gefolgert werden können.

Im Dezember 2012 traten Vertreter des FKIE und des Flughafens Köln/Bonn erstmals in Kontakt, um über eine mögliche Vernetzung von Sensordaten zu beraten. Was an einem Flughafen geschieht, nennen Informatiker gerne eine »komplexe Prozesslandschaft« – übersetzt heißt das nichts anderes als: eine Herausforderung! Dieser stellte sich das Projektteam und entwickelte Ideen, wie die vorhandenen Daten in einem System zusammengeführt und dann konkret genutzt werden können. Im Februar 2013 begann die Entwicklung des Systems, das von Softwareentwickler Claus J. Weber modular gebaut und mit einer Regel-Engine ausgestattet ist. Die Abläufe am Flughafen

Hier erfolgt die Bekanntgabe, dass die Nutzung einer Start-/Landebahn temporär nicht möglich ist. Diese sogenannte »Betriebsunterbrechung« wird über Intelsys dokumentiert. Das bisher manuell auszufüllende Formular wird dabei vom System generiert. So können sich die Mitarbeiter am Flughafen voll auf ihr Kerngeschäft konzentrieren.



werden für die Berücksichtigung durch das System in Regeln abgebildet und können dadurch jederzeit flexibel angepasst oder ergänzt werden. Die mathematisch-technische Assistentin Monika Meister sowie der Fachinformatiker Bastian Weltjen entwickeln die benutzungsfreundliche und übersichtliche grafische Oberfläche. Als erstes Testfeld wurde der Winterdienst auserkoren.

Die Informatiker Arne Schwarze und Ron Becker sind für den Kundenkontakt zuständig: sie stehen sowohl im Austausch mit den Mitarbeitern des Winterdienstes als auch mit den Technikern am Flughafen. Sie ermitteln die Anforderungen und die Probleme, die es zu meistern gilt. Die Zusammenarbeit klappt hervorragend, erklärt Becker: »Was wir vor Ort auf Papier und mit PowerPoint entwerfen, können Claus, Monika und Bastian hier im Institut dynamisch umsetzen: in Code gießen und testen.« Und Schwarze fügt an: »Claus überrascht uns dabei immer wieder, woran er schon alles denkt.«

Der Winterdienst ist am Flughafen Köln/Bonn vom 1. November bis zum 30. April aktiv. Entsprechend ging Intelsys am 1. November 2013 als Pilotprojekt an den Start. »Wir zapfen vorhandene Subsysteme an, die dann in Intelsys zusammengeführt werden«, erläutert Schwarze das Prinzip. Die Meteo-Sensoren am Flughafen liefern Luft- und Bodentemperatur, Gefrier- und Taupunkt, relative Feuchte, Niederschlagsart und -menge. Dazu werden in Intelsys auch die Flugdaten verarbeitet, aktuelle Wettervorhersagen sowie die Tankfüllstände der Enteisungsmittel. Sämtliche Daten fließen dann in der übersichtlichen Lagedarstellung zusammen und können von den Mitarbeitern des Winterdienstes in der Verkehrszentrale des Flughafens bearbeitet werden. Ein Areal wie das eines Flughafens bietet viele unterschiedliche Wetterzonen, die alle individuell betrachtet sein wollen. Becker: »Bislang sammelt eine Person alle Informationen in ihrem Kopf und koordiniert die Arbeit der Mitarbeiter im Winterdienst – das können je nach Wetterlage knapp 30 Mitarbeiter sein.« Niemand bezweifelt, dass das funktioniert. Aber das Team ist auch überzeugt: die moderne Technik und ihre Vernetzung mit Intelsys kann dazu beitragen, die Abläufe übersichtlicher und vorhersehbarer zu machen.

Ihre Aufträge erhalten die Mitarbeiter im Winterdienstteam über ein Handheld. Die zentrale Lagedarstellung zeigt dann den Status der Bearbeitung an: »Icons informieren, wo es beispielsweise einen Sprühauftrag gibt«, erläutert Becker. Ist die Fläche gesprüht, erscheint sie auch in Intelsys unmittelbar wieder im Normalzustand: der Auftrag ist erledigt. Und auch für den Enteiser-Nachschub wird zuverlässig gesorgt: Dazu lassen sich Bestellungen direkt aus der Lagedarstellung beauftragen, sobald die Regelverarbeitung vor einem potenziellen Engpass warnt – selbstverständlich unter Berücksichtigung von Wetteraussichten und Lieferfristen. »In Bezug auf proaktives Handeln gibt es noch ein unglaubliches Optimierungspotenzial«, ist Teamleiter Dr. Michael Wunder überzeugt: »An einem Flughafen laufen ja hunderte Prozesse ab, man denke allein an die Passagierströme.« Wunder sieht große Fortschritte, die das Team an dem Flughafen machen konnte: »Wir haben hier eine richtig gute Mannschaft.«

Das zeigt sich auch bei den Mitarbeitern vor Ort: »Die Akzeptanz am Flughafen war rasch sehr hoch«, erinnert sich Becker: »Nachdem wir glaubhaft vermitteln konnten, dass es nicht unser Ziel ist, Stellen überflüssig zu machen oder wegzurationalisieren.« Spätestens ab dem Punkt habe es guten Zuspruch gegeben. Arne Schwarze ergänzt: »Am Flughafen sieht man uns als echten Partner mit technischem Know-how. Wir konnten das Bewusstsein vermitteln, dass wir sehr breit aufgestellt sind.« Der Flughafen seinerseits lobt die exzellente Zusammenarbeit und das fundierte Wissen der FKIE-Mitarbeiter auf einer gemeinsamen Pressekonferenz im Frühjahr 2014. Athanasios Titonis, Technischer Geschäftsführer des Flughafens Köln/Bonn, schätzt Intelsys: »It's a smart revolution in our system.« Dr. Michael Wunder knüpft da gerne an: »Wir möchten unser gesamtes Know-how nach und nach einbringen. Wir haben einen Kern geschaffen, der weiter wachsen kann.« Die Verkehrszentrale nutzt das System inzwischen bereits auch außerhalb des Winterdienstes, um zum Beispiel auf der Karte zu sehen, wo welcher Flieger steht.

Bis Ende April 2014 wurde das System im Live-Betrieb erprobt. Die Zusammenarbeit soll fortgesetzt und das Projekt mit weiteren Modulen ergänzt werden. Angestrebt wird ein »Real Time Overview«, in dem sämtliche Prozesse am Flughafen im System abgebildet sind und gesteuert werden können.

INFORMATIONSTECHNIK FÜR FÜHRUNGSSYSTEME

Leitung:
Prof. Dr.-Ing. Frank Flemisch
Telefon +49 228 9435-573
frank.flemisch@fkie.fraunhofer.de

ERGONOMIE UND MENSCH-MASCHINE-SYSTEME (EMS)

Ausrichtung der Abteilung

Das Zusammenspiel zwischen komplexer Technik und Menschen ist nicht trivial und kann bei Versagen, wie eine Reihe schwerer Unfälle mit Waffensystemen, Industrieanlagen, Zügen, Schiffen, Flugzeugen und Kraftfahrzeugen zeigen, katastrophale Folgen haben. Dies lässt sich durch ein systematisches Vorgehen bei der Gestaltung von Mensch-Technik-Systemen entscheidend verbessern. Dazu wird am FKIE der Grundgedanke der nutzerzentrierten Gestaltung mit der hier seit Jahrzehnten etablierten Systemergonomie fusioniert und zu einer nutzerorientierten, balancierten Mensch-System-Integration (Balanced Human-Systems-Integration) weiterentwickelt. Dabei wird, ausgehend von fundierten Analysen, Modellen und Simulationen des Ist- und Sollzustandes, das angestrebte Systemverhalten und die dazu optimale Mensch-Technik-Schnittstelle zusammen mit Nutzern, Entscheidern und anderen Anspruchsgruppen (Stakeholdern) in eigens dafür optimierten Laboren partizipativ gestaltet. Die Systemlösungen werden prototypisch umgesetzt, in Labor- und Feldversuchen evaluiert und iterativ verbessert.

Ziel ist dabei eine optimale Balance in Bezug auf Leistungsfähigkeit, Sicherheit, Gebrauchstauglichkeit/-freundlichkeit sowie Umwelt- und Kostenfaktoren zu erreichen.

Forschungs- / Entwicklungsbereiche

- Methoden und Werkzeuge der Human-Systems-Integration
- Mensch-Maschine-Schnittstellen für Einsatzsysteme
- Analyse und Gestaltung von Prozessen in sicherheitskritischen Systemen
- Visualisierung und Interaktion für mobile Computer
- Führung kooperativer mobiler Systeme

Schwerpunkte / Kernkompetenzen

- System- und Anforderungsanalyse
- System- und Menschmodellierung und -simulation
- Partizipativer Entwurf des Systemverhaltens und HMI-Gestaltung (Ecological Interface Design)
- Prototypische Implementierung
- Evaluierung in Labor- und Feldversuchen

Beispielprojekte / Produkte

- VerSiA – Visualisierung verteilter Simulationsdaten
- Operationszentrale der Zukunft
- VesperPlus – Steigerung der Effektivität und Effizienz von Prozessen zur Verbesserung der Gefahrenabwehr im Fährverkehr und zur Unterstützung der Akteure
- Persönliche Ausrüstung Soldat
- StrassRob – hochautomatisiertes Fahren von Lkw-Konvois

SCHÖNE AUSSICHTEN: DATENBRILLEN MENSCH-ZENTRIERT GESTALTEN

Ein Head-Mounted Display ist ein kleindimensioniertes Display, welches vor dem Auge angebracht ist. Mit dem Gerät können Arbeiter, z. B. in der Industrie, Arbeitsanleitungen zeitgleich zu ihrer Tätigkeit betrachten, ohne dass sie dabei am Rechner sitzen müssen.

Spätestens seit »Google Glass« sind Datenbrillen ein Thema. In speziellen Bereichen der Arbeitswelt existieren ähnliche Modelle bereits, durchgesetzt haben sie sich bis heute kaum. Das lag vor allem an Hardware, die sich nicht ausreichend an den Bedürfnissen des Menschen orientiert. Mit Modellen der neuen Generation könnte sich das ändern: Für die Bundesanstalt für Arbeitsschutz und Arbeitsmedizin entwickelt ein FKIE-Team Einsatzempfehlungen – und gewinnt dabei überraschende Erkenntnisse.

Wer je ein Regal aus fertigen Einzelteilen zusammenbauen musste, der versteht sofort, warum ein Head-Mounted Display (HMD) eine hilfreiche Sache zu sein verspricht: Mit einem kleinen, vor dem Auge positionierten Display können komplexe Montageanleitungen für den Hobbymonteur bequem und direkt im Sichtfeld angezeigt werden. Gleichzeitig können die vorgegebenen Abläufe mit beiden Händen umgesetzt werden. Besonders im industriellen Umfeld, zum Beispiel in der Fertigung oder Kommissionierung, ist das Interesse besonders groß, solche Hilfsmittel einzusetzen. Ob so ein Gerät aber tatsächlich als »bequem« empfunden wird und wie Nutzer unmittelbar auf den Gebrauch reagieren, das hat die Forschungsgruppe Human Factors des FKIE in einer zweijährigen Studie zwischen 2011 und 2013 erforscht. Für eine ganzheitliche und interdisziplinäre Betrachtung in Zusammenarbeit mit der RWTH Aachen waren daran Informatiker, Medizintechniker, Ingenieure, Psychologen sowie ein Sportwissenschaftler beteiligt. Für die Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA) werden aus den Untersuchungen nun Einsatzempfehlungen sowie Gestaltungshinweise für die Hersteller und Anwender formuliert.

In Werbeclips für die Google-Datenbrille sieht alles spielerisch leicht und angenehm aus. Doch in der Realität, noch dazu im industriellen Arbeitsalltag, mag sich das anders darstellen. Die vom Team in der Untersuchung verwendete Datenbrille ist deutlich robuster – und damit wohl auch näher an der Realität für den Einsatz in der Industrie. Sabine Theis erläutert den Fokus beim Versuchsaufbau mit insgesamt 60 Teilnehmern: »Für uns lautete die Fragestellung: Wie wirkt sich eine Datenbrille auf das visuelle und muskuläre System des Menschen aus, wenn wir sie während einer typischen Arbeitsschicht tragen?« Dazu entwickelte das Team einen Versuchsaufbau inklusive einer dreieinhalbstündigen Fahrzeugmontage- und Wartungsaufgabe, die die Versuchsteilnehmer mit Hilfe der auf einer Datenbrille dargestellten Anleitungen absolvieren mussten. »Die Arbeit wird mit so einem Gerät nicht unbedingt schneller verrichtet«, erläutert Theis eines der Ergebnisse der Studie, »der kognitive Prozess, durch den wir Informationen aufnehmen, wird durch eine Datenbrille nicht per se verkürzt. Wir reduzieren lediglich den Schritt, mit dem wir uns einer Darstellung zuwenden.« Anders formuliert: Ein Display am Kopf macht nicht schneller und auch nicht klüger.

ERGONOMIE UND MENSCH-MASCHINE-SYSTEME

Dennoch bietet eine Datenbrille viele positive Aspekte. Immerhin ermöglicht es ein solches Gerät, ohne besondere Ausbildung komplexe Aufgaben zu absolvieren. Naheliegende Probleme scheinen sich bei genauer Betrachtung zu zerstreuen: Anhand der Untersuchungen wurden auch nach dreieinhalbstündigem Tragen eines HMD keinerlei Beeinträchtigungen der Sehfähigkeit festgestellt. Dr. Thomas Alexander, Leiter der Forschungsgruppe, beurteilt die Ergebnisse der Untersuchung überwiegend positiv. Er verweist auf einen immens bedeutsamen Aspekt bei der Hinführung zum Arbeiten mit einem HMD: »Wichtig ist, dass die Einführung solcher Geräte in den Arbeitsalltag gut kommuniziert wird.« Die Untersuchungsergebnisse des Teams zeigen, dass es sich empfiehlt, die Geräte langsam und schrittweise in die Arbeitsabläufe zu integrieren und dabei keine künstliche Konkurrenzsituation zwischen Mensch und Maschine zu erzeugen. »Außerdem sollte man die Arbeitnehmer bei der Arbeitsplatzgestaltung und Datenbrillennutzung miteinbeziehen, um die Akzeptanz zu erhöhen«, erklärt Alexander. Neue Nutzer berichten über eine physiologische Eingewöhnungszeit von rund 20 bis 30 Minuten. Erstaunlich findet Alexander, dass ältere Probanden sich besser mit dem Arbeitsgerät arrangierten, wie die Abfrage der subjektiven Wahrnehmung ergab: »Die Jüngeren fühlten sich rascher beansprucht, obwohl sie der Technologie zu Anfang aufgeschlossener gegenüberstehen.« Dafür deute sich bei älteren Teilnehmern ein Hinweis auf eine stärkere Aktivität des linken Nackenmuskels, Splenius Capitis, an. Generell konnten die subjektiven Eindrücke der Teilnehmer Verbesserungspotential eher identifizieren als die physiologisch messbaren Ergebnisse. Entsprechend wichtig sei eine behutsame Einführung des neuen Arbeitsgerätes in der Praxis, so ein erstes Fazit des Teams.

Bei der Studie ging es übrigens nicht um einen Blick durchs Schlüsselloch in die Zukunft: die »Augmented Reality« mit aktuellen Informationen, die sich als Erweiterung in die Umgebung konsistent einfügen, spielte bei der Untersuchung keine Rolle. Theis: »Wir haben nur das getestet, was praktische Relevanz für die Unternehmen besitzt.« Die »Erweiterte Realität« betrachtet das Team in anderen Forschungsprojekten. Mögliche Einsatzgebiete für HMDs zur Informationsbereitstellung sowie prozessbegleitend sieht Alexander in spezifischen Bereichen der Industrie, »zum Beispiel bei der Wartung von Windanlagen, für Logistiker, Instandsetzer, aber auch für Nachtsichtgeräte zum Beispiel im militärischen Einsatz«.

Ob sich diese Technik im Freizeit- und Privatbereich durchsetzen kann? Hier ist Alexander zurückhaltender: »Das ist jetzt so eine Mode – vielleicht setzt es sich durch, vielleicht nicht.« Ein großes Problem für die Alltagsnutzung sieht er aber sehr wohl: »Kein HMD funktioniert draußen im Freien, das ist einfach zu hell.« Dazu müsste das Display so hell sein, dass damit wiederum eine Schädigung des Auges doch nicht ausgeschlossen sei. Und dann bereitet selbst die schönste Erweiterte Realität keine Freude.

MIT DEN ZÜGELN IN DER HAND GEMEINSAM ANS ZIEL

Geht es nach den Wissenschaftlern der Abteilung Ergonomie und Mensch-Maschine-Systeme (EMS), dann funktioniert die Automation in Fahrzeugen bald wie ein zuverlässiger Teampartner des Menschen. Mit einer gut abgestimmten kooperativen Interaktion ist ein Team aus Fahrer und Automation allen Anforderungen besser gewachsen als Fahrer oder Automation allein. Ein Vierbeiner spielt bei diesem Grundgedanken eine wichtige Rolle.

Alles ist vorbereitet für die Probefahrt: die virtuelle Fahrbahn ist auf eine Leinwand projiziert, Lenkrad, Gas-, Brems- und Kupplungspedal sowie die Gangschaltung in Position, die Rechner laufen sich warm für die Spritztour. In einem entscheidenden Detail unterscheidet sich der Versuchsaufbau im Erdgeschoss des Instituts jedoch von einer gewöhnlichen Testfahrt im Simulator: Nicht der Mensch soll hier mit der Maschine vertraut gemacht werden., sondern die Maschine mit dem Menschen: »Kooperative Fahrzeugführung« lauten der Name der Forschungsgruppe und zugleich das Forschungsziel des Teams in der von Prof. Dr. Frank Flemisch geleiteten Abteilung Ergonomie und Mensch-Maschine-Systeme (EMS). Was hier erprobt wird, ist nichts weniger als die perfekte Harmonie zwischen Mensch und Maschine.

Ein möglicher Weg zu diesem gar nicht mehr allzu fern scheinenden Ziel führt nach Auffassung der Wissenschaftler über ein uraltes Fortbewegungskonzept, das schon immer für den Menschen mitdachte und dennoch aus der Mode geriet: Pferde waren einst nicht nur das Transportmittel schlechthin – sie verfügten auch über den siebten Sinn, der manchem Fahrzeugführer bis heute abgeht. Die Fortbewegungsmaschine der Zukunft soll sich daher die guten Eigenschaften der Rösser zu eigen machen und für den Menschen mitdenken. Das Vorbild der Beziehung zwischen Reiter und Pferd dient als Designmetapher, die »H(orse)-Metapher« oder »H-Mode« haben bereits Einzug in den Fachjargon gehalten, von ihnen sollen sinnvolle Konzepte

Simulator zur Gestaltung einer biologisch inspirierten Bedienart für hochautomatisierte Fahrzeuge.

für die Fahrer-Fahrzeug-Interaktion abgeleitet werden. »Wie ein gutmütiges, gut trainiertes Pferd«, so stellt sich Professor Flemisch die Technik der Zukunft vor: Der Mensch kann entweder mehr Kontrolle ausführen, sinnbildlich also den Zügel fest halten, oder mehr Kontrolle der Fahrzeugautomation überlassen, was dem Lockerlassen des Zügels entspricht – ganz so, wie es die Situation erfordert.

