IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 21, 2020, accepted June 8, 2020, date of publication June 17, 2020, date of current version July 2, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3003032

Medical Device Safety Management Using Cybersecurity Risk Analysis

DONG-WON KIM[1], JIN-YOUNG CHOI[1], (Member, IEEE), AND KEUN-HEE HAN[2]
[1]Information Security Department, Korea University, Seoul 02841, South Korea
[2]Software Security Department, Korea University, Seoul 02841, South Korea

Corresponding author: Keun-Hee Han (khhan@formal.korea.ac.kr)

This research was supported by the Konyang University Research Fund of 2019.

ABSTRACT Hospital biomedical engineering teams are responsible for establishing and regulating medical equipment management programs (MEMPs); these programs ensure the safety and reliability of medical devices. Concomitant with rapid technological advancements, medical devices have been developed that are now being integrated with information and communication technology. However, with the convergence of such diverse technologies, internal and external security threats are continuously increasing. Thus, to reduce medical device security threats, important devices must be identified and prioritized. In this study, we propose a multicriteria decision-making model that prioritizes medical devices by extending the Fennigkoh and Smith model to include security threats. First, we formulate criteria for evaluating medical device functions based on the classification of the medical devices according to their unique functions, connections, and data types. Then, through threat modeling, we develop a method of identifying and evaluating security threats to these devices. We discuss establishing a safer MEMP by analyzing the attack occurrence probability (AOP) and attack success probability (ASP) of medical devices and the inherent security threats that these devices face, none of which are considered in the existing model. Thus, by using the enhanced Fennigkoh and Smith model, our proposed approach enables the development of improved security-enhanced MEMPs, including cybersecurity risk assessments.

INDEX TERMS Biomedical equipment, cybercare, security management.

I. INTRODUCTION

The unexpected nature of risks associated with the use of medical devices and equipment causes the safety of such devices and equipment to be constantly under threat; these threats can lead to physical damage or financial loss to people. This problem is further exacerbated by the proliferation and combination of medical devices and equipment [1]–[4]. Risk management—the use of a system or activity to analyze and evaluate risks that can occur during the lifespan of a product and to mitigate them to permissible levels [5]—is necessary to prevent or reduce such damage. In light of the continuous technological advancements being made in various fields, the importance of risk management is also increasing. While risk management is essential in various industries, it is particularly important in medicine, wherein safety is of the utmost importance because medical devices are used on human patients.

In recent times, with the development of Internet of Things (IoT) technology, the interconnection of various devices, objects, and systems without restrictions on time and location for enhanced control and operational ease is becoming inevitable, with fields such as medicine and electronics at the center of this advancement [6]. Healthcare will soon be delivered as a seamless continuum of care, instead of the clinic-centered point-of-care model, with an increased focus on prevention and early intervention [7]–[11].

Implantable medical devices (IMDs) are already enabling a shift in healthcare models. IMDs are electronic devices implanted in the human body that can be used to monitor patient health conditions; enable, support, or improve bodily functions; and treat diseases [12]. Examples of currently available IMDs include automated external defibrillators that monitor heart conditions and restore its normal rhythm when necessary, deep brain stimulators for patients with epilepsy or Parkinson's disease, drug delivery systems using infusion pumps, and various sensors to collect and process vital signs [13]. Furthermore, IMDs equipped with advanced

The associate editor coordinating the review of this manuscript and approving it for publication was Luis Javier Garcia Villalba.

computing and communication capabilities have several benefits for patients; however, these advanced IMDs also present numerous security and privacy threats. In some cases, IMDs can also result in fatalities; for example, intentionally tampering with an IMD can cause death [1], [12], [14]–[23]. The US Food and Drug Administration (FDA) has also acknowledged that it is significantly more difficult to detect intentional attacks than accidental attacks [24].

IMDs store and transmit extremely sensitive healthcare information, which should be protected in accordance with EU and US guidelines (e.g., 95/46/ECC and CFR 164.312, respectively) [25], [26]. Among the potential attacks on wireless IMDs, techniques to deactivate or reprogram onboard therapy functions and deliver shocks to patients have been proven possible in experimental settings [14]–[16]. Moreover, intentional battery drain to prevent the operation of an IMD has also been reported; in such situations, surgery is often required. The power to a cardiac IMD can easily be turned off using magnetic fields [17]. Because of this concern, former US Vice President Dick Cheney had the wireless feature in his implantable cardioverter defibrillator disabled [18].

As discussed earlier, because medical devices significantly influence the lives and welfare of patients, the importance of security management for such devices is continuously increasing [19]. In particular, cybersecurity for the processing and management of large amounts of data transmitted wirelessly from existing fixed-line communication infrastructure is indispensable, and this need has only increased with the development of electronic medical devices [19]. The feasibility of hacking medical devices has already been reported [20], [21] and security incidents in healthcare have been shown to be plausible.

Overall, although medical devices and equipment play critical roles in healthcare, they can be harmful if improperly used, maintained, or managed. Considering this, in this study, an approach was developed to assess medical device security risks based on security threats and vulnerabilities according to the type of medical device. Using this approach, safer medical equipment management programs (MEMPs) can be established; in addition, the reported results can be used to improve the Fennigkoh and Smith risk-assessment model for medical devices by incorporating various approaches to study and assess cybersecurity risks that are currently not considered in the model.

In this study, the Fennigkoh and Smith model was chosen for extension because it has been approved by the "Joint Commission on Accreditation of Healthcare Organizations" as a standard (EC6.10) and is commonly used in assessing the risks of medical devices [54].

The remainder of this paper is organized as follows. Section II presents the motivation and background for this study. Section III describes the research methodology and presents the criteria and risk analysis methods for assessing the functions, risks, and maintenance requirements of medical devices. In particular, via use-case scenarios, we demonstrate the selection of the most relevant modeling techniques according to application requirements using tables. Section IV discusses the feasibility and limitations of our proposed method. Finally, Section V summarizes our findings and outlines the directions for future research related to our study.

II. RESEARCH BACKGROUND

A. TRENDS IN MEDICAL DEVICE SECURITY BY COUNTRY AND INTERNATIONAL STANDARDS (ISO)

Although a wide range of industries require risk management, it is particularly crucial in medicine because patient safety is of the utmost importance. The current trends of medical device security management in major countries are summarized in Table 1.

Security measures for the protection of medical devices are actively being researched worldwide and international standards are being developed for them. Table 2 lists the current international standards regarding medical device security.

B. RESEARCH ON MEDICAL DEVICE RISK MANAGEMENT

Biomedical engineering departments in hospitals are responsible for establishing and regulating MEMPs to ensure the safety and reliability of medical devices [54]. To achieve this objective, important medical equipment must be identified and prioritized [54]. As the number and complexity of medical devices steadily increase, hospitals must also develop and regulate MEMPs, so that important medical devices are safe and reliable and operate at the required performance level [54].

In addition, as previously indicated, with technological advancements, medical devices with significant interconnection capabilities are being developed [1], and as diverse technologies converge, internal and external security threats increase.

Attacks on critical medical devices threaten patient safety [15]. Experimentally controlled cyberattacks on medical devices have targeted implantable cardiac defibrillators [16], wearable insulin pumps [4], and tele-operated surgical robots [55]. The US Department of Homeland Security warned recently that numerous medical devices made by Medtronic are vulnerable to cyberattacks [56]; the US federal government and General Electric (GE) Healthcare have also announced that certain of the company's patient monitoring devices are vulnerable to cyberattacks [57].

Fennigkoh and Smith proposed a risk-assessment method that groups medical devices based on their equipment management (EM) score, i.e., the sum of values assigned to the criticality of the device's function, physical risk (PR), and maintenance required [54], [58]:

$$\text{EM} = \text{Critical Function} + \text{PR} + \text{Required Maintenance}. \tag{1}$$

TABLE 1. Medical device security trends in major countries.

Country	Organization	Notes
US	FDA [1]	• Medical device cybersecurity guidance • Pre- and post-market management of cybersecurity in medical devices • FDA cybersecurity safety communications • Workshops and webinars on cybersecurity: Cybersecurity in medical devices
	GAO [27]	• Recommendations to FDA regarding medical device information security
	HIMSS [28]	• Manufacturer disclosure statement for medical device security
	DHS [29]	• ICS-CERT Alert (Medical Devices)
	HITRUST [30]	• Practical cybersecurity for medical devices
	HIPAA [31]	• Health Insurance Portability and Accountability Act
Europe	EU [32—34]	• The European Commission (EC), European Public Health Alliance (EPHA), and European Medicines Agency (EMA) provide three sets of medical device guidelines that are in place under EU management • Medical device regulations, active IMD regulations, and in vitro diagnostic device regulations • EU General Data Protection Regulation • Guidance on cybersecurity for medical devices
Japan	IPA [35,36]	• Healthcare information security manual for manufacturers • Security risk-assessment guide for industrial control systems • Remote service security guidelines • Establishes policies to facilitate the development and distribution of medical devices, and maintains a technology task force • Created remote service security guidelines and a healthcare information security manual for manufacturers in coordination with JIRA
Korea	KISA [37]	• Cybersecurity guide for smart medical services
	KHIDI [38]	• Information protection guidelines for healthcare institutions

TABLE 2. International standards on medical device security.

