Design and performance testing of a safety instrumented system for water level control simulator using plc with cause-effect matrix implementation

Safira Firdaus Mujiyanti[1*], Fadhil Ahmadi [1], Sefi Novendra Patrialova[1], Ahmad Fauzan Adziimaa[1], Dwi Oktavianto Wahyu Nugroho[1], Tepy Lindia Nanta[1]

[1] Departement of Instrumentation Engineering, Institut Teknologi Sepuluh Nopember, Surabaya, 60111, Indonesia. E-mail: safira.firdaus@its.ac.id

Email of corresponding: safira.firdaus@its.ac.id

Present Address:
Building A ITS Campus, Keputih, Sukolilo District, Surabaya, East Java 60117, Indonesia

Received: 21 March 2025 Revised: 23 April 2025 Accepted: 30 June 2025

Abstract— Safety Instrumented Systems (SIS) are widely employed in industrial settings to ensure operational safety and prevent system failures that could pose risks to the environment, personnel, and assets. This research presents the design of an SIS for a water level control system, utilizing Programmable Logic Control (PLC) to enhance safety and mitigate the risk of leakage or flooding. The SIS design is developed based on the Layers of Protection Analysis (LOPA) methodology, incorporating multiple protective layers, including water level measurement instruments, controllers, and final control elements to manage risk effectively. Following the LOPA-based design process, system testing was conducted using a cause-and-effect matrix to evaluate performance under various operational scenarios. The findings indicate that implementing SIS in water level control systems significantly enhances operational safety. In simulated test conditions, the SIS effectively detected potentially hazardous situations, such as excessive water levels that could lead to overflow or dangerously low levels that might disrupt process continuity. The system then executed appropriate mitigation measures, such as alerting operators or automatically shutting off water flow, to prevent accidents and equipment damage. The results demonstrate that integrating an SIS into water level control systems provides substantial benefits in managing operational risk, ensuring system reliability, and safeguarding industrial processes.

Keywords—Cause Effect Matrix, Layers of Protection Analysis , Process Safety, Safety Instrumented System

1. INTRODUCTION

Water level control is a critical process in various industrial applications. This study focuses on the implementation of a Safety Instrumented System (SIS) in water level tank systems, which play a vital role in industries such as petrochemicals, water treatment, and power generation. Failure to maintain appropriate water levels in these tanks can lead to severe consequences, including leakage, flooding, equipment damage, resource loss, and potential hazards to both the environment and personnel. For instance, in power plants (PLTU), water level control is essential in the water treatment process, where storage tanks hold seawater before it undergoes demineralization [1]. Maintaining the water level within the specified range ensures process efficiency and compliance with safety standards [2].

The SIS design process involves selecting and configuring suitable sensors, actuators, and a Programmable Logic Controller (PLC). The PLC is programmed to continuously monitor the water level and trigger control actions when predefined safety thresholds are exceeded. These control actions may include activating alarms, adjusting valve positions, or initiating emergency shutdown procedures to mitigate potential risks [3][4].

This research highlights the importance of SIS in industrial operations to enhance safety and prevent system failures that could lead to hazardous incidents affecting workers, assets, and the environment. SIS is specifically designed to detect potential hazards and implement appropriate safety measures to reduce risks [5][6].

The study adopts the Layer of Protection Analysis (LOPA) methodology for designing an SIS in water level tank systems. LOPA is a structured approach used to identify and evaluate the necessary layers of protection to effectively manage risks [7]. The protection layers in this design include water level measurement instruments, controllers, and final control elements, all of which serve as safety mechanisms to prevent system failures [8].

The integration of SIS into water level tank systems presents significant advantages in operational risk management. This research aims to enhance the understanding of SIS applications in safeguarding water level control systems and preventing failures that could pose substantial risks to industrial operations and the environment.

2. Previous Researches

2.1. State of the Art Solutions

Numerous studies have been conducted to enhance Safety Instrumented Systems (SIS) in both industrial and educational contexts. The following research contributions provide significant insights into advancements in this field:

1. Iqbal et al. (2017) developed an Overflow Protection System for Level Tanks utilizing a Programmable Logic Controller (PLC). Their study replaced conventional relay-based control systems with PLCs, offering improved control efficiency and successfully preventing tank overflow.
2. Goeritno et al. (2017) conducted a Safety Integrity Level (SIL) analysis for SIS enhancement in a Geothermal Power Plant. Their findings revealed potential risks, such as condensate water entering turbines and steam pressure reduction, necessitating the implementation of redundant actuators for increased safety.
3. Kurniawan (2018) designed an Alarm System for a Heat Exchanger Simulator based on Layer of Protection Analysis (LOPA). This system effectively detected system errors, activated alarms, and stored error logs, ensuring uninterrupted operation without requiring an immediate shutdown.
4. Alam (2022) developed an SIS Simulator for a Pressurized Tank, incorporating LOPA's fifth layer (relief device) with Raspberry Pi as the primary controller. The system facilitated real-time monitoring and control through an interactive interface.
5. Huda (2018) created an SIS Prototype for a Steam Plant, integrating Atmega controllers with multiple safety mechanisms, such as temperature and level sensors, to prevent operational hazards.

2.2. Research Gap

Despite substantial progress in SIS development, several critical challenges remain unaddressed:

1. The majority of existing research focuses on industrial-scale applications, with limited emphasis on educational implementations.
2. The integration of SIS within laboratory-based learning environments has not been extensively explored.
3. Previous studies lack user-friendly Human-Machine Interface (HMI) integration, which is crucial for enhancing interactive educational experiences.
4. Most existing solutions rely on single-layer safety mechanisms, whereas a multi-layered approach could significantly improve system reliability and effectiveness.

