Universidad Carlos III de Madrid
www.uc3m.es

END OF BACHELOR WORK

TITLE: Optimization of safe introduction of the mixture air + fuel into an industrial boiler, complying with the SIL2 safety level.

AUTHOR: Jorge Fuentes Lozano

DEGREE: Bachelor in Industrial Electronics and Automatics

PROFESSOR: Enrique San Millán Heredia

DATE: 20 - June - 2014

CONTENTS

FIGUERES INDEX

1. INTRODUCTION

1.1. Industrial Boilers

Industrial boilers are mainly used in the industries of energy and oil&gas, concretely in refineries and thermal or solar power stations, in order to boil water and use the resultant steam to make the turbines rotate so that electricity is produced.

This process of boiling water involves a combustion that has to be both safe and efficient. This means that a control of the mixture air-fuel has to be carried out: the less amount of gas per unit of amount of air, the less efficient the combustion is; but an excess of fuel in the mixture can produce an uncontrolled burst that could cause an accident.

Traditionally, when developing the control system of a boiler, the actions of modulating itself would be developed with analog equipments (continuous). The start and stop sentences, as well as interlocks, are digital (all/nothing) that might imply digital equipments. Nowadays, due to advances in microprocessor-based systems, it is possible to achieve safety function with analog equipments that permit to evaluate different setting points in a unique device as well as provide a continuous measure of the variables in the whole operating range.

In order to develop a control application is needed to understand three basic targets:

- Make the boiler provide a continuous supply of steam in the required conditions of pressure and temperature.

- Operate continuously the boiler in the less cost of fuel possible, keeping a high safety level.

- Start and stop in a safety way, watch and detect insecure conditions and make the necessary decisions to a safe operation every time.

The two first targets would be carried out by an analog control, while the third one would be work of the safety system and burners management.

A basic diagram of a boiler could be represented as shown in the figure below:

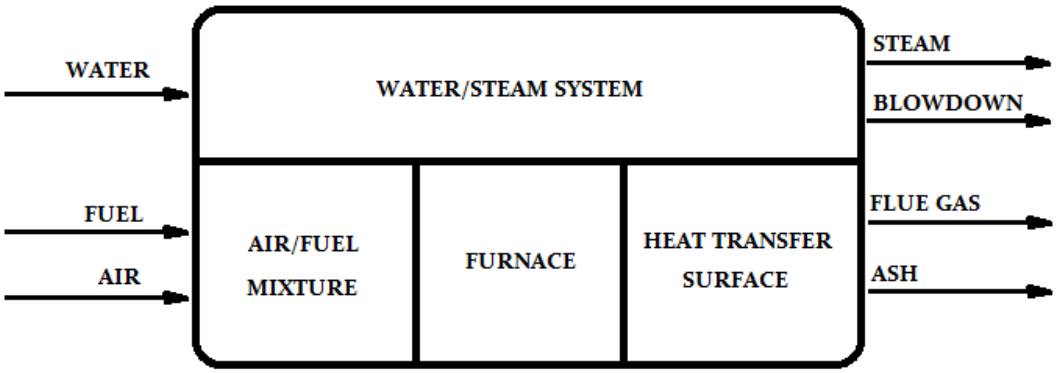

Figure 1: Basic diagram of a boiler

In this figure we can observe that fuel and air are mixed up in order to be burned inside the furnace. The furnace consists of walls of water pipes that receive the radiant heat from the flame, where the maximum heat transfer is produced. The resultant combustion gases are cooled up and they exit the furnace, passing to the heat recovery area.

The optimum air-fuel ratio is marked by each fuel by a percentage of oxygen excess and CO_2 at flue gas outlet. While the percentage of O_2 is unique and valid as an unequivocal rating of combustion quality, the CO_2, as we can see in the figure below, could have the same value in optimum or unsafe conditions, so its use as a variable of the main process is discarded and it is only used as a secondary variable. Higher O_2 concentration than required will cause cold combustion, lower O_2 concentration will cause unburned fuel that could ignite unexpectedly. Consequently the correct design and adjustment of the combustion control will assure both safe and efficient operation.

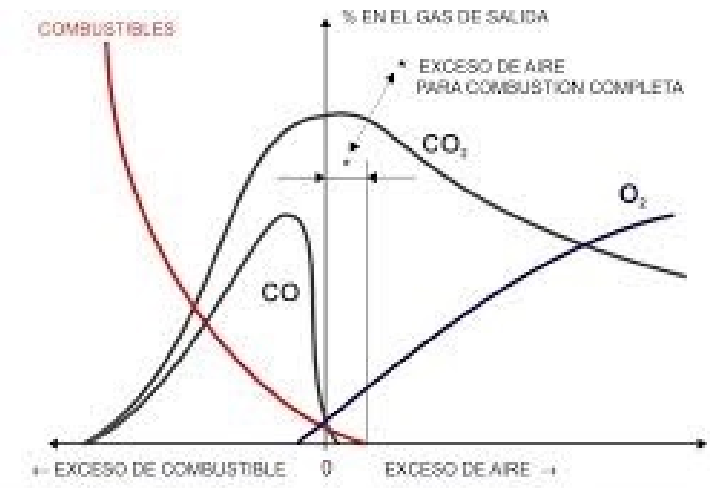

Figure 2: Air-fuel ratio diagram

On the other hand, the unburned rating in the combustion is defined by the existing CO in the gases. The increase of the level of CO in the gases is an indicative of the incompleteness of the combustion which means also reduction in plant efficiency. [1]

1.2 Industrial safety: safety systems and PLC

The control and safety systems needed for the mixture of air and gas should satisfy the safety specifications detailed in the industries standards, as there is no specific normative for this scope. In this case, the standard that regulates the safety instrumented systems for the process industry sector is the IEC 61511. This standard names this kind of systems as SIS (Safety Instrumented System).

In this standard, between other many considerations, a description of the different Safety Integrity Levels (SIL) is given. These levels are discrete (from 1 to 4) and have to be calculated taking into account the individual SILs of all devices involved in the SIF (Safety Integrated Function), that is to say sensors, programmable logic, and actuators.

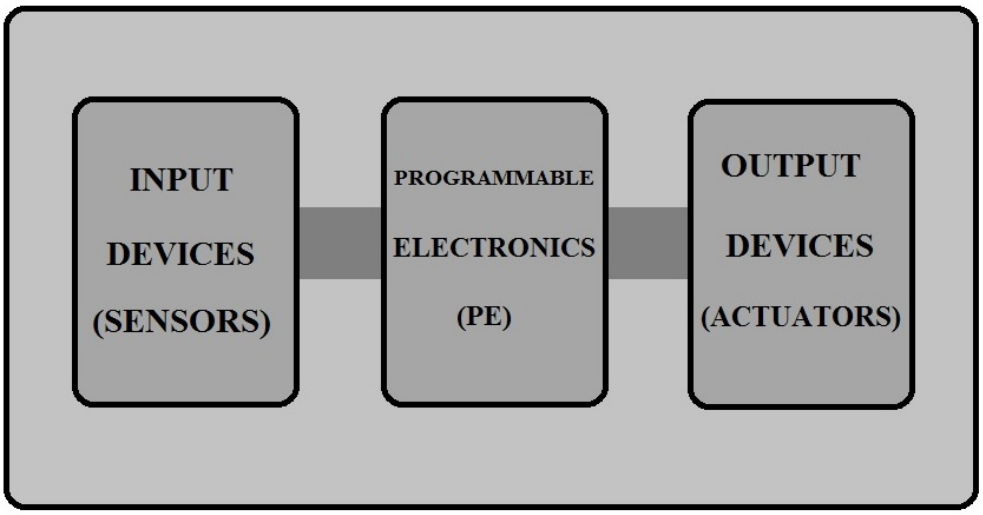

Figure 3: Basic diagram of a SIF

Safety Systems

Safety systems are designed to protect people, equipment and environment to conditions that may be hazardous. In these cases they must act immediately carrying plant or equipment to a safe position.

The IEC technical committee examined 34 accidents which were the direct result of failures in the systems of control and safety in different industries, in which results are the following:

- Specifications: 44%
- Changes after commissioning: 20%
- Operation and maintenance: 15%
- Design and implementation: 15%
- Installation and commissioning: 6%

These results show that almost half of the errors were due to incorrect specifications. As a consequence of this study, the Committee established some general requirements and strategies in order to obtain the functional safety for safety instrumented systems. These requirements have to be taken into account in each of the 16 steps of the safety global lifecycle:

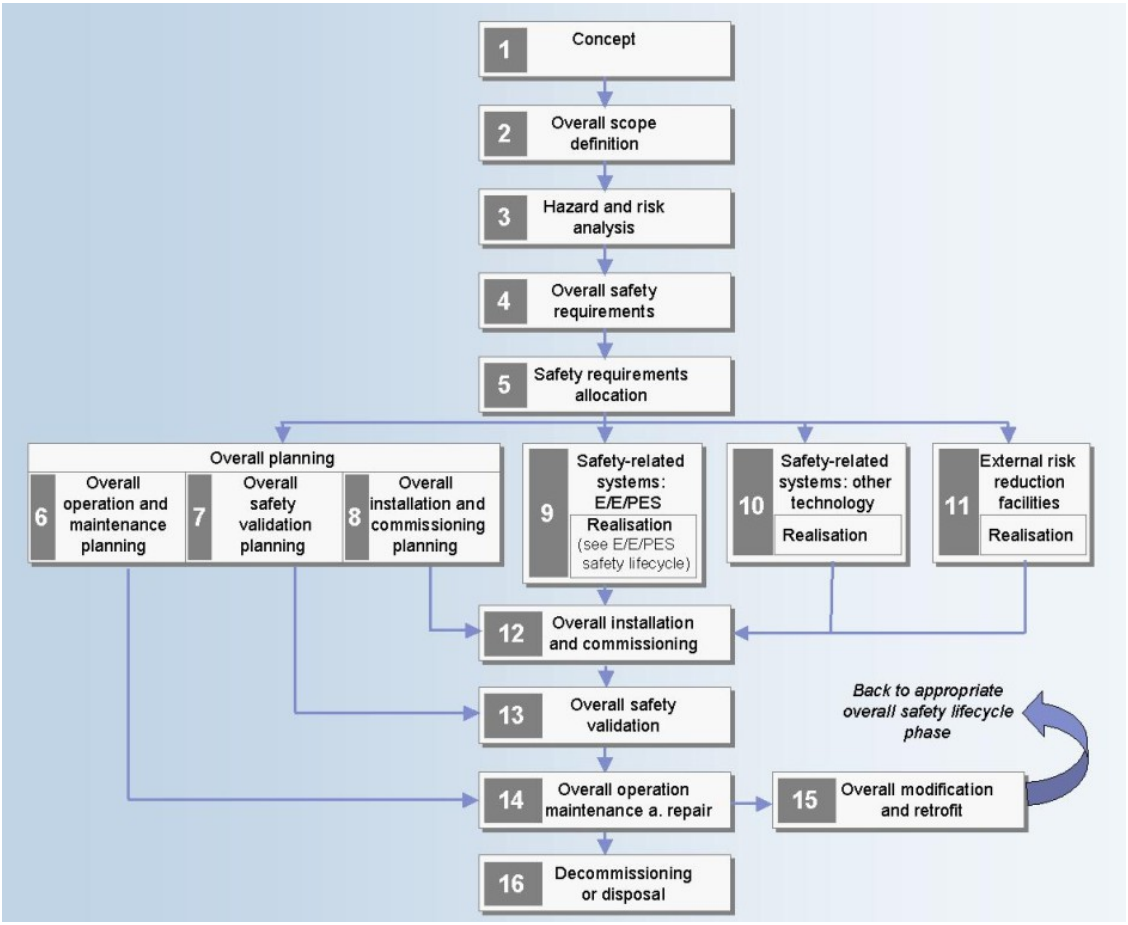

Figure 4: Safety global lifecycle

The IEC 61511 standard defines the concepts of SIS, SIF and SIL as following:

- **Safety Instrumented System (SIS):** Instrumented system used to implement one or more safety instrumented functions. An SIS is composed of any combination of sensors, logic solvers, and final elements.