Optimale Brücke zwischen Mensch, Technik und Umwelt

Um diesem Ziel näher zu kommen, bitten die Forscher für ihre Studien erfahrene Fahrer in ihr »Exploroscope«, das eingangs beschriebene Versuchslabor, in dem die Interaktion zwischen Fahrer, Technik und der virtuellen Verkehrssituation erforscht wird. Denn wer die »optimale Brücke zwischen Mensch, Technik und Umwelt« bauen möchte, weiß Flemisch, der benötigt Erfahrungswerte – und die sammelt das Team hier im Labor. Auch rechtliche Aspekte müssen die Forscher beachten, ebenso gilt es, die Nachfrage auf dem Markt im Auge zu behalten und mit all dem letztlich auch die gesellschaftliche Akzeptanz für solche Systeme.

Als Psychologe kann Matthias Heesen einen wertvollen Beitrag dazu leisten. Er forscht seit einigen Jahren an der »Kooperativen Fahrzeugführung« und ist seit Juli 2013 verantwortlich für die Forschungsgruppe, die sich derzeit noch vornehmlich mit Bodenfahrzeugen beschäftigt. »Das Konzept lässt sich zwar auch in der Luft anwenden, unser Fokus liegt aber auf der kooperativen zweidimensionalen Bewegung«, verrät Heesen. Bis auf weiteres bleibt man im EMS-Exploroscope also auf dem Boden der Tatsachen, gleichwohl sind die Konzepte für die Interaktion mit hochautomatisierten Fahrzeugen schon weit fortgeschritten, bei weitem aber noch nicht abgeschlossen.

Kontrolle zwischen Mensch und Maschine sinnvoll verteilen

Wer sich heute in ein modern ausgestattetes Auto setzt, stellt fest, dass es im Cockpit bei allerlei Gelegenheiten piepst und blinkt. Das ist zwar bisweilen hilfreich, bereitet aber bei weitem nicht jedem Fahrer Freude. Hier kommt der Psychologe Heesen ins Spiel: »Wir verfolgen eine Strategie der nutzerorientierten balancierten Gestaltung, welche die beiden Pole ›technikorientiert‹ und ›nutzerorientiert‹ berücksichtigt«, erklärt er. Dabei gelte es, »die Kontrolle zwischen Mensch und Maschine sinnvoll und der Situation angepasst zu verteilen. Wir verfolgen dabei einen kooperativen Ansatz.«

Der Teamgedanke hält also Einzug in die Verbindung zwischen Mensch und Maschine und in der Forschungsgruppe hat man klare Vorstellungen davon, wie das funktionieren kann: Der Fahrer solle grundsätzlich frei entscheiden können, ob er selbst steuern möchte oder wann er wie viel Verantwortung an die Technik abgibt. Er muss aber auch nachvollziehen können, wann der »Teampartner« Automation an seine Grenzen gerät, um dann entsprechend die Kontrolle übernehmen zu können. Da noch keine Automation so perfekt sei, dass sie in allen Situationen, in die sie geraten kann, stets die richtigen Entscheidungen trifft, sollte der Fahrer stets zu einem gewissen Grad in die Fahraufgabe eingebunden bleiben oder diese zumindest innerhalb einer gewissen Zeit wieder übernehmen können. In einigen Situationen kann es hingegen sinnvoll sein, wenn die Automation kurzzeitig die Kontrolle ganz an sich zieht, z.B. in kritischen Notfallsituationen, in denen der Mensch wiederum rasch an seine Grenzen stößt.

Ohne Liftboy im Aufzug?

Professor Flemisch ist als Ingenieur und Ergonom von seinem Forschungsfeld fasziniert. Dabei hat er nicht allein den technischen Fortschritt im Blick: »Eine wichtige Frage ist: wie führe ich eine solche neue Technik ein?« Er erinnert an ein Transportmittel, das heute für jeden selbstverständlich automatisch fährt, was vor noch gar nicht langer Zeit aber völlig undenkbar gewesen wäre: »Früher konnte sich niemand vorstellen, ohne Liftboy in einem Aufzug zu fahren. Es war eine anspruchsvolle Aufgabe, so einen Lift zu führen und die Kabine im richtigen Augenblick anzuhalten. Heute ist das überall ganz selbstverständlich automatisiert.« Die Aufgabe, den Menschen Vertrauen in ein technisches Artefakt zu geben und sich selbst zurückzunehmen, stehe im Vordergrund der Arbeit. »Die Gefahr ist, dass die Probanden einem System entweder zu viel vertrauen – oder sie vertrauen ihm zu wenig. Beides ist nicht gut«, beobachtet Flemisch immer wieder. Die Nachvollziehbarkeit von Automationsfähigkeiten und Handlungen könne hier ein wichtiger Schlüssel zum Erfolg sein. Und die Konkurrenz schläft nicht: Erst kürzlich hat Toyota das Concept Car FV2 vorgestellt, das auf der Horse-Metapher basiert.

»Wir sind spezialisiert darauf, Fachleute aus verschiedenen Bereichen an einen Tisch zu bringen«, erklärt Flemisch. Von diesem ganzheitlich-systemischen Herangehen verspricht sich das Team große Fortschritte und wichtige Erkenntnisse. Klar formuliert bleibt das Ziel mit dem »H-Mode«: Das volle Potenzial der Automation nutzbar machen, aber dem Menschen erlauben, die Zügel in der Hand zu behalten – wie beim Pferd.

ERGONOMIE UND MENSCH-MASCHINE-SYSTEME

Leitung:
Dr. Dirk Schulz
Telefon +49 228 9435-483
dirk.schulz@fkie.fraunhofer.de

FORSCHUNGSGRUPPE UNBEMANNTE SYSTEME (US)

Ausrichtung der Abteilung

Die Forschungsgruppe Unbemannte Systeme forscht seit mehr als zwanzig Jahren auf dem Gebiet der Robotik. Unser Forschungsgebiet ist die Entwicklung und Evaluation komplexer Mensch-Robotersysteme. Insbesondere liegt der Schwerpunkt auf der Informationsgewinnung mit heterogenen Mehrrobotersystemen in gefährlichen Umgebungen.

Für den Operateur ist die Interaktion mit solch komplexen Systemen eine schwierige Aufgabe. Intelligente Assistenzfunktionen sollen den Operateur auf allen Funktionsebenen unterstützen: angefangen mit der Navigation eines einzelnen Roboters bis hin zu Koordinationsproblemen bei Mehrrobotersystemen. Diese Unterstützung des Operateurs wird erreicht durch die Erweiterung der autonomen Roboterfähigkeiten und der Entlastung des Operateurs durch Assistenzfunktionen.

Die Entwicklung innovativer Werkzeuge für die Interaktion und Kooperation in Mensch-Mehrrobotersystemen stellt somit eine unserer Kernkompetenzen dar. Dafür werden kontinuierlich neue Entwicklungen in Experimentalsysteme integriert und in Zusammenarbeit mit den Nutzern aus der Bundeswehr und weiteren Behörden und Organisationen mit Sicherheitsaufgaben (BOS) evaluiert.

Forschungs- / Entwicklungsbereiche

- Konzeption und Entwicklung von Mensch-Mehrrobotersystemen
- Autonome Fähigkeiten für mobile Robotersysteme
- Assistenzfunktionen zur Entlastung des Operateurs
- Interoperabilität von Robotersystemen

Schwerpunkte / Kernkompetenzen

- Autonome Navigation für drinnen und draußen
- Umgebungserfassung: Sensorbasierte Modellerstellung, Tracking, Objekterkennung und semantische Sensordateninterpretation
- Explorations-, Planungs- und Koordinierungsverfahren
- Mobile Manipulation
- Direkte / indirekte Mensch-Roboter-Interaktion
- Software-Frameworks und Standards (z.B. JAUS, BML, ROS, DDS)
- Software- und Hardwareintegration sowie Evaluation von Anwendungssystemen
- Unabhängige Analyse- und Bewertungsfähigkeit

Projekte

- Assistenzfunktionen für Teilautonomie in mobilen unbemannten Systemen (ARMINIUS)
- Modularer Manipulatorroboter (ManipuR)
- Vernetzungsstrategien und Anwendungsszenarien für unbemannte Systeme (VARUS)
- Modulare CBRNE-Roboter und Manipulatorfahrzeuge
- Kommunikationsaspekte bei kleinen und mittleren UGVs (KoKus)
- RoboGasInspector
- Robot}air{

KÖNNER IN FILIGRANER MANIPULATION

Eine spezielle Jacke genügt Forscher Bernd Brüggemann, um einen Roboterarm zu bewegen: »Wearable Motion-capture« heißt diese Steuerung, die mittels Sensoren funktioniert. Was in der Demonstration wie gelungenes Synchronballett aussieht, ist in der praktischen Anwendung hilfreich bei Einsätzen, bei denen es auf Genauigkeit ankommt.

Entwickler autonomer Robotersysteme stehen nicht nur stets vor der Herausforderung, ihre Geräte mit neuen Fähigkeiten auszustatten. Zentrale Fragestellung für die Forscher lautet immer auch: wie kann die Interaktion zwischen Mensch und Roboter funktionieren? Zunehmend komplexere Funktionen moderner Robotersysteme erfordern oft auch komplexe Lösungen für die Steuerung. Dabei gilt natürlich: je einfacher und umstandsloser ein solches System gesteuert werden kann, desto besser. Entsprechend beeindruckend ist die Kontrolle, die das Team am Fraunhofer FKIE für einen Roboterarm demonstriert: Sie funktioniert intuitiv – man zieht einfach eine Jacke an und kann so den metallenen Arm sofort steuern.

Seit über 20 Jahren forschen die Wissenschaftler der Forschungsgruppe Unbemannte Systeme (US) in Wachtberg-Werthhoven an der Entwicklung komplexer Mensch-Mehrroboter-Systeme. Die Verwendung intelligenter Assistenzsysteme, die den Operateur unterstützen, gehört zum Ansatz, den die Forschungsgruppe verfolgt und der über die Jahre hinweg innovative Werkzeuge hervorbrachte, die das Team in Versuchssysteme einbauen und testen konnte. Zu diesen Assistenzfunktionen gehören die autonome Navigation ebenso wie sensorbasierte Umgebungsmodellierung, aber auch die direkte und indirekte Mensch-Roboter-Interaktion sowie mobile Manipulation.

Das Wort »Manipulation« ist in diesem Kontext streng wissenschaftlich und deshalb ausschließlich positiv konnotiert. Dementsprechend verwendet es Forscher Bernd Brüggemann vollkommen unbefangen, wenn er den Roboterarm vorstellt. Brüggemann benötigt dazu: Eine Jacke vom Textildiscounter. Einen Handschuh. Den Roboterarm. Und eine Handvoll Inertialsensoren. Aus diesen »Zutaten« hat das Team der Forschungsgruppe mit Jochen Welle, Bastian Gaspers und Brüggemann den Demonstrator gebaut. Brüggemann streift sich Jacke und Handschuh über. Fünf Inertialsensoren sind im rechten Ärmel sowie im Handschuh eingebaut und messen nun ständig die exakte Haltung von Schulter, Ober- und Unterarm, Handgelenk und Finger. Gibt Brüggemann die Verbindung frei, werden diese Daten unmittelbar an den Roboterarm weitergegeben, der daraufhin fließend die gleiche Haltung einnimmt wie Brüggemanns rechter Arm. Synchronisierte Präzision.

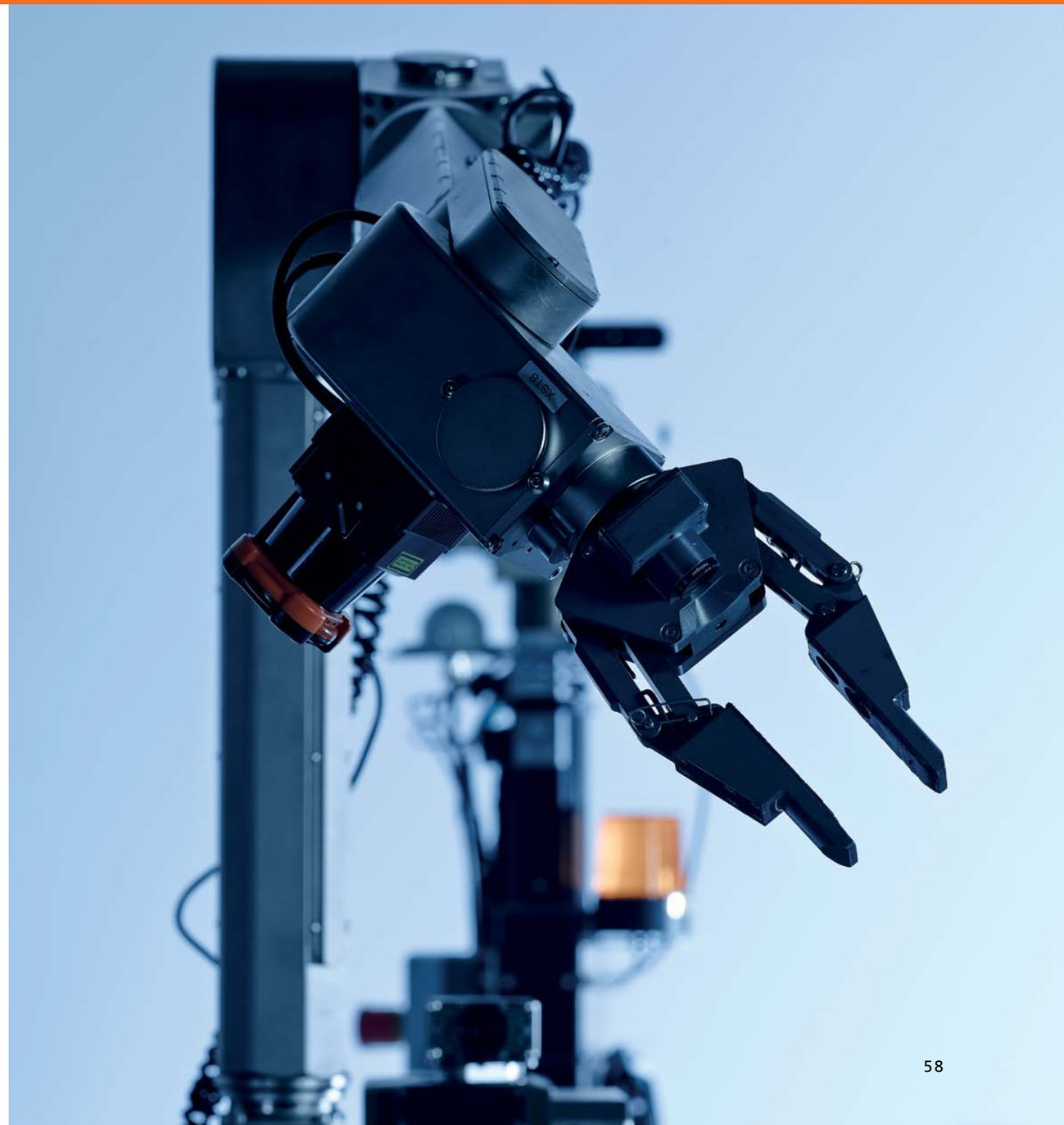
Roboterarm intuitiv bewegen

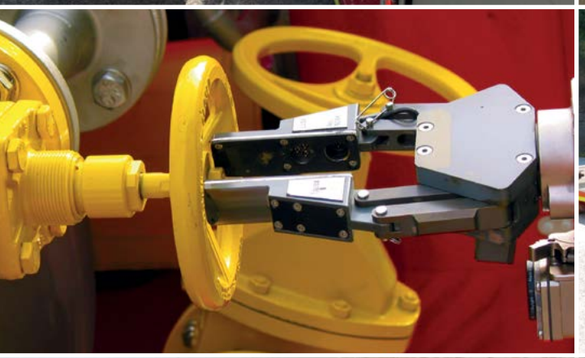
»Diese Jacke kann jeder anziehen und den Roboterarm mithilfe der eingebauten Sensorik dann intuitiv bewegen«, erläutert Brüggemann die Vorzüge dieser Bedienung, »man muss nicht mehr intensiv die Steuerung mit Joystick oder Bedienpult trainieren.« Zumal eine Steuerung der komplexen Abläufe, die eine einzige Armbewegung umfasst, ohnehin schwierig nachzuahmen sei, fügt er an. Das erklärte Ziel des Forscherteams ist die Entwicklung einer Fernsteuerung, die einfach und intuitiv zu benutzen ist, den Wechsel des Bedieners erlaubt, platzsparend, transportabel und ohne vorherige Schulung einsetzbar ist. Mit dieser Lösung darf dieses Ziel als erreicht gelten.

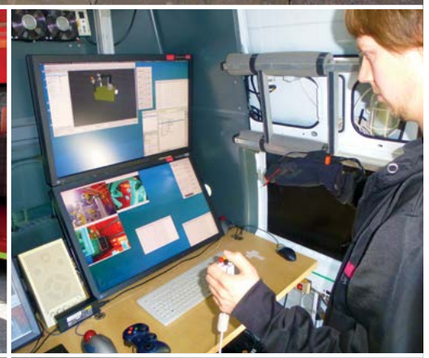
Der Aufbau des Roboterarms ähnelt dem eines menschlichen Arms, nur ein wenig »besser«: Ein Teleskopgelenk im Oberarm erlaubt das Erreichen einer Gesamtlänge von bis zu 170 Zentimetern. Der Arm ist um neunzig Grad verdreht im Vergleich zum menschlichen Arm, so dass das Schultergelenk statt in der vertikalen Ebene in der horizontalen Ebene dreht. Installiert auf einer Fahrplattform kann ein solcher Arm nun zu verschiedenen Einsätzen gesteuert werden und dort via Manipulation verschiedene Aufgaben ausführen: Gegenstände aufnehmen und bewegen, Bodenproben entnehmen, verdächtige Taschen öffnen – ein Helfer in vielen Situationen. Natürlich kann Brüggemann mittels des Metallarms zu Demonstrationszwecken auch gediegen eine Tasse Tee einschenken, ohne einen Tropfen zu verschütten. Da der Operateur im Einsatz vermutlich nicht unmittelbar neben dem Arm steht, helfen ihm drei Kameras, einen Überblick über Umfeld und die Bewegungen zu erhalten.

Die Versuche des Teams im abgelaufenen Jahr haben gezeigt, dass eine Steuerung durch Übertragen der menschlichen Bewegung auf den Manipulator mit Inertialsensoren möglich ist. Auch beim Roboter-Wettbewerb »EURATHLON« 2013 in Berchtesgaden konnte das FKIE-Team verschiedene Aufgaben mit dem Arm sehr gut meistern. Die Jacke ist dank der eingebauten Sensoren zu einem hochwertigen Einzelstück avanciert, die Steuerung ist einfach an- und abzulegen, transportabel und daher bestens für den mobilen Einsatz geeignet. In einigen Punkten erkennt das Team freilich noch Verbesserungspotenziale: So könnte der Überblick durch eine dreidimensionale Erfassung der Umgebung noch weiter verbessert werden. Aber die erreichten Erfolge zeigen: Mit der Steuerung kann das Team gute Fortschritte verzeichnen.