2.3. Significance, Novelty, and Contribution

This study aims to bridge the identified research gaps by:

1. Developing an SIS platform specifically designed for educational purposes, providing students with hands-on experience in instrumentation and control engineering.
2. Integrating an interactive HMI, allowing real-time monitoring and intuitive control to enhance user experience and operational understanding.
3. Implementing a multi-layered safety mechanism, incorporating alarms, float level switches, and PLC-based logic solvers to ensure greater system reliability.
4. Enhancing accessibility and adaptability, making the SIS system suitable for laboratory-based training while maintaining industrial relevance.

By addressing these gaps, this research contributes to the advancement of SIS applications in both educational and industrial domains, fostering improved safety, system effectiveness, and engineering education.

3. METHOD

3.1. Design of Safety Instrumented System for the Water Level Tank

The design of the Safety Instrumented System (SIS) for the water level tank follows a structured control system block diagram, which serves as a fundamental guideline for system development and implementation [9]. This block diagram provides a comprehensive overview of the control architecture, illustrating the integration of sensors, controllers, and actuators to ensure reliable and safe water level management. The block diagram is presented in Figure 1 below.

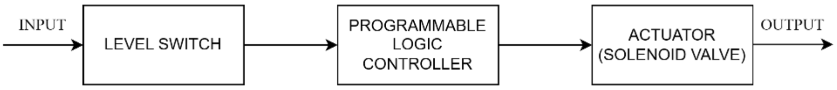

Figure. 1. Safety System Block Diagram

Additionally, an alarm system block diagram is included as a guideline for the development of this system [10]. This diagram outlines the alarm mechanisms designed to detect and respond to abnormal water level conditions, ensuring prompt hazard mitigation. The alarm system block diagram is presented in Figure 2 below.

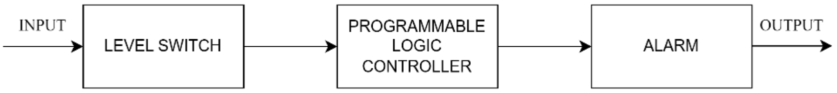

Figure. 2. Alarm System Block Diagram

Furthermore, the design process for the Safety Instrumented System (SIS) for the water level tank included the development of a Process Flow Diagram (PFD), a Piping and Instrumentation Diagram (P&ID), and a Cause and Effect Table. The PFD visually represents the process, its components, and their sequential interactions, serving as a critical tool for conceptualizing and communicating the system design. The PFD diagram is presented in Figure 3 below.

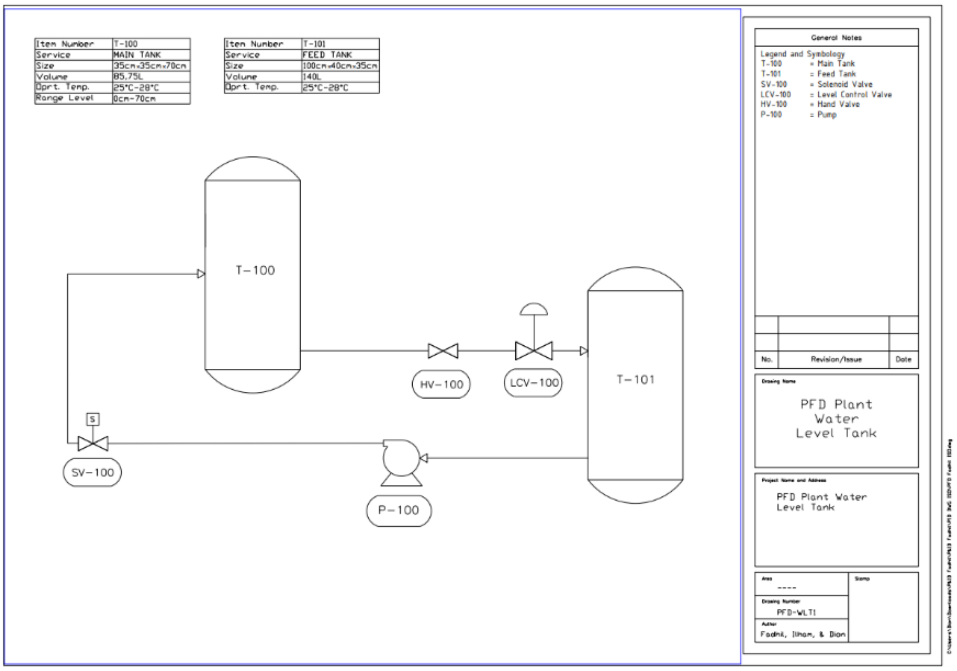

Figure. 3. Process Flow Diagram

The operation of the Safety Instrumented System (SIS) in the Water Level Tank plant begins with water flowing from the feed tank into the level tank. The water in the level tank is then discharged through an outlet, which directs it back to the feed tank via a control valve. Once returned to the feed tank, the water is pumped back into the level tank, forming a continuous closed-loop system. The control system governing this process is depicted in the Piping and Instrumentation Diagram (P&ID) shown in Figure 4 below.

