Evaluation of safety instrumented system using "HAZOP-LOPA-FTA" methodology: Case study: Column C-63 at Skikda-RA1K refinery

Article *in* Algerian Journal of Signals and Systems · December 2024

DOI: 10.51485/ajss.v9i4.249

4 authors, including:

Yasser Rehail
University of Science and Technology Mohammed boudiaf, Oran_algeria (USTO-MB)

Zennir Youcef
University of Skikda

Khalid Larit
University of Skikda

Evaluation of safety instrumented system using "HAZOP-LOPA-FTA" methodology

Case study: Column C-63 at Skikda-RA1K refinery

REHAIL YASSER(1) *, ZENNIR YOUCEF(2), LARIT KHALID (3),TCHOUAR NOUREDDINE(4)

(1),(4)LIPE (Laboratoire d'Ingénierie des Procédés de l'Environnement), Department of Chemistry Physics, University of Science and Technology of Oran Mohamed Boudiaf, USTO-MB, Oran, Algeria.
(2)Automatic Laboratory of Skikda University Skikda, Algeria.
(3)Laboratory LRPCSI Skikda, Université 20 Août 1955 August 1955 Skikda, Algeria.

* yasser.rehail@univ-usto.dz; y.zennir@univ-skikda.dz

Abstract: Following the IEC 61508 standard, this paper presents a combined "HAZOP-LOPA-FTA" method for evaluating the safety level of a High Integrity Pressure Protection System (HIPPS) which is a type of SIS. The technique combines hazard and operability analysis (HAZOP), layers of protection analysis (LOPA), and fault tree analysis (FTA). This paper aims to confirm that a safety instrumented system achieves the intended safety integrity level as per IEC 61508. If not, suggest upgrading the safety instrumented system to lessen the effects of the scenario under study. The technique was used in the C-63 distillation column at RA1K Skikda refinery. HAZOP identified important causes and effects. According to LOPA, a minimum safety level was determined. The real SIL rating was calculated using the Tree module in the GRIF software.

Keywords: Safety Instrumented System (SIS), STPA, Layers of Protection Analysis (LOPA), Fault Tree Analysis (FTA).

1. INTRODUCTION

The IEC 61508 [1] presents safety instrumented systems (SIS) requirements for all the relevant lifecycle phases and has become the standard for SIS specification, design, implementation, and operation. A SIS is a collection of one or more input components (such as sensors and transmitters), logic solvers (such as programmable logic controllers [PLC]), and one or more end elements (such as safety valves). The safety integrity level is a statistical representation of the integrity of the SIS when a process demand occurs. IEC 61508 defines four discrete safety integrity levels, with SIL 4 the highest level and SIL 1 the lowest [1]. Each level corresponds to an interval in the average probability of failure ondemand (PFDAvg) and the probability of a dangerous failure per hour (PFH), as shown in Table 1.

Safety instrumented systems (SIS) evaluation is necessary for ensuring the trustworthy and efficient reduction of chemical risks in industrial processes [2]. This paper attempts to check how well our SIS performed, focusing on developing the "HAZOP-LOPA-FTA" technique. This all-encompassing and integrated methodology makes it possible to evaluate the safety integrity of SIS [3].

HAZOP technique is a process hazard analysis (PHA) method that seeks to identify potential deviations from a design operation and to analyze the hazards associated with these deviations [4]. Usually, this is achieved by employing particular guide words to facilitate the identification of potential hazards and their consequences [5].

LOPA is a widely used semi-quantitative safety analysis method that determines the minimum SIL required to reduce risk levels of SIFs to acceptable levels[6]. The method relies on hazard scenarios to identify the required number of independent protection layers needed to control the risk of each scenario.

FTA is a systematic and deductive method used to analyze and understand the relationships between events and their underlying causes within a system [7]. It begins with a top undesired event and systematically considers all known events and faults that could cause or contribute to the occurrence of the top event of logical gates to determine the different causes that could lead to a specific top event enabling a comprehensive understanding of how the top event can occur [8].

