

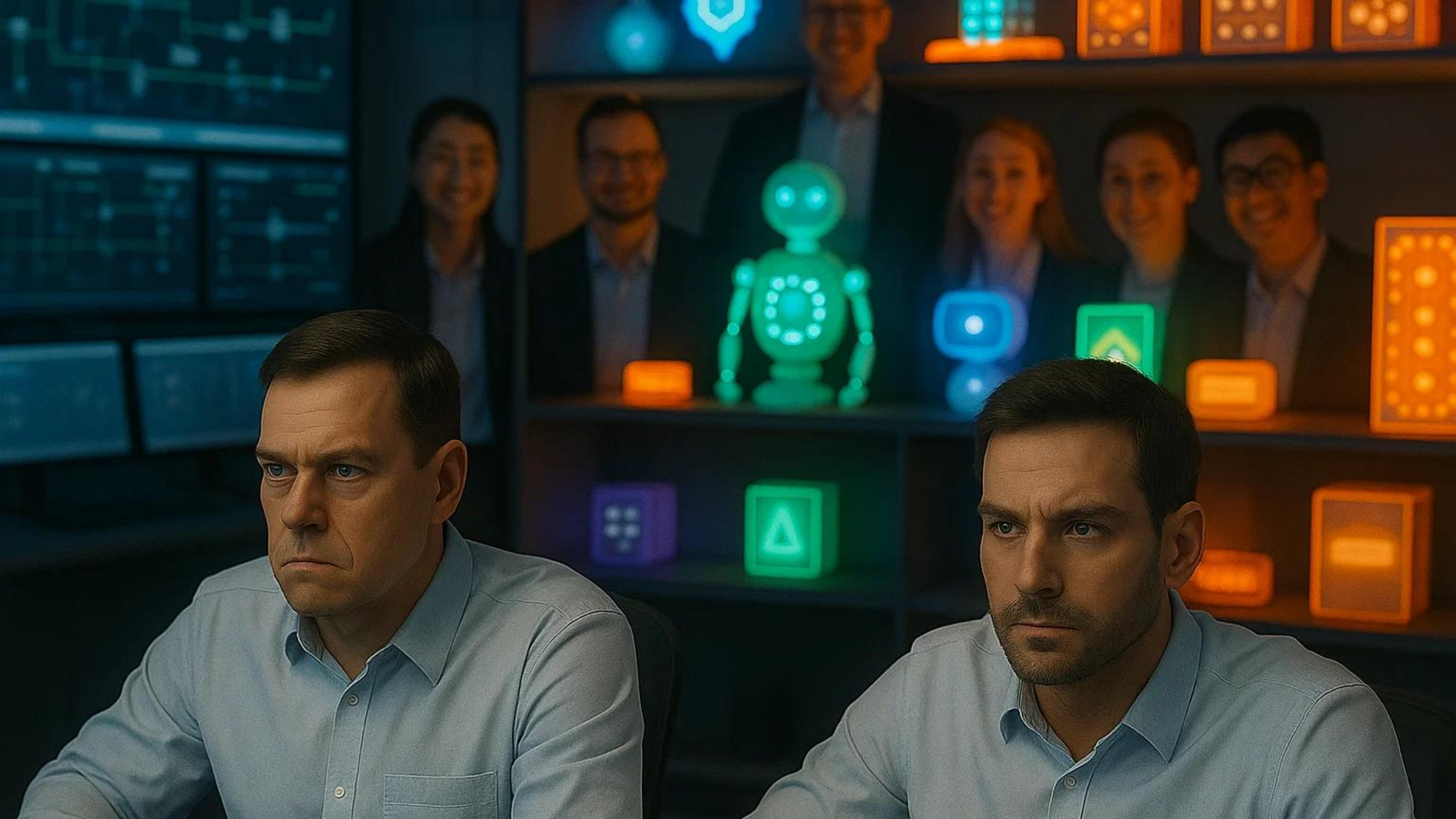


# Bereit für KI?

## Über die Projektierung von KI- Anwendungen

Dr. Andreas Kubis, c.con Management Consulting GmbH





**KI-Prototypen zeigen technische Machbarkeit, aber selten betriebliche Tragfähigkeit.**

*Mitten in der Leitwarte, aber nicht im Betrieb*



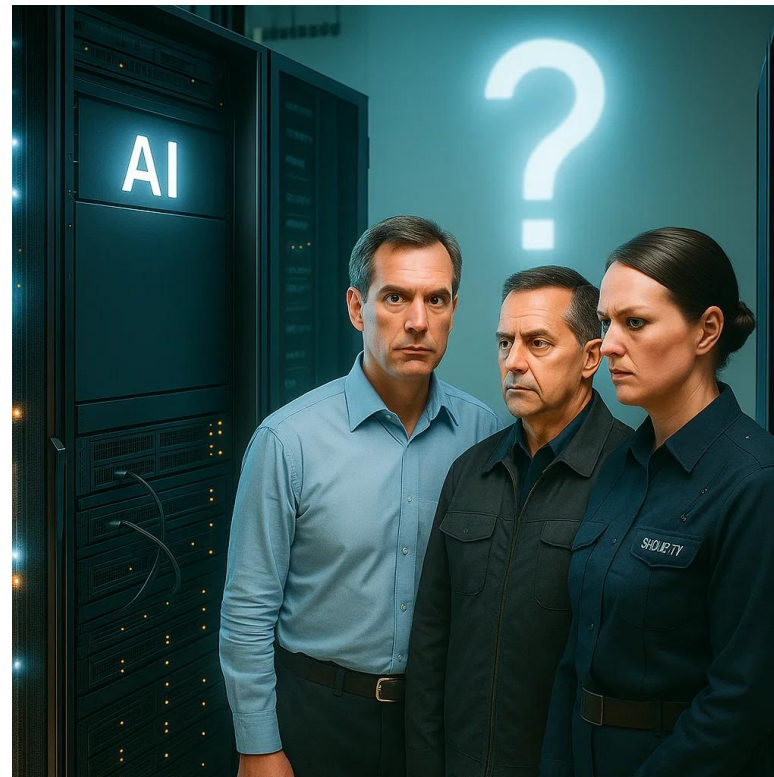
**Zwischen Entwicklung, Sichtbarkeit und Applaus entsteht das Bild eines Erfolgs.**

## Wie KI-Projekte erfolgreich werden

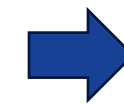


