Fraunhofer
FKIE

FRAUNHOFER-INSTITUT FÜR KOMMUNIKATION, INFORMATIONSVERARBEITUNG UND ERGONOMIE FKIE

JAHRESBERICHT 2014/15

JAHRESBERICHT
2014/15

VORWORT

Liebe Leserinnen und Leser,

wir bei FKIE verstehen uns als ein Fraunhofer-Institut »besonderer Art«, das im Kern seit über 50 Jahren und auch in Zukunft beständig und klar auf die Unterstützung hoheitlicher Aufgaben ausgerichtet ist. In diesem Kern, der unlängst noch deutlich gewachsen ist, sind wir auf Technik für Aufklärung und Führung konzentriert und haben herausragende Aktivitäten im Bereich Schutz etabliert.

Der Aufbau einer soliden zivilen Vertragsforschung war die Herausforderung, der wir uns darüber hinaus in den vergangenen Jahren überaus erfolgreich gestellt haben. Die Anschubfinanzierung, die uns über fünf Jahre diesen Aufbau der zivilen Vertragsforschung ermöglicht hat, endete im Dezember 2014. Wir sind stolz, dass die uneingeschränkt positive Evaluation uns den Weg geebnet hat, zukünftig für die zivilen Aktivitäten eine Grundfinanzierung aus Mitteln des Bundesministeriums für Bildung und Forschung zu erhalten. Seit Januar 2015 sind wir damit auch ein »ganz normales« Fraunhofer-Institut. Wir danken all jenen, die durch ihren persönlichen Einsatz dazu beigetragen haben, dass wir gemeinsam diesen Weg so vorbildlich gehen konnten. Dass FKIE nun als Paradebeispiel für eine gelungene Integration in die Fraunhofer-Gesellschaft genannt wird, freut uns natürlich besonders.

Ob nun »ganz normales« Fraunhofer-Institut oder eines »besonderer Art« – unser Credo »Wir arbeiten jeden Tag daran, die Welt sicherer zu machen« erstreckt sich auf vielgestaltige Herausforderungen unserer Gegenwart.

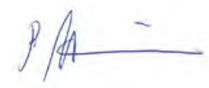
Das Thema IT-Sicherheitsforschung steht dabei für uns hoch im Kurs. »Wir können als Minister die wichtigen Fragen hinsichtlich der Zukunftsfähigkeit nur stellen«, erklärte Bundesbildungsministerin Prof. Dr. Johanna Wanka im Frühjahr 2014 bei der CeBIT in Hannover. Anlass war die Übergabe des Strategie- und Positionspapiers »Cyber-Sicherheit 2020« durch den Präsidenten der Fraunhofer-Gesellschaft unter Beteiligung des FKIE bei der weltgrößten Computermesse. Und die Ministerin fügte an: »Die Antworten müssen in einem so innovativen Bereich von Ihnen aus der Forschung kommen.« Dies ist ein Anspruch, dem sich unsere Forscher gerne stellen: Unsere IT-Experten greifen auf einen fundierten Erfahrungsschatz zurück, wenn es darum geht, den Werkzeugkasten von Kriminellen und auch Spionen im Cyberspace auszuforschen, und sie arbeiten tagtäglich daran, unser aller Systeme vor deren Methoden zu sichern. Der Schutz sowohl vor Cyberspionage als auch vor »Cyber Crime« ist unser erklärtes Ziel.

Ein zentraler Baustein der Forschungsarbeit an unserem Institut ist die enge Anbindung sowohl an die Universität Bonn als auch an die RWTH Aachen. Wir freuen uns, dass wir den damit einhergehenden Wissenstransfer weiter ausbauen konnten. Durch eine interne Umstrukturierung unserer Abteilungen wird universitären Aktivitäten nun noch mehr Platz eingeräumt. Der Bereich der Cyber Security zeigt beispielhaft, wie die enge akademische Anbindung unsere Forschung beflügelt. Überdies ist das FKIE in den Fraunhofer-Allianzen Embedded Systems, Big Data und Space bestens vernetzt.

Im Rahmen unseres Strategieprozesses mit Audit im November 2014 haben wir Wege vorgezeichnet, auf denen wir künftig die Kompetenzen unserer Abteilungen noch stärker und effektiver bündeln. Mit der Fortführung von öffentlichkeitsnahen Veranstaltungen wie dem Bonner Dialog für Cyber-Sicherheit, den wir gemeinsam mit der Deutschen Telekom begonnen und jetzt auch mit der Stadt Bonn zu einer regelmäßigen Diskussionsplattform ausgebaut haben, haben wir eine hohe Sichtbarkeit in unserer Region erreicht. Gerne helfen wir mit, die Stärke Bonns als »Hidden Champion für Datensicherheit und Datenschutz« auszubauen und nach außen zu kommunizieren. Einen sowohl sehr breiten als auch sehr tiefen Einblick in die Arbeit an unserem Institut hat unser Technologieforum im August 2014 geboten: Mit Vorträgen und Exponaten, vor allem aber mit viel Zeit für Austausch mit unseren Mitarbeitern hatten unsere Gäste Gelegenheit, Neues und bereits Bewährtes im Detail zu entdecken.

Die persönlichen Gespräche, zu denen wir Sie herzlich einladen, kann der Ihnen vorliegende Jahresbericht nicht ersetzen. Doch gibt er Ihnen einen Überblick über die aktuelle Arbeit an unserem Institut. Wir zeigen damit, auf welch vielfältige Weise unsere Mitarbeiter helfen, unterschiedlichste Risiken frühzeitig zu erkennen, zu minimieren und für uns alle beherrschbar zu machen. Unser Dank gilt unseren inzwischen mehr als 400 Mitarbeitern, deren Engagement unseren Erfolg ermöglicht.

Wir wünschen Ihnen eine interessante
und spannende Lektüre!



Prof. Dr. Peter Martini
Institutsleiter

Prof. Dr. Christopher Schlick
Stellv. Institutsleiter

INHALT

KURZPORTRAIT

Das Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE ist ein führendes Institut für anwendungsorientierte Forschung und praxisnahe Innovation in der Informations- und Kommunikationstechnologie. Es 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«. Wir unterstützen primär das Bundesministerium der Verteidigung und dessen nachgeordneten Bereich als strategischer Forschungspartner zu zentralen Fragestellungen der Themen Führung, Aufklärung, Unterstützung und Schutz. Weiterhin sind wir strategischer Partner des Bundesministeriums des Innern und dessen nachgeordneten Bereichs in Fragen der IT-Sicherheit und Kriminalitätsbekämpfung, wobei hier die Schwerpunkte beim Bundesamt für Sicherheit in der Informationstechnik und bei der Bundespolizei liegen.

Bei den zivilen Forschungsaktivitäten, mit denen das FKIE unmittelbar an seine traditionell wehrtechnisch ausgerichtete Forschung anschließt, liegt der Schwerpunkt auf Informations- und Telekommunikationstechnologie. Wir helfen Industriepartnern bei der Beherrschung existenzbedrohender Risiken und bringen unsere innovativen Lösungen in die Entwicklung neuer Produkte ein.

Die Ausrichtung des Instituts liegt auf der anwendungsorientierten 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 bis hin zu Assistenzsystemen für Entscheidungsträger. Entsprechend breit ist das Spektrum wissenschaftlicher Kompetenzen und domänenspezifischer Kenntnisse.

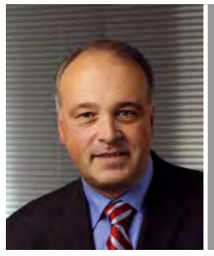
Die technische Umsetzung der Konzepte wird von Beginn an mitgedacht. Im Sinne anwendungsorientierter Wissenschaft werden am Institut erarbeitete Konzepte und Methoden experimentell verifiziert und mittels Prototypen evaluiert. Ein »proof of concept« gehört zum Standard. Wir legen besonderen Wert auf nutzerorientierte Lösungen, die wesentliche physiologische und kognitive Fähigkeiten, Fertigkeiten, das Wissen sowie die Erfahrung des Menschen einbeziehen.

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 FKIE ist Teil der Fraunhofer-Verbünde Verteidigungs- und Sicherheitsforschung VVS und IuK-Technologie. Außerdem ist das Institut in den Allianzen Embedded Systems, Big Data und Space bestens vernetzt. Das Fraunhofer FKIE betreibt Standorte in Wachtberg und Bonn und beschäftigt inzwischen mehr als 400 Mitarbeiterinnen und Mitarbeiter.

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.«

IHRE ANSPRECHPARTNER



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

VERWALTUNGSLEITERIN

Ursula Fuchs
Telefon 0228 9435-280
ursula.fuchs@fkie.fraunhofer.de

Abteilungsleiter
SENSORDATEN- UND INFORMATIONSFUSION

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

Abteilungsleiter
KOMMUNIKATIONSSYSTEME

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

Abteilungsleiter
INFORMATIONSTECHNIK FÜR FÜHRUNGSSYSTEME

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

Abteilungsleiter
HUMAN FACTORS

Dr. Thomas Alexander
Telefon 0228 9435-480
thomas.alexander@fkie.fraunhofer.de

Abteilungsleiterin
MENSCH-MASCHINE-SYSTEME

Annette Kaster
Telefon 0228 9435-492
annette.kaster@fkie.fraunhofer.de

Abteilungsleiter
SYSTEMERGONOMIE

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

Abteilungsleiter
CYBER ANALYSIS & DEFENSE

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

Abteilungsleiter
CYBER SECURITY

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

Abteilungsleiter
KOGNITIVE MOBILE SYSTEME

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

Abteilungsleiter
ZENTRALE INFORMATIONSTECHNIK

Wolfgang Moll
Telefon 0228 9435-483
wolfgang.moll@fkie.fraunhofer.de

KOMPETENZ, DIE VERBINDET

Interdisziplinarität öffnet den Blick für neue Anwendungsszenarien und ist nach unserem Verständnis zugleich ein Schlüssel zu überzeugenden Lösungsansätzen. Das Fraunhofer FKIE verfügt über Fachkompetenzen auf höchstem wissenschaftlichem Niveau sowie einzigartige Domänenkompetenzen.

Die fachliche Expertise unserer wissenschaftlichen Abteilungen und die abteilungsübergreifende Zusammenarbeit ermöglichen Exzellenz im Detail mit dem Blick auf das Ganze. Bei der Bearbeitung von Projekten können wir grundsätzlich auf alle erforderlichen Kompetenzbausteine zurückgreifen. Im Zuge der strategischen Weiterentwicklung im vergangenen Jahr hat sich das FKIE organisatorisch neu aufgestellt. Das Institut umfasst nunmehr neun Fachabteilungen, von denen drei eine besondere Nähe zu Hochschulen (der RWTH Aachen und der Universität Bonn) aufweisen.

Diese neuen Abteilungen bilden den »FKIE-Kosmos«:

- Sensordaten- und Informationsfusion (SDF)
- Kommunikationssysteme (KOM)
- Informationstechnik für Führungssysteme (ITF)
- Human Factors (HF)
- Mensch-Maschine-Systeme (MMS)
- Systemergonomie (SE)
- Cyber Analysis & Defense (CA&D)
- Cyber Security (CS)
- Kognitive Mobile Systeme (CMS)

Darüber hinaus gibt es eine im Aufbau befindliche Projektgruppe an der Universität Bonn, die sich im Themenfeld Informationstechnologie mit dem Schwerpunkt

- Usable Security und Privacy (USP)

beschäftigt.

Ordnet man die einzelnen Abteilungen den drei grundlegenden Forschungsbereichen des FKIE zu – also den Themen Kommunikation, Informationsverarbeitung und Ergonomie – ergibt sich ein Bild, das diese neun Abteilungen innerhalb des FKIE-Kosmos im Verhältnis zueinander und in Bezug zu den Forschungsbereichen positioniert. Die Größe der Hexagone verdeutlicht die Abteilungsgröße. Gleichzeitig wird ersichtlich, dass aus der Verknüpfung der verschiedenen abteilungsspezifischen Kompetenzen sehr fruchtbare Kooperationen entstehen.

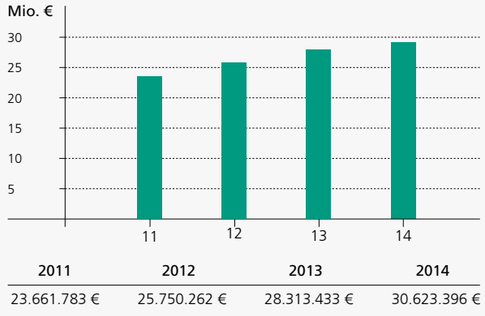
Das Schaubild des »FKIE-Kosmos« hilft dabei, Arbeitsschwerpunkte und potenziell komplementäre Ergänzungen der Fachabteilungen zu erkennen. In dem vorliegenden Jahresbericht stellen wir Ihnen einige Beispiele solcher abteilungsübergreifenden Projekte vor. Ist zum Beispiel die Verbesserung der Sicherheit im Flugverkehr das angestrebte Ziel, kann es mit Blick auf die Komplexität der Problemstellung erforderlich sein, Kompetenzen aus mehreren Abteilungen heranzuziehen.

Die neun Abteilungen am FKIE vereinen vielfältige Kompetenzen, mit denen Antworten auf die Herausforderungen einer stetig komplexer werdenden Welt gegeben werden können, und aus denen sich insgesamt ein differenziertes Portfolio ergibt, das systematisch genutzt und strategisch weiterentwickelt wird. In diesem Jahresbericht erfahren Sie mehr über die Forschungsschwerpunkte der einzelnen Abteilungen, die sich zu einer vernetzten Problemlösungskompetenz des Fraunhofer FKIE zusammenfügen.

ENTWICKLUNG IN ZAHLEN

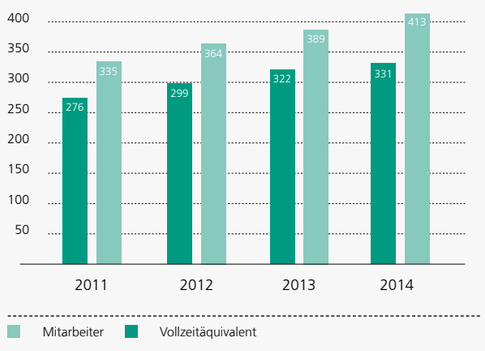
Wachstum in allen Bereichen

Budgetentwicklung 2011 - 2014



2011	2012	2013	2014
23.661.783 €	25.750.262 €	28.313.433 €	30.623.396 €

Mitarbeiterentwicklung 2011 - 2014 (*)



(*) Stichtag: 01. Dezember

Das Fraunhofer FKIE ist weiterhin auf Wachstumskurs: Mit einem Gesamtbudget in Höhe von 30,6 Millionen Euro konnte 2014 erstmals die 30-Millionen-Grenze durchbrochen werden Im Vergleich zum Vorjahr ist das Budget um 8,1 Prozent gestiegen, im Vergleich zum Jahr 2010 um 51 Prozent.

Auf zuverlässig stabilem Niveau blieb dabei die institutionelle Förderung durch unseren wichtigsten Zuwendungsgeber, das Bundesministerium der Verteidigung. Daneben bearbeitet FKIE eine Vielzahl von Projekten und Aufträgen, in deren Rahmen das Institut eng mit Zuwendungs- und Auftraggebern der öffentlichen Hand und verschiedener Industriezweige zusammenarbeitet.

Im letzten Jahr der Anschubfinanzierung konnte das Institut die Wirtschaftserträge im Vergleich zum Vorjahr erneut steigern und erreichte damit den bislang höchsten Wert seit der Fusion des früheren Trägers FGAN mit der Fraunhofer-Gesellschaft. Die erzielten Wirtschaftserträge machten im Bereich der zivilen Vertragsforschung einen Anteil von ca. 35 Prozent aus.

Ungebrochen auf Expansionskurs befindet sich auch die Mitarbeiterentwicklung am Fraunhofer FKIE: 413 Mitarbeiterinnen und Mitarbeiter beschäftigte das Institut im Dezember 2014 (2013: 389). Fast 70 Prozent von ihnen sind als Wissenschaftler, Ingenieure oder Techniker in den Forschungsabteilungen tätig. Darüber hinaus leisten auch die administrativen Bereiche einen wichtigen Beitrag zum Erfolg des Instituts.

FÜHRUNGSLEITBILD UND FÜHRUNGSAKADEMIE

Fraunhofer-Institute weisen eine vergleichsweise hohe Personaldynamik auf. Junge Wissenschaftler bringen ihre Kenntnisse für einige Jahre in die anwendungsorientierte Forschung ein und können parallel dazu promovieren. In vielen Fällen verfolgen sie im Anschluss daran eine akademische oder industrielle Karriere. Dies ist ein Teil des Selbstverständnisses von Fraunhofer. Von uns als Institut verlangt das eine kontinuierliche und zielgerichtete Personalarbeit.

Zudem steht FKIE durch das starke Wachstum des Instituts in den letzten Jahren sowie durch den intensiven Wettbewerb um die besten Köpfe am Standort Bonn vor großen Herausforderungen. Neben der Gewinnung von Mitarbeitern sind hier die Ausdifferenzierung der Führungsstrukturen, eine zielgerichtete Weiterentwicklung des Kompetenzprofils, der Führungs- und Managementqualitäten sowie der FKIE-Kultur entscheidend. Ein erster und wichtiger Schritt in Richtung eines gemeinsamen Verständnisses von Führung wurde 2013 mit dem FKIE-Führungsleitbild getan, an dem sich gute Führung bei FKIE in Zukunft orientieren soll.

»Ziel des neuen FKIE-Führungsleitbildes ist es, eine gemeinsam getragene, partizipative Führungskultur weiterzuentwickeln und zu etablieren, die von allen Mitgliedern des Instituts mitgetragen wird und in allen Hierarchieebenen verankert ist«, sagt Institutsleiter Professor Peter Martini. »Im Ergebnis streben wir insbesondere eine verbesserte Zusammenarbeit mit positivem Effekt für Mitarbeiter-Zufriedenheit und Arbeitsklima an. Schon jetzt ist eine positive Tendenz in der Belegschaft spürbar, dass wir uns dem so wichtigen Thema Führung konzentriert widmen und uns als Institut systematisch weiterentwickeln«.

Das Führungsleitbild benennt für FKIE wesentliche Aspekte guter Führung und gibt auf diese Weise den Orientierungsrahmen für das alltägliche Führungshandeln vor. Um die Leitlinien mit Leben zu füllen, diese neue Führungskultur zu etablieren und Nachwuchs-Führungskräfte systematisch zu entwickeln, wurde die FKIE-Führungsakademie ins Leben gerufen, deren erster Jahrgang 2014 gestartet ist.

Die über ein Bewerbungsverfahren ausgewählten Mitarbeiterinnen und Mitarbeiter absolvieren über einen Zeitraum von zwei Jahren ein curriculares Programm, in dem sie Schlüsselqualifikationen der Führungsarbeit erlangen. Das Talentprogramm der FKIE-Führungsakademie ist strukturell angelehnt an ein erprobtes, dreigliedriges Modell der Führungskräfteentwicklung. Es bietet neben einem maßgeschneiderten Seminarprogramm auch ein Mentoring-Programm sowie die Möglichkeit zur Mitgestaltung des FKIE durch betriebliche Projektarbeiten in zukunftsrelevanten Themen. Gleichzeitig entstehen aus der Konzeption der Akademie heraus über internes Networking hinausgehend weitere Kontakte und Netzwerke zu Industriepartnern, Ministerien und Behörden sowie innovative Ideen zur Weiterentwicklung der Aktivitäten und Strukturen des Institutes.

Parallel zur Führungsakademie werden spezifische Qualifikations- und Entwicklungspfade für weitere Mitarbeiter mit hohem Potential ausgearbeitet, um einerseits hohe Attraktivität als Arbeitgeber zu gewinnen und andererseits großen Nutzen für das Institut und damit für unsere Kunden zu schöpfen. Diese strategisch wichtigen Aktivitäten der Kultur- und Personalentwicklung werden auch in den kommenden Jahren fortgesetzt und weiter ausgebaut.

KURATORIUM

VORSITZENDER DES KURATORIUMS

Prof. Dr.-Ing. Gerd Ascheid
RWTH Aachen, Aachen

Alois Bader
Airbus Defence & Space, Ulm

Prof. Dr. Reinhard Klein
Rheinische Friedrich-Wilhelms-Universität Bonn

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

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

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

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

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

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

Prof. Dr. Stefan Fischer
Universität zu Lübeck, Lübeck

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

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

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

STRATEGIEENTWICKLUNG UND THEMENFELDER

Mit einer »Strategie 2019« richtet das FKIE den Blick in die Zukunft: Die vergangenen fünf Jahre waren geprägt von Wachstum und der Erschließung neuer Anwendungsfelder. Das lässt sich deutlich anhand des Ertragsvolumens, der Mitarbeiterzahl und der Struktur des Kundenportfolios ablesen. In den kommenden fünf Jahren werden wir unsere Weiterentwicklung mit einer vorausschauenden Zukunftsstrategie gezielt steuern und unsere Forschungsthemen kontinuierlich ausbauen.

Nicht nur quantitativ ist unser Institut auf einem klar erkennbaren Expansionskurs: Parallel zum Wachstum in Sachen Mitarbeiterzahl, Ertragsvolumen und Kundenportfolio baute FKIE zugleich qualitativ seine Reputation als eine der weltweit führenden Forschungseinrichtungen für Informations- und Kommunikationstechnologie aus. Dazu zählen beispielsweise die Bereiche Sensordatenfusion, Signalverarbeitung, sichere Nutzung des Cyberraums und Ergonomie. Aus **dieser positiven Dynamik heraus ist die Entwicklung neuer FKIE Geschäftsfelder** eine logische Konsequenz.

An der **FKIE-Kernausrichtung** als enger Partner **des Bundesministeriums der Verteidigung** wird sich auch in Zukunft nichts ändern. Die erzielten Erfolge in der zivilen Vertragsforschung bestärken uns jedoch darin, den Dual-Use-Gedanken und bridging technologies zusätzlich weiter voranzutreiben. Wir wollen den Anforderungen des freien Marktes gerecht werden und ganz im Sinne anwendungsorientierter Forschung direkten Nutzen für unsere Auftraggeber schaffen. Diese Aktivitäten befassen sich entsprechend unserer Mission mit der Erkennung, Minimierung und Beherrschung existenzbedrohender Risiken.

Leitgedanke bei der Konzeption von Geschäftsfeldern war die **Bündelung komplementärer Abteilungskompetenzen** in übergreifenden Themenfeldern. Das ermöglicht uns fortan mit Blick auf die Interessen unserer Kunden eine Verknüpfung inhaltlich verwandter, aber wissenschaftlich-methodisch unterschiedlicher Forschungsbereiche.

Unser Ziel mit der »Strategie 2019« ist es, unsere Position als eine der **weltweit führenden Forschungsinstitutionen** auf dem Gebiet der Informations- und Kommunikationstechnologie mit klarem wehrtechnisch ausgerichtetem Kernprofil und stabiler ziviler Vertragsforschung weiter zu festigen. Unsere bestehenden Alleinstellungsmerkmale sollen durch die tiefe Integration mensch-zentrierter Ergonomie und Usability in Zeiten immer komplexer werdender technischer Umgebungen signifikant ausgebaut werden. Ebenso machen wir es uns als IT-Institut zur Kernaufgabe, wesentliche Beiträge zu den Themen **Schutz und Handlungsfähigkeit im Cyberspace** zu leisten – wie etwa mit dem Fraunhofer-Positionspapier Cyber-Sicherheit 2020 für die Bundesrepublik Deutschland, an dem auch FKIE maßgeblich beteiligt ist.

Ein weiteres Ziel stellt die Verstärkung der Hochschulkooperationen dar. Die **Zusammenarbeit mit der Universität Bonn und mit der RWTH Aachen** wird weiter intensiviert. Selbstverständlich bauen wir auch unsere internationalen Kooperationen mit führenden Forschungseinrichtungen zielgerichtet aus. Durch die Verzahnung mit herausragenden wissenschaftlichen Institutionen in der Region kann das FKIE sich durch Sichtbarkeit und Vernetzung in den einschlägigen Communities als wichtiges Mitglied positionieren. Diese verstärkte Präsenz an den Hochschulen ist auch für die Gewinnung von **Nachwuchswissenschaftlern** für das FKIE von großer Bedeutung. Das Institut bietet herausragenden Absolventen die Möglichkeit, wissenschaftlich und zugleich anwendungsorientiert zu forschen.

Im November 2014 diskutierten wir im Rahmen eines Strategieaudits die Optionen der strategischen Weiterentwicklung des FKIE mit hochrangigen Auditoren aus Ministerien, Forschung und Wirtschaft. Dieser offene Austausch brachte uns wertvollen Input, den wir in unsere zukünftige Ausrichtung einfließen lassen werden. Die Umsetzung dieser Strategie verstehen wir als einen kontinuierlichen und dynamischen Prozess mit periodischen Phasen der Überprüfung, Verbesserung und Anpassung. An der schrittweisen Weiterentwicklung der Strukturen und Prozesse werden alle Institutsteile aktiv beteiligt sein: Wir legen Wert darauf, dass **diese Entwicklung vom gesamten Institut getragen und befördert wird**. Dies allein verspricht eine behutsame, aber zielgerichtete Veränderung, um die hohe Qualität des Instituts dauerhaft zu erhalten, auszubauen und so den Herausforderungen der Zukunft vorausschauend zu begegnen.

