International Journal of Advanced Research in Engineering Innovation
e-ISSN: 2682-8499 | Vol. 4, No. 1, 23-34, 2022
http://myjms.mohe.gov.my/index.php/ijarei

Hazard Analysis Techniques, Methods and Approaches: A Review

Kiriyadhatshini Gunaratnam[1*], Azma Abdullah[1], Rohani Abu Bakar[1], Fadhl Hujainah[2]

[1] College of Computing and Applied Sciences, Universiti Malaysia Pahang (UMP), Pahang, Malaysia
[2] Computer Science and Engineering, Department Chalmers and University of Gothenburg, Gothenburg, Sweden

*Corresponding Author: kiriyadatshini@gmail.com

Accepted: 15 March 2022 | Published: 1 April 2022

DOI: https://doi.org/10.55057/ijarei.2022.4.1.3

Abstract: *Hazard analysis (HA) is an indispensable task during the specification and development of safety-critical systems. It involves identifying potential forms of harm, their effects, causal factors, and the level of risk associated with them. Systems are always vulnerable to mishaps, hazards, or risks that result in system failures, resulting in injuries, loss, and damage. Even though previous studies have made a significant contribution to the study of hazard analysis, little effort has been made to give an overview of the common HA techniques, highlighting their responsibilities, advantages, and disadvantages. Thus, this paper aims to focus on and feature the existing HA techniques along with their respective functions. An overall picture of the advantages and disadvantages of listed HA techniques is presented as well in this paper. Such a study may be utilized as a guide to aid researchers and practitioners in understanding hazard analysis. The investigation is conducted using a process-oriented approach that consists of three steps: formulation of the research questions, the gathering of related studies, and the analysis of the extracted studies. The study revealed a total of 22 HA techniques. A further study is to propose and carry out a systematic literature review to identify to what extent the hazard analysis techniques have been implemented and evaluated in case studies.*

Keywords: hazard analysis, hazard analysis techniques, safety-critical system

---

1. Introduction

In a safety-critical system (SCS), Although the term "safety-critical system" (SCS) has various meanings, the intuitive concept works well. Failure's consequences are a source of concern, both intuitively and formally. A system is considered safety-critical if its failure could have unacceptably severe consequences [59]. In other words, a safety-critical system is one whose failure could result in the loss of human lives or serious injury, severe injury or loss of expensive and sensitive instrumentation, or the release of pollutants, nuclear radiation, and wastes that could harm the environment severely [45], which is a term that means "any real or possible condition that could result in injury, sickness, or death to personnel; loss of a system, equipment, or proper" [4].

A hazard is a condition in which people, or the environment are in danger, either directly or indirectly. A state or collection of conditions in a system that, when combined with other conditions in the system's surroundings, ultimately leads to an accident [5,6]. The severity, damage, and probability are two fundamental criteria of danger [4]. The worst potential accident that could occur as a result of the hazard in its most unfavorable state is characterized as hazard severity, whereas hazard probability of occurrence can be specified subjectively or statistically [4]. Hazards are present for one of two reasons: they are either unavoidable because hazardous elements must be used in the system, or they are the result of inadequate design safety considerations [4]. Inadequate design safety consideration is caused by poor or insufficient design, or the wrong implementation of a competent design, which includes neglecting to address the consequences of hardware failures, sneak paths, software defects, human errors, and other issues [4].

Meanwhile, Hazard analysis is the process of observing a system or subsystems to identify each potential hazard that could occur, and it must be done early in the system's development. Hazard analysis is used to ensure that a system does not provide an unacceptable risk to its end-user or the environment in which it is installed [2,3]. Hazard analysis can be performed using a variety of methodologies, each of which provides a unique perspective on the characteristics of the system under consideration. Apart from that, hazard analysis plays a significant role in ensuring and maintaining the safety and security level by understanding how, when, and where hazards can be identified and holding up a proper control measure by applying the usage of HA methods or techniques. [4,29].

Ignoring the execution of hazard analysis can cause serious issues that are related to either software or hardware damage, which also affect the scheduled operation and the quality of human workload. Therefore, the purpose of this research is to examine, analyze, and describe safety-critical systems, hazards, hazard analysis, and the existing hazard analysis techniques for finding hazards along with their respective pros and cons.

