Life Cycle Reliability and Safety Engineering
https://doi.org/10.1007/s41872-026-00400-6

CASE STUDY

STPA-FTA hybrid hazard analysis framework applied to a high integrity pressure protection system

Yasser Rehail[1] · Noureddine Tchouar[1] · Youcef Zennir[2] · Andrei Carniel[3]

Received: 28 May 2025 / Accepted: 18 February 2026
© The Author(s), under exclusive licence to Society for Reliability and Safety (SRESA) 2026

Abstract
The increasing complexity of petrochemical systems demands innovative hazard analysis methods capable of capturing both component and systemic failures. In this paper, we propose a new hazard analysis framework that integrates System-Theoretic Process Analysis (STPA) with traditional Fault Tree Analysis (FTA). Initially, STPA is applied to identify Unsafe Control Actions (UCAs) and associated loss scenarios. Subsequently, FTA is employed to model dysfunctional component behaviors and quantify critical risk metrics, including the Probability of Failure on Demand (PFDavg), Minimal Cut Sets (MCSs), and Safety Integrity Level (SIL) using GRIF software. Finally, STPA outputs are incorporated into the traditional FTA by treating UCAs as basic developed events. The framework is applied to a High Integrity Pressure Protection System (HIPPS 2351) safeguarding the C-63 distillation column at the Skikda RA1K refinery. The results revealed additional MCSs that were not discovered by the traditional FTA, which increased the number of MCSs from 8 to 39. Furthermore, the Birnbaum Importance Factor is applied to rank and prioritize UCAs, identifying the most critical UCAs (UCA 1 through UCA-15) that have a significant impact on the HIPPS 2351 reliability. Overall, the proposed framework provides a comprehensive hazard analysis covering both qualitative and quantitative aspects.

Keywords System-theoretic process analysis (STPA) · Fault tree analysis (FTA) · Unsafe control actions (UCAs) · Minimal cut sets (MCSs) · High integrity pressure protection system (HIPPS) · GRIF software

1 Introduction

The petrochemical and refinery industries involve inherently high-risk operations due to the handling of hazardous substances under extreme conditions, such as high temperatures and pressures. These conditions pose significant risks, including toxic chemical releases, explosions, and fires, which can lead to severe consequences for human life, the environment, and property (Tathod and Yadav 2024). To mitigate these risks and ensure safer operations, various methodologies have been applied since the 1960s, including Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Bow Tie (BT), Failure Modes and Effects Analysis (FMEA), and Hazard and Operability Study (HAZOP). Each of these methodologies offers unique insights into risk management.

For instance, FTA is a deductive hazard analysis method that examines all known faults and contributing events that could lead to its occurrence by starting with a top undesired event (Jiang et al. 2022). FTA involves the use of logic gates to connect the different causes that could lead to a specific top event enabling a comprehensive understanding of how the top event can occur. Numerous industries have used FTA extensively as a reliability analysis method (Giraud and Galy 2018). The FTA can be used for new or modified modeled products in all design phases to identify potential design problems. Determining minimal cut sets (MCS), or combinations of defective components that result in a particular top event, is an important element of FTA. Important information about system reliability can be gained by identifying MCSs. Binary decision diagrams (BDDs) can be used

✉ Yasser Rehail
rehailyasser6@gmail.com

[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), 31000 Oran, Algeria

[2] LAS (Laboratoire d'Automatique de Skikda), Institute of Applied Sciences and Techniques, University of 20Août 1955, 21000 Skikda, Algeria

[3] Computer Science Department, Instituto Tecnológico de Aeronáutica (ITA), São José dos Campos 12228-900, Brazil

Published online: 26 March 2026

for computing MCSs (Luo et al. 2017). In contrast, ETA follows an inductive approach, beginning with the assumption of an initial failure to determine its possible consequences (Lacasse et al. 2008). FMEA assesses the potential effects of failure modes by analyzing how individual component failures impact system performance (Lipol and Haq 2011; Larit et al. 2024). HAZOP is a process hazard analysis (PHA) method designed to identify potential deviations from intended operations and analyze the associated risks based on guide-words (Siddiqui et al. 2014). BT is a popular risk analysis method that combines aspects of FTA and ETA (Chevreau et al. 2006). The BT method is used to avoid, manage, or reduce recognized scenarios by implementing safety barriers in high-hazard industries (such as aviation, chemistry, and petrochemicals).

These methods share common limitations, they primarily consider accidents as chains of events caused by component failures, thereby oversimplifying the role of human errors. Additionally, they fall short when applied to complex systems, as they fail to identify systemic issues, software failures, and unsafe interactions between components (Leveson 2011). Nevertheless, FTA remains the most commonly used method for assessing the probability or frequency of system failures (Erdem et al. 2024; Roozbahani and Ghanian 2024; Muram et al. 2019a; Yazdi and Zarei 2018; Kim et al. 2011).

Over the last decade, researchers have explored hybrid methodologies to enhance hazard analysis by combining FTA with other qualitative techniques. One of them is HAZOP and FTA integration, which incorporates the advantages of each method. Kim et al. (2011) developed optimized codes for hydrogen fueling stations through risk analysis, including standard comparisons, leakage experiments, and safety assessments using HAZOP and FTA methodologies. In the same context, Fuentes et al. (2017) combined HAZOP and FTA methodologies to conduct a comprehensive risk analysis of a fuel storage terminal, focusing on identifying and prioritizing potential hazards and their causes. Muram et al. (2019b) developed a hazard identification and mitigation method for safety–critical quarry production systems by integrating HAZOP and FTA techniques to address individual and emergent behaviors of machines used in the quarry operations.

Another widely investigated integration is the combination of FTA and FMEA, and several studies have explored their application in industrial sectors. Kholida et al. (2024) conducted a risk assessment of work accidents at a construction project using FMEA and FTA methods to identify significant risks and their causes. Shafiee et al. (2019) proposed an integrated FTA and FMEA model, where minimal cut sets from FTA are weighted using Birnbaum's importance measure to refine Risk Priority Numbers (RPNs) in FMEA and improve risk analysis for a system of Blowout Preventer (BOP) system. In the same context, Renosori et al. (2023) combined FTA and FMEA to identify failure causes and prioritize corrective actions in toroidal inductor manufacturing, finding that worker inattention was the highest-risk factor and proposing improvements such as enhanced supervision, training, and equipment maintenance. Mutlu and Altuntaş (2019) proposed an integrated FTA and FMEA approach to analyze hazards in the ring-spinning yarn production process, identifying 57 hazard root causes, categorizing them into process, machine, and fire-related failures, and ranking risks to improve occupational health and safety.

HAZOP-FTA and FTA-FMECA combinations remain limited, particularly in complex systems where failures are highly interconnected. These approaches lack a structured methodology for identifying software errors and unintended interactions between system components that may contribute to hazardous scenarios. Additionally, in emergency cases, they fail to capture all the variability in human behavior.

Given the increasing complexity of modern process systems, risk analysis should extend beyond component failures to address software errors, controller interactions, coordination and delays in decision-making, human errors, and environmental factors. In response to these challenges, Leveson proposed the System-Theoretic Process Analysis (STPA) method as a promising alternative for hazard analysis in various domains (Siddiqui et al. 2014; Leveson and Thomas 2018).

STPA is a hazard analysis method based on system theory rather than component failure analysis that identifies unsafe control actions, systemic interactions, and dynamic behaviors within complex systems. It has been applied in several industries, including autonomous vehicles (Kholida et al. 2024; Shafiee et al. 2019; Renosori et al. 2023; Mutlu and Altuntas 2019; Leveson and Thomas 2018; Kaneko et al. 2020), automotive (Abdulkhaleq et al. 2018), aerial transportation (Fleming et al. 2013; Leveson 2004), space exploration (Ishimatsu et al. 2014), robotic surgical systems (Alemzadeh et al. 2015), autonomous vessels (Banda and Kannos 2017), autonomous ships (Rokseth et al. 2017; Chaal et al. 2020), process industry (Ishimatsu et al. 2014; Alemzadeh et al. 2015; Banda and Kannos 2017), autonomous multi-robot systems (Bensaci et al. 2021, 2023), petrochemical systems (Rehail et al. 2024), and nuclear process systems (Thomas 2013). Furthermore, several evaluations and comparisons of STPA have been performed combined with more traditional hazard analysis techniques such as FMEA and HAZOP. These studies suggest that the STPA is the most promising hazard identification method for software-intensive systems compared to traditional methods.

Several studies have compared STPA with conventional hazard analysis methods like FMEA and HAZOP. Sultana et

al. (2019) evaluated STPA against traditional hazard analysis methods like HAZOP, focusing on a specific LNG ship-to-ship transfer system. Yousefi and Rodriguez Hernandez (2019) integrated STPA with Bowtie analysis for multi-robot systems in dangerous environments. A similar comparison between STPA and Bowtie approaches for pipeline transportation hazard identification was performed by Benhamlaoui et al. (Heikkilä et al. 2023), specifically examining a condensate pipeline in the SKIKDA area. Bensaci et al. (2020) introduced STPA as a STAMP-based hazard analysis technique to aid practitioners in selecting the most suitable method for systemic hazard analysis in the process sector, highlighting its differences from traditional approaches such as HAZOP. STPA methodology is considered a viable option that may complement or substitute conventional hazard analysis methods, particularly in the process industry. Benhamlaoui et al. (2020) compared STPA and HAZOP approaches for hazard analysis of an automated container handling system. They found that both methods effectively identify risks in autonomous machinery, but noted distinctions, especially regarding their underlying accident models. Sulaman et al. (2019) demonstrated the strengths and weaknesses of FMEA and STPA techniques for identifying and mitigating potential risks in software-intensive safety–critical systems.

STPA has indeed gained significant attention from researchers in a short period due to its suitability for analyzing complex systems and its ability to identify systemic hazards beyond traditional failure-based methods. However, the original STPA remains a fully qualitative technique, lacking the ability to model and assess hazard scenarios quantitatively (Sultana et al. 2019; Bensaci et al. 2021, 2023, 2020; Rehail et al. 2024; Thomas 2013; Yousefi and Rodriguez Hernandez 2019; Heikkilä et al. 2023; Benhamlaoui et al. 2020; Sulaman et al. 2019).

To address the above limitations, we develop and apply a hybrid hazard analysis framework that combines the qualitative strengths of STPA with the quantitative capabilities of FTA. In the proposed framework, STPA is used to systematically identify Unsafe Control Actions (UCAs) and their causal scenarios, capturing software logic flaws, human interactions, and unsafe system interactions that are not represented in traditional hazard analysis methods. These STPA outputs are then explicitly incorporated into the FTA as developed basic events, enabling their inclusion in quantitative calculations. The proposed framework is applied to the High Integrity Pressure Protection System 2351 (HIPPS 2351), a type of Safety Instrumented System (SIS) designed to protect the C-63 naphtha distillation column at the Skikda RA1K refinery from overpressure risks.

The novelties of the proposed methodology can be summarized as follows:

- Provides a comprehensive framework that integrates qualitative results from STPA with quantitative metrics derived from FTA, ensuring a comprehensive framework for hazard analysis.
- Adapts the STPA method to HIPPS architectures, including redundancy and voting logics (e.g., 2oo3, 1oo2 configurations), ensuring applicability to complex industrial systems.
- Extends FTA to include software malfunctions, human errors, and complex system interactions by incorporating obtained UCAs from the STPA into the traditional FTA structure.
- Improves FTA quantification metrics such as PFDavg, SIL, and MCS.
- Prioritizes critical UCAs based on their contribution to system failure by applying The Birnbaum Importance Factor.

The remainder of this paper is structured as follows: Sect. 2 provides a background review of the STPA and FTA hazard analysis methods. Section 3 presents the proposed methodology for integrating STPA with FTA. Section 4 describes the case study of HIPPS 2351, which ensures the safety of the C-63 distillation column. Section 5 details the results of applying the related methods to the HIPPS 2351 system. Section 6 discusses the methodology, results, and opportunities. Finally, Sect. 7 presents the conclusion of this study.

2 Background

This study uses two hazard analysis methods, the System Theoretic Process Analysis (STPA) for qualitative analysis and Fault Tree Analysis (FTA) for quantitative analysis.

2.1 STPA hazard analysis method

STPA is a hazard analysis method grounded in the System-Theoretic Accident Model and Processes (STAMP) framework, developed by Leveson (2004). Unlike traditional methods that focus on preventing component failures, STPA processes safety as a dynamic control problem. It identifies potential hazards by examining all the interactions between system components and identifying each one that could lead to an unsafe state. Given the growing prevalence of automation across various domains, it has been specifically designed to analyze complex automated systems (Wu et al. 2022). STPA employs a structured, top-down approach to identify unsafe or undesired system behaviors. From the results of the analysis, requirements are generated to address these unsafe behaviors effectively (Leveson and Thomas 2018). STPA views safety as an emergent property

of systems. This perspective makes it particularly suitable for identifying potentially hazardous design flaws, including software and hardware failures, external disturbances, and improper interactions within the system's control structure. These hazards often stem from inadequate control of safety constraints during the system's design, development, or operation.

The STPA method consists of the following four steps:

Step 01: Define the purpose of the analysis

The first step is to identify the purpose of the analysis, which is to identify preventable losses at a high level. These losses may include risks, such as human life loss or broader system property risks.

