International Journal Of Health, Engineering And Technology (IJHET) *E-ISSN 2829 - 8683*
Volume 4, Number 6, March 2026, *Page. 2328 - 2336*
Email : editorijhess@gmail.com

System Failure Analysis Using FTA, LOPA, And Aspen HYSYS Approaches: The 2005 BP Texas City Case Study

Lucky Yudanto Anggoro[1)*], Fauzul Azmi[2)], Agrytia Rut Meiriski Aritonang[3)], Favian Hafiz Zain[4)], Bani Isnain Rochmatan Imannudin[5)], Selly Purwasi[6)], Eka Fitriani Ahmad[7)]
[1,2,3,4,5,6,7)] D4 - Occupational Safety and Health, Politeknik Ketenagakerjaan, Indonesia

*Corresponding Author
Email : luckyudanto@gmail.com

Abstract

This research aims to comprehensively analyze the 2005 BP Texas City accident by integrating Fault Tree Analysis (FTA), Layers of Protection Analysis (LOPA), and Aspen HYSYS conceptual simulation. Using a qualitative descriptive approach, this study reconstructs systemic failures based on official investigation reports. FTA results reveal complex interactions between instrumentation failures, operational deviations, and design weaknesses as primary causes, while LOPA evaluation demonstrates the ineffectiveness of all independent protection layers in preventing hazard escalation. Furthermore, Aspen HYSYS simulation visualizes the dynamics of mass and energy imbalance during the start-up phase leading to column overfilling. This research contributes significantly to the development of process safety education by providing an integrated risk analysis framework to understand the evolution of industrial accidents holistically. The practical implications emphasize the urgency of implementing inherently safer designs, improving start-up management, and strengthening safety culture to prevent the recurrence of catastrophic incidents in the future.

Keywords: Aspen HYSYS, BP Texas City, Fault Tree Analysis, Layers Of Protection Analysis, Process Safety.

INTRODUCTION

The major accident that occurred at the BP Texas City Refinery on March 23, 2005, constitutes one of the deadliest industrial tragedies in United States history. The explosion, which took place during the start-up process of the C6/C7 paraffin isomerization unit, resulted in the deaths of 15 workers, injured more than 180 individuals, and caused economic losses exceeding one billion US dollars. A series of investigations—including the report of the Chemical Safety and Hazard Investigation Board (CSB, 2007), BP's interim investigation report (Mogford, 2005), and the Baker Panel review (Baker et al., 2007)—identified fundamental weaknesses in safety culture, ineffective operational oversight, and inconsistent procedural practices at the facility.

Although organizational and managerial factors played a significant role in the occurrence of this accident, a comprehensive understanding requires a deeper analysis of the evolution of process phenomena occurring within the system. On the day of the incident, a series of abnormal process conditions—including excessive liquid accumulation in the raffinate splitter tower, the formation of two-phase flow, the opening of pressure safety valves, and the large-scale release of hydrocarbons into the blowdown system—occurred sequentially and were mutually interconnected. This chain of events indicates multiple failures across several layers of protection that were intended to prevent hazard escalation during the start-up phase, a condition widely recognized as a high-risk operating state (Nurjaman et al., 2021).

This study aims to analyze the BP Texas City accident in a structured manner by integrating several process safety approaches. Root causes and failure pathways are examined using Fault Tree Analysis (FTA) to identify combinations of technical, human, and organizational failures that led to the top event. Subsequently, the effectiveness of safety systems is evaluated using Layers of Protection Analysis (LOPA) to assess failures and weaknesses within each existing protection layer, ranging from operational procedures and instrumentation to relief systems.

To support this analysis, Aspen HYSYS is employed as a conceptual simulation tool to reconstruct process evolution based on the findings of the CSB investigation. Aspen HYSYS is a process simulation software widely used to model equipment behavior and process systems in the oil

and gas industry (Miledhiya & Sari, 2024). In this study, Aspen HYSYS is utilized as a conceptual simulation tool to represent the evolution of process conditions during the start-up phase, with particular emphasis on the operational interrelationships among pressure, temperature, and liquid level variations within the column, and how these conditions—based on CSB investigation findings—contributed to the activation of pressure protection systems and flow discharge into the blowdown system.

