

PROBABILISTIC SAFETY AND RELIABILITY ASSESSMENT OF STEAM BOILER INSTRUMENTATION AND CONTROL SYSTEMS IN A UNIVERSITY HOSPITAL: A CASE STUDY FROM PATHUM THANI, THAILAND

Kanutsawan Maksuk and Arroon Ketsakorn^{*}

Received: January 4, 2025; Revised: December 29, 2025; Accepted: January 26, 2026

Abstract

Fires and explosions caused by steam boiler malfunctions can lead to severe injuries, fatalities, and extensive property damage, particularly in hospital environments where uninterrupted and safe operation is essential for patient care. This study evaluated the reliability of a steam boiler at a university hospital by quantifying the overall process failure probability, annual probability of failure, and mean time before failure (MTBF) of its instrumentation and control system components. A Hazard and Operability (HAZOP) study was conducted to identify potential fire and explosion hazards and operability deviations. The qualitative HAZOP findings were integrated with quantitative reliability analysis using a Reliability-Centered Maintenance (RCM) framework. Data was obtained from piping and instrumentation diagrams and classified into four system nodes: feed water tank, fuel oil tank, critical alarm, and steam node. The results revealed substantial variability in reliability across subsystems. The feed water tank subsystem (Loop 1) exhibited a high failure probability of 0.926 and a short MTBF of 0.385 years, indicating the need for frequent preventive maintenance. In contrast, the steam boiler loop control subsystem (Loop 6) showed a lower failure probability of 0.287, an annual failure probability of 33.8%, and a longer MTBF of 2.956 years. These findings confirm an inverse relationship between failure probability and MTBF and provide practical guidance for hospital safety managers to prioritize high-risk components, optimize maintenance strategies, and strengthen operational controls to enhance boiler safety and operational continuity.

Keywords: Failure Probability; Hazard and Operability Study (HAZOP); Mean Time Before Failure (MTBF); Steam Boiler

*Faculty of Public Health, Thammasat University, Klong Luang, Pathum Thani, Thailand. E-mail: kanutsawan.mak@dome.tu.ac.th, arroon.k@fph.tu.ac.th**

** Corresponding author*

DOI: <https://doi.org/10.55766/sujst8134>

Suranaree J. Sci. Technol. 33(4):070113(1-12)

Introduction

A steam boiler is a closed vessel constructed from durable materials to generate steam and serves as a critical source of energy in industries such as power generation, hospitality, and healthcare. It primarily consists of a water-containing chamber and a steam storage unit. The generated steam can be utilized for a variety of purposes (Elie Tawil & Leed, 2009). In hospitals, the boiler system plays a vital role in heating, production, and supplying steam to equipment and tools. It is also essential for sterilizing medical equipment, providing hot water for patient care, sterilizing medical supplies, preparing food, and other consumption within the hospital. However, the operation of a boiler can pose severe dangers, such as the occurrence of fires and explosions. These potential hazards may be attributed to various factors including the steam boiler running dry, malfunction of a safety valve, the age of the boiler, low water level, excessive deposits, and inadequate ventilation for hot gas outlets. These conditions can lead to dangerously high temperatures and explosions. The DEPARTMENT OF INDUSTRIAL WORKS, Ministry of Industry of Thailand, serves as the governmental authority responsible for overseeing industrial machinery, production processes, environmental protection, occupational safety, hazardous substances, energy use, and corporate social responsibility. According to official reports, steam boiler malfunctions in Thailand between 2020 and 2022 caused an average of 20 fire and explosion incidents per year, resulting in approximately 22 injuries and fatalities annually and property losses of around 100 million baht. A steam boiler system relies on a Basic Process Control System (BPCS) to ensure safe operation. The BPCS manages process control and monitoring by processing inputs from sensors and instrumentation and generating outputs according to predefined control strategies. In many applications, the BPCS serves as the first layer of protection against unsafe operating conditions. Despite its protective role, equipment failures within the system may still occur, potentially leading to errors and catastrophic outcomes. To prevent serious fire and explosion incidents, Layers of Protection Analysis (LOPA) is applied to evaluate high-consequence scenarios by assessing whether the combined likelihood and severity of events fall within acceptable risk limits. Such scenarios typically involve both equipment and human failures and are initially identified through qualitative hazard analyses, such as Process Hazards Analysis (PHA) or Hazard and Operability (HAZOP) studies. LOPA is subsequently employed

