IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 21 May 2024, accepted 16 June 2024, date of publication 17 July 2024, date of current version 26 July 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3429568

SURVEY

Application of Systems Theoretic Accident Model and Processes in Railway Systems: A Review

ABHIMANYU TONK[1] **AND ABDERRAOUF BOUSSIF**[2]
[1]Technological Research Institute Railenium, 59300 Valenciennes, France
[2]COSYS-ESTAS, Université Gustave Eiffel, 59650 Villeneuve d'Ascq, France

Corresponding author: Abhimanyu Tonk (abhimanyu.tonk@railenium.eu)

This work was supported in part by French Collaborative Project DRAISY funded by French Government within the Program ''Investissements d'Avenir'' and the framework of France 2030 operated by Agence De l'Environnement et de la Maîtrise de l'Énergie (ADEME).

ABSTRACT This paper provides a bibliometric analysis and literature review to explore the current application landscape of the Systems Theoretic Accident Model and Processes (STAMP) principles and techniques in the railway transportation domain. Following PRISMA guidelines, we systematically reviewed 118 research documents retrieved from prominent bibliographic databases, covering the period from 2008 to September 2023. The investigated research works, involving STAMP, mainly focus on two topics: 1) applications of STAMP to railway accident modeling/analysis and 2) applications of Systems Theoretic Process Analysis (STPA) to railway hazard analysis and risk assessment. In this paper, while the STAMP related studies are discussed with respect to the considered railway accidents, the studies related to STPA analysis are discussed with respect to three subjects, STPA applications, STPA comparative studies, and STPA extensions and improvements. Ultimately, this review aims to provide academic researchers and railway practitioners with a comprehensive exploration and analysis of the current state of knowledge on STAMP within the railway sector.

INDEX TERMS Accident analysis, hazard analysis, railway safety, STAMP, STPA.

I. INTRODUCTION

Safety engineering is an interdisciplinary field of engineering. It encompasses a multitude of activities implemented during the overall lifecycle of a (socio-)technological system. Even though there is a lack of consensus about the definition of safety amongst various industrial domains, the most accepted definition of safety is *freedom from unacceptable risk* [1]. The basic principles and the mechanics of safety engineering are collectively known as *safety science*.

The objective of safety engineering activities is to assure the safe design and deployment of the system within its operational environment. These safety-related activities are broadly classified into two categories, (*i*) proactive and (*ii*) reactive activities. The proactive activities pursue risk and safety assessments that lead to a system that is safe for use by its design. On the other hand, the reactive activities are carried out as a response to a failure of the system, incident, or accident, with the aim to prevent future ones.

Railway systems are safety-critical sociotechnical systems with high interactive complexity [2], [3], [4]. To guarantee and maintain a high level of safety, railway companies (infrastructure managers, railway undertakings, etc.) establish and implement a safety management system [5], [6], [7]. According to the European Union Agency for Railways (ERA),[1] a Safety Management System (SMS) is defined as *the organization, arrangements, and procedures established by an infrastructure manager or a railway undertaking to ensure the safe management of its operations*. The main activities on railway safety management system encompasses safety monitoring, investigation, analysis, and reporting of safety occurrences (accidents and incidents), as well as assessing and controlling the associated risks.

The scientific literature on railway safety has garnered significant attention from both academic and industrial

The associate editor coordinating the review of this manuscript and approving it for publication was Amjad Mehmood.

[1] https://www.era.europa.eu/

researchers, primarily focusing on two key topics: (*i*) accident modeling and analysis, and (*ii*) hazard analysis and risk assessment. The former plays a fundamental role in comprehending the nature of railway safety, investigating accident causation, and implementing measures for preventing future incidents [3]. The latter, on the other hand, is crucial for the design and operation of railway systems, ensuring a consistently high level of safety throughout their operation.

A. RAILWAY ACCIDENT MODELING AND ANALYSIS

Recently, a considerable number of theories, frameworks, approaches, and tools have been proposed to support accident causation modeling and analysis, enabling researchers and practitioners to understand the ''causal chains'' from different perspectives [8]. Researchers categorized accident analysis models into three categories based on their underlying assumptions: (i) *sequential* (simple linear) models, *epidemiological* (complex linear) models, and *systemic* (complex nonlinear models) [9], [10].

All these types of accident models have been exploited, to varying extents, by the railway research community. While sequential and epidemiological accident models were historically privileged, the past two decades have witnessed a significant increase in interest towards systemic models, namely, AcciMap [11], Functional Resonance Analysis Method (FRAM) [12], and System Theoretic Accident Model and Processes (STAMP) [13]. This has resulted mainly due to the inadequacy of the traditional accident modeling to explain or analyze accidents that occur in modern railway systems, such as the ones where accident causation is not the result of an individual component failure, human error, or energy-related event [13], [14]. On the other hand, accident models based on system theory have proven efficient to describe and explain unexpected, uncontrolled relationships between a system's components (technical, operational, organizational, etc.) [13], [15].

Several research works have already revisited the evolution of accident models, conducted comprehensive reviews, and categorizations of these models, and offered critical analyses of their fundamental principles and practical applications [10], [14], [15], [16], [17], [18], [19]. Among these reviews, only a few have specifically focused on railway accident causation models [8], [20], [21].

B. RAILWAY HAZARD ANALYSIS & RISK ASSESSMENT

The ultimate objective of railway risk management is to demonstrate that all identified hazards and risk associated to a proposed change, in the railway system, are suitably analyzed, evaluated and reasonably controlled [6]. This ensures that safety of the railway system is maintained at an acceptable level (*the globally or at least equivalent principle*). Hazard analysis and risk assessment is a core part of the railway safety management process specified in standard EN 50126 (IEC 62278) [1].

At railway system (or subsystem) level, the risk assessment includes risk analysis and risk evaluation. Risk analysis is derived from the system definition and includes hazard identification, consequence analysis and selection of the risk acceptance principles. This assessment reflects a reasonable analysis of hazard(s) and their associated risk(s) upon railway operations and technologies. The result of such risk assessment is a set of safety measures and requirements allocated to clearly-identified function, systems or operating rules [22] in order to eliminate, mitigate, and control clearly-specified hazards.

Whilst EN 50126 standard does not mandate a specific method for conducting the hazard analysis and risk assessment, its Annex F provides a non-exhaustive list of the approaches to be used, with a certain privilege given to Preliminary Hazard Analysis (PHA), Failure Mode and Effect Analysis (FMEA), Fault Tree Analysis (FTA), and Hazard and Operability Analysis (HAZOP) approaches. Notice that several factors have to be considered while selecting the adequate method for the analysis of a system. Moreover, each of these techniques brings its own nuances to assessment of hazards in a system [23], [24]. Thus, with increasing complexity of the railway system (through integration of new technologies, more (cyber-)interaction between the rail components, etc.), new methods shall be considered to complete and support the traditional ones in hazard analysis. In just two decades, System Theoretic Process Analysis (STPA) [25] has emerged as an efficient deductive hazard analysis, mainly when it comes to identify causal factors related to control issues and misinteractions between system components. Previously, STPA has already seen remarkable success in nuclear and aviation domains and, more recently, its applications have garnered increasing attention in the railway sector.

C. CONTRIBUTIONS AND OBJECTIVE OF THE PAPER

Recognized by both academia and industrial practitioners, STAMP (and its associated techniques) has firmly established its popularity for accident and hazard analysis. Even though the founding principles of STAMP lie in the aerospace domain, it has expanded rapidly into several other safety-critical industries, mainly nuclear, land and marine transportation, healthcare. Besides application and assessment of STAMP, researchers have also proposed to combine STAMP with other approaches and to adapt/extend it to specific contexts and domains.

The advent of STAMP methods, in the railway, is also pursuing this cross-industry trend but unfortunately it is not progressing at the same pace observed in other transportation domains. To the best of authors' knowledge there is no reviewing work or scientometric analysis specifically dedicated to the application and assessment of STAMP/STPA in railway, except [21] that reviewed STAMP as part of an overall analysis of system thinking accident methods; and thus, without analyzing its methods related to hazard analysis.

This paper provides an extensive bibliometric analysis and literature review of the research works related to the investigation of STAMP and its associated techniques in the railway domain. The review mainly focuses on the applications of STAMP to railway accident modeling and analysis, as well as, the applications of STPA to hazard analysis and risk assessment, as parts of the railway safety management. The authors sight to offer academic researchers and industrial practitioners with a holistic understanding of the current state of knowledge regarding STAMP theory and practices within railway. The prime focus remains on understanding how STAMP principles and associated techniques have been perceived, implemented, and customized to align with the specific (organizational, operational, and technical) railway context. Additionally, the aim is to critically discuss the existing works, with the intent to identify perspectives and future directions for the adoption and integration of STAMP/STPA within railway safety management processes.

This review is organized as follows: Section II presents the fundamentals of STAMP and its underlying methods. Section III describes the research methodology based on PRISMA framework. Section IV details the statistical analysis of the eligible studies. A detailed review and scientific discussion is provided in Section V. Finally, the conclusive discussions and future directions are summarized in Section VI.

II. OVERVIEW OF STAMP

The story of STAMP starts with the seminal works of Prof. Nancy G. Leveson [13], [26], [27], where she revisited and examined the classic assumptions and paradigms underlying safety engineering (involving complex sociotechnical systems); namely, the relationship between safety and reliability, the accident causality models, the retrospective and prospective analysis, and the operational (and organizational) failures. As previously asserted by Rasmussen [11], Leveson also highlighted the necessity for novel assumptions and paradigms in system safety. In fact, she went one step further and proposed an up-to-date accident model (STAMP) and safety analysis tool (STPA) to address the safety of current sociotechnical systems [13], [27].

A historical analysis of the STAMP development timeline was conducted in [28]. Chronologically, the authors in [26] showcased the STAMP model and the associated hazard analysis methodology (STPA). In [27], a detailed guidance on STPA application was provided while providing an accident analysis approach (Causal Analysis based on System Theory - CAST). This was followed by STPA and CAST handbooks for safety practitioners [29], [30]. In the following sections, we present STAMP, CAST and STPA.

A. STAMP

STAMP is relatively a new accident model based on systems and control theory. Built on a set of (new) assumptions about how accidents occur, it expands the traditional model of causation beyond a chain of directly-related failure events or component failures to include more complex processes and unsafe interactions among system components. Accordingly, safety is viewed as a control problem, and then managed by a control structure embedded within the sociotechnical system which enforces a set of safety constraints on the system behavior [13], [27]. Notice that, no classic causes are omitted from the STAMP model, but more are included and the emphasis changes from preventing failures to enforcing constraints on system behavior.

The three main principles of STAMP are (*i*) safety constraints, (*ii*) hierarchical control structure, and (*iii*) process models. *Safety constraints* are enforced through safety controls which, if adequately implemented, will prevent adverse events from taking place. In STAMP, systems are viewed as *hierarchical structures*, in which people, organizations, engineering activities, and physical system elements are the components. Each level of the hierarchy imposes constraints to the level below it, and each level below provides feedback on how these constraints are successfully implemented or ineffectively failed [27], [31]. Based on control theory, the *process model* is a behavioral representation of the system process to be controlled (in a system control structure). Four conditions have to be considered with the control structure, the goal (i.e., the safety constraint), the control action conditions (from controller to the process), the observation (sensed) conditions (from the process to controller) and the model condition (the internal controller's model of controlled process) which is the process model, see Figure 1.

With respect to STAMP principles, safety is treated as an emergent property of the system that is achieved when appropriate constraints on the behavior of the system and its components are satisfied. Hence, accidents are the results of violation of safety constraints, which is mainly caused by four types of inadequate control actions: (1) incorrect or unsafe control commands, (2) absence of required control (3) wrong timing delivery of control commands and (4) control is stopped too soon or applied too long. These four types of inadequate control actions are the basis of hazard analysis using STAMP.

Equivalent to traditional safety analysis techniques (FTA, FMEA, HAZOP, etc.), which are based on the assumption that accidents are caused by the occurrence of a chain of failure events, new analysis methods are (and can be) built on the STAMP assumption. Illustratively, CAST and STPA are the primary STAMP-based approaches [27]. CAST is a retroactive analysis method that examines accidents/incidents that have occurred and identifies the causal factors that were involved [13]. STPA is a proactive analysis method that analyzes the potential cause of accidents during development so that hazards can be eliminated or controlled [29].

B. CAST

CAST is a framework, based on STAMP theory, established for understanding the accident process and analyzing the prominent systemic causal factors involved. Concretely, STAMP can be seen as the accident causality model that

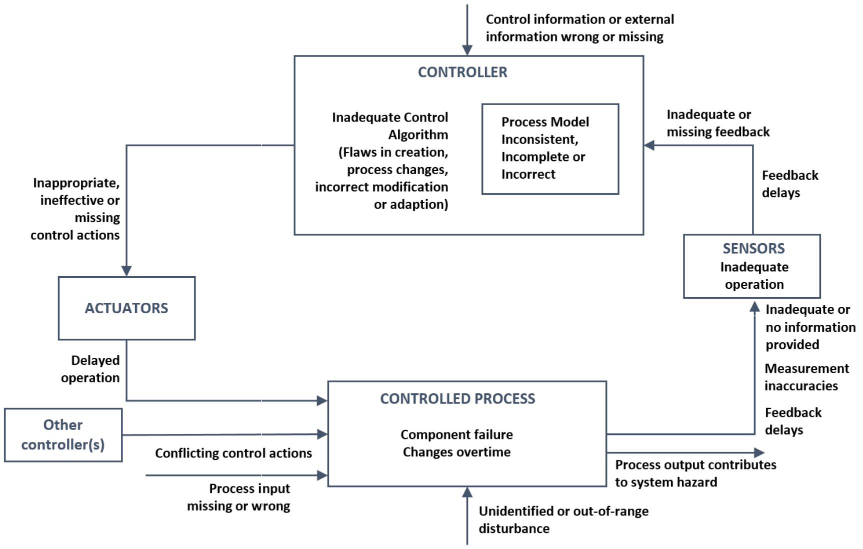

Control information or external information wrong or missing
CONTROLLER
Inadequate Control Algorithm (Flaws in creation, process changes, incorrect modification or adaption)
Process Model Inconsistent, Incomplete or Incorrect
Inadequate or missing feedback
Feedback delays
Inappropriate, ineffective or missing control actions
ACTUATORS
SENSORS Inadequate operation
Inadequate or no information provided
Measurement inaccuracies
Feedback delays
Delayed operation
Other controller(s)
Conflicting control actions
CONTROLLED PROCESS
Component failure Changes overtime
Process output contributes to system hazard
Process input missing or wrong
Unidentified or out-of-range disturbance

FIGURE 1. Control structure and unsafe control actions.

underlies CAST. The primary goal of CAST is to eliminate the so-called ''blame culture'' and redirect the focus towards understanding why human operators involved behaved the way they did, considering the information available to them at the time. Furthermore, CAST establishes a systematic approach for learning from incidents and events with the potential to lead to such incidents [30].

According to CAST handbook [30], CAST aims to identify, for accidents/incidents, why the safety control structure was unable to enforce the safety constraint that was violated and to determine what changes in the control structure are required to prevent a related loss in the future. The process of CAST can be performed in 5 steps: (1) assemble basic information, (2) model the safety control structure, (3) analyze each component in loss, (4) identify control structure flaws, and finally (5) create an improvement program.

