

Curriculum für

Certified Professional for
Software Architecture (CPSA)[®]
Advanced Level

**Modul
SWARC4AI**

Softwarearchitektur für KI-Systeme

2024.1-RC2-DE-20241030



Inhaltsverzeichnis

Verzeichnis der Lernziele	2
Einführung: Allgemeines zum iSAQB Advanced Level	6
Was vermittelt ein Advanced Level Modul?	6
Was können Absolventen des Advanced Level (CPSA-A)?	6
Voraussetzungen zur CPSA-A-Zertifizierung	6
Grundlegendes	7
Was vermittelt das Modul „SWARC4AI“?	7
Struktur des Lehrplans und empfohlene zeitliche Aufteilung	7
Dauer, Didaktik und weitere Details	7
Voraussetzungen	7
Gliederung des Lehrplans	8
Ergänzende Informationen, Begriffe, Übersetzungen	8
1. Einführung in softwarearchitekturelevante Konzepte für Künstliche Intelligenz	9
1.1. Begriffe und Konzepte	9
1.2. Lernziele	9
1.3. Referenzen	11
2. Compliance, Security, Alignment	12
2.1. Begriffe und Konzepte	12
2.2. Lernziele	12
2.3. Referenzen	14
3. Architektur von KI-Systemen	15
3.1. Begriffe und Konzepte	15
3.2. Lernziele	15
3.3. Referenzen	18
4. Datenmanagement und Datenverarbeitung für KI-Systeme	19
4.1. Begriffe und Konzepte	19
4.2. Lernziele	19
4.3. Referenzen	19
5. Skalierbarkeit und Leistungsoptimierung von KI-Systemen	21
5.1. Begriffe und Konzepte	21
5.2. Lernziele	21
5.3. Referenzen	23
6. Systemarchitekturen und Plattformen für Generative KI-Systeme	24
6.1. Begriffe und Konzepte	24
6.2. Lernziele	24
6.3. Referenzen	26
7. Fallstudien und Praxisprojekte	27



7.1. Lernziele 27

Referenzen 28

© (Copyright), International Software Architecture Qualification Board e. V. (iSAQB® e. V.) 2023

Die Nutzung des Lehrplans ist nur unter den nachfolgenden Voraussetzungen erlaubt:

1. Sie möchten das Zertifikat zum CPSA Certified Professional for Software Architecture Foundation Level® oder CPSA Certified Professional for Software Architecture Advanced Level® erwerben. Für den Erwerb des Zertifikats ist es gestattet, die Text-Dokumente und/oder Lehrpläne zu nutzen, indem eine Arbeitskopie für den eigenen Rechner erstellt wird. Soll eine darüber hinausgehende Nutzung der Dokumente und/oder Lehrpläne erfolgen, zum Beispiel zur Weiterverbreitung an Dritte, Werbung etc., bitte unter info@isaqb.org nachfragen. Es müsste dann ein eigener Lizenzvertrag geschlossen werden.
2. Sind Sie Trainer oder Trainingsprovider, ist die Nutzung der Dokumente und/oder Lehrpläne nach Erwerb einer Nutzungslizenz möglich. Hierzu bitte unter info@isaqb.org nachfragen. Lizenzverträge, die alles umfassend regeln, sind vorhanden.
3. Falls Sie weder unter die Kategorie 1. noch unter die Kategorie 2. fallen, aber dennoch die Dokumente und/oder Lehrpläne nutzen möchten, nehmen Sie bitte ebenfalls Kontakt unter info@isaqb.org zum iSAQB e. V. auf. Sie werden dort über die Möglichkeit des Erwerbs entsprechender Lizenzen im Rahmen der vorhandenen Lizenzverträge informiert und können die gewünschten Nutzungsgenehmigungen erhalten.

Wichtiger Hinweis

Grundsätzlich weisen wir darauf hin, dass dieser Lehrplan urheberrechtlich geschützt ist. Alle Rechte an diesen Copyrights stehen ausschließlich dem International Software Architecture Qualification Board e. V. (iSAQB® e. V.) zu.

Die Abkürzung "e. V." ist Teil des offiziellen Namens des iSAQB und steht für "eingetragener Verein", der seinen Status als juristische Person nach deutschem Recht beschreibt. Der Einfachheit halber wird iSAQB e. V. im Folgenden ohne die Verwendung dieser Abkürzung als iSAQB bezeichnet.

Verzeichnis der Lernziele

- LZ 1-1: Definition Künstliche Intelligenz inklusive der Einordnung von Machine Learning, Data Science, Deep Learning, Generative AI
- LZ 1-2: Spezifikation typischer allgemeiner Anwendungsfälle für KI
- LZ 1-3: Einsatzmöglichkeiten in verschiedenen Branchen
- LZ 1-4: Einsatzmöglichkeiten in Endnutzeranwendungen
- LZ 1-5: Risiken bei der Anwendung von KI
- LZ 1-6: Unterschiede zu traditioneller Software
- LZ 1-7: Entscheidungsfähigkeit zur Lösung von Problemen mittels KI oder klassischer SW-Entwicklung
- LZ 1-8: Rollen und deren Aufgaben im Kontext von KI
- LZ 1-9: Zusammenarbeit der Rollen im Team (Team Topologies für ML-Teams)
- LZ 1-10: Identifikation und Priorisierung von KI Anwendungsfällen
- LZ 1-11: KI Stärken und Grenzen
- LZ 1-12: Kennen Productivity J-Curve Konzept in Verbindung mit KI-Technologie (Dieses Phänomen hilft zu verstehen, warum Unternehmen bei der Implementierung von KI zunächst einen Produktivitätsrückgang verzeichnen können, dem bei der weiteren Entwicklung aber Produktivitätsgewinne folgen können.).
- LZ 2-1: Einfluss der Datenschutzgesetze auf die Implementierung und Nutzung von KI
- LZ 2-2: Ziele und Regelungen des EU AI Act
- LZ 2-3: Einfluss des EU AI Act (Trustworthy AI) auf den Entwicklungsprozess und die Architektur des Softwaresystems
- LZ 2-4: Klassifikation von KI-Systemen nach EU AI Act Risikolevel
- LZ 2-5: Urheberrechtsproblematik von KI-generierten Inhalten
- LZ 2-6: Arten bzw. Grade der Offenheit freier ML-Modelle
- LZ 2-7: Arten von Lizenzen freier ML-Modelle
- LZ 2-8: Strategien für die Einhaltung des europäischen AI-Acts und mögliche Herausforderungen
- LZ 2-9: Dokumentation von Modellen und Datensätzen für die Nachvollziehbarkeit und Transparenz
- LZ 2-10: Fallstricke hinsichtlich Security
- LZ 2-11: Angriffsarten auf ML-Modelle
- LZ 2-12: AI-Risk Minimierung Strategien
- LZ 2-13: Möglichkeiten zur Absicherung gegen Angriffe (AI Security)
- LZ 2-14: Grundproblematik und Facetten von AI-Safety
- LZ 2-15: Probleme hinsichtlich Ethik, die KI-Systeme mit sich bringen können
- LZ 2-16: Ansätze zum Umgang mit ethischen Problemen
- LZ 2-17: Ethik-Leitlinien
- LZ 2-18: Kernprinzipien zu AI Governance und Responsible AI für Unternehmen

- LZ 2-19: Einblick in die Einrichtung von "Regulatory Sandboxes" und die mögliche rechtliche Konsequenzen bei Nichteinhaltung der Vorschriften des AI-Acts.
- LZ 2-20: Strukturen und Prozesse für die Steuerung und Kontrolle von KI-Systemen, um ethische und gesetzliche Anforderungen zu erfüllen.
- LZ 2-21: Effektive Datenverwaltung für die Sicherstellung von Qualität und Sicherheit von Daten in KI-Anwendungen
- LZ 2-22: Bedeutung und Umsetzung der Transparenzpflicht bei KI-Systemen
- LZ 3-1: Life-Cycle eines Machine-Learning- bzw. Data-Science-Projekts
- LZ 3-2: Vorgehensmodelle für software development von KI-Systemen
- LZ 3-3: Arten von Daten und typische ML-Probleme
- LZ 3-4: Anforderungen an die Daten für ML
- LZ 3-5: Machine Learning Problemstellungen und deren Anforderungen
- LZ 3-6: Validierung und Kenntnis der typischen Datenaufteilung in Trainings-, Validierungs- und Testdaten
- LZ 3-7: Input Daten für verschiedene KI-Algorithmen
- LZ 3-8: Herausforderungen wie Nicht-Determinismus, Datenqualität und Concept- und Modell-Drift
- LZ 3-9: Transfer-Learning bzw. Fine Tuning
- LZ 3-10: Design Patterns für KI-Systeme
- LZ 3-11: Definition der Aufgabe eines ML-Modells
- LZ 3-12: Eingaben und Ausgaben für das Funktionieren eines ML-Systems
- LZ 3-13: Metriken zur Messung der Performance von ML-Modellen
- LZ 3-14: Integration von ML-Modellen in bestehende Systeme
- LZ 3-15: Gestaltung von Benutzeroberflächen
- LZ 3-16: Leistungskennzahlen wie Latenz und Durchsatz in KI-Systemen
- LZ 3-17: Skalierbarkeit auf erhöhte Datenmengen
- LZ 3-18: Verstehen, was Robustheit in KI-Systemen bedeutet, und können Strategien zur Erhöhung der Robustheit in verschiedenen Anwendungskontexten anwenden.
- LZ 3-19: Zuverlässigkeit und Verfügbarkeit von KI-Systemen
- LZ 3-20: Reproduzierbarkeit und Prüfbarkeit von KI-Ergebnisse
- LZ 3-21: Anforderungen an Sicherheit, Datenschutz und Compliance
- LZ 3-22: Entwicklung von KI-Modellen und -Systeme
- LZ 3-23: Erklärbarkeit und Interpretierbarkeit in KI-Systemen
- LZ 3-24: Bias in Daten und Modellen
- LZ 3-25: Fehlertoleranz in KI-Systemen
- LZ 4-1: Methoden, um Daten zu akquirieren und Daten zu labeln
- LZ 4-2: Gängige Plattformen für öffentlich zugängliche Daten
- LZ 4-3: Überblick über relevante Werkzeuge für das Daten-Labeln

