Familienname, Vorname: _____

Firmenadresse: _____

_____

_____

Telefon: _____

Fax: _____

E-Mail-Adresse: _____

Rechnungsanschrift: _____

_____

_____

Schulungsunternehmen: _____

Referent: _____

Specialist KI Test – Probeprüfung

SET A (Version 2.2 D) – GTB Edition – ANTWORTEN

CT-AI-Lehrplan Version 2.0 D

ISTQB® Certified Tester Specialist KI Test (CT-AI)

Urheberrechtshinweis

Urheberrechtshinweis © International Software Testing Qualifications Board (im Folgenden als ISTQB® bezeichnet).

ISTQB® ist eine eingetragene Marke des International Software Testing Qualifications Board.

Alle Rechte vorbehalten.

Die Autoren übertragen hiermit das Urheberrecht an das ISTQB®. Die Autoren (als derzeitige Urheberrechtsinhaber) und das ISTQB® (als künftiger Urheberrechtsinhaber) haben sich auf die folgenden Nutzungsbedingungen geeinigt:

- Auszüge aus diesem Dokument dürfen für nichtkommerzielle Zwecke kopiert werden, sofern die Quelle angegeben wird.
- Jeder akkreditierte Schulungsanbieter darf diese Probeprüfung in seinen Schulungskursen verwenden, sofern die Autoren und das ISTQB® als Quelle und Urheberrechtsinhaber der Probeprüfung genannt werden und vorausgesetzt, dass jegliche Werbung für einen solchen Schulungskurs erst nach Erhalt der offiziellen Akkreditierung der Schulungsunterlagen durch ein vom ISTQB® anerkanntes nationales Mitglieds-Board erfolgt.
- Jede Einzelperson oder Gruppe von Personen darf diese Probeprüfung in Artikeln und Büchern verwenden, sofern die Autoren und das ISTQB® als Quelle und Urheberrechtsinhaber der Probeprüfung genannt werden.
- Jede andere Verwendung dieser Probeprüfung ist ohne vorherige schriftliche Genehmigung des ISTQB® untersagt.
- Jedes vom ISTQB® anerkannte nationale Mitglieds-Board darf diese Probeprüfung übersetzen, sofern es den oben genannten Urheberrechtshinweis in der übersetzten Version der Probeprüfung wiedergibt.

Verantwortung für das Dokument

Die Exam Working Group des ISTQB® ist für dieses Dokument verantwortlich.

Das Dokument wird von einem Kernteam des ISTQB® gepflegt, das sich aus der Exam Working Group und der Syllabus Working Group des ISTQB® zusammensetzt.

Danksagungen

Dieses Dokument wurde von einem Kernteam des ISTQB® erstellt: Klaudia Dussa-Zieger, Stuart Reid, Vipul Koch, Kyle Siemens, Qin Liu, Werner Henschelchen, Jarosław Hryszko

Das Kernteam dankt dem Review-Team der Exam Working Group und der Syllabus Working Group des ISTQB® sowie den nationalen Mitglieds-Boards für ihre Vorschläge und Beiträge.

Revisionsverlauf

Probeprüfung – Antworten, verwendete Vorlage: Version 2.12 Datum: 09.11.2026

Version	Datum	Anmerkungen
1.0	01.10.2021	Veröffentlichung für den allgemeinen Einsatz
2.0 Beta	05.01.2026	Beta-Review
2.0	17.04.2026	Veröffentlichung der allgemeinen Version

Versionsverlauf der deutschsprachigen Version

Probeprüfung – Antworten, verwendete Vorlage: Version 2.0 Datum: 27.11.2026

Version	Datum	Anmerkungen
2.0 D Alpha	17.08.2026	Alpha-Review
2.0 D	12.11.2026	Veröffentlichung

Inhalt

Urheberrechtshinweis 2
Verantwortung für das Dokument 2
Revisionsverlauf 3
Versionsverlauf der deutschsprachigen Version 3
Inhalt 4
Einführung 5
Lösungsschlüssel 6
Lösungsschlüssel der Zusatzfragen 6
Frage 1 7
Frage 2 8
Frage 3 9
Frage 4 10
Frage 5 11
Frage 6 12
Frage 7 13
Frage 8 15
Frage 9 16
Frage 10 17
Frage 11 19
Frage 12 20
Frage 13 21
Frage 14 22
Frage 15 23
Frage 16 24
Frage 17 25
Frage 18 26
Frage 20 28
Frage 21 29
Frage 22 30
Frage 24 32
Frage 25 33
Frage 26 34
Frage 27 35
Frage 28 36
Frage 29 37
Frage 30 38
Frage 31 39
Frage 32 40
Frage 33 42
Frage 34 43
Frage 35 45
Frage 36 46
Frage 37 47
Frage 38 48
Frage 39 49
Frage 40 50
Anhang: Zusätzliche Fragen 51
Frage A1 51
Frage A2 53
Frage A3 54
Frage A4 55
Frage A5 56
Frage A6 58

Einführung

Dies ist eine Probeprüfung. Sie hilft den Kandidaten bei ihrer Vorbereitung auf die Zertifizierungsprüfung. Enthalten sind Fragen, deren Format der regulären ISTQB®/ GTB-Prüfung Certified Tester Specialist KI Test (CT-AI) ähnelt. Es ist strengstens verboten, diese Prüfungsfragen in einer echten Prüfung zu verwenden.

1. Jede Einzelperson und jeder Schulungsanbieter kann diese Probeprüfung in einer Schulung verwenden, wenn ISTQB® als Quelle und Copyright-Inhaber der Probeprüfung anerkannt wird.
2. Jede Einzelperson oder Gruppe von Personen kann diese Probeprüfung als Grundlage für Artikel, Bücher oder andere abgeleitete Schriftstücke verwenden, wenn ISTQB® als Quelle und Copyright-Inhaber der Probeprüfung bestätigt wird.
3. Jedes vom ISTQB® anerkannte nationale Board kann diese Probeprüfung übersetzen und öffentlich zugänglich machen, wenn ISTQB® als Quelle und Copyright-Inhaber der Probeprüfung bestätigt wird.
4. Bei Fragen mit Einfachauswahl ist genau eine Antwort korrekt. Fragen mit Mehrfachauswahl oder Zuordnungsaufgaben sind entsprechend gekennzeichnet

Feedback zur vorliegenden Probeprüfung als Ganzes (40 + 6 Fragen) oder zu einzelnen Fragen wurden in den deutschsprachigen Alpha-Versionen des SET A im Zeitraum Oktober - November 2026 abgegeben von: Martin Klonk, Robert Pucher, Horst Pohlmann, Mario Winter.

Lösungsschlüssel

Fragenummer (#)	Richtige Antwort	LO	K-Stufe	Punkte		Fragenummer (#)	Richtige Antwort	Lernziel	K-Stufe	Punkte
1	a	AI-1.1.1	K2	1		21	d	AI-4.2.2	K3	2
2	c, e	AI-1.1.2	K2	1		22	b	AI-4.3.1	K2	1
3	a	AI-1.1.3	K2	1		23	a	AI-4.3.2	K2	1
4	b	AI-1.1.4	K2	1		24	a	AI-5.1.1	K2	1
5	a	AI-1.1.5	K2	1		25	c	AI-5.1.2	K2	1
6	b	AI-1.1.6	K2	1		26	d	AI-5.1.3	K2	1
7	c	AI-2.1.1	K2	1		27	b	AI-5.1.4	K2	1
8	b	AI-2.1.2	K2	1		28	c	AI-5.1.5	K3	2
9	c	AI-2.2.1	K2	1		29	b	AI-5.1.6	K2	1
10	c	AI-3.1.1	K2	1		30	b	AI-6.1.1	K2	1
11	d	AI-3.1.2	K2	1		31	a	AI-6.1.2	K2	1
12	d	AI-3.1.4	K2	1		32	a	AI-6.1.3	K2	1
13	c	AI-3.2.1	K2	1		33	c	AI-6.1.4	K2	1
14	b	AI-3.2.3	K2	1		34	b	AI-6.1.5	K3	2
15	c	AI-3.3.1	K3	2		35	b	AI-6.1.7	K2	1
16	a	AI-3.4.1	K2	1		36	c	AI-6.1.8	K2	1
17	a	AI-4.1.1	K2	1		37	c	AI-6.1.9	K2	1
18	b	AI-4.1.2	K2	1		38	d	AI-6.1.10	K2	1
19	b	AI-4.1.3	K2	1		39	b, d	AI-7.1.1	K2	1
20	b	AI-4.2.1	K2	1		40	b	AI-7.1.2	K2	1

Lösungsschlüssel der Zusatzfragen

Fragenummer (#)	Korrekte Antwort	LO	K-Stufe	Punkte
A1	Neuer Fragetyp	AI-1.1.2	K2	1
A2	a	AI-1.1.7	K2	1
A3	c	AI-1.1.8	K2	1
A4	Neuer Fragetyp	AI-3.1.1	K2	1
A5	Neuer Fragetyp	AI-3.1.2	K2	1
A6	c	AI-3.4.3	K2	1

Frage 1	AI-1.1.1	K2	Punkte 1.0

Welche der folgenden Aussagen verdeutlicht am BESTEN den Unterschied zwischen konventionellen Systemen und KI-basierten Systemen?

Wählen Sie EINE Antwort aus!

a)	KI-basierte Systeme lernen in der Regel aus Mustern in den Daten und können sich an neue Szenarien anpassen, während konventionelle Systeme vordefinierten Regeln folgen und bei gleichen Eingaben konsistente Ergebnisse liefern	☒
b)	KI-basierte Systeme sind in der Regel schneller als konventionelle Systeme, da sie nicht auf expliziter Programmierung beruhen, während konventionelle Systeme aufgrund ihrer starren, regelbasierten Verarbeitung langsamer sind	☐
c)	KI-basierte Systeme sind in der Regel deterministisch und haben eine hohe Erklärbarkeit, während konventionelle Systeme probabilistisch sind und oft eine geringe Interpretierbarkeit haben	☐
d)	KI-basierte Systeme eignen sich in der Regel besser für kritische Aufgaben, bei denen Erklärbarkeit entscheidend ist, während konventionelle Systeme komplexe Aufgaben in unregulierten Branchen besser bewältigen können	☐

Begründung

KORREKT — Dies unterscheidet KI-basierte Systeme korrekt von konventionellen Systemen. KI-basierte/ML-Systeme lernen Muster in den Daten und viele können sich durch Selbstlernen anpassen, während konventionelle Systeme vordefinierte Logik verwenden und vorhersehbare Ergebnisse liefern.
Hinweis: Dies gilt nicht für regelbasierte Expertensysteme.

FALSCH — Zwar können KI-basierte Systeme Daten manchmal schneller verarbeiten, doch ist dies nicht immer der Fall, und ihr Vorteil liegt eher in der Anpassbarkeit und der Bewältigung von Komplexität als in der Geschwindigkeit.

FALSCH — Hier werden die Eigenschaften der beiden Systemtypen vertauscht. Viele KI-basierte Systeme sind probabilistisch und haben eine geringere Erklärbarkeit, während konventionelle Systeme deterministisch und einfacher zu interpretieren sind.

FALSCH — Konventionelle Systeme eignen sich besser für kritische Aufgaben, bei denen die Erklärbarkeit der Ergebnisse wichtig ist; KI-basierte Systeme weisen in der Regel eine geringe Transparenz und Erklärbarkeit auf und sind daher eher für den Einsatz in unregulierten Bereichen geeignet. Außerdem sind KI-basierte Systeme oft besser für komplexere Probleme geeignet.

Frage 2	AI-1.1.2	K2	Punkte 1.0

Welche ZWEI der folgenden Aussagen unterscheiden am BESTEN zwischen schwacher KI, allgemeiner KI und Super-KI?

Wählen Sie ZWEI Antworten aus!

a)	Schwache KI ist selbstlernend, allgemeine KI konzentriert sich auf die Lösung spezialisierter Probleme und Super-KI ist auf Aufgaben beschränkt, die während ihrer Entwicklung definiert wurden	☐
b)	Schwache KI arbeitet unabhängig von menschlichen Eingaben, allgemeine KI wird nur in der fortgeschrittenen Robotik eingesetzt, und Super-KI verbessert die menschliche Entscheidungsfindung in spezialisierten Bereichen	☐
c)	Schwache KI führt bestimmte Aufgaben effizient aus, allgemeine KI kann wie ein Mensch ein breites Spektrum an intellektuellen Aufgaben bewältigen, und Super-KI übertrifft die menschliche Intelligenz	☒
d)	Schwache KI ist auf bestimmte Aufgaben beschränkt, allgemeine KI ist ein Konzept mit eher wenigen praxisrelevanten Anwendungsmöglichkeiten, und Super-KI beschreibt modernste generative KI-Modelle	☐
e)	Schwache KI entspricht dem aktuellen Stand der KI; die Verwirklichung allgemeiner KI ist ungewiss, doch sobald allgemeine KI erreicht ist, könnte Super-KI eventuell folgen	☒

Begründung

a) FALSCH — Schwache KI ist nicht in allen Fällen selbstlernend; sie ist auf bestimmte Aufgaben beschränkt. Allgemeine KI ist nicht auf spezielle Probleme beschränkt, und Super-KI ist nicht auf vordefinierte Aufgaben beschränkt.

b) FALSCH — Schwache KI funktioniert nicht unabhängig von menschlichen Eingaben, allgemeine KI ist nicht ausschließlich auf die Robotik beschränkt, und Super-KI verbessert nicht lediglich die menschliche Entscheidungsfindung, sondern übertrifft hypothetisch die menschliche Intelligenz vollständig.

c) KORREKT — Dies unterscheidet die drei Arten von KI zutreffend und hebt den aufgabenspezifischen Charakter der schwachen KI, die menschenähnliche Vielseitigkeit der allgemeinen KI sowie den hypothetischen Charakter und die überlegenen Fähigkeiten der Super-KI hervor.

d) FALSCH — Während schwache KI zu Recht als aufgabenbezogen identifiziert wird, hätte allgemeine KI, sofern sie erreicht würde, viele Anwendungsmöglichkeiten in der realen Welt. Zudem ist unklar, in welcher Beziehung Super-KI zu Generativen KI-Modellen stünde.

e) KORREKT — Die gesamte heutige KI ist schwache KI. Wann allgemeine KI erreicht wird, ist unklar. Sobald wir über allgemeine KI verfügen, ist es angesichts der Verfügbarkeit von Wissen im Internet möglich, dass auch Super-KI erreicht wird.

Frage 3	AI-1.1.3	K2	Punkte 1.0

Welche der folgenden Aussagen beschreibt die Beziehung zwischen den Begriffen Künstliche Intelligenz (KI), Maschinelles Lernen (ML) und Deep Learning (DL) am BESTEN?

Wählen Sie EINE Antwort aus!

a)	ML ist ein Kernzweig der KI, und DL ist eine Untergruppe von ML, was eine Hierarchie spezialisierter Technologien darstellt	☒
b)	DL ist die grundlegende Technologie, und sowohl ML als auch KI sind spezialisierte Anwendungen, die auf dessen Prinzipien aufbauen	☐
c)	DL und ML sind im Wesentlichen austauschbare Begriffe, während KI einen eigenständigen Ansatz zur Problemlösung darstellt	☐
d)	KI umfasst sowohl ML als auch DL als unterschiedliche, aber wichtige Methoden, die parallel zur Lösung komplexer Probleme eingesetzt werden	☐

Begründung

a) KORREKT — KI ist der umfassendste Begriff. Er bezieht sich auf das allgemeine Konzept der Entwicklung von Maschinen, die Aufgaben ausführen können, für die normalerweise menschliche Intelligenz erforderlich ist. Dies umfasst eine breite Palette von Ansätzen und Techniken, nicht nur maschinelles Lernen. ML ist eine Untergruppe der KI. Es handelt sich um einen spezifischen Ansatz zur Realisierung von KI, bei dem Maschinen die Fähigkeit erhalten, aus Daten zu lernen, ohne explizit programmiert zu werden. Anstatt für jede Situation spezifische Regeln zu schreiben, lernen ML-Algorithmen Muster und treffen auf der Grundlage der Daten Vorhersagen. DL ist eine Untergruppe des maschinellen Lernens. Es handelt sich um eine spezialisierte Form des maschinellen Lernens, die künstliche neuronale Netze mit mehreren Schichten nutzt, daher Deep Learning (*deep learning*).

b) FALSCH — KI und ML existierten bereits als Konzepte und Forschungsgebiete, lange bevor DL an Bedeutung gewann. DL ist eine relativ neue Entwicklung innerhalb der breiter gefassten Bereiche des maschinellen Lernens und der KI.

c) FALSCH — DL und ML sind nicht austauschbar. DL ist eine spezifische Form von ML. Außerdem stellt KI keinen „separaten Ansatz“ dar – ML und DL sind Ansätze zur Umsetzung von KI.

d) FALSCH — Zwar umfasst KI sowohl ML als auch DL, doch „parallel arbeiten“ ist keine zutreffende Beschreibung ihrer Beziehung. DL ist eine Form von ML, keine parallele Methodik auf derselben Ebene, die parallel ausgeführt werden kann.