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

ABTEILUNG
SENSORDATEN- UND INFORMATIONSFUSION [SDF]

Ausrichtung der Abteilung

Bereits vor jeder wissenschaftlichen Reflexion oder technischen Umsetzung ist Sensordaten- und Informationsfusion ein allgegenwärtiges Phänomen: Jedes Lebewesen verknüpft Eindrücke unterschiedlicher, sich ergänzender Sinnesorgane mit zuvor erlerntem Erfahrungswissen und Mitteilungen anderer Lebewesen. Daraus formt es ein Modell seiner Umwelt – die Grundlage für situationsgerechtes Handeln.

Als Zweig der angewandten Informatik versucht die Sensordaten- und Informationsfusion, diese Informationsverknüpfung zu verstehen, sie soweit wie möglich zu automatisieren und über das natürliche Vermögen hinaus zu steigern. Insofern ist sie ein Zweig der Automatisierungstechnik, eine Art Maschinenbau für »kognitive Tools«, die menschliche Fähigkeiten zur Datenauswertung und -verknüpfung ebenso steigern wie mechanische Werkzeuge die Körperkraft.

Dabei profitiert die Sensordatenfusion von generellen Technologietrends wie Vernetzung, Mobilität, Sensor- und Datenbanktechnologie. Sie schafft zugleich die Basis für effektives manned-unmanned-Teaming, also für die Interaktion zwischen Menschen und den sie unterstützenden technischen Systemen.

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

- TRAX - Tracking in Complex Sensor Systems (EU Marie Curie)
- AMSEL - Assistenzsystem zur Multisensoriellen Emitterlokalisierung
- PlasmA - Plattformschutz mittels Audiosensorik
- 3DMapping - Lagebildeerstellung mit AUS und UGV
- PASSAGES - Protection and Advanced Surveillance for the Arctic

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

ABTEILUNG **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 umsetzen. Aufgrund der Heterogenität der Informations- und Kommunikationssysteme erarbeiten wir Interoperablitätslösungen, die wir in unseren Laboren testen und auf Konformität zu Standards überprüfen. In unseren Forschungsfeldern unterstützen wir die Bundeswehr und Behörden für die zivile Sicherheit bei der Wahrnehmung hoheitlicher Aufgaben und arbeiten mit der Industrie an der Umsetzung unserer Forschungsergebnisse in innovative Produkte.

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

- Zivile Kommunikationsverfahren für militärischen Einsatz
- Protokolle und Test von akustischen Unterwassernetzen
- Störungsanalyse im Funkbereich

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

ABTEILUNG
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, dynamische Prozesse, 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 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 System-verbünde entwickelt, prototypisch implementiert sowie verifiziert.

Die Abteilung entwickelt Architekturen und Interoperabilitätslösungen für Führungs- und Assistenzsysteme zur Unterstützung einer vernetzten Operations- bzw. Unternehmensführung. Zur Beherrschung der Informationsflut werden außerdem Verfahren zur automatischen Informationsanalyse und Fusion entwickelt.

Forschungs- / Entwicklungsbereiche

- Interoperabilität heterogener IT-Systeme
- Systemarchitekturen
- Informationsanalyse und -verdichtung
- Prozessoptimierung

Schwerpunkte / Kernkompetenzen

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

Projekte

- InAus - Intelligente Auswertung großer Datenmengen
- IntelsysPRO - Integriertes Entscheidungsunterstützungs- und Lagedarstellungssystem
- GVA Testbed - Generic Vehicle Architecture Testbed
- TET - Test- u. Emulationsumgebung, taktisch
- ePoolice

Leitung:
Dr. Thomas Alexander
Telefon +49 228 9435-480
thomas.alexander@fkie.fraunhofer.de

ABTEILUNG
HUMAN FACTORS [HF]

Ausrichtung der Abteilung

Flexibilität, Mobilität und der damit verbundene zuverlässige und sichere Zugriff auf Daten und Informationen von jedem Ort und zu jeder Zeit sind heute von hoher Bedeutung. Dies gilt nicht nur für den Privatbereich, sondern speziell für Anwendungen in sicherheitskritischen Bereichen. Hier sind die Einsatzkräfte und Entscheidungsträger auf aktuelle Informationen essenziell angewiesen, um in kurzer Zeit unter hoher Belastung wichtige Entscheidungen fehlerfrei zu treffen und zu handeln. Durch solche Rahmenbedingungen und den ständigen Informationsbedarf ergeben sich weitere Anforderungen an die Gestaltung der Mensch-Computer-Interaktion, des mobilen Geräts, wie Smartphones, Tablets und Wearables, und die eigentlichen Organisationsprozesse. Ziel unserer Arbeiten ist es, durch die Entwicklung, Anwendung und Evaluation von innovativen Methoden und Verfahren zur Integration des Menschen in die Konzeption und Gestaltung von Mensch-Technik Systemen die Welt jeden Tag ein wenig sicherer zu machen. Bei uns steht dabei der Mensch im Mittelpunkt.

Forschungs- / Entwicklungsbereiche

- Ergonomische Gestaltung mobiler IT-Systeme und Smart Devices
- Methoden zur Analyse und Modellierung von Teamoperationen in sicherheitskritischen Bereichen
- Visualisierung und Interaktion für mobile Computer
- Virtual und Augmented Reality (VR/AR)
- Sicherheitsmanagementsysteme

Schwerpunkte / Kernkompetenzen

- Systemorientierte, benutzerzentrierte Gestaltung mobiler IT-Systeme
- Modellierung und Simulation des Menschen zur Produkt- und Produktionsgestaltung
- Physiologische und mentale Belastung und Beanspruchung

Projekte

- SeMPOs - Systemergonomische Modellierung von Prozessen für urbane Operationsszenare
- WAvE - Wearable and Adaptable Environment for Personal Equipment
- HeMoDe - Head-Mounted Displays – Bedingungen des sicheren und beanspruchungsoptimalen Einsatzes
- ENgAGE4Pro - Ergonomie-Navigator für die alters- und alternsgerechte Produktion

Leitung:
Annette Kaster
Telefon +49 228 9435-573
annette.kaster@fkie.fraunhofer.de

ABTEILUNG
MENSCH-MASCHINE-SYSTEME [MMS]

Ausrichtung der Abteilung

Die Verwendung von anspruchsvoller, komplexer Technik ist bei der Bewältigung von Sicherheitsaufgaben nicht wegzudenken, ob bei der Polizeiarbeit oder im Katastrophenschutz, bei der Überwachung von Kraftwerken oder im Rahmen von militärischen Missionen. Diese muss jedoch für den Anwender leicht und intuitiv zu bedienen sein, denn der Einsatz von Sicherheitsanwendungen erzeugt häufig Stresssituationen. Deshalb sollten diese Anwendungen so gestaltet sein, dass sie einem mangelnden Systemverständnis und menschlichem Versagen optimal vorbeugen. Die Abteilung MMS ist darauf spezialisiert, komplexe Technologien und Prozessabläufe für den Menschen eindeutig und transparent darzustellen und die Interaktionen von Mensch und Technik zeit- und stressrobust zu gestalten.

Die Vorgehensweise bei der Bearbeitung von Projekten und Studien setzt auf der Norm für die benutzerzentrierte Gestaltung interaktiver Systeme DIN ISO 9241-210 auf, deren Methoden, Verfahren und Werkzeuge laufend angewendet, überprüft und weiterentwickelt werden. Für den Praxistest werden neue Ideen in Hard- und Software nutzerzentriert umgesetzt: Vom Prototyp bis zum fertigen Produkt, von der Anforderungsanalyse bis zur Bewertung. Der Anwender wird immer in die Entwicklung mit einbezogen.

Forschungs- / Entwicklungsbereiche

- Analyse und Gestaltung von Prozessen in sicherheitskritischen Systemen
- Methoden und Werkzeuge zur ergonomischen Gestaltung von Mensch-Maschine-Systemen
- Mensch-Maschine-Schnittstellen für Führungs- und Einsatzsysteme
- Informationsvisualisierung und Mensch-Maschine-Interaktion

Schwerpunkte / Kernkompetenzen

- Analyse von Aufbau- und Ablauforganisation
- Modellierung/Simulation von Arbeitsumgebungen
- Optimierung von Prozessen
- Analyse/Konzeption/Gestaltung von Leitzentralen
- Untersuchung ergonomischer Interaktionskonzepte
- Assistenz- und Entscheidungsunterstützungssysteme
- Ergonomisches HMI-Design
- Georeferenzierte Lagedarstellung und Ressourcendarstellung

Projekte

- VERSIA - Visualisierung verteilter Simulationsdaten
- SIREVA - Sicherheit von Personen bei Rettungs- und Evakuierungsprozessen von Passagierschiffen
- IntelsysPRO - Integriertes Entscheidungsunterstützungs- und Lagedarstellungssystem für Flughäfen
- AMIGOS - Adaptive Mensch-Maschine-Interaktion
- Telekom - Cyber Threat Radar
- HC SV MMS - Human Centered Security Visualizer / Logdatenvisualisierung

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

ABTEILUNG **SYSTEMERGONOMIE [SE]**

RWTH AACHEN UNIVERSITY

Ausrichtung der Abteilung

Die Abteilung Systemergonomie ist spezialisiert auf die ganzheitliche Gestaltung von Systemen und auf die Integration von Menschen mit komplexen technischen Systemen und Prozessen (Human-Systems Integration) sowohl für militärische als auch für zivile Anwendungen. Ziel ist es, mit dem Blick aufs Ganze und Exzellenz im Detail existenzbedrohende Risiken zu kontrollieren und minimieren, und dabei nutzenorientiert eine ausgewogene Balance aus Leistungsfähigkeit, Betriebssicherheit (Safety), Angriffssicherheit (Security), Gebrauchstauglichkeit (Usability), Ökologie und Ökonomie zu erreichen.

Die Abteilung ist eng verbunden mit dem Forschungs- und Lehrgebiet Systemergonomie an der RWTH Aachen, und verfügt über eine ausgewiesene Profilierung in der Frühphase der Um- oder Neugestaltung von sicherheitskritischen Systemen z.B. im Bereich Verkehr und Verteidigung, sowie bei der Gestaltung, Entwicklung und Einführung von Assistenz- und Automationssystemen.

Forschungs- / Entwicklungsbereiche

- Systemergonomie (Balanced Human Systems Integration)
- Kooperative Bewegungs- und Fahrzeugführung
- Verhandlung zwischen Mensch und Automation

Schwerpunkte / Kernkompetenzen

- Partizipative Technologie- und HMI-Exploration
- Rapid Prototyping
- Simulationsunterstütztes Requirement Engineering; Simulator- und Realtests

Projekte

- StrAsRob - Systemergonomie und Interface-Gestaltung zum Hochautomatisierten Fahren von LKW-Konvois
- SiFaU - Sicht- und Fahrunterstützung z.B. durch Sichtersatz-Brillen und Sichtunterstützung-Monitore
- Arbitrierung - Schnelle Verhandlungsprozesse zwischen Mensch und Maschine in zeit- und sicherheitskritischen Systemen

Leitung
Dr. Jens Tölle
Telefon +49 228 9435-513
jens.toelle@fkie.fraunhofer.de

ABTEILUNG
CYBER ANALYSIS & DEFENSE [CA&D]

Ausrichtung der Abteilung

Die Abteilung Cyber Analysis & Defense widmet sich der Erkennung, Analyse und Abwehr von Bedrohungen auf die Kommunikationsnetze und daran angeschlossenen Geräte. Das Ziel der Forschungsarbeiten ist die Schaffung eines sicheren Cyberraumes, der auch Cyber-Physical-Systems umfasst. Dies sind all die Bereiche, in denen IT als Vernetzungskomponente komplexer Anlagen und Systeme eingesetzt wird.

Zur Erreichung dieses Ziels sind umfassende Kompetenzen notwendig: Präventive Maßnahmen sind Basis sicherer Systeme, die bestmöglich vor Angreifern geschützt sind. Unter reaktiven Maßnahmen versteht man die Überwachung der Netze und Geräte, um im Falle einer erkannten Bedrohung eingreifen, die Bedrohung melden und abwehren zu können. Weiterhin muss man aus erfolgten Angriffen lernen. Dies umfasst sowohl die technische Seite, als auch Wissen über Täter, deren Motivationen und Vorgehensweisen. Im Bereich Cyber Analysis werden dazu betroffene Systeme untersucht und neue Gegenmaßnahmen entwickelt.

Forschungs- / Entwicklungsbereiche

- Secure Mission Networks
- Cyber Situational Awareness
- Cyber Analysis

Schwerpunkte / Kernkompetenzen

- Sicherheitstests und Bewertung von Komponenten, Architekturen und Systemen (Penetrationstests, Fuzzing, Lasttests, Simulationen)
- Erkennung, Analyse und Abwehr von Schadsoftware (Ködersysteme/Honeypots, Reverse Engineering, Statische und dynamische Analyse, Botnetz-Monitoring und -infiltration)
- Überwachung, Darstellung und Bewertung der Sicherheitslage (Intrusion Detection & Prevention, Threat Intelligence, Visualisierung, von Monitoring-Daten)
- Absicherung von Kommunikationsinfrastrukturen (Gruppenkommunikation, Schlüsselmanagement)

Projekte

- ENAN - Erkennung Nichtautorisierter Netzübergänge
- CERT-BPol - CERT (Computer Emergency Response Team) Bundespolizei
- QUAKSBw - Querschnittlicher Anteil KommServer Bw
- IDP/MIKE - IPsec Discovery Protocol / Multicast Internet Key Exchange
- Botman

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

ABTEILUNG
CYBER SECURITY [CS]

universitätbonn

Ausrichtung der Abteilung

Vertrauen ist gut, Kontrolle ist besser! In der Welt der IT sollte es heute lauten: Vertrauen ist unangebracht und Kontrolle dringend erforderlich!

IT-Systeme sowie deren Nutzer werden dem in sie gesetzten Vertrauen oftmals nicht gerecht und sind vielfältig verwundbar. Die Kontrolle sicherheitsrelevanter Abläufe bei der IT-Nutzung ist zum Schutz vor Angriffen und zur Gewährleistung von Handlungsfähigkeit unentbehrlich.

Wir entwickeln vertrauensbildende Maßnahmen und etablieren Kontrollmechanismen. Das Monitoring sicherheitsrelevanter Abläufe und deren Beurteilung hinsichtlich Sicherheitskonformität ermöglicht eine kontinuierliche Übersicht.

Wir analysieren Angriffstechniken und entwickeln Ansätze zur Erkennung und Abwehr. Außerdem untersuchen und testen wir die (Un-)Überwindbarkeit von Schutzmaßnahmen. Dabei betrachten wir u.a. erst kürzlich von IT durchdrungene und vernetzte Bereiche.

Wir unterstützen vertrauensvolle rechtskonforme Kooperation von unterschiedlichen Partnern zu gemeinsamen Schutzzielen.

Die Abteilung ist eng mit der Arbeitsgruppe IT-Sicherheit der Universität Bonn verbunden und an grundlagenorientierten Forschungsprojekten, der universitären Lehre sowie der Weiterqualifikation des wissenschaftlichen Nachwuchses beteiligt.

Forschungs- / Entwicklungsbereiche

- Verteiltes kooperatives Sicherheitsmonitoring
- Erkennung und Analyse von Internet-Routing-Anomalien
- Sicherheit in der Gebäudeautomation
- Messung von IT-Sicherheits-Awareness
- Cyber-Threat-Intelligence

Schwerpunkte / Kernkompetenzen

- Daten- und Vertraulichkeitsschutz beim Sicherheitsmonitoring mittels Pseudonymen
- Systematisches Awareness-Penetration-Testing
- Analyse und Simulation von Angriffstechniken sowie Entwicklung von Erkennungsansätzen
- Verkehrsnormalisierung und Anomalieerkennung in Gebäudeautomations-Netzen

Projekte

- ITS.APT - IT Security Awareness Penetration Testing
- BARNI - Building Automation Reliable Network Infrastructure
- CYSPA - European Cyber Security Protection Alliance
- Smart Home Security
- Threat Intelligence Driven Intrusion Detection
- Analyse und Erkennung von QuantumInsert-Angriffen

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

ABTEILUNG
KOGNITIVE MOBILE SYSTEME [CMS]

Ausrichtung der Abteilung

Die Abteilung Kognitive Mobile 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

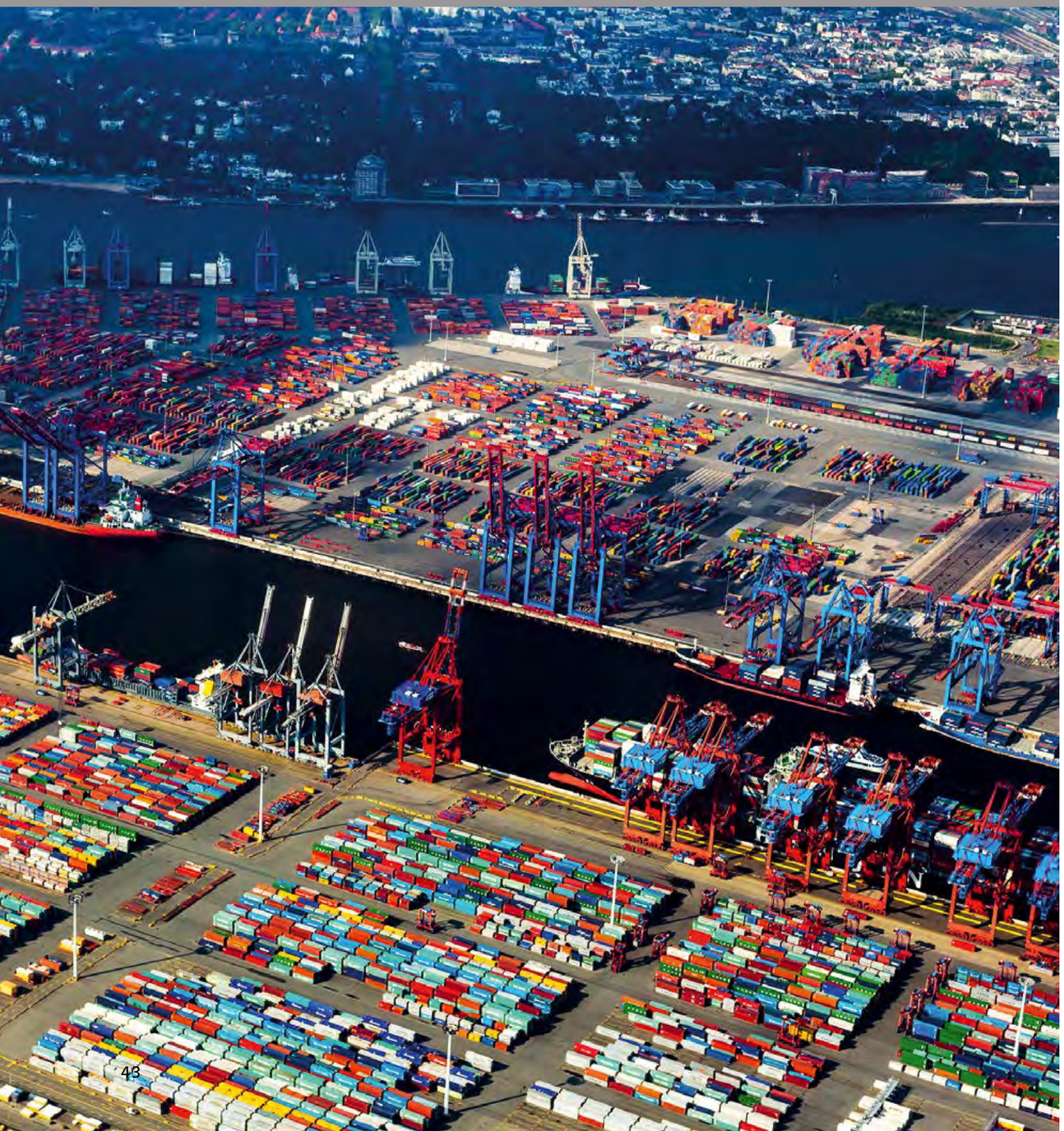
- Autonome Navigation für drinnen und draußen
- Umgebungserfassung: Sensorbasierte Modellerstellung, Tracking, Objekterkennung und semantische Sensordateninterpretation
- Explorations-, Planungs- und Koordinierungsverfahren
- Mobile Manipulation
- Direkte / indirekte Mensch-Roboter-Interaktion
- Software-Frameworks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

Projekte

- ARMINIUS - Assistenzfunktionen für Teilautonomie in mobilen unbemannten Systemen
- VARUS - Vernetzungsstrategien und Anwendungsszenarien für unbemannte Systeme
- STARO - Standardisierte Anbindung von Roboterschwärmen an Führungsinformationssysteme
- MANIPUF - Modulares Manipulatorfahrzeug
- Robot}air{ - Boden-Luft-Servicerobotersystem zur Inspektion industrieller Druckluftversorgung

I / FÜHRUNGSSYSTEME & PROZESS-ORIENTIERTE SYSTEMINTEGRATION

Bei zunehmender Komplexität gewinnen Entscheidungsunterstützung und Prozessorganisation an Bedeutung. Hierfür analysiert und optimiert FKIE sicherheitskritische Systeme im Zusammenspiel von Mensch, Technik, Organisation und Umgebung, entwickelt IT-Lösungen und integriert diese in die bestehende Architektur des Kunden.



TRANSPARENZ FÜR MEHR SICHERHEIT

Nach den Anschlägen von New York kam weltweit auch die Sicherheit der Seeschifffahrt vor Terrorangriffen auf den Prüfstand. Seit 2004 gilt eine EU-Richtlinie unter anderem für die Risikobewertung von Hafenanlagen. Forscher der FKIE-Abteilung »Mensch-Maschine-Systeme« entwickelten eine neue Methode, die seit 2014 Hafenbetreibern in Deutschland hilft, Risikoanalysen transparenter und plausibler zu gestalten.

Häfen und der internationale Seeverkehr sind wesentlicher Bestandteil der Versorgungskette – und gelten daher als potenzielles Ziel für Terroristen. Der International Ship and Port Facility Security Code, kurz: ISPS-Code, wurde nach den Terroranschlägen von New York mit dem Ziel etabliert, maritime Infrastruktur besser vor Terrorangriffen zu schützen – Stichwort: Maritime Security.

Anhand einer Risikobewertung wurden Hafenanlagen binnen kurzer Zeit zu Sicherheitsbereichen umgewidmet. Im Januar 2014 trat in Deutschland mit der »szenariobasierten Bedrohungsanalyse« jüngst eine neue Methode zur Risikobewertung in Kraft. Sie wurde am Beispiel des Fährverkehrs im Rahmen eines Projekts des Bundesministeriums für Bildung und Forschung (BMBF) mit verschiedenen Projektpartnern und Endnutzern entwickelt. Als Projektkoordinator fungierte die FKIE-Abteilung »Mensch-Maschine-Systeme« mit der Gruppe »Organisationsergonomie« unter Leitung von Florian Motz.

Die wissenschaftlichen Mitarbeiter Gina Linkmann und Daniel Ley stellten sich der Herausforderung, die Risikoevaluierung, die der ISPS-Code fordert, transparenter und anwendungsfreundlicher zu gestalten. Dazu fokussierten sie zunächst die Schwächen bisheriger Risikoanalysen. Elementarer Bestandteil des ISPS-Codes ist die Risikobewertung von Häfen durch geschulte Experten vor Ort. Bisherige Methoden verlangen unter anderem Annahmen darüber, wie viele Menschenleben bei einem Angriff gefährdet würden: 0, 1 bis 4, 5 bis 9 oder 10 und mehr. Von der unklaren Aussagekraft einer solchen Einschätzung abgesehen hält Ley dies »ethisch mindestens für fragwürdig«. Und am Ende einer jeden Risikobewertung steht schließlich nichts weiter als – eine Zahl. »Gewonnene Erkenntnisse zu Risiken in Hafenanlagen gehen in den Zahlen verloren«, bemängelt Ley, diese nur scheinbare Exaktheit vermittele »bestenfalls eine vermeintliche Sicherheit.«

Mit der neuen, von Linkmann und Ley entwickelten Methode werden Bewertungsprozess und Risikoverständnis sehr viel transparenter dokumentiert. Die Objekte werden anhand ihrer Auswirkungen für Wirtschaft, Umwelt und Menschen sowie anhand ihres Symbolwertes eingestuft. Mithilfe von sieben konkreten Szenarien terroristischer Angriffe wird dann analysiert, ob ein solcher für das Objekt infrage kommt – »nach gesundem Menschenverstand«, ergänzt Ley. Für jedes »Ja« gibt es einen Punkt. Damit wird, wie von der Richtlinie gefordert, wieder eine Zahl ermittelt. Doch die gewonnenen Daten bieten weitere Informationen: Zum Beispiel, warum ein Szenario vorstellbar erscheint oder nicht, und vor allem, welche Maßnahmen dagegen unternommen werden können. Eine Farbkodierung macht die Risikoanalyse überdies anschaulich.