- LZ 4-4: Gestaltung effizienter Datenpipelines und -architekturen, Betrachtung von Datenqualität, Speicherlösungen und deren Management
- LZ 4-5: Architekturmuster für Data-Engineering-Pipelines und ETL-Prozesse
- LZ 4-6: Strategien für Datenaggregation, -bereinigung, -transformation, -anreicherung und -augmentierung.
- LZ 4-7: Werkzeuge für Data Engineering Pipelines
- LZ 4-8: Möglichkeiten zur Speicherung der Daten
- LZ 5-1: (Hardware)-Anforderungen an Training und Inferenz
- LZ 5-2: Trade-Offs verschiedener Modellarchitekturen bezüglich der Qualitätsmerkmale
- LZ 5-3: Abstimmung verschiedener Qualitätsmerkmale eines ML-Modells
- LZ 5-4: Kosten, Stromverbrauch und nachhaltige Nutzung von KI (Green IT)
- LZ 5-5: MLOps für die Automatisierung des Life-Cycles eines Data-Science-Projekts
- LZ 5-6: Tracking von Modelltraining, Parametern, Metriken und Ergebnissen.
- LZ 5-7: Evaluation von ML-Modellen und darauf aufbauenden KI-Systemen
- LZ 5-8: Arten von Drift sowie mögliche Ursachen und Lösungsansätze dafür.
- LZ 5-9: CI/CD-Pipelines, Modellmanagement und Deployment-Strategien für KI-Modelle
- LZ 5-10: Zusammenarbeit und Verantwortungsaufteilung zwischen den verschiedenen Rollen
- LZ 5-11: Plattformen für die Modellbereitstellung
- LZ 5-12: Werkzeuge für das Erstellen von POCs von KI-Systemen
- LZ 5-13: Deployment-Möglichkeiten von KI-Modellen
- LZ 5-14: Vor- und Nachteile von SaaS und Self-Hosting
- LZ 5-15: SaaS-KI-Lösungen
- LZ 5-16: Embedded Deployments von ML-Modellen
- LZ 5-17: Monitoring im Hinblick auf KI-spezifische Anforderungen
- LZ 5-18: Relevante Metriken für das Monitoring
- LZ 5-19: Beispiel-Werkzeuge für Monitoring
- LZ 5-20: Nutzer-Feedback für das weitere Modelltraining
- LZ 5-21: Methoden und Werkzeuge zur Sammlung von Nutzer-Feedback
- LZ 5-22: Methoden zur Nutzung von Feedback für das Modell-Training
- LZ 5-23: [OPTIONAL] MLOps-Pipeline an einem Praxisbeispiel
- LZ 5-24: [OPTIONAL] Treffen von Build vs. Buy Entscheidungen für MLOps Systeme/Komponenten
- LZ 5-25: [OPTIONAL] MLOps-Werkzeuge und End-to-End Plattformen
- LZ 6-1: Integrationsebenen von KI
- LZ 6-2: Bibliotheken, Schnittstellen und Tools zur Integration von KI-Modellen
- LZ 6-3: [OPTIONAL] Integration von KI-Systemen in die Gesamtarchitektur einer IT-Landschaft
- LZ 6-4: Relevante Qualitätsmerkmale für KI-Systeme

- LZ 6-5: [OPTIONAL] Evaluations-Frameworks für KI-Systeme
- LZ 6-6: [OPTIONAL] Diskussion eines Fallbeispiels mit einer ausgedachten Fachlichkeit
- LZ 6-7: Verständnis von generativer KI
- LZ 6-8: Funktionsweise von LLMs
- LZ 6-9: Bekannte Patterns bei der Nutzung von LLMs
- LZ 6-10: Use-Cases für RAG (Retrieval-Augmented Generation)
- LZ 6-11: RAG-Techniken
- LZ 6-12: Arten von Prompt Engineering
- LZ 6-13: Agentic Workflows
- LZ 6-14: Design Patterns für Generative AI-Systeme
- LZ 6-15: Techniken zur Evaluation von LLM-Anwendungen
- LZ 6-16: Bekannte LLMs und Auswahlkriterien
- LZ 6-17: Bedeutung von Cost Management für GenAI Applikationen
- LZ 6-18: Beispiele von verbreiteten Bibliotheken, Schnittstellen und Tools im Zusammenhang mit LLM-Anwendungen
- LZ 6-19: [OPTIONAL] Agentic AI Software Architekturen, AI Agent Architekturkomponenten, Typen von AI Agentarchitekturen
- LZ 7-1: Üben anhand von Fallstudien und Praxisprojekten, das erworbene Wissen in realen Szenarien anzuwenden.

Einführung: Allgemeines zum iSAQB Advanced Level

Was vermittelt ein Advanced Level Modul?

Das Modul kann unabhängig von einer CPSA-F-Zertifizierung besucht werden.

- Der iSAQB Advanced Level bietet eine modulare Ausbildung in drei Kompetenzbereichen mit flexibel gestaltbaren Ausbildungswegen. Er berücksichtigt individuelle Neigungen und Schwerpunkte.
- Die Zertifizierung erfolgt als Hausarbeit. Die Bewertung und mündliche Prüfung wird durch vom iSAQB benannte Expert:innen vorgenommen.

Was können Absolventen des Advanced Level (CPSA-A)?

CPSA-A-Absolventen können:

- eigenständig und methodisch fundiert mittlere bis große IT-Systeme entwerfen
- in IT-Systemen mittlerer bis hoher Kritikalität technische und inhaltliche Verantwortung übernehmen
- Maßnahmen zur Erreichung von Qualitätsanforderungen konzeptionieren, entwerfen und dokumentieren sowie Entwicklungsteams bei der Umsetzung dieser Maßnahmen begleiten
- architekturelevante Kommunikation in mittleren bis großen Entwicklungsteams steuern und durchführen

Voraussetzungen zur CPSA-A-Zertifizierung

- erfolgreiche Ausbildung und Zertifizierung zum Certified Professional for Software Architecture, Foundation Level® (CPSA-F)
- mindestens drei Jahre Vollzeit-Berufserfahrung in der IT-Branche; dabei Mitarbeit an Entwurf und Entwicklung von mindestens zwei unterschiedlichen IT-Systemen
 - Ausnahmen sind auf Antrag zulässig (etwa: Mitarbeit in Open-Source-Projekten)
- Aus- und Weiterbildung im Rahmen von iSAQB-Advanced-Level-Schulungen im Umfang von mindestens 70 Credit Points aus mindestens drei unterschiedlichen Kompetenzbereichen
- erfolgreiche Bearbeitung der CPSA-A-Zertifizierungsprüfung



Grundlegendes

Was vermittelt das Modul „SWARC4AI“?

Das Modul präsentiert den Teilnehmer:innen moderne Softwarearchitektur-Konzepte für KI-Systeme als Mittel, um leistungsfähige, skalierbare und integrierbare KI- Lösungen zu gestalten. Am Ende des Moduls kennen die Teilnehmer:innen die wesentlichen Prinzipien der Softwarearchitektur für KI-Systeme und können diese bei Entwurf und Implementierung von Machine Learning und Generative KI- Systemen anwenden. Mit Hilfe der vermittelten Modellierungstechniken und Architekturwerkzeuge können sie KI-Komponenten nahtlos in bestehende Softwaresysteme integrieren. Die Schulung umfasst sowohl Machine Learning Systeme als auch Generative KI und vermittelt, wie diese mit klassischen Softwaresystemen kombiniert werden können. Die Teilnehmer:innen lernen, wie die Architektur für solche hybriden Systeme aussehen muss, um Skalierbarkeit, Wartbarkeit und Erweiterbarkeit zu gewährleisten.

