signals

MDPI

Review

Towards Integration of Security and Safety Measures for Critical Infrastructures Based on Bayesian Networks and Graph Theory: A Systematic Literature Review

Sandeep Pirbhulal [1,2,*], Vasileios Gkioulos [1] and Sokratis Katsikas [1]

[1] Department of Information Security and Communication Technology, Norwegian University of Science and Technology, 2815 Gjøvik, Norway; vasileios.gkioulos@ntnu.no (V.G.); sokratis.katsikas@ntnu.no (S.K.)
[2] Norwegian Computing Center, P.O. Box 114, Blindern, 0314 Oslo, Norway
* Correspondence: sandeep@nr.no; Tel.: +47-41-393-687

Abstract: In recent times, security and safety are, at least, conducted in safety-sensitive or critical sectors. Nevertheless, both processes do not commonly analyze the impact of security risks on safety. Several scholars are focused on integrating safety and security risk assessments, using different methodologies and tools in critical infrastructures (CIs). Bayesian networks (BN) and graph theory (GT) have received much attention from academia and industries to incorporate security and safety features for different CI applications. Hence, this study aims to conduct a systematic literature review (SLR) for co-engineering safety and security using BN or GT. In this SLR, the preferred reporting items for systematic reviews and meta-analyses recommendations (PRISMA) are followed. Initially, 2295 records (acquired between 2011 and 2020) were identified for screening purposes. Later on, 240 articles were processed to check eligibility criteria. Overall, this study includes 64 papers, after examining the pre-defined criteria and guidelines. Further, the included studies were compared, regarding the number of required nodes for system development, applied data sources, research outcomes, threat actors, performance verification mechanisms, implementation scenarios, applicability and functionality, application sectors, advantages, and disadvantages for combining safety, and security measures, based on GT and BN. The findings of this SLR suggest that BN and GT are used widely for risk and failure management in several domains. The highly focused sectors include studies of the maritime industry (14%), vehicle transportation (13%), railway (13%), nuclear (6%), chemical industry (6%), gas and pipelines (5%), smart grid (5%), network security (5%), air transportation (3%), public sector (3%), and cyber-physical systems (3%). It is also observed that 80% of the included studies use BN models to incorporate safety and security concerns, whereas 15% and 5% for GT approaches and joint GT and BN methodologies, respectively. Additionally, 31% of identified studies verified that the developed approaches used real-time implementation, whereas simulation or preliminary analysis were presented for the remaining methods. Finally, the main research limitations, concluding remarks and future research directions, are presented

Keywords: graph theory; Bayesian networks; safety; security; critical infrastructures; literature review

Citation: Pirbhulal, S.; Gkioulos, V.; Katsikas, S. Towards Integration of Security and Safety Measures for Critical Infrastructures Based on Bayesian Networks and Graph Theory: A Systematic Literature Review. *Signals* **2021**, *2*, 771–802. https://doi.org/10.3390/signals2040045

Academic Editors: Vessela Krasteva and Toshihisa Tanaka

Received: 15 June 2021
Accepted: 28 October 2021
Published: 2 November 2021

1. Introduction

In recent times, the growth of the internet of things (IoT) and information communication technologies (ICT) have revolutionized the modern era and critical infrastructures (CIs), including smart manufacturing, healthcare, energy sector, education, and maritime transportation, among others [1,2]. On the one hand, modern communication and electronic technologies have provided many facilities to individuals and nations in different CIs. On the other hand, safeguarding security and safety are essential requirements to offer authenticated operations against possible cyber threats and crises within the respective CIs [3]. Generally, the security mechanisms focus on recognizing and managing risks interrelated with accessibility, privacy, and integrity of devices in CIs. However, safety

approaches are inclined to predict, classify, and resolve the vulnerabilities linked with the safety of humans, systems, and infrastructures. Therefore, integrating both aspects can help identify potential vulnerabilities and threats and the evaluate probable risks associated with the security and safety of CIs.

The incorporation of security and safety aspects has received massive attention worldwide [4,5]. Recent research shows that safety, especially cybersecurity, share interdependencies in many products, especially cyber-physical systems (CPS) [6]. Besides safety regulations interfering in possible security solutions, a fundamental problem is the rising number of cybersecurity threats that negatively impact the affected functional safety and reliability of systems [7]. In safety-sensitive environments, such as the in railway, aircraft, or automotive industries, the consideration of security is widespread [8]. Decision-makers must determine whether the identified issue is due to an attack or technical failure. A precise diagnosis is crucial for an effective response to identified problems. For example, fixing or exchanging the module responsible for the observed issue could be a reasonable response tactic for a technical failure. Simultaneously, blocking an attack vector, utilizing an identified adversary-caused problem, might be an efficient response monitoring strategy.

If the decision-makers can calculate that the apparent problem is an attack, the efficient response policies to resist each attack vector would be dissimilar. For example, the operative response approach for an information manipulation threat on the device could acquire data integrity checks. In contrast, the active response approach against the physical tampering of the device would augment access control. Remarkably, the decision supporting the regulation of the utmost probable root cause for evident problems is not available. In these conditions, Bayesian networks (BNs) could be helpful to solve this problem, mainly cybersecurity and safety applications [4–7]. In BNs, both qualitative and quantitative components are included, such as the directed acyclic graph (DAG) and conditional probability table (CPT), for each node in the DAG, respectively [8]. Furthermore, the graph theory (GT) and neutral network are also incorporated with the safety aspects of network security [9].

Some systematic literature reviews (SLRs) or literature reviews related to safety and security, based on BNs or GT, are available in the literature. Sharma et al. presented a systematic review of safety and security measures for machine learning-enabled agricultural applications. The focus of this study was BN approaches; however, GT was not addressed [10]. Gupta et al. performed a systematic review on blockchain-oriented security outbreak resilience systems for self-governing automobiles. The main limitations are that vehicle applications and their safety aspects are not considered [11]. Chockalingam et al. conducted SLR on 17 BN-based models for integrating cybersecurity and safety measures in different applications [12]. The main drawback of this SLR includes that it merely emphasized BN models; however, GT was not addressed. Lallie et al. reviewed the threat graphs and visual tree syntax-based GT mechanisms, which describe the cyber-attacks central theory, before elaborating on how vital components of a cyber-attack are characterized in attack graphs and outbreak trees. However, safety concerns are not addressed [13]. The main problem with the studies mentioned above is that the SLR or review, based on either GT or BN, ensures safety and security. Since GT and BN are practical approaches to analyzing safety and security risks, there is still a lack of SLR based on both these approaches.

This SLR aims to present current inclinations and advancements, as well as the limitations of incorporating safety and security using GT and BN. The chief contributions of this study are the following:

(a) To identify records, using search queries from numerous databases, including Scopus, ACM, and the Web of Sciences, focusing on united safety and security using GT and BN models.
(b) To perform a comprehensive comparative interpretation of classified approaches, regarding threat actors, performance verification mechanisms, the number of applied nodes for system development, and implementation scenarios, among others, for combining safety and security aspects using GT or BN methodologies.

(c) To illustrate the research consequences of this SLR, based on pre-defined research questions (RQs).
(d) To elaborate pros and cons, limitations, and future research directions of BN and GT approaches for integrating safety and security.

The organization of this paper is stated as follows: the background, to analyze security and safety risks for CIs using BN and GT approaches, is represented in Section 2. In Section 3, the research design, including research questions (RQs), search query, and pre-defined criteria of records, are demonstrated. In Section 4, the identified studies were compared in different aspects, such as application sectors, implementation criteria, applicability, etc. The discussion of RQs, based on included studies, as well as the limitations, are presented in Section 5. Finally, in Section 6, the concluding remarks and future research directions are represented.

2. Background

Incorporating safety and security has received great attention for different applications; a few unified approaches have been designed to evaluate both measures. Though security analysis is implemented in the overall design procedure, it is generally not combined into the safety analysis development [5,14]. Recently, the introduced approaches comprehended the significance of integrated safety and security analysis and intended to incorporate both into a joint methodological process. Two applicable techniques, which describe the integration of security into safety analysis, recommend a merging of fault tree analysis (FTA) with attack tree analysis (ATA) [14] or boolean driven Markov processes (BDMP) [15]. Other introduced approaches either combine safety and security methods, e.g., ATA and bowtie analysis [16], or integrate both fields. However, there are not any practical mechanisms to deal with safety and security integration in real-time applications. Moreover, BN- and GT-enabled approaches have received much attention worldwide, as a solution offering safety and security in several domains.

2.1. Bayesian Networks

The BN (referred to as belief networks) represents a hypothesis of rationalizing from uncertain evidence to uncertain conclusions, since it can perform the factorization of the collective distribution of variables, based on the conditional dependencies. BN is helpful in addressing uncertainty and incompleteness problems; thus, it is extensively applied in several domains. BN graphically depicts the logical associations between variables and recognizes the connections between these variables by conditional probabilities. By interpretation, a BN represents a directed acyclic graph (DAG), which encodes a conditional probability distribution. Nodes and arcs are vital components of BN, the nodes symbolize arbitrary variables and the arcs signify random relations between variables. There is a probability function for each state of the node, and conditional probabilities are used to exhibit the associations between variables.

BNs are probabilistic graphical models; these visual structures characterize the information about an uncertain system [17]. BNs are generally utilized for examining the hazards and vulnerabilities of networks, which are acyclic graphs that provide a quantitative and qualitative assessment of risks. Judea Pearl initially proposed the BN-based approach in 1985 and was usually utilized to distribute random information in AI. Owing to the unique functionality of BN for constructing the structures and algorithms, it is successfully used in e-commerce, transportation, data mining, energy control, etc. It is a DAG-based probability rationalization and appropriate for uncertainty representation of queries. BN must be a DAG and CPT (conditional probability table).

BN has been demonstrated to be a powerful tool for solving several problems with uncertain knowledge illustration and reasoning [18–20]. The BN formula is represented in Equation (1):

$$P(X_j|Y) = \frac{P\left(\frac{Y}{X_j}\right)P(X_j)}{\sum_{j=1}^{m} P\left(\frac{Y}{X_j}\right)P(X_j)} \quad (1)$$

where P(. | .) stands for the conditional probability distribution. Suppose the sample space N of experiment L, "Y" is the random event of L. $X_1, X_2, \ldots, X_n$ is the incompatible set of possibilities in experiment L, and "X_j" represents the entire group event from (j = 1, 2, . . . , m).

Figure 1 represents the three-variable examples of BN structure. A BN comprehends two types of nodes, i.e., the parent and child nodes. The parent node (cause) is at the start of any directed edge; the child node (fruit) is at the end. The directed edge specifies that the two nodes are interrelated. In Figure 1, X, Y are the two-parent nodes of Z. Z is the child nodes of X and Y. Prior probability: P(X) characterizes the probability of event X; P(Y) is the probability of event Y; P(Z | X, Y) is the probability that the event Z occurs before the condition that occurs at X and Y. The posterior probability, P(X | Z), P(Y | Z), and so on, can be obtained through the known prior probability.

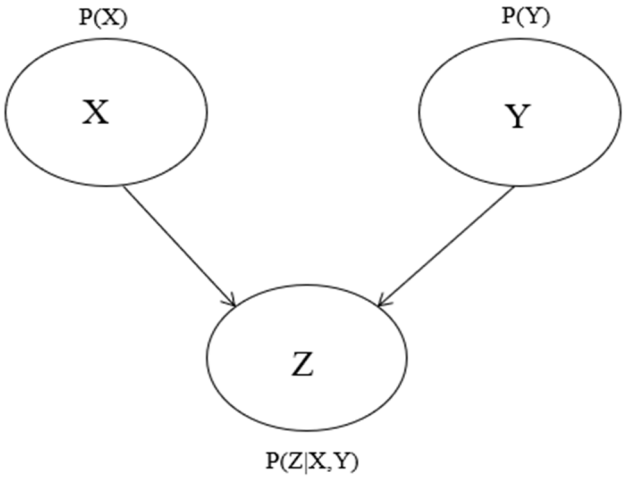

Figure 1. Three variable Bayesian network examples.

A node without a parent is known as a root node, and a node without children is termed as a leaf node. In BNs, nodes with links represent system variables demonstrating uncertain dependencies. Specifically, every node in the graph characterizes an arbitrary variable, whereas the ends between the nodes represent the dependencies of respective random variables [21]. Usually, statistical and computational techniques are used to calculate these provisional dependencies in the chart. Hereafter, BNs merges concepts from statistics, GT, and probability theory [22]; also, Bayesian probabilistic (BP) are used by considering probability as a mark of belief. The BP is less severe, concerning evidence, than the typically utilized probability methods. BN represents a combination of likelihood and GT; thus, it computes dependencies between several information or fact uncertainties [23]. FTA and ATA can be easily transferred to BN because it familiarizes the assemblies of various data, knowledge, functional associations, and approaches; also, it allows for conducting the extensively utilized interpretation for additional analysis [24–27]. In current studies of safety and security co-engineering methods, some factors are not considered, such as parameter optimization and balancing; thus, BN-based techniques can solve these essential issues.

2.2. Graph Theory

CIs are a highly interrelated and interdependent system, comprising several components, services, and nodes containing crucial information. There are numerous threats and

risks that may endanger critical data security and privacy in different CIs. After recognizing the CI risks, the next step for the CI safety and security evaluation is to offer an appropriate model for demonstrating the connection among potential risk sources. The GT model represents the study of mathematical structures applied to prototypical pairwise associations between entities, including nodes and points connected by edges or links. For GT analysis, graphs can be divided into various types, comprising of directed and undirected graphs and connected and disconnected charts, as well as weighted, bipartite, and simple graphs. GT analyzed the connectivity properties for susceptibility, trustworthiness, and risk analysis for several applications, i.e., vehicle networks using different graphs [28–30]. Moreover, topological properties enable techniques, flow-based approaches, and hybrid methods to analyze the reliability, hazards, and safety of systems [31].

There are several benefits of using the graphs model in different sectors. The first and foremost strength of GT is to describe the topological association between several nodes, connecting links between locations (Figure 2). It helps review the connectivity and the degree distribution of every location in a topological space. Those notions are essential for examining the networks. In the case of a spatial network, the vector and geometric characteristics are incredibly beneficial. Vectors properties provide a directional links; for transportation modeling, this property is applied to model flows between locations. The usage of geometrics properties is to insert distance into the model, allowing spatializing the system in Euclidian space. Moreover, GT also offers a description of relations through the graph. Based on the path, i.e., a course among components into the graph, and cycle (a path with a similar origin and endpoint), these characteristics allow for the study of the relationships between various parts of the charts [32–34].

