Fraunhofer SIRIOS

Fraunhofer Center for the Security of Socio-Technical Systems SIRIOS

Fraunhofer SIRIOS

Greater public safety and security through simulation of urban infrastructures

Prof. Dr. Stefan Hiermaier, Institute Director of Fraunhofer EMI

Prof. Manfred Hauswirth, Executive Director of Fraunhofer FOKUS

Prof. Jürgen Beyerer, Institute Director of Fraunhofer IOSB

Prof. Matthias Klingner, Institute Director of Fraunhofer IVI

Combined Fraunhofer competencies

Based in Berlin, the Fraunhofer Center for the Security of Socio-Technical Systems SIRIOS brings together the experience and expertise of four Fraunhofer Institutes specializing in public safety and security. Through this cross-institutional cooperation housed at one central location with a unique infrastructure, new synergies are created to meet present-day challenges.

Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institut, EMI www.emi.fraunhofer.de/en.html

Fraunhofer Institute for Open Communication Systems FOKUS
www.fokus.fraunhofer.de/en

Fraunhofer Institute for Optronics, System Technologies and Image Exploitation IOSB
www.iosb.fraunhofer.de/en.html

Fraunhofer Institute for Transport and Infrastructure Systems IVI
www.ivi.fraunhofer.de/en.html

Introduction

How safe are we?

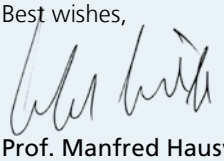
Maintaining public safety and security is one of the great challenges we face in the 21st century. Many of the threats that arise from both man-made and natural sources, and the manifold interrelationships that exist between people, technology and infrastructures, are difficult to understand and control. In science we talk about modern society as being a "socio-technical system". In litterally all areas of life, people and technology are highly interconnected.

As researchers working in the field of civil security, we focus on the threats and security of our society from within, addressing scenarios such as flood events that paralyze regional power and telecommunications networks, major events resulting in panic situations that are almost impossible to control, digital crimes that transcend borders – and, last but not least, the global pandemic. The effects of these are felt by everyone and demonstrate just how interconnected everything is, even in everyday life. They also show how quickly isolated incidents have the potential to develop and cascade. Consequently, public safety and security is a major and recurring theme in public and political debates. Many members of the public are also becoming increasingly concerned about perceived risks and subjective perceptions of safety, asking themselves how safe we really are.

We are noticing several opposing trends emerging in this context. Systemic challenges are becoming increasingly far-reaching, and in some cases are being met by highly specialized, isolated solutions. However, local disruptions – or shocks, as they are also called – can quickly escalate and begin to impact many other areas. This makes it incredibly difficult to accurately predict the impact of disruptions, reliably assess risks and, where possible, prevent these risks from arising. Unfortunately, the tools and resources that authorities and organizations with security tasks (the police, fire department, disaster control agencies, and so on) currently have at their disposal for defending against hazards and managing crises are often not at all adequate for systemically addressing the complex interrelationships that exist. The same applies to the private and public operators of critical infrastructures (CRITIS), such as telecommunications, energy and water supplies, and transportation. Disruptions to any of these have a direct impact on vital societal functions – and without the right measures being implemented in the right place at the right time, a local incident can quickly escalate into a major emergency.

The aim of the Fraunhofer Center for the Security of Socio-Technical Systems SIRIOS is to provide a systemic overall view of public safety and security. Using new models of urban living spaces and technical infrastructures, plus simulations based on these involving virtual and real elements, we support authorities and organizations with security tasks, as well as CRITIS, in deciding on the right measures in the right place at the right time – so that everyone can enjoy a greater level of safety and security in their lives.

Best wishes,



Prof. Manfred Hauswirth

Spokesperson at Fraunhofer SIRIOS and Executive Director of Fraunhofer FOKUS

Fraunhofer SIRIOS in Berlin

The Fraunhofer Center for the Security of Socio-Technical Systems SIRIOS uses coupled simulations to make complex crisis scenarios manageable and to increase security and resilience in society.