Step 02: Model the control structure

A control structure is created to serve as a system model. This structure depicts the functional relationships and interactions within the feedback control loops. The emphasis then shifts to investigating the control actions contained within this structure to determine their potential contribution to the losses identified in the first step.

Step 03: Identify unsafe control actions (UCAs)

A contextual assessment is employed to identify UCAs. Within this framework, several categories of UCAs can be recognized:

- A hazard occurs when the necessary control action is provided incorrectly or not provided.
- A hazard occurs when a control action is provided incorrectly or inappropriately. A hazard results from providing the control action at the wrong time (too soon or too late).
- A hazard results from providing the control action for too long or stopping it too soon.

Step 04: Identify loss scenarios

This step allows us to identify the potential causes of unsafe control in the system. Loss scenarios illustrate how unsafe control actions may be provided but not followed or executed properly, resulting in a loss. Additionally, we identify the recommendations for each loss scenario.

2.2 FTA hazard analysis method

FTA has been adopted as a reliability tool across various industries such as nuclear power facilities, automotive systems, chemical plants, and other industrial processes to analyze and understand the relationships between events and their underlying causes within a system (Lambert 1975). The main objective of the FTA is to identify all the causes of undesirable events, as well as their combinations, and to attempt to reduce the frequency of these events and the severity of their consequences. FTA involves starting from the undesirable event and, through a deductive process, searching for the immediate causes of this event. The process starts with a top undesired event and systematically examines all recognized events and failures that might cause or contribute to the occurrence of the Top Event (TE) using logical gates (e.g., AND-gate, OR-gate, etc.) (Bujna et al. 2023). We distinguish between qualitative FTA, which takes into account the structure of the FTA, and quantitative FTA, which computes quantitative calculations like the top event frequency.

Quantitative FTA involves calculating the Probability of Failure on Demand average (PFDavg) or the frequency of the TE occurrence. To quantify the probability of the top event in FTA, it is essential to consider several parameters including the failure rate (λ) which represents the probability of failure per unit of time for each BE and is crucial for estimating the PFDavg of the TE, the Mean Time to Repair (MTTR) and periodic test (T) for each equipment within the studied system, and the Beta Factor (β), which accounts for Common Cause Failures (CCF), where multiple components fail simultaneously due to a shared root cause (Dibaei et al. 2023). The general formula for PFDavg is expressed as:

$$PFD_{Avg} = \frac{1}{T}\int_0^T Q\,(t)\,dt \tag{1}$$

In the context of redundant architectures, the total unavailability Q(t) is divided into two components:

1. Independent Failures: Failures that occur randomly and independently across components.
2. Common Cause Failures (CCF): Failures where multiple components fail simultaneously due to a shared root cause.

The total unavailability is calculated as:

$$Q\,(t) = ((1-\beta) \times Q_{Independent}\,(\mathrm{t})) + (\beta \times Q_{CCF}\,(\mathrm{t}) \tag{2}$$

Where β: The Beta Factor, representing the fraction of failures attributed to common cause failures ($0 \leq \beta \leq 1$). $Q_{\mathrm{Independent}}\,(\mathrm{t})$: Unavailability due to independent failures. $Q_{CCF}\,(\mathrm{t})$: Unavailability due to common cause failures.

For independent failures, the unavailability is modeled using the Full Periodic Test Law with exponential failure distribution:

$$Q_{Independent}\,(\mathrm{t}) = \frac{\lambda_{\mathrm{D}}}{\lambda_{\mathrm{D}}+\mu}\left(1-\mathrm{e}^{-(\lambda_{\mathrm{D}}+\mu)\mathrm{t}}\right) \tag{3}$$

where λ_D: Dangerous failure rate (failures per hour). μ: Repair rate (repairs per hour). t: Elapsed time since the last test or repair.

For common cause failures (CCF), the unavailability is modeled using the Full Periodic Test Law with exponential failure distribution:

$$Q_{CCF}(\mathrm{t}) = \frac{\lambda_D \times t}{n} \tag{4}$$

where n: Total number of redundant components.

Another crucial aspect of understanding fault tree behavior is the determination of minimal cut sets (MCSs). By examining these minimal combinations, engineers can pinpoint the most vulnerable parts of the system and prioritize improvements. Determining the MCSs that result in a particular top event is essential for simplifying the fault tree and directing quantitative analysis (Giraud and Galy 2018). Several techniques, such as the application of Binary Decision Diagrams (BDDs), have been proposed for computing MCSs (Luo et al. 2017). Since a minimal cut set is an intersection of BEs, the probability of a minimal cut set is simply the product of the individual BE probabilities. Thus, the probability of the top event is expressible as the sum of the products of individual BE probabilities. Mathematically, the probability of the top event is given by:

$$P_{TopEvent} = \sum P_{cutset} \tag{5}$$

where each cut set probability is calculated as:

$$P_{cutset} = P(BE_1) \times P(BE_2) \times \cdots \times P(BE_n) \tag{6}$$

This method provides an efficient and reliable estimation of system failure probability, especially when the basic event probabilities remain below 10E-1. In cases where system components are repairable, unavailability calculations provide a more accurate measure of system reliability over time.

3 Methodology description

This section presents the proposed framework composed of three main steps as depicted in Fig. 1.

In the first phase, we employ the STPA to identify UCAs and their associated causal scenarios that may lead to the failure of HIPPS 2351. Unlike FTA, this step is not limited to hardware malfunctions and explicitly captures unsafe control logic, timing errors, software-related issues, and human–system interaction hazards that may occur even when system components are functioning correctly.

In the second phase, we employ the FTA to quantify the failure of HIPPS 2351 based on hardware-related failures of sensors, logic solver, and final elements. Component failure rates are used to quantify the system behavior and to compute the PFDavg, MCSs, and determine the corresponding SIL.

In the final phase, we integrate the STPA findings into the traditional FTA by incorporating the identified UCAs as developed basic events at the lowest level of the fault tree,

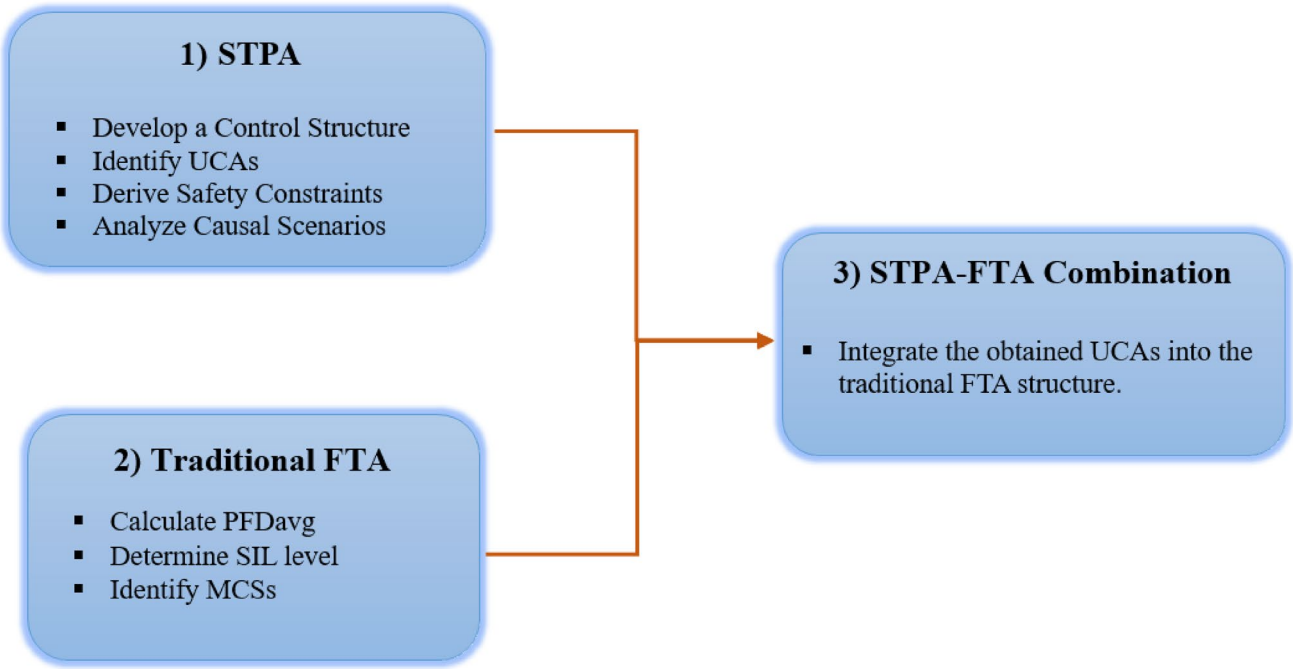


Fig. 1 Proposed framework for comprehensive hazard analysis

under the relevant intermediate events. Each UCA is introduced as an alternative failure pathway, allowing unsafe control behavior to be quantitatively assessed alongside conventional hardware failures. Following this integration, the PFDavg and SIL are recalculated, and the MCS analysis is expanded to include additional failure pathways that are not captured by traditional FTA alone. Furthermore, the Birnbaum Importance Factor is applied to rank the UCAs based on their contribution to HIPPS 2351 failure, enabling the identification and prioritization of the most safety–critical unsafe control actions.

4 Case study

The High Integrity Pressure Protection System (HIPPS) is a reactive barrier designed following the IEC 61508, and IEC 61511 standards to stop or mitigate the consequences of the chain events following a hazardous situation, it is one of the best choices to protect the plants and to increase safety. A specific combination of one or more input components (such as sensors and transmitters), one or more logic solvers (such as programmable logic controllers [LS]), and one or more end elements (such as safety valves) makes up a Safety Instrumented System (SIS), as shown in Fig. 2. HIPPS is a type of SIS operating in low-demand mode, this ensures the section's automatic total stop to minimize the overpressure risk.

The HIPPS 2351 installed in the C-63 distillation column, located in Splitter-I at Topping Unit 10 of the Skikda refinery, Algeria, is a critical safety barrier designed to prevent overpressure scenarios (Fig. 3).

The C-63 column operates under controlled conditions to ensure safe naphtha separation. When the pressure exceeds established safety limits, the system responds quickly to control it, often by rapidly closing specific valves or implementing other control measures to prevent overpressure scenarios. To mitigate overpressure scenarios, HIPPS 2351 continuously monitors pressure levels within the C-63 column and automatically intervenes when safety limits are exceeded. The system responds by rapidly closing the UV 2353 and UV 2356 valves and opening the TV 2351 valve. Figure 4 (Rehail et al. 2024) presents the HIPPS 2351 configuration.

- The sensor layer comprises three identical pressure transmitters arranged in a 2oo3 configuration.
- The logic solver layer, named LS 2351, is set up in a 1oo1 configuration.
- The final element layer incorporates three valves: two for isolation (UV 2353 and UV 2356) and one for control (TV 2351). The control valve is organized in a 1002 configuration with the isolation valves, while the isolation valves themselves are set up in a 2oo2 configuration.

The pressure transmitters PT 2351 A/B/C monitor the liquid pressure within the C-63 column and send this information to LS2351. Subsequently, LS 2351 treats and transmits the received signals to close UV 2353 and UV 2356, while simultaneously opening TV 2351.

5 Application and results

This section presents the application and results of the proposed STPA-FTA methodology for HIPPS 2351. Section 5.1 details the STPA results, including the identification of UCAs, loss scenarios, and safety constraints. Section 5.2 presents the FTA results, covering the PFDavg, MCSs, and SIL determination. Finally, Sect. 5.3 discusses the integration of STPA into FTA, where UCAs are incorporated as basic events.