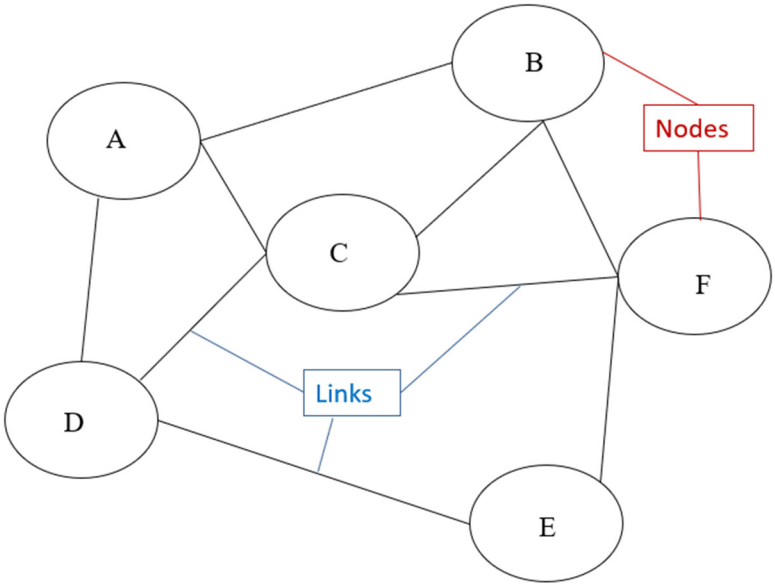

Figure 2. An illustration of graph theory.

In existing studies, GT has been applied in protecting systems [35]. An undirected graph H = (U, F) represents a mathematical structure, comprising two sets, U and F, where $U = \{u_1, u_2, \ldots, u_m\}$ defines the set of nodes. The set of edges is presented by $F = \{f_1, f_2, \ldots, f_n\}$. The undirected graph may be useful in presenting CIs or any other complex systems. Furthermore, each subsystem, such as oil and gas, power, and networks, can be exhibited by a subgraph. In GT, each component of the system represents a link, and the nodes are the connections between components, as per the topology of the network. Interdependencies among subsystems are modeled as definite links between end terminals of the two relevant components or subsystems. The CI graph model is supposed to have m nodes and n connections [36].

GT has become a critical component in various computing applications, such as CI security and network development. However, it is also among the most challenging areas to comprehend and apply for protecting networks, as well as infrastructures. Chung and Lu discussed GT and its real-time implementation in different threat and vulnerability analyses [37]. Ahmat et al. discussed the optimization problems associated with GT and its security applications, using GT concepts to characterize various networks, assess network protocols for multiple scenarios in networking and security, and tools used to generate graphs for demonstrating real-world systems [38]. Shirinivas et al. demonstrated GT's applicability in heterogeneous fields but primarily focused on technical applications that utilize theoretical graph notions [39].

3. Research Design

This section presents the fundamental stages for designing this SLR. This study follows the recommendations of the preferred reporting items for systematic reviews and meta-analyses (PRISMA) statement [40]. This design is used to select the security and safety literature, based on BN and GT, to compare and analyze the included studies.

3.1. Search Querry Process and Research Questions

In this SLR, ScienceDirect, IEEE Xplore, Web of Sciences, Scopus, and ACM databases were included. Later, a query was asked from identified databases for integrating safety and security, based on Bayesian networks or graph theory (also a combination of both). The search query for this SLR is given below:

("security" AND "safety") AND ("bayesian network" OR "graph theory")

The SLR is a series of associated arguments in support of the research questions (RQs). The RQs of this SLR is stated as follows:

1. Why is the integration of security and safety needed?
2. How have BN- and GT-based methodologies been utilized for security and safety studies in CI?
3. What have been the targeted application domains?
4. What solutions have been developed in the identified studies?
5. How is performance validated for developed techniques and algorithmic solutions?
6. What are the advantages and disadvantages of existing studies?

3.2. Exclusion and Inclusion Criteria

This study applies the web application Rayyan QCRI to eliminate duplicate records from different databases and estimate the eligibility of recognized records [41]. Moreover, in this SLR, we used the following exclusion criteria (EC):

(a) Studies that are not focused on the integration of safety and security, based on Bayesian networks or graph theory (also a combination of both).
(b) Studies that merely provide background about the integration of both measures.
(c) Studies that do not develop or design a novel method/approach/model/tool.

In this SLR, we followed specific inclusion criteria for considering studies to be included for analysis. The inclusion steps for this SLR are stated as below:

(a) Published in a conference or journal classified in the identified databases.
(b) The records are identified from January 2011 to September 2020.
(c) Developed a tool or technique for integrating safety and security measures using Bayesian Networks or Graph Theory (also a combination of both approaches).

4. Results

This section discusses BN and GT approaches for security and safety to recognize the significant patterns and findings in applying different applications. Moreover, this study analyzes the identified studies, based on organization and classification, citation index,

applied data source, number of used nodes, application, application sector, threat actor, functionality, implementation scenarios, and validation methodologies.

4.1. Organization and Classification of Included Studies

In this study, at the initial stage, 2295 records were identified during the search process, including ScienceDirect (n = 1610), Scopus (n = 213), ACM (n = 205), IEEE Xplore (n = 193), and Web of Science (n = 74). Later, 2093 unique records were recognized, after deleting the duplicate records by applying the screening tool. The title and abstract review recommend that 1853 records be excluded by following the exclusion and inclusion criteria, as elaborated on in Section 3.2. From examining the full-text articles of 240 records, based on the eligibility check process stated in Section 3, 176 were excluded. Merely, 64 papers have discussed the security and safety integration for different CI applications based on BN and GT and can be considered to perform comparative analysis in this SLR [42–105]. Figure 3 presents a flowchart of the multiple record processing stages in this SLR.

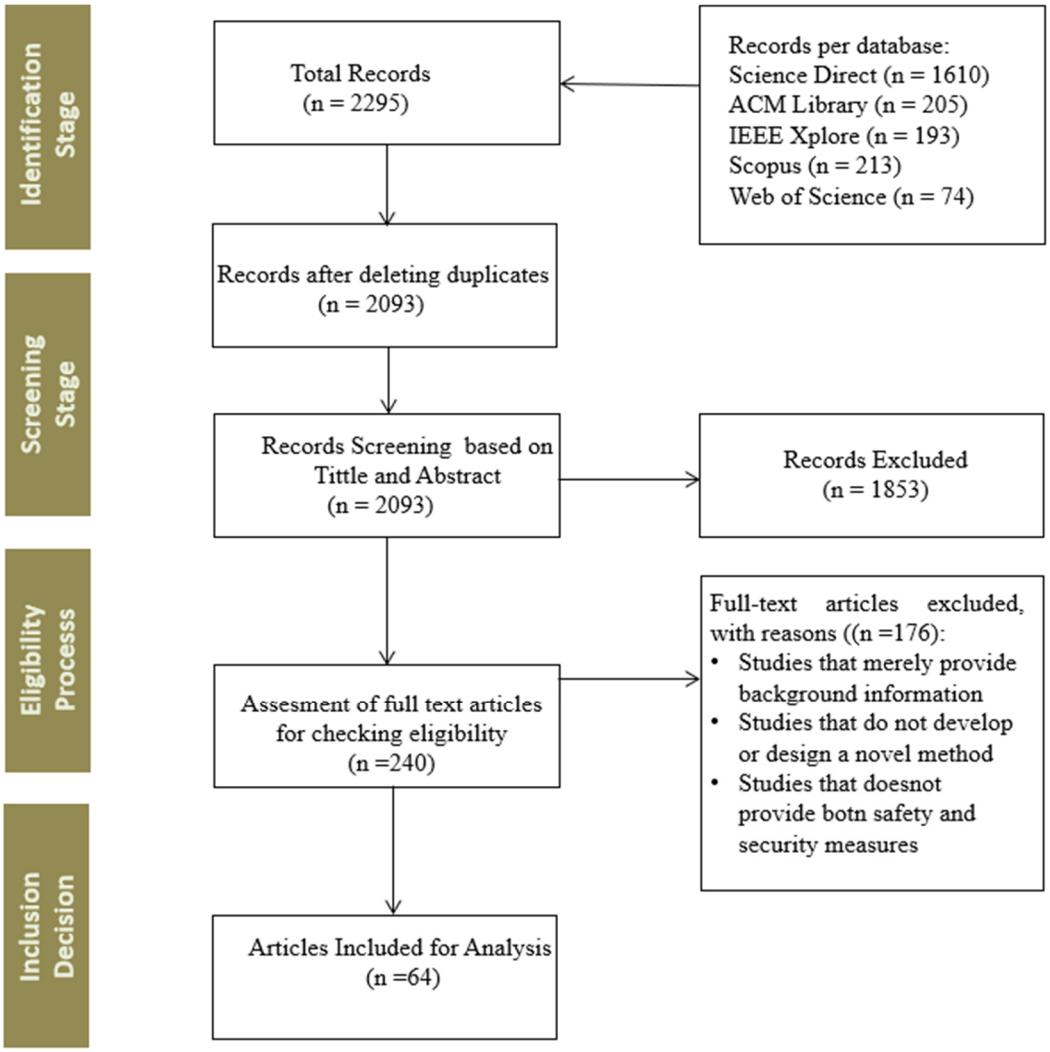

Figure 3. A flowchart of records processing stages.

The details of the included papers, including study year, number of used references, and category are shown in Table 1. Figure 4 demonstrates that the journal and conference proceedings are 61% and 39% of total articles, respectively.

Table 1. Details of included articles.

S.No.	Study	Year	References	Category
1	Xiaorong et al. [42]	2020	32	Journal
2	Lipeng et al. [43]	2020	63	Journal
3	Meizhi et al. [44]	2020	44	Journal
4	Raditya et al. [45]	2020	40	Journal
5	Tai-hua et al. [46]	2020	4	Conference
6	Mingjing et al. [47]	2020	42	Journal
7	Xiaoxue et al. [48]	2020	38	Journal
8	Xin et al. [49]	2020	10	Conference
9	Meizhi et al. [50]	2020	40	Journal
10	Niamat et al. [51]	2019	78	Journal
11	Chengpeng et al. [52]	2019	46	Journal
12	Yi et al. [53]	2019	7	Conference
13	Barry et al. [54]	2019	48	Journal
14	Alexandre et al. [55]	2019	98	Journal
15	Sabarathinam et al. [56]	2019	17	Conference
16	Seyedmohsen et al. [57]	2019	33	Journal
17	Mario et al. [58]	2019	20	Conference
18	Chao et al. [59]	2019	61	Journal
19	Nima et al. [60]	2019	27	Journal
20	Hui et al. [61]	2019	39	Journal
21	Xiqiang et al. [62]	2019	6	Journal
22	Jamal et al. [63]	2019	30	Conference
23	Elvin et al. [64]	2018	27	Conference
24	Xiaoyan et al. [65]	2018	31	Journal
25	Ying et al. [66]	2018	71	Journal
26	Subhojeet et al. [67]	2017	30	Conference
27	Huai et al. [68]	2017	64	Journal
28	Gabriele et al. [69]	2017	41	Journal
29	Zhiqiang et al. [70]	2017	22	Journal
30	Jinsoo et al. [71]	2017	23	Journal
31	Donya et al. [72]	2017	42	Journal
32	Xianyou et al. [73]	2016	15	Journal
33	Galizia et al. [74]	2016	13	Conference
34	Francesca et al. [75]	2016	21	Journal
35	Zhao et al. [76]	2016	8	Conference
36	Mark et al. [77]	2016	14	Journal
37	Remya et al. [78]	2016	14	Conference
38	Xin Chen [79]	2016	25	Journal
39	Mark et al. [80]	2015	9	Conference
40	Martin et al. [81]	2015	15	Conference
41	Jinsoo et al. [82]	2015	29	Journal
42	Marco et al. [83]	2015	28	Journal
43	Matti et al. [84]	2015	21	Conference
44	Xiqiang et al. [85]	2015	6	Conference
45	Yongjia et al. [86]	2015	16	Conference
46	Kairan et al. [87]	2015	9	Conference
47	Amal et al. [88]	2014	19	Journal
48	Guannan et al. [89]	2014	36	Journal
49	Jiali et al. [90]	2014	17	Journal
50	Sher et al. [91]	2014	39	Journal
51	LONG et al. [92]	2014	20	Conference
52	Zeng Xianfeng [93]	2014	4	Conference
53	TIAN et al. [94]	2013	5	Conference
54	William et al. [95]	2013	34	Conference
55	Jinsoo et al. [96]	2013	23	Journal
56	Stefan et al. [97]	2013	15	Journal
57	Jingjing et al. [98]	2013	15	Conference

Table 1. *Cont.*

S.No.	Study	Year	References	Category
58	John et al. [99]	2013	15	Conference
59	Heung et al. [100]	2013	21	Journal
60	Chaze et al. [101]	2012	16	Conference
61	Mo Ming [102]	2012	4	Journal
62	Shuliang et al. [103]	2012	68	Journal
63	Song et al. [104]	2011	23	Conference
64	André et al. [105]	2011	16	Journal

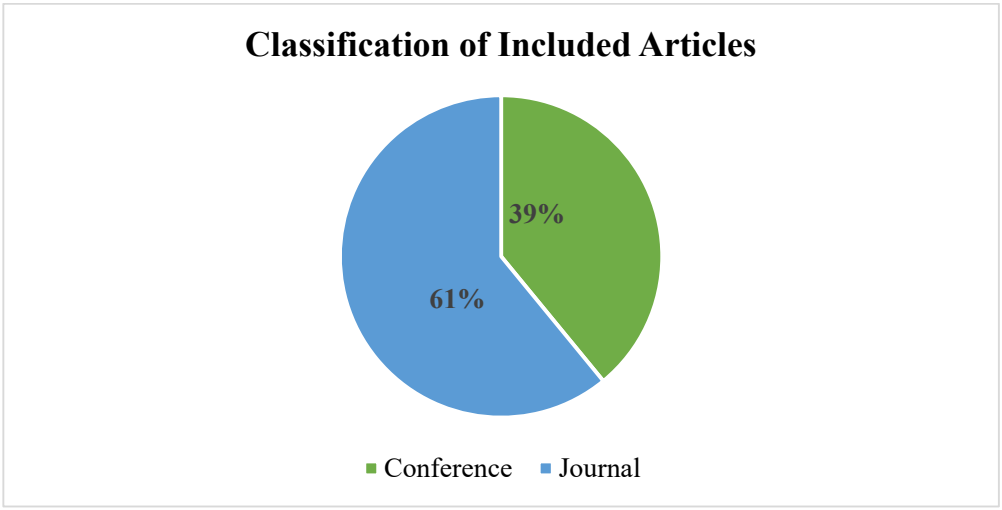

Figure 4. Analysis of identified articles in this SLR.

4.2. Included Studies Based on GT and BN for Safty and Security

In recent times, security and safety problems are rapidly converging on different applications, leading to conditions where these closely associated measures that need to be integrated, instead of applied discretely or categorized. Several scholars have developed innovative methodologies to solve risk analysis and evaluation from safety, security, and united security risk management. Table 2 includes existing techniques, based on BN and GT, to resolve safety and security concerns and their respective application sectors.

Table 2. Description of included studies.

