MOTIVECTION
Journal of Mechanical Electrical and Industrial Engineering

Volume: 8, Number: 2, 2026
ISSN: 2655 – 7215 [printed] ; 2685-2098 [online]
DOI: https://doi.org/10.46574/motivection.v8i1.552

Quantifying Manual Safeguard Failure Probability in High-Flow Gasoline Tank Overfill: An Integrated SLIM–SHIPP–ETA–LOPA Framework for SIL Specification

Rafi Adisasmito Syamsudin[1], Ahmad Dani[1], Indrawan Christano[1], Adhitya Ryan Ramadhani[1]*

ABSTRACT

High-flow gasoline tank filling can escalate to overfill, fire, or explosion when level control relies on manual safeguards. This study quantified manual safeguard failure in a gasoline storage facility operating at 300 kL/h and specified the required automation level. HAZOP identified the critical deviation, ALOHA characterized consequence zones, SLIM estimated operator error probabilities, SHIPP and ETA represented sequential barrier failure, and LOPA determined the required risk reduction. The "More Level" deviation obtained the highest HAZOP priority. Under the adopted modeling assumptions and an assumed initiating event frequency of 1.0 demand per year, ETA estimated failure probabilities of 3.10×10^{-1} for the Ignition Prevention Barrier and 8.54×10^{-1} for the Escalation Prevention Barrier, producing a major fire/explosion scenario frequency of 1.88×10^{-3} per year. This value exceeded the adopted target risk of 1.0×10^{-4} per year and required an RRF of 18.8. The results support implementing a SIL 1 Safety Instrumented System to supplement manual safeguards.

Keywords
Gasoline tank overfill; Manual safeguard failure; Human error probability; Event Tree Analysis; Safety Integrity Level

[1] Department of Mechanical Engineering, Faculty of Industrial Technology, Universitas Pertamina
Jalan Teuku Nyak Arief, Jakarta Selatan 12220, Indonesia

* Corresponding Author: adhitya.rr@universitaspertamina.ac.id

Submitted : May 02, 2026. Accepted : July 07, 2026. Published : August 05, 2026

INTRODUCTION

Gasoline storage facilities are critical components of the liquid-fuel supply chain because they support the receiving, storage, and distribution of high-volume petroleum products. However, these facilities also involve substantial process-safety hazards when level monitoring, transfer control, and emergency response depend heavily on manual intervention. Tank overfill is one of the most critical scenarios because loss of level control can release a large volume of flammable liquid, generate vapor, and create conditions for pool fire or vapor-cloud explosion. Previous studies on crude-oil storage tanks, LPG storage systems, accidental releases, and gas-transmission hazards show that fire and explosion consequences are influenced by release volume, fuel volatility, vapor formation, release momentum, congestion, ignition condition, and thermal or blast exposure radius [1]–[4]. These factors become more critical in high-flow transfer operations because the available time for detection, communication, and manual shutdown decreases as the filling rate increases.

Contemporary process-safety research has increasingly moved from isolated consequence estimation toward integrated risk assessment that connects hazard identification, consequence modeling, barrier performance, human reliability, and decision support. Dynamic storage-tank risk assessment has combined consequence modeling with probabilistic reasoning to represent evolving accident pathways [5]. Broader process-safety reviews also indicate that modern risk assessment should not only estimate accident frequency or consequence severity, but also explain how initiating events, safety barriers, and operational decisions interact during accident escalation [6]. In this context, human reliability becomes important because manual monitoring, valve operation, alarm response, and emergency communication can determine whether an abnormal condition is interrupted or allowed to escalate.

Human Reliability Assessment (HRA) provides a structured approach for estimating the probability of operator error in safety-critical operations. In fuel-handling and fire/explosion contexts, HRA has been used to identify operational weaknesses, evaluate human error probability, and support risk-reduction planning [7]. The Success Likelihood Index Method (SLIM) is relevant because it evaluates operator performance through Performance Shaping Factors such as workload, procedure clarity, training adequacy, communication quality, and available response time [8]. Recent fire and explosion risk studies have also shown that integrating SLIM-based human reliability with event-tree logic can provide a clearer representation of how operator error contributes to accident progression, rather than treating human failure as an isolated event [9].

Several analytical frameworks can support the assessment of overfill risk in manually operated gasoline storage systems. The System Hazard Identification, Prediction and Prevention (SHIPP) methodology provides a sequential structure for mapping initiating events, accident pathways, and prevention barriers [10]. Layer of Protection Analysis (LOPA) provides a semi-quantitative basis for evaluating whether safeguards can be credited as Independent Protection Layers, especially when initiating event frequency, enabling conditions, and Probability of Failure on Demand must be considered [11]. For petroleum storage facilities, API 2350 emphasizes overfill prevention through structured management, alarm response, operating discipline, and protection-layer requirements [12]. In addition, IEC 61511 provides the functional-safety basis for specifying Safety Instrumented Systems and Safety Integrity Levels in process-industry applications [13].

Although these methods are well established, previous studies often examine consequence modeling, human reliability, accident propagation, and protection-layer adequacy as separate analytical components. This separation creates a methodological limitation for high-flow gasoline storage facilities that rely on manual gate valves, local level observation, and operator communication as primary safeguards. In such facilities, the key safety issue is not only whether an overfill can produce severe consequences, but also how manual monitoring failure, delayed response, and sequential barrier degradation combine to determine the final risk level and the required automation. This issue is particularly relevant to the studied facility, where gasoline is transferred at 300 kL/h and the manual response window is limited.

This study addresses this gap by applying an integrated HAZOP–ALOHA–SLIM–SHIPP–ETA–LOPA framework to quantify manual safeguard failure probability in a high-flow gasoline tank overfill scenario and to support Safety Integrity Level specification. HAZOP is used to identify critical overfill deviations, ALOHA is used to estimate consequence zones, SLIM is used to quantify operator error probability, SHIPP and Event Tree Analysis are used to represent sequential barrier failure, and LOPA is used to determine the required Risk Reduction Factor and SIL category. The contribution of this study is a traceable risk-assessment workflow that links human reliability, accident propagation, and protection-layer adequacy for decision support in gasoline storage safety.

METHOD

This study used a quantitative risk-assessment design to evaluate manual safeguard failure in a high-flow gasoline tank overfill scenario and to determine the required automation level. The assessment was conducted through an integrated HAZOP–ALOHA–SLIM–SHIPP–ETA–LOPA framework. This framework was selected because the study required a structured procedure that could connect hazard identification, consequence modeling, human reliability estimation, sequential barrier modeling, and protection-layer evaluation. The overall methodological workflow is presented in Figure 1.

