Process Safety and Environmental Protection 177 (2023) 1181–1196

Contents lists available at ScienceDirect

Process Safety and Environmental Protection

journal homepage: www.journals.elsevier.com/process-safety-and-environmental-protection

A System-Theoretic Fuzzy Analysis (STheFA) for systemic safety assessment

A.J. Nakhal A. [a], R. Patriarca [a], F. De Carlo [b,*], L. Leoni [b]

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

ARTICLE INFO

Keywords:
System thinking
Industrial accident analysis
Fuzzy logic
STAMP model
Expert opinion

ABSTRACT

The interactions among distinct systems and components have attracted more attention recently due to safety concerns. Indeed, modern industrial plants could be regarded as complex socio-technical systems influenced by human, social, and organizational aspects. To model this level of complexity, System Theory (ST) and related frameworks, such as System-Theoretic Accident Model and Processes (STAMP) have been introduced. Despite their strengths and abilities, ST techniques are mainly qualitative and provide much information, eventually complicated to analyse and summarize. Fuzzy Set Theory (FST) and expert elicitation could be employed to cope with the former challenges. However, addressing the uncertainty arising from differences in expert opinions is necessary. To this end, this paper aims to develop a framework to conduct system safety assessments based on the integration of STAMP and FST. In this context, an improved version of the Similarity Aggregation Method is adopted to aggregate judgments. To demonstrate the application of the approach, a Natural Gas Regulating and Metering Station (NGRMS) is considered as the case study. The results show that the methodology is able to provide quantitative information by associating a level of criticality with each control action. Accordingly, managers could exploit the framework to identify priorities for directing efforts.

1. Introduction

Over recent years, adopting new digital transformation technologies (digitalization) and implementing modern automatization in the industrial plant processes have demanded increasing attention towards the interactions and interconnections among the system components (Elmaraghy et al., 2012). Therefore, current industrial plants may be considered complex socio-technical since managerial decisions and technical design aspects involve human, social, and organizational factors (Nakhal A, Patriarca et al., 2022). Moreover, the need for using analytical frameworks and management guidelines to deal with the complex nature of modern systems has progressively become more evident over time. Indeed, the complexity perspective has gained traction in safety domains as it has provided insights into investigating accidents and incidents casual factors (Dekker, 2019). Traditional risk assessment analysis and safety techniques methods (e.g., Fault Tree Analysis, Bow Tie, Failure Mode and Effects Analysis, etc.) are rooted in event chain modeling and looking for individual points of failure or faults as consequences or causes of the accidents. Hence, Safety Management Systems (SMSs) seek to determine how the system design could be improved to avoid or prevent such undesired scenarios. One strategy to achieve these the former objective is the accident model analysis that supports the essential elements of the safety risk process (Li et al., 2017; Rasmussen and Svedung, 2000). However, modern risk assessment and safety analysis techniques must deal with large-scale systems constituted by a wide number of interactions among technical, social, and organizational elements. Therefore, due to the increase in systems complexity, many accidents do not result from a linear causal chain but 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).

Consequently, complex-oriented accident analysis models seem necessary, possibly relying on System Theory (ST) supported by fuzzy

Abbreviations: BN, Bayesian Network; CA, Control Action; CAST, Causal Analysis based on System Theory; CC, Consensus Coefficient; DA, Defuzzied Number; FB, Feedback; FBN, Fuzzy Bayesian Network; FRAM, Functional Resonance Analysis Method; FST, Fuzzy Set Theory; ICA, Inappropriate Control Action; ML, Machine Learning; NGRMS, Natural Gas Regulating and Metering Station; PN, Priority Number; RA, Relative Agreement; ROV, Ratio of Variation; SAM, Similarity Aggregation Method; SCS, Safety Control Structure; SD, Similarity Degree; SMS, Safety Management System; ST, System Theory; STAMP, Systems-Theoretic Accident Model and Process; STPA, System-Theoretic Process Analysis; THT, Tetrahydrothiophene; UCA, Unsafe Control Action; W, Weight; WAA, Weighted Absolute Agreement.

* Corresponding author.
E-mail address: filippo.decarlo@unifi.it (F. De Carlo).

https://doi.org/10.1016/j.psep.2023.07.014
Received 24 April 2023; Received in revised form 29 June 2023; Accepted 3 July 2023
Available online 7 July 2023

logic to investigate accidents and prevent their occurrence of them. ST consists of three aspects (N. Leveson, 2004, 2011): (i) elements' characteristics; (ii) interconnections among the elements; (iii) systems' functional purpose. On these premises, systems theory can be applied within safety management to analyze interactions among system components and systems' behaviors (Patriarca et al., 2022). In this context, one interesting stream of research is built around the System-Theoretic Process Analysis (STPA) technique, which is rooted in control theory and hierarchical safety control structures to identify the unsafe and inappropriate control actions of the system process (Abdulkhaleq et al., 2015; N. Leveson and Thomas, 2018). These items are meant to allow recognition of causes and prevent potential system failures as well as undesired events. In the STPA technique, undesired events are examined in terms of control system failure and how they may not allow the prevention or detection of hazards. Therefore, a detailed STPA usually leads to identifying several Unsafe Control Actions (UCAs), but it could be tough to provide them with suitable solutions to reduce their occurrence or impact. In this context, identifying the most critical ones could be useful to determine which UCAs should be prioritized (i.e., which are the UCAs that must be treated first, and which direct the most efforts) to reduce or prevent such conditions (Chaal et al., 2020). Another complex-oriented accident analysis is the Functional Resonance Analysis Method (FRAM) defined as a systemic approach used to understand and analyze complex socio-technical systems and their resilience (Saurin and Werle, 2017). FRAM helps identify and analyze the functional dependencies within a system and how they contribute to system performance and resilience. It focuses on understanding how different functions in a system interact and how performance variability arises from these interactions. It aims to provide a systemic understanding of how a system operates and adapts under varying conditions (Lundberg et al., 2008).

In the context of accident analysis models based on ST, some works integrate Fuzzy Set Theory (FST) to develop the associations among various system components and the functional interaction among them (N. G. Leveson, 2017; Pasman, 2009; Patriarca et al., 2021). Therefore, the following section describes some works on how these topics have been previously applied in industrial processes, highlighting the advantages of each one. Within the Natural Hazards Triggering Technological Accidents (NATECH), a fuzzy-based technique has been used to simulate and quantify the failure magnitude in a Water System combined with the System Dynamics model (Milašinović et al., 2023). The methodology uses a causal approach where each subsystem's failure depends on external disturbance and subsystem reliability, which are used as input variables for a fuzzy logic-based failure magnitude simulator (Milašinović et al., 2023). While FRAM primarily focuses on functional resonance and functional analysis representation, STAMP approaches safety as a control problem. As a result, STAMP generates a hierarchical control structure that is characterized by control and feedback loops (Adriaensen et al., 2022).

Within accident investigation, the integration of Bayesian Network (BN) and Fuzzy Set Theory (FST) known as Fuzzy Bayesian Network (FBN) (Yazdi and Kabir, 2017; Zarei et al., 2019) has been adopted and combined with Similarity Aggregation Method (SAM). Indeed, SAM allows to consider the consensus degree, tackling the uncertainty arising from the different cognitive levels of individuals in the process of aggregation. A more recent study proposes an approach for risk assessment of storage tank accidents, combining an improved SAM and FBN to handle epistemic uncertainty caused by insufficient data and incomplete knowledge (Chen et al., 2006; Guo et al., 2021). The improved methodology better reflects expert judgments and reduces sensitivity to unidentifiable factors. Considering maritime applications, a study proposed a modified quantitative System-Theoretic Accident Model and Processes (STAMP) framework. Considering STAMP, it is possible to state that it is a subjective and qualitative approach rather than a quantitative analysis (one of its limitations). Therefore, previous research presents a modified quantitative methodology for complex process accident analysis based on a system engineering perspective to fill the mentioned gap using fuzzy theory (Ceylan et al., 2022; Zhang et al., 2019). Specifically, the former study proposes a novel quantitative approach based on the STAMP model and rule-based fuzzy technique to investigate complex process accidents.

However, current research is still missing information on how to employ judgments or expert opinions (e.g., operators, managers, researchers, etc.) to prevent or reduce undesired events identified through ST-based approaches. Moreover, there is a need to incorporate quantitative information into the former techniques to direct efforts towards the most critical CAs. Thus, this study aims to identify and prioritize the criticalities of a hazardous system by integrating a quantitative analysis and ST. Specifically, a combination of the STPA technique and FST is exploited to address safety concerns and prevent accidents in a system process. First, by adopting STPA, the present research aims to identify interactions and unsafe conditions within the system that could lead to accidents. Subsequently, FST and the improved SAM for expert opinion aggregation are employed. FST allows for the representation and analysis of vague or imprecise information arising from the experts (Zhou and Thai, 2016). By integrating expert opinions into the STPA, it is possible to identify and prioritize inappropriate or unsafe conditions by assigning to each unsafe condition a priority index. Accordingly, the exploitation of FST and expert opinions could help to improve the exploration of conditions that could potentially lead to accidents. Indeed, the proposed novel approach leads to the development of SMSs, along with the identification of leading indicators related to hazards, to improve decision-making domains and strengthen accidents/loss analyses. Indeed, the identification of priorities allows to direct efforts towards the most critical unsafe conditions, which could be targeted with appropriate countermeasures. To demonstrate the application of the proposed framework, a Natural Gas Regulating and Metering Station (NGRMS) has been chosen as a case study. A NGRMS is an industrial plant that reduces the pressure of the gas flow, adds a predefined quantity of odorizer, and tracks the mass flow of the natural gas. A particular focus will be devoted to the filtration stage of the plant.

The remainder of this paper is organized as follows; Section 2 presents the adopted tools and the developed framework arising from the integration of STPA and FST. In Section 3, the application of the developed framework to the NGRMS is illustrated, while, in Section 4, the discussions are presented. Finally, in Section 5, the conclusions, along with limitations and possible future research avenues are drawn.

2. Methodology

This section provides information on how FST supports the hazard analysis method using an extended model on accident causation as STPA to simplify the identification process of inadequate or inappropriate safety control in a design process. Therefore, the section defines the STPA technique and the FST as the basis of this novel safety analysis approach. Lastly, the section explains step by step the integration of both techniques.

2.1. System-Theoretic Process Analysis (STPA) technique

The STPA technique is rooted in STAMP. The technique aims to analyze the system and its interactions among different operational, social, and technological levels to identify safety issues and enforce them through safety recommendations and constraints (N. Leveson, 2004). Hence, the STPA method proposes four phases defined as follows (N. Leveson and Thomas, 2018):

1. Define the purpose of the analysis: the technique requires the definition of the scope of the analysis in terms of System Boundaries (processing system and corresponding parameters), Losses of concern (concerning stakeholders), and Hazards (the set of conditions with the potential to lead to a loss).

2. Model the Safety Control Structure (SCS): the core of the technique is a hierarchical control structure, as for the STAMP. The latter models socio-technical processes in terms of control loops: every process is intended as controlled through specific actions that are performed by controllers described via Process Model and Control Algorithms (for human controllers, this is the knowledge/understanding of the process, and for the automated controllers, this is a PID controller algorithm). The Process Model uses process feedback to determine the controller's beliefs about the system's state. The Control Algorithm determines the controller's response to its beliefs.
3. Identify UCAs: once the SCS has been developed, every control loop is studied to identify the possible ways it might lead to a loss. The STPA proposes some ways in which a control action might be inappropriate or inadequate: (i) in terms of execution (the control loop is provided or not provided); (ii) in terms of timing o sequence (the control loop provides too early/too late or wrong/inappropriate/out of order); and (iii) in terms of duration (the control loop is stopped too soon or applied too long).
4. Identify Causal Scenarios: once relevant UCAs have been recognized, the last step of the technique is to identify scenarios that could lead to them with the ultimate purpose of identifying safety recommendations.