Standard	Focus area
IEC 62304 [39]	• Medical device software, software life cycle processes
IEC 80001-1 [40]	• Application of risk management for IT networks incorporating medical devices
ISO 14971 [41]	• Application of risk management for medical devices
ISO 13485 [42]	• Medical devices, quality management systems, requirements for regulatory purposes
ISO 60601-1 series [43]	• Medical electrical equipment, Part 1: General requirements for basic safety and essential performance • Medical electrical equipment, general requirements for basic safety and essential performance, collateral standard
ISO 60601-2series [44]	• Medical electrical equipment, particular requirements for basic safety and essential performance standards
IEC 62366-1 [45]	• Medical devices, application of usability engineering for medical devices
IEC 82304-1 [46]	• Health software, Part 1: General requirements for product safety
ISO/DTS ISO 11633-1 [47]	• Health informatics, information security management for remote maintenance of medical devices and medical information systems, Part 1: Requirements and risk analysis
ISO/TR 11633-2 [48]	• Health informatics, information security management for remote maintenance of medical devices and medical information systems, Part 2: Implementation of an information security management system
ISO/AWI TR 22696 [49]	• Guidance for an identification and authentication framework of networked personal health devices
ISO 27799 [50]	• Information security management in health using ISO/IEC 27002
ISO 10993-x [51]	• Biological evaluation of medical devices standards
UL 2900-2-1 [52,53]	• Standard for software cybersecurity for network-connectable products

The Joint Commission on Accreditation of Healthcare Organization recognized the importance of Fennigkoh and Smith's method in 1989 [58] and eventually approved it as a standard in 2004 [54].

With technological advancements, medical devices are being implemented with information and communication technology (ICT) capabilities. The handling and management of large volumes of wirelessly transmitted data necessitates security management; however, the evaluation of security management approaches against modern cybersecurity risks is not possible using the existing model alone [58]. This is because the Fennigkoh and Smith model considers only the critical function, PR, and maintainability values of a given device. To address this gap, we propose a medical device risk management method based on security criticality for cybersecurity risk assessment.

III. METHODS

A. SECURITY CRITICALITY ASSESSMENT MODEL FOR MEDICAL DEVICES

A medical device is an instrument, a machine, an apparatus, a material, or a similar product used independently or in combination with another device to (1) diagnose, treat, alleviate, or prevent a disease; (2) diagnose, treat, alleviate, or correct an injury or disorder; (3) test, replace, or transform a structure or function; and (4) control pregnancy in animals

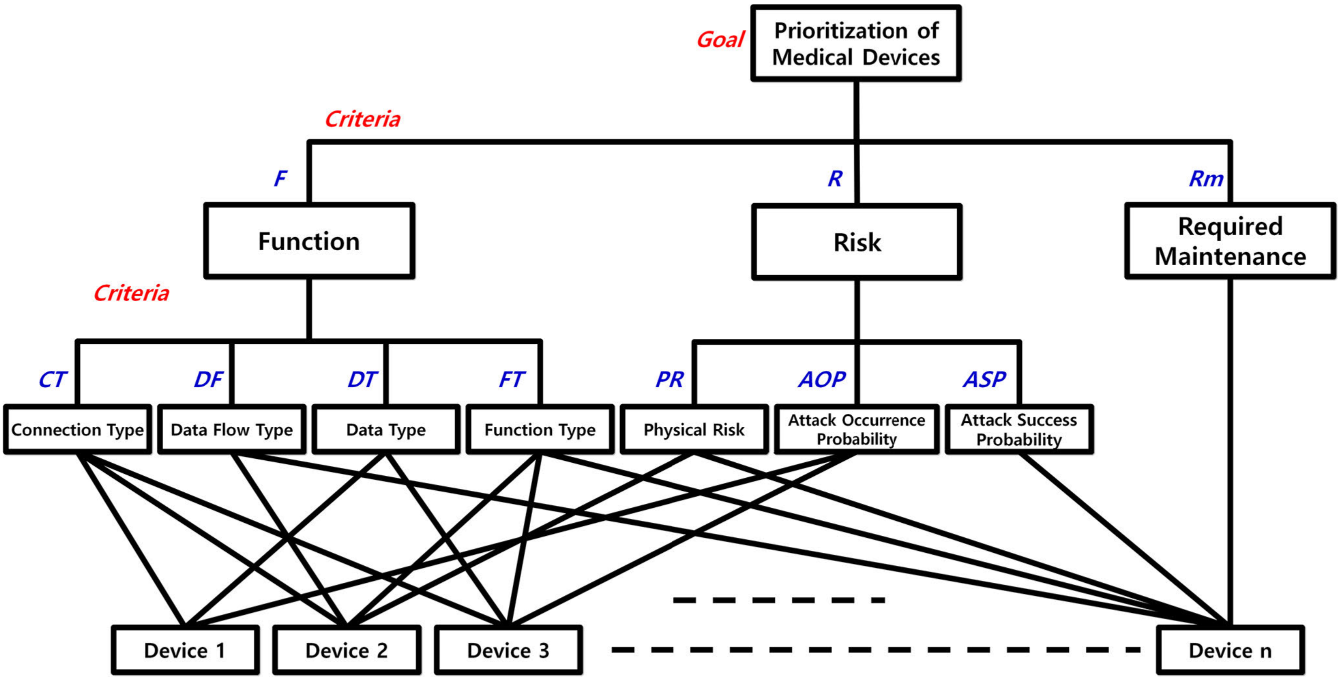


FIGURE 1. Decision-making model for medical device prioritization [54].

or humans [59]. The FDA forecasts that medical devices will transition to software because software is playing an increasingly important role in the medical field [60]. Accordingly, it is essential to develop a method to evaluate the safety and security of software implemented in medical devices for diagnostic and healthcare purposes [22].

In this study, we use the analytic hierarchy process (AHP) [54], [61] to address the complex problem of assessing the security criticality of medical devices. AHP is a powerful analytical method for assessing complex problems with several objectives or evaluation criteria; in particular, the evaluation criteria are stratified and decomposed into their main and detailed factors, and then, their importance is calculated through duality comparison. The AHP method for analyzing a complex problem by decomposing it into a hierarchical three-stage process is widely used for prioritization analysis [62]. Fig. 1 illustrates the decision-making model for medical device prioritization, considering the security risk associated with AHP.

In general, model creation in all threat tree-based methodologies starts with the identification of a threat event represented as the root node. Then, depending on the specific approach, the causes or consequences of the event are deduced and depicted as refining nodes [54], [74]–[80].

Fig. 1 has been expanded to consider security based on previous studies [54]. The evaluation criteria constitute the second stage of the hierarchical structure. In our proposed approach, medical devices are prioritized based on the sum of values assigned to the critical function, PR, cybersecurity risk, and maintenance. These formalisms provide a systematic, intuitive, and practical representation of several different possible attacks, vulnerabilities, and countermeasures; moreover, they also allow for an efficient formal and quantitative analysis of security scenarios. Thus, the contribution of this work is provision of a complete overview of the field and systematization of existing knowledge [74], [75], [79], [80].

Medical device risk analysis follows a three-step process, as illustrated in Fig. 1.

- [Step 1] Evaluation based on the function of medical devices (connection type, data flow type, data type, function type).
- [Step 2] Assessment of the security risk (attack occurrence probability, attack success probability) and physical risk (physical risk).
- [Step 3] Assessment of the maintenance requirements of the medical devices.

The step-by-step analysis and evaluation methods to establish a secure MEMP are described in detail in the following subsections.

B. MEDICAL DEVICE FUNCTION EVALUATION CRITERIA

In healthcare institutions, medical devices such as machines and equipment are managed as fixed assets, whereas consumable medical devices (e.g., insulin syringes) are not. The number of medical devices managed as fixed assets ranges from several thousands to several tens of thousands, depending on the hospital size. In some cases, medical instruments may be managed as consumable medical devices (blood glucose meter, Barovac, etc.).

Because different healthcare institutions have different medical device classification criteria and systems, it is difficult to agree on a single set of definitions for medical devices.

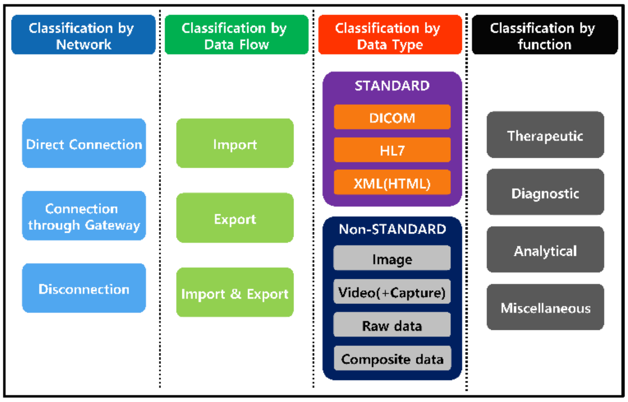


FIGURE 2. Classification of medical devices according to type.