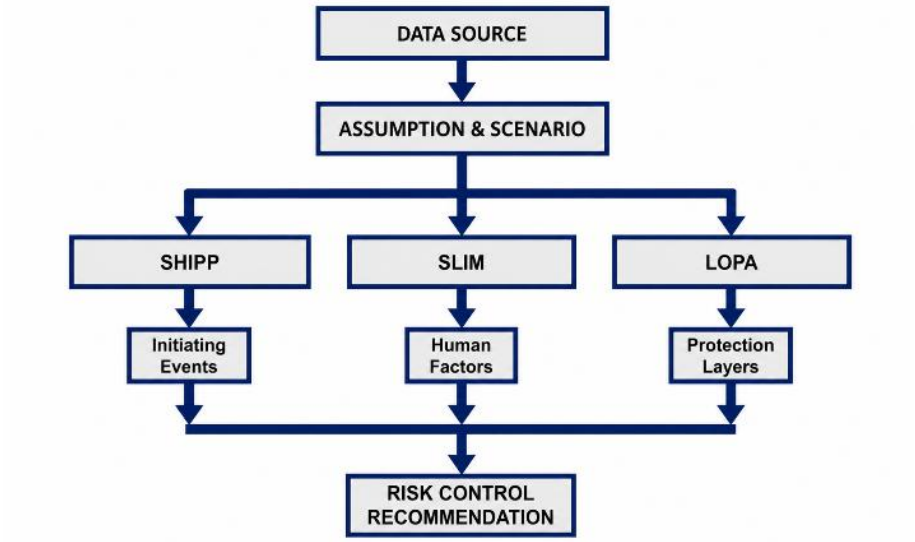

Figure 1. Proposed integrated risk assessment framework for gasoline tank overfill analysis.

As shown in Figure 1, the assessment began with data-source identification and scenario definition. The data and assumptions were then used in three connected analytical streams. SHIPP was applied to structure initiating events and accident propagation, SLIM was used to quantify human-related failure probability, and LOPA was used to evaluate protection-layer adequacy. The outputs of these analytical streams were integrated to formulate risk-control recommendations and determine the required Safety Integrity Level (SIL) category.

The first phase was system characterization. Technical data for twelve gasoline storage tanks, coded T-03 to T-14, were reviewed using facility documentation, including tank specification records and Piping and Instrumentation Diagrams (P&IDs). Table 1 summarizes the tank dimensions and nominal capacities used in the analysis. The studied facility operates with a gasoline intake rate of 300 kL/h and relies on manual gate valves for transfer control. This operating condition was considered critical because a 300 kL/h intake rate is equivalent to 5,000 L/min, or approximately 83.33 L/s. Therefore, delayed manual response during an overfill condition may rapidly increase the volume of released gasoline. This conversion was used to characterize the response-time constraint in the overfill scenario, not to represent a measured release frequency.

Table 1. Gasoline storage tank specifications used in the overfill assessment

Tank ID	Diameter (m)	Height (m)	Capacity (kL)
T-03	17	11	2400
T-04	17	6	1500
T-05	17	10	2000

Tank ID	Diameter (m)	Height (m)	Capacity (kL)
T-06	12	9	1000
T-07	20	12	3000
T-08	12	9	1000
T-09	20	9	2500
T-10	19	9	2500
T-11	17	11	2400
T-12	17	10	2400
T-13	16	10	2000
T-14	20	10	3000

The second phase was hazard identification. A Hazard and Operability (HAZOP) study was conducted to identify credible deviations related to gasoline filling and tank overfill. The HAZOP review followed the guide-word logic recommended in IEC 61882, in which process deviations are systematically examined by considering causes, consequences, existing safeguards, and possible recommendations [14]. In this study, the HAZOP focused on level-related deviations during gasoline transfer, particularly the "More Level" deviation, because this deviation directly represents the overfill condition under high-flow operation.

The third phase was consequence modeling. ALOHA software was used to estimate the potential consequence zones of a major gasoline spill scenario. ALOHA was selected because it is designed to model accidental chemical releases and estimate threat zones associated with toxic vapor dispersion, thermal radiation from fires, and blast effects [15]. Because commercial gasoline is a mixture of volatile hydrocarbons, n-hexane was used as a representative flammable component for dispersion and consequence modeling. The modeled environmental condition represented a conservative nighttime dispersion scenario, with an ambient temperature of 30°C, relative humidity of 70%, wind speed of 2.22 m/s, and atmospheric stability class F. These inputs were used to estimate the potential spatial extent of hazardous vapor dispersion and thermal or flammable threat zones. The consequence results should therefore be interpreted as scenario-based estimates under the specified model inputs, not as universal consequence distances for all gasoline overfill events.

The fourth phase was human reliability assessment. The Success Likelihood Index Method (SLIM) was applied to estimate Human Error Probability (HEP) for operator actions associated with manual level monitoring, communication, and valve operation. SLIM was selected because it allows operator performance to be quantified using Performance Shaping Factors (PSFs), such as workload, procedure clarity, training adequacy, communication quality, and available response time [8]. For each critical operator task, PSF ratings and normalized weights were used to obtain a Success Likelihood Index (SLI). The SLI was then converted into Probability of Success (POS) using calibration constants derived from expert judgment. The relationship is expressed as follows:

$$\log_{10}(POS) = a(SLI) + b \quad (1)$$

where Log(POS) is the base-10 logarithm of the probability of success, SLI is the Success Likelihood Index, and a and b are calibration constants. After Log(POS) was obtained, POS was calculated as:

$$POS = 10^{\log_{10}(POS)} \quad (2)$$

where POS is the probability that the operator successfully completes the required action. The Human Error Probability was then calculated as:

$$HEP = 1 - POS \quad (3)$$

where HEP represents the probability of operator failure for the analyzed task. The calculated HEP values were then used as human-related failure inputs in the sequential accident modeling. Because field-based simulator data and facility-specific operator response records were not available, the PSF ratings, normalized weights, and calibration boundaries were treated as expert-based modeling inputs. Therefore, the resulting HEP values should be interpreted as scenario-specific estimates for the modeled manual overfill response, rather than as directly observed operator failure frequencies. This assumption was carried forward into the SHIPP and ETA calculations.

The fifth phase was dynamic accident modeling. The System Hazard Identification, Prediction and Prevention (SHIPP) methodology was used to structure the accident pathway from the initiating overfill event to possible major fire or explosion outcomes. SHIPP was applied because it supports sequential representation of initiating events, barrier functions, and accident escalation pathways [10]. In this study, safeguards were grouped into four sequential barrier categories: Release Prevention Barrier (RPB), Dispersion Prevention Barrier (DPB), Ignition Prevention Barrier (IPB), and Escalation Prevention Barrier (EPB). Human-related failure probabilities were obtained from the SLIM calculation. Because facility-specific mechanical failure records were not available, equipment-related probabilities were adopted as scenario-modeling inputs and used for conservative screening of the barrier model. These values should therefore be interpreted as adopted input assumptions, not as independently verified facility-specific failure rates. Event Tree Analysis (ETA) was then used to map the progression from the initiating event through the sequential barrier states and to calculate the probability of the final major fire/explosion scenario. This approach is consistent with quantitative risk-analysis practice, in which event-tree logic is used to represent accident progression through successful or failed safety functions [16].

The final phase was protection-layer evaluation and SIL specification. Layer of Protection Analysis (LOPA) was used to evaluate whether existing safeguards could provide valid Probability of Failure on Demand (PFD) credits as Independent Protection Layers (IPLs). The LOPA step followed the principle that a protection layer should be independent, auditable, reliable, and capable of reducing the frequency or consequence of the defined scenario [11]. The analysis also referred to API 2350 for tank overfill prevention requirements and IEC 61511 for functional-safety and Safety Instrumented System requirements in the process industry [12], [13]. For the annualized risk comparison, the initiating event frequency was assumed to be 1.0 demand per year. No additional enabling condition or conditional modifier was credited unless explicitly represented in the ETA structure. Therefore, the ETA-derived scenario probability was interpreted as an annualized scenario frequency for comparison with the adopted tolerable risk target of 1.0×10^{-4} per year. The required Risk Reduction Factor (RRF) was determined from the ratio between the calculated scenario frequency and the target risk. The resulting RRF was then used to identify the required SIL category for the proposed automated safety function.

