Qualitative Failure Analysis of IoT-enabled Industrial Fire Detection and Prevention System

2023 26th International Conference on Computer and Information Technology (ICCIT)
13-15 December 2023, Cox's Bazar, Bangladesh

Qualitative Failure Analysis of IoT-enabled Industrial Fire Detection and Prevention System

Md Mokhlesur Rahman*, Alhassan Abdulhamid†, Sohag Kabir†
*Department of Computer Science and Engineering, Military Institute of Science and Technology, Bangladesh
†School of Computer Science, AI and Electronics, University of Bradford, UK
Email: mokhles@cse.mist.ac.bd, a.abdulhamid2@bradford.ac.uk, s.kabir2@bradford.ac.uk

***Abstract*—The Internet of Things (IoT) has improved our lives through various applications such as home automation, smart city monitoring, environmental monitoring, intelligent farming, and a host of others. IoT is increasingly being used for environmental monitoring to prevent fire incidents and other environmental hazards. However, for IoT systems to function effectively in preventing fire incidents, they must operate in a safe, reliable, and dependable manner. The intelligent sensors and devices that constitute the system are prone to different types of failures, which can lead to unsafe or dangerous conditions. Failure of a fire prevention system can pose significant risks to Health, Safety, and the Environment (HSE). To address these concerns, it is essential to understand how component failures can contribute to the overall system failure. This paper adopts Fault Tree Analysis, a widely used framework for failure behaviour analysis in other safety-critical domains, to qualitatively analyse an intelligent fire detection system in an industrial setting. The analysis outlines the ways in which the system can fail and the necessary prevention mechanism to guard against undesired system failure.**

***Index Terms*—Internet of Things, smart fire control system, system failure analysis, fault tree analysis**

I. Introduction

The rapid development and use of Internet of Things (IoT) applications and systems have cut across areas such as home automation, smart city monitoring, environmental monitoring, and intelligent farming [1]. In environmental monitoring, IoT is increasingly used to safeguard the environment from the hazard of fire incidents through an intelligent-controlled fire detection and extinguishing system. To prevent fire incidents, the first step is to obtain an early warning and prompt response to a fire outbreak [2]. An IoT-enabled fire prevention system provides quick and accurate detection and restriction to fire hazards.

Frequent fire incidents constitute a significant hazard, causing huge loss of life and property. They also harm social and environmental affairs and result in colossal financial losses [3]. Bangladesh has unfortunately experienced several significant fire incidents over the years. According to a report released by Bangladesh Fire Service and Civil Defence Authority, at least 24,102 fire incidents occurred in 2022, killing around 98 persons, including 13 firefighters [4]. In the year 2023, some of the horrendous fire incidents recorded are: fire at Bongo Bazar clothing market in Dhaka on 4 April [5], Cox's Bazar Rohingya camp on 19 April [6], garment factory at Gazipur on 1 May [7], garment factory in Narayanganj BSCIC industrial area on 24 July [8]. Going by these unpleasant records of fire incidents and the untoward harm to HSE and enormous financial loss involved, an effective prevention mechanism such as IoT-enabled systems, can significantly help Bangladesh to curtail fire incidents.

Albeit the use of IoT for intelligent fire protection systems has modernised various fire fighting activities, they have also brought forth new difficulties that could negatively undercut the advantages they provide. The complexity that results from the expanding use of information and communication technology to link the offline and online worlds makes it more challenging to establish secure and reliable systems [9]. Moreover, the various components that compose the system can fail for various reasons. For instance, hardware components can be damaged or fail, security-induced problems, configuration and update challenges, conflicting interactions between components and many others can affect the system's dependability [10]. Accordingly, it is essential to evaluate how such systems function and how they could malfunction to increase their assurance in meeting their expected reliability.

System safety analysis is one of the non-functional analysis and verification processes in a system development life cycle (SDLC) to identify potential issues that could cause a system to fail to determine whether a system can be safely operated [11]. There are several methodologies for conducting safety analysis, and the prominent ones include Fault Tree Analysis (FTA), Failure Mode Effects Analysis, and their extensions. Notably, FTA is at the forefront of system safety analysis [12]. The approach graphically models the overall undesired event (the IoT system failure) based on logical relationships between the various component failures and their underlying causes. Going by the methodological and coherent approach of the FT framework, it is a viable option for systematic failure analysis to design safe and reliable IoT-based systems [10]. Accordingly, this article will provide a brief qualitative failure analysis for IoT-based fire prevention systems based on the application of the FT framework. The paper presented the failure analysis result of the system, showing how it can fail using the graphical tree approach and generated minimum cut sets (MCSs) from the tree. This shows the various ways the system fails due to the combination of different basic failures.