5.1 STPA of the HIPPS 2351 system

The hazard analysis of the HIPPS 2351 system using the STPA method follows a structure of four steps:

- Step 1: Define the purpose of the analysis

The primary goal of the analysis is to identify and evaluate potential losses associated with the operation of HIPPS

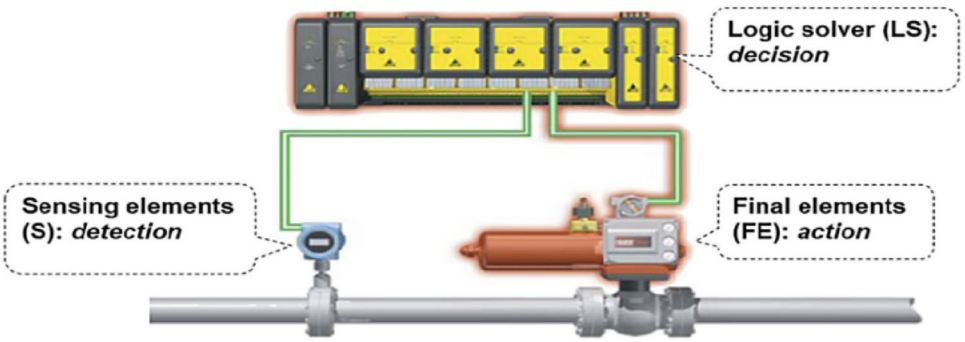


Fig. 2 Typical SIS configuration (IEC 2010)

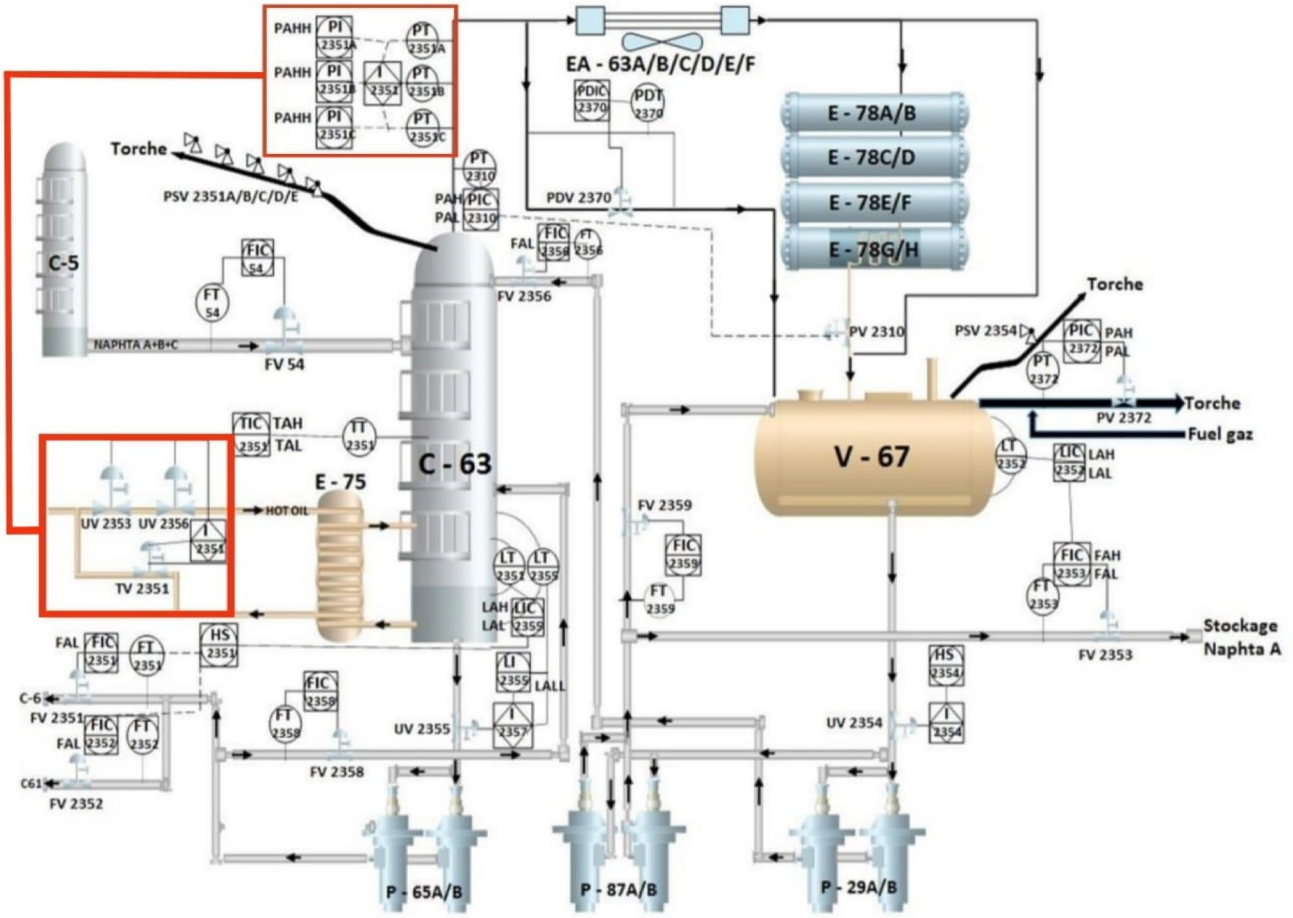


Fig. 3 Simplified diagram of C-63 column (Ayachi et al. 2018)

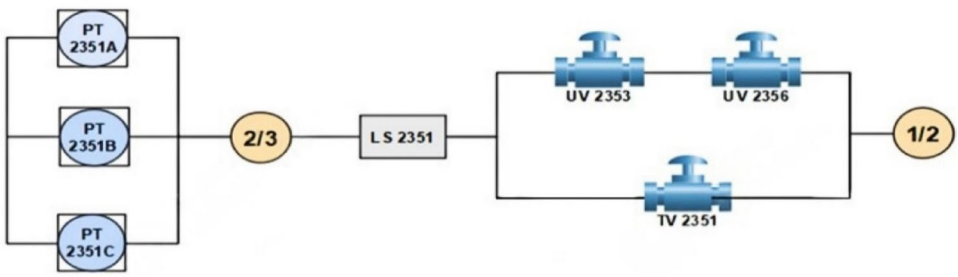


Fig. 4 Configuration of the HIPPS 2351 (Rehail et al. 2024)

2351. In accordance with Step 1 of the STPA methodology, potential losses were identified by defining system-level accidents associated with the failure of HIPPS 2351. The following losses have been identified for the system:

- L-1: Unavailability of HIPPS 2351.
- L-2: Loss of naphtha due to release into the atmosphere.
- L-3: Damage or loss of the column (C-63).
- L-4: Environmental damage.
- L-5: Loss of human life.
- L-6: Loss of reputation.

The resulting losses (L1–L6) represent unacceptable system-level outcomes and form the basis for identifying hazards and safety constraints in subsequent STPA steps (Leveson and Thomas 2018). By systematically identifying these losses, the analysis provides a comprehensive understanding of the potential risks related to the C-63. This understanding is a foundation for developing and implementing effective risk mitigation strategies, including enhancements to the HIPPS 2351 system. These strategies aim to improve the safety and reliability of the distillation process.

Table 1 details the high-level system hazards associated with overpressure scenarios in the C-63 column, offering

Table 1 High-level system hazards

System level accident	High-level system hazards
Overpressure in C-63	H1: high pressure in the C-63 column due to HIPPS 2351 failure. [L-1, L-2, L-3, L-4, L-5, L-6] H2: high temperature in the C-63 column due to HIPPS 2351 failure. [L-1, L-2, L-3, L-4, L-5, L-6]

further insight into the risks and constraints that need to be managed for effective hazard control.

High-level safety constraints are also identified:

SC 1: The HIPPS 2351 should prevent the Pressure in the C-63 column from exceeding a defined limit. [H-1, H-2]

SC 2: The HIPPS 2351 should prevent the Temperature in the C-63 column from exceeding a defined limit. [H-1, H-2]

- Step 2: Model the control structure

The second step in the STPA process involves creating a detailed model of the hierarchical control structure for the HIPPS 2351 system. This control structure provides a comprehensive representation of the system's functional relationships and interactions within its feedback control loops. The control structure presents how commands, signals, interactions, and feedback occur between system components, such as pressure transmitters, the logic solver, valves, and operator actions. Additionally, this step presents the interactions between operators and manual actions, which can influence system behavior and introduce HIPPS 2351 failure. This modeling helps to identify potential points of failure or unsafe interactions that could lead to hazardous scenarios. Figure 5 illustrates the control structure for the HIPPS 2351 system, outlining the key components and their interdependencies within the operational framework. This visual representation forms the foundation for identifying UCAs in the subsequent analysis steps. To ensure a systematic and thorough analysis, we consider feedback mechanisms and different types of control actions. The control action types are listed below:

- *Controls/Commands*: Actions that explicitly instruct a system component to perform a function. For example, the Logic Solver (LS 2351) sends signals to open TV 2351 or close UV 2353 and UV 2356 valves to regulate column pressure.
- *Component Interactions*: Exchanges of information between components without explicit commands, such

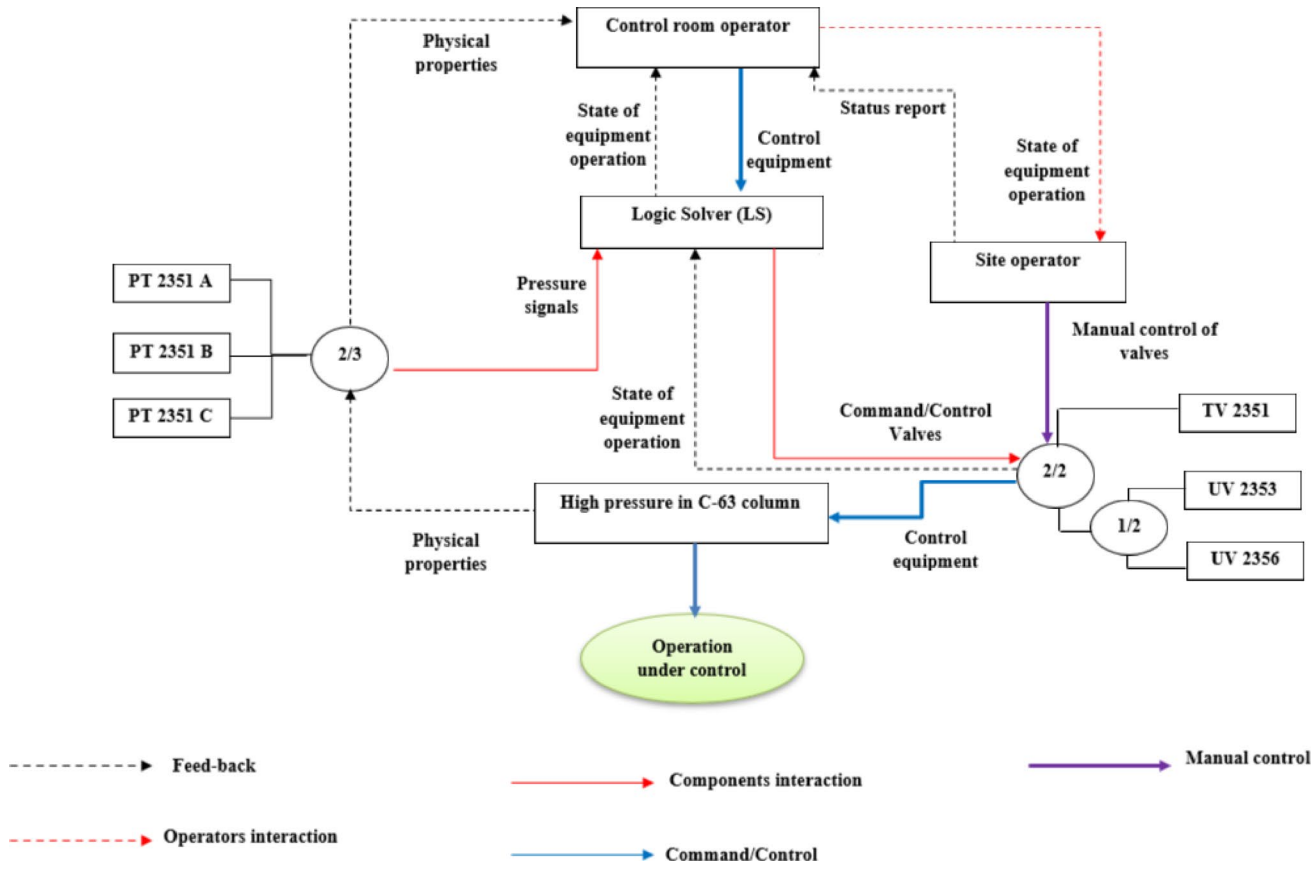


Fig. 5 High-level control structure of HIPPS 2351

as the transmitters layer (PT 2351 A/B/C) transmitting pressure signals to LS 2351.

- *Operator Interactions*: Control room operators communicate with site operators to directly manipulate valve positions.

- *Manual Control*: Direct human control actions that can override automated responses, providing an additional layer of safety in the system. In our HIPPS 2351 system the site operator closes UV 2353 and 2356 and opens TV 2351 when the pressure in the column gets too high if the LS 2351 fails to actuate the valves.Step 3: Identify Unsafe Control Actions

After modeling the control structure, the next step in the STPA is to identify UCAs that could lead to hazardous scenarios. UCAs are actions that either occur incorrectly, fail to occur when needed, are provided too early or too late, or continue for too long or stop too soon, thereby violating system safety constraints. For this study, the UCAs for the HIPPS 2351 system were systematically identified and are summarized in Table 7 of Appendix 1. These UCAs highlight potential points of failure or unsafe interactions across key components, such as pressure transmitters (PT 2351), the logic solver (LS 2351), control valves (TV 2351), isolation valves (UV 2353 and UV 2356), and operator actions. Identifying these unsafe actions enables the development of safety constraints and recommendations to address the associated risks effectively.

Following the identification of UCAs, the next step involves establishing Controller Constraints, which are detailed in Table 8 of Appendix 1. These constraints are directly tied to the identified UCAs and serve as safeguards to limit or regulate control actions, preventing unsafe outcomes and ensuring the system operates within defined safety boundaries. Controller constraints are designed to mitigate the risks posed by UCAs by addressing issues such as improper timing, absence of required actions, or the continuation of actions beyond acceptable durations.

- Step 4: Identify Loss Scenarios

The final step in the STPA process involves identifying potential loss scenarios associated with the previously identified UCAs (Wu et al. 2022). These loss scenarios are outlined in Table 9 of Appendix 1, and provide detailed insights into how command failures, feedback delays, and unsafe interactions could lead to hazardous outcomes. By analyzing these scenarios, the relationships between control system vulnerabilities and potential hazards become clear, enabling the development of targeted mitigation strategies to address these risks effectively.

