CHEMICAL ENGINEERING TRANSACTIONS

VOL. 91, 2022

A publication of AIDIC

The Italian Association
of Chemical Engineering
Online at www.cetjournal.it

Guest Editors: Valerio Cozzani, Bruno Fabiano, Genserik Reniers
Copyright © 2022, AIDIC Servizi S.r.l.
ISBN 978-88-95608-89-1; **ISSN** 2283-9216

DOI: 10.3303/CET2291068

A STAMP Model for Safety Analysis in Industrial Plants

Antonio Javier Nakhal Akel[a], Riccardo Patriarca[a], Massimo Tronci[a], Patrizia Agnello[b], Silvia Maria Ansaldi[b], Alessandro Ledda.[b]

[a] Department of Mechanical and Aerospace Engineering, Sapienza University, Rome, Italy

[b] Department of Technological Innovations and Safety of Plants, Products and Anthropic Settlements, INAIL (Italian National Institute for Insurance against Accidents at Work), Rome, Italy
antonio.nakhal@uniroma1.it

Traditional safety risk analysis methods are rooted in event chain modeling and looking for individual points of failure. This approach allowed tremendous improvement in safety management but starts to be difficult to apply when dealing with large-scale systems constituted by a wide number of interactions among technical and social elements. Therefore, systemic safety management poses new challenges, demanding approaches capable of complementing techno-centric investigations with social-oriented analyses. For this purpose, this study adopts the Systems-Theoretic Accident Model and Processes (STAMP) as a new accident causation model based on systems theory. Such a model is the first element to gain a complete understanding of the system at hand, and subsequently to create a set of safety recommendations. STAMP can lead to both the development or evaluation of safety management systems and the identification of leading indicators related to hazards, in order to improve decision-making domains and strengthen accidents/loss analyses.

The present research incorporates three basic components of systems theory for STAMP models: constraints, hierarchical control structure, and process loops. These items are meant to allow recognizing causes and preventing potential system failures as well as undesired events. In the proposed model, accidents are examined in terms of the ways controls fail and how they may not allow prevention or detection of hazards. This study proposes a hierarchical safety control structure on a demonstrative use case referred to an industrial plant for gas and oil production, The model consists of system-level safety constraints, and a preliminary investigation of system's components with the purpose of supporting physical and organizational safety requirements elicitation.

1. Introduction

Safety and risk management are intended to understand how undesired events (accidents/incidents) occur, with the purpose to improve systems' condition of the process to reduce or eliminate the hazard related to the past events. In these domains, one strategy to achieve these aims is the accident model analysis that supports the basic elements of safety and risk process (Li et al., 2017; Rasmussen and Svedung, 2000). The aim of accident models is to identify accident causal factors, and hence determine what measures need to be implemented to avoid similar consequences or reduce their likelihood (Bugalia et al., 2020). The present accident reports are sometimes poorly defined when referring to causes, since accident analyses may focus on finding someone or something to blame: this situation leads to miss the opportunity to learn important lessons to improve system safety (Leveson, 2011). Currently, due to the increase in systems' complexity, many accidents do not result from a linear causal chain, but they are caused by non-trivial socio-technical interactions e.g., human factors, mission profile, equipment, financial pressures, and information that increase the normal operational variability of the system process (Rong and Tian, 2015). Therefore, other complex-oriented accident analysis models seem necessary, possibly relying on systems' thinking. This latter focuses on a combination of thinking about the operation or/and management process related with the analyzed system (Leveson, 2011). More formally, systems thinking consists of three aspects: (i) elements' characteristics; (ii) interconnections between the elements; (iii) systems functional purpose. On these premises, systems theory can be applied within safety manage to analyze interactions among system

Paper Received: 16 January 2022; Revised: 8 April 2022; Accepted: 2 May 2022
Please cite this article as: Nakhal Akel A.J., Patriarca R., Tronci M., Agnello P., Ansaldi S.M., Ledda A., 2022, A Stamp Model for Safety Analysis in Industrial Plants, Chemical Engineering Transactions, 91, 403-408 DOI:10.3303/CET2291068

components and systems' behaviors (Patriarca et al., 2022). One interesting stream of research in this sense is built up around the Systems-Theoretic Accident Modelling and Processes model (STAMP), which is rooted in control theory and hierarchical safety control structures.