## Zwischen KI-Pilot und Betrieb klaffen Lücken, an Schnittstellen, in Prozessen und in der Verantwortung.

### Was im Betrieb *wirklich* passiert



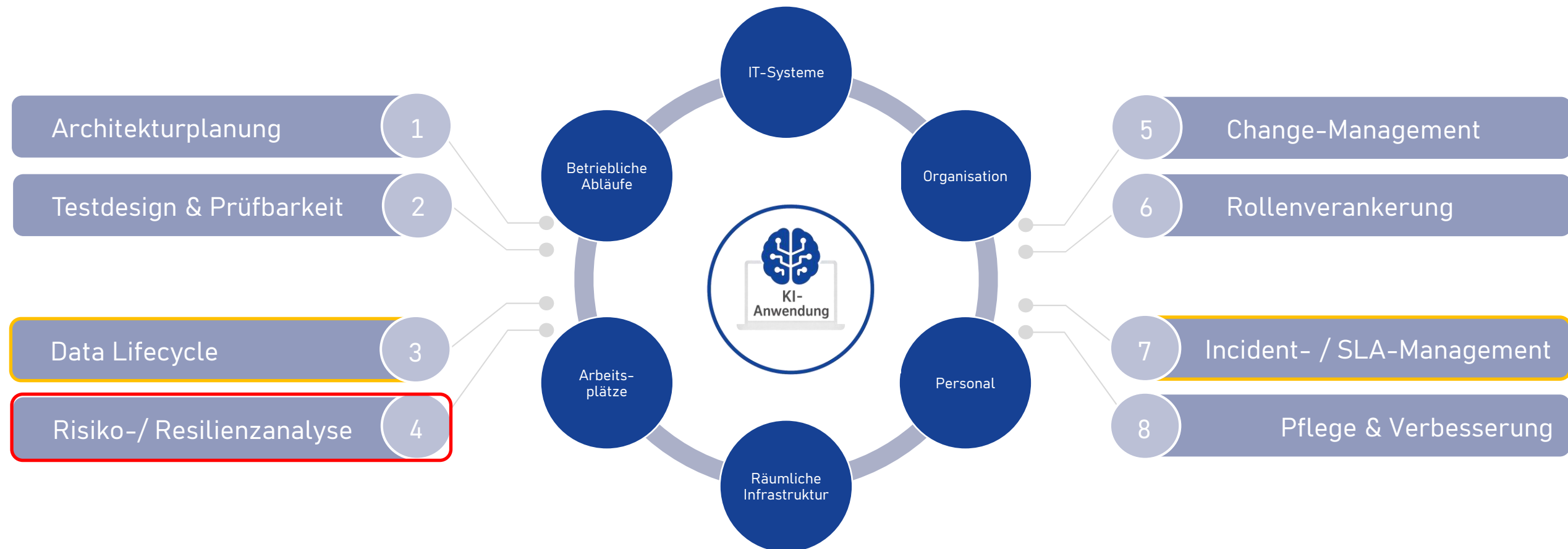
- Der Betrieb erfordert mehr:
  - Rollenmodelle
  - Prozessintegration
  - Monitoring, IT-Betriebsprozesse
  - Sicherheitsarchitektur
  - Prozesse zur Pflege und Bewertung
  - Service Level Agreements
  - **Change-Management**