Frage 4	AI-1.1.4	K2	Punkte 1.0

Welche der folgenden Aussagen erklärt generative KI am BESTEN?

Wählen Sie EINE Antwort aus!

a)	Sie ist darauf ausgelegt, vorhandene Daten wie Texte oder Bilder zu analysieren und zu verstehen, sodass Maschinen Informationen kategorisieren und wichtige Erkenntnisse gewinnen können	☐
b)	Sie erstellt neue Inhalte wie Texte, Bilder oder Audiodateien, indem sie Muster aus Trainingsdaten lernt und Ergebnisse ähnlicher Art generiert	☒
c)	Sie konzentriert sich hauptsächlich auf die Verbesserung bestehender Inhalte wie Text, Bilder oder Audio, indem sie diese für Aufgaben der Klassifikation oder Vorhersage optimiert	☐
d)	Sie erstellt Modelle, die auf die Generierung von Text und Bildern beschränkt sind und nicht für kreative Aufgaben wie die Wirkstoffforschung oder Datensimulationen verwendet werden können	☐

Begründung

a) FALSCH — Es beschreibt Analyse und Verständnis, was keine Fähigkeiten sind, die GenAI definieren, und konzentriert sich nicht auf den generativen Aspekt der Generativen KI.

b) KORREKT — Dies beschreibt Generative KI zutreffend und hebt ihre Fähigkeit hervor, auf der Grundlage gelernter Muster in Trainingsdaten neue Inhalte zu erstellen.

c) FALSCH — Generative KI konzentriert sich auf die Erstellung neuer Inhalte und nicht auf die Verbesserung bestehender Inhalte als Vorstufe zu traditionelleren KI-Aufgaben wie Klassifikation- und Vorhersageaufgaben.

d) FALSCH — Generative KI ist nicht auf Text und Bilder beschränkt; sie findet Anwendung im Gesundheitswesen, in der Arzneimittelforschung, bei Datensimulationen und in anderen Bereichen.

Frage 5	AI-1.1.5	K2	Punkte 1.0

Welche der folgenden Aussagen vergleicht die für die Implementierung von Systemen für maschinelles Lernen verfügbaren Arten von Hardware am BESTEN?

Wählen Sie EINE Antwort aus

a)	GPUs eignen sich aufgrund ihrer Fähigkeit zur massiv-parallelen Verarbeitung gut für das Training und die Ausführung von ML-Modellen, während CPUs besser für allgemeine Rechenaufgaben geeignet sind	☒
b)	CPUs sind bei ML-Aufgaben effizienter als GPUs, da sie höhere Taktraten aufweisen und komplexe Operationen bewältigen können	☐
c)	KI-spezifische Hardware wie ASICs wird in erster Linie zum Training von ML-Modellen verwendet, während GPUs besser für Edge-Computing geeignet sind	☐
d)	Neuromorphe Prozessoren sind eine Form von KI-Hardware, die speziell für den Betrieb auf der Von-Neumann-Architektur optimiert ist	☐

Begründung

a) KORREKT — Dieser Vergleich verdeutlicht treffend die Vorteile von GPUs gegenüber CPUs beim maschinellen Lernen aufgrund ihrer Parallelverarbeitungsfähigkeiten, während CPUs bei allgemeinen Rechenaufgaben überlegen sind.

b) FALSCH — CPUs haben zwar höhere Taktraten, sind jedoch für ML-Aufgaben weniger effizient als GPUs, da sie den Anforderungen für Datenverarbeitungsaufgaben wie Matrixmultiplikation nicht die erforderlichen umfangreichen Parallelverarbeitungsfähigkeiten erfüllen.

c) FALSCH — KI-spezifische Hardware wie ASICs eignet sich besser für Edge-Computing als für das ML-Modelltraining, das in der Regel in der Cloud erfolgt.

d) FALSCH — Neuromorphe Prozessoren sind entworfen, um die Struktur des Gehirns nachzuahmen, und basieren nicht auf der Von-Neumann-Architektur; daher ist diese Aussage unzutreffend.

Frage 6	AI-1.1.6	K2	Punkte 1.0

Gegeben seien folgende Aussagen zur Entwicklung und zum Hosting von KI-Modellen:

i) Es senkt durch die Nutzung öffentlicher Cloud-Ressourcen die Entwicklungskosten, da die Notwendigkeit von Investitionen in lokale Hardware wegfällt

ii) Es nutzt die lokale Entwicklung für Komponenten zur Datenvorbereitung für sensible Daten, um die Sicherheit zu erhöhen, bevor das gesamte System zum Training in die Cloud verlagert wird

iii) Es führt zu geringeren Kosten, da Laptops für die lokale Entwicklung genutzt werden und durch das Hosting von KI-Modellen in öffentlichen Clouds nur geringe Vorabkosten für Hardware anfallen

iv) Es vereinfacht die Entwicklung und das Hosting, indem es die Prozesse auf lokalen Servern standardisiert und die Notwendigkeit komplexer cloudbasierter Konfigurationen beseitigt

v) Es garantiert höchste Sicherheit (*security*) durch das Hosting von KI-Modellen in privaten Clouds, wodurch die mit Sicherheitslücken lokaler Hardware verbundenen Risiken vermieden werden

Welche der folgenden Aussagen spiegelt die Vorteile eines hybriden Ansatzes für Entwicklung und Hosting von KI-Modellen am BESTEN wider?

Wählen Sie EINE Antwort aus!

a)	i, ii und v	☐
b)	ii und iii	☒
c)	iii und iv	☐
d)	i, iv und v	☐

Begründung

Gegeben seien folgende Aussagen zur Entwicklung und zum Hosting von KI-Modellen:

i) Es senkt durch die Nutzung öffentlicher Cloud-Ressourcen die Entwicklungskosten, da die Notwendigkeit von Investitionen in lokale Hardware wegfällt

• Dies ist kein hybrider Ansatz, da hier ausschließlich von der Entwicklung in der Cloud die Rede ist.

ii) Es nutzt die lokale Entwicklung für Komponenten zur Datenvorbereitung für sensible Daten, um die Sicherheit zu erhöhen, bevor das gesamte System zum Training in die Cloud verlagert wird

• Dies ist ein hybrider Ansatz, da die Datenvorbereitung lokal erfolgt und das Training in der Cloud stattfindet.

iii) Es führt zu geringeren Kosten, da Laptops für die lokale Entwicklung genutzt werden und durch das Hosting von KI-Modellen in öffentlichen Clouds nur geringe Vorabkosten für Hardware anfallen

• Dies ist ein hybrider Ansatz, da die Entwicklung lokal auf Laptops erfolgt und das Hosting in öffentlichen Clouds stattfindet

iv) Es vereinfacht die Entwicklung und das Hosting, indem es die Prozesse auf lokalen Servern standardisiert und die Notwendigkeit komplexer cloudbasierter Konfigurationen beseitigt

• Dies ist kein hybrider Ansatz, da sich alles auf lokalen Servern befindet.

v) Es garantiert höchste Sicherheit (*security*) durch das Hosting von KI-Modellen in privaten Clouds, wodurch die mit Sicherheitslücken lokaler Hardware verbundenen Risiken vermieden werden

• Dies ist kein hybrider Ansatz, da sich alles in privaten Clouds befindet.

Daher ist die richtige Antwort b) ii und iii.

Frage 7	**AI-2.1.1**	**K2**	**Punkte 1.0**

Gegeben seien die folgenden Qualitätsmerkmale gemäß ISO/IEC 25059:

1) KI-Robustheit

2) Kontrollierbarkeit durch Benutzer

3) Funktionale Anpassbarkeit

4) Eingreifbarkeit

und die folgenden Beispiele für Qualitätsmessungen:

A. Die Erfolgsquote, mit der ein Bediener mittels Fernsteuerung die Sicherheitslandung der Drohne auslösen kann, wenn deren KI-Navigationssystem gefährliches Verhalten zeigt

B. Die durchschnittlich benötigte Zeit, um die automatisierte Entscheidung eines Betrugsmanagementsystems zur Sperrung einer Kundentransaktion erfolgreich aufzuheben

C. Der F1-Wert eines Modells zur Objekterkennung in einem autonomen Fahrzeug bei starkem Regen

D. Die benötigte Zeit, bis eine E-Commerce-Empfehlungsmaschine ihre Vorschläge für einen neuen, schnell aufkommenden Modetrend aktualisiert hat

Welche der folgenden Optionen ordnet die Qualitätsmerkmale am BESTEN den Beispielen für Qualitätsmessungen zu?

Wählen Sie EINE Antwort aus!

a)	1D – 2A – 3C – 4B	☐
b)	1C – 2D – 3B – 4A	☐
c)	1C – 2B – 3D – 4A	☒
d)	1A – 2D – 3C – 4B	☐

Begründung
Betrachten wir die einzelnen Beispiele der Reihe nach:

A) *Die Erfolgsquote, mit der ein Bediener mittels Fernsteuerung die Sicherheitslandung der Drohne auslösen kann, wenn deren KI-Navigationssystem gefährliches Verhalten zeigt.* Diese Messung bewertet die Effektivität menschlicher Eingriffe in den Systembetrieb bei gefährlichem KI-Verhalten und steht im Einklang mit der Definition von Eingreifbarkeit: der Fähigkeit, externe Eingriffe in automatisierte Prozesse zuzulassen. Dies entspricht der Eingreifbarkeit (**4**).

B) *Die durchschnittlich benötigte Zeit, um die automatisierte Entscheidung eines Betrugsmanagementsystems zur Sperrung einer Kunden-Transaktion erfolgreich aufzuheben.* Diese Messung befasst sich damit, wie schnell ein Benutzer die Entscheidung eines automatisierten Systems außer Kraft setzen kann und inwieweit ein Benutzer die Aktionen des Systems steuern oder beeinflussen kann. Dies ist ein direkter Indikator für die Benutzerkontrollierbarkeit (**2**).

C) *Der F1-Wert eines Modells zur Objekterkennung in einem autonomen Fahrzeug bei starkem Regen.* Der F1-Wert unter widrigen Bedingungen (starker Regen) testet, wie gut das Modell in anspruchsvollen Szenarien funktioniert, was ein Maß für die KI-Robustheit ist (**1**).

D) *Die benötigte Zeit, bis eine E-Commerce-Empfehlungsmaschine ihre Vorschläge für einen neuen, schnell aufkommenden Modetrend aktualisiert hat*. Die Geschwindigkeit, mit der ein System seine Empfehlungen für neue Trends aktualisiert, spiegelt seine Fähigkeit wider, seine Funktionalität an sich ändernde Anforderungen anzupassen – dies ist die funktionale Anpassbarkeit (**3**).

In diesem Fall lautet die korrekte Kombination:
1C – 2B – 3D – 4A, womit c) KORREKT ist.

Frage 8	AI-2.1.2	K2	Punkte 1.0

Welche der folgenden Aussagen beschreibt am BESTEN eine zentrale Herausforderung beim Einsatz von KI in sicherheitsrelevanten Systemen?

Wählen Sie EINE Antwort aus!

a)	Wenn die Anforderungen zu detailliert sind, bleibt dem ML-System kaum Spielraum, um aus den in den Trainingsdaten enthaltenen impliziten Zielen zu lernen	☐
b)	Das Potenzial für Nichtdeterminismus und Selbstlernen macht manche KI-basierten Systeme unvorhersehbar, da sie von ihrem ursprünglich getesteten Zustand abweichen	☒
c)	Da selbstlernende sicherheitsrelevante Systeme nach der Bereitstellung nicht mehr anpassbar sind, wird die Sicherheit oft durch die Notwendigkeit manueller Aktualisierungen des im Betrieb befindlichen KI-basierten Systems beeinträchtigt	☐
d)	Die ausgereiften sicherheitsrelevanten Normen sind in der Regel veraltet und erfordern den Einsatz überholter KI-Technologien, was innovative KI-Lösungen in KI-basierten Systemen behindert	☐

Begründung

a) FALSCH — Das eigentliche Problem ist genau das Gegenteil: Anforderungen sind in der Regel zu vage und werden oft nur implizit durch Daten vorgegeben, was zu einer schlechten Verfolgbarkeit führt.

b) KORREKT — Diese Unvorhersehbarkeit stellt eine zentrale Herausforderung der Sicherheit (*safety*) bei der Bereitstellung von KI in sicherheitsrelevanten Systemen dar, da sie die Verifizierung, Validierung und die fortlaufende Gewährleistung eines sicheren Betriebs erschwert.

c) FALSCH — Das Problem besteht darin, dass selbstlernende Systeme auch nach der Bereitstellung weiter anpassen und sich somit von ihrem ursprünglich getesteten Verhalten entfernen.

d) FALSCH — Ausgereifte Normen für die Sicherheit enthalten derzeit keine Bestimmungen für KI, und einige schränken deren Einsatz ausdrücklich ein.

Frage 9	AI-2.2.1	K2	Punkte 1.0

Welches der folgenden Beispiele ist am WENIGSTEN geeignet, als gültiges Akzeptanzkriterium für KI-spezifische Qualitätsmerkmale zu dienen, die in der Norm ISO 25059 für ein KI-basiertes System definiert sind?

Wählen Sie EINE Antwort aus!

a)	Der Sicherheitsmitarbeiter im Kontrollraum des Museums kann einen sofortigen „Alles-Stop“-Befehl auslösen, der den Patrouillenroboter dazu veranlasst, alle Bewegungen innerhalb von 0,5 Sekunden einzustellen, um die Kollision mit einer Skulptur zu verhindern	☐
b)	Ein Gewächshaus-Steuerungssystem reagiert innerhalb von 20 Minuten, wenn die Messung der Luftfeuchtigkeit mehr als 10 % von der optimalen Luftfeuchtigkeit abweicht	☐
c)	Das Kontrollsystem für Spam-Warnungen lässt sich vom Benutzer leicht einrichten und erfordert nur minimale technische Kenntnisse für die Wartung	☒
d)	Wenn das Analyse-Tool einen Netzhautscan als Hinweis auf schwere diabetische Retinopathie kennzeichnet, muss es eine visuelle Überlagerung (*heatmap*) anzeigen, welche die relevantesten Merkmale hervorhebt	☐

Begründung

a) FALSCH — Dies bezieht sich auf die Eingreifbarkeit gemäß der Definition in ISO 25059, die die Fähigkeit des Benutzers beschreibt, den autonomen Patrouillenroboter zu steuern, wenn er bemerkt, dass dieser möglicherweise gegen eine Skulptur stoßen könnte. Außerdem wird ein spezifischer, messbarer Zeitrahmen für die Intervention angegeben.

b) FALSCH — Dies bezieht sich auf die funktionale Korrektheit, die in ISO 25059 definiert ist. Sie beschreibt, wie sich das System an Änderungen der Luftfeuchtigkeit anpasst, um das gewünschte Raumklima aufrechtzuerhalten. Sie legt einen konkreten, messbaren Luftfeuchtigkeitswert sowie einen Zeitrahmen fest, innerhalb dessen das Steuerungssystem reagieren muss.

c) KORREKT — Es ist die am WENIGSTEN wahrscheinliche Option, da sie sich auf einige der Untermerkmale der Gebrauchstauglichkeit konzentriert, wie z. B. Erlernbarkeit und Operabilität, bei denen es sich um allgemeine Qualitätsmerkmale handelt, die auf die meisten Systeme anwendbar sind und nicht direkt mit den KI-spezifischen Merkmalen in ISO 25059 in Verbindung stehen (d. h. Kontrollierbarkeit durch Benutzer durch und Transparenz, die Untermerkmale der Gebrauchstauglichkeit für KI-basierte Systeme sind). Das Akzeptanzkriterium ist zudem subjektiver als die anderen Optionen und daher schwieriger zu testen.

d) FALSCH — Dies bezieht sich auf die Transparenz, die in ISO 25059 definiert ist. Sie beschreibt die Bereitstellung zusätzlicher Informationen durch das System zur Erläuterung seiner Entscheidungsfindung.

