Failure analysis of IoT-based smart agriculture system: towards sustainable food security

Failure Analysis of IoT-based Smart Agriculture System: Towards Sustainable Food Security

Md Mokhlesur Rahman*, Alhassan Abdulhamid†, Sohag Kabir†, and Prosanta Gope‡

*Department of Computer Science and Engineering, Military Institute of Science and Technology, Bangladesh
†School of Computer Science, AI and Electronics, University of Bradford, UK
‡Department of Computer Science, University of Sheffield, UK
Email: mokhles@cse.mist.ac.bd, a.abdulhamid2@bradford.ac.uk, s.kabir2@bradford.ac.uk, p.gope@sheffield.ac.uk

***Abstract*—Internet of Things (IoT)-based smart agriculture systems are increasingly being used to improve agricultural yield. IoT devices used for agricultural monitoring are often deployed in outdoor environments in remote areas. Due to the exposure to harsh environments and the nature of deployment, sensors and other devices are susceptible to an increased rate of failure, which can take a system to unsafe and dangerous states. Failure of a smart agriculture system can cause significant harm to nature and people and reduce agricultural production. To address the concerns associated with the failure of the system, it is necessary to understand how the failures of the components of a system can contribute to causing the overall system failure. This paper adopts Fault Tree Analysis, a widely used framework for failure behaviour analysis in other safety-critical domains, to demonstrate the qualitative failure analysis of smart irrigation systems based on the components' failure.**

***Index Terms*—Internet of Things, smart agriculture, failure analysis, fault tree analysis, sustainability**

I. Introduction

Agriculture plays an important role in the survival of humankind since it produces most of the food and other raw materials. It contributes significantly to a country's economy while employing a large population. The global population is estimated to reach 9.8 billion by 2050 [1]. Therefore, agricultural yield should be increased considerably to ensure food security for the growing population. Albeit the world continues to champion various initiatives for food security, cultivable land in many parts of the world is decreasing faster for the habitation of a growing population, urbanisation and industrialisation. For instance, Bangladesh being an example of a densely populated country lost 2.41 million acres of cultivable land within the year from 2008 to 2019 which indicates a reduction of 0.19% of arable land per year [2]. Besides decreasing land fertility and depletion of groundwater, climate change as a whole affects agricultural yield negatively. For these and many other reasons, the employment of emerging technologies can assist farmers in automating a significant portion of modern farming to tackle different issues and produce more foods from less land. As such, the Bangladesh government has rightly picked up on the strategy to incorporate the use of Fourth Industrial Revolution (4IR) technologies to implement smart agriculture to ensure food security for its large population, and in the course of time it is going to adopt 5IR in this sector as well [3].

The advancement of technologies is contributing to improving the quality of our lives in many different ways. With the help of various emerging technologies, intelligent and sustainable farming has been introduced in the agricultural domain to modernise the food production process to increase yield and productivity. For instance, many state-of-the-art information and computing technologies such as the IoT, cloud/edge computing, artificial intelligence (AI), and AI-powered drones are employed to create sustainable agriculture systems [4]. Notably, different AI approaches, such as machine learning (ML) and/or deep learning (DL), are used for processing and supporting the agricultural value chain. A prominent study conducted on designing and applying an IoT-enabled agricultural system using DL techniques can be found in [5]. Similarly, another research proposed IoT-based architecture for smart surveillance systems to assist farmers in identifying appropriate crops to plant on the soil [6]. Technology-enabled systems use innovative ideas and research to improve numerous farming practices, including but not limited to plant health monitoring, detecting insects, crop growth monitoring and assessment, irrigation, detecting soil nutrients, pest control, weed detection, predicting crop yield, field analysis, crop spraying, and livestock monitoring. Even IoT-enabled crop fields can be architected into power-producing fields using photovoltaic cells [7]. IoT helps monitor and collect agricultural data automatically, which are then processed further in edge and/or cloud servers for intelligent decision-making. Over the years, many IoT-based innovative agriculture systems have been developed. An extensive review of such systems can be found in [1], [8]. Due to the limited scope, in this article, we consider the IoT-based automation of irrigation systems in smart farming. Among other natural resources, water plays a central role in agriculture. The alarming rate of the world's population growth and the increased demand for freshwater have led to the emerging global water crisis. This necessitates genuine efforts in sustainable water usage in every aspect of our lives, including farming. Smart irrigation systems (SIS) can monitor relevant parameters and control physical devices (e.g. water pumps) to irrigate whenever necessary instead of irrigating at a predefined regular interval, thus facilitating sensible water use.

