

Generative KI Chancen und Risiken in der Nutzung

Intro

Hans-Jörg Schäuble



VP Customer

Unsere Mission

Europa als entscheidenden Akteur im Bereich der künstlichen Intelligenz zu etablieren und digitale Souveränität zu sichern.

Unser Kern

Wir sind ein unabhängiges Unternehmen, das generative KI-Sprachmodelle erforscht, entwickelt und in reale Anwendungen einführt.

Key Data

- Gegründet im Jahr 2019
- Standorte:
 - Heidelberg (Hauptsitz)
 - Berlin
 - Bayreuth (Rechenzentrum)
- Ca. 70 Mitarbeiter
- CEO: Jonas Andrulis

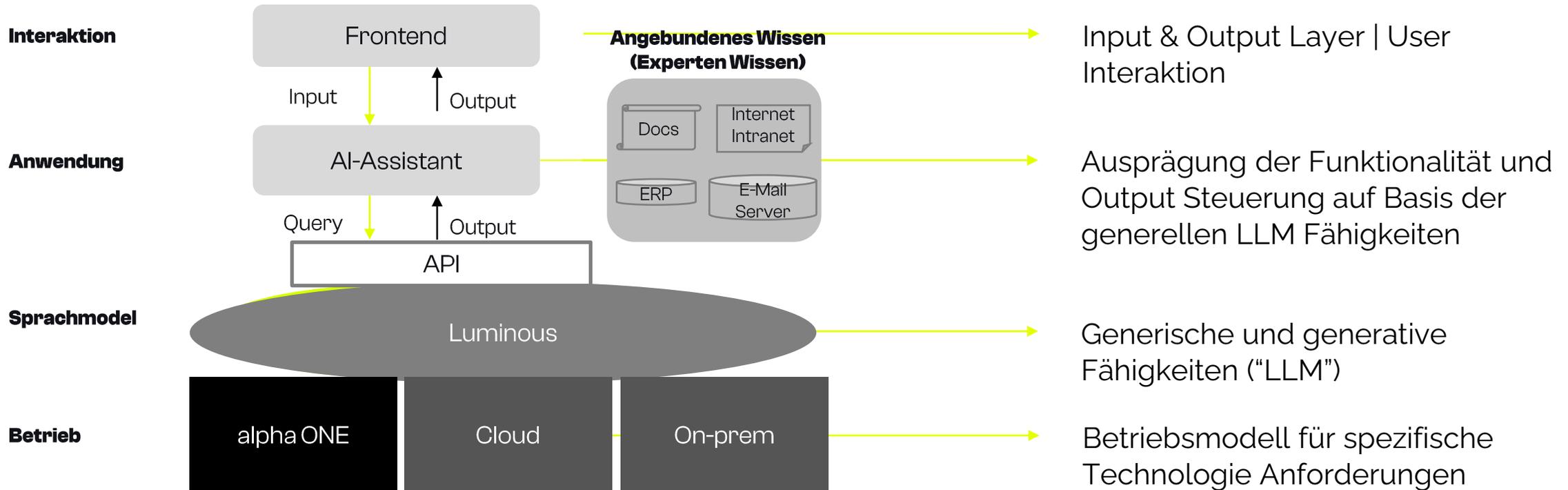
Computers and robots used to be the bicycle of the mind...

