embraceableAI

Warum KI-Systeme ein professionelles Konfigurations- und Lebenszyklus- Management brauchen

> Wie klare Versionierung, Transparenz und Governance aus einem Experiment ein produktives System machen.

Einführung: Zwei Chatbot-Antworten – zwei Risiken

Stellen Sie sich vor, Sie stellen einem unternehmensinternen Chatbot dieselbe geschäftskritische Frage an zwei aufeinanderfolgenden Tagen – und erhalten zwei völlig unterschiedliche Antworten. Am ersten Tag leitet Sie das System zu einem bestimmten Entscheidungsweg. Am nächsten Tag rät es Ihnen vom selben Vorgehen ab.

Was ist passiert? Wurde das zugrunde liegende Modell verändert? Wurden Parameter angepasst? Oder wurde die Wissensbasis aktualisiert – ohne dass Sie es wissen? Genau hier beginnt das Problem: Ohne klare Transparenz über Konfiguration und Änderungen ist jede KI-Antwort ein Blindflug. Und je kritischer die Entscheidung, desto größer das Risiko.

Das unterschätzte Problem: KI ist keine klassische Software

KI-Anwendungen, insbesondere solche mit generativen Modellen oder Multi-Agent-Strukturen, sind keine einfachen Programme. Sie bestehen aus einer Vielzahl von Bestandteilen, die sich schnell und oft unbemerkt ändern können:

- Modellvarianten (z. B. GPT-4, LLaMA 3, Mistral),
- Prompt-Design und Agenten-Rollen,
- Konfigurationsparameter wie Temperatur oder Top-k,
- Wissensquellen, Vector Stores und Retrieval-Strategien.

Jede kleine Änderung kann das Verhalten der KI verändern. Ohne strukturierte Versionierung und Konfigurationsmanagement sind Nachvollziehbarkeit, Reproduzierbarkeit und Rechtskonformität nicht möglich. Was bei klassischen Software-Systemen längst Standard ist, fehlt heute in vielen KI-Projekten noch vollständig.

embraceableAI

Unkontrollierter KI-Agenten-Einsatz: Wenn aus Innovation Kontrollverlust wird

Der Trend zu Multi-Agent-Systemen verschärft die Lage. Moderne KI-Anwendungen bestehen nicht mehr aus einem einzigen System, sondern aus Dutzenden spezialisierten Agenten, die miteinander kommunizieren. Jeder Agent basiert auf:

- eigener Modellkonfiguration,
- individueller Funktionslogik (z.B. mit Function Calling),
- eigener Wissensbasis,
- spezifischer Parametern

Fehlt ein systematisches Management, entstehen schnell folgende Risiken:

Agent Sprawl
Unkontrolliertes Wachstum von Agenten ohne zentrale Steuerung,

Knowledge Sprawl
Widersprüchliche Datenlagen durch unsynchronisierte Wissensquellen,

Configuration Drift
Inkonsistente Umgebungen zwischen Test, Staging und Produktion.

Monitoring-Tools können diese Probleme höchstens im Nachhinein sichtbar machen – aber sie verhindern sie nicht. Präventive Governance muss an der Quelle ansetzen: bei der Erstellung, Konfiguration und Freigabe der Agenten.

embraceableAI

embraceableAI

Die Lösung:
Service Management für KI

Was IT-Service-Management (ITSM) für klassische Systeme leistet, übernimmt SM4AI (Service Management for AI) für moderne KI-Anwendungen.
Das Ziel: Struktur, Kontrolle und Nachvollziehbarkeit von Anfang an.

Ein SM4AI-konformes System bietet:

Versionierung aller KI-relevanten Komponenten (Prompts, Modelle, Retrieval-Strategien etc.),

Lifecycle-Management für Agenten und ihre Abhängigkeiten,

Change-Management für Wissensquellen und externe Tools,

Freigabeprozesse und Audit-Trails für produktive KI-Systeme.

Damit wird aus einer KI-Anwendung ein beherrschbares, rechtssicheres System – und nicht ein Experiment mit unbekannten Variablen.

So setzt embraceableAI dieses Prinzip um

Die embraceable Plattform begegnet dem Problem mit einem konsequent strukturierten Ansatz:

Versionierbare Konfiguration statt flüchtiger Laufzeitparameter

Jede Konfiguration – vom Prompt bis zur Wissensquelle – wird als versionierbares Objekt behandelt. Änderungen erzeugen Revisions-Events, die in einem Event Store dokumentiert werden. Diese Events sind atomar, rückverfolgbar und auditierbar – egal, ob es sich um einen System-Prompt oder eine Änderung der Chunk-Größe im Retrieval handelt.

Deterministische Anwendungskonfiguration

Eine konkrete KI-Anwendung ist immer die Komposition eindeutig referenzierter Artefakte. Ihre Identität ergibt sich aus Revisions-IDs. Änderungen an Komponenten führen nicht automatisch zu neuen Versionen, sondern erfordern eine bewusste Rekombination und Freigabe.

Systemische Transparenz von Anfang an

Der Ansatz der embraceable Plattform verlagert Verantwortung vom späteren Monitoring auf die Designphase. So wird jede Entscheidung dokumentiert – und nicht erst analysiert, wenn etwas schiefläuft.

Fazit: Wer KI auf kontrollierte und steuerbare Art nutzen will, sollte sich embraceableAI ansehen

Der Übergang von Pilotprojekten zu produktiven KI-Anwendungen verlangt mehr als nur leistungsfähige Modelle. Er verlangt Struktur, Steuerbarkeit und Verantwortung. Genau das liefert die Idee, Grund-Prinzipien des IT-Service-Management auf KI-Systeme zu übertragen und zu erweitern – und die embraceable Plattform zeigt, wie es geht:

- Jede Applikation ist **klar versioniert**
- Jede Konfiguration ist **dokumentiert**
- Jede Änderung ist **nachvollziehbar**

So wird KI nicht nur leistungsfähig, sondern auch vertrauenswürdig – und strategisch steuerbar.

KI sicher & effektiv?

Wir zeigen Ihnen, wie man KI in Unternehmen & Behörden sicher & effektiv einsetzen kann.

embraceableAI (und die dahinterstehende embraceable Technology GmbH) ist ein deutsches Software- und KI-Unternehmen, das 2018 mit der Mission gegründet wurde, Künstliche Intelligenz alltagstauglich und praxisnah in den Business-Kontext zu integrieren. Ein interdisziplinäres Team aus KI-Spezialisten sowie Cloud- und Software-Ingenieuren entwickelt leistungsstarke und zuverlässige Lösungen, inspiriert von biologischen Prinzipien. Die Technologie unterstützt Unternehmen dabei, Routineaufgaben zu automatisieren, komplexe Abläufe effizienter zu gestalten und Innovationen schneller voranzutreiben.

Redaktionell verantwörtlich

Dr.-Ing. Christian Gilcher
Telefon: +49-721-9861-7690
E-Mail: info@embraceable.ai