It should be noted that until 2011, the term STAMP encompassed both the STAMP theory and its accident analysis technique. Subsequently, CAST was introduced as the accident analysis technique based on the STAMP theory. Therefore, in certain research publications, the terms STAMP and CAST are used interchangeably to denote the accident analysis technique.

C. STPA

STPA is an iterative deductive (top-down) hazard analysis method, based on the STAMP model, that seeks to analyze the potential causes of accidents during design phases so that safety risks can be eliminated or controlled. As argued by Leveson [27], the primary reason for proposing the new hazard analysis STPA was to include the new causal factors identified in STAMP that are not handled by the traditional techniques (such as software flaws, component unsafe interactions, cognitive complex human decision-making errors, social and organizational contributing factors, etc.). In addition, STPA is providing a systematic way and clear guidance for identifying scenarios that could lead to hazardous system states involving unsafe interactions among components.

Notice that STPA can be used at any phase of the system lifecycle (i.e., for an existing design or even before the design has been created) [27]. The STPA process is based on the (functional) control architecture, with the aim of identifying the potential inadequate control actions of the system and the related causes that could lead to a hazardous state. Thus, STPA is advocating to impose safety constraints and requirements necessary to enforce or limit system behavior rather than preventing the component failures, as is the case in traditional methods.

STPA is a qualitative-based analysis approach. Leveson [32] argues that quantitative estimates are inaccurate in practice and often important causal factors (such as operator error, flawed decision-making, and software errors) for which probability estimates of unsafe behavior are difficult, and perhaps impossible, to determine are always omitted. Thus, it is unfeasible to calculate the failure probability of dysfunctional interactions and environment-dependent potential impacts of hazards. Thus, STPA analysis is generally conducted with an assumption that all safety hazards are equal [33].

According to the STPA Handbook [29], the hazard analysis process is generally conducted based on four main steps: (1) define the purpose of the analysis by identifying losses, system environment, and system-level hazards and constraints, (2) build the hierarchical control structure of the system to capture the functional relationships and interactions through the feedback control loops, (3) analyze the control actions and identify the potential unsafe control actions that, under particular environment conditions, could lead to losses, and finally (4) identify the causal factors and scenarios leading to unsafe control actions and to hazards.

Notice that there exists an extension of STPA, called SPTA-Sec, used to deal with (cyber)-security [34]. STPA-Sec aims to analyze cyber-security threats, while considering the impact on system safety [35].

III. RESEARCH METHODOLOGY AND OVERVIEW

To provide a comprehensive overview on the state-of-the-art of STAMP-based research studies and applications in railway domain, we followed the PRISMA framework (*Preferred Reporting Items for Systematic Reviews and Meta-analyses*) and best practice guidelines proposed in [36]. The methodological procedure for our literature review combines individual documentary studies supported by a structured review framework created in Microsoft Excel (for statistical analysis purposes). The review procedure is performed in 4 steps, as illustrated in Figure 2, and described hereafter.

A. IDENTIFICATION

In order to collect the research works, in this review, we chose to begin with Google Scholar as a starting database as it performs a free search in publications titles and texts. The results obtained from `Google Scholar` were cross-referred with the following databases: `EBSCO, ScienceDirect, IEEE Xplore, Springer, Semantic scholar.` This process is completed by a specific (manual) search in the International and European STAMP workshops and conferences. The search query applied across all database search platforms is regrouping two parts of terms, the first part belongs to STAMP terminology (`STAMP, STPA, or CAST`) and second one to railway terminology (`Railway, Rail, train, metro, tram, rolling stock, and subway`).[2] Notice that even though no temporal filter is used, the selection explicitly considers the papers published after 2008, coinciding with the initial discussions about STAMP, and till September 2023. At the end of this initial search, we obtained a total of 118 references.

B. SCREENING

The initial search was followed by a preliminary investigation of the abstracts obtained in the previous step, during which 29 papers were judged irrelevant (mainly related to the use of abbreviations STAMP, STPA for other different meanings). By carefully reading the abstracts at this early stage, we were able to screen in manuscripts that are closely related to our subject. It may be noticed that 4 works were identified even though these were not directly related to the research objectives of this review, yet, we opine that the analysis provided by these studies is quite relevant for a detailed discussion, namely [28], [31], [37], [38].

TABLE 1. Inclusion and exclusion criteria.

Characteristics	Inclusion Criteria	Exclusion Criteria
Language	English	Other than English
Type	Academic journal articles, conference papers, graduate theses, technical reports, STAMP workshop reports	Review articles, books, presentations, book chapters, editorials, and meetings
Full-text	Full-text available	Studies available only as abstracts
Scope	Original articles focused on STAMP application in railway accident and/or hazard analysis	Publications not using STAMP for railway accident and/or hazard analysis
Date	From 2008 and indexed up to September 2023	Before 2008 and after September 2023

C. ELIGIBILITY

At this stage, the main focus was to classify the remaining 89 papers separately into different categories. The process begin by excluding papers whose main content was not presented in English, even if their abstracts and/or titles were available in English. Subsequent to the above, the full-text papers that pursued the accident modeling and investigation using STAMP and/or CAST were distinguished from those dedicated to hazard and safety analysis using STPA. The latter category (concerned with hazard and safety analysis using STPA) was further divided into three groups. The first group is concerning the research works proposing a straightforward application of STPA to railway systems, while the second one is related to works which indulge in a comparative analysis related to STPA. The works in the third group are concerned with the various extensions of STPA methodology to enhance its application in railway industry. A structured result of this grouping process is depicted in Figure 3.

D. INCLUSION AND ANALYSIS

This review encompasses two distinct analyses: (*i*) a statistical and bibliometric analysis of the eligible manuscripts and (*ii*) a comprehensive technical and scientific analysis of the research works. While all the selected 89 papers are included in the statistical and bibliometric analysis, only 72 relevant papers written in English are considered for the scientific research analysis. The criteria for inclusion and exclusion are provided in Table 1; a list of 17 studies excluded from the scientific analysis is provided in Table 2. The bibliometric analysis is presented in Section IV and the scientific analysis in Section V.

IV. STAMP/STPA IN RAILWAY – BIBLIOMETRIC ANALYSIS

This section details the statistical findings related to the 89 eligible papers. Beginning with the type of publications, type of analysis, yearly distribution, etc, an overall analysis of the research works is conducted. Then, we present a specific

[2] The search query can simply be formulated as follow: `(‘STAMP’ or ‘STPA’ or ‘CAST’) & (‘Railway’ or ‘Train’ or ‘Metro’ or ‘Tram’ or ‘Rolling Stock’ or ‘Subway’)`. Notice that STAMP, STPA and CAST were used within both full terms and the abbreviation.

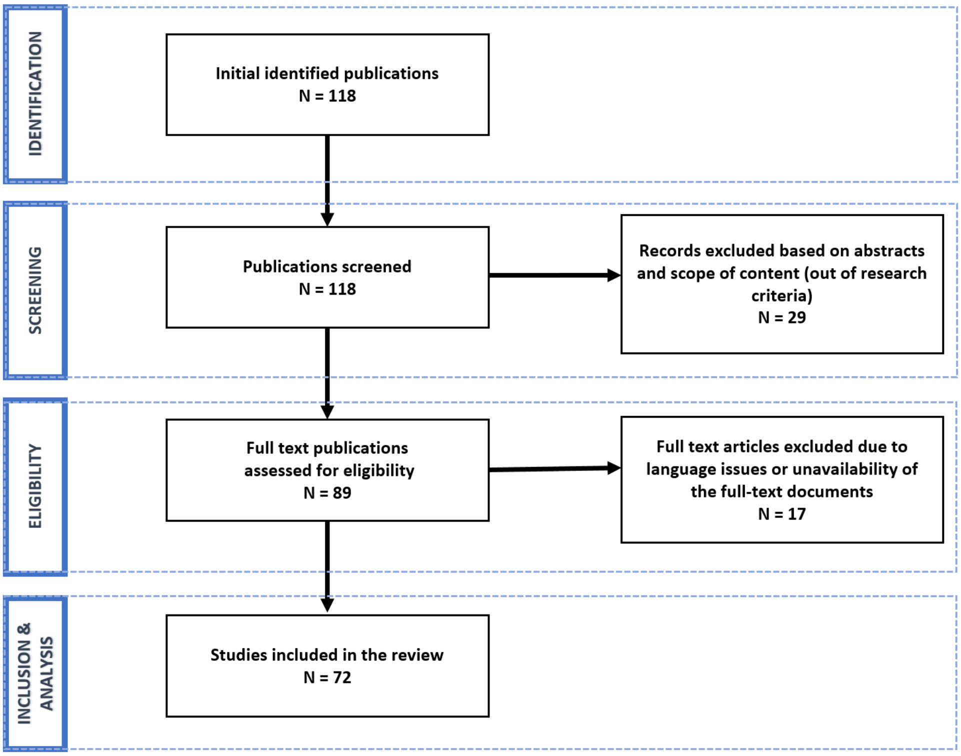

IDENTIFICATION
Initial identified publications
N = 118
SCREENING
Publications screened
N = 118
Records excluded based on abstracts and scope of content (out of research criteria)
N = 29
ELIGIBILITY
Full text publications assessed for eligibility
N = 89
Full text articles excluded due to language issues or unavailability of the full-text documents
N = 17
INCLUSION & ANALYSIS
Studies included in the review
N = 72

FIGURE 2. PRISMA procedural steps and results obtained in our review.

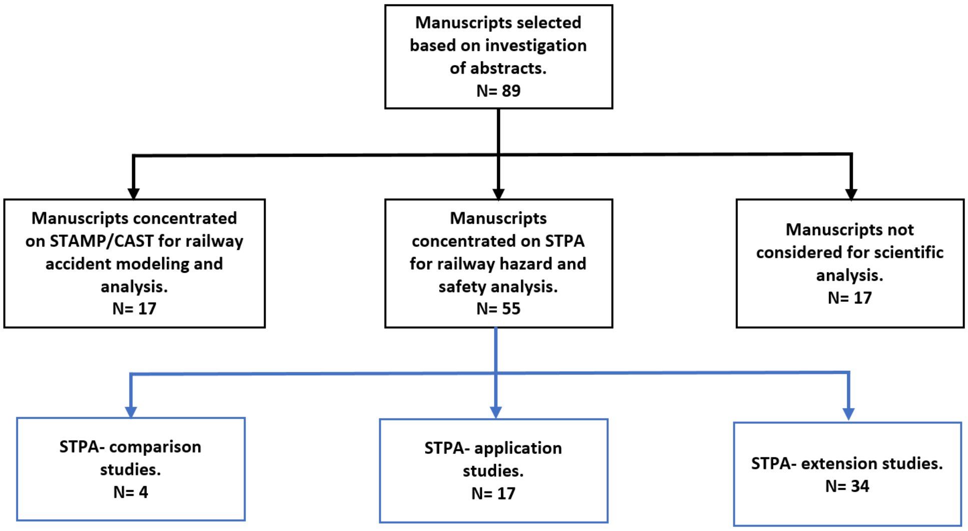

Manuscripts selected based on investigation of abstracts.
N= 89
Manuscripts concentrated on STAMP/CAST for railway accident modeling and analysis.
N= 17
Manuscripts concentrated on STPA for railway hazard and safety analysis.
N= 55
Manuscripts not considered for scientific analysis.
N= 17
STPA- comparison studies.
N= 4
STPA- application studies.
N= 17
STPA- extension studies.
N= 34

FIGURE 3. Classification of selected manuscripts into groups.

analysis regarding the studied methods, contributions, railway domains, and railway systems.

Out of the 89 studies, 97.8% (87 manuscripts) primarily represent research publications, including 9.1% (8 manuscripts) as thesis. The remaining 2.2% (2 manuscripts) are technical reports. Figure 4 graphically illustrates these results. Moreover, as depicted in Figure 5, almost 69% (61 studies) of the publications are related to hazard and safety analysis and 31.5% (28 studies) to accident modeling and analysis. With respect to the type of publication, there is 50.5% (45 studies) of works which are published in conference and STAMP workshop proceedings. Peer-reviewed journal publications represent 38.2% (34 manuscripts) of the total, with: 4 papers in *Safety Science*, 2 papers each in *Applied Ergonomics*, *Journal of the Korean Society for Railway*, *China Safety Science Journal*, *Journal of Traffic and Transportation Engineering Infrastructures*, and then, one paper in each of the remaining journals. Table 3 details

TABLE 2. List of excluded publications.

Reason for Exclusion	Studies
Language barrier	[39–45]
Unavailable or inaccessible manuscripts	[46–55]

these journals along with the corresponding published works listed therein.

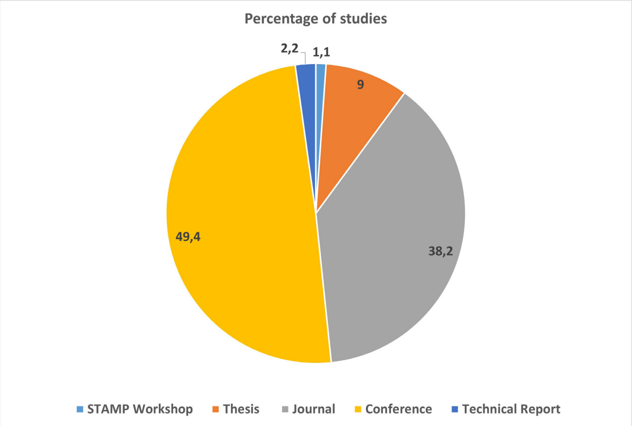


FIGURE 4. Distribution of reviewed studies by type of publication.

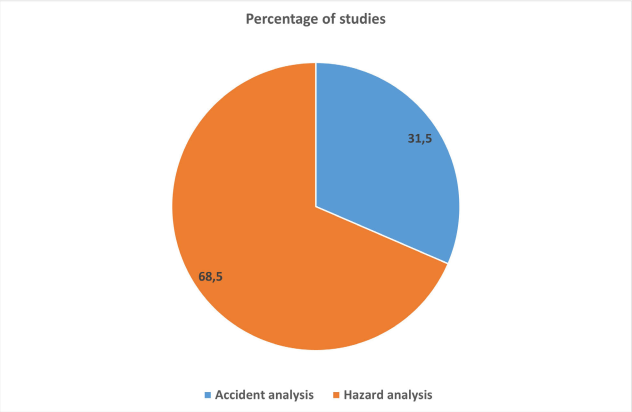


FIGURE 5. Distribution of reviewed studies by type of analysis.

To the best of our knowledge, the earliest work investigating STAMP in railway dates back to 2008, a Master thesis[3] supervised by Prof. Leveson. The first research paper, published in a journal, was published two years later [57] in the *Safety Science* Journal. Starting from these, and over the years, there were a gradual and non-continual increase in STAMP studies in railway. With a record of 25 studies in 2019, a steep decline was observed afterward (see Figure 6). Remarkably, this finding aligns with the statistical information provided in the other review of the literature [37], [58] about the study of STAMP in safety critical industries, providing that this trend exists in more than just the railway sector (see Figure 7).

