Generative KI-Agenten

Inhaltsverzeichnis

Einführung

In den letzten Jahren hat die Künstliche Intelligenz (KI) enorme Fortschritte gemacht und ist zu einem zentralen Thema in vielen Bereichen unseres Lebens geworden. Besonders hervorzuheben ist die Entwicklung sprachbasierter KI-Modelle, wie dem GPT-3.5-turbo von OpenAI, das im Herbst 2022 in ChatGPT[1] integriert und der Öffentlichkeit zugänglich gemacht wurde. Diese Innovation hat nicht nur das Interesse an KI im Allgemeinen geweckt, sondern auch die Aufmerksamkeit auf Chatbots und intelligente Assistenten stark erhöht.

ark erhöht.

Ursprünglich wurden diese Sprachmodelle hauptsächlich für die Erstellung von Texten und als virtuelle Gesprächspartner eingesetzt. Sie konnten einfache Fragen beantworten, Informationen bereitstellen und bei der Texterstellung unterstützen. Mit den neuesten Entwicklungen in der Technologie sind jedoch bedeutende Verbesserungen erzielt worden. Die neuen Modelle bieten ein größeres Kontextvolumen, sie können also mehr Informationen gleichzeitig verarbeiten. Zudem sind sie schneller und kostengünstiger in der Nutzung geworden.

Bislang war es notwendig, bei der Formulierung von Anfragen – sogenannten "Prompts" – besonders darauf zu achten, wie viel Inhalt man bereitstellt, um die gewünschten Ergebnisse zu erzielen. Heute ist es jedoch möglich, diese Anfragen mit zusätzlichen Anweisungen zu erweitern.

Die Kombination dieser erweiterten Funktionen mit speziellen Werkzeugen führt zu dem, was als Sprachmodell-erweiterten „KI-Agenten"[2] oder generative KI-Agenten bezeichnet wird.

In diesem Dokument wird das Konzept der KI-Agenten näher erläutert. Es werden die Funktionsweise, die Vorteile sowie die Herausforderungen bei ihrer Implementierung untersucht. Ziel ist es, ein besseres Verständnis für die Potenziale und Möglichkeiten zu schaffen, die KI-Agenten in einer zunehmend digitalisierten Welt bieten.

Zum Begriff „Agent"

Zunächst sollte der Begriff „Agent" näher betrachtet werden. Den englischen Begriff „agent" kann man im Deutschen

Was sind „KI-Agenten"?

„Ein [KI-Agent] bezieht sich auf ein System oder Programm, das in der Lage ist, autonom Aufgaben im Namen eines Benutzers oder eines anderen Systems auszuführen, indem es seinen Workflow gestaltet und verfügbare Tools benutzt." [6]

Grundsätzlich handelt es sich damit um eine ähnliche Beschreibung wie „Software-Agenten"[7], erweitert um Fähigkeiten der Künstlichen Intelligenz.

[1] (OpenAI, 2022)
[2] (Huang, 2024)
[3] (LEO GmbH, n.d.)
[4] (Kagan, 2024)
[5] https://www.investopedia.com/terms/a/agent.asp
[6] (Gutowska, What are AI agents?, 2024)
[7] (Zwass, n.d.)

hat formatiert: Deutsch (Deutschland)

hat formatiert: Deutsch (Deutschland)

hat formatiert: Deutsch (Deutschland)

Kommentiert [DH1]: Gibt es hier Definitionen, welche man referenzieren kann?

Kommentiert [LS2R1]: https://www.investopedia.com/terms/a/agent.asp

Kommentiert [TR3]: Das war mir so nicht bewusst. WO kommt das her? Wirkt als wäre ein "Agent" eine Entität zwischen Nutzer und LLM aber im GenAI SInne ist ein Agent doch ein LLM meist nform einer Persona mit bestimmten Vorgaben und Konfigurationen + Tools?

Kommentiert [LS4R3]: Ich verstehe darunter, dass eine KI Agent teilweise Aktionen unternimmt, die normalerweise ein Mensch machen müsste. Bsp: Chatbot der um eine Suchfunktion erweitert wurde. Eine Suchmaschine kann ohne entsprechende Eingabe nicht funktionieren, wenn natürliche Sprache genutzt wird. Der User Query muss erstmal zusammengebaut werden. Das kann ein LLM aus der Frage des Users und den bisherigen Chatverlauf im Hintergrund erledigen, die Suche triggern und das Ergebniss an den User schicken. Dem User ist nicht klar, dass seine Frage mit relevanten Infomrationen aus dem Kontext ergänzt wurde.

Dazu gehören folgende Eigenschaften[8]:

- **Autonomie**: Autonomie und Kontrolle über Problemlösungsaufgaben ohne direkte menschliche Intervention.
- **Soziale Fähigkeit:** Interaktion mit anderen zur Unterstützung bei Problemlösungen und Aktivitäten.
- **Reaktionsfähigkeit:** Umgebung wahrnehmen und zeitnah auf Veränderungen reagieren.
- **Proaktivität**: Opportunistisches, zielgerichtetes Verhalten und Initiative ergreifen.

Das Konzept eines KI-Agenten lässt sich wie folgt zusammenfassen: Ein KI-Agent ist ein Software-Programm, das in der Lage ist, autonom Informationen zu verarbeiten, Entscheidungen zu treffen und Aktionen auszuführen. Er stellt eine spezielle Form eines KI-Systems dar und nutzt Eigenschaften der Künstlichen Intelligenz.

Darüber hinaus kann der Agent mit seiner Umgebung kommunizieren, auf vorhandenes Wissen zugreifen und verschiedene Werkzeuge einsetzen, um seine Aufgaben effizient und effektiv zu erfüllen

Generative KI-Agenten

Bei generativen KI-Agenten handelt es sich um KI-Agenten, die mithilfe von Sprachmodellen erweitert werden. Das Sprachmodell fungiert als Steuerungskomponente[9].

Die Leistungsfähigkeit aktueller Sprachmodelle (LLM) trägt einerseits dazu bei, die Bereitstellung dieser Agenten zu erleichtern, und erweitert andererseits die Vielfalt ihrer möglichen Einsatzgebiete.

Hinweis: In den folgenden Abschnitten wird der Leserlichkeit wegen von KI-Agenten gesprochen. Dabei handelt es sich um LLM-erweiterte KI-Agenten.

Kommentiert [TR5]: Sehr gut, bitte auf Grundlagenquellen referenzieren und Deutlich machen, dass es hier verschiedene Definitions Ansätze gibt.

Kommentiert [LS6R5]: Unterschiede zwischen Software-Agent, KI-Agent und GenAI-Agent hervorgehoben

[8] (Jennings & Wooldridge, 1996)
[9] (Huang, 2024)

Vom Chatbot zum KI-Agenten

Geschichtliche Betrachtung

Die Entwicklung von Künstlicher Intelligenz (KI) hat in den letzten Jahrzehnten eine bemerkenswerte Transformation durchlaufen, die die Art und Weise, wie wir mit Technologien interagieren, grundlegend verändert hat.

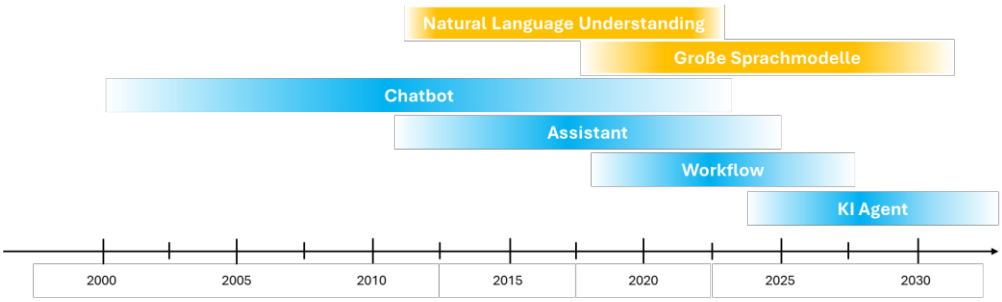


Abbildung 1 - Entwicklung vom Chatbot zum KI Agenten

Diese Timeline zeigt die evolutionären Schritte in der Entwicklung von vier bedeutenden KI-Tools: Chatbots z.B. Jabberwacky[10] , virtuellen Assistenten z.B. Siri[11], KI-gestützten Workflows und KI-Agenten. Jedes dieser Tools hat seinen eigenen Ursprung und Fortschritt, wobei sie zunehmend komplexere Aufgaben übernehmen und in verschiedenen Branchen Anwendung finden. Von den frühesten Chatbots bis hin zu hochentwickelten KI-Agenten spiegelt diese Entwicklung die rasanten Fortschritte in der Technologie und die wachsenden Erwartungen der Benutzer wider.

Natural Language Understanding

Natural Language Understanding (NLU) ist ein Teilbereich der Künstlichen Intelligenz (KI), der sich mit der Verarbeitung und dem Verständnis natürlicher Sprache beschäftigt. NLU ermöglicht es Maschinen, menschliche Sprache in einem Kontext zu verstehen, zu interpretieren und darauf zu reagieren[12].

Mit der Einführung neuer Techniken, wie statistischer Sprachverarbeitung in den 1990er Jahren und der Entwicklung neuronaler Netzwerke in den 2010er Jahren, begann NLU, an Bedeutung zu gewinnen. Insbesondere die Fortschritte im Bereich des maschinellen Lernens und der tieferen neuronalen Netze haben die Fähigkeit von Maschinen, menschliche Sprache zu verstehen, deutlich verbessert[13].

Die Anwendung von NLU ist besonders relevant in der Entwicklung von Chatbots und KI-Assistenten. Diese Systeme nutzen NLU, um mit Nutzern in natürlicher Sprache zu interagieren, Fragen zu beantworten und Aufgaben zu erledigen. Vor der Einführung von NLU waren Chatbots oft auf vordefinierte Skripte angewiesen, die nur in der Lage waren, einfache, regelbasierte Anfragen zu verarbeiten[14] [15].

Kommentiert [DH7]: Finde die Abbildung gut, im ersten Moment wunderte ich mich, dass es ab 2020 keine Assisstenten mehr geben sollte … aber ich glaube du meinst die Entwicklung, oder?

und noch 2 Anmerkungen:
1. Bitte das aktuelle Jahr 2025 mit anzeigen: Man will ja den aktuellen Stand wissen.
2. Beispiele nennen

Kommentiert [DH8]: Referenzen/Verweise nennen.

