Algerian Journal of Environmental Science and Technology
March edition. Vol.9. N°1. (2023)
ISSN : 2437-1114
www.aljest.org

Evaluation of Safety Instrumented System in a petroleum plant and its impact on the environment

S. Bouasla[1], E. Mechhoud[1], Y. Zennir[1*], R.Bendib[1], M. Rodriguez[2]

[1]Automatic laboratory, University of 20 Aout 1955, Skikda, Algeria
[2]Autonomous Systems Laboratory, Technical University of Madrid, Spain

*Corresponding author: y.zennir@univ-skikda.dz; Tel.: +213 664 73 52 77.

ARTICLE INFO

Article History :

Received ***: 02/01/2021***
Accepted ***: 06/05/2021***

***Key Words*:**
Risk analysis;HAZOP; LOPA ;Fault Tree ; Petrinets;Safety instrumented system;IEC61508;Environment impact;Environment protection.

ABSTRACT/RESUME

Abstract:*The purpose of this work is to check the calculations to consolidate the safety instrumented system (SIS) in order to preserve the safety of the plant and the environment,and consider the consequences in case of failure. The application of our study will be focused ontheNaphta Stabilizer-B Reflux Drum in Skikda refinery using the combination of HAZOP-LOPA-Fault Tree methods. The aim of this paper is to verify that the intended safety integrity level of a safety instrumented system is achieved. Otherwise propose a solution to ameliorate the safety instrumented system to mitigate the studied scenario. In case of failure of the safety instumented system, severe damage to the installation and serious impact on the environment will be considered; the use of petri nets allows us to model the behavior of the system. So the objective of our work is to ensure that the appropriate and efficient safety system is installed.*

I. Introduction

The petroleum industry can roughly be divided into four sectors: 1) exploration, development and production; 2) hydrocarbon processing (refineries and petrochemical plants); 3) storage, transportation, and distribution; and 4) retail or marketing [1−3]. These four sectors are also known as upstream, midstream and downstream processes [4, 5]. Environmental impacts are associated with every sector of the industry [3].

The environment protection is needed, and to achieve that, risk analysis must be carried outusing some methods such as HAZOP, FTA and LOPA.

Risk analysis is a process to comprehend the nature of risk and to determine the level of risk [6]. It is a systematic use of available information to identify hazards and to estimate the risk to persons, property, and the environment [7].

The use of Petri Nets allows modeling the behavior of a system.

Petri Net is a graph model for the control behavior of systems [8]. Petri nets are excellent net works with great characteristics of combining a mathematical theory with a graphical representation of the dynamic behavior of systems. The theoretical aspect of Petri nets allows precise modeling and analysis of system behavior, at the same time, the graphical representation enable visualization of state changes of the modeled system [9].

HAZOP is one of the process hazard analysis techniques [10].Itis a systematic examination of a process or operation [11], the primary purpose of HAZOP study is to identify and evaluate hazards [12]. In addition, recommendations to reduce the probability and consequences of an incident should be offered [13].

The fault tree analysis is typically applied in the reliability analysis [14–16].FTA is a graphical design technique [17].It is concerned with the identification and analysis ofconditions and factors that cause the occurrence of a defined top event [18]. FTA is a systematic safety analysis tool that proceeds deductively from the occurrence of an undesired event [19]. It represents basic causes of an unwanted event and estimates the like lihood (probability) as well as the contribution of different causes leading to the top event [20−23].

LOPA is a semiquantitative tool for analyzing and assessing risk [24].It is a risk assessment methodology to define risk as function of both frequency and potential consequence severity [25];

itis typically used to approximate the risk [26].LOPA starts with data developed in qualitative hazard evaluation such as HAZOP and accounts for each identified hazard by documenting the initiating cause and the protection layers. If risk reduction is required in the form of a Safety Instrumented Function, LOPA allows determining the appropriate Safety Integrity Level (SIL) for the SIF [27].
Safety Instrumented System (SIS) is an independent system to reduce potential risk of process. SIS includes sensors, transmitters, logic solver and final control elements [28].A typical composition of a SISis represented in Figure1.

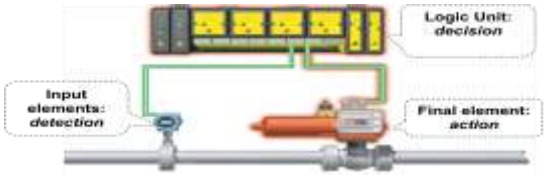

Figure 1.*Typical composition SIS*

Safety Integrity Level is classification of failures into specific levels. IEC61508 standard establishes four risk levels as shown in the Table 1[28].

Table 1.*Safety integrity level based on PFD* [28]

SIL	PFD_{avg}	Availability Required
4	$\geq 10^{-5}$ to$< 10^{-4}$	99.99% ~ 99.999%
3	$\geq 10^{-4}$ to$< 10^{-3}$	99.90% ~ 99.99%
2	$\geq 10^{-3}$ to$< 10^{-2}$	99.00 ~ 99.90%
1	$\geq 10^{-2}$ to$< 10^{-1}$	90.00% ~ 99.00%

IEC 61508 is a standard that provides a structured approach relying on hazards identification in order to establish the safety requirements for SIS. It aims at designing and operating the SIS within reliability confidence that meets these requirements [29].
IEC 61508 procedure diagram is shown in Figure 2.

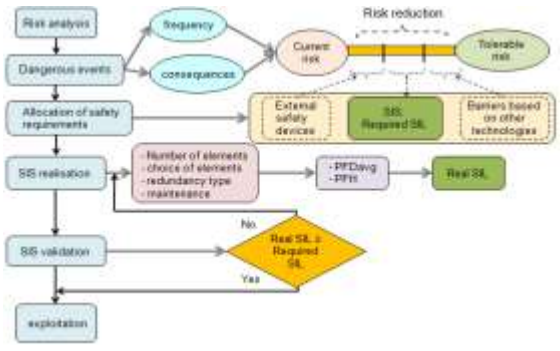

Figure2.*IEC 61508 approach: risk and safety integrity level [30].*

In the context of what said before, the main purpose of this paper is to evaluate a safety instrumented system starting with risk analysis, and then allocate a safety integrity level to the SIS and finally, validation of the SIS. The main work is organized as follows: in the section II we presentethe proposed methodology: First, risk analysis using HAZOP to identify risks, and then Fault Tree to calculate the frequency, and using ALOHA to appreciate the severity.The second step is to illustrate the allocation of the required SIL using LOPA method, and finaly, we verify and validate the real SIL using Fault Tree analysis. After that we describe the system in the section III and apply the proposed methodology in section IV.The section V presents the obtained results and discussion. Finally, the recommendations aregiven in the section VI and conclusion in the section VII.

II. Proposed methodology

The proposed methodology is performed to achieve the objective of study as follow:

- Risk analysis.
- Allocation of safety integrity level (required SIL).
- Realization and validation of the SIS (real SIL).

The methodology steps are represented in figure 3.

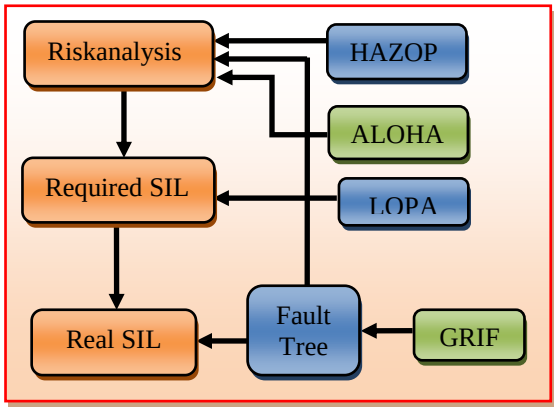

Figure 3.*Methodology steps.*

II.1. Risk analysis

Risk analysis is the development of a quantitative risk estimation based on engineering evaluation and mathematical techniques to combine between the incident consequences estimation and its frequencies [31].
During this step, all the dangerous situations (accident scenarios) are established in terms of severity and probability (frequency) of occurrence, in order to compare their criticality with a limit value constituting the safety objective to be achieved. If this criticality exceeds the aforementioned threshold value, then it will be necessary to reduce it. The extent of this reduction is broken down into specific safety requirements allocated to the various means of risk reduction. For SIS, these requirements are established in terms of safety functions and safety integrity levels (required

SIL). The greater the risk reduction to be achieved, the higher the SIL will be. This observation underlines the importance and the capital role that risk analysis plays in the IEC 61508 approach. It should be noted that the determination of the accident scenarios can be carried out using conventional methods such as HAZOP [29].