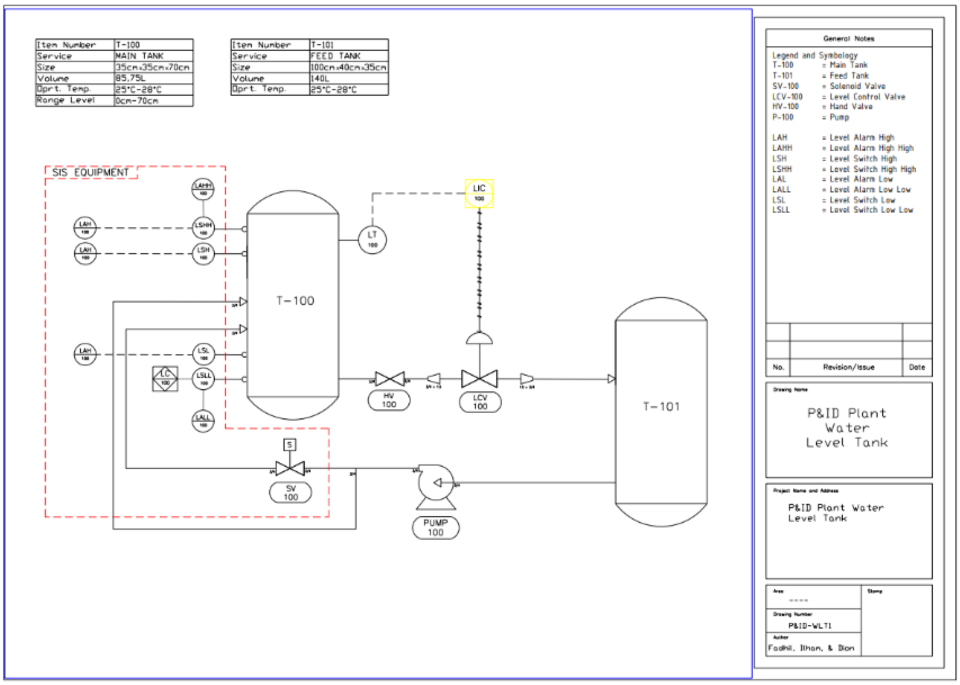

Figure. 4. Piping & Instrumentation Diagram

In the control system of the Safety Instrumented System (SIS) Simulator for the Water Level Tank, three key components play a crucial role: sensors, controllers, and actuators. In this system, the level switch sensors (LSLL, LSL, LSH, LSHH) are used to detect deviations in the tank's water level from the predefined set point. When the low-low level switch (LSLL) detects that the water level has reached a critical low point, it transmits a signal to the controller. The controller then instructs the actuator (SV 100) to open, increasing the water inflow to restore the level to the set point as quickly as possible. Conversely, when the high-high level switch (LSHH) detects an excessive water level, it sends a signal to the controller, which triggers a pump trip to stop the inflow until the water level returns to the desired set point. A Cause and Effect matrix is utilized to illustrate the process flow. This matrix defines the relationships between inputs, set points, and triggers, serving as a critical reference for identifying potential system failures. By mapping these relationships, the matrix facilitates the identification of failure sources and root causes, thereby improving system diagnostics and reliability [11][12]. The Cause and Effect table for the SIS in the Water Level Tank plant is presented in Table 1 below.

Table I. Cause and Effect Matrix

CAUSE & EFFECT MATRIX PLANT WATER LEVEL TANK CONTROL									
			1	2	3	4	5	6	
	CAUSE	EFFECT	HMI INDICATOR	CONTROL ROOM ALARM	STOP PUMP	OPEN SOLENOID VALVE	CLOSE CONTROL VALVE	OPEN CONTROL VALVE (	SET POINT
NO	ALARM AND SAFETY CASE	DEVICE ID							
1	LEVEL TANK 100 HIGH HIGH LEVEL	LSHH - 100	x	x	x			x	60 CM
2	LEVEL TANK 100 HIGH LEVEL	LSH - 100	x	x					50 CM
3	LEVEL TANK 100 LOW LEVEL	LSL - 100	x	x					20 CM
4	LEVEL TANK 100 LOW LOW LEVEL	LSLL - 100	x	x		x	x		10 CM
		NOTE :	x	=	MAIN ACTION				

In the Cause and Effect table, the alarm system is activated when it receives triggers from the LSHH, LSH, LSL, and LSLL sensors. Additionally, the pump operation will shut down upon receiving a trigger from the LSHH sensor. Conversely, the solenoid valve will open when triggered by the LSLL sensor.