- **Safety Instrumented Function (SIF):** Safety function with a specified safety integrity level which is necessary to achieve functional safety and which can be either a safety instrumented protection function or a safety instrumented control function.

- **Safety Integrity Level (SIL):** discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems. Safety integrity level 4 has the highest level of safety integrity; safety integrity level 1 has the lowest.

Technology Selection

Each one of them has advantages and disadvantages. It depends on many factors: budget, size, level of risk, flexibility, maintenance, interface requirements and communications, safety, etc..

Concretely, PLC-based systems offer many advantages: low cost, communication capabilities and interfaces, graphics for the operator and self-documenting, among others. Most PLCs are not designed with sufficient capacity to self and are not recommended for safety applications SIL2 or SIL3. The absence of self-diagnosis is the weak point of most of PLCs in safety applications

There are many differences between a Standard PLC, general purpose, and a safety PLC. The following are the most important.

PLC fail-safe	Standard PLC
Meets strict standards of safety system design such as IEC61508, NFPA, FM.	Does not meet any safety standard.
Certified by prestigious institutions such as TÜV competent.	The absence of a labor self diagnostics require extra maintenance frequent testing sometimes requires system shutdown.
Self-diagnostic routines incorporate all hardware and software that detect any dangerous internal failure (> 99%).	The dangerous failure "hidden" not detected, so that dangerous situations can occur. They are not safe from failure.
The fault is guaranteed safe situation if any internal component failure.	Examples of undetected dangerous failures: Output short circuit, memory loss or corruption of data transfer or internal bus, blocking of I / O to state "1" or "0", the CPU failures, etc.
The changes are automatically self-documented so errors are minimized.	
[1] [2]	

1.3 IEC and IEC 61511 standard

The object of the IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. The IEC meets an international consensus of opinions on the relevant subjects since each technical committee has representation from all interested National Committees.

Concretely, the International Standard IEC 61511 had been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement and control.

This International Standard gives requirements for the specification, design, installation, operation and maintenance of a safety instrumented system (SIS), so that it can be confidently entrusted to place and/or maintain the process in a safe state. This standard had been developed as a process sector implementation of IEC 61508.

In particular, this standard:

- Specifies the requirements for achieving functional safety but does not specify who is responsible for implementing the requirements.

- Applies when equipment that meets the requirements of IEC 61508, or of 11.5 of IEC 61511-1, is integrated into an overall system that is to be used for a process sector application.

- Defines the relationship between IEC511 and IEC61508.

- Applies when application software is developed for systems having limited variability or fixed programs.

- Applies to a wide variety of industries within the process sector including chemicals, oil refining, oil and gas production, pulp and paper, non-nuclear power generation.

- Outlines the relationship between safety instrumented functions and other functions.

- Specifies for system architecture and hardware configuration, application software, and system integration.

- Defines requirements for implementing safety instrumented functions as a part of the overall arrangements for achieving functional safety.

- Uses a safety life cycle and defines a list of activities which are necessary to determine the functional requirements and the safety integrity requirements for the safety instrumented systems.

- Requires that a hazard and risk assessment is to be carried out to define the safety functional requirements and safety integrity levels (SIL).

- Establishes numerical targets for average probability of failure on demand and frequency of dangerous failures per hour for the safety integrity levels.

- Specifies minimum requirements for hardware fault tolerance (HFT).

- Specifies techniques/measures required for achieving the specified integrity levels.

- Defines a maximum of performance (SIL 4) and a minimum of performance (SIL 1) which can be achieved for a safety instrumented function.

- Provides a framework for establishing safety integrity levels but does not specify the safety integrity levels required for specific applications.

- Defines the information that is needed during the safety life cycle.

- Does not place any direct requirements on the individual operator or maintenance person.

[3]

1.4 Project Targets:

- Find the source of the problem

- Investigate the available technology and design industry standards to develop an optimized design.

- Solve the problem:

  - Examining required the level of safety depending on the severity of the hazard and the consequences of accidents.

  - Evaluate devices and replace the failed ones to be able to mitigate the consequences that could cause the accident.

  - Develop an integrated safety system that meets the required safety level risk analysis (HAZOP).

  - Quantitatively and qualitatively verify the validity of the safety system intended.

2. BACKGROUND

2.1 Problem to be solved explanation

This project is designed to cover an actual technical necessity in the alumina refinery of Aughinish located in Limerick (Ireland), whose boiler was designed by Foster Wheeler. The client, Rusal, noticed and accident carried out in this boiler and a team of experts investigated what happened.

The boiler had experimented an explosion and the experts determined that it was caused by an error in the air/fuel mixture inside the boiler. The figure below shows the main elements of the boiler.

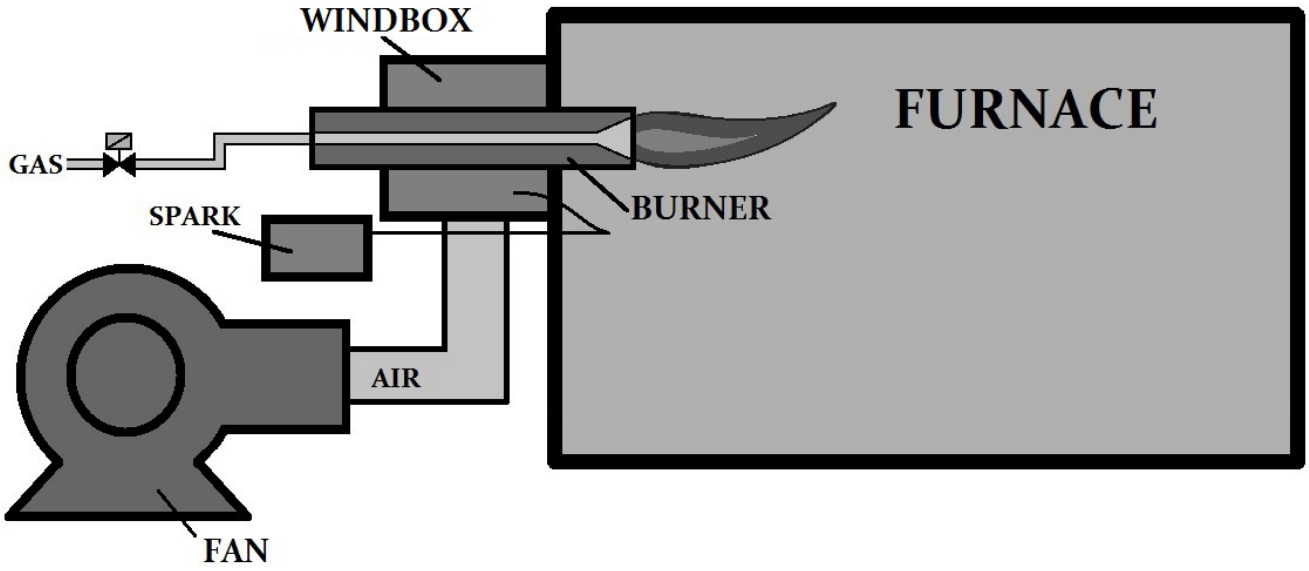

Figure 5: Boiler basic diagram

2.2 ¿Why did this happen?

What the experts committee concluded was that the air flowmeter performed an incorrect measurement of the air that was getting into the furnace, showing a quantity lower than the actual air getting inside. This fact made the system to put into the furnace more gas than required, storing a gasbag inside it. Then, the flowmeter noticed its own error and introduced an air jet, which reacted with the stored gasbag, causing the explosion.

In Annex 5 we can observe the different optimal amounts of fuel and air per percentage of maximum load. In other words, the graphics in this annex show the most suitable mixture of air and gas in different behaviors of the boiler. We can see that the optimal gas ratio at 23% boiler load is 4,78%, and 5,80% at 100% load. Then, it can be considered that the boiler is operating properly at 5,5% gas ratio considering an approximation for every percentage of maximum load. Foster Wheeler's engineers consider that the air/fuel mixture starts to be consider hazardous when the gas ratio overcomes 7% in order to have a 1,5% margin of fuel excess, so as not to stop the boiler in case the flow in the gas pipe increases.

Therefore, this accident was caused by two main factors: the impossibility of the system to recognize its measurement errors, and the little margin of actuation of the system for avoiding an accident in case an error occurred.

Steps of the accident

1. The boiler was operating in its regular behavior, burning 8581 Kg/h of gas, which implies 148906 Kg/h of air.

2. An increase of load until 12302Kg/h of gas within the next 2 minutes is produced. The measurement of air is less increased than what flowmeter shows.

3. Load stays stable in the mentioned value, but too much gas is being introduced than it could be all burned by the available air.

4. The measurement of air returns to be correct and the amount of air in the furnace increases, which produces the sudden combustion of a great amount of unburned gas.

2.3 How problem could be solved

Once we have defined the problem, we are going to analyze several ways to solve it. Hereunder, the most reasonable ones are described in detail.

The former system consisted of the following elements:

- A flowmeter for the measurement of the gas entering the boiler.
- A flowmeter for the measurement of the air entering the boiler.
- An electro-pneumatic positioner for the regulation of the gas entering the boiler.

- A damper for the regulation of the air entering the boiler, governed by a pneumatic actuator activated by an electro-pneumatic positioner.
- A PLC for the regulation of all the system (valves actuation as a function of the flowmeters measurements).

The functionality of the above mentioned elements shall be optimized in a safety way in order to avoid the future recurrence of the problem.

2.3.1 Increasing maintenance works

The maintenance works of the elements of the system carried out in the plant were those whose manufacturers recommended. However, the study has concluded that if this maintenance would be more frequent, the probability of the occurrence of the accident would have been lower.

Therefore, one solution for the problem could consist of the following actions:

- Carrying out an exhaustive inspection of all the elements in order to check its capability to continue working properly.
- Getting rid of the damaged elements and substituting them by new elements with the same characteristics.
-
- Checking the performance of the whole system once installed and energized (Site Acceptance Test and Commissioning).
-
- Once the system is working as before the accident, the proposed solution would consist of:
-
- Increasing the maintenance personnel in order to reduce the time between the functional tests to be performed in each element.
-
- Substituting the elements that are damaged or suspect to fail, instead of trying to repair them. In other words, trying to have the elements new at any time.
-

The proposed solution has the following advantages and disadvantages:

Advantages:

-It reduces risk although does not assure functional safety.
-It is a very easy solution to be implemented.

Disadvantages:

-A lot of personnel would have to be contracted and some elements would be occasionally purchased.

