System Theoretic Model Checking for Safety Management in Industrial Plants

Nakhal Akel A.J. [a], Simone F.[a], Stefana E.[a], Di Gravio G.[a], Patriarca R.[a]

[a]*Department of Mechanical and Aerospace Engineering, Sapienza University of Rome Via Eudossiana, 18, 00184 - Rome - Italy (antonio.nakhal@uniroma1.it)*

Abstract: In recent years, the complexity of systems has increased significantly, leading to an increase in the potential for accidents or incidents in industrial plants. Therefore, such advancements and causes of accidents are frequently beyond the detection capabilities of standard safety assessment models. Traditional models define safety as managing failures and taking only direct causality into account, whereas System-Theoretic Accident Modelling and Process (STAMP) considers the causality of the accidents. STAMP is based on systems theory, in that, a STAMP system is a control system, and that control system enforces safety constraints. However, applying STAMP alone may not guarantee the correctness of the system's behavior. In this paper, the research proposes the STAMP model and Model Checking for the safety analysis of a complex socio-technical industrial system. The STAMP model identifies potential hazards and analyzes their causes and consequences. Then model checking technique is applied to verify the correctness of the system's behavior under different scenarios. In particular, the model checker technique has been used to evaluate the system's behavior against specifications, ensuring no unsafe or inappropriate behaviors. Integrating both methodologies ensure the identification of safety violations by the system giving room for improvement in system design to handle hazards and satisfy all the safety constraints identified by STAMP. On this premise, the manuscript has been grounded in the Oil & Gas sector, specifically in the Natural Gas Storage process. This approach provides a systematic way to identify hazards and verify the system's behavior's correctness, ultimately improving the system's safety.

Keywords: System Thinking; Socio-Technical System; Model Checker; Safety Control Structure; Finite State Model.

I. INTRODUCTION

The systems in industrial plants are becoming increasingly complex: different factors act on the variability of their normal operations and nonlinear behaviors and interactions among the components (Nakhal Akel et al., 2022). The current systems are much more than the equipment they contain: they are socio-technical systems where people, equipment, and technology interact within a physical, social, managerial, organizational, regulatory, and societal environment (Baybutt, 2021).

In such a context, it is necessary to move toward systems theory and models that capture hazardous scenarios that cannot be identified by traditional hazard analysis and safety assessment techniques (Dakwat and Villani, 2018; Tsuji et al., 2020). Systems theory focuses on system operations and management processes related to the system under investigation (Leveson, 2012). Systems Theoretic Accident Modelling and Processes (STAMP) is an accident causality model based on system theory, which considers safety as a continuous control task managed by a control structure embedded in an adaptive socio-technical system (Leveson, 2004). In STAMP, systems are interrelated components that are kept in a state of dynamic equilibrium by feedback loops of information and control (Leveson, 2004).

However, STAMP and its associated techniques (i.e., System-Theoretic Process Analysis (STPA) and Causal Analysis based on System Theory (CAST)) suffer from some limitations that make their validity a debatable issue: (i) they lack formalism, (ii) they depend on available information, and those who perform it, (iii) they are time-consuming, and (iv) they tend to rely on abstraction for managing the complexity of a system (Dakwat and Villani, 2018; de Souza et al., 2020; Sadeghi and Goerlandt, 2023). Tsuji et al. (2020) emphasize that generally, the number of scenarios obtained by STAMP and its accompanied methods can be huge, and the validation testing involves a considerable cost. Furthermore, Ye et al. (2020) argue that the STAMP application relies on manual analyses and, thus, on the subjective judgments of analysts.

To overcome these drawbacks, the adoption of formal verification and methods can provide valuable support. Indeed, formal verification is a robust approach that can rigorously verify whether a specification can be satisfied by a model or not (Han et al., 2019) and, differently from simulation and testing approaches, it permits conducting an exhaustive exploration of all possible behaviors of the system (Clarke et al., 2018; Simone et al., 2023). Formal methods could add confidence in using the system by revealing errors during development in the systems' modeling and implementation (Eleftherakis and Kefalas, 2001). Model checking represents one well-known example among the various formal verification methods (Han et al., 2019). This determines whether a given property is valid in any, some, or all states of the model (Eleftherakis and Kefalas, 2001). In other words, model checking permits examining if the model of a system (specified in some modeling formalism) meets its requirements (Razzaq and Ahmad, 2015). It is fully automatic and produces a counterexample demonstrating