The rest of the paper is organised as follows. Section II provides a conceptual overview and related research. Section III gave a detailed system design and qualitative failure analysis. Finally, Section IV summarises the key aspects and suggests future research directions.

979-8-3503-5901-5/23/$31.00

II. Conceptual Overview and Related Works

A. IoT-Based Fire Prevention Systems

The IoT concept has enabled smart devices (e.g. sensors, actuators) to connect to the Internet and interact with each other or central controllers to exchange information using advanced communication technologies with minimal human intervention [12]. The rapid growth of IoT and other emerging technologies have opened avenues for their utilisation in monitoring and actuation activities in various domains. Fire detection and prevention systems are one such domain where the monitoring capability of IoT devices has been successfully applied to develop many intelligent applications. In the fire prevention system field, at home, in offices or in industrial settings, intelligent sensors are deployed to monitor the smoke particles, heat and other parameters responsible for the fire.

Ready Made Garments (RMG) products accounted for 81.82% of Bangladesh's total export earnings in 2021-22 [13]. Realising the importance of the RMG sector in the national economy, Bangladesh Govt. has taken adequate measures to reduce safety hazards in the industries. As a result, by now, among 4000+ garment industries, 197 industries have obtained Leadership in Energy and Environmental Design (LEED) certification from the U.S. Green Building Council, and 500 more factories are in the process of getting LEED certification [14]. Many of these factories have employed IoT-Based Fire Prevention Systems to take fast and appropriate measures to mitigate fire incidents.

B. Fault Tree Analysis Technique

FTA is a commonly used method to assess the safety of a system design by examining its failure behaviour. The approach uses a tree-like structure containing a hierarchy of events and gate symbols to represent the system's failure scenario [1]. The analysis begins by defining the top event (TE), which represents the overall system failure, and its connection to the intermediate events (IEs) at the next level, which are the direct causes of the TE. The tree is further broken down into basic events (BEs), representing component-level failures that cannot be further divided. Gate symbols connect the events in the tree, with the simplest tree using Boolean AND and OR logic gates to show how IEs and BEs contribute to the TE [15]. The given Fig. 2 represents a typical instance of FTA. The TE showcased in the diagram is the Failure of Fire Prevention System, while the other IEs, BEs, and logic gates are aptly depicted.

FTA can conduct both qualitative and quantitative safety analyses of the system. The qualitative analysis determines the MCSs, which are the smallest combinations of failure events that can cause a system failure [16]. Quantitative analysis is an essential process that predicts the probability of system failure by examining the failure rates and probabilities of its components and logic gates [17]. By determining the overall system-level failure, this analysis enables the establishment of minimum safety thresholds and ensures compliance.

C. Related Works

To conceptualise an IoT-enabled intelligent fire detection and prevention system in an industrial environment, an extensive literature review was conducted. Some of the notable research works are narrated further. Mukherjee *et al.* [18] implemented an intelligent fire detection system integrating wireless sensor networks, artificial intelligence (AI), and IoT devices. Thereby mitigating fire or other environmental hazards to save human lives and property. Mekni *et al.* [19] proposed a low-cost innovative system to monitor temperature, humidity, smoke, etc., along with the number of people staying in a building and alert the homeowner using a buzzer, red light and messaging system if collected parameter crosses a defined threshold. Besides using flame, smoke, temperature and humidity sensors, Khalid *et al.* [20] used light intensity sensors to detect early fire incidents. To develop the quality of the indoor environment vis-a-vis monitoring accidental fires and take preventive measures, Mahbub *et al.* [21] developed an embedded system using HTTP protocol-based real-time monitoring using smartphones or PCs. Early detection of forest fire initiation is a prime requirement to stop it from spreading into a big area [22]. Surveillance systems using sensors with IoT devices are used to identify hazardous environmental issues in extensive forests. Cui [23] proposed a deep learning model using a Convolution Neural Network (CNN) to monitor forests, identify abnormalities, and take precautionary measures. Huang *et al*. [24] proposed a Wavelet-CNN method using 2D Haar transform to extract spectral features from fire images taken by using conventional CCTV cameras. Tianxiang and Hou [25] proposed an intelligent fire detection system using narrow-band IoT (NB-IoT) and LoRa (Long Range) modulation techniques. Thereby, implementing a LoRaWAN wireless smoke sensor platform that operates on ultra-low power-consuming end devices, long-range gateways and high-capacity network servers.

