TÜV AUSTRIA

Leading Innovation /3

Sichere Anwendung künstlicher Intelligenz

Impulse aus dem TÜV AUSTRIA Innovationsbeirat

IMPULSE AUS DEM
TÜV AUSTRIA INNOVATIONSBEIRAT
BAND 3
SICHERE ANWENDUNG VON KÜNSTLICHER INTELLIGENZ
DEZEMBER 2019

TÜV AUSTRIA GROUP
INNOVATIONSMANAGEMENT
TÜV AUSTRIA-Platz 1
2345 Brunn am Gebirge
innovation@tuvaustria.com
www.tuvaustria.com

Leading Innovation

Impulse aus dem TÜV AUSTRIA Innovationsbeirat

3

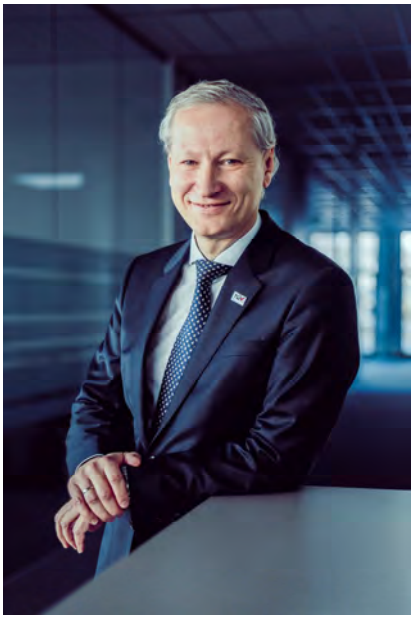
Sichere Anwendung von Künstlicher Intelligenz

Dezember 2019

Textbeiträge: Franz Kühmayer | Grafiken: zukunftsinstitut | Redaktion: Christoph Schwald
Fotos: Andreas Amsüss, Saskia Jonasch (S.4), Shutterstock (Liu zishan, CoreDESIGN)

Sichere Anwendung von Künstlicher Intelligenz

Eine Einführung von DI Dr. Stefan Haas, CEO TÜV AUSTRIA Group



Künstliche Intelligenz (KI) gilt als der stärkste Treiber der digitalen Transformation. Leistungsfähige Rechner- und Datenübertragungskapazitäten verhelfen der an sich nicht neuen Technologie zu einer schnell wachsenden Verbreiterung in immer mehr Wirtschafts- und Lebensbereichen. Als die Schlüsseltechnologie der kommenden Jahre hat sie das Potenzial nicht nur Märkte neu zu gestalten, sondern auch die Gesellschaft zu beeinflussen. Laut Marktforschungsunternehmen Gartner verdreifachte sich 2018 die Zahl der Unternehmen, die KI einsetzen. Die Bitkom unterstellt der Technologie sogar ein jährliches Wachstum von fast 40 Prozent, wodurch der europäische KI-Markt bis 2020 auf 10 Milliarden Euro steigen wird.

In der Öffentlichkeit wird der Einsatz von Künstlicher Intelligenz zuweilen im dystopischen Ausmaß diskutiert, was davon ablenkt sich zu vergegenwärtigen, in welchen alltäglichen und teilweise höchst persönlichen Bereichen des Lebens die Verwendung von KI bereits zur Normalität geworden ist: In Online-Shops werden uns Produkte vorgeschlagen, Streaming-Dienste empfehlen uns die passende Musik und selbstlernende Systeme steuern nicht nur die Sprach- sondern auch die Gesichtserkennung in Smartphones. Auch wenn solche Anwendungen, unter anderem im Licht von Datenschutzverordnungen, nicht mehr ganz so harmlos erscheinen mögen, wird eine ganz andere Kritikalitätsstufe erreicht, wenn künstliche Intelligenz in Bereichen Entscheidungen trifft, die Auswirkungen auf die persönliche Sicherheit haben können. Als Beispiel muss hier nicht immer die Zukunftsvision des vielzitierten Autonomen Fahrens herangezogen werden; schon im industriellen Umfeld muss man Aussagen einer künstlichen Intelligenz vertrauen können, etwa wie lange kritische Infrastrukturen oder Maschinen gefahrenfrei ohne Wartung betrieben werden können.

Im Strategiedokument „Künstliche Intelligenz für Europa“, stellte die EU-Kommission bereits 2018 fest, dass ein geeigneter ethischer und rechtlicher Rahmen geschaffen werden muss, da KI ein Klima des Vertrauens erfordert. Die deutsche Bundesregierung identifizierte in ihrer KI-Strategie die Standardisierung als zentrales Handlungsfeld und schließlich findet sich im Ergebnisbericht der österreichischen Initiative zur Erarbeitung einer nationalen KI-Strategie ebenfalls die Forderung, dass die Rechtssicherheit sowohl für Anwender als auch für Hersteller rund um Haftung, Zertifizierung und Datenschutz sichergestellt werden muss.
Um diesen Forderungen nachkommen zu können, braucht es aber zunächst neue Methoden, um KI-basierte Systeme in ihrer Funktionalität überhaupt als sicher und beherrschbar einstufen zu können. Dabei muss sowohl die funktionale Sicherheit (Safety), als auch die IT-Security während der Entwicklung und in der Nutzung solcher Systeme betrachtet werden.
Entlang mehrerer Initiativen entwickelt der TÜV AUSTRIA bereits heute entsprechende Werkzeuge, um morgen die Industrie vollumfänglich bei der Absicherung KI-basierter Systeme unterstützen zu können. Dabei wird das Fachwissen und die praktische Markterfahrung der TÜV AUSTRIA Experten mit dem nötigen technischen Knowhow von Technologieführern verbunden. So wird unter anderem mit dem Team des Machine Learning Instituts der Johannes-Kepler-Universität in Linz unter der Leitung von Professor Sepp Hochreiter, einem der gefragtesten Experten zum Thema Künstliche Intelligenz, gemeinsam an Lösungen gearbeitet.

In der aktuellen Sitzung des TÜV AUSTRIA Innovationsbeirats haben wir uns gemeinsam mit Professor Hochreiter und unter der Moderation von Franz Kühmayer, Trend- und Zukunftsforscher am renommierten Think Tank des Zukunftsinstituts, ausführlich dem Themenkreis „Sichere Anwendung von Künstlicher Intelligenz“ gewidmet. Wesentliche Auszüge wollen wir mit Ihnen im Folgenden teilen. Lernen Sie dabei, zu welchen Einschätzungen und Ausblicken führende Innovations- und Technologieführer aus Industrie und Wissenschaft kommen.

TÜV AUSTRIA INNOVATIONSBEIRAT

O. Univ. Prof. DI Dr. Sabine Seidler
Rektorin der TU Wien

– Seit 10/2011: Rektorin der Technischen Universität Wien
– Aufsichtsrat des Helmholtz-Zentrums Berlin für Materialien und Energie GmbH
– Aufsichtsrat der AMAG (Austria Metall AG)
– Kuratoriumsvorsitzende des Naturhistorischen Museums Wien
– Mitglied im Verwaltungsrat des Österreichischen Gewerbevereins

Die TU Wien ist Österreichs größte naturwissenschaftlich-technische Forschungs- und Bildungseinrichtung mit 28.918 Studierenden (Stand 01/2018).

Johann Christof
CEO und Eigentümer Christof Industries Firmenverbund

– Seit 2015 CEO und Eigentümer Christof Industries Global GmbH
– 2003-2015 CEO Christof Holding AG Mitbegründer und Geschäftsführer bei J. Christof GmbH
– 2011: Jahrgangscaptain des Lehrganges Innovationsmanagement an der Fachhochschule Campus02

Christof Industries errichtet und serviciert weltweit Knowhow-getrieben Industrieanlagen für die produzierenden Branchen und die Energiewirtschaft mit dem Schwerpunkt auf Umsetzung von Kreislaufwirtschaft.
Das Unternehmen beschäftigt ca. 2.400 Mitarbeiter weltweit (Stand Q2 2019)

Prof. Dr. Volker Gruhn
Vorsitzender Aufsichtsrat und Mitbegründer Adesso AG

– Vorsitzender Aufsichtsrat und Mitbegründer Adesso AG
– Inhaber des Lehrstuhls für Software Engineering an der Universität Duisburg-Essen
– Seit 1. März 2019 Hochschulrat der Universität Leipzig

Die Adesso AG ist ein internationaler Anbieter von Beratungsleistungen, IT-Dienstleistungen und Software und beschäftigt 3.715 Mitarbeiter (Stand Q2 2019) an 30 Standorten.

DI Franz Mittermayer
Vorstandsdirektor EVN AG

– Seit Oktober 2017 Vorstand der EVN AG
– Verantwortlich für die Segmente Erzeugung, Netze, Umwelt und für die Konzernfunktionen Informations- Verarbeitung, Beschaffung und Einkauf sowie Revision

Die EVN AG ist Anbieter für Strom, Gas, Wärme, Trinkwasserver- sowie Abwasserentsorgung und thermische Abfallverwertung auf Basis modernster Infrastruktur, Betrieb von Netzen für Kabel-TV und Telekommunikation sowie Anbieter verschiedener Energiedienstleistungen für Privat- und Businesskunden sowie für Gemeinden Das Unternehmen beschäftigt ca. 7.000 Mitarbeiter (Stand Q3 2019)

DI Dr. Stefan Poledna
Vorstand und Mitbegründer TTTech Computertechnik AG

– Vorstand und Mitbegründer der TTTech Group: verantwortlich für die Technologie Roadmap des Unternehmens, alle forschungsrelevanten Themen, IT, DevOps und Qualität
– 1998 Gründer TTTech Computertechnik AG
– Universitätsdozent für Dependable Computer Systems an der TU Wien
– 2013 zum Österreicher des Jahres in der Kategorie „Unternehmertum“ gewählt (Vergabe durch „diePresse“)

TTTech Computertechnik AG ist führender Lösungsanbieter für zuverlässige Netzwerklösungen, basierend auf zeitgesteuerter Technologie und modularen Sicherheitsplattformen, entwickelt Lösungen für komplexe Probleme für Embedded System Designs von cyber-physischen Systemen und dem Internet der Dinge. Weltweit beschäftigt das Unternehmen rund 1.700 Mitarbeiter (Stand 2018)