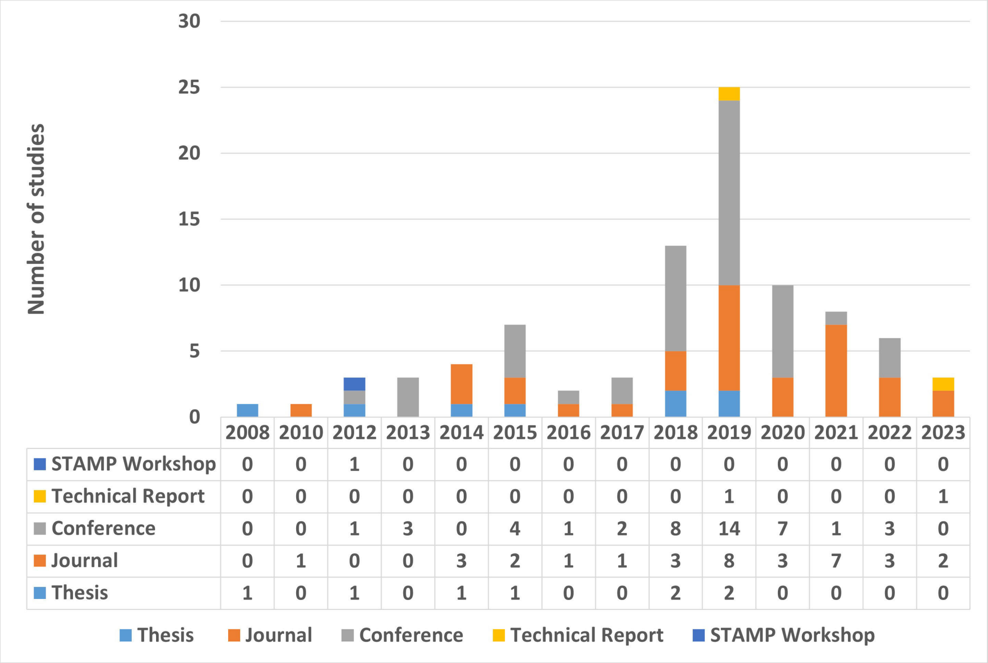
TABLE 3. List of journals with identified manuscripts.

Name of the Journal	N° of papers	Studies
Safety Science	4	[33, 57, 59, 60]
Applied Ergonomics	2	[2, 61]
Journal of the Korean Society for Railway	2	[44, 50]
China Safety Science Journal	2	[43, 54]
Journal of Traffic and Transportation Engineering	2	[62, 63]
Infrastructures	1	[64]
Accident Analysis and Prevention	1	[65]
Smart and Resilient Transportation	1	[66]
International Journal of Environmental Research and Public Health	1	[67]
Journal of Beijing Jiaotong University	1	[40]
Journal of the China Railway Society	1	[41]
China Railway Science	1	[42]
Journal of Korean Institute of Information Scientists and Engineers	1	[51]
Human Factors in Japan	1	[45]
Science of computer engineering	1	[68]
Trends in computer science and technology	1	[69]
Applied Sciences	1	[70]
International Journal of Hybrid Information Technology	1	[71]
Dependability	1	[72]
Safety & Reliability	1	[73]
International Journal of Industrial and Systems Engineering	1	[55]
Part F: Journal of rail and rapid transport	1	[74]
Reliability Engineering and System Safety	1	[75]
Journal of Rail Transport Planning and Management	1	[76]
IEEE Access	1	[77]
Journal of control, measurement and system integration	1	[78]
Chinese Journal of Electronics	1	[79]

Figure 8 provides a geographical distribution of published works. It is noteworthy to emphasize that substantial contributions, analyzed in this review, originate predominantly from China (42.7% - 38 papers) rather than the United States of America (USA) (6.7% - 6 papers), where the origins of STAMP are rooted. Surprisingly, even the number of manuscripts from Japan (19.1% - 17 papers) surpass that from the USA. We hypothesize that this trend may be attributed to the comparatively lower popularity of railway transportation systems in the USA compared to countries in Asia and Europe. Additionally, it is interesting to observe contributions from almost all continents, including a solitary paper from Africa.

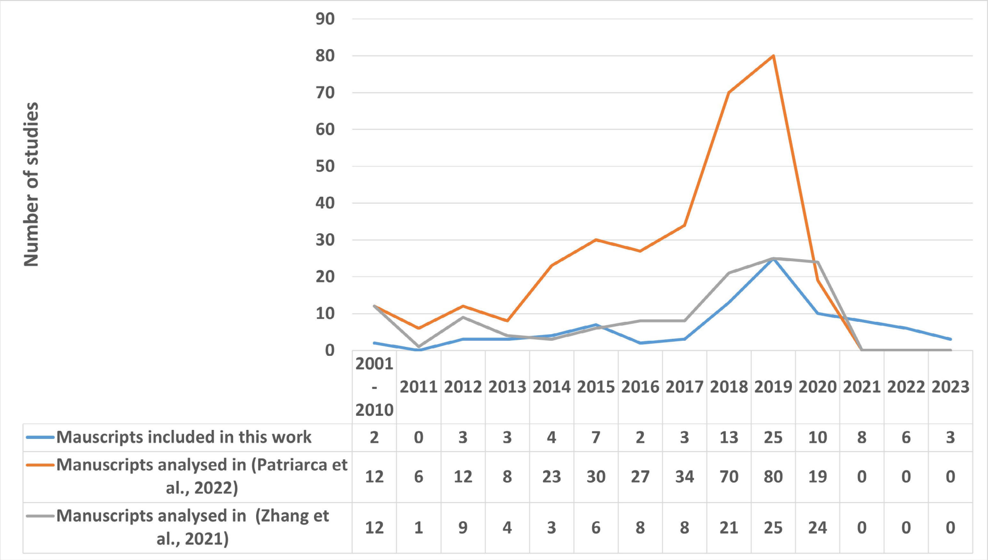
Analysis of the eligible works highlight that technical safety and risk analysis are the predominant subjects studied, with more than 68% (61 papers). Then, it comes respectively formal methods (18% - 16 papers), human factors/ ergonomics (5.6% - 5 papers) and security (3.4% - 3 papers). Figure 9 shows the distribution of the published studies according to these different safety engineering domains. Furthermore, Figure 10 categorizes the reviewed papers as per the railway subdomains. The majority of the contributions fall under the mainline passenger category (with more than 83% - 75 papers). Then, Urban Guided Transportation, Magnetic levitation (Maglev) and Mainline Freight systems

[3] Master thesis [56] of Shuichiro Daniel Ota.



	2008	2010	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
STAMP Workshop	0	0	1	0	0	0	0	0	0	0	0	0	0	0
Technical Report	0	0	0	0	0	0	0	0	0	1	0	0	0	1
Conference	0	0	1	3	0	4	1	2	8	14	7	1	3	0
Journal	0	1	0	0	3	2	1	1	3	8	3	7	3	2
Thesis	1	0	1	0	1	1	0	0	2	2	0	0	0	0

FIGURE 6. Distribution of railway systems-based studies by year.



	2001 - 2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
Mauscripts included in this work	2	0	3	3	4	7	2	3	13	25	10	8	6	3
Manuscripts analysed in (Patriarca et al., 2022)	12	6	12	8	23	30	27	34	70	80	19	0	0	0
Manuscripts analysed in (Zhang et al., 2021)	12	1	9	4	3	6	8	8	21	25	24	0	0	0

FIGURE 7. Comparison of manuscripts with other prominent literature reviews.

share more than 11% - 10 papers, 1% and 1% respectively. Other domain make up 2.2% of the remaining total.

Finally, Figure 11 presents an additional category pertaining to the railway components. Control-command and signaling (CCS) is the system that has been studied the most. This makes sense considering that CCS are safety-related systems (e.g., automatic train protection systems), with more than 39% (35 papers). The (global) railway system follows with a share of around 27% (24 papers) along with infrastructure (22.5% - 20 papers); followed by rolling stock and, operation and traffic management with each providing more than 10% and 1%, respectively.

V. STAMP/STPA IN RAILWAY - SCIENTIFIC ANALYSIS

In this section, we begin by examining research works pertaining to the modeling and analysis of accidents using STAMP/CAST in railway domain. Subsequently, we review the investigation of STPA in the hazard analysis and risk assessment of railway systems.

A. STAMP/CAST FOR RAILWAY ACCIDENT MODELING AND ANALYSIS

While carrying out the analysis (refer to Figure 3), 17 such research studies were identified that investigated (or partially included) STAMP or CAST in their railway accidents

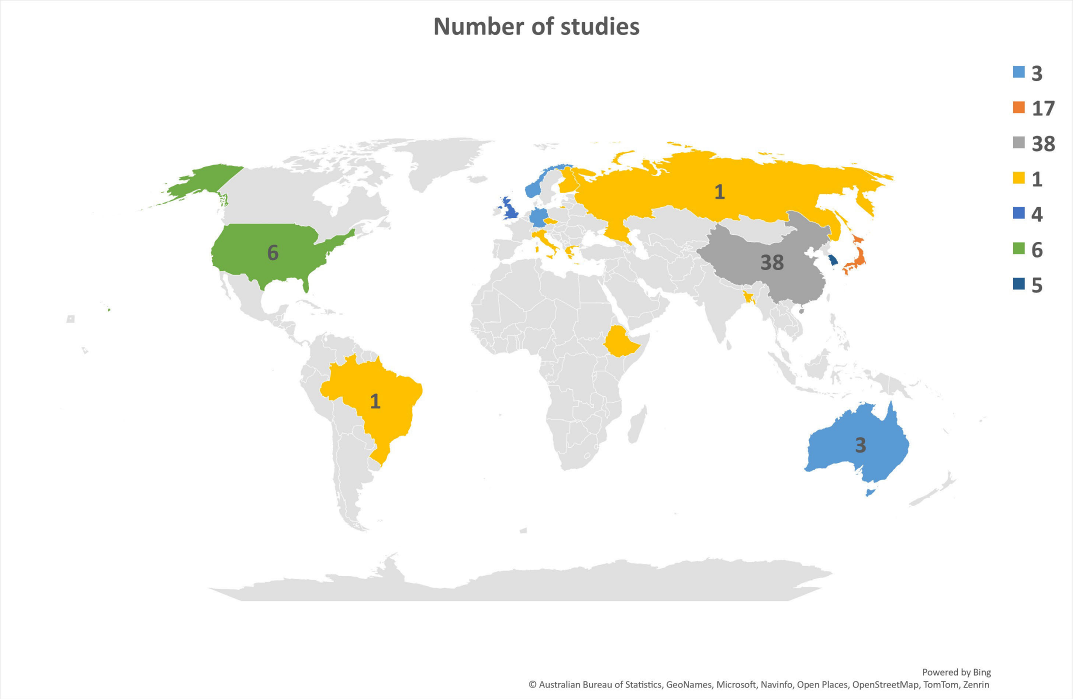

Number of studies
■ 3
■ 17
■ 38
■ 1
■ 4
■ 6
■ 5
1
6
38
1
3
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

FIGURE 8. Distribution of studies according to their country of origin.

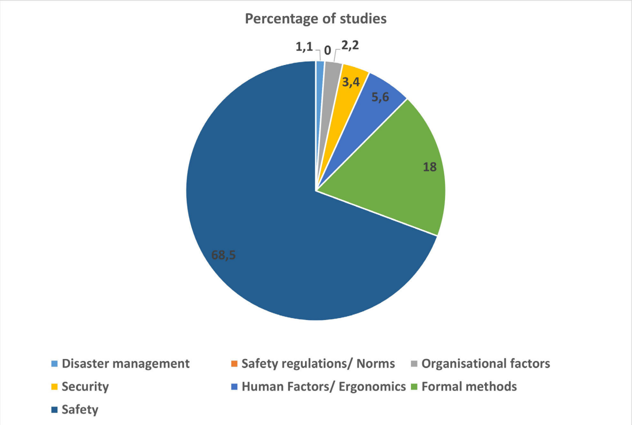


FIGURE 9. Distribution of studies according to safety engineering domains.

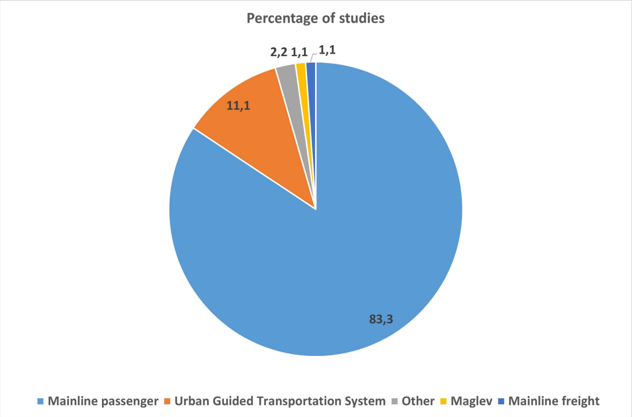


FIGURE 10. Distribution of studies according to railway systems.

modeling and analysis. These studies assessed 10 railway accidents that occurred in 5 different counties (China, USA, UK, Japan, and Bangladesh). The pioneering effort in investigating STAMP for railway analysis was undertaken in 2010 [57]. It was further noticed that the earlier studies used STAMP/CAST methodology to re-analyze railway accidents that occurred in the past, whereas other studies aimed to compare the results of their analysis with other conventional accident analysis methods (and the authorities' investigation reports). A third and interesting group of studies have attempted to extend the STAMP-based approach by considering some railway-specific features, or to combine it with other accident analysis techniques. Table 4 summarizes the considered research studies, the type of conducted analysis and the investigated accident. Hereafter, we provide a succinct discussion of these research studies with respect to the accidents considered and the type of the analysis performed.

The China-Jiaoji railway accident[4] took place near the city of Zibo in Shandong province of Republic of China. The complete accident took place in two phases. A first train was derailed, and then this derailment led to a collision with another train. Reference [57] implemented the STAMP approach as presented in [26] in order to discuss the accident spreading process. The authors modeled the overall hierarchical control structure to ensure the safe operation of

[4] https://en.wikipedia.org/wiki/Zibo_train_collision

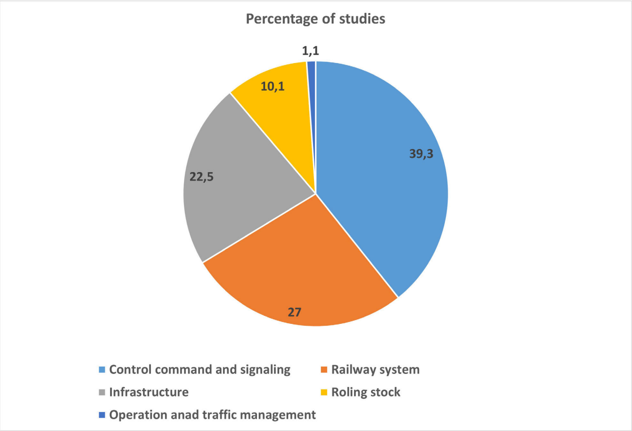


FIGURE 11. Distribution of studies according to railway subsystems.

trains in China, starting from the government level and up till the direct control of the train by the driver. Then, they analyzed the roles of each component in the control structure (including ministry of railways, local railway administration, local railway station bureau, and finally the driver and the technical systems). The results of the causal analysis demand more feedback and communication channels in the control structure and the deployment of effective hardware devices.