Struktur des Lehrplans und empfohlene zeitliche Aufteilung

Inhalt	Empfohlene Minstdauer (min)
Einführung in softwarearchitekturelevante Konzepte für Künstliche Intelligenz	120
Compliance, Security, Alignment	120
Architektur von KI-Systemen	320
Datenmanagement und Datenverarbeitung für KI-Systeme	90
Skalierbarkeit und Leistungsoptimierung von KI-Systemen	160
Systemarchitekturen- und Plattformen für Generative KI-Systeme	160
Fallstudien und Praxisprojekte	110
Gesamt	1080

Dauer, Didaktik und weitere Details

Die Dauer einer Schulung zum Modul SWARC4AI sollte mindestens 3 Tage betragen, kann aber länger sein. Anbieter können sich durch Dauer, Didaktik, Art und Aufbau der Übungen sowie der detaillierten Kursgliederung voneinander unterscheiden. Insbesondere die Art der Beispiele und Übungen lässt der Lehrplan komplett offen. Lizenzierte Schulungen zu SWARC4AI tragen zur Zulassung zur abschließenden Advanced-Level-Zertifizierungsprüfung folgende Credit Points) bei:

Methodische Kompetenz:	10 Punkte
Technische Kompetenz:	20 Punkte
Kommunikative Kompetenz:	0 Punkte

Voraussetzungen

Teilnehmer:innen **sollten** folgende Kenntnisse und/oder Erfahrung mitbringen:

- Ein grundlegendes Verständnis von Künstlicher Intelligenz, Machine Learning und Data Science

- Vertrautheit mit Machine Learning-Methoden, wie Supervised Learning, Unsupervised Learning und Reinforcement Learning, einschließlich Klassifikation, Clustering, Regression und Dimensionality Reduction
- Grundkenntnisse über gängige Algorithmen, wie z. B. lineare und logistische Regression, Entscheidungsbäume, Random Forests, Support Vector Machines, K-Means Clustering sowie neuronale Netze und Deep Learning
- Ein Verständnis der Modellevaluation, einschließlich Cross-Validation, relevanter Metriken (Accuracy, Precision, Recall, F1-Score) und des Bias-Variance Tradeoffs
- Erfahrung mit typischen Frameworks wie scikit-learn, TensorFlow und PyTorch
- Vertrautheit mit Jupyter Notebooks oder ähnlichen Werkzeugen zur schnellen Anwendungsentwicklung (Rapid Application Development, RAD)
- Ein grundlegendes Verständnis der technischen Verfahren hinter Künstlicher Intelligenz, einschließlich Maschinellen Lernens (insbesondere Deep Learning und LLMs) sowie Ansätzen im Bereich Natural Language Processing (NLP) und Transformationsmodellen
- Praktische Erfahrung im Training von Künstlichen Intelligenz-Modellen

Gliederung des Lehrplans

Die einzelnen Abschnitte des Lehrplans sind gemäß folgender Gliederung beschrieben:

- **Begriffe/Konzepte:** Wesentliche Kernbegriffe dieses Themas.
- **Unterrichts-/Übungszeit:** Legt die Unterrichts- und Übungszeit fest, die für dieses Thema bzw. dessen Übung in einer akkreditierten Schulung mindestens aufgewendet werden muss.
- **Lernziele:** Beschreibt die zu vermittelnden Inhalte inklusive ihrer Kernbegriffe und -konzepte.

Dieser Abschnitt skizziert damit auch die zu erwerbenden Kenntnisse in entsprechenden Schulungen.

Ergänzende Informationen, Begriffe, Übersetzungen

Soweit für das Verständnis des Lehrplans erforderlich, haben wir Fachbegriffe ins [iSAQB-Glossar](#) aufgenommen, definiert und bei Bedarf durch die Übersetzungen der Originalliteratur ergänzt.

1. Einführung in softwarearchitekturelevante Konzepte für Künstliche Intelligenz

Dauer: 120 Min.	Übungszeit: 0 Min.
-----------------	--------------------

1.1. Begriffe und Konzepte

KI, Generative KI, Machine Learning, Symbolische KI, Evolutionäre Algorithmen, Statistical Learning, Deep Learning, LLMs, Halluzination, Bias, Jagged Technological Frontier, Data Preparation, Model Training, Model Evaluation, Feature Engineering, Data Science, Data Engineering

1.2. Lernziele

In diesem Kapitel erreichen die Teilnehmer:innen die folgenden Lernziele:

LZ 1-1: Definition Künstliche Intelligenz inklusive der Einordnung von Machine Learning, Data Science, Deep Learning, Generative AI

Die Teilnehmer:innen wissen wie man Künstliche Intelligenz definiert und wie Machine Learning, Data Science, Deep Learning, Generative AI darin eingeordnet werden.

LZ 1-2: Spezifikation typischer allgemeiner Anwendungsfälle für KI

Die Teilnehmer:innen wissen wie typische allgemeine Anwendungsfälle für KI spezifiziert werden können. Dies umfasst Anwendungsfälle für z.B. Bilderkennung & -erzeugung, Sprachverarbeitung, Vorhersagen, Personalisierung und Anomalieerkennung.

LZ 1-3: Einsatzmöglichkeiten in verschiedenen Branchen

Die Teilnehmer:innen kennen die möglichen Einsatzmöglichkeiten in verschiedenen Branchen, z.B. Marketing, Medizin, Robotik und Content-Creation.

LZ 1-4: Einsatzmöglichkeiten in Endnutzeranwendungen

Die Teilnehmer:innen überblicken die Einsatzmöglichkeiten in Endnutzeranwendungen von KI. Darunter fallen z.B. Sprachassistenten (Chatbots) und Empfehlungssysteme (Recommender Engine).

LZ 1-5: Risiken bei der Anwendung von KI

Die Teilnehmer:innen kennen und verstehen die Risiken, die bei der Anwendung von KI auftreten können. Dazu gehören beispielsweise

- Halluzinationen
- Bias
- (un-)Fairness
- gesellschaftlichen Risiken wie Deepfakes, AI-enabled Cyberattacks, Safety Risks in Critical Systems, Social Manipulation, Intellectual Property Issues usw.

LZ 1-6: Unterschiede zu traditioneller Software

Die Teilnehmer:innen verstehen die Unterschiede von KI-Systemen zu traditioneller Software:

- Datengetrieben (bei ML) - Daten-zentrierte statt Code-zentrierte Entwicklung

- Probabilistische Ergebnisse (Non-deterministic behavior)
- Statistische Validierung
- Experimentelles Design: Unterstützung für schnelle Iteration und Testen von Modellen.
- Modellkomplexität und Interpretierbarkeit: ML-Modelle, insbesondere Deep-Learning-Modelle, können äußerst komplex sein. Der „Black-Box“-Charakter erschwert die Interpretierbarkeit und Erklärbarkeit.
- Debugging und Tests sind aufgrund des Nichtdeterminismus komplexer.
- Model Decay: Continuous monitoring und Retraining sind notwendig, um die Leistung der Modelle aufrecht zu erhalten.
- AI-spezifische Regulatorik von Branchen und auf EU-Ebene müssen berücksichtigt werden.
- Interoperabilität: Nahtlose Integration in bestehende Systeme und Technologiestacks.

LZ 1-7: Entscheidungsfähigkeit zur Lösung von Problemen mittels KI oder klassischer SW-Entwicklung

Teilnehmer:innen können entscheiden und erklären, ob und warum ein Problem mittels KI oder klassischer SW-Entwicklung zu lösen ist.

LZ 1-8: Rollen und deren Aufgaben im Kontext von KI

Die Teilnehmer:innen kennen typische Rollen und deren Aufgaben in diesen Kontexten. Die Rollen umfassen insbesondere:

- Data Scientist
- Data Analyst
- Data Engineer
- Machine Learning Engineer
- MLOps Engineer
- AI Architect
- Data Architect
- Business Intelligence (BI) Developer
- Data Governance Specialist
- ML-Researcher

LZ 1-9: Zusammenarbeit der Rollen im Team (Team Topologies für ML-Teams)

Die Teilnehmer:innen wissen, wie diese Rollen im Team zusammenarbeiten könnten (Team Topologies für ML-Teams).

LZ 1-10: Identifikation und Priorisierung von KI Anwendungsfällen

Die Teilnehmer:innen können KI Anwendungsfälle identifizieren und priorisieren.

LZ 1-11: KI Stärken und Grenzen

Die Teilnehmer:innen verstehen die Stärken und die Grenzen von KI und kennen die sog. "Jagged Technological Frontier".

LZ 1-12: Kennen Productivity J-Curve Konzept in Verbindung mit KI-Technologie (Dieses Phänomen hilft zu verstehen, warum Unternehmen bei der Implementierung von KI zunächst einen Produktivitätsrückgang verzeichnen können, dem bei der weiteren Entwicklung aber Produktivitätsgewinne folgen können.).

1.3. Referenzen

[Roser 2022], [Burkov 2019], [Géron 2022], [Kelleher 2015], [Vaughan 2020], [Bahree 2024], [Harvard et al. 2024], [Dell'Acqua 2022], [Visengeriyeva], [Visengeriyeva], [Agrawal et al.], [Tan et al.], [Chong et al.], [Hall et al. 2023], [Huyen 2022], [Wang et al. 2024]

2. Compliance, Security, Alignment

Dauer: 120 Min.	Übungszeit: 30 Min.
-----------------	---------------------

2.1. Begriffe und Konzepte

EU AI Act, Datenschutz, Urheberrecht, Lizenz, Open (Source), AI Security, Jailbreak, Adversarial Attack, Data Poisoning, Model Inversion & Extraction, AI Safety, AI Ethics, AI Alignment, Model und Data Dokumentation, Transparenzpflicht, Human Oversight, Data Governance, AI Governance, AI Systems by Risk Levels (Prohibited, High-Risk, Limited Risk, Low-Risk)

2.2. Lernziele

Die Teilnehmer:Innen erreichen mit diesem Kapitel die folgenden Lernziele:

LZ 2-1: Einfluss der Datenschutzgesetze auf die Implementierung und Nutzung von KI

Die Teilnehmer:innen kennen die Datenschutzgesetze, wie die DSGVO, und wissen wie diese die Sammlung, Verarbeitung und Speicherung von Daten durch KI-Systeme beeinflussen.

LZ 2-2: Ziele und Regelungen des EU AI Act

Die Teilnehmer:innen verstehen die Ziele und Regelungen des EU AI Act und wissen welchen Einfluss dies auf die Entwicklung und den Einsatz von KI-Systemen hat.

