International Journal of Safety and Security Engineering
Vol. 15, No. 4, April, 2025, pp. 835-846
Journal homepage: http://iieta.org/journals/ijsse

Hazard Analysis with STPA Methods: Application to Mould Level Control Within Continuous Casting Free Stream Operations

Khalid Larit[1*], Youcef Zennir[2], Manuel Rodriguez[3]

[1] LRPCSI Laboratory Skikda, Université 20 Aout 1955 Skikda, Skikda 21000, Algeria
[2] Automatic Laboratory of Skikda, Université 20 Août 1955 Skikda, Skikda 21000, Algeria
[3] Chemical Engineering Department, Higher Technical School of Industrial Engineers, Polytechnic University of Madrid, Madrid 28006, Spain

Corresponding Author Email: kh.larit@univ-skikda.dz

https://doi.org/10.18280/ijsse.150419

Received: 19 February 2025
Revised: 25 March 2025
Accepted: 13 April 2025
Available online: 30 April 2025

Keywords:
Mould Level Control, STPA (System-theoretic Process Analysis), continuous casting, hazard analysis, process safety, free stream, steel manufacturing

ABSTRACT

In the continuous casting process, maintaining precise control over the mould level is essential to ensure product quality, prevent defects, and optimize operational efficiency. Mould Level Control (MLC) in Free Stream operations presents unique challenges, as it requires accurate and stable control amidst dynamic process variations and complex interdependencies between sensors, actuators, and controllers. This paper presents a case study conducted at a steel plant located in Bellara, El Milia – Jijel, Algeria, which utilizes a 120-ton Electric Arc Furnace (EAF) operating at a tap temperature of approximately 1630°C. The process is controlled via a Siemens PLC-based automation system. Continuous casting is performed using a curved-type machine (3BLC 0905), featuring five strands, a casting section of 150 ×150 mm, and a maximum casting speed of 3.5 m/min. The system includes a ladle turret, 30-ton tundish, mould, and withdrawal system, and is used to produce low-carbon steel grades (C < 0.13%, Al < 0.006%). System-Theoretic Process Analysis (STPA) is applied to identify and mitigate hazards in MLC systems under Free Stream conditions. The analysis highlights unsafe control actions (UCAs), actuator delays, and sensor inaccuracies, and proposes improvements in control logic, calibration, and response strategies to enhance system safety and reliability.

1. INTRODUCTION

Continuous casting is a fundamental process in steel manufacturing, where molten steel is transformed into solid billets. This method enables efficient, high-volume production with precise control over the dimensions and quality of steel products [1]. At the center of this process is MLC, which keeps the molten steel at a consistent level in the mould. Maintaining this level is critical because even small fluctuations can result in defects like surface cracks, slag inclusions, or internal voids, compromising the steel's quality and structural integrity [2].

The MLC system operates through a closed-loop control structure. A radioactive sensor monitors the steel level in real time, feeding data to a Programmable Logic Controller (PLC), which uses a Proportional-Integral-Derivative (PID) algorithm to adjust the withdrawal speed of the strand [3]. This setup is effective under regular casting conditions, providing stability and accuracy that meet quality requirements. However, under Free Stream mode, where the steel flows freely into the mould without the stabilization of a submerged entry nozzle, MLC faces unique challenges. In this mode, the absence of hydraulic damping and directional control from the nozzle makes the steel surface highly unstable, leading to amplified level oscillations. The inflow becomes more turbulent, and the system must cope with rapid and nonlinear fluctuations in flow rate, which are harder to predict and control. In this mode, the system must adjust dynamically to constant variations in flow rate and respond quickly to prevent unsafe fluctuations [4].

These dynamic variations are further complicated by delays in sensor feedback, noise in signal processing, and limited actuator response times [5].

Compounding this challenge are potential delays in feedback from sensors and actuator response times, making it difficult to maintain steady levels and increasing the risk of hazardous situations like overflow or underfill [6].

Traditional hazard analysis methods, such as Failure Mode and Effects Analysis (FMEA) and Fault Tree Analysis (FTA), are commonly used to evaluate risks in systems like MLC. These methods are effective in examining single-point failures or identifying linear cause-and-effect relationships. However, they are less capable of modelling the dynamic and time-sensitive nature of control systems operating in Free Stream mode. For example, traditional analyses may not detect risks arising from the combined effect of slight actuator lag and sensor drift, which—though individually insignificant—can jointly create UCAs [7].

Continuous casting in Free Stream mode is a complex system, where hazards often emerge from interactions between multiple components and control loops, rather than isolated failures. Traditional methods can struggle to account

for these interactions, potentially leaving critical risks unaddressed.

To address these limitations, this study employs STPA, a systems-based hazard analysis technique that takes a broader view of safety by considering the entire control structure. STPA differs from conventional methods by focusing on UCAs and feedback loop dependencies rather than just component failures. Developed for complex, interdependent systems, STPA is especially suitable for analyzing MLC under Free Stream conditions, as it allows analysts to detect hazards that emerge from incomplete, delayed, or incorrect control actions, even when system components are technically functioning.

In this study, STPA is used to model the MLC control structure and systematically identify UCAs that could lead to hazards, such as unstable level fluctuations, overflow, or underfill—all of which have serious implications for safety and product quality. This analysis uncovers potential vulnerabilities that might not be detected by traditional methods, such as delayed actuator responses, inaccurate sensor feedback, and unintended feedback loop effects. The insights gained from this approach allow for targeted recommendations to enhance system reliability.

The primary contributions of this study are as follows:

First application of STPA to MLC in Free Stream mode: No prior study has analyzed this system using a system-theoretic approach, despite frequent issues like breakouts, mould overflow, and unstable level fluctuations.

Identification of critical unsafe control actions: This study uncovers previously unrecognized risks arising from sensor inaccuracies, actuator delays, and operator interventions, which traditional methods may overlook.

Targeted recommendations for improved safety and reliability: By addressing control system weaknesses, this work provides insights to enhance sensor accuracy, improve actuator response, and refine operator decision-making, reducing the likelihood of serious accidents.

In summary, this work demonstrates the value of applying STPA to the complex challenges of MLC in continuous casting. By identifying and mitigating risks that arise from control interactions and system dependencies, this study contributes to advancing safety, quality, and stability in steel manufacturing. Ultimately, these insights support more robust and reliable production, reducing the likelihood of defects and enhancing the overall efficiency of the casting process.

2. LITERATURE REVIEW

Studies on hazards in continuous casting and MLC have identified several critical risks and strategies for addressing them. Research by Shuaib et al. [8] on metal processing factories in Malaysia highlights significant hazards such as poor training, failure to follow Standard Operating Procedures (SOPs), and lack of personal protective equipment (PPE), which can lead to consequences like fire, explosions, and improper handling of molten materials. Their study emphasizes the importance of risk management frameworks like Hazard Identification, Risk Assessment, and Risk Control (HIRARC) to manage these risks effectively.

In another study, Sadi et al. [9] focus on traditional metal casting in Ceper Klaten, Indonesia, identifying risks such as improper handling of raw materials, exposure to heat, and chemical radiation. They stress the importance of implementing SOPs, better workplace organization, and regular training to reduce these hazards. While their study does not directly address continuous casting, its emphasis on improving safety practices is highly relevant to similar operations.

