

Failure Analysis of Vital Sign Monitoring System in Digital Healthcare with FTA

Faiza Sabir¹, Sarfaraz Ahmed², Gihwon Kwon^{3*}

Abstract

Digital healthcare system requires safety critical software and more attention among human perception and assistance of computer. Apparently, it becomes serious challenge for engineers and doctors in assuring the secure and reliable healthcare system. The main target is patient safety here, thus important factor to consider in healthcare is system protection. In recent research vital signs such as heart rate (HR) and breathing rate (BR) are extracted using a non-invasive IR-UWB radar sensor. Hence, safety of the contact-less device is necessary for proper and accurate measurement of HR and BR in digital healthcare system. Therefore, in our research we drawn and performed fault tree analysis (FTA) of such system which analyze potential hazards of measuring subject's HR and BR in a non-contact fashion. We emphasize on crucial issues and safety factors which are important in patient safety and protection before the proper deployment of such healthcare system.

Key Words: Software Safety, Digital Healthcare, Signal Processing, Radar.

I. INTRODUCTION

Software safety is a critical aspect of healthcare systems, where the use of technology is rapidly growing. The integration of software systems into healthcare has improved patient care and made medical procedures more efficient. However, with this increased reliance on software, there is also an increased risk of system failures and errors that could negatively impact patient safety. Apart from healthcare system many other systems such as transportation control, avionics, electronic, communication and engineering systems are also required critical safety measures [1]. All systems must be designed, specified, used, processed, and conserved with the utmost care because they could cause harm or death as well as material loss. Software safety in healthcare systems involves ensuring that the software is designed, developed, and implemented in a way that minimizes the risk of harm to patients [2]. This includes identifying and addressing potential risks, ensuring that the software complies with regulatory standards, and providing appropriate training and support to users [3]. A safety-critical system's software engineering demands complete comprehension of the program's component and cooperation with

the system [4-5]. Further, software safety in healthcare systems becomes complex and critical issue that requires careful attention to ensure that patients receive safe and effective care. It involves a range of activities, including risk management, compliance with regulatory standards, data security, software safety, system protection and user training with support [6-7].

These days' electronic and computer system is wildly used in a medical diagnosis with integration in digital healthcare system. Latest technology, radar transceiver based vital design monitoring system is used to capture patient's heart rate and breathing rate in a non-contact fashion [8]. Contact-free continuous monitoring allows for privacy while also providing the resident with a safe means of being seen as they recover in their house or room without compromising their quality of life [9]. Subject's data transmit and receive remotely through infrared waves and extract heart rate wirelessly from vital sign raw data [10]. Thus, most critical aspect here is safety of software and data in such digital healthcare application. Therefore, we have drawn and analyzed system's fault analysis or risk management which is necessary to be noticed before implementation of such system in our daily lives.

Manuscript received June 06, 2023; Revised June 22, 2023; Accepted July 03, 2023. (ID No. JMIS- 23M-06-026)

Corresponding Author (*): Gihwon Kwon, +82-31-249-9666, khkwon@kyonggi.ac.kr

¹Department of Computer Science, Kyonggi University, Suwon, Korea, faiza_60@kyonggi.ac.kr

²Department of Electronics Engineering, Hanyang University, Seoul, Korea, sarfaraz687@hanyang.ac.kr

³Department of Computer Science, Kyonggi University, Suwon, Korea, khkwon@kyonggi.ac.kr

In Section II of the paper, we discussed about radar sensor and vital sign monitoring system. Software safety protocols and standards are discussed in Section III. Section IV is about fault tree analysis of vital sign monitoring system in digital healthcare system. Last, Section V covers experimented results. Section VI comprised on conclusion.

