

Annual Report 2022

—  
**Innovating with security**

# Annual Report 2022

---

**Fraunhofer Institute for Applied  
and Integrated Security AISEC**





Prof. Claudia Eckert,  
Managing director



Prof. Georg Sigl,  
Director

# Welcome to Fraunhofer AISEC!

Dear Reader,

When it came to cybersecurity, 2022 was anything but a good year. The war in Ukraine made us see the fragility of ideals that we had believed to be unshakable, namely peace in Europe. The suffering of those affected is immeasurable. Fraunhofer AISEC has declared its solidarity with Ukraine and condemned Russia's acts of aggression in the strongest terms. The incidence of large-scale, targeted cyberattacks has increased significantly since the war broke out. It was not for nothing that the German Federal Office for Information Security (BSI) described "the threat level in cyberspace [as] higher than ever" in its report on The State of IT Security in Germany in 2022, released in the latter half of the year. Ransomware attacks and IT supply chain disruptions in particular represent the greatest threats to social, state and industrial security. However, some rays of hope did break through the gloom in 2022: In September's European Cyber Resilience Act, the EU presented a long-awaited proposal for a law on cyber resilience.

In 2022, we at Fraunhofer AISEC continued our intensive work to stay one step ahead of the attacks, by systematically tackling future-oriented issues. For example, we have launched the Competence Center for Post-Quantum Cryptography, contributed to the 6G-ANNA lighthouse project with our cybersecurity expertise and worked with our partners to develop the Zentrum für vertrauenswürdige Künstliche Intelligenz (center for trusted artificial intelligence, ZVKI). In the area of secure digital identities, we are participating in all major national-level projects and playing an essential role in creating secure data spaces. In the Zentrum Trusted Electronic Bayern (Bavarian center for trusted electronics, TrEB) and the Bavarian Chip-Design-Center, we are driving research and development activities in secure, trusted, integrated electronic systems. What is more, we are also promoting international dialogue in the world of cybersecurity research, for example, through our collaborations with our new partner, Fraunhofer Singapore.

However, Fraunhofer AISEC is far more than just these activities: It has more than 220 highly qualified employees who work every day to analyze, shape and safeguard IT security through applied research. Our ability to methodically evaluate the security of solutions and designs or even architectures, to identify the risks associated with using them in a verifiable, tool-supported way and to develop suitable solutions proposals is in particularly high demand. We bring our knowledge into practice and to people in research projects with companies, public authorities and facilities and through the services we offer via the Cybersecurity Training Lab. Each and every one of us must live the reality of security culture if we are to overcome the digital threats we are facing. We hope that our Annual Report for 2022 will give you the inspiration you need to do this, along with useful information and interesting insights into our work.

Best regards,

Prof. Dr. Claudia Eckert

Prof. Dr. Georg Sigl

# Contents

<b>Welcome to Fraunhofer AISEC</b> .....	<b>5</b>
<b>Accurate cybersecurity assessments</b> .....	<b>8</b>
<b>Areas of expertise at Fraunhofer AISEC</b> .....	<b>12</b>
Industrial and automotive security   Secure in the knowledge .....	12
Digital sovereignty   Data sovereignty? No doubt! .....	16
Post-quantum cryptography   We have to reckon with all eventualities .....	20
Trusted electronics   The hardware hardeners .....	24
Cybersecurity Training Lab   Closing gaps in expertise .....	28
<b>In brief</b> .....	<b>32</b>
<b>About Fraunhofer AISEC</b> .....	<b>34</b>
Our mission .....	34
Facts and figures .....	35
The world of labs at Fraunhofer AISEC .....	36
Fraunhofer AISEC — a great place to work .....	38
Members of the advisory board .....	40
<b>Fraunhofer CCIT</b> .....	<b>42</b>
<b>A word from our customers</b> .....	<b>44</b>
Thomas Caspers (BSI) .....	44
Dirk Kretzschmar (TÜVIT) .....	45
<b>People of Fraunhofer AISEC</b> .....	<b>46</b>
Sandra Kostic .....	46
Michael Hehl .....	48
Vivija Čepkalo-Simić .....	50
Philip Sperl .....	52
<b>Looking to the future</b> .....	<b>54</b>
Quantum computing   It's time to take the leap .....	54
The future of telecommunications   Cybersecurity for 6G .....	56
<b>Publications</b> .....	<b>58</b>
<b>Editorial notes</b> .....	<b>62</b>



## Accurate cybersecurity assessments

The digital transformation is forging ahead and our world is becoming ever more connected. Ensuring cybersecurity is an ever more complex task. Accurate assessments are the only way to stay on top of this issue — and Fraunhofer AISEC has all the necessary expertise.

In the computers used today, it is typical for there to be shared memory for both program instructions and data. These computers do not differentiate between types of data, like numbers, values and code — such as commands. Even today, incorrectly coded programs, which do not check input or return values, for example, form the starting point for many successful attacks. As the input parameters are not monitored, attackers can use them to smuggle harmful executable code into the system instead of parameter values, i.e., data, and then run the code. “Depending on the type of program that is infiltrated and the harmful code that is used, cybercriminals can even access critical information,” explains Prof. Claudia Eckert, managing director of Fraunhofer AISEC.

### Always one step ahead

However, hackers are not content to focus on these simple attacks alone; instead, they constantly refine their techniques, combining them to form more complex attacks and frequently disguising their activities. “This is why we absolutely must constantly drive our analysis methods and security expertise to the highest possible level, so that we can stay that one decisive step ahead of the attackers,” says Prof. Eckert.

“It’s true that software is attacked far more often than hardware, but the consequences of hardware attacks are worse. Because hardware functions as a kind of anchor, it forms the basis for all software security functions,” points out Prof. Georg Sigl, director of Fraunhofer AISEC. “For example, there has yet to be any scientific evidence of trojans in hardware. However, the concept is not inconceivable and, provided the trojan remained undiscovered, it could have far-reaching consequences. Because IT infrastructures are built like onions: the hardware forms the core and the outer layers contain the operating system, the program libraries and finally, the applications.”

When it comes to attacks on hardware, the target is usually the secure element — a root of trust where cryptographically secure computations can be conducted and encryption information is stored. If the system has not been “hardened up,” then keys can be read via side-channel and error attacks. To do this, attackers analyze the physical effects of the hardware’s operation, e.g., the electromagnetic emissions or the way in which the hardware reacts when errors are fed in. This gives them insight into the cryptosystem’s weak points. Even the hardware interfaces (such as debuggers) that developers use for troubleshooting can serve as a gateway for cybercriminals.



Trusted electronics are a must for IT security. In Fraunhofer AISEC's hardware security lab, security researchers test electronic chips for their susceptibility to manipulation, e.g., via error attacks that use laser pulses.



### More digitalized, more connected, more complex

Due to increasing levels of digitalization and connection, IT systems can now be found in all important areas of modern economies. However, in many cases, progress has lagged when it comes to incorporating risk prevention measures to ensure the cybersecurity of this kind of open, connected system. Major security gaps often crop up in digital control components or sensors in devices used in both industry and everyday life. However, with the ongoing spread of the internet of things (IoT), the number of digital interfaces in operation even today far surpasses what can be monitored. Every single one of these interfaces represents a possible gateway for cybercriminals. "Systematic, automated analyses and hardening measures are indispensable tools for shutting these gateways for good," argues Prof. Eckert.

Attackers that acquire the necessary access credentials from employees using methods like phishing can then manipulate the system. If this method fails, e.g., because the employees have had the appropriate training, the criminals can try tackling the target system using freely available attack programs known as "exploits." "This is why it is important for every company to always install the latest security patches in order to put a stop to this kind of 'ready-made' attack," explains Prof. Eckert.

### Always able to assess

Preventing cyberattacks on vulnerabilities in IT systems is a complex problem. It can only be solved if you can assess how individual IT components influence the sequence of events, how they function and where their weak points lie. It is equally important to know what functions are essential to achieving the level of cybersecurity that is necessary from a company point of view, or formally required by legislation, or expected by society.

Fraunhofer AISEC supports companies, institutions and facilities in overcoming these challenges. Its staff of experts in applied cybersecurity research can assess what the

IT component in question consists of and its significance in the context of IT security. This requires an in-depth, systemic understanding of the way that hardware and software are structured, and of how they interact with each other. The Fraunhofer AISEC scientists can also gain a detailed understanding of the functionalities of individual components — both for chips and code. In many cases, this requires a combination of specialist knowledge about a certain domain, e.g., automotive or industry applications, and technical knowledge from the fields of computer science, electrical engineering, physics and mathematics.

It also explicitly calls for knowledge of the possibilities and limits of automated tools, as the ongoing increase in digitalization and connectedness represents a heightened security risk for automated elements. Finally, the Fraunhofer AISEC team also needs to be able to identify component functionalities that could contain malware such as trojans, for example, even though these functionalities may not be immediately apparent. "It is also very important to take other influencing factors apart from technology into account, e.g., supply chains or global developments in industry and politics. The individual countries' security legislation must also be considered during risk assessments, as the current geopolitical situation is unfortunately demonstrating in a dramatic way," Prof. Eckert explains.

Fraunhofer AISEC has developed a method for conducting risk analyses of connected IT systems that makes it possible to approach this multifaceted task in a holistic way: the Modular Risk Assessment (MoRA). "MoRA gives our experts the ability to proceed methodically, to ask the right questions and to gain a complete understanding of the situation and all the problem areas," adds Prof. Sigl. Once the teams acquire this comprehensive basic understanding, they work their way deep into the component's internal structure. "We're not squeamish about that, especially when it comes to hardware," says Prof. Sigl. The methods used by the hardware specialists at Fraunhofer AISEC range from fuzzing to actually physically breaking open microelectronic

chips using systematic laser attacks on the electronic circuits. Meanwhile, the software security specialists delve deep into the program code. If the information they need is not in the source code, the researchers can fall back on reverse-engineering techniques, which involve using their tools and know-how to reconstruct the original program from its binary code, so that they can conduct an in-depth analysis of it. "Our customers are looking for two things in particular: risk analyses for product development and existing products and the development of security strategies along with support in implementing them correctly," says Prof. Eckert.

### A never-ending task

Cybersecurity is a continuous process that has to be integrated into operations at a very deep level. At the same time, however, there is no such thing as 100 percent security, because technology is being developed at an ever faster rate. That said, there is hope: Just as there are many ways of securing software and hardware, in the future, there will be many ways of stemming new threats. "However, a prerequisite here is that we maintain our ability to assess the risks and possibilities of

IT components accurately," says Prof. Eckert. "All the same, analyses and risk assessments absolutely have to be complemented by precisely the right security strategies and monitoring systems."

When it comes to monitoring systems in particular, a paradigm shift that experts have long been calling for is currently taking place in the business world: a gradual switch to zero-trust architectures. "This does not mean that I have to trust no one and nobody in order to be able to assess security. That would be very expensive and energy-intensive to implement," says Prof. Sigl. Instead, zero trust is about finding ways to reliably differentiate between areas in terms of their security level and to monitor access to these areas in accordance with the requirements of the specific case.



#### Contact

**Prof. Claudia Eckert**  
 Managing director  
 Phone +49 89 3229986-292  
 claudia.eckert@aisec.fraunhofer.de



#### Contact

**Prof. Georg Sigl**  
 Director  
 Phone +49 89 3229986-292  
 georg.sigl@aisec.fraunhofer.de

### Projects

#### Codyze

Codyze supports both developers and auditors in programming and evaluating security-critical software.



#### Clouditor

Clouditor is a tool that reviews the configuration of cloud services and applications in terms of their security.



#### IntelliSecTest

Four Fraunhofer institutes have joined forces in the IntelliSecTest research project to develop a cost-effective, user-friendly security testing process.



#### Trusted Electronic Bayern

Researchers in the Trusted Electronic Bayern project are working to develop a hardened secure element based on open-source RISC-V processors.



(in German)



## Secure in the knowledge

Every one of Fraunhofer AISEC's industrial security labs fulfills all the requirements needed for testing vehicles and production lines and developing and evaluating defense mechanisms. The information generated in these labs is laying the foundation for industrial security both now and in the future.

There are three vehicles in the Fraunhofer AISEC automotive security lab. "We can use our facilities to test all digital functionalities relevant to the topic of security on these vehicles," explains Bartol Filipovic. He is head of the Product Protection and Industrial Security department at Fraunhofer AISEC and at key moments, he has a vital role to play in ensuring that customers can rely on the IT security of their systems — for everything from connected vehicles and production facilities to the products themselves. That is why Filipovic or another of the almost 20 experts in Fraunhofer AISEC's industrial and automotive security labs can — or to be precise, must — try out every conceivable IT attack on these three vehicles. After all, unauthorized individuals and criminals can try these attacks too.

"Anyone who carries out a successful attack will also know what the vulnerabilities for industry espionage and sabotage are and can formulate appropriate countermeasures. This is important not only for complying with the ever stricter legal regulations, but also for ensuring that security is as comprehensive as possible in the future," says Mr. Filipovic. As he goes on to point out, this is also important because it can take years for new vehicles or industrial equipment to reach the market, where they will have to face attacks. Due to growing supplier dependency and the increasing connectedness of production processes, many weak points already exist even today. They are being

exploited now, but may not be discovered until a later stage. All this can result not only in financial damages but also in loss of reputation.

### Assessing the status quo — getting an overview

For example, in the context of the product piracy studies that Fraunhofer AISEC regularly conducts for the German industry association for machinery and equipment manufacturing (Verband Deutscher Maschinen- und Anlagenbau, VDMA), the data collected in 2022 showed that 72 percent of the member companies that responded are currently being affected by product piracy. In 2022, the damages caused by this reached 6.4 billion euros.

