

## Session Seven:

# **SIL Application in Burner Management Systems - A Case Study: Thermal Burner**

**Jorge Sanchez**

Process Engineer: Fluor Corp

---

## **1. ABSTRACT**

Boiler, furnaces and other burning equipments are considered as high-risk areas within the Process Industry. This is due to extreme operating conditions and processing of hazardous materials resulting in wide safeguarding measures being applied to prevent accidents. One of the best known and widely accepted technical solutions concerns the use of safety-related systems implemented through PES technology.

New risk-based standards published in recent years control the design of these technical solutions. They include technology-oriented requirements with their ‘adequate’ implementation and the ‘fit-to-purpose’ tailoring of the equipment. However, to obtain functional safety this approach demands more management, competency and planning than the prescriptive requirements of original codes.

This paper presents a case study about the identification of safety functions. It includes lifecycle activities carried out to achieve functional safety requirements and comply with the original approach for Burner Management Systems.

## **2. A BRIEF OVERVIEW OF THE PROCESS INDUSTRY**

The Process Industry applies the technology in order to physically and chemically transform raw materials into commodities or specialties of fine chemistry. This transformation is made through unit operations that use large amounts of heat and energy. These industries help to meet the world's most fundamental needs for human beings. And the major challenges to be faced in the future are to meet the needs of the present without compromising the needs of the future. The necessity to make processes much more energy efficient, safer and more flexible to meet these challenges entails an increase of industrial competitiveness within the global economy.

A new trend characterizes the Chemical Process Industry in order to change the scale in facilities and activities [1]. In the past, the main interest was focused on reactors, separators and other unit operations. Nowadays the modeling, design, controls and

optimization of the process is a new interest for the chemical plants and complexes, where new process technologies are developed and with less historical experience for a safer operation.

There is a continuous growing of complexity in the Industrial Processes as result of new trends and changes that the Industry is facing, as summarized in Table 1. This results in safety and more effective control instrumentation systems but at the same time there are more difficulties to manage them as consequence of the automation increase and complexity. New kind of problems has arisen due to new failure modes as PES technology is implemented in these systems using microprocessors as PLC.

**Table 1 Actual and Emerging Situation**

NOW	FUTURE
Low-cost production materials – Commodities	High-tech and performance materials
Long-lifecycle products	Short-lifecycle products
Competency in national markets	Competency in global markets
High capacity process	Low scale process
Continuous process	Batch process
Construction of dedicated plants to one product	Construction of flexible and versatile plants
Low and simple analysis equipment	Very sophisticated analysis systems

### **3. SAFETY AND INSTRUMENTED SYSTEMS IN THE PROCESS INDUSTRY**

Most of equipment installed in today's plants with industrial processes operate at high conditions of pressure and temperature with the purpose of achievement the prime goal of transformation. Also the processing of materials with flammable and toxic properties entails hazards. Therefore a large amount of energy is involved in the chemical processes with risk for major accidents and their control is demanded by the Authorities.

The concept of safety is directly related to risk because of as much safety is obtained as less risks are present. The safety is understood as the freedom from unacceptable risk of physical injury or of damage to the health of people, either directly or indirectly as a result of damage to property or to the environment. Over the years, the *reactive safety* is manifested when you spend amounts of money to achieve safety but there is a certain maximum level where the minimum risks never can be achieved as much money is spent. This *safety* covers the investment of equipment, safety-related devices and the stamps and verification of the equipment according to the norms and regulations. The advance on quantitative assessments to calculate the process risk numerically is known as *calculus safety*. Current regulations demand the implementation of management systems where risk analyses are framed to calculate the process risks and keep them under tolerable levels for the Society. The purpose of the Process Safety Management Systems is to ensure the achievement of Process Safety. These analyses are very useful tools for decision making but have a maximum monetary level too. Nowadays there exists also a *preventive safety* that is being enhanced to empower the corporative culture and safety

values, such programs as “zero incidents”. This stage emphasizes the safety culture because create value within the companies and improve the accident rates [13].

Recently people and latest standards talk about the *functional safety*. This concept is part of the overall safety. The functional safety depends on a system or equipment operating correctly in response to its inputs. Examples of Functional Safety are overpressure protection devices for relieving of a pressure vessel and stopping material and heat input by a pressure sensor. Providing thicker wall thickness to withstand high pressures is however not functional safety but protect against the same hazard.

The process safety management embodies all kinds of safety and includes all measures and activities in industry to achieve an acceptable safe operation. Mismanagement and wrong decisions are demonstrated to be the deepest roots that cause accidents.

The main application of fire equipment is to provide heat input into the process by burning fuel in a combustion chamber. However there are other more specific applications such as the selective catalytic reduction systems, aimed to the general goal of transformation. There are multiple undesirable events that put process hazards in fired equipment. The event consequences are unacceptable because of the handling of hazard materials and the operation with extreme conditions. Some examples are excess combustibles, accumulation of flammable materials, failure to purge or misaligned of fuel valves, when those fired equipment are operated under any of their operation modes. The control of these chemical processes is carried out by automatic and instrumented systems. Their safety and control systems select and apply several techniques to operate the process plants safety, steady and efficiency during the mission time. Fired equipment as any other process equipment of the plant is continually subjected to external disturbances or influences, i.e. composition upsets, turn-downs or utility consumptions due to loss of efficiency, quality changes, etc. These disturbances require continuous surveillance and automatically actuation to correct them and keep the equipment under control.

Normally there is no a single cause that leads to hazard scenario. A severe accident's consequences are obtained after an event sequence or failure chain. This sequence is initiated by such event as equipment failure, process disturbances or human error. But some times a failure event is not enough and must be enabled by other events as safeguard failure, ignition source, personnel within vicinity, wind direction, etc. The automatic and control systems are implemented to operate the plant in a steady and safety manner. Therefore these systems are directly related to functional safety because they shall perform an action to keep a safe state of the plant. The functional safety is achieved with multiple hierarchic and protection layers.

1. Indication and local or remote measurement of process variables. These safeguards are not considered valid protection layers because they do not trigger a corrective action.
2. Control and regulation that correct automatically changing when a variable is manipulated to control other process variable on a set point. The main purpose is

to give stability and there are significant concerns to consider these safeguard as a real protection layer. The reliability and redundancy of these systems can be “good enough” for safety. But their dynamic is high and any failure can be revealed so the system either works or it does not [5].

3. The first two layers constitute the control system, herein referred to as BPCS. Alarms on elements allocated to the BPCS are implemented via sounds or lights in order to alert the operator. There is only a communication from the BPCS to the operator that something is wrong so an operator response is required to perform an action and prevent an incident.

