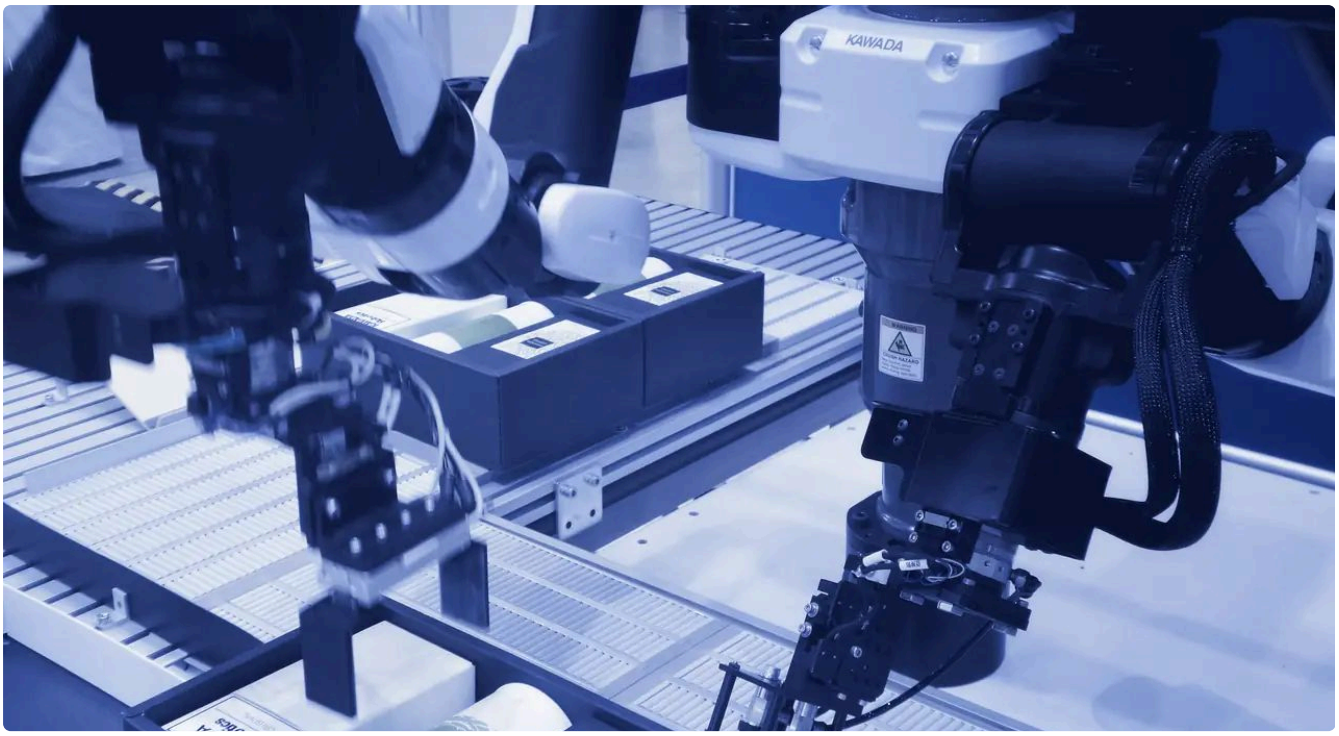


PERSPEKTIVE · NOVEMBER 2026 · 6 MIN. LESEZEIT

Wenn Modelle die Halle erreichen

Wo Physical AI heute naheliegt und welche Regeln ab 2027 für Maschinen gelten



Philipp Pöschke
Founder, Paice

AUF EINEN BLICK

- Von den deutschen Unternehmen, die 2025 AI nutzten, setzten sie nur 6 Prozent für die autonome Bewegung von Maschinen ein; Physical AI ist in der Breite noch ein kleines Feld.
- Am leichtesten gelingt der Einstieg dort, wo Aufgaben stark schwanken und ein einzelner Fehler begrenzte Folgen hat, etwa bei der Prüfung mit Bildverarbeitung.
- Ab 20. Januar 2027 gilt die Maschinenverordnung, die lernende Sicherheitsfunktionen einer Prüfung durch Dritte unterwirft; die Pflichten aus dem Cyber Resilience Act laufen parallel.

Lange fand AI vor allem auf Bildschirmen statt. Inzwischen wandert sie in Maschinen, in Kameras an der Linie, in Roboterarme, Fahrzeuge und Geräte. Diese Entwicklung wird unter dem Begriff Physical AI zusammengefasst.