HAZOP study is a highly disciplined procedure that identifies how a process may deviate from its design intent [32]. It is a structured and systematic technique for examining a defined system [33], for which detailed design information is available, carried out by a multidisciplinary team [12]. This is done by using a set of guidewords in combination with the system parameters to seek meaningful deviations from the design intention. A meaningful deviation is one thatis physically possible—for example, no flow, high pressure… It's a method used for hazard identification [7].The steps to develop hazop study are shown in the fowchart of the HAZOP examination procedurewhichis represented in figure 4.

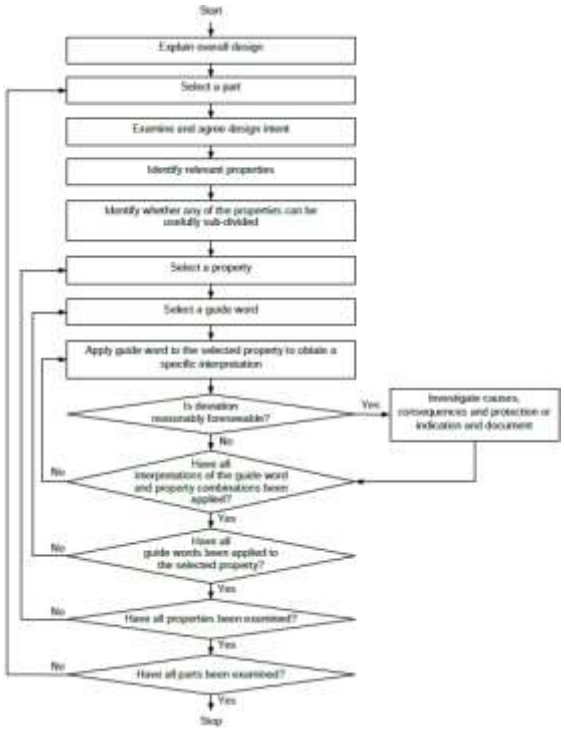

Figure 4.*The flow chart of the HAZOP examination procedure [33].*

II.2. Allocation of safetyintegritylevel (required SIL)

This allocation is carried out according to certain specific methods making it possible to define the required SIL for a safety function: SIL must be reached by a SIS in order to achieve the necessary reduction of risk level [29]. One of the most used methods is LOPA.

LOPA is an analytical tool that builds on hazard identification and characterization information developed during a HAZOP [24].

The relationship between HAZOP and LOPA information is represented in figure 5.

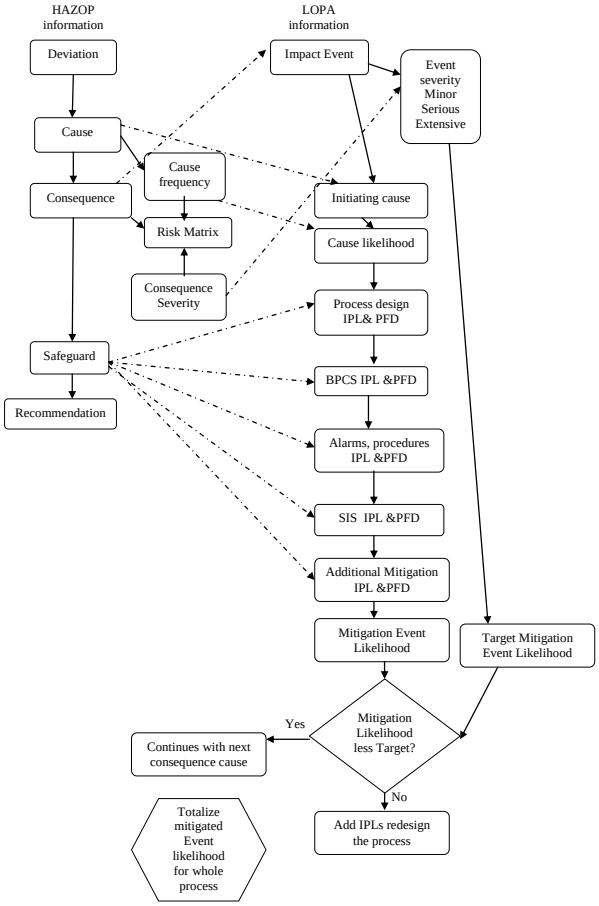

Figure 5.*Relationsship between HAZOP and LOPA information [34].*

LOPA (layers of protection analysis) is widely used as quantitative (semi-quantitative) method for the allocation of safety integrity levels. This method integrates all protection layers of the installation, both technical and organizational. It assesses the risk reduction by analyzing the contribution of the different layers. Its principle is to estimate the residual risk, expressed in frequency of accidents, by quantifying the frequency of the initiating event and the (average) probabilities of failure on demand of each layer. A major condition that must be satisfied is the independence of the different layers of protection (IPL: independent protection layers) [24].Table 2 below shows an example of the spreadsheet format that can be used in a LOPA study [27].

Table2.*Spreadsheet format of LOPA*

Ref no?	1	2	3	4	5				6	7	8		9	10
					Protection layers (PLs)									
	Impact event description	Severity level	Initiating cause	Initiation likelihood	General design	Control system	alarms		Additional mitigation restricted access	Additional mitigation	Intermediate event likelihood		PFD_{avg} and required SIL	Tolerable mitihated event likelihood
1	Overspeed, of rotor leading to fracture of casing	Loss of life of persons located adjacent to casing, fatalities will not exceed 2	Speed control system fails	0.1	1	1	1		0.1	0.1	10^{-3}		5.10^{-3} (SIL 2 will a minimum PFD_{AVG} of 5.10^{-3})	10^{-5} **FT**
			Loss of load	1	1	0.1	1		0.1	0.1	10^{-3}			
			Cutch failure	0.1	1	0.1	1		0.1	0.1	10^{-4}	Total $2,1.10^{-3}$ **FC**		Tolerable frequency if fatalities do not exceed 5
						0.1 credit given to control system			Occupency limited, persons not present 90% of he time	Fatality will onlu occur if fragments contact persons				
2	Repeat obove case for environmental risk analysis													
3														
.														
.														
N														

Continued as required

Note 1: severity levels maybe classified as C (catastrophic), E (extensive), S (serious), M (minor). Tolerate mitigated event likelihood will depend on severity level.
Note 2: units in columns 4, 8 and 10 are events per year.
Note 3: units in columns 5 to 7 and 9 are dimentionless. The numbers between 0 and 1 are the factors by which event likelihood maybe multiplied to represent the mitigating effect of the associated protection layer. Thus 1 means no mitigating effect and 0.1 means a factor of 10 risk reduction.

The frequency of the feared event (accident scenario: column n ° 8 of Table 2) is obtained by multiplying the frequency of the initiating event and the mean probabilities of failure on demand (PFDavg) of each IPL opposing this same event.

$$f^{C} = f^{IE} \times \prod_{i} PFD_{avg}^{i} \qquad (1)$$

f^{C}: occurrence frequency of consequence C
f^{IE} : initiating event frequency
PFD_{avg}^{i} : Average probability of failure on demand of the barrier i.
The assigned risk reduction to the SIS safety function is obtained by comparing the frequency of the feared event to the safety objective (tolerable frequency ft).

$$PFD_{avg}^{SIS} \leq \frac{f_t}{f^{IE} \times \prod_{i \neq SIS} PFD_{avg}^{i}} \qquad (2)$$

The quantity corresponding to the right side of the inequality represents the maximum allowable average probability of failure that the SIS could have, such that the necessary risk reduction is achieved. Reading this quantity in Table 1 makes it possible to define the corresponding SIL.