Putri et al. [10] provide a more specific examination of hazards in MLC and continuous casting. They identify key risks, including molten metal splashes, uneven casting results, and ergonomic challenges, and recommend measures such as improving lighting, redesigning workspaces, providing PPE, and conducting regular safety training. Their use of the Hazard Identification Risk Assessment and Risk Control (HIRARC) method demonstrates its effectiveness in identifying and mitigating high-risk activities in casting processes.

Adding to this, the Hazard Identification and Risk Assessment (HIRA) study at the Bokaro Steel Plant offers a broader perspective on the risks associated with continuous casting operations. It highlights high-risk activities like handling molten metals and hazardous gases, with hazards such as gas leaks, explosions, and toxic cloud dispersion posing significant threats. The study recommends advanced measures, including regular inspections, use of gas monitoring systems, improved emergency response protocols, and strict adherence to engineering and procedural standards to contain potential hazards within plant premises. These measures underline the importance of integrating robust safety mechanisms into high-risk operations like MLC [11].

Together, these studies demonstrate the utility of traditional methods like HIRARC and HIRA for addressing immediate risks but also highlight the limitations of these approaches for managing systemic and dynamic hazards.

Advanced techniques such as STPA offer a way to address these gaps by considering the interactions between humans, machines, and control systems in continuous casting. For instance, Naeini and Nadeau [12] applied STPA to assess occupational health and safety (OHS) and operational risks associated with the use of data gloves in industry 4.0 assembly contexts. Their findings indicate that STPA provides a systemic view of control structures, effectively identifying UCAs and loss scenarios in complex manufacturing systems.

Further expanding on systemic approaches, Naeini and Nadeau [13] conducted a critical review of the application of FRAM and STAMP in manufacturing within the industry 4.0 context. They concluded that, despite limited studies, these methods are promising for analyzing digital manufacturing risks, especially concerning wearable technologies, and emphasized the need for further research in this area.

In the domain of human-robot collaboration, Zacharaki et al. [14] introduced a method combining STPA with partially observable markov decision processes (POMDP) to enhance decision-making in collaborative environments. Their framework enables real-time safety assessments by associating system states with safety levels, thereby guiding the system towards safer operational states.

Addressing energy storage systems, Bu et al. [15] utilized STPA alongside fuzzy evaluation to analyze operational risks in containerized lithium-ion battery energy storage systems. Their study identified numerous UCAs and proposed countermeasures to improve system safety and reliability.

Moreover, Karevan and Nadeau [16] reviewed the role of industry 5.0 in mitigating human error risks in manufacturing, particularly through the use of Internet of things (IoT) and wearable devices. They highlighted the necessity for comprehensive models to assess human error risks associated

with these technologies, suggesting that systemic methods like STPA could be instrumental in this endeavor.

In the maritime industry, Manzur et al. [17] conducted a literature review on risk and safety management of autonomous systems, recommending STPA as the optimal method for handling complex socio-technical systems due to its comprehensive nature and ability to provide actionable safety recommendations.

By integrating traditional methods like hirarc and hira with advanced systemic approaches such as stpa, organizations can develop a more holistic understanding of risks in continuous casting and MLC processes. This combination facilitates the identification of both immediate and systemic hazards, enabling the implementation of more effective safety measures in complex industrial environments.

3. SYSTEM DESCRIPTION

The key control parameter of continuous casting is matching the flow of liquid steel into the mold with the withdrawal speed of the strand out of the mold [18]. The control of flow rates is accomplished by the tundish, a small, refractory-lined distributer that is placed over the mold and that receives steel from the furnace ladle (see Figure 1). Withdrawal speed is controlled by driven rolls, which contact the strand at a point where it has already developed a thick, solidified shell [19].

3.1 Mould level control free stream:

The mould level is acquired by a radioactive transducer and is controlled by adjusting the withdrawal speed of the casting process. The MLC system consists of the following equipment: Radioactive Level Detector - A001: This device is responsible for measuring the molten metal level in the mould. The detector is strategically positioned to ensure accurate and consistent level monitoring [20].

The Figure 2 illustrates the radioactive level detector in both side and top views. The side view highlights the horizontal positioning and mechanical connections, while the top view provides an overview of the detector's alignment and its interface with the mould system.

The casting speed is automatically controlled in order to perform:

- Machine start
- Mold level holding to the set point

The machine start (auto start) is performed to fill the mould with steel until the proper level set point is achieved; the casting speed is then controlled to maintain the level constant at the set point.

The mould level is maintained at the target value by controlling the withdrawal speed. The control is performed by mean of closed loop controller, which is executed by the PLC. The controller compares the current mould level with the target value; the difference is computed by a PID algorithm that generates the casting speed reference [21].

The response of the level PID algorithm is automatically changed based on the mould size; the PID response is also changed in order to better react to the situations that during the cast may require a different response time.

There are two families of regulator constants:

- Autostart constants
- PID Regulator constants

Autostart constants (initial speed, speed ramp, initial tundish weight for autostart…) are stored in cast practice recipes.

PID Regulator constants (Kp, Ki, Kd, output limits…) are saved in several data tables in PLC. Cast practice recipes just select which one of the tables must be used for the product.

The machine stop is done by actuating the Calibrated Nozzle Change (CNC) device. Fast Nozzle Change (FNC) system inserts a blind nozzle in order to close the strand when needed, both in normal and emergency situations.

Casting speed depends by the level regulator so it can only be changed by inserting a different size metered nozzle. Nozzle change is done using the CNC device.

The Figure 3 shows the control algorithm schematic [20].