LZ 2-3: Einfluss des EU AI Act (Trustworthy AI) auf den Entwicklungsprozess und die Architektur des Softwaresystems

Die Teilnehmer:innen verstehen die Anforderungen des EU AI Act (Trustworthy AI) und welchen Einfluss diese Anforderungen auf den Entwicklungsprozess und die Architektur des Softwaresystems hat. Insbesondere kennen sie den Einfluss auf einige der folgenden Aspekte:

- Risikomanagementsystem (Risikominimierung)
- Datenqualität und Datengovernance (Qualitätsmanagementsystem)
- Erstellung und Pflege einer umfassenden technischen Dokumentation des KI-Systems
- Automatische Aufzeichnung/Logging von Events im KI-System.
- Bereitstellung klarer und verständlicher Informationen für Nutzer
- Implementierung der Maßnahmen zur menschlichen Aufsicht
- Gewährleistung eines angemessenen Maßes an Genauigkeit/Accuracy und Robustheit
- Implementierung von Maßnahmen zur Cybersicherheit

LZ 2-4: Klassifikation von KI-Systemen nach EU AI Act Risikolevel

Die Teilnehmer:innen kennen die Klassifikation von KI-Systemen nach den EU AI Act Risikolevel (verboten, hochrisikoreich, begrenzt risikoreich, niedrigrisikoreich) und wissen, welche regulatorischen Anforderungen jeweils gelten.

LZ 2-5: Urheberrechtsproblematik von KI-generierten Inhalten

Die Teilnehmer:innen verstehen die Urheberrechtsproblematik für KI-generierte Inhalte und kennen die Auswirkungen auf bestimmte Software-Lizenzmodelle sowie mögliche Umgänge damit.

LZ 2-6: Arten bzw. Grade der Offenheit freier ML-Modelle

Die Teilnehmer:innen überblicken verschiedene Arten bzw. Grade der Offenheit freier ML-Modelle. Das betrifft beispielsweise die Offenlegung der Daten und der Modellparameter.

LZ 2-7: Arten von Lizenzen freier ML-Modelle

Die Teilnehmer:innen kennen verschiedene Arten von Lizenzen freier ML-Modelle sowie deren Auswirkungen auf das KI-System

LZ 2-8: Strategien für die Einhaltung des europäischen AI-Acts und mögliche Herausforderungen

Die Teilnehmer:innen verstehen die Grundaussagen des europäischen AI-Acts (insbesondere Transparenzpflichten) und kennen Strategien für deren Einhaltung sowie mögliche Herausforderungen dabei.

LZ 2-9: Dokumentation von Modellen und Datensätzen für die Nachvollziehbarkeit und Transparenz

Die Teilnehmer:innen wissen, wie man Modelle und Datensätze effektiv dokumentiert, um Nachvollziehbarkeit und Transparenz zu gewährleisten.

LZ 2-10: Fallstricke hinsichtlich Security

Die Teilnehmer:innen kennen mögliche Fallstricke hinsichtlich Security.

LZ 2-11: Angriffsarten auf ML-Modelle

Die Teilnehmer:innen kennen typische Angriffsarten auf ML-Modelle und Beispiele dafür, beispielsweise:

- LLM-Jailbreaks durch Prompt-Engineering
- Adversarial Attacks
- Data Poisoning
- Model Inversion & Extraction.

LZ 2-12: AI-Risk Minimierung Strategien

Die Teilnehmer:innen können Strategien zur AI-Risikominimierung entwickeln und anwenden. Insbesondere die folgenden Strategien kennen die Teilnehmer:innen:

- Stärkung der Robustheit durch umfangreiche Tests
- Fehlertolerante KI-Systeme
- Transparente Entwicklung
- Erklärbare KI (explainable AI)

LZ 2-13: Möglichkeiten zur Absicherung gegen Angriffe (AI Security)

Die Teilnehmer:innen kennen verschiedene Möglichkeiten zur Absicherung gegen Angriffe (AI Security) und insbesondere kennen sie Möglichkeiten zur Integration von Sicherheitsstandards in die Architektur und können diese beim Entwurf berücksichtigen.

LZ 2-14: Grundproblematik und Facetten von AI-Safety

Die Teilnehmer:innen verstehen die Grundproblematik von AI-Safety und kennen die verschiedenen Facetten dazu. Insbesondere kennen die Teilnehmer:innen spezifische Probleme wie beispielsweise "AI

model risks by poisoning" und "Bias".

LZ 2-15: Probleme hinsichtlich Ethik, die KI-Systeme mit sich bringen können

Die Teilnehmer:innen wissen um die Probleme hinsichtlich Ethik, die KI-Systeme mit sich bringen können.

LZ 2-16: Ansätze zum Umgang mit ethischen Problemen

Die Teilnehmer:innen kennen Ansätze und Möglichkeiten, mit ethischen Problemen umzugehen. Dies umfasst beispielsweise KI-Alignment (und dessen Grenzen) sowie die Erstellung eigener KI-Richtlinien.

LZ 2-17: Ethik-Leitlinien

Die Teilnehmer:innen überblicken wichtige Ethik-Leitlinien wie die „EU-Ethik-Leitlinien für vertrauenswürdige KI“ sowie die „Google AI Ethics Guidelines“.

LZ 2-18: Kernprinzipien zu AI Governance und Responsible AI für Unternehmen

Die Teilnehmer:innen kennen die wichtigsten Dokumente zu AI Governance, um die Kernprinzipien zu AI Governance und Responsible AI für das Unternehmen auszuarbeiten. Dies betrifft insbesondere die folgenden Dokumente:

- OECD AI Principles, <https://oecd.ai/en/ai-principles>
- The Asilomar AI Principles, <https://futureoflife.org/open-letter/ai-principles/>
- The IEEE Ethically Aligned Design framework, https://standards.ieee.org/wp-content/uploads/import/documents/other/ead_v2.pdf

LZ 2-19: Einblick in die Einrichtung von "Regulatory Sandboxes" und die mögliche rechtliche Konsequenzen bei Nichteinhaltung der Vorschriften des AI-Acts.

Die Teilnehmer:innen erhalten einen Einblick in die Einrichtung von "Regulatory Sandboxes" zur Förderung von Innovationen und in die möglichen rechtlichen Konsequenzen bei Nichteinhaltung der Vorschriften des AI-Acts.

LZ 2-20: Strukturen und Prozesse für die Steuerung und Kontrolle von KI-Systemen, um ethische und gesetzliche Anforderungen zu erfüllen.

Die Teilnehmer:innen verstehen die Strukturen und Prozesse, die zur Steuerung und Kontrolle von KI-Systemen notwendig sind, um ethische und gesetzliche Anforderungen zu erfüllen.

LZ 2-21: Effektive Datenverwaltung für die Sicherstellung von Qualität und Sicherheit von Daten in KI-Anwendungen

Die Teilnehmer:innen wissen, wie effektive Datenverwaltung die Qualität und Sicherheit von Daten in KI-Anwendungen sicherstellt.

LZ 2-22: Bedeutung und Umsetzung der Transparenzpflicht bei KI-Systemen

Die Teilnehmer:innen verstehen die Bedeutung der Transparenzpflicht bei KI-Systemen und wissen, wie sie diese in der Praxis umsetzen können.

2.3. Referenzen

[Engler et al.], [Nist], [Hall et al. 2023], [Masood et al. 2023], [CSIRO et al. 2023], [Pruksachatkun et al. 2023], [Chen et al. 2022], [ATLAS], [Visengeriyeva], [EU AI Act], [Hotz], [Bhalaria 2022], [Jarmul 2023], [Molnar 2024]

3. Architektur von KI-Systemen

Dauer: 320 Min.	Übungszeit: 45 Min.
-----------------	---------------------

3.1. Begriffe und Konzepte

CI/CD, MLOps, CRISP-ML(Q), AI-Application, AI-Engineering, ML-Modellentwicklung, ML-Infrastruktur, Performance, Robustheit, Zuverlässigkeit, Fehlertoleranz, Model-as-Service, Model-as-Dependency, Precompute, Model-on-Demand, Hybrid-Serving, Multi-Agent System (MAS)

3.2. Lernziele

Die Teilnehmer:Innen erreichen die folgenden Lernziele.

LZ 3-1: Life-Cycle eines Machine-Learning- bzw. Data-Science-Projekts

Die Teilnehmer:innen haben ein Verständnis für den Life-Cycle eines Machine-Learning- bzw. Data-Science-Projekts. Dabei kennen sie insbesondere die folgenden Phasen:

- Exploratory Data Analysis
- Data Cleansing und Aufbereitung
- Feature Engineering
- Modell Training und Auswahl
- POC
- Deployment
- Maintenance

LZ 3-2: Vorgehensmodelle für software development von KI-Systemen

Die Teilnehmer:innen kennen typische Vorgehensmodelle für software development von KI-Systemen:

- CRISP-ML(Q)
- Team Data Science Process
- GenAI Life Cycle

LZ 3-3: Arten von Daten und typische ML-Probleme

Die Teilnehmer:innen kennen verschiedene Arten von Daten und typische ML-Probleme sowie Anwendungsfälle.

LZ 3-4: Anforderungen an die Daten für ML

Die Teilnehmer:innen haben ein Verständnis für verschiedene Anforderungen an die Daten, z.B. Vorhandensein von Labels verschiedener Art.

LZ 3-5: Machine Learning Problemstellungen und deren Anforderungen

Die Teilnehmer:innen verstehen die verschiedenen Machine Learning Problemstellungen wie beispielsweise

- Supervised Learning
- Unsupervised Learning
- Reinforcement Learning

und wissen, welche Anforderungen diese haben.

LZ 3-6: Validierung und Kenntnis der typischen Datenaufteilung in Trainings-, Validierungs- und Testdaten

Die Teilnehmer:innen haben ein gutes Verständnis für die Notwendigkeit von Validierung und Kenntnis der typischen Datenaufteilung in Trainings-, Validierungs- und Testdaten.