2.2. Fuzzy set theory and expert opinion aggregation

FST is a mathematical tool that deals with uncertainty and imprecision. It is widely used in risk assessment and decision-making processes, especially in cases where the data is incomplete, ambiguous, or vague (Langari, 1996; Markowski et al., 2009). The theory defines a fuzzy set as a set that allows partial membership of elements. It allows the possibility of having an element in a set with varying degrees of membership, unlike classical set theory, where elements are either in or out of a set. Therefore, expert opinion aggregation is a method of combining expert judgments to obtain a more accurate assessment (Guo et al., 2021). It is commonly used when the problem is complex and the available data is insufficient or uncertain. FST can be used to aggregate expert opinions by representing the expert judgments as fuzzy sets. The degree of membership of an element in a fuzzy set represents the expert's confidence in their judgment. Hence, the FST using Expert Opinion Aggregation proposes six steps to perform the analysis (Dutta Majumder and Majumdar, 2004; Gentile et al., 2003):

1. Define the purpose of the analysis: the theory requires the identification of the problem and the definition of the scope of the analysis. Therefore, identify the input data: Identify the data that will be used as input for the FST analysis (e.g., expert opinions, survey data, or historical data) and define the output that will be generated by the analysis, i.e., probability estimates, decision recommendations, or predicted outcomes. In addition, it is important to determine the level of detail required for the analysis. Moreover, the granularity of the input data, the complexity of the fuzzy logic operators, or the resolution of the output.
2. Define fuzzy scales: the fuzzy scale is the measurement that allows for degrees of membership or uncertainty. To define a fuzzy scale, it is essential to determine the variable to be measured and its range of values. Then, divide the range into intervals or categories and assign a degree of membership or degree of certainty to each category. The degree of membership specifies how closely a value matches the idealized description of that category.
3. Collect the experts' judgments: to collect expert judgments it is essential to identify the experts and develop the information necessary to ask to cover the domain of the problem. Later, collect the responses, analyze them, and develop the fuzzy sets for the linguistic variables. Statistical methods can be used to analyze the responses and determine the degree of agreement or disagreement. Expert judgments play a crucial role in fuzzy logic, as they reflect the knowledge and experience of the experts in the field and ensure that the system accurately represents the problem domain.
4. Aggregate the experts' judgments: due to different experiences, backgrounds, and education levels, experts may express diversified judgments on the same subject. Accordingly, it becomes pivotal to properly aggregate the judgments coming from different experts, considering both the credibility of each expert and the overall consensus. The SAM allows for aggregating experts' opinions, considering both individual credibility and overall consensus levels. Recently, a proposed an improved SAM, less sensitive to a user-defined parameter than the original SAM, and able to consider experts' weights during the calculation of the degree of consensus (Guo et al., 2021). For this reason, this paper adopts the SAM (Almeida et al., 2023; Azadeh et al., 2014; Soltanali et al., 2021), considering an improved version of the former approach (Guo et al., 2021), summarized hereafter.

Given two trapezoidal fuzzy numbers $\widetilde{A} = (a_1, a_2, a_3, a_4)$ and $\widetilde{B} = (b_1, b_2, b_3, b_4)$ arising from two distinct experts (E_a and E_b), the similarity or Agreement Degree (SD) can be estimated through Eq. (1).

$$SD(\widetilde{A}, \widetilde{B}) = 1 - \frac{1}{4} * \sum_{i=1}^{4} |a_i - b_i| \tag{1}$$

where the greater $SD\left(\check{A}, \check{B}\right)$, the more similar the judgments of the two experts and vice versa. The next step of aggregation requires calculating the Weighted Absolute Agreement (WAA) of each expert according to Eq. (2).

$$WAA(E_i) = \frac{\sum_{j=1, j\neq i}^{n} W(E_j) SD(\widetilde{A}_i, \widetilde{A}_j)}{\sum_{j=1, j\neq i}^{n} W(E_j)} \tag{2}$$

where n identifies the number of experts, while $W(E_j)$ denotes the weight associated with the j-th expert. The weight can be estimated as shown in Eq. (3).

$$W(E_i) = \frac{Score_i}{\sum_{j=1}^{n} Score_j} \tag{3}$$

where $Score_j$ is the total score related to the j-th expert, computed as the sum of the score obtained by the j-th expert on different categories (e.g., education, age, experience, etc…). After estimating the WAA for each expert, the Relative Agreement (RA) and the Consensus Coefficient (CC) are calculated in Eq. (4) and Eq. (5) respectively.

$$RA(E_i) = \frac{WAA(E_i)}{\sum_{j=1}^{n} WAA(E_j)} \tag{4}$$

$$CC(E_i) = \beta W(E_i) + (1 - \beta) RA(E_i) \tag{5}$$

where $\in [0, 1]$, and it is named the relaxation factor. Next, the aggregated fuzzy number can be obtained through Eq. (6).

$$\begin{aligned} \widetilde{A}_{agg} &= CC(E_1) * \widetilde{A}_1 + CC(E_2) * \widetilde{A}_2 + \ldots + CC(E_n) * \widetilde{A}_n \\ &= (a_{agg1}, a_{agg2}, a_{agg3}, a_{agg4}) \end{aligned} \tag{6}$$

Finally, the defuzzification is conducted according to Eq. (7) (Allahviranloo and Saneifard, 2012).

$$D\widetilde{A}_i = \frac{1}{3}\left(a_{agg1} + a_{agg2} + a_{agg3} + a_{agg4} - \frac{a_{agg4}a_{agg3} - a_{agg1}a_{agg2}}{\left(a_{agg4} + a_{agg3}\right) - \left(a_{agg1} + a_{agg2}\right)}\right) \tag{7}$$

where $D\widetilde{A}_i$ refers to the defuzzied number.

Within this context, it is worth mentioning that a triangular fuzzy number can be treated as a trapezoidal fuzzy number where $a_2 = a_3$.

5. Estimate the Priority Number (PN): a PN is a value assigned to each rule, evaluation, or variable to indicate its level of importance or relevance in the study. Therefore, the number is used to resolve conflicts that arise when multiple evaluations or opinions apply to a given input value, and higher priority rules are given more weight in the decision-making process. Indeed, it is fundamental to define an indicator based on which system components can be ranked. The aforementioned PN bears similarities to the well-known risk priority number used in Failure Modes, Effects, and Criticality Analysis. However, the present study focuses on unsafe CAs rather than failure modes. Thus, a different name is chosen for the priority indicator to prevent any confusion or misunderstanding.
6. Define the priority and the criticalities: based on the PN associated with each variable or evaluation, it is possible to rank them and define appropriate thresholds. It is pivotal to identify the critical path or element in the system, otherwise, to prioritize a zone or section in the process.

2.3. System-Theoretic Process Analysis (STPA) technique supported by aggregated fuzzy experts' opinions

A graphical representation of the developed methodology is shown in Fig. 1, which shows how FST is integrated with the STPA technique for evaluating and prioritizing UCAs (black arrows in Fig. 1). First, S1 and F1 have been combined to define the problem and identify the boundaries of the systems. Later, the fuzzy scales are defined (F2 in Fig. 1). Then, the information is gathered to build the control structure and collect expert opinions (S2 & F3 in Fig. 1). Next, the opinions arising from different experts are aggregated, and a priority number is estimated for each action (F4 and f5 in Fig. 1). Therefore, the methodology identifies the UCAs, the causal scenarios, and the criticalities of the system (S3, S4 & F6 in Fig. 1). In Fig. 1, the steps to perform an STPA are represented in blue rectangles, while the steps related to FST are reported in red rectangles.

Initially, the methodology follows the first step to perform the STPA technique (S1) and FST (F1) by defining the purpose of the analysis and the system to study. Later, the research plans to define and identify the fuzzy scale to evaluate and rank the criticalities of the systems (F2). Next, a collection of information and data is required to build the SCS according to the STAMP principles (S2). Accordingly, the CAs and related FBs are identified for the different levels of the hierarchical structure, along with studying the interactions among the different SCS levels. On the other hand, the experts should evaluate each in terms of frequency and severity of each element. Specifically, the CAs and FBs are evaluated based on the three categories of inadequacy listed in Section 3.1 (i.e., action provided or not provided, error of timing or sequence, wrong duration).

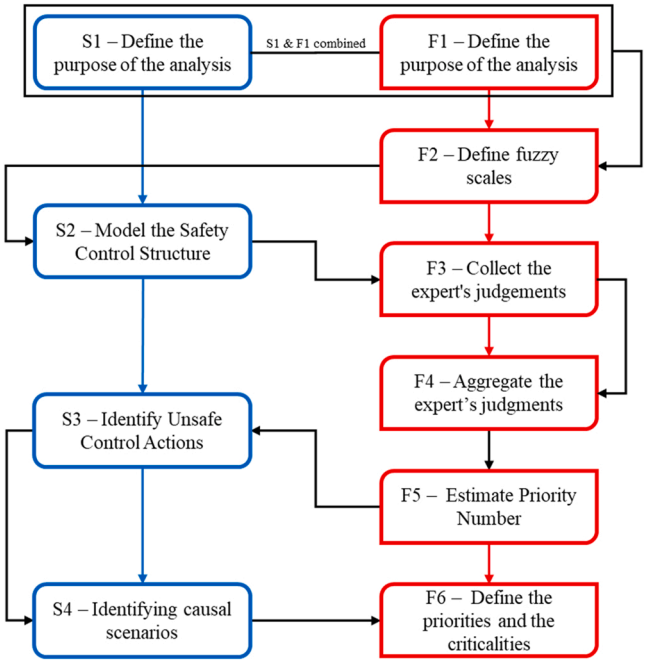

Fig. 1. Flowchart of the developed methodology.

It is at this stage that the integration of FST comes to enhance the traditional STPA. FST is indeed meant to associate with each CA and FB a PN. Thus, a fuzzy severity scale and a fuzzy occurrence scale are identified and, subsequently, shared with the subject matter experts on the system at hand. The experts are asked to specify a level of severity and occurrence for each category of inappropriate CA and FB (i.e., action provided or non-provided, error of timing or sequence, error of duration). Consequently, the judgments arising from different experts are collected (F3). This step requires an iterative process to obtain judgments as coherent as possible for each expert. For instance, the plant is characterized by different valves that have the same purpose, which is isolating parts of the gas line. Let valve A and valve B be two different valves that operate with similar gas pressure and temperature. It is possible to assume that the consequences arising from valve A not closing could be similar to the consequences caused by valve B not closing. Accordingly, a given expert should evaluate similarly the former consequences. When two particularly different opinions are expressed by the same expert for the former cases, the expert is interviewed again to clarify his judgment, and possibly correct it in case an error emerges. A similar procedure could be applied for the occurrence. The only purpose of the former process is to reduce the possibility of human error during expert elicitation. After the aggregation (F4) and defuzzification processes, a PN is obtained for each CA and FB (F5). Specifically, the PN associated with each CA and FB is estimated as the maximum PNs of the related inadequacy categories. To conclude this phase, the CAs and FBs are ranked through their PNs, effectively prioritizing the most critical Unsafe Control Actions (UCAs) or Inappropriate Control Actions (ICAs) (S3). At this stage, FST has enabled a systematic prioritization of the UCAs, and consequently, of the causal scenarios to be investigated to identify a sequence of events that describes how a particular situation or condition might lead to a loss over time. In addition, the FST allows for the prioritization of the scenarios to explore and understand the underlying causes and effects of it (S4 and F6).

In addition, it is possible to summarize the methodology in the following steps (Bingham and Ostaszewski, 2019; Falch and Silva, 2018; Yazdi et al., 2022):

- Define purpose and system (S1, F1): The analysis begins by defining the purpose of the analysis and the system under study using the STPA technique.
- Define fuzzy scales (F2): Fuzzy scales are established to evaluate and rank the criticalities of the systems, providing a basis for the subsequent analysis.
- Collect information and build SCS (S2): Information and data are collected to construct the System Constraint Structure (SCS) based on the STAMP principles. Causal Factors (CAs) and related Feedbacks (FBs) are identified at different levels of the hierarchical structure, studying their interactions.
- Expert evaluation (F3): Subject matter experts evaluate the frequency and severity of each CA and FB using the identified fuzzy severity and occurrence scales (Yazdi et al., 2019). Three categories of inadequacy are considered. The process of expert selection follows a methodical approach that involves several important steps. Firstly, it requires determining the necessary qualifications for the task at hand. Afterwards, an extensive research effort is conducted to identify potential experts who possess the desired expertise.

