

Technisches White Paper

Safety Software | Aktualizacja: 18.12.2025 | <https://safetysoftware.eu>

Technisches White Paper

Abstract

Die Norm ISO 12100:2010 – *Safety of machinery – General principles for design – Risk assessment and risk reduction* legt die allgemeinen Grundsätze für die sichere Konstruktion von Maschinen sowie den Rahmen des Prozesses zur Risikobeurteilung und Risikominderung fest.

Diese Norm schreibt weder ein einheitliches Datenmodell noch eine bestimmte relationale Struktur vor, sondern definiert Begriffe, Identifikationsbereiche und Prozessschritte.

Dieses Dokument beschreibt die Implementierung eines Prozesses, der dem **wortlautgetreuen Inhalt** der ISO 12100:2010 entspricht, **ohne Einführung nicht-normativer Begriffe, ohne Etablierung von Beziehungen, die von der Norm nicht definiert werden**, sowie **ohne logische Vervollständigung dort, wo die Norm bewusst Flexibilität zulässt**.

1. Anwendungsbereich und normativer Ansatz

Dieses Dokument bezieht sich ausschließlich auf die Norm ISO 12100:2010.

Es verwendet keine nationalen Verweise und keine Interpretationen aus anderen Normen, Richtlinien oder Branchenpraktiken.

Der gewählte Ansatz:

- basiert ausschließlich auf den Definitionen und Festlegungen der Norm,
- unterscheidet zwischen normativen Anforderungen und methodischen Lösungen,
- schreibt der Norm keine Intentionen oder Strukturen zu, die sie nicht ausdrücklich enthält.

2. Im Prozess verwendete normative Begriffe

Das System operiert ausschließlich mit Begriffen, die in **Kapitel 3 der ISO 12100:2010** definiert sind, insbesondere:

- **hazard (Gefährdung)** – potenzielle Quelle eines Schadens (3.6),
- **hazardous situation (Gefährdungssituation)** – Situation, in der eine Person mindestens einer Gefährdung ausgesetzt ist (3.10),
- **hazardous event (gefährliches Ereignis)** – Ereignis, das einen Schaden verursachen kann (3.9),
- **harm (Schaden)** (3.5),
- **risk (Risiko)** – Kombination aus der Wahrscheinlichkeit des Auftretens eines Schadens und der Schwere dieses Schadens (3.12),
- **task (Aufgabe)** – bestimmte Handlung an oder in der Nähe einer Maschine, die während ihres Lebenszyklus durchgeführt wird (3.25).

Es werden keine Ersatzbegriffe und keine in der Norm nicht vorhandenen Sammelbegriffe eingeführt.

3. Identifikation gemäß Abschnitt 5.4

Gemäß Abschnitt **5.4 Hazard identification** fordert die Norm die Identifikation von:

- **hazards,**
- **hazardous situations,**
- **and/or hazardous events.**

Die Verwendung der Konjunktion **and/or** bedeutet, dass:

- Gefährdungen,

- Gefährdungssituationen,
- gefährliche Ereignisse

gleichwertige Identifikationsobjekte sind.

Die Norm:

- legt keine Hierarchie zwischen diesen Objekten fest,
- definiert keine Über- oder Unterordnungsbeziehungen,
- verlangt nicht das gleichzeitige Vorhandensein aller drei Kategorien.

Die Identifikation eines gefährlichen Ereignisses ist nicht verpflichtend und hängt vom Charakter des analysierten Falls ab.

4. Aufgaben und Maschinenoperationen

In Abschnitt 5.4 weist die Norm auf die Notwendigkeit hin:

- die **operations performed by the machine** zu bestimmen,
- die **tasks performed by humans** zu bestimmen.

Das bedeutet, dass:

- von der Maschine ausgeführte Operationen,
- vom Menschen ausgeführte Aufgaben

gleichwertige Analysebereiche im Identifikationsprozess darstellen.

Die Tatsache, dass der Begriff **task** eine formale Definition in Kapitel 3 besitzt, während der Begriff **machine operation** keine eigenständige terminologische Definition hat, bedeutet keinen Unterschied in ihrer normativen Bedeutung. Es handelt sich um einen redaktionellen, nicht um einen inhaltlichen Unterschied.