Through the integration of FTA, LOPA, and Aspen HYSYS-based process simulation, this study is expected to provide a more comprehensive understanding of the systemic failure characteristics underlying the BP Texas City accident. Furthermore, lessons learned are formulated to derive practical implications for improving process safety, particularly in the management of start-up operations, protection system design, and the strengthening of safety culture, in order to prevent the recurrence of similar major industrial accidents in the future.

RESEARCH METHODS

This study employs a descriptive qualitative approach to analyze the sequence of process phenomena that contributed to the accident in the C6/C7 isomerization unit at the BP Texas City Refinery in 2005. This approach was selected because the study focuses on developing a narrative understanding of the evolution of process variables and the technical mechanisms that formed hazardous conditions (Aminestia, 2023).

The research was conducted through four main stages. First, a literature review was carried out on official investigation documents, including the CSB report (2007), BP's investigation report (Mogford, 2005), and the Baker Panel safety review (2007). This review aimed to identify the event sequence, operating conditions during the start-up phase, and technical factors relevant to column overfilling and hydrocarbon release into the blowdown system.

The second stage involved qualitative analysis of process phenomena by mapping the relationships among variables such as pressure, temperature, liquid level, and two-phase flow that emerged during start-up operations. This analysis was performed by reconstructing the sequence of events based on textual information contained in the investigation reports, thereby producing a systematic narrative representation of process condition changes from the beginning of start-up until shortly before the explosion occurred.

The third stage consisted of process safety analysis using Fault Tree Analysis (FTA). At this stage, FTA was applied to decompose the top event into a series of intermediate events and basic events in order to identify combinations of technical failures, human errors, and organizational weaknesses that collectively contributed to the accident. The FTA structure provides a foundation for understanding dominant causal pathways and the interactions among process deviations.

The fourth stage involved the evaluation of protection layers using Layers of Protection Analysis (LOPA). LOPA was conducted to assess whether safety layers—ranging from operating procedures, alarms and critical instrumentation, to relief systems—performed in accordance with their intended design effectiveness or instead experienced functional degradation. This stage provides a qualitative assessment of the adequacy and failure of each Independent Protection Layer (IPL).

The fifth stage consisted of developing a simulation model using Aspen HYSYS. At this stage, the software was utilized as a modeling tool to conceptually represent the start-up process flow. The model was constructed to illustrate fluid flow pathways, liquid level accumulation within the distillation column, the formation of two-phase flow, and fluid discharge routes toward relief valves and the blowdown system. The simulation supports clarification of cause-and-effect relationships and reinforces the narrative explanation of process dynamics.

The sixth stage involved qualitative interpretation by integrating findings from the literature review, process phenomenon analysis, Fault Tree Analysis (FTA) outputs, Layers of Protection Analysis (LOPA) evaluation, and process simulation using Aspen HYSYS. This integration was undertaken to

produce a comprehensive description of the technical evolution of events. The interpretation was used to identify critical points during the start-up phase and to understand how seemingly routine operating conditions could evolve into severe system failures. Through this qualitative approach, the study provides a comprehensive depiction of process dynamics in the BP Texas City case and highlights the role of process visualization as a supporting tool in analyzing start-up operational risks within the process industry.

RESULTS AND DISCUSSION

Analysis of Accident Causes Using Fault Tree Analysis (FTA) Techniques

Fault Tree Analysis (FTA) is a deductive safety analysis method used to identify logical relationships among component failures, process deviations, and organizational factors that may lead to the occurrence of a top event. Over the past decade, FTA has continued to evolve as an essential tool for risk evaluation in the chemical and oil and gas industries due to its capability to systematically and quantitatively model multilayer failure interactions (Zarei et al., 2020). FTA enables clear mapping among basic events, intermediate events, and conditioning events, allowing the analysis to identify dominant causal pathways as well as critical vulnerability points within a process.

In the context of the 2005 BP Texas City accident, the application of FTA provides an analytical framework capable of reconstructing how combinations of process deviations, instrumentation failures, operational errors, and weaknesses in blowdown system design contributed to hydrocarbon release leading to the explosion. This approach is consistent with modern process safety best practices that emphasize multi-layer analysis of technical causes and human factors (Sousa et al., 2021).

