KASTEL Security Research Labs

Topic Engineering Secure Systems

Insight

Special Issue 2025

KASTEL

Focus on: Topic Engineering Secure Systems ESS

Editorial Notes

Published by

KASTEL – Institute of Information Security and Dependability,
Topic “Engineering Secure Systems”
Head of institute: Prof. Dr. Jörn Müller-Quade

Editorial Team

Dr. Klaus Lehmann,
Dr. Martin Schmidt,
Dr. Mario Strefler,
Annette Wettach

Copy-Editing

mentorium GmbH, Berlin

Layout & Print

modus: medien + kommunikation gmbh
76829 Landau in der Pfalz
www.modus-media.de

Contact

KASTEL – Institute of Information Security and Dependability
Topic “Engineering Secure Systems”
Am Fasanengarten 5, 76131 Karlsruhe, Germany
E-mail: geschaeftsstelle@kastel.kit.edu
https://ess.kastel.kit.edu/

Graphics

Dorfjungs., Karlsruhe
modus: medien + kommunikation gmbh, Landau

Photos & Figures

Adobe Stock: p. 5; Patricia Arias Cabarcos: pp. 20, 44;
CRC 1608 Convide, KIT: p. 20; Fraunhofer IEM, p. 10;
Patricia Guerra-Balboa: p. 44; Emilia Grass: pp. 20, 44, 46;
Sebastian Hahner: p. 44; Robert Heinrich: p. 45;
Karlsruhe Institute of Technology (KIT): pp. 7, 9, 13, 20, 21, 23, 31, 33, 39, 71;
Raffaela Mirandola: p. 20; Peter Mayer: pp. 20, 45;
Maximilian Noppel: p. 45; André Platzer: p. 21;
Ralf Reussner: p. 21; Andy Rupp: p. 21;
Indra Spiecker gen. Döhmann: p. 21; Ali Sunyaev: p. 21;
Marcel Tiepelt: p. 45; WIBU-SYSTEMS AG: p. 11;
Marcus Wiens: p. 21; Christian Wressnegger: pp. 7, 21, 45, 48;
J. Marius Zöllner: p. 20; Frederike Zufall: p. 20

April
2025

CONTENTS

Castel del Monte

Castel del Monte is one of the most impressive buildings of the Hohenstaufen Emperor Frederick II (1194-1250), which was built in the 1240s. It is situated on a hill dominating the landscape, some 15 km south of the city of Andria in northern Puglia (in the present-day province of Barletta-Andria-Trani, southern Italy). Many aspects of the layout, architecture, and purpose of the building are still not definitively understood. However, the *Castel* gives the viewer the ideal image of a fortified castle. The "ideal" architecture whose external clarity stands in confusing contradiction to the labyrinthine spatial structure of the building. Upon entering the *Castel*, visitors quickly lose their orientation despite (or because of) the seemingly perfect symmetry of the structure.[1]

We have chosen the image of Castel del Monte as the symbol of the Competence Center for Applied Security Technology KASTEL, and since 2021 KASTEL Security Research Labs (SRL), to figuratively express the fact that an attacker cannot reach the target of the attack directly and only with great difficulty, even after overcoming massive protective walls. As part of the KASTEL SRL, the Helmholtz Topic ESS aims to further advance the security of critical infrastructures.

[1] Cf.: Th. Biller (2021): Die Burgen Kaiser Friedrichs II. in Süditalien. Höhepunkt staufischer Herrschaftsarchitektur. – Wissenschaftliche Buchgesellschaft, Darmstadt, 287 pp.

Editorial & Opening Messages

Executive Board of the Topic Engineering Secure Systems (ESS)

Prof. Dr. Jörn Müller-Quade
Spokesperson

Prof. Dr. Christian Wressnegger
Co-Spokesperson

Dr. Mario Strefler
Topic Office Manager

Big Science in KASTEL: The Helmholtz Topic Engineering Secure Systems

Europe is in the middle of a transition towards CO_2 neutrality. The increasing reliance on renewable energy sources leads to decentralization of production and fundamental changes in the control of our energy networks. In the mobility sector, the transition towards sustainability goes beyond the electromobility; with increasing autonomy of vehicles, we must re-think mobility concepts that include car-sharing and ride-sharing. Production systems that form the backbone of Germany's economic strength also need to be adapted. High wage costs make automation and the close human-machine interaction necessary.

While digitalization is a crucial enabler of these changes, it also creates new challenges. Attacks on networked systems benefit from effects of scale, as simultaneous attacks on large numbers of components at the same time now become possible. Beyond the possibility of cyber-sabotage by nation-state actors, criminal organizations engage in blackmail using the threat of releasing sensitive data, locking up systems, and/or distributed denial of service attacks.

As a cybersecurity research center, KASTEL Security Research Labs is concerned with those problems yet unsolved. The goal of the Topic "Engineering Secure Systems" (ESS) is to find new solutions today that tackle the difficult security problems of tomorrow, so that the development of future systems can be adapted. In contrast, cybersecurity problems resulting from insufficient or inadequate application of established principles not part of Helmholtz research and are therefore not addressed further in the Topic ESS.

Traditional cybersecurity research at universities aims to solve specific disciplinary problems, often on a mostly academic level. Industrial R&D, on the other hand, usually aims to solve only problems of a specific system and often does not generalize sufficiently to be applicable elsewhere. Moreover, results are usually kept secret. Topic ESS follows a scientific engineering approach that focuses on critical infrastructures and takes a system perspective.

Thus, comprehensive engineering for secure systems is at the heart of the Topic ESS. Engineering in this context refers to

systematically achieving working solutions that are not only secure, private, and safe, but also yield guaranteed quality properties (e.g., performance, dependability, usability, and also costs) and achieve the best possible trade-offs between conflicting goals regarding different quality requirements, as well as societal aspects.

One key feature of Helmholtz research is the ability to take a long-term view. Anticipating the problems that future systems will face and striving for actual practical solutions is what distinguishes the Topic ESS from other research. This can only be achieved by focusing on defined application areas. What substantially distinguishes Topic ESS is the emphasis placed on interdisciplinary research and on quantifying security. Quantifying security is what enables engineering of secure systems; it stays clear of heuristics and allows systematic trade-offs between security goals and other requirements instead. Arguably, it fosters broader understanding of the security of the system under consideration.

A security-engineering approach must be investigated in domain-specialization and done in interdisciplinary research team to yield relevant results. Therefore, the Topic ESS established application-specific security-engineering labs connected to existing infrastructures which are dedicated to a specific application area. Research groups complement this approach by focusing on cross-cutting issues.

Our Vision

- As one of the leading international research institutions, we make significant contributions to interdisciplinary research into comprehensive solutions for security and privacy for complex networked systems.
- We encompass the spectrum from basic research to applied research, including transfer to industry, society, and politics.
- We are researching the quantification of security and privacy.
- With the results of our research, we strengthen the free and democratic society based on European characteristics.

Our Mission

- We achieve our goals through socially relevant preventive research, particularly safety and security in the application domains of energy, mobility, and production. To this end, we operate dedicated laboratories and associated research groups.
- Our goals are to understand security at a theoretical level, to improve security in the application domains, and to quantify security for specific demonstrators.
- We actively and promptly contribute our research findings to the economy, society, and politics.
- We are guided by the unity of research, teaching, and innovation.

Impressions I

Team discussions during a meeting at the Karlsruhe Research Factory:

Hannes Hartenstein, Martina Zitterbart, Ingmar Baumgart, Thorsten Strufe, ...

... Jörn Müller-Quade, ...

... Christopher Gerking, Jürgen Beyerer, Bernhard Beckert, and Christian Wressnegger.

PROF. DR. ERIC BODDEN

- Member of Steering Committee, Fraunhofer Institute for Mechatronic Systems Design IEM, Paderborn
- Vice-Dean and Professor, Department of Computer Science, Paderborn University
- Member of the Executive Board, Heinz Nixdorf Institute, Paderborn
- Head of Specialist Group Secure Software Engineering, Heinz Nixdorf Institute, Paderborn

Fraunhofer IEM, Paderborn University, Heinz Nixdorf Institute

Dear reader,

Due to billions in ransomware payments and looted cryptocurrency, over the last decade hacker organizations were able to significantly professionalize their operations. Moreover, radical shifts in the geopolitical landscape have heightened the threat of nation-state attacks to Germany's and Europe's critical infrastructures.

It remains a constant challenge to engineer software and software-intensive systems securely despite this changed threat landscape. Yet, unfortunately, experience has shown that we must accept any larger system to be insecure. Even if we are unaware of vulnerabilities right now, it is just a matter of time before someone – hopefully one of us – uncovers some.

We therefore must engineer future systems to guarantee a strong level of attack resilience despite yet unknown vulnerabilities, e.g., through multifaceted security controls that allow for defense in depth. To be able to take well-informed design decisions, we require methods and tools to quantify such attack resilience, not just after the fact but already at design time.

As a professor for Secure Software Engineering at the Heinz Nixdorf Institute at Paderborn, one of Germany's research hubs on cyber-physical systems security, I am extremely pleased by the excellent progress that KASTEL has achieved in this important research direction.

I wish all researchers involved a continued success!

Prof. Dr. Eric Bodden

OLIVER WINZENRIED

- Co-founder and CEO of WIBU-SYSTEMS AG, Karlsruhe

WIBU-SYSTEMS AG

Dear reader,

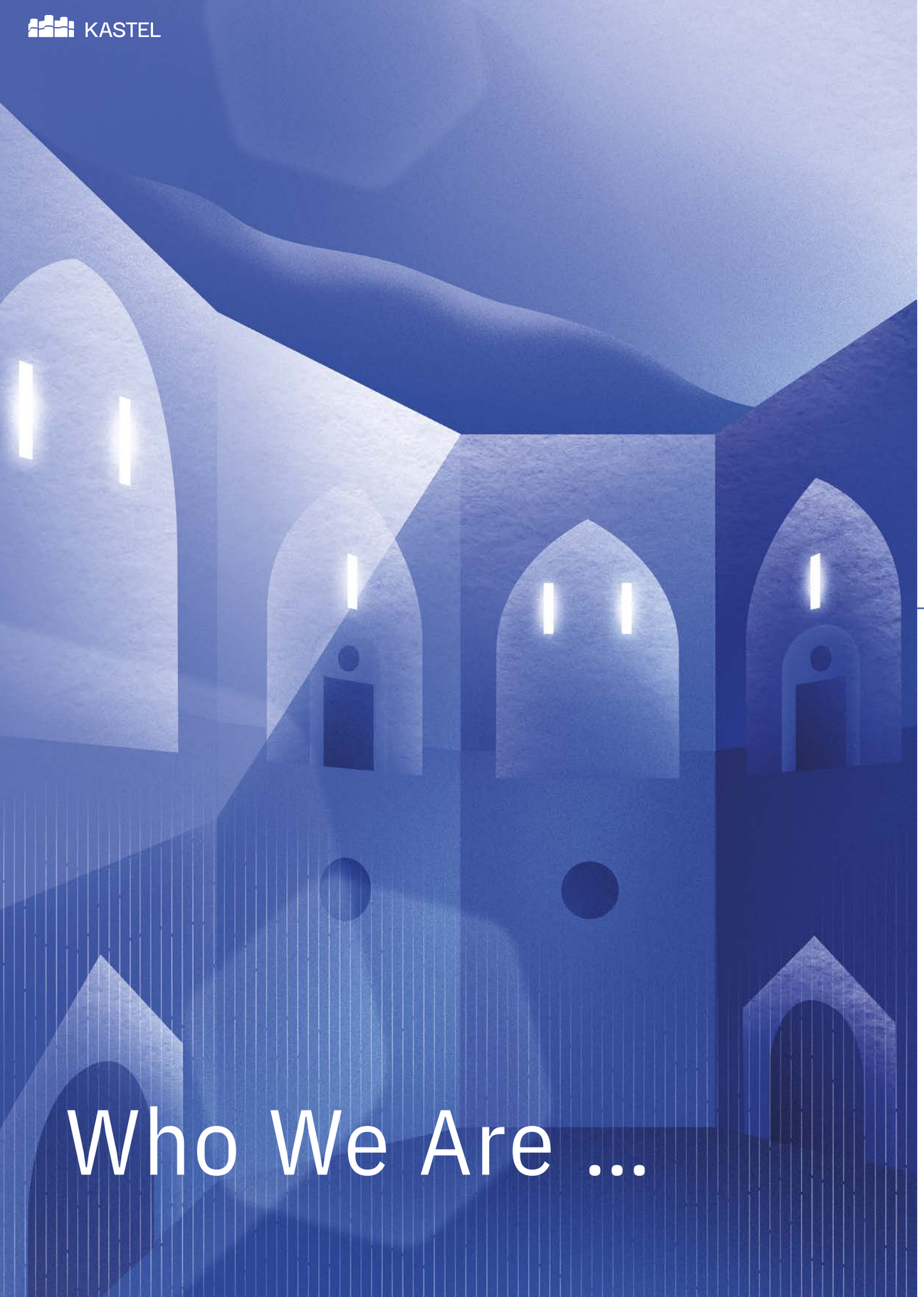
KASTEL and WIBU-SYSTEMS have been working together over the course of many years with the common goal of advancing IT security. Back in 2014, we were able to celebrate an important milestone in our collaboration: together with KASTEL and the FZI, we won the prestigious German IT Security Award of the Horst Görtz Foundation. The prize was awarded for "Blurry Box cryptography", which provides special protection for software. The process was integrated into a successful product and the demonstrator is still in use, regularly being part of scientific exhibitions, e.g., at the ZKM – Center for Art and Media Karlsruhe.

Since then, we have continued to be partners in a number of BMBF-funded research projects, first with the KASTEL Competence Center, later with KASTEL Security Research Labs and the Topic Engineering Secure Systems (ESS). We were particularly interested in the security of hardware components, e.g., for medical end devices, in the post-quantum era, which led to impressive results.

In view of the current international situation, the goal of protecting society is becoming increasingly important. And we are proud, as part of the security research location Karlsruhe, to be able to work in concert with KASTEL and the Topic ESS and contribute to safeguard society with novel solutions.

I am sure that the Topic ESS will carry on the spirit of cybersecurity and I look forward to continuing our fruitful cooperation.

Oliver Winzenried



KASTEL –
from Competence Center to Helmholtz-Topic

The "Competence Center for Applied Security Technology" KASTEL was founded in 2011 as one of three national competence centers for IT security funded by the German Federal Ministry of Education and Research (BMBF) for a period of four years.

The unique situation in Karlsruhe as a research location was of great benefit: the extensive expertise of the institutional partners (1) Karlsruhe Institute of Technology (KIT), (2) FZI Research Center for Information Technology, and (3) Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB in various areas of theoretical and applied cybersecurity were part of an unprecedented line-up. From the beginning, KASTEL has explicitly focused on interdisciplinary research that combines the most diverse aspects of cybersecurity. The successes achieved since then show that this concept has proven its worth. This also contributed to the funding being extended and significantly increased by the BMBF following a successful evaluation in 2014.

KASTEL was established as an important part of the cybersecurity location Karlsruhe and as a permanent element in the German cybersecurity landscape. In 2017/2018, KASTEL participated in the Helmholtz Association's evaluations for the fourth period of program-oriented funding (PoF IV: 2021–2027). The reviewers emphasized the particular scientific excellence of KASTEL and recommended KASTEL for permanent Helmholtz funding.

At the beginning of the funding period in 2021, key research fields of KASTEL were transferred to the Topic "Engineering Secure Systems" (ESS), as an integral part of the Program "Engineering Digital Futures" (EDF) within the Helmholtz Information research field. This provides the basis for pursuing long-term research goals that are of direct relevance to the well-being of society.

Milestones

2011
Establishment of "Competence Center for Applied Security Technology" KASTEL, funded by the BMBF, as one of three national competetence centers for IT security.

2014
Successful evaluation by BMBF.

2017, 2018
Successful evaluations by the Helmholtz Association for the PoF IV.

2021
Perpetuation of KASTEL as Topic ESS in the Program "Engineering Digital Futures" (EDF) of Helmholtz Information and as KASTEL Security Research Labs as the overarching brand.

2025
Scientific Evaluation of Topic ESS by the Helmholtz Association.

2026
Strategic Evaluation of Topic ESS by the Helmholtz Association regarding the PoF V.

Highlights

2014
"Blurry Box®" – First prize, 5th German IT Security Award of the Horst Görtz Foundation: FZI, KIT, and WIBU-SYSTEMS AG.

2016
DFG Research Training Group 2153 "Energy Status Data – Informatics Methods for its Collection, Analysis and Exploitation": KIT, participation of four KASTEL-PIs.

2023
Alexander von Humboldt Professorship for Artificial Intelligence: André Platzer.

2023
Start of Helmholtz Investigator Group "Building Network Resilience in Healthcare against Cyber-Attacks": Emilia Grass.

2023
Funding of the Collaborative Research Center 1608 "Convide".

2024
KASTEL-PIs are Spokespersons of Research Division "Cybersecurity and Law" at FZI Research Center for Information Technology.

Competence Center for Applied Security Technology

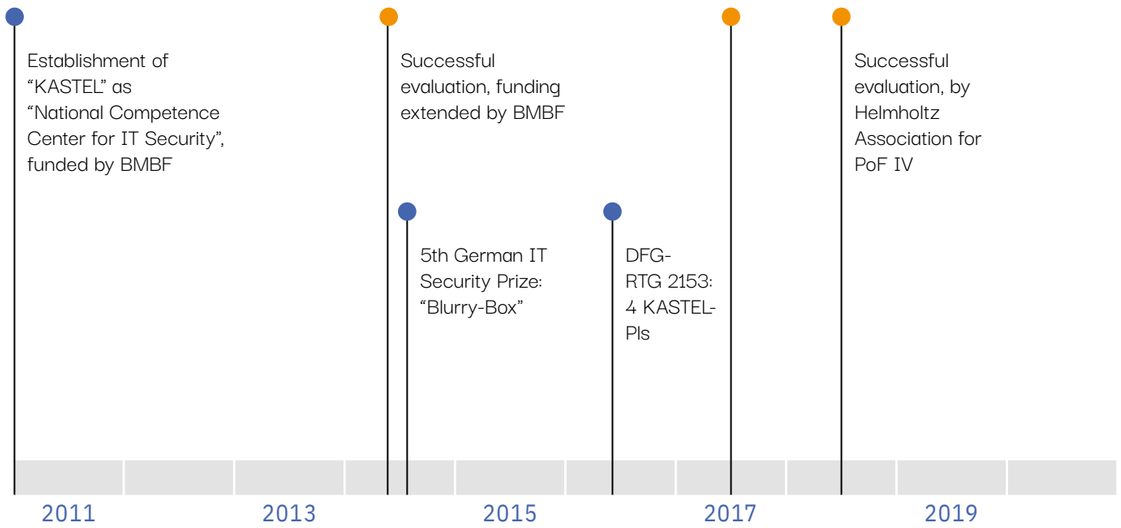
Bundesministerium für Bildung und Forschung

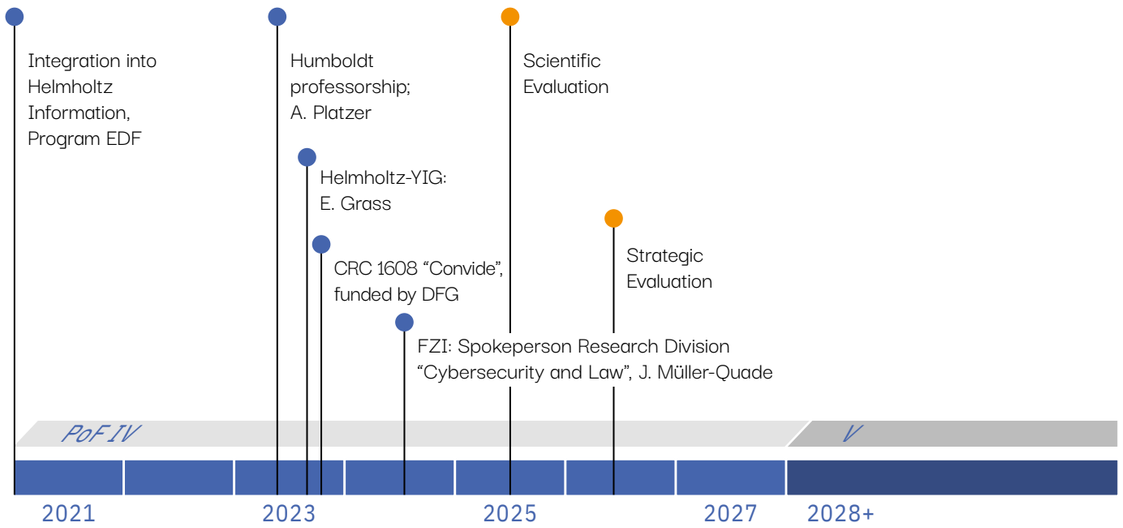
KASTEL Security Research Labs

Top Engineering Secure Systems

HELMHOLTZ

Topic Dependable Intelligent Cyberphysical Systems





KASTEL – IT Security Research in Karlsruhe

The Topic Engineering Secure Systems (ESS)

Our Topic ESS is dedicated to researching theoretically sound, targeted and effective IT security measures to protect critical infrastructures. This is achieved by considering both the social and human as well as the technical aspects of cyber-physical systems. In this context, security encompasses the aspects of safety, dependability, and privacy.

