SIL Level Requirements throughout Development

# Acronyms / Document Conventions

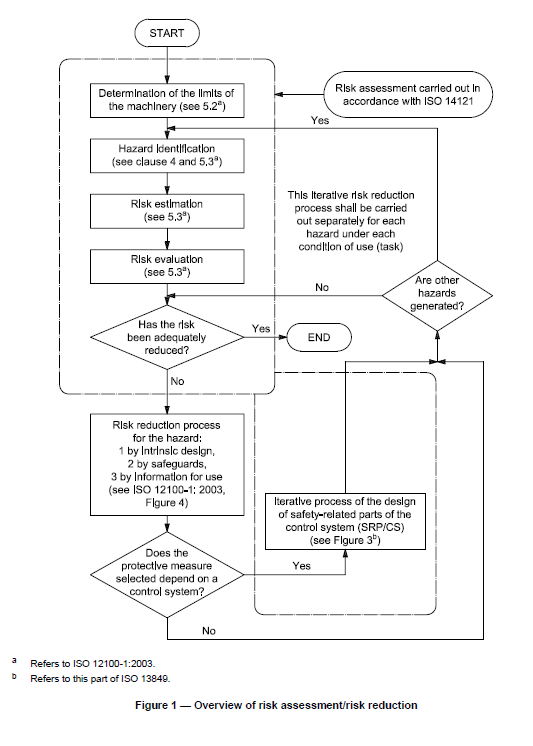
SRP/CS = Safety-related part of a control system  
MTTF = Mean time to failure  
MTTFd = Mean time to dangerous failure  
DC = Diagnostic coverage  
DCavg= Average diagnostic coverage  
CCF = Common cause failure

This document references ISO 13849 and EN280.

# Risk Reduction

The design of the SRP/CS is to provide the required risk reduction for the overall design procedure for the machine.

The schematic below will be followed as an overview of the process recorded within this document.



1. Determine the limits of the machine with its current controller, checking any risks or hazards and do an evaluation.
2. If there is risk, determine essentials, safeguards, and any other protective measures
3. If the protective measure is dependent on a functional system, the check for minimal achievement of PL and SIL for that functionality begins.

# SIL and PL for Modular Development

When working with an industry involving machinery and risk, a safety standard comes side-by-side with functional requirements, to ensure that the developments of the industry will minimize the risk that comes with usage.

SIL, or a Safety Integrity Level comes with the IEC 61508 to ensure we define the relative level of risk for each safety functionality. The goal is to achieve functional safety within development, meaning that the risks of a product from injury or worse are minimized.

SIL ratings correlate to frequency and severity of hazards. They not only determine the probability of failure for system functionalities, they also determine the performance required to maintain and achieve safety.

There are four SIL levels – SIL 1, SIL 2, SIL 3, and SIL 4.

The higher the SIL level, the greater the risk of failure, which equates to stricter safety requirements.

|  |  |  |
| --- | --- | --- |
| **Safety Integrity Level** | **Probability of Failure on Demand** | **Risk Reduction Factor** |
| SIL 4 | ≥105 to <104 | 100,000 to 10,000 |
| SIL 3 | ≥104 to <103 | 10,000 to 1,000 |
| SIL 2 | ≥103 to <102 | 1,000 to 100 |
| SIL 1 | ≥102 to <101 | 100 to 10 |

For IEC 61508, SIL level only comes up to Level 3, as Level 4 is only treated as a global threat.

Performance level (PL) is directly related to SIL. It is defined as a discrete level used to specify the ability of SRP/CS to perform a safety function under foreseeable conditions.

Therefore, we need PL to determine at what ability the SRP/CS have to be performed.

PL is determined by:

* MTTFd value for single components
* DC
* CCF
* Structure
* Behavior under fault conditions
* Safety-related software
* Systematic failure
* Expected performance

**Quantifiable**

**Qualitative**

While the performance level can determine the capability of performing a safe function, the bare minimum requirements to ensure safety must be achieved.