a behavior that falsifies the property when the design fails to save a desired property (Clarke et al., 2018).
Consequently, integrating STAMP (or its nested techniques STPA or CAST) and model checking may obtain more effective accident analysis, give a formal and unambiguous representation of the investigated system and the threats identified by systems theory methods, and improve the knowledge about the system (Dakwat and Villani, 2018; Yang et al., 2019). In the literature, different contributions investigate the topic by implementing a broad spectrum of approaches (e.g., Abdulkhaleq and Wagner (2015), Ando et al. (2018), Chen et al. (2017), Dakwat and Villani (2018), de Souza et al. (2020), Okano et al. (2020), Tsuji et al. (2020), Wang and Wagner (2016), Xu and Lin (2023), Yang and Tian (2015), Yang et al. (2019), Ye et al. (2020), Zhang and Liu (2019), Zhong et al. (2022)). Still, none are focused on industrial plants' domain and peculiarities. To fill this gap, this paper proposes an approach combining STAMP and model checking for the safety analysis of a complex socio-technical industrial system.
The remainder of this paper is organized as follows. **Section II** summarizes the main STAMP and model checking elements and presents the proposed approach. **Section III** describes its application to a case study about the transformation of natural gas processing and storage plant to a hydrogen (H2) processing and storage plant. Concluding remarks and future research directions are provided in **Section IV**.

II. METHODOLOGY

The following section contains the methodological fundamentals to drive the proposed system theoretic model checking analysis. Moreover, we define a step-by-step procedure that integrates system theoretic principles and the model checking technique. The process is generalized to ensure its application in different domains and cases.

A. System-Theoretic Accident Model and Processes

STAMP is an accident causality model based on systems theory that can be used as a baseline to analyze and prevent accidents in complex socio-technical systems. The rationale behind STAMP denotes accidents to result from the interactions within the system, rather than the failure of individual components. On this basis, STAMP seeks to identify and mitigate the system hazards by focusing on the relationships and dependencies between system components. Accordingly, the underlying element of a STAMP model is the Safety Control Structure (SCS), i.e., a schematic representation mapping all the interactions between the various system components. At a first stage, to apply STAMP, there is the need to identify all the system hazards and, consequently, the safety constraints resulting from them. Once safety constraints have been derived, it is then possible to construct the hierarchical SCS imposing safety constraints on the system, thus guaranteeing system safety. To build the SCS, the first step is to select all variables that need to be detected by sensors. These measured variables are then transmitted to the controller as feedback. The controller then analyzes the feedback to generate the controlled variables. These latter are then sent to the actuators, which drive them in the controlled process as control actions. The inputs and outputs of the controller and controlled process are indicated by a rightward and leftward arrow, respectively. Between the different hierarchical levels of the SCS, a downward reference channel provides the necessary information to impose safety constraints on the level below. Similarly, an upward measuring channel provides feedback about the effectiveness of the constraints being fulfilled.

B. Model checking analysis

Model checking is an automated technique employed to verify whether a system model meets the prescribed safety constraints. The first step in model checking involves developing a Finite State Model (FSM) for the system. The FSM represents the system's dynamic behavior through the use of states and state transitions. Each state denotes a unique behavior of the system, and inputs trigger transitions between states. To construct the FSM at first, there is the need to identify all possible states and their transitions to specify the expected dynamic behaviors of the system and the triggers that induce changes in dynamic behavior. Once all states and triggers have been identified, the FSM construction starts with the initial state (which represents the first dynamic behavior exhibited by the system after it starts), describing how the system responds to all inputs in that state, and moving onto the next state until returning to the initial state. During normal operation, the FSM must be updated with hazardous inputs and design modifications that can manage those hazardous inputs. The model's functionality is verified by providing proper inputs and checking how the system is tackling the hazardous ones.

C. Integration of STAMP model and model checking technique

The STAMP model and the model checking technique are combined based upon the notions from **Section II.A** and **Section II.B**. Specifically, the SCS is used as a baseline to develop the FSM, and the safety constraints serve as drivers to generate hazardous inputs. Accordingly, the following steps are defined for the integration:

- Step 1. *Identification of system hazards*. This step involves the identification of all possible hazards that the system may encounter, including internal and external factors. This step also includes analyzing the system in relation to its environment to identify potential sources of risk and other factors that may impact the system safety.
- Step 2. *Definition of safety constraints*. Safety constraints define the safe boundaries within which the system must operate to prevent or mitigate hazardous events. This step involves identifying the system's safety requirements and

developing specific constraints to guarantee those requirements.