Conversely, numerous studies are also ongoing in areas of failure analysis over the years and across a variety of other systems and domains. A significant number of research works in the current literature suggest various methods for failure analysis of diverse systems based on the compositional structures and behaviours of those systems. For instance, in 1980, the US Military proposed Failure Mode and Effect Analysis (FMEA) for the methodical identification of probable failures in a system along with their causes and effects [26]. Besides, system failure analysis using the Markov Chain Analysis (MCA) framework was developed as a formal graphical and mathematical modelling approach for specifying and analysing the behaviour of systems based on the exponential distribution of failure [27]. Similar to this, the Bayesian Network (BN), a probabilistic reliability modelling technique, was created on the basis of the Bayes theorem to estimate the likelihood of system failure using probabilistic reasoning under unknown situations [26]. While these current approaches are impressive in terms of failure analysis, the International Electrotechnical Commission (IEC) cited the FTA method as being one of the most important failure analysis methods [28].

FTA was developed in 1962 by Bell Phone Laboratories and used for the evaluation of failure behaviours of the launch control system of LGM-30 Minuteman [16]. Since then, it has taken its place as a prevalent method for analysing a safety critical system and its use has extended to several other domains. Though the use of FTA is increasing rapidly in other high-consequence domains, its use in IoT applications is still in its early stages. Among the existing literature FTA framework has been used in the safety analysis of smart homes [29], smart agriculture [15], smart traffic management system [30], smart power system [31]. [32] proposed a dependability evaluation tool for IoT applications where a fault tree has been used to model the failure behaviour of different components in an IoT system. In [29], a fault tree has been used for security risk analysis on a light bulb system in an IoT-enabled smart home environment. While it is evident from the existing studies that FT is a viable safety analysis framework, its applicability in IoT-enabled fire detection systems is yet to be established. To this end, it is worthwhile to apply the FTA framework to our IoT-enabled fire detection system as a case study in order to conduct a comprehensive safety analysis of the system.

III. Proposed System Design and Analysis

A. System model and description

Fig. 1 shows the architecture of a hypothetical IoT-based Smart Fire Alerting and Extinguishing System (SFAES) in an industrial setting. Using this system, the safety department can remotely monitor the status of a fire incident in the Company, and various fire extinguishing mechanisms can be activated whenever needed without being physically present on the company premises.

The system will monitor different parameters constituting a fire in a typical operating condition. Based on the monitoring knowledge, it will decide when and how the fire can be quenched. Basically, the system is made of three sensors which are responsible for continuous monitoring of the environment and sending data to the Smart Hub System (SHS). SHS performs a 2-out-of-3 voting to determine the accurate value. Based on this value, SHS determines whether there is a fire using a predefined set of rules. If a fire is detected, SHS will turn on the sprinkler system, blow the siren, send an SMS, and send a notification to the users' mobile application. After receiving the SMS or after listening to the siren, users can notify the Firefighting department and will try to stop the fire manually by utilising the Fire Extinguishing System. Using the mobile application, users can monitor the sprinkler system's status (ON/OFF). If the sprinkler system is OFF, it can be turned on by a remote signal from the mobile app. Using the mobile app, users can also notify the firefighting department.

Going by the IoT layered architecture, at the perception layer of the system, there are three battery-enabled sensors: temperature sensors, smoke detectors and carbon monoxide detectors. These sensors are placed in various parts of the industrial layout to detect the presence of heat, smoke, and flames for further processing. From a design perspective, at least two of the three sensors must function well for detection. The sensors via wireless interface transmit their sensing data to the Hub at the transportation layer.

