processes

MDPI

Review

Comprehensive Review of Safety Studies in Process Industrial Systems: Concepts, Progress, and Main Research Topics

Jialu Zhang [1,2,†], Haojie Ren [3,†], Hao Ren [1,*,†], Yi Chai [4], Zhaodong Liu [2] and Xiaojun Liang [1]

[1] Industrial Intelligence Basic Research Studio, Department of Mathematical Science and Cross Frontiers, Peng Cheng Laboratory, Shenzhen 518066, China; crystalzjl6603@foxmail.com (J.Z.); liangxj@pcl.ac.cn (X.L.)
[2] College of Automation and Electrical Engineering, Linyi University, Linyi 276000, China; liuzhaodong2017@sina.cn
[3] State Key Laboratory of Ocean Engineering, Shanghai Jiao Tong University, Shanghai 200240, China; renhaojie@sjtu.edu.cn
[4] The Key Laboratory of Complex System Safety and Control, School of Automation, Chongqing University, Chongqing 400044, China; chaiyi@cqu.edu.cn
* Correspondence: renh@pcl.ac.cn
† These authors contributed equally to this work.

Abstract: This paper focuses on reviewing past progress in the advancement of definitions, methods, and models for safety analysis and assessment of process industrial systems and highlighting the main research topics. Based on the analysis of the knowledge with respect to process safety, the review covers the fact that the entire system does not have the ability to produce casualties, health deterioration, and other accidents, which ultimately cause human life threats and health damage. And, according to the comparison between safety and reliability, when a system is in an unreliable state, it must be in an unsafe state. Related works show that the main organizations and regulations are developed and grouped together, and these are also outlined in the literature. The progress and current research topics of the methods and models have been summarized and discussed in the analysis and assessment of safety for process industrial systems, which mainly illustrate that the dynamic operational safety assessment under the big data challenges will become the research direction, which will change the future study situation.

Keywords: process industrial systems; safety; safety assessment; research review; research topics

Citation: Zhang, J.; Ren, H.; Ren, H.; Chai, Y.; Liu, Z.; Liang, X. Comprehensive Review of Safety Studies in Process Industrial Systems: Concepts, Progress, and Main Research Topics. *Processes* **2023**, *11*, 2454. https://doi.org/10.3390/pr11082454

Academic Editors: Jie Zhang, Zhe Zhou and Dong Gao

Received: 18 July 2023
Revised: 8 August 2023
Accepted: 9 August 2023
Published: 15 August 2023

1. Introduction

Modern industrial processes have become increasingly complex as a result of the advancement of computers, sensors, and communication technologies. This has led to numerous catastrophes, including those that occurred in Bhopal, West Virginia, DuPont, Texas, Fukushima, and Mexico [1–4]. In general, human error, technical defects, failures, abnormalities, etc., which frequently include several physical and chemical changes, are the main causes of accidents. All of these mishaps, including leaks, pollution, explosions, poisoning, etc., have the potential to seriously harm people's health, property, and the environment [3–5]. As a result, safety analysis and assessment for industrial processes have emerged as one of the most popular research areas for academics and industry professionals globally.

A basic process control system can be considered the system that is applied for the response of the input signals during the process, which is caused by the generated output signals, the operator, programmable systems, and associated equipment. The corresponding equipment is applied to the operation in a desirable way. However, there is no safety-instrumented function being conducted with a claimed safety integrity level [6,7]. Generally speaking, the process industrial systems mainly include petrochemical [3,4,8,9],

petroleum [8,10,11], and chemical industries [12–14], hydrogen stations [15–19], liquefied natural gas [20,21], oil- and gas-producing companies [22], cryogenic fuel-loading systems [23,24], offshore drilling [25–28], etc.

The degree of risk and the need for control measures often determine the safety level of the process industry. As shown in Figure 1, a typical way of categorizing is as follows:

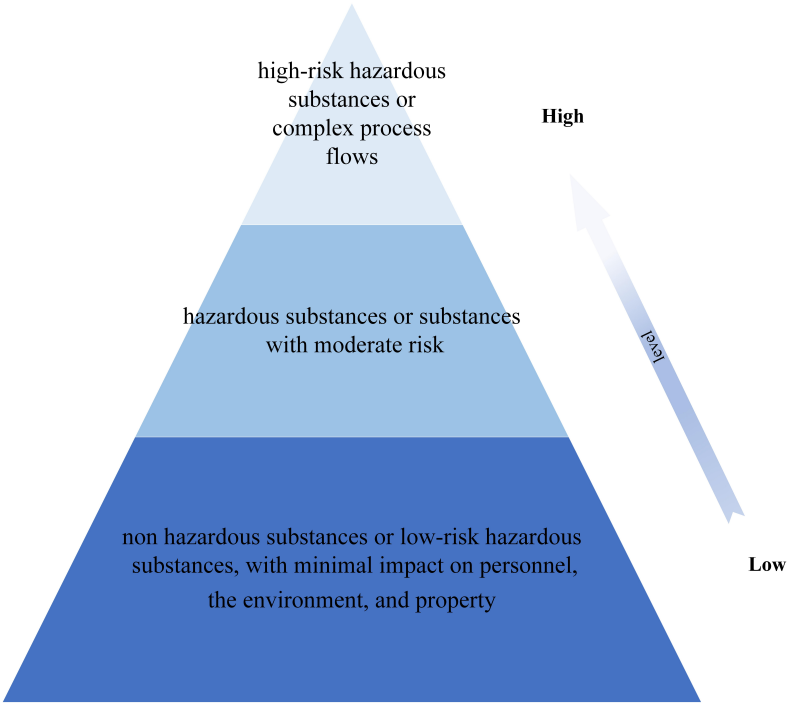


Figure 1. The safety level of the process industry.

1. Low risk level: this level is appropriate for industrial activities that have minimal risk and reasonably predictable outcomes. These procedures may use low-risk or nonhazardous substances with little effect on people, the environment, or property. Standard operating procedures and generic safety measures can satisfy safety needs at this level.
2. Moderate risk level: this degree of risk is appropriate for industrial activities that could have substantial negative effects on people, the environment, and property. Hazardous or moderately risky compounds may be used in these processes. To guarantee efficient risk control at this level, stringent security measures and management systems must be put in place.
3. High risk level: this level applies to industrial procedures that have a significant likelihood of endangering people, the environment, or property. These procedures frequently involve dangerous substances with a high degree of risk or intricate process flows. At this level, security must be ensured using the toughest management practices, security procedures, and tactics.

To reduce the safety risk, analysis and assessment methods for safety in industrial processes are required so that appropriate measures can be planned. IEC 61508, which is a safety-related system standard, has been developed by the International Electrotechnical Commission (IEC) [29]. There are some standards for the activities that are defined that need to be followed. Furthermore, this system can be employed to provide a series of measures and techniques that can be used, based on the safety integrity level. Based on this standard, a large number of others were later derived, such as IEC 61511 for process industries, IEC 61513 for nuclear power, IEC 62061 for machinery, IEC 60335 for household appliances, etc. [7,30–32]. Significance indications in any of the above standards can be

employed to deal with the constraints of, and evaluate the safety risks existing in, the minute hazard possibilities.

In the past few decades, a huge number of review articles have been published that focus on various areas of process safety, for instance, risk management, domino effects, safety indices, safety management, safety-related quantitative risk analysis, etc. [1,2,33–46]. Looking at the recent review articles, no articles have been found that discuss the latest progress made in terms of safety issues and current research trends in process industrial systems. The significance of this article can be summarized as follows:

1. The definition of process safety in process industrial systems has been described, discussed, and summarized. Then, the perspective of safety usually emerges from specific research views based on the above reviews.
2. There are some interdependencies between safety and some other related concepts that have been discussed and compared, such as reliability, risk, operational safety, and its analysis and assessment. And all of above these can be inspired to provide peer research and scholars with some research ideas.
3. The progress of methods and models has also summarized and discussed in the analysis and assessment of safety for process industrial systems, which mainly include analysis, assessment, and decision support of safety.
4. Similarly, developments in recent years have laid a solid foundation for the current trends, and these are also outlined, including inherent safety, operational safety, safety barriers, safety integrity levels, total safety management, human error probability, and so on.

In Section 2, the knowledge and understanding of safety in process industrial systems is presented, and comparisons between safety and other related concepts are also given. Section 3 considers the progress in recent years, in the context of the past, of models, and approaches to safety evaluation and analysis. Developments in recent years lay the foundation for the current main research topics, and this is discussed in Section 4. Finally, conclusions and future directions in these fields are outlined.

2. Knowledge with Respect to Safety

To identify the scope and also to make clear about the adopted terms applied in process industrial systems, and to guarantee consistency of this research, the related definitions on safety and its related safety have been presented.

2.1. Definitions

Generally, safety can be considered as one of the most abstract and broad notions, which is generally described as a specific situation or state that may not lead to negative results, such as harm, loss, or damage to the environment, humans, and equipment. In other words, safety can be considered as the condition that has no unacceptable risks in any basic process industrial system [6,7,39–41,47–50].

According to the standard named IEC 61511:2016, some safety related concepts should be made clear to ensure consistency throughout the paper. These safety-related definitions can be summarized as follows [6,7].

1. Accident: unexpected or undesirable event leading to loss, death, suffering, or damage [39].
2. Harm: physical damage or injury to the wellbeing of people, both directly and indirectly, serving as an outcome of the damage to the environment or property [6].
3. Hazard: possible source of damage [6] or system state that may result in a mishap in specific environmental situations [7].
4. Risk: the combination of the severity of the harm and the frequency of the harm [6], or a combination of the outcomes of the failure or event and the possibility of the failure or abnormal event having an effect on the environment, users, operators, or components of the system [7].

5. Process risk: the risk that the process is triggered by abnormal events. Necessary risk management is viewed as the risk reduction that is required to guarantee that the risk is decreased to a tolerable degree [6].
6. Fault: abnormal situation that might lead to a loss of or decrease in the capacity of the functional unit to conduct the function that is required [6].
7. Failure: termination of the capacity of the functional unit to conduct its function as required [6]. In other words, the event in which the subsystem or the system component does not demonstrate an expected environmental condition or external behavior under which it should be documented and exhibited in the specification of the requirements [6].
8. Common cause failure: failure, serving as the outcome of one or more events, leading to the failures of at least two separate channels in various channel systems, resulting in system failure [6].
9. Common mode failure: the failure of at least two channels, leading to the same erroneous outcome [6].
10. Dangerous failure: failure with the potential to impose great threats to the safety instrumented system or lead to the nonfunction state [6].
11. Dependent failure: failure, the probability of which cannot be shown through the simple product of the unconditional possibilities of the individual events that triggered it [6].
12. Systematic failure: failure that is relevant with a specific cause in a deterministic way, which can only be dealt with through the adjustment of the manufacturing process, the operational procedures, the design or the documentation, or any other related factors [6].
13. Safe failure: failure with no potential to expose the system to a failure or hazardous status [6].
14. Safety: freedom from a risk that is unacceptable; freedom obtained from those events that can lead to loss of equipment, damage, occupational illness, or death [6,7].
15. Safe state: status where the safety can be realized [6].
16. Safety function: function to be carried out by an SIS (safety instrumented mechanism), external risk, reduction facilities technology, and safety-related system, which plans to keep the process safe when carrying out a specific hazardous event [6].
17. Safety integrity: the possibility of the safety instrumented mechanism to conduct the required safety instrumented functions satisfactorily in all situations during a specific period of time [6].
18. Safety integrity level (SIL): the discrete level (one out of four) for the illustration of the safety standards of the safety instrumented functions to be distributed to the safety instrumented systems [6].
19. Safety life cycle: the inevitable activities engaged with during the implementation of the safety instrumented functions taking place during the period of time either at the beginning or the end of the project when all the safety instrumented functions are no longer available for use [6].
20. Safety instrumented function: safety function at a particular safety integrity level, which is of great importance to realize the functional safety, which can be realized either through a safety instrumented control function or a safety instrumented protection function [6].
21. Safety instrumented system: an instrumented system that is applied for the implementation of at least one safety instrumented function. It consists of a combination of the final elements, the logic solver, and sensors [6].
22. Functional safety: part of the general safety relevant to the process and the BPCS, namely the basic process control system, which relies on the correct functioning of the safety instrumented system and other protection layers [6].
23. Functional safety assessment: exploration, based on the evidence, that can be used to evaluate the functional safety realized by at least one protection layer [6].

24. Hardware safety integrity: the safety integrity of the safety instrumented function is related to the random hardware failures of the dangerous failure mode [6].
25. System safety: the application of the management and engineering principles, standards, and skills to utilize the safety processes and to decrease the risks of the constraints of operational efficiency, cost, and time during all the processes of the system [7].
26. Safety requirement: the limits or the actions that have been depicted to improve or support the safety of the system [39]. Simply, any standard that can be adopted to specify a mandatory and minimum amount of safety in the minimum level of the associated metric [39].
27. Safety management system: systemic management of the physical environment, machine performance, and worker performance [40], or the management activities, elements, and procedures that are targeted to enhance the safety performance of the organization [40,49].
28. Human mistake (error): human action or inaction that produces an unintended result [6].
29. Usefulness: the fact of being useful and bringing value for practitioners [39].

From all of the above safety-related concepts, it should be noted that safety can be considered as the state that has no unacceptable risk in any basic process control system. And the risk is the probability of injury and combination of the frequency of occurrence of harm and the severity of that harm. Injury is generally to be directly or indirectly caused by damage to property or the environment as a result of personal damage. To sum up, the safety in process industrial systems can be attributed to the fact that the entire system does not have the ability to produce casualties, health deterioration, and other accidents, which ultimately cause threats to human life and health damage.

2.2. Perspectives

In order to understand the scope, motivations, and objectives of the safety in process industries better, it is of great significance to define clearly the interdependencies between process safety and its concerns, or similar definitions.

2.2.1. Interdependencies between Process Safety and Its Concerns

The history of research on process safety was started by the pioneer of industrial safety, Heirish [47], who pointed out the distinction between accidents and injuries, where the former denoted the cause and the latter the effect. Furthermore, later thinkers and scholars employed the term safety to cover not only injuries but also the events that cause accidents. However, the relationships between process safety and its concerns are not clear, and, so far, there are few studies discussing their interdependencies, which can be considered the aim of the diagram shown in Figure 2.