Factors to consider for medical device security evaluation include the unique function and purpose of the medical device, type, and purpose of the included network connection, and data type (standard, non-standard).

The data generated or handled by medical devices are binary and digital signal data, which do not take into account classification at the information level (public, private, confidential, secret, top-secret, etc.). The data generated from medical devices can be identified and classified based on a standard (HL7, DICOM, etc.) in the Healthcare Information System (HIS) or Picture Archiving and Communication System (PACS). Thus, in this study, data types are classified as either standard or non-standard.

As illustrated in Fig. 2, medical device capability, considering security, is classified and evaluated according to the type of network connection (direct connection, gateway, or disconnected), data flow (import, export, or mixed), data type (standard or non-standard), and unique function of the medical device (therapeutic, diagnostic, analytical, or miscellaneous).

To help US institutions of all classes comply with the Federal Information Security Management Act, the US National Institute of Standards and Technology (NIST) developed the Risk Management Framework (RMF) to integrate and describe relevant standards and guidelines [64]. The RMF promotes risk management activities using the security life cycle approach, which comprises the following six steps: categorization based on the potential impacts of risks to information and the system from the perspectives of confidentiality, integrity, and availability; selection of minimum security controls based on such factors as minimal security requirements and cost analysis; implementation of the security controls in accordance with the security environment; assessment of whether the desired outcome has been derived from the implementation; authorization of the operation of an information system based on decision-making regarding risk with respect to organizational operation and assets; and monitoring of security situations.

The Federal Information Processing Standards Publication 199 (FIPS PUB 199) defined standards for categorizing information and information systems based on the potential impacts on an organization in order to provide a common framework and understanding for expressing security. The publication defined security objectives—confidentiality, integrity, and availability—and categorized the potential impacts of security breaches on individuals or organizations as low, moderate, and high [63].

Medical devices differ in importance according to their functions. For example, life-support devices must be protected from internal and external attacks because they serve to maintain the lives of patients. Functional evaluation, which is based on the Fennigkoh and Smith model, involves using a total function value that is determined by summing individual values assigned to each of the functions of the medical device under consideration, as indicated below. The function value (FV) is the total value (3–12 points) determined by evaluating function F and summing across the relevant areas according to the function of the device (e.g., connection type (CT), data flow type (DF), data type (DT), and function type (FT)):

$$FV = \sum_{i=1}^{n} F_i. \tag{2}$$

Medical devices are graded using a three-point classification scale, which is described in Table 3 [5], [41], [65], [66]. Specifically, a score is determined for each area, then a total FV is computed by adding the area-specific scores, after which the evaluation grade is determined based on the total FV. The FT is determined by appropriately applying the equipment function criteria of the Fennigkoh and Smith model [67] (Table 4).

As presented in Table 3, for the FV, the impact level is evaluated in terms of CT, DF, DT, and FT. Area-specific values are added using (2) to obtain a total FV ranging from 5 to 18 points. The total FVs are then categorized into prioritization grades 1–5. Table 5 lists the definitions of the criticality categories based on the FVs obtained via the method described above.

For function evaluation, risk is determined by appropriately applying international criteria, namely ISO/IEC 27005 [5] and ISO 31000 RM [65], conducting risk assessment based on NIST 800-37 RMF [66] and FIPS PUB 199, and performing failure mode, effect, and criticality analyses [68].

C. USE CASES

As an example, consider a pulse oximeter, which has a CT of 2 (connection through gateway), DF of 1 (export), DT of 2 (nonstandard, raw data), and FT of 6 (additional physiological monitoring and diagnostic). Thus, the FV of a pulse oximeter can be computed as follows:

$$\begin{aligned} \mathrm{FV} &= \mathrm{CT} + \mathrm{DF} + \mathrm{DT} + \mathrm{FT} \\ &= 2 + 1 + 2 + 6 \\ &= 11 \end{aligned} \tag{3}$$

Hence, a pulse oximeter has a total FV of 11, and thus, it can be classified as a medical device with a Grade 4 function.

TABLE 3. FV evaluation criteria [5], [41], [65], [66].

Division		Potential impact	Point	Description
CT	Direct connection	High	3	Medical devices directly connected to a network. High probability of network security threat.
	Connection through gateway	Moderate	2	Medical devices connected to a network through a gateway. Probability of a security threat occurring indirectly through the network.
	Disconnection	Low	1	Medical devices not connected to a network. Zero probability of network security threat, but some probability of physical security threat.
DF	Import and export	High	3	Medical devices with input and output capabilities. Some probability of security threat.
	Import	Moderate	2	Medical devices with input capability only. Some probability of security threat.
	Export	Low	1	Medical devices with output capability only. Low probability of security threat.
DT	Nonstandard	High	2	Medical devices with nonstandard data (raw data, capture, logarithms, etc.). High probability of unknown insider security threat.
	Standard	Low	1	Medical devices with standard data type (DICOM, HL7, XML, etc.). Standardized security measures are implemented.

TABLE 4. Equipment function [67].

Category	Function Description	Point
Therapeutic	Life support	10
	Surgical and intensive care	9
	Physical therapy and treatment	8
Diagnostic	Surgical and intensive care monitoring	7
	Additional physiological monitoring and diagnostic	6
Analytical	Analytical laboratory	5
	Laboratory accessories	4
	Computers and related	3
Miscellaneous	Patient related and other	2

TABLE 5. Criteria for function evaluation [5], [65], [66], [68].

Importance grade	Total score	Description
1	5–6	Medical devices that have no network capabilities, use standard protocols, have data export capability, and are classified as analytical or miscellaneous.
2	7–8	Medical devices that have some network capabilities, use standard and nonstandard protocols, have data export and import capabilities, and are classified as analytical or miscellaneous.
3	9–10	Medical devices that have network capabilities through a gateway, use standard and nonstandard protocols, have data export capability, and are classified as diagnostic, analytical, or miscellaneous.
4	11–15	Medical devices that are connected to a network either directly or through a gateway, use nonstandard protocols, have data import and export capabilities, and are classified as therapeutic or diagnostic.
5	16–18	Medical devices that are directly connected to a network, use nonstandard protocols, have data import and export capabilities, and are classified as therapeutic.

Fig. 3 depicts an example of the function assessment for a pulse oximeter.

Fig. 3 shows the function evaluation use case of a pulse oximeter used in hospitals. Pulse oximeters will vary depending on the vendor; however, the connection type of a pulse oximeter will still be ‘‘connected via a gateway’’: CT=2.

Because the pulse oximeter uses a data format defined by the vendor instead of a standard data format, it is connected to hospital information system (HIS) via standardization or normalization on the gateway. Therefore, depending on the evaluation criteria described above, the following points will be included: CT=2, DF=1, and DT=2. Furthermore, because the pulse oximeter is a medical device that monitors oxygen saturation, it belongs to the ‘‘diagnostic’’ category, with FT=6, as shown in Table 4, which specifies ‘‘additional physiological monitoring and diagnosis.’’

It should be noted that Fig. 3 is just a use-case example, and connection methods, data types, and data flow may vary because of different system configurations between hospitals.

D. CRITERIA FOR MEDICAL DEVICE RISK ASSESSMENT

As previously specified, with technological advancements made in recent years, medical devices are being integrated with ICT capabilities [1]. Because such devices are closely linked to patient lives and welfare, management of their security is crucial. Integrating the healthcare enterprise (IHE) defines medical device security threats; these are presented in Fig. 4. To identify medical device risks, Badawi *et al.*

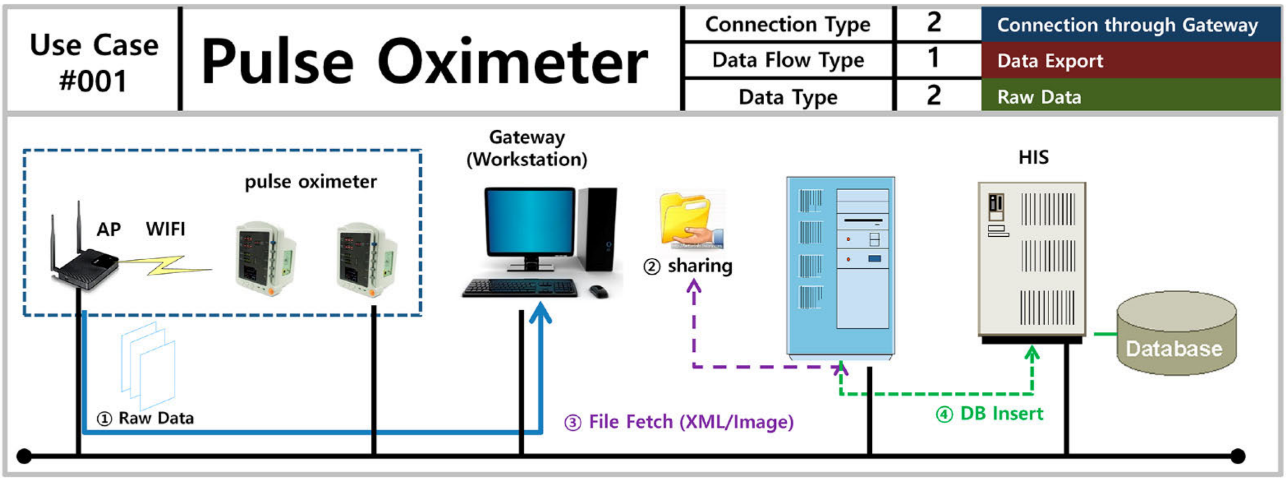


FIGURE 3. Function assessment use case for a pulse oximeter.

