Fraunhofer SIRIOS

Fraunhofer-Zentrum für die Sicherheit
Sozio-Technischer Systeme SIRIOS

Fraunhofer SIRIOS

Mehr öffentliche Sicherheit durch Simulation urbaner Infrastrukturen

Dr. Tobias Leismann, Geschäftsführer und stell-vertretender Institutsleiter Fraunhofer EMI

Prof. Dr. Manfred Hauswirth, geschäftsführender Instituts-leiter Fraunhofer FOKUS

Prof. Dr. Jürgen Beyerer, Institutsleiter Fraunhofer IOSB

Prof. Dr. Matthias Klingner, Institutsleiter Fraunhofer IVI

Vereinte Fraunhofer-Kompetenzen

Das Fraunhofer-Zentrum für die Sicherheit Sozio-Technischer Systeme SIRIOS mit Sitz in Berlin bietet die Erfahrungen und Kompetenzen von vier Fraunhofer-Instituten im Bereich der öffentlichen Sicherheit aus einer Hand. Durch diese institutsüber-greifende Kooperation an einem zentralen Standort mit einer einzigartigen Infrastruktur werden neue Synergien geschaffen, um aktuelle Herausforderungen zu bewältigen.

Fraunhofer-Institut für Kurzzeitdynamik, Ernst-Mach-Institut, EMI
www.emi.fraunhofer.de

Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
www.fokus.fraunhofer.de

Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB
www.iosb.fraunhofer.de

Fraunhofer-Institut für Verkehrs- und Infrastruktursysteme IVI
www.ivi.fraunhofer.de

Vorwort

Wie sicher sind wir?

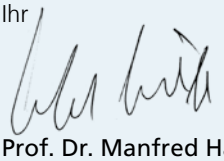
Die öffentliche Sicherheit ist eine der großen Herausforderungen des 21. Jahrhunderts. Viele der menschengemachten, aber auch natürlichen Bedrohungen mit ihren vielfältigen Wechselbeziehungen zwischen Mensch, Technik und Infrastrukturen sind schwer versteh- und beherrschbar. In der Wissenschaft sprechen wir über die moderne Gesellschaft als »sozio-technisches System«. In so gut wie allen Lebensbereichen sind Mensch und Technik hoch vernetzt.

Als Forscherinnen und Forscher für die zivile Sicherheit konzentrieren wir uns auf die Bedrohungen und die Sicherheit unserer Gesellschaft von innen: Hochwasserereignisse, die regional Strom- und Telekommunikationsnetze lahmlegen, Großveranstaltungen mit kaum kontrollierbaren Paniksituationen, grenzüberschreitende Verbrechen im digitalen Raum und nicht zuletzt das globale Pandemiegeschehen. Die Auswirkungen davon bekommen alle zu spüren und zeigen uns, wie sehr alles auch im alltäglichen Leben miteinander zusammenhängt und wie schnell sich punktuelle Gefahren entwickeln und verbreiten können. Öffentliche Sicherheit ist dementsprechend ein wichtiges und immer wiederkehrendes Thema in öffentlichen und politischen Debatten. Und auch viele Bürgerinnen und Bürger thematisieren die Risikowahrnehmung und das subjektive Sicherheitsempfinden immer stärker: Wie sicher sind wir eigentlich?

Wir stellen dabei mehrere gegenläufige Tendenzen fest: Den systemisch immer mehr in die Breite wachsenden Herausforderungen stehen zum Teil hoch spezialisierte Fach- und Insellösungen gegenüber. Doch lokale Störungen – »Schocks« – können extrem schnell kaskadieren und viele weitere Bereiche erfassen. Das macht es enorm schwer, die Auswirkungen der Störungen präzise vorherzusagen, Risiken verlässlich abzuschätzen und wenn möglich zu verhindern. Leider sind die Werkzeuge und Mittel, die Behörden und Organisationen mit Sicherheitsaufgaben (BOS) – also Polizei, Feuerwehr, Katastrophenschützer usw. – derzeit zur Gefahrenabwehr und Krisenbewältigung zur Verfügung stehen, oftmals gar nicht in der Lage, die komplexen Zusammenhänge systemisch zu erfassen. Das Gleiche gilt für die privaten und öffentlichen Betreiber von kritischen Infrastrukturen (KRITIS), wie z. B. der Telekommunikation, der Energie- und Wasserversorgung oder im Verkehrswesen, deren Störungen unmittelbare Auswirkungen für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen haben. Ohne die richtigen Maßnahmen zur richtigen Zeit an der richtigen Stelle wird eine lokale Störung schnell zu einer Großschadenslage!

Ziel des Fraunhofer-Zentrums für die Sicherheit Sozio-Technischer Systeme SIRIOS ist es, diesen systemischen Gesamtblick für die öffentliche Sicherheit zu ermöglichen. Mithilfe neuer Modelle urbaner Lebensräume und technischer Infrastrukturen sowie darauf basierenden Simulationen mit virtuellen und realen Elementen unterstützen wir BOS und KRITIS bei der Entscheidung für die richtige Maßnahme zur richtigen Zeit an der richtigen Stelle. Damit alle sicherer leben können.

Ihr



Prof. Dr. Manfred Hauswirth

Sprecher des Fraunhofer SIRIOS und geschäftsführender Institutsleiter Fraunhofer FOKUS

Das Fraunhofer SIRIOS in Berlin

Das Fraunhofer-Zentrum für die Sicherheit Sozio-Technischer Systeme SIRIOS macht mithilfe gekoppelter Simulationen komplexe Krisenszenarien beherrschbar und erhöht die Sicherheit und Resilienz in der Gesellschaft.

