Karlsruher Institut für Technologie

aifb

Security and Privacy made in Karlsruhe
AIFB-Themenheft 2024

Einladung
des Vereins Angewandte Informatik Karlsruhe e.V.
zum 39. AIK-Symposium

Karlsruhe
8. November 2024

Einladung
des Vereins Angewandte Informatik Karlsruhe e.V. zum 39. AIK-Symposium
„Security and Privacy made in Karlsruhe“

Karlsruhe, 8. November 2024
Novotel Karlsruhe City,
Festplatz 2, 76137 Karlsruhe – und im Internet

Fast ein Viertel der Menschen in Deutschland – 24 Prozent – waren laut Cybersicherheitsmonitor 2024 von BSI und Polizei schon einmal Opfer von Cyberkriminalität. Der Geschäftsbetrieb von Unternehmen und Organisationen ist durch Ransomware stark bedroht. Auf dem 39. AIK-Symposium „Security and Privacy made in Karlsruhe“ diskutieren Expertinnen und Experten den aktuellen Stand in den Forschungsfeldern IT-Sicherheit und Privatsphärenschutz sowie Unterstützungsangebote und aufklärende Maßnahmen zur Erhöhung des Gefahrenbewusstseins – von psychologischen Faktoren bis zum Verhalten in Krisensituationen.

Programm

14:15 **Eröffnung und Begrüßung**
Dr. Ingo Mauser, EnBW Energie Baden-Württemberg AG, Vorstand Verein AIK e.V.
Prof. Dr. Melanie Volkamer, Institut AIFB, Karlsruher Institut für Technologie (KIT)

14:30 **Das menschliche Element in der IT-Sicherheit**
Dr. Benjamin Berens, Institut AIFB, KIT

15:00 **Privacy and Security in a Hyperconnected World**
Prof. Dr. Thorsten Strufe, KASTEL – Institut für Informationssicherheit und Verlässlichkeit, KIT

15:30 **Ehrungen**

15:45 **Kaffeepause**

16:45 **Security and Privacy in Crisis Situations**
Prof. Dr. Oksana Kulyk,
IT-Universität Kopenhagen, Dänemark

17:15 **Neue Sicherheitsherausforderungen für den Mittelstand – ein Update**
Dr. Dirk Achenbach,
FZI Forschungszentrum Informatik, Karlsruhe

17:45 **Psychologie der IT-Sicherheit**
Dipl.-Inform. Dirk Fox,
Secorvo Security Consulting GmbH, Karlsruhe

anschließend **Gemeinsames Abendessen**

Das 39. AIK-Symposium findet im Novotel Karlsruhe City beim Kongresszentrum am Festplatz Karlsruhe statt. Alternativ können Sie an den Vorträgen auch gerne per Livestream teilnehmen.

Die diesjährige Mitgliederversammlung des Vereins AIK e.V. wird am 18. Oktober 2024 abgehalten. Den Mitgliedern geht eine separate Einladung zu.

Anmeldung

Den Link zur Anmeldung und weitere organisatorische Informationen finden Sie unter: www.aik-ev.de

	Präsenz	Livestream
Teilnahmebeitrag für AIK-Mitglieder	€40	kostenlos
Teilnahmebeitrag für Nichtmitglieder*	€80	kostenlos
Beitrag zum Abendessen	€35	

*Bei gleichzeitigem Vereinsbeitritt sind nur der Mitgliedsbeitrag von €25 für das Jahr 2024 sowie der Teilnahmebeitrag für Mitglieder zu entrichten. Unternehmen, die eine Firmenmitgliedschaft im AIK e.V. haben, können bis zu drei Firmenangehörige zum Mitgliederpreis entsenden.

Für die Teilnahme vor Ort empfehlen wir wegen des Platzkontingents eine möglichst frühzeitige Anmeldung. Grundsätzlich bitten wir um Ihre Anmeldung und um Überweisung des Beitrags bis zum 18.10.2024. Bei Rücktritt bis zum 25.10.2024 werden die entrichteten Gebühren erstattet.

Übernachtungen im Novotel Karlsruhe City (Festplatz 2, 76137 Karlsruhe) können über die Webseite des Hotels und andere übliche Portale gebucht werden.

Sehr geehrte Damen und Herren,
liebe Freunde und Förderer des
Instituts AIFB,

im Jahr 2023 wuchs die Menge der Schadprogramm-Varianten nach Angaben des BSI-Lageberichts IT-Sicherheit täglich um durchschnittlich 250.000 neue an. Die Zahl kennzeichnet nur die bekannten Varianten. Während die Bedrohung größer wird, finden Angriffe immer diversifizierteren Zugang zu sensiblen Daten der Gesellschaft, Wirtschaft, von Staat und Verwaltung. „Eine effektive Abwehr setzt benutzbare Schutzmechanismen sowie effektive Sensibilisierungsmaßnahmen voraus", so Melanie Volkamer, Leiterin der Forschungsgruppe Security • Usability • Society (SECUSO). Die Professorin und ihr Team haben das 39. AIK-Symposium inhaltlich zusammengestellt.

Auf dem 39. AIK-Symposium „Security and Privacy made in Karlsruhe" zeigen Referentinnen und Referenten aus Wissenschaft und Wirtschaft, wie IT-Sicherheit und Privatsphärenschutz erforscht und im betrieblichen wie im privaten Alltag gefördert werden können, und sie beleuchten, wo die Problemstellungen liegen.

Der Titel des 39. AIK-Symposiums trägt neben „Security and Privacy" den Zusatz „made in Karlsruhe". Die Region Karlsruhe ist mit ihrer vielfältigen Sicherheitsforschung am KIT und weiteren Forschungseinrichtungen, ihren zahlreichen innovativen Unternehmen und weitverzweigten, organisationsübergreifenden Netzwerken ein Zentrum der IT-Sicherheit. Ein Blick in die Geschichte zeigt, dass IT-Sicherheit im Verein Angewandte Informatik Karlsruhe (AIK) e.V. lange Tradition hat. „Sicherheit im Electronic Business" stand bereits 1999 im Fokus des 3. AIK-Symposiums, organisiert von der damaligen Forschungsgruppe Effiziente Algorithmen von Hartmut Schmeck. Im Jahr 2016 widmete sich das 32. AIK-Symposium dann der Frage, wie man „Sicherheit und Vertrauen in der vernetzten Welt" schaffen kann. Ausgerichtet hatte es die Forschungsgruppe Betriebliche Informationssysteme (BIS) von Andreas Oberweis. Das führt den hohen Querschnittscharakter des Forschungsfeldes IT-Sicherheit vor Augen, das in alle Informatik-Anwendungsbereiche hineinwirkt.

