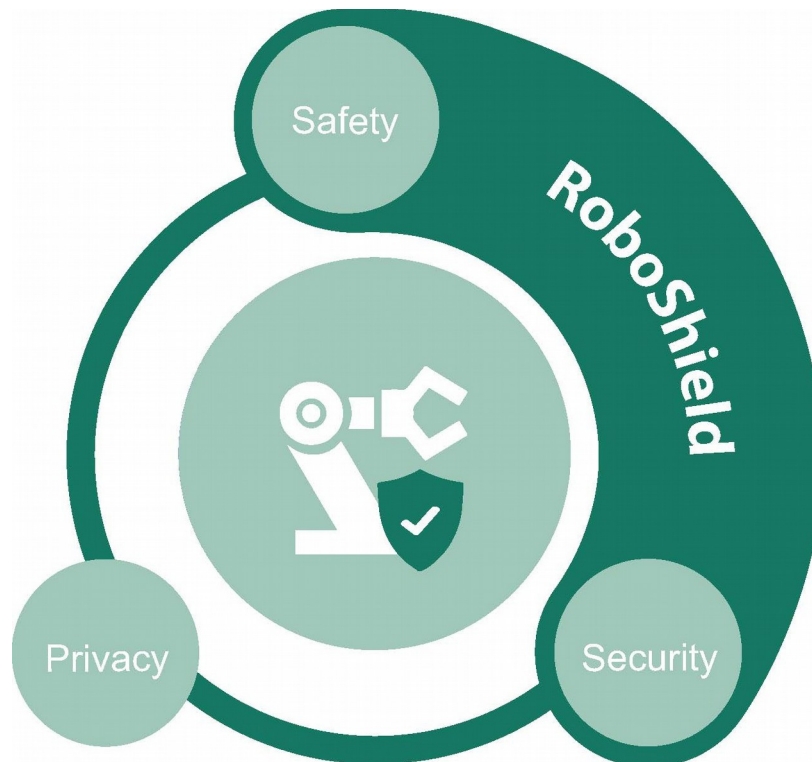


Praktische Empfehlungen und Beispiele zur Durchführung einer Risikobeurteilung

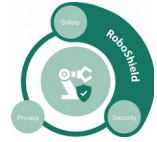
entstanden im Rahmen eines
RoboShield-QuickChecks



Durchgeführt von:

Dr.-Ing. Christoph Ledermann,
M. Sc. Tom Huck

Karlsruher Institut für Technologie (KIT)
Institut für Anthropomatik und Robotik –
Intelligente Prozessautomation und Robotik (IAR-IPR)

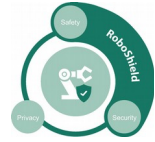


Haftungsausschluss & Ziel des Dokuments

Das vorliegende Dokument dient lediglich zur Orientierung sowie zu Informationszwecken und soll einen Einblick in das Vorgehen bei der Risikobeurteilung liefern. Es stellt keine Grundlage für die tatsächliche Durchführung der Risikobeurteilung oder CE-Kennzeichnung dar. Enthaltene Informationen wurden sorgfältig recherchiert, es besteht jedoch weder ein Anspruch auf Korrektheit noch auf Vollständigkeit. Zu Teilen enthält das Dokument Interpretationen der Anforderungen aus Normen durch die Autoren. Es wird keinerlei Haftung für Schäden und jedwede weitere Folgen, die sich aus der Verwendung dieses Dokuments ergeben, übernommen. Die alleinige Grundlage für die Durchführung der Risikobeurteilung und die CE-Kennzeichnung eines Produkts stellen die jeweils geltenden gesetzlichen Vorschriften, insbesondere das Produktsicherheitsgesetz und die EU-Maschinenrichtlinie, sowie die gegebenenfalls hierzu harmonisierte Normen dar.

