Automation & Safety Solutions

Safety: The First Priority

Safety Integrity Level (SIL)

www.adico.co
info@adico.co

Table Of Contents

1. Introduction

1.1 Safety related systems in accordance with IEC/EN 61508

The international standard IEC/EN 61508 has been widely accepted as the basis for the specification, design and operation of **S**afety **I**nstrumented Systems (SIS).

As the basic standard, IEC/EN 61508 uses a formulation based on risk assessment: An assessment of the risk is undertaken and on the basis of this the necessary Safety Integrity Level (SIL) is determined for components and systems with safety functions. SIL evaluated components and systems are intended to reduce the risk associated with a device to a justifiable level or "tolerable risk".

1.2 Introduction of safety related systems

This document explores some of the issues arising from the recently published international standards for safety systems, particularly within the process industries, and their impact upon the specifications for signal interface equipment. When considering safety in the process industries, there are a number of relevant national, industry and company safety standards:

- IEC/EN 61511 (user)
- ISA S84.01 (USA) (user)
- IEC/EN 61508 (product manufacturer)

Which need to be implemented by the process owners and operators, alongside all the relevant health, energy, waste, machinery and other directives that may apply. These standards, which include terms and concepts that are well known to the specialists in the safety industry, may be unfamiliar to the general user in the process industries.

In order to interact with others involved in safety assessments and to implement safety systems within the plant it is necessary to grasp the terminology of these documents and become familiar with the concepts involved. Thus the safety life cycle, risk of accident, safe failure fraction, and probability of failure on demand, safety integrity level and other terms need to be understood and used in their appropriate context.

2. Safety Life Cycle

It is seldom, if ever, that an aspect of safety in any area of activity depends solely on one factor or on one piece of equipment. Thus the safety standards concerned here, IEC/EN 61511 and IEC/EN 61508, identify an overall approach to the task of determining and applying safety within a process plant. This approach, including the concept of a Safety Life Cycle (SLC), directs the user to consider all of the required phases of the life cycle. In order to claim compliance with the standard it ensures that all issues are taken into account and fully documented for assessment.

Essentially, the standards give the framework and direction for the application of the overall SLC, covering all aspects of safety including conception, design, implementation, installation, commissioning, validation, maintenance and de-commissioning. The fact that "safety" and "life" are the key elements at the core of the standards should reinforce the purpose and scope of the documents. For the process industries the standard IEC/EN 61511 provides relevant guidance for the user, including both hardware and software aspects of safety systems.

To implement their strategies within these overall safety requirements the plant operators and designers of safety systems, following the directives of IEC/EN 61511 for example, utilise equipment developed and validated according to IEC/EN 61508 to achieve their Safety Instrumented Systems (SIS).

The standard IEC/EN 61508 deals specifically with "functional safety of electrical/ electronic/ programmable electronic safety-related systems" and thus, for a manufacturer of process instrumentation interface equipment, the task is to develop and validate devices following the demands of IEC/EN 61508 and to provide the relevant information to enable the use of these devices by others within their SIS.

The SLC, includes a series of steps and activities to be considered and implemented. Within the SLC the various phases or steps may involve different personnel, groups, or even companies, to carry out the specific tasks. For example, the steps can be grouped together and the various responsibilities understood as identified below.

- **Analytical measures:**

  The first five steps can be considered as an analytical group of activities:

1. Concept
2. Overall scope definition
3. Hazard and risk analysis
4. Overall safety requirements
5. Safety requirements allocation

   And would be carried out by the plant owner / end-user, probably working together with specialist consultants. The resulting outputs of overall definitions and requirements are the inputs to the next stages of activity.

- **Implementation measures:**

  The second group of implementation comprises the next eight steps:

6. Operation and maintenance planning
7. Validation planning
8. Installation and commissioning planning
9. Safety-related systems: E/E/PES implementation (further detailed in Figure 2.3)
10. Safety-related systems: other technology implementation
11. External risk reduction facilities implementation
12. Overall installation and commissioning
13. Overall safety validation

    And would be conducted by the end user together with chosen contractors and suppliers of equipment. It may be readily appreciated, that whilst each of these steps has a simple title, the work involved in carrying out the tasks can be complex and time-consuming.