Table 2 Input data (Hauge et al. 2013)

Components	λ_D (h^{-1})	MTTR (h)	B (%)	T(h)
PT 2351 A/B/C	8E-7	8	4%	8760
TV 2351	4.4E-6	8	–	26,280
UV 2353/UV 2356	1.1E-8	8	3%	26,280

5.2 FTA of the HIPPS 2351 system

The Probability of Failure on Demand average (PFDavg) is an important metric for assessing the reliability of HIPPS. It represents the likelihood that a system fails to perform its intended function when required. In GRIF software (Workshop 2023), the Albizia computation engine calculates the PFDavg by averaging the HIPPS 2351 unavailability (Q(t)) over the entire test period (T). The reliability data for the HIPPS 2351 are provided in Table 2. The supplier has determined the PFDavg value of the LS 2351 to be 5E-4, which corresponds to SIL 3. This analysis is conducted over a mission time of 25 years.

The HIPPS 2351 implementation using FTA is presented in Fig. 6. The FTA shows several events that could lead to the failure of 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.

To calculate the PFDavg of the undesirable event (HIPPS 2351 Failure), we use the Tree module of the GRIF software (Workshop 2023). Figure 7 illustrates the PFD(t) variation over time for the HIPPS 2351 system. The obtained PFDAvg value is 5.69E-2, corresponding to a SIL 1 rating according to IEC 61508 standards.

The FTA yielded 8 minimal cut sets (Table 3). The identified cut sets mean that there are 8 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.

Based on the analysis of Table 3, the critical component of the HIPPS 2351 system is TV 2351. Its independent failure has the highest probability of 1.091E-1. This high probability indicates that TV 2351 failure is a single point of failure that could lead to the failure of the entire system if it malfunctions. Enhancing the reliability of TV 2351 through measures such as implementing a redundant configuration (e.g., 2002 architecture) or improving fault tolerance would significantly reduce the overall PFDavg of HIPPS 2351. Other critical contributors include the CCFs of the pressure transmitters (PT 2351 A/B/C) and the isolation valves (UV 2353 and UV 2356).

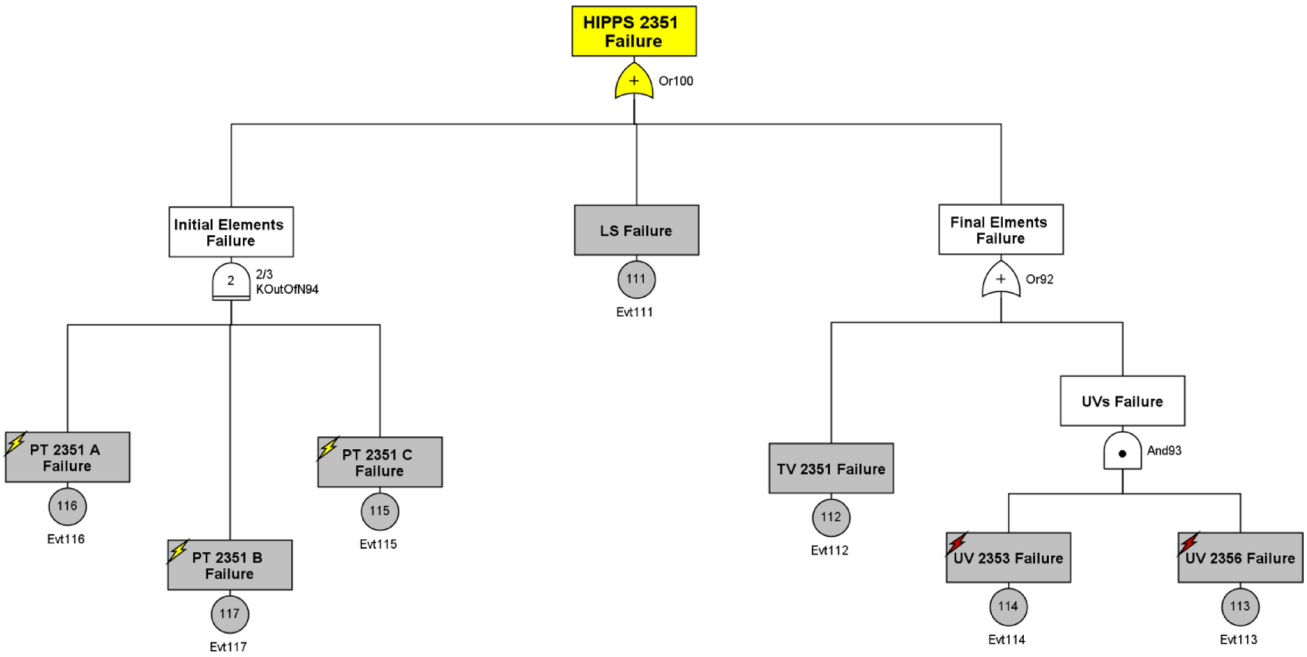


Fig. 6 FTA for HIPPS 2351 failure

Fig. 7 PFD(t) of the HIPPS 2351

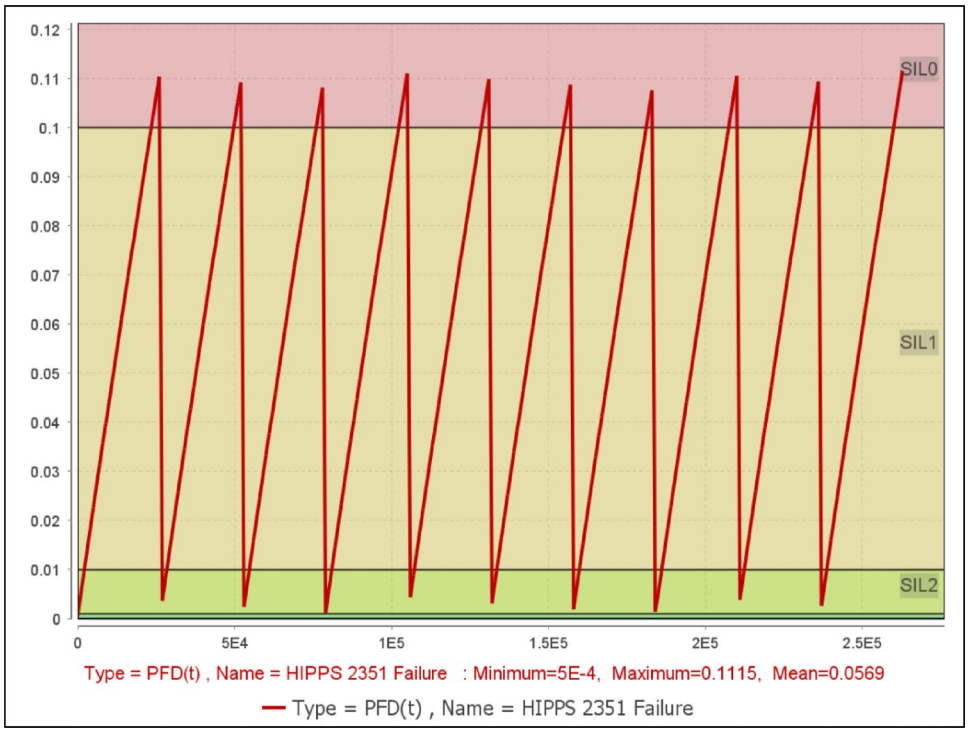
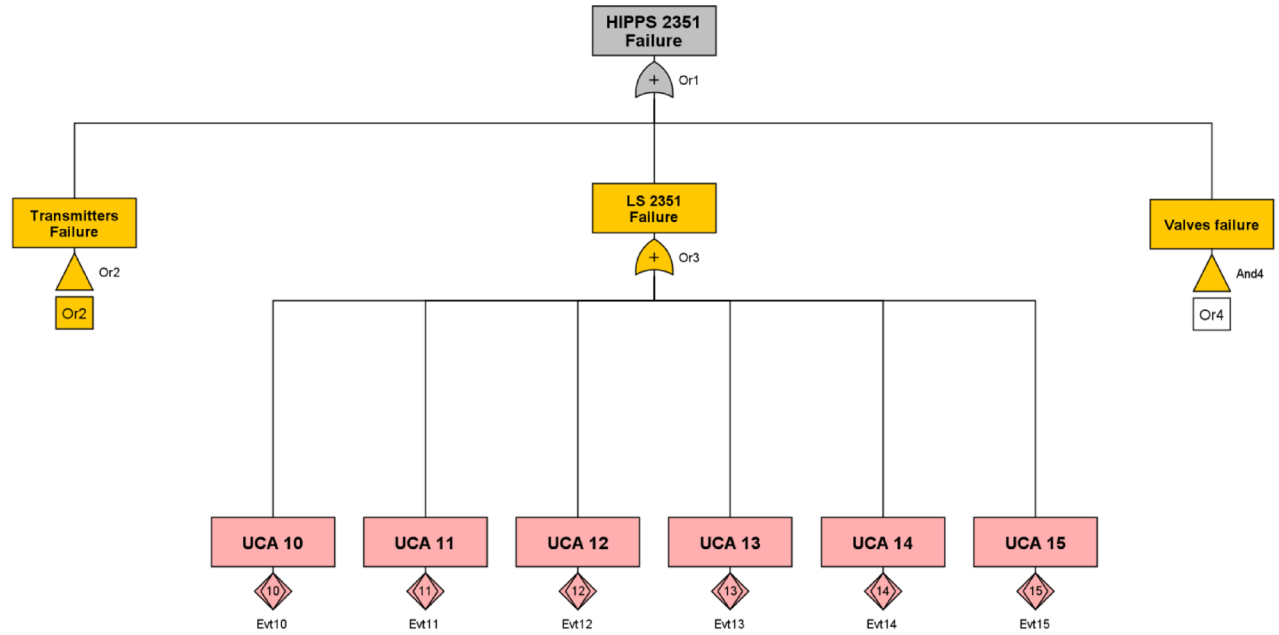


Table 3 MCSs of HIPPS 2351 system failure

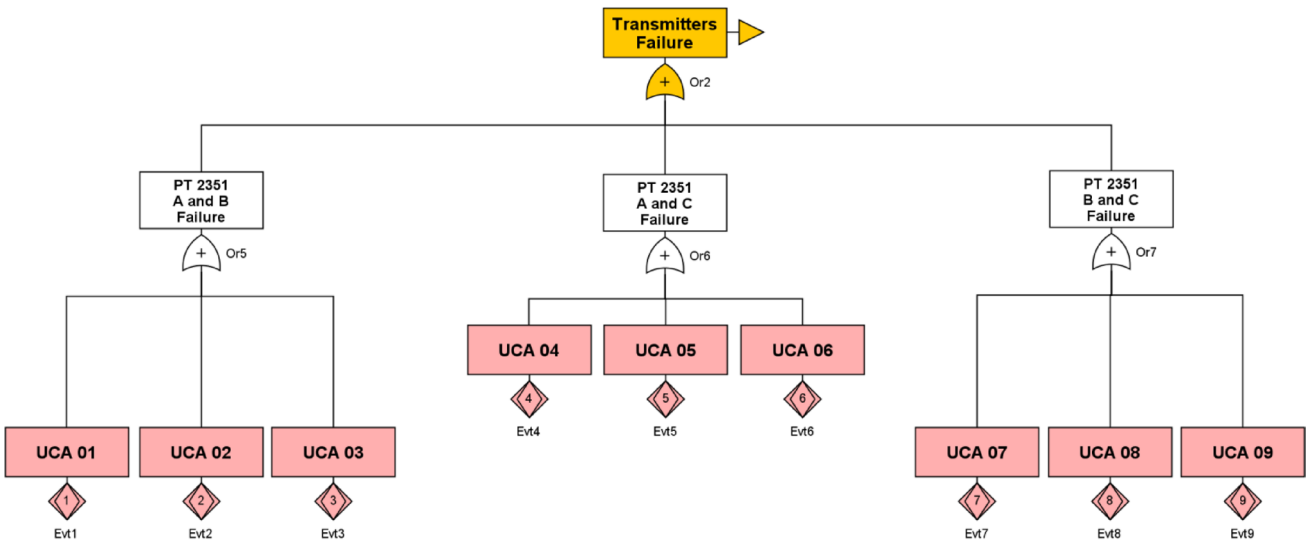
System	Order	Cut set	Probability (Cut Set)
HIPPS 2351	1	LS 2351 Failure	5E-4
	1	**TV 2351 Failure**	**1.091E-1**
	1	CCF (PT)	2.8028E-4
	1	CCF (UV)	8.6668E-4
	2	PT 2351 A, PT 2351B	4.4958E-5
	2	PT 2351 A, PT 2351C	4.4958E-5
	2	PT 2351 B, PT 2351C	4.4958E-5
	2	UV 2353, UV 2356	7.6458E-4

5.3 STPA-FTA combination for a complete hazard analysis

STPA findings are integrated into the traditional FTA model by incorporating UCAs as basic events (BEs) within the FTA structure. The new FTA structure covers not only component failures but also extends the analysis to capture software failures, component interactions, and human errors, as shown in Fig. 8.

