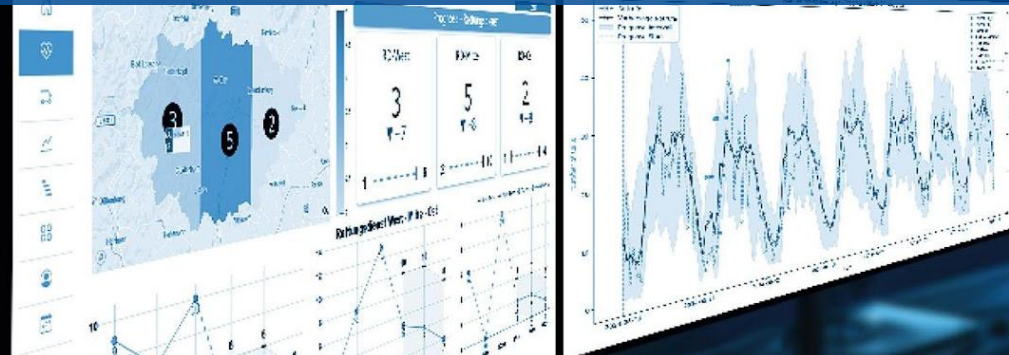




AI ASSURANCE

ABSICHERUNG VON KI BASIERTEN SYSTEMEN

Thorsten Hansler, Dr. Willfried Wienholt



1 Jahr IABG in der Schweiz

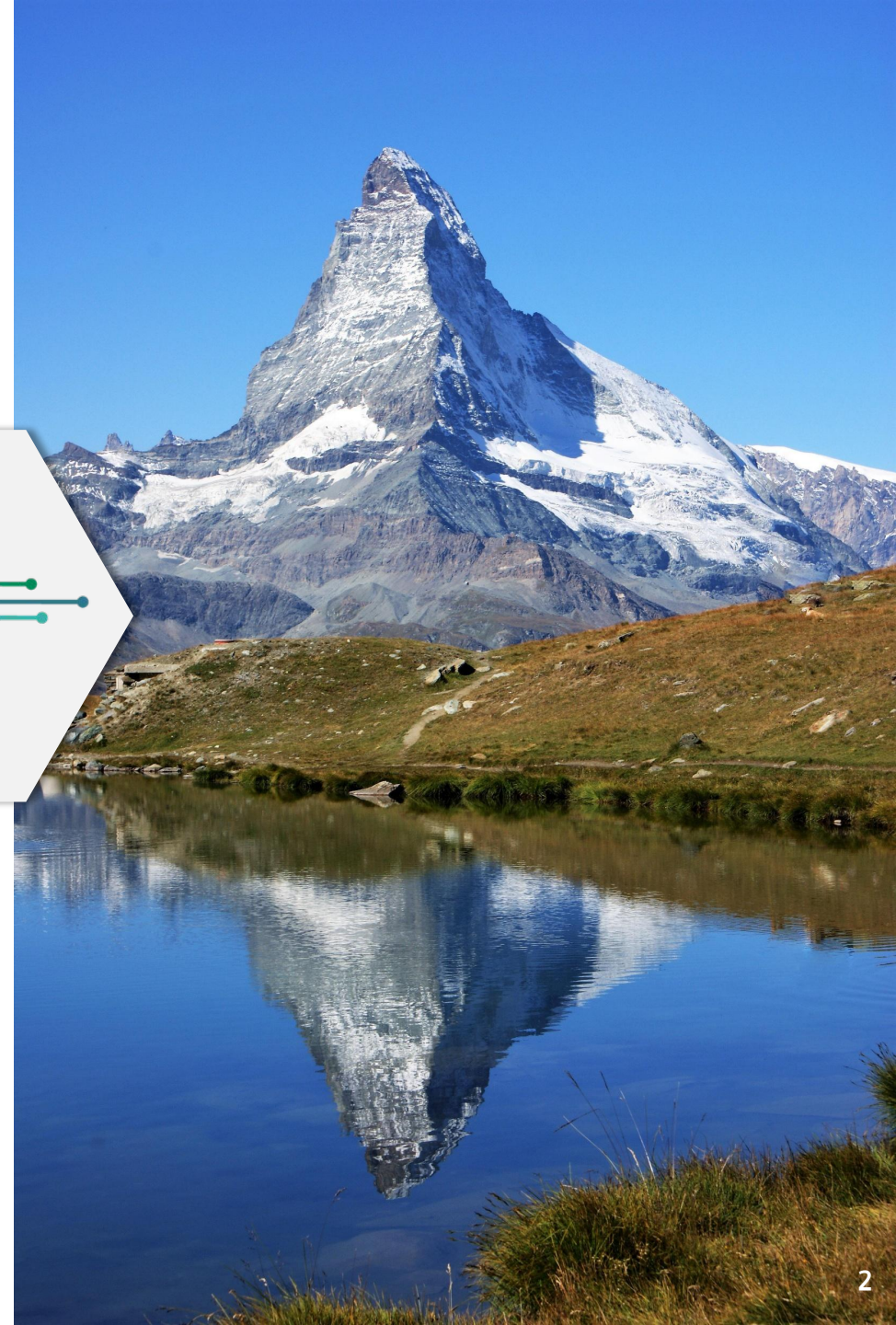
**Leitstellen-
planung – KI
in
der Leitstelle**

SPiK
SWISS POLICE ICT

easyCab
MEDICAL

APPROVED
MEDICAL
TRANSPORT
www.144.ch
SAVING LIVES

IABG
DIGITALISIERUNG
SICHER GESTALTEN.
LEISTUNG • FÖRDERUNG • SÜDLICH
INNOVATIONEN FÜR ZUKUNFT





01

Anwendungsfall – Einführung von KI in der Leitstelle

Lessons Learned: Was gibt es technisch zu beachten und welche Hürden sind zu überwinden um für die neue Technik eine Akzeptanz bei den Disponenten zu erzielen?

Zuständig für



250.000 Einwohner

Erfasst



90.000 Ereignisse pro Jahr

Veranlasst

13.700 Gebietsabsicherungen¹ im Jahr

Zusammenarbeit mit



22 freiwilligen Feuerwehren

162 Ortsteilfeuerwehren

5 Werksfeuerwehren

1 Universitätsklinikum

2 Krankenhäuser der Grundversorgung



Besteht aus
22 Städten und Gemeinden

¹ Verlegefahrten der Rettungswagen, um lokale Engpässe zu vermeiden

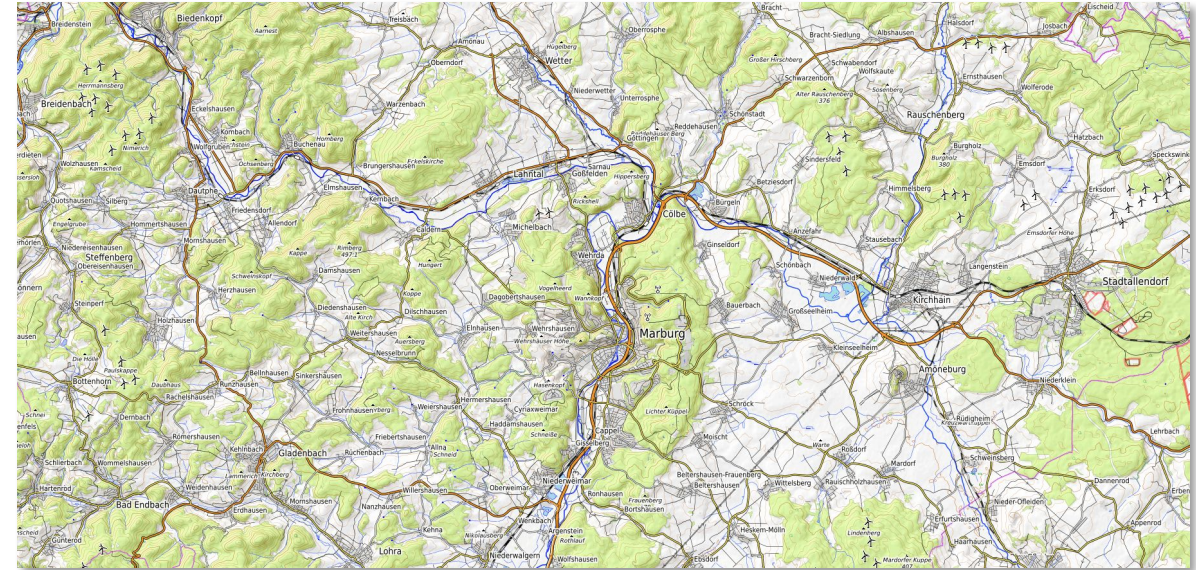
Herausforderungen der Leitstelle Marburg-Biedenkopf

Besonderheiten im Landkreis

- Ländliche Prägung und anspruchsvolle Topografie
- Hohes Hilfsfristniveau in Hessen: 10min in 90% der Fälle

Einhaltung der Hilfsfrist über ein risikoabhängiges Gebietsabsicherungskonzept

- Besetzen von nicht besetzten Rettungswachen nach festgelegtem Schema
- 13.700 Einsätze in 2022 zur Gebietsabsicherung
- Auf etwa 50% der Verlegefahrten erfolgt ein Anschlusseinsatz
- Erheblicher Mehraufwand



Quelle: <https://opentopomap.org/#map=12/50.8280/8.7661>

Die allgemeine Steigerung der Einsatzzahlen, die höhere Auslastung des Rettungsdienstes und die Personalproblematik machen die Gebietsabsicherung immer schwieriger.