Die acht Forschungsgruppen am Institut AIFB haben sich natürlich im Berichtszeitraum in ihrer Lehre, Forschung und Entwicklung mit vielen weiteren hoch aktuellen Fragen zur Anwendung von Informatik in grundverschiedenen Einsatzgebieten beschäftigt. Ihre Schwerpunkte reichen von der Entwicklung autonomer technischer Fahrzeuge und Systeme über Produktionsautomatisierung und Geschäftsprozesssteuerung bis hin zur Erforschung und Gestaltung von Informationsdiensten. Auf den hinteren Seiten dieses Themenheftes erfahren Sie mehr dazu. Highlights aus dem Institutsleben waren diesmal 5 Rufe auf Professuren, 10 Promotionen und 6 Auszeichnungen. Michael Färber erhielt einen Ruf an die TU Dresden. Tobias Käfer hat von ihm die kommissarische Leitung der Forschungsgruppe Web Science übernommen. Sascha Alpers wird Professor an der Hochschule Heilbronn. Jurlind Budurushi, Michael Decker und Roland Schätzle wurden als Professoren an die Duale Hochschule Baden-Württemberg (DHBW) berufen. Herzlichen Glückwunsch allen und weiterhin viel Erfolg!

Vielen Dank für Ihr Interesse an der Lehre und Forschung des Instituts AIFB – und eine herzliche Einladung zum 39. AIK-Symposium!

Die wachsende Bedeutung der IT-Sicherheit

Melanie Volkamer

Die Bedrohung im Cyberraum ist so hoch wie nie zuvor. Laut dem Lagebericht des BSI von 2023 stellt Ransomware nach wie vor die Hauptbedrohung dar. Ransomware ist bösartige Software, die den Zugang zu Daten, Programmen und Services auf den Computern der Angriffsopfer blockiert. Die Cyberkriminellen drohen, die Computer nur gegen Lösegeld oder die Erfüllung ideeller Forderungen wieder freizugeben, oder auch, sensible Daten publik zu machen oder zu verkaufen. Oft auch beides.

Im Fokus der Angriffe stehen zunehmend leichte Ziele wie kleine und mittelständische Unternehmen (KMU) sowie Behörden und Bildungseinrichtungen. Durch den rasanten Fortschritt der Technologie, aber auch durch neue Verfahren wie Online-Umfragen, Online-Abstimmungen und Online-Wahlen sowie die breite Nutzung von Werkzeugen und Serviceangeboten, die mit künstlicher Intelligenz (KI/AI) arbeiten, sind neue Bedrohungen und Angriffsvektoren entstanden. Überall gilt es daher, die technischen und organisatorischen Schutzmaßnahmen zu erhöhen und neuartige Schutzmaßnahmen zu entwickeln. Die Region Karlsruhe hat sich in Deutschland als ein führendes Zentrum der IT-Sicherheit etabliert.

Die Arbeit der Forschungsgruppe SECUSO am Institut AIFB gilt effektiven Maßnahmen, um in der Gesellschaft ein breites Bewusstsein für die Risiken und Gefahren aus der digitalen Welt zu schaffen, sowie benutzbarer Sicherheitstechnologie. Bei der Untersuchung und Erforschung von Methoden für die Entwicklung von wirkungsvollen, gut anwendbaren Maßnahmen steht der Mensch im Mittelpunkt. SECUSO stellt Lehr- und Selbstlernverfahren sowie Sicherheitsschulungs- und Trainingswerkzeuge unter anderem in Form von Erklärvideos, Rate- und Lernspielen zum Thema Cybersicherheit bereit, die sich Interessierte auf der Webseite ansehen bzw. ausprobieren können. Die Forschungsgruppe hat zudem datenschutzfreundliche Apps für Alltagsanwendungen wie Schrittzähler oder die Taschenlampe im Mobiltelefon entwickelt, die den Schutz der Privatsphäre verbessern. Diese sogenannten Privacy Friendly Apps für Android-Betriebssysteme fordern nur Berechtigungen an, die für die Funktionalität notwendig sind, und enthalten keine Tracking-Mechanismen, die Nutzungsdaten sammeln.

Alle Maßnahmen, die SECUSO zum Schutz der IT-Sicherheit in Unternehmen, Organisationen und im privaten Umfeld der Nutzerinnen und Nutzer untersucht oder entwickelt, werden wissenschaftlich evaluiert, ihre nachhaltige Wirksamkeit überprüft. Die Forschungsgruppe bringt sich mit ihrem Wissen und Können über das Institut und die Fakultät hinaus in die vielfältige IT-Sicherheitsforschung am KIT sowie weiterer Einrichtungen, Unternehmen und Netzwerke ein.

SECUSO
SECURITY · USABILITY · SOCIETY

Karlsruhe: Ein Zentrum der IT-Sicherheit
Karlsruhe hat sich in Deutschland als ein führendes Zentrum für IT-Sicherheit etabliert, in dem sich Widerstand gegen Cybercrime gleichermaßen wissenschaftlich wie wirtschaftlich formiert. Mit einer Vielzahl von Forschungsgruppen, Forschungsverbünden, spezialisierten Unternehmen und starken Kooperationsnetzwerken bietet die Region einerseits eine ideale Umgebung für Wissenschaftlerinnen und Wissenschaftler, Studierende und Unternehmen, die sich für Cybersicherheit interessieren. Auf der anderen Seite gibt es hier viel Unterstützung gerade für KMU, Behörden und Bildungseinrichtungen zum Schutz vor Cyberangriffen. Den größten Forschungsverbund stellen die KASTEL Security Research Labs dar. Dieser Verbund besteht aus Forschenden des Karlsruher Instituts für Technologie (KIT), dem Fraunhofer IOSB und dem Forschungszentrum Informatik (FZI). Die Security Forschung am KIT wird maßgeblich durch die Helmholtz-Gemeinschaft Deutscher Forschungszentren mit ihrem Programm „Engineering Digital Futures", Unterpunkt 3 „Engineering Secure Systems" finanziert. Daran beteiligt sind die drei Forschungsgruppen „Quantifying Security", „Communication & Computation" und „Human & Societal Factors" sowie die drei Labore „Mobility", „Energy" und „Production". Neben der Forschung und Ausbildung im Bereich IT-Sicherheit bieten die KASTEL Security Research Labs verschiedene Formate zum Wissenstransfer und Netzwerken an. Hierzu zählen die KIT Graduate School Cyber Security, die Distinguished Lectures in Cyber Security sowie ein Security Lunch jeden zweiten Dienstag im Monat im Oxford Pub in Karlsruhe. Der Security Lunch ist für alle Interessierten offen. Ein weiteres nennenswertes Projekt ist StartUp-Secure KASTEL. Es unterstützt StartUps im Bereich der IT-Sicherheit. Einen wichtigen Beitrag zur Sichtbarkeit und Stärke der Region in Sachen IT-Sicherheit leisten auch das Lernlabor Cybersicherheit des Fraunhofer IOSB, das Kompetenzzentrum IT-Sicherheit des FZI sowie die Cyberwehr Baden-Württemberg, die maßgeblich vom FZI betrieben wird. Im Hochschulbereich umfassen weitere relevante Aktivitäten den Forschungsschwerpunkt Security für Cyber-Physikalische und Automotive Systeme am Institut für Energieeffiziente Mobilität (IEEM) der Hochschule Karlsruhe sowie an der Dualen Hochschule Baden-Württemberg (DHBW in Karlsruhe) die Berufung einer Professur zu Themen wie Cyber-Sicherheit, benutzbare Sicherheit und KI-unterstützte Sicherheit. SAP-Research forscht ebenfalls in Karlsruhe zu IT-Sicherheitsthemen.