The rest of this paper is organized as follows. Section 2 presents the background of the terms of hazards in hazard analysis, while Section 3 explains the research methodology. Section 4 presents the findings and discussion of RQ1 and RQ2, while Section 5 concludes the paper.

2. Background

To obtain an overall picture of the adopted terms used in hazard analysis in the safety-critical system to ensure uniformity throughout this paper, we present the following definitions, organized in alphabetical order:

Error: Inconsistency between a computed, determined, or measured value or condition and its real, specified, or theoretically correct counterpart [4,20,28,31,32].
Failure: When an intended function is terminated or incomplete, the event happens [4,20,28,31,32].
Fault: The inability to conduct a required operation, barring the absence of preventative maintenance or other planned measures, or due to a lack of external resources, defines the status of an associate degree item [4,20,28,31,32].
Hazard: Any actual or potential situation that could result in personnel injury, illness, or death; damage to or loss of a system, equipment, or property; or harm to the environment [4,20,28,32].
Mishap: An unforeseen occurrence or chain of events that result in death, injury, disease, equipment or property damage or loss, or environmental harm [4,20,28,32].

These terms listed above might differ in their severity or other factors, yet they end up with similar consequences.

3. Research Methodology

The research method used consists of three steps as shown in figure 1 below:

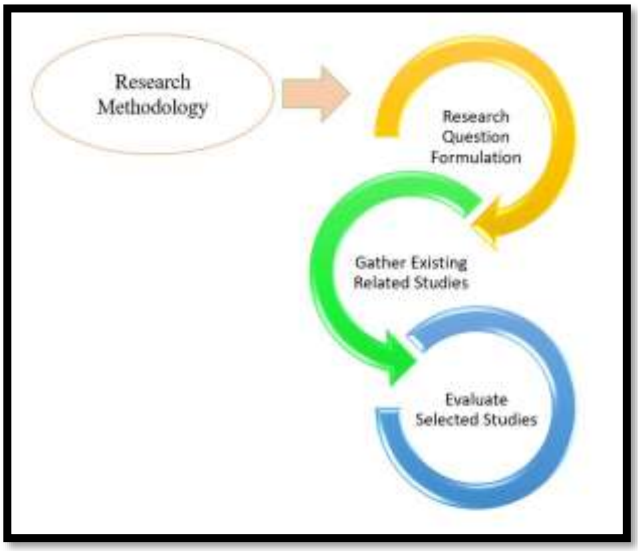

Figure 1: Three Steps in Research Methodology

This study aims to review, analyze, and summarize hazard analysis techniques in safety-critical systems. A pair of research questions were formulated to support this aim, as shown in Table 1.

Table 1: Research Questions

Research Questions	Motivation	Findings
RQ1: What are the existing hazard analysis techniques in safety-critical systems?	To reveal the existing techniques that are focused particularly on identifying and mitigating hazards in safety-critical systems.	22 hazard analysis techniques are tabulated in section 4 (Table 2)
RQ2: What are existing hazard analysis techniques' respective descriptions, advantages, and disadvantages?	To reveal the basic descriptions of each stated HA technique and how they contribute to identifying hazards as well as their respective pros and cons in safety-critical systems.	Tabulated in section 4 (Table 3)

The selection of related studies is then carried out based on the above-mentioned research questions. The first step in this process is to create a keyword list. The search terms in this paper were created using a step-by-step procedure that included: (1) defining key terms based on research questions, (2) defining alternate synonyms of defined key terms, (3) validating search terms in any relevant research sample, and finally (4) combining these strings with Boolean operators (AND/OR) to make the search process more specific and extend the search process. We specified the mentioned search phrases being used to search inside titles, keywords, abstracts, and full text of the papers discovered after all these rounds.

The following is the final list of search terms:
• (“hazard analysis” OR “hazard identification” OR “hazard assessment”) AND
• (“safety-critical system” OR “critical system”) AND
• (“hazard analysis techniques” OR “hazard analysis methods”) AND
• (“significance of hazard analysis” OR “importance of hazard analysis” OR “significance of hazard identification” OR “significance of hazard assessment” OR “importance or hazard identification” OR “importance of hazard assessment”)

A search for similar studies was conducted using a variety of electronic database services, including the IEEE Xplore digital library, Google Scholar, Springer, ScienceDirect, and Web of Science. Furthermore, only current studies that apply to the specified domain and use the specified research questions were considered during the collection of similar analysis phases. Finally, to obtain the results, the review of related studies was completed by collecting data from relevant studies that could address the study questions within the year of publications range of 1970 to 2021.