[10] https://www.jabberwacky.com/
[11] https://www.apple.com/siri/
[12] (MacCartney, 2014)
[13] (Foote, 2023)
[14] (Adamopoulou & Moussiades, 2020)
[15] (Codecademy Team, n.d.)

Sprachmodelle

Sprachmodelle[16] sind spezialisierte Algorithmen oder mathematische Modelle, die entwickelt wurden, um die Struktur und das Verhalten natürlicher Sprache zu erfassen. Sie analysieren große Mengen an Textdaten, um Muster, Zusammenhänge und Wahrscheinlichkeiten zwischen Wörtern und Phrasen zu lernen. Sprachmodelle sind ein zentraler Bestandteil von Natural Language Processing (NLP) und somit auch von Natural Language Understanding (NLU).

Sprachmodelle arbeiten in der Regel auf der Basis von statistischen Methoden oder maschinellem Lernen. Moderne Sprachmodelle, wie die Transformer-Architektur, nutzen tiefe neuronale Netzwerke, um kontextuelle Informationen zu erfassen und die Bedeutung von Wörtern in Abhängigkeit von ihrem Umfeld zu analysieren.

nellem Lernen. Moderne Sprachmodelle, wie die Transformer-Architektur, nutzen tiefe neuronale Netzwerke, um kontextuelle Informationen zu erfassen und die Bedeutung von Wörtern in Abhängigkeit von ihrem Umfeld zu analysieren.

Ein bekanntes Beispiel für ein leistungsfähiges Sprachmodell ist GPT (Generative Pre-trained Transformer), das von OpenAI entwickelt wurde. GPT kann Texte generieren, Fragen beantworten und sogar kreative Inhalte erstellen, indem es auf die zuvor gelernten Muster in der Sprache zurückgreift.

hat formatiert: Deutsch (Deutschland)

hat formatiert: Deutsch (Deutschland)

hat formatiert: Deutsch (Deutschland)

Kommentiert [TR9]: Alles richtig, geht meiner Meinung nach aber zu sehr ins Detail. Ich würde diesen Parts aus der Abbildung und den Text rausnehmen und das als gegebenes Wissen vorraussetzen.
@Dr. Christian Hillebrand Wir siehst du das?

Begriffsdifferenzierung / Abgrenzung

Chatbots, die bereits seit vielen Jahren im Einsatz sind, haben mittlerweile die Fähigkeit erlangt, Eingaben von Nutzern zuverlässig zu erkennen und darauf zu reagieren. Begriffe wie „KI-Assistenten" werden häufig synonym für KI-Modelle verwendet, die in der Lage sind, natürliche Sprache zu verstehen. Dies führt jedoch zu einer Verwischung der Begriffe „Chatbot", „Assistent" und „Agent".

Darüber hinaus entstehen neue Begriffe wie „KI-Workflow[17]" und „Agentic AI[18]", die ebenfalls zur Verwirrung beitragen können. Im folgenden Abschnitt werden wir diese Begriffe genauer betrachten und klar voneinander abgrenzen, um ein besseres Verständnis für ihre jeweiligen Bedeutungen und Anwendungen zu schaffen.

Typ	Zweck und Funktionalität	Interaktivität	Komplexität und Intelligenz
KI-Chatbots	Interaktion mit Benutzern, Beantwortung von Fragen	Dialoge basierend auf Text- oder Spracheingaben	Einfache Regel-basierte oder maschinelles Lernen-Modelle
KI-Assistenten	Umfassende Unterstützung, Aufgabenmanagement	Proaktive Unterstützung, kontextbewusst	Fortgeschrittene Algorithmen für Empfehlungen
KI-Workflows	Automatisierung komplexer Prozesse	Weniger interaktiv arbeiten im Hintergrund	Integration mehrerer KI-Technologien
KI-Agenten	Autonome Entscheidungen, Problemlösung	Interaktion mit Systemen/Benutzern ohne Anfrage	Setzt fortgeschrittene KI-Techniken ein, um selbstständig zu lernen
Agentic AI	Selbstständige Entscheidungsfindung und Handlungen	Hohe Interaktivität mit Anpassungsfähigkeit	Fortgeschrittene Lernalgorithmen, die dynamisch auf Veränderungen reagieren

Kommentiert [DH10]: Tabelle gefällt mir sehr gut - bin gespannt, wie sie das schriftsetzen.

Kommentiert [TR11R10]: Stimme mit Christian überein

[16] (Naveed, et al., 2024)
[17] (Intel Corporation)
[18] (Purdy, 2024)

Wir sehen, dass sich die Begriffe inhaltlich – technisch wie funktionell – unterscheiden. Dabei müssen wir bedenken, dass es bei Software-Systemen durchaus möglich ist, die einzelne Typen zu kombinieren, die eine klare Differenzierung schwieriger macht.

Das Konzept von KI-Agenten

Folgende Grafik visualisiert die Struktur eines KI-Agenten und zeigt die wesentlichen Komponenten, die zusammenarbeiten, um seine Funktionalität zu gewährleisten:

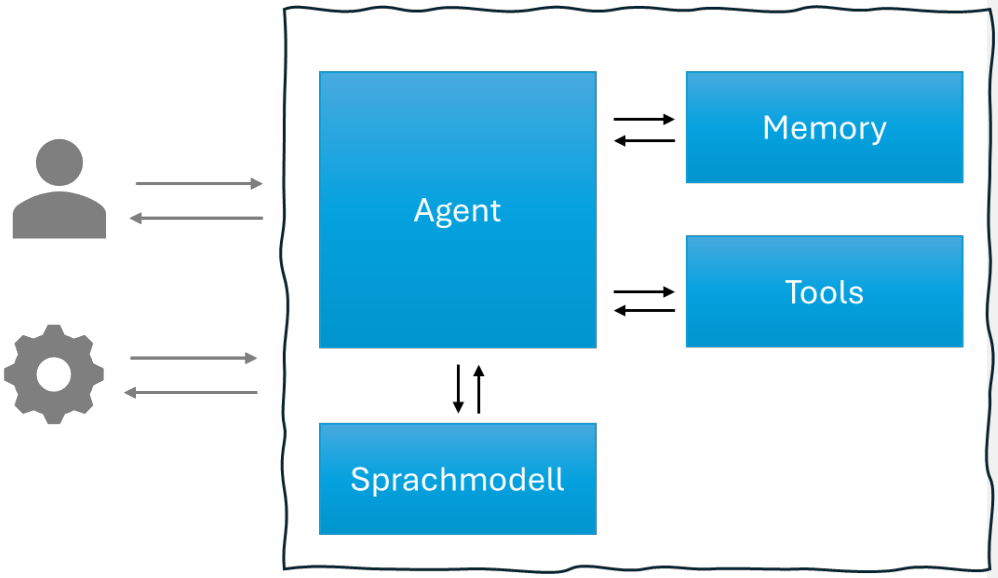


Abbildung 2 - prinzipieller Aufbau eines KI-Agenten

Agent

Der Agent ist das Programm, das Eingaben von Usern oder anderen Systemen aufnehmen kann. Ausgehend von einer Anfrage in natürlicher Sprache wird diese an das Sprachmodell (LLM) weitergeleitet.

Der Agent übernimmt die Steuerung der Eingaben, die Kommunikation mit dem Sprachmodell und die Reaktion auf Ergebnisse des Sprachmodells. Stellen wir uns vor, der Agent übernimmt weitestgehend die Funktion des Anwenders als Kommunikationspartner mit dem Sprachmodell und reagiert auf Ergebnisse von Anfragen an das Sprachmodell.

Im Agenten ist festgelegt, welche Werkzeuge (Tools) zur Verfügung stehen.

Sprachmodell

Das Sprachmodell befähigt den KI-Agenten, Sprache zu verstehen, zu interpretieren und darauf zu reagieren. Es analysiert Benutzeranfragen, um sowohl die Absicht als auch den Kontext zu erfassen.

Zusätzlich kann das Sprachmodell auf die Tools des Agenten zugreifen, die über die reine Sprachverarbeitung hinausgehen, wie in der Abbildung dargestellt. So kann der Agent beispielsweise auf externe Datenquellen zugreifen, Informationen abrufen, Berechnungen durchführen oder Bilder generieren. Diese erweiterten

Kommentiert [TR12]: Dopplung zu oben oder nicht? Da wo du die Begriffe bereits erklärt hast.

Kommentiert [LS13R12]: Hier ist eher technische betrachtung

Funktionen ermöglichen es dem Agenten, komplexere Anfragen zu bearbeiten und den Benutzern nützliche, handlungsorientierte Ergebnisse zu liefern.

Beispiele für Sprachmodelle: GPT-4o[19], GPT-4o-mini[20] von OpenAI, Llama 3[21] von Meta, Mistral Large[22] von Mistral.

Memory

Unter Speicher verstehen wir in diesem Zusammenhang die temporäre Speicherung des Gesprächsverlaufs, die entscheidend für das Verständnis des Kontextes ist.

Es können auch langlebige[23] Speichertechnologien verwendet werden, das sollte vom Einsatzzweck des Agenten abhängig gemacht werden.

Tools

Mit Tools werden Techniken beschrieben, die es dem Agenten ermöglichen, Aktionen auszuführen, die für die Bearbeitung einer Query notwendig sind.