In der Breite ist sie noch klein. Von den deutschen Unternehmen, die 2025 AI nutzten, setzten sie 52 Prozent für die Auswertung von Texten ein, 17 Prozent für Bilderkennung und 6 Prozent für die autonome Bewegung von Maschinen, also für Roboter, fahrerlose Fahrzeuge oder Drohnen. Für Hersteller und Betreiber von Maschinen ist das Thema trotzdem dringend, denn ab Januar 2027 ändern sich die Regeln.

Was sich ändert

Klassische Automatisierung folgt festen Programmen. Sie ist präzise und gut abzusichern, aber unflexibel. Modelle, die sehen, greifen und sich anpassen, können mit Abweichungen umgehen, mit unterschiedlichen Teilen, wechselnden Lagen und neuen Aufgaben. Das macht Automatisierung dort denkbar, wo sie bisher zu teuer oder zu starr war, etwa bei kleinen Losgrößen.

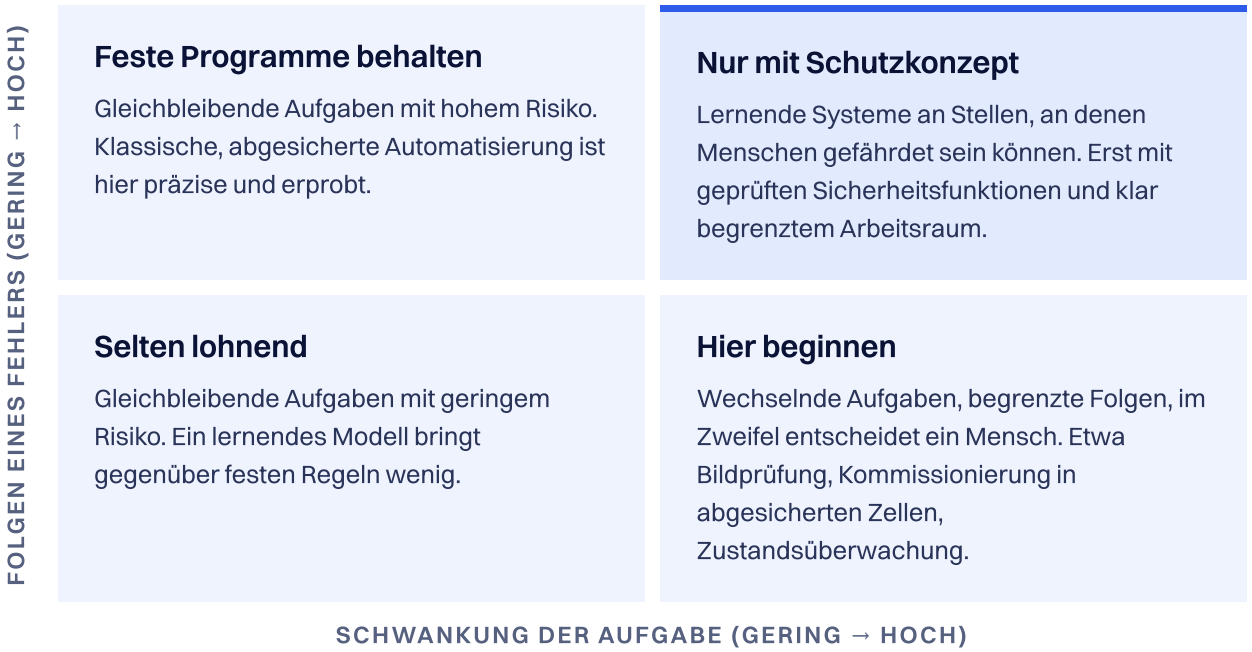
Im Modell des AI-Deltas ist Physical AI vor allem eine Frage des Bauens. Zwischen einer überzeugenden Vorführung und dem Dauerbetrieb an einer Linie liegen Sicherheit, Taktzeit, Wartung und die Menschen, die mit dem System arbeiten.

Wo der Einsatz heute naheliegt

Zwei Fragen helfen bei der Auswahl: Wie stark schwankt die Aufgabe, und was kostet ein Fehler? Wo die Aufgabe kaum schwankt, sind feste Programme schwer zu schlagen. Wo ein Fehler Menschen gefährden kann, braucht jede lernende Komponente ein Schutzkonzept und, wenn sie eine Sicherheitsfunktion übernimmt, ab 2027 eine Prüfung durch Dritte.