Etwas Übung benötigt man freilich weiterhin, möchte man mit dem eigenen über Kameras einen fremden Arm bewegen. Bei Demonstrationen kann es schon mal passieren, dass der Proband nicht gleich ein Erfolgserlebnis hat und sich dann mit charakteristischer Handbewegung ärgert. »Dann muss ich den Roboter rasch abschalten, damit nichts passiert«, hat Brüggemann dabei stets den Finger am »Aus«-Knopf. Zumal Ärgern zu einem Roboter auch gar nicht passt. Bis das soweit ist, wird es noch eine Weile dauern, da ist sich Brüggemann sicher: »Dass ein Roboter ein eigenes Bewusstsein entwickelt, das werde ich sicher nicht mehr erleben. Wenn das überhaupt jemals gelingen wird.«







»EURATHLON« STELLT AUSGEKLÜGELTE ROBOTER-SYSTEME AUF DIE PROBE

Die Forschungsgruppe Unbemannte Systeme (US) entwickelt am FKIE seit über 20 Jahren Mensch-Mehrroboter-Systeme. Beim durch das FKIE mitorganisierten »EURATHLON«-Wettbewerb im September 2013 in Berchtesgaden absolvierten Entwickler aus aller Welt verschiedene Parcours mit ihren Robotern und bewiesen: Moderne Robotersysteme sind immer flexibler einsetzbar.

Spuren von Rasen und Erdreich an den Reifen des Gefährts verraten es: Die Roboter in der Halle der Forschungsgruppe Unbemannte Systeme (US) auf dem FKIE-Gelände in Wachtberg-Werthhoven werden vom Entwicklerteam nicht auf Hochglanz poliert, sondern in der Natur erprobt und kontinuierlich weiterentwickelt. Ob mobil auf Rädern oder auf Ketten, ob mit Greifarm, einer Feuerlöschkanone oder Sensoren zum Beispiel für das Aufspüren chemischer Kampfstoffe ausgerüstet – das Arsenal in der kleinen Halle bietet bemerkenswert vielseitig einsetzbare Systeme. Bisweilen staunt man über einzelne Bausteine der Roboter: Eine Spielkonsolen-Kamera zum Beispiel, auch Joypads haben sich für die Fernlenkung offensichtlich bewährt. »Wir konzentrieren uns auf die Entwicklung der Software«, erklärt Forscher Bernd Brüggemann die mannigfache Auswahl an Hardware. Alles, was man selber bauen müsse, koste Aufwand: »Da gilt es, jede Hardware, die es bereits gibt, zu nutzen.« Für Demonstratoren spielt keine übergeordnete Rolle, aus welchen Einzelteilen sie zusammengebaut sind – wichtig ist, dass die Robotersysteme rasch in ihren Fähigkeiten und in ihrer Bedienbarkeit weiterentwickelt werden können. Daran arbeitet das FKIE-Team. Ohnehin biete die phänomenale Entwicklung der Unterhaltungselektronik nicht selten Gelegenheit, einen Demonstrator vergleichsweise umstandslos mit neuen Funktionen auszustatten.

Berchtesgaden im September 2013: Beim vom FKIE in Zusammenarbeit mit sieben Konsortialpartnern ausgerichteten Wettbewerb »EURATHLON« demonstrieren Entwickler, was ihre Roboter alles können – und wo (noch) die Grenzen liegen. Teilnehmen dürfen Robotik-Teams von Universitäten, Forschungsgruppen und der Industrie, die sich für den Wettbewerb an strikte Vorgaben und Spielregeln halten müssen. »Aufklärung und Erkundung« war beispielsweise eines von fünf Szenarien: Die Teams sollten zum Erreichen des Missionsziels in der Lage sein, mit ihrem Roboter ein unbekanntes Gebäude zu erkunden und möglichst umfassend zu kartografieren.

Seit über 20 Jahren entwickelt die Forschungsgruppe Unbemannte Systeme (US) flexibel einsetzbare Roboter. Die Bandbreite der Einsatzgebiete ist groß: »Wir haben immer irgendwo einen Anwender, sei es der Feuerwehrmann, der Soldat oder der Arbeiter in der Industrie«, erklärt Brüggemann. Aufklärung und Erkundung gehören längst zu klassischen Aufgaben für Roboter sowohl im militärischen Einsatz als auch bei zivilen Bergungsmissionen oder im Katastrophenschutz: Wo Einsatzkräfte auf unbekanntem Terrain oder z.B. in einsturzgefährdeten Gebäuden Leib und Leben riskieren, riskiert man mit einem Roboter lediglich Materialverlust. Entsprechend groß sind die Hoffnungen, die Institutionen wie Feuerwehr oder das Technische Hilfswerk seit jeher in die Entwicklung preiswerter, vielseitig einsatzbarer und leicht bedienbarer Robotersysteme für den Katastrophenschutz setzen. Brüggemann: »Der Einsatz von Robotern kann in vielen derer Einsatzbereiche große Vorteile bieten.« Herausforderungen sind für die Forscher Hindernisvermeidung und die Entwicklung neuer technischer Möglichkeiten. Dazu versammelt das FKIE Informatiker, die mit Algorithmen arbeiten können, ebenso wie Techniker oder Elektroniker, die Schaltungen herstellen können. Brüggemanns Spezialgebiet sind sogenannte »Mehrrobotersysteme«: Er forscht daran, Roboter zu befähigen, gemeinsam zu arbeiten. Zum Beispiel sollen sich bis zu sechs Roboter untereinander so koordinieren, dass sie mit ihren heterogenen Fähigkeiten gemeinsam eine Aufgabe erledigen können.

Vor große Probleme stellen einen Roboter gelegentlich schon scheinbar einfachste Aufgaben: Treppauf und treppab muss sich der Roboter in dem zu erkundenden Parcours beim EURATHLON-Wettbewerb bewegen können. Überdies darf es nicht zum Abbruch der Funkverbindung kommen. Das Gefährt, das Dr. Dirk Schulz mit seinem Team vom FKIE mitgebracht hat, ist mit Laserscannern ausgerüstet, die Hindernisse und Stufen erkennen. Dank abwerfbarer Sender kann auch über größere Distanz der Funkkontakt gehalten werden. Trotz vieler Hindernisse, von denen eine abwärtsführende Treppe eines der größeren ist, gelingt es mit dem FKIE-Roboter, das Gebäude gut zu kartografieren. »Der Wettbewerb hat gezeigt, dass unser System konkurrenzfähig ist«, resümiert Schulz zufrieden. Mit weiteren Robotersystemen hat das FKIE-Team auch an den Szenarien »Autonome Navigation« und »Mobile Manipulation« teilgenommen. Nicht nur dank der guten Leistungen mit den eigenen Systemen war der Wettbewerb ein Erfolg, über den sich neben Schulz auch Dr. Frank Schneider, Frank Höller, Achim Königs und Jochen Welle freuen.

Der Wettbewerb bietet den Entwicklern die Chance, einander über die Schulter zu schauen, sich auszutauschen und so neue Ideen zu entwickeln. Auch in der Öffentlichkeit weckte EURATHLON Interesse, unter anderem begleitete »Heise Online« den von der EU geförderten Wettbewerb über die fünf Tage mit gleich mehreren Artikeln. 2014 wird es eine Fortsetzung für EURATHLON geben: Im italienischen La Spezia werden dann Unterwasserfahrzeuge ihr Können beweisen.

Leitung (v.l.n.r.):
Dr. Jens Tölle
Telefon +49 228 9435-513
jens.toelle@fkie.fraunhofer.de

Prof. Dr. Michael Meier
Telefon +49 228 73-54249
michael.meier@fkie.fraunhofer.de

FORSCHUNGSGRUPPE CYBER SECURITY & DEFENSE

Ausrichtung der Abteilung

Gewährleistung von Schutz und Handlungsfähigkeit im Cyberspace ist Mission der Forschungsgruppe. Dabei wird IT-Sicherheit als integraler Bestandteil von Systemen und Prozessen interpretiert: neben präventiven Maßnahmen stehen Monitoring, Vorfallserkennung sowie Umsetzung geeigneter Gegenmaßnahmen im Fokus der Forschungstätigkeit. Parallel zur Weiterentwicklung von Schutzmaßnahmen gehört auch die Aufklärung und Analyse der Fähigkeiten möglicher Angreifer zu den Forschungsschwerpunkten.

Die Forschungskompetenzen und umfangreiche Erfahrungen aus Arbeiten mit und für BOS sowie die Herstellerunabhängigkeit ergeben ein spezifisches Leistungsspektrum: Zusätzlich zur Erforschung konkreter Sicherheitsfragestellungen sowie Entwicklung von Demonstratoren und Werkzeugen zu diversen Sicherheitsaspekten enthält dieses die Aufbereitung und Dokumentation des Entwicklungsstands bei Schutz- und Angreifertechniken. Der Aufbau und Betrieb von Test- und Analyselaboren gehört ebenso dazu wie das Testen von Komponenten und die objektive Begleitung bei der Entwicklung und Umsetzung von Sicherheitskonzepten. Auch Aufklärung von Sicherheitsvorfällen sowie Schulungen zur Vorfallsanalyse und zu Verwundbarkeitstests zählen zu den Aktivitäten.

Forschungs- / Entwicklungsbereiche

- Digitale Forensik und Bekämpfung von Schadsoftware
- Monitoring & Situational Awareness
- Ressourceneffiziente Kryptographie
- Sichere Kommunikationsarchitekturen

Schwerpunkte / Kernkompetenzen

- Sicherheitstests und Bewertung von Komponenten, Architekturen und Systemen (Penetrationstests, Fuzzing, Lasttests, Simulationen)
- Erkennung, Analyse und Abwehr von Schadsoftware und Botnetzen (Ködersysteme/ Honeypots, Reverse Engineering, Statische und dynamische Analyse, Botnetz-Monitoring und -Infiltration)
- Überwachung, Darstellung und Bewertung der Sicherheitslage (Intrusion Detection & Prevention, Threat Intelligence, Visualisierung, Pseudonymisierung von Monitoring-Daten)
- Absicherung von Kommunikations-Infrastrukturen (Gruppenkommunikation, Schlüsselmanagement, Sicherheit für Gebäudeautomation, Sicherheitsprotokolle und -dienste)

Projekte

- MonIKA, ACDC, BOTMAN®, QuaksBW, CYSPA, IDP/MIKE
- APT-Kompetenzzentrum, Security Test Center

Kooperatives verteiltes Sicherheitsmonitoring.

DATENSICHERHEIT: »DEN BLICK FÜR ALLE ERWEITERN«

Gemeinsam ist man stärker. Diesem Grundsatz folgend entwickelt die Abteilung Cyber Security & Defense (CS&D) am FKIE eine Software, mit der verschiedene Partner gemeinsam nach kriminellen Aktivitäten Ausschau halten können: Mit »MonIKA« werden Anomalien organisationsübergreifend erkannt, ohne dass der Datenschutz in Mitleidenschaft gezogen wird.

Konkurrenz belebt das Geschäft. Leider bisweilen auch dort, wo das nicht erwünscht ist: Die Konkurrenz zwischen Wettbewerbern erleichtert Cyberkriminellen ihr unerbetenes Werk; denn deren Aktivitäten könnten viel schneller enttarnt werden, hätten Firmen alle Datenströme im Blick – und nicht nur die eigenen. Das widerspricht jedoch nicht nur dem Konkurrenzgedanken von Unternehmen, sondern verstößt womöglich auch gegen geltendes Recht: Denn sollen beispielsweise sensible Kundendaten ausgetauscht werden, hat man rasch – und mit Recht – den Datenschutzbeauftragten in der Leitung, der unangenehme Fragen stellt.

Gleichwohl, die Chancen kooperativen Monitorings, so der Fachbegriff, und organisationsübergreifender Recherche nach kriminellem Verhalten im Netz hat man am FKIE erkannt. Um das Problem mit dem Datenschutz in den Griff zu bekommen, hat man seinerseits den Datenschutzbeauftragten angerufen – genau genommen das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein. Das Team um Prof. Dr. Michael Meier entwickelt daher federführend ein Konzept, mit dem verschiedene Partner ihre Daten sehr wohl sorgenfrei austauschen können, in Zusammenarbeit mit dem Landeszentrum sowie den weiteren Projektpartnern: der Airbus Defence and Space und dem Institut für Informations-, Telekommunikations- und Medienrecht der Universität Münster.

Das Projekt trägt den Namen »Monitoring durch Informationsfusion und Klassifikation zur Anomalieerkennung« – kurz klingt das hübscher: »MonIKA«. Matthias Wübbeling erklärt die Idee hinter MonIKA: »Ziel ist es, Anomalien im Netzverkehr zu erkennen, die man ohne organisationsübergreifende Kooperation nicht oder nicht so schnell erkennen könnte. Es geht darum, den Blick für alle Teilnehmer zu erweitern.« Und damit der Blick dabei auf das Wesentliche konzentriert bleibt – nämlich auf die Anomalien im Datenstrom, die auf kriminelle Umtriebe hinweisen, und nicht auf die sensiblen Daten des Wettbewerbers – werden sämtliche Daten vor dem Versand pseudonymisiert. Die Pseudonymisierung als elementarer Bestandteil des MonIKA-Projekts sorgt dafür, dass der verantwortliche Datenschutzbeauftragte keine Bedenken anmelden muss, ein Intrusion-Detection-Programm aber dennoch problemlos seine Arbeit mit den erhaltenen Daten verrichten kann.

Gestartet wurde das vom Bundesministerium für Bildung und Forschung (BMBF) geförderte Projekt 2012. Das vergangene Jahr konnte das Team nicht nur dazu nutzen, das Software-Framework und die Pseudonymisierungs-Komponente fertigzustellen. Auch drei Anwendungsbereiche konnten exemplarisch dargestellt und konkrete Verfahren erarbeitet und evaluiert werden: Zum einen für das Erkennen von Konflikten im Interdomain-Routing für das Border Gateway Protocol, einer für das Internet elementaren Infrastruktur. Zum anderen für das Aufspüren von Botnetzen, einer ernsten Bedrohung im Internet. Schließlich wurde in einer Simulation mit einem imaginären Autohersteller und dessen Kommunikation mit seinen Zulieferern das Konzept für den Anwendungsbereich des Enterprise-Monitoring auf Herz und Nieren getestet: »Wir haben den Versuch, das Zulieferer-System zu stören, simuliert«, erklärt Wübbeling. Sein zufriedenes Fazit: »Man sieht einfach mehr anhand aller Vorgänge, als wenn jeder allein draufschaut.« Konkrete Fälle können dann an die betroffenen Firmen zurückgegeben werden. Und nicht weniger wichtig für Wübbeling: »Die Lösung bietet genug Transparenz für den Datenschutzbeauftragten jedes beteiligten Unternehmens, der die Verantwortung für die Verarbeitung schutzwürdiger Daten hat!«

Auf Basis der gewonnen Erkenntnisse wird das Team seine Arbeit an MonIKA fortsetzen und weitere Anwendungsfälle umsetzen, in denen sensible Daten für kooperatives verteiltes Monitoring genutzt werden sollen. Wenn am Ende der Datenschutzbeauftragte staunt und grünes Licht gibt und die Cyberkriminellen sich wundern – dann haben das Cyber-Defense-Team und seine Partner alles richtig gemacht.

HINTER GITTERN AUF DER JAGD NACH CYBERKRIMINELLEN

Botnetze gehören zu den signifikanten Bedrohungen im Internet. Sie werden von Betreibern mit hoher krimineller Energie erstellt und richten erhebliche Schäden an. Mit den BOTMAN®-Aktivitäten entwickelt die Abteilung Cyber Security & Defense (CS&D) beim Fraunhofer FKIE systematisch Strategien, mit deren Hilfe Botnetze bekämpft werden können.

In einem Kellerraum des Instituts verbirgt sich so etwas wie die zentrale Kommandoeinheit im Kampf gegen Botnetze – zumindest sieht es wohl danach aus: »Wenn Journalisten kommen«, berichtet Dr. Elmar Gerhards-Padilla, »möchten die immer unbedingt den Käfig sehen.« Dabei gebe es dort nicht viel zu sehen, der Käfig sei allein aus Gründen des Einbruchschutzes vorhanden, erklärt der Cyber-Defense-Experte: Ein paar Server, ein Schreibtisch mit zwei Rechnern, das ganze hinter Gittern und unterlegt von einem Höllenlärm der Server. Auf dem Schreibtisch prangt symbolisch der rote Knopf, mit dessen Auslösen desinfiziert wird, was vorher infiziert wurde. Willkommen im BOTMAN®-Labor!

Die Journalisten, die sich zuletzt immer häufiger für die Arbeit der Abteilung Cyber Security & Defense (CS&D) des Fraunhofer FKIE interessieren, freuen sich an dieser etwas grimmig anmutenden Atmosphäre – dabei geschieht das nach Auffassung des Experten wirklich Interessante auf den handelsüblichen Servern: Auf ihnen läuft die vom Fraunhofer FKIE entwickelte Software, mit der das Team eine Analysestraße und ein Analyselabor betreibt. Ziel ist in beiden Fällen die Bekämpfung von Cyberkriminalität: Die Analysestraße ermöglicht es, aus verschlüsselter

Botkommunikation Daten zu extrahieren, die die Experten für nützlich halten, um sie später zur Bekämpfung der Botnetze einzusetzen. Im Analyselabor wiederum können in einer von anderen Netzwerken oder dem Internet abgeschotteten und gesicherten Umgebung Botnetze analysiert und Gegenmaßnahmen getestet werden. Gerhards-Padilla nennt es liebevoll »unsere kleine Spielwiese«.

Bundeskriminalamt schätzt den Schaden allein für 2012 auf 42,5 Millionen Euro

Im Internet gibt es für alles einen Preis: fremde Kreditkarten, Bankverbindungen, Versand von Spam-Mails, DDoS-Angriffe – auf einschlägigen Seiten bieten Kriminelle ihre zwielichtigen Dienste an und machen erst gar keinen Hehl aus ihrer Skrupellosigkeit. So wie der Betreiber einer Webseite, der erklärt, für Geld alles zu tun und anfügt: »I am no pussy!« Das Geschäft ist offenkundig lukrativ, das »Lagebild Cybercrime« des Bundeskriminalamtes schätzt den Gesamtschaden, der durch Internetkriminalität entstanden ist, allein für das Jahr 2012 auf 42,5 Millionen Euro. Andere Schätzungen reichen sogar bis zu dreistelligen Milliardenbeträgen. Bei solchen Summen ist es kaum verwunderlich, dass das Geschäft floriert. In Bezug auf Entschlossenheit und Fähigkeiten der Cyberkriminellen gibt sich Dr. Gerhards-Padilla keinen Illusionen hin: »Da haben wir es mit gut organisierten, professionellen Tätern zu tun!«

Im Labor tüftelt das Experten-Team des FKIE an Strategien gegen die Botnetze. Die Umsetzung der Strategien aber ist für die Forscher alleine nicht möglich, dazu benötigen sie Unterstützung: »Alleine können wir keine Maßnahmen umsetzen. Dabei arbeiten wir dann eng mit den Strafverfolgungsbehörden, dem Bundesamt für Sicherheit und Informationstechnik und der Staatsanwaltschaft zusammen«, erläutert Gerhards-Padilla. Leider sei es sehr schwierig die Drahtzieher zu erwischen, bedauert er: Meist enttarne man zunächst die niedrigeren Hierarchieebenen, zum Beispiel die sogenannten »Money mules«. Aber die Identifizierung der Täter macht nur einen Teil der Arbeit aus, Prävention und Schadensanalyse gehören ebenso zu den Zielen der BOTMAN®-Aktivitäten, mit denen das FKIE-Team besonders gefährliche Botnetze unter die Lupe nimmt, um Strategien zu ihrer Bekämpfung zu entwickeln.