Kein Übergang in den Regelbetrieb

**Die Defizite sind nicht technisch.**

## Diese acht Faktoren entscheiden über Betriebsfähigkeit von KI



## Risikoklassen nach AI Act und einhergehende Betreiberpflichten

### Unacceptable Risk

KI-Anwendungen, die Menschen manipulieren, diskriminieren oder in unzulässiger Weise überwachen

- Einsatz grundsätzlich verboten

### High Risk

KI-Anwendungen, die sicherheitskritische oder betriebsrelevante Entscheidungen beeinflussen – direkt, automatisiert und **ohne menschliche Validierung\***.

**\*Grenzfall:** wenn KI-Einflussnahme auf Entscheidung vorliegen könnte

- **Zweckbindung**
- Monitoring & Systemkontrolle
- Protokollierung & Dokumentation (Aufbewahrungspflichten!)
- Meldepflicht bei Vorfällen
- Menschliche Aufsicht
- Risikobewertung

### Limited Risk

KI-Anwendungen mit funktionalem Einfluss auf Entscheidungen, bei denen jedoch menschliche Aufsicht oder manuelle Verarbeitung vorgesehen ist.

- **Zweckgemäßer** Einsatz
- Nutzerinformation & Aufklärung
- Kennzeichnungspflicht

### Minimal Risk

KI-Anwendungen ohne Einfluss auf Echtzeit- oder Entscheidungsprozesse

- Datenschutz (DSGVO)

**Ob eine KI-Anwendung als hoch, begrenzt oder minimal riskant gilt, hängt nicht davon ab, was sie tut, sondern davon, wie sie in betriebliche Prozesse eingreift.**

Beispielanwendung:  
**Prognosen im Netzbetrieb**

**Unacceptable Risk**

**High Risk**



z. B. im Bilanzkreis- und Fahrplanmanagement, Netzzustandserfassung, ...

Automatisierte Erstellung von Fahrplänen und/oder Ersatzwerten

**unmittelbarer Einfluss auf Entscheidung/Prozess**

**Limited Risk**



z. B. manueller Prognoseanstoß im Leitsystem

Erhöhung der Situational Awareness

**mittelbarer Einfluss auf Entscheidung/Prozess**

**Minimal Risk**



z. B. Offline-Analysen

Beistellung von Informationsgrundlagen für nachgelagerte Entscheidungsprozesse

**indirekter Einfluss auf Entscheidung / Prozess**

## Fallbeispiel: KI-gestütztes Assistenzsystem für die souveräne Beherrschung unvorhergesehener Systemzustände

### Szenario:

- Das Verbundsystem gerät aufgrund einer unvorhergesehenen Störung in den gestörten Betrieb.
- Die Systemführung muss die Situation stabilisieren und das System in einen sicheren Betriebspunkt zurückführen.
- Das KI-System ist designed, um Systemführern situationsadäquate Maßnahmen vorzuschlagen.

### Wirkmöglichkeiten des Assistenzsystems:

- Das Assistenzsystem besitzt vollständigen Lese-Zugriff auf das Prozessdatenmodell des Leitsystems und nutzt dieses als Datengrundlage.
- Das Assistenzsystem wird im Open-Loop betrieben. Es ist also technisch unfähig Maßnahmen eigenständig zu veranlassen.
- Ausschließlich textuelle und visuelle Orientierung



**Fällt das „KI-gestützte Assistenzsystem für die souveräne Beherrschung unvorhergesehener Systemzustände“ unter die „High-Risk“-Kategorie des AI Act?**

## Nicht das Systemverhalten entscheidet über das Risiko, sondern seine Wirkung auf kritische Entscheidungen unter Unsicherheit.

### Technische Sicht:

- Kein automatischer Eingriff
- Open-Loop, d.h. keine technische Eingriffsmöglichkeit des Systems
- Mensch behält vollständig Entscheidungsverantwortung
- Keine personenbezogenen Daten o. ä.