- **Process operation:**

  The third group is essentially one of operating the process with its effective safeguards and involves the final three steps:

14. Overall operation and maintenance
15. Overall modification and retrofit
16. De-commissioning

    These normally being carried out by the plant end-user and his contractors.

Within the overall safety life cycle, we are particularly interested here in considering step 9 in greater detail, which deals with the aspects of any electrical/electronical/ programmable electronical systems (E/E/PES).

To return to the standards involved for a moment: Following the directives given in IEC/EN 61511 and implementing the steps in the SLC, when the safety assessments are carried out and E/E/PES are used to carry out safety functions, IEC/EN 61508 then identifies the aspects which need to be addressed.

There are essentially two groups, or types, of subsystems that are considered within the standard:

- The Equipment Under Control (EUC) carries out the required manufacturing or process activity.
- The control and protection systems implement the safety functions necessary to ensure that the EUC is suitably safe.

Fundamentally, the goal here is the achievement or maintenance of a safe state for the EUC. You can think of the "control system" causing a desired EUC operation and the "protection system" responding to undesired EUC operation.

Note that, dependent upon the risk-reduction strategies implemented, it may be that some control functions are designated as safety functions. In other words, do not assume that all safety functions are to be performed by a separate protection system.

When any possible hazards are analyzed and the risks arising from the EUC and its control system cannot be tolerated (see section 2.1), then a way of reducing the risks to tolerable levels must be found.

Perhaps in some cases the EUC or control system can be modified to achieve the requisite risk-reduction, but in other cases protection systems will be needed. These protection systems are designated safety-related systems, whose specific purpose is to mitigate the effects of a hazardous event or to prevent that event from occurring.

2.1 Risks and their reduction

One phase of the SLC is the analysis of hazards and risks arising from the EUC and its control system. In the standards the concept of risk is defined as the probable rate of

- occurrence of a hazard (accident) causing harm and
- The degree of severity of harm.

So risk can be seen as the product of "incident frequency" and "incident severity". Often the consequences of an accident are implicit within the description of an accident, but if not they should be made explicit. There is a wide range of methods applied to the analysis of hazards and risk around the world and an overview is provided in both IEC/EN 61511 and IEC/EN 61508.

These methods include techniques such as:

HAZOP: HAZard and **OP**erability study

FME(C)A: Failure **M**ode **E**ffect (and **C**riticality) **A**nalysis

FMEDA: Failure **M**ode **E**ffect and **D**iagnostics **A**nalysis

ETA: Event **T**ree **A**nalysis

FTA: Fault **T**ree **A**nalysis

And other study, checklist, graph and model methods.

This step of clearly identifying hazards and analyzing risk is one of the most difficult to carry out, particularly if the process being studied is new or innovative.

When there is a history of plant operating data or industry-specific methods or guidelines, then the analysis may be readily structured, but is still complex.

The standards embody the principle of balancing the risks associated with the EUC (i. e. the consequences and probability of hazardous events) by relevant dependable safety functions. This balance includes the aspect of tolerability of the risk. For example, the probable occurrence of a hazard whose consequence is negligible could be considered tolerable, whereas even the occasional occurrence of a catastrophe would be an intolerable risk.

If, in order to achieve the required level of safety, the risks of the EUC cannot be tolerated according to the criteria established, then safety functions must be implemented to reduce the risk.

The goal is to ensure that the residual risk – the probability of a hazardous event occurring even with the safety functions in place – is less than or equal to the tolerable risk.

The diagram shows this effectively, where the risk posed by the EUC is reduced to a tolerable level by a "necessary risk reduction" strategy. The reduction of risk can be achieved by a combination of items rather than depending upon only one safety system and can comprise organizational measures as well.

The effect of these risk reduction measures and systems must be to achieve an "actual risk reduction" that is greater than or equal to the necessary risk reduction.

