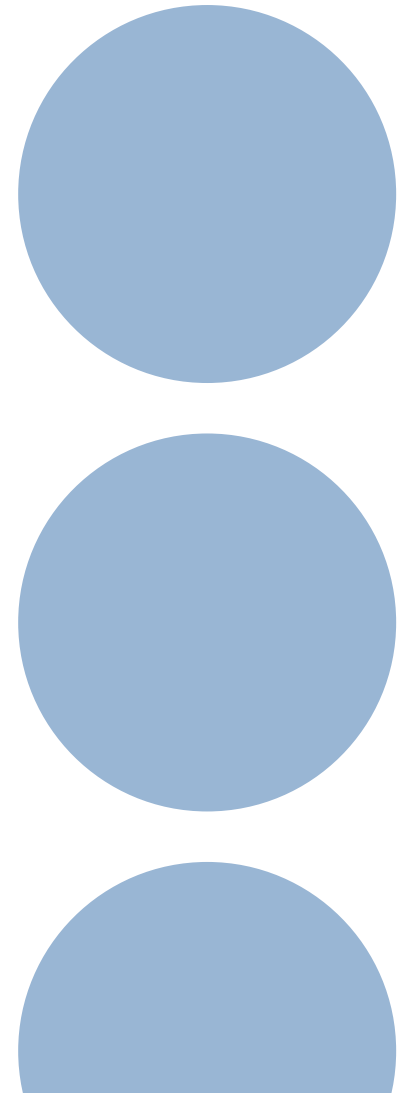


„Self-evolving behavior“: Anforderungen an KI gemäß MVO und KI-Verordnung

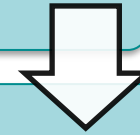
Schnittstellenbetrachtung

Fachveranstaltung Maschinen
S. Granderath, 30.06.2026

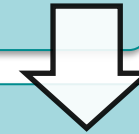


Übersicht

KI in der Praxis



Rahmenbedingungen der MVO



Schnittstelle KI-VO



Normung und Fristen

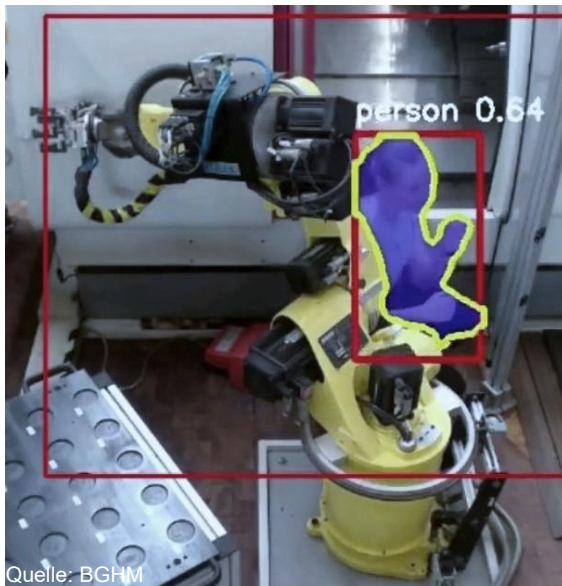
KI in der betrieblichen Realität

Zunehmende Nutzung von KI zur Prozessüberwachung, Steuerung und in Assistenzsystemen:



Beispiel: Personenerkennung

Solche Systeme werden zunehmend in sicherheitsrelevanten Anwendungen eingesetzt. Heute meist als Assistenzsystem, künftig auch in Sicherheitsfunktionen.



Ein KI-basiertes Personenerkennungssystem kann:

1. definierte Gefahrenbereiche **überwachen**,
2. Personen im Gefahrenbereich **erkennen**,
3. eine Reaktion **auslösen** (z. B. Roboterstopp).

Nennung in der Maschinenverordnung (MVO)

Vorgaben aus Anhang 1, Teil A, Nr. 5 und 6

Betrachtet Sicherheitsbauteile, die „**self-evolving**“ Systeme beinhalten.