II.3. Realization and validation of the SIS (real SIL)

Once the required SIL is determined, it remains to design the SIS that must meet the requirements attached to this required SIL.One of the most used methods to do this Fault Tree [28].
Fault tree is used in reliability and safety risk assessments. It represents graphically the logical interactions and probabilities of occurrence of component failures and other events in a system [35].
It is used to develop the causes of an event. It starts with the event of interest, the top event, such as a hazardous event or equipment failure, and is developed from the top-down. Events that lead to a predefined undesired event (top event).
The fault tree is both a qualitative and a quantitative technique. Qualitatively it is used to identify the individual paths that led to the top event, while quantitatively it is used to estimate the frequencyor probability of that event [36].
Fault Treeis chosenbecause it is a very structured, systematic, and rigorous technique that lends itself well to quantification. It is the best way to priorities the multitude of potential hazards of loss of production by determining numerically how much each cause contributed to the loss. In this way, solid interactions between the actions taken to improve safety or production and the actual events generated could be established [28].
The construction of the fault tree aims to determine the chain of events that can lead to the selected final event. This analysis ends when all the potential causes correspond to elementary events. The development of the fault tree is shown in diagram represented in the figure 6.

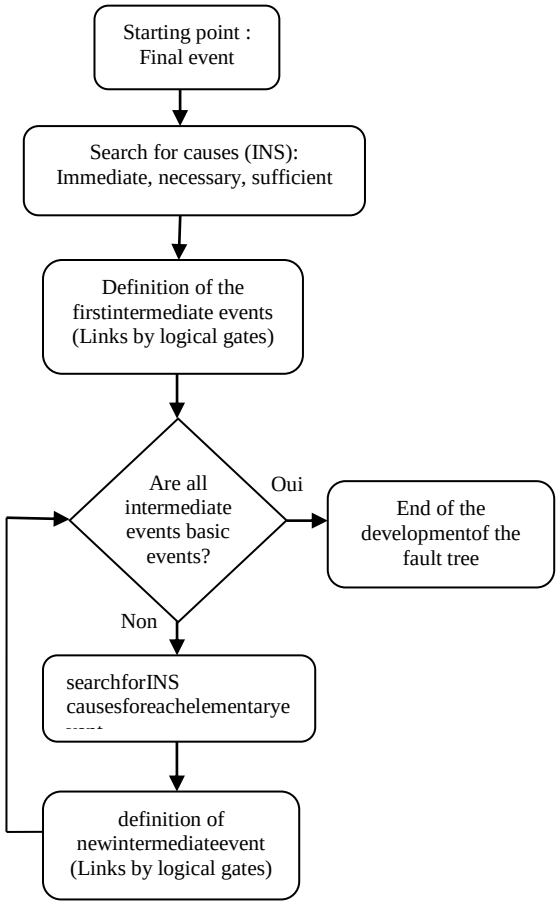

Figure 6.*flow diagram of Fault Tree* [37]

III. Process description [38]

Before each development of a risk analysis, it is first necessary to define the different dimensions (operation, control loop, safety system, etc.) related to the plant to be studied. In this study the plant concerned is a Naphta stabilizer-b reflux drum (Figure 7) [39], located at crude oil unit in Skikda refinery (Algeria).

Unstabilized naphtha after preheating is divided into two parts. 70% of total unstabilized naphtha is fed into existing Stabilizer column (C-5) & balance 30% is sent to new Stabilizer column (C-62).

Part of preheated naphtha is sent to C-62 via flow control valve in the feed line FV-2151 through cascade control between FIC-2151 and LIC-2152.

The vapors of column C-62 overhead are condensed in air cooler Stabilizer-B Overhead Product Condenser (EA-62A/B/C/D), and Stabilizer-B Overhead Trim Condenser (E-71), and then collected in accumulator Stabilizer-B Reflux Drum (V-62).

The reflux drum is operated at temperature and pressure condition of 43°C and 7.0 kg/cm2 g. Pressure in the reflux drum V-62 is controlled by PIC-2252 acting in "split control" on valves PV-2252A and PV-2252B.

Uncondensed vapor fuel gas flow is controlled through PV-2252A and further incondensable materials accumulated in stabilizer-B Reflux Drum (V-62) can be discharged to the blow-down through PV-2252B.

The liquid which is accumulated in the receiving tank of overhead V-62 is sucked by pumps MP-63A/B.

A party of the sucked product is sentto the overhead of column C-62 as reflux under flow controlled of FIC-2252 through flow control valve FV-2252.

The other party constituting the production of column overhead in unit 30 with the flow rate controlled by FIC-2251 operating in cascade with level controller LIC-2253, equipped with alarm for low level LAH/LAL-2253.

Interface level between LPG and oily water in V-62 is controlled by LIC-2255 by controlling flow through LV-2255 located in discharge line of boot.

As an extra safety hydrocarbon detector AI-2251 and AI-2252 has been provided near the reflux drum (V-62) bottom and reflux pump (MP-63 A/B).

Further as a part of safety LI-2257 has been provided with High-High and Low-Low level alarm LAHH-2257 & LALL-2257.

In case of LAHH-2257 interlock I-2257 will get actuated and UV-2254 in the overhead line of V-62 will get closed.

In case of LALL-2257 gives signals the interlock I-2257 will get actuated to close the on/off valve UV2252 installed in the suction line of MP-63 A/B and stop the pump MP-63.

For the boot level another interlock I-2259 will be actuated by LALL-2259 to close UV-2255 A/B in order to protect LPG leaking.

All safety systems (pressure safety devices, alarms, interlocks and gas detectors) of the studied system (Naphta stabilize-B reflux drum in crude oil unit at Skikda refinery) are described and represented in table 3.

