WHITEPAPER

Physical AI in der industriellen Realität

Eine Vertrauensinfrastruktur für humanoide Robotik, Service-Robotik und belastbaren Betrieb

Leitgedanke

Humanoide und mobile Roboter werden nicht dadurch marktfähig, dass sie in Demonstrationen funktionieren. Sie werden marktfähig, wenn ihr Einsatz in konkreten Umgebungen technisch, organisatorisch, rechtlich und betrieblich nachvollziehbar beherrscht wird.

Maucher CNC Robotic GmbH

Perspektive aus Maschinenbau, industrieller Fertigung, Robotik-Integration und CE-naher Risikobetrachtung

Stand: Juni 2026

Hinweis zur Einordnung

Dieses Whitepaper ersetzt keine Rechtsberatung, keine Konformitätsbewertung und keine Prüfung durch eine notifizierte Stelle. Es beschreibt eine industrielle Herangehensweise zur Vorbereitung, Strukturierung und Absicherung von Physical-AI-Anwendungen. Formale Prüf- und Zertifizierungsentscheidungen bleiben den zuständigen Stellen, Sachverständigen und verantwortlichen Organisationen vorbehalten.

Inhalt

1. Management Summary

Physical AI beschreibt KI-Systeme, die nicht nur Daten verarbeiten, sondern über Sensorik und Aktorik in der physischen Welt handeln. In humanoiden Robotern, mobilen Servicerobotern und autonomen Erfassungssystemen wird künstliche Intelligenz damit zu einer bewegenden, greifenden, wahrnehmenden und potenziell risikobehafteten Technologie. Die zentrale Frage lautet nicht mehr allein, ob ein Roboter eine Aufgabe ausführen kann. Entscheidend ist, ob er sie in einer konkreten Umgebung, mit konkreten Menschen, konkreten Schnittstellen und konkreten Grenzen verantwortbar ausführen darf.

1.1 Entstehung und Motivation

Über viele Jahre lag auch mein eigener Fokus auf der Frage, wie sich neue Robotiksysteme mit den etablierten Werkzeugen des Maschinenbaus erfassen, bewerten und absichern lassen. Der naheliegende Weg bestand darin, Physical AI durch bestimmungsgemäße Verwendung, Risikobeurteilungen, Sicherheitsfunktionen, Normenabgleiche, technische Dokumentation und Konformitätsbewertungen zu beschreiben. Diese Werkzeuge haben sich über Jahrzehnte bewährt und bilden bis heute die Grundlage für sichere und zuverlässige technische Systeme.

Mit zunehmender praktischer Erfahrung im Umgang mit modernen, datengetriebenen Robotiksystemen wurde jedoch deutlich, dass dieser Ansatz allein nicht ausreicht. Je stärker Systeme ihre Umgebung interpretieren, Wahrscheinlichkeiten bewerten, Entscheidungen situationsabhängig treffen und ihr Verhalten durch Softwarestände, Daten oder Updates verändern können, desto häufiger stößt man an die Grenzen einer rein deterministischen Betrachtungsweise.

Die daraus entstandene Erkenntnis war kein theoretisches Konstrukt, sondern das Ergebnis zahlreicher Diskussionen und praktischer Erfahrungen. Über Jahre hinweg entstand immer wieder das Gefühl, gegen eine unsichtbare Wand zu laufen. Nicht weil bestehende Richtlinien und Normen falsch wären, sondern weil sie für eine Welt entwickelt wurden, in der das Verhalten eines Systems vollständig aus seiner Konstruktion und Programmierung ableitbar war. Viele der neuen Fragestellungen rund um Physical AI lassen sich innerhalb dieser Denkmodelle zwar beschreiben, aber nicht mehr vollständig beantworten.

Dieses Whitepaper ist daher nicht aus der Suche nach neuen Regeln entstanden, sondern aus der Erkenntnis, dass bestehende Regelwerke um neue Bewertungs- und Betrachtungsansätze ergänzt werden müssen. Die klassischen Methoden bleiben unverzichtbar. Sie bilden weiterhin das Fundament für Sicherheit, Qualität und Vertrauen. Gleichzeitig benötigen wir zusätzliche Werkzeuge, um Systeme bewerten zu können, deren Verhalten nicht mehr ausschließlich deterministisch, sondern in Teilen probabilistisch, datengetrieben und lernfähig ist.

> **Kernaussage zur Motivation**
>
> Die bisherige deterministische Sicherheitslogik wird nicht ersetzt, sondern erweitert. Physical AI braucht zusätzlich eine nachvollziehbare Betriebslogik, die Einsatzdomäne, reale Umgebungsdaten, Tests, Monitoring, Änderungen und menschliche Verantwortung dauerhaft miteinander verbindet.

Der Markt für humanoide Robotik wird nur dann skalieren, wenn die Lücke zwischen Demonstration und belastbarem Betrieb geschlossen wird. Ein Roboter kann auf einer Bühne laufen, Gegenstände greifen und Sprache verstehen. Daraus folgt jedoch nicht, dass er in einer Produktionshalle, einem Krankenhaus, einem Hotel, einer Bankfiliale oder einem öffentlichen Gebäude rechtlich und sicherheitstechnisch sauber eingesetzt werden kann. Diese Differenz zwischen technischer Fähigkeit und verantwortbarer Einsatzfähigkeit ist der eigentliche Engpass.

Dieses Whitepaper geht deshalb über eine allgemeine Beschreibung hinaus. Es beschreibt die notwendige Vertrauensinfrastruktur für Physical AI: Operational Design Domain, reale Umgebungsdaten, Risikobeurteilung, technische Akte, Testfälle, Simulation, Monitoring, Cybersecurity, Datenschutz, Änderungsmanagement und eine klare Aufteilung menschlicher Verantwortung. Dabei wird AURA ONE als Beispiel einer industriellen Vorgehensweise beschrieben. Der Kern ist nicht, dass zwingend dieses eine System verwendet werden muss. Entscheidend ist, dass reale Umgebungen so erfasst, versioniert, validiert und dokumentiert werden, dass daraus belastbare Einsatzgrenzen und prüfbare Nachweise entstehen können.

Die Maucher-Perspektive unterscheidet sich von rein softwaregetriebenen Betrachtungen. Maucher CNC Robotic und Maucher Formenbau verbinden Maschinenbau, Robotik-Integration und die Fertigung hochkomplexer Bauteile unter realen industriellen Anforderungen. Diese Doppelperspektive ist wesentlich: Wer Physical AI sicher in die Realität bringen will, muss nicht nur Algorithmen verstehen, sondern auch Taktzeiten, Bedienerrealität, Prozesssicherheit, Qualitätsnachweise, technische Dokumentation, Produktionsstörungen und Verantwortung im laufenden Betrieb.

Kernaussage

Physical AI braucht keine weitere Präsentationsebene, sondern eine belastbare Betriebs- und Nachweisstruktur. Die Zukunft liegt nicht in der Frage, welcher Roboter am spektakulärsten wirkt, sondern welcher Einsatz in welcher Umgebung nachvollziehbar beherrscht werden kann.

Die fünf zentralen Aussagen

- **Einsatz statt Show:** Die technische Demonstration eines humanoiden Roboters ist kein Nachweis für einen sicheren und dauerhaften Betrieb.
- **ODD als Fundament:** Ohne präzise Operational Design Domain kann keine seriöse Aussage über den zulässigen Einsatz getroffen werden.
- **Realitätsdaten statt Annahmen:** Gebäude, Produktionsflächen und Prozessumgebungen müssen gemessen, strukturiert und versioniert werden, bevor sie als Grundlage für Simulation und Freigabe dienen.
- **AURA ONE als Beispiel:** AURA ONE zeigt eine konkrete Vorgehensweise, reale Umgebungen maschinenlesbar zu machen. Andere Systeme können denselben Zweck erfüllen, wenn sie vergleichbare Nachweiskriterien erfüllen.
- **Agentenlogik als Werkzeug:** KI-Agenten können Struktur, Vollständigkeit und Widerspruchsprüfung verbessern. Sie ersetzen aber keine menschliche Verantwortung und keine formale Prüfstelle.

2. Ausgangslage: Warum Physical AI eine neue industrielle Disziplin ist

Klassische Industrieautomation beruht auf einer weitgehend kontrollierten Umgebung. Ein Roboter steht in einer Zelle, arbeitet definierte Programme ab und wird durch trennende Schutzeinrichtungen, Lichtgitter, sichere Steuerungen, Not-Halt-Konzepte und klar beschriebene Betriebsarten beherrscht. Diese Welt bleibt wichtig. Sie reicht jedoch nicht aus, um humanoide oder mobile KI-gestützte Systeme in offenen menschlichen Umgebungen zu bewerten.

Humanoide Roboter und mobile Serviceroboter sollen in Räumen arbeiten, die nicht für Maschinen, sondern für Menschen gebaut wurden. Dort gibt es Türen, Aufzüge, Besucher, Wagen, Regale, Glasflächen, wechselnde Lichtverhältnisse, Funklöcher, Treppen, enge Passagen, temporäre Hindernisse, Reinigungsarbeiten, Lieferverkehr und Menschen, die sich nicht immer regelkonform verhalten. Diese Realität ist nicht störend. Sie ist der normale Betriebszustand.