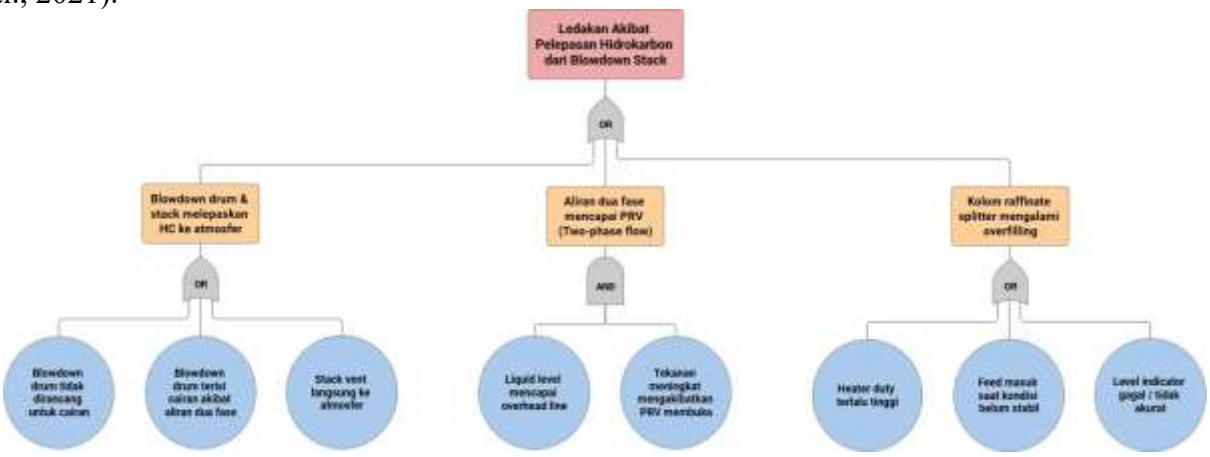

Figure 1. Fault Tree Analysis (FTA) Diagram Of The Causes Of The 2005 BP Texas City Accident

The results of the Fault Tree Analysis (FTA) indicate that the 2005 BP Texas City accident was the consequence of complex interactions among technical failures, operational deviations, and deficiencies in safety system design. The FTA structure shows that the top event—hydrocarbon release from the blowdown stack—was triggered through three primary causal pathways. The first pathway involves blowdown system failure, which appears as an intermediate event triggered by several basic events, including an outdated blowdown design lacking a flare system, insufficient drum capacity to accommodate two-phase flow, and the absence of a liquid separation mechanism prior to discharge to the vent stack. The second pathway relates to the entry of two-phase flow into the pressure relief valve (PRV). This event occurred only when two simultaneous conditions were met: liquid level escalation reaching the overhead line and column pressure exceeding the PRV set point. The “AND logic” characteristic of this pathway highlights that the combination of operational failures and adverse process conditions constituted a fundamental factor leading to hydrocarbon release into the relief system. The third pathway involves overfilling of the raffinate splitter column, caused by basic events such as excessive heater duty during start-up, feed introduction under unstable operating conditions,

malfunction of the LT-5100 level instrument, and operator noncompliance with standard start-up procedures.

In addition to these three primary pathways, the FTA also identifies several conditioning events that increased the likelihood of the top event, including inherently unstable start-up operating conditions, the use of an atmospheric blowdown system without a flare, and meteorological conditions that enabled the formation of hydrocarbon vapor clouds near ground level. These factors did not act as direct causes but amplified the consequences of the existing failure sequence. These findings align with developments in process safety literature over the past decade indicating that major industrial accidents are rarely caused by a single failure but instead result from multilayer barrier failures occurring simultaneously (Stempniak et al., 2019). The conducted FTA is also consistent with modern studies on dynamic and hybrid FTA applications, which emphasize that interactions between technical and organizational factors play a significant role in high-risk accidents, particularly under transient operating conditions such as start-up (Zhang et al., 2022).

Through the FTA approach, it can be concluded that the 2005 BP Texas City accident was not the result of a single error but rather a combination of instrumentation failures, operational errors, procedural inconsistencies, and inadequate safety system design. The elaboration of the FTA structure enables clearer identification of system vulnerabilities, ranging from malfunctioning level instrumentation to the inability of the blowdown system to handle two-phase relief flow. These results underscore the urgency of improving process safety management, particularly in pressure protection, instrumentation reliability, and start-up operational control, which represents the operational phase most vulnerable to process deviations.

Evaluating the Causes of Accidents Using the Layers of Protection Analysis (LOPA) Technique

The first protection layer identified is the Basic Process Control System (BPCS). The tower level control system failed to function effectively, as the level transmitter provided erroneous readings indicating a low level while the tower was actually overfilled. Consequently, the control valve did not discharge liquid as required. This BPCS failure represents the primary initiating event in the LOPA analysis because it eliminated normal control over the overfilling hazard.