3. Safety Integrity Level (SIL)

As we have seen, analysis of hazards and risks gives rise to the need to reduce the risk and within the SLC of the standards this is identified as the derivation of the safety requirements. There may be some overall methods and mechanisms described in the safety requirements but also these requirements are then broken down into specific safety functions to achieve a defined task.

In parallel with this allocation of the overall safety requirements to specific safety functions, a measure of the dependability or integrity of those safety functions is required.

What is the confidence that the safety function will perform when called upon?

This measure is the safety integrity level or SIL. More precisely, the safety integrity of a system can be defined as "the probability (likelihood) of a safety-related system performing the required safety function under all the stated conditions within a stated period of time."

Thus the specification of the safety function includes both the actions to be taken in response to the existence of particular conditions and also the time for that response to take place. The SIL is a measure of the reliability of the safety function performing to specification.

3.1 Probability of failure

To categorise the safety integrity of a safety function the probability of failure is considered in effect the inverse of the SIL definition, looking at failure to perform rather than success.

It is easier to identify and quantify possible conditions and causes leading to failure of a safety function than it is to guarantee the desired action of a safety function when called upon.

Two classes of SIL are identified, depending on the service provided by the safety function.

- For safety functions that are activated when required (on demand mode) the probability of failure to perform correctly is given, whilst
- For safety functions that are in place continuously the probability of a dangerous failure is expressed in terms of a given period of time (per hour) (continuous mode).

In summary, IEC/EN 61508 requires that when safety functions are to be performed by E/E/PES the safety integrity is specified in terms of a safety integrity level. The probabilities of failure are related to one of four safety integrity levels, as shown in Table below:

Probability of failure		
Safety Integrity Level (SIL)	**Mode of operation – on demand** (average probability of failure to perform its design function upon demand)	**Mode of operation – continuous** (probability of dangerous failure per hour)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

We have seen that protection functions, whether performed within the control system or a separate protection system, are referred to as safety related systems. If, after analysis of possible hazards arising from the EUC and its control system, it is decided that there is no need to designate any safety functions, then one of the requirements of IEC/EN 61508 is that the dangerous failure rate of the EUC control system shall be below the levels given as SIL1. So, even when a process may be considered as benign, with no intolerable risks, the control system must be shown to have a rate not lower than 10^{-5} dangerous failures per hour.

3.2 The system structure

3.2.1 Safe failure fraction

The safe failure fraction (SFF) is the fraction of the total failures that are assessed as either safe or diagnosed/detected. When analyzing the various failure states and failure modes of components they can be categorised and grouped according to their effect on the safety of the device.

Thus we have the terms:

λ_{safe} : Failure rate of components leading to a safe state

$\lambda_{dangerous}$: Failure rate of components leading to a potentially dangerous state

These terms are further categorised into "detected" or "undetected" to reflect the level of diagnostic ability within the device. For example:

λ_{dd} : Dangerous detected failure rate

λ_{du} : Dangerous undetected failure rate

The sum of all the component failure rates is expressed as:

$$\lambda_{total} = \lambda_{safe} + \lambda_{dangerous}$$

And the SFF can be calculated as:

$$SFF = 1 - \lambda_{du} / \lambda_{total}$$

3.2.2 Hardware fault tolerance

One further complication in associating the SFF with a SIL is that when considering hardware safety integrity two types of subsystems are defined. For type A subsystems it is considered that all possible failure modes can be determined for all elements, while for type B subsystems it is considered that it is not possible to completely determine the behavior under fault conditions.

Subsystem type A (e. g. a field transmitter):

- failure mode of all components well defined, and
- behavior of the subsystem under fault conditions can be completely determined, and
- Sufficient dependable failure data from field experience show that the claimed rates of failure for detected and undetected dangerous failures are met.