Bis 2030 wird
50%+ aller Arbeit durch KI erledigt

KI liefert ~14% des globalen BIP*

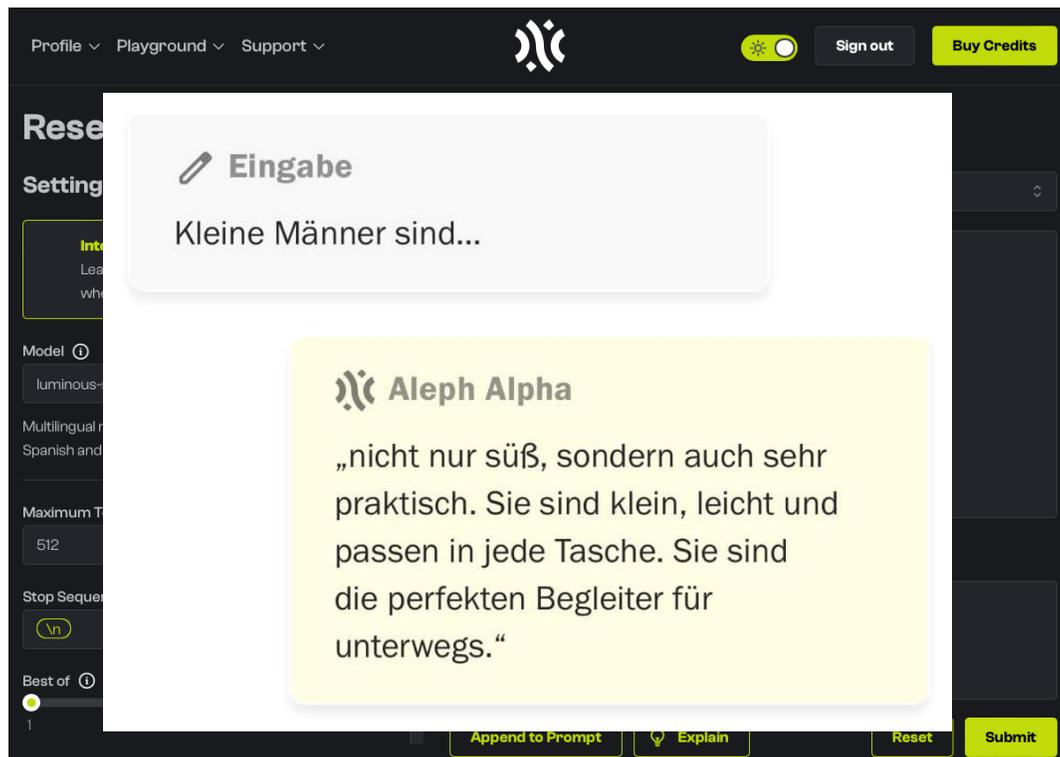
LLM basierte Anwendung („KI System“)

KI Value Chain Architektur am Bsp. eines Assistenten



Risiken generativer KI – ein Beispiel

- Input & Output layer (Visualisierung: Aleph Alpha Research Playground)



Verwendetes Modell: Aleph Alpha Luminous Supreme

Aufgabe: Vervollständigung (Completion)

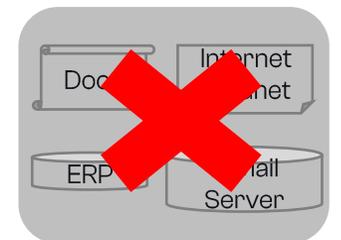
Abstraktion / Filter: keine (Basis Modell)

Angebundenes Wissen: keines

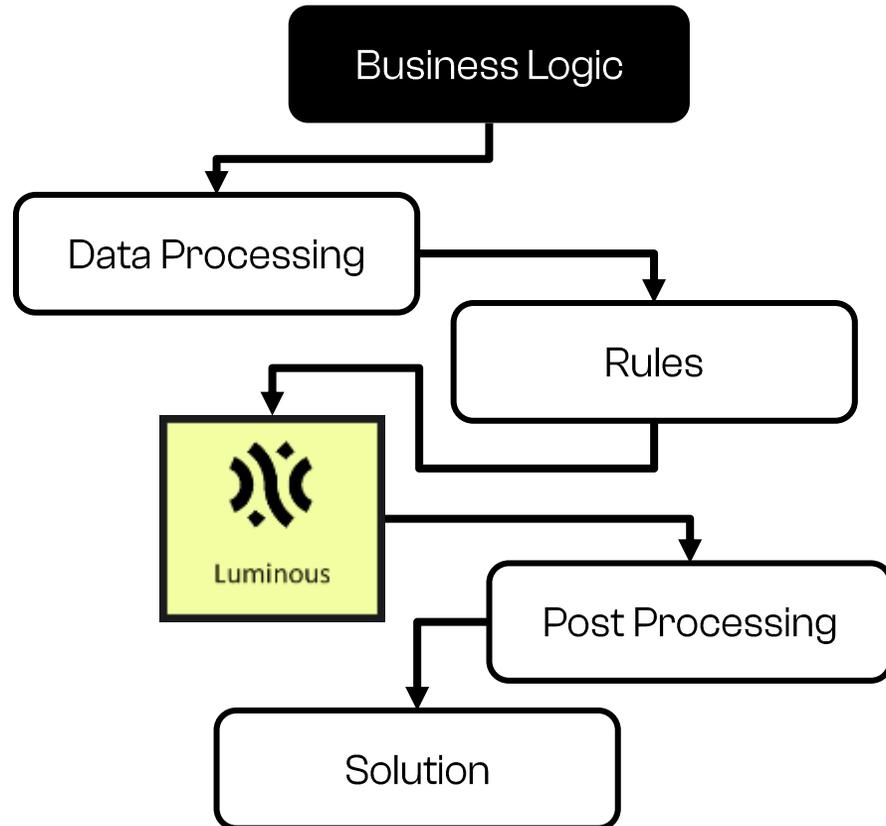
Kontext: keiner

Ergebnis: **unsinnig**

**Angebundenes Wissen
(Experten Wissen)**



Chancen nutzen und Risiken minimieren



LLMs sind nur ein Teil einer Gesamtarchitektur

ermöglichen Lösungen z.B. im

- Verständnis von Inhalten und Wissen im Umgang mit Daten
- Hinterlegung von individuellen Regeln
- Einbindung in individuellen Kontext
- Nutzbarkeit von Ergebnissen durch Nachvollziehbarkeit

