CARLO GAVAZZI

## Introduction

The free goods circulation, according to the people safety, is one of the basic principles considered by the common European market. This circulation is guaranteed for products meeting the main safety requirements as stated by the European standards. In order to harmonize the national standards and regulations of all of the EC Member States, the internal Directives, have to be implemented in the domestic legislation of the individual Member States.
The European Directives are then transposed in the national law system of the countries being part of the European community; in this way the juridical references are common inside the EC. Also the European norms get transposed in national norms by the relevant Normative Bodies, giving VDE or DIN norms in Germany, NF norms in France, etc.
The European Machinery Directive (98/37/EC) gives particular importance to the essential requirements concerning the machine safety through its three different levels of norms:

**A type norms:**

basic norms involving general design principles applicable to each type of products:

EN 292-1: “Safety of machinery –Basic terminology, methodology”;

EN 292-2: “Safety of machinery – Technical principles and specification”;

EN 1050: “Safety of machinery – Risk assessment”.

**B type norms:**

family of norms subdivided in B1 norms, considering the safety aspects, and B2 groups including safety devices applicable to different kinds of machines:

**B1 group norms:**

EN 954-1: “Safety of machinery - Safety- related parts of control systems - Part 1: general principles for design”;

EN 294: “Safety of machinery - Safety distance to prevent danger zones being reached by the upper limbs”;

EN 349: “Safety of machinery - Minimum gaps to avoid crushing of parts of the human body”.

**B2 group norms:**

EN 418: “Safety of machinery – Emergency stop device - Design principles”;

EN 574: “Safety of machinery - Two-hand control devices – Functional aspects - Principles for design”;

EN 1088: “Safety of machinery – Interlocking devices associated with guards - Principles for design and selection”;

EN 61496-1: “Safety of machinery - Electrosensitive protective equipment - General requirements and test”;

EN 61496-2: “Safety of machinery - Electrosensitive protective equipment - Particular requirements for equipment using active optoelectronic protective device”;

EN 60204-1: “Electric equipment of machines - Part 1: general requirements”.

**Specifications C:**

norms including the detailed requirements for a machine or a particular group of machines, with reference to the B type norms:

pr EN 693: “Safety requirements for hydraulic forging press”;

pr EN 847: “Machinery for wood working - Safety Requirements”;

EN ISO 11111: “Safety requirements for textile machines”;

EN 775: “Manipulating industrial robots – Safety”

The norms are drawn up by the two standard Organizations, CEN and CENELEC as mandate from the EC Commission in order to fulfil the requirements of the EU Directives for specific products.
The area of application of the Machinery Directive is given by the definition of machinery in the Article 1: ”Machinery means an assembly of linked parts or components, at least one of which moves…” which includes a wide range. The area of application has been later extended to ”safety components” and ”interchangeable equipment”. This means that the application area of the Machinery Directive ranges from a basic machine up to a complete plant.
The Annex 1 of the Machinery directive lists the basic health and safety requirements which are mandatory for the safety of machinery. The manufacturer must apply the following principles, in the order given:

- Eliminate or reduce risks as much as possible (in relation to safe machinery design and construction);
- Take the necessary protection measures as for risks that cannot be eliminated;
- Inform users of the residual risks, indicate whether any particular training is required.

By applying the relevant harmonized standards, the manufacturer of a machine proves that the basic requirements are fulfilled. The conformance to the relevant safety requirements can be self-certified by the manufacturer except from machines listed in the Annex IV of the Machinery Directive, which representing a higher hazard potential, require a certification by an external Notified Body.

**Risk assessment**

In general, since machineries represent potentially dangerous items, it is required by the Machinery Directive a risk assessment for every machine; if necessary, it can be followed by risk reduction so as to limit the residual risk within the tolerable risk.
The fundamental norm which should be applied in this process is the EN 1050 “Safety of machinery – principles for risk assessment”. EN 292 “Safety of machinery – Basic concepts, general principles for design” also includes relevant aspects.

The risk assessment is the procedure allowing to detect and remove hazards as much as possible and includes:

- **Risk analysis:**
  It basically consists of:
  – Determination of the machine limits;
  – Identification of the hazards;
  – Risk estimation.

**• Risk evaluation:**
Once the risks have been determined, the risk evaluation is carried out. If the residual risk does not fall within the tolerable risk level, a risk reduction must be applied, through the implementation of appropriate measures and the risk evaluation must be operated again: the **Fig. 1** shows the iterative process of the risk evaluation which can be followed by risk reduction if necessary, to systematically achieve safety.

### Residual risk

Unfortunately, the word safety is related to a technical environment, which means that a zero – risk situation, where no hazards can occur under any circumstance, cannot be reached. As stated above, in order to obtain a tolerable risk, protective measures must be taken if needed.

- Tolerable risk: risk which is acceptable in a specific moment, even taking into consideration social-economic aspects;
- Residual risk: risk remaining once applied the risk reduction and all the protective measures related;
- Hazard: situation where risk is higher than tolerable risk;
- Safety: situation where risk is not higher than tolerable risk.

### Risk reduction

If necessary, the risk reduction for a machinery can be carried out by applying safety control functions which must be in accordance with special requirements given by EN 954-1. The requirements are classified into categories depending on the level of the risk. It is not secondary to note that all the components being part of the safety control functions must fulfil the above-mentioned requirements. In the determination of the categories, norms specify to take into account the possible failure of the components constituting the safety function or to indicate cases where faults can be excluded.
In order to keep objectivity in the evaluation criteria, the EN 954-1 lists possible failure of the components to be considered in the analysis of the control circuit.
The graph showed in **Fig. 2** can be used for estimating the risk of the safety-related parts of the control circuit and for the selection of the opportune safety category.
There are different levels of risk for machines depending on the extent of the damages to operators, on the frequency and term of exposure to the risk and on the possibility to avoid accidents.

