Reliability Assessment of IoT-enabled Systems using Fault Trees and Bayesian Networks

Alhassan Abdulhamid, Sohag Kabir, Ibrahim Ghafir, and Ci Lei

School of Computer Science, AI, and Electronics, University of Bradford, Bradford, UK
a.abdulhamid2; s.kabir2; i.ghafir; c.lei1{@bradford.ac.uk}

Abstract. The Internet of Things (IoT) has brought significant advancements in various domains, providing innovative and efficient solutions. However, ensuring the safe design and operation of IoT devices is crucial, as the consequences of component failure can range from system downtime to dangerous operating states. Several methods have been proposed to evaluate the failure behaviours of IoT-based systems, including Fault Tree Analysis (FTA), a methodology adopted from other safety-critical domains. This study integrated FTA and Bayesian Network (BN) models to assess IoT system reliability based on components' reliability data and other statistical information. The integrated model achieved efficient predictive failure analysis, considering combinations of 12 basic events to quantify the overall system's reliability. The model also enables criticality analysis, ranking basic events based on their contributions to system failure and providing a guide for design modification in order to enhance IoT safety. By comparing failure data in FTA and criticality indices obtained using the BN model, the proposed integration offers a probabilistic estimation of IoT system failure and a viable safety guide for designing IoT systems.

Keywords: Internet of Things · System Safety· Reliability Analysis · Fault Tree · Bayesian Network · Risk Assessment

1 Introduction

IoT has become an integral part of modern life with its applications ranging from smart homes, cities and cars to healthcare, agriculture and supply chain [1–4]. Despite the convenience and efficiency that IoT systems offer, the development of safe and dependable systems remains crucial for their acceptance [5]. While state-of-the-art features such as decision-making autonomy have been introduced to IoT systems, they also come with safety concerns. Factors such as physical device failure, cyber attacks, conflicting interactions, and human error can lead to dangerous situations that may cause significant harm to people and the environment [6, 7]. Therefore, it is necessary to adequately assess dependability issues as part of the system development process to ensure that users and the environment are protected from potential hazards of IoT systems.

Fault Tree Analysis (FTA) is a widely used framework for analysing failure behaviours across safety-critical domains such as avionics and automotive. The International Electrotechnical Commission (IEC) cited the FTA method as one of the most important failure analysis methods [8]. FTA uses both qualitative and quantitative approaches to explore the logical relationships between system failures and their underlying causes. For logically connecting different failure events, a FT model usually uses Boolean 'OR' and 'AND' gates. Qualitative analysis of an FT identifies all possible paths leading to an undesired system state, while quantitative analysis helps compute the probability of system-level failure based on the probabilities of component-level failures. While the FTA framework has been successful, it has some limitations in its analysis method. One such limitation is that it assumes statistical independence of component failures [9]. Furthermore, the FTA framework has restricted quantitative analysis features, such as a lack of efficient support for posterior and criticality analyses, among other [10–13].

In real-world scenarios, the statistical independence assumption between basic events may not always hold true, resulting in inaccurate evaluations of failure behaviours between mutually exclusive basic events [10, 14]. To address this issue, the Bayesian network (BN) framework provides an accurate and flexible approach to probabilistic risk assessment, accurately modelling different dependencies between various events, including statistical dependency. BN models are built using Directed Acyclic Graph (DAG) models, and probability estimation is done based on prior knowledge of any of the events, supporting posterior and criticality analyses, among other things [11].

Many studies have proposed the conversion of Fault Trees (FTs) to BNs for a more efficient probabilistic analysis [10–13]. However, most of the conversion frameworks lack a traceability link between the BN model and the system architecture [10]. This traceability link is crucial to limit errors that may have propagated from the FT, support design modification, and facilitate the iterative nature of the system development process [10, 11]. Although translating FT to BN has been attempted in many safety-critical domains, its application in the IoT domain is still in its early stages [3]. Additionally, unlike other mechanical or electronic systems, the failure behaviour of IoT systems is more complicated since safety hazards can result from both component failures and cyber-attacks [7]. This paper proposes combining the FTA and BN frameworks to enable a more rigorous reliability analysis of IoT systems. The effectiveness of this combined approach was validated using a case study of an IoT-enabled Smart Fire Detection and Prevention System (SFDS).