Table 1 Safety Integrity Levels according to PFDAvg and PFH[9]

Safety Integrity Level (SIL)	Probability of failure on demand (PFDAvg)	Probability of failure per hour (PFH)
4	$\geq 10^{-5}$ to $<10^{-4}$	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-4}$ to $<10^{-3}$	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-3}$ to $<10^{-2}$	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-2}$ to $<10^{-1}$	$\geq 10^{-6}$ to $<10^{-5}$

Therefore, the main objective of this paper is to apply the "HAZOP-LOPA-FTA"methodology to evaluate the safety integrity level of the High Integrity Pressure Protection System (HIPPS) installed in the C-63 column at the Skikda refinery. If the achieved SIL does not meet the standard, suggestions for improvements will be provided.

The rest of the paper is structured as follows: Section 2 presents the proposed methodology. Section 3 describes the C-63 distillation column and its SIS named HIPPS 2351. The proposed methodology is then applied in Section 4. Section 5 highlights the results, such as the achieved SIL and their implications for process safety, while Section 6 concludes with the main findings and recommendations for potential improvements.

2. METHODOLOGY

The methodology followed to achieve the objective of this study is summarized as shown in Figure 1. an application of the HAZOP-LOPA-FTA approach, in other words, the application of the HAZOP, LOPA, and FTA methods in order of installation in C63 Column of the Splitter I installation.

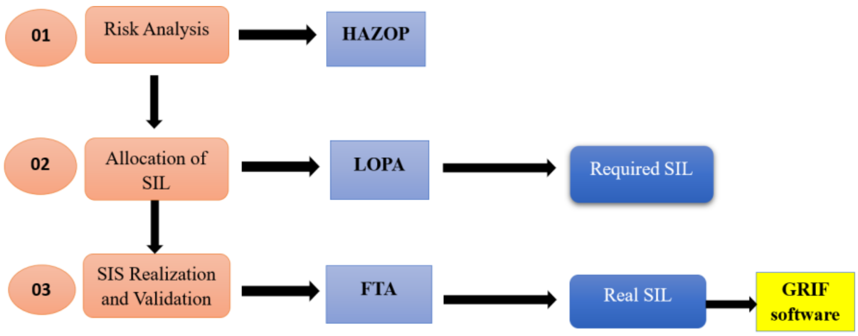

Fig.1. Methodology steps.

3. CASE STUDY

A. Functional description of the studied plant

Before each development of a risk analysis [10], 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 C-63 Column (Figure 2), located in Splitter-I at Topping unit 10 in Skikda refinery (Algeria).

The stabilized bottom naphtha from the stabilizer column is directed to the Cascade Splitter-I column (10-C-63), which consists of 36 trays operating at 57°C and a pressure of 1.0 kg/cm²g. Gasoline is introduced at tray 23, with its flow regulated by 10-FIC-54. The overhead vapor is condensed by heat exchangers 10-EA-63AF and 10-E-78AH, maintaining a temperature of 40°C. The condenser liquid level is used to control the column pressure through 10-PIC-2310 and 10-PV-2310. Safety measures include a relief valve system (10-PSV-2351A~E) and a Safety Instrumented System (I-2351). The condensed overhead liquid is collected in the reflux drum (10-V-67). At the column's base, the product is heated using hot oil via the 10-E-75A/B reboiler, with its outlet temperature monitored and controlled by 10-TIC-2351 based on tray 3 temperature. Reflux is supplied by pumps 10-P-29A/B, with flow regulated by 10-FIC-2356. The bottom naphtha stream from pumps 10-P-65A/B is divided: one portion is sent to the Splitter-II column (10-C-61) controlled by 10-FIC-2351, while the remainder is directed to the C6 Cut Splitter (10-C-6) under the control of 10-FIC-2352 via cascade regulation of the bottom level using 10-LIC-2355.