Study	Application Sector	Technique	Description
Xiaorong et al. [42]	Cyber–Physical Systems (CPS)	BN	The advanced, BN-based method is proposed to offer a combined solution to the cyber-to-physical (C2P) risk evaluation for CPS. Additionally, for verifying the developed model, two scenarios are constructed.
Lipeng et al. [43]	Public Sector	BN	A systematic causation model for evaluating the main reasons for the failure of security in the 2022 Olympics.
Meizhi et al. [44]	Maritime Industry	BN	A BN-based model is proposed for the dynamic emergency risk estimation.
Raditya et al. [45]	Industrial Control Systems (ICS)	BN and GT	A decision-making methodology for analyzing risk is proposed to examine and estimate in ICS.

Table 2. *Cont.*

Study	Application Sector	Technique	Description
Tai-hua et al. [46]	Public Sector	BN	To develop public safety and safety evaluation approach using fuzzy logic and BN methods.
Mingjing et al. [47]	Vehicle Transportation	BN	Development of BN enabled model to analyze the risk aspects of urban transportation.
Xiaoxue et al. [48]	Maritime Industry	BN	A framework is developed for maritime to offer a balance between resilience and vulnerability.
Xin et al. [49]	Education	BN	An ideological security evaluation approach is developed to examine the risk factors for college students.
Meizhi et al. [50]	Maritime Industry	BN	To develop and validate the developed model for pirate attack mitigation by recognizing the most significant risk factors.
Niamat et al. [51]	Smart grid	BN	This research quantifies the resilience of electrical systems to address risks, based on BN model power.
Chengpeng et al. [52]	Maritime Industry	BN	To evaluate the risk assessment using fuzzy rule and BN model in maritime supply chains.
Yi et al. [53]	Maritime Industry	BN	To evaluate the possibility of several risks associated with shipping in navigation environments.
Barry et al. [54]	Vehicle Transportation	BN	A proactive cyber-risk classification model is proposed, based on BN in transportation.
Alexandre et al. [55]	Air Transportation	BN	This research presented a framework using BN for the command-and-control support systems of air transportation.
Sabarathinam et al. [56]	CPS	BN	A framework is developed for the decision-maker to determine the root cause of problems in CPSs.
Seyedmohsen et al. [57]	Vehicle Transportation	BN	Development of model, which includes both qualitative and quantifiable measures for vehicular electrical systems.
Mario et al. [58]	Vehicle Transportation	BN	A system is proposed for the recognition of threats in automotive-enabled applications.
Chao et al. [59]	Chemical Industry	GT	Integrating security and safety resources to protect the chemical industry.
Nima et al. [60]	Process Plants	BN and GT	A low-capacity approach is proposed for process plants, as a temporary mode of eliminating vulnerabilities.
Hui et al. [61]	Railways	BN	A risk analysis method is proposed for managing operative risks in the railway.
Xiqiang et al. [62]	Railways	BN	A model is developed to predict and diagnose risks for urban railway.

Table 2. *Cont.*

Study	Application Sector	Technique	Description
Jamal et al. [63]	Systems of Systems (SoS)	BN	Development of an approach to determine cyber-attacks propagation in SoS.
Elvin et al. [64]	Vehicle Transportation	BN	To develop a framework for trust model using ML and DL for vehicle transportation.
Xiaoyan et al. [65]	Oil and Gas Sector	BN	This research identifies risk in the oil and gas sector by proposing a graphic model and BN approach.
Ying et al. [66]	Railways	BN	A risk identification method based on BN for metro construction is developed.
Subhojeet et al. [67]	Vehicle Transportation	GT	A graph enabled based risks recognition approach in vehicle-vehicle communication.
Huai et al. [68]	Gas Pipelines	GT	Development of a method to examine the reliability in gas pipeline systems.
Gabriele et al. [69]	Chemical Industry	BN	A probabilistic risk assessment method is developed based on BN to monitor threats in the chemical industry.
Zhiqiang et al. [70]	Oil wharf Handling	BN	To develop a risk analysis model based on a static incident approach.
Jinsoo et al. [71]	Nuclear	BN	A methodology is proposed for diagnostic outcomes from BN model for risk assessment.
Donya et al. [72]	Gas and Pipelines	BN	A novel methodology is proposed for vulnerability calculation of gas pipelines.
Xianyou et al. [73]	Networks Security	BN	Development of vulnerability analysis method that may eliminate the cyber-attacks.
Galizia et al. [74]	Socio-Technical Systems	BN	This study aims to examine what factors could influence sociotechnical systems.
Francesca et al. [75]	Chemical Industry	BN	The developed approach addresses the vulnerability evaluation using BN model.
Zhao et al. [76]	Navigation Environment	BN	Establishment of an index system by integrating BN with fuzzy theory to offer safety evaluation.
Mark et al. [77]	Chemical Industry	BN	Development of vulnerability analysis approach methodology for monitoring intentional attacks.
Remya et al. [78]	Unmanned Aerial Vehicles (UAV)	BN	A technique to solve issues related to software risks and failures are developed by using BayesiaLab.
Xin Chen [79]	Complex Systems	GT	A polynomial-time system is proposed to recognize critical nodes for ensuring security in complex systems, such as the power and energy sectors.

Table 2. *Cont.*

Study	Application Sector	Technique	Description
Mark et al. [80]	Petroleum Plants	BN	Development of extended risk analysis methods at various stages of plants to ensure unauthorized access.
Martin et al. [81]	Maritime Industry	GT	This study develops an approach for validating the vulnerability in the maritime sector.
Jinsoo et al. [82]	Nuclear	BN	To develop a model for evaluating security for the nuclear domain in a unified way.
Marco et al. [83]	Railways	BN	Development of methodology for transferring attacks trees into BNs.
Matti et al. [84]	Mobile Networks	BN	Establishment of probabilistic risk evaluation approach for risk assessment and sensitivity analysis.
Xiqiang et al. [85]	Railways	BN	To develop BN enabled model for train control center that can be quantifiable for safety analysis in railway.
Yongjia et al. [86]	Cognitive Radio Networks (CRNs)	BN	Establishing an innovative system to diagnose and protect from malicious attacks.
Kairan et al. [87]	Vehicle Transportation	BN	Development of transportation security evaluation method to estimate a real-world mountainous expressway.
Amal et al. [88]	Maritime Industry	BN	A novel solution related to offshore piracy is proposed to characterize threats and probable targets.
Guannan et al. [89]	Software	BN	An estimation model is proposed for internet-based software applications.
Jiali et al. [90]	Maritime Industry	BN	To develop a fuzzy enabled BN system in shipping to evaluate the security of passengers.
Sher et al. [91]	Railways	GT	Incorporation of mobile agent notions with Petri nets offers one-dimensional control, which raises the safety of the train system.
LONG et al. [92]	Smart Grid	BN	An integrated method of FTA and BN is developed for analyzing risks in power systems.
Zeng Xianfeng [93]	Railways	BN	To develop a security evaluation method using BN model to improve train equipment and repair and maintenance work reliability.
TIAN et al. [94]	Water Traffic System	BN	This research develops a system that can monitor the safety issues associated with water traffic to realize the initial warning efficiently.
William et al. [95]	Networks Security	BN	An incorporated framework is developed to monitor for computing a mean time to compromise the system by the known-unknown vulnerability.

Table 2. *Cont.*

Study	Application Sector	Technique	Description
Jinsoo et al. [96]	Nuclear	BN	To establish a risk investigation approach for instrumentation and control (I and C) for identifying mitigating vulnerabilities.
Stefan et al. [97]	Vehicle Transportation	GT	Three graph-based protocols were developed, by means of wide-ranging simulations, to detect insider threats.
Jingjing et al. [98]	Railways	BN	To propose an approach to meet the necessities of accuracy in high safety for the train control system for a fault diagnosis system.
John et al. [99]	Air Transportation	GT	Development of method using game theory and GT concepts and graph theory for security risk mitigation.
Heung et al. [100]	Nuclear	BN	This study analytically modeled management approach, which offers the progress of safety-critical software.
Chaze et al. [101]	Maritime Industry	BN	This study presents the architecture based on incorporated BNs for its feedback planning.
Mo Ming [102]	Network Security	GT	An integrated GT approach is developed to have a safety evaluation in the network security domain.
Shuliang et al. [103]	Smart Grid	GT	A framework is proposed to investigate the susceptibilities in interdependent systems.
Song et al. [104]	Asian Games	BN	The proposed BN model accomplishes fire risk evaluation along with conducting fast disaster condition valuation.
André et al. [105]	Medical	BN and GT	This study presents an application for risk mitigation in ventricular-enabled devices.

4.3. Citation Index of Included Studies

In this SLR, the citation index is adapted to evaluate the research quality of each included technique, i.e., BN or GT or unified BN and GT. The citation index represents the number of citations of the included studies as per Google Scholar, accessed on 20th November 2020, as revealed in Table 3. The most extensive cited studies were 139 citations for Shuliang et al. [103], 76 citations are Jinsoo et al. [82], and 60 citations for Huai et al. [68], which are published in 2012, 2015, and 2017, respectively. Whereas the following studies have not received any citations: Tai-hua et al. [46], Xiaoxue et al. [48], and Xin et al. [49] (published in 2020), Sabarathinam et al. [56], Xiqiang et al. [62], and Jamal et al. [63] (published in 2019), Zhao et al. [76] (published in 2016), Jiali et al. [90], and Zeng Xianfeng [93] (published in 2014), and Mo Ming [102] (published in 2012).

Table 3. Citation index and data sources of included studies.

Study	Citations	Data Source	Nodes	Applicability
Xiaorong et al. [42]	2	EK, ED	9	Risk Management
Lipeng et al. [43]	2	EK, ED	31	Holistic Event Investigation
Meizhi et al. [44]	2	EK, ED	15	Risk Management
Raditya et al. [45]	1	ED	8	Risk Management
Tai-hua et al. [46]	0	EK		Risk Management

Table 3. *Cont.*

Study	Citations	Data Source	Nodes	Applicability
Mingjing et al. [47]	1	EK, ED	11	Risk Management
Xiaoxue et al. [48]	0	EK	16	Vulnerability Assessment
Xin et al. [49]	0	ED		Risk Management
Meizhi et al. [50]	1	EK, ED	14	Risk Management
Niamat et al. [51]	30	EK, ED	5	Resilience Quantification
Chengpeng et al. [52]	32	EK, ED	11	Risk Management
Yi et al. [53]	1	EK, ED	24	Risk Management
Barry et al. [54]	48	EK, ED	51	Risk Management
Alexandre et al. [55]	4	ED	13	Cyber Impact Assessment
Sabarathinam et al. [56]	0	EK, ED	8	Root Cause Analysis
Seyedmohsen et al. [57]	37	EK, ED	6	Risk Management
Mario et al. [58]	7	ED	5	Intrusion Detection
Chao et al. [59]	30	ED	4	Risk Management
Nima et al. [60]	8	ED	6	Vulnerability Assessment
Hui et al. [61]	4	ED	24	Risk Management
Xiqiang et al. [62]	0	EK, ED	19	Risk Management
Jamal et al. [63]	0	EK	8	Risk Management
Elvin et al. [64]	10	ED		Trust Computation
Xiaoyan et al. [65]	25	ED	40	Risk Management
Ying et al. [66]	16	EK, ED	31	Risk Management
Subhojeet et al. [67]	7	ED	6	Anomaly Detection
Huai et al. [68]	60	EK, ED	53	Reliability Assessment
Gabriele et al. [69]	16	EK	8	Risk Management
Zhiqiang et al. [70]	4	ED	47	Risk Management
Jinsoo et al. [71]	27	ED	13	Risk Management
Donya et al. [72]	17	EK	30	Vulnerability Assessment
Xianyou et al. [73]	3	ED	20	Vulnerability Assessment
Galizia et al. [74]	4	EK	12	Risk Management
Francesca et al. [75]	12	EK, ED	8	Vulnerability Assessment
Zhao et al. [76]	0	EK	24	Risk Management
Mark et al. [77]	9	EK, ED	8	Vulnerability Assessment
Remya et al. [78]	2	EK, ED	6	Safety Assessment
Xin Chen [79]	6	EK	60	Vulnerability Assessment
Mark et al. [80]	4	EK, ED	17	Risk Management
Martin et al. [81]	1	ED	3	Vulnerability Assessment
Jinsoo et al. [82]	76	ED	64	Vulnerability Assessment
Marco et al. [83]	22	EK	10	Risk Management
Matti et al. [84]	1	EK	5	Risk Management
Xiqiang et al. [85]	3	EK	47	Risk Management
Yongjia et al. [86]	7	ED	4	Attacks Analysis
Kairan et al. [87]	4	EK	36	Risk Management
Amal et al. [88]	60	EK	20	Risk Management
Guannan et al. [89]	1	ED	20	Risk Management
Jiali et al. [90]	0	EK, ED	58	Risk Management
Sher et al. [91]	17	ED	14	Software Verification
LONG et al. [92]	2	EK	4	Risk Management
Zeng Xianfeng [93]	0	ED	22	Safety Assessment

Table 3. *Cont.*

Study	Citations	Data Source	Nodes	Applicability
TIAN et al. [94]	1	ED	12	Water Traffic Management
William et al. [95]	33	ED	20	Risk Management
Jinsoo et al. [96]	17	ED	16	Risk Management
Stefan et al. [97]	49	ED	8	Attack Analysis
Jingjing et al. [98]	10	EK, ED	7	Fault Analysis
John et al. [99]	3	EK	16	Risk Management
Heung et al. [100]	32	EK, ED	8	Fault Analysis
Chaze et al. [101]	11	EK	4	Risk Management
Mo Ming [102]	0	ED	6	Attack Analysis
Shuliang et al. [103]	139	ED	182	Vulnerability Assessment
Song et al. [104]	1	EK, ED	45	Risk Management
André et al. [105]	15	ED	4	Risk Management

However, the record number of included articles per year is reported in Figure 5, which demonstrates the research trend of applying GT and BN to implement safety and security, based on the included studies. The analysis suggests that scholars have been publishing more articles, addressing united safety and security aspects, in the last two years. From 2019 and 2020, 13 (9 BN, 1 GT, 1GT, and BN), and 9 (8 BN, 1 BN, and GT) papers are included in this SLR, respectively.