4. Findings and Discussion

To address the listed research questions, each technique was revealed and analyzed critically concerning its descriptions, advantages, and disadvantages.

I. RQ1: What are the existing hazard analysis techniques in safety-critical systems?

The list of existing HA techniques in the safety-critical system is shown in table 2 below along with their respective years of extracted studies:

Table 2: HA Technique and Respective Years of Retrieved Studies

HA Techniques	Years
Fault Tree Analysis (FTA)	1999, 2010, 2011, 2013, 2014, 2017
Failure Modes and Effect Analysis (FMEA)	2010, 2013, 2014, 2017, 2019
Systems-Theoretic Accident Modelling and Process (STAMP)	2013, 2017, 2019
Software Hazard Analysis and Resolution in Design (SHARD)	2002, 2018
Hazard and Operability Analysis (HAZOP)	2010, 2017, 2018
Computer Hazard and Operability Studies (CHAZOP)	1998, 2010
System Theoretic Process Analysis (STPA)	2013, 2014, 2017, 2019
Error Model Annex	2014, 2017
Functional Hazard Analysis (FHA)	2016, 2017
STAMP hazard analysis Based on Formalization Model (BFM-STAMP)	2013, 2016
Hazard Analysis of Systems of Systems (SimHAZAN)	2000, 2013
Situation-based Qualitative Modelling and Analysis (SQMA)	1995
Hazardous Control Action Tree STPA (HCAT-STPA)	2004, 2019
Preliminary Hazard Analysis (PHA)	2016, 2017, 2018
Resilience-based Integrated Process Systems Hazard Analysis (RIPSHA)	2018
Probabilistic Seismic Hazard Analysis (PSHA)	1970, 2010
Deductive Cause-Consequences Analysis (DCCA)	2006, 2014
Software Hazard Analysis (SWHA)	2012, 2017, 2019
Early Warning Sign Analysis based on the STPA (EWaSAP)	2009, 2013
Process Failure Mode and Effect Analysis (PFMEA)	2017, 2018, 2019
Architecture-level hazard analysis using AADL	2014
Root-State Hazard Identification (RSHI)	2021

II. RQ2: What are existing hazard analysis techniques' respective descriptions, advantages, and disadvantages?

This research question has been answered by presenting the HA techniques' respective descriptions, advantages, and disadvantages in table 3 below:

Table 3: HA Techniques, Descriptions, Advantages, and Disadvantages

Techniques	Description	Advantages	Disadvantages
Fault Tree Analysis (FTA) [6,16,17,35,36,37]	During the design stage, deductive safety analysis and a top-down approach are used. It uses tree traces to find component problems.	• Estimate the probability of the top event occurring.	• Requires the engagement of a high-level professional expert to input the stakeholder's weight • Techniques' results are not commonly recognized
Failure Modes and Effect Analysis (FMEA) [7,15,16,17,38,39]	The bottom-up analysis method is used to determine potential failure modes with causes for all elements in a system to search out negative effects.	• Tracing all conceivable outcomes of component failures, as well as all possible environmental and system states	• Not suitable for early stages of analysis • Analysis is limited to analyzing only a single cause of an effect • Tends to focus on technological failures • Not ideal for computer-controlled systems because the control logic is ignored
Systems-Theoretic Accident Modelling and Process (STAMP) [8,17,30,36]	Identify the controls and response loops that ensure safe operation and verify that they have not allowed future accidents to intervene.	• Considers safety and security considerations	• Inability to precisely characterize component interactions, which limits the elicitation of component-interaction-related requirements
Software Hazard Analysis and Resolution in Design (SHARD) [9,56]	Analyze designs to determine system safety requirements for elaborated design development.	• It's considered to be useful for looking into the safety elements of a range of computer-based systems.	• May cause manufacturers to assume that their hazard assessment is complete when it is not, thus jeopardizing their responsibility and exposing their products to public risk.
Hazard and Operability Analysis (HAZOP) [3,10,43,44]	Investigates the system's dangers as well as its operability issues, as well as the consequences of any deviation from design circumstances.	• Determine how a process could depart from its original design goal.	• It's a time-consuming, expensive, and mostly human-centered procedure. • Does not evaluate failure modes as part of the FMECA process. • Does not consider the effects of external threats in detail.