Pilot projects in the development phase

- Secure supply networks and infrastructure
- Protection and response capability of emergency responders, aid workers and the population
- Interactive, virtual situation visualization
- Communication and operational efficiency

Partners and network

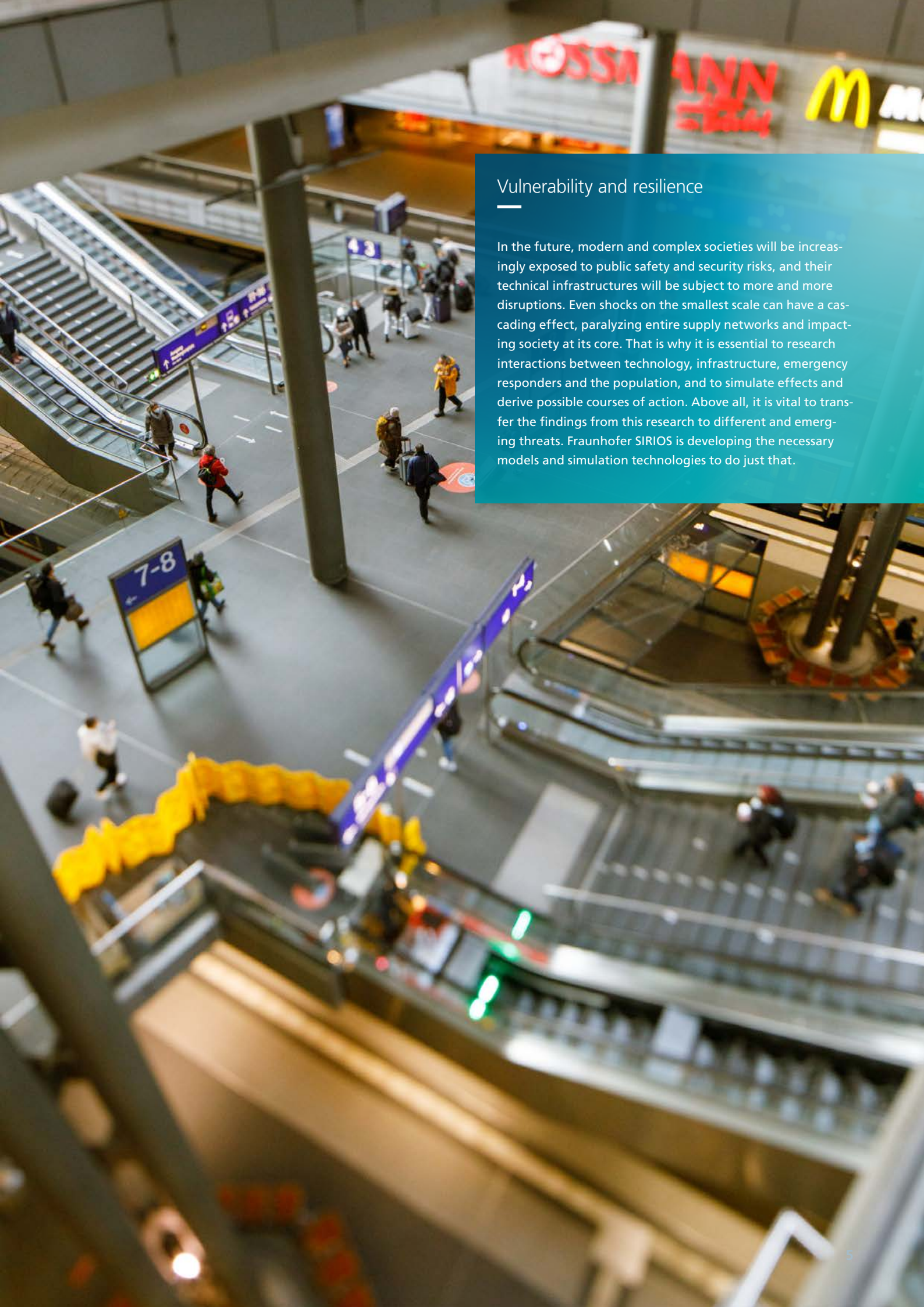
- Politics and administration
- Authorities and organizations with security tasks
- Operators of critical infrastructures (CRITIS)
- Industry and technology
- Research and development
- Associations and interest groups

Simulations for emergencies

Fraunhofer SIRIOS views itself as an incubator for new simulation-based technologies. The center brings together the expertise of different Fraunhofer Institutes at its premises in Berlin. Working on various projects, new teams develop solutions and offerings dedicated to public safety and security within five strategic areas of application: 1. digitization of security and protection of critical infrastructures (CRITIS); 2. reconnaissance, communication and operational management; 3. virtual planning and supervision of major events; 4. participation, risk and crisis communication; and 5. visualization and hybrid test environments for authorities and organizations with security tasks and CRITIS.