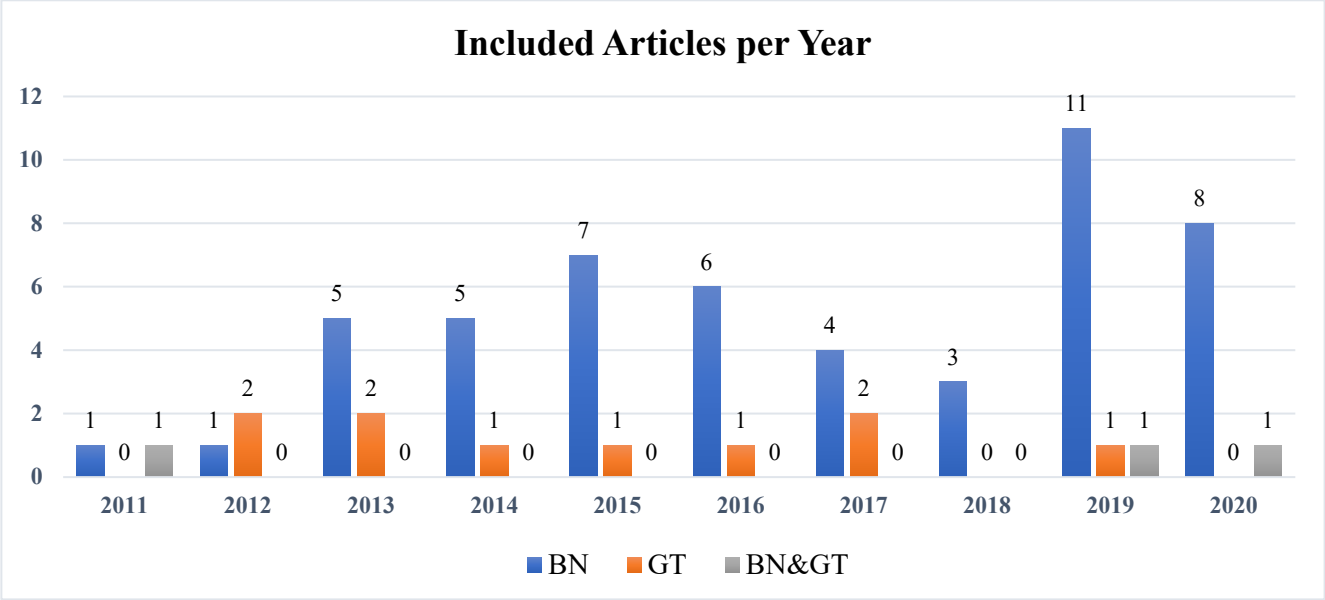

Figure 5. Research trend of included studies.

4.4. Data Sources and Number of Nodes Used to Construct BN/GT

The BN and GT play a significant role in predicting and unintentionally diagnosing failures and targeted risks by using numerous tools and models, based on the information collected from the system expert's knowledge (EK) and/or from empirical data (ED). EK represents the opinions collected by interviewing the system or domain expert, and ED is the historical or experimental data gathered by real-time scenarios or the literature [50–54]. It is revealed in existing studies that a reliable strategy can be attained for the developed model by applying collective EK and ED. Figure 6 demonstrates that 26 out of 64 of the included studies used only ED to developed BN or GT approaches. Whereas 16 out of 64 applied EK and 26 out of 64 of included studies that utilized both ED and EK to develop

GT- or BN-enabled models. It is observed that 3 out of 64 of the included studies were based on integrating GT and BN for addressing united security and safety measures, and these studies employed ED analysis for the system development. Though 10 out of 64 included studies were based on GT, in which 7 uses ED, 2 applies EK, and 1 utilizes both. Besides, BN models are applied in 51 out of 64 studies, which categorize as EK (14), ED (16), and collective EK and ED (21).

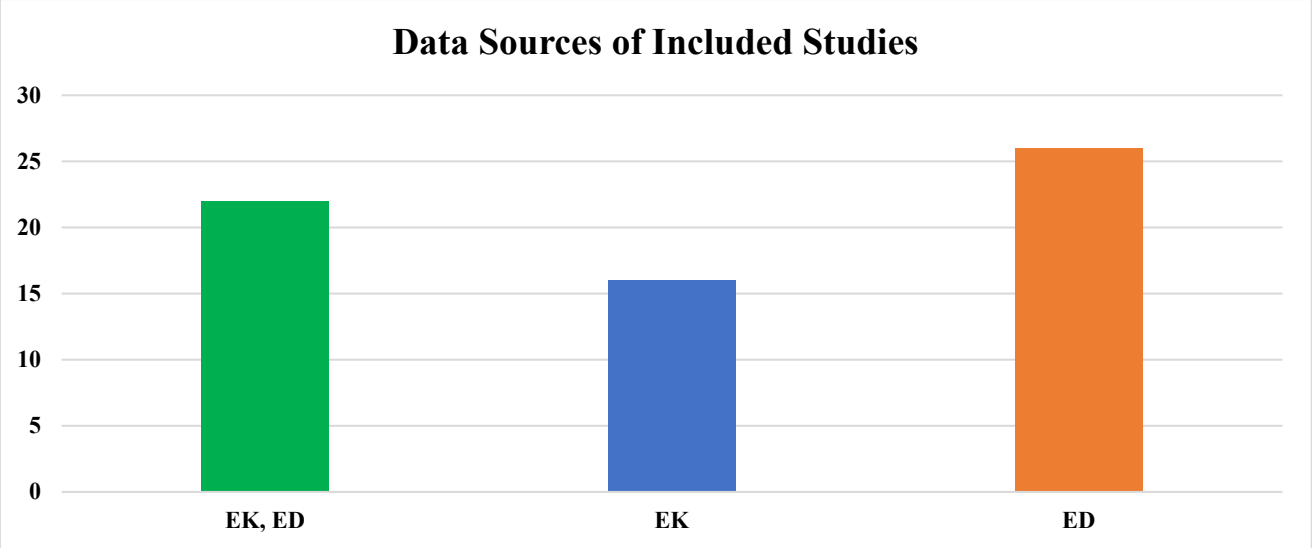

Figure 6. The used data sources for developing BN and GT models.

Several nodes are linked together to represent BN or GT enabled systems for assessing risks and vulnerabilities in different applications. Moreover, the quantity of nodes can be utilized to represent the model complexity of the system. A large number of nodes may reflect the incapacitated association between input and output nodes by introducing in-between layers between source and destination. Chockalingam et al. [106] stated that it is suggested to have a total number of nodes in BN models less than 40. In this SLR, it is observed that 43 out of 51 BN-based model have used less than 40 nodes. However, the remaining eight have used equal or more than 40, including Xiaoyan et al. [65], Song et al. [104], Zhiqiang et al. [70], Xiqiang et al. [85], Barry et al. [54], Jiali et al. [90], Remya et al. [78], and Jinsoo et al. [82], 40, 45, 47, 47, 51, 58, 60, and 64, respectively. However, all models that utilized GT and BN simultaneously have used less than 40 nodes in the developed system. Moreover, it is also noticed that 2 out of 10 GT-based approaches have utilized more than 40 nodes comprising Huai et al. [68] and Shuliang et al. [103], 53 and 182, respectively. Whereas, remaining 8 included studies of GT employ less than 40 nodes.

4.5. Applicability, Threat Actor, and Implementation Criteria

The characteristic applicability is used to comprehend the type of evaluation that is acquired from the developed methodologies. In this SLR, it is observed that 37 out of 64 studies ensure risk management in the proposed system for identifying, analyzing, evaluating, and treating loss exposures, as well as monitoring risk control and financial resources, to mitigate the adverse effects of loss. There are three main stages: identifying, assessing, and evaluating risk. The procedure for assessing risk is the main element in the risk management process. Generally, there are two sorts of risk assessment approaches, including quantitative and qualitative strategies. The qualitative assessment techniques primarily rely on proficient knowledge and attention for revealing the risks. In contrast, the quantitative assessment methods can compute the risk value of the system and emphasize the system's quantitative performance under the risks.

In general, the quantitative methods are chosen to conduct risk analysis and assessment, owing to the accurate explanations of system risks that can optimize the distribution

of protected resources. Whereas 10 out of 64 perform the task of vulnerability assessment for evaluating whether the network is vulnerable to any identified vulnerabilities, allocates severity levels to those susceptibilities, and recommends remediation or mitigation, if and whenever required. Moreover, 3 out of 64, 2 out of 64, and 2 out of 64 perform attack analysis, fault analysis, and safety assessment, respectively. Besides, 10 out 64 studies perform distinct functionalities, comprising of Lipeng et al. [43], Niamat et al. [51], Alexandre et al. [55], Sabarathinam et al. [56], Mario C et al. [58], Elvin et al. [64], Subhojeet et al. [67], Huai et al. [68], Sher et al. [91], and TIAN et al. [94], holistic event investigation, resilience quantification, cyber impact assessment, root cause analysis, intrusion detection, trust computation, anomaly detection, reliability assessment, software verification, and water traffic management, respectively.

In this SLR, the threat actor is used to identifying that the included studies help prevent the attack. It is observed that the threat actor is classified into two types, such as external and internal. It is observed from Figure 7 that 7 out of 64 and 2 out of 64 studies have mentioned that the developed methodology is applicable against external and internal threats, respectively. Moreover, 2 out 64 developed approaches help prevent both internal and external threats. However, the remaining 53 included articles have not specified any particular kind of threat but rather concentrated on warnings and alarms, which may be suitable for various possible threats.

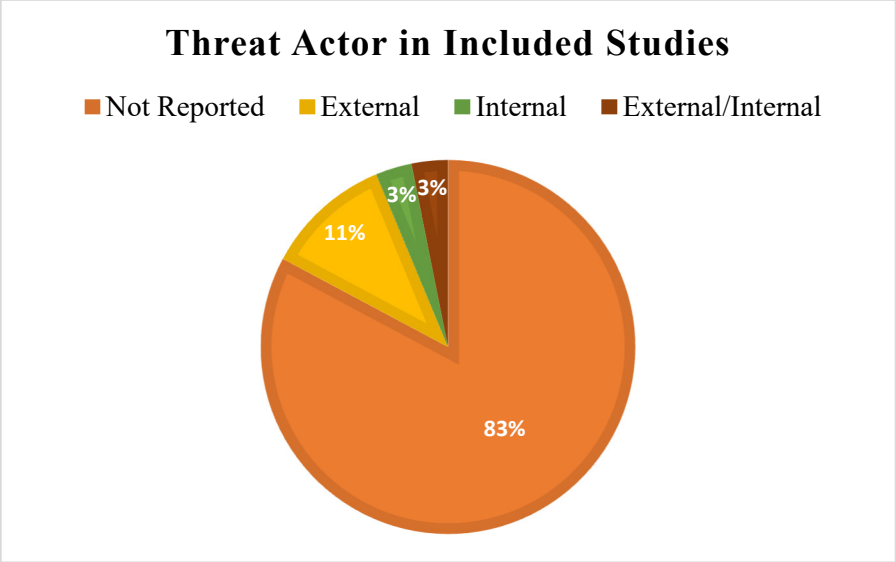

Figure 7. Threat Actor in Included Studies.

Implementing GT- or BN-based models is vital to measure network performance, transform strategic plans to monitor failures and risks in the system, and apply the necessary actions to achieve integrated safety and security for different applications. During the review process, it is observed that GT- or BN-based development scenarios are an association of nodes, modules, and the implementation subsystems. This SLR suggests that 42%, 31%, and 27% of the included studies performed simulated, real-time, and preliminary analysis, respectively, as shown in Table 4.

Table 4. Threat Actor and Implementation Criteria of Included Studies.

Study	Implementation Criteria	Threat Actor
Xiaorong et al. [42]	Simulation	Not Specified
Lipeng et al. [43]	Simulation	Outsider
Meizhi et al. [44]	Simulation	Not Specified
Raditya et al. [45]	Real-time	Insider
Tai-hua et al. [46]	Real-time	Outsider

Table 4. *Cont.*

Study	Implementation Criteria	Threat Actor
Mingjing et al. [47]	Simulation	Not Specified
Xiaoxue et al. [48]	Real-time	Not Specified
Xin et al. [49]	Real-time	Not Specified
Meizhi et al. [50]	Preliminary	Not Specified
Niamat et al. [51]	Preliminary	Outsider, Insider
Chengpeng et al. [52]	Real-time	Not Specified
Yi et al. [53]	Simulation	Not Specified
Barry et al. [54]	Preliminary	Not Specified
Alexandre et al. [55]	Simulation	Outsider
Sabarathinam et al. [56]	Simulation	Not Specified
Seyedmohsen et al. [57]	Simulation	Not Specified
Mario et al. [58]	Simulation	Not Specified
Chao et al. [59]	Preliminary	Not Specified
Nima et al. [60]	Real-time	Outsider
Hui et al. [61]	Real-time	Outsider
Xiqiang et al. [62]	Real-time	Not Specified
Jamal et al. [63]	Simulation	Not Specified
Elvin et al. [64]	Preliminary	Not Specified
Xiaoyan et al. [65]	Real-time	Not Specified
Ying et al. [66]	Real-time	Outsider
Subhojeet et al. [67]	Simulation	Not Specified
Huai et al. [68]	Simulation	Not Specified
Gabriele et al. [69]	Preliminary	Not Specified
Zhiqiang et al. [70]	Simulation	Not Specified
Jinsoo et al. [71]	Real-time	Insider
Donya et al. [72]	Preliminary	Not Specified
Xianyou et al. [73]	Preliminary	Not Specified
Galizia et al. [74]	Simulation	Not Specified
Francesca et al. [75]	Simulation	Outsider
Zhao et al. [76]	Real-time	Not Specified
Mark et al. [77]	Real-time	Outsider, Insider
Remya et al. [78]	Simulation	Not Specified
Xin Chen [79]	Simulation	Not Specified
Mark et al. [80]	Preliminary	Not Specified
Martin et al. [81]	Preliminary	Not Specified
Jinsoo et al. [82]	Real-time	Not Specified
Marco et al. [83]	Simulation	Not Specified
Matti et al. [84]	Simulation	Not Specified
Xiqiang et al. [85]	Real-time	Not Specified
Yongjia et al. [86]	Preliminary	Not Specified
Kairan et al. [87]	Preliminary	Not Specified
Amal et al. [88]	Preliminary	Not Specified
Guannan et al. [89]	Simulation	Not Specified
Jiali et al. [90]	Real-time	Not Specified
Sher et al. [91]	Real-time	Not Specified
LONG et al. [92]	Simulation	Not Specified
Zeng Xianfeng [93]	Simulation	Not Specified
TIAN et al. [94]	Real-time	Not Specified
William et al. [95]	Simulation	Not Specified
Jinsoo et al. [96]	Simulation	Not Specified
Stefan et al. [97]	Simulation	Insider
Jingjing et al. [98]	Simulation	Not Specified
John et al. [99]	Preliminary	Not Specified
Heung et al. [100]	Preliminary	Not Specified
Chaze et al. [101]	Simulation	Not Specified
Mo Ming [102]	Real-time	Not Specified
Shuliang et al. [103]	Simulation	Not Specified
Song et al. [104]	Simulation	Not Specified
André et al. [105]	Real-time	Not Specified

5. Discussion

This section includes answers based on comparative analysis of included articles to find solutions for given RQs in Section 2.

5.1. Why Is the Integration of Security and Safety Needed?

In recent times, computer networks have been widely applied in several applications; any failure in these systems could have critical outcomes. There are various hypotheses about the characteristics such crucial systems must maintain, and the methods employed to protect them. Two such attributes are security and safety. Nevertheless, modern designs are usually needed to meet these two attributes simultaneously. Considering safety and security, common goals are needed to protect peoples or systems; therefore, safety-critical assets are considered.