While the utilisation of IoT, edge and AI for smart agriculture have modernised different farming practices, they have brought new challenges that can adversely undermine the benefits they offer. The increased use of information and communication technologies to connect the physical and cyber worlds leads to additional complexity; making system development, system safety and reliability more challenging. Moreover, sensors and other smart devices in smart agriculture are more vulnerable to failure because they are mostly deployed in harsh outdoor environments. Therefore, to make such systems more reliable, it is necessary to understand how they work and how they may fail during operation.

Hazard analysis systematically explores potential safety-related issues (e.g., issues that may cause system failure) to verify whether a system is safe to operate. Fault Tree Analysis (FTA) is a widely used hazard analysis technique that can aid systematic system failure analysis. The approach graphically modelled system failure based on the logical connections between the various failures and their causes. Although hazard analysis approaches are widely used in many safety-critical domains for systems' failure behaviour analysis, in IoT-enabled applications, especially in IoT-based smart agriculture, they are still not that prevalent. While system failure can be catastrophic in other safety-critical domains such as aviation, automobile and industrial control systems, the field of agriculture is equally not left behind. Failure of key enabling technologies in large-scale smart farming can adversely cause significant harm to nature and people, reduce agricultural production and cause enormous financial loss. Accordingly, credible failure analysis of IoT-based technology from the conceptual design stage is imperative to ensure the design of safe and dependable IoT-based agricultural systems. This effort will support the global drive towards smart farming for sustainable development. Accordingly, the inspiration of this article is to conduct a qualitative failure analysis of an IoT-based SIS. The analysis shows how the failures of different components of the SIS can cause the system to fail.

After this brief preamble, the rest of the paper is organised as follows. Section II provides an overview of IoT in agriculture, emphasising smart irrigation systems and the dependability analysis of IoT system with a focus on the FTA technique. Section III is a brief overview of related studies, while Section IV gives a detailed SIS design and qualitative failure analysis. Finally, Section V summarises the key aspects and suggests future research directions.

II. Background

This section gives an overview of some of the notable studies of IoT in the field of agriculture and dependability analysis concepts and attributes.

A. *IoT in agriculture: smart irrigation 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 (e.g. cloud/edge servers) to exchange information using advanced communication technologies with minimal human intervention. The rapid growth of IoT and other emerging technologies have opened avenues for their utilisation in monitoring and actuation activities in various domains. Agriculture is one such domain where the monitoring capability of IoT devices has been successfully applied to develop many smart farming applications. Due to brevity, we provide a review of only some of the available IoT-based systems used in agriculture in this article. Interested readers can find detailed reviews of IoT-based smart farming applications in [1].

Smart irrigation systems are one of the developed concepts in smart farming. Examples of IoT-based SISs can be found in [9]–[11]. In such systems, different types of sensors are deployed in the outdoor environment to monitor different parameters from the plants, soil and water, which include, but are not limited to, moisture, temperature and nutrients of soil; temperature, conductivity, level and flow of water; wetness of leaves and height of plants [8]. 6G-IoT technology can play a big role in establishing and maintaining communication among a huge number of sensors and IoT devices enabling accurate data collection which can augment precision agriculture [12], [13]. The data collected from a field and the surrounding environment are then processed to make intelligent decisions about the irrigation schedule. Based on the irrigation requirement, semi-automatic or automatic actuation actions are performed to control physical devices like water pumps.

Although IoT-based SIS can help to ensure the sustainable use of water and improve agricultural yields, there exist many issues that can cause significant disruption. Firstly, the smart devices used in the SIS are mostly deployed in an outdoor environment, which makes them highly susceptible to failure. Failure of the components will cause the overall system to fail, which may lead to a disastrous outcome. Secondly, communications between the sensors and edge devices/clouds primarily take place via a wireless medium. Wireless communication between different devices can fail for many different reasons, including intentional security attacks. A communication failure will cause the SIS to fail, irrespective of why the communication failure occurs. Thirdly, the edge cloud or central controller uses a data-driven approach to make a decision. Hence, the quality of data and their timely arrival affect the robustness of the decision. Moreover, failure of the edge cloud or the central controller will cause the SIS to fail. Finally, as a large number of heterogeneous devices are used in the system, bad interactions between them can take a system to an unsafe state. For the above-mentioned reasons, it is necessary to analyse an SIS to identify the potential causes of its failure.