-The system design keep being unsafe, and therefore more accidents can be caused. This solution merely tries to mitigate a very gauffer system by increasing maintenance works.

2.3.2 Increasing process safety margin

As shown in the attached tables of Annex 5, the air/fuel mixture in a normal performance of the boiler is around 94,5% air – 5,5% fuel.

The former safety system was design following a very basic solution. This system triggered an emergency signal which cut off the gas valve when the air and gas flowmeters stated that the mixture had a 7% of gas, which is considered to be hazardous.

Therefore, one solution for the problem would be to increase the air/fuel rate that enters the boiler, increasing the process safety margin. In order not to get a too much inefficient combustion, but obtaining a considerable risk reduction, the air/fuel mixture entering the boiler could be modified to 96,5% air – 3,5% fuel. Therefore, we would have a 3,5% process safety margin of gas entering the boiler.

This solution has the following advantages and disadvantages:

Advantages:

-The risk situation is more unlikely because it is a very remote situation of performance of the system.

- It is the cheapest solution in terms of implementation. The only costs are those related to the reprogramming of the corresponding PLC.

Disadvantages:

- Although the implementation costs are very low, this solution is the most expensive one for the customer, inasmuch as the combustion is more inefficient. The more air is introduced in the boiler, the colder the flame gets.

-Although the probability of the risk occurring is reduced, it remains being an unsafe system and the system itself does not detect any hazard.

2.3.3 Increasing equipment functional safety

As stated in 2.2, the failure in the system was produced by an incorrect measurement of the air entering the boiler and the no-existence of a system detecting such an error. This error was a random error that happened among a wide variety of possible errors in the system, taking into account that any of the elements of the list above, except the PLC, comply with the IEC 61511 and IEC 61508 standards.

Therefore, what is broadly needed to be modified in the system are flowmeters and actuators, and the way they are installed. Besides, the new Safety Instrumented Function includes a 2 ways / 2 positions electro-pneumatic valve that cuts off the supply of gas when an error occurs.

For the air measurement, a venturi tube is needed. This necessity comes from the fact that a device for the measurement of the flow does not exist per se. The venturi tube is based on the Benouilli's principle.

This principle states that an increase in the speed of the fluid occurs simultaneously with a decrease in pressure, as the following formula shows:

$$\frac{v^2}{2} + gz + \frac{p}{\rho} = \text{constant}$$

where:

v is the fluid flow speed at a point on a streamline,

g is the acceleration due to gravity,

z is the elevation of the point above a reference plane, with the positive z-direction pointing upward – so in the direction opposite to the gravitational acceleration,

p is the pressure at the chosen point, and

ρ is the density of the fluid at all points in the fluid. [4]

Therefore, in our system, we need a device (Venturi Tube) that could modify the value of any of those variables that could perform an equivalent variation on the flow value. In this case, as shown in the figure below, the fluid has to pass through a tube of a diameter D, and then trough a diameter d, thinner than D, which makes the fluid increase its pressure and flow.

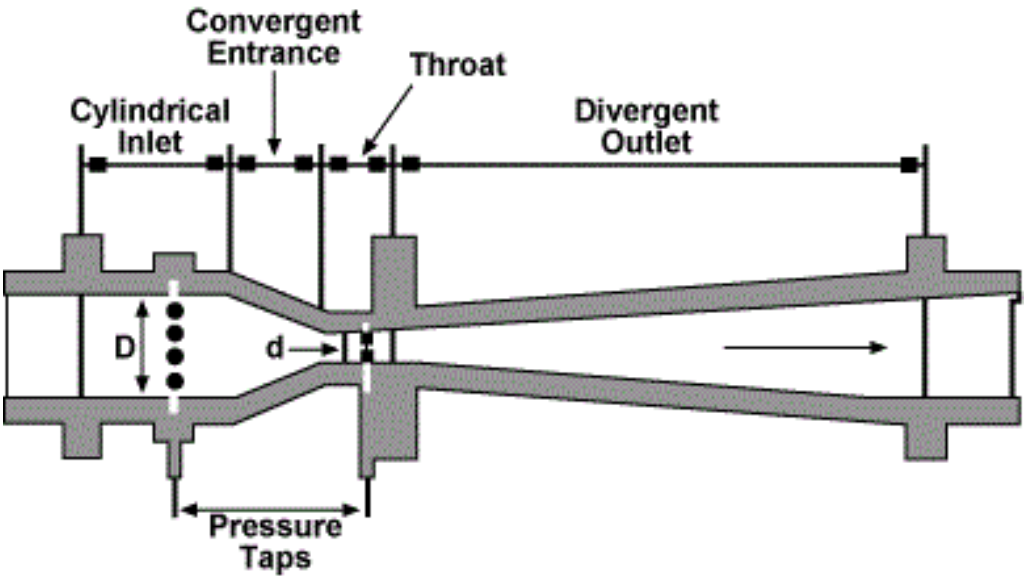

Figure 6: Venturi Tube graphic

As a consequence, we can measure the differential pressure at the ends of the tube and, using Benuilli's principle, we can compute the flow measurement. [5]

This solution has the following advantages and disadvantages:

Advantages:

-It is the safest system by far. Although a risk situation is reached, it is very unlikely that the system does not detect it, and, once detected, it is very unlikely that it does not mitigate it.

-The client only has to make an investment in the implementation of the new system. It would not have to face additional maintenance or inefficient-performance-related costs.

Disadvantages:

-A technically complex designed is required to be carried out.

2.3.4 Selection of the most suitable solution

The selected solution for the proposed problem will be the explained in header 2.3.3, inasmuch as it is the most economical solution for the client in the long term and it is the safest by far.

2.4 Project Planning

For the time being, we have defined the problem, identified the causes, proposed different solutions, and chosen the most appropriate one, according to the related standard of functional safety (IEC 61511).

Our target now is to define which are going to be the next steps in order to execute this solution, under the guidance of the mentioned standard. IEC61511 defines the safety lifecycle (see figure 4), that is to say, the necessary steps to be followed in order to achieve functional safety required in the project. However, this project only covers one specific safety function inside the whole safety instrumented system of an existing plant. For this reason, most of the steps indicated in this safety cycle does not apply in this project.

The necessary steps to be followed in the execution of the project are listed hereunder:

- Overall explanation of the IEC61508 and IEC61511.
- Description of boiler elements involved in the project
- State the risk evaluation, using the HAZOP method.
- Definition of the required SIL level, considering the characteristics of the evaluated risk.
- Assignation of the required safety instrumented function to its risk.
- Definition of the safety instrumented system requirements.
- Safety instrumented system design.
- Calculations for verification the required SIL level.

3. REGULATORY FRAMEWORK: IEC61508 AND IEC61511

In 1998 the IEC, which stands for International Electrotechnical Commission published a document, IEC 61508, entitled: "Functional safety of electrical/electronic/programmable electronic safety-related systems". This document sets the standards for safety-related system design of hardware and software. IEC 61508 is generic functional safety standard, providing the framework and core requirements for sector specific standard. Three sector specific standards have been released using the IEC 61508 framework, IEC 61511 (process), IEC 61513 (nuclear) and IEC 62061 (manufacturing). IEC 61511 provides good engineering practices for the application of safety instrumented systems in the process sector. [3]

In the United States ANSI/ISA 84.00.01-2004 was issued in September 2004. It primarily mirrors IEC 61511 in content with the exception that it contains a grandfathering clause:

For existing safety instrumented systems (SIS) designed and constructed in accordance with codes, standards, or practices prior to the issuance of this standard (e.g. ANSI/ISA 84.01-1996), the owner/operator shall determine and document that the equipment is designed, maintained, inspected, tested, and operated in a safe manner. [6]

The European standards body, CENELEC, has adopted the standard as EN 61511. This means that in each of the member states of the European Union, the standard is published as a national standard. For example, in Great Britain, it is published by the national standards body, BSI, as BS EN 61511. The content of these national publications is identical to that of IEC 61511. Note, however, that 61511 is not harmonized under any directive of the European Commission.

IEC 61511 covers the design and management requirements for SISs from cradle to grave. Its scope includes: initial concept, design, implementation, operation, and maintenance through to decommissioning. It starts in the earliest phase of a project and continues through startup. It contains sections that cover modifications that come along later, along with maintenance activities and the eventual decommissioning activities.

The standard consists of three parts:

- Framework, definitions, system, hardware and software requirements
- Guidelines in the application of IEC 61511-1
- Guidance for the determination of the required safety integrity levels

4. BOILER ELEMENTS

4.1 Forced draft fan

This device supplies the required air flow in the combustion. The fan its calculated so that it gives 0 pressure in the fund of the smokestack in conditions of nominal load.

The movement of these fans could be performed by a motor or by the steam-turbine.

Figure 7: Forced draft fan

4.2 Windbox

Air enters a box called windbox. In this area are the guns, burners, flame detectors and registers. These registers are the equipment surrounding the burners causing air turbulence so that the fuel to burn properly.

4.3 Flame detectors

Flame detectors are devices used to confirm the presence of flame inside the boiler furnace when burners are firing. Ultra-violet and infra-red optics are the most common principles of measurement for this purpose. By

this way, a wide range of colors of flames can be detected with these instruments, which allows installing these equipments for any kind of fuel.

Figure 8: Flame detector

4.4 Economizer

It handles the cooling of the hot air from the furnace, transferring its heat to the water of the steam-water circuit.

4.5 Evaporator

It handles the warming of the water coming from the economizer up to the boiling point temperature.

4.6 Superheater

It handles the heating of the steam generated in the boiling process up to the temperature that assures the absence of water, what is called superheated steam.

4.7 Stack

It handles the exhaust gases to the atmosphere by creating a slightly negative pressure at the stack outlet.

4.8 Instrumentation

The instruments would be placed in:

- Pressure and temperature variation points (e.g.: before and after a fan, before and after a heat exchanger)
- Safety points as:

  a) Furnace pressure: in this zone, pressure cannot be higher than the pressure that was designed.

  b) Oxygen excess in the stack: it is necessary to control the fuel air flow for ensuring a proper burning.

4.9 Venturi tube

The Venturi tube allows flow measurement with an accurate 60% higher than the orifice plate in the same conditions, and with a pressure drop of only 10 or 20% of the created differential pressure. It possesses great accuracy and allows the passage of fluids with a relatively large percentage of solids, although abrasive solids influence how they affect the accuracy of the measurement.

For the calculation of the diaphragms, nozzles, Venturi tubes and various standards are used, among which are the following:

- ISO 5167-1980. Measuring fluid flow through-orifice plates, nozzles or Venturi tubes inserted in circular section
- ASME 19.5 standard - Flowmeter Computation Handbook.
- A.P.I 2530 standard - September, 1985 for natural gas.
- Principle and Practice of Flow Meter Engineering L.K. Spink (1978).
- AGA-3 and AGA-7 - Gas Measurement Committee Report - American Gas Association, Cleveland, Ohio.

[7]

5. SAFETY SPECIFICATIONS AND SIL STUDY

5.1 Generalities

Throughout a safety system, all hazardous situations have to be taken into account and, for each of them, there should exist a mechanism that minimizes risks in order to avoid its consequences.

Generally, the proper steps to follows should be:

-Hazard evaluation: The first thing to do should be numbering and identifying the present risks. A complete evaluation would avoid design and equipment supply changes. In the evaluation, the requested SIL should be computed for each case.