DI Armin Rau
Geschäftsführer TRUMPF Maschinen Austria GmbH + Co KG

– Von 2004 bis 2019 Geschäftsführer der TRUMPF Maschinen Austria GmbH + Co. KG.
– von 1982 bis 2003 in der TRUMPF Entwicklung tätig - verantwortlich für Steuerungstechnik, Software und Sensorik
– Aufsichtsrat Firma Engel

TRUMPF Maschinen Austria ist eine Tochtergesellschaft der deutschen TRUMPF Gruppe und beschäftigt 660 Mitarbeiter (Stand 2018). Das Unternehmen ist Kompetenzzentrum für Biegetechnologie der TRUMPF Gruppe. 2011 staatlich ausgezeichneter Ausbildungsbetrieb und Fabrik des Jahres, 2012 Staatspreis Innovation

KI in Zahlen

15.7 Billionen USD
Einfluss von KI auf das Wachstum der Weltwirtschaft bis zum Jahr 2030
Das ist mehr als die aktuelle Wirtschaftsleistung von China und Indien zusammengezählt. Ein Drittel davon wird aus höherer Produktivität stammen, zwei Drittel aus neuem Absatz.
Quelle: PwC, Sizing the Prize, 2017

25 Milliarden USD
weniger Kreditkartenbetrug, pro Jahr
Die Zahl stammt nur von VISA alleine. Das Unternehmen schätzt, im abgelaufenen Geschäftsjahr durch den Einsatz von KI massiv gegen Kreditkartenbetrügereien vorgegangen zu sein.
Quelle: Payments Journal, Using AI to combat fraud at the speed of light, 2019

47 Prozent
Erfolgsrate von KI-Projekten
Etwa die Hälfte der Führungskräfte erwarten sich bedeutende Resultate aus KI Projekten, die ihr Unternehmen gestartet hat. Eine gewisse Ernüchterung, denn noch im Jahr davor lag der Anteil bei 62%
Quelle: KPMG, Controlling AI, 2019

58 Millionen Jobs
Mehr Jobs, netto
KI und andere digitale Technologien werden Arbeitsplätze vernichten. Aber sie schaffen auch neue, besser qualifizierte und höherwertige. Die Nettobilanz bis 2022 wird knapp 60 Millionen zusätzlicher Arbeitsplätze ausmachen.
Quelle: World Economic Forum, The Future of Jobs, 2018

114 Millionen Bürger
Anzahl der US-Amerikaner, die bereits Sprachassistenten in ihrem Auto benutzt haben
Fast die Hälfte aller Bürger der USA haben bereits auf Sprachassistenten in ihrem Auto zurückgegriffen. Das sind mehr als doppelt soviele, wie derartige Systeme zu Hause benutzen.
Quelle: Voicebot, In-Car Voice Assistant Consumer Adoption Report, 2019

20 Millionen Roboter
Weltweite Anzahl der digitalen Arbeitskräfte
70 Prozent der Heerschar von Robotern sind in China aktiv.
Quelle: Oxford Economics, How Robots change the world, 2019

4.400 Nachrichten
Wirtschaftsnachrichten-Texte, die von KI pro Quartal verfasst werden.
Menschliche Reporter schreiben etwa 300 Wirtschaftsnachrichten-Texte pro Quartal. Die KI der Firma Automated Insights verfasst in der gleichen Zeit 4.400 solcher Artikel für die Nachrichten Agentur Associated Press. Andere Medien, die vergleichbare Systeme einsetzen, sind Bloomberg, Washington Post, CNBC und viele andere.
Quelle: AP, 2015

40 Tage
bis zum perfekten Go-Spieler
AlphaGo Zero brauchte etwas mehr als einen Monat, um das hochkomplexe Spiel Go zu beherrschen. Ohne jegliche menschliche Interaktion und ohne historische Daten, nur durch selbstlernende Algorithmen erreicht das System 5.185 Elo-Punkte, der Messzahl der Spielstärke. Zum Vergleich: Der weltbeste menschliche Spieler, Ke Jie, hat 12 Jahre gebraucht, um es auf 3.627 Punkte zu bringen.
Quelle: NZZ Digital, Der Computer macht sich selbst schlau, 2017

1 Stunde
schneller werden Pakete für den Versand vorbereitet.
Mit der sogenannten “Click-to-ship”-Zeit misst der Internet-Gigant Amazon, wie lange es nach dem Abgeben einer Bestellung dauert, bis das jeweilige Produkt im Lager gefunden, eingepackt und für den Versand bereitgestellt wird. Vor der Einführung von KI dauerte das im Schnitt 75 Minuten - danach nur noch 15.
Quelle: McKinsey, AI - the next digital frontier, 2017

Wir müssen deutlich mehr von
KI verstehen als bisher

Wir müssen deutlich mehr von KI verstehen als bisher

Thematische Einführung von Franz Kühmayer, zukunftsInstitut

Ein typisches Kennzeichen unreifer Märkte ist eine ausufernde Begriffsvielfalt, verknüpft mit diffusen Abgrenzungen. Das weite Feld der KI ist davon ganz besonders betroffen: Unterschiedslos werden Begriffe wie Machine Learning, Deep Learning, Big Data, neuronale Netze und viele mehr verwendet. Ist mein Telefon mit seinem Sprachassistenten noch smart oder bereits „intelligent“? Beruhen die Ergebnisse einer CRM-Analyse auf Big Data oder auf KI, und macht das überhaupt einen Unterschied?

Abseits einer wissenschaftlichen Diskussion um die Exaktheit von Begrifflichkeiten, steckt dahinter die Tatsache, dass uns vielfach gar nicht bewusst ist, ob wir KI bereits einsetzen – im Alltag, aber auch im wirtschaftlichen Kontext. Das Buzzwort KI genügt: Dann trifft sich die vollmundige Ansage des Marketingmanagers, dass die neue Kampagne selbstverständlich KI-gesteuert ist, mit der Zusicherung des Produktionsleiters, dass ebenso selbstverständlich der Mensch nach wie vor die Kontrolle über alle sicherheitsrelevanten Fragen hat – beides im Ernstfall möglicherweise fraglich.

Im gleichen Maße werden übersteigerte Erwartungen an heilsbringende Technologien genährt, wie auch die uralte Angst des Menschen befeuert, demnächst von unkontrollierbaren Maschinen hinweggerafft zu werden. Die kollektive Verunsicherung, die den Prozess der digitalen Transformation schon generell begleitet, wird durch die neue technologische Qualität von KI auf eine weitere Stufe gehoben. Das darf uns aber nicht von einem klaren, nüchternen Urteil abhalten. Denn die fortschreitende KI-Durchdringung hat unsere Gesellschaft bereits verändert und neue Realitäten geschaffen.

Wer ist schuld am Diesel-Gate der deutschen Automobil-Industrie? Ein Ingenieur, der den Algorithmus programmiert hat? Ein Vertriebsleiter? Ein Vorstand? Der Hersteller oder der Zulieferer? Wenn es schon schwerfällt, die Verantwortung für den Missbrauch eines „nicht-intelligenten“ Algorithmus klar zu benennen, wieviel herausfordernder wird es erst, den sicheren und verantwortungsbewussten Einsatz von KI in Unternehmen zu gewährleisten.

KI-Systeme unterscheiden sich fundamental von Technologien und Verfahren, die wir bislang im Einsatz hatten. War Software bislang ein deterministisches System, das bei gleichem Input stets den gleichen Output produziert hat, ist dies bei selbstlernenden und sich weiterentwickelnden KI-Systemen nicht mehr notwendigerweise der Fall. Kommt die KI zu neuen Erkenntnissen, kann sich auch das Ergebnis seiner Berechnungen verändern.

Erschwert wird unser Verständnis von KI-Abläufen noch durch deren inhärente Logik, die auf Mustern, statistischen Modellen basiert, nicht jedoch auf regelbasierten Erklärungsmodellen. KI produziert aufgrund großer Datenmengen Ergebnisse, nicht, weil sie – im menschlichen Sinne – etwas von der Sache „versteht“. In der Konsequenz staunen wir über das Ergebnis, wissen aber nicht, wie es entstanden ist. Das ist bei Schachprogrammen, die den Menschen besiegen, vielleicht nicht relevant (außer für den Schachspieler), übertragen wir KI jedoch schwerwiegende Entscheidungen, sehr wohl. Soll KI dafür eingesetzt werden, Krankheiten zu besiegen (was sich 66% der Menschen wünschen, vgl. PWC 2017), das Energieproblem der Welt zu lösen (62% Zustimmung) oder das Bildungswesen voranzutreiben (58%), dann sollten wir sehr genau nachvollziehen können, wie Ergebnisse zustande gekommen sind.

Was für das große Bild gilt, ist für den Einsatz im Unternehmen natürlich genauso gültig. Wer nicht weiß, welcher Werkzeuge er sich bedient, kann auch kein Verständnis für die Chancen, Potentiale und Risiken der Anwendung entwickeln und keine zielsicheren Erkenntnisse daraus ableiten.

Es ist daher für uns als Konsumenten, Bürger aber gerade auch für Führungskräfte in Unternehmen entscheidend, sich ein ausreichend hohes Kompetenzniveau im Bereich KI anzueignen – nicht nur, um „mitreden“ zu können, sondern weil der verantwortungsvolle Umgang damit eine ganz selbstverständliche Anforderung geworden ist.

Wie funktionieren Systeme Künstlicher Intelligenz? Was kann KI – und was nicht? In welchen Themen läuft KI dem Menschen den Rang ab – und wo nicht? Wo wird KI heute bereits eingesetzt – und wo ist ein Einsatz perspektivisch angedacht? Wovon sollen KI-Systeme lernen? Welche Entscheidungen kann, soll und darf ich KI übertragen – und welche nicht?

Wir dürfen erwarten, dass Führungskräfte und Verantwortungsträger auf diese Fragen treffsichere Antworten für den eigenen Einflussbereich parat haben. Denn eine Welt ohne KI wird es nicht mehr geben, umso wichtiger ist es, einschätzen zu können, welche Chancen und Risiken sich daraus ergeben und wie Vertrauen in KI etabliert werden kann. Oder anders gesagt: Wie KI sicher angewendet werden kann.