On these remarks, this paper aims to explore the usage of STAMP as a systemic model to create a safety control structure for the analysis of systems' criticalities. This aim has been contextualized to model the hydrocracking process, i.e., an industrial process in which the components of gas oil fractions are (partially or completely) converted into lighter molecules under the influence of hydrogen, in the presence of a catalyst.

2. Methodology

The System-Theoretic Accident Model and Processes (STAMP) is a model which transform safety management system in a control problem. Emergent properties are controlled by imposing safety constraints on the behavior of, or the interaction among, systems' components. Accidents result thus from inadequate control or enforcement of safety related constraints on the development, design, and operation of the system. The interactions must be established to accomplish the control of the system's behavior by enforcing the safety constraints in its design and operation. The STAMP model is founded on three basic concepts (Leveson, 2011):

1. *The safety constraints*. In STAMP, constraints are equally important to the event/hazards: STAMP modeling assumes that events lead to losses only because safety constraints have not been successfully applied. However, an active feedback/control mechanism shall be provided to ensure system constraining.
2. *The Hierarchical Safety Control Structure*. Incidents occur when processes provide insufficient control and/or safety constraints are violated: among the hierarchical levels of each control structure, downward communication channels are required to provide information, and upwards communications channels are meant to acquire feedback and measures about the level of constraints satisfaction.
3. *The Process Model.* Each systems' component needs a process model: models can be simple or built upon dozens of parameters. For defining a process model, it is necessary to define a set of variables, their value over time, and the control laws to relate them to varieties of executions.

3. Case study

For demonstration purposes, the manuscript has been focused on the petroleum refineries sector. In particular, the refining technology that converts a variety of feedstocks to a range of products, and units, known as hydrocracking. Hydrocracking is a catalytic refining process widely used to remove sulfur from crude oil products such as naphtha, gasoline, diesel fuel, kerosene, and fuel oil (Speight, 2020). This process has been largely used due to its potential to maximize the yield of transportation fuels and its production flexibility, along with the suitability to use the unconverted oil as a feedstock for the conventional thermal catalytic cracker (Wei et al., 2020).

3.1 Detailed process description

The single-stage recycling hydrocracking has been chosen to perform the analysis. Figure 1 lists each component providing numbered elements and sketches functional relationships to facilitate process description. The process starts In the reactor (1), in which conversion of Nitrogen and Sulphur compounds, saturation and partial saturation of olefins, and polycyclic aromatic hydrocarbons take place (Rigutto et al., 2007). The oil is combined with a preheated mixture of makeup hydrogen and hydrogen-rich recycled gas and then heated to reactor inlet temperature via heat exchanger I (feed-effluent exchanger, (3)) and a heat exchanger II (reactor charge heater, (4)). From heater (2), the partially vaporized flow is loaded into separate beds in the reactor. The reactor discharged effluent is then cooled through a heat exchanger IV (11) and heat exchanger III (12). The deaerator (10) is inserted into the reactor discharge effluent before the removal of ammonia. The reactor effluent passes into the high-pressure separator (6) to be divided into hydrogen-rich recycle gas, sour water stream, and hydrocarbon liquid stream. The gas is recycled back to the reactor feed by using a recycling compressor (5). The hydrocarbon-rich stream is fed to the distillation section after low-boiling products are flashed off in a low-pressure separator (7). The distillation section consists of a hydrogen sulfide stripper and a recycling splitter. This latter separates the product into the desired cuts passing through the fractioner (8) (Speight, 2020; Thybaut and Marin, 2016).

3.2 System-Theoretic Accident Model and Processes analysis

The STAMP model has been used to define the Safety Control Structure (SCS) of the process and describe how components functionally interact with each other.