-Assignation of the safety functions to the hazards: Once risks are defined, we would study the safety function we have to apply in order to avoid the risk or mitigate its consequences.

-Safety system requirements: This is the most important phase in the process of the SIS. In it, we have to define the safety requirements: the kind of instrumentation to be used, the failure to response mode, and the characteristics of the performance of the SIS.

-Design of the safety system: In order to guarantee safety of an installation, a series of considerations of design have to be taken into account to minimize or avoid failures. The design has to consider the redundancy of components and the characteristics of performance of the SIS.

5.2 Risk Evaluation

According to IEC 61511, the risk evaluation has to include:

- A description of each risk and the factors that causes them.

- A description of the consequences and the probability of the event.

- Determination of the requirements in order to the reduction or avoidance of additional risks and obtaining the safety requirements.

- A description about the measures taken to reduce hazards and risks.

- A description of the considerations taken into account in relation to the average of the risk demand, average equipment failure, operation limitations, and human factors.

- A first identification of the Safety Instrumented Function (SIF).

For our case, only one hazard will be evaluated (as described in previous chapters), and a detailed HAZOP analysis is the most understandable way to include the previous mentioned requirements.

Hereunder, a typical HAZOP is shown for the SIF of our project: safe air+fuel introduction in the boiler. The remaining SIFs of the whole SIS are not described because is not the aim of this work. Additionally, only the NODE for air+fuel and the DEVIATION less flow will be studied.

The HAZOP analysis will be performed in a table with the following format:

GW	DEVIATION	CAUSES	CONSEQUENCES	SAFEGUARDS	RECOMMENDATIONS

where

-NODE: It is the part of the process to be analyzed.

-GW: Guided Word. It is the word that is used to establish the deviation that is going to be studied. E.g. : more, less.

-DEVIATION: It is the situation to be analyzed in the corresponding node.

-CAUSES: They are the reasons by which the deviation occurs.

-CONSEQUENCES: They are the negative results in the installation occurred due to the deviation.

-SAFEGUARDS: They are the entire protections foreseen in the design to mitigate the effects of the deviation or to remove it.

-RECCOMENDATIONS: They are additional cautions and safeguards to be taken into account for improving safety in the node.

5.2.1. HAZOP

Node: Air and gas according to drawing 1 (Annex 3.1) and drawing 2 (Annex 3.2).

GW	DEVIATION	CAUSES	CONSEQUENCES	SAFEGUARDS	RECOMMENDATIONS
Less	Less Air/Fuel Flow Ratio	1.Fan Failure	Unstable flame. Flame out. Unburned fuel to the combustion chamber. HC accumulation. Explosion risk	1.Boiler trip in case of fan failure signal activated in motor control centre. 2.Boiler trip in case of flame out signal activated in boiler flame detector. 3.Boiler trip in case of Low Air Flow Signal activated in air flow transmitters.	Establish a maintenance plan for the fan, the motor and their accessories.
		2. Fuel flow increase (e.g. more boiler load required by the plant)	Unstable flame. Flame out. Unburned fuel to the combustion chamber. HC accumulation. Explosion risk	1. Boiler trip in case of Low Air Flow Signal activated in air flow transmitters.	As only one safeguard is available for this cause, the associated SIF must comply with very strict safe requirements.

5.3 Determination of the required SIL

SIL is a measurement of a safety system performance, measured as a function of the Probability of Failure on Demand (PFD) of the loop (Safety Function). To compute the SIL level of a hazard, the range of the PFD is obtained for the Safety Instrumented Function (SIF) to be included in the Safety Instrumented System (SIS).

The quantitative methods of the SIL computations would be quite tedious and they would involve making assumptions that could lead to error in the calculations. Therefore, we would better perform an alternative method called Risk Graph, which consist of 4 variables identified for each risk:

- Degree of consequences (**C**): Measures the degree or quantity of fatalities that may happen as a consequence of the hazard to occur.

  - **C1**: Minor damages and some slightly injured person.
  - **C2**: Seriously injured several people and one death.
  - **C3**: Several dead people.
  - **C4**: High fatality: many deaths

- Exposure frequency (**F**): possibility of the presence of people in the danger zone

  - **F1**: From rarely to frequently
  - **F2**: From frequently to permanently

- Probability of danger avoidance (**P**): depending on whether the dangerous variable is controlled and monitored, if it takes much or little time to occur, whether or not easily detectable and whether there are loopholes

  - **P1**: Possible under certain conditions
  - **P2**: Almost impossible

- Probability of danger (**W**): Always taking into account the worst case

➢ **W1**: There is little likelihood of danger and of little consequence if it occurs

➢ **W2**: There is little likelihood of danger

➢ **W3**: There is a relatively high probability of the hazard occurring

The following graphic shows the SIL levels needed for guaranteeing safety in a plant taking into account the C, P, F and W variables:

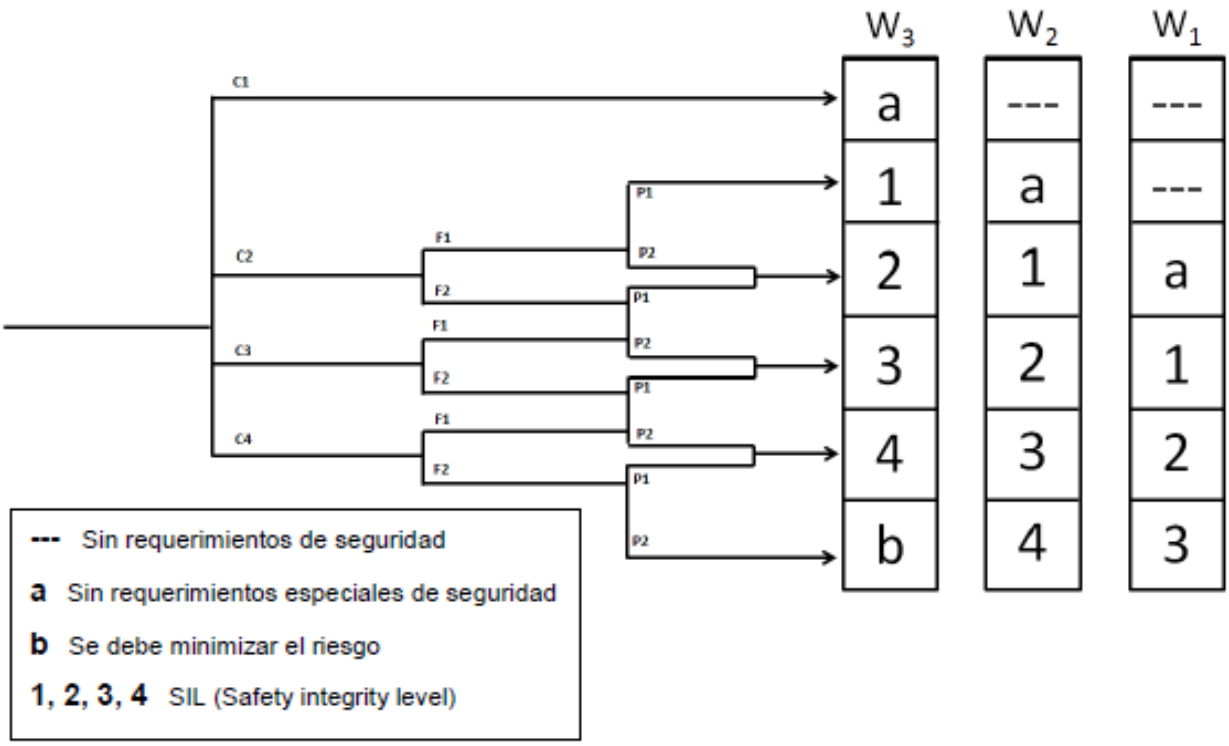

Figure 9: SIL Levels needed for guaranteeing safety.

For the case at hand, the mentioned parameters have the following values:

- Degree of consequences (C): As shown in the HAZOP, the worst consequence of the hazard studied is the explosion of the boiler. Usually, several maintenance operators are working in the proximity of the boiler during its normal operation. Besides, it is also frequently to find one operator in boiler platforms helping control room operators to solve the problems that appears in the control system screens. For the mentioned reasons, the degree of consequences assigned to this SIF is:

- **C2**: Seriously injured several people and one death

- Exposure frequency (F): Because of boiler demand is higher during the day, the maintenance requirements are higher too. Therefore, it can be inferred that the possibility of finding operators near the boiler is reduced at nights. For this reason, the exposure frequency assigned to this SIF is:

- **F1**: From rarely to frequently

- Probability of danger avoidance (P): It can be said that unique medium to detect the correct mixture of air-fuel is through the measurement of the flow of each fluid using the current technology. If the flow measurement fails, there is no way to avoid the occurrence of the risk. For this reason, the probability of danger avoidance is:

- **P2**: Almost impossible

- Probability of danger (W): As the defined danger is a boiler load increase (fuel flow increase), it can be assured that the probability of the occurrence of this danger is relatively high, because apart from the load changes required by the plant, the operators have a certain level of freedom to changer the boiler load under their responsibility.

- **W3**: There is a relatively high probability of the hazard occurring

Therefore, introducing the obtained parameters in the table shown in figure 7, the result is that we need a **SIL 2** level for guaranteeing safety in our system.

5.4 Assignation of the Safety Instrumented Function

Once the risks are defined, we should have to determine the strategy of prevention that our safety instrumented function (SIF) is going to apply.

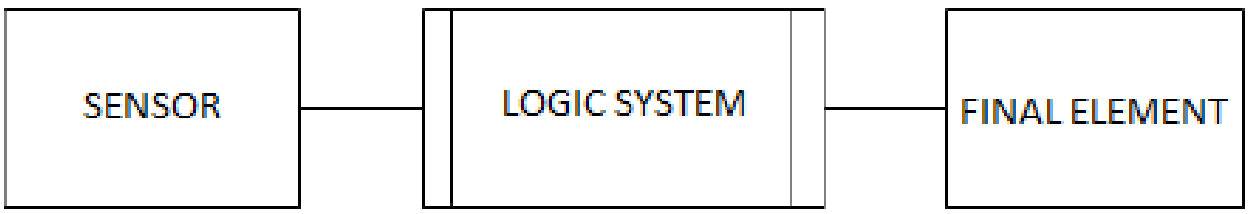

Figure 10: SIF basic diagram

To find out which sensor should be used, the first thing that should be done is to consider what type of variable can be measured to prevent the risk.

The logical system is typically a shared resource for all safety instrumented functions. Therefore, it must have the highest SIL of all process safety functions.

As a result of the HAZOP, the following assignation corresponds to the SIF object of the present project.

HAZARD: Fuel flow increase (e.g. more boiler load required by the plant)

SIF: Boiler trip in case of Low Air Flow Signal activated in air flow transmitters.

SIF COMPONENTS:

-SENSOR: Venturi and air flow transmitter/s (complying with IEC 61508 requirements) installed in the duct that introduces air in the combustion chamber.

-LOGIC SYSTEM: Safety PLC (complying with IEC 61508 requirements).

-FINAL ELEMENT: Fuel shut-off valve/s (complying with IEC 61508 requirements) that causes boiler trip when closing.

5.5 SIS Safety Requirements

Before the SIS design phase, the requirements that will be taken into account in all components and safety actions should be defined.