B. *Dependability analysis of IoT: Fault Tree Analysis*

Dependability is a broad term that covers different non-functional system properties such as reliability, safety, availability, and maintainability. The dependability property gives a system the capability to avoid more severe and more frequent failures [14]. For this reason, in many domains, such as the automotive and aerospace industries, significant efforts have been made to carry out dependability assessment early in the design phase to identify and rectify potential hazards as soon as possible to prevent unacceptable costs with regard to loss of life, loss of resources, and environmental damage. Among the several attributes of dependability, the emphasis of this article is to address the safety and reliability analysis. To do so, FTA is one of the prominent techniques identified for safety analysis in many domains.

The FTA [15] is a prominent technique among all the different techniques used for dependability analysis. It is a graphical method that primarily uses Boolean AND and OR logic gates to show how combinations of component failures can cause an overall system failure. For instance, the failure behaviour of a series system can be modelled using an OR gate, where the failure of any one of the components will cause the system failure. In other words, when at least one of the inputs to the OR gate becomes true the output will become true. On the other hand, for the failure behaviour modelling of a parallel system, an AND gate is used because it will ensure that the system fails only when all the components fail, i.e., all inputs to the AND gate become true. The creation of a fault tree follows a top-down approach and it starts by defining a top event (TE), which is a failure condition for the system under study. With the help of logic gates, the TE is then logically linked to the next-level intermediate events, which are the immediate causes of TE. The intermediate events are recursively broken down until the bottom level (leaves) of the fault tree is reached. The leaves of the tree are known as the basic events (BEs), which are the component level failure or root causes of system-level that cannot be decomposed any further.

Once a fault tree is created, it can be analysed both qualitatively and quantitatively. Through a qualitative analysis minimal cut sets which are the smallest combination of root causes that can cause the system failure can be obtained. On the other hand, quantitative analysis involves utilising failure rates/probabilities of root causes to predict the failure probability of the system. The failure rates and probabilities of the components, which are the metrics of the BEs in the FT, are calculated by taking cognisance of the logic gates between events to determine the overall system-level failure [16].

III. Related Works

Given that Section II-A has discussed some notable studies on IoT-based smart agriculture systems, especially with an emphasis on smart irrigation systems among other IoT applications, this section discusses related studies concerning failure analysis. In the existing literature, several studies proposed different techniques for failure analysis of various systems based on their compositional structures and behaviours. For instance, Failure Mode and Effect Analysis (FMEA) was proposed by the US Military in 1980 for systematic identification of potential failures in a system along with their causes and effects [17]. Also, 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. Similarly, Bayesian Network (BN), which is a probabilistic modelling technique, was developed based on Bayes theorem to predict the probability of failure of systems using probabilistic reasoning in the conditions of uncertainty [17]. Although these existing approaches are remarkable for failure analysis, the International Electrotechnical Commission (IEC) 61508, recommended the FTA method as one of the most prominent methods for failure analysis [18].

Since the development of FTA in 1962 by Bell Phone Laboratories and its initial use for the evaluation of failure behaviours of the launch control system of LGM-30 Minuteman, it has been extensively extended to several other domains [16], [19]. However, despite the increasing applicability of the FTA method in other high-consequence domains, its applicability in IoT-based applications is at an early stage. The FTA framework was used in the safety analysis of smart homes [20], generic IoT systems [21] and smart agriculture systems [22], [23]. An FTA-based tool has been proposed in [21] for reliability analysis of IoT systems. In the proposed approach, a fault tree has been used to model the failure behaviour of different components in an IoT system. The fault tree is then analysed using the proposed tool to evaluate IoT system reliability and availability. In [20], a fault tree has been used to perform a security risk analysis of a light bulb system in an IoT-based smart home environment. Limited research on FTA-based failure behaviour analysis of smart agriculture has been performed. For instance, in aquaculture, FTA-based reliability analysis of an automated pond oxygen management system has been performed in [22]. In this work, the failure behaviours of different components of a pond's automated oxygen management system are modelled using a fault tree to show how the system can fail. In another work [23], Chen *et al.* proposed a fault diagnosis method for aquaculture by combining FTA with fuzzy neural networks. The proposed method was demonstrated via a case study of an outdoor pond where different components are deployed in an open and harsh environment. While an elaborate discussion on FTA can be found in [15], this research only focuses on its adaptation in qualitative failure analysis of IoT-enabled SIS.