Computer Hazard and Operability Studies (CHAZOP) [10,11]	Pondering the safety features of computer-controlled systems.	• A methodical investigation of software faults. Software and process control systems are subjected to a systematic application of a set of guiding words.	• It can be costly and time-consuming. There will be a significant number of computer systems to examine for a complex procedure.
System Theoretic Process Analysis (STPA) [7,12,15,36]	Analyze sociotechnical systems that are large and complex. Appropriate for use in the initial stages of safety-guided design.	• Considers the evaluated system and its components as a series of interconnected control loops, considering system component interactions. • Assists in recognizing the interconnections between system components • Allows for the discovery of additional scenarios involving component interactions	• Lacks a sound formal methodology • Human-centred process • Designing new countermeasures and evaluating existing ones can be difficult and identifying causal elements can be tough.
Error Model Annex [13,46]	It solely identifies error events and states and is used in embedded system safety assessments.	• Support safety analysis methodologies with analyzable architecture fault models to automate them.	• The relationship between risks cannot be displayed; only the error occurrences and states inside and between components can be described.
Functional Hazard Analysis (FHA) [14,45]	Inductive, qualitative method. It specifies the functions of the system as well as the repercussions of failures.	• It may be used to assess all types of systems, equipment, and software. • It can be used to implement a single subsystem, a complete working system, or a collection of systems. • The level of depth in the study may vary depending on the degree of functions being evaluated.	• It is not as methodical as it is for single failures. The analyst must choose which failure combinations to employ.
STAMP hazard analysis Based on Formalization Model (BFM-STAMP) [17,49]	To evaluate socio-technical control structure models, discover risks, and generate hazard logs, we combined STAMP hazard analysis with the formalization method of colored Petri nets.	• All subsystem failures and interactions that stray from design assumptions, as well as human errors and socio-technical drawbacks, are included.	• It is not suitable for early-stage analysis
Hazard Analysis of Systems of Systems (SimHAZAN) [18,50,51]	Includes a systematic modelling procedure as well as a separate analytic strategy that should be applied to models created through that process as well as models created through other means.	• The advantages of SimHAZAN are particularly apparent in SoS, where the intricacy makes manual analysis approaches difficult to employ.	• Generates a large amount of output data
Situation-based Qualitative Modelling and Analysis (SQMA) [19,52]	On the component level, it allows for the systematic determination and description of effects and states.	• Any potential hazards caused by malfunctioning parts can be discovered	• Only considers qualitative arithmetic and situations.

		by including hypothetical component breakdowns.	
Hazardous Control Action Tree STPA (HCAT-STPA) [20,57]	An examination of the system's planned risks and the identification of the HCAs as the root causes.	• HCAT-STPA generates and identifies more conflicts. The HCAT-STPA findings are more consistent.	• Not suitable to be used when there are multiple controllers.
Preliminary Hazard Analysis (PHA) [21,40,42]	Applied to the early stage of safety-critical systems, providing stakeholders with an understanding of upcoming hazards and associated causes.	• Assists in recognizing, considering, monitoring, and avoiding human-related errors that can result in injuries or accidents during the service and/or maintenance of process plants.	• Inability to deal with multiple failures in a focused manner
Resilience-based Integrated Process Systems Hazard Analysis (RIPSHA) [22,41]	A unique approach to hazard analysis that includes both technical and social elements into a single analysis process, based on resilience engineering theories.	• Looks at both internal and external disruptions. • Considers both static and dynamic situations and a variety of operational modes. • Exhibited ability to assess various types of operations	• Does not provide a method for systematically creating an organizational structure.
Probabilistic Seismic Hazard Analysis (PSHA) [23,53]	Performed to discover which distances and magnitudes have the greatest impact on hazards.	• It has the necessary structures in place to deal with the situation. Inherent ambiguity and the study's integration of different meanings	• Without a genuine and detailed site-specific study, venturing into PSHA is fruitless and worthless activity.
Deductive Cause-Consequences Analysis (DCCA) [24,54]	The generality of methodologies like FMEA and FTA is maintained while properly confirming the outcomes of informal safety analysis procedures.	• The method works backward and forwards from the events to determine their causes and effects.	• Each event must be thoroughly studied by the approach in order for it to be measured and the reasons discovered, and to do so, an expert assessment team is necessary. Otherwise, logical mistakes may occur.
Software Hazard Analysis (SWHA) [3,25,28]	Agile qualitative technique for clarifying software-intensive system safety requirements, which facilitates the identification of safety-critical functions, software, and general safety requirements guidelines.	• Provides a thorough and objective assessment of cyber security.	• This method focuses on software
Early Warning Sign Analysis based on the STPA (EWaSAP) [26,55]	Controllers try to justify the presence of defects in the controlled process by	• Can recognize and explain early warning indications associated with a variety of	• Detecting the large number of warning flags that may occur in eWaSAP could be

