V - Risk assessment

A number of European Standards deal comprehensively with the categorization and evaluation of risk as part of the overall procedure for ensuring that machinery meets the essential health and safety requirements of applicable EC Directive(s). A risk assessment is a series of logical steps to enable the systematic examination of the hazards associated with machinery. Below we offer some advice to help you carry out a risk assessment procedure. **This advice is intended purely as a guideline, because individual circumstances will dictate different approaches.**

A machinery risk can be defined as the possible occurrence of a hazardous event that can cause injury to users and/or damage to their health. Risks fall into several categories:

- **Mechanical** (e.g. perforation, puncturing, severing, cutting, crushing, shock, etc.)
- **Electrical** (e.g. electrocution)
- **Physical-chemical** (e.g. contact with dangerous substances, burns, etc.)

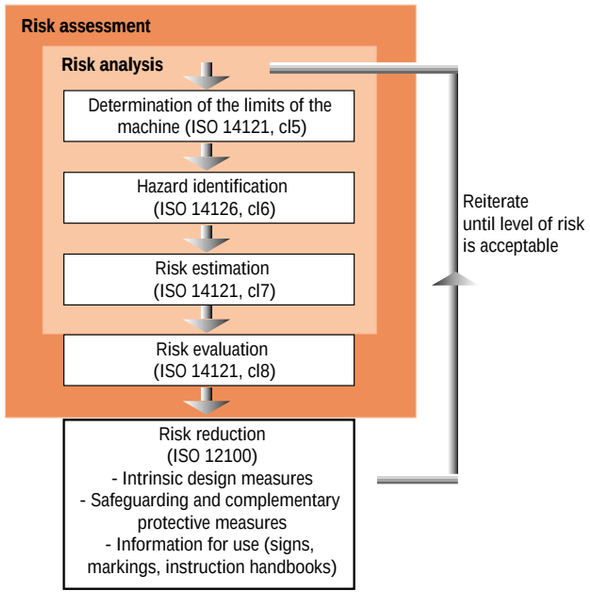


Diagram V.1

Annex A of EN 1050 gives more precise details on these phenomena.

The process of **Risk Assessment** is broken down into several stages (Ref Diagram V.1).

- Determination of the limits of the machinery, then,
- An analysis to identify potentially hazardous phenomena,
- Estimation of the degree of risk, followed by
- A risk evaluation, where existing safety measures are evaluated to determine whether they are adequate, or if additional measures are required.

This process is then followed by steps to **Reduce the Risk** if necessary. Additional safety measures, derived from the Risk Assessment, can be introduced and re-evaluated until they are considered satisfactory. It is important that you document each stage systematically.

To reduce or eliminate hazards or hazardous events, you must first assemble relevant information on the nature, design, life cycle and limits of your machinery, as well as a history of any accident or incidents, if possible. The absence of accident history, a small number of accidents or low severity of accidents should not be taken as an automatic presumption of a low risk. You must then implement a rigorous procedure to access the level of risk. There are several methods for doing this, for example:

- Ishikawa diagram
- “What if?” method and tree diagrams (per IEC 61026)
- Preliminary Hazards Analysis
- Failure modes and effect analysis (per IEC 60812)
- EN Standards approach (outlined below)

Risk assessment: one of the methods…

Type A Standards EN 1050 (Risk Assessment), EN 292 (Basic Principles, General Design Principles) and Type B Standard EN 954-1 (Safety related parts of control systems) are essential reading. They offer a succession of logical steps that help categorize and evaluate risk. EN 1050 and EN 954-1 offer a selection guide that defines the categories of safety equipment that are necessary to address the type of risk you assess.

Standard EN 954-1 describes these categories and highlights what risks they correspond to and their significance in terms of obligations.

Table V.1 summarizes Risk Categories, consequences of faults and control system requirements as per EN 954-1 and also Honeywell's interpretation of examples and techniques that address them.