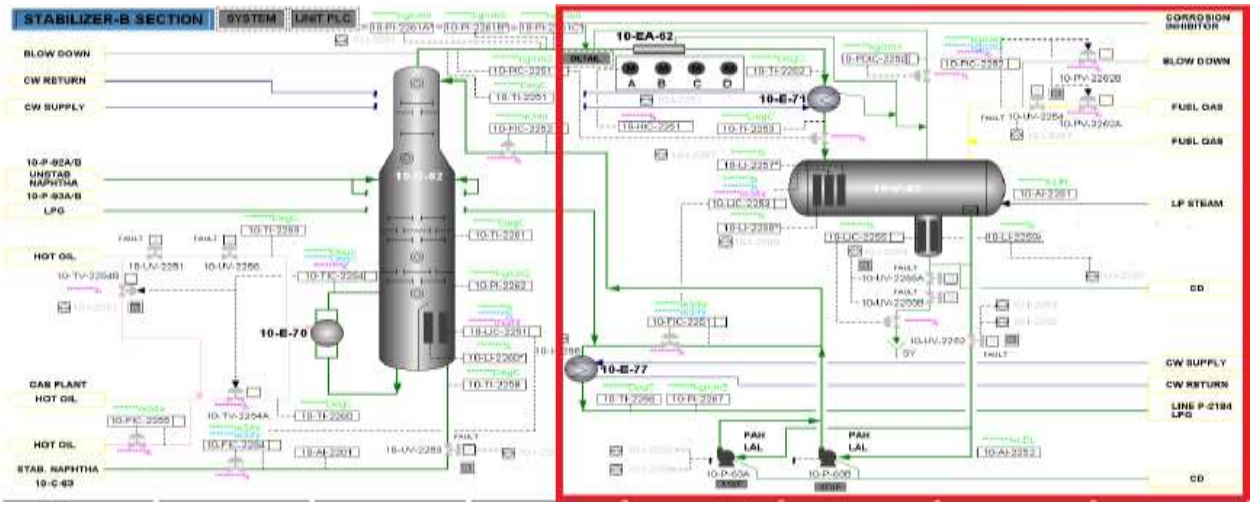

Figure 7.*diagram related to the naphta stabilize-B reflux drum [39].*

Table 3.*Different safety systems protecting stabilizer-b reflux drum [38]*

Safety systems	Landmark	Description
Pressure Safety Devices	PV-2252A	Discharge To FG line
	PV2252B	Discharge To Blow down
Interlocks	I-2253	- Activated by HS-2252A/B - Action on: Close UV-2252 Stop MP63
	I-2257	- Activated by LT/LAHH-2257 - Action on: Close UV-2254. Close PV-2252A. Open PV-2252B
		- Activated by LT/LALL-2257 - Action on: Close UV-2252 Stop Pump P-63A/B
	I-2259	- Activated by LT/LALL-2259 - Action on: Close UV-2155A/B
Alarms	PAH-2252	V-62 Pressure
	PAL-2252	V-62 Pressure
	LALL-2257	V-62 Level
	LAHH-2257	V-62 Level
	LALL-2259	V-62 Boot Level
	LAL-2253	V-62 Level
	LAH-2253	V-62 Level
	LAL-2255	V-62 Interface Level
	LAH-2255	V-62 Interface Level
	FAL-2251	LPG Flow (MP-63 A/B)
Gas detectors	AI-2251	near the reflux drum (V-62)
	AI-2252	Near pump (MP-63 A/B)

IV. Application of the proposed methodology

In this section, we apply the proposed approach on the Naphta Stabilizer-B Reflux Drum in Skikda refinery.

The first step is risk analysis using HAZOP to identify diffrent scenarios, then Fault Tree analysis to estimate and evaluate the risk by determining the frequency of the top event, and in order to appreciate the severity of this event we use ALOHA to determine the threated zones. The second step ist o determine the required SIL using LOPA.

The final step is to validate the sis by determining the real SIL using Fault Tree which is represented by GRIF software which is used for the interactive charts for reliability.

IV.1. Risk analysis

As we said before, the first step of the proposed approach is risk analysis to identify different accident scenarios that may occur in the system to be studied (Naphta Stabilizer-B Reflux Drum). To do that, HAZOP will be used. The end result of HAZOP should express each consequence in terms of severity and probability (frequency) of occurrence.

IV.1.1. Identifyrisksby HAZOP

HAZOP study leads to identify different accident scenarios resulting from parameters deviations. Thanks to its global analysis which facilitates the choice of a consequence to be evaluated by using Fault tree [7]. In our case we have chosen two deviations (no level of LPG in the vessel and no level of oily water in the boot). The results are shown in the table 5. Risk Acceptance is based on frequency and severity.

The frequency is obtained by using Fault Tree and the severity is related to the impact event given by the ALOHA simulation results. Risk matrix of SKIKDA Refinery- Algeria is shown in the table 4.

Algerian Journal of Environmental Science and Technology
March edition. Vol.9. N°1. (2023)
ISSN : 2437-1114
www.aljest.org

Table 4.*Risk acceptance matrix for Skikda refinery (RA1K)* ***[40]***

Severity	Frequency				
	5: P< 10^{-5}	**4:** 10^{-4}>p> 10^{-5}	**3:** 10^{-3}>P> 10^{-4}	**2:** 10^{-2}>P> 10^{-3}	**1:** P> 10^{-2}
G5: disastrous	M	H	H	H	H
G4:catastrophic	M	M	H	H	H
G3: important	M	M	M	H	H
G2: serious	L	L	M	M	H
G1: moderate	L	L	L	L	M

L	Low risk (accepted)
M	Moderate risk (tolerated)
H	High risk (not accepted)

Table 5.*HAZOP Analysis "no level of LPG" and "no level of oily water" related to reflux drum V-62*

deviation		Causes	Conseque-nces	Warnings	Protection means	criticality	
parameter	Guide word					G	P
Level of LPG in V62	NO	- Insufficientcooling of overheadvapor due to EA62 and E11 failure. - BPCS of LPG levelfailures: LT 2253 failures LIC 2253 failures FIC 2251 failures FV 2251 failures (does not close) - BPCS of LPG flowfailures FT 2251failures, FIC 2251 failures	- cavitations of MP 63 - gasleaking - fire - UVCE	- Alarm LAL on LIC 2253 - Alarm LALL on LIC 2157 - Alarm AAH on AI 2251	- Interlock 2257 (close UV 2252 andstop pump MP 63) - Interlock 2253 (close UV 2252 andstop pump MP 63)	4	3
Level of oilywater in boot	NO	- BPCS of oilywaterlevelfailures : LT 2255 failures, LIC 2255 failures LV 2255failures (does not close)	- gasleaking - jetfire - poolfire - UVCE	- Alarm LAL on LIC 2255 - Alarm LALL on LIC 2259 - Alarm AAH on AI 2252	- Interlock 2259 (close UV 2255 A/B)	4	3

The normal function of our system is ensured by safety barriers. In case of failure of the safety instrumented system which is the most important of our safeguards; LPG could be released to the atmosphere. Then it depends on the condition of the leak and the probability of ignition to determine what could happen, so we have three cases:

- UVCE: delayed ignition of gas leak.
- Jet fire: Instant ignition of Pressurized leak.
- Pool fire: Ignition of vaporising liquid.

The results of developing situation of LPG leak after the safety instrumented system failure is shown in petri net represented in figure 8.

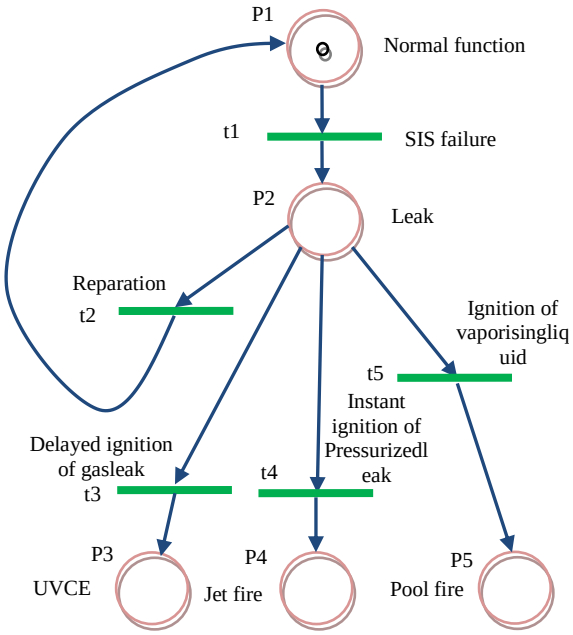

Figure 8.*Petri net related to the LPG leak*

IV.1.2. Estimateandevaluaterisksby FTA

The Fault Tree allows us to determine quantitative values concerning the reliability and the failure frequency [7]. The computation of these values depends on the complexity of the studied system. In this paper we used the GRIF software [41] to calculate the occurrence frequency of the top event (LPG leak), it is necessary to use reliability and failure data which are shown in Table 6. The chosen scenario is LPG leak; it is represented in Figure 9.