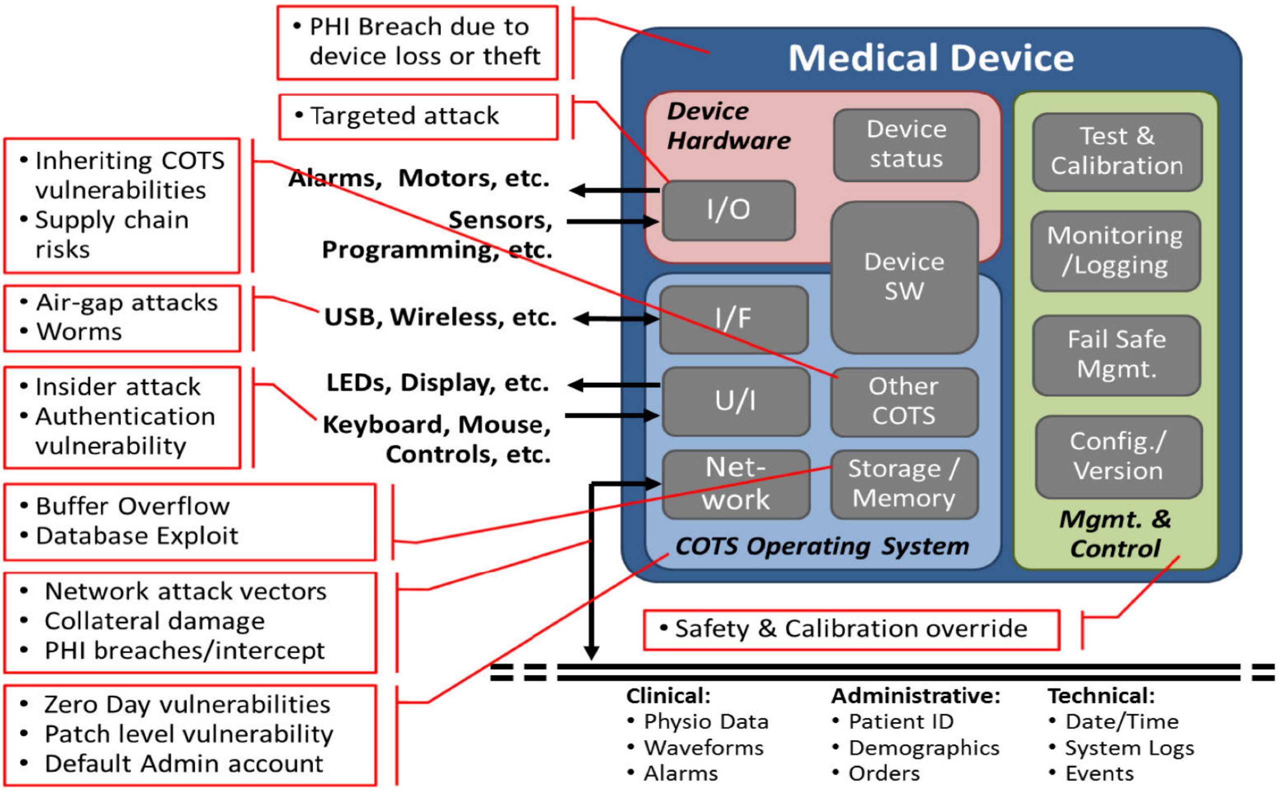


FIGURE 4. IHE medical device security threat examples [1].

analyzed a potential threat using a pulse oximeter as an example; this analysis is depicted in Fig. 5 [69].

Once a threat is analyzed, the attack tree method is used to compute the actual attack occurrence probability (AOP). The attack tree technique, which was introduced by Schneier, is a systematic method of defining the security features of a system according to various attacks [70], [74]–[80]. In this method, the AOP is calculated based on OR and AND connectors with the premise of achieving an attack goal at each node representing an attack.

1) AOP

In the use case described herein, an AOP was computed using the attack tree method. The AOP is defined as the ratio of attack event occurrences at a child node to those at a parent node to achieve an attack goal at the child node. AOPs are computed in the following manner [71].

If child node x is a leaf node, AOP $= 1$ (see (4) and (5)). If x is reached as a combination of AND connectors, then

$$\text{AOP} = \frac{\text{number of AND combinations}}{\text{number of x}}. \tag{4}$$

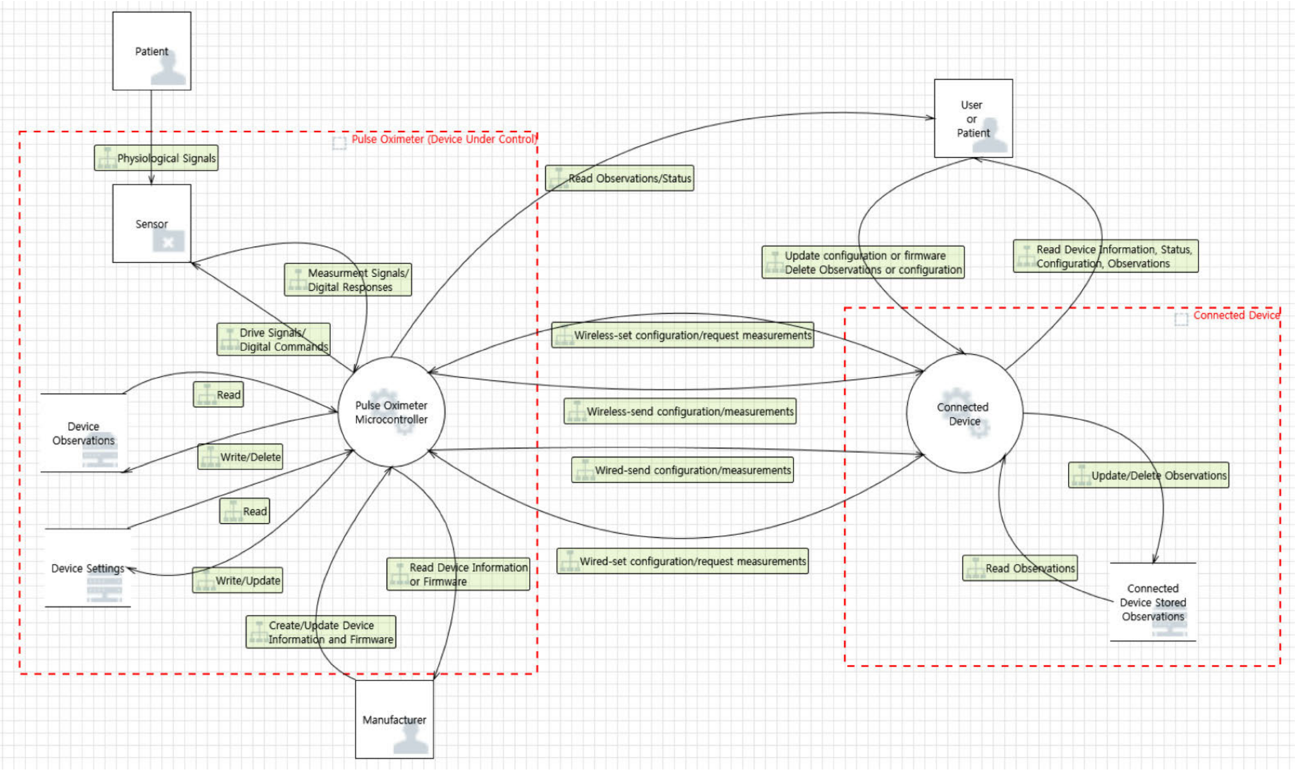

Patient
Pulse Oximeter (Device Under Control)
Physiological Signals
Sensor
Measurment Signals/ Digital Responses
Drive Signals/ Digital Commands
Read
Device Observations
Write/Delete
Read
Device Settings
Write/Update
Pulse Oximeter Microcontroller
Read Device Information or Firmware
Create/Update Device Information and Firmware
Manufacturer
Read Observations/Status
User or Patient
Update configuration or firmware Delete Observations or configuration
Read Device Information, Status, Configuration, Observations
Connected Device
Wireless-set configuration/request measurements
Wireless-send configuration/measurements
Wired-send configuration/measurements
Wired-set configuration/request measurements
Connected Device
Update/Delete Observations
Read Observations
Connected Device Stored Observations

FIGURE 5. Pulse oximeter threat model example [69].