II. COMPONENTS OF CRITICAL SOFTWARE BASED MEDICAL DEVICES

Software based medical equipment is getting common and commercialize in medical application for multiple diagnosis. Such devices are now expected to perform better, and their increasing ubiquity has presented designers with difficult design challenges. The most crucial thing is to ensure device's safety and security. Because of the surrounding software's rapidly increasing intricacy, it is now more challenging. Digital healthcare devices equipped with many functions such as failure of electric components, malfunctioning of electric sensors, imperfect software module can create intense outcomes. Therefore, device makers need to be aware of the fundamental distinctions between software and hardware parts and set up reliable development of software procedures based on acknowledged engineering principals suitable for safety critical systems [3]. In opposition to software, medical device developers frequently patent and establish their products for a specific use in a specific device. For software components, there is sadly no well-known path log. Therefore, it is the device developers' duty to ensure the safety and effectiveness of software-based medical devices. It requires expertise in effective risk management effort, a grasp of software safety, and consideration of risk management implementation to overcome such challenges in medical diagnosis [6].

Safety-critical software in healthcare systems refers to software that is designed to operate without causing harm to patients, medical staff, or the environment, and whose failure could result in serious injury or death. Such software is essential in healthcare because it is responsible for controlling critical medical devices, such as patient monitors, infusion pumps, and anesthesia systems. Overall, the study of safety-critical software in healthcare systems is critical to ensuring the safety and well-being of patients and medical staff, and to maintaining the trust and integrity of healthcare systems. Although, significant importance of software based medical devices is there but those services can affect patient health by posing hazards [11-12]. The potential risks associated with software-based medical devices focuses on the design and development of software in safety-critical medical devices, such as infusion pumps, radiation therapy systems, and patient monitor [13]. Several

cybersecurity threats that can affect medical devices, including denial-of-service attacks, malware, and unauthorized access. These threats can compromise the safety and security of medical devices, potentially leading to harm to patients [14]. The US Food and Drug Administration (FDA) analyzed 937 recalls of medical devices, of which 12% (or 113 recalls) were related to software. It was found that software-related recalls were more likely to result in serious harm or death compared to non-software related recalls [14]. Device manufacturers have a moral, legal, and financial obligation to ensure that their products do not cause harm. Despite significant investments made by manufacturers to ensure product safety, failures still occur. For example, the Food and Drug Administration reported that 200 thousand pacemakers were evoked due to software problems. In the unites state, there were 30 thousand fatalities and around 600 thousand injuries caused by medical devices, with 8% of these involving faulty software [7]. Thus, several solutions were discussed of addressing these challenges, including the use of formal methods for software verification, the adoption of standardized testing methods, and the development of best practices for software design and testing [15].

IR-UWB radar sensor is a non-contact vital sign monitoring system which measures our body's health information through electromagnetic waves and frequencies. Recently, non-contact based vital sign extraction from human data got serious attention in digital healthcare systems. In many clinical applications, real-time tracking of vital signs like respiratory rate (RR), oxygen saturation, heart rate (HR), blood pressure (BP), and body temperature is essential. Preclinical evaluation of those vital signs was monitored in a noncontact fashion using IR-UWB radar sensor in a similar way of electrocardiography (ECG) sensor. Latest, assessment of fatigue and rest is also classified based on heart rate variability (HRV) using radar sensor [9]. IR-UWB radar sensor (NVA6201, Novelda AS, Kviteseid, Norway) consists on Microcontroller unit (MCU), radar chip, external RAM and Transmitter/Receiver antenna. IR-UWB radar sensor with integrated processors and software that allows for comfortable real-time HR and RR tracking from a comfortable distance on the chest or neck. The radar chip inside the system transmit and receive frequencies and then capture vital sign of the subject which further helps in computing heart rate and breathing rate using digital signal processing algorithm in [10]. The vital sign information can further send remotely to physician for instant observation. In this way contact-less radar based system is very comfortable in monitoring vital sign remotely while patient stays in home. Though privacy of data and safety of such system is a main challenge to focus on. Hence, we proposed fault tree study of such monitoring system which could help in drawing software hazard analysis and validation of vital sign