ABBILDUNG 1

Wo Physical AI heute naheliegt



Darstellung: Paice

Das Feld unten rechts ist der natürliche Anfang. Dazu gehören:

- Qualitätsprüfung mit Bildverarbeitung an der Linie, bei der ein Mensch über Ausschuss entscheidet
- Kommissionierung und Handhabung wechselnder Teile in abgesicherten Zellen
- Assistenz für Instandhaltung und Service, etwa bei der Suche nach Fehlerursachen
- Zustandsüberwachung von Anlagen mit Auswertung direkt am Gerät

Bei vielen dieser Anwendungen läuft das Modell am Gerät selbst oder in einem Rechner an der Linie, in der Fachsprache Edge AI. Das hat drei Gründe. Die Antwort muss oft in Millisekunden kommen, schneller als ein Weg über das Netz. Die Anlage soll weiterlaufen, wenn die Verbindung ausfällt. Und Bilder aus der Halle, auf denen auch Beschäftigte zu sehen sein können, verlassen den Standort gar nicht erst. Der Preis ist begrenzte Rechenleistung und ein eigener Weg, um Modelle auf viele Geräte zu verteilen und zu aktualisieren.

Was anders ist als bei Software

Ein Fehler in einer Software lässt sich zurückrollen. Ein Fehler an einer Maschine kann Menschen verletzen oder Material zerstören. Deshalb gehören das Verhalten im Fehlerfall, die Reaktionszeit und die Grenzen des Arbeitsraums in jede Bewertung, bevor über Genauigkeit gesprochen wird.

Dazu kommen Updates. In einer Büroanwendung ist ein neues Modell ein Fortschritt, an einer Maschine ist es zuerst eine Änderung des Verhaltens. Sicherheitsrelevante Funktionen brauchen nach einem Update eine neue Bewertung, und die Wartung muss das einplanen. Schließlich arbeiten an der Linie Menschen, die Störungen beheben, Teile nachlegen und Ergebnisse prüfen. Sie gehören von Anfang an dazu, ebenso der Betriebsrat, der nach § 90 BetrVG über die Planung technischer Anlagen rechtzeitig zu unterrichten ist.

Welche Regeln ab 2027 gelten

Stand: 17. November 2026. Für Physical AI greifen mehrere Regelwerke ineinander. Die wichtigsten Termine zeigt die Übersicht.

ABBILDUNG 2

Neue Pflichten für Maschinen mit AI

11. September 2026
Cyber Resilience Act: Meldepflicht für aktiv ausgenutzte Schwachstellen und schwere Sicherheitsvorfälle

9. Dezember 2026
Neues Produkthaftungsrecht, das Software ausdrücklich einbezieht

20. Januar 2027
Maschinenverordnung gilt; lernende Sicherheitsfunktionen brauchen eine Prüfung durch eine benannte Stelle

11. Dezember 2027
Cyber Resilience Act gilt vollständig

2. August 2028
AI Act: Hochrisiko-Pflichten für AI in regulierten Produkten nach Anhang I, für Maschinen nur eingeschränkt

Quellen: Verordnungen (EU) 2023/1230, 2024/2847, 2026/1744, Richtlinie (EU) 2024/2853; Stand 17.11.2026

Maschinenverordnung. Die Verordnung (EU) 2023/1230 ersetzt ab 20. Januar 2027 die Maschinenrichtlinie. Sie erfasst AI über den Begriff des selbstentwickelnden Verhaltens. Sicherheitsbauteile und eingebettete Systeme, die ihr Verhalten mit Ansätzen des maschinellen Lernens ganz oder teilweise selbst weiterentwickeln und dabei Sicherheitsfunktionen gewährleisten, stehen in

Anhang I Teil A. Für sie ist eine Konformitätsbewertung unter Beteiligung einer benannten Stelle vorgeschrieben. Hersteller müssen außerdem die Lernphase in der Risikobeurteilung berücksichtigen und ihre Grenzen vorab festlegen.

AI Act. Mit dem Omnibus (Verordnung (EU) 2026/1744) wurde die Maschinenverordnung in Abschnitt B von Anhang I verschoben. Für AI in Maschinen gelten die Hochrisiko-Pflichten des AI Act damit nur noch eingeschränkt; AI-spezifische Anforderungen sollen über Änderungen der Maschinenverordnung kommen. Für andere regulierte Produkte nach Anhang I, etwa Medizinprodukte, gelten die Hochrisiko-Pflichten ab 2. August 2028.