Ley: »Mit dieser Methode zur Risikobewertung erhalten die Endnutzer eine sehr viel transparentere Risikoevaluierung.« Die Resonanz auf die Methode sei durchweg positiv. Auch der EU-Kommission in Brüssel wurde die Methode unlängst vorgestellt, mit Erfolg: Andere Mitgliedsstaaten prüfen derzeit eine mögliche Umsetzung der deutschen Methode.

KONTAKT

Florian Motz
Telefon 0228 9435-271
florian.motz@fkie.fraunhofer.de

DIE »GOLDENE STUNDE« DANK TWITTER HALBIEREN

Bei medizinischen Notfällen sprechen Ärzte von der »goldenen Stunde«, innerhalb der Patienten gerettet und versorgt werden sollen, um ihre Überlebenschancen deutlich zu erhöhen. Mit der CATO-Toolbox soll unter anderem auch Social Media helfen, im Krisenfall mit nuklearen, biologischen, chemischen oder radiologischen Stoffen wertvolle Zeit zu gewinnen. Ein Team des Fraunhofer FKIE tüftelt die entsprechenden Algorithmen aus.

London, King's Cross – in der simulierten Notrufzentrale gehen erste Meldungen über eine Explosion in der Nähe einer U-Bahn-Station ein. Die Lage vor Ort ist noch äußerst unklar; Anrufer melden unterschiedliche Beobachtungen, die sich zum Teil auch widersprechen; es soll Verletzte geben.

»CATO« ist der Name eines EU-Forschungsprojekts, in dem Rettungsstrategien für den Fall von terroristischen Attacken mit nicht-konventionellen Waffen entwickelt werden. An dem Projekt beteiligen sich 25 Partner mit Erfahrung in Notfallmanagement aus zwölf Ländern. Anhand eines vergleichsweise harmlosen Szenarios wird der Ernstfall geprobt – freilich rein virtuell. Ziel ist es, Einsatzkräften einen »Werkzeugkasten« mit Hilfsmitteln an die Hand zu geben, mit denen sie im Falle eines Angriffs mit nuklearen, biologischen, chemischen oder radiologischen Stoffen möglichst rasch und effizient reagieren können. Ein Team des Fraunhofer FKIE entwickelt für CATO Algorithmen für ein Programm, das die Einsatzkräfte auch mit Hilfe von Informationen aus Sozialen Medien schneller als gewöhnlich einen Überblick über die Situation verschaffen soll.

Die ersten Einsatzkräfte sind auf den Weg zum Unglücksort. Weitere Anrufer melden einen seltsamen chemischen Geruch am Unglücksort. Dieser Geruch innerhalb einer chemischen Wolke wird von Augenzeugen auch bei Twitter beschrieben; es soll einige leicht verletzte Personen geben.

Joachim Biermann leitet das FKIE-Team, das sich aus Mitgliedern der Abteilungen »Sensordaten- und Informationsfusion« sowie »Informationstechnik für Führungssysteme« zusammensetzt: »Unser Ziel ist es, im Katastrophenfall auf verschiedene verfügbare Informationen aufzubauen, die wichtigen herauszufiltern und den Entscheidern vor Ort eine vernünftige Grundlage für ihre Entscheidungen an die Hand zu geben.« Dabei liegt die Idee nahe, nicht allein Notrufe zu sammeln, findet Biermann: »Junge Leute posten oder twittern heutzutage doch erst einmal, bevor sie telefonieren.« Neben den Informationen aus verschiedenen Quellen werden auch Daten vorhandener Sensoren für chemische oder radioaktive Stoffe ausgewertet.

Bei Twitter gehen weitere Meldungen aus der Umgebung des Unglücksortes ein. Diese Meldungen sind durch ihre übermittelten GPS-Informationen erkennbar sowie durch Stichworte wie »Bomb« oder »Explosion«.

Forscherin Kellyn Rein erläutert, wie die Algorithmen aufgebaut sind, um auch kleine Hinweise erfassen zu können: »In einem ersten Schritt filtern wir die Informationen, im zweiten Schritt gruppieren wir sie, und in einem dritten Schritt versuchen wir, diese Informationen in einen Sinnzusammenhang zu bringen.« Für eine gute Filterfunktion können auch Straßenbezeichnungen aus der Umgebung dienen. Dem Datenschutz wird dabei jederzeit genüge getan: Alle gewonnenen Informationen werden ohne Namen vorgehalten und auch nur so lange, bis sich die Lage wieder normalisiert hat. Ziel ist, dass dieses System europaweit verfügbar sein wird und dabei auch nicht länderspezifische Rechte etwa in Bezug auf den Datenschutz verletzt. »Wir werten alle Informationen nur ereignis-, nicht personenbezogen aus; alle Daten werden anonymisiert«, betont Rein.

First Responders geben der Einsatzleitung ein Bild von der Lage vor Ort. Auf einer Karte lassen sich jetzt verschiedene Tweets mit Standortdaten darstellen. Eine Heatmap zeigt rote Bereiche, aus denen besonders viele Meldungen kommen, die offenbar Bezug auf das Ereignis nehmen.

Alle eingehenden Informationen, auch Notrufe, werden in Text umgewandelt. So kann die Datenfusion vollständig textbasiert durchgeführt werden. Philip Schmiegelt hat sich insbesondere der Einbettung von Tweets in die Lagedarstellung gewidmet. »Ich bin sehr zufrieden mit dem Ergebnis. Das Programm konnte sehr schnell einen Überblick darüber geben, was wo aktuell passiert.« Da es sich nur um ein simuliertes Katastrophenszenario handelt, hat man echte Daten aus Twitter als »Hintergrundrauschen« genutzt, und diesen beispielsweise Tweets mit dem Hashtag #explosion beigemischt. Durchgespielt wurde das Szenario zu einer Zeit, als es in England gerade Schulzeugnisse gab: »Das konnten wir an Begriffen wie #happy, #alevelresults oder #results sehr schnell erkennen«, erklärt Schmiegelt die Funktionsweise.

Die Karte bietet einen Überblick, in welchem Bereich sich die Wolke ausbreitet. Sensible Orte wie Krankenhäuser oder Schulen werden besonders markiert. Aus diesen Daten können die Einsatzleiter eine Bedrohungsanalyse erstellen, die Einsatzkräfte vor Ort mit Informationen versorgen und besser koordinieren.

Rettungskräfte sind bemüht, im Katastrophenfall verletzte Personen binnen 60 Minuten, der »goldenen Stunde«, medizinisch zu versorgen. Dies verspreche den Verletzten eine besonders hohe Überlebenschance. Biermann möchte die Rettungskräfte dabei so effektiv wie möglich unterstützen: »Unser Ziel sollte es sein, mit unseren Methoden die Reaktionszeit auf eine halbe Stunde zu verkürzen.« Besonders im Fall eines terroristischen Angriffs mit gefährlichen Stoffen kann ein solcher Zeitgewinn entscheidend sein, um Leben zu retten.

Das Team ist mit den Ergebnissen bei den zwei durchgeführten Tests mit verschiedenen Szenarien sehr zufrieden: »Mit einer möglichst zutreffenden Beschreibung des Vorfalls sollen die Einsatzkräfte vor Ort mit einem möglichst aktuellen Lagebild versorgt werden können«, fasst Biermann zusammen: »Und mit unseren Tests konnten wir zeigen, mit welch unterschiedlichen Quellen und Schnittstellen welche Informationen zusammengeführt und ausgewertet werden können.« Wenn die Software einsatzbereit ist, soll sie als Bestandteil der CATO-Toolbox über das Europäische Krisenreaktionszentrum in das europäische Katastrophenschutz-Netzwerk integriert werden.

Weblink: www.cato-project.eu

KONTAKT

Joachim Biermann
Telefon 0228 9435-276
joachim.biermann@fkie.fraunhofer.de

Prof. Dr. Ulrich Schade
Telefon 0228 9435-376
ulrich.schade@fkie.fraunhofer.de

II / KOMMUNIKATION & INTEROPERABILITÄT

Den sicheren und zuverlässigen Betrieb unterschiedlicher Informations- und Kommunikationstechnologien sowie deren Kompatibilität zu gewährleisten, ist das Ziel der folgenden Projekte. Dazu entwickelt FKIE mit State-of-the-Art- und Zukunftstechnologien neue Lösungen und begleitet sie bis zur Standardisierung.

AUF DER SUCHE NACH DER PERFEKTEN WELLE

WLAN, LTE oder WiMAX fit machen für den militärischen Einsatz: Die zivile Nutzung von modernen Funktechnologien ist, getrieben durch den Markt, rasant fortgeschritten. Somit liegt es nahe, diese Technologien auch im Hinblick auf militärische Anwendungen zu untersuchen und daraus Anregungen für Weiterentwicklungen zu gewinnen. Die Forscher der FKIE-Abteilung Kommunikationssysteme (KOM) machen große Fortschritte bei der Untersuchung einer geeigneten Breitband-Wellenform für militärische Anforderungen.

Aus dem zivilen Alltag sind die modernen Funktechnologien, wie sie bei WLAN, LTE oder WiMAX verwendet werden, nicht mehr wegzudenken: Kaum ein ziviles Gerät kommt heute ohne Anteile dieser Technologien aus. Sie gewährleisten eine effektive Vernetzung mehrerer Nutzer über verschiedene Entfernungsbereiche hinweg. Im militärischen Bereich ist die Entwicklung auf diesem Sektor seit vielen Jahren langsamer verlaufen. »Früher waren militärische Entwicklungen wegweisend für die Kommunikationstechnik«, weiß FKIE-Wissenschaftler Dr. Ferdinand Liedtke, »da hat ein Wandel stattgefunden.« Längst ist die zivile Technologie, vom Markt getrieben, eindeutig führend.

Einfach in den nächsten Elektrofachmarkt spazieren und ein paar der neusten Geräte für die Truppe einkaufen – so simpel ist die Modernisierung der Kommunikationsausrüstung freilich nicht: Taktisch nutzbare Kommunikationstechnik für das Militär muss besondere Anforderungen hinsichtlich Sicherheit und Robustheit erfüllen, auf die die Ziviltechnik leichter Hand verzichten kann. Sollen Soldaten zukünftig also in der Lage sein, mit modernen Breitbandnetzen schnell Sprache, Bilder und Videos untereinander oder an übergeordnete Instanzen zu übermitteln, dann müssen die zivilen Technologien an die militärischen Anforderungen angepasst werden. Diesem Ziel widmet sich die Forschungsgruppe Software Defined Radio von Dr. Marc Adrat in der Abteilung KOM – und macht dabei bemerkenswerte Fortschritte.

Handsprechfunkgerät bietet nur Schmalband-Wellenform

»Wir versuchen, uns etwas von den zivilen Technologien abzuschauen«, verrät Liedtke das Vorgehen. Das für kurze und mittlere Distanzen ausgelegte traditionelle Handsprechfunkgerät etwa, grün, stoß- und wasserfest, sei »wie ein dickes Handy«, biete aber nur eine Schmalband-Wellenform mit geringer Übertragungskapazität. Das Problem für die Forscher auf der Suche nach der perfekten Wellenform fasst Liedtke lakonisch zusammen: »Eine Lösung für alle Anwendungsfälle gibt es nicht!«

Deshalb gelte es, schrittweise vorzugehen: »Unser Ziel ist zunächst die Konzeption einer Breitband-Wellenform für das sogenannte Data Distribution Subsystem, beispielsweise für kleinere Einsatzgruppen, zu entwickeln«, erläutert Matthias Tschauner, der seit 2011 als wissenschaftlicher Mitarbeiter in diesem Bereich forscht. Das Data Distribution Subsystem biete eine größere Bandbreite und Datenrate, die auch das Übertragen von Videos gestattet, und ermögliche zusätzlich die Teilnahme vieler Sender und Empfänger. Dass dieses Unterfangen nicht ganz einfach ist, liegt auf der Hand: »Das verfügbare Frequenzspektrum ist begrenzt und somit ein kostbares Gut«, erinnert Liedtke, und da liegt ein zentrales Problem: Ein Teil der möglichen Leistungsfähigkeit einer Breitband-Wellenform wird den besonderen Ansprüchen an militärische Kommunikation Tribut zollen müssen. Liedtke: »Man spendiert einiges für die Sicherheit und nimmt Einbußen bei der Übertragungskapazität in Kauf.« Sicher, robust und vor Täuschungen geschützt soll ein militärisch genutztes Kommunikationssystem sein. Selbstverständlich muss der Kommunikationsinhalt sowohl vor dem unbefugten Zugriff geschützt, als auch stabil gegen absichtliche Störungen sein. Ein modernes Frequenzmultiplexverfahren, kurz OFDM (Orthogonal Frequency Division Modulation / Multiplex), erscheint dem Forscherteam daher die richtige Wahl, zumal es eine hohe Datenrate und Robustheit verspricht.

»Wir preschen vor und schauen, was wir erreichen können«

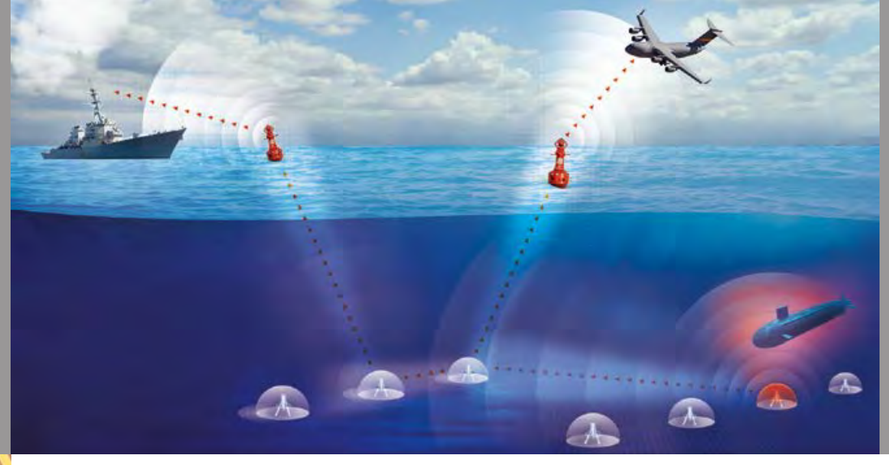
Die neue Wellenform, an der die FKIE-Wissenschaftler forschen, wird dann auf einen Demonstrator, bestehend aus moderner Hardware, portiert, um ihre Einsatzfähigkeit für verschiedene Szenarien zu zeigen. »Wir preschen vor und schauen, was wir erreichen können«, erläutert Tschauner das Vorgehen. »Wir versuchen jetzt erst einmal, die WLAN-Wellenform anzupassen«, verrät Liedtke, »später können wir noch weitere notwendige Module konzipieren.« Die WLAN-Wellenform erlaube das Experimentieren vergleichsweise problemlos: »Dafür kann man Tools einfach herunterladen und damit simulieren«, erklärt Tschauner.

Immerhin werde derzeit international nach einer neuen Breitbandwellenform gesucht, alle NATO-Verteidigungskräfte sind interessiert an moderner Kommunikationstechnik. Als ersten Schritt, erläutert Tschauner, »testen wir zunächst eine nationale Breitband-Wellenform«. Bald, so die Hoffnung des Forscherteams, könne dann eine ganze Wellenform-Familie die nötige Flexibilität bieten, die im militärischen Bereich erforderlich ist. Diese könnte dann auch auf NATO-Ebene vorgestellt werden.

KONTAKT

Dr. Marc Adrat
Telefon 0228 9435-807
marc.adrat@fkie.fraunhofer.de

NACH DEM VORBILD DER WALE



KONTAKT

Peter Sevenich
Telefon 0228 9435-317
peter.sevenich@fkie.fraunhofer.de

Unterwassersensoren sind von großer Bedeutung für die maritime Aufklärung, sei es für den Hafenschutz, militärische Zwecke oder Tsunami-Frühwarnsysteme. Doch wie können Sensoren unter Wasser ihre Daten effektiv weiterleiten? Mit einer ausgeklügelten Methode und einem neuen Netzwerkprotokoll schafft ein Team des Fraunhofer FKIE in Kooperation mit der Wehrtechnischen Dienststelle 71 in Kiel mit schallwellenbasierter Technologie Voraussetzungen für die Unterwasserkommunikation der Zukunft.

Die Wale machen es vor: Wer unter Wasser kommunizieren möchte, der sollte Schallwellen in Betracht ziehen. Denn während zu Land und in der Luft unterschiedlichste Wellen Kommunikation ermöglichen, gelten unter Wasser andere Gesetze: Hier bleiben Distanzen jenseits von 100 Metern für elektromagnetische Wellen unüberwindbar. Schallwellen hingegen, zumal in niedrigen Frequenzen, verlieren auch unter der Meeresoberfläche nur wenig ihrer Kraft durch Absorption. »Schall ist bei größeren Distanzen alternativlos«, erklärt Michael Goetz. Dies macht sich der Forscher für das akustische Unterwassernetzwerk zunutze. Ein Problem jedoch bleibt: »Hochfrequente Töne reichen nicht so weit wie Bässe«, erläutert Goetz, die zur Verfügung stehende Bandbreite sinke bei steigender Entfernung. Es gilt also die Entfernungen möglichst gering zu halten.

Für das Projekt »RACUN« setzten sich Institute, Partner aus der Industrie und Marinen europäischer Länder das Ziel, ein robustes ad-hoc-Unterwassernetzwerk zu entwickeln. Um das Problem der Entfernung zu lösen, wurde eine sogenannte Multi-Hop-Strategie eingesetzt: Bodenknoten, die auf den Meeresgrund herabgelassen werden und dank Sensoren in der Lage sind, akustische Signaturen, Druckunterschiede oder auch magnetische Veränderungen wahrzunehmen, leiten die Daten weiter.

Bei der Abschlussdemonstration in La Spezia in Italien wurden sowohl das Nachrichtenformat GUWAL als auch das Netzwerkprotokoll GUWMANET®[1] erfolgreich vorgeführt. Beide wurden vom FKIE-Team um Goetz entwickelt. Dabei konnte den beteiligten Marinen die Kommunikation innerhalb eines heterogenen Unterwassernetzwerkes aus Bodenknoten, Schiffsknoten, einer Gatewayboje und einem autonomen Tauchfahrzeug in verschiedenen Anwendungsszenarien erfolgreich demonstriert werden. GUWMANET erzielte mit einer Übertragungsrate von 90% ein deutlich besseres Ergebnis als das Konkurrenzprotokoll mit 70%.

Das Problem, das Goetz und seine Forscherkollegen zu lösen hatten: »Wie gehen wir mit Schallwellen-Kollisionen um, wenn mehrere Übertragungen gleichzeitig laufen und sich gegenseitig stören?« Ihre Lösung: »Alles kurz und knapp!« Indem das Nachrichtenformat GUWAL die Daten komprimiert, können GPS-Daten, Kommandos, Detektions-Events und andere Statusmeldungen gesendet werden. Dabei finden die Bodenknoten selbstständig die kürzeste Verbindung über die unterschiedlichen Multi-Hop-Knoten zum Empfänger und wieder zurück. Brechen solche Verbindungen ab, etwa weil ein Knoten ausfällt, finden sie automatisch einen neuen Weg.

»Wir konnten zeigen, dass die Detektions-Events zur Oberfläche weitergegeben werden können. Das hätten wir 2013 selbst noch nicht gedacht«, freut sich Goetz. Die Versuche bei den Tests im Mittelmeer haben funktioniert. Damit konnte für die Unterwasserkommunikation der Zukunft eine wichtige technologische Grundlage geschaffen und ein richtungsweisender Schritt gemacht werden.

[1] *Marke der Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V., München, in Deutschland.*

III / INFORMATIONSGEWINNUNG & ENTSCHEIDUNGSUNTERSTÜTZUNG

Eine Vielzahl von Sensoren und Datenerfassungssystemen liefert eine Masse an Informationen, die es zu gewinnen, verarbeiten und verdichten, zu übertragen, zu analysieren und benutzergerecht darzustellen gilt. Diese gesamte Kette der Informationsverarbeitung deckt FKIE mit seinen Kompetenzen ab.

DAS RISIKO IN DER TEXTWÜSTE AUFSPÜREN

Der Flugverkehr wird penibel überwacht, nicht nur in Europa. Selbst kleinere Zwischenfälle und Störungen werden in oft ausführlichen Berichten dokumentiert. Ein disziplinübergreifendes FKIE-Team konnte im Auftrag der EASA demonstrieren, wie diese Berichte künftig automatisiert ausgewertet und so Probleme und Risiken noch besser entdeckt werden können, die sich in erschöpfenden Texten verbergen.

Fliegen halten viele Menschen, seien sie privat oder beruflich unterwegs, offenkundig für eine feine Sache – die Zahlen der Internationalen Zivilluftfahrtorganisation ICAO künden beeindruckend davon: Mehr als 33 Millionen Flüge jährlich weltweit mit über 3 Milliarden Passagieren zählt sie. Bis zum Jahr 2030, so schätzt die Organisation, werde sich dieses Aufkommen gar verdoppeln. Die Schnelligkeit ist natürlich ein gutes Argument für eine Flugreise, auch der Service an Bord mag in aller Regel höchst erfreulich sein, charmante Stewards und Stewardessen sowieso. Das entscheidende Argument dafür, eine Flugreise anzutreten, ist freilich das Gefühl, mit dem Flugzeug sicher am Zielort anzukommen.

Flugsicherheit ist ein äußerst sensibles Thema und wird von allen Beteiligten entsprechend ernst genommen. Der stetig wachsende Flugverkehr bringt für die Flugsicherheit und ihre Überwachung neue Herausforderungen mit sich. Die zuständige Dachorganisation für Flugsicherheit innerhalb der Europäischen Union ist die EASA, die mit dem Projekt »Investigation Report Text Mining Study«, kurz IRTMS, die Auswertung der verschiedenen nationalen Berichte über Zwischenfälle im Luftverkehr noch effizienter gestalten möchte. Ein Forscherteam der FKIE-Abteilungen Sensordaten- und Informationsfusion (SDF) und Informationstechnik für Führungssysteme (ITF) konnte im Rahmen dieser Studie zeigen, wie die Berichte maschinell ausgewertet werden können. Teamleiter Joachim Biermann: »Die EASA wollte wissen, ob es möglich und sinnvoll ist, die Auswertung der Berichte automatisiert durchzuführen und systematisch in ihrer Datenbank zu hinterlegen. Mit unserem Demonstrationssystem konnten wir zeigen: Ja, das ist es!«

Nationale Berichte in vollkommen heterogenen Formaten

An dem System tüftelten Ulrich Schade, außerplanmäßiger Professor für Linguistik an der Uni Bonn, und der Diplom-Informatiker Philip Schmiegelt. Sie haben dabei eine überzeugende Auswertung vorliegender Berichte, die z.B. in Deutschland von der Bundesstelle für Flugunfalluntersuchung (BFU) erstellt werden, in mehreren Schritten erreicht. Diese birgt natürlich Tücken, erläutert Schade: »Die verschiedenen nationalen Behörden senden ihre Berichte jeweils an die EASA, allerdings in vollkommen heterogenen Formaten, auch in Bezug auf Sprache, Umfang oder Inhalt.« Der Vorteil einer systematisch zusammengestellten Datenbank liegt daher auf der Hand: »Vorfälle, die man gemeinsam betrachten sollte, können nun besser einander zugeordnet werden.« Denn das, was ohne systematische Betrachtung womöglich als Einzelfall abgelegt würde, könnte sich mithilfe der neuen Datenbank und systematischer Betrachtung als struktureller Fehler entpuppen.

Schade erläutert das an einem fiktiven Beispiel: »Wenn an zwei unterschiedlichen Flughäfen in unterschiedlichen Ländern bei unterschiedlichen Fluggesellschaften bei einer Maschine gleicher Bauart ein Problem mit, sagen wir, einer Bremsleitung bei einer bestimmten Außentemperatur auftaucht, dann legt die bisherige Systematik den Experten nicht unbedingt nahe, diese Fälle miteinander zu vergleichen.« Mit einer systematischen, textbasierten Auswertung könne dies automatisiert geschehen und die Fachleute veranlassen, einen zweiten Blick auf die Sache zu werfen.

Die erste Hürde bei der automatisierten Auswertung muss bereits beim Textformat genommen werden, insbesondere dann, wenn der Bericht nur als Scan vorliegt. Manche nationale Behörde schickt auch nicht einen Bericht pro Vorfall, sondern sammelt die Berichte aller Vorfälle aus drei Monaten in einem Gesamtbericht. Schade: »Das war uns vorher nicht klar.« Problematisch sei es auch, dem Bericht die Ursache zu entnehmen, wenn das gebräuchliche Wort dafür schlicht nicht vorkomme: »Wenn sich der Berichterstatter die Mühe macht, den Vogel genau zu beschreiben, der ins Triebwerk geraten ist, etwa einen ›Red-tailed Hawk‹, dann fehlt uns das Stichwort ›birdstrike‹ im Text«, erinnert sich Schade an eines der Probleme, mit denen die automatische Auswertung zu kämpfen hat. Aber das Programm sei in der Lage, aus solchen Fällen zu lernen.