Physical AI ist deshalb keine reine Weiterentwicklung klassischer Robotertechnik. Es ist eine Systemdisziplin. Mechanik, Elektrik, Sensorik, Software, KI-Modelle, Mensch-Maschine-Interaktion, Datenflüsse, Cybersecurity, Datenschutz, Betrieb und Recht wirken gleichzeitig zusammen. Ein Fehler kann aus jeder dieser Ebenen kommen und sich in einer physischen Bewegung manifestieren.

Ebene	Klassische Automation	Physical AI / humanoide Robotik
Umgebung	Meist abgegrenzt, vorhersehbar, technisch kontrolliert	Offen, menschlich, dynamisch und oft nur teilweise vorhersehbar
Verhalten	Programmierte Abläufe mit klaren Zuständen	Wahrnehmung, Interpretation, Planung und adaptive Reaktion
Nachweis	Fokus auf Maschine, Sicherheitsfunktionen und definierte Betriebsarten	Zusätzlich Einsatzdomäne, Daten, Updates, Monitoring und organisatorische Verantwortung

Ebene	Klassische Automation	Physical AI / humanoide Robotik
Risikoquelle	Mechanik, Steuerung, Energie, Bedienfehler	Zusätzlich KI-Verhalten, Semantik, Datenqualität, Cyberangriffe und Grenzfälle
Freigabelogik	Inbetriebnahme und wesentliche Veränderung	Lebenszyklus mit Revalidierung bei Aufgaben-, Modell-, Software- oder Umgebungsänderungen

Der industrielle Kern von Physical AI besteht daher darin, eine Brücke zwischen Wahrnehmung und Verantwortung zu bauen. Der Roboter muss seine Umgebung erkennen. Das Unternehmen muss aber zugleich erklären können, was er erkennen muss, welche Grenzen gelten, wann er stoppen muss, welche Daten gespeichert werden, wer Änderungen freigibt und wie Vorfälle ausgewertet werden.

3. Der Kernkonflikt: deterministische Sicherheitslogik und adaptive Systeme

Maschinensicherheit ist historisch stark deterministisch geprägt. Eine Maschine soll unter definierten Bedingungen ein definiertes Verhalten zeigen. Gefährdungen werden identifiziert, Risiken bewertet und Schutzmaßnahmen abgeleitet. Diese Logik bleibt richtig und unverzichtbar. Der Konflikt entsteht, weil moderne KI-gestützte Roboter zusätzlich probabilistische Komponenten enthalten. Sie bewerten Situationen anhand von Datenmustern, Wahrscheinlichkeiten, Kontexten und Modellannahmen.

Probabilistisch bedeutet nicht, dass ein System beliebig handeln darf. Genau das wäre ein untragbares Missverständnis. Probabilistische Fähigkeiten müssen in deterministische Sicherheitsgrenzen eingebettet werden. Die KI kann helfen, Objekte zu erkennen, Wege zu planen, Sprache zu verstehen oder Situationen einzuschätzen. Die sicherheitsrelevanten Grenzen müssen jedoch eindeutig, prüfbar und durchsetzbar sein. Wenn eine Grenze verletzt wird, muss das System in einen sicheren Zustand wechseln.

Architekturprinzip

KI darf Wahrnehmung und Assistenz verbessern. Sicherheitsgrenzen müssen jedoch so gestaltet sein, dass sie auch bei Unsicherheit, Fehlklassifikation, Datenlücken, Funkverlust oder Softwareänderungen wirksam bleiben.

Typische Konfliktstellen

- **Wahrnehmung:** Der Roboter erkennt einen Gegenstand, eine Person oder eine Tür möglicherweise nicht immer gleich. Sicherheitsrelevante Entscheidungen dürfen nicht allein auf einer unsicheren Klassifikation beruhen.
- **Softwareupdates:** Ein Update kann Verhalten, Prioritäten, Pfadplanung oder Reaktion auf Grenzfälle verändern. Daraus kann eine sicherheitsrelevante Änderung entstehen.
- **Semantik:** Der Roboter muss nicht nur Geometrie sehen, sondern Bedeutung verstehen: Fluchtweg, Patientenzimmer, Reinraum, Sperrbereich, sensible Zone, Übergabepunkt.
- **Menschliches Verhalten:** Menschen können Wege blockieren, den Roboter testen, Lasten verändern, Gegenstände anhängen oder Aufgaben anders formulieren als vorgesehen.
- **Datenqualität:** Fehlerhafte Karten, veraltete Raumdaten, transparente Objekte, Spiegelungen oder bewegte Hindernisse können zu falschen Annahmen führen.

Der entscheidende industrielle Schritt besteht darin, adaptive Fähigkeit nicht zu verbieten, sondern sie in ein beherrschbares Betriebsmodell zu übersetzen. Dafür braucht es eine klare Operational Design Domain, eine belastbare reale Datengrundlage und eine Dokumentationslogik, die Änderungen und Abweichungen sichtbar macht.

4. Operational Design Domain: der Vertrag zwischen Technik und Realität

Die Operational Design Domain, kurz ODD, beschreibt die zulässige Einsatzdomäne eines Roboters. Sie beantwortet nicht abstrakt, ob ein Roboter sicher ist, sondern konkret: Sicher wofür, in welcher Umgebung, mit welcher Aufgabe, mit welcher Last, mit welchen Menschen, mit welcher Geschwindigkeit, mit welcher Aufsicht, mit welchen Schnittstellen und mit welchen Abbruchkriterien?

Eine ODD ist damit der Vertrag zwischen Technik und Realität. Sie verhindert, dass ein Roboter schleichend immer weiter eingesetzt wird, ohne dass die neuen Risiken geprüft werden. Gerade bei humanoiden Systemen ist diese Begrenzung entscheidend, weil die Bauform und die Fähigkeiten schnell den Eindruck erzeugen, der Roboter könne beliebig flexibel eingesetzt werden.

ODD-Feld	Zu klärende Fragen
Räume und Wege	Welche Gebäude, Etagen, Flure, Aufzüge, Türen, Übergabepunkte und Sperrbereiche sind freigegeben?
Aufgaben	Welche Tätigkeiten sind erlaubt, welche ausdrücklich nicht? Transport, Greifen, Türbedienung, Kommunikation, Begleitung, Assistenz?
Menschen	Welche Personengruppen sind anwesend? Mitarbeiter, Besucher, Patienten, Kinder, externe Dienstleister?
Lasten und Objekte	Welche Gewichte, Abmessungen, Temperaturen, Gefahrstoffe, Medikamente, Werkzeuge oder sensiblen Güter werden bewegt?
Geschwindigkeit und Nähe	Welche maximalen Geschwindigkeiten, Sicherheitsabstände, Interaktionszonen und Kontaktarten sind zulässig?
Umgebungsbedingungen	Licht, Boden, Steigungen, Nässe, Glasflächen, Spiegelungen, Funkabdeckung, Temperatur, Lärm, Staub, Verkehrsdichte.
Daten und IT	Welche Daten werden erfasst, verarbeitet, gespeichert oder übertragen? Welche Systeme sind angebunden?
Fallbacks	Wann muss der Roboter stoppen, Hilfe anfordern, zurückfahren, die Aufgabe abbrechen oder in einen sicheren Zustand wechseln?
Änderungen	Welche Änderungen erfordern eine Revalidierung? Neue Aufgabe, neue Karte, Update, Umbau, anderer Bereich, andere Last?

Die ODD darf nicht nur als Textdokument existieren. Für Physical AI muss sie mit realen Daten verbunden werden: Karten, Punktwolken, Zonenmodelle, semantische Markierungen, Testfälle, Freigabestände, Versionshistorien und Betriebslogs. Erst dann kann sie praktisch genutzt und geprüft werden.

ODD als lebendes Artefakt

Eine ODD ist kein einmaliges Dokument für den Projektordner. Sie muss gepflegt werden. Wenn sich Wege ändern, neue Regale aufgestellt werden, ein Aufzug anders genutzt wird, eine Brandschutztür hinzukommt, ein Softwareupdate erfolgt oder ein neuer Transporttyp eingeführt wird, muss geprüft werden, ob die ODD noch gültig ist. Genau hier entstehen in der Praxis viele Risiken, weil technische und organisatorische Änderungen häufig voneinander getrennt betrachtet werden.

5. Vertrauensinfrastruktur: vom Roboterprodukt zum beherrschten Betrieb

Vertrauen in Physical AI entsteht nicht durch die Aussage, ein Roboter sei intelligent oder sicher. Vertrauen entsteht, wenn der Einsatz nachvollziehbar, wiederholbar, prüfbar und im Betrieb überwachbar wird. Das eigentliche marktfähige Produkt ist nicht nur der Roboter. Es ist der dokumentierte und beherrschte Betrieb des Roboters in einer konkreten Umgebung.