IV. System Design and Analysis

A. System model and description

Fig. 1 shows the architecture of an IoT-based smart irrigation system, which is similar to the example shown in [10], [11]. Using this system, a farmer can remotely monitor the status of a field and control the water pump(s) to irrigate the field whenever needed without being physically present in the field. In a normal operating condition, this system will monitor different parameters of a field and based on the monitoring knowledge it will decide when and for how long to irrigate the field. For monitoring, it uses a temperature sensor (TS) and a moisture sensor (MS). TS monitors the temperature of the field and MS monitors the soil moisture. TS and MS continuously sense the respective parameters and report them to the IoT gateway/controller for further processing. The communication between the sensors and the IoT gateway takes place via a wireless medium. As an IoT gateway, an Arduino board or Raspberry Pi can be considered. For instance, in [11], an Arduino board is used as an IoT gateway. The board is powered by a battery. The IoT gateway converts the analog signals received from the sensors to digital values and sends these values to the edge cloud server. The communication between the edge cloud server and the gateway takes place wirelessly.

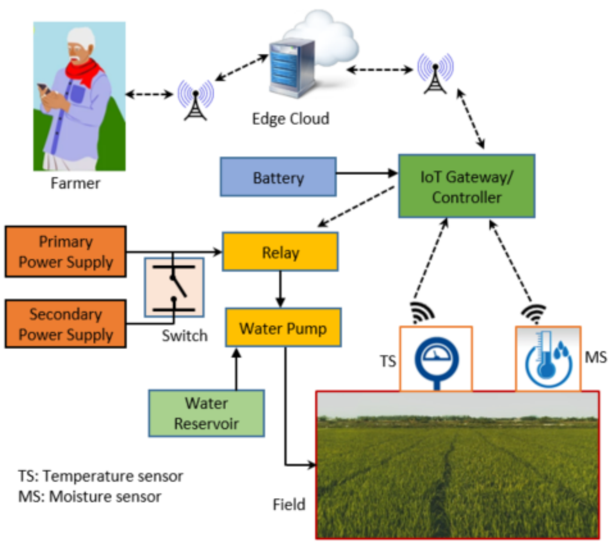

Fig. 1: Architecture of an IoT-based smart irrigation system

After receiving the readings from TS and MS, based on these values, an expert system within the edge cloud server uses some predefined rules to make a decision about irrigating the field. To make a highly precise decision, the expert system would require readings from both sensors. However, it can make a decision with reasonable accuracy in the presence of a single value. Once the server determines the current state of the field, it shares the information with the farmer via wireless communication so that the farmer can decide whether to turn on/off the pump and for how long. Based on the received information, if the farmer decides to turn on the pump, (s)he sends a command to the server instructing it to turn on the pump. The server will then pass this command to the IoT gateway, which will then send a command to the relay to activate it. If the relay is activated, the pump can draw the necessary power from the power supply system to pump water from the reservoir to the field. The power supply system consists of two power sources to have increased availability. In the normal operating scenario, the primary power supply delivers power to the pump and the secondary power supply remains in standby mode. If the primary power supply fails, the secondary power supply takes over its job and the switch connects the secondary supply to deliver power to the pump.

B. Qualitative failure behaviour analysis

As seen in Fig. 1, the smart irrigation system has some fault-tolerant mechanism built into it. For instance, the power supply system for the pump has a primary and a secondary power supply. Also, there are two sensors to detect two parameters from the field and only one parameter is sufficient to make a decision. Note that the system is generic which shows the general design pattern for a smart irrigation system instead of a specific system. Moreover, the devices used in the system are abstract hence there is no dependence on any particular technology. For a practical application, specific sensors, actuators, controllers and other types of devices can be used.

As mentioned before, depending on the role(s) of a component in the system and its interactions with other components in the system, the failure of the component can have an enormous impact on the failure of the system. Therefore, the aim of the qualitative failure behaviour analysis of this system is to identify the potential causes of its failure. For failure behaviour analysis, we have identified *"the failure of the system to irrigate the field when needed"* as a system failure condition. Considering this event as the top event of the fault tree, we have developed the fault tree shown in Fig. 2. This FT contains 19 unique basic events, which are the root causes that can contribute to the system failure. These root causes are either an internal failure of the devices or the failure of the communication between devices. Table I shows the ID and the description of all the events of the FT.

