

HU-RSC

Humanide Robotics Safety Class

Klassifikationssystem für die physische Sicherheit
smarter Robotiksysteme im DACH-Mittelstand

Impulspapier

Version: v0.2.11 (Mai 2026)

Stand: 16. Mai 2026

Herausgeber: Humanide GmbH, Köln (HRB 115169)

Schwester-Modell: HU-RAC — Humanide Robotics Assurance Class (Daten und Resilienz), v0.3.1

Status: Öffentliches Impulspapier. Verwendung und Weitergabe unter Angabe der Quelle (Humanide GmbH, HU-RSC v0.2.11, Mai 2026) erbeten.

Inhalt

0	Methodischer Disclaimer und Lese-Hinweise.....	4
0.0	Zweck, Adressaten und Reichweite.....	4
0.1	Was HU-RSC ist und was es nicht ist.....	4
0.2	Methodische Schwellenwert-Findung.....	5
0.3	Verhältnis zu anderen Humanide-Dokumenten.....	5
1	Verortung im Klassifikationssystem (HU-RAC × HU-RSC).....	6
1.1	Zwei Modelle, ein System.....	6
1.2	Was HU-RSC nicht abdeckt.....	6
1.3	Sieben Use-Case-Felder im Fokus.....	6
2	Regulatorischer Rahmen.....	8
2.1	Maschinenverordnung (EU) 2023/1230.....	8
2.2	KI-Verordnung (EU) 2024/1689.....	9
2.3	Produktsicherheits- und Produkthaftungsregime.....	9
2.4	Cyber Resilience Act (Verordnung (EU) 2024/2847).....	10
2.5	Einschlägige Sicherheitsnormen.....	11
3	Architektur des Modells.....	13
3.1	Strukturparallele zu HU-RAC.....	13
3.2	HU-RSC-spezifische Erweiterungen.....	13
3.3	Tier-Skala — Begriffsklärung.....	13
4	Die sechs Achsen — Bewertungsinhalt im Detail.....	15
4.1	Achse 1 — Einsatzumgebung.....	15
4.2	Achse 2 — Bauart, Bewegungsraum und kinetisches Schadenspotenzial.....	15
4.3	Achse 3 — Schadenstypen und Schadensschwere.....	16
4.4	Achse 4 — Autonomiegrad.....	17
4.5	Achse 5 — Sicherheitsarchitektur (dreisäulig).....	17
4.5.1	Säule 1 — Klassische Sicherheitsarchitektur.....	17
4.5.2	Säule 2 — KI-Sicherheitsarchitektur.....	18
4.5.3	Säule 3 — Lifecycle-Update-Mechanik.....	19
4.6	Achse 6 — Exponierte Personen und Expositionsfrequenz.....	19
5	Tier-Skala 1–5 mit Schwellenwerten.....	21
5.1	Tier 1 — minimales Restrisiko.....	21
5.2	Tier 2 — begrenztes Restrisiko.....	21
5.3	Tier 3 — erhöhtes Restrisiko.....	22
5.4	Tier 4 — hohes Restrisiko.....	22
5.5	Tier 5 — kritisches Restrisiko.....	23
6	Erwartungsmatrizen (E-Min, E-Plus, R).....	24

6.1	Erwartungsmatrix Achse 1 — Einsatzumgebung.....	24
6.2	Erwartungsmatrix Achse 2 — Bauart und kinetisches Schadenspotenzial.....	25
6.3	Erwartungsmatrix Achse 3 — Schadenstypen und Schadensschwere.....	26
6.4	Erwartungsmatrix Achse 4 — Autonomiegrad.....	27
6.5	Erwartungsmatrix Achse 5 — Sicherheitsarchitektur (dreisäulig).....	28
6.6	Erwartungsmatrix Achse 6 — Exponierte Personen und Expositionsfrequenz.....	32
7	Sekundärdimensionen.....	34
7.1	Business-Kritikalität A/B/C.....	34
7.2	Anbieter-Resilienz R1/R2/R3.....	34
7.3	Verhältnis zu Achse 5 Säule 3.....	35
8	Aggregations- und Reklassifikationsregeln.....	36
8.1	Aggregation der sechs Achsen.....	36
8.2	Aggregation innerhalb Achse 5 — Mindest-Floor-Logik.....	36
8.3	Reklassifikation bei wesentlichen Veränderungen.....	37
9	Mindestkopplung HU-RSC × HU-RAC.....	38
9.1	Die asymmetrische Mindestkopplung.....	38
9.2	Begründung der Kopplung.....	38
9.3	Asymmetrie.....	38
9.4	Operative Konsequenzen.....	39
10	Anwendung in der Beschaffungspraxis.....	40
10.1	Drei-Schritte-Logik.....	40
10.2	Anbindung an HU-RAC und Anforderungskatalog.....	40
10.3	Anwendungsbeispiel — humanoider Roboter in KMU-Werkstatt.....	40
11	Schlusswort.....	42
12	Anhang — Mapping-Tabellen ISO-Klassen.....	43
12.1	Hinweise zur Verwendung der Mapping-Tabelle.....	43
13	Anhang — Glossar.....	44
14	Anhang — Referenzen.....	45

0 Methodischer Disclaimer und Lese-Hinweise

0.0 Zweck, Adressaten und Reichweite

HU-RSC bildet zusammen mit dem Schwester-Modell HU-RAC einen Kommunikationsrahmen. Es wird intern von der Humanide GmbH als gemeinsame Sprache zwischen drei Parteien entwickelt und verwendet:

- die Humanide GmbH selbst als Inverkehrbringerin der Produkte unter ihren Marken (Mowio, Wuffi, Robofixx, Robokitchen, Omtanke);
- Dienstleister, Distributoren und Hersteller, die Komponenten und Plattformen für die Humanide GmbH liefern oder mitdeployen;
- Einkäufer und Kunden, einschließlich der Einkaufs- und Procurement-Abteilungen von Kundenorganisationen, die Humanide-Produkte gegen ihre eigenen internen Anforderungen prüfen.

Zweck ist die strukturierte Verständigung über das Datensouveränitätsprofil (HU-RAC) und das physische Sicherheitsprofil (HU-RSC) eines Robotik-Systems vor der Beschaffung — zu einem Zeitpunkt, in dem kein einheitliches, öffentlich anerkanntes Regelwerk humanoide Robotik, KI-gestützte Sicherheitsfunktionen und den vollständigen Lifecycle cyber-physischer Robotik integriert abdeckt.

HU-RSC ist deshalb weder ein Konformitätsbewertungssystem, eine Zertifizierung noch ein Konkurrent zu ISO-, IEC-, EN- oder anderen Branchennormen. Aussagen der Form „Dieses Produkt erreicht HU-RAC X / HU-RSC Y“ sind interne Eigeneinordnungen der Humanide GmbH; Dritte, die diese Einordnungen übernehmen, tun das freiwillig als gemeinsamen Bezugsrahmen. Der Rahmen ist ausdrücklich darauf angelegt, durch harmonisierte Normen abgelöst zu werden, sobald diese vorliegen (ISO 25785-1, ISO/IEC TS 22440 und andere).

Gewährleistungs- und Haftungsausschluss. Dieses Papier ist weder eine wissenschaftliche Veröffentlichung noch ein juristisches Gutachten noch eine verbindliche Konformitätsbewertung. Es ist ein Arbeitsdokument der Humanide GmbH, das aus Transparenz- und Diskussionsgründen öffentlich zugänglich gemacht wird. Die Inhalte wurden vor der Veröffentlichung nicht durch externe anwaltliche Beratung validiert. Die Humanide GmbH stellt die Inhalte ohne jegliche ausdrückliche oder konkludente Gewährleistung hinsichtlich Richtigkeit, Vollständigkeit, Aktualität, Eignung für einen bestimmten Zweck oder Freiheit von Schutzrechten Dritter bereit. Aussagen zum regulatorischen oder normativen Umfeld können ohne Vorankündigung veraltet sein. Soweit gesetzlich zulässig, schließt die Humanide GmbH einschließlich der für sie handelnden natürlichen Personen jegliche Haftung für direkte, indirekte, beiläufige, mittelbare, besondere oder pönale Schäden aus, die aus der Nutzung dieses Papiers oder dem Vertrauen auf seine Inhalte resultieren oder mit ihnen in Verbindung stehen. Leser und Adopter handeln auf eigene Verantwortung. Die rechtsverbindliche Beurteilung zur Konformität, Sicherheit und zum Datenschutz bleibt bei den verantwortlichen Parteien nach den einschlägigen Normen und Regulierungen und wird durch ein HU-RSC-Tier nicht ersetzt. Sollten einzelne Bestimmungen dieses Haftungsausschlusses unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

0.1 Was HU-RSC ist und was es nicht ist

HU-RSC ist eine Beschaffungs-Heuristik, kein Sicherheits-Engineering-Werkzeug.

Eine HU-RSC-Tier-Klassifikation **ersetzt keine Risikobeurteilung** nach ISO 12100 und ist keine Konformitätsbewertung im Sinne der Maschinenverordnung (EU) 2023/1230. Verantwortung für Konformität, Risikobeurteilung, Inverkehrbringer-

Pflichten nach Maschinenverordnung sowie Betreiber-Pflichten nach BetrSichV bleibt vollständig bei den jeweils Verpflichteten.

HU-RSC unterstützt Beschaffer und Betreiber dabei, *vor dem Kauf* systematisch einzuschätzen, welches Sicherheits-Anspruchsniveau ein Robotiksystem erreichen muss und ob ein konkretes Produkt dieses Niveau plausibel adressiert. Die rechtsverbindliche Bewertung erfolgt durch die zuständigen Akteure (Hersteller, benannte Stellen, Sachverständige) und ist nicht Gegenstand dieses Modells.

0.2 Methodische Schwellenwert-Findung

Die numerischen Tier-Schwellenwerte dieses Modells (kinetische Energie in Joule, Mindest-PL/SIL pro Tier, Schadensschwere-Klassen) sind aus den einschlägigen Normen abgeleitet — namentlich ISO 12100 Tabelle B.3 für die Schadensschwere-Skala, ISO 13849-1 für Performance Levels, ISO/TS 15066 für Mensch-Roboter-Kollaborationsschwellen und IEC 61508 für Safety Integrity Levels. Sie sind nicht aus den Beispielprodukten der bewerteten Anbieter abgeleitet.

Diese Reihenfolge ist methodisch zwingend: Wer Schwellen aus Produkten ableitet, betreibt Confirmation Bias und kalibriert das Modell auf die Anbieter, die zufällig auf dem Markt sind. Die Anbieter-Validierung dient der Prüfung der vorab fixierten Schwellen, nicht ihrer Definition.

0.3 Verhältnis zu anderen Humanide-Dokumenten

Dieses Impulspapier definiert das HU-RSC-Modell. Konkrete anbieter-bezogene Bewertungen finden sich nicht hier, sondern im Anforderungskatalog v2.x (Dokument 01, intern) und im Anforderungsprofil v2.x (Dokument 03, extern). Diese Trennung hält das Impulspapier zeitstabil — Anbieter-Bewertungen können aktualisiert werden, ohne dass das Modell selbst neu publiziert werden muss.

Das HU-RAC-Schwester-Modell behandelt Datenschutz und Anbieter-Resilienz und wird in Kapitel 1 ausführlich verortet.

1 Verortung im Klassifikationssystem (HU-RAC × HU-RSC)

1.1 Zwei Modelle, ein System

Das Humanide-Klassifikationssystem besteht aus zwei nominell unabhängigen, strukturell parallelen Modellen mit asymmetrischer Kopplung. HU-RAC bewertet die digitale Souveränität und Anbieter-Resilienz eines Robotiksystems, HU-RSC bewertet seine physische Sicherheit gegenüber Personen. Beide Modelle teilen Architektur, Tier-Skala 1–5, Sechs-Achsen-Logik, Aggregationsprinzip und Erwartungsmatrix-Struktur.

Die Strukturparallele ist nicht ästhetisch, sondern methodisch zwingend: Beschaffer sollen ein einheitliches mentales Modell anwenden können. Wer mit HU-RAC vertraut ist, kann HU-RSC ohne neue Lernkurve nutzen — und umgekehrt. Die externe Kommunikation lautet einheitlich „Dieses Produkt erreicht HU-RAC X / HU-RSC Y“.

1.2 Was HU-RSC nicht abdeckt

Drei Bewertungsdimensionen liegen ausdrücklich außerhalb von HU-RSC und werden anderswo behandelt:

- **Digitale Souveränität** — Datenschutz und Anbieter-Resilienz im Sinne von Datensouveränität — Gegenstand von HU-RAC.
- **Cybersicherheit** — Cyber-Aspekte werden ausschließlich in HU-RAC Matrix 5.3 geführt. HU-RSC adressiert Cyber-Sicherheit nicht direkt, sondern nur indirekt über die Mindestkopplung (siehe Kapitel 9), weil Sicherheits-Telemetrie integritätsgeschützt sein muss.
- **Funktionale Capability** — Nutzlast, MTBF, Reichweite, Autonomiegrad als Leistungsmerkmal werden im Anforderungskatalog Teil 5 als kontextspezifische Bewertung pro Use Case geführt — nicht als universell vergleichbares Tier.

Sachwertschäden werden nicht in HU-RSC, sondern als nachrangige Erwartung im Anforderungskatalog Teil 5 (Funktionale und betriebliche Eignung) behandelt. HU-RSC fokussiert auf Personenschutz im Sinne der ISO-12100-Logik.

1.3 Sieben Use-Case-Felder im Fokus

HU-RSC ist auf die Robotik-Anwendungsfelder kalibriert, die im DACH-Mittelstand kurzfristig kommerziell relevant sind:

- **Konsumentennahe Robotik** — Mäh-, Saug-, Reinigungsroboter im Privatkunden- und Light-Commercial-Bereich (B2C/SoHo).
- **Service-Robotik im halböffentlichen Raum** — Reinigungs-, Inspektions-, Sicherheitsroboter in Hotels, Krankenhäusern, Pflegeeinrichtungen, Schulen.
- **Industrielle Robotik im KMU-Mittelstand** — Produktions-, Logistik-, Inspektionsroboter im KMU-Industriebereich (außerhalb klassischer Großindustrie-Sicherheitskäfige).

- **Outdoor-Robotik** — Outdoor-Roboter in landwirtschaftlichen, kommunalen und gewerblichen Außenbereichen.
- **Humanoide Robotik (Pilotphase)** — Erste Pilotanwendungen humanoider Roboter im KMU-Bereich (z. B. Pick-and-Place, Werkstückzuführung).
- **Assistenzrobotik** — Persönliche Assistenz, Pflegeunterstützung, Edutainment.
- **Mobile Logistikrobotik** — AGV/AMR im KMU-Logistikkontext.

Die Tier-Skala ist so kalibriert, dass alle sieben Felder abgedeckt sind. Spezialdomänen wie Medizinprodukte (MDR), Außenanlagen kerntechnischer Anlagen oder militärische Robotik sind nicht im Skopus.

Hinweis zur Begrifflichkeit: Ein humanoider Roboter ist ein Robotik-System mit anthropomorpher Morphologie (Oberkörper und zwei Arme, plus zwei Beine oder andere geeignete Fortbewegungsmittel), mit Umwelt-Wahrnehmungsfähigkeit, vorgesehen für eine Vielfalt menschlicher Aufgaben; kann autonom oder teleoperiert betrieben werden. Der Roboter kann Greifer einschließen; andernfalls sind Greifer Teil des umgebenden humanoiden Robotersystems, welches mindestens einen humanoiden Roboter, Endeffektoren, Werkstücke, periphere Komponenten und Ladeinfrastruktur umfasst. Adaptiert nach Fraunhofer IPA KMUmanoid (2025).

Praxisorientierte Einordnung (verbrauchernahe Robotik). Ein typischer Mowio-Klasse-Mähroboter mit rotierender Schneideklinge in einem privaten Garten, der ohne lokale RTK-Infrastruktur, aber mit Cloud-basierter Positionierung arbeitet, platziert sich auf Achse 2 um Tier 3 (kinetische Energie im 10–80-J-Bereich plus rotierende Werkzeugbewegung) und auf Achse 1 ebenfalls um Tier 3 (teilkontrollierte Umgebung mit möglichem Drittpartei-Kontakt). Achse 6 erreicht typischerweise Tier 3 mit Haustierkontakten als Restrisiko. Die Gesamteinordnung Tier 3 ist für die meisten gegenwärtigen Marktangebote plausibel.

2 Regulatorischer Rahmen

HU-RSC steht im Spannungsfeld eines Bündels regulatorischer Vorgaben, die sich in den Jahren 2026 bis 2027 stark verdichten. Dieses Kapitel skizziert die für Beschaffer und Betreiber relevanten Rechtsakte und Normen — ohne Anspruch auf juristische Vollständigkeit. Bei konkreten Compliance-Fragen ist anwaltliche oder sachverständige Beratung erforderlich.