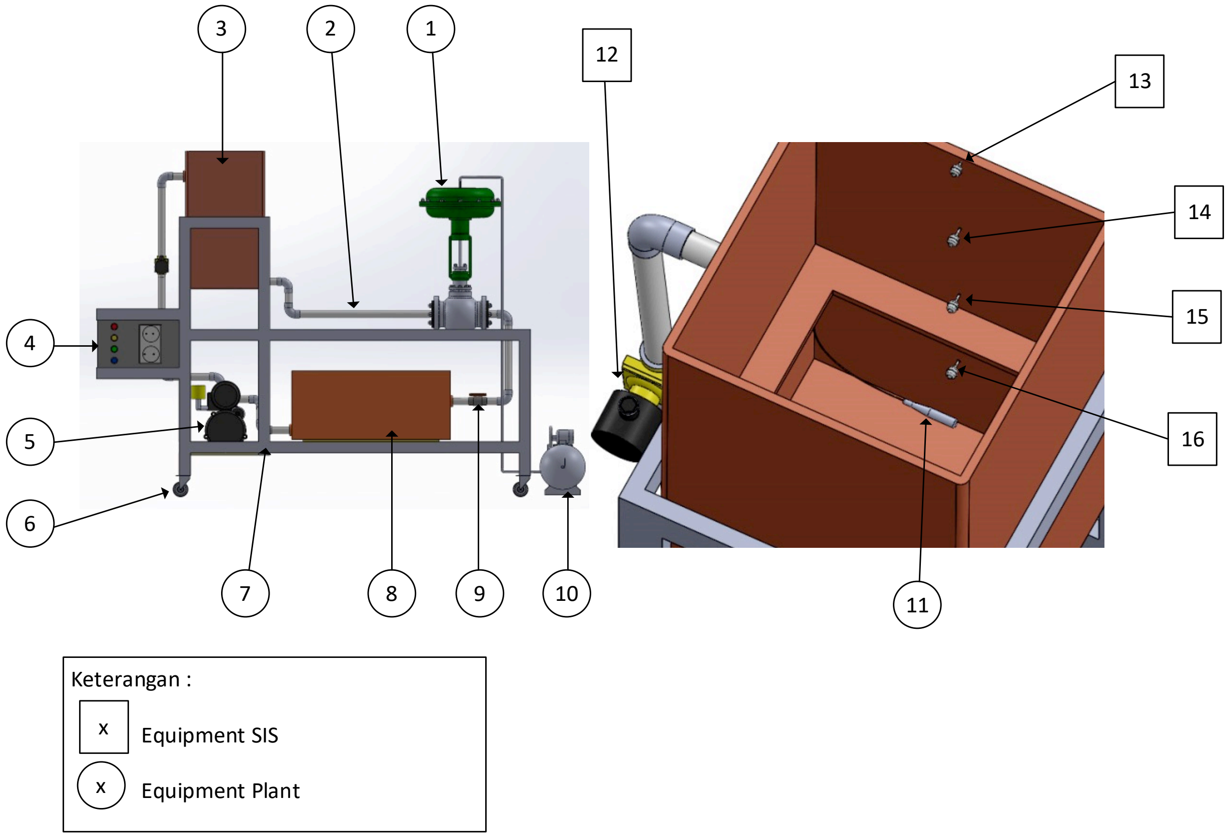

Figure. 5. 3D Design *Hardware Design*

Numbering Explanation :

1. Flow Control valve
2. Pipe
3. Level Tank.
4. Panel Box
5. Water Pump
6. Wheel
7. Rack
8. Feed tank
9. Hand Valve
10. Kompresor
11. Level sensor
12. Solenoid Valve
13. Level Switch Highhigh (LSHH)
14. Level Switch High (LSH)
15. Level Switch Low (LSL)
16. Level Switch Lowlow (LSLL)

The low-low level switch (LSLL) is installed 10 cm above the tank base to prevent complete depletion of water and enable the system to respond promptly. The low level switch (LSL) is positioned 20 cm above the tank base, allowing a time delay for the alarm to activate before a system trip occurs when the water level reaches the LSLL threshold. The high level switch (LSH) is installed 50 cm above the tank base to provide an interval for the alarm to trigger before the solenoid valve closes when the water level reaches the high-high level switch (LSHH). The LSHH is set at 60 cm to ensure that the solenoid valve effectively shuts off the water inlet before an overflow occurs.

Furthermore, a wiring diagram is essential for system design, as it facilitates the creation, maintenance, and troubleshooting of the electrical circuitry. The wiring diagram, illustrated in Figure 6, provides a visual representation of the electrical connections and components, ensuring a clear understanding of the system’s wiring configuration and guaranteeing proper installation and functionality.

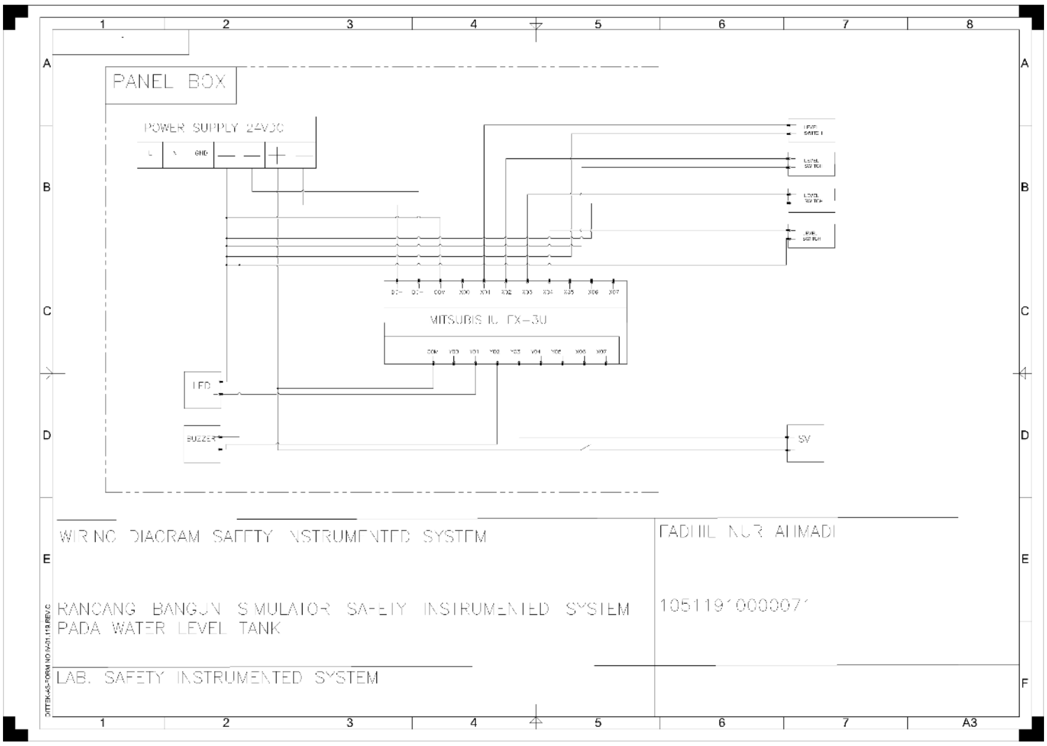
PANEL BOX
POWER SUPPLY 24VDC
MITSUBISHI FX-3U
LED
BUZZER
SV
WIRING DIAGRAM SAFETY INSTRUMENTED SYSTEM
RANCANG BANGUN SIMULATOR SAFETY INSTRUMENTED SYSTEM PADA WATER LEVEL TANK
LAB. SAFETY INSTRUMENTED SYSTEM
FADHIL NUR AHMADI
105119100007
A3