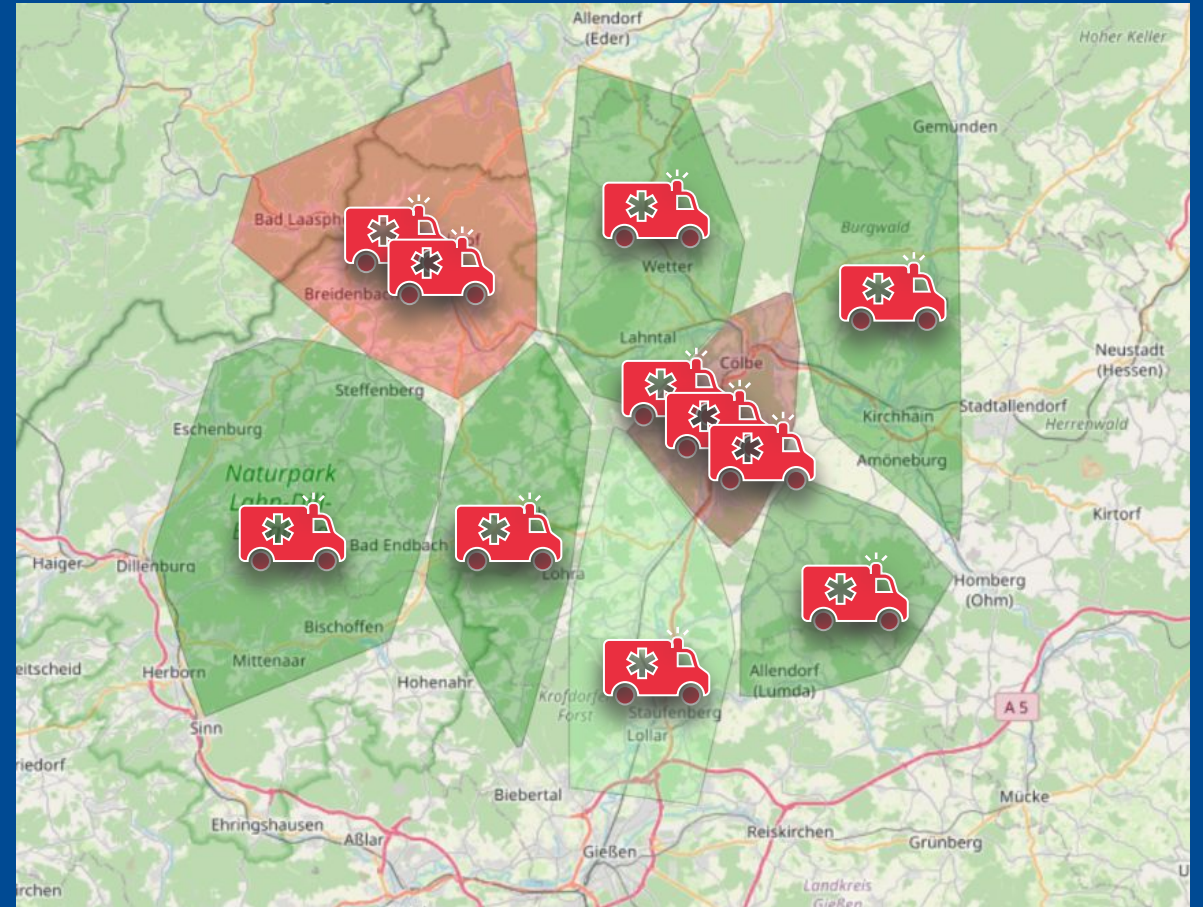
Optimierung der Ressourcenplanung

Einsparung an Ressourcen durch bessere Vorhersage

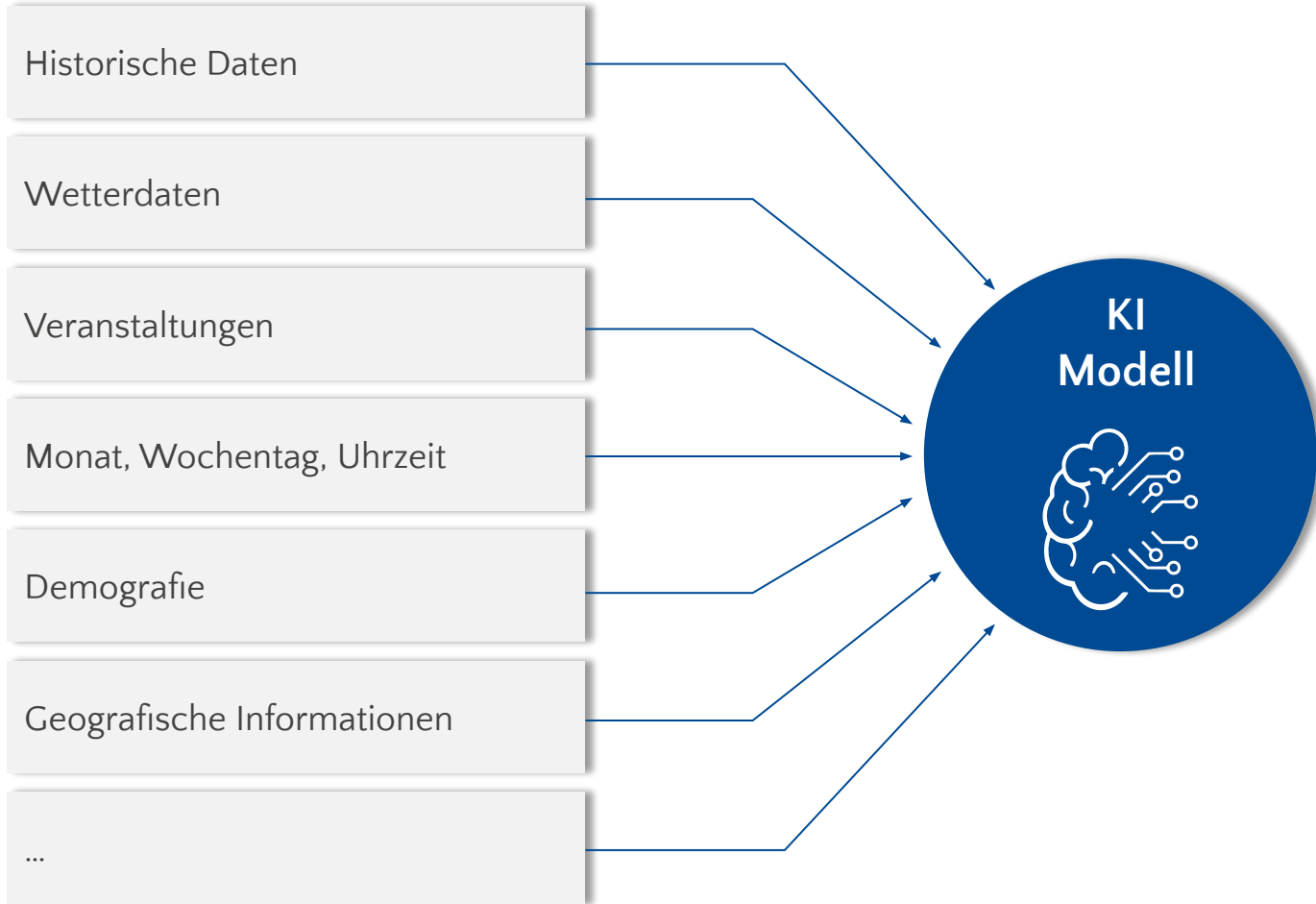
- des Einsatzaufkommens für die nächsten Stunden und Tage und
- der räumlichen Verteilung der Einsätze