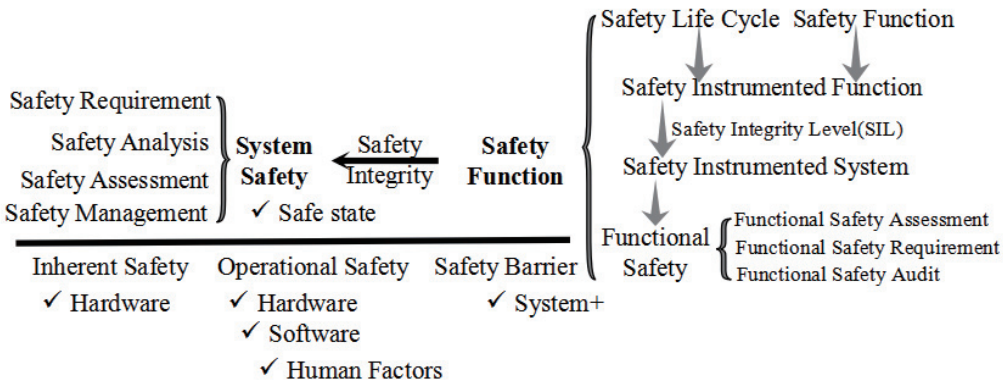


Figure 2. Schematic diagram of interdependencies between safety and its related concerns.

A significant number of safety functions, as measured by safety integrity, can be merged, as illustrated in Figure 2, as the authors are aware, to actualize the safety of the complete system. Similar to how functional safety is a component of safety function, functional safety is typically defined in terms of three aspects: functional assessment, functional requirement, and functional safety audit. Additionally, a safety instrumented system with a safety instrumented function, which is accomplished by every safety function in the system's safety life cycle, frequently achieves functional safety in stages.

Some related concerns are also discussed as followed, including safety assessment, inherent safety, operational safety assessment, safety barriers, safety management systems, etc.

1. Safety assessment/evaluation: generally, this serves as both an important approach for the satisfying and implementation of the policy of safety first, and is prevention oriented, and also the base for the implementation of standardized and scientific management of companies [51]. Meanwhile, it is also helpful to develop the theoretical, methodological, and empirical approaches to grasp better in foresight what is being processed in hindsight, or to shift from the research about past failures to an anticipation of future ones [52].
2. Inherent safety: in general, the inherent safety means the ideal design, which only a limited amount of the hazardous materials would be leaked out or it is capable to ensure the deviations from the ideal performance of the equipment failures and operators with none severe damage on the safety, efficiency or output, or the hazardous materials can be applied under a situation with low operating conditions to avoid hazard conflagrations [9].Guaranteeing the inherent safety would exactly guarantee the safety of the system. The system is free of the situations that can lead to loss of the equipment, the damage, occupational illness, injury or death [7].
3. Operational safety assessment: as promoted by the CCPS, namely the United States Center for Chemical Process Safety, facilities are required to manage the real-time performance of the management system activities instead of just waiting for the occurrence of accidents. Such performance monitoring would allow the issues to be found early on and hence allow corrective actions to be taken as the issues occur [53]. It means that operational safety assessment can be considered as a kind of dynamic system, whose aim is to discover the potential safety risks online, and then to eliminate them in time [54].
4. Safety barrier: safety barriers can be implemented to protect people, the environment, and assets from hazards or dangers. In other words, safety barriers can be considered as physical and/or nonphysical means planned to prevent, control, or mitigate undesired events or accidents [25]. Thus, safety barriers can be considered as the means, and system safety can be considered as the intent.
5. Safety management system: the safety management system is commonly defined as the management procedures, elements, and activities that aim to improve the safety performance within an organization [40]. Obviously, a safety management system can be considered as a very practical concept, widely used in different industries.

2.2.2. Interdependencies between Process Safety and Its Similar Definitions

Interdependencies between process safety and its similar definitions are studied by examining how requirements and measures from one field may impact another, and what similarities they share, which indicate that some of the techniques applicable to one field could also be applicable to the other [34]. Interdependencies between process safety and its similar definitions have been recognized by many researchers and scholars [1,2,33–46]. In order to highlight these interdependencies, the differences and similarities have been discussed more extensively, as shown in Figure 3.

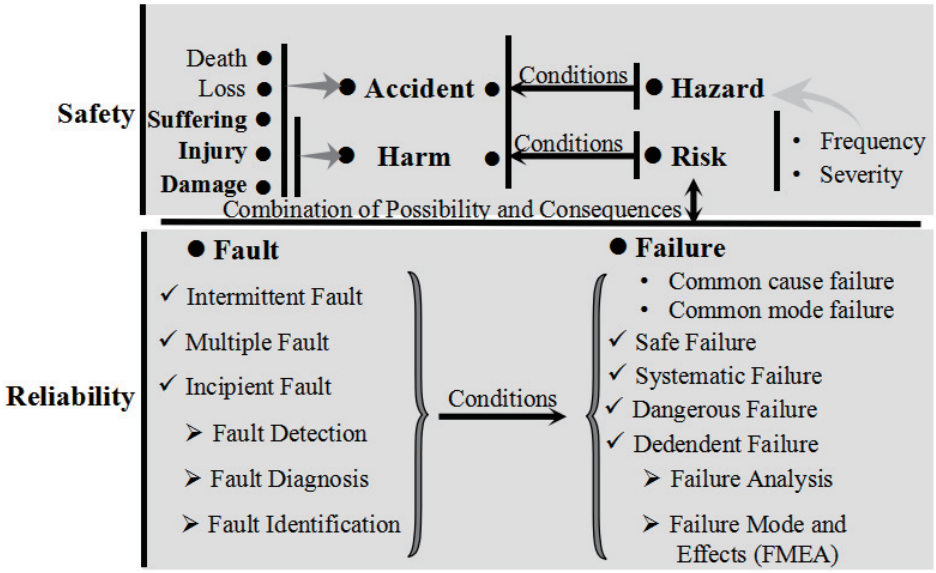


Figure 3. Schematic diagram of interdependencies between safety and its similar definitions.

1. Safety versus reliability: as shown in Figure 3 and as mentioned above, the essence of safety in process industrial systems can be considered to prevent accidents, and to reduce casualties, damage, environmental pollution, and so on. The goal of reliability is to prove the compliance and effectiveness of the process industrial system [55]. Safety can be considered as the idea that is used to measure whether a system is available or is able to be used, and reliability can be used to measure whether a system is reliable and available. Faults and failures will keep a system's reliability at a lower level, and the safety can be kept at a lower level by the abnormal operational state that the related devices are in, viz., if the system is in an unreliable state, then the system must be in an unsafe state.
2. Safety versus risk: as shown in Figure 2, safety considers hazards or risks in a system that may harm people, equipment, or the environment due to the system faults/failures or some combination of accidental conditions, while risk just considers the combination of possibility and consequences of faults or failures [34].

2.3. Related Works

In order to ensure safety in process industrial systems, the main work in safety science should serve as an international medium for research in the science and technology for human safety. Furthermore, studies on safety science should be focused on the methodology that can be used to identify the system's hazard sources, and to take effective measures to minimize the risk, so that the system can be pushed into the specified performance.

2.3.1. Main Organizations and Regulations

Generally, the research organizations and programs started after several serious accidents during 1970 to 1990, which can be considered as the main force to advance the study on the process safety in process industries [2,40].

In 1974, the Health and Safety Commission and Health and Safety Executive (HSE) were established one after another after the Flixborough accident, and they advanced the development of hazard identification [2,40].

In 1982, the Seveso Directive was established by the European Commission, and it can be considered as the response to the industrial catastrophic accident that occurred in Seveso, Italy, in 1976 [2,40].

In 1985, the Center of Chemical Process Safety (CCPS) was established by the American Institute of Chemical Engineers (AIChE) after the Bhopal accident, and after five

years, its representative guidebook, named *Guidelines for Hazard Evaluation Procedures*, was published [2,40].

After then, the European Process Safety Center (EPSC) was established by the European Federation of Chemical Engineering (EFCE) in 1994, and its aim can be considered to promote safety practices across Europe [2,40].

In 1995, Texas A & M University established the Mary Kay O'Connor Process Safety Center, aiming to offer services, research, education, research for safety operation training, emergency management, risk management, expertise, and education [2,40].

In 1996, the Seveso II Directive was reported to replace the Seveso Directive, and its main lights stood at the Control of Major Accident Hazards regulation passes in 1984 in the UK [2,40].

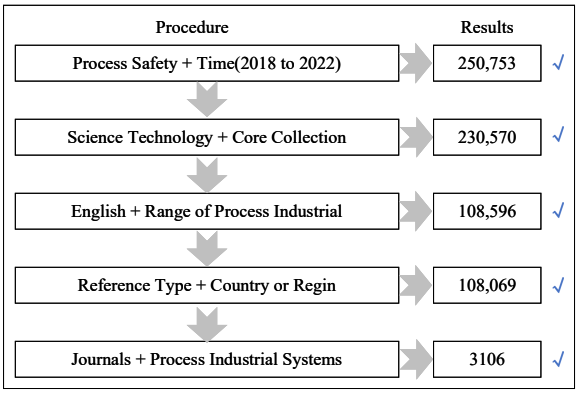
Occupational Health and Safety Administration (OSHA) serves as the most famous standard, and originated from major accidents, for instance the nuclear meltdown (Three Mile Island, 1979), Union Carbide plant toxic release accident (Institute, West Virginia, 1985), etc., that occurred during the period of 1970 to 1990. Later, it was not only used in USA, but also become the industrial best practice all around the world [2,40].

Before entering the 21st century, the study of system safety had made violent progress, and many guidebooks and standards had been reported. The ground-safety-related standard, named IEC 61508, was pushed out by the International Electrotechnical Commission (IEC), and its intent is to enable the development of programmable electronic-safety-related systems [7,40]. Then, the process sector implementation of IEC 61508, named IEC 61511, was developed as the international standard that was used to provide requirements for specification, design, installation, operation, and maintenance. After two decades of developments, the IEC 61511 has issued its second edition [3,6,40].

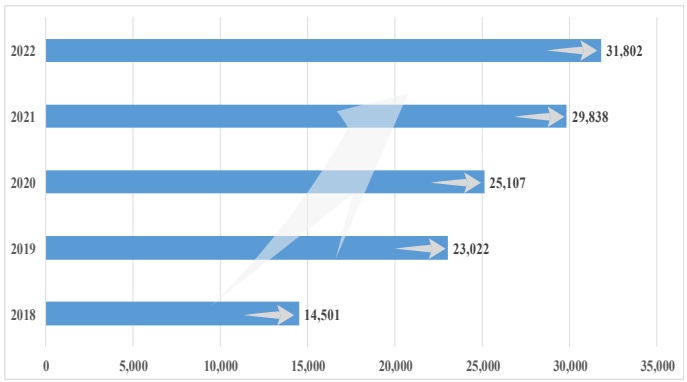
2.3.2. Literature Review

With the development of science and technology, the opinions on the safety of process industrial systems have changed into identifying the potential safety issues and risk factors that should be recognized and eliminated before accidents occur. Therefore, traditional methods are rarely used to meet the requirements to ensure process safety. And in order to solve this problem, a huge number of researchers and scholars around the world have focused their studies in one stage.

The search of the literature on the indexing system, Web of Science, covered a broad range of process industries, with process safety used as the keywords. The broad range includes engineering, chemistry, energy fuels, and nuclear industrial systems. The search procedure is shown in Figure 4.



(a)Search procedure and its results in Web of Science.



(b)Search results and the analysis of related research trends.

Figure 4. The search procedure and its results in Web of Science (**a**), and its analysis of related research trends (**b**).

As shown in Figure 4, there are a large number of results from Web of Science. In just a few years, the number of articles increased from 14,501 to 31,802, which means that many safety issues still exist in modern process industrial systems and these attract the attention of many scholars.

Generally, the major research reports are available in the public domain, such as journals, conferences, etc., as shown in Figure 5a, and consist of articles (96.74%), other (24.29%), reviews (14.54%), and so on. It especially needs to be noted that there is about 0.19% of reference material, which means that safety in process industrial systems can be considered as the most difficult. Furthermore, these studies are distributed in various countries and regions around the world, such as the United States (25.12%), China (29.94%), Germany (5.44%), England (6.39%), France (4.00%), Canada (4.56%), and so on, as shown in Figure 5b. And this is also in line with the current states of economic development. The highest number of published articles in journals can be ranked as follows: *Journal of Hazardous Materials* (10.39%), *Applied Sciences-Basel* (9.9%), *Sensors* (8.64%), *Sensors (Basel, Switzerland)* (8.56%), *Applied Sciences* (8.26%), *Chemical Engineering Journal* (6.93%), *Safety Science* (6.42%), *Journal of Loss Prevention in the Process Industries* (6.13%), etc., as shown in Figure 5c.

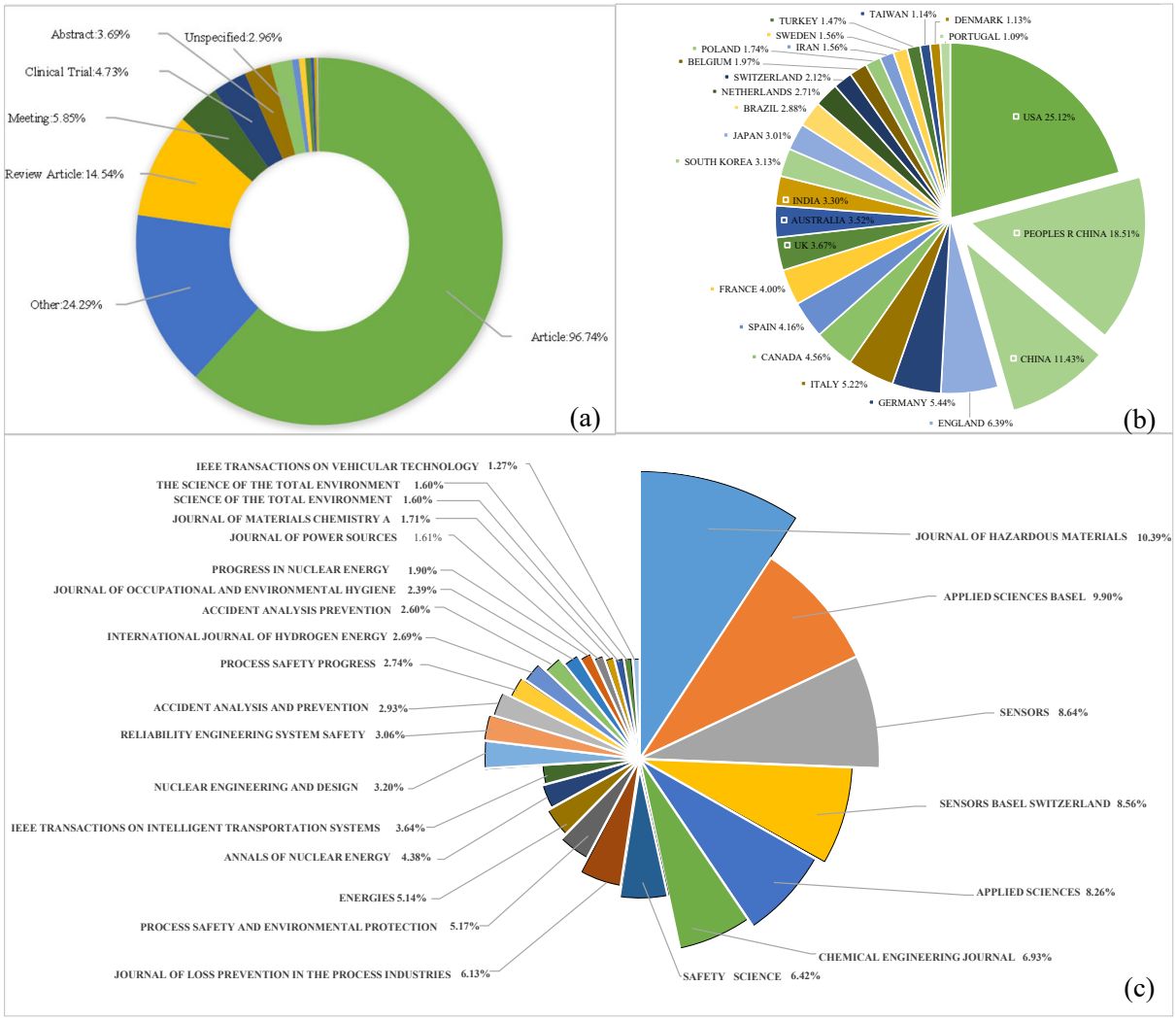


Figure 5. A simple analysis of the search results in the proportion of various literature (**a**), the proportion of various countries and regions around the world (**b**), and the proportion of various journals and magazines (**c**).