LZ 3-7: Input Daten für verschiedene KI-Algorithmen

Die Teilnehmer:innen haben ein gutes Verständnis für Input Daten für verschiedene KI-Algorithmen wie beispielsweise

- Neuronale Netze als numerische Vektoren und Matrizen bzw. Tensoren
- One-Hot-Encodings
- Embeddings.

LZ 3-8: Herausforderungen wie Nicht-Determinismus, Datenqualität und Concept- und Modell-Drift

Die Teilnehmer:innen verstehen, wie man mit Herausforderungen wie Nicht-Determinismus, Datenqualität und Concept- und Modell-Drift umgeht.

LZ 3-9: Transfer-Learning bzw. Fine Tuning

Die Teilnehmer:innen kennen Transfer-Learning bzw. Fine Tuning als Möglichkeit, um die vortrainierten Basismodelle auf bestehende Anwendungsfälle zu adoptieren.

LZ 3-10: Design Patterns für KI-Systeme

Die Teilnehmer:innen wissen welche Design Patterns für KI-Systeme existieren und wie man passende Patterns auswählt. Das betrifft die folgenden Design Patterns:

- ML Systems Topology Patterns
- Pipeline Architecture Patterns
- Model Training Pattern
- Model Serving Patterns
- Model Deployment Patterns

Funktionale Anforderungen

LZ 3-11: Definition der Aufgabe eines ML-Modells

Die Teilnehmer:innen wissen, wie man die Anwendungsfälle / Aufgaben eines ML-Modells definiert, wie beispielsweise die Klassifikation von Bildern oder die Erkennung von Betrug.

LZ 3-12: Eingaben und Ausgaben für das Funktionieren eines ML-Systems

Die Teilnehmer:innen verstehen, welche Eingaben und Ausgaben für das Funktionieren eines ML-Systems

erforderlich sind und können diese spezifizieren.

LZ 3-13: Metriken zur Messung der Performance von ML-Modellen

Die Teilnehmer:innen kennen verschiedene Metriken zur Messung der Performance von ML-Modellen, wie beispielsweise:

- Precision, Recall
- F1
- Accuracy

und wissen, wie man Bewertungskriterien zur Leistungsbeurteilung festlegt.

LZ 3-14: Integration von ML-Modellen in bestehende Systeme

Die Teilnehmer:innen verstehen, wie ML-Modelle in bestehende Systeme integriert werden können und kennen die Schnittstellen und Integrationspunkte.

LZ 3-15: Gestaltung von Benutzeroberflächen

Die Teilnehmer:innen wissen, wie Benutzeroberflächen gestaltet werden sollten, um effektive Interaktionen mit dem ML-System zu ermöglichen und die Benutzererfahrung zu optimieren.

Nicht-funktionale Anforderungen

LZ 3-16: Leistungskennzahlen wie Latenz und Durchsatz in KI-Systemen

Die Teilnehmer:innen verstehen die Bedeutung von Leistungskennzahlen wie Latenz und Durchsatz in KI-Systemen und wissen, wie diese optimiert werden können.

LZ 3-17: Skalierbarkeit auf erhöhte Datenmengen

Die Teilnehmer:innen verstehen die Bedeutung der Skalierbarkeit auf erhöhte Datenmengen und wissen, wie man KI-Systeme entwickelt, die mit steigenden Datenvolumen umgehen können, ohne an Leistung zu verlieren.

LZ 3-18: Verstehen, was Robustheit in KI-Systemen bedeutet, und können Strategien zur Erhöhung der Robustheit in verschiedenen Anwendungskontexten anwenden.

Die Teilnehmer:innen haben Verständnis davon, was Robustheit in KI-Systemen bedeutet, und können Strategien zur Erhöhung der Robustheit in verschiedenen Anwendungskontexten anwenden.

LZ 3-19: Zuverlässigkeit und Verfügbarkeit von KI-Systemen

Die Teilnehmer:innen verstehen die Konzepte der Zuverlässigkeit und Verfügbarkeit und wissen, wie sie KI-Systeme bauen, die stabil und konstant verfügbar sind.

LZ 3-20: Reproduzierbarkeit und Prüfbarkeit von KI-Ergebnisse

Die Teilnehmer:innen wissen, wie wichtig es ist, dass KI-Ergebnisse reproduzierbar und prüfbar sind, und wissen, welche Methoden zur Sicherstellung dieser Eigenschaften eingesetzt werden können.

LZ 3-21: Anforderungen an Sicherheit, Datenschutz und Compliance

Die Teilnehmer:innen kennen die Anforderungen an Sicherheit, Datenschutz und Compliance und wissen, wie diese in KI-Systemen umgesetzt werden.

LZ 3-22: Entwicklung von KI-Modellen und -Systeme

Die Teilnehmer:innen wissen, wie man KI-Modelle und -Systeme entwickelt, die ressourcenschonend arbeiten, indem sie Speicher, Rechenleistung und Speicherplatz effizient nutzen.

LZ 3-23: Erklärbarkeit und Interpretierbarkeit in KI-Systemen

Die Teilnehmer:innen verstehen die Bedeutung von Erklärbarkeit und Interpretierbarkeit in KI-Systemen und wissen, wie man diese sicherstellen kann, um Vertrauen und Transparenz zu fördern.

LZ 3-24: Bias in Daten und Modellen

Die Teilnehmer:innen wissen, wie Bias in Daten und Modellen erkannt und reduziert werden können, um Fairness und Gleichbehandlung in KI-Anwendungen sicherzustellen.

LZ 3-25: Fehlertoleranz in KI-Systemen

Die Teilnehmer:innen kennen die Konzepte der Fehlertoleranz und können erläutern, wie KI-Systeme trotz Fehlern oder Störungen funktionsfähig bleiben.

3.3. Referenzen

[TU Berlin], [Bornstein et al.], [Crowe et al. 2024], [Lakshmanan et al.], [Alake], [Lakshmanan et al.], [Lakshmanan et al.], [Koc], [Cdteliot], [Visengeriyeva], [Zaharia et al.], [Savarese], [tdcox], [Studer et al.], [Hotz], [Hotz], [Saltz], [Serban], [Heiland et al. 2023], [Nahar et al.], [ML software architecture],

4. Datenmanagement und Datenverarbeitung für KI-Systeme

Dauer: 90 Min.	Übungszeit: 0 Min.
----------------	--------------------

4.1. Begriffe und Konzepte

Datenakquise, Labelling, Daten-Pipeline, ETL-Prozesse, Datenaggregation, Datenbereinigung, Transformation, Augmentierung, Dateien, RDBMS, NoSQL, Data Products, Data Contracts, Data Architectures: Data Warehouse, Data Lake, Data Mesh

4.2. Lernziele

Die Teilnehmer:innen erreichen in diesem Kapitel die folgenden Lernziele:

LZ 4-1: Methoden, um Daten zu akquirieren und Daten zu labeln

Die Teilnehmer:innen überblicken verschiedene Methoden, um Daten zu akquirieren und Daten zu labeln.

LZ 4-2: Gängige Plattformen für öffentlich zugängliche Daten

Die Teilnehmer:innen können gängige Plattformen für öffentlich zugängliche Daten nennen.

LZ 4-3: Überblick über relevante Werkzeuge für das Daten-Labeln

Die Teilnehmer:innen kennen relevante Werkzeuge fürs Daten-Labeln wie beispielsweise CVAT, Amazon Mechanical Turk.

LZ 4-4: Gestaltung effizienter Datenpipelines und -architekturen, Betrachtung von Datenqualität, Speicherlösungen und deren Management

Die Teilnehmer:innen haben ein Verständnis für die Gestaltung effizienter Datenpipelines und -architekturen, die Betrachtung von Datenqualität, sowie für Speicherlösungen und deren Management.

LZ 4-5: Architekturmuster für Data-Engineering-Pipelines und ETL-Prozesse

Die Teilnehmer:innen kennen Architekturmuster für Data-Engineering-Pipelines und ETL-Prozesse.

LZ 4-6: Strategien für Datenaggregation, -bereinigung, -transformation, -anreicherung und -augmentierung.

Die Teilnehmer:innen kennen Strategien für Datenaggregation, -bereinigung, -transformation, -anreicherung und -augmentierung.

LZ 4-7: Werkzeuge für Data Engineering Pipelines

Die Teilnehmer:innen überblicken relevante Werkzeuge für Data Engineering Pipelines wie beispielsweise Apache Spark und Flink.

LZ 4-8: Möglichkeiten zur Speicherung der Daten

Die Teilnehmer:innen kennen verschiedene Möglichkeiten zur Speicherung der Daten sowie deren Vor- und Nachteile. Zu den Möglichkeiten gehören die folgenden Technologien: * CSV-Dateien * Spaltenorientierte Dateien * Relationale und NoSQL-Datenbanken * Data Warehouses * Data Lakes

4.3. Referenzen

[Sarkis], [Serra], [Dehghani], [Reis et al.], [Bornstein et al.], [Ford et al.], [Bhajaria 2022], [Sanderson et al.], [Jones]

5. Skalierbarkeit und Leistungsoptimierung von KI-Systemen

Dauer: 160 Min.	Übungszeit: 30 Min.
-----------------	---------------------

5.1. Begriffe und Konzepte

Monitoring, Logging, Feedback, FinOps für KI-Plattformen

5.2. Lernziele

Die Teilnehmer:innen erreichen in diesem Kapitel die folgenden Lernziele:

LZ 5-1: (Hardware)-Anforderungen an Training und Inferenz

Die Teilnehmer:innen kennen unterschiedliche (Hardware)-Anforderungen für beispielsweise TPU, GPU oder CPU an Training und Inferenz.