CASE STUDY: Sichere Suche und Recherche mit internen Daten

+ EIGENE TEXT-QUELLE i



ALLES LÖSCHEN


Wann spricht das Land BW von einer geringen Menge Cannabis? 

UNSICHERE ANTWORTEN AUSBLENDEN ^


- Das Land BW spricht von einer geringen Menge Cannabis, wenn die Menge Cannabis, die der Beschuldigte mit sich führt, sechs Gramm beträgt.
- Das Land BW spricht von einer geringen Menge Cannabis, wenn die Menge des Wirkstoffs THC 15 mg nicht überschreitet.
- Das Land BW spricht von einer geringen Menge Cannabis, wenn die Menge Cannabis, die ein Konsument besitzt, nicht mehr als 5 Gramm beträgt.

QUELLE AUSBLENDEN ^

Quelle: 17_1000-17_1928_D.pdf: Landtag von Baden-Württemberg Drucksache 17 / 1928 24 Berst schlechte Qualität mit einem sehr niedrigen Wirkstoffgehalt von 0,75 Prozent THC zugrunde zu legen. Die Grenze der geringen Menge ist bei Cannabispunkten demnach **bei einer Gewichtsmenge von sechs Gramm erreicht** (6 Gramm Cannabis x 0,75 Prozent ergibt 0,045 Gramm THC; das entspricht drei Konsumeinheiten zu je 15 Milligramm THC). Mittlerweile orientieren sich fast alle Länder an dieser Bestimmung anhand des Bruttogewichts und legen in den jeweiligen Verwaltungsvorschriften als geringe Cannabismenge sechs Gramm fest. Auch in Baden-Württemberg, das entsprechend der dargestellten Historie in seiner Verwaltungsvorschrift für eine einheitliche Praxis der Strafverfolgung bei Verfahren nach dem BtMG auf „drei Konsumeinheiten“ abstellt, ist letztlich ebenfalls das Bruttogewicht von sechs Gramm bei einem zugunsten der Beschuldigten unterstellten sehr niedrigen Wirkstoffgehalt von unter einem Prozent THC die entscheidende Obergrenze. Bei höheren Mengen kommt eine Einstellung gemäß § 31a BtMG in der Regel nicht mehr in Betracht. Auch sofern der Konsum mit Betäubungsmitteln im Zusammenhang mit dem Führen eines Kfz steht, wird von der Einstellungsmöglichkeit nach § 31a BtMG ungeachtet der Menge in der Regel kein Gebrauch gemacht.

17_1000-17_1928_D.pdf: Weitere Faktoren, wie zum Beispiel Wirkungsweise, Gefährlichkeit, Reinheitsgehalt und konkreter Gebrauch des Betäubungsmittels, bleiben bei der Berücksichtigung der geringen Menge im Sinne des § 29 Absatz 5 BtMG zunächst unberücksichtigt, können aber im Rahmen der Ermessensentscheidung herangezogen werden. Für das Rauchen von Haschisch/Marihuana hat der Bundesgerichtshof bereits in den 1980er-Jahren ent-

+ WEITERE FRAGE

 Sie haben Weltwissen aktiviert. Antworten können ungenau sein.

DEMO: Umgang mit widersprüchlichen Informationen

Your question:

What is the former capital of Germany? Send →

Answer:

There are contradicting answers saying the former capital of Germany is Bonn or Berlin. Hide sources ↑

Bonn was the former capital of Germany. 51%

*'In 1949, the three western occupation zones (American, British, and French) were combined into the Federal Republic of Germany (FRG, West Germany). The government was formed under Chancellor Konrad Adenauer and his conservative CDU/CSU coalition. The CDU/CSU was in power during most of the period since 1949. The capital was Bonn until it was moved to Berlin in 1990. In 1990, FRG absorbed East Germany and gained full sovereignty over Berlin. At all points West Germany was much larger and richer than East Germany, which became a dictatorship under the control of the Communist Party and was closely monitored by Moscow. Germany, especially Berlin, was a cockpit of the Cold War, with NATO and the Warsaw Pact assembling major military forces in west and east. However, there was never any combat. * - [History of Germany](#)*