As seen in Fig. 2, physical damage to the sensors or erroneous readings from the sensors is considered as the failure of the TS and MS, which are represented by the events TSF (temperature sensor failure) and MSF (moisture sensor failure). In the fault tree, five basic events – FCRG, FCGC, FCFC, FCTG, and FCMG – represent communication failures between different components of the system. Note that, due to simplicity and brevity, we have considered these communication failure-related events at an abstract level. This means we do not decompose these events further to show why a particular communication failure occurs. However, one can consider all the causes of a typical wireless communication failure to further explore these events. Similarly, the failure of the edge cloud is presented by the event ICS (internal failure of the edge cloud server) due to simplicity. Again, this event can be decomposed further by considering many potential causes of a cloud server failure including hardware and software failures.

We have analysed the fault tree in Fig. 2 to identify the minimal cutsets (MCSs) and obtained 21 MCSs. The MCSs are: *1. PDTS . PDMS; 2. PDTS . ERMS; 3. PDTS .FCMG; 4. ERTS . PDMS; 5. ERTS . ERMS; 6. ERTS. FCMG; 7. FCTG . PDMS; 8. FCTG . ERMS; 9. FCTG .FCMG; 10. FCGC, 11. BF; 12. IFG; 13. ICS; 14. FCFC; 15. HE; 16. FCRG; 17. IFR; 18. IFWP; 19. SWF. PPSF; 20. SPSF. PPSF; 21. WLIR.* In these logical expressions of the MCSs, the symbol '.' represents a logical AND operation. Out of these 21 MCSs, 11 MCSs are of order 2 and 10 are of order 1. The order of an MCS represents the number of basic events contributing to that MCS. If all the basic events are equally probable to occur then the higher the order of an MCS the lower the criticality of that MCS is. Therefore, in this example, the first-order MCSs such as "failure of communication between the