Permanente Berechnung der optimalen Ressourcenallokation, um

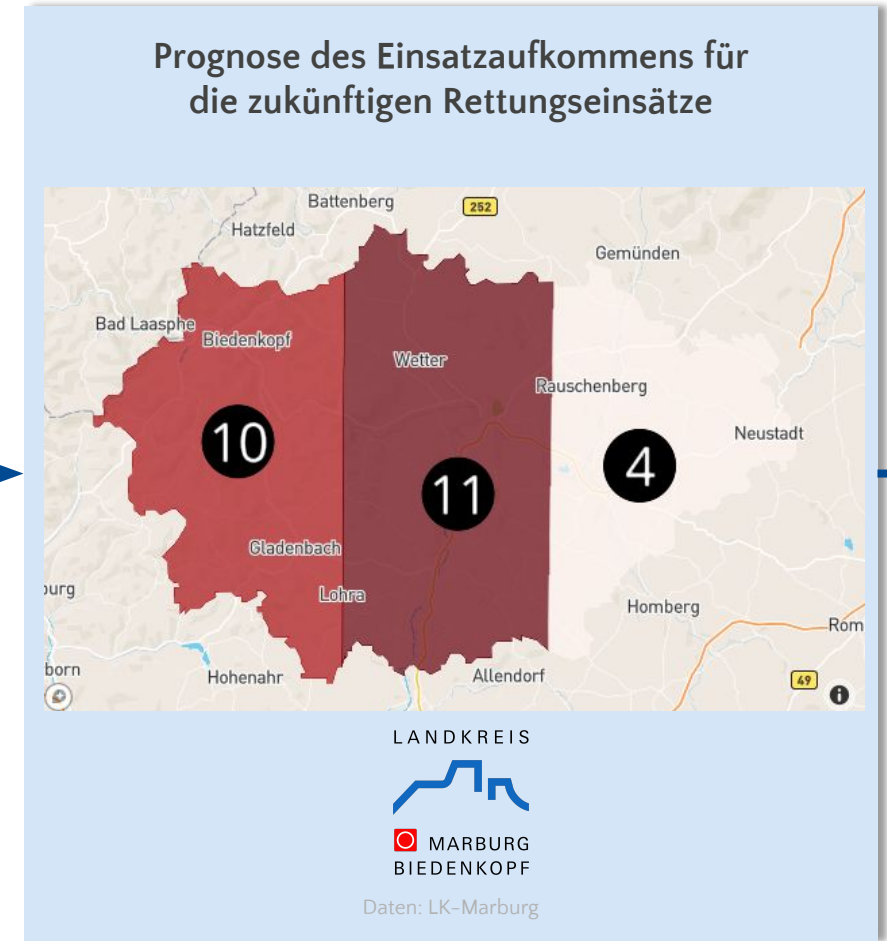
- Verlegefahrten zu reduzieren und
- die Anschlusseinsatzquote zu erhöhen



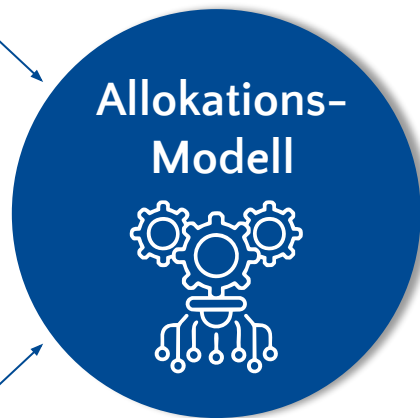
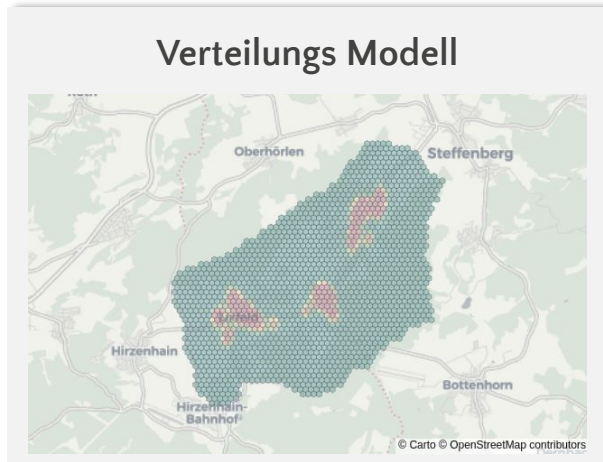
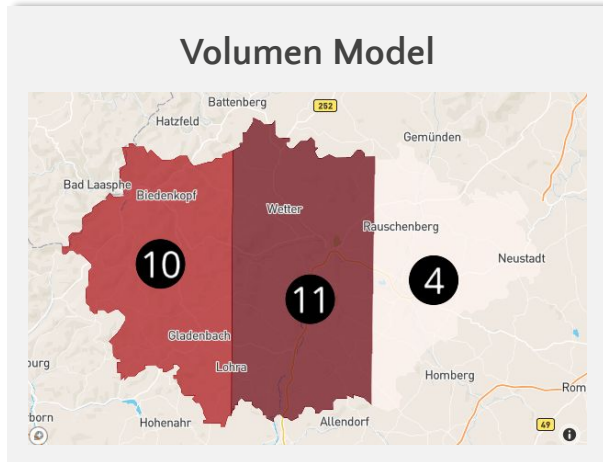
Inputs



Output



Inputs



Output



Ergebnisse seit Einführung der KI

Reduzierung der Verlegefahrten

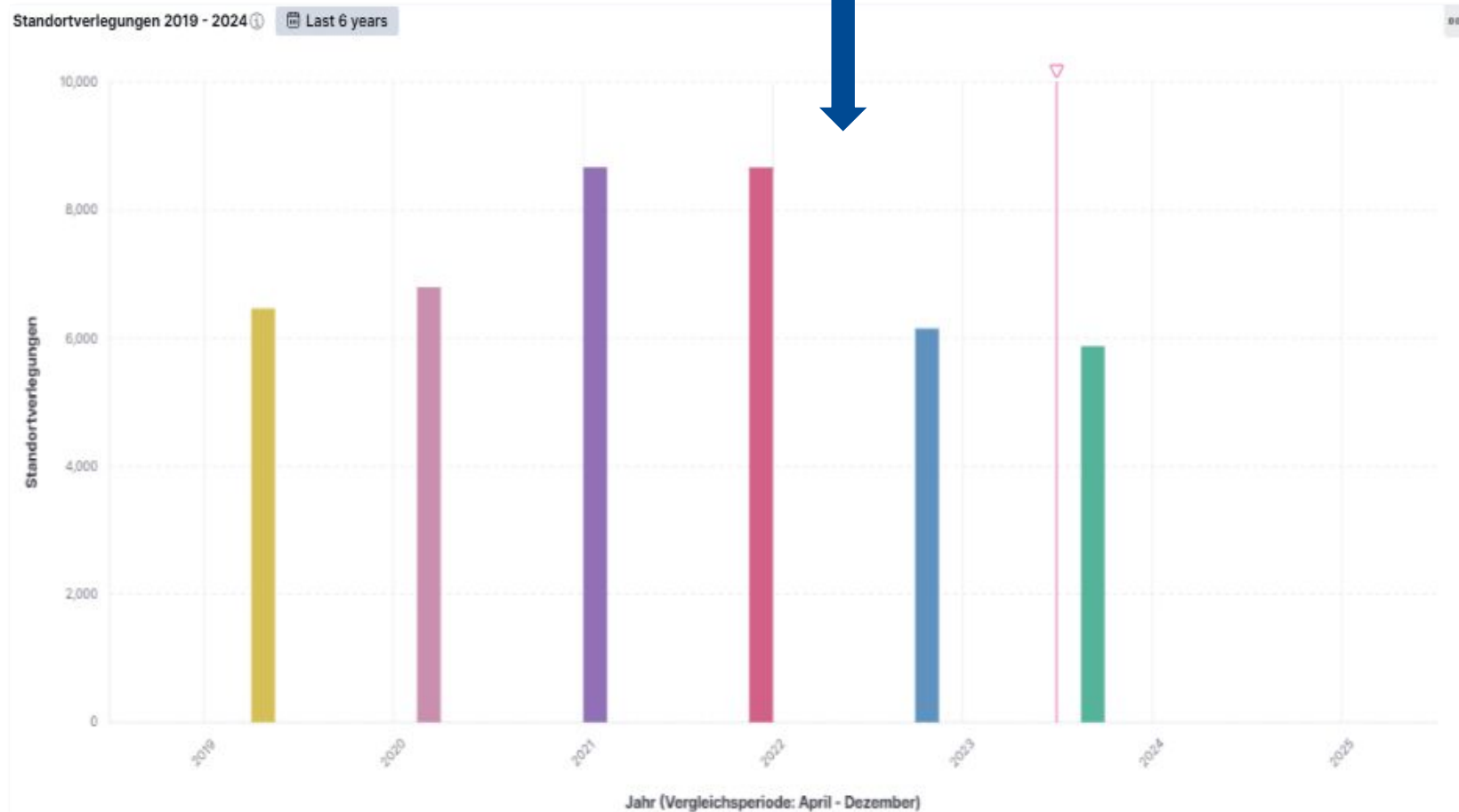
2022 bis 2023:

ca. 30%

2023 bis 2024:

ca. 5%

Einführung KI im Jahr 2023



Ergebnisse seit Einführung der KI

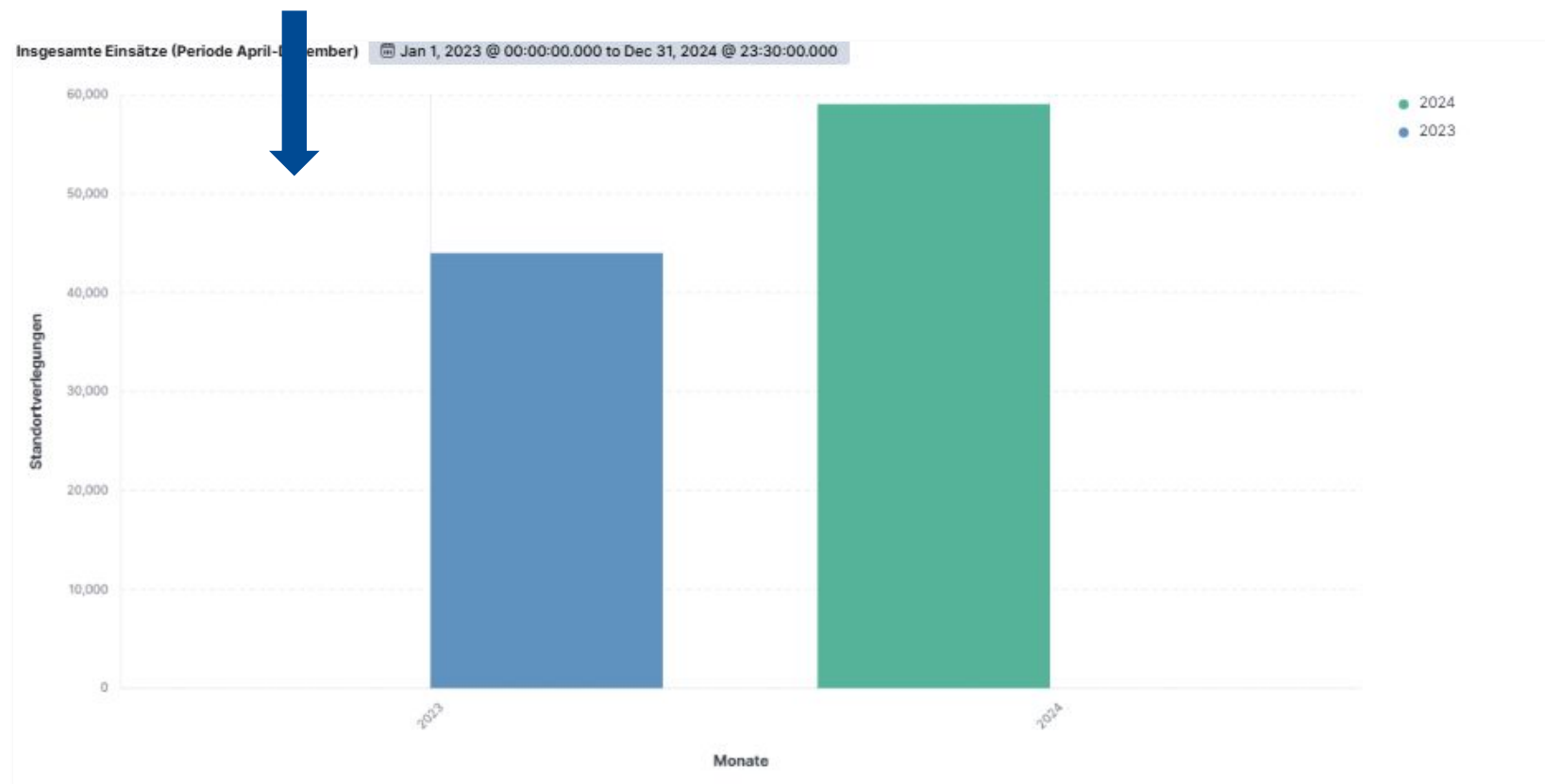
Erhöhung der Einsatzzahl

2023 bis
2024:

↑
ca.
34%

Keine Neubeschaffung
von Fahrzeugen

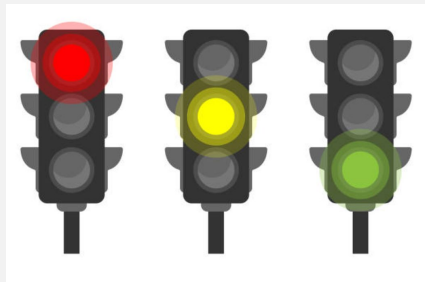
Einführung KI im Jahr 2023



Faktor Mensch



- Schnittstelle Mensch zu KI rein audiovisuell
- Keine automatische Dispo
- Klare Darstellung, ohne Interpretationsmöglichkeiten

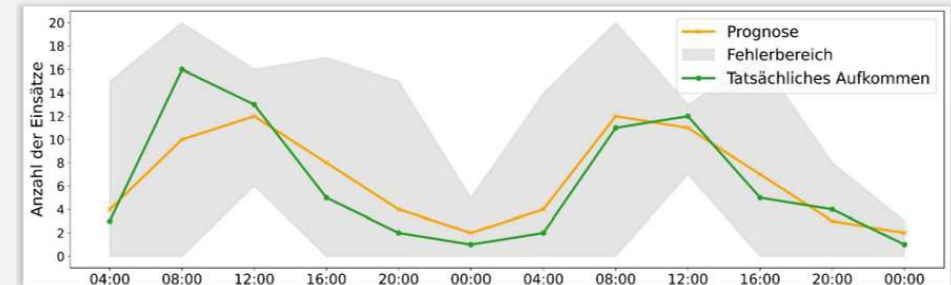


- Rechtssichere Grundlage zur Verwendung der Informationen
- Nachvollziehbar
- Dokumentation der Prozesse

Faktor Technik



- Evaluation, passen die Prognosen zur Realität?



- Gegenüberstellung Prognose/Auslasung/Vorhaltung
- Qualitätssicherung Prognose – Realität
- Grundlage ist eine hohe Datenqualität
- Einsatzdaten, Wetterdaten usw.
- Quantifizierte Unsicherheit (ISO / IEC 42)



Der Mensch entscheidet,
die KI gibt Empfehlungen

KI ist kein Produkt, sondern ein Prozess,
der etabliert werden muss

Vertrauen & Akzeptanz durch zusätzliche
Quantifizierung der Unsicherheit

KI muss lernen – Lernen benötigt Zeit!

KI unterstützt den Disponenten

KI erhöht die Qualität in der Leitstelle

blaulicht
| gyrophare bleu | girofaro blu |

DAS FACHMAGAZIN DER INFORMATIONSVERLAG SCHWEIZ GMBH

2/2025

TITELSTORY
SPIK 2025
Der Schweizer Polizei Informatik Kongress steht dieses Jahr ganz im Zeichen von KI

RÜCKLICHT WHEELCHAIR RESCUE
LERNEN, WORAUF BEI DER RETTUNG KÖRPERLICH BEHINDERTER MENSCHEN GEACHTET WERDEN MUSS.

AUS- UND WEITERBILDUNG
DAS 1. RESCUE FORUM WÄLLIS
Ein brandneues Bildungsangebot für Rettungskräfte

FOKUS
PROJEKT «MSK»
Weshalb, bis wann und wie die Schweiz ein «mobiles sicheres Mobilfunknetz» für BORS realisieren will

MITTEL & METHODEN
DIE ELZ DER ZUKUNFT PLANEN
Wie eine Einsatzleitzentrale geplant wird – und was KI damit zu tun hat



MITTEL & METHODEN KI-Lösungen in der Einsatzleitzentrale
Autoren: Thorsten Hansler und Jörg Rothweiler

«In der Einsatzleitzentrale der Zukunft spielen künstliche Technologien, insbesondere KI, eine grosse Rolle.»

Wie plant man eine Einsatzleitzentrale – und welche Rolle spielt KI dabei?