The Alarms and Operator Intervention layer also failed to provide adequate protection. The high-level alarm and redundant high-level alarm did not operate as intended, preventing operators from receiving early warning signals. Furthermore, operator intervention proved ineffective due to misinterpretation of process conditions, work fatigue, poor shift communication, and excessive reliance on faulty instrumentation. As a result, this human-based protection layer demonstrated very low reliability.

Within the Safety Instrumented System (SIS) layer, it was identified that the unit was not equipped with an independent safety instrumentation system capable of automatically stopping feed input or terminating heating when the tower level reached a critical limit. The absence of an adequate SIS resulted in the lack of automatic interruption of event escalation, leaving risk control entirely dependent on the BPCS and operator actions.

The Physical Protection (Relief Devices) layer, represented by the pressure relief valve (PRV), functioned by opening when pressure increased. However, within the LOPA context, this layer failed to reduce consequence risk because discharged fluids were routed to an unsafe system. The PRV protected equipment from mechanical failure but did not protect personnel or facilities from hydrocarbon release hazards.

At the Physical Containment (Bund/Secondary Containment) layer, no effective containment system was available to retain hydrocarbons released from the blowdown drum. The blowdown drum and stack overflowed, allowing liquid hydrocarbons to spread into the unit area and sewer system. The absence of adequate secondary containment enabled the formation of liquid pools and flammable vapor clouds.

The Fire and Gas System likewise did not function as an effective protection layer. Gas and fire detection systems were unable to prevent vapor cloud formation or isolate the release source prior

to ignition. Additionally, no interlock system was available to automatically eliminate ignition sources in the vicinity of the blowdown drum area.

At the Plant Emergency Response layer, internal emergency response actions were largely reactive and incapable of preventing the initial explosion impacts. No effective area evacuation was conducted during start-up operations, and the presence of occupied trailers near the process unit indicated failures in implementing safety procedures under high-risk conditions. Consequently, fatalities occurred in large numbers immediately following the explosion.

The final layer, Community Emergency Response, became active only after the main incident had occurred. Shelter-in-place measures were implemented for surrounding communities; however, this layer played no role in preventing or mitigating direct impacts on workers within the plant area. In the LOPA framework, this layer serves only to limit off-site consequences rather than prevent the accident itself.

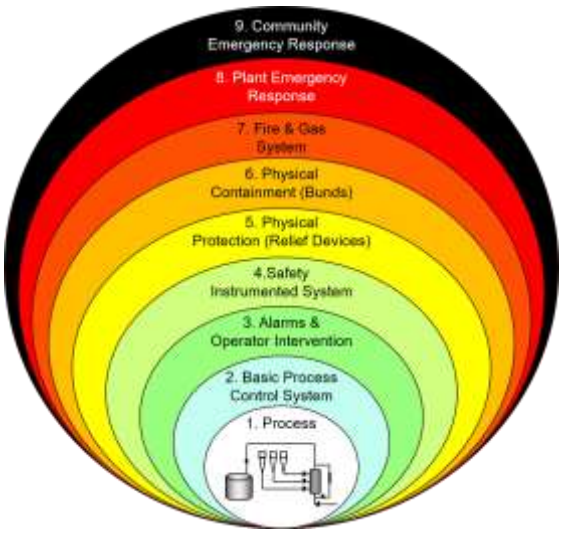

Figure 2. The Layers Of Protection Analysis (LOPA) Structure Depicting Nine Independent Layers Of Protection

The LOPA analysis based on nine layers of protection indicates that the BP Texas City accident resulted from systemic failure across nearly all protection layers rather than from a single isolated failure. The initial layers, which should have provided the highest reliability (BPCS, alarms, and SIS), were proven to be neither independent nor effective, thereby failing to prevent the escalation of abnormal conditions into a catastrophic event.

Furthermore, this LOPA analysis highlights that the emergency disposal system design constituted a critical weakness. Relief devices connected to an atmospheric blowdown drum without a flare system caused the protection layer itself to create a new hazard. From a modern LOPA perspective, such a system should be replaced with a flare system or an inherently safer design to ensure that the fifth and sixth protection layers genuinely function as risk-reduction measures.