2.3.3. Related Available Literature

As explained above, a great amount of literature has focused on studies on the matter of safety in industrial processes, and several reference publications are available in this paper. However, although a great amount of work covers almost any aspect related to the safety of industrial processes, none of them provides an extensive, comprehensive, and in-depth understanding and summary of the existing research work. In about 97 available references, 16 review articles have focused their content on process safety [1,2,33–46].

Nassim A, et al. [1] conducted research focusing on offering a critical revision of the process for the identification of domino effect scenarios and also an analysis of the existing regulations for the evaluation of the domino effect.

In addition, there were a comparison and a discussion on the current standards obtained from the recent progress achieved in the escalation hazards and safety distance assessments.

Khan F, et al. [2] focused on offering a historical development method in the field on the driving forces, hoping it would help industrial practitioners and researchers to obtain a better comprehension of the current relevant safety concepts and offering a new direction to bridge the current gaps via research and developments.

Roy N, et al. [33] conducted a review on the progress being achieved in terms of the safety indices, with special concentration on their application during the design process, and depicted the type of information and the output yielded from the use of these indices. Some examples of recent applications, including the safety issues, have been integrated into the design of multiple chemical processes.

Kriaa S, et al. [34] offered comprehensive research on current methods for industrial risk evaluation and facility design that need to consider both security and safety issues, and offered a detailed analysis on the methods being identified in the literature.

Necci A, et al. [35] conducted a study about the work carried out during the past three decades in the field. Meanwhile, a critical evaluation of the knowledge gaps and available tools has also been carried out. The analysis carried out in the scientific publications about the domino effect during the process led to a database consisting of over 60 documents, dealing with three major problems, including the risk evaluation and safety management of domino scenarios, the models for equipment damage, and past accident analysis.

Shafiee M, et al. [36] conducted a review of the prior literature and classified the frameworks related to the industrial practices concerning the life extension of the safety critical systems and also the installations. A systematic review was conducted of the existing highend and new progress achieved in the field of asset life extension in different industries. The classification framework was promoted to support the decision-making process of the life extension concerning the category of the asset and the industry sectors in which the notion of life extension is of interest. The condition evaluation techniques were applied for the asset's qualification for life extension. In addition, an exhaustive list of the scientific references was compiled on the current topic, including the articles published in technical reports and government documents, university dissertations, conference proceedings, books, industry magazines, and journals.

Broadribb M P, Freiburger E. [42] discussed a method to identify a manageable number of safety critical equipment or element (SCE) items, and approaches for successfully managing inspection, testing, and preventive maintenance (ITPM) tasks for SCE. The application of criticality analysis for process safety purposes can assist with identification of equipment that requires high reliability in order to prevent or mitigate major incidents.

Yuling L and Frank W. G. [40] described safety management systems (SMSs) with five core aspects: definition, evolution, models, purpose, and common elements of SMSs. The SMS studies and models are developed for two main purposes: control and compliance. To control means that, by implementing safety systems or subsystems, an SMS is able to control risks and to improve continuously, as well as comply with the appropriate standard management systems. As the key to implementing a functional SMS is to carry out common managerial processes, Yuling Li and Frank W. Guldenmund mapped the elements of various SMSs to a generic SMS to explore the extent to which they correspond.

Goerlandt F, et al. [41] conducted a review exploring the validation and validity of qualitative risk analysis in a safety context. Meanwhile, they also reviewed the empirical, methodological, and theoretical contributions of the scientific literature and concentrated on three problems, including (a) what theoretical views about validation and validity of quantitative risk analysis can be found? (b) what characteristics of quantitative risk evaluation are proven to be helpful for the validation of a specific quantitative risk evaluation, and which frameworks have been established to deal with such effects? and (c) what types of claims are proposed regarding the quantitative risk analysis and what evidence is used for the quantitative risk analysis being valid for the stated purposes?

Yuan S, Yang M, Reniers G, et al. [43] first provided an overview of the history of the development of the safety barrier concept. Subsequently, they elaborated a systematic review of the definition, classification, evaluation, performance assessment, and management of safety barriers in the chemical process industries. Based on the literature review, they proposed a practical classification of safety barriers benefiting the identification of performance indicators and the collection of indicator-related data for safety barriers. The safety barrier functions were extended and illustrated by involving the resilience concept. Performance assessment criteria were proposed, corresponding to the adaptability and recoverability of the safety barriers. Finally, the management of safety barriers was discussed. The roadmap for future studies to develop integrated management of safety and security barriers to ensure the resilience of chemical plants was suggested.

Han Y, Zhen X, Huang Y, et al. [44] proposed a new integrated methodology to determine the maintenance interval of a specific group of safety barriers, which require periodic testing. Specifically, they dealt with the trade off between risk increase and reduction associated with maintenance, which optimizes the allocation of maintenance cost. The aims were minimizing the total risk level whilst reducing the maintenance cost. The dynamic data model was established, firstly to predict the state and trend of the risk level for the safety barriers. Then, the classification model was established to classify the risk level and optimize the allocation of maintenance cost. Finally, the maintenance decision model was established to balance the maintenance-related risks.

Gao X, Raman A A A, Hizaddin H F, et al. [45] investigated the development spectrum of inherent safety with a primary focus on the ISMs in chemical processes. Firstly, the basic cognition for inherent safety was encapsulated from its origin, early development, principles, implementation stages, and benefits. Subsequently, its current practice for creating FCP was highlighted via synthesizing the implementation spectrum of inherently safer design (ISD), ISMs and selection guidelines, and cost metrics. Meanwhile, the prominent industrial applications in the offshore industry, nuclear industry, dust explosion prevention, and risk-based safety interventions were also presented. Finally, some findings-based future research recommendations were concluded as the way forward.

Park S, Xu S, Rogers W, et al. [46] reviewed principal concepts, tools, and metrics for risk management and inherently safer design (ISD) during the conceptual stage of process design. Mainly, they analyzed ISD and inherent safety assessment tools (ISATs) from the perspective of inclusion in conceptual process design. They also highlighted the need to consider safety as a major component of process sustainability. In their paper, 73 ISATs were selected, and these tools were categorized into three groups: hazard-based inherent safety assessment tools (HISATs) for 22 tools, risk-based inherent safety assessment tools (RISATs) for 33 tools, and cost-optimal inherent safety assessment tools (COISATs) for 18 tools. They also introduced an integrated framework for coordinating the conventional process design workflow with safety analysis at various levels of detail.

From the existing research literature, researchers, except for Khan F, et al. [2], mainly focus on several research areas related to safety, like the domino effect [1,35], safety indices [33,38], risk assessment [34], life extension of safety critical systems [36,39], safety critical equipment [42], safety management [40], the validity and validation of quantitative risk analysis [41], safety barriers [43,44], inherent safety [45,46], etc. This article follows the footsteps of the literature [2] in some sense. However, the contributions of this article are

more in depth, more extensive, and more comprehensive with regard to the concepts of process safety, the interdependencies between safety and some others, progress of methods and models, development trends, characteristics, and challenges.

3. Progress of the Methods and Models in Process Safety

In general, the approach can be applied for the depiction of systematic guidelines or procedures for approaching or accomplishing the development of process safety. Correspondingly, the model covers the computational, probabilistic, empirical, analytical, and mathematical models that have been developed to conduct an analysis of the failures or hazards [2]. The progress of these methods and models is further categorized into three subcategories: the analysis methods and models, the assessment methods and models, and the decision support methods and models.

3.1. The Analysis Methods and Models

Generally speaking, safety and reliability need to be high in modern process industrial systems, which are often affected by human error, external causes, technique failure, and equipment or subsystem faults. In order to prevent accidents scientifically, comprehensive analysis of the mechanism of the accident process, evolving from initiation to the termination stage, is becoming an importance issue in order to avoid accidents. Currently, the widely used methods and models for safety analysis include mainly failure mode and effect analysis (FMEA) [21,56,57], hazard and operability analysis (HAZOP) [21,56], layer of protection analysis (LOPA) [58], fault tree analysis (FT) [5,24,27], event tree analysis (ET) [5,27,56], bowtie analysis (BT) [59–61], human reliability analysis (HRA) [26,62–66], loss functions (LF) [53,67], structural reliability analysis (SRA) [68], etc.

3.1.1. Failure Mode and Effect Analysis (FMEA)

The effect analysis and failure model concentrates mainly on the failure modes and individual components. Every failure mode is usually considered for once. All of the controls and effects are listed together [21]. In other words, FMEA is a comprehensive technique that is commonly used in fault scenarios resulting in multiple failure modes, and it can be used to examine potential failures in processes. It can be viewed as a type of bottom-up inductive risk evaluation tool, which is applied for the identification of the failure modes that can influence the general system in a negative way, and can be used for the assessment of the effect of these potential failure modes to confirm if changes are indeed necessary at any level to manage these adverse events [56].

The benefits of this approach are as follows:

1. A significant quantitative and qualitative analysis approach applied for the assessment of the potential failure modes and their impact on a system;
2. A systematic, inductive, and structure reasoning method involving the failure rates of every failure model to realize a quantitative probabilistic evaluation;
3. Extended to assess the failure modes that might lead to an undesired system condition, for instance the system hazard;
4. This would be very beneficial to use at the initial state of the system to enhance safety.

The major weaknesses are that:

1. It would be quite hard for this technique to identify the accident dependencies between human actions and equipment [21];
2. It focuses on the single failure of isolation;
3. It is not possible that several failures would occur, even though some hazards would arise originating from some other events and hazards;
4. It is not absolutely suitable for electrical and mechanical failure modes [56].

The goal of the FMEA technique in the available literature (Giardina M, et al. [21]) can be considered as the estimation of the component failure modes and their major effects. Kim S K, et al. [57] presented an evaluation process for determining the hardware safety integrity

level through failure modes, effects, and diagnostic analysis (FMEDA), which combines standard FMEA techniques with extensions to identify online diagnostic techniques.

3.1.2. Hazard and Operability (HAZOP) Analysis

Hazard and operability analysis can be considered as one of the most successful and widely used qualitative hazard identification methods. The ICI, namely Imperial Chemical Industries, first developed and used it to identify hazards and equipment failures [2].

A major feature of this method is that it can be applied to review systematically new or existing projects to assess the potential hazards, which are caused by misoperations or failures in parts of equipment. Therefore, HAZOP analysis is usually used in five stages of the system life cycle, viz., prototype, detailed design, use stage, accident investigation, and upgrade.

Furthermore, it is useful in engaging human behavior and performance, or any system that engages hazards that are difficult to identify or quantify. Correspondingly, the main limit is that it cannot be used as a quantitative analysis method, which is to rank the failures and effects to explore the relative efficiency of the corrective actions being proposed [21].

Moreover, it often does not consider the contact between various components within a process or a system, and it also can be lengthy, time consuming, and expensive [56]. Giardina M, et al. [21] employed HAZOP analysis to provide an identification of the operability issues and hazards via the logical sequences of the cause deviation consequence of process variables.

3.1.3. Layer of Protection Analysis (LOPA)

A process hazard analysis (PHA), such as a hazard and operability study (HAZOP), is a useful tool for identifying potential hazard scenarios; however, a PHA can only give a qualitative indication of whether sufficient safeguards exist to mitigate the hazards. Layer of protection analysis (LOPA) is a risk management technique commonly used in the chemical process industry that can provide a more detailed, semiquantitative assessment of the risks and layers of protection associated with hazard scenarios. LOPA allows the safety review team an opportunity to discover weaknesses and strengths in the safety systems used to protect employees, the plant, and the public. LOPA is a means to identify the scenarios that present the most significant risk and determine if the consequences could be reduced by the application of inherently safer design principles. LOPA can also be used to identify the need for safety instrumented systems (SISs) or other protection layers to improve process safety. Willey R J. [58] provides a brief overview of the technique, intended for a novice interested in the basic principles involved.

3.1.4. Fault Tree (FT) Analysis

Accident models are actually a type of theoretical system illustrating the relationship between the triggers and the outcomes, and vividly illustrate how and why accidents took place. From this perspective, the event/fault tree can be considered a graphic methodology, which can be employed to determine the failure probability of modern process industrial systems [5].

Generally, the top event, representing a major accident-initiating hazard, is set at the top of the tree, which is graphically modeled downward to permit the visualization of all the potential combinations of the wrong actions and malfunctions that would initiate the top event. The failure probability of the top event in parallel structure (AND gate) and in series structure (OR gate) can be calculated by Equations (1) and (2), respectively [5].

$$P = \prod_i P_i \tag{1}$$

$$P = \prod_i (1 - P_i). \tag{2}$$

The main advantage of the event/fault tree is that it can be considered as a proactive analysis method that can be applied to identify and explore the possible event sequence to achieve both quantitative and qualitative representation [5].

The fault tree in in the available literature Collong S, et al. [24] is proposed to analyze the reliability of explosion model. Similarly, fault tree analysis, in Ramzali N, et al. [27], is also used to quantify barriers failure probability of barriers.

3.1.5. Event Tree (ET) Analysis

Event tree analysis can be considered as a systematic approach for the exploration of the accident scenario. The event sequence is analyzed via the initiating event. The event tree usually begins with a particular initiating event and usually ends with potential outcomes, referred to as end states. The calculation of the state consequences and the occurrence probabilities can be conducted by Equation (3) [5].

$$P(C_k) = \prod_{SB_k} x_j^{\theta_{j,k}} \left(1 - X_j\right)^{1-\theta_{j,k}} \tag{3}$$

where SB_k is the prevention barrier related to level k ; $\theta_{j,k}$ means that level k failure passes through the failure branch of the prevention barrier i; $\theta_{j,k} = 0$ when level k failure passes through the success branch of prevention barrier i; and x_j is the failure probability of the prevention barrier.