Kooperationen und Netzwerke über die Hochschulen hinaus
Karlsruhe ist bekannt für seine starken Kooperationen und Netzwerke über die Hochschulen hinaus: Besonders zu nennen ist hier die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si), ein Zusammenschluss zahlreicher Partner und Unterstützer, die gemeinsam an der Stärkung der IT-Sicherheitslandschaft arbeiten. Über die Stadt hinaus renommiert sind auch der European Digital Innovation Hub für angewandte Künstliche Intelligenz und Cybersicherheit sowie das Wibu-Systems House of IT-Security. Sie bieten Plattformen für den Austausch von Wissen und Erfahrungen im Bereich der IT-Sicherheit. In Karlsruhe angesiedelt ist zudem der European Digital Innovation Hub für angewandte Künstliche Intelligenz und Cybersicherheit, und mit dem Cybercrime-Zentrum Baden-Württemberg der Justiz gibt es seit Januar 2024 in Karlsruhe ein neues Organ zur Bekämpfung von Cyberkriminalität.

Starke regionale Wirtschaftsstruktur
Last but not least gibt es in der Region zahlreiche Unternehmen, die sich auf IT-Sicherheit spezialisiert haben. Beispielhaft zu nennen sind hier Secorvo Security Consulting, EnBW Cyber Security GmbH, Sophos Cybersecurity, Next Iteration, AVK EDV-Systemtechnik GmbH, Valid-AItor, TelemaxX Telekommunikation GmbH, Aramido GmbH, InterConnect System- und Softwarehaus, BFK edv-consulting GmbH, Atruvia und Tortuga Webspace Security. Karlsruhe bietet mit dieser Mischung eine einzigartige Kombination aus exzellenter Forschung, starken Netzwerken und innovativen Unternehmen, die die Stadt zu einem führenden Zentrum für IT-Sicherheit machen.

Prof. Dr. Melanie Volkamer ist seit 2018 Professorin am KIT. Zuvor lehrte und forschte sie an der TU Darmstadt und der Universität Karlstad, Schweden. Seit 2011 leitet sie die von ihr gegründete Forschungsgruppe SECUSO (Security • Usability • Society). Volkamers Forschungsinteresse gilt dem Faktor Mensch in der Cybersicherheit. Ein weiterer Interessensschwerpunkt sind elektronische Wahlen und Abstimmungen. Melanie Volkamer promovierte 2008 an der Universität Koblenz-Landau. Ihr Diplom in Informatik erwarb sie 2004 an der Universität des Saarlandes.

39. AIK-Symposium
Die Fachvorträge

Fünf Vortragende zeigen beim Symposium auf, wie breit gefächert die Forschungsfragen zu IT-Sicherheit und Privatheit sind und wie dynamisch sie sich mit der Weiterentwicklung der computerbasierten Technologien und der weltumspannenden Vernetzung immer wieder neu präsentieren. Freuen Sie sich auf jüngste Forschungserkenntnisse, Erfahrungen und spannende Diskussionen!

Das menschliche Element in der IT-Sicherheit
Benjamin Berens

Das Bewusstsein für sicherheitsrelevante Gefahren im Umgang mit digitalen Systemen und damit verbundene Entscheidungen sind wesentliche Elemente der IT-Sicherheitsforschung. Wie kann verhindert werden, dass Nutzende auf Phishing-Mails hereinfallen und ungewollt Zugangsinformationen preisgeben? Da es nicht für alles technische Lösungen gibt, ist es wichtig, den Faktor Mensch in den Blick zu nehmen und Nutzende bei sicherheitsrelevanten Entscheidungen zu unterstützen. Im Vortrag geht es daher um Interventionen, welche durch die Aufbereitung von Wissen eine informierte Entscheidung ermöglichen (Awareness), aber auch Interventionen in Form von Tools, welche die Aufmerksamkeit auf relevante Aspekte lenken und so sicherheitsförderndes Verhalten unterstützen (Tool Support). Die Herausforderungen liegen hier in der langfristigen Schaffung von Awareness sowie der Erstellung unterschiedlicher Maßnahmen auf Basis eines einheitlichen Konzepts. Der Vortrag gibt Einblicke in IT-Sicherheitsstudien mit dem Fokus auf dem Faktor Mensch, präsentiert aktuelle Erkenntnisse und stellt offene Fragen zur Diskussion.

***Dr. Benjamin Berens** hat sich im Bereich der IT-Sicherheit auf den Schwerpunkt Mensch spezialisiert. Er entwickelt und evaluiert unter anderem Maßnahmen zum Erkennen von Phishing-Nachrichten. Berens hat im Fach Informatik am KIT zu folgendem Thema promoviert: „When Awareness Fades and There Is No Support, the Phisher Has an Easy Game". Er hat einen Master in Psychologie von der TU Darmstadt und seinen Bachelorabschluss in Wirtschaftspsychologie an der Hochschule Fresenius erworben.*

Privacy and Security in a Hyperconnected World
Thorsten Strufe

Extended realities (XR), including Augmented reality (AR) and virtual reality (VR), are emerging technologies with a wide range of potential applications, including networking, gaming, healthcare, and education. However, as with any new technology, AR/VR also introduces new security and privacy challenges. AR and VR devices collect a wide range of personal data about users, including their physical movements, eye movements, and voice recordings. This data can be used to track users' activities, identify them, or even infer private attributes like health conditions or private preferences. Furthermore, XR applications integrate multiple modalities, such as audio, video, and haptic data streams, enlarging security and privacy exposure. Yet, there are always claims of how "anonymization" and "pseudonymization" were helping to achieve "GDPR compliance". In this talk I will present results of several of our recent studies, and we will discuss how claimed protection is ineffective under scrutiny.

***Prof. Dr. Thorsten Strufe** is professor of IT Security at KIT, and adjunct professor for Privacy and Network Security at TU Dresden. He is a deputy speaker of the Excellence Centre for Tactile Internet with Human-in-the-Loop (CeTI), and a Principal Investigator (PI) in the national IT security competence center KASTEL Security Research Labs. His research interests lie in the areas of privacy and network security, especially in the context of social networking services and novel mixed reality applications. Recently, he has focused on studying privacy implications of user behavior.*

Security and Privacy in Crisis Situations
Oksana Kulyk

Cybersecurity and privacy are increasingly being recognized as not just a technical issue but also a complex subject at the intersection of technology, human behavior and societal aspects. The field of human-centered security and privacy has emerged to focus on specifically that intersection by applying methods such as empirical studies to investigate and address human and social aspects of cybersecurity and privacy. In this talk I will discuss applications of these methods to situations of crisis, where both individual behavior and societal attitudes differ greatly from what is considered normal. A first example will focus on security and privacy concerns during the COVID-19 pandemic. The second example will describe preliminary findings from a trip to Ukraine and conversations with both individuals and institutions there, dealing with the impact of cyberwarfare on the civilian population. Concluding the talk, the differences in challenges of addressing cybersecurity and privacy in crisis situations compared to non-crisis states will be discussed and potential future research directions outlined.

