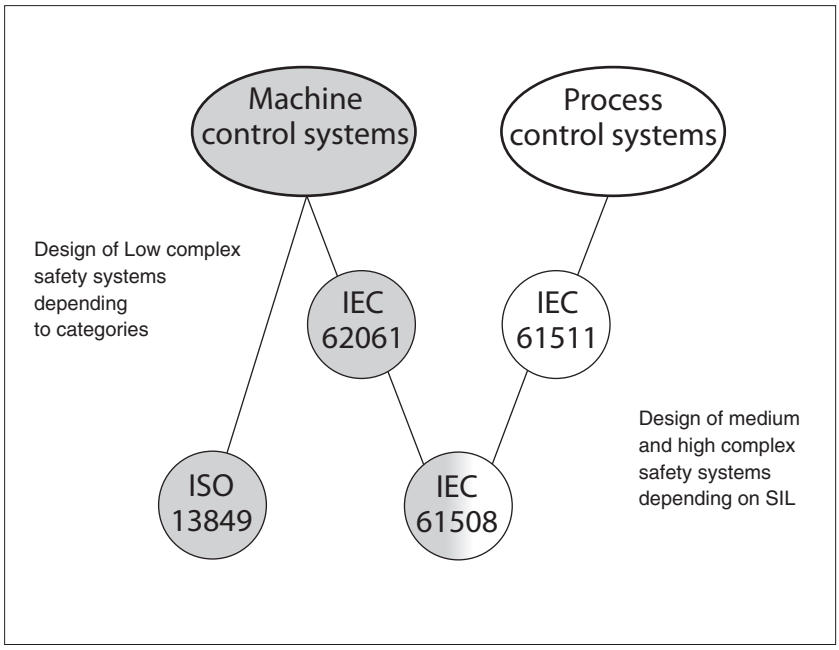
Functional safety, - $MTTF_d$ reliability data

according to EN ISO 13849-1/2



The new European Machine Directive 2006/42/EC imposes to fulfill additional safety requirements to all machines or systems delivered into the European market. The approach to define the compliance with above safety requirements refers to different standards according to the product classification:

- Machine control systems refer to the European harmonized standard EN ISO 13849. The safety requirements are evaluated according to reliability calculation procedures performed on any single component of the safety system. In the specific case of hydraulic components $MTTF_d$ (mean time to dangerous failure) is applied.
  $MTTF_d$ is a reliability parameter determined by statistical approach, which value is defined by the EN ISO 13849 = 150 years if all safety principle, as those listed in section 1 are fulfilled by the analyzed component.
- Process control systems follow different standards and their components related to safety are classified according to SIL (Safety Integrity Level).

In the following sections are reported the criteria for $MTTF_d$ determination and the values for each Atos component suitable to be used in safety related controls.

1 DETERMINATION of $MTTF_d$ values according to EN ISO 13849-1/2

The evaluation of *$MTTF_d$* values has been accomplished according to the basic and well-tried safety principles suggested in the standard EN ISO 13849-1/2 .
Furthermore an FMEDA calculation has been carried out using failure data taken from recognized international database.
If the components design fulfills requirements of the above principles, the *$MTTF_d$* of the device can be evaluated equal to 150 years, that it means to perform a Performance Level equal to “c” for the architecture corresponding to category 1.

For hydraulic components, the standard ISO 13849-1:2023 defines an MTTFD value of 150 years with a number of operations ≥ 1.000.000 cycles per year, assuming that basic and well-tried safety principles are applied.
This is the condition reported in the Atos technical tables of each specific component

Each type of devices can be classified as follows, according to EN ISO 13849-1/2:
- category 1
- single channel (the component performs a single function)
- high $MTTF_d$
- Diagnostic Coverage: not applicable
- CCF (Common Cause Failure): applicable only to categories > 1
- maximum obtainable Performance Level is “c”
- Service life = 20 years (according to EN ISO 13849-1 is the maximum period of using)

The above described classification is valid if the following characteristics of the hydraulic valves are respected:
- the spool returns in rest position in case of valve’s de-energization
- the spool must keep the rest position when the valve is de-energized
- the spool must ensure a sufficient overlapping in rest position

2 GENERAL NOTES

- **The reliability values reported in the Atos technical tables of each specific component are guaranteed if the operating conditions described in each component’s technical table are respected**

The manufacturer who has to design a machine or a system with specific safety requirements, has to consider the following important notes:

- **Low complex safety systems designed according to EN ISO 13849**
  The manufacturer must define the Performance Level (PL) according to the risk analysis. This reliability characteristics is obtainable starting from MTTFd values of each hydraulic components used in the equipment.
- **Medium and high complex safety systems designed according to EN 62061**
  The manufacturer must define the Safety Integrity Level (SIL) according to the risk analysis. This characteristics is obtainable starting from Performance Level (PL) defined by EN ISO 13849 and calculated as described in the previous step.