International Journal of Safety and Security Engineering
Vol. 16, No. 1, January, 2026, pp. 43-53
Journal homepage: http://iieta.org/journals/ijsse

Application of Systems-Theoretic Process Analysis and D-HiGraph Modeling for Risk Analysis in a Continuous Casting Machine

Khalid Larit[1], Islam Berri[1], Youcef Zennir[2], Manuel Rodriguez[3], Mohamed Benghanem[4*], Yiliu Liu[5]

[1] LRPCSI Laboratory Skikda, University of Skikda, Skikda 21000, Algeria
[2] Automatic Laboratory of Skikda, University of Skikda, Skikda 21000, Algeria
[3] Department of Chemical Engineering, Polytechnic University of Madrid, Madrid 28006, Spain
[4] Department of Physics, Islamic University of Madinah, Madinah 42351, Saudi Arabia
[5] Faculty of Engineering, NTNU University, Trondheim NO-7491, Norway

Corresponding Author Email: mbenghanem@iu.edu.sa

https://doi.org/10.18280/ijsse.160104

Received: 4 October 2025
Revised: 6 January 2026
Accepted: 14 January 2026
Available online: 31 January 2026

Keywords:
industrial safety, Systems-Theoretic Process Analysis, continuous casting machine, risk analysis, control structure modeling, D-HiGraph

ABSTRACT

Continuous casting machines (CCMs) play a crucial role in steel production, but their complexity and high level of automation pose significant challenges to ensuring operational safety. This study explores a combined approach using Systems-Theoretic Process Analysis (STPA) and D-HiGraph modeling to identify and better understand potential hazards in a CCM unit. STPA is used to define possible losses, hazards, and unsafe control actions (UCAs) within the system. To support the analysis, a control structure model is developed using D-HiGraph, which provides a clear, hierarchical view of how controllers, sensors, actuators, and human operators interact. The results highlight several critical UCAs, particularly in areas such as mold level regulation, adjustment of withdrawal speed, and emergency shutdown procedures. By visualizing these relationships with D-HiGraph, it becomes easier to trace the origin of unsafe scenarios and gain deeper insight into system behavior. Overall, this integrated method offers a structured and effective way to improve safety analysis in CCMs and contributes to more robust design and operational strategies in steelmaking environments.

1. INTRODUCTION

Safety is of paramount importance in the steelmaking industry, especially within continuous casting machine (CCM) systems, which are critical, automated subsystems [1]. The integration of technical, operational, and organizational changes to enhance the capacity and performance of rail networks highlights the ever-growing challenge of ensuring safety in complex systems [2]. Traditional risk analysis methods like Failure Mode and Effects Analysis (FMEA) and Hazard and Operability Studies (HAZOP) have been foundational in identifying potential hazards [3]. However, these methods often fall short when dealing with the intricate, dynamically evolving nature of modern industrial processes. Modern industrial processes are developing toward large scale, diversification, and complexity, exhibiting strong non-linearity and dynamically time-varying characteristics, leading to a challenge in fault monitoring [4]. FMEA, for instance, typically focuses on component failures and their direct effects, which may not adequately capture system-level interactions and emergent behaviors that can lead to accidents. HAZOP studies, while more comprehensive, can be resource-intensive and may not effectively address the complexities arising from software and human factors in automated systems [5]. The limitations of traditional methods necessitate the adoption of more advanced techniques that can provide a holistic view of system safety. Traditional methods may struggle to fully capture the nuances of complex automated systems, especially in identifying potential losses. Systems-Theoretic Process Analysis (STPA) offers a more relevant approach for analyzing safety in complex automated systems like CCMs. STPA, rooted in system theory, allows for the identification of hazards arising from inadequate control actions and system-level interactions rather than just component failures. By modeling the control structure and identifying unsafe control actions (UCAs), STPA provides a framework for understanding how system design and operational decisions can contribute to potential accidents. The initial step in STPA involves defining the purpose of the analysis, followed by modeling the control structure to understand the system's control mechanisms. Identifying UCAs and loss scenarios (LS) is a crucial step in preventing accidents and hazards. The motivation for combining STPA with D-HiGraph modeling stems from the need for a structured approach to capture both the functional and structural aspects of process plants. D-HiGraph is a functional modeling technique that represents the functionality of the system, its goals, and the relationships between these functions, goals, and the devices that perform them. By integrating D-HiGraph with STPA, a more comprehensive and traceable analysis of hazards becomes possible. D-HiGraph captures functional and structural aspects, presenting the system's functionality and the

relationships between functions, goals, and devices. The use of D-HiGraph facilitates visualization of system dynamics and improves the traceability of hazards, offering a clearer understanding of how various components interact and contribute to potential risks [6]. This research aims to enhance safety and reliability in CCM systems by applying a joint approach of STPA and D-HiGraph modeling to identify potential system-level hazards. The primary objective is to model system-level losses, hazards, constraints, control actions, and UCAs using STPA, while implementing D-HiGraph to build a structured control model that represents the hierarchical interactions among controllers, sensors, actuators, and operators [7]. This integrated methodology seeks to provide a more effective framework for safety design and operation in steelmaking plants, ultimately promoting safer and more reliable continuous casting processes. Continuous casting production is an important stage in smelting high-quality steel, and automatic casting control based on artificial intelligence is a key technology to improve the continuous casting process and the product quality. The ability to predict the quality of each continuous casting product will greatly increase the rolled product rate and reduce the scrap rate and production management cost [8].

2. PRINCIPLE OF CONTINUOUS CASTING MACHINE

Continuous casting is a crucial process in steelmaking, directly impacting product quality and production efficiency. It involves a complex interplay of operational procedures, automation features, and safety-critical components [9]. Artificial intelligence is used to improve the continuous casting process and product quality. The continuous casting process, illustrated by Figure 1, begins with molten steel being transferred from a furnace to a tundish, which acts as a reservoir to ensure a consistent flow rate. From the tundish, the molten steel flows through a submerged entry nozzle (SEN) into a water-cooled mold, where the outer layer of the steel solidifies. The solidifying strand is then continuously withdrawn from the mold through a series of rollers that support it and control its shape. The water flow rate in the secondary cooling zone is crucial to the slab quality. As the strand moves further down the line, it is cooled by water sprays, completing the solidification process [10]. Finally, the fully solidified strand is cut into desired lengths by mechanical shears or torches. Modern CCMs incorporate a variety of automation features to optimize the process and ensure consistent quality. Automatic casting control systems regulate the flow of molten steel into the mold by controlling the opening degree of the stopper rod. These systems often use feedback from sensors that monitor the level of molten steel in the mold, adjusting the flow rate to maintain a stable level. Real-time simulation models replicate the continuous casting process based on the input parameters, allowing for a virtual representation of what is happening in the actual casting machine. Another important automation feature is the control of the roll gap in the caster segment. Precise control of the roll gap is essential for maintaining the desired shape and dimensions of the cast strand [11]. Automated systems use sensors to measure the roll gap and make adjustments to compensate for thermal expansion and wear. The CCM operation involves data collection, testing for correctness, and use in calculations. Safety is a paramount concern in continuous casting operations due to the high temperatures and heavy machinery involved. Several safety-critical components are integrated into the design of the machine to protect workers and prevent accidents. Emergency shutdown systems are in place to quickly stop the machine in the event of a malfunction or hazardous condition. These systems are designed to halt the flow of molten steel, stop the movement of the strand, and activate alarms. The SEN is also a critical component for safety. It is designed to deliver the liquid steel into the mold in a controlled manner, minimizing turbulence and protecting the liquid steel from oxidation. Clogging on SEN not only impairs the quality of the product but also results in lower process yield, resulting in losses [12]. Monitoring systems are used to detect clogging in the SEN, which may disrupt the smooth flow of liquid steel and affect the quality and productivity of the casting process. The rollers that support the strand are also safety-critical components. If a roller fails, it can cause the strand to sag or break, potentially leading to a spill of molten steel. Regular inspection and maintenance of the rollers are essential to ensure their proper functioning. The reconditioning of CCM rollers can be done by laser cladding [13].