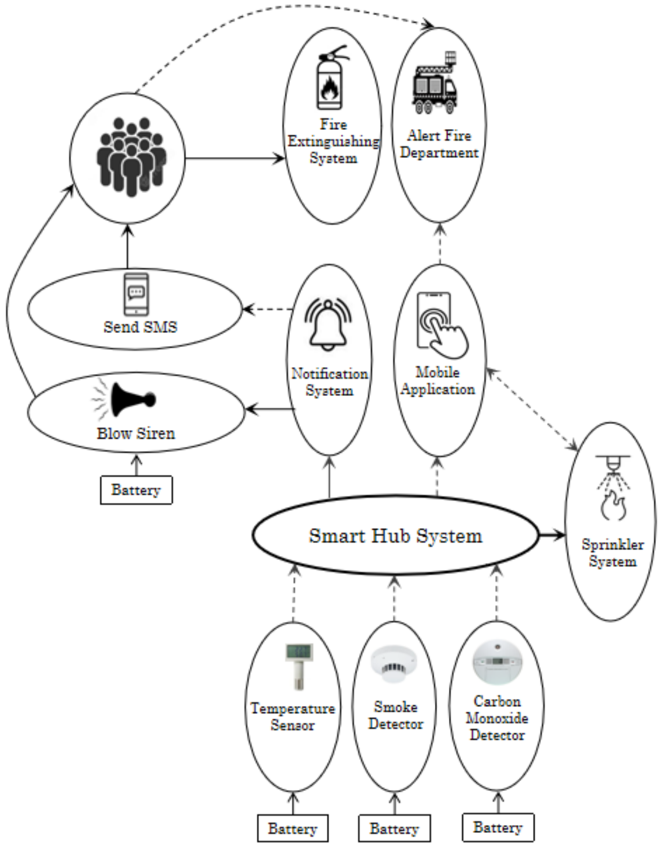

Fig. 1: Architecture of an IoT-based Industrial Fire Detection and Prevention System

The intelligent Hub resides in the data-processing layer. The hub stores and analyses data from the various sensors in the system. The transmitted data can be used to identify patterns and trends, which can help the system optimise its performance and detect potential fires before they become a significant threat. At the Hub, data processing is based on predefined rules to detect fire incidents. Once the heat and flame reading received from the perception layer reaches a threshold set, the system will assume the likelihood of a fire incident on the premises. Accordingly, a notification system will be activated, which involves sending SMS messages via the SMS API module, one of the widely used event-driven SMS frameworks. Other activities include activating the siren system and alerting the operator's smartphone's IoT application. Fire prevention mechanisms are also activated besides the intelligent Hub's notification system. This process involves activating sprinkler systems, dedicated smart extinguishers and notification to the fire department of the Company. As a redundancy mechanism in the system, these fire prevention mechanisms can also be activated from the operator's mobile application. The smart IoT application can be used to view the status of various sensors, control the sprinkler system, and receive alerts when a fire is detected. The smartphone application can also be used to monitor the fire hazard in the company remotely.

B. *Failure Analysis of the Proposed System*

As mentioned before, depending on the role(s) of a component in the system and its interactions with other components, the failure of the component can have an enormous impact on the failure of the system. The qualitative failure behaviour analysis aims to identify the potential causes of the system failure based on its components and their configuration. For failure behaviour analysis, we have identified *"the failure of the system to prevent fire incident when needed"* as the system's overall failure condition. Considering this event as the top event for the fault tree, we have developed the fault tree shown in Fig. 2. For convenient and manageability the tree has corresponding transfer symbols 1 and 2 as shown in Figs. 3 and 4, respectively.

These FTs contain 41 unique and essential events, which are the root causes that can contribute to the system failure. These root causes are either internal failures of the devices or the failure of the communication between devices. Tables I and II show the ID and the description of all the events of the FT.