To allow companies to get an overview of their individual piracy and manipulation risks, Fraunhofer AISEC has developed an industry 4.0 and IT security audit that has already been deployed by a wide range of international industry companies. "The core element of the audit is a systematic risk analysis that assesses the status quo and makes it possible to get an overview of the situation," explains Mr. Filipovic. The audit asks questions such as, what elements do individual objects, vehicles and industrial production lines contain? And how are these modules connected? Thanks to the Modular Risk Assessment method (MoRA) [see glossary] that the audit is based on, it is possible that it



may only be necessary to replace an individual component in order to achieve a much higher security standard.

The IUNO Insec consortium project, which was coordinated by Fraunhofer AISEC, is also focusing on the idea of gaining an overview as a first step toward helping companies help themselves. "The goal was to develop solutions specially for small and medium-sized enterprises, so that they can increase their IT security levels independently," reveals Mr. Filipovic. Now, he adds, it is possible to conduct anomaly detection and security tests on control devices with tools that are comparatively easy to use.

### A team that combines user and technology know-how

Mr. Filipovic and his team have all the know-how needed for extensive analyses and tests and the development of security tools. In addition to combining knowledge from various research fields and industry sectors, they also have a variety of special instruments and tools — some of which they developed themselves — that can be used to subject individual components and embedded systems to diverse, advanced security tests. To allow them to simulate a wide range of threat scenarios, the experts in the industrial and automotive security labs have created

*The cybersecurity experts at Fraunhofer AISEC run tests on a vehicle in the protected environment of the automotive lab.*



models of the electronic infrastructures of vehicles and industrial production systems, such as a cutting-edge industrial production line with connections, docking sites and mobile and stationary robots. In addition, the experts also provide digital twins, i.e., digital models of processes that can be used to conduct many different simulations.

**Autonomous vehicles, sensor technology, industry 4.0 — IT security for real-world applications**

The labs are not only used to search for ways of attacking real or virtual objects in response to specific customer requests and needs; they also serve as a launchpad for pioneering research projects in the area of industrial and automotive security. This includes the project ATLAS-L4, for example, which is laying the foundations for mostly autonomous trucks that can not only avoid accidents, but also fulfill all existing and planned security requirements, such as those set out in the EU's Cyber Resilience Act (CRA-E) [see glossary]. Meanwhile, the project DigitalTWIN focused on another angle: In this project, the Fraunhofer AISEC team formulated and published security guidelines for sensors in facade elements. "The industry now has access to procedures that give answers to basic security questions in the context of sensors, communications with central units and cloud usage," explains Mr. Filipovic. Researchers in the PoQsiKom (Post-quantum secure communication for Industry 4.0) project are also attempting to provide concrete answers to security questions. With Fraunhofer AISEC at their head,

the partners of this consortium project are working to develop novel hardware root-of-trust devices for operating technology and edge devices. "This form of high-security chip will also be able to resist attacks by quantum computers. As such, they can be used to secure devices in smart factories so as to preserve security functions such as taking the human element into account in all cases," says Mr. Filipovic. This method will also provide reliable protection for complete remote control of machinery.

**Glossary**

*The Modular Risk Assessment (MoRA) is a risk assessment method created specially for the development of secure automotive systems.*

*The Cyber Resilience Act (CRA-E) is a proposed directive from the European Commission. This law is intended to increase cybersecurity in Europe in the long term, by setting out fundamental IT security requirements for digital products and their manufacturing processes.*

*In the Fraunhofer AISEC industrial security lab's highly realistic simulation environments, real, field-tested industry components can be used.*



**Projects**

**PoQsiKom**

In the PoQsiKom (Post-quantum secure communication for Industry 4.0) project, Fraunhofer AISEC is developing a novel hardware root of trust.

**DigitalTWIN**

In this project, the Fraunhofer AISEC team studied the security of digital twins and developed and published scenarios and protection models.

**ATLAS-L4**

The aim of the ATLAS-L4 project is to bring autonomous trucks to Germany's highways.

**IUNO Insec**

In the IUNO Insec project, Fraunhofer AISEC drove further advances in solutions that specifically support SMEs in increasing their own IT security levels.

**Industry 4.0 & IT Security Audit**

This audit developed by Fraunhofer AISEC is based on a risk assessment that uses the Modular Risk Assessment (MoRA) method.

**Product Piracy 2022**

The VDMA commissioned Fraunhofer AISEC to conduct the study Product Piracy 2022.



**Contact**

**Bartol Filipovic**

Head of the Product Protection and Industrial Security department  
 Phone +49 89 3229986-128  
 bartol.filipovic@aisec.fraunhofer.de



PoQsiKom



DigitalTWIN

(in German)



ATLAS-L4

(in German)



IUNO Insec



Industry 4.0 & IT Security Audit



Product Piracy study 2022

(in German)



# Data sovereignty? No doubt!

Digital sovereignty is becoming an ever more critical factor in a market context. Now, with the tools developed by Fraunhofer AISEC, companies can improve their security levels in a systematic way.

For a third of companies in Germany, digital self-determination has become a core element of their IT and business strategies. This trend could intensify further, as digital sovereignty means that a company can determine how its data is used and reused, even if it is processed outside of its direct control, e.g., on cloud platforms. In this way, not only is the data optimally protected against theft, manipulation and sabotage, but the company's dependency on individual suppliers is reduced, making it possible to resort to alternatives where necessary.

"Data sovereignty and technological sovereignty have become critical market factors and a hallmark of future-oriented industry," says Christian Banse, head of the Service and Application Security department at Fraunhofer AISEC. Implementing basic defense measures, such as encrypted data communication, authentication for system access and monitoring the legitimacy of any instances of access to the system, is a good starting point. However, these measures will not be enough to guarantee sovereignty in the event of a specific, targeted attack — as company leaders in sectors like the digital economy, industry 4.0, and the automotive and financial branches are well aware. This is why inquiries concerning confidential computing have risen in recent years. The expression is used to describe

technologies that ensure the confidentiality and integrity of data when it is transmitted, processed and stored.

### Constructing resilient, distributed systems

In 2022, Fraunhofer AISEC's experts initiated, continued and completed a wide range of foundational, user-focused projects, all with the goal of laying the groundwork for assessments of cyber threats and facilitating data sovereignty. Their particular focus was on companies that intend to systematically improve their security levels in the coming years. For example, Fraunhofer AISEC is continuously working to further develop the operating system GyroidOS, which is a tap-proof solution that can be used with IoT and edge device applications, as well as in the cloud. "GyroidOS, which is based on the Linux kernel, offers all the functionalities needed to harden a system," says Sascha Wessel, head of the Secure Operating Systems department.

GyroidOS is breaking new ground in many different ways, for example, by allowing data center operators to protect their customers' data in areas such as confidential computing and 5G infrastructure components or by helping defend powerful control devices in vehicles against attacks. The operating system



is also used in projects such as IMMUNE, in which Fraunhofer AISEC and the other consortium partners from science and industry developed an SDN [see glossary] platform for industry 4.0 scenarios.

In 6G-ANNA, a project funded by the German Federal Ministry of Education and Research (BMBF), GyroidOS is being used to show how future 6G services could be secured. The research results will allow the industry to make concrete advances toward constructing cyber-resilient, distributed systems in the future. Cyber-resilient systems will be able to detect attacks on devices, for example, and, if the worst comes to the worst, isolate the affected functions or migrate them to another node, so that functionality can be maintained securely in spite of attacks. GyroidOS is also being used in the trusted connector the institute developed — this is one of the research results generated by the International Data Spaces (IDS) initiative organized by Fraunhofer. “The trusted connector is a software that offers a secure execution environment and an IDS protocol for data exchange and interactions with a service broker, as well as supporting a clearing house,” explains Mr. Banse.

**Security check tools**

New German and European regulations and the European Union Cybersecurity Certification Scheme on Cloud Services (EUCS), which is likely to be passed, require that companies make further improvements in the area of data sovereignty. “It’s possible that some people are not yet prepared for these and other regulations, so they now have to go through those lists point by point to check

whether they have fulfilled the requirements in question,” says Mr. Banse. To make this process easier, Fraunhofer AISEC has developed the Clouditor tool. This examines the security of cloud connections and summarizes all the relevant information for necessary changes or later audits. The analysis tool Codyze works in a similar way but with a focus on applications. Fraunhofer AISEC is making this tool available in conjunction with the German Federal Office for Information Security (BSI). Codyze reviews programs’ cryptocode and reports any anomalies or vulnerabilities. Both Clouditor and Codyze are undergoing continuous further development. They are also essential for projects like MEDINA, an initiative funded by the European Commission, in which Fraunhofer AISEC and its partners are developing a toolkit for automatically conducting a variety of security assessments on the basis of existing standards. “Our goal is to provide companies and institutions with a tool suited to their specific application, which they can use to review their data sovereignty,” explains Mr. Banse.

**Glossary**

*Software-defined networking (SDN) refers to networks that are controlled by the software in the network’s central server rather than the hardware.*



**Contact**

**Sascha Wessel**

Head of the Secure Operating Systems department  
Phone +49 89 3229986-155  
sascha.wessel@aisec.fraunhofer.de

**Projects**

**Clouditor**

Developed by Fraunhofer AISEC, Clouditor is a tool that continuously reviews the requirements for services and applications and that can indicate whether the cloud services a company is using fulfill the agreed security and compliance requirements.

**Trusted connector**

Fraunhofer AISEC’s trusted connector, which was awarded the IDS-ready label in 2021, is an approach for securely exchanging data across company boundaries, while maintaining control of data flows and data usage.

**MEDINA**

In the project MEDINA, a consortium of industry and research partners are combining their expertise in the area of cloud security in order to automate security assessments based on future standards (e.g., standardized European certification catalogs) and to continuously review compliance with these certification criteria.

**Codyze**

Developed by Fraunhofer AISEC and the BSI, the automated analysis tool Codyze provides support for programming and evaluating security-critical software.

**GyroidOS**

Developed at Fraunhofer AISEC, GyroidOS is a virtualization solution for IT security that isolates applications and data that are particularly worthy of protection in service containers, that are disconnected from critical components.

**IMMUNE**

In the project IMMUNE, Fraunhofer AISEC and its partners are developing a self-defending, resilient SDN platform for industry 4.0 scenarios.



**Contact**

**Christian Banse**

Head of the Service and Application Security department  
Phone +49 89 3229986-119  
christian.banse@aisec.fraunhofer.de



Clouditor



Trusted connector

(in German)



MEDINA

(in German)



Codyze



GyroidOS



IMMUNE

(in German)





## We have to reckon with all eventualities

In this interview, Prof. Daniel Loebenberger, Prof. Marian Margraf and Dr. Matthias Hiller discuss post-quantum cryptography (PQC) and preparing IT security for the quantum age.

Prof. Loebenberger, you lead the Secure Infrastructure department at Fraunhofer AISEC, and together with Prof. Margraf and Dr. Hiller, you are the main point of contact for the Competence Center for Post-Quantum Cryptography. What specific services does the center offer for companies and institutions?

**Prof. Loebenberger:** We support companies in making the switch to quantum-resistant cryptography. To do this, we essentially combine the cumulative PQC expertise of the individual departments at Fraunhofer AISEC. This includes

migrating PQC processes, conducting security analyses and continuously expanding our knowledge around PQC. We also deal with standardization and provide training, and we are constructing an information portal.

You outlined some of these services at the annual PQC networking event that Fraunhofer AISEC has been hosting since 2022.

**Prof. Margraf:** That event was focused on the research, from protocols and cryptographic issues to implementation,

crypto-agility, domain-specific knowledge and analyses. The goal of the event is to bring together a wide range of different areas of expertise from these fields. With around 200 participants from science and industry, it's one of the largest PQC events in the German-speaking world.

The interest in the event also clearly indicates the growing importance of post-quantum cryptography.

**Prof. Loebenberger:** PQC is concerned with a threat situation that could arise — emphasis on “could.” However, if it were to become a reality, the consequences would be extreme. It's possible that the coming years will see the creation of a quantum computer that could break our current encryption technology and wreak havoc on IT security. It is very likely that this moment will come; what we do not know is when.

**Prof. Margraf:** This shows the conflict between research and practice. If it does come to that, and companies and institutions are not prepared for it, the damage would be almost unquantifiable. It's what we refer to as the “cryptographic Armageddon” here. We have to be prepared for this scenario. And simply developing existing cryptographic processes further — e.g., increasing key length — is not going to help in every case.

At the same time, switching cryptographic processes is often very complicated as the infrastructures are not prepared for it. That's why we at Fraunhofer AISEC are working intensively to find ways of securing encryption methods against potential attacks by quantum computers going forward and to develop possible security structures for the future.

**Prof. Loebenberger:** Our goal is a kind of crypto-agility that makes companies and institutions more secure in general. We are working on using hybrid processes that combine existing cryptographic methods with PQC. At the same time, the implementation has to be affordable.

Prof. Margraf, you are the head of the Secure Systems Engineering department at the institute, and among other things, your responsibilities include the Full Lifecycle Post-Quantum PKI (FLOQI) project, which uses these hybrid procedures.

**Prof. Margraf:** That's correct. In FLOQI, we have joined a consortium project that aims to implement this approach in the context of digital certification. We want to ensure that the transition from the existing process to the new version is as seamless as possible. To that end, we are developing public key infrastructure processes that facilitate simultaneous use of quantum-computer-resistant processes even today.

Aquorypt, a project that aims to bring quantum-computer-resistant cryptography into application, is another practice-oriented initiative. Dr. Hiller, you are the head of the Hardware Security department, which is working on this consortium project.

**Dr. Hiller:** In Aquorypt, we are investigating the applicability and practical implementation of quantum-computer-resistant cryptographic processes in embedded systems and chip-card-based security applications. The focus here is on implementing PQC to counter vulnerability to side-channel attacks. In addition, we are searching for possible new attack techniques, so that we can assess cyber threats accurately and develop suitable defense mechanisms.