Normal process control actions are generally not considered safety functions. But when operator is expected to take action in response to an alarm to prevent a safety incident, the operator alarm and associated action is considered as safety function. These alarms are classified as safety-related and are designed and managed in a manner that supports the allocated risk reduction.

4. An interlock system that detects an out-of-limit condition or improper sequence and either stops further action or starts corrective action.

When a component of “process interlocks” and “non-safety” interlocks fails it does not result in serious injury to personnel or in significant environment impact. However, when a safety function is allocated to this protection layer it constitutes a SIF and shapes the SIS. A SIF must be implemented via an independent instrumented system from the BPCS.

If a control failure to operate properly directly results in a catastrophic release of toxic, flammable, reactive or explosion material, the instrumented system is considered as safety critical control.

5. Finally, in case all previous protection layers failing, mitigation instrumented systems are activated to reduce the final consequences of an undesired hazardous event.

Then two capabilities of these systems are required to allocate a safety function to this protection layer:

- a. Detect the loss of containment of hazardous material.
- b. Take an effective automatic action to mitigate the release impact.

#### **4. WHERE ARE STANDARDS AND REGULATIONS PLACED?**

The industrial development demands more and more quality and help to preserve the environment and security. Unfortunately historical and also recent incidents confirm us

that there exists the possibility of disasters and there is still a probability of occurrence in the future. Table 2 summarizes most recent incidents in the Process Industries.

**Table 2 Most recent incidents in Process Industry**

DATE	INCIDENT	DESCRIPTION
Feb 2008	<b>Imperial Sugar Company Explosion and Fire</b>	Caused 13 deaths and left others critically injured with severe burns by combustible sugar dust
Dec 2007	<b>T2 Laboratories Inc. Explosion and Fire</b>	4 people were killed and 13 others were transported to the hospital when an explosion occurred during the production of a gasoline additive
Jan 2007	<b>Little General Store Propane Explosion</b>	4 people were killed and 5 others were seriously injured when propane vapors from a storage tank ignited and exploded
Dec 2005	<b>Buncefield Incident</b>	Explosion resulted from the ignition of a vapor cloud emanating from an overfill of unleaded petrol
Mar 2005	<b>BP America Refinery Explosion</b>	A series of explosions occurred at the BP Texas City refinery during the restarting of a ISO unit. 15 workers were killed and 180 others were injured.
Sep 2001	<b>AZF Chemical Fertilizer Factory Explosion</b>	29 deaths and 2,200 injuries caused by a blast explosion of unknown NH <sub>4</sub> NO <sub>3</sub> amount
Jun 2000	<b>Kuwait National Oil Refinery Gas Explosion</b>	5 people were killed and 49 seriously injured
Dec 1999	<b>Thai Oil Refinery Gasoline Storage Tank Explosion and Fire</b>	7 people died and thousands forced to flee their homes

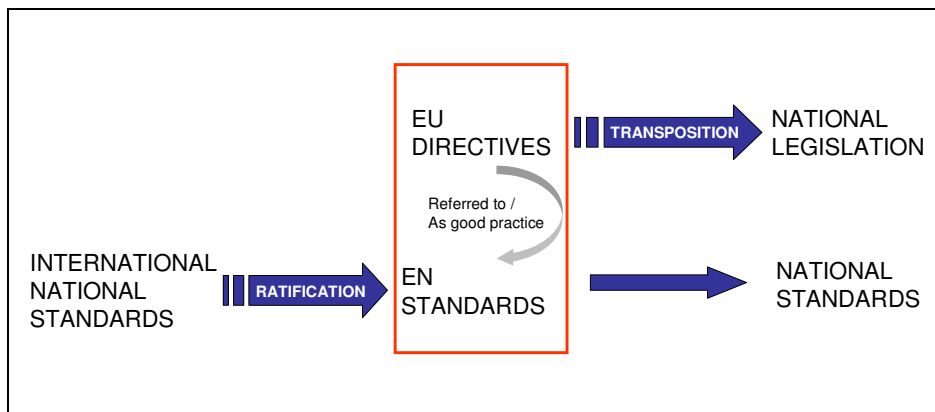
The national and European regulations related to safety and control of major hazards state requirements in a general way. That implies that some tools that help us are needed to fulfill them. Normative references are used as good practices only for information with voluntary application. These references help to demonstrate that the generic requirements stated in the regulations are fulfilled. Normative and standards content technical specifications based on the experience and technology developments. The interested parts consent their contents and are approved by recognized standardization bodies. Standards are tools that contribute to the industrial development because they improve quality, design, manufacturing and services and therefore they increase the competitiveness.

Since the mid-1970s, the Process Industry is focused on a distinctive approach for hazards and failures. Greater emphasis is put on such technological measures to control hazards. One of the best known and widely accepted solutions concerns the use of dedicated SIS in the Process Industry using PES technology. Several standards have been published recently in order to control the design and implementation of these technical solutions. The contents comprise of technology-oriented requirements and risk-based concepts to consider the implementation of this solution as adequate [8].

The reader should already know that we are talking about the generic standard IEC 61508 related to functional safety and safety-related systems. This standard is valid for all relevant sectors - Process, Power Plants, Traffic and Machinery - and there are application standards for end users as IEC 61511 to the Process Industry and IEC 62061 to Machinery.

The minimum requirements for safety in the Process Industry are stated by Directives in the European Union. The adoption of “New Approach” consists of the application of harmonized EU standards accordingly. The compliance of technical standards gives the suspicion of compliance with the essential requirements of specific legislation that are defined in general terms. The adoption of international standards such as ISO or IEC is not mandatory but the European standardization bodies require their members the adoption of European standards. These standards facilitate the remove of technical boundaries between the members of the EU. With this common policy, the voluntary nature is kept but there is a presumption or proof of compliance with the European directives requirements. In recent years, IEC 61508 Part 1-7, IEC 61511 Part 1-3 and IEC 62061 standards have been ratified by CELENEC as EN standards. As well IEC-EN 62061 standard is constituted as reference and title of harmonized standard under Directive 98/37/EC on Machinery to provide CE marking since 2005.