To this end, Topic ESS is organized in three Research Groups focusing on cross-sectional methodology on Quantifying Security (Q), Engineering Secure Computation and Communication (C&C), and Human and Societal Factors (HSF) – in Subtopic 1 – and three domain-specific Security Labs focusing on engineering security in the application domains energy, mobility, and production – in Subtopics 2 to 4, respectively.

- Subtopic 1:
  Methods for Engineering Secure Systems
  - Research Group Quantifying Security
  - Research Group Secure Computation and Communication
  - Research Group Human and Societal Factors
- Subtopic 2:
  Engineering Security for Energy Systems
- Subtopic 3:
  Engineering Security for Mobility Systems
- Subtopic 4:
  Engineering Security for Production Systems

KASTEL Security Research Labs (SRL)

Even after the end of the funding period of the "Competence Center for Applied Security Technology" in 2021, the name KASTEL will live on in "KASTEL Security Research Labs" (KASTEL SRL) and refers to an alliance for joint research in the field of IT security in Karlsruhe. KASTEL SRL acts as an umbrella brand that is supported by its institutional partners

- Karlsruhe Institute of Technology KIT
- Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB
- FZI Research Center for Information Technology

KASTEL SRL encompasses the activities of the Topic ESS, but also goes beyond this by covering a broader spectrum of research in the field of IT security, in which other Fellows and working groups are involved.

IT Security Region Karlsruhe

Karlsruhe is an outstanding research location in the field of cybersecurity due to its broad spectrum of research and application. In addition to the contribution of KASTEL SRL, the Karlsruhe IT security region is also supported by

- Karlsruher IT Sicherheitsinitiative (KA IT-Si)
  (Karlsruhe IT Security Initiative, initiated and coordinated by Secorvo GmbH),
- Kompetenzzentrum IT-Sicherheit
  (IT Security Competence Center), further developed into the research area "Cybersecurity and Law" at FZI in 2024.

with an extensive network of developers, practitioners, and users from business and industry.

KASTEL – IT Security Research in Karlsruhe

IT Security Region
Karlsruhe

KASTEL
KASTEL Security Research labs

HELMHOLTZ
Topic "Engineering Secure Systems" (ESS)

FZI Research Center for Information Technology

Fraunhofer IOSB
Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB

Kompetenzzentrum IT-Sicherheit
Competence Center for IT Security (at FZI)

KA-IT-Si
Karlsruher IT-Sicherheitsinitiative
(Karlsruhe IT Security Initiative)

Karlsruher Institut für Technologie

KASTEL	Institute of Information Security and Dependability
IAI	Institute for Automation and Applied Informatics
TM	Institute of Telematics
IAR	Institute for Anthropomatics and Robotics
AIFB	Institute of Applied Informatics and Formal Description Methods
ZAR	Center for Applied Legal Studies

In cooperation with:
- University of Luxembourg
- University of Cologne
- TU Bergakademie Freiberg

The different organizational layers

- Topic "Engineering Secure Systems" (ESS)
- KASTEL Security Research Labs
- IT Security Region Karlsruhe

of IT security research in Karlsruhe and their constituting and supporting institutions become apparent in this structural presentation.

Our Principal Investigators

The Topic Network

Prof. Dr.
Patricia Arias
Cabarcos

TT-Prof. Dr.
Frederike Zufall

Prof. Dr.
J. Marius Zöllner

Prof. Dr.
Martina Zitterbart

Prof. Dr. Christian
Wressnegger

Prof. Dr.
Marcus Wiens

Prof. Dr.
Melanie
Volkamer

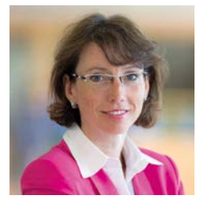
PD Dr.-Ing.
Ingmar
Baumgart

Prof. Dr.
Ali Sunyaev

Prof. Dr.
Bernhard
Beckert

Prof. Dr.
Thorsten
Strufe

Prof. Dr.-Ing.
habil. Jürgen
Beyerer



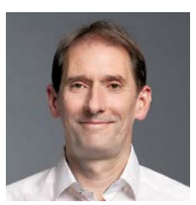
Prof. Dr.
Indra Spiecker
gen. Döhmann

Jun.-Prof. Dr.
Emilia
Grass

Prof. Dr.-Ing.
Ina Schaefer

Prof. Dr.
Veit
Hagenmeyer

Dr. Andy
Rupp



Prof. Dr.
Hannes
Hartenstein

Prof. Dr.-Ing.
Anne Koziolek

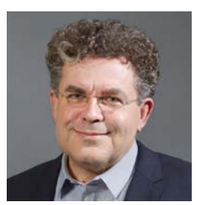
Prof. Dr.-Ing.
Peter Mayer

Prof. Dr. Raffaela
Mirandola

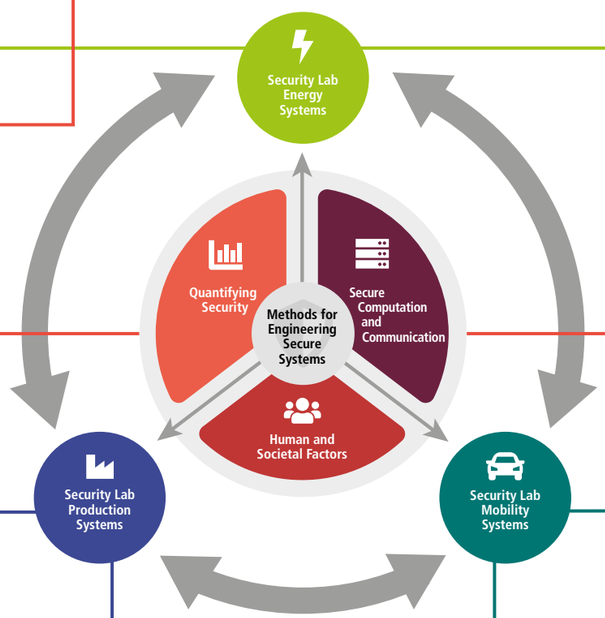
Prof. Dr. Jörn
Müller-Quade

Prof. Dr.
André Platzer

Prof. Dr. iur.
Oliver Raabe



Prof. Dr.
Ralf Reussner

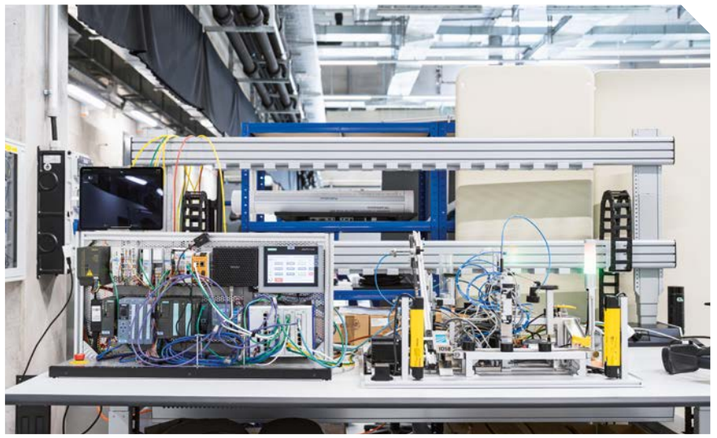


Research Foci

Impressions II

FENCE: Future ENergy Cybersecurity Evaluation: Security Lab Energy.

Attacks on Traffic Light Recognition and Countermeasures: Security Lab Mobility.



Continuous Automated Risk Management (CARM) System for Industrial Networks: Security Lab Production.

Subtopics, Research Groups, and Security Labs

The structure of Topic ESS with its three Research Groups in "Methods" (Subtopic 1) and its Security Labs (Subtopics 2–4) was chosen in order to establish an efficient framework for implementing newly developed theoretical approaches and methods for direct use in the application areas of energy, mobility, and production.

Subtopic 1 – Methods for Engineering Secure Systems

Research Group "Quantifying Security" (Q)

Our Research Group is highly interdisciplinary with PIs from the disciplines Cryptography, IT Security, Privacy, Formal Methods, Software Engineering, Business Economics, and Operations Research, allowing to cover the most important aspects of a system as well as its use.

Quantitative security analyses are necessary to determine the risk and pave the way to practical adoption (e.g., VINKRYPTOR with Mercedes-Benz AG, IIP 2.0 with S.A.F.E e.V., SECAIMED with German Cancer Research Center, DKFZ).

In comparison to our competitors, our methods for quantitative analyses have the same rigor as established qualitative ones.

Research Group "Secure Computation and Communication" (C&C)

We work on formal modeling, design, analysis, and evaluation of methods for securing computation architectures and communication infrastructures. Our focus is on generic cross-cutting challenges of great importance with broad applications and benefits to our Security Labs, on three layers:

- *Secure protocols* striking a balance between user privacy and diametral real-world requirements stemming from laws, regulations, business models, etc.
- *Secure communication* in increasingly digitalized critical infrastructures for electricity, water, and goods for basic human and industrial needs.
- *Secure software* through a continuous combination of modeling and analysis across all phases of the software development lifecycle.

Research Group "Human and Societal Factors" (HSF)

Our research covers the area of human- and law-aligned security and privacy by design.

Our Research Group has four research areas and one cross-cutting topic (digital democracy).

Our demonstrators like security awareness videos and games are available for society (e.g., ZKM – Center for Art and Media Karlsruhe, German Spy Museum Berlin).

Subtopic 2 – Engineering Security for Energy Systems

Security Lab Energy Systems

Our Lab is providing security to the critical energy infrastructure by bundling the Helmholtz energy competencies at KIT (especially: world-leading energy informatics, software engineering, etc.) and applying them in physical hardware labs for real solutions.

We focus on a demonstrator that highlights the interconnectivity of DERs (distributed energy resources), e-mobility, and substations.

We are engaged with international energy research centers, industry partners, standardization committees, and partnering with international labs that focus on energy systems.

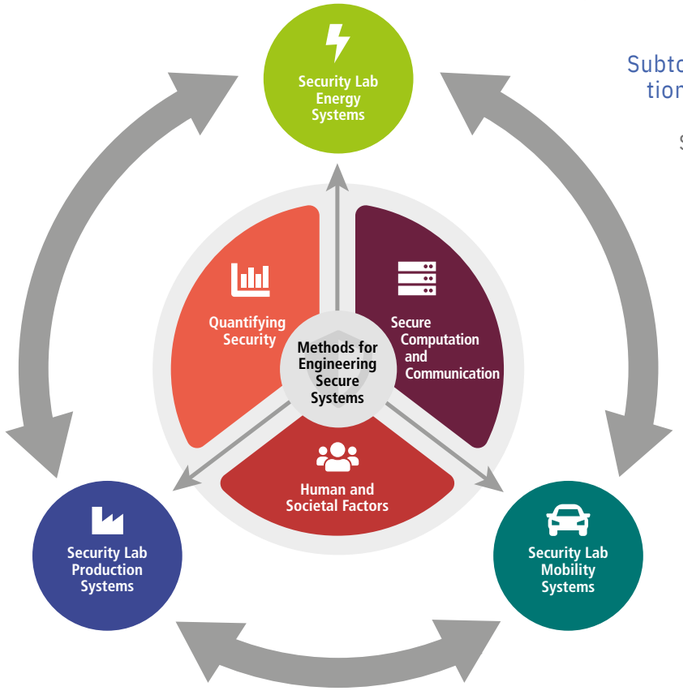
Subtopic 3 – Engineering Security for Mobility Systems

Security Lab Mobility Systems

Our mission is shaping the future of secure mobility in application fields such as autonomous driving, vehicular communication and mobility services.

Our research is intertwined into dependable protection mechanisms and flexible development measures.

Our research will be demonstrated in Test Area Autonomous Driving Baden-Württemberg (TAF BW).



Subtopic 4 – Engineering Security for Production Systems

Security Lab Production Systems

We conduct cybersecurity research in production, i.e., investigate cybersecurity and privacy questions ranging from manual assembly to fully-automated production.

Industrial systems are critical infrastructure as soon as they control, e.g., the production of food or pharmaceutical goods.

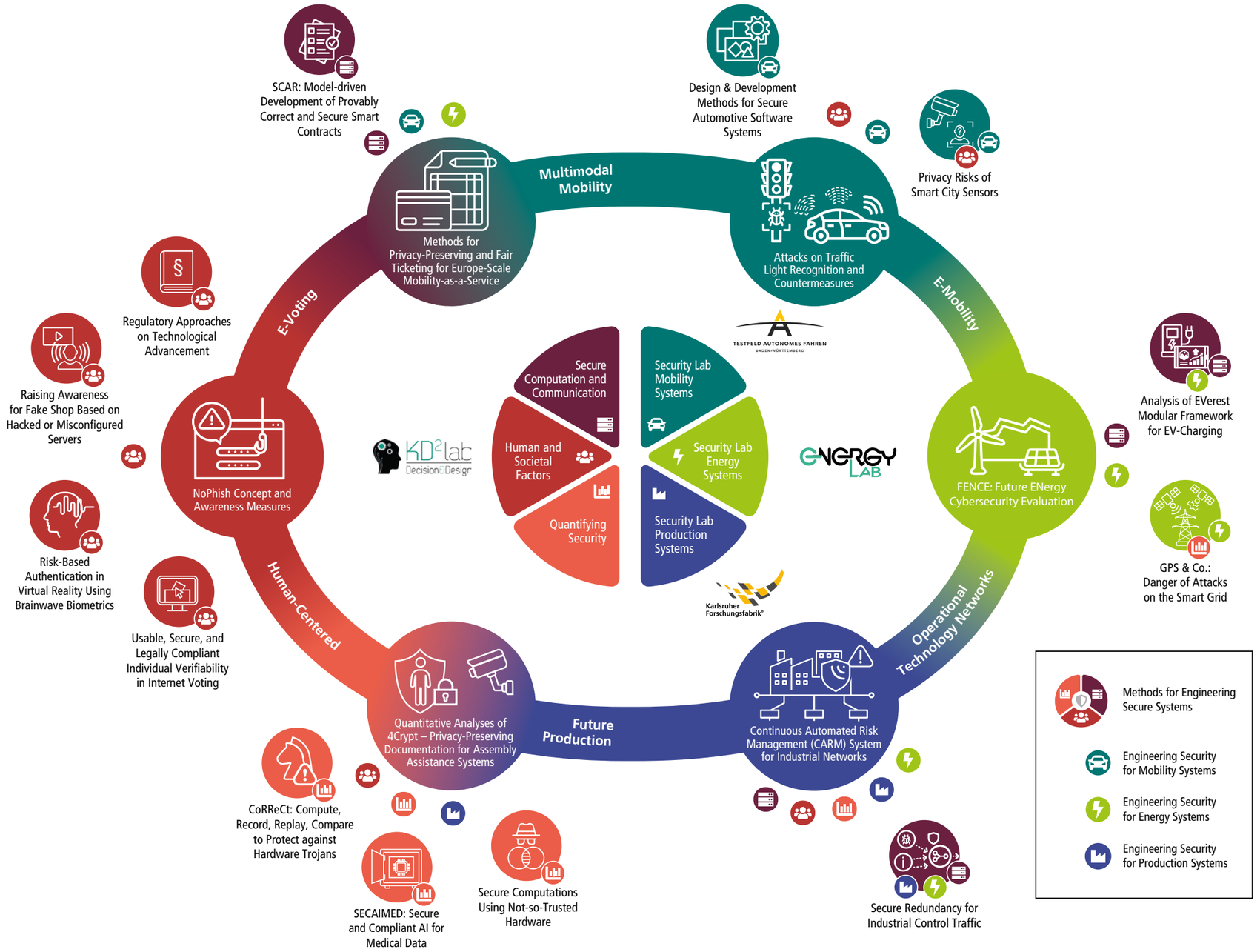
We use miniaturized automation processes with real control system components and an interactive assembly station for collecting data as well as for developing and evaluating security mechanisms.

Demonstrator Landscape

We present our research results in the form of "demonstrators" that illustrate the developed concepts with of prototypes or visualizations. Especially in IT security research, this has proven to be a suitable means of making the effects of abstract methods and concepts understandable.

The demonstrator "landscape" presents the demonstrators of the individual Research Groups and Security Labs and thus reflects the broad thematic diversity and the multiple cross-references between them. This shows that all contributions are geared towards the common goal of strengthening IT security in line with our mission.

The demonstrators are arranged thematically and use color coding – according to the inner circle – to represent interconnection and targeted collaboration. Color gradients indicate main contributors, while Research Group, Security Lab, and Subtopic symbols highlight additional contributors.



Color scheme:

- *Shades of red: Subtopic 1: Methods for Engineering Secure Systems*
  - *Light Red: Research Group "Quantifying Security" (Q)*
  - *Dark Red (berry): Research Group "Secure Computation and Communication" (C&C)*
  - *Red: Research Group "Human and Societal Factors" (HSF)*
- *Light green (lime): Subtopic 2: Engineering Security for Energy Systems (Security Lab Energy Systems)*
- *Dark green (pine green): Subtopic 3: Engineering Security for Mobility Systems (Security Lab Mobility Systems)*
- *Blue: Subtopic 4: Engineering Security for Production Systems (Security Lab Production Systems)*

Demonstrators (1)

Our demonstrators have emerged from the networked, interdisciplinary research activities in the Research Groups and Security Labs and illustrate the most important research results in the Topic ESS. Results that have made further contributions to the Topic as part of our IT security roadmap are also presented in the form of demonstrators. These represent relevant specific aspects that are of great value for achieving our goals.