Safe failure fraction (SFF)	Hardware Fault Tolerance (HFT)		
	0	1	2
<60%	SIL1	SIL2	SIL3
60% … 90%	SIL2	SIL3	SIL4
90% … 99%	SIL3	SIL4	SIL4
>99%	SIL3	SIL4	SIL4

Subsystem type B (e. g. a logic solver):

- the failure mode of at least one component is not well defined, or
- behavior of the subsystem under fault conditions cannot be completely determined, or
- Insufficient dependable failure data from field experience show that the claimed rates of failure for detected and undetected dangerous failures are met.

Safe failure fraction (SFF)	Hardware Fault Tolerance (HFT)		
	0	1	2
<60%	Not allowed	SIL1	SIL2
60% … 90%	SIL1	SIL2	SIL3
90% … 99%	SIL2	SIL3	SIL4
>99%	SIL3	SIL4	SIL4

These definitions, in combination with the fault tolerance of the hardware, are part of the "architectural constraints" for the hardware safety integrity as shown in Tables.

Note that although mathematically a higher reliability might be calculated for a subsystem it is this "hardware safety integrity" that defines the maximum SIL that can be claimed.

In the tables above, a hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function. For example, if a subsystem has a hardware fault tolerance of 1 then 2 faults need to occur before the safety function is lost.

3.2.3 Connecting risk and safety integrity level

Already we have briefly met the concepts of risk, the need to reduce these risks by safety functions and the requirement for integrity of these safety functions.

One of the problems faced by process owners and users is how to associate the relevant safety integrity level with the safety function that is being applied to balance a particular risk. The risk graph shown in the Figure below, based upon IEC/EN 61508, is a way of achieving the linkage between the risk parameters and the SIL for the safety function.

Risk Parameters:

Consequence (severity)