	comparing perceptible data to accident scenario models.	contributing variables to accidents, such as latent conditions and component failures.	considered a drawback. This is especially true when the system in question is "big" and contains a large number of human controllers who may find management challenges.
Process Failure Mode and Effect Analysis (PFMEA) [27,33,34]	It is used in process hazard analysis to analyze anomalous conditions of one factor and then determine safety implications for all of them.	• Process hazard analysis is made simple thanks to the independence hypothesis.	• Take only one aberrant state into account, and then look for safety implications one by one.
Architecture-level hazard analysis using AADL [13]	Designed to assess hazard/mishap acceptance, identify risks, devise specific mitigation solutions, and identify hazards.	• Hazard analysis data at the system and component levels can be obtained, supporting engineers in identifying significant potential hazards.	• AADL lacks formal semantics and executability
Root-State Hazard Identification (RSHI) [58]	Identify the threats for risk management in underground coal mines.	• Identifies a greater number of root and state dangers, reducing the need for collaborative risk identification and coordination among different types of personnel.	• Focuses on coal mine risk management for now

To summarize the findings in RQ2, HA techniques are pruned to drawbacks such as time-consuming and in need of experts' opinions or decisions, limitation of component failures detection scopes and stages, reliability of input or output data whether they are large or small, and low compatibility to detect multiple controllers or failures. Regardless of the techniques used, the main purpose of hazard analysis is to develop a scenario-based understanding of a system's safety vulnerability [28].

5. Conclusion

Deciding on the advisability of a particular course of action will consider the hazards associated with the activity and the risks associated with the hazards [4]. Hazard analysis acts as the initial step that needs to be carried out during the early stages of development such as the requirements stage to identify roots of hazards, effects, causal factors, and set appropriate measures for reduction while some analysis takes place during the software development process. Unlike other stages, this may reduce the cost of modification and error rectification process [8,14,22,28,35,36,60,61,62]. Any hazard analysis program's ultimate goals, as far as concerned, are to identify and rectify faults, as well as provide information on the essential safeguards [63].

The purpose of this paper is to highlight the available common hazard analysis techniques by presenting their respective functions along with the advantages and disadvantages of these techniques. The overall picture of presented information about hazard analysis techniques helps researchers and practitioners to understand and carry out a successful hazard analysis in safety-critical systems. In this paper, both research questions have been answered by presenting a total of 22 HA techniques in table 2, while their respective descriptions, advantages, and disadvantages are in table 3. In the future, a systematic literature review will be proposed and carried out to identify to what extent the hazard analysis techniques have been implemented and evaluated in case studies.

Acknowledgment
This work was supported in part by UMP under grant number RDU210313.