Quantitative Analyses of 4Crypt – Privacy-Preserving Documentation for Assembly Assistance Systems

We present a privacy-friendly and trustworthy interactive assembly table as a show-case for our methodological results with respect to quantification. It uses cameras and AI to provide support during assembly tasks. The video feed can also be recorded for later analysis of critical work steps.

While this is useful for quality control, it also entails a major privacy concern, as workers may be subjected to unfounded video surveillance by their employer. We quantify the privacy-related technical mechanisms of 4Crypt with respect to their security as well as their effect on workers.

Methods for Privacy-Preserving and Fair Ticketing for Europe-Scale Mobility-as-a-Service

This demonstrator showcases three different methods to realize key functionalities of a multi-provider check-in/out transportation system such as billing, clearance, payments, and further data analytics in a privacy-preserving and scalable way. Our distributed architecture based on trusted execution environments can handle the check-in/out volume of a Europe-scale system even under server dropouts.

Our architecture based on secure multi-party computation shows that very strong privacy guarantees for a city-scale system are achievable. With our payment channel network-based protocol, we demonstrate how instantaneous payment and clearing with formally verifiable security can be realized.

NoPhish Concept and Awareness Measures

The "NoPhish Concept and Awareness Measures" demonstrator provides, on the one hand, background information about the Human and Societal Research Group and applied research methods; and on the other hand, it showcases four developed anti-phishing awareness measures: the NoPhish videos, two serious games for different target audiences, and the Security Teaching & Awareness Robot (STAR).

Additionally, the demonstrator provides information on the extent to which the NoPhish concept and its measures have been implemented in the scientific community, by organizations, and by end-users. Notably, 11 federal institutions, including the BSI, as well as 29 research institutions, have adopted and/or recommended the NoPhish measures, and the videos have garnered over 30,000 views on YouTube.

FENCE: Future ENergy Cybersecurity Evaluation

FENCE is a cybersecurity research platform bridging theoretical methods and practical security implementations within the energy sector. Built upon a realistic infrastructure at KIT's Campus North – the KASTEL Security Lab Energy – it comprises several subsystems modeling renewable energy plants, multi-vendor digital substations, software-defined network setups, and PLC-based power plant simulations. We demonstrate a multi-stage cyber-attacks exploiting vulnerabilities in the S7 protocol, widely used in industrial control systems of power plants.

FENCE facilitates a thorough analysis of vulnerabilities, supports research in intrusion detection, and enables effective mitigation strategies and systematic risk assessment. It specifically targets critical cybersecurity challenges within energy systems and presents our research findings through an intuitive web interface for enhanced accessibility and usability.

Attacks on Traffic Light Recognition and Countermeasures

"Attacks on Traffic Light Recognition" demonstrates practical real-world attacks against neural networks in autonomous driving (AD). By exploiting backdoor and inference time attacks, an adversary can manipulate the perception module's predictions, resulting in hazardous actions – such as running red lights.

While such attacks were previously demonstrated using offline datasets, we are the first to effectively compromise a full-fledged autonomous vehicle in real-world conditions. Our research demonstrates that attacks against camera-based perception in AD are practical. To mitigate these threats, we explore the security of XAI-based defenses and propose anti-backdoor learning techniques.

Continuous Automated Risk Management (CARM) System for Industrial Networks

Continuous Automated Risk Management (CARM) is a non-intrusive industrial network security monitoring framework designed to assist Asset Owners of operational industrial systems in managing risks and developing the IEC 62443-mandated security architecture.

CARM automates system information collection, assesses security posture, and measures descriptive security metrics using machine learning and graph theory-based analyses. It also helps select the optimal set of technical countermeasures while considering constraints such as budget limitations.

Demonstrators (2)

Secure Computations Using Not-so-Trusted Hardware

At the Lindau Nobel Laureate Forum, we presented a demonstrator for the task of private set intersection based on a novel combination of cryptography and secure hardware.

SCAR: Model-driven Development of Provably Correct and Secure Smart Contracts

The SCAR approach enables model-driven development of smart contract applications with formally proven correctness and security properties.

SECAIMED: Secure and Compliant AI for Medical Data

In "SECAIMED", researchers from DKFZ and Topic ESS jointly develop a novel and legally compliant approach for secure machine learning with applications in medicine.

Secure Redundancy for Industrial Control Traffic

We demonstrate a novel attack against packet redundancy mechanisms, as used in industrial automation, on a model production process.

CoRReCt: Compute, Record, Replay, Compare to Protect against Hardware Trojans

CoRReCt provides a novel approach to protect against corrupted hardware based on a secure architecture. A centrally trusted component underwent formal verification.

Risk-based Authentication for Virtual Reality Using Brainwave Biometrics

We demonstrate how brainwave authentication enhances the VR experience during routine tasks while securing critical actions, such as payments via graphical passwords.

Analysis of EVerest Modular Framework for EV-Charging

Continuous analysis of software system requirements, design, and implementation is important to detect vulnerabilities in EV-charging units to ensure security.

Usable, Secure, and Legally Compliant Individual Verifiability in Internet Voting

The processes of casting and verifying one's vote are shown to demonstrate how voters can detect dishonest voting devices / voting systems manipulating their vote.

Raising Awareness for Fake Shops Based on Hacked or Misconfigured Servers

We present the development of two awareness videos aimed at making website owners aware of attacks on webservers that redirect users to fake online shops.

Privacy Risks of Smart City Sensors

The demonstrator visualizes proposed smart city sensors such as thermal and depth cameras, lidar and radar in real-time and thus highlights their privacy risks.

Regulatory Approaches on Technological Advancement

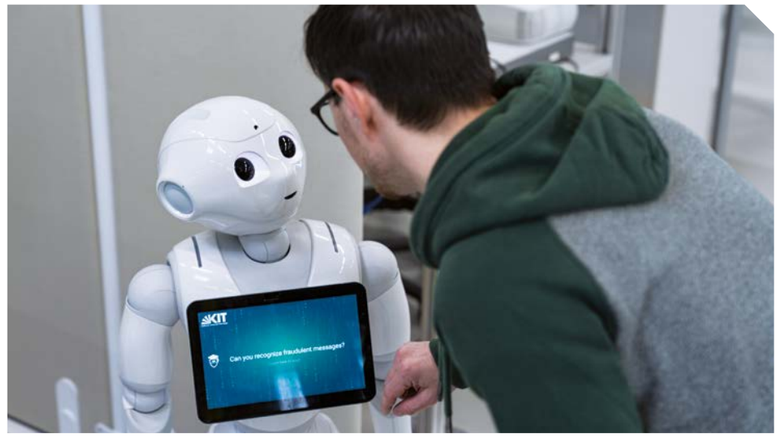
We work on identifying potential improvements of law patterns and operationalization through a legal and technological view regarding risks originating from technical advancement.

Design & Development Methods for Secure Automotive Software Systems

With this demonstrator, we focus on engineering secure software systems using constructive and analytical methods, spanning multiple design/development phases including legal analysis.

GPS & Co.: Danger of Attacks on the Smart Grid

This demonstrator is used to investigate critical threats from manipulated GNSS signals compromising precise time synchronization necessary for digital substation operations.



Transfer from Methods into Application Domains

To ensure that our research can achieve the greatest possible benefit for society, the structure of Topic ESS with its Research Groups in "Methods" (Subtopic 1) and its Security Labs (Subtopics 2–4) was successfully used to tailor newly developed security approaches and methods to the application domains of energy, mobility, and production. The interlinking of methods and applications thus enables an effective transfer that facilitates practicable security solutions for specific real-world issues. The demonstrators developed in the Topic ESS are illustrative examples of this transfer.

From Methods to Energy:

- **Analysis of EVerest Modular Framework for EV-Charging**

We developed an approach for continuous requirements validation with design and source code analysis, and their combination. This approach detects if requirements are met at every stage of software engineering and uncovers vulnerabilities missed by isolated analysis. We applied this approach to EVerest, a system for EV-charging units. We revealed that authentication information was logged in clear text, violating confidentiality requirements.

From Methods to Mobility:

- **Methods for Design & Development**

Our method enables software architects to analyze and quantify the impact of uncertainty on the confidentiality of software systems during the software design by extracting data flow diagrams and propagating uncertainty sources. This method is especially helpful for cyber-physical systems that are operated in uncertain environments such as mobility systems. The application minimizes the analysis complexity of highly interdependent systems such as connected cars, infrastructure, and the cloud.

From Methods to Production:

- **Privacy-preserving Documentation for Interactive Manufacturing**

Together with the Research Group Quantifying Security, we performed quantitative analyses of "4Crypt". Starting from a cryptographic security proof, we quantified the cost of the adversary performing an attack relative to 4Crypt's adversarial model. Based on this analysis, we performed a quantitative game-theoretic analysis of 4Crypt, quantifying the systematic incentive of an employer to make illegitimate requests, as well as the benefits of 4Crypt's security measures.

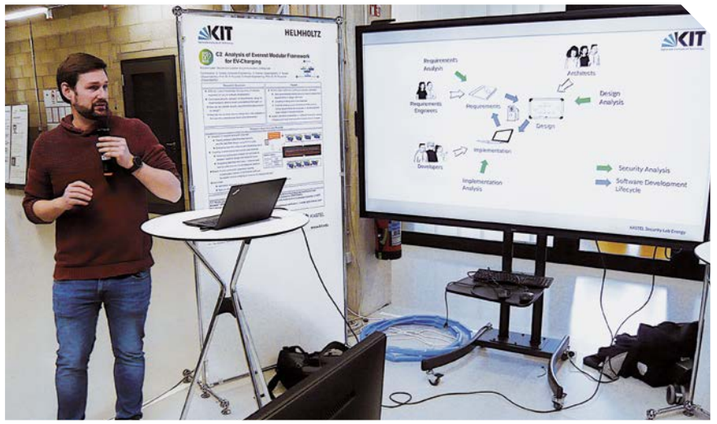
- **Augmented Reality Authentication**

The miniaturized production of the Security Lab Production process can be controlled via a user interface in augmented reality (AR). The process can be stopped, and production jobs can be modified. If this happens without authorization, there will be at least financial damage due to loss of production. Authentication in AR is therefore required to protect against unauthorized interference with the production process. In the Research Group HSF, we addressed this by developing an authentication scheme for AR with graphical passwords, which is usable and secure.

- **Secure Redundancy for Industrial Control Traffic**

During the conceptual work in the Research Group C&C, a theoretical attack was devised. The attack was considered against a generic group of mechanisms. It was however unclear, how specifically this attack could be used in the real world. Cooperation with the Security Lab Production enabled hands-on work with a representative industrial process and corresponding hardware. This enabled refining the attack to the point that it can be shown in the Secure Redundancy Demonstrator on real hardware.

Impressions III



Analysis of EVerest Modular Framework for EV-Charging: Frederik Reiche (Research Groups Q, C&C, in collaboration with the Security Lab Energy).

Quantitative Analyses of 4Crypt – Privacy-Preserving Documentation for Assembly Assistance Systems: Matin Fallahi, Paul Wagner (Research Groups Q, HSF and Security Lab Production).

Secure Redundancy for Industrial Control Traffic: Felix Neumeister (Research Group C&C and Security Lab Energy, in collaboration with the Security Lab Production).

Highlights

2021

Brainwave-based User Authentication

A common issue that many IT technology users encounter daily is the widespread use of text password-based user authentication. This method is not only unpopular among users but also has well-known drawbacks in the scientific community. An alternative is the use of brainwaves as a biometric means of proving one's identity. Specifically, the research focuses on implicit brainwave-based user authentication – that is, authentication based on electroencephalograms (EEG) that occurs continuously in the background without active user intervention. The research has shown that the developed methods can achieve very low error rates even with low-cost devices. In terms of user-friendliness, the method received high marks; test subjects found it appealing and easy to use. Overall, the results indicate that biometrics in the form of brainwave-based authentication is a promising technology and will therefore be the focus of further research.

P. Arias-Cabarcos, T. Habrich, K. Becker, C. Becker & **T. Strufe** (2021): Inexpensive Brainwave Authentication: New Techniques and Insights on User Acceptance. – Proceedings of the 30th USENIX Security Symposium (USENIX Security 21): 55–72.

2022

DISTINGUISHED PAPER AWARD

Dos and Don'ts of Machine Learning in IT Security

Learning-based systems have been increasingly used in computer security for some time. However, the use of machine learning in security involves subtle pitfalls and can significantly distort the results. In a cooperation with the London universities UCL, KCL, and Royal Holloway, as well as the TU Braunschweig and the TU Berlin, KASTEL researchers systematized ten such sources of error and surveyed their distribution in publications of the top four computer and system security conferences (IEEE S&P, ACM CCS, USENIX Security, NDSS).

D. Arp, E. Quiring, F. Pendlebury, A. Warnecke, F. Pierazzi, **C. Wressnegger**, L. Cavallaro & K. Rieck (2022): Dos and Don'ts of Machine Learning in Computer Security. – Proceedings of the 31st USENIX Security Symposium (USENIX Security 21): 3971–3988.

2023

Collaborative Research Center 1608 Convide

In 2023, we succeeded in establishing the new Collaborative Research Center (CRC) 1608: "Consistency in the View-Based Development of Cyber-Physical Systems" (Convide), funded by the German Research Foundation (DFG). The CRC aims to research novel methods for engineering cyber-physical systems (CPS), i.e., software-intensive technical systems such as modern cars or production facilities to increase their reliability, security, and adaptability. This also reflects the efforts of the Topic ESS to extend the view of security to include the characteristic "safety". These systems combine electronic, mechanical, and software-controlled components that have to interact closely with each other and thus reach a level of complexity, even at abstract architectural levels. For this reason, so-called "views" of the system are used during development. Due to the manifold dependencies between the views, the CRC is dedicated to new methods of maintaining consistency. The starting point for this are methods from software engineering, product design, and formal methods already developed within the Topic ESS. As part of the CRC, methods for "Advanced Systems Engineering" are researched in order to make the design of CPS more agile and thus more efficient. This should enable shorter development cycles and faster updates. The aim is to continuously adapt CPS to changing requirements, improve reliability and therefore also security, and introduce new features. Together with KIT, the University of Mannheim, and the Technical Universities of Dresden and Munich are also involved in the project.

https://www.sfb1608.kit.edu/

Vulnerability Analysis and Risk Assessment in Energy Systems

Vulnerability analysis in energy systems includes assessing different types of testbeds, i.e., physical, virtual, and hybrid ones for Smart Grids (SGs) from different perspectives of cybersecurity. Preliminary work on characterization of these testbeds based upon MITRE ICS Attack Matrix was published. First, the evaluation was based upon different qualitative metrics such as costs, fidelity, and flexibility. The second contribution focuses on the applicable tactics and techniques for each testbed assessing how well attack experiments can be realistically simulated using them. It was successfully highlighted how different implementations of testbeds come with their own limitations and challenges, which must be considered by a researcher while selecting a testbed for a specific use case. Current research focuses on in-depth assessment of testbeds from IT and OT perspective which could serve as foundation to the development of defensive techniques. Different vulnerabilities of components at "KASTEL Security Lab Energy" and EPIC testbed are tabulated. Additionally, the work also covers exploiting the limitations of industrial protocols, such as Modbus TCP, S7, and MMS. To further analyze the different vulnerabilities, a hybrid risk assessment process using fuzzy analytical hierarchy processes was developed.

A. Mumrez, M.M. Roomi, H.C. Tan, D. Mashima, **G. Elbez** & **V. Hagenmeyer** (2023): Comparative Study on Smart Grid Security Testbeds Using MITRE ATT&CK Matrix. – 2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm): 7 pp.

S. Canbolat, G. Elbez & **V. Hagenmeyer** (2023): A New Hybrid Risk Assessment Process for Cyber Security Design of Smart Grids Using Fuzzy Analytic Hierarchy Processes. – at-Automatisierungstechnik, 71 (9): 779–788.

2024

Adversarial Attacks and Robust Perception Methods for Autonomous Driving

Effective traffic light detection is a critical component of perception in autonomous vehicles. Within the scope of the Security Lab Mobility, we develop a novel deep-learning perception module and extensively test it in real-world traffic. Unfortunately, current solutions often are not robust against attacks, and existing defences based on explainable AI (XAI) are not as effective as initially thought. Hence, we investigate means and methods that can increase the security of traffic light detection. For instance, we show that "Mixture of Expert" (MoE) models for semantic segmentation of traffic scenes are more robust to per-instance and universal white-box input manipulation attacks and transfer attacks. Moreover, we develop approaches to withstand model manipulation attacks introduced during model training through data poisoning. In combination, these techniques push the boundaries for future, adversarially robust perception of autonomous driving.

N. Polley, S. Pavlitska, Y. Boualili, P. Rohrbeck, P. Stiller, A.K. Bangaru & **J.M. Zöllner** (2024): TLD-READY: Traffic Light Detection. – Relevance Estimation and Deployment Analysis. – IEEE International Conference on Intelligent Transportation Systems (ITSC), in press.

M. Noppel & **C. Wressnegger** (2024): SoK: Explainable Machine Learning in Adversarial Environments. – 2024 IEEE Symposium on Security and Privacy (SP), 2441–2459.

S. Pavlitska, E. Eisen & **J.M. Zöllner** (2024): Towards Adversarial Robustness of Model-Level Mixture-of-Experts Architectures for Semantic Segmentation. – IEEE International Conference on Machine Learning and Applications (ICMLA): 1460–1465.

Q. Zhao & **C. Wressnegger** (2024): Two Sides of the Same Coin: Learning the Backdoor to Remove the Backdoor. – In: T. Walsh, J. Shah & Z. Kolter (eds.): 39th AAAI Conference on Artificial Intelligence, AAAI-25 Technical Tracks, 39 (21): 22804-22812.

Publications at ICSE 2024, the Premier Software Engineering Conference

At this year's prestigious ICSE conference (IEEE/ACM International Conference on Software Engineering), the premier venue for software engineering research held in Lis-bon, three outstanding papers were presented, showcasing cutting-edge contributions to software engineering research. The research presents novel approaches for plagiarism detection in software development and education. A language-independent method effectively prevents automated obfuscation attacks by plagiarism generators while maintaining a low false positive rate. Another approach combines automated analysis with human inspection to detect plagiarism in model-based artefacts such as diagrams, even when obfuscated using AI tools like ChatGPT. Both methods demonstrate significantly higher detection rates and resilience against automated attacks compared to the state of the art.

T. Sağlam, M. Brödel, L. Schmid & **S. Hahner** (2024): Detecting Automatic Software Plagiarism via Token Sequence Normalization. – 2024 IEEE/ACM 46th International Conference on Software Engineering (ICSE), 1384–1396.

J. Keim, S. Corallo, D. Fuchß, T. Hey, T. Telge & **A. Koziolek** (2024): Recovering Trace Links between Software Documentation and Code. – 2024 IEEE/ACM 46th International Conference on Software Engineering (ICSE), 2655–2667.

T. Sağlam, L. Schmid, **S. Hahner** & **E. Burger** (2024): Automated Detection of AI-Obfuscated Plagiarism in Modeling Assignments. – ICSE-SEET '24: Proceedings of the 46th International Conference on Software Engineering: Software Engineering Education and Training, 297–308.