Pilotprojekte in der Aufbauphase

- Sichere Versorgungsnetze und Infrastrukturen
- Schutz und Reaktionsfähigkeit von Einsatzkräften, Helfern und Bevölkerung
- Interaktive, virtuelle Lagevisualisierung
- Kommunikations- und Handlungseffizienz

Partner und Netzwerk

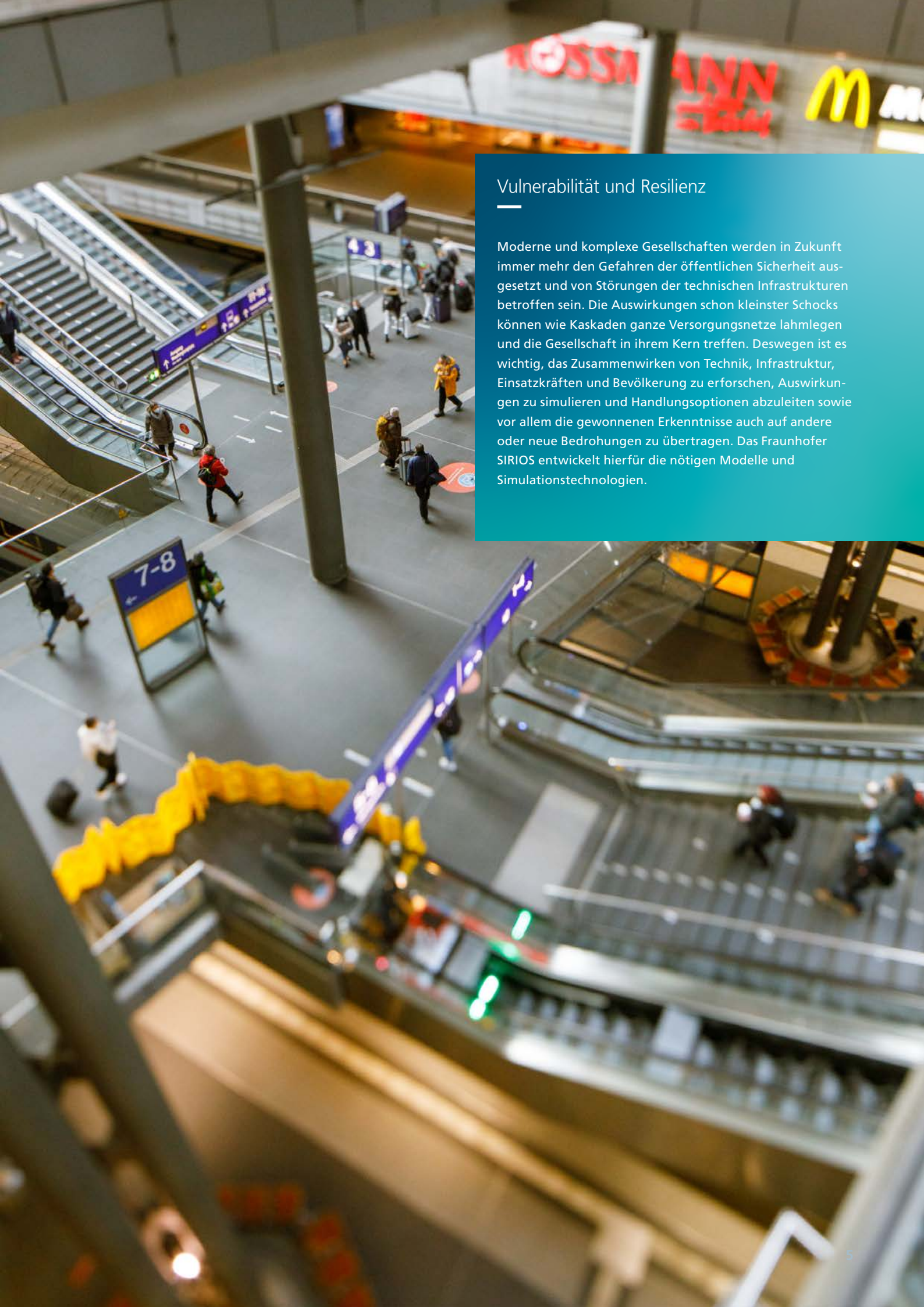
- Politik und Verwaltung
- Behörden und Organisationen mit Sicherheitsaufgaben (BOS)
- Betreiber kritischer Infrastrukturen (KRITIS)
- Industrie und Technologie
- Forschung und Entwicklung
- Verbände und Interessenvertretungen

Simulationen für den Ernstfall

Das Fraunhofer SIRIOS versteht sich als Inkubator für neue simulationsbasierte Technologien. Das Zentrum bündelt die Expertise verschiedener Fraunhofer-Institute am Standort in Berlin. In verschiedenen (Pilot-)Projekten erarbeiten die Mitarbeiterinnen und Mitarbeiter Lösungen und Angebote für die öffentlichen Sicherheit innerhalb von fünf strategischen Anwendungsfeldern: 1. Digitalisierung der Sicherheit und Schutz von Kritischen Infrastrukturen (KRITIS), 2. Aufklärung, Kommunikation und Einsatzführung, 3. Virtuelle Planung und Begleitung von Großveranstaltungen, 4. Partizipation, Risiko- und Krisenkommunikation sowie 5. Visualisierung und hybride Testumgebungen für BOS und KRITIS.

Ein besonderer Fokus liegt auf der Überführung der Arbeiten in die Praxis: Dafür baut das Zentrum ein unabhängiges Partnernetzwerk mit Bedarfsträgern aus dem öffentlichen und privaten Sicherheitssektor auf. Auf diese Weise werden rechtliche Rahmenbedingungen, Arbeitsweisen der Behörden und Sicherheitsorganisationen, Vorgehensweisen in Forschung und Entwicklung, Geschäftsmodelle von Technologieunternehmen sowie die Akzeptanz der Bevölkerung »by Design«, d. h. von Anfang an, in den wissenschaftlichen Entwicklungsprozess integriert. Szenario-orientierte Simulationen versteht das Fraunhofer SIRIOS als technologieoffene und ressortübergreifende Methodik für alle beteiligten Stakeholder.