2 Related Works

Various studies have focused on the safety analysis of different systems. For instance, Xing's survey [15] delved into the current issues that affect IoT safety across its layered structure. Similarly, Alhassan *et al.* [3] explored the present state of existing failure analysis frameworks for IoT systems. Their overview provided insight into FT, BN, and other frameworks, highlighting their effectiveness

and limitations. In addition, many studies in other safety-critical domains have adopted the FT framework and its extension to assess the failure analysis of diverse case studies, including mechanical and industrial control systems [16–18, 14]. Although the FTA framework has been successful, it has some limitations in its analysis method. The method assumes statistical independence of component failures, which may not always be the case, resulting in limited quantitative analysis features. Additionally, the process for conducting predictive, diagnostic, and criticality analyses can be cumbersome, which further limits the framework's potential for accurate quantitative failure analysis. [10–13].

The process of reliability analysis based on the FTA method is often oversimplified, with assumptions made that failures are statistically independent and represented through Boolean gates such as *AND* and *OR* [10, 3]. This approach, however, is inadequate for representing complex failure circumstances in IoT systems, given the heterogeneity of components and various failure modes, the statistical dependency between components' failure, the quest for criticality analysis, time-dependent analysis, multiple operating states, and repairability of components after failure. Representing such analysis constraints using the static FT framework can potentially make the reliability assessment process of IoT systems inconsistent, incomplete, cumbersome, or prone to error [10]. Multiple research efforts have begun to address some of these limitations by considering mapping the FT framework to other statically viable models, such as the BN for quantitative failure analysis by mapping dynamic fault trees and temporal fault trees into BNs [12, 13, 10]. The BN safety analysis approach is based on the Bayes theorem and uses probabilistic reasoning to estimate the likelihood of system failure given the various components' failure. Although mapping FT to BN is still in its infancy in the IoT domain, it has the potential to bring numerous benefits to IoT safety analysis. Previous studies have proposed translating the FT to BN for quantitative safety analysis and illustrating various events and logic gates mapped to corresponding nodes in the BN [11, 10, 12, 13].

3 Proposed System Design and Fault Tree Generation

The proposed system is a hypothetical IoT-based Smart Fire Detection System (SFDS) that employs intelligent and smart components to detect fire situations, alert the user, and activate intelligent fire control mechanisms in a smart home. Fig. 1 shows a high-level overview of the system.

Under normal operating conditions, the system monitors various parameters that constitute fire hazards at home. The system uses a temperature sensor (TS) and a smoke sensor (SS) for monitoring. The TS monitors the temperature, while the SS monitors gas particles that are constituents of the fire situation. The TS and SS continuously sense the respective parameters and report them to the IoT smart hub (SH) for further processing. Based on the monitoring knowledge, the system establishes the likelihood of a fire hazard. The communication between the sensors and the IoT gateway takes place via a wireless medium. The two sensors are powered by a battery, while the SH is connected to the main supply of the house. The intelligent hub system processes the sensors' information based on