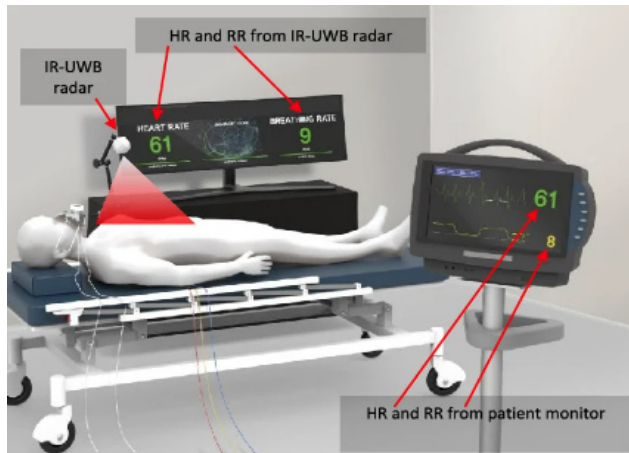


Fig. 1. Noncontact vital sign monitoring system using radar [10].

monitoring system in digital healthcare (Fig. 1).

III. SOFTWARE RISK MANAGEMENT IN DIGITAL HEALTHCARE SYSTEM

These days' healthcare devices in medical diagnosis incorporate many engineering software and hardware engineering technologies. Due to the complexity of the software application in many clinical devices, full testing is required in addition to other techniques like design verification, assessment of fault analysis and other safety related methods. Abnormalities on healthcare devices can produce catastrophic outcomes to patients.

The fundamental ideas behind risk management are founded on engineering principle and good conducts toward safety. Risk management for software effectiveness compromises on three steps are as follows. Developers must first recognize that some device risks may be caused by software flaws. Second, developers need to take the right steps to reduce the dangers. Third, the developers must

show that the steps made to reduce the risks are effective. The risk of harm to the patient, the caregiver, and the therapy setting is the main concern throughout these activities [2]. Safety risks increases with embedded medical systems consist on complex software and hardware which is a serious challenge for device manufacturer. Therefore, initial risk analysis, and proper risk management is a good practice of handling faulty software in healthcare devices. Here some foundational standards are considered for proper risk management in software engineering [3].

Device manufacturers have to consider the potential dangers to patients, operators, third parties such as service technicians, and the surroundings. In the United States, the Food and Drug Administration oversees the creation and advancement of medical equipment, demanding that they are not only effective but also safe. The Quality System Regulation of the FDA mandates manufacturers to include risk management in their design, manufacturing, and support procedures. These practices provide both a framework for assessing a device manufacturer's current software development competency and guidance for producing devices with acceptable risk [3].

When developing a system, it is essential to consider all components, including hardware, software, users, and the environment. Each part of the system must be safe and secure. The quality of a system determines its level of security, whether in theory or practice. It is not enough to focus solely on software security because the behavior of the entire system cannot be predicted. Therefore, system safety analysis is necessary to determine the software safety requirements, which must be included in the software requirements specification and communicated to the developer (Table 1).

The system safety analysis needs to be carried out throughout the entire project life cycle. It is important to evaluate the impact of the system analysis and ensure that

Table 1. Software risk management in healthcare applications: Some international standards of software risk management system [3].

No	Standards	Category	Description
IEC 60601-1	Risk management standard	Safety and essential performance of medical electrical equipment	This is the basic standard that refers to the minimum safety and performance required of a medical device before it can be sold.
IEC 61025	Functional safety standard	Applied to safety related systems that include electric/electronic systems installed in production	Describes fault tree analysis and provides guidance on its application to perform an analysis, identifies appropriate assumptions, events and failure modes, and provides identification rules and symbols.
ISO/IEC/IEEE 1633	Software failure modes, software reliability	Software quality and management software engineering	This standard provides guidance on the application of FTA to computer-based systems. It includes guidance on how to identify and analyses failure events, how to develop fault trees, and how to interpret the results of the analysis.
ISO 1497	Risk management	Application of risk management	Defines several risk management.

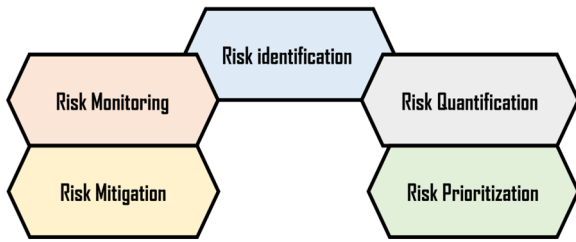


Fig. 2. Risk management in healthcare systems.

any necessary modifications and solutions at the system level are incorporated into the software. Additionally, the software safety analysis provides input for the system safety analysis. The software safety analysis is an integral part of the overall system safety examination and cannot be conducted independently. Therefore, the system development process includes four important elements related to security: identifying threats and safety requirements, designing the system to meet safety requirements, testing the system to ensure it meets safety requirements, and producing a safety case to prove the system's safety [13]. Healthcare organizations and risk managers must take certain steps to manage the risks associated with healthcare (Fig. 2).