„Der Betrieb und die Steuerung eines Stromnetzes wären ohne KI gar nicht mehr möglich. So könnte die Kapazitätsplanung tagesgenau für ganz Europa durch einen Menschen niemals durchgerechnet und dann noch optimiert werden.“

DI Franz Mittermayer
Vorstandsdirektor EVN AG

Univ.-Prof. Dr. Sepp Hochreiter

Lernende Systeme überstrahlen aktuell alles im KI Bereich und Deep Learning hat einen wahren KI Boom ausgelöst. Deep Learning ermöglicht es uns, Daten zu Wissen zu machen. Und dieses Wissen ist für jedes Unternehmen unfassbar wertvoll um die eigenen Prozesse und Produkte besser zu verstehen und gezielte Entscheidungen für Optimierungen treffen zu können.

Johann Christof

Im industriellen Umfeld gelten vorsorgende Service Maßnahmen – predictive maintenance – bei Anlagen als DIE Aufgabe für Effizienzsteigerung. Diese Herausforderung kann nur mit KI-Systemen umgesetzt werden. Die Brücke zu finden zwischen digitaler Aufnahme, Datenverarbeitung und -vergleich sowie Sicherheit ist noch mit vie Aufklärungsarbeit im Industriesektor verbunden. Das Verständnis zwischen Datenexperten und Fachpersonal in verschiedenen Disziplinen gehört verbunden und erweitert. Dann funktioniert der effektive Anwendungsbereich der KI mit Vertrauen und kann auch gut dokumentiert ablaufen

DI Franz Mittermayer

Der Betrieb und die Steuerung eines Stromnetzes wären ohne KI gar nicht mehr möglich. So könnte die Kapazitätsplanung tagesgenau für ganz Europa durch einen Menschen niemals durchgerechnet und dann noch optimiert werden.

DI Armin Rau

Durch den Einsatz von KI hat Spracherkennung einen riesigen Entwicklungssprung gemacht und damit auch einen hohen Level an Akzeptanz erreicht. So ist Maschinenbedienung über Sprachsteuerung in der industriellen Anwendung für uns interessant geworden. Wir haben auch einen Laservollautomaten auf den Markt gebracht, bei dem wir durch den Einsatz von KI die Produktionsqualität wesentlich verbessern konnten. Voraussetzung dafür ist dass all diese Maschinen ihre Daten teilen und so im Kollektiv lernen und verbessert werden.

DI Dr. Stefan Haas

Für den Erfolg von KI ist die industrielle Umsetzung entscheidend. Hier liegt die Stärke der österreichischen Industrie. Die Basis an technischem Knowhow und Kompetenz ist vor allem in der DACH Region stark vorhanden und eine einmalige Chance die österreichische Maschinenbauindustrie zu stärken.

DI Dr. Stefan Poledna

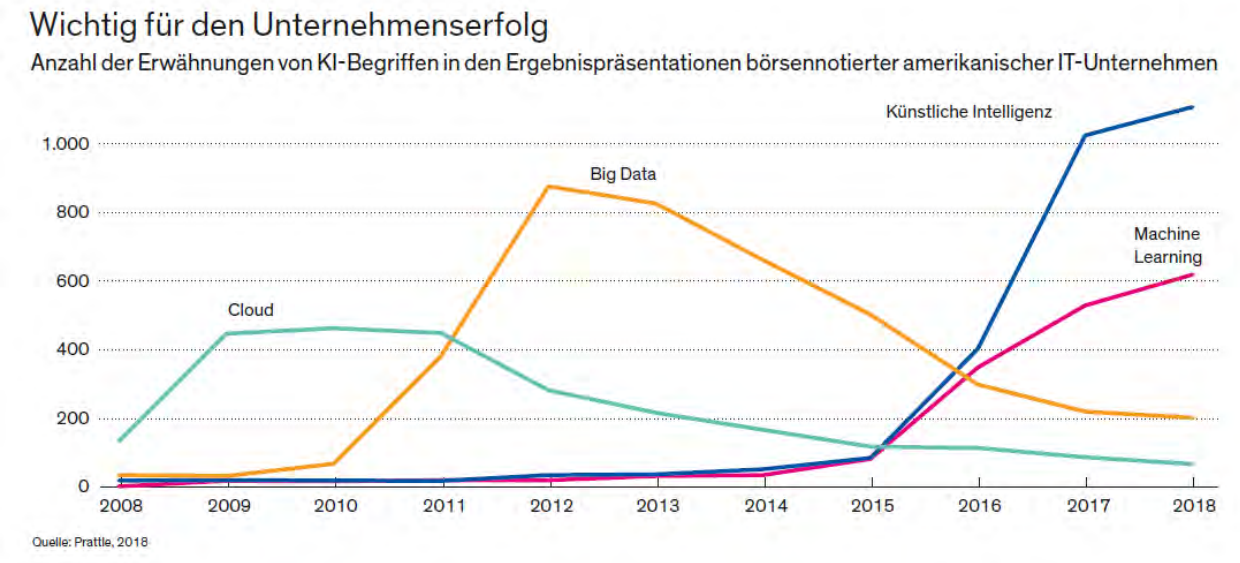
Wir müssen die Produktbereiche, bei denen wir stark sind, mit KI erweitern und damit aufwerten. So werden wir nicht zum Shopfloor derer, die nur das Service vertreiben und die Kundenmacht haben. KI Technologie muss genutzt werden, um bestehende Produkte nicht zur Commodity und damit wertlos zu machen.

Prof. Dr. Volker Gruhn

KI-Systeme sind oft keine isolierten Systeme. Oft sind sie eng integriert mit Informationssystemen und eng gekoppelt mit Objekten der realen Welt. Solche Systeme zu entwickeln und zu betreiben ist eine schwierige Engineering-Herausforderung, bei der uns traditionelle Vorgehensmodelle kaum helfen.

O. Univ. Prof. DI Dr. Sabine Seidler

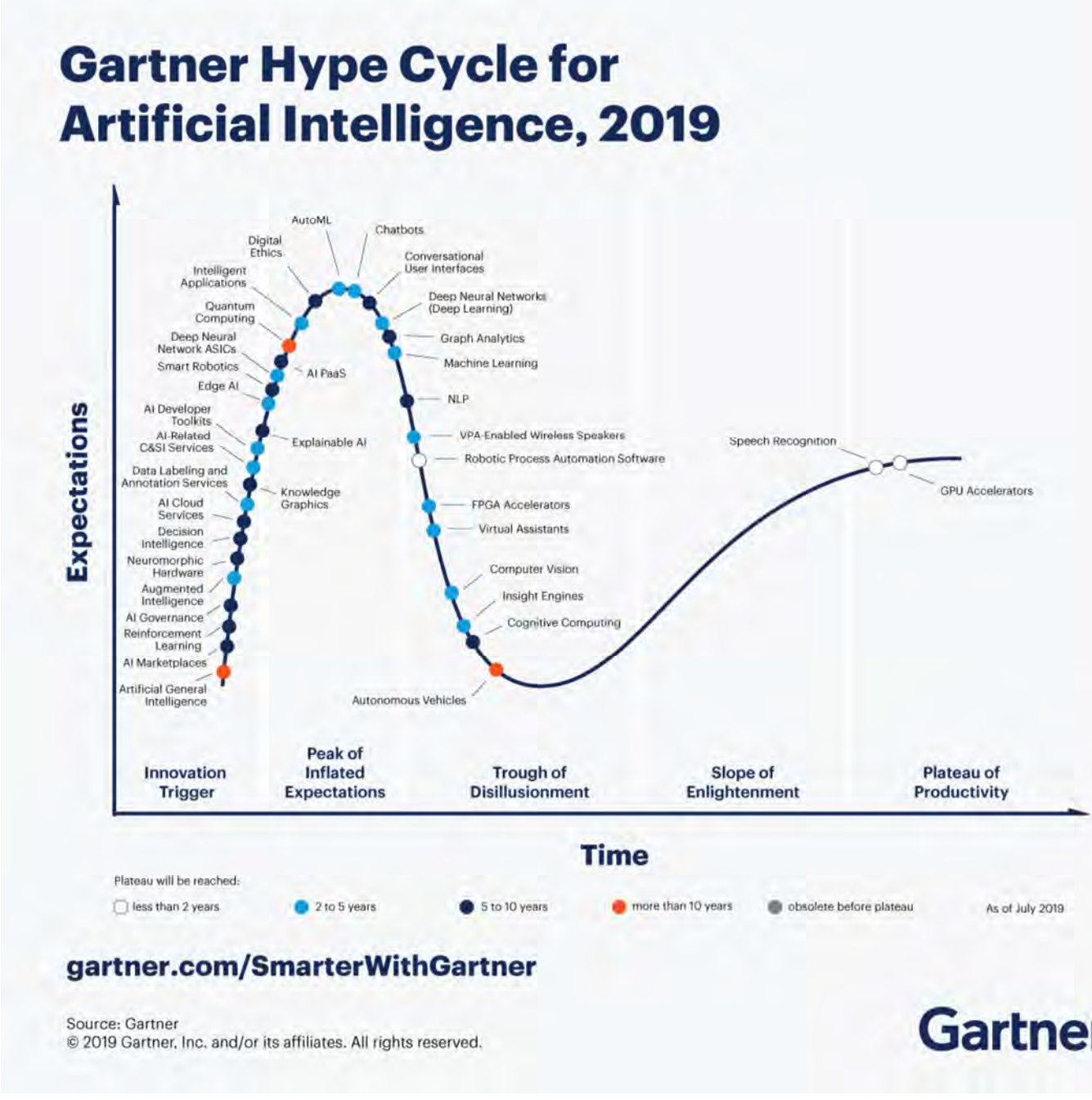
Im Einsatz von KI in der industriellen Praxis steckt ohne Zweifel ein riesiges Potenzial, damit sind aber auch Risiken verbunden. Neben den für alle IT-Systeme gültigen Sicherheitsrisiken ist an dieser Stelle insbesondere die Schnittstelle zwischen KI und Mensch hervorzuheben, auf die besonderes Augenmerk in der Forschung gelegt werden muss.