Einfach zu bedienender webbasierter Prototyp

Den dazugehörigen Algorithmus hat der Informatiker Schmiegelt entwickelt. »Ich habe einen einfach zu bedienenden webbasierten Prototypen gebaut, der die Berichte in wenigen Minuten auszuwerten und im Excel-Format darzustellen in der Lage ist«, fasst Schmiegelt seinen Part zusammen. Zunächst galt es, den Text an sich zu extrahieren, insbesondere bei Scans. Im nächsten Schritt erkennt die entwickelte Software die Sprache, in der der Bericht verfasst ist. Anschließend sammelt die Software über die computerlinguistische Methode der Informationsextraktion alle Informationen aus dem Bericht, die für dessen Klassifikation und Einordnung in die EASA-Datenbank relevant sind. Das sind zum Beispiel Flugzeug-Hersteller, -Modell oder die Registrationsnummer, Angaben zum Zeitpunkt und zum Ort des Zwischenfalls sowie Angaben zum Ersteller des Berichts selbst. Abschließend erfolgt eine statistische Analyse des Textes, um eine Aussage über die Ursache des Zwischenfalls zu erhalten. Schmiegelt staunte nicht wenig über die Vielgestaltigkeit der Berichte: »Manche Berichte sind geradezu liebevoll gestaltet, zum Beispiel mit Bildern. Das hilft bei der textbasierten Auswertung natürlich nicht weiter.«

Schade freut sich, mit diesem Projekt ganz gemäß des FKIE-Mission Statements Risiken frühzeitig erkennbar gemacht zu haben. Und auch Teamleiter Biermann ist zufrieden mit dem Ergebnis, das das Team der EASA vorlegen kann: »Diese Software arbeitet in Bezug auf die Auswertung zuverlässiger als ein Experte – und nimmt ihm zudem diese Trivialarbeit ab.« Natürlich müsse am Feintuning noch gearbeitet werden; dennoch rät er, neben der Überarbeitung der EASA-Datenbank auch dazu, alte Berichte auf diese Weise auszuwerten: »Das ist sicher eine Option, die schnell neue Erkenntnisse bringen kann.«

KONTAKT

Joachim Biermann
Telefon 0228 9435-276
joachim.biermann@fkie.fraunhofer.de

Prof. Dr. Ulrich Schade
Telefon 0228 9435-376
ulrich.schade@fkie.fraunhofer.de

BLUE CHIPS FÜR DIE SENSORSTEUERUNG

Alexander Charlish hat mit seinem Team einen Algorithmus entwickelt, der dem Rechner mit einem einfachen Marktmechanismus hilft, die ihm zur Verfügung stehenden Ressourcen in jeder Situation effektiv zu verteilen. Nach dem Prinzip von Angebot und Nachfrage verrichten moderne Sensoren, etwa ein Multifunktionsradar, ihre Arbeit dort, wo sie gerade am dringendsten benötigt wird.

Immer wenn er im Autoradio auf dem Weg zu seinem Büro in der FKIE-Abteilung Sensordaten- und Informationsfusion (SDF) die Börsennachrichten hört, freut sich Dr. Alexander Charlish. Jede aktuelle Börsennachricht wird Einfluss auf den Handel an diesem Tag nehmen und für steigende oder fallende Kurse sorgen. Was andere mit Sorgen oder Frohlocken in Bezug auf ihr persönliches Aktiendepot verfolgen, ist für den 30-jährigen Elektrotechniker einfach ein äußerst nützlicher Mechanismus. Eine ganze Weile hat er sich mit der Frage beschäftigt, wie er einem Rechner beibringen könnte, diesen Marktmechanismus ebenso souverän zur Anwendung zu bringen wie ein Händler an der Börse. Mit seinem Team hat er eine überzeugende Lösung gefunden.

Eine einzige elektronisch steuerbare Arrayantenne eines Radars ermöglicht eine hohe Beweglichkeit des Radarstrahls, der fast unmittelbar gelenkt und die verfügbare Leistung zwischen den verschiedenen zu beobachtenden Zielen aufgeteilt werden kann. Sind sogar verschiedene Sensorsysteme untereinander verknüpft, muss ein Rechner in der Lage sein zu ermitteln, in welche Aufgaben er seine begrenzten Ressourcen wie Zeit, Energie und Kommunikationsfähigkeit investieren sollte. Ein solches automatisiertes System intelligent und effizient zu nutzen ist die Herausforderung, der sich Charlish mit seinem Team gestellt hat: »Das Ziel war eine Sensorsteuerung, die die beste Leistung ermöglicht.«

KONTAKT

Alexander Charlish
Telefon 0228 9435-651
alexander.charlish@fkie.fraunhofer.de

Das System muss dynamisch und in Echtzeit arbeiten

Angebot und Nachfrage – nach diesem Prinzip schöpft ein von Charlish entworfener Ressourcenmanagement-Algorithmus die Möglichkeiten voll aus, die zunehmend komplexer und detailreicher arbeitende moderne Sensorsysteme bieten. Ein solches System muss dynamisch und in Echtzeit arbeiten, sich also den Gegebenheiten vor Ort unmittelbar anpassen. Charlish vergleicht dies mit einem Autofahrer, der seine Aufmerksamkeit je nach Fahrsituation intuitiv anpasst: »Wenn ich auf der Autobahn fahre, dann konzentriere ich mich auf andere Autos auf der Straße, achte darauf, ob ich von schnelleren Autos überholt werde oder ob vor mir ein Auto ausschert. Auf Fußgänger achte ich auf einer Autobahn normalerweise weniger.« Das ändert sich natürlich, sobald er die Autobahn verlässt: »Wenn ich in der Stadt fahre, achte ich auf ganz andere Sachen wie Ampeln, Fußgänger oder Radfahrer«. Überholende oder ausscherende Fahrzeuge stehen dafür nun weniger im Fokus des Fahrers. Diese dynamisch angepasste Fokussierung überträgt Charlish mit dem konkurrierenden Element des Marktmechanismus innerhalb des von ihm fortentwickelten »Continuous Double Auction Parameter Selection«-Algorithmus auf einen Rechner. Jeder Aufgabe eines Sensorsystems ist ein zielorientierter Makler zugeordnet. Der Algorithmus priorisiert dazu die aktuellen Sensoraufgaben, so dass die Ressourcen verteilt und Kontrollparameter so gewählt werden können, dass die Bewältigung der Aufgaben alle eine optimale Leistung des Sensorsystems ermöglichen, fortwährend handeln die Agenten miteinander um die vorhandenen Ressourcen. Charlish: »Das sind tausende Deals in jeder Sekunde«. Anders als auf dem Börsenparkett spielen Dollar oder Euro bei diesem Handel aber natürlich keine Rolle: »Die Währung, in der die Makler handeln, ist der Nutzen, den eine Aufgabe in diesem Augenblick zum Gesamtziel beitragen kann«, erläutert Charlish.

Bei manövrierenden Objekten muss der Radar häufiger »hinschauen«

Im Fallbeispiel, das das Team untersucht hat, geht das wie folgt vonstatten: Beobachtet ein Radar mehrere Flugzeuge zur gleichen Zeit, errechnet das System anhand der vorliegenden Daten, wo sich die Flugzeuge voraussichtlich im nächsten Augenblick befinden. Fliegt ein Flugzeug mit gleichbleibender Geschwindigkeit in eine Richtung, genügt es, alle paar Augenblicke den Radarstrahl dorthin zu werfen. Stellt sich aber heraus, dass die angenommene Position von der tatsächlichen abweicht, das Flugzeug also offenbar manövriert und Richtung oder Geschwindigkeit verändert muss der Radar häufiger »hinschauen«, um sich der Position zu vergewissern. Die »Aktien« für diese Aufgabe steigen folglich. Je größer die Abweichung, desto kürzer müssen die Abstände sein, mit denen der Radar das Objekt erfasst – entsprechend hoch handelt der Makler diese Aufgabe, ihr Wert gegenüber anderen Aufgaben wird steigen. Auch der Abstand zu einem Objekt bestimmt über die Intensität, mit der es beobachtet werden muss. Charlish: »Nahe Dinge muss ich nur kurz anschauen, entfernte Objekte etwas länger«. Charlish: »Das Neue an unserer Arbeit ist, dass wir einem Rechner Antizipation ermöglichen anstelle das starre Abarbeiten fester Regeln.« Einen Software-Demonstrator, der diesen stetigen, wechselseitigen Auktionsmarktmechanismus nutzt, um die Verteilung der Ressourcen zwischen den Sensoraufgaben zu managen, hat das von Charlish geleitete Team erstellt. Im Vergleich zu anderen Lösungen sei diese zwar »schwerer zu installieren«, betont Charlish, »aber die Leistung ist dafür auch ungleich höher«.

Eine elektronisch steuerbare Arrayantenne auf einem Flugzeug (links) muss ihre begrenzte Zeit und ihr Energiebudget zwischen Sensoraufgaben, wie der Suche nach neuen Objekten (grün) oder dem Tracken bekannter Objekte (rot und blau) aufteilen. Die Ressourcenzuteilung kann mit dem entwickelten, marktbasierten Algorithmus optimiert werden.

DEM ELEKTROSMOG AUF DER SPUR

WLAN, WLAN-Repeater, PDAs, tragbare Telefone, alte Netzteile: Erwünschte und unerwünschte elektromagnetische Strahlung ist längst im Alltag angekommen und betrifft jeden Haushalt. Mit einem ausgeklügelten Algorithmus und der neuen Generation eines Spektrumanalysators entwickeln die Forscher am FKIE das Equipment des Kammerjägers der Zukunft.

Drahtlose digitale Datenübertragung ist ein Segen: Mit dem tragbaren Festnetztelefon lassen sich Gespräche auch im Garten führen, der Fernseher empfängt sein Programm ohne Kabelverbindung, die Digitalkamera verbindet sich mit dem Drucker. Und Smartphone oder Tablet sind nicht nur pausenlos online, sondern verbinden den Nutzer auch mit seiner Musikanlage, dem Kühlschrank oder der Klimaanlage, dank WLAN-Repeater selbst im hintersten Winkel des Hauses.

Die schier unbegrenzt erscheinende Möglichkeit zur Datenübertragung ist jedoch zugleich Fluch: Denn je mehr Endgeräte im elektromagnetischen Spektrum aktiv sind, desto größer ist die Gefahr, dass sie sich im selben oder in überlappenden Frequenzbändern gegenseitig stören oder eine Übertragung sogar vollständig unmöglich machen. »Häufig bemerkt man das, wenn man ein neues Gerät zu Hause aufstellt und plötzlich feststellt, dass andere Geräte nicht mehr richtig funktionieren«, erläutert Prof. Frank Kurth von der FKIE-Abteilung Kommunikationssysteme, »und in der Regel weiß dann niemand, woran es eigentlich liegt«. Billigprodukte aus Fernost ohne geeignete Prüfung und Zulassung führen besonders oft zu solchen Interferenzen, aber sie sind nicht allein das Problem. Hinzu kommt: Dieses Phänomen wird in Zukunft eher zu- als abnehmen, eine effektive Störungssuche ist daher für Endnutzer, aber auch für die Telekommunikations- und Netzanbieter, gefragt. Freilich steckt eine geeignete Störungssuche, die solchen Problemen Abhilfe zu leisten imstande wäre, lange noch in den Kinderschuhen.

Dieser Herausforderung haben sich Kurth und sein Team seit einigen Jahren angenommen: Sie entwickelten eine neue Methode zur Darstellung des elektromagnetischen Spektrums mittels digitaler Signalanalyse. Mithilfe dieser Methode können vornehmlich moderne Signaltypen besser visualisiert werden als mit herkömmlichen Spektrumanalysatoren. Sie basiert auf einer patentierten FKIE-Technologie und arbeitet mit Methoden der digitalen Mustererkennung. Dabei werden aus allen Funkkanälen des breitbandigen Funksignals systematisch verschiedene Muster erzeugt. Der Clou: Jeder Mustertyp ist so beschaffen, dass bestimmte Eigenschaften digitaler Funksignale besonders stark hervortreten.

Die Technologie kann durch Entwicklung charakteristischer Muster zur effizienten Detektion und Klassifikation bekannter Funksignaltypen verwendet werden. Und sie ist auch geeignet für die Erkennung von Störsignalen – dazu gehören solche, die durch defekte, fehlerhafte oder nicht zugelassene elektronische Geräte erzeugt werden. Als besonders große Problemquelle entpuppen sich darunter solche Geräte, die eigentlich gar keine Strahlung abgeben sollen, es wegen eines Defekts aber tun.

Einen besonders dicken Fisch hatte das Team gleich bei den ersten Versuchen am Haken, erinnert sich Mitentwickler Robert Peter: »Als wir unseren Demonstrator erstmals hier auf dem Institutsgelände angewendet haben, haben wir gleich ein nicht entstörtes Netzteil in einem Aufzugsschacht detektiert. Eine weitere Störquelle in einem Nachbargebäude hat vermutlich schon seit Jahren fröhlich elektromagnetische Strahlung abgegeben.« Solche völlig unerwünschten Abstrahlungen beschränken sich natürlich auch nicht auf einen kleinen Frequenzbereich, im Gegenteil: sie können breitbandig auftreten und damit gleich eine ganze Reihe von Funkkanälen stören.

Kurth und sein Team haben die Entwicklung der zugrundeliegenden Technologie für verschiedene Funktionsmuster, mit denen eine Signaldetektion auf Breitband-Funksignalen entsprechender Bandbreite möglich ist, in Soft- und Hardware vorangetrieben. Durch die Portierung der entwickelten Algorithmen auf schnelle Grafikprozessoren ist es gelungen, eine echtzeitfähige Signaldetektion in größeren Megahertzbereichen zu ermöglichen. Ein weiteres Funktionsmuster erlaubt eine musterbasierte Betrachtung des elektromagnetischen Spektrums, Kurth vergleicht dies mit »einem Blick durch eine andere Brille«. Damit können bestimmte Signaltypen für den Betrachter wesentlich klarer hervortreten, als dies mit herkömmlichen Spektraldarstellungen möglich ist. Kurth: »Auch ein schwaches Störsignal wird so gut detektiert«.

Kurth ist davon überzeugt, dass die praktische Anwendung dieser Technik in nicht mehr allzu ferner Zukunft liegt: »Ich kann mir sehr gut vorstellen, dass der moderne Kammerjäger des 21. Jahrhunderts bald mit einem kleinen Empfänger nebst Antenne durch Haushalte läuft und Störsignale erst detektiert und klassifiziert – und anschließend unschädlich macht.« Das Equipment dieses modernen Kammerjägers wird patentierte Technologie von Fraunhofer FKIE in sich tragen.

KONTAKT

Prof. Dr. Frank Kurth
Telefon 0228 9435-868
frank.kurth@fkie.fraunhofer.de

IV / SCHUTZ & HANDLUNGSFÄHIGKEIT IM CYBER SPACE

Der Cyberraum enthält mittlerweile eine Masse an hochsensiblen Daten über fast jeden Nutzer. Das FKIE schützt IT-Systeme und Datenübertragung sowohl präventiv als auch reaktiv und steigert die Resilienz der Systeme, falls doch einmal eine Gefahr real geworden ist. Dabei wird weder die praktische Einsetzbarkeit gemindert noch der menschliche Nutzer überfordert.

»ANGRIFFSVEKTOR MENSCH«

Gegen Cyberangriffe schützen sich Betreiber insbesondere kritischer Infrastrukturen mit hohem technischem Aufwand. Nicht selten versuchen Angreifer deshalb, den Nutzer für ihre Zwecke zu instrumentalisieren. In einem Verbundprojekt erforscht ein Bonner Team in zwei Feldstudien das Nutzerverhalten und damit Methoden, mit denen die User effektiv sensibilisiert werden können, um im Falle des Falles nicht den falschen Klick zu machen.

Im Klinikalltag kann es rasch hektisch werden. Wenn auf dem Monitor zur Unzeit auch noch Warnmeldungen aufflackern, dann ist für guten Rat oft nicht ausreichend Zeit. Und egal, ob der Oberarzt, die Sekretärin oder der Praktikant dann mit einem Klick die falsche Entscheidung trifft: die Konsequenz ist die gleiche. Ist erst ein Rechner mit unerwünschter Schadsoftware befallen, dauert es oft nicht lange, bis auch das gesamte Betriebsnetzwerk betroffen ist.

Phishing, Malware im E-Mail-Anhang, Links auf verseuchte Webseiten – die Gefahren sind vielfältig und wenn der Nutzer im Falle eines Angriffs die falsche Entscheidung trifft, ist auch die beste Sicherheitssoftware machtlos. Arnold Sykosch forscht als wissenschaftlicher Mitarbeiter an der Universität Bonn und am Fraunhofer FKIE auf dem Gebiet der IT-Sicherheit und befasst sich mit der Frage, wie der Mensch vor dem Computer vorbereitet werden kann, um im Falle eines Angriffs die richtige Entscheidung zu treffen – nämlich die, die den Angriff abwehrt. »Viele Betriebe engagieren externe Dienstleister, sogenannte Penetrations-Tester, die versuchen, in ein Betriebsnetzwerk einzudringen, um die Schwachstellen aufzudecken«, weiß Sykosch, »das gibt es aber nur für die Sicherheitstechnik, nicht für den Menschen, der vor dem Rechner sitzt.« Und dabei machen Angreifer vor dem Nutzer eben nicht Halt.

Wissenschaftlich ist dieses Feld bislang allerdings nur unzureichend aufbereitet. Das soll sich mit einem Projekt nun ändern: Das Uniklinikum Schleswig-Holstein in Lübeck wird in einem im Dezember 2014 gestarteten und vom Team des Fraunhofer FKIE und der Universität Bonn koordinierten Verbundprojekt bis 2017 die Anwenderperspektive auf dieses Unterfangen bieten. Das Cyber-Security-Team um Prof. Dr. Michael Meier ist in dem Förderschwerpunkt »IT-Sicherheit für Kritische Infrastrukturen« im vom Bundesministerium für Bildung und Forschung geförderten Projekt neben der Koordination für den sicherheitstechnischen Part zuständig.

»Wir sind überzeugt von diesem Projekt«

Als Ergebnis versprechen sich die beteiligten Forscher ein Werkzeug zur kosteneffizienten Messung des kollektiven IT-Sicherheitsbewusstseins ganzer Unternehmen. Dieses Werkzeug könne Erkenntnisse für alle an dem Projekt beteiligten Forschungsbereiche bieten: Rechtswissenschaften, Psychologie und Informatik, aber auch das IT-Risikomanagement von Unternehmen soll verfeinert werden. Sykosch verspricht sich aufschlussreiche Einsichten aus der Studie: »Wir sind überzeugt von diesem Projekt, mit unseren Verbundpartnern sind wir sehr gut aufgestellt.« Für die wissenschaftlichen Mitarbeiter in der Abteilung Cyber Security geht es dabei darum, das Zusammenspiel zwischen Nutzer und Technik zu erforschen und dann zu optimieren, sodass die Sicherheit von kritischen Infrastrukturen nachhaltig erhöht werden kann.

Dazu wird das Team ein Penetrations-Testing konzipieren, das die Sensibilisierung des Nutzers zum Ziel hat. Sykosch: »Das wollen wir systematisch etablieren und damit das Sicherheitsniveau merklich erhöhen.« Besonders im Fokus stehen dabei Betreiber kritischer Infrastrukturen, dazu gehören Kraftwerke, Krankenhäuser, aber auch Supermärkte: »Wenn eine große Supermarktkette nur wenige Tage ihre Waren nicht an die Filialen ausliefern kann, dann droht schon der Notstand. Wir stehen auf einer fragilen Infrastruktur«, erinnert Sykosch – und die gelte es besser zu schützen: »Es gibt viele Einfallstore, die wir möglichst alle prüfen möchten.«

Neben dem Team vom Fraunhofer FKIE und der Universität Bonn gehören die Universität Duisburg-Essen mit dem Fachgebiet Allgemeine Psychologie und Kognition sowie das Institut für Informations-, Telekommunikations- und Medienrecht an der Westfälischen Wilhelms-Universität Münster zu dem Verbund. Zudem ist das Unabhängige Landeszentrum für Datenschutz in Schleswig-Holstein mit im Boot. Dank dessen Input kann es den Forschern möglich werden, den Betrieb am alltäglichen Arbeitsplatz zu testen, ohne Rechte zu beschneiden. Denn eine wichtige Frage, die beantwortet werden muss, lautet: »Was muss passieren, damit sich der Nutzer im alltäglichen Betrieb vor dem Rechner sicher oder unsicher fühlt?«

»Wie funktioniert der Sicherheitsblick?«

Technik mittels Usability Engineering nutzerfreundlicher zu gestalten ist ein wichtiger Schritt, räumt Sykosch ein. Aber es gehe vielmehr darum, das Verständnis in Bezug auf Sicherheit zu erhöhen: »Wie funktioniert der Sicherheitsblick? Und wie kann ich den User optimal unterstützen?« Sykosch: »Wir müssen wissen, was ganz genau im Nutzer vor sich geht, wenn eine Phishingmail am Spamfilter vorbei kommt.« Oft sei schon viel gewonnen, wenn der Nutzer »nicht jede Anfrage abnickt«. Erhält man beispielsweise eine E-Mail, die in auffallend schlechtem Englisch verfasst ist, sollte das bereits abschreckend wirken. »Aber wie viele reagieren darauf wirklich skeptisch? 20, 50 oder doch 80 Prozent?«, fragt Sykosch: »Das wollen wir herausfinden!«

Zum Nutzerverhalten liegen jedoch nur wenige wissenschaftliche verwertbare empirische Daten vor, denn eine Datenerhebung ist nicht nur aufwändig und kostspielig, sondern auch datenschutz- und arbeitsrechtlich problematisch. Auch Schulungen, die das Sicherheitsbewusstsein der Angestellten verbessern sollen, seien oft umstritten, nicht selten wegen hoher Kosten und unklarem Nutzen, der mit traditionellen wissenschaftlichen Messwerkzeugen bisher nicht praktikabel nachgewiesen werden konnte. Mit der wissenschaftlichen Aufarbeitung könne deren Nutzen auf eine wissenschaftliche Basis gestellt werden: Mit dem Indikator »IT-Sicherheitsbewusstsein« sollen in dem Projekt auch im Hinblick auf Kosten und zeitlichen Erhebungsaufwand wesentliche Erkenntnisse gewonnen werden.

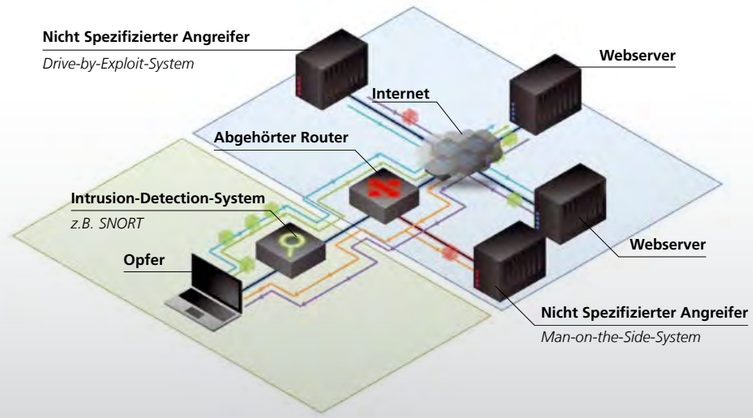
»Wir wollen eine neue Perspektive auf eine alltägliche Mensch-Maschine-Interaktion bieten«, so Sykosch. Dabei werde man nicht wie ein echter Angreifer agieren, sondern solche Angriffe nur kontrolliert simulieren. Dennoch sitze das Team auch nicht mit der Eieruhr neben den Usern, versichert Sykosch: »Wir möchten eine saubere Methodik und ein sauberes Werkzeug entwickeln.« Bis 2017 werden die Forscher eine Menge Daten gewinnen und diese Erkenntnisse unmittelbar in Handlungsanweisungen umsetzen können, mit der der »Faktor Mensch« besser auf Cyberattacken vorbereitet sein wird.

KONTAKT

Prof. Dr. Michael Meier
Telefon 0228 7354-249
michael.meier@fkie.fraunhofer.de

KONTAKT

Prof. Dr. Michael Meier
Telefon 0228 7354-249
michael.meier@fkie.fraunhofer.de



DEN WERKZEUGKASTEN DER NSA OFFENLEGEN

Seit den Enthüllungen von Whistleblower Edward Snowden wissen wir, dass internationale Geheimdienste das Internet überwachen. Die Informatiker am Fraunhofer FKIE entwickeln Konzepte, mit denen die Methoden der Cyberspione sichtbar gemacht werden können: Mit einfachen Mitteln helfen sie, den »Mann an der Seite« zu erkennen.

Der tiefe Einblick in die Vorgehensweise amerikanischer Geheimdienste, den internationalen Datenverkehr zu dokumentieren und auszuwerten, hat eine gesellschaftliche Debatte über Cyberspionage und Privatsphäre angestoßen. Zugleich wurde damit der Werkzeugkasten der NSA offengelegt – und steht damit auch anderen Angreifern potenziell zur Verfügung. Diplom-Informatiker Matthias Wübbeling hat sich auf Netzwerke spezialisiert und interessiert sich daher besonders für die »Quantum-Suite«, den Werkzeugkasten der NSA für Netzwerkangriffe. Vor allem dem Werkzeug »Quantuminsert« und seiner Funktionsweise widmen sich Wübbeling und sein Kollege Arnold Sykosch sowie Prof. Dr. Michael Meier, Leiter der Abteilung »Cyber Security« am Fraunhofer FKIE.