The former capital of Germany was Bonn. 48%

**** West Germany (Bonn Republic) *** * - [History of Germany](#)*

Berlin was the former capital of Germany. 47%

*'United Germany was considered the enlarged continuation of West Germany so it retained its memberships in international organisations. Based on the Berlin/Bonn Act (1994), Berlin again became the capital of Germany, while Bonn obtained the unique status of a Bundesstadt (federal city) retaining some federal ministries. The relocation of the government was completed in 1999, and modernisation of the East German economy was scheduled to last until 2019. Since reunification, Germany has taken a more active role in the European Union, signing the Maastricht Treaty in 1992 and the Lisbon Treaty in 2007, and co-founding the Eurozone. Germany sent a peacekeeping force to secure stability in the Balkans and sent German troops to Afghanistan as part of a NATO effort to provide security in that country after the ousting of the Taliban. In the 2005 elections, Angela Merkel became the first female chancellor. In 2009 the German government approved a €50 billion stimulus plan. Among the major German political projects of the early 21st century are the advancement of European integration, the energy transition (Energiewende) for a sustainable energy supply, the debt brake for balanced budgets, measures to increase the fertility rate (pronatalism), and high-tech strategies for the transition of the German economy, summarised as Industry 4.0. During the 2015 European migrant crisis, the country took in over a million refugees and migrants. * - [Germany](#)*

Qualitätssicherung durch Adjustierung (nicht nur des LLMs)

Umgang mit unterschiedlichsten Anforderungen

- Mehrere Antworten auf eine Frage
- Veränderung in der Bedeutung von Begriffen, Werten und Normen
- Versionierung & Updates

Minimierung von Risiken nur durch Regulierung?

Regulierung ist notwendig

So hilft Ihnen die KI bei der Arbeit

Schon heute kann Künstliche Intelligenz – ganz besonders generative Sprachmodelle – Standardarbeit erledigen. Wie sie am besten verwendet werden sollte und was erlaubt ist.

 Christian Mayer

09.06.2023 - 15:14 Uhr • [Kommentieren](#) • [Jetzt teilen](#)



ChatGPT von OpenAI als Hilfe bei der Arbeit

ChatGPT kann eine große Hilfe sein, wenn man das Programm [nutzt](#)

[ChatGPT: So hilft Ihnen die KI bei der Arbeit \(handelsblatt.com\)](#)

Die Angst der Deutschen vor der Künstlichen Intelligenz

Eine Umfrage zeigt, welche Chancen und Risiken Arbeitskräfte bei Künstlicher Intelligenz sehen. Experten warnen vor einer überzogenen Panikmache.

 Jürgen Klöckner

 Frank Specht

09.06.2023 - 14:30 Uhr • [3 x geteilt](#)

