Application of STPA for Comprehensive Risk Analysis of Naphtha Explosion Hazards

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

REHAIL YASSER[(1) *], ZENNIR YOUCEF[(2)], TCHOUAR NOUREDDINE[(3)]
[(1)] 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)] LAS (Laboratoire d'Automatique de Skikda), Institute of Applied Sciences and Techniques, University of 20Août 1955, Skikda, Algeria
[(3)] 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
[*] y.zennir@univ-skikda.dz

Abstract: Chemical accidents always result in significant losses due to the flammable, explosive, and toxic characteristics of hazardous chemicals. Analysis of process safety parameters is an effective way to prevent hazardous chemical accidents and reduce losses. System-theoretic process analysis (STPA) is a newer hazard analysis technique that is based on systems theory. It has been shown to be effective in identifying hazards in other industries, but its application in oil and gas plants is still rare and limited due to systems complexities and other challenges. This paper aims to apply the STPA method to a complex system "column C-63" at the Skikda RA1K refinery to prevent the explosion scenario of naphtha. The results show that STPA was able to identify the root causes of the explosion scenario, which is important for preventing chemical risks.

Keywords: STPA, Systems-Theoretic Accident Model and Processes (STAMP), Hazard Analysis, Naphtha, Explosion accident.

1. INTRODUCTION

The process of hazardous chemical production is complex, and the production materials (hazardous chemicals) are flammable and explosive[1], [2]. The risk analysis represents the heart of such processes, which aims to understand the nature of the risk and its characteristics, including possible causes and potential consequences to reduce the likelihood of these risks[3] It is a methodical way to find, understand, and deal with dangers that may harm persons, equipment, and the environment.

Traditional hazard analysis techniques in the chemical process industry such as HAZOP[4], FMEA[5], and FTA[6] have been working well to prevent losses caused by failures of physical components and for relatively simple systems[7]. However, these approaches have several limitations, especially in complex systems.

A new hazard analysis method called STPA (Systems Theoretic Process Analysis) has the same goals as traditional analysis methods like FTA, FMEA, HAZOP, Bow-Tie, ETA, etc. which is to create a set of hazardous scenarios[8-10], but STPA includes a broader set of potential scenarios, including those in which no failures occur but the problems arise due to unsafe and unintended interactions among the system components. (See Figure 1).

A scoping review [11]remarked that there has been an increase in the number of STPA publications in different industrial sectors, whereas the validation of the STPA application in oil and gas plants is rare because of systems complexity and its results have not been discussed briefly.

Naphtha is a term used to describe a class of hydrocarbon mixtures obtained from the distillation of Petroleum which refers to a combustible and volatile liquid capable of initiating fires and explosions[12]. Being regulated by OSHA (Occupational Safety and Health Administration) is the reason why it

finds a place on the Hazardous Substance List.
Therefore, the main objective of this paper is to prevent the hazardous explosion accident of naphtha by applying the STPA method in a complex petrochemical system (Column C-63).

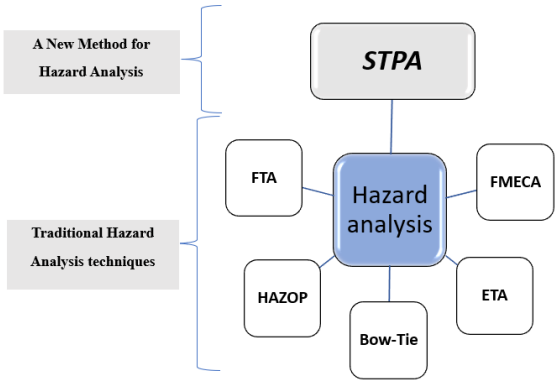

Fig. 1. Risk Analysis Methods

The rest of the article is structured as follows. Section 2 briefly describes the expanded causality model (STAMP), which has been described in detail elsewhere [4], and describes STPA. Then in Section 3, a description of the studied system (Column C-63) with its control systems is presented. Next in Section 4, the results of applying the proposed method to the Column C-63 are depicted. The recommendations related to the related method and the results are then provided in Section 5. Finally, in Section 6, the conclusions of this study are presented.

2. METHODOLOGY

A. Systems theoretic Hazard Analysis approach (STAMP)

Targeting the analysis of socio-technical complexity, the System-Theoretic Accident Model and Processes (STAMP) was proposed by Leveson [13]. In STAMP, systems are defined as interrelated components that are maintained in a dynamic equilibrium through feedback loops of information and control. STAMP and its associated technique, namely the System-Theoretic Process Analysis (STPA) have proved their capability of analyzing complex systems.