to provide a more detailed and systematic assessment. LOPA is a quantitative screening tool which provides a consistent, objective, and defensible approach (Crowl and Louvar, 2001). Previous studies have analyzed the hazard and risk assessment processes in BPCS and other safety instrumentation systems. For example, Holub and Börcsök studied Layer of Protection Analysis (LOPA) as a quantitative risk analysis method to assess and reduce risk to an acceptable level by considering all protection layers and possible initiating events. They recommend installing a Safety Instrumented System (SIS) when the risk is unacceptable to ensure that the Safety Integrity Levels (SIL) meet the IEC 61511 standard (Holub & Börcsök, 2007). Babouri and Bendib conducted a study to describe the key concepts of Safety Integrity Level (SIL) of identified Safety Instrumented Functions (SIFs). This was done in accordance with various national and worldwide safety standards such as ANSI/ISA84 and IEC 61508/61511, and carried out on a process industry fired heater installed in the existing crude distillation unit located in industrial zone at Skikda in Algeria (Babouri & Bendib, 2019). Famuyiro studied risk assessment in a chemical process. Highly flammable liquids, such as hexane were assessed for the potential leakage, leading to fires and explosions (Famuyiro, 2018). Noriyati *et al.* utilized the Fault Tree Analysis (FTA) technique to analyze the potential hazards that might occur with superheat burners in fertilizer industry petrochemicals. They concluded that the level of risk of potential harm must be balanced with the Safety Instrumented System (SIS) (Noriyati *et al.*, 2017). Nur Qadri Lutfianto *et al.* used hazard identification and risk assessment to determine the control measures in the crude palm oil (CPO) manufacturing industry (Lutfianto *et al.*, 2021). Additionally, a study by Baratchi *et al.* (Baratchi *et al.*, 2018) focused on health, safety, and environmental hazard identification, applying the Hazard Identification (HAZID) method and Analytical Network Process (ANP) to assess the risk. One aspect that these studies did not address is assessing the risk in the BPCS of steam boilers, particularly in a university hospital. Most existing studies have focused on risk assessment of safety-instrumented systems in industrial settings, while reliable safety evaluations of BPCS in steam boilers remain limited. This gap is particularly critical in university hospitals, where system failures may directly affect occupant safety. Therefore, this study aims to assess the reliability of a steam boiler at a

university hospital by estimating the overall process failure probability, annual probability of failure, and mean time before failure (MTBF) of its instrumentation and control system components using a probabilistic risk assessment approach based on the HAZOP method.

Materials and Methods

Study Design and Setting

A cross-sectional study was conducted between April and August 2023 in a university hospital in Pathum Thani, Thailand. The boiler is a combination of systems and equipments for the purpose of converting chemical energy from fossil fuels into thermal energy and transferring the resulting thermal energy to a working fluid, usually water, for use in high-temperature processes or for partial conversion to mechanical energy in a turbine. The boiler was used for probabilistic safety and reliability evaluation. Before assessing the probabilistic safety and reliability, the HAZOP method was used for identifying the fire and explosion hazard (Signoret and Leroy, 2021). In this study, the probabilistic safety and reliability assessment focused exclusively on the BPCS of the steam boiler, while the SIS was not included in the quantitative analysis. This decision was made for several reasons. First, the BPCS serves as the primary and continuously operating layer of protection, responsible for routine monitoring and control of key process variables such as pressure, temperature, flow, and level. As a result, BPCS components are subject to frequent operational demand and are more susceptible to random failures that may initiate hazardous scenarios. Second, preliminary system review indicated that failures of BPCS final control elements could directly lead to

unsafe operating conditions, thereby increasing the likelihood of serious consequences if not promptly mitigated. In contrast, the SIS is designed as an independent and demand-based protection layer that is activated only when predefined safety limits are exceeded. Evaluating SIS performance typically requires a separate SIL assessment, including demand rate estimation and proof-test interval analysis, which was beyond the scope of the present study. Therefore, this research emphasizes the reliability of the BPCS as a critical determinant of overall boiler safety in a hospital environment. By strengthening the reliability of the first layer of protection, the frequency of SIS demands and the risk of escalation to high-consequence events can be effectively reduced.

Instrument Development and Data Analysis

The P&IDs were used to describe the details of instrumentation and control systems of the steam boiler and were classified into four nodes: feed water tank, fuel oil tank, critical alarm and steam node. All four nodes consisted of 13 loop control systems as shown in Table 1. The details of instrumentation and control systems of the steam boiler are shown in Figure 1. The HAZOP technique was used to identify probabilistic safety of fire and explosion due to the failure of steam boiler equipment. The full HAZOP study required a committee composed of a cross-section of experienced plants, laboratory, technical, and safety professionals. Assessment of the probabilistic safety was based on brainstorming by the HAZOP committee. The HAZOP committee consisted of steam boiler operators (two persons), preventive maintenance engineers (two persons), and a safety professional (one person). The researcher brainstormed the possible hazards in this study. All committee members have more than 5 years'