***Prof. Dr. Oksana Kulyk** is an associate professor at the IT University of Copenhagen (ITU) and a member of the Center for Information Security and Trust (CISAT). She had previously worked as a post-doc in the SECUSO research group at KIT and at TU Darmstadt, where she received her doctorate in 2017. Kulyk's research interests focus on human factors in security and privacy, including privacy-related decision support for end users and risk communication, as well as issues of security and privacy in electronic voting.*

Neue Sicherheitsherausforderungen für den Mittelstand – ein Update
Dirk Achenbach

Das Kompetenzzentrum IT-Sicherheit am FZI Forschungszentrum Informatik hat zum Ziel, dem baden-württembergischen Mittelstand als Ansprechpartner in Fragen der IT-Sicherheit zu dienen. In Projekten zu anwendungsnaher IT-Sicherheit arbeiten Forscherinnen und Forscher an neuen Erkenntnissen und daran, diese für den praktikablen Einsatz in KMU aufzubereiten. Zu den Themen Digitalisierung, Vernetzung, Cloud Computing und Internet der Dinge, die bereits 2016 auf dem 32. AIK-Symposium diskutiert wurden, sind neue hinzugekommen: Die Blockchain als vermeintlich heilsbringende Zukunftstechnologie; Quantencomputer als Bedrohung der asymmetrischen Kryptographie; Ransomware als kriminelles Geschäftsmodell; die Künstliche Intelligenz als „Game Changer" auch in der IT-Sicherheit; und nicht zuletzt die zweite EU-Richtlinie zu Netzwerk- und Informationssicherheit (NIS-2-Richtlinie). Der Vortrag geht einigen Entwicklungen der letzten Jahre nach und beleuchtet ausgewählte Projekte am FZI. Abschließend wird eine Abgrenzung zwischen Hypes, Dauerbrennern und wirklichen Problemen versucht.

***Dr. Dirk Achenbach** leitet das Kompetenzzentrum IT-Sicherheit am FZI Forschungszentrum Informatik. Der Informatiker forschte im Anschluss an sein Studium am KIT im Bereich formaler Sicherheitsmodelle in der Kryptographie. Er unterstützte den Aufbau des Kompetenzzentrums für angewandte Sicherheitstechnologie KASTEL. Nach seiner Promotion wechselte er zum FZI, wo er das Kompetenzzentrum IT-Sicherheit mit aufbaute und die Leitung der Cyberwehr Baden-Württemberg übernahm. Achenbachs Leidenschaft gilt dem Schulterschluss von Theorie und Praxis für einen sicheren digitalen Wandel.*

Psychologie der IT-Sicherheit
Dirk Fox

Warum kümmern wir uns meist erst um IT-Sicherheit, wenn etwas passiert ist? Und warum gelingt es häufig nicht, die Notwendigkeit von IT-Sicherheit – und die dafür erforderlichen Verhaltensänderungen – Kollegen und Mitarbeitern zu vermitteln? Die Ursachen dafür sind tief in uns verankert: Die Abläufe und Entscheidungsprozesse des menschlichen Gehirns arbeiten nach Heuristiken, denen systematische Fehler unterlaufen. Ein tieferes Verständnis dieser Ursachen hilft, Sicherheitsprobleme durch „Missverständnisse" zwischen den Anforderungen der IT-Sicherheit und den Anwendern zu vermeiden. Mit den Erkenntnissen des Nobelpreisträgers Daniel Kahneman lassen sich zahlreiche Verhaltensweisen im Umgang mit Informationssicherheit erklären – und umgekehrt Regelungen und Kommunikation so umgestalten, dass die gewünschte Wirkung nicht durch „kognitive Verzerrungen" abgeschwächt oder sogar aufgehoben wird.

***Dirk Fox** ist Diplom-Informatiker und Geschäftsführer der Secorvo Security Consulting GmbH in Karlsruhe. Er beschäftigt sich seit 40 Jahren mit Fragen der Informationssicherheit und des Datenschutzes in Forschung, Entwicklung und Beratung. Seit 1997 ist er Herausgeber der Fachzeitschrift „Datenschutz und Datensicherheit" (DuD, Springer-Verlag), seit 2008 geschäftsführender Vorstand des IT-Unternehmernetzwerks CyberForum in Karlsruhe. Fox ist Autor von mehr als 150 Veröffentlichungen und Träger des Bundesverdienstkreuzes am Bande.*

Institut AIFB
Die Forschungsgruppen 2023/24
Zahlen, Fakten, Erfolge

8 Forschungsgruppen
5 Rufe
10 Promotionen
6 Auszeichnungen
8 Projekte
169 Publikationen
28 Vorlesungen
3068 Prüfungen
78 Mitarbeiterinnen und Mitarbeiter

8 Forschungsgruppen

Angewandte technisch-kognitive Systeme (ATKS)
Prof. Dr.-Ing. J. Marius Zöllner

Die Forschungsgruppe ATKS fokussiert sich auf Technologien der maschinellen Intelligenz, einschließlich maschineller Wahrnehmung, Situationsverständnis und kooperativer Verhaltensentscheidung. Ein Schwerpunkt liegt auf maschinellen lernbasierten Lösungen für hochautomatisierte Mobilität und interaktive Benutzerunterstützung. Autonome Fahrzeuge wie CoCar NextGen, CoCar und die FZI-Shuttles werden in der Forschung und Lehre eingesetzt und ständig weiterentwickelt. Im Projekt SofDCar befasst sich ATKS mit Unsicherheiten in hochautomatisierten Fahrzeugen und der realitätsnahen virtuellen Simulation dieser Fahrzeuge. Im Mobilitätslabor werden, in Kooperation mit KASTEL, sicherheitskritische Schwachstellen autonomer Mobilitätssysteme untersucht. Ein weiterer Schwerpunkt liegt im Bereich Robotik. Der neue Laufroboter Unitree Go2 der Forschungsgruppe dient zur Evaluierung und Weiterentwicklung von Reinforcement Learning (RL) Algorithmen. RL erlaubt dem Roboter, sich in unterschiedlichen Umgebungen zu bewegen und komplexe Aufgaben zu bewältigen. Die Kombination von fortschrittlicher Hardware und modernen RL-Methoden im Unitree Go2 bietet eine Plattform für Forschung in der autonomen Robotik und praxisnahe Einblicke für Studierende im Praktikum Maschinelles Lernen.