References

[1] Haider, A. A., & Nadeem, A. (2013). A Survey of Safety Analysis Techniques for Safety-Critical Systems. International Journal of Future Computer and Communication, 2(2), 134–137.Harris, A. L., Lang, M., Yates, D., & Kruck, S. E. (2008). Incorporating Ethics and Social Responsibility in IS Education. Journal of Information Systems Education, 22(3), 183-189.
[2] Abdullah, A. B., & Liu, S. (2013). Hazard analysis for safety-critical systems using SOFL. Proceedings of the 2013 IEEE Symposium on Computational Intelligence for Engineering Solutions, CIES 2013 - 2013 IEEE Symposium Series on Computational Intelligence, SSCI 2013, 133–140.
[3] Vilela, J., Castro, J., Martins, L. E. G., & Gorschek, T. (2017). Integration between requirements engineering and safety analysis: A systematic literature review. Journal of Systems and Software, 125, 68–92.
[4] Popović, V., & Vasić, B. (2008). Review of hazard analysis methods and their basic characteristics. FME Transactions, 36(4), 181–187.
[5] Ericson, C. A. (2005). Hazard Analysis Techniques for System Safety. Hazard Analysis Techniques for System Safety. John Wiley and Sons.
[6] Sere, K., & Troubitsyna, E. (1999). Hazard Analysis in formal specification. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 1709, 1564–1583.
[7] Sulaman, S. M., Beer, A., Felderer, M., & Höst, M. (2019). Comparison of the FMEA and STPA safety analysis methods–a case study. Software Quality Journal, 27(1), 349–387.
[8] Guo, H., Su, G., Jia, Y., Feng, G., Zhou, R., & Wang, Y. (2019). A systemic approach to hazard analysis and control based on energy function. Proceedings of 2018 IEEE International Conference of Safety Produce Informatization, IICSPI 2018, 20–25.
[9] Foster, N., & Jacob, J. (2002). Hazard Analysis for Security Protocol Requirements, 75–92.
[10] Dunjó, J., Fthenakis, V., Vílchez, J. A., & Arnaldos, J. (2010). Hazard and operability (HAZOP) analysis. A literature review. Journal of Hazardous Materials, 173(1–3), 19–32.
[11] Yang, S., & Chung, P. W. H. (1998). Hazard analysis and support tool for computer controlled processes. Journal of Loss Prevention in the Process Industries, 11(5), 333–345.
[12] Asare, P., Lach, J., & Stankovic, J. A. (2013). FSTPA-I: A Formal Approach to Hazard Identification via System Theoretic Process Analysis. 2013 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS), 150.
[13] Wei, X., Dong, Y., Yang, M., Hu, N., & Ye, H. (2014). Hazard analysis for AADL model. RTCSA 2014 - 20th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications, 1–10.
[14] Muller, M., Roth, M., & Lindemann, U. (2016). The hazard analysis profile: Linking safety analysis and SysML. 10th Annual International Systems Conference, SysCon 2016