Viele Einsatzleitzentralen (ELZ) sind ins Alter gekommen. Dann ist der Entscheid «Neubau oder Nachrüstung?» nötig. Wir haben bei der IABG mbH nachgefragt, wie man Klarheit für eine langfristige Lösung schafft – und welche Rolle KI in der ELZ dabei spielt.

Geblieben sind zwei Dinge: Die hochkomplexen Systeme einer ELZ müssen ebenso hochverfügbar sein wie die in der ELZ tätigen Personen, die 24/7 unter teils hohem Stress Notrufe annehmen und adäquate Massnahmen auslösen, steuern und koordinieren müssen.

Damit dies gelingt, sind, zusätzlich zu einer genügend hohen Zahl motivierter und hochprofessioneller Kräfte, eine intelligente Infrastruktur, ergonomisch gestaltete Arbeitsplätze in sinnvoller Anordnung zueinander sowie eine hocheffiziente ICT, welche die Einsatzkräfte bestmöglich unterstützt und entlastet, unabdingbar.

Die erste Frage bei der Neukonzeption einer ELZ

Ist der Tag gekommen, an dem die Gesamtkonzeption einer ELZ überdacht werden muss, müssen viele Fragen beantwortet werden – und zwar mit Blick auf das «Heute» eben-

so wie mit Blick auf das «Morgen» und «Übermorgen». Immerhin hat eine ELZ einen Nutzungshorizont von 25 bis 30 Jahren, wovon bis zu zehn Jahre auf Planung und Realisierung entfallen.

Die Antwort auf die Frage, wo man beginnt, ist dabei noch mit am leichtesten zu beantworten: beim Flächenbedarf. Denn dieser entscheidet darüber, ob die ELZ im Bestand verbleiben kann, ob eine Erweiterung oder ob gar ein Neubau nötig sein wird.

So einfach es ist, diese erste Frage zu formulieren, so komplex ist deren Beantwortung. Denn bei der Ermittlung des Flächenbedarfs spielen die technologischen Lösungen, die vom Personal dereinst genutzt werden sollen, eine zentrale Rolle. Technologische Entwicklungen beeinflussen die Rollen und Aufgabengebiete stark – in der ELZ wie auch bei Führungs- und Einsatzmitteln. Mancherorts sinkt der Arbeitsaufwand, andernorts steigt er – und bisweilen entstehen völlig neue Aufgaben. Dies wiederum verändert die Kollaboration der Akteure in der ELZ – weshalb deren Arbeitsplätze künftig möglicherweise räumlich anders zueinander angeordnet werden sollten. Diese «Raumbeziehungen» indes müssen bekannt sein, damit ein gesamtheitlich stimmiges Raumkonzept (sowohl in der eigentlichen ELZ als auch hinsichtlich der angrenzenden Räumlichkeiten) entwickelt werden kann – wobei auch Aspekte der physischen Sicherheit (Sicherheitszonen, Zugangskontrollen), der Arbeitsplatzergonomie sowie der Rechtskonformität (geltende Richtlinien und Gesetze, z. B. hinsichtlich Brandschutz) zu berücksichtigen sind.

Fazit und Zusammenfassung



«Thorsten Hansler ist Programm Manager Leitstellen & Lagezentren / CTF50 der IABG mbH.»

Für eine vorausschauende Planung einer ELZ sind viele Aspekte zu berücksichtigen. Eine zentrale Rolle nimmt dabei das Technologieradar ein, das es ermöglicht, technologiebedingte Veränderungen bei den Rollen und Aufgabenbereichen zu erkennen, welche sich unmittelbar auf die Ausstattung und Anordnung der Arbeitsplätze und damit den Flächenbedarf und die Strukturierung einer ELZ auswirken. Aufgrund der nach wie vor rasanten Entwicklung im Bereich Digitalisierung sollte das Technologieradar in kurzen Intervallen (dreimal bis fünf Jahre) überprüft und adaptiert werden.

Wird der Einsatz von KI, die bereits heute hilfreiche Dienste leisten kann, in der künftigen ELZ erwogen, hilft AI Assurance bei der Prüfung erwoogener Lösungen und bei der Schaffung der nötigen Akzeptanz dieser Technologien.

Unabhängig von den Technologien muss bei der Planung einer ELZ auch an die benötigten Nebenumgebungen und die physische Sicherheit gedacht werden. Daher ist mit einem Planungs- und Realisierungshorizont von bis zu zehn Jahren zu rechnen.

Mehr Informationen erhalten Interessierte bei Thorsten Hansler, Programm Manager Leitstellen & Lagezentren / CTF50 der IABG mbH, Bonn, www.iabg.de, hansler@iabg.de, sowie am SPIK 2025, wo das Unternehmen mit einem Stand sowie einem Referat zum Thema «SafeAI – Absicherung von KI-basierten Systemen» vertreten sein wird.



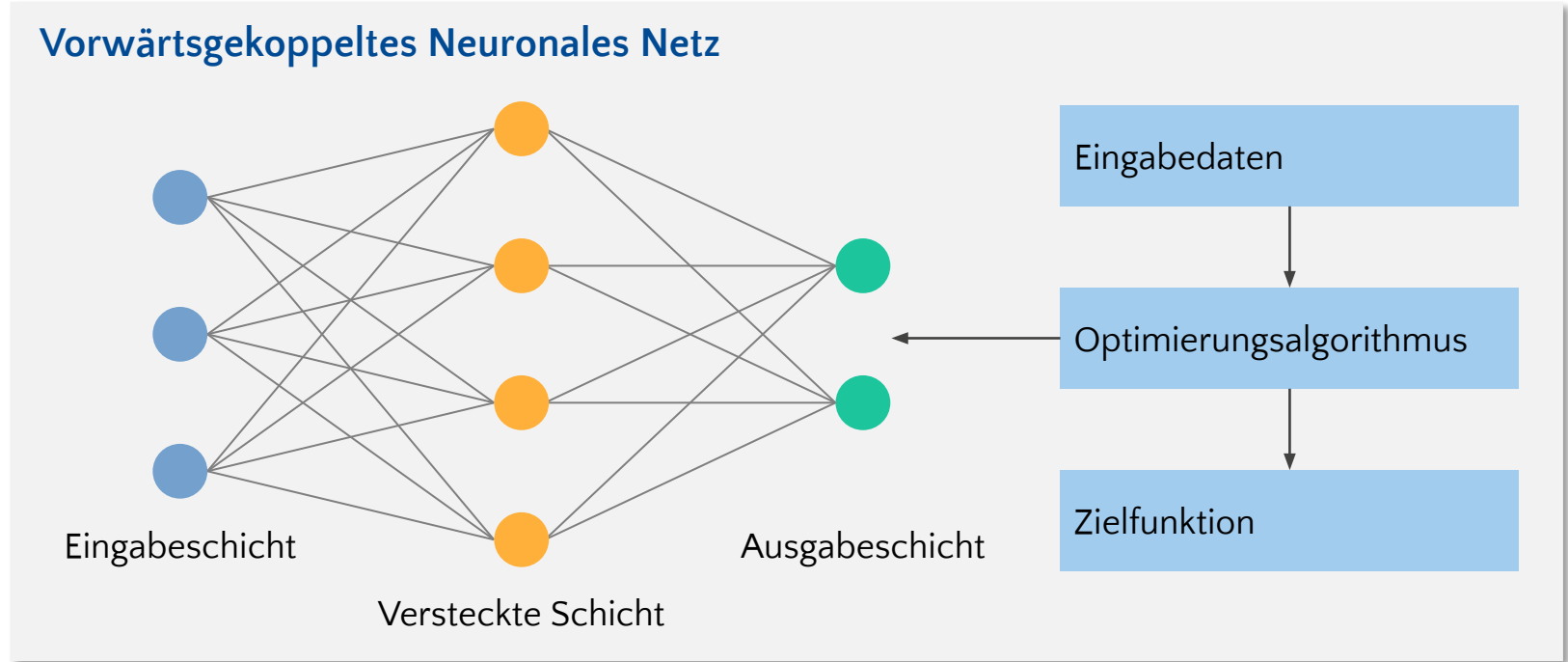
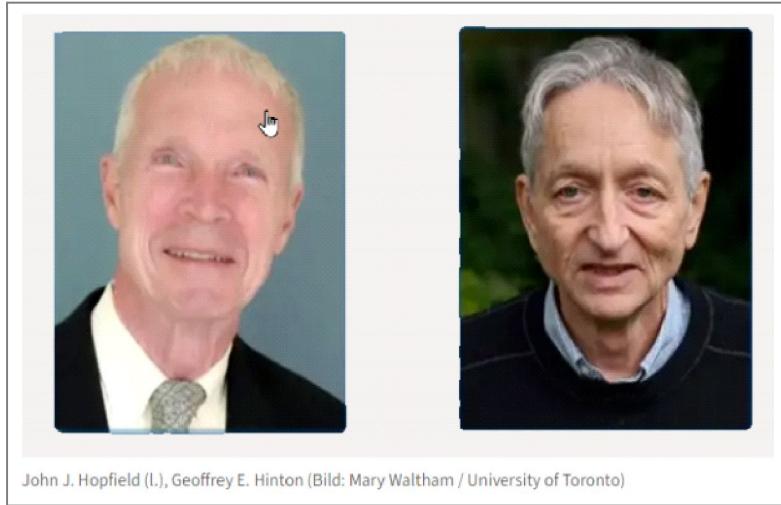
0

AI Assurance

"A fool with a tool is still a fool"

2

Nobelpreise 2024 in Physik und Chemie für maschinelles Lernen KI Basics



Stark vereinfacht: die Kombination aus **Architektur** (Feedforward Neural Network), **Modell** (Konkrete Ausprägung der Architektur), **Optimierungsalgorithmus** (Backpropagation), **Zielfunktion** (Quadratischer Fehler) und **Daten** als **Metapher** für den **Lernvorgang in biologischen neuronalen Netzen**.