Thorough evaluation is then carried out, meticulously scrutinizing their expertise, background, reputation, and credibility to ensure they have a commendable standing in their respective field. Additionally, a comprehensive review is conducted to examine their relevant experience and assess their suitability for the task. The communication skills of potential experts are meticulously assessed to ensure effective conveyance of knowledge and opinions. Throughout the selection process, strict adherence to principles of independence and objectivity is maintained. Furthermore, their availability and capacity are verified to ascertain their ability to commit to the assigned responsibilities. Lastly, if necessary, multiple opinions are deliberately considered to foster a comprehensive and well-rounded analysis (Simić et al., 2017). By following these systematic steps, an expert is chosen who possesses the necessary expertise and qualifications, thereby ensuring the provision of an impartial and well-informed opinion for the purpose of analysis.

- Expert judgment collection (F4): The judgments provided by different experts regarding severity and occurrence are collected. An iterative process is employed to ensure coherence and consistency among expert judgments.
- Aggregation and defuzzification (F5): The collected judgments are aggregated and defuzzied to obtain a PN for each CA and FB. The PN represents the level of severity and occurrence. Ascertain the ranking of the PNs evaluated for each CAs and FBs, thereby prioritizing pivotal actions and scenarios.
- Ranking of CAs and FBs (S3): The CAs and FBs are ranked based on their PNs, allowing for the prioritization of Unsafe Control Actions (UCAs) or Inappropriate Control Actions (ICAs). This helps identify the most critical scenarios to investigate.
- Prioritization of scenarios (S4, F6): FST enables the systematic prioritization of UCAs and the associated causal scenarios to explore their underlying causes and effects. This helps understand how particular situations or conditions may lead to losses over time.

By implementing these strategies, the methodology endeavors to minimize subjectivity, ensuring an objective and robust analysis of system processes and potential hazards.

3. Results and analysis

The developed methodology is instantiated in an NGRMS, which holds a vital role in any Natural Gas distribution network, being the one designed to reduce the pressure of the gas flow before it can be distributed to customers.

3.1. Case study description

An NGRMS is a hazardous plant whose objective is twofold: (i) Reducing the pressure of the gas flow to adapt it to the subsequent utilities (both for industrial and public applications) and (ii) Measuring the most relevant parameters of the gas flow (e.g., upstream pressure, downstream pressure, etc.). The considered NGRMS is located in Tuscany, Italy. It has approximately a dimension of 10 m x 8 m and processes 2000 $m^3/g$of natural gas. The gas flow pressure should be reduced from 24 to 4.5 bar. This is fundamental to avoid eventual overpressure downstream of the NGRMS. As with most of the natural gas installations, the NGRMS has to follow the Italian standards and regulations related to the natural gas distribution systems.

The plant handles two hazardous substances, which are methane and tetrahydrothiophene (THT). Indeed, a precise quantity of odorizer is added to the gas flow since methane is an odorless gas. Furthermore, the plant processes water required for heating the gas flow. Any NGRMS is characterized by two or three parallel lines that work simultaneously to satisfy the gas demand and avoid interruption of the distribution. For instance, in case a maintenance intervention is required for a line, or a component of the line fails, the other lines are expected to be able to continue working. A schematic representation of the plant is shown in Fig. 2, in which the color-coded arrows represent different pressures of the process.

Following the gas flow, the first component along a line is the filter, which is in charge of removing the impurities (both solid and liquid), as they could damage the downstream devices. Next, the gas is preheated to avoid the formation of ice during the subsequent pressure reduction process. Indeed, reducing the pressure results in a temperature decrease due to the gas' law. The preheating group oversees the temperature increase of the gas flow. Specifically, a water flux is heated by a boiler, and it is sent toward the exchangers through two pumps. Then, the heated gas is sent to the pressure regulation stage, where a pressure regulator is provided. The pressure regulator could be considered the core part of the plant since it is charged with the reduction of the gas pressure. The pressure regulator maintains the downstream pressure at a pre-determined through the variation of the cross-sectional flow area. Each pressure regulator is associated with a pilot, which is adopted for faster and more precise pressure changes. After the pressure reduction, methane's most relevant parameters are measured. In this stage, the most important parameter is mass flow, which is measured through counters or meters. Finally, the odorizer is added to the gas that flows through a tank containing the THT. Based on the previous description, six main stages can be identified inside an NGRMS: filtration stage, heating stage, pressure regulation stage, measuring stage, odorization stage, and pre-heating stage (see Fig. 2). In addition to the previous stage, each line has several valves that are designed to block the gas flow in case an intervention is required on a line. For instance, in case a given pressure regulator should be replaced, the valves downstream and upstream of the pressure regulator can be closed to allow safe dismounting.

3.2. Application of the developed methodology

3.2.1. Define the purpose of the analysis

Following the first step of the methodology, this section aims to define the system, boundaries, hazards, scenarios, and losses to be investigated. By the time the system is being assessed for residual safety risk, the system hazard logs should already contain a list of the system hazards. Therefore, the following section defines the scenarios, hazards, and losses of the system.

Scenario/Mission: the scenario to be analyzed on the process is the steady state operation process of the presented NGRMS. Additionally, the systems losses are defined as certain conditions to be avoided (see Table 1), as well as the corresponding hazards (see Table 2).

3.2.2. Modeling the Safety Control Structure (SCS)

This section maps the system elements and their interactions in a STAMP SCS, adopting the controller/controlled process logic. The SCS has been divided into three different levels:

(i) High Organizational Level
(ii) Low Organizational & High Operational Level, and
(iii) Operational – Technical Level.

A High Organizational Level SCS (level i) is represented in Fig. 3 and it has been segmented into: Cabinet of Minister; Government Regulatory Office & Industries Associations; and Company Management. These three system elements constitute the authority bodies on the process and represent the organizational-business level of the system (green box in Fig. 3), they act together via regulations and laws. Hence, the enterprise organization (level ii) is made up of the following elements: Central Utilities Plant Operations; Plant Engineering office; Operators & Contractors. These elements represent the lowest organizational level and contemporarily, the highest technical-operating level of the system (blue box in Fig. 3). In addition, the plant operating system (level iii, yellow box in Fig. 3) is made up of: Central Control Room System; Control Room for NGRMS; Filtration stage; Heating stage; Pressure Regulation stage;

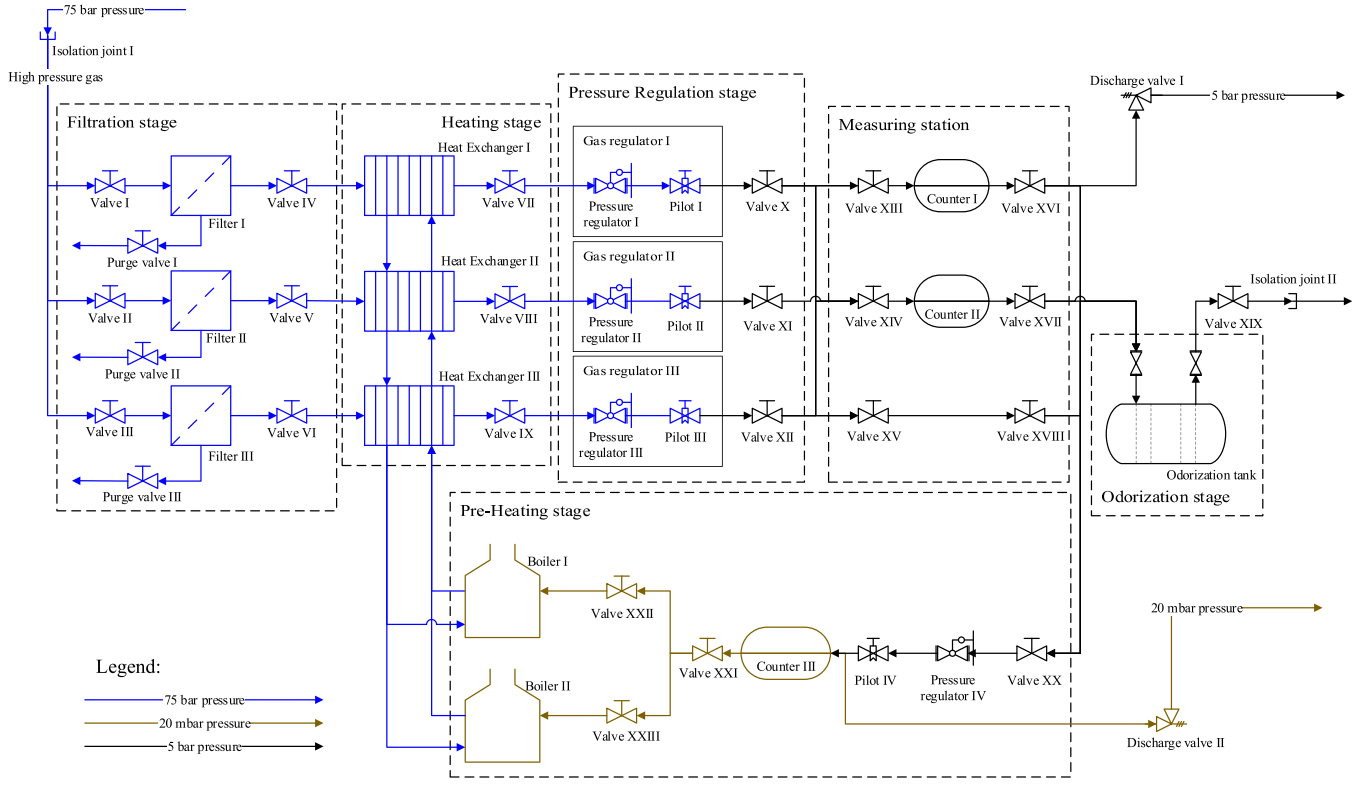

Fig. 2. Schematic representation of an NGRMS.

Table 1
System losses identified in the NGRMS.

Losses description	Loss ID
Occupational damage (fatalities or injuries)	L-01
Operational damage (to the equipment or to the plant)	L-02
Financial loss	L-03
Reputation loss	L-04
Environmental contamination	L-05
Gas supply production reduction or stop	L-06

Table 2
System hazards identified in the NGRMS.

Hazard description	Hazard ID	Linked Losses
Pressure Regulation Stage violates the safety margins	H-01	L-01; L-02; L-06
Odorization Stage does not comply with the standard	H-02	L-01; L-02; L-03; L-04; L-05; L-06
Operation condition disrupts the requirements	H-03	L-03; L-04; L-06

Measuring station; Odorization stage; Pre-Heating stage; Pipeline and Automated Control sub-systems for other NGRMS processes; Other controlled refinery processes. The case study has been highlighted in purple color in Fig. 3 (interaction between the automated control room and the stage in the NGRMS).

For the sake of the process, a more granular SCS is proposed by isolating the Control Room for NGRMS and the respective processes. This SCS excerpt is proposed in Fig. 4, in which the filtration stage, the control room for NGRMS, and the pipeline have been mapped in detail for demonstrative purposes. The fractal nature of STAMP allows indeed exploiting control loop at different levels of abstraction: this detailed SCS has been defined to highlight the CAs and FBs between the Control Algorithm and the Controlled Process, marked with a (*) in Fig. 3. The interactions have been codified to increase readability (see Table 3).

Additionally, the STAMP model has been transcribed into a task record to describe the CAs and FBs involved in Fig. 3 they will be used in the following analysis, as presented in Table 3 documented in purple arrows in Fig. 4.

These items were then used as entry points for the FST application, which was meant to prioritize the criticalities to be further investigated.

3.2.3. *Identification and evaluation of the unsafe/inappropriate actions*

As described in Section 3.2, severity and occurrence fuzzy scales need to be defined (see F1 of Fig. 1). The severity and occurrence scales along with the associated linguistic and crisp scales are shown in Table 4 and Table 5 respectively. The scales are built from previous used cases (Garcia et al., 2005; Renjith et al., 2018).

The severity and occurrence scales are shared with experts who are asked to associate with each CA and FB a level of occurrence and severity (see F2 of Fig. 1). This process is iterated to assure a higher coherence of the opinions expressed by each expert.