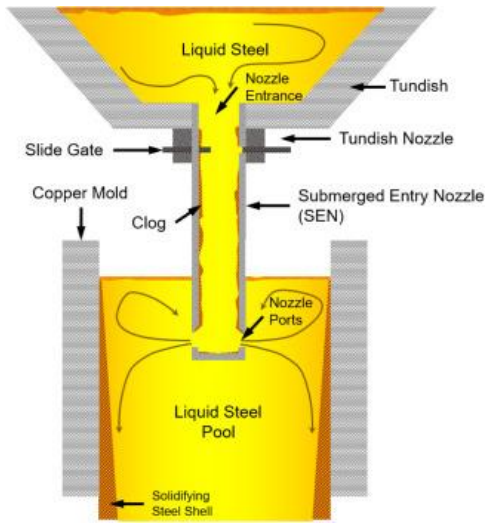

Figure 1. Schematic diagram of the continuous casting process

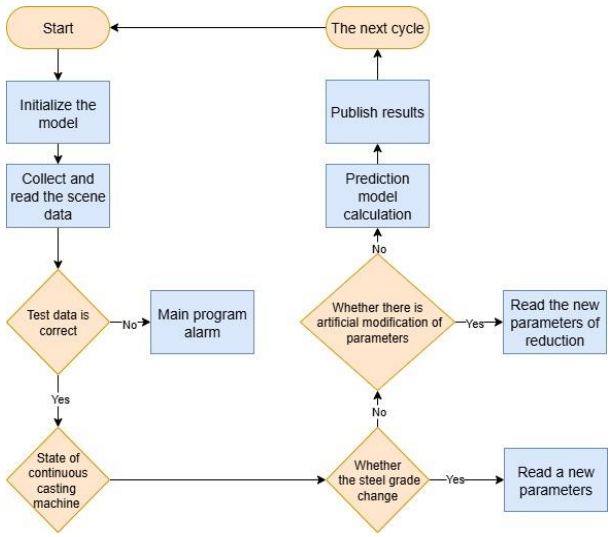

Figure 2. Cyclic process for managing and predicting aspects related to the continuous casting machine (CCM) operation

The diagram shows the tundish, nozzle entrance and tundish nozzle, slide gate, copper mold, SEN, and nozzle ports.

Liquid steel first enters the tundish, then passes through the tundish nozzle and the slide-gate controlled section, then enters the SEN and is discharged into the liquid-steel pool in the mold through the nozzle ports.

The flowchart in Figure 2 starts with the "Start" node, which initiates the process and continues in a cyclic fashion. The first step is to "Initialize the model", then "Collect and read the scene data" is carried out. If the "Test data is correct," the process proceeds to check the "State of continuous casting machine". After the prediction model calculation, the results are "Publish[ed]", and then the process loops back to the start for "The next cycle". The steel industry accounts for a large proportion of power consumption in industries, so optimization of steelmaking energy efficiency is very important. Production scheduling can be combined with equipment energy efficiency indicators, establishing an optimization model for steelmaking energy efficiency scheduling and determining the shutdown strategy of steelmaking equipment sets [14]. A computer-aided planning and scheduling system can be used for CCM.

3. METHODOLOGY

STPA originates from the Systems-Theoretic Accident Model and Processes (STAMP), which considers accidents as a result of inadequate control actions rather than component failures [15]. It employs a top-down strategy to pinpoint potential hazards and formulate safety constraints [16].

Different from traditional methods like Fault Tree Analysis (FTA) or FMEA, which primarily address component failures, STPA broadens its scope to include the entire system and its interconnected elements. The high impact factor of the journal where the integration of FRAM and STPA was detailed underscores the significance of this method. STPA is notable for identifying software-related scenarios often missed by traditional methods [17]. The STPA process includes several key steps. Initially, the purpose of the analysis must be defined. This could involve evaluating the safety of a new industrial procedure or assessing the risk associated with a specific machine operation. The next step involves creating a model of the control structure, representing the control mechanisms in place. This encompasses safety interlocks, control loops for machinery, and operational sequences designed for safety and efficiency. Subsequently, UCAs are identified, referring to actions or behaviors within the control system that could potentially lead to unsafe conditions. Finally, LS are identified, which are potential situations where losses could occur due to the UCAs. Figure 3 illustrates the key steps of the STPA methodology, starting with defining the purpose of the analysis, followed by modeling the control structure, identifying UCAs, and ultimately deriving LS. In this approach, D-HiGraph modeling is introduced as a supporting tool during the control structure modeling phase.

The integration of STPA with methodologies like Functional Resonance Analysis Method (FRAM) can improve the analysis of complex systems. FRAM is used to model how functions interact within a system, potentially leading to unexpected outcomes. Combining FRAM and STPA can lead to a more complete understanding of system safety. STPA is particularly well-suited for analyzing safety in complex automated systems, such as CCMs, due to its ability to manage the complex interactions and feedback loops inherent in these systems [18]. The method is effective in identifying potential hazards arising from both component failures and UCAs [1, 3, 7, 10, 13, 19, 20]. CCMs feature a complex control structure involving numerous sensors, actuators, and control algorithms. STPA enables analysts to model this control structure and identify potentially UCAs that could lead to accidents or quality defects. For example, STPA can analyze the control system regulating the flow of molten steel into the mold. By identifying potential UCAs, such as overfilling the mold or causing excessive turbulence, safety constraints can be designed to prevent these scenarios. STPA can be used to supplement existing risk management frameworks. An integrated safety assessment framework, such as one combining STPA, the analytic network process (ANP), and system dynamics, is essential to identifying critical risk factors and evaluating the safety level. D-Higraphs model systems through two core elements: blobs and edges [21-27]. Blobs represent hierarchical nodes containing three attributes: function (purpose, e.g., "Regulate mould temperature"), actor (physical component, e.g., Cooling Pipes 11 LEAX 111), and condition (state variable, e.g., "Pipe_Leak=TRUE"). Edges define directed relationships categorized as mass flows (molten steel → mould), energy transfers (electrical arcing → pipe damage), or information signals (sensor → PLC). Structural features include nesting (Cooling System ⊃ Pipes/Pumps/Sensors) and orthogonality (modeling alternative paths like Pneumatic OR Hydraulic backups).