Eine Vertrauensinfrastruktur verbindet technische, organisatorische und dokumentarische Elemente. Sie schafft die Grundlage, um Herstellerangaben, Betreiberrealität, Integrationsleistung und Prüfanforderungen zusammenzuführen. Sie ist besonders wichtig, weil humanoide Roboter typischerweise nicht isoliert arbeiten, sondern in bestehende Organisationen, Gebäude, IT-Systeme und Prozesse integriert werden.

Baustein	Zweck	Typisches Ergebnis
Einsatzbeschreibung	Klärung der bestimmungsgemäßen Verwendung und konkreten Aufgabe	Use Case, Prozessbeschreibung, Rollenmodell

Baustein	Zweck	Typisches Ergebnis
Reale Umgebungsdaten	Erfassen der räumlichen, dynamischen und semantischen Bedingungen	Punktwolke, Karte, Zonenmodell, Änderungsstand
ODD	Festlegen der zulässigen Einsatzgrenzen	Freigegebene Räume, Aufgaben, Lasten, Zeiten und Fallbacks
Risikobeurteilung	Identifikation und Bewertung technischer, organisatorischer und datenbezogener Gefährdungen	Gefährdungsliste, Maßnahmen, Restrisiko, offene Punkte
Testfälle	Überprüfung von Normalfällen, Randfällen und Fehlerszenarien	Testprotokolle, Abbruchkriterien, Nachweise
Technische Akte	Strukturierte Sammlung der relevanten Nachweise	Herstellerunterlagen, Integrationsunterlagen, Versionen, Freigaben
Monitoring	Erkennen von Abweichungen, Near Misses und Änderungsbedarf	Logs, Ereignisklassen, Auswertungen, Revalidierungsauslöser
Governance	Klärung von Verantwortung, Rollen und Freigabeprozessen	Betreiberpflichten, Schulung, Eskalationswege, Change Management

Konsequenz für Betreiber

Der Kauf eines Roboters ist nur der Anfang. Entscheidend ist die Fähigkeit, den konkreten Einsatz zu beschreiben, zu begrenzen, zu testen, zu dokumentieren und über den Lebenszyklus zu überwachen.

6. AURA ONE als Beispiel für eine industrielle Erfassungs- und Nachweislogik

AURA ONE wird in diesem Whitepaper nicht als einzig möglicher Weg beschrieben, sondern als Beispiel, wie Maucher CNC Robotic reale Umgebungen für Physical AI technisch erschließbar macht. Der Grundgedanke ist einfach: Bevor ein humanoider oder mobiler Roboter in einer Umgebung sicher handeln soll, muss diese Umgebung verstanden, vermessen, strukturiert und versioniert werden. Reale Räume dürfen nicht nur als Hintergrundkulisse der Robotik betrachtet werden. Sie sind ein aktiver Teil des Sicherheitssystems.

AURA ONE steht damit exemplarisch für eine Vorgehensweise, die aus der industriellen Praxis kommt: erst messen, dann strukturieren, dann bewerten, dann testen, dann freigeben und anschließend überwachen. Der Roboter oder die Erfassungseinheit erzeugt keine Zertifizierung. Sie erzeugt eine Datenbasis, die ODD, Simulation, Testplanung, Risikobeurteilung und spätere Betriebsüberwachung deutlich belastbarer machen kann.

6.1 Zweck von AURA ONE

Der primäre Zweck von AURA ONE ist nicht die spektakuläre Vorführung eines vierbeinigen Roboters, sondern die systematische Erfassung realer Betriebsumgebungen. Der Fokus liegt auf der Frage: Welche Informationen über den Einsatzort müssen verfügbar sein, damit ein späterer Robotereinsatz nicht auf Annahmen, sondern auf nachvollziehbaren Daten beruht?

- **Maschinenlesbare Umgebung:** Räume, Wege, Türen, Engstellen, Höhenunterschiede, Übergabepunkte, Sperrbereiche und potenzielle Gefahrenstellen werden als Datenobjekte verfügbar gemacht.
- **ODD-Unterstützung:** Die tatsächliche Umgebung wird mit den geplanten Einsatzgrenzen verbunden. Dadurch wird sichtbar, wo Annahmen fehlen oder nicht zur Realität passen.
- **Simulationsgrundlage:** Geometrie, Navigationsflächen und relevante Objekte können in Simulationen, digitale Zwillinge oder Testumgebungen überführt werden.
- **Testfallableitung:** Aus realen Engstellen, Kreuzungen, Türen, Aufzügen oder sensiblen Bereichen lassen sich konkrete Prüfszenarien ableiten.

- **Änderungserkennung:** Wiederholte Erfassungen ermöglichen den Vergleich von Raumzuständen und helfen, Umbauten oder neue Risiken zu erkennen.
- **Nachweisstruktur:** Die Umgebung wird nicht nur beschrieben, sondern mit Daten, Versionen, Metadaten und Freigabeständen verknüpft.

6.2 Referenzarchitektur

Eine AURA-ONE-Konfiguration kann aus einem mobilen oder quadrupeden Trägersystem, hochauflösender 3D-Erfassung, RGB- oder RGB-D-Sensorik, optionaler Thermalsensorik, Inertialsensorik, Gimbal- oder Schwenkeinheiten, lokaler Rechenleistung und einer angebundenen Workstation bestehen. Die konkrete Hardware ist nicht der entscheidende Punkt. Entscheidend ist, dass die Daten reproduzierbar, kalibriert, zeitlich zuordenbar, geometrisch validiert und für spätere Prüfprozesse verwendbar sind.

Ebene	Funktion	Beispielhafte Umsetzung
Trägersystem	Bewegung durch reale Umgebungen, Erreichbarkeit unterschiedlicher Messpositionen	Quadruped, AMR, Handscanner, mobiles Mapping-System, statischer Laserscanner oder Kombination daraus
Primäre 3D-Erfassung	Geometrische Grundlage für Karten, Punktwolken, Navigationsflächen und Kollisionsräume	LiDAR, Tiefenkamera, Photogrammetrie, strukturierte Punktwolken
RGB-Erfassung	Visuelle Referenz, Objektklassifikation, semantische Annotation und Nachvollziehbarkeit	RGB-Kameras, Panoramen, Videosequenzen, Referenzbilder
Thermalsensorik optional	Ergänzende Detektion bestimmter Oberflächen, Anlagenzustände oder schwer sichtbarer Bereiche	Wärmebildkamera als Zusatzsensor, nicht als alleinige Geometriequelle
Gimbal / Sensorkopf	Erweiterung des Sichtfeldes und strukturierte Erfassung aus definierten Blickrichtungen	360-Grad-Schwenk, definierte Neigungsbereiche, wiederholbare Messposen
Lokale Verarbeitung	Vorfilterung, Synchronisation, SLAM, Streaming und Datenkontrolle	Edge-PC, Industrie-PC, NUC, Workstation, ROS2-Knoten
Workstation / Backend	Speicherung, Visualisierung, Qualitätssicherung, Versionierung und Export	Punktwolken-Viewer, Datenbank, Simulationspipeline, Dokumentationssystem

In einer industriellen Umsetzung ist besonders wichtig, dass Sensorik, Koordinatensysteme und Datenflüsse nicht lose nebeneinanderstehen. Jede Messung muss einem Zeitpunkt, einer Pose, einem Sensorzustand, einer Softwareversion und einem Verarbeitungsstand zugeordnet werden können. Nur so entsteht aus einer Punktwolke ein verwertbarer Nachweis.

6.3 Erfassungsmodi

AURA ONE kann als Beispiel für mehrere Erfassungsmodi verstanden werden, die je nach Einsatzfall kombiniert werden. Diese Modi lassen sich auch mit anderen Systemen abbilden.

Modus	Ziel	Nutzen für Physical AI
Initiale Kartierung	Einmalige oder wiederholte Grundaufnahme des Einsatzortes	Grundlage für ODD, Navigationsmodell und erste Risikobetrachtung
Geführte Begehung	Mensch führt das System durch relevante Bereiche	Schneller Einstieg, fachliche Kommentierung vor Ort, Erkennen kritischer Punkte
Autonome Messpunktfahrt	Definierte Messpunkte werden wiederholbar angefahren	Vergleichbarkeit, Änderungsdetektion, reproduzierbare Datensätze
Stationäre 360-Grad-Erfassung	Vollständige Aufnahme eines Raumpunktes	Dokumentation komplexer Bereiche, Türen, Kreuzungen, Übergabepunkte

Modus	Ziel	Nutzen für Physical AI
Änderungserkennung	Vergleich mehrerer Erfassungsstände	Erkennen von Umbauten, neuen Hindernissen, veränderten Wegen oder Risikozonen
Pilotbegleitung	Erfassung während eines begrenzten Robotikpiloten	Abgleich zwischen geplanter ODD und realem Betriebsverhalten

6.4 Datenpipeline von Rohdaten zu prüfbaren Artefakten

Der eigentliche Wert entsteht nicht in der Aufnahme allein, sondern in der Datenpipeline. Rohdaten müssen gefiltert, registriert, verdichtet, validiert, semantisch angereichert und in prüfbare Artefakte überführt werden. Ein industrielles System muss deshalb nachvollziehbar machen, welche Schritte zwischen Sensoraufnahme und Entscheidungsvorlage liegen.