»Wir möchten diesen Angriff gerne erkennen«, erläutert Wübbeling das besondere Interesse an diesem Werkzeug, das bislang die größte Aufmerksamkeit auf sich zog, weil es ein verbreitetes Angriffsszenario der Cyberspione darstellt. Das Prinzip eines Quantuminsert-Angriffs folgt nicht dem klassischen »Man-in-the-Middle«-Prinzip, sondern vielmehr eines »Mannes an der Seite«: Der Angreifer ist fortan in der Lage, sämtliche Daten mitzulesen, kann aber selber nicht eingreifen oder Daten manipulieren.

Technisch ist das Erkennen eines Angriffs für die FKIE-Spezialisten also bereits möglich, allerdings besteht – ironischerweise – noch ein datenschutzrechtliches Problem, soll es breite Anwendung finden: »Wir müssen dazu in den sogenannten Payload hineinschauen, sehen also die Daten und Texte, die beispielsweise ein Mitarbeiter in einer Firma über seinen E-Mail-Account ausgetauscht hat.« Um die Software also als Produkt anbieten und in Betrieb nehmen zu können, um zu schauen, ob ein oder mehrere Rechner »gequantuminserted« wurden, müssen vorab datenschutzrechtliche Vorkehrungen getroffen werden. Das gilt auch für eine institutsinterne Implementierung, die die Forscher aber planen.

Im Rahmen des FKIE-Technologieforums stellten die Fachleute den Demonstrator vor. Wübbeling und seine Kollegen stießen auf großes Interesse: »Das ist eine schöne Demonstration, weil es so einfach ist.« Das Interesse war gewiss auch deshalb groß, weil sich nach den Snowden-Enthüllungen eigentlich alle im Visier der Geheimdienste sehen. Nicht unbedingt zu Unrecht: »Jeder kann Opfer sein«, merkt Wübbeling an.

Der Erfolg bei Quantuminsert soll nur der Auftakt sein. Denn hat man erstmal einen Angriff auf einen Rechner identifiziert, ist man in der Lage, zu schauen, was auf dem Rechner dann noch passiert, welche bislang im Verborgenen bleibenden Funktionen die Schadsoftware auszuführen in der Lage ist. Und auch weitere kleine und große Bestecke aus dem NSA-Handwerkskoffer wollen die Forscher im kommenden Jahr ins Visier nehmen. Wübbeling: »Das können wir uns dann ja genüsslich anschauen, das ist ein wenig wie ein Spieltrieb.«

DER UNSICHTBARE FEIND IM BETRIEBSSYSTEM-KERNEL

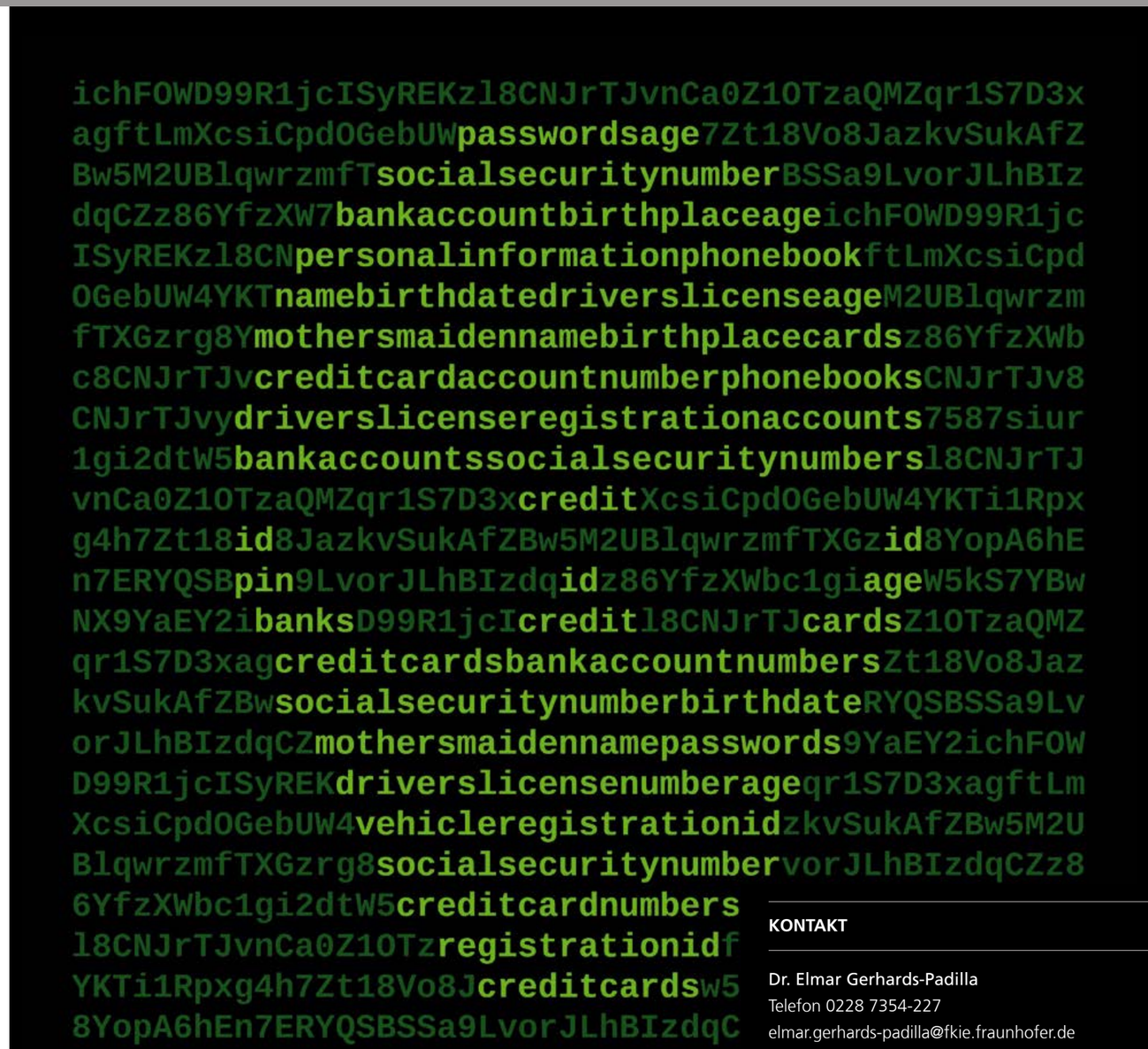
Rootkits gehören zu den unbekannteren Bedrohungen im Cyberspace. Sie verbergen sich meist tief im Betriebssystem und bedrohen ganze IT-Systeme. Informatiker der Forschungsgruppe Cyber Analysis haben ein Programm entwickelt, das dabei hilft, die hartnäckige Malware aufzuspüren.

In der Debatte um Cyber-Gefahren fallen Begriffe wie »Viren«, »Trojaner« oder »Phishing«. Nahezu jeder hat von diesen Bedrohungen gehört. »Rootkit« hingegen ist ein weniger geläufiger Begriff – obwohl es sich dabei um eine äußerst gefährliche und hartnäckige Bedrohung handelt.

Die Diplom-Informatiker Peter Weidenbach und Raphael Ernst, wissenschaftliche Mitarbeiter bei FKIE, haben sich der Rootkits angenommen. »Einer unserer Studenten hat sich im vergangenen Jahr im Rahmen einer Bachelor-Arbeit mit Rootkits befasst«, erklärt Ernst, »wir geben unseren Studenten gerne aktuelle Themen. Die Ergebnisse der Arbeit waren interessant, damit haben wir weitergearbeitet«. Generell erfordern Rootkit-Angriffe hohes technisches Verständnis. Sie seien daher wenig verbreitet und prädestiniert für »persistierende, langanhaltende Angriffe auf hochrangige Ziele«, erläutert Ernst. So funktioniere auch die vor Jahren in die Schlagzeilen geratene »Stuxnet«-Malware. Ebenso nutzten Firmen aus der Unterhaltungsindustrie in der Vergangenheit Rootkits, um ihren Kunden unbemerkt eine Kopiersperre auf den Rechner zu laden.

»Ein Rootkit versteckt sich meistens als integraler Bestandteil des Kernels«, erläutert Weidenbach das Funktionsprinzip, und Ernst ergänzt: »So eine Malware im Kernelbereich kann alles tun und ist unheimlich mächtig. Und sie sind quasi nicht auffindbar.« Denn weil es auf dem Prozessor im privilegierten »Ring-0« agiert, könne ein Rootkit nicht nur alles anrichten, sondern sich auch wirkungsvoll verbergen. So tragen sich Rootkits selbst aus der Liste mit den laufenden Prozessen aus und sind nicht auffindbar.

Der Student hat das Open-Source-Programm entworfen, das Rootkits finden können soll. Dazu nutzte er nicht die bekannten Ansätze, für die alte mit aktuellen Systemabbildern verglichen werden, sondern suchte im Betriebssystem-Kernel nach Anomalien, die ein Rootkit erzeugt, um sich zu verstecken und dennoch agieren zu können. Weidenbach: »Es gibt ein paar Funktionen an ein, zwei zentralen Stellen, die alle Rootkits benötigen.« Um diese aufzuspüren, müsse man im physikalischen Speicher charakteristische Byte-Folgen suchen. Das könne zu falschem Alarm führen, dennoch biete die Software die Möglichkeit, beliebige Rootkits zu finden, während die klassischen Verfahren nur bekannte Rootkits finden können. Das Programm, nun unter dem Namen KEROKID, haben Weidenbach und Ernst verallgemeinert, nutzerfreundlicher gestaltet und frei zur Verfügung gestellt. Mit dem Ergebnis, das sie in der Fachzeitschrift für Informationstechnik »iX« veröffentlichten, sind sie sehr zufrieden: »Das Programm bietet einen Proof-of-Concept, es gibt viele Zugriffe und auch ein paar Firmen haben angefragt«, freut sich Ernst. Immerhin sei man mit dem Programm in bestimmten Bereichen der Rootkit-Erkennung »weitgehend konkurrenzlos«.



KONTAKT

Dr. Elmar Gerhards-Padilla
Telefon 0228 7354-227
elmar.gerhards-padilla@fkie.fraunhofer.de

V / TEILAUTONOME UNTERSTÜTZUNGSSYSTEME

Um die Sicherheit von Soldaten und zivilen Einsatzkräften zu gewährleisten, werden zur Aufklärung oder zum Lastentransport häufig mobile Roboter eingesetzt. FKIE entwickelt für solche Robotersysteme – zu Land, zu Wasser und in der Luft – innovative Steuerungslösungen und intelligente Assistenzfunktionen.

SCHLUSS MIT LUSTIG: SERIOUS GAMING

Wie reagiert der Mensch, wenn aus Spaß Ernst wird? Für die Abteilung Human Factors testet Martin Westhoven Konzepte virtueller Welten aus Spielen im Hinblick auf ihre Einsatzmöglichkeiten für die Simulation gezielter Operationen: Einsatz- oder Rettungskräfte sollen Übungen in virtuell erstellten Häusern durchführen können.

Auf den ersten Blick erscheint der Arbeitsplatz von Informatiker Martin Westhoven wie der wahr gewordene Traum eines Computerspiel-Nerds: Riesige Monitore, Gamepads und Gamer-Utensilien – und über den Schirm flimmert ein angesagtes 3D-Spiel. Doch ganz im Gegenteil: Westhoven erprobt anhand dieses Equipments mit wissenschaftlichen Methoden, was eigentlich geschieht, wenn aus Spaß Ernst werden soll.

An der Spielkonsole tauchen Menschen in zunehmend realistischer anmutende virtuelle Welten ein. Hard- und Software der Unterhaltungsindustrie setzen stetig neue Standards. »Mit solchen Konzepten ist es vorstellbar, jemandem Tätigkeiten beizubringen, beispielsweise ganz konkret, sich in einem noch unbekannten Gebäudekomplex zurechtzufinden oder Teamoperationen einzustudieren«, erläutert Westhoven sein wissenschaftliches Interesse.

Die Grenzen der Nutzung gilt es so zu erforschen, dass verbindliche Regeln für den professionellen Umgang mit diesen Technologien aufgestellt werden können. »Bei einem Spiel kann ich jederzeit sagen: ›Ich mache eine Pause!‹«, erklärt Westhoven, »Im professionellen Bereich geht das normalerweise nicht.« Die Unterhaltungsindustrie liefert die Hardware und »wir können uns auf die Frage konzentrieren: ›Was kann man damit machen?‹«, erklärt Westhoven. »Nur die 3D-Modellierung und Szenariengestaltung auf Basis vorhandener Spiele-Engines stehen wissenschaftlichen Fragestellungen dann noch im Weg.«

Abteilungsleiter Dr. Thomas Alexander erklärt das Ziel der Untersuchungen bei Fraunhofer FKIE: »Unsere Aufgabe sehen wir darin, das Potenzial solcher virtuellen Welten für den professionellen Einsatz herauszufinden. Dazu arbeiten wir experimentell daran, welche Technologien für den Wissenstransfer von Bedeutung sein können und wie der Transfer effektiv funktionieren kann.« Verschiedene Studien, die in jüngerer Vergangenheit gemacht wurden, haben vielversprechende Ergebnisse geliefert, aber auch die Probleme im Umgang mit der Technik aufgezeigt.

Sei es mit einem »Head-Mounted Display« oder in einer »Cave«-Umgebung – je tiefer man in eine virtuelle Welt eintaucht, desto größer ist der Einfluss auf das Orientierungsvermögen. So sieht man mit der Oculus-»Taucherbrille«, die die virtuelle Welt über zwei Displays unmittelbar vor Augen führt, sprichwörtlich die eigene Hand vor Augen nicht mehr. Das zieht spannende ergonomisch-psychologische Fragestellungen in Bezug auf das eigene Präsenzempfinden in der virtuellen Welt nach sich, nicht zuletzt nach negativen Begleiterscheinungen, wie der »Simulatorkrankheit«. So seien Interaktion und Intuitivität bereits durch geringste Abweichungen gestört und können Schwindel und Desorientierung zur Folge haben. Westhoven: »Da stellt sich dann rasch die Frage, wie anstrengend es ist, nur einen Flur entlangzulaufen.«

Mit den Studien des FKIE-Teams können Messverfahren für die Sicherheit in der Anwendung entwickelt und die Einsatzszenarien vielfältiger und komplexer gestaltet werden.

KONTAKT

Dr. Thomas Alexander
Telefon 0228 9435-480
thomas.alexander@fkie.fraunhofer.de

RISIKOFREIE RETTUNG VON VERWUNDETEN

Die Rettung von Verwundeten ist eine überaus wichtige, für die Einsatzkräfte oft jedoch auch hochriskante Aufgabe – im militärischen Gefecht oder bei Naturkatastrophen und Unfällen. Robotersysteme, die Aufgaben wie das Auffinden oder gar die Rettung von Verletzten übernehmen können, stellen daher eine große Entlastung dar. Ein solches Mehrrobotersystem präsentierte ein Team des FKIE beim ELROB-Wettbewerb 2014 in Warschau.

Das Robotersystem, das zum Verwundetentransport dienen soll, besteht zunächst aus einem sogenannten Manipulator, einem Roboterarm, für den Dr. Bernd Brüggemann und seineKollegen aus der Abteilung Kognitive Mobile Systeme (CMS) eine Intuitive Steuerung entwickelten. Eine Demonstration zeigt die Besonderheit: Gelenkt wird der Arm mittels einer mit Inertialsensoren präparierten Jacke, also intuitiv mit den eigenen Armbewegungen –und nicht, wie üblich, mit einem Joystick. Die Entwicklung solch intelligenter Assistenzfunktionen ist einer von zwei Ansätzen, mit denen das FKIE die Bedienung von unbemannten Fahrzeugen merklich vereinfachen will. Der zweite Ansatz widmet sich der Verbesserung des Autonomiegrades.

Für den ELROB-Wettbewerb 2014 in Warschau setzt das FKIE-Team den Arm auf die fernsteuerbare Roboterplattform »GARM«, die in Kooperation mit der Schweizer RUAG/ armasuisse W+T konstruiert wurde und dank neuester Lithium-Ionen-Batterien und einem Kettenfahrwerk für schwieriges Terrain wie Geröll und Schutt oder auch unebene Grasflächen geeignet ist. »Für das Team ist es natürlich spannend, den Roboter möglichst nahe an der Wirklichkeit zu testen«, erläutert Brüggemann. Neben solch einem militärischen Rettungsszenario kann der Roboter auch in zivilen Szenarien zum Einsatz kommen, beispielsweise für die Rettung von Menschen nach einem Chemieunfall, die für die Einsatzkräfte lebensgefährlich wäre.

Der Auftrag im Wettbewerb war klar formuliert: Ein Verwundeter – simuliert durch einen Dummy mit wahlweise zehn, 35 oder 74 Kilogramm Gewicht – musste zunächst auf einem Feld gefunden und dann ein Bild sowie die exakten GPS-Daten an die Einsatzleitung geschickt werden. Und die wichtigste Aufgabe war natürlich, den Verletzten aus der Gefahrenzone abzutransportieren. Die Aufgabe bestimmte das Design des Robotersystems, die Fähigkeiten der einzelnen Systemkomponenten hingegen das Vorgehen des Teams: »GARM« besitzt zwar als einziger Roboter seiner Klasse die Fähigkeit bis zu 200 Kilogramm Gewicht zu transportieren, der Roboterarm jedoch kann lediglich bis zu fünf Kilo heben. Team und System lösten das Problem, indem sie einen Haken an der Ausrüstung des Soldaten-Dummies befestigten und ihn zu einem Unterstand in rund 150 Metern Entfernung zogen – dies alles ohne Sichtkontakt.

Den ersten Platz sicherte sich das Team nicht nur, weil es in der Lage war, den schwersten Dummy zu transportieren. Auch die zeitsparende Steuerung brachte wichtige Punkte ein und ist im realen Einsatz ein lebensrettender Faktor: Sieben Minuten eher als die Zweitplatzierten brachte das FKIE-Team seinen »Verwundeten« in Sicherheit. »Das ist der intelligenten Steuerung zu verdanken, die auch in Stresssituationen eine einfache Bedienung gewährleistet«, ist Brüggemann überzeugt. Sie wurde mit dem Sonderpreis »Best Novel Scientific Solution« honoriert.

»Unser System hat sich bewährt«, konstatiert Brüggemann. Dass ein solcher Transport von Verwundeten – je nach der Beschaffenheit des Untergrundes – möglicherweise als holprig empfunden werde, stellt er nicht in Abrede. Nicht anders jedoch würde auch ein Soldat vorgehen, der einen verwundeten Kameraden aus einer Gefahrenzone befördern wolle. Es gilt, was ein Angehöriger des polnischen Militärs anmerkte: »Was ist schlimmer, als die Person einfach liegen zu lassen?«

Im unmittelbaren Umgang mit Menschen sieht Brüggemann ohnehin noch Entwicklungsbedarf: »Ein Verwundeter, zu dem plötzlich ein riesiger Roboter mit einem großen Haken herangefahren kommt, dürfte kaum zu dessen Beruhigung beitragen.« Daher soll im nächsten Schritt die Ansprache des Verwundeten per Funk ermöglicht werden. Biosensoren, mit denen ein Rettungsroboter ausgestattet wird, könnten die Sanitäter über die Vitaldaten wie etwa Puls und Sauerstoffwerte des Verwundeten informieren. Brüggemann: »Das würde für einen Verwundeten eine deutliche Steigerung seiner Überlebenschancen bedeuten.«

Noch sind bei der Bundeswehr keine Roboter zur medizinischen Evakuierung im Einsatz. Aber Brüggemann, der 2014 seine Promotion über die Koordination und Kooperation von Mehrrobotersystemen abschloss, sieht das Potenzial für Roboter in diesem Bereich und arbeitet mit seinem Team daran, einen solchen Einsatz möglich zu machen.

KONTAKT

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

SPÄHPANZER OHNE FENSTER

Eine effektive Panzerung ist für die Insassen von Fahrzeugen im Gefechtsfeld eine Lebensversicherung. Doch geht Panzerung immer zulasten der eigenen Sicht, daher sollen Kameras und Monitore Abhilfe schaffen. Ein Team der Abteilung Systemergonomie erforscht die effektivsten Möglichkeiten, mit denen Fahrzeuglenker in Zukunft womöglich auch ganz ohne Fenster auskommen können.

Im großen Werkraum der Abteilung für Systemergonomie laden gleich mehrere Aufbauten zu einer Spritztour ein – freilich ohne dass sich der Fahrer auch nur einen Meter von der Stelle bewegt. Sämtliche Ausflüge dienen ausschließlich wissenschaftlichen Zwecken und sind rein virtueller Natur. Dafür, dass diese so realistisch wie nur möglich wirkt, sorgt die Abteilung von Prof. Dr. Frank Flemisch, und für dieses Projekt besonders die wissenschaftlichen Mitarbeiter Alexander Krasni, Pasqual Boehmsdorff und Thorsten Linder.

Um den erhöhten Bedarf an gepanzerten Fahrzeugen im militärischen Bereich decken zu können, ist der Einsatz virtueller Steuerungsmöglichkeiten von zunehmender Bedeutung. Das FKIE-Team unter Leitung von Prof. Dr. Frank Flemisch erforscht die verschiedenen Einsatzmöglichkeiten für eine effektive Sichtunterstützung in gepanzerten Fahrzeugen. Dabei helfen Kameras rund um das Fahrzeug, eingeschränkte Sicht ganz oder zumindest teilweise auszugleichen.

An seine Grenzen stößt diese Technik dort, wo ein Wechsel stattfindet, etwa bei Monitoren in den A-Säulen der Fahrzeuge links und rechts der Frontscheibe. »Das Problem ist, dass sich das Auge beim Übergang zwischen Fenster und Monitor zwischen Fern- und Nahsicht immer neu fokussieren muss«, erläutert Krasni. Das ist auf Dauer zu ermüdend für den Fahrer, so ihre Erkenntnis. Gute Ergebnisse liefert hingegen eine vollständig virtuelle Rundumsicht auf 160 Grad mithilfe von fünf um den Fahrer angeordneten Monitoren.

Diese Lösung birgt allerdings ihrerseits ein ergonomisches Problem: Um Fahrzeuge wie etwa den Bundeswehr-Spähpanzer Fennek damit nachzurüsten, ist der Raum in der Regel zu beengt. Krasni: »Der Wagen müsste um diese Lösung herumgebaut werden.«

Daher sehen die Forscher das größte Potenzial in den Oculus-Brillen, die dem Fahrer ein Bild der Umgebung auf zwei kleinen TFT-Monitoren unmittelbar vor Augen führen. Damit ist das Platzproblem zwar gelöst, doch erweist sich hier die Technologie als noch nicht ausgereift: Die Verzögerung der Übertragung, insbesondere wenn der Fahrer den Kopf dreht, ist derzeit noch zu groß, die Auflösung zu niedrig. Brillen, die diese Standards bieten, gibt es bereits, allerdings sind sie noch sehr teuer. Außerdem gilt es hier zu bedenken, dass der Fahrer weder die Instrumente noch den Rückspiegel sehen kann. Diese müssten virtuell eingebaut werden. »Dennoch erkennen wir hier das vielversprechendste Potenzial für die Zukunft«, erklärt Boehmsdorff.

KONTAKT

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

HIGHLIGHTS 2014/15

Der Dialog mit Kunden, Austausch und Networking mit der wissenschaftlichen Community, der Öffentlichkeit und dem Nachwuchs nahm auch dieses Jahr wieder breiten Raum ein: Fraunhofer FKIE präsentierte sich auf verschiedensten Veranstaltungen. Das Spektrum reicht vom »Technologieforum« über den erfolgreichen »Bonner Dialog für Cybersicherheit« bis hin zum »Girls' Day«.

BDCS
Bonner Dialog für Cybersicherheit

mit der Deutschen Telekom

Fest etabliert im Bonner Terminkalender ist der 2013 gestartete und halbjährlich ausgerichtete »Bonner Dialog für Cyber-Sicherheit«, eine Kooperation der FKIE-Abteilung von Prof. Dr. Michael Meier mit der Deutschen Telekom und der »Allianz für Cyber-Sicherheit«. Die Veranstaltungsreihe gewann die Stadt Bonn 2014 als Mitveranstalter hinzu. Oberbürgermeister Jürgen Nimptsch hob im November im alten Rathaus das versammelte Fachwissen hervor: Bonn sei ein »Hidden Champion für Datensicherheit und Datenschutz«.