Particular emphasis is placed on putting research into practice, which is why the center is developing an independent partner network with stakeholder organizations from the public and private security sectors. This approach makes it possible to integrate legal framework conditions, working methods of authorities and security organizations, procedures in research and development, business models of technology companies as well as the acceptance of the general public into the scientific development process by design; that is, from the very beginning. Fraunhofer SIRIOS views scenario-based simulations as a methodology that is not restricted to a particular technology and is interdisciplinary, taking in all the stakeholders involved.

As a result, Fraunhofer SIRIOS will be able to offer comprehensive support to all its partners. As a neutral, solution-independent and scientific institution, the center is creating a collaborative environment for training and simulation based on virtual missions in two- or three-dimensional space, plus an open architecture for different systems so that vulnerabilities and technical/organizational synergies can be evaluated.



Vulnerability and resilience

In the future, modern and complex societies will be increasingly exposed to public safety and security risks, and their technical infrastructures will be subject to more and more disruptions. Even shocks on the smallest scale can have a cascading effect, paralyzing entire supply networks and impacting society at its core. That is why it is essential to research interactions between technology, infrastructure, emergency responders and the population, and to simulate effects and derive possible courses of action. Above all, it is vital to transfer the findings from this research to different and emerging threats. Fraunhofer SIRIOS is developing the necessary models and simulation technologies to do just that.

Simulation – Transfer – Impact

Fraunhofer SIRIOS views itself as an incubator for new public safety and security technologies, which is why it is developing a partner network with stakeholder organizations from the public and private security sectors. The aim of the partner network is to work together on identifying and researching relevant parameters and interdependencies in modern society. The evaluations will reveal existing security vulnerabilities and open up space for new defense and resilience strategies.

Coupled simulations and new models

Understand the emergence and impact of complex socio-technical threat or damage situations and derive scientifically substantiated measures.

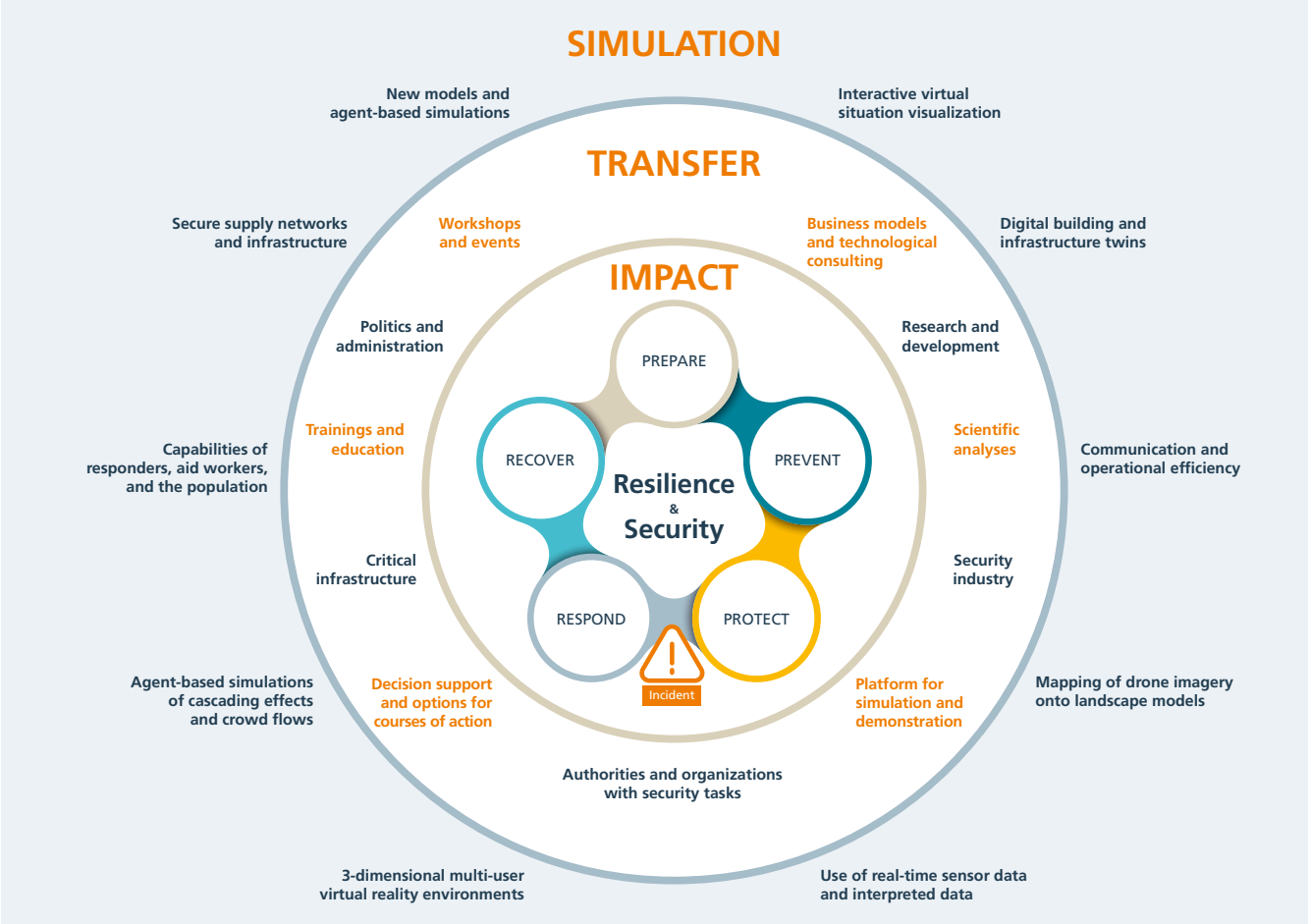
Transfer to those responsible for safety and security