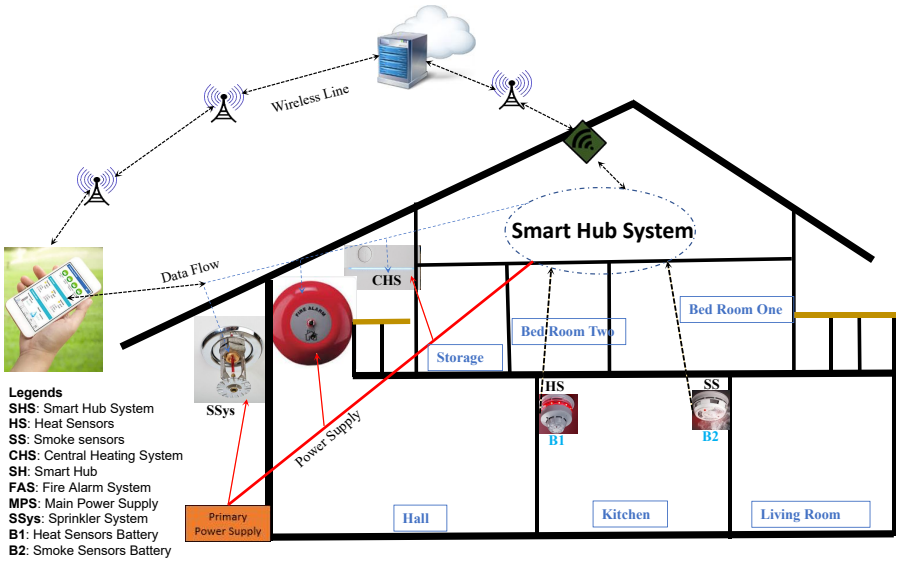

Fig. 1. Case Study of IoT-based System

predefined thresholds from the two sensor readings and determines the likelihood of a fire incident. Once the likelihood of a fire incident has been detected, the Hub passes the information via the cloud to the user's mobile IoT application.

The actuation process involves two steps. Firstly, the Hub is responsible for activating various actions such as turning ON/OFF the alarm system, sprinkler system (SpSys), and central heating system (CHS). Secondly, remote users can also activate these actions using their mobile IoT application. If the local mechanisms fail to extinguish the fire, the user can inform the fire service department for assistance. However, this study assumes that the fire elements, after being detected and processed, will be quenched by any of the three actuation processes. Once the user is notified of the situation, they can use appropriate firefighting equipment in the house or call additional support from the fire service department. The proposed IoT design does not cover additional support beyond this, and hence, it is not included as part of the failure analysis of the IoT system.

The failure condition analysed for the system requirements is *"Failure of SFDS to carry out its expected functions over a specified mission time "*. This failure condition is represented as the top event (TE) in the FTA model in Fig. 2. For the top event to occur, the system should be unable to sense the fire incident, process the information, alert the user, and activate the IoT-based fire-fighting components. The TE is broken down into intermediate events (IEs) and their causes of occurrence serve as the basic events (BEs) of the tree. The various events in the tree are connected based on *AND* and *OR* Boolean Gates in the case of a static tree or other additional gates in other modifications of the FT. To analyse this failure condition, various failure modes of the sub-systems, which are either faults or failures of the components or interaction behaviour, are

modelled to understand their contribution towards the overall failure condition of the system. To conduct a quantitative safety analysis of the system, a mission time (the time frame of operation set for which the reliability is to be determined) is required, and we set 1000 hours for all the BEs. Also, the failure probability of various BEs is populated using data from Table 1 based on the Reliability Data Handbook. In the actual scenario, the design team will provide the statistical data of the components, such as failure rates of physical components and bit error rate for software.