- Step 3. *Design of the SCS*. The current SCS of the system must be derived following the hierarchical relationships between system agents, such that each layer can impose the desired safety constraints on the layer below it.
- Step 4. *Design of the FSM*. The FSM is built from the SCS of the STAMP model. On this basis, feedbacks in the SCS becomes inputs of the FSM. This happens as long changes in input causes a change in the FSM state and, similarly, a change in feedbacks causes a change in control actions. On the other hand, a parallelism between control actions and outputs exists. This happens since control actions in the SCS prescribe which action should be performed next, and, similarly, the FSM output decides which action must be taken next. Accordingly, control actions in the SCS can be seen as outputs for the FSM. This connections permit to derive the states of the FSM starting from the system behavior depicted in the STAMP model. Subsequently the FSM should be developed in a model checking software which enables the model verification. UPPAAL has been used in this work for this purpose.
- Step 5. *Verification of the FSM*. Safety constraints that have been derived in Step 2 are used to run simulation and verify whether the FSM (developed based upon the SCS) is able to meet them or not. Please note that safety constraints will be in verbal form, to use them in model checking software there is the need to derive equivalent logical expressions.
- Step 6. *Update of the SCS*. The SCS must be designed to ensure that the system remains within the defined safety constraints, even in the event of unexpected disturbances. Accordingly, if from Step 5 some safety constraints result to be unmet, there is the need to update the SCS and, consequently, the system process design.

Figure 1 shows a schematization of the proposed methodology. The identified steps can be applied only after the selection of a proper system to be analyzed.

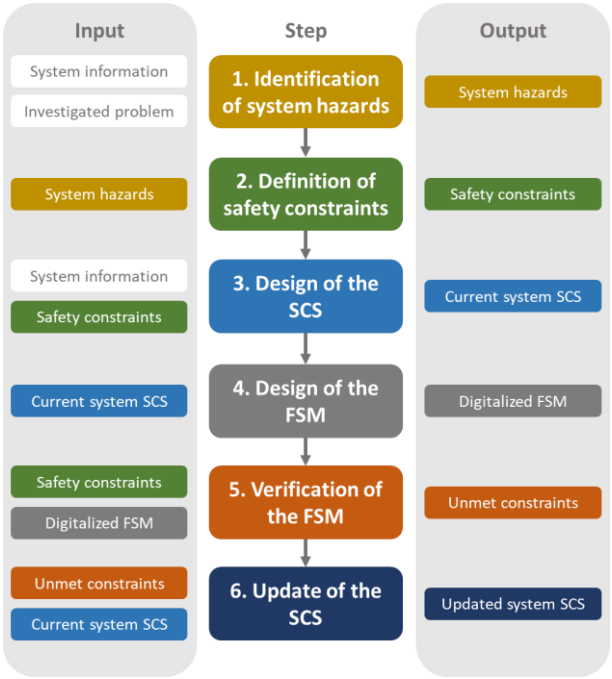

Fig. 1 Schematization of the proposed methodology to integrate STAMP and model checking. The color code relates input/output blocks with the corresponding methodology step. White blocks enter as pre-required input to apply the methodology.

III. Results and Discussion

This section demonstrates the applicability of the proposed methodology through a case study in the Oil & Gas industry, specifically in a natural gas storage plant. The industrial processes involved converting raw wellhead gas into clean sales gas for sustainable power generation, which can be delivered to customers with minimal environmental impact. The process can be resumed as follow (Mokhatab et al., 2014): the natural gas is received at shallow temperatures to be transferred to the storage tanks (element (1), cf. **Figure 2**). Later, the gas passes through the pipelines that join the arms to the tanks, and it is stored inside the tanks at a low temperature, i.e., between 105 K and 115 K (element (3), cf. **Figure 2**). Subsequently, the compressor (element (2), cf. **Figure 2**) and the recondensing system (element (4), cf. **Figure 2**) collect the gas and convert it into a liquid state to be transferred into the pumping system. The pumping stage (element (5), cf. **Figure 2**) is used to transport the liquid natural gas from the storage tanks to the vaporizer (element (6), cf. **Figure 2**). Then the heat exchangers convert the liquid into gas to be pressurized (between 7 MPa – 10 MPa) and delivered into the supply pipeline (element (7), cf. **Figure 2**).