C_1 minor injury or damage

C_2 serious injury or one death, temporary serious damage

C_3 several deaths, long-term damage

C_4 many dead, catastrophic effects

Frequency/exposure time

F_1 rare to quite often

F_2 frequent to continuous

Possibility of avoidance

P_1 avoidance possible

P_2 unavoidable, scarcely possible

Probability of occurrence

W_1 very low, rarely

W_2 low

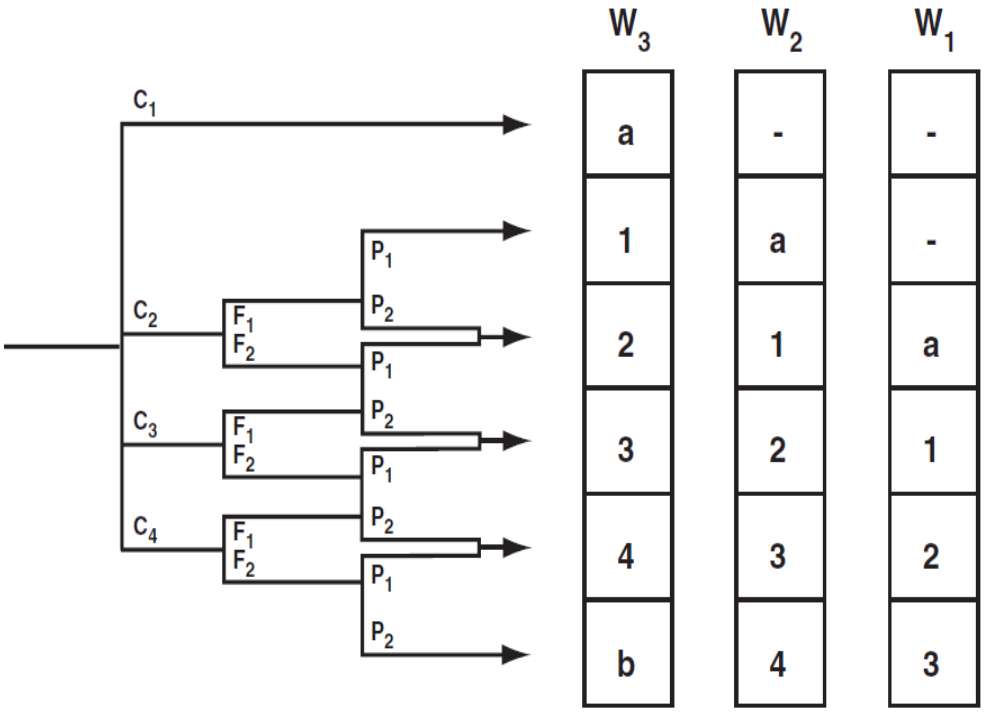
W_3 high, frequent

1, 2, 3, 4 = Safety integrity level

- = Tolerable risk, no safety requirements

a = No special safety requirements

b = A single E/E/PE is not sufficient



For example, with the particular process being studied, the low or rare probability of minor injury is considered a tolerable risk, whilst if it is highly probable that there is frequent risk of serious injury then the safety function to reduce that risk would require an integrity level of three.

4. Probability of failure

4.1 Overview

An important consideration for any safety related system or equipment is the level of certainty that the required safe response or action will take place when it is needed. This is normally determined as the likelihood that the safety loop will fail to act as and when it is required to and is expressed as a probability.

The standards apply both to safety systems operating on demand, such as an emergency shut-down (ESD) system, and to systems operating "continuously" or in high demand, such as the process control system. For a safety loop operating in the demand mode of operation the relevant factor is the PFD_{avg}, which is the average probability of failure on demand. For a continuous or high demand mode of operation the probability of a dangerous failure per hour (PFH) is considered rather than PFD_{avg}.

Obviously the aspect of risk that was discussed earlier and the probability of failure on demand of a safety function are closely related.

Using the definitions

F_{np} : frequency of accident/event in the absence of protection functions

F_t : tolerable frequency of accident/event

Then the risk reduction factor (ΔR) is defined as:

$\Delta R = F_{np} / F_t$

Whereas PFD is the inverse:

$PFD_{avg} = F_t / F_{np}$

Since the concepts are closely linked, similar methods and tools are used to evaluate risk and to assess the PFD_{avg}.