2.1 Maschinenverordnung (EU) 2023/1230

Die Maschinenverordnung 2023/1230 löst die Maschinenrichtlinie 2006/42/EG ab und ist ab dem 20. Januar 2027 nach Artikel 54 anzuwenden. Sie ist als Verordnung unmittelbar wirksam, eine nationale Umsetzung ist nicht erforderlich. Für Robotiksysteme bringt sie wesentliche Verschärfungen:

Maßgeblich ist die Berichtigung im Amtsblatt OJ L 169 vom 4. Juli 2023; der ursprüngliche Erstdruck OJ L 165 vom 29. Juni 2023 enthielt einen Berechnungsfehler („14. Januar 2027“), der inzwischen amtlich korrigiert ist.

- **Anhang III** — Sie regelt Sicherheitsanforderungen an Maschinen mit selbstentwickelndem Verhalten und an Sicherheitsbauteile mit Software, die für die Sicherheitsfunktion wesentlich sind.
- **Wesentliche Veränderung** — Wesentliche Veränderungen einer in Verkehr gebrachten Maschine — etwa durch Software-Updates, die das Sicherheits- oder Funktionsverhalten verändern — können eine erneute Konformitätsbewertung auslösen. Die Auslegung ist im Detail noch offen.
- **Sicherheitsbauteil-Definition** — Artikel 3(3) definiert „Sicherheitsbauteil“ als „eine körperliche oder digitale Komponente, einschließlich Software, eines Produkts im Anwendungsbereich dieser Verordnung, die dazu bestimmt ist, eine Sicherheitsfunktion zu erfüllen, und die unabhängig in Verkehr gebracht wird; ihr Versagen oder ihre Fehlfunktion gefährdet die Sicherheit von Personen“. Software-basierte Sicherheitsbauteile sind ausdrücklich im Anwendungsbereich.
- **Anhang III (EHSRs)** — **Anhang III enthält die grundlegenden Sicherheits- und Gesundheitsschutzanforderungen, einschließlich Abschnitt 1.1.6 zu selbstentwickelnden Systemen, Abschnitt 1.1.9 „Schutz vor Korruption“ und Abschnitt 1.2.1 „Sicherheit und Zuverlässigkeit von Steuerungssystemen“.** Wo dieses Impulspapier später „MR Anhang III“ als Tier-Anforderung referenziert, ist die Gesamtheit der EHSRs gemeint, mit Schwerpunkt auf den KI- und Cybersecurity-Abschnitten.

Status der Kommissions-Leitlinien. Die Europäische Kommission bereitet ein Leitfaden-Dokument und einen Durchführungsbeschluss mit einer Liste harmonisierter Normen vor. Entwürfe zu „KI-gestützten Sicherheitsfunktionen“ und „Software als Sicherheitsbauteil“ werden Mitte 2026 erwartet; der Durchführungsbeschluss zu harmonisierten Normen wird bis Ende 2026 erwartet. Stand März 2026 hat die Industrie ihre Forderung nach Verschiebung der KI-Bestimmungen der Maschinenverordnung zurückgezogen, fordert aber weiterhin die Angleichung der Cybersecurity-Anforderungen an das CRA-Anwendungsdatum 11. Dezember 2027 — eine zehnmonatige Lücke zwischen MR-Anwendung (20. Januar

2027) und CRA-Anwendung (11. Dezember 2027), die Beschaffungsentscheidungen einbeziehen müssen.

2.2 KI-Verordnung (EU) 2024/1689

Die KI-Verordnung ist im August 2024 in Kraft getreten; ihre Pflichten gelten gestaffelt nach Artikel 113. Für HU-RSC sind zwei Pfade zu unterscheiden. Nach Artikel 6(1) — KI als Sicherheitsbauteil eines Produkts, das von der in Anhang I aufgeführten Harmonisierungsrechtsetzung der Union erfasst ist, einschließlich der Maschinenverordnung — gelten die Hochrisiko-Pflichten ab 2. August 2027. Nach Artikel 6(2) — KI-Systeme im Sinne des Anhangs III — gelten die Hochrisiko-Pflichten ab 2. August 2026. Die meisten verbrauchernahen und industriellen Robotiksysteme mit sicherheitsrelevanten KI-Funktionen fallen in den Pfad nach Artikel 6(1). Mit dem Vorschlag für ein Digital Omnibus on AI vom 19. November 2025 hat die Europäische Kommission Verschiebungen vorgeschlagen: Hochrisiko-Pflichten nach Anhang III auf 2. Dezember 2027, und in Anhang-I-Produkten eingebettete KI-Systeme auf 2. August 2028. Rat und Parlament haben im Frühjahr 2026 Verhandlungspositionen erarbeitet, die diese Verschiebungs-Daten im Wesentlichen unterstützen; eine formale Annahme stand zum Redaktionszeitpunkt jedoch noch aus. Bis zur Veröffentlichung des förmlichen Textes im Amtsblatt bleiben die obigen Artikel-113-Termine rechtsverbindlich. Artikel 6(5) verpflichtet die Kommission, bis spätestens 2. Februar 2026 Leitlinien zur praktischen Umsetzung des Artikel 6 zusammen mit einer umfassenden Liste praktischer Anwendungsbeispiele für Hochrisiko- und Nicht-Hochrisiko-KI-Systeme vorzulegen; die Kommission hat diese Frist versäumt, ein Entwurf zur Konsultation wurde anschließend in die Omnibus-Verhandlungen integriert. Beschaffungsentscheidungen in 2026 erfolgen somit ohne verbindliche Leitlinien der Kommission zur Hochrisiko-Klassifikation von Robotik-KI. Für HU-RSC sind drei Punkte zentral:

- **Hochrisiko-KI im Maschinenkontext** — Robotiksysteme, die als Sicherheitsbauteil für Maschinen im Sinne der Maschinenverordnung wirken, fallen typischerweise in die Hochrisiko-Klassifikation der KI-Verordnung. Die Pflichten umfassen Risikomanagement, Datenqualitätsanforderungen, Transparenz-Dokumentation und Aufsichtsmechanismen.
- **Erklärbarkeit** — Die KI-Verordnung verlangt Erklärbarkeit der Entscheidungslogik in einem Maß, das für viele Robotik-KI-Systeme noch nicht etabliert ist — insbesondere für Vision-Language-Action-Modelle (VLAs).
- **Schnittstelle MVO/KI-VO** — Die Verzahnung mit der Maschinenverordnung (Anhang III) ist ein offenes Auslegungsthema. ISO/IEC TR 5469 „Artificial Intelligence — Functional Safety and AI Systems“ bietet einen ersten technischen Rahmen.

2.3 Produktsicherheits- und Produkthaftungsregime

Drei weitere Rechtsakte rahmen den Beschaffungsentscheid:

- **GPSR** — Die Verordnung (EU) 2023/988 über die allgemeine Produktsicherheit gilt seit Dezember 2024 und ergänzt die sektorspezifischen Anforderungen — insbesondere bei Verbraucherprodukten wie konsumentennaher Robotik.

- **PLD-Neufassung — Die Richtlinie (EU) 2024/2853 ist nach Artikel 22 der Richtlinie bis zum 9. Dezember 2026 in deutsches Recht umzusetzen. Das Bundesministerium der Justiz hat am 11. September 2025 einen Referentenentwurf vorgelegt. Das überarbeitete Regime erweitert den Produktbegriff nach Artikel 4(1) der Richtlinie ausdrücklich auf Software. Der bisherige Selbstbehalt von 500 € und die Haftungsobergrenze von 85 Mio. € entfallen. Eine zugunsten der Geschädigten gestaltete Beweismittel-Offenlegung wird eingeführt. Für Hersteller und Integrierte von Robotik ist das eine strukturelle Erhöhung des Produkthaftungsrisikos.**
- **BetrSichV und Verkehrssicherungspflichten —** Die Betriebssicherheitsverordnung (BetrSichV) regelt die Pflichten des Betreibers (Arbeitgebers) beim Einsatz von Arbeitsmitteln einschließlich Robotik. Verkehrssicherungspflichten gelten zudem in Bereichen, die Dritten zugänglich sind.
- **Funkanlagenrichtlinie (RED) —** Richtlinie 2014/53/EU gilt für jedes Robotik-System mit Funkfrequenzkomponenten (4G/5G, Wi-Fi, Bluetooth, GPS-Empfänger). In Deutschland ist die Bundesnetzagentur die Marktüberwachungsbehörde. Die RED-Konformität wird unabhängig von der Konformität nach der Maschinenverordnung bewertet. Im HU-RSC-Anwendungsbereich gilt RED insbesondere für verbrauchernahe Robotik, mobile Logistik-Robotik und humanoide Roboter mit drahtloser Konnektivität.

2.4 Cyber Resilience Act (Verordnung (EU) 2024/2847)

Der Cyber Resilience Act adressiert Produkte mit digitalen Elementen. Nach Artikel 71 gilt die Verordnung ab 11. Dezember 2027. Zwei frühere Termine ergeben sich aus Artikel 71: Kapitel IV (Notifizierung der Konformitätsbewertungsstellen) gilt ab 11. Juni 2026, Artikel 14 (Meldepflichten) gilt ab 11. September 2026. Beschaffungsentscheidungen in 2026 müssen die Artikel-14-Meldepflichten für danach in Verkehr gebrachte Produkte bereits berücksichtigen. Für HU-RSC relevante Punkte:

- **Risikobeurteilung —** Robotiksysteme mit digitalen Elementen müssen eine Cybersecurity-Risikobeurteilung durchlaufen.
- **Update-Pflicht —** Hersteller müssen über die erwartete Lebensdauer Sicherheitsupdates bereitstellen — Artikel 13 CRA setzt eine Support-Periode von mindestens fünf Jahren; ist die erwartete Nutzungsdauer kürzer, entspricht die Support-Periode dieser Nutzungsdauer. Artikel 13 ermächtigt zudem die Kommission, durch delegierte Rechtsakte produktkategorie-spezifische Mindest-Support-Perioden festzulegen, wenn Marktüberwachungsdaten unzureichende Support-Perioden nahelegen.
- **Meldepflichten —** Artikel 14 CRA verpflichtet Hersteller, aktiv ausgenutzte Schwachstellen über die zentrale Meldeplattform (Artikel 16) gleichzeitig an das benannte CSIRT (Coordinator) und an ENISA zu melden: eine Frühwarnmeldung innerhalb von 24 Stunden nach Kenntnisnahme und eine vollständige Schwachstellenmeldung innerhalb von 72 Stunden. Für die Beschaffung muss der Lieferant operativ nachweisen können, diese Fristen einzuhalten.

Die Verzahnung von CRA und Maschinenverordnung beim Begriff der wesentlichen Veränderung durch Software-Update ist ein zentrales offenes Auslegungsthema, das in HU-RSC über Achse 5 Säule 3 (Lifecycle-Update-Mechanik) abgebildet wird.

2.5 Einschlägige Sicherheitsnormen

Folgende Normen sind für die Tier-Schwellenwerte und die Erwartungsmatrizen leitend:

- **ISO 12100** — ISO 12100 — grundlegende Risikobeurteilung; Tabelle B.3 liefert die Schadensschwere-Skala für HU-RSC Achse 3.
- **EN ISO 13849-1:2023 — Sicherheit von Maschinen — Sicherheitsbezogene Teile von Steuerungen — Teil 1: Allgemeine Gestaltungsgrundsätze. Vierte Ausgabe veröffentlicht 2023, im EU-Amtsblatt im Mai 2024 gelistet. Die Vorgänger-Ausgabe EN ISO 13849-1:2015 bleibt während der OJEU-Übergangsfrist relevant; ihre Vermutungswirkung läuft am 15. Mai 2027 aus, während CEN als Date of Withdrawal den 31. Mai 2026 listet. Wesentliche Änderungen 2023 sind die Subsystem-Terminologie (anstelle von SRP/CS), ein eigenes Kapitel zur Safety Requirements Specification, ein EMV-Immunitäts-Anhang L und eine alternative PL-Bestimmungsmethode. Informiert HU-RSC Achse 5 Säule 1.**
- **ISO 10218** — ISO 10218-1 und ISO 10218-2 (Neufassungen Februar 2025) — Sicherheit für Industrieroboter und Roboteranwendungen; einschlägig für KMU-Industriekontext.
- **ISO/TS 15066** — ISO/TS 15066 — Sicherheit kollaborativer Roboter; Kollisionsschwellen sind leitend für HU-RSC Achse 2 (kinetisches Schadenspotenzial).
- **ISO 25785-1 — Robotik — Sicherheitsanforderungen für dynamisch stabile industrielle mobile Roboter. Derzeit Working Draft, entwickelt von ISO TC 299 WG 12 mit Industriebeteiligten von Agility Robotics, Boston Dynamics, A3 Association und Fraunhofer IPA. Die finale Veröffentlichung wird für 2027 oder 2028 erwartet. Nach Veröffentlichung wird dies die primäre Type-C-Referenz für humanoide Pilot-Deployments unter HU-RSC; die Mapping-Tabelle in Anhang 12 wird entsprechend aktualisiert.**
- **ISO/IEC TR 5469** — ISO/IEC TR 5469 — funktionale Sicherheit von KI-Systemen; einschlägig für HU-RSC Achse 5 Säule 2.
- **IEC 61508** — IEC 61508 — Safety Integrity Levels (SIL 1–4); einschlägig für sicherheitsrelevante elektrische und elektronische Systeme.
- **IEC TS 62998-1** — Sicherheit von Maschinen — Sicherheitsbezogene Sensorik zum Schutz von Personen; einschlägig für HU-RSC Achse 5 Säule 1 volumetrische Sicherheitsüberwachung (Kameras, LIDAR, Radar) und Bezugspunkt für sensorbasierte sichere Personenerkennung ab Tier 3 aufwärts.
- **ISO/IEC TS 22440** — Künstliche Intelligenz — Funktionale Sicherheit und KI-Systeme (Teile 1, 2, 3); Committee Draft seit Februar 2026, Kommentarfrist im April 2026 abgeschlossen; löst ISO/IEC TR 5469 als verbindliche Technische Spezifikation für KI-funktionale Sicherheit ab, Veröffentlichung erwartet für 2027 oder 2028. Zusammen mit ISO 25785-1 die wichtigsten kommenden Normen für HU-RSC Säule 2.

- **ISO 13482** — Sicherheitsanforderungen für Personal-Care-Roboter; einschlägig für die HU-RSC-Anwendungsdomänen Assistenz- und teilöffentliche Service-Robotik; deckt Humanoide nur für nichtindustrielle Anwendungsfälle ab.
- **ISO 3691-4** — Flurförderzeuge — Sicherheitsanforderungen für fahrerlose Flurförderzeuge; einschlägig für die HU-RSC-Anwendungsdomäne Mobile Logistik-Robotik (AGVs, AMRs). Humanoide Roboter sind nicht im Anwendungsbereich von ISO 3691-4.

3 Architektur des Modells

Methodischer Hinweis zu diesem Impulspapier (v0.2.11). Das Papier formuliert drei Modellbildungsentscheidungen, die in dieser Diskussionsfassung bewusst als vorläufig markiert sind: (1) die Auswahl der sechs Bewertungsachsen (Kapitel 4); (2) die Wahl einer HU-RSC-eigenen Tier-Skala 1–5 mit ISO-Mapping-Tabellen anstelle einer direkten Aggregation existierender ISO-Klassen (Kapitel 11); (3) die asymmetrische Mindestkopplung $HU-RSC \geq 4$ verlangt $HU-RAC \geq 3$ (Kapitel 9). Alle drei können in v0.3 aufgrund von Praktiker-Rückmeldungen revidiert werden. Adoptoren von HU-RSC sollten sie als Tendenzen des aktuellen Modells behandeln, nicht als endgültige Festlegungen.

3.1 Strukturparallele zu HU-RAC

HU-RSC trägt dieselbe Modellarchitektur wie HU-RAC. Die folgenden Architekturmerkmale sind für beide Modelle identisch und werden hier ohne erneute Begründung übernommen:

- **Achsen** — sechs Bewertungsachsen mit Tier-Skala 1–5
- **Aggregation** — Aggregationsregel „Prinzip der stärksten Belastung“ über die Achsen — die schwächste Achse bestimmt das Tier des Gesamtsystems
- **Matrizen** — Erwartungsmatrizen E-Min, E-Plus und R pro Achse und Tier
- **Sekundärdimensionen** — Sekundärdimensionen Business-Kritikalität (A/B/C) und Anbieter-Resilienz (R1/R2/R3)
- **Dynamik** — dynamische Reklassifikation bei wesentlichen Veränderungen i.S.d. Maschinenverordnung 2023/1230

3.2 HU-RSC-spezifische Erweiterungen

Drei Erweiterungen unterscheiden HU-RSC architektonisch von HU-RAC:

- **Dreisäulige Achse 5** — Eine der sechs Achsen — Achse 5 (Sicherheitsarchitektur) — ist dreisäulig aufgebaut: SIL/PL-zertifizierte klassische Sicherheit, KI-Sicherheitsarchitektur, Lifecycle-Update-Mechanik. Die Aggregation innerhalb dieser Achse folgt einer modifizierten Regel (siehe Kapitel 8).
- **Asymmetrische Mindestkopplung** — Zwischen HU-RSC und HU-RAC besteht eine asymmetrische Mindestkopplung: $HU-RSC \geq 4$ verlangt $HU-RAC \geq 3$. Begründung in Kapitel 9.
- **Eigenständige R-Spalten-Funktion** — Die R-Spalte der Erwartungsmatrizen erhält in HU-RSC eine eigenständige Funktionsklarstellung als Warnfunktion im Sinne der Sorgfaltspflicht — sie ist kein Haftungsausschluss und keine Modell-Lücke. Erläuterung in Kapitel 6.