From organizational and human-factor perspectives, the LOPA results demonstrate that administrative protection layers and emergency response measures cannot be relied upon to compensate for failures in technical protection layers. Dependence on operators, procedures, and manual response during start-up significantly increased the probability of failure. This finding is consistent with the CSB conclusion that the safety culture at BP Texas City lacked adequate focus on process safety.

Overall, the application of LOPA based on these nine protection layers shows that the residual risk in the BP Texas City case remained far above acceptable risk criteria due to the absence of sufficiently robust independent protection layers capable of interrupting the accident pathway. Therefore, the accident can be characterized as predictable and preventable had LOPA been properly implemented during both the design and operational stages.

International Journal Of Health, Engineering And Technology (IJHET) *E-ISSN 2829 - 8683*
Volume 4, Number 6, March 2026, *Page. 2328 - 2336*
Email : editorijhess@gmail.com

Process Modeling and Visualization Using Aspen HYSYS

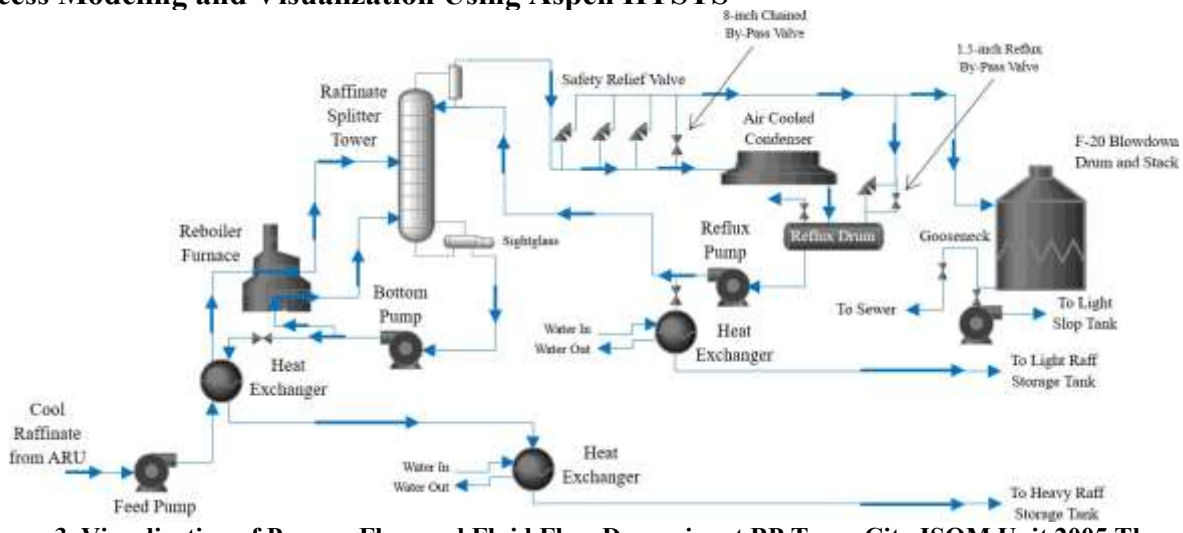

Figure 3. Visualization of Process Flow and Fluid Flow Dynamics at BP Texas City ISOM Unit 2005 Through Aspen HYSYS Simulation

The process visualization shown in the figure illustrates the complete configuration of the raffinate section of the ISOM Unit, including the raffinate splitter tower, reboiler furnace, reflux system, heat exchangers, air-cooled condenser, as well as the blowdown drum and stack. Aspen HYSYS simulation enables the entire sequence to be visualized as an integrated distillation system consisting of raffinate liquid feed input, reboiling through the reboiler, overhead cooling via the condenser, and partial flow return as reflux to maintain column stability. Under normal operating conditions, interactions among these units maintain mass and energy balance within the column. However, investigation findings indicate that on the day of the incident this balance completely failed due to procedural errors, instrumentation problems, and operational control failures—conditions that can be reconstructed through dynamic modeling in Aspen HYSYS.