RESULTS AND DISCUSSION

Facility Configuration and Overfill Scenario

The studied fuel terminal consisted of twelve atmospheric gasoline storage tanks, identified as T-03 to T-14. All tanks used the same transfer-entry arrangement and were operated under a gasoline intake rate of 300 kL/h. The transfer system relied on conventional manual gate valves, which required field operators to stop the inflow manually using a handwheel. The simplified Piping and Instrumentation Diagram (P&ID) in Figure 2 shows the transfer configuration evaluated in this study. Based on the available diagram and facility description, the observed configuration did not include automated shut-off valves, remote

actuation mechanisms, or independent High-Level Alarms (HLA). Therefore, the transfer operation depended on local level observation, manual valve operation, and communication between field operators and the pump house.

At the specified transfer rate, the incoming gasoline flow was equivalent to 5,000 L/min, or approximately 83.33 L/s. This value was used as the scenario basis for modeling the overfill condition and evaluating the consequence of delayed manual intervention during high-flow filling. The value represents the modeled inflow condition used in this study and should not be interpreted as a measured failure frequency.

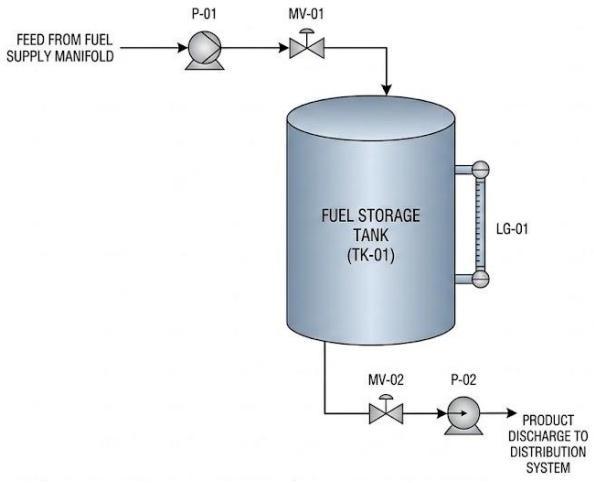

TABLE I

EQUIPMENT & INSTRUMENTATION LEGEND	
TAG	FUNCTIONAL DESCRIPTION
TK-01	Bulk Fuel Storage Tank
P-01	Feed Transfer Pump (Centrifugal)
P-02	Discharge Transfer Pump (Positive Disp.)
MV-01	Manual Feed Isolation Valve (Inlet)
MV-02	Manual Discharge Isolation Valve (Outlet)
LG-01	Level Indicating Sight Glass (Gage)

PIPING & SYMBOL LEGEND

SYMBOL	DESCRIPTION
	PROCESS LINE (Primary Fluid Flow)
	PUMP (Generic, e.g., Centrifugal)
	MANUAL VALVE (Isolation Type)
	LEVEL GAUGE (Tubular-type)

Figure 2. Simplified Piping and Instrumentation Diagram of the gasoline storage tank transfer system.

ALOHA Consequence Modeling Results

ALOHA modeling was conducted to estimate the potential hazardous zones generated by the gasoline overfill scenario. Because the model requires a defined chemical input, n-hexane was selected as a representative flammable surrogate for the gasoline spill scenario. This selection was treated as a modeling assumption because commercial gasoline is a mixture of hydrocarbons and is not identical to n-hexane. The modeled meteorological condition used an ambient temperature of 30°C, relative humidity of 70%, wind speed of 2.22 m/s, and atmospheric stability class F. These values were applied as the specified scenario inputs for consequence modeling.

The flammable vapor-cloud modeling result is presented in Figure 3. The Red Threat Zone, corresponding to 100% of the Lower Explosive Limit (LEL), extended 64 m from the release source. The Orange Threat Zone, corresponding to 60% LEL, extended 83 m. The Yellow Threat Zone, corresponding to 10% LEL, extended 222 m. These results indicate the modeled spatial extent of flammable vapor concentration under the selected n-hexane surrogate and meteorological assumptions.

Figure 3. Flammable vapor-cloud threat zones generated from the modeled gasoline overfill scenario.

The pool-fire consequence modeling result is presented in Figure 4. The modeled scenario was applied to tank T-14 as the selected pool-fire case in this study. Under the specified model inputs, the Red Threat Zone extended 138 m from the source at a thermal radiation level above 10.0 kW/m^2. The Yellow Threat Zone extended 301 m from the source. These distances represent the modeled thermal-radiation threat zones under the specified scenario assumptions.

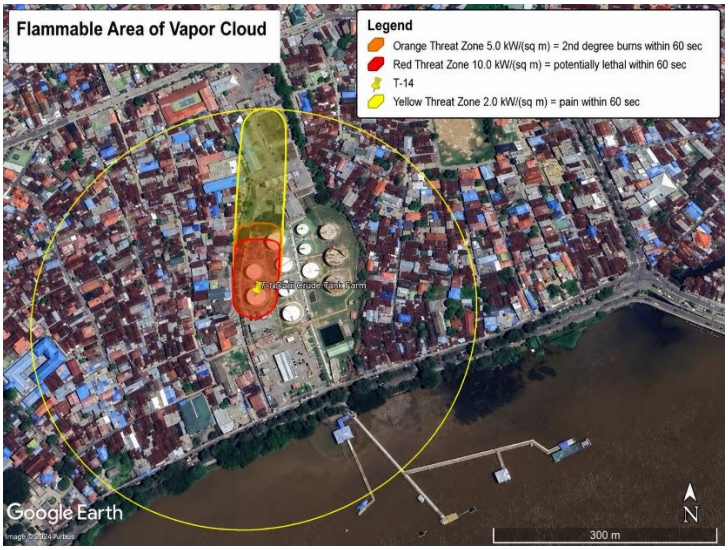

Figure 4. Pool-fire thermal radiation threat zones for the modeled gasoline overfill scenario.

Error Mode Identification and Performance Shaping Factors

Human error modes were identified from historical overfill and fire/explosion incident mechanisms reported in the Buncefield and CAPECO investigation reports [17], [18]. These historical failure mechanisms were then mapped against the observed facility configuration, particularly the use of manual gate valves, local level observation, and the absence of independent High-Level Alarms. Table 2 summarizes the five error modes selected for SLIM-based human reliability assessment.

Table 2. Error modes used for SLIM-based human reliability assessment

No.	Error Mode	Source
1	Field operators did not perform the required hourly manual level checks or manual dipping.	[17]
2	Control room operators failed to recognize that the tank level remained static while the pump was operating.	[18]
3	Technicians forgot to re-enable safety systems, such as alarms or switches, after testing or maintenance.	[18]
4	Communication failure occurred between pipeline operators and tank operators during emergency pump-shutdown coordination.	[18]
5	Critical information regarding the tank being filled and the last known level status was not clearly communicated during shift handover.	[17]

The identified error modes were evaluated using five Performance Shaping Factors (PSFs): procedures, training, workload, communication quality, and supervision. These PSFs were used to represent operational conditions that may affect operator performance during manual transfer control. The PSFs used in the SLIM assessment are presented in Table 3.