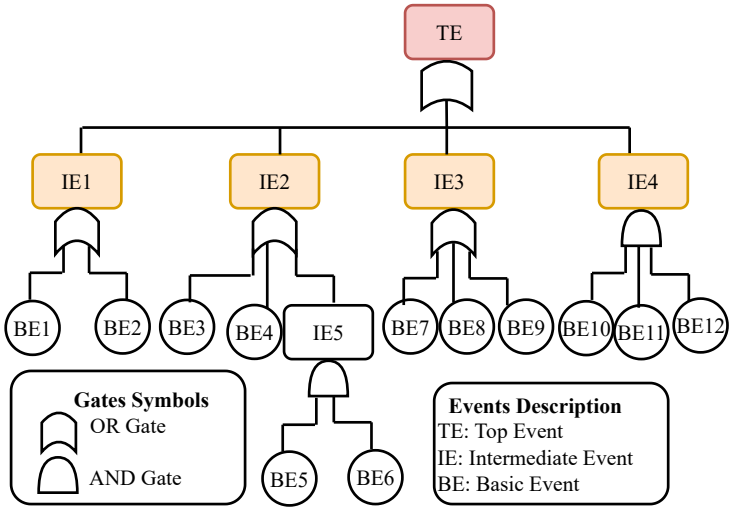

Fig. 2. Fault Tree of the IoT-enabled SFDS

4 Conversion of Fault Tree to Bayesian Network

Mapping the FT of the Safety-Critical SFDS to the BN model involves translating FT events and gates into corresponding BN nodes, as demonstrated in Ref.[19]. Specifically, TEs, IEs, and BEs are mapped to corresponding leaf, intermediate, and root nodes, while the failure probabilities of BEs in the FT are substituted with the prior probabilities of the root node. Boolean logic gates, such as *AND* and *OR*, are represented in the conditional probability tables for the other nodes [10].

The BN model of the system was created using the open-source version of the Genie tool, and the tool automated the quantification estimation seamlessly while reducing the risk of human error caused by a large dataset. The corresponding BEs, IEs, TEs, and logic gates were mapped to corresponding chance and deterministic nodes using the tool. The resulting BN of SFDS' FT is illustrated in Fig. 3.

Table 1. Description of the FT Events and their Failure Data

ID	Description	Failure Probability (in 10^3 hrs)	ID	Description	Failure Probability (in 10^3 hrs)
TE	Failure of Smart Fire Detection and Prevention	N/A	IE1	Failure of Sensing Components	N/A
IE2	Failure of Wireless Communication	N/A	IE3	Failure of Smart Hub Device	N/A
IE4	Failure of Actuation Components	N/A	IE5	Failure of SH Wireless Devices	N/A
BE1	Failure of Heat Sensor	0.007114571	BE2	Failure of Smoke Sensor	0.007114571
BE3	Failure of Communication from HS to SH	0.000669776	BE4	Failure of Communication from SS to SH	0.000709748
BE5	Failure of Communication from SH to Actuation Devices	0.000669776	BE6	Failure of Communication from SH to Cloud	0.001798381
BE7	Smart Hub Physical Failure	0.001349838	BE8	Power Failure to Smart Hub	0.001798381
BE9	Erroneous Reading from Smart Hub	0.000659782	BE10	Sprinkler System Failure	0.008910068
BE11	CHS Failure	0.000659782	BE12	Alarm System Failure	0.001798381

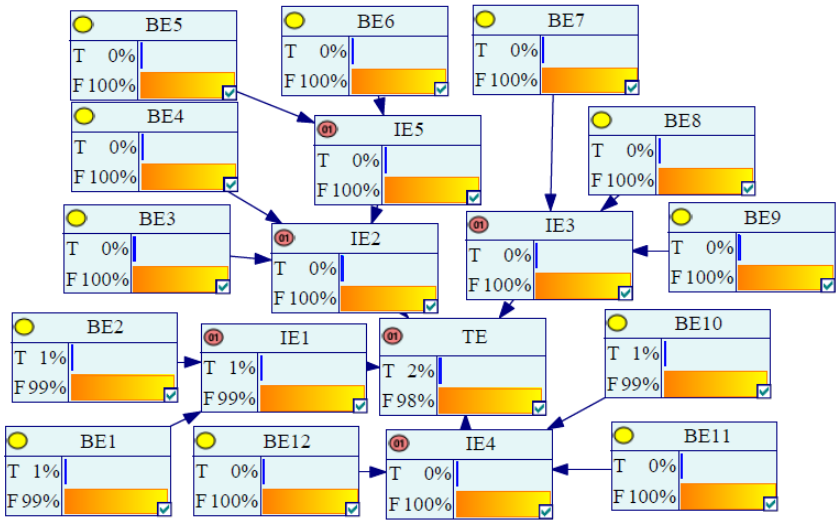

Fig. 3. BN Generated from FT of IoT-enabled SFDS

5 Reliability Analysis

By conducting a quantitative analysis, the reliability of the system design can be predicted based on the probabilities of basic events and their contribution to