B. Safety Instrumented system of C-63 column

The BPCS handles a majority of the process control operations, the SIS acts as a second automated line of defense in the case of failure of the BPCS or due to any other condition that prevents the BPCS from controlling on its own. In our case, this action is ensured by the activation of the High Integrity Pressure Protection System (HIPPS), which is indeed a type of SIS.

The HIPPS 2351 system installed in column C-63 is a type of SIS operating in low-demand mode. Looking back to C-63-Column, this ensures the section's automatic total stop to minimize the explosion risk. [11]
All the elements constituting the HIPPS 2351 system in column C-63 are grouped in Table 02 with the definition of the associated functions in the process.

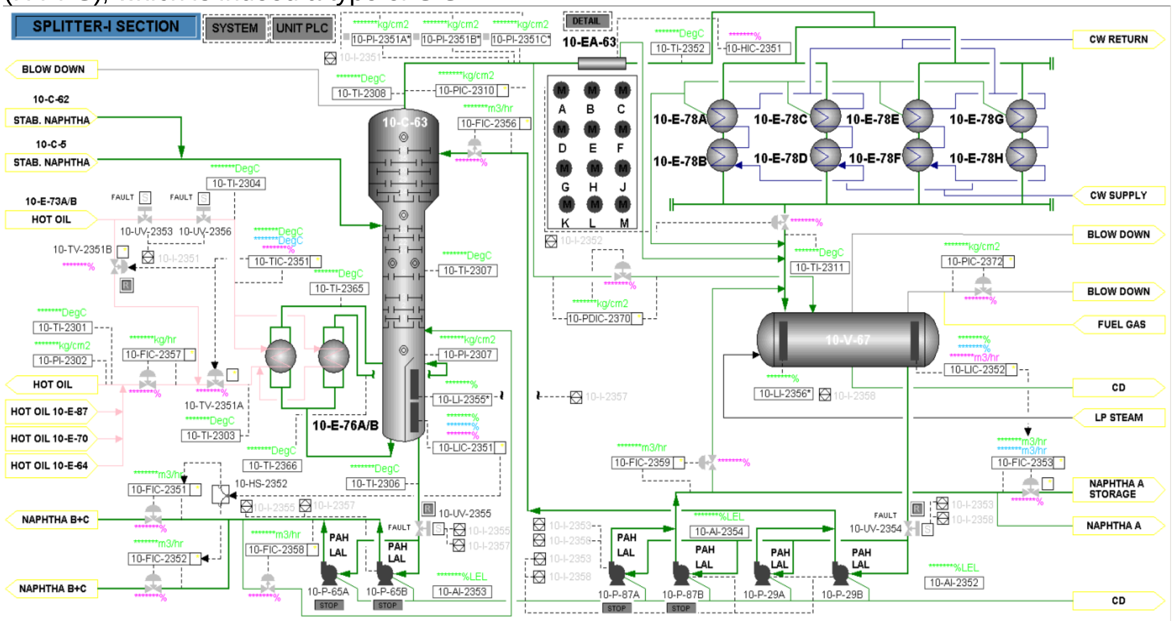

Fig.2. C-63 Column-related diagram

Table 2 HIPPS components[11]

Element	Type	Process Function
PT 2351 A	Pressure Transmitter	Detect High Pressure in C-63
PT 2351 B		
PT 2351 C		
PLC 2351	Process Logic Controller	Collects information from the detection part, carries out the decision-making process, and transmits it to the actuators
UV 2353	Isolation valve	Close to stop the hot oil supply at the entrance to column C-63
UV 2356		
TV 2351	Control valve	Opening to evacuate the extra flow in the column

4. APPLICATION OF THE METHODOLOGY

A. Execution of HAZOP method

The first step involves conducting a thorough risk analysis to identify the potential risks associated with the industrial process under consideration. The HAZOP method, a systematic and structured technique for hazard identification, is applied in this step to analyze the deviation "High Pressure inside C-63." By breaking down the process into specific nodes and using guidewords to explore possible deviations. Table 3 summarizes the identified scenarios, including the contributing factors, such as equipment failures or operational anomalies, and their potential impacts on the system, such as overpressure, loss of containment, or explosion risks. This step lays the groundwork for subsequent layers of analysis and safety improvement measures.