IV. FAULT TREE ANALYSIS FOR CRITICAL VITAL SIGN MONITORING SYSTEM

Fault analysis of vital sign monitoring system is necessarily to focus on as it's directly attached to a patient. Device designer and developers must aware hazards and failure modes that lead to serious threats to the healthcare systems. Administrations frequently mix up risks and failure modes. Failure modes are descriptions of how a device can malfunction. Hazards may arise as a result of failure modes; however, failure modes may not always constitute hazards. Prior to determining failure modes and fault analysis that can result in those dangers, device developers should concentrate on identifying hazards. Excellent focusing tools include failure modes impacts criticality analysis and fault tree analysis.

Fault Tree Analysis (FTA) is a systematic method used to identify the causes of system failures and the events that can lead to those failures. It is commonly used in engineering and safety analysis to identify and understand the factors that contribute to complex system failures. In FTA, a graphical representation called a fault tree is used to represent the logical relationships between events and their causes. The fault tree is a tree-like diagram, with the top event (i.e., the system failure) at the top of the tree and the contributing events and causes branching out below it. The events and causes are connected by logical gates, such as "AND" and "OR" gates, which represent the relationships between events.

FTA is an effective technique used to identify the failures of the system and also used identifying the causes of system failures and help in the development of the policies to alleviate the risks and by alleviate the risk we can improve the system safety and ensure reliability. The FTA is typically involves five key steps explained in Fig. 3.

Here, we present Fault tree analysis (FTA) of vital sign monitoring system in digital healthcare by considering Table 1 risk management standards. The vital sign monitoring system here measures heart rate (HR) and breathing rate (BR) of the patient in a non-contact way using radar sensor. We followed top to bottom hierarchy of failure analysis and showed that system could fail through any incorrect measurement or abnormalities in data during monitoring vital signs such as HR and BR. At the top level when incorrect HR or BR monitored that could be because of incorrect frequencies measurement or inappropriate extraction of vital signal. Here, HR. (0.8 Hz–2 Hz) and BR (0.2 Hz–0.5 Hz) are the approx. estimated frequency ranges produced after extraction of accurate vital signal from raw data of the subject. However, vital sign extraction failure can be due to either radar sensor failure or error occurred during computation of vital signs signal. On the other hand, erroneous artefacts present in the signal or noisy vital signal can cause to inaccurate frequencies measurement. In the last step, other casual events such as error while recoding patient's data or error in the algorithm at bottom layer can be root cause of failures described earlier. These all are the possible failures of vital sign monitoring system that could create hazards in digital healthcare system. Illustration of this system FTA with other causalities described in Fig. 4.

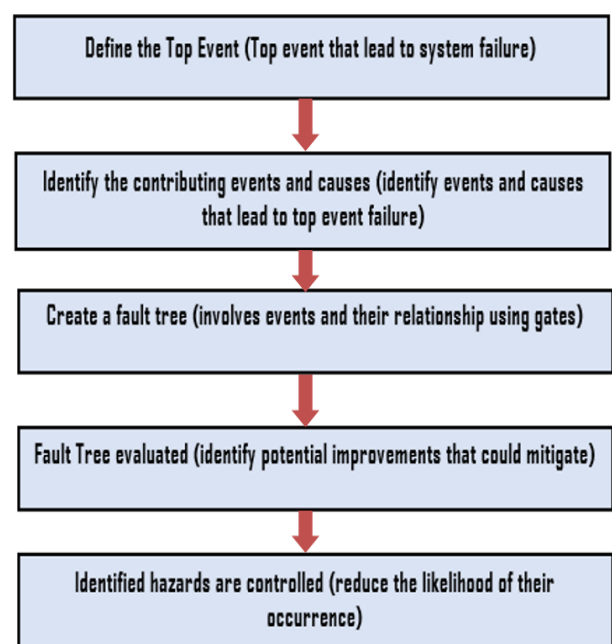


Fig. 3. Steps to apply the fault tree analysis.