3.3 Tier-Skala — Begriffsklärung

Die HU-RSC-Tier-Skala 1–5 misst das nach Schutzmaßnahmen verbleibende Restrisiko, nicht das ursprüngliche inhärente Risiko der Technologie. Ein humanoider Roboter mit aufwendiger Sicherheitsarchitektur kann ein niedrigeres Tier erreichen als ein Mähroboter ohne nennenswerte Sicherheitsarchitektur, obwohl der humanoide Roboter inhärent gefährlicher ist.

Diese Lese-Logik entspricht der ISO-12100-Risikobeurteilung: Sicherheitsmaßnahmen reduzieren das Risiko, und das nach Maßnahmen verbleibende Restrisiko ist das, was beurteilt und kommuniziert werden muss.

4 Die sechs Achsen — Bewertungsinhalt im Detail

Dieses Kapitel beschreibt die sechs Bewertungsachsen im Detail. Jede Achse trägt eine Bewertungsdimension der physischen Sicherheit und ist gegen die anderen fünf Achsen orthogonal — im Sinne der Modell-Logik, nicht der mathematischen Strenge. Doppelungen mit HU-RAC sind ausgeschlossen, insbesondere wird Cybersicherheit nicht in HU-RSC geführt, sondern ausschließlich in HU-RAC Matrix 5.3.

Die Achsen werden in der natürlichen Lese-Reihenfolge eines Beschaffers behandelt: zuerst der Einsatzkontext (Achse 1), dann das System selbst (Achsen 2 bis 5), dann die exponierten Personen (Achse 6).

4.1 Achse 1 — Einsatzumgebung

Achse 1 unterscheidet, in welcher Umgebung das Robotiksystem eingesetzt wird, und wie diese Umgebung sicherheitsbezogene Faktoren beeinflusst. Drei Klassen sind leitend:

- **Kontrollierte Umgebung** — vollständig kontrolliert (Sicherheitskäfig, abgesperrte Industriezelle, sichere Lichtverhältnisse, definierte Wegeföhrung, kein Personenzugang während Betrieb).
- **Halbkontrollierte Umgebung** — Personenzugang ohne durchgängige Absperrung, aber mit organisatorischen Schutzmaßnahmen (Privathaushalt, Krankenhausflur außerhalb Patientenzimmer, Hotelflur, Werkstatt mit Mitarbeitenden).
- **Öffentlich-ungeschützte Umgebung** — Personenzugang ungeschützt, Dritte ohne Vorinformation, Kinder, Tiere, Verkehrsteilnehmende (öffentlicher Außenbereich, Park, Gehweg, Einkaufszentrum).

Sekundärfaktoren der Einsatzumgebung, die die Klasse modifizieren können: Lichtverhältnisse (Tag/Nacht/wechselnd), Bodenbeschaffenheit (eben/uneben/rutschig), Witterung (innen/außen), Lärmpegel (akustische Warnsignale wirksam?), Sichtbarkeitsbedingungen (Spiegel, blinde Ecken).

4.2 Achse 2 — Bauart, Bewegungsraum und kinetisches Schadenspotenzial

Achse 2 bewertet das physische Schadenspotenzial des Systems im Falle eines Personenkontakts oder einer Sachkollision. Vier Bewertungsfaktoren sind leitend:

- **Kinetische Energie** — Aufprallenergie nach $E_{kin} = \frac{1}{2} m v^2$. Orientierungswerte aus ISO/TS 15066 (Kollisionsschwellen für Mensch-Roboter-Kollaboration).
- **Bewegungsraum** — Umfang des freien Bewegungsraums, Reichweite des Greifarms, maximale Hubhöhe, Schwenkradien.
- **Werkzeuge und Aufprallflächen** — rotierende Klingen (Mähroboter), Bürsten und Saugöffnungen (Saugroboter), Werkzeuge an Greifarmen, Schweißelektroden, scharfe Kanten am Chassis.
- **Stabilität bei Notabschaltung** — Stand- und Fallverhalten — kann das System eigenständig stehen bleiben? Kann es geföhrt fallen (Safe Guided Falling)? Kann ein Stoppen die Lage destabilisieren (Inverses-Pendel-Problem bei Humanoiden)?

Bei humanoiden Robotern gilt die Sonderlogik des Inversen-Pendel-Problems: Stoppen ist nicht gleich sicher (anders als bei klassischen Industrierobotern). Die Tier-Bewertung berücksichtigt dies über höhere Anforderungen an Achse 5 Säule 1 (Safe Guided Falling, Safe Stability Control).

Transparenz-Hinweis ISO/TS 15066. Die in ISO/TS 15066:2016 ursprünglich angegebenen biomechanischen Grenzwerte beruhen — wie die zugrundeliegende Literaturrecherche im Anhang der Norm selbst offenlegt — auf nicht experimentell verifizierten Daten. Behrens et al. (Frontiers in Robotics and AI, 2022) lieferten erstmals mit einer Studie an 112 Probanden über 28 Körperregionen experimentell abgesicherte Grenzwerte mit explizitem Geschlechter-Effekt. Weitere Arbeiten (Svarný et al. (2020); Kirschner et al. (2021); Fischer et al. 2023) zeigten zudem, dass die ISO/TS-15066-Formeln zur Kraftabschätzung Impact-Forces sowohl unter- als auch überschätzen können. Diese Befunde stützen die methodische Grundhaltung des HU-RSC: ISO/TS 15066 dient als Beleggrundlage, nicht als Konformitätsnachweis.

4.3 Achse 3 — Schadenstypen und Schadensschwere

Achse 3 bewertet, welche Schadenstypen plausibel sind und welche Schadensschwere zu erwarten ist, wenn ein Sicherheitsereignis eintritt. Die Bewertung folgt der Systematik der ISO 12100 Tabelle B.3:

- **Mechanisch** — Quetschungen, Stoß- und Aufprallverletzungen, Schnittverletzungen durch Werkzeuge oder scharfe Kanten, Sturzverletzungen Dritter ausgelöst durch das System.
- **Thermisch** — Verbrennungen durch heiße Oberflächen, Erfrierungen durch Kühlmittel, Brandgefahr.
- **Chemisch** — austretende Reinigungsmittel, Hydraulikflüssigkeit, Akku-Elektrolyt; selten relevant in den hier behandelten Use Cases.
- **Elektrisch** — Stromschlag bei Defekt, Funkenbildung in explosionsfähigen Atmosphären; bei batteriebetriebenen Systemen meist gering.
- **Biologisch** — Kontamination durch nicht steril gereinigte Greifarme im Krankenhaus oder Pflege; Use-Case-spezifisch.
- **Psychisch** — Erschrecken Dritter (Sturzfolge), Vertrauensverlust gegenüber Robotik insgesamt, in seltenen Fällen Trauma; bei vulnerablen Personen relevant. Bei längerer Ko-Präsenz mit humanoiden Robotern und AGVs in Arbeitskontexten ist zusätzlich die strukturelle psychische Belastung gemäß DIN EN ISO 10075-1 (Ergonomische Grundlagen bezüglich der psychischen Arbeitsbelastung) zu bewerten. Dies ist betreiberseitig, nicht lieferantenseitig, wechselwirkt aber mit dem HU-RSC-Tier in der R-Spalte ab Tier 3 aufwärts.

Empirischer Bezug zur Mensch-Roboter-Interaktion. Morandini et al. (2025) systematisieren in einem präregistrierten Scoping-Review 23 Studien zu Cobots, die ihr Verhalten an psychologische Zustände (Workload, Aufmerksamkeit, situatives Bewusstsein) der Bediener anpassen. Dies markiert eine Brücke zwischen der KI-Verhaltens-Achse und der HRI-/Mental-Workload-Achse: Dynamische Verhaltensadaption auf Basis physiologischer Marker

(Herzratenvariabilität, elektrodermale Aktivität, Blickfixation) ist methodisch nicht nur denkbar, sondern empirisch fundiert.

Sekundärdimension der Achse 3 ist die Reversibilität: vollständig reversibel, langfristig reversibel, irreversibel. Die ISO-12100-Skala unterscheidet vier Schadensschwere-Klassen (geringfügig, mäßig, schwer, sehr schwer/letal), die in HU-RSC den Tiers 1–5 zugeordnet werden.

4.4 Achse 4 — Autonomiegrad

Achse 4 bewertet, in welchem Umfang das System eigenständig sicherheitsrelevante Entscheidungen trifft. Die Klassifikation folgt einer fünfstufigen Autonomie-Skala, abgeleitet aus ISO 25785-1 (Working Draft) und gängigen Robotik-Autonomie-Taxonomien:

- **A0** — ferngesteuert oder vorprogrammiert, kein autonomes Handeln; Bediener trägt jede sicherheitsrelevante Entscheidung.
- **A1** — assistiert; das System unterstützt einen menschlichen Bediener mit Sensor- und Wegplanungs-Daten, der Bediener entscheidet.
- **A2** — teilautonom; das System trifft Routineentscheidungen selbstständig (Hindernisausweichen, Routenplanung), Sicherheitsentscheidungen werden eskaliert.
- **A3** — hochautonom mit Aufsicht; das System trifft auch sicherheitsrelevante Entscheidungen autonom, ein Mensch kann jederzeit eingreifen und behält Letztkontrolle.
- **A4** — vollautonom ohne menschliche Letztkontrolle im Operationsmoment; das System entscheidet eigenständig auch in Sicherheitssituationen.

Achse 4 misst den Autonomiegrad als Anforderung an die Sicherheitsarchitektur, nicht ihre Erfüllung. Wie gut die Sicherheitsarchitektur den geforderten Autonomiegrad bewältigt, wird in Achse 5 bewertet — beide Achsen zusammen ergeben das Bild.

Sekundärfaktor: Häufigkeit und Dauer der autonomen Entscheidung mit Sicherheitsbezug. Ein A3-System, das pro Tag drei sicherheitsrelevante autonome Entscheidungen trifft, ist anders zu bewerten als eines mit dreitausend solchen Entscheidungen.

4.5 Achse 5 — Sicherheitsarchitektur (dreisäulig)

Achse 5 ist die einzige dreisäulige Achse des Modells. Sie bewertet, wie gut die Sicherheitsarchitektur des Systems die Anforderungen aus Achse 4 (Autonomiegrad) und den ISO-Normen erfüllt. Drei Säulen werden unterschieden:

4.5.1 Säule 1 — Klassische Sicherheitsarchitektur

Säule 1 bewertet die klassische funktionale Sicherheit nach ISO 13849 und IEC 61508. Bewertungsfaktoren:

- **Zertifizierte Safety Functions** — Vorhandensein und Klassifikation zertifizierter Sicherheitsfunktionen (Notabschaltung, Safe Torque Off, Safe Stop, Safe Limited Speed, Safe Brake Control). Performance Level nach ISO 13849-1.

- **Redundanz und Diversität** — Architektur der Sicherheitsfunktionen (Kategorie B, 1, 2, 3, 4 nach ISO 13849-1); Hardware- und Softwarefehler-Toleranz.
- **Safe-State-Konzept** — Existiert ein universeller sicherer Zustand (Stoppen)? Wenn nicht (Humanoide, AGV in Kurvenfahrt): existieren Active Damping (z. B. durch Active Short Circuit auf Gelenkebene), Safe Guided Falling, Safe Stability Control?

Empirischer Befund zu dynamischen Sicherheits-Schwellen. Rustler et al. (IEEE Humanoids 2024) zeigen mit einer empirischen Studie an einem UR10e mit elektronischer Sensorhaut (AIRSKIN), dass dynamisch — auf Basis von Link-Geschwindigkeit und effektiver Masse — gesetzte Schwellenwerte gegenüber statisch-uniformen Einstellungen einen messbaren Produktivitätsgewinn ohne Sicherheits-Einbuße ermöglichen. Für HU-RSC ist das methodisch relevant: Statische PFL-Konformität und produktive Mensch-Roboter-Kollaboration schließen sich nicht aus.

4.5.2 Säule 2 — KI-Sicherheitsarchitektur

Säule 2 bewertet die spezifische Sicherheitsarchitektur der KI-Komponenten. Bewertungsfaktoren:

- **KI-VO-Konformität** — Hochrisiko-Klassifikation nach KI-Verordnung 2024/1689 — wenn die Komponente Sicherheitsbauteil im Sinne der Maschinenverordnung ist, gelten die KI-VO-Hochrisiko-Pflichten (Risikomanagement, Datenqualität, Transparenz, Aufsicht).
- **Erklärbarkeit** — Erklärbarkeit der Entscheidungslogik (Determinismus, Reproduzierbarkeit, Konfidenzwerte, post-hoc-Erklärungen).
- **Behavioral Safety** — ISO/IEC TR 5469-konforme Risikobeurteilung der KI-Komponenten; Behavioral Safety, Safe Situational Motion, Safe Behavior Supervision (proprietäre Industrie-Featuredefinitionen, noch nicht durchgängig genormt).
- **MVO Anhang III** — Konformität mit Maschinenverordnung Anhang III — Sicherheitsbauteile mit selbstentwickelndem Verhalten.

Begriffsklärung: Behavioral Safety bezeichnet Sicherheitsmaßnahmen, die nicht klassisch-mechanisch (Notabschaltung, Schutzzaun) und nicht klassisch-elektronisch (zertifizierte Safety Functions nach ISO 13849) wirken, sondern durch KI-gestützte Verhaltensanpassung des Roboters — etwa Geschwindigkeits-Reduktion bei Personennähe, vorausschauende Bewegungsanpassung, Behavior-Supervision-Layer, der KI-Entscheidungen gegen Verhaltensmuster prüft. Die Begriffe Safe Situational Motion und Safe Behavior Supervision sind proprietäre Featuredefinitionen einzelner Hersteller (z. B. Synapticon, Neura) und noch nicht durchgängig genormt; ISO/IEC TR 5469 bietet einen ersten Rahmen, konkretisierende Folgenormen sind in Erarbeitung.

Empirischer Bezug zur KI-Verhaltenssicherheit. SafeVLA (Zhang et al., 2025) demonstriert über Constrained Reinforcement Learning eine empirisch belegbare Methode zur Sicherheits-Alignment von Vision-Language-Action-Modellen: 83,58 % Reduktion kumulativer Sicherheits-Verstöße bei gleichzeitig 3,85 % Zuwachs der Aufgaben-Erfolgsrate gegenüber dem zuvor besten Verfahren. Für die HU-RSC-Bewertung ist relevant, dass damit ein konkreter Aligner-Mechanismus existiert — die Frage nach nachweisbar abgesicherter VLA-Steuerung ist also keine ausschließlich theoretische mehr.

4.5.3 Säule 3 — Lifecycle-Update-Mechanik

Säule 3 bewertet die technische Update-Fähigkeit als System-Eigenschaft — nicht die empirische Update-Lieferfähigkeit des Anbieters (das ist die Sekundärdimension R1/R2/R3). Bewertungsfaktoren:

- **Patchbarkeit** — ist die Software-Architektur des Systems update-fähig? Modulare Komponenten? Klare API-Grenzen? Dokumentierte Update-Prozesse?
- **Sichere OTA-Mechanik** — kryptografische Signatur, Rollback-Mechanismus, Atomare Updates, sichere Boot-Kette, geschütztes Update-Backend.
- **Wesentliche-Veränderungs-Detektion** — ermittelt das System bei einem Update selbstständig, ob eine „wesentliche Veränderung“ i.S.d. Maschinenverordnung 2023/1230 vorliegt? Logging der Update-Auswirkungen auf Sicherheitsfunktionen.
- **CRA-Konformität** — Konformität mit Cyber Resilience Act 2024/2847 (Sicherheitsupdate-Pflichten, Meldepflichten, Risikobeurteilung).