https://atks.aifb.kit.edu/

Betriebliche Informationssysteme (BIS)
Prof. Dr. Andreas Oberweis

Mit Sprachen, Methoden und Werkzeugen der Angewandten Informatik entwickelt die Forschungsgruppe BIS Lösungen für aktuelle gesellschaftliche und unternehmerische Herausforderungen. Betriebliche Informationssysteme betrachten wir dabei als Schlüssel, um Geschäftsprozesse und ihre Auswirkungen auf die Umwelt zu verstehen und zu verbessern. In verschiedenen Forschungsschwerpunkten setzen wir dazu Technologien wie Process Mining, Robotik und Maschinelles Lernen ein. Die Grundlage unserer Forschungsarbeit bilden innovative Datenbanktechnologien sowie neue Methoden der Softwaretechnik und des Geschäftsprozessmanagements. Beispielsweise werden in dem vom der Cyberagentur finanzierten Vorhaben MANTRA zur Hochsicherheit in sicherheitskritischen und verteidigungsrelevanten Szenarien große Sprachmodelle (LLM) für die zielgruppenspezifische Darstellung von Cyber-Risiken genutzt. Für die Transformation zur digitalen Hochschule überarbeiten und digitalisieren wir Prozesse partizipativ mit Studierenden, nutzen KI für die automatisierte Kompetenzextraktion aus wissenschaftlichen Veröffentlichungen und erweitern eine eigenentwickelte Modellierungsplattform zur stärkeren Kompetenzorientierung in Lehre und digitalen Prüfungen.

https://bis.aifb.kit.edu/

Cooperative Autonomous Systems (CAS)
Prof. Dr. Alexey Vinel

Die Forschungsgruppe CAS betreibt vielfältige Forschung zu kooperativen autonomen Fahrzeugen. Im Rahmen der Real-World-Lab-Aktivitäten entwickeln wir innovative Mobilitätslösungen der Zukunft – kooperative E-Bikes und Roboter – mit neuen Erkenntnissen in den Bereichen Fahrzeugkommunikation (V2X), Mensch-Maschine-Interaktion und Soziale Robotik. Im kompetitiven KIT-Future Fields-Programm (Stufe 2) haben wir gemeinsam mit den Instituten KASTEL und IAR eine zusätzliche Förderung von 600.000 Euro dafür erhalten. Zusammen mit dem Institut ITAS sind wir Partner im Projekt CulturalRoad (2024-2027), das von der EU mit 3,5 Millionen Euro gefördert wird. In diesem Projekt werden nachhaltige Einsatzpläne für kooperative, vernetzte und autonome Mobilitätsdienste (CCAM) entwickelt, die von der Bevölkerung akzeptiert werden. Um das zu erreichen, wird partizipative Planung mit einem neuartigen Fünf-Sterne-Bewertungssystem kombiniert, welches kulturelle und geografische Vielfalt erfasst. Des Weiteren interessiert sich CAS für die Integration künstlicher Intelligenz in kooperative intelligente Transportsysteme, z. B. im Projekt TyreRoadNoise (2023-2026) zur Geräuschmodellierung von Fahrzeugen.

https://cas.aifb.kit.edu/

Critical Information Infrastructures (cii)
Prof. Dr. Ali Sunyaev

cii beschäftigt sich mit der Erforschung zuverlässiger, sicherer, zweckorientierter und dezentraler Informationssysteme mit Bezug zu kritischen Informationsinfrastrukturen, Health-IT-Anwendungen und Digital Health, Cloud- und Edge-Computing-Diensten, Distributed Ledger Technology und Blockchain, wirtschaftlichen Anwendungen von künstlicher Intelligenz sowie der Auditierung und Zertifizierung von IT-Systemen. Im Berichtszeitraum durfte sich die Gruppe cii wieder über mehrere Auszeichnungen als Anerkennung ihrer Arbeit freuen (siehe nächste Doppelseite) und es konnte eine Reihe neuer Forschungsprojekte eingeworben werden, z. B. das BMBF-Projekt „GameUP" sowie drei im Rahmen der KASTEL Security Research Labs geförderte Projekte. Zur Summer School #Data2Health im Juli 2023 in Koblenz wurde Prof. Sunyaev eingeladen, eine Keynote zu halten. Seit Januar 2024 ist er Mitglied des Experimentallabors Karlsruhe Decision & Design Lab (KD²Lab). Im Februar 2024 wurde Prof. Sunyaev in den Vorstand der Gesellschaft für Informatik e.V. (GI) gewählt und in das DFG-Fachkollegium Informatik berufen. cii veröffentlichte wie schon in den Vorjahren wieder einen cii Student Papers Sammelband für sehr gute studentische Seminararbeiten der Gruppe.

https://cii.aifb.kit.edu/deutsch/index.php

Information Service Engineering (ISE)
Prof. Dr. Harald Sack

ISE untersucht Modelle und Methoden zur Entwicklung und Bereitstellung von innovativen Informationssystemen. Im Fokus stehen effiziente semantische Erschließung, Aggregation und Retrieval umfangreicher heterogener und verteilter Datenquellen. Forschungsschwerpunkte liegen in der Optimierung und Anwendung von Deep-Learning-basierten Verfahren zur Informations- und Wissensgewinnung aus heterogenen multimodalen Daten sowie, darauf aufbauend, in der Entwicklung semantischer und explorativer Suchtechnologien und Empfehlungssysteme. ISE ist an fünf Konsortien zum Aufbau der DFG-geförderten Nationalen Forschungsdateninfrastruktur (NFDI) beteiligt (NFDI4Culture, MaRDI, NFDI4Matwerk, NFDI4DataScience und NFDI4Memory). Hier arbeitet ISE mit an der Konzeption und Implementierung von Ontologien und Wissensgraphen zur bereichsübergreifenden Vernetzung von Forschungsdaten. Generelles Ziel ist deren systematische Erschließung, nachhaltige Sicherung, Verfügbarmachung und internationale Vernetzung.

https://ise.aifb.kit.edu/

Security • Usability • Society (SECUSO)
Prof. Dr. Melanie Volkamer

SECUSO forscht zum Thema Sicherheit und Privatheit. Im Mittelpunkt der Forschung steht der Mensch. Untersucht werden Methoden zur Entwicklung und Evaluation von benutzerfreundlichen Maßnahmen zum Schutz der Privatsphäre und zur Erhöhung der Sicherheit, zur Bewusstseinsbildung bezüglich der Privatheit im Digitalen und für Sicherheitstrainings insbesondere für Unternehmen. Darüber hinaus forscht die Gruppe an Sicherheitsfragen zum Thema elektronische Wahlen (E-Voting). SECUSO arbeitet aktuell an zwei Projekten: dem von der Leibniz-Gesellschaft geförderten Projekt „Digital Transformation in Research – DiTraRe" und dem Projekt „Decision-Making in Hybrid Adaptive Systems for Better Work and Life – An Open Science Approach" im Rahmen der Exzellenzuniversität. Im Subtopic „Engineering Secure Systems" des Forschungsfeldes Information (Key Technologies) in der Helmholtz-Gemeinschaft ist SECUSO maßgeblich im Bereich „Human and Societal Factors" (HSF) beteiligt und betreibt einen Showroom, u. a. mit Videos und Spielen zu den Themen Phishing und Passwortsicherheit.