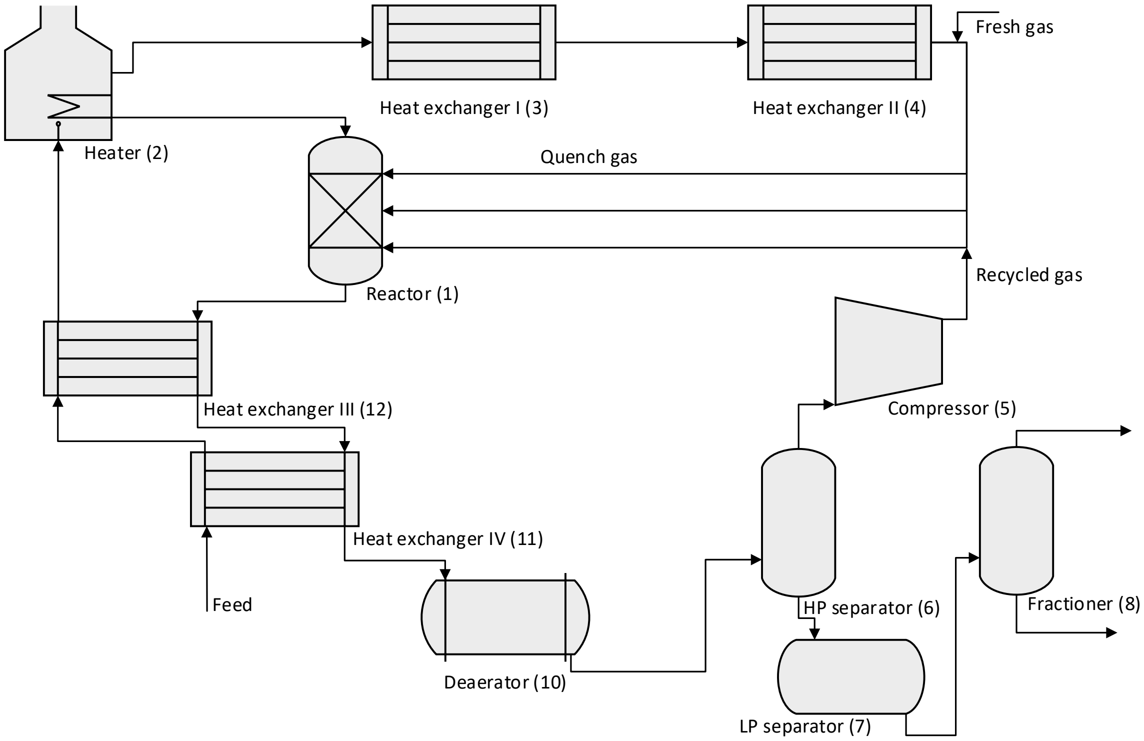

Figure 1. Single stage recycling hydrocracking process diagram

This paragraph presents two stages of analysis: (i) the description of the high-level SCS; (ii) an excerpt detailed on three components (highlighted in red color, in Figure 2) of the SCS that concentrates control process elements.

The high-level SCS is represented in Figure 2 and it has been sectioned into: The Cabinet of Minister through the different Department; The Government Regulatory Office & Industries Associations; Company management. These three components compound the governance on the process considerer. The plant organization (green box in Figure 2) has instead the following components: Central Utilities Plant Operations; Plant Engineering office; Operators & Contractors; Central Automated Control System; Automated Control sub-systems for hydrocracking; Heater; Heat exchanger I; Heat exchanger II; Heat exchanger III; Heat exchanger IV; Compressor; Reactor; Deaerator; High-Pressure (HP) separator; Low-Pressure (LP) separator; Fractioner; Automated Control sub-systems for other refinery processes; Other controlled refinery processes.