Wichtige Abgrenzung:

Säule 3 misst die technische Update-Fähigkeit als System-Eigenschaft („ist das System patchbar?“). Die empirische Wahrscheinlichkeit, dass der Anbieter Updates liefert („wird der Anbieter Patches liefern?“), ist eine Anbieter-Eigenschaft und wird in der Sekundärdimension R1/R2/R3 (siehe Kapitel 7) bewertet. Ein patchfähiges System nützt nichts ohne lieferfähigen Anbieter — und umgekehrt. Beide Dimensionen sind notwendig.

4.6 Achse 6 — Exponierte Personen und Expositionsfrequenz

Achse 6 bewertet, wer dem System ausgesetzt ist und in welcher Häufigkeit. Die Bewertung folgt der ISO-12100-Logik (Number of Persons Exposed, Frequency of Exposure):

- **Erwachsene Mitarbeitende** — trainierte und sensibilisierte Personen, ohne vulnerable Gruppen.
- **Erwachsene Bewohner** — Privatpersonen, untrainiert, mit Hausrechten — typisch im Konsumentenkontext.
- **Gemischte Adressaten** — trainiertes Klinikpersonal plus untrainierte Patienten und Besucher — typisch im Healthcare-Kontext.
- **Vulnerable Gruppen** — Kinder, ältere Menschen mit eingeschränkter Mobilität oder Aufmerksamkeit, Patienten mit kognitiven Einschränkungen, körperlich beeinträchtigte Personen.
- **Öffentliche Allgemeinheit** — Dritte ohne Vorinformation, einschließlich Kinder und Senioren — typisch im öffentlichen Außenraum.

Sekundärdimension: Expositionsfrequenz und -dauer. Eine kurze einmalige Exposition (Roboter passiert Flur, Mensch geht vorbei) wird anders gewichtet als eine dauerhafte (Pflegeroboter im Zimmer eines Patienten über Stunden).

Procurement-Hinweis zur anthropometrischen Heterogenität. Fischer et al. (2024) belegen über eine Studie mit 31 Probanden, dass die anthropometrische Variation des Bedieners signifikant beeinflusst, welche Körperregion bei gleicher Roboter-Konfiguration getroffen wird

— Brust, Bauch oder Becken können je nach Statur dieselbe Trajektorie betreffen. Für Procurement bedeutet das: Eine biomechanische Verifikation gegen ein einziges anthropometrisches Standardmodell ist nicht ausreichend, wenn die Belegschaft anthropometrisch heterogen ist. Diese Erkenntnis fließt in die HU-RSC-Tier-Bewertung über die Achse Betroffenenkreis ein.

5 Tier-Skala 1–5 mit Schwellenwerten

Die HU-RSC-Tier-Skala 1–5 misst das nach Schutzmaßnahmen verbleibende Restrisiko. Die folgenden Tier-Beschreibungen sind semi-quantitativ formuliert: sie nennen Orientierungswerte aus den einschlägigen Normen, ohne den Anspruch auf Engineering-Präzision zu erheben. Die rechtsverbindliche Bewertung verbleibt bei der Risikobeurteilung nach ISO 12100.

Methodische Klarstellung zu den Achsen-Werten in den folgenden Tier-Beschreibungen: Die pro Tier genannten Achsen-Werte zeigen typische Konstellationen, in denen ein Robotersystem auf das jeweilige Tier fällt. Sie sind keine notwendigen Bedingungen pro Achse — die Aggregationsregel „Prinzip der stärksten Belastung“ bedeutet, dass bereits eine einzelne Achse das Gesamt-Tier setzen kann, auch wenn die anderen Achsen niedriger liegen. Ein humanoider Roboter mit Tier-5-Stand- und Sturzpotenzial in Achse 2 erreicht Tier 5 als Gesamt-Tier, auch wenn Achse 4 (Autonomiegrad) nur A2 erreicht.

Hinweis zur Achse-5-Aggregation:

Die Aggregation innerhalb der dreisäuligen Achse 5 folgt einer modifizierten Mindest-Floor-Logik: Säule 3 (Lifecycle-Update-Mechanik) zieht erst ab Tier 3 in die Achsen-Aggregation ein, weil die CRA-Relevanz und die Update-Pflicht-Tragweite bei Tier-1- und Tier-2-Systemen marginal sind. Säulen 1 und 2 werden über alle Tiers nach dem Prinzip der stärksten Belastung aggregiert. Detail-Begründung in Kapitel 8.

5.1 Tier 1 — minimales Restrisiko

Charakter: stationäre oder sehr leichte mobile Systeme in vollständig kontrollierter Umgebung; kinetisch quasi unbedenklich; keine sicherheitskritischen KI-Funktionen.

- **Achse 2** — $E_{kin} < 1 \text{ J}$ (Orientierung an ISO/TS 15066 Kollisionsschwellen für Soft-Tissue) oder vollständig stationär.
- **Achse 3** — Schadensschwere geringfügig nach ISO 12100 Tab. B.3, vollständig reversibel.
- **Achse 4** — Autonomiegrad A0–A1 (ferngesteuert oder assistiert).
- **Achse 5** — Sicherheitsarchitektur Säulen 1–2: ISO 13849 PL a oder Basis-Schutzmaßnahmen ausreichend.

Beispiele: Tisch-Roboterarm zu Edutainment-Zwecken in trainierter Umgebung; einfache Saugroboter ohne rotierende Bürstenwalzen oder scharfe Werkzeuge; stationäre Inspektionsarme mit begrenzter Nutzlast in einer kontrollierten Industrie-Zelle. Hinweis: Säule 3 (Lifecycle-Update-Mechanik) ist auf Tier 1 unter der Mindest-Floor-Regel (Kapitel 8.2) nicht aggregationsrelevant. Cyber-Resilience-Act-Konformität bleibt jedoch unabhängig vom HU-RSC-Tier verbindlich — siehe Säule-3-R-Spalte in der Achse-5-Erwartungsmatrix.

5.2 Tier 2 — begrenztes Restrisiko

Charakter: leichte mobile Systeme in halbkontrollierter Umgebung; reversible Schäden plausibel, irreversible Schäden unwahrscheinlich.

- **Achse 2** — E_{kin} 1–10 J; geringe Geschwindigkeit (typisch < 0,5 m/s); keine schneidenden oder rotierenden Werkzeuge.
- **Achse 3** — Schadensschwere geringfügig bis mäßig, langfristig reversibel.
- **Achse 4** — Autonomiegrad A1–A2.
- **Achse 5** — Sicherheitsarchitektur Säule 1: PL b, einfache Notabschaltung; Säule 2: einfache KI-Plausibilitätsprüfung; Säule 3: noch nicht aggregationswirksam.

Beispiele: Saugroboter im Privathaushalt; einfache AGV in Industrieumgebung mit Sicherheitsabständen; Inspektionsroboter in Gewerberäumen. Hinweis: Säule 3 (Lifecycle-Update-Mechanik) ist auf Tier 2 unter der Mindest-Floor-Regel (Kapitel 8.2) nicht aggregationsrelevant. Die CRA-Konformität bleibt unabhängig vom HU-RSC-Tier verbindlich.

5.3 Tier 3 — erhöhtes Restrisiko

Charakter: mobile Systeme mit signifikanter kinetischer Energie oder schneidenden/rotierenden Werkzeugen; Personenkontakt in halbkontrollierter Umgebung möglich.

- **Achse 2** — E_{kin} 10–80 J ODER Werkzeugbewegung mit Verletzungsmöglichkeit (rotierende Klingen, Bürsten).
- **Achse 3** — Schadensschwere mäßig bis schwer; teilweise irreversibel (Schnittverletzung, Quetschung mit Folgen).
- **Achse 4** — Autonomiegrad A2–A3.
- **Achse 5** — Sicherheitsarchitektur typische Erwartung Säule 1: PL c oder höher; Säule 2: ISO/IEC TR 5469-konforme KI-Risikobeurteilung; Säule 3 ab hier aggregationswirksam: Patchbarkeit, sichere OTA-Mechanik.

Beispiele: Mähroboter mit rotierenden Klingen im Privatgarten; Reinigungsroboter im Hotelflur außerhalb der Belegungszeiten; AGV in gemischter Mensch-Roboter-Umgebung.

5.4 Tier 4 — hohes Restrisiko

Charakter: Systeme mit signifikantem Verletzungspotenzial in halbkontrollierter oder öffentlicher Umgebung; vulnerable Personengruppen plausibel exponiert; KI-getriebene Entscheidungen mit Sicherheitsrelevanz.

- **Achse 2** — typischerweise E_{kin} 80–200 J als Orientierung; alternativ humanoide Bauart mit Sturzpotenzial; Reichweite und Hubhöhe relevant.
- **Achse 3** — Schadensschwere typischerweise schwer; irreversible Schäden plausibel.
- **Achse 4** — typischerweise Autonomiegrad A3 mit hoher Häufigkeit sicherheitsrelevanter autonomer Entscheidungen.
- **Achse 5** — Sicherheitsarchitektur typische Erwartung Säule 1: PL d, redundante Architektur; Säule 2: dokumentierte und risikobewertete KI-Behavioral-Safety-Funktionen (Drittprüfung wo verfügbar), KI-VO-Hochrisiko-Pflichten erfüllt; Säule 3: CRA-konforme Update-Mechanik mit Wesentliche-Veränderungs-Detektion.
- **Achse 6** — vulnerable Gruppen typischerweise plausibel oder regelmäßig exponiert.

Beispiele: humanoide Pilotanwendungen im KMU-Industriebereich; Reinigungsroboter im Krankenhaus außerhalb sensibler Zonen; Outdoor-Mähroboter in öffentlich zugänglichen Park-Anlagen.

5.5 Tier 5 — kritisches Restrisiko

Charakter: Tier 5 ist gegenüber Tier 4 kein quantitativer, sondern ein qualitativer Sprung. Drei Konstellationen prägen Tier 5 — einzelne genügen, das Tier zu erreichen: Mehrfachgefährdung mit kumulativen Schadenstypen, Letalitätspotenzial in der Schadensschwere, oder direkte und dauerhafte Exposition vulnerabler Gruppen ohne menschliche Letztkontrolle. Die Tier 4 / Tier 5-Grenze für humanoide Systeme ist nicht trennscharf: Tier 4 erfasst humanoide Systeme mit Sturzpotenzial in strukturierten Umgebungen (definierte Arbeitszone, Geofencing, regelmäßige Bodenprüfung, beaufsichtigte Ko-Präsenz mit geschulten Erwachsenen). Tier 5 erfasst Fälle, in denen die Umgebung unstrukturiert ist (wechselnde Untergründe, freier Drittzugang, kein Geofencing) oder mehrere Tier-5-Bedingungen kumulieren (Mehrfachgefährdung, kontinuierlich exponierte vulnerable Gruppen). Der Einkäufer dokumentiert die Einordnungsbegründung in der Beschaffungsakte.

- **Achse 2** — typischerweise sehr hohe E_{kin} (oberhalb der Tier-4-Orientierungsschwelle) oder Mehrfachgefährdung (kinetisch + thermisch oder kinetisch + chemisch); humanoide Bauart in unstrukturierter Umgebung. Die Joule-Schwelle ist Heuristik — die Engineering-Bewertung erfolgt über ISO/TS 15066:2016 Anhang A (Tabellen 2 und 3), nun auch in ISO 10218-2:2025 reproduziert (körperregionen-spezifische Kraft- und Druck-Schwellen), nicht über E_{kin} allein.
- **Achse 3** — Schadensschwere typischerweise sehr schwer bis letal; ausschließlich irreversibel.
- **Achse 4** — typischerweise Autonomiegrad A4 (vollautonom ohne menschliche Letztkontrolle); alternativ A3 mit sehr hoher Frequenz sicherheitsrelevanter Entscheidungen, bei der menschliche Aufsicht praktisch nicht durchhaltbar ist.
- **Achse 5** — Sicherheitsarchitektur typische Erwartung Säule 1: PL e, Cat 4 redundante Architektur; Säule 2: vollumfänglich KI-VO-Hochrisiko-konform, MVO Anhang III erfüllt, Behavioral Safety dokumentiert, risikobewertet und Drittprüfung wo verfügbar; Säule 3: CRA-Konformität mit Notfall-Update-Pfaden.
- **Achse 6** — vulnerable Gruppen typischerweise direkt exponiert (Pflege, Kinderbetreuung).

Beispiele: Pflege-Assistenzroboter mit körperlichem Personenkontakt in Pflegeeinrichtungen; vollautonome Healthcare-Robotik mit eigenständigen Sicherheitsentscheidungen am Patienten.

Methodischer Ausblick: Behrens-S0-Framework. Behrens et al. (IEEE ISR 2021) schlagen mit der neuen Schwellenstufe „S0“ eine Verfeinerung des PFL-Frameworks vor, bei der drei Substufen tolerierter Belastung mit unterschiedlichen Risikoniveaus unterschieden werden — ein Mapping-Ansatz, der methodisch nahe an der HU-RSC-Tier-Logik liegt und bei einer späteren Version als Referenz für die Tier-Verfeinerung herangezogen werden kann.

6 Erwartungsmatrizen (E-Min, E-Plus, R)

Dieses Kapitel ist das Herzstück des Modells. Pro Achse und pro Tier werden drei Erwartungssätze geführt — strukturparallel zu HU-RAC:

- **E-Min** — erwartete Mindestmaßnahmen, die ein Produkt bzw. ein Anbieter zwingend zeigen muss, damit das Tier vergeben wird.
- **E-Plus** — zusätzliche Maßnahmen, die das Tier robust absichern (gehobener Stand der Technik, Vorbereitung auf wesentliche Veränderungen).
- **R** — Restrisiken, die außerhalb des jeweiligen Tiers liegen und durch den Beschaffer bzw. Betreiber zusätzlich adressiert werden müssen.

Funktion und Verwendung der R-Spalte

Die R-Spalte ist kein Haftungsausschluss und keine Modell-Lücke. Sie ist eine Warnfunktion im Sinne der Sorgfaltspflicht: Sie macht dem Beschaffer transparent, welche Restrisiken das jeweilige Tier strukturell nicht abdeckt und welche zusätzlichen organisatorischen, technischen oder vertraglichen Maßnahmen nötig sind.

Diese Klarstellung ist haftungsrechtlich relevant — ein Beschaffer, der die R-Spalte als „akzeptable Risiken“ missversteht statt als „erfordert zusätzliche Maßnahmen“, trifft falsche Beschaffungsentscheidungen.

Querverweise statt Wiederholung

Mehrere Sicherheitsmaßnahmen tauchen logisch in mehreren Achsen auf — etwa die Notabschaltung in Achse 5 Säule 1 und in Achse 3 (mechanische Schadensvermeidung). Um Redundanz und Inkonsistenz zu vermeiden, führt das Modell jede Maßnahme primär in einer Achse und verweist in den anderen Achsen kurz darauf. Wo dies erfolgt, ist es im Text mit „siehe Achse X“ kenntlich gemacht.