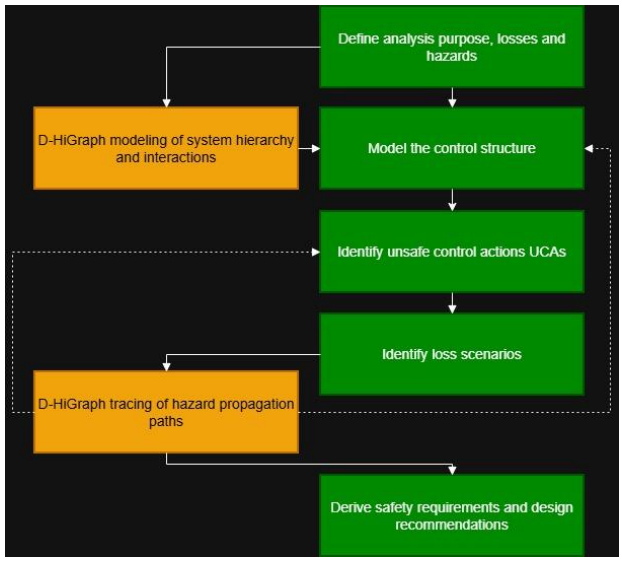

Figure 3. Integration of D-HiGraph modeling within the Systems-Theoretic Process Analysis (STPA) process

3.1 Multi-layer model construction

The CCM D-Higraph integrated three interconnected layers, illustrated by Figure 4. In the mechanical layer, Cooling System blobs specified pipe actors (11 LEAX 111) with corrosion rate conditions (0.8mm/year), connected via mass edges to slag accumulation zones. The control layer modeled PLC emergency functions with delayed response conditions (1.8 s at 150 °C), highlighting missing information edges to moisture sensors. The safety layer defined interlock functions preventing unsafe operation, with energy edges tracing wet slag → steam pressure (15 bar) → explosion pathways.

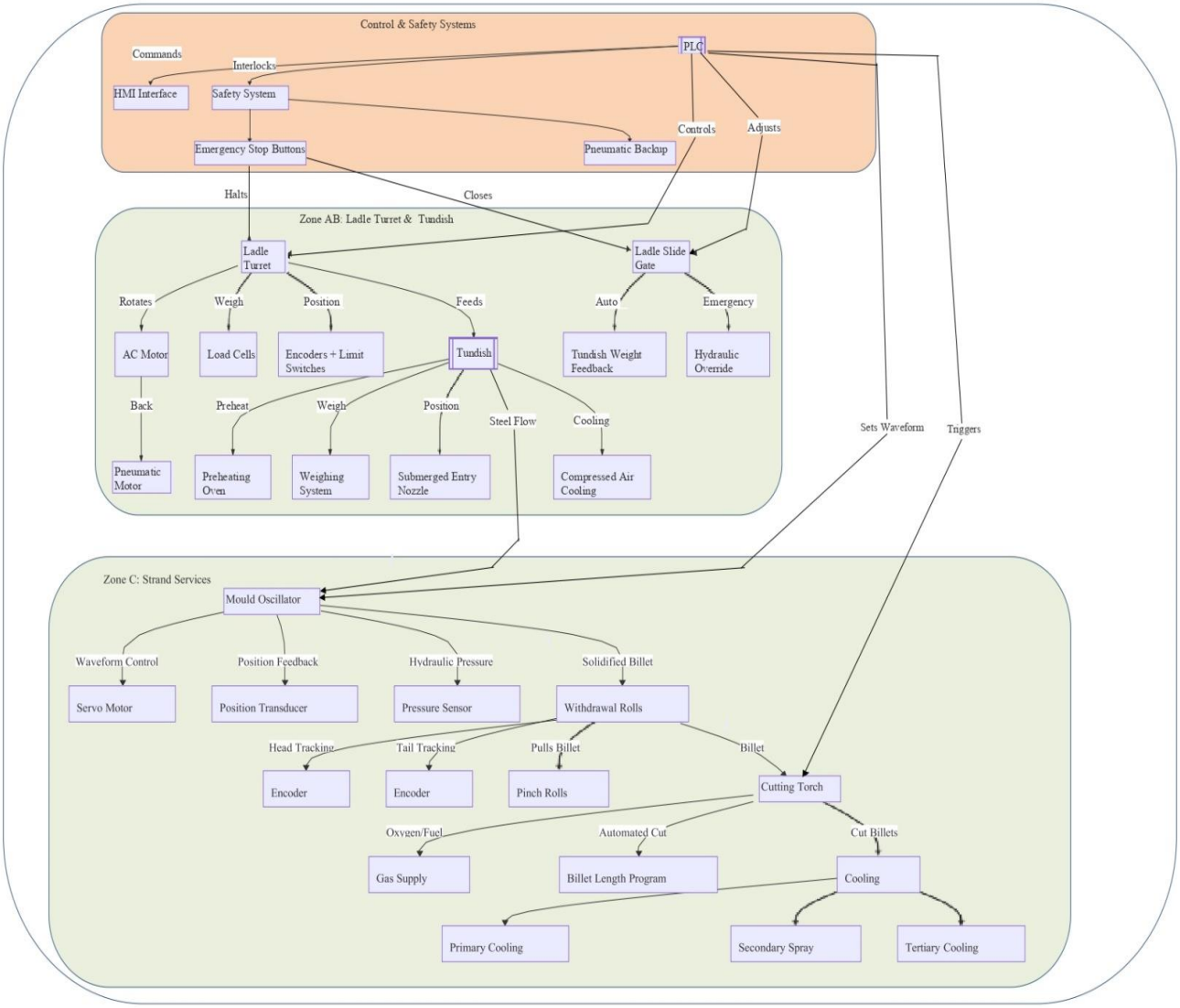

Figure 4. D-Higraph of continuous casting systems

In the intricate landscape of industrial steel production, the seamless transfer and control of molten steel demand a meticulously engineered system that integrates mechanical operations, automation, and fail-safe safety protocols. The system described here, anchored in Zone AB: Ladle Turret and Tundish, forms the backbone of a continuous casting process, where precision, reliability, and safety are paramount. This system governs the movement of molten steel from ladles to casting molds, ensuring optimal flow rates, temperature management, and operational stability in high-stakes environments. At its core, the Ladle Turret serves as a rotating mechanism that positions ladles, large containers holding molten steel, over the Tundish, a secondary reservoir designed to regulate steel flow into molds. The turret's rotation is driven by an AC Motor, with positional accuracy ensured by encoders and limit switches, which provide real-time feedback to the control systems. The Tundish, mounted on a mobile Tundish Car, collaborates with the Ladle Slide Gate to modulate steel discharge. Critical to this process is the SEN, which directs molten steel into molds while minimizing exposure to air, thereby reducing oxidation and impurities. Central to the system's intelligence is the Steel Flow Control and Safety Systems, a hierarchical network governed by programmable logic controllers (PLCs). These PLCs execute automated commands to adjust ladle positioning, gate openings, and cooling rates, while integrating real-time data from sensors such as load cells (for weight monitoring) and Tundish Weight Feedback mechanisms. The human-machine interface (HMI) acts as the operational nerve center, enabling operators to monitor variables like temperature, flow rates, and equipment status, and to intervene manually when necessary. Safety is woven into every layer of the architecture. Emergency Stop Buttons trigger instantaneous halts, closing the Ladle Slide Gate and activating backup systems like the Hydraulic Override and Pneumatic Motor, ensuring fail-safe responses during power failures or mechanical faults. Interlocks enforce conditional operations, for instance, preventing ladle rotation unless the tundish is correctly positioned to avert collisions or spills. Redundant utilities, including Compressed Air Cooling and Preheating Ovens, maintain equipment integrity under extreme thermal conditions, while Pneumatic Backup systems guarantee continuity during hydraulic or electrical disruptions. The system's adaptability is further exemplified by its Weighing and Positioning Subsystems, which combine Load Cells and motorized actuators to balance ladle weight distribution and align components with micron-level precision. This synergy between mechanical hardware and digital control logic not only optimizes production efficiency but also minimizes human error and downtime.