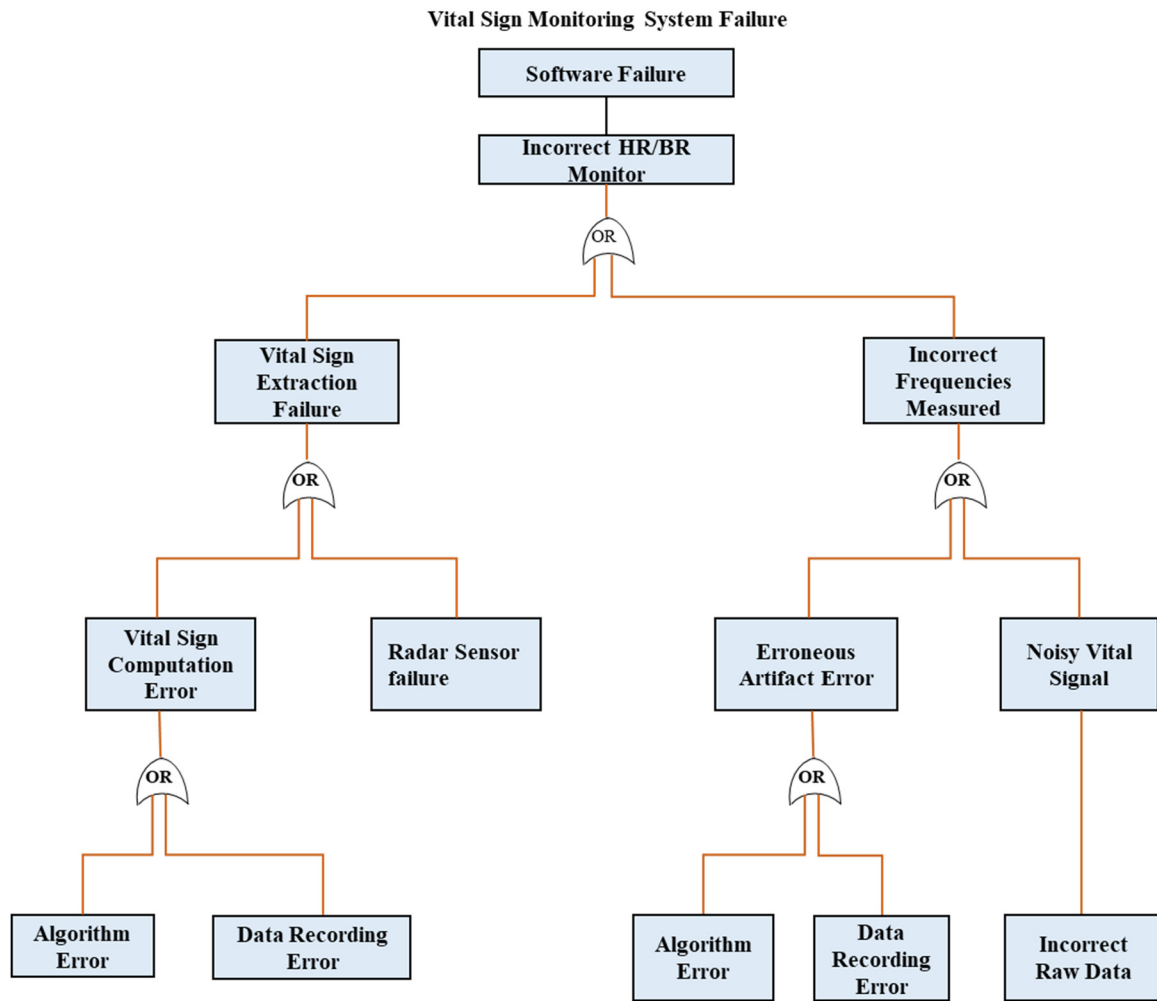


Fig. 4. Fault tree analysis for the vital sign monitoring system.