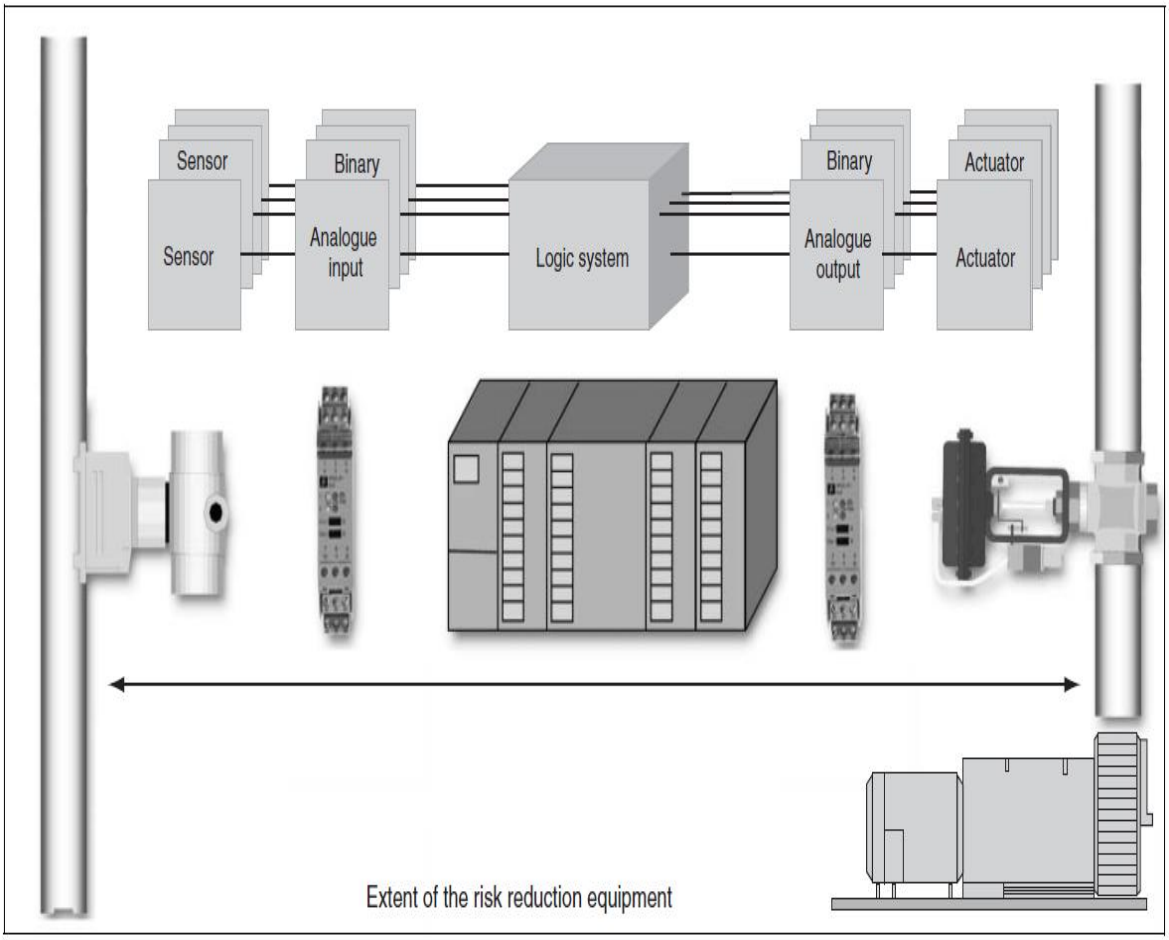
4.2 Safety loop example

Let us summarise these points in a simple example from the processing industry. The IEC/EN 61508 standard states that a safety integrity level can be properly associated only with a specific safety function – as implemented by the related safety loop – and not with a stand-alone instrument or piece of equipment.

In our context, this means that – strictly speaking – it is only possible to state the compliance with the requirements of a specific SIL level after having analysed the whole safety loop.

It is however possible – and sensible – to analyse a single building block of a typical safety loop and to provide evidence that this can be used to finally obtain a SIL-rated safety loop. Since all the elements of a safety loop are interdependent in achieving the goal it is relevant to check that each piece is suitable for the purpose. For our example we will consider a single electronic isolator component.

Within the context of this example, the safety loop is a control system intended to implement a safety function. In the Figure below, a typical safety loop is shown, including Intrinsically Safe signal input and output isolators for explosion protection and let us assume that the safety integrity level required has been determined as SIL2. This is for reference only, and doesn't imply that a full safety loop assessment has been performed.