Im Agenten werden die Werkzeuge mit mindestens zwei Informationen beschrieben:

- **Beschreibung**: hierbei handelt es sich um eine ausformulierte Beschreibung des Tools, inkl. Name des Tools, was es kann und welche Parameter benötigt werden
- **Funktion des Tools**: Beschreibung der Funktion selbst, das kann z.B. Programm-Code oder ein API-Aufruf sein

[19] https://openai.com/index/hello-gpt-4o/
[20] https://openai.com/index/gpt-4o-mini-advancing-cost-efficient-intelligence/
[21] https://ai.meta.com/blog/meta-llama-3/
[22] https://mistral.ai/news/mistral-large
[23] (Pędich, 2024)

Arten von Agenten

Je nach ihrer spezifischen Einsatzart lassen sich KI-Agenten in verschiedene Kategorien einteilen[24], die in der nachstehenden Übersicht detailliert dargestellt sind:

Art	Beschreibung
Simple reflex agents	Ein einfacher Reflexagent ist eine grundlegende Art von künstlicher Intelligenz, die Entscheidungen nur auf Basis der Informationen trifft, die sie gerade erhält. Er reagiert sofort auf das, was in seiner Umgebung passiert, ohne dass er sich an frühere Erfahrungen erinnert oder etwas lernen muss. Sein Verhalten wird durch festgelegte Regeln bestimmt, die sagen, wie er auf bestimmte Situationen reagieren soll. **Komponenten** • Sensoren: Diese Geräte sammeln Informationen aus der Umgebung, ähnlich wie unsere Sinne. Bei einfachen Reflexagenten sind die Sensoren oft einfache Geräte, die bestimmte Dinge wie Temperatur oder Licht erkennen. • Regeln für Reaktionen: Diese festgelegten Regeln legen fest, wie der Agent auf bestimmte Informationen reagieren soll. Wenn er eine bestimmte Situation erkennt, führt er sofort die passende Aktion aus. • Aktuatoren: Diese setzen die Entscheidungen des Agenten in die Tat um. Sie machen Dinge wie das Einschalten von Lichtern oder das Aktivieren eines Heizsystems. **Anwendungsbeispiele** Einfache Reflexagenten sind besonders nützlich in klaren und vorhersehbaren Umgebungen. Zum Beispiel können sie in Fabriken eingesetzt werden, um Maschinen sofort abzuschalten, wenn ein Hindernis erkannt wird. Auch Sprinklersysteme, die bei Rauch automatisch angehen, oder E-Mail-Auto-Responder, die sofort auf bestimmte Nachrichten reagieren, sind gute Beispiele für den Einsatz solcher Agenten.
Modell-based reflex agents	Ein modellbasierter Reflexagent ist eine fortgeschrittene Art von intelligenten Agenten, die in Umgebungen arbeiten, die nicht vollständig beobachtbar sind. Im Gegensatz zu einfachen Reflexagenten, die nur auf aktuelle Sinneseingaben reagieren, hat ein modellbasierter Agent ein internes Modell von seiner Umgebung. Dieses Modell hilft dem Agenten, zu verstehen, wie sich die Umgebung verändert, und ermöglicht es ihm, auch Dinge zu erkennen, die er nicht direkt sehen kann. Obwohl diese Agenten nicht wirklich wie komplexere Agenten "erinnern", nutzen sie ihr Weltmodell, um bessere Entscheidungen zu treffen. **Komponenten** • Zustandsverfolger: Dieser Teil hält Informationen über den aktuellen Zustand der Umgebung fest, basierend auf dem Weltmodell und den Sensorinformationen. • Weltmodell: Es enthält Wissen darüber, wie sich die Umgebung unabhängig vom Agenten verändert und wie die Handlungen des Agenten die Umgebung beeinflussen. • Überlegungsmechanismus: Dieser nutzt das Weltmodell und den aktuellen Zustand, um die passenden Aktionen basierend auf festgelegten Regeln zu bestimmen. **Anwendungsbeispiele** Modellbasierte Reflexagenten sind besonders nützlich in Situationen, in denen der aktuelle Zustand nicht nur aus den Sensordaten abgeleitet werden kann. Zum Beispiel können sie in Smart Home Sicherheitssystemen eingesetzt werden. Diese Agenten,erkennen dann Muster normaler Aktivitäten, um zwischen alltäglichen Ereignissen und möglichen Bedrohungen zu unterscheiden. Auch in Qualitätssicherungssystemen, die Herstellungsprozesse überwachen, oder in Netzwerküberwachungstools, die den Zustand und den Datenverkehr im Netz beobachten, finden sie Anwendung.

[24] (Doria, 2024)

Goal-based agents	Zielgestützte Agenten sind eine Art von KI, die darauf ausgelegt ist, bestimmte Ziele zu erreichen. Sie schauen nicht nur auf die aktuellen Umweltdaten, sondern planen auch, welche Schritte sie unternehmen müssen, um ihr Ziel zu erreichen. Diese Agenten wählen immer den besten und effizientesten Weg, um ihre Aufgaben zu erfüllen. **Wichtige Merkmale** • Zielzustand: Eine klare Beschreibung dessen, was der Agent erreichen möchte. • Planungsmechanismus: Die Fähigkeit, verschiedene Aktionsfolgen zu untersuchen, die zum Ziel führen könnten. • Zustandsevaluation: Methoden, um zu bewerten, ob zukünftige Zustände näher zum Ziel führen oder nicht. • Aktionsauswahl: Der Prozess, bei dem der Agent entscheidet, welche Aktionen am besten zum Erreichen des Ziels beitragen. **Anwendungsbeispiele** Zielgestützte Agenten sind besonders nützlich für komplexe Aufgaben mit klaren Zielen. Dazu gehören industrielle Roboter, die Produkte montieren, automatisierte Lagersysteme, die optimale Wege zum Abrufen von Artikeln planen, sowie smarte Heizsysteme, die Temperaturanpassungen für optimalen Komfort planen.
Learning agents	Ein lernender Agent ist ein KI-System, das sich ständig verbessert, indem es aus seinen Erfahrungen lernt. Er nutzt sensorische Eingaben und Feedbacks, um sein Verhalten anzupassen und zu optimieren. Außerdem hat er einen Problemgenerator, der neue Aufgaben erstellt, damit der Agent sich auf Basis gesammelter Daten weiterentwickeln kann. **Wichtige Merkmale** • Lernmechanismus: Der Agent passt sein Verhalten an, basierend auf dem Feedback, das er von seinen Erfahrungen erhält. • Problemgenerator: Er entwickelt neue Aufgaben, um dem Agenten zu helfen, noch besser zu werden. **Anwendungsbeispiele** Lernende Agenten sind besonders nützlich in Bereichen, in denen sie durch Erfahrung besser werden müssen, wie zum Beispiel in der industriellen Prozesskontrolle, bei Energiemanagementsystemen oder in Kundenservice-Chatbots, die ihre Antwortgenauigkeit verbessern, indem sie aus den Interaktionen mit Nutzern lernen.
Utility-based agents	Ein nutzengestützter Agent trifft Entscheidungen, indem er die möglichen Ergebnisse seiner Handlungen bewertet und das auswählt, was den größten Nutzen bringt. Dieser Agent vergleicht verschiedene Optionen und deren Vorteile, um die beste Wahl zu treffen. Zum Beispiel kann ein solcher Agent Kunden helfen, die schnellste Flugroute zu finden, ohne dass der Preis für die Tickets eine Rolle spielt. **Wichtige Merkmale** • Nutzungsbewertung: Der Agent verwendet eine Methode, um den Wert verschiedener Optionen zu bestimmen. • Entscheidungsfindung: Er wählt Aktionen aus, die den höchsten Nutzen versprechen. **Anwendungsbeispiele** Nutzengestützte Agenten sind besonders hilfreich in Situationen, in denen mehrere Ziele in Einklang gebracht werden müssen, wie zum Beispiel bei der Ressourcenverteilung in Unternehmen, im Gebäudemanagement oder bei der Planung von Aufgaben, wo Prioritäten und Fristen berücksichtigt werden müssen.
Autonome Agenten	Ein autonomer Agent ist ein KI-System, das die Fähigkeit besitzt, unabhängig Entscheidungen zu treffen und Aktionen auszuführen, ohne dass kontinuierlich ein Mensch interveniert. Der autonome Agent nutzt seine Programmierung, um Umgebungsdaten zu analysieren, Ziele zu definieren und Strategien zu entwickeln, um diese Ziele zu erreichen. Zudem lernt er oft aus seinen Erfahrungen, um seine Leistung im Laufe der Zeit zu optimieren. **Wichtige Merkmale** • Unabhängige Entscheidungsfindung: Der Agent trifft Entscheidungen basierend auf der Analyse von Umgebungsdaten und definierten Zielen. • Lernmechanismus: Er verbessert seine Leistung kontinuierlich, indem er aus seinen Erfahrungen lernt. **Anwendungsbeispiele** Autonome Agenten sind besonders nützlich in Bereichen, in denen sie selbstständig agieren müssen, wie zum Beispiel bei autonomen Fahrzeugen, die Verkehrsbedingungen analysieren und sicher navigieren, oder bei intelligenten Robotern in der Industrie, die Aufgaben eigenständig erledigen.

Model Context Protocol

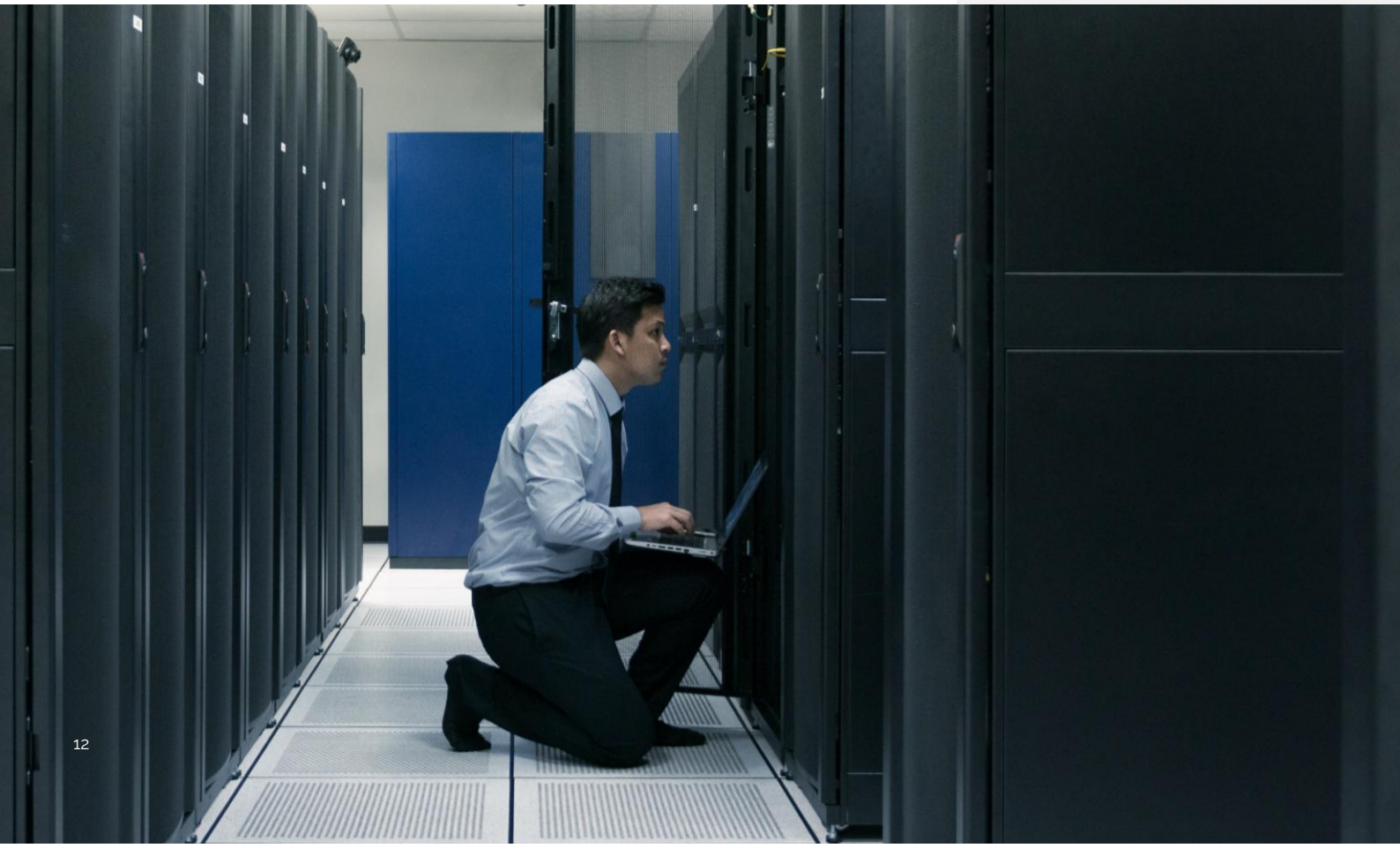
„MCP is an open protocol that standardizes how applications provide context to LLMs. Think of MCP like a USB-C port for AI applications. Just as USB-C provides a standardized way to connect your devices to various peripherals and accessories, MCP provides a standardized way to connect AI models to different data sources and tools.“ [25]