Die Themen der Dialoge 2014 waren »Cyber Security for the Masses« und »Industrie 4.0«: »Wer versucht, den Speiseplan der Kantine in gleicher Weise zu schützen wie die sensibelsten Konstruktionspläne, der wird Schiffbruch erleiden«, prophezeite Prof. Dr. Peter Martini, Leiter des Fraunhofer FKIE und des Instituts für Informatik 4 an der Universität Bonn, der das Thema Cyber Security intensiv vorantreibt. »Wir brauchen Konzepte abgestufter Sicherheit – im Cyberspace wie auch in der physischen Welt«, erklärte er im Austausch mit Fachleuten aus Politik und Wirtschaft. Prof. Dr. Matthew Smith, der sich an seinem Lehrstuhl dem Thema »Usable Security and Privacy« widmet, forderte beim 3. BDCS, IT-Sicherheit solle »sicher und benutzbar« sein: Technik müsse sich dem Menschen anpassen, soll die breite Masse von digitaler Sicherheit profitieren.

CeBIT Hannover 2014

Das Strategie- und Positionspapier »Cyber-Sicherheit 2020« mit Empfehlungen zur künftigen Ausrichtung der IT-Sicherheitsforschung überreichte der Präsident der Fraunhofer-Gesellschaft auf der weltgrößten Computermesse CeBIT in Hannover an die Bundesministerin für Bildung und Forschung Prof. Dr. Johanna Wanka und den Bundesminister des Innern Dr. Thomas de Maizière. FKIE-Institutsleiter Prof. Dr. Peter Martini gehörte als einer der beiden Initiatoren des Positionspapiers und Mitglied des vierköpfigen Redaktionsteams zu der Fraunhofer-Delegation. »Die ersten Reaktionen sind überaus positiv«, resümierte Prof. Martini anschließend.

HIGHLIGHTS
2014/15

9th Workshop Sensor Data Fusion

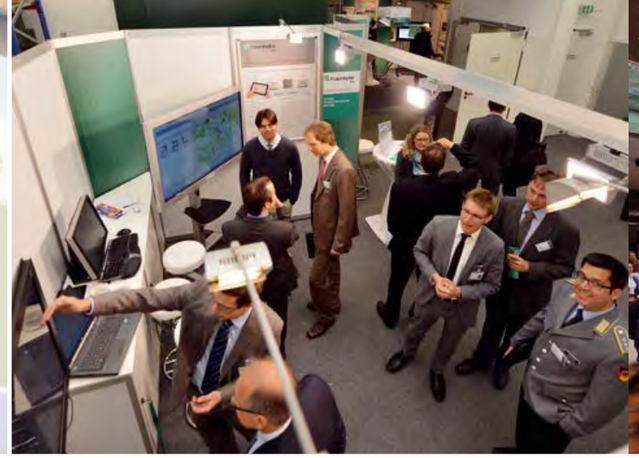
Nutzer, Software-Entwickler, Ingenieure und Forscher im Bereich der Sensordatenfusion nahmen im Oktober am dreitägigen Workshop »Sensor Data Fusion: Trends, Solutions and Applications« im Universitätsclub Bonn teil, ausgerichtet durch das Fraunhofer FKIE. Organisiert wurde die neunte Auflage dieses Workshops von Priv.-Doz. Dr. Wolfgang Koch, dem Leiter der FKIE-Abteilung Sensordaten- und Informationsfusion, und Dr. Felix Govaers, FKIE-Wissenschaftler auf dem Gebiet der Sensordatenforschung. Im Vordergrund standen Maßnahmen, Entwicklungen und neue Anwendungsmethoden sowohl für den zivilen Bereich, etwa den Logistik- oder Gesundheitssektor oder die produzierenden Industrie, als auch für den wehrtechnischen Bereich.

Immer größer werdende Datenmengen sind in der Lage ein immer aktuelleres und detaillierteres, aber auch komplexeres Porträt der Gegenwart abzubilden. Die Teilnehmer aus Wissenschaft und Industrie erörterten die Frage, wie diese anschwellenden Datenströme für den Menschen beim Treffen von Entscheidungen auf unterschiedlichen Hierarchieebenen nicht zu einer Überlastung führen, sondern sinnvoll zu seiner unmittelbaren Unterstützung und Entlastung zusammengeführt werden können.

FKIE Technologieforum 2014

Eine Auswahl an Exponaten aus allen Abteilungen des Instituts präsentierte im August das »Fraunhofer FKIE Technologieforum 2014« in Zusammenarbeit mit dem Bundesministerium für Verteidigung. Einen Tag lang bot die Hausmesse geladenen Gästen Gelegenheit, Einblicke in die Arbeit vor Ort zu gewinnen: Über 25 Exponate und Demonstratoren in der Robotikhalle, einem eigens aufgebauten Zelt oder in Laboren veranschaulichten das vielfältige Panorama der Forschungsarbeit am FKIE.

Eine Reihe von Vorführungen und Kurzvorträgen begleitete die Ausstellung: Impulsvorträge am Vormittag boten einen ersten Einblick, vom »multisensoriellen Schutz von Häfen, Konvois oder fliegende Plattformen« bis zum »Robotersystem zur Aufspürung und Rettung von Personen«. War das Interesse geweckt, konnten sich die Gäste ausführlicher über gefährliche Botnetze, Unterwassernetzwerke oder eine »Battle Management Language als Interlingua zwischen Mensch und System« informieren. Die Besucher hatten nicht nur die Möglichkeit zu Fragen und Diskussionen, sondern auch zu persönlichen Gesprächen mit den Wissenschaftlern. Bei schönem Wetter und einem Imbiss wurden die Gespräche auch draußen geführt und entsprechend positiv fiel das Echo aus.



Internationale Luft- und Raumfahrtausstellung ILA

Spektakuläre Darbietungen und spannende Neuentwicklungen auf dem Gebiet der Aviatik verspricht alle zwei Jahre die Internationale Luft- und Raumfahrtausstellung, kurz ILA, in Berlin: Die Abteilung Sensordaten- und Informationsfusion (SDF) des Fraunhofer FKIE stellte bei der »Berlin Air Show 2014« im Mai einen Teil ihrer Arbeit im Bereich der unbemannten Luftfahrt vor und demonstrierte den Einsatz der ausgestellten sowie weiterer Luftfahrzeuge als Sensorplattformen. Schwerpunkt der Forschungsarbeit am FKIE ist die Fusion umfangreicher Datenströme aus einander ergänzenden Sensorquellen; in einem Impulsvortrag im Rahmen der ILA-Konferenzen stellte FKIE-Diplom-Informatiker Marek Schikora interessante Perspektiven für die Nutzung unterschiedlicher Sensordaten in der vernetzten Luftfahrt vor.

Thementag »Unbemannte Systeme«

2014 wurde der Thementag »Unbemannte Systeme« von FKIE ausgerichtet. Dieser als Dialogreihe gedachter Workshop innerhalb des Fraunhofer VVS hat den Technologietrend der autonomen und teilautonomen mobilen Systeme sowie deren Kooperation und Assistenzsysteme zum Thema. So wurden 2014 die Bedarfsträger und -decker in Dialog mit der Forschung gebracht, um auf diese Weise Zukunftsperspektiven insbesondere im Bereich von bodengebundenen Systemen und kleinen Luftsystemen aufzuzeigen.

Woman & Work

Doch: mehr Frauen gehören in herausfordernde Berufe! Frauenkarrieren stehen nicht nur in der Politik hoch im Kurs, auch die Fraunhofer-Gesellschaft unterstützt Frauen bei ihrer Karriereplanung. Mit einem starken Frauenteam präsentierte sich das Fraunhofer FKIE daher im Juni bei der »Women & Work«, der Karrieremesse für Frauen im WCCB in Bonn: Verwaltungsleiterin Ursula Fuchs, Herrad Schmidt aus der Unternehmenskommunikation und die wissenschaftliche Mitarbeiterin Jessica Conradi zeigten Interessentinnen vielfältige Berufsperspektiven am Institut auf, und nicht allein im Bereich der angewandten Forschung. Mit einer eigenen Kampagne und einem Mini-Slam machte unser Institut auf sich aufmerksam: Viele Frauen und Bewerberinnen nutzten diese Gelegenheit zur Kontaktaufnahme und informierten sich über die Möglichkeiten, wie sie Familie und eine Karriere bei Fraunhofer vereinbaren können.

Girls' Day
Mädchen-Zukunftstag

Girls' Day: Einblick in Wissenschaft und Technik

Labore, Büros und Werkstätten öffnete das Fraunhofer FKIE auch 2014 wieder zum Girls' Day: Schülerinnen ab Klasse 5 durften im März für einen Tag die Bereiche Technik, IT und Forschung erkunden, Wissenschaftler und Techniker des FKIE gewährten den Nachwuchsforscherinnen konkrete Einblicke in Projekte auf dem Wachtberg und beantworteten ihre Fragen. Interaktive Darstellungen illustrierten die Arbeit am Institut. Die Fraunhofer-Gesellschaft unterstützt das Ziel, mehr Frauen in die angewandte Forschung zu bringen.

GESPRÄCH MIT **JUN.-PROF.DELPHINE CHRISTIN**

PRIVATSPHÄRE IM CYBER-SPACE: »WIR WOLLEN NICHT DIE SPASSVERDERBER SEIN!«

Frau Professor Christin, welches Gerät, das Ihnen den Alltag erleichtert, haben Sie sich jüngst zugelegt?

CHRISTIN: Ich habe mir einen neuen PC gekauft, besitze aber kein Smartphone. Ich muss zugeben, ich bin immer mit meinem »vintage«-Handy unterwegs. Es gibt verschiedene Gründe dafür: Mein Handy kann zwar auch meinen Aufenthaltsort verraten, aber bei weitem nicht so genau wie ein Smartphone. Außerdem möchte ich meinen Akku nicht täglich laden müssen und zudem ist mir die Möglichkeit, zwischen Privatleben und Beruf zu trennen, sehr wichtig. Die Informationen, die auf meinem Handy sind, bleiben so beispielsweise von meinen E-Mails getrennt.

Privatsphäre im Cyberspace ist Ihr Forschungsfeld. Welches Gerät, das Sie nutzen, bereitet Ihnen denn diesbezüglich die größten Sorgen?

CHRISTIN: Ganz klar mein Computer. Es fehlt einfach die Transparenz dessen, was im Hintergrund alles passiert – selbst dann, wenn man auf diesem Gebiet Expertin ist. Man weiß etwa nicht, welche Informationen über einen wo verfügbar werden: Wenn ich etwas online kaufe, wird das mit anderen Daten verknüpft? Was genau macht ein Online-Shop mit meinen Daten; Verkauft er sie oder betreibt er damit Marktforschung? Man verliert die Kontrolle, sobald man sein Einkaufverhalten im Internet preisgibt.

Sind sogenannte Smart Devices ein Problem in Sachen Privatsphäre?

CHRISTIN: Die »Intelligenz« der Geräte ist gar nicht das zentrale Problem, es ist eher ihre Kombination. Ein Lichtschalter gilt eher nicht als »sehr intelligent«, aber ein Lichtschalter genügt, um festzustellen, ob jemand anwesend ist oder nicht. Und nur daran, wie lange oder in welcher Reihenfolge Lichtschalter ein- oder ausgeschaltet werden, kann man die Verhaltensmuster verschiedener Personen in einem Haushalt unterscheiden, wie ein Versuch gezeigt hat. Und mit neuen, sogenannten »Smart meters«, intelligenten Zählern, die den Stromverbrauch ganz exakt messen, ist sogar nachvollziehbar, welche Geräte gerade eingeschaltet sind oder welcher Film gerade im TV läuft.

Sie plädieren dafür, den »Nutzer in den Mittelpunkt« zu stellen. Was bedeutet das?

CHRISTIN: Man kann tolle technische Lösungen entwickeln, aber wenn man den Nutzer nicht ins Spiel nimmt, besteht das Risiko, dass auch die beste Technologie nicht angewendet wird – entweder die grundlegende Technologie, die man schützen möchte, oder die Schutzmechanismen selbst. Man sieht es bei E-Mail-Verschlüsselungen: Die Technologie gibt es seit Jahrzehnten, aber so gut wie niemand benutzt sie. Ein Nutzer muss wissen: Was passiert hinter den Kulissen? Welche Daten über mich gebe ich preis? Habe ich Kontrolle über diese Daten? Und welche Kompromisse bin ich bereit einzugehen, um Angebote im Netz nutzen zu können?

Neue Hard- und Software führt zu verändertem Nutzerverhalten. Was ist Ihre Aufgabe dabei?

CHRISTIN: Das betrifft nicht nur den Bereich Privatsphäre, sondern auch den Bereich Security. Es gibt immer Leute, die versuchen anzugreifen, und man muss Lösungen dagegen suchen. Man läuft dem immer ein wenig hinterher, aber gerade deshalb sollte man dem sogenannten Privacy-by-design-Konzept folgen und die zu schützende Privatsphäre der Leute mitbedenken, wenn man eine neue Anwendung entwickelt. Das Problem sind die verschiedenen Interessen: Die Industrie möchte neue Märkte erreichen, die Nutzer ihre Privatsphäre schützen, es gibt die Regulierung durch das Datenschutzrecht und so weiter. Es ist die Frage, wer fängt an, die Privatsphäre wie zu schützen – jeder trägt einen Teil der Verantwortung.

Welche Hilfestellung bietet Ihre Forschung dazu?

CHRISTIN: Wir arbeiten primär auf der technologischen Ebene, aber wir realisieren derzeit auch Projekte mit juristischen Aspekten. Dabei setzen wir uns mit der Frage auseinander, wie man die Richtlinien der EU einfach implementieren und beispielsweise Transparenz gewährleisten kann. Nehmen wir zum Beispiel ein Smart Home, in dem die Bewohner sehen können sollen, welche Daten gesammelt werden. Wir versuchen allgemeingültig herauszufinden, wie das verwirklicht werden kann.

Was geben Sie Ihren Studenten mit auf den Weg?

CHRISTIN: Es ist ein Fach, das unbedingt interdisziplinär zu sehen ist. Da ist zum einen der ökonomische Aspekt, denn Daten haben einen Wert. Auch die Selbstdarstellung im Netz ist von Bedeutung, hier spielen wiederum juristische Aspekte eine wichtige Rolle. Wir sind heutzutage nicht mehr in einem Netzwerk mit Computern, die fest verbunden sind, sondern leben zukünftig in Smart Cities mit verschiedenen, beweglichen Geräten mit unterschiedlichen Ressourcen. Nicht zuletzt aufgrund dieser stetig zunehmenden Komplexität ist es eine große Herausforderung, in diesem Bereich zu arbeiten.

Muss man den Umgang mit sozialen Medien üben?

CHRISTIN: Studien haben gezeigt, dass es drei Usertypen gibt: Diejenigen, die sorglos mit ihren Daten umgehen, und die, die sehr vorsichtig und zurückhaltend damit umgehen. Den größten Anteil nehmen aber die ein, die dazwischen liegen: Die überlegen sich, welchen Vorteil sie haben und wägen dann ab, dafür ihre Daten herzugeben – oder eben nicht. Beim Girls' Day habe ich Mädchen im Alter zwischen 10 und 14 gefragt, was für sie »Privatsphäre« ist – und ich war erstaunt, wie gut sie dafür sensibilisiert waren. Das Wissen, dass man nicht alles bei Facebook posten sollte, ist vorhanden.

Wie kann man die, die zu sorglos sind, an die Hand nehmen?

CHRISTIN: Ich würde das nicht unbedingt korrigieren wollen. Jeder soll die Freiheit haben, selbst zu entscheiden, was er mit seinen Daten macht. Aber man sollte die Konsequenzen kennen, und da setzt meine Arbeit an: »Was könnte passieren, wenn…« Jeder weiß, dass Rauchen tödlich ist, aber man kann entscheiden, es trotzdem zu tun. Da endet meine Verantwortlichkeit.

WISSENSCHAFTLICHE PRÄSENZ

Wie weist man die Nutzer auf drohende Konsequenzen hin?

CHRISTIN: Es ist schwer, dieses Bewusstsein zu schaffen. Man könnte Popup-Meldungen mit einer Warnung einbauen, aber den Benutzern werden ohnehin schon zu viele Warnungen angezeigt. Wir haben einmal für eine Handy-App einen Vorschlag gemacht zu den Daten, die gesammelt werden. Statt einer Warnung in Texten haben wir Bilder gezeigt, die verschiedene Szenarien illustrierten: Wenn beispielsweise die Lokation feingranular gesammelt wurde und das Risiko besteht, dass jemand dem Nutzer des Handys folgt. So sollte eine Schockwirkung hervorgerufen werden, vergleichbar mit Warnungen auf Zigarettenpackungen. Das funktioniert vielleicht ein-, zweimal – aber dann muss man etwas anderes finden. Man muss den Menschen immer ein wenig austricksen.

Sensibilisierung bleibt ein wichtiges Thema.

CHRISTIN: Und wir reden hier jetzt nur über den Umgang mit Computer, Internet und Sozialen Medien, das ist schon ein alter Hut. In Zukunft wird immer häufiger zur Frage stehen, wie private Daten in intelligenten Gebäuden oder ganzen »Smart-Cities« verarbeitet werden. Wir sind da erst am Anfang im Bereich »intelligenter Umgebungen« oder »Big Data«, und auf diesem noch wenig erforschten Gebiet zu arbeiten ist wirklich spannend.

Wie verändert die allgegenwärtige Datenverarbeitung, das sogenannte »Ubiquitous Computing« den Alltag?

CHRISTIN: Früher stand mehreren Menschen nur ein einzelner Computer zur Verfügung. Mit der zunehmenden Verbreitung des PCs kam dann ein Mensch auf einen Computer. Heute ist es üblich, dass auf einen Menschen mehrere Geräte kommen. Ubiquitous Computing meint, dass man diese Rechner in seinem Umfeld gar nicht mehr wahrnimmt. Die Rechner sind überall, zum Beispiel im E-Reader: Man sagt nicht mehr, »Ich schalte jetzt den Computer ein«, sondern »Ich lese mein Buch«, als handele es sich um ein ganz normales Buch.

Reden wir über den Wissenschaftsstandort Bonn. Was führte Sie von der TU Darmstadt hierher?

CHRISTIN: Bonn hat mir die Möglichkeit geboten, nach meiner Promotion die wissenschaftliche Laufbahn als Juniorprofessorin hier einzuschlagen. Ich kannte auch schon einige Mitarbeiter aus der Arbeitsgruppe von Prof. Peter Martini, die ich bei verschiedenen Wissenschaftskonferenzen getroffen habe.

Welche Chancen liegen in der Professur auf der einen und der Tätigkeit am FKIE auf der anderen Seite?

CHRISTIN: Es ist schwierig, hier eine klare Trennung vorzunehmen. Wenn ich auftrete, trete ich immer zugleich für Fraunhofer und die Uni auf – und die Nähe von Forschung und Praxis ist sicher ein Vorteil. Die Kombination macht den Unterschied, das lässt sich am Beispiel »Privatsphäre« vielleicht gut zeigen: Das Thema ist eher schwer zu vermarkten. Die Industrie steht nicht gerade Schlange und sagt: »Bitte schützt die Privatsphäre unserer Kunden!« Wir wollen auch nicht die Spaßverderber sein und den Fortschritt bremsen. Meine Aufgabe an der Universität sehe ich darin, auf die Existenz der Gefahren hinzuweisen, Lösungen dafür zu finden und Methoden an die Studenten weiterzugeben. Und bei Fraunhofer habe ich die Möglichkeit, Szenarien zu erarbeiten und an anwendungsbezogenen Lösungen zu forschen. Diese Nähe zur Praxis ist sehr wichtig.

Welche Projekte möchten Sie für die Forschung im Bereich »Privacy« anstoßen?

CHRISTIN: Ein Projekt wäre, einen Prototyp eines »Smart-Space« zu entwerfen, um zu sehen, was man über die Nutzer erfahren kann, und darauf eine Gefahranalyse durchzuführen. Und dann natürlich Methoden zu entwickeln, um diese Gefahren zu beseitigen: Wie kann dem Nutzer Werkzeug an die Hand gegeben werden, mit dem er seine Privatsphäre schützen kann? Ein solches Projekt ist bei uns zurzeit in Planung.

Wie sind Sie eigentlich zu dem Thema »Privatsphäre« gekommen?

CHRISTIN: Ich habe in Frankreich ein Projekt im Bereich »Drahtlose Sensornetze« und später dann meine Promotion am Zentrum für IT-Sicherheit in Darmstadt begonnen. Ich bin keine Kryptoexpertin, daher war das Thema Privatsphäre ein guter Weg für mich, sowohl im Bereich »Sicherheit« als auch im Bereich »Sensoren« zu forschen. Bei einer Summer School, an der ich teilgenommen habe, war einer der Vortragenden Andrew Campbell, der erste, der den Begriff »Participatory Sensing« für die Erhebung von Sensordaten durch mobile Gruppen von Nutzern eingeführt hat. Natürlich war die Themenwahl auch ein wenig strategisch, denn dass dem Thema Privatsphäre zunehmend Bedeutung zukommen wird, liegt auf der Hand.

Vielen Dank für das Gespräch!

PROMOTIONEN UND BERUFUNGEN

PROMOTIONEN

Brüggemann, B.
»*Koordination und Kooperation in Mehrrobotersystemen unter spatialen Nebenbedingungen*«, Promotion zum Dr. rer. nat. an der mathematisch-naturwissenschaftlichen Fakultät der Universität Bonn.

Brunner, M.
»*Rough Terrain Motion Planning for Actively Reconfigurable Mobile Robots*«, Promotion zum Dr.-Ing. an der Fakultät für Maschinenwesen der RWTH Aachen University.

Haarmann, B.
»*Ontology On Demand – Vollautomatische Ontologieerstellung aus deutschen Texten mithilfe moderner Textmining-Prozesse*«, Promotion zum Dr. phil. an der philologischen Fakultät der Ruhr-Universität Bochum.

Kreuzer, S.
»*Beiträge zur robusten und effizienten Erschließung von digitalen Funksignalen*«, Promotion zum Dr. rer. nat. an der mathematisch-naturwissenschaftlichen Fakultät der Universität Bonn.

Oispuu, M.
»*Passive Emitter Localization by Direct Position Determination with Moving Array Sensors*«, Promotion zum Dr.-Ing. an der naturwissenschaftlich-technischen Fakultät der Universität Siegen.

Schikora, M.
»*Airborne Multiple Emitter Tracking by Fusing Heterogeneous Bearing Data*«, Promotion zum Dr. rer. nat. an der Fakultät für Informatik der Technischen Universität München.

Schüller, G.
»*Probabilistic Tracking with Database Systems*«, Promotion zum Dr. rer. nat. an der mathematisch-naturwissenschaftlichen Fakultät der Rheinischen Friedrich-Wilhelms-Universität Bonn.

AUSGEWÄHLTE ABSCHLUSSARBEITEN

MASTER- UND DIPLOMARBEITEN

Ayan, S.
»*Untersuchung und Erkennung fortgeschrittener Persistenzmechanismen bei aktueller Malware*« (Universität Bonn).

Ducke, M.
»*Kinodynamische lokale Trajektorienplanung für Roboter mit veränderbarem Fahrwerk*« (Universität Bonn).

Faust, A.
»*Fortentwicklung eines Prototyps zur Luftraumüberwachung durch Erweiterung des Visualisierungssystems, Integration datenbankgestützter Statistiken und Methoden zur Analyse luftfahrtspezifischer Problemstellungen*« (FH Bingen).

Fritz, A.
»*Aufnahme und Wiedergabe von Tastatur-Eingabesequenzen mittels Arduino Mikrocontroller*« (Universität Bonn).

Guevara Lazo, A. L.
»*Semantic Exploration of Binaries*« (Universität Bonn).

Haidar, S.
»*Nichtnegative Matrixfaktorisierung Quantitative Analyse einiger Verbesserungen des Basis-NMF-Algorithmus*« (Universität Bonn).

Hamdorf, S.
»*Konzeption der Benutzeroberfläche einer forensischen Analysesoftware anhand ergonomischer Designprinzipien*« (Universität Bonn).

Hartmann, T.
»*Automatisiertes Patchmanagement*« (Universität Bonn).

Hauck, S.
»*Heuristisches Verfahren zur Erkennung von Botnetz-Aktivitäten anhand von DNS-Failure-Graphen*« (FernUniversität Hagen).

Hoffman, F.
»*Radar Resource Management for the Search Function*« (Universität Bonn).

Jost, E.
»*Vergleich von Mechanismen zur Audiofilterung in Betriebssystemen*« (FernUniversität Hagen).

Kaur, J.
»*Countering Covert Channel-internal Control Protocols with Covert Channel-internal Control Protocols*« (Universität Bonn).

Khanna, A.
»*Authentication Mechanisms in Wireless Sensor Networks with Node Compromise to Observe Railway Facilities*« (Universität Bonn).

Meiling, M.
»*Coupling the Sensor Data Transmission and Management Protocol with an End-to-End Congestion Control Mechanism*« (Universität Bonn).

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

Naumann, J.
»*Symbolzuweisung in verdeckten Kanälen bei probabilistischer Mehrfachzuweisung*« (FernUniversität Hagen).

AUSGEWÄHLTE ABSCHLUSSARBEITEN

MASTER- UND DIPLOMARBEITEN

Naumann, M.
»*Kontrollprotokolle für steganografische Kanäle*« (FernUniversität Hagen).

Negi, S.
»*Evaluation and Optimization of IDP-MIKE-System over VHF Data Links*« (Universität Bonn).