B. System-Theoretic Process Analysis (STPA)

STPA is a risk analysis method based on STAMP. focusing on creating a set of potentially hazardous scenarios and understanding the system's behavior based on the causality model rather than the reliability theory [14], [15]. It evaluates the causes, processes, and conditions leading to an accident, and suggests ways to prevent or mitigate them.
STPA utilizes a top-down approach to evaluate and analyze the safety-critical controls within a system, and it emphasizes the importance of system safety constraints to minimize risks[14]. It employs a top-down methodology for the assessment and examination of safety-critical controls within a system. According to STPA Handbook [7], four steps should be followed to apply the STPA method, which are presented in Figure 2.

C. M. Hirata et all [16] claimed that STPA identifies more loss scenarios and recommendations when compared to other hazard analysis techniques.

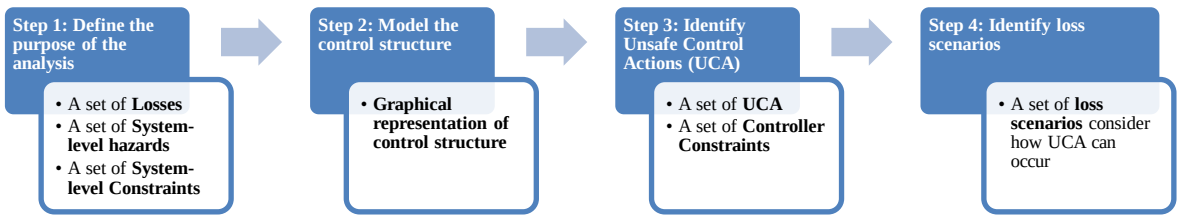

Fig. 2. The framework of STPA

3. CASE STUDY

A. Functional description of the studied plant

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 C-63 Column (Figure 3), located in Splitter-I at Topping unit 10 in Skikda refinery (Algeria).

Detailed description of the system Splitter 01

The stabilized bottom naphtha of the stabilizer column is fed to the column of Cascade (10- C-63) flow/level control splitter. The column consists of 36 trays operating at a temperature and pressure of **57 °C and 1.0 kg/cm2g** respectively.

The charged Naphtha enters the column on the 23rd tray with the flow controlled by **10-FIC-54** on the bottom of column 10-C-5. 10-FIC-54 can send low-flow alarm 10-FAL-54 to the control room.

The steam at the top of the column is condensed in the chiller to the condenser of the Splitter-I 10- EA-63A~F product and to the grille side of the control of the Splitter-I Head (10-E-78 A~H) condenser. The steam at the top is condensed by these heat exchangers at a temperature of 40°C.

The pressure of C-63 is controlled by the condenser liquid level by the pressure control **10-PIC-2310** via control valve 10 PV-2310 at the 10-E-78 A~H condensate and also by the pressure difference indicator controller **10-PDIC-2370**.

The column head is supplied with the safety valve **10-PSV-2351 A~E** at the starting pressure of 3.5kg/cm2g. Further, as a part of safety, I-2351 had been installed in column C-63 as a type of low-demand mode. The condensed overhead liquid is collected in a Splitter-I Reflux Drum (10-V-67).

Column bottom product is heated in shell side exchanger Splitter-I Reboiler (10-E-75A/B) through Hot Oil. The reboiler outlet temperature is controlled by regulating the hot oil flow through the reboiler via temperature controller **10-TIC-2351** which acts by sensing the 3rd tray temperature of the column.

The accumulated liquid in the reflux drum is sucked by pumps Splitter-I Reflux Pump (10-P-29 A/B) and sent as reflux to the column overhead (on the 36th tray) with the flow rate controlled by **10-FIC-2356**.

The bottom of the splitter (Naphtha B+C), sucked by Splitter-I bottom pumps 10-P-65A/B at the temperature indicated by 10-TI-2306, is partly sent to Splitter-II (10-C-61) and the rest to C6 Cut Splitter (10-C-6). Flow to Splitter II & C6 Cut Splitter is controlled by cascade control of 10-LIC-2355 (Splitter-I bottom level control) with 10-FIC-2351 & 10-FIC-2352 respectively via flow control valve 10-FV-2351 and 10-FV-2352 located in the relevant feed lines to columns.