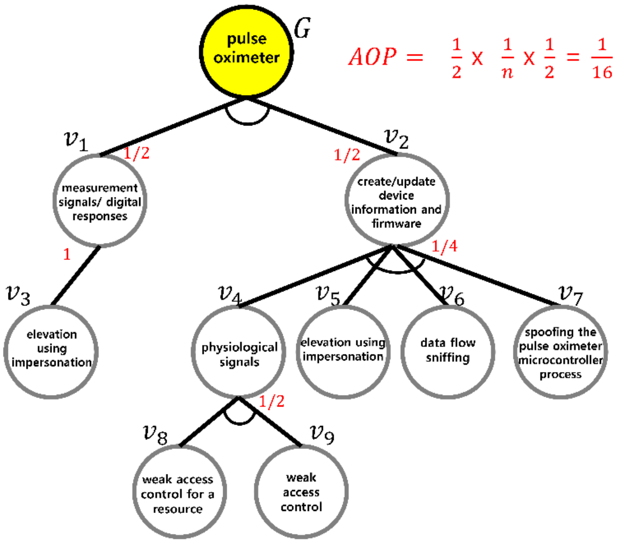

pulse oximeter
G
AOP = 1/2 x 1/n x 1/2 = 1/16
v_1
1/2
v_2
1/2
measurement signals/ digital responses
create/update device information and firmware
1
1/4
v_3
elevation using impersonation
v_4
physiological signals
v_5
elevation using impersonation
v_6
data flow sniffing
v_7
spoofing the pulse oximeter microcontroller process
1/2
v_8
weak access control for a resource
v_9
weak access control

FIGURE 6. Pulse oximeter attack tree example.

Otherwise, if x is a combination of ORs, then

$$\text{AOP} = \frac{1}{\text{number of x}}. \tag{5}$$

These attack tree scenarios are limited because each node is assigned the same weight, even though nodes are not the same in terms of threat level, and the extent of damage due to a threat differs among nodes as well. In addition, the scenarios do not compare the AOPs across each of the nodes, but rather only show the probability of achieving an attack goal from a lower node to an upper node. Because the frequency of attack occurrences and extent of a threat are not considered at each node, the quantification of the level of medical device security threat is limited. Thus, AOPs are computed by designing an attack tree based on each of the medical device security threat scenarios, as shown in the example in Fig. 6.

TABLE 6. AOP evaluation criteria.

Division	Low	Moderate	High
	1	2	3
AOP	1–50%	51–80%	81–100%

The computation of AOPs based on the example shown in Fig. 6 is described below. The AOP at ν_4 is 1/2, because there are two paths to ν_4, through ν_8 and through ν_9. One of four ways, through ν_4, ν_5, ν_6, or ν_7, should be selected to arrive at ν_2; thus, the AOP is 1/4. To arrive at ν_1, the single node ν_3 is selected; therefore, the AOP is one. Thus, if an attack targets a user or patient, the AOP of patient information theft is 6.25%, which can be computed as follows:

$$AOP = \frac{1}{2} \times \frac{1}{4} \times \frac{1}{2} = \frac{1}{16} \times 100. \tag{6}$$

The AOPs calculated at each of the nodes of an attack tree designed according to the medical device security threat are categorized using the three-level classification system shown in Table 6.

TABLE 7. RATINGS of aspects of attack potential.

Factor	Level	Value
Elapsed time	≤1 day	0
	≤1 week	1
	≤1 month	4
	≤3 months	10
	≤6 months	17
	>6 months	19
	Not practical	∞
Expertise	Layman	0
	Proficient	3
	Expert	6
	Multiple experts	8

Factor	Level	Value
Knowledge of system	Public	0
	Restricted	3
	Sensitive	7
	Critical	11
Window of opportunity	Unnecessary/unlimited	0
	Easy	1
	Moderate	4
	Difficult	10
	None	∞
Equipment	Standard	0
	Specialized	4
	Bespoke	7
	Multiple bespoke	9

TABLE 8. ASP ratings.

Value	Attack potential required to identify and exploit attack scenario	ASP
0–9	Basic	5
10–13	Enhanced-basic	4
14–19	Moderate	3
20–24	High	2
≥25	Beyond high	1

2) ATTACK SUCCESS PROBABILITY (ASP)

The definition of ASP can be found in ISO/IEC 15408 [72] and ISO/IEC 18045 [73]. In essence, ASP increases as the effort required to perform an attack decreases and the motivation of the attacker increases. The following factors are considered in the evaluation of ASP [73].

- Time taken by an attacker to identify a vulnerability, develop an attack method, and execute the attack;
- Specialist expertise required;
- Knowledge of the system under investigation;
- Window of opportunity to access the target of the attack;
- IT hardware/software or other equipment required to identify and exploit the vulnerability.

These factors are not mutually exclusive and may be substituted for each other, considering different perspectives. For example, professional skills or equipment may be substituted for each other or with time (Table 7). ASP is obtained by applying the values of the factors presented in Table 7 based on the medical device security threat (Table 7) and then classified into one of the five levels listed in Table 8 based on the criteria presented in Table 7. Once the ASP levels are determined, they are mapped onto leaf nodes of the attack tree. For example, each leaf node in Fig. 6 is annotated with the corresponding ASP level; some of these examples are listed in Table 9.

3) RISK

The risk value (RV) is computed by determining the PR, AOP, and ASP, which correspond to the characteristics of each of the terms, and multiplying them together to assess the risk grade:

$$RV = PR \times AOP \times ASP. \tag{7}$$

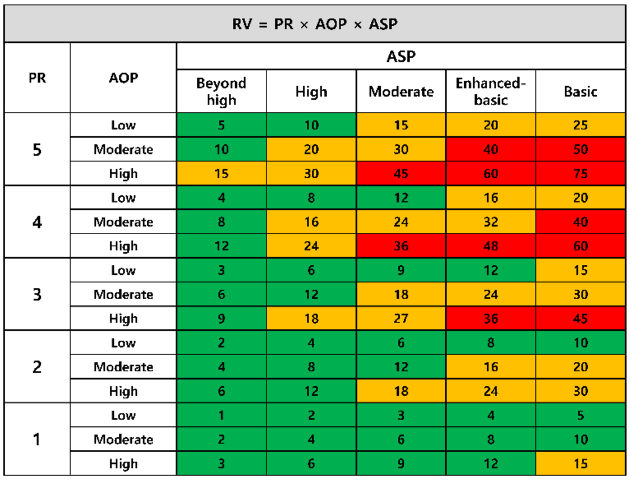
To determine PR, the criteria from the Fennigkoh and Smith model for PR are appropriately applied (Table 10) [67]. Once the RV is computed, the risk is assessed by using the classification system of “high (H),” “normal (M),” and “low (L),” as listed in Table 11 and shown in Fig. 7. As illustrated in Fig. 7, the risk level increases with increasing PR, AOP, and ASP.

E. CRITERIA FOR EVALUATING MAINTENANCE REQUIREMENTS

Maintenance requirements are determined by appropriately applying the criteria of the Fennigkoh and Smith model [67]. According to the model, types of equipment that are predominantly mechanical, pneumatic, or fluidic often demand the most extensive maintenance [67]. A device is considered to have an average maintenance requirement if it necessitates only performance verification and safety testing. Equipment that require only visual inspection, basic performance checks,

TABLE 9. Examples of ASP estimates.

Attack	Elapsed time	Expertise	Knowledge of system	Window of opportunity	Equipment	Required attack potential	
						Sum	Rating
Pulse oximeter spoofing	0	6	7	4	4	21	High
Elevation using impersonation	0	3	0	4	4	11	Moderate
Weak access control for a resource	0	6	3	10	4	23	High
Data flow sniffing	0	0	0	4	4	8	Basic



RV = PR × AOP × ASP

PR	AOP	ASP				
		Beyond high	High	Moderate	Enhanced-basic	Basic
5	Low	5	10	15	20	25
	Moderate	10	20	30	40	50
	High	15	30	45	60	75
4	Low	4	8	12	16	20
	Moderate	8	16	24	32	40
	High	12	24	36	48	60
3	Low	3	6	9	12	15
	Moderate	6	12	18	24	30
	High	9	18	27	36	45
2	Low	2	4	6	8	10
	Moderate	4	8	12	16	20
	High	6	12	18	24	30
1	Low	1	2	3	4	5
	Moderate	2	4	6	8	10
	High	3	6	9	12	15

FIGURE 7. Examples of RV estimates.

TABLE 10. PR classification.

Description of use risk	Point
Potential patient death	5
Potential patient or operator injury	4
Inappropriate therapy or misdiagnosis	3
Equipment damage	2
No significant identified risk	1

and safety testing are classified as having minimal maintenance requirements [54].