Table 3 HAZOP Worksheet

Deviation		Causes	Consequences	Safeguards	Criticality	
Parameter	**Guide Word**				**S**	**P**
Pressure	**High**	Temperature increase Level increase BPCS 2310 failures: PT 2310 failures PIC 2310 failures PV 2310 failures (does not open) BPCS 2370 Failure: PDT 2370 failures PDIC 2370 failures PDV 2310 failures (does not open)	Loss of containment, leading to the release of Naphtha into the atmosphere (Leak) Overpressure Vapor cloud explosion (VCE) Flash fire Pool fire	PAH on PIC 2310 PAHH on LS 2351 Interlock 2351	**4**	**2**

B. Allocation of the required SIL using LOPA

LOPA is a highly effective method for analyzing complex systems across various industries, offering a systematic framework for selecting appropriate risk-reducing measures. In this study, the LOPA method is applied to assess the explosion risk scenario in the C-63 column of a petroleum refinery. The goal is to determine the appropriate Safety Integrity Level (SIL) that the High Integrity Pressure Protection System (HIPPS 2351) must achieve to ensure the safe and reliable operation of the process.In this case, LOPA focuses on the overpressure scenario in the C-63 column, identifying the minimum SIL required to reduce the risk to an acceptable level. Table 04 presents the results of the LOPA study, which indicates that the required SIL for the C-63 column's safety instrumented system is SIL 2. This corresponds to a minimum Probability of Failure on Demand (PFDavg) of 1.41E-3. This means that the HIPPS 2351 must be designed and maintained to meet this level of performance to effectively reduce the likelihood of a hazardous explosion and ensure the overall safety of the process.

Table 4 LOPA method related to overpressure in the C-63 Column

Impact Event		**Initiating Event**		**Protection Layers (PLs) (Probabilities)**				**Intermediate event likelihood**	**PFD_{Avg} required and SIL**	**Tolerable mitigated event likelihood**
Impact event description	Severity	Description	Frequency per year	General design	Control systems	Alarms, etc.	Additional mitigation restricted access			
C-63 Column Overpressure	**05**	**PT-2310 Failure**	$3,3883.10^{-3}$	1	1	0.1	1	$3,3883.10^{-5}$	**1.41E-3** **(SIL 02 with a minimum PFD_{Avg} of 1.41E-3**	**10^{-5}**
		PIC-2310 Failure	$2.1260.10^{-5}$	1	0.1	1	1	$2.1260.10^{-7}$		
		PV-2310 Failure	$6,7593.\ 10^{-3}$	1	1	1	1	$6,7593.\ 10^{-4}$		
								Total: $7.1.\ 10^{-3}$		

C. Realization and validation of the SIS

The HIPPS 2351 implementation using FTA is presented in Figure 3. The FTA shows the various events that could lead to the failure of the HIPPS 2351 to protect the distillation column C-63 from overpressure. The top event of the FTA is labeled "HIPPS 2351 Failure," which indicates that the entire HIPPS system has failed. Overall, the FTA provides a valuable tool for understanding the different ways in which the HIPPS can fail. Several factors are considered, including the loop architecture that incorporates voting levels and redundancy, the maintenance and test policy (frequency and coverage rate),dangerous undetected (DU) failures and common cause failures (CCF). The results obtained specified for HIPPS 2351 are:

- The average probability of failure on demand (PFDAvg (t)).
- Number of cut sets.
- The maximum probability of failure on demand (PFD Maximum).
- The percentage of time spent by the loop in the different SIL levels.