Das Model Context Protocol (MCP) ist ein offenes Protokoll, dass eine standardisierte Kommunikation mit Sprachmodellen erlauben soll.

Aktuell muss für die Kommunikation mit Sprachmodellen auf die jeweilige Erfordernissen der vom Modellhersteller bereitgestellten Schnittstelle Rücksicht genommen werden. Das heißt, für jedes Software-Projekt müssen die modell-spezifischen Erweiterungen integriert und beachtet werden, damit die Applikation mit verschiedenen Sprachmodellen der unterschiedlichen Hersteller funktionieren.

Das MCP ist ein Ansatz, ein standardisiertes Protokoll für die Nutzung der jeweiligen Schnittstelle zu etablieren, um Sprachmodelle mit Funktionen zu erweitern.

[25] (modelcontextprotocol.io, n.d.)



Multi-Agenten-Systeme

Bisher wurden die grundlegenden Eigenschaften und Fähigkeiten eines einzelnen KI-Agenten betrachtet. Diese sind für einen bestimmten Einsatzzweck spezifiziert und geschaffen, was bedeutet, dass sie für bestimmte, einfache Aufgaben optimiert sind.

Steigen die Anforderungen bzw. Komplexität der Aufgaben, kommen einzelne KI-Agenten an ihre Grenzen. Eine Lösung ist der Ansatz, mehrere KI-Agenten, optimiert für verschiedene Aufgaben, in einem Verbund zusammen zu fassen, um eine Aufgabe zu bearbeiten.

"A multiagent system (MAS) consists of multiple artificial intelligence (AI) agents working collectively to perform tasks on behalf of a user or another system.[26]"

Vergleich mit Single-KI-Agenten

Im Folgenden eine Gegenüberstellung von Single-Agenten und Multi-Agenten-Systemen:

Eigenschaft	Single-Agenten	Multi-Agenten-Systeme (MAS)
Definition	KI-Systeme, die in einer isolierten Umgebung operieren und auf festgelegte Aufgaben spezialisiert sind.	Systeme, die aus mehreren Agenten bestehen, die kommunizieren und zusammenarbeiten, um komplexe Probleme zu lösen.
Autonomie	Arbeiten in der Regel isoliert und basierend auf klar definierten Regeln und Algorithmen.	Agieren autonom, können jedoch Informationen austauschen und sich gegenseitig unterstützen.
Anpassungsfähigkeit	Weniger anpassungsfähig an Veränderungen in ihrer Umgebung; reagieren auf spezifische Eingaben oder vorprogrammierte Szenarien.	Höhere Flexibilität durch Zusammenarbeit; können dynamisch auf Änderungen in der Umgebung reagieren.
Beispiel	Ein einfacher Chatbot, der auf spezifische Fragen antwortet.	Systeme in der logistischen Planung, Robotik oder Simulation sozialer Interaktionen, wo Agenten gemeinsam Entscheidungen treffen.
Koordination	Keine oder begrenzte Koordination; arbeitet unabhängig.	Erfordert Koordination, Verhandlung und Zusammenarbeit zwischen den Agenten, um gemeinsame Ziele zu erreichen.
Ressourcennutzung	Ressourcen und Fähigkeiten sind auf den einzelnen Agenten beschränkt.	Effizientere Ressourcennutzung durch die Zusammenarbeit mehrerer Agenten.
Komplexität der Probleme	Typischerweise fokussiert auf einfachere Probleme oder Aufgaben.	Eignen sich gut für komplexe Probleme, die mehrere Dimensionen oder Variablen beinhalten.

[26] (Gutowska, What is a multiagent system?, 2024)

Fazit

Die Analyse zeigt, dass Single-Agenten und Multi-Agenten-Systeme grundlegend unterschiedliche Ansätze zur Problemlösung bieten. Während Single-Agenten in der Regel innerhalb eines festgelegten Rahmens operieren und auf spezifische, isolierte Aufgaben fokussiert sind, bieten Multi-Agenten-Systeme eine dynamischere und flexiblere Lösung für komplexe Herausforderungen.

Single-Agenten sind ideal für Anwendungen, in denen die Aufgaben klar definiert und die Anforderungen stabil sind. Sie arbeiten unabhängig auf Basis vorprogrammierter Regeln, was sie weniger anpassungsfähig an Veränderungen macht. Im Gegensatz dazu ermöglichen Multi-Agenten-Systeme eine koordinierte Zusammenarbeit zwischen mehreren Agenten, die Informationen austauschen und sich gegenseitig unterstützen. Diese Interaktion führt zu einer effizienteren Ressourcennutzung und einer höheren Flexibilität, insbesondere in komplexen und dynamischen Umgebungen.

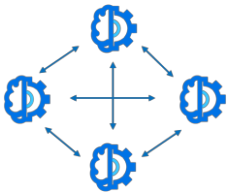
Insgesamt lässt sich festhalten, dass die Wahl zwischen einem Single-Agenten und einem Multi-Agenten-System stark von den spezifischen Anforderungen der jeweiligen Anwendung abhängt. Während einfache Aufgaben effizient von einem einzelnen Agenten gelöst werden können, erfordern komplexere Szenarien häufig die Synergien, die nur durch die Zusammenarbeit mehrerer Agenten erreicht werden können. Daher sind Multi-Agenten-Systeme besonders wertvoll in Bereichen wie Logistik, Robotik und sozialen Simulationen, wo die Dynamik und Komplexität der Probleme eine adaptive und kooperative Herangehensweise erfordern.

Architekturen

Es gibt verschiedene Typen von Multi-Agenten-Architekturen, die unterschiedliche organisatorische Strukturen und Interaktionsmuster zwischen den Agenten aufweisen. Im Folgenden werden einige der gängigsten Architekturtypen vorgestellt:

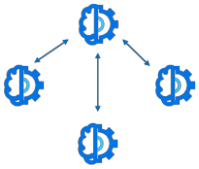
Netzwerkkonfiguration

In dieser Architektur werden Agenten als Knotengraphen definiert, wobei jeder Agent mit jedem anderen Agenten (viele-zu-viele-Verbindungen) kommunizieren kann. Jeder Agent entscheidet, welchen anderen Agenten er als nächstes aufruft. Diese Architektur eignet sich für Probleme ohne klare Hierarchie oder spezifische Reihenfolge der Agentenaufrufe.



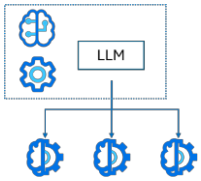
Supervisor-Architektur

Hier entscheidet ein Supervisor-Agent, welche Agenten als nächstes aufgerufen werden sollen. Der Supervisor kann Entscheidungen basierend auf dem aktuellen Zustand treffen und die Ausführung entsprechend weiterleiten. Diese Architektur unterstützt das parallele Ausführen mehrerer Agenten und die Verwendung von Map-Reduce-Mustern.



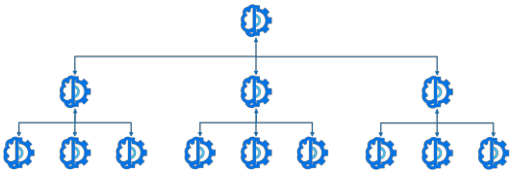
Supervisor (Werkzeugaufruf) Architektur

Eine Variante der Supervisor-Architektur, bei der einzelne Agenten als Werkzeuge dargestellt werden. Ein Werkzeugaufruf-LLM im Supervisor-Knoten entscheidet, welche Agentenwerkzeuge aufgerufen werden, und welche Argumente übergeben werden sollen. Dies kann als ReAct-Style-Agent mit einem LLM-Knoten (Supervisor) und einem Werkzeugausführungsknoten implementiert werden.



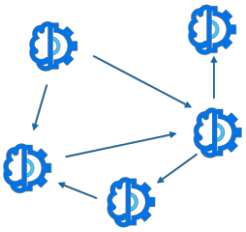
Hierarchische Architektur

Diese Architektur umfasst die Erstellung einer Hierarchie von Agenten mit Supervisors, die spezialisierte Teams von Agenten verwalten. Ein Top-Level-Supervisor überwacht diese Teams und sorgt für effizientes Management und Entscheidungsfindung innerhalb des Systems. Dieser Ansatz adressiert die Komplexitäts- und Skalierbarkeitsprobleme, die in großen MAS auftreten können.