Als Ergebnis wird das Fraunhofer SIRIOS seinen Partnern umfassende Unterstützung bieten: Als neutrale, lösungsunabhängige und wissenschaftliche Einrichtung schafft das Zentrum eine kollaborative Umgebung für Trainings- und Simulationsmöglichkeiten mit virtuellen Einsätzen im zwei- oder dreidimensionalen Raum sowie eine offene Architektur für verschiedene Systeme, um Schwachstellen und technisch-organisatorische Synergien zu evaluieren.



Vulnerabilität und Resilienz

Moderne und komplexe Gesellschaften werden in Zukunft immer mehr den Gefahren der öffentlichen Sicherheit ausgesetzt und von Störungen der technischen Infrastrukturen betroffen sein. Die Auswirkungen schon kleinster Schocks können wie Kaskaden ganze Versorgungsnetze lahmlegen und die Gesellschaft in ihrem Kern treffen. Deswegen ist es wichtig, das Zusammenwirken von Technik, Infrastruktur, Einsatzkräften und Bevölkerung zu erforschen, Auswirkungen zu simulieren und Handlungsoptionen abzuleiten sowie vor allem die gewonnenen Erkenntnisse auch auf andere oder neue Bedrohungen zu übertragen. Das Fraunhofer SIRIOS entwickelt hierfür die nötigen Modelle und Simulationstechnologien.

Simulation – Transfer – Impact

Das Fraunhofer SIRIOS versteht sich als Inkubator für neue Technologien der öffentlichen Sicherheit. Dafür baut es ein Partnernetzwerk mit Bedarfsträgern aus dem öffentlichen und privaten Sicherheitssektor auf. Ziel des Partnernetzwerks ist es, gemeinsam relevante Parameter und wechselseitige Abhängigkeiten der modernen Gesellschaft zu identifizieren und zu erforschen. Die Auswertungen offenbaren vorhandene Sicherheitsschwachstellen und schaffen Raum für neue Abwehr- und Resilienzstrategien.

Gekoppelte Simulationen und neue Modelle

Die Entstehung und Auswirkungen komplexer sozio-technischer Bedrohungs- oder Schadenslagen erfassen und wissenschaftlich fundierte Maßnahmen ableiten.