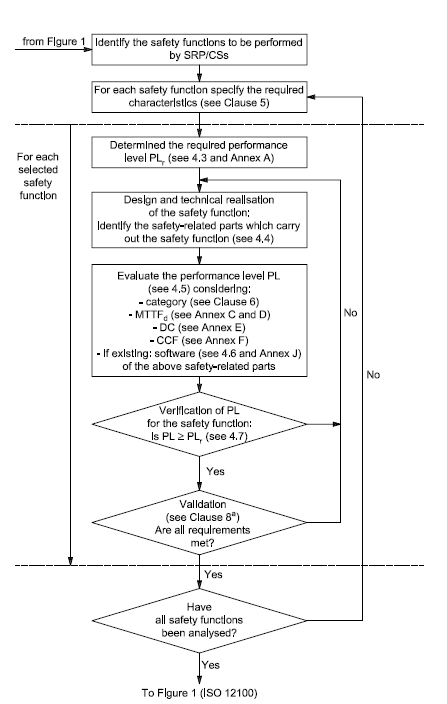
PLR (or required performance level)indicates the PL that is **required** for risk reduction of each safety function. This can be determined through Annex A.

PL>= PLR

In this case, PLR will be used as a verification tool to ensure that the safety function utilizing a PL is equivalent or greater than the minimum PL.

If the condition is not satisfied, a reiteration of the figure below will be necessary. The figure is an overview of the process that will be used to determine SIL for the function.

­



1. Figure 1 is the general process of risk reduction for the machine. When there is a risk identified and the ECU is related, it will enter.
2. Identify the purpose, mechanisms and all possible results from the selected safety function.
3. Follow procedures to ensure that PL is realized and accurate to the necessary safety specifications
4. Ensure that all safety functions are analyzed.

To categorize a machine function into a SIL level, we will be looking at all the attributes of that function that define the PL.

# Determining PLR

The method used provides an estimation of required performance level and is to guide the creation of standard maker.

When assessing the risk, the situation and interdependence of the control system are assumed and taken into account when measuring the level for the intended safety function.

The main parameters that are taken into account for determining the PLR are:

S (Severity of Injury)

F (frequency and time of exposure to hazard)

P (possibility of avoiding the harm).

S estimation is dependent on F and P to determine the frequency of occurrence. Combined, these will determine a qualitative process to estimate the risk.

**S (Severity of Injury) – S1, S2**

The estimation ranges from reversible injuries to serious irreversible injuries [where death is considered].

The severity is split into two sections, where S1 would include usual accidents and normal healing times without complications, while S2 would be amputation or death.

**F (Frequency & time of exposure to hazard) – F1, F2**

While a time period cannot be specified to the exact, you can separate two potentially different exposure levels.

If any of company property or personnel is exposed frequently and continuously to the same hazard, regardless of differentiating time intervals or the affected, it is assumed to be F2.

The frequency of exposure to the hazard should be evaluated as an average value seen in relation to the total period of time in which equipment is used.

Time Used↑ = F↑

F1 should be selected if only used from time to time.

**P (possibility of avoiding the harm) – P1, P2**

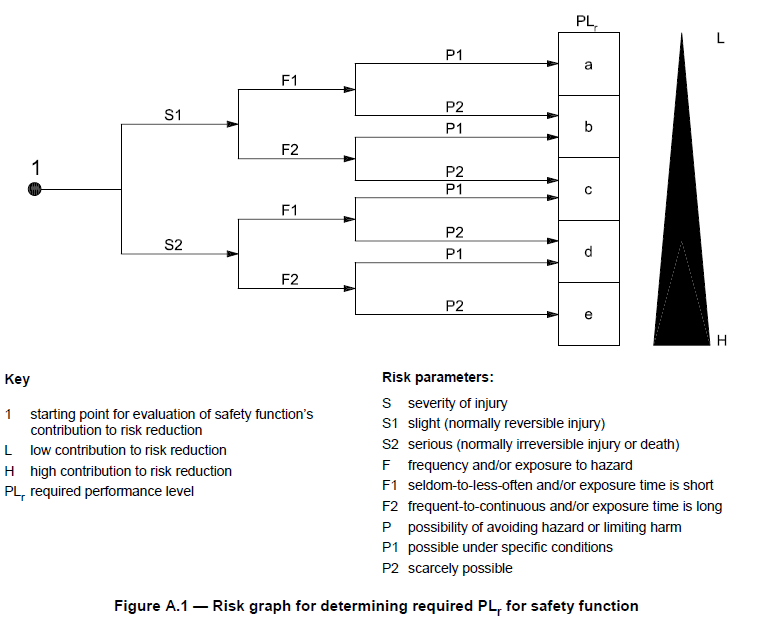
Many hazards can be recognized and avoided before leading to an unfortunate event, but some cannot be identified and are absent of indicators.