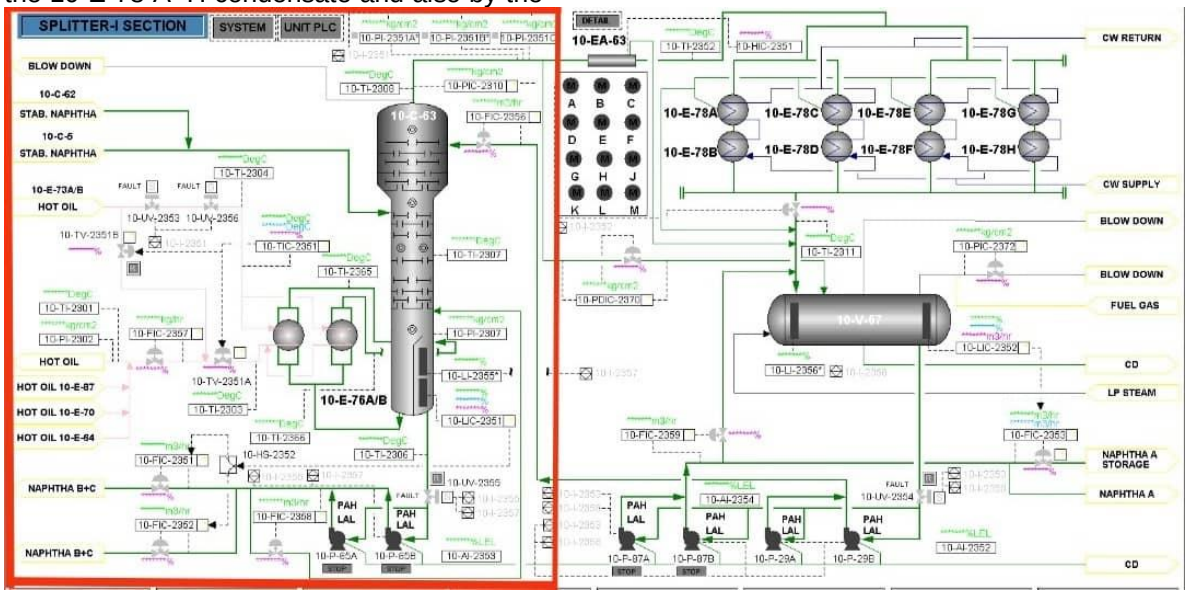

Fig. 3.C-63 Column-related diagram

In our case study, we take into account changes in temperature and pressure parameters. Under normal operating conditions for column 10-C-63, the various control and control systems are shown in the following table:

Table 1 control systems of column C-63

BPCS 2310: Pressure Control System 2310		
PT 2310 Pressure Transmitter	**PIC 2310** Pressure Indicator Controller	**PV 2310** Pressure Valve
BPCS 2370: Pressure Difference Control System 2370		
PDT 2370 Pressure Difference Transmitter	**PDIC 2370** Pressure Difference Indicator Controller	**PDV 2370** Pressure Difference Valve
BPCS 2356 : Flow Control System 2356		
FT 2356 Flow Transmitter	**FIC 2356** Flow Indicator Controller	**FV 2356** Flow Valve
BPCS 2351 : Temperature Control System 2351		
TT 2351 Temperature Transmitter	**TIC 2351** Temperature Indicator Controller	**TV 2351A** **TV 2351B** Temperature Valves

B. Safety instrumented safety of column C-63

A majority of the process control operations are handled by the BPCS, 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 High Integrity Protection System (HIPPS 2351) 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. All the elements constituting the HIPPS 2351 system in columns C-63 are grouped in Table 2 with the definition of the associated functions in the process.

Table 2 Safety instrumented safety of column C-63

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	Collects information from the detection part, carries out the decision-making process, and transmits it to the actuators
	Controller	
UV 2353	Isolation valve	Close to stop the hot oil entrance to column C-63
UV 2356		
TV 2351B	Control valve	Opening to evacuate the extra flow in the column

4. APPLICATION OF THE PROPOSED METHOD

a) Defining the purpose of the analysis

Table 3 shows high-level system hazards and safety constraints for the Explosion scenario.

The following losses are identified for the system under study:

L-1: Loss of distillation (mission).
L-2: Loss of naphtha (release to atmosphere).
L-3: Loss of the column (C-63).
L-4: Environmental loss.
L-5: Loss of life.