Auf deutsch: *„mit vollständig oder teilweise selbstentwickelndem Verhalten unter Verwendung von Ansätzen des maschinellen Lernens“.*

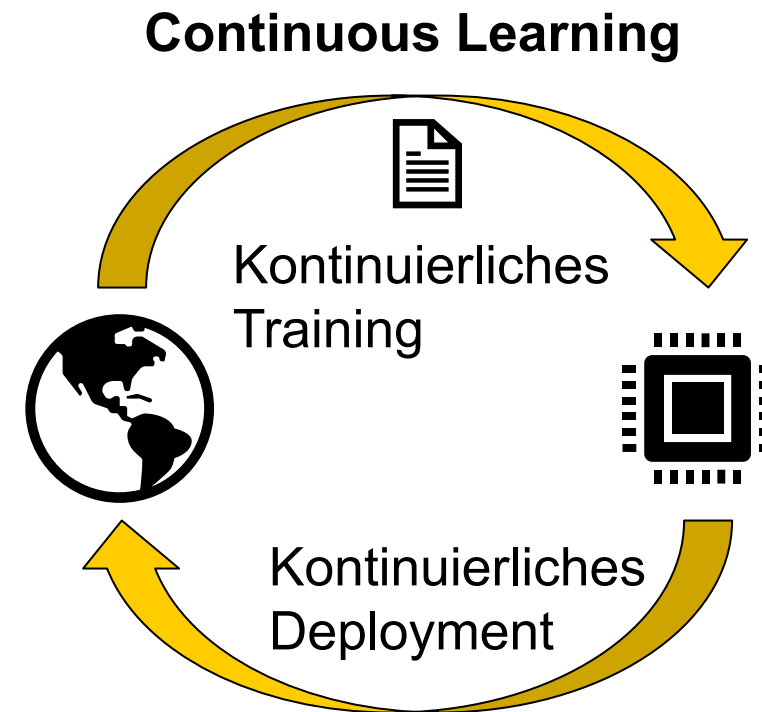
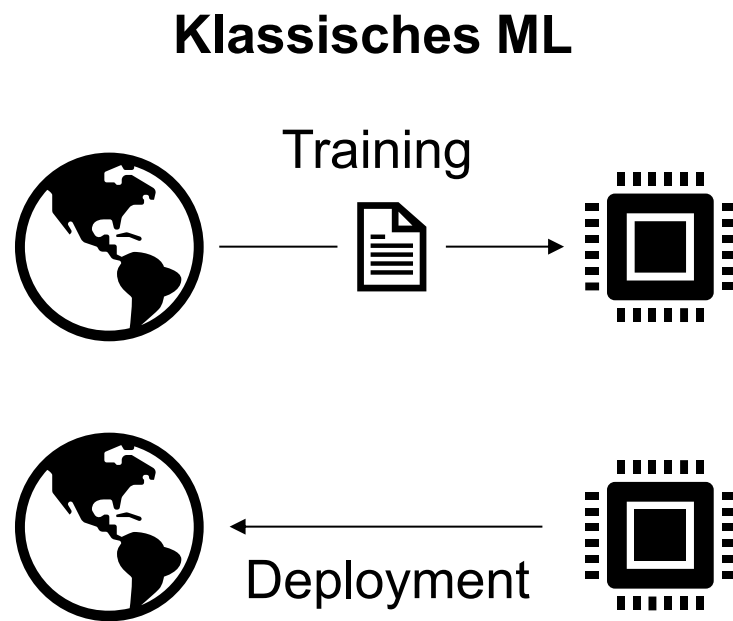
Art. 25

Konformitätsbewertung

Die in Anhang 1 Teil A genannten Produkte müssen eine Konformitätsbewertungsprüfung durch eine unabhängige dritte Stelle durchlaufen.

Eine interne Fertigungskontrolle ist für diese spezifischen Bauteile **nicht erlaubt!**

Was bedeutet eigentlich „self-evolving“?



Knackpunkt: Bedeutung „self-evolving“

Option A: Nur weiterlernende KI

Nur KI, die sich im laufenden Betrieb weiterentwickelt und weiterlernt.

- Auch *Online Learning* oder *Continuous Learning* genannt.
- Permanente Updates im Betrieb.

Fazit: Schließt klassisch "austrainierte" (offline) Systeme explizit aus.

Option B: Umfassende Definition

Self-evolving = KI gemäß der Definition aus der KI-Verordnung (KI-VO).

- Der Lebenszyklus umfasst Datensammlung, Training, Validierung und Betrieb (bis zum nächsten manuellen Update).

Fazit: Beinhaltet alle KI-Systeme, also auch fest austrainierte Algorithmen.