the overall probability of system failure. This information can then be used to develop necessary mitigating strategies to reduce the failure of TE and improve the safety threshold of the system to meet the design requirements. The calculation of the TE is built from the aggregated probabilities of basic events. The occurrence probability of a basic event, BE_i, which usually represents a component failure, is calculated using equation (1), provided that the exponentially distributed failure rate (λ) of BE_i and the operating time t are given. In the case of FT, the assumption is that all events in the tree are statistically independent, and the occurrence probabilities of the outcomes of N inputs 'OR' and 'AND' gates are calculated using equations (2) and (3) [20], respectively.

$$Pr(BE_i)(t) = 1 - \exp^{-\lambda t} \tag{1}$$

$$Pr(BE_1 + BE_2 + BE_3 + \cdots + BE_{N-1} + BE_N)\,(t) = 1 - \prod_{i=1}^{N} \left(1 - Pr(BE_i)(t)\right) \tag{2}$$

$$Pr(BE_1 \cdot BE_2 \cdot BE_3 \cdot \ \cdots \ \cdot BE_{N-1} \cdot BE_N)(t) = \prod_{i=1}^{N} Pr(BE_i)(t) \tag{3}$$

In the case of BN model, the statistical independence assumption between basic events is relaxed to enable the evaluation of failure behaviours between mutually exclusive basic events. Accordingly, the BN model of IoT-enabled SFDS developed in Section 4 will be used to conduct predictive failure and criticality analysis to further assess the failure behaviours of the system design.

5.1 Predictive Analysis

The failure behaviour of an IoT-enabled SFDS, as depicted in Fig. 2, has been analysed and translated into a BN model. This analysis has facilitated a predictive failure analysis of the system at different points in time. The analysis employed prior probability tables for the root nodes associated with the component constant failure data, as given in Table 1. Moreover, conditional probability distribution tables were used to represent the failure behaviours of the logic gates between the hierarchy of the nodes. Based on the failure events of its components and the operation time of 1000 hours, the overall failure probability of the SFDS was calculated. The findings indicate that the proposed IoT system under analysis has a failure probability of 0.019283611 and 0.98071639 as its reliability. The system's reliability is approximately 98.07 %. The likelihood of the system failing within 1000 hours of operation is around 1.93 %.

5.2 Criticality Analysis

The criticality analysis is used to examine various safety hazards that may cause system failures and determine the occurrence rate of those hazards. Qualitative analysis has adequately covered the identification of potential hazards through the minimum cut sets (MCS) concept based on the basic events already captured in Table 1. This quantitative research focuses on ranking the BEs to help the design team understand the criticality of the components to the failure of the

proposed design. Among the existing criticality analysis techniques, the Birnbaum Importance Measure (BIM) was used to rank the 12 BEs. The BIM of each BE was estimated by calculating the difference between TE Probabilities given evidence of the BEs as 100 % failed and 0 % failed using BIM equation (4).

$$I_{BE_i}^{BIM} = Pr(TE|Pr(BE_i) = 1) - Pr(TE|Pr(BE_i) = 0) \quad (4)$$

The criticality of the 12 BEs based on the BIM approach is tabulated in Table 2. The TE probabilities given the evidence of the BEs as 100 % failed are represented as X1 whereas the TE probabilities given the evidence of the BEs as 0 % failed are represented as X2. It is essential to note that the criticality analysis conducted confirmed that the criticality of the component is hugely dependent on the logic gates between events more than the failure rate data. For instance, all the basic components have a relatively lower probability of failure, but the criticality of their contribution to the overall system failure varies remarkably. The SFDS has a high chance of failing, given the evidence that either BE1, BE2, BE8, BE7, or BE4 have failed. Therefore, they are the most critical events. This criticality analysis cannot be easily accomplished using the FT framework. Hence, integrating the two approaches provides a better insight into the failure behaviour of IoT systems.