https://secuso.aifb.kit.edu/

Systems, Data, Simulation & Energy (SYDSEN)
Prof. Dr. Sanja Lazarova-Molnar

SYDSEN ist eine dynamische und expandierende Forschungsgruppe, die sich der Weiterentwicklung von Modellierung und Simulation widmet. Sie entwickelt innovative Methoden zur Nutzung von Daten aus dem Internet der Dinge (IoT) und erforscht Synergien zwischen künstlicher Intelligenz und Simulation. Das Hauptaugenmerk liegt auf der Verbesserung von digitalen Zwillingen mit dem Ziel, die Leistung von cyber-physischen Systemen wie intelligenten Fabriken und Energiesystemen zu verbessern. Das SYDSEN-Team arbeitet daran, die technologischen Grenzen zu verschieben, um intelligentere, effizientere und zuverlässigere Systeme für die Zukunft zu entwickeln. SYDSEN ist an bedeutenden Projekten wie ONE4ALL und DMaaST im Rahmen von „Horizon Europe" sowie an anderen nationalen und internationalen Aktivitäten beteiligt. Prof. Lazarova-Molnar hat Keynotes auf renommierten Konferenzen der Modellierungs- und Simulations-Community gehalten, insbesondere auf dem EUROSIM-Kongress 2023 und der SIMULTECH 2024. Außerdem war sie Co-Chair des Tracks Reliability Modeling and Simulation auf der Winter Simulation Conference 2023, einer der wichtigsten Veranstaltungen in diesem Bereich. Prof. Lazarova-Molnar bekleidet eine Führungsrolle innerhalb des IEEE und als Director-at-Large in der Society for Modeling and Simulation International.

https://sydsen.aifb.kit.edu/deutsch/index.php

Web Science
Prof. Dr. York Sure-Vetter (beurlaubt). Vertretung: Dr. Tobias Käfer

Die Gruppe Web Science erforscht Methoden der künstlichen Intelligenz (KI) und deren praktische Anwendung. Im Fokus stehen vor allem semantische Technologien und Wissensgraphen, neben maschinellem Lernen und der Verarbeitung natürlicher Sprache. Mit ihrer Forschung trägt die Gruppe bei zu aktuellen Entwicklungen in den Bereichen großer Sprachmodelle, ML-basierter Digitalisierung und interoperablen souveränen Datenökosystemen. Tobias Käfer leitet die Forschungsgruppe in Vertretung von York Sure-Vetter, der seit 2020 Direktor der Nationalen Forschungsdateninfrastruktur (NFDI) ist. Web Science ist an mehreren – teilweise sehr interdisziplinären – Projekten beteiligt, u.a. der DFG-geförderten KI-Forschungsgruppe 5339, die an einer KI-basierten Methodik für die schnelle Ertüchtigung unreifer Produktionsprozesse arbeitet, dem Projekt KIWI, dessen Ziel es ist, Wirbelschleppen in LiDAR-Messungen durch KI automatisch in nahezu Echtzeit zu erkennen, sowie am Projekt NeSyPlan zu neurosymbolischen Verfahren zur Planung mittels künstlicher Intelligenz. Auf europäischer Ebene koordiniert die Forschungsgruppe ein Netzwerk in Form einer COST-Aktion mit Partnern aus mehr als 30 Ländern zum Thema verteilte Wissensgraphen.

https://websci.aifb.kit.edu/

5 Rufe

Prof. Dr.-Ing. Sascha Alpers, Professor für Wirtschaftsinformatik, insb. Datenplattformen und Informationssysteme, Hochschule Heilbronn
Prof. Dr. Jurlind Budurushi, Duale Hochschule Baden-Württemberg (DHBW)
Prof. Dr. Michael Decker, Duale Hochschule Baden-Württemberg (DHBW)
Prof. Dr.-Ing. Michael Färber, Professur für Skalierbare Software-Architekturen für Data Analytics, TU Dresden
Prof. Dr. Roland Schätzle, Duale Hochschule Baden-Württemberg (DHBW)

Zudem hat **Dr. Sebastian Lins** im Wintersemester 2023/24 eine Professurvertretung an der Universität Kassel mit der Vorlesung „Business Information Systems Analysis and Design" übernommen.

10 Promotionen

Benjamin Berens: „When Awareness Fades and There Is No Support, the Phisher Has an Easy Game" (Melanie Volkamer)
Mathis Borowsky: „Constrained Neural Networks for Safety-Critical Environments - In the Context of Automated Driving and Driver Assistance" (J. Marius Zöllner)
Jonas Friederich: „Data-Driven Assessment of Reliability for Cyber-Physical Production Systems" (University of Southern Denmark, Sanja Lazarova-Molnar)
Faris Janjos: „Learning to Predict Vehicle Trajectories for Autonomous Driving from Latent Features" (J. Marius Zöllner)
Niclas Kannengießer: „Purposeful Information System Decentralization based on Distributed Ledger Technology" (Ali Sunyaev)
Karl Kurzer: „Implicit Cooperative Decision-Making for Automated Vehicles" (J. Marius Zöllner)
Konstantin Pandl: „Trustworthy Decentralized Machine Learning Systems" (Ali Sunyaev)
Maximilian Renner: „Revealing Trust Transfer Mechanisms in the Context of Artificial Intelligence" (Ali Sunyaev)
Tarek Saier: „Data Mining and Information Extraction Methods for Large-Scale High-Quality Representations of Scientific Publications" (Michael Färber)
Meike Ullrich: „Kompetenzorientiertes E-Assessment für die grafische Modellierung in der Hochschullehre" (Andreas Oberweis)

6 Auszeichnungen

Scott Thiebes aus der Gruppe cii wurde für seine Dissertation „A Socio-Technical Analysis of Genetic Privacy and its Role in Genetic Data Sharing" von der Gesellschaft für Datenschutz und Datensicherheit (GDD) mit dem Dissertationspreis im Bereich IT-Sicherheit 2023 ausgezeichnet.

Ausgezeichnete Beiträge zu internationalen Konferenzen:

• Distinguished Paper Award: „Exploring Phishing Threats through QR Codes in Naturalistic Settings" von Filipo Sharevski, Mattia Mossano (SECUSO), Maxime Veit (SECUSO), Gunther Schiefer (BIS), Melanie Volkamer (SECUSO), Symposium on Usable Security and Privacy (USEC) 2024, San Diego, USA.

• Best Paper Award: „Challenges in Developing Digital Twins for Labor-Intensive Manufacturing Systems: A Step towards Human-centricity" von Manuel Götz, Sanja Lazarova-Molnar (SYDSEN), The 7th International Conference on Emerging Data and Industry 4.0, Hasselt, Belgien.

• Mario Gerla Best Paper Award: „Impact of Persistence on the Age of Information in 5G NR-V2X Sidelink Communications" von Alexey Rolich, Ion Turcanu, Alexey Vinel (CAS), Andrea Baiocchi, 2023 21st Mediterranean Communication and Computer Networking Conference (MedComNet), Ponza, Italien.

• Best Poster Award: „Beware of website hackers: Developing an awareness video to warn for website hacking" von Anne Hennig, Leoni Schmidt-Enke, Miriam Mutter, Peter Mayer (SECUSO), 19th Symposium on Usable Privacy and Security (SOUPS 2023), Anaheim, USA.

Yannick Erb aus der Forschungsgruppe cii hat für seine Masterarbeit „From Affordances to Business Value – How Can Organizations Use Fog Computing to Create Business Value?" den Fujitsu NEXT „IT Innovation" Award 2023 erhalten.