Figure 1 “New Approach” in the European Policy



The IEC standards adopt a new risk-based approach that tailors the safety instrumented equipment to the needs of the application. This approach has significant safety and economic benefits as it is intended to be demonstrated by this paper. The approach of original standards as NFPA 85 or API 556 is prescriptive to design the control systems of fired equipment. These design guidelines state specific equipment to be used to ensure a steady and safety operation. In fact the original codes identify the process variables that have to be measured and where the valves have to be located to protect them. However the increase of complexity in new applications of available equipment has made the prescriptive approach insufficient. The functional safety standards require independency between control and safeguarding functions and the original approach describe the implementation of both functions in combined and dedicated control system defined as BMS. Also the risk-based approach demands more management, competency of personnel, planning and technical judgment during all design stages.

## 5. FIRE EQUIPMENT AND BURNER MANAGEMENT SYSTEM – CASE STUDY: THERMAL BURNER

This paper presents a case study of a Thermal Burner designed to oxidize the H<sub>2</sub>S. The sulphur compound is contained in the acid gas produced in the amine and sour water stripping units of a Refinery. The H<sub>2</sub>S is then transformed into SO<sub>2</sub> within this thermal stage. The material is partially burnt with air and sent to two conventional Claus catalytic reactors. The design was developed during the FEED phase by a Licensing company and completed during the detailed engineering by a Contractor company. The general purpose was to complete the basic design developed in accordance to NFPA 85 and EN 746-2 codes with the new risk-based approach required by the functional standards in order to optimize the equipment design. These design codes as well as the functional standards were required by the owner.

The original codes are like a “design *cookbook*” of good engineering practices to operate the fire equipment safety. These guidelines provide requirements and recommendations for designs with the purpose of prevent the fire and explosions hazards. One of those requirements is an automatic instrumented system for the burner operation or BMS. The BMS is a dedicated combustion system to operate fired equipment with no operator intervention to minimize the human errors during start-up, shut-down and normal operation. Current engineering practices entail the integration of control and safety functions within the same logic controllers under next considerations:

- Functions of control system do not compromise the safety function performance.
- HMI and communications of control system do not compromise the safety function performance.
- The safety logic controller is fail-safe and de-energize-to-trip.
- Authorization access is required for the safety logic controller settings.
- Safety software is independent than control software.
- Changes in service are not allowed.

The safety devices required by the harmonized EN 746 standard are summarized in Table 3 for the different subsystems of Thermal Burner.

**Table 3 Safety devices required by EN 746 standard**

Sub-system	Safety Device
<b>Process</b>	<ul style="list-style-type: none"> <li>▪ Temperature measurement at the process outlet</li> <li>▪ Flow measurement at the process inlet</li> </ul>
<b>Air-gas</b>	<ul style="list-style-type: none"> <li>▪ Blower status indicator</li> <li>▪ Air flow measurement</li> <li>▪ Firebox pressure transmitter</li> </ul>
<b>Fuel gas</b>	<ul style="list-style-type: none"> <li>▪ Isolation manual valve</li> <li>▪ Filter</li> <li>▪ Fuel-gas measurement</li> <li>▪ Double block and bleed valves</li> </ul>
<b>Flame</b>	<ul style="list-style-type: none"> <li>▪ Self-checking flame detector</li> </ul>

However the original codes approach does not tailor the equipment's safety functions 'fit-for-purpose' as oriented in the functional standards. Additionally these standards require complete independency between the control and safety systems. The design can be optimized reducing investment and operation costs without compromising on safety. IEC-EN 61511 standard establishes to the Process Industry two main requirements to achieve the Functional Safety and optimize the safety design:

- A safety lifecycle defined for the activities involved in the analysis, design and operation of sis to prevent systematic failures. Most of those failures are result of design faults, so the systems are not capable to perform its intended function.
- Performance-based verification to prevent random or physical failures via reliability analysis.

The safety lifecycle is a document step procedure intended to make no mistakes during the design and operation of SIS. A working model is shown in the Figure 2 in a simplified way for a project level.

**Figure 2**

**Error! Not a valid link.**

## **5.1. Process Hazard Analysis**

IEC standards require an initial process hazard analysis to determine the event sequence or failures that can lead to hazardous scenarios. A regular HAZOP was carried out as hazard analysis for the case study. This analysis enables to identify those safety functions implemented by PES or SIF. SIF includes specific sensors, logic solvers and final elements to detect the hazard within the demand scenario. They take the specific actions based on the design intent to bring the system into a safe state and avoid the possible consequences of failure on demand.

As HAZOP result a total number of 17 Safety Instrumented Functions were identified and implemented by the elements that compose the BMS. Table 4 indicates the identified SIF and their design to prevent a specific hazardous event.

One of the many common errors that are made during the identification of SIF [6] is not to include all the process measurements that can detect the hazardous condition. The demand scenario and design intent are the same in the case of SIF BMS-2, 9, and 16. Therefore the air flow transmitter, air pressure transmitter and flame detectors are included in the same SIF because any of them can detect the loss of flame in the burner and the risk of internal fire inside the firebox.

**Table 4 Process Hazard Analysis**

Safety Function:	Description:	Demand scenario:	Design Intent:	Consequence at failure on demand:
BMS-1	Low flow of nitrogen purge	- Valve inadvertently closed	Impossibility to start-up the unit	Increase of H <sub>2</sub> S burnt in incinerator with downtime
BMS-2 BMS-9 BMS-16	Low flow of combustion air Low pressure of combustion air (2oo3) Flameout (2oo2)	- Air blower failure - Manual valves inadvertently closed - Pressure control loop failure	No flame in the burner with loss of sulphur recovery and accumulation of flammable material	Internal fire with no loss of containment
BMS-3	Low flow of amine acid gas	- Operator error - Demister blocked - Flow control loop failure	Loss of acid gas feed and bad combustion in burner with possible plugging of reactor downstream	Increase of H <sub>2</sub> S burnt in incinerator with downtime
BMS-4	High level in Amine Acid Gas KO Drum (2oo3)	- Abnormal incoming liquid feed - Level control loop failure - Manual valves inadvertently closed	Liquid carryover to the burner with pressure increase due to liquid expansion leading to internal potential mechanical damage to equipment	Increase of H <sub>2</sub> S burnt in incinerator with downtime and partial replacement of internals
BMS-5	High level in Sour Water Acid Gas KO Drum (2oo3)	- Abnormal incoming liquid feed - Level control loop failure - Manual valves inadvertently closed	Liquid carryover to the burner with pressure increase due to liquid expansion leading to internal potential mechanical damage to equipment	Increase of H <sub>2</sub> S burnt in incinerator with downtime and partial replacement of internals
BMS-6	Low level in Waste Heat Boiler (2oo3)	- Flow control loop failure	More amine acid gas flow with heat duty increase in thermal reactor with loss of sulphur recovery	Increase of H <sub>2</sub> S burnt in incinerator with downtime
BMS-7	Low level in Waste Heat Boiler (2oo3)	- Level control loop failure - BW valves inadvertently closed	Potential tube rupture with loss of cooling in the process gas leading to mechanical damage	Increase of H <sub>2</sub> S burnt in incinerator with downtime and replacement of damaged equipment
BMS-8	High level in Fuel Gas system	- Abnormal heavier hydrocarbon	Liquid carryover to the burner with loss of flame and potential accumulation of flammable material with risk of uncontrolled fire or explosion	H <sub>2</sub> S burning in flare system and partial replacement of burner internals