Answering “what would happen if...” questions seems to drive your research activities as regards PQC.

**Prof. Loebenberg**: Exactly. In addition to general research and our information services, we are also establishing security standards, for example, taking stock of possible, real attack points at companies and migrating practical applications.

**Prof. Margraf**: Examples of this include our research in consortium projects such as “BOTAN cryptographic library: long-lasting security for IT applications and services” (KBLS) and QuaSiModO (Quantum-resistant VPN Modules and Operating Modes). In KBLS, we are implementing quantum-computer-resistant processes in the Botan cryptographic library, while also considering mechanisms that will allow developers to exchange cryptographic algorithms efficiently. Botan provides unlicensed crypto-algorithms that have been designed so as to allow users to avoid implementation errors. We have now expanded this service to include post-quantum algorithms.

The background context to QuaSiModO is that implementing post-quantum mechanisms in virtual private networks is currently still associated with significant disadvantages,

for example, because the system is prone to breakdowns. Together with the Internet Engineering Task Force [see glossary], we are working to develop standards that will help remedy this handicap.

Many thanks for taking the time for this interview.

**Glossary**

*The Internet Engineering Task Force is an internet standards development organization responsible for the technical standards underlying internet protocols.*

*Prof. Daniel Loebenberg at the post-quantum cryptography workshop speaking about crypto-agility and the migration to quantum-resistant encryption processes.*



**Projects**

**FLOQI**

The objective of the Full Lifecycle Post-Quantum PKI (FLOQI) project is to develop a quantum-computer-resistant PKI.

**QuaSiModO**

The QuaSiModO (Quantum-resistant VPN Modules and Operating Modes) project investigates, tests and implements new quantum-computer-resistant algorithms.

**KBLS**

As part of the BOTAN cryptographic library: long-lasting security for IT applications and services (KBLS) project, Botan, an established free cryptographic library, is being expanded to include quantum-computer-resistant processes.

**Aquorypt**

The Applicability of Quantum-computer-resistant Cryptographic Algorithms (Aquorypt) project is investigating the application and practical implementation of cryptographic processes that are resistant to quantum computers.

**Contact**



**Prof. Daniel Loebenberg**

Head of the Secure Infrastructure department  
Phone +49 89 3229986-139  
daniel.loebenberg@aisec.fraunhofer.de



**Prof. Marian Margraf**

Head of the Secure Systems Engineering department  
Phone +49 89 3229986-152  
marian.margraf@aisec.fraunhofer.de



**Dr. Matthias Hiller**

Head of the Hardware Security department  
Phone +49 89 3229986-162  
matthias.hiller@aisec.fraunhofer.de



**FLOQI**  
(in German)



**QuaSiModO**  
(in German)



**KBLS**  
(in German)



**Aquorypt**  
(in German)

The **Competence Center for Post-Quantum Cryptography** provides support in the switch to quantum-resistant cryptography and protocols.





## The hardware hardeners

**Identifying security vulnerabilities in hardware components such as chips or electronic circuits not only takes comprehensive electrical engineering know-how, but also in-depth knowledge of the laboratory technology required. Fraunhofer AISEC has both, and much more besides.**

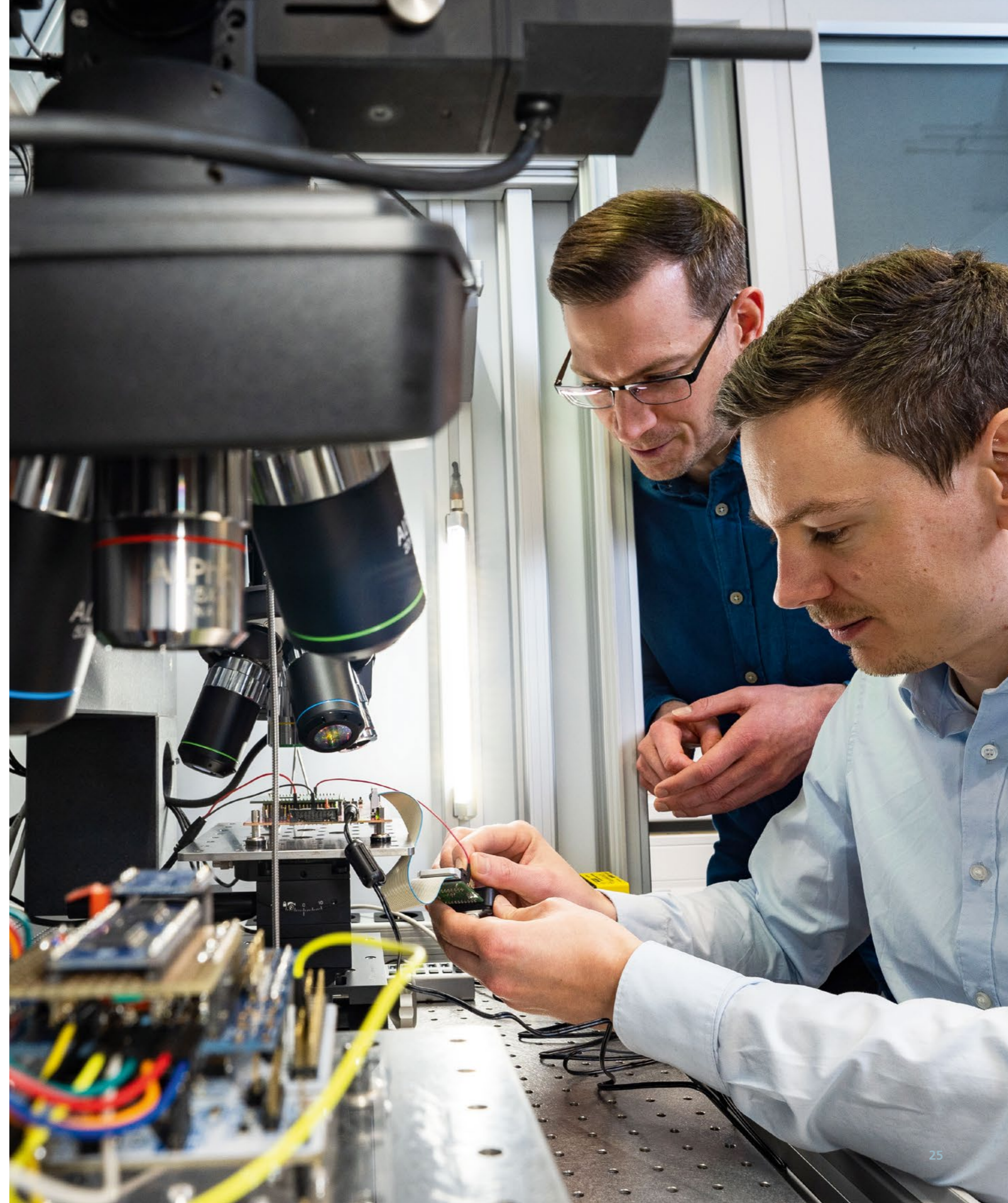
The object of desire is a fraction of a millimeter in size. A near-field probe is precisely placed close above it. “Now,” says Dr. Matthias Hiller, indicating the connected oscilloscope, “the signal can be easily recorded and the noise is reasonably low.” The attack on the exposed chip, which measures three by three millimeters, and its millions of transistors can get underway. The probe begins to move forward micrometer by micrometer, recording small electromagnetic pulses as it goes. When the probe reaches the right position, a structure can be read from the data. The results of each measurement are then transferred to a connected computer in order to carry out a side-channel analysis [see glossary]. This involves using a set of various analysis tools that build upon each other to expose the secrets of the supposedly secure chip. This requires comprehensive knowledge in areas such as developing specialized analysis tools and using them in a targeted way. Patience is required here, as it can take days, weeks or possibly even months before a chip will yield its cryptographic key and, ultimately, the data that was encrypted with it.

Now Dr. Hiller and his team can make a start on the second phase of their work: They are investigating mechanisms for securing processors and microcontrollers and the code that runs on them, as well as FPGAs [see glossary], to prevent future attacks similar to

their own side-channel attack. This is why security experts at Fraunhofer AISEC are conducting research into developing secure hardware, implementing secure cryptographic processes that are resistant to side-channel attacks, and processor hardening. “Our goal is to continuously expand our knowledge of attacks and countermeasures, so that we can reliably evaluate and improve hardware components such as chips or microcontrollers in the future,” says Dr. Hiller. To improve the general level of IT security, it is also essential to secure its foundation — the hardware.

### In attack mode

In his role as head of the Hardware Security department at Fraunhofer AISEC, Dr. Hiller is an important point of contact at the institute’s almost 120 meter-square hardware security lab. Day after day, more than a dozen experts launch attacks from here. A chip’s side channels are only one potential path of attack. Design or implementation flaws can facilitate espionage or even sabotage through methods such as sniffing bus communications, exploiting debug interfaces and reading out memories. The hardware hardeners at Fraunhofer AISEC have reserved their own laboratory space for using high-precision lasers to carry out fault injection attacks [see glossary]. At the high-end dual-laser station, for example, they can change the values





on a chip in a specific way so that it goes on to make calculations based on false conditions. "This makes it possible to evade protective measures in the chip, or to alter processes, for instance," says Dr. Hiller. As an alternative to this type of active attack on chip performance, the hardware security lab can also carry out glitching attacks [see glossary], for which it is equally well equipped. Here, the supply voltage or clock frequency is changed for fractions of a second to force the system to make faulty calculations.

### Securing the industrial value chain

The knowledge the team has acquired over the almost 15 years of the laboratory's existence not only supports customers and institutions with high or top-level security requirements. It also feeds into the development of new and far-reaching security systems. The

VeLelektronik collaborative project, for instance, which is under the technical coordination of Fraunhofer AISEC, focuses not just on one item of hardware, but on the entire microelectronics industry value chain. "Because development and production generally involves the participation of multiple global suppliers, designers and manufacturers, it has been almost impossible until now to guarantee that a system actually contains only what was specified," explains Dr. Hiller. Fraunhofer AISEC, together with its partners, is researching ways of making design methods and analysis as well as manufacturing processes more trustworthy, for example, by installing unique features in every chip that allow the individual steps of the value chain to be traced securely. In 2024, the collaborating partners plan to present an accompanying portfolio of concepts and methods that will then be made accessible via a platform.

*Security experts at the hardware lab analyze embedded systems for hardware-based attack vectors.*



### Tamper-proof protective film

The founding of the Zentrum Trusted Electronic Bayern (Bavarian center for trusted electronics, TrEB) illustrates how crucial it is for Fraunhofer AISEC to collaborate with experts from other Fraunhofer institutes. At TrEB, the Fraunhofer Institute for Electronic Microsystems and Solid State Technologies EMFT and the Fraunhofer Institute for Integrated Circuits IIS are working closely with the hardware teams from Fraunhofer AISEC to establish a competence center for researching and developing secure, trustworthy integrated electronic systems. "One goal of this project, which is being funded by the state of Bavaria, is to develop a protective film that will encase critical circuits to make them tamper-proof and give them better protection," says Dr. Hiller. This will prevent physical manipulation, especially in systems for high-security sectors, such as

official identity documents, for example. The RISC-V open standard [see glossary] allows processors to be developed specifically to suit the customer's purposes, and to be hardened in line with their requirements. What's more, researchers are constantly working on developing the hardware security lab itself. "It is crucial for the laboratory and its research to expand into increasingly sophisticated security mechanisms — crucial, too, for the customers who will be approaching us in the years to come," says Dr. Hiller. This is the only way to ensure that to the greatest extent possible, the security of industrial hardware remains that one decisive step ahead of actual attacks.

### Glossary

*In a side-channel analysis, the physical implementation of a cryptosystem, e.g., a smart card or hardware security module, is examined for vulnerabilities.*

*A FPGA (field-programmable gate array) is a microchip containing configurable circuit blocks that can still be programmed even after manufacturing is complete.*

*In a glitching attack, a processor's calculations are manipulated in a targeted way.*

*RISC-V (reduced instruction set computer) is an open-source instruction set architecture for controlling processors.*

*Fault injection is a testing technique for understanding how computer systems behave when stressed in unusual ways.*



### Contact

#### Dr. Matthias Hiller

Head of the Hardware Security department  
Phone +49 89 3229986-162  
matthias.hiller@aisec.fraunhofer.de

### Projects

#### VeLelektronik

In the VeLelektronik project, the Leibniz Association, the Research Fab Microelectronics, the edacentrum and the Fraunhofer-Gesellschaft are working together to secure value chains in the microelectronics industry.



#### TrEB

The Zentrum Trusted Electronic Bayern (trusted electronic center Bavaria, TrEB) carries out research and development activities around secure, trustworthy integrated electronic systems.



(in German)





## Closing gaps in expertise

**Vivija Čepkalo-Simić is project manager at Fraunhofer AISEC's Cybersecurity Training Lab. In this interview, she explains how the Training Lab's range of further training courses can support companies, and who this training is suitable for. Highlights include training in the areas of machine learning, vehicular communications and embedded systems security.**

**Why should companies or public authorities send their employees to the Fraunhofer AISEC Cybersecurity Training Lab?**

Anyone who comes to us leaves better equipped to assess the threats to their institution's IT security and minimize risks. Knowledge is key here. We can provide this knowledge — to specialist employees and managers alike. And this can happen either here in our laboratory in Garching near Munich or at Weiden in der Oberpfalz in Bavaria. However, these one- or two-day seminars and workshops, with content tailored to the client's specific needs, are also frequently held on-site at the company's own premises.