- Proceedings.
[15] Mason-Blakley, F., Weber, J., & Habibi, R. (2014). Prospective hazard analysis for information system. Proceedings - 2014 IEEE International Conference on Healthcare Informatics, ICHI 2014, 256–265.
[16] Zhang, H., Li, W., & Chen, W. (2010). Model-based hazard analysis method on automotive programmable electronic system. Proceedings - 2010 3rd International Conference on Biomedical Engineering and Informatics, BMEI 2010, 7(Bmei), 2658–2661.
[17] Wang, R., & Zheng, W. (2013). Research and application of the BFM-STAMP hazard analysis method. IEEE ICIRT 2013 - Proceedings: IEEE International Conference on Intelligent Rail Transportation, 174–178.
[18] Alexander, R., & Kelly, T. (2013). Supporting systems of systems hazard analysis using multi-agent simulation. Safety Science, 51(1), 302–318.
[19] Laufenberg, X. (1995). Modeling and Model-Based Analysis for Safety and Hazard Analysis. IFAC Proceedings Volumes, 28(25), 263–268.
[20] Zhu, D., & Yao, S. (2019). A Hazard Analysis Method for Software-Controlled Systems Based on System-Theoretic Accident Modeling and Process. Proceedings of the IEEE International Conference on Software Engineering and Service Sciences, ICSESS, 2018–Novem, 90–95.
[21] Zhou, J., Hänninen, K., Lundqvist, K., & Provenzano, L. (2018). An ontological approach to identify the causes of hazards for safety-critical systems. 2017 2nd International Conference on System Reliability and Safety, ICSRS 2017, 2018–January, 405–413.
[22] Jain, P., Rogers, W. J., Pasman, H. J., Keim, K. K., & Mannan, M. S. (2018). A Resilience-based Integrated Process Systems Hazard Analysis (RIPSHA) approach: Part I plant system layer. Process Safety and Environmental Protection, 116, 92–105.
[23] Fernandez Ares, A., & Fatehi, A. (1970). Development of probabilistic seismic hazard analysis for international sites, challenges and guidelines. Nuclear Engineering and Design, 259(Usgs 2008), 222–229.
[24] Ortmeier, F. (2014). Deductive Cause-Consequence Analysis (DCCA), (January 2006).
[25] Oh, H.-J., & Hong, J.-P. (2012). A Study of Software Hazard Analysis for Safety Critical Function in Military Aircraft. Journal of IKEEE, 16(2), 145–152.
[26] Dokas, I. M., Feehan, J., & Imran, S. (2013). EWaSAP: An early warning sign identification approach based on a systemic hazard analysis. Safety Science, 58, 11–26.
[27] Wu, Y., Zhao, T., & Chu, J. (2017). A Hybrid Process Coupling Hazard Analysis Method based on PFMEA and BN, (Tcrse).
[28] Zahabi, M., & Kaber, D. (2019). A fuzzy system hazard analysis approach for human-in-the-loop systems. Safety Science, 120(April), 922–931.
[29] Song, H., & Schnieder, E. (2018). Evaluating Fault Tree by means of Colored Petri nets to analyze the railway system dependability. Safety Science, 110(January), 313–323.
[30] Pereira, D. P., Hirata, C., & Nadjm-Tehrani, S. (2019). A STAMP-based ontology approach to support safety and security analyses. Journal of Information Security and Applications, 47, 302–319.
[31] Radosavljević, S., Lilić, N., Ćurčić, S., & Radosavljević, M. (2009). Risk assessment and managing technical systems in case of mining industry. Strojniski Vestnik/Journal of Mechanical Engineering, 55(2), 119–130.
[32] B, P. M., Zhang, Y., & Jones, P. (2017). A Hazard Analysis Method for Systematic Identification of Safety Requirements for User Interface Software in Medical Devices, 1, 284–299.
[33] Höfig, K., Klein, C., Rothbauer, S., Zeller, M., Vorderer, M., & Koo, C. H. (2019). A Meta-model for Process Failure Mode and Effects Analysis (PFMEA). IEEE International

Conference on Emerging Technologies and Factory Automation, ETFA, 2019–September, 1199–1202.
[34] Banduka, N., Tadic, D., Macužic, I., & Crnjac, M. (2018). Extended process failure mode and effect analysis (PFMEA) for the automotive industry: The FSQC-PFMEA. Advances in Production Engineering And Management, 13(2), 206–215.
[35] Li, W., & Zhang, H. (2011). A software hazard analysis method for automotive control system. Proceedings - 2011 IEEE International Conference on Computer Science and Automation Engineering, CSAE 2011, 3, 744–748.
[36] Wang, H., Zhong, D., Zhao, Y., & Sun, R. (2017). A system safety analysis method based on multiple category hazard factors. Proceedings - 4th International Conference on Dependable Systems and Their Applications, DSA 2017, 2018–Janua, 29–34.
[37] Du, J., Wang, J., & Feng, X. (2014). A safety requirement elicitation technique of safety-critical system based on scenario. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 8588 LNCS, 127–136.
[38] Liu, H. C., Chen, X. Q., Duan, C. Y., & Wang, Y. M. (2019). Failure mode and effect analysis using multi-criteria decision making methods: A systematic literature review. Computers and Industrial Engineering, 135(April), 881–897.
[39] Alsammak, A. K., & Yahia, H. (2017). Hazard Analysis of Real-Time Safety Critical System Using Hierarchical Communicating Real-Time State Machines Formal Model, 628–634.
[40] Guiochet, J. (2016). Hazard analysis of human-robot interactions with HAZOP-UML. Safety Science, 84, 225–237.
[41] Jain, P., Rogers, W. J., Pasman, H. J., & Mannan, M. S. (2018). A resilience-based integrated process systems hazard analysis (RIPSHA) approach: Part II management system layer. Process Safety and Environmental Protection, 118, 115–124.
[42] Basu, S. (2017). Qualitative Hazard Analysis. Plant Hazard Analysis and Safety Instrumentation Systems.
[43] Pasman, H. J., Rogers, W. J., & Mannan, M. S. (2018). 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. Journal of Loss Prevention in the Process Industries, 55(January), 80–106.
[44] Rao, C., Guo, J., Li, N., Lei, Y., Zhang, Y. D., & Li, Y. (2018). Safety-critical system modeling in model-based testing with hazard and operability analysis. Proceedings - 2018 IEEE 18th International Conference on Software Quality, Reliability, and Security, QRS 2018, 397–404.
[45] Kritzinger, D. (2017). Functional Hazard Analysis. Aircraft System Safety, 37–57.
[46] Gabsi, W., Zalila, B., & Jmaiel, M. (2017). Development of a parser for the AADL error model annex. Proceedings - 16th IEEE/ACIS International Conference on Computer and Information Science, ICIS 2017, 233–238.
[47] Casson Moreno, V., & Cozzani, V. (2018). Integrated hazard identification within the risk management of industrial biological processes. Safety Science, 103(September 2017), 340–351.
[48] Lin, J.-W., & Chiou, J.-S. (2019). Active Probability Backpropagation Neural Network Model for Monthly Prediction of Probabilistic Seismic Hazard Analysis in Taiwan. IEEE Access, 7, 108990–109014.
[49] Li, Z., Wang, S., Zhao, T., & Liu, B. (2016). A hazard analysis via an improved timed colored petri net with time–space coupling safety constraint. Chinese Journal of Aeronautics, 29(4), 1027–1041.
[50] Alexander, R., & Kelly, T. (2013). Supporting systems of systems hazard analysis using