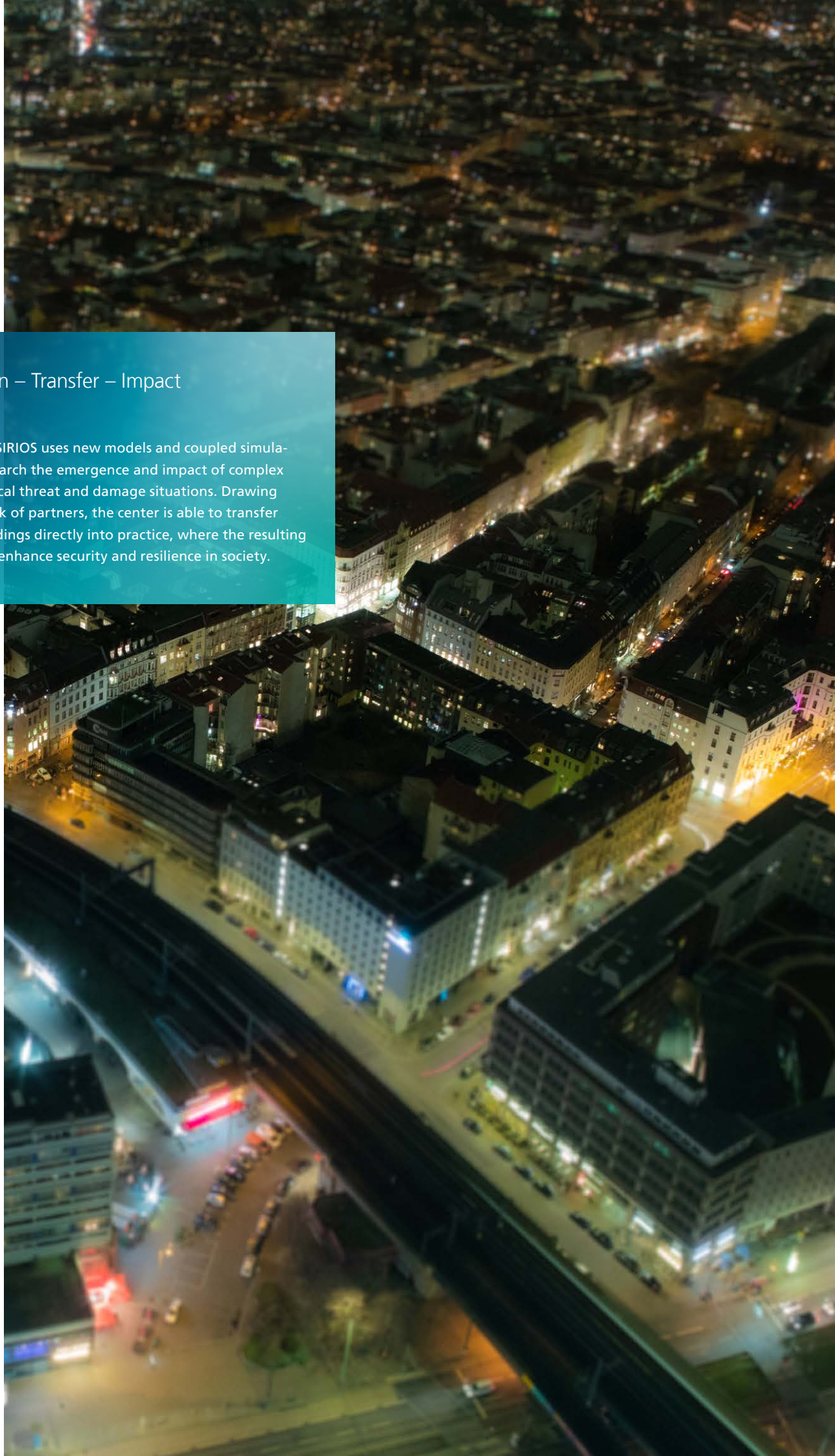
Work with stakeholders to develop solutions for interactions between technology, infrastructure, emergency responders and the population in complex situations, and put them into practice for real-life operations.