Benutzerdefinierter Multi-Agenten-Workflow

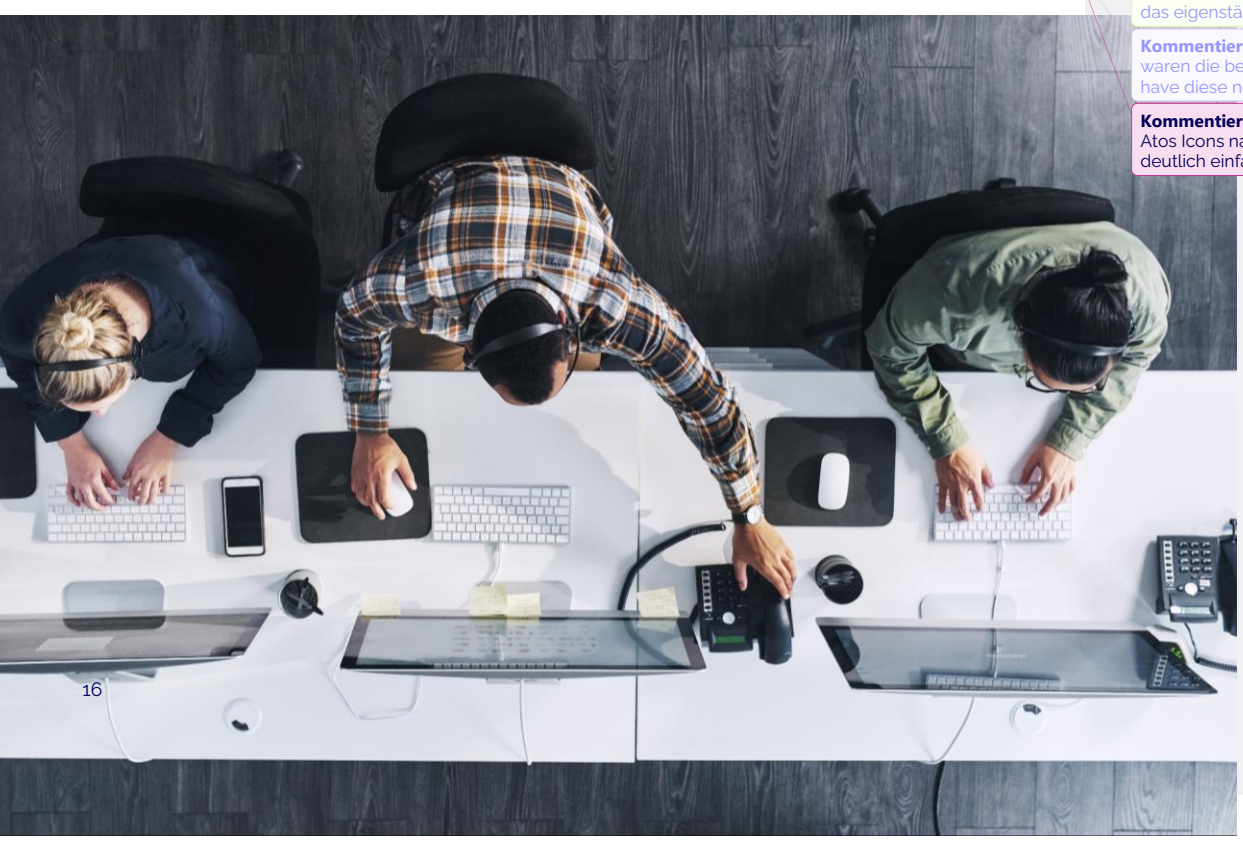
In dieser Architektur ist der Workflow vordefiniert, wobei die Agenten in einer bestimmten Reihenfolge kommunizieren. Dies kann durch:
Expliziter Kontrollfluss: Die Reihenfolge der Agentenkommunikation wird über normale Graph-Kanten explizit definiert, was einen deterministischen Kontrollfluss ermöglicht.
Dynamischer Kontrollfluss: LLMs dürfen Teile des Anwendungskontrollflusses entscheiden, indem sie Command-Objekte verwenden. Ein spezieller Fall davon ist die Supervisor-Werkzeugaufruf-Architektur, bei der das Werkzeugaufruf-LLM des Supervisor-Agenten über die Reihenfolge der Werkzeuge (Agenten) entscheidet.



Kommentiert [DH14]: Gehört das unter "5. Benutzerdefinierter Multi-Agent-Workflow"? Oder ist das eigenständig ?

Kommentiert [LS15R14]: In der whitepaper vorlage waren die begrifflichkeiten nicht 100% eindeutig. Ich have diese neu geordnet

Kommentiert [TR16]: Hier gibt es Grafiken zu die mit Atos Icons nachgebildet werden sollten. Macht es deutlich einfacher zu verstehen und kürzer.



Frameworks für KI-Agenten

Frameworks für KI-Agenten sind strukturierte Softwareumgebungen, die Entwicklern helfen, KI-Agenten zu erstellen, zu implementieren und zu verwalten. Diese Frameworks bieten eine Vielzahl von Werkzeugen, Bibliotheken und vorgefertigten Algorithmen, die den Entwicklungsprozess erleichtern.

Folgende Übersicht soll einen Einblick geben:

Name	Beschreibung	Key Funktionalitäten
AutoGen	Das Framework AutoGen von Microsoft ist eine umfassende Lösung zur Erstellung und Verwaltung von AI Agents, insbesondere für Multi-Agenten-Workflows	1. Multi-Agenten-Workflows: AutoGen ermöglicht die Erstellung und Verwaltung von komplexen Multi-Agenten-Workflows. Dies bedeutet, dass mehrere AI Agents gleichzeitig interagieren und zusammenarbeiten können, um Aufgaben effizient zu lösen. 2. Schichtweises und erweiterbares Design: Das Framework ist in verschiedenen Schichten aufgebaut, die klar voneinander abgegrenzt sind. Jede Schicht baut auf der darunterliegenden auf, was die Erweiterbarkeit und Anpassungsfähigkeit des Systems erleichtert.. 3. Integrierte Kommunikationsschnittstellen: AI Agents, die mit AutoGen erstellt werden, verfügen über einheitliche Kommunikationsschnittstellen. Diese Schnittstellen ermöglichen es den Agents, Nachrichten zu senden und zu empfangen sowie entsprechende Antworten zu generieren. 4. Automatisierte Agenten-Interaktion: Die Kommunikation und Interaktion zwischen den Agents erfolgt automatisiert, bis vordefinierte Bedingungen erfüllt sind. Dies reduziert den manuellen Eingriff und erhöht die Effizienz. 5. Integration mit Semantic Kernel: AutoGen arbeitet eng mit Microsofts Semantic Kernel zusammen, um eine erstklassige Entwicklererfahrung zu bieten. Semantic Kernel bietet enterprise-fähige AI-Funktionalitäten, und die Zusammenarbeit mit AutoGen ermöglicht eine nahtlose Integration und Unterstützung für die Entwicklung von Agenten-Anwendungen.
MetaGPT	MetaGPT ist ein innovatives Framework, das darauf abzielt, die Funktionsweise eines kompletten KI-Softwareunternehmens zu simulieren. Durch die Orchestrierung von menschlichem prozeduralem Wissen und AI Agents, die von großen Sprachmodellen (LLMs) angetrieben werden, bietet MetaGPT eine hochgradig anpassungsfähige und transformative Plattform zur Entwicklung von Softwarelösungen	1. Multiagenten-Framework: MetaGPT organisiert mehrere spezialisierte AI Agents, die zusammenarbeiten, um komplexe Aufgaben zu erledigen, ähnlich wie die Abteilungen in einem traditionellen Softwareunternehmen. 2. gen, ähnlich wie die Abteilungen in einem traditionellen Softwareunternehmen. 3. Automatische Softwareentwicklung: Das Framework kann natürliche Sprachanforderungen in vollständige Softwareimplementierungen umwandeln und den gesamten Entwicklungsprozess automatisch generieren, einschließlich Design, Codierung, Testen und Bereitstellung. 4. Orchestrierung von menschlichem Wissen und AI: Durch die Kombination von menschlichem prozeduralem Wissen mit AI Agents ermöglicht MetaGPT eine effiziente und intelligente Steuerung der Entwicklungsprozesse. 5. Flexibilität und Anpassungsfähigkeit: MetaGPT ist darauf ausgelegt, sich schnell an verschiedene Anforderungen und Umgebungen anzupassen, was es zu einer agilen Lösung für unterschiedliche Softwareprojekte macht.

hat formatiert: Deutsch (Deutschland)

hat formatiert: Deutsch (Deutschland)

hat formatiert: Deutsch (Deutschland)