**The focus here is on updating expertise, rather than upgrading it in the sense of simply providing a general, basic briefing.**

If those responsible for IT security are to fend off cyber threats, they must assess them correctly. At Fraunhofer AISEC, we develop specialized knowledge that we can transfer to companies and public authorities through the Cybersecurity Training Lab. We are not a training company

with a strict teaching plan that provides off-the-peg information. While our work is oriented toward the actual needs of our customers from industry, we also cover future-oriented issues so our customers will be able to assess the cybersecurity challenges to come, and can act early to apply the appropriate countermeasures. By taking this approach, we focus both on the company's interests and the legal requirements for fulfilling security criteria. This means the training programs are concisely tailored to each company's current circumstances.

**What content do you offer, and which topics have been the most popular recently?**

The Training Lab at Fraunhofer AISEC specializes in the fields of embedded systems, the internet of things and mobile security. Other Fraunhofer institutes offer courses on additional topics under the umbrella of the Fraunhofer Academy's Cybersecurity Training Lab. We focus on providing training in areas such as improving security through machine learning, securing FPGA-based systems, vehicular communications and hardware-supported analysis of embedded systems.





A look at the *Charlie and the Quantum Factory* game

Over the past year, we have also seen very high demand for training in post-quantum security. This may be due to the fact that our institute has a leading role in this area of research. We also get a lot of bookings for courses on risk analysis. We work with the client to create custom learning content tailored as closely as possible to their needs.

So the Training Lab's website, which you can access through the Fraunhofer AISEC website, only gives a general overview of the topics available.

Exactly. Since our service focuses on high-level security measures for specific issues, it would not be beneficial to offer generalized training courses. So what you can see on our website is only an outline of possible topics. We design and create courses in line with customers' needs — that is our specific approach, and companies appreciate it: in 2022, our revenue from training courses grew by 50 percent.

Now, in early 2023, our experts are already in such demand that we are having to plan individual training courses well in advance.

So does that mean the trainers are not just technical experts, but also experienced teachers?

Many of our trainers give seminars and lectures at universities, so they also have teaching experience. They are constantly working on expanding their expertise in this area. For example, they attend the Train the Trainer workshops run by the Fraunhofer Academy, which we are involved with at an organizational level and in terms of the content of the courses.

Finding accessible ways to communicate knowledge is clearly important to you, as demonstrated by "Charlie," who initially seems to be trapped in a quantum world.


Charlie and the Quantum Factory is a web-based computer game incorporating puzzles and mini games that we developed at the institute in 2022 as a playful introduction to learning about the workings of quantum computers. Accessible options like these were a big hit at the Girls' Day in 2022. In addition, we offer self-guided courses free of charge as an introduction to the functions and applications of quantum computers. Having these links to interested members of the public is also important to us, because we want to communicate knowledge across the widest range of levels using different approaches. Serious games and online resources are part of this.

At the Cybersecurity Training Lab, this also includes having strong links to practical implementation.

This is vital to us, as we want to offer clear benefits to participants and their companies. That's why we give people the space — in the truest sense of the word — to test out tailor-made solution strategies. For example, we have a modern training room with its own shrouded network into which we can feed viruses for practical defense training. Our laboratories — whether for hardware security or industrial and automotive security — offer specialized demonstrators and instruments for "testing out" side-channel attacks and tools for securing communications, for

example. This allows us to link our research to ongoing and upcoming security issues experienced by companies. Participants come away from our training with practical knowledge aimed at keeping pace with the current state of affairs while also remaining oriented toward the future.





**Contact**

**Vivija Čeprkalo-Simić**  
 Project manager, Cybersecurity Training Lab  
 Phone +49 89 3229986-138  
 vivija.ceprkalo@aisec.fraunhofer.de

### Further training and seminars on IT security

The **Cybersecurity Training Lab at Fraunhofer AISEC** specializes in the areas of embedded systems, the internet of things and mobile security.



(in German)

The serious game **Charlie and the Quantum Factory** provides a playful introduction to learning about the workings of quantum computers.



(in German)

The **Fraunhofer Academy's Cybersecurity Training Lab** coordinates the transfer of knowledge from the Fraunhofer institutes into actual practice.







## Fraunhofer Singapore becomes a center for cybersecurity



[Read the press release](#)

Fraunhofer Singapore, a legally independent, international Fraunhofer affiliate, became a center for cybersecurity (Fraunhofer Center for Applied and Integrated Security CAIS) in 2022. The center's research activities focus on secure communications using quantum technology and quantum security. Since 2022, Fraunhofer AISEC has been a partner institute to the new center, which will also be working in close collaboration with Singapore's Nanyang Technological University (NTU). "This partnership will allow us to systematically expand our expertise in secure quantum communications, which will also benefit our customers in Germany and Europe," says Prof. Georg Sigl, director at Fraunhofer AISEC.

## Zentrum für vertrauenswürdige Künstliche Intelligenz (center for trusted artificial intelligence) creates non-discriminatory AI



[Read the press release \(in German\)](#)

"AI systems must operate in a non-discriminatory manner. We want to guarantee this at a technological level," says Prof. Marian Margraf, head of the Secure Systems Engineering department at Fraunhofer AISEC in Berlin and project manager for basic research at the Zentrum für vertrauenswürdige Künstliche Intelligenz (ZVKI). The ZVKI is laying the foundations for implementing AI systems that are more comprehensible and, above all, more secure. Trust in the technology plays an important role here. To build this trust, and to harness AI in line with ethical principles, the necessary conditions must be created. Protecting personal data and ensuring transparency in AI decision-making are necessary parts of this process. The goal of the ZVKI is to map out comprehensive methods for regulation and test their technical applicability. The center is being set up by the independent think tank iRights.Lab in collaboration with Fraunhofer AISEC and Fraunhofer IAIS and Freie Universität Berlin, with the support of the German Federal Ministry for the Environment, Nature Conservation, Nuclear Safety and Consumer Protection (BMUV).

## Prof. Claudia Eckert is inducted into the Hall of Fame der deutschen Forschung (German research hall of fame)

Prof. Claudia Eckert, managing director at Fraunhofer AISEC, has been one of the most prominent figures in IT security for over 20 years. As one of Germany's leading computer scientists, in 2022 she was honored for her outstanding contribution to cybersecurity research and inducted into the Hall of Fame der deutschen Forschung (German research hall of fame). Her constant mission is to translate excellent IT security research into solutions of immediate value to the industry and society. Each year, the Hall of Fame der deutschen Forschung honors scientists whose achievements have helped to ensure Germany's future viability as a science and business hub. The award was launched in 2009 by manager magazine. Since 2015, the award has been presented in conjunction with the company Merck.



[Watch a video profiling the award winner \(in German\)](#)

## Cybersecurity blog launch

In July 2022, Fraunhofer AISEC launched a new resource for IT security research topics in the form of a cybersecurity blog, where our experts offer exciting insights into their scientific work. The blog articles address the latest innovative topics, such as trusted AI, IoT security, post-quantum cryptography, white-hat hacking, secure digital identities and industrial security. These articles are drawn directly from the scientists' everyday research and present new scientific findings and provide solutions to specific problems. Anyone with an interest in these topics can gain an insight into the main research areas and into the working methods of IT security researchers.



[Read the cybersecurity blog](#)





## Our mission: to evaluate, design and safeguard cybersecurity

While negotiating the conflicting demands of economic pressures, user-friendliness and security requirements, over 230 cybersecurity specialists at Fraunhofer AISEC systematically assess the IT security of products, networked systems and infrastructures, make them more robust against attacks and preserve their long-term security.

### Evaluate: measure, understand, assess

Does the software just do what I expect it to, and nothing more? Can its decisions be verified? Where did my hardware components originate from?

Evaluating the extent to which systems can be trusted requires tools that can seek out vulnerabilities using in-depth approaches that are automated to the greatest extent possible; this exploration must span the entire life cycle, from the design phase, to production and programming, to integration into existing systems, right through to operative use.

In the test laboratories at Fraunhofer AISEC, researchers are creating the transparency required to evaluate the consequences of using a piece of hardware or software. Whether conducted on behalf of customers or in the context of in-house research, testing is carried out on the functionality, interoperability, conformance and compliance of networked and embedded systems, hardware and software products and web- and cloud-based services. Strategic alliances with international partners and universities mean this research is grounded in the latest scientific findings and processes.

### Design: conceptualize, integrate, harden

Researchers are developing security solutions that can not only keep pace with the increasing complexity of our IT systems,

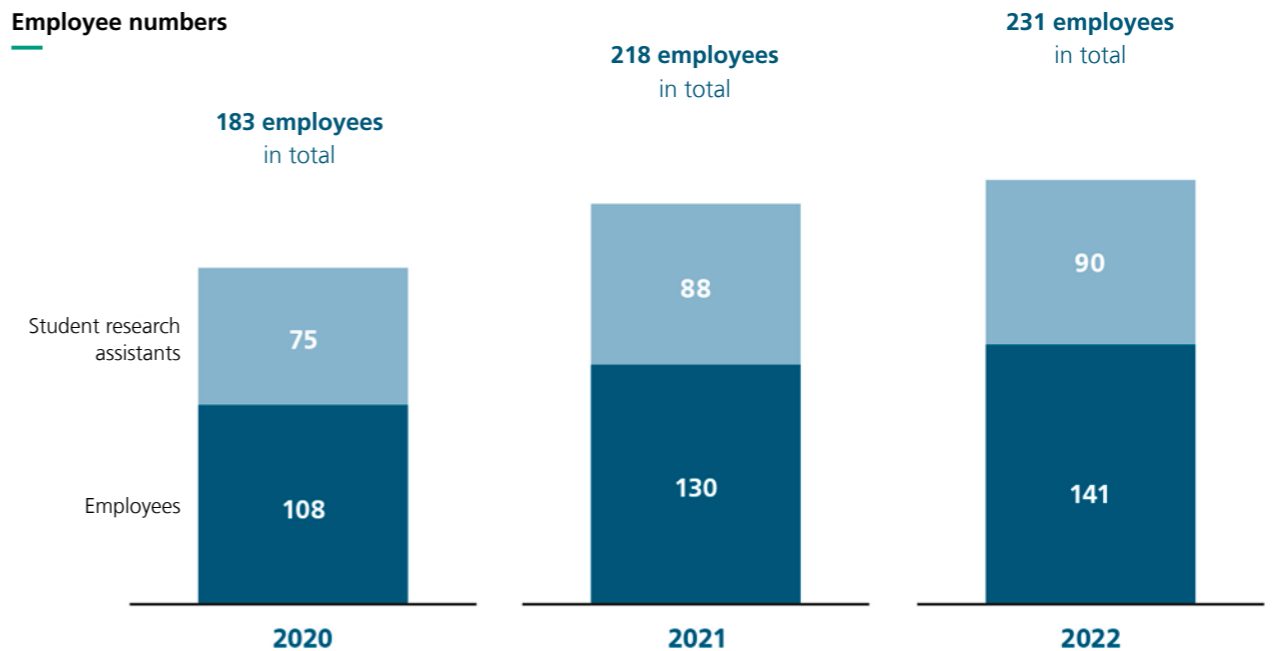
but also stay one step ahead of attackers. Tailor-made security policies safeguard data and provide effective protection against cybercrime. This comes about through trusted, secure design, secure integration of otherwise insecure elements and continuous monitoring of security conditions. Our researchers work closely with globally operating industry companies as well as specialized SMEs and companies in the public sector. They understand the needs of clients, working with them to implement solutions in line with market requirements and training them to assess cybersecurity developments and continuously improve their own level of security.

### Safeguard: preserve, strengthen, protect

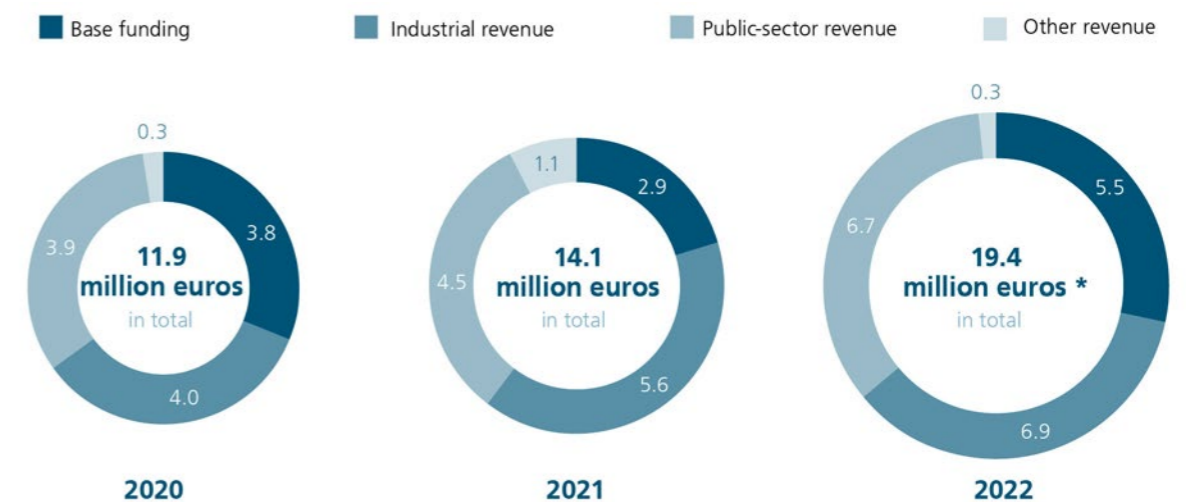
These applied cybersecurity solutions provide the Fraunhofer AISEC customers of today with protective measures for tomorrow, which can be continuously assessed and adapted to keep up with the rapid pace of technological progress. In this way, they can safeguard the long-term integrity, availability and confidentiality of their data and IT systems. Research by Fraunhofer AISEC protects not only private individuals, our infrastructure and democracy, but bolsters the competitiveness of customers and partners and makes a crucial long-term contribution to the digital sovereignty of Germany and Europe.