The plant presents similar components sharing similar CAs, and in turn, similar levels of severity and occurrence should be assigned to them. For instance, considering Valve I and Valve IV (see Fig. 2), it is possible to state that the valves are almost identical as they serve the same role (i.e., interrupting the gas flow through the filter) they operate at the same pressure. Consequently, the valves are associated with identical CAs. Based on the previous considerations, it is reasonable to assume that the same category of inadequacy for the same CA of Valve I and Valve IV should present similar, if not identical, levels of severity and occurrence. However, during the fill-in process, experts could make mistakes such as specifying an undesired or wrong level of severity or occurrence. Therefore, in case a given expert expressed a conflicting answer, the expert was asked to clarify the answers and correct them if required. For example, if an expert assigned a severity level equal to 1 and 5 for the same category of inadequacy associated with the same CA of Vale I and Valve IV, respectively, the expert was questioned once

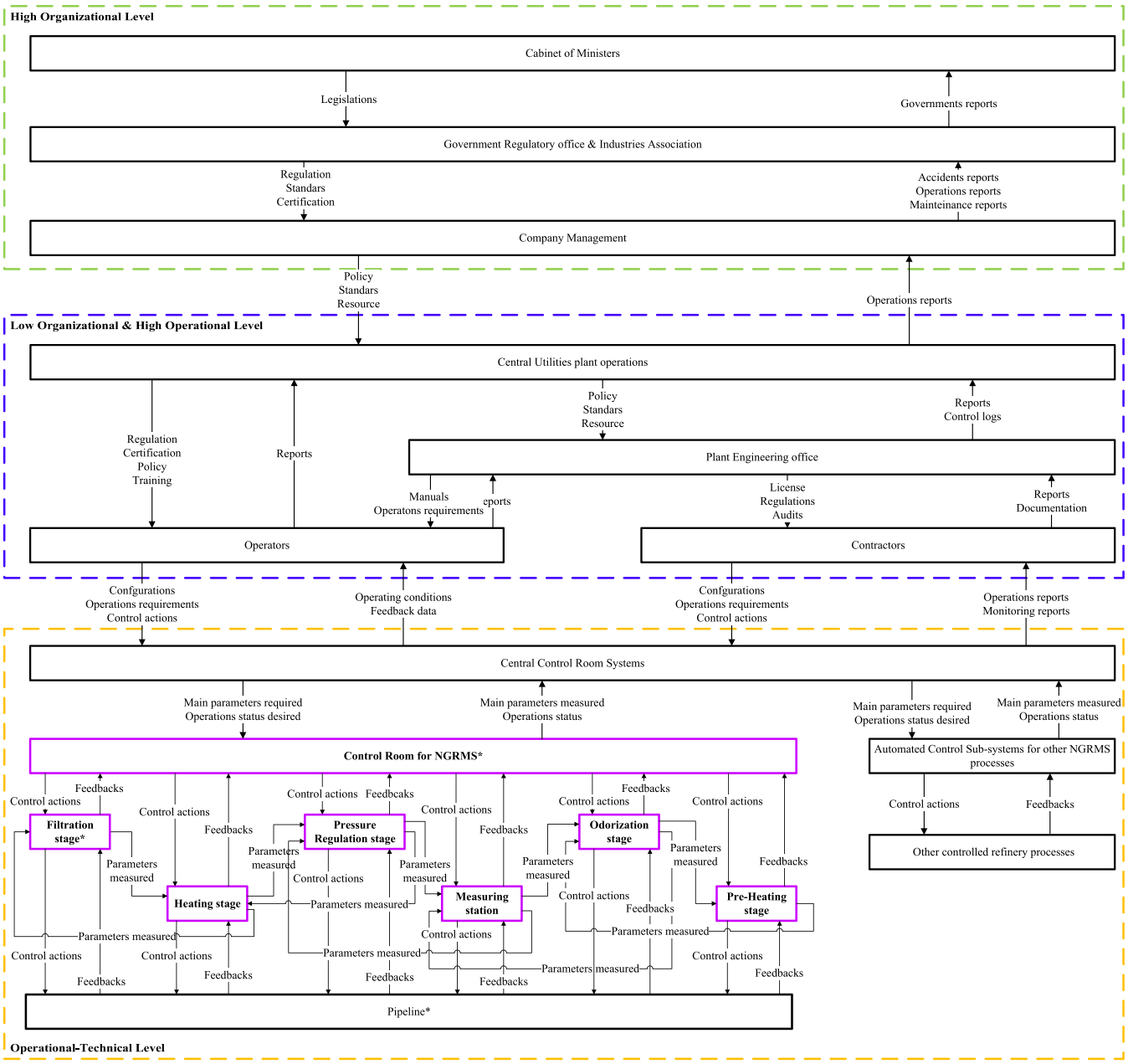

Fig. 3. High-Level Safety Control Structure for the NGRMS plant.

more to ensure higher reliability of his answers.

When the aforementioned iterative process is terminated, the judgments from different experts are aggregated through the improved SAM (see F3 of Fig. 1), adopting a relaxation factor equal to 0.5, the typical adopted value (Jianxing et al., 2021). The improved SAM requires specifying a weight for each expert. The weight of each expert is estimated based on Eq. (3), considering the criteria listed in Table 6. In this context, it is worth mentioning that the adoption of different experts, or different weighting criteria could lead to different results. However, the sensitivity analyses related to the expert selection and weighting criteria were outside of the scope of this paper.

Therefore, in this study, four experts have been involved (two of them have worked in the SMS of the NGRMS plants, instead, the other two are experts in Safety techniques in different domains), as per the corresponding weights shown in Table 7.

It is worth mentioning that the third expert preferred to not specify their judgments on the system due to the lack of information or irrelevance of the CAs. Accordingly, some CAs are characterized by three opinions instead of four, still not implying a loss of generalization or capabilities. The judgements expressed by the experts are shown in Table 8 and Table 9 for the severity and occurrence respectively.

To estimate the criticalities, the aggregation of the judgments is applied separately for the severity and occurrence levels at first as shown in Table 10. Thus, each CA is associated with three distinct aggregated severity and occurrence levels (one for each category of inadequacy).

After the defuzzification process for the occurrence and severity aggregated numbers, the PN is estimated for each category of inadequacy and each CA as the product of the aggregated severity and the aggregated occurrence (see F4 of Fig. 1). In other words, three distinct PNs are estimated for each CA (one for each category of inadequacy). Then, the maximum PN estimated for each CA is considered. The former maximum PN is exploited to identify the most critical UCAs through the adoption of the risk matrix reported in Table 11. The risk matrix also reports the traditional color-coded association. It follows that any CA

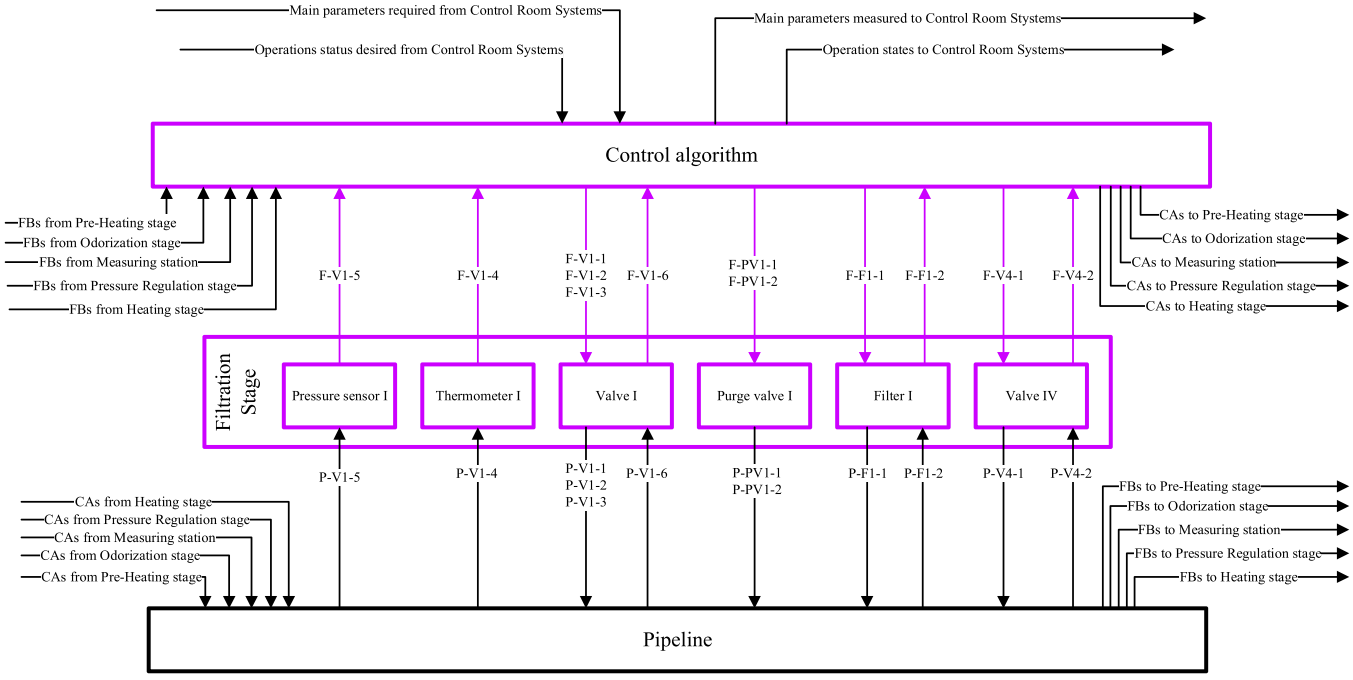

Fig. 4. A detailed SCS for the filtration stage (an excerpt of the NGRMS plant).

Table 3
The CAs and FBs description for the studied process.

Code	Task	Type
Control Room & Filtration stage (F)		
Control Room - Valve I (V1)		
F-V1–1	On/Off condition Pre-filtration	CA
F-V1–2	Pre-filtration temperature condition	CA
F-V1–3	Pre-filtration pressure condition	CA
F-T1–4	Gas temperature before filtering	FB
F-PS1–5	Gas pressure before filtering	FB
F-V1–6	Valve positioning	FB
Control Room - Filter I (F1)		
F-F1–1	Clogging control	CA
F-F1–2	Differential gas pressure upstream and downstream the filter	FB
Control Room - Valve IV (V4)		
F-V4–1	On/Off condition after filtering	CA
F-V4–2	Valve positioning	FB
Control Room - Purge Valve I (PV1)		
F-PV1–1	On/Off condition	CA
F-PV1–2	Valve positioning	FB

characterized by a maximum PN higher than 8 is associated with a high risk, while a medium risk is assigned to each CA with a maximum PN between 4 and 8. Finally, a maximum PN lower than 4 identifies a low-risk CA. The choice of the risk matrix and the former risk thresholds was guided by expert opinions. Specifically, the same experts involved in the evaluation of the CAs and FBs also in recommended the risk level of the considered risk matrix. The former choice was made to assure a good fit for the requirements of the NGRMS.

Following 11 the identified CAs and FBs for the filtration stage are classified according to the three risk levels, allowing to identify the most critical UCAs (i.e., the ones associated with high risk). The selection criteria have been defined with the higher PN number of the three criteria (action, timing or sequence, and duration) highlighted by color (previously defined in the risk matrix). Therefore, six CAs or FBs are regarded as high risk, while six are associated with a medium risk level (Table 12).

It is possible to observe how the F-V1–1, F-V4–1, and F-PV1–1 are critical since they have a high risk in terms of timing or sequence to develop the task. Moreover, the F-V1–2, F-V1–3, and F-V1–5 have a high

Table 4
Linguistic scale, descriptions, crisp values, and fuzzy numbers adopted for the severity.

Linguistic scale	Description	Crisp value	Fuzzy number
None (N)	No reason to expect failure to have any effect on safety, health, environment, or mission.	1	(0,1,2)
Minor (MI)	Minor effect on product or system performance to have any effect on safety or health. The system can require repair.	2	(1,2,3)
Moderate (MO)	Moderate effect on system performance. The system requires repair. A failure which may cause moderate injury, moderate property damage, or moderate system damage which will result in delay or loss of system availability or mission degradation.	3	(2,3,4)
Major (MA)	System performance is severely affected but functions (reduced level of safety performance). The system may not operate. Failure could involve noncompliance with government regulations or standards.	4	(3,4,5)
Serious (S)	Failure is hazardous and occurs without warning. It affects safe operation. A failure is serious enough to cause fatality or injury, property damage, or system damage. Failure will occur without warning.	5	(4,5,5)

Table 5
Linguistic scale, rate, crisp values, and fuzzy numbers adopted for the occurrence.