Table 6.*PFD of components used in GRIF [42, 43]*

Component	PFD	Component	PFD
LT	$6{,}7746.10^{-3}$	FT	$6{,}7746.10^{-3}$
LU	$2{,}126.10^{-5}$	FIC	$2{,}126.10^{-5}$
UV	$1{,}344.10^{-4}$	LIC	$2{,}126.10^{-5}$
UY	4.10^{-7}	LV	$6{,}7593.10^{-2}$
LAL	$6{,}7746.10^{-3}$	HS	$6{,}3222.10^{-4}$
Human error	10^{-1}		

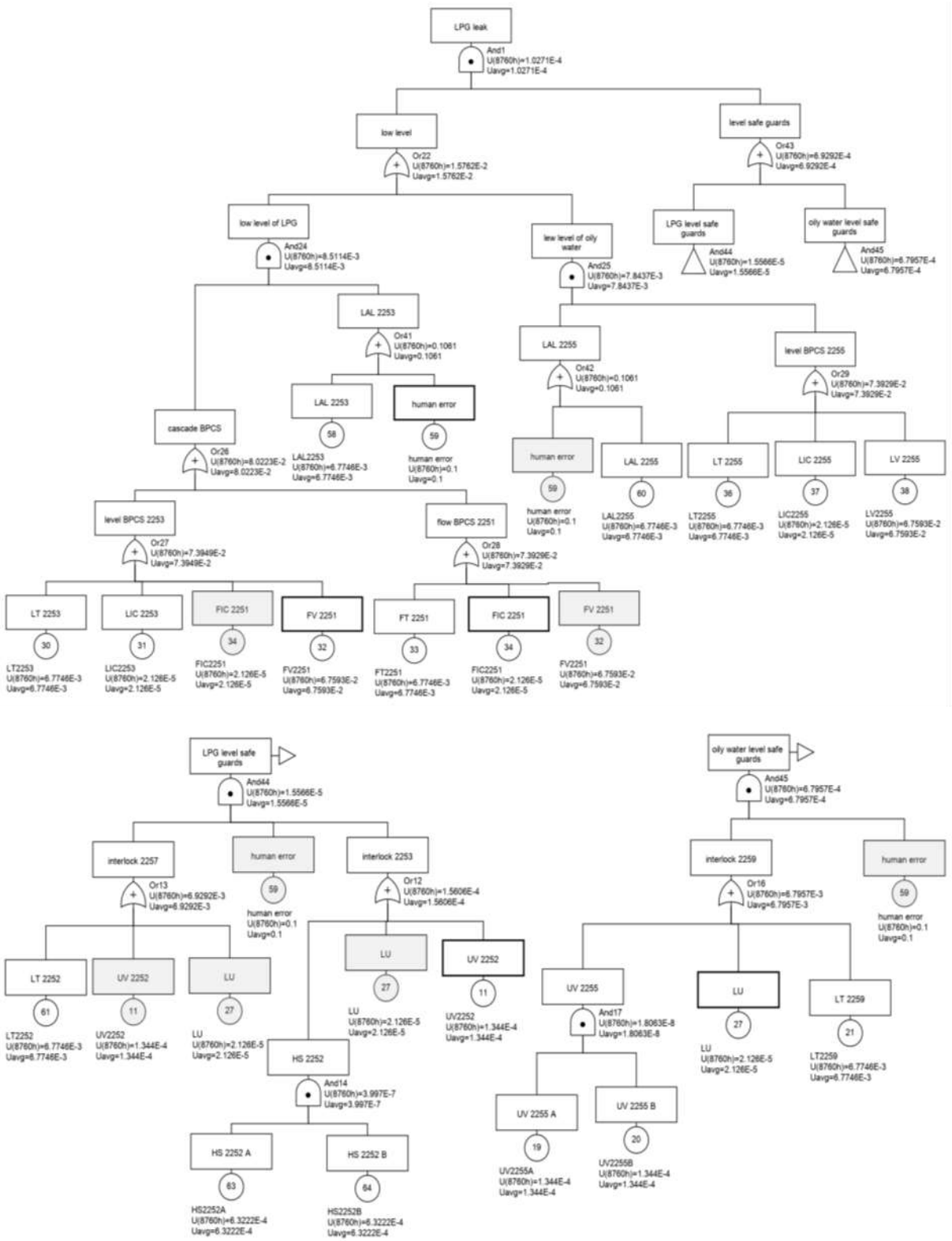

Figure 9.*Fault Tree of the consequence "LPG leak from stabilizer B reflux drum V-62".*

In case of LPG leak, there is an impact on the environment due to air pollution resulting from gas dispersion or gas combustion.
To appreciate the impact of the obtained consequences, we simulate threat zones of thermal and overpressure effects related to the UVCE, and the dispersion of polluants resulting from LPG release using ALOHA [44].
Results of thermal effects are shown in figure 10.

Figue10.*Thermal effects*

Thermal effects shown in figure 10 are represented by MARPLOT. Impacted zones could extend to reach 90 m.
Distances and threat zones related to the UVCE thermal effects resulting from LPG leak in stabilizer-B reflux drum are shown in the table 7.

Table 7.*Distances and areas threated by thermal effects*

Threshold	distance	Threat zones
10 KW/M2	45 m	U10, South of U100
05 KW/M2	60 m	U10, U100
02 KW/M2	90 m	U10, North of U11, U100

The results of overpressure effects are shown in figure 11.

Figure 11.*overpressure effects*

Overpressure effects shown in figure 11 are represented by MARPLOT. Impacted zones could extend to reach 105 m.

Distances and thre at zones related to the UVCE overpressure effects resulting from LPG leak in stabilizer B reflux drum are shown in the table 8.

Table 8.*Distances and areas threated by overpressure effects*

Threshold	distance	Threat zones
08 Psi	/	/
3.5 psi	70 m	U10, South of U100
01 Psi	105 m	U10, North of U11, U100

The results related to the dispersion of pulluants are shown in figure 12.

Figue12.*Dispersion of pulluants*

Dispersion of polluants shown in figure 12 is represented by MARPLOT. Impacted zones could extend to reach 107 m.

Distances and threat zones related to the dispersion of polluantsresulting from LPG leak in stabilizer-B reflux drum are shown in the table 9.

Table 9.*Distances and areas threated by pollutants dispersion*

Threshold	distance	Threat zones
53000 ppm	25 m	U10
17000 ppm	53 m	U10
5500 ppm	107 m	U10, West of U10

Figures 13, 14, 15 and 16 represent the concentration of polluants at different points from the release onset.

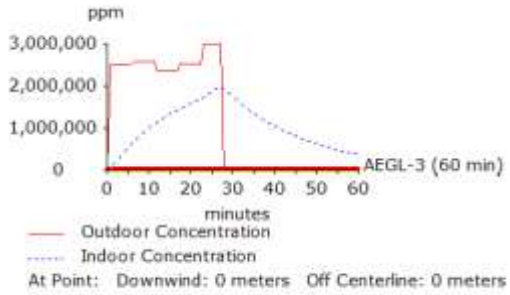

Figure13.*concentration of pollutants at point (0m)*

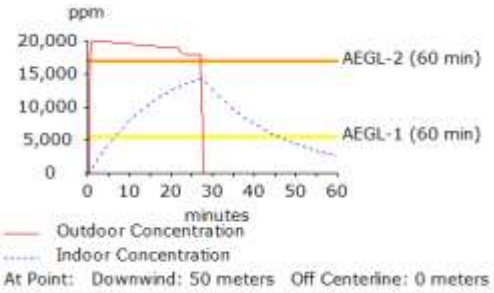

Figure14.*concentration of pollutants at point (50m)*

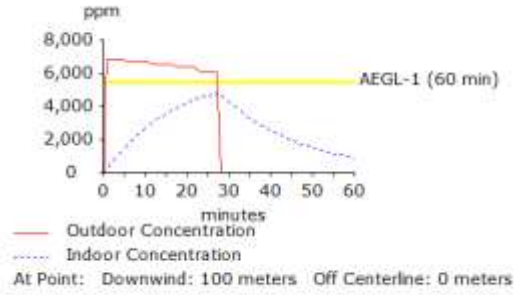

Figure15.*concentration of pollutants at point (100m)*

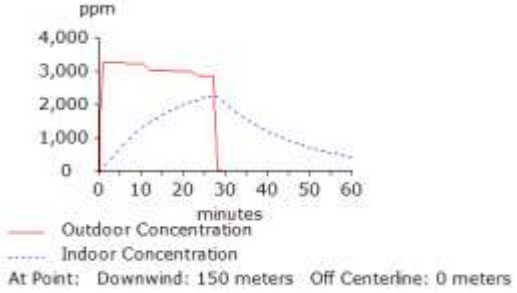

Figure16.*concentration of pollutants at point (150m)*

Figure 13 shows that concentration of pollutants reaches the value of 2,500,000 ppm just at the onset of depression, it increases to reach the maximum value of 3,000,000 ppm within 25 min.