Some of the factors influencing P include:

* Having physical characteristics
* Operation with or without supervision
* Operation by experts or non-professionals
* Speed with which the hazard arises (ex. Quickly or slowly)
* Possibilities for hazard avoidance (e.g. by escaping)
* Practical safety experiences relating to the process.

P1 should only be selected if there is a tangible chance to avoid the accident or of significantly reducing its effects. P2 should be selected if there is no chance of avoidance.

If the above definitions are followed, the graph below should help identify the PLR level.

****

Table

Description automatically generated with medium confidence

# Estimating PL

Once PLR is set for the function, PL must be determined to get an accurate SIL level from the safety function.

PL can be calculated through quantifiable methods using Markov modelling, generalized stochastic petri nets (GSPN), reliability block diagrams, etc. The qualitative methods used in the document is a simplified estimate of the PL, which in turn will turn into an estimated SIL.

For SRP/CS that are considered simplistic, such as PL a to c, a qualitative estimation be justified in the design rationale.

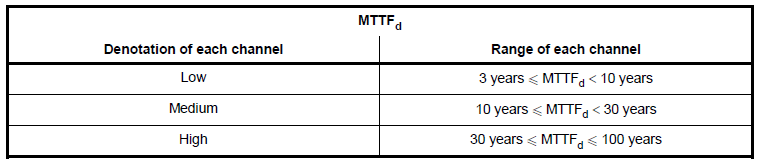
Using the attributes outlined to define a PL level can directly translate to SIL.

PL a is used to reduce the risk of very slight and reversible injury. Every other PL level corresponds to a SIL, with PL e corresponding to the highest SIL level of 3.

## 2a. Mean time to dangerous failure (MTTFd) – Annex C and D

One of the qualities that determines PL is mean time to dangerous failure.

According to the ISO 13849, each channel of a system is categorized in three levels based on the amount of years it takes to endanger a worker.



The maximum amount of years considered are 100 years.

To estimate the MTTFd, the data chosen [from greatest consideration to least] should be…

1. Manufacturer’s data;
2. Methods in Annexes of C and D;
3. Choose ten years

### Calculations – Single Components

*B*10d = mean number of cycles until 10% of the components fail dangerously.

Typical values for all components can be found in Table C.1 in ISO 13849.

**Hydraulic components**

MTTFd for a single hydraulic component, e.g. a valve, is dependent if the following criteria below are met.

NOTE: Information can be found in data sheet of the component manufacturer.

1. Hydraulic components are manufactured according to well-tried safety principles and designs that are agreeable with ISO 13849, Tables C.1 and C.2 in ISO 13849.
2. Manufacturer of hydraulic component specifies appropriate application and OS for the user. Information provided shall be agreeable with documents in a).

If the conditions are met, the MTTFd can be estimated at 150 years. If not, the value must be given by the manufacturer.