6.1 Erwartungsmatrix Achse 1 — Einsatzumgebung

Tier	E-Min — Mindestmaßnahmen	E-Plus — Robustheits-Plus	R — Restrisiken & Maßnahmen
Tier 1	<ul style="list-style-type: none"> • vollständig kontrollierte Umgebung • sichere Lichtverhältnisse, definierte Wegeführung • kein Personenzugang während Betrieb 	<ul style="list-style-type: none"> • Sensorgestützte Umgebungsüberwachung • protokollierte Zugangsregelung • redundante Beleuchtung 	<ul style="list-style-type: none"> • bei Wechsel der Umgebungs-kategorie: Reklassifikation erforderlich • Drittpersonen-Zugang außerhalb Vorgaben begründet Tier-Verletzung
Tier 2	<ul style="list-style-type: none"> • halbkontrollierte Umgebung mit organisatorischen Schutzmaßnahmen • Beschilderung und Einweisung der Mitarbeitenden • definierte Sperrzeiten oder Personenfreihaltung 	<ul style="list-style-type: none"> • sensorische Personenerkennung mit niedriger Empfindlichkeit • klare Trennung Robotereinsatz / Personenzugang 	<ul style="list-style-type: none"> • unangekündigter Drittpersonen-Zugang erfordert organisatorische Nachschärfung • Tierschutz nicht abgedeckt (Haustier-Begegnungen)

Tier	E-Min — Mindestmaßnahmen	E-Plus — Robustheits-Plus	R — Restrisiken & Maßnahmen
Tier 3	<ul style="list-style-type: none"> • halbkontrollierte Umgebung; klare Verhaltensregeln für Mitarbeitende • akustisches/visuelles Warnsignal bei Annäherung • ausreichende Beleuchtung in allen Betriebszeiten 	<ul style="list-style-type: none"> • dokumentierte Risikobeurteilung der Einsatzumgebung • Absperrungen bei sensiblen Vorgängen • Lichtverhältnisse-Sensorik 	<ul style="list-style-type: none"> • Kinder- oder Tierbegegnungen in halbkontrollierter Umgebung sind Restrisiko, das organisatorisch (Sperrzeiten, Aufsicht) zu adressieren ist • wechselnde Bodenverhältnisse können stabilitätskritisch werden
Tier 4	<ul style="list-style-type: none"> • Risikobeurteilung der Einsatzumgebung dokumentiert • Geo-Fencing / definierte Operationszone • klare Eskalationspfade bei Umgebungsänderungen 	<ul style="list-style-type: none"> • KI-gestützte Umgebungsanalyse mit Konfidenzwerten • vorab kartierte Umgebung mit Live-Update • Witterungs-/Lichtsensorik mit adaptiver Verhaltensanpassung 	<ul style="list-style-type: none"> • spontane Umgebungsänderungen durch Dritte (Hindernisse, andere Roboter) erfordern Eingriffsbereitschaft • öffentliche Bereiche bleiben in der Regel außerhalb des erwarteten Operationsraums
Tier 5	<ul style="list-style-type: none"> • umfassende Risikobeurteilung für maximal anspruchsvolle Umgebungsbedingungen • redundante Umgebungserkennung mit unabhängigen Sensorpfaden • Notfall-Übergabe-Protokoll an menschliche Aufsicht bei unvorhergesehenen Bedingungen 	<ul style="list-style-type: none"> • mehrkanalige sensorische Umgebungsmodellierung • Geo-Fencing mit Hard-Stop-Zonen • Wetter-, Licht- und Akustik-Adaption mit dokumentierter Validierung 	<ul style="list-style-type: none"> • nicht antrainierte Umgebungsbedingungen sind Restrisiko, das durch betriebliche Aufsicht und Notfallpläne adressiert werden muss • Outdoor-Wetterereignisse (Schnee, Eis, Sturm) bleiben strukturelles Restrisiko

6.2 Erwartungsmatrix Achse 2 — Bauart und kinetisches Schadenspotenzial

Tier	E-Min — Mindestmaßnahmen	E-Plus — Robustheits-Plus	R — Restrisiken & Maßnahmen
Tier 1	<ul style="list-style-type: none"> • $E_{kin} < 1 \text{ J}$ oder vollständig stationär • keine schneidenden oder rotierenden Werkzeuge • kein Sturzpotezial 	<ul style="list-style-type: none"> • mechanische Energiebegrenzung redundant ausgelegt • weiche Materialien an Kontaktflächen 	<ul style="list-style-type: none"> • bei Hardware-Modifikation (Anbauteile, Werkzeugwechsel): Reklassifikation prüfen
Tier 2	<ul style="list-style-type: none"> • $E_{kin} 1\text{--}10 \text{ J}$ • Geschwindigkeit typisch $< 0,5 \text{ m/s}$ • abgerundete Kanten, weiche Stoßfänger 	<ul style="list-style-type: none"> • mechanische Geschwindigkeitsbegrenzung redundant • deformierbare Außenhülle • definierte Bewegungsraum-Grenzen 	<ul style="list-style-type: none"> • Sturzfolgen für Dritte (Stolperunfälle) bleiben Restrisiko • Beschädigung von Sachwerten an Kontaktflächen außerhalb HU-RSC-Skopus (siehe

Tier	E-Min — Mindestmaßnahmen	E-Plus — Robustheits-Plus	R — Restrisiken & Maßnahmen
			Anforderungskatalog Teil 5)
Tier 3	<ul style="list-style-type: none"> • E_{kin} 10–80 J ODER schneidende/rotierende Werkzeuge • ISO/TS 15066-konforme Kollisionsvermeidung • Notabschaltung der Werkzeuge bei Personenkontakt 	<ul style="list-style-type: none"> • sensorische Werkzeugerkennung mit Stop-on-Touch • doppelte mechanische Sicherung (z. B. Klängen-Hochheben + Stop) • Geschwindigkeitsadaption an Personenpräsenz 	<ul style="list-style-type: none"> • bei Kindern oder bewegungseingeschränkten Personen ist die Mindesterkennungszeit kritisch — siehe Achse 6 • Beschädigung von Sachwerten bleibt Restrisiko (siehe Anforderungskatalog Teil 5)
Tier 4	<ul style="list-style-type: none"> • E_{kin} 80–200 J als Orientierung; alternativ humanoide Bauart • umfassende sensorische Umfelderkennung • Safe Limited Speed / Safe Limited Position als Standardfunktion 	<ul style="list-style-type: none"> • Multi-Modal-Sensorik (Vision + LiDAR + taktil) • Active Damping bei drohendem Sturz (z. B. Synapticon ASC oder Äquivalent) • modellbasierte Kollisionsvorhersage • mechanisch nachgiebige (backdrivable) Gelenkkonstruktion als passive Aufprallabsicherung 	<ul style="list-style-type: none"> • humanoide Systeme: Inverses-Pendel-Problem bedeutet, dass Stoppen nicht gleich sicher ist — siehe Achse 5 Säule 1 • Sturzfolgen auf Dritte oder vulnerable Personen bleiben Hauptrestrisiko
Tier 5	<ul style="list-style-type: none"> • E_{kin} oberhalb der Tier-4-Orientierung (> 200 J) oder Mehrfachgefährdung (kinetisch + thermisch o. ä.) • redundante sensorische Umfelderkennung mit Diversität • Safe Guided Falling / Safe Stability Control für humanoide Bauart 	<ul style="list-style-type: none"> • mehrkanalige Bewegungs- und Umfeldmodellierung • vorausschauende Sturzvermeidung • vollständige mechanische Energiebegrenzung in jedem Operationszustand 	<ul style="list-style-type: none"> • bei Mehrfachgefährdung sind Notfallpläne und Erste-Hilfe-Vorhaltung Betreiberpflicht • vollständiger Kollisionsschutz gegenüber unerwarteten Dritten bleibt strukturell unsicher • die Joule-Schwelle ist Heuristik — Engineering-Bewertung über ISO/TS 15066:2016 Anhang A (Tabellen 2 und 3), nun auch reproduziert in ISO 10218-2:2025 (körperregionenspezifische Schwellen)

6.3 Erwartungsmatrix Achse 3 — Schadenstypen und Schadensschwere

Tier	E-Min — Mindestmaßnahmen	E-Plus — Robustheits-Plus	R — Restrisiken & Maßnahmen
Tier 1	<ul style="list-style-type: none"> • Schadenstyp ausschließlich mechanisch und geringfügig • vollständig reversible 	<ul style="list-style-type: none"> • dokumentierte Schadenstyp-Analyse als Beilage zur 	<ul style="list-style-type: none"> • psychische Schadensfolgen (Erschrecken Dritter) bleiben außerhalb des

Tier	E-Min — Mindestmaßnahmen	E-Plus — Robustheits-Plus	R — Restrisiken & Maßnahmen
	Schadensschwere nach ISO 12100 Tab. B.3	Risikobeurteilung	Modellumfangs auf dieser Stufe
Tier 2	<ul style="list-style-type: none"> • Schadenstypen mechanisch, ggf. elektrisch (Stromschlag bei Defekt) • Schadensschwere geringfügig bis mäßig, langfristig reversibel 	<ul style="list-style-type: none"> • Erste-Hilfe-Plan für vorhersehbare Schadensereignisse • redundante elektrische Isolation 	<ul style="list-style-type: none"> • bei nicht-trainierten Personen oder Kindern können auch geringfügige Schäden überproportionale Folgen haben
Tier 3	<ul style="list-style-type: none"> • Schadenstypen mechanisch und thermisch möglich • Schadensschwere mäßig bis schwer • teilweise irreversible Folgen plausibel (Schnittverletzung) 	<ul style="list-style-type: none"> • dokumentierte Schadenstyp-Matrix mit Reversibilitätsanalyse • Schutzeinrichtungen pro Schadenstyp • Erste-Hilfe-Maßnahmen am Einsatzort 	<ul style="list-style-type: none"> • langfristige Folgen bei mäßig-schweren Schäden (z. B. Narben, Bewegungseinschränkungen) sind Restrisiko, das vom Betreiber abzudecken ist
Tier 4	<ul style="list-style-type: none"> • Schadenstypen mechanisch, thermisch, ggf. biologisch (im Healthcare-Kontext) • Schadensschwere schwer, irreversible Folgen plausibel 	<ul style="list-style-type: none"> • umfassende Schadenstyp-Matrix mit Eintrittswahrscheinlichkeiten • Notfallpläne mit Schadenstyp-spezifischer Reaktion • Versicherungsdeckung dokumentiert 	<ul style="list-style-type: none"> • irreversible Schäden trotz Schutzmaßnahmen bleiben Hauptrestrisiko • biologische Kontamination im Krankenhaus erfordert eigene Hygieneprotokolle
Tier 5	<ul style="list-style-type: none"> • Mehrfachschadenstypen plausibel (mechanisch + thermisch oder biologisch) • Schadensschwere sehr schwer bis letal • ausschließlich irreversible Folgen 	<ul style="list-style-type: none"> • formelle Risikobeurteilung mit zertifizierter Sachverständigenprüfung • Notfall-Eskalationskette zu medizinischer Versorgung • umfassende Versicherung inkl. Cyber-Komponente 	<ul style="list-style-type: none"> • letale Folgen trotz Schutzmaßnahmen sind Restrisiko, das durch organisatorische Maßnahmen (Aufsichtspflicht, Notfallpräsenz) zu mindern ist • Mehrfachgefährdung bedeutet kumulative Restrisiken, die einzeln bewertet werden müssen

6.4 Erwartungsmatrix Achse 4 — Autonomiegrad

Tier	E-Min — Mindestmaßnahmen	E-Plus — Robustheits-Plus	R — Restrisiken & Maßnahmen
Tier 1	<ul style="list-style-type: none"> • Autonomiegrad A0 (ferngesteuert) oder A1 (assistiert) • Bediener trägt jede sicherheitsrelevante Entscheidung 	<ul style="list-style-type: none"> • geschulter Bediener mit Zertifikat • Fernsteuerungsverbindung mit Latenzgarantien 	<ul style="list-style-type: none"> • Verbindungsausfall bei Fernsteuerung: Safe-State-Verhalten zwingend (siehe Achse 5)

Tier	E-Min — Mindestmaßnahmen	E-Plus — Robustheits-Plus	R — Restrisiken & Maßnahmen
	<ul style="list-style-type: none"> klare Bedien-Schnittstelle mit Notabschaltung 		
Tier 2	<ul style="list-style-type: none"> Autonomiegrad A1 oder A2 Routineentscheidungen autonom, Sicherheitsentscheidungen eskaliert klare Eskalations-Schnittstelle zum Bediener 	<ul style="list-style-type: none"> protokollierte Eskalations-Historie Bediener-Reaktionszeit-Vorgaben 	<ul style="list-style-type: none"> bei seltenen sicherheitsrelevanten Eskalationen: Bediener-Reaktionszeit kritisch — Tier-Verletzung möglich, wenn keine Bedienerpräsenz garantiert
Tier 3	<ul style="list-style-type: none"> Autonomiegrad A2 bis A3 definierter Katalog autonom getroffener Sicherheitsentscheidungen menschliche Aufsicht jederzeit möglich 	<ul style="list-style-type: none"> Logging aller sicherheitsrelevanten autonomen Entscheidungen Reaktionszeit-Garantien Eingriffs-Schnittstelle ohne Komplexität 	<ul style="list-style-type: none"> unerwartete Entscheidungssituationen außerhalb des Katalogs können zu unvorhergesehenem Verhalten führen kognitive Überlastung des Aufsichts-Personals bei vielen Eskalationen
Tier 4	<ul style="list-style-type: none"> Autonomiegrad A3 mit hoher Häufigkeit autonomer Sicherheitsentscheidungen kontinuierliche menschliche Aufsicht plausibel unmittelbar erreichbare Eingriffsmöglichkeit 	<ul style="list-style-type: none"> Aufsichts-Dashboard mit Konfidenz-Visualisierung automatische Warnstufen Trainingsprogramm für Aufsichtspersonal 	<ul style="list-style-type: none"> bei hoher Entscheidungshäufigkeit ist permanente Aufsicht praktisch nicht durchhaltbar — Restrisiko ist menschliche Aufmerksamkeitsmüdigkeit
Tier 5	<ul style="list-style-type: none"> Autonomiegrad A4 (vollautonom ohne menschliche Letztkontrolle im Operationsmoment) umfassende Risikobeurteilung der autonomen Entscheidungslogik klare Übernahme-Schnittstelle für Notfälle 	<ul style="list-style-type: none"> mehrstufige Eskalation an menschliche Letztverantwortung auditierbare Entscheidungs-Historie regelmäßige Trainings- und Validierungsläufe 	<ul style="list-style-type: none"> A4-Systeme im Personenkontakt sind regulatorisch und ethisch hoch umstritten — Beschaffer sollte Einsatz mit besonderer Vorsicht prüfen, ggf. Tier-5-Einsatz in vulnerablen Kontexten vermeiden MVO Anhang III und KI-VO-Hochrisiko-Pflichten greifen vollständig

6.5 Erwartungsmatrix Achse 5 — Sicherheitsarchitektur (dreisäulig)

Die Erwartungsmatrix für Achse 5 ist dreisäulig aufgebaut: Pro Tier werden Säule 1 (klassische Sicherheitsarchitektur), Säule 2 (KI-Sicherheitsarchitektur) und Säule 3 (Lifecycle-Update-Mechanik) jeweils eigenständig bewertet. Die Aggregation der drei Säulen zum Achsen-Tier folgt der Mindest-Floor-Logik — Säule 3 wird erst ab Tier 3 aggregationswirksam (siehe Kapitel 8).

T	Säule	E-Min	E-Plus	R
T1	1 — Klass. SiArch.	<ul style="list-style-type: none"> ISO 13849 PL a oder Basis-Schutzmaßnahmen Notabschaltung vorhanden 	<ul style="list-style-type: none"> redundante Notabschaltung 	<ul style="list-style-type: none"> bei Hardware-Defekt vor Update: Stillstand möglich
T1	2 — KI-SiArch.	<ul style="list-style-type: none"> KI ohne Sicherheitsfunktion oder nicht vorhanden 	<ul style="list-style-type: none"> wenn KI: einfache Plausibilitätsprüfung 	<ul style="list-style-type: none"> —
T1	3 — Lifecycle	<ul style="list-style-type: none"> nicht aggregationswirksam (siehe Kap. 8.2) 	<ul style="list-style-type: none"> — 	<ul style="list-style-type: none"> Säule 3 ist auf diesem Tier nicht aggregationswirksam (Kap. 8.2); CRA-Konformität bleibt unabhängig vom Tier verpflichtend
T2	1 — Klass. SiArch.	<ul style="list-style-type: none"> PL b einfache Notabschaltung mit definierter Reaktionszeit 	<ul style="list-style-type: none"> zweikanalige Notabschaltung Selbstdiagnose der Sicherheitsfunktionen 	<ul style="list-style-type: none"> Single-Point-Failures in nicht-redundanten Pfaden bleiben Restrisiko
T2	2 — KI-SiArch.	<ul style="list-style-type: none"> wenn KI vorhanden: einfache Plausibilitätsprüfung der Entscheidungen 	<ul style="list-style-type: none"> dokumentierte Trainings- und Testdaten 	<ul style="list-style-type: none"> KI-Entscheidungen außerhalb des Trainingsraums (Distribution Shift) nicht abgedeckt
T2	3 — Lifecycle	<ul style="list-style-type: none"> nicht aggregationswirksam (siehe Kap. 8.2) 	<ul style="list-style-type: none"> wenn vorhanden: regelmäßige Updates kommuniziert 	<ul style="list-style-type: none"> Säule 3 ist auf diesem Tier nicht aggregationswirksam (Kap. 8.2); CRA-Konformität bleibt unabhängig vom Tier verpflichtend
T3	1 — Klass. SiArch.	<ul style="list-style-type: none"> PL c oder höher Safe Limited Speed, Safe Brake Control definiertes Safe-State-Konzept 	<ul style="list-style-type: none"> Cat-3-Architektur nach ISO 13849-1 Safe Stop 1/2 mit überwachter Reaktion 	<ul style="list-style-type: none"> bei Werkzeugen mit hoher Energiedichte (rotierende Klingen): Mindesterkennungszeit kritisch — siehe Achse 6
T3	2 — KI-SiArch.	<ul style="list-style-type: none"> KI-Entscheidungen mit Sicherheitsbezug haben Plausibilitätsprüfung ISO/IEC TR 5469-konforme Risikobeurteilung der KI-Komponenten 	<ul style="list-style-type: none"> dokumentierte Trainings- und Validierungsdaten Konfidenz-basierte Eskalation 	<ul style="list-style-type: none"> nicht-deterministisches KI-Verhalten in Edge Cases bleibt Restrisiko Erklärbarkeit eingeschränkt
T3	3 — Lifecycle	<ul style="list-style-type: none"> aggregationswirksam ab dieser Stufe Patchbarkeit durch Architektur 	<ul style="list-style-type: none"> Rollback-Mechanismus atomare Updates mit Sicherheitsfunktion- 	<ul style="list-style-type: none"> wesentliche-Veränderungs-Detektion noch unscharf — Auslegung im Vollzug