8 Projekte

C2CBridge – Country to City Bridge verfolgt das Ziel, einen attraktiven Mobilitätsdienst mit hoher gesellschaftlicher Akzeptanz als Alternative zum privaten Pkw zur Anbindung vom Land an die Stadt zu erforschen. Er soll auf automatisierten Fahrzeugkonzepten und deren vernetztem Betrieb in einer Ridepooling-Flotte aufsetzen. **ATKS** arbeitet an der Automatisierung der Fahrfunktion, analysiert und entwickelt kooperatives Fahrverhalten und Platooning, sodass mehrere autonome Fahrzeuge in einem flexiblen Verbund das Land mit der Stadt verbinden. Gefördert vom Bundesministerium für Digitales und Verkehr (BMDV) ist C2CBridge Teil von „Deutsches Zentrum – Mobilität der Zukunft" (DZM).

https://www.kamo.one/c2c-bridge/

Scope3transparent unterstützt Unternehmen in der Elektronikindustrie dabei, ihre Treibhausgasemissionen zu ermitteln und zu reduzieren. **BIS** konzentriert sich auf die Herausforderungen des Datenaustauschs und der Datenintegration bei der Berechnung von Treibhausgasbilanzen in den komplexen Lieferketten der Elektronikindustrie. Dazu werden Modellierungs-, Simulations- und Visualisierungsansätze entwickelt und in praxisnahen Schulungen für Unternehmen eingesetzt. Das Bundesministerium für Wirtschaft und Klimaschutz fördert das Projekt in der Nationalen Klimaschutzinitiative.

https://bis.aifb.kit.edu/317_93.php

TyreRoadNoise entwickelt ein datenbasiertes Berechnungsmodell zur Geräuschbestimmung von Fahrzeugen mit Hilfe von künstlicher Intelligenz. **CAS** und **SYDSEN** bringen Forschungs- und Entwicklungsleistungen ein. Weitere Projektpartner sind das KIT-Institut FAST, die Audi AG, die BMW AG, die Bundesanstalt für Straßenwesen, die Continental AG, die EYYES Deutschland GmbH, die Dr. Ing. h.c. F. Porsche AG, die RA Consulting GmbH, die RWTH Aachen und die Volkswagen AG. Im Rahmen der Innovationsinitiative mFUND fördert das BMDV die Projekte mit rund 3 Mio. Euro.

https://projekt-tyre-road-noise.de/

DigiAct – Digitale Transformation im Gesundheitswesen: Von digitalen Werkzeugen zu digitalen Akteuren wird federführend von **cii** geleitet. Ziel ist, das Aufkommen digitaler Akteure im Gesundheitswesen empirisch zu untersuchen und auf Basis dieser Analyse eine Theorie zu entwickeln, die das Zusammenspiel zwischen menschlichen und nicht-menschlichen Akteuren im Gesundheitswesen umfasst. In einer großen Klinik, die derzeit eine signifikante digitale

Transformation durchläuft, soll die erarbeitete Theorie durch Anwendung qualitativer Methoden angewandt werden. DigiAct wird von der Deutschen Forschungsgemeinschaft (DFG) gefördert.

https://cii.aifb.kit.edu/

„Wiedergutmachung nationalsozialistischen Unrechts“ ist ein Pilotprojekt, das am Beispiel des Staatsarchivs Ludwigsburg Archivunterlagen digitalisiert und zugänglich macht. **ISE** erprobt und entwickelt dafür automatische Verfahren der Text- und Mustererkennung unter Einsatz von maschinellem Lernen. Diese werden auf einen ausgewählten Dokumentenbestand angewendet, um ihr Potenzial für die Erschließung und Veröffentlichung zu ermitteln. Im Mittelpunkt stehen Methoden zur Verbesserung und Nachbearbeitung der OCR-Transkripte. Die Forschung wird vom Bundesministerium der Finanzen (BMF) gefördert.

https://www.fiz-karlsruhe.de/de/projekte/wiedergutmachung

DiTraRe – Digitale Transformation der Forschung untersucht die Auswirkungen und Potenziale der Digitalisierung des wissenschaftlichen Arbeitens. Primäres Forschungsziel von **SECUSO** in DiTraRe ist, Awareness für Sicherheits- und Datenschutzaspekte bei Wissenschaftlerinnen und Wissenschaftlern im Bereich Data Science, insbesondere bei jenen, die maschinelle Lerntechniken in ihrer Forschung anwenden, zu erhöhen. Zunächst werden mentale Modelle von Forschenden zu Sicherheits- und Datenschutzaspekten in ihrer Forschung erhoben. SECUSO kooperiert hier mit Dr. Karen Renaud, University of Strathclyde. DiTraRe wird von der Leibniz-Gemeinschaft gefördert.

https://secuso.aifb.kit.edu/2557.php

DMaaST – Innovative modelling and assessment capabilities through MaaS for Manufacturing Ecosystem resiliency, an dem **SYDSEN** beteiligt ist, will das Ökosystem der Fertigung grundlegend verändern. Durch eine vertrauenswürdige, organisationsübergreifende Echtzeit-Datenintegration und Kommunikation zwischen Unternehmen soll die Fähigkeit der Wertschöpfungskette, auf externe und unvorhergesehene Ereignisse zu reagieren, ebenso verbessert werden wie die Produktionsplanung im Bezug auf Funktionsfähigkeit, Kapazität, Kreislauffähigkeit und Nachhaltigkeit. DMaaST will die Adaption von Manufacturing-as-a-Service (Maas) beschleunigen. DMaaST wird aus dem Programm „Horizon Europe“ finanziert.

https://sydsen.aifb.kit.edu/96_176.php

MANDAT – Methoden zum Austausch von unternehmensbezogenen Daten in treuhänderbasierten Datenökosystemen erforscht, wie Web-Technologien fit gemacht werden können für den dezentralen und interoperablen Austausch von Daten, um den gestiegenen Anforderungen nach Datensouveränität gerecht zu werden. **Web Science** entwickelt in diesem Rahmen die Protokollfamilie Solid (Social Linked Data) weiter und klärt Forschungsfragen rund um selbst-souveräne Identitäten (SSI), deren Sicherheit, die Verarbeitung dezentral gehaltener semantischer Daten und wie in dezentralen, interoperablen Umgebungen Apps erstellt werden können. MANDAT ist ein EU-gefördertes BMBF-Projekt.

https://websci.aifb.kit.edu/Projekte_MANDAT.php

169

169 Publikationen

wurden im Jahr 2023 aus dem Institut AIFB veröffentlicht. 1 Buch wurde herausgegeben. 11 Buchbeiträge und 30 Veröffentlichungen in Zeitschriften stammen ebenso von Angehörigen des Instituts AIFB wie 127 Beiträge in Tagungsbänden.

https://www.aifb.kit.edu/386.php

28

28 Vorlesungen

mit jeweils bis zu 600 Zuhörerinnen und Zuhörern sowie 29 Seminare und Praktika mit insgesamt 287 Teilnehmenden wurden im Sommersemester 2023 und Wintersemester 2023/24 vom Institut angeboten.