3.2 Subsystem analysis

The Ladle Turret subgraph modeled position control functions executed by AC motor actors, with information edges linking position data to Strand PLCs and HMI overrides. This revealed how UCA-30 (unscheduled rotation) propagated through misalignment conditions. The Emergency Closure subgraph traced energy edges from electrical arcing through pipe damage to leak risks, connecting to UCA-16 through delayed command conditions in safety PLCs. In 2025, an explosion occurred at the Electric Arc Furnace (EAF01) in a steel plant during a routine delta roof replacement operation, injuring 10 workers and causing significant equipment damage. The explosion was triggered by wet slag, a mixture of water and molten slag falling into the furnace. This reaction resulted from recurrent water leaks in the cooling system, specifically in pipes labeled \11 LEAX 111\, which allowed water to contact slag accumulating on the furnace roof. The rapid vaporization of water within the slag generated high-pressure steam, destabilizing the molten steel bath and leading to an explosive release of dust, fines, and molten material. Key causal factors included cooling system failures due to corrosion, thinning, and mechanical stress from misaligned electrodes; inadequate grounding of electrical arcs, which exacerbated pipe damage; procedural gaps in leak detection, repair, and emergency response protocols; deficiencies in personal protective equipment (PPE), including missing safety glasses and substandard helmets; and design flaws in the delta roof's inclination and welding joints, which allowed slag accumulation and hindered leak containment. Immediate actions involved evacuating personnel, securing the area, and repairing leaks, while long-term corrective measures focused on replacing the roof, enhancing grounding systems, revising welding procedures, and improving PPE protocols. The D-Higraph (hierarchical graph) of the incident maps systemic failures across safety, control, and mechanical layers, illustrating interdependencies that led to the explosion. In the safety layer, the absence of clear PPE protocols (referenced as IT LEAX 311) left workers unprotected, while interlocks designed to prevent unsafe furnace operations lacked integration with moisture sensors to detect wet slag or cooling leaks. The emergency stop mechanism, activated manually to halt the AC motor and close the ladle slide gate via hydraulic override, suffered from delayed human response. Poor electrical grounding (\11 LEAX 211\) caused arcing, further damaging cooling pipes. In the control layer, sensors such as load cells and encoders provided limited feedback: load cells failed to detect abnormal moisture levels in slag, and encoders tracked turret positioning but did not flag cooling system leaks. PLCs adjusted electrode positioning and steel flow but lacked adaptive algorithms for wet slag scenarios. The HMI displayed real-time mould level data but omitted alerts for cooling system integrity or slag accumulation, relying instead on manual operator input, which introduced delays. The mechanical layer housed critical components directly involved in the hazard. The cooling system's water-cooled pipes (\11 LEAX 111\) leaked due to age-related thinning and corrosion, worsened by electrode misalignment. Compressed air backup systems proved inadequate to counteract thermal overload during steam buildup. The AC motor and drives powered ladle turret rotation and electrode positioning but could not prevent pre-existing pipe damage. The SEN, responsible for directing steel flow into moulds, exacerbated turbulence due to wet slag obstruction. Pipes and panels, already compromised by poor grounding and mechanical stress, failed under thermal pressure. The hazard propagation pathway began with cooling leaks allowing water to contact slag, forming wet stag on the furnace roof. Thermal exposure vaporized the water, generating steam that destabilized the molten steel. Emergency stops halted operations but failed to mitigate the steam explosion, which ejected molten material, causing injuries and damage. Systemic gaps included the absence of real-time moisture or slag monitoring sensors, fragmented communication between control subsystems (e.g., PLCs, HMI, sensors), and overreliance on pneumatic backups without thermal redundancy.

The D-Higraph relationships highlight hierarchical nodes and edges. The root cause of cooling system leaks (\11 LEAX 111\) is linked to mechanical wear and grounding issues. Wet slag accumulation is connected to safety layer failures, such as inadequate interlocks and PPE. The explosion is tied to control layer delays in HMI alerts and operator response. Solid lines in the graph denote direct causation (e.g., water leaks leading to wet slag), while dashed lines indicate indirect relationships (e.g., poor grounding contributing to pipe damage). Key takeaways emphasize the relevance of STPA to identify latent risks, such as grounding flaws affecting cooling integrity, which traditional methods like HIRARC overlook. The D-Higraph's utility lies in visualizing multi-layered failures, enabling targeted improvements: preventive measures like installing moisture sensors and automating interlocks; corrective actions such as redesigning cooling pipes and enhancing grounding; and recovery protocols, including strengthened PPE enforcement and emergency response training. This analysis demonstrates how hierarchical modelling bridges theoretical hazard analysis and practical safety enhancements, critical for mitigating risks in high-risk industrial environments like steel plants. Spatial analysis through blob placement exposed cooling pipes positioned 1.2-1.8 meters from slag zones, a proximity risk undetected in STPA. Cross-layer mapping revealed how grounding flaws (safety) accelerated pipe corrosion (mechanical), causing electromagnetic interference in control sensors. Systemic gaps included absent edges between load cells and slag moisture detection, and pneumatic backup inadequacy during thermal overload at 150 °C.

3.3 Enhancing Systems-Theoretic Process Analysis with D-Higraph

The integration of STPA with D-HiGraph establishes a structured *what–how–why* analytical cascade that is firmly grounded in system theory principles. Within this framework, STPA defines *what* can go wrong by identifying UCAs, violated safety constraints, and system-level hazards arising from inadequate control. D-HiGraph complements this perspective by explaining *how* these unsafe conditions propagate through the system's hierarchical structure and *why* they persist due to interactions between physical components, control logic, and organizational factors. From a system-theoretic standpoint, STPA conceptualizes safety as an emergent property of a controlled system rather than a function of individual component reliability. D-HiGraph operationalizes this perspective by providing an explicit representation of system hierarchy, functional decomposition, and cross-layer interactions. Its modeling constructs reflect key system theory concepts, including layered control structures, feedback dependencies, and constraint enforcement

across system boundaries. This alignment allows UCAs identified by STPA to be directly mapped onto the physical and functional architecture of the CCM. In the CCM context, this synergy is particularly valuable due to the high density of interactions between subsystems such as mold level control, withdrawal and straightening units, cooling circuits, automation systems, and human operators. For example, a UCA related to mold level regulation may originate at the control layer but propagate through sensor feedback loops, actuator behavior, and physical process dynamics before resulting in a hazardous state. D-HiGraph makes these propagation paths explicit by linking control actions to structural dependencies, spatial proximity, and energy or material flows within the system. By integrating both methods, the analysis moves beyond identifying isolated unsafe actions to revealing systemic causal mechanisms. STPA ensures completeness and consistency in hazard identification, while D-HiGraph provides traceability across hierarchical levels, enabling a coherent explanation of how control deficiencies interact with physical and organizational structures. This combined approach enhances conceptual rigor by translating abstract system-theoretic principles into a concrete modeling framework, thereby supporting a deeper understanding of hazard emergence in complex, highly automated CCM operations. The D-Higraph representation of cooling system leaks and explosion pathways in steel casting operations its illustrated by Figure 5.