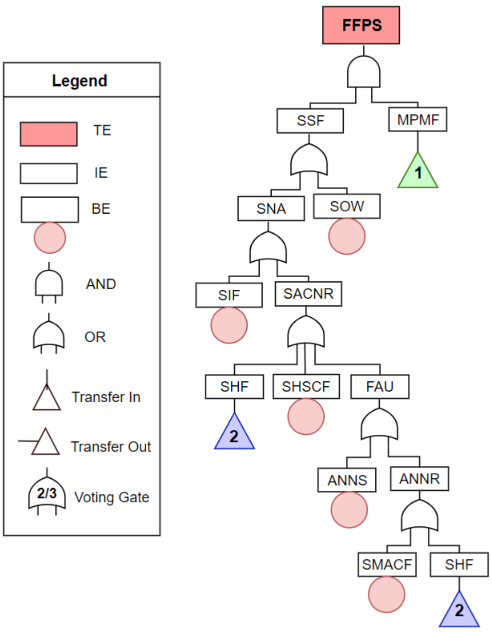

Fig. 2: Fault Tree-1

The concept of minimal cut sets is a fundamental approach in risk and reliability analysis. It refers to a group of sets comprising the smallest possible combinations of basic events, which, when occurring, lead to the occurrence of the top event [12]. These sets represent all the possible ways in which the BEs cause the TE. Once the MCSs have been identified, developing effective risk management strategies to mitigate them is viable. Based on the qualitative analysis of the fault tree generated in Figs. 2, 3, 4, and 5, various MCSs were generated using framework explained in Ref. [16]. In the logical expressions of the MCSs, the symbol '.' represents a logical AND operation. Out of these 41 MCSs, 2 MCSs are of order 1, 12 are of order 2, 18 are of order 3 and 9 are of order 4. The order of an MCS represents the number of primary

TABLE I: ID and Description of the events of the fault trees

ID	Description
FFPR	Failure of Fire Prevention System
SSF	Sprinkler System Failure
MPMF	Manual Prevention Mechanism Failure
SNA	Sprinkler Not Activated
SIF	Sprinkler Internal Failure
SACNR	Sprinkler Activation Command Not Received
SHF	Smart Hub Failure
SHSCF	Smart Hub to Sprinkler Communication Failure
FAU	Failure of Apps User
ANNS	Apps Notification Not Seen
ANNR	Apps Notification Not Received
SMACF	Smart Hub to Mobile Apps Communication failure
FESF	Fire Extinguishing System Failure
FENU	Fire Extinguisher Not Used
UENK	Use of Extinguisher Not Known
NUFE	Neglect to Use Fire Extinguisher
AON	Absence of Notification
FEF	Fire Extinguisher Failure
FDF	Fire Department Failure
FDNN	Fire Department Not Notified
FGP	Failure of General People
PDNFD	People Didnot Notify Fire Dept
ANNS	Apps Notification Not Seen
ANNR	Apps Notification Not Received
SMACF	Smart Hub to Mobile Apps Communication failure
FDDTU	Fire Department Didnot Turn Up
FDRL	Fire Department Reached Late
SHIF	Smart Hub Internal Failure
SDNR	Sensor Data Not Received
SSHCF	Sensor to Smart Hub Communication Failure
SF	Sensor Failure
TSF	Temperature Sensor Failure
TSIF	Temperature Sensor Internal Failure
TSBF	Temperature Sensor Battery Failure
SMSF	Smoke Sensor Failure
SSIF	Smoke Sensor Internal Failure
SSBF	Smoke Sensor Battery Failure
CMDF	Carbon Monoxide Detector Failure
SNG	SMS Not Generated
NSIF	Notification System Internal Failure

TABLE II: ID and Description of the events of the fault trees (continued)

ID	Description
NSACNR	Notification System Activation Command Not Received
SHNSCF	Smart Hub to Notification System Communication Failure
SNB	Siren Not Blown
SOO	Siren Out of Order
SBF	Siren Battery Failure
SINA	Siren Not Activated
NMSCF	Notification Module to Siren Communication Failure
NSIF	Notification System Internal Failure
MNF	Mobile Network Failure

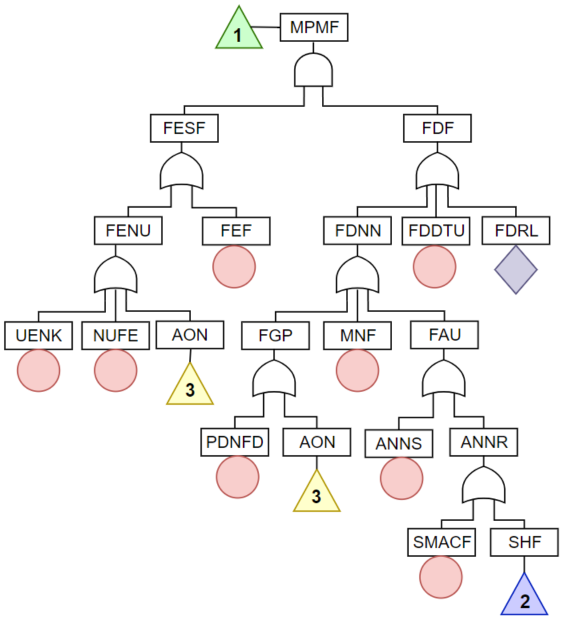

Fig. 3: Fault Tree-2

events contributing to that MCS. If all the essential events are equally probable to occur, then the higher the order of an MCS, the lower the criticality of that MCS is. Therefore, the first-order MCSs such as 'Smart Hub Internal Failure (SHIF)" and "Sensor to Smart Hub Communication Failure (SSHCF)" are the most critical in this example. Therefore, actions should be taken to reduce the likelihood of these events. After that, the events related to order 2 MCSs should be handled.