Table 1. The details of loop control systems

Nodes	Loop control systems
Node 1: Feed water tank	Loop 1: Feed water tank
Node 2: Fuel oil tank	Loop 10: Fuel oil tank
Node 3: Critical alarm	Loop 2: LIT to Check valve 1
	Loop 3: LIT to Check valve 2
	Loop 4: FIT to Check valve 1
	Loop 5: FIT to Check valve 2
	Loop 6: TIT to RB
	Loop 7: PIT to RB
	Loop 8: PIT to Safety valve 1
	Loop 9: PIT to Safety valve 2
	Loop 12: TIT to Critical alarm
	Loop 13: PIT to Critical alarm
Node 4: Steam	Loop 11: Steam to plant process

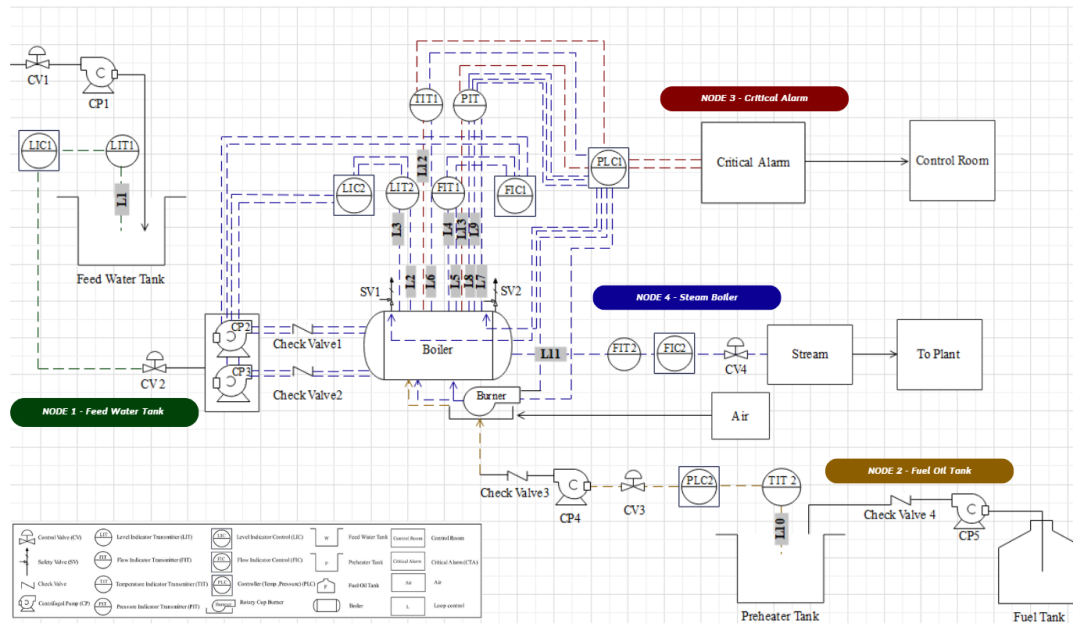


Figure 1. P&ID

experience in steam boiler production and process hazard analysis. In this approach, the process was broken down into steps, and every variation in work parameters was considered for each step, to see what could go wrong and the results of each scenario for identifying possible hazards. The HAZOP procedure used the following steps:

- Begin with a detailed flow sheet, including up to date Process Flow Diagrams (PFDs), P&IDs, detailed equipment specifications, and materials of construction. Break the flow sheet into a number of process units.
- Choose a study node (4 nodes: feed water tank, fuel oil tank, critical alarm and steam node).
- Describe the design intent of the study node.
- Pick a process parameter: flow, level, temperature, and pressure.
- Apply a guide word to the process parameter to suggest possible deviation.
- If the deviation was applicable, determine possible causes and note any protective systems.

The combination of guidewords and work parameters are shown in Table 2. The failure rate (μ) of each instrumentation and control system component of the steam boiler is identified in Table 3. In this study, failure rates (μ) of instrumentation and control system components were assumed to be constant over time and modeled using an exponential distribution, consistent with established reliability engineering practice for electronic and control components operating within their useful

life period (Mannan, 2012). This assumption is commonly applied to sensors, controllers, relays, and logic solvers, where random failures dominate and wear-out effects are minimized through routine inspection and preventive maintenance. In a hospital context, critical equipment such as steam boilers is subject to scheduled maintenance, periodic calibration, and regulatory oversight, which reduces the likelihood of early-life failures and delays wear-out-related degradation. Under these conditions, the exponential distribution provides a reasonable and conservative approximation for probabilistic safety and reliability assessment. Similar assumptions have been adopted in prior studies evaluating boiler systems and safety-instrumented functions in industrial and institutional settings. Nevertheless, it is acknowledged that mechanical components and aging infrastructure may exhibit time-dependent failure behavior under certain conditions. Therefore, the results of this study should be interpreted as reflecting average reliability performance under normal operating and maintenance regimes. The reliability of instruments was then determined by considering equation (1). After that, the probability of failure was calculated using equation (2).

$$R(t) = e^{-\mu t} \quad (1)$$

Where: R is the reliability of instruments; μ is a constant failure rate of instruments with units of faults per time; t is time interval (0, t), given by a Poisson distribution.