Eigene Schattenwirtschaft in einem hierarchischen Netzwerk

Rund um Botnetze ist eine eigene Schattenwirtschaft entstanden, die Betreiber verschleiern ihre Identität hinter einem streng hierarchischen Netzwerk. Da gibt es den Programmierer, der die Software erstellt, den Betreiber, der das »Construction Kit« des Programmierers an Helfer verkauft, die ihrerseits wiederum weitere Helfer engagieren. Die Experten teilen ein Botnetz grob in drei Teile ein, die sehr komplex miteinander vernetzt sind: erstens die

infizierten Systeme, das sind einzelne Bots, zweitens die »Command & Control«-Infrastruktur und drittens den oder die Täter. Gerhards-Padilla: »Für eine effektive und nachhaltige Lösung muss man alle drei Teile adressieren.« Dabei geht er strategisch vor: »Wir müssen die Gewinne der Täter minimieren. Dafür müssen wir ihre Kosten erhöhen und Erträge minimieren.« Denn derzeit verdienen die zum Teil ungeheure Summen und haben dabei fast kein Risiko. Es gibt aber auch immer wieder Fälle, in denen es den FKIE-Experten in ihrem Analyselabor gelingt, effektive Maßnahmen gegen spezielle Botnetze zu entwickeln. In der realen Welt zum Einsatz kommen diese Maßnahmen dennoch selten, denn wer noch hinterherhinkt ist die Rechtsprechung: Derzeit darf noch niemand den »roten Knopf« drücken, um Botnetze abseits der Spielwiese im Institutskeller anzugreifen.

Inzwischen hat das FKIE-Team ein weiteres bestehendes Botnetz in den Fokus genommen, für das Analyse-Tools entwickelt werden. Schritt für Schritt kommen sie den Funktionsweisen jedes untersuchten Botnetzes auf die Spur und erarbeiten gründliche Gegenmaßnahmen. Bis auch das letzte Botnetz stillgelegt ist, wird Dr. Gerhards-Padilla noch vielen Kamerateams die »kleine Spielwiese« im Keller zeigen müssen – und auf das Recht warten, die gewonnen Erkenntnisse auch zum Einsatz bringen zu dürfen.

CYBER-DETEKTIVE IN DEN WÄNDEN

Nicht allein der Mobilität widmet sich der technische Fortschritt, längst sind auch Immobilien technisch bemerkenswert hochgerüstet. Das dient der Gebäudesicherheit oder ist allermindestens furchtbar praktisch, es bietet aber zugleich Angriffsfläche für Cyberangriffe. Am FKIE entwickelt ein Team kluge Strategien, mit denen auch fest in Wände installierte Gebäudeautomation aus digitaler Steinzeit nachträglich sicher gemacht werden kann.

Gebäudeautomation ist eine enorm praktische Sache: Niemand muss mehr eine Kurbel betätigen, wenn die Sonne blendet, oder die Heizung aufdrehen, wenn die Temperaturen frösteln machen. Ein Knopfdruck genügt – wenn nicht ohnehin Sensoren das Problem längst automatisch erkannt und behoben haben, bevor der Mensch dessen überhaupt gewahr werden kann. Klimatechnik, Aufzüge, Rolltreppen, Beleuchtung, Brandschutz: in modernen Gebäuden ist heutzutage nahezu nichts mehr nicht automatisiert. Ganz gleich, ob es sich ums schmucke Einfamilienhaus handelt oder den Großflughafen.

Doch der Nutzen hat auch eine Kehrseite: Wer in einem bis unter das Dach technisierten Haus sitzt, der ist auch jenseits klassischer Cyberangriffe aus dem Internet angreifbar. Überwachungskameras könnten angezapft und gegen den Hausbesitzer eingesetzt werden, Serveranlagen durch Manipulation der Belüftung lahmgelegt, Brandmeldeanlagen deaktiviert werden, bevor ein Feuer gelegt wird. Der Phantasie findiger Angreifer sind nahezu keine Grenzen gesetzt, um die Gebäudetechnik in ihrem boshaften Sinne einzusetzen. Dabei mag es in Bezug auf die Boshaftigkeit durchaus Abstufungen unter den Angreifern geben, manch potenzieller Angriff mutet geradezu drollig an:

So ist es z.B. denkbar, dass ein Unternehmen bei der Konkurrenz regelmäßig nachts Licht und Heizung im Keller eingeschaltet, um dessen Stromrechnung in die Höhe zu treiben. »Zahlreiche solcher Fälle werden in Fachkreisen bereits diskutiert«, weiß Dr. Steffen Wendzel.

Auch neue Systeme sind schlecht gesichert

Wendzel forscht am FKIE im Team von Professor Michael Meier in dem Bereich IT-Sicherheit in der Gebäudeautomation – und ihm ist es einerlei, wie böse ein Angreifer ist: Ihm ist daran gelegen, jeden Angriff zu unterbinden. »Es gibt immer mehr Features und Funktionen in der Gebäudeautomation, aber in der Praxis sind alle Systeme, auch die neuen, die bis heute eingebaut werden, schlecht gesichert«, erklärt er. Wendzel betont, dass sämtliche Technik, zwar »richtig gut gemacht ist« – doch fügt er gleich einschränkend hinzu: »Aus Sicht von Ingenieuren.« Als IT-Sicherheitsfachmann warnt er: »Man hat nie die Sicherheit dieser Systeme adressiert.« Das liege zum einen daran, dass die Hersteller »gar nicht das Know-how haben, um Sicherheit in ihren Geräten zu implementieren«. Eigentlich müsste dazu ein ganz neuer Protokoll-Standard erarbeitet werden, das jedoch sei bei der Vielfalt der Hersteller kaum durchführbar.

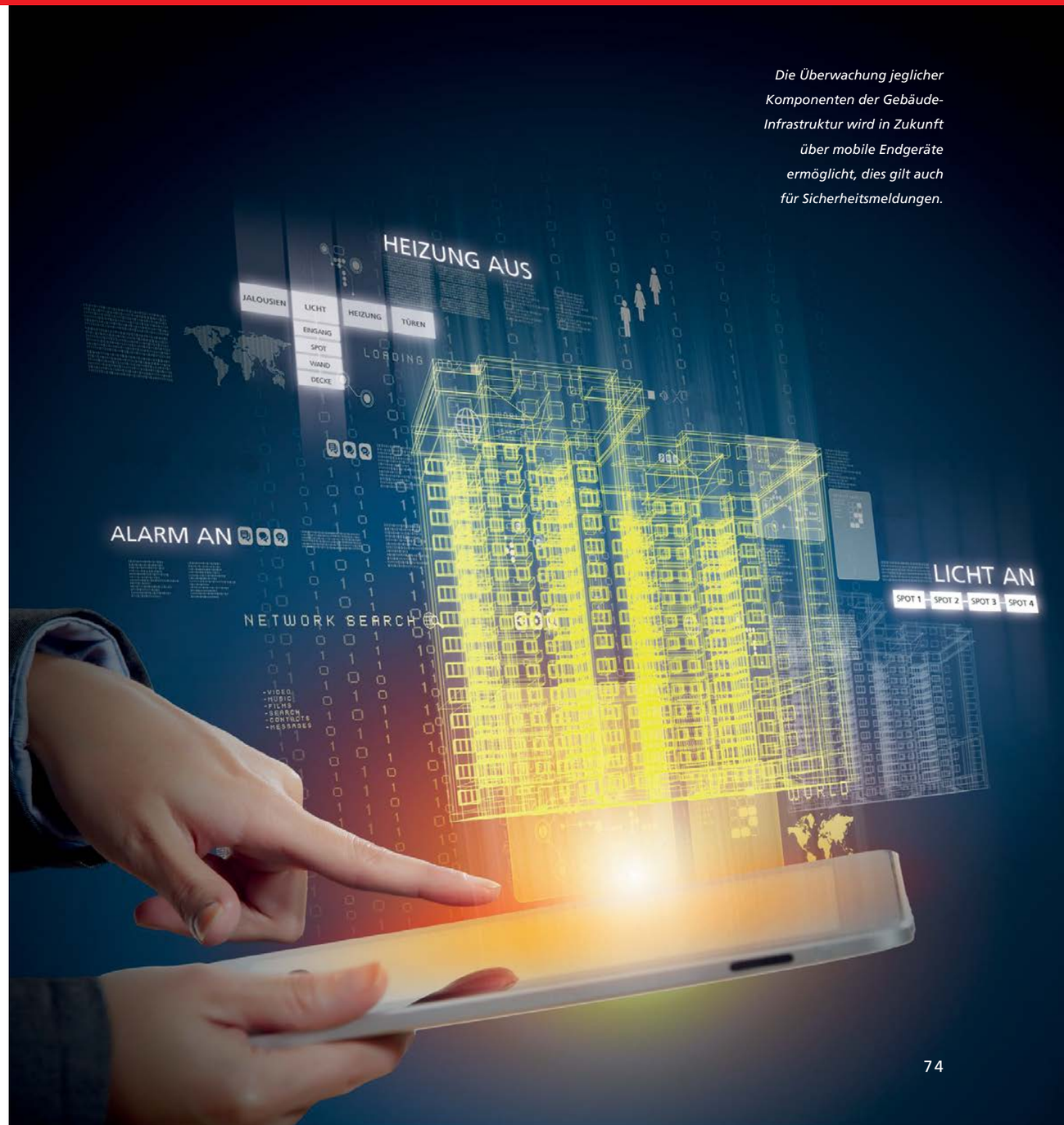
Und auch das Nachrüsten gestalte sich kompliziert: Einerseits sei vor allem ältere Technik von der Rechenleistung her gar nicht in der Lage, mit modernen kryptographischen Sicherheitsprogrammen gefüttert zu werden. Außerdem schaffen die Architekten nicht selten dauerhaft Fakten, wenn so ein Gerät tief in der Wand eingebaut ist: Nachrüsten unmöglich! Gleichwohl kann Technik, die ursprünglich unvernetzt eingebaut wurde, nachträglich mit dem Internet vernetzt worden sein. Das FKIE-Team verfolgt daher einen anderen Ansatz, um die Technik in den Wänden gegen Cyberangriffe zu sichern. Es klinkt sich in die Vernetzung der Geräte untereinander ein. Wendzel: »Wir schalten Analyzer und Normalizer zwischen die Subnetze und versuchen so, Angriffe zu erkennen und abzuwehren.«

»Analyzer« und »Normalizer« überwachen das »Internet der Dinge«

Ein »Analyzer« ist gewissermaßen ein Detektiv, der sämtliche Ereignisse, die auf den Weg zu den Systemen geschickt werden, genau unter die Lupe nimmt und auf Plausibilität prüft. Kommt ihm etwas eigenartig vor, geht der Vorfall unmittelbar an den Normalizer. Der blockiert das unplausible Ereignis im Datenverkehr entweder ganz oder wandelt es in ein plausibles um. »Das System verwirft oder verändert ungewöhnliche Ereignisse«, erklärt Wendzel, »so wird es Angreifern zumindest sehr schwer, wenn nicht unmöglich gemacht, Angriffe erfolgreich auszuführen.« Überdies wird jeder ungewöhnliche Vorgang protokolliert, sodass ein Gebäude-Operator sich das Problem später noch einmal ansehen und manuell bearbeiten kann. »Der Einfluss auf die Technik ist dabei minimal«, betont Wendzel.

Und das ist auch das Ziel: Der Aufwand für die Nachrüstung ist erheblich minimiert und die eigentliche Gebäudetechnik soll möglichst wenig beeinflusst werden. Das Team ist überzeugt davon, Gebäude-Netzwerken mit dieser zwischengeschalteten Plausibilitätsprüfung Sicherheit und zusätzliche Stabilität verleihen zu können. Mittelfristig werde mit dem Prinzip der Traffic-Normalisierung auch dem Vertrauen in das »Internet der Dinge« Vorschub geleistet. Denn Sicherheit und Vertrauen sind wichtig, wenn in Zukunft unser Energieverbrauch optimiert gesteuert wird oder Krankenhäuser sensible Patientendaten in technische Systeme einspeisen.

CYBER SECURITY & DEFENSE



Die Überwachung jeglicher Komponenten der Gebäude-Infrastruktur wird in Zukunft über mobile Endgeräte ermöglicht, dies gilt auch für Sicherheitsmeldungen.

VERANSTALTUNGEN 2013

Am Fraunhofer FKIE wird nicht nur hinter Zäunen still geforscht: Mit verschiedenen Veranstaltungen präsentiert sich das FKIE auch nach außen. 2013 etablierte sich der »Bonner Dialog für Cybersicherheit« in Zusammenarbeit mit der Deutschen Telekom. »Girls`Days« gab es gleich zwei: in Berlin und in Wachtberg-Werthhoven. Beim Girls´Day in Berlin erkundete auch Bundeskanzlerin Angela Merkel mit Schülerinnen die »Cyberspace City« des Fraunhofer FKIE.

BDCS Bonner Dialog für Cybersicherheit

mit der Deutschen Telekom

Cybersicherheit betrifft längst jeden, gleich, ob Staat, Industrie oder private Haushalte – und nicht erst seit den Enthüllungen über die Spionagemethoden internationaler Geheimdienste oder den jüngst bekannt gewordenen Industriespionagefällen. Deshalb lädt das Fraunhofer FKIE gemeinsam mit der Deutschen Telekom AG seit 2013 zu den Bonner Dialogen für Cybersicherheit ein, um einen Austausch zwischen Vertretern aus Wissenschaft, Wirtschaft, Behörden und interessierten Bürgern zu ermöglichen. Im April feierte die Veranstaltung in der Telekom-Zentrale mit Vorträgen zur aktuellen IT-Sicherheitslage und Verfahren in der Computerforensik Premiere. Bei der zweiten Veranstaltung im November sprach unter anderem der frühere Außenminister Dr. Klaus Kinkel darüber, wie sich der Cyberraum auf die Außenpolitik auswirkt. Initiatoren des Bonner Dialogs sind von Seiten des FKIE Prof. Dr. Michael Meier, zugleich Professor für Informatik IV an der Universität Bonn, und von Seiten der Deutschen Telekom Thomas Tschersich, Leiter der IT-Sicherheit. »Wir wollen damit die Diskussion über sinnvolle Maßnahmen zur Verbesserung der IT-Sicherheit fördern«, erklärt Meier das Ziel der Veranstaltungsreihe, die 2014 erfolgreich fortgesetzt wird.

Girls'Day – Mädchen-Zukunftstag

Girls'Day im Berliner Kanzleramt und in Wachtberg-Werthhoven

Bundeskanzlerin Angela Merkel höchstpersönlich gab den Startschuss zum bundesweiten Girls'Day 2013. Mit von der Partie im eigens im Berliner Kanzleramt aufgebauten Unternehmensparcours, das die Kanzlerin mit 24 Schülerinnen erkundete, war auch das Fraunhofer FKIE: In der »Cyberspace City« des FKIE tummelten sich zahllose Viren, vor den Toren der Stadt lauerte ein trojanisches Pferd – lauter Gefahren für die »Cyberspace City«, und die Mädchen konnten sich davon überzeugen, wie Leitstelle, Feuerwehr und Krankenhaus sämtliche Eindringlinge und ungebetenen Gäste unschädlich machten. Gezeigt hat das FKIE-Team auch, wie das Login einer Webseite angegriffen und gegen Angriffe geschützt werden kann. Ihr eigenes Geschick ausprobieren konnten die Mädchen, indem sie versuchten, einen chiffrierten Text zu entschlüsseln.

Auch das Fraunhofer FKIE in Wachtberg-Werthhoven öffnete anlässlich des Girls'Day, mit dem Mädchen mit Berufen aus dem Bereich der MINT-Fächer vertraut gemacht werden, Labore, Büros und Werkstätten für Mädchen ab Jahrgangsstufe 5, um ihnen spannende Einblicke in die vielfältigen Arbeitsfelder zu bieten. Bei der alljährlich stattfindenden Veranstaltung hatten im April wieder rund 60 Schülerinnen Gelegenheit, Berufsfelder aus dem technisch-naturwissenschaftlichen Bereich zu erkunden. »Mehr Frauen in die angewandte Forschung« lautet auch ein wichtiges Ziel der Fraunhofer-Gesellschaft: Bei den Fraunhofer-Instituten steigt der Anteil an Frauen am wissenschaftlichen Personal seit 2008 stetig an und lag 2013 bereits bei über 20 Prozent.

Technologie-Forum bot Einblicke in zahlreiche Forschungs-Bereiche

Ein Besuchstag ganz im Zeichen der Forschung am FKIE: Am 16. April präsentierte unser Institut beim Technologie-Forum einen Tag lang 150 Besuchern eine breite Auswahl an spannenden Exponaten aus allen Abteilungen des Instituts. Themen waren u.a. neue Methoden zur effizienten Breitbandaufklärung, Testbed für IT-Systeme im taktischen Umfeld, Ergonomische Interaktionsgestaltung für sicherheitskritische Mensch-Maschine-Systeme, Mobile Manipulationsaufgaben sowie das Advanced Cyber Defence Centre. Neben Fachvorträgen zu aktuellen Forschungsaktivitäten bestand auch die Gelegenheit, im Gespräch mit den Wissenschaftlern sich direkt zu informieren.

Fraunhofer FKIE bei der Cyber Defense Conference (CDC)

Über das facettenreiche und komplexe Themengebiet »Handlungsfähige Streitkräfte in einem sicheren IT-Umfeld« berieten mehr als 250 Teilnehmer bei der Cyber Defence Conference (CDC) im November in Bonn-Bad Godesberg, ausgerichtet von der Studiengesellschaft der deutschen Gesellschaft für Wehrtechnik mbH. Fachlich unterstützt wurde die Konferenz durch Vortragende des Fraunhofer FKIE. Institutsleiter Prof. Dr. Peter Martini, einer der fachlichen Leiter der Veranstaltung, betonte in seiner grundlegenden Einführung die Notwendigkeit, ein sicheres IT-Umfeld auszubauen, zu schützen und zu erhalten. Bei der Konferenz stand IT-Sicherheitsbewusstsein im Vordergrund. Das Credo lautete: »Niemand ist sicher« – ein Grund mehr für unser Institut, unsere Forschungen auf diesem Gebiet voranzutreiben.

EINGESPIELTER FORSCHUNGS-TRANSFER MIT DER UNI BONN

Von ihrer Zusammenarbeit profitieren die Universität Bonn und das Fraunhofer FKIE gegenseitig: Das gebündelte Know-how beider Institutionen beschleunigt den Weg von der Idee zur Marktreife. Mit Einrichtung des Kompetenzzentrums »Usable Security and Privacy« 2013 bauen das FKIE und das Institut für Informatik IV der Universität diese Kooperation im Bereich der »Cyber Security« aus.