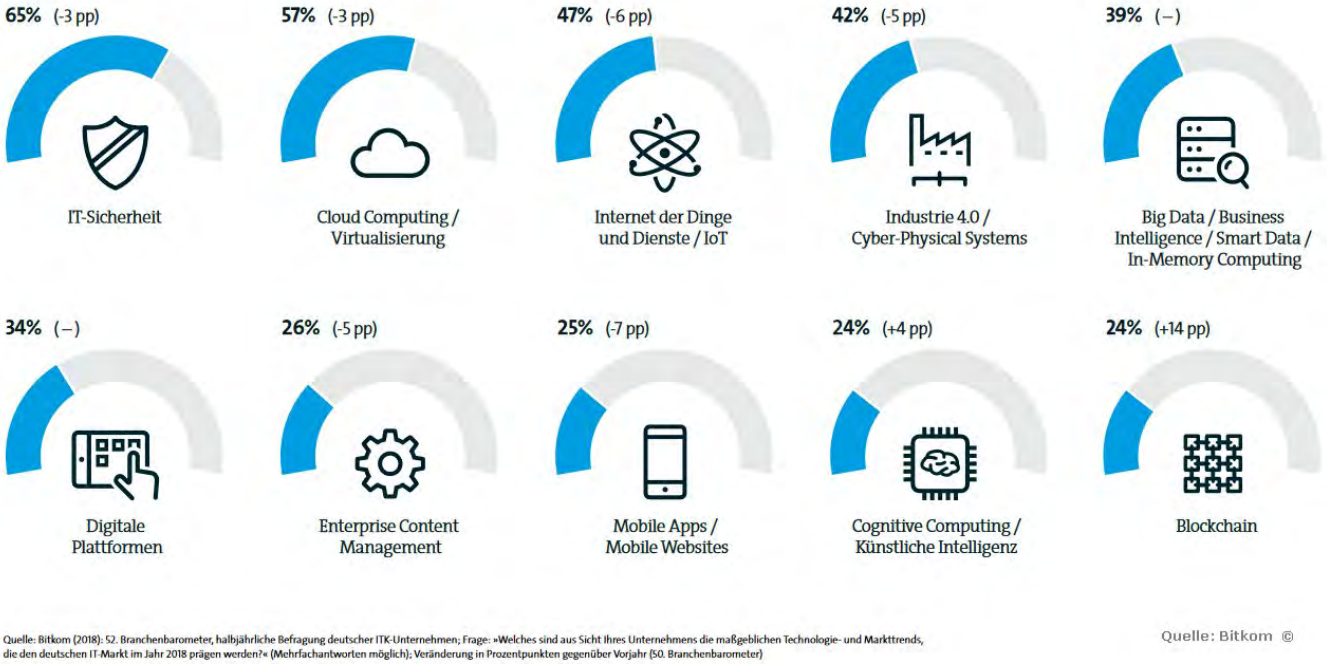
Quelle: zukunftsinstitut

Durch das Tal der Enttäuschung zur digitalen Erleuchtung

Der IT-Branchenanalyst Gartner stellt den Reifegrad der wichtigsten Entwicklungen in seinem sogenannten Hype Cycle dar. Während Spracherkennung und Rechenleistung ganz vorne liegen, steht die “Allgemeine KI”, also die dem Menschen ebenbürtige, mit breitem Verständnis ausstattete Künstliche Intelligenz noch ganz am Anfang — und das wird auch noch mindestens 10 Jahre so bleiben. Bemerkenswert: Keine einzige KI Anwendung hat nach Einschätzung von Gartner bereits wirklichen Reifegrad erreicht. Bestätigt wird das durch das Branchenbarometer des deutschen Bundesverbandes der IT-Branche, Bitkom. Während sich zwei Drittel der Unternehmen für IT-Sicherheit begeistern und noch etwa jedes zweite für Cloud Technologien oder IoT-Dienste, steht KI nur bei jedem Vierten Betrieb tatsächlich auf der Agenda. Die Zukunft liegt also tatsächlich noch vor uns.



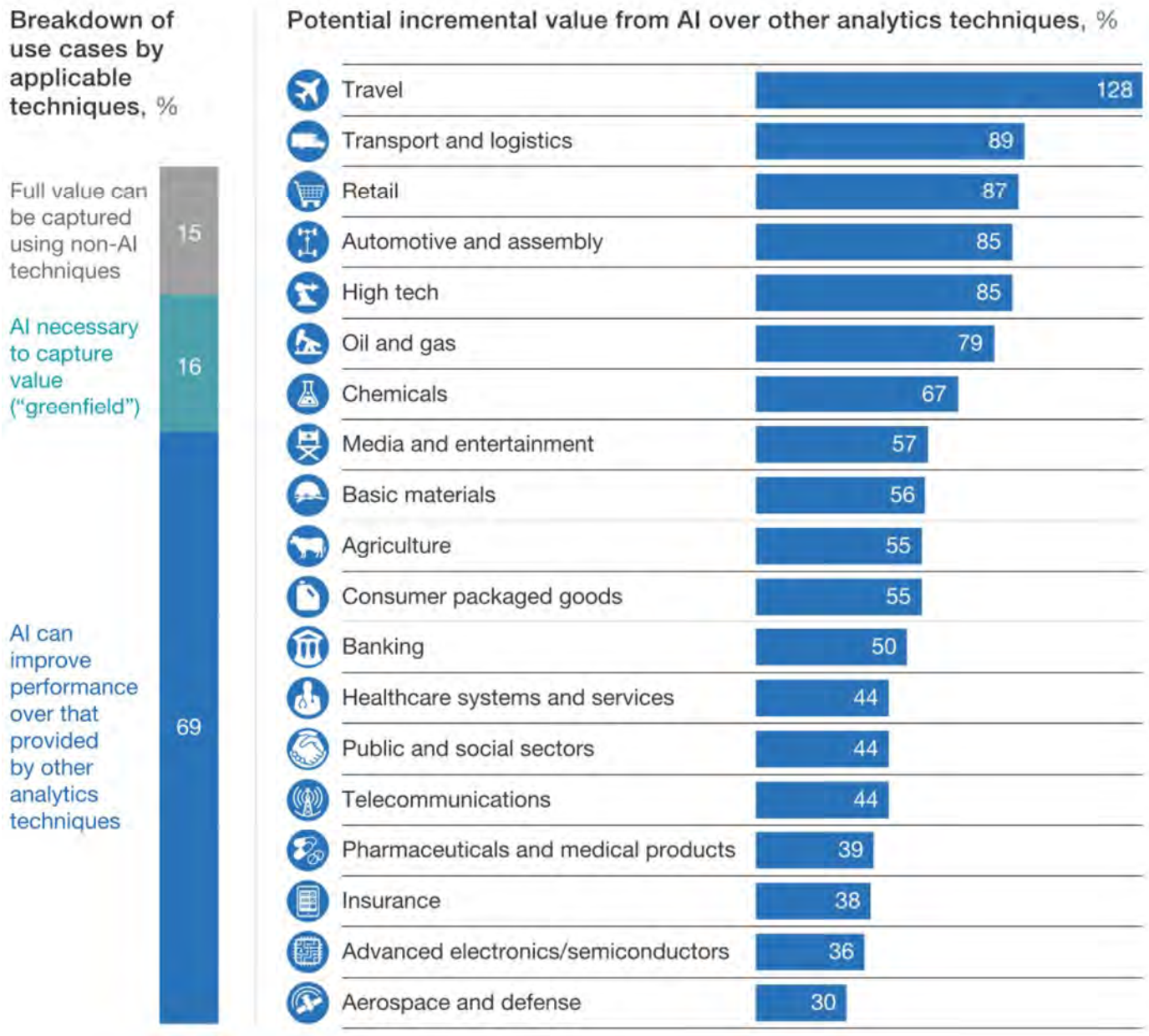
Top-Trends im IT-Mittelstand



Quelle: Bitkom (2018): 52. Branchenbarometer, halbjährliche Befragung deutscher ITK-Unternehmen; Frage: »Welches sind aus Sicht Ihres Unternehmens die maßgeblichen Technologie- und Markttrends, die den deutschen IT-Markt im Jahr 2018 prägen werden?« (Mehrfachantworten möglich); Veränderung in Prozentpunkten gegenüber Vorjahr (50. Branchenbarometer)

Quelle: Bitkom ©

Quellen: Gartner, Bitkom, zukunftsinstitut



KI ist schlauer als 85% aller anderen Werkzeuge.
Abgesehen von der Mystik der denkenden Maschinen, sind es vor allem konkrete Anwendungsgebiete, die KI so reizvoll machen. Der Strategieberater McKinsey hat in einer Studie mehr als 400 Anwendungen in 19 Branchen untersucht und ist dabei zu einem eindeutigen Ergebnis gelangt: KI ist unersetzlich. In 69% der Anwendungsgebiete liefert KI bessere Ergebnisse als andere Analyse-Methoden, weitere 15% der Anwendungen lassen sich überhaupt nur mit KI erschließen. Nach der Reisebranche zählen vor allem Transport und Logistik, Handel, Automotive und die High-Tech-Produktion zu den lohnendsten Anwendungsgebieten.

Quellen: zukunftsinstitut; McKinsey, Insights from hundreds of AI use cases, 2018

Was KI gefährlich oder sicher macht, ist viel zu unklar

Was KI gefährlich oder sicher macht, ist viel zu unklar.

Thematische Einführung von Franz Kühmayer, zukunftsInstitut

Diskussionen darüber, ob Roboter uns die Arbeit wegnehmen und um den ethisch verantwortlichen Einsatz von KI sind so lohnend, wie naheliegend. Andererseits erlaubt uns dieses abstrakte, philosophisches Niveau auch auf bequeme Art, uns den heute schon sehr realen Problemstellungen des sicheren Einsatzes von KI nicht stellen zu müssen.

Wir füttern – mehr oder weniger bewusst – smarte Systeme mit Daten, und diese Systeme spucken Entscheidungsgrundlagen aus oder treffen sogar selbst Entscheidungen, die zunehmend für unser Leben von zentraler Bedeutung sind. Werden wir für ein Jobinterview eingeladen? Erhalten wir einen Kredit? Hat dieser Kunde ein berechtigtes Garantie-Anliegen? Stimmen die Aussagen von Politikern und Medien? KI beeinflusst unsere Wahrnehmung und unser Leben im privaten, wie auch im beruflichen Kontext.

