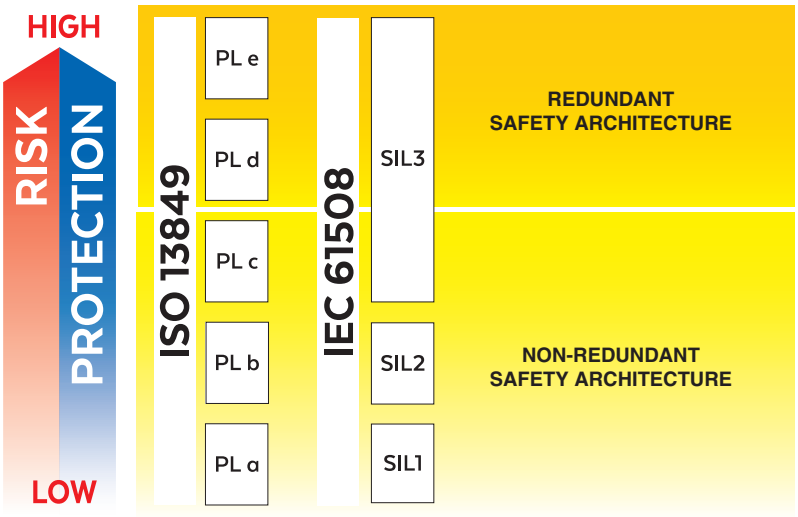
# Basics for safety components

**IEC 61508** Safety Integrity Level and **ISO 13849** Performance Level - certified by




Safety in engineering of modern machinery is becoming a primary issue to protect people from potential risks caused by accidental failures of machines and systems.

The **Machine Directive 2006/42/EC** with relevant norms **IEC 61508 Safety Integrity Level** (SIL) and **ISO 13849 Performance Level** (PL), represents the framework of the functional safety, which is a key aspect in terms of general principles of prevention concerning safety of devices or systems with health implications.

It defines the safety requirements that the machine manufacturer must comply with, in order to obtain the certification and thus the possibility to apply the CE mark required to sell the machine within the European market.

Machine Directive 2006/42/EC replaces the existing 98/37/EC and it is universally applicable to machinery, safety components, and other specific equipment.

## 1 SAFETY NORMS

**IEC 61508** and relevant norms **IEC 61511** (process control system) plus **IEC 62061** (machine control systems) introduce the integrated probabilistic approach to the functional safety. They specify the Safety Integrity Levels (SIL) required to perfom safety functions.

**ISO 13849** norm provides safety requirements and guidance on the principles for the design and integration of safety-related parts of control systems including the design of software.

It specifies the Performance Level (PL) required to perform safety functions.
PL: discrete value that specify the ability of safety related parts of control systems to perform a safety function under forseeeable conditions.

The requirements are classified into five Performance Levels, where **PL e** identifies the highest protection level.

## 2 CERTIFICATION

Atos safety valves (on-off and proportionals) are certified by TÜV in compliance with IEC 61508, IEC 61511, IEC 62061, ISO 13849

**The certification guarantees the valve compliance with related safety norms and it proves that all requirements have been met for the SIL and PL levels claimed for the specific valve.**

The certification also confirms the following data which can be used by the machine manufacturer for the certification of the whole system:

- the design process used by the valve manufacturer to avoid failures
- the design techniques and measures used to control failures
- the methods used to define hardware fault tolerances
- the methods used to measure the safe failure fractions
- the methods used to measure the probabilities of failure

⚠ **The use of non-certified products invests the machine manufacturer of the responsability for validating that all above aspects have been carried out according to the applicable standards.**

Without valve's certification the machine manufacturer has to alternatively:

- collect from valve's manufacturer all the reliability data necessary to evaluate the safety level of the whole system
- consider the worst case concerning the safety level (e.g. assign to valves the lower safety level **PL a** or **SIL 1** in order to calculate system safety)

## 3 RISK ASSESSMENT

The first step for determining the necessary risk reduction is the Risk Assessment.
It is a procedure carried out to identify which risks in the machine require a mitigation by means of safety control systems (e.g. laser barriers, shut-off valves, enabling devices, etc). Each of these control systems become a Safety Function.
At that point the safety functions must be defined and satisfied by the machine design (see 3.1).

⚠ **It is the responsibility of the machine manufacturer to ensure that all safety requirements are satisfied and to conduct a documented risk assessment to ensure that all potential machine hazards are covered.**

### 3.1 Machine Manufacturer

With the name of “Machine Manufacturers” are identified OEMs or end users who manufacture machinery for their own needs or everybody who performs “significant modifications “as:

- change the machine function
- change the machine application area
- change the equipment
- change the machine performance

If changing any of the above parameters results in either change of intended use or change of safety system or safety component, a machine modification should be treated as “significant”.