IV. DISCUSSION

We performed risk assessment for each of the medical devices listed in Table 13. The model proposed in this study includes all the criteria for medical device prioritization suggested in biomedical engineering (i.e., the Fennigkoh and Smith model).

The AHP method enables efficient formalisms that provide a systematic, intuitive, and practical representation of a large amount of possible attacks, vulnerabilities, and countermeasures; in addition, it allows for efficient formal and quantitative analysis of security scenarios.

In this study, data were collected through site verification and security vulnerability analysis (penetration testing, threat modeling) of 22 types of medical devices, as listed in Table 13, and models were analyzed based on hypotheses.

TABLE 11. RV ratings.

Values	Grade
1–12	Low
13–32	Normal
≥ 33	High

TABLE 12. Maintenance requirements.

Maintenance requirement	Point
Extensive: Routine calibration and part replacement required	5
Above average	4
Average: Performance verification and safety testing	3
Below average	2
Minimal: Visual inspection	1

In medical institutions, disposable materials and devices are also considered as medical devices; this poses limitations in classifying only medical devices that should be addressed from a cybersecurity perspective. From an attacker's perspective, the elements necessary to pose a risk to medical institutions through medical devices are connectivity and the importance (which can be of monetary benefit) of the information handled. Thus, connection type, data type, and direction of data transfer are important; in particular, the functional classification presented in Table 4 determines the importance of medical devices.

Table 3 lists a three-point classification approach based on the RMF [63], [64]; in addition, the functional importance of medical devices can be evaluated by referring to Table 5. An assessment of the functional importance of these medical devices will help to determine priorities based on the unique functional elements of medical devices from a security perspective.

Our proposed model estimates the total risk of a medical device, considering security threats by assessing ASP, AOP, and PR (Fig. 8). Hence, this research will enable the development of improved security-enhanced MEMPs, including cybersecurity risk assessments not considered in the existing security model by utilizing the enhanced Fennigkoh and Smith model.

A limitation of the model proposed in this study is that expert participation is required when applying the model to medical devices. More specifically, analysis of security threats in medical devices requires the participation of information security experts with medical expertise and the cooperation of biomedical engineering experts. In addition,

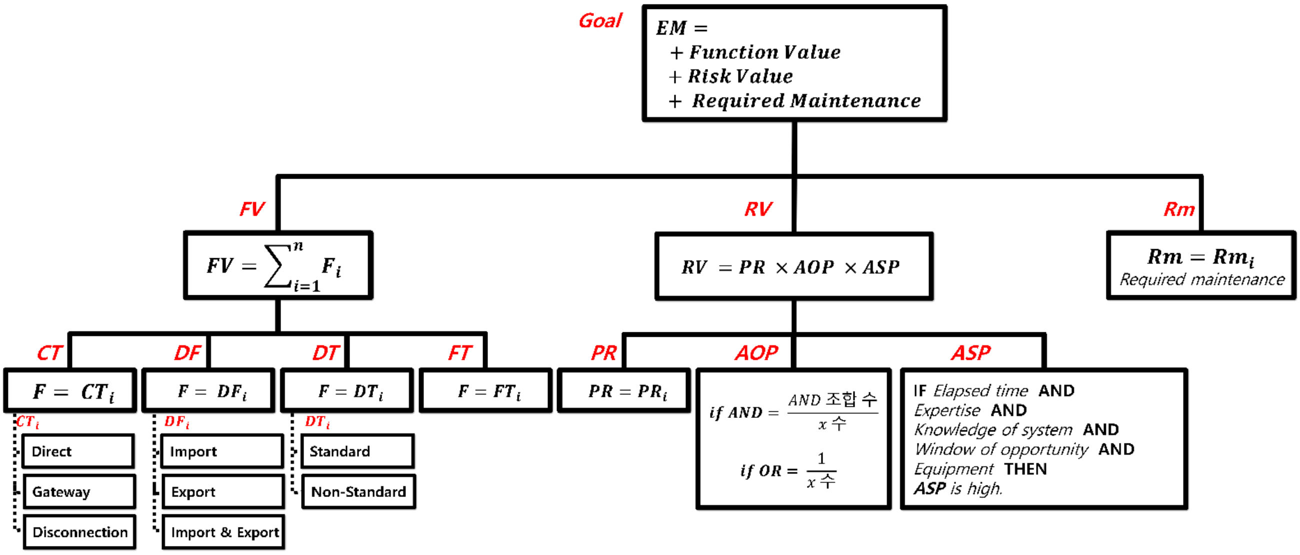


FIGURE 8. Decision-making model for medical device risk assessment.

TABLE 13. Examples of medical device risk assessment considering security.

No	Device name	$\mathbf{FV} = \sum_{i=1}^{n} F_i$					$\mathbf{RV = PR \times AOP \times ASP}$				Maintenance requirements	EM
		FT	CT	DF	DT	FV	PR	AOP	ASP	RV		
1	Infant incubator	Life support (10)	DR (3)	Export (1)	Raw data (2)	5	5	H (3)	BH (1)	N (2)	3	10
2	Defibrillator	Life support (10)	DR (3)	Export (1)	Raw data (2)	5	5	H (3)	BH (1)	N (2)	3	10
3	Intra-aortic balloon pump	Life support (10)	DR (3)	Export (1)	Raw data (2)	5	5	H (3)	BH (1)	N (2)	3	10
4	External pacemaker	Life support (10)	Dis (1)	Export (1)	Raw data (2)	4	5	H (3)	N (3)	H (3)	3	10
5	Neuro navigation	Surgical (9)	DR (3)	Import (2)	DICOM (1)	4	4	M (2)	BH (1)	N (2)	3	9
6	Gamma camera	Diagnostic (6)	DR (3)	Export (1)	DICOM (1)	4	3	M (2)	M (3)	N (2)	2	8
7	CT scanner	Diagnostic (6)	DR (3)	Export (1)	DICOM (1)	4	3	H (3)	M (3)	N (2)	3	9
8	CT scanner	Diagnostic (6)	DR (3)	Export (1)	Raw data (2)	4	3	H (3)	EB (4)	H (3)	3	10
9	Linac	Treatment (8)	DR (3)	Import (2)	DICOM (1)	4	3	H (3)	BH (1)	L (1)	3	8
10	Hemostatic dialysis machine	Treatment (8)	DR (3)	Export (1)	Raw data (2)	4	3	M (2)	H (2)	L (1)	2	7
11	Patient monitoring	Surgical monitoring (7)	DR (3)	Export (1)	Raw data (2)	4	3	M (2)	M (3)	N (2)	2	8
12	Patient monitoring	Surgical monitoring (7)	DR (3)	Export (1)	HL7 (1)	4	3	M (2)	M (3)	N (2)	2	8
13	Portable EKG	Analytical (5)	Gate (2)	Export (1)	Raw data (2)	3	3	M (2)	M (3)	N (2)	2	7
14	OCT & field analyzer	Analytical (5)	DR (3)	Export (1)	DICOM (1)	3	3	M (2)	H (2)	L (1)	2	6
15	CT	Analytical (5)	DR (3)	Import/Export (3)	DICOM (1)	4	3	H (3)	M (3)	N (2)	3	9
16	EEG	Analytical (5)	DR (3)	Export (1)	Raw data (2)	4	2	M (2)	M (3)	N (2)	3	9
17	Laboratory	Analytical (5)	Gate (2)	Export (1)	DB (2)	3	2	M (2)	H (2)	L (1)	3	7
18	Sonography workstation	Computer (3)	DR (3)	Export (1)	DICOM (1)	3	3	H (3)	B (5)	H (3)	2	8
19	Blood pressure modules	Diagnostic (6)	DR (3)	Export (1)	Raw data (2)	4	3	M (2)	H (2)	L (1)	2	7
20	Computer terminal	Analytical (5)	DR (3)	Import/Export (3)	Raw data (2)	4	2	H (3)	B (5)	N (2)	1	7
21	Water bath circulator	Analytical (5)	DR (3)	Import (2)	Raw data (2)	4	2	H (3)	M (3)	N (2)	2	8
22	Sterilizer	Miscellaneous (2)	Dis (3)	Export (3)	Raw data (2)	3	1	M (2)	M (3)	L (1)	1	5

discussions should be made on how to select meaningful values for ratings related to values calculated through expert participation (Figure 7). Naturally, these scores and thresholds may vary depending on different systems, so guidance will be needed on how these scores and thresholds can be selected.

Another limitation is that biomedical engineers may not always be able to accept the outcome of prioritization of security threats, and the weight of each criterion and/or the severity of the assigned security grade may have to be reassessed and reassigned. Nevertheless, this study contributes to the enhancement of medical device security by integrating AHP to facilitate the assessment and prioritization of cybersecurity risk factors for which prior research is lacking.