Frage 10	AI-3.1.1	K2	Punkte 1.0

Gegeben seien die folgenden Ansätze des maschinellen Lernens:

1) Clusterbildung

2) Bestärkendes Lernen

3) Klassifikation

4) ML-Regression

Betrachten Sie dazu die folgenden Anwendungsbeispiele:

A) Die mobile Spiele-App passt ihr Feedback, die Reaktionszeiten und die Anzahl der angebotenen Benutzeroptionen daran an, wie viel die Spieler ausgeben

B) Die Sprachübersetzungs-App durchsucht das Internet nach Texten, die in verschiedenen Sprachen zur Verfügung stehen, um ihre Übersetzungsfunktion zu verbessern

C) Ein Fertigungsunternehmen prognostiziert anhand von Sensordaten und historischen Aufzeichnungen über die Wartung, wann Anlagen wahrscheinlich ausfallen werden

D) Eine Social-Media-Plattform gruppiert ihre Benutzer anhand ihrer Interaktionen untereinander und ihrer angegebenen Interessen in Communities

Welche der folgenden Aussagen ordnet die Ansätze des maschinellen Lernens am BESTEN den Beispiel-Anwendungen zu?
Wählen Sie EINE Antwort aus!

a)	1B – 2D – 3A – 4C	☐
b)	1C – 2A – 3D – 4B	☐
c)	1D – 2A – 3B – 4C	☒
d)	1D – 2C – 3B – 4A	☐

Begründung

Durch Betrachtung der Beschreibungen der Beispielsysteme ergeben sich folgende richtige Zuordnungen:

1) Clusterbildung – In (D) kann die Social-Media-Plattform durch die Analyse von Benutzerinteraktionen (z. B. Likes, Kommentare, geteilte Inhalte) und angegebenen Interessen Muster und Ähnlichkeiten unter den Benutzern erkennen. Diese Muster können dann verwendet werden, um Benutzer in Communities oder „Cluster“ zu gruppieren, die gemeinsame Interessen und Verhaltensweisen aufweisen.

2) Bestärkendes Lernen – In (A) kann der ausgegebene Betrag als Belohnungsfunktion für dieses System betrachtet werden, wobei das System sein Verhalten so anpasst, dass der ausgegebene Betrag steigt.

3) Klassifikation – In (B) nutzt die App Texte in einer Sprache, die als Ausgangssprache betrachtet werden kann, sowie entsprechende „korrekte“ Übersetzungen dieser Ausgangssprache und wendet dabei eine Form des überwachten Lernens an, ohne dass eine explizite Belohnungsfunktion erwähnt wird. Bei der Klassifikation werden parallele Trainingsdaten verwendet – Paare aus übereinstimmenden Sätzen in zwei Sprachen (z. B. „Hello“ auf Englisch und „Bonjour“ auf Französisch) –, wobei jedes Paar ein Kennzeichen aufweist, das den Ausgangs- mit dem Zieltext verknüpft. Das Modell lernt Zuordnungen durch überwachtes Lernen, indem es Merkmale des Eingabetextes kodiert und die korrekte Übersetzungsausgabe vorhersagt, wobei es Fehler über viele solcher Paare hinweg minimiert, um auf neue Sätze zu verallgemeinern.

4) ML-Regression - In (C) wird ein kontinuierliches Ergebnis (in diesem Fall die Zeit bis zum Ausfall einer Anlage) auf der Grundlage einer Reihe von Eingabevariablen (Sensordaten und historische Aufzeichnungen der Wartung) vorhergesagt. Durch die Analyse der Beziehung zwischen diesen Variablen kann das ML-Modell Muster und Trends identifizieren, die darauf hindeuten, wann bei einer Anlage das Risiko eines Ausfalls besteht.

Daher ist 1D – 2A – 3B – 4C richtig, und somit ist Option c) die richtige Antwort.

Frage 11	AI-3.1.2	K2	Punkte 1.0

Gegeben seien folgende Aktivitäten des ML-Workflows:

1) Bereitstellung des Modells

2) Vorbereitung und Test der Daten

3) Test des Modells

4) Evaluierung des Modells

Betrachten Sie dazu die folgenden Beschreibungen:

A) Die Leistung des Modells wird anhand von Validierungsdaten getestet

B) Die Herkunft der zum Testen des Modells verwendeten Testdaten wird ermittelt

C) Die Testdaten werden verwendet, um zu überprüfen, ob die vereinbarten Leistungskriterien von ML erfüllt sind

D) Das Modell wird auf der Zielplattform getestet

Welche der folgenden Optionen ordnet die Aktivitäten im ML-Workflow am BESTEN den Beschreibungen zu?

Wählen Sie EINE Antwort aus!

a)	1A – 2C – 3B – 4D	☐
b)	1C – 2D – 3B – 4A	☐
c)	1D – 2B – 3A – 4C	☐
d)	1D – 2B – 3C – 4A	☒

Begründung

1) Die Modellleistung wird anhand von Validierungsdaten getestet. Dies ist Teil der Aktivität „Evaluierung des Modells“. (D)

2) Die Herkunft der zum Testen des Modells verwendeten Testdaten wird ermittelt. Dies ist Teil der Aktivität „Vorbereitung und Test der Daten“. (B)

3) Anhand der Testdaten wird festgestellt, ob die vereinbarten Leistungskriterien von ML erfüllt sind. Dies ist Teil der Aktivität „Test des Modells“. (C)

4) Das Modell wird auf der Zielplattform getestet. Dies ist Teil der Aktivität „Bereitstellung des Modells“. (A)

Daher lautet die richtige Antwort: 1D – 2B – 3C – 4A, und somit ist d) richtig.

Frage 12	AI-3.1.4	K2	Punkte 1.0

Welche der folgenden Aussagen über die Verwendung vortrainierter Modelle ist RICHTIG?

Wählen Sie EINE Antwort aus!

a)	Bei der Anwendung auf ein neuronales Netz funktioniert die Retrieval-augmentierte Generierung (RAG) durch das Hinzufügen zusätzlicher Schichten, welche speziell auf den Prompt bezogene Dokumentation enthalten	☐
b)	Das Fein-Tuning eines verzerrten LLM mit aufgabenspezifischen Daten hoher Qualität verhindert unfaire Ergebnisse, die auf sensiblen Attributen basieren	☐
c)	Um ein vortrainiertes neuronales Netz erfolgreich anzupassen, erfordert das Fein-Tuning, dass alle Schichten des Netzes mit neuen Daten zusätzlich trainiert werden	☐
d)	Retrieval-augmentierte Generierung erfordert zwar vorab die Identifizierung und Beschaffung aufgabenrelevanter Daten, aber keine Änderungen am vortrainierten Modell	☒

Begründung

a) FALSCH — Der RAG-Ansatz fügt dem neuronalen Netz keine neuen Schichten hinzu, um Dokumentation zu speichern; stattdessen ruft er zum Zeitpunkt der Inferenz relevante externe Daten ab und führt eine Anreicherung der Eingabe des Modells mit diesen Informationen durch.

b) FALSCH — Zwar kann Fein-Tuning mit Daten hoher Qualität Verzerrungen reduzieren, doch garantiert es nicht, dass unfaire Ergebnisse vermieden werden, da Verzerrungen bestehen bleiben oder sogar während des Fein-Tuning-Prozesses entstehen können.

c) FALSCH — Fein-Tuning kann auf allen Schichten oder nur auf einer Teilmenge durchgeführt werden. Oft werden je nach Aufgabe und Verfügbarkeit nur einige Schichten aktualisiert, während andere unverändert bleiben.

d) KORREKT — RAG basiert darauf, relevante externe Daten vor der Verwendung zu kuratieren und zu indizieren, erfordert jedoch keine Änderung der Architektur oder der Parameter des vortrainierten Modells selbst; stattdessen erfolgt eine Anreicherung der Eingaben des Modells zur Laufzeit mit den abgerufenen Informationen.

Frage 13	AI-3.2.1	K2	Punkte 1.0

Welche der folgenden Aussagen beschreibt eine Schlüsselaktivität bei der Datenvorbereitung für maschinelles Lernen am BESTEN?

Wählen Sie EINE Antwort aus!

a)	Die Datenvorbereitung umfasst die Identifizierung und das Sammeln von Daten aus verschiedenen Quellen, um dem Lernalgorithmus Rohdaten zum Lernen bereitzustellen	☐
b)	Die Merkmalsermittlung der Daten erfolgt nach dem Training des ML-Modells, um seine Leistung für die Bereitstellung in der Praxis zu optimieren	☐
c)	Die Datenvorverarbeitung umfasst die Erweiterung der Daten sowie Stichprobenziehungen, wodurch die Anzahl der Beispiele in den Trainingsdaten entweder erhöht oder verringert wird	☒
d)	Die explorative Datenanalyse (EDA) ist eine Form des explorativen Tests, die auf die Aktivitäten Datenbeschaffung, Datenvorverarbeitung und Datenkennzeichnung bei der Datenvorbereitung angewendet wird	☐

Begründung

a) FALSCH — Diese Aussage hebt nur einen grundlegenden Schritt bei der Datenvorbereitung hervor: das Sammeln und Zusammenführen von Daten aus verschiedenen Quellen, bevor mit der Verarbeitung oder Analyse begonnen wird. Zur Datenvorbereitung gehören jedoch in der Regel neben dem Sammeln von Rohdaten auch das Bereinigen, Transformieren und Organisieren der Daten.

b) FALSCH — Diese Aussage ist unzutreffend, da Merkmalsermittlung in der Regel vor (oder während) des ML-Modelltrainings durchgeführt wird, nicht danach. Der Zweck der Merkmalsermittlung besteht darin, Merkmale zu erstellen oder zu modifizieren, um die Leistung des ML-Modells während der Trainingsphase zu verbessern.

c) KORREKT — Hier werden zwei gängige Techniken der Datenvorverarbeitung korrekt benannt: Erweiterung der Daten durch die Erstellung modifizierter Versionen und Sampling (Reduzierung der Daten durch die Auswahl von Teilmengen).

d) FALSCH — Diese Aussage erfasst teilweise den Zweck der EDA, der darin besteht, Datenmerkmale zu verstehen und Probleme durch Visualisierung und zusammenfassende Statistiken zu erkennen. EDA ist jedoch kein „explorativer Test“, sondern vielmehr ein analytischer Prozess, der als Grundlage für nachfolgende Schritte der Datenvorbereitung dient.

Frage 14	AI-3.2.3	K2	Punkte 1.0

Welche der folgenden Aussagen stellt die Rollen von Trainingsdatensätzen, Validierungsdatensätzen und Testdatensätzen bei der Entwicklung von ML-Modellen am BESTEN gegenüber?

Wählen Sie EINE Antwort aus!

a)	Der Trainingsdatensatz wird zur Optimierung der Hyperparameter verwendet, der Validierungsdatensatz zur Feinabstimmung der Vorhersagen und der Testdatensatz zur Generierung von Trainingsdaten	☐
b)	Der Trainingsdatensatz dient zum Training des Modells, der Validierungsdatensatz zum Tuning des Modells und der Testdatensatz zur Evaluierung seiner Leistung anhand bisher unbekannter Daten	☒
c)	Der Trainingsdatensatz wird für die abschließende Modellevaluierung verwendet, der Validierungsdatensatz stellt sicher, dass das Modell nicht von Überanpassung betroffen ist, und der Testdatensatz dient zum Hyperparameter-Tuning	☐
d)	Der Trainingsdatensatz stellt sicher, dass das Modell gut verallgemeinert, der Validierungsdatensatz dient der Bereitstellung des Modells und der Testdatensatz dient der ersten Evaluierung	☐

Begründung

a) FALSCH — Der Trainingsdatensatz wird in erster Linie dazu verwendet, die Parameter des Modells anzupassen, nicht aber zur Optimierung der Hyperparameter. Der Validierungsdatensatz wird typischerweise zum Tuning der Hyperparameter verwendet, und der Testdatensatz wird niemals zur Generierung von Trainingsdaten herangezogen.

b) KORREKT — Der Trainingsdatensatz dient dazu, das Modell anzupassen oder zu erstellen, der Validierungsdatensatz dient dazu, die Hyperparameter des Modells zu optimieren und Überanpassung zu verhindern, und der Testdatensatz ist für die Evaluierung der Modellleistung anhand bisher unbekannter Daten reserviert. Dies beschreibt genau die unterschiedlichen und aufeinanderfolgenden Rollen der einzelnen Datensätze im ML-Workflow.

c) FALSCH — Der Trainingsdatensatz wird nicht für die abschließende Modellevaluierung verwendet – dies ist die Aufgabe des Testdatensatzes. Außerdem wird der Testdatensatz nicht für das Hyperparameter-Tuning verwendet, da dies das Risiko einer Überanpassung an den Testdatensatz mit sich bringen würde.

d) FALSCH — Die primäre Aufgabe des Trainingsdatensatzes besteht nicht darin, die Generalisierbarkeit sicherzustellen, sondern das Modell anzupassen. Der Validierungsdatensatz wird nicht für die Bereitstellung verwendet, und der Testdatensatz dient nicht der anfänglichen Evaluierung, sondern der abschließenden Evaluierung nach der Modellentwicklung

Frage 15	AI-3.3.1	K3	Punkte 2.0

Betrachten Sie die folgende Konfusionsmatrix für einen Bildklassifikator:

Konfusionsmatrix	Tatsächlich Positiv	Tatsächlich Negativ
Vorhergesagt Positiv	**78**	**22**
Vorhergesagt Negativ	**6**	**14**

Welche der folgenden Optionen stellt die RICHTIGE Formel zur Berechnung der Präzision des Klassifikators dar?

Wählen Sie EINE Antwort aus!

a)	(20/120) * 100 %	☐
b)	(78/120) * 100 %	☐
c)	(78/100) * 100 %	☒
d)	(22/100) * 100 %	☐

Begründung

a) FALSCH — Die richtige Formel und Berechnung ist unter Option c.

b) FALSCH — Die richtige Formel und Berechnung ist unter Option c.

c) KORREKT — Die Formel für die Präzision lautet: Präzision = RP / (RP + FP) * 100 = 78 / (78 + 22) = 78/100 * 100 %

d) FALSCH — Die richtige Formel und Berechnung ist unter Option c.

Frage 16	AI-3.4.1	K2	Punkte 1.0

Während des Trainings eines tiefen neuronalen Netzes erzeugt das Netz eine Ausgabe, und der Verlust wird berechnet.

Welche der folgenden Aussagen beschreibt den nächsten Schritt im Trainingsprozess RICHTIG?

Wählen Sie EINE Antwort aus!

a)	Die Verbindungsgewichte und Verschiebungswerte (*biases*) im gesamten Netz werden angepasst, um den berechneten Verlust zu verringern	☒
b)	Dieselben Trainingsdaten werden erneut durch das Netz geleitet, um den Verlustwert zu bestätigen	☐
c)	Die Aktivierungsfunktionen werden auf andere nichtlineare Formeln umgestellt, um eine bessere Anpassung zu erzielen	☐
d)	Die versteckten Schichten des Netzes werden mit neuen zufälligen Gewichtswerten zurückgesetzt	☐

Begründung

a) KORREKT — Dies ist der nächste Schritt in der ML-Trainingsschleife. Der Verlust wird durch das Netz zurückgeführt, um die Werte der Gewichtungen der Verbindungen und die Verschiebungswerte (*biases*) der Neuronen anzupassen.

b) FALSCH — Das Training fährt mit dem nächsten Datensatz fort oder schließt die Epoche ab. Es werden nicht dieselben Daten erneut verarbeitet, nur um den Verlustwert zu bestätigen.

c) FALSCH — Aktivierungsfunktionen werden beim Entwurf des Modells ausgewählt und während eines Trainingsdurchlaufs in der Regel nicht geändert.

d) FALSCH — Das Zurücksetzen der Gewichtungen erfolgt zu Beginn des Trainings (Initialisierung), nicht nach der Berechnung des Verlustwerts für einen Datenbatch.