Impact on security and resilience

Support the evaluation and controllability of new technologies in the event of an emergency, ensure that data and personal rights are protected, and increase citizens' perceived sense of security.

Incubator for new public safety and security technologies: Research into interdependencies in modern society lays the groundwork for new defense and resilience strategies.





Simulation – Transfer – Impact

Fraunhofer SIRIOS uses new models and coupled simulations to research the emergence and impact of complex socio-technical threat and damage situations. Drawing on a network of partners, the center is able to transfer research findings directly into practice, where the resulting approaches enhance security and resilience in society.

Areas of application

Digitization of security and protection of critical infrastructures

Critical infrastructures (CRITIS) such as energy, water, finance and communications form the lifeblood of a society. Failures in critical infrastructure have a major impact on public safety and security. Take, for example, a power outage and mobile networks shutting down as a result over an extended period of time, or disruption to public transport due to a massive cyber-attack. CRITIS systems are becoming increasingly complex and interconnected, which in turn raises the risk of localized incidents having a huge cascading impact spanning multiple networks. The processes of planning, operating and monitoring CRITIS systems are becoming increasingly digital and internet-based. For example, digital twins representing supply networks and buildings enable different "what if" scenarios to be played out virtually, making it possible to assess their impact on specific security situations.

Reconnaissance, communication and operational management

By developing advanced procedures for data-based reconnaissance, communication and operational management, the simulation center supports emergency responders in the immediate management of complex threat situations. In view of different federal responsibilities and the fact that security forces are equipped according to country-specific or state-specific requirements, the interoperability of command and control systems is key. Interoperability refers to the ability to exchange information and data, even in heterogeneous integrated networks (data and interface compatibility). This ability has to be ensured through technical means. In addition, an overarching and decentralized (ad hoc) networking approach takes into account not only authorities and organizations with security tasks, but also all other relevant stakeholders (including public authorities, aid organizations, CRITIS operators, affected companies and the general public).

Digitization of security and protection of critical infrastructures – focal points

- Modeling and simulation of damage scenarios in coupled, interdependent infrastructure systems
- Development and use of digital building and infrastructure twins (e. g., for train stations and water supplies) to plan for safety, security and protection
- Bringing together digital city models and sensor data from buildings and infrastructures to optimize security concepts
- Coupling of sensor-based environment detection and simulation
- Development of predictive simulations for early detection of attacks and overloads

