SAFETY COMPONENTS: OVERVIEW OF THE STANDARDS

INTRODUCTION

The issue of safety in the workplace is of absolute importance and over the years the standard setters have developed a series of continuously evolving standards, the focal point of which remains the Machinery Directive.
In order to ensure conformity of the machine, the manufacturer must verify that it meets the safety requirements listed in the directive and guarantee compliance with the harmonised standards published in the European Union's Official Journal and relating to the product in question.
There are three types of safety standard for machinery:

- type **A**, which establish general principles applying to the design of all machinery
- type **B**, which deal with one or more safety aspects for a wide range of machinery
- type **C**, which deal in detail with the specific category of machines

Type **A** standards include EN ISO 12100, which cover the basic concepts and general principles for the design of safe machinery, and EN ISO 14121, which describe a hazard identification and risk assessment method.

Type **B** standards include EN ISO 13840, which provides the tools for designing parts of control systems linked to machine safety, mainly the control systems, which are made of components featuring various kinds of technology to reduce risks associated with use of the machine, and IEC 62061, which only refers to systems using electrical and electronic technologies.
One of the main affinities between EN ISO 13849 and IEC 62061 is that the former establishes as the desired safety parameter an index called PL (performance level) and the latter identifies a similar parameter called SIL (safety integrity level). Both indices represent the machine's reliability in terms of the probability of a dangerous failure. The table below shows their relationship:

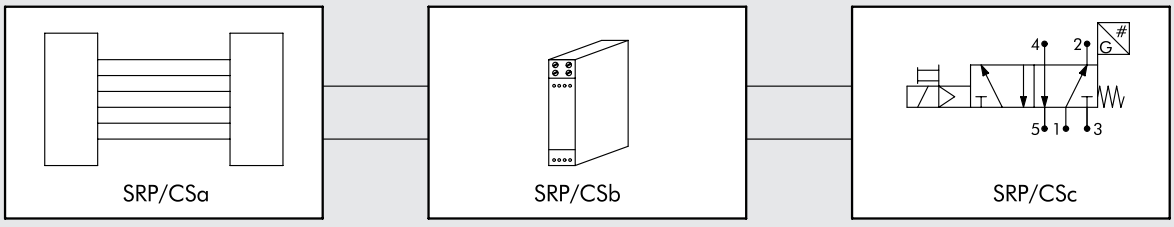
PL	SIL
a	No correspondence
b	1
c	1
d	2
e	3

EN 982 and EN 983 are also type B standards and both deal with safety, but unlike the previous standards they concern components (hydraulic and pneumatic respectively) rather than controlled devices.

When type **C** standards exist for a particular machine, the manufacturer can adopt them directly to achieve the presumption of compliance with the Machinery Directive; if no type C standard exists, it is still necessary to implement a risk-reduction strategy like the one described in harmonised standards type A and B.
Since revision 98/37/EC, the Machinery Directive has dealt not only with machines but also with safety components, namely components made and sold specifically to achieve a safety function and the breakage or malfunction of which jeopardizes personal health and safety.

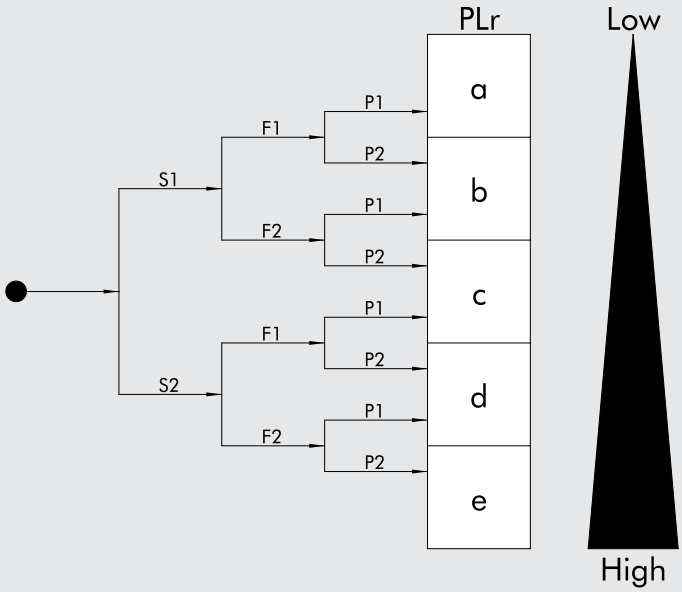
EN ISO 13849

When type C standards do not exist for a particular machine, the manufacturer can adopt the risk-reduction strategy indicated in EN ISO 13849. This standard is divided into two parts: the first part sets out the general principles and the method to follow; the second part is dedicated to validation of the results.
According to the first part of the standard, a machine designer can reduce the risk by designing special safety-related parts of control systems (SRP/CS) that perform one or more safety functions, such as emergency stops, prevention of unexpected start-up, isolation and energy dissipation.
We quote the example of a function comprising three SRP/CSs: a safety barrier (input – sensor), a PLC (processing - logic) and a valve (output - actuator). In the event of intrusion, the barrier relays a signal to the PLC, which activates the valve, the job of which is to relieve a section of the pressurized pneumatic circuit, thereby providing isolation and energy dissipation.