Event trees are often easy to learn and apply and they can be used to combine machine, environment, and human interactions [56]. The main drawback can be considered to be that it lacks the ability to capture human error with the complexity of human behavior that will complicate the analysis [56].

In Ramzali N, et al. [27], event tree analysis is employed to assess the barriers of the initiating event, and to evaluate the sequence of events in a potential accident scenario following the occurrence of an initiating event.

3.1.6. Bowtie (BT) Analysis

In general, a bowtie diagram successfully combines the event tree and fault tree to investigate the primary causes and the outcomes of a critical event. It is suitable for the accident scenario and the model, which begin with the triggers and end with the outcomes of the accident scenario. In general, a bowtie diagram is mainly composed of a fault tree on the left-hand side to stand for the basic events leading to the top event, and an event tree on the right-hand side to explore the potential outcomes resulting from the top event, considering the operational failure of the safety barriers [59–61].

The superiority of this method is that:

1. It can be used to provide an accident scenario with qualitative modeling, being applied to offer a clear representation of the logic correlations between the basic and intermediate events leading to the top event, and how the failure of the safety barriers can eliminate the top event to accident consequences;
2. It can also be considered as quantitative modeling, with the quantitative assessment of the fault tree part, which requires the occurrence and failure possibility of the basic event.

Ferdous, et al. [59] used evidence theory and coefficient-based fuzzy methods to manage the model uncertainty for bowtie analysis, which was developed to analyze the BP Texas City accident. A bowtie risk model was mapped into a Bayesian network model by Staalduinen M A V, et al. [61], allowing for the application of different logical relaxation assumptions.

3.1.7. Human Reliability (HRA) Analysis

This takes the reliability of human operators as one of the determinant factors for the modern process industrial system, and its analysis methods can be employed to produce a human error probability for a given task or context. Generally, the analysis of human reliability can be viewed as a comprehensive system to evaluate the contribution of humans

to the system risk, which engages the evaluation process of the human performance, and also the corresponding influence over the structure, components, and system for a complex facility [62].

Dependence analysis is the evaluation of the impact of the failure on the operators to conduct an assignment on failure probabilities of the tasks afterwards, and it is very important to prevent the underestimation of the risk, since the dependent failure probability may be an order of magnitude larger than the independent one [62]. Obviously, the result should be a conditional human error probability on the given failure of the preceding task.

Assume that task T_B is subsequent to task T_A, and the corresponding basic probabilities of failure of task $T_{A,B}$ are marked as P_A and P_B, respectively, and A, B are the corresponding failure events. Then, the conditional human error probability of B, given A, can be determined by Equation (4).

$$P_{XD}(B \mid A) = (1 + k \cdot P_B)/(K + 1). \quad (4)$$

Therefore, the joint probability of dependent human failure events A, B can be calculated by Equation (5).

$$P_{XD}(B, A) = P_A \times (1 + k \cdot P_B)/(K + 1) \quad (5)$$

where $K = 0, 1, 6, 19, \infty$ for the dependence levels, labeled as complete (C), zero (Z), low (L), moderate (M), and high (H) dependence.

One of its drawbacks is that not enough data for the data analysis are accessible. Therefore, related conditional probabilities are inferred qualitatively from the essence of the tasks and also their corresponding interrelationships [62].

Abbassi R, et al. [26] proposed a novel method for the probability evaluation of human error by exploring the success likelihood index method with technique of human error rate prediction.

This study was conducted with the purpose, according to Su X, et al. [62], of illustrating a computational model to manage the dependence of human reliability analysis.

It can be applied to offer conclusions automatically on the general level of dependence and calculate the the conditional human error probability when the evaluations of the input factors are provided. Kim Y, et al. [63] put forward a scheme to classify the erroneous behaviors that the human reliability data extraction framework identified via the review on the related literature and a case study exploring the probability of human errors for the verification of the proposed scheme and its successful implementation for the categorization of the erroneous behaviors, and to evaluate whether the scheme would be helpful for the human error probability quantification goal.

Baybutt P [64] conducted an analysis of the different human factor issues that can impact the quality of process hazard analysis and layer of protection analysis, focusing on the offering, following up, documenting, recording, and conducting of the guidelines to minimize the degree to which such issues might destroy the research quality.

Noroozi A, et al. [65,66] conducted a study focusing on the analysis of human factors during pre-and-post pump maintenance operations, and took the removal procedures for the equipment from the service into consideration for possible failure scenarios.

The probability of human error for every scenario can be computed for every activity via the success likelihood index method in Ref. [65]. The human error assessment and reduction technique in Ref. [66] is used, while the corresponding outcomes are also evaluated based on this methodology.

3.1.8. Loss Functions (LF)

One important issue in any process industrial operation is the conformance to standards, which need to measure the distance between the process safety and the operational performance to match the design specifications. Recently, a new process performance indicator, namely loss functions, can be considered as the widely used method to quantify losses associated with the deviation from the expected level of conformance [67]. Generally,

loss functions can be used to model the system loss to identify the maximum loss and determine the shape parameters.

During recent years, various researchers and scholars have explored the four main categories of potential losses, which are composed of the environmental cleanup cost (ECC), human health loss (HHL), asset loss (AL), and production loss (PL). The human health loss, environmental cleanup cost and asset loss generally take place instantaneously during an accident. The quantification of such loss categories usually has the worst conditions as the basis for the evaluation of the maximum loss in each category, and the total estimated maximum loss for each abnormal event can be calculated by Equation (6) [53].

$$EML_j = \sum_i EML_{i,j}. \quad (6)$$

where *EML* is the estimation of maximum loss, and i and j counts the number of different losses, and denotes the number of undesired event scenarios, respectively. Loss functions are generally chosen to reflect the loss associated with process deviations, which trigger such losses when all the major process features deviate beyond the boundary of a safe operation [53].

Although there are many successful applications of LFs, it is obviously difficult to determine their exact form, as the performance of an LF is related to a key characteristic, and therefore using an inappropriate LF may lead to inaccurate results that either underestimate or overestimate the loss [6].

Hashemi S J, et al. [53] used loss functions to construct a risk-based process performance assessment methodology, which can be used to overcome the existing challenges in assessing impacts of deviations of process variables on the safety and economy of a process operation. Loss functions were used by Hashemi S J, et al. [67] to define the relationship between process deviations and system loss, and, moreover, properties associated with quadratic loss functions and a set of inverted probability loss functions were investigated and compared to achieve the purpose.

3.1.9. Structural Reliability Analysis (SRA)

Risk assessment is regarded as an effective tool for the design of ship structures, based on the safety level approach (SLA). However, there are gaps between the theoretical realization of the approach and its practical application, such as the lack of specific risk analysis tools for different structural failure modes. Ship structures have various failure modes under different hazards (e.g., ultimate limit state, accidental limit state, and fatigue limit state). In an accidental limit state, structural failure is generally a casual process from local damage to overall hull collapse, and is affected by structural uncertainty factors and accidental random impacts.

Li X, Tang W. [68] proposed a structural reliability analysis (SRA) model based on a Bayesian belief network (BBN) for the hull girder collapse risk after accidents. In this model, a BBN is used to represent the random states of variable risk events after accidents, as well as the dependencies between events; and an SRA is used to evaluate the failure probability of hull girders for each possible accident condition. Compared with the conventional methods, the risk level obtained is more reliable, given that different possible accident conditions are considered using the new model. The extreme accidental condition of the LNG leak, and subsequent cryogenic impacts on the structural strength, are also considered using the nonlinear finite element analysis (FEA) method.

3.2. The Assessment Methods and Models

Currently, safety evaluation can serve both as an important approach for the implementation and the satisfying of the policy of safety first and prevention orientation and also as the basis for the implementation of standardized and scientific enterprise management [51]. Meanwhile, a safety evaluation should be based on some indications of what to derive and where to look for these observations [52]. In general, such safety evaluation always involves

facility inspection, testing, and reviews of the materials, and covers the evaluation of the system and also the personnel and processes engaged during such development [5,69–72].

3.2.1. Safety Automation of Safety Critical Operations

Acharyulu, et al. [7] established an evaluation framework for the safety automation of safety critical operations to investigate multiple underlying risk evaluations, impacts, and factors to confirm the risk probabilities, attributes, and magnitude, based on practical conditions. It is on the basis of the results of the hazards analysis that the elements for the identification of the significance, the consequence, hazard detectability, probability of failure or accident, etc., are defined . Thus, the general framework consists mainly of six steps, which are shown in Figure 6.

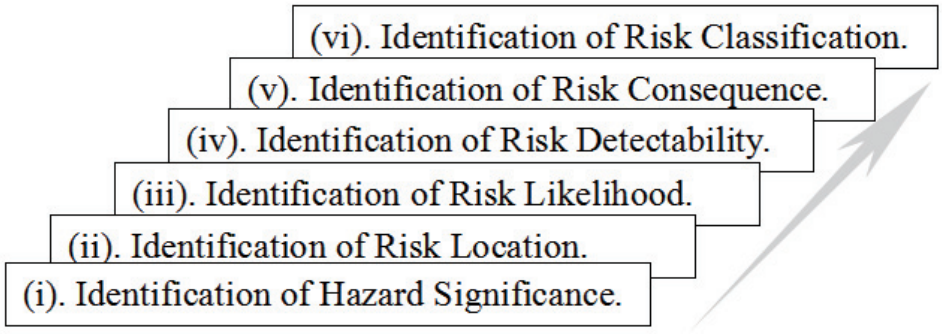


Figure 6. Procedures of assessment framework in Ref. [7].

By the same token, the superiority of such an approach can be thought of as that:

1. It offers clarity for the enhancement of the safety of humans, regulatory compliance, identified aspects, equipment, and the environment;
2. It is helpful in presenting documented evidence of the safe management of routine jobs and it updates the risk evaluation when there is operational change, which can demonstrate the new risks and identify the possible risks that might be missed by other methodologies;
3. It can be applied to offer information about the identification of risk classification, aspects impact, risk ranking, risks, and significant operations;
4. It helps to review the current risk category and make a comparison with the deeply addressed likelihood according to detect ability, consequence, and likelihood;
5. Its reports have been given great attention due to the safety measures being taken for each of the safety critical operations [7].

However, the constraints are also quite obvious. The safety automation for the safety critical mechanism operation actually requires strong expertise, apart from the technical know how, and strong logical extension to offer satisfactorily acceptable degrees [7].

3.2.2. American Petroleum Institute (API)

The American Petroleum Institute (API) Standard 780 Security Risk Assessment (SRA) methodology was issued in June 2013, serving as a U.S. standard for the evaluation of the security risk in petrochemical and petroleum facilities [8]. It can be viewed as a standard for the assessment of all the security risks of petrochemical and petroleum operations [8,73]. The significant and major issue of security risk evaluation is that the petrochemical and petroleum companies need to identify the risk holistically and systematically, which makes it a team-based approach, combing the knowledge of different participants and multiple skills to offer a comprehensive security evaluation of a facility and its operations.

As shown in Figure 7, step-1 of the methodology is the identification of those assets whose damage, loss of containment, theft, contamination, or degradation can result in severe consequences; step-2 is to identify the critical assets based on the severity of consequences thereof; step-3 and step-4 are to analyze the threats and attractiveness, respectively;

step-5 is to conduct scenario analysis to determine act-specific consequences and vulnerability; and step-6 and step- 7 are to assess risk against security criteria, and to evaluate security upgrades as required, respectively [8,73].

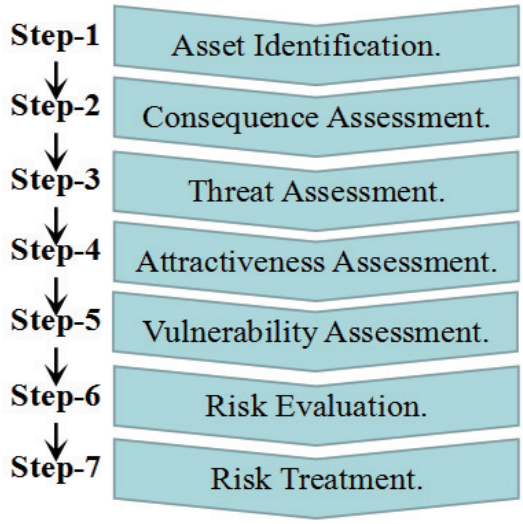


Figure 7. Seven steps of API security risk assessment methodology.

The superiority of this standard is that it assists management in decision making regarding risk-based performance measures to provide confidence that planned objectives will be achieved cost effectively with acceptable degrees of residual risk [8].

3.2.3. Numerical Descriptive Inherent Safety Technique

The numerical descriptive inherent safety technique can be considered as an outstanding approach for inherent safety assessment. Generally, such a method needs to have the logistic function in its implementation, which is suitable and also simpler for the research and development process [9].

Generally, two parts, namely process safety and chemical safety, make up this method. And each part considers four parameters. The four parameters of the former are reactivity, toxicity, explosiveness, and flammability. The assessment scores for all parameters can be calculated via a logistic equation. More details are available in Ref. [9].

Compared with current methods using an index-based method, this method is based on numerical methods, which can manage the constraints of the index-based approaches, and offers insights to explore the influence of the eight safety variables [9].

Moreover, the outcomes of the evaluation can be applied for the identification of the safest route among a series of alternatives for the process retrofitting and chemical synthesis, apart from emphasizing the possible hazard sources.The disadvantage is that it would not be applicable for the evaluation of the inherent safety issues during the research and design stage due to the limited amount of data available [9].

3.2.4. Safety Risk-Based Assessment Methodology

This considers safety risk evaluation as a kind of iterative process, indicating that a feedback loop from the risk assessment is made from the system depiction. This is conducted to evaluate whether the measures have decreased the risk to a degree that is acceptable [18]. Figure 8 presents the risk-oriented evaluation methodology that makes the analysis more exact.

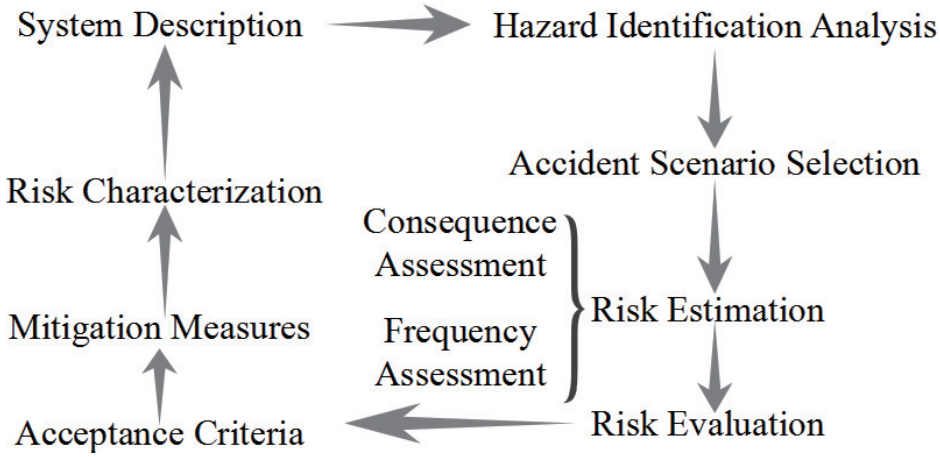


Figure 8. Procedures of safety risk based assessment methodology.