Table 2. Criticality of BEs based on BIM Approach

BEs	**Probability of Failure**	**X1**	**X2**	**BIM**	**Rank**
BE1	0.007114571	1	0.012256237	0.987743763	1
BE2	0.007114571	1	0.012256237	0.987743763	1
BE3	0.000669776	1	0.01862631	0.98137369	5
BE4	0.000709748	1	0.018587055	0.981412945	4
BE5	0.000669776	0.021046133	0.019282429	0.001763704	7
BE6	0.001798381	0.01993929	0.019282429	0.000656861	8
BE7	0.001349838	1	0.017958013	0.982041987	3
BE8	0.001798381	1	0.017516732	0.982483268	2
BE9	0.000659782	1	0.018636124	0.981363876	6
BE10	0.008910068	0.019284764	0.0192836	1.164E-06	11
BE11	0.000659782	0.019299315	0.0192836	1.5715E-05	9
BE12	0.001798381	0.019289365	0.0192836	5.765E-06	10

5.3 Comparison With Other Approaches

As discussed in Section 2, prior research has demonstrated the feasibility of mapping the FTA model to the BN for quantitative failure assessment [11, 10, 12, 13]. However, most of these studies have not linked the BN model to the

system architecture, which creates gaps in traceability. Such gaps can lead to potential errors or inadequate support for iterative processes in system design. Other studies have developed FTA models from the system architecture and mapped FTs to BN, but for a different system model that does not apply to internet-enabled systems [14]. The method outlined in this article presents an integrated approach that incorporates the FTA into the BN model based on IoT system architecture and ensures traceability across different analysis stages of IoT systems. Furthermore, this approach facilitates other quantitative analyses of IoT systems.

6 Conclusion

The utilisation of IoT advancements is progressively becoming more widespread. However, giving priority to their safety and reliability is crucial. Our paper emphasises the significance of safety analysis and recommends adapting established methods like FT and BN to provide quantitative insights into the failure behaviour of an IoT system. This article offers a practical assessment of the IoT system's failure behaviour by integrating the two models. The approach calculated the reliability of IoT-enabled SFDS based on the failure rates of its 12 BEs to be 98.07 %. The approach was also used to establish the ranking of basic events based on their contributions to system failure, serving as a guide for assessing IoT design safety. By comparing failure data in FTA and criticality indices obtained using the BN model, this paper offers a reliable safety guide for designing IoT systems. Moving forward, we plan to automate this process using the Model-Based System Engineering Approach and explore uncertainty analyses and dynamic failure conditions of complex IoT case studies.

References

1. Ştefan, V.K., Otto, P., Alexandrina, P.M.: Considerations regarding the dependability of internet of things. In: 2017 14th International Conference on Engineering of Modern Electric Systems (EMES). pp. 145–148. IEEE (2017)
2. Raza, U., Lomax, J., Ghafir, I., Kharel, R., Whiteside, B.: An IoT and business processes based approach for the monitoring and control of high value-added manufacturing processes. In: Proceedings of the International Conference on Future Networks and Distributed Systems. pp. 1–8 (2017)
3. Abdulhamid, A., Kabir, S., Ghafir, I., Lei, C.: An overview of safety and security analysis frameworks for the internet of things. Electronics **12**(14), 3086 (2023)
4. Hammoudeh, M., Ghafir, I., Bounceur, A., Rawlinson, T.: Continuous monitoring in mission-critical applications using the internet of things and blockchain. In: Proceedings of the 3rd International Conference on Future Networks and Distributed Systems. pp. 1–5 (2019)
5. Abdulhamid, A., Kabir, S., Ghafir, I., Lei, C.: Developing Dependable IoT Systems: Safety Perspective. In: UNIfied Conference of DAMAS, IncoME and TEPEN Conferences. pp. 1–6. Springer (2023)
6. Diab, D.M., AsSadhan, B., Binsalleeh, H., Lambotharan, S., Kyriakopoulos, K.G., Ghafir, I.: Anomaly detection using dynamic time warping. In: 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC). pp. 193–198. IEEE (2019)