**Pneumatic, mechanical and electromechanical components**

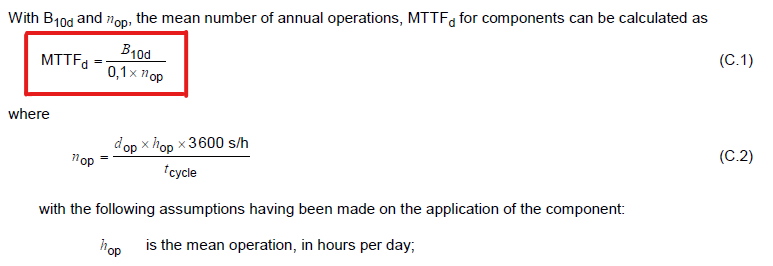
For pneumatic/mechanical/electromechanical components, the manufacturers often only give the mean number of cycles until 10% of dangerous failure of components (*B*10d).

If the criteria below is met, then the MTTFd value for the component can be estimated through calculation.

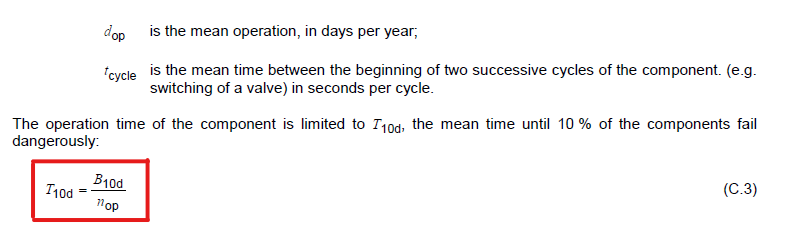
NOTE: Information can be found in data sheet of the component manufacturer.

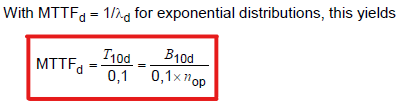
1. Components are manufactured in accordance with ISO 13849-2:2003, Table B.1 or Table D.1 in ISO13849, for the design.
2. Components to be used in category 1, 2, 3, or 4 are manufactured according to the documents listed in a)
3. Manufacturer of components specifies appropriate application and operating conditions for user. Both manufacturer and user have to be informed and responsible for completing a) and b).

If not all the components fail dangerously during the tests using *B*10d, an analysis should be performed on the combination of components.

****

****

****

****

**Data of electrical components**

Tables C.2 to C.7 in ISO 13849 contain values given to electronic components that clarify the MTTFd for each component.

The values given are valid for a temperature of 40°C. When there is doubt for the MTTFd, a worst case value is assigned where the safety margin is 10.

**Passive components**

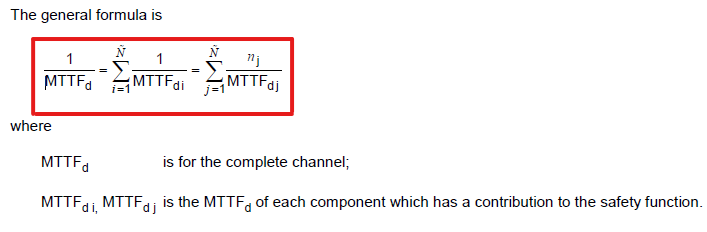
Tables C.4 to C.7 in ISO 13849 contain values given to passive components, e.g. capacitors, resistors, inductors, etc. that clarify the MTTFd for each component.

### Calculations – Channels

**Parts count method**

To estimate the MTTFd for channels, there are several calculation at play depending on which method you choose.

The parts count method estimates the dangerous failure time for each channel separately. All of the single components with MTTFd values are used if they are part of the specific channel.

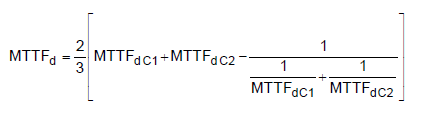


If individual components have the same MTTFd value, they go into the second sum. If the values maintain their individuality, they go into the first sum.

**MTTFd for different channels**

If the channels differ, there are two possibilities:

1. The lower value should be taken into account as worst case situation
2. The equation below should be used as an estimation of a value that can be substituted for MTTFd for each channel



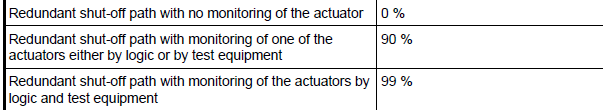
## 2b. Diagnostic Coverage (DC)

For the whole or parts of a safety-related system, a diagnostic coverage can be assigned. The purpose of the diagnostic is to assess the ratio between the failure rate of detected dangers and the total failure rate.