The system description serves as the first stage, and the work relates to the equipment and product features, processes, and related assumptions. The influence of the economy of a process operation and deviations of process variables also serve as an example [52]. There are massive devices conducting complex operations [59]. The subsequent step of the safety-risk-oriented evaluation method is applied for the identification of the possible hazards. This focuses on the major hazards of interest and also the mishap types that these hazards might generate [18].

The safety checklist analysis is then carried out [12,53], and the master logic diagram is also established [53]. At present, the major idea is to combine different techniques and hence guarantee that possible hazards are not overlooked [18]. When the identification of all these hazards is finished, it should select the accident scenario through one hazard, or via the combination of a series of hazards [18], which is connected with the possible deviations [53].

Generally, the accident scenario could engage a variety of factors, including health loss, safety loss, quality loss, or a combination of all of them [53,59]. As illustrated above, risk can be viewed as the combination of the severity of the harm and the occurrence of the harm [6]. This suggests that risk assessment is supposed to be viewed from two perspectives, namely consequence evaluation and frequency evaluation [18,53,59].

In general, after evaluating the severity and frequency, risk assessment can be computed through the risk matrix [4,59] through which the mitigation measures would be confirmed [18]. Safety refers to staying away from the unacceptable risk factors [6].

Thus, the acceptance standard is of great importance and can be built up according to the safety goals, which can be applied to confirm whether the risk degree can be accepted [18,53]. When the risk is assumed acceptable, there are some new mitigation measures that need to be introduced, while the risks associated with each scenario are supposed to be discussed again [18].

For the analysis of the options of the measures for risk mitigation, the majority of the issues are about whether the risk mitigation would be sufficient to decrease the risk to a tolerable degree. Ultimately, risk characterization illustrates the predicted incidence of adverse influences among a specific population group, identifying and emphasizing the risk conclusions and related uncertainties [18].

The benefit of this safety-risk-oriented evaluation approach is that:

1. It is capable of covering all the potential risk scenarios;
2. It offers risk profiles corresponding to various processes and conditions, which makes the continuous monitoring of process safety and integrated evaluation possible.

However, it is difficult to use due to it being complicated and time consuming. One issue that needs to be explained is that the procedure of safety-risk-based assessment methodology in Figure 6 is motivated by Ref. [18], and it is agreed with in this paper.

Furthermore, the differences of other safety-risk-based assessment methodologies are the different focuses, such as examining and evaluating the final outcomes of hydrogen release accident scenarios [18], overcoming the existing challenges in assessing the impacts of deviations of process variables on the safety and economy of a process operation [53], and so on.

3.2.5. Hybrid Assessment Model

The hybrid assessment method is proposed by Zhou J L, et al. [51,72], often incorporating some complementary methods, and considers the contact between self-feedback and the factors that should be applied to solve the issues with various levels of effects among the clusters [51]. By applying effective evaluation approaches, it assesses the importance of every factor in the system and the variables that need to beimproved [51]. In general, there are five phases in the hybrid evaluation model, which are presented in Figure 9.

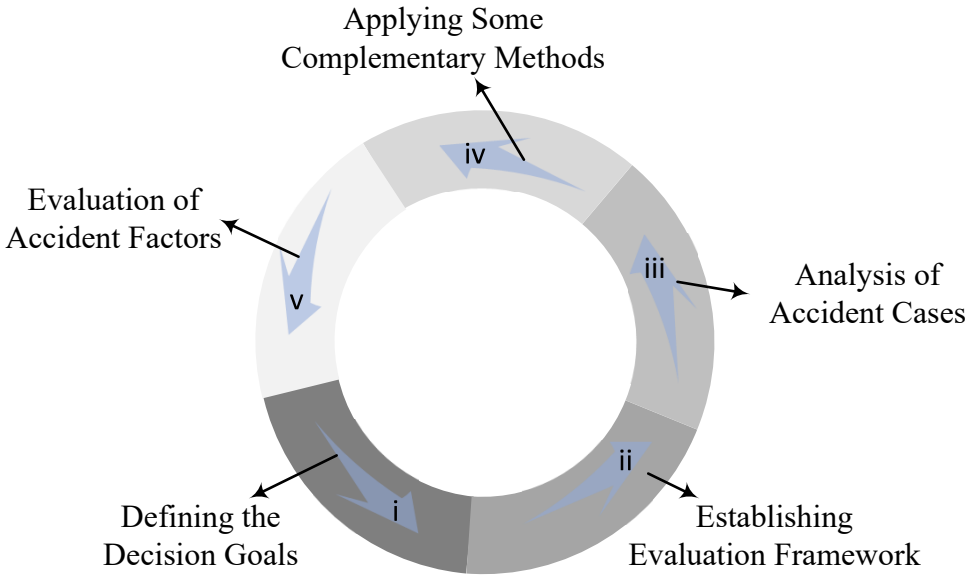


Figure 9. The procedures of the hybrid assessment model.

This approach mainly enjoys the following advantages:

1. It explores the active failures of the operators, combined with the latent situations upstream of the company;
2. It stimulates the accident researchers to look for the latent factors, taking the technological environment, physical atmosphere, and human unsafe behavior as examples [51,72];
3. The combination can be employed to make up the shortcomings of each model and to be closer to a real system.

3.2.6. Metrics Design Methods

Generally, safety assessment is refered to safety assurance and certification, and can be used to certify that the safety critical system meet the requirements [69]. As mentioned in the aviailable literature Luo Y, et al. [69], the idea of metrics can be considered as to identify costly processes, viz estimate the overall cost and monitor the whole compliance process.

Although a large number of methods have been reported for metric design, the goal question metric can be considered the most common one, where the metrics can be derived and collected to define the objectives and refine them into questions. Practical software and systems measurement have also been developed. However, this review is not be intended to start introducing various metrics design methods; instead, it will start with the perspective from Luo Y, et al. [69] to discuss this safety measure methodology.

Before using metrics design, three questions must be answered, as shown in Figure 10. Relevant metrics, therefore, can be composed by the intersection of what we want to measure and what we can measure, which are unified with the intersection of what we should measure and what we can measure [69].

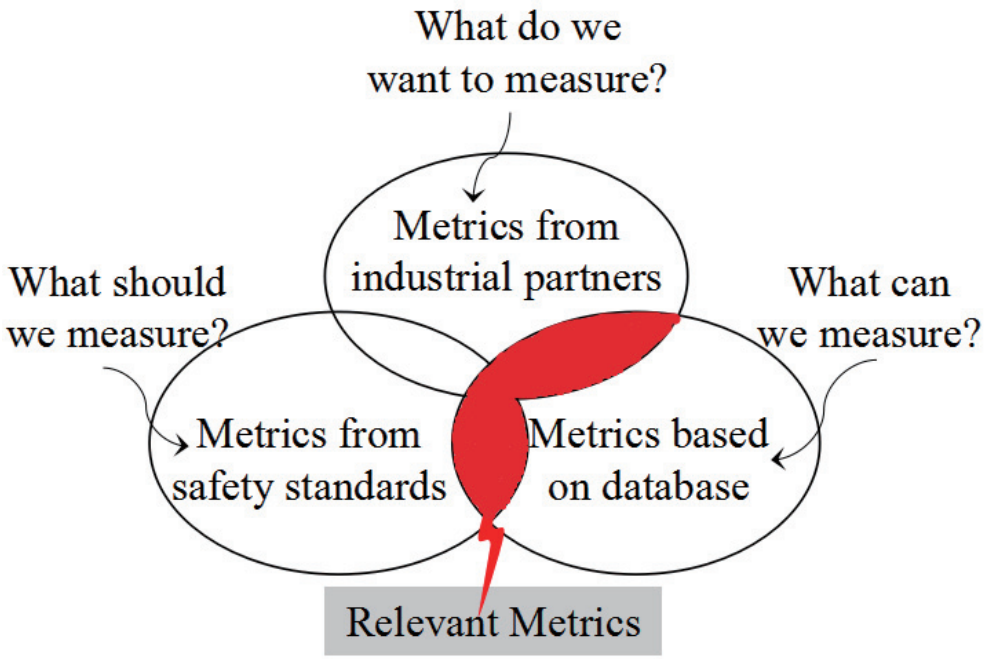


Figure 10. Three questions and their answers for metrics design.

Industrial interests can be considered as the answer to what do we what to measure?, because producers are strongly engaged in the actual process of their products, and their interests should be considered. Safety standards should be the answer to what should we measure? The reason is that the safety standards can be used to monitor safety processes and to show the degree of compliance with safety standards, which can be considered one of the crucial parts of safety assessment. The answer to what can we measure? is the available data: the way to eliminate some metrics can be considered to be based on the measurements of the available data for a given project or in some database [69].

As briefly discussed before, a huge amount of literature has been reported for describing the metrics design of software and models in both products and processes. These metrics are mainly used to measure complexity, quality, development effort, maintenance effort, etc., while few works deal with safety assessment, which is a relatively young domain. Therefore, metrics design for safety assessment can be considered as an area that is worthy of attention and continuous in-depth study.

3.2.7. Probabilistic Graphical Bayesian Network Method

The typical probabilistic graphical method is the Bayesian network (BN), which can be commonly applied to stand for a series of random variables and their conditional reliance through the directed acyclic graph and an associated joint probability distribution [54,74–77]. Obviously, graphical-model-based safety assessment, such as a graphical descriptive technique for inherent safety evaluation, is just referred to as the Bayesian network.

Generally, the nodes of a directed acyclic graph are often used to present random variables in the Bayesian sense, while edges are conditional dependencies between the connected ones. And each one is associated with a probability distribution as a function of the states of the nodes' parent variables [75,77]. The Bayesian network can be considered as a popular method for modeling and risk analysis for large and complex systems with its

flexible structure and probabilistic reasoning engine, and the joint probability distribution of various variables $U = X_1, X_2, \cdots, X_n$ can be calculated by Equation (7).

$$P(U) = \prod_{i=1}^{n} P(X_i / P_a(X_i)) \tag{7}$$

where $P_a(X_i)$ is the parent set of variable X_i, while the probability of X_i can be calculated by Equation (8).

$$P(X_i) = \sum_{U \setminus X_i} P(U) \tag{8}$$

The Bayesian network is based on the Bayes theorem to achieve the previous possibility of events, updated based on the named evidence, E, and new information, which can be in the form of occurrence of near incidents, mishaps and misses, or the observation of the outcomes of accidents that might be available in the lifecycle of the process. The evidence would be computed based on Equation (9).

$$P(U/E) = \frac{P(U,E)}{P(E)} = \frac{P(U,E)}{\sum_U P(U,E)} \tag{9}$$

The main advantage of the Bayesian network is the ability to evaluate the safety online by capturing all the information that can be possibly sampled by engineering systems [54]. On the other hand, the Bayesian network can be considered as a comprehensive and dynamic safety risk modeling system, and can be used to provide a risk-based investigation to identify the risk levels of all equipment [75].

3.2.8. Other Methods

Due to safety involving many aspects, models of safety assessment in different areas are numerous, safety assessment in the maritime domain [70], the American National Standards Institute (ANSI)/American Petroleum Institute (API) Standard 780 security risk assessment (SRA) methodology for the assist sectors and the petrochemical and petroleum operations and infrastructure [8], the fuzzy analytic hierarchy process for safety evaluation of coal mines [78], and so on. Other methods will not be covered in detail due to the limited space in this paper.

3.3. Decision Support Methods and Models

Safety control and management can be considered as a process in complex engineering, where relative parameters would truly change along within time and space. The goal of decision support methods and models is to ensure the safety of heath, the environment, and equipment during the operational period.

3.3.1. Safety Control Hierarchical Architecture

This safety control hierarchical architecture is based on safety instrumented systems and the standards IEC61511 and IEC 61508, and it consists of four modules [79], as shown in Figure 11.

As illustrated in Figure 11, prevention control should be applied for elimination of the risks through the application of the safety diagnosability principle of those critical/events faults that are initially unwanted. It consists of the hardware elements listed as follows, including the safety controller, safety actuators, and safety sensors. The mitigation control function is to mitigate or release the outcomes of the occurrence of the critical faults or unwanted events that are not appropriately treated, diagnosed, or detected by the prevention control system module. There are three hardware factors for mitigation control, including the safety controller, safety actuators, and safety sensors. The safety coordination control is to prevent the events that are unwanted initially through prevention control.

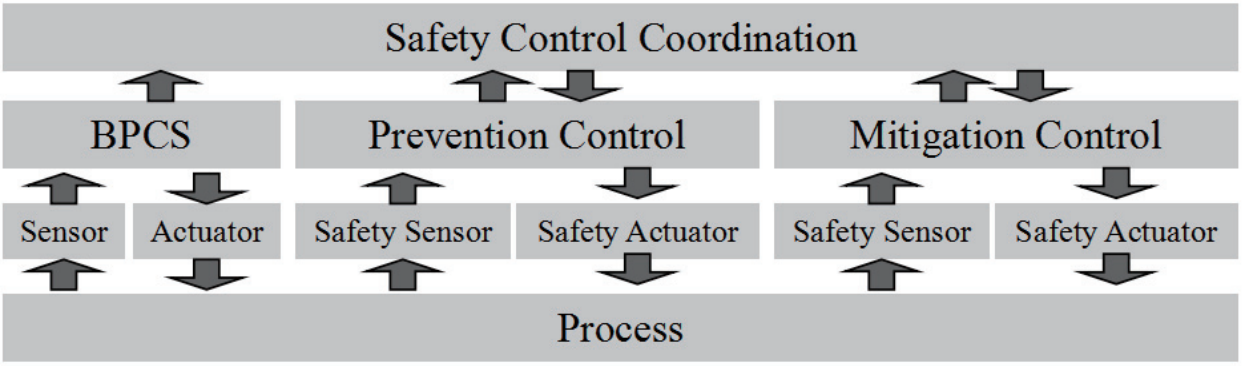


Figure 11. The safety control hierarchical architecture.

This system is composed of the following elements: safety controller, mitigation control safety sensors, prevention control safety sensors, and BPCS. The BPCS, namely the basic process control system, has a basic function, which is to impose the desired dynamic behavior on the process. It is composed of hardware factors, including a programmable logical controller, actuators, and sensors [79].

This control system guides the process with the control to a safety state by degenerating, controlled based on the reactive systems [79]. This method enjoys the advantage that it can be applied for the integration of the concept of reactivity related to the safety diagnosability and defense in depth, dealing with aspects that are relevant to critical fault description, mitigation, and prevention [79].