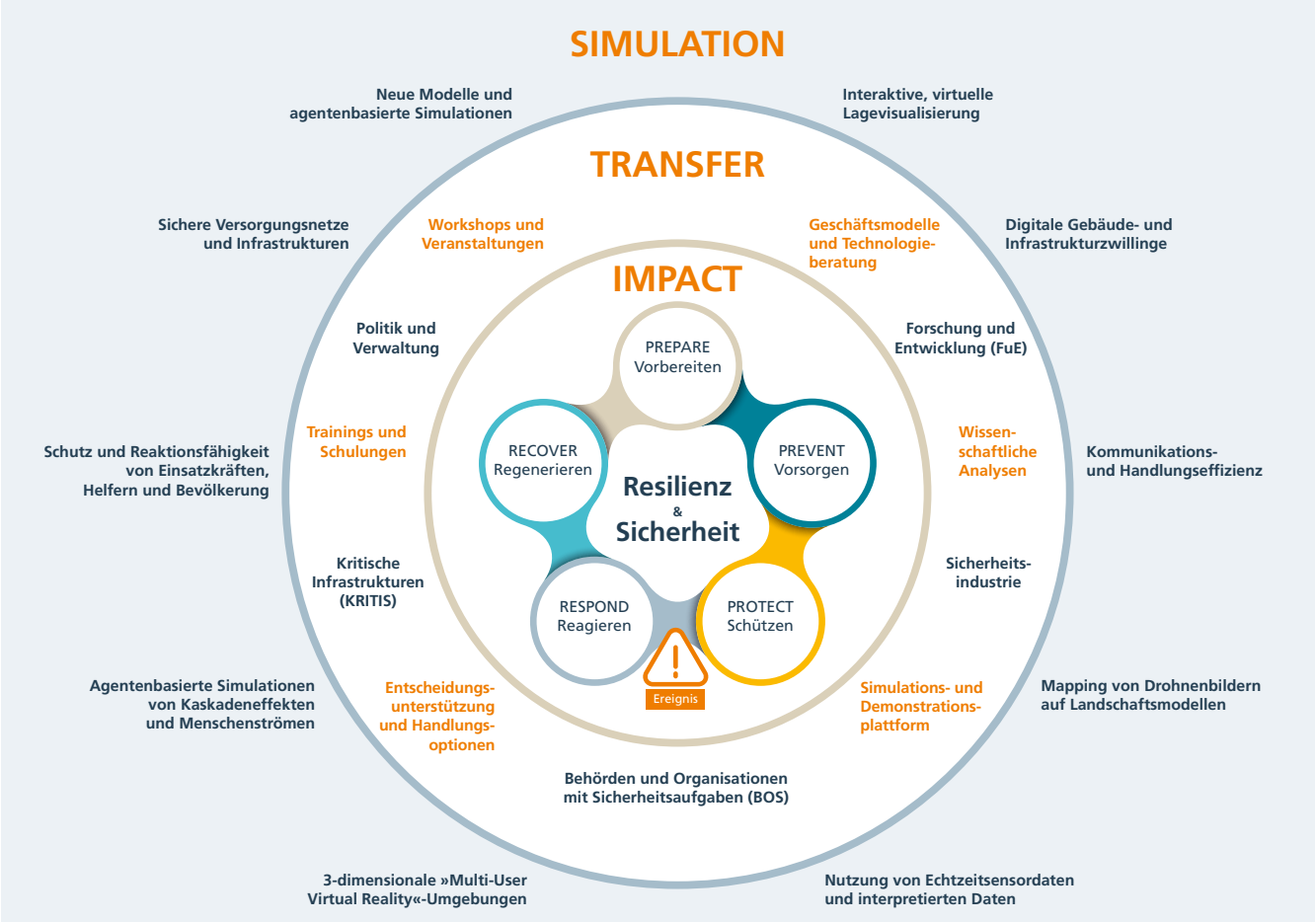
Transfer an Sicherheitsverantwortliche

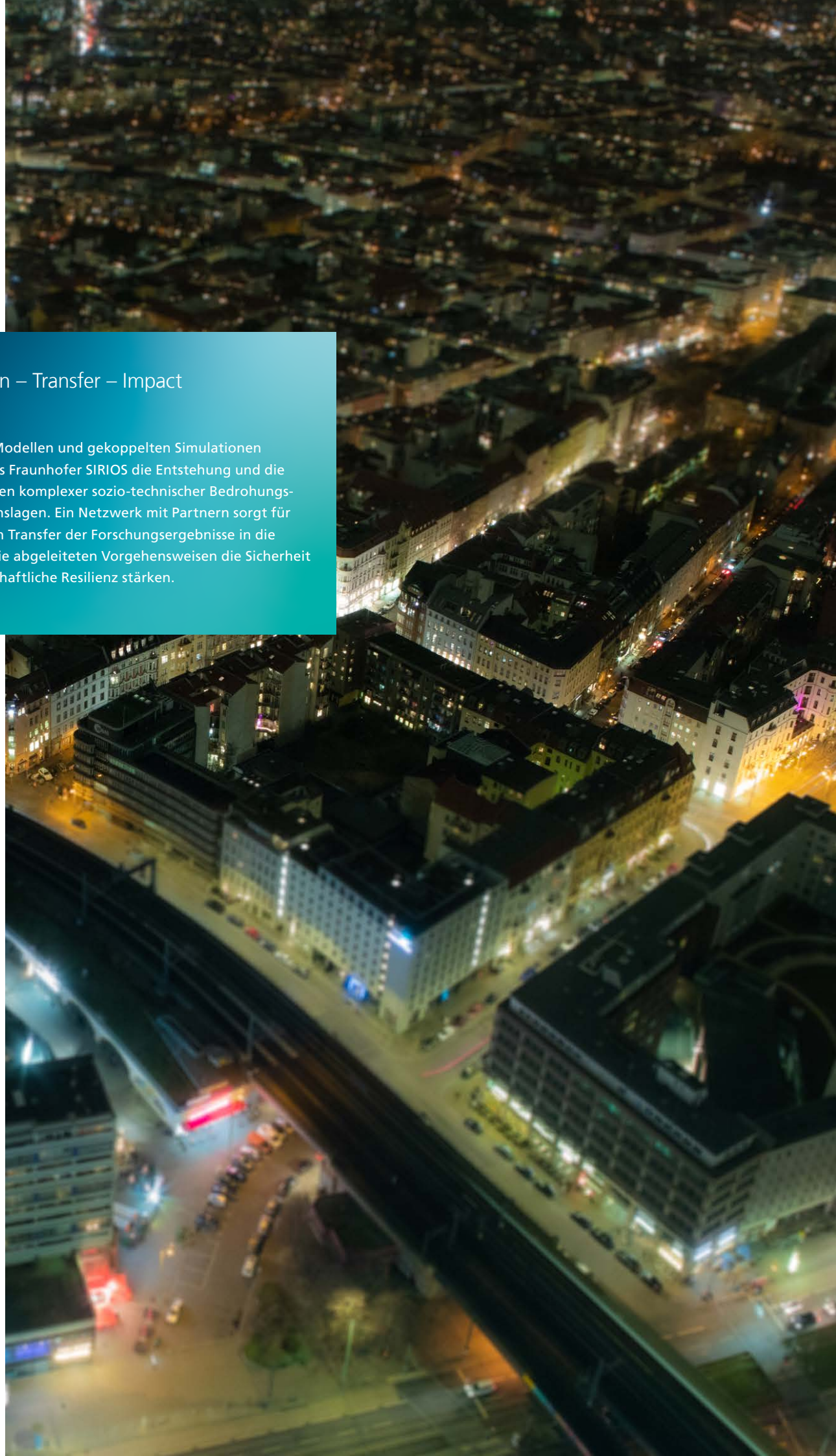
Lösungen für das Zusammenwirken von Technik, Infrastruktur, Einsatzkräften und Bevölkerung bei komplexen Lagen gemeinsam mit Bedarfsträgern entwickeln und für den realen Einsatz in die Praxis überführen.

Impact für Sicherheit und Resilienz

Die Bewert- und Beherrschbarkeit neuer Technologien im Ernstfall unterstützen, den Schutz von Daten- und Persönlichkeitsrechten sicherstellen und das subjektive Sicherheitsgefühl der Bürgerinnen und Bürger erhöhen.

Inkubator für neue Technologien der öffentlichen Sicherheit: Die Erforschung wechselseitiger Abhängigkeiten der modernen Gesellschaft schafft Grundlagen für neue Abwehr- und Resilienzstrategien.





Simulation – Transfer – Impact

Mit neuen Modellen und gekoppelten Simulationen erforscht das Fraunhofer SIRIOS die Entstehung und die Auswirkungen komplexer sozio-technischer Bedrohungs- und Schadenslagen. Ein Netzwerk mit Partnern sorgt für den direkten Transfer der Forschungsergebnisse in die Praxis, wo die abgeleiteten Vorgehensweisen die Sicherheit und gesellschaftliche Resilienz stärken.

Anwendungsfelder

Digitalisierung der Sicherheit und Schutz von Kritischen Infrastrukturen

Kritische Infrastrukturen (KRITIS) wie Energie, Wasser, Finanzen und Kommunikation sind die Arterien der Gesellschaft und lebenswichtig. Ihre Verfügbarkeit bzw. ein Ausfall hat auch auf die öffentliche Sicherheit großen Einfluss. Man denke an einen Strom- und damit verbundenen Mobilfunknetzausfall über einen längeren Zeitraum oder einen Ausfall des ÖPNV aufgrund eines massiven Cyberangriffs. Durch die steigende Komplexität und Vernetzung von KRITIS-Systemen steigt zudem das Risiko massiver netzübergreifender Kaskadeneffekte durch lokale Schäden. Die Planung, der Betrieb und die Überwachung von KRITIS ist zunehmend digital und internetbasiert. So ermöglichen es Digitale Zwillinge von Versorgungsnetzen und Gebäuden, unterschiedliche Was-wäre-wenn-Szenarien virtuell darzustellen und ihre Auswirkungen auf konkrete Sicherheitslagen bewertbar zu machen.