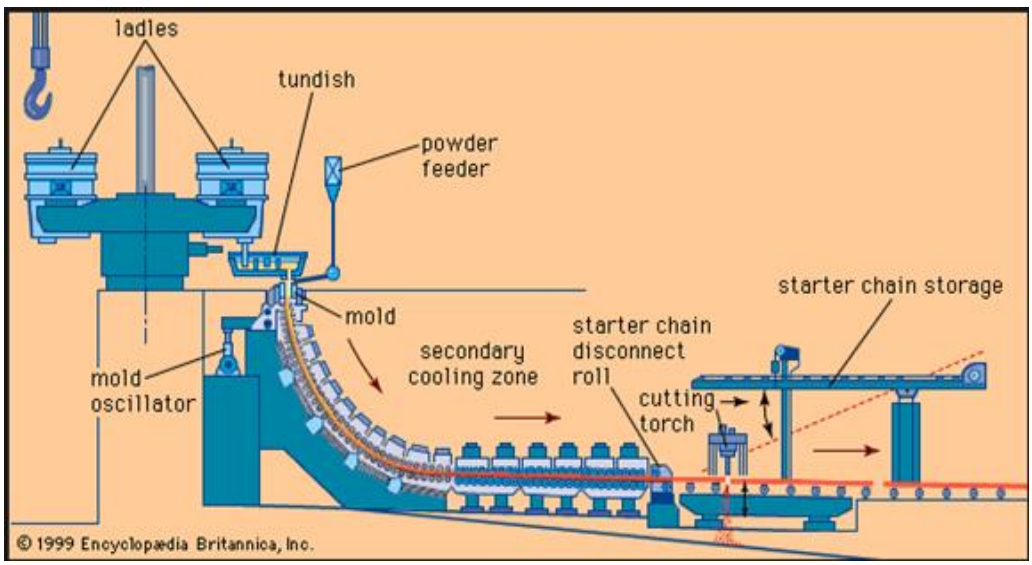

Figure 1. Continuous casting process in steel manufacturing

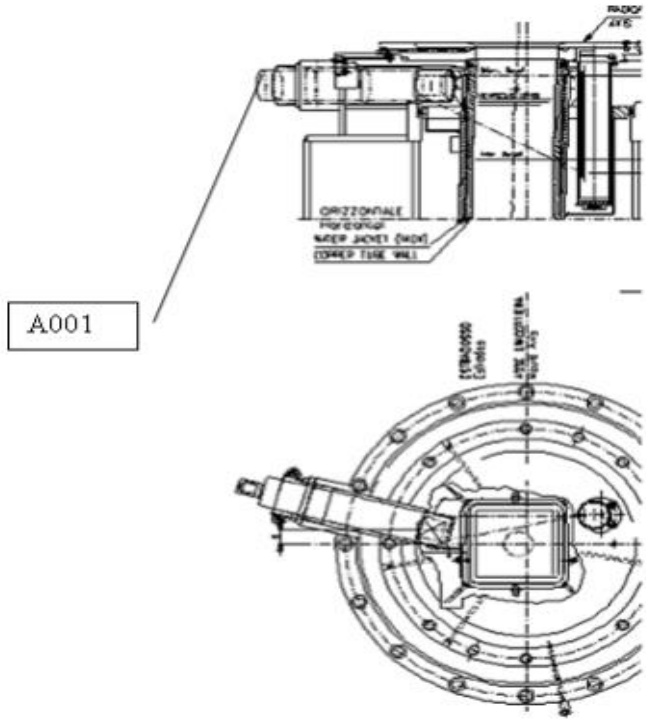

Figure 2. Mould level detector arrangement [21]

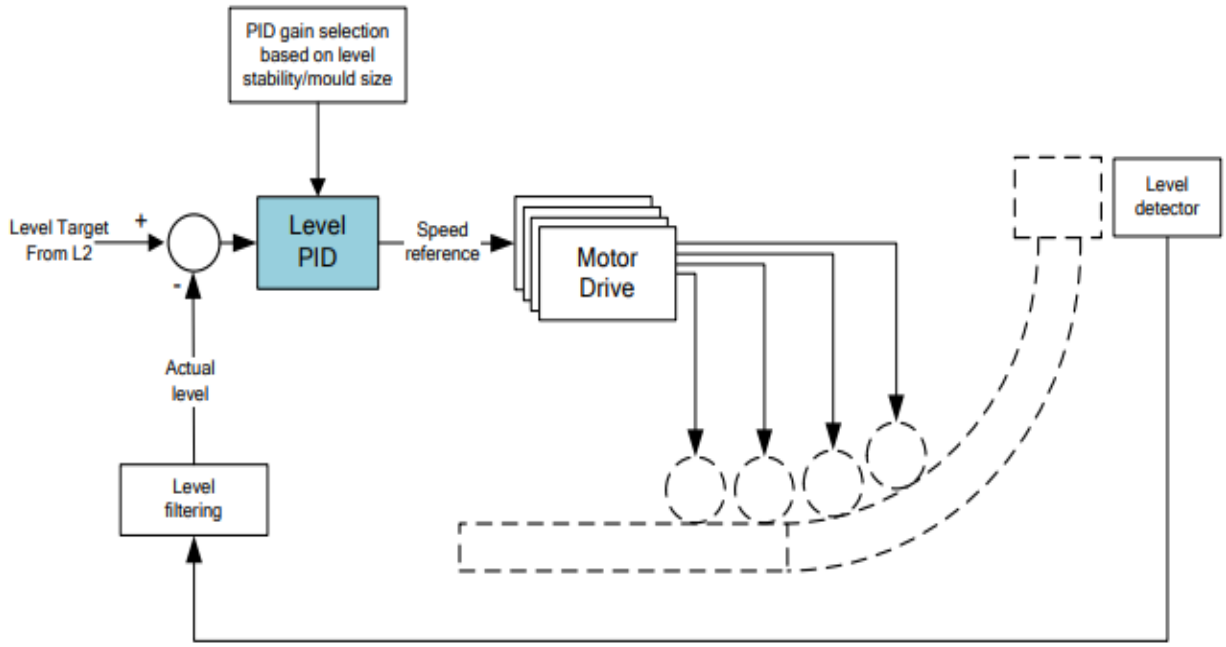

Figure 3. Free stream level control block diagram

3.2 Operator basic interfaces

Control level:

- **Remote mode**: The mould level is controlled by changing the casting speed; it is the normal operating level for casting.
- **Local mode**: The mould level is controlled by the operator from the strand control station, it is used in case of level sensor failure.

Control modes:

- **Manual**: This mode is enabled when on the strand control station the speed control is set to local; the selection is performed using the REMOTE SPEED pushbutton.

When the manual mode is selected, the cast speed is switch to the manual preset reference with the preset ramp coefficient. This manual reference can then be adjusted by acting on the zero spring return selector switch increase - 0 - decrease.

- **Automatic:** This mode is enabled when on the strand control station the speed control is set to remote.