Table 3 High-level system hazards and safety constraints

System Level Accident	High-Level System Hazard	High-Level Safety Constraint
Explosion	**H**1: High Pressure in the column. [L-1, L-2, L-4, L-5]	**SC 1**: The Pressure in the column should not exceed a defined limit. [H-1]
	H2: High Temperature in the column. [L-1, L-2, L-4, L-5]	**SC 2**: The Temperature in the Column should not exceed a specified limit. [H-1, H-2]
		SC 3: A nearby fire should not affect the column. [H-1, H-2]

In this case, the hazards can be reduced by BPCS 2310, BPCS 2370, BPCS 2351, BPCS 2356, SIS 2351 (Interlock-2351), and PSVs (A-E) Activation.

The control actions here are the activation of BPCSs, SIS, and PSVs (A-E).

b) control structure of the system

In this step, it is necessary to model the control structure. Figure 4 shows the control structure of the system within the plant including the process model and its variables.

From the model shown in Figure 4, we can observe that a single control operation is being carried out by controllers and actuators, who are getting input from controller actions, roles, and entities in the process model.

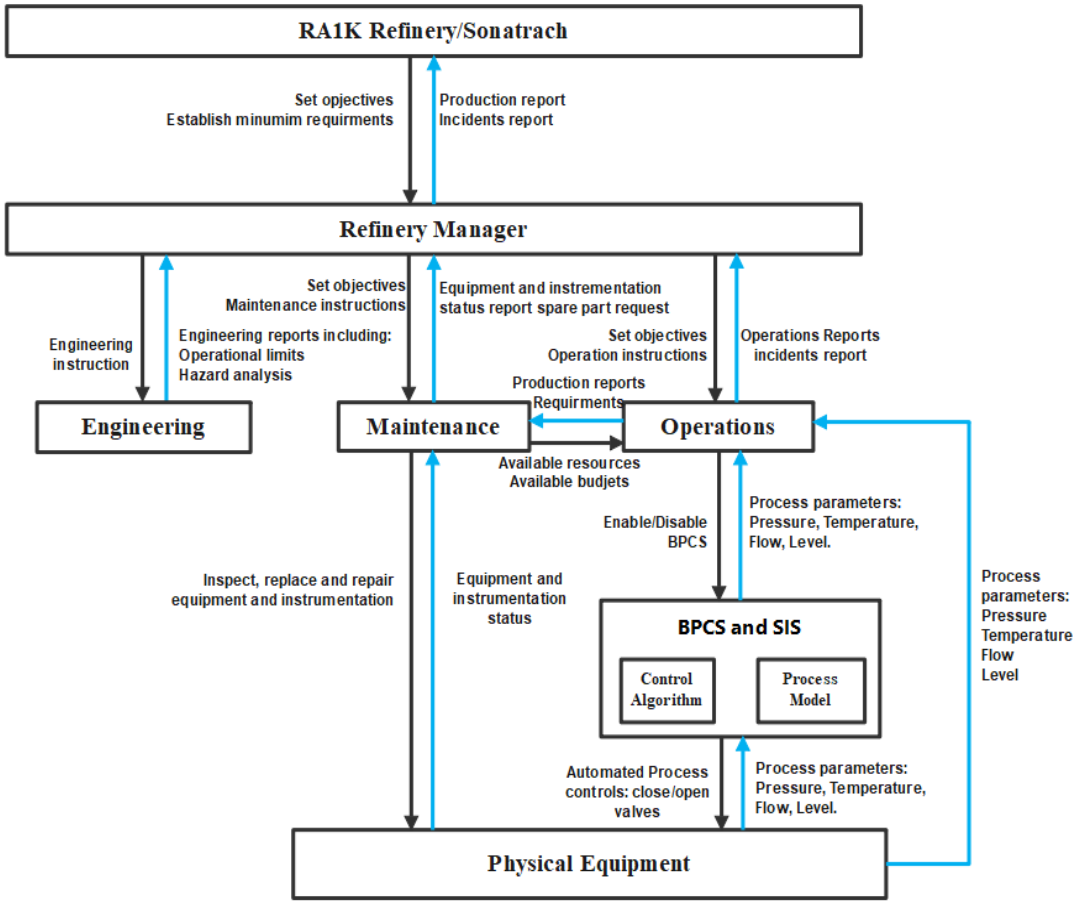

Figure 4 General control structure of the system

C) Identification of Unsafe Control Actions

Once the control structure has been modeled, the next step is identifying Unsafe Control Actions (UCA).