V. CONCLUSION

In this study, we proposed a multicriteria decision-making model to prioritize medical devices based on security threats against them. The model uses AHP to identify medical devices of high importance that need to be included in hospital MEMPs. The proposed hierarchical structure includes eight assessment criteria: CT, DF, DT, FT, PR, AOP, ASP, and maintenance requirements. The output of the model is an estimate of the total risk considering security threats assessed using ASP, AOP, and PR. In addition, the proposed model may be useful for establishing guidelines for the selection of appropriate maintenance strategies for medical devices by utilizing the scores of medical devices for individual criteria or a combination of several criteria.

We believe that our proposed model will be useful for biomedical engineering departments in hospitals to establish and regulate programs for safe and reliable medical equipment management. As the number and complexity of medical devices steadily increase, hospitals are required to establish and regulate MEMPs so that important medical devices are safely and reliably operated at the required security levels; our model is a step in that direction.

A limitation of our study is that, although the proposed security threat analysis model was validated through a simulated penetration test on some medical devices, verification of the model on additional medical devices is required to ensure feasibility for a large range of medical devices.

As future research, we will expand penetration testing (to include white box, black box, and fuzzy tests) to validate cybersecurity threats. Furthermore, the use cases for this testing will be developed in conjunction with medical institution certification programs (such as HL7, HL7 FHIR, ONC-HIT, CCHIT, IHE), and it will be implemented as a tool available in the field.

DATA AVAILABILITY

The data used to support the findings of this study are included in the manuscript.

CONFLICTS OF INTEREST

There are no conflicts of interest to declare regarding the publication of this paper.

REFERENCES

[1] *Medical Equipment Management (MEM): Medical Device Cyber Security*, document, IHE International, IHE PCD Technical Committee, Jul. 2015. [Online]. Available: https://ihe.net/uploadedFiles/Documents/PCD/IHE_PCD_WP_Cyber-Security_Rev1.0_PC_2015-07-01.pdf

[2] Y. Xu, D. Tran, Y. Tian, and H. Alemzadeh, "Poster abstract: Analysis of cyber-security vulnerabilities of interconnected medical devices," presented at the IEEE/ACM Int. Conf. Connect. Health, Appl. Syst. Eng. Technol. (CHASE), Sep. 2019, doi: 10.1109/CHASE48038.2019.00017.

[3] H. Almohri, L. Cheng, D. Yao, and H. Alemzadeh, "On threat modeling and mitigation of medical cyber-physical systems," presented at the IEEE/ACM Int. Conf. Connected Health, Appl. Syst. Eng. Technol. (CHASE), Jul. 2017, doi: 10.1109/CHASE.2017.69.

[4] T. Bonaci, J. Yan, J. Herron, T. Kohno, and H. J. Chizeck, "Experimental analysis of denial-of-service attacks on teleoperated robotic systems," in *Proc. ACM/IEEE 6th Int. Conf. Cyber-Phys. Syst.*, Seattle, WA, USA, Apr. 2015, pp. 11–20.

[5] *Information Security Risk Management*, Standard ISO/IEC 27005:2011, 2011.

[6] T.-Y. Kim, S. Youm, J.-J. Jung, and E.-J. Kim, "Multi-hop WBAN construction for healthcare IoT systems," presented at the Int. Platform Technol., Jan. 2015, doi: 10.1109/PlatCon.2015.20.

[7] B. Zhang, X. W. Wang, and M. Huang, "A data replica placement scheme for cloud storage under healthcare IoT environment," presented at the 11th Int. Conf. Fuzzy Syst. Knowl. Discovery, Aug. 2014, doi: 10.1109/FSKD.2014.6980892.

[8] M. Wehde, "Healthcare 4.0," *IEEE Eng. Manage. Rev.*, vol. 47, no. 3, pp. 24–28, Sep. 2019.

[9] N. Mohamed and J. Al-Jaroodi, "The impact of industry 4.0 on healthcare system engineering," in *Proc. IEEE Int. Syst. Conf. (SysCon)*, Orlando, FL, USA, Apr. 2019, pp. 1–7.

[10] M. Alloghani, D. Al-Jumeily, A. Hussain, A. J. Aljaaf, J. Mustafina, and E. Petrov, "Healthcare services innovations based on the state of the art technology trend industry 4.0," presented at the 11th Int. Conf. Develop. eSyst. Eng. (DeSE), Sep. 2018, doi: 10.1109/DeSE.2018.00016.

[11] C. Thuemmler and C. Bai, Eds., *Health 4.0: How Virtualization and Big Data are Revolutionizing Healthcare*. New York, NY, USA: Springer, 2017.

[12] J. A. Hansen and N. M. Hansen, "A taxonomy of vulnerabilities in implantable medical devices," in *Proc. 2nd Annu. Workshop Secur. Privacy Med. Home-Care Syst. (SPIMACS)*, Chicago, IL, USA, 2010, pp. 13–20.

[13] C. Camara, P. Peris-Lopez, and J. E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey," *J. Biomed. Informat.*, vol. 55, pp. 272–289, Jun. 2015.

[14] K. Fu, "Inside risksReducing risks of implantable medical devices," *Commun. ACM*, vol. 52, no. 6, pp. 25–27, Jun. 2009.

[15] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *Proc. IEEE Symp. Secur. Privacy (SP)*, Oakland, CA, USA, May 2008, pp. 129–142.

[16] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," presented at the IEEE 13th Int. Conf. e-Health Netw. Appl. Service, Jun. 2011, doi: 10.1109/HEALTH.2011.6026732.

[17] Medtronic. *Implantable Pacemaker and Defibrillator Information*. Accessed: Apr. 2015. [Online]. Available: http://www.medtronic.com/rhythms/downloads/3215ENp7_magnets_online.pdf

[18] T. Verge. (2013). *Dick Cheney Had The Wireless Disabled on His Pacemaker to Avoid Risk of Terrorist Tampering*. [Online]. Available: http://www.theverge.com/2013/10/21/4863872/dick-cheney-pacemaker-wireless-disabled-2007

[19] *Postmarket Management of Cybersecurity in Medical Devices*, U.S. Food Drug Admin., Silver Spring, MD, USA, Dec. 2016.

[20] N. Paul, T. Kohno, and D. C. Klonoff, "A review of the security of insulin pump infusion systems," *J. Diabetes Sci. Technol.*, vol. 5, no. 6, pp. 1557–1562, Nov. 2011.

[21] I. Ray and N. Poolsapassit, "Using attack TPees to identify malicious attacks from authorized insiders," presented at the 10th Eur. Symp. Res. Comput. Secur., Sep. 2005, doi: 10.1007/11555827_14.

[22] International Medical Device Regulators Forum. Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations. IMDRF Software as a Medical Device (SaMD) Working Group, 2014. Accessed: Jun. 9, 2015. [Online]. Available: http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-140918-samd-framework-risk-categorization-141013.pdf

[23] A. Tabasum, Z. Safi, W. AlKhater, and A. Shikfa, "Cybersecurity issues in implanted medical devices," presented at the Int. Conf. Comput. Appl. (ICCA), Aug. 2018, doi: 10.1109/COMAPP.2018.8460454.

[24] U.S. Food and Drug Administration. *Medical Device Safety*. Accessed: Nov. 2013. [Online]. Available: http://wireless.fcc.gov/services/index.htm?job=service_bandplan&id=medical_implant

[25] *Security Standards: Technical Safeguards*, U.S. Dept. Health Hum. Services, Washington, DC, USA, Apr. 2007, vol. 2, Paper 2. [Online]. Available: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf

[26] K. Summerhayes and S. Shivshankar, "Challenges of conducting medical device studies," Inst. Clin. Res., Tech. Rep., 2007.

[27] U.S. Government Accountability Office. *FDA Medical Device Reviews: Evaluation is Needed to Assure Requests for Additional Information Follow a Least Burdensome Approach*. Accessed: Jan. 16, 2018. [Online]. Available: https://www.gao.gov/products/GAO-18-140

[28] Healthcare Information and Management Systems Society. (Oct. 8, 2019). *Manufacturer Disclosure Statement for Medical Device Security*. [Online]. Available: https://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx#download

[29] U.S. Department of Homeland Security. *ICS-CERT Alerts*. Accessed: Mar. 2020. [Online]. Available: https://www.us-cert.gov/ics/alerts

[30] Health Information Trust Alliance. *Practical Cybersecurity for Medical Devices*. Accessed: May 21, 2019. [Online]. https://hitrustalliance.net/content/uploads/Healthcare_May21_200PM_PracticalCybersecurityMedicalDevices.pdf

[31] Health Insurance Portability and Accountability Act of 1996. *US Department of Health and Human Services*. Accessed: Sep. 14, 2018. [Online]. Available; https://www.cdc.gov/phlp/publications/topic/hipaa.html

[32] European Medicines Agency. *Medical Devices*. Accessed: Apr. 2017. [Online]. Available: https://www.ema.europa.eu/en/human-regulatory/overview/medical-devices

[33] European Union. *EU General Data Protection Regulation*. Accessed: Apr. 27, 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[34] EU Medical Device Coordination Group Document. *Guidance on Cybersecurity for Medical Devices*. Accessed: Dec. 16, 2019. [Online]. Available: https://ec.europa.eu/docsroom/documents/38941/attachments/1/translations/en/renditions/native

[35] Information-technology Promotion Agency. *In Medical Equipment Information Security Survey*. Accessed: Apr. 2014. [Online]. Available: https://www.ipa.go.jp/files/000038223.pdf

[36] Information-Technology Promotion Agency. *Security Risk Assessment Guide for Industrial Control Systems*. Accessed: Oct. 2019. [Online]. https://www.ipa.go.jp/files/000078098.pdf

[37] Korea Internet and Security Agency. *Cyber Security Guide for Smart Medical Service*. Accessed: May 2018. [Online]. Available: http://www.kisa.or.kr/uploadfile/201805/201805290956314977.pdf

[38] Korea Health Industry Development Institute. *Information Protection Guidelines for Healthcare Institutions*. Accessed: Dec. 2016. [Online]. Available: http://www.kosmi.org/rang_board/inc/download.php?code=notice&num=238

[39] *Medical Device Software: Software Life Cycle Processes*. Standard IEC 62304, 2015.