Martin et al. [81] stated that the marine industry is a critical sector, and it is essential to combine safety and security concerns on the sea. The integration of two aspects concentrates on analyzing the energy supply vulnerabilities and introduces a methodology to evaluate the system's exposure using the spatial composition of maritime regions. This study contributes a GT-based model for offering safety and security in a maritime territory. Indeed, the developed model utilizes links, such as roads and ports, as nodes. Matti et al. [84] demonstrate the significance of public safety and security (PSS) in mobile networks. In this study, a risk evaluation model, using BN, is proposed for the current PSS telecommunication services.

5.2. How Have Bayesian Network- and Graph Theory-Based Methodologies Been Utilized for Security and Safety Studies in CI?

This RQ assists in knowing which models are used for safety and security integration, functionalities, and applicability. In this SLR, it is observed that 80%, 15%, and 5% of the included studies use BN and GT, as well as both GT and BN, respectively, as shown in Figure 8.

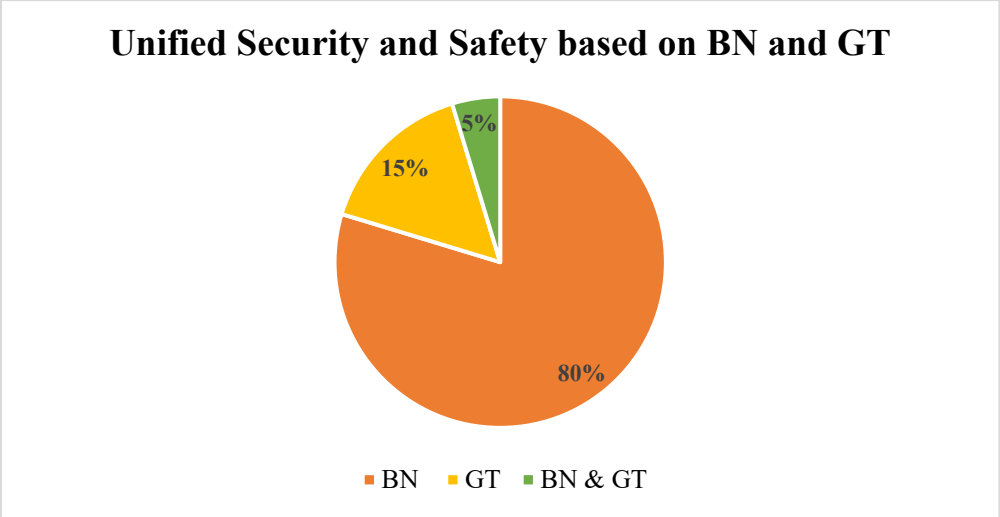

Figure 8. Characterization of BN and GT models in included studies.

From Figure 9, it is observed that the developed models based on BN or GT in included studies were utilized to have two sorts of purposes, including diagnosis and prediction. The term diagnosis represents identifying the nature or cause of the incidents or other risks in the systems. In contrast, the prediction is associated with forecasting potential cyber threats in the respective CIs. This study identifies that 48% of approaches perform a diagnosis of the risks in different applications. However, 36% and 16% of papers ensure performance prediction and both prediction and diagnosis, respectively.

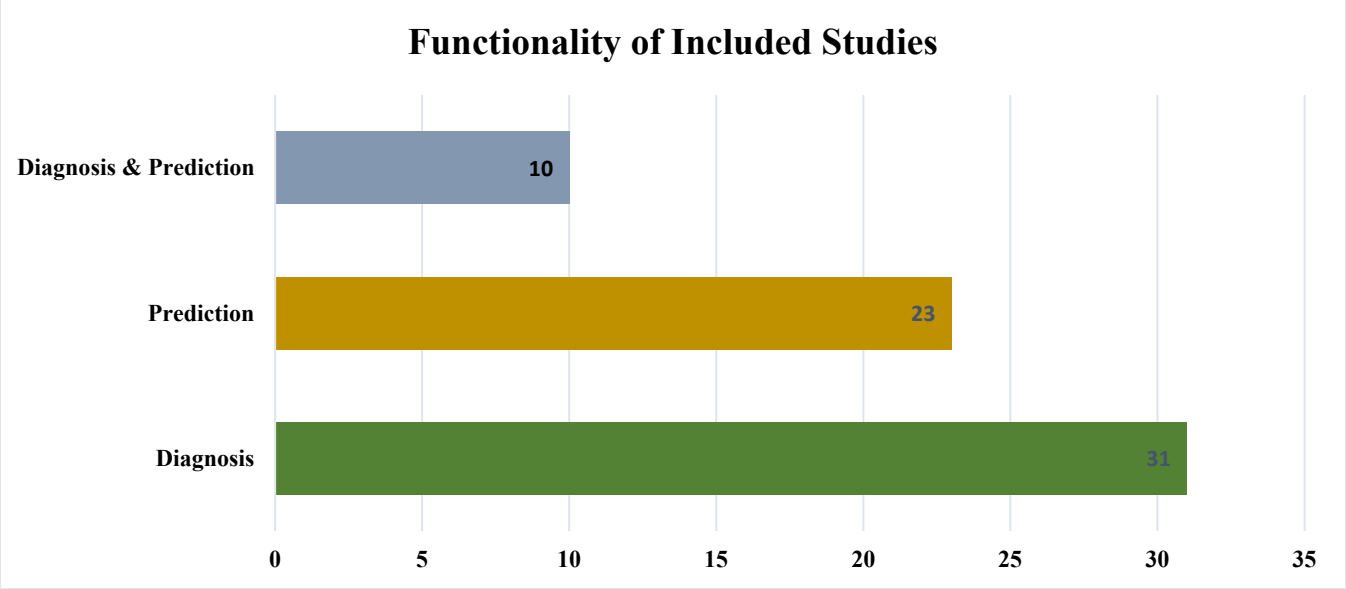

Figure 9. Functionality of included studies.

However, the applicability of included studies is demonstrated in Figure 10. The key applicability area for integrating safety and security using GT or BN is risk assessment (60%) of included studies. It is observed that vulnerability assessment, attack analysis, safety analysis, and fault analysis are 16%, 5%, 3%, and 3%, respectively. Moreover, the applicability of approximately 1% of total studies is in holistic event investigation, resilience quantification, cyber impact assessment, root cause analysis, intrusion detection, trust computation, anomaly detection, reliability assessment, software verification, and water traffic management.

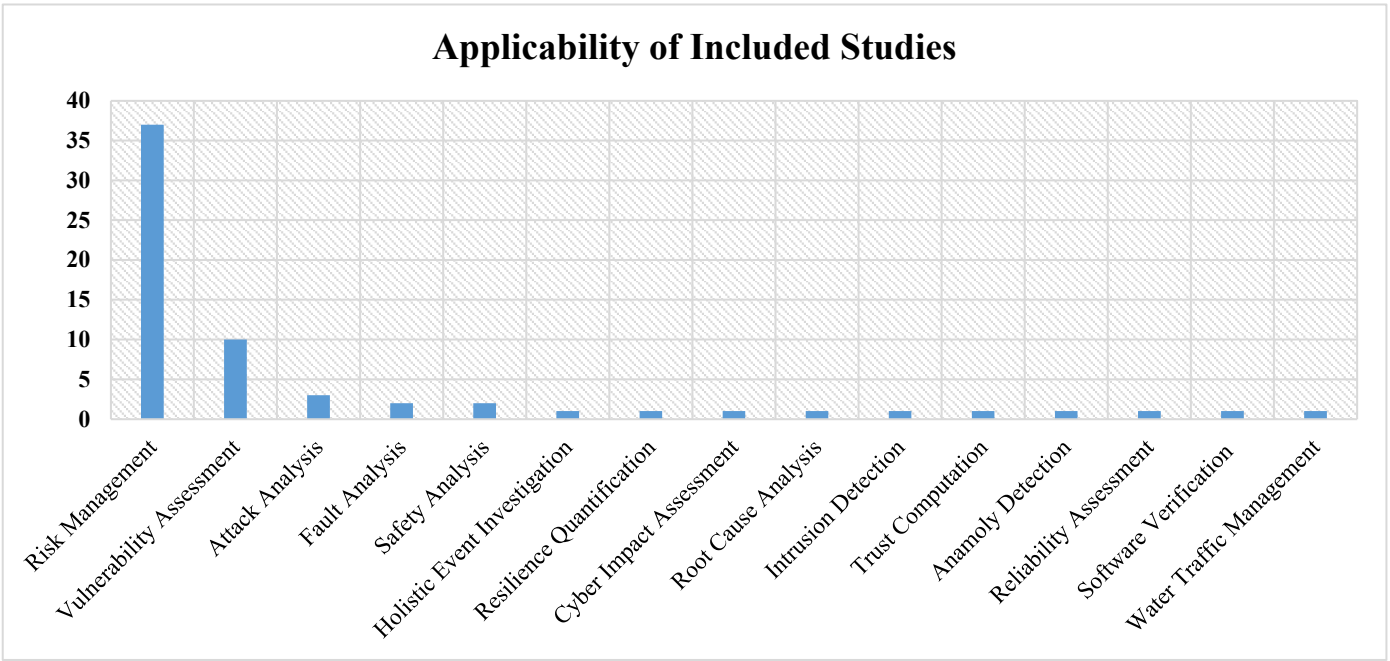

Figure 10. Applicability of included studies.

5.3. What Have Been the Targeted Application Domains?

Figure 11 demonstrates the application sectors of BN and GT models for jointly monitoring safety and security events. The key sectors are the maritime (14%), vehicle transportation (13%), railway (13%), nuclear (6%), chemical (6%), gas and pipelines (5%), smart grid (5%), network security (5%), air transportation (3%), public sector (3%), and CPS (3%) industries. The other preferred application sectors were software (2%), water traffic system (2%), ICS (2%), education (2%), UAV (2%), complex systems (2%), oil wharf handling (2%), process plant (2%), socio-technical systems (2%), SoS (2%), navigation environment (2%), petroleum plants (2%), mobile networks (2%), cognitive radio networks (2%), Asian games (2%), and medical (2%).

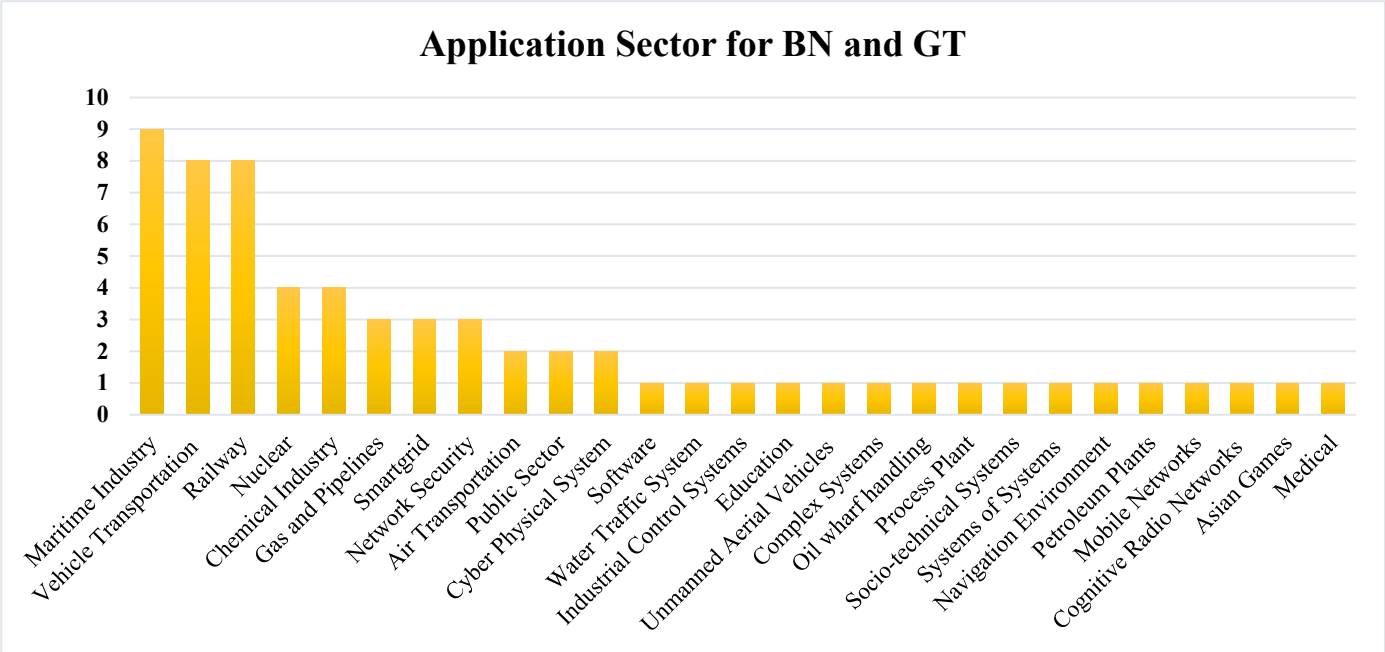

Figure 11. Application sectors of included studies.

5.4. What Solutions Have Been Developed in the Identified Studies?

This RQ aims to provide insight into the existing solutions, based on GT or BN, for integrating security and safety. The research outcomes of the included studies were shown in Table 5. It has been observed that 60% of the included studies have focused on risk assessment and monitoring. Meizhi et al. [44] presented a statistical evaluation of risks to achieve valuable insights into ports protection and build the fundamental BN approach. A dynamic model was introduced, using expert judgment and historical data to evaluate the emergency risk of sea lanes. André et al. [105] focused on protecting ventricular assist devices (VAD)-related risks that have great significance for patient safety, having customized VAD, regarding patients' intensity of sickness and metabolism. Moreover, safety-oriented guidelines are introduced, which also plays an indispensable role in decreasing risk reduction.

Table 5. Research outcomes of included studies.