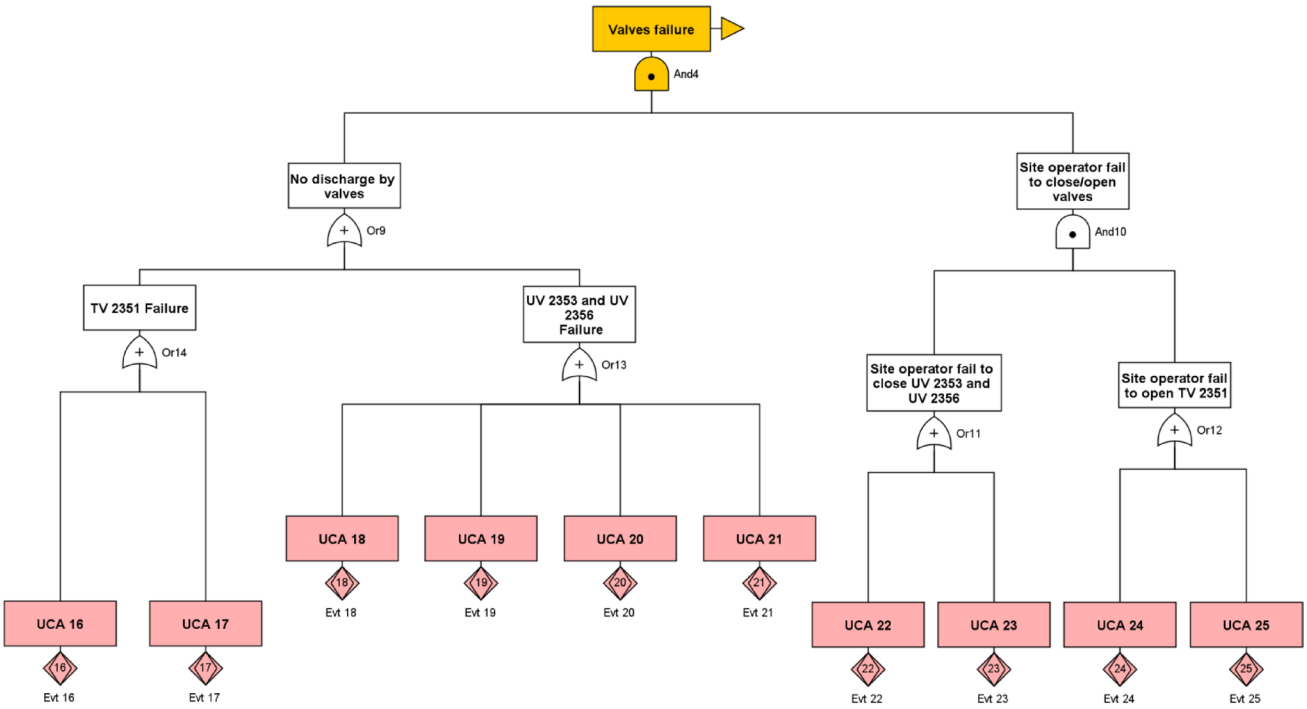


(a)



(b)

Fig. 8 New FTA Structure for the STPA-FTA combination (**a**) New FTA Structure for the STPA-FTA combination (**b**). New FTA Structure for the STPA-FTA combination (**c**)



(c)

Fig. 8 (continued)

Following the integration of UCAs into the FTA structure, the revised model was analyzed using GRIF software to obtain an updated PFDavg. The resulting PFDavg for the HIPPS 2351 is 8.8354E-3 which corresponds to SIL 2 following the IEC 61508 standard (Fig. 9).

The new FTA reveals 39 distinct minimal cut sets (15 with order 1, and 24 with order 3), each MCS represents a potential failure pathway that could lead to the HIPPS 2351 failure which can result in an overpressure scenario in Column C-63, as presented in Table 4.

Table 4 indicates that the Unsafe Control Actions associated with LS 2351 namely, UCA 10, UCA 11, UCA 12, UCA 13, UCA 14, and UCA 15 emerge as MCSs with an individual failure probability of 5E-4. These UCAs highlight vulnerabilities in the operation of LS 2351. Their high probability emphasizes that any deviation in the performance of the LS 2351 can significantly compromise the

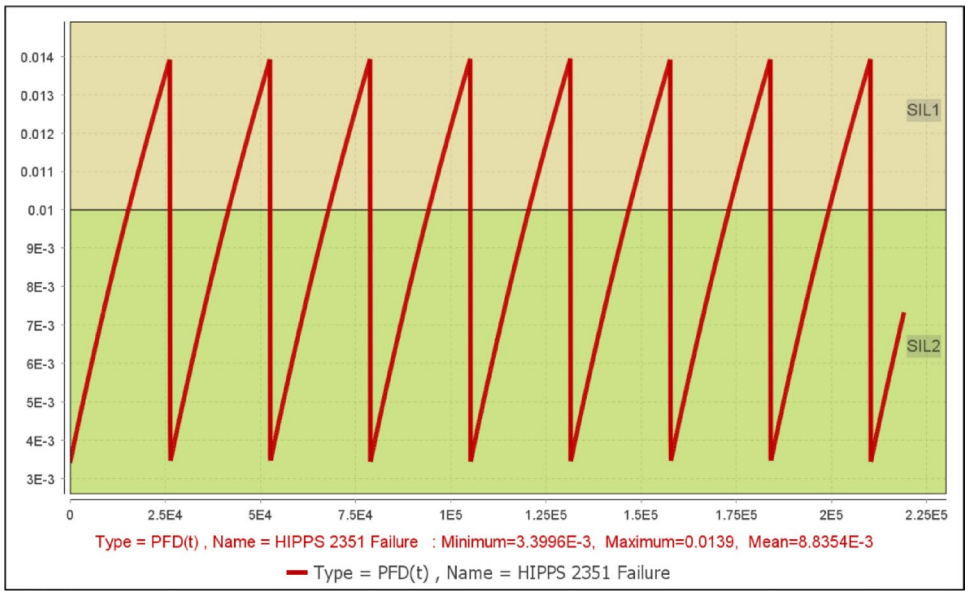


Fig. 9 Updated PFD(t) of the HIPPS 2351 after including STPA outputs in the FTA structure

Table 4 MCSs of HIPPS 2351 system failure identified by the Revised FTA

System	Order	Minimal cut set (MCS)	Probability (cut set)
HIPPS 2351	1	UCA 1	4.4958E-5
	1	UCA 2	4.4958E-5
	1	UCA 3	4.4958E-5
	1	UCA 4	4.4958E-5
	1	UCA 5	4.4958E-5
	1	UCA 6	4.4958E-5
	1	UCA 7	4.4958E-5
	1	UCA 8	4.4958E-5
	1	UCA 9	4.4958E-5
	1	**UCA 10**	**5E-4**
	1	**UCA 11**	**5E-4**
	1	**UCA 12**	**5E-4**
	1	**UCA 13**	**5E-4**
	1	**UCA 14**	**5E-4**
	1	**UCA 15**	**5E-4**
	3	UCA 16, UCA 22, UCA 24	3.78106E-4
	3	UCA 17, UCA 22, UCA 24	3.78106E-4
	3	UCA 16, UCA 22, UCA 25	3.78106E-4
	3	UCA 17, UCA 22, UCA 25	3.78106E-4
	3	UCA 16, UCA 23, UCA 24	3.78106E-4
	3	UCA 17, UCA 23, UCA 24	3.78106E-4
	3	UCA 16, UCA 23, UCA 25	3.78106E-4
	3	UCA 17, UCA 23, UCA 25	3.78106E-4
	3	UCA 21, UCA 22, UCA 24	9.58972E-5
	3	UCA 20, UCA 22, UCA 24	9.58972E-5
System	Order	Minimal cut set (MCS)	Probability (cut set)
HIPPS 2351	3	UCA 19, UCA 22, UCA 24	9.58972E-5
	3	UCA 18, UCA 22, UCA 24	9.58972E-5
	3	UCA 19, UCA 22, UCA 24	9.58972E-5
	3	UCA 21, UCA 22, UCA 25	9.58972E-5
	3	UCA 20, UCA 22, UCA 25	9.58972E-5
	3	UCA 19, UCA 22, UCA 25	9.58972E-5
	3	UCA 18, UCA 22, UCA 25	9.58972E-5
	3	UCA 21, UCA 23, UCA 24	9.58972E-5
	3	UCA 20, UCA 23, UCA 24	9.58972E-5
	3	UCA 19, UCA 23, UCA 24	9.58972E-5
	3	UCA 18, UCA 23, UCA 24	9.58972E-5
	3	UCA 21, UCA 23, UCA 25	9.58972E-5
	3	UCA 20, UCA 23, UCA 25	9.58972E-5
	3	UCA 19, UCA 23, UCA 25	9.58972E-5
	3	UCA 18, UCA 23, UCA 25	9.58972E-5

ability of HIPPS 2351 to prevent overpressure scenarios in the C-63 column.

Sensitivity analysis is performed using the Birnbaum Importance Factor (also referred to as the Marginal Importance Factor, MIF). The Birnbaum measure quantifies the sensitivity of the top event probability (HIPPS 2351 failure) to variations in the failure probability of individual basic events, including UCAs. A higher Birnbaum importance value indicates that a small improvement or degradation in the reliability of that event will result in a relatively large change in the top event probability. This metric is selected because it directly measures how the failure probability of each UCA influences the PFDavg of HIPPS 2351 Failure as shown in Table 5. In our integrated STPA-FTA approach, where UCAs are developed and incorporated as basic developed events in the fault tree, Birnbaum Importance Measure enables us to address the most critical UCAs, thereby enhancing the overall reliability of the HIPPS 2351.

The MIF rankings in Table 5 highlight a clear hierarchy of UCAs regarding their impact on overall HIPPS 2351 reliability. The LS 2351 and the pressure transmitters (PT 2351 A/B/C) exhibit higher MIF values, indicating that UCAs from 1 through 15 are the most vulnerable UCAs of the HIPPS 2351. In contrast, the valves (UV 2353, UV2356, and TV 2351) failure and the failure of the site operator to take action on them have lower MIF values, indicating that UCAs from 16 to 25 have a more limited influence on the HIPPS 2351 failure.

The above findings from the combined approach STPA-FTA allow us to rank the Safety recommendations. These recommendations are prioritized according to the failure probabilities calculated by the traditional FTA. Table 6 presents the prioritized safety recommendations.

6 Result discussion

The results of our integrated STPA-FTA approach provide a comprehensive perspective on the hazards and vulnerabilities of the HIPPS 2351 system, revealing both the component failures and the systemic failures that traditional methods alone often overlook. STPA findings are integrated into the traditional FTA model by incorporating UCAs as basic events within the fault tree structure. Following this combination, the PFDavg, SIL, and MCSs are recalculated to assess the influence of the implemented UCAs in the FTA structure.

(a) STPA Analysis Outcomes

The STPA application defined 23 UCAs and 72 associated loss scenarios. This qualitative analysis exposed a wide range of potential hazards arising from not only hardware failures but also from human errors, software malfunctions, and unsafe interactions among system components.

(b) Traditional FTA results

The traditional FTA primarily focused on hardware failure probabilities, calculated a PFDavg of 5.69E-2 over a 25-year mission time, corresponding to SIL 1 according to the IEC

Table 5 Ranking UCAs using the Birnbaum importance measure

Type = MIF, System = HIPPS 2351 fails		
Intermediate event	**UCA**	**Value**
PT 2351 A and B failure	UCA1, UCA2, UCA3	9.927E-1
PT 2351 A and C failure	UCA4, UCA5, UCA6	9.927E-1
PT 2351 B and C failure	UCA7, UCA8, UCA9	9.927E-1
LS 2351 Failure	UCA10, UCA11, UCA12, UCA13, UCA14, UCA15	9.932E-1
TV 2351 Failure	UCA16, UCA17	3.33E-2
UV 2353 and UV 2356 Failure	UCA18, UCA19, UCA20, UCA21	3.24E-2
The site operator fails to close UV 2353 and UV 2356	UCA22, UCA23	1.86E-2
The site operator fails to open TV 2351	UCA24, UCA25	1.86E-2

61508 standard. Moreover, eight MCSs were identified, which highlighted different failure combinations leading to the HIPPS 2351 failure. TV 2351 was identified as the critical component due to its relatively high failure probability of 1.091E-1. Other significant contributors were the CCFs of the pressure transmitters (PT 2351 A/B/C) and isolation valves (UV 2353/UV 2356). These results underscored the importance of robust design and redundancy for the valves and transmitters to reduce the PFDavg of the HIPPS 2351.

(c) Combining STPA with FTA

By integrating STPA outputs into the traditional FTA through incorporating UCAs as basic developed events within the fault tree structure, we expanded the fault tree to include component failures and systemic vulnerabilities such as software errors, control delays, and operator errors. In the revised FTA model, each UCA was developed as a basic event based on its corresponding causal scenarios identified through STPA. This integration led to several significant improvements in the hazard analysis:

- Updating PFDavg and SIL

The combination produced an updated PFDavg of 8.8354E-3 using the GRIF software. This marked a substantial improvement over the initial analysis, improving the SIL from SIL 1 to SIL 2. The observed SIL improvement reflects an analytical outcome of the revised fault tree model and represents a theoretical potential for risk reduction, rather than a change to the certified SIL of the existing HIPPS 2351 installation.

- Expanding MCSs

The new FTA model identified 39 distinct MCSs, 15 single-failure (order 1) and 24 triple-failure (order 3). These MCSs represent. Notably, the integration of UCAs revealed additional pathways that were not discovered by the traditional FTA. For instance, UCAs associated with LS 2351 (UCA 10 through UCA 15) emerged as the critical MCSs within the HIPPS 2351, highlighting the significant influence of LS 2351 on overall system safety.