Versuch einer Abgrenzung

Erwägungsgrund 55:

Die Bestimmungen dieser Verordnung über die Konformitätsbewertung von Software [...] durch unabhängige Dritte sollten nur für Systeme mit vollständig oder teilweise selbstentwickelndem Verhalten unter Verwendung von Ansätzen des maschinellen Lernens [...] gelten.

Dagegen sollten diese Bestimmungen nicht für Software gelten, die **weder lern- noch weiterentwicklungsfähig** ist und nur für die **Ausführung bestimmter automatisierter Funktionen** von Maschinen oder dazugehörigen Produkten programmiert ist.

Konsequenzen für Maschinenhersteller

Konsequenz für Option A:

Lediglich weiterlernende Systeme müssen eine Drittstellenprüfung durchlaufen.

Austrainierte Systeme fallen nicht darunter.

Frage: Entsteht hier eine regulatorische Lücke?

Konsequenz für Option B:

Alle betroffenen KI-Systeme (auch austrainierte Modelle) müssen zwingend eine Drittstellenprüfung durchlaufen.

Frage: Wie sollen Prüfstellen das stemmen?

Aktueller Diskussionsstand

- Momentan gibt es keinen Konsens.
- Antwort der Kommission ausstehend.

Zurzeit wird der Guide zur MVO erstellt.

 Hoffnung: Klärung im Guide.

- Aber auch dort Diskussionen während der Erarbeitung.
- Ebenso unter den benannten Stellen.

Aktuell wird die wörtliche Auslegung, die sich lediglich auf weiterlernende Systeme nach Inverkehrbringen beschränkt, anscheinend bevorzugt.

Schnittstelle zur KI-VO

Die KI-VO klassifiziert KI-Systeme nach Risikoklassen.