1. **Aufnahmeplanung:** Festlegung von Bereichen, Messpunkten, benötigten Genauigkeiten, Sensoren, Datenschutzgrenzen und Betriebszeiten.
2. **Rohdatenerfassung:** Aufnahme von 3D-Daten, Bildern, optionalen Zusatzsensoren und Pose-Informationen mit eindeutigen Zeitstempeln.
3. **Kalibrierung und Synchronisation:** Abgleich von Sensorframes, Gimbalstellungen, Robotpose, IMU, Kamerazeit und Netzwerklatenzen.
4. **Registrierung und Mapping:** Zusammenführung einzelner Scans zu einer konsistenten Karte, inklusive Loop Closure, Driftkontrolle und Qualitätsprüfung.
5. **Filterung und Verdichtung:** Entfernung ungültiger Messwerte, Ausreißer, temporärer Störungen und Datenreduktion ohne Verlust sicherheitsrelevanter Geometrie.
6. **Semantische Annotation:** Kennzeichnung von Türen, Fluchtwegen, No-Go-Zonen, Übergabepunkten, Glasflächen, Aufzügen, engen Passagen und sensiblen Bereichen.
7. **ODD-Verknüpfung:** Zuordnung der gemessenen Realität zu zulässigen Aufgaben, Wegen, Geschwindigkeiten, Lasten und Fallbacks.
8. **Export und Nachweis:** Bereitstellung für Simulation, Testfallgenerierung, technische Akte, Betreiberfreigabe und spätere Änderungsvergleiche.

6.5 Qualitätskriterien für die Erfassungsdaten

Nicht jede 3D-Aufnahme ist automatisch geeignet, eine Sicherheits- oder Betriebsbewertung zu unterstützen. Für Physical AI müssen Mindestkriterien definiert werden. Diese Kriterien gelten unabhängig davon, ob AURA ONE, ein stationärer Laserscanner, ein mobiles Mapping-System oder eine andere Plattform eingesetzt wird.

Kriterium	Warum es wichtig ist	Möglicher Prüfpunkt
Vollständigkeit	Nicht erfasste Bereiche können in Simulation und ODD unsichtbare Risiken erzeugen	Abdeckungsbericht, Heatmap, Liste offener Bereiche
Metrische Genauigkeit	Abstände, Durchfahrtsbreiten und Kollisionsräume müssen belastbar sein	Vergleich mit Referenzmaßen, Toleranzdefinition
Wiederholbarkeit	Änderungen sollen vom Messrauschen unterscheidbar sein	Mehrfachmessung gleicher Bereiche, Abweichungsstatistik
Zeitliche Zuordnung	Dynamische Umgebungen verändern sich; Erfassungsstand muss eindeutig sein	Zeitstempel, Schicht, Betriebszustand, Versionsnummer
Kalibrierung	Sensorfehler können systematische Geometriefehler erzeugen	Kalibrierprotokoll, Sensorparameter, Prüfdatum
Koordinatensysteme	Daten müssen zwischen Roboter, Gebäude, Karte und Simulation eindeutig transformierbar sein	Dokumentierte Frames und Transformationskette

Kriterium	Warum es wichtig ist	Möglicher Prüfpunkt
Semantische Qualität	Geometrie allein sagt nicht, was ein Bereich bedeutet	Freigabe durch Betreiber, Markierung von Zonen und Rollen
Datenschutz	Bilddaten können Personen, Kennzeichen, Bildschirme oder vertrauliche Inhalte enthalten	Maskierung, Zugriffskonzept, Zweckbindung, Löschfristen
Versionierung	Spätere Prüfungen müssen wissen, auf welchem Raumstand sie beruhen	Change Log, Freigabestand, Änderungsvergleich

6.6 Grenzen von AURA ONE und vergleichbaren Systemen

AURA ONE ist ein Werkzeug zur Datenerhebung, Strukturierung und Vorbereitung. Es ist kein Ersatz für eine Risikobeurteilung, keine formale Zertifizierung und keine Garantie, dass ein späterer humanoider Roboter in jeder Situation sicher agiert. Die Datenbasis verbessert die Qualität der Bewertung, ersetzt aber nicht die Bewertung selbst.

- **Dynamik bleibt kritisch:** Menschen, Wagen, offene Türen, temporäre Hindernisse und wechselnde Betriebszustände können nie vollständig in einer statischen Aufnahme abgebildet werden.
- **Sensorik hat Grenzen:** Glas, Spiegelungen, transparente Objekte, dunkle Flächen, glänzende Oberflächen, Rauch, Staub oder direkte Sonneneinstrahlung können Messungen erschweren.
- **Semantik muss validiert werden:** Ein Algorithmus kann eine Tür erkennen. Ob sie Brandschutztür, Fluchtweg, Sperrbereich oder Lieferzugang ist, muss fachlich bestätigt werden.
- **Simulation bleibt Annahme:** Auch eine gute Simulation ist nur so belastbar wie ihre Modelle, Parameter und validierten Randbedingungen.
- **Betrieb erzeugt neue Erkenntnisse:** Erst im Pilot und im laufenden Betrieb werden manche Randfälle sichtbar. Deshalb braucht es Monitoring und Revalidierung.

7. Welche Anforderungen auch alternative Erfassungssysteme erfüllen müssen

AURA ONE ist ein Beispiel, keine zwingende Systemvorgabe. Für viele Einsatzfälle können andere Systeme sinnvoller sein: stationäre Laserscanner, mobile Mapping-Trolleys, Handscanner, AMR-basierte Erfassung, Drohnen in geeigneten Innenräumen, vorhandene BIM-Daten, Kamerarigs, LiDAR-Rucksacksysteme oder eine Kombination aus mehreren Quellen. Entscheidend ist nicht die Marken- oder Plattformfrage, sondern die Nachweisfähigkeit der erzeugten Daten.

Ein alternatives System ist dann geeignet, wenn es nicht nur schöne Visualisierungen erzeugt, sondern robuste Daten für ODD, Simulation, Risikobeurteilung und Änderungsmanagement liefert. Dafür muss die Erfassung nachvollziehbar geplant, dokumentiert, validiert und versioniert sein.

Anforderung	Mindestfrage an jedes alternative System
Messzweck	Wurde vor der Aufnahme festgelegt, welche Entscheidungen auf Basis der Daten getroffen werden sollen?
Datenqualität	Sind Genauigkeit, Vollständigkeit, Auflösung und Toleranzen bekannt und dokumentiert?
Validierung	Wurden kritische Maße und Bereiche gegen reale Referenzen geprüft?
Semantik	Können Zonen, Türen, Sperrbereiche, Fluchtwege, Übergabepunkte und kritische Objekte fachlich markiert werden?
Versionierung	Ist eindeutig erkennbar, welcher Raumstand für welche Freigabe verwendet wurde?
Exportfähigkeit	Können die Daten in Simulation, Karten, technische Akten oder Monitoring-Systeme überführt werden?
Datenschutz	Sind personenbezogene oder vertrauliche Bildinformationen geschützt?
Wiederholbarkeit	Kann die Aufnahme zu einem späteren Zeitpunkt vergleichbar wiederholt werden?

Anforderung	Mindestfrage an jedes alternative System
Auditierbarkeit	Ist nachvollziehbar, wer wann mit welchem System welche Daten aufgenommen und verarbeitet hat?

Praktische Einordnung

Für eine einfache Voranalyse kann ein pragmatisches Mapping-System genügen. Für sicherheitsnahe Freigaben in sensiblen Umgebungen steigen die Anforderungen an Genauigkeit, Semantik, Validierung, Datenschutz und Versionierung erheblich.

8. Gaussian Splats: nützlich für Visualisierung, kritisch als Sicherheitsnachweis

Gaussian Splats, genauer 3D Gaussian Splatting, sind ein leistungsfähiger Ansatz zur fotorealistischen Darstellung realer Umgebungen aus Bilddaten. Die Szene wird dabei nicht klassisch als geschlossenes CAD-Modell oder reine Punktwolke dargestellt, sondern durch viele räumlich verteilte, halbtransparente Gauß-Elemente, die aus bestimmten Blickrichtungen sehr realistisch wirken können. Für Physical AI ist diese Technologie interessant, aber sie muss richtig eingeordnet werden.

Der große Vorteil liegt in der visuellen Verständlichkeit. Ein Gaussian Splat kann eine reale Halle, einen Flur, einen Maschinenbereich oder einen Übergabepunkt sehr anschaulich darstellen. Für interne Abstimmungen, Schulungen, Remote-Review, Standortdokumentation, Vorplanung und Kommunikation ist das wertvoll. Die Gefahr entsteht, wenn eine fotorealistische Darstellung mit einem belastbaren geometrischen oder sicherheitstechnischen Nachweis verwechselt wird.