LangGraph	LangGraph ist ein fortschrittliches Framework, das speziell für die Erstellung und Verwaltung von Multi-Agenten-Systemen entwickelt wurde. Es gehört zum LangChain-Ökosystem und bietet eine strukturierte Plattform zur Entwicklung, Orchestrierung und Kontrolle von AI Agents.	1. Modularität und Kontrolle: LangGraph ist so konzipiert, dass es Modularität und Kontrolle in Anwendungen bringt, die komplexe logische Strukturen erfordern. Es ermöglicht Entwicklern, verschiedene AI Agents in einem kontrollierten und koordinierten Umfeld zu orchestrieren. 2. Integration von Wissensgraphen: Das Framework nutzt Wissensgraphen, um Beziehungen und Verbindungen zwischen Daten zu modellieren. Diese Graphen unterstützen AI Agents bei der Verarbeitung und Interpretation komplexer Datenstrukturen. 3. Agentic Search Capabilities: LangGraph integriert agentische Suchfähigkeiten, die es AI Agents ermöglichen, Wissen effizient zu durchsuchen und relevante Informationen schnell zu finden. 4. Entwicklung, Debugging und Wartung: Das Framework bietet umfassende Werkzeuge zur Entwicklung, Debugging und Wartung von AI Agents. Dies erleichtert den gesamten Lebenszyklus der Agentenentwicklung und stellt sicher, dass sie optimal funktionieren. 5. Zusammenarbeit von AI Agents: LangGraph ermöglicht die Zusammenarbeit mehrerer spezialisierter AI Agents, die gemeinsam komplexe Aufgaben lösen können. Dies umfasst die Fähigkeit zur parallelen Verarbeitung und Koordination.
LlamaIndex	LlamaIndex Agents ist ein leistungsstarkes Framework, das speziell für die Erstellung und Verwaltung von AI Agents entwickelt wurde, die auf die Verarbeitung und Analyse großer Datenmengen spezialisiert sind. Dieses Framework nutzt fortschrittliche Indexierungs- und Suchtechnologien, um AI Agents in die Lage zu versetzen, effizient und zielgerichtet auf relevante Informationen zuzugreifen.	1. Fortschrittliche Indexierung: LlamaIndex Agents nutzt fortschrittliche Indexierungstechnologien, um große Datenmengen effizient zu organisieren und zu durchsuchen. Dies ermöglicht AI Agents, schnelle und präzise Suchergebnisse zu liefern. 2. Skalierbare Datenverarbeitung: Das Framework ist darauf ausgelegt, große Datenmengen zu verarbeiten und zu analysieren. Es bietet skalierbare Lösungen für Daten-intensive Aufgaben und unterstützt die effiziente Handhabung wachsender Datenbestände. 3. Integrierte Suchfunktionen: LlamaIndex Agents bietet leistungsstarke Suchfunktionen, die es den AI Agents ermöglichen, relevante Informationen schnell und präzise zu finden. Dieser Ansatz verbessert die Effizienz und Genauigkeit der Datenanalysen. 4. Modulare Architektur: Die modulare Architektur des Frameworks ermöglicht es Entwicklern, spezifische Module und Erweiterungen hinzuzufügen, um die Funktionalität der AI Agents an individuelle Anforderungen anzupassen. 5. Einfache Integration: LlamaIndex Agents lässt sich leicht in bestehende Systeme und Anwendungen integrieren, was eine nahtlose Erweiterung der Funktionalitäten ermöglicht. 6.
CrewAI	CrewAI ist ein innovatives Framework, das speziell für die Entwicklung und Verwaltung von kollaborativen AI Agents entwickelt wurde. Diese Plattform ermöglicht es, mehrere AI Agents in einem koordinierten Umfeld zusammenarbeiten zu lassen, um komplexe Aufgaben effizient zu lösen.	1. Kollaborative AI Agents: CrewAI ist darauf ausgelegt, mehrere spezialisierte AI Agents zu koordinieren, die zusammenarbeiten, um komplexe Problemstellungen zu bewältigen. Dieser Ansatz ermöglicht eine effiziente Verteilung und Bearbeitung von Aufgaben. 2. Modulare Architektur: Das Framework besitzt eine modulare Architektur, die es Entwicklern ermöglicht, spezifische Module und Erweiterungen hinzuzufügen, um die Funktionalität der AI Agents an individuelle Anforderungen anzupassen. 3. Task Management: CrewAI bietet umfassende Werkzeuge für das Task Management, einschließlich der Zuweisung, Überwachung und Koordination von Aufgaben, die von verschiedenen AI Agents bearbeitet werden. 4. Kommunikationsprotokolle: Das Framework integriert fortschrittliche Kommunikationsprotokolle, die eine reibungslose Interaktion und Datenübertragung zwischen den AI Agents ermöglichen, was die Zusammenarbeit und Effizienz verbessert. 5. Skalierbarkeit: CrewAI ist darauf ausgelegt, skalierbar zu sein und kann sowohl kleine als auch große Implementierungen unterstützen. Dies macht es ideal für den Einsatz in unterschiedlichsten Projekten und Unternehmensgrößen.

Phidata	Phidata ist ein spezialisiertes Framework, das sich auf die Erstellung und Verwaltung von AI Agents konzentriert, die Datenanalyse und maschinelles Lernen (ML) in Unternehmen unterstützen. Das Framework bietet eine umfassende Plattform zur Integration von AI-Technologien in Datenpipelines und analytische Prozesse.	1. Integrierte Datenpipelines: Phidata ermöglicht die Erstellung und Verwaltung von Datenpipelines, die Daten aus verschiedenen Quellen extrahieren, transformieren und laden (ETL). Diese Pipelines sind darauf ausgelegt, AI Agents mit den notwendigen Daten zu versorgen. 2. Automatisierte Datenanalyse: Das Framework bietet Tools zur automatisierten Datenanalyse, die es AI Agents ermöglichen, Muster und Erkenntnisse aus großen Datenmengen zu extrahieren und zu verarbeiten. 3. Maschinelles Lernen (ML) und AI: Phidata integriert fortschrittliche ML-Modelle und AI-Algorithmen, um Vorhersagen, Klassifizierungen und andere datenbasierte Entscheidungen zu treffen. Diese Modelle können in die Datenpipelines eingebettet werden, um kontinuierlich aktualisierte Analysen zu liefern. 4. Modulare Architektur: Das Framework ist modular aufgebaut, was es Entwicklern ermöglicht, spezifische Funktionen und Erweiterungen hinzuzufügen, um die AI Agents an individuelle Anforderungen anzupassen. 5. Visualisierung und Berichterstattung: Phidata bietet umfassende Werkzeuge zur Visualisierung und Berichterstattung, die es ermöglichen, die Ergebnisse der Datenanalyse und ML-Modelle in verständlichen und ansprechenden Formaten darzustellen.
Pydantic AI	Pydantic AI ist ein Python-Agenten-Framework, das die Entwicklung von KI-Anwendungen vereinfacht, indem es die Stärken von Pydantic (Datenvalidierung) mit spezialisierten Features für generative KI (GenAI) kombiniert.	1. Strukturierte Datenverwaltung: Pydantic Agents nutzt Pydantic zur strikten Typisierung und Validierung von Datenmodellen. Dies gewährleistet die Konsistenz und Zuverlässigkeit der Daten, die von den AI Agents verarbeitet werden. 2. Erstellung und Verwaltung von AI Agents: Das Framework bietet umfassende Werkzeuge zur Erstellung, Verwaltung und Orchestrierung von AI Agents, die verschiedene Aufgaben und Prozesse automatisieren können. 3. Nahtlose Integration mit FastAPI: Pydantic Agents ist nahtlos in FastAPI integriert, ein schnelles Web-Framework für Python, das auf Pydantic basiert. Dies ermöglicht die einfache Erstellung und Bereitstellung von Webdiensten und APIs. 4. Erweiterbarkeit und Anpassungsfähigkeit: Die modulare Architektur von Pydantic Agents ermöglicht es Entwicklern, spezifische Funktionen und Erweiterungen hinzuzufügen, um die AI Agents an individuelle Anforderungen anzupassen. 5. Einfache Fehlerbehandlung und Debugging: Durch die strikte Typisierung und Validierung von Datenmodellen wird die Fehlerbehandlung und das Debugging vereinfacht, was die Entwicklungszeit verkürzt und die Zuverlässigkeit erhöht.
N8N	n8n ist ein Open-Source-Framework, das für die Workflow-Automatisierung entwickelt wurde und sich insbesondere durch seine Flexibilität und Benutzerfreundlichkeit auszeichnet. Es bietet umfassende Möglichkeiten, AI Agents in verschiedene Prozesse zu integrieren und diese effizient zu automatisieren.	1. Visuelle Workflow-Erstellung: n8n bietet eine Drag-and-Drop-Oberfläche, die es ermöglicht, Workflows einfach zu erstellen und zu verwalten, ohne dass Programmierkenntnisse erforderlich sind. 2. Multi-Triggering: Workflows können durch verschiedene Auslöser wie Webhooks, Zeitpläne oder externe Ereignisse gestartet werden, was die Flexibilität erhöht. 3. Integration mit AI-Diensten: n8n ermöglicht eine nahtlose Verbindung mit verschiedenen AI-Diensten und APIs, wodurch AI-Funktionen leicht in bestehende Workflows integriert werden können. 4. Open-Source und Selbst-Hosting: Als Open-Source-Tool bietet n8n die Möglichkeit, die Software selbst zu hosten und anzupassen, was volle Kontrolle und Flexibilität bei der Anpassung an spezifische Bedürfnisse ermöglicht.

Botpress	Botpress ist eine leistungsstarke Open-Source-Plattform zur Erstellung und Verwaltung von AI Agents, speziell für die Entwicklung von Chatbots und virtuellen Assistenten. Diese Plattform zeichnet sich durch ihre Benutzerfreundlichkeit, Flexibilität und umfassende Funktionsvielfalt aus, die es Entwicklern ermöglicht, maßgeschneiderte und skalierbare Chatbots zu erstellen.	1. Visuelle Entwicklungsumgebung: Botpress bietet eine benutzerfreundliche, visuelle Oberfläche, die es Entwicklern ermöglicht, Chatbots durch Drag-and-Drop-Interaktionen zu erstellen und zu verwalten, ohne tiefgehende Programmierkenntnisse zu benötigen. 2. h Drag-and-Drop-Interaktionen zu erstellen und zu verwalten, ohne tiefgehende Programmierkenntnisse zu benötigen. 3. Modulare Architektur: Das Framework basiert auf einer modularen Architektur, die es Entwicklern erlaubt, spezifische Funktionen und Erweiterungen hinzuzufügen, um die Chatbots an individuelle Anforderungen anzupassen. 4. Natürliche Sprachverarbeitung (NLP): Botpress integriert fortschrittliche NLP-Techniken zur Intent-Klassifizierung und Entitätserkennung, um die Absichten der Benutzer zu verstehen und relevante Antworten zu generieren. 5. Multichannel-Unterstützung: Die Plattform ermöglicht die nahtlose Integration und Bereitstellung von Chatbots auf verschiedenen Messaging-Kanälen wie Websites, Facebook Messenger, WhatsApp und mehr. 6. Open-Source und Selbst-Hosting: Als Open-Source-Plattform bietet Botpress die Möglichkeit, die Software selbst zu hosten und anzupassen, was volle Kontrolle über die Daten und die Implementierung ermöglicht.
RASA	RASA ist ein leistungsstarkes Open-Source-Framework zur Erstellung von AI Agents, insbesondere spezialisierter Chatbots und virtueller Assistenten. Es bietet eine flexible und anpassbare Plattform, die sich durch ihre Fähigkeit auszeichnet, natürliche Sprache zu verstehen und darauf zu reagieren.	1. Natürliche Sprachverarbeitung (Natural Language Understanding, NLU): RASA nutzt fortschrittliche NLU-Techniken zur Intent-Klassifizierung und Entitätserkennung, um die Absichten der Benutzer präzise zu verstehen und relevante Informationen zu extrahieren. 2. d relevante Informationen zu extrahieren. 3. Dialogverwaltung (Dialogue Management): Das Framework bietet ein robustes Dialogmanagement-System, das es ermöglicht, komplexe Gesprächsabläufe zu modellieren und dynamisch auf Benutzereingaben zu reagieren. 4. Anpassbarkeit und Erweiterbarkeit: RASA ist hochgradig anpassbar und kann leicht in verschiedene Messaging-Plattformen und Chat-Tools wie Slack, Facebook Messenger und WhatsApp integriert werden. 5. Open-Source und Selbst-Hosting: Als Open-Source-Framework bietet RASA die Möglichkeit, die Software selbst zu hosten und anzupassen, was volle Kontrolle über die Daten und die Implementierung ermöglicht.
Semantik Kernel	Der Semantik Kernel (SK) ist ein innovatives Framework zur Erstellung und Verwaltung von AI Agents, das sich durch seine Fähigkeit auszeichnet, semantische Technologien zu nutzen, um intelligentes Verhalten zu erzeugen.	1. Semantische Datenverarbeitung: Der Semantik Kernel nutzt semantische Technologien und Ontologien, um Wissen zu repräsentieren und zu verarbeiten. Dadurch können AI Agents kontextbezogene und bedeutungsvolle Antworten generieren. 2. Wissensgraphen: Das Framework ermöglicht die Erstellung und Nutzung von Wissensgraphen, die Beziehungen zwischen verschiedenen Entitäten und Konzepten modellieren. Diese Graphen unterstützen die AI Agents dabei, komplexe Abfragen zu verstehen und zu beantworten. 3. NLP-Integration: Der Semantik Kernel integriert fortschrittliche natürliche Sprachverarbeitungs-Techniken (NLP), um die Bedeutung von Benutzereingaben zu analysieren und zu interpretieren. Dies verbessert die Fähigkeit der AI Agents, natürliche und menschenähnliche Konversationen zu führen. 4. Anpassbarkeit und Erweiterbarkeit: Das Framework ist modular aufgebaut und kann leicht erweitert werden, um spezifische Anforderungen und Domänen zu unterstützen. Entwickler können eigene Module und Erweiterungen hinzufügen, um die Funktionalität der AI Agents zu erweitern.