The Wenzhou 7.23 high speed train collision accident[5] is the academically most investigated accident as per our search. In this accident, a rear-end collision of two high speed trains led to their derailments. The government report identified that the accident was caused by a technical failure (HW/SW components). Three research studies have conducted a STAMP-based accident analysis for this accident. The analysis conducted in [79] and [80] have shown that complex causal factors (throughout the process of project development and operations combined with the errors of human controllers) are behind the HW/SW failure. Simultaneously, the study conducted by [81] concluded that the outputs of the STAMP analysis are consistent with the accident investigation report; however, contrary to the accident investigation which just identifies the causal factors and human responsibility, STAMP analysis provides a more comprehensive view to understand the accident.

For the same accident, the authors of [82] conducted a comparative study of two systematic accident analysis methods, STAMP and AcciMap. Concretely, the authors applied the AcciMap approach to get a thorough perspective of the accident. They described the entire accident trajectory and assembled the contributing factors into a coherent causal diagram that illustrates the interrelationships between them. As a result of the study, two new causes were further identified compared with the STAMP-based analysis conducted in [81]. The first one is at the level of the Railway Bureau, regarding logic errors in decisions; and a second one, common to all levels, regarding the weak level of safety awareness of the agents over the whole process of train operation.

In [2], the authors analyzed the accident from the viewpoint of human and organizational factors by means of a hybrid approach combining STAMP and HFACS (Human Factors Analysis and Classification System). Taking advantage of the human error categories derived from HFACS and the structured systematic analysis process of STAMP, this hybrid method provides a detailed causal analysis of human errors that occur while receiving information to implement control actions. The application of this method to Wenzhou accident and comparative analysis of the results with other analyses [83], [84] demonstrate that the aspect of human factor in STAMP is somewhat limited and under-specified, and the managerial and social issues in a sociotechnical system are simply viewed as sources of failure in terms of control constraints.

With the aim of extending STAMP/CAST with a formal layer, [85] proposed the so-called `formalSTAMP` approach, that endows the STAMP model with the Petri net modeling features (based on `proFunD` formal methodology [86]). While STAMP/CAST mainly focuses on the qualitative analysis including organizational aspects, `proFunD` method supports both qualitative and quantitative analyses. However, `proFunD` is not adequate for the analysis of the high levels of organizations. Hence, by their integration, `formalSTAMP` facilitates both qualitative and quantitative analysis while considering organizational factors. The analysis of the Wenzhou 7.23 accident with this extension of STAMP identified the same hazards as in [84], yet, it identified more concrete safety constraints due to a formal background.

Another railway accident, a train derailment that led to an end-of-track collision in the USA - Hoboken terminal,[6] has been analyzed using STAMP. The analysis conducted in [66] aims to provide a qualitative and explicit understanding of the systems hazards, safety constraints and hierarchical control structure of train operations on terminating tracks in US passenger station. This work provides a detailed safety analysis of technical components, human errors, environmental factors and their interrelationships in the complex terminal operating system. The results disclose the inadequate safety constraints at each hierarchical level, leading to end-of-track collisions, and contribute to the establishment of adequate recommendations. Indeed, four policy recommendations and practical operations are presented to improve the safety level and mitigate the risk of end-of-track collisions at passenger stations.

Another such train derailment in UK-Grayrigg [87] has been analyzed using STAMP in [64] and [65]. Reference [65] performed a comparative analysis of three accident analysis techniques: a variant of Swiss Cheese Model (ATSB model [88]) and two systematic accident analysis (AcciMap and STAMP). Concretely, the analysis techniques were evaluated against two subjects: (1) coverage

[5] https://en.wikipedia.org/wiki/Wenzhou_train_collision

[6] https://www.ntsb.gov/safety/safety-studies/Pages/DCA17SR001.aspx

of systems theory concepts (in terms of system structure, system component relationships, and system behavior) and (2) usage characteristics (in terms of data requirements, validity, reliability, usability and graphical representation of the accident). The comparative study showed how ATSB model and AcciMap do not directly address all the keys concepts of systems theory, still graphically present their findings in a more succinct manner. Conversely, STAMP more clearly encapsulated the concepts of systems theory but did not provide a graphical scheme of the accident. Recently, [64] applied STAMP/CAST to analyze the accident and concluded that the method offered a systematic and comprehensive perspective of the incident and permitted the findings relating to flaws and defects within different organizational levels. The authors also highlighted that while the original accident recommendations were limited to modifications in the process system and documentary aspects, STAMP/CAST provided further recommendations regarding systematic factors and design flaws.

In Japan, a serious accident occurred as a result of cracks in bogeys.[7] The STAMP analysis conducted in [33] led to the identification of relevant influencing factors, such as safety-related communication between the operator and the rolling stock manufacturer. Similarly, [89] analyzed the London subway accident,[8] where a passenger got stuck between the train doors. The case was analyzed using two different methods, STAMP and RAIB. Applying RAIB, the authors modeled the scenario of the accident and the sequence of causal events, but failed to clearly understand the complex relationship among the various events. However, through STAMP, they succeeded in the examination of the entire sociotechnical system design and identified weakness in the safety control structure.

Recently, in case of the China-Joo Koon station train collision,[9] the authors in [90] used STAMP to analyze the accident and provide a better explanation of the accident scenario. For another incident at the Jinguang Expressway North Tunnel [67], [93] set out to identify the deficiencies of the existing emergency management system by applying CAST. The complexity of the emergency management system renders CAST method suitable for such systems. The authors concluded that even though CAST method is effective to analyze social systems, yet, some fundamental changes are required. They also recommended that the government agencies use CAST method to summarize the issues exposed during post-incident exercises, as it is efficient in determining future improvements.

Finally, we highlight some interesting Master and PhD research studies that we stumbled upon. These works have also considered STAMP-based approach for railway accident analysis purposes. Succinctly, the authors in [91] discussed a generic system-based safety control methodology for Light Rail Transit, based on lessons learned from past accident analyzes. The authors in [92] used CAST method and compared it with AIBN (Accident Investigation Board Norway) method in order to evaluate its benefit, as a systematic approach, for the accidents involving ERTMS (European Rail Traffic Management System). The authors in [61] compared three accident analysis approaches, AcciMap, CAST and Perceptual Cycle Model (PCM) cognitive approach, to support the analysis of a level crossing incident in Bangladesh. Lastly, [56] discussed an approach to analyze safety in high-speed maglev systems while analyzing the Fukuchiyama line derailment accident in Japan.

B. STPA FOR RAILWAY HAZARD AND SAFETY ANALYSIS

Based on our analysis (refer Figure 3), we have identified 55 research studies that have applied STPA (or partially incorporated it) for their railway hazard and safety analysis. Similar to the studies on STAMP railway accident analysis, the STPA hazard analysis studies can be categorized into 3 groups. The first group focused on exploring the application of the STPA approach to railway systems (see Table 5). The focus of the second group was on comparing the STPA approach and its outcomes with the conventional methods used in railway safety analysis (see Table 6). The last group aimed to adapt, enhance, or extend STPA when applied in the context of railways (see Table 7). Hereafter, we provide a succinct overview of works within each group.

1) STPA APPLICATION STUDIES

In order to explore this new hazard analysis approach, several research studies have applied STPA to analyze the overall rail system. Indeed, with the aim of understanding the railway safety management, [75] investigated STPA methodology to establish a control structure model of the Australian railway system. The proposed control structure describes the whole railway system, identifies the actors involved in managing safety, and shows the control actions and feedback mechanisms that comprise the adaptive feedback function to maintain safety. As the primary goal of the work was not to address the hazards, not all steps of the STPA method were implemented. In contrast, [94] carried out a hazard analysis using STPA for a guided transportation system (at overall level). The analysis focused on typical rolling stock operating scenarios, such as obstacle avoidance. The study applied the key steps of STPA method, starting with examining a predefined list of hazards, establishing a control structure, identifying unsafe control actions and finally enforcing the safety constraints. Similarly, [76] investigated STPA with the aim of identifying the hierarchical safety indicators in urban rail transit systems. Based on the unsafe control actions and detailed causal scenarios identified by STPA, two levels of leading indicators are identified (operation and daily management levels). Thanks to these indicators, the operators could understand the operating conditions of the train and

[7] https://www.mlit.go.jp/jtsb/eng-rail_report/English/RI2019-1-1e.pdf

[8] https://www.railwaysarchive.co.uk/documents/RAIB_Clapham South2015.pdf

[9] https://en.wikipedia.org/wiki/Joo_Koon_rail_accident

TABLE 4. **STAMP/CAST based accident analysis in railways.**

Railway Accident	Studies	Contribution
China- Jiaoji (Train derailment and High-Speed Rail collision accident)	[57]	Accident analysis
China- Wenzhou/ Yongwen 7.23 accident (High-speed train collision)	[81]	Accident analysis
	[82]	Comparative analysis
	[80]	Accident analysis
	[79]	Accident analysis
	[85]	Extension and combination
	[2]	Extension and combination
US- Hoboken terminal (End-of-track collision)	[66]	Accident analysis
UK- Grayrigg (Train derailment)	[65]	Comparative analysis
	[64]	Accident analysis
Japan- HSR accident	[33]	Accident analysis
Japan- Fukuchiyama line derailment accident	[56]	Accident analysis
UK- London subway accident (Passenger trapped between doors)	[89]	Comparative analysis
China- Joo koon station (Train collision)	[90]	comparative analysis
China- Zhengzhou metro (Power loss due to water ingress)	[67]	Accident analysis
Bangladesh- Railroad crossing incident	[61]	Accident analysis
Unspecified	[91]	(Theoretic work)
Unspecified	[92]	(Theoretic work)

the management of the line, capture anomalies timely and be aware of the consequence of the indicators. In this work, the cross-line shunting scenario of interconnection in Chongqing Metro is used as a case study.

Further, few research works have investigated the STPA method at the railway sub-systems level. Reference [63] applied STPA to analyze the safety of the interlocking function for CBTC system based on the concept of "*securing a train traveling path*". The key steps of STPA were performed, and the authors concluded that an effective analysis can be achieved by linking the analysis using the STPA concept and the Fault Tree model; further, they stressed that the STPA and FTA should not be compared on the same level. The authors in [97] conducted a safety analysis for the train control system based on virtual coupling. STPA method is used to identify the high level hazards related to the system and put forward the corresponding safety constraints. The authors expanded the method to propose and visualize the (safe) state-space of the system to assist the safety analysis. In [98], STPA is used to analyze the security[10] of the train control system. Concretely, the STPA key steps have been performed to analyze the safety of Temporary Speed Restriction (TSR) sending scenario based on vehicle-to-vehicle communication. As a result of the analysis, security design requirements were formulated according to the obtained control defects and then modeled using time automata for verification. Similarly, [99] aimed to understand dependencies among, safety, reliability, and security in cyber-physical systems. A methodology to perform hazard-driven modeling of cyber and physical threats and impact assessment following an attack is presented. In this methodology, STPA is applied to the functional model to highlight high-level abuse cases. Even though the methodology is presented in a general framework of cyber-physical systems, the authors illustrated the approach using a Communication based train control (CBTC) system.

The authors in [100] conducted STPA analysis on Regional Data Center and the core track-side equipment of Chinese Train Control System Level 1 (CTCS-1). The study aimed to identify potential hazards related to train collision and derailment based on the hierarchical control structure of CTCS-1, and then generate Safety Design Demands (SDD) to guide the system design. A similar approach is presented in [101], with an application of STPA to the positioning integrity of CTCS-4. In this work, safety requirements are elaborated on the basis of causal factors of the UCAs, and the generated SSDs are verified using UPPAAL model-checking. The authors in [104] conducted a study to examine the factors that contribute to the hazard "*run through switches*" (RTS) at different railway system levels. To do so, the authors conducted interviews with railroad employees in different roles and at different levels in the organization. In this work, STPA is used to identify how interacting factors (related to physical infrastructure, individual, team and organizational) can lead to RTS. A more detailed version of the work was also published as a technical report [105].

During this review, we observed that STPA has often been applied to control systems such as (automated) protection systems, railroad crossing, door system control, etc. This is mainly due to the fact that such control systems are safety-related functions. For instance, [102] proposed a rule-based approach to help analyze hazardous contexts (in terms of control actions, variables and internal states) with STPA. The aim of the approach is to identify contexts which require verification and prevent repeated verification for those that

[10] The authors interchangeably employed the terms *security* and *safety*, seemingly attributable to the analysis's direct association with telecommunication systems.

TABLE 5. STPA-based hazard analysis & risk analysis in railways (Application).

Studies	Research work	STPA-application
[75]	Complexity on the rails: A systems-based approach to understanding safety management in rail transport	(Global) railway system
[72]	Safety model construction for a complex automatic transportation system	(Global) railway system
[76]	Identification of causal scenarios and application of leading indicators in the interconnection mode of urban rail transit based on STPA	(Global) railway system
[94]	Safety analysis on typical scenarios of GTCS based on STAMP and STPA	Control command & signaling
[95]	Autonomous Train Operational Safety assurance by Accidental Scenarios Searching	Control command & signaling
[96]	Scenarios Oriented Safety Analysis of Fully Automatic Operation Metro	Control command & signaling
[63]	Interlocking System for CBTC (Communication Based Train Control) System	Control command & signaling
[97]	A key step to virtual coupling	Control command & signaling
[98]	Application of STPA in Temporary Speed Restriction Sending Scenario of Train Control System Based on Vehicle-Vehicle Communication	Control command & signaling
[99]	Hazard driven threat modelling for cyber physical systems	Control command & signaling
[100]	STPA based safety analysis of regional data center in CTCS-1 train control system	Control command & signaling
[101]	Safety Analysis Research of Train Integrity Based on STPA	Control command & signaling
[102]	A rule-based approach for safety analysis using STAMP/STPA	Rolling stock
[103]	Safety Analyses on the use of tram doors in GoA1 and GoA4 autonomy levels	Rolling stock
[62]	Safety assessment of closed-loop level crossing control systems by means of STAMP	Infrastructure
[104, 105]	Understanding Why Railroad Yard Crews Run Through Misaligned Switches Through The Lens of Sociotechnical Systems; Why Do Passenger Trains Run through Switches in the Rail Yard?	Infrastructure

are similar. This approach is applied to a hazardous train passenger fall scenario. Regarding the railroad level crossing system, [62] applied STPA for hazard analysis of three types of closed-loop level crossing control systems. The main objective was to compare the safety effectiveness of these systems with respect to the conventional one. The keys steps of STPA have been performed and combined with some outputs of STAMP analysis regarding accidents analysis.