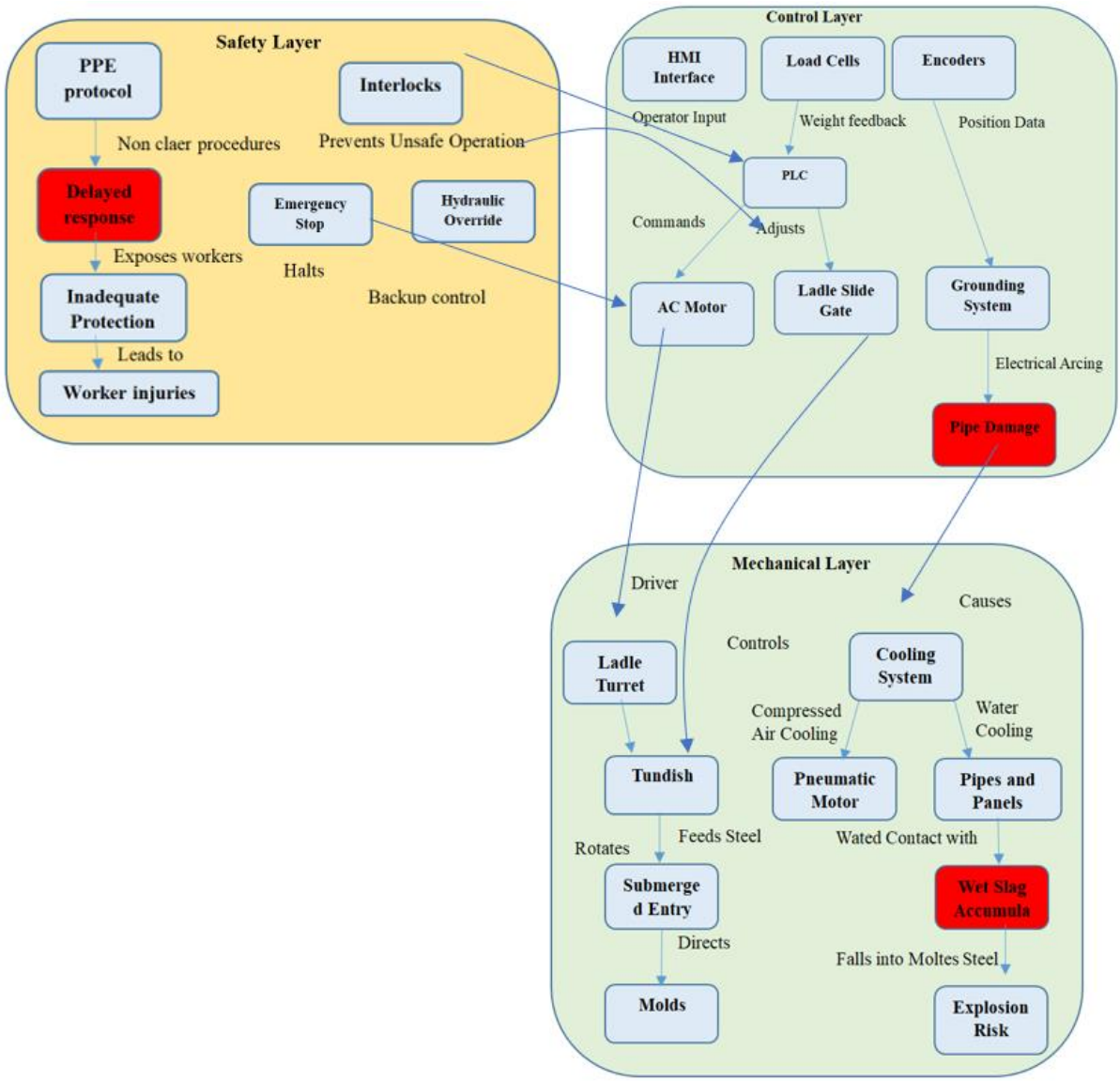

Figure 5. D-Higraph representation of cooling system leaks and explosion pathways in steel casting operations

Despite these advantages, the use of D-HiGraph also involves certain limitations that should be acknowledged. The construction of D-HiGraph models depends on expert judgment to define system boundaries, functional groupings, and interaction paths, which may introduce a degree of subjectivity. Moreover, D-HiGraph primarily emphasizes structural and hierarchical relationships and does not explicitly model performance variability or adaptive behavior over time. Alternative STPA-complementary approaches, such as FRAM, are well-suited for capturing variability-driven phenomena and emergent behaviors during normal operations. However, in the case of CCMs, where safety risks are strongly influenced by physical layout, control logic, and tightly coupled automation, D-HiGraph provides clearer structural traceability between UCAs and their propagation across system layers. For this reason, D-HiGraph was selected as a complementary modeling approach to STPA in this study.