Ofner, S.
»*Cross-Platform Implementation and Evaluation of the Proposed ILDA Digital Network (IDN) Protocol*« (Universität Bonn).

Öktem, A.
»*Person Identification and Topic Segmentation for News Broadcast Using Banner Text Recognition*« (Universität Bonn).

Pauksztelo, P.
»*Simulation of an Enterprise Network with Realistic User Behaviour*« (Universität Bonn).

Raikar, H.
»*Membership Handling in a Group Key Management after Network Failure or Crash*« (Universität Bonn).

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

Schmidt, W.
»*Covert Channels und Schutzmaßnahmen beim Festplatten-Blockcache im Genode Operating System Framework*« (FernUniversität Hagen).

Tasnim Oshim, Md.
»*Optimierte Signalraum-Konstellationen für hierarchische Modulation mit iterativer Decodierung*« (RWTH Aachen).

Traianos, G.
»*Signal classification based on spectral ACF features*« (Universität Bonn).

Urrigshardt, S.
»*Sprachdetektion in Breitbandsignalen*« (Universität Bonn).

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

Xu, R.
»*Hypervisor-Level Malware Analysis*« (Universität Bonn).

BACHELORARBEITEN

Anhaus, E.
»*Data Leakage Protection für Gebäude*« (FernUniversität Hagen).

Bergmann, N.
»*Erkennung von Code-Injektions-Angriffen durch Differenzierung von Speicherabbildern*« (Universität Bonn).

Christou, P.
»*Entwicklung und Evaluation einer Steuerung von Laser-Pong über eine Android-App*« (Universität Bonn).

Dombeck, A.
»*Live-Beobachtung von Botnetzen mittels Memorydump-Analyse*« (Universität Bonn).

Härpfer, H.
»*Implementierung eines Snort Normalizers für den BACnet/IP Network Layer*« (FernUniversität Hagen).

Herzog, M.
»*The Invisible Rootkit*« (Universität Bonn).

Jenke, T.
»*Clustering von Citadel-Packern*« (Universität Bonn).

Maqua, T.
»*Entwurf und Entwicklung einer graphischen Benutzeroberfläche für ein Softwareframework zum datenschutzkonformen kooperativen Sicherheitsmonitoring*« (Universität Bonn).

Neff, R.
»*Realisierung externer kryptographischer Funktionen für Arduino*« (Universität Bonn).

Oster, C.
»*Analyse von TCP-Verbindungen mit Markov-Modellen*« (Universität Bonn).

Plöger, S.
»*Entschleierung von Code mit Hilfe der LLVM Compiler Infrastruktur*« (Universität Bonn).

Ruland, T.
»*Einsatz von Kryptowährungen zur SPAM-Vermeidung in Bezug auf die Privatsphäre*« (Universität Bonn).

Siebert, N.
»*Plattformübergreifende Erkennung von Kernel-Rootkits in Memorydumps*« (Universität Bonn).

Stucke, J.
»*Verfahren zur Optimierung von Malware-Signatur-Datenbanken*« (Universität Bonn).

Thomanek, D.
»*Zustandsbasierte Anomalieerkennung in lokalen Netzwerken*« (Universität Bonn).

Tost, A.
»*Analyse der Normalisierungsmöglichkeiten im Kontext von Safety-Funktionen im BACnet*« (FernUniversität Hagen).

Trimborn, T.
»*Internet Routing Situationen mit GNS3 darstellen*« (Universität Bonn).

Weg, M.
»*Implementierung eines Active Wardens für BACnet*« (FernUniversität Hagen).

Weile, F.
»*Heuristische Detektion von Code-Injektionen in Speicherabbildern*« (Universität Bonn).

Yilmaz, T.
»*Tracking und Analyse eines bestehenden P2P Pay-Per-Install Botnetzes*« (Universität Bonn).

Zemanek, S.
»*Konzeption und Implementierung eines sicheren Messaging-Protokolls für mobile Endgeräte mit Fokus auf der Vermeidung von Metadaten*« (Universität Bonn).

AUSGEWÄHLTE LEHRVERANSTALTUNGEN

SOMMERSEMESTER 2014

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

Jun.-Prof. Dr.-Ing. D. Christin,
»*Mobile Sensing Systems*« (Praktikum), Universität Bonn.

Dr. F. Govaers,
»*Advanced Sensor Data Fusion in Distributed Systems*«
(Vorlesung & Übung), Universität Bonn.

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

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

Dr. W. Koch,
»*Einführung in die Sensordatenfusion*« (Vorlesung & Übung),
Universität Bonn.

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

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

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

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

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

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

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

Prof. Dr. P. Martini / Dr. W. Moll,
»*Selected Topics in Malware Analysis*« (Blockseminar),
Universität Bonn.

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

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

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

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

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

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

Prof. Dr. C. Schlick,
»*Aktuelle Forschungsfragen und Lösungsansätze in der
Arbeitswissenschaft*« (Kolloquium), RWTH Aachen.

Prof. Dr. C. Schlick,
»*Beiträge zur Produktions- und Dienstleistungsforschung*«
(Kolloquium), RWTH Aachen.

Prof. Dr. C. Schlick
»*Benutzerorientierte Systemgestaltung*«
(Vorlesung & Übung), RWTH Aachen.

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

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

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

Prof. Dr. M. Smith,
»*Sketching with Hardware – Kreative Mensch-Maschine-
Interaktion mit Hardware*« (Projektgruppe), Universität Bonn.

Prof. Dr. M. Smith,
»*Usable Security and Privacy*« (Vorlesung & Übung),
Universität Bonn.

Dr. S. Wendzel,
»*Datenkommunikation*« (Vorlesung), Hochschule Augsburg.

AUSGEWÄHLTE LEHRVERANSTALTUNGEN

WINTERSEMESTER 2014/15

Jun.-Prof. Dr.-Ing. D. Christin,
»*Privacy in Ubiquitous Computing*«
(Vorlesung & Übung), Universität Bonn.

Dr. M. Esch,
»*Principles of Distributed Systems*«
(Vorlesung & Tutorium), Universität Bonn/B-IT.

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

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

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

Dr. W. Koch / Dr. M. Schikora / J. Wildt / T. Fiolka,
»*Sensordatenfusion*« (Projektgruppe), Universität Bonn.

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

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

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

Prof. Dr. P. Martini,
»*Computer Networks, Mobile Communication and Network Security*« (Praktikum), Universität Bonn.

Prof. Dr. P. Martini / Dr. M. Esch,
»*Principles of Distributed Systems*«
(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*« (Projektgruppe), Universität Bonn.

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

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

Prof. Dr. M. Meier / Prof. Dr. P. Martini,
»*IT Security*« (Semesterbegleitendes Praktikum & Blockpraktikum), 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 IT Security*« (Seminar), Universität Bonn.

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

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

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

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

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

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

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

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

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

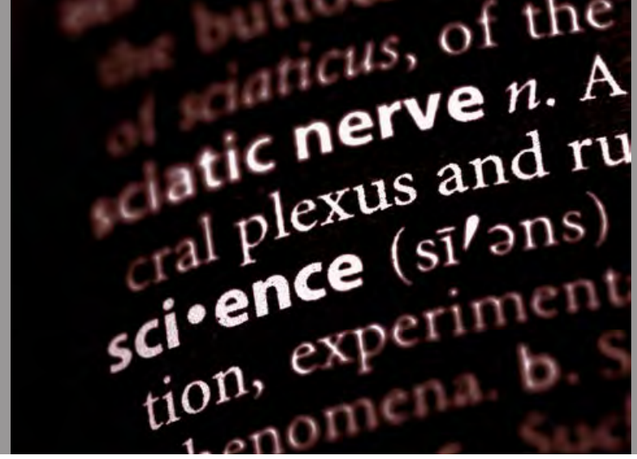
Prof. Dr. M. Smith,
»*Systemnahe Programmierung*«
(Vorlesung & Übung), Universität Bonn.

Prof. Dr. M. Smith,
»*Usable Security and Privacy*« (Praktikum), Universität Bonn.

Prof. Dr. M. Smith,
»*Security in Distributed Systems*«
(Praktikum), UniversitätBonn.

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

AUSGEWÄHLTE PUBLIKATIONEN



SDF

Verfasser	Titel
Demissie, D. & Berger, C.R.	*High-Resolution Range-Doppler Processing by Coherent Block-Sparse Estimation.* In: IEEE Transactions on Aerospace and Electronic Systems, 50(2014) pp. 843-857.
Demissie, B.	*Clutter cancellation in passive radar using GSM broadcast channels.* In: IET Radar, Sonar & Navigation, 8(2014) pp. 787-796.
Gonzalez. J. ; Battistello G. ; Schmiegelt, P. & Biermann J.	*Semi-Automatic Extraction of Ship Lanes and Movement Corridors from AIS Data.* In: 2014 IEEE International Geoscience and Remote Sensing Symposium (IGARSS). Quebec City, QC: 13-18th July 2014. IEEE Press, 2014, pp. 1847-1850. ISBN 978-1-4799-5775-0
Govaers, F. & Koch, W.	*Generalized Solution to Smoothing and Out-of-Sequence Processing.* In: IEEE Transactions on Aerospace and Electronic Systems, 50(2014) pp. 1739-1748.
Hörst, J. ; Oispuu M. & Koch, W.	*Accuracy Study for a Piecewise Maneuvering Target with Unknown Maneuver Change Times.* In: IEEE Transactions on Aerospace and Electronic Systems. 50(2014) pp. 737-755.
Koch, W.	*Towards Cognitive Tools: Systems Engineering Aspects for Public Safety and Security. In: IEEE* Aerospace and Electronic Systems Magazine. 15(2014)9, pp. 14-26.
Koch, W. & Govaers, F.	*On Decorrelated Track-to-Track Fusion based on Accumulated State Densities.* In: Information Fusion (FUSION) 2014. 17th International Conference on ... . Salamanca: 7-10th July 2014. IEEE, 2014, 6 p.
Mertens, M. ; Kirubarajan, T. & Koch, W.	*Exploiting Doppler Blind Zone Information for Ground Moving Target Tracking with Bistatic Airborne Radar.* In: IEEE Transactions on Aerospace and Electronic Systems, 50(2014) pp. 130-148.
Schikora, M. ; Gning, A. ; Mihaylova, L. ; Cremers, D. & Koch, W.	*Box-Particle Probability Hypothesis Density Filtering.* In: IEEE Transactions on Aerospace Systems, 50(2014) pp. 1660-1672.
Zemmari, R. ; Brötje, M. ; Battistello, G. & Nickel, U.	*GSM passive coherent location system: performance prediction and measurement evaluation.* In: IET Radar, Sonar Navigation, 8(2014) pp. 94-105.
Adrat, M.; Osten, T.; Leduc, J.; Antweiler, M. & Elders-Boll, H.	*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. ; Tschauner, M. ; Antweiler, M. & Lewandowsky, J.	*Novel Transformations of Extrinsic Information Applied to Innovative BICM-ID Receivers: Fundamentals and Limits.* In: Proceedings of WInnComm- Europe 2014 Wireless Innovation European Conference on Wireless Communications Technologies and Software Defined Radio. Rome: 4.-6. November 2014. Pucker, Lee et al. (Eds.). SDR Software Defined Radio Forum, 2014, pp. 1-5.
Argumánez, H. E. & Tschauner, M.	*Tactical Communication Systems based on Civil Standards: Modeling in the MiXiM Framework.* In.: Proceedings of the 1st OMNeT++ Community Summit 2014. Hamburg: 2nd September 2014. Förster, Anna. et al. (Eds.)., OMNET++ Community Summit, 2014. Report No.: OMNET/2014/06
Barz, C. & Antweiler, M.	*Network Centric Warfare in a Coalition Environment.* In: Military Scientific Research. Annual Report 2013. Defence Research for the German Armed Forces. Federal Ministry of Defence (Ed.), 2014, pp. 16-17.
Couturier, S. & Rauschen, D.	*Energy Detection Based on Long-Term Estimation of Gaussian Noise Distribution.* In.: Proceedings of the 8th Karlsruhe Workshop on Software Radios. Karlsruhe: 12th-13th March 2014. Karlsruhe Institute of Technology, Communication Engineering Lab, 2014, pp. 89-95.
Hanspach, M. & Goetz, M.	*Recent Developments in Covert Acoustical Communication.* In: Sicherheit 2014 – Sicherheit, Schutz und Zuverlässigkeit : Beiträge der 7. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI). Wien: 19.-21. März 2014. Katzenbeisser, S. (Hrsg.). Köllen, 2014, S. 243-254 (GI-Edition. Proceedings ; 228) ISBN: 978-3-88579-622-0
Kurth, F.	*Robust Detection and Pattern Extraction of Repeated Signal Components Using Subband Shift-ACF.* In: IEEE International Conference on Cloud Engineering (IC2E). Boston: 11-14th March 2014. IEEE Press, 2014, pp. 520-525. ISBN: 978-1-4799-3766-0
Kurth, F. ; Cornaggia Urrigshardt, A. & Urrigshardt, S.	*Robust F0 Estimation in Noisy Speech Signals Using Shift Autocorrelation.* In: 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). Florence: 4-9 May 2014. IEEE Press, 2014, pp. 1468-1472. ISBN 978-1-4799-2893-4
Kurth, F. ; Kamlage, R. ; Cornaggia Urrigshardt, A. & Höck, A.	*Vorrichtung und Verfahren zur Detektion und Klassifikation von Sprachsignalen innerhalb breitbandiger Quellsignale.* Deutsches Patent- und Markenamt, 2014. (DE102013021955 (B3) – 2015-01-08)

AUSGEWÄHLTE PUBLIKATIONEN

	Verfasser	Titel
KOM	Meyer, S.	*Optimization of the Stop-and-Go- and Dual-Mode-Algorithms for Real-time Baseband Transmission.* In: Proceedings of the 18th IEEE SPA Conference. Signal, Processing. Algorithms, Architectures, Arrangements, and Applications. Poznan: 22-24th September 2014. IEEE, 2014
	Rauschen, D. ; Couturier, S. ; Adrat, M. ; Antweiler, M. & Elders-Boll, H.	*Cooperative Spectrum Sensing for a Real-Time Cognitive Radio Demonstrator.* In: Cognitive Radio and Future Networks. The Hague: 12-13th May 2014. NATO, STO, 2014. (STO-MP-IST-123) (AC/323(IST-123)TP/573)
ITF	Bense, H. ; Dembach, M. ; Kioscha, K. ; Schade, U. & Sikorski, L.	*Corporate Semantic Web – Die wissensbasierte Methode zur Verbesserung der Suchfunktionen in Unternehmensnetzen.* In: Knowtech – Kongress für Wissensmanagement 2014. Hanau: 15.-16. Oktober 2014. http://ontology4.us/download/presentations/141016_CSWS-Coporate_Semantic_Web_Search_Knowtech2014.pdf
	Bense, H. ; Schade U. ; Ohrem, F. & Sikorski, L.	*Recherche-Unterstützung durch Ontologie-Visualisierung im EnArgus2-Projekt.* In: 3. DGI-Konferenz. 66. Jahrestagung der DGI. Ockenfeld, M. [Hrsg.]. Frankfurt am Main: 8.-9. Mai 2014. DGI, 2014, S. 15-24 (Tagungen der Deutschen Gesellschaft für Informationswissenschaft und Informationspraxis ; 17). ISBN 978-3-925474-73-6
	Biermann, J. ; Garcia, J. ; Krenc, K. ; Nimier, V. ; Rein, K. & Snidaro, L.	*Multi-Level Fusion of Hard and Soft Information.* In: Information Fusion (FUSION) 2014. 17th International Conference on ... . Salamanca: 7-10th July 2014. IEEE Press, 8 p.
	Dragos, V. & Rein, K.	*Integration of soft data for information fusion: pitfalls, challenges and trends.* In: Information Fusion (FUSION) 2014. 17th International Conference on ... . Salamanca: 7-10th July 2014. IEEE Press, 8 p.
	Jansen, N. ; Krämer, D. & Spielmann, M.	*GIS-basierte Nutzerschnittstelle für Führungsinformationssysteme.* In: Strobl, J. et al. (Hrsg.). AGIT 2014. Angewandte Geoinformatik. Salzburg: 2.-4. Juli 2014. Herbert Wichmann Verlag, 2014, S. 701-706. ISBN 978-3-87907-543-0
	Jansen, N. ; Krämer, D. & Spielmann, M.	*Testbeds for IT Systems in Tactical Environments.* In: Military Communications Conference (MILCOM 2014). Baltimore, MD: 6-8th October 2014. IEEE Press, 2014, pp. 1293-1298. ISBN 978-1-4799-6770-4

	Verfasser	Titel
ITF	Menychtas, A. ; Kranas, P. ; van der Graaf, S. ; Vanobberghen, W. ; Schade, U. ; Coote, R. & Dirkx, M.	*EPIC: A holistic approach for Smart City Services.* In: CMI's 6th Annual International Conference: Developing the future ICT infrastructure technologies, markets, and policies. Copenhagen: 28–29th November 2013. 15 p. http://www.shenja.org/Site/playlist_files/EPIC_A_holistic_approach_for_Smart_City_Services_FINAL.pdf
	O'Neill, D. ; Klucznik, F. ; Burkhart, L. ; Connelly, I. ; Roberts, W. ; Beck, G. ; Gerz, M. & Bau, N.	*MIM – NIEM Options Analysis: Report to the NATO Data Management Syndicate of the Information and Integrated Services Capability Team.* Atlanta, GA: Georgia Tech Research Institute & Wachtberg: Fraunhofer FKIE, October 2014.
	Remmersmann, T. ; Schade, U. & Schlick, C.	*Interactive Multi-Robot Command and Control with Quasi-Natural Command Language.* In: Systems, Man and Cybernetics (SMC) 2014. Proceedings of the IEEE Conference on ... . San Diego, CA: 5-8 October 2014. IEEE Press, 2014, pp. 470-475. ISBN 978-1-4799-3840-7
	Remmersmann, T. , Schade, U. & Tiderko, A.	*Commanding Heterogeneous Multi-Robot Teams.* In: 19th International Command and Control Research and Technology Symposium (ICCRTS). Alexandria, VA: 16-19 June 2014. 2014, 32 p. (Report AD-A606783) http://www.dtic.mil/get-tr-doc/pdf?AD=ADA606783.
	Wollermann, C. ; Schröder, B. & Schade, U.	*Audiovisual prosody of uncertainty: An overview.* In: Ricerche di Pedagogia e Didattica – Journal of Theories and Research in Education, 9 (2014) 1, pp. 137-157.
	Wunder, M. et al.	*Framework for Semantic Interoperability. Final Report.* NATO STO, April 2014, 168 pp. (AC/323(IST094)TP/525) (STO-TR-IST-094).
HF	Alexander, T. ; Conradi, J. ; Theis, S. & Schlick, C. M.	*Anforderungen an die Benutzung von Mobilgeräten und Smartphones aus Sicht der Ergonomie.* In: Gestaltung der Arbeitswelt der Zukunft. GfA Gesellschaft für Arbeitswissenschaft: Bericht zum 60. Kongress. München: 12.-14. März 2014. Jäger, M. [Hrsg.]. GfA-Press, 2014, S. 221-223. ISBN 978-3-936804-17-1
	Alexander, T. & Paul, G.	*Ergonomic DHM Systems – Limitations and Trends – A Review Focused on the 'Future of Ergonomics'.* In: Proceedings of the 3rd Digital Human Modeling Symposium. Odaiba (Tokyo): 20-22nd May 2014. National Institute for Advanced and Industrial Science and Technology (AIST), 2014.

AUSGEWÄHLTE PUBLIKATIONEN

HF

Verfasser	Titel
Alexander, T. & Tölle, J.	*Safety and IT-Security: Transfer of Methods, Knowledge and Lessons-Learned?* In: 9th Future Security 2014. Security Research Conference: Berlin: 16-18th September 2014. Thoma, K. et al. (Eds.). Fraunhofer Verlag, 2014, pp. 535 -542. ISBN: 978-3-8396-0778-7
Conradi, J. & Alexander, T.	*Analysis of Visual Performance during the Use of Mobile Devices While Walking.* In: EPCE 2014. Engineering Psychology and Cognitive Ergonomics. Heraklion: 22-27th June 2014. Hutchison, T. et al. [Eds.] Springer, 2014, pp. 133-142 (Lecture Notes in Computer Science ; 8532). ISBN 978-3-319-07514-3
Henrich, T. ; Plegge, C. ; Westhoven, M. & Alexander, T.	*Haltungserfassung zur Anpassung mobiler Nutzungsschnittstellen.* In: Mensch & Computer 2014. 14. Fachübergreifende Konferenz für Interaktive und Kooperative Medien. München: 31st August - 3rd September 2014. Koch, Michael et al. [Eds.] Oldenbourg, 2014, S. 214-224. ISBN 978-3-11-034415-8
Klaproth, O. W. ; Döring, B. & Alexander, T.	*Implementation of an urban operations simulation model.* In: Systems, Man and Cybernetics (SMC) 2014. Proceedings of the IEEE Conference on ... . San Diego, CA: 5-8th October 2014. IEEE Press, 2014, pp. 57-62. ISBN 978-1-4799-3840-7
Klaproth, O. W.	*Strategic planning in dynamic urban operations: Problem solving under time constraints.* In: ECCE ,14. Proceedings of the 2014 European Conference on Cognitive Ergonomics. Vienna: 1-3rd September 2014. ACM Press, 2014, 4 p. (Article No.17). ISBN 978-1-4503-2874-6
Theis, S. ; Alexander, T. ; Mertens, A. ; Schlick, C. M. & Wille, M.	*Physiologische Auswirkungen der Langzeitnutzung von Head- Mounted Displays im industriellen Kontext.).* In: Gestaltung der Arbeitswelt der Zukunft. GfA Gesellschaft für Arbeitswissenschaft: Bericht zum 60. Kongress. München: 12.-14. März 2014. Jäger, M. [Hrsg.]. GfA-Press, 2014, S. 106-108. ISBN 978-3-936804-17-1
Theis, S. ; Wille, M. & Alexander, T.	*The nexus of human factors in cyber-physical systems: ergonomics of eyewear for industrial applications.* In: ISWC'14 Adjunct Proceedings of the 2014 ACM International Symposium on Wearable Computers. Seattle, WA: 13-17th September 2014. ACM Press, 2014, pp. 217-220. ISBN 978-1-4503-3048-0
Theis, S. ; Alexander, T. ; Wille, M. ; Mertens, A. ; & Schlick, C. M.	*Younger Beginners, Older Retirees: Head-mounted Displays and Demographic Change.* In: Advances in the Ergonomics in Manufacturing: Managing the Enterprise of the Future. Proc. of the 5th AHFE Conference: Advances in Human Factors and Ergonomics 2014. Krakow: 19-23rd July 2014. AHFE, 2014, pp. 295-302. ISBN 978-1-4951-2103-6

MMS

Verfasser	Titel
Fuchs, S. ; Schwarz, J. & Flemisch, F.	*Two steps back for one step forward: Revisiting Augmented Cognition principles from a perspective of (social) system theory.* In: Schmorrow, D.D. et all (Eds.): Foundations of Augmented Cognition. Advancing Human Performance and Decision-Making through Adaptive Systems: 8th International Conference, AC 2014, held as Part of HCI International 2014. Heraklion <Crete>: 22-27th June 2014. Springer, 2014, pp. 114-124. ISBN 978-3-319-07526-6 (Lecture Notes in Computer Science ; 8534)
Fuchs, S. & Schwarz, J.	*Vom passiven Werkzeug zum sozialen Akteur: Ansatz einer ganzheitlicheren Betrachtung adaptiver automatisierter Systeme.* In: Grandt, M. u.a. (Hrsg.): Der Mensch zwischen Automatisierung, Kompetenz und Verantwortung. 56. DGLR Fachausschusssitzung Anthropotechnik. Ottobrunn: 14.-15. Oktober 2014. DGLR Deutsche Gesellschaft für Luft- und Raumfahrt e.V., 2014, S. 285-288. ISBN 978-3-932182-81-2 (DGLR-Bericht ; 2014-01)
Holder, E. ; Motz, F. ; Horoufchin, H. & Baldauf, M.	*Concept for the integration of information received via communication equipment with on-board navigational systems.* In: Stanton, N. et all (Eds.): Advances in Human Aspects of Transportation. Part I. Proc. of the 5th AHFE Conference: Advances in Human Factors and Ergonomics 2014. Krakow: 19-23rd July 2014. AHFE, 2014, pp. 203-214. ISBN 978-1-4951-2097-8
Ley, D.	*Methoden und Werkzeuge zur Unterstützung sicherheitskritischer Prozesse in der zivilen Schifffahrt.* In: Gemeinsam gegen Kriminalität 2.0 und »Underground Economy«. VfS-Kongress. Leipzig: 8.-9. April 2014.
Özyurt, E. ; Döring, B., & Flemisch F.	*Evaluation and extension of the Cognitive Assistant System (COGAS) for user-oriented support of Air Target Identification.* In: IEEE International Inter-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support. CogSIMA 2014. San Antonio, TX: 3-6th March 2014. IEEE Press, 2014, pp. 66-72. ISBN 978-1-4799-*3563-5*
Özyurt, E. ; Döring, B. & Flemisch, F.	*Kognitives und kooperatives Assistenzsystem (COGAS) zur Luftzielidentifizierung an Bord von Marineschiffen.* In: Kognitive Systeme: Mensch, Teams, Systeme und Automaten. Verstehen, Beschreiben und Gestalten Kognitiver (Technischer) Systeme. 3. Interdisziplinärer Workshop. Magdeburg: 25.-27. März 2014.
Schwarz, J. ; Fuchs, S. & Flemisch, F.	*Towards a More Holistic View on User State Assessment in Adaptive Human-Computer Interaction.* In: Systems, Man and Cybernetics (SMC) 2014. Proceedings of the IEEE Conference on Systems, Man and Cybernetics (SMC). San Diego, CA: 5-8th October 2014. IEEE Press, 2014, pp. 1228-1234. ISBN 978-1-4799-3840-7