7. Abdulhamid, A., Kabir, S., Ghafir, I., Lei, C.: Dependability of the internet of things: Current status and challenges. In: 2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME). pp. 1–6. IEEE (2022)
8. Dale, C., Anderson, T.: Advances in Systems Safety: Proceedings of the Nineteenth Safety-Critical Systems Symposium, Southampton, UK, 8-10th February 2011. Springer Science & Business Media (2010)
9. Abdulhamid, A., Kabir, S., Ghafir, I., Lei, C.: Adaptation of Model Transformation for Safety Analysis of IoT-based Applications. In: The UNIfied Conference of DAMAS, InCoME and TEPEN Conferences. Springer (2023)
10. Kabir, S., Walker, M., Papadopoulos, Y.: Reliability analysis of dynamic systems by translating temporal fault trees into bayesian networks. In: Model-Based Safety and Assessment: 4th International Symposium, IMBSA 2014, Munich, Germany, October 27-29, 2014. Proceedings 4. pp. 96–109. Springer (2014)
11. Abbassi, R., Bhandari, J., Khan, F., Garaniya, V., Chai, S.: Developing a quantitative risk-based methodology for maintenance scheduling using bayesian network. Chemical Engineering Transactions **48**, 235–240 (2016)
12. Boudali, H., Dugan, J.B.: A new bayesian network approach to solve dynamic fault trees. In: Annual Reliability and Maintainability Symposium, 2005. Proceedings. pp. 451–456. IEEE (2005)
13. Montani, S., Portinale, L., Bobbio, A., Varesio, M., Codetta-Raiteri, D.: A tool for automatically translating dynamic fault trees into dynamic bayesian networks. In: RAMS'06. Annual Reliability and Maintainability Symposium, 2006. pp. 434–441. IEEE (2006)
14. Kabir, S., Taleb-Berrouane, M., Papadopoulos, Y.: Dynamic reliability assessment of flare systems by combining fault tree analysis and Bayesian networks. Energy Sources, Part A: Recovery, Utilization, and Environmental Effects **45**(2), 4305–4322 (2023)
15. Xing, L.: Reliability in Internet of Things: Current status and future perspectives. IEEE Internet of Things Journal **7**(8), 6704–6721 (2020)
16. Wongvises, C., Khurat, A., Fall, D., Kashihara, S.: Fault tree analysis-based risk quantification of smart homes. In: 2nd International Conference on Information Technology (INCIT). pp. 1–6. IEEE (2017)
17. Kabir, S., Azad, T., Walker, M., Gheraibia, Y.: Reliability analysis of automated pond oxygen management system. In: 2015 18th International Conference on Computer and Information Technology (ICCIT). pp. 144–149. IEEE (2015)
18. Niloofar, P., Lazarova-Molnar, S.: Fusion of data and expert knowledge for fault tree reliability analysis of cyber-physical systems. In: 2021 5th International Conference on System Reliability and Safety (ICSRS). pp. 92–97. IEEE (2021)
19. Bobbio, A., Portinale, L., Minichino, M., Ciancamerla, E.: Improving the analysis of dependable systems by mapping fault trees into bayesian networks. Reliability Engineering & System Safety **71**(3), 249–260 (2001)
20. Kabir, S.: A fuzzy data-driven reliability analysis for risk assessment and decision making using Temporal Fault Trees. Decision Analytics Journal **8**, 1–12 (2023)