Technical White Paper

Abstract

The standard **ISO 12100:2010 – Safety of machinery – General principles for design – Risk assessment and risk reduction** defines general principles for the design of safe machinery and establishes a framework for the process of risk assessment and risk reduction.
This standard **does not impose a single data model or a fixed relational structure**, but defines terms, scopes of identification and stages of the process.

This document describes an implementation that is **strictly consistent with the literal wording of ISO 12100:2010**, without introducing non-normative concepts, without establishing relations that are not defined by the standard, and without closing logical structures where the standard intentionally leaves flexibility.

1. Scope and normative approach

This document refers exclusively to **ISO 12100:2010**.
No national deviations, additional standards or industry-specific interpretations are applied.

The adopted approach:

- relies solely on the definitions and provisions of the standard,
- clearly distinguishes **normative requirements** from **methodological solutions**,
- does not attribute intentions or structures to the standard that are not explicitly stated.

2. Normative terms used in the process

The system operates exclusively on terms defined in Clause 3 of ISO 12100:2010, in particular:

- **hazard** – potential source of harm (3.6),
- **hazardous situation** – circumstance in which a person is exposed to at least one hazard (3.10),
- **hazardous event** – event that can cause harm (3.9),
- **harm** (3.5),
- **risk** – combination of the probability of occurrence of harm and the severity of that harm (3.12),
- **task** – specific activity performed by one or more persons on, or in the vicinity of, the machine during its life cycle (3.25).

No substitute terms or aggregated concepts not present in the standard are introduced.

3. Hazard identification in accordance with Clause 5.4

According to **Clause 5.4 Hazard identification**, the standard requires identification of:

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

The use of the conjunction **“and/or”** means that:

- hazards,

- hazardous situations,
- hazardous events

are **equivalent objects of identification**.

The standard:

- does not establish a hierarchy between these objects,
- does not define relations of subordination or dependency,
- does not require all three categories to be present simultaneously.

Identification of a hazardous event **is not mandatory** and depends on the nature of the assessed case.

4. Tasks and machine operations

In Clause 5.4, the standard requires:

- identification of **operations performed by the machine**,
- identification of **tasks performed by humans**.

This means that:

- machine operations,
- human tasks

constitute **two parallel areas of analysis** within the hazard identification process.

The fact that:

- the term *task* has a formal definition in Clause 3,

- while *machine operation* does not have a separate terminological definition,

does not imply a lower normative status of machine operations.
This is a redactional difference, not a substantive one.

The standard does not establish any structural relation between:

- task,
- machine operation,
- hazardous situation,
- hazardous event.

5. Absence of normative hierarchical relations

ISO 12100:2010:

- does not define sequences such as “task → hazardous situation → hazardous event”,
- does not state that a hazardous event results from a task,
- does not state that a hazardous situation contains a hazardous event.

Any relations between these elements may be applied **only as methodological support** for analysis and documentation, but **do not have normative character**.

6. Hazardous event and occurrence of a hazardous event in risk estimation

6.1 Status of a hazardous event

A hazardous event is a normative term defined in Clause 3.9 of the standard.
It may be identified at the hazard identification stage (Clause 5.4) as one of the possible objects of identification.

A hazardous event:

- is not an element of the definition of risk,
- is not a component of risk,
- is not required in every risk assessment.

6.2 Definition of risk

The definition of **risk** (3.12) describes risk as a combination of:

- the probability of occurrence of harm,
- the severity of that harm.

This definition **does not include any reference to a hazardous event**.

6.3 Occurrence of a hazardous event in Clause 5.5.2

In **Clause 5.5.2 Elements of risk**, the standard states that the probability of occurrence of harm is a function of, among others:

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

In this context, the standard:

- refers **exclusively to the occurrence of a hazardous event**,
- does not refer to the hazardous event as an object or entity.

The occurrence of a hazardous event is one of the possible factors considered when estimating the probability of harm, in accordance with Clause 5.5.2.

7. Iterative nature of the process

According to Clause 5.6.1, the process of risk assessment and risk reduction is iterative.
After the application of protective measures, it shall be verified whether:

- new hazards have been introduced,
- new hazardous situations have appeared,
- new hazardous events have occurred.

The standard does not limit the scope of re-identification to a single category of objects.

8. Documentation of the process

In accordance with Clause 7, documentation of the risk assessment and risk reduction process shall demonstrate:

- identified hazards, hazardous situations and hazardous events,
- assumptions made,
- results of risk estimation and risk evaluation,
- applied protective measures,
- residual risks,
- records generated during the process.

The standard does not prescribe a specific documentation structure or data model.

9. Conclusions

The implementation described:

- is consistent with the literal wording of ISO 12100:2010,
- does not introduce non-normative concepts,
- does not establish hierarchical relations not defined by the standard,
- clearly separates hazard identification from risk estimation,
- treats hazardous events as normative objects,
- considers only the **occurrence of hazardous events** at the risk estimation stage.

This is an implementation **compliant with the standard**, not an interpretation or simplification of it.