V. EXPERIMENTAL RESULT

An accurate vital sign signal is very imported to categorize patient's health information such as heart rate, respiration rate, temperature etc. In this work, we will discuss extraction of respiration rate (RR) and heart rate (HR) from accurate and inaccurate vital signal and what outcomes can appears as a perspective of failure analysis.

The right side of fault tree analysis was experimented to make sure if the vital sign monitoring system has potential faults. Because of improper raw data recording, noisy vital signal was obtained. Vital signal can be obtained through signal processing algorithm [16]. An example of such improper raw data containing artifacts is shown in Fig. 5(a). While noisy vital signal signal is shown in Fig. 5(b). As a result, inaccurate HR was estimated in frequency domain analysis. Fig. 5(c) demonstrates that the spectrum exhibits a prominent peak at 18 (per minute), indicating the fundamental RR. The spectrum also displays the presence of breathing harmonics and HR components. However, when the HR coincides with the proximity of the breathing harmonics, the

filter has the potential to attenuate both the HR and the breathing harmonics. Therefore, it is hard to choose an accurate HR statistically.

Typically, normal human respiration rate range from 12 to 18 breaths per minute (approx. 0.15 Hz–0.5 Hz) and heart rate ranges between 48 to 100 beats per minutes (approx. 0.8 Hz–2 Hz).

Fig. 5 depicts the results obtained from raw data collected by a radar sensor, as detailed in the referenced article [10]. The study involved extracting vital signs while the subject was lying on the bed, employing a signal processing algorithm explained in the same reference [10]. After successfully extracting the vital signs, the heart and respiration waveforms were separated using a bandpass filter, which was designed based on specific frequency ranges outlined above it is worth noting that the vital signs captured can sometimes be affected by noise and imperfections, as illustrated in Fig. 4. These issues can lead to inaccuracies in measuring heart and respiration rates, as demonstrated in Fig. 5.

Fig. 5 represents the outcome derived from the proposed

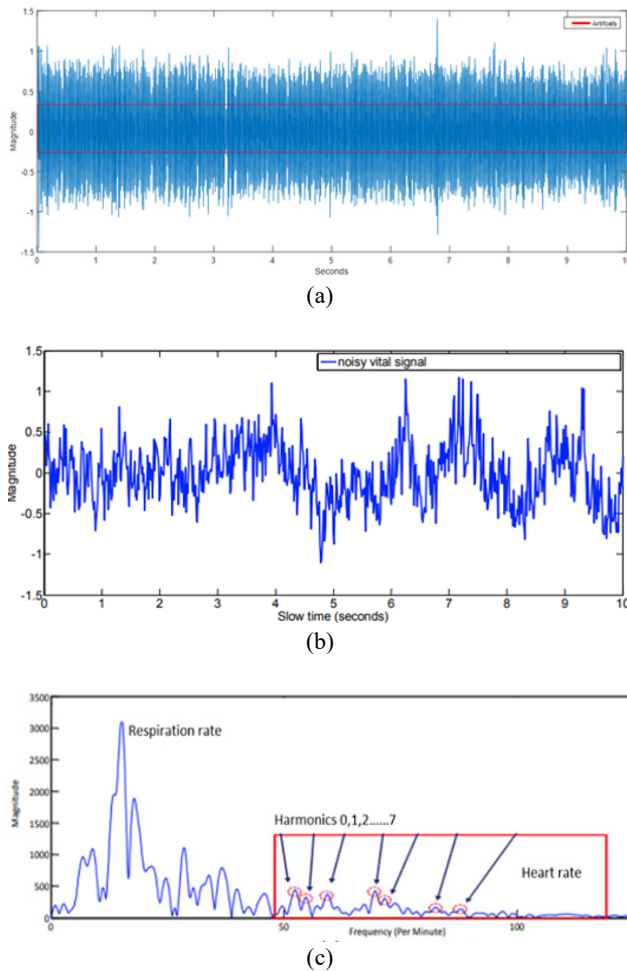


Fig. 5. Improper raw data and vital sign signal containing artifacts and noises and then resultant respiration and heart rate.