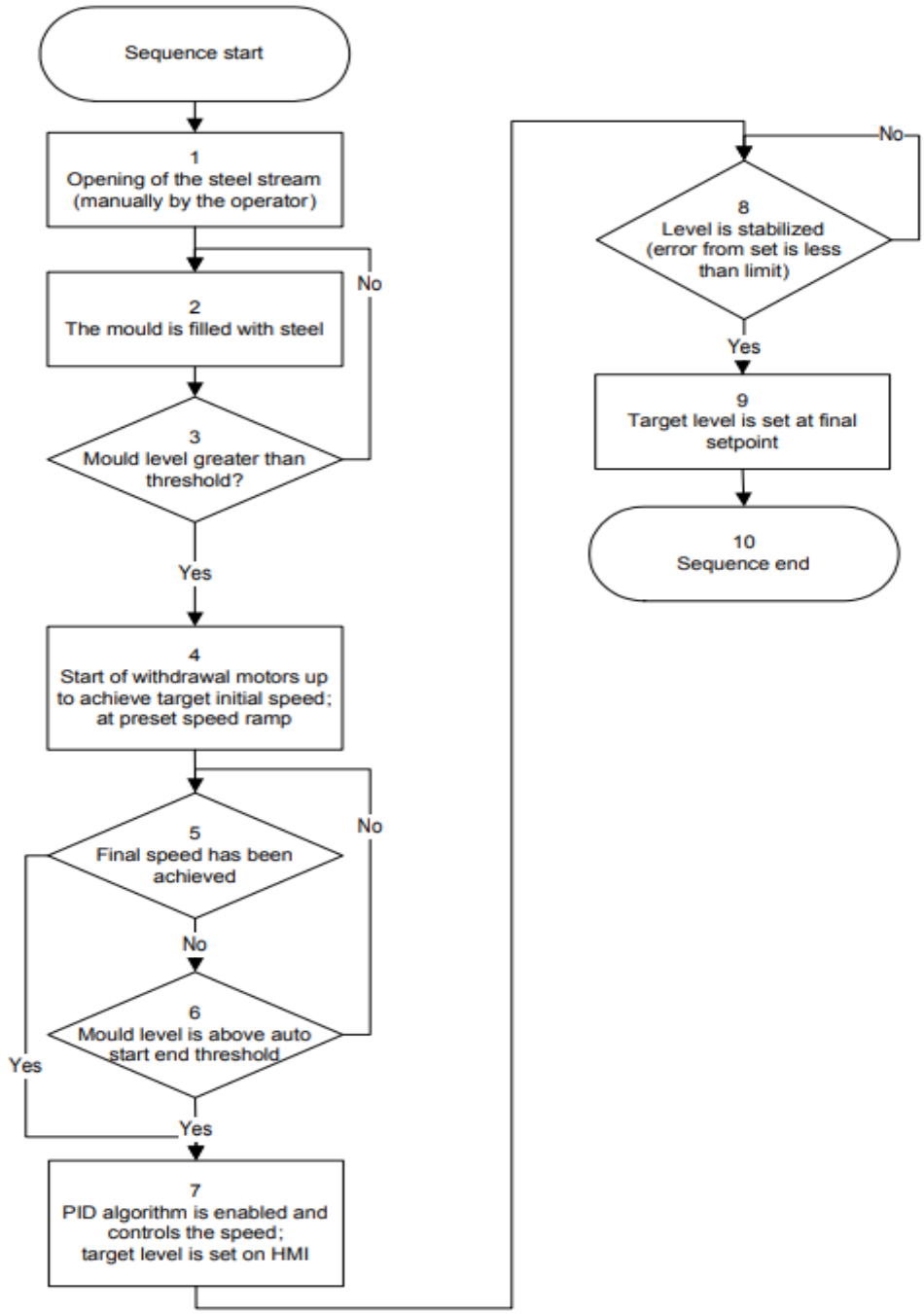

Figure 4. Autostart sequence graph

When the automatic mode is enabled the casting speed is controlled automatically in order to maintain constant the mould level.

The strand control station horn is activated to indicate a system failure as:

- Automatic is selected but the permissions are not achieved
- Mould level is above 90%
- Mould level is below 30%
- Level deviation from setpoint is above 20% [22].

Emergency Closing

It is always enabled and performed with the CNC system.

3.3 Operating sequences

Automatic start sequence

This sequence is started as soon as the auto mode for MLC is selected, then the sequence waits for the operator to manually open the strand.

When the mould level threshold for machine start is reached, the extraction motors are started. Once the level has reached the target level, the sequence ends and the control is switched in automatic [20].

Sequence start

This flowchart (Figure 4) outlines an automated sequence for maintaining and stabilizing the mold level, using PID control to fine-tune the process as it progresses.

4. STPA METHODOLOGY AND APPLICATION

4.1 System-Theoretic Process Analysis (STPA)

STPA is a relatively new hazard analysis technique based

on an extended model of accident causation [23]. In addition to component failures, STPA assumes that accidents can also be caused by unsafe interactions of system components [24, 25].

The STPA can be used even before a design is complete, as it helps guide the design process based on its findings [26]. By focusing on the dynamic, top-down interactions of various system components through control loops [27]. The STPA hazard analysis involves four main steps:

Step 1: Define the Purpose of the Analysis

- **Identify Losses**: Determine unacceptable losses to stakeholders, such as loss of life, property, or mission [28].
- **Identify System-Level Hazards:** Define hazardous system states or conditions that, in worst-case environmental conditions, will lead to losses [29].
- **Identify System-Level Constraints**: Derive constraints that need to be enforced to prevent hazards [30].
- **Refine Hazards (Optional):** Break down system-level hazards into more detailed sub-hazards for complex analyses.

Step 2: Model the Control Structure

Develop a hierarchical control structure that represents the functional relationships and interactions within the system [31]. Include:

- Controllers
- Control actions
- Feedback loops
- Controlled processes [32].

Use abstraction and iteration to manage complexity, starting with a high-level structure and refining it as needed [33].

Step 3: Identify Unsafe Control Actions (UCAs)

For each control action:

Examine how it could lead to the identified hazards [34].

Classify UCAs:

- Not Provided when needed.
- Provided Incorrectly or in an unsafe manner.
- Provided at the Wrong Time or in the Wrong Order.
- Stopped Too Soon or Applied Too Long [35].

Step 4: Identify Loss Scenarios

Develop scenarios explaining how UCA might arise due to:

- Inadequate or incorrect feedback.
- Design errors or inadequate requirements.
- Component failures or unsafe interactions.
- Situations where safe actions are improperly executed [36].

Outputs

- Functional safety constraints and requirements to prevent hazards.
- Mitigation measures or design improvements [37].
- Test plans and evaluation criteria [38-41].

The Figure 5 illustrates the systematic steps involved in conducting a STPA.

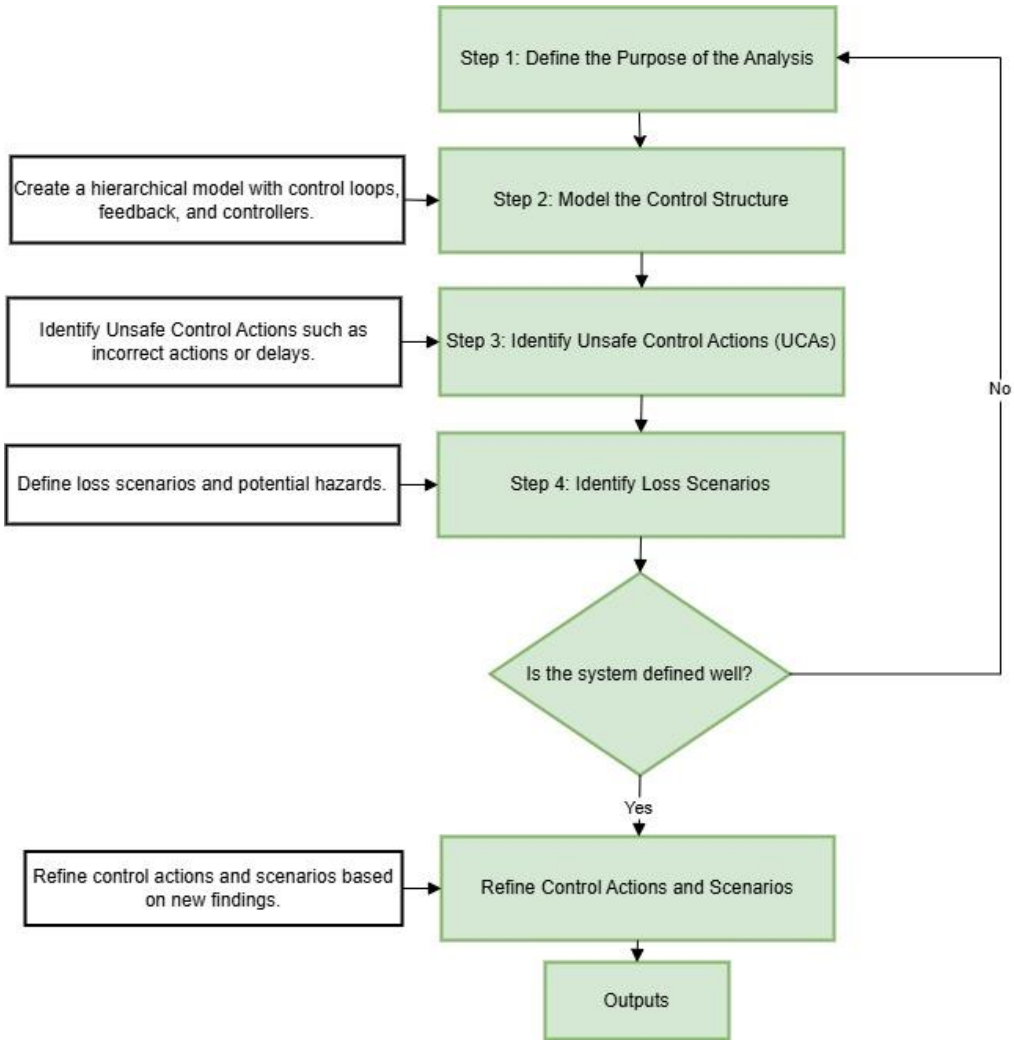

Figure 5. STPA process flowchart

4.2 STPA application

4.2.1 Define purpose of the analysis

Losses:

- **L1**: Personnel Injury or Fatalities: Potential for serious injury or fatalities to operators or nearby personnel.
- **L2**: Environmental Contamination: Emission of potentially harmful byproducts.
- **L3**: Equipment Damage (Economic Loss):

Significant damage to the MLC system components, such as radioactive detectors, PLCs, actuators, or motorized withdrawal drives, leading to expensive repairs or replacement costs. Structural damage to the casting mould or surrounding equipment due to uncontrolled molten steel overflow or other process malfunctions.

- **L4**: Loss of Process Efficiency or Production

Downtime: Reduced production efficiency, quality control issues, or a complete halt in operations resulting in substantial economic losses.

4.2.2 System-level hazards

H-1: Mould level exceeds upper threshold (overflow) [L1, L2, L3, L4]. Potential for molten steel overflow due to failure to control level, leading to safety hazards, environmental contamination, equipment damage, and production downtime.

H-2: Mould level drops below lower threshold (underfill) [L3, L4]. Insufficient steel level in the mould, which may result in casting defects, equipment wear, and interruptions in production.

H-3: Significant instability in the molten steel level [L1, L3, L4]. The mould level fluctuates excessively, reducing control precision, affecting steel quality, and increasing the likelihood of process inefficiencies.

H-4: Loss of controlled molten steel flow from the mould [L1, L3, L4]. The system is unable to regulate the flow of molten steel, resulting in an uncontrolled release that could endanger equipment and personnel.

H-5: Interruption of continuous casting [L1, L3, L4]. A mould level issue disrupts the continuous casting process, causing production delays and reducing overall efficiency.

4.2.3 System-level contraints

SC1: The mould level must not exceed the upper allowable threshold under any operating conditions to prevent overflow and associated hazards [H-1].

SC2: The mould level must be maintained above the lower threshold at all times to ensure adequate steel flow and prevent casting defects [H-2].

SC3: The MLC system must maintain stable operations by minimizing fluctuations in molten steel level to prevent instability and ensure process reliability [H-3].

SC4: The MLC system must regulate molten steel flow precisely under all operating conditions to prevent uncontrolled releases from the mould [H-4].

SC5: The continuous casting process must operate without interruptions caused by MLC issues, ensuring consistent production flow [H-5].

4.2.4 Model the control structure

The control structure for the MLC system in the continuous casting process is illustrated in the Figure 6. This structure integrates human interaction with automated systems to maintain safe and precise control over the molten steel level (see Table 1).