3.3.2. Total Safety Management

Total safety management can be used to establish a safe work environment that is conducive to peak performance and continual improvement [49]. The typical framework can be considered as the total operation management for safety critical activities (TOSCA), which was developed within the European Project and is aimed at integrating and enhancing safety, quality, and productivity [80,81]. This paper considers the TOSCA as an example to illustrate total safety management, as shown in Figure 12.

As shown in Figure 12, the total safety management framework is generally composed of several interrelated modules, including mainly the common operational picture, risk assessment for design, risk assessment for operations, and risk assessment for critical activities [49,80,81].

The common operational picture (COP) can be considered as a mental model of how the system works and to guide the use of the safety management system during the daily practice, where the aim is to manage, process, and collect information on the real-time emergency conditions that might occur during the process industry. It should offer a common understanding of multiple kinds of information visualized and required for the mitigation and avoidance of the accident, and offer information relevant to the human tasks and errors, evaluated by the task analysis, and overall risks assessed via quantitative risk assessment methods [49,80,81].

Risk and safety management often starts with the design phase of the whole lifecycle, where risk assessment should be conducted, which contributes to ensuring that risks are tolerable and helps in the refining of the design and in the identification of risks impacting on subsequent lifecycle phases [49,80,81].

The total safety management framework for operations is composed mainly of the supervision and control of the risks in the operational process. The operator performance data and system functioning data monitored by the knowledge system mainly include the functional depictions of the maintenance planning policies, work permits, checklists, current operating procedures, operational hazards, failure modes, effect analysis, P&ID of process equipment, and functional descriptions of subsystems and plant equipment [49,80,81].

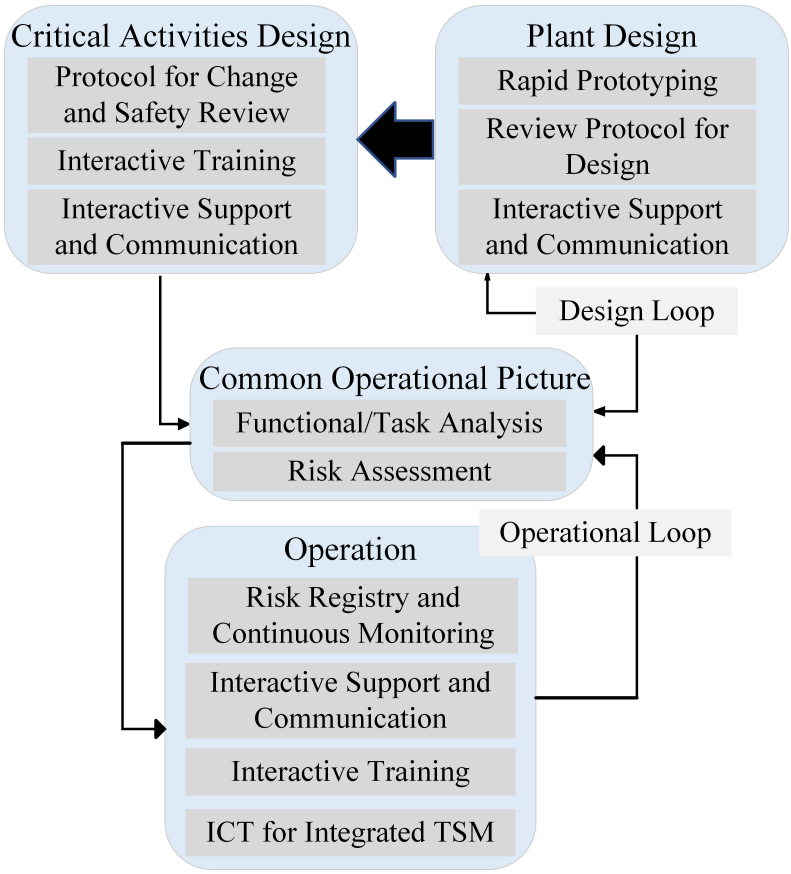


Figure 12. Typical framework TOSCA of total safety management.

It seems that the total safety management framework for critical activities can understand how these activities might either be a high risk or introduce major changes to the company. The procedure and methodology can be used for the distinction of the three major processes, including risk integration, assessment of the consequences, and the frequency of occurrence. The tasks of the plant damage states are to identify the possible accident initiators, evaluate the response of the plant to these initiators, and build up the end damage states of the plant leading to the release of dangerous substances into the environment. Evaluation of the outcomes is held with the purpose of confirming the outcomes of the released hazardous substances, or evaluating the possibility of injury to an individual receiving the dose calculated in the prior step. Risk integration successfully combines the consequences and results with the corresponding frequencies [49,80,81].

The main advantage of total safety management, especially the TOSCA, is that it can be used to determine a well-established and economically suitable framework, where innovative tools and techniques can be operated together to take advantage of the possible synergies in processing standards requirements, fulfilling regulations, improving safety, and enhancing productivity [49,80,81].

3.3.3. Situation Awareness Support System

Situation awareness can be considered as a state of mind of human beings, which is of great importance for the implementation of decision-making activities. It involves mainly three aspects, including the projection of the status in the near future, the comprehension of its meaning, and the perception of the elements in the environment [82]. In general, situation awareness is susceptible to the results of the relevant work status, for instance, stress and fatigue etc., which are quite common in the high-risk sectors, where personnel need to work in a remote installation or are exposed to dangerous conditions or a time-

pressured status [28]. Thus, the purpose of such a situation awareness support system is to deal with these uncertain statuses.

During the last few decades, situation awareness of operators has been regarded as the most important requirement for the process of decision making, and situation awareness is possibly the root of a series of accidents in safety critical environments where a series of goals can be simultaneously pursued. There are a series of tasks requiring the attention of the operator. The performance of the operator is also influenced by the time pressure and also possible negative results [83]. Currently, researchers and scholars around the world have developed many situation awareness support systems, and the typical one is the one created by Naderpour M, et al. [82–84], and this paper focuses on this method to introduce the aspects of the situation awareness support system.

Naderpour M, et al. [82–84] developed the situation awareness support system to conduct management, even under abnormal situations and in safety critical environments. It is made up by four major factors, including:

1. A condition that the data collection unit considers the online situations according to the supervising systems to offer the status quo of the observable variables;
2. A condition evaluation unit that applies the capacity of DBN, namely the dynamic Bayesian network, to model the mental model of the operator under abnormal conditions and a fuzzy logic mechanism to resemble the thinking of the operator when they are faced with these abnormal conditions;
3. A condition recovery unit that lays the foundation for the decision-making process to decrease the risk level of the conditions;
4. A human computer interface, as shown in Figure 13.

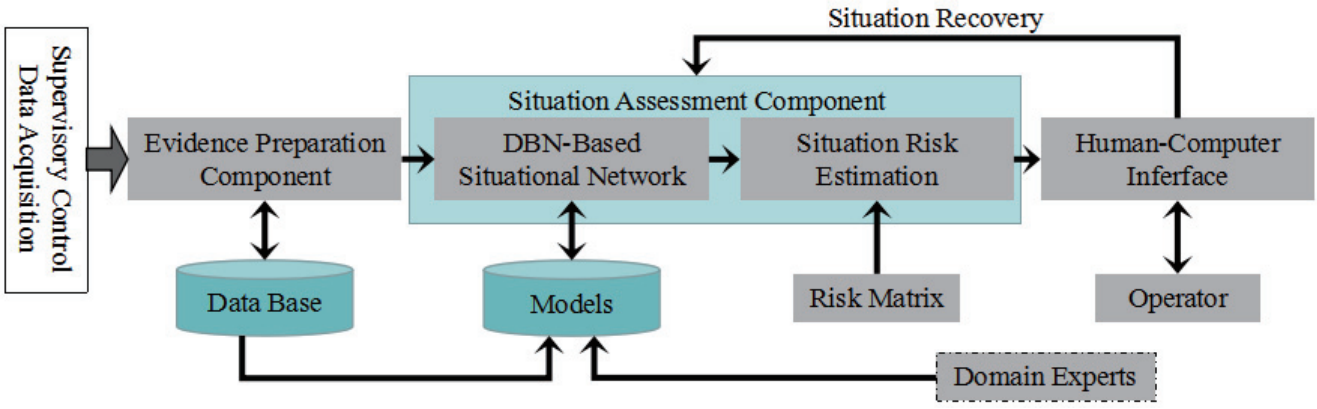


Figure 13. The model of the situation awareness support system.

As shown in Figure 13, the situation awareness support system is often developed based on the practice of design research. The situation data collection unit is used to collect the observable factors in the environment from field sensors. A discretization process is used to prepared the factors for application as evidence in the DBN-based models. An evaluation of the risk is made through the situation evaluation unit for every possible status, and demonstrates whether the risk is acceptable [82–84].

In general, the previous and posterior probabilities of the situation are provided by the DBN-based models, which are computed through a consequence severity matrix. Afterwards, a fuzzy logic system is utilized to predict the level of the situation risk. A basis for the decision making of the operator for the recovery of the situation is required for the prediction that the estimated risk is unacceptable [82–84].

Such a situation awareness support system graphical user interface had been developed, based on the capabilities of object-oriented BNs (OOBNs), which comprise both the usual nodes and the instance nodes, which are used for the development of the interface, as modeling the situation network in many safety critical systems has a number of variables that lead to complex models [82–84].

The main advantages of the situation awareness support system are that:

1. It is suitable for handling uncertain situations in humans with its essential characteristics;
2. It can be used to improve operator situation awareness, particularly in level 2 and 3.

The main limitation of this method is that its effect on operator workload needs more investigation.

3.3.4. HSE Management Systems

The HSE (Health, Safety and Environment) management system is a systematic and integrative management system developed in the 1980s [11]. It aims to ensure safe production, reduce risks, prevent accidents, and achieve sustainable development.

The principle of the HSE system is now well recognized in more process plants, like petrochemical plants, for its good performance. And several HSE system standards and systems have been formulated and developed by some organizations [11], like the International Organization for Standardization (ISO), European Union member states, Chinese government, etc. Initially, developing and improving the HSE system standards and guidelines was the main work. And currently, more attention has been paid to the performance measurement methods of HSE system effectiveness [11].

Generally, effective HSE system management should result in injury reduction, environment protection, performance improvement, and a distinctive leadership position. In other words, the task of the HSE system is to judge management levels and continuously improve performance, which can help enterprise managers to find defects and take remedial measures [85].

The disadvantage of HSE system management methods is that it is always time consuming to assess HSE system performance because there are so many evaluation indicators. A large number of studies have been reported in recent years, but this paper does not detail them.

3.3.5. Risk-Based Management for Safety Methods

In security risk management, the implementation of safety can be a complex and resource-demanding process, and its application may be quite unattractive and demanding, as it has strong requirements for iteration and can result in a large workload. However, there are continuous developments in the risk-based management framework to offer a scientific tool to support the decision-making process and to minimize the associated time by providing a real-time risk estimate.

The advantages and limitations of the different risk-based management methods reported and the existing technological and management challenges toward development of an efficient and practical dynamic risk management approach need to be considered [86–88]. A large number of studies have also been reported in recent years, but this paper does not detail them.

These methods mainly have the following advantages [86–88], including:

1. They can be applied to guarantee improvement of the risk management process according to the real-time process performance, which is revised based on the process and the failure history;
2. Their use can promote the risk-informed decision-making process through continuous monitoring, evaluation, and the enhancement of the process performance.

The major constrains of the current methods identified [86–88] include:

- The consideration of the univariate major features of the system that impact the risk;
- The ignorance of the possible complex dependency among the risk factors;
- The application of the deterministic probability values that add to the uncertainty of the estimated risk.

3.3.6. Other Methods

Due to the definition of safety in process industries, researchers and scholars around the world focus their studies on how to avoid the accident state, viz., make the systems free from the conditions that cause damage to humans, or loss of equipment or property.

And for the process industries, the damage to or loss of equipment or property means that the system operates in a unstable state, which will cause damage to humans. Therefore, almost all methods and models on safety decision-making support systems concentrate their targets on health, safety, and being environment friendly, such as life-extension decision making of safety critical systems [36], ensuring the quality of occupational safety [89], etc.

Because there are so many studies on safety decision making, many methods and models have not been introduced in detail. This paper just focuses on some typical methods and models that have the potential for future research.

4. Some Main Research Topics

According to the authors and the available literature in recent years, the main research should be focused on the assessment, design, and verification of safety in process industries, including inherent safety, safety integrity levels, operational safety, safety barriers, safety management, and human factors.

4.1. Inherent Safety

In some senses, inherent safety can be considered as one of the safety management procedures. However, it could be a independent one with its unique assessment and design methods.

In the early design stage of the process industries, when process operations and system designs are considered, the inherent safety design options could make the process system a better option to achieve higher standards and cost benefits [2]. However, a key factor that cannot be ignored is how to measure the level of inherent safety.

Most of the traditional approaches to the analysis or evaluation of inherent safety are based on hazard-based developments, viz., inherent safety evaluation indices studied by considering the worst potential hazards that could develop due to the operational conditions and cartographic emissions. Warnasooriya S, et al. [14] presented an inherent chemical process route index (ICPRI) that can be employed for the selection of the process routes of the early design stage, according to the inherent health and environmental friendliness based on the influence of the daily plant operational activities.

However, the principles of inherent safety should be made to concentrate on both hazard reduction and likelihood reduction. Ahmad S I, et al. [90] proposed a graphical descriptive technique for inherent safety assessment (GRAND) that can be used to evaluate the inherent safety during the research and development stage of process design. GRAND can be employed to show that hazard reduction and elimination play a major role in designing a user-friendly plant to prevent accidents.

Thus, the main focus of inherent safety should be to develop new inherent safety assessment techniques that will contribute to understanding the hazards and potential hazards of the processes [9]. Rusli R, et al. [91] aimed their study at the limitations and trade offs and conflicts that arose from the suggested modifications, and they used the risk-based method at the preliminary design stage to present a methodology for producing and evaluating inherent safety design alternatives, which can be applied to nitration of toluene with the objective of preventing and minimizing runway reactions.

In conclusion, incorporation of process design simulators is helpful in designing an inherent safety design process. But they are not suitable for assessing inherent safety due to unavailable data during the research and design stage. Therefore, the future research trend on inherent safety should be focused on incorporation of different methods and models, such as quantitative and qualitative techniques [92], etc., to ensure process safety and prevent hazards and potential hazards.

4.2. Safety Integrity Level

In general, the SIL, namely the safety integrity level, can be regarded as a system like the SIS, namely the safety instrumented system. This serves as an important protection layer to decrease the risks in the safety sector. In addition, the SIL is applied for the categorization of risk reduction, which suggests a sequence in the magnitude levels of the reduction of the risks. This is an important parameter in the majority of the processes of the safety lifecycle of the SIS. Based on the IEC 61508 Standard [29], the SIS has the capacity to realize a specific SIL, which needs to be validated at every process of the design and previous to any change occurring during the design subsequent to the commissioning [93].