In the context of automated railways, [95] conducted STPA-based hazard analysis for automated railway operations with the help of accidental scenarios searching while taking Beijing Yanfang Line as a case study. The authors have shown how the obtained results can be exploited for scenarios testing and validation. In [96], STPA was also applied on fully automated Beijing Yangfang Line metro. The study is focused on the analysis of the abnormal operations related to the interactions between the new automated functions and the CBTC system. The key steps of STPA method were performed, and the causal scenarios are identified with respect to three factors, namely environment, human, and equipment factors. Similarly, [103] have applied STPA to a tram door in the case of Grade of Automation 1 (GoA1) and GoA4. The authors applied two risk analysis methods (PHA and STPA) at the concept level to identify new safety risks related to the tram automated operations. The study have identified different operating situations of the above-mentioned system, analyzed the safety and availability related risks and defined the adequate safety measures. The results of the analyses show that parts of the train door system are able to operate in GoA4. Furthermore, the findings suggested enhancing the safety measures for doors by preventing their opening during train motion and implementing obstacle detection between the doors. Finally, [72] investigated several approaches to analyze a safety model of multi-loop transportation systems. The work used STPA process and the safety principles in the SOTIF[11] standard [106] to describe the safety model and preform the analysis.

2) STPA COMPARISON STUDIES

By now it has become evident that for STPA to be integrated into railway practices, it is necessary to demonstrate its relevance and efficiency compared to conventional hazard analysis approaches. Accordingly, various comparative studies have been conducted with respect to conventional ones. For instance, a comparative study of the STPA with HAZOP was performed in [107]. The authors were interested on the safety impact of the replacement of human by technical components, during emergency conditions, in highly automated systems. Hence, they conducted a scenario-based STPA analysis for the fully automated operation systems with respect to 4 hazardous scenarios (collision, obstacles, derailment, and passenger injuries in doors). The comparison is then performed with respect to existing HAZOP study. The conclusion of the study highlighted the process of conducting hazard analysis than the actual outputs of the study.

The work by [108] aimed to compare three safety analysis techniques (FMEA, FTA and STPA) with regards to the criteria of effectiveness, applicability, ease-of-use and efficiency in identifying software safety requirements at the system level. Three railway sub-systems were considered (train door control, anti-lock braking and traffic collision and avoidance), and several controlled experiment were conducted in order to have some statistic results. The comparison results are obtained from three data sources (questionnaires, final reports analysis, and time sheets). The study concluded that even though there is no statistically significant difference between the approaches, in terms

[11] Safety of The Intended Functionality

of effectiveness and efficiency, the STPA addressed more software safety requirements than the traditional techniques. However, the conduct of STPA require more time from safety analysts with short or no prior experience. Similarly, [109] compared STPA and Software FMEA through a simultaneous application of both techniques on a level crossing system. The authors concluded that STPA was more effective, particularly in identifying the (root) causes and the safety constraints.

Recently, [73] discussed how STPA can be used and integrated within the European railway safety management process, known as Common Safety Method for Risk Evaluation and Assessment (CSM-RA[12]). In this regard, the authors simultaneously scrutinized the process activities of both CSM-RA and STPA, aiming to identify the tasks within the CSM-RA process where STPA steps could be integrated. The focus was particularly placed on system definition, hazard identification and classification, as well as risk analysis and evaluation. The authors proposed the application of STPA, and potentially RiskSOAP [110], to real case studies from complex rail projects. They further emphasized that STPA is not intended to replace conventional techniques, but to shift the attention from hardware/reliability focus to more intangible factors, such as human behavior for complex systems that could have an impact on the railway safety.

3) STPA EXTENSIONS STUDIES

Within this category, the main objective of studies was to identify pertinent synergies between STPA and other approaches, or to enhance it through the incorporation of formal methods and modeling languages. This was done with the aim to refine the study, improve the control structure model, and/or enhance the quality and details of the analysis.

At the overall railway system level, [77] contended that STPA hierarchical control structure comprises numerous layers, rendering it challenging to track causes effectively. To handle this issue, the authors proposed a new control structure model for multiple control processes in time sequence and propose to endow STPA with an automated accident causal scenario identification. The control model is extended with respect to four aspects: control actions, input variables, external disturbances, and synchronous timings. The feasibility and efficiency of the approach is evaluated through the operational scenarios of parking in a station of Beijing Yanfang Line. Similarly, [70] proposed a hazard analysis approach to capture and evaluate the emergent SOTIF-related hazardous factors (functional inefficiencies, performance limitation, and reasonable foreseeable misuses) in automated railway systems. This approach is a customization of STPA with focus on two facets: (*i*) the hazardous factor identification and (*ii*) the hazardous factors evaluation based on complex network theory [111]. The first aspect tends to extend the control structure of STPA in order to integrate the situational awareness process modeling, while the second one aims a quantitative evaluation of hazardous factors for heterogeneous networks and customized topological indexes. The proposed approach is applied to a train driving assistance system in Tsuen Wan Line of Hong Kong metro. Further, [71] used STAMP/STPA to analyze thse organizational factors that impact the safety of automatic operation systems in railway. Recognizing the limitations of STAMP in organizational-level analysis, the authors proposed to support it with a theoretical model of organization (Viable System Model — VSM [112]). In this study, VSM is used to improve the safety analysis of inadequate constraints of organization, and the dynamics models of organizational safety process in the system.

Applying conventional methods to their advantage, [113] integrated risk estimation and evaluation into STPA process by means of FMEA. The authors illustrated their approach on a level crossing system. They further claim that safety constraints identified through this study were almost twice more than the individual application of STPA during previous work [109]. Aiming to enhance the determination of control actions in STPA, [114] extended the STPA process by taking into account further (environment) variables in the control structure modeling. The authors argued the necessity of a methodology for an accurate identification of such environmental variables and illustrated the approach on the case of automatic train door control system.

Aiming to perform a risk assessment that integrates both safety hazards and security threats, [115] proposed a hybrid method, called Systems- Theoretic Likelihood and Severity Analysis (STLSA), as a combination of both STEP-Sec [34] and FMVEA [116]. The approach provides and enriches the top-down view of the functional control structure of a system with threat/failure scenarios with a semi-quantitative risk analysis. The approach is illustrated on a train braking system. Similarly, [117] proposed a design framework to facilitate the application of STPA, while integrating hazard/threat analysis related to safety, security and human factors. The approach take advantages of several frameworks, as Integrating Requirements and Information Security (IRIS) and Computer Aided Integration of Requirements and Information Security (CAIRIS), as tool-supports. The approach is illustrated with a case study related to Cambrian coastline Railway incident.[13]

Several research works have enhanced the STPA analysis by incorporating formal modeling features. For instance, [74] were interested in the temporal sequential relation (in terms of order of control actions) when performing hazard analysis using STPA. The authors illustrated the limitation of STPA in dealing with this issue through the train braking scenario in CTCS-3. To capture such a temporal relation between inadequate control actions leading to hazards, the authors proposed a new logic called "*Control*

[12] https://www.era.europa.eu/domains/common-safety-methods/risk-evaluation-assessment-csm_en

[13] https://assets.publishing.service.gov.uk/media/64f09d6ffdc5d10010284934/R172019_191219_Cambrian_Coast_line.pdf

TABLE 6. STPA-based hazard analysis & risk analysis in railways (Comparison).

Studies	Research work	Comparison with
[107]	Scenario-based STPA analysis in automated urban guided transport system	HAZOP
[108]	A Controlled Experiment for the Empirical Evaluation of Safety Analysis Techniques for Safety-Critical Software	FMEA and FTA
[73]	Introducing a system theoretic framework for safety in the rail sector: supplementing CSM-RA with STPA	CSM-RA
[109]	Comparing the Effectiveness of SFMEA and STPA	SFMEA

Action Temporal Logic" to endow the STPA process (called STPA-T). Application of STPA-T to analyze a CTCS-3 system illustrate increased accuracy and permit a more detailed refinement of safety constraints. In [118], the authors combined STPA with Colored Petri Nets formalism (CPN), so-called `formalSTPA`, in order to add a formal analysis layer to STPA. The approach is illustrated using hazardous scenarios on CTCS-3 system. Using simulation and dynamic verification, the authors aimed to identify unsafe paths leading to unsafe states from the system reachability graph. A similar work is presented in [119], where three-layer CPN models are used in modeling the STPA control structure. These models aim to depict the dynamic behaviors of the CBTC system and the specific internal interactions of the components. The approach allowed to efficiently identify technical deficiencies and organizational vulnerabilities when applied to the *process movement authority generation*. Also, the authors in [59], [120] proposed a STPA hazard analysis based on formal modeling (BFM-STPA). BFM-STPA exploits CPN to establish a formal sociotechnical control structure, efficiently identify hazards and generate a hazard log. This method is applied to CTCS-3 system, with the scenario of *Temporary Speed Restriction*. According to the authors, in comparison with HAZOP approach, the hazard log generated by BFM-STPA covered not only the subsystem failures, but also the deviation of interactions among subsystems from design intent, human errors and sociotechnical drawbacks related to the *Temporary Speed Restriction* scenario.

During the design phase, the combination of STPA is also possible with modeling activities, including simulation and formal verification of systems models [137]. In a series of research studies [69], [78], [124], the authors sought to enhance the STPA process by providing specific and concise descriptions of the various elements involved in STPA process using UML (Unified Modeling Language). At first, [124] used the UML diagrams to formally (and graphically) describe the elements of STPA process. Namely, use-case and class diagrams depict the control structure and sequence diagrams illustrate unsafe control actions and hazard scenarios. An improved version of the work was proposed in [69] where, in addition to UML, FMEA was used for specific analysis of each hazard causal factor. Similarly, [135] extended UML multi-views to facilitate the execution of STPA analysis. This approach is illustrated on a train door software control system. Also, [125] used UML modeling mechanisms to graphically depict STAMP/STPA models and system specification requirements. Since existing UML modeling mechanism cannot be directly applied to STAMP/STPA models, the authors proposed a tailored UML extension according to the characteristics of control structures in STAMP/STPA. The approach is applied to a Chinese high-speed railway train control system. Recently, [78] tried to enhance the conventional STPA using techniques for (i) describing the components of a system in hierarchical detail, (ii) clearly defining the components' behavior, and, (iii) tracking the structured control process to clarify the causes of hazards. The proposed approaches were applied to safety analysis of a railroad crossing system.

As stated by [138], more effective accident and hazard analysis outcomes can be obtained by combining STAMP/STPA and formal verification methods [139]. Accordingly, a trend of application of formal methods and tools can be noticed with STPA in railway. Reference [127] aimed to obtain more effective hazard analysis by combining STPA approach (using STAMP Workbench tool) and a formal verification one (model-checking using UPPAAL tool [140]). The main idea relies on partially automated analysis procedure in order to reduce the load on analysts. As per the procedure, firstly model the hierarchical control structure as timed automata using UPPAAL and then perform the identification of unsafe control actions, and determination of hazard causal factors as a violation of timed temporal logic properties in the model-checking process. The railroad crossing system was considered for the study, with a focus on the *fallen barrier trap hazardous* scenario. An improvement of STPA/UPPAAL approach was latterly proposed in [128]. Concretely, the authors proposed a method for deriving hazard transition sequences by using SAT/SMT [141] solver in order to automate the model checking process in UPPAAL. Similarly, [129] proposed a statistical model-checking to prioritize the hazardous scenarios identified by STPA. A procedure for systematically transforming the STPA control structure model into a formal model for using statistical model-checking tool, which calculate the probability of hazardous scenarios, is proposed. The approach is applied to a train gate control system. Likewise, [126] proposed a method that combines STPA and intent specification [142] to enhance the process of safety requirement generation and verification. The approach consists in using State flow toolbox to model the system, verify the requirements correctness and completeness (as a supplement step to STPA). The approach is illustrated through an automatic train protection system. Finally,

TABLE 7. STPA-based hazard analysis & risk analysis in railways (Extension).

Studies	Research work	STPA extensions	Quantitative extension (Yes / No)	Railway applications
[117]	Integrated Design Framework for Facilitating Systems-Theoretic Process Analysis	IRIS and CAIRIS	No	(Global) railway system
[84]	Application of CAST and STPA to railroad safety in China		No	(Global) railway system
[71]	A hybrid system dynamics modeling method for organizational factors in fully automatic operation system	Viable system modeling	No	(Global) railway system
[121]	Application of a systems-theoretic approach to risk analysis of high-speed rail project management in the US		No	(Global) railway system
[122]	Bayesian Safety Analysis of Railway Systems	Bayesian networks	Yes	Control command & signaling
[119]	Safety Analysis of Communication-Based Train Control System by STPA and Colored Petri Net (CPN)	Colored Petri Net	Yes	Control command & signaling
[74]	An extended system-theoretic hazard analysis method for the safety of high-speed railway train control systems	Control Action Temporal Logic	No	Control command & signaling
[123]	Realization of Combined Systemic Safety Analysis of Adverse Train Control System Using Model Checking	Model Checking		Control command & signaling
[118]	Safety Analysis of Train Control System Based on Colored Petri Nets and System-Theoretic Process Analysis	Colored Petri Nets	Yes	Control command & signaling
[77]	An automated accident causal scenario identification method for fully automatic operation system based on STPA	New control structure model	No	Control command & signaling
[70]	A hazard analysis approach for the SOTIF in intelligent railway driving assistance systems using STPA and complex network	Complex network theory	Yes	Control command & signaling
[124]	A Proposal for a Hazard Analysis Method for Embedded Control Software Using STAMP	UML	No	Control command & signaling
[125]	A Safety Modeling Method for High-speed Train Control Systems Based on UML Extension	UML	No	Control command & signaling
[120]	Research and application of the BFM-STAMP hazard analysis method	Colored Petri Net	Yes	Control command & signaling
[59]	An integrated hazard identification method based on the hierarchical Colored Petri Net	Colored Petri Net	Yes	Control command & signaling
[126]	Research on methodology for safety generation and verification	Intent specification	No	Control command & signaling
[68]	A hierarchical verification approach to verify complex safety control systems based on STAMP	Formal verification	Yes	Control command & signaling
[69]	A Hazard Analysis Method for Embedded Control Software with STPA	UML	No	Infrastructure
[78]	A proposal of hazard analysis method using structured system theoretical process analysis	UML	No	Infrastructure
[127]	Automated inspection method for an STAMP/STPA-fallen barrier trap at railroad crossing	Formal modeling	Yes	Infrastructure
[128]	Deriving of time constants in timed automata for hazard transition sequences for STAMP/STPA	Timed automata	Yes	Infrastructure
[129]	Prioritizing scenarios based on STAMP/STPA using statistical model checking	Statistical model checking	Yes	Infrastructure
[130]	Can STAMP provide a complete safety argument?	GSN	No	Infrastructure
[113]	Risk Assessment for STPA with FMEA Technique	FMEA	Yes	Infrastructure
[131]	FRAM/STPA: Hazard analysis method for FRAM model	FRAM	Yes	Infrastructure
[60]	STAMP goes EAST: Integrating systems ergonomics methods for the analysis of railway level crossing safety management	EAST framework	Yes	Infrastructure
[132]	Combining GSN and STPA for safety arguments	GSN	No	Rolling stock
[133]	Extend STPA Method Using Hybrid Dynamic Theory	Hybrid Dynamic Theory	No	Rolling stock
[134]	A novel real-time safety level calculation approach based on STPA	Mathematical modeling	Yes	Rolling stock
[114]	An extraction Method of STPA Variable Based on Four-Variable Model	New system variables	No	Rolling stock
[115]	Systems-theoretic likelihood and severity analysis for safety and security co-engineering	STPA-Sec and FMVEA	Yes	Rolling stock
[135]	A multi-view extended software control structure modeling and safety analysis method	UML	No	Rolling stock
[136]	SafeT-next generation safety assessment framework for railway: development of a framework for the practical implementation and facilitation of STPA	Framework for implementation	No	Rolling stock

[123] presented safety analysis of advance train controls system (ATCS)[14] by integrating two systematic approaches, STPA and FRAM. STPA is used to identify software safety constraints, to prevent the identified hazards, while FRAM is used to model the system based on the STPA control structure. Additionally, a formal verification using NuSMV model checker is used to examine whether the FRAM model meets the safety constraints identified using STPA. The application of the proposed methodology on ATCS showed that STPA and FRAM can be combined to overcome their limitations.