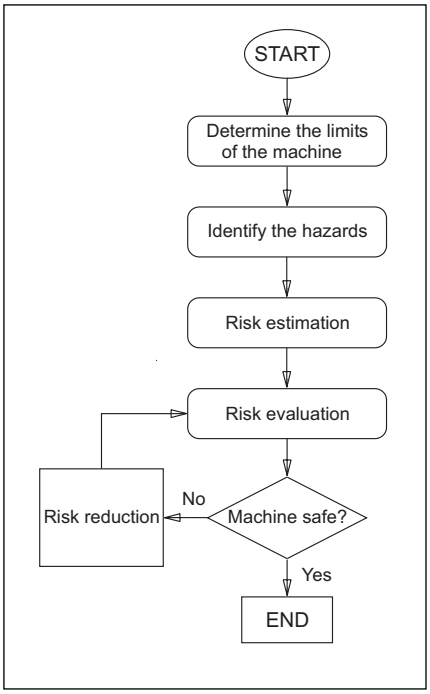



*Fig. 1*

The elements to be considered are:

**S:** severity of the injury;
S1 = Slight (normally reversible) injury;
S2 = Serious (normally irreversible) injury, including death.

**F:** Frequency and/or exposure time to the hazardous condition:
F1 = Seldom up to quite often and/or the exposure time is short;
F2 = Frequent up to continuous and/or the exposure time is long.

**P:** Possibility of avoiding the hazard:
P1 = Possible under specific conditions;
P2 = Scarcely possible.

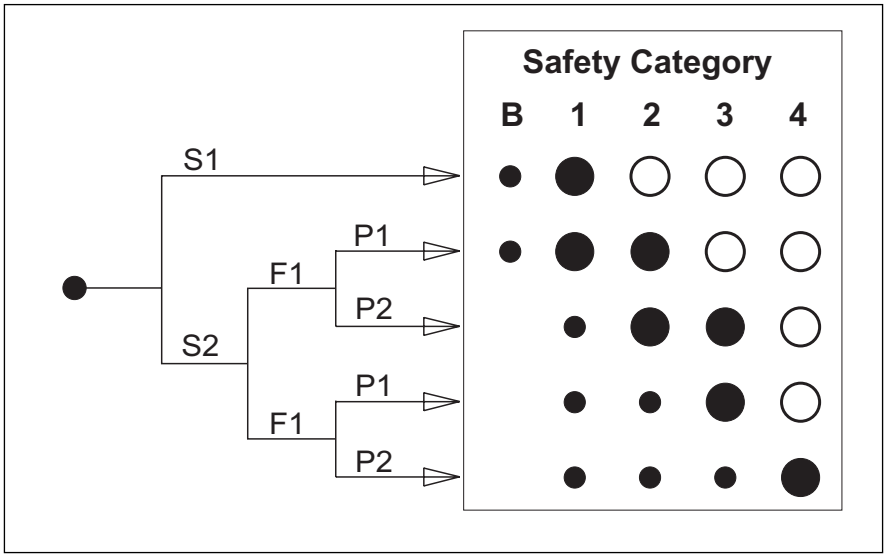
### Category selection:

B, 1 to 4 Categories for safety-related parts of control systems

- ● Possible categories requiring further steps
- ⬤ Preferred categories for reference points
- ○ Measures over-dimensioned for the relevant risk

A brief summary of the requirements for the different risk categories is shown in **Tab. 1**; for the complete text of the requirements, refer to the EN 954-1, “Safety – related parts of control systems”

*Fig. 2*



CARLO GAVAZZI

## Risk categories: requirements summary

| Category | Summary of requirements | System behaviour | Basic principle to achieve safety |
|---|---|---|---|
| **B** | Safety-related parts of control systems and/or their protective equipment, as well as their components, shall be designed, constructed, selected, assembled and combined in accordance with relevant standards so that they can withstand the expected influence | The occurrence of a fault can lead to the loss of the safety function | Mainly characterized by selection of components. |
| **1** | Requirements of B shall apply.<br>Well-tried components and well-tried safety principles shall be used | The occurrence of a fault can lead to the loss of the safety function but the probability of occurrence is lower than for category B | |
| **2** | Requirements of B and the use of well-tried safety principles shall apply.<br>Safety function shall be checked at suitable intervals by the machine control system | The occurrence of a fault can lead to the loss of the safety function between the checks.<br>The loss of the safety function is detected by the check | |
| **3** | Requirements of B and the use of well-tried safety principles shall apply.<br>Safety-related parts shall be designed, so that:<br>• a single fault in any of these parts does not lead to the loss of the safety function;<br>• whenever reasonably practicable, the single fault is detected. | – When the single fault occurs, the safety function is always performed.<br>– Some but not all faults will be detected.<br>– Accumulation of undetected faults can lead to the loss of the safety function | Mainly characterized by structure of the system |
| **4** | Requirements of B and the use of well-tried safety principles shall apply.<br>Safety-related parts shall be designed, so that:<br>• a single fault in any of these parts does not lead to a loss of the safety function;<br>• the single fault is detected at or before the next demand upon the safety function. If this is not possible, then an accumulation of faults shall not lead to a loss of the safety function. | – When the faults occur the safety function is always performed.<br>– The faults will be detected in time to prevent the loss of the safety function. | |

*Tab. 1*