Stärke von Gaussian Splats	Grenze im Physical-AI-Kontext
Sehr anschauliche Visualisierung realer Räume	Fotorealismus ist kein Nachweis für metrische Genauigkeit oder Kollisionssicherheit
Schnelle Orientierung für Projektteams und Entscheider	Nicht automatisch geeignet für Durchfahrtsbreiten, Sicherheitsabstände oder Freigabezonen
Gute Ergänzung zu RGB-basierten Raumansichten	Problematisch bei Glas, Spiegelungen, transparenten Flächen, bewegten Personen und verdeckten Bereichen
Kann Remote-Begehungen und Schulungen unterstützen	Enthält nicht automatisch belastbare Semantik wie Fluchtweg, Sperrbereich oder Maschinenzustand
Kann visuelle Layer eines digitalen Zwillings verbessern	Für Simulation mit Physik, Kollision und Navigation werden zusätzliche Geometrieformen wie Mesh, Occupancy Grid, SDF oder Punktwolke benötigt
Kann Unterschiede zwischen Versionen sichtbar machen	Änderungsdetektion muss validiert werden; visuelle Ähnlichkeit kann reale Geometrieänderungen überdecken

Das Problem ist also nicht Gaussian Splatting selbst. Das Problem ist die falsche Rolle im Nachweissystem. Ein Gaussian Splat sollte als Visualisierungs- und Kommunikationsschicht verstanden werden, nicht als alleinige Sicherheitsbasis. Für belastbare Robotikfreigaben braucht es zusätzlich metrisch geprüfte Geometrie, semantisch validierte Zonen, dokumentierte Toleranzen, Kollisionsmodelle, Navigationskarten und eine Verbindung zur ODD.

Besonders kritisch sind transparente und reflektierende Flächen. Glas kann in Bilddaten sichtbar, in Tiefendaten unklar, in LiDAR-Daten fehlerhaft oder je nach Sensor stark unterschiedlich erscheinen. Spiegelungen können Objekte erzeugen, die physisch nicht existieren. Bewegte Personen oder Wagen können in der Rekonstruktion verwischen. Verdeckte Bereiche werden nicht zuverlässig rekonstruiert, sondern können visuell plausibel erscheinen, ohne tatsächlich geprüft zu sein. Genau solche Stellen sind im sicherheitsnahen Kontext gesondert zu markieren.

Empfehlung

Gaussian Splats eignen sich hervorragend als visuelle Schicht eines digitalen Zwillings. Sie sollten jedoch mit Punktwolken, validierten Karten, semantischen Zonen, Kollisionsgeometrien und ODD-Metadaten gekoppelt werden. Kurz gesagt: fotorealistische Anschauung ja, alleiniger Sicherheitsnachweis nein.

9. KI-Agenten als strukturierende Prüf- und Dokumentationslogik

KI-Agenten können im Kontext von Physical AI eine wichtige Rolle übernehmen, wenn sie klar begrenzt eingesetzt werden. Sie können Betreiberangaben strukturieren, Widersprüche suchen, offene Nachweise markieren, Normenfelder zuordnen, Testfälle vorschlagen, Datenstände vergleichen und Entscheidungsvorlagen vorbereiten. Sie dürfen jedoch keine formale Prüfstelle ersetzen und keine menschliche Verantwortung übernehmen.

Die sinnvolle Architektur ist daher nicht ein einzelner Agent, der eine Freigabe ausspricht, sondern ein verteiltes Agentensystem mit klaren Rollen. Jeder Agent betrachtet denselben Einsatzfall aus einer anderen Perspektive. Ein Orchestrator führt die Ergebnisse zusammen, kennzeichnet Unsicherheiten und erzeugt eine Vorlage für Fachleute.

Agentenrolle	Prüfperspektive	Typischer Output
ODD-Agent	Einsatzgrenzen, Räume, Aufgaben, Lasten, Zeiten, Aufsicht	ODD-Entwurf, offene Felder, Grenzverletzungen
Risiko-Agent	Mechanische, elektrische, thermische, organisatorische und menschliche Gefährdungen	Gefährdungsliste, Maßnahmenvorschläge, Restrisiko
Normen- und Rechtsrahmen-Agent	Relevante Regelwerksfelder, Maschinenrecht, KI-Recht, Datenschutz, Cybersecurity	Zuordnung, Prüffragen, Nachweisanforderungen
Daten-Agent	Umgebungsdaten, Punktwolken, Karten, Versionen, Qualität, Datenschutz	Datenqualitätsbericht, fehlende Messbereiche
Testfall-Agent	Normalfälle, Randfälle, Fehlerszenarien, Abbruchkriterien	Testkatalog, Prioritäten, Akzeptanzkriterien
Cybersecurity-Agent	Zugriff, Rollen, Updates, Fernwartung, Netzwerke, Logs	Security-Anforderungen, offene Risiken
Runtime-Agent	Monitoring, Near Misses, Stoppereignisse, Abweichungen	Betriebskennzahlen, Revalidierungsauslöser
Konflikt-Agent	Widersprüche zwischen Herstellerangaben, Betreiberrealität und ODD	Konfliktliste, Klärungsbedarf
Orchestrator	Zusammenführung und Priorisierung	Entscheidungsvorlage für Menschen und Prüfinstanzen

Wichtig: Agenten brauchen Evidenzdisziplin

Ein Agentensystem darf nicht nur plausibel formulieren. Es muss Evidenz fordern. Jede Aussage sollte auf Betreiberangaben, Herstellerunterlagen, Messdaten, Testprotokolle, Regelwerkszuordnung oder dokumentierte Annahmen zurückgeführt werden. Wo diese Evidenz fehlt, muss das System nicht so tun, als sei der Punkt geklärt. Es muss den offenen Punkt sichtbar machen.

- **Keine Scheinsicherheit:** Ein nicht beantworteter Betreiberpunkt ist kein Fehler im Fragebogen, sondern ein Hinweis auf Prüfbedarf.
- **Keine automatische Freigabe:** Agenten bereiten vor. Menschen, verantwortliche Organisationen und formale Stellen entscheiden.

- **Keine Normen-Halluzination:** Regelwerksbezüge müssen gepflegt, versioniert und fachlich geprüft werden.
- **Keine Blackbox:** Eingaben, Annahmen, Quellen, Ergebnisse und Änderungen müssen nachvollziehbar sein.

10. Rollen und Anforderungen: Hersteller, Inbetriebnehmer und Betreiber

Ein zentraler Punkt für Physical AI ist die saubere Trennung der Rollen. Bei klassischen Maschinen ist diese Trennung oft bereits anspruchsvoll. Bei humanoiden Robotern, mobilen Servicerobotern und adaptiven KI-Systemen wird sie noch wichtiger, weil Produktfähigkeit, Integration, Einsatzumgebung, Softwareversion, Datenlage und Betreiberorganisation zusammenwirken. Ein Roboter kann als Produkt technisch leistungsfähig sein und trotzdem für einen konkreten Einsatz ungeeignet sein. Umgekehrt kann ein Einsatz technisch sinnvoll sein, aber scheitern, wenn Herstellerangaben, Inbetriebnahme und Betrieb nicht sauber verbunden werden.

Die Verantwortung darf deshalb nicht diffus werden. Hersteller, Inbetriebnehmer beziehungsweise Integrator und Betreiber müssen jeweils eigene Anforderungen erfüllen. Entscheidend ist nicht nur, wer ein Dokument erstellt, sondern wer welche Annahme trifft, welche Grenze definiert, welche Änderung freigibt und welche Evidenz für den sicheren Betrieb vorliegt. Dieses Whitepaper behandelt diese Rollentrennung bewusst als Kernbestandteil der Vertrauensinfrastruktur.

Kernaussage zur Rollentrennung

Physical AI wird nicht sicher, wenn jede Rolle davon ausgeht, dass die jeweils andere Rolle das Problem bereits gelöst hat. Der Hersteller muss Fähigkeiten und Grenzen des Systems belastbar beschreiben. Der Inbetriebnehmer muss diese Grenzen auf die konkrete Umgebung übertragen und verifizieren. Der Betreiber muss den freigegebenen Betrieb dauerhaft organisatorisch beherrschen.

10.1 Hersteller: Produktfähigkeit, Grenzen und Nachweise

Der Hersteller liefert nicht nur Hardware. Er liefert ein System mit Sensorik, Aktorik, Software, Schnittstellen, Updatepfaden, Betriebsarten, Sicherheitsfunktionen und dokumentierten Grenzen. Für Physical AI reicht es nicht aus, allgemeine Leistungsversprechen zu machen. Der Hersteller muss verständlich und prüfbar beschreiben, wofür das System vorgesehen ist, wofür es nicht vorgesehen ist und unter welchen Bedingungen seine Aussagen gelten.