Table 3. Performance Shaping Factors used in the SLIM assessment

PSF	Description	Source
Procedures	Adequacy, clarity, and enforcement of written operating and maintenance procedures, including compliance with required safety checks.	[8]
Training	Level of operator and technician knowledge, skill, and understanding of system behavior, failure modes, and safety consequences.	[8]
Workload	Physical and cognitive task demand imposed on personnel, including time pressure, multitasking, and staffing level.	[8]
Communication Quality	Effectiveness, reliability, and clarity of information exchange between operators, control room, and field personnel during abnormal conditions.	[8]
Supervision	Effectiveness of oversight, monitoring, and enforcement of safe work practices by supervisors and management.	[8]

SLIM-Based Human Error Probability Results

The Success Likelihood Index Method (SLIM) was applied by scoring the five error modes against the five PSFs. Each PSF was assigned a normalized weight, and each error mode was rated according to the corresponding PSF condition. The weighted PSF ratings were then summed to obtain the Success Likelihood Index (SLI). The resulting SLI values ranged from 61.00 to 67.00, as shown in Table 4.

Table 4. Success Likelihood Index calculation based on PSF weight and rating

PSF	NORMALIZED WEIGHT	EM 1		EM 2		EM 3	
		PSF Rating	P1	PSF Rating	P2	PSF Rating	P3
Procedures	0.26	80	20.57	40	10.29	95	24.43
Training	0.29	60	17.14	95	27.14	70	20.00

PSF	NORMALIZED WEIGHT	EM 1		EM 2		EM 3	
		PSF Rating	P1	PSF Rating	P2	PSF Rating	P3
Workload	0.17	95	16.29	85	14.57	60	10.29
Communication Quality	0.20	30	6.00	50	10.00	40	8.00
Supervision	0.09	70	6.00	20	1.71	50	4.29
SLI	**1.00**		**66.00**		**63.71**		**67.00**

PSF	NORMALIZED WEIGHT	EM 4		EM 5	
		PSF Rating	P4	PSF Rating	P5
Procedures	0.26	70	18.00	90	23.14
Training	0.29	60	17.14	30	8.57
Workload	0.17	20	3.43	60	10.29
Communication Quality	0.20	95	19.00	90	18.00
Supervision	0.09	40	3.43	40	3.43
SLI	**1.00**		**61.00**		**63.43**

The SLI values were converted into Probability of Success (POS) and Human Error Probability (HEP) using the SLIM calibration constants. Table 5 presents the calibration boundaries, constant values, POS, and HEP for each error mode. The highest HEP was obtained for EM4, communication failure during emergency pump-shutdown coordination, with a value of 0.040843. The second highest HEP was obtained for EM5, shift-handover information failure, with a value of 0.038409. EM2, failure to recognize a static tank level while the pump was operating, produced a HEP of 0.038123.

Table 5. SLIM calibration and Human Error Probability results

Error Mode	HEP Best Case	HEP Worst Case	a Constant	b Constant	Log(POS)	POS	HEP
EM1	10^{-4}	10^{-2}	0.000043	-0.004365	-0.001513	0.996523	0.003477
EM2	10^{-3}	10^{-1}	0.000453	-0.045757	-0.01688	0.961877	0.038123
EM3	10^{-4}	10^{-2}	0.000043	-0.004365	-0.001469	0.996622	0.003378
EM4	10^{-3}	10^{-1}	0.000453	-0.045757	-0.01811	0.959157	0.040843
EM5	10^{-3}	10^{-1}	0.000453	-0.045757	-0.01701	0.961591	0.038409

SHIPP and Event Tree Analysis Results

The human error probabilities obtained from SLIM were used as human-related inputs in the SHIPP and Event Tree Analysis. The accident pathway was organized into four sequential prevention barriers: Release Prevention Barrier (RPB), Dispersion Prevention Barrier (DPB), Ignition Prevention Barrier (IPB), and Escalation Prevention Barrier (EPB). Figure 5 presents the RPB and DPB structures, while Figure 6 presents the IPB and EPB structures.

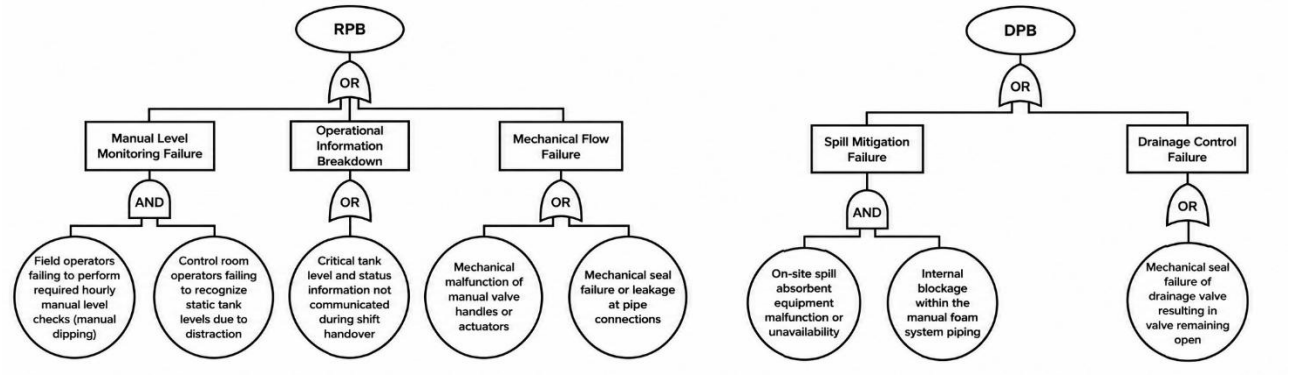

Figure 5. Release Prevention Barrier and Dispersion Prevention Barrier structures.

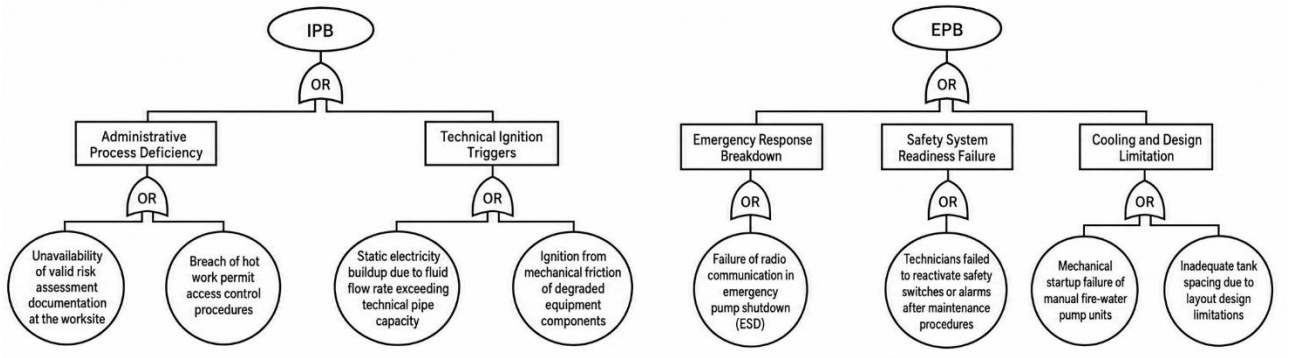

Figure 6. Ignition Prevention Barrier and Escalation Prevention Barrier structures.