AUSGEWÄHLTE PUBLIKATIONEN

MMS

Verfasser	Titel
Varga, M. ; Winkelholz, C. ; Träber, S. & Varga, C.	*Visualization for Cyber Situation Awareness.* In: Analysis Support to Decision Making in Cyber Defence and Security. Proceedings of the NATO SAS-106 Symposium, Tallinn: 9-10th June 2014. NATO, STO, 2014. (STO-MP-SAS-106) (AC/323(SAS-106)TP/576)
Witt, O, ; Mihatsch, E. & Küttelwesch, H.	*Komplexe Einsatzsysteme verstehen : Fregatte Klasse 124 und Korvette Klasse 130.* In: Europäische Sicherheit & Technik, 63(2014)2, S.60-61
Wagner, A. & Motz, F.	*A Guide for preparing and executing an Effective Port Security Exercise.* In: 9th Future Security 2014. Security Research Conference: Berlin: 16-18th September 2014. Thoma, K. et al. (Eds.). Fraunhofer Verlag, 2014, pp. 353-359. ISBN: 978-3-8396-0778-7

SE

Ohneiser, O. ; Heesen, M. ; Flemisch, F. & Rataj, J.	*Migration Tolerant Human Machine Interface Concepts in the domains of Air Traffic Control and Automotive.* In: DLRK 2014. Deutscher Luft- und Raumfahrtkongress 2014. Augsburg: 16-18th September 2014. DGLR Deutsche Gesellschaft für Luft- und Raumfahrt – Lilienthal-Oberth e.V., 2014.
Özyurt, E. ; Döring, B. & Flemisch, F.	*Untersuchungen zur kooperativen Prozessführung mit Hilfe des Assistenzsystems COGAS.* In: Grandt, M. u.a. (Hrsg.): Der Mensch zwischen Automatisierung, Kompetenz und Verantwortung. 56. DGLR Fachausschusssitzung Anthropotechnik. Ottobrunn: 14.-15. Oktober 2014. DGLR Deutsche Gesellschaft für Luft- und Raumfahrt e.V., 2014, S. 47-62. ISBN 978-3-932182-81-2 (DGLR-Bericht ; 2014-01)

CMS

Brunner, M. ; Fiolka, T. ; Schulz, D. & Schlick, C.	*Design and Comparative Evaluation of an Iterative Contact Point Estimation Method for Static Stability Estimation of Mobile Actively Reconfigurable Robotics.* In: Robotics and Autonomous Systems, 63 (2015), pp. 89–107.
Höller, F. ; Königs, A. & Schulz, D.	*Autonomous Reconnaissance and Surveillance in Urban Structures – Eurathlon 2013.* In: Autonomous Robot Systems and Competitions (ICARSC), 2014 IEEE International Conference on ... . Espinho <Portugal>: 14-15th May 2014. IEEE Press, 2014, pp. 223-228. ISBN 978-1-4799-4254-1.
Remmersmann, T. & Tiderko, A. ; Schade, U. & Schneider, F. E.	*Interacting with Multi-Robot Systems using BML.* In: EXTREME ROBOTICS. Proceedings of the International Scientific and Technological Conference. Saint-Petersburg: 1-2nd October 2014.

CMS

Verfasser	Titel
Röhling, T.	*Fast Classification of Accessible Terrain with a 3D Laser Range Finder.* In: Proceedings of 13th International Conference on Intelligent Autonomous Systems (IAS13). Padova: 15-18th July 2014.
Schneider, F. E. & Wildermuth, D.	*Aims and Outcome of Professional Ground Robotic Competitions - A Systematic Comparison.* In: New technologies – assistance and limitations of the EOD in post-ISAF era. Proceedings of the 3rd NATO EOD Demonstrations & Trials Workshop. Trenčín: 30th September – 2nd October 2014.
Winfield, A.F.T. ; Franco, M.P. ; Brüggemann, B. ; Castro, A. ; Djapic, V. ; Ferri, G. ; Petillot,Y.; Röning, J. ; Schneider, F.E. ; Sosa. D. & Figuria, A.	*euRathlon Outdoor Robotics Challenge: Year 1 Report.* In: Advances in Autonomous Robotics Systems. 15th Annual Conference, TAROS 2014. Birmingham: 1-3rd September 2014. Mistry, M.; et al. (Eds.). Springer, 2014, pp. 267-268. (Lecture Notes in Computer Science ; 8717). ISBN 978-3-319-10400-3

CS

Kiesling, T. ; Motsch, N. ; Kaufmann, H. ; Elsner, T. ; Wübbeling, M. & Meier, M.	*Collaborative Security Monitoring based on the MonIKA Framework for Privacy-Preserving Information Sharing.* In: 9th Future Security 2014. Security Research Conference. Berlin: 16-18th September 2014. Thoma, K. ; et al. (Eds.). Fraunhofer Verlag, 2014, pp. 461-469. ISBN: 978-3-8396-0778-7
Mazurczyk, W.; Wendzel, S.; Villares, I. A. & Szczypiorski, K.	*On Importance of Steganographic Cost for Network Steganography.* In: Security and Communication Networks (2014) 10 pp.
Sykosch, A. ; Neff, R. & Meier, M.	*Policy-Driven Pseudonymization.* In: 9th Future Security 2014. Security Research Conference: Berlin: 16–18th September 2014. Thoma, K. et al. (Eds.). Fraunhofer Verlag, 2014, pp. 445-452. ISBN 978-3-8396-0778-7
Szlósarczyk, S.; Wendzel, S.; Kaur, J.; Meier, M. & Schubert, F.	*Towards Suppressing Attacks on and Improving Resilience of Building Automation Systems - an Approach Exemplified Using BACnet.* In: Sicherheit 2014 - Sicherheit, Schutz und Zuverlässigkeit: Beiträge der 7. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI). Wien: 19.-21. März 2014. Katzenbeisser, S. (Hrsg.). Köllen, 2014, S. 407-418 (GI-Edition. Proceedings ; 228). ISBN 978-3-88579-622-0
Wendzel, S.; Mazurczyk, W.; Caviglione, L. & Meier, M.	*Hidden and Uncontrolled – On the Emergence of Network Steganographic Threats.* In: ISSE 2014 Securing Electronic Business Processes – Highlights of the Information Security Solutions Europe 2014 Conference. Springer-Vieweg, 2014, pp. 123-133. ISBN 978-3-658-06707-6

AUSGEWÄHLTE PUBLIKATIONEN

CS

Verfasser	Titel
Wendzel, S. & Keller, J. Wendzel, S. ; Herdin, C. ; Wirth, R. ; Masoodian, M. ; Luz, S. & Kaur, J.	***Hidden and under control.*** In: Annals of Telecommunications (ANTE), 69(2014)7-8, pp. 417-430 Mosaic-chart based Visualization in Building Automation Systems. In: 9th Future Security 2014. Security Research Conference. Berlin: 16-18th September 2014. Thoma, K. et al. (Eds.). Fraunhofer Verlag, 2014, p. 690-693. ISBN 978-3-8396-0778-7
Wendzel, S.; Zwanger, V. [CA&D]; Meier, M. & Szlósarczyk, S.	***Envisioning Smart Building Botnets.*** In: Sicherheit 2014 – Sicherheit, Schutz und Zuverlässigkeit: Beiträge der 7. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI). Wien: 19.-21. März 2014. Katzenbeisser, S. (Hrsg.). Köllen, 2014, S. 319-329 (GI-Edition. Proceedings ; 228). ISBN 978-3-88579-622-0
Wübbeling, M. ; Elsner, T. & Meier, M.	***Inter-AS Routing Anomalies: Improved Detection and Classification.*** In: Cyber Conflict (CyCon 2014). 6th International Conference on ... . Tallinn: 3rd-6th June 2014. IEEE Press, 2014, p. 223-238. ISBN 978-9949-9544-0-7
Wübbeling, M. & Meier, M.	***Utilization of Traceroutes to Improve Cooperative Detection of Internet Routing Anomaly Detection.*** In: 9th Future Security 2014. Security Research Conference. Berlin: 16-18th September 2014. Thoma, K. et al. (Eds.). Fraunhofer Verlag, 2014, p. 470-478. ISBN 978-3-8396-0778-7

CA&D

Verfasser	Titel
Barabosch, T.; Eschweiler, S. & Gerhards-Padilla, E.	***Bee Master: Detecting Host-Based Code Injection Attacks. In: Detection of Intrusions and Malware, and Vulnerability Assessment.*** Egham: 10-11th July 2014. Springer, 2014, pp. 235-254 (Lecture Notes in Computer Science ; 8550). ISBN 978-3-319-08508-1
Barabosch, T. & Gerhards-Padilla, E.	***Host-Based Code Injection Attacks: A Popular Technique Used By Malware.*** In: 9th IEEE International Conference on Malicious and Unwanted Software (MALCON 2014). Fajardo <Puerto Rico>: 28-30th October 2014.
Ernst, R. ; Jopen, S. & Bartelt, T.	***Reducing MANET Neighborhood Discovery Overhead. In: 2014 IEEE 39th Conference on Local Computer Networks (LCN). Edmonton, AB: 8-11th September 2014. IEEE Press, 2014, pp. 374-377. ISBN 978-1-4799-3778-3***
Ernst, R. & Weidenbach, P.	***Erkennungsmethoden für Kernel-Level Rootkits – Die unsichtbare Bedrohung.*** In: iX Magazin für professionelle Informationstechnik, (2014) 12, S. 112-115.
Guevara, L.; Plohmann, D. & Gerhards-Padilla, E.	***Semantic Exploration of Binaries.*** In: The Botnet Fighting Conference - Botconf. Nancy: 3-5th December 2014.

CA&D

Verfasser	Titel
Plohmann, D.	***Patchwork: Stitching against malware families with IDA Pro.*** In: 9. GI FG SIDAR Graduierten-Workshop über Reaktive Sicherheit. Spring. Meyer, M. (Hrsg.). Bochum: 31st July-1st August 2014. p. 7 (SIDAR-Report SR-2014-01). ISSN 2190-846X
Salmanian, M.; Brown, J.D.; Mason, P.C.; Tang, H.; Song, R.; Simmelink, D.; Fongen, A. & Hunke, S.	***Provisioning Graded Services for Dynamic Secure Wireless Networks in Coalition Environments.*** In: NATO IST-122 Symposium on Cyber Security Science and Engineering. Tallinn: 13-15th October 2014. NATO, RTO, 2014
Zwanger, V [CA&D].; Gerhards-Padilla; E. & Meier, M. [CS]	***Codescanner: Detecting (Hidden) x86/64 Code in Arbitrary Files.*** In: 9th IEEE International Conference on Malicious and Unwanted Software (MALCON 2014). Fajardo <Puerto Rico>: 28-30th October 2014.

Sonstige

Verfasser	Titel
Christin, D.; Engelmann, F. & Hollick, M.	***Usable Privacy for Mobile Sensing Applications. In: Information Security Theory and Practice.*** Securing the Internet of Things. Naccache, David; et all (Eds.). Springer, 2014, pp. 92-107 (Lecture Notes in Computer Science ; 8501). ISBN 978-3-662-43825-1
Christin, D. ; Pons-Sorolla, D. R. ; Hollick, M. & Kanhere, S. S.	***TrustMeter: A Trust Assessment Framework for Collaborative Path Hiding in Participatory Sensing Applications.*** In: Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2014 IEEE Ninth International Conference on ... . Singapore: 21-24th April 2014. IEEE Press, 2014, p. 6. ISBN 978-1-4799-2842-2
Fahl, S. ; Dechand, S. ; Perl, H. ; Fischer, F. ; Smrcek, J. & Smith, M.	***Hey, NSA: Stay Away from my Market! Future Proofing App Markets against Powerful Attackers.*** In: ACM CCS'14. Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. Scottsdale, AZ: 3-7th November 2014. ACM Press, 2014, pp. 1143-1155. ISBN 978-1-4503-2957-6
Harbach, M. ; Zezschwitz, E. von; Fichtner, A. ; Luca, A. de & Smith, M.	***It's a Hard Lock Life: A Field Study of Smartphone (Un)Locking Behavior and Risk Perception.*** In: 10th Symposium On Usable Privacy and Security (SOUPS). Menlo Park, CA: 9-11th July 2014. USENIX Ass. 2014, pp. 213-230. ISBN 978-1-931971-13-3
Neugebauer, R. (Hrsg.) ; Jarke, M. (Hrsg.) ; Thoma, K. (Hrsg.) ; Beyerer, Jürgen (Red.) ; Eckert, C. (Red.) ; Martini, P. (Red.) & Waidner, M. (Red.)	***Strategie- und Positionspapier Cyber-Sicherheit 2020: Herausforderungen für die IT-Sicherheitsforschung.*** Fraunhofer-Verbund Informations- und Kommunikationstechnologie -IuK-, Berlin. Stuttgart, FhG, 2014, 52 ***S.***

AUSGEWÄHLTE TÄTIGKEITEN IN GREMIEN

Wiss. Mitarbeiter/in	Arbeitsgruppe bzw. Gremium
Adrat, M.	Technical Program Committee Member of NATO STO IST-123-RSY-029 Symposium on Cognitive Radio and Future Networks
Adrat, M.	EDA Ad-hoc Working Group on SDR Standardization Strategic Guidance
Alexander, T.	NATO STO MSG-127 RTG on Reference Architecture for Human Behavior Modeling in Military Training Applications, Co-Chairman
Alexander, T.	EDA CAPTECH ESM04 on Human Factors and CBRNE Protection, CAPTECH Government Expert, CGE
Aurisch, T.	NATO STO IST-103-RTG-049 Task Group on Selected Issues for PCN
Barz, C. & Jansen N.	NATO-STO IST-RTG-118: Research Task Group on SOA recommendations for disadvantaged grids in the tactical domain
Biermann, J.	IST-106 /RTG-051 Research Task Group on Information Filtering and Multi Source Information Fusion
Charlish, A.	NATO STO SET-ET-085 Exploratory Team on Adaptive Radar Resource Management..
Charlish, A.	NATO STO SET-RTG-199 Research Task Group on Evaluating the Effectiveness of Coordination Methods for Distributed Mobile Sensors
Couturier, S.	Chairman of NATO-STO IST-ET-074 Network Aspects of Cognitive Radio.
Flemisch, F.	NATO-STO Human Factors & Medicine Panel
Fuchs, C.	STO IST-ET076 Exploratory Team on Internet of Military Things
Fuchs, C.	STO IST-ET075 Exploratory Team on Integration of Sensor and Communications Networks.
Ginzler, T.	Technical Program Committee Member of NATO STO IST-120-RWS-018 on Future Internet Architectures for Military Networks.
Heesen, M.	HFM-247 Research Task Group Human-Autonomy Teaming: Supporting Dynamically Adjustable Collaboration

Wiss. Mitarbeiter/in	Arbeitsgruppe bzw. Gremium
Koch, W.	NATO Lecture Series Battlefield Acoustic Sensing, Multi-modal Sensing and Networked Sensing for ISR Applications (SET-189)
Rein, K.	STO IST-106 Information Filtering and Multi-Source Fusion
Remmersmann, T. & Schade, U.	STO MSG-085 Research Task Group on Standardization for C2-Simulation Interoperation
Tölle, J.	NATO-IST 122 RSY-030 Cyber Security Science and Engineering
Tölle, J.	ATO-IST-ET-078 Cyber Security of Military Platforms
Winkelholz, C.	Technical Team Member, NATO RTO IST-110 »Visualization for Analysis«
Winkelholz, C.	Programme Committee NATO IST-116 Symposium »Visual Analytics«
Wunder, M.	STO IST-Panel, Vice Chairman

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.

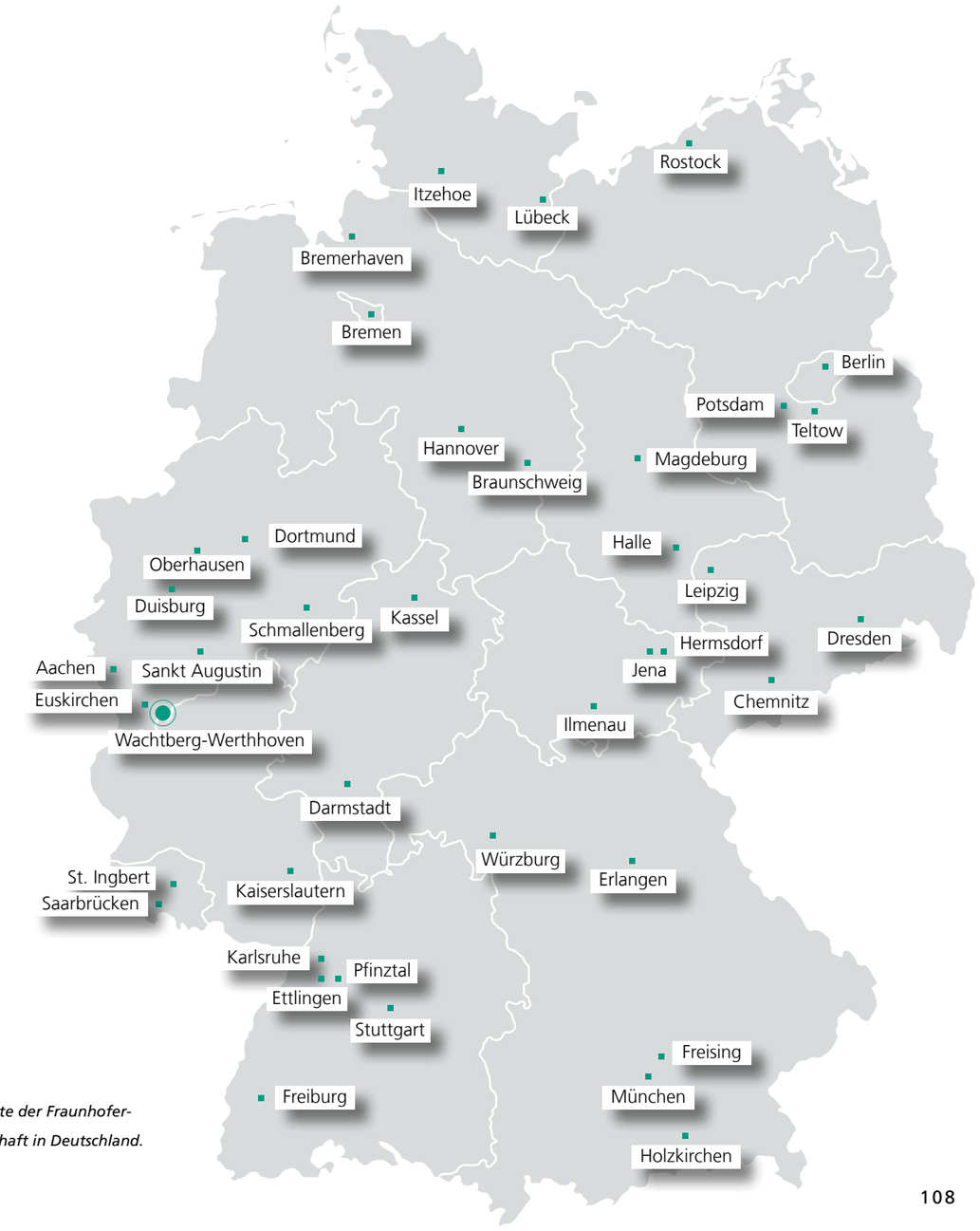
Die Fraunhofer-Gesellschaft betreibt in Deutschland derzeit 67 Institute und Forschungseinrichtungen. Rund 24 000 Mitarbeiterinnen und Mitarbeiter, überwiegend mit natur- oder ingenieurwissenschaftlicher Ausbildung, erarbeiten das jährliche Forschungsvolumen von 2 Milliarden Euro. Davon fallen rund 1,7 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.

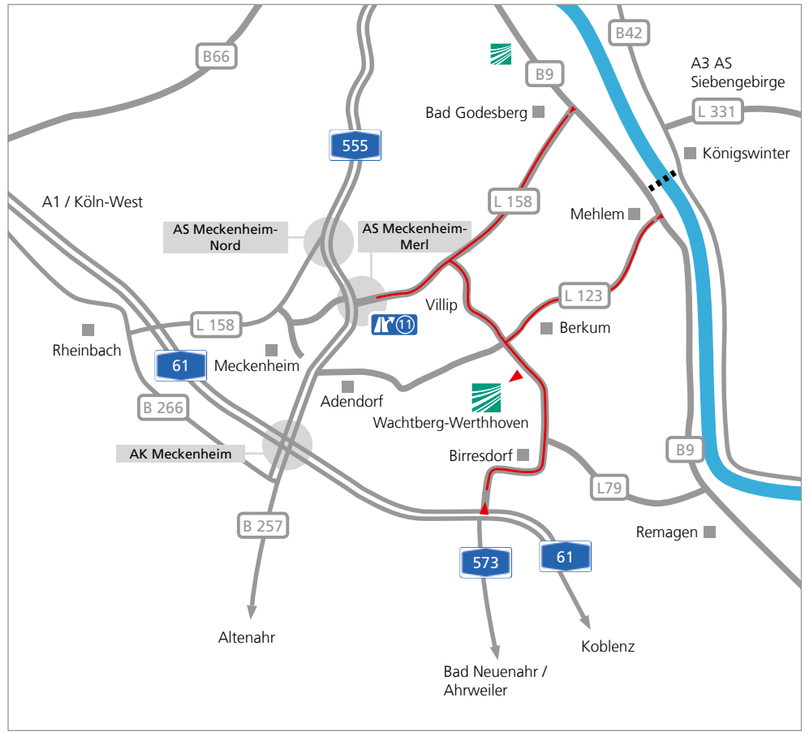
Ihren Mitarbeiterinnen und Mitarbeitern bietet die Fraunhofer-Gesellschaft die Möglichkeit zur fachlichen und persönlichen Entwicklung für anspruchsvolle Positionen in ihren Instituten, an Hochschulen, in Wirtschaft und Gesellschaft. Studierenden eröffnen sich aufgrund der praxisnahen Ausbildung und 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 9435-0
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 9435-0
Fax: +49 (0)228 9435-685

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

REDAKTION UND LEKTORAT
Dr. Eva Kneise, Anne Rindt, Herrad Schmidt

TEXTE
Stefan Andres und
Mitarbeiterinnen / Mitarbeiter des Fraunhofer FKIE

LAYOUT, SATZ, FOTOMONTAGE
Volker Kurzidim, Petra Kaiser

FOTOGRAFIE
Uwe Bellhäuser / das bilderwerk

BILDQUELLEN
Bilder © Fraunhofer FKIE

AUSNAHMEN
Seite 08 Technical background / iStock. *Fotomontage*
Seite 10 - 11 Internet Cyber Security / iStock
Seite 15 Business & Technical / iStock. *Fotomontage*
Seite 17 Business Team / iStock
Seite 18 - 19 Business Meeting / 123RF®
Seite 20 Technical background / iStock. *Fotomontage*
Seite 21 Business Strategy / iStock
Seite 25 Business Graph / iStock
Seite 27 Abstract date transfering / iStock. *Fotomontage*
Seite 35 Computer virus detected / iStock
Seite 37 Datenschutzkonzept / 123RF®
Seite 44 Hamburg Harbour, Cargo Terminal / iStock
Seite 45 Gas pollution / iStock
Seite 46 - 47 Touch Screen Network / iStock
Seite 49 Geländeüberwachung / © Bundeswehr, Heinrichs
Seite 51 GUWMANET® / iStock. *Fotomontage*
Seite 52 - 53 Laptop / iStock. *Fotomontage*
Seite 55 Airplane taking off / iStock
Seite 57 Börse auf dem Computerscreen / 123RF®
Seite 57 Norwegian town Sorland / iStock Fotomontage
Seite 58 - 59 Aufnahme mit Infrarot - Thermografie / 123RF®
Seite 60 - 61 Firewall & Antivirus-Konzept / 123RF®
Seite 63 You´ ve been hacked! / iStock
Seite 64 Geschäftsmann sucht Virus / 123RF®
Seite 67 Cyphertext / 123RF®
Seite 68 - 69 Digitale Informationen / 123RF®. *Fotomontage*
Seite 74 Spähtrupp mit Fennek / © Bundeswehr, Heinrichs
Seite 77 CeBIT Hannover 2014 / Deutsche Telekom
Seite 95 Science / iStock.
Seite 108 Radar - Touch - Screen / iStock.