## Facts and figures

### Employee numbers



### Research revenues (in millions of euros)



\*preliminary figures



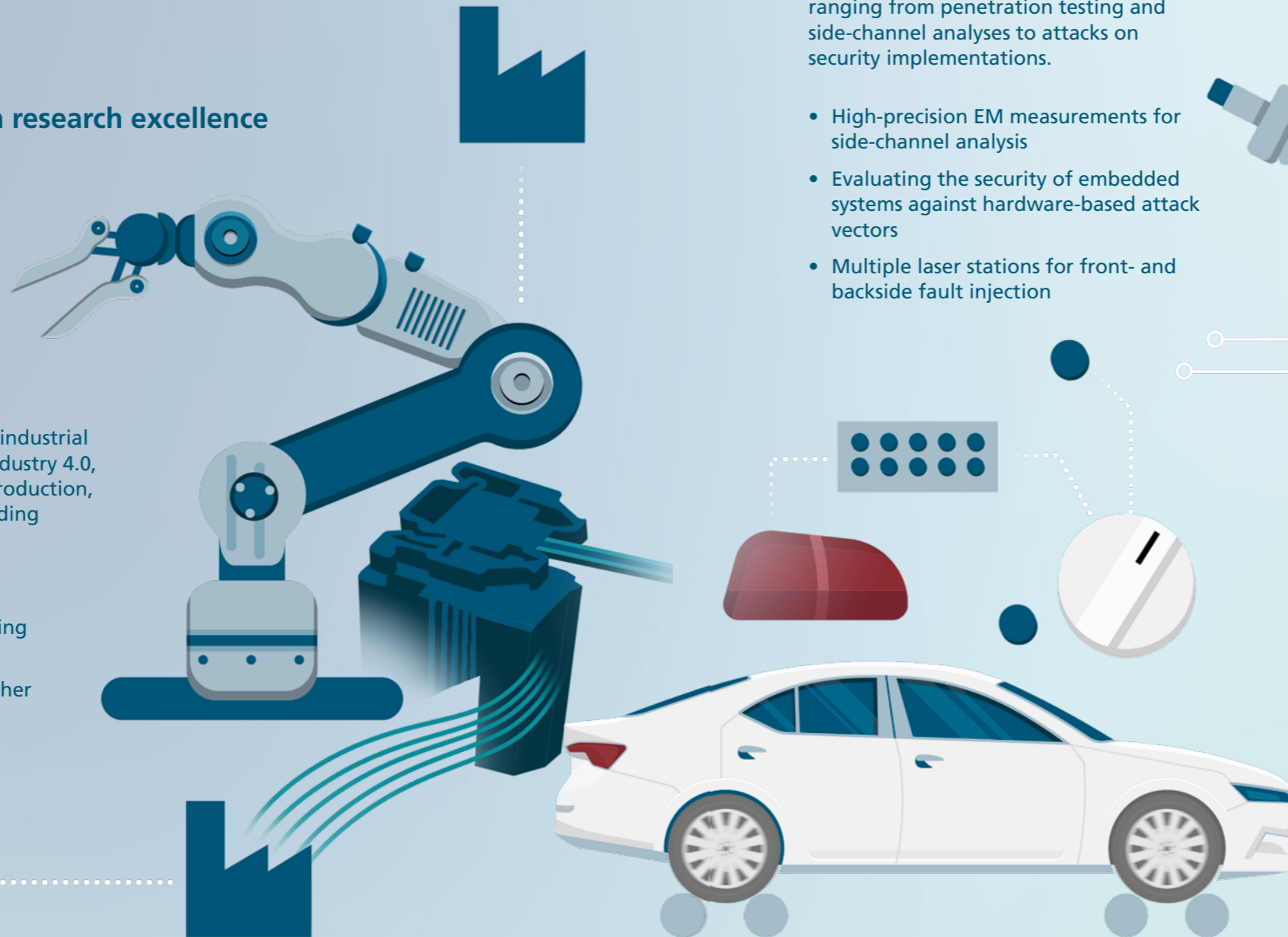
# The world of labs at Fraunhofer AISEC

Tailor-made solutions based on research excellence

## INDUSTRIAL SECURITY LAB

The spectrum of services offered by the industrial security labs ranges from analyses for industry 4.0, the internet of things and networked production, right up to investigating security in building automation.

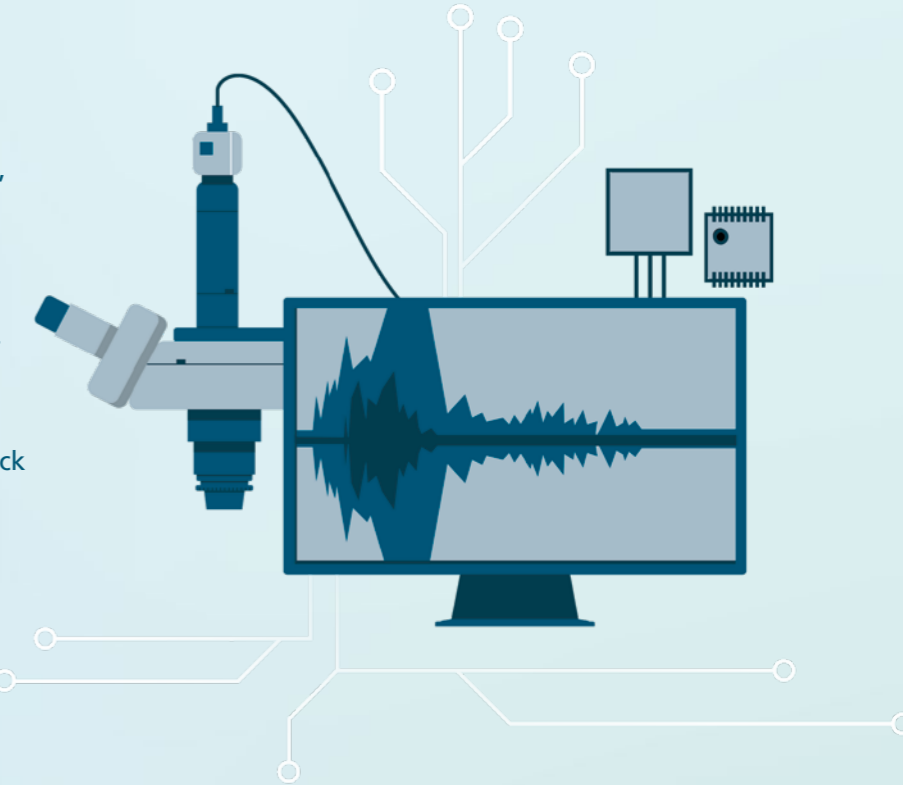
- Risk analysis and penetration testing
- Realistic environmental simulation using actual components
- Increased computing capacity for further simulations (AR and VR)



## HARDWARE SECURITY LAB

The Hardware Security Lab offers a spectrum of hardware security analyses, ranging from penetration testing and side-channel analyses to attacks on security implementations.

- High-precision EM measurements for side-channel analysis
- Evaluating the security of embedded systems against hardware-based attack vectors
- Multiple laser stations for front- and backside fault injection



## AUTOMOTIVE SECURITY LAB

The Automotive Security Lab enables security testing of complete vehicles and multiple, interacting components in a secure, trusted environment.

- Risk analysis and penetration testing
- Security engineering and vehicle development methods
- Development and testing of security measures

## LAB FOR ISOLATION MECHANISMS

The test lab for isolation mechanisms conducts tests on modularized software stacks. The key focus areas are evaluating isolation mechanisms in system-related components and eliminating of vulnerabilities.

## SYSTEM SECURITY LAB

The System Security Lab develops and evaluates secure system solutions for embedded and mobile devices, as well as servers. Its main focus is resilience and resistance against attacks.

## SOFTWARE SECURITY LAB

The Software Security Lab researches methods for analyzing and hardening software. The goal is to find and fix vulnerabilities in programs and prevent the exploitation of vulnerabilities.

## CLOUD SECURITY LAB

The Cloud Security Lab offers a variety of options for evaluating and securing cloud services.

## SMART SENSOR LAB

The Smart Sensor Lab uses software-defined radio components to examine all common radio standards and their linked IoT protocols for vulnerabilities.

## IOT SECURITY LAB

The test lab for IoT security analyzes the software of networked devices and eliminates vulnerabilities. The focus is on devices with incomplete source code.

## SECURE DATA ECOSYSTEMS LAB

The Secure Data Ecosystems Lab provides the infrastructure for developing, planning and implementing trusted data spaces for cloud and edge computing.



# Fraunhofer AISEC — a great place to work

## Ten reasons to work at Fraunhofer AISEC

Experience the diversity of cybersecurity research across various fields of application.

Work in a research field that is only growing in importance: cybersecurity.

Increase the usability and trustworthiness of digital applications.

Find and eliminate security-related vulnerabilities in both hardware and software.

Conduct research in cybersecurity laboratories equipped with cutting-edge facilities.

Translate the latest research findings into practical application.

Enjoy an excellent work-life balance with flexible hours and remote working.

Work with the latest cybersecurity technologies, drive rapid progress in the field and accelerate your own personal development.

Gain practical experience while completing a doctorate in your chosen field.

Bring research and industry together and connect both worlds.

### Awards for Fraunhofer-Gesellschaft as an employer





## Members of the advisory board



**Dr. Stefan Hofschien**  
Spokesperson for the advisory board and CEO, Bundesdruckerei GmbH



**Naby Diaw**  
Chief Information Security Officer, Vice President, Lufthansa Group



**Dr. Astrid Elbe**  
Vice President Product Development, Aviat Networks



**Prof. Georg Carle**  
Chair of Network Architectures and Services, School of Computation, Information and Technology, Technical University of Munich



**Andreas Könen**  
Director-general of Cyber and Information Security, German Federal Ministry of the Interior and Community (BMI)



**Dr. Manfred Paeschke**  
Chief Visionary Officer, Bundesdruckerei GmbH



**Dr. Heike Prasse**  
Head of Communication and Security of Digital Systems department, German Federal Ministry of Education and Research (BMBF)



**Thomas Rosteck**  
Division President Connected Secure Systems, Infineon Technologies AG



**Dr. Stefan Wimbauer**  
Head of Applied Research and Cluster Policy department, Bavarian Ministry of Economic Affairs, Regional Development and Energy



**Dr. Bettina Horster**  
Executive board  
VIVAI Software AG



**Dr. Andreas Kind**  
Vice President Cybersecurity & Trust, Head of Technology SiGREEN, Siemens AG



**Prof. Mira Mezini**  
Head of Software Technology Group, Department of Computer Science, Technical University of Darmstadt



**Vera Schneevoigt**  
Former Chief Digital Officer/Senior Vice President Engineering, Bosch Security and Safety Systems GmbH





## A neutral technology supplier for the data economy

Digitalization is improving both processes and products; however, it will only give rise to new business models if it is based on trustworthy, automated means of collecting, storing and processing data. In pursuit of this goal, the Fraunhofer Cluster of Excellence Cognitive Internet Technologies CCIT is bringing together the latest scientific findings, knowledge and problem-solving expertise along the entire digital value chain. Fraunhofer AISEC is the spokesperson institute for the cluster and is responsible for security in the projects.

Digitalization in Germany is stagnating. The Digitalization Index [see glossary] by the German Federal Ministry for Economic Affairs and Energy (BMWi) confirms this: in 2022, the average index point level rose by just one point to reach a total of 108.9 points. As a comparison: the leading sector, information and communication technologies, achieved an index value of 275.9 points. This means we still have a long way to go before we can securely consolidate data across all sectors to bring about energy- and cost-efficient use of resources, improved processes, innovative products and new business models.

### Bringing data and users together

To turn the vision of a digital economy into a reality, countless stakeholders need to collect, consolidate and exchange enormous volumes of data from heterogeneous data sources, such as from sensors in mobile end devices and machines, saved documentation and entire production processes.

This data must then be automatically analyzed, processed and put into application in services that create added value. This requires trusted data exchange and application processes, which must be automated in light of the huge quantities of data involved. Only then will the data become "intelligent," which will in turn make it possible to apply techniques such as machine learning (ML) so that we can extract the new insights we need from it in order to bring about process and product innovations. One example of this is the Catena-X data space that is currently being set up. In Catena-X, very heterogeneous data sets, e.g., data from product use and production data, are used to meet a wide variety of user needs, such as optimizing traceability for goods and reducing carbon footprints. In addition, the development times and commercialization methods involved in the technologies required to build this data space (such as electronic components for the hardware and software apps) are very different. "Bringing all these aspects together as part of our vision of creating a functional,

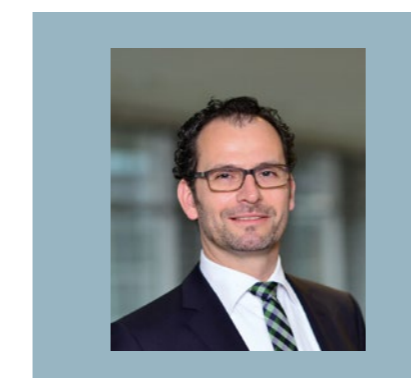
trustworthy digital economy is a complex task," says Michael Fritz, head of the central office at Fraunhofer CCIT.

### Technologies to cover the entire data value chain

Fraunhofer CCIT aims to contribute a crucial part of the solution to this challenge. As one of the few stakeholders on the market, the cluster is bringing together the latest scientific findings, know-how and problem-solving expertise along the entire data value chain. What's more, as a neutral technology supplier, it can offer an open system for all other stakeholders. Cutting across disciplinary borders, Fraunhofer CCIT combines pre-competitive research with the Fraunhofer institutes' applied research. "Users and technology institutes are working hand in hand and tackling industry-related problems together, in a manufacturing-vendor-neutral way," says Mr. Fritz. Partners and customers benefit from solutions that have a proof-of-concept maturity level, and from knowledge on how different technologies can be combined to produce a marketable overall solution. To achieve this, experts within Fraunhofer CCIT take findings from pre-competitive research that already show promise for developing products and either work with customers to adapt them to fit their applications or work with users to adapt specific technological know-how to suit their own specifications. This intensive dialogue generates highly practical solutions with

### Glossary

Every year, the **Digitalization Index** measures how industrial digitalization is progressing in Germany on the basis of 37 indicators.