		sichergestellt	Test	
T4	1 — Klass. SiArch.	<ul style="list-style-type: none"> • kryptografische Signatur der Updates 	<ul style="list-style-type: none"> • Cat-4-Architektur mit Diversität • Active Damping und Safe Guided Falling für humanoide Systeme (z. B. via Active Short Circuit) 	<ul style="list-style-type: none"> • bei humanoider Bauart: vollständige Sturzkontrolle ist nach Stand der Technik nicht durchgängig erreichbar • klassischer Safe Torque Off (STO) erzeugt bei humanoiden Bauformen keinen sicheren Zustand — ohne aktive Stabilitätskontrolle führt STO zu unkontrolliertem Sturz. STO ist daher mit Active Damping (z. B. über Active Short Circuit auf Gelenkebene) und Safe Guided Falling zu kombinieren; die Kombination, nicht STO allein, bildet den Safe-State-Mechanismus • Sturzrisiko durch Batteriezustand: niedrige Batteriestände können einen unkontrollierten Sturz auslösen, sofern kein batteriezustandsbewusster Safe-State-Eingriff (präemptives Safe Guided Falling bei kritischem Batteriestand) implementiert ist
T4	2 — KI-SiArch.	<ul style="list-style-type: none"> • KI-VO-Hochrisiko-Pflichten erfüllt (Risikomanagement, Datenqualität, Transparenz, Aufsicht) • MVO Anhang III einschlägig und erfüllt • dokumentierte Behavioural-Safety-Funktionen mit Hersteller-Eigenerklärung; Risikoanalyse nach ISO/IEC TR 5469 (und der kommenden ISO/IEC TS 22440 sobald veröffentlicht); Drittprüfung empfohlen wo verfügbar 	<ul style="list-style-type: none"> • formelle ISO/IEC TR 5469-Risikobeurteilung • Live-Monitoring mit Konfidenzwerten • Mechanismus zur Detektion von Distribution Shift 	<ul style="list-style-type: none"> • KI-Verhalten in unbekanntenen Situationen bleibt strukturell unsicher • Erklärbarkeit von VLAs ist Stand der Forschung
T4	3 — Lifecycle	<ul style="list-style-type: none"> • CRA-konforme Update-Mechanik • wesentliche- 	<ul style="list-style-type: none"> • redundante Update-Pfade • Notfall-Patches 	<ul style="list-style-type: none"> • Update-Verfügbarkeit hängt empirisch von Anbieter-Lebensdauer

		<p>Veränderungs-Detektion implementiert</p> <ul style="list-style-type: none"> Mindest-Update-Pfad über erwartete Lebensdauer (mind. 5 J.) 	<p>innerhalb 72 h kommuniziert</p>	<p>ab — Sekundärdimension R1/R2/R3 prüfen</p> <ul style="list-style-type: none"> Support-Periode-Lücken-Risiko: Wenn die wirtschaftliche Nutzungsdauer eines Robotik-Einsatzes die Support-Periode des Herstellers nach Artikel 13 CRA (mindestens 5 Jahre) überschreitet, trägt der Betreiber ein verbleibendes Cybersecurity-Support-Lückenrisiko. Vertragliche Support-Periode-Verlängerung sollte als Beschaffungsmaßnahme erwogen werden
T5	1 — Klass. SiArch.	<ul style="list-style-type: none"> PL e, Cat-4-Architektur mit Diversität vollumfängliches Safe-State-Konzept redundante Stillstandspfade 	<ul style="list-style-type: none"> mehrkanalige Sicherheitsfunktionen mit unabhängiger Energieversorgung kontinuierliche Selbstdiagnose 	<ul style="list-style-type: none"> selbst PL-e-Architekturen haben begrenzte Wahrscheinlichkeit gefährlicher Ausfälle, nicht null bei humanoiden Bauformen ist klassischer Safe Torque Off (STO) kein Safe-State-Mechanismus — STO ist mit Active Damping und Safe Guided Falling zu kombinieren, um einen sicheren Stopp nachzuweisen Sturzrisiko durch Batteriezustand: niedrige Batteriestände können einen unkontrollierten Sturz auslösen, sofern kein batteriezustandsbewusster Safe-State-Eingriff (präemptives Safe Guided Falling bei kritischem Batteriestand) implementiert ist
T5	2 — KI-SiArch.	<ul style="list-style-type: none"> vollumfängliche KI-VO-Hochrisiko-Konformität MVO Anhang III erfüllt Behavioral Safety dokumentiert, risikobewertet und Drittprüfung wo verfügbar umfassende Erklärbarkeit 	<ul style="list-style-type: none"> formale Verifikation kritischer KI-Komponenten (soweit Stand der Technik) redundante KI-Modelle mit Cross-Check 	<ul style="list-style-type: none"> vollständige Verifikation neuronaler Netze ist nicht erreichbar — strukturelles Restrisiko

T5	3 — Lifecycle	<ul style="list-style-type: none"> • CRA-Konformität mit Notfall-Update-Pfaden • Wesentliche-Veränderungs-Detektion dokumentiert und unabhängig geprüft, soweit ein anerkannter Prüfpfad verfügbar ist • regelmäßige Audit-Updates dokumentiert 	<ul style="list-style-type: none"> • redundante OTA-Pfade • vorgeplante Eskalation bei Update-Versagen • kontinuierliche Compliance-Überwachung 	<ul style="list-style-type: none"> • Anbieter-Insolvenz oder Marktexit kann Update-Lieferung in Frage stellen — Sekundärdimension R1/R2/R3 entscheidend • Support-Periode-Lücken-Risiko: Wenn die wirtschaftliche Nutzungsdauer eines Robotik-Einsatzes die Support-Periode des Herstellers nach Artikel 13 CRA (mindestens 5 Jahre) überschreitet, trägt der Betreiber ein verbleibendes Cybersecurity-Support-Lückenrisiko. Vertragliche Support-Periode-Verlängerung sollte als Beschaffungsmaßnahme erwogen werden
----	---------------	--	--	--

6.6 Erwartungsmatrix Achse 6 — Exponierte Personen und Expositionsfrequenz

Tier	E-Min — Mindestmaßnahmen	E-Plus — Robustheits-Plus	R — Restrisiken & Maßnahmen
Tier 1	<ul style="list-style-type: none"> • nur trainierte Mitarbeitende exponiert • ggf. nur einzelne Personen • Expositionsfrequenz: kurze Begegnung, keine dauerhafte Mitbewesenheit 	<ul style="list-style-type: none"> • dokumentierte Schulungs-Historie • Anwesenheitskontrolle 	<ul style="list-style-type: none"> • bei Wechsel des Personenkreises Reklassifikation prüfen
Tier 2	<ul style="list-style-type: none"> • erwachsene Personen exponiert • Hausrechte bei Privatpersonen anwendbar • ohne vulnerable Gruppen • Expositionsfrequenz: kurze bis mittlere Mitbewesenheit (Minuten bis wenige Stunden) 	<ul style="list-style-type: none"> • Verhaltensregeln dokumentiert • Zugang von Kindern und Tieren ausgeschlossen 	<ul style="list-style-type: none"> • Tierbegegnungen (Haushund, Katze) sind im Privatkontext nicht ausschließbar — Restrisiko bleibt
Tier 3	<ul style="list-style-type: none"> • gemischte Adressaten möglich • Kinder oder Senioren ausschließbar oder organisatorisch geschützt • Expositionsfrequenz: mittlere Mitbewesenheit, planbar begrenzt 	<ul style="list-style-type: none"> • Sperrzeiten für sensible Personenkreise • akustische/visuelle Annäherungswarnung 	<ul style="list-style-type: none"> • spontane Drittpersonen-Anwesenheit nicht vollständig ausschließbar — organisatorische Aufsichtspflicht

Tier	E-Min — Mindestmaßnahmen	E-Plus — Robustheits-Plus	R — Restrisiken & Maßnahmen
Tier 4	<ul style="list-style-type: none"> ▪ vulnerable Gruppen plausibel oder regelmäßig exponiert (Kinder, Senioren, Patienten) ▪ Expositionsfrequenz: längere oder häufige Mitwesenheit (mehrere Stunden täglich oder regelmäßig wiederkehrend) ▪ Aufsichts- oder Schutzkonzept dokumentiert 	<ul style="list-style-type: none"> ▪ adaptive Verhaltensanpassung an Personentyp (z. B. langsamer in Kinderbereichen) ▪ redundante Personenerkennung 	<ul style="list-style-type: none"> ▪ spontane Reaktionen vulnerabler Personen (Erschrecken, Sturz) nicht vollständig vermeidbar ▪ psychische Schadensfolgen sind Mit-Restrisiko
Tier 5	<ul style="list-style-type: none"> ▪ vulnerable Gruppen direkt und dauerhaft exponiert (Pflegekontext, Kinderbetreuung) ▪ Expositionsfrequenz: dauerhafte Mitwesenheit oder direkter Personenkontakt über Stunden täglich ▪ umfassendes Schutzkonzept mit Aufsichtspersonal ▪ Notfallpräsenz garantiert 	<ul style="list-style-type: none"> ▪ personenbezogene Adaption (z. B. Patienten-Profile) ▪ kontinuierliche Anwesenheitsüberwachung des Aufsichtspersonals 	<ul style="list-style-type: none"> ▪ dauerhafter direkter Kontakt mit vulnerablen Gruppen ist regulatorisch und ethisch besonders sensibel — Beschaffer sollte Einsatz nur mit ausdrücklicher Vorab-Beurteilung durch Sachverständige erwägen

7 Sekundärdimensionen

Die Tier-Skala 1–5 ist die primäre Bewertungsdimension von HU-RSC. Zwei Sekundärdimensionen ergänzen sie — strukturell parallel zu HU-RAC, inhaltlich aber sicherheits-spezifisch reinterpretiert.

7.1 Business-Kritikalität A/B/C

Die Business-Kritikalität misst die wirtschaftliche und reputative Tragweite eines Sicherheits-Vorfalles für den Betreiber. Drei Klassen sind leitend:

- **A — kritisch** — ein Sicherheits-Vorfall hat existenzgefährdende Wirkung (Betriebsstillstand, schwere Personenschäden mit Strafverfolgung, Reputationsverlust mit Marktexit). Typisch im Healthcare-Kontext, in regulierter Industrie, bei kommunalen Auftraggebern.
- **B — erheblich** — ein Sicherheits-Vorfall hat erhebliche Wirkung (mehrwöchiger Betriebsstillstand, signifikante Schadensersatz-Ansprüche, lokale Reputationsverluste). Typisch im KMU-Industriebereich.
- **C — begrenzt** — ein Sicherheits-Vorfall hat begrenzte Wirkung (kurzfristiger Betriebsausfall, versicherte Schadensersatz-Ansprüche). Typisch im Konsumentenkontext, B2C-Service.

Die Business-Kritikalität ist nominell unabhängig vom HU-RSC-Tier, tatsächlich aber häufig korreliert: Healthcare-Anwendungen (typisch Tier 4 oder 5) sind meist auch A-kritisch, Konsumenten-Anwendungen (typisch Tier 2 oder 3) meist C-kritisch.

7.2 Anbieter-Resilienz R1/R2/R3

Die Anbieter-Resilienz bewertet die Wahrscheinlichkeit, dass die in den Achsen 1–6 nachgewiesene technische Sicherheitsfähigkeit über typische Robotik-Lifecycle-Zeiträume von 5–10 Jahren erhalten bleibt. Drei Klassen sind leitend:

- **R1 — hoch resilient** — etablierter Anbieter mit nachweislicher Marktstellung, dokumentierter Update-Lieferhistorie und klaren Lifecycle-Zusagen. Bonität geprüft (Creditreform, CRIF, North Data o. ä.). Notfall-Update-Pfad definiert.
- **R2 — mittel resilient** — Anbieter mit funktionierendem Geschäftsmodell, aber ohne durchgängige Lifecycle-Erfahrung oder mit höherem Bonitätsrisiko. Update-Lieferung wahrscheinlich, aber nicht garantiert. Sekundärquellen (z. B. Open-Source-Komponenten) als Risikomilderung.
- **R3 — schwach resilient** — junges Unternehmen, Pre-Revenue-Startup, instabile Marktlage oder bekannte Bonitätsprobleme. Update-Lieferung über erwartete Lebensdauer nicht plausibel sicher. Vendor-Lock-in mit hohem Restrisiko.

Inhaltsdifferenzierung gegenüber HU-RAC:

In HU-RAC misst R1/R2/R3 Anbieter-Resilienz im Sinne von Datensouveränität (Schutz gegen Anbieter-Übernahme, Cloud-Lock-in, Dateninhaber). In HU-RSC misst R1/R2/R3 Anbieter-Stabilität im Sinne von Lifecycle-Persistenz und Compliance-Kapazität (Bonität,

Marktstellung, Fähigkeit zur Lieferung sicherheitsrelevanter Updates und Ersatzteile). Beide Skalen sind strukturell parallel, aber nicht inhaltlich identisch — Beschaffer dürfen sie nicht als 1:1-Kopie behandeln.

Hinweis zur vertikalen Integrationstiefe. Die vertikale Integrationstiefe des Anbieters ist ein zusätzliches Resilienz-Signal — sowohl positiv (Lifecycle-Lieferfähigkeit bei in-house entwickelten Sub-Systemen) als auch negativ (Konzentrationsrisiko, eingeschränkte Sub-System-Substitution). Eine Branchenübersicht der OEM-Strategie-Verteilung liefert FEV Consulting (Q3 2025): 100 % in-house Vollentwicklung bei allen 11 erfassten Leading-Humanoid-OEMs, aber stark differenzierte Outsourcing-Quoten in Vision-Sensorik, Compute, Aktuatorik und Batterie-System.

7.3 Verhältnis zu Achse 5 Säule 3

Achse 5 Säule 3 (Lifecycle-Update-Mechanik) und Sekundärdimension R1/R2/R3 (Anbieter-Resilienz) sind komplementär. Achse 5 Säule 3 misst die technische Update-Fähigkeit als System-Eigenschaft — kann das System überhaupt sicher gepatcht werden? R1/R2/R3 misst die empirische Wahrscheinlichkeit, dass der Anbieter die Updates auch tatsächlich liefert.

Ein patchfähiges System nützt nichts ohne lieferfähigen Anbieter. Umgekehrt nützt ein finanziell stabiler Anbieter nichts, wenn das System architektonisch nicht patchbar ist. Beide Dimensionen sind notwendig.

8 Aggregations- und Reklassifikationsregeln

8.1 Aggregation der sechs Achsen

Das Tier des Gesamtsystems ergibt sich aus den Tiers der sechs Achsen nach dem Prinzip der stärksten Belastung — die schwächste Achse (das höchste einzelne Tier) bestimmt das Gesamt-Tier des Systems.

Diese Regel ist methodisch konservativ und entspricht der ISO-12100-Logik: Das höchste relevante Risiko definiert die Schutzmaßnahmen-Anforderung. Sie schützt Beschaffer vor der Versuchung, niedrige Achsen-Tiers gegen hohe zu verrechnen — was sicherheitstechnisch unzulässig wäre.

Defense-in-depth als architektonisches Prinzip. HU-RSC operationalisiert das Prinzip, dass Sicherheit in der Mensch-Roboter-Interaktion ab Tier 3 aufwärts auf der geschichteten Kombination von Maßnahmen beruht — Umgebungstrennung, sensorbasierte Erkennung, Software-Grenzen, organisatorische Abläufe. Keine Einzelmaßnahme reicht, solange anbieterzertifizierte Sicherheitsfunktionen noch nicht durchgängig verfügbar sind. Die obenstehende Weakest-Link-Aggregationsregel ist die formalisierte Ausprägung dieses Prinzips: der Einkäufer kann schwache Maßnahmen auf einer Achse nicht durch starke Maßnahmen auf einer anderen ausgleichen.

8.2 Aggregation innerhalb Achse 5 — Mindest-Floor-Logik

Die dreisäulige Achse 5 wird nicht durch eine reine Anwendung des Prinzips der stärksten Belastung aggregiert. Stattdessen gilt eine modifizierte Mindest-Floor-Logik:

- **Säule 3 nicht aggregationswirksam für Tier 1/2** — für Tier 1 und Tier 2 wird Säule 3 (Lifecycle-Update-Mechanik) bei der Aggregation nicht aggregationswirksam
- **Säule 3 aggregationswirksam ab Tier 3** — ab Tier 3 aufwärts wird Säule 3 voll aggregationswirksam
- **Säulen 1 und 2** — Säulen 1 und 2 sind über alle Tiers nach dem Prinzip der stärksten Belastung aggregiert

Die Begründung ist zweisträngig. Sicherheitstechnisch: Bei Tier-1- und Tier-2-Systemen — kinetisch unbedenkliche oder nur mäßig belastende Anwendungen ohne sicherheitskritische KI — sind Säulen 1 und 2 (initiale Sicherheitsarchitektur) bereits auf niedrigem Anforderungsniveau, sodass eine zusätzliche Verschärfung des Achsen-Tiers durch eine schwache Säule 3 die aggregierte Sicherheitsbewertung nicht verbessern, sondern lediglich verschieben würde — bei gleichbleibend niedrigem Risikoprofil. Methodisch: Die Mindest-Floor-Logik vermeidet, dass eine schwache Lifecycle-Update-Mechanik bei einem ansonsten harmlosen System auf ein Achsen-Tier wirft, das die regulatorische und betriebliche Tragweite nicht trägt.