The requirements that should be specified in the safety system are:

- A description of all the safety functions needed for obtaining the required safety: In this case, a single safety function is being studied, which consists in controlling that the air-fuel mixture is enough safe so that, on the one hand, the amount of air is enough for the combustion to be carried out, and on the other hand, fuel pockets in the furnace of the boiler, that could burst unexpectedly, are avoided.

- The requirements for identifying and taking into account all the failures of common cause: Single point failure In this case, the single point failures are the venturi and the CPU of the PLC, which are the only two non-redundant elements of this SIF. The venturi is an element which is introduced inside the process conduit and a failure of the venturi equals a failure of the process,

which seems to be a very unlikely situation. Besides, very large conduits would be required to install more than one venturi to get redundancy.

On the other hand, the CPU is a very tested element and its failure rates are very low, thus it is not necessary to redound them inside a SIF.

- A description of the safety status that should be reached for each of the safety functions: Each time this SIF acts, the cut-off valves are de-energized, which will result in the shutdown of the combustion in the boiler.

- A description of the frequency with which the performance test and equipment maintenance would be developed: For this SIF, it has been considered that the frequency of performance test and equipment maintenance is carried out is 1 year.

-The SIL and the mode of operation for each safety function: The required SIL for this SIF is SIL 2, and its operation will be continuous inasmuch as how combustion is produced has to be monitored at all times.

-A description of the acquired measurements by the SIS and its trip settings: In the head 6.2 the measuring principle and the selected instrumentation for the measurement of the air flow is explained. The trip value of this SIF is variable, as at each moment it depends on the fuel flow introduced in the boiler.

-A definition of the relationship between inputs and outputs of the SIS, including logic, mathematic functions and required permissions: The measurement of the air flow is carried out by three transmitters whose signals are sent to the PLC of the SIS, where a 2oo3 logic is applied (see head 6.6). The result of this logic is compared with the minimum flow value required in each moment. In case this value is less than the minimum required value, the energization of the valves is deactivated in order to proceed to close them.

-Manual stop requirements. If there existed a concrete motive by which the operator should take an action to carry the system to a safe state, this should be specified: For this SIF a manual stop is not considered necessary by the operator since the system can detect at all times that the system is operating in safe conditions.

-Requirements related to the energization or de-engization for trips: The final elements of this SIF are pneumatic valves actuated by single effect solenoids. The de-energization of these solenoids will provoke the expulsion of the compressed air of the pneumatic actuators and the force of the spring will push the valve to its safe position (closed).

-Requirements for restarting the SIS after an emergency shutdown: Whenever the safety actuation of the FIS occurs, the operator is required to press a acknowledge button before re-introducing fuel into the boiler. Thus, it is intended to require the operator to evaluate the cause for which the trip occurs.

-Maximum percentage admissible of false trips: The maximum percentage of false shots has to be minimized as much as possible taking always into account the high safety requirements of this SIF.

-The requirements for the software application: The software application has to comply with the IEC61508 and has to be provided with the necessary diagnosis for the detection of possible failures in the execution of the programmed logic.

-Requirements for the bypasses including how they will be reset: Inasmuch as the considered equipment for this SIF is redundant, it is not necessary to install bypasses. In case of maintenance, one of the devices can be removed without affecting safety.

6. SIS DESIGN

The IEC 61511 states in its 11th chapter the SIS requirements to guarantee the maximum degree of safety in the plant. These requirements are divided in the following chapters:

- General Requirements
- Field Devices Requirements
- Interface Requirements (with the operator, with the engineering/maintenance, with other systems)
- Test and maintenance requirements

For this SIS, the following design has been considered according to guidelines of the mentioned standard. In figure 11 we can see a schematic graphic of the FIS.

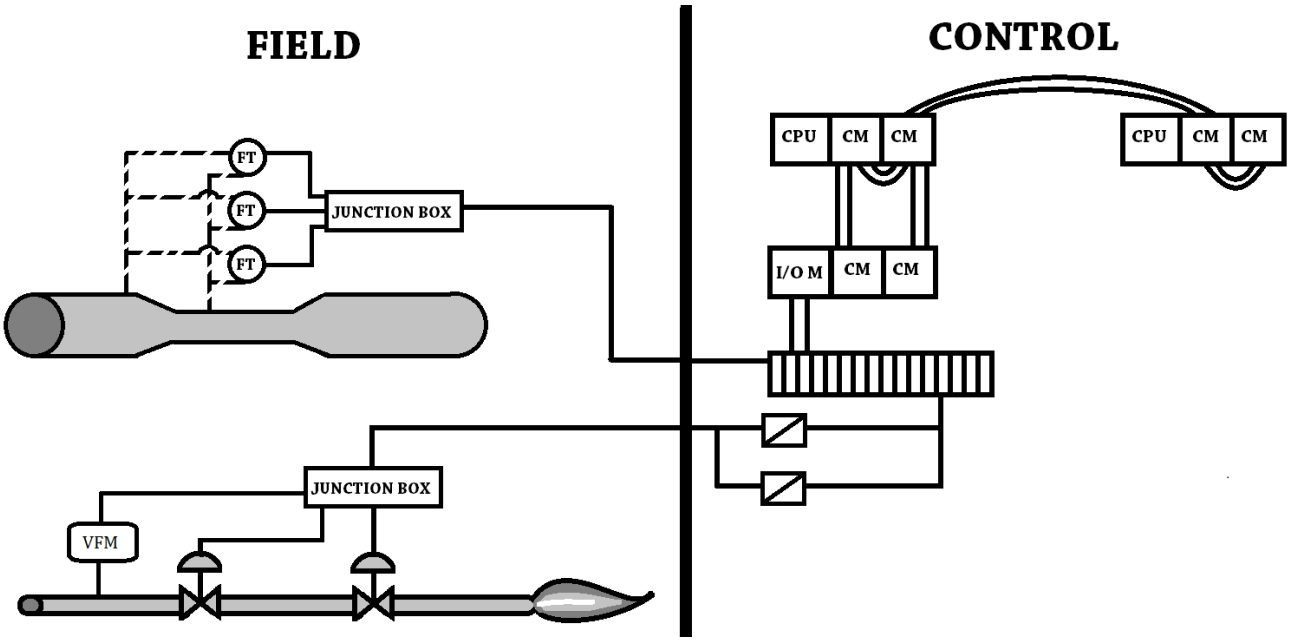

Figure 11: SIF elements and connections

In it, we can identify the following elements:

- Venturi
- Flow Transmitters (FT)
- Junctions Boxes

- Valves
- Vortex Flow Meter (VFM)
- PLC
- Relays
- Communications / Wiring

6.1 VENTURI

As previously mentioned, the selected primary flow element for this application was a venturi tube. This device is designed considering the specific conditions of the process, such as pressure and temperature of air and operating flow. According to the process information provided by the plant company, the following combustion air parameters have to be considered for venturi design (values for 100% load):

- Flow Rate 222603 Kg/h
- Static pressure 1,040 Bar
- Temperature 275 ºC
- Density (At indicated pressure and temperature) 0,661 Kg/m3

According to the previous data, for venturi design, it has been selected a differential pressure of 11 mbar for full scale flow (maximum flow) as it is standard value and fits for this application.

Additionally, following transmitters manufacturers, flow rate for 100% load will be set at 75% of full scale range. Consequently, for full scale value (11 mbar) the flow rate to be considered shall be 222603 x (1 /0.75)Kg/h = 296804 Kg/h .

Relationship between differential pressure and flow is shown in the following equation:

$$Q= K \sqrt{(\Delta P)}$$

where:

Q= flow in Kg/h

K= fluid dependant value

ΔP= Differential pressure in venturi taps

Considering this equation, to calculate the differential pressure for 100% load flow, the following steps shall be performed:

1) Calculate the square ratio between 100% load flow and maximum flow:

$$(222603 \text{ Kg/h} / 296804 \text{ Kg/h})^2 = 0{,}5625$$

2) Multiply the previous ratio by the full scale differential pressure.

$$0.5625 \text{ x } 11 \text{ mbar} = 6.1875 \text{ mbar}$$

Once the venturi performance values are defined, the only mechanical parameters to completely design the device are the size and material.

The selected material for this purpose is carbon steel. This material is appropriate for many corrosion fluids and good resistance to high temperatures and environmental agents. Therefore, as recommended in Annex 1.1, a carbon steel venturi tube of 6 mm thickness will guarantee its durability and proper performance for many years.

On the other hand, we have to calculate the diameter of the venturi tube. For that, we have to calculate first the section of the tube with the following equation:

$$S = Q_{max} / \rho \text{ x } V$$

where:

Q= Maximum air flow: 222603 kg/h = 61.834 kg/s

V= Air speed: 25 m/s

ρ= Air density: 0.661 kg/m3

The section of the tube would be then:

S= 61.834 kg/s / (25 m/s x 0.661 kg/m3) = 3.742 m2

For calculating the diameter:

$S = \pi \text{ x } r2 = \pi \text{ x } (D/2)2$

D = 2 √(S/π) = 2 √(3.742 m2/π)= **2.183 m**

6.2FLOW TRANSMITTERS

As we have chosen a venturi as a primary flow element for the measurement of the flow rate, we will use differential pressure transmitters connected to both taps of the venturi tube, using the equation:

$$Q= K \sqrt{(\Delta P)}$$

For this project we will use the Emerson's Rosemount 3051 differential pressure transmitter, because we consider it as the most economic device in the market, considering its high reliability, and having Exida's SIL 3 capable certificate, according to IEC61508.

Looking at Rosemount 3051 flow transmitter datasheet, attached in the Annex 1.2 we realize that the flow transmitter we would need will be the following model:

3051CD1A02A1AM5B9DFE8H2P1Q4Q8QT

Whose characters stand for:

3051C: Coplanar Pressure Transmitter. Integrated differential pressure transmitter + sensor.

D: Differential measurement type

1: Pressure range: -25 to 25 inches H2O (-62,16 to 62,16 mbar)

A: Transmitter signal output: 4-20 mA with Digital Signal Based on HART Protocol.

0: Alternate Process Connection: Process connection selected to be suitable for flanged installation to manifold.

2: 316LSST Isolating diaphragm: Sensor material selected in stainless steel 316L quality, suitable for most process conditions.

A: Glass-filled PTFE O-ring: PTFE gasket for tight process installation.

1: Silicone-filled: Silicone enclosure for sensor protection.

A: Aluminum housing material (1/2 – 14 NPT Conduit entry size)

M5: LCD Display for local indication

B8: Traditional flange bracket, B3 with SST bolts

DF: ½ - 14 NPT flange adapter(s)

E8: ATEX Flameproof and Dust certification

H2: Traditional Flange, 316 SST, SST Drain/Vent

P1: Hydrostatic Testing with Certificate, in order to check leakage.

Q4: Calibration Certificate.

Q8: Material Traceability Certification per EN 10204 3.1

QT: Safety certified to IEC 61508 with certificate of FMEDA, in order to assure the suitability for installation in safety integration functions.