The basic event probabilities used in the barrier calculation are presented in Table 6. The human-related probabilities were obtained from the SLIM results in Table 5. The equipment-related probabilities were retained as adopted basic-event inputs in the study because the available manuscript data do not provide a separate mechanical reliability database or facility-specific failure-rate record. Therefore, these equipment-related values should be interpreted as input assumptions for the barrier model rather than independently verified mechanical reliability data.

Table 6. Basic event probabilities used in the SHIPP and ETA calculations

No.	Basic Event	Barrier	Probability	Source
1	Mechanical malfunction of manual valve handles or actuators	RPB1	5.0×10^{-2}	Adopted study input
2	Mechanical seal failure or leakage at pipe connections	RPB2	5.0×10^{-7}	Adopted study input
3	Mechanical seal failure of the drainage valve	DPB1	4.0×10^{-5}	Adopted study input
4	On-site spill absorbent equipment malfunction	DPB2	1.0×10^{-1}	Adopted study input
5	Internal blockage within the manual foam-system piping	DPB3	8.0×10^{-1}	Adopted study input
6	Static electricity buildup due to flow exceedance	IPB1	1.0×10^{-1}	Adopted study input
7	Ignition from mechanical friction of degraded components	IPB2	1.0×10^{-1}	Adopted study input

No.	Basic Event	Barrier	Probability	Source
8	Unavailability of valid risk-assessment documentation	IPB3	1.0×10^{-1}	Adopted study input
9	Breach of hot-work permit access control	IPB4	1.0×10^{-2}	Adopted study input
10	Mechanical startup failure of manual fire-water pump	EPB1	8.0×10^{-1}	Adopted study input
11	Inadequate tank spacing or layout-design failure	EPB2	1.0×10^{-2}	Adopted study input
12	Field operators failed to perform required hourly manual level checks or manual dipping	RPB3	3.5×10^{-3}	Table 5
13	Control room operators failed to recognize static tank levels during pump operation	RPB4	3.8×10^{-2}	Table 5
14	Critical tank level and status information was not communicated during shift handover	RPB5	3.8×10^{-2}	Table 5
15	Failure of radio coordination for emergency pump shutdown	EPB3	4.1×10^{-2}	Table 5
16	Technicians failed to re-enable safety switches or alarms after maintenance	EPB4	3.4×10^{-3}	Table 5

Note: Equipment-related probabilities in Table 6 were adopted as scenario-modeling inputs for the barrier calculation because facility-specific mechanical failure-rate records were not available. These values were used to support conservative screening within the SHIPP–ETA framework and should not be interpreted as directly measured reliability data from the studied facility.

The barrier failure probabilities were calculated using the Boolean logic represented in Figure 5 and Figure 6. The calculation assumed statistical independence among basic events. AND-type combinations were represented by multiplication. OR-type combinations were represented using an additive approximation because the analysis was intended as a conservative screening model for SIL specification. Since several adopted basic-event probabilities were not very small, the additive OR-gate approximation may overestimate the exact union probability. Therefore, the calculated barrier values should be interpreted as model-based screening estimates under the adopted assumptions rather than exact measured barrier-failure probabilities. Under this approximation, the calculation expressions are shown below.

$$RPB = RPB_1 + RPB_2 + (RPB_3 \times RPB_4) + RPB_5 = 8.9 \times 10^{-2} \quad (4)$$

$$DPB = DPB_1 + (DPB_2 \times DPB_3) = 8.0 \times 10^{-2} \quad (5)$$

$$IPB = IPB_1 + IPB_2 + IPB_3 + IPB_4 = 3.1 \times 10^{-1} \quad (6)$$

$$EPB = EPB_1 + EPB_2 + EPB_3 + EPB_4 = 8.54 \times 10^{-1} \quad (7)$$

The Event Tree Analysis result is presented in Figure 7. Based on the ETA structure and the barrier probabilities calculated in this study, the probability of the major fire/explosion outcome, identified as Outcome S5, was 1.88×10^{-3} per year.

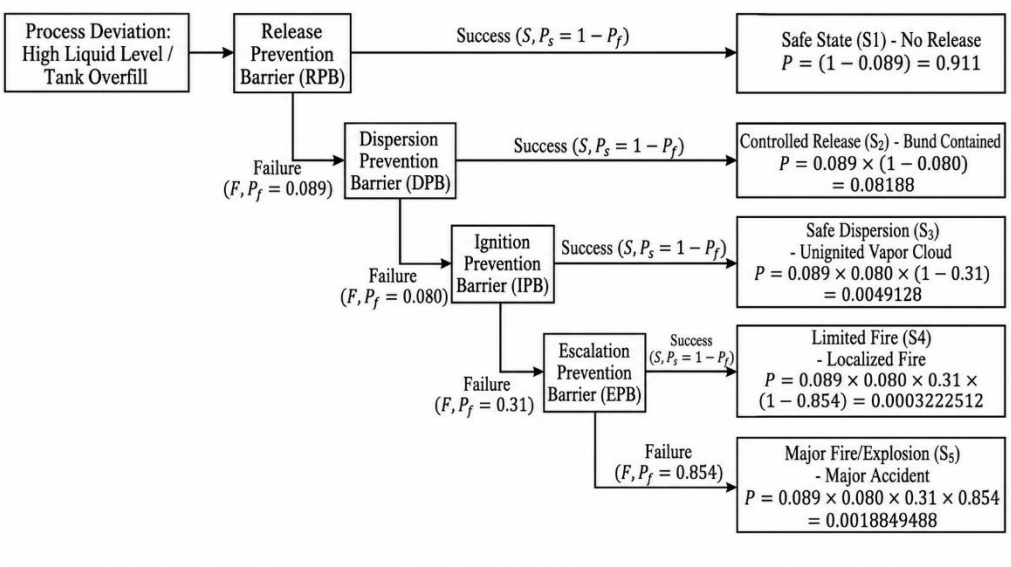

Figure 7. Event Tree Analysis for the gasoline tank overfill scenario.

HAZOP Results

A HAZOP study was conducted on the gasoline storage tank node. The guide words "More," "Less," and "No" were applied to the process parameters of level, pressure, and flow. Risk ranking was determined using the 5 × 5 risk matrix adopted in this study, where severity ranged from 1 to 5 and likelihood ranged from 1 to 5. The scores were applied to classify the relative priority of deviations in the HAZOP worksheet. The HAZOP worksheet is presented in Table 7, and the risk matrix is presented in Table 8.

Table 7. HAZOP worksheet for gasoline storage tank operation

HAZOP			**Project :** Storage Facility RA					
			SYSTEM : Gasoline Storage Tank					
P&ID : Gasoline Storage Tank			**EQUIPMENT :** Gasoline Storage Tank, Pump, Valve, Level Glass					
No	**Deviation**	**Causes**	**Consequences**	**Risk Ranking**			**Safeguards**	**Action Required**
				S	**L**	**RR**		
1	More level	Input valve left open	Tank overfill	5	5	25	Level Glass	Mandatory hourly manual dipstick gauging to verify level glass.
2	Less Level	Output pump runs too long	Output pump damage	3	3	9	Level Glass	Establish "Minimum Level" mark on tank.