Frage 17	AI-4.1.1	K2	Punkte 1.0

Betrachten Sie die folgenden Beispiele für KI-basierte Systeme:

i) Ein System, das aus Echtzeitdaten lernt, um seine Vorhersagen von Ausfällen zu verbessern, und Wartungspläne automatisch aktualisiert

ii) Ein KI-basierter Spamfilter für eine E-Mail-App, der Spam anhand vordefinierter Regeln identifiziert

iii) Eine Empfehlungsmaschine bei einem Streaming-Dienst, die ihre Vorschläge basierend auf den sich ändernden Sehgewohnheiten und Vorlieben eines Benutzers aktualisiert

iv) Ein persönlicher Assistent, der kontinuierlich von seinem Benutzer lernt

v) Ein regelbasiertes KI-Expertensystem für die medizinische Diagnose

Welche der folgenden Aussagen umfasst die Systeme, die als fixierte KI-basierte Systeme betrachtet werden können, am BESTEN?

Wählen Sie EINE Antwort aus!

a)	ii und v	☒
b)	i, iii und iv	☐
c)	i und iii	☐
d)	ii, iv und v	☐

Begründung

Betrachtet man die angegebenen Beispiele für KI-basierte Systeme:

i) *Ein System, das aus Echtzeitdaten lernt, um seine Prognosen für Ausfälle zu verbessern, und Wartungspläne automatisch aktualisiert.* Dies ist eine Form eines adaptiven KI-basierten Systems, das die Pläne auf der Grundlage von Echtzeitdaten anpasst.

ii) *Ein KI-basierter Spamfilter für eine E-Mail-App, der Spam anhand vordefinierter Regeln identifiziert* Dies ist eine Form eines fixierten KI-basierten Systems, das vorhersehbare Testergebnisse liefert, da es auf der Befolgung vordefinierter Regeln zur Spam-Identifizierung basiert, die erst bei einer Neugestaltung des regelbasierten Modells geändert werden.

iii) *Eine Empfehlungsmaschine bei einem Streaming-Dienst, die ihre Vorschläge basierend auf den sich ändernden Sehgewohnheiten und Vorlieben eines Benutzers aktualisiert* Hierbei handelt es sich um eine Form eines adaptiven Systems, das sich an die Sehgewohnheiten und Vorlieben des Benutzers anpasst.

iv) *Ein persönlicher Assistent, der kontinuierlich von seinem Benutzer lernt.* Hierbei handelt es sich um ein adaptives KI-basiertes System, da es seine Parameter auf der Grundlage der Interaktionen der Benutzer mit dem System anpasst.

v) *Ein regelbasiertes Expertensystem für die medizinische Diagnose.* Hierbei handelt es sich um eine Form eines fixierten KI-basierten Systems, bei dem die Domänenregeln erst dann geändert werden, wenn das regelbasierte Modell neu aufgebaut wird.

Daher wären der Spamfilter und die medizinischen Diagnosesysteme einfacher zu testen, da es sich bei beiden um fixierte Systeme handelt, die vorhersehbare Testergebnisse liefern.

KORREKT ist daher Option a) ii und v

Frage 18	AI-4.1.2	K2	Punkte 1.0

Welche der folgenden Optionen erklärt am BESTEN, warum beim Testen eines KI-basierten Systems ein statistischer Ansatz erforderlich ist?

Wählen Sie EINE Antwort aus!

a)	Das System ist in der Regel groß und komplex, sodass eine Testautomatisierung ohne den Einsatz statistischer Stichproben nicht praktikabel ist	☐
b)	Das System zeigt in der Regel nichtdeterministisches Verhalten, was ausreichend große und repräsentative Testdatensätze erfordert, um aussagekräftige Schlussfolgerungen ziehen zu können	☒
c)	Ein einzelner Testfall reicht aus, um festzustellen, ob ein Modell gut kalibriert ist, doch nur statistische Methoden können die Genauigkeit überprüfen	☐
d)	Das System wird mit realen Daten trainiert und benötigt daher keinen separaten Testdatensatz; stattdessen ist eine statistische Validierung erforderlich	☐

Begründung

a) FALSCH — Zwar können KI-basierte Systeme groß und komplex sein, doch der Grund für die Verwendung eines statistischen Ansatzes liegt in erster Linie in ihrer nicht-deterministischen Natur und nicht in der nicht praktikablen Automatisierung oder ihrer Größe.

b) KORREKT — Viele KI-basierte Systeme sind nicht-deterministisch und erfordern ausreichend umfangreiche, repräsentative Testdatensätze, um statistische Signifikanz zu erreichen, insbesondere bei der statistischen Evaluierung der funktionalen Korrektheit.

c) FALSCH — Diese Option stellt das Konzept falsch dar. Ein einzelner Testfall reicht nicht aus, um die Qualität des KI-basierten Systems zu bewerten. Eine statistische Auswertung über viele Vorhersagen hinweg ist erforderlich.

d) FALSCH — Dies widerspricht den Best Practices. Ein separater Testdatensatz (unabhängig von Trainingsdatensatz und Validierungsdatensatz) ist unerlässlich, nicht optional, und Teil der erforderlichen statistischen Stringenz.

Frage 19	AI-4.1.3	K2	Punkte 1.0

Welche der folgenden Aussagen beschreibt am BESTEN, warum selbstlernende KI-Systeme unter dem Test-Orakel-Problem leiden können?

Wählen Sie EINE Antwort aus!

a)	Die explorative Natur der Entwicklung dieser KI-Systeme bedeutet, dass sich die Systemanforderungen während der Entwicklung häufig ändern	☐
b)	Das erwartete Verhalten dieser KI-Systeme ändert sich nach der ersten Veröffentlichung, ohne dass sich die Systemspezifikation entsprechend ändert	☒
c)	Jedes dieser KI-Systeme kann auf unterschiedliche Weise lernen, was die Korrektheit dieser Systeme zu einer Frage der subjektiven Beurteilung macht	☐
d)	Die Komplexität dieser KI-Systeme macht es besonders schwierig, ihre erwarteten Ausgaben manuell zu bestimmen	☐

Begründung

a) FALSCH — Die explorative Entwicklung von KI-Systemen kann oft bedeuten, dass sich die Systemanforderungen während der Entwicklung ändern, aber selbstlernende KI-Systeme müssen nicht mit einem explorativen Entwicklungsansatz entwickelt werden.

b) KORREKT — Selbstlernende KI-basierte Systeme aktualisieren ihre internen Modelle kontinuierlich nach der Bereitstellung. Dies führt dazu, dass sich das „korrekte“ Verhalten des KI-basierten Systems ändert, wenn sich das System weiterentwickelt – und dieses Verhalten wird nicht in aktualisierten Spezifikationen widergespiegelt.

c) FALSCH — Jedes selbstlernende KI-System kann auf unterschiedliche Weise lernen, da jedes unterschiedliche Betriebserfahrungen machen wird, aber dies bedeutet normalerweise, dass sie leicht unterschiedliche erwartete Verhaltensweisen haben werden – es bedeutet nicht, dass die Bestimmung dieser erwarteten Verhaltensweisen ein subjektives Urteil erfordert.

d) FALSCH — FALSCH — Einige selbstlernende KI-Systeme können komplex sein, aber das ist nicht ihr definierendes Attribut – einige können in Bezug auf das erlernte Verhalten relativ einfach sein. Daher gibt es keinen systematischen Grund, warum ihre erwarteten Ausgaben nicht von menschlichen Testern bestimmt werden können.

Frage 20	AI-4.2.1	K2	Punkte 1.0

Welche der folgenden Aussagen beschreibt am BESTEN einen gängigen Ansatz zum Testen von GenAI-Modellen?

Wählen Sie EINE Antwort aus!

a)	GenAI-Modelle werden getestet, indem überprüft wird, ob ihre Ausgaben genau mit vordefinierten erwarteten Ergebnissen übereinstimmen	☐
b)	Beim Test von GenAI-Modellen werden diverse Eingaben und Parameter variiert und dann die Einhaltung von Regeln durch die Ausgabe bewertet, da eine direkte Übereinstimmung zwischen Eingabe und Ausgabe nicht möglich ist	☒
c)	Da GenAI-Modelle probabilistisch sind, ist ein formaler Test unnötig, da die Ausgaben immer variieren und nicht mit ausreichender Effektivität bewertet werden können	☐
d)	GenAI-Modelle werden hauptsächlich manuell durch Reviews getestet, da automatisierte Tests auf kreative KI-Ausgaben nicht anwendbar sind	☐

Begründung

a) FALSCH — Generative KI-Modelle liefern in der Regel keine deterministischen Ergebnisse, daher ist ein exakter Abgleich mit vordefinierten erwarteten Ergebnissen kein geeigneter Ansatz für das Testen.

b) KORREKT — Aufgrund der Variabilität und Komplexität der GenAI-Ausgaben konzentriert sich das Testen auf Kohärenz, Konformität mit Regeln und Plausibilität, anstatt auf die Übereinstimmung mit festgelegten erwarteten Ergebnissen. Vielfältige Eingaben, optionale Eingabeaufforderungen und Parameter beeinflussen die Testergebnisse.

c) FALSCH — Obwohl Generative KI-Modelle probabilistisch sind, können Testansätze (z. B. explorativer Test, metamorpher Test und gegnerischer Test) dennoch eingesetzt werden.

d) FALSCH — Eine manuelle Review ist möglich, aber automatisierte Methoden, einschließlich anderer GenAI-Tools oder Bilderkennungssysteme, können generierte Inhalte ebenfalls effektiv bewerten. Daher ist die Aussage, dass automatisiertes Testen „nicht anwendbar“ sei, unzutreffend.

Frage 21	AI-4.2.2	K3	Punkte 2.0

Ihr Unternehmen plant die Bereitstellung eines GenAI-basierten Generators für juristische Dokumente. Während der Implementierungsplanung plädiert das Sicherheitsteam dafür, die Red-Teaming-Maßnahmen auf die Verhinderung von indirekten promptübergreifenden Einschleusungsangriffen zu konzentrieren, während das Compliance-Team der Erkennung von Verzerrungen bei der Erstellung von Rechtsgutachten Vorrang einräumen möchte. Das Entwicklungsteam schlägt vor, Red-Teaming erst nach der Inbetriebnahme des Systems durchzuführen, um Zeit zu sparen.

Welche der folgenden Strategien ist die EFFEKTIVSTE Umsetzung von Red-Teaming in diesem Szenario?

Wählen Sie EINE Antwort aus!

a)	Zuerst Sicherheitsschwachstellen priorisieren, dann in einer separaten Phase nach der Bereitstellung Verzerrungen angehen	☐
b)	Konzentration auf die Erkennung von Verzerrungen, da die Genauigkeit der Rechtsberatung wichtiger ist als Bedenken hinsichtlich der Sicherheit	☐
c)	Sofort bereitstellen und Red-Teaming reaktiv auf der Grundlage von Vorfällen und Nutzer-Feedback durchführen	☐
d)	Vor der Bereitstellung Angriffsszenarien verwenden, die sowohl Sicherheitslücken als auch Verzerrungen abdecken	☒

Begründung

a) FALSCH — Red-Teaming wird in der Regel vor der Bereitstellung durchgeführt.

b) FALSCH — In der Frage gibt es keinen Hinweis darauf, dass Sicherheit wichtiger oder weniger wichtig ist als das Testen auf Verzerrung.

c) FALSCH — Red-Teaming wird proaktiv vor der Bereitstellung durchgeführt.

d) KORREKT — Red-Teaming sollte vor der Bereitstellung durchgeführt werden, nicht danach, und verschiedene Arten von schädliche Fähigkeiten (Sicherheitslücken und Verzerrungen) können gemeinsam getestet werden (LP 4.2.2., 2. Absatz).

Frage 22	AI-4.3.1	K2	Punkte 1.0

Ein ML-basiertes Wettervorhersagesystem liefert für die meisten Standorte hervorragende Ergebnisse; es wurde jedoch festgestellt, dass die Vorhersagen für Gebiete in Großbritannien (Vereinigtes Königreich) mit einer Höhe von mehr als 1250 Metern regelmäßig ungenau sind.

Welche der folgenden Teststufen hätte GRÜNDLICHER durchgeführt werden sollen?

Wählen Sie EINE Antwort aus!

a)	Systemtest	☐
b)	Eingabedatentest	☒
c)	Komponentenintegrationstest	☐
d)	ML-Modelltest	☐

Begründung

a) FALSCH — Zwar hätte dieser Fehlerzustand möglicherweise auch bei Systemtests entdeckt werden können, doch ist der Eingabedatentest die effektivste Teststufe, um ihn zu erkennen, da er dort bereits in einer früheren Phase entdeckt worden wäre.

b) KORREKT — Beim Eingabedatentest liegt der Schwerpunkt auf der Qualität der Daten und der Repräsentativität der Daten. Es scheint, dass Gebiete im Vereinigten Königreich mit einer Höhe von mehr als 1.250 Metern in den Trainingsdaten nicht ausreichend vertreten waren (In GB nur 6 Erhebungen > 1250 m).

c) FALSCH — Beim Komponentenintegrationstest wird auf Fehlerzustände in den Schnittstellen und den Interaktionen zwischen Komponenten geprüft; der Fokus liegt nicht auf bestimmten Datenwerten.

d) FALSCH — Der ML-Modelltest hätte diesen Fehler zwar möglicherweise identifiziert, doch wäre der Eingabedatentest die effektivste Teststufe, um ihn zu erkennen, da er dort bereits früher entdeckt worden wäre.

Frage 23	AI-4.3.2	K2	Punkte 1.0

Welche der folgenden Aussagen zur Anwendung risikobasierter Tests auf ML-Systeme ist RICHTIG?

Wählen Sie EINE Antwort aus!

a)	Risiken hinsichtlich der Sicherheit (*security*) und Gebrauchstauglichkeit können bei jedem System auftreten, während Risiken im Zusammenhang mit Datenverzerrungen und mit der Leistung von ML-Modellen spezifisch für ML-Systeme sind	☒
b)	Konventionelle Systeme bergen Risiken im Zusammenhang mit Datenverzerrungen, während bei ML-Systemen Risiken im Zusammenhang mit algorithmischen Verzerrungen wahrscheinlicher sind	☐
c)	Das Risikomanagement für konventionelle Systeme ist ein statischer Ansatz, während Risiken eines selbstlernenden Systems dynamisch angepasst werden müssen	☐
d)	In konventionellen Systemen ist die funktionale Korrektheit der primäre Risikofaktor, während bei einem ML-System die funktionale Anpassbarkeit der primäre Risikofaktor ist	☐

Begründung

a) KORREKT — Sicherheit und Gebrauchstauglichkeit sind allgemeine Qualitätsmerkmale und können auf jedes System zutreffen. Datenverzerrung und Modellleistung sind potenzielle Risiken, die spezifisch für ML-Systeme sind.

b) FALSCH — Sowohl Datenverzerrung als auch algorithmische Verzerrung sind Risiken, die ausdrücklich mit einem ML-System verbunden sind und daher nicht auf konventionelle Systeme zutreffen.

c) FALSCH — Das Risikomanagement sowohl für Nicht-KI-Systeme als auch für KI-Systeme (einschließlich selbstlernender ML-Systeme) sollte dynamischer Natur sein.

d) FALSCH — Funktionale Korrektheit mag zwar der primäre Risikofaktor für konventionelle Systeme und für ML-Systeme sein, dies ist jedoch kontextabhängig.