Study	Research Outcome	Study	Research Outcome
Xiaorong et al. [42]	Risk Assessment Model	Galizia et al. [74]	Risk Analysis Framework
Lipeng et al. [43]	Systematic Causation Model	Francesca et al. [75]	Vulnerability Assessment Method
Meizhi et al. [44]	Dynamic Bayesian Network Model	Zhao et al. [76]	Safety State Assessment Model
Raditya et al. [45]	Risk Oriented Decision-Making Method	Mark et al. [77]	Vulnerability Assessment
Tai-hua et al. [46]	Risk Assessment Model	Remya et al. [78]	System Safety Approach
Mingjing et al. [47]	Interpretative Structural Model	Xin Chen [79]	Polynomial-Time Algorithm
Xiaoxue et al. [48]	An Integrated Security and Safety Framework	Mark et al. [80]	Extended Risk Evaluation Model
Xin et al. [49]	Ideological Security Assessment Method	Martin et al. [81]	Spatial Agent Enabled Model
Meizhi et al. [50]	Analytical Model	Jinsoo et al. [82]	Security Risk Model
Niamat et al. [51]	Resilience Framework	Marco et al. [83]	Transformational Approach
Chengpeng et al. [52]	Risk Assessment Model	Matti et al. [84]	Risk Assessment Method
Yi et al. [53]	Risk Probability Evaluation Model	Xiqiang et al. [85]	BN-Based Structure Learning Algorithm
Barry et al. [54]	Cyber Risk Classification Model	Yongjia et al. [86]	Three-Layer Bayesian Model
Alexandre et al. [55]	Cyber Impact Evaluation Framework	Kairan et al. [87]	Security Assessment Model
Sabarathinam et al. [56]	A Root Cause Evaluation Framework	Amal et al. [88]	Offshore Piracy Solution
Seyedmohsen et al. [57]	Decision-Making Tool	Guannan et al. [89]	Dependability Evaluation Model
Mario et al. [58]	Intrusion Recognition System	Jiali et al. [90]	Fuzzy-Based BN Model
Chao et al. [59]	Vulnerability Assessment Graph Model	Sher et al. [91]	Mobile Petri Net Model
Nima et al. [60]	Cost Robust Approach for Domino Effects	LONG et al. [92]	Combined BN an FTA Model
Hui et al. [61]	Risk Interaction Analysis Method	Zeng Xianfeng [93]	BN enabled Model
Xiqiang et al. [62]	Risk Management Model	TIAN et al. [94]	Multi-layer System
Jamal et al. [63]	Model-Driven Assessment Approach	William et al. [95]	Unified Framework
Elvin et al. [64]	Malicious Node Detection Approach	Jinsoo et al. [96]	Security Risk Model
Xiaoyan et al. [65]	Risk Identification Model	Stefan et al. [97]	Attack Detection Method
Ying et al. [66]	Risk Analysis Method	Jingjing et al. [98]	Fault Diagnosis Method
Subhojeet et al. [67]	Graph-based Anomaly Detection Technique	John et al. [99]	Security Risk Assessment Method
Huai et al. [68]	GT-BNbased Method	Heung et al. [100]	Fault Estimation Method
Gabriele et al. [69]	A Probabilistic Risk Evaluation Approach	Chaze et al. [101]	Risk Management System
Zhiqiang et al. [70]	Risk Assessment Model	Mo Ming [102]	New GT Method

Table 5. *Cont.*

Study	Research Outcome	Study	Research Outcome
Jinsoo et al. [71]	A Cyber Security Risk Model	Shuliang et al. [103]	Vulnerability Analysis Framework
Donya et al. [72]	Security Vulnerability Valuation Method	Song et al. [104]	BN-Enabled Model
Xianyou et al. [73]	Network Security Model	André et al. [105]	Risk Mitigation Approach

5.5. How Is Performance Validated for Developed Techniques and Algorithmic Solutions?

Validation approaches are essential for BN or GT methods, in order to analyze the performance of developed methodologies. In this SLR, it is observed that 56 out of 64 studies were validated by different mechanisms, and the remaining 8 studies have not reported the validation process, as shown in Figure 12. Sensitivity analyses (20% of included studies) perform a critical function in estimating the robustness of the outcomes on the principal analyses of the developed approaches. It is an important measure to evaluate the influence or impact of key hypotheses or variations on the specific infrastructure, including different analysis methods, protocol variations, outliers, definitions of results, and missing data, among others [48–52]. Another important aspect for validating the proposed technique is comparative analysis (20% of included studies), in which the outcomes of distinct models with different assumptions are compared with the developed approaches [79,80]. The other validation mechanisms recognized in the included studies were expert evaluation, scenarios development, statistical analysis, empirical analysis, reachability graph, diagnostic analysis, checklists, cross-validation, and minimax analysis, 16%, 12%, 8%, 3%, 2%, 2%, 2%, 2%, and 2%, respectively.

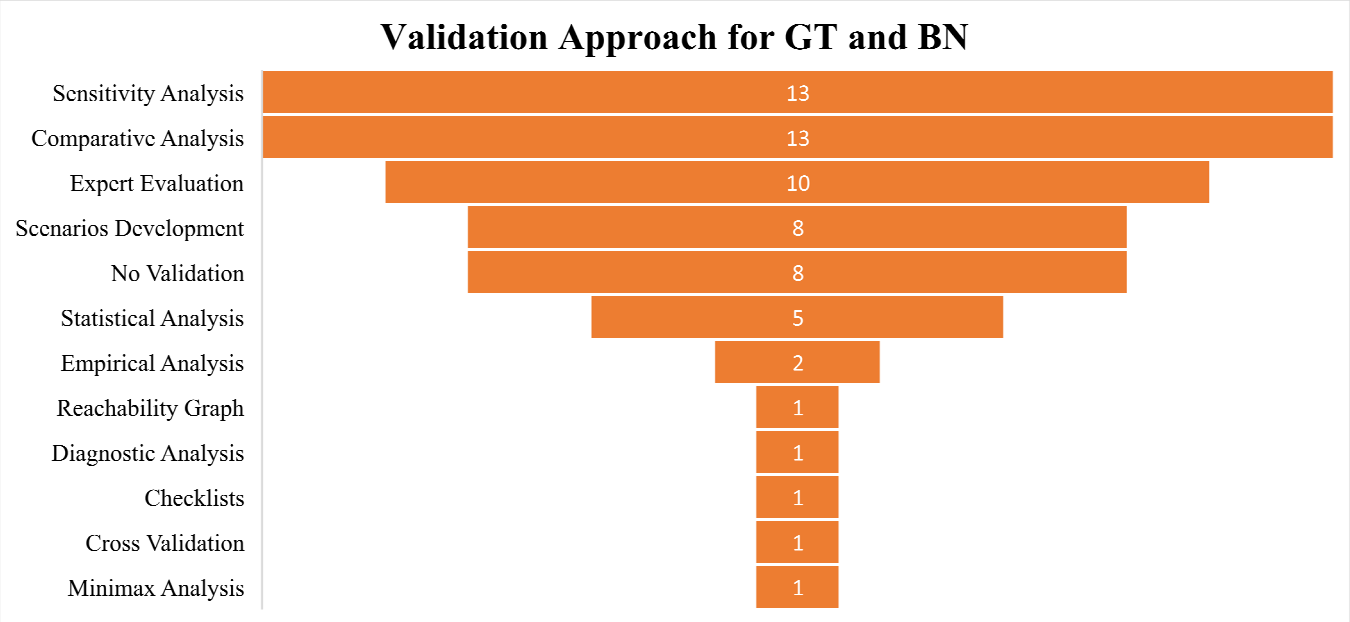

Figure 12. Validation approaches of included studies.

5.6. What Are the Advantages and Disadvantages of Existing Studies?

As elaborated in the included studies, the incorporation of safety and security measures based on GT and BN can benefit different CIs. Although there are certain shortcomings with the developed solutions, the advantages and disadvantages of existing BN or GT methods are discussed in this section, as shown in Table 6.

Table 6. Pros and cons of included studies.

Study	Pros	Cons
Xiaorong et al. [42]	Offers a feasible solution for risk assessment in CPS, the feasibility is verified based on two event scenarios.	Lacks in presenting the finished model of the research.
Lipeng et al. [43]	The key benefit of the proposed model is that its applicability is checked in multiple scenarios.	The process consumes a lot of time, thus restricting the model's application up to few only.
Meizhi et al. [44]	Utilization of vast dataset.	The use case areas are fixed.
Raditya et al. [45]	This study is useful in offering real-time risk management options to mitigate cyber threats.	This study has not provided conclusive data, as it was an early study.
Tai-hua et al. [46]	Potential to be applied for Chinese enterprises in presenting efficient anomaly prevention and response policies.	It is specified for Chinese enterprises for a Chinese problem. Readjustment is needed if used in other places.
Mingjing et al. [47]	Efficient in enhancing security in urban express logistics and avoiding safety hazards.	Merely a prototype is proposed.
Xiaoxue et al. [48]	The authors recommended low vulnerable and improved resilient perspective for the northern sea route.	Resilience level needs improvement.
Xin et al. [49]	Improves evaluation accuracy and reduces estimation error for the educational sector.	It has a limited use case to demonstrate its developed method.
Meizhi et al. [50]	Various significant influencing factors for maritime piracy are identified, and the applicability is authenticated using sensitivity analysis.	Feasibility issues, due to limited data.
Niamat et al. [51]	The capability of framework to be applied for different sectors.	This study does not offer decision-theoretic troubleshooting. Moreover, the framework is still preliminary.
Chengpeng et al. [52]	Offers efficient and flexible risk management for real circumstances.	It is limited up to only operational aspects. In contrast, complete analysis is not focused on this tool.
Yi et al. [53]	More accuracy in the navigation risk of ships in the bridge area in distinct conditions.	This research is validated based on a specific use case.
Barry et al. [54]	High prediction accuracy (nearly 100%) of the qualitative and quantitative risk factors.	It is used for specific sectors only.
Alexandre et al. [55]	Efficient in demonstrating cyber impacts in whole systems based on invaders and defenders' plans, without knowing the hard-to-assess attacker's activities.	Limited scenarios and tested situations.
Sabarathinam et al. [56]	To assist in determining the root cause of risks within the systems.	The results are based on simulations.
Seyedmohsen et al. [57]	Both qualitative and quantitative factors are used with rigorous testing.	Perhaps overspecialized. Only to be used in its sector.
Mario et al. [58]	The accuracy of the developed model is reasonably optimal.	Lacking in measuring efficiency in real-time scenarios.
Chao et al. [59]	Ability to decrease the risk of intended attacks by continuous monitoring	Allocation optimization is not considered.

Table 6. *Cont.*

Study	Pros	Cons
Nima et al. [60]	A cost-efficient solution for vulnerability assessment.	Limited to restricted sectors.
Hui et al. [61]	Offers practical recommendations for establishing countermeasures in diminishing risk events in railway.	A risk mitigation strategy is not presented.
Xiqiang et al. [62]	Efficient in diagnosing of main factors, which may put threats to rail transport.	Threat actors are not specified.
Jamal et al. [63]	High efficiency in autonomous quarry mitigation associated with signal interference.	Cannot protect from all high impact attacks.
Elvin et al. [64]	Improved malicious detection in vehicular networks, due to inclusion of perception and reasoning in the decision building process.	Results are still preliminary.
Xiaoyan et al. [65]	Continuous evaluation of possible incident frequencies and outcomes by providing unique risk awareness.	Conditional probability tables are not presented.
Ying et al. [66]	The casual diagnostic analysis in complex and uncertain environments. More accurate than fault tree analysis.	Complex data collection process, an automatic technology for collecting required information, is not considered.
Subhojeet et al. [67]	Capability to recognize malicious threats and differentiate them from safety-critical activities.	The developed model is still preliminary.
Huai et al. [68]	Failure analysis from different prospects, such as topology, functional restriction, environmental, and dynamic.	There needs an improvement for analyzing network measurements and results of unit failures.
Gabriele et al. [69]	Accurate quantitative estimation of attack success probability and for the classification of the more hazardous escalation situations.	Lacks in performing a quantitative evaluation of the credibility of attack success.
Zhiqiang et al. [70]	An efficient quantitative risk assessment for finding security weaknesses.	The results need to be verified based on real-time scenarios.
Jinsoo et al. [71]	A generic approach toward monitoring and mitigating security and safety risks.	This study is conducted for a specific sector.
Donya et al. [72]	This study efficiently resolves uncertainties in the failure probability of elements and the temporal classification of occurrences.	The developed model is still preliminary.
Xianyou et al. [73]	Using multiple BN models to accurately assess vulnerabilities.	The developed model is still preliminary.
Galizia et al. [74]	New recommendations for resilience in socio-technical systems.	Lacks in presenting real-time analysis.
Francesca et al. [75]	A systematic procedure for vulnerability assessment against outside threats.	Insider threats are not considered in this study.
Zhao et al. [76]	An experiential analysis that effectively exhibits the safety status for the navigation environment.	Threats are not specified.
Mark et al. [77]	Increase awareness in vulnerability management for the chemical industry.	This study is conducted for a specific sector.
Remya et al. [78]	Robustly monitoring of unmodeled and unexpected failures.	This study does not robustly manage unexpected and unmodeled failures.
Xin Chen [79]	Efficiently evaluate vulnerabilities and crucial devices of the system.	The simulation results still need to be modified.

Table 6. *Cont.*

Study	Pros	Cons
Mark et al. [80]	Efforts in delivering awareness to society for the development of databases about associated security failures.	The developed methodology is still preliminary.
Martin et al. [81]	The accuracy of the developed model is reasonably well in comparing existing approaches.	The developed model is still preliminary.
Jinsoo et al. [82]	An efficient mitigation measures for real-time analysis of risks in the nuclear sector.	The proposed research affects BN accuracy.
Marco et al. [83]	Results verified for combined attacks with mutual and non-trivial influences.	Limited to only one case study.
Matti et al. [84]	This research is helpful in documenting the expert knowledge.	Real-time traffic monitoring control has not been performed.
Xiqiang et al. [85]	Applicability in emergency cases with high accuracy.	Specific for the case study. Challenging implementing in other fields.
Yongjia et al. [86]	Having low-SNR and better availability.	The results are only preliminary. Testing on the different scenarios is needed.
Kairan et al. [87]	A security assessment is verified using a use case study.	The results are only preliminary.
Amal et al. [88]	BN implementation improves the Sargos system with is inherent abilities.	A specific approach is developed for the maritime industry; a lot of modifications are needed for use in other sectors.
Guannan et al. [89]	A dynamic and optimal risk assessment for the software industry.	The simulation results still need to be modified.
Jiali et al. [90]	Increases accuracy for risk assessment in the maritime industry.	Lacks in empirical data for circumstantial results.
Sher et al. [91]	Offers support mobility, protection, and concurrency for software verification.	Threat actors are not specified.
LONG et al. [92]	Offer recommendations for the designing and implementing of the energy sector to decrease the potential risks.	Specific use cases are hard to emulate outside of the sector or system.
Zeng Xianfeng [93]	Presented reliable dataset for research purposes in the railway sector.	Lack of practicality in railways.
TIAN et al. [94]	More robust solution for the water traffic system.	The human factor is not considered in real-time monitoring and is lacking for managing adequate personnel.
William et al. [95]	Applicable for both known and unknown vulnerabilities.	Limited applicability domains.
Jinsoo et al. [96]	This study assists in identifying fundamental factors that may pose cybersecurity hazards.	The simulation results still need to be modified.
Stefan et al. [97]	Reduces communication redundancies and enables data uniformity inspection in transportation.	Limited usability.
Jingjing et al. [98]	Improved accuracy and effective use of train control system.	Merely a preliminary analysis for the high-speed railway.
John et al. [99]	Feasibility and compatibility for protecting air transportation.	The results are only preliminary.
Heung et al. [100]	Systematic evaluation of the anticipated faults in the system.	There is not sufficient data of safety-critical software, assembled for real-time systems.