Fault Tree Analysis (FTA). In this analysis, we specifically focus on the errors located on the right side of the tree, such as the case of Incorrect raw data, which results in a noisy vital signal as illustrated in Fig. 5. When the system receives improper vital sign data, there is a high probability of obtaining inaccurate frequencies through the signal processing algorithm [10]. Consequently, these abnormal frequencies lead to incorrect measurements of the heart rate (HR) and respiration rate (RR). This occurrence can be classified as a software failure, as it failed to capture the correct raw data initially, thereby preventing the extraction of accurate vital signs and resulting in improper measurements of HR and RR. Hence, we refer to this as a failure of the vital sign monitoring system. There could be other failures and errors within the tree (left side) of FTA, which can be processed and verified the system failure.

So, it is very crucial to address the issue of inaccurate measurement of the heartbeat signal as it directly affects the medical diagnosis of a patient's health. When the system fails to extract a reliable vital sign, physicians are unable to effectively monitor the subject's well-being, potentially

posing risks to the patient's health. Therefore, it is imperative to rectify any inaccuracies in order to ensure proper health monitoring and mitigate potential dangers.

Such inaccurate measurement errors followed by possible fault tree analysis (FTA) are predicted through experimental results. Subject's data were taken from [9-10] for the assessment of vital sign monitoring system using radar technology. Those inaccurate measurements of RR and HR in vital sign could cause patient health assessment in medical diagnosis. Therefore, precise and correct measurement of vital signs are necessary to assess health information to avoid unnecessary danger to patient.

VI. CONCLUSION

In conclusion, ensuring software safety in healthcare systems is crucial to avoid potential harm to patients, such as incorrect diagnoses, incorrect treatments, or even fatalities. In this paper we presented possible events in one of the standard method Fault Tree Analysis (FTA). These events can happen during real time patient's health monitoring and cause system at risk which ultimately effects on subject's health. Therefore, development and implementation of software safety measures require a thorough understanding of the risks involved, including risk assessment, risk management, and risk mitigation strategies described by ISO, FDA and other organizations in Table 1.

From the experimental results, an accurate vital sign measurement is a main key of extraction RR and HR. The inaccurate measurement of vital signs can pose potential risks or dangers. Therefore, following FTA tree, developers should carefully consider such inaccuracies of vital signs measurement which could cause potential hazard to patient in medical diagnosis

To ensure software safety in healthcare systems, several measures can be taken, such as thorough testing and validation of software systems, regular maintenance and updates, appropriate documentation, and compliance with regulatory standards and guidelines. However, FTA and risk measures explained in this paper also helps to developer to consider those events at the development stage rather than considering after deployment of system. Medical system software developers should also endorse software safety by following product development cycle and software risk management. If the features and practices mentioned above are thoroughly examined, it will result in a decrease in the risks associated with software faults in digital healthcare applications.

ACKNOWLEDGMENT

This work was supported by the Institute of Information

& Communications Technology Planning & Evaluation (IITP) grant funded by the Korean government (MSIT) (No. 2021-0-00122, Safety Analysis and Verification Tool Technology Development for High Safety Software Development).