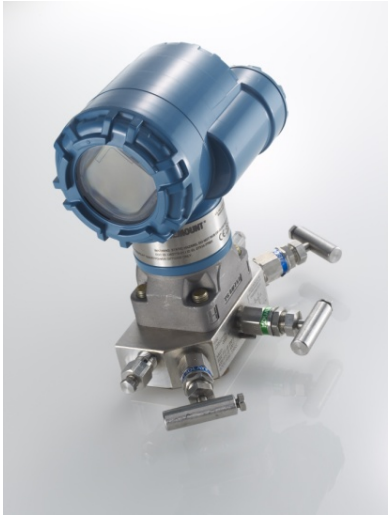

Figure 12: Rosemount 3051C differential pressure transmitter

The Rosemount 3051C Coplanar design is offered for Differential Pressure (DP), Gage Pressure (GP) and Absolute Pressure (AP) measurements. The Rosemount 3051C utilizes Emerson Process Management capacitance sensor technology for DP and GP measurements.

The major components of the Rosemount 3051 are the sensor module and the electronics housing. The sensor module contains the oil filled sensor system (isolating diaphragms, oil fill system, and sensor) and the sensor electronics. The sensor electronics are installed within the sensor module and include a temperature sensor (RTD), a memory module, and the capacitance to digital signal converter (C/D converter). The electrical signals from the sensor module are transmitted to the output electronics in the electronics housing. The electronics housing contains the output electronics board, the local zero and span buttons, and the terminal block.

For the Rosemount 3051C design pressure is applied to the isolating diaphragms, the oil deflects the center diaphragm, which then changes the capacitance. This capacitance signal is then changed to a digital signal in the C/D converter. The microprocessor then takes the signals from the RTD and C/D converter calculates the correct output of the transmitter. This signal is then sent to the D/A converter, which converts the signal back to an analog signal and superimposes the HART signal on the 4-20 mA output.

6.3 VORTEX FLOWMETER

For the measurement of gas flow in a pipe, several types of instruments can be used. The most common ones are the coriolis flowmeter, the magnetic flowmeter, the ultrasoinc flow meter, the turbine flowmeter and the vortex flowmeter, although there are a lot more. The most suitable instrument for this application is the vortex flowmeter due to its low price and easy installation.

The vortex flowmeter method of flow measurement involves placing a bluff body (called a shedder bar) in the path of the fluid. As the fluid passes this bar, disturbances in the flow called vortices are created. The vortices trail behind the cylinder, alternatively from each side of the bluff body. This vortex trail is called the Von Kármán vortex street after von Kármán's 1912 mathematical description of the phenomenon.

The frequency at which these vortices alternate sides is essentially proportional to the flow rate of the fluid. Inside, atop, or downstream of the shedder bar is a sensor for measuring the frequency of the vortex shedding. This sensor is often a piezoelectric crystal, which produces a small, but measurable, voltage pulse every time a vortex is created. Since the frequency of such a voltage pulse is also proportional to the fluid velocity, a volumetric flow rate is calculated using the cross sectional area of the flow meter.

The frequency is measured and the flow rate is calculated by the flowmeter electronics using the equation $f = SV/L$ where f is the frequency of the vortices, L the characteristic length of the bluff body, V is the velocity of the flow over the bluff body, and S is the Strouhal number, which is essentially a constant for a given body shape within its operating limits.

The selected vortex flowmeter for this project is Rosemount 8800D Series Vortex Flowmeter

Figure 13: Rosemount 8800D Series Vortex Flowmeter

Looking at Rosemount 8800D series vortex transmitter datasheet, attached in the Annex 1.3, we realize that the vortex transmitter we would need will be the following model:

8800DF030SA1N1D1

Whose characters stand for:

8800D: Vortex Flowmeter

F: Flanged style of metering

030: 3 in. (80 mm) line size

S: 316 wrought stainless and CF-3M cast stainless steel for the wetted materials

A1: ASME B16.5 (ANSI) RF Class 150

N: Standard sensor process temperature range (-40 to 232 ºC)

1: 1/2 - 14 NPT - Aluminum housing

D: 4-20 mA digital electronics (HART protocol) output

1: Flow calibration

6.4 JUNCTION BOXES

In industrial installations, where a high volume of instrumentation devices are installed around the whole area, junction boxes are used to reduce electrical installation works and costs.

Junction boxes allow grouping some quantity of signals to be wired to PLCs located in control rooms, using a common multi-core cable.

In this case, 2 junction boxes are needed. One junction box will be used for grouping the 2-wire cables of the 3 flow transmitters round the venturi tube (6 wires in total) and another junction box for grouping the 2-wire cables of the 2 solenoids of the valves and the fuel vortex flowmeter. Both boxes will use 6 wire cables for PLC interconnection.

A junction box consists of the following components:

- Enclosure: the enclosure protects the devices installed inside the junction box. Therefore, it shall have a high degree of protection against the entry of water and dust. Besides, it shall have a high mechanical resistance to breakage.

  The International Electrotechnical Commission (IEC) standardizes the measurement of the degree of protection against water and solid particles, through IEC 60529, and against external mechanical impacts, through IEC 62262.

  IEC 60529 qualifies as an alphanumerical way the level of protection of equipments against the entry of foreign materials through the code IPXX, being IP the acronym of "Ingress Protection", the first X a numerical digit for describing the level of protection against dust entry, and the second X another numerical digit for describing the level of protection against water entry.

  This standard rates from 0 to 6 the protection against dust entry (0: no protection, 6: no entry under any circumstances), and from 0 to 8 the protection against water entry (0: no protection, 8: no entry under complete and continuous immersion in water under more than 2 meters depth and for more than 2 minutes.

Solid particle protection table:

Level	Object size protected against	Effective against
0	—	No protection against contact and ingress of objects
1	>50 mm	Any large surface of the body, such as the back of a hand, but no protection against deliberate contact with a body part
2	>12.5 mm	Fingers or similar objects
3	>2.5 mm	Tools, thick wires, etc.
4	>1 mm	Most wires, screws, etc.
5	Dust protected	Ingress of dust is not entirely prevented, but it must not enter in sufficient quantity to interfere with the satisfactory operation of the equipment; complete protection against contact (dust proof)
6	Dust tight	No ingress of dust; complete protection against contact (dust tight)

Liquid ingress protection table:

Level	Protected against	Testing for	Details
0	Not protected	—	—
1	Dripping water	Dripping water (vertically falling drops) shall have no harmful effect.	Test duration: 10 minutes Water equivalent to 1 mm rainfall per minute
2	Dripping water when tilted up to 15°	Vertically dripping water shall have no harmful effect when the enclosure is tilted at an angle up to 15° from its normal position.	Test duration: 10 minutes Water equivalent to 3 mm rainfall per minute
3	Spraying water	Water falling as a spray at any angle up to 60° from the vertical shall have no harmful effect.	Test duration: 5 minutes Water volume: 0.7 litres per minute Pressure: 80–100 kPa
4	Splashing of water	Water splashing against the enclosure from any direction shall have no harmful effect.	Test duration: 5 minutes Water volume: 10 litres per minute Pressure: 80–100 kPa
5	Water jets	Water projected by a nozzle (6.3 mm) against enclosure from any direction shall have no harmful effects.	Test duration: at least 15 minutes Water volume: 12.5 litres per minute Pressure: 30 kPa at distance of 3 m
6	Powerful water jets	Water projected in powerful jets (12.5 mm nozzle) against the enclosure from any direction shall have no harmful	Test duration: at least 3 minutes

		effects.	Water volume: 100 litres per minute Pressure: 100 kPa at distance of 3 m
6K	Powerful water jets with increased pressure	Water projected in powerful jets (12.5 mm nozzle) against the enclosure from any direction, under elevated pressure, shall have no harmful effects.	Test duration: at least 3 minutes Water volume: 75 litres per minute Pressure: 1000 kPa at distance of 3 m
7	Immersion up to 1 m	Ingress of water in harmful quantity shall not be possible when the enclosure is immersed in water under defined conditions of pressure and time (up to 1 m of submersion).	Test duration: 30 minutes Immersion at depth of at most 1 m measured at bottom of device, and at least 15 cm measured at top of device
8	Immersion beyond 1 m	The equipment is suitable for continuous immersion in water under conditions which shall be specified by the manufacturer. Normally, this will mean that the equipment is hermetically sealed. However, with certain types of equipment, it can mean that water can enter but only in such a manner that it produces no harmful effects.	Test duration: continuous immersion in water Depth specified by manufacturer, generally up to 3 m
9k	Powerful high temperature water jets	Protected against close-range high pressure, high temperature spray downs.	—

The required IP protection of the junction boxes for this project (established by the client) is IP66, which means no dust entry under any circumstances, and no water entry through a nozzle diameter of 12.5 mm, an average of 100 liters per minute and a pressure of 100 kN / m² for not less than 3 minutes at a distance of not less than 3 meters.

On the other hand, the IEC 62262 qualifies the level of protection against mechanical impacts, rating from IK00 (no protection), up to IK10 (20 Jules protection, checked by dropping a 5kg object from a height of 40 cm).

Mechanical impact protection table:

IK number	Impact energy (joules)	Equivalent impact
00	Unprotected	No test
01	0.15	Drop of 200 g object from 7.5 cm height
02	0.2	Drop of 200 g object from 10 cm height
03	0.35	Drop of 200 g object from 17.5 cm height
04	0.5	Drop of 200 g object from 25 cm height
05	0.7	Drop of 200 g object from 35 cm height
06	1	Drop of 500 g object from 20 cm height
07	2	Drop of 500 g object from 40 cm height
08	5	Drop of 1.7 kg object from 29.5 cm height
09	10	Drop of 5 kg object from 20 cm height
10	20	Drop of 5 kg object from 40 cm height

In this case, the client requires a IK07 protection, which means the junction box should resist an impact of 2 Joules (500 grams dropped from a height of 40 cms).

Because of its strength and its economic prize, the selected material for the junction boxes will be cast aluminum.

For these reasons, the selected enclosure for the junction box is the SA202012 model of Cortem (see Annex 1.4).

- Din rail: The din rail is used as a standard bracket for electrical components. In this case, the din rail is used for the installation of terminals inside the junction box. For this project, the selected din rail is the NS 35/15-2,3 UNPERF 2000MM – 1201798, of Phoenix Contact (see Annex 1.5).

- Terminals: For this application, each junction box holds 3 pairs of wires, but they must have enough room for holding 2 more pairs for alternative purposes. Therefore, we would need a rack of 10 terminals. These terminals should have the following features:

  -Maximum Load Current: 16 A
  -Rated Surge Voltage: 6 kV
  -Nominal Voltage: 500 V

  Taking into consideration these factors, the most suitable terminals for these projects are the UK 4-TG – 2812018 of Phoenix Contact, whose datasheet is attached in Annex 1.6.

- Cable glands: Cable glands are used in order to ensure the sealing of the cable entrance to the junction box, avoiding the entry of water and dust. As the enclosure, the client states an IP and IK level for cable glands, in this case, IP67 and IK07.

  The most suitable cable glands for this project are the FL- series of Cortem, whose main features are:
  -Niquel-plated brass covering
  -CESI 00 ATEX 052 (Elfit) certificate: Explosion-proof certificate
  -IP 66/67 protection

Figure 14: Cortem FL- Series Cable Gland

For this project, two types of cable glands are needed. One type for the single-pair cables (from instruments/valves to the junction boxes), and other type for five-pair cables (from junction boxes to PLC).