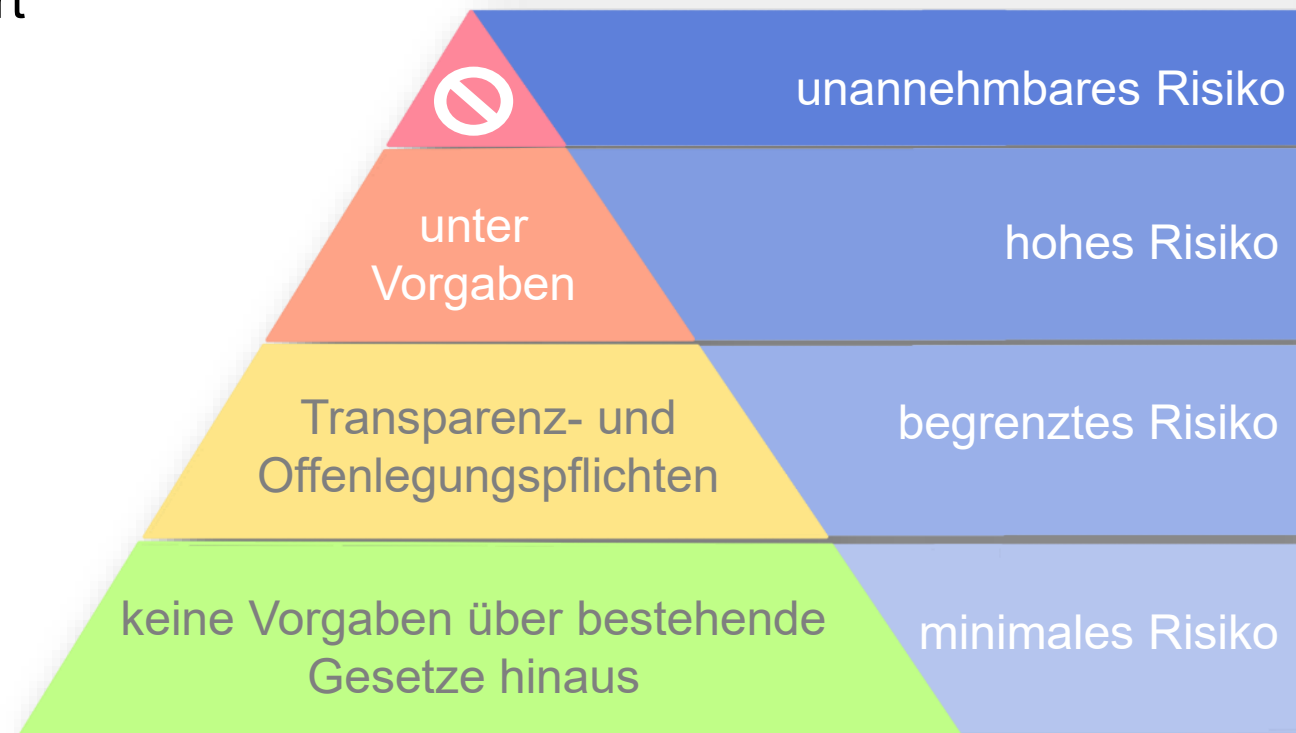
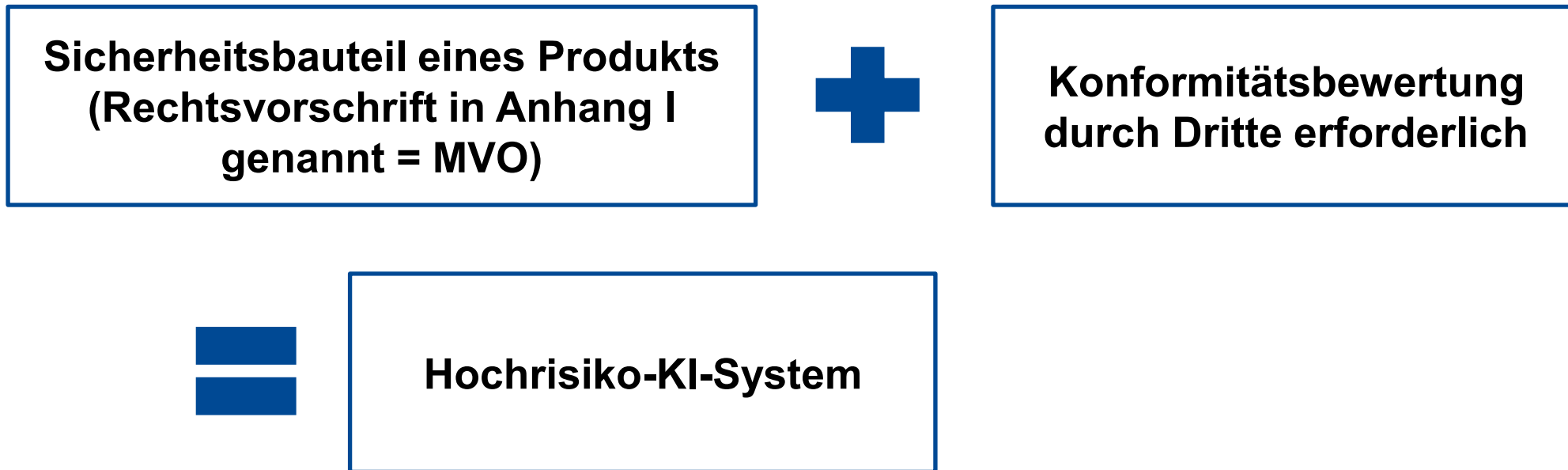


Bild von: BGHM

Hochrisiko-KI-Systeme

Artikel 6 Abs. 1:

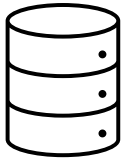


[Oder laut Artikel 6 Abs. 2, Einsatz in **sensiblen Anwendungsbereichen** genannt in Anhang III.
Bspw. Biometrie, kritische Infrastruktur, Bildung, Strafverfolgung, etc...]

Anforderungen an Hochrisiko-KI-Systeme



Risikomanagement über gesamten Lebenszyklus



Hohe Datenqualität und Data Governance



Robustheit und Cybersicherheit



Transparenz und menschliche Aufsicht

Harmonisierte Normen

Produktsicherheitsgesetz
formuliert

Schutzziele

**Standardisation
Request**

Harmonisierte Norm liefert

**Technische Umsetzung
der Schutzziele +
Vermutungswirkung**

Harmonisierte Normen für die KI-VO

Erster Standardisation Request für die Anforderungen zu Hochrisiko-KI-Systemen

- wurde im Mai 2023 veröffentlicht.
- ist an das europäische Normungskomitee CEN/CLC/JTC 21 gerichtet.

Frist der Normenerstellung der Kommission war ursprünglich der **30. April 2025**.

JTC21 meldet im Mai 2025, dass ein realistisches Ziel eher Ende 2026 ist.

Aus Erfahrung zusätzliche Verzögerung bis Sommer 2027 erwartbar.