A list of all the MCSs in the system tree is available below, and their corresponding event interpretations can be found in the tables I and II.

```
1. SHIF;2. SSHCF;3. TSIF.SSIF;4. TSBF.SSIF
5. TSIF.SSBF; 6. TSBF.SSBF; 7. TSIF.CMDIF;
8. TSBF.CMDIF;9. TSIF.CMDBF;10. TSBF.CMDBF
11. SSIF.CMDIF;12.SSBF.CMDIF;13.SSIF.CMDBF
```

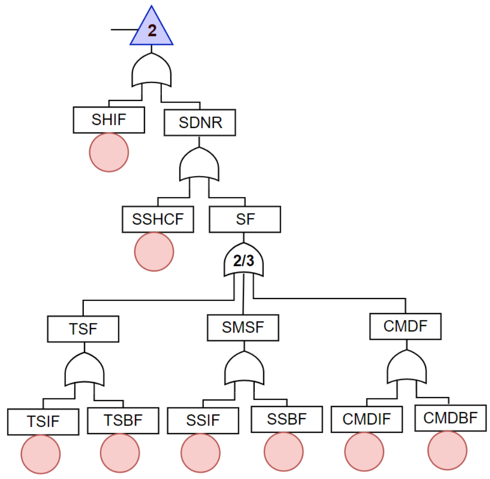

Fig. 4: Fault Tree-3

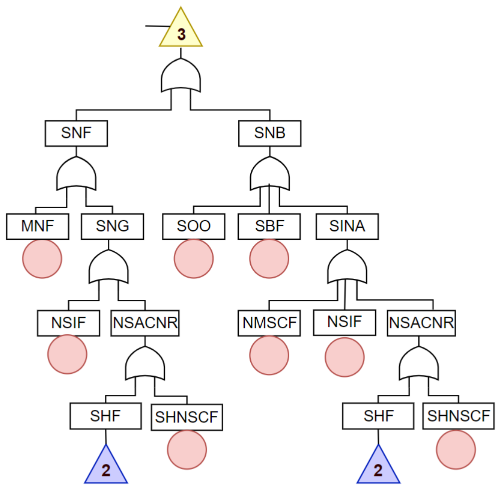

Fig. 5: Fault Tree-4

```
14. SSBF.CMDIF; 15. SHSCF.UENK.FDDTU;
16. SIF.UENK.FDDTU; 17. SOW.UENK.FDDTU;
18. SHSCF.FEF.FDDTU;19. SIF.FEF.FDDTU;
20. SOW.FEF.FDDTU; 21. SHSCF.MNF.SOO;
22. SIF.MNF.SOO;23. SOW.MNF.SOO;
24. SHSCF.MNF.SBF; 25. SIF.MNF.SBF;
26. SOW.MNF.SBF; 27. SHSCF.MNF.NMSCF;
28. SIF.MNF.NMSCF; 29. SOW.MNF.NMSCF;
30. SHSCF.SMACF.SHNSCF;31.SIF.SMACF.SHNSCF;
32.SOW.SMACF.SHNSCF; 33.SHSCF.MNF.NUFE.PDNFD;
34.SIF.MNF.NUFE.PDNFD;35.SOW.MNF.NUFE.PDNFD;
36.SHSCF.SMACF.NUFE.PDNFD;
37.SIF.SMACF.NUFE.PDNFD;
38.SOW.SMACF.NUFE.PDNFD;
39.SHSCF.ANNS.NUFE.PDNFD;
40.SIF.ANNS.NUFE.PDNFD;
41.SOW.ANNS.NUFE.PDNFD.
```