REFERENCES

- [1] O. Rafal and M. G. Park, "A study on the software safety assessment of healthcare systems," *Journal of Multimedia and Information System*, vol. 2, no. 3, pp. 215-220, Jun. 2015.
- [2] C. Lindholm, J. Notander, and M. Höst, "Software risk analysis in medical device development," in *Proceedings of the 37th EUROMICRO Conference on Software Engineering and Advanced Applications*, Finland, Aug. 2011, pp. 362-365.
- [3] R. Rakitin, "Coping with defective software in medical devices," *Presented at the IEEE Computer Society*, vol. 39, no. 4, pp. 40-45, Apr. 2006.
- [4] D. Wang, F. B. Bastani, and I. L. Yen, "Automated aspect-oriented decomposition of process-control systems for ultra-high dependability assurance," *IEEE Transactions on Software Engineering*, vol. 31, no. 9, pp. 713-732, Sep. 2005.
- [5] P. V. Bhansali, "Software safety: Current status and future direction," *SIGSOFT Software Engineering Notes*, vol. 30, no. 1, Jan. 2005.
- [6] C. Heneghan, M. Thompsin, M. Billingsley, and D. Cohen, "Medical-device recalls in the UK and the device-regulation process: Retrospective review of safety notices and alerts," *BMJ Open*, vol. 1, no. 1, p. e000155, 2011.
- [7] DCB0129, "Clinical risk management: Its application in the manufacture of health IT systems".
- [8] Y. Lee, J. Y. Park, Y. W. Choi, H. K. Park, S. H. Cho, and S. H. Cho, et al., "A novel non-contact heart rate monitor using impulse-radio ultra-wideband (IR-UWB) radar technology," *Journal of Scientific Reports*, vol. 8, no. 1, p. 13053, Aug. 2018.
- [9] S. Ahmed, Y. Lee, Y. H. Lim, S. H. Cho, H. K. Park, and S. H. Cho, "Noncontact assessment for fatigue based on heart rate variability using IR-UWB radar," *Journal of Scientific Reports*, vol. 12, no. 1, p. 14211, Aug. 2022.
- [10] J. Y. Park, Y. Lee, R. Heo, H. K. Park, S. H. Cho, and S. H. Cho, et al., "Preclinical evaluation of noncontact vital signs monitoring using real-time IR-UWB radar and factors affecting its accuracy," *Journal of Scientific Reports*, vol. 11, no. 1, p. 23602, Dec. 2021.
- [11] J. C. Knight, "Safety critical systems: Challenges and directions," in *Proceedings of the 24th International Conference on Software Engineering*, 2002, pp. 547-550.
- [12] R. H. Taylor and D. Stoianovici, "Medical robotics in computer-integrated surgery," *IEEE Transactions on Robotics and Automation*, vol. 19, no. 5, pp. 765-781, Oct. 2003.
- [13] J. A. McDermid, "Software hazard and safety analysis. in formal techniques in real-time and fault-tolerant systems," in *Proceedings in Formal Techniques in Real-Time and Fault-Tolerant Systems 7th International Symposium*, 2002, pp. 23-34.
- [14] T. C. Liebel, T. Daugherty, A. Kirsch, S. A. Omar, and T. Feuerstein, "Analysis: using the FDA MAUDE and medical device recall databases to design better devices," *Journal of Biomedical Instrumentation & Technology*, vol. 54, no. 3, pp. 178-188, May 2020.
- [15] W. J. Gordon and A. D. Stern, "Challenges and opportunities in software-driven medical devices," *Journal of Nature Biomedical Engineering*, vol. 3, no. 7, pp. 493-497, Jul. 2019.
- [16] J. Y. Park, Y. Lee, Y. W. Choi, R. Heo, H. K. Park, and S. H. Cho, et al., "Preclinical evaluation of a noncontact simultaneous monitoring method for respiration and carotid pulsation using impulse-radio ultra-wideband radar," *Journal of Scientific Reports*, vol. 9, no. 1, p. 11892, Aug. 2019.

AUTHORS



Faiza Sabir has received her B.S. degrees in the Department of Software Engineering from Bahria University, Pakistan, in 2017. In 2022, he joined the Department of Computer Engineering for pursuing her M.S. degree at Kyonggi University. Her research interests include Software safety, Model checking and Machine learning. She is currently M.S. student in Software Safety Lab, Kyonggi University.



Sarfaraz Ahmed has received his B.S. degrees in 2012 from Bahria University, Pakistan. He received his M.S. degree from NED university, Pakistan. Further, he completed his Ph.D. degree in 2023 from Hanyang University, Seoul, South Korea. His research area belongs to Signal processing for medical diagnosis in digital healthcare applications.



Gi Hwon Kwon has received B.S. degree in 1985 from Kyonggi University, Suwon, Korea and M.S. degree and Ph.D. degree from Chungang Korea, Seoul, Korea in 1987 and 1991, respectively. Since then, he has worked as a professor for the school of AI Computer Engineering at Kyonggi University. He also serves as the dean for the college of Software Management. His research interests are software engineering, formal verification, and software safety.