2025

DUMPLING: Fine-Grained Differential JavaScript Engine Fuzzing

DISTINGUISHED PAPER AWARD

Diverging assumptions of the optimization steps employed by JavaScript engines in modern Web browsers may lead to severe vulnerabilities and arbitrary code execution in the worst case. Differential fuzzing can compare interpreted code against optimized code to detect differences in execution. Recent approaches to doing so instrument the JavaScript code, which allows for rather coarse-grained comparison only. Our approach, in turn, instruments the JavaScript engine (responsible for optimization and execution), enabling deep and precise introspection. We found eight new vulnerabilities in the Google V8 JavaScript engine and collected $11,000 from Google's Vulnerability Rewards Program for reporting the vulnerabilities. Additionally, our paper has won the Distinguished Paper Award at the 32nd Network and Distributed System Security (NDSS) Symposium.

L. Wachter, J. Gremminger, **C. Wressnegger,** M. Payer & F. Toffalini (2025): DUMPLING: Fine-Grained Differential JavaScript Engine Fuzzing. - Network and Distributed System Security (NDSS) Symposium 2025: 17 pp.

Topic ESS' Demonstrators Ready for Use

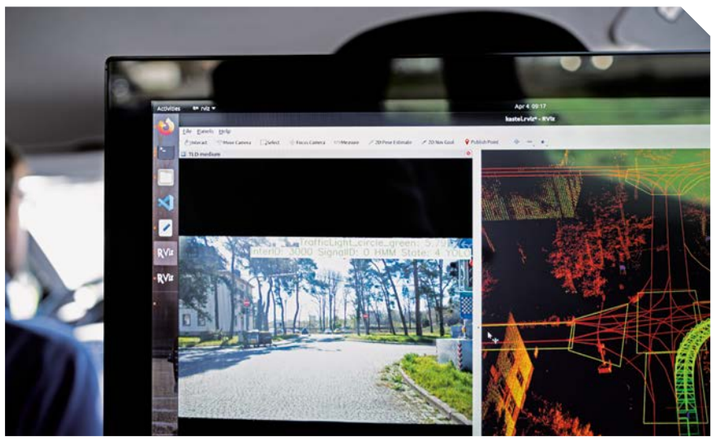
One of the major goals planned for 2024 has been achieved: demonstrators to present efficient, secure multi-party computing, and secure and reliable critical infrastructures (energy, mobility, and production) have been developed and are ready for testing and optimization. These demonstrators will be presented to represent a wide range of specific facets of the development. Currently, these could be provided in an overall view of the Topic ESS and visualize the key aspects of the research.

Based on the progress made, it is anticipated that a quantitative risk analysis for the demonstrators will be prepared by 2027/end of PoF IV as planned.

Impressions IV

Privacy Risks of Smart City Sensors: Security Lab Mobility in collaboration with the Research Group HSF.

Risk-based Authentication for Virtual Reality Using Brainwave Biometrics: Matin Fallahi, Philipp Matheis (Research Group HSF and Security Lab Production).



Attacks on Traffic Light Recognition and Countermeasures: Security Lab Mobility.

Awards 2021–2025

Our success is also reflected in the awards that members of Topic ESS have received for their contributions at international conferences and for the transfer of research results. In this compilation, we list prestigious awards for excellent publications as well as prizes of national or international importance in the period since 2021.

2021

- **"10-year Most Influential Paper Award"**, 18th IEEE International Conference on Software Architecture (ICSA 2021), March 22–26, 2021, Stuttgart. – CORE A conference.
  A. Koziolek, H. Koziolek & R. Reussner (2011): PerOpteryx: Automated Application of Tactics in Multi-Objective Software Architecture Optimization. – Joint Proceedings, 7th International ACM SIGSOFT Conference on the Quality of Software Architectures and 2nd ACM SIGSOFT International Symposium on Architecting Critical Systems (QoSA-ISARCS 2011): 33–42.

- **"10-year Most Influential Paper Award"**, 12th ACM/SPEC International Conference on Performance Engineering (ICPE 2021), April 19–23, 2021, Rennes, France. – CORE B conference.
  C. Trubiani & A. Koziolek (2011): Detection and Solution of Software Performance Antipatterns in Palladio Architectural Models. – ICPE '11: Proceedings of the 2nd ACM/SPEC International Conference on Performance Engineering: 19–30.

- **"Best Paper Award (runner-up)"**, 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, CVPR), June 19–25, 2021, online. – CORE A* conference.
  M.-R. Vemparala, N. Fasfous, A. Frickenstein, S. Sarkar, Q. Zhao, S. Kuhn, L. Frickenstein, A. Singh, C. Unger, N. S. Nagaraja, C. Wressnegger & W. Stechele (2021): Adversarial Robust Model Compression using In-Train Pruning. – Proceedings of the 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW): 66–75.

- **"Best Paper Award"**, NetSys 2021, September 13–16, 2021, Lübeck.
  P. Walther, M. Richter & T. Strufe (2021): Ray-tracing based Inference Attacks on Physical Layer Security. – Electronic Communications of the EASST, 80: 4 pp.

2022

- **"Digital Autonomy Award"**, "Digital Autonomy Hub": Privacy Friendly Apps, March 28, 2022: Research Group SECUSO.

- **"Best Paper Award (runner-up)"**, ACM Web Conference 2022, April 25–29, 2022, online. – CORE A* conference.
  N. Demir, M. Große-Kampmann, T. Urban, C. Wressnegger, T. Holz & N. Pohlmann (2022): Reproducibility and Replicability of Web Measurement Studies. – Proceedings, ACM Web Conference 2022 (WWW '22): 533–544.

- **"Alexander von Humboldt Professorship for Artificial Intelligence 2023"**, Alexander von Humboldt Foundation, June 2022: André Platzer.

- **"Best Paper Award"**, 2022 IEEE 13th International Symposium on Power Electronics for Distributed Generation Systems (PEDG), June 26–29, 2022, Kiel.
  D. Schulz, K. Schneider, M. Weßbecher, V. Hagenmeyer, M. Zitterbart & M. Hiller (2022): Hardware Realization of Participants in an Energy Packet-based Power Grid. – 2022 IEEE 13th International Symposium on Power Electronics for Distributed Generation Systems (PEDG): 1–6.

- **"Distinguished Paper Award"**, USENIX Security Symposium 2022, August 10–12, 2022, Boston, Massachusetts, USA. – CORE A* conference.
  *D. Arp, E. Quiring, F. Pendlebury, A. Warnecke, F. Pierazzi, **C. Wressnegger**, L. Cavallaro & K. Rieck (2022): Dos and Don'ts of Machine Learning in Computer Security. – Proceedings of the 31st USENIX Security Symposium (USENIX Security 22): 3971–3988.*

- **"Most Influential Paper Award"**, 26th ACM International Systems and Software Product Line Conference (SPLC 2022), September 12–16, 2022, Graz, Austria. – CORE B conference.
  ***I. Schaefer**, L. Bettini, V. Bono, F. Damiani & N. Tanzarella (2010): Delta-oriented Programming of Software Product Lines. – In: J. Bosch & J. Lee (eds.): Software Product Lines: Going Beyond. – SPLC 2010. Lecture Notes in Computer Science, vol. 6287: 77–91.*

2023

- **"Most Influential Paper Award"**, 7th International Conference on the Art, Science, and Engineering of Programming (<Programming> 2023), March 13–17, 2023, Tokyo, Japan.
  *S. Schulze, O. Richers & **I. Schaefer** (2013): Refactoring Delta-oriented Software Product Lines. – AOSD '13: Proceedings of the 2013 ACM on Aspect-Oriented Software Development: 73–84.*

- **"EDPL Young Scholar Award"**, European Data Protection Law Review, 16th International Conference Computers, Privacy & Data Protection (CPDP 2023), May 24–26, 2023, Brussels, Belgium: Mona Winau.

- **"Best Reviewer Award"**, 14th ACM International Conference on Future Energy Systems (ACM e Energy 2023), June 20–23, 2023, Orlando, Florida, USA: Veit Hagenmeyer.

- ***"Fellowship für Lehrinnovationen und Unterstützungsangebote in der digitalen Hochschullehre Baden-Württemberg 2023"*** (Fellowship for teaching innovations and support services in digital university teaching), Ministry of Science, Research and Arts Baden-Württemberg; Stifterverband für die Deutsche Wissenschaft e.V., July 2023: Anne Koziolek.

- **"Best Reviewer Award"**, 16th European Conference on Software Architecture (ECSA 2022), 16th European Conference on Software Architecture (ECSA 2022), September 19-23, 2022, Prague, Czech Republic: Anne Koziolek. – CORE A conference.

- **"Federal Consumer Protection Award"**, German Foundation for Consumer Protection (DSV): Research Group SECUSO.

- **"Notable Reviewer Award"**, IEEE Conference on Secure and Trustworthy Machine Learning (SaTML 2023), February 8–10, 2023, Raleigh, North Carolina, USA: Christian Wressnegger.

- **"Best Paper Award"**, 19th European Conference on Modelling Foundations and Applications (ECMFA 2023), July 20–21, 2023, Leicester, UK. – CORE B conference.
  *J.W. Wittler, **T. Saglam** & T. Kühn (2023): Evaluating Model Differencing for the Consistency Preservation of State-based Views. – The Journal of Object Technology, 22 (2): 1–14.*

- **"Poster Award"**, 19th Symposium on Usable Privacy and Security (SOUPS 2023), August 6–8, 2023, Anaheim, California, USA. – CORE B conference.
  ***A. Hennig**, L. Schmidt-Enke, M. Mutter & **P. Mayer** (2023): Beware of Website Hackers: Developing an Awareness Video to Warn for Website Hacking.*

- **"Distinguished Reviewer Award"**, 32nd USENIX Security Symposium (USENIX Security '23), August, 9–11, 2023, Anaheim, California, USA: Christian Wressnegger. – CORE A* conference.

- **"Best Paper Award"**, 14th International Conference on Network of the Future (NoF), October 4–6, 2023, Izmir, Turkey.
  ***S. Kopmann** & **M. Zitterbart** (2023): eMinD: Efficient and Micro-Flow Independent Detection of Distributed Network Attacks. – 2023 14th International Conference on Network of the Future (NoF): 159–167.*

- **"*Public Service Fellowship Preis*"**, Alfons und Gertrud Kassel-Stiftung, November 2023, Frankfurt/Main: Indra Spiecker gen. Döhmann.

- **"Best Presentation Award"**, 7th International Conference on System Reliability and Safety (ICSRS 2023), November 22–24, 2023, Bologna, Italy.
  ***M. Ramadan, G. Elbez** & **V. Hagenmeyer** (2023): Verifiable Certificateless Signcryption Scheme for Smart Grids. – 2023 7th International Conference on System Reliability and Safety (ICSRS): 181–189.*

- **"Top Reviewer Award"**, ACM Conference on Computer and Communications Security (CCS 2023), November 26–30, 2023, Austin, Texas, USA: Patricia Arias Cabarcos. – CORE A* conference.

- **"Top Reviewer Award"**, Annual Computer Security Applications Conference (ACSAC 2023), December 4–8, 2023, Austin, Texas, USA: Christian Wressnegger. – CORE A conference.

- **"YoungWomen4OR Award (YW4OR-2023)"**, WISDOM (Women in Society: Doing Operational Research and Management Science), December 2023: Emilia Grass.

2024

- **"Stefano Rodotà Data Protection Award 2024, Article Category"**, Council of Europe, Convention 108 on Data Protection.
  *L. Kyi, S. Ammanaghatta Shivakumar, C. Teixeira Santos, F. Roesner, **F. Zufall** & A.J. Biega (2023): Investigating Deceptive Design in GDPR's Legitimate Interest. – CHI '23: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, art. no. 583: 16 pp.*

- **"Distinguished Paper Award"**, Symposium on Usable Security and Privacy (USEC) 2024, February 26, 2024, San Diego, California, USA.
  *F. Sharevski, **M. Mossano**, M.F. Veit, G. Schiefer & **M. Volkamer** (2024): Exploring Phishing Threats through QR Codes in Naturalistic Settings. – Symposium on Usable Security and Privacy (USEC) 2024: 17 pp.*

- **"10-year Most Influential Paper Award"**, 15th ACM/SPEC International Conference on Performance Engineering (ICPE 2024), May 7–11, 2024, South Kensington, London, UK. – CORE B conference.
  *D. Perez-Palacin & **R. Mirandola** (2014): Uncertainties in the Modeling of Self-adaptive Systems: A Taxonomy and an Example of Availability Evaluation. – ICPE '14: Proceedings of the 5th ACM/SPEC International Conference on Performance Engineering: 3–14.*

- **"Best Paper Award"**, 2nd International Workshop on Re-design Industrial Control Systems with Security (RICSS), October 14, 2024, Salt Lake City, Utah, USA.
  ***A. Erba**, A.F. Murillo, R. Taormina, S. Galelli & N.O. Tippenhauer (2024): On Practical Realization of Evasion Attacks for Industrial Control Systems. – RICSS '24: Proceedings of the 2024 Workshop on Re-design Industrial Control Systems with Security: 9–25.*

2025

- **"Distinguished Paper Award"**, Network and Distributed System Security (NDSS) Symposium 2025, February 24–28, 2025, San Diego, California, USA. – CORE A* conference.
  *L. Wachter, J. Gremminger, **C. Wressnegger**, M. Payer & F. Toffalini (2025): DUMPLING: Fine-Grained Differential JavaScript Engine Fuzzing. – Network and Distributed System Security (NDSS) Symposium 2025: 17 pp.*

Young Talents

Promising scientific careers have already begun in the Topic ESS or will continue in this productive research environment. We have highlighted some impressive examples in this section. Moreover, four postdocs and doctoral students are introduced here, who will present their outstanding research results as part of the Helmholtz Association's scientific evaluation.

Prof. Dr. Patricia Arias Cabarcos

Patricia obtained her PhD in Telematic Engineering from the University Carlos III in Madrid in 2013 and stayed there as an assistant professor until 2018. By 2019, she was also a Humboldt Fellow at the University of Mannheim. After joining KASTEL, Patricia has been a **Topic ESS** PI and **professor at the University** of Paderborn since 2021, where she heads the **IT Security Group**.

Jun.-Prof. Dr. Emilia Grass

Emilia leads a **Helmholtz Young Investigator Group** "Building Network Resilience in Healthcare against Cyber-Attacks" as a **junior professor** in the Topic ESS. With a background in business administration and mathematics, she completed her PhD on numerical algorithms in disaster management at TU Hamburg in 2018. Before joining KIT, she was a postdoc at the University of Mannheim and Imperial College London, where she remains a guest lecturer.

Patricia Guerra-Balboa, M.Sc.

Patricia is a **PhD student** at the Chair for IT Security at KIT, with a background in mathematics. Her research focuses on privacy-preserving data analysis, particularly **Differential Privacy and location data**. Beyond conducting research, she enjoys communicating her work to both scientific and general audiences, which led her to the **FameLab Germany national finals**.

Dr.-Ing. Sebastian Hahner

Sebastian is a **postdoctoral researcher** at the Topic ESS, where he finished his dissertation at the chair of Prof. Reussner in 2024. His research is centered around **data flow analysis**, **confidentiality**, and **uncertainty of cyber-physical systems**. He has over a decade of experience in video production and has one of Germany's largest social media presences in tech education and science communication.

Prof. Dr. Robert Heinrich

Robert received a doctoral degree from Heidelberg University and a habilitation from Karlsruhe Institute of Technology (KIT). He leads the **Quality-driven System Evolution research group** at KIT. Robert accepted an offer of the **W3-professorship for Software Engineering at Ulm University** starting in April 2025.

Prof. Dr.-Ing. Peter Mayer

As a postdoc, Peter held the role of a coordinator of the "Human and Societal Factors" Research Group at the Topic ESS. Since 2023, he is an **assistant professor for usable security at the University of Southern Denmark**. Peter is still associated researcher at KIT contributing with his research as a **Topic ESS PI**.

Maximilian Noppel, M.Sc.

As a **doctoral researcher** within the Topic ESS, Maximilian investigates the **limitations of eXplainable Artificial Intelligence** (XAI) in adversarial environments. His works demonstrate how adversaries can manipulate predictions, explanations, or both in ML systems. With his background in algorithm engineering and cryptography, he aims to develop explanation methods with robustness guarantees.

Dr. Marcel Tiepelt

Marcel recently **completed his doctorate** at the Chair for **Cryptography and Security** at KIT. His research contributed to the **NIST post-quantum cryptography competition** and was applied with the German Aerospace Center to develop Europe's next civil aviation communication system. Previously, he worked in India, Japan, and other countries, bringing diverse international experience and collaborations to the Topic ESS.

Prof. Dr. Christian Wressnegger

After beginning his career in cybersecurity in industry, Christian "switched sides" to academia and leads the "**Artificial Intelligence & Security**" (IntelliSEC) group at KIT, specializing in artificial intelligence applications in cybersecurity. From 2020 to 2024, he was tenured professor at KIT, and in 2025, he became **full professor for IT security and is now co-spokesperson of the Topic ESS**.

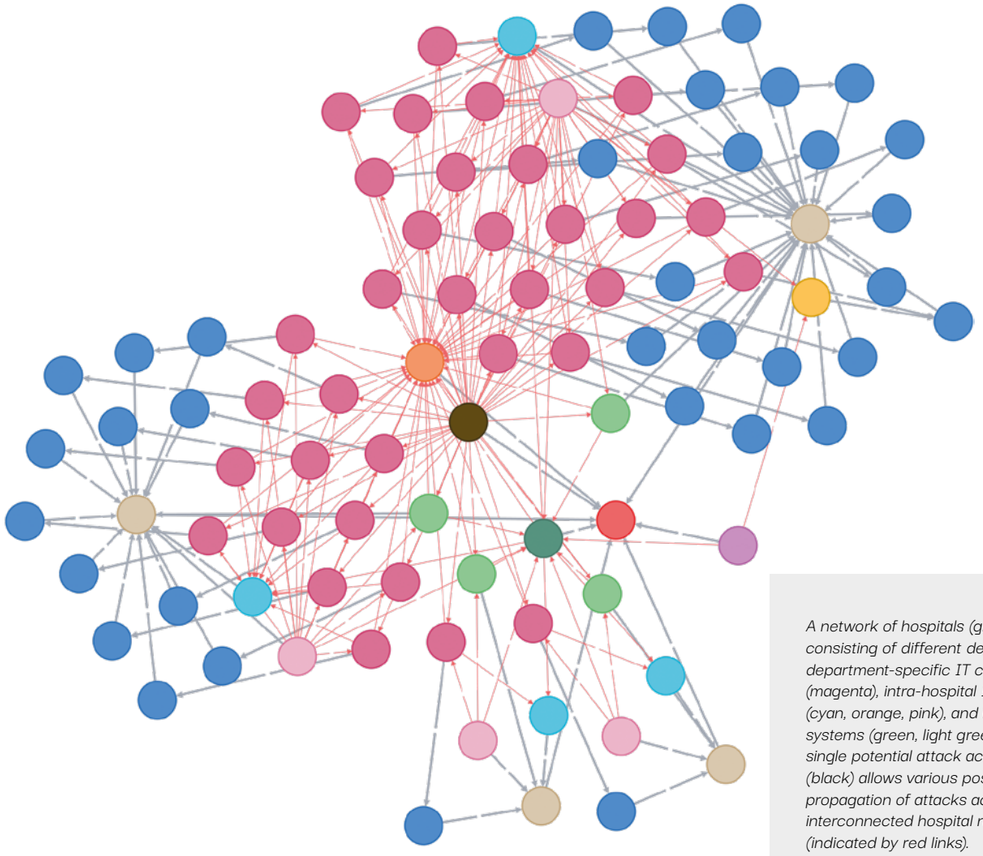
Building Network Resilience in Healthcare against Cyber-Attacks

OPERATIONS of Critical Infrastructures

Helmholtz Investigator Group

In recent years, the number and severity of cyber-attacks against healthcare providers and hospitals worldwide has increased significantly, resulting in blocked access to computer systems, electronic patient records, critical services, appointment cancellations, patient transfers, and closed emergency departments. In 2021, healthcare cyber-attacks worldwide averaged 109 incidents per organization each week, affecting approximately 45 million individuals and costing an average of $4.6 million per attack.