Frage 24	AI-5.1.1	K2	Punkte 1.0

Ein Team entwickelt ein neues ML-Modell und hat einen Datensatz von einem neuen, nicht verifizierten Drittanbieter erhalten. Es ist sich über die Herkunft dieses Datensatzes unsicher und befürchtet, dass die Rohdaten manipuliert worden sein könnten.

Welcher der folgenden Testansätze eignet sich am BESTEN, um diesem spezifischen Risiko zu begegnen?

Wählen Sie EINE Antwort aus!

a)	Datenprovenienztest	☒
b)	Datenrepräsentativitätstest	☐
c)	Merkmalstest	☐
d)	Datensatzeinschränkungstest	☐

Begründung

a) KORREKT — Das Szenario beschreibt die Notwendigkeit, die Herkunft der Daten zu überprüfen und sicherzustellen, dass sie nicht manipuliert wurden. Dies entspricht dem Datenprovenienztest.

b) FALSCH — Das Team würde zwar wahrscheinlich einen Datenrepräsentativitätstest an einem neuen Datensatz durchführen, doch dabei geht es darum, ob die Eigenschaften der Daten mit denen der realen Welt übereinstimmen, und nicht darum, ob die dokumentierte Herkunft korrekt ist oder ob es sich um gültige Rohdaten handelt.

c) FALSCH — Beim Testen der Merkmale wird die Vorhersagekraft der Merkmale bewertet, was ein anderes Anliegen ist als die Überprüfung der Quelle und der Integrität des Datensatzes selbst.

d) FALSCH — Beim Datensatzeinschränkungstest wird die interne Konsistenz des Datensatzes (z. B. Bereiche, Typen) überprüft, jedoch kann dabei nicht verifiziert werden, woher die Daten stammen oder ob sie unrechtmäßig verändert wurden.

Frage 25	AI-5.1.2	K2	Punkte 1.0

Ein Finanzdienstleistungsunternehmen entwickelt ein ML-System zur Kreditgenehmigung. Ein Tester dieses Systems möchte feststellen, ob im System potenzielle Verzerrungen in Bezug auf Faktoren wie Geschlecht und Alter bestehen.

Welcher der folgenden Ansätze ist am BESTEN geeignet, um Verzerrungen in den Trainingsdaten frühzeitig zu erkennen?

Wählen Sie EINE Antwort aus!

a)	Durchführung einer statischen Analyse des Quellcodes des Modells, um festzustellen, wie dessen Verarbeitung der alters- und geschlechtsbezogenen Merkmale zu Verzerrungen führen könnte	☐
b)	Testen mit einem repräsentativen Datensatz und Analyse der Vorhersagen auf statistisch signifikante Unterschiede bei den Ergebnissen über Alter und Geschlecht hinweg	☐
c)	Review des gesamten ML-Workflows und der Prozesse der Datenvorbereitung, um potenzielle Ursachen für das Auftreten von Verzerrungen zu identifizieren	☒
d)	Durchführung einer Analyse auf mittelbare Diskriminierung anhand kontrafaktischer Modelleingaben, bei denen Geschlecht, Alter oder beide Attribute verändert werden	☐

Begründung

a) FALSCH — Dieser Ansatz konzentriert sich auf die Modelllogik und nicht auf die Eigenschaften der Trainingsdaten. Er deckt keine in den Daten vorhandenen Verzerrungen direkt auf.

b) FALSCH — Dieser Ansatz untersucht die Modellausgaben und nicht die Trainingsdaten selbst. Er eignet sich gut zur Identifizierung von Verzerrungen in den Vorhersagen, jedoch nicht zur ersten Erkennung von Verzerrungen in den Daten.

c) KORREKT — Dieser Ansatz könnte dazu beitragen, aufzuzeigen, wo Verzerrungen auftreten könnten, stützt sich jedoch auf Prozesskontrollen und nicht auf tatsächliche Belege aus den Daten.

d) FALSCH — Die Analyse auf mittelbare Diskriminierung bewertet die Ergebnisse oder Vorhersagen unter hypothetischen Änderungen und zielt dabei auf Verzerrungen der Modell-Ausgaben ab, anstatt den Trainingsdatensatz direkt zu bewerten.

Frage 26	AI-5.1.3	K2	Punkte 1.0

Was ist ein WESENTLICHER Unterschied in der Teststrategie für eine Trainingsdaten-Pipeline im Vergleich zu einer Produktivdaten-Pipeline?

Wählen Sie EINE Antwort aus!

a)	Beim Testen einer Produktivdaten-Pipeline würde der Schwerpunkt hauptsächlich auf der Validierung einzelner Transformationsskripte liegen, während beim Testen einer Trainingsdaten-Pipeline Ende-zu-Ende-Systemtests Vorrang hätten	☐
b)	Eine Trainingsdaten-Pipeline würde sich fast ausschließlich auf Fehlereinfügung und Back-to-Back-Tests stützen, während sich eine Produktivdaten-Pipeline auf Komponententests und Komponentenintegrationstests beschränken würde	☐
c)	Reviews des Konfigurationsmanagements wären für eine Produktivdaten-Pipeline von entscheidender Bedeutung, gelten jedoch für explorative Trainingsdaten-Pipelines aufgrund ihres weniger formellen Charakters als unnötig	☐
d)	Beim Testen einer Trainingsdaten-Pipeline würde der Schwerpunkt in erster Linie auf der korrekten Verarbeitung der Daten liegen, während beim Testen einer Produktivdaten-Pipeline der Schwerpunkt auf hoher Performanz und Zuverlässigkeit unter Last liegen würde	☒

Begründung

a) FALSCH — Beide Pipeline-Typen würden von einem umfassenden, schichtbasierten Ansatz profitieren. Eine operative Pipeline würde umfangreiche Ende-zu-Ende-Systemtests erfordern, nicht nur die Validierung einzelner Skripte.

b) FALSCH — Beide Pipeline-Typen würden eine Reihe von Tests nutzen. Die Beschränkung des einen auf einen reinen Testansatz auf Systemebene und des anderen auf einen reinen Testansatz auf Komponenten- und Integrationsebene entspricht keinem mehrschichtigen Ansatz.

c) FALSCH — Das Konfigurationsmanagement stellt sicher, dass „über Training, Test und Produktion hinweg“ die richtigen Versionen verwendet werden, was bedeutet, dass Konsistenz und Reproduzierbarkeit für beide Arten von Pipelines wichtig sind, nicht nur für operative.

d) KORREKT — Der Zweck der Pipeline bestimmt die Teststrategie. Tests der Trainingsdaten-Pipelines legen den Schwerpunkt auf die Generierung hochwertiger Daten, während Tests für Produktivdaten-Pipelines sich auf nicht-funktionale Aspekte wie Performanz, Skalierbarkeit und KI-Robustheit konzentrieren.

Frage 27	AI-5.1.4	K2	Punkte 1.0

Was ist der Zweck der Erstellung eines Referenzdatensatzes bei einem Datenrepräsentativitätstest?

Wählen Sie EINE Antwort aus!

a)	Er dient als allgemein anwendbarer Datensatz, der aus vertrauenswürdigen Branchen-Benchmarks abgeleitet wird	☐
b)	Er dient als Basis für den formalen Vergleich der statistischen Eigenschaften der Trainingsdaten mit denen der erwarteten Produktivdaten	☒
c)	Er wird verwendet, um eine geschichtete Stichprobenziehung direkt auf die Trainingsdaten anzuwenden und so sicherzustellen, dass alle Untergruppen abgedeckt sind	☐
d)	Er dient als primärer Datensatz für die Durchführung der abschließenden Validierung und des Tests des Modells mit hoher Unabhängigkeit	☐

Begründung

a) FALSCH — Ein Referenzdatensatz muss weder universell anwendbar sein noch ausschließlich aus Branchen-Benchmarks abgeleitet werden. Er ist in der Regel so zugeschnitten, dass er den betrieblichen und kontextbezogenen Merkmalen der Zielgruppe des KI-Systems entspricht.

b) KORREKT — Der Hauptzweck des Referenzdatensatzes besteht darin, eine statistische Basis bereitzustellen, die es Praktikern ermöglicht, die Verteilungen, die Merkmal-Korrelationen und die Überdeckung des Trainingsdatensatzes objektiv mit den Erwartungen in realen Produktivumgebungen zu vergleichen (vgl. LP 5.1.4, 2, 2. Punkt).

c) FALSCH — Die geschichtete Stichprobenziehung wird in der Regel auf den Referenzdatensatz angewendet, um eine umfassende Daten-Baseline zu erstellen, und nicht direkt auf den Trainingsdatensatz selbst. Der Referenzdatensatz zielt darauf ab, dass alle relevanten Untergruppen vertreten sind, und dient als Maßstab für die Bewertung der Repräsentativität der anderen Datensätze.

d) FALSCH — Der Referenzdatensatz ist nicht als Hauptquelle für abschließende ML-Modelltests oder für Tests mit hoher Unabhängigkeit gedacht. Er dient dazu, die Repräsentativität der Daten vor dem ML-Modelltraining zu bewerten.

Frage 28	AI-5.1.5	K3	Punkte 2.0

Sie testen einen ML-Datensatz für ein System zur Genehmigung von Bankkrediten. Der Datensatz enthält die folgenden Attribute:

- **Antragsteller_ID (Ganzzahl, eindeutig)**
- **Jahreseinkommen (Dezimalzahl, in USD)**
- **Kreditbetrag (Dezimalzahl, in USD)**
- **Kreditwürdigkeit (Ganzzahl, 300–850)**
- **Beschäftigungsdauer (Ganzzahl, 0–50)**
- **Monatsrate (Dezimalzahl, in USD)**

Es gelten die folgenden Geschäftsregeln:

- **Der Kreditbetrag darf das Fünffache des Jahreseinkommens nicht überschreiten**
- **Monatsrate = Kreditbetrag / 360 (bei einer Laufzeit von 30 Jahren)**
- **Die Kreditwürdigkeit muss im Standardbereich liegen**
- **Alle Geldwerte müssen positiv sein**

Welche Art von Einschränkung wäre am BESTEN geeignet, wenn man einen Datensatzeinschränkungstest durchführt, um die Monatsrate für 30-jährige Kredite zu validieren?

Wählen Sie EINE Antwort aus!

a)	Einzelwert-Einschränkung: Bereich	☐
b)	Multiwert-Einschränkung: Anzahl	☐
c)	Vergleichs-Einschränkung: Korrelation	☒
d)	Multiwert-Einschränkung: Duplikate	☐

Begründung

a) FALSCH — Eine Bereich-Einschränkung führt lediglich eine Validierung durch, ob die Werte eines einzelnen Attributs innerhalb der angegebenen Grenzen liegen, überprüft jedoch nicht die mathematische Beziehung zwischen der Monatsrate und dem Kreditbetrag.

b) FALSCH — Eine Anzahl-Einschränkung prüft die Anzahl der Nicht-Null-Werte, nicht die mathematische Korrektheit berechneter Felder.

c) KORREKT — In diesem Szenario muss die Validierung einer mathematischen Beziehung zwischen zwei Attributen (Monatsrate und Kreditbetrag) durchgeführt werden. Die Korrelation-Einschränkung wurde speziell dafür entwickelt, zu prüfen, ob die Werte eines Attributs gemäß einer definierten Regel mit den Werten eines anderen Attributs korrelieren – in diesem Fall, dass die Monatsrate gleich Kreditbetrag / 360 ist.

d) FALSCH — Eine Duplikat-Einschränkung identifiziert identische Werte, doch doppelte monatliche Zahlungen können legitim sein (verschiedene Antragsteller können dieselbe Monatsrate haben).

Frage 29	AI-5.1.6	K2	Punkte 1.0

Welche der folgenden Aussagen beschreibt die Rolle von multipler Annotation beim Kennzeichen-Korrektheitstest am BESTEN?

Wählen Sie EINE Antwort aus!

a)	Multiple Annotation kann verwendet werden, um die Verifizierung der Kennzeichen zu automatisieren und so Konsistenz sicherzustellen	☐
b)	Multiple Annotation kann durch den Vergleich der Annotationen auf Fehler bei der Kennzeichnung hinweisen	☒
c)	Multiple Annotation vergleicht die Verteilung der Kennzeichen über verschiedene Datensätze hinweg, um potenzielle Fehlerzustände zu erkennen	☐
d)	Multiple Annotation weist auf Fehlerzustände in Datenpunkten mit hohem Modell-Verlust hin	☐

Begründung

a) FALSCH — Multiple Annotation wird normalerweise nicht automatisiert. Multiple Annotationen stützen sich in der Regel auf menschliche Annotatoren und gewährleisten keine Konsistenz; stattdessen machen sie Inkonsistenzen deutlich.

b) KORREKT — Bei der Multiplen Annotation werden Datenpunkte von mehreren Annotatoren unabhängig voneinander gekennzeichnet. Der Vergleich dieser Kennzeichnungen führt zur Erkennung von Meinungsverschiedenheiten zwischen den Annotatoren und hebt potenzielle Fehlerzustände hervor.

c) FALSCH — Der Vergleich von Kennzeichen-Verteilungen ist Teil der Analyse der Verteilungen von Daten, nicht der Multiplen Annotation.

d) FALSCH — Das Markieren von Datenpunkten mit hohem Verlust ist Aufgabe der Modell-Verlustanalyse, nicht der Multiplen Annotation.

Frage 30	AI-6.1.1	K2	Punkte 1.0

Gegeben seien die folgenden Testansätze:

1) Testen der funktionalen Leistung von ML

2) Testen auf Verzerrung

3) Gegnerischer Test

4) Drift-Test

Weiterhin die folgenden Risiken:

A) Das ML-Modell könnte bei verschiedenen demografischen Gruppen unterschiedliche Ergebnisse erbringen

B) Leicht veränderte Eingaben in das ML-Modell könnten zu ganz anderen und unerwarteten Ausgaben führen

C) Die vom ML-Modell erstellten Vorhersagen könnten in einigen Fällen ungenau sein

D) Die Genauigkeit des ML-Modells könnte seit seiner Bereitstellung erheblich abgenommen haben

Welche der folgenden Optionen ordnet den Testansätzen am BESTEN die Risiken zu?

Wählen Sie EINE Antwort aus!

a)	1A – 2D – 3C – 4B	☐
b)	1C – 2A – 3B – 4D	☒
c)	1B – 2A – 3C – 4D	☐
d)	1A – 2C – 3D – 4B	☐

Begründung

Betrachtet werden die einzelnen Risiken nacheinander:

A) Das ML-Modell könnte bei verschiedenen demografischen Gruppen unterschiedliche Ergebnisse erbringen. Hierfür eignet sich am besten das Testen auf Verzerrung, bei dem die Fairness über verschiedene Bevölkerungsgruppen hinweg explizit untersucht wird. (2)

B) Leicht veränderte Eingaben in das ML-Modell können zu ganz anderen und unerwarteten Antworten führen. Hierfür eignet sich der Gegnerische Test, bei dem gezielt die Fähigkeit eines ML-Modells getestet wird, mit kleinen Störungen der Eingaben umzugehen. (3)

C) Die vom ML-Modell erstellten Vorhersagen könnten in einigen Fällen ungenau sein. Dies lässt sich am besten durch Testen der funktionalen Leistung von ML angehen, bei dem direkt bewertet wird, ob das ML-Modell genaue Ergebnisse liefert. (1)

D) Die Genauigkeit des ML-Modells könnte seit seiner Bereitstellung erheblich abgenommen haben. Hierfür eignet sich der Drift-Test der die Leistungsänderungen im Laufe der Zeit in der Produktion überwacht. (4)

Somit lautet die richtige Zuordnung zwischen Risiken und Testansätzen: 1C – 2A – 3B – 4D, und somit ist b) die richtige Antwort.

Frage 31	**AI-6.1.2**	**K2**	**Punkte 1.0**

Welche der folgenden Aussagen zur Dokumentation von ML-Modellen ist RICHTIG?