Aufklärung, Kommunikation und Einsatzführung

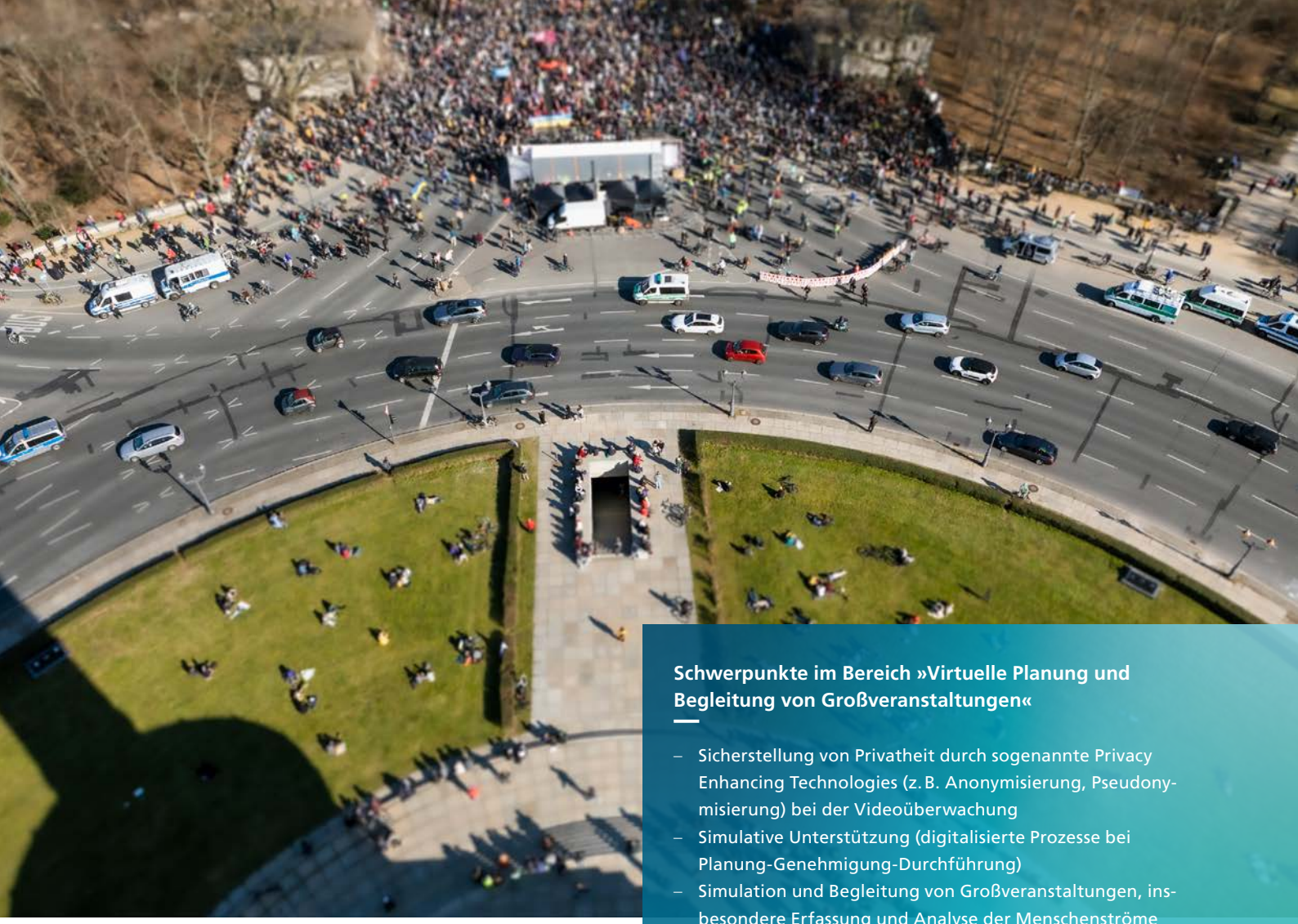
Mit der Entwicklung leistungsfähiger Verfahren zur datenbasierten Aufklärung, Kommunikation und Einsatzführung unterstützt das Simulationszentrum die Einsatzkräfte bei der unmittelbaren Bewältigung von komplexen Bedrohungslagen. Angesichts föderaler Zuständigkeiten sowie länderspezifischer Ausstattung der Sicherheitskräfte kommt der Interoperabilität der Einsatzführungssysteme eine besondere Bedeutung zu: Die Interoperabilität bezieht sich dabei auf die technisch zu gewährleistende Austauschbarkeit von Informationen und Daten auch in heterogenen Systemverbünden (Daten- und Schnittstellenkompatibilität). Zusätzlich werden in einem übergreifenden und dezentralen (Ad-hoc-)Vernetzungsansatz neben den BOS auch alle weiteren relevanten Akteure (von Behörden, Hilfsorganisationen, KRITIS-Betreibern und betroffenen Unternehmen bis hin zur Bevölkerung) betrachtet.