HAZOP			**Project :** Storage Facility RA					
			SYSTEM : Gasoline Storage Tank					
P&ID : Gasoline Storage Tank			**EQUIPMENT :** Gasoline Storage Tank, Pump, Valve, Level Glass					
3	More Pressure	High gasoline temperature	Tank rupture	5	2	10	Vent	Ensure a manual vent valve is opened before any transfer.
4	Less Pressure	Sudden cooling of tank	Tank implosion	4	2	8	-	Mandatory "Open Vent" procedure during discharge.
5	No Flow	Input valve closed	Empty tank	1	3	3	Manual check of valve	Use "Open/Closed" position tags on all manual valves.
6	Less Flow	Input valves are not perfectly open	Low capacity	2	1	2	Manual check of valve	Use "Open/Closed" position tags on all manual valves.
7	More Flow	Input pump surge	Tank overfill	5	4	20	Level Glass	Mandatory hourly manual dipstick gauging to verify level glass.

Table 8. Risk matrix used for HAZOP ranking

	Likelihood				
Severity	**1**	**2**	**3**	**4**	**5**
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

The HAZOP results showed that “More Level” had the highest risk ranking, with a risk score of 25. The second highest ranking was obtained by “More Flow,” with a risk score of 20. These two deviations were therefore identified as the main level- and flow-related deviations requiring further protection-layer evaluation.

LOPA and SIL Specification Results

LOPA was conducted for the critical overfill-related deviations identified in the HAZOP. As defined in the Method, the initiating event frequency was assumed to be 1.0 demand per year for the purpose of annualized LOPA comparison. The scenario probability obtained from the ETA was 1.88×10^{-3} per year. This value was compared with the adopted tolerable risk target of 1.0×10^{-4} per year. In the LOPA calculation, the existing manual safeguards and process-design features were not assigned risk-reduction credit because the available data indicate that the system lacked automated logic, remote actuation, and independent High-Level Alarm protection. Therefore, the evaluated protection layers were treated as having a Probability of Failure on Demand value of 1.0 for the purpose of the RRF calculation. Under this assumption, the scenario probability remained 1.88×10^{-3} per year.

The Risk Reduction Factor required to meet the adopted target was calculated as follows:

$$RRF = \frac{1.88 \times 10^{-3}}{1.0 \times 10^{-4}} = 18.8 \quad (8)$$

The calculated RRF of 18.8 falls within the SIL 1 risk-reduction range used in the study and is consistent with the SIL/PFD range specified in IEC 61511 [13]. Therefore, the overfill scenario was classified as requiring SIL 1-level risk reduction for the proposed automated safety function. Table 9 summarizes the protection layers identified for each HAZOP deviation.

Table 9. Layer of Protection Analysis worksheet for the gasoline storage tank

Layer of Protection Analysis (LOPA) - Gasoline Storage Tank

No	Parameter	Deviation	Scenario (Consequence)	Layer 1	Layer 2	Layer 3	Layer 4
1	More	Level	Tank overfill, spill, pool fire, and potential fatalities	Process Design	-	-	-
2	Less	Level	Output pump damage; Large explosive vapor space	Process Design	-	-	-
3	More	Pressure	Tank rupture; Catastrophic shell failure	Process Design	-	-	-
4	Less	Pressure	Tank implosion / Collapse	-	-	-	-
5	No	Flow	Empty tank; Operational delay; Loss of production	Process Design	-	-	-
6	Less	Flow	Low capacity; Operational inefficiency	Process Design	-	-	-
7	More	Flow	Tank overfill, spill, pool fire, and potential fatalities	Process Design	-	-	-

Note: The protection layers listed in Table 9 represent existing safeguard categories identified during the LOPA review. They were not assigned formal IPL credit in the RRF calculation unless they met the independence, reliability, auditability, and functional criteria required for credited protection layers.

Discussion

The results of this study indicate that the overfill risk in the studied gasoline storage facility is shaped by the interaction between high-flow transfer, manual level control, human reliability limitations, and sequential barrier degradation. As shown in Figure 2, the evaluated transfer configuration relies on manual gate valves, local level observation, and communication between field operators and the pump house, while the available system description does not indicate independent High-Level Alarm (HLA), remote actuation, or automated shutdown functions. Under the modeled 300 kL/h filling condition, this configuration narrows the available response window because a delay in detection, communication, or manual valve closure may rapidly increase the released gasoline volume. This finding strengthens previous storage-tank risk studies by showing that overfill risk should not be interpreted only from consequence severity, but also from the reliability of detection, communication, barrier response, and protection-layer independence [5], [6], [16].

The SLIM results explain why manual safeguards become vulnerable under high-flow transfer conditions. Based on Table 5, the highest Human Error Probability (HEP) was obtained for communication failure during emergency pump-shutdown coordination (EM4 = 0.040843), followed by shift-handover information failure (EM5 = 0.038409) and failure to recognize static tank-level indication during pumping (EM2 = 0.038123). These values do not mean that operators will necessarily fail in every emergency condition. Rather, they indicate that communication, situation awareness, and information transfer are the most vulnerable human-related elements in the modeled scenario. This interpretation is consistent with recent Human Reliability Assessment studies showing that fire and explosion risk is strongly influenced by workload, procedure clarity, communication quality, training, and supervision [7]–[9]. It also extends recent process-safety management studies by showing that organizational and communication factors can be translated into quantitative accident-propagation inputs rather than being discussed only as qualitative contributors [19]–[21].

The integrated framework used in this study provides a more traceable interpretation than applying HAZOP, ALOHA, SLIM, ETA, or LOPA separately. HAZOP identifies the critical deviation, ALOHA estimates the spatial consequence under defined assumptions, SLIM quantifies human-related failure probability, SHIPP and ETA represent the sequential failure pathway, and LOPA links the calculated scenario probability to the required risk reduction. This integrated logic is consistent with SHIPP-based accident modeling, which emphasizes the progression from initiating events to prevention-barrier failure [10]. It also extends recent integrated risk-assessment approaches in chemical and petroleum systems by applying them to a high-flow gasoline tank overfill scenario where manual safeguards remain the dominant protection mechanism [22], [23].

The SHIPP and ETA results clarify how the overfill scenario can progress through the Release Prevention Barrier (RPB), Dispersion Prevention Barrier (DPB), Ignition Prevention Barrier (IPB), and Escalation Prevention Barrier (EPB). Figures 5 and 6 show that each barrier consists of several human-related and equipment-related basic events. Based on the additive OR-gate approximation adopted in the Results, Table 6 produces barrier failure probabilities of 8.9×10^{-2} for RPB, 8.0×10^{-2} for DPB, 3.1×10^{-1} for IPB, and 8.54×10^{-1} for EPB. The EPB value is therefore retained in this discussion because it is consistent with the current calculation basis in the manuscript: $EPB = 8.0 \times 10^{-1} + 1.0 \times 10^{-2} + 4.1 \times 10^{-2} + 3.4 \times 10^{-3} = 8.544 \times 10^{-1}$, rounded to 8.54×10^{-1}. However, this value should be interpreted as a model-based result under the adopted Boolean approximation and input assumptions, not as a directly measured field failure rate. This cautious interpretation is important because recent dynamic risk-evolution studies emphasize that accident progression in chemical processes may be sensitive to dependency assumptions, barrier interactions, and changing operational states [24], [25].