Safety Function:	Description:	Demand scenario:	Design Intent:	Consequence at failure on demand:
BMS-10	High burner pressure (2oo3)	- Reactor plugging downstream	Pressure drop increase causing higher pressure in the burner with loss of sulphur recovery	Increase of H <sub>2</sub> S burnt in incinerator with downtime
BMS-11	High burner pressure (2oo3)	- Flow control loop failure	More amine acid gas with potential pressure increase in thermal burner with loss of sulphur recovery	Increase of H <sub>2</sub> S burnt in incinerator with downtime
BMS-12	High burner pressure (2oo3)	- Hand valve inadvertently open - Heater partially plugged downstream	Pressure drop increase causing higher pressure in the burner with loss of sulphur recovery	Increase of H <sub>2</sub> S burnt in incinerator with downtime
BMS-13	High burner pressure (2oo3)	- Steam tracing failure - Temperature control loop failure downstream	Potential line plugging causing pressure increase in Claus unit sending unconverted SO <sub>2</sub> sent to the quench column causing operational problems	Shutdown of the unit with associated maintenance costs
BMS-14	High burner pressure (2oo3)	- Manual valve inadvertently closed - Line/Sulfraps plugging - No liquid sulphur outlet	Accumulation of sulphur inside the waste heat boiler and the condensers causing a pressure increase in the Claus unit	Shutdown of the unit with associated maintenance costs
BMS-15	Low pressure in Fuel Gas	- Pressure control loop failure - Manual valves inadvertently closed - Filter plugging	No fuel gas to burner during start-up not being able to light it on	Maintenance and cleaning of demister. Spare fuel gas supply
BMS-17	Flameout (2oo2)	- Loss of fuel gas supply during start-up	Loss of flame during start-up causing the presence of air around the catalyst damage during start-up	Increase of H <sub>2</sub> S burnt in incinerator with short downtime and unit shutdown

## 5.2. Allocation of Risk reduction to Safety Functions

Next step in the IEC workflow shown in Figure 2 is the allocation of risk reduction. This activity implies to determine the total quantity of required risk reduction first. The SIL represents the amount of risk reduction that an SIS can provide [10] so the required risk reduction determines a Target SIL.

$$RRF = \frac{\text{Unmitigated Process Risk}}{\text{Tolerable Risk}}$$

IEC-EN 61511 requires an allocation process resulting in determine the required SIF and determine the associated SIL for each SIF. The standard establishes four SIL categories [3] as shown in Table 5 depending on the demand mode of operating SIF and defines the SIL in terms of  $PFD_{AVG}$ . The mode of operation is the way in which the SIF is operated with respect to the frequency of demands. Low demand mode for each SIF is considered because of its frequency of demands is intended no greater than one per year or no greater than twice the proof-test frequency. The target  $PFD_{AVG}$  is determined by the required risk reduction.

$$PFD_{AVG} = \frac{1}{RRF} \rightarrow SIL$$

**Table 5 Safety Integrity Levels for Demand mode of Operation**

SIL	$PFD_{AVG}$	RRF
4	$\geq 10^{-5}$ to $< 10^{-4}$	$> 10.000$ to $\leq 100.000$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$> 1.000$ to $\leq 10.000$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$> 100$ to $\leq 1.000$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$> 10$ to $\leq 100$

The total risk reduction can be achieved using several protection layers. Each protection layer performs a specific function in accordance to its design intent to prevent the hazardous situation. The engineering, installation and operation of SIS can be very expensive if the integrity requirements are overspecified in accordance to the total risk reduction. So other technologies must be used to reduce the SIL requirements of SIS.

The allocation of risk reduction to other protection layers with assigned safety functions may include SIS layers as well as non-SIS layers. This allocation must be done under considerations to give credit to non-SIS layers and subtract the equivalent level of integrity to the total quantity of risk reduction. This SIL credit is assigned in accordance to the PFD values of each protection layer but other considerations must be taken account such as intended function for the demand scenario, correct design and effectiveness. Not all protection layers are valid. IEC-EN 61511 standard proposes guidelines to identify those reliable protection layers or IPL. Specificity, independence, dependability and audit ability are characteristics that have to be met to categorize a protection layer as IPL. Minimum 100-fold risk reduction as well as 90% availability are requirements demanded for IPL.

In the proposed case study of a Thermal Burner only BPCS alarms with associated operator response and pressure relief devices are categorized as Independent Protection Layers. This classification is made in accordance with the IEC-EN 61511 guidelines. Next SIL credits are specified in Table 6.

**Table 6 SIL credit for IPL**

Protection layer	PFD	SIL credit
BPCS alarm with human response with 20 min response time	$10^{-1}$	1
Relief Valve	$10^{-2}$	1

The Human response PFD is limited by IEC-EN 61511 and therefore care is needed when credit is taken for risk reduction. When the risk reduction claimed is greater than 10, and then the alarm system has to be designed according to IEC-EN 61511. The sensor used has not to be used for control purposes and to be part of the SIS. Finally SIL credit 1 is allocated to operator response to BPCS alarms but next considerations also shall be taken into account [7]:

- Alarm criticality.
- Analysis of operator action and recording in operator manual as critical action.
- Enough sufficient time for operator response.

The final SIL selection is presented in Table 7. This selection is made for each SIF and determined subtracting the equivalent level of integrity of the independent protection layer based on its PFD. Some SIF perform safety actions under scenarios that the hazard analysis identified as low risk. Their allocated risk reduction is very small so a target SIL is not required for them.