Table 2. Guidewords and work parameters used for the HAZOP procedure

Parameters	Guidewords	Definition
Flow	More, Higher, Greater	Quantitative increase
	No, Not, None	Quantitative decrease
	Reverse	The logical opposite direction
	Less, Lower	Quantitative decrease
	As well as	Qualitative increase
	Part of	Qualitative decrease
	Other than	Complete substitution
	Sooner, Faster	Too early or in the wrong order
Pressure	Later, slower	Too late or in the wrong order
	More, Higher, Greater	Quantitative increase
	Less, Lower	Quantitative decrease
	As well as	Qualitative increase
	Later, Slower	Too late or in the wrong order
	Sooner, Faster	Too early or in the wrong order
	More, Higher, Greater	Quantitative increase
	Less, Lower	Quantitative decrease
	As well as	Qualitative increase
	Part of	Qualitative decrease
	Other than	Complete substitution
	Sooner, Faster	Too early or in the wrong order
Composition	Different from	Solid or liquids (if applicable)
		Corrosive
		Explosive
		Out of specification
	Later, slower	Too late or in the wrong order
Other	Where else	In additional locations
Other	Leakage and spillage	Leakage or release to atmosphere
Utilities	No, Less	Loss of utilities
Operation and maintenance	No	Maintenance cannot be safely carried out
	Other than	Improper isolation

Table 3. The failure rate of instrumentation and control system components

Instrument	Faults/year
Controller (Pressure, Temperature)	0.29
Control valve	0.60
Safety relief valve	0.022
Check valve	0.019
Level Indicator Controller	0.29
Level Indicator Transmitter	1.70
Flow Indicator Controller	0.29
Flow Indicator Transmitter	1.14
Pressure Indicator Transmitter	1.41
Temperature Indicator Transmitter	0.027
Alarm indicator lamp (Critical alarm)	0.044
Centrifugal pump	1.752
Rotary cup burner	0.018
Solenoid valve	0.42
Main valve	0.01
Relay	0.003
DCS (Logic solver)	0.0002

$$P(t) = 1 - R \quad (2)$$

Where: P is failure probability (sometimes the unreliability)

The process components interacted in a series. This means that a failure of any single component in the series of components would result in failure of the process. This was represented by the logical OR function in this study. For series components or loop control systems, the overall process reliability was found by multiplying the reliabilities for the individual components as expressed in equation (3). After that, the overall process failure probability and overall failure rate were also computed from the individual component probabilities shown in equation (4) and (5), respectively. The process components interacted in two different fashions. In some cases, a process failure required the simultaneous failure of a number of components in parallel. This parallel structure was represented by the logical AND function.

$$R = \prod_{i=1}^n R_i \quad (3)$$

Where: R is the overall process reliability; R_i is the reliabilities for the individual components

$$P = 1 - \prod_{i=1}^n (1 - P_i) \quad (4)$$

Where: P is the overall process failure probability; P_i is the failure probabilities for the individual components

$$\mu = -\ln(R) \quad (5)$$

The time interval of loop control system components was called the mean time before failure, MTBF, and given by the first moment of the failure function as shown in equation (6).

$$MTBF = \int_0^{\infty} tf(t) dt = 1/\mu \quad (6)$$

Results and Discussion

The HAZOP analysis identified credible fire and explosion scenarios associated with deviations in level, flow, pressure, and temperature across all loop control systems (Table 4). When combined with probabilistic reliability analysis, these results revealed substantial differences in failure behavior among subsystems (Table 5), highlighting critical vulnerabilities within the steam boiler's instrumentation and control architecture. Subsystems associated with feed water supply exhibited the highest overall process failure probabilities and the shortest MTBF values. In

particular, the feed water tank loop (Loop 1) showed a failure probability of 0.926 and an MTBF of only 0.385 years, indicating that failures are likely to occur multiple times within a year under normal operating conditions. This high risk can be attributed to the serial configuration of multiple components with relatively high individual failure rates, which amplifies system-level unreliability. In a hospital context, inadequate feed water control represents a critical hazard, as low water levels are a well-documented initiating cause of boiler explosions. In contrast, loop control systems related to temperature control and combustion, such as the steam boiler loop (Loop 6), demonstrated significantly lower failure probabilities and longer MTBF values. These findings suggest that digitally controlled components and logic solvers, which generally have lower random failure rates, contribute to improved reliability when compared with mechanically intensive subsystems. The observed inverse relationship between failure probability and MTBF across all loops confirms the internal consistency of the reliability model and aligns with established reliability theory. As an illustrative example, the feed water tank loop (Loop 1) was used to demonstrate the calculation of overall process failure probability, annual probability of failure, and MTBF. These calculation parameters were divided into the following steps:

- The failure rate for the individual components (LIT1=1.7 faults/year, Relay=0.003 faults/year, LIC1=0.29 faults/year, and CV2=0.6 faults/year) were identified and the reliabilities for the individual components were obtained according to equation (1). The reliabilities for the LIT1, Relay, LIC1, and CV2 were 0.18, 0.99, 0.75, and 0.55, respectively.