Anforderungsfeld an den Hersteller	Erwarteter Inhalt
Bestimmungsgemäße Verwendung	Klare Beschreibung der vorgesehenen Aufgaben, Betriebsarten, Umgebungen, Lasten, Geschwindigkeiten, Interaktionsformen und Ausschlüsse.
Systemgrenzen	Was darf der Roboter nicht tun? Welche Böden, Lichtverhältnisse, Funkbedingungen, Personengruppen, Gegenstände oder Räume sind ausgeschlossen?
Sicherheitsarchitektur	Beschreibung sicherheitsrelevanter Funktionen, Stoppkonzepte, Fallbacks, Überwachungen, Grenzwertlogiken und manueller Eingriffsmöglichkeiten.
ODD-Rahmen	Ein herstellerseitiger Einsatzrahmen, der vom Integrator in eine konkrete ODD des Standorts übersetzt werden kann.
Sensorik und Wahrnehmung	Leistungsgrenzen der Sensoren, Blindbereiche, Probleme mit Glas, Spiegelungen, Dunkelheit, Menschenmengen, engen Bereichen und verdeckten Objekten.
Software- und Modellversionen	Versionierung, Freigabestand, bekannte Einschränkungen, Updateverfahren, Rollbackfähigkeit und Bewertung sicherheitsrelevanter Änderungen.

Anforderungsfeld an den Hersteller	Erwarteter Inhalt
Schnittstellen	Dokumentierte APIs, Datenformate, Netzwerkbedingungen, Fernwartung, Rollenrechte, Logging-Schnittstellen und Integrationsgrenzen.
Cybersecurity	Zugriffsschutz, Updatekette, Authentifizierung, Verschlüsselung, Härtung, Fernzugriff und bekannte Sicherheitsannahmen.
Dokumentation und Nachweise	Technische Unterlagen, Betriebsanleitung, Restrisiken, Wartungsvorgaben, Prüfprotokolle, Integrationshinweise und Schulungsanforderungen.

Besonders kritisch ist die Versuchung, allgemeine Fähigkeiten zu verkaufen, ohne die Grenzen gleichwertig zu dokumentieren. Für einen Betreiber ist nicht nur interessant, was der Roboter kann. Mindestens genauso wichtig ist, was er nicht sicher kann. Ein Hersteller, der seine Grenzen sauber beschreibt, wirkt nicht schwächer. Er schafft die Grundlage für seriöse Integration.

10.2 Inbetriebnehmer und Integrator: Übersetzung in den konkreten Einsatz

Der Inbetriebnehmer oder Integrator verbindet das Produkt mit der Realität des Standorts. Genau hier entstehen viele der entscheidenden Risiken. Der Hersteller kennt sein System. Der Betreiber kennt seine Organisation. Der Inbetriebnehmer muss prüfen, ob beides zusammenpasst, und aus Herstellerangaben, Standortdaten und Betreiberzielen eine belastbare Einsatzfreigabe vorbereiten. Diese Rolle darf nicht auf das technische Einschalten des Roboters reduziert werden.

Anforderungsfeld an Inbetriebnehmer / Integrator	Erwarteter Inhalt
Standortaufnahme	Erfassung von Wegen, Engstellen, Böden, Türen, Aufzügen, Sperrzonen, Funkabdeckung, Lichtverhältnissen und Personenströmen.
ODD-Konkretisierung	Übersetzung des herstellerseitigen Einsatzrahmens in eine standortspezifische Operational Design Domain.
Risikobetrachtung der Integration	Bewertung von Schnittstellen, Verkehrswegen, Übergaben, Notfällen, Brandschutz, Fluchtwegen, Mensch-Roboter-Begegnungen und Fehlanwendungen.
Konfiguration	Einrichtung von Geschwindigkeiten, Zonen, Karten, Rollenrechten, Betriebsmodi, Stopplogik, Übergabepunkten und Fallbacks.
Abnahmeprüfung	Durchführung von Standorttests, Grenzfalltests, Fehlerszenarien, Kommunikationsabbrüchen, Not-Halt-Tests und Wiederanlaufbedingungen.
Dokumentation der Ist-Installation	As-built-Dokumentation mit Kartenstand, Softwarestand, Konfiguration, freigegebenen Aufgaben, Restrisiken und offenen Punkten.
Schulung und Übergabe	Einweisung von Betreiber, Aufsichtspersonen, Wartung, IT, Datenschutz, Arbeitssicherheit und betroffenen Mitarbeitern.
Änderungslogik	Festlegung, welche späteren Änderungen eine erneute Prüfung, Anpassung der ODD oder Revalidierung auslösen.

Der Inbetriebnehmer ist damit die Brücke zwischen Produktkonformität und Betriebskonformität. Er muss Widersprüche sichtbar machen: Wenn der Betreiber eine freie Publikumsumgebung beschreibt, der Hersteller aber nur kontrollierte Bereiche vorsieht, darf dieser Konflikt nicht in der Projektdynamik verschwinden. Er muss dokumentiert, entschieden und gegebenenfalls durch technische oder organisatorische Maßnahmen aufgelöst werden.

10.3 Betreiber: Betrieb innerhalb der freigegebenen Grenzen

Der Betreiber trägt die Verantwortung dafür, dass der Roboter im Alltag innerhalb der freigegebenen Grenzen eingesetzt wird. Genau hier entsteht bei Physical AI ein besonderes Risiko: Die schleichende Ausweitung. Was im Pilot als klar begrenzte Transportaufgabe beginnt, wird im Alltag schnell erweitert: andere Wege,

andere Zeiten, andere Lasten, andere Nutzergruppen oder zusätzliche Aufgaben. Jede solche Erweiterung kann die ursprüngliche Bewertung entwerten.

Anforderungsfeld an den Betreiber	Erwarteter Inhalt
Organisatorische Verantwortung	Benennung verantwortlicher Personen für Betrieb, Freigaben, Schulung, Ereignisauswertung, Datenschutz, IT und Arbeitssicherheit.
Betrieb innerhalb der ODD	Keine Nutzung außerhalb der freigegebenen Räume, Aufgaben, Lasten, Zeiten, Geschwindigkeiten, Personengruppen und Betriebsbedingungen.
Schulung	Einweisung aller betroffenen Personen: Bedienung, Verhalten bei Störung, Not-Halt, Eskalation, Datenschutz und Grenzen des Systems.
Tägliche Betriebsdisziplin	Vorstartprüfungen, Sichtkontrolle, klare Betriebsmodi, bekannte Sperrzonen, sichere Übergaben und dokumentierte Abweichungen.
Ereignismanagement	Erfassung von Stopps, Near Misses, Fehlklassifikationen, Bedienproblemen, ungewöhnlichen Situationen und Eingriffen.
Update- und Änderungsfreigabe	Keine unkontrollierten Softwareupdates, Kartenänderungen, neuen Aufgaben oder Prozessänderungen ohne Bewertung.
Datenschutz und IT-Betrieb	Regelung von Datenzugriff, Speicherung, Löschung, Fernwartung, Rollenrechten und Protokollierung.
Revalidierung	Auslösung erneuter Prüfung bei Änderungen an Aufgabe, Umgebung, Software, Sensorik, Organisation oder auffälligen Betriebserfahrungen.

Der Betreiber muss vor allem verhindern, dass praktische Bequemlichkeit die Sicherheitslogik überholt. Wenn Mitarbeiter beginnen, den Roboter für nicht freigegebene Aufgaben zu nutzen, ist das kein Randthema, sondern ein Governance-Problem. Ein belastbarer Physical-AI-Betrieb benötigt deshalb klare interne Regeln, technische Begrenzungen, Schulung und ein Ereignismanagement, das nicht bestraft, sondern lernt.

10.4 Übergabekette und Mindestnachweise

Zwischen Hersteller, Inbetriebnehmer und Betreiber sollte eine dokumentierte Übergabekette entstehen. Jede Rolle übergibt nicht nur ein Produkt oder eine Dienstleistung, sondern Annahmen, Grenzen, Nachweise und offene Punkte. Das Ziel ist keine Papierübung, sondern eine prüfbare Kette: Was wurde geliefert? Was wurde integriert? Was wurde getestet? Was wurde freigegeben? Was bleibt ausgeschlossen?

Übergabepunkt	Mindestinhalt der Übergabe	Zweck
Hersteller an Inbetriebnehmer	Systembeschreibung, Grenzen, Integrationsanleitung, Schnittstellen, Softwarestand, Sicherheitsfunktionen, Restrisiken, Wartung und Updateverfahren.	Der Inbetriebnehmer kann prüfen, ob das Produkt für den geplanten Standort überhaupt geeignet ist.
Betreiber an Inbetriebnehmer	Anwendungsfall, Räume, Prozesse, Personen, Lasten, Zeiten, Datenanforderungen, IT-Vorgaben, Sicherheitsanforderungen und organisatorische Verantwortliche.	Der Inbetriebnehmer kann den Einsatz realistisch bewerten und die ODD konkretisieren.
Inbetriebnehmer an Betreiber	Standortspezifische ODD, Konfiguration, Testprotokolle, Abnahmeergebnis, Schulungsnachweis, offene Punkte, Restrisiken und Revalidierungsauslöser.	Der Betreiber weiß, was freigegeben ist, was verboten bleibt und wann erneut geprüft werden muss.
Betreiber an Prüfstelle / Sachverständige	Strukturierte technische Akte, ODD, Herstellerunterlagen, Integrationsnachweise, Testfälle, Betriebsorganisation, Monitoringkonzept und Änderungsmanagement.	Eine fachliche Bewertung kann auf nachvollziehbarer Evidenz statt auf Projektbehauptungen beruhen.