The constructed FTA and following simulation results are obtained using GRIF software [12]. The reliability data including dangerous undetected (DU) failure rates [13]and beta factors [14] corresponding to HIPPS 2351 components failure are given in Table 4.

Table 4 Input data for HIPPS 2351 [13], [14-15]

Components	λD (h-1)	β	T1(h)	MTTR
PT 2351 A/B/C	2.8E-6	0.15	8760	24
LS 2351	7E-7	/	8760	24
UV 2353 UV 2356 TV 2351	2.1E-6	0.12	8760	12

The FTA can help identify areas where the system can be improved by identifying critical failure paths, the FTA has defined 08 cut sets (Table 5).

Table 5 Number of cut sets related to the failure of HIPPS 2351

System	Order	Number of cut sets
HIPPS 2351 Failure	All	**8**
	0	0
	1	2
	2	6

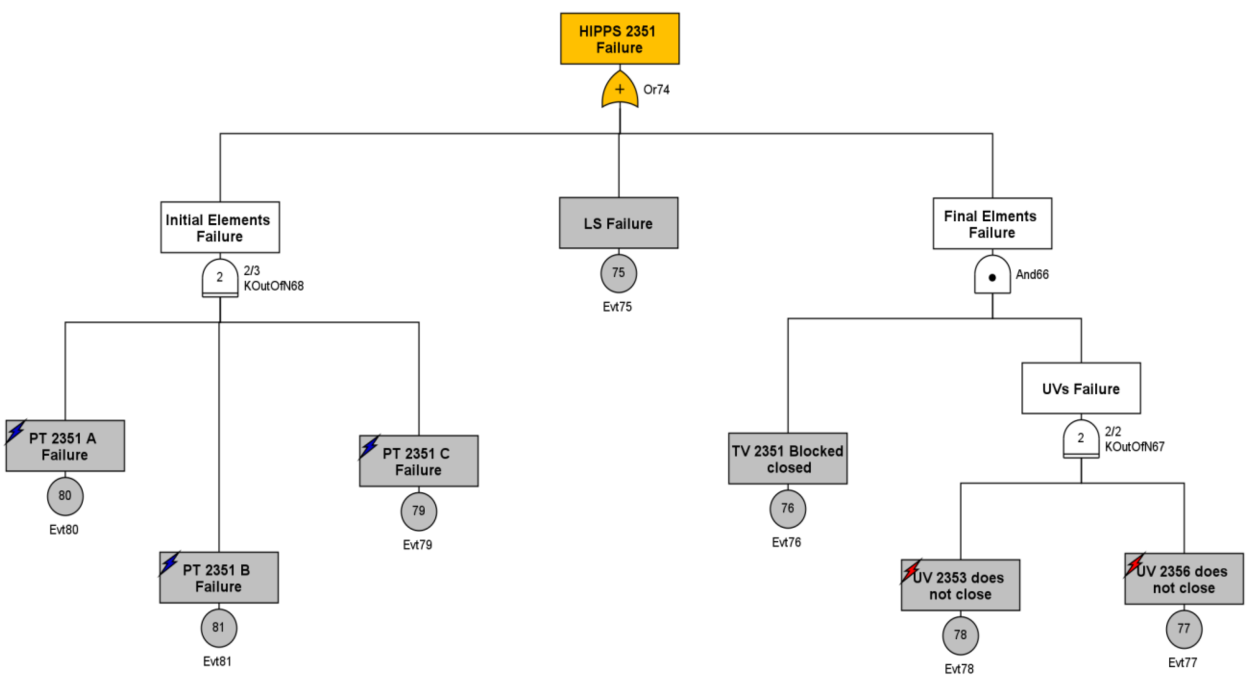

Fig. 3. FTA related to the HIPPS 2351 Failure

The identified cut sets mean that there are 08 different ways in which the failure event can occur, each of which would result in HIPPS 2351 failure which could have a significant impact on the pressure within Column C-63, potentially leading to an overpressure scenario. The results shown in Figure 4 allowed us to extract the PFDAvg and SIL of the studied SIS.