Wichtige Klarstellung — keine CRA-Freistellung:

Die Mindest-Floor-Logik bedeutet ausdrücklich nicht, dass Tier-1- und Tier-2-Systeme von Cyber-Resilience-Act-Pflichten oder Update-Lieferpflichten freigestellt sind. Der CRA gilt produktklassenübergreifend und unabhängig vom HU-RSC-Tier. Säule 3 wird bei Tier

1/2 nur in der HU-RSC-internen Tier-Aggregation nicht wirksam — als regulatorische und betriebliche Anforderung bleibt sie für jedes Robotiksystem mit digitalen Elementen relevant. Die Erwartungsmatrix Achse 5 Säule 3 weist diesen Sachverhalt in der R-Spalte für Tier 1/2 entsprechend aus.

Diese Mindest-Floor-Logik wird im Vollzug auf zeitversetzte Wirksamkeit hin nochmals geprüft. Säule 3 wirkt anders als Säulen 1 und 2 nicht initial, sondern über die Lebensdauer. Die Aggregationsregel kann in einer Folgeversion verfeinert werden, falls die Praxis Hinweise auf Fehlanreize liefert.

8.3 Reklassifikation bei wesentlichen Veränderungen

Robotiksysteme sind dynamisch: Software-Updates können das Verhalten verändern, Werkzeugwechsel können kinetische Profile verschieben, Einsatz-Kontext-Änderungen können Achse 1 oder Achse 6 verschieben. HU-RSC fordert daher eine Reklassifikations-Prüfung bei jedem der folgenden Trigger:

- **Software-Trigger** — Software-Update mit Auswirkung auf Sicherheitsfunktionen (siehe Achse 5 Säule 3 — wesentliche-Veränderungs-Detektion).
- **KI-Trigger** — KI-Modell-Update bei Hochrisiko-KI nach KI-VO 2024/1689 (siehe MVO Anhang III — selbstentwickelnde Systeme).
- **Hardware-Trigger** — Werkzeug- oder Anbau-Modifikation, die Bauart oder kinetisches Schadenspotenzial verändert (Achse 2).
- **Kontext-Trigger** — Wechsel der Einsatzumgebung oder des Personenkreises (Achse 1 oder Achse 6).
- **Regulatorischer Trigger** — regulatorische Änderungen (z. B. Inkrafttreten neuer ISO-Normen, geänderte Auslegung der Maschinenverordnung).

Die Auslegung des Begriffs der „wesentlichen Veränderung“ nach Maschinenverordnung 2023/1230 ist im Detail noch offen. HU-RSC orientiert sich konservativ und behandelt jeden Trigger als Reklassifikations-Anlass — die rechtsverbindliche Bewertung verbleibt beim Inverkehrbringer und den zuständigen Behörden.

9 Mindestkopplung HU-RSC × HU-RAC

9.1 Die asymmetrische Mindestkopplung

HU-RSC und HU-RAC sind nominell unabhängige Modelle, tragen aber eine harte Mindestkopplung in einer Richtung.

HU-RSC \geq 4 verlangt HU-RAC \geq 3

asymmetrisch — die umgekehrte Richtung gilt nicht

9.2 Begründung der Kopplung

Sicherheitsfunktionen ab HU-RSC-Tier 4 erzeugen sicherheitsrelevante Telemetrie (Notabschaltungen, Kollisionereignisse, KI-Konfidenzwerte, Stabilitätsverluste). Die Maschinenverordnung 2023/1230 fordert in Anhang III ausdrücklich Schutz gegen Korruption sicherheitsrelevanter Daten und Software. Wenn diese Telemetrie nicht hinreichend integritätsgeschützt ist, ist die Safety-Argumentation des Tier-4-Systems unterbrochen — die Sicherheitsfunktion liefert dann keine vertrauenswürdige Evidenz mehr.

Der konkrete Anker für die Mindestkopplung HU-RAC \geq 3 liegt in der HU-RAC-Architektur selbst. HU-RAC v0.3.1 Achse 5 (Cybersicherheit) führt erst auf Tier 3 als E-Min-Anforderung den Integritätsschutz sicherheitsrelevanter Daten und die abgesicherte Update-Mechanik ein — Tier 1 und Tier 2 adressieren primär Datenschutz, Authentifizierung und Vertraulichkeit, nicht aber den Integritätsschutz von Telemetrie und Steuerungsdaten gegen Korruption. Die HU-RSC-Tier-4-Systeme verlangen aber genau diesen Integritätsschutz (MVO Anh. III). HU-RAC 3 ist damit nicht eine willkürliche Setzung, sondern das niedrigste HU-RAC-Tier, in dem die regulatorische Mindestanforderung der MVO an die Daten-Integrität strukturell adressiert ist.

Eine hohe HU-RSC-Klasse ohne hinreichende HU-RAC-Klasse ist daher nicht hochintegritätsfähig betreibbar — die Kopplung ist regulatorisch erzwungen, nicht ästhetisch. Existierende Safety-Bus-Implementierungen — etwa FSoE (Fail-Safe over EtherCAT) — liefern Safe Process Data mit Integritätsschutz auf Protokollebene. Ab HU-RSC Tier 4 muss der Pfad sicherheitsrelevanter Telemetrie nachweisbar einen äquivalenten Integritätsschutz implementieren; dies ist der technische Anker für die Mindestkopplung zu HU-RAC Tier 3.

9.3 Asymmetrie

Die umgekehrte Richtung — eine hohe HU-RAC-Klasse erzwingt keine hohe HU-RSC-Klasse — ist nicht gegeben. Ein datensensibler, aber stationärer und kinetisch harmloser Roboter ist denkbar (z. B. ein Telepräsenz-System mit Videoaufzeichnung in einem Anwaltsbüro). Die Kopplung ist asymmetrisch, weil Datenschutz ohne kinetisches Risiko ein realistisches Szenario ist, kinetisches Risiko ohne Datenschutz dagegen nicht.

Empirischer Bezug HU-RAC \leftrightarrow HU-RSC. AttackVLA (Li et al., 2025) zeigt parallel, dass Backdoor-Angriffe auf VLA-Modelle in Simulation und realer Roboterumgebung mit einem

mittleren gezielten Erfolg von 58,4 % möglich sind, einzelne Aufgaben sogar mit 100 %. Dieser Befund macht die Schnittstelle HU-RAC ↔ HU-RSC empirisch greifbar: Eine kompromittierte KI-Steuerung wird unmittelbar zur physikalischen Gefährdung. Die Cybersicherheits-Achse (HU-RAC) ist damit kein analytisch sauber von HU-RSC trennbares Konzept, sondern ein operativ verschränktes.

9.4 Operative Konsequenzen

Für die Beschaffungspraxis bedeutet die Mindestkopplung:

- **Bei Tier 4 oder 5** — ein Robotiksystem mit HU-RSC-Tier 4 oder 5 muss vom Anbieter zwingend mit einer HU-RAC-Tier-3-tauglichen Daten- und Update-Architektur ausgestattet sein.
- **Im Mittelstand außerhalb Healthcare** — ist HU-RAC ≥ 3 für Tier-4-/Tier-5-Anwendungen empfohlen, kann aber unter strengeren betrieblichen Aufsichts-Auflagen abgesenkt werden.
- **Im Healthcare-Kontext** — ist HU-RAC ≥ 3 nicht verhandelbar — die Kombination Tier-5-System mit schwacher HU-RAC-Klasse begründet ein nicht hinnehmbares Compliance-Risiko.

10 Anwendung in der Beschaffungspraxis

HU-RSC ist als Beschaffungs-Heuristik konzipiert. Dieses Kapitel skizziert, wie das Modell in einem Beschaffungsprozess eingesetzt wird, und führt das Vorgehen an einem durchgerechneten Beispiel vor. Detaillierte Operationalisierung — Fragebögen, Bewertungsraster, anbieter-spezifische Scorecards — findet sich nicht hier, sondern im Anforderungskatalog v2.x (Dokument 01, intern) und im Anforderungsprofil v2.x (Dokument 03, extern).

10.1 Drei-Schritte-Logik

- **Schritt 1 — Anspruchsniveau bestimmen** — Beschaffer identifiziert das Anspruchsniveau, das der konkrete Use Case erfordert. Was muss das System mindestens leisten? Diese Bewertung ist unabhängig vom konkreten Produkt. Ergebnis: Soll-HU-RSC-Tier.
- **Schritt 2 — Produkt einordnen** — Beschaffer prüft das angebotene Produkt entlang der sechs Achsen und der Erwartungsmatrizen. Erfüllt es die E-Min-Anforderungen seines Soll-Tiers? Ergebnis: Ist-HU-RSC-Tier des Produkts.
- **Schritt 3 — Vergleich und Entscheidung** — Wenn Ist-Tier \geq Soll-Tier: Beschaffung möglich, R-Spalte als Aufgabenliste für ergänzende Maßnahmen abarbeiten. Wenn Ist-Tier $<$ Soll-Tier: alternatives Produkt prüfen oder Use Case anpassen.

10.2 Anbindung an HU-RAC und Anforderungskatalog

Für die vollständige Bewertung sind beide Modelle gemeinsam anzuwenden — HU-RAC für Daten und Resilienz, HU-RSC für Sicherheit. Die Mindestkopplung (Kapitel 9) gibt die Untergrenze. Anbieter-spezifische Bewertungen (NEURA, Agile Robots, PAL, Hexagon, Yarbo, Nexaro u. a.) finden sich im Anforderungskatalog v2.x, der separat publiziert wird und unabhängig von diesem Impulspapier aktualisiert wird.

Verifikation von Konformitätsbehauptungen. Hersteller-Aussagen wie „PLe“, „SIL3“, „AI-Act-konform“, „CRA-ready“ oder Vergleichbares sind durch ein Konformitätszertifikat einer benannten oder zuständigen Stelle zu belegen, das Norm-Version, Anwendungsbereich der Sicherheitsfunktion, Gültigkeitsdatum des Zertifikats und Kennnummer der benannten Stelle ausweist. Whitepaper- oder Marketingaussagen reichen für sich nicht als Nachweis der HU-RSC E-Min-Konformität ab Tier 4 aufwärts. Einkäufer sollten Zertifikatskopien anfordern und in der Beschaffungsakte ablegen.

10.3 Anwendungsbeispiel — humanoider Roboter in KMU-Werkstatt

Zur Veranschaulichung der Drei-Schritte-Logik wird ein fiktiver, aber realitätsnaher Beschaffungsfall durchgerechnet. Ein metallverarbeitender mittelständischer Betrieb mit 35 Mitarbeitenden möchte einen humanoiden Roboter für Werkstückzuführung und Werkzeug-Bestückung an einer CNC-Maschine pilotieren. Der Roboter soll sich frei in einem definierten Werkstattbereich bewegen, Werkstücke vom Lager zur Maschine bringen und unbeaufsichtigt zwischen den geschulten Mitarbeitenden arbeiten.

Schritt 1 — Soll-Tier bestimmen

Die sechs Achsen werden im Use Case eingeordnet:

- **Achse 1 (Einsatzumgebung)** — halbkontrollierte Werkstatt-Umgebung mit Mitarbeitenden — Tier 3 als Soll.
- **Achse 2 (Bauart)** — humanoide Bauart mit Sturzpotenzial, kinetisch im Bereich 80–200 J — Tier 4 als Soll.
- **Achse 3 (Schadenstypen)** — mechanische Schadensschwere schwer plausibel, irreversible Folgen möglich — Tier 4 als Soll.
- **Achse 4 (Autonomiegrad)** — teilautonom mit menschlicher Aufsicht (A3), mehrmals stündlich sicherheitsrelevante autonome Entscheidungen — Tier 4 als Soll.
- **Achse 5 (Sicherheitsarchitektur)** — Sicherheitsarchitektur muss humanoide Bauart und KI-getriebene Entscheidungen tragen — Tier 4 als Soll.
- **Achse 6 (Exponierte Personen)** — erwachsene Mitarbeitende, geschult, ohne vulnerable Gruppen, mehrere Stunden tägliche Mitbewesenheit — Tier 3 als Soll.

Aggregation nach dem Prinzip der stärksten Belastung: Soll-HU-RSC-Tier = 4. Die Mindestkopplung (Kap. 9) verlangt damit auch HU-RAC ≥ 3 .

Schritt 2 — Konkretes Produkt einordnen

Der Anbieter offeriert einen humanoiden Roboter mit folgenden ausgewiesenen Merkmalen: PL d für die kritischen Sicherheitsfunktionen, Active Damping (über Active Short Circuit) implementiert (aber nicht durch Dritte bewertet), KI-VO-Hochrisiko-Selbstauskunft vorhanden ohne externe Zertifizierung, dokumentierte Update-Mechanik mit OTA aber ohne ausdrückliche Wesentliche-Veränderungs-Detektion, Anbieter ist ein Pre-Revenue-Startup mit 18 Monaten Marktexistenz.

Bewertung entlang der Erwartungsmatrizen:

Achsenweise Bewertung des angebotenen Produkts: Achse 1 (Einsatzumgebung) — teilkontrollierte Werkstattumgebung mit Beschäftigten, organisatorische Schutzmaßnahmen, definierte Ausschlusszeiten — erfüllt Tier-3 E-Min, mit zusätzlichen Maßnahmen gegen das Tier-4-Ziel zu bewerten. Achse 2 (Bauart / kinetisches Schadenspotenzial) — humanoide Bauform, Gehgeschwindigkeit ca. 1 m/s, Sturzpotenzial vorhanden — erfüllt Tier-4-Typkonfiguration, aber nicht Tier-5. Achse 3 (Schadenstypen) — mechanisch mit plausibel schwerer Schadensschwere, irreversible Folgen möglich — Tier-4-Ziel erfüllt. Achse 4 (Autonomiegrad) — teilautonom (A3) mit mehreren sicherheitsrelevanten autonomen Entscheidungen pro Stunde — Tier-4-Ziel erfüllt. Achse 6 (exponierte Personen) — geschulte erwachsene Beschäftigte, keine vulnerablen Gruppen, mehrere Stunden tägliche Ko-Präsenz — Tier 3 in Übereinstimmung mit Tier-4 Mindest-Betreibermaßnahmen. Achse 5 detaillierte Bewertung (drei Säulen):

- **Säule 1** — Achse 5 Säule 1 erfüllt die Tier-4-E-Min (PL d) — passt.
- **Säule 2** — Achse 5 Säule 2 erfüllt die Tier-4-E-Min nicht vollständig — KI-VO-Hochrisiko-Pflichten ohne externe Zertifizierung sind grenzwertig, MVO-Anh.-III-Erfüllung unklar.
- **Säule 3** — Achse 5 Säule 3 erfüllt die Tier-4-E-Min nicht — fehlende Wesentliche-Veränderungs-Detektion ist ein E-Min-Mangel auf Tier 4.
- **Sekundärdimension R-Klasse** — Anbieter ist Pre-Revenue-Startup ohne dokumentierte Lifecycle-Erfahrung — R3 (schwach resilient).

HU-RAC-Parallelbewertung. Der Anbieter erklärt, dass das Backend innerhalb der EU auf einer Infrastruktur betrieben wird, die von einer europäischen Tochtergesellschaft eines US-Mutterkonzerns betrieben wird. Update-Signaturen sind vorhanden; Mandantentrennung ist in den technischen und organisatorischen Maßnahmen des Anbieters dokumentiert. Nach HU-RAC v0.3.1 erreicht dieser Anbieter Tier 3 auf der Datensouveränitäts-Achse nur bedingt — die US-Mutterbeteiligung löst eine Prüfung nach Artikel 48 DSGVO unter dem CLOUD Act aus. Ohne diese Prüfung ist HU-RAC Tier 3 nicht belegbar, und die Mindestkopplung ($\text{HU-RSC} \geq 4$ verlangt $\text{HU-RAC} \geq 3$) ist nicht erfüllt. Dies blockiert Tier 4 bereits, bevor die sicherheitsseitigen Lücken adressiert werden.