Linguistic scale	Rate	Crisp value	Fuzzy number
Remote (R)	< 1:20000	1	(0,1,2)
Low (L)	1:20000 or 1:10000	2	(1,2,3)
Moderate (M)	1:2000; 1:1000; or 1:200	3	(2,3,4)
High (H)	1:100 or 1:20	4	(3,4,5)
Very High (VH)	1:10 or 1:2	5	(4,5,5)

Table 6
Criteria and Score to estimate the weight of each expert (Guo et al., 2021).

Criteria	Class	Score
Professional position	Senior Manager	10
	Junior Academic / Professor	8
	Engineer / Tenure Research	6
	Technician	4
	Worker	2
Service time	≥ 30	10
	between 20 and 29	8
	between 10 and 19	6
	between 6 and 9	4
	≤ 5	2
Education level	Ph.D. Degree	10
	Master Degree	8
	Bachelor Degree	6
	Higher National Diploma	4
	School Degree	2
Age	≥ 50	8
	between 40 and 49	6
	between 30 and 39	4
	< 30	2

risk in terms of how the task has been developed. On the other hand, the rest of the CAs and FBs had a medium risk related to the timing or the action of the task.

Therefore, it is worth noting that most of the critical CAs and FBs are related to opening and closing the valves. Indeed, the valves are charged with interrupting the gas flow in case it is required to operate on a certain line. Thus, if the gas flow is not interrupted when required, it could lead to catastrophic consequences. The considered CAs refer to a single line, however, the results could be extended to any of the three lines inside an NGRMS.

3.2.4. *Identify the causal scenarios and prioritize the critical path*

This section of the analysis has been performed using the last two steps of the STPA technique (S3 and S4 in Fig. 1). Therefore, the analysis seeks to describe a set of conditions in which the CAs and FBs with the higher PN number could lead to a loss. Table 13 describes a systematic way to describe the causal scenarios to be used to improve the system design through new safety constraints. In addition, the table shows two types of indents (i) the first one (•) is linked with the CAs in charge to change the position of the valve to close or open them; and (ii) the other

Table 7
Weight score of each expert to evaluate the UCAs of the system.

Expert	Professional position	Service time	Education level	Age	Weight
E1	Junior Academic / Professor	20–29	PhD	40–49	0.333
E2	Junior Academic / Professor	10–19	PhD	30–39	0.292
E3	Engineer / Tenure Research	≤ 5	MSc	< 30	0.188
E4	Engineer / Tenure Research	≤ 5	MSc	< 30	0.188

Table 8
Opinions judgments expressed by the experts for the severity.

CAs & FBs	Criteria	Opinions by Expert			
		E1	E2	E3	E4
F-V1–1: On/Off condition Pre-filtration	Action	5	5	5	5
	Timing or Sequence	5	3	4	5
	Duration	4	3	4	5
F-V1–2: Pre-filtration temperature condition	Action	3	4	4	3
	Timing or Sequence	2	4	2	1
	Duration	2	3	3	1
F-V1–3: Pre-filtration pressure condition	Action	3	4	5	3
	Timing or Sequence	2	4	3	3
	Duration	2	4	4	2
F-V1–4: Gas temperature Pre-filtration	Action	1	4	3	2
	Timing or Sequence	1	2	2	1
	Duration	1	3	2	1
F-V1–5: Gas pressure Pre-filtration	Action	1	5	5	3
	Timing or Sequence	1	3	4	3
	Duration	1	4	4	2
F-V1–6: Valve position	Action	1	-	4	4
	Timing or Sequence	1	-	2	3
	Duration	1	-	2	3
F-F1–1: Clogging control	Action	3	-	4	3
	Timing or Sequence	2	-	2	1
	Duration	1	-	3	2
F-F1–2: Differential gas pressure upstream and downstream the filter	Action	1	4	3	2
	Timing or Sequence	1	2	1	1
	Duration	1	1	1	2
F-V4–1: On/Off condition after filtering	Action	5	5	5	5
	Timing or Sequence	5	3	4	5
	Duration	4	3	4	5
F-V4–2: Valve position	Action	1	2	4	4
	Timing or Sequence	1	1	2	3
	Duration	1	1	2	3
F-PV1–1: On/Off condition	Action	3	-	3	4
	Timing or Sequence	4	-	4	3
	Duration	4	-	2	3
F-PV1–2: Valve position	Action	1	-	3	4
	Timing or Sequence	1	-	4	3
	Duration	1	-	2	3

Table 9
Opinions judgments expressed by the experts for the occurrence.

CAs & FBs	Criteria	Expert opinion			
		E1	E2	E3	E4
F-V1–1: On/Off condition Pre-filtration	Action	2	2	1	2
	Timing or Sequence	3	1	2	3
	Duration	3	2	1	3
F-V1–2: Pre-filtration temperature condition	Action	4	3	2	2
	Timing or Sequence	4	3	3	3
	Duration	4	2	2	3
F-V1–3: Pre-filtration pressure condition	Action	4	2	3	2
	Timing or Sequence	4	3	2	3
	Duration	4	3	2	3
F-V1–4: Gas temperature Pre-filtration	Action	2	2	3	3
	Timing or Sequence	2	1	2	3
	Duration	2	1	1	3
F-V1–5: Gas pressure Pre-filtration	Action	2	3	3	4
	Timing or Sequence	2	2	3	4
	Duration	2	3	2	4
F-V1–6: Valve position	Action	2	-	2	2
	Timing or Sequence	2	-	1	2
	Duration	2	-	1	2
F-F1–1: Clogging control	Action	2	-	2	2
	Timing or Sequence	3	-	2	3
	Duration	3	-	2	3
F-F1–2: Differential gas pressure upstream and downstream the filter	Action	2	1	2	4
	Timing or Sequence	2	2	2	4
	Duration	2	2	1	4
F-V4–1: On/Off condition after filtering	Action	2	2	1	2
	Timing or Sequence	3	1	2	3
	Duration	3	2	1	3
F-V4–2: Valve position	Action	2	1	2	2
	Timing or Sequence	2	2	3	2
	Duration	2	1	2	2
F-PV1–1: On/Off condition	Action	2	-	3	2
	Timing or Sequence	2	-	2	3
	Duration	2	-	2	3
F-PV1–2: Valve position	Action	2	-	2	2
	Timing or Sequence	2	-	2	2
	Duration	2	-	2	2

one (-) are associated with the CAs related to change and regulate pressure and temperature of the process.

In addition, the methodology allows not only to trace the issues that occur among the interlevel but also to identify and define problems that may occur between each level (orange lines in Fig. 5), allowing to recognize the issues that arise indirectly in the other processes of the system.

Therefore, the methodology provides information on what other CAs and FBs should be critical downstream and upstream. Fig. 5, shows the path of how F-V1–1, F-V1–2, F-V1–3, F-V1–5, F-V4–1, and F-PV1–1 involve other components of the process e.g., Pipeline, Pressure Sensor I, Valve I, Purge Valve I, Valve IV and the Control Algorithm (red boxes in Fig. 5) and its interactions (red arrows in Fig. 5).

Moreover, the advantage of the system theory is the abstraction of the study. Based on this, Fig. 6 represents a high-level SCS identifying the critical path of each component and its interactions involved in the UCAs. This information is essential since it is possible to prioritize which part of the process could be relevant to improve the SMS and prevent such conditions that could lead to a loss. Therefore, the analysis gives indent into how the UCAs could be approached to reduce or prevent such undesired events, e.g., it is possible to identify and discuss at the organization level in terms of guidelines, laws, and regulations to guarantee new safety constraints to ensure that F-V1–1, F-V1–2, F-V1–3, F-V1–5, F-V4–1, and F-PV1–1 have been provided correctly. Besides, it is possible to study the company policy and the process conditions to ensure new safety constraints or update the old ones to guarantee that F-V1–1, F-V1–2, F-V1–3, F-V1–5, F-V4–1, and F-PV1–1 have been applied accurately.

It is important to note that the critical path underlined in Fig. 6 shows the hierarchically higher components of the process. This means that if the analysis wants to focus on describing each level of the STAMP model with its interactions, the critical path will be similar to Fig. 5, which describes the specific components of each phase of the process and their interactions (where the criticality of the process is highlighted in red color).

4. Discussion

4.1. Advantages and limitations

STPA technique allows users to systematically study a given system process, providing information on the interactions among different levels (e.g., operational, technical, and social). However, applying STPA often results in a long list of CAs and FBs, especially for complex systems processes. Thus, addressing all the UCAs and understanding their priorities is challenging. Furthermore, since finite resources characterize any organization, it is not possible to focus on all the CAs and FBs with the same efforts to evaluate the system hazards that could lead to a loss. The integration of STPA and FST allows associating each CA and FB with a level of priority, highlighting the most critical ones. Considering the case study, only 50% of the detected CAs are identified as critical due to a PN higher than 8. Therefore, the managers of the plant are provided with a reduced list of CAs to consider in the first place. These activities should be monitored and controlled thoroughly, and proper countermeasures should be adopted to avoid errors (e.g., extensive operator training). Besides, the former reduced list allows for wasting less time in identifying the most critical UCAs since only a reduced number of CAs could be considered at first. Finally, the proposed framework could support the decision-making processes related to asset management. The efforts and investments should be directed toward the identified most

Table 10
Aggregated fuzzy numbers for the severity and occurrence of the identified CAs and FBs.

CAs & FBs	Criteria	Severity aggregated			Occurrence aggregated		
		a	b	c	a	b	c
F-V1–1: On/Off condition Pre-filtration	Action	4.00	5.00	5.00	0.80	1.80	2.80
	Timing or Sequence	3.27	4.27	4.75	1.27	2.27	3.27
	Duration	2.95	3.95	4.74	1.32	2.32	3.32
F-V1–2: Pre-filtration temperature condition	Action	2.49	3.49	4.49	1.84	2.84	3.84
	Timing or Sequence	1.28	2.28	3.28	2.28	3.28	4.28
	Duration	1.30	2.30	3.30	1.78	2.78	3.78
F-V1–3: Pre-filtration pressure condition	Action	2.69	3.69	4.48	1.78	2.78	3.78
	Timing or Sequence	1.98	2.98	3.98	2.08	3.08	4.08
	Duration	1.97	2.97	3.97	2.08	3.08	4.08
F-V1–4: Gas temperature Pre-filtration	Action	1.46	2.46	3.46	1.43	2.43	3.43
	Timing or Sequence	0.49	1.49	2.49	0.94	1.94	2.94
	Duration	0.73	1.73	2.73	0.70	1.70	2.70
F-V1–5: Gas pressure Pre-filtration	Action	2.53	3.53	4.02	1.92	2.92	3.92
	Timing or Sequence	1.68	2.68	3.68	1.62	2.62	3.62
	Duration	1.72	2.72	3.72	1.68	2.68	3.68
F-V1–6: Valve position	Action	1.93	2.93	3.93	1.00	2.00	3.00
	Timing or Sequence	0.89	1.89	2.89	0.72	1.72	2.72
	Duration	0.89	1.89	2.89	0.72	1.72	2.72
F-F1–1: Clogging control	Action	2.29	3.29	4.29	1.00	2.00	3.00
	Timing or Sequence	0.72	1.72	2.72	1.72	2.72	3.72
	Duration	0.89	1.89	2.89	1.72	2.72	3.72
F-F1–2: Differential gas pressure upstream and downstream the filter	Action	1.46	2.46	3.46	1.11	2.11	3.11
	Timing or Sequence	0.26	1.26	2.26	1.37	2.37	3.37
	Duration	0.20	1.20	2.20	1.16	2.16	3.16
F-V4–1: On/Off condition after filtering	Action	4.00	5.00	5.00	0.80	1.80	2.80
	Timing or Sequence	3.27	4.27	4.75	1.27	2.27	3.27
	Duration	2.95	3.95	4.74	1.32	2.32	3.32
F-V4–2: Valve position	Action	1.58	2.58	3.58	0.74	1.74	2.74
	Timing or Sequence	0.62	1.62	2.62	1.20	2.20	3.20
	Duration	0.62	1.62	2.62	0.74	1.74	2.74
F-PV1–1: On/Off condition	Action	2.29	3.29	4.29	1.29	2.29	3.29
	Timing or Sequence	2.72	3.72	4.72	1.29	2.29	3.29
	Duration	2.11	3.11	4.11	1.29	2.29	3.29
F-PV1–2: Valve position	Action	1.53	2.53	3.53	1.00	2.00	3.00
	Timing or Sequence	1.53	2.53	3.53	1.00	2.00	3.00
	Duration	0.89	1.89	2.89	1.00	2.00	3.00

Table 11
Adopted risk matrix to evaluate the criticality of the CAs and FBs.