**Table 7 SIL selection**

Safety Function	Target SIL	Required SIL	Independent Protection Layer
BMS-1	NR	NR	
BMS-2 BMS-9 BMS-16	1	1	
BMS-3	1	1	
BMS-4	1	1	
BMS-5	1	1	
BMS-6	NR	NR	High Flow Alarm for operation
BMS-7	1	NR	Pressure Relief Valve
BMS-8	1	1	High Level Alarm with no credit for operator response due to required time less than 20min
BMS-10	NR	NR	
BMS-11	NR	NR	High Flow Alarm for operation
BMS-12	NR	NR	
BMS-13	1	NR	High Temperature Alarm with credit for operator response
BMS-14	1	1	
BMS-15	NR	NR	
BMS-17	NR	NR	

The SIL selection method used in this case study is a Hazard Matrix accordingly to the guidelines of IEC-EN 61511 standard. Table 8 indicates what kind of receptors determined the most severe SIL ranking.

**Table 8 SIL Hazard Matrix Receptors**

Target SIL	SIF	%	Hazard Matrix Selection		
			Safety	Asset Losses	Environment
NR	10	59	4	5	1
SIL1	7	41	1	4	2
SIL2	--	0	--	--	--
SIL3	--	0	--	--	--
SIL4	--	0	--	--	--
<b>Total SIF</b>					
	17	100			

### 5.3. Determination of SIS Functional Requirements

The SIF definition is the next step to continue with the workflow required by IEC-EN 61511. This definition covers to specify integrity and functional requirements. The safety functional requirements are the definition of the safe state of the process. This specification is made for each identified events and involves sequencing and intermediate state. Considerations for response time are made. Once more the design codes as well as functional standards are used in combination for the BMS design. The NFPA 86 standard indicates that each burner has to be monitored by individual flame detectors with 4 seconds as maximum response time when the maximum firebox temperature exceeds 760 °C. The SIF definition includes the functional relationship between the process measurements that detects the hazard and the final elements that have to be actuated to achieve the safe state of the Thermal Burner.

Another very common error made during the definition of SIF for BMS [6] is include secondary actions that are not intended to achieve or maintain a safe state. The results of this error have significant impact in the required performance calculations. This reliability analysis is required by functional standards in order to validate the proposed design of equipment and system architecture. The validation verifies that the achieved SIL obtained after calculations of  $PFD_{AVG}$  is in accordance with the required SIL determined by the required risk reduction.

The BMS concept consists of detectors, shut-down devices, interlocks, alarms and shut-off valves to ensure safe conditions during the various operation modes of fired equipment. In a general way the sequences are:

- [1] Master Fuel Trip or total shutdown.
- [2] Pre-firing cycle or purging of chamber.

[3] Burner light-on cycle.

[4] Normal operation.

The design code requires a log of trips depending on the burner configuration and the operation mode. The safety functions of pre-firing cycle require permissives to confirm the purge of chamber is done properly and there is no flame. When the fired equipment is under light-on cycle same loss of flame protections are required but with a time delay service. Therefore the SIL application in BMS is performed only during normal operation. Furthermore during this operating sequence the demand mode of each SIF is kept low because of the SIF demand is not intended greater than once a year or twice the proof-test frequency.

A master fuel trip is defined as intended function for most of the SIF. This trip isolates all fuel sources when a possible mechanical damage to equipment is identified. However the SIF BMS-5 only requires the stop of sour water acid gas. The Thermal Burner operates normally with acid gas from amine and sour water units. But also it operates with acid gas coming from amine unit. Therefore a sour water liquid carryover only demands the isolation of sour water knock-out drum because the fired equipment is available to operate with amine acid gas.

There is other issue for applying the risk-based concepts into the BMS design in combination with the prescriptive requirements. A master fuel trip is required by the original design codes and demands multiple actions. The BMS logic responses with a total shutdown. The verification results shall confirm that the required risk reduction is achieved. But this validation can be compromised when a SIF is not defined properly and its functional requirements are bad specified. There is a mistake when all actions for total shutdown are included in the same functional requirements of the same SIF.

The SIF concept is defined as a set of sensors, logic solvers and final elements intended to achieve or maintain a safe state for the equipment in respect of a specific hazardous event. In fired equipment there are multiple consequence scenarios for the same demand scenario. And multiple initiating causes can lead to same demand scenario. The Process Hazard Analysis carried out for this case study identified the demand scenarios that require the execution of a SIF. This SIF is implemented by the BMS. However the multiple consequence scenarios that lead to different hazardous situations can be classified as separate SIF [14].

The final elements and required actions to bring the process to safe state are selected and included in the SIF definition. The rest of interlock actions are considered as non-safety. The other point is the hierarchy or sequence of the safety actions. In the case study the safety actions are sequenced in main four groups:

- Main fuel sources of amine and sour water acid gas are isolated to avoid uncombusted flammable material in the firebox. Thermal Burner is fed with only with both combustible during normal operation.
- Fuel gas isolation is considered as a secondary preventive action as fuel gas is not supplied to the Thermal Burner under normal operation.

- Combustion air is not a flammable material with inherent risk of explosion or fire. But the continuous feed of air to the system can carry potential fire risk in reactors downstream due to contact with liquid sulphur.
- The tail gas vent is considered as a safety action to divert the Thermal Burner outlet to the Tail Gas Section and bring the unit to safe state.

A breakdown of the SIF implemented by BMS for a master fuel trip is summarized in Table 9. Non-safety actions shall be tripped when a hazard is detected but they are not part of each SIF and therefore no functional and integrity requirements have to be specified neither validated.

**Table 9 Functional Requirements of SIF**

Master Fuel Trip Safety Functions	Master Fuel Trip Non-safety Functions
Main fuel sources (2oo2) of amine acid gas and sour water acid gas cut-off	Amine Acid gas control valve Sour water acid gas control valve
Fuel gas source double-block-and-bleed arrangement (1oo2)	Fuel Gas Bleed Valve
Combustion air source (1oo1)	Quench steam
Tail gas vent (2oo2)	Nitrogen purge valve cut-off

#### 5.4. Determination of SIS Integrity Requirements

The specification of functional requirements for SIS design means what the safety function is intended to do. Furthermore the functional standards require integrity requirements to design the equipment ‘fit-for-purpose’. This tailoring optimizes the design in order to achieve the target functional safety required by the risk reduction. Overspecifications and unnecessary redundancy encompasses larger investment and operational cost but also higher rate of spurious trips with loss of production and monetary losses.

The safety lifecycle model requires the specification of functional requirements to avoid systematic failures about what the system should do. But it also requires the integrity requirements specification to prevent random failures about how well it should do. The integrity requirements are the likelihood of a safety function performing its actions satisfactorily.