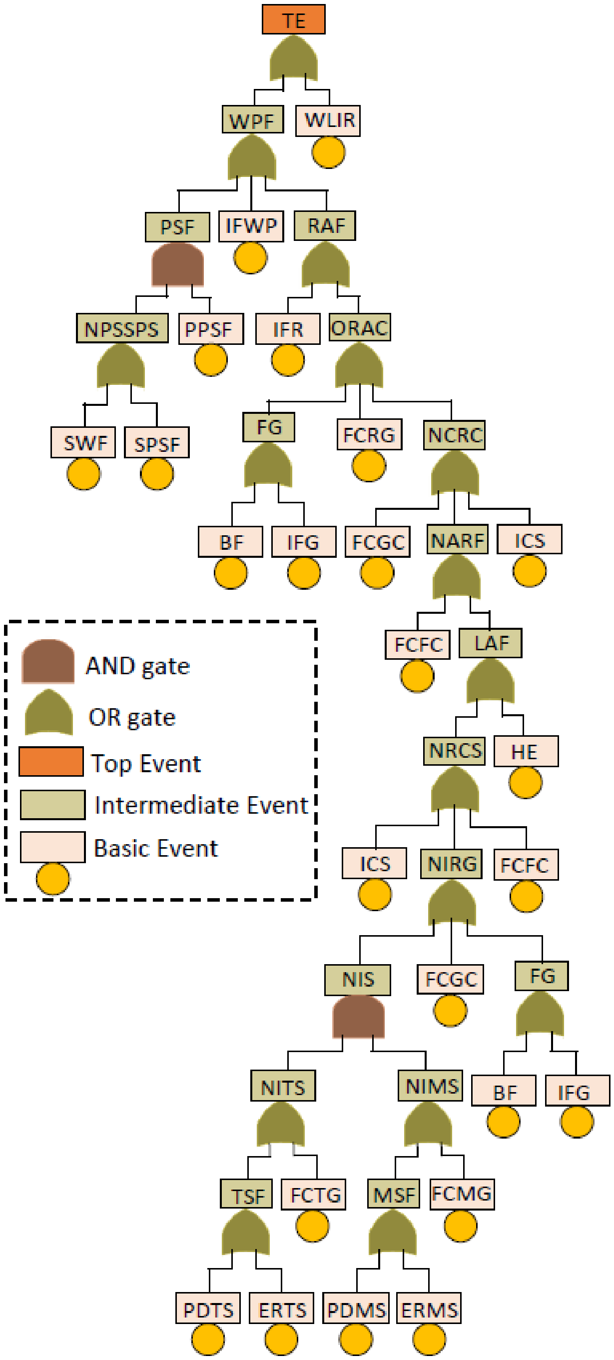

Fig. 2: Fault tree of the smart irrigation system

TABLE I: ID and Description of the events of the fault tree of Fig. 2

ID	**Description**
TE	Failure of the irrigation system
WPF	Water pump fails to pump water to the field
WLIR	Water level inadequate in the reservoir
PSF	Power supply failure
IFWP	Internal failure of the water pump
RAF	Relay activation failed
NPSSPS	No power supplied from the secondary power supply
PPSF	Primary power supply failure
IFR	Internal failure of the relay
ORAC	Omission of the relay activation command
SWF	Switch failure
SPSF	Secondary power supply failure
FG	Failure of the IoT gateway
FCRG	Failure of communication between the relay and the IoT gateway
NCRC	No command received by the IoT gateway from the edge cloud server
BF	Battery Failure
IFG	Internal failure of the IoT gateway
FCGC	Failure of communication between the IoT gateway and the edge cloud server
NARF	No action recommended by the farmer
ICS	Internal failure of the edge cloud server
FCFC	Failure of communication between the farmer and the edge cloud server
LAF	Lack of action from the farmer
NRCS	No recommendation received by the farmer from the edge cloud server
HE	Human error
NIRG	No input received by the edge cloud server from the IoT gateway
NIS	No input received from sensors
NITS	No input from the temperature sensor
NIMS	No input from the moisture sensor
TSF	Temperature sensor failure
FCTG	Failure of communication between the temperature sensor and the IoT gateway
MSF	Moisture sensor failure
FCMG	Failure of communication between the moisture sensor and the IoT gateway
PDTS	Physically damaged temperature sensor
ERTS	Erroneous reading from the temperature sensor
PDMS	Physically damaged moisture sensor
ERMS	Erroneous reading from the moisture sensor

IoT gateway and the edge cloud server (FCGC)", "internal failure of the IoT gateway (IFG)", "internal failure of the edge cloud server (ICS)", "failure of communication between the farmer and the edge cloud server (FCFC)", "human error (HE)", "failure of communication between the relay and the IoT gateway (FCRG)", "battery failure of the IoT gateway (BF)", "internal failure of the relay (IFR)", and "water level inadequate in the reservoir (WLIR)" are the most critical ones. Therefore, actions should be taken to reduce the likelihood of the occurrence of these events. For instance, for the events related to communication failure, multiple communication media can be considered for communication so that if one medium fails another can be used for successful communication.

C. Potential Security Considerations

For any IoT-enabled smart agriculture system, an end-user must always receive valid information from the field sensors. However, in many cases, it has been noticed that an adversary can intercept and alter the field data collected by the sensors and then send them to the farmers. To protect against such attacks a secure MAC can be used, where an unforgeable tag generated by the MAC will be able to ensure the integrity of the data. In addition, a lightweight signature scheme can be used to validate the integrity of the sources. Finally, since IoT devices such as TS and MS are deployed in the open and public field, which makes them vulnerable to physical and cloning attacks, the end-user can receive the wrong information. To deal with such an issue, PUF-enabled devices [24] can be deployed to collect the field information, where any attempt to tamper with the PUF will change the behaviour of the device and render the PUF useless.

V. Conclusion

Many developing countries like Bangladesh have continued to follow the wake of other technologically advanced societies in areas of value-driven smart sustainable technology (5IR) in agriculture to enhance the food value chain of their growing population. Research efforts in developing analysis and verification frameworks to support agricultural-based intelligent systems are novel efforts toward supporting food sustainability. This article shows the qualitative failure behaviour analysis of an abstract IoT-based smart irrigation system. The analysis was conducted using the FTA framework, one of the most widely used techniques employed in other critical domains. The developed fault tree displays different component failures as basic events, and how these failures can be propagated 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 failure. 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 exactly used components and model their behaviour in more detail. For illustration, we have considered the inability of the system to irrigate the land 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] M. Ayaz, M. Ammad-Uddin, Z. Sharif, A. Mansour, and E.-H. M. Aggoune, "Internet-of-Things (IoT)-based smart agriculture: Toward making the fields talk," *IEEE Access*, vol. 7, pp. 129 551–129 583, 2019.