For each safety function it is necessary to determine the Performance Level requested (PLr), according to the procedure indicated in Annexe A to the standard. The following are assessed:

- the severity of the lesion (S), resulting from the failure
- the hazard exposure frequency (F)
- the possibility of avoiding the hazard (P)



If, for example, the severity of a lesion resulting from a failure is low and/or the hazard exposure frequency is low and/or the hazard avoidance possibility is high, the PLr will be low. On the contrary, if the severity and/or exposure frequency is/are high and/or the hazard avoidance possibility is low, then the PLr for that safety function will be high.
Therefore, for each SRP/CS or combination of SRP/CSs performing a safety function, the machine designer must determine the achievable performance level PL.
Certain parameters including the following must be used for this calculation:

- MTTFd (Mean Time to dangerous Failure) of the single components
- DC (Diagnostic Coverage)
- CCF (Common Cause Failure)
- function structure
- compliance of the components used with the basic and/or proven safety principles.

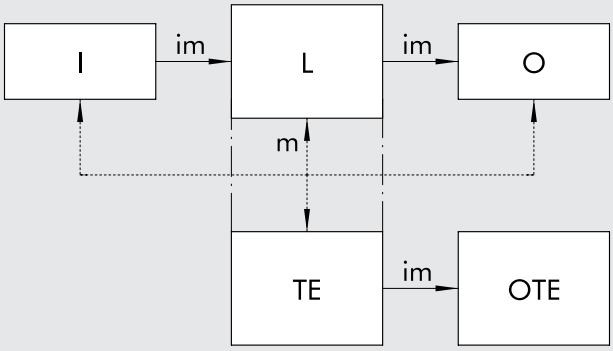
The **MTTFd**, which is the mean time between two dangerous failures, can be obtained from values referring to the operating cycles of the safety function and the B10d of the components, namely the number of cycles 10 percent of the components suffer a dangerous failure. The B10d is equal to double B10, which in turn is an index of the reliability of the component obtainable by following the instructions in EN ISO 19973.
The B10d values of Metal Work products are published on the company's website: http://www.metalwork.it/ita/dirett_macchine.html.

DC (diagnostic coverage) and **CCF** (common cause failure) are obtained using the appendices to EN ISO 13849-1; DC can be determined using failure mode and effects analysis (FMEA) or a similar method.

The structure of the function depends on the architecture. One possible kind is unmonitored single-channel architecture:

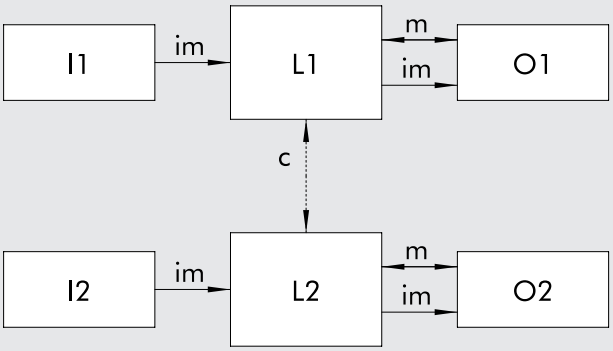
Were:
im: interconnection means
I: input device, e.g. sensor
L: logic
O: output device, e.g. valve

Then comes single-channel architecture with diagnostics. In this case, a module called Test Equipment (TE) provides an output (OTE) in some way linked to the status of the safety function:



Were:
im: interconnection means
I: input device, e.g. sensor
L: logic
m: means of surveillance
O: output device, e.g. valve
OTE: Test Equipment OUTPUT
TE: Test Equipment

A third example is double-channel architecture, which exploits the redundancy of a function – if one channel fails the other remains active:



Were:
im: interconnection means
I1, I2: input device, e.g. sensor
L1, L2: logic
m: means of surveillance
O1, O2: output device, e.g. valve
c: crossed check

As regards the conformity of components used to the basic and/or proven safety principles, reference should be made to a series of considerations presented in EN ISO 13849 standards, which guarantee that the SRP/CS and related components comply with the design, construction and assembly principles.
With these data, the machine designer can determine the safety function category (B, 1, 2, 3 or 4, in increasing order of importance) and the PL achieved; It is important therefore to check it is equal to or greater than the PLr required.