Exzellenz in der Forschung und Zielstrebigkeit beim Forschungstransfer – die enge Kooperation zwischen der Rheinischen Friedrich-Wilhelms-Universität Bonn und dem Fraunhofer FKIE hat beide Ziele im Blick. Zu den bereits bestehenden Anknüpfungspunkten kam 2013 das Kompetenzzentrum »Usable Security and Privacy« hinzu: Nach dem etablierten Kompetenzzentrum Schadsoftware / Botnetze erhält auch dieser Bereich am Standort von Deutscher Telekom und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) akademische Anbindung. Mit **Professor Dr. Matthew Smith** und der **Juniorprofessorin Dr. Delphine Christin** konnte für das Kompetenzzentrum kürzlich gleich doppelt wissenschaftliche Exzellenz hinzugewonnen werden: Smith hat den Ruf der Universität Bonn zum Professor für Praktische Informatik am Institut für Informatik IV angenommen und ist zugleich Leiter der Arbeitsgruppe **»Usable Security and Privacy«**. Zuvor hielt er eine Professur für Distributed Computing & Security an der Leibniz-Universität Hannover. Er forscht und entwickelt auf dem Gebiet nutzerfreundlicher Lösungen für größere Sicherheit von IT-Systemen und hat unter anderem Sicherheits- und Benutzbarkeitsprobleme bei mobilen Systemen, beim Cloud Computing, dem Social Web und im Bereich »Big Data« untersucht. Christin hat den Ruf aus Bonn als Juniorprofessorin im Bereich der Praktischen Informatik angenommen, einen Schwerpunkt ihres Forschungsbereiches bildet die Suche nach Lösungen für Sicherheitsrisiken, die das »Internet der Dinge« von heute birgt. Bereits zuvor forschte sie auf dem Gebiet »Sichere Mobile Netze« an der Technischen Universität Darmstadt.

GESPRÄCH MIT
PROFESSOR
MATTHEW SMITH

Herr Professor Smith, Sascha Lobo erklärte das Internet jüngst für »kaputt«. Wo lässt sich ansetzen, um es zu reparieren?

SMITH: Ich müsste erstmal zurück fragen: Welche Stellen meint Lobo? Das Internet ist an relativ vielen Stellen »kaputt«. Mein Bereich ist die »Usable Security« und bezogen darauf muss ich sagen: seine Äußerung stimmt, aber wir arbeiten hart daran, es zu verbessern! Das Internet ist in seiner Grundstruktur schon sehr alt. Security-Maßnahmen mussten immer wieder nachgerüstet werden. Und von allen Arten von Programmcode ist Sicherheitscode nach meiner Einschätzung mit Abstand die komplexeste Art von Code. Denn während man bei normalem Programmcode relativ schnell feststellen kann, ob er das macht, was er soll, muss man bei Sicherheitscodes auf Unbekanntes testen. Das macht es natürlich deutlich schwieriger.

Nennen Sie uns ein Beispiel?

SMITH: Wenn Sie in Ihrem Browser auf eine Online-Banking-Seite gehen, dann färbt sich mit aller Wahrscheinlichkeit oben der Balken des Browsers grün, weil das signalisieren soll, dass es sicher sei. Dieser grüne Balken signalisiert, dass Sie diesem Zertifikat vertrauen und die Verbindung verschlüsselt ist. Doch ist dieses System grundlegend kaputt: Es gibt circa 650 verschiedene Institutionen, die solche **Zertifikate** *beliebig ausstellen dürfen und zwar flächendeckend.*

Worin besteht dann die Gefahr für den Nutzer?

SMITH: Dann passiert es, dass Sie auf diese Seite surfen und Ihnen dieser grüne Balken angezeigt wird, aber in Wahrheit findet gerade ein Angriff gegen Sie statt, ein so genannter ***»man-in-the-middle«-Angriff****. Das heißt, zwischen Ihnen und ihrem eigentlichen Kommunikationspartner sitzt jemand »in der Mitte« und fängt ihre Kommunikation ab. Eigentlich soll das Zertifikat Sie genau davor schützen. Wenn der Angreifer aber in der Lage ist, ein gültiges Zertifikat vorzulegen, dann kann er Sie angreifen und Sie als Nutzer bemerken einen solchen Angriff gar nicht. Der jüngst bekannt gewordene Heartbleed Bug macht die ganze Lage noch viel kritischer. Das ist die technische Seite des Problems – unter dem Aspekt von Benutzbarkeit sieht das Bild noch viel schlimmer aus.*

Aber an Warnmeldungen mangelt es doch nicht?

SMITH: Man gewöhnt sich an die Warnungen, wir sprechen von ***»habituation«****: Der Nutzer ist darauf trainiert, Warnungen wegzuklicken. In den wenigen Fällen, in denen dann tatsächlich ein Angriff stattfindet, ist die Wahrscheinlichkeit extrem hoch, dass der Nutzer wie gewohnt einfach die Warnung wegklickt und dann findet der Angriff statt, obwohl die Technik da gewesen wäre, ihn abzuwehren. Wir untersuchen beispielsweise das Verhalten der Nutzer. Bei den Warnungsstudien lautet das Ergebnis: Die Leute klicken da großflächig durch. Das heißt, die Warnungen sind nicht effektiv. Andere Untersuchungen haben gezeigt, dass auf etwa 15.000 falsche Warnungen – sogenannte* ***»false positives«*** *– gerade mal eine echte kommt. Da wird der Nutzer die eine echte Warnung einfach nicht sehen.*

Mit der Berufung von Smith und Christin setzen das Fraunhofer FKIE und die Universität Bonn den Ausbau der gemeinsamen Aktivitäten im Bereich der »Cyber Security« fort, nachdem bereits 2012 **Prof. Dr. Michael Meier** eine Professur am Institut für Informatik IV der Universität angetreten hat und zugleich mit Dr. Tölle gemeinsam die Forschungsgruppe Cyber Security & Defense leitet. Institutsleiter Professor Peter Martini, zugleich Leiter des Instituts für Informatik IV an der Universität Bonn, ist überzeugt, dass der Bereich »Usable Security and Privacy« nicht nur weiter ausgebaut, sondern neu geprägt werden wird. Der Anwender steht im Mittelpunkt und mit der Verbindung aus wissenschaftlicher Kompetenz und marktgerichteter Forschung nutzt das FKIE wertvolle Synergien für den Forschungstransfer.

Eine außerplanmäßige Professur verlieh die Universität Bonn **Dr. Frank Kurth** im Februar 2013: Sie würdigt damit seine wissenschaftlichen Leistungen in Forschung und Lehre auf dem Gebiet von Signalaufklärung und Sprachdetektion. Kurth ist seit 1997 am Institut für Informatik der Universität Bonn tätig und seit 2007 als Mitarbeiter am FKIE, wo er eine Arbeitsgruppe zu den Themen Funksignalerfassung und Effiziente Signaldetektion und Erschließung von Audiomassendaten leitet. Kurth schloss sein Informatikstudium 1997 in Bonn mit Diplom ab und promovierte bereits zwei Jahre später mit einer Arbeit, in der er das Problem von Generationseffekten in der Audiocodierung löste. 2004 habilitierte sich Kurth zum Thema Multimediaretrieval.

Wo setzt »Usable Security and Privacy« an?

SMITH: Wir waren mit die ersten, die die administrative Seite angeschaut und für eine Studie Interviews mit Administratoren geführt haben. Wir sind dabei auf zahlreiche Benutzbarkeitsprobleme beim Installieren von Zertifikaten gestoßen, aber auch auf viele Fehleinschätzungen seitens der Administratoren. Um auf den oberen Ebenen Benutzbarkeit sicherstellen zu können, wenden wir uns an die Entwickler, diejenigen, die Protokolle entwerfen, die Systeme bauen, unter anderem das Ökosystem der Zertifikate.

Was können die Entwickler aus Ihrer Sicht zukünftig besser machen?

SMITH: Das ist ganz oft ein Trade-off: Wir erhöhen die Benutzbarkeit und machen dafür Kompromisse bei der Sicherheit. Denn ***80 Prozent Sicherheit, die richtig und konsequent genutzt werden, sind besser, als 100 Prozent Sicherheit, die gar nicht genutzt werden****. Aber in diesem konkreten Fall können wir sagen, dass wir sowohl die Angriffsfläche verringern als auch die Benutzbarkeit erhöhen können. Zum Beispiel über das internationale Google-Projekt »Certificate Transparency«, an dem wir über die Universität beteiligt sind.*

Ist mangelnde Awareness seitens der Nutzer auch Teil des Problems?

SMITH: Awareness-Kampagnen sind aus meiner Sicht das Werkzeug der letzten Wahl. Denn immer dann, wenn es eine Awareness-Kampagne gibt, dann hat vorher irgendwo etwas auf technischer Ebene versagt. Unser Wunsch ist natürlich, dass die Technik intuitiv funktioniert und sich dem Menschen so anpasst, dass sie immer gut funktioniert. Denn der Mensch steht im Mittelpunkt – das System muss sich dem Menschen anpassen.

Wie bewerten Sie das Risiko durch die Smartphone-Kultur?

SMITH: Die Welt stellt auf Smartphones um – und wir installieren Apps, die gewisse Rechte haben. Zahlreiche Nutzerstudien meiner Kollegen und mir haben gezeigt: Nutzer setzen sich mit diesen Rechten kaum auseinander. Unsere Untersuchungen betrachten vor allem Rechte wie: »Darf auf die aktuelle Position zugreifen«, »Darf auf Adressbuch oder Fotos zugreifen«, »Darf auf Nachrichten zugreifen«, »Darf Informationen ins Internet versenden«. Wir fokussieren aber nicht nur das technische Recht, sondern die Person dahinter. Im Rahmen einer Studie haben wir z.B. festgestellt, dass die Versuchskandidaten durch persönliche Warnmeldungen privatsphärenbewusstere Entscheidungen bei der Installation von Apps getroffen haben.

Ist die Gratiskultur im Internet Teil des Problems?

SMITH: Hier gilt immer der Satz: »Wenn wir nicht dafür bezahlen, dann sind wir die Ware.« Und woran ich als Forscher dann natürlich interessiert bin ist: Wenn wir die Ware sind, dass wir als Nutzer zumindest abschätzen können, wie sehr wir die Ware sind. Was ich mir als Ziel gesetzt habe, ist, dass wir dem Menschen ermöglichen, zu sehen, was sie über sich preisgeben, und das besser kontrollieren zu können. Ich persönlich finde es nicht schlimm, dass Apps Rechte besitzen, aber es sollte eine bewusste Entscheidung des Nutzers zugrunde liegen, welche Rechte er vergibt.

An welchen aktuellen Themen arbeiten Sie derzeit noch im Bereich »Usable Security«?

SMITH: Aus dem Zertifikats-Thema lässt sich ein Grundlagenproblem extrahieren, nämlich das Schlüsselmanagement zum Verschlüsseln von Informationen. Das findet in ganz vielen Bereichen Anwendung. Wir betrachten auf grundlegender Ebene Schlüsselmanagement und Verschlüsselung als Konzept, anwenden lässt es sich dann auf Internetverschlüsselungen, E-Mail-Verschlüsselungen oder Sprachverschlüsselungen. Wir schauen auf allen Ebenen, wie wir Verschlüsselung sicherer und leichter anwendbar machen können. Am Herzen liegt uns auch das Thema Passwortsicherheit: Auf dem Gebiet verfolgen wir Ansätze, wie man Passwortsysteme stärker auf den Menschen zuschneiden kann, damit Passwörter leichter memorierbar und dennoch sicher werden.

Wie profitieren Sie von der bestehenden Kooperation zwischen dem Fraunhofer FKIE und der Universität Bonn?

SMITH: Wissenschaftliche Forschung verfolgt natürlich immer das Ziel, dass wir etwas in der Welt bewegen. Ein großer Vorteil besteht darin, dass wir unsere Ergebnisse deutlich schneller in die Wirklichkeit umsetzen und auf den Markt bringen können, wenn eine Institution wie Fraunhofer mit all ihren Ressourcen, Fähigkeiten und Kontakten dahintersteht. Außerdem wird die universitäre Forschung durch das Fraunhofer-Institut ganz unmittelbar mit den Problemen konfrontiert, die aktuelle Relevanz besitzen. Durch den Kontakt zum Institut bekommen wir die kritischen Probleme aus verschiedenen Bereichen überhaupt erst mit. Was ich auch sehr an unserer Situation hier in Bonn schätze: Wir haben hier ein ganz breites Spektrum an verschiedenen Leuten, die gemeinsam an den Problemen arbeiten. Die Kombinationen der vielen Sichtweisen und Fähigkeiten ist es, die uns einen ganzheitlichen Verteidigungsansatz ermöglichen wird.

Sie verfolgen demnach einen multiperspektivischen und interdisziplinären Ansatz?

SMITH: Das ist sicherlich ein Aspekt, der meine Forschungsgruppe von vielen anderen Forschungsgruppen unterscheidet: Wir arbeiten ein ganzes Stück interdisziplinärer, mit Psychologen, Soziologen, Juristen, Marktforschern. Denn die beste technische Lösung nutzt nichts, wenn sie nicht benutzbar ist. Die beste technische und benutzbare Lösung nutzt nichts, wenn es keinen Markt dafür gibt. Und die beste technische, benutzbare Lösung, für die es einen Markt gibt, nutzt nichts, wenn sie gegen geltendes Recht verstößt. Wir müssen immer alle Bereiche im Blick behalten, und das können wir natürlich nicht mit einem einzigen Team abdecken. Der Input aus den Bereichen Psychologie und Soziologie ist sehr wichtig für uns, aber auch aus den Bereichen Mediendesign oder Linguistik. Das ist eine der großen Freuden, dass wir hier mit so vielen interessanten und pfiffigen Leuten gemeinsam an einem so spannenden und weiten Themenfeld arbeiten.

Vielen Dank für das Gespräch!

PROMOTIONEN UND BERUFUNGEN

PROMOTIONEN

Govaers, F.
»*Enhanced Data Fusion in Communication Constrained Multi Sensor Applications*«, Promotion zum Dr. rer. nat. an der Mathematisch-Naturwissenschaftlichen Fakultät der Universität Bonn.

Wieneke, M.
»*Probabilistic Framework for Person Tracking and Classification in Security Assistance Systems*«, Promotion zum Dr. rer. nat. an der Mathematisch-Naturwissenschaftlichen Fakultät der Universität Bonn.

Damm, D.
»*A Digital Library Framework for Heterogenous Music Collections – from Document Acquisition to Cross-Model Interaction*«, Promotion zum Dr. rer. nat. an der Mathematisch-Naturwissenschaftlichen Fakultät der Universität Bonn.

Kleiber, M.
»*Konzeption und Entwicklung eines integrierten stereoskopischen Systems der Erweiterten und Virtuellen Realität für die Ferninstandsetzung*«, Promotion zum Dr.-Ing. an der Fakultät für Maschinenwesen der RWTH Aachen.

Schneider, F. E.
»*Formation Navigation and Relative Localisation of Multi-Robot Systems*«, Promotion zum Dr. rer. nat. an der Mathematisch-Naturwissenschaftlichen Fakultät der Universität Bonn.

Wendzel, S.
»*Novel Approaches for Network Covert Storage Channels*«, Promotion zum Dr. rer. nat. an der FernUniversität Hagen.

Pustina, L.
»*Dynamische Instruktionstrace-Komposition. Ein Verfahren zur realistischen Leistungsbewertung von Entwürfen für Smartphoneanwendungen*«, Promotion zum Dr. rer. nat. an der Mathematisch-Naturwissenschaftlichen Fakultät der Universität Bonn.

Schwarzer, S.
»*Automatisierte Erstellung parametrisierbarer Lastmodelle für die Performanzanalyse mobiler Geräte*«, Promotion zum Dr. rer. nat. an der Mathematisch-Naturwissenschaftlichen Fakultät der Universität Bonn.

BERUFUNGEN

Kurth, F.
Verleihung der Bezeichnung »*außerplanmäßiger Professor*« an der Mathematisch-Naturwissenschaftlichen Fakultät der Universität Bonn.

Smith, M.
Berufung zur W2-Professur für Praktische Informatik an der Mathematisch-Naturwissenschaftlichen Fakultät der Universität Bonn, Institut für Informatik IV; Leiter der Arbeitsgruppe »Usable Security and Privacy«.

Christin, D.
Berufung zur W1-Juniorprofessorin »*Praktische Informatik / Systemnahe Informatik, IT-Sicherheit*« an der Mathematisch-Naturwissenschaftlichen Fakultät der Universität Bonn, Institut für Informatik IV.

AUSGEWÄHLTE ABSCHLUSSARBEITEN

MASTER- UND MAGISTERARBEITEN

Bahlke, F.
»*Mismatched Filtering for GSM passive radar*« (Technische Universität Darmstadt).

Briant, R.
»*Gegenüberstellung von Nomenklaturen verschiedener semantischer Lexika*« (Universität Bonn).

Cornaggia-Urrigshardt, A.
»*Decomposition of 2D Feature Representations with Applications to Acoustic Event Detection*« (Universität Bonn).

Huang, J.
»*Network-based Classification of Application Behaviour*« (Universität Bonn).

Ivanova, A.
»*Robot-human interaction: Investigation of the uncanny valley using different designed robot appearances*« (RWTH Aachen).

Kirchhoff, J.
»*Quality of Sevice Routing with the Optimized Link State Routing Protocol in MANETs using Multiple Metrics*« (Universität Bonn).

Koch, J.
»*Identification of Functions by Symbolic Execution*« (Universität Bonn).

Lambertz, M.
»*Parallel File Carving for Fragmented JPEG Files*« (Universität Bonn).

Mohammadi, A.
»*Evaluation of the relevance of the source IP address for collected malware*« (Universität Bonn).

Narasimhappa, M.
»*Aerial Image Mosaicing*« (Universität Bonn).

Rauschen, D.
»*Echtzeit-Demonstrator einer skalierbaren SDR Wellenform für dynamischen Spektrumszugriff*« (Cologne University of Applied Science).

Reuße, S.
»*Resolving Pronominal Anaphora*« (Ruhr-Universität Bochum).

Rieber, J.
»*Speech Recognition as a Retrieval Problem*« (Universität Bonn).

Routabi, F.
»*Two SVM-based methods for the classification of airborne LiDAR data*« (Hochschule Bonn-Rhein-Sieg).

Sheikh, A.
»*Note Carrier: A Nomadic Application for Bi-Directional Class-Room Communication*« (Universität Bonn).

Tungathurthi, C.
»*Unsupervised structure discovery in speech data*« (B-IT/Universität Bonn/RWTH Aachen).

Varela, M.
»*Computer Aided Dislocation of a Passive Radar System Using Intelligent Information Service*« (Universität Bonn).

Wilden, S.
»*Entwicklung eines Funkempfängers für den SLF-Bereich*« (Hochschule Koblenz).

AUSGEWÄHLTE ABSCHLUSSARBEITEN

DIPLOMARBEITEN

Bartelt, T.
»Verbesserung der Skalierbarkeit der Nachbarschaftserkennung des Optimized Link State Routings in Mobilen Ad Hoc Netzwerken« (Universität Bonn).