During the early start-up phase, raffinate feed entered the middle section of the tower while the bottom pump discharged bottom product toward the heat exchanger and storage. In the visualization, tower inventory increases when outflow is restricted, which corresponds to actual field conditions where the bottoms level control valve remained closed for several hours. The diagram shows that a single level transmitter (LT) and sight glass were intended to monitor liquid accumulation. However, because the level transmitter had a limited measurement range and the sight glass could not be used reliably, operators received misleading level indications. Consequently, liquid accumulation inside the tower went undetected while the actual volume continued to increase beyond safe operating limits. This process corresponds to field conditions in which the liquid level in the raffinate splitter tower rose to approximately 98 feet—far exceeding the normal operating range. This condition indicates excessive liquid accumulation (liquid flooding) within the column, as described in the CSB investigation report (2007), resulting from nonfunctional bottom outflow during the start-up phase.

Thermal flow simulation further demonstrates that when the tower becomes completely filled and liquid reaches the overhead line, pressure increases progressively. The diagram presents three safety relief valves intended to maintain pressure control; however, during the actual event, relief valve activation discharged approximately 52,000 gallons of hydrocarbons into the blowdown drum and stack, clearly depicted on the right side of the schematic. In HYSYS simulation, when relief is configured to vent to the atmosphere, liquid blowdown accumulation appears as drum venting overcapacity, illustrating how this 1950s-era blowdown drum was incapable of returning liquid to the system or routing vapor to a flare.

The subsequent flow path illustrated in the figure shows vapor discharge from the drum to the atmosphere through the stack. Based on pressure and temperature conditions reconstructed by the CSB, the massive hydrocarbon release through the blowdown drum and stack resulted in the formation

of a flammable vapor cloud around the stack area, as confirmed by field investigation findings and post-incident analysis. This demonstrates that the blowdown drum design failed to comply with inherently safer design principles, particularly when compared with modern flare systems implemented in contemporary refining units.

From a process control perspective, the overhead pressure monitoring system failed to provide operators with adequate indication of flooding conditions within the column. Pressure increased gradually and was not perceived as a critical abnormal condition, leading operators to fail to recognize that the tower had entered a hazardous state. In the actual control room, operators observed only a slow pressure increase and were unable to predict that the tower had reached a critical threshold. This reflects the ineffectiveness of the control system—particularly during start-up—which can be visually demonstrated in HYSYS by displaying inflow–outflow imbalance trends that are typically not visible on conventional control panel displays.

The reflux drum, reflux pump, and air-cooled condenser shown in the figure further illustrate how overhead flow should normally be processed before partial return to the tower. However, because the tower was already fully flooded, HYSYS simulation shows that condensate could not enter the upper trays and instead contributed to pressure buildup toward the relief valves. This explains why the relief valves opened prematurely and why the blowdown drum received volumes far exceeding its design capacity.

The overall visualization using Aspen HYSYS confirms that this incident did not originate from a single point of failure but rather constituted a systemic process failure. Malfunctioning instrumentation, improper valve operation, and inadequate blowdown system design can all be visualized as unresolved mass–energy imbalances within the process. The HYSYS simulation reinforces investigative conclusions indicating that the start-up operation was conducted without adequate control, without functioning alarm systems, and without technical supervision capable of understanding the highly sensitive dynamics of distillation processes, which are strongly affected by small variations in flow and liquid level.

Accordingly, process visualization–based analysis demonstrates that the sequence of interactions among equipment shown in the raffinate splitter tower configuration—including the reboiler furnace, reflux system, heat exchangers, relief valves, and blowdown drum—served as the primary determinants in explaining how overfilling, pressure escalation, hydrocarbon release, and ultimately the formation of a flammable vapor cloud occurred (CSB, 2007).

Lesson Learned

Lessons learned from the BP Texas City explosion emphasize the necessity of mitigation efforts encompassing comprehensive improvements in technical design, operational systems, and process safety management, as recommended in the CSB Final Report. One of the most critical mitigation measures is the elimination of atmospheric blowdown drums for flammable fluids and their replacement with flare systems capable of safely containing and destroying hydrocarbon releases. The CSB concluded that open blowdown systems are inherently unsafe because they allow liquid and vapor hydrocarbons to be discharged directly into the atmosphere, thereby increasing the potential for the formation of explosive vapor clouds. Accordingly, the implementation of inherently safer design represents a primary mitigation strategy to prevent recurrence of similar scenarios.

Beyond design mitigation, the CSB report emphasizes the importance of strengthening operational control during the start-up phase, which has been identified as a high-risk operating condition. Start-up procedures must incorporate clearly defined operating limits, rigorous verification systems, and consistent implementation of pre-startup safety reviews (PSSR). Failure to ensure the proper functioning of critical instrumentation—such as level indicators and alarm systems—must not be tolerated, and operations should be suspended whenever safe operating conditions cannot be verified. Restricting non-essential personnel from process areas during start-up also represents an important mitigation measure to reduce consequences in the event of system failure.