Nennung von Firmen und Produkten

Im Rahmen des Dokuments werden verschiedene Firmen und teilweise durch sie vermarktete Produkte aufgeführt. Diese dienen lediglich als Beispiele und zur Veranschaulichung und sollen keine Empfehlung darstellen. Die Erstellung dieses Dokuments wurde durch genannte Firmen nicht finanziell unterstützt.



1. Einführung

Im Rahmen des Forschungsprojekts “RoboShield” hat das KIT, Institut für Anthropomatik und Robotik/Intelligente Prozessautomation und Robotik (IAR-IPR) am Beispiel einer Risikobeurteilung der ESSERT GmbH praxisnahe Beispiele und Empfehlungen für die Durchführung der Risikobeurteilung zusammengestellt.

Für Risikobeurteilungen im Maschinenbau bzw. in der Automatisierungstechnik gelten im Wesentlichen die Anforderungen der EU-Maschinenrichtlinie und der harmonisierten Normen, insbesondere der Norm ISO 12100. Das vorliegende Dokument soll einen ersten Einstieg in die Materie bieten, praxisnahe Hinweise geben und dabei helfen, einige häufig gemachte Fehler zu vermeiden. Es kann aber die Lektüre der Maschinenrichtlinie und der Normen nicht ersetzen.

Der Anwendungsfall, aus dem dieses Dokument entstanden ist, stammt von einer Roboter-Applikation. Einige Aspekte aus diesem Dokument beziehen sich speziell auf diesen Anwendungsfall. Die daraus abgeleiteten Empfehlungen sind jedoch allgemeingültig und können auf andere Anwendungsfälle übertragen werden.

2. Normative Grundlagen

Folgende Normen kamen bei der von uns betrachteten Risikobeurteilung zur Anwendung:

- ISO 12100: Sicherheit von Maschinen – allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung
- ISO/TR 14121-2: Sicherheit von Maschinen – Risikobeurteilung – Teil 2: Praktischer Leitfaden und Verfahrensbeispiele
- ISO 13849-1: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze
- ISO 13850: Sicherheit von Maschinen – Not-Halt – Gestaltungsleitsätze
- ISO 13855: Sicherheit von Maschinen – Anordnung von Schutzeinrichtungen im Hinblick auf Annäherungsgeschwindigkeiten von Körperteilen

Empfehlung 1: Verwandte Normen

Den Erstellern von Risikobeurteilungen wird empfohlen, soweit anwendungsrelevant, sich ergänzend mit folgenden verwandten Normen vertraut zu machen:

- ISO 10218: Industrieroboter – Sicherheitsanforderungen – Teil 2: Robotersysteme und Integration
- ISO 13857: Sicherheit von Maschinen – Sicherheitsabstände gegen das Erreichen von Gefährdungsbereichen mit den oberen und unteren Gliedmaßen
- ISO/TS 15066: Roboter und Robotikgeräte – Kollaborierende Roboter
- ISO 13854: Sicherheit von Maschinen – Mindestabstände zur Vermeidung des Quetschens von Körperteilen



3. Allgemeine Empfehlungen zur Risikobeurteilung

Die Risikobeurteilung ist ein iterativer Prozess, zu dem laut ISO 12100, Kapitel 4, folgende Schritte gehören:

- a) Festlegen der Grenzen der Maschine
- b) Identifizieren von Gefährdungen/Gefährdungssituationen
- c) Einschätzen des Risikos für die jeweilige Gefährdung/Gefährdungssituation
- d) Risikobewertung, Entscheidung über Notwendigkeit zur Risikominderung
- e) Festlegen von Maßnahmen zur Risikominderung

Danach ist eine erneute Risikobeurteilung durchzuführen, um sicherzustellen, dass die Risiken tatsächlich reduziert wurden und dass durch die ergriffenen Maßnahmen keine neuen Risiken dazugekommen sind. Die Risikobeurteilung ist also ein **iterativer Prozess**. Solange noch nicht die endgültige Form erreicht ist, wird die zugehörige Dokumentation also mit jedem Iterationsschritt **ständigen Änderungen unterworfen** sein.