Praktischer Prüfgedanke

Jede Rolle sollte die Frage beantworten können: Welche Aussage treffe ich, auf welcher Grundlage treffe ich sie, für welchen Einsatz gilt sie und wodurch wird sie ungültig? Wenn diese Frage nicht beantwortet werden kann, ist die Vertrauensinfrastruktur noch nicht belastbar.

10.5 Wenn Rollen verschwimmen

In der Praxis können Rollen ineinander übergehen. Ein Betreiber kann durch eigene Softwareänderungen, neue Aufgaben, selbst erstellte Karten, geänderte Greifer, andere Lasten oder nachträgliches Training faktisch Aufgaben übernehmen, die ursprünglich beim Hersteller oder Integrator lagen. Ebenso kann ein Integrator durch tiefgreifende Veränderungen am System neue Verantwortung erzeugen. Dieses Whitepaper ersetzt keine rechtliche Bewertung solcher Fälle. Industriell betrachtet gilt jedoch: Jede wesentliche Veränderung muss sichtbar, bewertet, dokumentiert und freigegeben werden.

Die entscheidende Schutzmaßnahme ist deshalb eine klare Change-Impact-Analyse. Vor jeder Änderung wird geprüft, ob sich Aufgabe, Umgebung, Sicherheitsfunktion, Softwareverhalten, Datenverarbeitung, Schnittstellen, Verantwortlichkeiten oder Restrisiken verändern. Falls ja, darf die Änderung nicht einfach im laufenden Betrieb untergehen, sondern muss in die Revalidierungslogik zurückgeführt werden.

11. Datenschutz, Cybersecurity und menschliche Verantwortung

Physical AI verbindet Sensorik, Datenverarbeitung und physische Handlung. Dadurch werden Datenschutz und Cybersecurity unmittelbar sicherheitsrelevant. Ein humanoider Roboter kann Kameras, Mikrofone, Tiefensensoren, LiDAR, Funkmodule, Karten, Zugangsdaten, Cloudschnittstellen und Fernwartung enthalten. In sensiblen Umgebungen können daraus erhebliche Risiken entstehen.

Die Grundhaltung sollte Zero Trust sein: Jede Identität, jedes Gerät, jeder Zugriff, jedes Update und jede Schnittstelle muss geprüft werden. Das gilt nicht nur für externe Angriffe, sondern auch für Fehlkonfigurationen, unklare Rollen, unkontrollierte Fernwartung oder unautorisierte Aufgabenerweiterungen. Bei einem körperlich handelnden System kann ein IT-Fehler zu einem physischen Risiko werden.

Thema	Leitfrage	Praktische Konsequenz
Datensparsamkeit	Welche Daten braucht der Roboter wirklich für die Aufgabe?	Keine unnötige Speicherung identifizierbarer Rohdaten
Edge-Verarbeitung	Kann Wahrnehmung lokal verarbeitet werden?	Reduktion von Cloudabhängigkeit und Datenschutzrisiken
Rollen und Rechte	Wer darf Aufgaben, Karten, Updates oder Betriebsmodi ändern?	Rollenmodell, Vier-Augen-Prinzip für kritische Änderungen
Updatekontrolle	Welche Softwareversion ist freigegeben?	Versionierung, Test vor Rollout, Rollback-Fähigkeit
Logging	Welche Ereignisse müssen nachvollziehbar sein?	Sicherheitsrelevante Ereignisdaten statt Dauerüberwachung
Fernwartung	Wann und wie darf extern zugegriffen werden?	Zeitlich begrenzter Zugriff, Protokollierung, Freigabe durch Betreiber
Sicherer Zustand	Was passiert bei Funkverlust, Sensorausfall oder Manipulationsverdacht?	Stoppen, Rückzug, Hilfeanforderung oder definierter Fallback

Menschliche Verantwortung bleibt die zentrale Klammer. Bei Routineaufgaben kann Autonomie sinnvoll sein. Bei Grenzüberschreitungen, Unsicherheit, gefährlichen Gütern, unklaren Übergaben oder sensiblen Interaktionen muss eine menschliche Kontroll- oder Eskalationslogik greifen. Human in the Loop bedeutet nicht, jede einzelne Bewegung manuell freizugeben. Es bedeutet, dass kritische Entscheidungen nicht in der Komplexität eines Modells verschwinden dürfen.

12. Pilotierung, Revalidierung und Skalierung

Ein seriöser Einstieg in Physical AI beginnt nicht mit maximaler Autonomie, sondern mit einem begrenzten, messbaren und kontrollierten Pilot. Der Pilot muss so gewählt sein, dass er einen echten Nutzen erzeugt, aber nicht sofort die schwierigste und sensibelste Aufgabe adressiert. Gute Startaufgaben sind wiederholbar, räumlich begrenzt, sicher abbrechbar und wenig körpernah.

1. **Anwendungsfälle sammeln:** Welche Aufgaben sind heute belastend, wiederkehrend, zeitkritisch oder organisatorisch aufwendig?
2. **Eignung bewerten:** Welche Aufgaben sind klar begrenzbar, messbar und sicher abtrennbar?
3. **ODD-Entwurf erstellen:** Räume, Wege, Lasten, Personen, Zeiten, Schnittstellen, Daten und Fallbacks beschreiben.
4. **Umgebung erfassen:** Reale Daten mit geeigneter Erfassungstechnik aufnehmen, validieren und versionieren.
5. **Risiken und Testfälle ableiten:** Normalfälle, Randfälle, Fehlerszenarien und Abbruchkriterien definieren.
6. **Pilot kontrolliert durchführen:** Begrenzte Freigabe mit klarer Aufsicht, Monitoring und Ereignisprotokollierung.
7. **Auswerten und revalidieren:** Near Misses, Stoppereignisse, Bedienprobleme und technische Abweichungen auswerten.
8. **Skalierung nur bei Evidenz:** Erweiterung erst, wenn ODD, Daten, Testfälle, Schulung und Betrieb belastbar sind.

Revalidierungsauslöser

- Neue Aufgabe oder erweiterte Tätigkeit des Roboters.
- Andere Lasten, Werkzeuge, Übergabeformen oder Interaktionsarten.
- Neue Räume, Etagen, Türen, Aufzüge, Verkehrsbereiche oder Sperrzonen.
- Softwareupdate, KI-Modellupdate, Kartenupdate oder Sensoränderung.
- Umbau der Umgebung, neue Regale, geänderte Fluchtwege oder veränderte Verkehrsströme.
- Wiederholte Near Misses, unerwartete Stopps, Fehlklassifikationen oder Bedienprobleme.
- Neue regulatorische, versicherungstechnische oder kundenspezifische Anforderungen.

13. Rolle von Maucher CNC Robotic und Maucher Formenbau

Die Stärke von Maucher liegt darin, aus der industriellen Realität zu kommen und zwei wesentliche Felder miteinander zu verbinden: den Maschinenbau auf der einen Seite und die Fertigung hochkomplexer Bauteile mit unterschiedlichsten Technologien auf der anderen. Genau diese Kombination ist entscheidend. Robotik wird nicht nur aus der Perspektive der Automatisierung gedacht, sondern auch aus der täglichen Erfahrung industrieller Produktion heraus.

Ein wesentlicher Faktor ist die enge Verbindung zwischen Maucher Formenbau und Maucher CNC Robotic. Beide Unternehmen kommen aus demselben industriellen Umfeld, arbeiten am selben Standort und sind tief in der praktischen Umsetzung verankert. Seit Jahrzehnten entstehen hier Bauteile, Prozesse und Lösungen unter echten industriellen Anforderungen. Maucher liefert aus drei Produktionswerken als Tier 1 Zulieferer an namhafte Automobilhersteller weltweit. Das prägt das Denken: Qualität, Wiederholbarkeit, Prozesssicherheit und Verantwortung sind keine Schlagworte, sondern tägliche Praxis.

Eine zentrale Rolle spielt dabei Peter Strittmatter, der als Inhaber beider Unternehmen den Raum für solche Entwicklungen schafft. Für ihn ist Robotik ein entscheidender Schlüssel, um auch unter den zunehmend schwierigen Rahmenbedingungen in Deutschland zukunftsfähig zu bleiben. Dabei versteht er Robotik nicht als isolierte Automatisierungslösung, sondern als Teil eines größeren industriellen Gesamtsystems. Genau diese Haltung prägt auch den Weg von Maucher CNC Robotic.

Mit Blick auf Physical AI sieht sich Maucher CNC Robotic nicht als notifizierte Stelle und nicht als Ersatz für formale Prüfstellen. Die Rolle liegt vielmehr darin, eine industrielle Blaupause für andere Unternehmen in Europa zu schaffen: Einsätze strukturieren, Risiken frühzeitig erkennen, technische Akten vorbereiten, Betreiberangaben in prüfbare Anforderungen übersetzen und eine klare Schnittstelle zu Auditoren, Sachverständigen oder Prüfstellen schaffen.