Gültigkeit der Anforderungen: Anhang I

Abschnitt A: New Legislative Framework (NLF)

Die detaillierten Anforderungen der KI-VO gelten **direkt und parallel** zu den bestehenden Sektor-Verordnungen.

Hersteller muss die Konformität in beiden Bereichen sicherstellen und dokumentieren.

Abschnitt B: Sektorspezifische Regulierungen

Die weitreichenden Pflichten für Hochrisiko-KI-Systeme aus der KI-Verordnung gelten ausdrücklich **nicht direkt**.

KI-Anforderungen müssen in die bestehenden sektorspezifischen Genehmigungsverfahren integriert werden.

Gültigkeit der Anforderungen: Anhang I

Abschnitt A: New Legislative Framework (NLF)

Die detaillierten Anforderungen der KI-VO gelten **direkt und parallel** zu bestehenden Sektor-Verordnungen

Hersteller muss die Konformität in beiden Bereichen sicherstellen und dokumentieren

Abschnitt B: Sektorspezifische Regulierungen

Die weitreichenden Pflichten für Hochrisiko-KI-Verordnungen gelten **direkt**

KI-Anforderungen müssen in die bestehenden sektorspezifischen Genehmigungsverfahren integriert werden

Wo ist die MVO?

Gültigkeit der Anforderungen: Anhang I

Abschnitt A: New Legislative Framework (NLF)

Die detaillierten Anforderungen der KI-VO gelten **direkt und parallel** zu bestehenden Sektor-Verordnungen

Hersteller muss die Konformität in beiden Bereichen sicherstellen und dokumentieren

Aktuell in Abschnitt A, aber ...

Abschnitt B: Sektorspezifische Regulierungen

Die weitreichenden Pflichten für Hochrisiko-KI-Verordnungen gelten **direkt**

KI-Anforderungen müssen in die bestehenden sektorspezifischen Genehmigungsverfahren integriert werden

Wo ist die MVO?

Digitaler Omnibus

- Soll unnötige Bürokratie aus der KI-VO entfernen und die europäische Wettbewerbsfähigkeit stärken.
- Ergebnis des Trilogs zwischen EU-Kommission, Europäischem Parlament und Rat der EU am **7. Mai 2026** veröffentlicht.

Wichtigste Änderungen:

1. Die **Hochrisiko-Fristen** sollen verschoben werden.
2. MVO soll **von Anhang I Abschnitt A zu Abschnitt B** verschoben werden.

Registrierungspflicht in EU-Datenbank soll laut Trilog-Einigung bestehen bleiben.

Übersicht der Fristen

**Heute,
Juni 2026**

20. Januar 2027
Stichtag zur
Anwendung der MVO

Parallel und fortlaufend
Warten auf den MVO-Guide und Erarbeitung
harmonisierter Normen

August 2026
Pflichten für
Hochrisiko-Systeme
gemäß Anhang III

August 2027
Pflichten für Hochrisiko-
Systeme gemäß
Anhang I (Maschinen)

- MVO
- KI-VO

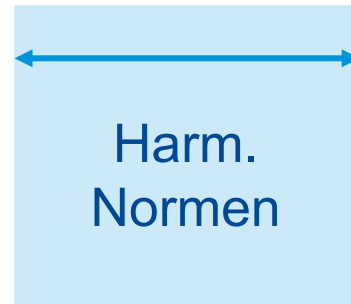
Übersicht der Fristen

**Heute,
Juni 2026**

20. Januar 2027
Stichtag zur
Anwendung der MVO

Parallel und fortlaufend
Warten auf den MVO-Guide und Erarbeitung
harmonisierter Normen

August 2026
Pflichten für
Hochrisiko-Systeme
gemäß Anhang III



August 2027
Pflichten für Hochrisiko-
Systeme gemäß
Anhang I (Maschinen)

- MVO
- KI-VO

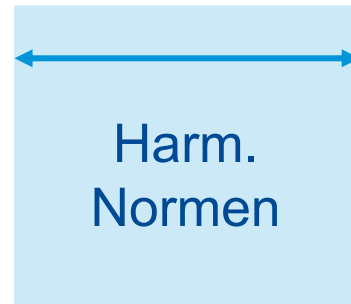
Übersicht der Fristen

Heute,
Juni 2026

20. Januar 2027
Stichtag zur
Anwendung der MVO

Parallel und fortlaufend
Warten auf den MVO-Guide und Erarbeitung
harmonisierter Normen