Occurrence level \ Severity level	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

Legend: High, Medium, Low

critical CAs. For the considered case study, the application of the proposed framework highlighted that the most critical CAs of the filtration stage of the NGRMS are related to valve management. It follows that particular attention should be devoted to the valve activation or closing processes. To validate the coherence of the former results, a validation workshop was conducted with the four experts involved in this study. The experts confirmed that the identified criticalities and priorities are aligned with their expectations and the considered installation. Accordingly, the methodology provides promising results for the considered case study.

It is worth mentioning that the application of the improved SAM allows for conducting quantitative analysis based on expert judgments, enhancing the qualitative nature of the STPA. However, the improved SAM is characterized by a user-defined parameter (i.e., the relaxation factor), whose choice could affect the results. Thus, during the following section, a sensitivity analysis is conducted to assess the impact of the relaxation factor on the detected critical CAs.

In addition, the STPA technique, before defining the system hazards and losses at the beginning of the analysis, does not consider the possibility that additional hazards or losses may appear in a second phase or evaluation of the analysis. Then, suppose any new hazard or loss is uncovered in the analysis. In that case, it is necessary to report them as part of the assessment's findings and raise them to management as quickly as possible to upgrade the safety management system of the process. Otherwise, the new hazards or losses in the analysis must be notified and updated to cover them and avoid such situations. Accordingly, the developed methodology should be applied once again to update the PNs and the priorities, based on which the decision-making to modify the system process to reduce or prevent undesired conditions should be conducted. Hence, the proposed methodology could be iterative in which after the evaluation the PN and the identification of the criticalities of the system the STPA analysis could be reapplied to prevent or improve the criticalities of the system identified previously.

4.2. Sensitivity analysis

It is pivotal to understand how the relaxation factor influences the analysis. Indeed, the relaxation factor is a user-defined parameter, and different values of the relaxation factor could lead to distinct critical CAs. Thus, it is important to identify eventual differences in criticalities arising from the variation of the relaxation factor. Indeed, new critical aspects could emerge. To this end, the aggregation method is carried out two more times, adopting a relaxation factor equal to 0 and 1 respectively. According to Eq. (5, a) relaxation factor (β) equal to 0 implies a higher impact of the experts' consensus. On the other hand, imposing a relaxation factor equal to 1 generates a higher impact of the experts' weights. To assess the differences among the PNs obtained through the adoption of three distinct relaxation factors (i.e., 0, 0.5, and 1), a Ratio of Variation (ROV) is estimated as shown in Eq. (8).

Table 12
Risk evaluation of the CAs and FBs for the filtration stage, the highest PN are mapped with bold font in the corresponding criterion.

Task description and its aspects	Type	Criterion	PN
F-V1-1: On/Off condition Pre-filtration	CA	Action	8.384
		Timing or Sequence	9.278
		Duration	9.009
F-V1-2: Pre-filtration temperature condition	CA	**Action**	9.907
		Timing or Sequence	7.466
		Duration	6.384
F-V1-3: Pre-filtration pressure condition	CA	**Action**	10.051
		Timing or Sequence	9.164
		Duration	9.153
F-V1-4: Gas temperature before filtering	FB	**Action**	5.992
		Timing or Sequence	2.895
		Duration	2.950
F-V1-5: Gas pressure before filtering	FB	**Action**	9.812
		Timing or Sequence	7.007
		Duration	7.297
F-V1-6: Valve position	FB	**Action**	5.859
		Timing or Sequence	3.246
		Duration	3.246
F-F1-1: Clogging control	CA	**Action**	6.576
		Timing or Sequence	4.663
		Duration	5.139
F-F1-2: Differential gas pressure upstream and downstream the filter	FB	**Action**	5.189
		Timing or Sequence	2.981
		Duration	2.602
F-V4-1: On/Off condition after filtering	CA	Action	8.384
		Timing or Sequence	9.278
		Duration	9.009
F-V4-2: Valve position	FB	**Action**	4.500
		Timing or Sequence	3.562
		Duration	2.816
F-PV1-1: On/Off condition	CA	Action	7.511
		Timing or Sequence	8.497
		Duration	7.111
F-PV1-2: Valve position	FB	**Action**	5.063
		Timing or Sequence	5.063
		Duration	3.785

$$ROV = \frac{\left|PN_{0.5} - PN_{0|1}\right|}{PN_{0.5}} \tag{8}$$

where $PN_{0.5}$ represents the PN estimated with a relaxation factor equal to 0.5, while $PN_{0|1}$ is computed for a relaxation factor equal to 0 and 1. Considering the CAs and FBs listed in 3, the results of the calculation are shown in Table 14. On the other hand, Fig. 7 provides a graphical representation of the values listed in Table 14.

The calculation depicted that the CAs or FBs whose PN is most affected by the relaxation factor choice are the following ones: F-V1–5 and F-V1–6. Specifically, adopting a relaxation factor equal to 0 leads to an increase in the PNs associated with F-V1–5 and F-V1–6. On the other hand, F-F1–1 and F-PV1–1 are the least affected by the relaxation factor variation. Considering F-V1–5 and F-V1–6, the first expert expressed low values of severity, while the other experts provided more similar and higher severity levels. Moreover, the first expert is associated with the highest weight, thus its judgment is predominant when the relaxation factor is equal to 1. Following the previous considerations, lower PNs are assigned to both F-V1–5 and F-V1–6 when the relaxation factor is equal to 1 due to the low severity values provided by the first expert and his importance. On the other hand, the opinions related to the occurrence and severity of F-F1–1 and F-PV1–1 are very similar across the three experts. For this reason, their PNs are slightly influenced by the relaxation factor choice.

In the former context, it is worth mentioning that the CAs and FBs formerly associated with a high-risk level are still identified as such for both the alternative relaxation factor. Accordingly, for this application, the detected criticalities are not much affected by the aforementioned user-defined parameter. Indeed, F-V1–1, F-V4–1, and F-PV1–1, with PNs higher than 8 for all the adopted relaxation factors. The former tasks are all related to valve management. Since opening and closing the valve is a manual task conducted by operators, there could be errors related to the sequence, timing, or even the absence of action when required. Thus, to avoid possible errors from occurring it is required to properly train the operators, while providing appropriate standards and procedures. Moreover, it could be useful to reduce the number of tasks a given operator should conduct in the plant. Indeed, the higher number of tasks, the higher the fatigue of the operators, which could be more prone to errors. Besides, F-V1–2, F-V1–3, and F-V1–5 emerged as critical for all three relaxation factors. F-V1–2, F-V1–3, and F-V1–5 are activities performed by specific sensors when the gas enters the plant. Accordingly, the parameters of the gas flow at the inlet of the installation are pivotal.

Table 13
Identification of the causal scenarios for the critical CAs and FBs.

Identify why would UCAs occur	Unsafe Controller Behavior	• *For F-V1–1, F-V4–1, and F-PV1–1*: The operator forgets to close or open valve I, IV, or purge valve I due to distractions, fatigue, or last-minute issues in a different area of the plant. - *For F-V1–2, F-V1–3, and F-V1–5:* The operator misreads wrong the valve I and the pressure sensor I due to distractions or fatigue.
	Inadequate Feedback or Data Information	• *For F-V1–1, F-V4–1, and F-PV1–1*: The operator forgets or makes a mistake to close or open valve I, IV, or purge valve I due to a misread of the temperature on thermometer I or pressure in pressure sensor I. This could also be related to broken or de-calibrated sensors that indicate a wrong measurement. - *For F-V1–2, F-V1–3, and F-V1–5:* The operator makes a mistake or conducts a wrong task because pressure sensor I indicates the wrong measure. Moreover, this measure could be read in the automated control room or in the pipeline both ways are electronic components in which the data information or feedback of the process could be wrong due to external factors or de-calibration of the instruments.
Identify why would CA(s) be improperly executed / not executed	Control Path	• *For F-V1–1, F-V4–1, and F-PV1–1*: The STPA technique provides information on the interlevel (down and upstream) of the CAs and FBs affected by the UCAs. Therefore, P-V1–1, P-V4–1, and P-FV1–1 (valve positioning angle for valve I, IV, and purge valve I) are involved in the actions that could lead to an unsafe or inappropriate scenario since they stop or allow the flow of the gas. - *For F-V1–2, F-V1–3, and F-V1–5:* On the other hand, for the other UCAs the P-V1–2, P-V1–3, and P-V1–5 (pre and post-filtration gas pressure) are involved in the actions that could lead and inappropriate reading and interpretation of the gas pressure in the process.
	Controlled Process Factors	• *For F-V1–1, F-V4–1, and F-PV1–1*: the pipeline and filter I are the controlled processes involved in these causal scenarios. In addition, the inappropriate development of these CAs leads to a sudden change in pressure or an abrupt decrease in temperature, the piping could start to freeze, causing problems in plant mobility and process control. - *For F-V1–2, F-V1–3, and F-V1–5:* the pipeline and filter I are the controlled processes involved in these causal scenarios. In addition, the inappropriate development of these CAs leads to a sudden change in pressure or an abrupt decrease in temperature, the piping could start to freeze, causing problems in plant mobility and process control.

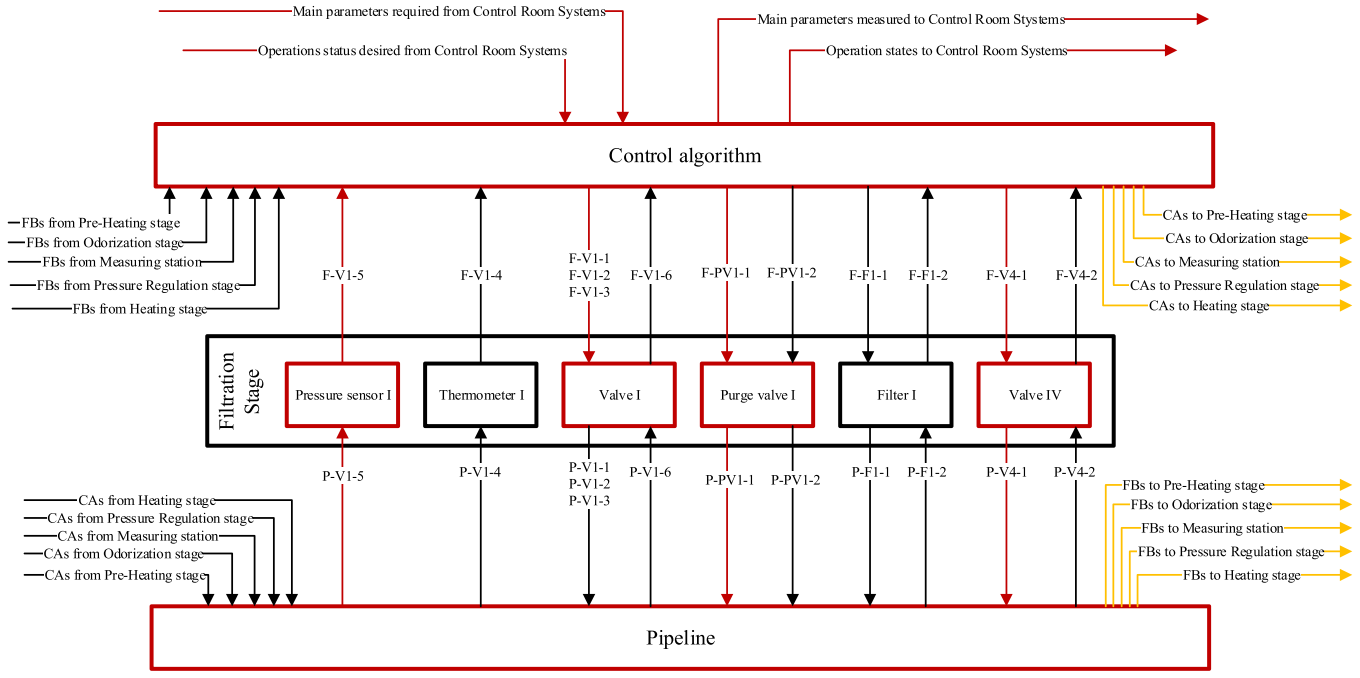

Fig. 5. Critical system components for the filtration stage of the NGRMS (orange lines are the problems related with the system components arise indirectly. On the other hand, the red elements show the critical path of the system).