Table 4 presents hazardous control actions. The process model helps to identify causal factors and scenarios.

Table 4 Identified Unsafe Control Actions from the refined control structure

Control Action	Not providing Causes Hazard [H1, H2]	providing Causes Hazard [H1, H2]	Too early, too late, out of order [H1, H2]	Stopped too soon, applied too long. [H1, H2]
BPCS 2310	**UCA-01**: BPCS 2310 does **not provide** an open valve (PV 2310) function when pressure/temperature is high.	**UCA-02**: BPCS **provides** an open valve (PV 2310) function when pressure/temperature is within acceptable limits.	**UCA-03**: BPCS provides an open valve (PV 2310) function **too late** when pressure/ temperature exceeds the high limit.	**UCA-04**: BPCS 2310 **stops providing** the open valve (PV 2310) function too soon when pressure/ temperature exceeds the high limit.
BPCS 2370	**UCA-05**: BPCS 2370 does **not provide** an open valve function (PDV2370)	**UCA-06**: BPCS 2370 **provides** an open valve function (PDV 2370) when	**UCA-07**: BPCS 2370 provides a close valve (PDV 2370) function	**UCA-08**: BPCS 2370 **stops providing** the open valve (PDV 2370)

	pressure/temperature is high.	pressure/temperature is within acceptable limits.	**too late** when pressure/ temperature exceeds the high limit.	function too soon when pressure/ temperature exceeds the high limit.
BPCS 2351	**UCA-09**: BPCS 2351 does **not provide** open valves (TV 2351A/B) function when pressure/temperature is high.	**UCA-10**: BPCS 2351 **provides** open valves (TV 2351A/B) function when pressure/temperature is within acceptable limits.	**UCA-11**: BPCS 2351 **provides** open valves (TV 2351A/B) function **too late** when pressure/ temperature exceeds the high limit.	**UCA-12:** BPCS 2351 **stops providing** the open valves (TV 2351A/B) function too soon when pressure/temperature exceeds the high limit
BPCS 2356	**UCA-13**: BPCS 2356 does **not provide** more flow from the valve FV 2356 when pressure/temperature is high.	**UCA-14**: BPCS 2356 provides more flow from valve FV 2356 when pressure/temperature is within acceptable limits.	**UCA-15**: BPCS 2356 **provides** more flow from the valve FV 2356 **too late** when pressure/temperature exceeds the high limit.	**N/A**
SIS 2351 (Interlock-2351)	**UCA-16**: SIS 2351 does **not provide** an open valve (TV 2351B) function and close isolated valves function (UV 2353 and UV 2356) when the pressure is too high.	**UCA-17**: SIS 2351 **provides** an open valve (TV 2351B) function and close isolated valves function (UV 2353 and UV 2356) when the pressure is within acceptable limits.	**UCA-18**: SIS 2351 **provides** an open valve (TV 2351B) function and close isolated valves function (UV 2353 and UV 2356) **too late** when pressure is too high.	**UCA-19**: SIS 2351 **stops providing** an open valve (TV 2351B) function and close isolated valves function (UV 2353 and UV 2356) when pressure is too high.
PSVs (A-E)	**UCA-20**: PSVs (A-E) **don't provide** open safety valve (PSVs 2351) functions when the pressure is too high.	**UCA-21**: PSVs (A-E)**provide** open safety valve (PSVs 2351) functions when the pressure is within acceptable limits.	**UCA-22**: PSVs(A-E)**provide** an open safety valve (PSVs 2351) that functions **too late** when pressure is too high.	**UCA-23:** PSVs(A-E) **stop providing** the open safety valve (PSVs 2351) function too soon when pressure is too high.
Operator responds to Alarms (TAH2351, PAH 2310, FAL2356, PAHH 2351)	**UCA-24:** Operator do not provide a response to alarms when the the process is out of normal conditions.	**N/A**	**UCA-25:** Operator Respond to alarms too late when the process is out of normal conditions. [H1, H2]	**N/A**
Repair and maintain equipment and instruments	**UCA-26:** The maintenance team **does not provide** the required repair and maintenance of the equipment and instrument	**N/A**	**UCA-27:** The maintenance team provided the required maintenance **too late**.	**N/A**

d) Identifying causal factors and loss scenarios

A loss scenario describes the causal factors that can lead to unsafe control actions and hazards identified in the previous step.