LZ 5-2: Trade-Offs verschiedener Modellarchitekturen bezüglich der Qualitätsmerkmale

Die Teilnehmer:innen können beispielhaft Trade-Offs verschiedener Modellarchitekturen bezüglich der Qualitätsmerkmale nennen. Insbesondere für Skalierung, Effizienz und Speicherlast sollten die Teilnehmer:innen die Trade-Offs sowie die Vor- und Nachteile von wichtigen Architekturen wie beispielsweise RNNs und Transformern kennen.

LZ 5-3: Abstimmung verschiedener Qualitätsmerkmale eines ML-Modells

Die Teilnehmer:innen kennen Möglichkeiten, um verschiedene Qualitätsmerkmale wie Genauigkeit, Effizienz und Speicherlast eines ML-Modells abzustimmen und gegeneinander einzutauschen. Insbesondere kennen die Teilnehmer:innen die folgenden Techniken: * Quantisierung * Pruning * Destillierung * LoRA.

LZ 5-4: Kosten, Stromverbrauch und nachhaltige Nutzung von KI (Green IT)

Die Teilnehmer:innen erlangen ein Verständnis für Kosten, Stromverbrauch und nachhaltige Nutzung von KI (Green IT).

LZ 5-5: MLOps für die Automatisierung des Life-Cycles eines Data-Science-Projekts

Die Teilnehmer:innen kennen den Begriff MLOps für die Automatisierung des Life-Cycles eines Data-Science-Projekts sowie den Zusammenhang mit DevOps.

LZ 5-6: Tracking von Modelltraining, Parametern, Metriken und Ergebnissen.

Die Teilnehmer:innen haben ein Verständnis vom Tracking im Modelltraining, Parametern, Metriken und Ergebnissen.

LZ 5-7: Evaluation von ML-Modellen und darauf aufbauenden KI-Systemen

Die Teilnehmer:innen überblicken Ansätze zur Evaluation von ML-Modellen und darauf aufbauenden KI-Systemen.

LZ 5-8: Arten von Drift sowie mögliche Ursachen und Lösungsansätze dafür.

Die Teilnehmer:innen kennen verschiedene Arten von Drift, wie beispielsweise Daten-Drift oder Modell-Drift, sowie mögliche Ursachen und Lösungsansätze dafür.

LZ 5-9: CI/CD-Pipelines, Modellmanagement und Deployment-Strategien für KI-Modelle

Die Teilnehmer:innen haben ein Verständnis von CI/CD-Pipelines, Modellmanagement und Deployment-Strategien für KI-Modelle.

LZ 5-10: Zusammenarbeit und Verantwortungsaufteilung zwischen den verschiedenen Rollen

Die Teilnehmer:innen kennen verschiedene Möglichkeiten der Zusammenarbeit und Verantwortungsaufteilung zwischen den verschiedenen Rollen, wie beispielsweise Data Engineer, ML-Engineer und Softwareentwickler:in bezogen auf die verschiedenen Phasen des Life-Cycles.

LZ 5-11: Plattformen für die Modellbereitstellung

Die Teilnehmer:innen kennen gängige Plattformen für die Modellbereitstellung, wie beispielsweise Huggingface Hub.

LZ 5-12: Werkzeuge für das Erstellen von POCs von KI-Systemen

Die Teilnehmer:innen können gängige Werkzeuge für das Erstellen von POCs von KI-Systemen, wie beispielsweise Gradi, nennen und verstehen die konzeptionelle Funktionsweise.

LZ 5-13: Deployment-Möglichkeiten von KI-Modellen

Die Teilnehmer:innen kennen verschiedene Deployment-Möglichkeiten von KI-Modellen. Insbesondere die folgenden Möglichkeiten verstehen die Teilnehmer:innen: * API Deployment * Embedded Deployment * Batch Prediction * Streaming * Containerization * Serverless Deployment * Cloud Services

LZ 5-14: Vor- und Nachteile von SaaS und Self-Hosting

Die Teilnehmer:innen kennen die Vor- und Nachteile von SaaS und Self-Hosting und können dazwischen abwägen.

LZ 5-15: SaaS-KI-Lösungen

Die Teilnehmer:innen überblicken bekannte SaaS-KI-Lösungen, wie beispielsweise Azure OpenAI Services.

LZ 5-16: Embedded Deployments von ML-Modellen

Die Teilnehmer:innen kennen verschiedene Möglichkeiten und Standards für Embedded Deployments von ML-Modellen.

LZ 5-17: Monitoring im Hinblick auf KI-spezifische Anforderungen

Die Teilnehmer:innen verstehen die Notwendigkeit für Monitoring, auch im Hinblick auf KI-spezifische Anforderungen wie das Tracking von Drift.

LZ 5-18: Relevante Metriken für das Monitoring

Die Teilnehmer:innen kennen relevante Metriken wie beispielsweise Accuracy, Precision, Recall, F1-Score, MAE, MSE, Perplexity, Latenz, Durchsatz und Ressourcenauslastung und verstehen, warum diese für das Monitoring relevant sind.

LZ 5-19: Beispiel-Werkzeuge für Monitoring

Die Teilnehmer:innen kennen Beispiel-Werkzeuge für Monitoring. Dies betrifft sowohl allgemeine Werkzeuge, wie beispielsweise Prometheus & Grafana, als auch ML-spezifische wie beispielsweise MLflow.

LZ 5-20: Nutzer-Feedback für das weitere Modelltraining

Die Teilnehmer:innen verstehen den Nutzen von Nutzer-Feedback für das weitere Modelltraining.

LZ 5-21: Methoden und Werkzeuge zur Sammlung von Nutzer-Feedback

Die Teilnehmer:innen kennen verschiedene Methoden und Werkzeuge zur Sammlung von Nutzer-Feedback, wie beispielsweise Auswahl zwischen mehreren Antworten und Flagging in Gradio.

LZ 5-22: Methoden zur Nutzung von Feedback für das Modell-Training

Die Teilnehmer:innen kennen verschiedene Methoden zur Nutzung von Feedback für das Modell-Training, wie beispielsweise RLHF, RLAIF und DPO.

LZ 5-23: [OPTIONAL] MLOps-Pipeline an einem Praxisbeispiel

Die Teilnehmer:innen erfahren anhand eines Praxisbeispiels, wie eine MLOps-Pipeline aussehen kann und welche Einsichten diese auf die Parameter, Metriken usw. bietet.

LZ 5-24: [OPTIONAL] Treffen von Build vs. Buy Entscheidungen für MLOps Systeme/Komponenten

Die Teilnehmer:innen sind in der Lage, Build vs. Buy Entscheidungen für MLOps Systeme/Komponenten zu treffen.

LZ 5-25: [OPTIONAL] MLOps-Werkzeuge und End-to-End Plattformen

Die Teilnehmer:innen kennen bekannte MLOps-Werkzeuge und End-to-End Plattformen, wie beispielsweise:
* Domino Data Lab, h2o.ai, DVC, activeloop, aporia, argo, arize, bentoml, comet ML, DagsHub, Databricks
MLOps Stacks, Feast, Kedro, Kubeflow, Metaflow, MLflow, MLRun, prefect, PrimeHub, Weights & Biases, WhyLabs, zenML, KNIME, RapidMiner, NVIDIA AI Enterprise, watsonx.ai * OpenSource: MLFlow, Weights & Biases, ClearML * PaaS: AWS SageMaker, Azure ML.

5.3. Referenzen

[Chen et al. 2022], [Treveil et al. 2020], [Haviv et al. 2023], [Osipov 2022], [Tan Wei Hao et al. 2024], [Wilson 2022], [Salama et al.], [Kumara et al.]

6. Systemarchitekturen und Plattformen für Generative KI-Systeme

Dauer: 160 Min.	Übungszeit: 30 Min.
-----------------	---------------------

6.1. Begriffe und Konzepte

Generative KI, LLMs, MLflow, Managed MLflow, Azure Machine Learning, Metaflow, Generative KI, LLM, (Stable) Diffusion, Vektor-DB, Embedding, RNN, Transformer, RAG, Agentic Workflows etc.

6.2. Lernziele

Die Teilnehmer:innen erreichen in diesem Kapitel die folgenden Lernziele:

LZ 6-1: Integrationsebenen von KI

Die Teilnehmer:innen kennen verschiedene Integrationsebenen von KI. Dazu gehören die folgenden Ebenen: * Anwendungen (z.B. Coding Assistenten) * AI-Engineering (z.B. Prompt Engineering) * ML-Modellentwicklung (z.B. pytorch) * ML-Infrastruktur (z.B. Vektor-DBs).

LZ 6-2: Bibliotheken, Schnittstellen und Tools zur Integration von KI-Modellen

Die Teilnehmer:innen kennen einige Beispiele von verbreiteten Bibliotheken, Schnittstellen und Tools zur Integration von KI-Modellen.

LZ 6-3: [OPTIONAL] Integration von KI-Systemen in die Gesamtarchitektur einer IT-Landschaft

Die Teilnehmer:innen können das strategische Design von DDD (insbesondere Context Maps) einsetzen, um die Art und den Grad der Integration von KI-Systemen zu bestimmen und zu dokumentieren.