Wählen Sie EINE Antwort aus!

a)	Informationen zur Latenz des Modells bei der Vorhersage sind Teil der Dokumentation einer KI-Komponente	☒
b)	Die Interaktion zwischen KI-Komponenten und Nicht-KI-Komponenten ist Bestandteil der Modelldokumentation	☐
c)	Verzerrungsbezogene Eigenschaften der Eingabedaten sind schwer zu bewerten, da die Modelldokumentation **keine** Angaben zur Quelle der Trainingsdaten enthält	☐
d)	Änderungen, die von selbstlernenden ML-Systemen vorgenommen werden, werden zum Zeitpunkt der Aktualisierung vollständig dokumentiert, um eine aktuelle Dokumentation zu gewährleisten	☐

Begründung

a) KORREKT — Die Latenz ist Teil der nicht-funktionalen Anforderungen/Dokumentation.

b) FALSCH — Die Interaktion zwischen KI-Komponenten und Nicht-KI-Komponenten fällt nicht in den Umfang der Modelldokumentation.

c) FALSCH — Die Modelldokumentation sollte die Quelle der Trainingsdaten enthalten.

d) FALSCH — Die Dokumentation der vom selbstlernenden System vorgenommenen Änderungen könnte nur vom System selbst zum Zeitpunkt der Aktualisierung erstellt werden.

Frage 32	AI-6.1.3	K2	Punkte 1.0

Nach der Bereitstellung lieferte ein ML-Modell nicht so oft korrekte Vorhersagen wie erwartet. Es wurden zusätzliche Tests durchgeführt, und die Genauigkeit bei diesen Tests wurde mit 83 % gemessen.

Zuvor hatte das ML-Modell bei einem Konfidenzniveau von 94 % eine Genauigkeit von 83 % bei einer Fehlerspanne von ± 4 % erreicht.

Welche der folgenden Optionen beschreibt die aktuelle Situation am WAHRSCHEINLICHSTEN?

Wählen Sie EINE Antwort aus!

a)	Genauigkeit von 83 % bei einer Fehlerspanne von ± 2 % bei einem Konfidenzniveau von 94 %	☒
b)	Genauigkeit von 83 % bei einer Fehlerspanne von ± 4 % bei einem Konfidenzniveau von 92 %	☐
c)	Genauigkeit von 83 % bei einer Fehlerspanne von ± 6 % bei einem Konfidenzniveau von 94 %	☐
d)	Genauigkeit von 85 % bei einer Fehlerspanne von ± 4 % bei einem Konfidenzniveau von 94 %	☐

Begründung

a) KORREKT — Wenn mehr Tests für dieselbe gemessene Genauigkeit (83 %) durchgeführt werden, verringert sich die Fehlerspanne in der Regel, sofern das Konfidenzniveau gleichbleibt. Dies liegt daran, dass eine größere Stichprobengröße die Fehlerspanne verringern und/oder unser statistisches Vertrauen in den gemessenen Wert erhöhen kann. Wenn das ML-Modell zuvor eine Genauigkeit von 83 % mit einer Fehlerspanne von ± 4 % bei einem Konfidenzniveau von 94 % erreicht hat und zusätzliche Tests unter Beibehaltung derselben Messung der Genauigkeit von 83 % und des Konfidenzniveaus von 94 % durchgeführt wurden, würde dies zu einer geringeren Fehlerspanne führen (z. B. ± 2 %). Dies deutet darauf hin, dass wir mit größerer Sicherheit davon ausgehen können, dass die tatsächliche Genauigkeit tatsächlich bei etwa 83 % liegt.

b) FALSCH — Wenn mehr Tests durchgeführt werden, nimmt die Fehlerspanne in der Regel ab und das Konfidenzniveau steigt in der Regel an, anstatt abzunehmen, vorausgesetzt, die gemessene Genauigkeit bleibt gleich. Ein Rückgang des Konfidenzniveaus von 94 % auf 92 % würde darauf hindeuten, dass weniger Tests durchgeführt wurden oder dass die Testergebnisse stärker schwankten, was im Widerspruch zu dem Szenario steht, in dem zusätzliche Tests durchgeführt wurden.

c) FALSCH — Wenn zusätzliche Tests durchgeführt wurden und die Genauigkeit bei 83 % blieb, würde die Fehlerspanne in der Regel sinken und nicht steigen, sofern das Konfidenzniveau bei 94 % gehalten wurde. Die erhöhte Fehlerspanne von ± 6 % macht diese Option weniger wahrscheinlich als die Option, bei der sie sinkt (a).

d) FALSCH — Im Szenario heißt es, dass die Genauigkeit des ML-Modells bei den zusätzlichen Tests mit 83 % gemessen wurde, nicht mit 85 %. Ein Anstieg der Genauigkeit würde darauf hindeuten, dass das ML-Modell bei den zusätzlichen Tests eine bessere Leistung erbracht hat, was im Widerspruch zu der Angabe steht, dass das ML-Modell „weniger oft als erwartet korrekte Vorhersagen lieferte“, während die gemessene Genauigkeit bei 83 % blieb.

Frage 33	AI-6.1.4	K2	Punkte 1.0

Welche der folgenden Aussagen fasst den gegnerischen Test von ML-Systemen am BESTEN zusammen?

Wählen Sie EINE Antwort aus!

a)	Es handelt sich um eine Form des Black-Box-Tests, bei dem Kenntnisse über die internen Abläufe des ML-Systems außer Acht gelassen werden, um gegnerische Beispiele zu erstellen	☐
b)	Der Schwerpunkt liegt auf der manuellen Erzeugung gegnerischer Beispiele ohne Automatisierung, um ML-Systeme auf Sicherheitslücken zu testen	☐
c)	Es identifiziert Sicherheitslücken in Modellen durch gegnerische Beispiele, bei denen es sich um gezielt veränderte Eingaben handelt, die fehlerhafte Ausgaben oder Klassifikationen hervorrufen	☒
d)	Es überprüft die Funktionalität des ML-Systems unter Verwendung zuvor funktionierender Tests, um Fehlerwirkungen des ML-Modells während der Evaluierung und des Tunings des ML-Modells zu vermeiden	☐

Begründung

a) FALSCH — Es impliziert fälschlicherweise, dass Kenntnisse über Interna des ML-Modells irrelevant sind, während solche Kenntnisse den Testprozess durch die Erstellung gezielterer gegnerischer Beispiele verbessern können.

b) FALSCH — Es wird fälschlicherweise suggeriert, dass manuelle Methoden der einzige Ansatz seien, wobei automatisierte Techniken außer Acht gelassen werden, die beim gegnerischen Test ebenfalls von entscheidender Bedeutung sind.

c) KORREKT — Beim gegnerischen Test werden die gegnerischen Beispiele oft erstellt, um Sicherheitslücken durch kleine Veränderungen funktionierender Eingaben zu identifizieren.

d) FALSCH — Dies verfehlt den Kern des gegnerischen Tests, bei dem bewusst aktualisierte Eingabewerte (d. h. Tests) verwendet werden, um gegnerische Beispiele zu erstellen.

Frage 34	AI-6.1.5	K3	Punkte 2.0

Ein KI-basiertes Suchsystem für Mobiltelefone stellt eine Liste von Smartphones bereit, die seiner Einschätzung nach am besten für den Benutzer geeignet sind, basierend auf seinen Erkenntnissen über die bisherige Smartphone-Nutzung des Benutzers und dessen angegebene Präferenzen.

Ein metamorpher Test soll nun aus dem folgenden Ausgangstestfall abgeleitet werden:

Eingaben	
Ausgewählte Preisspanne:	200–300 €
3D-Kamera:	beliebig
Bildschirmgröße:	mittel bis groß
Betriebssystem:	Android oder iOS
Akkulaufzeit:	beliebig

Ausgänge
Empfohlene Smartphones:
SnapHappy_X1
SnapHappy_M2
SnapHappy_M3
ClickNow_1000x
ClickNow_1000xs

Folgende Testdaten wurden für zwei entsprechende Folgetestfälle erstellt:

Eingabe T1	
Ausgewählte Preisspanne:	200–300 €
3D-Kamera:	ja
Bildschirmgröße:	mittel bis groß
Betriebssystem:	Android oder iOS
Akkulaufzeit:	beliebig
Eingabe T2	
Ausgewählte Preisspanne:	200–300 €
3D-Kamera:	nein
Bildschirmgröße:	mittel bis groß
Betriebssystem:	Android oder iOS
Akkulaufzeit:	beliebig

Welche der folgenden Optionen ist am WAHRSCHEINLICHSTEN eine gültige Liste empfohlener Smartphones als erwartete Ausgabe für die Folgetestfälle?

Wählen Sie EINE Antwort aus!

a)	T1: SnapHappy_X1, SnapHappy_M2 T2: ClickNow_1000x, ClickNow_1000xs	☐
b)	T1: SnapHappy_M2, SnapHappy_M3, ClickNow_1000xs T2: SnapHappy_X1, ClickNow_1000x	☒
c)	T1: SnapHappy_X1, SnapHappy_M2, SnapHappy_M3, ClickNow_1000x, ClickNow_1000xs T2: SnapHappy_X1, SnapHappy_M2, SnapHappy_M3	☐
d)	T1: SnapHappy_X1, SnapHappy_M2, SnapHappy_M3, ClickNow_1000x, ClickNow_1000xs T2: SnapHappy_X1, SnapHappy_M2, SnapHappy_M3, ClickNow_1000x, ClickNow_1000xs	☐

Begründung

Angenommen, es liegen die folgenden Folgetestfälle vor:
Der Testfall T1 unterscheidet sich vom Ausgangstestfall durch die geänderten Anforderungen an eine 3D-Kamera; diese sind nun spezifischer. Eine 3D-Kamera muss enthalten sein. Das bedeutet also, dass die erwarteten Ergebnisse der Folgetests höchstens die ursprünglichen Testergebnisse umfassen können (die zuvor empfohlenen Smartphones, jedoch mit einer 3D-Kamera).

Auch der Testfall T2 unterscheidet sich vom Ausgangstestfall durch die geänderten Anforderungen an eine 3D-Kamera; auch hier sind die Anforderungen spezifischer. Es darf keine 3D-Kamera enthalten sein. Das bedeutet also, dass die erwarteten Ergebnisse des Folgetests höchstens die ursprünglichen Testergebnisse umfassen können (die zuvor empfohlenen Smartphones, jedoch ohne 3D-Kamera).

Da T1 Smartphones mit einer 3D-Kamera auflistet, müssen die übrigen Smartphones aus dem Ausgangstestfall diejenigen ohne 3D-Kamera sein und sollten daher in T2 enthalten sein.

Daher sollten T1 und T2 zusammen alle Kameras aus dem Ausgangstestfall enthalten, wobei es jedoch keine Überschneidungen zwischen den beiden geben darf.

a) FALSCH — Die Kamera „SnapHappy M3“ fehlt in den kombinierten Ergebnissen von T1 und T2

b) KORREKT — Es gibt keine Überschneidung zwischen den Ergebnissen von T1 und T2, und es fehlt keine Kamera.

c) FALSCH — Die SnapHappy-Kameras sind in beiden Testfällen aufgeführt.

d) FALSCH — Die Ausgabe der beiden Testfälle ist identisch, obwohl die Anforderungen an die 3D-Kamera unterschiedlich sind.

Frage 35	AI-6.1.7	K2	Punkte 1.0

Ein Unternehmen nutzt ein ML-Modell zur Vorhersage der Kundenabwanderung, verfügt jedoch über keinen Mechanismus, um direktes Benutzer-Feedback einzuholen oder zu erfassen, wann Kunden das Unternehmen verlassen. Man möchte auf Drift testen, indem die im Produktivbetrieb in das ML-Modell eingegebenen Daten analysiert werden.

Welche Testart wäre in dieser Situation am BESTEN geeignet und warum?

Wählen Sie EINE Antwort aus!

a)	Dynamischer Drift-Test, da er durch die Analyse der statistischen Eigenschaften der Eingabedaten die aktuelle Grundwahrheit ableiten kann	☐
b)	Statischer Drift-Test, da er Drift durch die Erkennung von Veränderungen in den statistischen Verteilungen der Daten identifiziert, ohne dass eine Grundwahrheit erforderlich ist	☒
c)	Dynamischer Drift-Test, da der Vergleich der Vorhersagen des ML-Modells mit den Ist-Ergebnissen der direkteste Weg ist, um eine Leistungsverschlechterung zu messen	☐
d)	Statischer Drift-Test, da dabei die Leistungskennzahlen des ML-Modells im Produktivbetrieb mit einem vordefinierten Akzeptanzschwellenwert verglichen werden	☐

Begründung

a) FALSCH — Dynamische Tests sind zwar geeignet, wenn Referenzdaten verfügbar sind, analysieren jedoch nicht die statistischen Eigenschaften der Eingabedaten.

b) KORREKT — Da keine Referenzwerte vorliegen, ist der statische Drift-Test die einzige praktikable Option, da er ohne Referenzwerte Veränderungen in der Eingabedatenverteilung erkennen kann.

c) FALSCH — Das Unternehmen „verfügt über keinen Mechanismus, um zu verfolgen, ob ein Kunde tatsächlich abwandert“. Daher liegen keine Ist-Ergebnisse zum Vergleich vor, was die Durchführung eines dynamischen Tests unmöglich macht.

d) FALSCH — Statische Tests untersuchen Datenverteilungen, während der Vergleich von Metriken mit der Grundwahrheit der Mechanismus eines dynamischen Tests ist.

Frage 36	AI-6.1.8	K2	Punkte 1.0

Beim Testen eines trainierten ML-Modells stellte das Entwicklungsteam fest, dass das Modell bei der Auswertung mit Validierungsdaten eine hohe Genauigkeit aufwies, bei unabhängigen Testdaten jedoch schlechte Ergebnisse lieferte.

Welche der folgenden Optionen erklärt diese Situation am WAHRSCHEINLICHSTEN?

Wählen Sie EINE Antwort aus!

a)	Unteranpassung	☐
b)	Konzeptdrift	☐
c)	Überanpassung	☒
d)	Niedrige Akzeptanzkriterien	☐

Begründung

a) FALSCH — Das ML-Modell schneidet bei den Daten der Validierung gut ab, daher ist es unwahrscheinlich, dass es sich um eine Unteranpassung handelt.

b) FALSCH — Unter Konzeptdrift versteht man Veränderungen, die nach dem ML-Modelltraining und den Phasen der Validierung auftreten.

c) KORREKT — Die schlechte Leistung bei den Testdaten und die gute Leistung bei den Daten der Validierung deuten auf Überanpassung hin.

d) FALSCH — Akzeptanzkriterien sollten für verschiedene Datensätze konsistent sein, daher ist es unwahrscheinlich, dass niedrige Akzeptanzkriterien zu einem Unterschied zwischen den Testergebnissen mit Daten der Validierung und unabhängigen Testdaten führen.

Frage 37	AI-6.1.9	K2	Punkte 1.0

Welche der folgenden Aussagen beschreibt am BESTEN, wie A/B-Tests im Zusammenhang mit einem ML-System (MLS) eingesetzt werden?

Wählen Sie EINE Antwort aus!

a)	A/B-Tests werden in erster Linie verwendet, um vielfältige Testfälle zu generieren, die alle möglichen Eingaben für ein MLS abdecken	☐
b)	A/B-Tests werden eingesetzt, um zu überprüfen, ob alle Komponenten innerhalb eines MLS korrekt miteinander interagieren	☐
c)	A/B-Tests ermitteln, ob eine aktualisierte Version eines MLS eine genauso gute oder bessere Leistung erbringt als die vorherige Version	☒
d)	A/B-Tests konzentrieren sich auf die Analyse der Struktur des internen Algorithmus eines MLS, um potenzielle Fehlerzustände zu identifizieren	☐

Begründung

a) FALSCH — Laut Lehrplan „erzeugt der A/B-Test keine Testfälle und bietet keine Anleitung dazu, wie die Tests entworfen werden sollten, obwohl in den Tests häufig operative Eingaben verwendet werden.“ Beim A/B-Test wird die Reaktion zweier Varianten verglichen, anstatt Testfälle zu generieren.

b) FALSCH — A/B-Tests konzentrieren sich nicht auf die Interaktionen zwischen Komponenten innerhalb eines Systems. Sie vergleichen zwei verschiedene Versionen eines Systems, nicht Komponenten innerhalb eines einzelnen Systems.

c) KORREKT — Wie im Lehrplan angegeben: „Wann immer das System aktualisiert wird, wird der A/B-Test eingesetzt, um zu prüfen, ob die aktualisierte Variante genauso gut oder besser funktioniert als die vorherige Variante.“ Dies beschreibt genau, wie der A/B-Test im Kontext von ML-Systemen eingesetzt wird.

d) FALSCH — A/B-Tests analysieren nicht die interne Algorithmusstruktur. Es handelt sich um einen „statistischen Testansatz, der typischerweise den Vergleich von Testergebnissen aus mehreren Testläufen erfordert, um den Unterschied zwischen den Programmen zu ermitteln.“ Der Schwerpunkt liegt auf dem Vergleich der Ergebnisse zweier Varianten, nicht auf der Untersuchung ihrer internen Strukturen.