The single-pair cables diameter is 7.6 mm (explained in 6.8). Therefore, the required corresponding cable glands must have a size of ½". Looking at Cortem's table of Fl- products, attached in Annex 1.7, the required cable glands are the FL1BK.

The five-pair cables diameter is 14.3 mm, so we would need a FL2BK cable gland of the same brand of Cortem.

6.5 VALVES

The required valves for this purpose are the on/off type which purpose is to cut-off the gas supply to the boiler in an emergency. Its characteristics are the following:

Type: Ball valve. This valve has a very good sealing and they are not so much expensive for the required size.

Internals: Both the valve itself and the other internals in contact with the fluid (wetted parts) are made of stainless steel, which is highly resistant to corrosion.

Seating: Due to temperature conditions, a Teflon seating is required. This Teflon seating guarantees a great sealing and durability (resistance to corrosion).

The valve is supplied with but-welded ends. This welding is very strong and the most suitable for flammable fluids.

Actuator: The pneumatic actuator is rack and pinion type, as for a ball valve is the required actuator.

Solenoid+electrovalve: The actuator is operated by a 3 ways and 2 positions electrovalve, which is actuated by a F type solenoid and a 24 VDC voltage level.

The selected electrovalve for the gas conduit is the EFR-Series of JC valves (see Annex 1.8).

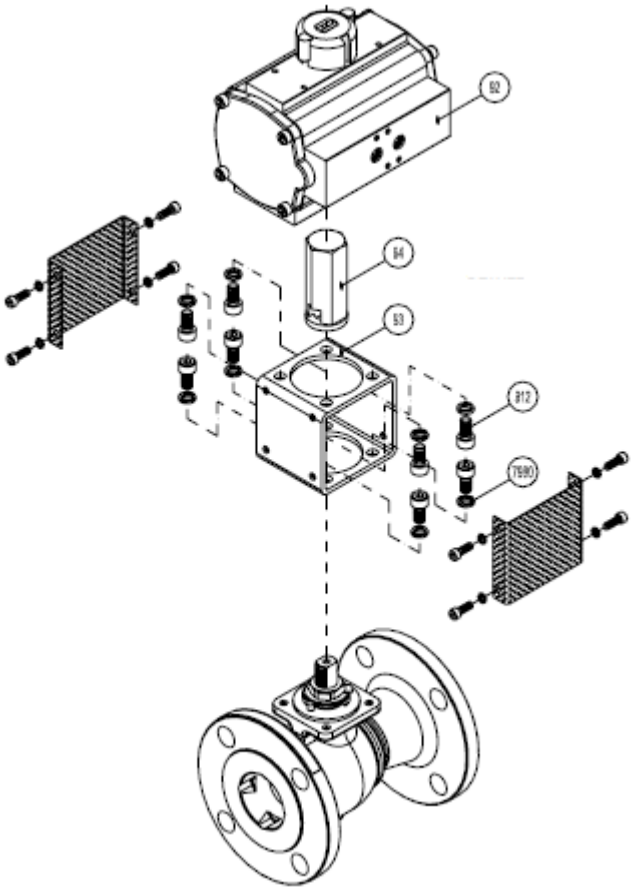

Figure 15: EFR-Series JC electrovalve

6.6 PLC

A Programmable Logic Controller, PLC or Programmable Controller is a digital computer used for automation of electromechanical processes, such as control of machinery on factory assembly lines, amusement rides, or light fixtures. PLCs are used in many industries and machines. Unlike general-purpose computers, the PLC is designed for multiple inputs and output arrangements, extended temperature ranges, immunity to electrical noise, and resistance to vibration and impact. Programs to control machine operation are typically stored in battery-backed-up or non-volatile memory. A PLC is an example of a hard real-time system since output results must be produced in response to input conditions within a limited time, otherwise unintended operation will result.

In recent years "Safety" PLCs have started to become popular, either as standalone models or as functionality and safety-rated hardware added to existing controller architectures (Allen Bradley Guardlogix, Siemens F-series etc.). These differ from conventional PLC types as being suitable for use in safety-critical applications for which PLCs have traditionally been supplemented with hard-wired safety relays. Such PLCs typically have a restricted regular instruction set augmented with safety-specific instructions designed to interface with emergency stops, light screens and so forth. The flexibility that such systems offer has resulted in rapid growth of demand for these controllers.

In the case of this application, as the previous PLC complied with the safety requirements of the IEC61508, it will not be replaced. This PLC is the Siemens S7-400 (see Annex 1.9).

Regarding the programming of the PLC, we will have to define the following logic in order to triplicate analog signals (from the flowmeters):

- For each signal, the logic compares the analog input value with the interlock setpoint, i.e. low/low, and the corresponding digital signal is generated, low/low interlock.

- In case of bad quality signal, out of range or open circuit or channel failure, the voting logic criteria will be to safe state. The digital output is set to safe state, low/low interlock in this example.

- Then, the 2 out of 3 logic (majority voting) is performed with the three resultant digital signals for each setpoint, obtaining the final interlock signal to be used in the logic.

- With the three bad quality signals, a 2oo3 logic is also performed to generate a bad quality alarm that will be used to filter the process alarms, low/low in this example, with the objective of adequately alarming if the interlock is due to process signals or bad quality in the analog input signals.

- The three analog inputs are compared pair by pair and a discrepancy alarm is generated if any of them has been deviated from the other two more than a certain percentage.

6.7 RELAYS

The digital outputs of the PLC pass through relays for energizing the gas valves. These relays must be safety relays suitable for SIF installation and they must meet the requirements of SIL. The selected relay for this application is the Phoenix Contact PSR-SCP- 24DC/ESP4/2X1/1X2 model, whose datasheet is attached in Annex 1.10, which has the following characteristics:

Input data

Nominal input voltage U_N: 24 V DC

Input voltage range in reference to U_N: 0.85 ... 1.1

Typical input current at U_N: 60 mA DC

Voltage at input/start and feedback circuit: Approx. 24 V DC

Typical response time: 60 ms

Typical release time: 20 ms

Recovery time: 1 s

Output data

Contact type: 2 enabling current paths, 1 signaling current path

Contact material: AgSnO2, + 0.2 µm Au

Maximum switching voltage: 250 V AC/DC

Minimum switching voltage: 15 V AC/DC

Limiting continuous current: 6 A

Maximum inrush current: 6 A

Inrush current, minimum: 25 mA

Figure 16: Phoenix Contact PSR-SCP- 24DC/ESP4/2X1/1X2 safety relay

6.8 COMMUNICATIONS /WIRING

For this installation two types of cables will be used:

- Cabling between instruments and junction boxes: 2x1.5 mm^2 (size recommended by manufacturer for field instrumentation). The requirements for this cable are:

  -Conductor: Annealed electrolytic copper. Class 5.
  -Insulation: Free Polyolefine halogenous nonpropagator of the fire (Z1).
  -Screen: Tinned copper drainage wire. (Generally 7x0.3mm-S=0.5mm².).
  -Sheath: Free Polyolefine halogenous nonpropagator of the fire Z1
  -Rank of temperature: For installation: [-5ºC / 50ºC]. In operation [30ºC to 70ºC]
  -Radius of curvature: 10 x d (d=outer diameter)
  -Service voltage: 300/500 V

  Taking into account these requirements, the selected cable for this application is the EOZ1 (ROZ1) - Z1OZ1 cable of Técnicas del Cable, whose datasheet is attached in Annex 1.11.

Figure 17: EOZ1 (ROZ1) - Z1OZ1 *Técnicas del Cable* cable

- Cabling between junction boxes and control room: 5x2x1 mm^2. In this case, a less section of the wires is used in order to reduce costs of installation (e.g. less weight of the cable, less radius of curvature, and less amount of copper).

  The selected cable for this application is the EHOZ1 (RHOZ1) - Z1HOZ1 cable of Técnicas del Cable, whose datasheet is attached in Annex 1.12.

Figure 18: EHOZ1 (RHOZ1) - Z1HOZ1 *Técnicas del Cable* cable

7. SIL VERIFICATION

In order to verify the SIL level of each of the SIF of the safety system, the required values for the IEC 61511 tables for Probability of Failure on Demand (PFD) must be fulfilled.

7.1 PFD Verification

The probability of failure on demand is a variable that can be calculated from the dangerous failure rate (λ_D) and the manual test interval (Ti expressed in hours). The PFD increases as a function of time following the formula:

$$PFD = 1 - e^{-\lambda D \cdot Ti}$$

This formula can be approximated by:

$$PFD = \lambda_D \cdot Ti$$

As for PFD values greater than 0.1 the error is less than 3% (the PFD we are going to compute are much lower). Due to the fact that the PDF increases over time, after a T_i period, test must be carried out in order to get the initial PFD value again. For that time T_i, the average PFD value that we will use for the global PFD is:

$$PFD_{avg} = \frac{1}{T}\int_0^{T_i} PFD(t)dt = \frac{1}{T}\int_0^{T_i} \lambda_D \cdot Ti\, dt = \lambda_D \cdot Ti/2$$

The PFD values must be introduced in the general formula of the loop of the safety function after checking it complies with the required SIL for this function. The general formula of the PFD is:

$$PFDsystem = PFD_S + PFD_{LS} + PFD_{FE}$$

Being

PFD_S: PFD of the sensor or measurement instrument

PFD_{LS}: PFD of the logic system

PFD_{FE}: PFD of the final element

Although equipment suppliers provide the SIL of those individually, the PFD and λ_D values must be required to them in order to calculate the PFD in case of redundant configurations, as in this case.

SIL-PFD Correspondence			
Safety Integrity Level (SIL)	Probability of failure on demand (PFDavg)	Availability	Reduction of target risk
4	≥10-5 to 10-4	>99.99%	>10.000 to ≤100.000
3	≥10-4 to 10-3	99.90 - 99.99%	>1.000 to ≤10.000
2	≥10-3 to 10-2	99.00 -99.90%	>100 to ≤1.000
1	≥10-2 to 10-1	90.00 - 99.00%	>10 to ≤100

Whenever low demand exists (less than 2 triggers per year per risk), the average PFD value will be used to calculate the SIL. However, in the case of high demand, or continuous demand (2 or more triggers per year), the value of the corresponding PFH will be used, following the below table:

Probability of Failure per Hour (PFH)	Safety Integrated Level (SIL)
≥10-8 to <10-7	3
≥10-7 to <10-6	2
≥10-6 to <10-5	1
≥10-5 to <10-4	With no special safety requirements

In the case of redundant configurations, the redundant formulas have to be applied and then we must calculate the average of the resultant PFD. As a general rule, the following formulas shall be used for redundant configuration unless the manufacturer provides specific formulas for redundant configuration.