Notably, the first patient death directly attributed to a cyber-attack occurred when the University Hospital Düsseldorf in Germany had to close its emergency department. Furthermore, the Irish health system experienced a widespread ransomware attack that severely disrupted critical services includeing gynaecology, maternity clinics, cancer treatments, and children's care units. These disruptions highlight the acute vulnerability of healthcare systems to cybersecurity threats, especially given their reliance on interconnected digital technologies and increasingly complex information technology infrastructures.



A network of hospitals (grey nodes) consisting of different departments (blue), department-specific IT components (magenta), intra-hospital IT components (cyan, orange, pink), and inter-hospital IT systems (green, light green, red). Even a single potential attack access point (black) allows various possibilities for the propagation of attacks across the interconnected hospital network (indicated by red links).

Despite these life-threatening consequences, cybersecurity awareness in healthcare remains alarmingly low, and systematic research aimed at enhancing the resilience of interconnected hospital networks consisting of different departments and IT systems with potential attack access points and spread is virtually non-existent.

The unique and heterogeneous characteristics of healthcare IT infrastructures, including outdated software, chronic underinvestment in cybersecurity measures, and insufficient staffing of cybersecurity specialists, exacerbate this vulnerability. Additionally, the operational dependencies and intensive data sharing among different hospitals significantly amplify the risk of rapid and extensive propagation of cyber-attacks.

To address this critical gap, our project develops a comprehensive, interdisciplinary approach employing advanced simulation techniques, machine learning methods, and stochastic optimization models. Our objective is to quantitatively measure and analyze cyber risks, predict the propagation of attacks across interconnected hospital networks, and identify critical vulnerabilities within these systems. By modeling the potential cascading impacts of cyber-attacks, our research aims to propose and validate effective preparation and response strategies tailored specifically for healthcare settings. This approach includes identifying key hospitals whose cybersecurity failures could critically impact the entire network, thereby requiring prioritized attention and resources.

Ultimately, by enhancing the ability of healthcare networks to prepare for, respond to, and recover swiftly from cyber incidents, our project aims to significantly bolster patient safety and ensure continuity of critical healthcare services, even under adverse cyber conditions.

References

E. Grass, C. Pagel, S. Crowe & S. Ghafur (2024): A Stochastic Optimisation Model to Support Cybersecurity within the UK National Health Service. – Journal of the Operational Research Society, 1–12.

A. Angler, S. Fleßa, **E. Grass** & O. Goetz (2024): Assessing the Impact of Technology Partners on the Level of Cyberattack Damage in Hospitals. – Journal Health Policy and Technology, 14 (1), art. no. 100955, 16 pp.

N. O'Brien, **E. Grass**, G. Martin, M. Durkin, A. Darzi & S. Ghafur (2021): Developing a Globally Applicable Cybersecurity Framework for Healthcare: a Delphi Consensus Study. – BMJ Innovations, 7 (1): 199–207.

S. Ghafur, **E. Grass**, N. Jennings & A. Darzi (2019): The Challenges of Cybersecurity in Health Care: the UK National Health Service as a Case Study. – The Lancet Digital Health 1 (1): 10–12.

N. O'Brien, G. Martin, **E. Grass**, M. Durkin & S. Ghafur (2020a): Safeguarding our healthcare systems: A global framework for cybersecurity. – Doha, Qatar, World Innovation Summit for Health. https://2020.wish.org.qa/app/uploads/2020/09/WISH-2020_Forum-Reports_Cyber-Security-and-Healthcare-Systems_ENG.pdf

N. O'Brien, G. Martin, **E. Grass**, M. Durkin, A. Darzi & S. Ghafur (2020b): Cybersecurity in Healthcare: Comparing Cybersecurity Maturity and Experiences Across Global Healthcare Organizations. – Preprint, SSRN 3688885.

S. Ghafur, F. Gianluca, G. Martin, **E. Grass**, J. Goodman & A. Darzi (2019): Improving Cyber Security in the NHS. – Imperial College London, White Paper. https://www.imperial.ac.uk/media/imperial-college/institute-of-global-health-innovation/Cyber-report-2020.pdf.

KIT Graduate School Cyber Security

The KIT Graduate School Cyber Security is the central hub of doctoral researchers working across different cybersecurity disciplines within and beyond the Helmholtz Topic ESS. As such, we actively facilitate the exchange of ideas among doctoral research but foster connections to postdoctoral and senior researchers.

We organize regular community and networking events

KASTEL Distinguished Lecture Series

(see next page) and our monthly

Security & Privacy Lunch.

Additionally, we collaborated on organizing the

MyPhD Workshop

bringing together researchers from 16 German universities and the

WinterHack 2024 Winter School.

Next a vibrant community, we aim to equip our currently 30 members with technical, scientific, and interdisciplinary skills, enabling them to respond effectively to present and future security challenges.

In cooperation with the Karlsruhe House of Young Scientists (KHYS) at KIT, we hence offer workshops on, for instance, interdisciplinary thinking and scientific presentations, and organize writing support measures and dedicate voice coaching to help doctoral research make a strong appearance.

KASTEL Distinguished Lecture Series in Cyber Security

The Topic ESS, the KASTEL Security Research Labs, and the KIT Graduate School Cyber Security jointly organize the "KASTEL Distinguished Lecture Series in Cyber Security". Several times a year, we invite outstanding national and international speakers who provide insight into their cutting-edge research.

The research issues covered in the presentaions are manifold, spanning the breadth of all disciplines and research domains involved in cybersecurity research at KIT. Additionally, the Lecture Series is designed to

- appeal to the interests of a diverse audience,
- advocate for interdisciplinary research, and
- strike a balance between academic and industry perspectives.

In the period from 2021 to 2025, we were able to recruit eight experienced scientists to speak on current research topics and thus give the topic scientists an insight into specific problem areas.

Presentations 2021–2025

- Johannes Buchmann (Technical University of Darmstadt, Computer Science):
  Sustainable Cybersecurity and Privacy.
- Christopher Kruegel (University of California, Santa Barbara, Computer Science Department):
  Finding Vulnerabilities in Embedded Software.
- Orla Lynskey (London School of Economics and Political Science):
  "Fake It 'Til You Make It?" The Legal Implications of Synthetic Data.
- Lorenzo Cavallaro (University College London, Department of Computer Science):
  Transcending Transcend: Revisiting Malware Classification in the Presence of Concept Drift.
- Angela Sasse (Ruhr-University Bochum, Human-Centred Security):
  Behavioural Science Meets Security: Why a Little Knowledge is a Dangerous Thing.
- Martin Kleppmann (Technical University of Munich, Chair for Decentralized Systems Engineering):
  Byzantine Fault Tolerance for Peer-to-Peer Collaboration Software.
- Dennis Hofheinz (ETH Zurich, Department of Computer Science):
  A Personal Perspective on Cryptography.
- Andreas Zeller (CISPA Helmholtz Center for Information Security and Saarland University, Saarbrücken):
  Personalized Fuzzing.

Scientific Impact

Our Scientific Publications

Publications of Topic ESS	2021	*2022*	*2023*	2024
Total number of publications*	106	123	147	161
Number of peer-reviewed publications	92	118	135	136
· thereof WoS-/Scopus-indexed publications	69	92	104	104
· thereof A*/A-ranked publications (CORE)	17	27	33	39
· thereof A*-ranked publications (CORE)	7	7	11	9
· thereof other peer-reviewed publications**	23	26	31	32
Number of scientists (FTE)	48,8	51,6	55,7	78,4

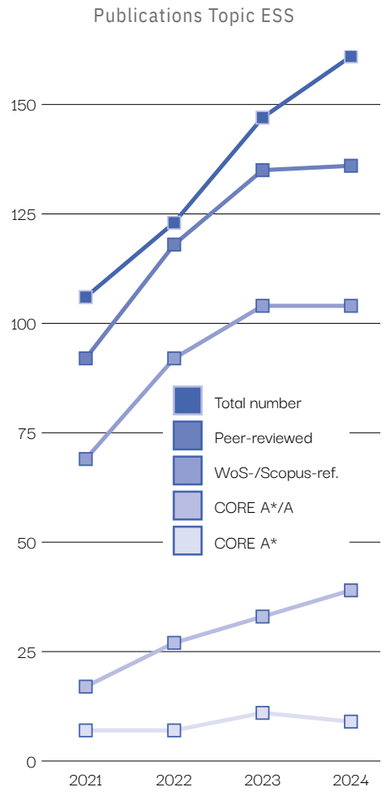
Publications and Performance

We have compiled the total number and the number of peer-reviewed publications published in the scope of the Topic ESS for the period from 2021 (start of PoF IV) to 2024. The number of publications for 2025 cannot yet be reliably determined.
According to the reporting criteria of the Helmholtz Association, publications referenced by Web of Science (WoS, Clarviate Analytics) and Scopus Source List (Scopus, Elsevier) are of particular interest.

Publications and Excellence

The number of top-rated publications can be used as an indicator of the scientific excellence of our research. For the field of computer science, the International CORE Conference Rankings (ICORE) with the A* and A-ranked publications are used. Accordingly, a complete list of our 34 A* publications that have emerged from Topic ESS research since 2021 is provided here.

* Proceedings and journal articles, book chapters, and books. Data as of April 2025.
** Publications with unique identifiers, e.g., doi or ISSN/ISBN.



CORE A* Publications 2021–2025

2021

- **P. Arias-Cabarcos**, T. Habrich, K. Becker, C. Becker & **T. Strufe** (2021): Inexpensive Brainwave Authentication: New Techniques and Insights on User Acceptance. – Proceedings of the 30th USENIX Security Symposium (USENIX Security 21): 55–72.
- F. Boenisch, R. Munz, **M. Tiepelt**, **S. Hanisch**, **C. Kuhn** & P. Francis (2021): Side-Channel Attacks on Query-based Data Anonymization. – CCS '21: Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security: 1254–1265.
- G. Couteau, **M. Klooß**, H. Lin & M. Reichle (2021): Efficient Range Proofs with Transparent Setup from Bounded Integer Commitments. – In: A. Canteaut & F.-X. Standaert (eds.): Advances in Cryptology – EUROCRYPT 2021. Lecture Notes in Computer Science, vol. 12698: 247–277.
- **R. Heinrich**, M. Strittmatter & **R.H. Reussner** (2021): A Layered Reference Architecture for Metamodels to Tailor Quality Modeling and Analysis. – IEEE Transactions on Software Engineering, 47 (4): 775–800.
- M. Maass, A. Stöver, H. Pridöhl, **S. Bretthauer**, D. Herrmann, M. Hollick & **I. Spiecker gen. Döhmann** (2021): Effective Notification Campaigns on the Web: A Matter of Trust, Framing, and Support. – Proceedings of the 30th USENIX Security Symposium (USENIX Security 21): 2489–2506.
- **P. Mayer**, Y. Zou, F. Schaub & A.J. Aviv (2021): "Now I'm a bit angry:" Individuals' Awareness, Perception, and Responses to Data Breaches that Affected Them. – Proceedings of the 30th USENIX Security Symposium (USENIX Security 21): 393–410.
- D. Monschein, M. Mazkatli, **R. Heinrich** & **A. Koziolek** (2021): Enabling Consistency between Software Artefacts for Software Adaption and Evolution. – 2021 IEEE 18th International Conference on Software Architecture (ICSA): 1–12.

2022

- D. Arp, E. Quiring, F. Pendlebury, A. Warnecke, F. Pierazzi, **C. Wressnegger**, L. Cavallaro & K. Rieck (2022): Dos and Don'ts of Machine Learning in Computer Security. – Proceedings of the 31st USENIX Security Symposium (USENIX Security 22): 3971–3988.
- G. Couteau, D. Goudarzi, **M. Klooß** & M. Reichle (2022): Sharp: Short Relaxed Range Proofs. – CCS '22: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security: 609–622.
- N. Demir, M. Große-Kampmann, T. Urban, **C. Wressnegger**, T. Holz & N. Pohlmann (2022): Reproducibility and Replicability of Web Measurement Studies. – WWW '22: Proceedings of the ACM Web Conference 2022: 533–544.
- **A. Hennig**, F. Neusser, A.A. Pawelek, D. Herrmann & **P. Mayer** (2022): Standing Out Among the Daily Spam: How to Catch Website Owners' Attention by Means of Vulnerability Notifications. – CHI EA '22: CHI Conference on Human Factors in Computing Systems Extended Abstracts, art. no. 317: 8 pp.
- **N. Kannengießer**, **S. Lins**, C. Sander, K. Winter, H. Frey & **A. Sunyaev** (2022): Challenges and Common Solutions in Smart Contract Development. – IEEE Transactions on Software Engineering, 48 (11): 4291–4318.
- **P. Mayer**, C.W. Munyendo, M.L. Mazurek & A.J. Aviv (2022): Why Users (Don't) Use Password Managers at a Large Educational Institution. – Proceedings of the 31st USENIX Security Symposium (USENIX Security 22): 1849–1866.
- **T. Runge**, M. Servetto, A. Potanin & **I. Schaefer** (2022): Immutability and Encapsulation for Sound OO Information Flow Control. – ACM Transactions on Programming Languages and Systems, 45 (1): art no. 3: 3-1–3-35.

2023

- D. Arp, E. Quiring, F. Pendlebury, A. Warnecke, F. Pierazzi, **C. Wressnegger**, L. Cavallaro & K. Rieck (2023): Lessons Learned on Machine Learning for Computer Security. – IEEE Security & Privacy, 21 (5): 72–77.
- T. Attema, S. Fehr & **M. Klooß** (2023): Fiat-Shamir Transformation of Multi-Round Interactive Proofs (Extended Version). – Journal of Cryptology, 36 (4), art. no. 36: 45 pp.
- C. Baum, L. Braun, C.D. De Saint Guilhem, **M. Klooß**, E. Orsini, L. Roy & P. Scholl (2023): Publicly Verifiable Zero-Knowledge and Post-Quantum Signatures from VOLE-in-the-Head. – In: H. Handschuh & A. Lysyanskaya (eds.): Advances in Cryptology – CRYPTO 2023. Lecture Notes in Computer Science, vol. 14085: 581–615.
- **M. Fallahi**, **T. Strufe** & **P. Arias-Cabarcos** (2023): BrainNet: Improving Brainwave-based Biometric Recognition with Siamese Networks. – 2023 IEEE International Conference on Pervasive Computing and Communications (PerCom): 53–60.
- **M. Fallahi**, **P. Arias-Cabarcos** & **T. Strufe** (2023): Poster: Towards Practical Brainwave-based User Authentication. – CCS '23: Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security: 3627–3629.
- **P. Mayer**, Y. Zou, B.M. Lowens, H.A. Dyer, K. Le, F. Schaub & A.J. Aviv (2023): Awareness, Intention, (In)Action: Individuals' Reactions to Data Breaches. – ACM Transactions on Computer-Human Interaction, 30 (5), art. no. 77: 1–53.
- C.W. Munyendo, **P. Mayer** & A.J. Aviv (2023): "I just stopped using one and started using the other": Motivations, Techniques, and Challenges When Switching Password Managers. – CCS '23: Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security: 3123–3137.
- **M. Noppel** & **C. Wressnegger** (2023): Poster: Fooling XAI with Explanation-aware Backdoors. – CCS '23: Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security: 3612–3614. doi: 10.1145/3576915.3624379.
- **M. Noppel**, L. Peter & **C. Wressnegger** (2023): Disguising Attacks with Explanation-aware Backdoors. – 2023 IEEE Symposium on Security and Privacy (SP): 664–681.
- A. Warneke, L. Pirch, **C. Wressnegger** & K. Rieck (2023): Machine Unlearning of Features and Labels. – Network and Distributed System Security (NDSS) Symposium 2023: 18 pp.
- Q. Zhao & **C. Wressnegger** (2023): Holistic Adversarially Robust Pruning. – Proceedings, 11th International Conference on Learning Representations (ICLR 2023): 22 pp.

2024

- N. Abou El Wafa & **A. Platzer** (2024): Complete Game Logic with Sabotage. – LICS '24: Proceedings of the 39th Annual ACM/IEEE Symposium on Logic in Computer Science, art. no. 1: 1–15.
- **B.M. Berens**, F. Schaub, **M. Mossano** & **M. Volkamer** (2024): Better Together: The Interplay Between a Phishing Awareness Video and a Link-centric Phishing Support Tool. – CHI '24: Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems, art. no. 826: 60 pp.
- N. Bindel, X. Bonnetain, **M. Tiepelt** & F. Virdia (2024): Quantum Lattice Enumeration in Limited Depth. – In: L. Reyzin & D. Stebila (eds.): Advances in Cryptology – CRYPTO 2024. Lecture Notes in Computer Science, vol. 14925: 72–106.
- T. Hiroka, F. Kitagawa, T. Morimae, R. Nishimaki, **T. Pal** & T. Yamakawa (2024): Certified Everlasting Secure Collusion-Resistant Functional Encryption, and More. – In: M. Joye & G. Leander (eds.): Advances in Cryptology – EUROCRYPT 2024. Lecture Notes in Computer Science, vol. 14653: 434–456.
- D. Jin, **N. Kannengießer**, R. Rank & **A. Sunyaev** (2024): Collaborative Distributed Machine Learning. – ACM Computing Surveys, 57 (4), art. no. 95: 1–36. doi: 10.1145/3704807.
- J. Keim, **S. Corallo**, D. Fuchß, T. Hey, T. Telge & **A. Koziolek** (2024): Recovering Trace Links Between Software Documentation and Code. – 2024 IEEE/ACM 46th International Conference on Software Engineering (ICSE): 2655–2667.
- **M. Noppel** & **C. Wressnegger** (2024): SoK: Explainable Machine Learning in Adversarial Environments. – 2024 IEEE Symposium on Security and Privacy (SP): 2441–2459.
- **T. Sağlam**, M. Brödel, L. Schmid & **S. Hahner** (2024): Detecting Automatic Software Plagiarism via Token Sequence Normalization. – 2024 IEEE/ACM 46th International Conference on Software Engineering (ICSE): 1384–1396.
- D. Schadt, **C. Coijanovic**, C. Weis & **T. Strufe** (2024): PolySphinx: Extending the Sphinx Mix Format with Better Multicast Support. – 2024 IEEE Symposium on Security and Privacy (SP): 4386–4404.
- Y. Zou, K. Le, **P. Mayer**, A. Acquisti, A.J. Aviv & F. Schaub (2024): Encouraging Users to Change Breached Passwords Using the Protection Motivation Theory. – ACM Transactions on Computer-Human Interaction, 31 (5), 1–45.