- UCAs ranking through the Birnbaum importance measure

The application of the Birnbaum Importance Measure provided a quantitative basis for ranking the UCAs. Our analysis in Table 5 showed that UCAs related to LS 2351 and the pressure transmitters (PT 2351 A/B/C) have the highest MIF values (UCA 1 through UCA-15). This indicates that even slight improvements in the reliability of these UCAs can lead to significant reductions in the overall PFDavg of the HIPPS 2351. In contrast, UCAs associated with valve failures and operator interventions exhibited lower MIF values, suggesting a limited influence on the PFDavg of the HIPPS 2351.

Table 6 STPA-FTA recommendations

	Recommendations
1	Add a redundant valve, diverse in design and function from TV 2351, to serve as a backup. This will ensure continued system operation if TV 2351 fails. The redundant valve should have its own independent control logic
2	Verify that the valve functions are defined correctly in the design, i.e. TV 2351 does not open when pressure is high in the column or UV 2353 and UV 2356 do not open when the pressure is high
3	Verify that the valves closing/opening time is short enough to ensure C-63 column is off from the upstream liquid source, preventing the pressure in the column from increasing any further
4	Implement a redundant logic solver (e.g., 2oo2 architecture), Since LS 2351 has the highest failure probability, introducing redundancy significantly reduces the risk of a single-point failure
5	Ensure the set point for PT 2351 A/B/C transmitters is correctly established during the design phase
6	Incorporate Heterogeneous Components for transmitters (PT 2351 A/B/C) and valves (UV 2353/UV 2356) to Reduce Common Cause Failures (CCFs)
7	Perform regular calibration and validation of the PT 2351 A/B/C to ensure accurate pressure detection
8	Conduct monthly partial stroke tests on TV 2351, UV 2353, and UV 2356 to ensure they close properly when signaled
9	Define and implement adequate maintenance (preventive and corrective) and calibration programs for transmitters, logic solver, and final elements to ensure correct detection, prevent faulty alarms, and prevent malfunctioning of the HIPPS 2351
10	Conduct proof testing every six months for valves and pressure transmitters
11	Establish robust communication protocols between control room operators and site operators
12	Ensure operators are competent in operating the plant (develop and implement a competency assurance system for operators)

7 Conclusion

This study presents a novel hybrid framework integrating System-Theoretic Process Analysis (STPA) and Fault Tree Analysis (FTA) to address the limitations of traditional hazard analysis methods in safety–critical systems. By applying this methodology to the High Integrity Pressure Protection System (HIPPS 2351) at the C-63 distillation column in the Skikda RA1K refinery, we demonstrate its efficacy in capturing systemic and component-level risks.

The STPA analysis identified 23 unsafe control actions (UCAs) and 72 loss scenarios, revealing critical vulnerabilities arising from human errors, software malfunctions, and unsafe interactions often overlooked by traditional FTA methods. Meanwhile, the traditional FTA determined a PFDavg of 5.69E-2, corresponding to a Safety Integrity Level 1(SIL 1) according to the IEC 61508 standard. Furthermore, the FTA identified eight minimal cut sets (MCSs). The FTA also pinpointed the TV 2351 as a critical single-point failure with the highest probability of failure (1.091E-1), emphasizing the need for redundancy (e.g., a 1002 architecture) to reduce the PFDavg of the HIPPS 2351 and enhance its reliability. Additionally, common-cause failures (CCFs) among pressure transmitters (PT 2351 A/B/C) and isolation valves (UV 2353 and UV 2356) were identified as major contributors to overall HIPPS 2351 unavailability, emphasizing the necessity for diverse component designs and improved maintenance strategies.

The integration of STPA findings into FTA enriched the fault tree model by systematically mapping UCAs as basic developed events, allowing for a more comprehensive representation of failure pathways. The study expanded the failure analysis to incorporate interactions between system components, operator actions, and software logic flaws in the HIPPS 2351. This integration resulted in the improvement of SIL from SIL 1 to SIL 2. The integration of UCAs revealed additional MCSs that were not discovered by the traditional FTA extending the MCSs from 8 to 39 where the UCAs associated with LS 2351 (UCA 10 through UCA 15) emerged as the critical MCSs within the HIPPS 2351. The use of MIF to rank UCAs allowed us to identify critical UCAs within the HIPPS 2351 (UCA 1 through UCA 15).

This integration not only bridges the gap between qualitative systemic analysis and quantitative reliability metrics but also prioritizes applicable recommendations based on quantitative metrics. The framework's adaptability to the HIPPS 2351 architectures, including redundancy configurations (e.g., 2oo3 sensors, 1oo2 valves), underscores its applicability to complex industrial systems.

Overall, this work demonstrates that the integration of STPA with FTA represents a significant advancement in safety analysis methodologies. It underscores the necessity of combining qualitative system insights with quantitative reliability metrics. Future applications of the STPA-FTA framework in other safety–critical domains (e.g., nuclear, aerospace) are necessary to generalize the effectiveness of the proposed framework.

Appendix 1: STPA application related to the HIPPS 2351

See Tables 7, 8 and 9.

Table 7 Unsafe Control Actions (UCAs) identified by the STPA method

Control Action	Not providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
PT 2351 A/B/C	**UCA-1**: PT 2351A and PT 2351B do not provide a pressure signal to LS 2351 **UCA-4**: PT 2351A and PT 2351C do not provide a pressure signal to LS 2351 **UCA-7**: PT 2351B and PT 2351C do not provide a pressure signal to LS 2351	**N/A** **N/A** **N/A**	**UCA-2**: PT 2351A and PT 2351B provide a pressure signal to LS 2351 too late **UCA-5**: PT 2351A and PT 2351C provide a pressure signal to LS 2351 too late **UCA-8**: PT 2351B and PT 2351C provide a pressure signal to LS 2351 too late	**UCA-3**: PT 2351A and PT 2351B stopped providing signals to the LS 2351 too soon **UCA-6**: PT 2351A and PT 2351C stopped providing signals to the LS 2351 too soon **UCA-9**: PT 235B and PT 2351C stopped providing signals to the LS 2351 too soon
LS 2351	**UCA-10**: LS does not provide a signal to open TV 2351 **UCA-13**: LS does not provide a signal to close UV 2353 and UV 2356	**N/A** **N/A**	**UCA-11**: LS provides a signal to open TV 2351 too late **UCA-14**: LS provides a signal to close UV 2353 and UV 2356 too late	**UCA-12**: LS stops providing a signal to open TV 2351 too soon **UCA-15**: LS stops providing signals to close UV 2353 and UV 2356 too soon
TV 2351	**UCA-16**: TV 2351 does not provide an open valve function	**N/A**	**UCA-17**: TV 2351 provides an open valve function too late	**UCA-18**: TV 2351 stops providing an open valve function too soon
UV 2353 and UV 2356	**UCA-19**: UV 2353 and UV 2356 do not provide a close vale function	**N/A**	**UCA-20**: UV 2353 and UV 2356 provide a close valve function too late	**UCA-21**: UV 2353 and UV 2356 stopped providing a close valve function too soon
Site operator manually close UV 2353 and UV 2356 valves	**UCA-22:** Site operator does not close UV 2353 and UV 2356 valves when required	**N/A**	**UCA-23:** Site operator close UV 2353 and UV 2356 valves too late	**N/A**
Site operator manually open TV 2351 valve	**UCA-24:** Site operator does not open valve TV 2351 when required	**N/A**	**UCA-25:** Site operator does not close valve TV 2351 when required	**N/A**

Table 8 Controller constraints related to the identified UCAs

UCAs	Controller constraints
UCA-1: PT 2351A and PT 2351B do not provide a pressure signal to LS 2351	**C-1**: PT 2351A and PT 2351B must provide a pressure signal to LS 2351
UCA-2: PT 2351A and PT 2351B provide a pressure signal to LS 2351 too late	**C-2**: PT 2351A and PT 2351B must not provide a pressure signal to LS 2351 too late
UCA-3: PT 2351A and PT 2351B stopped providing signals to the LS 2351 too soon	**C-3**: PT 2351A and PT 2351B must not stop providing signals to the LS 2351 too soon
UCA-4: PT 2351A and PT 2351C do not provide a pressure signal to LS 2351	**C-4**: PT 2351A and PT 2351C must provide a pressure signal to LS 2351
UCA-5: PT 2351A and PT 2351C provide a pressure signal to LS 2351 too late	**C-5**: PT 2351A and PT 2351C must not provide a pressure signal to LS 2351 too late
UCA-6: PT 2351A and PT 2351C stopped providing signals to the LS 2351 too soon	**C-6**: PT 2351A and PT 2351C must not stop providing signals to the LS 2351 too soon
UCA-7: PT 2351B and PT 2351C do not provide a pressure signal to LS 2351	**C-7**: PT 2351B and PT 2351C must provide a pressure signal to LS 2351
UCA-8: PT 2351B and PT 2351C provide a pressure signal to LS 2351 too late	**C-8**: PT 2351B and PT 2351C must not provide a pressure signal to LS 2351 too late
UCA-9: PT 235B and PT 2351C stopped providing signals to the LS 2351 too soon	**C-9**: PT 2351B and PT 2351C must not stop providing signals to the LS 2351 too soon
UCA-10: LS does not provide a signal to open TV 2351	**C-10**: LS must provide a signal to open TV 2351
UCA-11: LS provides a signal to open TV 2351 too late	**C-11**: LS must not provide a signal to open TV 2351 too late
UCA-12: LS stops providing a signal to open TV 2351 too soon	**C-12**: LS must not stop providing a signal to open TV 2351 too soon
UCA-13: LS does not provide a signal to close UV 2353 and UV 2356	**C-13**: LS should provide a signal to close UV 2353 and UV 2356
UCA-14: LS provides a signal to close UV 2353 and UV 2356 too late	**C-14**: LS must not provide a signal to close UV 2353 and UV 2356 too late
UCA-15: LS stops providing signals to close UV 2353 and UV 2356 too soon	**C-15**: LS must not stop providing signals to close UV 2353 and UV 2356 too soon
UCA-16: TV 2351 does not provide an open valve function	**C-16**: TV 2351 must provide an open valve function
UCA-17: TV 2351 provides an open valve function too late	**C-17**: TV 2351 must not provide an open valve function too late
UCA-18: TV 2351 stops providing an open valve function too soon	**C-18**: TV 2351 must not stop providing an open valve function too soon
UCA-19: UV 2353 and UV 2356 do not provide a close vale function	**C-19**: UV 2353 and UV 2356 should provide a close vale function
UCA-20: UV 2353 and UV 2356 provide a close valve function too late	**C-20**: UV 2353 and UV 2356 must not provide a close valve function too late
UCA-21: UV 2353 and UV 2356 stopped providing a close valve function too soon	**C-21**: UV 2353 and UV 2356 must not stop providing a close valve function too soon
UCA-22: Site operator does not manually open/close safety valves (TV 2351, UV 2353, UV 2356) when required	**C-22:** Site operator must manually open/close safety valves (TV 2351, UV 2353, UV 2356) when required
UCA-23: Site operator manually opens/closes safety valves (TV 2351, UV 2353, UV 2356) too late	**C-23:** Site operator must not manually open/close safety valves (TV 2351, UV 2353, UV 2356) too late