Functional standards require including a set of parameters and factors for the  $PFD_{AVG}$  calculations such as:

- Requirements for Diagnostic to notify when a problem occurs.
- Requirements for Maintenance and Testing to ensure that the system satisfies the functional requirements.
- Reliability requirements for spurious trips related to safety and economic losses.

Most of the design codes do not cover this kind of risk-based specifications. However EN 746 normative specifies briefly the necessity for providing auto-checking in the flame detectors.

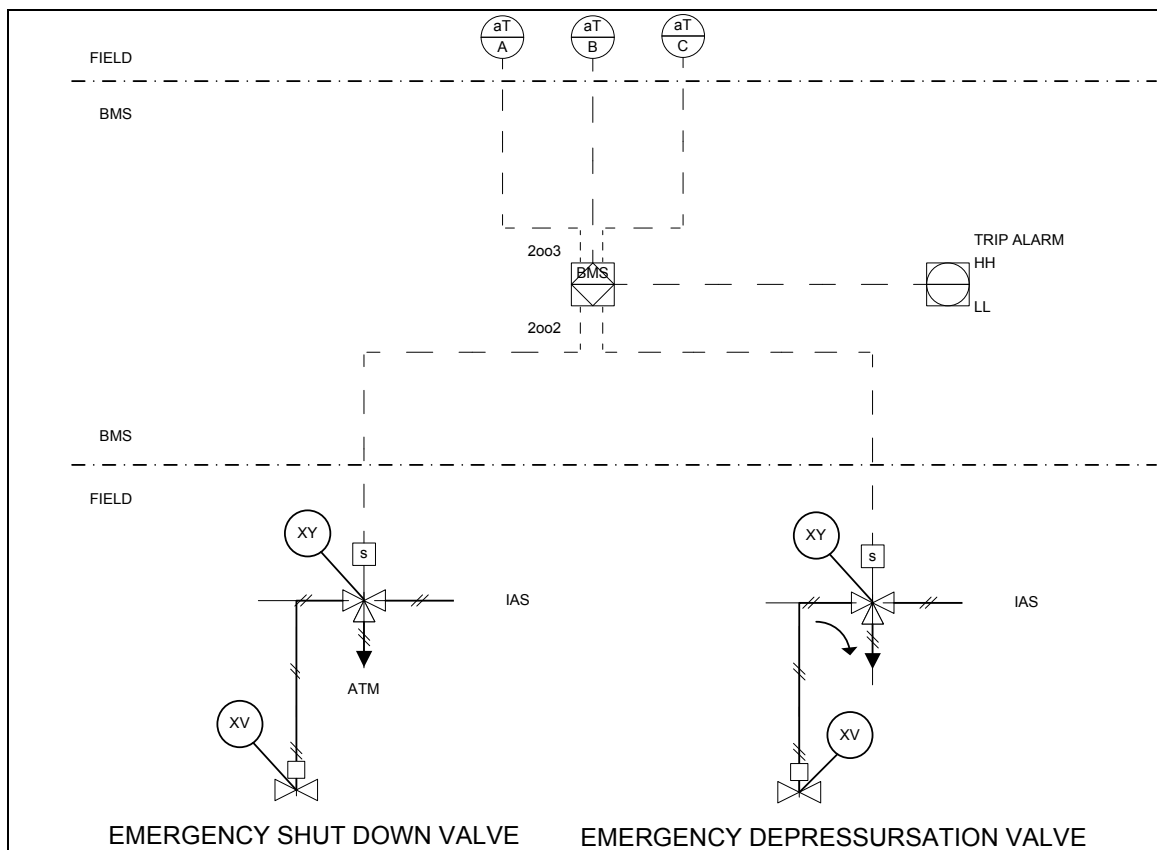
## 5.5. Performance Analysis of Proposed Equipment

As part of the required workflow the proposed design from FEED phase must be validated through a reliability analysis to verify the performance is in accordance with the required risk reduction. The probabilistic calculations are carried out considering the maximum interval between proof-testing for the SIF that corresponds to the interval at which the process plant is shut down for maintenance.

The initial selected equipment and architecture after the FEED phase is indicated in Figure 3. This configuration is selected for implementing SIS functions with SIL1 or higher requirements. The scheme shows sensor architecture with voting type 2oo3 and final elements with voting type 2oo2 to close shut-off valve and to open depressurization valve. Transmitters are selected as sensor technology due to their higher reliability and because due to the fact that measurements can be compared enhancing the diagnostics capabilities.

Part of the objectives of this technical paper alternative is to evaluate architectures in detail engineering looking at the most effective cost-benefit ratio.

Figure 3



In Table 10 the results of SIL performance analysis are presented for the initial configuration proposed during the FEED phase. A Honeywell FSC 2oo4D is used as programmable system with fault diagnostics. Failure rates are obtained from a

commercial database [4]. The SIL requirements are achieved for all SIF implemented via BMS. And there are even some safety actions that are performed with excess of reliability with respect to the required risk reduction. The performance analysis is carried out for 24 months as proof test that is the period stated between shut downs for maintenance purposes. The spurious trip criteria are also satisfied for all SIF because of the MTTFS is higher than 10 years as required.

**Table 10 SIL Performance Analysis for proposed equipment in FEED**

Safety Function:	Description:	SIL Required	Proof Test (month)	MTTR (hr)	Safety Action	SIL Achieved	PFDavg	RRF Achieved	MTTFS (yrs)
BMS-2	Low flow of combustion air	1	24	8	Acid gas	1	5.34E-02	19	158.61
BMS-9	Low pressure of combustion air (2oo3)				Fuel gas	2	2.39E-03	419	32.81
BMS-16	Flameout (2oo2)				Tail gas	1	4.75E-02	21	158.47
					Combustion Air	1	2.22E-02	45	54.66
BMS-3	Low flow of amine acid gas	1	24	8	Acid gas	1	5.82E-02	17	103.85
					Fuel gas	1 <sup>(1)</sup>	8.73E-03	115	30.77
					Tail gas	1	5.36E-02	19	120.07
					Combustion Air	1	2.84E-02	35	49.23
BMS-4	High level in Amine Acid Gas KO Drum (2oo3)	1	24	8	Acid gas	1	5.73E-02	17	394.54
					Fuel gas	2	6.43E-03	156	37.44
					Tail gas	1	5.14E-02	19	393.65
					Combustion Air	1	2.61E-02	38	68.84
BMS-5	High level in Sour Water Acid Gas KO Drum (2oo3)	1	24	8	SW acid gas	1	3.21E-02	31	69.21
BMS-8	High level in Fuel Gas system	1	24	8	Acid gas	1	7.71E-02	13	301.27
					Fuel gas	1	2.73E-02	37	36.37
					Tail gas	1	7.13E-02	14	300.75
					Combustion Air	1	4.66E-02	21	65.31
BMS-14	High burner pressure (2oo3)	1	24	8	Acid gas	1	5.43E-02	18	370.63
					Fuel gas	1 <sup>(1)</sup>	3.29E-03	304	37.22
					Tail gas	1	4.84E-02	21	369.84
					Combustion Air	1	2.31E-02	43	68.07