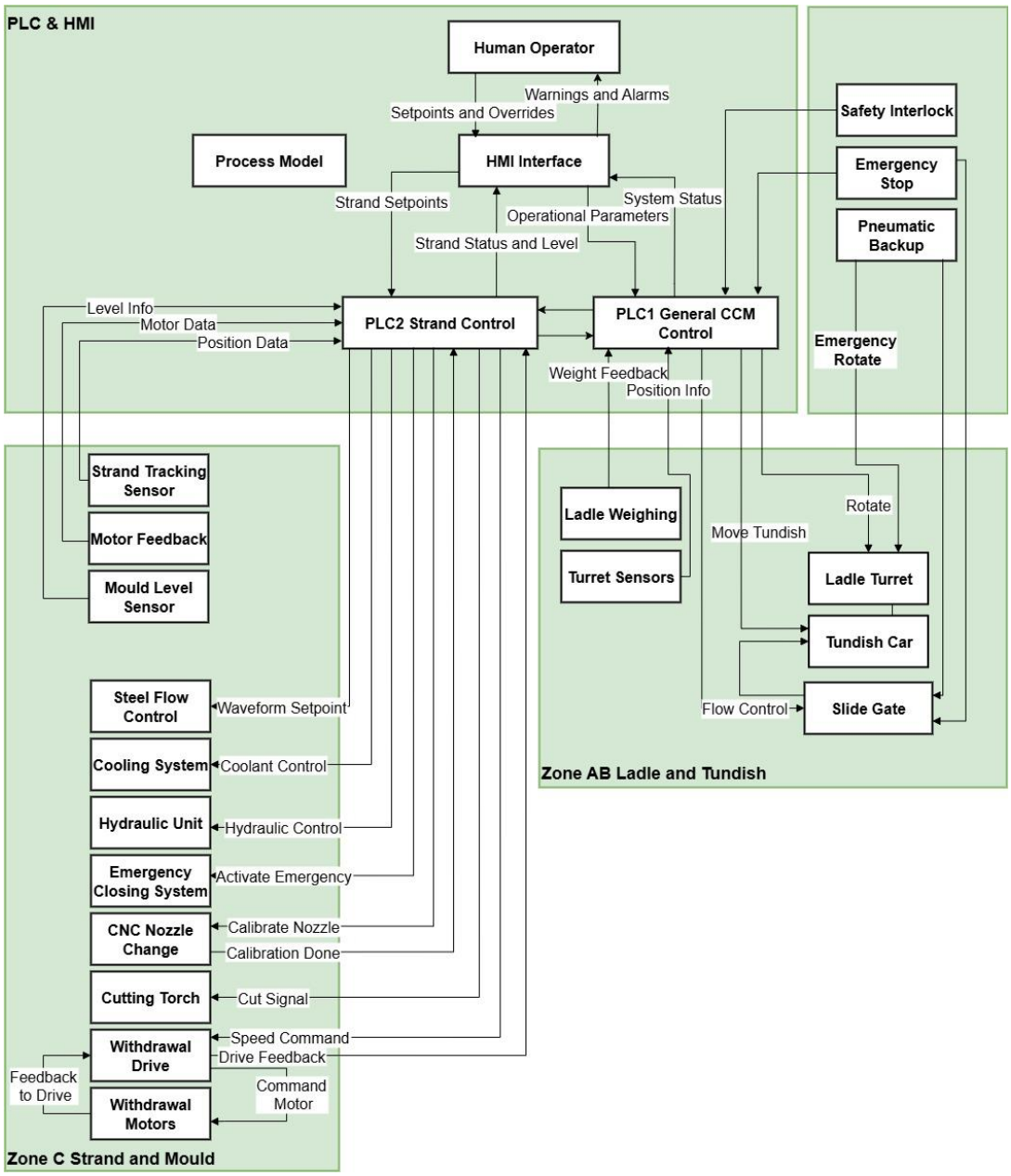

Figure 6. Control structure model of the continuous casting machine (CCM) system

3.4 Systems-Theoretic Process Analysis–D-Higraph application to continuous casting machine

- **System-Level Losses**
- L1: Injury or death of personnel due to exposure to molten steel.
- L2: Severe damage to casting equipment (ladle, tundish, mould, slide gate, withdrawal motors, etc.).
- L3: Unplanned casting interruptions and production downtime.
- L4: Quality degradation in cast steel (e.g., surface cracks, inclusions, dimensional issues).
- L5: Environmental contamination due to uncontrolled molten steel release.
- **System-Level Hazards**
- H1: Molten steel level in the mould exceeds the upper operational threshold. [L1, L2, L3, L5]
- H2: Molten steel level in the mould drops below the minimum operational threshold. [L3, L4]
- H3: Significant instability or fluctuations in the mould level. [L1, L2, L3, L4]
- H4: Uncontrolled molten steel flow from ladle or tundish. [L1, L2, L3, L5]
- H5: Emergency closure mechanism fails to activate when required. [L1, L2]
- H6: Mould level or ladle weighing sensors provide missing or inaccurate feedback. [L3, L4]
- H7: Casting starts or continues despite unmet process conditions (e.g., low ladle level, cold steel, misaligned shroud). [L1, L2, L3]
- H8: Human operator performs a critical task without appropriate safety equipment or safeguards. [L1]
- **System-Level Safety Constraints**
- SC1: The molten steel level in the mould shall not exceed the upper safety threshold at any time. [H1]
- SC2: The molten steel level in the mould shall be maintained above the lower safety threshold. [H2]
- SC3: The mould level control system shall ensure timely and stable responses to maintain a consistent level. [H3]

- SC4: The flow of molten steel from ladle to tundish and mould shall be precisely regulated under all conditions. [H4]
- SC5: The emergency closing mechanism shall always activate under defined unsafe conditions. [H5]
- SC6: All level and weighing sensors shall provide accurate, continuous, and reliable feedback. [H6]
- SC7: Casting shall not proceed unless all safety and process readiness conditions are met. [H7]
- SC8: Operators shall always wear PPE and follow safety protocols during casting operations. [H8]

3.5 Model the control structure

The control structure of the CCM system is illustrated in Figure 6. It represents the interaction between human operators, PLCs, safety systems, sensors, and actuators to manage both the general casting process and strand-specific operations. The system is divided into two main layers of control: a general PLC responsible for ladle positioning, slide gate regulation, and tundish handling, and a dedicated strand PLC that governs mould level control, withdrawal speed, cutting, and emergency actions. Human operators interact with the system through an HMI, providing setpoints and overrides while receiving feedback, alarms, and process data in real time. Each component from mould level sensors to CNC nozzle changers and emergency closing mechanisms operates within a structured feedback loop, ensuring stable and responsive control of molten steel flow, strand withdrawal, and billet formation. This model provides the foundation for identifying UCAs and understanding how control failures could lead to hazardous system states in the context of STPA.

We used the control architecture developed in Figure 6 to identify UCA. The different UCAs find its illustrated in Table 1.

Table 1. Unsafe control actions (UCAs) for the continuous casting machine (CCM)

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too Early / Too Late / Out of Order	Stopped Too Soon / Applied Too Long
Adjust Mould Level	**UCA-1**: PLC-2 does not send a command to adjust mould level when deviation occurs, resulting in overflow or underfill [H-1, H-2, H-3, H-5]	**UCA-2**: PLC-2 sends mould level adjustment when level is already stable, creating unnecessary disturbances [H-2, H-3, H-5]	**UCA-3**: Adjustment is delayed or issued too early, causing overreaction or prolonged instability [H-1, H-3, H-5]	N/A
Increase Withdrawal Speed	**UCA-4**: No speed increase command when mould level is too high, causing overflow [H-1, H-2]	**UCA-5**: Speed increase is given when mould level is already low or optimal, risking underfill [H-2, H-3]	**UCA-6**: Speed command issued too late to prevent overflow [H-1, H-3]	N/A
Decrease Withdrawal Speed	**UCA-7**: No command to reduce withdrawal speed when the level is falling, leading to underfill [H-2, H-5]	**UCA-8**: Speed is decreased when the level is already high or stable, leading to overflow [H-1, H-3, H-5]	**UCA-9**: Delay in decreasing speed causes the level to drop excessively [H-2, H-3]	N/A

Table 2. Mapping of loss scenarios (LS) to safety requirements for the continuous casting machine (CCM)

LS	Safety Requirements
LS (1, 4, 5, 6, 11, 14, 17, 18, 23, 24)	- Use faster and more responsive sensors (especially mould level and turret position). - Ensure periodic calibration of level sensors and turret encoders.
LS (2, 9, 12, 15, 20, 22, 25, 35, 37)	- Optimize control logic and software filtering routines to reduce processing delay. - Upgrade PLC processing performance where needed.
LS (3, 7, 13, 19, 32, 33, 38)	- Reduce communication latency using higher-performance protocols. - Separate critical and non-critical communication channels.
LS (8, 10, 16, 27, 36)	- Improve grounding and shielding to protect against EMI. - Validate sensor reliability using redundant checks.
LS (21, 23, 26, 29, 30, 31, 34, 39, 41)	- Provide regular training for operators on setpoints, overrides, and turret operation. - Develop clear, step-by-step procedures and guidance on HMI.

Identify LS:

- **Control Action: Adjust Mould Level**

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

UCA-2: The controller provides “adjust mould level” command when the level is already optimal [H-2, H-3, H-5].

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

- **Control Action: Increase Withdrawal Speed**

UCA-4: The controller does not provide “increase speed” when the level is high [H-2].

UCA-5: The controller increases speed when the level is already low [H-1, H-3].

UCA-6: Speed increase happens too late [H-2, H-3].

- **Control Action: Decrease Withdrawal Speed**

UCA-7: No decrease when the level is falling [H-2, H-5].

UCA-8: Speed is decreased unnecessarily [H-1, H-3, H-5].