Frage 38	AI-6.1.10	K2	Punkte 1.0

Wie lässt sich ein Pseudo-Orakel zur Unterstützung von Back-to-Back-Tests eines ML-Modells am BESTEN erstellen?

Wählen Sie EINE Antwort aus!

a)	Durch Variieren der Hyperparameter, die für das Training des zu testenden ML-Modells verwendet werden	☐
b)	Durch Fein-Tuning des zu testenden ML-Modells	☐
c)	Durch Ergänzung des zu testenden ML-Modells um Retrieval-augmentierte Generierung (RAG)	☐
d)	Durch Nutzung eines anderen ML-Entwicklungs-Frameworks als dem, das für das zu testende ML-Modell verwendet wurde	☒

Begründung

a) FALSCH — Die Variation von Hyperparametern stellt eine geringfügige Anpassung desselben ML-Modells dar. Sie verändert das Modell nicht grundlegend. Ein Pseudo-Orakel sollte sich idealerweise deutlich unterscheiden, um Fehlerzustände effektiv zu erkennen. Diese Option ist dem SUT zu ähnlich.

b) FALSCH — Fein-Tuning ist eine Modifikation desselben ML-Modells, die typischerweise ein weiteres Training auf einem spezifischen Datensatz beinhaltet. Es handelt sich nicht um eine ausreichend wesentliche Änderung, um ein wirklich unabhängiges Pseudo-Orakel zu schaffen. Es stützt sich weiterhin auf dasselbe Kernmodell und denselben ML-Framework-Code, was das Risiko gemeinsamer Fehlerzustände erhöht.

c) FALSCH — Retrieval-augmentierte Generierung (RAG) erweitert ein Sprachmodell durch die Integration eines Abrufmechanismus. RAG erhöht zwar die Komplexität, baut aber weiterhin auf dem zu testenden ML-Modell auf. Die grundlegende Architektur und der Trainingsprozess des Basismodells bleiben unverändert. RAG führt zwar eine Abweichung ein, stellt jedoch eher eine Anreicherung des ursprünglichen Modells dar als eine unabhängige Alternative.

d) KORREKT — Die Verwendung eines anderen ML-Entwicklungs-Frameworks für das Pseudo-Orakel bedeutet den Einsatz anderer Bibliotheken, möglicherweise anderer zugrundeliegender Algorithmen oder Algorithmus-Implementierungen sowie einer anderen ML-Entwicklungsumgebung. Diese Option maximiert die Unabhängigkeit des Pseudo-Orakels vom SUT, verringert das Risiko gemeinsamer Fehlerzustände und erhöht die potenzielle Effektivität von Back-to-Back-Tests.

Frage 39	AI-7.1.1	K2	Punkte 1.0

Welche ZWEI der folgenden Szenarien beschreiben ML-Entwicklungsrisiken, die durch die Durchführung von Tests der funktionalen Leistung von ML EFFEKTIV gemindert werden können?

Wählen Sie ZWEI Antworten aus!

a)	Ein Team stellt fest, dass sein ML-Entwicklungs-Framework bei der Verarbeitung großer Datenmengen langsam wird und sogar nicht mehr reagiert	☐
b)	Eine neue Version einer vom ML-Entwicklungs-Framework verwendeten Kernbibliothek scheint dazu zu führen, dass das ML-Modell unerwartete und ungenaue Ergebnisse liefert	☒
c)	Nach einer Neuinstallation benötigt das Entwicklungsteam einen schnellen Test, um festzustellen, ob die wesentlichen Dienste des ML-Entwicklungs-Frameworks korrekt laufen	☐
d)	Ein einzelnes Testergebnis lässt sich während der Auswertung nur schwer reproduzieren und zeigt bei jeder Ausführung leichte Schwankungen in der funktionalen Leistung von ML	☒
e)	Ein Projektleiter muss sich zwischen zwei möglichen Algorithmen entscheiden, basierend auf deren Eignung für die Projektziele	☐

Begründung

a) FALSCH — Dies beschreibt ein Risiko einer schlechten Performanz. Die richtige Abhilfemaßnahme wäre ein Performanztest (Effizienz-Test), der sich von dem Test der funktionalen Leistung von ML (welcher die funktionale Korrektheit bewertet) unterscheidet.

b) KORREKT — Dies beschreibt einen potenziellen Fehler in einer verwendeten Bibliothek. Testen der funktionalen Leistung von ML kann das Modellverhalten bewerten und Anomalien aufdecken, die auf den Fehlerzustand einer neuen, fehlerhaften Bibliothek zurückzuführen sind und zu einer Veränderung der Testergebnisse führen.

c) FALSCH — Dies beschreibt die Notwendigkeit, das Risiko einer fehlerhaften Installation des ML-Entwicklungs-Frameworks zu mindern. Die geeignete Maßnahme hierfür ist das Smoke-Testen, nicht ein vollständiger Test der funktionalen Leistung von ML für die ML-Funktionalität.

d) KORREKT — Dies beschreibt das Risiko einer fehlerhaften Interpretation der Testergebnisse aufgrund des stochastischen Charakters des Lernprozesses. Test der funktionalen Leistung von ML unter Verwendung mehrerer Durchläufe und statistischer Analysen sind die geeignete Maßnahmen zur Risikominderung.

e) FALSCH — Dies beschreibt eine suboptimale Algorithmusauswahl. Die geeignete Maßnahme ist eine Überprüfung der Algorithmus-Eignung oder ein A/B-Test, nicht ein Test der funktionalen Leistung von ML eines einzelnen Algorithmus, der noch nicht ausgewählt wurde.

Frage 40	AI-7.1.2	K2	Punkte 1.0

Welche der folgenden Aussagen beschreibt RICHTIG, wie sich Shadow-Tests von Kanarien-Tests bei der Bereitstellung von ML-Modellen unterscheiden?

Wählen Sie EINE Antwort aus!

a)	Der Shadow-Test beeinflusst die Antworten an echte Benutzer, während beim Kanarien-Test keine echten Benutzer beteiligt sind	☐
b)	Shadow-Tests spiegeln den Datenverkehr wider, ohne die Benutzer zu beeinträchtigen, während der Kanarien-Test auch Ausgaben vom neuen ML-Modell liefert	☒
c)	Kanarien-Tests werden für Performanztests verwendet, während Shadow-Tests hauptsächlich für Komponentenintegrationstests eingesetzt werden	☐
d)	Beim Kanarien-Test werden offline ausgeführte ML-Modelle verglichen, während der Shadow-Test auf der Verwendung von Live-Nutzerdaten basiert	☐

Begründung

a) FALSCH — Hier werden die Rollen beider Testarten vertauscht. Beim Kanarien-Test wird das neue ML-Modell direkt einer kleinen Gruppe echter Benutzer bereitgestellt, während beim Shadow-Test der Live-Traffic im Hintergrund verarbeitet wird, ohne dass die Reaktionen für die Benutzer beeinflusst werden.

b) KORREKT — Shadow-Tests bieten eine risikofreie Möglichkeit, das Verhalten eines neuen ML-Modells mit Produktionsdaten zu beobachten, während beim Kanarien-Test bewusst eine kleine Untergruppe von Benutzern dem neuen Modell ausgesetzt wird, um dessen Leistung und Auswirkungen in der Praxis zu beobachten.

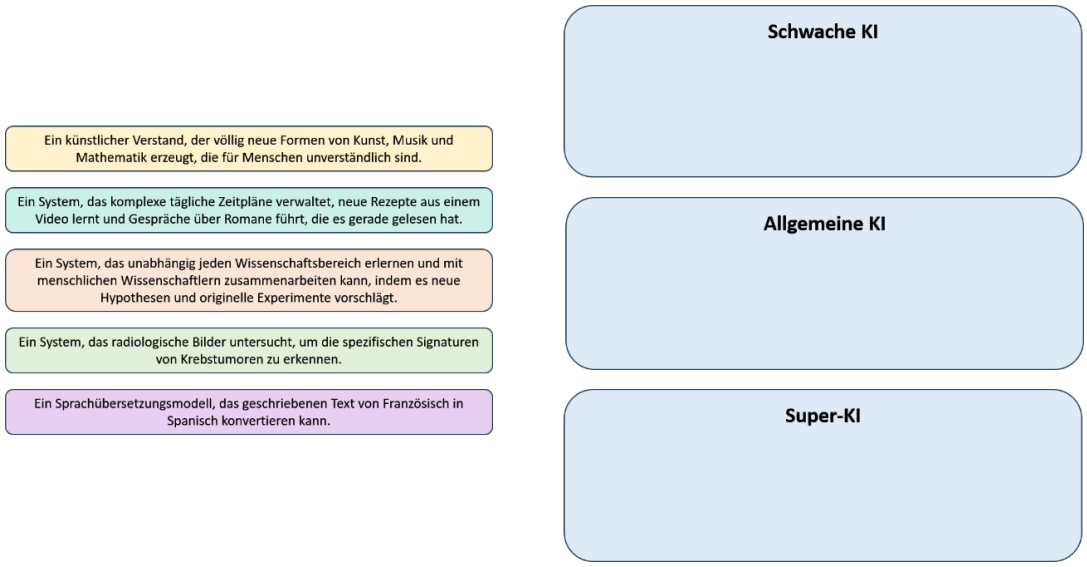
c) FALSCH — Beide Testarten dienen dazu, die Leistung und funktionale Korrektheit eines Modells anhand von Live-Traffic zu validieren. Der Hauptunterschied liegt im Risikoprofil, nicht darin, ob die eine Methode für Performanztests und die andere für Komponentenintegrationstests vorgesehen ist.

d) FALSCH — Hier wird der Kanarien-Test fälschlicherweise als Offline-Aktivität dargestellt. Sowohl der Kanarien-Test als auch der Shadow-Test sind Online-Methoden, die Live-Nutzerdaten verwenden. Der entscheidende Unterschied besteht darin, ob die Antwort des neuen ML-Modells tatsächlich an den Benutzer gesendet oder nur zur späteren Analyse protokolliert wird.

Anhang: Zusätzliche Fragen

Frage A1	KI-1.1.2	K2	Punkte 1.0

Betrachten Sie die folgenden Beispiele für KI-Systeme und die drei verschiedenen Formen von KI:



Aufgabe: Ordnen Sie jedes der aufgeführten KI-Systeme der am BESTEN passenden Form von KI zu. Jeder Form von KI muss mindestens ein Beispiel zugeordnet werden. (Hinweis: bei e-Prüfungen Zuordnung durch Drag & Drop, bei Papierprüfungen durch Linien.)

Begründung

Betrachten wir nacheinander jedes der Beispielsysteme:

• Eine KI, die völlig neue Formen von Kunst, Musik und Mathematik erzeugt, welche für Menschen unverständlich sind.

Dieses System zeigt Kreativität und Intelligenz, die weit über die menschlichen Fähigkeiten hinausgehen, und erzeugt Ergebnisse, die für Menschen nicht nachvollziehbar sind. Solche Fähigkeiten übertreffen sowohl die allgemeine Intelligenz auf menschlichem Niveau als auch die für allgemeine KI (*artificial general intelligence*, AGI) angenommenen Fähigkeiten, weshalb es sich hierbei um ein Beispiel für eine Super-KI handelt.

• Ein System, das komplexe Tagespläne verwaltet, neue Rezepte aus einem Video lernt und Gespräche über gerade gelesene Romane führt.

Diese KI führt eine Vielzahl komplexer Aufgaben aus, die Lernen, Wahrnehmung, Planung und Sprachverständnis erfordern und mit der Vielseitigkeit eines Menschen vergleichbar sind. Sie zeigt Anpassbarkeit und Kompetenz in neuen Bereichen. Somit handelt es sich um ein Beispiel für AGI.

• Ein System, das sich selbstständig in jedes wissenschaftliche Fachgebiet einarbeiten und mit menschlichen Wissenschaftlern zusammenarbeiten kann, indem es neue Hypothesen und originelle Experimente vorschlägt.

Dieses System ist in der Lage, mehrere wissenschaftliche Disziplinen autonom und mit Flexibilität zu beherrschen und kreative Forschung zu betreiben. Seine Kompetenz umfasst Lernen, Schlussfolgern und innovatives Denken auf dem Niveau eines menschlichen Experten. Somit ist es ein Beispiel für AGI.

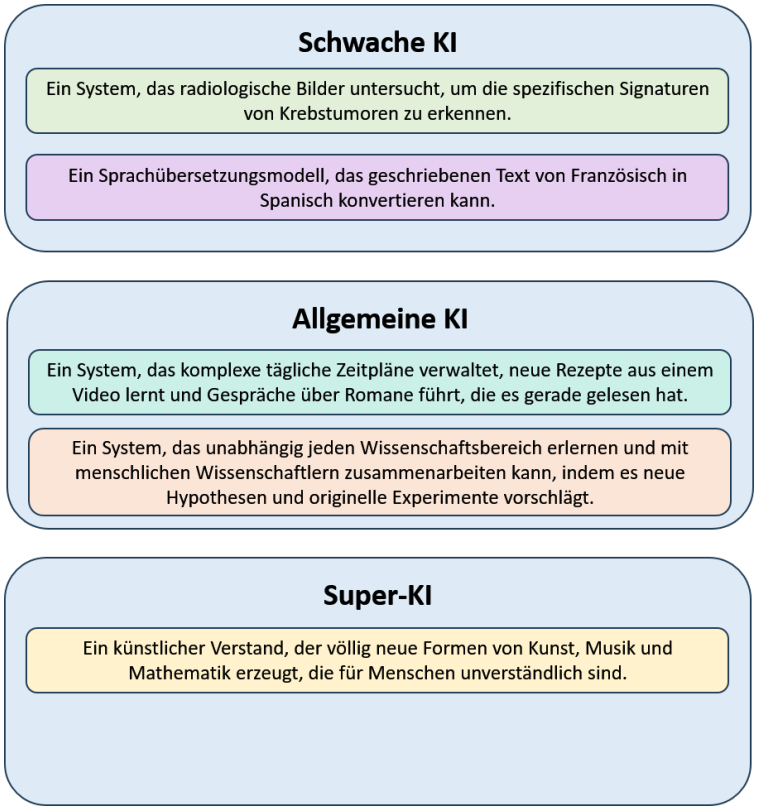
• Ein System, das radiologische Bilder untersucht, um spezifische Merkmale von Krebstumoren zu erkennen.

Diese KI zeichnet sich durch die Bewältigung einer klar definierten, spezialisierten Aufgabe (medizinische Bildanalyse) aus, ohne über ein umfassenderes Verständnis oder Fähigkeiten außerhalb ihres Fachgebiets zu verfügen. Ihre Anwendung beschränkt sich auf die Mustererkennung innerhalb radiologischer Daten und erstreckt sich nicht auf allgemeine Kognition. Somit handelt es sich um ein Beispiel für eine schwache KI.

• Ein Sprachübersetzungsmodell, das schriftlichen Text vom Französischen ins Spanische übersetzen kann.

Dieses Modell ist darauf ausgelegt, eine einzige Funktion auszuführen – die Übersetzung zwischen zwei Sprachen. Es verfügt über Fachkompetenz bei einer abgegrenzten Aufgabe und besitzt kein umfassendes Verständnis oder Anpassbarkeit über die Sprachkonvertierung hinaus. Somit handelt es sich um ein Beispiel für eine schwache KI.