Furthermore, to avoid possible errors or even the absence of measurements, it is essential to adopt very reliable and precise sensors. Indeed, sensors with high reliability and precision could reduce the occurrence of non-proper measurements.

5. Conclusion

Using the STPA technique in combination with the FST method has been proven effective in identifying and prioritizing the CAs and FBs involved in the related system process hazards (Leoni, De Carlo et al., 2021). In addition, the STPA technique allowed a comprehensive analysis of the system and its potential losses. At the same time, the FST method provided a flexible and adaptable framework for assessing the occurrence and severity of each CAs and FBs to be ranked to facilitate the selection of the hazard to be mitigated in the future. This paper provides detailed guidance on integrating an STPA and FST method to quantify each interaction. The obtained results demonstrate the feasibility of the proposed methodological solution to assess and identify the criticalities of the system. Based on this analysis, managers could develop and implement appropriate mitigation strategies and new safety constraints to prevent or reduce future undesired events (Nakhal A, Gravio et al., 2022). Expert opinion may also complement the estimated PNs to validate or improve the prioritization process (Dorsey et al., 2020; Garg and Mhaskar, 2018). For instance, a validation workshop was adopted in this

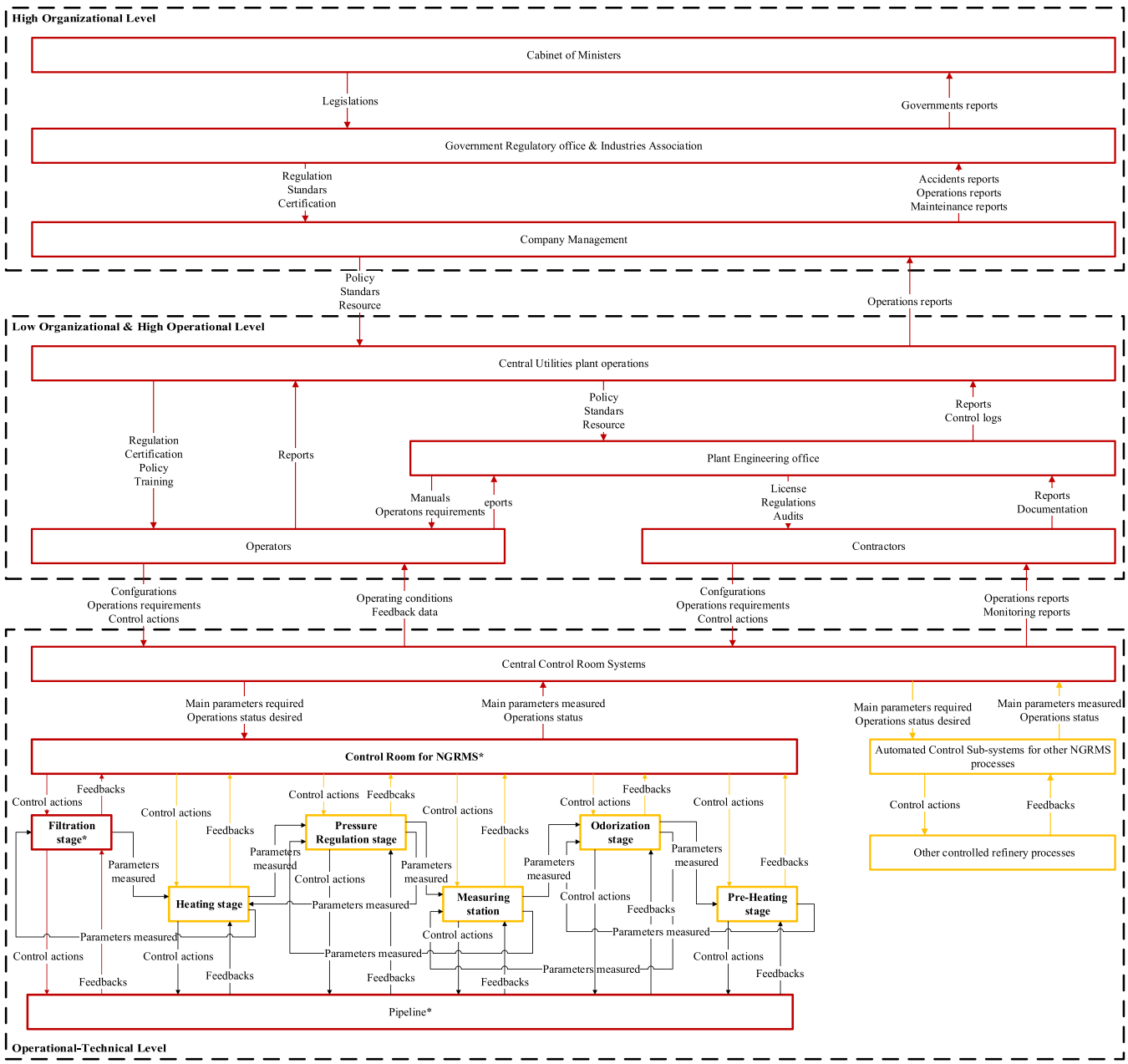

Fig. 6. A high-level SCS of the critical path of how UCAs could affect the entire system process.

Table 14
PNs and ROVs associated with the high risk CAs and FBs for a relaxation factor equal to 0 and 1.

CAs and FBs	PN		ROV	
	Beta = 0	Beta = 1	Beta= 0	Beta= 1
F-V1–1	9.52	9.04	0.03	0.03
F-V1–2	9.52	10.29	0.04	0.04
F-V1–3	9.81	10.29	0.02	0.02
F-V1–4	6.20	5.79	0.03	0.03
F-V1–5	10.72	8.94	0.09	0.09
F-V1–6	6.53	5.19	0.11	0.11
F-F1–1	6.61	6.54	0.01	0.01
F-F1–2	5.30	5.08	0.02	0.02
F-V4–1	9.52	9.04	0.03	0.03
F-V4–2	4.88	4.13	0.09	0.08
F-PV1–1	8.52	8.48	0.002	0.002
F-PV1–2	5.47	4.66	0.08	0.08

study.

As for most of the works, this study has some limitations. For instance, only the operative level (micro-perspective) was considered in this analysis. In this regard, further research may include considering the fractal nature of resilience and exploring more dimensions: (i) micro-perspective referring to the study of single components (technical or human); (ii) meso-perspective, considering the whole organization, and (iii) macro-perspective to extend impacts evaluation also considering society involvement. To perform the former task, it is required to provide more details regarding CAs and FBs related to meso-perspective and macro-perspective. Subsequently, a first viable option could be evaluating the severity and occurrence of each CA and FB through expert judgements as described in this paper. Another viable option could be considering the critical CAs and FBs detected for the micro-level. Next, it could be possible to study and define their relationships and impacts on meso-perspective and macro-perspective. In other words, a bottom-up approach could be followed to detect meso-perspective or macro-

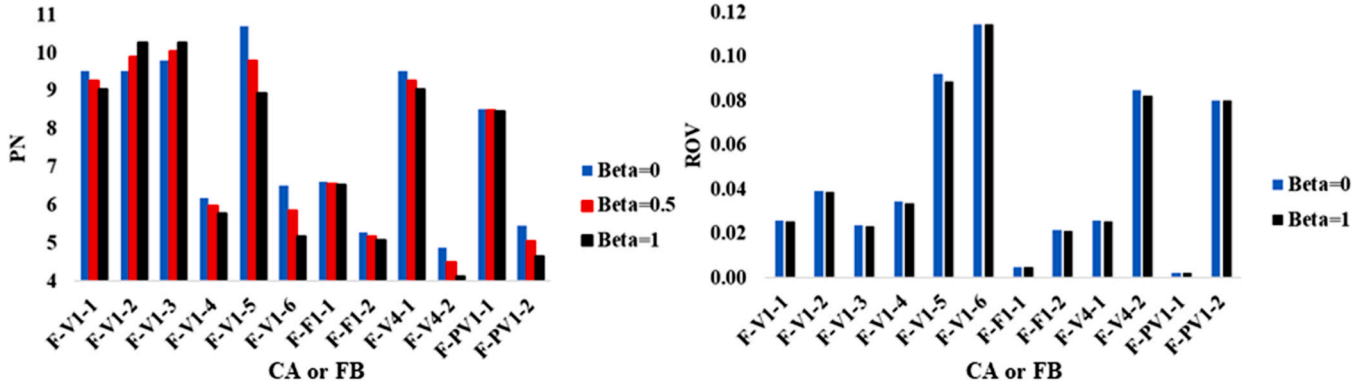

Fig. 7. Left) PN obtained with a relaxation factor equal to 0 and 1. In addition, (right) ROV associated with the CAs and FBs of the filtration stage.

perspective criticalities. Adopting the aforementioned solutions could allow to have a more comprehensive view on safety matters, allowing to conduct a more informative decision-making process related to possible countermeasures.

Besides, triangular fuzzy numbers have been considered. Thus, it could be interesting to extend the framework for hesitant or intuitionistic fuzzy numbers, which are usually more suited for treating the uncertainty arising from expert opinions. In this context, it is worth mentioning that different experts, different opinions, or different weighting criteria could lead to different results. Accordingly, it could be useful to investigate the impacts that different expert groups and weight criteria have on the criticalities.

Moreover, only a single case study is considered. Thus, it could be interesting to apply the proposed framework to different contexts such as manufacturing, transportation, and aerospace. Indeed, extending the methodology to other fields of application could be useful to evaluate its generalizability, along with identifying its weaknesses and strengths more in-depth. In this context, it is worth mentioning that FST has been successfully integrated with other tools in several fields. Thus, it is possible to expect a similar capability for the integration of FST and STAMP.

Furthermore, in this work, the comparison of the methodology with similar frameworks was outside of the scope. Thus, a future development could be integrating FST with other techniques to map and assess hazards such as the Functional Resonance Analysis Method (FRAM) (Hollnagel, 2012). The FRAM has been advocated as a systemic approach useful to understand and analyse complex socio-technical systems and their resilience, with specific focus on functional interactions being useful for detailed mapping of actual system interdependencies under varying conditions (Patriarca et al., 2020). When integrated with FRAM, FST allows for the modeling and propagation of uncertainties, providing a more comprehensive understanding of system dynamics and potential hazards. By leveraging FST, there is a possibility to offer valuable support by addressing uncertainties and imprecisions in system parameters. FST enables the representation and reasoning of imprecise and incomplete information, leading to more realistic assessments and improved decision-making for risk mitigation strategies (Lundberg et al., 2008). Then, a comparison could be conducted to address the advantages and the limitations arising from the different integration frameworks. This structured analysis should improve the quality of the data gathering using Machine Learning (ML) algorithms such as Deep Learning or Decision Tree complemented with some ML data analysis in safety domains (Nakhal A et al., 2021; Nakhal A, Hovstad et al., 2022). Finally, another future development of this research could be the reinforcement of the current framework with the implementation of the BN (Leoni, BahooToroody et al., 2021; Leoni et al., 2019) supported by FST to evaluate the probabilities of the critical CAs and FBs identified through the frameworks.

References

Abdulkhaleq, A., Wagner, S., Leveson, N., 2015. A comprehensive safety engineering approach for software-intensive systems based on STPA. Procedia Eng. 128, 2–11. https://doi.org/10.1016/j.proeng.2015.11.498.