Empfehlung 2: Versionierung, Änderungshistorie

Aufgrund des iterativen Charakters kann es hilfreich sein, die Risikobeurteilung intern als "lebendes Dokument" anzulegen (z.B. mit einem Versionsverwaltungs-Tool) und eine entsprechende Änderungshistorie zu führen. Soll das Produkt auf den Markt gebracht werden, kann aus diesem Dokument dann im Rahmen einer Review eine marktreife Variante abgeleitet werden. Im Idealfall sollte der Reviewer eine fachkundige Person sein, die jedoch nicht an der Erstellung der Risikobeurteilung beteiligt war. Zur Bezeichnung bietet sich folgende Konvention an:

0.x: Vor erster Review

1.0 Erste Review – Markteintritt erste Produktgeneration

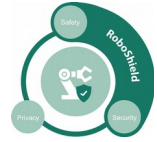
1.x Änderungen nach erster Review

2.0 Zweite Review – Markteintritt zweite Produktgeneration

2.x usw...

Anmerkung: Die Risikobeurteilung muss dem Kunden nicht zur Verfügung gestellt werden. Dies wird aber von vielen Kunden gewünscht und kann dabei helfen, das Vertrauen des Kunden in die CE-Konformität zu stärken.

Eine besondere Herausforderung ist die Identifizierung von Gefährdungen (s. Schritt b) oben). Während einige Gefährdungen aus der Erfahrung heraus oft direkt erkannt werden können, gibt es mitunter auch "**versteckte**" **Gefährdungen**, die nicht offensichtlich sind. Ein **strukturiertes Vorgehen** kann dabei helfen, möglichst alle Gefährdungen aufzudecken. Eine Garantie, dass alle Gefährdungen aufgedeckt werden, gibt es dabei jedoch nicht.



Empfehlung 3: Vorgehen zur Gefährdungsidentifikation

Für eine möglichst umfassende und **strukturierte Identifikation** der Gefährdungen kann wie folgt vorgegangen werden:

- Definition aller möglichen **Maschinenzustände** für die jeweiligen **Lebensphase** (Kann sinnvollerweise mit Schritt a) "Festlegen der Grenzen der Maschine" kombiniert werden).
- **Gefährdungs-Checklisten** für jede Lebensphase durchgehen und überlegen, welche der Gefährdungen in der jeweiligen Lebensphase bzw. dem jeweiligen Maschinenzustand relevant sind. Geeignete Gefährdungs-Checklisten können gefunden werden in:
 - ISO 12100, Anhang B (allgemeine Gefährdungen)
 - ISO 10218-2, Anhang A (speziell auf Roboter-Applikationen bezogene Gefährdungen)
- Brainstorming/Expertengespräch/sonstige Maßnahmen, um Gefährdungen aufzudecken, die ggf. nicht in den Checklisten repräsentiert werden (s. ISO/TR 14121-2, Kap. 5.3.4).

4. Empfehlungen zu speziellen Aspekten der Risikobeurteilung

4.1 Definition der Grenzen der Maschine

Wie bereits in Empfehlung 3 erwähnt, ist eine möglichst genaue Definition der Grenzen der Maschine wichtig für eine zuverlässige Identifikation möglicher Gefährdungen. Dabei sollten insbesondere die folgenden Aspekte beachtet werden:

- **Betriebsarten:** Eine möglichst genaue Definition der Betriebsarten ist hilfreich, weil sie die Identifikation der Gefährdungen erleichtert (siehe auch Empfehlung 3). Bei der Definition der Betriebsarten sollte insbesondere definiert werden, in welchem Zustand sich die Maschine jeweils befindet (z.B.: Wann sind Türen geöffnet, Abdeckungen abgenommen, befindet sich der Roboter im Automatikbetrieb oder ist er stillgesetzt, etc.) und welche Tätigkeiten vom Bediener ausgeführt werden (z.B. Eingreifen nur im Fehlerfall, ständiges Eingreifen erforderlich durch Arbeitsaufgabe, Betreten/Hineinkriechen in die Maschine für Wartungs- oder Reinigungsaufgaben, etc.). Aus all diesen Definitionen können später direkte Aussagen für die Risikobeurteilung abgeleitet werden.
- **Lebensphasen:** Obige Erklärung gilt sinngemäß auch für die Definition der Lebensphasen der Maschine. Besondere Aufmerksamkeit sollte Lebensphasen gelten, in denen Sicherheitsmaßnahmen (noch) nicht vollständig verfügbar sind, deaktiviert werden müssen oder Bereiche der Maschine zugänglich gemacht werden müssen, die im regulären Betrieb nicht zugänglich sind. Beispiele für relevante Lebensphasen sind Inbetriebnahme, Wartung, Behebung von Störungen etc.
- **Vernünftigerweise vorhersehbare Fehlanwendung:** Auch hier besteht eine direkte Verbindung zur Identifikation von Gefährdungen. Vorhersehbare Fehlanwendungen können bei der Risikobeurteilung zumeist direkt in Gefährdungssituationen übersetzt werden. *Anmerkung:* Hier handelt es sich um Fehlanwendungen, die im Zusammenhang mit der Applikation/Arbeitsaufgabe stehen. Dazu gehören auch Gefährdungssituationen, die entstehen, wenn das Bedienpersonal aus betrieblichen Gründen Sicherheitsregeln missachtet oder Schutzmaßnahmen außer Kraft setzt (z.B. aufgrund mangelnder Einweisung oder um die Arbeit zu beschleunigen). Eine mutwillige, gezielte Herbeiführung von Unfällen (z.B. durch Sabotage) muss jedoch im Normalfall nicht berücksichtigt werden.



Empfehlung 4: Grenzen der Maschine

Bei der Definition der Grenzen der Maschine sollte besonderes Augenmerk auf die **genaue Definition der Betriebsarten, Lebensphasen und vernünftigerweise vorhersehbaren Fehlanwendungen** gelegt werden. Diese sollten möglichst detaillierte Angaben (Zustand der Maschine, Tätigkeiten, Beschreibung der Fehlanwendung etc.) enthalten, da daraus meist **direkt Gefährdungsszenarien für die Risikobeurteilung konstruiert** werden können (siehe auch Empfehlung 3). Somit wird der Aufwand bei der Gefährdungsidentifikation verringert und die Zuverlässigkeit erhöht.

4.2 Beschreibung der Gefährdungsszenarien

Bei Verwendung der Checkliste aus ISO 12100 (Anhang B) ist zu beachten, dass die dort aufgeführten Gefährdungen sehr allgemein gehalten sind. Deswegen ist es wichtig, klar zu beschreiben, welche konkrete Gefährdungssituation jeweils gemeint ist. Hierzu zwei Beispiele:

“Während des Betriebes der Anlage (Einrichten, Automatik, Instandhaltung) kommt es vermehrt zu Scher-/Quetschgefährdung durch Maschinenteile oder Werkstücke”

→ Hier wird nicht klar, wo genau an der Maschine die vermeintliche Scher/Quetschgefährdung auftritt. Ebenso ist unklar, welche Handlung die Gefährdung herbeiführt oder welche Körperteile betroffen sind.

“Während des Betriebes der Anlage (Einrichten, Automatik, Instandhaltung) kommt es am Einlauf- und Auslaufbandes zu Scher-/Stoß-/ Quetschgefährdung durch Maschinenteile oder Werkstücke”

→ Hier ist klar beschrieben, wo an der Maschine die Gefährdung auftritt. Die Frage nach der die Gefährdung auslösenden Handlung beantwortet sich hier aufgrund der beschriebenen Situation von selbst (hineingreifen). Für die Risikobewertung, genauer gesagt die Bewertung der möglichen Verletzungsschwere, wäre es noch hilfreich, zu beschreiben, welche Körperteile betroffen sind (vermutlich: Hand/Arm).