Die KORREKTE Lösung ist demnach:



Frage A2	AI-1.1.7	K2	Punkte 1.0

Welche der folgenden Optionen beschreibt am BESTEN einen Vorteil der Verwendung von ML-Entwicklungs-Frameworks bei der Entwicklung und beim Training von ML-Modellen?

Wählen Sie EINE Antwort aus!

a)	Sie bieten Unterstützung beim Entwerfen der Architektur des ML-Modells, beispielsweise der Struktur eines Entscheidungsbaums	☒
b)	Sie machen eine Datenvorverarbeitung überflüssig, indem sie die Daten vor dem Training automatisch optimieren	☐
c)	Sie erfordern, dass alle Datenwissenschaftler, die sie nutzen, fortgeschrittene Programmierer mit fundierten Programmierkenntnissen sind	☐
d)	Sie machen die Modellentwicklung sehr effizient, binden jedoch die entwickelten ML-Modelle an das ML-Entwicklungs-Framework	☐

Begründung

a) KORREKT — Die Modellerstellung ist eine Schlüsselfunktion, und ML-Entwicklungs-Frameworks bieten „Werkzeuge zur Definition der Architektur des ML-Modells“, einschließlich der Möglichkeit, die Struktur des ML-Modells, wie beispielsweise einen Entscheidungsbaum, festzulegen.

b) FALSCH — Das Wort „eliminieren“ ist übertrieben. ML-Entwicklungs-Frameworks unterstützen die Datenvorverarbeitung, machen sie jedoch nicht überflüssig. Die Datenverarbeitung ist eine unterstützende Funktion, die keine vollständige Automatisierung durchführt und die Aufgabe somit nicht eliminiert.

c) FALSCH — ML-Entwicklungs-Frameworks existieren auf verschiedenen Abstraktionsebenen, darunter „eine übergeordnete API, die die Modellerstellung vereinfacht“. Dies deutet darauf hin, dass Programmierkenntnisse keine allgemeine Anforderung sind und die Auswahl des Frameworks von der „Fachkompetenz der Benutzer“ abhängt.

d) FALSCH — Es ist nicht richtig, dass ML-Entwicklungs-Frameworks entwickelte ML-Modelle an dieses Framework binden. Im Allgemeinen können alle entwickelten ML-Modelle (im Rahmen des Zumutbaren) überall bereitgestellt werden.

Frage A3	AI-1.1.8	K2	Punkte 1.0

Ein Unternehmen entwickelt ein KI-basiertes System zur Steuerung eines vollständig autonomen Fahrzeugs, ohne die damit verbundenen Risiken zu berücksichtigen.

Welche der folgenden Normen und Standards bzw. Regulierungen wird in diesem Szenario am WAHRSCHEINLICHSTEN verletzt?

Wählen Sie EINE Antwort aus!

a)	ISO/IEC/IEEE TR 29119-11	☐
b)	OECD-KI-Grundsätze	☐
c)	KI-Verordnung der EU	☒
d)	ISO/IEC 25059	☐

Begründung

a) FALSCH — Bei ISO/IEC/IEEE TR 29119-11 geht es nicht um das Testen von KI, sondern wie bei allen Normen um die Bereitstellung von Leitlinien, und es werden keine Sanktionen bei Nicht-Konformität verhängt.

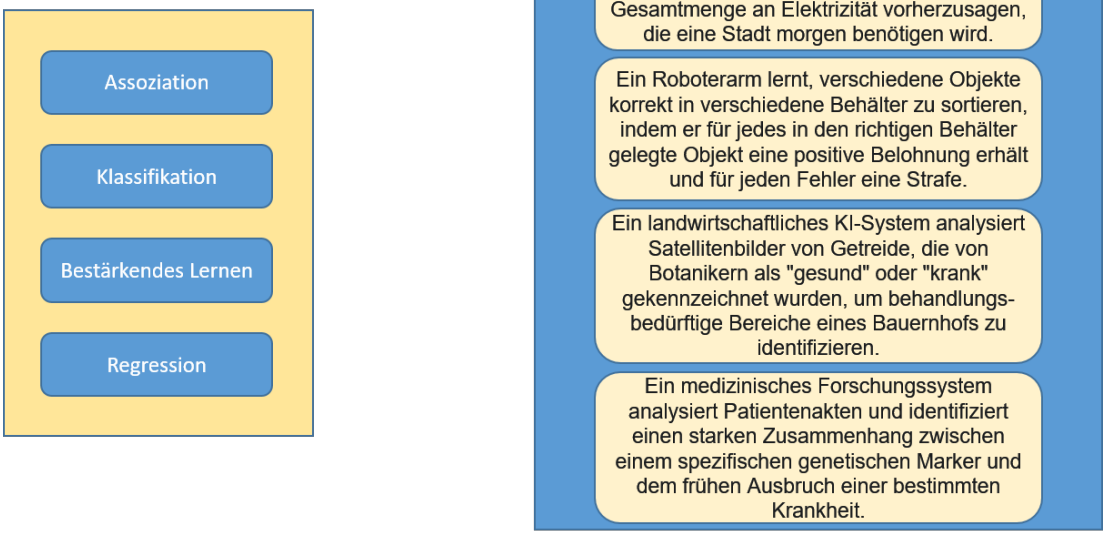
b) FALSCH — Die OECD-KI-Grundsätze sind nicht verbindlich.

c) KORREKT — Wenn das System unter die KI-Verordnung der EU fällt (d. h., wenn es in Europa genutzt wird), kann die Nichtbeachtung eines risikobasierten Ansatzes zu schweren Strafen führen.

d) FALSCH — ISO/IEC 25059 beschreibt die spezifischen Qualitätsmerkmale von KI-Systemen, bietet jedoch – wie alle Normen – lediglich Leitlinien und sieht keine Sanktionen bei Nicht-Konformität vor.

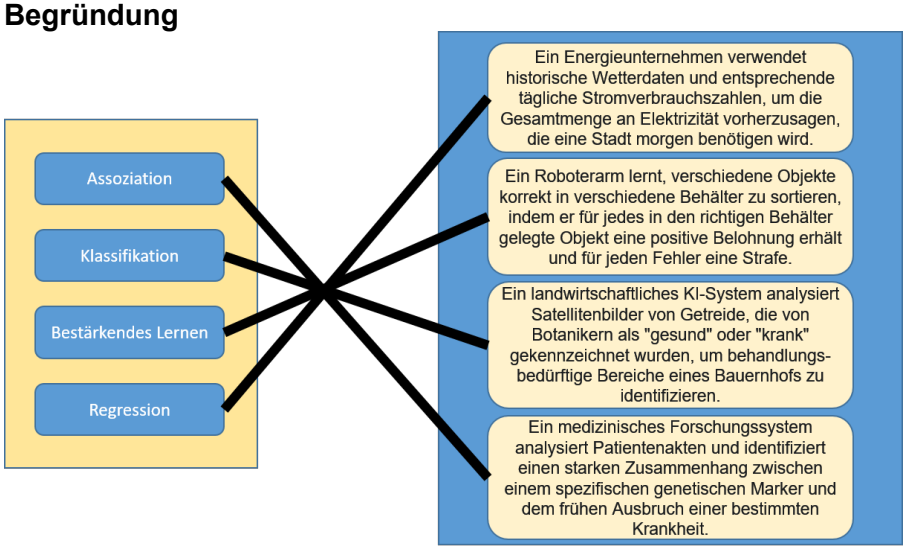
Frage A4	AI-3.1.1	K2	Punkte 1.0

Betrachten Sie die folgenden Arten bzw. Aufgaben des maschinellen Lernens (ML) und die folgenden Beispiele für ML-Systeme:



Aufgabe: Ordnen Sie jede Art bzw. Aufgabe von ML dem am BESTEN passenden Beispiel-ML-System zu! (Hinweis: Bei ePrüfungen Zuordnung durch Drag & Drop, bei Papierprüfungen durch Linien.)

Begründung



Die Zuordnung erfolgt anhand der Beschreibungen der Beispiel-ML-Systeme in der Reihenfolge der Arten bzw. Aufgaben von ML von oben nach unten:

• Assoziation – Dieses System nutzt Assoziation, indem es (ungekennzeichnete Rohdaten aus) Patientenakten auswertet, um Abhängigkeiten zwischen verschiedenen Attributen, wie beispielsweise einem Gen und einer Krankheit, zu identifizieren. Es sagt keine Klasse voraus, sondern deckt stattdessen die Stärke der Beziehung zwischen Variablen innerhalb der Daten auf.

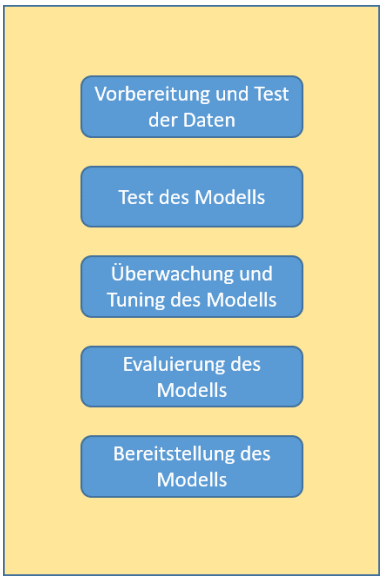
• Klassifikation – Das System lernt aus einem Datensatz von Bildern, die zuvor mit diskreten Kategorien („gesund“ oder „erkrankt“) gekennzeichnet wurden. Sein Zweck besteht darin, neue Bilder einer dieser spezifischen, nicht-numerischen Klassen zuzuordnen, wodurch es sich von der Regression unterscheidet.

• Bestärkendes Lernen – Das System lernt durch direkte Interaktion mit seiner physischen Umgebung und nicht anhand eines bereits vorhandenen Datensatzes. Das Verhalten des Roboters wird im Laufe der Zeit durch ein System aus Belohnungen (für korrekte Platzierung) und Strafen (für falsche Platzierung) geprägt.

• Regression – Das ML-Modell wird anhand von gekennzeichneten Daten trainiert, um einen bestimmten, kontinuierlichen numerischen Wert vorherzusagen, nämlich die Strommenge. Die Ausgabe des Modells ist keine Kategorie, sondern eine Größe auf einer Skala, was das Hauptmerkmal der Regression ist.

Frage A5	**AI-3.1.2**	**K2**	**Punkte 1.0**

Gegeben sind die folgenden Aktivitäten des ML-Workflows:

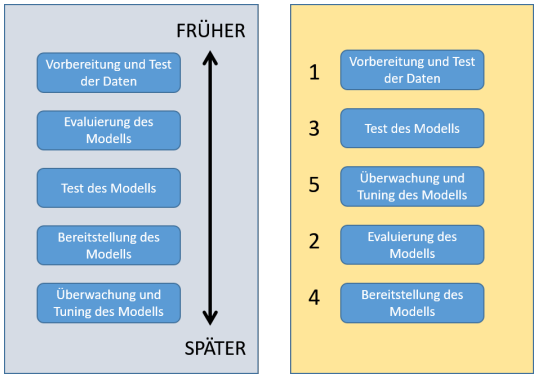


Aufgabe: Ordnen Sie diese Aktivitäten in der am BESTEN zum ML-Workflow passenden logischen Reihenfolge von der frühesten (oben) zur spätesten Aktivität (unten) an. (Hinweis: Bei ePrüfungen Verschieben durch Drag & Drop, bei Papierprüfungen durch Nummerierung.)

Begründung

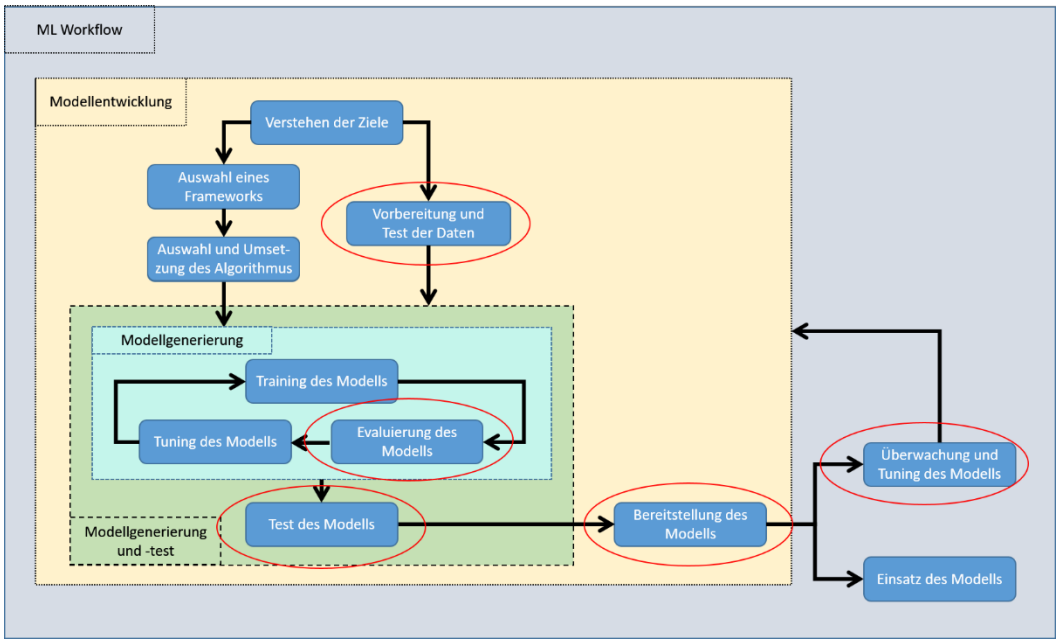
Korrekte Antwort

Die logische Reihenfolge von der frühesten zur spätesten Aktivität im ML-Workflow ist:



Erläuterung/Begründung

Vgl. Lehrplan Abbildung 1: ML-Workflow:



Frage A6	AI-3.4.3	K2	Punkte 1.0

Was ist ein wesentlicher Grund dafür, dass strukturelle Überdeckung allein als Grundlage für das Testen neuronaler Netze NICHT AUSREICHEND ist?

Wählen Sie EINE Antwort aus!

a)	Strukturelle Überdeckung neigt dazu, die Leistung bei Aufgaben mit menschlichem Feedback zu überschätzen	☐
b)	Strukturelle Überdeckung kann beim Vergleich von Testergebnissen Unterschiede in der Modellgröße nicht berücksichtigen	☐
c)	Strukturelle Überdeckung zeigt nicht, ob sich das Netz auf irreführende oder irrelevante Merkmale stützt	☒
d)	Durch strukturelle Überdeckung entfällt die Notwendigkeit, die Aussagekraft einzelner Modellergebnisse zu bewerten	☐

Begründung

a) FALSCH — Die zentrale Einschränkung liegt in der Art der internen Entscheidungsfindung des Modells, einem allgemeinen Problem, das auf viele Aufgaben zutrifft, nicht speziell auf solche, die menschliches Feedback beinhalten.

b) FALSCH — Die strukturelle Überdeckung ist eine Methode zur Bewertung der Testvollständigkeit eines einzelnen Modells, nicht zum Vergleich verschiedener Modelle. Zwar kann die Modellgröße die reinen Überdeckungszahlen beeinflussen, doch werden die berechneten Werte in der Regel als Prozentsätze dargestellt, weshalb dies für den beabsichtigten Zweck keine Einschränkung darstellt.

c) KORREKT — Es geht direkt auf die wesentlichen Einschränkungen von Messungen der Überdeckung ein, die isoliert verwendet werden. Neuronale Netze können Scheinkorrelationen erlernen, was zu korrekten Aktivierungen aus falschen Gründen führt; das bedeutet, dass das Modell eine hohe strukturelle Überdeckung erreichen könnte, während es Entscheidungen auf der Grundlage irrelevanter Merkmale trifft.

d) FALSCH — Die strukturelle Überdeckung ist eine wertvolle Ergänzung, die mit anderen Methoden kombiniert werden sollte. Sie soll andere Testaktivitäten, wie z. B. die Bewertung der funktionalen Korrektheit und der Nützlichkeit der Modellausgaben, ergänzen, nicht ersetzen.