Boehmsdorff, P.
»Echtzeitfähige Konzeption und Entwicklung eines Software-Baukastens für die Visualisierung von Trajektorien hochautomatisierter Fahrzeuge«
(Universität Koblenz-Landau).

Braß, C.
»Implementierung und Evaluation von Netzwerksicherheitsverfahren mit OpenFlow in Software-Defined-Networks« (Universität Bonn).

Bubb, I.
»Konzeptentwicklung eines Systems zur Unterstützung mobilitätseingeschränkter Personen unter Berücksichtigung ergonomischer Kriterien« (RWTH Aachen).

Dammann, J.
»Asynchronous Tracking of Peer-to-Peer Botnets« (Universität Bonn).

Domnich, R.
»Konzeption eines Simulationsmodells zur Leistungsbewertung von ARM-Systemen« (Universität Bonn).

Hermanns, L.
»Methodik zur Definition von Anlagenstandards bei hoher Produktvielfalt am Beispiel von Automatikstationen in der Montage von BMW-Baukastenmotoren« (RWTH Aachen).

Heupel, D.
»Automatisiertes Patchmanagement« (Universität Bonn).

Knödler, B.
»Strategies for Improving Range Resolution and Target Detection for GSM Passive Radar« (Universität Stuttgart).

Meimberg, V.
»Entwicklung einer Checkliste zur alters- und alternsgerechten Gestaltung von Arbeitssystemen in der Montage«
(RWTH Aachen).

Michaelis, M.
»State dependent IMM transition models«
(Universität Bonn).

Schmid, M.
»Simulativer Vergleich von Multicast Routing-Protokollen für Sprachkommunikation in MANETs« (Universität Bonn).

Wildt, J.
»Optisches Tracking mittels eines unbemannten Hubschraubers« (Universität Bonn).

BACHELORARBEITEN

Busch, O.
»Untersuchung zur Auslegung der Steuerelemente bei mobilen Geräten für die Interaktion während des Gehens«
(Hochschule Koblenz, Rhein-Ahr-Campus Remagen).

Danilova, A.
»Bewertung des IDP-MIKE Systems in Bezug auf Replay- und DoS-Angriffe« (Universität Bonn).

Flacke, J.
»Vergleich verschiedener Konzepte zur anwendungsspezifischen Komprimierung von Laser-Projektionsdaten im Netzwerk« (Universität Bonn).

Ihling, P.
»Telemedizin – Chancen und Anforderungen der medizinischen Versorgung älterer Menschen« (RWTH Aachen).

Mateo, G.
»Development of a module for qualification requirements of working persons in versatile production systems using the example of welding processes with cooperating robots«
(RWTH Aachen).

Mellouk, H.
»Konsistente UML-Klassendiagramme mithilfe einer formalen Diagrammbeschreibungssprache«
(Hochschule Bonn-Rhein-Sieg).

Meyer, L.
»Evaluierung eines verteilten Sensornetzes zur laufzeitbasierten Lokalisierung akustischer Ereignisse«
(Hochschule Koblenz, Rhein-Ahr-Campus Remagen).

Schirmer, L.
»Konzeption und Konstruktion eines ergonomisch angepassten Montagewagens für die RATIONAL Montage GmbH« (RWTH Aachen).

Simon, K.
»Messung der Leistungsfähigkeit einer Netzwerk-basierten Ansteuerung von Laser-Projektoren« (Universität Bonn).

vom Dorp, J.
»Forensische Untersuchung der Firefox-History durch Analyse gelöschter SQLite-WAL-Dateien« (Universität Bonn).

AUSGEWÄHLTE LEHRVERANSTALTUNGEN

SOMMERSEMESTER 2013

Dr. M. Adrat,
»*Forward Error Correction and Digital Modulation*«
(Vorlesung & Übung), RWTH Aachen.

B. Haarmann,
»*Grundlagen der Informationsextraktion*« (Seminar),
Ruhr-Universität Bochum.

Dr. S. Hawlitschka,
»*Technische Physik*« (Vorlesung & Übung),
Hochschule Bonn-Rhein-Sieg.

Dr. S. Hawlitschka,
»*Technische Physik*« (Praktikum),
Hochschule Bonn-Rhein-Sieg.

PD Dr. W. Koch / Dr. F. Govaers,
»*Advanced Methods and Applications of Sensor Data Fusion*«
(Vorlesung & Übung), Universität Bonn.

apl. Prof. Dr. F. Kurth,
»*Selected Topics in Signal Processing*« (Vorlesung & Übung),
Universität Bonn.

Prof. Dr. P. Martini,
»*Systemnahe Informatik*« (Vorlesung & Übung),
Universität Bonn.

Prof. Dr. P. Martini,
»Mobile Communication« (Vorlesung & Übung),
Universität Bonn.

Prof. Dr. P. Martini,
»*Selected Topics in Communication Management*«
(Seminar), Universität Bonn.

Prof. Dr. P. Martini,
»*Selected Topics in Malware Analysis and Computer / Network Security*« (Blockseminar), Universität Bonn.

Prof. Dr. P. Martini,
»*Rechnernetze / Communication Systems*« (Seminar),
Universität Bonn.

Prof. Dr. P. Martini,
»*Kommunikationssysteme*« (Projektgruppe),
Universität Bonn.

Prof. Dr. P. Martini,
»*Malware Boot Camp*« (Block-Projektgruppe),
Universität Bonn.

Prof. Dr. P. Martini / W. Moll,
»*Sicherheit in lokalen Netzen*« (Projektgruppe),
Universität Bonn.

Prof. Dr. P. Martini,
»*Communication and Communicating Devices*«
(Praktikum), Universität Bonn.

Prof. Dr. P. Martini,
»*Communication and Communicating Devices*«
(Blockpraktikum), Universität Bonn.

Prof. Dr. P. Martini,
»*Rechnernetze / Mobilkommunikation / Netzwerksicherheit*«
(Praktikum), Universität Bonn.

Prof. Dr. P. Martini,
»*High Performance Networking*« (Praktikum),
Universität Bonn.

Prof. Dr. P. Martini,
»*Malware Analysis*« (Blockpraktikum), Universität Bonn.

Prof. Dr. P. Martini,
»*Begleitseminar Bachelorarbeit*« (Seminar),
Universität Bonn.

Prof. Dr. P. Martini,
»*Begleitseminar Master Thesis*« (Seminar),
Universität Bonn.

Prof. Dr. P. Martini,
»*Diplomandenseminar*« (Seminar), Universität Bonn.

Prof. Dr. P. Martini,
»*Doktorandenseminar*« (Seminar), Universität Bonn.

Prof. Dr. M. Meier,
»*IT-Security*« (Praktikum), Universität Bonn.

Prof. Dr. M. Meier,
»*IT-Sicherheit*« (Projektgruppe), Universität Bonn.

Prof. Dr. M. Meier,
»*Selected Topics in IT-Security*« (Seminar),
Universität Bonn.

apl. Prof. Dr. U. Schade,
»*Language Processing*« (Vorlesung), Universität Bonn.

Prof. Dr.-Ing. C. Schlick,
»*Einführung in die Arbeitswissenschaft*«
(Vorlesung & Übung), RWTH Aachen.

Prof. Dr.-Ing. C. Schlick,
»*Ergonomie und Mensch-Maschine-Systeme*«
(Vorlesung & Übung), RWTH Aachen.

Prof. Dr.-Ing. C. Schlick,
»*Qualitäts- und Projektmanagement*«
(Vorlesung & Übung), RWTH Aachen.

Dr. D. Schulz, J. Welle / B. Gaspers,
»*Autonomous mobile Robots*« (Praktikum),
Universität Bonn.

Dr. J. Tölle / Prof. Dr. P. Martini,
»*Network Security*« (Vorlesung & Übung),
Universität Bonn.

Dr. M. Ulmke,
»*Measurement Techniques*« (Vorlesung & Praktikum),
Hochschule Bonn-Rhein-Sieg.

WINTERSEMESTER 2013/14

Dr. M. Esch,
»*High Performance Networking*« (Vorlesung & Übung),
Universität Bonn.

Dr. M. Esch / Prof. Dr. P. Martini,
»*Data Communication and Internet Technology*«
(Vorlesung & Übung), B-IT /
Universität Bonn / RWTH Aachen.

Prof. Dr. F. Flemisch,
»*Systemergonomie / Human-Systems-Integration*«
(Vorlesung & Übung), RWTH Aachen.

Dr. M. Gerz / Dr. M. Spielmann,
»*Verification of Complex Systems*« (Seminar),
Universität Bonn.

B. Haarmann, »*Grundlagen der Ontologie-Anwendung*«
(Seminar), Ruhr-Universität Bochum.

AUSGEWÄHLTE LEHRVERANSTALTUNGEN

WINTERSEMESTER 2013/14

PD Dr. W. Koch,
»*Introduction to Sensor Data Fusion – Methods and Applications*« (Vorlesung & Übung), Universität Bonn.

apl. Prof. Dr. F. Kurth,
»*Foundations of Audio Signal Processing*«
(Vorlesung & Übung), Universität Bonn.

Prof. Dr. P. Martini,
»*Kommunikation in Verteilten Systemen*«
(Vorlesung & Übung), Universität Bonn.

Prof. Dr. P. Martini,
»*Kommunikationssysteme*«
(Projektgruppe), Universität Bonn.

Prof. Dr. P. Martini,
»*Malware Boot Camp*« (Block-Projektgruppe),
Universität Bonn.

Prof. Dr. P. Martini,
»*Communication in Mobile / Distributed Systems*« (Praktikum), Universität Bonn.

Prof. Dr. P. Martini,
»*Begleitseminar Bachelorarbeit*« (Seminar),
Universität Bonn.

Prof. Dr. P. Martini,
»*Diplomandenseminar*« (Seminar), Universität Bonn.

Prof. Dr. P. Martini,
»*Doktorandenseminar*« (Seminar), Universität Bonn.

Prof. Dr. P. Martini,
»*Malware Analysis*« (Blockpraktikum), Universität Bonn.

Prof. Dr. M. Meier / Prof. Dr. P. Martini,
»*IT-Sicherheit*« (Projektgruppe), Universität Bonn.

Prof. Dr. M. Meier / Prof. Dr. P. Martini,
»*IT-Security*« (Praktikum), Universität Bonn.

Prof. Dr. M. Meier / Prof. Dr. P. Martini,
»*Selected Topics in IT-Security*« (Seminar), Universität Bonn.

Prof. Dr. M. Meier / Prof. Dr. P. Martini,
»*Selected Topics in Communication Management*«
(Seminar), Universität Bonn.

Prof. Dr. M. Meier / Prof. Dr. P. Martini,
»*Communication and Communicating Devices*« (Praktikum), Universität Bonn.

Prof. Dr. M. Meier / Prof. Dr. P. Martini,
»*Selected Topics in Malware Analysis and Computer / Network Security*« (Blockseminar), Universität Bonn.

Prof. Dr. M. Meier,
»*Systemnahe Programmierung*« (Vorlesung & Übung),
Universität Bonn.

Prof. Dr. M. Meier,
»*Diplomandenseminar*« (Seminar), Universität Bonn.

Prof. Dr. M. Meier,
»*Doktorandenseminar*« (Seminar), Universität Bonn.

Prof. Dr. M. Meier,
»*Begleitseminar Master Thesis*« (Seminar), Universität Bonn.

apl. Prof. Dr. U. Schade,
»*Language Acquisition*« (Vorlesung), Universität Bonn.

Prof. Dr.-Ing. C. Schlick,
»*Dynamische Unternehmensmodellierung und -simulation*«
(Vorlesung & Übung), RWTH Aachen.

Prof. Dr.-Ing. C. Schlick,
»*Industrial Engineering and Ergonomics*«
(Vorlesung & Übung), RWTH Aachen.

Prof. Dr.-Ing. C. Schlick,
»*Simulation of Discrete Event Systems*«
(Vorlesung & Übung), RWTH Aachen.

Dr. M. Ulmke,
»*Practical Physics*« (Vorlesung & Praktikum),
Hochschule Bonn-Rhein-Sieg.

Dr. S. Wendzel,
»*Tunnel und verdeckte Kanäle in Netzen*«
(Vorlesung), Hochschule Augsburg.

AUSGEWÄHLTE PUBLIKATIONEN

SDF

Verfasser	Titel
Bender, D.; Schikora, M.; Sturm, J. & Cremers, D.	***Graph-based bundle adjustment for INS-camera calibration.*** In: International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences. Vol. XL-1/W2, 2013 UAV-g2013. Rostock (4.–6. September 2013). (2013), pp. 39–44.
Biermann, J.; Hörling, P. & Snidaro, L.	***Experiences and Challenges in Automated Support for Intelligence in Asymmetric Operations.*** Journal of Advances in Information Fusion, 8 (2013) 2, pp. 1–18.
Brötje, M.	***Person tracking for WiFi based multistatic passive radar.*** In: FUSION 2013. 16th International Conference on Information Fusion. Istanbul (9–12 July 2013). IEEE Press (2013), pp. 280–287 (ISBN 978-605-86311-1-3).
Degen, C.; Govaers, F. & Koch, W.	***Emitter localization under multipath propagation using SMC-intensity filters.*** In: FUSION 2013. 16th International Conference on Information Fusion. Istanbul (9–12 July 2013). IEEE Press (2013), pp. 1–8 (ISBN 978-605-86311-1-3).
Govaers, F.; Charlish, A. & Koch, W.	***Covariance debiasing for the Distributed Kalman Filter.*** FUSION 2013. 16th International Conference on Information Fusion. Istanbul (9–12 July 2013). IEEE Press (2013), pp. 61–67 (ISBN 978-605-86311-1-3).
Koch, W.; Govaers, F. & Charlish, A.	***An Exact Solution to Track-to-Track Fusion using Accumulated State Densities.*** In: Sensor Data Fusion: Trends, Solutions, Applications (SDF), Workshop. Bonn (9–11 October 2013). IEEE Press (2013), 5 pp. (ISBN 978-1-4799-0777-9).
Mertens, M.; Kirubarajan T. & Koch, W.	***Minimum Detectable Velocity Evaluation of Bistatic Radar and Its Relevance for Ground Target Tracking.*** In: 14th International Radar Symposium. IRS 2013. Dresden (19–21 June 2013). Cuvillier Verl. (2013), pp. 343–354 (ISBN 978-1-4673-4821-8).
Mertens, M. & Ulmke, M.	***Ground target tracking with RCS estimation utilizing probability hypothesis density filters.*** In: FUSION 2013. 16th International Conference on Information Fusion. Istanbul (9–12 July 2013). IEEE Press (2013), pp. 2145–2152 (ISBN 978-605-86311-1-3).
Michaelis, M.; Govaers, F. & Koch, W.	***State Dependent Mode Transition Probabilities.*** In: Sensor Data Fusion: Trends, Solutions, Applications (SDF), Workshop. Bonn (9–11 October 2013). IEEE Press (2013), 6 pp. (ISBN 978-1-4799-0777-9).
Zemmari, R.;Knoedler, B. & Nickel, U.	***GSM passive coherent location: Improving range resolution by mismatched filterings.*** In: 2013 IEEE Radar Conference (RadarCon13). Ottawa (29 April-3 May 2013). IEEE Press (2013), 6 pp. (ISBN 978-1-4673-5792-0).

KOM

Verfasser	Titel
Adrat, M.; Osten, T.; Leduc, J.; Antweiler, M. & Elders-Boll, H.	***Can an Added Value be offered to SDR Operators in Scenarios where Interoperability to Legacy Radios is a Requirement?*** In: Proc. of SDR-WInnComm (Wireless Innovation Forum Conference), Washington (8–11 January 2013), SDR (2013), Session 6A.
Adrat, M.; Osten, T.; Leduc, J.; Antweiler, M. & Elders-Boll, H.	***On Considering Hierarchical Modulation in the Porting Process of Legacy Waveforms to Software Defined Radio.*** In: Analog Integrated Circuits and Signal Processing, 78 (2014) pp. 729–739.
Barz, C.; Niewiejska, J. & Rogge, H.	***NHDP and OLSRv2 for Community Networks. In: Wireless and Mobile Computing, Networking and Communications (WiMob).*** 2013 IEEE 9th International Conference. Lyon (7–9 October 2013). IEEE Press (2013), pp. 96–102 (ISSN 2160-4886).
Braem, B.; Blondia, C.; Barz, C.; Rogge, H. et al.	***A case for research with and on community networks.*** In: ACM SIGCOMM Computer Communication Review, 43 (2013) 3, pp. 68–73.
Cornaggia-Urrigshardt, A. & Kurth, F.	***Decompositions of 2D Feature Representations with Applications to Acoustic Event Detection.*** In: Horbach, M. (Hrsg.): INFORMATIK 2013: Informatik angepasst an Mensch, Organisation und Umwelt. Koblenz (16.–19. September 2013). GI Press (2013), S. 2853–2867. (GI-Edition – Lecture Notes in Informatics LNI; P-220) (ISBN 978-3-88579-614-5).
Dennisen, D.; Abut, F. ; Gläsel, D.; Bogenfeld, J.; Barz, C.; Aktas, I.; Wehrle, K. & Sevenich, P.	***Using Cross-Layer Design to detect Jamming Attacks in the CoNSIS Scenario.*** In: Military Communications and Information Systems Conference (MCC2013). St. Malo (7–9 October 2013). IEEE Press (2013), 7 pp. (ISBN 978-83-934848-8-1).
Fuchs, C. & Schneider, T.	***A Controlled Loss Transport Service for Sensor Data Transmission.*** In: Military Communications and Information Systems Conference (MCC2013). St. Malo (7–9 October 2013). IEEE Press (2013), 8 pp. (ISBN 978-83-934848-8-1).
Goetz, M.; et al.	***Performance Evaluation of Forwarding Protocols for the RACUN Network.*** In: WUWNet '13. Proceedings of the 8th ACM International Conference on Underwater Networks and Systems. Kaohsiung (11–13 November 2013). ACM Press (2013), Article 36 (ISBN 978-1-4503-2584-4).