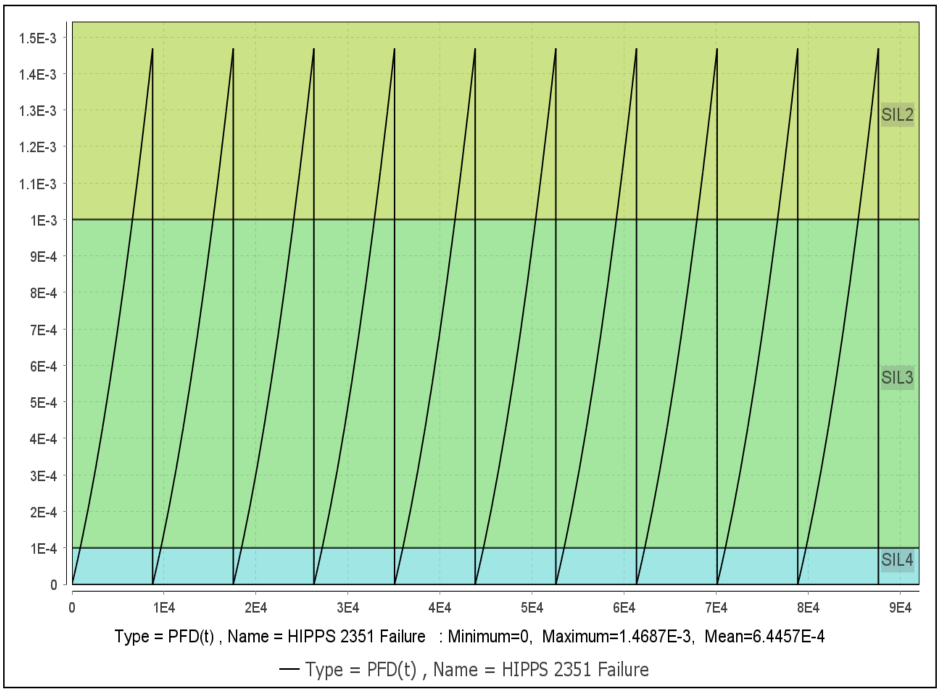

Fig.4. PFD(t) of the HIPPS 2351

5. Results and discussion

The application of the integrated "HAZOP-LOPA-FTA" methodology yielded significant insights into the safety integrity of the High Integrity Pressure Protection System (HIPPS) installed in the C-63 column at the Skikda refinery. The HAZOP study identified "High Pressure inside C-63" as a critical deviation with potentially severe consequences, including overpressure, loss of containment, vapor cloud explosions (VCE), flash fires, and pool fires. This initial step established a clear foundation for the subsequent quantitative analyses.

TheLOPA analysis built on the HAZOP findings to quantify the minimum required SIL to reduce the identified risks to acceptable levels. The required SIL was determined to be SIL 2, with a PFDAvg of 1.41E-3.

By using the Fault Tree based on the calculation of the PFD, the result of PFDAvg is 6.4457E-4, this value corresponds to a Safety Integrity Level (SIL) rating of SIL 3 according to IEC 61508 standards. This SIL value serves as an excellent benchmark and demonstrates how the HIPPS can maintain its performance in terms of safety and dependability even in the presence of CCFs.

6. Conclusion

The safety integrity level (SIL) of the High Integrity Pressure Protection System (HIPPS) 2351 was evaluated in this work using an integrated "HAZOP-LOPA-FTA" methodology per IEC 61508 standards. For the distillation column C-63, HAZOP determined that an overpressure scenario posed a serious risk. LOPA states risk reduction necessitates a minimum SIL 2 (PFDavg ≤ 1.41E-3). The achieved PFDavg for HIPPS 2351 was determined by fault tree analysis using GRIF software to be 6.4457E-4, corresponding to SIL 3. According to IEC 61508, HIPPS 2351 achieves SIL 3 to reduce the overpressure risk by attaining the SIL 2 requirement.Without requiring design changes, the integrated "HAZOP-LOPA-FTA" technique effectively verified that the HIPPS 2351 in use satisfies the required safety standards. This thorough methodology works well for comparing safety instrumented systems in the process industry to functional safety standards.