Failure rate [detected] / Failure rate [total]

To estimate DC, consider all relevant faults and/or failure modes, as well as if the PL used on the SRP/CS is enough to be PLR.

### Estimates

In Annex E, Table E.1 of ISO 13948, each aspects of SRP/CS should be referenced when estimating individual DC for functions/modules.

Estimates for:

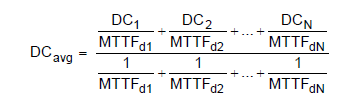
* Input Devices
* Logic
* Output Devices

…will be in table format, with the DC percentages associating with each measure example given.

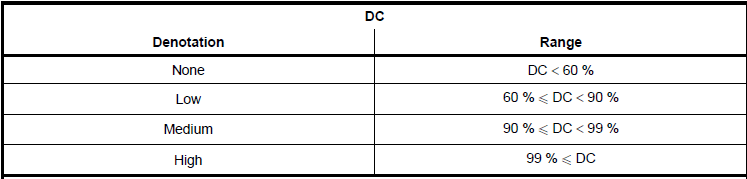
### Calculations of Average (DCavg)

For an estimation of the PL, an average DC needs to be given for the whole SRP/CS performing the safety function.

Since the DC is determined as the ratio between detected failure rate and total dangerous failures, the average adapts the formula into the following:

Components without failure detection (e.g. which are not tested) have DC = 0 and have contribute only to the denominator of DCavg

These are the ranges DC can land on, establishing the denotation level.



# Determine Architecture Category

## The SRP/CS shall be in accordance with the requirements of one or more of the five categories according to the built architecture.

Each category expands on its safety measures and improves resistance to faults as the categories progress.

The categories’ purpose is to state the required behavior of the SRP/CS in respect of their resistance to faults. Improved performance and security warrants increase in category.

The selection of a category for particular SRP/CS may depend on:

* Reduction in risk due to the safety function
* Required Performance level (PLr)
* Tech used
* Risk arising in the case of a fault
* Possibilities of fault avoidance
* Probability of fault occurrence
* MTTFd, DC, CCF

## Categories

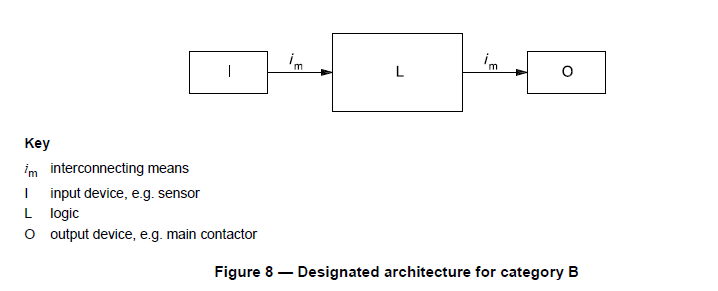
**Category B**

In category B, there is no diagnostic coverage (DCavg = none), low or medium MTTFd for each channel, and no relevance for CCF consideration.

The purpose of a function under this category is that at a minimum, it should be designed and assembled under standard regulations and use safety principles to withstand stresses and harmful influences.

The maximum achievable PL is b.

It should have an input device, output device, logic and interconnection.

****

**Category 1**

The same requirements for category B apply, where instead of basic safety principles they must be “well-tried”, meaning:

1. Widely used in the past with successful results
2. Made and verified using principles which demonstrate its reliability for SRP

The maximum achievable PL is c.