### Funktionale Sicht:

- Systemführer orientieren sich an Vorschlägen
- Handlungspfad wird in kritischen Situationen maßgeblich von KI-Empfehlung beeinflusst
- System kann kognitiven Bias erzeugen
- Eingeschränkte Validierbarkeit der KI bei „Untrained Scenarios“

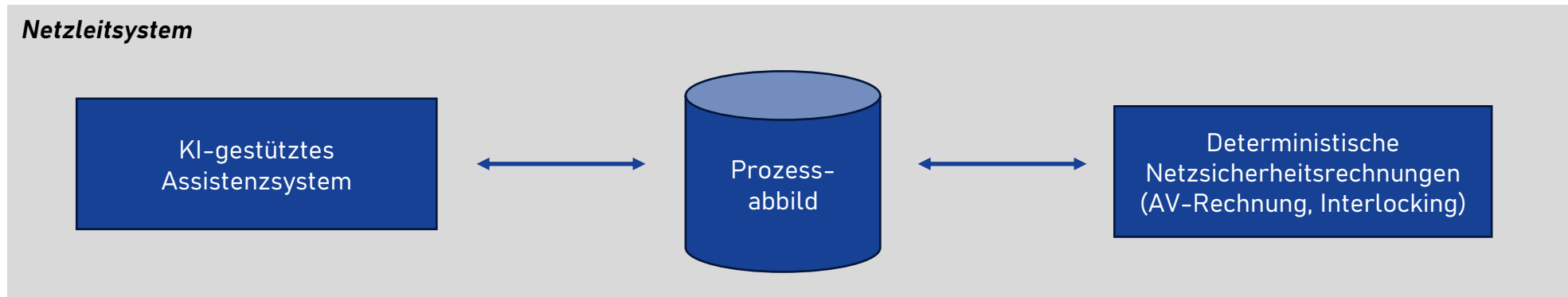


- Einordnung
  - Technisch betrachtet ist das System kein High-Risk-System
  - Funktional betrachtet wirkt das System entscheidungsleitend in sicherheitskritischen Situationen und ist somit High-Risk
- Fazit
  - Die Klassifizierung allein anhand technischer Merkmale greift zu kurz
  - Die tatsächliche Risikowirkung ergibt sich aus Kontext, Nutzung und Vertrauen

## KI benötigt keine perfekte Fehlerquote, sondern eine Architektur, die Fehler systematisch begrenzt und sicher beherrscht.

- Warum funktionale Sicherheit bei KI nötig ist:
  - KI-Systeme sind nicht deterministisch. **Fehler sind wahrscheinlich**, nicht außergewöhnlich
  - **Klassische Testabdeckung funktioniert nicht** bei untrainierten Zuständen
  - **Vertrauen** in das Modell **schützt nicht** vor systemischem Fehlverhalten
  - **Architektur ersetzt Kontrolle**: Begrenzung von Wirkung statt Annahme von Perfektion
- Was funktionale Sicherheit ermöglicht:
  - **Fehler beherrschbar machen**: Auch bei Fehlfunktionen darf kein gefährlicher Systemzustand entstehen.
  - **Sicheres Zurückführen**: Bei Unsicherheit muss das System kontrolliert und zuverlässig in einen sicheren Zustand überführt werden können.
  - **Technische Schutzgrenzen definieren**: Interlock-Mechanismen verhindern ungewollte oder unkontrollierte Eingriffe der KI.
  - **Systemtransparenz sichern**: Mensch und Maschine müssen Zustand, Wirkung und Grenzen der KI jederzeit nachvollziehen können.

**KI wird nicht dann sicher, wenn sie alles richtig macht, sondern wenn sie nichts Gefährliches machen kann.**



## Technische Sicht:

- Kein automatischer Eingriff
- Open-Loop, d.h. keine technische Eingriffsmöglichkeit des Systems
- Mensch behält vollständig Entscheidungsverantwortung
- Keine personenbezogenen Daten o. ä.



## Funktionale Sicht:

- Systemführer orientieren sich an Vorschlägen
- Handlungspfad wird in kritischen Situationen maßgeblich von KI-Empfehlung beeinflusst
- System kann kognitiven Bias erzeugen
- **Fehlschaltungen und Verschlimmernde Situationen werden über funktionale Sicherheit ausgeschlossen**





## Schlüsselbotschaften

- 1** Technik ≠ Betrieb: Governance, Prozesse und Zuständigkeiten entscheiden über Tragfähigkeit.
- 2** High-Risk? Kontext, Wirkung und Vertrauen zählen mehr als technische Details.
- 3** Sicherheit ≠ Modellvertrauen: Ohne Architektur keine Beherrschbarkeit.
- 4** Funktionale Sicherheit wirkt: Interlocks, Fail-Safes und Rollenverankerungen sind betrieblich erforderlich.
- 5** Verantwortung statt Hoffnung: Sicherheit entsteht durch Struktur, nicht durch Vertrauen.



Ahead with energy





---

Ihr Ansprechpartner

---

Dr. Andreas Kubis

c.con Management Consulting GmbH

andreas.kubis@ccon.com

 [Profil](#)