- Failure probabilities for the individual components were obtained according to equation (2) (LIT1=0.82, Relay=0.01, LIC1=0.25, and CV2=0.45).

- The Loop control system (LIT1, Relay, LIC1, and CV2), the overall process reliabilities were calculated with equation (3) based on the logical AND function. The overall process reliability showed a value of 0.074. The overall process failure probability was then determined according to equation (4) and showed a value of 0.926.

- The overall failure rate was calculated with equation (5). The overall failure rate was 2.600.

- The mean time before failure was computed as the reciprocal of overall failure rate based on equation (6). This value was equal to 0.385. Therefore, on average, one failure is expected every 140.5 days of operation.

From a maintenance perspective, the results provide a quantitative basis for prioritizing preventive maintenance. Unlike previous studies that reported MTBF values without translating them into actionable schedules, this study explicitly links MTBF to recommended maintenance intervals. Loop control systems with MTBF values below one year require frequent inspection and preventive intervention, whereas systems with longer MTBFs may be managed through extended maintenance cycles. This risk-based prioritization is particularly important in hospital environments, where boiler failures can disrupt essential services and compromise patient safety. These findings were consistent with previous studies (Igboanugo *et al.*, 2013; Pamungkas *et al.*, 2020; Hatala *et al.*, 2023; Yunos & Ibrahim, 2023; Yusof & Mohammad, 2023). Our study used the HAZOP technique to identify the hazards. Previous studies used other techniques such as fault tree analysis (FTA), failure modes and effect analysis (FMEA), failure mode effect analysis and critical analysis (FMECA), and event tree analysis (ETA) to identify the possible hazards. These different methods showed competent performance for identifying the hazards. The advantage of the HAZOP technique though is that it is comprehensive, creative, proactive, and collaborative. It covers all aspects of a process or system, allowing team members to explore different perspectives and use their experience and intuition to generate ideas and solutions. This technique also helps to identify and address potential hazards before they occur or escalate. It involves a diverse group of stakeholders who can share their knowledge, opinions, and feedback. After the probability of failure per year was obtained, the MTBF was calculated to determine the instrument preventive maintenance plan. Loop control system (Loop 1), loop control system (Loop 2) and loop

control system (Loop 3) were set at a frequency for preventive maintenance plan approximately once every 140.5 days. Loop control system (Loop 4), loop control system (Loop 5) and loop control system (Loop 11) were set at a frequency for preventive maintenance plan approximately once every six months or 180 days. Loop control system (Loop 13) was set at a frequency for preventive maintenance plan approximately once every 208 days. Loop control system (Loop 7), loop control system (Loop 8), and loop control system (Loop 9) were set at frequency for preventive maintenance plan approximately once every seven months or 210 days, and remaining three loop control systems set at a frequency for preventive maintenance plan approximately once every year, 2.786 years, and 2.956 years in the loop control system (Loop 10), loop control system (Loop 12), loop control system (Loop 6), respectively. These findings were consistent with the previous studies (Igboanugo *et al.*, 2013; Polhong & Rukijkanpanich, 2017; Pamungkas *et al.*, 2020; Preangprom *et al.*, 2021; Patil *et al.*, 2022; Hatala *et al.*, 2023; Yunos & Ibrahim, 2023) which calculated the mean time before failure and recommended preventive maintenance plans. However, no prior studies specified the frequency of preventive maintenance based on considering the mean time before failure. Overall, integrating HAZOP with probabilistic reliability analysis enhances the practical value of the assessment by not only identifying hazardous scenarios but also quantifying their likelihood and operational implications. This combined approach supports more informed decision-making for hospital safety managers by enabling targeted allocation of maintenance resources, reducing the probability of high-consequence events, and improving the long-term reliability and safety of steam boiler systems.