hat formatiert: Deutsch (Deutschland)

hat formatiert: Deutsch (Deutschland)

hat formatiert: Deutsch (Deutschland)

hat formatiert: Deutsch (Deutschland)

hat formatiert: Deutsch (Deutschland)

hat formatiert: Deutsch (Deutschland)

hat formatiert: Deutsch (Deutschland)

Use-Cases

KI-Agenten sind vielfältig einsetzbar. Hier sind einige Ansätze für Use Cases, in denen KI-Agenten eingesetzt werden können:

Auftragsmanagement

KI-Agenten, die nach definierten Regelsatz Dokumente analysieren und in Abhängigkeit von deren Inhalte Aktionen auslösen.

Ein Beispiel wäre die Eingangsanalyse von Ausschreibungen, die folgende Schritte durchläuft:

- Kategorisierung der Ausschreibung
- Extraktion von Kontaktdaten, Zeiträumen und angefragten Services und damit verknüpfte Mengen
- Automatisches Matching mit Service-Katalog
- Automatische Kontaktierung der Service-Owner
- Erstellung eines Vorschlags für ein Angebot inkl. Kalkulation

Hier würden KI-Agenten bereits Vorarbeit leisten, um die Mitarbeiter zu entlasten, den Gesamtvorgang beschleunigen und sich auf wichtige Fragen fokussieren lassen

Kundensupport

Automatisierte Chatbots, die in der Lage sind, Kundenanfragen in Echtzeit zu beantworten und maßgeschneiderte Unterstützung anzubieten, umfassen folgende Funktionen:

- Identifizierung der Sprache, in der die Anfrage eingegeben wurde
- Erfassung relevanter Kundendaten
- Recherche von Lösungen in entsprechenden Wissensdatenbanken
- Bearbeitung und Lösung des Anliegens
- Übersetzung der Antworten in die ursprüngliche Eingabesprache

KI-Agenten helfen insbesondere bei der schnellen Erfassung von Kundendaten, Erkennung der Absicht und Bereitstellung von Wissen. Darüber hinaus werden dem KI-Agenten Mittel bereitgestellt, um Maßnahmen zur Lösung zu initiieren, beispielsweise für die Bestellung eines Ersatzteils oder für die Änderung von Kundendaten.

Energieerzeugung

Ausbalancieren der Energieerzeugung und des Energieverbrauchs in einem Versorgungsnetz durch folgende Ansätze:

- Echtzeit-Datenanalyse
- Vorhersagemodelle
- Automatisierte Laststeuerung
- Optimierung der Energieerzeugung

Die Einführung generativer KI-Agenten macht komplexe Prozesse verständlicher und handhabbarer, beispielsweise durch die Analyse von „Was wäre, wenn"-Szenarien. Durch die Vernetzung dieser Agenten und die Koordination durch einen übergeordneten KI-Agenten können weitere Optimierungen des Gesamtsystems und eine Verbesserung des Lastmanagements erreicht werden, ohne die Integration in Anwendungsschnittstellen fest zu koppeln.

Manufacturing

Zur Vermeidung von Ausfallzeiten werden „klassische“ KI-Systeme in folgenden Teildisziplinen eingesetzt:

- Überwachung und Datenanalyse
- Vorhersage
- Wartungsplanung und Benachrichtigung
- Einsatz- und Ressourcenoptimierung

Die genannten Punkte sind komplex und werden von spezialisierten Fachabteilungen betrieben, zum Einsatz kommen verschiedene Anwendungen.
Jede Teildisziplin wird um KI-Agenten erweitert und verknüpft von einem übergeordneten KI-Agenten, der koordinatorische Aufgaben übernimmt.
Dabei ist der Bereitstellungsaufwand reduziert, da die harte Integration in die Systeme entfällt.

Finanzanalyse

Hier handelt es sich um KI-Agenten, die große Datenmengen analysieren, Markttrends vorherzusagen und Anlageempfehlungen geben.

- Automatische Analyse verschiedener Quellen wie Gerichtsbeschlüsse, Marktanalysen oder Prospekte von Produkten
- Regelkonformitätsprüfung
- Erstellung eines Entscheidungsvorschlags
- Automatisierte Meldung an die zuständige Behörde

Der Einsatz von KI-Agenten automatisiert manuelle Aufgaben und unterstützt Mitarbeiter, indem er zeitaufwändige, repetitive Tätigkeiten übernimmt. Die Zusammenarbeit zwischen Menschen und KI optimiert den Prozess, beschleunigt Entscheidungen und steigert die Effizienz.

Herausforderungen für Unternehmen

Die Implementierung von KI-Agenten bringt mehrere bedeutende Herausforderungen mit sich, die im Folgenden beleuchtet werden.

Herausforderungen sind grundsätzlich:

- Digitalisierung der Arbeitsschritte und Prozesse im Einsatzgebiet
- Integration in bestehende IT-Landschaften
- Ethische Überlegungen
- Anforderungen durch EU-Gesetzgebung

Digitalisierung

Der Einsatz von KI-Systemen im allgemeinen und KI-Agenten im Speziellen setzt voraus, dass die Zielgebiete für deren Einsatz bereits digitalisiert[27] [28] sind. Somit kommen hier zusätzlich zu Aufwänden für die Entwicklung und Integration von KI-Agenten auch Aufwände hinsichtlich Umstellung von Arbeitsprozessen auf digitale Systeme und Arbeitsmittel hinzu.

Bestehende IT-Landschaften

Bestehende IT-Umgebungen können für die Integration aktueller KI-Technologien insbesondere dann eine bedeutende Herausforderung sein, wenn die IT-Landschaft über Jahre – wenn nicht sogar über Jahrzehnte – gewachsen ist.

Diese Herausforderungen können u.a. sein:

- Komplexität: Mit der Zeit können unterschiedliche Systeme, Anwendungen und Technologien integriert werden, was die IT-Landschaft komplex macht. Diese Komplexität kann die Verwaltung und Wartung erschweren.
- Inkompatibilität: Ältere Systeme und Software können inkompatibel mit neuen Technologien sein, was zu Integrationsproblemen führt. Dies kann die Effizienz beeinträchtigen und die Implementierung neuer Lösungen erschweren.
- Mangel an Fachkräften: Mit der Zeit können sich die Technologien ändern und es kann schwierig sein, Mitarbeiter zu finden, die die erforderlichen Fähigkeiten zur Wartung und Weiterentwicklung älterer Systeme besitzen.
- Unzureichende Datenintegration: Daten können über verschiedene Systeme verstreut sein, was die Fähigkeit beeinträchtigt, sinnvolle Analysen durchzuführen oder Entscheidungen zu treffen.

Hier bietet es sich an, bei einer Konsolidierung der IT-Umgebung ein Augenmerk auf die Fähigkeit der Zielsysteme und Software zur Zusammenarbeit mit KI-Agenten zu achten.

Ethische Überlegungen

Da es sich bei KI-Agenten um eine Variante von KI-Systemen handelt, gelten hierfür die gleichen ethischen Fragestellungen[29] [30]. Die Wichtigkeit erhöht sich bereits durch die Annahme, dass KI-Agenten nicht als ein einzigartiges KI-System zum Einsatz kommen, sondern sehr häufig und in unterschiedlichster Ausprägung zur Anwendung kommen werden.

Kommentiert [SP17]: Fußnoten zu einer zusammenfassen?

Sofern es sich um eine Neueinführung von KI handelt, sollten u.a. folgende Punkte betrachtet werden:

Vorrang menschlichen Handelns und menschlicher Aufsicht: Menschen sollten befähigt werden, fundierte Entscheidungen zu treffen und ihre Grundrechte zu fördern. Angemessene Aufsichtsmechanismen und Konzepte wie „Human-in-the-Loop" sind erforderlich.

[27] (Bundesnetzagentur, 2024)
[28] (Handelsblatt, 2025)
[29] (DIN e.V. & DKE, 2020)
[30] (EU Kommision, 2019)

Technische Robustheit und Sicherheit: KI-Systeme müssen widerstandsfähig, sicher und zuverlässig sein, mit Rückfallplänen, um unbeabsichtigte Schäden zu minimieren.

Privatsphäre und Datenqualitätsmanagement: Achtung der Privatsphäre und des Datenschutzes ist entscheidend, ebenso wie geeignete Daten-Governance-Mechanismen zur Sicherstellung der Datenqualität und -integrität.

Transparenz: Geschäftsmodelle, Daten und Systeme sollten transparent sein. Entscheidungen der KI-Agenten müssen verständlich erklärt werden, und Nutzer sollten über die Interaktion mit KI-Agenten informiert sein.

Vielfalt, Nichtdiskriminierung und Fairness: Unfaire Verzerrungen müssen vermieden werden, um Marginalisierung und Diskriminierung zu verhindern. KI-Agenten sollten für alle zugänglich sein und relevante Interessenträger einbeziehen.