IV. Conclusion

Accidental fires occurring in an industrial setup, residential areas, or forest causes colossal loss of lives, property and the environment. Countries like Bangladesh, dependent on the RGM sector for earning foreign currencies, have seen several heart-rending fire incidents in garment industries for decades. It has recently followed in the footsteps of other developed and developing countries in adopting technology-driven intelligent fire detection and mitigation systems, vowing to make its garment factories green. Research efforts in developing analysis and verification frameworks to support fire detection and prevention systems are novel efforts to protect precious lives, property and the environment. This article shows the qualitative failure behaviour analysis of a tentative workable and implementable IoT-enabled industrial fire detection and prevention system. The analysis used the FTA framework, one of the most widely used techniques in other critical domains. The developed fault tree displays different component failures as essential events, and how these failures can propagate to cause the system failure is represented. As a result of this analysis, individuals can identify a range of different causes for the failure of the system and can take action accordingly to prevent failures. To keep the analysis generic, we considered the system, its components and their failure behaviours at the abstract level. However, for any specific system, one can consider strictly used components and model their behaviour in more detail. For illustration, we have considered the inability of the system to stop fire in an industrial setting when needed as the failure condition of the system. The current study is limited only to qualitative analysis; in the future, quantitative analysis can be performed, given the failure rate or probability of the components.

References

[1] A. Abdulhamid, S. Kabir, I. Ghafir, and C. Lei, "Dependability of the internet of things: Current status and challenges," in *2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*. IEEE, 2022, pp. 1–6.

[2] V. ramana Karumanchi, S. H. Raju, S. Kavitha, V. L. Lalitha, and S. V. Krishna, "Fully smart fire detection and prevention in the authorized forests," in *2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS)*. IEEE, 2021, pp. 573–579.

[3] M. I. Mobin, M. Abid-Ar-Rafi, M. N. Islam, and M. R. Hasan, "An intelligent fire detection and mitigation system safe from fire (sff)," *Int. J. Comput. Appl*, vol. 133, no. 6, pp. 1–7, 2016.

[4] The Daily Star, "Bangladesh saw 24,102 fire incidents last year," 2023. [Online]. Available: https://www.thedailystar.net/news/bangladesh/accidents-fires/news/bangladesh-saw-24102-fire-incidents-last-year-3240521

[5] Al Jazeera, "Massive fire guts popular clothing market in bangladesh capital," 2023. [Online]. Available: https://www.aljazeera.com/news/2023/4/4/major-fire-at-popular-clothing-market-in-bangladesh-capital

[6] Tribune Desk, "Fire at Rohingya camp razes dozens of shelters," 2023. [Online]. Available: https://www.dhakatribune.com/bangladesh/nation/283582/fire-at-rohingya-camp-razes-dozens-of-shelters

[7] Star Report, "18 staffers of gazipur garment factory burnt in fire caused by gas leak," 2023. [Online]. Available: https://www.thedailystar.net/news/bangladesh/accidents-fires/news/18-staffers-gazipur-garment-factory-burnt-fire-caused-gas-leak-3308756

[8] New Age Report, "Fire at garment factory in Narayanganj BSCIC industrial area doused," 2023. [Online]. Available: https://www.newagebd.net/article/207706/fire-at-garment-factory-in-narayanganj-bscic-industrial-area-doused

[9] L. Xing, "Reliability in Internet of Things: Current Status and Future Perspectives," *IEEE Internet of Things Journal*, 2020.

[10] S. Kabir, P. Gope, and S. P. Mohanty, "A Security-enabled Safety Assurance Framework for IoT-based Smart Homes," *IEEE Transactions on Industry Applications*, vol. 59, no. 1, pp. 6–14, 2022.

[11] A. Abdulhamid, S. Kabir, I. Ghafir, and C. Lei, "Developing Dependable IoT Systems: Safety Perspective," in *UNIfied Conference of DAMAS, IncoME and TEPEN Conferences*. Springer, 2023, pp. 1–6.

[12] ——, "An overview of safety and security analysis frameworks for the internet of things," *Electronics*, vol. 12, no. 14, p. 3086, 2023.

[13] Daily Sun, "Bangladesh regains 2nd position in rmg exports," 2022. [Online]. Available: https://www.daily-sun.com/printversion/details/659836/Bangladesh-regains-2nd-position-in-RMG-exports

[14] BGMEA. (2023) Bangladesh home to world's highest number of green garment factories. [Online]. Available: https://www.bgmea.com.bd/page/Sustainability_Environment

[15] S. Kabir, T. Azad, M. Walker, and Y. Gheraibia, "Reliability analysis of automated pond oxygen management system," in *2015 18th International Conference on Computer and Information Technology (ICCIT)*. IEEE, 2015, pp. 144–149.