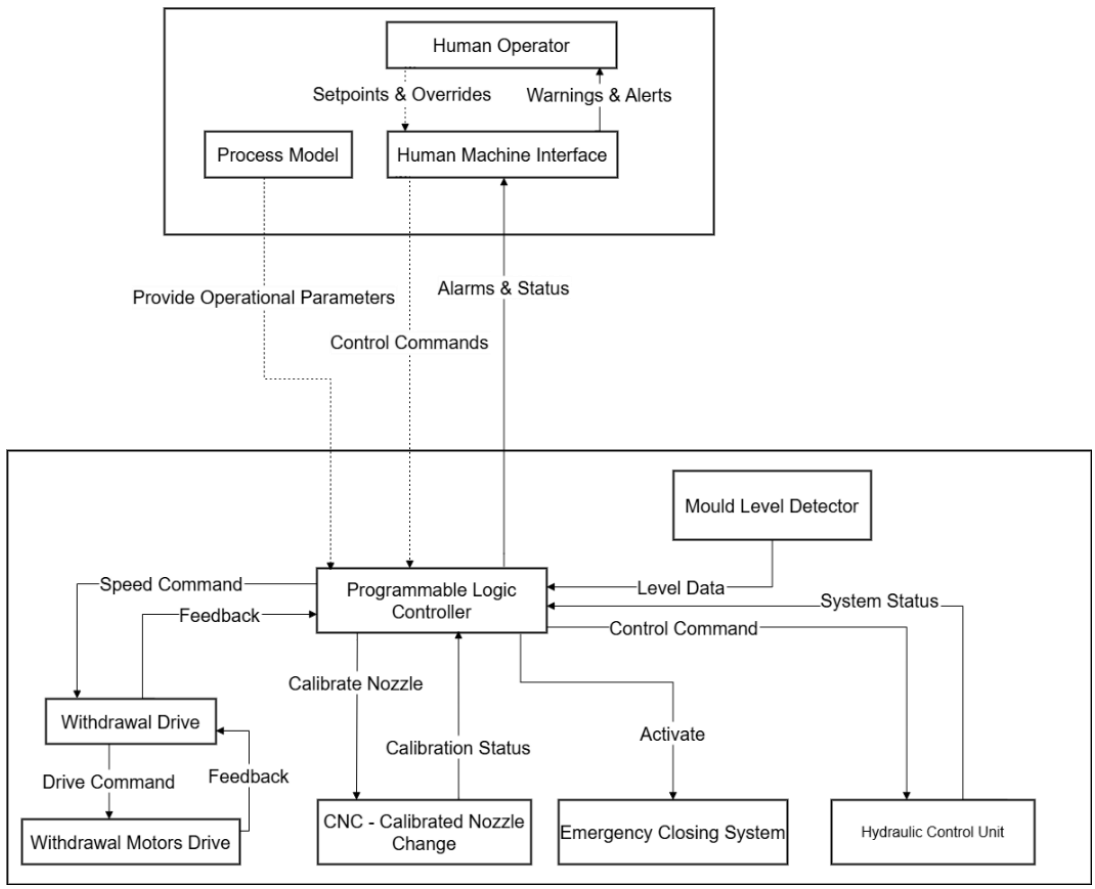

Figure 6. Control structure for the case study

Table 1. Unsafe control action

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too Early, Too Late, out-off Order	Stop Too Soon, Applied Too Long
Adjust Mould Level	UCA-1: The controller does not provide "adjust mould level" command when level is too high or low, causing overflow or underfill [H-1,2,3,4,5]	UCA-2: The controller provides an 'adjust mould level' command when the level is already optimal, causing unnecessary level changes, which can lead to high or low levels and potentially result in overflow or underfill [H-2,3,5]	UCA-3: The controller provides "adjust mould level" command too late, causing excessive level deviation before correction [H-1,3,5]	N/A
Increase Withdrawal Speed	UCA-4: The controller does not provide "increase speed" command when required to prevent overflow [H-2]	UCA-5: The controller provides "increase speed" command when level is optimal or low, leading to potential underfill [H-1,3]	UCA-6: The controller provides "increase speed" command too late, failing to prevent overflow [H-2,3]	N/A
Decrease Withdrawal Speed	UCA-7: The controller does not provide "decrease speed" command when required to prevent underfill [H-1]	UCA-8: The controller provides "decrease speed" command when level is optimal or high, causing overflow [H-2,5]	UCA-9: The controller provides "decrease speed" command too late, leading to excessive fill [H-1,2]	N/A
Setpoints & Overrides from Human Operator to HMI	UCA-10: operator does not set the correct mould level target during initialization, process changes, or adjustments, leading to deviations from the optimal level and resulting in potential overflow or underfill [H-1,2]	UCA-11: Operator sets a level override unnecessarily, causing unpredictable level changes [H-2,3]	UCA-12: Operator adjusts setpoints too late to correct level deviation, causing prolonged instability [H-1,2]	UCA-13: Operator keeps override active too long, leading to non-standard operation [H-2]
Emergency Closing System	UCA-14: The emergency close command is not activated during a critical level event, risking overflow [H-2,5]	UCA-15: The emergency close system is triggered without need, disrupting flow and causing underfill [H-1,5]	UCA-16: The emergency close command is delayed, failing to prevent overflow in time [H-2,3]	N/A

Table 2. UCA prioritization and risk level

UCA ID	Prob. (P)	Sev. (S)	RL = P×S
UCA-1	4	5	20
UCA-2	3	4	12
UCA-3	4	4	16
UCA-4	3	4	12
UCA-5	3	3	9
UCA-6	4	4	16
UCA-7	3	3	9
UCA-8	3	4	12
UCA-9	4	4	16
UCA-10	4	5	20
UCA-11	3	3	9
UCA-12	4	4	16
UCA-13	3	3	9
UCA-14	4	5	20
UCA-15	3	3	9
UCA-16	4	5	20

4.2.5 Identify UCA

To identify Unsafe Control Actions (UCAs), the control structure of the Mould Level Control (MLC) system is first analyzed (see Figure 6). This structure captures the interactions between the human operator, Programmable Logic Controller (PLC), Human-Machine Interface (HMI), and actuating elements such as the withdrawal drive and emergency closing system. For each control action issued by these components, we examine the conditions under which that action—if not provided, provided incorrectly, provided too early or too late, or applied for too long—could lead to hazardous states. These scenarios are systematically listed in the tables to highlight how inadequate or inappropriate control decisions can compromise system safety and stability. The identified UCAs form the foundation for subsequent loss scenario development and mitigation strategies.

Table 3. UCA risk ranking

UCA ID	RL = P×S
UCA-1 UCA-10 UCA-14 UCA-16	20
UCA-3 UCA-6 UCA-9 UCA-12	16
UCA-2 UCA-4 UCA-8	12
UCA-5 UCA-7 UCA-11 UCA-13 UCA-15	9

4.2.6 Prioritization and risk ranking of UCAs

In coordination with the Electrical and Instrumentation Maintenance Department, the Safety Department, and the production team of our meltshop plant, we utilized the existing HIRA of the plant to prioritize and rank the UCAs. Based on

the HIRA, we evaluated the probability (P) and severity (S) of each UCA, and calculated the risk level (RL) as the product of P and S. Tables 2 and 3 illustrate the prioritization of UCAs according to their respective risk levels. This risk ranking allows us to focus on the most critical UCAs.

4.2.7 Identify loss scenarios

➢ **Control Action: Adjust Mould Level:**

UCA-1: The controller does not provide "adjust mould level" command when level is too high or low, causing overflow or underfill [H-1,2,3,4,5].

- **LS-1**: The controller does not provide "adjust mould level" command due to incorrect sensor feedback showing level within the acceptable range.
- **LS-2**: The controller does not provide "adjust mould level" command due to logic errors in the software causing the level condition to be misinterpreted.
- **LS-3**: The controller does not provide "adjust mould level" command due to a failure in the control hardware (e.g., power issue or communication failure with the HMI).

UCA-2: The controller provides "adjust mould level" command when level is optimal, causing unnecessary level change [H-2,3,5].

- **LS-4**: The controller provides "adjust mould level" command unnecessarily due to a miscalibrated sensor indicating an incorrect level.
- **LS-5**: The controller provides "adjust mould level" command due to an erroneous software update or bug affecting the controller logic.

UCA-3: The controller provides "adjust mould level" command too late, causing excessive level deviation before correction [H-1,3,5].

- LS-6: The controller provides "adjust mould level" command too late due to delayed response from the level sensor.
- LS-7: The controller provides "adjust mould level" command too late due to communication latency between the sensor and the controller.

➢ **Control Action: Increase Withdrawal Speed**

UCA-4: The controller does not provide "increase speed" command when required to prevent overflow [H-2].

- **LS-8**: The controller does not provide "increase speed" command due to sensor malfunction, failing to detect the need for speed increase.
- **LS-9**: The controller does not provide "increase speed" command due to a fault in the controller logic misinterpreting level data.

UCA-5: The controller provides "increase speed" command when level is optimal or low, leading to potential underfill [H-1,3].

- **LS-10**: The controller provides "increase speed" command due to a software error in the HMI.
- **LS-11**: The controller provides "increase speed" command due to faulty sensor data, misinterpreting a low-level condition.

UCA-6: The controller provides "increase speed" command too late, failing to prevent overflow [H-2,3].

- **LS-12**: The controller provides "increase speed" command too late due to a communication delay between the HMI and PLC.
- **LS-13:** The controller provides "increase speed" command too late due to slow processing in the controller caused by software inefficiencies.

➢ **Control Action: Decrease Withdrawal Speed**

UCA-7: The controller does not provide "decrease speed" command when required to prevent underfill [H-1].

- **LS-14**: The controller does not provide "decrease speed" command due to faulty sensor readings indicating adequate level.
- **LS-15**: The controller does not provide "decrease speed" command due to a hardware issue in the controller preventing proper command issuance.

UCA-8: The controller provides "decrease speed" command when level is optimal or high, causing overflow [H-2,5].

- **LS-16**: The controller provides "decrease speed" command due to incorrect feedback from the level sensor.
- **LS-17**: The controller provides "decrease speed" command due to a programming error in the controller.

UCA-9: The controller provides "decrease speed" command too late, leading to excessive fill [H-1,2].

- **LS-18**: The controller provides "decrease speed" command too late due to delayed sensor response.
- **LS-19**: The controller provides "decrease speed" command too late due to delayed processing within the control logic.

➢ **Control Action: Setpoints & Overrides from Human Operator to HMI**

UCA-10: Operator does not set correct mould level target, leading to deviation from optimal level [H-1,2].

- **LS-20**: Operator does not set correct target due to a display error on the HMI, causing misinterpretation of level requirements.
- **LS-21**: Operator fails to set correct target due to inadequate training on override functions.

UCA-11: Operator sets a level override unnecessarily, causing unpredictable level changes [H-2,3].

- **LS-22**: Operator sets an override unintentionally due to HMI interface complexity.
- **LS-23**: Operator sets an override based on incorrect sensor data indicating a deviation.

UCA-12: Operator adjusts setpoints too late to correct level deviation, causing prolonged instability [H-1,2].

- **LS-24**: Operator delays adjustment due to poor data visualization on the HMI.
- **LS-25:** Operator delays adjustment due to inadequate alerts or communication issues.