multi-agent simulation. Safety Science, 51(1), 302–318.
[51] Paolo, E.A.D., Noble, J., Bullock, S., (2000). Simulation models as opaque thought experiments. in: Proceedings of the Seventh International Conference on Artificial Life. MIT Press, pp. 497–506.
[52] Laufenberg, X. (1995). Modeling and Model-Based Analysis for Safety and Hazard Analysis. IFAC Proceedings Volumes, 28(25), 263–268.
[53] Ares, A. F. (2010). Development of probabilistic seismic hazard analysis for international sites, challenges and guidelines. 2010 1st International Nuclear and Renewable Energy Conference, INREC'10, 1(Usgs 2008), 1–6.
[54] Eschenburg, J. (2006). Failure-Sensitive Specification: A Formal Method for Finding Failure Modes, (April).
[55] Woods, D.D., 2009. Escaping failures of foresight. Safety Science 47 (4), 498–501.
[56] Wei, X., Dong, Y., Li, X., & Wong, W. E. (2018). Architecture-level hazard analysis using AADL. Journal of Systems and Software, 137, 580–604.
[57] Leveson, N. G. (2004). A Systems-Theoretic Approach to Safety in Software-Intensive Systems, 1(1), 66–86.
[58] Liu, Q., Peng, Y., Li, Z., Zhao, P., & Qiu, Z. (2021). Hazard identification methodology for underground coal mine risk management - Root-State Hazard Identification. Resources Policy, 72(19), 102052.
[59] Knight, J. C. (2002). Safety critical systems: Challenges and directions. Proceedings - International Conference on Software Engineering, 547–550.
[60] Daramola, O., Stålhane, T., Sindre, G., & Omoronyia, I. (2011). Enabling hazard identification from requirements and reuse-oriented HAZOP analysis. 2011 4th International Workshop on Managing Requirements Knowledge, MaRK'11 - Part of the 19th IEEE International Requirements Engineering Conference, RE'11, 3–11.
[61] Baybutt, P. (2014). Requirements for improved process hazard analysis (PHA) methods. Journal of Loss Prevention in the Process Industries, 32, 182–191.
[62] Burns, D. J., & Pitblado, R. M. (1993). A Modified Hazop Methodology For Safety Critical System Assessment. Directions in Safety-Critical Systems, 232–245.
[63] Lawrence, J. D., & Gallagher, J. M. (1997). A proposal for performing software safety hazard analysis. Reliability Engineering and System Safety, 55(3), 267–282.