LZ 6-4: Relevante Qualitätsmerkmale für KI-Systeme

Die Teilnehmer:innen verstehen die Qualitätsmerkmale, die für KI-Systeme besonders relevant sind. Dazu gehören insbesondere die folgenden Qualitätsmerkmale: * Verlässlichkeit * Skalierbarkeit * Effizienz * Sicherheit * Wartbarkeit * Interpretierbarkeit

LZ 6-5: [OPTIONAL] Evaluations-Frameworks für KI-Systeme

Die Teilnehmer:innen kennen gängige Evaluations-Frameworks, wie beispielsweise LangSmith oder LangFuse, um mit Unbestimmtheit und Fehlern in KI-Systemen umzugehen.

LZ 6-6: [OPTIONAL] Diskussion eines Fallbeispiels mit einer ausgedachten Fachlichkeit

Die Teilnehmer:innen üben und diskutieren anhand eines Fallbeispiels mit einer ausgedachten Fachlichkeit, Integrationsoptionen für KI in eine bestehende Software-Landschaft abzuwägen.

LZ 6-7: Verständnis von generativer KI

Die Teilnehmer:innen haben ein grundlegendes Verständnis von generativer KI wie beispielsweise LLMs und Stable Diffusion.

LZ 6-8: Funktionsweise von LLMs

Die Teilnehmer:innen verstehen die Funktionsweise von LLMs und können die zugehörige Begriffswelteinordnen: Token, Embedding, RNN, Transformer, Attention.

LZ 6-9: Bekannte Patterns bei der Nutzung von LLMs

Die Teilnehmer:innen kennen bekannte Patterns bei der Nutzung von LLMs. Dies umfasst die folgenden Patterns: * RAG und Retrieval-Strategien * Function Calling * Finetuning * Assistenten * Agenten

LZ 6-10: Use-Cases für RAG (Retrieval-Augmented Generation)

Die Teilnehmer:innen kennen typische Use-Cases für RAG wie beispielsweise „Talk to your documents/database/API“.

LZ 6-11: RAG-Techniken

Die Teilnehmer:innen kennen eine Auswahl der folgenden RAG-Techniken:

- Simple RAG
- Context Enrichment Techniques
- Multi-faceted Filtering
- Fusion Retrieval
- Intelligent Reranking
- Query Transformations
- Hierarchical Indices
- Hypothetical Questions
- Dynamic Chunk Sizing
- Semantic Chunking
- Contextual Compression
- Explainable Retrieval
- Retrieval with Feedback Loops
- Adaptive Retrieval
- Iterative Retrieval
- Ensemble Retrieval
- Knowledge Graph Integration
- Multi-modal Retrieval
- RAPTOR: Recursive Abstractive Processing for Tree-Organized Retrieval

LZ 6-12: Arten von Prompt Engineering

Die Teilnehmer:innen kennen verschiedene Arten von Prompt Engineering, wie beispielsweise * Few-Shot-Learning * Chain-of-Thought * Role-Playing

sowie allgemeine Best Practices für das Prompting.

LZ 6-13: Agentic Workflows

Die Teilnehmer:innen wissen, was Agentic Workflows sind und kennen die Begriffe Reflexion, Werkzeug-Nutzung, Planung und Multi-Agenten-Kollaboration.

LZ 6-14: Design Patterns für Generative AI-Systeme

Die Teilnehmer:innen wissen welche Design Patterns für Generative AI-Systeme existieren. Sie kennen eine Auswahl der folgenden Patterns:

- AI Query Router [Simple Router; Ranking-based Router; Learning-based Router]
- Layered Caching Strategy Leading to Fine-Tuning
- Multiplexing AI Agents
- Fine-Tuning LLMs for Multiple Tasks
- Blending Rules-Based and Generative Approaches
- Utilizing Knowledge Graphs with LLMs
- Swarm of Generative AI Agents
- Modular Monolith LLM Approach with Composability
- Memory Cognition for LLMs
- Red and Blue Team Dual-Model Evaluation

LZ 6-15: Techniken zur Evaluation von LLM-Anwendungen

Die Teilnehmer:innen kennen mehrere Techniken zur Evaluation von LLM-Anwendungen. Dies können beispielsweise die folgenden Techniken sein:

- Scoring
- Human Feedback
- Comparative Evaluation
- Model Based Evaluation

LZ 6-16: Bekannte LLMs und Auswahlkriterien

Die Teilnehmer:innen kennen bekannte LLMs, wie beispielsweise GPT, Claude, Gemini, Llama, Mistral oder Luminous, und Auswahlkriterien für ein geeignetes LLM.

LZ 6-17: Bedeutung von Cost Management für GenAI Applikationen

Die Teilnehmer:innen verstehen die Bedeutung von Cost Management für GenAI Applikationen.

LZ 6-18: Beispiele von verbreiteten Bibliotheken, Schnittstellen und Tools im Zusammenhang mit LLM-Anwendungen

Die Teilnehmer:innen kennen einige Beispiele von verbreiteten Bibliotheken, Schnittstellen und Tools im Zusammenhang mit LLM-Anwendungen, wie beispielsweise OpenAI-API oder LangChain.

LZ 6-19: [OPTIONAL] Agentic AI Software Architekturen, AI Agent Architekturkomponenten, Typen vom AI Agentarchitekturen

Die Teilnehmer:innen kennen Agentic AI Software Architekturen, AI Agent Architekturkomponenten, Typen vom AI Agentarchitekturen.

6.3. Referenzen

[Koc], [Dibia 2025], [Gradient Flow], [bornstein-radovanic], [Bahree 2024], [Spirin et al.], [Foster 2023], [Parnin]

7. Fallstudien und Praxisprojekte

Dauer: 110 Min.	Übungszeit: 110 Min.
-----------------	----------------------

7.1. Lernziele

Die Teilnehmer:Innen ...

LZ 7-1: Üben anhand von Fallstudien und Praxisprojekten, das erworbene Wissen in realen Szenarien anzuwenden.

Referenzen

Dieser Abschnitt enthält Quellenangaben, die ganz oder teilweise im Curriculum referenziert werden.

A

- [Agrawal et al.] A. Agrawal, J. Gans, A. Goldfarb: Prediction Machines: The Simple Economics of Artificial Intelligence <https://www.predictionmachines.ai/>
- [Alake] R. Alake: ML Pipeline Architecture Design Patterns (With 10 Real-World Examples) <https://neptune.ai/blog/ml-pipeline-architecture-design-patterns>
- [ATLAS] ATLAS - Adversarial Threat Landscape for Artificial-Intelligence Systems. <https://github.com/mitre/advmthreatmatrix>

B

- [Bahree 2024] Bahree, A.: Generative AI in Action <https://www.manning.com/books/generative-ai-in-action>
- [Bhajaria 2022] N. Bhajaria: Data Privacy - A runbook for engineers <https://www.manning.com/books/data-privacy>
- [Bornstein et al.] M. Bornstein, J. Li, M. Casado: Emerging Architectures for Modern Data Infrastructure <https://a16z.com/emerging-architectures-for-modern-data-infrastructure/>
- [bornstein-radovanic] M. Bornstein and R. Radovanovic: Emerging Architectures for LLM Applications <https://a16z.com/emerging-architectures-for-llm-applications/>
- [Burkov 2019] Burkov, A.: The Hundred-Page Machine Learning Book <https://themlbook.com/>

C

- [Cdteliot] AI Agents: Understanding Their Impact and Functions <https://www.perplexity.ai/page/ai-agents-understanding-their-bL1Mg8FeStyUB4o9u3HT5Q>
- [Chen et al. 2022] C. Chen, N. R. Murphy, K. Parisa, D. Sculley, T. Underwood: Reliable Machine Learning <https://www.oreilly.com/library/view/reliable-machine-learning/9781098106218/>
- [Chong et al.] J. Chong, Y. C. Chang: How to Lead in Data Science <https://www.manning.com/books/how-to-lead-in-data-science>
- [Crowe et al. 2024] R. Crowe, H. Hapke, E. Caveness, D. Zhu: Machine Learning Production Systems <https://learning.oreilly.com/library/view/machine-learning-production/9781098156008/>
- [CSIRO et al. 2023] CSIRO, Q. Lu, J. Wittle, X. Xu, L. Xhu: Responsible AI: Best Practices for Creating Trustworthy AI Systems <https://www.oreilly.com/library/view/responsible-ai-best/9780138073947/>

D

- [Dehghani] Z. Dehghani: Data Mesh <https://learning.oreilly.com/library/view/data-mesh/9781492092384/>
- [Dell'Acqua 2022] Fabrizio Dell'Acqua et al.: Paper: "Navigating the Jagged Technological Frontier: Field Experimental Evidence of the Effects of AI on Knowledge Worker Productivity and Quality" https://www.hbs.edu/ris/Publication%20Files/24-013_d9b45b68-9e74-42d6-a1c6-c72fb70c7282.pdf
- [Dibia 2025] V. Dibia with C. Wang: Multi-Agent Systems with AutoGen <https://www.manning.com/>

[books/multi-agent-systems-with-autogen](#)

E

- [Engler et al.] M. Engler, N. Dhamani: Generative AI. Misuse and Adversarial Attacks. <https://learning.oreilly.com/library/view/introduction-to-generative/9781633437197/OEBPS/Text/05.html>
- [EU AI Act] EU AI Act <https://artificialintelligenceact.eu/de/ai-act-explorer/>

F

- [Ford et al.] N. Ford, M. Richards, P. Sadalage, Z. Dehghani Software Architecture: The Hard Parts. <https://learning.oreilly.com/library/view/software-architecture-the/9781492086888/>
- [Foster 2023] D. Foster: Generative Deep Learning, 2nd Edition <https://www.oreilly.com/library/view/generative-deep-learning/9781098134174/>