Selbstverständnis

Maucher CNC Robotic will nicht nur für sich selbst die Lücke zwischen Robotikvision und belastbarem Betrieb schließen. AURA ONE ist dabei ein Beispielbaustein, weil reale Produktionsumgebungen erfassbar und technisch bewertbar werden. Die Agentenlogik ist ein weiterer Baustein, weil Prüfprozesse strukturiert und nachvollziehbar werden. Die industrielle Erfahrung aus Maucher Formenbau und Maucher CNC Robotic sorgt dafür, dass daraus keine reine Präsentation entsteht, sondern ein Ansatz aus echter Produktionsnähe.

14. Europäische Perspektive

Europa steht bei Physical AI vor einer strategischen Aufgabe. Es wird nicht ausreichen, auf globale Plattformanbieter zu warten und deren Systeme unverändert in europäische Betriebe zu stellen. Wenn Europa handlungsfähig bleiben will, muss es eigene Kompetenz in sicherer Integration, Nachvollziehbarkeit, Betrieb, Normung, Datenhoheit und industrieller Skalierung aufbauen.

Die Stärke Europas liegt nicht nur in einzelnen KI-Modellen. Sie liegt in Maschinenbau, Automatisierung, CE-Erfahrung, technischer Dokumentation, Qualitätsmanagement, Datenschutz, Sicherheitskultur und mittelständischer Umsetzungskompetenz. Genau diese Fähigkeiten werden gebraucht, um Physical AI aus dem Labor in reale Arbeitswelten zu bringen.

Wenn Unternehmen stärker lernen, Wissen zu teilen, Schnittstellen zu standardisieren und sich gegenseitig bei sicheren Pilotierungen zu unterstützen, kann daraus eine europäische Vertrauensinfrastruktur entstehen. In einer Welt, in der autoritäre Großmächte technologisch und wirtschaftlich zunehmend Druck ausüben, ist diese Fähigkeit mehr als ein technisches Detail. Sie ist Teil industrieller Souveränität.

15. Praxisanhang: Checklisten, Reifegradmodell und Begriffe

15.1 Hersteller-Checkliste

Prüffrage	Warum sie wichtig ist
Ist die bestimmungsgemäße Verwendung konkret und nicht nur werblich beschrieben?	Nur konkrete Angaben können in eine standortspezifische ODD übersetzt werden.
Sind Ausschlüsse und Einsatzgrenzen klar dokumentiert?	Grenzen sind für sichere Integration genauso wichtig wie Fähigkeiten.
Sind Sensorgrenzen, Blindbereiche und problematische Umgebungsbedingungen beschrieben?	Glas, Spiegelungen, Licht, Funklöcher und Menschenmengen können die Wahrnehmung beeinflussen.
Sind Software-, Modell- und Firmwarestände versioniert?	Ohne Versionierung ist spätere Nachvollziehbarkeit nicht möglich.
Gibt es ein kontrolliertes Update- und Rollbackverfahren?	Updates können sicherheitsrelevantes Verhalten verändern.
Sind Logs, Schnittstellen und Ereignisdaten für den Betrieb nutzbar?	Der Betreiber benötigt Evidenz für Monitoring, Ereignisanalyse und Revalidierung.
Sind Schulungs-, Wartungs- und Integrationsanforderungen definiert?	Unscharfe Betreiberanforderungen führen später zu Fehlbedienung und Verantwortungsunklarheit.

15.2 Inbetriebnehmer-Checkliste

Prüffrage	Warum sie wichtig ist
Wurde die reale Umgebung technisch und organisatorisch aufgenommen?	Der Einsatz muss auf realen Wegen, Personenströmen, Sperrzonen und Schnittstellen beruhen.
Wurde aus Herstellerangaben und Betreiberziel eine konkrete ODD erstellt?	Nur so wird aus einer Produktfähigkeit eine standortbezogene Freigabelogik.

Prüffrage	Warum sie wichtig ist
Wurden Normalfälle, Randfälle und Fehlerszenarien getestet?	Der kritische Wert liegt oft nicht im normalen Ablauf, sondern in Grenzsituationen.
Sind Karten, Zonen, Geschwindigkeiten, Rollenrechte und Fallbacks dokumentiert?	Konfiguration ist Teil der Sicherheits- und Nachweisstruktur.
Wurden offene Punkte, Restrisiken und Ausschlüsse übergeben?	Der Betreiber darf nicht glauben, dass ungeklärte Punkte automatisch freigegeben sind.
Wurde festgelegt, welche Änderungen eine Revalidierung auslösen?	Ohne Änderungslogik wird der geprüfte Einsatz im Alltag schleichend verlassen.

15.3 Betreiber-Checkliste für den Einstieg

Bereich	Fragen
Aufgabe	Was soll der Roboter konkret tun? Was soll er ausdrücklich nicht tun?
Nutzen	Welche Entlastung, Qualität, Geschwindigkeit oder Verfügbarkeit wird erwartet?
Umgebung	Welche Räume, Wege, Engstellen, Türen, Aufzüge, Böden und Sperrbereiche sind betroffen?
Menschen	Wer begegnet dem Roboter? Mitarbeiter, Besucher, Patienten, Kinder, externe Dienstleister?
Objekte	Welche Lasten, Güter, Werkzeuge oder sensiblen Gegenstände werden bewegt?
Daten	Welche Sensoren erfassen personenbezogene oder vertrauliche Informationen?
IT	Welche Netzwerke, Schnittstellen, Zugänge und Updates sind beteiligt?
Sicherheit	Wann muss der Roboter stoppen? Wie wird Hilfe angefordert? Wer darf eingreifen?
Betrieb	Wer ist verantwortlich? Wer schult? Wer wertet Ereignisse aus?
Änderungen	Was löst eine erneute Prüfung aus?

15.4 Reifegradmodell für Physical-AI-Einsätze

Stufe	Beschreibung	Typisches Risiko
0 - Demonstration	Technische Vorführung ohne belastbare Einsatzgrenzen	Show wird mit Betrieb verwechselt
1 - Geführter Test	Manuelle oder überwachte Tests in begrenztem Bereich	Nutzen sichtbar, aber Nachweis noch schwach
2 - Strukturierter Pilot	ODD, Testfälle, Umgebungsdaten und Monitoring sind definiert	Randfälle und Änderungen müssen ausgewertet werden
3 - Begrenzter Betrieb	Freigegebene Aufgabe in klarer Umgebung mit Rollen, Logs und Revalidierung	Schleichende Einsatzweiterung ohne Prüfung
4 - Skalierter Betrieb	Mehrere Bereiche oder Standorte mit standardisierter Nachweislogik	Komplexität von Versionen, Updates und Standortunterschieden
5 - Kontinuierlich auditierbarer Betrieb	Betriebserfahrung, Änderungen, Testfälle und Nachweise bilden einen geschlossenen Lebenszyklus	Hohe Anforderungen an Governance und Datenqualität

15.5 Begriffe

Begriff	Arbeitsdefinition
Physical AI	KI-Systeme, die über Sensorik und Aktorik in der realen Welt handeln und damit physische Wirkung erzeugen.
ODD	Operational Design Domain: zulässige Einsatzdomäne eines Systems mit Aufgaben, Räumen, Menschen, Lasten, Bedingungen und Grenzen.
Near Miss	Ereignis, bei dem kein Schaden eintritt, aber ein sicherheitsrelevanter Grenzfall sichtbar wird.
Digitale Vertrauensinfrastruktur	Gesamtheit aus Daten, Prozessen, Nachweisen, Rollen und Monitoring zur beherrschten Nutzung von Physical AI.
Gaussian Splat	Fotorealistische 3D-Darstellung aus Bilddaten, nützlich für Visualisierung, aber nicht automatisch metrisch oder sicherheitstechnisch belastbar.
Revalidierung	Erneute Bewertung nach Änderungen an Aufgabe, Umgebung, Software, Daten, Sensorik oder Betriebsbedingungen.
Technische Akte	Strukturierte Dokumentation der relevanten Unterlagen, Nachweise, Annahmen, Versionen und Freigaben.

Schlussbemerkung

Physical AI wird nicht durch eine einzelne Technologie verantwortbar. Sie wird verantwortbar durch das Zusammenspiel aus realer industrieller Erfahrung, präzise beschriebenen Einsatzgrenzen, belastbaren Umgebungsdaten, klarer Verantwortlichkeit, sinnvoller Simulation, dokumentierten Testfällen, kontrollierter Pilotierung und kontinuierlichem Lernen aus dem Betrieb. AURA ONE zeigt beispielhaft, wie reale Umgebungen in diese Logik überführt werden können. Andere Systeme können denselben Zweck erfüllen, wenn sie die gleichen Anforderungen an Datenqualität, Nachvollziehbarkeit und Validierung erfüllen. Entscheidend ist die Haltung: nicht zuerst versprechen, sondern zuerst beherrschbar machen.