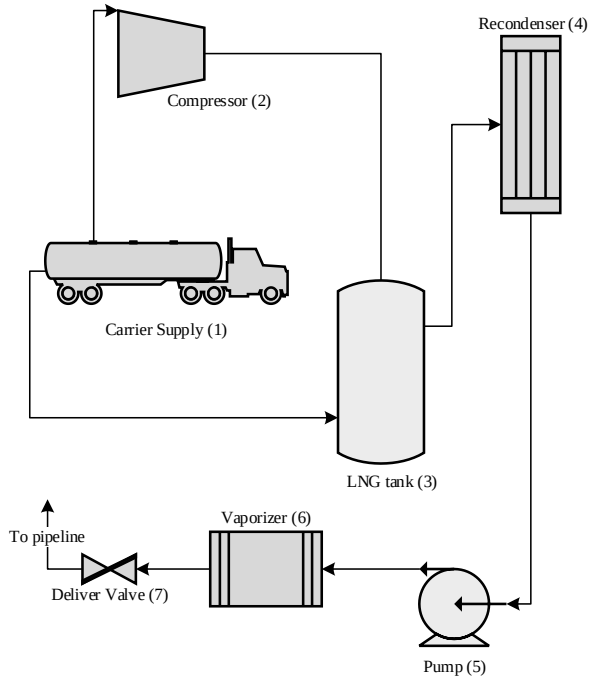

Fig. 2 Natural gas storage plant process diagram.

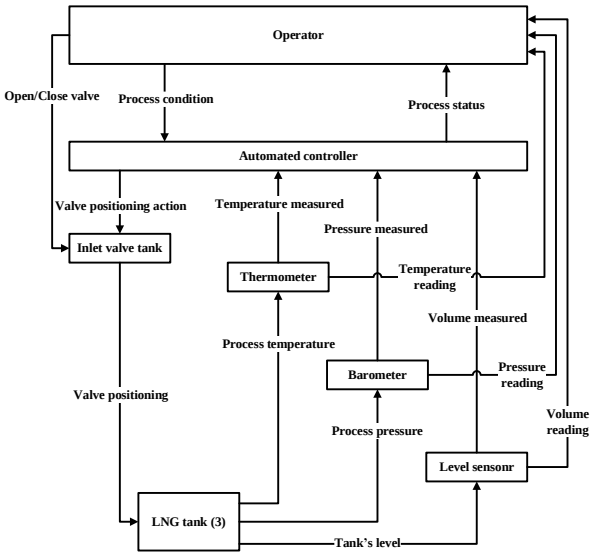

Fig. 3 Safety Control Structure of LNG tank.

For demonstration purposes, the presented case of study has been focused on the LNG tank (element (3), cf. **Figure 2**). **Figure 3** shows the detailed SCS of the storage tank and its components. Hence, it is possible to highlight the following elements in the STAMP model:

- "Operator" and "Automated controller" (cf. **Figure 3**) are the components in charge to control and manage the process;
- "Inlet valve tank" (cf. **Figure 3**) is the actuator in charge to modify and operate all the changes and information by the controller;
- "Thermometer", "Barometer", and "Level sensor" are the sensors in charge to provide information and the status of the process; and
- "LNG tank (3)" is the controlled process.

In addition (cf. **Figure 3**):

- The downstream arrows represent the control actions referring to the activity, task, and actions that the actuator must perform to manage the process;
- The upstream arrows are the feedbacks that map the information moving from the process to the controller; and
- The horizontal arrows represent the process input and output that are necessary to manage or change the process itself.

Figure 3 allows mapping the procedures to manage the process, i.e., control loops. A first loop involves the operator, all the sensors and the actuator, and the LNG tank. This configuration is explicated during maintenance operations or when the control room doesn't work properly, and the operator must modify the process manually (i.e., "Open/close valve" arrow, cf. **Figure 3**). The second loop involves the operator, the automated controller, all the sensors and the actuator, and the LNG tank. These interactions depict a steady state condition in which the operator manages and controls the automated controller, leaving it in charge of the process control.