Typische Architekturen der KI

(begleitet von einer Vielzahl Bibliotheken mit Zielfunktionen und Optimierungsverfahren)

Beispiel
e

Neuronale Netze

- 1957 **Perceptron**, das erste künstliche neuronale Netz
- 1982 Einführung von **Rekurrenten Neuronalen Netzen**
- 1997 Einführung von **LSTM** (Long Short-Term Memory) Netzen
- 2006 Durchbruch im **Deep Learning** beim Training tiefer neuronaler Netze (viele Schichten / Parameter)
- 2024 **Kolmogorov-Arnold Netze** (Basierend auf Arbeiten von A.N. Kolmogorov in 1956)

Objekterkennung

- 1980 Neocognitron, ein hierarchisches neuronales Netz für visuelle Mustererkennung
- 1989 CNN LeNet, die erste erfolgreiche Anwendung von **Convolutional Neural Networks**
- 2012 AlexNet gewinnt den ImageNet-Wettbewerb: bedeutender Fortschritt bei tiefen CNNs
- 2015 ResNet führt tiefes residuales Lernen für Bilderkennung ein

Sprache-zu-Text

- 1998 Erste Software zur kontinuierlichen Spracherkennung mit großem Vokabular
- 2014 **Encoder-Decoder-Architektur** für maschinelle Übersetzung
- 2013 Mit **Word2Vec** gelingt effiziente Erfassung von Semantik

Natürliche Sprachverarbeitung / LLM

- 2017 **Transformer-Modell**, basierend auf Encoder-Decoder-Architektur
- 2018 **BERT** (Bidirectional Encoder Representations from Transformers)
- 2020 GPT-3, ein Sprachmodell mit 175 Milliarden Parametern
- 2022 ChatGPT, eine Konversations-KI basierend auf GPT-3.5
- 2023 GPT-4 □ zunehmender „Hunger an Ressourcen“
- 2025 Januar: DeepSeek V3 (671 Milliarden Parameter)

Vertrauen & Akzeptanz

2024 **EU AI Act**

Wettstreit LLM:
Open Source versus proprietäre Lösungen
<https://huggingface.co/>

Typische Anwendungsfälle für KI am Beispiel Militär

Aufgaben fallen bei vielen Systemen an, Lösungen wollen verschiedene KI Technologien nutzen

Missionsplanung und Durchführung	Zieldetektion, -erkennung und -identifikation (DRI)	Situationsbewusstsein (Situational Awareness)	Navigation und Steuerung	Cyber Security und Resilienz
<ul style="list-style-type: none"> • Missionsplanung mit Hilfe von Reinforcement Learning • Routenoptimierung 	<ul style="list-style-type: none"> • Bildklassifizierung • (Multi-)Objekterkennung 	<ul style="list-style-type: none"> • Prädiktive Analytik • Autonome Überwachung • Sprache-zu-Text-Anwendungen 	<ul style="list-style-type: none"> • Optimierung Manned/Unmanned Teaming • Autonome Routenplanung 	<ul style="list-style-type: none"> • Jamming-Detektion • Erkennung von Hackingversuchen

KI Technologien

- | | | | | |
|--|---|---|--|--|
| <ul style="list-style-type: none"> • Hybrid (KI plus Graphentheorie) | <ul style="list-style-type: none"> • Convolutional Neural Network • Transformer | <ul style="list-style-type: none"> • Recurrent Neural Network • Transformer • Hybrid (KI plus Graphentheorie) | <ul style="list-style-type: none"> • Recurrent Neural Network • Reinforcement Learning • Hybrid (KI plus Graphentheorie) | <ul style="list-style-type: none"> • Convolutional Neural Network • Reinforcement Learning |
|--|---|---|--|--|



Problemlösung

Früher

Heute

Forschung

So wenig Daten und Rechenkapazität ... Was soll ich tun?

Definiere Rahmenbedingungen, entwickle **ein** Modell und beweise (mathematisch), dass das Modell die Lösung des Problems ist. Nutze Daten, um die Parameter des Modells zu schätzen.

- + Mathematischer Beweis
- Mangelnde Passung des Modells an die Realität

Source: Midjourney *"/imagine a mathematician writing a lengthy formula on the chalk board"*

Empirie

So viele Daten und Rechenkapazität ... Was soll ich tun?

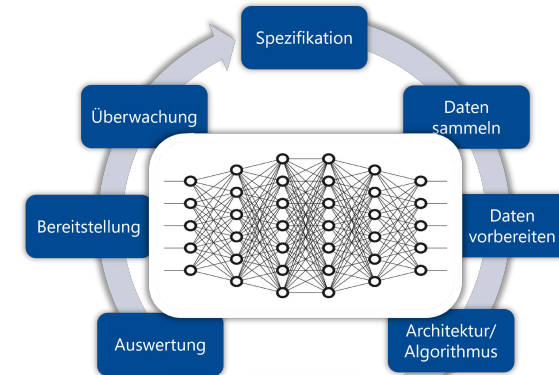
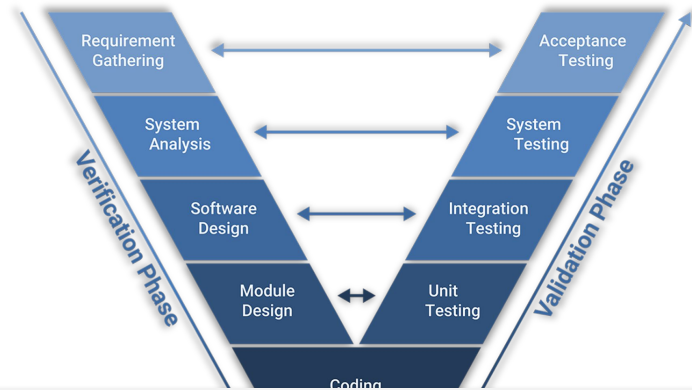
Wähle eine Architektur und Zielfunktion und finde durch Nutzung von Daten und Variation von Architektur- und Modell-Parametern eine Lösung, die das Problem bestmöglich löst.

- + Meist gute Passung des Modells an die Realität
- Fehlender "Beweis"

Source: Midjourney *"/imagine an ai specialist using data to find a solution"*

V-Modell versus KI-Zyklus

Ist KI *automatisch* die bessere Lösung?



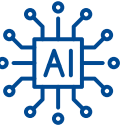
"Typische" **Ingenieurlösungen**, z.B.
 Regelungstechnik: Kalman Filter
 Zeitreihen: Autoregressive Modelle
 Encoder / Decoder: Hauptkomponentenanalyse (PCA)

Viel **Empirie** am Werk (leider):
 Architektur, Optimierungsverfahren, Zielfunktion, Daten?
 Oft fehlt Bezug zur einer typischen Referenzlösung
 Leistungsversprechen meist unklar

**EU AI Act:
 Vertrauen & Akzeptanz in KI**

Für die **Bewertung, Prüfung** und **Beurteilung** von KI-Systemen mit Blick auf Sicherheit und Vertrauenswürdigkeit sind (**neue**) **Methoden und Standards** erforderlich!

EU Artificial Intelligence Act



AI Assurance bezeichnet den Ansatz zur Sicherstellung, dass KI-Systeme ...