Table 9 Loss scenarios related to UCAs

Unsafe control action	Loss scenarios
UCA-1: PT 2351A and PT 2351B do not provide a pressure signal to LS 2351	**Scenario 1**: PT 2351A and PT 2351B do not detect high pressure, because PT 2351 A/B/C is faulty, resulting in the absence of a pressure signal to LS 2351 **Scenario 2**: PT 2351A and PT 2351B do not detect high pressure due to inadequate testing and maintenance of transmitters, resulting in the absence of a pressure signal to LS 2351 **Scenario 3**: PT 2351A and PT 2351B do not detect high pressure, because the set point of transmitters is modified wrongly in the operation, resulting in the absence of a pressure signal to the LS
UCA-2: PT 2351A and PT 2351B provide a pressure signal to LS 2351 too late	**Scenario 1**: PT 2351A and PT 2351B detected high pressure too late, because PT 2351 A/B/C received delayed feedback about high pressure due to inadequate testing and maintenance, resulting in the delayed pressure signal to LS 2351 **Scenario 2**: PT 2351A and PT 2351B detected high pressure too late, because PT 2351 A/B/C received delayed feedback about high pressure due to the sensors' wrong set point, resulting in a delay of a pressure signal to LS 2351 **Scenario 3**: PT 2351A and PT 2351B detected high pressure too late, because PT 2351 A/B/C received delayed feedback about high pressure due to the wrong modification of the transmitter set point, resulting in a delay of a pressure signal to LS 2351
UCA-3: PT 2351A and PT 2351B stopped providing signals to the LS 2351 too soon	**Scenario 1**: PT 2351A and PT 2351B stopped detecting high pressure because PT 2351 A/B/C stopped receiving feedback about high pressure due to instrumentation failure, resulting in the absence of a pressure signal to LS 2351 **Scenario 2**: PT 2351A and PT 2351B stopped detecting high pressure too soon, because PT 2351 A/B/C stopped receiving feedback about high pressure due to errors with the communication pathways between PT 2351 A/B/C and LS 2351, such as problems, with cables, connectors, or network communication protocols, resulting in the absence of a pressure signal to LS 2351
UCA-4: PT 2351A and PT 2351C do not provide a pressure signal to LS 2351	**Scenario 1**: PT 2351A and PT 2351C do not detect high pressure, because PT 2351 A/B/C is faulty, resulting in the absence of a pressure signal to LS 2351 **Scenario 2**: PT 2351A and PT 2351C do not detect high pressure due to inadequate testing and maintenance of transmitters, resulting in the absence of a pressure signal to LS 2351 **Scenario 3**: PT 2351A and PT 2351C do not detect high pressure, because the set point of transmitters is modified wrongly in the operation, resulting in the absence of a pressure signal to the LS
UCA-5: PT 2351A and PT 2351C provide a pressure signal to LS 2351 too late	**Scenario 1**: PT 2351A and PT 2351C detected high pressure too late, because PT 2351 A/B/C received delayed feedback about high pressure due to inadequate testing and maintenance, resulting in the delayed pressure signal to LS 2351 **Scenario 2**: PT 2351A and PT 2351C detected high pressure too late, because PT 2351 A/B/C received delayed feedback about high pressure due to the sensors' wrong set point, resulting in a delay of a pressure signal to LS 2351 **Scenario 3**: PT 2351A and PT 2351C detected high pressure too late, because PT 2351 A/B/C received delayed feedback about high pressure due to the wrong modification of the transmitter set point, resulting in a delay of a pressure signal to LS 2351
UCA-6: PT 2351A and PT 2351C stopped providing signals to the LS 2351 too soon	**Scenario 1**: PT 2351A and PT 2351C stopped detecting high pressure because PT 2351 A/B/C stopped receiving feedback about high pressure due to instrumentation failure, resulting in the absence of a pressure signal to LS 2351 **Scenario 2**: PT 2351A and PT 2351C stopped detecting high pressure too soon, because PT 2351 A/B/C stopped receiving feedback about high pressure due to errors with the communication pathways between PT 2351 A/B/C and LS 2351, such as problems, with cables, connectors, or network communication protocols, resulting in the absence of a pressure signal to LS 2351
Unsafe control action	Loss scenarios
UCA-7: PT 2351B and PT 2351C do not provide a pressure signal to LS 2351	**Scenario 1**: PT 2351B and PT 2351C do not detect high pressure, because PT 2351 A/B/C is faulty, resulting in the absence of a pressure signal to LS 2351 **Scenario 2**: PT 2351B and PT 2351C do not detect high pressure due to inadequate testing and maintenance of transmitters, resulting in the absence of a pressure signal to LS 2351 **Scenario 3**: PT 2351B and PT 2351C do not detect high pressure, because the set point of transmitters is modified wrongly in the operation, resulting in the absence of a pressure signal to the LS
UCA-8: PT 2351B and PT 2351C provide a pressure signal to LS 2351 too late	**Scenario 1**: PT 2351B and PT 2351C detected high pressure too late, because PT 2351 A/B/C received delayed feedback about high pressure due to inadequate testing and maintenance, resulting in the delayed pressure signal to LS 2351 **Scenario 2**: PT 2351B and PT 2351C detected high pressure too late, because PT 2351 A/B/C received delayed feedback about high pressure due to the sensors' wrong set point, resulting in a delay of a pressure signal to LS 2351 **Scenario 3**: PT 2351B and PT 2351C detected high pressure too late, because PT 2351 A/B/C received delayed feedback about high pressure due to the wrong modification of the transmitter set point, resulting in a delay of a pressure signal to LS 2351
UCA-9: PT 2351B and PT 2351C stopped providing signals to the LS 2351 too soon	**Scenario 1**: PT 2351B and PT 2351C stopped detecting high pressure because PT 2351 A/B/C stopped receiving feedback about high pressure due to instrumentation failure, resulting in the absence of a pressure signal to LS 2351 **Scenario 2**: PT 2351B and PT 2351C detecting high pressure too soon, because PT 2351 A/B/C stopped receiving feedback about high pressure due to errors with the communication pathways between PT 2351 A/B/C and LS 2351, such as problems, with cables, connectors, or network communication protocols, resulting in the absence of a pressure signal to LS 2351

Table 9 (continued)

Unsafe control action	Loss scenarios
UCA-10: LS does not provide a signal to open TV 2351	**Scenario 1**: LS does not provide a signal to open TV 2351, because LS 2351 does not receive a signal from PT 2351 A/B/C due to transmitters PT 2351 A/B/C failure, resulting in the absence of TV 2351 open valve function **Scenario 2**: LS does not provide a signal to open TV 2351, because LS 2351 is faulty due to software errors, resulting in the absence of TV 2351 open valve function **Scenario 3**: LS does not provide a signal to open TV 2351B due to a hardware failure of LS 2351, such as a malfunctioning output port or damaged wiring, resulting in the absence of a pressure signal to TV 2351
UCA-11: LS provides a signal to open TV 2351 too late	**Scenario 1**: LS provides a signal to open TV 2351 too late, because LS received a delayed signal from PT 2351 A/B/C due to transmitters PT 2351 A/B/C failure, resulting in the delayed TV 2351 open valve function
UCA-12: LS stops providing a signal to open TV 2351 too soon	**Scenario 1**: LS stops providing a signal to open TV 2351 too soon, because LS stops receiving signals from PT 2351 A/B/C due to transmitters PT 2351 A/B/C failure, resulting in the absence of TV 2351 open valve function **Scenario 2**: LS stops providing a signal to open TV 2351 too soon, because LS is faulty due to a software error, resulting in the absence of TV 2351 open valve function **Scenario 3**: LS stops providing a signal to open TV 2351 too soon, due to a hardware failure of the LS, such as a malfunctioning output port, damaged wiring, or a defective component, resulting in the absence of TV 2351 open valve function

Unsafe control action	Loss scenarios
UCA-13: LS does not provide a signal to close UV 2353 and UV 2356	**Scenario 1**: LS does not provide a signal to close UV 2353 and UV 2356, because LS does not receive a signal from PT 2351 A/B/C due to transmitters PT 2351 A/B/C failure, resulting in the absence of UV 2353 and UV 2356 close valve function **Scenario 2**: LS does not provide a signal to close UV 2353 and UV 2356, because the LS is faulty due to a software error, resulting in the absence of UV 2353 and UV 2356 close valve function **Scenario 3**: LS does not provide a signal to close UV 2353 and UV 2356, due to a hardware failure of the LS, such as a malfunctioning output port, damaged wiring, or a defective component that prevents the signal from reaching TV 2351A, resulting in the absence of UV 2353 and UV 2356 close valve function
UCA-14: LS provides a signal to close UV 2353 and UV 2356 too late	**Scenario 1**: LS provides a signal to close UV 2353 and UV 2356 too late, because LS received a delayed signal from PT 2351 A/B/C due to transmitters PT 2351 A/B/C failure, resulting in the delayed TV 2351A open valve function
UCA-15: LS stops providing signals to close UV 2353 and UV 2356 too soon	**Scenario 1**: LS stops providing signals to close UV 2353 and UV 2356 too soon, because LS stops receiving signals from PT 2351 A/B/C due to transmitters PT 2351 A/B/C failure, resulting in the absence of UV 2353 and UV 2356 close valve function **Scenario 2**: LS stops providing signals to close UV 2353 and UV 2356 too soon, because the LS is faulty due to a software error, resulting in the absence of UV 2353 and UV 2356 close valve function **Scenario 3**: LS stops providing signals to close UV 2353 and UV 2356 too soon, due to a hardware failure of the LS, such as a malfunctioning output port, damaged wiring, or a defective component, resulting in the absence of UV 2353 and UV 2356 close valve function
UCA-16: TV 2351 does not provide an open valve function	**Scenario 1**: TV 2351 does not provide an open valve function, because TV 2351 doesn't receive a signal from the LS due to failures in the LS or PT 2351 A/B/C **Scenario 2**: TV 2351 does not provide an open valve function, because TV 2351 is faulty due to BPCS 2351 failures because TV 2351 is a common component between BPCS 2351 of temperature and the safety instrumented system (HIPPS 2351) **Scenario 3**: TV 2351 does not provide an open valve function, because TV 2351 is faulty due to mechanical failure (blockage or fouling) **Scenario 4** TV 2351 does not provide an open valve function, because TV 2351 is faulty due to instrumentation failure
UCA-17: TV 2351 provides an open valve function too late	**Scenario 1**: TV 2351 provides an open valve function too late because TV 2351 received a delayed signal from the LS **Scenario 2**: TV 2351 provides an open valve function too late, due to mechanical failure of TV 2351 **Scenario 3:** TV 2351 provides an open valve function too late due to a delayed signal from PT 2351 A/B/C
UCA-18: TV 2351 stops providing an open valve function too soon	**Scenario 1**: TV 2351 stops providing an open valve function too soon because TV 2351 stops receiving signals from the LS due to failures in the LS **Scenario 2**: TV 2351 stops providing an open valve function too soon because PT 2351 A/B/C is faulty and stops sending a signal to LS. As a result, TV 2351 stops receiving a signal from LS **Scenario 3**: TV 2351 stops providing an open valve function too soon because TV 2351 is faulty due to BPCS 2351 failures because TV 2351 is a common component between BPCS 2351 of temperature and the HIPPS 2351 **Scenario 4**: TV 2351 stops providing an open valve function too soon because TV 2351 is faulty due to mechanical failure (blockage or fouling) **Scenario 5:** TV 2351 stops providing an open valve function too soon because TV 2351 is faulty due to instrumentation failure

Table 9 (continued)

Unsafe control action	Loss scenarios
UCA-19: UV 2353 and UV 2356 do not provide a close valve function	**Scenario 1**: UV 2353 and UV 2356 do not provide a close valve function because UV 2353 and UV 2356 do not receive signals from the LS due to failures in the LS **Scenario 2**: UV 2353 and UV 2356 do not provide a close valve function because UV 2353 and UV 2356 do not receive a signal from the LS due to failures in PT 2351 A/B/C **Scenario 3**: UV 2353 and UV 2356 do not provide a close valves function, due to a common cause failure (CCF) of UV 2353 and UV 2356 because the valves are redundant homogenously and share a common control circuitry or power source **Scenario 4**: UV 2353 and UV 2356 do not provide a close valves function, because UV 2353 and UV 2356 are faulty due to mechanical failure (blockage or fouling) **Scenario 5:** UV 2353 and UV 2356 do not provide a close valve function, because UV 2353 and UV 2356 are faulty due to instrumentation failure
UCA-20: UV 2353 and UV 2356 provide a close valve function too late	**Scenario 1**: UV 2353 and UV 2356 provide a close valve function too late, because UV 2353 and UV 2356 received a delayed signal from the LS due to failures in the LS **Scenario 2**: UV 2353 and UV 2356 provide a close valve function too late, due to mechanical failure of UV 2353 and UV 2356 **Scenario 3:** UV 2353 and UV 2356 provide a close valve function too late, due to a delayed signal from PT 2351 A/B/C **Scenario 4:** UV 2353 and UV 2356 provide a close valve function too late, due to a common cause failure (CCF) of UV 2353 and UV 2356 because the valves are homogenously redundant and share a common control circuitry or power source
UCA-21: UV 2353 and UV 2356 stopped providing a close valve function too soon	**Scenario 1**: UV 2353 and UV 2356 stopped providing a close valve function too soon because UV 2353 and UV 2356 stopped receiving signals from the LS due to faults in the LS **Scenario 2**: UV 2353 and UV 2356 stopped providing a close valve function too soon because PT 2351 A/B/C is faulty and stopped sending signals to LS **Scenario 3**: UV 2353 and UV 2356 stop providing a close valve function too soon, due to a common cause failure (CCF) of UV 2353 and UV 2356 because the valves are redundant homogenously and share a common control circuitry or power source **Scenario 4**: UV 2353 and UV 2356 stopped providing a close valve function too soon because they were faulty due to mechanical failure (blockage or fouling) **Scenario 5:** UV 2353 and UV 2356 stopped providing a close valve function too soon because UV 2353 and UV 2356 are faulty due to instrumentation failure
UCA-22: Site operators do not manually open/close safety valves (TV 2351, UV 2353, UV 2356) when required	**Scenario 1**: Site operators do not manually open/close the safety valves due to a lack of training or unclear procedures for manual intervention **Scenario 2**: Site operators do not manually open/close the safety valves because they assume the logic solver (LS) has already taken corrective action **Scenario 3**: Site operators do not manually open/close the safety valves due to a lack of communication between the control room operator and site operators regarding the necessary action **Scenario 4**: Site operators do not manually open/close the safety valves due to hesitation or lack of confidence in taking manual action, fearing unintended consequences
UCA-23: Site operators manually open/close safety valves (TV 2351, UV 2353, UV 2356) too late	**Scenario 1**: Site operators manually open/close the safety valves too late due to delayed information from the control room operator to take action on the valves **Scenario 2**: Site operators manually open/close the safety valves too late because they are occupied with other tasks and do not immediately respond to the high-pressure condition **Scenario 3**: Site operators manually open/close the safety valves too late due to a lack of training or unclear procedures for manual intervention **Scenario 4**: Site operators manually open/close the safety valves too late due to hesitation or lack of confidence in taking manual action, fearing unintended consequences

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1007/s41872-026-00400-6.