[40] *Application of Risk Management for IT-Networks Incorporating Medical Devices, Part 1: Roles, Responsibilities and Activities*, Standard IEC 80001-1:2010, 2010.

[41] *Medical Devices: Application of Risk Management to Medical Devices*, Standard ISO 14971:2007, 2007.

[42] *Medical Devices: Quality Management Systems: Requirements for Regulatory Purposes*, Standard ISO 13485:2016, 2016.

[43] *Medical Electrical Equipment Part 1: General Requirements for Basic Safety and Essential Performance*, Standard IEC 60601-1, 2012.

[44] *Medical Electrical Equipment Part 1–2: General Requirements for Basic Safety and Essential Performance-Collateral Standard: Electromagnetic Disturbances-Requirements and Tests*, Standard IEC 60601-2, 2014.

[45] *Medical Devices: Application of Usability Engineering to Medical Devices*, Standard IEC 62366-1, 2015.

[46] *Health Software, Part 1: General Requirements for Product Safety*, Standard IEC 82304-1, 2016.

[47] *Health Informatics—Information Security Management for Remote Maintenance of Medical Devices and Medical Information Systems—Part 1: Requirements and Risk Analysis*, ISO/DTS Standard 11633-1, 2019.

[48] *Health Informatics—Information Security Management for Remote Maintenance of Medical Devices and Medical Information Systems—Part 2: Implementation of an Information Security Management System (ISMS)*, Standard ISO/CD TR 11633-2, 2009.

[49] *Health Informatics—Guidance on the Identification and Authentication of Connectable Personal Healthcare Devices (PHDs)*, Standard ISO/TR 22696:2020, 2020.

[50] *Health Informatics—Information Security Management in Health Using ISO/IEC 27002*, Standard ISO 27799:2016, 2016.

[51] *Biological Evaluation of Medical Devices—Part 1: Evaluation and Testing Within a Risk Management Process*, Standard ISO 10993-1, 2018.

[52] *Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements*, UL Standard 2900-1, 2017.

[53] *Software Cybersecurity for Network-Connectable Products, Part 2–1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems*, UL Standard 2900-2-1, 2017.

[54] S. Taghipour, D. Banjevic, and A. K. S. Jardine, "Prioritization of medical equipment for maintenance decisions," *J. Oper. Res. Soc.*, vol. 62, no. 9, pp. 1666–1687, Sep. 2011.

[55] P. R. Prasad, S. Butakov, and F. Jaafar, "Information security considerations for wireless infusion pumps," presented at the IEEE Int. Conf. Softw. Quality Rel. Secur. Companion (QRS-C), Jul. 2018, doi: 10.1109/QRS-C.2018.00081.

[56] IEEE Spectrum. *Can 'Internet-of-Body' Thwart Cyber Attacks on Implanted Medical Devices*. Accessed: Mar. 28, 2019. [Online]. Available: https://spectrum.ieee.org/the-human-os/biomedical/devices/thwart-cyber-attacks-on-implanted-medical-devices

[57] Mass Device. *Certain GE Healthcare Patient-Monitoring Devices Vulnerable to Cyberattack*. [Online]. Available: https://www.massdevice.com/certain-ge-healthcare-patient-monitoring-devices-vulnerable-to-cyberattack/

[58] L. Fennigkoh and B. Smith, "Clinical equipment management," *JCAHO PTSM Ser.*, vol. 2, pp. 5–14, Jan. 1989.

[59] P. A. Williams and A. J. Woodward, "Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem," *Med. Devices, Evidence Res.*, vol. 8, pp. 305–316, Jul. 2015.

[60] U.S. Food and Drug Administration. (2014). *Is the Product a Medical Device?* Accessed: Jun. 9, 2015. [Online]. Available: http://www.fda.gov/medicaldevices/deviceregulationandguidance/overview/classifyyourdevice/ucm051512.htm

[61] T. L. Saaty, "How to make a decision: The analytic hierarchy process," *Interface*, vol. 24, no. 6, pp. 719–743, Dec. 1994.

[62] T. L. Saaty, "Decision making with the analytic hierarchy process," *Int. J. Serv. Sci.*, vol. 1, no. 1, pp. 83–98, Jan. 2008.

[63] K. M. Stine, R. L. Kissel, W. C. Barker, A. Lee, J. Fahlsing, and J. Gulick. Guide for Mapping Types of Information and Information Systems to Security Categories. National Institute of Standard and Technology, 2008. Accessed: Mar. 6, 2019. [Online]. Available: https://www.nist.gov/publications/guide-mapping-types-information-and-information-systems-security-categories-2-vols

[64] R. S. Ross and L. A. Johnson. (2010). *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-37r1.pdf

[65] *Risk Management*, Standard ISO 31000, 2018.

[66] *Risk Management Framework for Information Systems and Organizations*, NIST Special Publication 800-37 Revision, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Dec. 2018.

[67] WHO, Switzerland. (Jun. 2011). *Introduction to Medical Equipment Inventory Management*. [Online]. Available: http://www.who.int/medical_devices/en/

[68] *Failure Mode, Effects and Criticality Analysis (FMECA)*, document MIL-P-1629, Public Works and Government Services Canada, AECOM and Golder Associates, 2007.

[69] H. F. Badawi, F. Laamarti, and A. El Saddik, "ISO/IEEE 11073 personal health device (X73-PHD) standards compliant systems: A systematic literature review," *IEEE Access*, vol. 7, pp. 3062–3073, Dec. 2019.

[70] B. Schneier. Attack Trees: Modeling Security Threats. Schneier on Security, 1999. [Online]. Available: https://www.schneier.com/academic/archives/1999/12/attack_trees.html

[71] I. Ray and N. Poolsapassit, "Using attack trees to identify malicious attacks from authorized insiders," presented at the 10th Eur. Symp. Res. Comput., Sep. 2005, doi: 10.1007/11555827_14.

[72] *Information Technology—Security Techniques—Evaluation Criteria for IT Security—Part 1: Introduction and General Model*, Standard ISO/IEC 15408-1:2009, 2009.

[73] *Information Technology-Security Techniques-Methodology for IT Security Evaluation*, Standard ISO/IEC 18045:2008, 2008.

[74] B. Kordy, L. Piètre-Cambacédès, and P. Schweitzer, "DAG-based attack and defense modeling: Don't miss the forest for the attack trees," *Comput. Sci. Rev.*, vols. 13–14, pp. 1–38, Nov. 2014.

[75] J. B. Hong, D. S. Kim, C.-J. Chung, and D. Huang, "A survey on the usability and practical applications of graphical security models," *Comput. Sci. Rev.*, vol. 26, pp. 1–16, Nov. 2017.

[76] L. Allodi and F. Massacci, "Security events and vulnerability data for cybersecurity risk estimation," *Risk Anal.*, vol. 37, no. 8, pp. 1606–1627, Aug. 2017.

[77] B. J. Anthony, N. C. Pa, M. S. Khalefa, H. A. A. Alasad, and H. F. Zmezm, "A proposed risk assessment model for decision making in software management," *J. Soft Comput. Decis. Support Syst.*, vol. 3, no. 5, pp. 31–43, Jul. 2016.

[78] A. P. H. de Gusmão, M. M. Silva, T. Poleto, L. C. e Silva, and A. P. C. S. Costa, "Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory," *Int. J. Inf. Manage.*, vol. 43, pp. 248–260, Dec. 2018.

[79] B. Anthony, Jr., "Validating the usability attributes of AHP-software risk prioritization model using partial least square-structural equation modeling," *J. Sci. Technol. Policy Manage.*, vol. 10, no. 2, pp. 404–430, Jun. 2019.

[80] A. A. Ganin, P. Quach, M. Panwar, Z. A. Collier, J. M. Keisler, D. Marchese, and I. Linkov, "Multicriteria decision framework for cybersecurity risk assessment and management," *Risk Anal.*, vol. 40, no. 1, pp. 183–199, Jan. 2020.