UCA-9: Decrease comes too late [H-1, H-2].

- **Control Action: Setpoints and Overrides from Operator to HMI**

UCA-10: Operator does not set the correct level target [H-1, H-2].

UCA-11: Operator sets unnecessary level override [H-2, H-3].

UCA-12: Operator updates setpoint too late [H-1, H-2].

UCA-13: Override kept active too long [H-2, H-3].

- **Control Action: Emergency Closing System**

UCA-14: Emergency close not activated during critical event [H-1, H-5].

UCA-15: Emergency close triggered without need [H-2, H-5].

UCA-16: Emergency close delayed [H-2, H-3].

- **Control Action: Turret Rotation**

UCA-29: Turret does not rotate to casting position on time [H-5].

UCA-30: Turret rotates unexpectedly [H-1, H-4].

UCA-31: Turret rotates too early or too late [H-1, H-4, H-5].

UCA-32: Rotation holds too long [H-5].

Different safety requirements obtained with the STPA method for the CCM are illustrated in Table 2.

4. RESULTS AND DISCUSSION

The integrated application of STPA and D-HiGraph to the CCM yielded a comprehensive understanding of potential hazards and the systemic mechanisms from which unsafe conditions can arise. The STPA phase systematically identified 32 UCAs distributed across nine core control functions. These UCAs encompassed critical operations: mold level regulation (UCAs 1–3), withdrawal speed control (UCAs 4–9), emergency closing functions (UCAs 14–16), cooling system management (UCAs 23–25), and turret rotation control (UCAs 29–32). Mold level control was highlighted as particularly critical, as even minor deviations could rapidly escalate into mold overflow, strand breakouts, or severe product quality issues if not promptly corrected. Similarly, failures or delays in the emergency closing system were assessed as posing severe risks to personnel and equipment.

The analysis was extended through loss scenario identification, which detailed 41 distinct contexts in which the UCAs could materialize. These scenarios stemmed from diverse causal factors, including delayed or inaccurate sensor feedback, misinterpretations of PLC logic, communication latency between system components, and deficiencies in HMI design. For example, one scenario linked delayed mold level correction to slow sensor response, while another associated overflow prevention failure with communication delays between the HMI and PLC. Notably, many scenarios intertwined technical and human factors, underscoring the socio-technical nature of CCM safety risks and emphasizing the necessity of a system-level analytical approach.

The subsequent D-HiGraph modeling phase enriched the analysis by providing a multi-layered visualization of hazard propagation pathways within the CCM. Moving beyond STPA's primarily tabular format, D-HiGraph explicitly mapped interactions across the control, safety, and mechanical layers. This revealed, for instance, how inadequate electrical grounding in the safety layer could accelerate corrosion in cooling pipes at the mechanical layer, which in turn induced electromagnetic interference affecting mold level sensors in the control layer. Such visualizations clarify how localized deficiencies could propagate systemically to generate UCAs.

Furthermore, D-HiGraph introduced a vital spatial dimension to the hazard analysis. It highlighted, for example, the physical proximity between cooling pipes and slag accumulation zones. This proximity, combined with an absence of moisture detection, significantly elevated the risk of hazardous water-slag interactions—a risk difficult to capture through control-focused analysis alone.

Independently, each method offered valuable but incomplete insights. STPA proved highly effective in systematically identifying system-level losses, hazards, safety constraints, and UCAs, clarifying what could go wrong and under which control conditions. However, STPA does not natively represent the physical structure of the CCM or the hierarchical and spatial relationships through which unsafe actions propagate. Conversely, D-HiGraph provided a detailed representation of the CCM's functional and physical architecture, illuminating interdependencies between subsystems. Yet, in isolation, it lacks a systematic mechanism for determining the specific conditions under which control actions become unsafe or for directly linking structural interactions to predefined system-level losses.

Beyond mere hazard identification, the results facilitate a conceptual classification of hazard types aligned with each method's analytical strengths. STPA primarily reveals control-related hazards, such as unsafe or missing control actions, incorrect timing, and violations of safety constraints within automation logic and human interaction. D-HiGraph excels at uncovering structural and interaction-driven hazards, including those arising from physical proximity, shared resources, cross-layer dependencies, and energy or material propagation paths. Their integration enables the identification of emergent systemic hazards that result from the interaction between inadequate control actions and the underlying physical and organizational structure.

By explicitly linking UCAs to their structural, functional, and spatial propagation pathways, the integrated STPA–D-HiGraph approach offers a generalizable framework for safety analysis in complex, automated systems. However, the insights from this case study must be viewed in light of its limitations. The analysis represents a single, in-depth application, and the generalizability of the specific findings to other CCM designs or different process industries requires validation through broader cross-application studies. Additionally, the construction of the D-HiGraph model involves expert judgment, introducing subjectivity in defining system boundaries and interactions. Most significantly, the derived safety requirements and potential performance benefits are, at this stage, well-founded hypotheses. Their practical efficacy in preventing incidents or improving operational resilience remains unproven without empirical validation.

Consequently, future work should focus on three key areas: applying the integrated methodology to diverse industrial systems to refine its general principles; developing more formalized modeling guidelines to reduce subjectivity; and implementing and longitudinally monitoring the proposed safety measures in an operational environment to quantitatively assess their real-world impact. This pathway from analytical derivation to empirical validation is essential for translating the methodological contribution of this work into tangible safety improvements.

5. CONCLUSIONS

This study shows how combining STPA with D-Higraph modeling can give us a much clearer picture of safety risks in CCMs. On its own, STPA is excellent for systematically identifying what can go wrong, highlighting UCAs and defining the safety rules needed to prevent them. D-Higraph, meanwhile, excels at showing how and why hazards spread by mapping out the physical layout, control systems, and safety layers of the CCM. By bringing these two methods together, we can trace a problem from its root cause through the entire system, leading to safety recommendations that are both precise and deeply informed by how the plant actually works. Our findings reinforce a key idea: in complex, automated

systems like a CCM, safety isn't just about individual parts or software commands. Real safety comes from understanding how everything: equipment, controls, and people, interacts. The STPA–D-Higraph framework provides a structured way to capture these interactions. Looking ahead, the practical value of this integrated approach lies in its potential. For engineers and plant safety managers, it offers a way to spot hidden risks, prioritize upgrades, and design more resilient systems from the start. Used during both the planning and operational phases, it could lead to fewer unplanned shutdowns, better prevention of accidents, and stronger protection for both personnel and equipment. Of course, these are potential benefits, not guaranteed outcomes. This research is based on a detailed analysis of a specific system, and applying the method relies on expert judgment. The safety improvements we suggest are, at this stage, well-founded hypotheses. The essential next step is to test them in the real world. Future work must focus on implementing the proposed safety measures in actual CCM operations and rigorously tracking their performance. This validation is crucial to confirm the framework's effectiveness and to adapt it for use in other complex industrial settings.

ACKNOWLEDGEMENTS

The researchers wish to extend their sincere gratitude to the Deanship of Scientific Research at the Islamic University of Madinah (KSA) for the support provided to the Post-Publishing Program.