Der Marketinghype der IT-Industrie, der stets von der Überlegenheit der intelligenten Maschine mit ihrer nüchternen, objektiven Entschlusskraft und ihrem Zugriff auf für Menschen unvorstellbare Datenmengen handelt, verleiht ihr eine mystische Aura des Unantastbaren. Doch KI ist nicht perfekt, sie macht Fehler.

Beruht etwa der Schlussfolgerungs-Algorithmus auf statistischen Modellen, liegt es nahe, dass unvollständige Datenquellen oder analytischer Bias zu fehlerhaften Voraussagen führen werden. Bekanntestes Beispiel ist eine Untersuchung des sogenannten High-Rise-Syndroms bei Katzen: Die Fellnasen werden manchmal Opfer ihrer Neugierde und stürzen von Hochhaus-Balkonen in die Tiefe. Die Studie des amerikanischen Tierärzte-Fachmagazins versuchte zu ergründen, warum – entgegen aller scheinbaren Logik – jene Katzen, die aus höheren Stockwerken gefallen waren, im Schnitt leichtere Verletzungen davontrugen, als jene, die aus geringeren Höhen gestürzt waren (WHITNEY, 1987). Der Haken daran: Die meisten von weit oben herabfallenden Katzen überlebten erst gar nicht und fanden daher auch keinen Eingang in die Statistiken von Tierärzten. Fütterte man Machine Learning Systeme mit Katzenunfalls-Daten ohne sie über verzerrende Effekte in der Auswahl der Daten zu informieren, würden sie zu völlig falschen Schlüssel gelangen. Übertragbar sind derartige Muster beispielsweise auf Versicherungsfälle, aber auch auf die Auswahl von geeigneten Kandidaten aus einer großen Menge von Bewerbern.

Hinzu kommt: Sind Systeme anfällig für Datensicherheits-Probleme, besteht das Risiko für Manipulation und Missbrauch. Die Einflussnahme von Algorithmen und Bots auf politische Stimmungsmache und demokratische Wahlen hat uns vor Augen geführt, wie anfällig unsere Welt auf digitale Angriffe geworden ist. Forscher der Cornell Universität konnten zeigen, dass mit einem simplen Aufkleber auf Stopp-Schildern die Software von autonomen Fahrzeugen ausgetrickst werden konnte (EYKHOLT 2018). Sind KI-Systeme nicht ausreichend abgesichert, droht potentielles Ungemach von Hackern im Alltag für Konsumenten ebenso wie für die Betriebssicherheit von Anlagen und Unternehmen – mit fatalen Folgen.

Überlagert werden Problemstellungen einzelner Programme von systemischen Fragen: Die Fragmentierung von Wissen statt der Förderung von Verständnis für Zusammenhänge, eine potentielle Überschätzung von Technologie, und allzu sorgenlose Delegation von Problemlösungen an KI können zu catastrophic fails ganzer Systeme führen. Die sogenannten Flash-Crashes an verschiedenen internationalen Börsen zeigen dies eindrucksvoll (vgl. BRUSH 2015). Übersteigen die Sensibilität, Komplexität und Interdependenz der beeinflussten Strukturen die Reaktionsfähigkeit der Steuerung, läuft das System Gefahr, außer Kontrolle zu geraten.

Gerade weil KI eine so wirkmächtige Technologie ist, ist es entscheidend, auf ihre Sicherheit zu drängen. Dazu ist, abseits jeglicher Technikfeindlichkeit, eine nüchterne Analyse hinsichtlich der Gefahrenpotentiale und Risiken entscheidend.

Abseits gesellschaftlich erwünschter staatlicher Regulierungen zum ethisch korrekten Einsatz von KI ist angesichts der Tragweite der Entscheidungen eine vertiefte Auseinandersetzung mit dem sicheren Betrieb dieser Schlüsseltechnologie keine Fleißaufgabe für Unternehmen und Führungskräfte, sondern muss selbstverständlich sein. Im Übrigen schafft dieser Diskurs entscheidende Wettbewerbsvorteile – nicht nur für einzelne Unternehmen, sondern standortpolitisch auch für Europa im Vergleich mit den USA und China.

„Bei der Zulassung wird es am Ende entscheidend sein, ob ein KI-basiertes System eine gesamtgesellschaftlich positive Risikobalance aufweist.“

DI Dr. Stefan Poledna
Vorstand und Mitbegründer TTTech Computertechnik AG

DI Dr. Stefan Poledna

Das Thema Sicherheit beim Einsatz von künstlicher Intelligenz ist ein ganz Wesentliches. Wenn ich mich einem System mit KI anvertraue, muss es besser sein als ich. Wenn Menschenleben in Gefahr sind, müssen andere Maßstäbe angesetzt werden. Wie viele Fehler kann ich mir bei einem KI gesteuerten System erlauben? Bei der Zulassung wird es am Ende entscheidend sein, ob ein System eine gesamtgesellschaftlich positive Risikobalance aufweist. Im Fall des Automatisierten Fahrens müsste beispielweise die Anzahl an Unfällen und Verletzten nachweislich sinken.

O. Univ. Prof. DI Dr. Sabine Seidler

Natürlich ist das Thema Sicherheit beim Einsatz von künstlicher Intelligenz essentiell, aber auch vielschichtig. Wir denken bei Sicherheit in diesem Zusammenhang primär an Sicherheit gegenüber Angriffen von außen. Es geht aber auch um die Sicherheit, dass die KI die „richtigen“ Entscheidungen trifft, Entscheidungen, die unseren rechtlichen und ethischen Prinzipien entsprechen.

Univ.-Prof. Dr. Sepp Hochreiter

In vielen Anwendungen muss man sehr lange in der Realumgebung testen bis man weiß, wie sicher das System tatsächlich ist. Das ist insofern schwierig, als dass man den Großteil der Zeit mit unkritischen Situationen verbringt und die herausfordernden, sicherheitskritischen Situationen eher Randerscheinungen sind. Die KI hat somit zu wenig Gelegenheit sein Verhalten anhand sicherheitskritischer Referenzsituationen zu trainieren. Solche Situationen muss man daher künstlich in Simulationsumgebungen herbeiführen.

Prof. Dr. Volker Gruhn

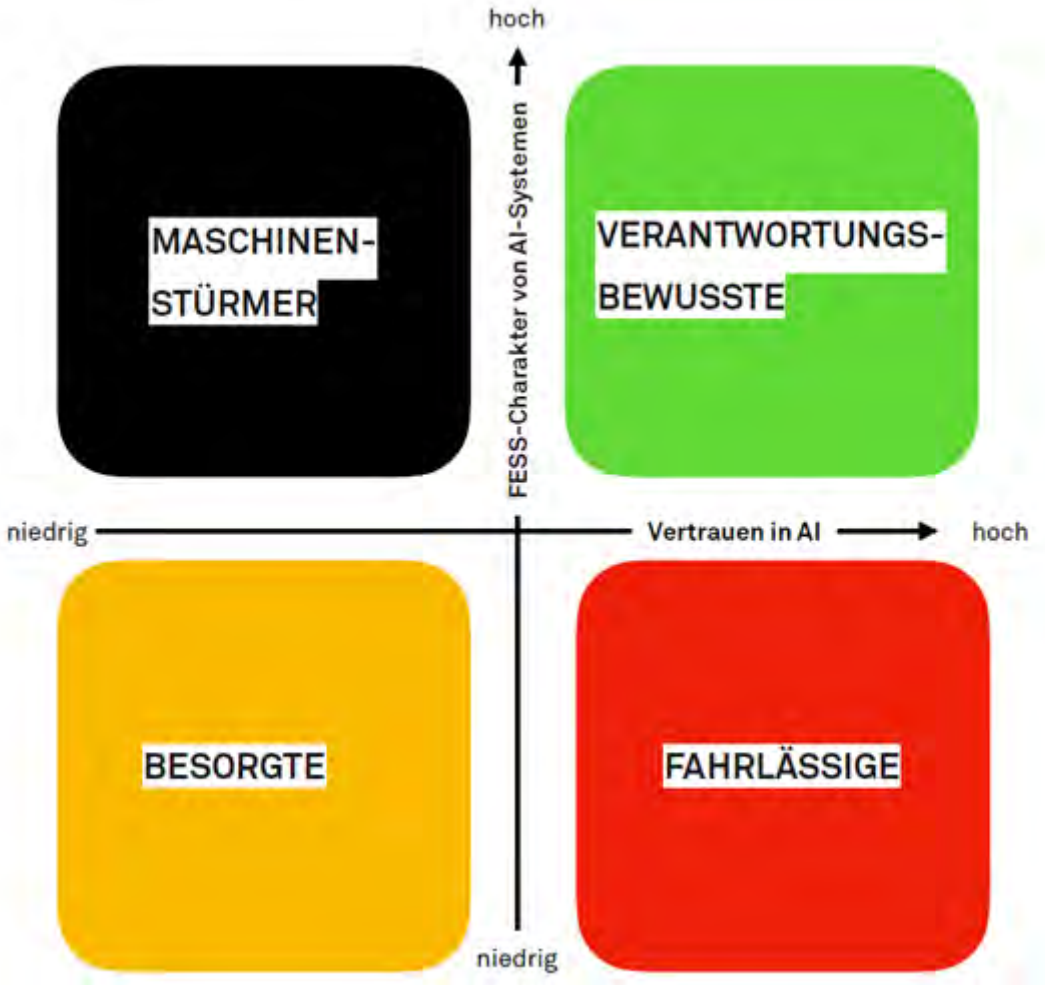
KI-Systeme müssen ethischen Prinzipien folgen. Autonome KI-Systeme mit potenziell gefährlichen Auswirkungen müssen verboten werden. Das sind aber nur wenige Typen von Systemen. Die meisten KI-basierten Systeme unterstützen derzeit „Allerwelts"-Entscheidungen, deren Gefährlichkeit überschaubar ist.