~~**August 2026**~~
~~Pflichten für
Hochrisiko-Systeme
gemäß Anhang III~~



~~**August 2027**~~
~~Pflichten für Hochrisiko-
Systeme gemäß
Anhang I (Maschinen)~~

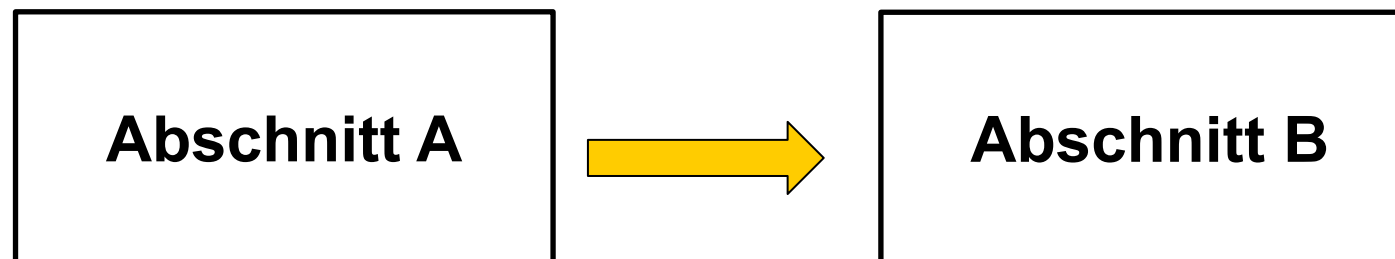
- MVO
- KI-VO

Dezember 2027
NEU: Anhang III

August 2028
NEU: Anhang I

Verschiebung von Abschnitt A zu B

- Verbindung zwischen MVO und KI-VO soll weiterhin bestehen bleiben, aber Anforderungen sollen nicht mehr direkt gültig sein.
- Zusätzliche Anforderungen sollen als **delegierte Rechtsakte** (Anhänge) zu MVO hinzugefügt werden.
- Die KI-Anforderungen erreichen den Hersteller nicht über den "direkten" Weg der KI-VO, sondern über den "Umweg" der MVO, in die sie nachträglich hineingeschrieben werden.



Was bedeutet das?

Die entsprechenden delegierten Rechtsakte sollen bis **August 2028** in Kraft treten.

1. Zunächst **neuer Verhandlungsprozess**. Erfahrungsgemäß dauert das mindestens 2 Jahre.
 - Straffer Zeitplan. Zusätzliche Unsicherheit: Was wird der neue Inhalt sein? Wird die MVO anderweitig nochmal verändert?
2. Nach Einigung zu delegierten Rechtsakten muss es einen **neuen Standardisation Request** geben
 - Sehr unrealistisch, dass die Normen rechtzeitig fertig werden. Wird langfristig womöglich für gleiche Anforderungen eine parallele Normenwelt aufgebaut?

In der Übergangsphase sollen Hersteller auf die harmonisierten Normen der KI-VO zurückgreifen.

Fokus auf MVO: Harmonisierte Normen zur MVO

„Gap Analyse“: Listung der harmonisierten Normen zur MRL auch für die MVO mit Einschränkungen bis Ende 2026.

Im Januar 2025 hat die Kommission zusätzlich einen Normungsauftrag für neue Themen wie Cybersicherheit und KI veröffentlicht.

Die Normen sollten eigentlich bis spätestens 20.1.2026 von CEN / CENELEC verabschiedet worden sein.

Relevante Normungsaktivitäten

ISO/IEC TS 22440: KI und funktionale Sicherheit

Soll dort anknüpfen, wo klassische Sicherheitsstandards (wie z. B. die ISO 13849 und die IEC 61508) an ihre Grenzen stoßen.

Diese Standards wurden nie dazu entworfen mit der nicht-deterministischen und adaptiven Natur von KI umzugehen.