Die Norm etabliert keine strukturelle Beziehung zwischen:

- Aufgabe,
- Maschinenoperation,
- Gefährdungssituation,
- gefährlichem Ereignis.

5. Fehlen normativer hierarchischer Beziehungen

ISO 12100:2010:

- definiert keine Sequenz vom Typ „Aufgabe → Situation → Ereignis“,
- legt nicht fest, dass ein gefährliches Ereignis aus einer Aufgabe resultiert,
- legt nicht fest, dass eine Gefährdungssituation ein gefährliches Ereignis enthält.

Jegliche Verknüpfungen zwischen diesen Elementen dürfen ausschließlich als **methodische Lösungen** zur Analyse und Dokumentation des Prozesses verwendet werden und haben keinen normativen Charakter.

6. Gefährliches Ereignis und sein Eintreten in der Risikoeinschätzung

6.1 Status des gefährlichen Ereignisses

Das **hazardous event** ist ein normativer Begriff, definiert in Abschnitt 3.9 der Norm. Es kann im Schritt 5.4 als eines der Identifikationsobjekte identifiziert werden.

Ein gefährliches Ereignis:

- ist kein Bestandteil der Risikodefinition,
- ist kein Element des Risikos,

- ist nicht in jeder Analyse erforderlich.

6.2 Definition des Risikos

Die Definition von **risk (3.12)** bestimmt Risiko als Kombination aus:

- der Wahrscheinlichkeit des Auftretens eines Schadens,
- der Schwere dieses Schadens.

Diese Definition enthält keinen Verweis auf ein gefährliches Ereignis.

6.3 Eintreten eines gefährlichen Ereignisses in Abschnitt 5.5.2

In Abschnitt **5.5.2 Elements of risk** gibt die Norm an, dass die Wahrscheinlichkeit eines Schadens unter anderem eine Funktion ist von:

- **exposure of persons to the hazard,**
- **occurrence of a hazardous event,**
- **possibility of avoiding or limiting the harm.**

In diesem Zusammenhang:

- bezieht sich die Norm ausschließlich auf das **Eintreten** eines gefährlichen Ereignisses,
- bezieht sie sich nicht auf das gefährliche Ereignis als eigenständiges Objekt.

Das Eintreten eines gefährlichen Ereignisses ist einer der möglichen Faktoren, die bei der Abschätzung der Schadenswahrscheinlichkeit gemäß Abschnitt 5.5.2 berücksichtigt werden.

7. Iterativität des Prozesses

Gemäß Abschnitt **5.6.1** ist der Prozess der Risikobeurteilung und Risikominderung iterativ.

Nach Anwendung von Schutzmaßnahmen ist jeweils zu überprüfen, ob:

- neue Gefährdungen entstanden sind,
- neue Gefährdungssituationen entstanden sind,
- neue gefährliche Ereignisse entstanden sind.

Die Norm beschränkt den Umfang der erneuten Identifikation nicht auf eine einzelne Objektart.

8. Dokumentation des Prozesses

Gemäß Kapitel 7 sollte die Dokumentation der Risikobeurteilung Folgendes umfassen:

- identifizierte Gefährdungen, Gefährdungssituationen und gefährliche Ereignisse,
- getroffene Annahmen,
- Ergebnisse der Risikoeinschätzung und Risikobewertung,
- angewandte Schutzmaßnahmen,
- Restrisiko,
- während des Prozesses entstandene Aufzeichnungen.

Die Norm schreibt weder eine Dokumentationsstruktur noch ein Datenmodell vor.

9. Schlussfolgerungen

Die dargestellte Implementierung:

- entspricht dem wortlautgetreuen Inhalt der ISO 12100:2010,
- führt keine nicht-normativen Begriffe ein,

- etabliert keine in der Norm nicht vorhandenen hierarchischen Beziehungen,
- trennt Identifikation von Risikoeinschätzung,
- behandelt das gefährliche Ereignis als normatives Objekt,
- berücksichtigt ausschließlich das **Eintreten** eines gefährlichen Ereignisses im Stadium der Risikoeinschätzung.

Es handelt sich um eine normkonforme Implementierung und nicht um eine Interpretation oder Vereinfachung der Norm.