Architecture	**PFDavg (Safety)**	**Rate of spurious trips (Availability)**
1oo1	$1/2 \cdot \lambda_D \cdot Ti$	λ_s
1oo2	$1/3 \cdot (\lambda_D \cdot Ti)2$	$2 \cdot \lambda s$
2oo2	$\lambda_D \cdot Ti$	$2 \cdot (\lambda s)2 \cdot MTTR$
2oo3	$(\lambda_D \cdot Ti)2$	$6 \cdot (\lambda s)2 \cdot MTTR$

Being:

λ_D = Dangerous failures rate

T_i = Manual test interval

λ_s = Safe failures rate

MTTR = Mean Time To Repair

7.1.1 PFD Calculation

The SIF configuration of this system is represented in the following figure:

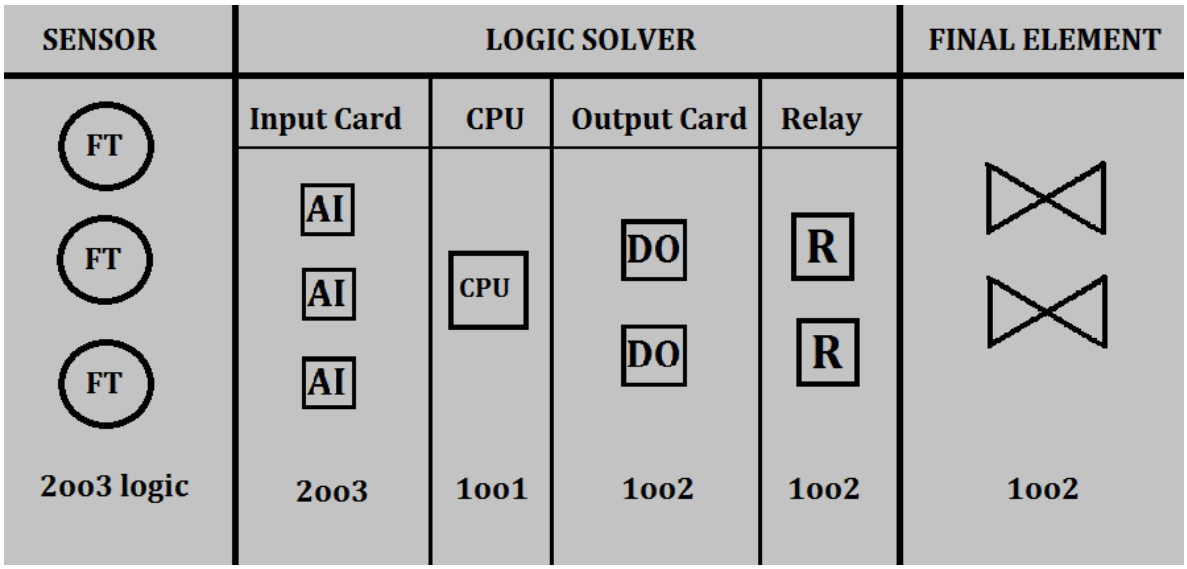

Figure 19: SIF Architecture

In order to simplify calculations, the devices will be grouped according to its redundancy. For example, for the sensor, the PFD will be calculated as the result of the 2oo3 logic of the sum of flow transmitters and analog input cards. The same criteria applies to the 1oo2 logic of the final element (digital output cards, relays and valves).

Therefore, in order to calculate the PFD of the whole system, we are going to calculate the PFD of the three main parts of the system PFD_{SENSOR}, PFD_{LS} and PFD_{FE} and then we will sum them in order to obtain the final result.

Values for PFD calculation are obtained from manufacturer documents, which are included in Annex 2 (SIL certificates and PFD values).

SENSOR: 2oo3 logic. Flow Transmitter (FT) + Input Card (AI: Analog Input)

- Rosemount 3051 flow transmitter: $\lambda_{Du} = 32 \cdot 10^{-9}$
- SM 336 F Analog Input Card (from Siemens PLC): $\lambda_{Du} = 1.1 \cdot 10^{-11}$
  As the flow transmitter and the analog input card follow a 2oo3 architecture, the following formula has to be used to calculate the PFD of the whole sensor.

$$PFD_{SENSOR} = (\lambda_{Du} \cdot T_i)^2 = [(\lambda_{DuFT} + \lambda_{DuAI}) \cdot T_i]^2$$

$$PFD_{SENSOR} = [(32 \cdot 10^{-9} + 1.1 \cdot 10^{-11}) \cdot 10 \cdot 365 \cdot 24]^2$$

$$\mathbf{PFD_{SENSOR} = 7.86 \cdot 10^{-6}}$$

LOGIC SOLVER: 1oo1 logic.

- Siemens CPU 414-4H: $\lambda_{Du}= 2.83 \cdot 10^{-8}$

  As the CPU follows a 1oo1 architecture, we have to use the following formula in order to calculate the PFD:

$$PFD_{LS} = 1/2 \cdot (\lambda_{Du} \cdot T_i)$$

$$PFD_{LS} = 1/2 \cdot (2.83 \cdot 10^{-8} \cdot 10 \cdot 365 \cdot 24)$$

$$\mathbf{PFD_{LS} = 1.24 \cdot 10^{-3}}$$

FINAL ELEMENT:

- SM 326 F Digital Output Card (From Siemens PLC): $\lambda_{Du}= 1.6 \cdot 10^{-9}$
- Phoenix Contact PSR-SCP- 24DC/ESP4/2X1/1X2 relay $\lambda_{Du}= 1.1 \cdot 10^{-7}$
- Valve: In the case of the valve, we only have to take into account the dangerous failure rates of the actuator (Prisma PI00 model) and the solenoid (Asco Controls 551 series)

  - $\lambda_{DuACTUATOR}= 4.48 \cdot 10^{-7}$
  - $\lambda_{DuSOLENOID}= 4.57 \cdot 10^{-10}$
  - $\lambda_{DuVALVE}= \lambda_{DuACTUATOR} + \lambda_{DuSOLENOID} = 4.48 \cdot 10^{-7}$

  As the final element follow a 1oo2 architecture, the following formula has to be used to calculate the PFD:

$$PFD_{FE} = 1/3 (\lambda_{DuFE} \cdot T_i)^2$$
$$PFD_{FE} = 1/3 [(\lambda_{DuDO} + \lambda_{DuRELAY} + \lambda_{DuVALVE)} \cdot T_i]^2$$

$$PFD_{FE} = 1/3 [(1.6 \cdot 10^{-9} + 1.1 \cdot 10^{-7} + 4.48 \cdot 10^{-7}) \cdot 10 \cdot 24 \cdot 365]^2$$

$$\mathbf{PFD_{FE} = 8.01 \cdot 10^{-4}}$$

$$PFD_{SYSTEM} = PFD_{SENSOR} + PFD_{LS} + PFD_{FE}$$

$$PFD_{SYSTEM} = 7.86 \cdot 10^{-6} + 1.24 \cdot 10^{-3} + 8.01 \cdot 10^{-4}$$

$$\mathbf{PFD_{SYSTEM} = 2.05 \cdot 10^{-3}}$$

Once we have calculated the PFD of the system, looking at the table we can verify the SIL level of the system:

SIL-PFD Correspondence			
Safety Integrity Level (SIL)	Probability of failure on demand (PFDavg)	Availability	Reduction of target risk
4	≥10-5 to 10-4	>99.99%	>10.000 to ≤100.000
3	≥10-4 to 10-3	99.90 - 99.99%	>1.000 to ≤10.000
2	**≥10-3 to 10-2**	**99.00 -99.90%**	**>100 to ≤1.000**
1	≥10-2 to 10-1	90.00 - 99.00%	>10 to ≤100

As our PFD_{SYSTEM} is $2.05 \cdot 10^{-3}$, which is between 10^{-3} and 10^{-2} , we can conclude that the SIL level of our system is **SIL2**.

8. CONCLUSION

8.1 Targets Fulfilled

Our targets in this project were:

- Finding the source of the problem: The experts committee concluded that the accident was caused due to a non-checked measurement error of the unique air flowmeter of the system (in the new SIS we dispose of three of them). As there was no Safety Integrated System implemented, a hazardous situation was very likely to be produced in case of a measurement error (or any other failure of the system).

- Investigating the available technology and design industry standards to develop an optimized design: During the process of writing the work, a high understanding of functional safety was acquired in order to face the problem to be solved as the main functional safety standards recommend.

  To sum up, the main functional safety standards are the IEC61508 and the IEC61511.

  IEC61508 describes the minimum requirements that the E/E/PES (Electrical/Electronic/Programmable Electronic Safety-related) systems have to fulfill to be installed in a safety function. These requirements mainly consist of the diagnostic carried out in the devices in order to check that the signal they transmit coincides with the value of the variable they are measuring.

  IEC61511 describes how HAZOP and SIL studies have to be carried about, and which are the main parameters of devices (transmitters, valves...) to be studied in order to comply the functional safety requirements. Additionally, this standard describes the steps to be followed since the identification of the risk, the design of the Safety Instrumented System (SIS), and the assignation of safety functions to the identified risks. Finally, the verification of the suitability of the SIS is carried out.

  Besides, we have found out that there exist several certification agencies (EXIDA is the most popular one) that measure this parameters in order to ensure the validity of calculations carried out in SIL studies.

- Solving the problem: For solving the problem, we had to follow the following steps:

1. **Examining the required level of safety depending on the severity of the hazard and the consequences of accidents**: As explained in 5.4, the required level of safety is determined by 4 main parameters: degree of consequences (**C**), exposure frequency (**F**), probability of danger avoidance (**P**) and probability of danger (**W**). The quantification of this parameters led us to conclude the required Safety Integrated Level (SIL) was SIL 2.

2. **Evaluating devices and replace the failed ones to be able to mitigate the consequences that could cause the accident.** Essentially, we have replaced the instruments by new ones having a safety certification for working in dangerous process that could require up to a SIL 3 level, and we have redound them following the IEC61511 requirements in order to guarantee functional safety.

3. **Develop a safety integrated system that meets the required safety level risk analysis (HAZOP).** Once the required SIL level has been assigned for the safety instrumented function we are analyzing, the main elements are chosen in order to achieve the assigned SIL. For this purpose, we have found in the market the available devices prior to decide the most suitable ones.

4. **Quantitatively and qualitatively verify the validity of the safety system intended.** By means of the information included in the certificates of the elements of the SIF (sensors, logic solver and final elements), both quantitatively and qualitatively verification can be performed to assure that the design and devices selection has been developed correctly.

8.2Importance of IEC61511 and IEC61508 standards

IEC61511 and IEC61508 are crucial in industry as a need for standardization of industrial safety.

Before these standards exist, each engineering company designed their own safety systems following their own rules based on their experience, or on the requirements stated by the client. This fact was the cause by which a lot of safety factors were not taken into account in the design of these safety systems, which led to the occurrence of many accidents which could be avoided if there existed some kind of standardization of functional safety.

Nowadays, the creation of these standards and certification agencies such as EXIDA© led to improve the design of safety systems, which in turn has led to reduce considerably the number of industrial accidents. Most of gas, petroleum and energy companies, such as Saudi Aramco (Saudi Arabia), Sonatrach (Algeria) or Eon (Germany) are requesting SIL 2 to their contractors, for the whole systems of their plants, and even SIL 3 for some specific applications.

Bibliography

[1] S. G. M. J. B. L. Alberto de la Sen Sanz, Control y Seguridades de Calderas, Madrid: FI Controllers S.A., 2000.

[2] W. Bolton, Programmable Logic Controllers, Newnes, 2009.

[3] I. E. Commission, Functional Safety - Safety instrumented systems forthe process industry sector - IEC61511.

[4] G. K. Batchelor, An Introduction to Fluid Dynamics, 1967.

[5] I. E. Center, Digital Direct Controls - Chapter 2: Input Devices and Sensors.

[6] A. E. Summers, ANSI/ISA 84.00.01-2004 and Existing Safety Instrumented Systems.

[7] Fi Controles S.A., Curso de Calderas, 1997.