Ist-HU-RSC-Tier des Produkts: Tier 3 (Achse 5 trägt nur Tier-3-Konformität, weil Säule 2 und 3 die Tier-4-E-Min nicht erfüllen — die schwächste Säule bestimmt das Achsen-Tier; das schwächste Achsen-Tier bestimmt das Gesamt-Tier).

Schritt 3 — Vergleich und Entscheidung

Soll-Tier = 4, Ist-Tier = 3. Das Produkt erreicht das Soll-Tier nicht. Hinzu kommt die Sekundärdimension R3, die für sicherheits-relevante Tier-4-Anwendungen problematisch ist (Update-Lieferung über Lebensdauer nicht plausibel sicher).

Mögliche Beschaffungsentscheidungen: Erstens, Verzicht auf das Produkt und Suche nach einem Alternativ-Anbieter, der Tier 4 Säule 2 und 3 erfüllt. Zweitens, Anpassung des Use Case auf Tier-3-Niveau — etwa durch zusätzliche Trennung Roboter und Mitarbeitende durch Sperrzeiten oder definierte Arbeitsphasen. Drittens, vertragliche Risikoverlagerung gezielt zur Adressierung der R3-Klasse: Update-Lieferzusicherung über die geplante Nutzungsdauer von 5–7 Jahren, Hinterlegung einer Bonitäts-Garantie oder Source-Code-Escrow für den Insolvenzfall, dokumentierte Ersatzteilverfügbarkeit. Die Wahl zwischen diesen Optionen ist eine betriebliche Risiko-Abwägungsentscheidung, kein Modell-Output — HU-RSC liefert die Diagnose, nicht das Therapie-Rezept.

Hinweis: Dieses Beispiel ist illustrativ und ersetzt keine konkrete Risikobeurteilung nach ISO 12100. Reale Beschaffungsentscheidungen erfordern eine vertiefte Prüfung durch Sachverständige und ggf. juristische Beratung.

11 Schlusswort

HU-RSC ist ein Modell für die Beschaffungspraxis im DACH-Mittelstand, kein universelles Klassifikationssystem. Es konkurriert nicht mit etablierten Normen, sondern ergänzt sie um eine Beschaffer-Perspektive, die in der Engineering-zentrierten Norm-Welt unterrepräsentiert ist. Anregungen, Korrekturvorschläge und Praxiserfahrungen aus der Anwendung sind ausdrücklich erwünscht und fließen in zukünftige Versionen ein.

12 Anhang — Mapping-Tabellen ISO-Klassen

Die folgende Tabelle ordnet HU-RSC-Tiers den einschlägigen ISO-Sicherheits-Klassen zu. Diese Zuordnung ist eine Orientierung, keine Konversion. ISO-Klassen bewerten einzelne Sicherheitsfunktionen, HU-RSC bewertet Gesamtsysteme — beide Granularitätsebenen sind nicht direkt verrechenbar. Die Tabelle dient dazu, einem mit ISO-Normen vertrauten Beschaffer eine schnelle Einordnung zu ermöglichen.

HU-RSC-Tier	ISO 13849-1 (PL)	IEC 61508 (SIL)	ISO 26262 (ASIL)*	ISO 25785-1**
Tier 1	PL a typisch	SIL 1 oder kein Anspruch	QM oder ASIL A (i.S.d. Robotik nicht direkt anwendbar)	Klasse niedrig (vorläufig)
Tier 2	PL b typisch	SIL 1	ASIL A–B (vorläufige Orientierung)	Klasse niedrig–mittel (vorläufig)
Tier 3	PL c typisch	SIL 1–2	ASIL B (vorläufige Orientierung)	Klasse mittel (vorläufig)
Tier 4	PL d typisch	SIL 2–3	ASIL C–D (vorläufige Orientierung)	Klasse hoch (vorläufig)
Tier 5	PL e typisch	SIL 3	ASIL D (vorläufige Orientierung)	Klasse sehr hoch (vorläufig)

* ASIL nach ISO 26262 stammt aus dem Automotive-Sektor und ist für Robotik nicht direkt anwendbar. Die Spalte ist als grobe Risiko-Niveau-Orientierung gedacht.

** ISO 25785-1 ist zum Stand April 2026 noch Working Draft (Klassifikation für dynamisch stabile mobile Roboter). Bei Veröffentlichung der finalen Norm (voraussichtlich 2027) wird die Mapping-Tabelle in einer Folgeversion dieses Impulspapiers aktualisiert. Bis dahin gilt die vorläufige Orientierung mit Vorbehalt.

Empirischer Referenzpunkt. Fraunhofer-IPA-KM Umanoid-Messungen (September 2025) an einem Unitree-G1-Humanoid-Roboter (35 kg, 1,32 m Höhe, Geschwindigkeit ca. 1 m/s) erreichen rund 530 N Vorwärts-Geh-Kontaktkraft am Bauch und 510 N am Brustkorb — etwa Faktor 2,4 über ISO 10218-2:2025 Schmerzbeginn-Schwellen. Ein 35-kg-Humanoid bei normaler Gehgeschwindigkeit platziert sich systematisch in HU-RSC Tier 4 auf Achse 2. Quelle: Fraunhofer IPA, Leitfaden Sicherheit Humanoider Roboter, 25. Oktober 2025.

12.1 Hinweise zur Verwendung der Mapping-Tabelle

- **PL/SIL als Hinweis, nicht als Beweis** — Hat ein Anbieter sein Produkt mit PL d zertifiziert, ist das ein Hinweis auf eine Tier-4-Eignung — nicht aber ein Beweis. Die anderen Achsen (Einsatzumgebung, exponierte Personen, Autonomiegrad usw.) sind separat zu prüfen.
- **PL und SIL nicht synonym** — ISO 13849-1 PL bewertet sicherheitsbezogene Steuerungsteile, IEC 61508 SIL bewertet Safety Integrity. Manche Komponenten

haben PL-Ausweisung, andere SIL-Ausweisung. Beide sind verwertbar, aber nicht identisch.

- **Joule-Heuristik vs. ISO/TS 15066:2016 Anhang A (Tabellen 2 und 3), nun auch in ISO 10218-2:2025 reproduziert** — Die in Achse 2 verwendeten Joule-Schwellen sind eine Beschaffungs-Heuristik. Die engineering-präzise Bewertung von Mensch-Roboter-Kollisionen erfolgt nicht über kinetische Energie als Skalar, sondern über ISO/TS 15066:2016 Anhang A (Tabellen 2 und 3), nun auch in ISO 10218-2:2025 reproduziert — diese definiert körperregionen-spezifische Kraft- und Druck-Schwellen für 29 Körperregionen. Eine Joule-Bewertung ohne Bezug zur Aufprallfläche und Aufprallrichtung ist sicherheitstechnisch unvollständig. Im Beschaffungskontext ist die Joule-Heuristik dennoch nützlich, weil sie eine schnelle erste Einordnung erlaubt — die ISO/TS-15066-Bewertung bleibt der Risikobeurteilung nach ISO 12100 vorbehalten.
- **Mapping-Updates** — Wenn die finalen Normen (ISO 25785-1 für humanoide und dynamisch stabile mobile Roboter, ISO/IEC TR 5469 für KI-Funktionssicherheit) veröffentlicht sind, wird das Mapping in einer Folgeversion des Impulspapiers aktualisiert. Das Modell selbst bleibt davon unberührt.

13 Anhang — Glossar

Dieser Anhang sammelt Arbeitsdefinitionen technischer Begriffe, die in diesem Papier verwendet werden. Wo ein Begriff aus einer bestimmten Herstellerquelle oder technischen Spezifikation stammt, ist die Quelle vermerkt. Die Definitionen sind als Beschaffungs-Orientierung gedacht und ersetzen die maßgeblichen Begriffsdefinitionen in den zugrunde liegenden Normen oder Hersteller-Unterlagen nicht.

Active Damping. Herstellerbegriff (Synapticon, 2026): die kontrollierte elektromagnetische Bremswirkung, die durch Active Short Circuit auf Gelenkebene erzeugt wird. Kein harmonisierter Normbegriff. In HU-RSC als Aktor-Komponente eines Safe-State-Mechanismus für humanoide Bauformen verwendet.

Active Short Circuit (ASC). Herstellerbegriff (Synapticon, 2026): eine Aktor-Funktion, die bei Fehlererkennung die Motorwicklungen elektronisch kurzschließt und so eine kontrollierte elektromagnetische Bremswirkung erzeugt. Baustein für Safe Guided Falling.

AI Behavioural Safety. Herstellerbegriff (Synapticon, 2026): Sicherheitsarchitektur unter Verwendung multimodaler KI-Foundation-Models, die auf Internetdaten vortrainiert und für robotik-spezifische Kontexte nachtrainiert sind, um Gefahr über Geometrie hinaus semantisch zu verstehen. Noch kein harmonisierter Normbegriff. Britische Schreibweise „Behavioural“ durchgängig in diesem Papier; entspricht US-„Behavioral Safety“.

Backdrivability. Mechanische Eigenschaft eines Aktors, bei der eine externe Kraft den Abtrieb bewegen kann und so Aufprallenergie durch kontrollierte Nachgiebigkeit absorbiert. Relevant für humanoide Gelenke unter Sturz- oder Stolperszenarien.

Defense-in-depth. Architektonisches Prinzip: Sicherheit ab Tier 3 aufwärts beruht auf der geschichteten Kombination von Maßnahmen (Umgebungstrennung, sensorbasierte Erkennung, Software-Grenzen, organisatorische Abläufe) anstelle einer Einzelmaßnahme.

FSoE (Fail-Safe over EtherCAT). Sicherheitsbewertetes industrielles Busprotokoll, das Safe Process Data (Safe Position, Safe Velocity etc.) mit Integritätsschutz auf Protokollebene liefert. Beispielhafter Anker für die Mindestkopplung HU-RSC × HU-RAC ab Tier 4.

Humanoider Roboter. Ein Robotik-System mit anthropomorpher Morphologie (Oberkörper und zwei Arme; zwei Beine oder andere geeignete Fortbewegung), mit Umfelderkennung, vorgesehen zur Ausführung für Menschen konzipierter Aufgaben.

Humanoides Robotersystem. Die vollständige einsetzbare Einheit, bestehend aus mindestens einem humanoiden Roboter, Endeffektoren oder Werkzeugen, Werkstücken, peripheren Komponenten und Ladeinfrastruktur. Sicherheitseinrichtungen und -maßnahmen sind notwendige systemseitige Elemente.

Inverted-pendulum problem. Die dynamische Instabilität eines humanoiden Roboters bei Energieabschaltung: Klassisches Safe Torque Off erzeugt keinen sicheren Zustand, sondern einen unkontrollierten Sturz. Die Mitigation erfordert Active Damping und Safe Guided Falling-Routinen.

Power and Force Limiting (PFL). Kollaborative Betriebsart nach ISO 10218-2:2025 (vormals ISO/TS 15066), bei der physischer Kontakt zwischen Roboter und Bediener unter kontrollierten Kraft- und Druckschwellen zulässig ist.

Safe Guided Falling (SGF). Herstellerbegriff (Synapticon, 2026): ein kontrollierter Kollaps eines humanoiden Roboters bei Fehlererkennung, der Active Damping anstelle von Safe Torque Off nutzt, um Aufprallenergie zu reduzieren und sowohl Hardware als auch nahestehende Personen zu schützen. Noch kein harmonisierter Normbegriff.

Safe Limited Position. Zertifizierte Sicherheitsfunktion (ISO 13849-1), die Bewegung auf ein definiertes Positionsfenster begrenzt.

Safe Limited Speed (SLS). Zertifizierte Sicherheitsfunktion (ISO 13849-1), die Geschwindigkeit unter eine definierte Schwelle begrenzt; auf Antriebsebene überwacht.

Safe Limited Torque (SLT). Zertifizierte Sicherheitsfunktion, die das Drehmomentausgangsverhalten unter eine definierte Schwelle begrenzt.

Safe Motion Monitoring (SMM). Familie zertifizierter Sicherheitsfunktionen, die Bewegungsparameter (Position, Geschwindigkeit, Beschleunigung) gegen definierte Grenzen überwacht.

Safe State. Ein Zustand, in dem die sicherheitsrelevante Gefährdung auf ein akzeptables Niveau reduziert ist. Bei den meisten ortsfesten Robotern ist dies ein Stopp; bei humanoiden Robotern erfordert es kombiniertes Active Damping und Safe Guided Falling.

Safe Torque Off (STO). Zertifizierte Sicherheitsfunktion (ISO 13849-1, IEC 61800-5-2), die drehmomenterzeugende Energie vom Motor entfernt. Ausreichend als Safe State für ortsfeste Roboter; nicht ausreichend für humanoide Bauformen (siehe Safe State).

Speed and Separation Monitoring (SSM). Kollaborative Betriebsart nach ISO 10218-2:2025: kontinuierliche Überwachung des Abstands zwischen Roboter und Bediener mit Geschwindigkeitsreduktion oder Stopp bei Annäherung.

Wesentliche Veränderung (MR 2023/1230). Eine Veränderung einer in Verkehr gebrachten Maschine, die eine neue Konformitätsbewertung auslösen kann, einschließlich Software-Updates, die sicherheitsrelevantes oder funktionales Verhalten verändern. Die detaillierte Auslegung wird derzeit durch die Kommission weiterentwickelt.

Transienter vs. quasi-statischer Kontakt. ISO/TS 15066:2016 (nun ISO 10218-2:2025) unterscheidet transiente (frei zurückfedernde) und quasi-statische (eingeklemmt-statische) Kontaktszenarien, mit jeweils eigenen Kraft- und Druckschwellen. Die Definitionen enthalten anerkannte Auslegungs-Ambiguitäten (Kirschner et al. 2022); Risikobeurteilungen sollten erklären, welche Auslegung angewendet wurde.

14 Anhang — Referenzen

Fraunhofer IPA, Leitfaden Sicherheit Humanoider Roboter, Stuttgart, 25. Oktober 2025.

Fraunhofer IPA, Leitfaden Wirtschaftlichkeit Humanoider Roboter, Stuttgart, 2025.

Synapticon GmbH, Powering the Humanoid Revolution — High-Dynamic, Safety-Rated Actuation for Unstructured Environments (White Paper), 23. Januar 2026.

Klindt, T. (Noerr), Humanoide Roboter: Diese Regeln gelten in Europa, ingenieur.de, 4. Mai 2026.

Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery (Machinery Regulation), OJ L 165, 29.6.2023, p. 1. Berichtigung: OJ L 169, 4.7.2023, p. 51 (korrigiertes Anwendungsdatum 20. Januar 2027).

Europäische Kommission, Vorschlag für ein Digital Omnibus on AI vom 19. November 2025, sowie Verhandlungspositionen von Rat und Parlament im Frühjahr 2026 (Stand zum Redaktionszeitpunkt: noch nicht förmlich angenommen).

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), OJ L of 12.7.2024.

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act), OJ L of 20.11.2024.

Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products (Product Liability Directive), OJ L of 18.11.2024.

Directive 2014/53/EU on radio equipment (Radio Equipment Directive), OJ L 153, 22.5.2014, p. 62.

Kirschner, R. J., Mansfeld, N., Abdolshah, S., et al., ISO/TS 15066: How Different Interpretations Affect Risk Assessment, arXiv:2203.02706, 2022.

Fischer, C., Neuhold, M., Steiner, M., et al., Collision Tests in Human-Robot Collaboration, IEEE Access 11, 118395–118413, 2023.

FEV Consulting GmbH, Humanoid robots — Potential or hype for automotive suppliers? (Insights), Q3 2025, 14 Seiten.

Behrens, R., et al., A Statistical Model to Determine Biomechanical Limits for Physically Safe Interactions With Collaborative Robots, Frontiers in Robotics and AI, 2022.

Behrens, R., et al., A Revised Framework for Managing the Complexity of Contact Hazards in Collaborative Robotics, 2021 IEEE International Conference on Intelligence and Safety for Robotics (ISR), 2021.

Fischer, C., et al., Personalized Safety: Considering the Worker's Anthropometry in Safety Evaluation of Human-Robot Collaboration, 2024.

Li, J., et al., AttackVLA: Benchmarking Adversarial and Backdoor Attacks on Vision-Language-Action Models, arXiv preprint, 2025.

Morandini, S., et al., Collaborative Robots Adapting Their Behavior Based on Workers' Psychological States: A Systematic Scoping Review, Human Behavior and Emerging Technologies, 2025.

Rustler, L., et al., Adaptive Electronic Skin Sensitivity for Safe Human-Robot Interaction, 2024 IEEE-RAS 23rd International Conference on Humanoid Robots (Humanoids), 2024.

Svarný, P., et al., 3D Collision-Force-Map for Safe Human-Robot Collaboration, 2021 IEEE International Conference on Robotics and Automation (ICRA), 2020.

Zhang, B., et al., SafeVLA: Towards Safety Alignment of Vision-Language-Action Model via Safe Reinforcement Learning, arXiv preprint, 2025.