Table 4. Loop control system, guide words and work parameters of steam boiler

Loop control system and Instrument	Guide words and work parameters	Scenario	Consequence
Feed water tank: Loop 1 (LIT1+Relay+LIC1+CV2)	High level	Measuring and control equipment failure	Water overflow
	Low level	Measuring and control equipment failure	The water has decreased, not enough to be fed to the steam boiler
Steam boiler: Loop 2 (LIT2+Relay+LIC2+CP2+Check valve1)	High flow	Measuring and control equipment failure	More water flows into the steam boiler
	Low flow	Measuring and control equipment failure	Water level below the glass tube level may cause the steam boiler an explosion

Table 4. Loop control system, guide words and work parameters of steam boiler (Continued)

Loop control system and Instrument	Guide words and work parameters	Scenario	Consequence
	No flow	Measuring and control equipment failure	There is no water entering the steam boiler, an explosion may occur
	Reverse flow	Water flows back into the feed water pump	Feed water pump is damaged
	High level	Measuring and control equipment failure	Water overflow
	Low level	Measuring and control equipment failure	Water level below the glass tube level may cause the steam boiler an explosion
Steam boiler: Loop 3 (LIT2+Relay+LIC2+CP3+Check valve2)	High flow	Measuring and control equipment failure	More water flows into the steam boiler
	Low flow	Measuring and control equipment failure	Water level below the glass tube level may cause the steam boiler an explosion
	No flow	Measuring and control equipment failure	There is no water entering the steam boiler, an explosion may occur
	Reverse flow	Water flows back into the feed water pump	Feed water pump is damaged
	High level	Measuring and control equipment failure	Water overflow
	Low level	Measuring and control equipment failure	Water level below the glass tube level may cause the steam boiler an explosion
Steam boiler: Loop 4 (FIT1+Relay+FIC1+CP2+Check valve1)	High flow	Measuring and control equipment failure	More water flows into the steam boiler
	Low flow	Measuring and control equipment failure	Water level below the glass tube level may cause the steam boiler an explosion
	No flow	Measuring and control equipment failure	There is no water entering the steam boiler, an explosion may occur
	Reverse flow	Water flows back into the feed water pump	Feed water pump is damaged
	High level	Measuring and control equipment failure	Water overflow
	Low level	Measuring and control equipment failure	Water level below the glass tube level may cause the steam boiler an explosion
	High flow	Measuring and control equipment failure	More water flows into the steam boiler
	Low flow	Measuring and control equipment failure	Water level below the glass tube level may cause the steam boiler an explosion

Table 4. Loop control system, guide words and work parameters of steam boiler (Continued)

Loop control system and Instrument	Guide words and work parameters	Scenario	Consequence
Steam boiler: Loop 5 (FIT1+Relay+FIC1+CP3+Check valve2)	High flow	Measuring and control equipment failure	More water flows into the steam boiler
	Low flow	Measuring and control equipment failure	Water level below the glass tube level may cause the steam boiler an explosion
	No flow	Measuring and control equipment failure	There is no water entering the steam boiler, an explosion may occur
	Reverse flow	Water flows back into the feed water pump	Feed water pump is damaged
	High level	Measuring and control equipment failure	Water overflow
	Low level	Measuring and control equipment failure	Water level below the glass tube level may cause the steam boiler an explosion
Steam boiler: Loop 6 (TIT1+Relay+PLC1+RB)	High temperature	Measuring and control equipment failure	Temperature higher than the Auto-Ignition Temperature: AIT cause fire and explosion
	Low temperature	Measuring and control equipment failure	Fuel is not atomized in a rotary cup burner
Steam boiler: Loop 7 (PIT+Relay+PIC1+RB)	High pressure	A failed safety relief valve causes the steam boiler to exceed specifications and measuring equipment and pressure control equipment failure	Increased pressure inside the steam boiler may cause an explosion and critical alarm failure
	Low pressure	Measuring and control equipment failure	None
Steam boiler: Loop 8 (PIT+Relay+PLC1+SV1)	High pressure	The pressure is greater than the specification and the pressure measurement and control equipment are faulty	Increased pressure inside the steam boiler may cause an explosion and critical alarm failure
	Low pressure	Measuring and control equipment failure	None
Steam boiler: Loop 9 (PIT+Relay+PLC1+SV2)	High pressure	The pressure is greater than the specification and the pressure measurement and control equipment are faulty	Increased pressure inside the steam boiler may cause an explosion and critical alarm failure
	Low pressure	Measuring and control equipment failure	None
Fuel oil tank: Loop 10 (TIT2+Relay+PLC2+CV3)	High temperature	Measuring and control equipment failure	Temperature higher than the Auto-Ignition Temperature: AIT causes fire and explosion
	Low temperature	Measuring and control equipment failure	Fuel is not atomized in a rotary cup burner

Table 4. Loop control system, guide words and work parameters of steam boiler (Continued)