Im Gegensatz zu einem klassischen System:

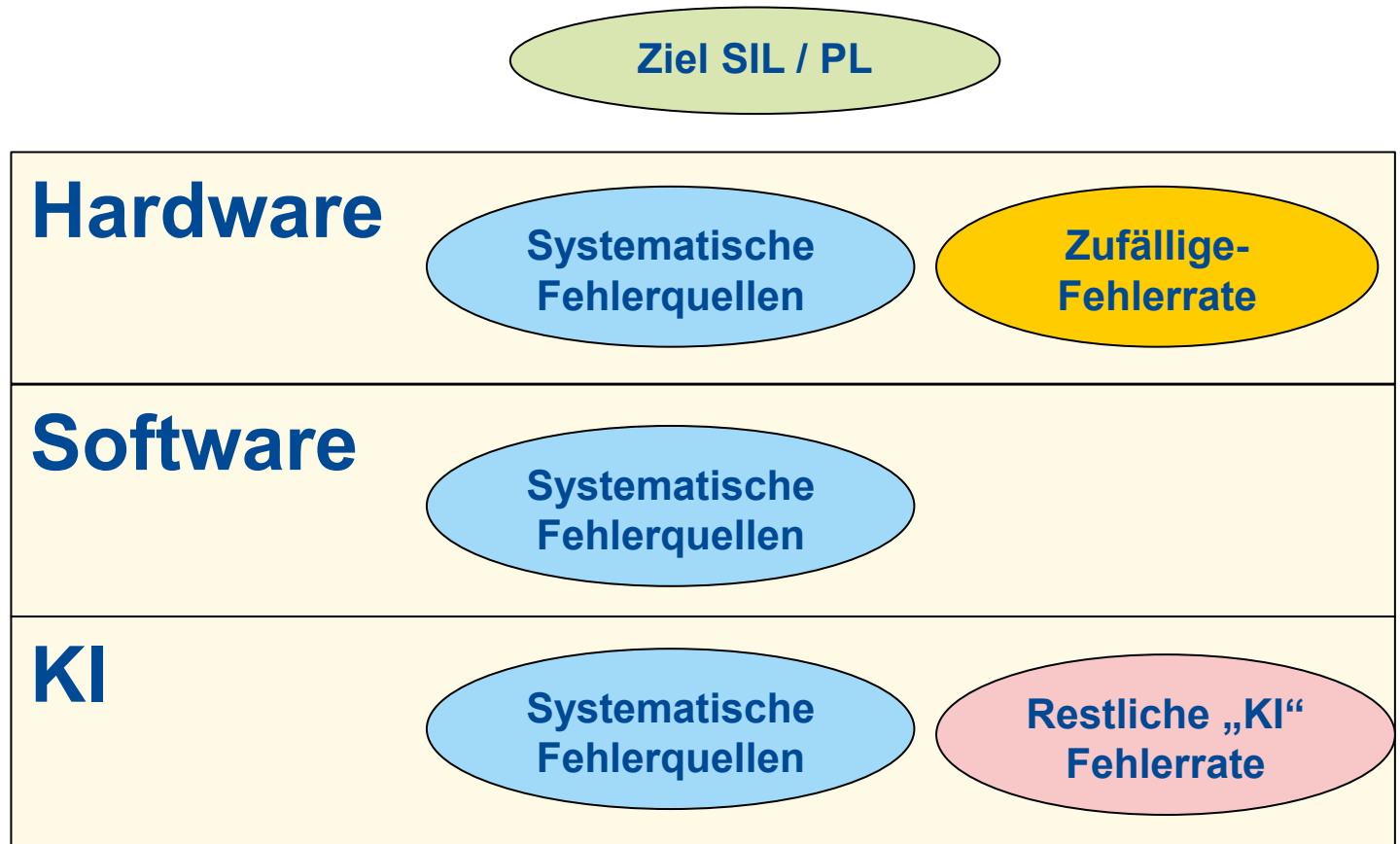
- kann die Verifizierung und Validierung nicht durch direktes Testen erfolgen.
- sind die Ausfallmodi nicht vollständig bekannt.

ISO/IEC TS 22440: KI und funktionale Sicherheit

Anforderungen werden je nach Anwendungslevel (AUL) definiert, bspw.:

- KI direkt in Sicherheitsfunktion
- KI im Entwicklungsprozess
- KI in Assistenzsystem

Für das Gesamtsystem gelten weiterhin die bekannten **SIL / PL** Anforderungen.



Fazit

- „Self-evolving“ bleibt ungeklärt
- MVO und KI-VO müssen gemeinsam betrachtet werden
- Praktische Umsetzung hängt von harmonisierten Normen ab
- Hersteller sollten jetzt vorbereiten

Fragen?

Danke für Ihre Aufmerksamkeit!

svenja.granderath@bghm.de