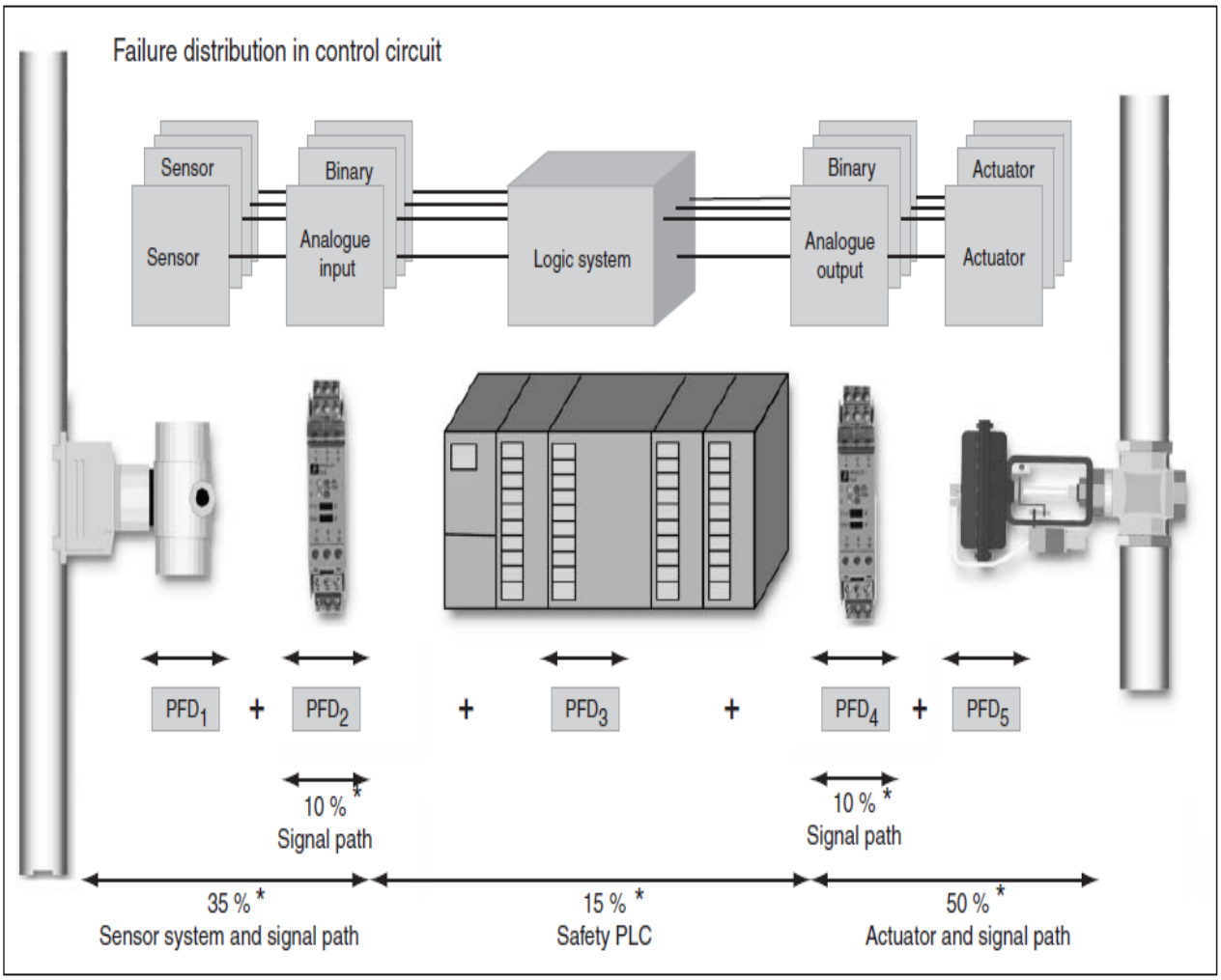


You can identify the various elements of the process loop

- Input sensor,
- Input line/input isolator block,
- Logic system (Logic solver, required to trigger the safety function),
- Output line/output isolator block (safe out) and finally
- Control valve (required to implement the safety function)

Considering that the typical safety loop as shown is made of many serially connected blocks, all of which are required to implement the safety function, the available PFD budget ($< 10^{-2}$ as for SIL2) has to be shared among all the relevant blocks.

For example, a reasonable, rather conservative, goal is to assign to the isolator no more than around 10 % of the available PFD budget, resulting in a PFD limit – at the isolator level – of around 10^{-3}, that is to say, 0.1 %. It should be clear, however, that this figure is only a reasonable guess, and doesn't imply that there is no need to evaluate the PFD at the safety loop level or that the isolator contribution can be neglected.



The PFD value for the complete safety device is calculated from the values of the individual components. Since sensors and actuators are installed in the field, these are exposed to chemical and physical loading (Process medium, pressure, temperature, vibration, etc.). Accordingly, the risk of faults is high for these components. For this reason 25 % of the overall PFD is assigned to the sensors and 40 % to the actuators. Thus 15 % remains for the fault tolerant control system and 10 % each for the interface modules (the interface modules and control system have no contact with the process medium and are housed in the protected control room).

References:

1. Safety Integrity Level Manual, by Pepperl + Fuchs. Part No. 180663 10/07 01.
2. Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques Part 1. ISA-TR84.00.02-2002 – Part 1. Approved 17 June 2002.
3. Understanding Safety Integrity Level, by Magnetrol. February 2009.