[14] ATCS is an embedded train control system which encompasses the following components: Train, Track, Sensors, and Controller.

Contrary to the previous works, where several approaches are used to improve or to extend the STPA process, [131] proposed to apply STPA as a hazard analysis method for FRAM-modeled systems [12]. In this combined method FRAM/STPA, hazard analysis is performed according to main keywords used to identify causes in STPA process. The authors hold the belief that FRAM/STPA has the potential to uncover additional hazards in comparison to conventional STPA. The approach is evaluated on a railroad crossing and compared to a classic STPA study. In the same spirit, [60] used the main principles of the STAMP/STPA control structure to support the EAST[15] framework in the analysis of the level crossing safety management. Concretely, a control network representation showing safety controls and their interrelations (i.e., STPA's control structure) was developed for use with EAST's existing task, social, and information network representations. The authors concluded that the extension STPA/EAST has enhanced the analytical and explanatory power of the EAST framework, and that the analysis presented has provided a rich understanding of the level crossing system lifecycle and its safety management. Also, the authors in [68] used STAMP/STPA model to enhance the formal verification of complex system. The authors proposed a conceptual verification framework to verify the safety control systems where STAMP/STPA is used to model the hierarchical control structure. Considering while using STAMP/STPA model a complex control system can be transformed into several interdependent simpler control structures with closed-loops. Then, verification of a global safety property can be decomposed into verifying the compliance of simpler control structures of the safety control system to their local properties. The approach is applied to a CTCS-3 system.

In the context of safety assurance, the authors in [132] discussed how STAMP/STPA can be combined with Goal Structuring Notation (GSN) in order to provide safety argument patterns for the safety assurance cases. This is done in a generic way by representing the STPA steps as part of the evidence and claim elements within GSN. The approach is illustrated through a train door control system.

Finally, [133] used the hybrid dynamical theory to extend STPA method. To do this, STPA control structure model is transformed into the hierarchical hybrid model where interactions and evolution of the systems included both continuous and discrete states. The approach is illustrated through a train door system that is modeled using Simulink/State flow. Reference [134] proposed an approach for the run-time monitoring of the system safety level based on STPA analysis. The approach consists of a mathematical model used to determine system safety level, where its dynamic calculations are based on STAMP/STPA model. Taking into account the operational mode of the system, and using the real-time system data and the outputs of the STPA analysis, the safety level is then calculated and updated in real time. The approach is illustrated through a case study of a train door system.

Table 7 summarizes the research works related to extension of STPA within the context of railway systems. The 3_{rd} column specifically delineates extensions pertaining to qualitative and/or quantitative analysis. With regard to quantitative analysis, the techniques and tools employed to enhance STPA predominantly encompass Bayesian networks, Colored Petri nets, formal verification (including timed automata and statistical model checking), FMEA, FRAM, and the EAST framework.

Ultimately, we would like to highlight the effort undertaken by young researchers, especially those engaged in Ph.D. and Master's theses. Notably, a significant number of studies have focused on the application of STAMP/STPA in railway systems. For instance, [136] presented a framework for the practical implementation and facilitation of the systems-theoretic process analysis for railway. Reference [84] applied STPA with the aim of including novel causal factors identified by CAST, for designing the CBTC system. Reference [130] attempted to combine STAMP and Goal Structuring Notation for safety cases. Reference [121] discussed applying STAMP in rail project management, based on lessons learned from past rail accidents. Finally, [122] used STPA and Bayesian networks in order to analyze railway safety, with a focus on the train drivers tasks and their common errors.

VI. DISCUSSION AND CONCLUSION

This study is the first review of the literature pertaining to STAMP/STPA within the railway domain. It provides an extensive bibliometric analysis and technical assessment of STAMP and its associated techniques in railway safety management. Throughout this review, a total of 118 relevant works were initially identified, with 89 included for statistical bibliographic analysis, and 72 manuscripts deeply reviewed and discussed for scientific and technical analysis.

The review mainly focused on two railway safety topics: applications of STAMP to accident modeling/analysis and applications of STPA to hazard analysis and risk assessment. As a general remark, a major part of the efforts have been made on hazard analysis using STPA, while a few researchers have focused on accident analysis using STAMP/CAST.

As regarding the accident analysis, the reviewed studies have analyzed accidents mostly related to train collision and/or derailment. It is recommended that parallel initiatives should be taken up leveraging different approaches for the analysis of diverse types of railway accidents. Consequently, we found it unfair to draw definitive conclusions regarding the efficacy of the STAMP approach in comparison to the conventional methods employed to prepare these reports. For comprehensive and meaningful assessments, conducting parallel investigations employing diverse approaches is crucial for a fair and relevant evaluation. Another noteworthy aspect pertains to the predominant involvement of academic researchers in the analyses, with minimal interaction from

[15] EAST: Event Analysis of Systemic Teamwork [143].

railway industry professionals and authorities. It is strongly recommended that, for the widespread adoption and deployment of STAMP in the railway sector, researchers have to work jointly with railway stake-holders (railway companies, railway authorities, and investigation Bureaus) in the future accident investigations.

In terms of safety and hazard analysis using STPA, the study reveals that there are three categories namely STPA applications, STPA comparison, and STPA extensions studies. Among the works involving direct STPA application, we note instances of analyzing a global railway system, yet the majority of studies focus on applying STPA to CCS systems, with limited attention to infrastructure and rolling stock systems. This is appropriately justified by the control process aspect of STAMP, inherently represented by CCS systems. On the other hand, only a few studies have compared STPA with other safety analysis methods, such as HAZOP and (S)FMEA, whereas many studies have focused on adapting and extending the STPA process to align with the specific features of the railway domain. The substantial number of studies within STPA extension category suggests that there is a willingness among railway safety researchers to adopt the method, yet, the approach is not fully tailored to their specific needs and requires further adaptations. While CAST and STPA handbooks provide guided steps for conducting the analysis, the review emphasizes that these steps have not been consistently followed. Further, each study customizes the process steps to its specific context, making the comparative studies a difficult task.

Additionally, it is important to note that STPA studies clearly highlight the fact that STPA remains a high-level (qualitative) hazard analysis method, in contrast to the conventional quantitative approaches that are already standardized in railway. Despite being recommended by several safety standards, STPA has not yet been adopted by railway safety standards. This may explain the limited enthusiasm for hazard analyzes based on STPA conducted by industrial companies. Obviously, when pursuing compliance, it is preferable to consider recommended approaches rather than taking the risk of adopting new ones.

As highlighted by several researchers, the lack of guidance from STPA regarding the development of the control structure coupled with its inability to quantitatively evaluate risks associated with identified hazards make it both time-consuming and less effective for railway engineers. STPA predominantly operates as a qualitative technique and even though some researchers have made efforts to remedy this limitation through proposed extensions, the foundations of STAMP model are not themselves established with a view to address quantification. Thus, the pursuit of quantitative safety assessments utilizing STAMP and its methodologies remains an unresolved challenge, requiring further research investigations. This is particularly significant given the quantitative nature of the railway safety analysis process.

While summing up it is important to state that the adoption of STAMP approach in the railway industry primarily depends on a shared willingness among stakeholders to collaborate on integrating the STAMP/CAST approach into accident investigations and implementing the STPA approach within the railway safety management process as part of railway standards (e.g., [1]).

REFERENCES

[1] *Railway Applications—The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAM)*, Standard EN50126, 2017

[2] C. Li, T. Tang, M. M. Chatzimichailidou, G. T. Jun, and P. Waterson, "A hybrid human and organisational analysis method for railway accidents based on STAMP-HFACS and human information processing," *Appl. Ergonom.*, vol. 79, pp. 122–142, Sep. 2019.

[3] K. Klockner and Y. Toft, "Railway accidents and incidents: Complex socio-technical system accident modelling comes of age," *Saf. Sci.*, vol. 110, pp. 59–66, Dec. 2018.

[4] P. Singh, M. A. Dulebenets, J. Pasha, E. D. R. S. Gonzalez, Y.-Y. Lau, and R. Kampmann, "Deployment of autonomous trains in rail transportation: Current trends and existing challenges," *IEEE Access*, vol. 9, pp. 91427–91461, 2021.

[5] Qamar Mahboob, Enrico Zio, and Pierre Dersin, "Introduction to the requirements of railway RAM, safety, and related general management," in *Handbook of RAM in Railway Systems*. U.K.: Taylor & Francis, 2018, pp. 3–12. [Online]. Available: https://www.taylorfrancis.com/chapters/edit/10.1201/b21983-1/introduction-requirements-railway-ram-safety-related-general-management-qamar-mahboob-enrico-zio-pierre-dersin

[6] Min An and Yong Qin, "Challenges of railway safety risk assessment and maintenance decision making," in *Handbook of Research on Emerging Innovations in Rail Transportation Engineering*. Hershey, PA, USA: IGI Global, 2016, pp. 173–211.

[7] A. Jabłoński and M. Jabłoński, "Safety management mechanisms in rail transport," in *Digital Safety in Railway Transport—Aspects of Management and Technology*. Cham, Switzerland: Springer, 2022, pp. 7–20.

[8] W.-T. Hong, G. Clifton, and J. D. Nelson, "Railway accident causation analysis: Current approaches, challenges and potential solutions," *Accident Anal. Prevention*, vol. 186, Jun. 2023, Art. no. 107049.

[9] K. Klockner and Y. Toft, "Accident modelling of railway safety occurrences: The safety and failure event network (SAFE-Net) method," *Proc. Manuf.*, vol. 3, pp. 1734–1741, 2015.

[10] P. Underwood and P. Waterson, "Accident analysis models and methods: Guidance for safety professionals," Loughborough Univ., Loughborough, U.K., Tech. Rep., 2013, p. 28. [Online]. Available: http://www.safeship.ca/uploads/3/4/4/9/34499158/accident_analysis_models_and_methods_-_guidance_for_safety_professionals.pdf

[11] J. Rasmussen, "Risk management in a dynamic society: A modelling problem," *Saf. Sci.*, vol. 27, nos. 2–3, pp. 183–213, Nov. 1997.

[12] E. Hollnagel, *FRAM: The Functional Resonance Analysis Method: Modelling Complex Socio-Technical Systems*. U.K.: Taylor & Francis, 2017. [Online]. Available: https://www.taylorfrancis.com/books/mono/10.1201/9781315255071/fram-functional-resonance-analysis-method-erik-hollnagel

[13] N. Leveson, "A new accident model for engineering safer systems," *Saf. Sci.*, vol. 42, no. 4, pp. 237–270, Apr. 2004.

[14] Z. H. Qureshi, "A review of accident modelling approaches for complex socio-technical systems," in *Proc. 12th Austral. Workshop Saf. Crit. Syst. Softw. Saf.-Related Program. Syst. (SCS)*, vol. 86. Adelaide, SA, Australia: Australian Computer Society, Inc., 2007, pp. 47–59.

[15] A. Hulme, N. A. Stanton, G. H. Walker, P. Waterson, and P. M. Salmon, "What do applications of systems thinking accident analysis methods tell us about accident causation? A systematic review of applications between 1990 and 2018," *Saf. Sci.*, vol. 117, pp. 164–183, Aug. 2019.

[16] M. Pillay, "Accident causation, prevention and safety management: A review of the state-of-the-art," *Proc. Manuf.*, vol. 3, pp. 1838–1845, 2015.

[17] G. Fu, X. Xie, Q. Jia, Z. Li, P. Chen, and Y. Ge, "The development history of accident causation models in the past 100 years: 24Model, a more modern accident causation model," *Process Saf. Environ. Protection*, vol. 134, pp. 47–82, Feb. 2020.

[18] H. J. Pasman, W. J. Rogers, and M. S. Mannan, "How can we improve process hazard identification? What can accident investigation methods contribute and what other recent developments? A brief historical survey and a sketch of how to advance," *J. Loss Prevention Process Industries*, vol. 55, pp. 80–106, Sep. 2018.

[19] P. Underwood and P. Waterson, "A critical review of the STAMP, FRAM and Accimap systemic accident analysis models," in *Advances in Human Aspects of Road and Rail Transportation*. U.K.: Taylor & Francis, Jan. 2016, pp. 385–394. [Online]. Available: https://www.taylorfrancis.com/chapters/edit/10.1201/b12320-45/critical-review-stamp-fram-accimap-systemic-accident-analysis-models-peter-underwood-patrick-waterson

[20] D. S. Kim and W. C. Yoon, "An accident causation model for the railway industry: Application of the model to 80 rail accident investigation reports from the UK," *Saf. Sci.*, vol. 60, pp. 57–68, Dec. 2013.

[21] M. Ahmadi Rad, L. M. Lefsrud, and M. T. Hendry, "Application of systems thinking accident analysis methods: A review for railways," *Saf. Sci.*, vol. 160, Apr. 2023, Art. no. 106066.

[22] A. Stelmach, I. Góra, and M. Zięba, "Application of risk assessment methods in rail transport," *WUT J. Transp. Eng.*, vol. 134, pp. 7–16, Jun. 2022.

[23] C.-L. Li, H.-H. Jung, S.-H. Oh, H.-S. Yun, and K.-S. Lee, "A study on hazard analysis techniques for railway signalling system," in *Proc. KSR Conf.*, 2011, pp. 232–238.

[24] M. Catelani, L. Ciani, D. Galar, G. Guidi, S. Matucci, and G. Patrizi, "FMECA assessment for railway safety-critical systems investigating a new risk threshold method," *IEEE Access*, vol. 9, pp. 86243–86253, 2021.

[25] N. G. Leveson, "Applying systems thinking to analyze and learn from events," *Saf. Sci.*, vol. 49, no. 1, pp. 55–64, Jan. 2011.

[26] N. G. Leveson, *System Safety Engineering: Back to the Future*. Cambridge, MA, USA: MIT Press, 2002. [Online]. Available: http://sunnyday.mit.edu/book2.pdf

[27] N. Leveson, *Engineering a Safer World: Systems Thinking Applied To Safety*. Cambridge, MA, USA: MIT Press, 2012.

[28] Y. Zhang, C. Dong, W. Guo, J. Dai, and Z. Zhao, "Systems theoretic accident model and process (STAMP): A literature review," *Saf. Sci.*, vol. 152, Aug. 2022, Art. no. 105596.