A more granular SCS is proposed by isolating only six components (case of study represented by the purple box in Figure 2) of the system process to have a more detailed description about the interactions between them. This excerpt has been represented in Figure 3. The fractal nature of STAMP allows indeed exploiting controls at different levels of abstraction: this detailed SCS has been defined to highlight the control actions and feedback between the heater (2) and the first two heat exchangers (3) and (4) (red boxes in Figure 3). The Automated Control sub-system has been described by means of two controllers: *Human Controller* (orange boxes in Figure 2 and Figure 3): that generates a control action to the Automated Controller and receives the feedback information regarded in the process controlled. *Automated Controller* (blue boxes in Figure 2 and Figure 3), that is responsible to receive the control action generated by the Human Controller and forward this control in the process in light of its process model. Additionally, the Central Automated Controller (light blue boxes in both figures) shall guarantee the presence of a feedback loop on the process being controlled, as well as process operability in terms of correct actioning (Khan et al., 2019; Sahin et al., 2005; Vasičkaninová et al., 2016). The interconnections (control actions, feedback, inputs, and outputs) highlighted in grey define the interactions between the components (Heater (2); Heat exchanger I (3); Heat exchanger II (4)) and the components not considered in the detailed analysis.

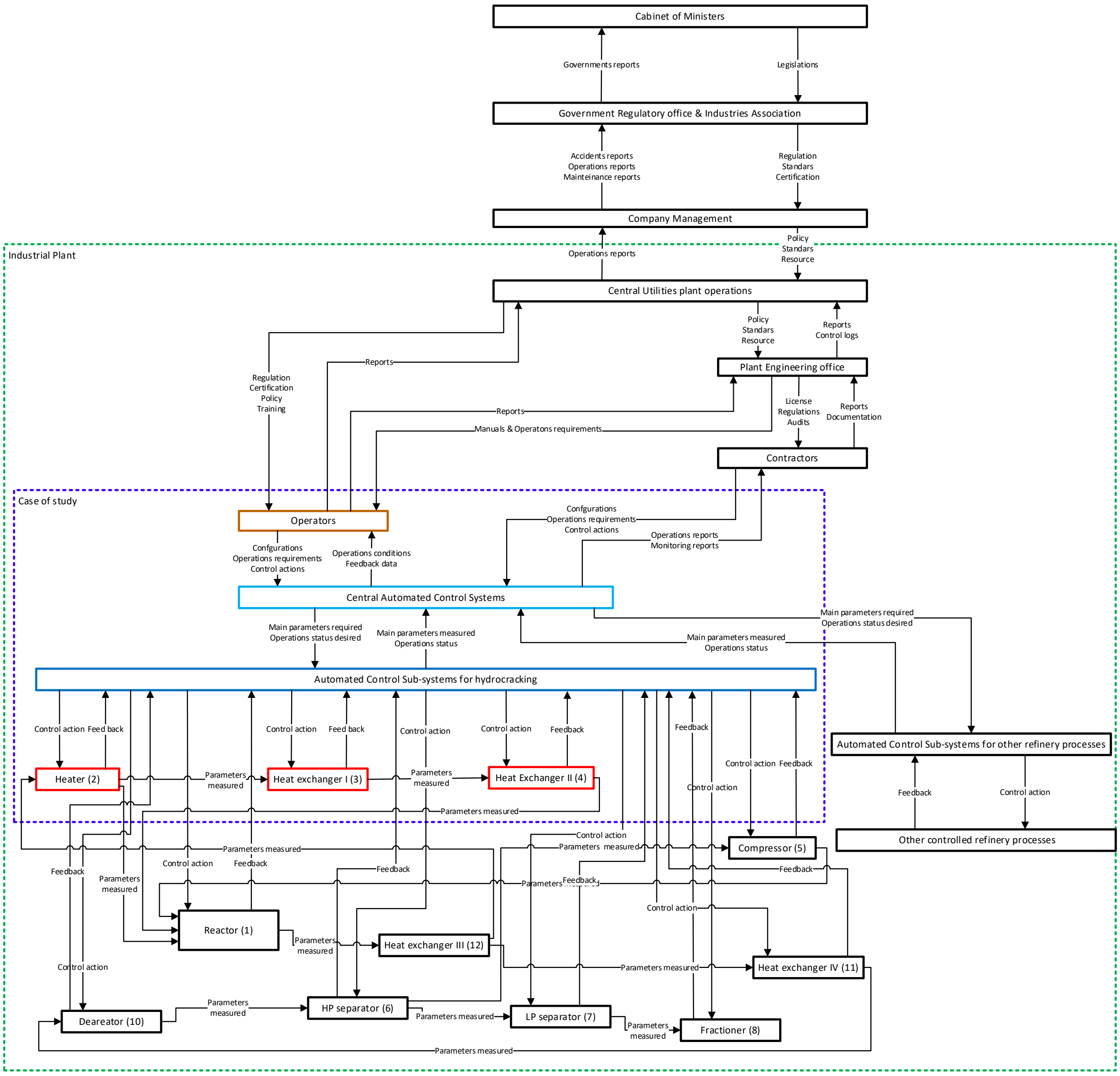

Figure 2. High-level Safety Control Structure for hydrocracking process.

Table 1 describes more in detail the main parameters involved in the single stage recycle hydrocracking, by means of the parameters involved in the process and interactions between components (Sahin et al., 2005). Besides, information regarding the parameters allows updating the detailed SCS where each control action defined as “Main parameters; Set points; Lead-Lag configurations”, must be replaced by new control actions. Similarly, feedback defined as "Status & Operations condition"; "Main parameters status" and "Main parameters" must be iteratively replaced by new feedbacks.

Table 1. Main parameters of the heater in the analysed hydrocracking process (Vasičkaninová et al., 2016)

Main parameters	Heater expected range of functioning
Fluid velocity (U) [kg/h]	0,5 ~ 2
Mean temperature (T) [K]	554 ~ 750
Pressure (P) [KPa]	35 ~ 200

The monitoring of the parameters is a critical task in the hydrocracking process since any condition change in the parameters might compromise the feedstocks quality. Both heater exchangers reflect the same logic.