... sicher

Ziele der AI Assurance

- Stärkung des **Vertrauens** in KI-Systeme
- Förderung der **Akzeptanz** bei den Anwendern und Stakeholdern
- Minimierung von **Risiken** und potenziellen Schäden

... zuverlässig

Schlüsselkomponenten

- **Transparenz:**
Nachvollziehbarkeit von Entscheidungen
- **Robustheit:**
Widerstandsfähigkeit gegen Angriffe und Störungen
- **Ethik:**
Vermeidung von Diskriminierung und Verzerrungen
- **Compliance:**
Einhaltung gesetzlicher Vorgaben und Standards

... fair &

Anwendungsszenarien im Militär/Sicherheitsbehörden

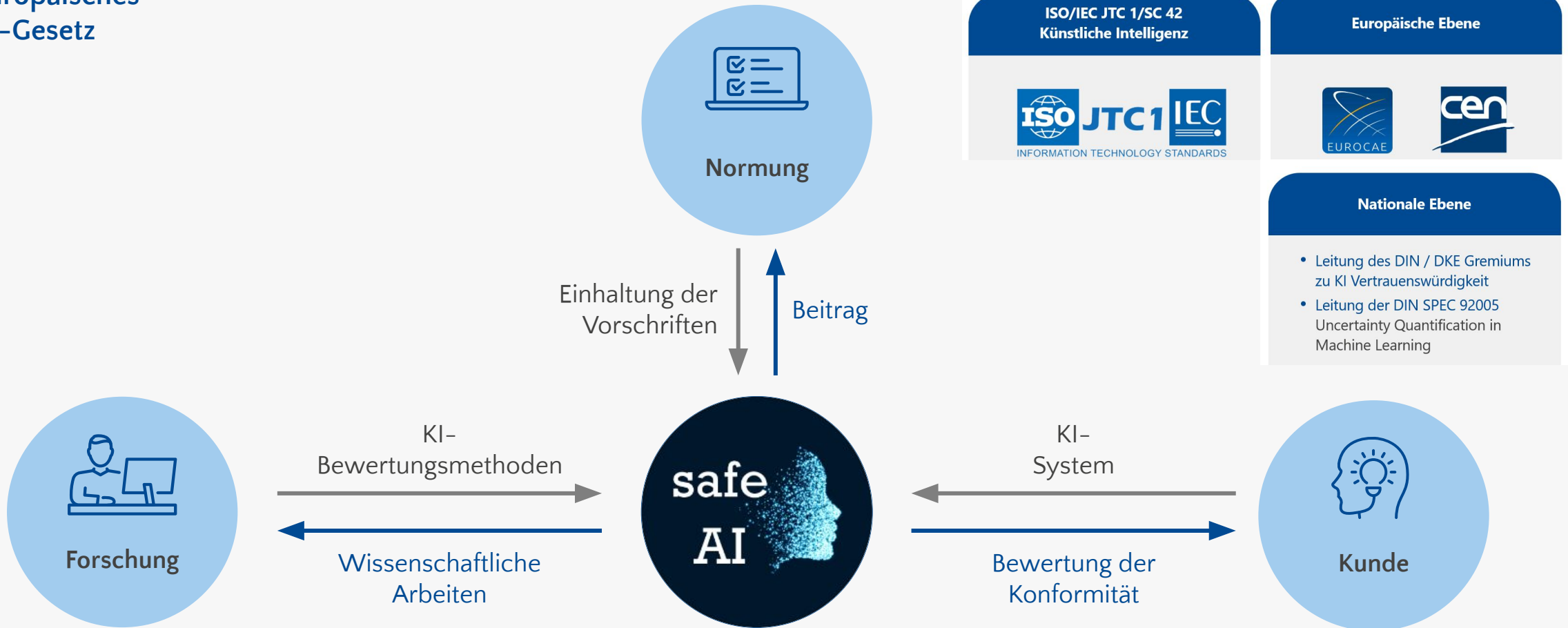
- Einsatz von KI zur Unterstützung von **Entscheidungsprozessen** in Echtzeit
- Entwicklung sicherer, **autonomer Systeme** für Aufklärung und Schutz
- Schutz militärischer Netzwerke und Systeme vor Cyberangriffen durch KI-basierte **Anomalie-Erkennung und automatisierte Abwehr-mechanismen**
- Einsatz von KI zur **Früherkennung** und **Prävention** von physischen und digitalen Angriffen auf kritische Infrastrukturen
- Simulationsbasierte Szenarien zur **Reduzierung von Risiken** bei der Entwicklung neuer Technologien.

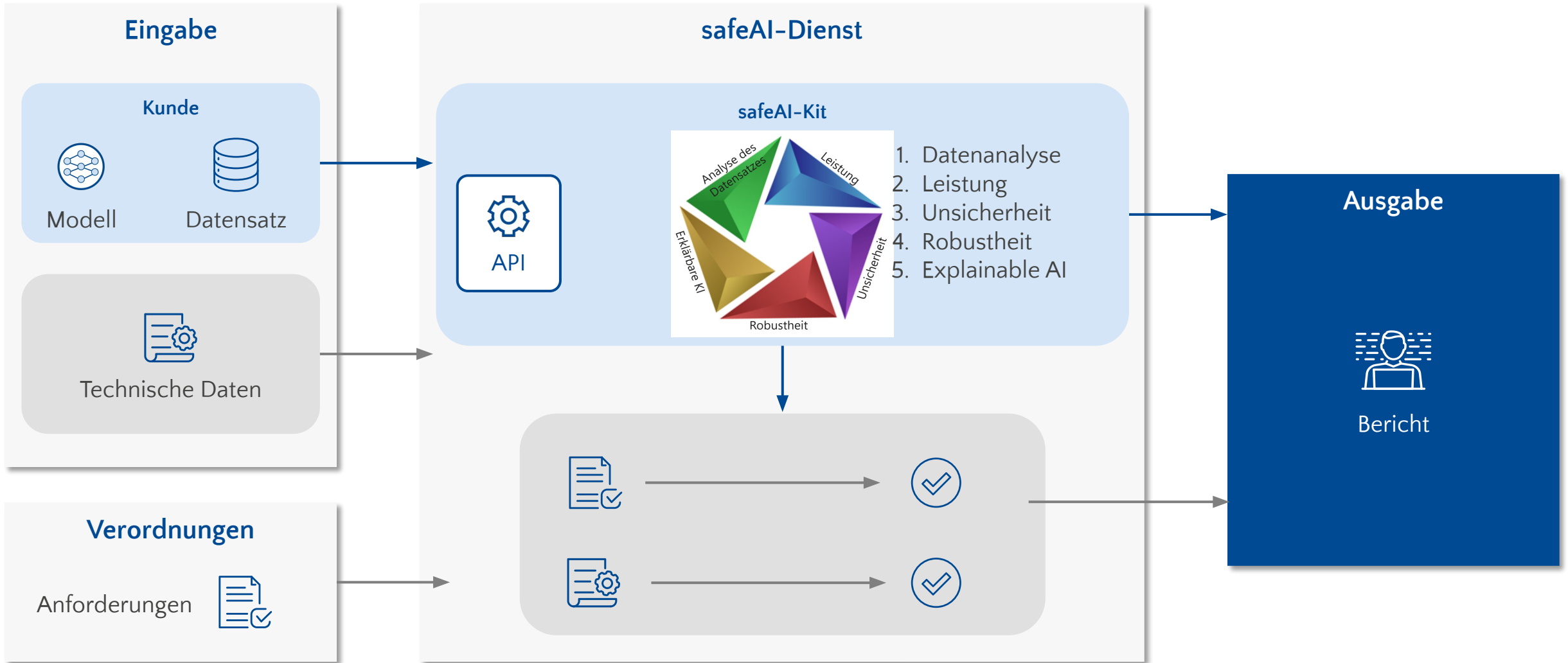
... rechtskonform sind

Herausforderungen

- **Schutz** sensibler Daten und Abwehr von Cyberbedrohungen
- **Nachvollziehbarkeit** von KI-Entscheidungen
- Einhaltung **gesetzlicher und normativer Vorgaben**
- **Robustheit** und Integration in bestehende Systeme
- Sicherstellung von qualitativ hochwertigen und vollständigen Daten
- **Anpassung** an sich ändernde Bedrohungen

Europäisches KI-Gesetz





Zusammenfassend: ein fundiertes und fachlich-übergreifendes Verständnis ist hilfreich, um das Beste *aus* und *mit* KI zu machen

- **Architekturen / Modelle / Zielfunktionen / Daten Optimierungsverfahren verstehen**
- **KI ist Software (!)**
SW-Entwicklung und -Prozess, Kubernetes, GitHub, KI-Bibliotheken, Nutzung von Open Source SW
- **Konformitätsbewertung**
 - Funktionale Sicherheit, Referenzmodell und quantifizierte Unsicherheit sollten Minimal-anforderungen sein
 - Offenlegung: Architektur, Modell, Daten, Methoden, SW-Entwicklungsprozess

- Einbettung / Kombination mit weiteren disruptiven Technologien: **Cloud Technologien**
- **Ressourceneffizienz**: eine Lösung sollte so einfach wie möglich sein (!)