Funding No specific funding was received to support this research.

Declarations

Conflict of interest The author declares that there are no conflicts of interest or competing interests associated with this manuscript.

References

Abdulkhaleq A, Baumeister M, Böhmert H, Wagner S (2018) Missing no interaction—using STPA for identifying hazardous interactions of automated driving systems. Int J Saf Sci 2(1):115–124. https://doi.org/10.24900/ijss/0201115124.2018.0301

Alemzadeh H et al (2015) Systems-theoretic safety assessment of robotic telesurgical systems. Comput Saf Reliab Secur 34:213–227. https://doi.org/10.1007/978-3-319-24255-2_16

Andrews J, Tolo S (2023) Dynamic and dependent tree theory (D2T2): a framework for the analysis of fault trees with dependent basic events. Reliab Eng Syst Saf 230:108959. https://doi.org/10.1016/j.ress.2022.108959

Ayachi K, Boudjoghra N (2018) Évaluation des risques au niveau d'une colonne de séparation NAPHTA par l'application de la démarche HAZOP-ROA-LOPA. Master thesis.

Banda OAV, Kannos S (2017) Hazard analysis process for autonomous vessels. Tech Rep. https://doi.org/10.1016/j.ress.2019.106584

Benhamlaoui W, Rouainia M, Liu Y, Medjram MS (2020) Comparative study of STPA and Bowtie methods: case of hazard identification for pipeline transportation. J Fail Anal Prev 20(6):2003–2016. https://doi.org/10.1007/s11668-020-01010-9

Bensaci C, Zennir Y, Pomorski D, Innal F, Liu Y (2021) Distributed vs. hybrid control architecture using STPA and AHP—application to an autonomous mobile multi-robot system. Int J Saf Secur Eng 11(1):1–12. https://doi.org/10.18280/ijsse.110101

Bensaci C, Zennir Y, Pomorski D, Innal F, Liu Y, Tolba C (2020) STPA and Bowtie risk analysis study for centralized and hierarchical control architectures comparison. Alexand Eng J 59(5):3799–3816. https://doi.org/10.1016/j.aej.2020.06.036

Bensaci C, Zennir Y, Pomorski D, Innal F, Lundteigen MA (2023) Collision hazard modeling and analysis in a multi-mobile robots system transportation task with STPA and SPN. Reliab Eng Syst Saf 234:109138. https://doi.org/10.1016/j.ress.2023.109138

Bujna M, Prístavka M, Lee CK, Borusiewicz A, Samociuk W, Beloev I, Makmur M (2023) Reducing the probability of failure in manufacturing equipment by quantitative FTA analysis. Agric Eng 27(1):255–272. https://doi.org/10.2478/agriceng-2023-0019

Chaal M, Valdez Banda OA, Glomsrud JA, Basnet S, Hirdaris S, Kujala P (2020) A framework to model the STPA hierarchical control structure of an autonomous ship. Saf Sci 132:104939. https://doi.org/10.1016/j.ssci.2020.104939

Chevreau F-R, Wybo J-L, Cauchois D (2006) Organizing learning processes on risks by using the bow-tie representation. J Hazard Mater 130(3):276–283. https://doi.org/10.1016/j.jhazmat.2005.07.018

Dibaei M, Arestova A, Hielscher K-S, German R (2023) A novel method for computing minimal cut sets of variant-rich systems in fault tree analysis. In: 2023 7th international conference on system reliability and safety (ICSRS), IEEE, pp 481–487. https://doi.org/10.1109/icsrs59833.2023.10381472

Erdem P, Akyuz E, Aydin M, Celik E, Arslan O (2024) Assessment of human error contribution to container loss risk under fault tree analysis and interval type-2 fuzzy logic-based SLIM approach. Proc Inst Mech Eng M J Eng Marit Environ 238(3):553–566. https://doi.org/10.1177/14750902231203074

Fleming CH, Spencer M, Thomas J, Leveson N, Wilkinson C (2013) Safety assurance in NextGen and complex transportation systems. Saf Sci 55:173–187. https://doi.org/10.1016/j.ssci.2012.12.005

Fuentes-Bargues JL, González-Cruz MC, González-Gaya C, Baixauli-Pérez MP (2017) Risk analysis of a fuel storage terminal using HAZOP and FTA. Int J Environ Res Public Health 14(7):705. https://doi.org/10.3390/ijerph14070705

GRIF Workshop, Graphical Interface for Reliability Forecasting, Software. (2023). http://grif-workshop.com

Ge G, Sun L, Li YF (2022) A systematic approach to develop an autopilot sensor monitoring system for autonomous delivery vehicles based on the STPA method. In: Proc IEEE Int Symp Softw Reliab Eng Workshops (ISSREW 2022), 318–325. https://doi.org/10.1109/issrew55968.2022.00087

Giraud L, Galy B (2018) Fault tree analysis and risk mitigation strategies for mine hoists. Saf Sci 110:222–234

Hardy K, Guarnieri F (2011) Using a systemic model of accident for improving innovative technologies: application and limitations of the STAMP model to a process for treatment of contaminated substances. In: 15th world multi-conference on systemics, cybernetics and informatics: WMSCI (2011)

Hauge S, Kråkenes T, Hokstad P, Håbrekke S, Jin H (2013) Reliability prediction method for safety instrumented systems: PDS Method Handbook—2013 Edition. SINTEF Technology and Society Safety Research Report. www.sintef.no

Heikkilä E, Malm T, Sarsama J, Tiusanen R, Ahonen T (2023) Hazard analysis of an autonomous container handling system—a comparison of STPA and HAZOP methods. Sci J Gdynia Marit Univ 125:25–39. https://doi.org/10.26408/125.02

IEC 61508 (2010) Functional safety of electrical/electronic/programmable electronic safety-related systems, part 1–7, 2nd ed. International Electrotechnical Commission, Geneva

Ishimatsu T et al (2014) Hazard analysis of complex spacecraft using systems-theoretic process analysis. J Spacecr Rockets 51(2):509–522. https://doi.org/10.2514/1.a32449

Jiang W, Liu S, Liu A (2022) A systematic method for identifying safety-related faults in formal specifications using FTA. In: Proceedings of the 13th international conference on availability, reliability and security (ICRMS 2022). https://doi.org/10.1109/ICRMS55680.2022.9944610

Kaneko T, Yoshioka N, Sasaki R (2020) STAMP SandS: safety and security scenario for specification and standard in the society of AI/IoT. In: Proc IEEE 20th Int Conf Softw Qual Reliab Secur Companion (QRS-C 2020), 168–175. https://doi.org/10.1109/qrs-c51114.2020.00037

Khastgir S, Brewerton S, Thomas J, Jennings P (2021a) Systems approach to creating test scenarios for automated driving systems. Reliab Eng Syst Saf 215:107610. https://doi.org/10.1016/j.ress.2021.107610

Khastgir S, Brewerton S, Thomas J, Jennings P (2021b) Systems approach to creating test scenarios for automated driving systems. Reliab Eng Syst Saf 215:107610

Kholida L, Lubis NTM, Citra Z, Hasdian E (2024) Risk assessment on the Bandung Hilton Hotel construction project utilizing the FMEA and FTA methods. CIVED 11(2):738–747. https://doi.org/10.24036/cived.v11i2.604

Kim E, Lee K, Kim J, Lee Y, Park J, Moon I (2011) Development of Korean hydrogen fueling station codes through risk analysis. Int J Hydrog Energy 36(20):13122–13131. https://doi.org/10.1016/j.ijhydene.2011.07.053

Lacasse S, Eidsvik U, Nadim F, Hoeg K, Blikra LH (2008) Event tree analysis of Aknes rock slide hazard. In: Proc 4th Can Conf Geohazards, Quebec City, Canada, 20–24

Lambert HE (1975) Fault trees for decision-making in systems analysis. University of California, Berkeley

Larit K, Rehail Y, Zennir Y, Rodriguez M (2024) FMEA-failure modes & effects analysis for incident investigation: electric arc furnace-EBT system. Alger J Signals Syst 9(4):212–221. https://doi.org/10.51485/ajss.v9i4.240

Leveson N (2004) A new accident model for engineering safer systems. Saf Sci 42(4):237–270

Leveson N (2011) Engineering a safer world: systems thinking applied to safety. MIT Press, Cambridge, p 560

Leveson N, Thomas J (2018) STPA handbook. Online Document 3:188

Lipol LS, Haq J (2011) Risk analysis method: FMEA/FMECA in the organizations. Int J Basic Appl Sci 11(5):74–82

Luo W, Wei O (2017) WAP: SAT-based computation of minimal cut sets. In: Proc IEEE 28th Int Symp Softw Reliab Eng (ISSRE), 146–151. https://doi.org/10.1109/issre.2017.13

Muram FU, Javed MA, Punnekkat S (2019) System of systems hazard analysis using HAZOP and FTA for advanced quarry production. In: Proc 4th Int Conf Syst Reliab Saf (ICSRS 2019), 394–401. https://doi.org/10.1109/icsrs48664.2019.8987613

Muram FU, Javed MA, Punnekkat S (2019) System of systems hazard analysis using HAZOP and FTA for advanced quarry production. In: 2019 4th international conference on system reliability and

safety (ICSRS), IEEE, pp 394–401. https://doi.org/10.1109/icsrs48664.2019.8987613
Mutlu NG, Altuntas S (2019) Hazard and risk analysis for ring spinning yarn production process by integrated FTA-FMEA approach. Text Apparel 29(3):208–218. https://doi.org/10.32710/tekstilvekonfeksiyon.482167
Rehail Y, Zennir Y, Tchouar N (2024) Application of STPA for comprehensive risk analysis of naphtha explosion hazards: case study: column C-63 at Skikda-RA1K refinery. Alger J Signals Syst 9(3):153–161. https://doi.org/10.51485/ajss.v9i3.225
Renosori P, Oemar H, Fauziah SR (2023) Combination of FTA and FMEA methods to improve efficiency in the manufacturing company. Acta Logistica. https://doi.org/10.22306/al.v10i3.422
Rodríguez M, Díaz I (2016) A systematic and integral hazards analysis technique applied to the process industry. J Loss Prev Process Ind 43:721–729. https://doi.org/10.1016/j.jlp.2016.06.016
Rokseth B, Utne IB, Vinnem JE (2017) A systems approach to risk analysis of maritime operations. Proc Inst Mech Eng Part O J Risk Reliab 231(1):53–68. https://doi.org/10.1177/1748006x16682606
Roozbahani A, Ghanian T (2024) Risk assessment of inter-basin water transfer plans through integration of fault tree analysis and Bayesian network modelling approaches. J Environ Manag 356:120703. https://doi.org/10.1016/j.jenvman.2024.120703
Shafiee M, Enjema E, Kolios A (2019) An integrated FTA-FMEA model for risk analysis of engineering systems: a case study of subsea blowout preventers. Appl Sci 9(6):1192. https://doi.org/10.3390/app9061192
Siddiqui DN, Nandan A, Sharma M, Srivastava A (2014) Risk management techniques HAZOP and HAZID study. Int J Occup Health Saf Fire Environ Allied Sci 1(1):5–8
Sulaman SM, Beer A, Felderer M, Höst M (2019) Comparison of the FMEA and STPA safety analysis methods—a case study. Softw Qual J 27(1):349–387. https://doi.org/10.1007/s11219-017-9396-0
Sultana S, Okoh P, Haugen S, Vinnem JE (2019) Hazard analysis: application of STPA to ship-to-ship transfer of LNG. J Loss Prev Process Ind 60:241–252. https://doi.org/10.1016/j.jlp.2019.04.005
Tathod P, Yadav S (2024) Eliminating the occurrence and consequences of toxic release in petrochemical industry through intervention of safety engineering tools. Int J Adv Res Sci Commun Technol 32:486–502. https://doi.org/10.48175/ijarsct-18952
Thomas J (2013) Extending and automating a systems-theoretic hazard analysis for requirements generation and analysis
Wróbel K, Montewka J, Kujala P (2018) Towards the development of a system-theoretic model for safety assessment of autonomous merchant vessels. Reliab Eng Syst Saf 178:209–224. https://doi.org/10.1016/j.ress.2018.05.019
Wu Y et al (2022) Comparison of the theoretical elements and application characteristics of STAMP, FRAM, and 24Model: a major hazardous chemical explosion accident. J Loss Prev Process Ind 80:104880. https://doi.org/10.1016/j.jlp.2022.104880
Yazdi M, Zarei E (2018) Uncertainty handling in the safety risk analysis: an integrated approach based on fuzzy fault tree analysis. J Fail Anal Prev 18:392–404. https://doi.org/10.1007/s11668-018-0421-9
Yousefi A, Rodriguez Hernandez M (2019) Using a system theory-based method (STAMP) for hazard analysis in the process industry. J Loss Prev Process Ind 61:305–324. https://doi.org/10.1016/j.jlp.2019.06.014
Zhang W, Meng X, Wang J, Li T, Shan Q, Teng F (2021) Safety analysis of automatic crane trolley running system based on STAMP/STPA. In: 2021 8th Int Conf Inf Cybern Comput Soc Syst (ICCSS), IEEE, 453–458. https://doi.org/10.1109/iccss53909.2021.9722016

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.