Johann Christof

Das Errichten und Betreiben einer Industrie- oder Produktionsanlage ist umfangreich mit Sicherheitsvorkehrungen verbunden. Somit ist im Anlagenbau das Thema Sicherheit ein wohlgesehener Begleiter.
E-Learning Tools und digitale intelligente Monitoring-Systeme machen Schulungen und Einsatzplanungen erst zeitgemäß. Da stellt sich gar nicht mehr die Frage ob KI eingesetzt wird, sondern nur, wie sicher man die Systeme gestalten kann. Und bis heute bedeutet Sicherheit auch hohe Investitionskosten.
Das Thema Sicherheit auf Anlagenzugriffe zur Steuerung und Manipulation lässt noch viel Spielraum im Gestalten von innovativen Lösungen offen. Die Emissionsüberwachung von Anlagen mit bildgebenden Systemen und Datenverwertung in Verbindung mit Algorithmen, die Steuerungen bespielen, wird in der Operation einer Anlage sehr bald eine große Rolle spielen.

DI Dr. Stefan Haas

Bei der Integration eines KI Systems muss auch auf die Absicherung vor unbefugten Eingriffen und Manipulation von außen geachtet werden. Wenn das System weiter selbstständig lernt, muss laufend kontrolliert werden, ob es das Richtige lernt und auch noch immer tut, was es tun soll. Im Bereich der Sicherheit und Qualität kommen wir daher zunehmend von einem statischen in einen dynamischen Zustand. Als TÜV sind wir gefragt, Prüfkonzepte für das Continuous Testing von KI Anwendungen zu entwickeln.

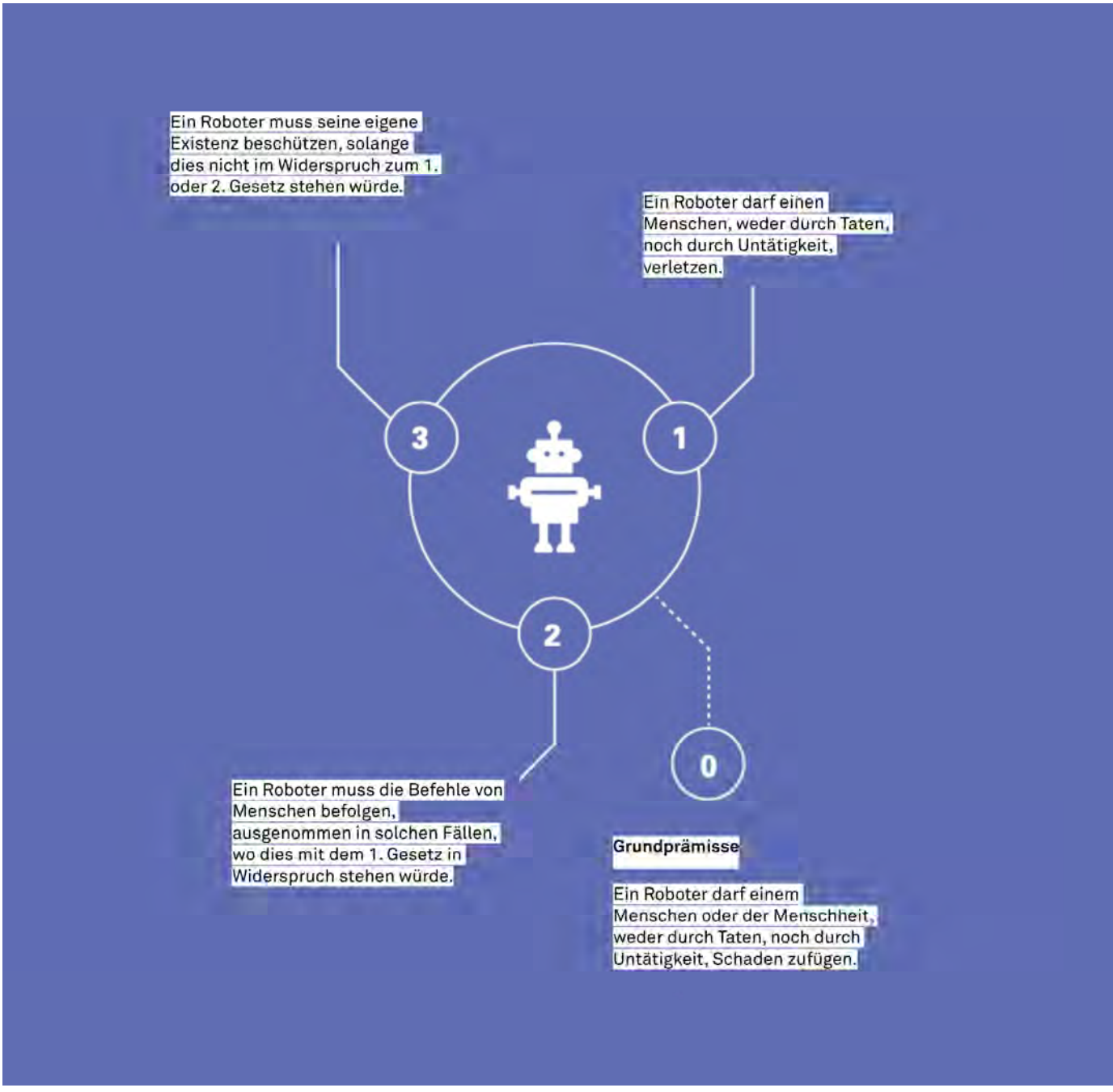


Einstellung zu AI: Von Fahrlässigkeit bis Maschinenstürmer

Für die Beurteilung des verantwortungsvollen Einsatzes von KI kann der FESS-Charakter des Systems herangezogen werden:
• F - Fairness: KI Systeme sollen in ihren Beurteilungsmodellen fair vorgehen, unbeeinflusst etwa Daten über Geschlecht, Alter, Religionszugehörigkeit o.ä.
• E - Erklärbarkeit: Ein KI System soll in der Lage sein, seine Ergebnisse und Herleitungen nachvollziehbar zu erläutern.
• S - Safe: Ein KI System soll derart konstruiert sein, dass es Menschen keinesfalls Schaden zufügt und idealerweise sogar Schaden von Menschen abwendet
• S - Secure: Ein KI System soll gegen Missbrauch und schädliche Einflüsse von außen abgesichert sein (etwa gegen Hacker-Angriffe).

Je nach persönlicher Einstellung zu KI und dem Grad an Vertrauen, das man einem KI System entgegenbringt, ergeben sich damit prinzipiell 4 mögliche Einstellungen:
• Fahrlässige: Auch einem KI-Systems, das nicht verantwortungsvoll (im Sinne des FESS-Prinzips) entworfen ist, werden keine Bedenken entgegengebracht.
• Besorgte: Jene, die eine skeptische Grundhaltung haben, ganz besonders im Angesicht von nicht vertrauenswürdigen KI-Systemen.
• Maschinenstürmer: Unabhängig davon, ob ein KI-System sich als vertrauenswürdig erweist, bleibt dieser Typ ablehnend.
• Verantwortungsbewusste: Um Vertrauen in ein KI-System zu entwickeln, wird die Einhaltung der FESS-Prinzipien gefordert.

Quelle: zukunftsinstitut



Asimow, die Roboter und KI.

Der Science-Fiction Autor Isaac Asimow hat mehr als 500 Bücher verfasst — und sich darin Gedanken zur Welt von morgen gemacht. 1942 hat er drei Gesetze entwickelt, die den sicheren Umgang von Robotern mit Menschen gewährleisten sollten. Die drei Gesetze hat er später noch um das Gesetz Null, die zugrundeliegende Prämisse, ergänzt.

In Zeiten von AI sind wir gefordert, über vergleichbare Regeln für Software nachzudenken — und Mechanismen, die Einhaltung dieser Regeln überwachen zu können.

Quelle: zukunftsinstitut

KI steckt in der Vertrauenskrise

KI steckt in der Vertrauenskrise

Thematische Einführung von Franz Kühmayer, zukunftsInstitut

„Was wäre nötig, damit wir den Entscheidungen einer Maschine uneingeschränkt vertrauen?“ So trivial die Frage klingt, so relevant ist sie für die Praxis. Und so vielschichtig und diffus sind die Antworten.

Umso mehr, als uns die menschliche Hybris immer wieder ein Bein stellt. Es hat Jahre gedauert, bis Autofahrer davon überzeugt werden konnten, dass ein klassisches Anti-Blockier-System „besser“ bremst, als sie selbst – allzu überzeugt war der Herrenfahrer von seinen überlegenen menschlichen Fähigkeiten am Volant. Heute führen wir vergleichbare Diskussionen rund um die unterschiedlichen Fahr-Assistenten (wer parkt besser ein, die Maschine oder ich?) und stellen uns die Frage, wann vollständig autonomes Fahren wirklich Realität sein kann.

Das vielleicht bekannteste KI-System der Welt ist IBMs Watson. Mit großem PR-Getöse hat der IT-Gigant angekündigt, dass Watson auch für die Bekämpfung von Krebs herangezogen würde. Und es erscheint ja auch nachvollziehbar, dass ein KI-System mit Zugriff auf Millionen von Patientenakten zutreffendere Diagnosen stellen kann, als auch der beste Facharzt, der im Laufe seines gesamten Berufslebens bestenfalls einige Tausend solcher Fälle sieht. Dennoch steckt Watson im eigenen Nimbus fest (FREEDMAN, 2017): Denn bestätigt das System die vom Arzt vorgefasste Diagnose, so haben die Medizinexperten keinen Zusatznutzen im Einsatz der KI; widerspricht es aber dem Arzt, so schenkt dieser dem System nur in seltenen Fällen Glauben.
Bei tausend Krebs-Patienten haben Ärzte nur in 14% der Fälle auf der Basis von Watson-Empfehlungen ihre eigene Entscheidung verworfen und stattdessen andere, von ihnen selbst ursprünglich nicht vorgesehene Behandlungsmethoden angewendet (SOMASHEKHAR, 2019). Sollten wir Nicht-Mediziner also im Zweifel eher Watson, Dr. Google oder unserem Hausarzt vertrauen?

Rund 80 Prozent der Menschen fühlen sich aktuell unwohl, wenn Computer über sie entscheiden (FISCHER PETERSEN 2018). Genährt wird das generelle Misstrauen gegenüber KI durch Ernüchterungen des Alltags. Viele Menschen machen die Erfahrung, dass Smartifizierungen fragwürdigen Nutzen stiften und nicht selten auch wenig treffsichere Ergebnisse bringen. Wenn bereits der banale digitale Alltag zu einem Mehr an Unzuverlässigkeit und lästigem Aufgefordertwerden führt – etwa in der Interaktion mit Sprachassistenten – wie sicher kann dann die Anwendung von KI an tatsächlich kritischen Stellen sein?