Cyber Resilience Act. Hersteller von Produkten mit digitalen Elementen müssen seit 11. September 2026 aktiv ausgenutzte Schwachstellen und schwere Sicherheitsvorfälle melden. Ab 11. Dezember 2027 gilt die Verordnung (EU) 2024/2847 vollständig, einschließlich der Anforderungen, die für die CE-Kennzeichnung erfüllt sein müssen.

Normen. Die Sicherheitsnormen für Industrieroboter, ISO 10218-1 und ISO 10218-2, sind im Februar 2025 in neuer Fassung erschienen. Teil 2 enthält nun auch die Anforderungen an kollaborative Anwendungen, bei denen Mensch und Roboter einen Arbeitsraum teilen.

Dieser Abschnitt ist eine allgemeine Einordnung und keine Rechtsberatung.

Wie man sicher beginnt

Am Anfang steht ein abgegrenzter Anwendungsfall mit Kriterien, die vor dem Bau feststehen: die nötige Erkennungs- oder Greifleistung, die Taktzeit, die zulässige Fehlerrate und das Verhalten, wenn das Modell unsicher ist. Ein Prototyp unter realen Bedingungen, mit echten Teilen, echtem Licht und echtem Takt, beantwortet diese Fragen schneller als jede Studie.

Parallel dazu sollte geklärt werden, ob die Lösung eine Sicherheitsfunktion übernimmt. Wenn ja, gehören Sicherheitsfachleute und gegebenenfalls eine benannte Stelle von Beginn an dazu, denn eine späte Zertifizierung kann den ganzen Entwurf infrage stellen. Erst danach lohnt die Investition in die Skalierung. Sie umfasst Wartung, Updates und Schulung an der Linie und die Frage, wer das Modell im Betrieb überwacht.

Diese Überwachung ist keine Nebensache. Ein Modell, das bei der Abnahme zuverlässig war, kann mit der Zeit schlechter werden, weil sich Beleuchtung, Material oder Zulieferteile ändern. Es braucht deshalb eine Kennzahl, die solche Verschiebungen früh zeigt, etwa den Anteil der Fälle, bei denen das Modell unsicher ist, und eine geregelte Reaktion darauf. Wird nachtrainiert, ist das wieder eine Änderung des Verhaltens, mit allen Folgen für die Sicherheitsbewertung.

Gängige Sicht, unsere Sicht

Physical AI wird gern als Thema für übermorgen diskutiert, mit humanoiden Robotern und vollautonomen Fabriken. Wir halten den näheren Horizont für wichtiger. Die Pflichten aus Maschinenverordnung und Cyber Resilience Act kommen 2027, und die meisten sinnvollen Einstiege beginnen mit Bildverarbeitung

an bestehenden Anlagen. Unternehmen, die dort Erfahrung mit lernenden Systemen sammeln, sind vorbereitet, wenn die anspruchsvolleren Anwendungen reif sind.

Quellen

- Unternehmen mit Nutzung von Technologien der künstlichen Intelligenz nach Beschäftigtengrößenklassen, Statistisches Bundesamt, Stand 24.11.2025
- Verordnung (EU) 2023/1230 über Maschinen, Amtsblatt der EU, 29.06.2023
- Maschinenverordnung (EU) 2023/1230, IHK zu Dortmund
- Verordnung (EU) 2026/1744 (Digital Omnibus on AI), Amtsblatt der EU, 24.07.2026
- Verordnung (EU) 2024/2847 (Cyber Resilience Act), Amtsblatt der EU, 20.11.2024
- Ready, respond, report: the Cyber Resilience Act's reporting regime is here, CMS, 11.09.2026
- Richtlinie (EU) 2024/2853 über die Haftung für fehlerhafte Produkte, Amtsblatt der EU, 18.11.2024
- ISO 10218-2:2025, Robotics – Safety requirements – Part 2, ISO, Februar 2025
- § 90 BetrVG, Bundesministerium der Justiz, gesetze-im-internet.de



AUTOR

Philipp Pöschke

Founder, Paice

Philipp Pöschke hat Paice 2026 in Bremen gegründet. Er verantwortet jedes Vorhaben persönlich und arbeitet selbst an Analysen, Prototypen und Lösungen mit. Die Beiträge unter Insights verantwortet er als Autor.