Further mitigation measures relate to organizational and human factors. The CSB highlighted

the need to enhance operator and supervisory competence through adequate technical training, including in-depth understanding of process dynamics and abnormal operating scenarios. Management of working hours, shift-to-shift communication, and supervision during critical operations must be improved to prevent decision-making based on incorrect assumptions. At the managerial level, long-term mitigation requires transformation of safety culture by shifting focus from solely personal safety indicators toward the control of major accident hazards. Through the integrated implementation of technical, operational, and organizational mitigation measures as recommended by the CSB, the risk of major industrial accidents can be managed more effectively and sustainably (CSB, 2007).

CONCLUSION

Based on the integrated analysis conducted, this study concludes that the 2005 BP Texas City accident was not caused by a single operator error but rather constituted a systemic failure involving complex interactions among process deviations, design deficiencies, and poor safety culture. The Fault Tree Analysis (FTA) successfully mapped that the primary failure pathways were triggered by a combination of level instrumentation malfunction, operational decisions that deviated from procedures during the start-up phase, and inadequate disposal system design.

These findings are reinforced by the Layers of Protection Analysis (LOPA), which demonstrates that all defense layers—from the Basic Process Control System (BPCS) to emergency response—failed to function independently and effectively in interrupting the event sequence. Furthermore, Aspen HYSYS simulation critically visualized how mass and energy imbalance dynamics within the raffinate splitter rapidly evolved, resulting in massive liquid flooding that exceeded the capacity of the atmospheric blowdown drum.

This study recommends a paradigm shift in process safety management within the chemical industry. First, the implementation of inherently safer design principles is essential, particularly through replacing atmospheric blowdown systems with enclosed flare systems to prevent hydrocarbon releases into the working environment. Second, the start-up phase must be treated as a critical operating condition requiring strict supervision, validated instrumentation verification, and zero-tolerance procedural compliance. Third, strengthening organizational safety culture should focus on maintaining chronic unease toward process risks rather than concentrating solely on personal safety, thereby preventing the recurrence of similar tragedies in the future.

REFERENCES

Alijoyo, A., Wijaya, B., & Jacob, I. (2021). *Layers of Protection Analysis* (Analisis Lapisan Proteksi). Dalam Teknik Penilaian Risiko Berbasis ISO 31010. CRMS Indonesia.

Aminestia, T. D. (2023). Identifikasi Risiko Kecelakaan Kerja Pada Proyek Pembangunan Gedung Rumah Sakit Siti Khodijah Sidoarjo. Jurnal Vokasi Teknik Sipil, 1(1), 59-65.

Baker, J. A., III, Leveson, N., Bowman, F. L. S., Priest, S., Erwin, G., Rosenthal, I. I., et al. (2007). The report of the BP U.S. refineries independent safety review panel.

CSB (U.S. Chemical Safety and Hazard Investigation Board). (2007). BP Texas City refinery explosion and fire e Investigation report. Texas City.

Miledhiya, S. A., & Sari, D. A. (2024). Evaluasi Menara Distilasi Melalui Program Aspen HYSYS. *Sprocket Journal of Mechanical Engineering, 5*(2), 76–85.

Mogford, J. (2005). Fatal accident investigation report, isomerization unit explosion final report. Texas City.

Nurjaman, J., Agustina, S., & Kosimaningrum, W. E. (2021). Studi Analisis Risiko pada Fasilitas Pencampuran dan Pengisian di Industri Minyak Pelumas Menggunakan Integrasi HAZOP (Hazard and Operability) dengan LOPA (Layers of Protection Analysis). Jurnal Integrasi

Proses, 10(2), 109–114.
Sousa, R. et al. (2021). Advances in process plant risk assessment using FTA. Safety Science, 143, 105414.
Stempniak, R., et al. (2019). Integrating human and organizational factors into fault tree models. Process Safety and Environmental Protection, 132, 16–28.
Zarei, E. et al. (2020). Hybrid FTA–Bayesian network approach for process risk analysis. Reliability Engineering & System Safety, 199.
Zhang, L., et al. (2022). Modern developments in FTA for process safety. Process Safety Progress, 41(3).