[2] Bangladesh Bureau of Statistics (BBS), "Agriculture census 2019: Structure of agricultural holdings and livestock & fisheries, national series volume-1," BBS, Statistics and Informatics Division, Ministry of Planning, Government of the People's Republic of Bangladesh, 2022. [Online]. Available: https://bbs.portal.gov.bd/sites/default/files/files/bbs.portal.gov.bd/page/c645bd51_3cb5_4f53_86f9_7d29244caa4e/2022-12-26-08-36-394361bc904a7651ef763a4ff8033b67.pdf"

[3] C. Anir. (2023) Smart agriculture for smart bangladesh. [Online]. Available: https://a2i.gov.bd/smart-agriculture-for-smart-bangladesh/

[4] N. Gondchawar, R. Kawitkar *et al.*, "IoT based smart agriculture," *International Journal of advanced research in Computer and Communication Engineering*, vol. 5, no. 6, pp. 838–842, 2016.

[5] T. Saranya, C. Deisy, S. Sridevi, and K. S. M. Anbananthen, "A comparative study of deep learning and internet of things for precision agriculture," *Engineering Applications of Artificial Intelligence*, vol. 122, p. 106034, 2023.

[6] R. D. Boddu, P. Ragam, S. P. Pendhota, M. Goni, S. Indrala, and U. R. Badavath, "Iot-based smart agricultural monitoring system," in *Proceedings of Fourth International Conference on Computer and Communication Technologies: IC3T 2022*. Springer, 2023, pp. 377–385.

[7] K. Huang, L. Shu, K. Li, Y. Chen, Y. Zhu, and R. Valluru, "Sustainable and intelligent phytoprotection in photovoltaic agriculture: New challenges and opportunities," *Electronics*, vol. 12, no. 5, p. 1221, 2023.

[8] L. García, L. Parra, J. M. Jimenez, J. Lloret, and P. Lorenz, "IoT-based smart irrigation systems: An overview on the recent trends on sensors and IoT systems for irrigation in precision agriculture," *Sensors*, vol. 20, no. 4, p. 1042, 2020.

[9] R. Shahzadi, M. Tausif, J. Ferzund, and M. A. Suryani, "Internet of things based expert system for smart agriculture," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 9, pp. 341–350, 2016.

[10] S. B. Saraf and D. H. Gawali, "IoT based smart irrigation monitoring and controlling system," in *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*. IEEE, 2017, pp. 815–819.

[11] G. Sushanth and S. Sujatha, "IOT based smart agriculture system," in *2018 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*. IEEE, 2018, pp. 1–4.

[12] S. Polymeni, S. Plastras, D. N. Skoutas, G. Kormentzas, and C. Skianis, "The impact of 6g-iot technologies on the development of agriculture 5.0: A review," *Electronics*, vol. 12, no. 12, p. 2651, 2023.

[13] F. Zhang, Y. Zhang, W. Lu, Y. Gao, Y. Gong, and J. Cao, "6g-enabled smart agriculture: A review and prospect," *Electronics*, vol. 11, no. 18, p. 2845, 2022.

[14] 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.

[15] 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.

[16] A. Abdulhamid, S. Kabir, I. Ghafir, and C. Lei, "An overview of safety and security analysis frameworks for the internet of things," *Electronics*, vol. 12, no. 14, p. 3086, 2023.

[17] 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.

[18] R. Bell, "Introduction and revision of iec 61508," in *Advances in Systems Safety: Proceedings of the Nineteenth Safety-Critical Systems Symposium, Southampton, UK, 8-10th February 2011*. Springer, 2010, pp. 273–291.

[19] 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.

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

[21] 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.

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

[23] Y. Chen, Z. Zhen, H. Yu, and J. Xu, "Application of fault tree analysis and fuzzy neural networks to fault diagnosis in the internet of things (IoT) for aquaculture," *Sensors*, vol. 17, no. 1, p. 153, 2017.

[24] P. Gope and B. Sikdar, "Lightweight and privacy-preserving two-factor authentication scheme for iot devices," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 580–589, 2018.