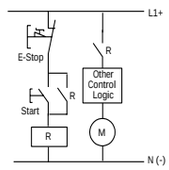
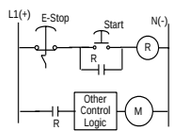
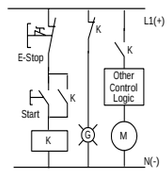
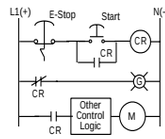
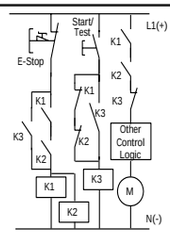
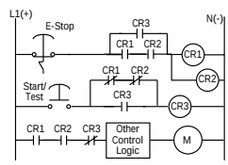
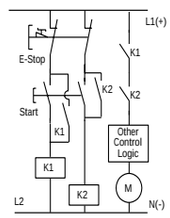
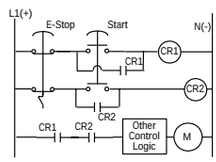
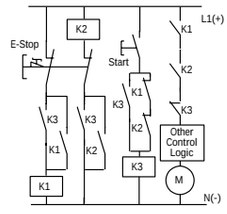
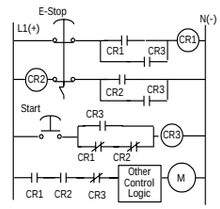
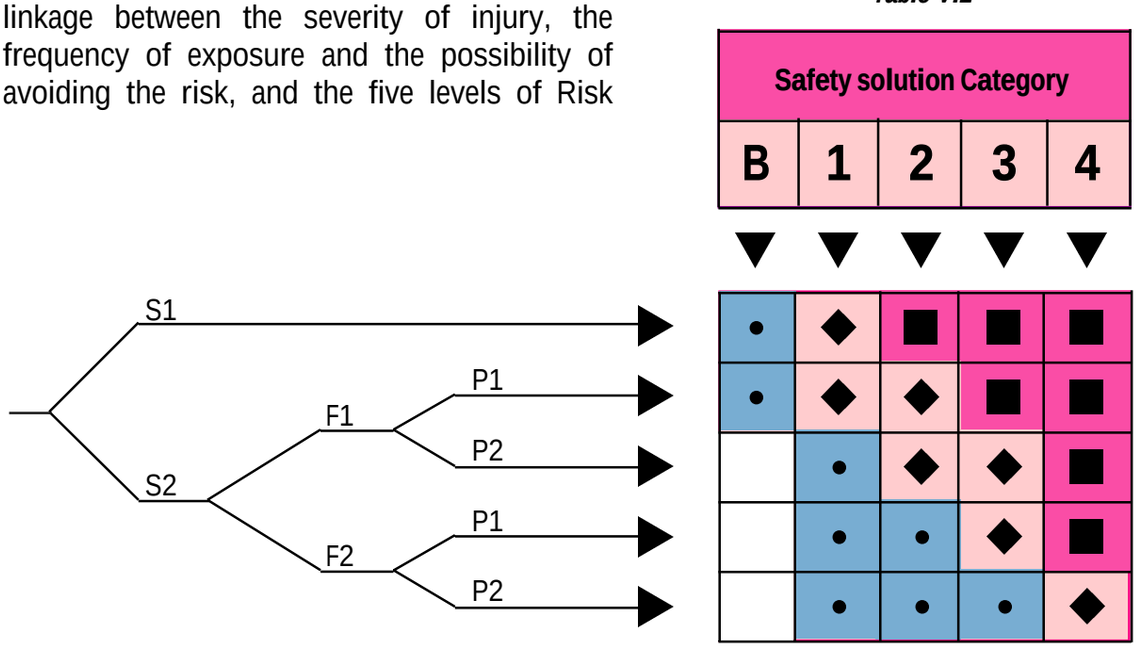
Categories	Consequences of faults	Requirements of the control system	Circuitry examples (not contractual) IEC symbols	Circuitry examples (not contractual) NEMA symbols	Techniques for circuitry Examples
B	Possibility of loss of safety function after a single fault	Equipment designed according to basic principles intended to ensure reliability			**Conventional relays**
1	Possibility of loss of safety function after a single fault	Design based on well tried components and principles			**Safety relay**; mechanically linked contacts (positive guided; reliability)
2	Possibility of loss of safety function if a fault appears between 2 verifications	The integrity of the safety is based upon a periodic test. A failure should be detected at the next coming test			**Safety relays**; **cyclical test**
3	Safety function maintained in case of a single fault	Design based on well tried safety components and principles. Accumulation of undetected and non dangerous faults may bring about the loss of safety			**Safety relays redundancy** (dual channel)
4	Maintained safety function in case of multiple faults	Same as Category 3, but accumulation of undetected faults never leads to the loss of safety	 Maximum voltage for ac: L1 = 48 Vac		**Safety relays; redundancy** (dual channel); **self-checking; input cross fault detection**

Table V.1

Table V.2 (as per EN 1050) - given for information purposes - only groups data that must be taken into consideration as per EN 1050 and EN 954-1. It offers a way of selecting safety equipment by looking at the linkage between the severity of injury, the frequency of exposure and the possibility of avoiding the risk, and the five levels of Risk Category.

Table V.2



Severity of the injury	**S1**	Naturally reversible slight injury
	S2	Irreversible serious injury or fatal injury
Frequency of exposure	**F1**	Rare to fairly frequent
	F2	Frequent to constant
Possibility of avoiding the risk	**P1**	Possible in some conditions
	P2	Highly unlikely

Measure possible but accompanied with additional protections

Measure proportional to the level of risk encountered

Measure of comfort, excessive categories