Following the methodology from **Section II**, the SCS has been translated into a FMS to verify and formally evaluate the industrial process. Accordingly, **Figure 4** and **Figure 5** show the excerpts of the FMS used in the case study. The process is divided into:

- a first model, which is meant to map the interactions and the correctness of the output of the "Inlet valve tank" (cf. **Figure 4**); and
- a second model representing the FMs of the "LNG tank", the "Thermometer", the "Barometer" and the "Level sensor" (cf. **Figure 5**). This FMS enables the modelling, the control, and the verification of the physical characteristic of the industrial process.

To this purpose, the "Filling_process" variable enables the formal verification of how the gas is stored into the LNG tank. The verification begins when the volume of gas is less than the maximum volume that the tank can contain. At this stage, the inlet valve is open, allowing the movement of the natural gas into the tank. The filling dynamics (i.e., f(v) in **Figure 4**) is represented by a function that depends on other system components such as the compressor (element (2), cf. **Figure 2**) and the carrier supply (element (1), cf. **Figure 2**). The "Filling_process" variable represents the steady condition in which the valve is open and allows the filling of the LNG tank, the "Tank_full" variable represents the condition in which the LNG tank is full.

Similarly, the FMS model in **Figure 5** checks the physical parameters through two formal verifications. The first verification checks the process working in its steady state condition.

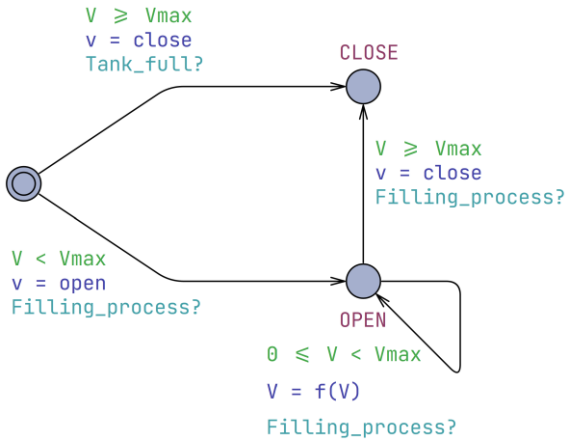

Fig. 4 FMS model involving the "Inlet valve tank".

The second one is meant to cover all the cases in which an anomaly is detected in the process and the controller stops it to prevent undesired events (i.e., "Emergency_stop" process). This model verifies the physical properties of the gas to evaluate both the steady state and the emergency stop during the filling process.

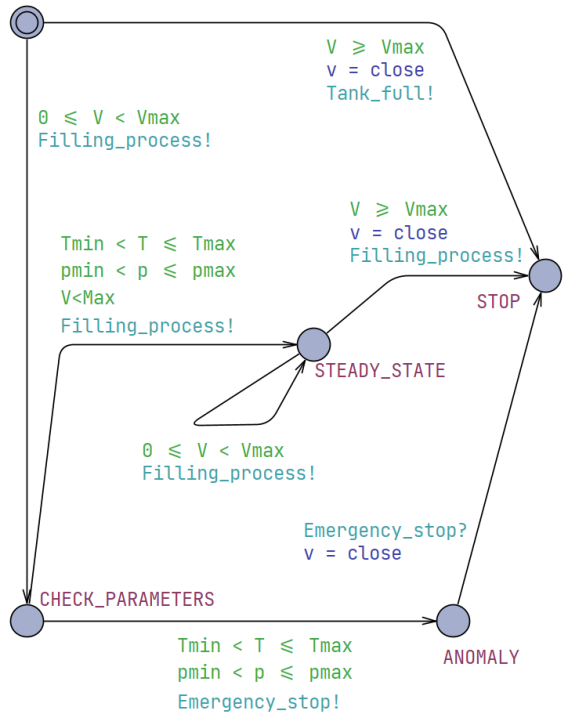

Fig. 5 FMS model involving: "LNG tank", "Thermometer", "Barometer", and "Level sensor".

Therefore, model checking simulation verifies the correctness of the process system by methodically exploring possible states and behaviors. It involves specifying the model and desired properties, generating the state space, checking if the properties hold, and analyzing any violations related to the process's design and/or operation. Moreover, the valve is used to control the LNG flow into or out of the tank. It can be opened or closed to regulate the supply or release of LNG in the pipeline ("Tank_full" and "Filling_process" in **Figure 4**). On the other hand, the model in **Figure 5** verifies the conditions of the physical properties of the process, i.e., volume, temperature, and pressure in the state "CHECK_PARAMETERS". If the process operates inside the established ranges of the temperature and pressure values, the "Filling_process" begins to fill the tank, otherwise, the process detects an anomaly and the "Emergency_stop" state occurs, closing the valve.
Moreover, the simulation has been checked upon the following.