Die nüchterne Faktenlage, etwa dass autonome Fahrzeuge eine objektiv niedrigere Unfallhäufigkeit als menschliche Fahrer haben, hilft nur eingeschränkt, das Vertrauen in KI zu etablieren. Nur 11% der Bankkunden vertrauen einem KI-System bei Kreditempfehlungen – auch wenn dieses System von menschlichen Experten programmiert wurde (HSBC 2017).

Dazu kommt, dass sich auch in Unternehmen die Beobachtung durchsetzt, dass KI nicht wie ein Magic Dust funktioniert, mit dem man eine Organisation von heute auf morgen smart macht. Zwar liefert nach einer Auswertung von hunderten Geschäftsfällen Künstliche Intelligenz in 85% aller Anwendungsgebiete bessere Analyseergebnisse als alle anderen Methoden (MCKINSEY 2018), doch ist die Implementierung von KI ein komplexer und komplizierter Prozess – gerade dann, wenn es nicht um Laborsituationen von Informatik-Forschungsinstituten geht, sondern um schwierige Aufgaben aus dem realen Business.

KI sollte immer im Hinblick auf den menschlichen Nutzen gesehen werden. Sie wirkt bei kognitiven Aufgaben leistungssteigernd, erweitert unsere Fähigkeiten und beschleunigt und verbessert damit die Lösung von Problemen. Wenn aber der Einzelne – in seiner Rolle als Konsument, Kunde, Mitarbeiter, Bürger – KI gegenüber wenig vertrauensvoll eingestellt ist, hat dies unmittelbare Konsequenzen auf der Handlungsebene. **Erst wenn die bereitgestellte Technologie auf glaubwürdige Weise als sicher qualifiziert ist, wird sich ein natürlicher Umgang damit ergeben.**

„Führungskräfte sind aktuell noch nicht ausreichend in der Lage zu verstehen, was sichere Anwendung von KI bedeutet.“

DI Dr. Stefan Haas
CEO TÜV AUSTRIA Gruppe

DI Armin Rau

Speziell im Maschinen- und Anlagenbau wird die Qualität von Entscheidungen stark von der eingesetzten Sensorik abhängig sein. Die Verlässlichkeit der Sensorik ist somit kritisch für eine sichere Entscheidungsfindung. Bei stark fehleranfälligen Systemen fehlt es meist schon von Beginn weg an der Akzeptanz

O. Univ. Prof. DI Dr. Sabine Seidler

Die meisten Befürchtungen im Zusammenhang mit KI lassen sich mit „drohendem Kontrollverlust“ zusammenfassen. Ich persönlich halte diese Ängste für irrational, aber sie sind ernst zu nehmen. Es ist Teil des Bildungsauftrages der Universität durch Information und Aufklärung dazu beizutragen, irrationale Ängste abzubauen, aber auch einen kritischen Diskurs zu Grenzen des Einsatzes von KI zu führen.

DI Franz Mittermayer

Die Anwender fürchten, dass sie beim Einsatz von Smart Metern überwacht, ihre Lebensgewohnheiten abgetastet werden und dass daraus ein Geschäftsmodell abgeleitet wird. Dabei dienen diese Geräte lediglich zum reinen Stromablesen und Übermitteln der Daten. Dort wo die Einzelperson jedoch den eigenen Nutzen erkennt, ist die Akzeptanz schnell wesentlich höher. Dieser Nutzen muss betont und Ängste genommen werden.

Univ.-Prof. Dr. Sepp Hochreiter

Die Akzeptanz von KI ist ein sehr wichtiges Thema. So können zum Beispiel täuschend echte Videomanipulationen und Bilder generiert werden (Deep Fake). Das führt auch zu viel Skepsis bei den Anwendern. So würden laut Studien mehr als 50% der Menschen nicht mit einem autonomen Fahrzeug mitfahren. Doch wie kann mehr Vertrauen für KI Systeme erzeugt werden? Ein Ansatz ist, dass die KI sich selbst erklärt und Aktionen ankündigt, bevor sie ausgeführt werden. Voraussetzung dafür ist es, dass die KI dabei auf menschliche Konzepte zurückgreifen kann. Das ist nicht notwendigerweise gegeben und ab einer gewissen Komplexität auch nur mehr schwer möglich.

Prof. Dr. Volker Gruhn

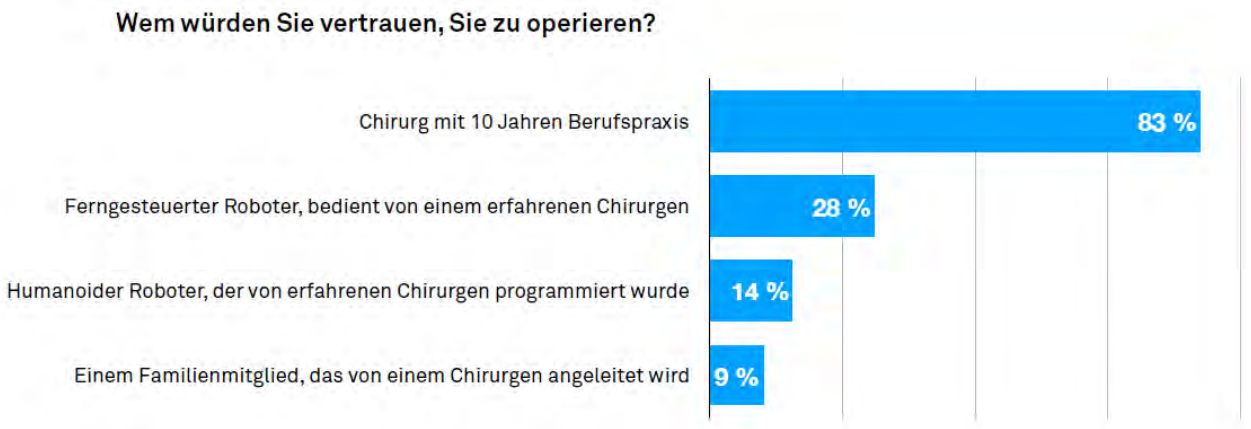
KI steckt vor allem deshalb in der Vertrauenskrise, weil die meisten Menschen, die über KI sprechen, sich nicht damit auseinandersetzen wollen, dass KI Mathematik, Statistik und Stochastik ist. Wir müssen dem trotzdem begegnen, mit Anforderungen an die Erklärbarkeit von KI und mit klaren Vorgaben zum Lernen während des Betriebs.

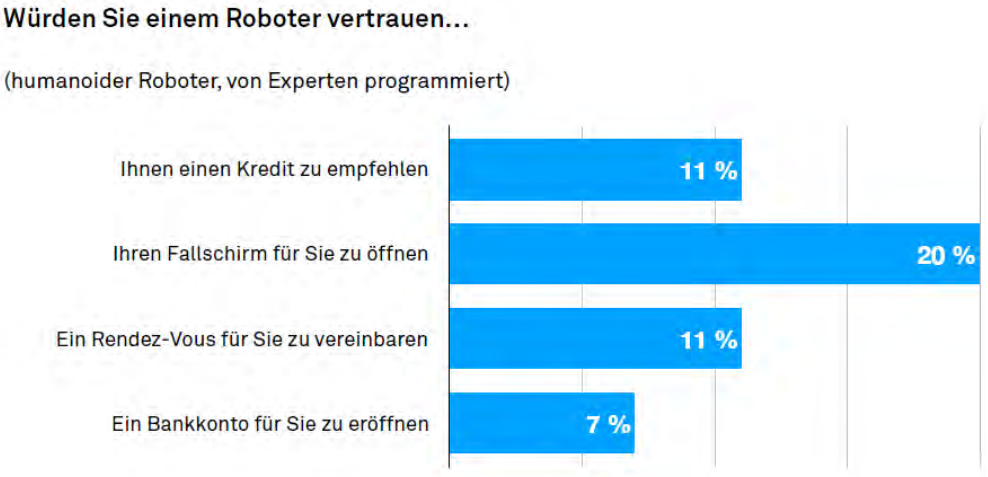
Johann Christof

In der Vertrauensfrage geht es immer um umfangreiche Entscheidungsgrundlagen. Künstliche Intelligenz wird von menschlicher Intelligenz gestaltet und programmiert. Wenn wir begreifen, dass KI eine Sammlung von Best Practice und Lessons Learned ist, wird das Vertrauen steigen, weil die Einsatzbereiche klar definiert werden können. Die Innovation, der neue Zugang zu einer Problemlösung, wird nach heutigem Wissensstand immer im Rahmen des menschlichen Gestaltungsumfangs bleiben. Wir vertrauen bereits heute in vielen Bereichen der KI.

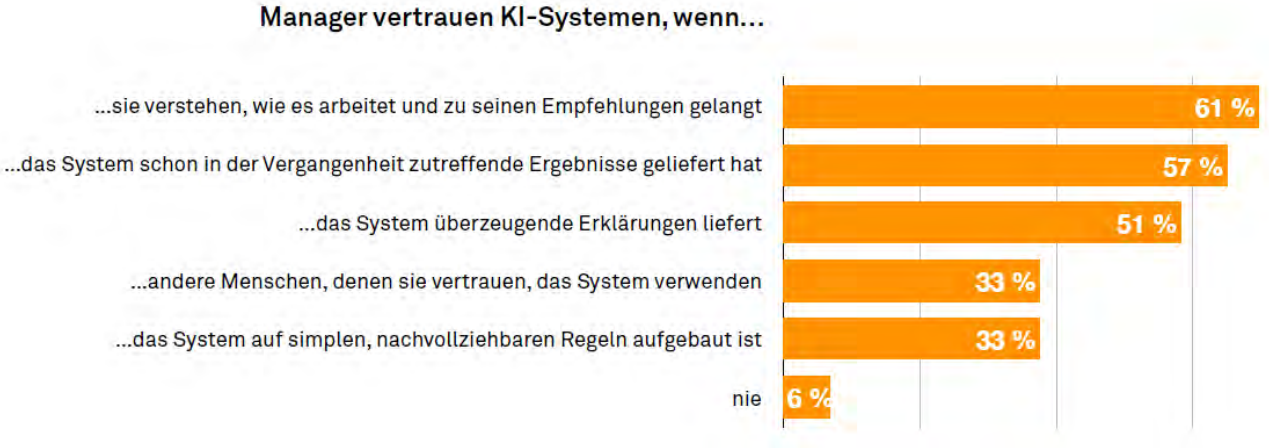
DI Dr. Stefan Haas

Führungskräfte sind aktuell noch nicht ausreichend in der Lage zu verstehen, was sichere Anwendung von K bedeutet. Alles was technisch möglich ist, wird aber auch zur Anwendung kommen. Deshalb ist es wichtig sich mit diesem Thema auch tatsächlich und rechtzeitig zu beschäftigen.