The HAZOP results further support the selection of overfill-related deviations as the main analytical focus. As shown in Table 7 and Table 8, the "More Level" deviation obtained the highest risk ranking, with a score of 25, while "More Flow" obtained the second-highest score of 20. These two deviations are closely connected because excessive inflow or delayed shutdown can increase the likelihood of tank overfill under high-flow operation. Nevertheless, the HAZOP score should be interpreted as a risk-prioritization result rather than a direct measurement of accident frequency. Its role in this study is to justify why the overfill scenario requires further quantitative evaluation through ALOHA, SLIM, SHIPP, ETA, and LOPA.

The ALOHA consequence modeling results in Figure 3 and Figure 4 show why the overfill scenario has implications beyond routine operational disruption. Figure 3 indicates that the modeled vapor-cloud threat zones extend up to 64 m at 100% LEL, 83 m at 60% LEL, and 222 m at 10% LEL. Figure 4 indicates that the modeled pool-fire thermal radiation zones extend to 138 m for the Red Threat Zone and 301 m for the Yellow Threat Zone. These results should not be interpreted as universal consequence distances for all gasoline overfill events because they depend on the selected n-hexane surrogate, meteorological inputs, source assumptions, and ALOHA modeling constraints [15]. However, they provide a conservative spatial basis for understanding why delayed manual response may create hazardous conditions beyond the immediate tank area. This interpretation is consistent with previous fire and explosion modeling studies showing that release volume, volatility, atmospheric condition, ignition pathway, and source characteristics influence the extent of hazardous zones [1]–[5].

Benchmarking against the Buncefield and CAPECO incidents shows important similarities but also clarifies the contribution of the present study. The similarity lies in the role of level-monitoring failure, weak or unavailable independent alarm protection, inadequate response to abnormal filling conditions, and communication breakdown during storage or transfer operations [17], [18]. However, this study does not claim that the studied facility will necessarily experience the same accident sequence. Instead, the comparison is used to show that the structural vulnerabilities identified in the present facility are consistent with failure mechanisms documented in major historical incidents. The contribution of this study is that these historical lessons are translated into a prospective quantitative workflow by combining SLIM-derived HEP, SHIPP barrier logic, ETA outcome probability, and LOPA-based RRF calculation.

The LOPA result provides the basis for specifying automation as a risk-reduction requirement. As summarized in Table 9, the existing safeguards were not credited as valid Independent Protection Layers in the RRF calculation because the available facility configuration does not show independent high-level detection, automated logic, remote actuation, or automatic shutdown. This treatment should not be interpreted as meaning that manual procedures have no operational value. Manual level checks, operator communication, shift handover, valve-position confirmation, and emergency coordination remain important administrative controls. However, under the LOPA assumption used in this study, these controls are not treated as independent credited IPLs because they depend on continuous human attention and shared operational conditions. Using the ETA-estimated major fire/explosion probability of 1.88×10^{-3} per year and the adopted target risk of 1.0×10^{-4} per year, the required Risk Reduction Factor is 18.8. This value falls within the SIL 1 range used in the study and supports the specification of an independent high-level detection and automated shutdown function to supplement existing manual safeguards [11]–[13], [26], [27].

From a practical perspective, the findings imply that risk reduction should combine administrative, instrumented, and passive controls. Administrative procedures remain necessary for operating discipline, but the results indicate that they should not be the only relied-upon protection mechanism for high-flow overfill prevention. The main risk-reduction

measure supported by the LOPA result is an independent Safety Instrumented System that includes high-high level detection, logic processing, and automatic isolation or pump shutdown. In addition, passive secondary containment, such as a properly designed containment dike, may be considered as a complementary mitigation measure because the ALOHA results indicate potentially extensive vapor-cloud and pool-fire zones. However, the containment dike is not assigned formal LOPA credit in this study because its quantitative effect on spill spreading, evaporation, vapor dispersion, and thermal-radiation distance was not modeled. Therefore, any formal claim regarding its risk-reduction credit should be supported by additional consequence modeling or facility-specific engineering assessment.

Several limitations should be acknowledged. First, the study is site-specific and should not be generalized to gasoline storage facilities with different tank dimensions, transfer rates, instrumentation, operating procedures, or emergency-response resources. Second, the ALOHA analysis used n-hexane as a representative flammable surrogate for gasoline. This assumption is useful for scenario modeling, but it cannot fully represent the physical and combustion behavior of complex commercial gasoline blends. Third, the SLIM analysis depends on PSF ratings and calibration assumptions, which introduces uncertainty into the HEP values. Fourth, the ETA and LOPA calculations assume statistical independence and use adopted basic-event probabilities, whereas real facilities may contain dependencies caused by shared operators, shared procedures, common maintenance practices, communication channels, and organizational conditions. Future work should therefore include sensitivity analysis, facility-specific reliability data, empirical validation of operator response time, and dependency modeling among protection layers.

CONCLUSION

This study integrated HAZOP, ALOHA, SLIM, SHIPP, ETA, and LOPA to assess manual safeguard failure in a high-flow gasoline tank overfill scenario. Under the modeled 300 kL/h transfer condition, the analysis showed that dependence on manual gate valves, local level observation, and operator communication created a risk profile that exceeded the adopted tolerable risk target. The SLIM results indicated that communication failure during emergency pump-shutdown coordination, shift-handover information failure, and failure to recognize abnormal level conditions were the most critical human-related vulnerabilities. Under the adopted modeling assumptions and the assumed initiating event frequency of 1.0 demand per year, the sequential barrier analysis estimated a major fire/explosion scenario frequency of 1.88×10^{-3} per year, while the consequence modeling indicated that hazardous vapor and thermal-radiation zones could extend beyond the immediate tank area.

The required Risk Reduction Factor was calculated as 18.8, indicating the need for SIL 1-level risk reduction for the proposed automated safety function. Therefore, the findings support the implementation of an independent high-level detection and automated shutdown function to supplement, rather than replace, existing manual procedures. The study contributes a traceable risk-assessment workflow that links human reliability, accident propagation, and protection-layer adequacy for overfill prevention in gasoline storage facilities. Future work should strengthen the analysis by incorporating facility-specific reliability data, sensitivity analysis, and field-based validation of operator response time and communication reliability.

REFERENCES

[1] L. Li and L. Dai, “Review on fire explosion research of crude oil storage tank,” E3S Web of Conferences, vol. 236, Art. no. 01022, 2021, doi: 10.1051/e3sconf/202123601022.