References

[1] IEC 61508 standard, Functional safety of electrical /electronic/ programmable electronic safety-related systems, International Electrotechnical Commission, Geneva, Switzerland, 2010.

[2] Y. Zennir, S. E. I. Bouasla, and E. A. Mechhoud, "Evaluation of Safety Instrumented System in a petrochemical plant using HAZOP-LOPA-Fault Tree Methodology: Case Study: Naphta Stabilizer-A Reflux Drum (LPG separation) in RA1K," in 2020 International Conference on Electrical Engineering, ICEE 2020, Institute of Electrical and Electronics Engineers Inc., Sep. 2020.L.

[3] Cui*etal.HASILT: an intelligent software platform for HAZOP, LOPA, SRS and SIL verificationReliab. Eng. Syst. Saf.*(2012).

[4] D. N. Siddiqui, A. Nandan, M. Sharma, and A. Srivastava, "Risk management techniques HAZOP and HAZID study," Int J Occup Health Saf, Fire Environ Allied Sci, vol. 1, no. 1, pp. 5–8, 2014.

[5] N. L. Rossing, M. Lind, N. Jensen, and S. B. Jørgensen, "A functional HAZOP methodology," Comput Chem Eng, vol. 34, no. 2, pp. 244–253, 2010.

[6] A. M. Dowell III, "Layer of protection analysis for determining safety integrity level," ISA Trans, vol. 37, no. 3, pp. 155–165, 1998.

[7] W. Jiang, S. Liu, and A. Liu, "A Systematic Method for Identifying Safety-related Faults in Formal Specifications Using FTA," in 13th International Conference on Reliability, Maintainability, and Safety: Reliability and Safety of Intelligent Systems, ICRMS 2022, 2022.

[8] Giraud L, Galy B. 'Fault tree analysis and risk mitigation strategies for mine hoists', Saf Sci, vol. 110, pp. 222–234; 2018.

[9] IEC 61511 standard, Functional safety – Safety instrumented systems for the process industry sector - Parts 1 to 3, InternationalElectrotechnical Commission, Geneva, Switzerland, 2003.

[10] P.K. Marhavilas, D. Koulouriotis, and V. Gemeni, "Risk analysis and assessment methodologies in the work sites: On a review, classification and comparative study of the scientific literature of the period 2000–2009," J Loss Prev Process Ind, vol. 24, no. 5, pp. 477–523, 2011.

[11] Y. REHAIL, Y. ZENNIR, N, TCHOUAR. "Application of STPA for Comprehensive Risk Analysis of Naphtha Explosion Hazards: Case study: Column C-63 at Skikda-RA1K refinery". *Algerian Journal of Signals and Systems*, *9*(3), 153-161, 2024.

[12] "GRIF Workshop, 2023. Graphical interface for reliability forecasting, software, available at: http://grif-workshop.com".

[13] S. Hauge, T. Kråkenes, P. Hokstad, S. Håbrekke, and H. Jin, SINTEF Technology and Society Safety Research Report Reliability Prediction Method for Safety Instrumented Systems PDS Method Handbook-2013 Edition, 2013.

[14] S. Hauge, Å. Snilstveit, H. Per, H. Solfrid, H. Mary, and A. Lundteigen, SINTEF Technology and Society Safety Research Common Cause Failures in Safety Instrumented Systems Beta-factors and equipment specific checklists based on operational experience, 2015.

[15] LijieGuo ,Jianxin Kang .An extended HAZOP analysis approach with dynamic fault tree. Journal of Loss Prevention in the Process Industries, Volume 38, 2015, Pages 224-232.