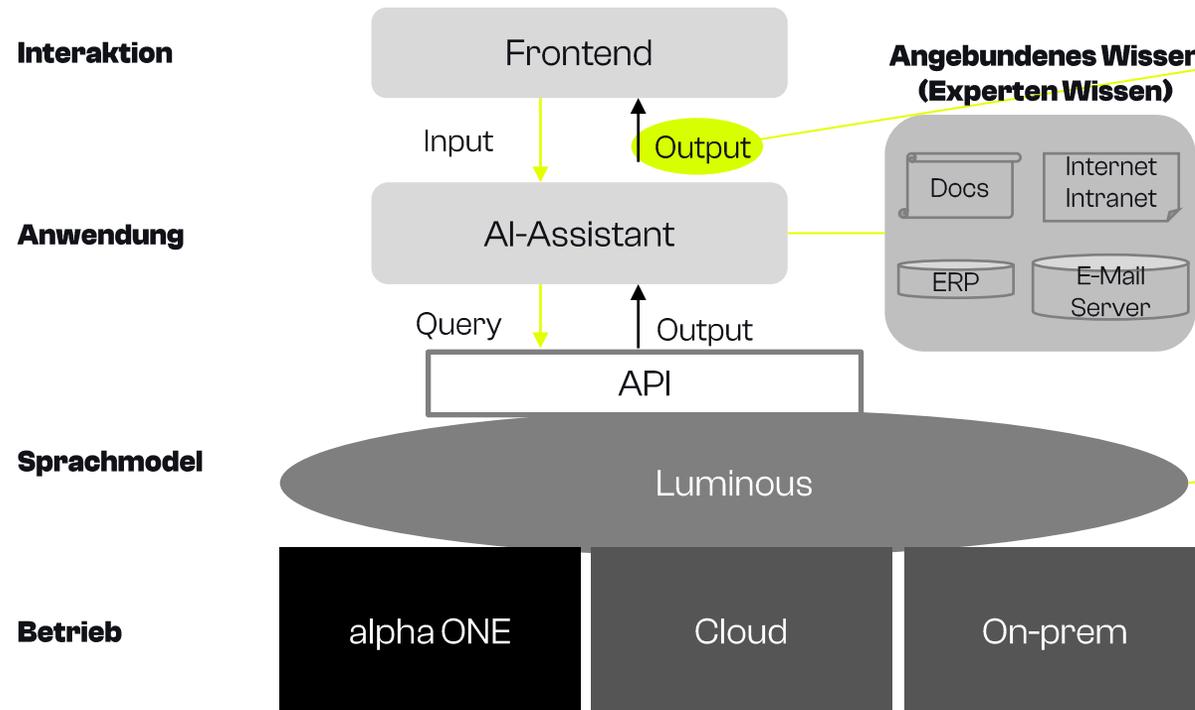


[KI: Die Angst der Deutschen vor der Künstlichen Intelligenz \(handelsblatt.com\)](#)

Wie sich die KI am Ende entwickeln wird, basiert darauf, wie wir sie gestalten...

Regulierung wird Sicherheit für Nutzer & Daten sicherstellen

KI Value Chain Architektur am Bsp. eines Assistenten



Auszüge

Vertrauen in Modell-Output, zur Übernahme der Verantwortung durch den Nutzer (**Usability**) (**EU AI Act**)

Expertenwissen und Unternehmensdaten müssen geschützt sein (**DSVGO**) (**Urheberrecht**) (**EU AI Act**)

Modelle lernen aus Daten (**Urheberrecht**) (**EU AI Act**)
 Modellinfrastruktursicherheit (**IT Sicherheit**), Datenübermittlung (**DSVGO**)

Infrastruktur und Betriebsmodell muss "sicher" sein (**IT Sicherheit**)

Sicherheit für Nutzer durch Nachvollziehbarkeit

AtMan: Understanding Transformer Predictions Through Memory Efficient Attention Manipulation

ATMAN: Understanding Transformer Predictions Through Memory Efficient Attention Manipulation

Mayukh Deb^{*,1}, Björn Deiseroth^{*,1,2,3}, Samuel Weinbach^{*,1},
Patrick Schramowski^{2,3,4}, Kristian Kersting^{2,3,4}

¹Aleph Alpha GmbH, Heidelberg, Germany

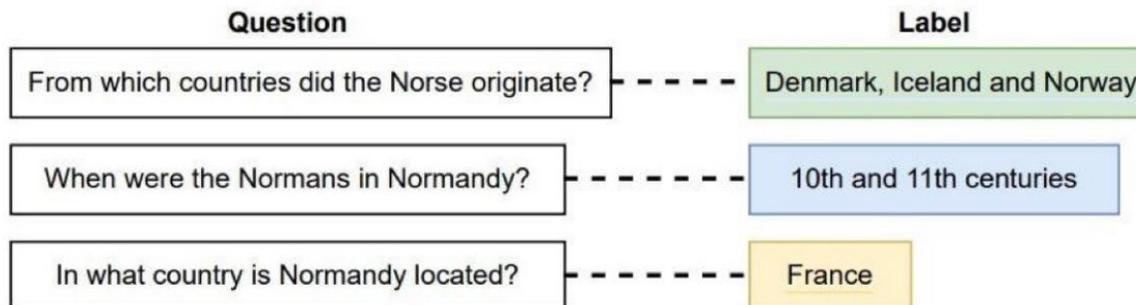
²Artificial Intelligence and Machine Learning Lab, TU Darmstadt, Germany

³Hessian Center for Artificial Intelligence (hessian.AI), Darmstadt, Germany

⁴German Center for Artificial Intelligence (DFKI)

Context with AtMan Explanation

The Normans (Norman: Nourmands; French: Normands; Latin: Normanni) were the people who in the 10th and 11th centuries gave their name to Normandy, a region in France. They were descended from Norse ("Norman" comes from "Norseman") raiders and pirates from Denmark, Iceland and Norway who, under their leader Rollo, agreed to swear fealty to King Charles III of West Francia.



Mensch-Maschine Interaktion muss weiter neu gedacht werden:

Der **Nutzer muss Verantwortung** in der Verwendung für den Output übernehmen können

Nachvollziehbarkeit und Verständnissfähigkeit und Erklärbarkeit hat verschiedene Dimensionen:

- auf Modellebene (Training, ...)
- in der Verarbeitung (Schritte, ...)
- auf Output-ebene (Ergebnis)

Thank you!