Reconnaissance, communication and operational management – focal points

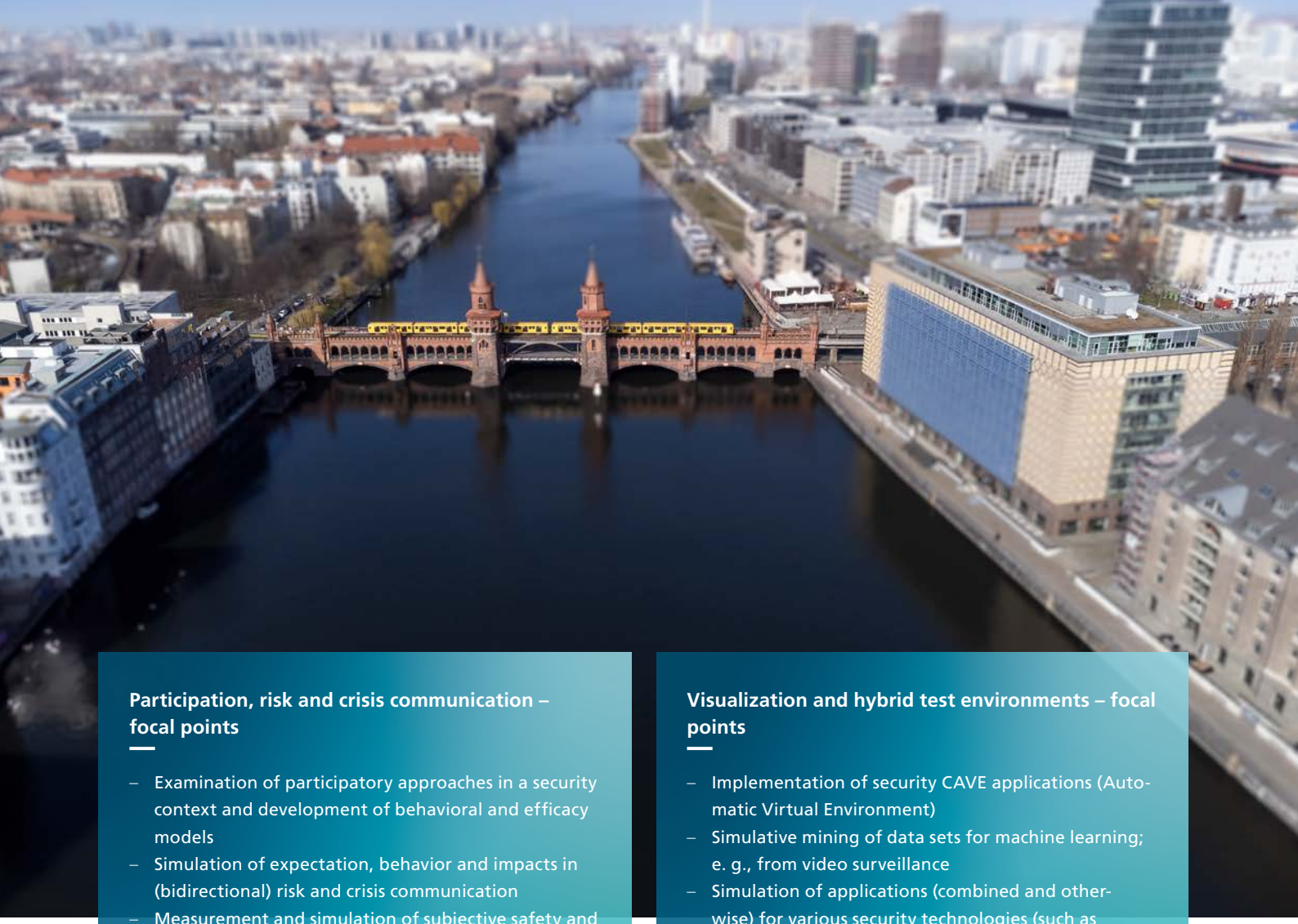
- Foundations for supporting networked and interoperable systems (e. g., for transnational and multi-agency operational management systems)
- Cybersecurity of data recording, communication and command systems
- Machine data analysis and decision support
- Models and architectures for the interoperability and decentralized (ad hoc) networking of heterogeneous systems
- Video and drone-based operational management as well as VR visualization of situations (e. g., threat situations, damage assessment)

Virtual planning and supervision of major events – focal points

- Ensuring privacy through the use of privacy enhancing technologies (e. g., anonymization, pseudonymization) in video surveillance
- Simulative support (digitized processes for planning, approval and execution)
- Simulation and monitoring of major events: in particular, recording and analysis of crowd flows (density, behavior) as well as event infrastructure
- Optimized planning of security infrastructure
- Agent-based simulation of deployment, relief and evacuation operations

Virtual planning and surveillance of major events

Major events are characterized by a multitude of potential hazards. These can be caused by human behavior (such as acts of violence, terrorism, mass shootings or panic situations involving a high density of people) or by technical disruptions (including power failures and breakdowns in communication infrastructures). Simulations can significantly assist in the process of planning, obtaining approval for and staging large-scale events, especially when it comes to the risk assessment before and during the event, the security infrastructure and targeted countermeasures should a safety or security risk occur. Due to the large number of people affected at major events, it is particularly important to focus on the protection of personal rights.