Loop control system and Instrument	Guide words and work parameters	Scenario	Consequence
Steam boiler: Loop 11 (FIT2+Relay+FIC2+CV4)	High flow	The steam flow rate leaving the steam boiler is higher than the specification and the flow measurement and control equipment are faulty	None
	Low flow	The steam flow rate leaving the steam boiler is lower than the specification and the flow measurement and control equipment are faulty	None
	No flow	The steam flow rate leaving the steam boiler is lower than the specification and the flow measurement and control equipment are faulty	There is no steam to dispense
Critical alarm: Loop 12 (TIT1+Relay+PLC1+CTA)	High temperature	The temperature is higher than the specification and the measurement and control equipment fails	Increased pressure may cause an explosion and critical alarm failed
Critical alarm: Loop 13 (PIT+Relay+PLC1+CTA)	High pressure	The pressure is higher than the specification and the measurement and control equipment fails	Increased pressure may cause an explosion and critical alarm failed
	Low pressure	Measuring and control equipment failure	None

Table 5. Probabilistic safety assessment for instrumentation and control systems of steam boiler

Loop control system and instrument	Overall process reliability (R)	Overall process failure probability (P)	PoF (%)	MTBF (Year)
Loop 1	0.074	0.926	2.600 (260.0)	0.385
Loop 2	0.074	0.926	2.603 (260.3)	0.384
Loop 3	0.074	0.926	2.603 (260.3)	0.384
Loop 4	0.132	0.868	2.027 (202.7)	0.493
Loop 5	0.132	0.868	2.027 (202.7)	0.493
Loop 6	0.713	0.287	0.338 (33.8)	2.956
Loop 7	0.176	0.824	1.735 (173.5)	0.576
Loop 8	0.176	0.824	1.735 (173.5)	0.576
Loop 9	0.176	0.824	1.735 (173.5)	0.576
Loop 10	0.400	0.600	0.916 (91.6)	1.092
Loop 11	0.132	0.868	2.025 (202.5)	0.494
Loop 12	0.698	0.302	0.359 (35.9)	2.786
Loop 13	0.173	0.827	1.756 (175.6)	0.570

Notes: PoF is probability of failure per year; MTBF is mean time before failure.

Conclusions

This study evaluated the overall process failure probability, annual probability of failure, and mean time between failures (MTBF) of a steam boiler at a university hospital by integrating the Hazard and Operability (HAZOP) technique with quantitative reliability analysis. Although HAZOP is primarily a qualitative method, it is widely recognized for systematically identifying potential hazards and operability issues, and its outcomes can effectively inform risk reduction measures when combined with reliability metrics. In this study, HAZOP findings supported the design of safety controls, operational parameters, and maintenance strategies, particularly when interpreted alongside MTBF values. The results were further applied within a Reliability-Centered Maintenance (RCM) framework to prioritize preventive maintenance activities, consistent with previous evidence demonstrating improvements in boiler reliability and maintenance cost efficiency. The reliability analysis also confirmed an inverse relationship between failure probability and MTBF, highlighting the importance of interpreting these indicators in a complementary manner to identify critical system vulnerabilities and prioritize high-risk components. Several limitations should be acknowledged. First, this study was conducted at a single university hospital, which may limit the generalizability of the findings to other hospital settings or boiler configurations. Second, failure rates were assumed to be constant and derived primarily from literature sources rather than site-specific historical data, which may not fully capture time-dependent degradation or operational variability. Finally, the analysis focused on the Basic Process Control System (BPCS) and did not include Safety Instrumented System (SIS) performance. Future research should extend this work by conducting multi-site studies across different hospital types and boiler configurations to improve the generalizability of reliability estimates and maintenance recommendations. Incorporating site-specific historical failure and maintenance records would allow the use of time-dependent reliability models, such as Weibull distributions, to better capture aging effects and degradation of mechanical and control components. Further studies should integrate the performance of the Basic Process Control System (BPCS) with Safety Instrumented Systems (SIS) to enable a comprehensive assessment of protection layers using advanced Layer of Protection Analysis

(LOPA) or Safety Integrity Level (SIL) verification. In addition, sensitivity and uncertainty analyses could be applied to evaluate the influence of key assumptions, such as constant failure rates and component independence, on reliability outcomes. Future work may also explore the application of digital maintenance technologies, including condition-based monitoring, predictive analytics, and real-time sensor data, to dynamically update failure probabilities and optimize maintenance scheduling. Such approaches would enhance hospital risk management, improve operational continuity, and further reduce the likelihood of high-consequence boiler failures.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

Author Contributions

Kanutsawan Maksuk: Methodology, Investigation, Data Collection, Writing - Original Draft, Project Administration

Arroon Ketsakorn: Conceptualization, Formal Analysis, Validation, Writing - Review & Editing, Supervision, Funding Acquisition

Ethics Approval and Consent to Participate

Ethical approval was not required because this study involved only technical safety and reliability assessment of a steam boiler system using technical documentation and expert HAZOP input, without human subjects, personal data, or health information.