2025 (as of April 2025)

- D. Fuchß, T. Hey, **J. Keim**, H. Liu, N. Ewald, T. Thirolf & **A. Koziolek** (2025): LiSSA: Toward Generic Traceability Link Recovery through Retrieval-Augmented Generation. – IEEE/ACM 47th International Conference on Software Engineering (ICSE), 2025: 723–723.
- L. Wachter, J. Gremminger, **C. Wressnegger**, M. Payer & F. Toffalini (2025): DUMPLING: Fine-Grained Differential JavaScript Engine Fuzzing. – Network and Distributed System Security (NDSS) Symposium 2025: 17 pp.
- Q. Zhao & **C. Wressnegger** (2025): Two Sides of the Same Coin: Learning the Backdoor to Remove the Backdoor. – In: T. Walsh, J. Shah & Z. Kolter (eds.): 39th AAAI Conference on Artificial Intelligence, AAAI-25 Technical Tracks, 39 (21): 22804-22812.

Our Support for the Scientific Community – CORE A* Conferences 2021–2025

In this section, we focus on our commitment in the Scientific Community. We have been active-ly involved in many events since the Topic ESS was founded in 2021. The following compilation lists 14 outstanding conferences in the field of computer science and systems security (CORE A*) and the contributions of Topic ESS scientists to these events.

AAAI – Annual AAAI Conference on Artificial Intelligence

- 2024 – February 20–27, 2024, Vancouver, Canada: Member of Program Committee: Paul Samuel Teuber.

ASE – IEEE/ACM International Conference on Automated Software Engineering

- 2022 – October 10–14, 2022, Oakland, Michigan, USA: Member of Program Committee: Anne Koziolek.
- 2023 – September 11–15, 2023, Kirchberg, Luxembourg. Member of Program Committee: Anne Koziolek.

CHI – ACM CHI Conference on Human Factors in Computing Systems

- 2024 – May 11–16, 2024, Honolulu, Hawaii, USA: Associate chair of Subcommittee Privacy and Security: Melanie Volkamer.
- 2025 – April 26–May 1, 2025, Yokohama, Japan: Associate chairs of Subcommittee Privacy and Security: Benjamin Berens, Peter Mayer, Melanie Volkamer.

CCS – ACM Conference on Computer and Communications Security

- 2021 – November 15–19, 2021, online: Member of Program Committee: Patricia Arias Cabarcos.
- 2022 – November 7–11, 2022, Los Angeles, California, USA: Members of Program Committee: Andy Rupp, Thorsten Strufe.
- 2023 – November 26–30, 2023, Copenhagen, Denmark: Members of Program Committee: Patricia Arias Cabarcos, Andy Rupp, Thorsten Strufe, Christian Wressnegger.
- 2024 – October 14–18, 2024, Salt Lake City, Utah, USA: Members of Program Committee: Patricia Arias Cabarcos, Tapas Pal, Thorsten Strufe, Christian Wressnegger.
- 2025 – October 13–15, 2025, Taipei, Taiwan: Member of Program Committee: Patricia Arias Cabarcos, Thorsten Strufe.

EUROCRYPT – International Association for Cryptologic Research

- 2024 - May 26-30, 2024, Zurich, Switzerland: Member of Program Committee: Andy Rupp.
- 2025 - May 4-8, 2025, Madrid, Spain: Member of Program Committee: Michael Klooß.

ICSE – International Conference on Software Engineering

- 2021 - May 23-29, 2021, online: Member of Program Committee: Anne Koziolek.
- 2022 - May 22-27, 2022, Pittsburgh, Pennsylvania, USA: Member of Program Committee: Anne Koziolek.
- 2023 - May 14-20, 2023, Melbourne, Australia: Members of Track Committees: Anne Koziolek, Ina Schaefer.
- 2024 - May 14-20, 2023, Melbourne, Australia: Members of Track Committees: Anne Koziolek, Raffaela Mirandola.
- 2025 - April 27-May 3, 2025, Ottawa, Canada: Area Co-Chair for Dependability and Security: Raffaela Mirandola; Members of Track Committees: Christopher Gerking, Anne Koziolek, Raffaela Mirandola.

IEEE INFOCOM – IEEE International Conference on Computer Communications

- 2021 - May 10-13, 2021, online: Member of Technical Program Committee (Area Chair): Thorsten Strufe.
- 2022 - May 2-5, 2022, online: Member of Technical Program Committee (Area Chair): Thorsten Strufe.

LICS – Annual ACM/IEEE Symposium on Logic in Computer Science

- 2023 - June 26-29, 2023, Boston, USA: Member of Program Committee: André Platzer.
- 2025 - June 23-26, 2025, Singapore: Member of Program Committee: André Platzer.

NeurIPS – Annual Conference on Neural Information Processing Systems

- 2024 - December 10-15, 2024, Vancouver, Canada: Member of Program Committee: Samuel Teuber.

PerCom – IEEE International Conference on Pervasive Computing and Communications

- 2021 - March 22-26, 2021, Kassel: Member of Technical Program Committee: Patricia Arias-Cabarcos, Thorsten Strufe.
- 2022 - March 21-25, 2022, Atlanta, USA: Member of Technical Program Committee: Patricia Arias-Cabarcos.
- 2023 - March 13-17, 2023, Atlanta, USA: Member of Technical Program Committee: Patricia Arias-Cabarcos.
- 2024 - March 11-15, 2024, Biarritz, France: Member of Technical Program Committee: Thorsten Strufe.
- 2025 - March 17-21, 2025, Washington DC, USA: Member of Technical Program Committee: Thorsten Strufe.

PLDI – ACM SIGPLAN Conference on Programming Language Design and Implementation

- 2025 - June 16-20, 2025, Seoul, South Korea: Member of Review Committee: André Platzer.

S&P – IEEE Symposium on Security and Privacy

- 2021 - May 24-27, 2021, online: Member of Program Committee: Thorsten Strufe.
- 2022 - May 23-26, 2022, San Francisco, California, USA: Member of Program Committee: Christian Wressnegger.
- 2023 - May 22-25, 2023, San Francisco, California, USA: Member of Program Committee: Christian Wressnegger.
- 2024 - May 20-23, 2024, San Francisco, California, USA: Member of Program Committee: Christian Wressnegger.

TheWebConf (formerly WWW) – ACM Web Conference

- 2021 - April 12-23, 2021, online: Member of Program Committee: Christian Wressnegger.
- 2022 - April 25-29, 2022, online: Member of Program Committee: Christian Wressnegger.
- 2023 - April 30-May 4, 2023, Austin, Texas, USA: Member of the Board of Reviewers: Thorsten Strufe.
- 2024 - May 13-17, 2024, Singapore: Member of the Board of Reviewers: Thorsten Strufe.

USENIX Security – USENIX Security Symposium

- 2021 - August 11-13, 2021, online: Member of Program Committee, Member of Artifact Evaluation Committee: Christian Wressnegger.
- 2022 - August 10-12, 2022, Boston, Massachusetts, USA: Member of Program Committee: Christian Wressnegger.
- 2023 - August 9-11, 2023, Anaheim, CA, USA: Member of Program Committee, Member of Artifact Evaluation Committee: Christian Wressnegger.
- 2024 - August 14-16, 2024, Philadelphia, USA: Members of Program Committee: Patricia Arias Cabarcos, Christian Wressnegger, Member of Artifact Evaluation Committee: Yilin Ji.
- 2025 - August 13-15, 2025, Seattle, Washington, USA: Members of Program Committee: Patricia Arias Cabarcos, Alessandro Erba, Thorsten Strufe, Christian Wressnegger, Member of Artifact Evaluation Committee: Yilin Ji, Gustavo Sánchez.

Our Third-Party Funded Projects 2025

The Topic ESS benefits from KIT's traditional strength as a Technical University: with its expertise in the fields of computer science, energy, mobility, and production: The Topic combines interdisciplinary application-specific research with research into generic methods. This is also expressed in cooperation with research institutions on the one hand and commercial enterprises on the other in the form of funded projects. These enable specific issues and facets of IT security research to be investigated in a close exchange with the community. These projects are funded by public institutions such as the European Union, scientific communities, federal or state ministries, as well as foundations.

Funded by ...

... the European Union

- "CyberSec4Europe". European Framework on Cybersecurity Research.

... the Helmholtz Association

- "Building Network Resilience in Healthcare against Cyber-Attacks".
- "HIDSS4Health – Helmholtz Information & Data Science School for Health".
- "ROCK-IT (remote, operando controlled, knowledge-driven, IT-based)".

... the Leibniz Association

- "DiTraRe – Digital Transformation of Research". Leibniz ScienceCampus.

... the Federal Ministry for Education and Research, BMBF

- "ANYMOS – *Anonymisierung für vernetzte Mobilitätssysteme*" (Anonymization for Networked Mobility Systems).
- "DataChainSec – *Sicherheit für KI-Anwendungen in der Lebensmittelversorgung*" (Safety for AI Applications in Food Supply).
- "DIRECTIONS – *Datenschutzzertifizierung für Bildungsinformationssysteme*" (Data Protection Certification for Educational Information Systems).
- "HardShiP – *Langfristige IT-Sicherheit für die Hardware von Produktionsanlagen*" (Long-term IT Security for Production Plant Hardware).
- "KARL – *Künstliche Intelligenz für Arbeit und Lernen in der Region Karlsruhe*" (Artificial Intelligence for Work and Learning in the Karlsruhe Region). Competence cluster.
- "Open6GHub – 6G for Society and Sustainability".
- "Sec4IoMT – *Sicherheit im Internet der Dinge für medizinische Endgeräte*" (Security for the Internet of Medical Things).
- "SynthiClick – *Synthetische Datenerzeugung anhand von Nutzungsverhalten im World Wide Web*" (Synthetic Data Generation based on User Behavior in the World Wide Web).
- "VE ASCOT – *Neuartige sichere Elektronikkomponenten für die 'Chain of Trust'*" (Advanced Security for the Chain of Trust).

... the Federal Ministry for Digital and Transport, BMDV

- "C2CBridge – Country to City Bridge".

... the Federal Ministry of Health, BMG

- "CanConnect – *Zusammenführung von Krebsregisterdaten und multimodalen, melderbasierten Diagnostikdaten zur KI-basierten Biomarker-Detektion*" (Merging Cancer Registry Data and Multimodal, Reporter-based Diagnostic Data for AI-based Biomarker Detection).

... the Ministry of Science, Research and Arts Baden-Württemberg

- "bwNET2020+ – Research and innovative services for a flexible network in Baden-Württemberg".

... the Ministry for Economic Affairs, Labour and Tourism Baden-Württemberg

- "SMIGAA – *Smarter, intelligenter Gesundheitsassistent am Arbeitsplatz*" (Smart, Intelligent Health Assistant at the Workplace). Project funded by invest BW on behalf of the Ministry.

... the Ministry of Transport Baden-Württemberg

- "Digit4TAF-BW – AI in the Mobility Sector".

... the German Research Foundation, DFG

- "Change aPS – Static Analysis to Support Change Management in Variant-rich Legacy Control Software for Machine and Plant Engineering Companies".
- "Convide – Consistency in the View-Based Development of Cyber-Physical Systems" (SFB 1608). Collaborative Research Centre.
- "KeY – A Deductive Software Analysis Tool for the Research Community".
- "NFDIxCS – National Research Data Infrastructure for and with Computer Science". Consortium funded in cooperation with the German National Research Data Infrastructure (NFDI).

... the Carl Zeiss Stiftung

- "JuBot – Stay Young with Robots".

Our Cooperation Projects 2025

Another aspect of our scientific impact can be experienced by our projects. As cooperation projects, we refer to defined projects that our researchers realize in collaboration with universities and research institutes, commercial enterprises from industry and business. These are research projects that are pursued in addition to the externally funded projects. In order to provide an overview of current research activities, only the most important ongoing collaborations in 2025 are listed here.

... with Research Institutions & Organizations

- **"Assessing the Impact of Technology Partners on the Level of Cyberattack Damage in Hospitals"**. Cooperation with Detecon International GmbH, University of Greifswald, APOLLON University for Health Care Management.
- **"Auditable Security"**. Cooperation with University of the Bundeswehr Munich, University of Wuppertal.
- **"Building Healthcare Resilience Against Cyber-Attacks"**. Young Investgator Group with University of Mannheim, Imperial College London: Centre of Excellence for Active Security and Resilience.
- **"Cyber Threat Intelligence"**. Cooperation with Ben-Gurion University of the Negev.
- **"*Effektive Security Awareness am KIT*"**. Project with Technical University of Darmstadt.
- **"End-to-End Verifiable and Secret Online Elections at KIT"**. Project with Scientific Computing Center (SCC) at KIT, Karlsruhe.
- **"Everlasting Security for Quantum Cryptographic Protocols for Encrypted Computing"**. Cooperation project with CISPA Helmholtz Center for Information Security.
- **"MEDI:CUS"**. Platform headed by the Ministry of the Interior, Digitalisation and Local Government Baden-Württemberg.
- **"Optimizing Resource Planning in Surgery Wards Through Data-driven Resilience"**. Cooperation with Taipei Medical University-Shuang-Ho Hospital.
- **"Principles of Machine Learning in Computer Security"**. Cooperation with University College London, King's College London, Ruhr-Universität Bochum, Technical University of Berlin.
- **"Privacy in a Dictatorship"**. Cooperation with University of the Bundeswehr Munich.
- **"SECAIMED – Secure and Compliant AI for Medical Data"**. Cooperation with German Cancer Research Center.
- **"Test Area Autonomous Driving Baden-Württemberg"**. Consortium funded by the Ministry of Transport and Ministry of Science, Research and Arts Baden-Württemberg.

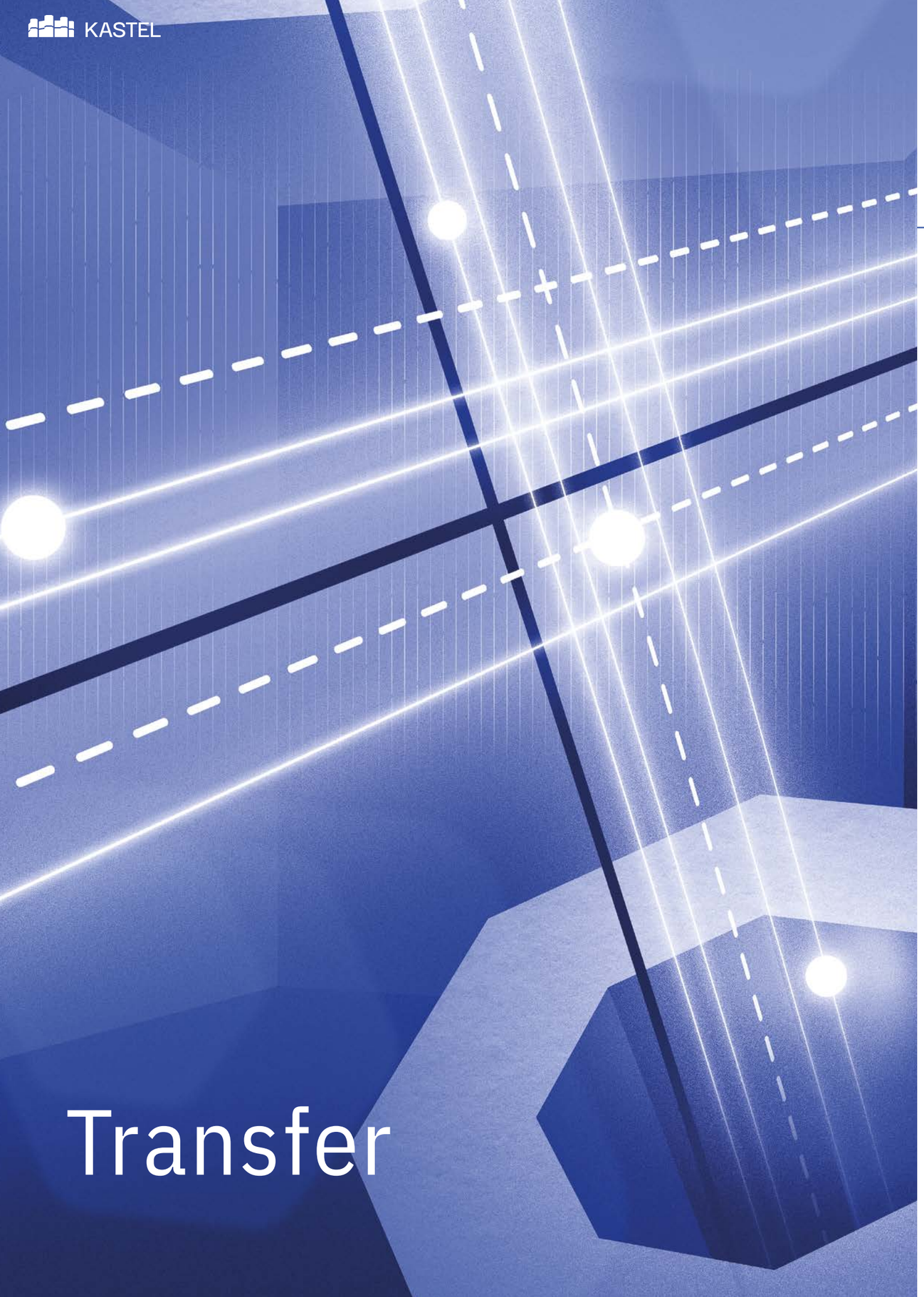
... with Business & Industry

- **"Automotive Security"**. Cooperation with ETAS GmbH.
- **"ChemCrypt" – Suitability of a specific approach for a physical Proof of Work.** Consulting, BASF SE.
- **"Design Methodologies for Cloud-native Systems in the Context of Industrial Automation"**. Project with ABB Asea Brown Boveri Ltd.
- **"Development of Platform for Smart Grid Cybersecurity R&D"**. Collaborative research project with Illinois Advanced Research Center at Singapore Ltd.
- **"EVerest"**. Cooperation with PIONIX GmbH.
- **"Group Verifiable Random Functions"**. Project with IBM Research Europe.
- **"Privacy-Preserving Bookkeeping and Analytics"**. Consulting, Init GmbH, Karlsruher Verkehrsverbund GmbH.
- **"Requirement-Engineering and Reality-Check of Architectures"**. Consulting, Karlsruher Verkehrsverbund GmbH.
- **"Quantum-Safe Encryption"**. Consulting, EnBW Energie Baden-Württemberg AG.
- **"Repliable Onion Routing"**. Project with NEC Laborates Europe.
- **"Security & Compliance Automation"**. Project with SAP SE.
- **"*Sichtenbasierte Entwicklung von Automotive Software*"** (View-based development of automotive software). Cooperation with Vector Informatik GmbH.
- **"VINCRYPTOR – Pseudonomization of Vehicle Identification Numbers"**. Contract by Mercedes-Benz AG.

The Topic ESS International Scientific Network

2025

89 National (German),
33 European,
23 International
institutions



Transfer

Transfer into Industry

Technology Transfer

As a Topic within the program-oriented funding of the Helmholtz Association, it is our concern and our mission to directly contribute to society with our research results, also by accelerating the transfer of research and application domains into specific applications and products in industry. This technology transfer can be impressively illustrated by the following examples.