AUSGEWÄHLTE PUBLIKATIONEN

KOM

Verfasser	Titel
Hanspach, M. & Keller, J.	***In Guards we trust: Security and Privacy in Operating Systems revisited.*** In: Social Computing (SocialCom). 2013 International Conference. Alexandria VA (8–14 September 2013). IEEE Press (2013), pp. 578–585 (ISBN 978-0-7695-5137-1).
Kempf, T.; Guenther, D.; Deidersen, U.; Yarmuch, A.; Ascheid, G.; Adrat, M. & Antweiler, M.	***Implementation of an ASIP based SDR Platform for MIMO OFDM Transceivers.*** In: Software Defined Radio Technical Conference. SDR-WinnComm Wireless Innovation Forum Conference. Washington: January 2013. SDR (2013).
Kurth, F.	***The Shift-ACF: Detecting Multiply Repeated Signal Components.*** In: Applications of Signal Processing to Audio and Acoustics (WASPAA), 2013 IEEE Workshop. New Paltz, NY (20–23 October 2013). IEEE Press (2013), 4 pp. (ISSN 1931-1168).
Liedtke, F.; Tschauner, M.; Adrat, M. & Antweiler, M.	***About Electronic Protection Measures (EPM) for an OFDM Wide Band Waveform.*** In: Military Communications and Information Systems Conference (MCC2013). St. Malo (7–9 October 2013). IEEE Press (2013), 8 pp. (ISBN 978-83-934848-8-1).
Singh, S.; Adrat, M. & Antweiler, M.	***About Business Models for future SDRs: Use Cases to tackle future Waveform Portability Issues during Procurement.*** In: Military Communications and Information Systems Conference (MCC2013). St. Malo (7–9 October 2013). IEEE Press (2013), 6 pp. (ISBN 978-83-934848-8-1).
v. Zeddelmann, D. & Urrigshardt, S.	***Ein Demonstrator zum Keyword-Spotting basierend auf gehörangepassten Audiomerkmalen.*** In: Horbach, M. (Hrsg.): INFORMATIK 2013: Informatik angepasst an Mensch, Organisation und Umwelt. Koblenz (16.–19. September 2013). GI Press (2013), S. 3026–3028 (GI-Edition – Lecture Notes in Informatics LNI ; P-220) (ISBN 978-3-88579-614-5)

ITF

Verfasser	Titel
Bense, H. & Haarmann, B.	***A Richer Textual and Graphical Notation for the Representation of Ontological Knowledge.*** In: ICMISE 2013 International Conference on Machine Intelligence and Systems Engineering, London (UK) (8–9 July 2013), (2013), 9 pp.
Bloebaum, T.H.; Jansen, N.; Johnsen, F.T.; Meiler, P.-P. & Owens, I.	***IST-118 SOA Recommendations for Disadvantaged Grids: Tactical SOA Profile, Metrics and the Demonstrator Development Spiral.*** In: Architecture Assessment for NEC. Papers presented at the Systems Concepts and Integration Panel (SCI) Symposium. Tallinn (Estonia) (13–14 May 2013) (AGARD STO-MP-SCI-254) (2013).

ITF

Verfasser	Titel
Coote, R.; Rein, K. & Schade, U.	***Search and Detection of Illegal Web Content. In: Future Security: 8th Security Research Conference.*** Berlin (17.-19. September 2013). Lauster, M. (Ed.). Berlin (u.a.): Fraunhofer Verl. (2013), S. 22–27. (ISBN 3-8396-0604-7).
Esch, M.; Geppert, H.; Gerz, M & Ota, D.	***Anforderungscontrolling für die einsatzbezogenen IT-Systeme der Bundeswehr.*** In: Mittler-Report Verlag, S. 91–94 (Wehrtechnischer Report 1/2013).
Gautreau, B.; Khimeche, L.; Martinet, J.; Remmersmann, T.; Pedersen, E.; Lillesoe, J.; De Reus, N.; Henderson, H. & Liberg, D.	***Lessons learned from NMSG-085 CIG Land Operation demonstration (Paper 13S-SIW-031).*** In: Simulation Interoperability Standards Organization -SISO- : Spring Simulation Interoperability Workshop, SIW 2013: San Diego (8–12 April 2013). Curran (2013), pp. 176–185 (ISBN 978-1-62748-019-2).
Jansen, N.; Krämer, D. & Spielmann, M.	***A model-based approach toward an executable middleware architecture for tactical C2IS.*** In: 18th NATO IST-115 Symposium on Architecture Definition & Evaluation, Toulouse. 13–14 May 2013. NATO, AGARD (2013), paper 14. (AGARD STO-MP-IST-115).
Jansen, N.; Krämer, D. & Spielmann, M.	***Testbed für IT-Systeme im taktischen Umfeld.*** In: Wehrtechnischer Report 8/2013: Simulation und Ausbildung. Mittler-Report Verl. (2013).
Johnsen, F.T.; Bloebaum, T.H.; Meiler, P.-P.; Owens, I.; Barz, C. & Jansen, N.	***IST-118 – SOA Recommendations for Disadvantaged Grids in the Tactical Domain.*** In: Proceedings of the 18th International Command and Control Research and Technology Symposium (ICCRTS2013). C2 in Underdeveloped, Degraded and Denied Operational Environments. Fairfax, VA (19–21 June 2013), 31 pp. (A928685).
Khayari, R.; Khimeche, L.; Lotz, H.B.; Gautreau, B.; Krosta, U.; Martinet, G. & Remmersmann, T.	***BML and MSDL enable to improve French and German Training with the tight coupling of national C2 and Simulation Systems.*** In: Fall Simulation Interoperability. Workshop 2013 Fall SIW. Orlando (16–20 September 2013). Curran Ass. (2013), pp. 230–237 (ISBN 978-1-62993-049-7).
Langerwisch, M.; Wittmann, T.; Thamke, S.; Remmersmann, T.; Tiderko, A. & Wagner, B.	***Heterogeneous Teams of Unmanned Ground and Aerial Robots for Reconnaissance and Surveillance – A Field Experiment.*** In: 11th Safety, Security, and Rescue Robotics (SSRR), 2013 IEEE International Symposium on Safety, Security and Rescue Robotics. Linköping (21–26 October 2013). IEEE Press (2013), 6 pp. (ISBN 978-1-4799-0879-0).

AUSGEWÄHLTE PUBLIKATIONEN

ITF

Verfasser	Titel
Noubours, S.; Pritzkau, A. & Schade, U.	***NLP as an essential ingredient of effective OSINT Frameworks.*** In: Military Communications and Information Systems Conference (MCC 2013). St. Malo (7–9 October 2013). IEEE Press (2013), 7 pp. (ISBN 978-83-934848-8-1).
Ohrem, F.; Haarmann, B. & Sikorski, L.	***EnArgus: A Knowledge-based Search Application for Energy Research Projects.*** In: International Journal of Computer, Information Science and Engineering. Vol. 7 (2013) 9, pp. 311–314.
Ota, D.; Esch, M.; Geppert, H. & Gerz, M.	***Architecture Assessment by Cross-Sectional Requirements.*** In: Architecture Assessment for NEC (SCI) Symposium. Tallinn (13–14 May 2013). NATO, AGARD (2013), paper (AGARD STO-MP-SCI-254).
Pritzkau, A.; Noubours, S.; Rein, K. & Schade U.	***Elaborated Search in the context of OSINT. In: Future Security: 8th Security Research Conference.*** Berlin (17.–19. September 2013). Lauster, M. (Ed.). Berlin (u.a.): Fraunhofer Verl. (2013), S. 55–62 (ISBN 3-8396-0604-7).
Pullen, J.M.; Corner, D.; Remmersmann, T. & Trautwein, I.	***Linked Heterogeneous BML Servers in NATO MSG-085. In: Fall Simulation Interoperability.*** In: IEEE ICC 2012. Workshop. 2013 Fall SIW. Orlando (16–20 September 2013). Curran Ass. (2013), S. 172–176 (ISBN 978-1-62993-049-7).
Pullen, J.M.; Corner, D.; Wittman, R.; Brook, A.; Gustavsson, P.; Schade, U. & Remmersmann, T.	***Multi-Schema and Multi-Server Advances for C2-Simulation Interoperation in MSG-085.*** In: M&S Support to Transitioning Forces and Emerged/Emerging Disruptive M&S Technologies. Sydney (17–18 October 2013). NATO, AGARD (2013), paper 4 (AGARD STO-MP-MSG-111).
Rein, K.	***Re-Thinking Standardization for Interagency Information Sharing.*** In: Akhgar, B. & Yates, S. (Eds.): Strategic Intelligence Management. Elsevier (2013), pp. 199–212 (ISBN 978-0-12-407191-9).
Rein, K. & Biermann, J.	***Your High-Level Information is My Low-Level Data: a New Look at Terminology for Multi-Level Fusion.*** In: FUSION 2013. 16th International Conference on Information Fusion. Istanbul (9–12 July 2013). IEEE Press (2013), pp. 412–417 (ISBN 978-605-86311-1-3).
Remmersmann, T.; Tiderko, A. & Schade, U.	***Interacting with Multi-Robot Systems using BML.*** In: Proceedings of the 18th International Command and Control Research and Technology Symposium (ICCRTS 2013). C2 in Underdeveloped, Degraded and Denied Operational Environments. Fairfax, VA (19–21 June 2013), 28 pp. (ADA588390). (ISBN 978-1-61839-719-5)
Remmersmann, T.; Tiderko, A.; Schade, U.; Langerwisch, M. & Thamke, S.	***Smart Control and Detection Feedback for a Multi-Robot Border Control System.*** In: Future Security: 8th Security Research Conference. Berlin (17.–19. September 2013). Lauster, M. (Ed.). Berlin (u.a.): Fraunhofer Verl. (2013), S. 239–247. (ISBN 3-8396-0604-7).

ITF

Verfasser	Titel
Savasan, H.; Caglayan, A.; Yildiz, F.; Schade, U.; Haarmann, B.; Mevassvik, O.M.; Sletten, G. & Heffner, K.	***Towards a Maritime Domain Extension to Coalition Battle Management Language: Initial Findings and Way Forward.*** In: 2013 Spring Simulation Interoperability Workshop. San Diego (April 2013). SIS (2013), 12 pp. (Paper 13S-SIW-022).
Schade, U.	***Informationsauswertung aus offenen Textquellen.*** In: AFCEA 2013. Fraunhofer FKIE. Behörden Spiegel-Gruppe, Sonderheft, April 2013, S. 56–57.
Sikorski, L.; Haarmann, B. & Ohrem, F.	***Implementing Ontology-supported Semantic Search Algorithms.*** In: ICISC2013. International Conference on Information and Computer Sciences. Zürich (30–31 July 2013). (2013), 4 pp.
Wunder, M. et al. (Eds.)	***Framework for Semantic Interoperability.*** PRE-RELEASE. NATO, AGARD, June 2013 (AGARD RTO-TR-IST-094) (2013).

EMS

Verfasser	Titel
Alexander, T. & Goldberg, S.	***Current and future directions for virtual simulation in operational platforms.*** In: Alexander, T.; Goldberg, S.: Improving Human Effectiveness Through Embedded Virtual Simulation. NATO, AGARD 2014, Chapter 7 (AGARD STO-TR-HFM-165) (2014) (ISBN 978-92-837-0181-1)
Conradi, J. & Alexander, T.	***Zum Einfluss der Immersion bei verschiedenartigen stereoskopischen Displays für Virtuelle Umgebungen.*** Zeitschrift für Arbeitswissenschaft 67 (2013) 2, S. 75–81 (ISSN 0340-2444).
Flemisch, F.; Bengler, B.; Bubb, H.; Winner, H. & Bruder, R.	***Beyond human-centered automation; Towards Cooperative Guidance and Control of Highly Automated Vehicles: H-Mode and Conduct-by-wire;*** Ergonomics 57 (2014) 3.
Flemisch, F.; Semling, C.; Heesen, M.; Meier, S.; Baltzer, M.; Krasni, A. & Schieben, A.	***Towards a balanced Human Systems Integration beyond time and space: Exploroscopes for a structured exploration of human-machine design spaces.*** In: NATO STO Symposium on Beyond Time and Space, Orlando: FL (14–16 October 2013). NATO, AGARD, 2013, p. 6.1-6.16 (NATO-STO-MP-HFM-231) (2013) (ISBN 978-92-837-0201-6).
Horoufchin, H.; Motz, F.; Mertens, A.; Bützler, J.; Bröhl, C.; Adolph, L. & Schlick, C. M.	***Mehrdimensionale Erfassung psychischer Beanspruchung für Operateure in Leitzentralen für die Fernbedienung und -überwachung technischer Anlagen,*** In: Gesellschaft für Arbeitswissenschaft (Hrsg.), Chancen durch Arbeits-, Produkt- und Systemgestaltung – Zukunftsfähigkeit für Produktions- und Dienstleistungsunternehmen, 59. Kongress der Gesellschaft für Arbeitswissenschaft. Dortmund: GfA-Press (2013), S. 723–726.

AUSGEWÄHLTE PUBLIKATIONEN

EMS

Verfasser	Titel
Kleiber, M.; Winkelholz, C.; Alexander, T.; Flemisch, F. & Schlick, C.M.	*Interacting and Cooperating Beyond Space: Tele-maintenance within a Virtual Visual Space.* In: NATO STO Symposium on Beyond Time and Space, Orlando, FL (14–16 October 2013). NATO, AGARD, 2013, pp. 7.1-7.14 (NATO-STO-MP-HFM-231) (ISBN 978-92-837-0201-6).
Özyurt, E.; Döring, B. & Flemisch, F.	*Simulation Based Development of a Cognitive Assistance System for Navy Ships.* In: Cognitive Methods in Situation Awareness and Decision Support (CogSIMA). 2013 IEEE International Multi-Disciplinary Conference. San Diego (25-28 February 2013). IEEE Press, pp. 22–29 (ISBN 978-1-4673-2437-3).
Theis, S.; Alexander, T. & Wille, M.	*Voruntersuchung zur Bewertung des sicheren und beanspruchungsoptimalen Einsatzes von Head-Mounted Displays.* Zeitschrift für Arbeitswissenschaft. 68 (2013) 3, S. 147–155.

US

Verfasser	Titel
Brüggemann, B.; Brunner, M. & Schulz, D.	*Asynchronous Flooding Planner for Multi-Robot Navigation.* In: Ferrier, J.L. et al. (Eds.): ICINCO 2013 – Proceedings of the 10th International Conference on Informatics in Control, Automation and Robotics, Vol. 2, Reykjavík (29–31 July 2013). SciTePress 2013, pp. 222-230 (ISBN 978-989-8565-71-6).
Brüggemann, B.; Gaspers, B.; Ciossek, A.; Pellenz, J. & Kroll, N.	*Comparison of Different Control Methods for Mobile Manipulation using Standardized Tests.* In: Safety, Security, and Rescue Robotics (SSRR). 2013 IEEE International Symposium. Linkoping (21–26 October 2013). IEEE Press (2013), 2 pp. (ISBN 978-1-4799-0879-0).
Brunner, M.; Brüggemann, B. & Schulz, D.	*Hierarchical Roadmap Approach to Rough Terrain Motion Planning.* In: ICAART 2013, 5th International Conference on Agents and Artificial Intelligence. Barcelona (15–18 February 2013). SciTePress (2013), Vol.1, pp. 35-46 (ISBN 978-989-8565-38-9).
Brunner, M.; Brüggemann, B. & Schulz, D.	*Hierarchical Rough Terrain Motion Planning using Optimal Sampling-Based Method.* In: Robotics and Automation (ICRA). 2013 IEEE International Conference. Karlsruhe (6–10 May 2013). IEEE Press, pp. 5539-5544 (ISBN 978-1-4673-5641-1).
Fiolka, T.; Stückler, J.; Klein, D.A.; Schulz, D. & Behnke, S.	*Distinctive 3D surface entropy features for place recognition.* In: Mobile Robots (ECMR). 2013 European Conference. Barcelona (25–27 September 2013). IEEE Press (2013), pp. 204-209.
Gaspers, B.; Welle, J. & Schulz, D.	*Opening Doors with a Mobile Manipulator without Force-Torque Feedback.* In: Safety, Security, and Rescue Robotics (SSRR). 2013 IEEE International Symposium. Linkoping (21–26 October 2013). IEEE Press (2013), 6 pp. (ISBN 978-1-4799-0879-0).

US

Verfasser	Titel
Königs, A. & Schulz, D.	*Fast Visual People Tracking using a Feature-Based People Detector and Thermal Imaging.* In: Safety, Security, and Rescue Robotics (SSRR). 2013 IEEE International Symposium. Linkoping (21–26 October 2013). IEEE Press (2013), 6 pp. (ISBN 978-1-4799-0879-0).
Königs, A. & Schulz, D. .	*Evaluation of the Fusion of Visible and Thermal Image Data for People Detection with a Trained People Detector.* In: Ferrier, J. L. et al. (Eds.): ICINCO 2013 – Proceedings of the 10th International Conference on Informatics in Control, Automation and Robotics, Vol. 2, Reykjavík (29–31 July 2013). SciTePress 2013, pp. 345-352 (ISBN 978-989-8565-71-6).

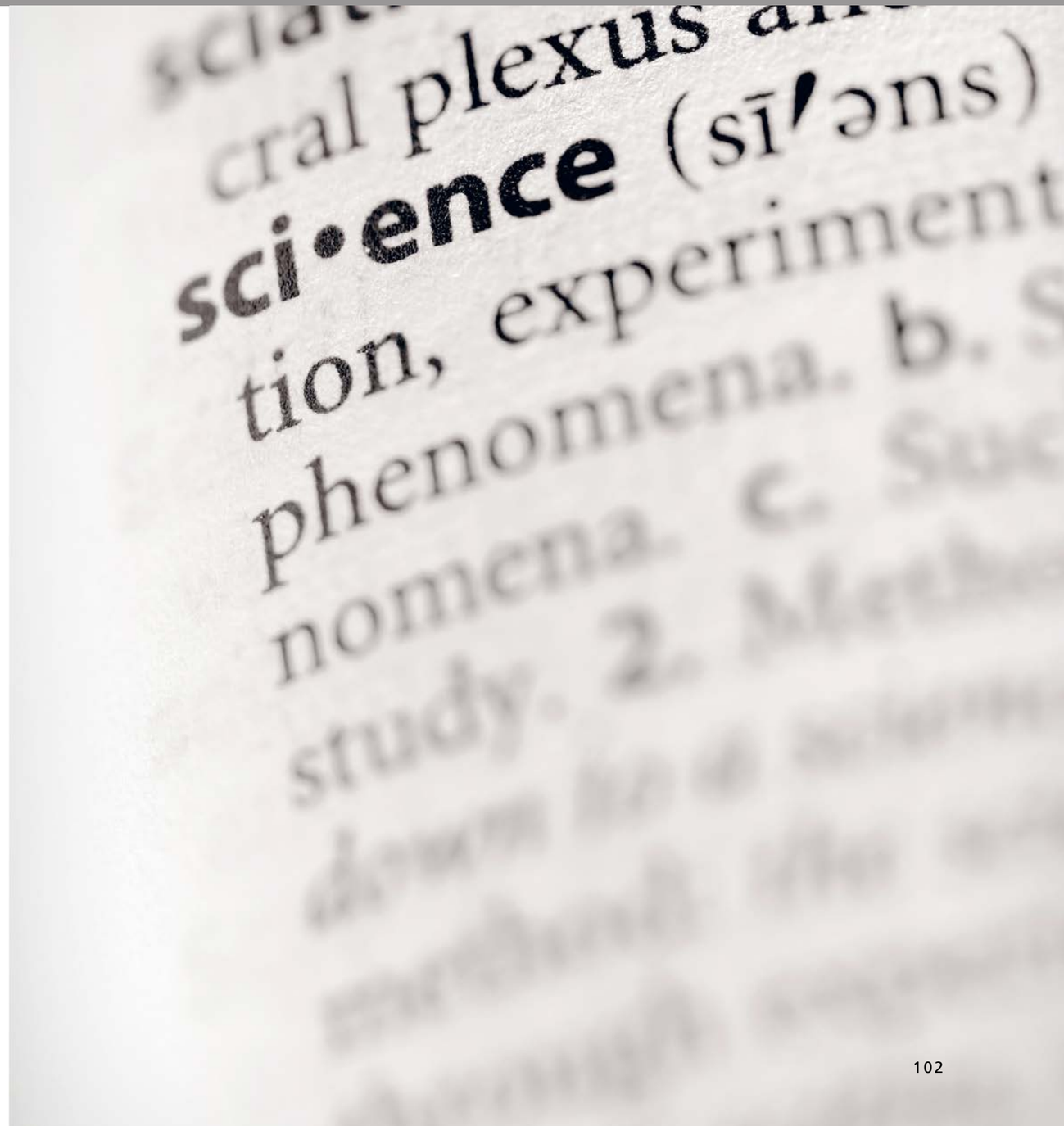
CD

Verfasser	Titel
Apel, M. & Meier, M.	*Automatic Generation of Generalizing Behavioral Signatures for Early Warning Systems.* In: Zeilinger, M. u.a. (Hrsg.): Advances in IT early warning. Stuttgart: Fraunhofer Verl. (2013), S. 102–112 (ISBN 978-3-8396-0474-8).
Barabosch, T.; Eschweiler, S.; Mohammad, Q.; Panteleit, D.; Plohmann, D. & Gerhards-Padilla, E.	*A General-purpose Laboratory for Large-scale Botnet Experiments.* In: Botconf 2013, 1st Botnet Fighting Conference. Nantes (5–6 December 2013).
Lambertz, M.; Uetz, R. & Gerhards-Padilla, E.	*File Carving for Fragmented JPEG Files.* In: Future Security: 8th Security Research Conference. Berlin (17–19 September 2013). Lauster, M. (Ed.). Berlin (u.a.): Fraunhofer Verl. (2013), S. 12–21. (ISBN 3-8396-0604-7).
Tiirmaa-Klaar, H.; Gassen, J.; Gerhards-Padilla, E. & Martini, P.	*Botnets.* London: Springer (2013), (Springer Briefs in Cybersecurity) (ISBN 978-1-4471-5215-6).