Adriaensen, A., Costantino, F., Di Gravio, G., Patriarca, R., 2022. Teaming with industrial cobots: a socio-technical perspective on safety analysis. Hum. Factors Ergon. Manuf. Serv. Ind. 32 (2), 173–198.

Allahviranloo, T., Saneifard, R., 2012. Defuzzification method for ranking fuzzy numbers based on center of gravity. *J. Fuzzy Syst.* Vol. 9 (Issue 6) (www.SID.ir).

Almeida, R.S., Vasconcelos da Silva, F., Vianna, S.S.V., 2023. Combining the bow-tie method and fuzzy logic using Mamdani inference model. Process Saf. Environ. Prot. 169, 159–168. https://doi.org/10.1016/J.PSEP.2022.11.005.

Azadeh, A., Salehi, V., Arvan, M., Dolatkhah, M., 2014. Assessment of resilience engineering factors in high-risk environments by fuzzy cognitive maps: a petrochemical plant. Saf. Sci. 68, 99–107. https://doi.org/10.1016/j.ssci.2014.03.004.

Bingham, N.H., Ostaszewski, A.J., 2019. Set theory and the analyst. Eur. J. Math. 5 (1), 2–48. https://doi.org/10.1007/s40879-018-0278-1.

Ceylan, B.O., Akyuz, E., Arslanoğlu, Y., 2022. Modified quantitative systems theoretic accident model and processes (STAMP) analysis: a catastrophic ship engine failure case. Ocean Eng. *253*. https://doi.org/10.1016/j.oceaneng.2022.111187.

Chaal, M., Valdez Banda, O.A., Glomsrud, J.A., Basnet, S., Hirdaris, S., Kujala, P., 2020. A framework to model the STPA hierarchical control structure of an autonomous ship. Saf. Sci. *132*. https://doi.org/10.1016/j.ssci.2020.104939.

Chen, C.T., Lin, C.T., Huang, S.F., 2006. A fuzzy approach for supplier evaluation and selection in supply chain management. Int. J. Prod. Econ. 102 (2), 289–301. https://doi.org/10.1016/j.ijpe.2005.03.009.

Dekker, S., 2019. *Foundations of Safety Science: A Century of Understanding Accidents and Disasters* (First). CRC Press,.

Dorsey, L.C., Wang, B., Grabowski, M., Merrick, J., Harrald, J.R., 2020. Self healing databases for predictive risk analytics in safety-critical systems. J. Loss Prev. Process Ind. *63*. https://doi.org/10.1016/j.jlp.2019.104014.

Dutta Majumder, D., Majumdar, K.K., 2004. Complexity analysis, uncertainty management and fuzzy dynamical systems: a cybernetic approach. Kybernetes 33 (7), 1143–1184. https://doi.org/10.1108/03684920410534489.

Elmaraghy, W., Elmaraghy, H., Tomiyama, T., Monostori, L., 2012. Complexity in engineering design and manufacturing. CIRP Ann. - Manuf. Technol. 61 (2), 793–814. https://doi.org/10.1016/j.cirp.2012.05.001.

Falch, L., & Silva, C. (2018). Fuzzy Techniques to Reduce Subjectivity and Combine Qualitative and Quantitative Criteria in a Multi-objective Design Problem. IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON).

Garcia, P.A.A., Schirru, R., Frutuoso e Melo, P.F., 2005. A fuzzy data envelopment analysis approach for FMEA. Prog. Nucl. Energy 46 (3–4), 359–373. https://doi.org/10.1016/j.pnucene.2005.03.016.

Garg, A., Mhaskar, P., 2018. Utilizing big data for batch process modeling and control. Comput. Chem. Eng. 119, 228–236. https://doi.org/10.1016/j.compchemeng.2018.09.013.

Gentile, M., Rogers, W.J., Mannan, M.S., 2003. Development of a fuzzy logic-based inherent safety index. Process Saf. Environ. Prot. 81 (6), 444–456. https://doi.org/10.1205/095758203770866610.

Guo, X., Ji, J., Khan, F., Ding, L., Yang, Y., 2021. Fuzzy Bayesian network based on an improved similarity aggregation method for risk assessment of storage tank accident. Process Saf. Environ. Prot. 149, 817–830. https://doi.org/10.1016/j.psep.2021.03.017.

Hollnagel, rik, 2012. FRAM: The FunctionAl Resonance Analysis Method. Ashgate.

Jianxing, Y., Shibo, W., Yang, Y., Haicheng, C., Haizhao, F., Jiahao, L., Shenwei, G., 2021. Process system failure evaluation method based on a Noisy-OR gate intuitionistic fuzzy Bayesian network in an uncertain environment. Process Saf. Environ. Prot. 150, 281–297. https://doi.org/10.1016/j.psep.2021.04.024.

Langari, R., 1996. Hierarchical approach to fuzzy logic control. Association for Computing Machinery.

Leoni, L., BahooToroody, A., De Carlo, F., Paltrinieri, N., 2019. Developing a risk-based maintenance model for a Natural Gas Regulating and Metering Station using Bayesian Network. J. Loss Prev. Process Ind. 57, 17–24. https://doi.org/10.1016/j.jlp.2018.11.003.

Leoni, L., BahooToroody, A., Abaei, M.M., De Carlo, F., Paltrinieri, N., Sgarbossa, F., 2021. On hierarchical bayesian based predictive maintenance of autonomous natural gas regulating operations. Process Saf. Environ. Prot. 147, 115–124. https://doi.org/10.1016/J.PSEP.2020.08.047.

Leoni, L., De Carlo, F., Paltrinieri, N., Sgarbossa, F., BahooToroody, A., 2021. On risk-based maintenance: A comprehensive review of three approaches to track the impact of consequence modelling for predicting maintenance actions. J. Loss Prev. Process Ind. 72 (10455) https://doi.org/10.1016/j.jlp.2021.104555.

Leveson, N., 2004. A new accident model for engineering safer systems. Saf. Sci. 42 (4), 237–270. https://doi.org/10.1016/S0925-7535(03)00047-X.

Leveson, N., 2011. Applying systems thinking to analyze and learn from events. Saf. Sci. 49 (1), 55–64. https://doi.org/10.1016/j.ssci.2009.12.021.

Leveson, N., & Thomas, J. (2018). STPA Handbook.

Leveson, N.G., 2017. Rasmussen's legacy: A paradigm change in engineering for safety. Appl. Ergon. 59, 581–591. https://doi.org/10.1016/J.APERGO.2016.01.015.

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. https://doi.org/10.1016/j.ssci.2016.10.001.

Lundberg, J., Lundblad, K., Scandpower, R., Speziali, J., Power, V., Ab, C., Woltjer, R., & Lundberg, J. (2008). FRAM as a risk assessment method for nuclear fuel transportation. https://www.researchgate.net/publication/237088893.

Markowski, A.S., Mannan, M.S., Bigoszewska, A., 2009. Fuzzy logic for process safety analysis. J. Loss Prev. Process Ind. 22 (6), 695–702. https://doi.org/10.1016/J.JLP.2008.11.011.

Milašinović, M., Ivetić, D., Stojković, M., Savić, D., 2023. Failure conditions assessment of complex water systems using fuzzy logic. Water Resour. Manag. 37 (3), 1153–1182. https://doi.org/10.1007/S11269-022-03420-W.

Nakhal A, A.J., Patriarca, R., Di Gravio, G., Antonioni, G., Paltrinieri, N., 2021. Investigating occupational and operational industrial safety data through Business Intelligence and Machine Learning. J. Loss Prev. Process Ind. *73*. https://doi.org/10.1016/j.jlp.2021.104608.

Nakhal A, A.J., Hovstad, J., Ruth, M.S., Parmeggiani, S., Patriarca, R., Paltrinieri, N., 2022. A machine learning approach to analyze natural hazards accidents scenarios. Chem. Eng. Trans. *91*. https://doi.org/10.3303/CET2291067.

Nakhal A, A.J., Gravio, G.D., Fedele, L., Patriarca, R., 2022. Learning from incidents in socio-technical systems: a systems-theoretic analysis in the railway sector. *Infrastructures*. https://doi.org/10.3390/infrastructures7070090.

Nakhal A, A.J., Patriarca, R., Tronci, M., Agnello, P., Ansaldi, S.M., Ledda, A., 2022. A STAMP model for safety analysis in industrial plants. Chem. Eng. Trans. *91*. https://doi.org/10.3303/CET2291068.

Pasman, H.J., 2009. Learning from the past and knowledge management: are we making progress. J. Loss Prev. Process Ind. 22 (6), 672–679. https://doi.org/10.1016/J.JLP.2008.07.010.

Patriarca, R., Di Gravio, G., Woltjer, R., Costantino, F., Praetorius, G., Ferreira, P., Hollnagel, E., 2020. Framing the FRAM: a literature review on the functional resonance analysis method. Saf. Sci. *129*. https://doi.org/10.1016/j.ssci.2020.104827.

Patriarca, R., Falegnami, A., Costantino, F., Di Gravio, G., De Nicola, A., Villani, M.L., 2021. WAx: An integrated conceptual framework for the analysis of cyber-socio-technical systems. Saf. Sci. *136*. https://doi.org/10.1016/j.ssci.2020.105142.

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 https://doi.org/10.1016/j.ssci.2021.105566.

Rasmussen, J., Svedung, I., 2000. Proactive risk management in a dynamic society. Swed. Rescue Serv. A Vol. 1.

Renjith, V.R., Jose kalathil, M., Kumar, P.H., Madhavan, D., 2018. Fuzzy FMECA (failure mode effect and criticality analysis) of LNG storage facility. J. Loss Prev. Process Ind. 537–547. https://doi.org/10.1016/j.jlp.2018.01.002.

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. https://doi.org/10.1177/0018720814551555.

Saurin, T.A., Werle, N.J.B., 2017. A framework for the analysis of slack in socio-technical systems. Reliab. Eng. Syst. Saf. 167, 439–451. https://doi.org/10.1016/j.ress.2017.06.023.

Simić, D., Kovačević, I., Svirčević, V., Simić, S., 2017. 50 years of fuzzy set theory and models for supplier assessment and selection: A literature review. J. Appl. Log. 24, 85–96. https://doi.org/10.1016/j.jal.2016.11.016.

Soltanali, H., Khojastehpour, M., Farinha, J.T., e Pais, J.E. de A., 2021. An integrated fuzzy fault tree model with bayesian network-based maintenance optimization of complex equipment in automotive manufacturing. Energies 14 (22). https://doi.org/10.3390/en14227758.

Yazdi, M., Kabir, S., 2017. A fuzzy Bayesian network approach for risk analysis in process industries. Process Saf. Environ. Prot. 111, 507–519. https://doi.org/10.1016/J.PSEP.2017.08.015.

Yazdi, M., Hafezi, P., Abbassi, R., 2019. A methodology for enhancing the reliability of expert system applications in probabilistic risk assessment. J. Loss Prev. Process Ind. 58, 51–59. https://doi.org/10.1016/j.jlp.2019.02.001.

Yazdi, M., Zarei, E., Adumene, S., Abbassi, R., Rahnamayiezekavat, P., 2022. Uncertainty modeling in risk assessment of digitalized process systems. *Methods in Chemical Process Safety* (Vol. 6, pp. 389–416). Elsevier. https://doi.org/10.1016/BS.MCPS.2022.04.005.

Zarei, E., Yazdi, M., Abbassi, R., Khan, F., 2019. A hybrid model for human factor analysis in process accidents: FBN-HFACS. J. Loss Prev. Process Ind. 57, 142–155. https://doi.org/10.1016/j.jlp.2018.11.015.

Zhang, H., He, X., Mitri, H., 2019. Fuzzy comprehensive evaluation of virtual reality mine safety training system. Saf. Sci. 120, 341–351. https://doi.org/10.1016/j.ssci.2019.07.009.

Zhou, Q., Thai, V.V., 2016. Fuzzy and grey theories in failure mode and effect analysis for tanker equipment failure prediction. Saf. Sci. 83, 74–79. https://doi.org/10.1016/j.ssci.2015.11.013.