Figure. 6. Wiring Diagram

The following illustrates the interface design of the water level control plant, which is integrated with a Safety Instrumented System (SIS). This interface is not only used for monitoring water levels but is also equipped with a status display for the level switches. When the green indicator light is illuminated, it signifies that the water level has not yet reached the corresponding switch height. Conversely, when the red indicator light is activated, it indicates that the water level has reached the switch threshold. This visual representation enhances real-time monitoring, allowing operators to promptly assess the system's condition and take necessary corrective actions to maintain safe and optimal operation. Figure 7 presents the interface design of the water level control plant equipped with SIS.

3.2. Design Human Machine Interface

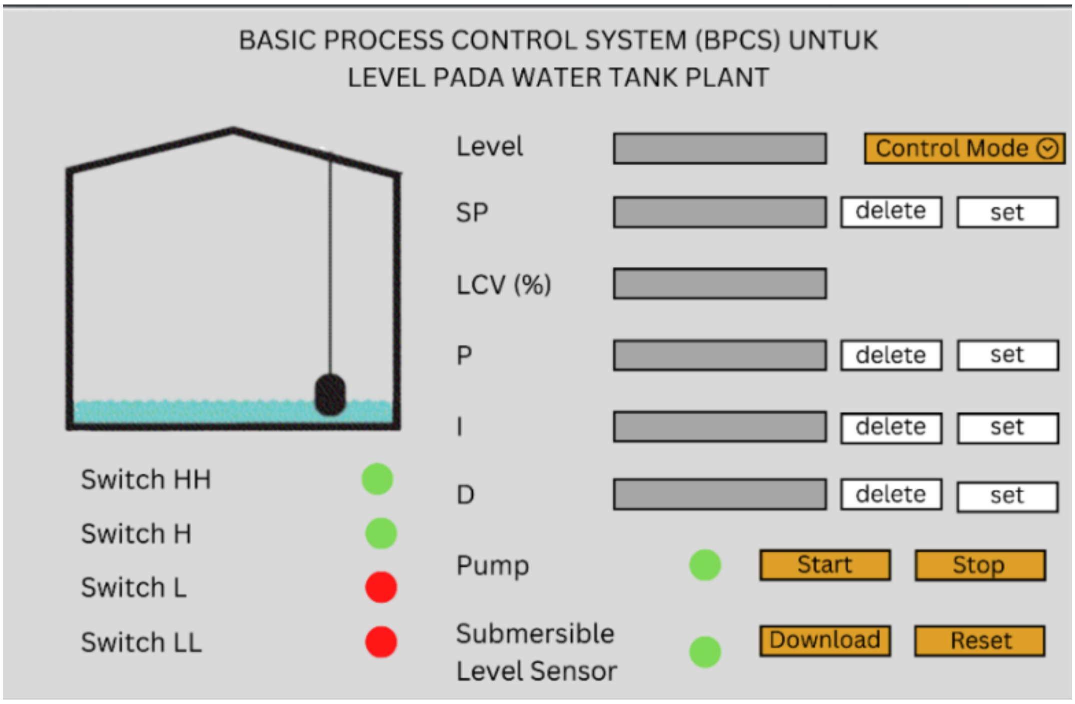
BASIC PROCESS CONTROL SYSTEM (BPCS) UNTUK LEVEL PADA WATER TANK PLANT

Figure. 7. Human Machine Interface

Figure 7 illustrates the Human-Machine Interface (HMI) design for the water level control plant, which integrates a Safety Instrumented System (SIS). This interface is designed not only to monitor water levels but also to display the status of the switches, providing real-time feedback on system conditions. The green indicator light signifies that the water level remains below the switch height, representing a normal operational state. Conversely, the red indicator light signals that the water level has reached the switch height, indicating a potentially abnormal condition requiring attention.

3.3. Hardware Integration with Software

The integration of hardware and software involves embedding the control program into a Programmable Logic Controller (PLC) after the assembly of instrumentation and electrical components. This process utilizes the RS232 Modbus protocol, ensuring seamless communication between the control system and the connected hardware. The integration phase is crucial for validating the real-time performance of the system, allowing for functional verification and optimization before deployment.

3.4. Device Performance Testing

To evaluate system functionality, a performance test was conducted on the Safety Instrumented System Simulator for the Water Level Tank. This testing process involved systematically filling the tank, continuously monitoring system responses, and recording operational data at one-second intervals. The objective was to verify the correct functionality of the designed and implemented SIS, ensuring that key system components such as level switches, actuators, and control algorithms, responded accurately and reliably.

If any errors or discrepancies were detected during testing, adjustments and refinements were made to ensure the system met its intended specifications. This iterative validation process was essential for confirming the system's reliability, stability, and adherence to safety standards.

3.5. Performance Testing of the Safety System in the Water Level Plant

During the performance evaluation, the Safety Instrumented System Simulator for the Water Level Tank was tested under controlled conditions. The tank was filled while system behavior was continuously monitored and data was collected at one-second intervals. The primary goal was to assess the system’s capability to maintain operational safety, ensuring that all critical components such as level switches, actuators, and control systems, functioned correctly in response to changing water levels.