Table 6. *Cont.*

Study	Pros	Cons
Chaze et al. [101]	To efficiently recognize and respond to risks in maritime piracy.	There is a need for an ontology for proper usability.
Mo Ming [102]	Correctly demonstrate the network safety situation and improve the safety of the system.	Heavily integrated with its system; therefore, difficult to use outside of network security analysis.
Shuliang et al. [103]	Efficiency in analyzing vulnerabilities in smart grid.	The developed model is more methodological than practical.
Song et al. [104]	The developed BN model plays a significant role in reducing fire risks.	The testing is not entirely performed before winter games.
André et al. [105]	Providing a better quality of life and more prolonged survival of patients.	The threat actors are not specified.

5.7. Limitations

This study has given below limitations:

(1) The inclusion of articles is solely based on the English language, which indicates that notable studies of security and safety integration based on BN or GT in other languages have not been considered.
(2) The results of this SLR are based on a restricted number of databases. These databases are used, due to the widespread usage for querying papers in the field of GT and BN.
(3) Included studies were performed in different applications, so it might be not possible to compare each perspective.

6. Conclusions

Modern systems must simultaneously guarantee security and safety to provide continuous and accurate execution of crucial roles and services. Since security and safety depend on each other, they must be collectively applied to acquire the root cause assessment of noticeable issues. Therefore, numerous methods are developed to integrate security and safety; however, BN and GT are considered in this SLR, due to their extensive usage in various applications. This SLR includes 64 studies, and given below are concluding points:

(a) It is observed that from the 64 included studies, 51 used BN models, 10 utilized GT models, and the remaining 3 were based on united BN and GT.
(b) Most development scenarios utilized 40 nodes for performing experiments to observe unintentional failures or risks for GT and BN models.
(c) It has been emphasized that approximately one-third of BN and GT models were evaluated in real-time; however, others were either based on simulation analysis or theoretical concepts.
(d) There were two types of data sources (EK and ED) used for developing BN and GT models for different applications.
(e) The key performance validation mechanisms for the included studies were statistical analysis, expert evaluation, and sensitivity analysis.

The future research directions for safety and security integration were the following:

(a) There is a need to develop a generic tool or method or standard to combine security and safety, which can be helpful for different applications, since the significance of integrating both measures was demonstrated in this SLR, and a generic approach may offer feasibility and flexibility.
(b) It is observed that there are various validation methods for evaluating BN or GT. A more extended investigation is necessary to estimate the accuracy and efficiency of validation mechanisms, in order to find the optimal option.

(c) Moreover, there is a need to research to acquire information about the suitable number of nodes to ensure reliable and accurate performance for ensuring safety and security based on BN or GT models.
(d) Further research could improve Bayesian analysis based on the Metropolis–Hastings algorithm and Gaussian distributions [107].

Author Contributions: S.P., V.G. and S.K. designed the study theme and conducted the literature study. S.P. and V.G. examined the data from different databases and performed initial data screening. S.P. interpreted the results and wrote the paper. V.G. and S.K. analyzed data, verified the results, and revised the paper. S.K. assisted in supervising the activities and study's well-organized procedure. All authors have read and agreed to the published version of the manuscript.

Funding: This research received funding from the Research Council of Norway through (a) the CybWin (Cybersecurity Platform for Assessment and Training for Critical Infrastructures-Legacy to digital twin), project no. 287808; and (b) the SFI Norwegian Centre for Cybersecurity in Critical Sectors (NORCICS), project no. 310105.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: This work has received funding from the Research Council of Norway through (a) the CybWin (Cybersecurity Platform for Assessment and Training for Critical Infrastructures-Legacy to digital twin), project no. 287808; and (b) the SFI Norwegian Centre for Cybersecurity in Critical Sectors (NORCICS), project no. 310105. Also, authors would like to express great appreciation to IIK Department at NTNU Gjovik Campus, and ICT Research Department at NR.

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

References

1. Baker, T.; Asim, M.; MacDermott, Á.; Iqbal, F.; Kamoun, F.; Shah, B.; Alfandi, O.; Hammoudeh, M. A secure fog-based platform for SCADA-based IoT critical infrastructure. *Softw. Pract. Exp.* **2020**, *50*, 503–518. [CrossRef]
2. Kotenko, I.; Saenko, I.; Kushnerevich, A.; Branitskiy, A. Attack detection in IoT critical infrastructures: A machine learning and big data processing approach. In Proceedings of the 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), Pavia, Italy, 13–15 February 2019; pp. 340–347.
3. Stellios, I.; Kotzanikolaou, P.; Psarakis, M.; Alcaraz, C.; Lopez, J. A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3453–3495. [CrossRef]
4. Kornecki, A.J.; Liu, M. Fault Tree Analysis for Safety/Security Verification in Aviation Software. *Electronics* **2013**, *2*, 41–56. [CrossRef]
5. Schmittner, C.; Ma, Z.; Schoitsch, E.; Gruber, T. A case study of fmvea and chassis as safety and security co-analysis method for automotive cyber-physical systems. In Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, Singapore, 14 April 2015; pp. 69–80.
6. Banerjee, A.; Venkatasubramanian, K.K.; Mukherjee, T.; Gupta, S.K.S. Ensuring safety, security, and sustainability of mission-critical cyber–physical systems. *Proc. IEEE* **2012**, *100*, 283–299. [CrossRef]
7. Kornecki, A.J.; Subramanian, N.; Zalewski, J. Studying interrelationships of safety and security for software assurance in cyberphysical systems: Approach based on bayesian belief networks. In Proceedings of the 2013 Federated Conference on Computer Science and Information Systems, Krakow, Poland, 8–11 September 2013; pp. 1393–1399.
8. John, A.; Yang, Z.; Riahi, R.; Wang, J. A risk assessment approach to improve the resilience of a seaport system using Bayesian networks. *Ocean Eng.* **2016**, *111*, 136–147. [CrossRef]
9. Zeng, J.; Wu, S.; Chen, Y.; Zeng, R.; Wu, C. Survey of attack graph analysis methods from the perspective of data and knowledge processing. *Secur. Commun. Netw.* **2019**, *2019*, 1–17. [CrossRef]
10. Sharma, R.; Kamble, S.S.; Gunasekaran, A.; Kumar, V.; Kumar, A. A systematic literature review on machine learning applications for sustainable agriculture supply chain performance. *Comput. Oper. Res.* **2020**, *119*, 104926. [CrossRef]
11. Gupta, R.; Tanwar, S.; Kumar, N.; Tyagi, S. Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review. *Comput. Electr. Eng.* **2020**, *86*, 106717. [CrossRef]
12. Chockalingam, S.; Hadžiosmanović, D.; Pieters, W.; Teixeira, A.A.; van Gelder, P. Integrated Safety and Security Risk Assessment Methods: A Survey of Key Characteristics and Applications. In *Critical Information Infrastructures Security*; Havarneanu, G., Setola, R., Nassopoulos, H., Wolthusen, S., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2017; Volume 10242. [CrossRef]

13. Lallie, H.S.; Debattista, K.; Bal, J. A review of attack graph and attack tree visual syntax in cyber security. *Comput. Sci. Rev.* **2020**, *35*, 100219. [CrossRef]
14. Fovino, L.N.; Masera, M.; De Cian, A. Integrating cyber attacks within fault trees. *Reliab. Eng. Syst. Saf.* **2009**, *94–99*, 1394–1402. [CrossRef]
15. Kriaa, S.; Bouissou, M. Modeling safety and security interdependencies with bdmp (boolean logic driven markov processes). In *SAFECOMP 2014*; Bondavalli, A., Ceccarelli, A., Ortmeier, F., Eds.; Springer: Cham, Switzerland, 2014.
16. Abdo, H.; Kaouk, M.; Flaus, J.-M.; Masse, F. A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie—Combining new version of attack tree with bowtie analysis. *Comput. Secur.* **2018**, *72*, 175–195. [CrossRef]
17. Galagedarage Don, M.; Khan, F. Process Fault Prognosis Using Hidden Markov Model—Bayesian Networks Hybrid Model. *Ind. Eng. Chem. Res.* **2019**, *58*, 12041–12053. [CrossRef]
18. Cooper, G.F.; Herskovits, E. A Bayesian method for the induction of probabilistic networks from data. *Mach. Learn.* **1992**, *9*, 309–347. [CrossRef]
19. Afenyo, M.; Khan, F.; Veitch, B.; Yang, M. Arctic shipping accident scenario analysis using Bayesian Network approach. *Ocean Eng.* **2017**, *133*, 224–230. [CrossRef]
20. Kabir, S.; Papadopoulos, Y. Applications of Bayesian networks and Petri nets in safety, reliability, and risk assessments: A review. *Saf. Sci.* **2019**, *115*, 154–175. [CrossRef]
21. Bruni, R.; Melgratti, H.; Montanari, U. Bayesian network semantics for Petri nets. *Theor. Comput. Sci.* **2020**, *807*, 95–113. [CrossRef]
22. Lichte, D.; Wolf, K.-D. Bayesian Network Based Analysis of Cyber Security Impact on Safety. In Proceedings of the 29th European Safety and Reliability Conference, Hannover, Germany, 22–26 September 2019; pp. 1502–1509.
23. Jensen, F.V.; Nielsen, T.D. *Bayesian Networks and Decision Graphs*; Springer: Berlin, Germany, 2007.
24. Heckerman, D.; Geiger, D.; Chickering, D.M. Learning bayesian networks: The combination of knowledge and statistical data. *Mach. Learn.* **1995**, *20*, 197–243. [CrossRef]
25. Liao, W.; Ji, Q. Learning Bayesian network parameters under incomplete data with domain knowledge. *Pattern Recognit.* **2009**, *42*, 3046–3056. [CrossRef]
26. Friedman, N. The bayesian structural em algorithm. In Proceedings of the Fourteenth Conference on Uncertainty in Artificial Intelligence, Madison, WI, USA, 24–26 July 1998; pp. 129–138.
27. Blei, D.M.; Kucukelbir, A.; McAuliffe, J.D. Variational inference: A review for statisticians. *J. Am. Stat. Assoc.* **2017**, *112*, 859–877. [CrossRef]
28. Pelikan, M.; Goldberg, D.E.; Lobo, F.G. A survey of optimization by building and using probabilistic models. *Comput. Optim. Appl.* **2002**, *21*, 5–20. [CrossRef]
29. Khakzad, N.; Reniers, G. Using graph theory to analyze the vulnerability of process plants in the context of cascading effects. *Reliab. Eng. Syst. Saf.* **2015**, *143*, 63–73. [CrossRef]
30. Ferrario, E.; Pedroni, N.; Zio, E. Evaluation of the robustness of critical infrastructures by Hierarchical Graph representation, clustering and Monte Carlo simulation. *Reliab. Eng. Syst. Saf.* **2016**, *155*, 78–96. [CrossRef]
31. Leitold, D.; Vathy-Fogarassy, A.; Abonyi, J. Controllability and observability in complex networks—The effect of connection types. *Sci. Rep.* **2017**, *7*, 151. [CrossRef]
32. Dwivedi, A.; Yu, X. A Maximum-Flow-Based Complex Network Approach for Power System Vulnerability Analysis. *IEEE Trans. Ind. Inform.* **2011**, *9*, 81–88. [CrossRef]
33. Kabir, M.; Mishra, Y.; Bansal, R. Probabilistic load flow for distribution systems with uncertain PV generation. *Appl. Energy* **2016**, *163*, 343–351. [CrossRef]
34. Fu, X.; Sun, H.; Guo, Q.; Pan, Z.; Zhang, X.; Zeng, S. Probabilistic power flow analysis considering the dependence between power and heat. *Appl. Energy* **2017**, *191*, 582–592. [CrossRef]
35. Johansson, J.; Hassel, H. An approach for modelling interdependent infrastructures in the context of vulnerability analysis. *Reliab. Eng. Syst. Saf.* **2010**, *95*, 1335–1344. [CrossRef]
36. Casoetto, B.; Flottes, E.; Ardeois, J.; Thanh, N.; Joliot, J.-B.; Nait-Abdallah, R. How to commercialize reliable capacities on a com-plex transmission network? *J. Nat. Gas. Sci. Eng.* **2011**, *3*, 657–663. [CrossRef]
37. Chung, F.R.K.; Lu, L. *Complex Graphs and Networks, Volume 107 of CBMS Regional Conference Series in Mathematics*; American Mathematical Society: Providence, RI, USA, 2006.
38. Ahmat, K. *Graph Theory and Optimization Problems for Very Large Networks*; City University of New York: New York, NY, USA, 2009.
39. Shirinivas, S.G.; Vetrivel, S.; Elango, N.M. Applications of graph theory in computer science—An overview. *Int. J. Eng. Sci. Technol.* **2010**, *2*, 4610–4621.
40. Hossain, N.U.I.; Nur, F.; Hosseini, S.; Jaradat, R.; Marufuzzaman, M.; Puryear, S.M. A Bayesian network based approach for modeling and assessing resilience: A case study of a full service deep water port. *Reliab. Eng. Syst. Saf.* **2019**, *189*, 378–396. [CrossRef]
41. Silva, A.; Silva, K.; Rocha, A.; Queiroz, F. Calculating the trust of providers through the construction weighted Sec-SLA. *Futur. Gener. Comput. Syst.* **2019**, *97*, 873–886. [CrossRef]
42. Lyu, X.; Ding, Y.; Yang, S.-H. Bayesian Network Based C2P Risk Assessment for Cyber-Physical Systems. *IEEE Access* **2020**, *8*, 88506–88517. [CrossRef]