Note (1): Achieved SIL by Architectural constraints IEC 61511

Other functional requirement is related to the system ability to continue to be able to perform the safety function in the presence of dangerous faults in hardware. This requirement is known as Hardware Fault Tolerance and is determined by the Safe Failure Fraction.

$$SFF = \frac{\lambda^{SD} + \lambda^{SU} + \lambda^{DD}}{\lambda^{SD} + \lambda^{SU} + \lambda^{DD} + \lambda^{DU}}$$

SFF is defined as the ratio of the average rate of safe failures plus dangerous detected failures of the system to the total average failure rate of the system. For PLC a minimum HFT is required in accordance to IEC-EN 61511 standard. For the SIF BMS-3 and BMS-14 the achieved  $PFD_{AVG}$  corresponds to SIL 2 but the HFT requirements by functional standards allow a maximum SIL 1. This architectural constraint ensures that the SIF shall perform in the presence of some dangerous faults in hardware.

During the detail engineering some modifications are proposed with the purpose of optimize the design and reduce de excess of reliability that is not required. This optimization is analyzed via cost-benefit analysis. The recommendations are:

- Voting type 1oo2 for pressure detection
- Single level transmitter to detect overfilling in acid gas knock-out drums.

The SIL performance calculations are shown in Table 11. The SIL requirements are also achieved for all SIF as well as the spurious trip criteria. MTTFS values are kept higher than 10 years.

Table 11 SIL Performance Analysis for proposed equipment after Detailed Engineering

Safety Function:	Description:	SIL Required	Proof Test (month)	MTTR (hr)	Safety Action	SIL Achieved	PFDavg	RRF Achieved	MTFS (yrs)
BMS-2	Low flow of combustion air	1	24	8	Acid gas	1	5.34E-02	19	34.85
BMS-9	Low pressure of combustion air (1oo2)				Fuel gas	1 <sup>(1)</sup>	2.38E-03	420	18.92
BMS-16	Flameout				Tail gas	1	4.75E-02	21	34.85
					Combustion Air	1	2.22E-02	45	24.58
BMS-4	High level in Amine Acid Gas KO Drum	1	24	8	Acid gas	1	7.71E-02	13	301.27
					Fuel gas	1	2.73E-02	37	36.37
					Tail gas	1	7.13E-02	14	300.75
					Combustion Air	1	4.66E-02	21	65.31
BMS-5	High level in Sour Water Acid Gas KO Drum	1	24	8	SW acid gas	1	2.88E-02	35	69.54
BMS-14	High burner pressure (1oo2)	1	24	8	Acid gas	1	5.39E-02	19	132.5
					Fuel gas	1 <sup>(1)</sup>	2.90E-03	345	31.53
					Tail gas	1	4.84E-02	21	134.71
					Combustion Air	1	2.27E-02	44	51.18

Note (1): Achieved SIL by Architectural constraints IEC 61511

Architectures 2oo3 are best performed. This voting type gives reliability in terms of PFD<sub>AVG</sub> due to the triple transmitter redundancy. But also it gives availability in terms of spurious trip because of two signals are required to trip. However architectures 1oo2 are still valid in terms of PFD<sub>AVG</sub>. This option is recommended as the spurious trip requirements for the design case are not very restricted. As well as risk reduction requirements are also not very tight the overfilling protection is covered by single level transmitters.

For comparison the Benefit-to-Cost Ratio is calculated for both system architectures in order to analyze the cost effectiveness of potential risk reduction [10]. There exists benefits for implementation when this ratio is higher than 1.

$$B - C_{RATIO} = \frac{F_{NO-SIS} \cdot EV_{NO-SIS} - F_{SIS} \cdot EV_{SIS}}{Cost_{SIS} + Cost_{N-T}}$$

Operation, design, installation and start-up are assumed to be very similar for both architectures in the SIS costs calculation. Earning value and nuisance trips are

evaluated on a 100,000 € basis. Calculations and results are shown in Tables 12-13 for comparing the FEED design in regards to the detailed design.

**Table 12 Cost-Benefit Analysis for proposed equipment in FEED**

Architecture system with 2oo3 voting type						
Safety Function:	Safety Action	SIS Costs	Cost N-T	F-EV event no-SIS	F-EV event SIS	B-C
BMS-2 BMS-9 BMS-16	Acid gas	44540	630	200000	1068	4.40
	Fuel gas	44540	3048	200000	47.8	4.20
	Tail gas	44540	631	200000	950	4.41
	Combustion Air	39540	1829	200000	444	4.82
BMS-4	Acid gas	35540	253	200000	11460	5.27
	Fuel gas	35540	2671	200000	1286	5.20
	Tail gas	35540	254	200000	10280	5.30
	Combustion Air	30540	1453	200000	5220	6.09
BMS-5	SW acid gas	30540	1445	200000	6420	6.05
BMS-14	Acid gas	35540	270	200000	10860	5.28
	Fuel gas	35540	2687	200000	658	5.21
	Tail gas	35540	270	200000	9680	5.31
	Combustion Air	30540	1469	200000	4620	6.10

**Table 13 Cost-Benefit Analysis for proposed equipment in Detail Engineering**

Architecture system with 1oo2 voting type						
Safety Function:	Safety Action	SIS Costs	Cost N-T	F-EV event no-SIS	F-EV event SIS	B-C
BMS-2 BMS-9 BMS-16	Acid gas	38540	2869	200000	1068	4.80
	Fuel gas	38540	5285	200000	47.6	4.56
	Tail gas	38540	2869	200000	950	4.81
	Combustion Air	33540	4068	200000	444	5.31
BMS-4	Acid gas	29540	332	200000	15420	6.18
	Fuel gas	29540	2750	200000	5460	6.02
	Tail gas	29540	333	200000	14260	6.22
	Combustion Air	24540	1531	200000	9320	7.31
BMS-5	SW acid gas	24540	1438	200000	5760	7.48
BMS-14	Acid gas	32540	755	200000	10780	5.68
	Fuel gas	32540	3172	200000	580	5.58
	Tail gas	32540	742	200000	9680	5.72
	Combustion Air	27540	1954	200000	4540	6.63

There is a significant improvement in Benefit-to-Cost ratio for SIF BMS-4 and BMS-5 where the architecture system is modified from 2oo3 to 1oo2 voting type for overfilling protection of Knock-out drums and prevention of liquid carryover to the Thermal Burner with risk of internal mechanical damage.