Schwerpunkte im Bereich »Digitalisierung der Sicherheit und Schutz von Kritischen Infrastrukturen«

- Modellierung und Simulation von Schadensszenarien in gekoppelten, interdependenten Infrastruktursystemen
- Aufbau und Nutzung digitaler Gebäude- und Infrastrukturzwillinge (z. B. Bahnhof, Wasserversorgung) zur Planung von Sicherheit und Schutz
- Zusammenführung von digitalen Stadtmodellen und Sensordaten aus Gebäuden und Infrastrukturen zur Optimierung von Sicherheitskonzepten
- Kopplung von sensorischer Umgebungserfassung und Simulation
- Entwicklung von prognosefähigen Simulationen zur Früherkennung von Angriffen und Überlasten

Schwerpunkte im Bereich »Aufklärung, Kommunikation und Einsatzführung«

- Grundlagen für die Unterstützung von vernetzten und interoperablen Systemen (z. B. für länder- und behördenübergreifende Einsatzführungssysteme)
- Cybersicherheit der Datenerfassungs-, Kommunikations- und Kommandosysteme
- Maschinelle Datenauswertung und Entscheidungsunterstützung
- Modelle und Architekturen für die Interoperabilität und dezentrale (Ad-hoc-)Vernetzung heterogener Systeme
- Video- und drohnenbasierte Einsatzführung sowie VR-Lagevisualisierung (z. B. Bedrohungslage, damage assessment)

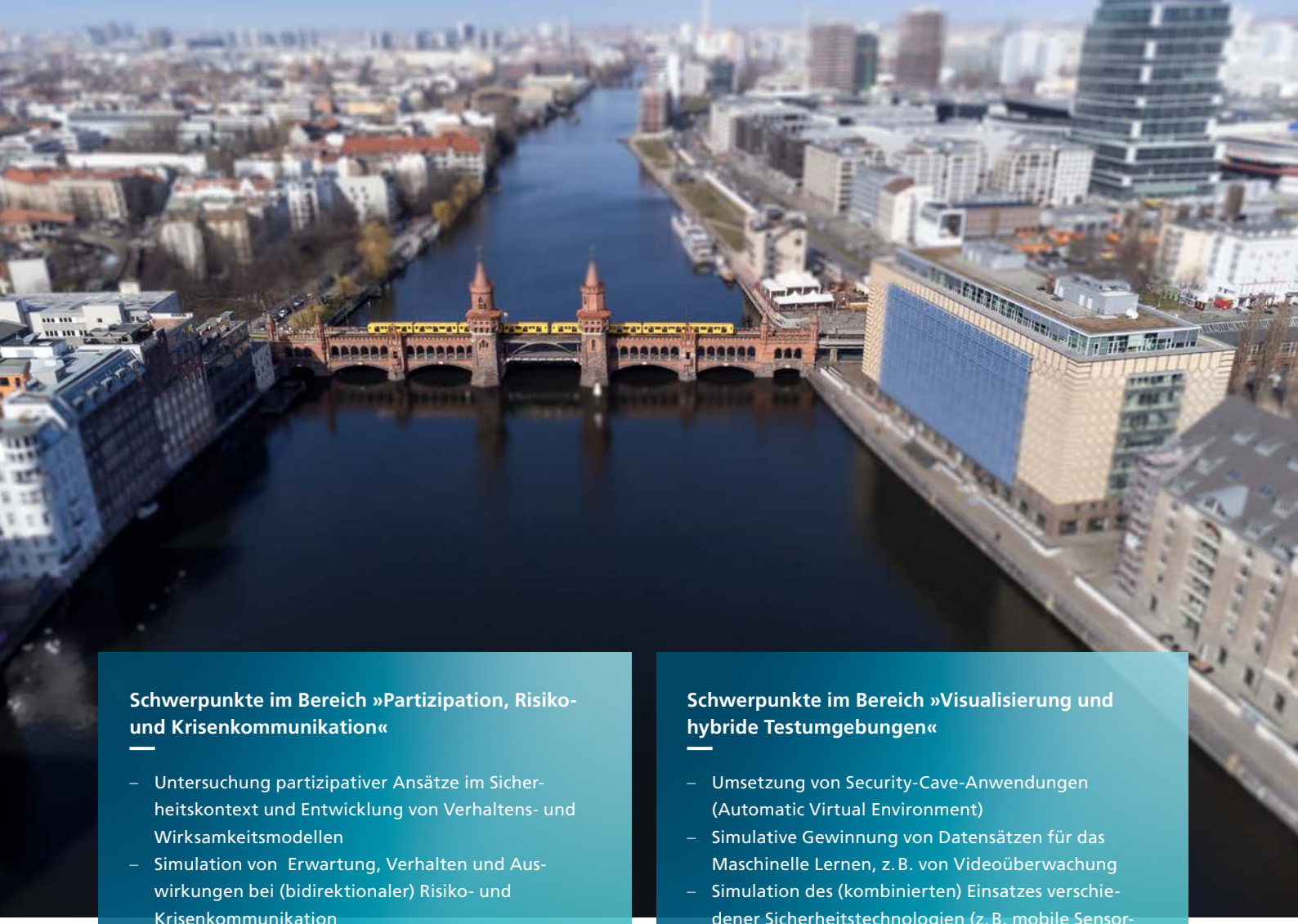


Schwerpunkte im Bereich »Virtuelle Planung und Begleitung von Großveranstaltungen«

- Sicherstellung von Privatheit durch sogenannte Privacy Enhancing Technologies (z. B. Anonymisierung, Pseudonymisierung) bei der Videoüberwachung
- Simulative Unterstützung (digitalisierte Prozesse bei Planung-Genehmigung-Durchführung)
- Simulation und Begleitung von Großveranstaltungen, insbesondere Erfassung und Analyse der Menschenströme (Dichte, Verhalten) sowie der Veranstaltungsinfrastruktur
- Optimierte Planung der Sicherheitsinfrastruktur
- Agentenbasierte Simulation von Einsatz-, Abhilfe- und Evakuierungsoperationen

Virtuelle Planung und Begleitung von Großveranstaltungen

Großveranstaltungen zeichnen sich durch vielfältige Gefährdungsmomente aus. Diese können einerseits durch menschliches Verhalten (z. B. durch Gewalt- und Terrorakte oder Amokläufe sowie Paniksituationen bei hoher Personendichte) sowie andererseits durch technische Störungen (z. B. Stromausfälle oder Zusammenbruch der Kommunikationsinfrastrukturen) zustande kommen. Simulationen können den Prozess der Planung-Genehmigung-Durchführung von Großveranstaltungen maßgeblich unterstützen. Das bezieht sich insbesondere auf die Gefährdungsbeurteilung vor und während der Veranstaltung, die Sicherheitsinfrastruktur sowie, im eingetretenen Gefährdungsfall, auf zielführende Gegenmaßnahmen. Durch die hohe Zahl an betroffenen Personen bei Großveranstaltungen kommt hier dem Schutz der Persönlichkeitsrechte eine besondere Bedeutung zu.