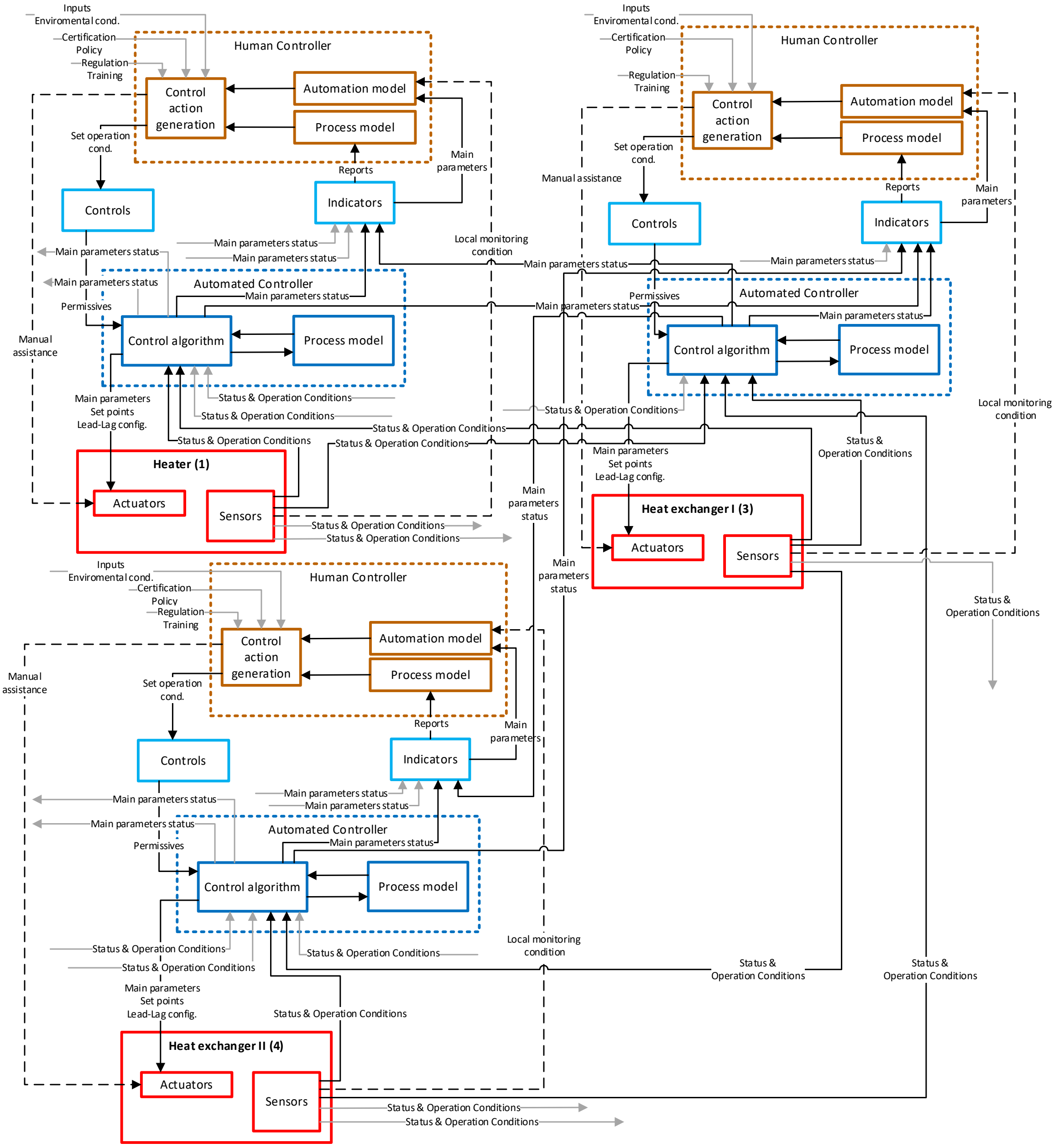

Figure 3. Detailed safety control structure to the Heater; Heat exchanger I; Heat exchanger II.

4. Conclusions

The present study provides a first demonstration of a system-theoretic approach for chemical industry systems applied, as instantiated into a single stage recycle hydrocracking process. This study shows how control systems can be integrated into a system engineering perspective to create models for systemic safety analyses. Safety is a top priority for managing effectively chemical facilities, and as such modern safety management theories can become valuable to extend traditional linear or combinatorial safety models (e.g. Heinrich domino model, Reason Swiss Cheese model) (Abbassi et al., 2016; Paltrinieri et al., 2014). The purpose of this application is to prove such extendibility, and to motivate the need for future research: this STAMP model could indeed be extended with Causal Analysis based on STAMP (CAST), where the STAMP model provides guidance to identify which control actions ineffectively have acted in the SCS. From a proactive perspective, the STAMP analysis included in this paper can be also used as a basis for the Systems Theoretic Process Analysis (STPA) technique, where safety constrains are designed to prevent the cascading effects of hazards (Lu et al., 2015). Especially in STPA analysis, the linguistic assessment can be further extended with quantitative methodologies, as for the system dynamics modelling (Hu et al., 2019); or the combination of statistical model checking to prioritize scenarios, losses or components to focus the study and to improve the safety system (Tsuji et al., 2020). Overall, these examples motivate the need for future research also in the chemical sector to incorporate systems thinking into management practices.

Acknowledgement

This work is partly funded by Department of Technological Innovations and Safety of Plants, Products and Anthropic Settlements, INAIL (Italian National Institute for Insurance against Accidents at Work), as for the project “Resilience analysis for the evolution of industrial sociotechnical systems in critical or highly complex contexts”.