Figures 14, 15 and 16 illustrate the displacement of the cloud following an accidental release. It shows the estimated concentration of polluants (in ppm) in outdoor, the value decreases in time. It reaches 20,000 ppm at point 50 m and decreases to almost 7000 ppm at point 100 m, then to 3400 at 150 m, the estimated time of the concentration at each point is 28 min.

Basingon the frequency obtained by Fault Tree analysis ($1{,}0271.10^{-4}$) and the severity concluded from the impact simulation using ALOHA (overpressure effects distance reach 105 m, thermal effects reach 90 m and the dispersion of polullants reach 60 m), then referring to the risk matrix of skikda refinery, the frequency of LPG release is classified (F3) and the severity in case of ignition is (G4), so the risk is judged not acceptable, to reduce the risk to an acceptable level, other protection layers must be taken in consideration or the amelioration of the safety instrumented system might be the solution.

For that it is necessary to verify the SIL of our safety instrumented system. First, we have to determine the required SIL, then we calculate the real SIL.

IV.2. Allocation of safety integrity level (required SIL)

The second step of this approach is to allocate the required SIL to the SIS. The most reliable method is LOPA, so it's chosen to define the SIL that must be reached by the SIS in order to achieve the necessary risk reduction. The results are shown in the table 9.

PFD values are taken from table 6. The chosen impact event is LPG release from the boot of Naphta stabilizer-B reflux (V-62) drum due to failure of BPCS, which leads to an UVCE if it is not mitigated.

Depending on the results that will be obtained from LOPA study, and comparing to the real SIL to be calculated, it will be decided wich modification will be taken in order to ameliorate the safety integrity level (SIL) of the safety instrumented system (SIS).

TABLE9.*LOPA related to impact event LPG release*

1	2	3	4	5				6	7	8	9	10
Impact event	Severity level	Initiating cause	Initiation likelihood	Protection layers (PLs)						Intermediate event likelihood	$PFD_{avg}$and required SIL	Tolerable mitihated event likelihood
				General design	Control system	alarms	Additional mitigation restricted access	Additional mitigation				
LPG realse to atmosphere	4	LT-2255 failures	$6,7746.10^{-3}$	1	1	0,1	1	1		$6,7746.10^{-4}$	$1,4643.10^{-4}$ SIL3	10^{-5}
		LIC-2255 failures	$2,126.10^{-5}$	1	0,1	1	1	1		$2,126.10^{-6}$		
		LV-2255 failures	$6,7593.10^{-2}$	1	1	1	1	1		$6,7593.10^{-2}$		
										Total $6,8291.10^{-2}$		

Following the result abtaind from LOPA method (table 9), which give us a PFD value of $1,4643.10^{-4}$, we conclude the riquired SIL for our studied system is SIL 3.

To verify this result we can use also a qualitative method using Risk matrix.

The classification methodology comprises of Classification of SIF dangerous failures, it takes into account:

- Demand rate of the SIF (interval between demands)
- Consequences related to personnel health and safety.
- Consequences related to production and equipment loss.
- Consequences related to the environmental impact.

The determination of all categories related to the demand rate, consequences on health and safety, economic and the environment is shown in tables 10, 11, 12 and 13.

TABLE 10.*Demand rate category [42]*

Category	Demand rate
D0	Negligible
D1	> 20 years
D2	4 to 20 years
D3	6 monthsto 4 years
D4	< 6 months

TABLE 11.*Environmental consequences category [42]*

Categ-ory	Conseq-uence	Description
E0	No Effect	No environmental damage. No financial consequences.
E1	Slight Effect	Local environmental effect. Within the boundary fence and within systems. Negligible financial consequences.
E2	Minor Effect	Contamination sufficiently large to damage the environment or single complaint. Single exceedance of statutory or prescribed limit. No permanent effect on the environment.
E3	Local Effect	Limited discharge of known toxicity. Repeated exceedance of statutory or prescribed limit. Affecting the neighborhood beyond the boundary fence.
E4	Major Effect	Severe environmental damage. The company is required to take extensive measures to restore the contaminated environment to its original state. Extended exceedance of statutory or prescribed limit.
E5	Massive Effect	Persistent severe environmental damage or severe nuisance extending over a large area. Loss of commercial, recreational use or nature conservancy resulting in major. financial consequences. Constant and high exceedance of statutory or prescribed limit.

TABLE 12.*Health and safety consequences category [42]*

Category	Healthandsafetyconsequences
S0	Noinjuryorhealtheffect
S1	Slightinjuryorhealtheffect
S2	Minor injuryorhealtheffect
S3	Major injuryorhealtheffect
S4	Onetothreefatalities
S5	Multiple fatalities

TABLE 13.*Economic consequences category [42]*

Category	Economicconsequences
L0	No loss
L1	Slight loss
L2	Minor loss
L3	Local loss
L4	Major loss
L5	Extensive loss

TABLE 14.*Risk matrix [42]*

Consequencecategory			Demand rate category				
S	E	L	D0	D1	D2	D3	D4
Health&safety	environmental	economic					
S0	E0	L0	-	-	-	-	-
S1	E1	L1	-	-	A1	A2	A2
S2	E2	L2	-	A1	A2	1	2
S3	E3	L3	-	A2	1	2	3
S4	E4	L4	-	1	2	3	4
S5	E5	L5	-	2	3	4	X

Basing on previous experiences and results obtained by ALOHA simulation we can determine the categories as follows:

- Demand rate: D3
- Health and safety consequences category: S4
- Economic consequences category: L4
- Environmental consequences category: E3

Using informations in risk matrix (table 14) allows to determine that the overall required SIL is SIL 3.

IV.3. Realizationandvalidation of the SIS (real SIL)

The final step is the validation of the SIS, the purpose of this step is to check the real SIL so we can juge if it is suitable to the SIS in our syetem, if not, we propose an other safety barrier or modify the architecture of our SIS. The best method to do that is Fault Tree, so it is chosen to evaluate the real SIL. The different reliability data used are shown in Table 6 [42, 43].

The obtained results using GRIF software are shown in figure 17 [41].

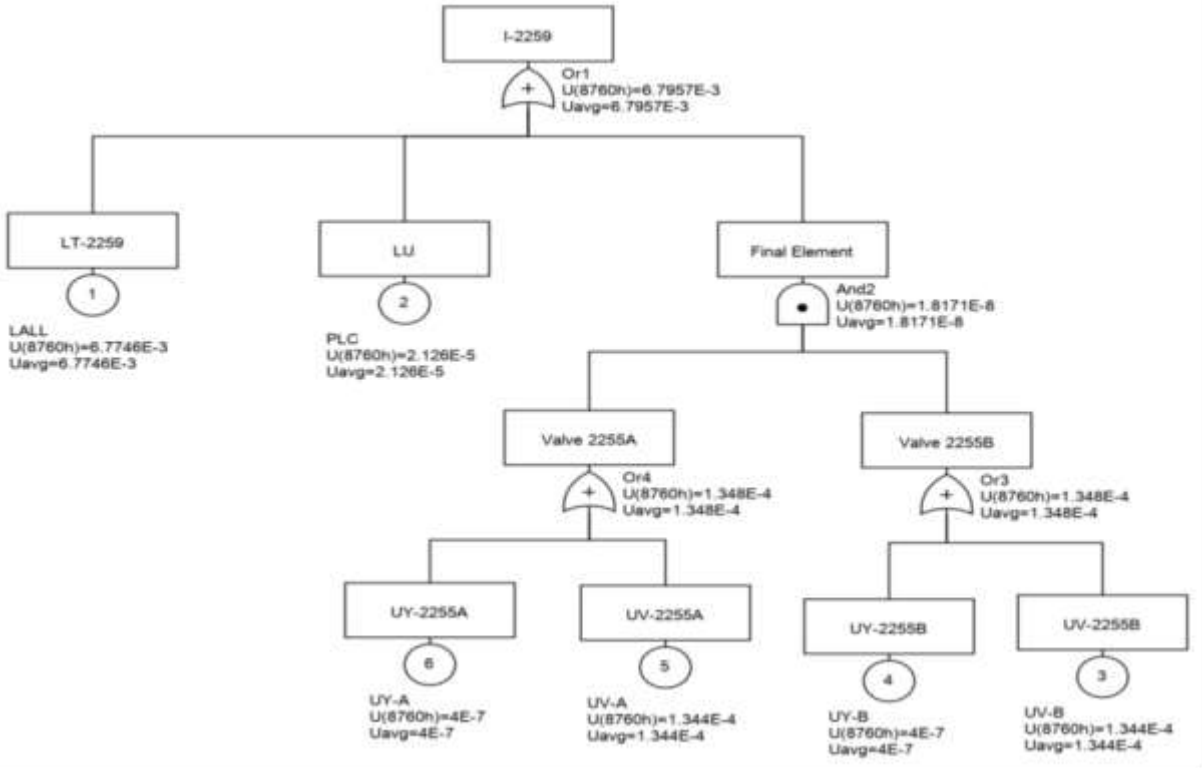

Figure 17.*Fault Tree related to the SIS.*

Using informations of table 1 and table 6 and Fault Tree in figure 17 allows us to define the real SIL related to the studied SIS in our system. The obtained result of PFD is $6{,}7957.10^{-3}$, so the real SIL of our SIS is SIL 2.