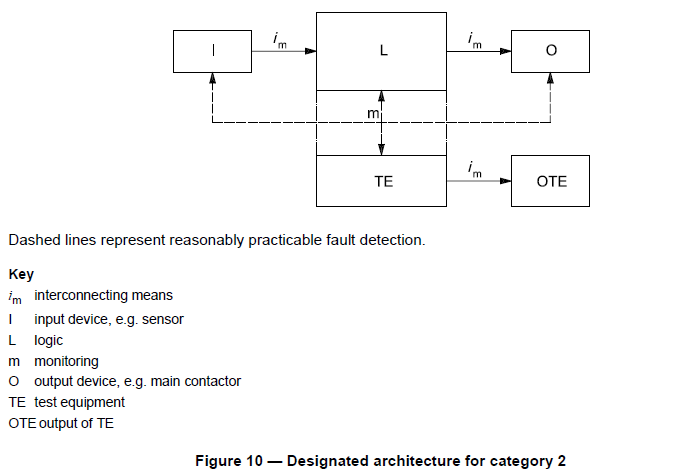
The same diagram as category B applies.

**Category 2**

Category B requirements and “well-tried” safety principles apply to category 2.

In addition, functions will be checked at suitable intervals by the machine control system. The intervals in question are:

* Machine start-up
* Prior to the initiation of any hazardous situation; e.g. start of a new cycle, start of other movements, etc.

The check can be automatic. It must generate an output which initiates appropriate control action if fault is detected, and allow operation if fault is non-existent.

The output of the check should also initiate a safe state when there is a fault, and maintain it until clearance. If it’s not possible to have a safe state, there must be some warning of the hazard.

The maximum achievable PL is d.

There is monitoring and test equipment integrated in the architecture.

**Category 3**

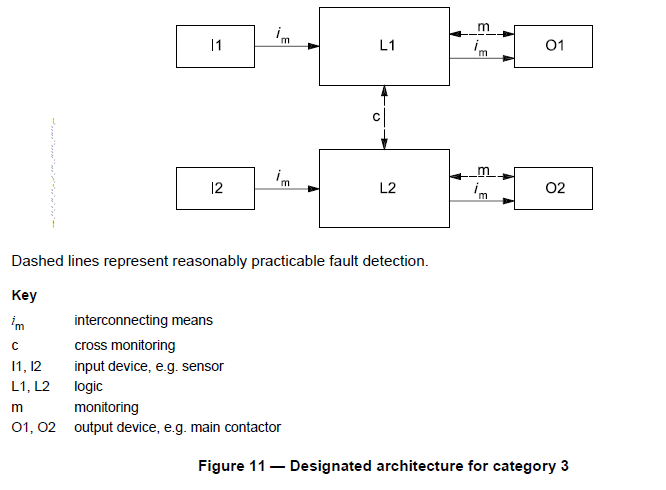
Category B requirements and “well-tried” safety principles apply to category 3.

A single fault in the architecture from the SRP/CS in the third category will not lead to the loss of a safety function. The fault will be detected before the next demand of the safety function.

Not all faults will be detected, so an accumulation of these undetected faults can lead to safety function loss.

The maximum achievable PL is d.

Cross-monitoring is integrated between logical functions.

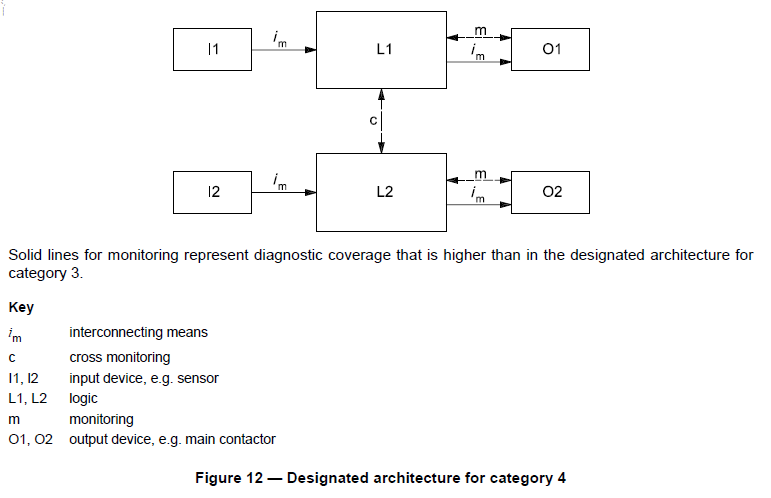


**Category 4**

Category B requirements and “well-tried” safety principles apply to category 4.