References

Abbassi, R., Bhandari, J., Khan, F., Garaniya, V., Chai, S., 2016. Developing a quantitative risk-based methodology for maintenance scheduling using Bayesian network. Chem. Eng. Trans. 48, 235–240. doi:10.3303/CET1648040

Bugalia, N., Maemura, Y., Ozawa, K., 2020. Organizational and institutional factors affecting high-speed rail safety in Japan. Saf. Sci. 128. doi:10.1016/j.ssci.2020.104762

Hu, S., Xuan, S., Li, Z., Hu, Q., Xi, Y., 2019. Dynamics simulation for process risk evolution mode on fueling of LNG-fueled vessel. ICTIS 2019 - 5th Int. Conf. Transp. Inf. Saf. 313–323. doi:10.1109/ICTIS.2019.8883559

Khan, S., Madnick, S.E., Moulton, A., 2019. Cyber-Safety Analysis of an Industrial Control System for Chillers Using STPA-Sec. SSRN Electron. J. July . doi:10.2139/ssrn.3370540

Leveson, N., 2011. Engineering a safer world: systems thinking applied to safety. The MIT Press.

Li, W., Zhang, L., Liang, W., 2017. An Accident Causation Analysis and Taxonomy (ACAT) model of complex industrial system from both system safety and control theory perspectives. Saf. Sci. 92, 94–103. doi:10.1016/j.ssci.2016.10.001

Lu, Y., Zhang, S.-G., Tang, P., Gong, L., 2015. STAMP-based safety control approach for flight testing of a low-cost unmanned subscale blended-wing-body demonstrator. Saf. Sci. 74, 102–113. doi:10.1016/j.ssci.2014.12.005

Paltrinieri, N., Scarponi, G.E., Khan, F., Hauge, S., 2014. Addressing dynamic risk in the petroleum industry by means of innovative analysis solutions. Chem. Eng. Trans. 36, 451–456. doi:10.3303/CET1436076

Patriarca, R., Chatzimichailidou, M., Karanikas, N., Di Gravio, G., 2022. The past and present of System-Theoretic Accident Model And Processes (STAMP) and its associated techniques: A scoping review. Saf. Sci. 146 November 2021 , 105566. doi:10.1016/j.ssci.2021.105566

Rasmussen, J., Svedung, I., 2000. Proactive risk management in a dynamic society. Swedish Rescue Services A.

Rigutto, M.S., van Veen, R., Huve, L., 2007. Zeolites in hydrocarbon processing. Stud. Surf. Sci. Catal. 168, 855–913. doi:10.1016/S0167-2991(07)80812-3

Rong, H., Tian, J., 2015. STAMP-based HRA considering causality within a sociotechnical system: A case of minuteman III missile accident. Hum. Factors 57 3 , 375–396. doi:10.1177/0018720814551555

Sahin, B., Yakut, K., Kotcioglu, I., Celik, C., 2005. Optimum design parameters of a heat exchanger. Appl. Energy 82 1 , 90–106. doi:10.1016/j.apenergy.2004.10.002

Speight, J., 2020. The refinery of the future, Second. ed. Gulf Professional Publishing, Laramie, Wyoming.

Thybaut, J.W., Marin, G.B., 2016. Multiscale Aspects in Hydrocracking: From Reaction Mechanism Over Catalysts to Kinetics and Industrial Application, 1st ed, Advances in Catalysis. Elsevier Inc. doi:10.1016/bs.acat.2016.10.001

Tsuji, M., Takai, T., Kakimoto, K., Ishihama, N., Katahira, M., Iida, H., 2020. Prioritizing Scenarios based on STAMP/STPA Using Statistical Model Checking. Proc. - 2020 IEEE 13th Int. Conf. Softw. Testing, Verif. Valid. Work. ICSTW 2020 124–132. doi:10.1109/ICSTW50294.2020.00032

Vasičkaninová, A., Bakošová, M., Čirka, L., Kalúz, M., 2016. Robust controller design for a heat exchanger. Chem. Eng. Trans. 52 2002 , 247–252. doi:10.3303/CET1652042

Wei, R., Li, H., Chen, Y., Hu, Y., Long, H., Li, J., Xu, C.C., 2020. Environmental Issues Related to Bioenergy, 2nd ed, Reference Module in Earth Systems and Environmental Sciences. Elsevier Inc. doi:10.1016/b978-0-12-819727-1.00011-x