### Contact

**Michael Fritz**  
 Head of central office, Fraunhofer Cluster of Excellence Cognitive Internet Technologies CCIT  
 Phone +49 89 3229986-1026  
 michael.fritz@aisec.fraunhofer.de

clearly defined added value. Some examples from 2022 include the cognitive T-slot, Smart Intersection and the Smart Screw Connection.

### The journey to the edge-cloud continuum

"In 2022, we have seen the trend of increased cloud usage continue, along with a rise in demand for cybersecurity and for voice assistant systems in the industrial sector. This trend will continue in 2023," says Mr. Fritz. For this reason, the cluster wants to drive progress in the area of the edge-cloud continuum in 2023. This relatively new term describes an end-to-end data value chain covering everything from sensors to edge devices through to cloud platforms. The continuum can be understood as an intelligent, distributed management software in which the processing of data is automated in such a way that the objectives set by customers, such as a low carbon footprint or a high degree of security, can be implemented in a consistent and traceable way. "As well as conducting potential analyses, we bring together the relevant stakeholders, identify the areas that require further research and define specific use cases," says Mr. Fritz.

### Projects

The **cognitive T-slot smartNOTCH** increases the efficiency of forming machines through the cognitive transformation of industrial processes.



The **Smart Intersection** uses an innovative sensor system that can consolidate and analyze traffic data at any point along the roads through an AI-based method that complies with data protection law.



The **Smart Screw Connection** can be monitored remotely at all times; this increases safety and lowers the level of inspection effort required.





## Thomas Caspers

### Director, German Federal Office for Information Security (BSI)

#### What topics did the BSI focus on in 2022, and why? Where will your attention lie in 2023?

The cyberspace threats the BSI faced in 2022 were greater than ever before. The most serious risk to the secure operation of IT infrastructures was ransomware, particularly for companies. Other new threats arose in connection with Russia's war of aggression against Ukraine, which needed to be effectively combated. 2023 is set to bring technological developments with disruptive potential that will challenge everyone that must create comprehensive, practical IT security solutions, as the BSI does. The BSI is working intensively in areas such as artificial intelligence, cryptography and quantum computing with world-leading research institutions to solve societal and political issues associated with IT security; quite rightly, there are high expectations here.

#### What topics did you work on with Fraunhofer AISEC in 2022, and what is on the agenda for 2023?

In 2022, our focus was on hardware security for microcontrollers, which are widely used in the industry. Certified chips offer a very high level of security. However, many sectors use commercially available chips that cannot withstand hardware-based attacks.

One example that stands out from 2022 was the hacking of the Starlink system — that could have potentially had very serious consequences. Together with Fraunhofer AISEC, the BSI carried out a study to find attack paths that can be used against microcontrollers, along with countermeasures that can be implemented to deal with them. Even if these countermeasures do not prevent attacks entirely, they can still make them so much more difficult for the attacker that making the attempt is no longer an attractive option.

System-on-a-chip systems (SoCs) [see glossary] follow the industry trend toward higher levels of integration. Instead of being on separate chips, security functionalities are directly integrated into the SoCs as subsystems. However, due to their high levels of complexity, integrating these functionalities is no easy feat. In 2023, the BSI will be working with Fraunhofer AISEC to determine whether we can still assume the same level of security of a subsystem after integration, which security vulnerabilities may potentially occur and how we can counter them.

#### What made you choose Fraunhofer AISEC as a partner?

Apart from the fact that this partnership meets our financial viability requirements, our main reason for collaborating with Fraunhofer AISEC is its high level of specialist expertise in the area of hardware security — as demonstrated by its numerous scientific publications, for example. It is especially important to the BSI that the resulting findings are more than just basic research — they need to have clear practical relevance, so that they can be incorporated directly into the BSI's technical work. Fraunhofer AISEC has an extensive range of technical equipment that means it can always carry out very challenging preparation and analysis work in the area of chip security, and that is a critical factor for the BSI's success.

**Thomas Caspers is head of division Technical Centers of Excellence and director of the German Federal Office for Information Security (BSI).**

#### Glossary

*In a system on a chip or monolithic integrated circuit, all or the majority of the functions of a programmable electronic system are built onto a chip.*



## Dirk Kretzschmar

### Managing director, TÜV Informationstechnik GmbH (TÜViT)

#### In your opinion, where do the greatest IT security challenges lie at the moment?

There are currently countless major challenges in IT security that are influenced by different factors. These include cybercriminals becoming increasingly professional and specialized, to the extent that they divide work up between themselves. Attackers have extensive customized services at their disposal on the dark web, so they themselves are not necessarily the experts exploiting vulnerabilities any more. This means there are more and more unscrupulous new criminals on the scene; these individuals just want to benefit financially with very little risk.

In my opinion, the biggest challenge is that too many C-suite executives are unaware of their own responsibilities — and because they can't imagine the risks, they doubt they even exist. Many simply don't know that cybercriminals gain access months before they start their attacks.

#### Where do you believe there is need for action to increase the reliability and security of AI systems?

I don't believe it's enough to just rely on established AI development processes, the associated training data and purely functional tests. Many people feel uneasy about letting AI take the wheel, so to speak. Their main concerns are that they will lose control and that the AI solutions will behave unpredictably.

However, there is also the fact that AI solutions can be deliberately misled. Their decisions can be manipulated in one direction or another, which can lead to catastrophic consequences in sensitive, critical application scenarios. Of course, that is also an IT security matter — preventing vulnerabilities from being exploited in the AI. The technical term for this is "adversarial attacks." Special stress tests can be used to examine AI solutions' resilience against these types of attacks and determine their robustness in certain application scenarios. So I think there is a need for action when it comes to the mandatory testing of AI solutions in sensitive areas.

#### How have you and your colleagues found your collaboration with Fraunhofer AISEC?

For a long time now, TÜViT has been successfully working with Fraunhofer AISEC in the field of cybersecurity. Fraunhofer AISEC is a renowned institute for applied research in the IT security sector. The expertise and experience that the institute has in this area are highly regarded, and utilized by many companies and institutes across the world.

The challenge for us is developing suitable, reliable testing processes for IT security, particularly for new technologies that have come on the market. We cannot do that without extensive research, but TÜViT is not in a position to act as a test site for research. Our collaboration with Fraunhofer AISEC means we can use their research findings to improve IT security testing in many sectors and areas of application. The same goes for developing a framework to test AI.

Overall, we consider our collaboration with Fraunhofer AISEC to be extremely valuable when it comes to improving IT security and minimizing risks.

**Dirk Kretzschmar is the managing director of TÜV Informationstechnik GmbH (TÜViT) and a member of the TÜV NORD GROUP executive committee.**





# Sandra Kostic

## Team lead for Usable Security & Privacy

“**Developing applications without the involvement of users creates the risk that they will not fully understand the security mechanisms and therefore will not apply them correctly. Usable security is about avoiding this eventuality when it comes to security-related applications.**”

With this as her motto, Sandra Kostic took over as the team lead for Usable Security & Privacy at Fraunhofer AISEC's Berlin location in fall 2022. The computer scientist believes the usability of applications is too seldom considered. For this reason, she and her team of five decided to systematically evaluate and promote the usability of IT-based systems and strengthen people's trust in the security of these systems.

Right from her bachelor's degree in computer science, Ms. Kostic was already forging a path toward making cybersecurity measures more user-friendly — it was at this time that she joined the ID Management working group at Freie Universität Berlin under Prof. Marian Margraf. Ms. Kostic has many varied interests, and she finds that user-oriented IT security research combines the pragmatic technology approach of computer science with the creativity of design while also providing insights into diverse fields. User-friendliness and usable security are needed everywhere, after all — from hardware, such as a simple remote control, to a smart TV in a smart home through to complex applications with very high security requirements, such as those that deal with sensitive digital patient data. As soon as an interaction with a user is foreseen during application design, it is time for this Berlin native to step in with her expertise on users' needs, knowledge and abilities.

### Practical research into secure digital identities

The researcher had the opportunity to apply her knowledge to specific solutions at Fraunhofer AISEC when she took over as head of the ONCE project in 2020. Building on her master's degree in computer science and her research experience in the area of digital identities at FU Berlin, she worked with the institute's partners to develop secure, user-friendly wallet solutions that enable members of the public to store various

identification documents, such as their ID card, driver's license, tickets and loyalty cards, on their smartphones. This allowed the users to provide digital proof of identity in a secure manner.

The key to Ms. Kostic's success with these kinds of applications is the way she takes the users' perspectives into account and brings her usable security expertise to bear right from the earliest design phase. The terminology used and the user interface's design, as well as the interaction flow, dictate whether users or programmers will trust the application and use it in such a way that its security features will be effective. Ms. Kostic is supported in this endeavor by her qualifications in graphic design, user interfaces (UI) and user experience (UX) from the California Institute of the Arts, which she obtained during her time at Fraunhofer AISEC.

She is writing her doctorate on what exactly it is that makes users trust the security of an application. In 2022, Ms. Kostic represented Fraunhofer AISEC by presenting her publications at renowned scientific conferences such as the Symposium on Usable Privacy and Security (SOUPS) and networked with experts in privacy and usable security from around the world. In her role as team leader too, she still prioritizes applied research. With her team of experts from the fields of usable security and machine learning, she hopes to integrate the topics of privacy and trust more fully into the domain of machine learning and artificial intelligence. She also takes a pragmatic approach that helps users directly, for example, by assisting them in understanding how AI systems process their data.



# Michael Heini

## Research scientist in the Product Protection and Industrial Security department

“ Looking at a problem from different perspectives and taking an unbiased approach to solving it — that’s my method for achieving long-term success.”

Michael Heini began his professional career by training as an information technology officer and then worked in that field as a network and system administrator for an automotive supplier. Students from university regularly came to the company for work experience and they would talk about their studies. These interactions made Mr. Heini more and more interested in studying at university. However, without his high-school diploma, that path was closed off to him at the time. So he reduced his hours to part-time and dedicated himself to getting his high-school diploma by attending night school.

### Visiting the USA and Israel

Right after attaining his diploma, he began studying for his bachelor’s degree in enterprise and IT security at the Offenburg University of Applied Sciences. Wanting to broaden his range of specialist expertise, he then obtained a master’s degree in computer science with a minor in philosophy from Ulm University. As his heart was still set on IT security, he spent a year on a Fulbright scholarship at George Mason University (Virginia, USA), studying for his master’s in information security and assurance.

Mr. Heini first came into contact with Fraunhofer in 2017 through the Hessian Israel Partnership Accelerator program, which involved spending time working both at Fraunhofer SIT and at the Hebrew University of Jerusalem in Israel. The topic of his

master’s thesis, which focused on developing a metric for evaluating certificate authority trustworthiness in public key infrastructures (PKIs), finally brought him to Fraunhofer AISEC.

### Working toward a doctorate

Mr. Heini was particularly interested in issues relating to the trustworthiness and security of PKIs due to the diverse applications, high level of relevance in everyday life and interdisciplinarity that characterize this field. PKIs are also a key element of Product Protection and Industrial Security, and as a research scientist in this department, Mr. Heini often deals with them in projects. He remains open to all possible solutions when tackling problems, considering them from different perspectives. “I want to understand technologies and their effects before I use them,” the scientist says. He also passes this approach on to students through his work as a doctoral student at the Technical University of Munich (TUM) and as a lecturer at Heilbronn University of Applied Sciences. The rapidly changing nature and complexity of the field of IT security requires a great deal of flexibility and willingness to learn. That is particularly motivating for Mr. Heini: in his doctorate project, he is working on issues from the fields of supply chain security and critical information infrastructures. He takes the scientific findings from his research and directly applies them to customer projects, thus bringing his knowledge directly into practice.





# Vivija Čepkalo-Simić

## Cybersecurity Training Lab project manager | Dual studies coordinator

One of Vivija Čepkalo-Simić's most vivid memories from her studies involves her jumping for joy in her student dorm. She had solved a challenging mathematical problem — her persistence had paid off. The rules and clarity of math had always fascinated her in particular, and led her to study mathematics at the Technical University of Munich (TUM). She discovered her interest in cryptography toward the end of her studies. She then specialized in the mathematical aspects of cryptography at the Queensland University of Technology (Brisbane, Australia) and at the Université Toulouse III — Paul Sabatier (Toulouse, France), where she began writing her thesis. There, she focused on Edwards curves, a special form of elliptic curves, and their application in the encryption of smart cards.

With a diploma in mathematics and computer science (as a minor), she remained at university for her first years in employment — starting with the Carl von Ossietzky University of Oldenburg. Shortly afterward, she worked at TUM in the service office for computer science studies, taking over responsibility for the master's program in computer science; later, she worked in the student advisory service for the former faculty of computer science. Her first years of employment taught her important soft skills, such as how to prioritize and work strategically, how to assert herself in a male-dominated field and how to put across her own perspective in a confident way, backing it up with facts. Her most important maxim is that you need to think ahead and develop personally and professionally, and since 2018, she has been passing this principle on to her students in her role as head of academic advising (TUM Informatics).