Empfehlung 5: Beschreibung von Gefährdungssituationen

Gefährdungssituationen sollten so beschrieben werden, dass klar wird, **wo an der Maschine bei welcher Handlung** die Gefährdung auftritt und (falls zutreffend) **welche Körperteile** betroffen sind. Dies erleichtert sowohl die Risikobewertung (z.B. die Einschätzung der Verletzungsschwere) und die Risikominderung (z.B. Entscheidung, ob konstruktive Lösung möglich).

4.3 Klassifikation und Beschreibung der Schutzmaßnahmen

Bei der Risikominderung wird zwischen Maßnahmen zur **inhärent sicheren Konstruktion** (kurz: konstruktive Maßnahme), **technischen Schutzmaßnahmen** und **Benutzerinformationen** unterschieden. Hierbei hat die inhärent sichere Konstruktion Vorrang, da nur diese Gefährdungen vollständig beseitigen kann. Wenn eine vollständige Beseitigung der Gefährdung nicht möglich ist, sollten technische Schutzmaßnahmen zur Risikominderung verwendet werden (dazu gehören beispielsweise Sicherheitssensoren und -steuerungen, die gefahrbringende Teile der Anlage stillsetzen).



Benutzerinformationen können diese Maßnahmen ergänzen, sollten jedoch nicht als alleinige Maßnahme zur Risikominderung verwendet werden. Im Folgenden einige Beispiele für die Klassifizierung der Maßnahmen:

“Robotergreifer [...] muss so konstruiert werden, dass dieser keine scharfe Kanten bzw. Abscherungen zur Folge hat” → Hierbei handelt es sich um eine konstruktive Maßnahme.

“Befestigung der Schutzeinrichtungen wird so ausgeführt, dass nicht mit einfachen Mitteln die Schutzeinrichtungen demontiert werden können” → Hierbei handelt es sich ebenfalls um eine konstruktive Maßnahme.

„Der Roboter ist vom Bediener durch einen Lichtvorhang getrennt. Bei Unterbrechung des Lichtvorhangs wird der Roboter stillgesetzt“ → Hierbei handelt es sich um eine technische Maßnahme.

“Tragen von PSA” → Hierbei handelt es sich nicht um eine konstruktive Maßnahme, sondern eine Benutzerinformation (Hinweis auf Tragen von PSA durch Piktogramme, Betriebsanleitung, etc.).

Empfehlung 6: Klassifikation der Schutzmaßnahmen

Schutzmaßnahmen sollten nach ISO 12100 (Abschnitt 3.20 bis 3.22) wie folgt klassifiziert werden:

- **Konstruktiv:** Beseitigt Gefährdungen oder mindert Risiken, indem Konstruktions- oder Betriebseigenschaften der Maschine verändert werden (ohne Anwendung von trennenden/ nicht-trennenden Schutzeinrichtungen)
- **Technisch:** Einsatz von Schutzeinrichtungen, wenn Risiken nicht durch konstruktive Maßnahmen beseitigt werden können (falls doch, hat die konstruktive Maßnahme Vorrang).
- **Benutzerinformation:** Schutzmaßnahme durch Kommunikation/Weitergabe von Informationen an Benutzer.

Die Beschreibung der Schutzmaßnahmen sollte möglichst spezifisch sein, wie z.B. in diesem Beispiel:

“Das Umfeld des Roboters wird durch einen Laserscanner abgesichert. Wird der Sicherheitsbereich betreten, so wird der Roboter in einen sicherheitsbewerteten überwachten Halt versetzt. Der Sicherheitsbereich ist nach ISO 13855 bemessen.”