SIL verification actually is a calculation of the possibility of failure for those process industries. Shu Y, et al. [93] put forward a simplified method by having a Markov analysis over every channel of a SIS via any kind of architecture. The results are combined together. However, how to evaluate the performance of a SIS in terms of operation integrity and safety integrity is an important issue. Innal F, et al. [94] conducted a study with a twofold focus:

1. It concentrates on the generic analytical formulations that can make the evaluation of a SIS performance possible, especially the operational integrity and safety integrity;
2. It focuses on the optimization of the SIS architecture design.

Because of the failure of the SIS in terms of realizing the expected functions, it would lead to serious consequence in terms of:

1. The safety issue of the supervising system (which is related to the safety integrity of the SIS);
2. Its availability in terms of production because of the false trips (related to the operational integrity of SIS) [94].

Thus, one of the future study trends in this sector is to concentrate on the verification and evaluation of the operational integrity and the safety integrity of the SIS. Cai B, et al. [74] conducted a study on the multiphase dynamic Bayesian networks of the SIS and put forward the novel safety integrity levels determination methodology. This approach can be applied for the analysis of the possibility of failure in the SIL of safety instrumented systems, the average possibility of failing safety, the possibility of failing safety, the average possibility of the failure on demands, and the possibility of failure on demands.

However, it is of great importance to consider one of the major factors, which is the uncertainty of the monitoring variables. In general, the design engineers make it possible to involve the rules of thumb and safety factors into the design and hence enhance the probability that the ultimate interlock installation will work as expected [93–97]. Freeman R, et al. [95] conducted a study focusing on the influence of uncertainty of data applied to the SIL computation of the quantitative assessment, which can decide the possibility of failure on the demands,and obtains the SIL of the SIS. Thus, future studies on the evaluation of the SIL for the SIS need to take the uncertainty into consideration.

4.3. Operational Safety

During the last few decades, engineering systems have become increasingly complex. In general, they work under various operational models. Operational safety serves as an important issue for the process industry and has attracted great attention from both scholars and industry. The differences between operational safety and safety are listed below. The former is well known. The operational safety of an engineering system might decrease when the process features drift with time, which leads to a dangerous situation [54].

It usually considers conventional safety evaluation as a kind of qualitative approach, for instance quantitative methods, FMEA (failure mode and effects) analysis, and HAZOP (hazards and operability analysis), such as the reliability block diagram, Markov models and fault trees. However, these methods need to work offline. It does not take multimode operating scenarios into account, which can quite possibly take place in practical engineering systems. Lin Y, et al. [54] put forward a probabilistic framework of online operational safety evaluation of the multimode engineering system through sample dependency. How-

ever, it has been shown that the topics covered by this research are quite limited. Thus, this is an important research topic.

4.4. Safety Barrier

Generally, a safety barrier is used for the protection of assets, the environment, and people from danger, and can be a type of nonphysical or physical method that is planned to mitigate, control, or prevent undesired events or accidents [25].

Xue L, et al. [25] proposed a new barrier-based accident model for the drilling of blowouts, based on a three-level well control theory. The extra well-monitoring barrier and primary and secondary well-control barriers are used for reservoir and blowout events.

Safety barriers are of great importance for the mitigation of possible risks. They can be applied in order to offer an organized way of considering the events relevant to safety system failure. The major advantages of the safety barrier are mitigating accidents and demonstrating directly the issues that are of primary concern to safety management [27].

Because the performance assessment of the safety barriers is dependent on the hazard scenarios, the operation procedures, and risk propagation, the existing industrial practices do not consider the performance assessment of the safety barriers for the avoidance of major accidents [98]. Kang J, et al. [98] built a new assessment approach that consists of three indicators, including the economic impact, the effectiveness, and the economic impact, to evaluate every indicator via mathematics theory.

As the qualitative and graphical descriptions are insufficient to implement practical prevent strategies, the safety barrier becomes more and more important in order to avoid or reduce the likelihood of escalation and the recommended use of multiple safety layers [99].

However, the accident model, the domino effect of risk, the safety measures, the accident control in safety barrier are all not studied clear, and these naturally become the focus of future research.

4.5. Industrial Big Data

During recent years, there has been growing attention on big data in this field because of the massive industrial data involved, which are generated mostly by the manufacturing industries. To stimulate the economic recovery and to grasp new chances for the development of this industrial revolution, developed nations have proposed some manufacturing-based stimulus policies to stimulate the integration of information technology with other, relevant advanced technologies, for instance the Industry 4.0 in Germany, Cyber Physical Systems in the US, etc. [100].

For intelligent systems, safety and reliability are of great importance, but they now have been challenged by a flexible, automated and complex industrial system. Moreover, it is believed that industrial big data enjoy 5V features, including value, veracity, variety, velocity, and volume. This challenges the models for the analysis of industrial big data and the application of conventional safety methods [100]. Special assessment techniques and safety analysis are required to process the unique properties of industrial big data, which are obviously different from the big data of social networks.

5. Conclusions and Future Research

The aims of this review article are to discuss the recent developments in process safety and present research trends in process industrial systems. It is hoped that the content can be used to inspire further improvements in process safety, security, and loss prevention for sustainable business performance. The scope of this review is restricted to the topics in the available literature; others sources, such as conference papers, are not considered due to limited space and availability.

The review article summarizes the definitions of process and safety and other related concepts, and it should be noted that safety in industrial processes, within this paper, can be attributed to the fact that the entire system does not have the ability to produce casualties,

health deterioration, and other accidents, which ultimately cause threats to human life and health damage.

There are some interdependencies between safety and its concerns, and similar definitions have been compared and discussed, especially reliability versus safety. It has been concluded that, if a system is in an unreliable state, then the system must be in an unsafe state. In addition, some related works have been summarized and discussed, including main organizations and regulations, literature reviews, and related available literature.

The progress of methods and models has also been summarized and discussed in the analysis and assessment of safety for process industrial systems, and mainly includes the safety on analysis, assessment and decision support. Each part has been detailed with the typical methods or models that have been reported in recent years, which can be used to illustrate the development of safety science in process industrial systems.

Finally, the developments over the last five years formulate the basis for the present trends, and these are also outlined, including inherent safety, operational safety, safety barriers, safety integrity levels, big data in industrial processes, and so on.

The systematic review of definitions, interdependencies, related works, and the models and methods developed, starting from original definitions to current studies in each area, can be used to motivate us to future research. It is clear that dynamic operational safety assessment under the big data challenges will be become the research direction and this will change the study situation. And this naturally becomes the primary research direction.

Author Contributions: Conceptualization, H.R. (Hao Ren); formal analysis, H.R. (Haojie Ren); investigation, Z.L.; writing—original draft preparation, J.Z.; writing—review and editing, H.R. (Hao Ren); visualization, X.L.; supervision, Y.C.; funding acquisition, Y.C. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Natural Science Foundation of China Under Grant 62103207, 52101323 and Grant 62103208, Shanghai Science and Technology Program Grant 22ZR1432300, the Chenguang Program of Shanghai Education Development Foundation and Shanghai Municipal Education Commission Grant 22CGA10, and the Major key project of Peng Cheng Laboratory (PCL) under Grant PCL2023AS7-1.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to thank the anonymous reviewers for careful reading and helpful remarks, and for making many contributions in improving the quality of this paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Nassim, A.; Cozzani, V.; Reniers, G.; Estel, L. Thresholds for domino effects and safety distances in the process industry: A review of approaches and regulations. *Reliab. Eng. Syst. Saf.* **2015**, *143*, 74–84.
2. Khan, F.; Rathnayaka, S.; Ahmed, S. Methods and models in process safety and risk management: Past, present and future. *Process. Saf. Environ. Prot.* **2015**, *98*, 116–147.
3. Sano, K.; Koshiba, Y.; Ohtani, H. Risk assessment and risk reduction of an acrylonitrile production plant. *J. Loss Prev. Process. Ind.* **2020**, *63*, 104015–104030.
4. Salehi, V.; Veitch, B. Measuring and analyzing adaptive capacity at management levels of resilient systems. *J. Loss Prev. Process. Ind.* **2020**, *63*, 104001–104034.
5. Adedigba, S.A.; Khan, F.; Yang, M. Dynamic safety analysis of process systems using nonlinear and non-sequential accident model. *Chem. Eng. Res. Des.* **2016**, *111*, 169–183.
6. *IEC 61511:2016*; Functional Safety-Safety Instrumented Systems for the Process Industry Sector. International Electrotechnical Commission: Geneva, Switzerland, 2016.
7. Acharyulu, P.V.S.; Seetharamaiah, P. A framework for safety automation of safety-critical systems operations. *Saf. Sci.* **2015**, *77*, 133–142.
8. Moore, D.A. Security Risk Assessment Methodology for the petroleum and petrochemical industries. *J. Loss Prev. Process. Ind.* **2013**, *26*, 1685–1689.

9. Fang, Y.; Rasel, M.A.K.; Richmond, P.C. Consequence risk analysis using operating procedure event trees and dynamic simulation. *J. Loss Prev. Process. Ind.* **2020**, *67*, 104235–104244.
10. Abílio Ramos, M.; López Droguett, E.; Mosleh, A.; Das Chagas Moura, M. A human reliability analysis methodology for oil refineries and petrochemical plants operation: Phoenix-PRO qualitative framework. *Reliab. Eng. Syst. Saf.* **2020**, *193*, 106672–106689.
11. Abrahamsen, E.B.; Moharamzadeh, A.; Abrahamsen, H.B.; Asche, F.; Heide, B.; Milazzo, M.F. Are too many safety measures crowding each other out? *Reliab. Eng. Syst. Saf.* **2018**, *174*, 108–113.
12. Dunn, A.L.; Payne, A.; Clark, P.R.; McKay, C. Process Safety in the Pharmaceutical Industry: A Selection of Illustrative Case Studies. *J. Chem. Educ.* **2020**, *98*, 175–182.
13. Teh, S.Y.; Chua, K.B.; Hong, B.H.; Ling, A.J.W.; Andiappan, V.; Foo, D.C.Y.; Hassim, M.H.; Ng, D.K.S. A hybrid multi-objective optimization framework for preliminary process design based on health, safety and environmental impact. *Processes* **2019**, *7*, 200–219. [CrossRef]
14. Warnasooriya, S.; Gunasekera, M.Y. Assessing Inherent Environmental, Health and Safety Hazards in Chemical Process Route Selection. *Process. Saf. Environ.* **2016**, *105*, 224–236.
15. Charolais, A.; Ammouri, F.; Vyazmina, E.; Werlen, E.; Harris, A. Safety Watchdog for universally safe gaseous high pressure hydrogen fillings. *Int. J. Hydrogen Energy* **2021**, *46*, 16019–16029. [CrossRef]
16. Ade, N.; Wilhite, B.; Goyette, H. An integrated approach for safer and economical design of Hydrogen refueling stations. *Int. J. Hydrogen Energy* **2020**, *45*, 32713–32729. [CrossRef]
17. Wang, K.; Zhang, X.; Miao, Y.; He, B.; Wang, C. Dispersion and behavior of hydrogen for the safety design of hydrogen production plant attached with nuclear power plant. *Int. J. Hydrogen Energy* **2020**, *45*, 20250–20255. [CrossRef]
18. Li, X.; Han, Z.; Zhang, R.; Zhang, Y.; Zhang, L. Risk assessment of hydrogen generation unit considering dependencies using integrated DEMATEL and TOPSIS approach. *Int. J. Hydrogen Energy* **2020**, *45*, 29630–29642. [CrossRef]
19. Yoo, B.H.; Wilailak, S.; Bae, S.H.; Gye, H.R.; Lee, C.J. Comparative risk assessment of liquefied and gaseous hydrogen refueling stations. *Int. J. Hydrogen Energy* **2021**, *46*, 35511–35524. [CrossRef]
20. Li, J.; Goerlandt, F.; Reniers, G.; Zhang, B. Sam Mannan and his scientific publications: A life in process safety research. *J. Loss Prev. Process. Ind.* **2020**, *66*, 104140–104151.
21. Giardina, M.; Morale, M. Safety study of an LNG regasification plant using an FMECA and HAZOP integrated methodology. *J. Loss Prev. Process. Ind.* **2015**, *35*, 35–45. [CrossRef]
22. Acheampong, T.; Kemp, A.G. Health, safety and environmental (HSE) regulation and outcomes in the offshore oil and gas industry: Performance review of trends in the United Kingdom Continental Shelf. *Saf. Sci.* **2022**, *148*, 105634–105656.
23. Lisowski, F.; Lisowski, E. Design of internal supports for double-walled liquefied natural gas road tanker. *Heat Transf. Eng.* **2021**, *43*, 238–247. [CrossRef]
24. Collong, S.; Kouta, R. Fault tree analysis of proton exchange membrane fuel cell system safety. *Int. J. Hydrogen Energy* **2015**, *40*, 8248–8260. [CrossRef]
25. Xue, L.; Fan, J.; Raus, M.; Zhang, L. A safety barrier-based accident model for offshore drilling blowouts. *J. Loss Prev. Process. Ind.* **2012**, *26*, 164–171. [CrossRef]
26. Abbassi, R.; Khan, F.; Garaniya, V.; Chai, S.; Chin, C.; Khandoker, A.H. An Integrated Method for Human Error Probability Assessment during the Maintenance of Offshore Facilities. *Process. Saf. Environ. Prot.* **2015**, *94*, 172–179. [CrossRef]
27. Ramzali, N.; Lavasani, M.R.M.; Ghodousi, J. Safety barriers analysis of offshore drilling system by employing Fuzzy Event Tree Analysis. *Saf. Sci.* **2015**, *78*, 49–59. [CrossRef]
28. Sneddon, A.; Mearns, K.; Flin, R. Stress, fatigue, situation awareness and safety in offshore drilling crews. *Saf. Sci.* **2012**, *56*, 80–88. [CrossRef]
29. *IEC 61508:2010*; Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. International Electrotechnical Commission: Geneva, Switzerland, 2010.
30. *IEC 61513:2011*; Nuclear Power Plants-Instrumentation and Control Important to Safety-General Requirements for Systems. International Electrotechnical Commission: Geneva, Switzerland, 2011.
31. *IEC 62061:2021*; Safety of Machinery-Functional Safety of Safety-Related Control Systems. International Electrotechnical Commission: Geneva, Switzerland, 2021.
32. *IEC 60335:2020*; Household and Similar Electrical Appliances-Safety. International Electrotechnical Commission: Geneva, Switzerland, 2020.
33. Roy, N.; Eljack, F.; Jiménez-Gutirrez, A.; Zhang, B.; Thiruvenkataswamy, P.; EI-Halwagi, M.; Mannan, M.S.. A review of safety indices for process design. *Curr. Opin. Chem. Eng.* **2016**, *14*, 42–48.
34. Kriaa, S.; Pietre-Cambacedes, L.; Bouissou, M.; Halgand, Y. A survey of approaches combining safety and security for industrial control systems. *Reliab. Eng. Syst. Saf.* **2015**, *139*, 156–178. [CrossRef]
35. Necci, A.; Cozzani, V.; Spadoni, G.; Khan, F. Assessment of domino effect: State of the art and research Needs. *Reliab. Eng. Syst. Saf.* **2015**, *143*, 3–18.
36. Shafiee, M.; Animah, I. Life extension decision making of safety critical systems: An overview. *J. Loss Prev. Process. Ind.* **2017**, *47*, 174–188.