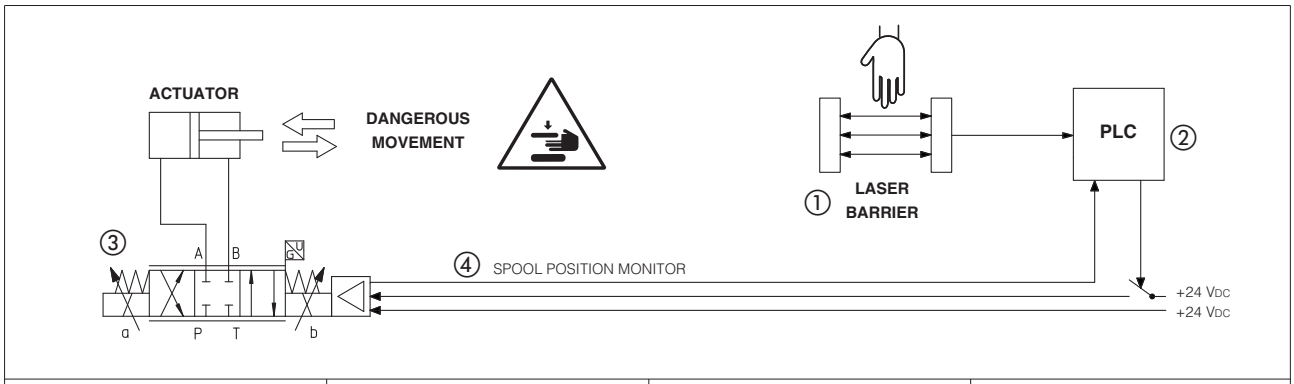
Example:

Adding air-gun pneumatic connection = NOT significant modification

Adding hydraulic accumulator to increase the speed and improve cycle time of the machine = significant modification

## 4 SAFETY RELATED PARTS

They are parts of machine control systems performing safety functions, allowing the system to achieve or maintain a safe status.
These parts consist of either hardware or software and stand-alone or integrated components of the machine control system.
Safety-related parts incorporate the entire effective chain of a safety function provided by control unit, valves, sensors and actuator.



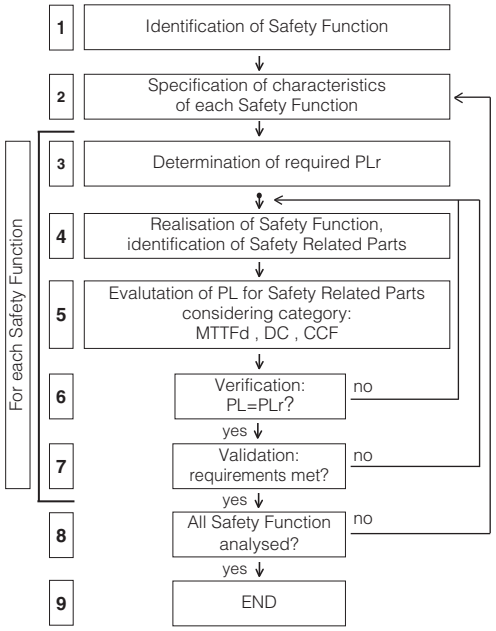

| ① | ② | ③ | ④ |
|---|---|---|---|
| SENSORS | LOGIC | VALVE | VALVE DIAGNOSTICS |
| Detect dangerous situations | Controls the machine operations and activates the safety procedures in case of dangerous situations | Controls the actuator and avoids the dangerous movement | Monitors the correct valve operation |

## 5 SAFETY ANALYSIS

The second step after the identification of the risk is the Safety Analysis.
The process for the design of the safety-related parts of control systems, is iterative.

The aside scheme shows the one used by EN ISO 13849-1:

- The first step consists in the identification of the Safety Functions.
- Any characteristics of all safety functions must be described and documented.
- The Performance Level required (PLr) by each safety function must be defined. ISO13849-1 uses a path like the one shown in section 5.1.
- The machine manufacturer must designe a system to protect the operator, granting a Performance Level (PL) equal or higher than the Performance Level required (PLr). The Performance Level (PL) must be defined considering following parameters:
  - MTTFd, reliability of safety system – see section 5.2
  - DC, capability to detect faults – see section 5.3
  - CCF, vulnerability of the system to failures – see section 5.4
  - architecture categories of the safety system – see section 6

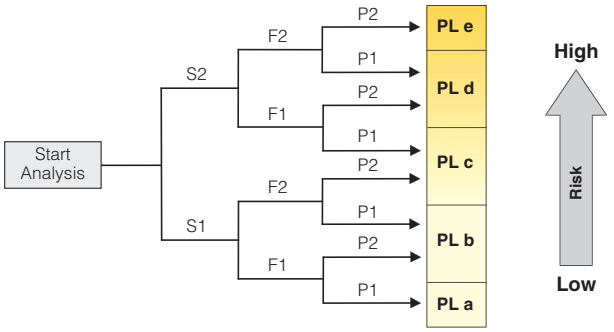


### 5.1 Performance Level required - PLr

The determination of PLr for ISO 13849-1 is carried out analysing the following parameters:

- Severity of harm:
  **S1** = slight
  **S2** = serious
- Frequency and duration of exposure to the hazard:
  **F1** = not often
  **F2** = frequent
- Possibility of avoiding the hazard or limiting the harm:
  **P1** = possible
  **P2** = rarely possible

Each of five performance levels corresponds to a further parameter scale, based on the probability of a dangerous failure per hour.




| Performance Level | Average probability of dangerous failures per hour, h-1 |
|---|---|
| PL e | ≥$10^{-8}$ to < $10^{-7}$ |
| PL d | ≥ $10^{-7}$ to < $10^{-6}$ |
| PL c | ≥$10^{-6}$ to < 3 x $10^{-6}$ |
| PL b | ≥ 3 x $10^{-6}$ to < $10^{-5}$ |
| PL a | ≥ $10^{-5}$ to < $10^{-4}$ |

### 5.2 Mean Time to Failure dangerous - MTTFd

The achievement of a specific PL or SIL relies on the reliability of the system.
The reliability is quantified by Mean Time to Failure dangerous (MTTFd ) which is measured in hours.

The MTTFd should be determined from the component manufacturer's data.

### 5.2 Diagnostic Coverage - DC

The Diagnostic Coverage (DC) is a measure of how effectively the potential dangerous failures can be detected by the monitoring system.

EN ISO 13849-1 suggests how to define DC.

Diagnostic Coverage is defined as the measure of the effectiveness of diagnostics: it is determined as the ratio between the failure rate of detected dangerous failures and the failure rate of total dangerous failures;

**DC = 0%** no dangerous faults are detected

**DC ≅ 100%** most of dangerous faults are detected (it is impossible to reach a DC = 100% because diagnostics are not considered to be completely reliable)

**Diagnostic Coverage categories:**

| Category | Range |
|---|---|
| None | DC < 60% |
| Low | 60% ≤ DC < 90% |
| Medium | 90% ≤ DC < 99% |
| High | DC ≥ 99% |

### 5.3 Common Cause Failure - CCF

The CCF value is a parameter for evaluating the measures against the common cause failure.
It is a failure in redundant systems where two or more channels fail at the same time in consequence of a single common cause.
The redundancy can be compromised if both channels fail simultaneously due to the same cause.
EN ISO 13849-1 provides a score for CCF, which is used to determine the Performance Level (PL).

For this score, EN ISO13849-1 defines a checklist of seven important countermeasures:

1. The signal paths of different channels are physically separated (score = 15 points)
2. Diversity in the technology, the design or the physical principles of the channels (score = 20 points)
3. Protection against possible overloading (15 points) and the use of well-tried components [which are those components which have been widely used or made and verified for safety related application (score = 5 points)]
4. Failure mode and effects analysis during development for the identification of potential common cause failures (score = 5 points)
5. Training of designer/service personnel in CCF and its avoidance (score = 5 points)
6. Protection against common failures caused by contamination (fluid filtration) and electromagnetic interference for electrical parts(score = 25 points)
7. Protection about common cause failures caused by unfavorable environmental conditions (score = 10 points)

For architecture categories 2, 3 and 4 a minimum score of 65 points is required (see section 6 ).

**Note:** CCF always depends on the system and application.

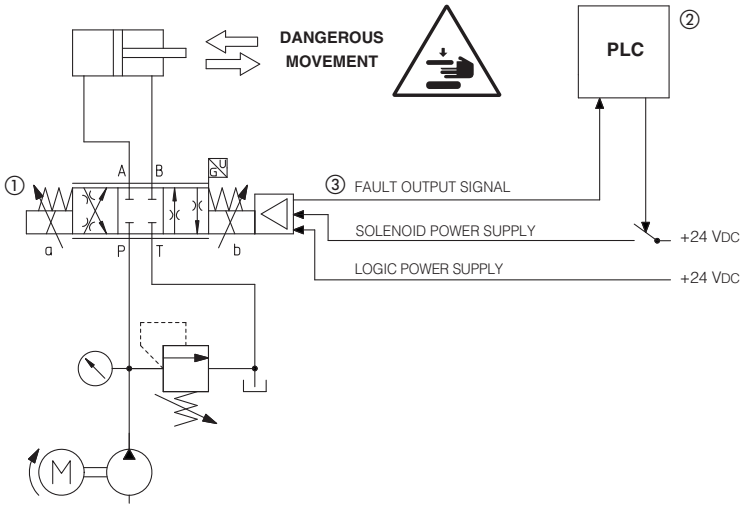
## 6 ARCHITECTURE CATEGORIES

SIL and PL levels depend not only on the characteristics of the single component but also on the architecture of the hydraulic system and of the signals diagnostic.
Architecture categories help to define the probability of failure and the PL of the safety related parts of a control system in relation to their resistance to faults and their subsequent behavior in the fault condition
There are five architecture categories, identified as : **B, 1, 2, 3, 4**
The higher is the number, the higher is the complexity of the safety system and the higher is the achieved Performance Level PL.