### Fostering people's talents

"I want to keep improving myself all the time and have the freedom to make my own contributions," Ms. Čepkalo-Simić says. That is how she became aware of Fraunhofer AISEC. From her work at TUM, including as a lecturer in algebraic methods in cryptography and post-quantum algorithms in the Information Technology faculty, it was no surprise that she landed in the office of Prof. Claudia Eckert, Chair of Security in Information Technology at TUM and managing director of Fraunhofer AISEC. An easy, open conversation on the subject of development opportunities at Fraunhofer AISEC came about spontaneously — Ms. Čepkalo-Simić was especially enthusiastic about the appreciation and care the institute director showed for her colleagues.

Since 2019, Ms. Čepkalo-Simić has been project manager for the Cybersecurity Training Lab at Fraunhofer AISEC. Her goal is to help customers from industry and the public sector to become more resilient in the area of IT security by means of training courses tailored to their individual needs. Through resources for lifelong learning and professional further development, she supports companies and public authorities in combating the financial and security-critical challenges they face today. She is helped in this by her people skills and passion for encouraging others to strengthen their skills — something she's very good at. In 2022, the Cybersecurity Training Lab exceeded its expected revenue by 50 percent.



**I need to learn and test myself. Because it's only through exploration and improvement that we can grow and tackle challenges."**





# Philip Sperl

## Co-director of the Cognitive Security Technologies department

Together with Dr. Konstantin Böttinger, Philip Sperl heads up the Cognitive Security Technologies department at Fraunhofer AISEC, which specializes in artificial intelligence. During the early years of his career, the electrical engineer and computer scientist took on various roles within the institute, including being a bachelor's and master's student and a research scientist.

He first came to Fraunhofer AISEC in 2015 to write his bachelor's thesis. His focus was on investigating error attacks on embedded systems. Having acquired a taste for applied research, he stayed at Fraunhofer AISEC in the Hardware Security department while studying for his master's degree at the Technical University of Munich (TUM), working as a research assistant for side-channel analysis. As he had made great connections and was open to researching many different IT security topics, Mr. Sperl decided to write an interdisciplinary master's thesis that paired hardware security with machine learning at Fraunhofer AISEC. The interdisciplinary, overarching topics that form the focus points for this young institute encouraged Mr. Sperl to stay loyal to applied IT security research even after he had finished his studies. As a research scientist in the Cognitive Security Technologies department, he took another step toward computer science and machine learning. Four years later, he progressed to the role of co-head of the department.

### An open mind and bundles of curiosity

The fact that Mr. Sperl's office is now right

next to the Hardware Security department is almost symbolic, as his research interests still span across multiple disciplines. He also values this quality in his team: His colleagues have degrees in mathematics, computer science, electrical engineering and physics. Together, they develop solutions that use AI methods to improve IT security and ensure the reliability of AI algorithms. Mr. Sperl believes that the team's diversity helps them consider problems from the right perspective and create cutting-edge solutions that offer practical help to partners and customers.

His doctoral project in computer science has proven the practical nature of his research. In this project, titled "Defending Neural Networks with Activation Analysis," he developed mechanisms to prevent attacks on AI systems that can be used for applications such as reliable object recognition in autonomous vehicles. Although he doesn't miss all the soldering he had to do as a student, Mr. Sperl has retained a hands-on mentality in his management role, and still supervises students' theses and publishes work on AI-driven anomaly detection and adversarial attacks (targeted attempts to use manipulated material to cause an AI system to break down).

The Munich-born scientist believes research is essential for shaping the sector's development and being better able to meet customers' needs. His team's goal is to carry out applied research that creates real added value for industry and society.



**The topic of AI is only going to become more important in the field of IT security. We are going to help shape this development, and are in the best possible position to tackle the challenges that will come with it."**



# Quantum computing — It's time to take the leap

Quantum computers are not very powerful yet. However, quantum computing (QC) holds enormous potential for solving specific issues such as optimization problems that cannot effectively be solved with today's computers due to the computation time required. Fraunhofer AISEC is carrying out crucial preparatory work for bringing QC securely into application.

In 2022, the most powerful quantum processor in the world had 433 qubits. In contrast to a bit, a qubit can not only be in a state of 1 or 0, but also in both states at the same time. This is called superposition and it is the reason why quantum-based computers are generating so much hype. Because if there is one thing you can count on, it is that many qubits in superposition result in an exponentially large number of states. This means quantum computers are able to solve specific mathematical problems more quickly and efficiently than a conventional computer ever could. "The hope is that QC will massively improve machine learning, which is key to every kind of artificial intelligence," says Pascal Debus, head of the Quantum Security Technologies group in the Cognitive Security Technologies department at Fraunhofer AISEC.

## Conventional encryption processes under threat

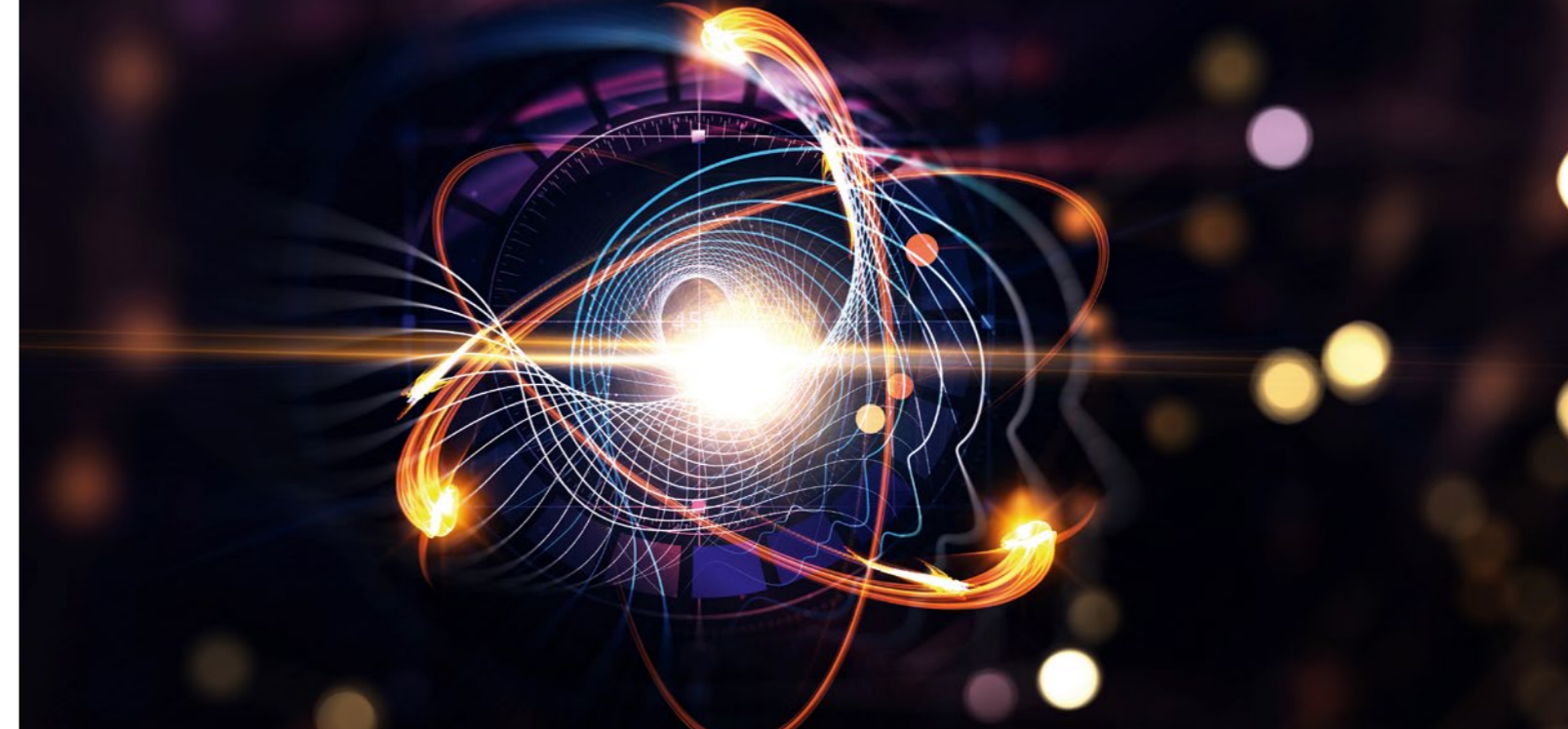
From a cybersecurity perspective, the outlook on the quantum era is less optimistic. Due to their computing power, quantum computers pose a threat to conventional encryption processes. These are often based on practically "unsolvable" mathematical computational problem, such as factorization problems [see glossary]. Quantum computers can solve these problems more quickly. For this reason, research into cybersecurity has been focused on the topic of post-quantum cryptography for a number of years already. Fraunhofer AISEC has established the Competence Center for Post-Quantum Cryptography to carry out this research (see page 20). However, at a second glance, it becomes apparent that quantum computers also create opportunities for cybersecurity. They can solve the verification problem in software development and help with anomaly detection in IT systems, to give two examples.

## QC algorithms in application

In addition to the Competence Center for Post-Quantum Cryptography, Fraunhofer AISEC is also involved with pre-competitive research into QC. At Munich Quantum Valley (MQV), experts are using QC-based machine learning for applications such as detecting fraud in the finance sector, developing secure software libraries to make it easier for even non-experts to create QC programs, and investigating how QC can be put into application while complying with data protection regulations. At the Bavarian Competence Center for Quantum Security and Data Science (BayQS), Fraunhofer AISEC is identifying the quantum benefits in regard to solving software issues, and is working to minimize the risks that arise concerning intellectual property. In the Quantum-enabling services and tools for industrial applications (QuaST) project, researchers are developing solutions and tools based on quantum computing that can be used for conventional software verification. "Because it won't stay at 433 qubits in the medium term," says Mr. Debus.

## Glossary

**Factorization problems** involve breaking a given number down into a product of prime factors.



## Projects

### Competence Center for Post-Quantum Cryptography

At the Competence Center for Post-Quantum Cryptography, scientists are researching quantum-resistant cryptography processes and crypto-agility.

### MQV

At MQV (Munich Quantum Valley), researchers are developing QC-based machine learning for fraud detection, software libraries for QC programming and QC methods that comply with data protection regulations.

### BayQS

At BayQS (Bavarian Competence Center for Quantum Security and Data Science), researchers are working to identify the advantages that quantum methods offer for software applications and minimize the risks they present regarding intellectual property.

### QuaST

In the QuaST project (Quantum-enabling services and tools for industrial applications), researchers are developing solutions and tools based on quantum computing that can be used for conventional software verification.



## Contact

### Pascal Debus

Team lead for Quantum Security Technologies  
Cognitive Security Technologies department  
Phone +49 89 3229986-180  
pascal.debus@aisec.fraunhofer.de



Competence Center for  
Post-Quantum Cryptography



MQV



BayQS  
(in German)



QuaST  
(in German)





# Cybersecurity for 6G

**While we are still working on achieving nationwide 5G coverage in Germany, the industrial and scientific sectors are paving the way for the next mobile communications standard — 6G. In the 6G-ANNA project funded by the German Federal Ministry of Education and Research (BMBF), Fraunhofer AISEC is bringing its cybersecurity expertise to the table.**

The new mobile communications standard 6G is expected to be launched on the market around 2030. It promises higher data rates, faster response times and improved location accuracy. This makes 6G an appealing prospect for specific applications such as remote-controlled robots and autonomous vehicles. To develop the technologies needed for this and build up a 6G infrastructure, technology hubs and universities have been setting up 6G test sites for several years now. The industrial and the scientific sectors are also working closely together on 6G. For example, 29 companies and research institutions are collaborating on the 6G-Access, Network of Networks, Automation & Simplification (6G-ANNA) research project. Fraunhofer AISEC is contributing its cybersecurity expertise in the fields of confidential computing and code analysis here. The goal is to set up a shared 6G infrastructure that is more powerful, sustainable and trustworthy than the 5G network.

One focus of Fraunhofer AISEC's research work is the area of confidential computing. This expression is used to describe

technologies that ensure the confidentiality and integrity of data when it is transmitted, processed and stored.

### Confidential computing with GyroidOS

The key to this is the secure container virtualization [see glossary] GyroidOS, which was developed by Fraunhofer AISEC based on the open-source operating system Linux. "GyroidOS protects the integrity, authenticity and trustworthiness of the data in the virtualized container. This is how we can bring confidential computing to future 6G architectures. These architectures will have a modular design, which means they will offer more attack surfaces," says Sascha Wessel, head of the Secure Operating Systems department at Fraunhofer AISEC.

### Automated code analysis for network software

Another Fraunhofer AISEC technology being used in 6G-ANNA is the code analysis tool Codyze. Codyze checks whether software complies with the applicable regulations for secure

communication, encryption, compliance and certification. Automated security checks shorten the development cycles for software.

### Glossary

*Virtualization refers to an abstraction from physical IT resources such as hardware, software, storage and network components.*

"In 6G-ANNA, we're using Codyze as a static code analysis tool to check software components in 6G networks for compliance with relevant standards and guidelines", says Christian Banse, head of the Service and Application Security department at Fraunhofer AISEC.

## Projects

### 6G-ANNA

6G-ANNA was launched in 2022 and will run until 2025. The German Federal Ministry of Education and Research (BMBF) is providing 38.4 million euros in funding for this project.

### GyroidOS

The secure container virtualization GyroidOS uses internal functions of the open-source operating system Linux to run applications on the same host system in isolation from each other.

### Codyze

The code analysis tool Codyze automatically checks software for compliance with the applicable security regulations. Codyze will be expanded for 6G-ANNA to allow for analysis of programming languages that are relevant to 6G, and for areas of application outside of secure encryption.