G

- [Géron 2022] Aurélien Géron: Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow <https://learning.oreilly.com/library/view/hands-on-machine-learning/9781098125967/>
- [Gradient Flow] LLM Routers Unpacked <https://gradientflow.com/llm-routers-unpacked/>

H

- [Hall et al. 2023] P. Hall, J. Curtis, P. Pandey: Machine Learning for High-Risk Applications <https://www.oreilly.com/library/view/machine-learning-for/9781098102425/>
- [Hall et al. 2023] P. Hall, J. Curtis, P. Pandey: Machine Learning for High-Risk Applications (Chapter 1 Chapter 1. Contemporary Machine Learning Risk Management <https://www.oreilly.com/library/view/machine-learning-for/9781098102425/ch01.html#:text=Contemporary%20Machine%20Learning%20Risk%20Management>)
- [Harvard et al. 2024] Harvard Business Review, E. Mollick, D. De Cremer, T. Neeley, P. Sinha: Generative AI: The Insights You Need. (Generative AI Use Cases) <https://learning.oreilly.com/library/view/generative-ai-the/9781647826406/>
- [Haviv et al. 2023] Y. Haviv, N. Gift: Implementing MLOps in the Enterprise <https://www.oreilly.com/library/view/implementing-mlops-in/9781098136574/>
- [Heiland et al. 2023] L. Heiland, M. Hauser, J. Bogner: Design Patterns for AI-based Systems: A Multivocal Literature Review and Pattern Repository. 2023 IEEE/ACM 2nd International Conference on AI Engineering–Software Engineering for AI (CAIN). IEEE, 2023.
- [Hotz] N. Hotz: 15 Data Science Documentation Best Practices <https://www.datascience-pm.com/documentation-best-practices/>
- [Hotz] N. Hotz: What is a Data Science Life Cycle? <https://www.datascience-pm.com/data-science-life-cycle/>
- [Hotz] N. Hotz: What is TDSP <https://www.datascience-pm.com/tdsp/>
- [Huyen 2022] C. Huyen: Designing Machine Learning Systems <https://www.oreilly.com/library/view/designing-machine-learning/9781098107956/>

J

- [Jarmul 2023] K. Jarmul: Practical Data Privacy <https://www.oreilly.com/library/view/practical-data-privacy/9781098129453/>
- [Jones] A. Jones: Driving Data Quality with Data Contracts <https://learning.oreilly.com/library/view/driving-data-quality/9781837635009/>

K

- [Kelleher 2015] John D. Kelleher, Brian Mac Namee, and Aoife D'Arcy: Fundamentals of Machine Learning for Predictive Data Analytics <https://mitpress.mit.edu/9780262029445/fundamentals-of-machine-learning-for-predictive-data-analytics>
- [Koc] V. Koc: Generative AI Design Patterns: A Comprehensive Guide <https://towardsdatascience.com/generative-ai-design-patterns-a-comprehensive-guide-41425a40d7d0>
- [Kumara et al.] I. Kumara, R., D. Di Nucci, W. J. Van Den Heuvel, D. A. Tamburri: Requirements and Reference Architecture for MLOps: Insights from Industry <https://www.techrxiv.org/doi/full/10.36227/techrxiv.21397413.v1>

L

- [Lakshmanan et al.] V. Lakshmanan, S Robinson, M. Munn: Machine Learning Design Patterns <https://learning.oreilly.com/library/view/machine-learning-design/9781098115777/>
- [Lakshmanan et al.] V. Lakshmanan, S Robinson, M. Munn: Machine Learning Design Patterns Chapter 4 <https://www.oreilly.com/library/view/machine-learning-design/9781098115777/ch04.html>
- [Lakshmanan et al.] V. Lakshmanan, S Robinson, M. Munn: Machine Learning Design Patterns Chapter 5 <https://www.oreilly.com/library/view/machine-learning-design/9781098115777/ch05.html>

M

- [Masood et al. 2023] A. Masood, H. Dawe: Responsible AI in the Enterprise <https://www.oreilly.com/library/view/responsible-ai-in/9781803230528/>
- [ML software architecture] ML software architecture <https://appliedaiinitiative.notion.site/ML-software-architecture-790b9f5fcfcf408884287acb82f4d75e>
- [Molnar 2024] C. Molnar: Interpretable Machine Learning, 2nd ed. <https://christophm.github.io/interpretable-ml-book/>

N

- [Nahar et al.] N. Nahar, et al.: A meta-summary of challenges in building products with ml components—collecting experiences from 4758+ practitioners. 2023 IEEE/ACM 2nd International Conference on AI Engineering—Software Engineering for AI (CAIN). IEEE, 2023.
- [NirDiamant] RAG Techniques https://github.com/NirDiamant/RAG_Techniques
- [Nist] NIST AI Risk Management Framework. <https://www.nist.gov/itl/ai-risk-management-framework>

O

- [Osipov 2022] C. Osipov: MLOps Engineering at Scale <https://www.manning.com/books/mlops-engineering-at-scale>

P

- [Parnin] Building Your Own Product Copilot: Challenges, Opportunities, and Needs <https://arxiv.org/pdf/2312.14231v1>
- [Pruksachatkun et al. 2023] Y. Pruksachatkun, M. Mcateer, S. Majudmar: Practicing Trustworthy Machine Learning <https://www.oreilly.com/library/view/practicing-trustworthy-machine/9781098120269/>

R

- [Reis et al.] J. Reis, M. Housley: Fundamentals of Data Engineering <https://learning.oreilly.com/library/view/fundamentals-of-data/9781098108298/>
- [Roser 2022] Roser, Max: Brief History of AI: <https://ourworldindata.org/brief-history-of-ai>

S

- [Salama et al.] K. Salama, J. Kazmierczak, D. Schut: Practitioners guide to MLOps: A framework for continuous delivery and automation of machine learning. https://services.google.com/fh/files/misc/practitioners_guide_to_mlops_whitepaper.pdf
- [Saltz] J. Saltz: The GenAI Life Cycle <https://www.datascience-pm.com/the-genai-life-cycle/>
- [Sanderson et al.] C. Sanderson, M. Freeman: Data Contracts <https://learning.oreilly.com/library/view/data-contracts/9781098157623/>
- [Sarkis] A. Sarkis: Training Data for Machine Learning <https://learning.oreilly.com/library/view/training-data-for/9781492094517/>
- [Savarese] S. Savarese: How AI Agents Will Revolutionize the AI Enterprise <https://blog.salesforceairesearch.com/how-ai-agents-will-revolutionize-the-ai-enterprise/>
- [Serban] A. Serban, J. Visser: "Adapting software architectures to machine learning challenges." 2022 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER). IEEE, 2022.
- [Serra] J. Serra: Deciphering Data Architectures <https://learning.oreilly.com/library/view/deciphering-data-architectures/9781098150754/>
- [Spirin et al.] N. Spirin, M. Balint: Mastering LLM Techniques: LLMops <https://developer.nvidia.com/blog/mastering-llm-techniques-llmops/>
- [Studer et al.] S. Studer et al.: Towards CRISP-ML(Q): A Machine Learning Process Model with Quality Assurance Methodology <https://arxiv.org/abs/2003.05155>

T

- [Tan et al.] D. Tan, A. Leung, D. Colls: Effective Machine Learning Teams <https://learning.oreilly.com/library/view/effective-machine-learning/9781098144623/>
- [Tan Wei Hao et al. 2024] B. Tan Wei Hao, S. Padmanabhan, V. Mallya: Design a Machine Learning System (From Scratch) <https://www.manning.com/books/design-a-machine-learning-system-design-from-scratch>
- [tdcox] MLOps Roadmap 2024 - DRAFT <https://github.com/cdfoundation/sig-mlops/blob/main/roadmap/2024/MLOpsRoadmap2024.md>
- [Treveil et al. 2020] M. Treveil, N. Omont, C. Stenac, K. Lefevre, D. Phan, J. Zentici, A. Lavoillotte, M.

Miyazaki, L. Heidmann: Introducing MLOps <https://www.oreilly.com/library/view/introducing-mlops/9781492083283/>

- [TU Berlin] Architecture of Machine Learning Systems (TU Berlin, SS 2024): https://mboehm7.github.io/teaching/ss24_aml/index.htm

V

- [Vaughan 2020] Vaughan, D.: Analytical Skills for AI and Data Science (AI Use Cases) <https://learning.oreilly.com/library/view/analytical-skills-for/9781492060932/>
- [Visengeriyeva] Visengeriyeva, L.: Defining Jagged Technological Frontier: <https://www.perplexity.ai/page/defining-jagged-technological-iF8sDPVFQEKsdd2oyytztA>
- [Visengeriyeva] Visengeriyeva, L.: The Productivity J-Curve of AI: <https://www.perplexity>
- [Visengeriyeva] Visengeriyeva, L.: AI Agents vs. Traditional Models https://www.perplexity.ai/page/ai-agents-vs-traditional-model-JFf4gKT0RySW_Ehvbxbho2g
- [Visengeriyeva] Model Governance, Ethics, Responsible AI (Linksammlung) <https://github.com/visenger/Awesome-ML-Model-Governance>

W

- [Wang et al. 2024] C. Wang et al.: Quality Assurance for Artificial Intelligence: A Study of Industrial Concerns, Challenges and Best Practices <https://arxiv.org/pdf/2402.16391>
- [Wilson 2022] B. Wilson: Machine Learning Engineering in Action <https://www.manning.com/books/machine-learning-engineering-in-action>

Z

- [Zaharia et al.] M. Zaharia et al.: The Shift from Models to Compound AI Systems <https://bair.berkeley.edu/blog/2024/02/18/compound-ai-systems/>