"VINKRYPTOR"

In a cooperation, called "VINKRYPTOR", between KIT, FZI, and Mercedes-Benz, a method for the pseudonymization of Vehicle Identification Numbers (VINs) has been developed. The VIN is a unique identifier storing the data associated with the vehicle which should not be passed to third parties. This data protection problem is solved with the new development.

"IIP 2.0"

The projects "IIP 2.0" with S.A.F.E e.V. (Software Alliance for E-mobility) led to the successful certification resp. legal review of Topic-ESS-developed privacy-enhanced techniques and subsequent broad practical use and impact.

BSI-Demonstrators

Demonstrators of current research results have already been transferred and are in use by the Federal Office for Information Security (BSI).

"ISuTest"

The "ISuTest" automated vulnerability assessment framework for industrial automation components as well as "SMILE4VIP" (Smart eMaIl Link domain Extractor to support Visual Impaired People), were finalists for the NEO Innovation price awarded by the Karlsruhe TechnologyRegion in 2022. Ideas from a proof of concept for the topic became part of a demonstrator for the BSI.

"Privacy Friendly Apps"

Our societal impact is further attested by the Consumer Protection Award of the German Consumer Protection Organisation for our contributions to e-mail and password security, the Digital Autonomy Award 2022 of the Digital Autonomy Hub for "Privacy Friendly Apps" increasing individual digital sovereignty. Over 60 reference users and organizations refer to NoPhish anti-phishing materials, e.g., the Federal Chancellery, the Federal Office for Information Security (BSI), the Consumer Organisation NRW e.V., Ruhr University Bochum, and the Police Headquarters in Baden-Württemberg.

Training courses

The expertise built up in security of industrial automation is transferred into training courses for the Fraunhofer Cybersecurity Training Lab, the German Engineering Federation (VDMA), and the International Society of Automation (ISA Europe), in cooperation with the Federal Office for Information Security (BSI).

Security architecture of LDACS

In collaboration with the German Aerospace Center (DLR), we analyzed the security architecture of LDACS, Europe's next-generation civil aviation communication system. LDACS not only establishes a reliable data link between civilian aircraft and ground stations but also enables critical functionalities such as positioning and navigation. Our analysis reveals that the protocol achieves a mutually authenticated key exchange that is robust against even the threats posed by quantum computers. This milestone shows LDACS's readiness to meet the evolving security challenges of the aviation industry, ensuring secure and future-proof communication for decades to come.

Contribution to Standardization

Knowledge for Stakeholders

In this section, we present the commitment of our researchers through active participation in standardization committees and standardization working groups. This represents a direct transfer to society by incorporating instructions or recommendations for action into the further development of the state-of-the-art in science and technology. Eight of our PIs, postdocs, and researchers are currently active in nine national and international committees and boards.

National

- *VDI-Gesellschaft Energie und Umwelt* (VDI-Association for Energy and Environment): *Fachbereich Energie- und Umwelttechnik: Expertenrat im Richtlinienausschuss* (VDI-EE 4603 Part 3 – Project "*IT-Sicherheit und Informationssicherheit für Betriebsmanagementsysteme in der Energiewirtschaft*" (IT security and information security for operational management systems in the energy industry).
- Industrial Digital Twin Association e.V. (IDTA): IDTA Working Group Security, Standardization Asset Administration Shell (AAS) Security.
- Federal Office for Information Security (BSI): BSI-CC-PP-0121 Protection Profile for E-Voting Systems for Non-Political Elections: development of common criteria, and protection profile for online voting products.
- *Deutsche Kommission Elektrotechnik Elektronik Informationstechnik* (DKE, German Commission for Electrical, Electronic, and Information Technologies): DKE/AK 901.0.42 *KI in der Energietechnik* (AI in energy technology). DKE/AK 952.0.15 *DKE-ETG-ITG Informationssicherheit in der Netz- und Stationsleittechnik* (Information security in network and substation control technology).

International

- International Electrotechnical Commission (IEC): IEC/TC 57: Power systems management and associated information exchange – Data and communication security – standard series IEC 608705, IEC 60870-6, IEC 61850, IEC 61970, IEC 61968, and IEC 62351.

Europe

- European Committee on Democracy and Governance (CDDG): Guidelines on the use of information and communication technology (ICT) in electoral processes in Council of Europe member states.
- International Society of Automation (ISA Europe): ISA99 standards committee (ISA 99 Industrial Automation and Control Systems Security). Training courses for ISA/IEC 62443 series of standards.

USA

- National Institute for Standards and Technology (NIST), Gaithersburg, Maryland, USA: Project Post-Quantum Cryptography.
- OPC Foundation, Arizona, USA: OPC UA Working Group Secure Elements (SecElem), specification of OPC UA extensions for the use of hardware trust anchors.

Canada

- Digital Governance Standards Institute (DGSI), Canada: CAN/DGSI 111-1: Online Electoral Voting – Part 1: Implementation of Online Voting in Canadian Municipal Elections.

Activities in Advisory Boards

Knowledge for Decision Makers

Transfer of professional expertise and competence from science into practice is also achieved through the exchange of specific experiences. This includes in particular involvement in advisory boards of government institutions and in working groups and scientific platforms of research institutions and initiatives. With our commitment, we jointly contribute our knowledge to society. Members of the Topic ESS are currently active in the following committees (as of April 2025):

Expert groups of German Federal Ministries

- Scientific Working Group of the National Cybersecurity Council *(Wissenschaftliche Arbeitsgruppe Nationaler Cyber-Sicherheitsrat, Cyber-SR)*, headed by the Federal Ministry of the Interior and Community, BMI, and the Federal Ministry for Education and Research, BMBF. Member: Jörn Müller-Quade.
- Federal Ministry for Economic Affairs and Climate Action, BMWK: Expert group "Transformation of the Automotive Industry" *(Expertenkreis "Transformation der Automobilwirtschaft")*. Co-chair: Ina Schaefer.
- Federal Ministry for Economic Affairs and Climate Action, BMWK: "Initative IT Security in Enterprises" *(Initiative IT-Sicherheit in der Wirtschaft)*. Member of Steering Committee: Melanie Volkamer.

Scientific advisory boards

- *acatech* – National Academy of Science and Engineering:
  - Topic network Safety and Security. Speaker: Jörn Müller-Quade; Deputy Speaker: Jürgen Beyerer; Member: Indra Spiecker gen. Döhmann.
  - Topic network Healthcare Technologies. Member: Indra Spiecker gen. Döhmann.
- *acatech*, BMBF: *Lernende Systeme* – Germany's Platform for Artificial Intelligence (funded by the BMBF):
  - Working group "IT Security, Privacy, Legal and Ethical Framework", Section "IT-Security and Privacy". Working Group Management: Jörn Müller-Quade; Member: Bernhard Beckert.
  - Working group "Learning Robotic Systems". Working Group Management: Jürgen Beyerer.
  - Working group "Mobility and Intelligent Transport Systems". Member: J. Marius Zöllner.
- *acatech*, German National Academy of Sciences Leopoldina, and Union of the German Academies of Sciences and Humanities:
  - Initiative "Energy Systems of the Future" (funded by the BMBF). Member of the Board of Directors: Indra Spiecker gen. Döhmann.
  - Working Group "Energy prices and security of supply". Participant: Indra Spiecker gen. Döhmann.
  - Working Group "Centralised vs. Decentralised Power Supply". Participant: Veit Hagenmeyer.
- Électricité de France, Paris, France. Member of the Scientific Advisory Board: Veit Hagenmeyer.
- Fraunhofer Segment for Defense and Security VVS. Chairman: Jürgen Beyerer.
- German National Academy of Sciences Leopoldina: Focus group Digitisation. Member: Indra Spiecker gen. Döhmann.

- German Research Foundation (DFG):
  - Review Board "Computer Science", Subject area "Software Engineering and Programming Languages", Member: Ina Schaefer; Subject area "Data Management, Data-Intensive Systems, Computer Science Methods in Business Informatics", Member: Ali Sunyaev.
  - Commission for Pandemic Research. Scientific Member: Jörn Müller-Quade.
- HRK German Rectors' Conference, Standing Committee "Digitization". Member: Hannes Hartenstein.

Research organizations

- ATHENE National Research Center for Applied Cybersecurity, Darmstadt. Coordinator "Legal Aspects of Privacy and IT Security (LeAP)": Indra Spiecker gen. Döhmann.
- Center for Critical Computational Studies (C3S), Goethe University Frankfurt/Main. Managing Director: Indra Spiecker gen. Döhmann.
- EIFER – European Institute for Energy Research by EDF and KIT, Karlsruhe. Member of the Board of Directors: Veit Hagenmeyer.
- Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB, Karlsruhe. Head of Institute: Jürgen Beyerer; Members of the Advisory Board: Ralf Reussner, Indra Spiecker gen. Döhmann.
- FZI Research Center for Information Technology, Karlsruhe. Member of the Boards of Trustees: Jürgen Beyerer; Members of the Board of Scientific Directors: Bernhard Beckert, Jörn Müller-Quade, Oliver Raabe, Ralf Reussner, Ina Schaefer, J. Marius Zöllner. Research Division "Cybersecurity and Law": Jörn Müller-Quade (Spokesperson), Oliver Raabe (Co-Spokesperson), Ingmar Baumgart (Division Manager).
- ineges – Institute for European Health Care Policy, Frankfurt/Main. Associated Member: Indra Spiecker gen. Döhmann.
- Research Center for Data Protection, Goethe University Frankfurt/Main. Director: Indra Spiecker gen. Döhmann.

German Informatics Society (GI)

- Member of Steering Committee and of the Board of Directors: Ali Sunyaev.
- *Fachbereich "Sicherheit"* (security, special field of GI). Member of Steering Committee: Christian Wressnegger.
  - Special Interest Group "Formal Methods in Software Engineering, Safety and Security" (FoMSESS). Member of Steering Committee: Bernhard Beckert.
  - Special Interest Group "Security – Intrusion Detection and Response" (SIDAR). Member of Steering Committee: Christian Wressnegger.
- Fachbereich "*Wirtschaftsinformatik*" (information systems, special field of GI). Spokesperson: Ali Sunyaev.
- Special Interest Group "Communication and Distributed Systems" (KuVS), GI, Fachbereich "*Betriebssysteme, Kommunikationssysteme, Verteilte Systeme*" (SYS), and Informationstechnische Gesellschaft im VDE (ITG). Members of the Extended Steering Board: Thorsten Strufe, Martina Zitterbart.

Research initiatives

- "AIDOaRt – AI-augmented Automation for DevOps, a model-based framework for continuous development at RunTime in cyber-physical systems". EU-project, program Horizon Europe. Member of the Advisory Board: Raffaela Mirandola.
- e-mobil BW GmbH – State Agency for New Mobility Solutions and Automotive Baden-Württemberg. Member of the Board of Advisors: J. Marius Zöllner.
- Fraunhofer Strategic Research Field Artificial Intelligence. Spokesman: Jürgen Beyerer.
- "ENSURE". Kopernikus project, funded by the Federal Ministry for Education and Research, BMBF. Director: Veit Hagenmeyer.
- "MEDI:CUS" – Platform headed by the Ministry of the Interior, Digitalisation and Local Government Baden-Württemberg. Member of the Advisory Board: Emilia Grass.
- National Research Data Infrastructure for and with Computer Science (NFDIxCS) (consortium funded by German Research Foundation, DFG, in cooperation with German National Research Data Infrastructure, NFDI). Member of the Executive Board: Anne Koziolek.
- "RED ROSES – Responsive, Data ecosystem for Resilient and Operational Security Strategies". EU-project, program Horizon Europe. Member of the Advisory Board: Marcus Wiens.
- Schloss Dagstuhl, Leibniz Center for Informatics, Wadern. Member of the Supervisory Board: Hannes Hartenstein; Member of Scientific Directorate: Martina Zitterbart.
- Test Area Autonomous Driving Baden-Württemberg. Spokesperson: J. Marius Zöllner.

StartUpSecure KASTEL

An Incubator for Cybersecurity and Privacy

StartUpSecure KASTEL is the KIT incubator for start-ups in the field of IT security. The aim of the program is to provide continuous support for IT security start-up projects from all over Germany throughout their entire lifecycle. In particular, we focus on financial support, qualification measures, and raising awareness of cybersecurity issues in line with the needs of our network partners, potential pilot customers, and investors. In addition, we regularly organize events to strengthen the networking of our community and provide a stage for relevant topics and dedicated speakers. StartUpSecure KASTEL works closely with the KIT-Gründerschmiede, which bundles and supports all activities related to start-ups and spin-offs at KIT.

Supported by:

- Federal Minstry of Education and Research (BMBF)
- Topic ESS / KASTEL Security Research Labs (SRL)
- KIT-Gründerschmiede

Support for start-ups:

- Consulting for regional & national teams
- Continuing education & technology check: Topic Engineering Secure Systems (ESS) / KASTEL SRL
- Networking with industry, government & start-up ecosystem
- Community management & networking events

Overview

Financial support	Personnel costs, materials, equipment, coaching
Funding	Funding phase I: max. 800.000 €; Funding phase II: max. 800.000 €
Duration	12-15 months / phase
Target groups	Students, researchers, graduates, young start-ups (max. 2 years)

Supporting start-ups throughout their entire life cycle!

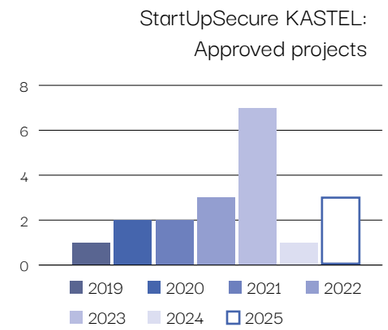
StartUpSecure KASTEL & Topic ESS

After a successful initial consultation, researchers and young, innovative startups prepare an abstract outlining their business idea, technology, and more. Experts from the Helmholtz Topic ESS and KASTEL SRL then assess its alignment with the IT security research program, level of innovation, and market potential, supported by the research coordination of the Topic ESS. If funding is recommended, the founding team receives guidance on funding opportunities and drafts a project outline, with StartUpSecure KASTEL providing active support. Following a successful evaluation, the project outline is submitted to the funding agency along with a positive statement.

Since the incubator's founding, KASTEL SRL has recommended 16 research projects, including three KIT spin-offs, with three more currently awaiting funding approval for launch in late 2025

Cooperation with the StartUpSecure network

StartUpSecure KASTEL is one of four incubators in Germany dedicated to cybersecurity and privacy. Together with ATHENE in Darmstadt, CISPA in Saarbrücken, and Cube 5 in Bochum, it organizes an annual accelerator program tailored to start-ups at different stages of development. This collaboration strengthens the cybersecurity ecosystem and provides start-ups with access to a strong network, offering valuable opportunities for growth and innovation.



Success stories from the community

- As a spin-off of KIT, *prenode* focuses on the transfer of research results to build decentralized and robust AI systems for industrial applications. With *prenode*'s solution, scalable machine learning models can be created and managed on distributed systems with full control over the data.
  Website: https://www.prenode.de/en

- *asvin* is standing for next level cybersecurity risk management to ensure security and protection for businesses and their valuable assets. At the forefront is their flagship product, Risk by Context, a game-changer in cybersecurity leveraging graph analytics and AI. Prioritizing threats with precision, it guarantees timely responses and maximizes efficiency, breaking down information silos for a comprehensive risk management strategy. Website: https://asvin.io/

- The KIT spin-off *Validaitor* is developing an all-in-one platform for the automated testing and validation of ML models, considering state-of-the-art AI safety techniques. They also enable compliance with the regulations of both the EU AI Act and ISO 42001. Website: https://validaitor.com/

StartUpSecure KASTEL: Procedural steps from application to funding.

Advancement

Impressions V

Secure Computations Using Not-so-Trusted Hardware: Research Group Q.

Raising Awareness for Fake Shop Based on Hacked or Misconfigured Servers: Anne Hennig (Research Group HSF).

Usable, Secure, and Legally Compliant Individual Verifiability in Internet Voting: Tobias Hilt (Research Group HSF).

Cross Cutting Issue

Quantifying Security

Given that cybersecurity, even when solely focusing on a technical perspective, has many facets, cyber-risk quantification necessarily is an interdisciplinary endeavor. In the Topic ESS, there is a dedicated interdisciplinary Research Group Quantifying Security with principal investigators from the domains of cryptography, IT security, privacy, formal methods, software engineering, business economics, as well as operations research. Within this Research Group, theoretical foundations of security quantification are researched, with the goal of researching an integrated methodology.

However, quantitative security in the Topic ESS has a much broader focus that goes beyond this single Research Group. As a cross-cutting issue across all Research Groups and Security Labs, quantification plays a role in many results and serves as a common language between different disciplines.

In the following, we will present several examples, highlighting the benefits of our interdisciplinary treatment of quantitative security applied in the Research Groups and Security Labs.

"[…] when you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meagre and unsatisfactory kind: it may be the beginning of knowledge, but you have scarcely, in your thoughts, advanced to the stage of science, whatever the matter may be."

Lord Kelvin (1824–1907)

W. Thomson [Lord Kelvin] (1889): Electrical Units of Measurements. – Popular Lectures and Addresses, Vol. I: 73–136, London, Macmillan and Co.

Research Group Human and Societal Factors

In the Research Group Human and Societal Factors, we measure to what extent the risk is reduced through awareness measures and/or tool support [1]. To this end, we measure, for example, the detection rate of phishing e-mails [2] or the remediation of vulnerabilities in web services. We are particularly interested in how the risk changes over time (months) after the awareness measure and when a new awareness measure is necessary in the form of a refresher [3] (see also: "NoPhish Concept and Awareness Measures", p. 28).

Research Group Secure Computation and Communication

To increase automation of risk assessment for Operation Technology (OT) systems, we develop risk quantification methods that do not rely on expert judgments. Using the established MITRE framework, our methods consider the system, possible attack techniques and countermeasures [4].

Besides prioritizing risks [5], the resulting quantifications are intended to judge the suitability of countermeasures for the specific system and its vulnerabilities. The evaluation of countermeasure selection is driven by maximizing the coverage of vulnerabilities under fixed budget constraints (see also: "Continuous Automated Risk Management (CARM) System for Industrial Networks", p. 29)

Security Lab Energy Systems

Quantification of attack impact is investigated in the Energy Lab. To this end, we simulate attacks on critical infrastructure in a realistic lab setup. This also helps to assess the resilience of systems under various attack scenarios that are specific to energy systems (e.g., SCADA systems, IEDs/RTUs devices). We also quantify the potential effects on substation operations and safety on the smart grid associated with GPS/GNSS spoofing and jamming attacks [6] (see also: "FENCE: Future ENergy Cybersecurity Evaluation", p. 29).

Security Lab Mobility Systems

Quantification through different security and privacy levels, resp. notions are also a common theme in the Topic ESS. In the Security Lab Mobility, a particular focus is secure software engineering, where different security levels are also considered, for example with security type systems using different security levels for secure information flow in object-oriented programs [7]. Quantitative security is also an aspect when deriving secure implementations from possibly different security levels of inputs and output of methods [8] (see also: "Design & Development Methods for Secure Automotive Software Systems", p. 31).

Security Lab Production Systems

We conducted two separate analyses of industrial components [9, 10] using automated testing tools, quantifying their vulnerability. These results serve also as a baseline for comparing future testing approaches and quantifying their performance with respect to identified vulnerabilities. We conducted automated tests as part of a test strategy specifically designed for industrial components, uncovering multiple types of vulnerabilities within them. Our experiments reveal findings for all considered OT components, which are quantified according to their severity including crashes, hangs, and information on outdated software (see also: "ISuTest", p. 63).