To introduce controlled disturbances, two variations of pump frequencies were applied using a Variable Speed Drive (VSD) to modify the water flow rate entering the tank. These variations were intentionally introduced to stress-test the Basic Process Control System (BPCS), inducing high-high and low-low water level conditions, which, in turn, triggered the SIS protective mechanisms.

Through these structured tests and induced operational disturbances, the effectiveness and robustness of the Safety Instrumented System were rigorously validated. The results confirmed the system’s ability to detect critical water level conditions, respond to anomalies, and maintain operational safety and stability, even under dynamic process conditions.

4. RESULT AND DISCUSSION

The device testing phase is conducted after the successful integration of all components based on the 3D mechanical design, electrical circuitry, and interface configuration as outlined in the wiring diagram. This testing process is essential for evaluating the functional performance of the designed system, ensuring its reliability and adherence to the intended operational specifications. By systematically testing each component and their interactions, potential malfunctions or inefficiencies can be identified and corrected before deployment in real-world applications. This evaluation phase also serves to verify that the system meets industry standards and operates effectively under various conditions, particularly in scenarios involving critical safety mechanisms.

4.1. The Result When The Water Level Reaches The High-High Level

Ensuring operational safety in industrial water level management systems is crucial for preventing overfill conditions that could lead to equipment damage, process inefficiencies, or hazardous operational failures. The Safety Instrumented System (SIS) plays a fundamental role in this context by autonomously monitoring water levels and initiating protective actions when predefined safety thresholds are exceeded. This mechanism enhances plant reliability and reduces the risk of unintentional system failures.

To assess the effectiveness of the SIS, a high-high water level test was conducted under controlled conditions, as illustrated in Figure 8. In this experiment, the pump was operated at a frequency of 55.5 Hz to increase the water level until it reached the designated high-high threshold. The water level progression was continuously monitored to ensure accuracy in detecting the critical threshold. Upon reaching this critical point, the High-High Level Switch (LSHH) promptly detected the excessive water level and transmitted an emergency signal to the control system, triggering an automatic pump shutdown (pump trip) to prevent further accumulation.

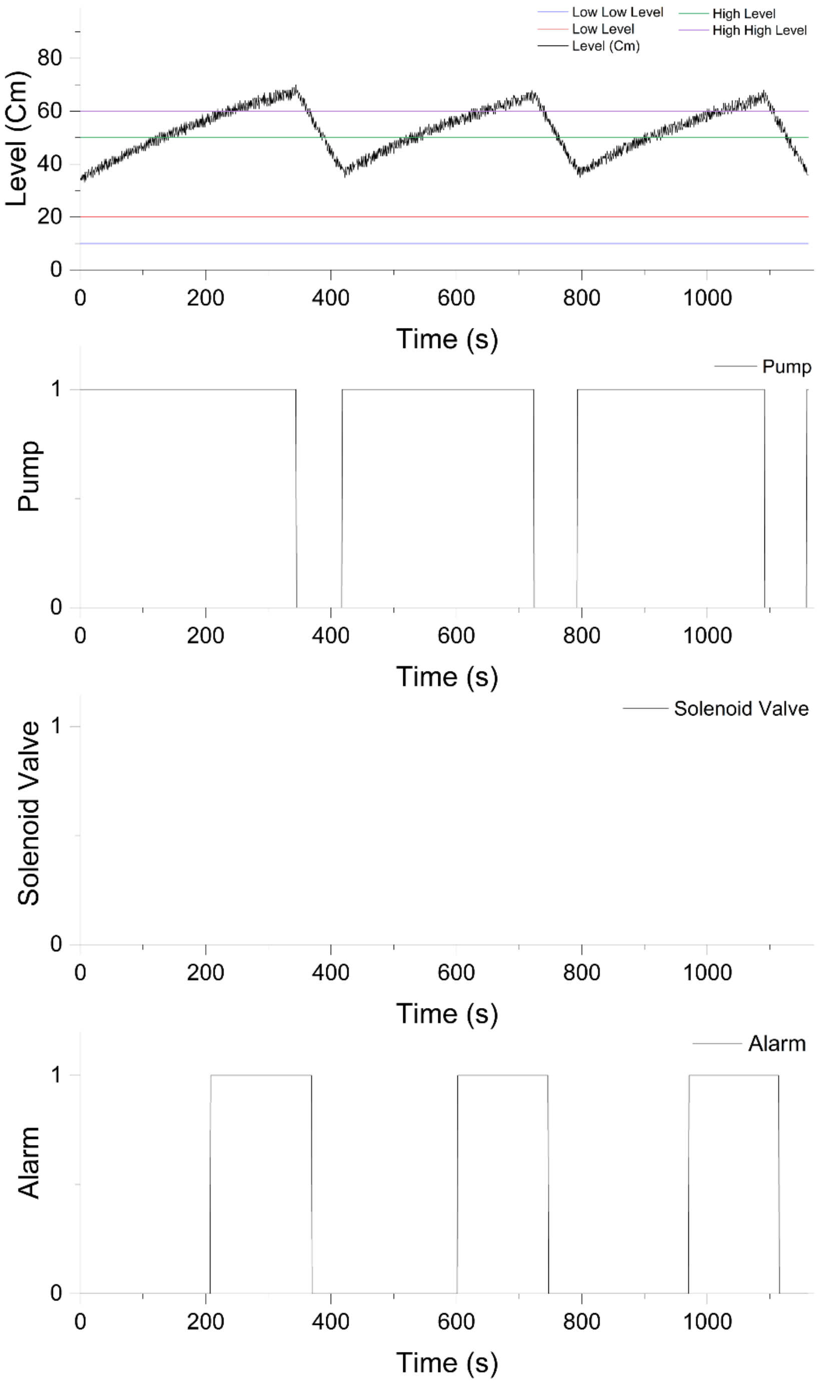

Figure. 8. Graph of Actuator Response in High-High Testing

The first plot in Figure 8 shows the fluctuations in water level over time, with marked reference lines representing predefined threshold levels. The activation of the LSHH at the high-high threshold is clearly observed, immediately leading to the pump shutdown, as depicted in the second plot. This immediate response ensures that excessive water accumulation is prevented, mitigating the risk of overflow. Once the pump is deactivated, the water level gradually decreases due to controlled drainage and natural system flow dynamics.