IV.3.1.Illustration ofthe real SILusingRBD

There are two configurations todefine the SIL:

- **NOON** configuration:

SIL = MIN (SIL (canal i, i = 1,…, N)).

- **KOON** configurtion:

SIL = MIN (MAX (SIL (canal i)) + N–K, SIL 4).

Algerian Journal of Environmental Science and Technology
March edition. Vol.9. N°1. (2023)
ISSN : 2437-1114
www.aljest.org

SIL (LT, LU) = min (SIL2, SIL4) = SIL2.
SIL (UV_A, UV_B) = min (max(SIL3, SIL3) + 1, SIL4) = SIL4.
SIL (global) = min (SIL2, SIL4) = SIL 2.
The result of the SIL is represented in figure 18.

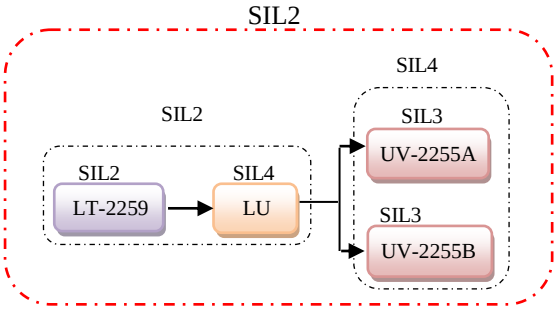

Figure 18.*existing architecture of the SIS*

V. Results and discussion

Following what mentionned before the required SIL for our studied SIS is SIL3 based on the result of PFD obtained by using LOPA ($1,4643.10^{-4}$), while the real SIL is SIL 2 based on the result of PFD obtained by using Fault Tree ($6,7957.10^{-3}$).

As we can see the real SIL is not enough to meet the requirments of our SIS, for that a modification of the SIS is necessary to reach the required SIL.
In this context we propose to modify the architecture of the SIS by modifying the architecture of transmitters, the existing is 1001, so we propose the architecture 2003 as it is represented in figure 19.

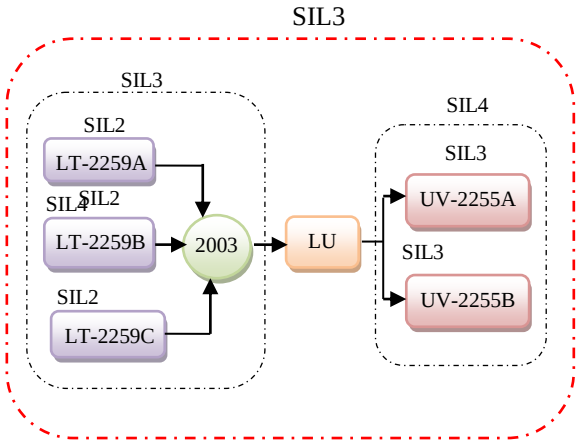

Figure 19.*proposed architecture of the SIS*

V.1.Validation of the results using Fault Tree

After modifying the architecture of the level transmitter from 1001 to 2003, we will use Fault Tree to calculate the new PFD of our SIS, so we can determine the value of the new SIL. The modified architecture of the level transmeter is represented inside the red square in figure 20.The obtained results of Fault Tree are shown in the same figure.
.

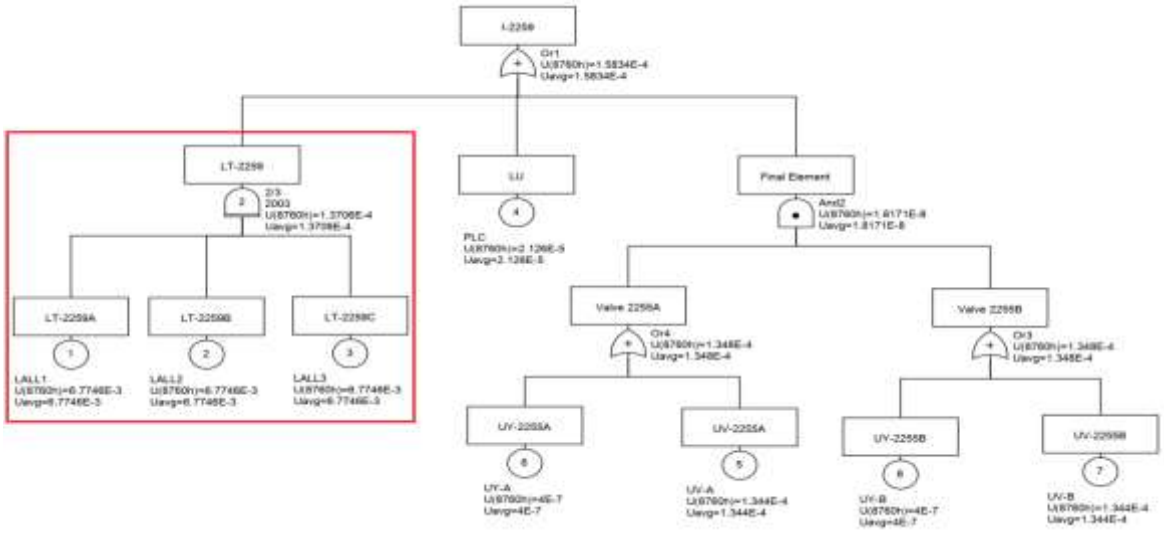

Figure 20.*Fault Tree related to the proposed architecture of the SIS.*

Using informations of table 1 and table 6 and Fault Tree in figure 20 allows us to define the new real SIL related to our studied SIS. The new obtained PFD after the modification is $1,5834.10^{-4}$, so the new SIL of the modified SIS will be SIL3.

VI. Recommendations

Basedon the obtained results after the proposed modification we confirm the proposed architecture of the level transmeter, so we recommend to:

- Modify the architecture of the level transmiter (LT-2259) of our SIS (I-2259) from 1001 to 2003.
- Increase the test frequency of the SIS, the test should be every six months instead of one year (4380 h instead of 8760 h), that leads to decrease the PFD value, so the SIL could be higher.

VII. Conclusion

The main objective of this work was to evaluate a safety instrumented system using HAZOP-LOPA Fault Tree methodology. We have first introduced the main steps of the proposed methodology. Then, we have briefly described the system on which we have illustrated this approach. It consists of Naphta stabilizer-B reflux drum of a crude oil unit in Skikda refinery.

The illustration was initiated by a risk analysis conducted using the HAZOP method. It has shown that the failure of the level regulation system constitutes an important source for triggering the accidental process.

The pplication of LOPA for determining the necessary riskreduction, which must be provided by the safety instrumented system (SIS), gaves us as a result SIL3 likea required SIL basing on the obtained PFD ($1{,}4643.10^{-4}$), while the real SIL was obtained by using Fault Tree based on the calculation of the PFD, the result of PFD ($6{,}7957.10^{-3}$) allows us to determine the value of SIL2. The real SIL is not enough to reach the required risk reduction.