https://www.aifb.kit.edu/96.php

3068

3068 Prüfungen

wurden im Sommersemester 2023 und im Wintersemester 2023/24 am Institut AIFB abgenommen. 106 Abschlussarbeiten legten Studierende im gleichen Zeitraum vor. 36 Masterarbeiten und 70 Bachelorarbeiten wurden geschrieben und betreut.

https://www.aifb.kit.edu/75.php

78

78 Mitarbeiterinnen und Mitarbeiter

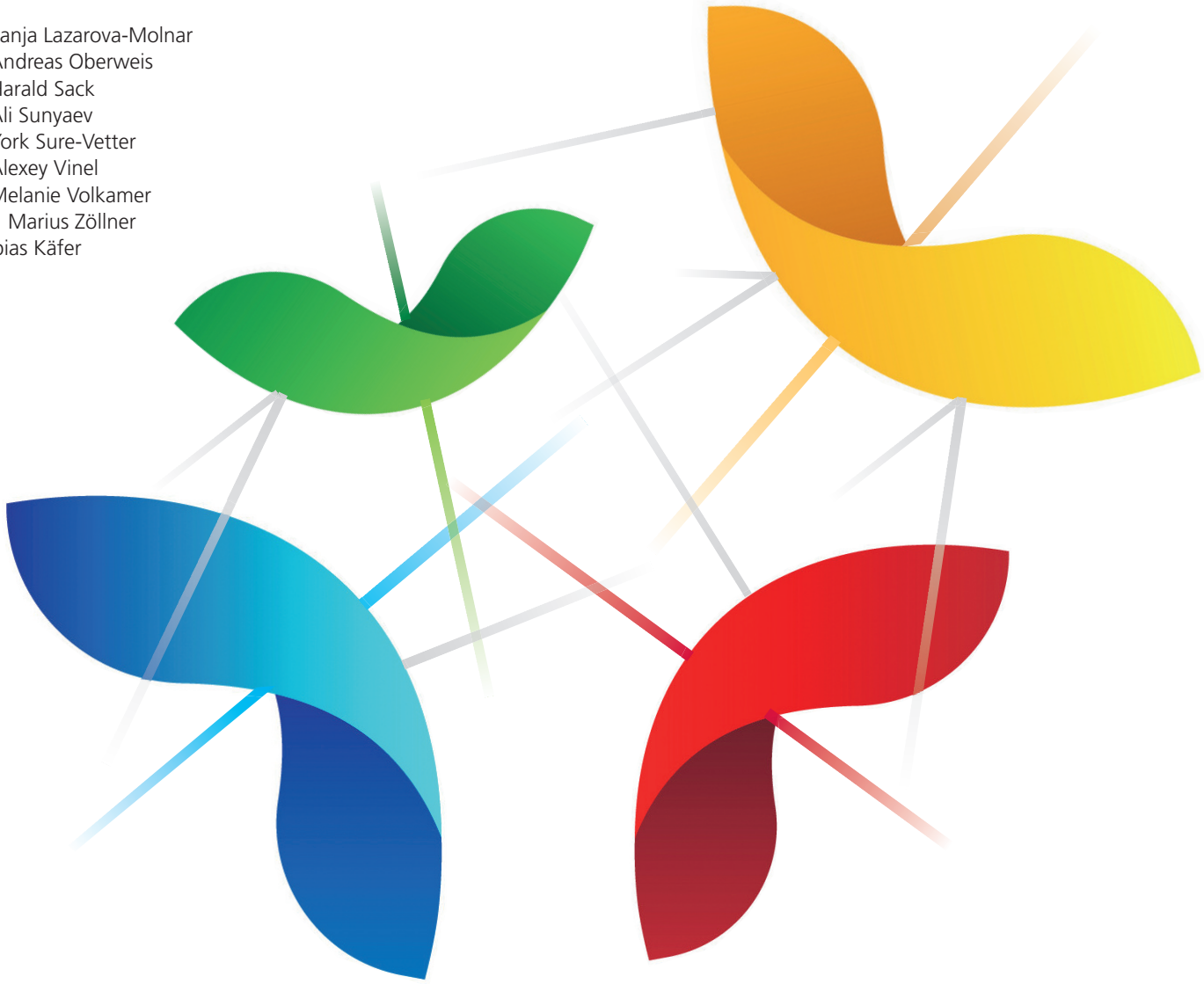
arbeiten am Institut AIFB. Sie unterstützen die Professorinnen und Professoren sowie die Studierenden im Lehrbetrieb, bearbeiten die Forschungsprojekte, viele im Rahmen einer Dissertation. Die Kolleginnen und Kollegen in Verwaltung und Technik sorgen für eine funktionierende Infrastruktur. 3 junge Menschen haben regelmäßig einen Ausbildungsplatz am Institut. 1 Honorarprofessor, 1 apl. Professor und 5 Lehrbeauftragte bereichern das Lehrangebot. Dem Institut nach wie vor eng verbunden sind 4 emeritierte bzw. pensionierte Professoren. Jeweils zwischen 80 und 100 studentische und wissenschaftliche Hilfskräfte sind in den Projekten bzw. als Tutorinnen und Tutoren für Lehrveranstaltungen aktiv. Zu unseren Forschungsgruppen gehören zudem über 60 weitere Doktorandinnen und Doktoranden, die am FZI Forschungszentrum Informatik und im FIZ Karlsruhe oder in kooperierenden Unternehmen arbeiten. Insgesamt umfasst das Institut derzeit ca. 250 Personen.

https://www.aifb.kit.edu/21.php

Institut AIFB: Wir machen Angewandte Informatik am KIT. Unser Ziel: Innovative Lösungen für Wirtschaft und Gesellschaft. Gerne auch für Sie und mit Ihnen.

Sprechen Sie uns bitte an!

Prof. Sanja Lazarova-Molnar
Prof. Andreas Oberweis
Prof. Harald Sack
Prof. Ali Sunyaev
Prof. York Sure-Vetter
Prof. Alexey Vinel
Prof. Melanie Volkamer
Prof. J. Marius Zöllner
Dr. Tobias Käfer



Kontakt
Karlsruher Institut für Technologie (KIT)
Institut AIFB
Postfach 6980
76049 Karlsruhe
www.aifb.kit.edu

Herausgegeben von
Karlsruher Institut für Technologie (KIT)
Prof. Dr. Oliver Kraft
in Vertretung des Präsidenten des KIT
Kaiserstraße 12
76131 Karlsruhe
www.kit.edu

Redaktionelle Bearbeitung
Dr. Daniel Sommer, Institut AIFB
daniel.sommer@kit.edu
Vera Münch, Alfeld
vera-muench@kabelmail.de
Ralf Baumann, REDACTIV
https://redactiv-text.de/
Gestaltung
Studio Quitta, München
www.studio-quitta.de
Druck
Systemedia GmbH, Wurmberg
www.systemedia.de

September 2024
ISBN 978-3-944361-10-9

100% Recyclingpapier mit dem Gütesiegel „Der Blaue Engel"