The third plot represents the solenoid valve operation, which is activated intermittently to facilitate controlled drainage, preventing excessive water retention in the system. This response ensures that the water level returns to a safe operational range before normal system function is restored. Additionally, the fourth plot illustrates the alarm system activation, which is triggered upon detecting a high-high water level condition. This alarm serves as an additional safety layer, providing immediate alerts to operators for necessary intervention if required.

These findings confirm the efficiency and reliability of the SIS in mitigating overfill risks and ensuring that water levels remain within designated operational limits. The system's rapid response to high-high level conditions enhances safety, minimizes the likelihood of operational disruptions, and maintains the overall stability and efficiency of the water level control process. Furthermore, the integration of automated safety mechanisms significantly reduces the need for manual intervention, increasing the reliability of industrial water management systems in both normal and emergency operating conditions.

4.2. The Result When The Water Level Reaches The Low-Low Level

The operational performance of the Safety Instrumented System (SIS) in water level control is depicted in Figures 10 and 11. The first subplot illustrates the water level variation over time, with predefined threshold lines representing critical levels: Low-Low Level, Low Level, High Level, and High-High Level. The subsequent subplots display the activation states of the pump, solenoid valve, and alarm, providing insights into the automated response mechanisms of the SIS.

During the low-low water level testing phase, the pump was operated at a frequency of 33 Hz to reduce the water level to the designated Low-Low threshold. As observed in the first subplot, the water level gradually declined until it reached this critical limit. At this moment, the Low-Low Level Switch (LSLL) detected the condition and transmitted a signal to the controller, as indicated by the activation of the solenoid valve in the third subplot. Consequently, the solenoid valve opened, allowing increased water inflow into the system.