Schwerpunkte im Bereich »Partizipation, Risiko- und Krisenkommunikation«

- Untersuchung partizipativer Ansätze im Sicherheitskontext und Entwicklung von Verhaltens- und Wirksamkeitsmodellen
- Simulation von Erwartung, Verhalten und Auswirkungen bei (bidirektionaler) Risiko- und Krisenkommunikation
- Messung und Simulation des subjektiven Sicherheitsempfindens und der Risikowahrnehmung in der Bevölkerung
- Technologien zur kommunikativen Ad-hoc-Vernetzung in Sicherheitslagen
- Privacy- und Security-by-Design-Modelle für Akzeptanz und Vertrauen der Bevölkerung in bürgernahe Sicherheitsanwendungen

Schwerpunkte im Bereich »Visualisierung und hybride Testumgebungen«

- Umsetzung von Security-Cave-Anwendungen (Automatic Virtual Environment)
- Simulative Gewinnung von Datensätzen für das Maschinelle Lernen, z. B. von Videoüberwachung
- Simulation des (kombinierten) Einsatzes verschiedener Sicherheitstechnologien (z. B. mobile Sensorträger, Drohnenabwehrsysteme, Bodycams)
- Interaktion mit Zielpersonen

Partizipation, Risiko- und Krisenkommunikation

Um die Herausforderungen der öffentlichen Sicherheit zu bewältigen, müssen neben den Kernakteuren wie BOS, Hilfsorganisationen und KRITIS-Betreibern auch die Bürgerinnen und Bürger selbst in einem partizipativen Ansatz einbezogen werden – von der Vorbereitung und den Präventionsmaßnahmen über die Reaktion und Selbsthilfe bei einem Schadensereignis bis hin zur Wiederherstellung der Normalität. Simulationen können hierfür einen entscheidenden Beitrag leisten, insbesondere um das Zusammenspiel von Kommunikationskanälen (z. B. soziale Medien), Rezeption und Verhalten der Menschen besser zu verstehen und das subjektive Sicherheitsempfinden der Bevölkerung sowie Akzeptanz und Vertrauen in die Maßnahmen zu erhöhen. Verlässliche Privacy- und Security-by-Design-Ansätze sind dabei unerlässlich.

Visualisierung und hybride Testumgebungen

Moderne Simulationen ermöglichen es, Einsatzszenarien durchzuspielen und Vorgehensweisen zu eruieren. Im Vergleich zu rein virtuellen Testumgebungen bieten dabei hybride Visualisierungs- und Interaktionstechniken mit realen Elementen einen noch höheren Grad an Praxisbezug: So können mit Security-Cave-Anwendungen (Automatic Virtual Environment) künstliche Einsatzszenarien geschaffen werden (z. B. Terrorszenario am Hauptbahnhof, Massenpanik bei Großveranstaltungen, Geiselnahme im Regierungsviertel, Drohnenangriffe), in denen die direkte Interaktion von Personen erprobt wird. Auch reale Sicherheitstechnologien (z. B. teilautonome mobile Sensorträger) kommen hier in Simulationen zum Einsatz und werden auf ihre Einsatztauglichkeit hin untersucht.

Unser Leistungsangebot

Das Fraunhofer SIRIOS baut einen neutralen und kollaborativen Raum für einen partnerschaftlichen Austausch auf. In diesem Transfernetzwerk erarbeiten wir gemeinsam mit Fachleuten in BOS, KRITIS und der Sicherheitsindustrie wissenschaftlich fundierte Maßnahmen und Unterstützungsleistungen für Planung und Training von möglichen Krisensituationen sowie für den Einsatz in der Realität.

Zugang zum Transferlab
In einem im Aufbau befindlichen Lab erhalten die Netzwerkpartner Zugang zu den in Foschungsprojekten entwickelten Simulatoren, um gemeinsam mit Fraunhofer-Expertinnen und -Experten und weiteren Netzwerkpartnern Tests und Präsentationen durchzuführen. Die Integration neuer Lösungen für technische Evaluationen und Stresstests ermöglicht zudem neue technisch-organisatorische Synergien auf wissenschaftlicher Basis.

Gemeinsame Simulationen
In Schulungen und Trainings profitieren unsere Netzwerkpartner von der Planung, Durchführung und Auswertung gekoppelter Simulationen sowie vom Zugang zu wissenschaftlichen Ergebnisstudien und internen Auswertungen für die Praxis.

Networking mit Partnern
Regelmäßige Workshops und Austauschformate bieten unseren Netzwerkpartnern den Rahmen, um mit Fraunhofer-Expertinnen und -Experten in den Austausch zu treten, eigene Bedarfe direkt in die Forschung einfließen zu lassen und einen gegenseitigen Transfer mit weiteren öffentlichen und privaten Stakeholdern zu realisieren.

Die Vision des Fraunhofer SIRIOS ist es, eine in Europa einzigartige Forschungs-, Test- und Trainingsumgebung aufzubauen, in der BOS, KRITIS-Betreiber, Industrie und Technologieunternehmen sowie Verbände und Interessenvertretungen einen unabhängigen Anlaufpunkt für ihre Bedarfe finden.