## **6. CONCLUSIONS**

- The increase of complexity and automation as well as new and advanced process technologies imply new risk and hazards in the Process Industry. And the use of PES technologies to ensure the safety in this new environment requires new approaches and concepts to design the Safety Instrumented Systems.
- The functional standards that present these concepts require a Process Hazard Analysis to design a SIS ‘fit-for-purpose’ and identify the demand scenario for the SIF. But multiple initiating causes can result in a hazardous situation which means that the overall addition of each initiator demand rate must be considered to determine the real likelihood of demand scenario
- Not including all sensors that detect a hazard, and include or exclude actions that are required or not to keep the equipment under control are common errors when a SIF is defined. A proper determination of what real safety actions are required is capital to validate the design. This issue can be addressed if we answer the question: “Does a safety component failure result in a hazard?”.
- SIF are specific actions for specific hazards. The inclusion of multiple safety actions in the same SIF implies poor results of the performance analysis to validate and leads to overspecification of the SIS. Overdesign results in higher frequencies of spurious trips and bad operability.
- Original design codes to design BMS in fired equipment must be used in combination with the functional standards. Such codes as NFPA 85, NFPA 86, API 556 or EN 746 are good design practices to determine the functional requirements that the BMS must perform as SIS. The specification of integrity requirements in accordance to functional standards IEC-EN 61508, IEC-EN 61511 and EN 50156-1 permit to optimize the design saving money and better operability without compromise safety.
- The correct selection of technology and system architecture has important benefits to costs. But any decision making about the equipment selection has to be made in accordance to the required risk reduction.

## **7. ACKNOWLEDGEMENTS**

I would like to thank in all the people in the Process and HSE taskforce who is leading the project to develop the design of this case study. As well as Mr. Victor Almenara, Fluor Project Management, who has managed for publishing this technical paper as an overall project success by all team.

I also want to thank to my colleagues Mr. Andre Fijan, Senior Process Control Engineer CFSE, and Mr. Simon Lucchini, Chief Control Specialist, from our Fluor Haarlem and Calgary offices for their assistance and review giving excellent help and feedback. And finally my special thanks to Mr. Paul Tullemans, Fluor Process and HSE Department Head, who provides me an outstanding support and confidence since

I joined to Fluor. As well as Mr. Hugo Barriaes, Fluor Business Development Director, for his encouragement and mentoring in the preparation of this paper.

## **8. ABBREVIATIONS**

1ooN	1 out of N
B-C Ratio	Ratio of benefits to costs
BMS	Burner Management System
BPCS	Basic Process Control System
CELENEC	European Committee for Electrotechnical Standardization
$COST_{NT}$	Total incurred by loss of production due to nuisance trips (annual basis)
$COST_{SIS}$	Total life-cycle cost of SIS (annual basis)
E/E/PE	Electrical, Electronic, Programmable Electronic
EN	European Normative
EU	European Union
$EV_{NO-SIS}$	Total expected value of loss of the event without SIS
$EV_{SIS}$	Total expected value of loss of the event with SIS
FEED	Front-End Engineering Design
$F_{NO-SIS}$	Frequency of unwanted event without SIS
$F_{SIS}$	Frequency of unwanted event with SIS
HAZOP	Hazard and Operability Analysis
HFT	Hardware Fault Tolerance
HMI	Human Machine Interface
IEC	International Electrotechnical Commission
IPL	Independent Protection Layer
ISO	International Organization for Standardization
MTTFS	Mean Time To Fail Spurious
MTTR	Mean Time To Repair
NFPA	National Fire Protection Association
NR	Not Required
PES	Programmable Electronic System
PFD	Probability of Failure on Demand
$PFD_{AVG}$	Probability of Failure on Demand Average
PLC	Programmable Logic Controller
SFF	Safe Failure Fraction
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System

## 9. REFERENCES

- [1] Wintermantel, K. *Process and Product Engineering Achievements, Present and Future Challenges*. Chemical Engineering Science 54 (1999): 1601-1620.
- [2] ANSI/ISA-91.00.01-2001: *Identification of Emergency Shutdown System and Controls That Are Critical to Maintaining Safety in Process Industries*.
- [3] BS IEC 61511:2003. *Functional safety – Safety instrumented systems for the process industry sector*.
- [4] Exsientia Version 2.4.0.25. Safety Equipment Reliability Handbook Database Version 2009.1.01. Exida, LLC.
- [5] Gruhn, Paul; Cheddie, Harry. *Safety Instrumented Systems: Design, Analysis, and Justification*. 2<sup>nd</sup> Edition, ISA, 2006.
- [6] ISA-dTR84.00.05: *The Application of ANSIISA 84.00.01-2004 Parts 1-3 to Safety Instrumented Functions (SIFs) in Burner Management System*. Draft version, 2007.
- [7] ISA-TR84.00.04-2005 Part 1: *Guidelines for the Implementation of ANSI/ISA-84.00.01-2004*.
- [8] Kenegterin, Berend. *Safety Lifecycle Management in the Process Industries*. CIP- Data Library Technische Universiteit Eindhoven, 2002.
- [9] Mannam Sam. *Lee's Loss of Prevention in Process Industries*. 3<sup>rd</sup> Edition.
- [10] Marszal, Edward M. *Systematic Methods Including Layer of Protection Analysis*, ISA.
- [11] NFPA 85. *Boiler and Combustion Systems Hazards Code*. 2007 Edition.
- [12] NFPA 86. *Standards for Ovens and Furnaces*. 2007 Edition.
- [13] Perez Martinez, José I., and Hurtado Secades, Carlos. *Hacia Un Nuevo Enfoque en Prevención: Mejorar La Cultura de Seguridad*, COASHIQ Boletín Num. 171.
- [14] Pijenburg, Marc; Wiegerinck, Jan; and Woltman, Arthur. *Definition of Safety Instrumented Functions*. IDC Technologies, Safety Control Systems Conference, 2007.
- [15] Scott, Mike, and Adler, Bud. *Case Study: Safety Instrumented Burner Management System (SI-BMS)*. AE Solutions.