AUSGEWÄHLTE TÄTIGKEITEN IN GREMIEN

Wiss. Mitarbeiter/in	Arbeitsgruppe bzw. Gremium
Adrat, M.	NATO-STO IST-123 RSY-029 Cognitive Radio & Future Networks.
Adrat, M.	EDA Project Team on Software Defined Radio.
Adrat, M. & Couturier, S.	EDA Adhoc Working Group on Software Defined Radio Standardization Strategic Guidance.
Alexander, T.	DEU government expert (CGE) in EDA CapTech ESM4 »Human Factors and CBRN Protection«.
Alexander, T.	SDEU representative in NATO-STO-HFM-216 on Synthetic Environments for HSI Application, Assessment, and Improvement.
Alexander, T.	DEU representative in NATO STO-HFM-237 on Assessment of Intelligent Tutoring System Technologies and Opportunities.
Alexander, T.	Co-Chairman in NATO STO-NMSG-127 on Reference Architecture for Human Behaviour Modelling. Steering, Technical Program Committee Member und Session Chairman,
Antweiler, M.	Military Communication and Information Systems Conference, Saint-Malo, 7–9 October 2013.
Argumánez, H.E. & Liedtke, F.	NATO CaP1/CIS Line of Sight Communications Capability Team, Aufgabe der Gruppe: Entwicklung und Standardisierung neuer Wellenformen.
Aurisch, T.	NATO-STO IST Task Group on Selected Aspects of PCN, IST-103/RTG-043.
Barz, C. & Jansen N.	NATO-STO IST-RTG-118: Research Task Group on SOA recommendations for disadvantaged grids in the tactical domain.
Barz, C. & Jansen, N.	NATO IST-118/RTG-058 SOA recommendations for disadvantaged grids in the tactical domain.
Biermann, J.	STO IST-106/RTG-051 Research Task Group on Information Filtering and Multi Source Information Fusion RTGonIFMSIF.
Couturier, S.	NATO-STO IST-ET-074 Network Aspects of Cognitive Radio.
Couturier, S.	NATO-STO IST-104 RTG-050: Research Task Group on Cognitive Radio in NATO II.
Flemisch, F.	DEU representative in NATO-STO-HFM Human Factors/Medicine Panel, Leader der research area HSI.
Flemisch, F.	DEU non-government expert (nCGE) in EDA CapTech ESM 04 »Human Factors and CBRN Protection«.
Fuchs, S.; Kleiber, M. & Winkelholz C.	Technical Team Member, NATO RTO IST-110 »Visualization for Analysis«.
Gerz, M.; Kaster, J.; Schüller, H. & Huy, S.	Deutsche Arbeitsgruppe im Rahmen des internationalen Coalition Warrior Interoperability Exercise (CWIX 2013).
Ginzler, T.	NATO-STO IST-120 Future Internet Architectures for Military Networks.
Heesen, M.	NATO STO HFM-247 RTG on Human-Autonomy Teaming: Supporting Dynamically Adjustable Collaboration.
Hunke, S.	NATO STO IST-109-RTG-054 Research Group on Dynamic Wireless Network Cross-layer Security and Security Awareness in Coalition Environments.
Koch, W.	STO IST-106/RTG-051 Research Task Group on Information Filtering and Multi Source Information Fusion RTGonIFMSIF.
Lies, M.	Vorsitz der NATO US/EURO »Technical Support Group to N&S CaT«.
Pritzkau, A.	NATO IST-102 Intelligence Exploitation of Social Media.
Rein, K.	NATO IST-106 Research Task Group on Information Filtering and Multi-Source Information Fusion.
Rogge, H. & Baccelli, E. (INRIA)	Packet Sequence Number based directional ETT Metric for OLSRv2 IETF-draft (draft-rogge-baccelli-olsrv2-ett-metric-01, draft-rogge-baccelli-olsrv2-ett-metric-01), June 2013.
Schade, U.; Rein, K. & Remmersmann, T.	NATO RTO MSG-085 Standardization of C2-Simulation Interoperability.
Schneider, F.E.	IST-107-RTG-052 on Standards Promoting Interoperability for Coalition UGVs.
Sevenich, P.	NATO-STO IST-ET-69: Exploratory Team on Heterogeneous Networks.

Wiss. Mitarbeiter/in	Arbeitsgruppe bzw. Gremium
Steinmetz, P. & Diefenbach, A.	NATO-STO IST-ET-70: Exploratory Team on Tactical chat.
Tölle, J.	NATO-STO IST-108-RTG-053 Cyber Defence Situational Awareness (CDSA).
Tschauner, M.	NATO-STO IST-ET-068 LTE vs WiMAX for Military Applications.
Wendzel, S.	Koordinator der SRA group C »Trustworthy and Resilient Infrastructure and Services«, WG3 (Secure ICT research and innovation) announced in the Cybersecurity Strategy of the European Union.
Wendzel, S.	Arbeitskreis »kritische Infrastruktur«, SECMGT-Gruppe, GI FB Sicherheit.
Wolski, M.	NATO IST-078/RTG-036 Machine Translation for Coalition Operations.
Wunder M. & Tölle, J.	Organisation und Durchführung IST-Symposium IST-111/RSY-026 on Information Warfare and Assurance – Cyber Defence, Koblenz.
Wunder, M.	NATO Research & Technology Organisation, deutscher Vertreter im IST-Panel.
Wunder, M.	Chairman der NATO-Arbeitsgruppe IST-094/RTG-044 Framework for Semantic Interoperability.



FRAUNHOFER-GESELLSCHAFT

Forschen für die Praxis ist die zentrale Aufgabe der Fraunhofer-Gesellschaft. Die 1949 gegründete Forschungsorganisation betreibt anwendungsorientierte Forschung zum Nutzen der Wirtschaft und zum Vorteil der Gesellschaft. Vertragspartner und Auftraggeber sind Industrie- und Dienstleistungsunternehmen sowie die öffentliche Hand.

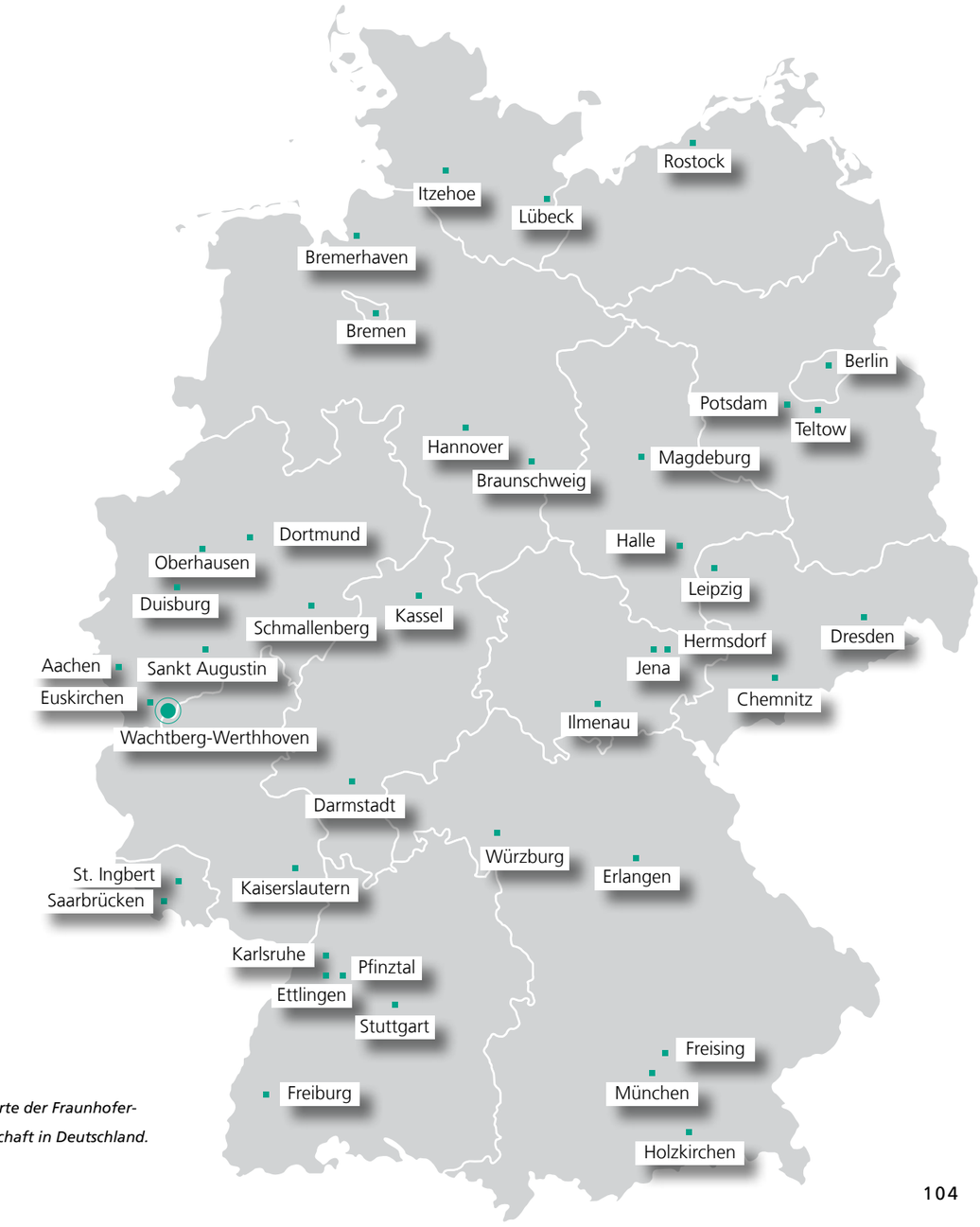
Die Fraunhofer-Gesellschaft betreibt in Deutschland derzeit 67 Institute und Forschungseinrichtungen. Rund 23 000 Mitarbeiterinnen und Mitarbeiter, überwiegend mit natur- oder ingenieurwissenschaftlicher Ausbildung, erarbeiten das jährliche Forschungsvolumen von 2 Milliarden Euro. Davon fallen rund 1,7 Milliarden Euro auf den Leistungsbereich Vertragsforschung. Über 70 Prozent dieses Leistungsbereichs erwirtschaftet die Fraunhofer-Gesellschaft mit Aufträgen aus der Industrie und mit öffentlich finanzierten Forschungsprojekten. Knapp 30 Prozent werden von Bund und Ländern als Grundfinanzierung beigesteuert, damit die Institute Problemlösungen entwickeln können, die erst in fünf oder zehn Jahren für Wirtschaft und Gesellschaft aktuell werden.

Internationale Kooperationen mit exzellenten Forschungspartnern und innovativen Unternehmen weltweit sorgen für einen direkten Zugang zu den wichtigsten gegenwärtigen und zukünftigen Wissenschafts- und Wirtschaftsräumen.

Mit ihrer klaren Ausrichtung auf die angewandte Forschung und ihrer Fokussierung auf zukunftsrelevante Schlüsseltechnologien spielt die Fraunhofer-Gesellschaft eine zentrale Rolle im Innovationsprozess Deutschlands und Europas. Die Wirkung der angewandten Forschung geht über den direkten Nutzen für die Kunden hinaus: Mit ihrer Forschungs- und Entwicklungsarbeit tragen die Fraunhofer-Institute zur Wettbewerbsfähigkeit der Region, Deutschlands und Europas bei. Sie fördern Innovationen, stärken die technologische Leistungsfähigkeit, verbessern die Akzeptanz moderner Technik und sorgen für Aus- und Weiterbildung des dringend benötigten wissenschaftlich-technischen Nachwuchses.

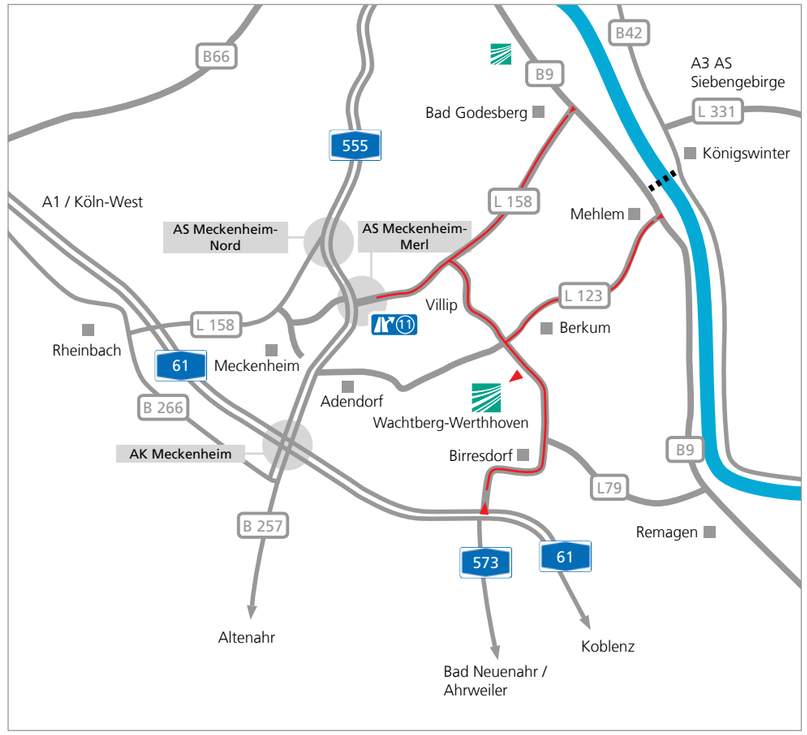
Ihren Mitarbeiterinnen und Mitarbeitern bietet die Fraunhofer-Gesellschaft die Möglichkeit zur fachlichen und persönlichen Entwicklung für anspruchsvolle Positionen in ihren Instituten, an Hochschulen, in Wirtschaft und Gesellschaft. Studierenden eröffnen sich aufgrund der praxisnahen Ausbildung und Erfahrung an Fraunhofer-Instituten hervorragende Einstiegs- und Entwicklungschancen in Unternehmen. Namensgeber der als gemeinnützig anerkannten Fraunhofer-Gesellschaft ist der Münchner Gelehrte Joseph von Fraunhofer (1787–1826). Er war als Forscher, Erfinder und Unternehmer gleichermaßen erfolgreich.

www.fraunhofer.de



Standorte der Fraunhofer-Gesellschaft in Deutschland.

SO FINDEN SIE UNS...



Hausanschrift:
Fraunhofer-Institut für
Kommunikation,
Informationsverarbeitung
und Ergonomie FKIE

Fraunhoferstraße 20
53343 Wachtberg-Werthhoven

Tel.: +49 (0)228 9435-103
Fax: +49 (0)228 9435-685

GPS-Koordinaten:
50°37.050´ N
07°07.917´ E

Anreise mit dem Auto
Über die Autobahn A565 zur Ausfahrt 11 »Meckenheim-Merl«, danach der Beschilderung folgen, für andere Routen siehe Karte.

Anreise mit der Bahn
Bis Remagen, Bad Godesberg oder Bonn Hbf., dann Taxi (ca. 10 km, 11 km bzw. 25 km) oder mit dem Bus.

Anreise mit dem Flugzeug
Bis Flughafen Köln/Bonn, anschließend mit Shuttle-Bus nach Bonn Hbf. Danach mit Bahn oder Taxi (ca. 25 km) oder mit dem Taxi direkt vom Flughafen (ca. 50 km).

Anreise mit dem Bus ab Bad Godesberg
Linien 856, 857 vom Bahnhof Bad Godesberg bis Berkum ZOB. Busse verkehren stündlich.

IMPRESSUM

HERAUSGEBER
Fraunhofer-Institut für Kommunikation,
Informationsverarbeitung und Ergonomie FKIE

Fraunhoferstraße 20
53343 Wachtberg-Werthhoven

Tel.: +49 (0)228 9435-103
Fax: +49 (0)228 9435-685

fkie@fkie.fraunhofer.de
www.fkie.fraunhofer.de

REDAKTION
Herrad Schmidt

TEXTE
Stefan Andres

LEKTORAT
Herrad Schmidt, Stefan Andres

LAYOUT, SATZ, FOTOCOMPOSING
Volker Kurzidim

FOTOGRAFIE
Uwe Bellhäuser / das bilderwerk

BILDQUELLEN
Bilder © Fraunhofer FKIE

AUSNAHMEN
Seite 10 - 11 Technologie-Hintergrund. 123 RF®
Seite 28 *Fotocomposing.* (istockphoto)
Seite 33 Business Graph. istockphoto
Seite 35 Laptop & Hands. istockphoto
Seite 46 Biometrics. istockphoto
Seite 58 - 59 Fotografie T. Zawadka & Fraunhofer FKIE
Seite 63 Internet Cyber Security. istockphoto
Seite 64 *Fotocomposing*. (istockphoto; 123 RF®)
Seite 61 Biometrics. istockphoto
Seite 73 Gebäudeautomatisierung. 123 RF®
Seite 74 Fotografie H.-J.Vollrath / Ahr-Foto
Seite 75 Girls´Day Bilder © Kompetenzzentrum Technik-Diversity-Chancengleichheit e.V.
Seite 76 Fotografie H.-J.Vollrath / Ahr-Foto

HINWEISE
BOTMAN® ist eine Marke der Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V., München.

EnArgus® ist eingetragene Wortmarke unter dem Amtsaktenzeichen DE 30 2012 001 033

Seite 70 - 71 Druck mit freundlicher Genehmigung durch Deutsche Post DHL Konzernkommunikation und Unternehmensverantwortung