UCA-13: Operator keeps override active too long, leading to non-standard operation [H-2].

- **LS-26**: Operator forgets to remove override due to lack of system prompts.
- **LS-27**: Operator keeps override due to inadequate knowledge of override timing requirements.

➢ **Control Action: Emergency Closing System**

UCA-14: The emergency close command is not activated during a critical level event, risking overflow [H-2,5].

- **LS-28:** The emergency close system does not activate due to power supply failure.
- **LS-29:** The emergency close system does not activate due to controller hardware malfunction.

UCA-15: The emergency close system is triggered without need, disrupting flow and causing underfill [H-1,5].

- **LS-30**: The emergency system triggers unnecessarily due to a sensor error indicating high level.
- **LS-31**: The emergency system triggers due to misconfiguration in the control logic.

UCA-16: The emergency close system is delayed, failing to prevent overflow in time [H-2,3].

- **LS-32**: The emergency close system is delayed due to communication delay between the sensor and the controller.
- **LS-33**: The emergency close system is delayed due to a controller software issue that slows the command execution.

Safety requirements are shown in the Table 4.

Table 4. Safety requirements

Loss Scenarios	Safety Requirements
LS-1, LS-5, LS-6, LS-11, LS-14, LS-17, LS-18, LS-21, LS-23, LS-24	- Use faster and more responsive sensors. - Ensure regular sensor calibration and testing to ensure accurate readings. - Optimize sensor placement to ensure quicker detection. - Improve feedback loop settings and reduce any unnecessary processing steps.
LS-2, LS-4, LS-9, LS-12, LS-15, LS-20, LS-22, LS-25	- Upgrade the controller's hardware or streamline the software for faster processing. - Prioritize critical control paths to minimize delays. - Optimize algorithms and, if necessary, upgrade the controller's resources.
LS-7, LS-16, LS-19, LS-26	- Upgrade to high-speed communication protocols and reduce network traffic. - Introduce redundant communication paths and improve error detection mechanisms.
LS-29, LS-30, LS-31, LS-32, LS-34	- Provide continuous operator training and feedback to build confidence. - Develop clear and concise operational procedures for operators. - Regularly review manual override settings to avoid unnecessary delays. - Periodically review and adjust setpoints based on actual performance. - Optimize task management to reduce operator fatigue. - Minimize external pressure and clarify operational priorities for operators. - Provide decision-support tools for setpoint adjustments.
LS-28, LS-33	- Redesign HMI for better usability, focusing on simplicity and clarity. - Highlight critical information on the HMI. - Ensure real-time updates and data accuracy on the HMI. - Improve the speed and accuracy of condition monitoring and alarms.
LS-3, LS-8, LS-10, LS-13, LS-27	- Use stable power sources, voltage regulators, or UPS systems to ensure consistent performance. - Install backup power systems to maintain stable operation during power outages.

5. CONCLUSION

In this study, we used STPA to examine the safety and reliability of MLC in Free Stream operations within the continuous casting process. Given the critical role of MLC in maintaining product quality and preventing defects, it's essential to manage hazards that could disrupt mould level stability. Free Stream operations pose unique challenges, as the system must handle a highly dynamic environment where traditional hazard analysis methods might overlook critical interactions.

Through STPA, we identified key UCAs and associated loss scenarios that could lead to issues like level instability, overflow, or underfill—each with potential consequences for both process safety and steel quality. Our analysis revealed specific areas for improvement, such as optimizing sensor accuracy and placement, refining controller feedback loops, and improving communication protocols within the system.

The insights gained from this study highlight the practical benefits of using STPA for complex industrial systems. The recommendations we provided—covering sensor upgrades, controller adjustments, and operator support enhancements—offer actionable steps to strengthen the MLC system's resilience. This work not only reinforces the value of a systems-theoretic approach in continuous casting but also opens doors for future studies to further enhance the safety and robustness of manufacturing processes in steel production.

However, this study also presents certain limitations. The proposed mitigation strategies have not yet been validated through simulation or experimental testing. Additionally, external disturbances such as signal noise, fluctuating casting speeds, or human operator delays were not quantitatively modelled in this analysis. These factors could influence system behaviour and should be considered in future evaluations.

Future work may include simulating the MLC control environment under varying operational conditions to test the effectiveness of proposed mitigation measures. Further studies could also explore hybrid approaches that combine STPA with traditional techniques (e.g., FMEA or HAZOP) for a more comprehensive safety assessment. Expanding the scope of the analysis to other subsystems involved in the continuous casting process may provide additional insights into systemic risks across the steel production line.

REFERENCES

[1] You, B., Kim, M., Lee, D., Lee, J., Lee, J.S. (2011). Iterative learning control of molten steel level in a continuous casting process. Control Engineering Practice, 19(3): 234-242. https://doi.org/10.1016/j.conengprac.2010.11.009

[2] Tacke, K.H. (2014). Irregular and fluctuating phenomena in continuous casting. In 8th European Continuous Casting Conference and Symposium in Numerical & Physical Modeling, ASMET, pp. 23-26.

[3] Smutný, L., Farana, R., Víteĉek, A., Kaĉmář, D. (2005). Mould level control for the continuous steel casting. IFAC Proceedings Volumes, 38(1): 163-168.