43. Fu, L.; Wang, X.; Liu, B.; Li, L. Investigation into the role of human and organizational factors in security work against terrorism at large-scale events. *Saf. Sci.* **2020**, *128*, 104764. [CrossRef]
44. Jiang, M.; Lu, J. Maritime accident risk estimation for sea lanes based on a dynamic Bayesian network. *Marit. Policy Manag.* **2020**, *47*, 649–664. [CrossRef]
45. Arief, R.; Khakzad, N.; Pieters, W. Mitigating cyberattack related domino effects in process plants via ICS seg-mentation. *J. Inf. Secur. Appl.* **2020**, *51*, 102450.
46. Yang, T.-H.; Qin, J.; Li, Z.-X. Public Safety Risk Assessment of Power Investment Project Based on Fuzzy Set and DS Evidence Theory. *E3S Web Conf.* **2020**, *143*, 02009. [CrossRef]
47. Zhao, M.; Ji, S.; Zhao, Q.; Chen, C.; Wei, Z.-L. Risk Influencing Factor Analysis of Urban Express Logistics for Public Safety: A Chinese Perspective. *Math. Probl. Eng.* **2020**, *2020*, 1–14. [CrossRef]
48. Ma, X.; Zhou, Q.; Liu, T.; Liu, Y.; Qiao, W. Security of the Arctic route from the resilience perspective: The ideal state, influencing factors, and evaluation. *Marit. Policy Manag.* **2020**, 1–14. [CrossRef]
49. Gao, X. Study on Ideological Safety Assessment Methods for College Students in the New Era. In Proceedings of the 12th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), Phuket, Thailand, 28–29 February 2020; pp. 962–966.
50. Jiang, M.; Lu, J. The analysis of maritime piracy occurred in Southeast Asia by using Bayesian network. *Transp. Res. Part E Logist. Transp. Rev.* **2020**, *139*, 101965. [CrossRef]
51. Hossain, N.U.I.; Raed, J.; Seyedmohsen, H.; Mohammad, M.; Randy, K.B. A framework for modeling and assessing system resilience using a Bayesian network: A case study of an interdependent electrical infrastructure system. *Int. J. Crit. Infrastruct. Prot.* **2019**, *25*, 62–83. [CrossRef]
52. Hosseini, S.; Ivanov, D. Bayesian networks for supply chain risk, resilience and ripple effect analysis: A literature review. *Expert Syst. Appl.* **2020**, *161*, 113649. [CrossRef] [PubMed]
53. Wan, Y.; Liu, C.; Qiao, W. An advanced fuzzy Bayesian-based FMEA approach for assessing maritime supply chain risks. *Transp. Res. Part E Logist. Transp. Rev.* **2019**, *125*, 222–240. [CrossRef]
54. Sheehan, B.; Finbarr, M.; Martin, M.; Cian, R. Connected and autonomous vehicles: A cyber-risk classification framework. *Transp. Res. Part A Policy Pract.* **2019**, *124*, 523–536. [CrossRef]
55. Barreto, A.B.; Costa, P. Cyber-ARGUS-A mission assurance framework. *J. Netw. Comput. Appl.* **2019**, *133*, 86–108. [CrossRef]
56. Chockalingam, S.; Katta, V. Developing a Bayesian Network Framework for Root Cause Analysis of Observable Problems in Cyber-Physical Systems. In Proceedings of the 2019 IEEE Conference on Information and Communication Technology, Baku, Azerbaijan, 23–25 October 2019; pp. 1–6.
57. Hosseini, S. Sarder Development of a Bayesian network model for optimal site selection of electric vehicle charging station. *Int. J. Electr. Power Energy Syst.* **2018**, *105*, 110–122. [CrossRef]
58. Casillo, M.; Simone, C.; De Santo, M.; Pascale, F.; Santonicola, E. Embedded Intrusion Detection System for Detecting Attacks over CAN-BUS. In Proceedings of the 4th International Conference on System Reliability and Safety (ICSRS), Rome, Italy, 20–22 November 2019; pp. 136–141.
59. Chen, C.; Reniers, G.; Khakzad, N. Integrating safety and security resources to protect chemical industrial parks from man-made domino effects: A dynamic graph approach. *Reliab. Eng. Syst. Saf.* **2019**, *191*, 106470. [CrossRef]
60. Khakzad, N.; Reniers, G. Low-capacity utilization of process plants: A cost-robust approach to tackle man-made domino effects. *Reliab. Eng. Syst. Saf.* **2019**, *191*, 106114. [CrossRef]
61. Xu, H.; Zhang, Y.; Li, H.; Skitmore, M.; Yang, J.; Yu, F. Safety risks in rail stations: An interactive approach. *J. Rail Transp. Plan. Manag.* **2019**, *11*, 100148. [CrossRef]
62. Zhou, X. Security Analysis about Switching Equipment Based on Bayesian Networks. In Proceedings of the Sixth International Conference on Transportation Engineering, Chengdu, China, 20–22 September 2019; pp. 385–391.
63. El Hachem, J.; Sedaghatbaf, A.; Lisova, E.; Causevic, A. Using Bayesian Networks for a Cyberattacks Propagation Analysis in Systems-of-Systems. In Proceedings of the 26th Asia-Pacific Software Engineering Conference (APSEC), Putrajaya, Malaysia, 2–5 December 2019; pp. 363–370.
64. Elvin, E.; Tepe, K.; Balador, A.; Nwizege, K.S.; Jaimes, L.M. Malicious node detection in vehicular adhoc network using machine learning and deep learning. In Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–6.
65. Guo, X.; Zhang, L.; Liang, W.; Haugen, S. Risk identification of third-party damage on oil and gas pipe-lines through the Bayesian network. *J. Loss Prev. Process Ind.* **2018**, *54*, 163–178. [CrossRef]
66. Zhou, Y.; Li, C.; Zhou, C.; Luo, H. Using Bayesian network for safety risk analysis of diaphragm wall deflection based on field data. *Reliab. Eng. Syst. Saf.* **2018**, *180*, 152–167. [CrossRef]
67. Mukherjee, S.; Walkery, J.; Rayz, I.; Daily, J. A precedence graph-based approach to detect message injection attacks in J1939 based networks. In Proceedings of the 15th Annual Conference on Privacy, Security and Trust (PST), Calgary, AB, Canada, 28–30 August 2017; pp. 67–76.
68. Su, H.; Zhang, J.; Zio, E.; Yang, N.; Li, X.; Zhang, Z. An integrated systemic method for supply reliability assessment of natural gas pipeline networks. *Appl. Energy* **2018**, *209*, 489–501. [CrossRef]

69. Landucci, G.; Argenti, F.; Cozzani, V.; Reniers, G. Assessment of attack likelihood to support security risk assessment studies for chemical facilities. *Process. Saf. Environ. Prot.* **2017**, *110*, 102–114. [CrossRef]
70. Hou, Z.; Zhao, P. Based on Fuzzy Bayesian Network of Oil Wharf Handling Risk Assessment. *Math. Probl. Eng.* **2016**, *2016*, 1–10. [CrossRef]
71. Shin, J.; Son, H.; Heo, G. Cyber Security Risk Evaluation of a Nuclear I&C Using BN and ET. *Nucl. Eng. Technol.* **2017**, *49*, 517–524. [CrossRef]
72. Donya, F.; Khakzad, N.; Reniers, G.; Cozzani, V. Security vulnerability assessment of gas pipelines using Discrete-time Bayesian network. *Process Saf. Environ. Prot.* **2017**, *111*, 714–725.
73. Liang, H.; Chen, X.; Lai, X. Computer network vulnerability assessment and safety evaluation application based on Bayesian theory. *Int. J. Secur. Its Appl.* **2016**, *10*, 359–368.
74. De Galizia, A.; Simon, C.; Weber, P.; Iung, B.; Duval, C.; Serdet, E. Modelling Non-Deterministic Causal Mechanisms involving Resilience in Risk Analysis. *IFAC-PapersOnLine* **2016**, *49*, 325–330. [CrossRef]
75. Argenti, F.; Landucci, G.; Reniers, G. Probabilistic vulnerability assessment of chemical plants subjected to external acts of interference. *Chem. Eng. Trans.* **2016**, *48*, 691–696. [CrossRef]
76. Chen, Z.; Zhang, Q.; Wu, X.; Yang, J.; Zhang, X. Safety state evaluation and risk management of navigation environment in harbour waters based on Bayesian network. In Proceedings of the 2016 IEEE International Conference on Intelligent Transportation Engineering (ICITE), Singapore, 20–22 August 2016; pp. 80–84.
77. van Staalduinen, M.A.; Khan, F.; Gadag, V. SVAPP methodology: A predictive security vulnerability assessment modeling method. *J. Loss Prev. Process. Ind.* **2016**, *43*, 397–413. [CrossRef]
78. Prabhakaran, R.; Krishnaprasad, R.; Nanda, M.; Jayanthi, J. System safety analysis for critical system applications using Bayesian networks. *Procedia Comput. Sci.* **2016**, *93*, 782–790. [CrossRef]
79. Chen, X. System vulnerability assessment and critical nodes identification. *Expert Syst. Appl.* **2016**, *65*, 212–220. [CrossRef]
80. van Staalduinen, M.; Khan, F. A barrier based methodology to assess site security risk. In Proceedings of the SPE E&P Health, Safety, Security and Environmental Conference, Denver, CO, USA, 16–18 March 2015. [CrossRef]
81. Tanguy, M.; Napoli, A. A methodology to improve the assessment of vulnerability on the maritime supply chain of energy. In Proceedings of the OCEANS 2015-MTS/IEEE Washington, Washington, DC, USA, 19–22 October 2015; pp. 1–6.
82. Shin, J.; Son, H.; Heo, G. Development of a cyber security risk model using Bayesian networks. *Reliab. Eng. Syst. Saf.* **2015**, *134*, 208–217. [CrossRef]
83. Gribaudo, M.; Iacono, M.; Marrone, S. Exploiting Bayesian Networks for the Analysis of Combined Attack Trees. *Electron. Notes Theor. Comput. Sci.* **2015**, *310*, 91–111. [CrossRef]
84. Peltola, M.J.; Kekolahti, P. Risk Assessment of Public Safety and Security Mobile Service. In Proceedings of the 10th International Conference on Availability, Reliability and Security, Toulouse, France, 24–27 August 2015; pp. 351–359.
85. Zhou, X.; Zhang, Y. Security Analysis about a Train Control Center Based on a Bayesian Network. *ICTE 2015* **2015**, 2525–2532. [CrossRef]
86. Huo, Y.; Wang, Y.; Lin, W.; Sun, R. Three-layer Bayesian model based spectrum sensing to detect malicious attacks in cognitive radio networks. In Proceedings of the 2015 IEEE International Conference on Communication Workshop (ICCW), London, UK, 8–12 June 2015; pp. 1640–1645.
87. Zhang, K.; Shi, P. Transportation Security Assessment Method for a Mountainous Freeway Using a Bayesian Network. *ICTE 2015* **2015**, 2891–2896. [CrossRef]
88. Bouejla, A.; Chaze, X.; Guarnieri, F.; Napoli, A. A Bayesian network to manage risks of maritime piracy against offshore oil fields. *Saf. Sci.* **2014**, *68*, 222–230. [CrossRef]
89. Si, G.; Xu, J.; Yang, J.; Wen, S. An evaluation model for dependability of Internet-scale software on basis of Bayesian Networks and trustworthiness. *J. Syst. Softw.* **2014**, *89*, 63–75. [CrossRef]
90. Wang, J.; Zhang, Q.; Ji, W. Construction of monitoring model and algorithm design on passenger security during shipping based on improved Bayesian network. *Sci. World J.* **2014**, *2014*, 1–8. [CrossRef] [PubMed]
91. Khan, S.A.; Zafar, N.A.; Ahmad, F.; Islam, S. Extending Petri net to reduce control strategies of railway interlocking system. *Appl. Math. Model.* **2014**, *38*, 413–424. [CrossRef]
92. Hang, L.; Shou-Xin, S.; Yu-Hui, Z.; Jia, X.; Qi, Y.; Qian-Hui, H. Probabilistic safety assessment for power transmission and transformation maintenance project based on fault tree analysis and Bayesian network. In Proceedings of the 2014 International Conference on Power System Technology, Chengdu, China, 20–22 October 2014; pp. 1300–1305.
93. Xianfeng, Z. Research on Security Assessment and Maintenance Decision of Trains Based on Bayesian Networks. In Proceedings of the 2014 Sixth International Conference on Measuring Technology and Mechatronics Automation, Zhangjiajie, China, 10–11 January 2014; pp. 534–537.
94. Tian, L.; Zhang, S. Real-Time, Multi-Factors-Coupled Early Warning Model in Water Transportation Safety. In Proceedings of the Fourth International Conference on Transportation Engineering, Chengdu, China, 19–20 October 2013; pp. 1726–1733. [CrossRef]
95. Nzoukou, W.; Wang, L.; Jajodia, S.; Singhal, A. A unified framework for measuring a network's mean time-to-compromise. In Proceedings of the 2013 IEEE 32nd International Symposium on Reliable Distributed Systems, Braga, Portugal, 30 September–3 October 2013; pp. 215–224.

96. Shin, J.; Son, H.; Heo, G. Cyber Security Risk Analysis Model Composed with Activity-quality and Architecture Model. In Proceedings of the International Conference on Computer, Networks and Communication Engineering (ICCNCE 2013), Beijing, China, 23–24 May 2013. [CrossRef]
97. Dietzel, S.; Petit, J.; Heijenk, G.; Kargl, F. Graph-Based Metrics for Insider Attack Detection in VANET Multihop Data Dissemination Protocols. *IEEE Trans. Veh. Technol.* **2012**, *62*, 1505–1518. [CrossRef]
98. Zhao, J.; Zheng, W. Study of fault diagnosis method based on fuzzy Bayesian network and application in CTCS-3 train control system. In Proceedings of the 2013 IEEE International Conference on Intelligent Rail Transportation, Beijing, China, 30 August–1 September 2013; pp. 249–254.
99. Hird, J.; Koelle, R.; Kolev, D. Towards mathematical modelling in security risk management in system engineering. In Proceedings of the 2013 Integrated Communications, Navigation and Surveillance Conference (ICNS), Herndon, VA, USA, 22–25 April 2013; pp. 1–13.
100. Eom, H.-S.; Park, G.-Y.; Jang, S.-C.; Son, H.S.; Kang, H.G. V&V-based remaining fault estimation model for safety-critical software of a nuclear power plant. *Ann. Nucl. Energy* **2012**, *51*, 38–49. [CrossRef]
101. Chaze, X.; Bouejla, A.; Napoli, A.; Guarnieri, F. Integration of a bayesian network for response planning in a maritime piracy risk management system. In Proceedings of the 2012 7th International Conference on System of Systems Engineering (SoSE), Genova, Italy, 16–19 July 2012; pp. 137–142.
102. Ming-Zhong, M. Network Security Analysis Based on Graph Theory Model with Neutral Network. In *Future Communication, Computing, Control and Management*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 551–557.
103. Wang, S.; Hong, L.; Chen, X. Vulnerability analysis of interdependent infrastructure systems: A methodological framework. *Phys. A Stat. Mech. Appl.* **2012**, *391*, 3323–3335. [CrossRef]
104. Lu, S.; Wu, D.; Lu, S.; Zhang, H. A Bayesian network model for the Asian Games fire risk assessment. In Proceedings of the International Conference on Information Systems for Crisis Response and Management (ISCRAM), Harbin, China, 19–22 October 2011; pp. 350–355.
105. Cavalheiro, A.C.; Fo, D.J.S.; Andrade, A.; Cardoso, J.R.; Horikawa, O.; Bock, E.; Fonseca, J. Specification of Supervisory Control Systems for Ventricular Assist Devices. *Artif. Organs* **2011**, *35*, 465–470. [CrossRef] [PubMed]
106. Chockalingam, S.; Pieters, W.; Teixeira, A.; van Gelder, P. Bayesian network models in cyber security: A systematic review. In *Secure IT Systems*; Springer: Cham, Switzerland, 2017; pp. 105–122.
107. Contreras-Reyes, J.E.; Quintero, F.O.L.; Wiff, R. Bayesian modeling of individual growth variability using back-calculation: Application to pink cusk-eel (Genypterus blacodes) off Chile. *Ecol. Model.* **2018**, *385*, 145–153. [CrossRef]