- The thermometer monitors the temperature inside the tank to maintain a low temperature to keep the natural gas in its liquid state.
- The barometer measures the pressure inside the tank. The model verifies that the barometer ensures the pressure to remain within safe operating limits.
- The level sensor is adequate to control and manage the LNG volume level inside the tank.
- The valve controls the LNG quantity in the process and regulates the LNG flow (and subsequently volume).

Overall, these elements have provided important data for monitoring and controlling the LNG tank. The thermometer and barometer help monitoring the temperature and pressure values, while the level sensor ensures the tank maintaining within the desired level. Therefore, the performed simulation has formally verified. The combination of these elements ensures safe and efficient operation of the LNG storage process.
The obtained results highlight that integrating STAMP and model checking can be effectively and efficiently applied for the safety analysis of a natural gas storage process. This provides a preliminary confirmation about the usefulness of adopting system theoretic model checking in industrial plants. Its application to a real case study also permits emphasizing the potentialities of such approach. Indeed, it could reduce the efforts required to conduct the safety analysis and management of systems when their designs (e.g., layout modifications, introduction of additional components) and/or the substances (and thus their physical-chemical properties) inside them change. The methodology appears to be particularly relevant in achieving a cost-effective energetic transition towards renewable resources by adapting existing infrastructures and plants, permitting to formally verify the system safety constraint. Implementing the described methodology of integrating formal verification through model checking with STAMP principles entails cost factors. One cost-saving advantage of the described methodology is its ability to implement safety simulations and address issues without disrupting the real industrial process. By utilizing formal verification techniques like model checking and integrating them with STAMP model, potential safety concerns can be identified and analyzed in a simulated environment. This allows for proactive testing of new safety constraints and detecting system vulnerabilities without costly shutdowns or interruptions to industrial

operations. This cost-effectiveness is especially valuable when considering the expenses associated with halting operations, potential equipment damage, and the negative impact on productivity that could arise from unplanned shutdowns.

IV. CONCLUSION

This paper presents a methodology to integrate formal verification based on model checking technique with the STAMP principles. The early results show how the methodology can be used to verify and test safety issues and constraints in industrial applications. The resulting analysis is twofold. The application of STAMP permits mapping and designing industrial processes. This analysis can be made at different levels (e.g., organizational, technical, and social levels), highlighting the interactions among the different elements of the system. On the other hand, model checking offers a quantification by verifying these interactions.

The methodology can be used proactively to test and model new safety constraints to implement in the Safety Management System. Moreover, the results of model checking point at potential system vulnerabilities that have to be solved by updating system design (e.g., through additional control loops) to ensure safe industrial operations. A limitation in this sense is related to the fact that it might be difficult to spot whether an unmet constraint is an actual system vulnerability or simply an imprecision in the SCS modeling (which is a subjective representation). Future works may address this problem by developing a comprehensive framework to differentiate between errors of the SCS and actual lacking elements.

Overall, the paper shows promising results in applying the methodology integrating STAMP and model checking for industrial plants, which exploits both approaches to treat industrial safety challenges. All these aspects could improve the economic sustainability performance of any type of organizations.

REFERENCES

[1] Abdulkhaleq, A., Wagner, S. (2015). Integrated Safety Analysis Using Systems-Theoretic Process Analysis and Software Model Checking. In: Koornneef, F., and van Gulijk, C. (Eds.), *Computer Safety, Reliability, and Security. SAFECOMP 2014. Lecture Notes in Computer Science*, 9337, 121-134. Springer International Publishing Switzerland.

[2] Ando, T., Wang, B., Hisazumi, K., Kong, W., Fukuda, A., Michiura, Y., Sakemi, K., and Matsumoto, M. (2018). Verification Model Translation Method toward Behavior Model for CAST. In: *2018 5th International Conference on Dependable Systems and Their Applications, DSA 2018*, 142-147.

[3] Baybutt P. (2021). On the need for system-theoretic hazard analysis in the process industries. *Journal of Loss Prevention in the Process Industries*, 69, 104356.

[4] Chen, L., Zhong, D., Jiao, J., and Zhao, T. (2017). Improving Accident Causality Analysis Based on STAMP Through Integrating Model Checking. In: *Annual Reliability and Maintainability Symposium*, 1-7.