Empfehlung 7: Beschreibung von Schutzmaßnahmen

Schutzmaßnahmen sollten so beschrieben werden, dass eine **konkrete Maßnahme** ersichtlich ist. Insbesondere bei steuerungstechnischen Maßnahmen sollte klar ersichtlich sein, welche **konkrete Sicherheitsfunktion** implementiert ist (z.B. nach dem Muster *“WENN Situation X, DANN wird Sicherheitsfunktion Y ausgeführt”*). Hilfreich ist auch der Verweis auf entsprechende B- oder C-Normen, welche die Anforderungen an die Schutzmaßnahme ausdetaillieren.



4.4 Definition des Performance Levels

Bei steuerungstechnischen Sicherheitsfunktionen ist die Angabe des Performance Levels (PL) erforderlich. Das erforderliche PL wird nach ISO 13849 bestimmt. Software-Tools wie SISTEMA können dabei helfen, zu verifizieren, ob das geforderte Performance Level tatsächlich erreicht wird. Für Sicherheitsfunktionen im Zusammenhang mit Robotern, d.h. solche, die Roboter-intern sind (wie z.B. sicherheitsbewerteter überwachter Halt) und solche, die auf den Roboter direkt einwirken (wie z.B. Laserscanner, Türüberwachung, etc.) fordert ISO 10218 jedoch Performance Level d. Da ISO 10218 eine C-Norm speziell für Roboter ist, hat sie in diesem Fall Vorrang gegenüber der (allgemeineren) B-Norm ISO 13849.

Empfehlung 8: Performance Level von Roboter-bezogenen Sicherheitsfunktionen

Für Sicherheitsfunktionen im Zusammenhang mit dem Roboter entfällt die Berechnung und es kann – mit entsprechendem Verweis auf ISO 10218 – PL d als erforderlich angenommen werden.

Anmerkung: Dies gilt nicht für sonstige Sicherheitsfunktionen, die nicht mit dem Roboter in Zusammenhang stehen. Hier erfolgt weiterhin die Berechnung nach ISO 13849.

Außerdem in der Dokumentation bei der Angabe von Performance Levels klar ersichtlich sein, an welcher Stelle das erforderliche und das tatsächlich erreichte Performance Level angegeben werden, da die Angaben sonst widersprüchlich erscheinen können.

5. Software-Tools zur Risikobeurteilung

Bei häufiger Erstellung und/oder großem Umfang von Risikobeurteilungen kann es unter Umständen hilfreich sein, kommerzielle Software-Tools einzusetzen. An dieser Stelle soll lediglich darauf hingewiesen werden, dass entsprechende Produkte am Markt verfügbar sind. Eine Empfehlung wird nicht ausgesprochen.

Einige Beispiele für verfügbare Produkte (ohne Anspruch auf Vollständigkeit):

- Safexpert
- WEKA Manager CE
- CE-CON
- CE-Safe
- Quentic

Es ist jedoch auch möglich, die Risikobeurteilung ohne spezielle Software-Tools durchzuführen. In diesem Fall können Office-Programme, wie z.B. Microsoft Word oder Excel, zur Dokumentation verwendet werden. Im Internet sind dazu kostenlose Word- und Excel vorlagen erhältlich, wie beispielsweise unter folgendem Link:

<http://www.maschinenrichtlinie.de/ce-tools/risikobeurteilung-maschinenrichtlinie-200642eg/>

Weiterhin können – soweit verfügbar – CAD-Daten, Simulationsmodelle oder digitale Zwillinge wertvolle Hilfen in der Risikobeurteilung sein, z.B. zur Visualisierung des Anlagenlayouts, zur Visualisierung von Sicherheitszonen oder zur Überprüfung von Sicherheitsabständen. Es ist daher empfehlenswert, zu überprüfen, welche Daten und Modelle zu welchem Zeitpunkt im Entwicklungsprozess zur Verfügung stehen, und ob diese in der Risikobeurteilung genutzt werden könnten.