[29] N. G. Leveson and J. P. Thomas, *STPA Handbook*, Cambridge, MA, USA, 2018. [Online]. Available: http://psas.scripts.mit.edu/home/materials/

[30] N. G. Leveson, *CAST Handbook: How To Learn More From Incidents and Accidents*, Cambridge, MA, USA, 2019. [Online]. Available: http://psas.scripts.mit.edu/home/materials/

[31] H. Altabbakh, M. A. AlKazimi, S. Murray, and K. Grantham, "STAMP–holistic system safety approach or just another risk model?" *J. Loss Prevention Process Industries*, vol. 32, pp. 109–119, Nov. 2014.

[32] N. Leveson, "A systems approach to risk management through leading safety indicators," *Rel. Eng. Syst. Saf.*, vol. 136, pp. 17–34, Apr. 2015.

[33] N. Bugalia, Y. Maemura, and K. Ozawa, "Organizational and institutional factors affecting high-speed rail safety in Japan," *Saf. Sci.*, vol. 128, Aug. 2020, Art. no. 104762.

[34] W. Young and N. Leveson, "Systems thinking for safety and security," in *Proc. 29th Annu. Comput. Secur. Appl. Conf.*, Dec. 2013, pp. 1–8.

[35] F. Simone, A. J. N. Akel, G. D. Gravio, and R. Patriarca, "Thinking in systems, sifting through simulations: A way ahead for cyber resilience assessment," *IEEE Access*, vol. 11, pp. 11430–11450, 2023.

[36] D. Moher, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *Ann. Internal Med.*, vol. 151, no. 4, p. 264, Aug. 2009.

[37] R. Patriarca, M. Chatzimichailidou, N. Karanikas, and G. Di Gravio, "The past and present of system-theoretic accident model and processes (STAMP) and its associated techniques: A scoping review," *Saf. Sci.*, vol. 146, Feb. 2022, Art. no. 105566.

[38] M. R. Suryoputro, A. D. Sari, and R. D. Kurnia, "Preliminary study for modeling train accident in Indonesia using Swiss cheese model," *Proc. Manuf.*, vol. 3, pp. 3100–3106, 2015.

[39] N. Kudo, M. Hayashida, and Y. Sato, "A study on the applicability of STAMP for design safety assessment of railway signal system," in *Proc. Transp. Logistics Conf.*, 2021, pp. 4–6.

[40] L. Hongjie, T. Tao, J. Xiayao, and D. Heng, "Analysis of safety requirements of level crossings based on STPA method," *J. Beijing Jiaotong Univ.*, vol. 42, no. 2, pp. 84–90, 2018.

[41] L. Jintao, T. Tao, L. Zhao, and L. Liu, "Functional safety analysis of CTCS-3 train control system based on control relationship model," *J. China Railway Soc.*, vol. 8, pp. 36–43, Apr. 2015.

[42] J. Liu, T. Tang, and L. Zhao, "Functional safety analysis method of CTCS-3 level system based on STPA," *China Railway Sci.*, vol. 35, no. 5, pp. 86–95, 2014.

[43] J. Li, L. Zhao, Y. Wang, and L. Meng, "Study on method for identifying hazardous factors in CRES: EETD taken as an example," *China Saf. Sci. J.*, vol. 29, no. 1, p. 106, 2019.

[44] S.-H. Lee and S.-M. Shin, "Analysis on risk factors of platform screen door failure based on STPA," *J. Korean Soc. Railway*, vol. 24, no. 11, pp. 931–943, Nov. 2021.

[45] K. Hayashi and A. Komatsubara, "Evaluation on functional safety condition of railway crossing system using STAMP/STPA," *Hum. Factors Jpn.*, vol. 24, no. 1, pp. 3–10, 2019.

[46] Y. Takano and T. Kawano, "Application of STAMP/STPA to railway signalling system," IEICE, Tokyo, Japan, vol. 119, no. 100, pp. 13–16, 2019, Paper SSS2019-10. [Online]. Available: https://ken.ieice.org/ken/paper/20190625i1nx/eng/

[47] T. Kobayashi, Y. Sugimoto, R. Kouduki, N. Morishima, U. Singh, M. S. Krishna, and T. Mizuma, "Consideration of safety analysis application in railway signal system–safety analysis using FMEA, STAMP and HAZOP," IEICE, Tokyo, Japan, Tech. Rep., vol. 119, no. 351, pp. 7–10, 2019, Paper DC2019-79. [Online]. Available: https://ken.ieice.org/ken/paper/20191220B1sL/eng/

[48] K. Okano, S. Ogata, P. Yang, and K. Okamoto, "Model checking application to the railway crossing problem for STAMP/STPA using timed automaton," IEICE, Tokyo, Japan, vol. 117, no. 477, pp. 1–6, 2018, Paper SS2017-64. [Online]. Available: https://ken.ieice.org/ken/paper/20180306R1cM/eng/

[49] S. Kitamura, K. Sugiura, and T. Kawano, "STAMP/STPA analysis of train approach warning system and safety 2.0," Inst. Electron., Inf. Commun. Engineers (IEICE), vol. 119, no. 100, pp. 17–20, 2019, Paper SSS2019-11. [Online]. Available: https://ken.ieice.org/ken/paper/20190625i1n1/eng/

[50] T. Takata and H. Nakamura, "Applicability of methods for safety analysis of railway signaling," *J. Korean Soc. Railway*, vol. 22, no. 7, pp. 538–549, Jul. 2019.

[51] H. Yang and G. Kwon, "Identifying causes of an accident in STPA using the scenario table," *J. KIISE*, vol. 46, no. 8, pp. 787–799, Aug. 2019.

[52] Y. Sugimoto, T. Kobayashi, R. Kouzuki, N. Morishima, T. Mizuma, U. Singh, and M. S. Krishna, "Examination of safety evaluation method of railway signal system–combined use of FMEA, FTA and STPA," IEICE, Tokyo, Japan, Tech. Rep., vol. 119, no. 351, pp. 17–20, 2019, Paper DC2019-81. [Online]. Available: https://ken.ieice.org/ken/paper/20191220f1sL/eng/

[53] Y. Zha, D. Zhong, and R. Sun, "An interactive fault detection method for cyber-physical system based on system-theoretic process analysis," in *Proc. 2nd Int. Conf. Mech., Electron., Electr. Autom. Control (METMS)*, Apr. 2022, pp. 944–949.

[54] W. Haitao and L. Shuangxi, "High-speed railway emergency dispatching safety analysis based on STAMP/STPA," *China Saf. Sci. J.*, vol. 31, no. 6, p. 113, 2021.

[55] Q. Xu and J.-T. Lin, "Safety requirement verification of train-centric CBTC by integrating STPA with coloured Petri net," *Int. J. Ind. Syst. Eng.*, vol. 43, no. 2, pp. 168–189, 2023.

[56] S. D. Ota, "Assuring safety in high-speed magnetically levitated (Maglev) systems: The need for a system safety approach," Ph.D. thesis, Massachusetts Inst. Technol., Cambridge, MA, USA, 2008.

[57] M. Ouyang, L. Hong, M.-H. Yu, and Q. Fei, "STAMP-based analysis on the railway accident and accident spreading: Taking the China–Jiaoji railway accident for example," *Saf. Sci.*, vol. 48, no. 5, pp. 544–555, Jun. 2010.

[58] Y. Zhang, W. Shao, M. Zhang, H. Li, S. Yin, and Y. Xu, "Analysis 320 coal mine accidents using structural equation modeling with unsafe conditions of the rules and regulations as exogenous variables," *Accident Anal. Prevention*, vol. 92, pp. 189–201, Jul. 2016.

[59] R. Wang, W. Zheng, C. Liang, and T. Tang, "An integrated hazard identification method based on the hierarchical colored Petri net," *Saf. Sci.*, vol. 88, pp. 166–179, Oct. 2016.

[60] P. M. Salmon, G. J. M. Read, G. H. Walker, N. Goode, E. Grant, C. Dallat, T. Carden, A. Naweed, and N. A. Stanton, "STAMP goes EAST: Integrating systems ergonomics methods for the analysis of railway level crossing safety management," *Saf. Sci.*, vol. 110, pp. 31–46, Dec. 2018.

[61] O. F. Hamim, S. Hasanat-E-Rabbi, M. Debnath, M. S. Hoque, R. C. McIlroy, K. L. Plant, and N. A. Stanton, "Taking a mixed-methods approach to collision investigation: AcciMap, STAMP-CAST and PCM," *Appl. Ergonom.*, vol. 100, Apr. 2022, Art. no. 103650.

[62] T. Takata, A. Asano, and H. Nakamura, "Safety assessment of closed-loop level crossing control systems by means of STAMP (systems-theoretic accident model and processes)," *J. Traffic Transp. Eng.*, vol. 6, no. 5, pp. 241–254, Oct. 2018.

[63] T. Takata, A. Asano, and H. Nakamura, "Interlocking system for CBTC (communication based train control) system," *J. Traffic Transp. Eng.*, vol. 7, no. 4, pp. 145–156, Aug. 2019.

[64] A. J. Nakhal Akel, G. Di Gravio, L. Fedele, and R. Patriarca, "Learning from incidents in socio-technical systems: A systems-theoretic analysis in the railway sector," *Infrastructures*, vol. 7, no. 7, p. 90, Jun. 2022.

[65] P. Underwood and P. Waterson, "Systems thinking, the Swiss cheese model and accident analysis: A comparative systemic analysis of the Grayrigg train derailment using the ATSB, AcciMap and STAMP models," *Accident Anal. Prevention*, vol. 68, pp. 75–94, Jul. 2014.

[66] Z. Zhang, X. Liu, and H. Hu, "Passenger rail station safety improvement and analysis of end-of-track collisions based on systems-theoretic accident modeling and processes (STAMP)," *Smart Resilient Transp.*, vol. 3, no. 2, pp. 94–117, Aug. 2021.

[67] J. Zhao, F. Yang, Y. Guo, and X. Ren, "A CAST-based analysis of the metro accident that was triggered by the zhengzhou heavy rainstorm disaster," *Int. J. Environ. Res. Public Health*, vol. 19, no. 17, p. 10696, Aug. 2022.

[68] X. Han, T. Tang, and J. Lv, "A hierarchical verification approach to verify complex safety control systems based on STAMP," *Sci. Comput. Program.*, vol. 172, pp. 117–134, Mar. 2019.

[69] M. Takahashi, Y. Anang, and Y. Watanabe, "A hazard analysis method for embedded control software with STPA," *Trends Comput. Sci. Inf. Technol.*, vol. 5, no. 1, pp. 82–96, 2020.

[70] S. Zhang, T. Tang, and J. Liu, "A hazard analysis approach for the SOTIF in intelligent railway driving assistance systems using STPA and complex network," *Appl. Sci.*, vol. 11, no. 16, p. 7714, Aug. 2021.

[71] B. Zhao and T. Tang, "A hybrid system dynamics modeling method for organizational factors in fully automatic operation system," *Int. J. Hybrid Inf. Technol.*, vol. 8, no. 12, pp. 97–116, Dec. 2015.

[72] A. V. Ozerov and A. M. Olshansky, "Safety model construction for a complex automatic transportation system," *Dependability*, vol. 21, no. 2, pp. 31–37, Jun. 2021.

[73] R. Dunsford and M. Chatzimichailidou, "Introducing a system theoretic framework for safety in the rail sector: Supplementing CSM-RA with STPA," *Saf. Rel.*, vol. 39, no. 1, pp. 59–82, Jan. 2020.

[74] J. T. Liu, T. Tang, J. B. Zhu, and L. Zhao, "An extended system-theoretic hazard analysis method for the safety of high-speed railway train control systems," *Proc. Inst. Mech. Engineers, F, J. Rail Rapid Transit*, vol. 231, no. 8, pp. 821–834, Sep. 2017.

[75] G. J. M. Read, A. Naweed, and P. M. Salmon, "Complexity on the rails: A systems-based approach to understanding safety management in rail transport," *Rel. Eng. Syst. Saf.*, vol. 188, pp. 352–365, Aug. 2019.

[76] M. Li, F. Yan, R. Niu, and N. Xiang, "Identification of causal scenarios and application of leading indicators in the interconnection mode of urban rail transit based on STPA," *J. Rail Transp. Planning Manage.*, vol. 17, Mar. 2021, Art. no. 100238.

[77] F. Yan, J. Ma, M. Li, R. Niu, and T. Tang, "An automated accident causal scenario identification method for fully automatic operation system based on STPA," *IEEE Access*, vol. 9, pp. 11051–11064, 2021.

[78] M. Takahashi, D. Morimoto, Y. Anang, and Y. Watanabe, "A proposal of hazard analysis method using structured system theoretical process analysis," *SICE J. Control, Meas., Syst. Integr.*, vol. 16, no. 1, pp. 192–202, Dec. 2023.

[79] R. Niu, Y. Cao, X. Ge, and T. Tang, "Applying system thinking to learn from accident of modern automatic control systems," *Chin. J. Electron.*, vol. 23, no. 2, pp. 409–414, 2014.

[80] D. Suo, "A system theoretic analysis of the '7.23'Yong-Tai-Wen railway accident," in *Proc. 1s STAMP Workshop*, Cambridge, MA, USA. MIT, 2012, pp. 1–22.

[81] T. Song, D. Zhong, and H. Zhong, "A STAMP analysis on the China-Yongwen railway accident," in *Proc. 31st Int. Conf. Comput. Saf., Rel., Secur. (SAFECOMP)*, Magdeburg, Germany. Berlin, Germany: Springer-Verlag, Sep. 2012, pp. 376–387.

[82] L. Chen, Y. Zhao, and T. Zhao, "An AcciMap analysis on the China-Yongwen railway accident," in *Proc. 8th World Congr. Eng. Asset Manag. (WCEAM) 3rd Int. Conf. Utility Manag. Safety (ICUMAS)*. Cham, Switzerland: Springer, 2015, pp. 1247–1253.

[83] Q. Zhan, W. Zheng, and B. Zhao, "A hybrid human and organizational analysis method for railway accidents based on HFACS-railway accidents (HFACS-RAs)," *Saf. Sci.*, vol. 91, pp. 232–250, Jan. 2017.

[84] A. Dong, "Application of CAST and STPA to railroad safety in China," Ph.D. thesis, Massachusetts Inst. Technol., Cambridge, MA, USA, 2012.

[85] S. Dirk, H. R. Sebastian, J. Welte, and E. Schnieder, "Integration of Petri nets into STAMP/CAST on the example of Wenzhou 7.23 accident," in *Proc. 1st IFAC Workshop Adv. Control Automat. Theory Transp. Appl.*, 2013, pp. 65–70.

[86] R. Slovák, "Methodische modellierung und analyse von sicherungssystemen des eisenbahnverkehrs," Ph.D. thesis, Fakultät für Maschinenbau, Technische Universität Dresden, Braunschweig, Germany, 2006.

[87] *Rail accident Report: Derailment at Grayrigg 23 February 2007*, Rail Accident Invest. Branch Dept. Transp. Derby., Derby, U.K., 2011.

[88] *Analysis, Causality and Proof in Safety Investigations*, Australian Transport Safety Bureau, Canberra, ACT, Australian, 2008.