Participation, risk and crisis communication – focal points

- Examination of participatory approaches in a security context and development of behavioral and efficacy models
- Simulation of expectation, behavior and impacts in (bidirectional) risk and crisis communication
- Measurement and simulation of subjective safety and risk perception within the population
- Technologies for ad hoc communicative networking in security situations
- Privacy and security-by-design models for public acceptance of and trust in security applications that are geared towards protecting citizens

Visualization and hybrid test environments – focal points

- Implementation of security CAVE applications (Automatic Virtual Environment)
- Simulative mining of data sets for machine learning; e. g., from video surveillance
- Simulation of applications (combined and otherwise) for various security technologies (such as mobile sensor carriers, drone defense systems and bodycams)
- Interactions with target persons

Participation, risk and crisis communication

Responding to public safety and security challenges requires a participatory approach involving not only core stakeholders such as authorities and organizations with security tasks, aid organizations and CRITIS operators, but also the citizens themselves. They all have a part to play in preparing for and taking preventive measures, responding to and taking care of themselves in the event of an incident, and ultimately returning to normality. Simulations can play a crucial role in this context, especially in gaining a better understanding of interactions between communication channels (such as social media) and people's receptiveness and behavior, and in increasing the population's subjective sense of security as well as acceptance and trust in the measures designed to create it. Reliable privacy and security-by-design approaches are essential in this process.

Visualization and hybrid test environments

Modern simulations make it possible to run through deployment scenarios and explore different courses of action. Compared to purely virtual test environments, hybrid visualization and interaction techniques incorporating real elements offer a higher degree of practical relevance. For example, security CAVE applications (Automatic Virtual Environment) can be used to create artificial deployment scenarios in which it is possible to test how people interact directly with one another: These may include a terrorist attack at a main train station, mass panic at a major event, a hostage situation in the government quarter of a city, or drone attacks. Real-life security technologies, such as semi-autonomous mobile sensor carriers, are also used in these simulations and are tested for their operational suitability.

Our range of services

Fraunhofer SIRIOS provides a neutral and collaborative space in which all parties can come together to exchange ideas in a spirit of partnership. In this transfer network, we collaborate with experts from authorities and organizations with security tasks, CRITIS and the security industry to develop scientifically substantiated measures and support services for planning and training for potential crisis situations, and for use in real-life applications.

Access to the Transfer-lab
In a lab currently under construction, the network partners will have access to simulators developed in research projects, enabling them to carry out tests and presentations together with Fraunhofer experts and other network partners. The integration of new solutions for technical evaluations and stress tests will also open up new technical and organizational synergies that are based on science.

Joint simulations
In education and training courses, our network partners benefit from the planning, execution and evaluation of coupled simulations, and from access to scientific outcome studies and internal evaluations for real-world applications.

Networking with partners
Regular workshops and other formats for interaction provide our network partners with a framework for exchanging ideas with Fraunhofer experts, incorporating their own requirements directly into research and facilitating a reciprocal transfer of knowledge with other public and private stakeholders.

The vision of Fraunhofer SIRIOS is to establish a research, test and training environment that is unique in Europe – one that provides authorities and organizations with security tasks, CRITIS operators, industry and technology companies, plus associations and interest groups with an independent point of contact to which they can turn for advice and support.

Transfer-lab and consulting

- Socio-technical simulation of complex security scenarios
- Visualization and analysis of deployment scenarios
- Development of courses of action and defense strategies
- Provider-independent environments for development and testing
- Support in the planning of new security solutions with special consideration given to data protection and the protection of personal rights
- Consulting for innovation and product development
- Scientific support for tenders

Education and training

- Simulation-based seminars and training sessions
- Design and execution of simulation games and virtual stress tests
- Interdepartmental large-scale emergency demonstrations
- Participation of citizens, e. g., to record subjective perceptions of security
- Training materials, studies and internal evaluations

Workshops and exchange formats

- Provider-independent exchange at expert- and decision-maker level
- Discussion of research results and simulations
- Evaluation of technical and organizational requirements and synergies
- Further development of current security scenarios and challenges
- Presentation and sharing of new security concepts