The obtained causal factors of the explosion accident scenarios are presented below in Table 5.

Table 5 Identified causal factors from the refined control structure

Unsafe Control Actions	**Causal Factors**

UCA-01 **UCA-05** **UCA-09** **UCA-13**	1. Mechanical valve failure (PV 2310, PDV 2370, TV 2351, FV 2356). 2. Failure of instrumentation related to the valves (PV 2310, PDV 2370, TV 2351, FV 2356). 3. Transmitter failure (PT 2310, PDT 2370, TT 2351, FT 2356). 4. The set point of transmitters is modified wrongly in the operation. 5. Software Glitch or Bug in the control system (PIC 2310, PDIC 2370, TIC 2351, FIC 2356). 6. Communication failure between transmitters, controllers, and valves. 7. Inadequate testing and maintenance of safety systems equipment.
UCA-02 **UCA-06** **UCA-10** **UCA-14**	1. Failure of instrumentation related to the valves (PV 2310, PDV 2370, TV 2351, FV 2356). 2. Incorrect Transmitters Calibration (PT 2310, PDT 2370, TT 2351, FT 2356). 3. Software Glitch or Bug in the control system (PIC 2310, PDIC 2370, TIC 2351, FIC 2356). 4. Communication delays between different parts of the control system. 5. Environmental conditions such as temperature, humidity, or vibrations. 6. Error in Executing Maintenance Specification of safety systems equipment.
UCA-03 **UCA-07** **UCA-11** **UCA-15**	1. Incorrect Transmitters Calibration (PT 2310, PDT 2370, TT 2351, FT 2356). 2. Transmitters wrong set point from operation (modifications). 3. Communication delays between the transmitters, control system, and valves. 4. Mechanical valve failure (Blockage or Fouling). 5. Inadequate testing and maintenance of safety systems equipment.
UCA-04 **UCA-08** **UCA-12**	1. The control logic responsible for deciding when to stop the valve function has errors (PLC 2351). 2. Environmental conditions such as temperature, humidity, or vibrations. 3. Mechanical valve failure (Blockage or Fouling) (PV 2310, PDV 2370, TV 2351, FV 2356). 4. Error in Executing Maintenance Specification of safety systems equipment.
UCA-20 **UCA-21** **UCA-22** **UCA-23**	1. PSV A-E Blockage or Fouling. 2. PSV A-E Corrosion. 3. Error in Executing Maintenance Specification on the PSVs A-E. 4. Instrumentation responsible for detecting high-pressure conditions fails to provide accurate readings.
UCA-24 **UCA-25**	1. Inadequate maintenance of the alarm system or the process equipment/instrumentation. 2. Alarms failure (TAH 2351, PAH 2310, FAL 2356, and PAHH 2351). 3. Not enough workers in the maintenance team.
UCA-26 **UCA-27**	1. Error in the execution of the maintenance requirements. 2. Inadequate maintenance planning. 3. Lack of spares and tools in the warehouse.

5. RECOMMENDATIONS

Finally, new safety measures are defined in the recommendation part to prevent loss scenarios that could cause the hazardous chemical explosion scenario of Naphtha which results in catastrophic losses. Safety measures corresponding to loss scenarios are defined in Table 6.

Table 6 STPA recommendations using refined control structure of air cooler and separator

Recommandations	
1.	Implement preventive maintenance procedures to inspect and replace the valves PV 2310, PDV 2370, TV 2351A/B, and FV 2356 as needed.
2.	Verify that the set point of pressure, temperature, and flow transmitters PT 2310, PDT 2370, TT 2351, and FT 2356 are established correctly in the design.
3.	Verify that the valves PV 2310, PDV 2370, TV 2351, and FV 2356 are operating (closing and opening) time is short enough to prevent high pressure in Column C-63
4.	Provide clear work instructions, standard operating procedures, and maintenance instructions.
5.	Reviewing and optimizing the alarm system to eliminate unnecessary alarms and ensure that each alarm provides valuable information.