https://doi.org/10.3182/20050703-6-CZ-1902.01706
[4] Kim, M., Moon, S., Na, C., Lee, D., Kueon, Y., Lee, J.S. (2011). Control of mold level in continuous casting based on a disturbance observer. Journal of Process Control, 21(7): 1022-1029. https://doi.org/10.1016/j.jprocont.2011.06.003
[5] Furtmueller, C., Del Re, L. (2008). Control issues in continuous casting of steel. IFAC Proceedings Volumes, 41(2): 700-705. https://doi.org/10.3182/20080706-5-KR-1001.00118
[6] Dussud, M., Galichet, S., Foulloy, L.P. (1998). Application of fuzzy logic control for continuous casting mold level control. IEEE Transactions on Control Systems Technology, 6(2): 246-256. https://doi.org/10.1109/87.664191
[7] Sotnik, S.V. (2024). Development of automated control system for continuous casting. Radio Electronics Computer Science Control, (2): 181-189. https://doi.org/10.15588/1607-3274-2024-2-18
[8] Shuaib, N.A., Sobri, S.A., Darmawan, V.E.B., Assyahid, W.A.R., Qian, O.J., Wei, S.J., Hern, T.Y. (2021). Risk assessment in a metal processing factory in Malaysia. AIP Conference Proceedings, 2339(1): 020208. https://doi.org/10.1063/5.0044243
[9] Sadi, S., Zuhrohtun, Z., Kusumawardhani, I. (2021). Risk management in the metal casting industry: Case in Ceper Klaten. IPTEK Journal of Proceedings Series, (1): 182-185. https://doi.org/10.12962/j23546026.y2020i1.8485
[10] Putri, A.S., Nuruddin, U.A. (2022). Occupational safety and health at metal casting company. Journal of Engineering and Applied Technology, 3(2): 80-86. https://doi.org/10.21831/jeatech.v3i2.52482
[11] Sharma, A., Mishra, M.K., Trivedi, A. (2023). Hazard assessment and its control in bulk material handling process of an integrated steel plant. International Research Journal of Engineering and Technology (IRJET), 10(2): 355-366.
[12] Naeini, A.M., Nadeau, S. (2022). STPA systemic approach for OHS and operational risk analysis of data glove use in 4.0 assembly. CIRP Journal of Manufacturing Science and Technology, 39: 317-331. https://doi.org/10.1016/j.cirpj.2022.09.003
[13] Naeini, A.M., Nadeau, S. (2021). FRAM and STAMP: New Avenue for Risk Analysis in Manufacturing in the Era of Industry 4.0. Arbeit HUMAINE gestalten, Paper B.12.7.
[14] Zacharaki, A., Kostavelis, I., Dokas, I. (2021). Decision making with STPA through Markov decision process, a theoretic framework for safe human-robot collaboration. Applied Sciences, 11(11): 5212. https://doi.org/10.3390/app11115212
[15] Bu, Y., Wu, Y., Li, X., Pei, Y. (2023). Operational risk analysis of a containerized lithium-ion battery energy storage system based on STPA and fuzzy evaluation. Process Safety and Environmental Protection, 176: 627-640. https://doi.org/10.1016/j.psep.2023.06.023
[16] Karevan, A., Nadeau, S. (2023). The role of industry 5.0 in reducing the risk of human error in manufacturing-A critical literature review. In CIGI Qualita MOSIM 2023-QC Canada, Paper 3812.
[17] Manzur Tirado, A.M., Brown, R., Valdez Banda, O.A. (2019). Risk and safety management of autonomous systems: A literature review and initial proposals for the maritime industry. Aalto University.
[18] Wang, Z., Shan, Q., Cui, H., Pan, H., Lu, B., Shi, X., Wen, J. (2024). Characteristic analysis of mold level fluctuation during continuous casting of Ti-bearing IF steel. Journal of Materials Research and Technology, 31: 1367-1378. https://doi.org/10.1016/j.jmrt.2024.06.156
[19] Wondris, E., Nutting, J. (2025). Continuous casting. https://www.britannica.com/technology/steel/Continuous-casting.
[20] Agarwal, P. K. (1979). Case study of spray design for a continuous billet caster. Doctoral dissertation, University of British Columbia.
[21] Nath, J. (2023). Casting Equipment Engineering Guide. ASM International.
[22] Šarler, B., Vertnik, R., Šaletić, S., Manojlović, G., Cesar, J. (2005). Application of continuous casting simulation at Štore Steel. BHM Berg-und Hüttenmännische Monatshefte, 150(9): 300-306. https://doi.org/10.1007/BF03165327
[23] France, M.E. (2017). Engineering for humans: A new extension to STPA, Doctoral dissertation, Massachusetts Institute of Technology.
[24] Krauss, S.S., Rejzek, M., Hilbes, C. (2015). Tool qualification considerations for tools supporting STPA. Procedia Engineering, 128: 15-24. https://doi.org/10.1016/j.proeng.2015.11.500
[25] Zou, J. (2018). Systems-Theoretic Process Analysis (STPA) applied to the operation of fully autonomous vessels. Master's thesis, NTNU.
[26] Guzman, N.H.C., Zhang, J., Xie, J., Glomsrud, J.A. (2021). A comparative study of STPA-extension and the UFoI-E method for safety and security co-analysis. Reliability Engineering & System Safety, 211: 107633. https://doi.org/10.1016/j.ress.2021.107633
[27] Merrett, H.C., Horng, J.J., Piggot, A., Qandour, A., Tong, C.W. (2019). Comparison of STPA and bow-tie method outcomes in the development and testing of an automated water quality management system. MATEC Web of Conferences, 273: 02008. https://doi.org/10.1051/matecconf/201927302008
[28] Oginni, D., Camelia, F., Chatzimichailidou, M., Ferris, T.L. (2023). Applying System-Theoretic Process Analysis (STPA)-based methodology supported by Systems Engineering models to a UK rail project. Safety Science, 167: 106275. https://doi.org/10.1016/j.ssci.2023.106275
[29] Abdulkhaleq, A., Wagner, S., Leveson, N. (2015). A comprehensive safety engineering approach for software-intensive systems based on STPA. Procedia Engineering, 128: 2-11. https://doi.org/10.1016/j.proeng.2015.11.498
[30] Abdulkhaleq, A., Wagner, S., Lammering, D., Boehmert, H., Blueher, P. (2017). Using STPA in compliance with ISO 26262 for developing a safe architecture for fully automated vehicles. arXiv preprint, arXiv:1703.03657. https://doi.org/10.48550/arXiv.1703.03657
[31] Bas, E. (2022). Application of systems theoretic process analysis and failure modes and effects analysis to process reliability and occupational safety and health in construction projects. International Journal of Safety and Security Engineering, 12(1): 1-11. https://doi.org/10.18280/ijsse.120101
[32] Leveson, N.G. (2011). Engineering a Safer World: Systems Thinking Applied to Safety. The MIT Press. https://doi.org/10.7551/mitpress/8179.001.0001

[33] Bensaci, C., Zennir, Y., Pomorski, D., Innal, F., Liu, Y. (2021). Distributed vs. hybrid control architecture using STPA and AHP-Application to an autonomous mobile multi-robot system. International Journal of Safety and Security Engineering, 11(1): 1-12. https://doi.org/10.18280/ijsse.110101

[34] Li, M., Yan, F., Niu, R., Xiang, N. (2021). Identification of causal scenarios and application of leading indicators in the interconnection mode of urban rail transit based on STPA. Journal of Rail Transport Planning & Management, 17: 100238. https://doi.org/10.1016/j.jrtpm.2021.100238.

[35] Shin, J., Choi, J.G., Lee, J.W., Lee, C.K., Song, J.G., Son, J.Y. (2021). Application of STPA-SafeSec for a cyber-attack impact analysis of NPPs with a condensate water system test-bed. Nuclear Engineering and Technology, 53(10): 3319-3326. https://doi.org/10.1016/j.net.2021.04.031

[36] Chaal, M., Banda, O.A.V., Glomsrud, J.A., Basnet, S., Hirdaris, S., Kujala, P. (2020). A framework to model the STPA hierarchical control structure of an autonomous ship. Safety Science, 132: 104939. https://doi.org/10.1016/j.ssci.2020.104939.

[37] Chen, S., Khastgir, S., Jennings, P. (2021). Analyzing national responses to COVID-19 pandemic using STPA. Safety Science, 138: 105195. https://doi.org/10.1016/j.ssci.2021.105195

[38] Yang, C. (2014). Software safety testing based on STPA. Procedia Engineering, 80: 399-406. https://doi.org/10.1016/j.proeng.2014.09.097

[39] Sulaman, S.M., Beer, A., Felderer, M., Höst, M. (2019). Comparison of the FMEA and STPA safety analysis methods–A case study. Software Quality Journal, 27: 349-387. https://doi.org/10.1007/s11219-017-9396-0

[40] Bensaci, C., Zennir, Y., Pomorski, D. (2020). A New Approach to System Safety of human-multi-robot mobile system control with STPA and FTA. Algerian Journal of Signals and Systems (AJSS), 5(1): 79-85.

[41] Bensaci, C., Zennir, Y., Pomorski, D. (2018). A comparative study of STPA hierarchical structures in risk analysis: The case of a complex multi-robot mobile system. In 2018 2nd European Conference on Electrical Engineering and Computer Science (EECS), Bern, Switzerland, pp. 400-405. https://doi.org/10.1109/EECS.2018.00080