### 6.1 Architecture categories B and 1

In categories B and 1, the resistance to faults is mainly achieved by the selection of proper components. They are not-redundant architecture so the occurence of a failure may lead to the loss of the safety function.
Category 1 has a greater resistance than category B because of the use of special components and principles which are considered well-tried and tested in a safety system.

**Example of architecture category 1**




**Safety function** = to prevent the dangerous cylinder movement in a certain phase of the cycle or in emergency

The safety function is achieved by disabling the current to the solenoids of safety proportional valve so that the spool is moved by the springs to the rest position with positive overlap.

Through the continuous monitoring of the valve's spool position, the machine PLC verifies if the "safe condition" is fully accomplished.

⚠ **The safety function is not performed in case of valve ① failure**
**Fault tolerance HFT = 0**

① Digital proportional valve with double power supply - option /U
(i.e. DHZO-TES-SN-NP-07*-L5 **/U**)

② Machine PLC supervising the safety function

③ Fault output signal used for safety diagnostics

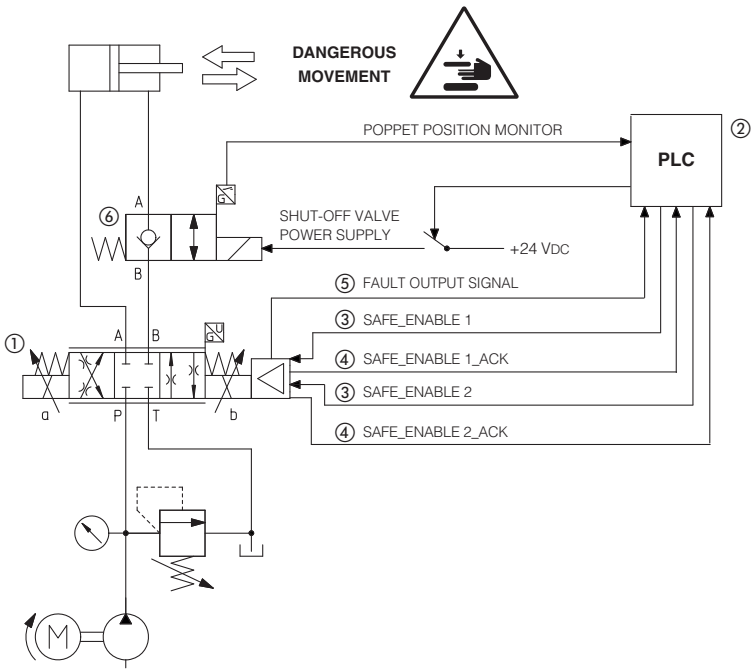
### 6.2 Architecture - category 2

In category 2 all of the requirements of architecture B and 1 are combined. In addition, the system is monitored to intercept faults affecting the safety function.
These monitors are made at regular intervals, e.g. at startup or before the next demand on the safety function.
By using an appropriate selection of test intervals, a suitable risk reduction can be obtained.

### 6.3 Architecture categories 3 and 4

In categories 3 and 4, the occurrence of a single fault does not result in the loss of the safety function.
In category 4 such faults are detected automatically.
Accumulation of faults will not lead to a loss of the safety function.

**Example of architecture category 4**




① Digital proportional valve - option /K
(i.e. DHZO-TES-SN-NP-07*-L5 **/K**)

② Machine PLC supervising the safety function

③ Signals used to enable/disable the current to the valve's solenoids

④ Signals confirming the valve safe status

⑤ Fault output signal used for safety diagnostics

⑥ Safety shut-off valve with poppet position monitor (i.e. JO-DL **/FV**)

**Safety function** = to prevent the dangerous cylinder movement in a certain phase of the cycle or in emergency

In this example a safety shut-off valve with poppet position switch has been added to the safety proportional valves to grant a **redundant safety architecture**.

The safety function is performed by disabling the current to the solenoid of safety proportional valve and safety shut-off valve so that the spool is moved by the springs to the rest position with positive overlap.

The safety condition is confirmed by:

- SAFE_ENABLE_ACK status = 24 VDC
- shut-off valve poppet position monitor signals

⚠ **The safety function is performed even in case of failure of one valve, ① or ⑥**
**Fault tolerance HFT = 1**