[16] S. Kabir, "An overview of fault tree analysis and its application in model based dependability analysis," *Expert Systems with Applications*, vol. 77, pp. 114–135, 2017.

[17] A. Abdulhamid, S. Kabir, I. Ghafir, and C. Lei, "Adaptation of Model Transformation for Safety Analysis of IoT-based Applications," in *The UNIfied Conference of DAMAS, InCoME and TEPEN Conferences*, 2023, pp. 1–6.

[18] A. Mukherjee, S. K. Shome, and P. Bhattacharjee, "Survey on internet of things based intelligent wireless sensor network for fire detection system in building," *Communication and Control for Robotic Systems*, pp. 193–200, 2022.

[19] S. K. Mekni, "Design and implementation of a smart fire detection and monitoring system based on iot," in *2022 4th International Conference on Applied Automation and Industrial Diagnostics (ICAAID)*, vol. 1. IEEE, 2022, pp. 1–5.

[20] W. Khalid, A. Sattar, M. A. Qureshi, A. Amin, M. A. Malik, and K. HUSSAIN, "A smart wireless sensor network node for fire detection," *Turkish Journal of Electrical Engineering and Computer Sciences*, vol. 27, no. 4, pp. 2541–2556, 2019.

[21] M. Mahbub, M. M. Hossain, and M. S. A. Gazi, "Cloud-enabled iot-based embedded system and software for intelligent indoor lighting, ventilation, early stage fire detection and prevention," *Computer Networks*, vol. 184, p. 107673, 2021.

[22] K. Mehta, S. Sharma, and D. Mishra, "Internet-of-things enabled forest fire detection system," in *2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2021, pp. 20–23.

[23] F. Cui, "Deployment and integration of smart sensors with iot devices detecting fire disasters in huge forest environment," *Computer Communications*, vol. 150, pp. 818–827, 2020.

[24] L. Huang, G. Liu, Y. Wang, H. Yuan, and T. Chen, "Fire detection in video surveillances using convolutional neural networks and wavelet transform," *Engineering Applications of Artificial Intelligence*, vol. 110, p. 104737, 2022.

[25] T. Li and P. Hou, "Application of nb-iot in intelligent fire protection system," in *2019 International Conference on Virtual Reality and Intelligent Systems (ICVRIS)*, 2019, pp. 203–206.

[26] S. Kabir and Y. Papadopoulos, "Applications of bayesian networks and petri nets in safety, reliability, and risk assessments: A review," *Safety science*, vol. 115, pp. 154–175, 2019.

[27] S. Kabir, K. Aslansefat, I. Sorokos, Y. Papadopoulos, and S. Konur, "A hybrid modular approach for dynamic fault tree analysis," *IEEE Access*, vol. 8, pp. 97 175–97 188, 2020.

[28] C. Dale and T. Anderson, *Advances in Systems Safety: Proceedings of the Nineteenth Safety-Critical Systems Symposium, Southampton, UK, 8-10th February 2011*. Springer Science & Business Media, 2010.

[29] C. Wongvises, A. Khurat, D. Fall, and S. Kashihara, "Fault tree analysis-based risk quantification of smart homes," in *2017 2nd International Conference on Information Technology (INCIT)*. IEEE, 2017, pp. 1–6.

[30] C. Liu and L. Ke, "Cloud assisted internet of things intelligent transportation system and the traffic control system in the smart city," *Journal of Control and Decision*, vol. 10, no. 2, pp. 174–187, 2023.

[31] M. O. Qays, M. M. Ahmed, M. Parvez Mahmud, A. Abu-Siada, S. Muyeen, M. L. Hossain, F. Yasmin, and M. M. Rahman, "Monitoring of renewable energy systems by iot-aided scada system," *Energy Science & Engineering*, vol. 10, no. 6, pp. 1874–1885, 2022.

[32] I. Silva, R. Leandro, D. Macedo, and L. A. Guedes, "A dependability evaluation tool for the internet of things," *Computers & Electrical Engineering*, vol. 39, no. 7, pp. 2005–2018, 2013.