To reach the SIL target a modification has been proposed. It consists to modify the architecture of the level transmiter from 1001 to 2003. Calculations after the proposed modification gave us the needed value of PFD ($1{,}5834.10^{-4}$), so the new SIL after modification will be SIL3 as required.

VIII. References

1. Jafarinejad, S. Control and treatment of sulfur compounds specially sulfur oxides (SOx) emissions from the petroleum industry: a review.*Chem. Inter2* (2016) 242–253.
2. Jafarinejad, S. Odours emission and control in the petroleum refinery: a review.*Curr. Sci. Perspec2*(2016) 78–82.
3. Jafarinejad, S. Petroleum Waste Treatment and Pollution Control.*First edition, Elsevier (2016)*378 pages.
4. Macini, P.; Mesini, E. The petroleum upstreamindustry: hydrocarbon exploration and production, in petroleum engineering-upstream. *Encyclopedia of Life Suport Systems (EOLSS)* (2011)76 pages.
5. Devold, H. Oil and gas production handbook, an introduction to oil and gas production, transport.Refining and petrochemical industry. *Third edition. ABB Oil and Gas*(2013) 162 pages.
6. IEC 31000 standard. Risk management – principles and guidelines. *First edition*(2009) 36 pages.
7. Bouasla, S.; Zennir,Y.; Mechhoud, E. Risk analysis using HAZOP-Fault Tree-Event Tree methodology. *Algerian journal of signals and systems.* vol. 5 (2)(2020) 98-105.
8. Leasure, B.; Kuck, D.; Gorlatch, S.;Cole, M.;Watson, G.;Darte, A.;Gärtner, K. Petri Nets. *Encyclopedia of Parallel Computing*(2011) 1525–1530.
9. Feng, L.;Obayashi, M.;Kuremoto, T.;Kobayashi, K. Construction and Application of Learning Petri Net.*Manufacturing and Computer Science*(2012) 143-176.
10. Dunjó, J.;Fthenakis, V.; Vílchez, J.; Arnaldos, J. Hazard and operability (HAZOP) analysis. A literature review. *J. Hazard. Mater 173* (2010), 19–32.
11. Macdonald, D.;Mackay, S. Practical HAZOPs, Trips and alarms. *IDC Technologies*(2004) 345 pages.
12. Crawley, F.;Preston, M.;Tyler, B. HAZOP: Guide to best practice, Guidelines to best practice for the process and chemical industries. *Institution of Chemical Engineers*(2000) 128 pages.
13. Chhadra, S.;Chichra, H.;Kumar, J. HAZOP/HAZID for IOCL BOTTLING plant. *PATTIKALAN* (2014) 60 pages.
14. Lin, S.; Wang, Y.; Jia, L. System Reliability Assessment Based on Failure Propagation Processes.*Complexity* (2018) 1-19.
15. Sihombing, F.;Torbol, M. Parallel fault tree analysis for accurate reliability of complex systems. *Structural Safety.* vol. 72(2018) 41–53.
16. Giraud, L.;Galy, B. Fault tree analysis and risk mitigation strategies for mine hoist. *Safety Science.*vol. 110 (2018) 222–234.
17. Rajkumar, L.; Patil, B. an overview of fault tree analysis (FTA) method for reliability analysis. *Journal of Engineering Research and Studies.* vol. 4(2013) 06-08.
18. IEC 61025 standard. Fault tree analysis (FTA). Second edition (2006) 112 pages.
19. Goodman, G. An assessment of coal mine escapeway reliability using fault tree analysis. *Mining Science and Technology 7(2)* (1988) 205–15.
20. Vesely, W.; Goldberg, F.; Roberts, N.; Haasl, D. Fault Tree Handbook. *Nuclear Regulatory Commission* (1981) 209 pages.
21. Haasl, D. Advanced concepts in fault tree analysis In System Safety Symposium. *Boeing Company* (1965) 14 pages.
22. Hauptmanns, U. Fault tree analysis of a proposed ethylene vaporization unit. *Industrial & Engineering Chemistry Fundamentals 19(3)*(1980) 300-309.
23. Hauptmanns, U. Fault tree analysis for process industries engineering risk and hazard assessment. *Engineering Risk & Hazard Assessment.* vol. 1. Boca Raton. FL: CRC Press (1988) 21–59.
24. CCPS, Layer of protection analysis, simplified process assessment. *Center for chemical process safety of the American institute for chemical Engineers*(2001) 280 pages.
25. Ronald, J. Layer of Protection Analysis. *Procedia Engineering 84*(2014)12–22.
26. Guidelines for Initiating Events and Independent Protection Layers. *Wiley*(2014) 381 pages.
27. IEC 61511 standard. Functional safety. Safety instrumented systems for the process industry sector. Parts 1 to 3, *International Electrotechnical Commission* (2003) 56 pages.
28. Kim, M.; Lee, W.; Kim, S. SIL verification report.*Skikda Refinery Rehabilitation & Adaptation Project*(2010) 16 pages.

29. IEC 61508 standard, Functional safety of electrical /electronic/ programmable electronic safety-related systems. *International Electrotechnical Commission* (2010) 236 pages.
30. Omeiri, H.; Innal, F. Safety Integrity Evaluation of a Butane Tank Overpressure Evacuation System According to IEC 61508 Standard. *Journal of FailureAnalysis and Prevention 15(6)* (2015) 892–905.
31. Arendt, J.; Lorenzo, D. Evaluating Process Safety in the Chemical Industry. A user's guide to quantitative risk analysis. *CCPS* (2000) 104 pages.
32. Luis, J.; Rodriguez, M. Abnormal Situation Diagnosis Using D-higraphs. *ESCAPE20, Elsevier B.V* (2010) 11 pages.
33. IEC 61882 standard, Hazard and operability studies (HAZOP studies). *Application guide. Second edition* (2016) 128 pages.
34. CCPS, Layer of protection analysis: a New PHA Tool after Hazop, before Fault Tree Analysis. *International Conference and Workshop on Risk Analysis in ProcessSafety* (1997) 17 pages.
35. Rajkumar, B.; Digvijay, A.; Pruthwiraj, B.; Kothavale, B. Fault Tree Analysis: A Case Study from Machine Tool Industry. *VJTI* (2018)5 pages.
36. Sam, M. Fault tree analysis. Lees' loss prevention in the process industries, hazard identification. *Assessment and control*. *Thirdedition.A&M University*(2004) 3708 pages.
37. Debray, B.; Chaumette, S.; Descouriere, S.; Trommeter, V. methodes d'analyse des risques générés par une installation industrielle. *INERIS-DRA-35* (2006) 140 pages.
38. Song, J.Operation and Maintenance Manual for CDU-10.*Skikda Refinery* (2012) 257 pages.
39. Kim, B. DCS Graphics Static Layout Printouts (SRR1).*Skikda refinery*(2011) 168 pages.
40. Nouger, N.;Verhaeghe, M. étude de dangers de la raffinerie de skikda, chapitre B1: distillation atmosphérique(2009) 182 pages.
41. GRIF-Workshop, Graphical interface for reliability forecasting software(2020)http://grif-workshop.com.
42. Majuno, S.; Shaakal, R. Safety integrity level (SIL) classification study report of crude distillation unit I&II (unit 10/11). *Skikda refinery* (2006) 161 pages.
43. Travaux du groupe d'échange « Fréquence des événements initiateurs d'accidents », Fréquence des événements initiateurs d'accidents et disponibilité des barrières de protection et de prévention. *ICSI(*2009) 31 pages.
44. ALOHA, Areal Locations of Hazardous Atmospheres. U.S. Environmental Protection Agency (EPA). *National Oceanic and Atmospheric Administration (NOAA)*(2006) 96 pages.

PleasecitethisArticleas:
Bouasla S., Mechhoud E., Zennir Y.,Bendib R., Rodriguez M., Evaluation of safety instrumented system in a petroleum plant and its impact on the environment. ***Algerian J. Env. Sc. Technology,* 9:1 (2023) 2908-2922**