[5] Clarke, E.M. Jr., Grumberg, O., Kroening, D., Peled, D., and Veith, H. (2018). *Model Checking*. Second Edition. The MIT Press, Cambridge, Massachusetts.

[6] Dakwat, A.L., and Villani, E. (2018). System safety assessment based on STPA and model checking. *Safety Science*, 109, 130-143.

[7] de Souza, F.G.R., de Melo Bezerra, J., Hirata, C.M., de Saqui-Sannes, P., and Apvrille, L. (2020). Combining STPA with SysML Modeling. In: *2020 IEEE International Systems Conference (SysCon)*, 1-8.

[8] Eleftherakis, G., and Kefalas, P. (2001). Towards model checking of finite state machines extended with memory through refinement. *Advances in signal processing and computer technologies*, 321-326.

[9] Han, X., Tang, T., and Lv, J. (2019). A hierarchical verification approach to verify complex safety control systems based on STAMP. *Science of Computer Programming*, 172, 117-134.

[10] Leveson N. (2004). A new accident model for engineering safer systems. *Safety Science*, 42, 237-270.

[11] Leveson, N. (2012). *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press, Cambridge, MA.

[12] Mokhatab, S., Mak, J.Y., Valappil, J.V., and W, D.A. (2014). *Handbook of Liquefied Natural Gas*. Gulf Professional, Oxford.

[13] Nakhal Akel, A.J., Di Gravio, G., Fedele, L., and Patriarca, R. (2022). Learning from Incidents in Socio-Technical Systems: A Systems-Theoretic Analysis in the Railway Sector. *Infrastructure*, 7, 90.

[14] Okano, K., Yang, P., Ogata, S., and Okamoto, K. (2020). Deriving of Time Constants in Timed Automata for Hazard Transition Sequences for STAMP/STPA. *Procedia Computer Science*, 176, 1392-1401.

[15] Razzaq, M., and Ahmad, J. (2015). Petri Net and Probabilistic Model Checking Based Approach for the Modelling, Simulation and Verification of Internet Worm Propagation. *PLoS ONE*, 10(12), e0145690.

[16] Sadeghi, R., and Goerlandt, F. (2023). A proposed validation framework for the system theoretic process analysis (STPA) technique. *Safety Science*, 162, 106080.

[17] Simone, F., Nakhal Akel, A.J., Di Gravio, G., and Patriarca, R. (2023). Thinking in Systems, Sifting Through Simulations: A Way Ahead for Cyber Resilience Assessment. *IEEE Access*, 11, 11430-11450.

[18] Tsuji, M., Takai, T., Kakimoto, K., Ishihama, N., Katahira, M., and Iida, H. (2020). Prioritizing Scenarios based on STAMP/STPA Using Statistical Model Checking. In: *2020 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, 9155811, 124-132.

[19] Wang, Y., and Wagner, S. (2016). Towards applying a safety analysis and verification method based on STPA to agile software development. In: *2016 IEEE/ACM International Workshop on Continuous Software Evolution and Delivery (CSED)*, 2896948, 5-11.

[20] Xu, Q., and Lin, J.T. (2023). Safety requirement verification of train-centric CBTC by integrating STPA with coloured Petri net. *International Journal of Industrial and Systems Engineering*, 43(2), 168-189.

[21] Yang, P., Karashima, R., Okano, K., and Ogata, S. (2019). Automated inspection method for an STAMP/STPA – Fallen Barrier Trap at Railroad Crossing. *Procedia Computer Science*, 159, 1165-1174.

[22] Yang, Q., and Tian, J. (2015). A formal approach to causal analysis based on STAMP (CAST). In: *2015 First International Conference on Reliability Systems Engineering (ICRSE)*, 7366434, 1-8.

[23] Ye, N., Zhang, J., and Wu, J. (2020). Components Interaction Safety Analysis Method Based on STAMP and Formal Verification. In: *ACM International Conference Proceeding Series*, 46-50.

[24] Zhang, Y., and Liu, S. (2019). STPA Based Safety Analysis of Regional Data Center in CTCS-1 Train Control System. In: *2018 IEEE International Conference of Safety Produce Informatization (IICSPI)*, 8690446, 240-245.

[25] Zhong, D., Sun, R., Gong, H., and Wang, T. (2022). System-Theoretic Process Analysis Based on SysML/MARTE and NuSMV. *Applied Sciences*, 12, 1671.