Transferlab und Beratung

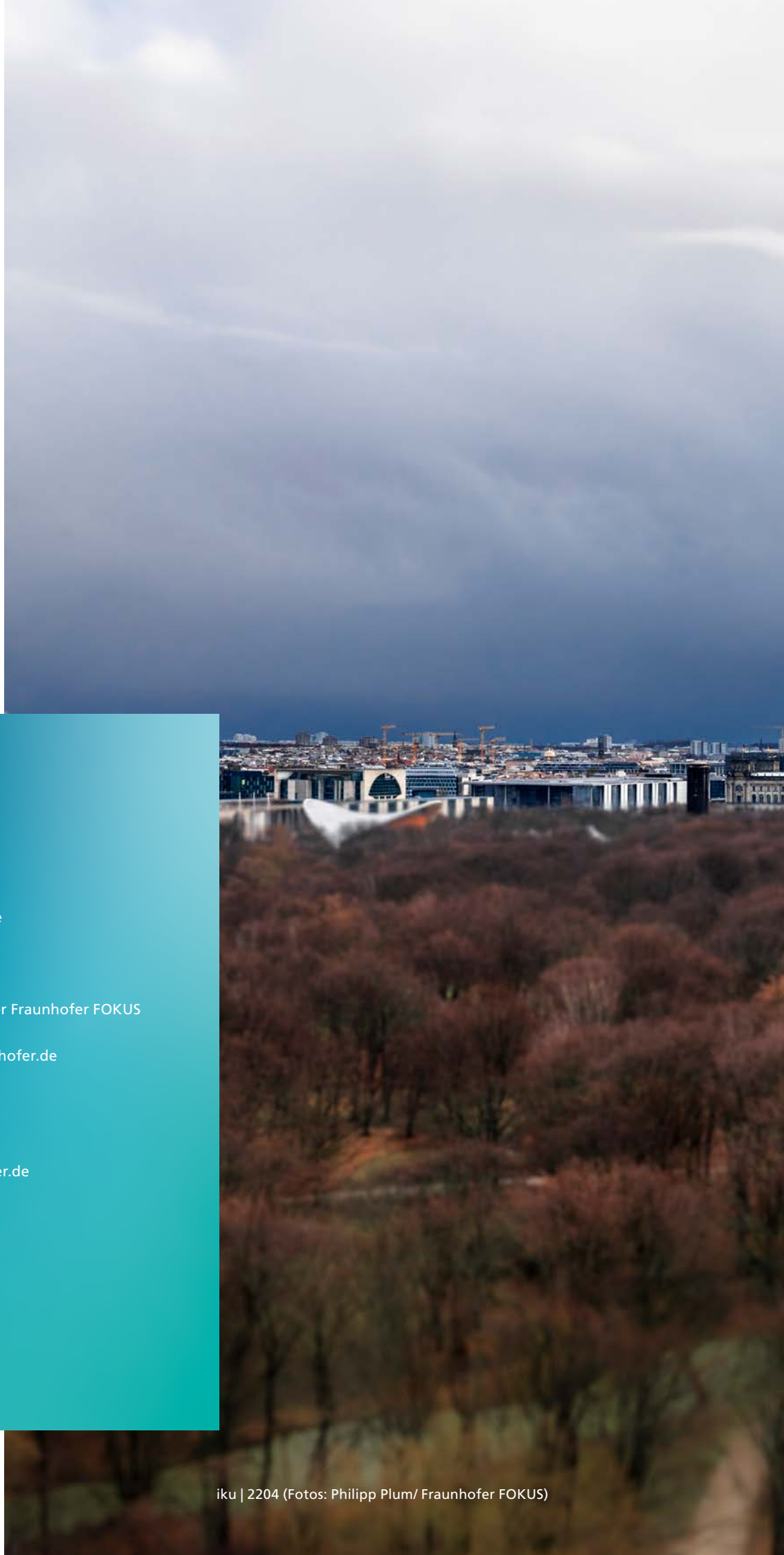
- Sozio-technische Simulation komplexer Sicherheitsszenarien
- Visualisierung und Analyse von Einsatzszenarien
- Ausarbeitung von Handlungsoptionen und Abwehrstrategien
- Anbieter-unabhängige Entwicklungs- und Testumgebungen
- Unterstützung bei der Planung neuer Sicherheitslösungen unter besonderer Berücksichtigung des Datenschutzes und Schutzes der Persönlichkeitsrechte
- Innovations- und Produktentwicklungsberatung
- Wissenschaftliche Ausschreibungsbegleitung

Schulungen und Trainings

- Simulationsgestützte Trainings und Schulungen
- Konzeption und Durchführung von Planspielen und virtuellen Stresstests
- Ressortübergreifende Demonstrationen von Großschadenslagen
- Partizipation von Bürgerinnen und Bürgern, z. B. um subjektives Sicherheitsempfinden zu erfassen
- Schulungsmaterial, Studien und interne Auswertungen

Workshops und Austauschformate

- Anbieter-unabhängiger Austausch auf Fach- und Entscheider-Ebene
- Diskussion der Forschungsergebnisse und Simulationen
- Evaluation von technisch-organisatorischen Bedarfen und Synergien
- Weiterentwicklung aktueller Sicherheitsszenarien und Herausforderungen
- Präsentation und Austausch neuer Sicherheitskonzepte



Kontakt

Geschäftsführer
Daniel Hiller
Telefon +49 160 90531810
daniel.hiller@sirios.fraunhofer.de

Sprecher
Prof. Dr. Manfred Hauswirth
Geschäftsführender Institutsleiter Fraunhofer FOKUS
Telefon +49 30 3463-7204
manfred.hauswirth@fokus.fraunhofer.de

Kommunikation und Netzwerk
Niklas Reinhardt
Telefon +49 30 3463-7594
niklas.reinhardt@sirios.fraunhofer.de

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

www.sirios.fraunhofer.de

iku | 2204 (Fotos: Philipp Plum/ Fraunhofer FOKUS)