6.	Carry out alarms management which involves configuring and monitoring alarms TAH 2351, PAH 2310, FAL 2356, and PAHH 2351, typically in control rooms or automation systems provide operators with essential information about the state of the process.
7.	Define and implement adequate maintenance (preventive and corrective) and calibration program for transmitters (PT 2310, PDT 2370, TT 2351, and FT 2356), logic solvers (PIC 2310, PDIC 2370, TIC 2351, and FIC 2356), and final elements (PV 2310, PDV 2370, TV 2351A/B, and FV 2356) to ensure correct detection and prevent malfunctioning of BPCS 2310, BPCS 2370, BPCS 2351, and BPCS 2356 respectively.
8.	Include High High alarms for BPCS 2310, BPCS 2370, and BPCS 2351
9.	Include Low Low alarm for BPCS 2356.
10.	Define and implement adequate maintenance (preventive and corrective) and calibration programs for I-2351 components to ensure they perform effectively and reliably.
11.	Include High High and Low Low alarms for BPCS 54 to ensure the appropriate control of the charged Naphtha flow coming from the bottom of column 10-C-5.
12.	Conduct regular functional safety assessments of both BPCS and SIS, including reviews of safety instrumented functions (SIFs) and state-based control strategies to ensure that they meet industry standards and requirements.

6. CONCLUSIONS

The main objective of this study has been to improve the safety of Column C-63 to prevent the hazardous explosion accident of Naphtha using a new method for risk analysis in complex systems called STPA. Possible causes identified by STPA cover hardware failures and communication errors, including communication delays and software errors. The results show that STPA is a systematic hazard analysis technique that can handle very complex systems in petrochemical plants, also it provides systematic guidance and recommendations for safety requirements.

References

[1] Z. Gyenes,M.H. Wood, and M. Struckl, “Handbook of scenarios for assessing major chemical accident risks”, Publications Office of the European Union. Luxembourg, 2017, pp. 1-116.

[2] H. J. Pasman, “Risk analysis and control for industrial processes-gas, oil and chemicals: a system perspective for assessing and avoiding low-probability, high-consequence events”. Butterworth-Heinemann, 2015.

[3] 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,” International Conference on Electrical Engineering, 2020.

[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] L. S. Lipol and J. Haq, “Risk analysis method: FMEA/FMECA in the organizations,” International Journal of Basic & Applied Sciences, vol. 11, no. 5, pp. 74–82, 2011

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

[7] E. Heikkilä, T. Malm, J. Sarsama, R. Tiusanen, and T. Ahonen, “Hazard Analysis of an Autonomous Container Handling System – a Comparison of STPA and HAZOP Methods,” Scientific Journal of Gdynia Maritime University, no. 125, pp. 25–39, Mar. 2023.

[8] J. T. N. Leveson, “STPA_Handbook,” MIT, Cambridge, pp. 0–188, 2018.

[9] M. El-Arkam, R. Bendib, A. Aribi, and Y. Zennir, “Risk Assessment in a Petrochemical Plant Using Socio-Technical Approaches (STAMP-STPA)”, Engineering Proceedings, vol. 29, no. 1, 2023.

[10] A. Plioutsias and N. Karanikas, “Using STPA in the evaluation of fighter pilots training programs,” Procedia Eng, vol. 128, pp. 25–34, 2015.

[11] Y. Wu, G, Fu, M. Han, Q. Jia, Q. Lyu, Y. Wang, and Z. Wu, “Comparison of the theoretical elements and application characteristics of STAMP, FRAM, and 24Model: A major hazardous chemical explosion accident,” J Loss Prev Process Ind, vol. 80, p. 104880, 2022.

[12] New Jersey Department of Health and Senior Services, "naphtha hazard summary reason for citation how to determine if you are being exposed", 2007.

[13] N. Leveson, “A new accident model for engineering safer systems,” Saf Sci, vol. 42, no. 4, pp. 237–270, 2004.

[14] C. Bensaci, Y. Zennir, and D. Pomorski, “New Approach to System Safety of human- multi-robot mobile system control with STPA and FTA,” Algerian Journal of Signals and Systems, vol. 5, no. 1, pp. 79–85, Mar. 2020.

[15] C. Bensaci, Y. Zennir, D. Pomorski, F. Innal, and Y. Liu, “Distributed vs. hybrid control architecture using STPA and AHP - Application to an autonomous mobile multi-robot system,” International Journal of Safety and Security Engineering, vol. 11, no. 1, pp. 1–12, Feb. 2021.

[16] F. G. R. De Souza, C. M. Hirata, and S.Tehrani, “Synthesis of a Controller Algorithm for Safety-Critical Systems,” IEEE Access, vol. 10, pp. 76351–76375, 2022.