[89] Y. Zhou and F. Yan, "Causal analysis to a subway accident: A comparison of STAMP and RAIB," in *Proc. MATEC Web Conf.*, vol. 160, 2018, p. 05002.

[90] F. Yan, T. Tang, and J. Ma, "An accident casual model for railway based on operational scenario cognition conflict," in *Proc. Int. Conf. Intell. Rail Transp. (ICIRT)*, Dec. 2018, pp. 1–5.

[91] G. Kedjela, "Development of safety control structure of Addis Ababa light rail transit using systemtheoretic approach," Ph.D. thesis, School Mech. Ind. Eng., Under Railway Mech. Eng. Stream, Addis Ababa Inst. Technol., Addis Ababa Univ., Addis Ababa, Ethiopia, 2015.

[92] M. W. Albert, "Investigation of complex accidents in the digitalised railway sector–A case study to investigate accidents involving the European rail traffic management system (ERTMS)," Master's thesis, NTNU, Trondheim, Norway, Tech. Rep., 2019. [Online]. Available: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2634920

[93] H. Yang, L. Zhao, and J. Chen, "Metro system inundation in zhengzhou, Henan province, China," *Sustainability*, vol. 14, no. 15, p. 9292, Jul. 2022.

[94] Y. Qi, Y. Cao, and Y. Sun, "Safety analysis on typical scenarios of GTCS based on STAMP and STPA," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 768, Jul. 2020, Art. no. 042042.

[95] F. Yan, S. Zhang, and T. Tang, "Autonomous train operational safety assurance by accidental scenarios searching," in *Proc. IEEE Intell. Transp. Syst. Conf. (ITSC)*, Oct. 2019, pp. 3488–3495.

[96] S. Lu, R. Niu, and T. Tang, "Scenarios oriented safety analysis of fully automatic operation metro," in *Proc. Int. Conf. Intell. Rail Transp. (ICIRT)*, Dec. 2018, pp. 1–5.

[97] A. Z. Hao, B. F. Yan, and C. R. Niu, "A key step to virtual coupling," in *Proc. IEEE 23rd Int. Conf. Intell. Transp. Syst. (ITSC)*, Sep. 2020, pp. 1–6.

[98] Y. Zhang and Y. Liu, "Application of STPA in temporary speed restriction sending scenario of train control system based on vehicle-vehicle communication," in *Proc. 5th Int. Conf. Control Sci. Syst. Eng. (ICCSSE)*, Aug. 2019, pp. 99–103.

[99] L. M. Castiglione and E. C. Lupu, "Hazard driven threat modelling for cyber physical systems," in *Proc. Joint Workshop CPS IoT Secur. Privacy*, Nov. 2020, pp. 13–24.

[100] Z. Yong and L. Shachen, "STPA based safety analysis of regional data center in CTCS-1 train control system," in *Proc. IEEE Int. Conf. Saf. Produce Informatization (IICSPI)*, Dec. 2018, pp. 240–245.

[101] W. Song, F. Yan, M. Zhang, and P. Wang, "Safety analysis research of train integrity based on STPA," in *Proc. Int. Conf. Electr. Inf. Technol. Rail Transp.* Singapore: Springer, 2022, pp. 297–305.

[102] D. L. Gurgel, C. M. Hirata, and J. De M. Bezerra, "A rule-based approach for safety analysis using STAMP/STPA," in *Proc. IEEE/AIAA 34th Digit. Avionics Syst. Conf. (DASC)*, Sep. 2015, pp. 7B2-1–7B2-8.

[103] R. Tiusanen, E. Heikkilä, T. Välisalo, and T. Malm, "Safety analyses on the use of tram doors in GoA1 and GoA4 autonomy levels," Saf. Complex sociotechnical Syst., VTT Tech. Res. Centre, Finland, Tech. Rep. VTT-R-00499-23, 2023.

[104] E. M. Roth, J. Multer, M. France, H. Safar, and R. Grice, "Understanding why railroad yard crews run through misaligned switches through the lens of sociotechnical systems," in *Proc. Hum. Factors Ergonom. Society Annual Meeting*. Los Angeles, CA, USA: SAGE, vol. 62, 2018, pp. 1853–1857.

[105] H. Safar, E. Roth, J. Multer, M. France, "Why do passenger trains run through switches in the rail yard?" Office of Res., Develop. Technol., Washington, DC, USA, Tech. Rep. DOT-VNTSC-FRA-16-07, 2019.

[106] *Road Vehicles—Safety of the Intended Functionality*, Standard, International Organization for Standardization, Geneva, 2022.

[107] F. Yan, T. Tang, and H. Yan, "Scenario based STPA analysis in automated urban guided transport system," in *Proc. IEEE Int. Conf. Intell. Rail Transp. (ICIRT)*, Aug. 2016, pp. 425–431.

[108] A. Abdulkhaleq and S. Wagner, "A controlled experiment for the empirical evaluation of safety analysis techniques for safety-critical software," in *Proc. 19th Int. Conf. Eval. Assessment Softw. Eng.*, Apr. 2015, pp. 1–10.

[109] T. La-Ngoc and G. Kwon, "Comparing the effectiveness of SFMEA and STPA in software-intensive railway level crossing system," in *Proc. Adv. Comput. Sci. Ubiquitous Comput. (CSA-CUTE)*. Singapore: Springer, 2018, pp. 1281–1288.

[110] M. M. Chatzimichailidou and I. M. Dokas, "RiskSOAP: Introducing and applying a methodology of risk self-awareness in road tunnel safety," *Accident Anal. Prevention*, vol. 90, pp. 118–127, May 2016.

[111] S. Guo, X. Zhou, B. Tang, and P. Gong, "Exploring the behavioral risk chains of accidents using complex network theory in the construction industry," *Phys. A, Stat. Mech. Appl.*, vol. 560, Dec. 2020, Art. no. 125012.

[112] M. I. Harrison, *Diagnosing Organizations: Methods, Models, and Processes*, vol. 8, 3rd ed., Newbury Park, CA, USA: Sage, 2005. [Online]. Available: https://us.sagepub.com/en-us/nam/diagnosing-organizations/book226749#description

[113] T. La-Ngoc and G. Kwon, "Risk assessment for STPA with FMEA technique," in *Proc. Int. Conf. Frontier Comput.* Singapore: Springer, 2019, pp. 444–455.

[114] M. Chen, L. Wang, J. Hu, and T. Feng, "An extraction method of STPA variable based on four-variable model," in *Proc. 3rd Int. Conf. Intell., Interact. Syst. Appl. (IISA3)*. Cham, Switzerland: Springer, 2019, pp. 375–381.

[115] W. G. Temple, Y. Wu, B. Chen, and Z. Kalbarczyk, "Systems-theoretic likelihood and severity analysis for safety and security co-engineering," in *Proc. 2nd Int. Conf. Rel., Saf., Secur. Railway Systems. Model., Anal., Verification, Certification (RSSRail)*, Kalba, Italy. Springer, Nov. 2017, pp. 51–67.

[116] C. Schmittner, T. Gruber, P. Puschner, and E. Schoitsch, "Security application of failure mode and effect analysis (FMEA)," in *Proc. 33rd Int. Conf. Comput. Saf., Rel., Security (SAFECOMP)*, Florence, Italy. Cham, Switzerland: Springer, Sep. 2014, pp. 310–325.

[117] A. Altaf, S. Faily, H. Dogan, E. Thron, and A. Mylonas, "Integrated design framework for facilitating systems-theoretic process analysis," in *Proc. Eur. Symp. Res. Comput. Secur.* Cham, Switzerland: Springer, 2022, pp. 58–73.

[118] S. Hu, D. Wu, and H. Wang, "Safety analysis of train control system based on colored Petri nets and system-theoretic process analysis," in *Proc. 3rd Int. Conf. Electr. Inf. Technol. for Rail Transp. (EITRT) Transp.* Singapore: Springer, 2018, pp. 175–184.

[119] Q. Xu and J. Lin, "Safety analysis of communication-based train control system by STPA and colored Petri Net," in *Proc. Int. Cyberspace Congr., CyberDI and CyberLife*, Beijing, China. Singapore: Springer, Dec. 2019, pp. 433–449.

[120] R. Wang and W. Zheng, "Research and application of the BFM-STAMP hazard analysis method," in *Proc. IEEE Int. Conf. Intell. Rail Transp.*, Aug. 2013, pp. 174–178.

[121] S. Kawakami, "Application of a systems-theoretic approach to risk analysis of high-speed rail project management in the US," Ph.D. thesis, Massachusetts Inst. Technol., Cambridge, MA, USA, 2014.

[122] M. M. Rekabi, "Bayesian safety analysis of railway systems with driver errors," Master's thesis, Dept. Mech. Ind. Eng., NTNU, Trondheim, Norway, 2018.

[123] A. Thapaliya and G. Kwon, "Realization of combined systemic safety analysis of adverse train control system using model checking," in *Proc. Int. Conf. Frontier Comput.* Singapore: Springer, 2019, pp. 419–430.

[124] M. Takahashi, Y. Anang, and Y. Watanabe, "A proposal for a hazard analysis method for embedded control software using STAMP," in *Proc. SICE*, 2019, pp. 595–600.

[125] J. Liu, H. Wang, and W. Zheng, "A safety modelling method for high-speed train control systems based on UML extension," in *Proc. Chin. Autom. Congr. (CAC)*, 2020, pp. 317–321.

[126] S. Yin and D. Zhong, "Research on methodology for safety generation and verification," in *Proc. Int. Conf. Mech. Sci., Electric Eng. Comput. (MEC)*, Dec. 2013, pp. 2182–2186.

[127] P. Yang, R. Karashima, K. Okano, and S. Ogata, "Automated inspection method for an STAMP/STPA–fallen barrier trap at railroad crossing," *Proc. Comput. Sci.*, vol. 159, pp. 1165–1174, 2019.

[128] K. Okano, P. Yang, S. Ogata, and K. Okamoto, "Deriving of time constants in timed automata for hazard transition sequences for STAMP/STPA," *Proc. Comput. Sci.*, vol. 176, pp. 1392–1401, 2020.

[129] M. Tsuji, T. Takai, K. Kakimoto, N. Ishihama, M. Katahira, and H. Iida, "Prioritizing scenarios based on STAMP/STPA using statistical model checking," in *Proc. IEEE Int. Conf. Softw. Test., Verification Validation Workshops (ICSTW)*, Oct. 2020, pp. 124–132.

[130] D. Grivicic, "Can STAMP provide a complete safety argument?" Master's thesis, School Humanities, Lang. Social Sci., Griffith Univ., Nathan, QLD, Australia, 2019.

[131] Y. Toda, Y. Matsubara, and H. Takada, "FRAM/STPA: Hazard analysis method for FRAM model," in *Proc. FRAM Workshop Cardiff, Wales*, 2018, pp. 1–17.

[132] C. Hirata and S. Nadjm-Tehrani, "Combining GSN and STPA for safety arguments," in *Proc. Comput. Saf., Rel., Security: SAFECOMP*. Cham, Switzerland: Springer, 2019, pp. 5–15.

[133] Z. Li, D. Zhong, R. Sun, and H. Wang, "Extend STPA method using hybrid dynamic theory," in *Proc. Int. Conf. Dependable Syst. Their Appl. (DSA)*, Oct. 2017, pp. 137–142.

[134] A. Zeleskidis, I. M. Dokas, and B. Papadopoulos, "A novel real-time safety level calculation approach based on STPA," in *Proc. MATEC Web Conf.*, vol. 314, 2020, p. 01001.

[135] D. Zhong, N. Wu, Q. Wang, and R. Sun, "A multi-view extended software control structure modeling and safety analysis method," in *Proc. Prognostics Syst. Health Manage. Conf. (PHM)*, Oct. 2015, pp. 1–5.

[136] S. B. N. Hansen, "SafeT-next generation safety assessment framework for railway: Development of a framework for the practical implementation and facilitation of STPA," Master's thesis, Norges Teknisk-Naturvitenskapelige Universitet, Trondheim, Norway, 2018.

[137] F. G. R. d. Souza, C. M. Hirata, and S. Nadjm-Tehrani, "Synthesis of a controller algorithm for safety-critical systems," *IEEE Access*, vol. 10, pp. 76351–76375, 2022.

[138] A. Abdulkhaleq, S. Wagner, and N. Leveson, "A comprehensive safety engineering approach for software-intensive systems based on STPA," *Procedia Eng.*, vol. 128, pp. 2–11, 2015.

[139] B. Bérard, M. Bidoit, A. Finkel, F. Laroussinie, A. Petit, L. Petrucci, and P. Schnoebelen, *Systems and Software Verification: Model-Checking Techniques and Tools*. Berlin, Germany: Springer, 2013.

[140] K. G. Larsen, P. Pettersson, and W. Yi, "Uppaal in a nutshell," *Int. J. Softw. Tools Technol. Transf.*, vol. 1, nos. 1–2, pp. 134–152, Dec. 1997.

[141] A. Biere, M. Heule, and H. van Maaren, *Handbook of Satisfiability*, vol. 185. Amsterdam, The Netherlands: IOS Press, 2009.

[142] N. G. Leveson, "Intent specifications: An approach to building human-centered specifications," *IEEE Trans. Softw. Eng.*, vol. 26, no. 1, pp. 15–35, Aug. 2000.

[143] N. A. Stanton, P. M. Salmon, L. A. Rafferty, G. H. Walker, C. Baber, and D. P. Jenkins, *Human Factors Methods: A Practical Guide for Engineering and Design*, 2nd ed., CRC Press, 2013, doi: 10.1201/9781315587394. [Online]. Available: https://www.taylorfrancis.com/books/mono/10.1201/9781315587394/human-factors-methods-daniel-jenkins-paul-salmon-guy-walker-chris-baber-laura-rafferty-neville-stanton

ABHIMANYU TONK received the bachelor's degree in electronics and instrumentation from Amity University Noida, the master's degree in health safety and environment from the University of Petroleum and Energy Studies, Dehradun, and the Mastère Spécialisé degree in safety engineering and management from the Institut National des Sciences Appliquées de Toulouse, France. He is currently pursuing the Ph.D. degree with Université Gustave Eiffel. He began his career as a Health Safety Environment and Industrial Risk Engineer at Suez India Pvt. Ltd., later undertaking internships with Oil and Natural Gas Corporation of India and EasyMile SAS, Toulouse, France. He is a Safety Research Engineer with the Technological Research Institute Railenium, Valenciennes, France. His research interests include safety assurance of autonomous transportation systems, AI safety, functional safety, and dependability engineering, with a particular emphasis on railway control command and signaling systems.

ABDERRAOUF BOUSSIF received the B.Eng. degree in system control engineering from the Polytechnic High School, Algiers, Algeria, in 2012, the master's degree in complex systems engineering from the École Normale Supérieure de Cachan, Paris, in 2013, and the Ph.D. degree in safety system engineering from the University of Lille, France, in 2016. He is currently a Research Associate with the Evaluation and Safety of Automated Transport Systems Research Team (COSYS/ESTAS), Université Gustave Eiffel. His research interests include dependability and safety assurance of railway systems, formal methods, MBSA, and AI safety, with a particular emphasis on railway control command and signaling systems.