Declaration of Generative AI

The authors declare that no Generative AI tools were used in the preparation of this manuscript.

Acknowledgement

The authors would like to acknowledge the safety experts who participated in this study.

References

- Babouri, K., & Bendib, R. (2019). Assessment of safety integrity requirements for fired heater system in accordance with IEC 61508. *International Journal of Latest Engineering Science*, 2(5), 43–49.
- Baratchi, M., Mansouri, N., & Ahmadi, A. (2018). Steam boiler hazard identification using analytical network process: A case study of Farabi Hospital. *International Journal of Occupational Hygiene*, 10(3), 172–179.
- Crowl, D. A., & Louvar, J. F. (2001). *Chemical process safety: Fundamentals with applications* (4th ed.). Pearson Education.
- Elie Tawil, P. E., & Leed, A. P. (2009). *Boiler classification and application*. CED Engineering.
- Famuyiro, S. (2018). Use of combustible gas detectors in safety instrumented systems: A practical application case study. *Journal of Loss Prevention in the Process Industries*, 54, 333–339. <https://doi.org/10.1016/j.jlp.2018.05.007>
- Hatala, M. H., Sukarsono, B. P., & Nukertamanda, D. (2023). Risk and reliability analysis of boiler system using the failure mode effect analysis & critical analysis (FMECA) method. *Spektrum Industri*, 21(1), 8–20. <https://doi.org/10.12928/si.v21i1.98>
- Holub, P., & Börsök, J. (2007). LOPA—A method to analyse safety integrity systems according to IEC 61511. In *Proceedings of the 6th WSEAS International Conference on Computational Intelligence, Man-Machine Systems and Cybernetics* (pp. 315–322).
- Igboanugo, A. C., Asalor, J. O., & Egbiremon, V. I. (2013). Assessment of some performance characteristics of refuse boiler before and after overhaul using failure mode effect and fault tree analyses. *Nigerian Journal of Technology*, 32(2), 333–349.
- Lutfianto, N. Q., Udhistira, G. A. Y., Febrianti, M. A., & Qurtubi. (2021). Management analysis on occupational health and safety in the boiler house using method of hazard identification, risk assessment and determining control. In *Proceedings of the 3rd International Sustainability and Resilience Conference: Climate Change* (pp. 358–361). IEEE. <https://doi.org/10.1109/IEEECONF53624.2021.9668034>
- Mannan, S. (2012). *Lees' loss prevention in the process industries* (4th ed.). Butterworth-Heinemann.
- Noriyati, R. D., Prakoso, A. B., Musyafa, A., & Soeprijanto, A. (2017). HAZOP study and determination of safety integrity level using fault tree analysis on fuel gas superheat burner of ammonia unit in petrochemical plant, East Java. *Asian Journal of Applied Sciences*, 5(2), 396–409. <https://doi.org/10.24203/ajas.v5i2.4683>
- Pamungkas, I., Irawan, H. T., & Saputra, A. (2020). Risk and reliability analysis on critical components of boiler in steam power plant. *IOP Conference Series: Materials Science and Engineering*, 1003(1), Article 012048. <https://doi.org/10.1088/1757-899X/1003/1/012048>
- Patil, S. S., Bewoor, A. K., Kumar, R., Ahmadi, M. H., Sharifpur, M., & Praveen Kumar, S. (2022). Development of optimized maintenance program for a steam boiler system using reliability-centered maintenance approach. *Sustainability*, 14(16), Article 10073. <https://doi.org/10.3390/su141610073>
- Polhong, W., & Rukijkanpanich, J. (2017). Predictive maintenance for centrifugal pumps in pulp industry. *The Journal of KMUTNB*, 27(4), 615–629. <https://doi.org/10.14416/j.kmutnb.2017.11.017>
- Preangprom, S., Tumrongsuk, S., & Anuntajalearchork, W. (2021). Increasing production efficiency by maintenance planning: A case study of a conveyor belt machine in the receiving-distribution room. *The Journal of KMUTNB*, 31(2), 201–215. <https://doi.org/10.14416/j.kmutnb.2020.12.014>
- Signoret, J. P., & Leroy, A. (2021). Hazard and operability study (HAZOP). In *Reliability assessment of safety and production systems* (pp. 157–164). Springer International Publishing. https://doi.org/10.1007/978-3-030-64708-7_9
- Yunos, Y. F. M., & Ibrahim, M. Y. (2023). Study of component safety level (reliability) in steam boiler. In *Proceedings of the 14th International Conference on Information and Communication Systems* (pp. 7–12).
- Yusof, M. F. M., & Mohammad, R. (2023). Risk management framework and practices for boiler operations in Malaysia. *Progress in Energy and Environment*, 23, 26–38. <https://doi.org/10.37934/progee.23.1.2638>