Quellen: zukunftsinstitut, HSBC, Trust in Technology, 2017



Quellen: zukunftsinstitut, Vegard Kolbjornrud, The promise of AI, Norwegian Business School, 2016

Weiterführende Literatur & Quellennachweise:

BRUSH, Silla; et al (2015): How a Mystery Trader With an Algorithm May Have Caused the Flash Crash; In: Bloomberg, 22. April 2015

EYKHOLT, Kevin; et al (2018): Robust Physical-World Attacks on Deep Learning Models; CVPR Conference in Computer Vision and Pattern Recognition, 2018

FISCHER, Sarah; PETERSEN, Thomas (2018): Was Deutschland über Algorithmen weiß und denkt; Bertelsmann Stiftung

FREEDMAN, David (2017): A Reality Check for IBM's AI Ambitions; in: MIT Technology Review, Juni 2017

HSBC (Hg.) (2017): Trust in Technology

KÜHMAYER, Franz; et al (2018): Hands-On Digital. Agenda für digitale Kompetenz; Verlag Zukunftsinstitut

MARCUS, Gary; DAVIS, Ernest (2019): Rebooting AI. Building Artificial Intelligence We Can Trust; Pantheon Verlag

MCKINSEY (Hg.) (2018): Insights from hundreds of AI use cases

PWC (Hg.) (2017): Bot.me: How artificial intelligence is pushing man and machine closer together

RUSSELL, Stuart (2019): Human Compatible. AI and the Problem of Control; Penguin Verlag

SCHULDT, Christian; et al (2017): Trendstudie Künstliche Intelligenz. Wie wir KI als Zukunftstechnologie produktiv nutzen können; Verlag Zukunftsinstitut

SOMASHEKHAR, S.P., et al (2019): A Prospective blinded study of 1000 cases analyzing the role of artificial intelligence; in: ASCO Meeting Juni 2019

WHITNEY, WO; Mehlhaff, CJ (1987): High-rise syndrome in cats; In: Journal of the American Veterinary Medical Association. 191 (11): 1399–403.


TÜV
AUSTRIA

Company Profile
TÜV AUSTRIA

Company Profile TÜV AUSTRIA

Der TÜV AUSTRIA ist ein internationales Unternehmen mit Niederlassungen in mehr als 20 Ländern der Welt. TÜV AUSTRIA beschäftigt etwa 2.000 Mitarbeiterinnen und Mitarbeiter (FTE) und erwirtschaftet ca. 200 Mio. Euro Umsatz.
Die Servicekompetenzen der vier Geschäftsfelder „Industry & Energy“, „Infrastructure & Transportation“, „Life, Training & Certification“ und „Service Providers and Public“ umfassen die Bereiche Prüfung, Überwachung, Zertifizierung, Aus- & Weiterbildung und Beratung.

Die Innovationsschwerpunkte

Die Verschmelzung der physischen und der Cyber-Welt im Zuge der Digitalisierung führt zu neuen Anforderungen und stärkerem Zusammenwachsen von sicherheitstechnischen Konzepten und Bewertungen in der funktionalen Sicherheit (Safety) und IT-Security. Auch die zunehmende Integration von Data Analytics und Künstlicher Intelligenz in IoT und IIoT Komponenten, fordert neuartige Prüf- und Zertifizierungsprozesse, um die umfängliche Sicherheit von cyberphysischen Systemen gewährleisten zu können.

NEXT HORIZON

Um von den Effekten der fortschreitenden Digitalisierung nicht negativ beeinflusst zu werden, sondern überdurchschnittlich profitieren zu können, wird in NEXT HORIZON, dem Digital Acceleration Incubator der TÜV AUSTRIA Gruppe, eine Vielzahl von Maßnahmen gesetzt.

Dabei werden folgende Ziele verfolgt:

- In einem interdisziplinären und Open-Innovation-Ansatz werden digitale Technologien erforscht und zukunftsorientierte Servicekonzepte entwickelt. Diese Konzepte werden am Markt erprobt und anschließend in das operative Geschäft überführt.
- Während des Entwicklungsprozesses werden agile und nutzerorientierte Methoden wie Service Design Thinking und Lean Startup verwendet, die im NEXT HORIZON LAB bereitgestellt werden.
- Ein besonderer Fokus liegt auf der Rekrutierung und Entwicklung von „Young Talents“, den sogenannten „NEXT HORIZON Pioneers“, parallel zur Entwicklung der Themen.

www.nexthorizon-lab.at


nexthorizon

Engagement in Forschungsprojekten

Als unabhängiger österreichischer TÜV begleiten wir die Industrie in der digitalen Transformation ihrer Unternehmenslandschaft.
Um schneller von einer Idee zum Produkt und einer Dienstleistung zu kommen, um mitzuhelfen, die Grundlagenforschung anwendungsnah und wettbewerbsorientiert zu gestalten und den Technologietransfer in Richtung Wirtschaft massiv zu unterstützen, engagiert sich der TÜV AUSTRIA in einer Reihe von kooperativen Forschungsprojekten zu den Innovationsschwerpunkten.

Exemplarisch wird im Folgenden je ein aktuelles Projekt zu den beiden Innovationsschwerpunkten vorgestellt.

Safe & Secure Systems

Motivation: Das Industrial Internet of Things (IIoT) wird schrittweise Realität und somit auch die Konvergenz von funktionaler Sicherheit (Safety) mit Cybersecurity. Um hochfunktionale und gleichzeitig sichere System zu konzipieren, betreiben und laufend modifizieren zu können, bedarf es vor allem im hochspezialisierten Produktionsbereich, sei es in der diskreten Fertigung oder in der Prozessindustrie, neuer technologischer Fertigkeiten.
Innovationsvorhaben: Um der Industrie die nötigen Werkzeuge für den Umgang mit Sicherheitsthemen in die Hand zu geben, erarbeiten die TU Wien und der TÜV AUSTRIA im „TÜV AUSTRIA Security in Industry - Research Lab“ entlang von mehreren Dissertationsprojekten entsprechende Lösungen. An diesem Vorhaben sind die Fakultäten für Maschinenwesen und Betriebswissenschaften, für Elektrotechnik und Informationstechnik, und für Informatik beteiligt.

Data Analytics & Artificial Intelligence

Motivation: Im Zeitalter der Digitalisierung ist die Anwendung von Künstlicher Intelligenz nicht wegzudenken. Um die Sicherheit und Robustheit einer KI-gestützten Anwendung zu gewährleisten, braucht es eine unabhängige Prüforganisation, die solche Anwendungen untersucht und zertifiziert.
Innovationsvorhaben: Gemeinsam mit dem Machine-Learning Institut der Johannes-Kepler-Universität Linz wird zur sicheren Anwendung von KI geforscht. Dabei werden verschiedene Methoden zur Interpretation von Machine Learning Modellen entwickelt um einen Werkzeugkasten zur Zusicherung der Eigenschaften eines Modells zu entwerfen.

Neue innovative Lösungen

Entlang der Forschungsprojekte werden innovative Dienstleistungen unmittelbar abgeleitet.
Ein Beispiel dafür ist das S3 (Safe Secure Systems) Lab, eine High-Tech Laborinfrastruktur, um unseren Kunden Test-, Zertifizierungs- und Beratungsleistungen zu Safety- und Security für den gesamten Lebenszyklus von cyberphysischen Systemen und Produkten (CPS) gebündelt an einem Ort anbieten zu können.

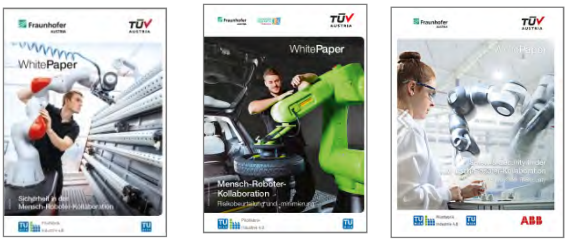
Weiterführende Informationen zum S3 Lab und anderen innovativen Services:
www.tuvaustria.com/i4.0
www.it-tuv.com/leistungen/zertifizierungen/pruefung-und-zertifizierung-von-iot-devices/

White Papers

Best Practices aus abgeschlossenen Projekten werden der interessierten Öffentlichkeit in Form von White Papers zur Verfügung gestellt.
/www.tuvaustria.com/next-generation/white-paper/

IoT im Smart Home: Seitenkanalangriffe als neue Angriffsform

Hoch-automatisiertes Fahren: Herausforderungen für Funktionale Sicherheit und Cyber-Security



White Paper Reihe zu Safety & Security in der Mensch-Roboter—Kollaboration

Creative Community

innovatüv® ist die Social Crowdsourcing Plattform der TÜV AUSTRIA Gruppe und ein hocheffizientes Werkzeug zur kollaborativen Ideenfindung und Ableitung von Innovationsvorhaben.
innovatüv® vernetzt die gesamte TÜV AUSTRIA Group zu einer Ideen-Community. Die global verteilte Intelligenz der Unternehmensgruppe wird dabei als Potenzial genutzt, informelle Netzwerke werden über einen Social Media-Ansatz gefördert und sichtbar gemacht. Dabei findet durch die Integration von spieltypischen Elementen eine signifikante Motivationssteigerung der User statt. Pro Jahr werden an die 200 Ideen eingereicht und eine Vielzahl davon umgesetzt.

TÜV AUSTRIA-Platz 1
2345 Brunn am Gebirge
innovation@tuvaustria.com
www.tuvaustria.com

TÜV AUSTRIA Group
TÜV AUSTRIA-Platz 1 | 2345 Brunn am Gebirge
info@tuvaustria.com | tuvaustria.com