Category 3’s single fault detection applies as well. If it is not detected, then it does not lead to a loss of the safety function. If an accumulated amount of undetected faults occurs, it shall not lead to the loss of safety function.

The maximum achievable PL is e.



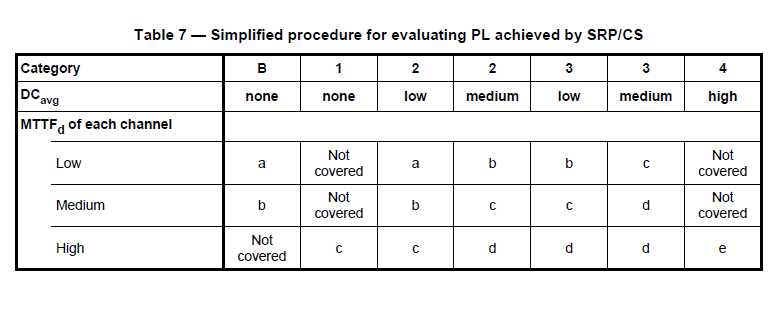
# Determining SIL through PL (Simplified)

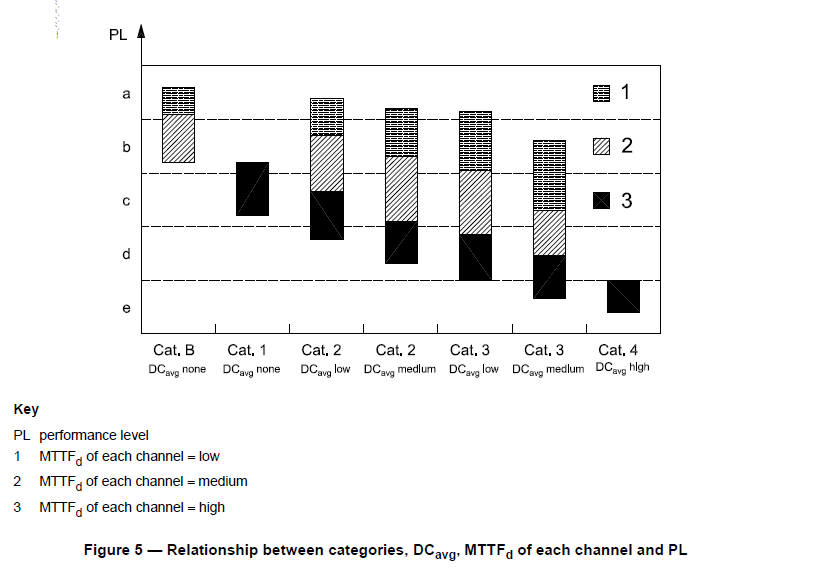
The PL of each SRP/CS depends on the architecture, the mean time to dangerous failure (MTTFd) in each channel and the DCavg.

There are several cases where the PL calculation is not as simple and has more variables/factors at play than the three named above.

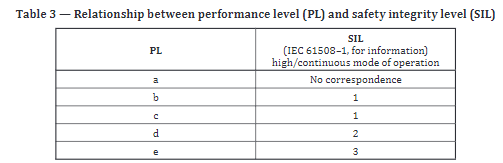
Some of the situations may have a combination of SRP/CS map to a PL (6.3 in ISO), have common cause failures (CCF) taken into account, or have missing qualitative data where relevant parameters should be chosen. Reference ISO 13489 if there is confusion on determining PL.

After determining all three attributes, use one of the figures to map the result to a PL.





Once you have a PL level, use Table 3 below to map the value to a SIL level for the safety function of SRP/CS.



The end result is an estimated level of SIL that can be used to determine the amount of precaution and safety measures to take for an according functionality or SRP/CS.