REFERENCES

[1] Larit, K., Zennir, Y., Rodriguez, M. (2025). Hazard analysis with STPA methods: Application to mould level control within continuous casting free stream operations. International Journal of Safety & Security Engineering, 15(4): 835-846. https://doi.org/10.18280/ijsse.150419

[2] Cai, M., Shi, Y., Liu, J., Niyoyita, J.P., Jahanshahi, H., Aly, A.A. (2023). DRKPCA-VBGMM: Fault monitoring via dynamically-recursive kernel principal component analysis with variational Bayesian Gaussian mixture model. Journal of Intelligent Manufacturing, 34(6): 2625-2653. https://doi.org/10.1007/s10845-022-01937-w

[3] Kong, Y., Chen, D., Liu, Q., Long, M. (2019). A prediction model for internal cracks during slab continuous casting. Metals, 9(5): 587. https://doi.org/10.3390/met9050587

[4] Benhamlaoui, W., Rouainia, M., Liu, Y., Medjram, M.S. (2020). Comparative study of STPA and Bowtie methods: Case of hazard identification for pipeline transportation. Journal of Failure Analysis and Prevention, 20(6): 2003-2016. https://doi.org/10.1007/s11668-020-01010-9

[5] Larit, K., Zennir, Y., Rodriguezh, M. (2024). Implementing FMEA for multi-stage centrifugal compressor in ASU "AQS". International Journal of Automation and Safety, 2(1): 24-32. https://asjp.cerist.dz/en/article/249641.

[6] Bouasla, S.E.I., Zennir, Y., EL-Arkam, M. (2022). Functional modeling using D-higraph for process hazard analysis. Algerian Journal of Signals and Systems, 7(2): 71-76. https://doi.org/10.51485/ajss.v7i2.161

[7] Dunsford, R., Chatzimichailidou, M. (2020). Introducing a system theoretic framework for safety in the rail sector: Supplementing CSM-RA with STPA. Safety and Reliability, 39(1): 59-82. https://doi.org/10.1080/09617353.2019.1709289

[8] Wu, X., Jiang, W., Yuan, S., Kang, H., Gao, Q., Mi, J. (2023). Automatic casting control method of continuous casting based on improved soft actor–critic algorithm. Metals, 13(4): 820. https://doi.org/10.3390/met13040820

[9] Diniz, A.P.M., Ciarelli, P.M., Salles, E.O.T., Coco, K.F. (2024). Use of deep neural networks for clogging detection in the submerged entry nozzle of the continuous casting. Expert Systems with Applications, 238: 121963. https://doi.org/10.1016/j.eswa.2023.121963

[10] Yu, Y., Luo, X., Liu, Q. (2018). Model predictive control of a dynamic nonlinear PDE system with application to continuous casting. Journal of Process Control, 65: 41-55. https://doi.org/10.1016/j.jprocont.2017.10.008

[11] Lei, Z., Su, W. (2019). Research and application of a rolling gap prediction model in continuous casting. Metals, 9(3): 380. https://doi.org/10.3390/met9030380

[12] Mehta, M., Singh, M., Francis, V., Singh, J., Taufik, M. (2024). Mathematical modelling, performance analysis and optimization for the availability of casting system using Markov integrated genetic algorithm approach. International Journal on Interactive Design and Manufacturing (IJIDeM), 18(7): 5139-5149. https://doi.org/10.1007/s12008-023-01572-6

[13] Makarov, A.V., Kudryashov, A.E., Nevezhin, S.V., Gerasimov, A.S., Vladimirov, A.A. (2020). Reconditioning of continuous casting machine rollers by laser cladding. Journal of Physics: Conference Series, 1679(4): 042047. https://doi.org/10.1088/1742-6596/1679/4/042047

[14] Wang, B., Wang, Y., Xu, F., Shi, Z. (2024). Intelligence-led accident prevention and its application in petrochemical enterprises. Process Safety and Environmental Protection, 184: 690-702. https://doi.org/10.1016/j.psep.2024.02.022

[15] Naeini, A.M., Nadeau, S. (2023). Proposed integrated FRAM/STPA risk analysis of data gloves in assembly 4.0 system. Robotics and Computer-Integrated Manufacturing, 81: 102523. https://doi.org/10.1016/j.rcim.2022.102523

[16] de Farias, J.C.L.A., Carniel, A., de Melo Bezerra, J., Hirata, C.M. (2024). Approach based on STPA extended with STRIDE and LINDDUN, and blockchain to develop a mission-critical e-voting system. Journal of Information Security and Applications, 81: 103715. https://doi.org/10.1016/j.jisa.2024.103715

[17] Rising, J.M., Leveson, N.G. (2018). Systems-theoretic process analysis of space launch vehicles. Journal of Space Safety Engineering, 5(3-4): 153-183. https://doi.org/10.1016/j.jsse.2018.06.004

[18] Jiao, J., Jing, Y., Pang, S. (2022). An integrated quantitative safety assessment framework based on the STPA and system dynamics. Systems, 10(5): 137. https://doi.org/10.3390/systems10050137

[19] Rehail, Y., Zennir, Y., Tchouar, N. (2024). Application of STPA for comprehensive risk analysis of naphtha explosion hazards: Case study: Column C-63 at Skikda-

RA1K refinery. Algerian Journal of Signals and Systems, 9(3): 153-161. https://doi.org/10.51485/ajss.v9i3.225

[20] Kontoravdi, C., Pistikopoulos, E.N., Mantalaris, A. (2010). Systematic development of predictive mathematical models for animal cell cultures. Computers & Chemical Engineering, 34(8): 1192-1198. https://doi.org/10.1016/j.compchemeng.2010.03.012

[21] Mechhoud, E.A., Rouaïnia, M., Rodriguez, M. (2016). Functional modeling of a HDPE reactor using dhigraphs for process hazard analysis. In 2016 8th International Conference on Modelling, Identification and Control (ICMIC), Algiers, Algeria, pp. 736-741. https://doi.org/10.1109/ICMIC.2016.7804247

[22] Mechhoud, E.A., Rodriguez, M., Zennir, Y. (2017). Automated depandability analysis of the HDPE Reactor using D-higraphs HAZOP assistant. Algerian Journal of Signals and Systems, 2(4): 255-265. https://doi.org/10.51485/ajss.v2i4.51

[23] Rodríguez, M., de la Mata, J.L. (2012). Automating HAZOP studies using D-higraphs. Computers & Chemical Engineering, 45: 102-113. https://doi.org/10.1016/j.compchemeng.2012.06.007

[24] Chen, X., Jiao, J., Rodriguez, M. (2017). The failure propagation analysis of flight control system based on D-higraph. In 2017 Second International Conference on Reliability Systems Engineering (ICRSE), Beijing, China, pp. 1-6. https://doi.org/10.1109/ICRSE.2017.8030749

[25] Bouasla, S.E.I., Zennir, Y., Mechhoud, E.A., Rodriguez, M. (2025). Risk assessment using a structured combined method. International Journal of Safety and Security Engineering, 15(2): 383-396. https://doi.org/10.18280/ijsse.150219

[26] Mechhoud, E.A., Bendib, R., Kared, S. (2024). Risk assessment of distillation column C5 at Skikda refinery using functional modeling (D-Higraph). International Journal of Automation and Safety, 2(2): 30-37. https://asjp.cerist.dz/en/article/260887.

[27] Hassaballa, A.E. (2024). Influence of red bricks infill walls on seismic response of a regular RC framed building by (SBC-CR-18) code. The Islamic University Journal of Applied Sciences (JESC), 2024(12): 194-225. https://doi.org/10.63070/jesc.2024.021