[2] K. Sarvestani, O. Ahmadi, and M. J. Alenjareghi, "LPG storage tank accidents: Initiating events, causes, scenarios, and consequences," Journal of Failure Analysis and Prevention, vol. 21, no. 4, pp. 1305–1314, 2021, doi: 10.1007/s11668-021-01174-y.
[3] H. Hisken, L. Mauri, G. Atanga, et al., "Assessing the influence of real releases on explosions: Selected results from large-scale experiments," Journal of Loss Prevention in the Process Industries, vol. 72, Art. no. 104561, 2021, doi: 10.1016/j.jlp.2021.104561.
[4] A. R. Ramadhani and A. Halfan, "Fire and explosion modelling of a gas transmission pipeline in a populated residential area," MOTIVECTION: Journal of Mechanical, Electrical and Industrial Engineering, vol. 6, no. 2, pp. 177–190, 2024, doi: 10.46574/motivection.v6i2.327.
[5] H. Mohammadi, F. Laal, F. Mohammadian, P. Yari, M. Kangavari, and S. M. Hanifi, "Dynamic risk assessment of storage tank using consequence modeling and fuzzy Bayesian network," Heliyon, vol. 9, no. 8, Art. no. e18842, 2023, doi: 10.1016/j.heliyon.2023.e18842.
[6] J. Xue, G. Reniers, J. Li, M. Yang, C. Wu, and P. H. A. J. M. van Gelder, "A bibliometric and visualized overview for the evolution of process safety and environmental protection," International Journal of Environmental Research and Public Health, vol. 18, no. 11, Art. no. 5985, 2021, doi: 10.3390/ijerph18115985.
[7] N. N. H. Tananta and A. R. Ramadhani, "Human reliability assessment (HRA) of fire and explosion cases at fuel filling stations (SPBU)," MOTIVECTION: Journal of Mechanical, Electrical and Industrial Engineering, vol. 6, no. 1, pp. 13–24, 2024, doi: 10.46574/motivection.v6i1.285.
[8] M. Z. Ramdhan, D. A. Rizq, A. Senna, and A. R. Ramadhani, "A comparative study of Human Reliability Assessment using Success Likelihood Index Method (SLIM) and Human Error Assessment & Reduction Technique (HEART): A case study from a Boeing 737 Max accident," MOTIVECTION: Journal of Mechanical, Electrical and Industrial Engineering, vol. 7, no. 1, pp. 61–74, 2025, doi: 10.46574/motivection.v7i1.431.
[9] F. P. Hanem and A. R. Ramadhani, "Bayesian Network Integration of Event Tree and SLIM-Based Human Reliability for Fire and Explosion Risk Assessment: BP-Husky Toledo Refinery Case Study," MOTIVECTION: Journal of Mechanical, Electrical and Industrial Engineering, vol. 7, no. 3, pp. 363–378, 2025, doi: 10.46574/motivection.v7i3.486.
[10] S. Rathnayaka, F. Khan, and P. Amyotte, "Accident modeling approach for safety assessment in an LNG processing facility," Journal of Loss Prevention in the Process Industries, vol. 25, no. 2, pp. 414–423, 2012, doi: 10.1016/j.jlp.2011.09.006.
[11] Center for Chemical Process Safety, Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis. Hoboken, NJ, USA: Wiley, 2015, doi: 10.1002/9781118948743.
[12] American Petroleum Institute, API Standard 2350: Overfill Prevention for Storage Tanks in Petroleum Facilities, 5th ed. Washington, DC, USA: American Petroleum Institute, 2020.
[13] International Electrotechnical Commission, IEC 61511-1:2016+AMD1:2017 CSV, Functional Safety—Safety Instrumented Systems for the Process Industry Sector—Part 1: Framework, Definitions, System, Hardware and Application Programming Requirements. Geneva, Switzerland: IEC, 2017.
[14] International Electrotechnical Commission, IEC 61882:2016, Hazard and Operability Studies (HAZOP Studies)—Application Guide. Geneva, Switzerland: IEC, 2016.
[15] R. Jones, W. Lehr, D. Simecek-Beatty, and R. M. Reynolds, ALOHA® (Areal Locations of Hazardous Atmospheres) 5.4.4: Technical Documentation, NOAA Technical Memorandum NOS OR&R 43. Seattle, WA, USA: Emergency Response Division, NOAA, 2013.
[16] Buncefield Major Incident Investigation Board, The Buncefield Incident 11 December 2005: The Final Report of the Major Incident Investigation Board, vol. 1. London, U.K.: Health and Safety Executive, 2008.

[17] U.S. Chemical Safety and Hazard Investigation Board, Caribbean Petroleum Corporation (CAPECO) Refinery Tank Explosion and Fire, Final Investigation Report. Washington, DC, USA: U.S. Chemical Safety and Hazard Investigation Board, 2015.
[18] M. S. Ab Rahim, G. Reniers, M. Yang, and S. Bajpai, "Risk assessment methods for process safety, process security and resilience in the chemical process industry: A thorough literature review," Journal of Loss Prevention in the Process Industries, vol. 88, Art. no. 105274, 2024, doi: 10.1016/j.jlp.2024.105274.
[19] B. Wang, J. Zhou, and Y. Wang, "Enhancing process safety management through evidence-based process safety management (EBPSM): A theoretical framework and case analysis," Journal of Loss Prevention in the Process Industries, vol. 91, Art. no. 105381, 2024, doi: 10.1016/j.jlp.2024.105381.
[20] Y. Niu, Y. Fan, X. Ju, C. Hao, and X. Yang, "Modeling the causal mechanism in process safety management (PSM) systems from historical accidents," Journal of Loss Prevention in the Process Industries, vol. 89, Art. no. 105298, 2024, doi: 10.1016/j.jlp.2024.105298.
[21] M. Gonyora and E. Ventura-Medina, "Investigating the relationship between human and organisational factors, maintenance, and accidents: The case of chemical process industry in South Africa," Safety Science, vol. 176, Art. no. 106530, 2024, doi: 10.1016/j.ssci.2024.106530.
[22] A. Soltanzadeh, E. Zarei, M. Mahdinia, and M. Sadeghi-Yarandi, "An integrated approach to assess safety and security risks in chemical process industries," Journal of Loss Prevention in the Process Industries, vol. 90, Art. no. 105344, 2024, doi: 10.1016/j.jlp.2024.105344.
[23] F. M. Eltahan, M. Toderas, M. S. Mansour, E. S. Z. El-Ashtoukhy, M. A. Abdou, and F. Shokry, "Applying a semi-quantitative risk assessment on petroleum production unit," Scientific Reports, vol. 14, Art. no. 7603, 2024, doi: 10.1038/s41598-024-57600-2.
[24] Q. Wang, S. Chen, F. Chen, J. Zhang, L. Chen, J. Li, and Z. Dou, "A dynamic assessment method for risk evolution in chemical processes based on MFM-HAZOP-FDBN," Chemical Engineering Research and Design, vol. 204, pp. 471–486, 2024, doi: 10.1016/j.cherd.2024.02.049.
[25] R. Tao, D. Li, H. Shi, S. Pang, Y. Lin, and C. Li, "A quantitative analysis method based on network evolution for risk factors of safety production in chemical enterprises," Scientific Reports, vol. 15, Art. no. 8173, 2025, doi: 10.1038/s41598-025-88279-8.
[26] B. Rabah, R. Younes, C. Djeddi, and L. Laouar, "Optimization of safety instrumented system performance and maintenance costs in Algerian oil and gas facilities," Process Safety and Environmental Protection, vol. 182, pp. 371–386, 2024, doi: 10.1016/j.psep.2023.11.081.
[27] W. Ye, J. Wang, Z. Wei, Z. Wang, and L. Zhang, "SIL assessment of safety instrumented systems in oil and gas stations based on STPA-Bow-tie," Journal of Safety Science and Resilience, vol. 7, no. 2, Art. no. 100251, 2026, doi: 10.1016/j.jnlssr.2025.100251.

This page is intentionally left blank.