[1] **B.M. Berens**, F. Schaub, **M. Mossano** & **M. Volkamer** (2024): Better Together: The Interplay Between a Phishing Awareness Video and a Link-centric Phishing Support Tool. – CHI '24: Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems, art. no. 826: 60 pp.

[2] J. Petelka, **B. Berens**, C. Sugatan, **M. Volkamer** & F. Schaub (2025): Restricting the Link: Effects of Focused Attention and Time Delay on Phishing Warning Effectiveness. – 2025 IEEE Symposium on Security and Privacy (SP), 2025: 21 pp.

[3] **B.M. Berens**, **M. Mossano** & **M. Volkamer** (2024). Taking 5 Minutes Protects You for 5 Months: Evaluating an Anti-Phishing Awareness Video. – Computers & Security, 137, art. no. 103620: 1–19.

[4] **A. Meshram**, M. Karch, **C. Haas** & **J. Beyerer** (2023): Towards Self-Learning Industrial Process Behaviour from Payload Bytes for Anomaly Detection. – 2023 IEEE 28th International Conference on Emerging Technologies and Factory Automation (ETFA): 8 pp.

[5] **S. Canbolat**, **G. Elbez** & **V. Hagenmeyer** (2023): A New Hybrid Risk Assessment Process for Cyber Security Design of Smart Grids Using Fuzzy Analytic Hierarchy Processes. – at-Automatisierungstechnik, 71 (9): 779–788.

[6] **S. Canbolat**, **C. Fruböse**, **E. Elbez** & **V. Hagenmeyer** (2024): Extended Abstract: Assessing GNSS Vulnerabilities in Smart Grids. – In: F. Maggi, M. Egele, M. Payer & M. Carminati (eds.): Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2024. Lecture Notes in Computer Science, vol. 14828: 545–555.

[7] T. Runge, M. Servetto, A. Potanin & **I. Schaefer** (2023): Immutability and Encapsulation for Sound OO Information Flow Control. – ACM Transactions on Programming Languages and Systems, 45 (1): 3-1–3-35.

[8] T. Runge, **A. Kittelmann**, M. Servetto, A. Potanin & **I. Schaefer** (2022): Information Flow Control-by-Construction for an Object-oriented Language. – In: B.H. Schlingloff & M. Chai (eds.): Software Engineering and Formal Methods. SEFM 2022. Lecture Notes in Computer Science, vol. 13550: 209–226.

[9] **A. Borcherding**, P. Takacs & **J. Beyerer** (2022): Cluster Crash: Learning from Recent Vulnerabilities in Communication Stacks. – Proceedings of the 8th International Conference on Information Systems Security and Privacy (ICISSP 2022), 334–344.

[10] **A. Borcherding**, **M. Giraud** & **L. Tzigiannis** (2025): Show Me What You Got: Vulnerabilities of Industrial Components Revealed by Automated Black Box Testing. – 20th International Conference on Availability, Reliability and Security (ARES 2025), submitted.

Focus Issue

Securing Democracies

The world changed dramatically since we submitted the proposal for the Topic 'Engineering Secure Systems':

(1) Due to the COVID-19 pandemic, remote electronic voting became very popular. As a consequence, we decided to research on understanding and mitigating threats associated with remote electronic voting in order to protect our democracies.

(2) In particular, in the beginning of the Russian invasion, fake information became an emerging topic. Therefore, it was decided to conduct research on the understanding and mitigation of threats in the context of fake information.

(3) Cambridge Analytics demonstrated the power of political microtargeting related to election campaigns on social media platforms. Therefore, it was decided to research political microtargeting.

Remote electronic voting

In the context of remote electronic voting, the main activities were:

- Two interdisciplinary projects ("Trust Through Explainability in Verifiable Online Voting Systems" [1] in collaboration with the Topic Knowledge for Action and "End-to-End Verifiable and Secret Online Elections at KIT" [2]).
- General Chair of the international conference of E-VOTE-ID [3] with the Topic ESS being the main sponsor.
- One ongoing PhD project in the area of "Usable Secure End-to-End Verifiable Voting Systems" and one finished PhD project on "Formal Methods for Trustworthy Voting Systems: From Trusted Components to Reliable Software".
- Providing a verifier for the GI (German Informatics Society) elections since 2023 to enable voters to verify that their vote was cast as intended and stored as cast, as well as a verifier to enable everyone to check that all stored votes were properly tallied.
- Consultation for the study "E-Voting – Status Quo and Perspectives for Germany" [4] from the Office of Technology Assessment at the German Bundestag (TAB).
- Consultation for the study "A Study of Mechanisms for End-to-End Verifiable Online Voting" [5] from the German Federal Office for Information Security (BSI).
- Setting up a webpage summarizing the various competences in the area of electronic voting [6].

Fake information

In the context of fake information, the main activities were:

- A paper on "How to Protect the Public Opinion Against New Types of Bots?" [7] in which the authors developed and evaluated an algorithm to detect social bots more effective than existing approaches do.
- A joint project between the Topics ESS and Knowledge for Action called "Interdisciplinary Approaches to Deepfakes" [8].

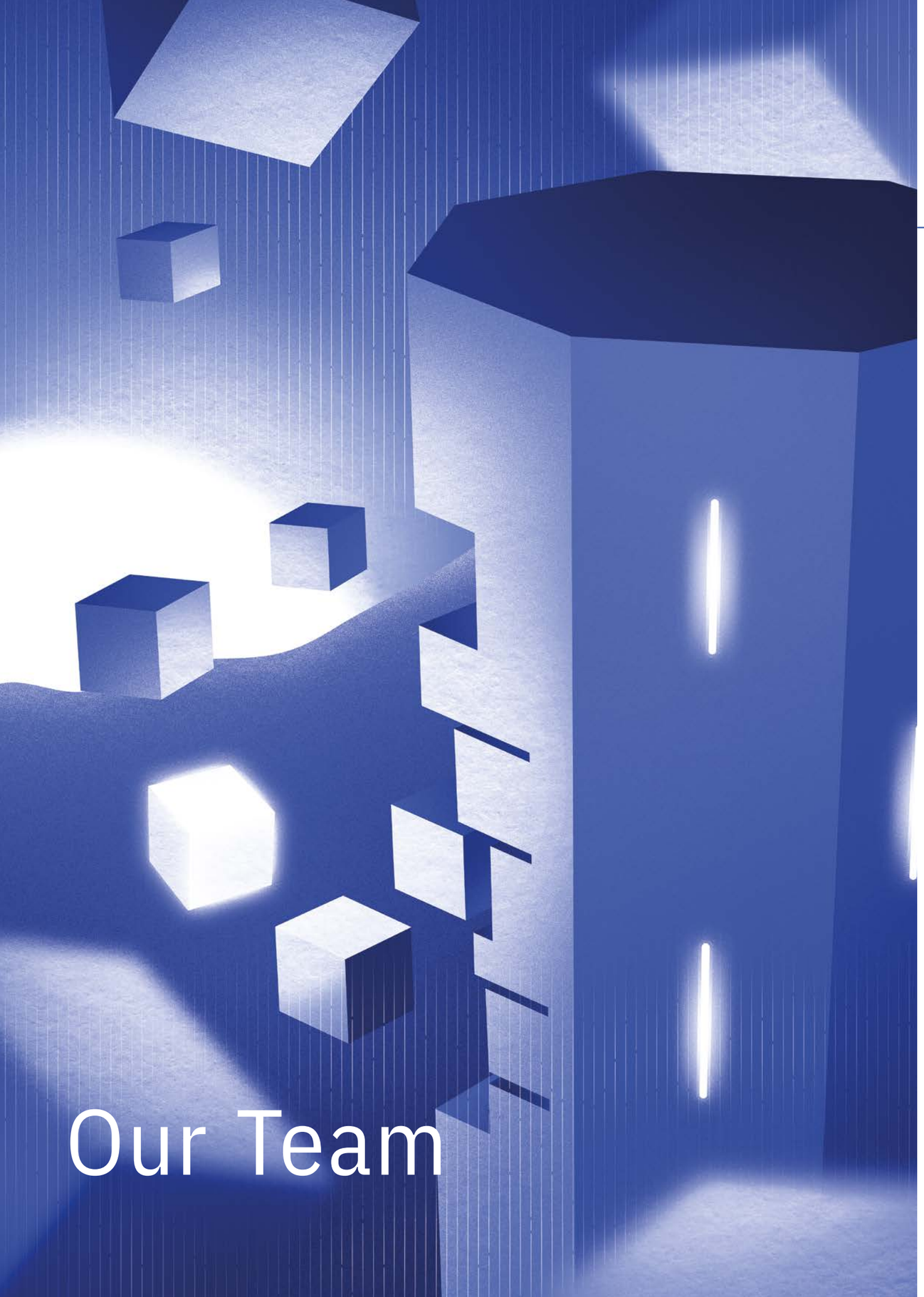
Political microtargeting

In the context of political microtargeting is a systematic legal analysis of the EU regulation on the transparency and targeting of political advertising from 2024 [9] available. This will be followed by an analysis from the voters' perspective focusing on their awareness.

Future democracies

Furthermore, several KIT-wide workshops titled "Future Democracies" [10] were organized to discuss the results and, more importantly to identify interdisciplinary research questions, e.g., in the context of liquid democracy as well as on trust and transparency in technology.

[1] Project "Trust Through Explainability in Verifiable Online Voting Systems". https://formal. kastel.kit.edu/projects/erklaerbareWahlsysteme/?lang=en.
[2] Project "End-to-End Verifiable and Secret Online Elections at KIT". https://formal.kastel.kit.edu/projects/e2eWahlenAmKIT/?lang=en.
[3] Tenth International Joint Conference on Electronic Voting, October 1-3, Nancy, France. https://www.e-vote-id.org/.
[4] Study "E-Voting – Status Quo and Perspectives for Germany", Office of Technology Assessment at the German Bundestag (TAB). https://www.tab-beim-bundestag.de/english/news-2023-09-e-voting-status-quo-and-future-prospects-for-germany.php.
[5] Project "A Study of Mechanisms for End-to-End Verifiable Online Voting". German Federal Office for In-formation Security (BSI). https://www.bsi.bund.de/EN/Service-Navi/Publikationen/Studien/Verifiable_Online-Voting/Verifiable_Online-Voting.html.
[6] Webpage "KIT E-Voting Kompetenzzentrum". https://evoting.kastel.secuso.org/.
[7] J.L. Reubold, S.C. Escher, C. Wressnegger & T. Strufe (2022): How to Protect the Public Opinion Against New Types of Bots? – 2022 IEEE International Conference on Big Data (Big Data): 1671-1680.
[8] Project "Interdisciplinary Approaches to Deepfakes". https://www.itas.kit.edu/english/projects_ jahn21_izdf.php.
[9] Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising. Official Journal of the European Union, L-Series. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202400900.
[10] Project "Future Democracies". https://secuso.aifb.kit.edu/english/2189.php.

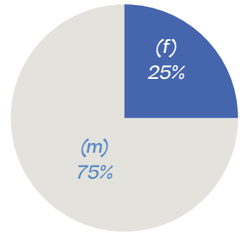


Our Team

Diversity 2025

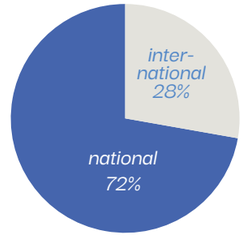
Gender Statistics

	Number of Individuals	(m)	(f)	Ratio of Female Individuals
Total number	114	86	28	24.6%
PIs	25	14	9	36.0%
Researchers	89	72	19	22.7%



Statistics on International Participation

	Number of Individuals	Number of Foreign Individuals	Ratio of Foreign Individuals
Total number	114	32	28.1%
PIs	25	3	12.0%
Researchers	89	29	32.6%



Represented Nations
Number of Individuals

6 India	5 China	3 Italy
3 Iran	3 Spain	2 Pakistan
1 Austria	1 Brazil	1 Denmark
1 Mozambique	1 Sudan	1 Tunesia
1 Turkey	1 Uruguay	1 Vietnam

(Data as of April 2025)

PI Contact

Prof. Dr. Patricia Arias Cabarcos
Research Group IT Security at University of Paderborn

PD Dr.-Ing. Ingmar Baumgart
Competence Center for IT Security at FZI Research Center for Information

Prof. Dr. Bernhard Beckert
Research Group Application-oriented Formal Verification at KIT

Prof. Dr.-Ing. habil. Jürgen Beyerer
Chair of the Vision and Fusion Lab at the Institute for Anthropomatics and Robotics (IAR) at KIT, Head of Fraunhofer IOSB

Jun.-Prof. Dr. Emilia Grass
Research Group Building Healthcare Resilience against Cyber-Attacks at KIT

Prof. Dr. Veit Hagenmeyer
Director of the Institute for Automation and Applied Informatics (IAI) at KIT

Prof. Dr. Hannes Hartenstein
Research Group Decentralized Systems and Network Services (DSN) at KIT

Prof. Dr.-Ing. Anne Koziolek
Research Group Modelling for Continuous Software Engineering (MCSE) at KIT

Prof. Dr.-Ing. Peter Mayer
Research Group Human and Societal Factors (HSF) at KIT and Research Group Artificial Intelligence, Cybersecurity and Programming Languages at University of Southern Denmark

Prof. Dr. Raffaela Mirandola
Research Group Self-Adaptive Software-Intensive Systems at KIT

Prof. Dr. Jörn Müller-Quade
Research Group Cryptography and Security at KIT

Prof. Dr. André Platzer
Research Group Logic of Autonomous Dynamic Systems at KIT

Prof. Dr. iur. Oliver Raabe
Research Group Legal Informatics and IT Security Law (ITR) at the Center for Applied Legal Studies (ZAR), KIT

Prof. Dr. Ralf Reussner
Research Group Dependability of Software-intensive Systems (DSiS) at KIT

Dr. Andy Rupp
Research Group Cryptographic Protocols at KIT and University of Luxemburg

Prof. Dr.-Ing. Ina Schaefer
Research Group Test, Validation and Analysis of Software-Intensive Systems (TVA) at KIT

Prof. Dr. Indra Spiecker gen. Döhmann
Chair for Law of Digitization at University of Cologne

Prof. Dr. Thorsten Strufe
Research Group Practical IT Security (PS) at KIT

Prof. Dr. Ali Sunyaev
Formerly Research Group Critical Information Infrastructures (cii) at KIT, now at TUM Campus Heilbronn

Prof. Dr. Melanie Volkamer
Research Group SECUSO (Security · Usability · Society) at KIT

Prof. Dr. Marcus Wiens
Chair of General Business Administration, in particular Innovation and Risk Management at TU Bergakademie Freiberg

Prof. Dr. Christian Wressnegger
Research Group Artificial Intelligence and Security (IntelliSec) at KIT

Prof. Dr. Martina Zitterbart
Research Group at Institute of Telematics (TM) at KIT

Prof. Dr. J. Marius Zöllner
Research Group Applied Technical Cognitive Systems at KIT

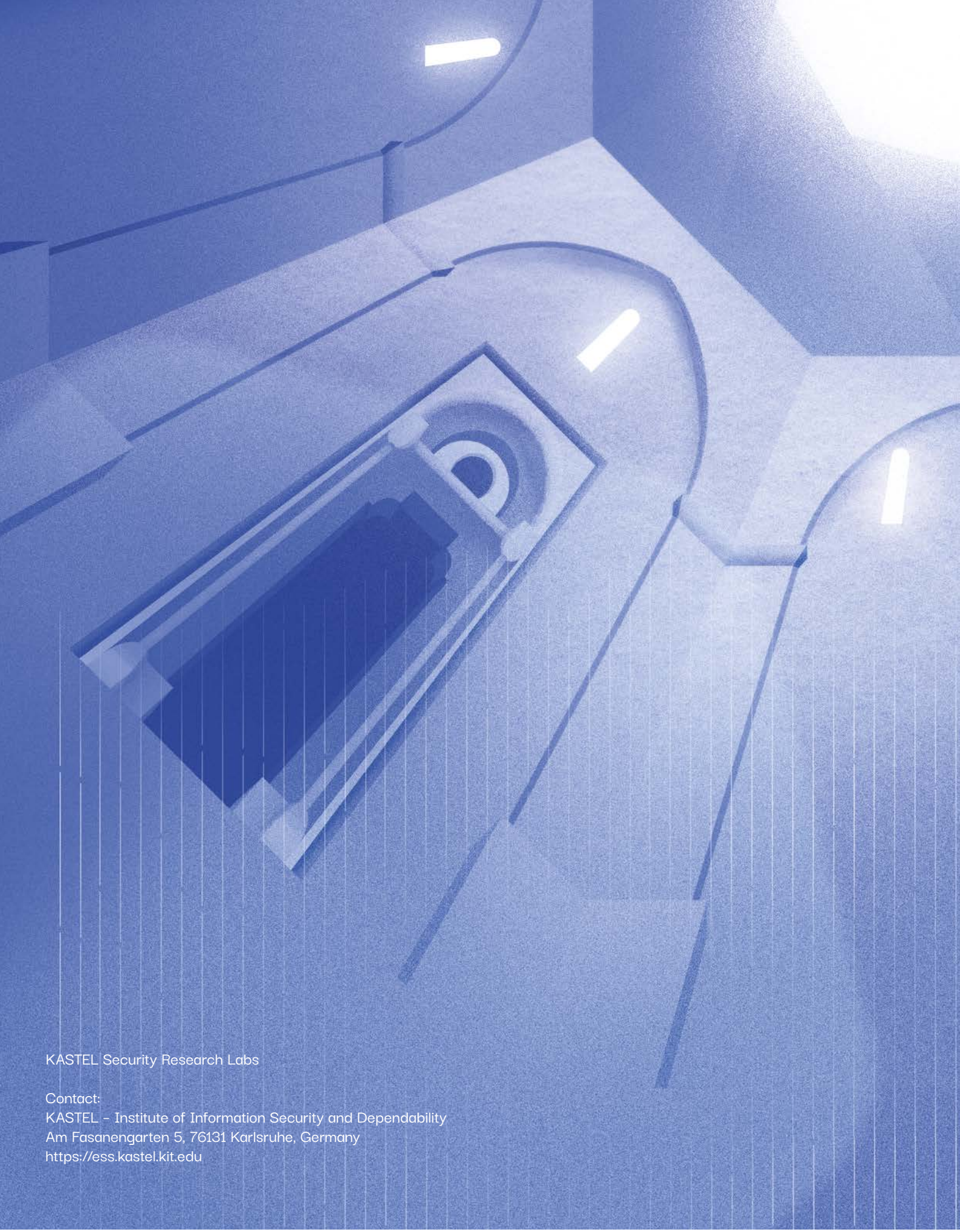
TT-Prof. Dr. Frederike Zufall
Chair for Public Law and Computer Science at the Center for Applied Legal Studies (ZAR), KIT

More About Topic ESS ...

... in our demonstrator videos

and on our Website

https://ess.kastel.kit.edu



KASTEL Security Research Labs

Contact:
KASTEL – Institute of Information Security and Dependability
Am Fasanengarten 5, 76131 Karlsruhe, Germany
https://ess.kastel.kit.edu

KASTEL

Focus on: Topic Engineering
Secure Systems ESS