- **Moderne Lernplattformen** bieten beeindruckende Lerner(l/g)ebnisse:
 - <https://www.coursera.org/>
 - <https://www.deeplearning.ai/>

Wie sicher ist künstliche Intelligenz?

Wir entwickeln **Lösungen** für die **Evaluierung** und **Prüfung** von KI-Systemen basierend auf neuesten Erkenntnissen aus **KI-Forschung**, **-Standardisierung** und **Regulierung** sowie auf unserer langjährigen Erfahrung bei **Test-**, **Analyse-** und **Zertifizierungsprozessen**.

Unser **Leistungsversprechen**:

- **Beratung** bei der Erfüllung von KI Standardisierung, Normierung und Regulierung inkl. der relevanten Prozesse
- **Evaluierung und Prüfung** der Leistung und Sicherheit von KI-Systemen und Datensätzen. Beispiel: KI in der Leitstelle.



Vielen Dank

Ihre Ansprechpartner

IABG mbH

Einsteinstr. 20
85521 Ottobrunn

Tel. +49 89 6608-0
Fax +49 89 6608-2220

info@iabg.de
www.iabg.de

IABG mbH, NL Bonn

Königswintererstr. 552b
53227 Bonn



Thorsten Hansler
Programm Manager
KI in der Leitstelle

hansler@iabg.de
Telefon: +49 228 91767-23



Dr. Willfried Wienholt
Ressortleiter InfoKom
Sichere Cloud & KI

wienholt@iabg.de
Telefon: +49 151 74431308



00

Unternehmen IABG

Europäisches Technologieunternehmen im Herzen Europas.

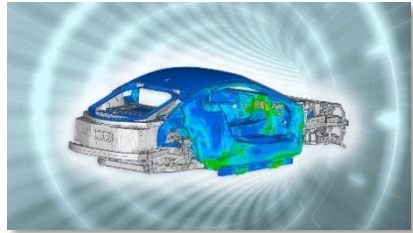
Unternehmensprofil.



Würde ich weglassen: Umsatz 2023 ist „alt“ und die Zahlen von 2024 sind noch nicht offiziell. Außerdem kann man das besser auf der Tonspur bringen, finde ich (spart Zeit).

> Name	Industrieanlagen-Betriebsgesellschaft mit beschränkter Haftung
> Gründung	1961
> Hauptsitz	Ottobrunn bei München, Deutschland
> Vorsitzender	Engelbert Kupka MdL a. D.
> Aufsichtsratsmitglieder	Prof. Dr. Rudolf F. Schwarz Thomas Köhler
> Mitarbeiter	Ca. 1.200
> Umsatz	Ca. 203 Mio. € (2023)
> Standorte	11
> Geschäftsfelder	<ul style="list-style-type: none"> • Automotive • InfoKom • Mobilität & Energie • Umwelt & Geodaten • Luftfahrt • Raumfahrt • Verteidigung & Sicherheit

Wir unterstützen Analyse, Konzeption, Realisierung und Einsatz von Hochtechnologie über deren gesamten Lebenszyklus.



Automotive

Versuch & Simulation; Entwicklung und Bau kundenspezifischer Prüfsysteme; Methoden-entwicklung & Virtuelle Qualifikation



InfoKom

Beratung öffentlicher und industrieller Kunden mit sicheren vernetzten Informations- und Kommunikationssystemen



Mobilität & Energie

Absicherung der Elektromobilität für Straße und spurgeführten Verkehr: Batterien, H2-Brennstoff-zellen, Antriebe, induktives Laden; Qualifikation alternativer Energien



Geodaten & Umwelt

Geodaten/Geoinformation für Katastrophenschutz & Krisenmanagement, Clean Energy, Land & Utility Management, Umweltengineering; Altlastensanierung & Flächenrecycling



Luftfahrt

Qualifikation von Bauteilen, Komponenten und komplexen Gesamtsystemen; Lebensdauer-vorhersagen; Digital Twins & virtuelle Qualifikation



Raumfahrt

Umwelt- & Qualifikationstests von Satelliten und Trägersystemen im Raumfahrtzentrum; Beratung zu Raumfahrtprogrammen; New-Space-Anwendungen



Verteidigung & Sicherheit

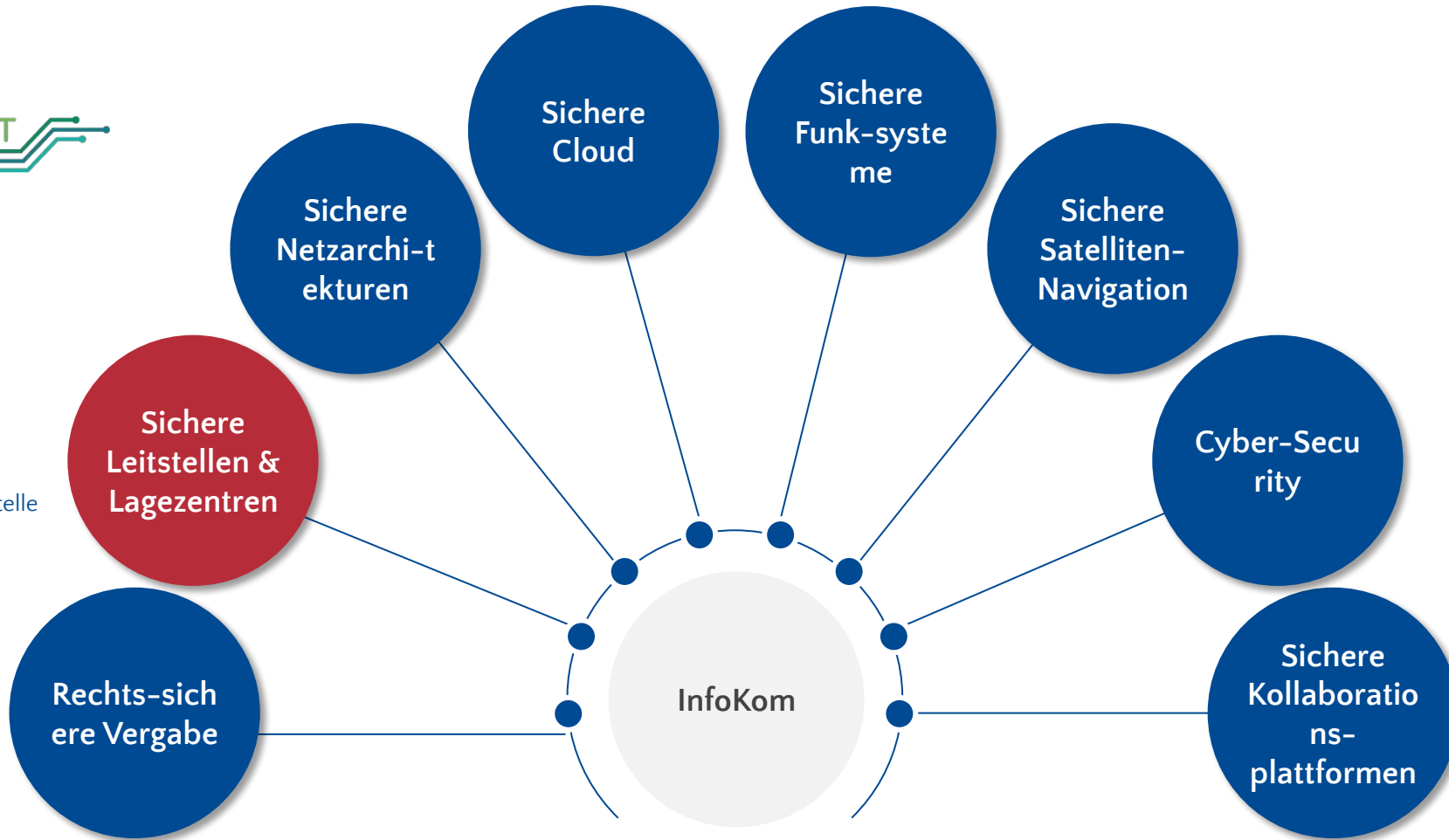
Unabhängige Beratung, Prüfdienstleistungen und Simulation für Streitkräfte in allen operationellen Dimensionen und Fähigkeits-domänen



Innovation

Innovationszentrum als Inkubator für das zukünftige Leistungsportfolio mit Fokus auf Digitalisierung, Data Science & KI sowie vernetzte, elektrische, autonome Systeme

Mitgliedschaften



BSI-zertifizierter IT-Dienstleister