37. Bergström, J.; Winsen, R.V.; Henriqson, E. On the rationale of resilience in the domain of safety: A literature review. *Reliab. Eng. Syst. Saf.* **2015**, *141*, 131–141. [CrossRef]
38. Swuste, P.; Theunissen, J.; Schmitz, P.; Reniers, G.; Blokland, P. Process safety indicators, a review of literature. *J. Loss Prev. Process. Ind.* **2015**, *40*, 162–173. [CrossRef]
39. Martins, L.E.G.; Gorschek, T. Requirements engineering for safetycritical systems: A systematic literature review.*Inf. Softw. Technol.* **2016**, *75*, 71–89. [CrossRef]
40. Yuling, L.; Frank, W.G. Safety management systems: A broad overview of the literature. *Saf. Sci.* **2018**, *103*, 94–123.
41. Goerlandt, F.; Khakzad, N.; Reniers, G. Validity and validation of safetyrelated quantitative risk analysis: A review. *Saf. Sci.* **2016**, *99*, 127–139. [CrossRef]
42. Broadribb, M.P.; Freiburger, E. Do you feel lucky? or do you want to identify and manage safety critical equipment? *Process. Saf. Prog.* **2018**, *37*, 340–346. [CrossRef]
43. Yuan, S.; Yang, M.; Reniers, G.; Chen, C.; Wu, J. Safety barriers in the chemical process industries: A state-of-the-art review on their classification, assessment, and management. *Saf. Sci.* **2022**, *148*, 105647–105664.
44. Han, Y.; Zhen, X.; Huang, Y.; Vinnem, J.E. Integrated methodology for determination of preventive maintenance interval of safety barriers on offshore installations. *Process. Saf. Environ. Prot.* **2019**, *132*, 313–324. [CrossRef]
45. Gao, X.; Raman, A.A.A.; Hizaddin, H.F.; Bello, M.M.; Buthiyappan, A. Review on the inherently safer design for chemical processes: Past, present and future. *J. Clean. Prod.* **2021**, *305*, 127154–127180.
46. Park, S.; Xu, S.; Rogers, W.; Pasman, H.; EI-Halwagi, M.M. Incorporating inherent safety during the conceptual process design stage: A literature review. *J. Loss Prev. Process. Ind.* **2020**, *63*, 104040–104105.
47. Hollnagel, E. Is safety a subject for science? *Saf. Sci.* **2013**, *67*, 21–24. [CrossRef]
48. Hopkins, A. Issues in safety science. *Saf. Sci.* **2013**, *67*, 6–14. [CrossRef]
49. Kontogiannis, T.; Leva, M.C.; Balfe, N. Total Safety Management: Principles, processes and methods. *Saf. Sci.* **2016**, *100*, 128–142.
50. Aven, T. What is safety science? *Saf. Sci.* **2013**, *67*, 15–20. [CrossRef]
51. Zhou, J.L.; Bai, Z.H.; Sun, Z.Y. A hybrid approach for safety assessment in high-risk hydro-power-construction-project work systems. *Saf. Sci.* **2014**, *64*, 163–172. [CrossRef]
52. Coze, J.C.L. Outlines of a sensitising model for industrial safety assessment. *Saf. Sci.* **2013**, *51*, 187–201. [CrossRef]
53. Hashemi, S.J.; Ahmed, S.; Khan, F.I. Risk-based operational performance analysis using loss functions. *Chem. Eng. Sci.* **2014**, *116*, 99–108. [CrossRef]
54. Lin, Y.; Chen, M.; Zhou, D. Online probabilistic operational safety assessment of multi-mode engineering systems using Bayesian methods. *Reliab. Eng. Syst. Saf.* **2013**, *119*, 150–157. [CrossRef]
55. Ouache, R.; Kabir, M.N.; Adham, A.A.J. A reliability model for safety instrumented system. *Saf. Sci.* **2015**, *80*, 264–273. [CrossRef]
56. Altabbakh, H. M.; Alkazimi, M.A.; Murray, S.; Grantham, K. STAMP-Holistic system safety approach or just another risk model? *J. Loss Prev. Process. Ind.* **2014**, *32*, 109–119. [CrossRef]
57. Kim, S.K.; Yong, S.K. An evaluation approach using a HARA and FMEDA for the hardware SIL. *J. Loss Prev. Process. Ind.* **2013**, *26*, 1212–1220. [CrossRef]
58. Willey, R.J. Layer of protection analysis. *Procedia Eng.* **2014**, *84*, 12–22. [CrossRef]
59. Ferdous, R.; Khan, F.; Sadiq, R. Analyzing system safety and risks under uncertainty using a bow-tie diagram: An innovative approach. *Process. Saf. Environ. Prot.* **2013**, *91*, 1–18.
60. Chen, L.; Li, X.; Cui, T.; Ma, J. Combining accident modeling and quantitative risk assessment in safety management. *Adv. Mech. Eng.* **2017**, *32*, 1–10.
61. Staalduinen, M.A.V.; Khan, F.; Gadag, V.; Reniers, G. Functional quantitative security risk analysis (QSRA) to assist in protecting critical process infrastructure. *Reliab. Eng. Syst. Saf.* **2016**, *157*, 22–34. [CrossRef]
62. Su, X.; Mahadevan, S.; Xu, P.; Deng, Y. Inclusion of task dependence in human reliability analysis. *Reliab. Eng. Syst. Saf.* **2014**, *128*, 41–55. [CrossRef]
63. Kim, Y.; Park, J.; Jung, W. A classification scheme of erroneous behaviors for human error probability estimations based on simulator data. *Reliab. Eng. Syst. Saf.* **2017**, *163*, 1–13. [CrossRef]
64. Baybutt, P. The role of people and human factors in performing process hazard analysis and layers of protection analysis. *J. Loss Prev. Process. Ind.* **2013**, *26*, 1352–1365. [CrossRef]
65. Noroozi, A.; Khakzad, N.; Khan, F.; MacKinnon, S.; Abbassi, R. The role of human error in risk analysis: Application to pre- and post-maintenance procedures of process facilities. *Reliab. Eng. Syst. Saf.* **2013**, *119*, 251–258.
66. Noroozi, A.; Khan, F.; Mackinnon, S.; Amyotte, P.; Deacon, T. Determination of human error probabilities in maintenance procedures of a pump. *Process. Saf. Environ. Prot.* **2014**, *92*, 131–141. [CrossRef]
67. Hashemi, S.J.; Ahmed, S.; Khan, F. Loss functions and their applications in process safety assessment. *Process. Saf. Prog.* **2014**, *33*, 285–291.
68. Li, X.; Tang, W. Structural risk analysis model of damaged membrane LNG carriers after grounding based on Bayesian belief networks. *Ocean. Eng.* **2019**, *171*, 332–344. [CrossRef]
69. Luo, Y.; Brand, M.G.J.V.D. Metrics design for safety assessment. *Inf. Softw. Technol.* **2016**, *73*, 151–163.
70. Montewka, J.; Goerlandt, F.; Kujala, P. On a systematic perspective on risk for formal safety assessment (FSA). *Reliab. Eng. Syst. Saf.* **2014**, *127*, 77–85.

71. Hamad, N.A.; El-Halwagi, M.M.; Elbashir, N.O.; Mannan, S.M. Safety assessment of potential supercritical solvents for Fischer-Tropsch Synthesis. *J. Loss Prev. Process. Ind.* **2012**, *26*, 528–533.
72. Zhou, J.L.; Bai, Z.H.; Sun, Z.Y. Safety Assessment of High-Risk Operations in Hydroelectric-Project Based on Accidents Analysis, SEM, and ANP. *Math. Probl. Eng.* **2013**, *2013*, 530198. [CrossRef]
73. Khakzad, N.; Reniers, G.; Gelder, P.V. A multi-criteria decision making approach to security assessment of hazardous facilities. *J. Loss Prev. Process. Ind.* **2017**, *48*, 234–243. [CrossRef]
74. Cai, B.; Liu, Y.; Fan, Q. A multiphase dynamic Bayesian networks methodology for the determination of safety integrity levels. *Reliab. Eng. Syst. Saf.* **2016**, *150*, 105–115.
75. Zarei, E.; Azadeh, A.; Khakzad, N.; Aliabadi, M.M.; Mohammadfam, I. Dynamic safety assessment of natural gas stations using Bayesian Network. *J. Hazard. Mater.* **2017**, *321*, 830–840. [CrossRef]
76. Abimbola, M.; Khan, F.; Khakzad, N.; Butt, S. Safety and risk analysis of managed pressure drilling operation using Bayesian network. *Saf. Sci.* **2015**, *76*, 133–144. [CrossRef]
77. Zhang, L.; Wu, X.; Qin, Y.; Skibniewski, M.J.; Liu, W. Towards a Fuzzy Bayesian Network Based Approach for Safety Risk Analysis of Tunnel-Induced Pipeline Damage. *Risk Anal.* **2016**, *36*, 278–301. [CrossRef]
78. Wang, Q.; Wang, H.; Qi, Z. An application of nonlinear fuzzy analytic hierarchy process in safety evaluation of coal mine. *Saf. Sci.* **2016**, *86*, 78–87. [CrossRef]
79. Squillante, R. J.; Filho, D.J.S.; Silva, R.M.D.; Souza, J.A.L.; Junqueira, F.; Miyagi, P.E. A Novel Safety Control Hierarchical Architecture for Prevention and Mitigation of Critical Faults in Process Industries based on Defense-in-depth, Reactive Systems and Safety-diagnosability. *IFAC Pap.* **2014**, *48*, 1326–1331. [CrossRef]
80. Aneziris, O.N.; Nivolianitou, Z.; Konstandinidou, M.; Mavridis, G.; Plot, E. A Total Safety Management framework in case of a major hazards plant producing pesticides. *Saf. Sci.* **2017**, *100*, 183–194. [CrossRef]
81. Leva, M.C.; Balfe, N.; Kontogiannis, T.; Plot, E.; Demichela, M. Total safety management: What are the main areas of concern in the integration of best available methods and tools. *Chem. Eng. Trans.* **2014**, *36*, 559–564.
82. Naderpour, M.; Lu, J.; Zhang, G. A situation risk awareness approach for process systems safety. *Saf. Sci.* **2014**, *64*, 173–189. [CrossRef]
83. Naderpour, M.; Lu, J.; Zhang, G. An intelligent situation awareness support system for safety-critical environments. *Decis. Support Syst.* **2014**, *29*, 325–340. [CrossRef]
84. Naderpour, M.; Lu, J.; Zhang, G. A safety-critical decision support system evaluation using situation awareness and workload measures. *Reliab. Eng. Syst. Saf.* **2016**, *150*, 149–159. [CrossRef]
85. Li, W.; Liang, W.; Zhang, L.; Tang, Q. Performance assessment system of health, safety and environment based on experts' weights and fuzzy comprehensive evaluation. *J. Loss Prev. Process. Ind.* **2015**, *35*, 995–103. [CrossRef]
86. Khan, F.; Hashemi, S.J.; Paltrinieri, N.; Amyotte, P.; Cozzani, V.; Reniers, G. Dynamic risk management: a contemporary approach to process safety management. *Curr. Opin. Chem. Eng.* **2016**, *14*, 9–17. [CrossRef]
87. Yuan, Z.; Khakzad, N.; Khan, F.; Amyotte, P.; Reniers, G. Risk-Based Design of Safety Measures To Prevent and Mitigate Dust Explosion Hazards. *Ind. Eng. Chem. Res.* **2013**, *52*, 18095–18108. [CrossRef]
88. Yuan, Z.; Khakzad, N.; Khan, F.; Amyotte, P. Risk-based optimal safety measure allocation for dust explosions. *Saf. Sci.* **2014**, *74*, 79–92. [CrossRef]
89. Pinto, A.; Ribeiro, R.A.; Nunes, I.L. Ensuring the Quality of Occupational Safety Risk Assessment. *Risk Anal.* **2013**, *33*, 409–419. [CrossRef]
90. Ahmad, S.I.; Hashim, H.; Hassim, M.H. A graphical method for assessing inherent safety during research and development phase of process design. *J. Loss Prev. Process. Ind.* **2015**, *42*, 59–69. [CrossRef]
91. Rusli, R.; Shariff, A.M.; Khan, F.I. Evaluating hazard conflicts using inherently safer design concept. *Saf. Sci.* **2012**, *53*, 61–72. [CrossRef]
92. Abidin, M.Z.; Rusli, R.; Buang, A.; Shariff, A.M.; Khan, F.I. Resolving inherent safety conflict using quantitative and qualitative technique. *J. Loss Prev. Process. Ind.* **2016**, *44*, 95–111. [CrossRef]
93. Shu, Y.; Zhao, J. A simplified Markov-based approach for safety integrity level verification. *J. Loss Prev. Process. Ind.* **2014**, *29*, 262–266. [CrossRef]
94. Innal, F.; Dutuit, Y.; Chebila, M. Safety and operational integrity evaluation and design optimization of safety instrumented systems. *Reliab. Eng. Syst. Saf.* **2014,** *134*, 32–50. [CrossRef]
95. Freeman, R.; Summers, A. Evaluation of uncertainty in safety integrity level calculations. *Process. Saf. Prog.* **2016**, *35*, 341–348. [CrossRef]
96. Baybutt, P. Overcoming challenges in using layers of protection analysis (LOPA) to determine safety integrity levels (SILS). *J. Loss Prev. Process. Ind.* **2017**, *48*, 32–40. [CrossRef]
97. Ding, L.; Wang, H.; Kang, K.; Wang, K. A novel method for SIL verification based on system degradation using reliability block diagram. *Reliab. Eng. Syst. Saf.* **2014**, *132*, 36–45. [CrossRef]
98. Kang, J.; Zhang, J.; Gao, J. Analysis of the safety barrier function: Accidents caused by the failure of safety barriers and quantitative evaluation of their performance. *J. Loss Prev. Process. Ind.* **2016**, *43*, 361–371. [CrossRef]

99. Landucci, G.; Argenti, F.; Spadoni, G.; Cozzani, V. Domino effect frequency assessment: The role of safety barriers. *J. Loss Prev. Process. Ind.* **2016**, *44*, 706–717. [CrossRef]
100. Yan, J.; Meng, Y.; Lu, L.; Li, L. Industrial Big Data in an Industry 4.0 Environment: Challenges, Schemes and Applications for Predictive Maintenance. *IEEE Access* **2017**, *5*, 23484–23491. [CrossRef]