### Contact

#### Sascha Wessel

Head of the Secure Operating Systems department  
Phone +49 89 3229986-155  
sascha.wessel@aisec.fraunhofer.de



#### Christian Banse

Head of the Service and Application Security department  
Phone +49 89 3229986-119  
christian.banse@aisec.fraunhofer.de



6G-ANNA



GyroidOS



Codyze



# Publications

Antoine d'Aligny, Emmanuel Benoist, Florian Dold, Christian Grothoff, Özgür Kesim, Martin Schanzenbach: »Who comes after us? The correct mindset for designing a Central Bank Digital Currency«. In: SUERF Policy Note 279 (2022).

Daniel Angermeier, Hannah Wester, Kristian Beilke, Gerhard Hansch, Jörn Eichler: »Security Risk Assessments: Modeling and Risk Level Propagation«. In: ACM Transactions on Cyber-Physical Systems. 2022.

Ahmed Alqattaa, Daniel Loebenberger, Lukas Moeges: »Analyzing the Latency of QUIC over an IoT Gateway«. In: IEEE International Conference on Omnilayer Intelligent Systems, COINS 2022, Barcelona, Spain, August 13, 2022. IEEE, 2022, pp. 1–6. DOI: 10.1109/COINS54846.2022.9854951.

Oliver Braunsdorf, Stefan Sessinghaus, Julian Horsch: »Compiler-based Attack Origin Tracking with Dynamic Taint Analysis«. In: Information security and cryptology - ICISC 2021 (2022). DOI 10.1007/978-3-031-08896-4\_9.

Manuel Brosch, Matthias Probst, Georg Sigl: »Counteract Side-Channel Analysis of Neural Networks by Shuffling«. In: Design, Automation & Test in Europe Conference & Exhibition, DATE 2022. Proceedings (2022). DOI 10.23919/DATE54114.2022.9774710.

Shanatip Choosaksakunwiboon, Karla Pizzi, Ching-Yu Kao: »Comparing Unsupervised Detection Algorithms for Audio Adversarial Examples«. In: International Conference on Speech and Computer (pp. 114-127). Springer, Cham. (2022).

Adam Dziedzic, Haonan Duan, Muhammad Ahmad Kaleem, Nikita Dhawan, Jonas Guan, Yannis Cattan, Franziska Boenisch, Nicolas Papernot: »Dataset inference for self-supervised models.« arXiv e-prints, pages arXiv-2209, NeurIPS'22. 2022.

Armando Miguel Garcia, Matthias Hiller: »Lightweight Authentication and Encryption for Online Monitoring in IIoT Environments«. In: International Symposium on Foundations and Practice of Security 2021 (2022). DOI 10.1007/978-3-031-08147-7\_17.

Mathieu Gross, Nisha Jacob, Andreas Zankl, Georg Sigl: »Breaking TrustZone memory isolation and secure boot through malicious hardware on a modern FPGA-SoC«. In: Journal of cryptographic engineering (2022). DOI 10.1007/s13389-021-00273-8.

Jan Dennis Gumz, Simon Sebastian Hunt, Michael Stemmer, Sebastian Bock, Nikolay Vassiley Tcholtchev, Denny Mattern, Adrian Paschke, Marian Margraf: »Quanten-IKT. Quantencomputing und Quantenkommunikation.« (2022).

Michael P. Heidl, Simon Gözl, Christoph Bösch: »Remote Electronic Voting in Uncontrolled Environments: A Classifying Survey«. In: ACM Comput. Surv. (2022). Just Accepted. ISSN: 03600300. DOI: 10.1145/3551386.

Alexander Hepp, Johanna Baehr, Georg Sigl: »Golden Model-Free Hardware Trojan Detection by Classification of Netlist Module Graphs«. In: Design, Automation & Test in Europe Conference & Exhibition, DATE 2022. Proceedings (2022). DOI 10.23919/DATE54114.2022.9774760.

Julius Hermelink, Silvan Streit, Emanuele Strieder, Katharina Thieme: »Adapting Belief Propagation to Counter Shuffling of NTTs«. In: IACR Transactions on Cryptographic Hardware and Embedded Systems 2023.1 (2022), 60–88. DOI: 10.46586/tches.v2023.i1.60-88.

Stefan Hristozov, Moritz Wettermann, Manuel Huber: »A TOCTOU Attack on DICE Attestation«. In: CODASPY 2022, Twelfth ACM Conference on Data and Application Security and Privacy. Proceedings (2022). DOI: 10.1145/3508398.3511507.

Monika Huber, Sascha Wessel, Gerd Brost, Nadja Menz: »Building Trust in Data Spaces«. In: Designing Data Spaces (2022). DOI: 10.1007/978-3-030-93975-5\_9; DOI: 10.24406/publica-654

Ching-Yu Kao, Junhao Chen, Karla Pizzi, Konstantin Böttinger: »Rectifying adversarial inputs using XAI Techniques.« In: Proceedings of the European Association for Signal Processing 2022 (EURASIP 2022).

Ching-Yu Kao, Hongjia Wan, Karla Pizzi, Konstantin Böttinger: »Real or Fake? A Practical Method for Detecting Tempered Images«. In: Proceedings of the international image processing application and systems 2022 (IPAS 2022). (Best session paper award).



Patrick Karl, Tim Fritzmann, Georg Sigl: »Hardware Accelerated FrodoKEM on RISC-V«. In: 25th International Symposium on Design and Diagnostics of Electronic Circuits and Systems, DDECS 2022. Proceedings (2022). DOI 10.1109/DDECS54261.2022.9770148.

Özgür Kesim, Christian Grothoff, Florian Dold, Martin Schanzenbach: »Zero-Knowledge Age Restriction for GNU Taler«. In: Proceedings of 27rd European Symposium on Research in Computer Security (ESORICS). Lecture Notes in Computer Science. Springer, 2022.

Sandra Kostic, Maija Poikela: »Do Users Want To Use Digital Identities? A Study Of A Concept Of An Identity Wallet«. In: SOUPS 22. 2022.

Alexander Küchler, Christian Banse: »Representing LLVM-IR in a Code Property Graph«. In: Information Security. Ed. by Willy Susilo, Xiaofeng Chen, Fuchun Guo, Yudi Zhang, and Rolly Intan. ISC '22. Springer, 2022, pp. 360–380.

Immanuel Kunz, Andreas Binder: »Application-Oriented Selection of Privacy Enhancing Technologies«. In: Annual Privacy Forum. Springer. 2022, pp. 75–87.

Immanuel Kunz, Angelika Schneider, Christian Banse, Konrad Weiss, Andreas Binder: »Poster: Patient Community – A Test Bed for Privacy Threat Analysis«. In: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. CCS '22. 2022. DOI: 10.1145/3548606.3564253.

Immanuel Kunz, Angelika Schneider, Christian Banse: »A Continuous Risk Assessment Methodology for Cloud Infrastructures«. In: 2022 22nd IEEE International Symposium on Cluster, Cloud and Internet Computing (CCGrid). IEEE. 2022, pp. 1042–1051.

Florian Lauf, Marcel Klöttgen, Hendrik Meyer zum Felde, Robin Brandstädter: »Donating Medical Data as a Patient Sovereignty: A Technical Approach«. In: 15th International Conference on Health Informatics (HEALTHINF 2022). 2022.

Christopher Mühl, Franziska Boenisch: »Personalized pate: Differential privacy for machine learning with individual privacy guarantees«. In: PoPETs'23. 2022.

Nicolas M. Müller, Pavel Czempin, Franziska Dieckmann, Froghyar Adam, Konstantin Böttinger: »Does Audio Deepfake Detection Generalize?«. In: Interspeech (2022).

Nicolas M. Müller, Franziska Dieckmann, Jennifer Williams: »Attacker Attribution of Audio Deepfakes«. In: Interspeech (2022).

Nicolas M. Müller, Karla Markert, Konstantin Böttinger: »Human Perception of Audio Deepfakes«. ACM Multimedia (2022).

Jannis Priesnitz, Rolf Huesmann, Christian Rathgeb, Nicolas Buchmann, Christoph Busch: »Mobile Contactless Fingerprint Recognition: Implementation, Performance and Usability Aspects«. In: Sensors. Online journal (2022). DOI 10.3390/s22030792.

Maximilian Richter, Magdalena Bertram, Jasper Seidensticker, Alexander Tschache: »A Mathematical Perspective on Post-Quantum Cryptography.« In: Mathematics 10, no. 15: 2579. 2022.

Paul Andrei Sava, Jan-Philipp Schulze, Philip Sperl, Konstantin Böttinger: »Assessing the Impact of Transformations on Physical Adversarial Attacks«. In: Proceedings of the 15th ACM Workshop on Artificial Intelligence and Security (AISec 2022).

Jan-Philipp Schulze, Philip Sperl, Konstantin Böttinger: »Double-Adversarial Activation Anomaly Detection: Adversarial Autoencoders are Anomaly Generators.« In: International Joint Conference on Neural Networks (IJCNN 2022).

Jan-Philipp Schulze, Philip Sperl, Konstantin Böttinger: »Anomaly Detection by Recombining Gated Unsupervised Experts.« In: International Joint Conference on Neural Networks (IJCNN 2022).

Jan-Philipp Schulze, Philip Sperl, Radutoiu, A., Sagebiel, C., Konstantin Böttinger: »R2-AD2: Detecting Anomalies by Analysing the Raw Gradient.« In: European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML-PKDD 2022).

Bodo Selmk, Maximilian Pollanka, Andreas Duensing, Emanuele Strieder, Hayden Wen, Michael Mittermair, Reinhard Kienberger, Georg Sigl: »On the application of Two-Photon Absorption for Laser Fault Injection attacks Pushing the physical boundaries for Laser-based Fault Injection«. In: IACR Trans. Cryptogr. Hardw. Embed. Syst. 2022.4 (2022), pp. 862–885. DOI: 10.46586/tches.v2022.i4.862-885.

Bodo Selmk, Emanuele Strieder, Johann Heyszl, S. Freud., T. Damm: »Breaking Black Box Crypto-Devices Using Laser Fault Injection«. In: Foundations and practice of security. 14th International Symposium, FPS 2021 (2022). DOI 10.1007/978-3-031-08147-7\_6.

Alexander Wagner, Felix Oberhansl, Marc Schink: »To Be, or Not to Be Stateful: Post-Quantum Secure Boot using Hash-Based Signatures«. In: Proceedings of the 2022 Workshop on Attacks and Solutions in Hardware Security (2022), pp. 85-94.

Konrad Weiss, Christian Banse: »A Language Independent Analysis Platform for Source Code.« (2022). arXiv: 2203.08424 [cs.CR]. DOI 10.48550/arXiv.2203.08424.

Felix Wruck, Vasil Sarafov, Florian Ralph Jakobsmeier, Michael Weiß: »GyroidOS: Packaging Linux with a Minimal Surface«. In: SaT-CPS 2022, ACM Workshop on Secure and Trustworthy Cyber-Physical Systems. Proceedings (2022). DOI 10.1145/3510547.3517917.



# Publishing Notes

## Published by

Fraunhofer Institute for Applied  
and Integrated Security AISEC  
Prof. Claudia Eckert  
Prof. Georg Sigl

Lichtenbergstr. 11  
85748 Garching near Munich  
Phone +49 89 3229986-0  
www.aisec.fraunhofer.de/en.html

## Editor

Maria Schwab-Kloe, Wiebke Ramm, Ramona Ursic,  
Tobias Steinhäuber (lead editor)

## Editorial assistance

Andreas Kunkel

## Layout

Maria Schwab-Kloe

## Graphics

Daniela Miedaner

## Printed by

Flyeralarm GmbH

## Contact

Fraunhofer Institute for Applied  
and Integrated Security AISEC  
Lichtenbergstr. 11  
85748 Garching near Munich  
Phone +49-89-3229986-170  
marketing@aisec.fraunhofer.de

## Photo acknowledgments

Cover image: HGEsch  
Page 4: Bernd Müller, Andreas Heddergott  
Pages 8/9: Oliver Bodmer  
Page 11: Bernd Müller, Andreas Heddergott  
Pages 12/13: Oliver Bodmer  
Page 14: Oliver Bodmer  
Page 15: Andreas Heddergott  
Pages 16/17: Freepik/@kanawatTH  
Pages 18/19: Andreas Heddergott  
Pages 20/21: Adobe/agsandrew  
Page 22: Fraunhofer AISEC  
Page 23: AllEyesOnYou.de, Oliver Bodmer  
Pages 24/25: Oliver Bodmer

Pages 26/27: Oliver Bodmer  
Pages 28/29: Oliver Bodmer  
Page 30: Fraunhofer AISEC  
Page 31: Andreas Heddergott  
Page 32: Adobe Stock  
Page 33: Merck/Thomas Pirot for manager magazine  
Page 34: HGEsch  
Page 35: Daniela Miedaner (graphic)  
Pages 36/37: Daniela Miedaner (graphic)  
Pages 38/39: Daniela Miedaner (graphic)  
Page 40: Andreas Heddergott/TUM, Oliver Rösler,  
Adam Bacher, Bundesdruckerei GmbH, Rene Bertrand,  
Bundesdruckerei GmbH  
Page 41: Werner Bartsch; Bavarian Ministry of Economic  
Affairs, Regional Development and Energy; Hessian.AI  
Page 42: Fraunhofer CCIT  
Page 43: Fraunhofer-Gesellschaft  
Page 44: Claudia Grosser  
Page 45: Udo Geisler Photographie  
Page 46: Fraunhofer ICT Group/Sasha Marie Runge  
Page 49: Oliver Bodmer  
Page 51: Oliver Bodmer  
Page 52: Oliver Bodmer  
Page 55: Freepik/@Serg Nivens  
Page 56: Freepik  
All other photos: © Fraunhofer AISEC

All rights reserved.  
Reproduction and distribution only with the editors' approval.

© Fraunhofer Institute for Applied  
and Integrated Security AISEC  
Garching near Munich, July 2023

Follow us!



Fraunhofer AISEC  
cybersecurity blog



LinkedIn



XING



Twitter