Contact

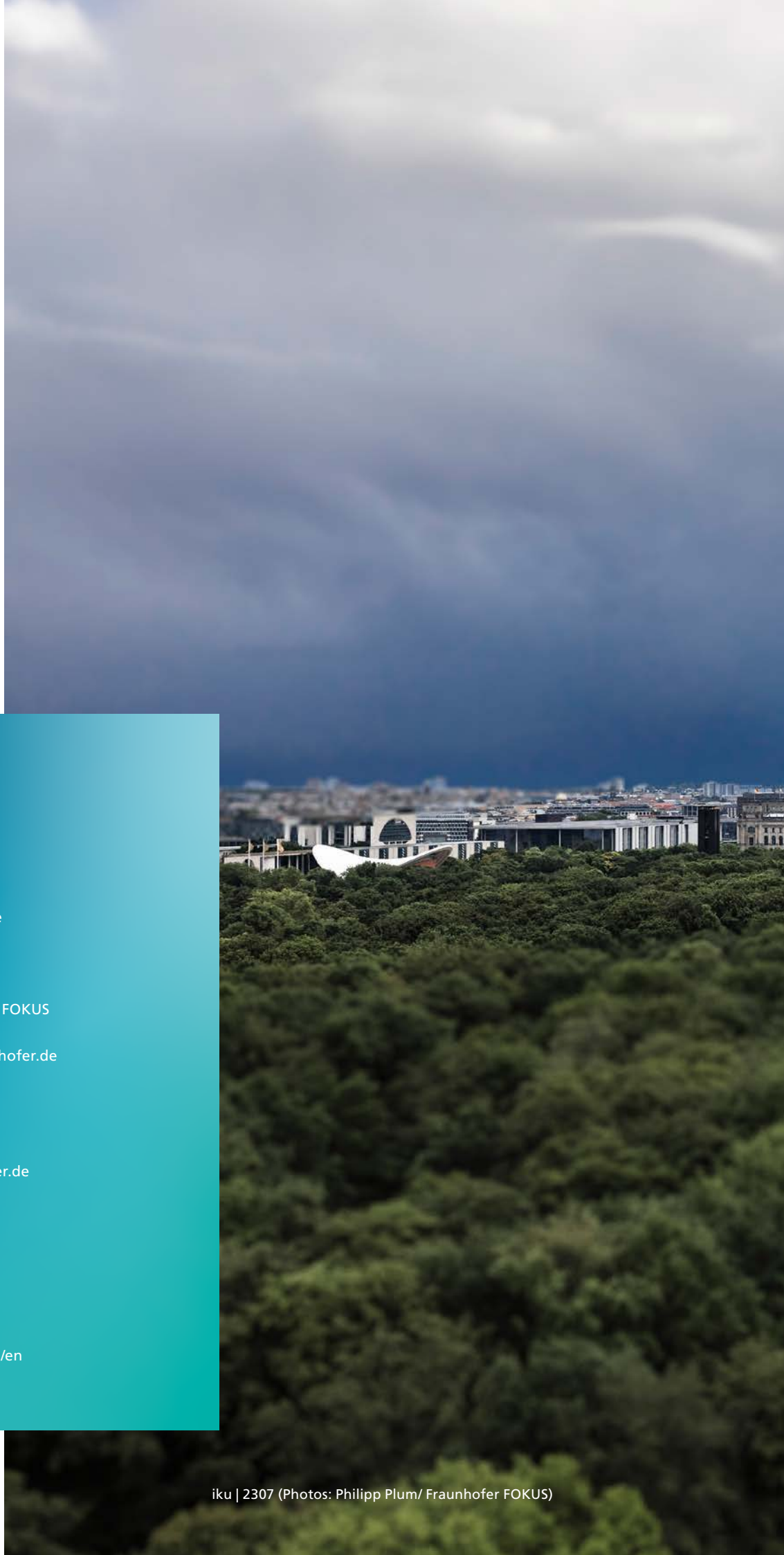
Managing Director
Daniel Hiller
Phone +49 160 90531810
daniel.hiller@sirios.fraunhofer.de

Spokesperson
Prof. Dr. Manfred Hauswirth
Executive Director of Fraunhofer FOKUS
Phone +49 30 3463-7204
manfred.hauswirth@fokus.fraunhofer.de

Communication and Network
Niklas Reinhardt
Phone +49 30 3463-7594
niklas.reinhardt@sirios.fraunhofer.de

Fraunhofer SIRIOS
c/o Fraunhofer FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin, Germany
info@sirios.fraunhofer.de

www.sirios.fraunhofer.com/sirios/en



iku | 2307 (Photos: Philipp Plum/ Fraunhofer FOKUS)