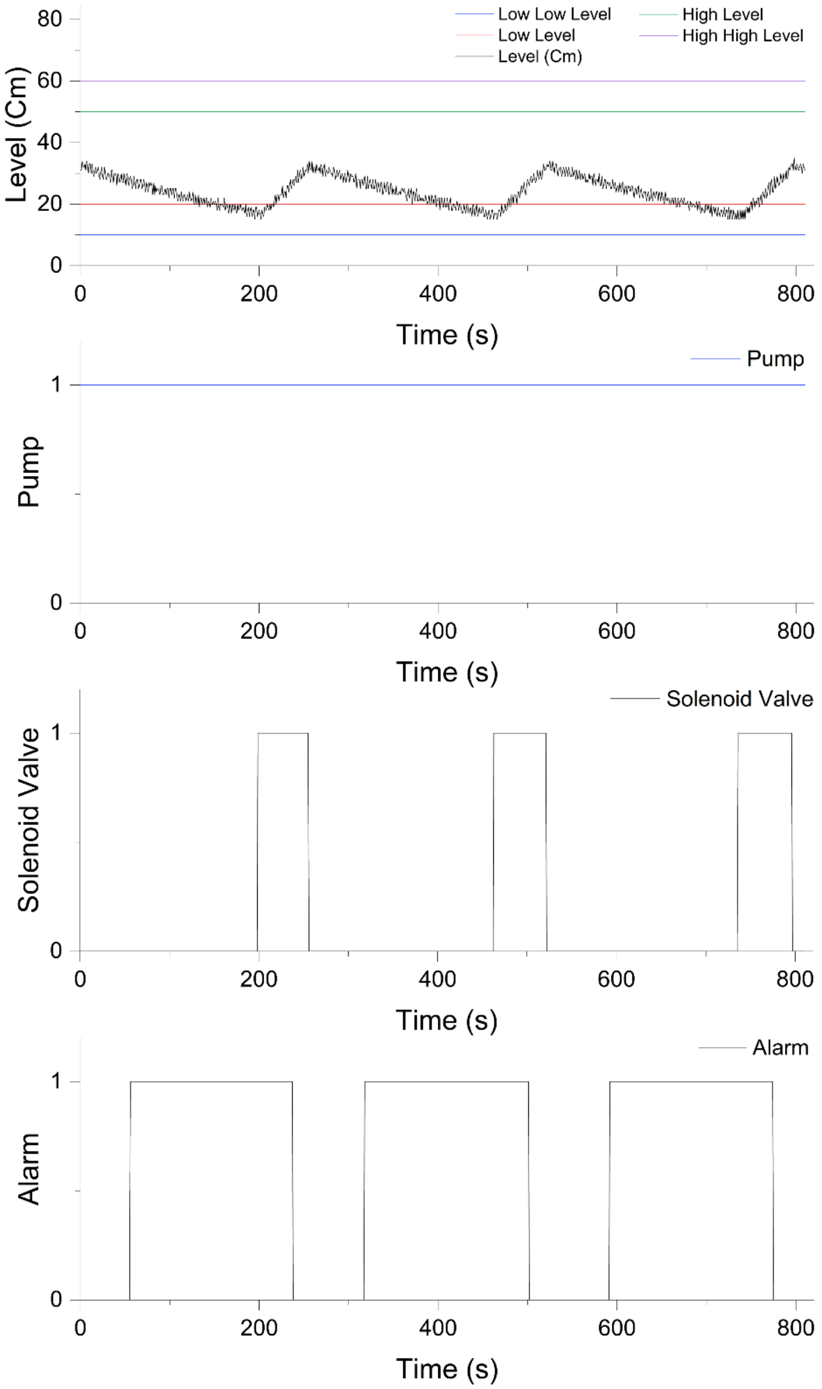

Figure. 9. Graph Of Actuator Response In Low-Low Testing

The automated response of the SIS successfully prevented the water level from reaching the tank's bottom and facilitated its return to the predefined set point. This is reflected in the recovery trend of the water level in the first subplot, which rises after each activation of the solenoid valve. Once the set point was achieved, the solenoid valve automatically closed, restoring normal operational conditions.

Additionally, the alarm system, as depicted in the fourth subplot, was triggered whenever the water level dropped to the low-low threshold. The periodic activation of the alarm further emphasizes the system's reliability in alerting operators about critical conditions.

These experimental results confirm that the SIS effectively mitigates the risk of water shortages within the water level control plant. By dynamically adjusting the water inflow rate in response to the low-low level switch signal, the system ensures that the water level remains within safe operating limits. This capability contributes to the overall stability, reliability, and operational integrity of the plant, demonstrating the effectiveness of the implemented safety control strategies.

5. Conclusion

Based on the testing and analysis, the system demonstrates effective water level regulation within the designated safe operating range. When the water level reaches 60 cm (high-high level), the system automatically shuts off the pump, allowing the water level to decrease until it reaches the predetermined set point. Upon reaching this set point, the pump restarts, ensuring stable water levels and preventing potential tank overflow. This automated control mechanism enhances system reliability by maintaining a consistent water level, thereby mitigating the risk of operational disruptions due to excessive water accumulation.

Similarly, when the water level drops to 10 cm (low-low level), the solenoid valve is activated, increasing the input water flow to restore the water level to the designated set point. This preventive action effectively prevents the water level from reaching the bottom of the tank, which could otherwise compromise system operations. By implementing these automated corrective measures, the system ensures that optimal water levels are consistently maintained within the desired operating range, thereby supporting uninterrupted plant operations and preventing potential failures.

CRediT

Conceptualization, Methodology, Writing - Original Draft Preparation, and Supervision: Safira Firdaus Mujiyanti; Formal Analysis and Investigation: Safira Firdaus Mujiyanti, Fadhil Ahmadi, Sefi Novendra Patrialova, Ahmad Fauzan Adziimaa, Dwi Oktavianto Wahyu Nugroho, Tepy Lindia Nanta; Writing - Review and Editing: Fadhil Ahmadi, Sefi Novendra Patrialova, Ahmad Fauzan Adziimaa, Dwi Oktavianto Wahyu Nugroho, Tepy Lindia Nanta; Funding Acquisition: Safira Firdaus Mujiyanti; Resources: Fadhil Ahmadi, Sefi Novendra Patrialova, Ahmad Fauzan Adziimaa, Dwi Oktavianto Wahyu Nugroho, Tepy Lindia Nanta

References

[1] L. S. L. Fernandes, J. B. A. Paulo, and J. A. Oliveira, *Development of a strategy to monitor and control the oil-water interface level of a liquid-liquid separator for treatment of wastewater using an image-based detector*, vol. 27, no. C. Elsevier Inc., 2009.

[2] L. Qiu *et al.*, "Study on water level control system of natural circulation steam generator," *Prog. Nucl. Energy*, vol. 153, no. September, p. 104436, 2022.

[3] L. Ye, "The Design of Practice Training System Based on PLC Programmable Automatic Control," *Proc. 2015 Int. Conf. Intell. Syst. Res. Mechatronics Eng.*, vol. 121, pp. 1931–1934, 2015.

[4] M. A. Sehr *et al.*, "Programmable Logic Controllers in the Context of Industry 4.0," *IEEE Trans. Ind. Informatics*, vol. 17, no. 5, pp. 3523–3533, 2021.

[5] Kevin J. Mitchell, P. Hereña, T. M. Longendelpher, and M. C. Kuhn, *Kenexis - Safety Instrumented Systems Engineering Handbook*. 2010.

[6] P. Gruhn and H. Cheddie, *Safety Instrumented Systems Analysis*, vol. 255. 2006.

[7] R. J. Willey, "Layer of protection analysis," *Procedia Eng.*, vol. 84, pp. 12–22, 2014.

[8] F. Crawley, "Layer of Protection Analysis (LOPA)," *A Guid. to Hazard Identif. Methods*, pp. 57–69, 2020.

[9] B. Schrörs, "Functional Safety: IEC 61511 and the industrial implementation," *INSS 2010 - 7th Int. Conf. Networked Sens. Syst.*, pp. 45–48, 2010.

[10] T. Stauffer and P. Clarke, "Using Alarms as a Layer of Protection," *Process Saf. Prog.*, vol. 25, no. 4, pp. 326–330, 2015.

[11] M. Giovani and E. Bonet, "A Comparison of Model Checking Techniques for Cause and Effect Matrix

Based Controller Logic of Safety Instrumented Systems," 2019.

[12] T. Hamaguchi, B. Mondori, K. Takeda, N. Kimura, and M. Noda, "A method for generation and check of alarm configurations using cause-effect matrices for plant alarm system design," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9173, pp. 549–556, 2015.