Gesellschaftliches und ökologisches Wohlergehen: KI-Systeme sollten nachhaltig und umweltfreundlich sein, um allen Menschen und zukünftigen Generationen zugutekommen, sowie soziale Auswirkungen berücksichtigen.

Rechenschaftspflicht: Mechanismen zur Gewährleistung von Verantwortlichkeit und Rechenschaftspflicht für KI-Systeme und deren Ergebnisse sind notwendig, einschließlich Überprüfbarkeit und angemessener Rechtsbehelfe.

EU-Anforderungen an Nutzung von KI-Systemen

Der EU AI Act [31] legt verschiedene Anforderungen an die Verwendung von künstlicher Intelligenz fest, um sicherzustellen, dass KI-Systeme sicher, transparent und ethisch eingesetzt werden.

Werden erstmalig KI-Systeme in Form von KI-Agenten implementiert, so ist hier eine Bewertung entsprechend den EU-Vorschriften notwendig. Das ist insbesondere dann wichtig, wenn durch KI-Agenten optimierte Prozesse Entscheidungen treffen, die sich auf Menschen auswirken können.

Darüber hinaus ist es aus Gründen von Transparenz und Nachvollziehbarkeit angebracht, zu jeder Zeit nachprüfen zu können wann und warum ein KI-Agent eine Entscheidung gefällt oder Aktion ausgelöst hat.

Ausblick

KI-Agenten sind im Trend. [32]

Die Entwicklung ist derzeit im Gange, sowohl hinsichtlich des Verständnisses von KI-Agenten als auch bezüglich ihrer optimalen Einsatzzwecke und der Umgebungen, in denen sie operieren.

Interessant erscheint die Erweiterung von Systemen mit hoher Komplexität, bei der KI-Agenten helfen können, solche Systeme einer breiteren Gruppe von Menschen zugänglicher zu machen, was im Anblick des Fachkräftemangel sicherlich hilfreich wäre. Einfach ausgedrückt könnte dies bedeuten, dass man mit technischen Komponenten „reden" könnte.

Ein weiterer Punkt kann die Intensivierung bei der Digitalisierung von Geschäftsprozessen sein, wo über spezialisierte KI-Agenten mit jeweiligem Spezialwissen über ganze Prozessketten hinweg Aufgaben bearbeitet, mit geschäftlichem Wissen –als auch z.B. regulatorische Vorgaben – angereichert und angepasst werden. Das könnte dazu führen, dass von Ausschreibungen über Kalkulationen bis hin zur Vertragsgestaltung KI-Agenten mitwirken und den Gesamtprozess beschleunigen und kostengünstiger machen.

Ein wichtiger Punkt dürfte hier auch die Wahl der optimalen Tools für die verschiedenen Lösungen sein, also für – einfache oder komplexe Aufgaben, Single-Agent oder Multi-Agent-Ansätze bis hin zu Agentic AI-Lösungen.

[31] (DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION, 2024)
[32] (Matzer, 2025)

References

Adamopoulou, E., & Moussiades, L. (2020, 12 15). *Chatbots: History, technology, and applications*. Retrieved from https://www.sciencedirect.com/science/article/pii/S2666827020300062?via%3Dihub

Bundesnetzagentur. (2024, 08 13). *Digitalisierung im Mittelstand in Zahlen*. Retrieved from Digitalisierung im Mittelstand in Zahlen: https://www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/Mittelstand/Kennzahlen/start.html

Codecademy Team. (n.d.). *History of Chatbots*. Retrieved from https://www.codecademy.com/article/history-of-chatbots

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION. (2024, 06 13). *Document 32024R1689*. Retrieved from Document 32024R1689: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32024R1689

DIN e.V. & DKE. (2020). *Ethik und Künstliche Intelligenz: Was können technische Normen und Standards leisten?* Retrieved from https://www.din.de/resource/blob/754724/00dcbccc21399e13872b2b6120369e74/whitepaper-ki-ethikaspekte-data.pdf

Doria, L. (2024, 07 09). Retrieved from https://www.staff.uni-mainz.de/doria/AI/AI_2.pdf

EU Kommision. (2019, 04 08). *Ethikleitlinien für vertrauenswürdige KI*. Retrieved from Ethikleitlinien für vertrauenswürdige KI: https://digital-strategy.ec.europa.eu/de/library/ethics-guidelines-trustworthy-ai

Foote, K. D. (2023, 07 06). Retrieved from https://www.dataversity.net/a-brief-history-of-natural-language-processing-nlp/

Gutowska, A. (2024, 07 03). *What are AI agents?* Retrieved from https://www.ibm.com/think/topics/ai-agents

Gutowska, A. (2024, 08 06). *What is a multiagent system?* Retrieved from https://www.ibm.com/think/topics/multiagent-system

Handelsblatt. (2025, 02 24). *Statistik: Was sind die größten Hürden für die Digitalisierung in Ihrem Unternehmen?* Retrieved from Statistik: Was sind die größten Hürden für die Digitalisierung in Ihrem Unternehmen?: https://live.handelsblatt.com/statistik-was-sind-die-groessten-huerden-fuer-die-digitalisierung-in-ihrem-unternehmen/

Huang, Y. (2024 , 03 06). *arxiv*. Retrieved from https://arxiv.org/pdf/2405.06643

Intel Corporation. (n.d.). *Künstliche Intelligenz (KI) – Workflows*. Retrieved from https://www.intel.de/content/www/de/de/learn/ai-workflows.html

Jennings, N., & Wooldridge, M. (1996, 01). *Software Agents*. Retrieved from https://www.cs.ox.ac.uk/people/michael.wooldridge/pubs/iee-review96.pdf

Kagan, J. (2024, 08 20). Retrieved from https://www.investopedia.com/terms/a/agent.asp

Kutsal, B. (2025, 03 06). *Bigdata Insider*. Retrieved from Diese neun Trends sind 2025 entscheidend: https://www.bigdata-insider.de/top-trends-2025-ki-agenten-projekte-a-ce347028b59f51799cc89b5cf1989c76/

LEO GmbH. (n.d.). Retrieved from https://dict.leo.org/englisch-deutsch/Agent

MacCartney, B. (2014, 07 16). *Understanding Natural Language Understanding*. Retrieved from https://nlp.stanford.edu/~wcmac/papers/20140716-UNLU.pdf

Matzer, M. (2025, 02 24). *Diese positiven Erfahrungen machen Unternehmen mit KI-Agenten*. Retrieved from Diese positiven Erfahrungen machen Unternehmen mit KI-Agenten: https://www.bigdata-insider.de/top-trends-2025-ki-agenten-projekte-a-ce347028b59f51799cc89b5cf1989c76/

Meta. (2024, 04 18). *Introducing Meta Llama 3: The most capable openly available LLM to date*. Retrieved from https://ai.meta.com/blog/meta-llama-3/

Mistral AI. (2024, 02 26). *Au Large*. Retrieved from https://mistral.ai/news/mistral-large

modelcontextprotocol.io. (n.d.). *Get started with the Model Context Protocol (MCP)*. Retrieved from https://modelcontextprotocol.io/introduction

Naveed, H., Khan, A. U., Qiu, S., Saqib, M., Anwar, S., Akhtar, N., . . . Mian, A. (2024, 10 17). *A Comprehensive Overview of Large Language Models*. Retrieved from https://arxiv.org/pdf/2307.06435

OpenAI. (2022, 11 30). *Introducing ChatGPT*. Retrieved from https://openai.com/index/chatgpt/

OpenAI. (2024, 07 18). *GPT-4o mini: advancing cost-efficient intelligence*. Retrieved from https://openai.com/index/gpt-4o-mini-advancing-cost-efficient-intelligence/

OpenAI. (2024, 05 13). *Hello GPT-4o*. Retrieved from https://openai.com/index/hello-gpt-4o/

Pędich, M. (2024, 10 22). Retrieved from https://fabrity.com/blog/llm-agents-the-next-big-thing-for-genai/

Purdy, M. (2024, 12 12). *What Is Agentic AI, and How Will It Change Work*. Retrieved from https://hbr.org/2024/12/what-is-agentic-ai-and-how-will-it-change-work

Zwass, V. (n.d.). *software agent*. Retrieved from https://www.britannica.com/technology/software-agent

Autor

Lars Scholze
Technical AI Manager
Atos Deutschland

Über Atos

Atos ist ein weltweit führender Anbieter für die digitale Transformation mit ca. 82.000 Mitarbeitern und einem Jahresumsatz von zirka 10 Milliarden Euro. Als europäischer Marktführer für Cybersecurity sowie Cloud und High Performance Computing bietet die Atos Gruppe maßgeschneiderte, ganzheitliche Lösungen für sämtliche Branchen in 69 Ländern. Als Pionier im Bereich nachhaltiger Dienstleistungen und Produkte arbeitet Atos für seine Kunden an sicheren, dekarbonisierten Digitaltechnologien. Atos ist eine SE (Societas Europaea), die an der Börse Euronext Paris notiert ist.

Societas Europaea), die an der Börse Euronext Paris notiert ist.

Das Ziel von Atos ist es, die Zukunft der Informationstechnologie mitzugestalten. Fachwissen und Services von Atos fördern Wissensentwicklung, Bildung sowie Forschung in einer multikulturellen Welt und tragen zu wissenschaftlicher und technologischer Exzellenz bei. Weltweit ermöglicht die Atos Gruppe ihren Kunden und Mitarbeitern sowie der Gesellschaft insgesamt, in einem sicheren Informationsraum nachhaltig zu leben, zu arbeiten und sich zu entwickeln.

entwickeln.

Weitere Informationen finden Sie unter www.atos.net

Unternehmen ist in 69 Ländern vertreten und erzielt einen Jahresumsatz von ca. 5 Milliarden Euro.

hat formatiert: Deutsch (Deutschland)

hat formatiert: Deutsch (Deutschland)

hat formatiert: Deutsch (Deutschland)

hat formatiert: Deutsch (Deutschland)

hat formatiert: Deutsch (Deutschland)

Über Tech Foundations

Tech Foundations umfasst den Managed-Services-Geschäftsbereich der Atos Gruppe mit Fokus auf Hybrid Cloud Infrastructure, Employee Experience und Technology Services. Mit seinen dekarbonisierten, automatisierten und KI-gestützten Lösungen ist Tech Foundations führend in diesem Bereich und treibt mit seinen 41.000 Mitarbeitern Themen voran, die Unternehmen, Institutionen und die Gesellschaft weltweit am dringendsten beschäftigen. Das