Journal of Biomedical Engineering Research 44: 99-108 (2023)
http://dx.doi.org/10.9718/JBER.2023.44.2.99

학 술 논 문

인공호흡기 원격 통합 모니터링 및 제어 시스템 개발을 위한 소프트웨어 위험관리 및 사이버보안

정지용[1] · 김유림[1] · 장원석[1,2]*

[1]연세대학교 대학원 의료기기산업학과
[2]연세대학교 의과대학 강남 세브란스병원 의료기기사용적합성연구센터

Software Risk Management and Cyber Security for Development of Integrated System Remotely Monitoring and Controlling Ventilators

Ji-Yong Chung[1], You Rim Kim[1] and Wonseuk Jang[1,2]*

[1]Department of Medical Device Engineering and Management, Yonsei University, College of Medicine, Seoul, Korea
[2]Medical Device Usability Research Center, Gangnam Severance Hospital, Yonsei University College of Medicine, Seoul, Korea
(Manuscript received 10 February 2023 ; revised 6 March 2023 ; accepted 8 March 2023)

Abstract: According to the COVID-19, development of various medical software based on IoT(Internet of Things) was accelerated. Especially, interest in a central software system that can remotely monitor and control ventilators is increasing to solve problems related to the continuous increase in severe COVID-19 patients. Since medical device software is closely related to human life, this study aims to develop central monitoring system that can remotely monitor and control multiple ventilators in compliance with medical device software development standards and to verify performance of system. In addition, to ensure the safety and reliability of this central monitoring system, this study also specifies risk management requirements that can identify hazardous situations and evaluate potential hazards and confirms the implementation of cybersecurity to protect against potential cyber threats, which can have serious consequences for patient safety. As a result, we obtained medical device software manufacturing certificates from MFDS(Ministry of Food and Drug Safety) through technical documents about performance verification, risk management and cybersecurity application.

Key words: Medical device software, Central remote monitoring, Risk management, Cybersecurity, Software validation

I. 서 론

최근들어 사물인터넷(IoT, Internet of Things) 기반으로 원격진료 또는 생명유지 기능 목적의 의료기기에 사용되는 소프트웨어들이 출시되고 있다[1]. 이러한 추세는 COVID-19 발생으로 인해 일상적인 대면활동이 비대면 방식으로 변화하면서 더욱 가속화되었다[2]. 특히 COVID-19 위중증 환자의 증가로 인공호흡기 사용의 중요성이 부각됨과 더불어 환자들을 보살필 수 있는 의료인력의 부족을 해결하기 위하여 인공호흡기를 적용한 환자들을 중앙에서 원격으로 모니터링할 수 있는 소프트웨어 시스템 도입에 관심이 높아졌다.

환자들을 모니터링하는 소프트웨어 시스템도 하나의 의료기기이기 때문에 사람의 생명과 밀접하게 연관되어 있으므로 안전성과 신뢰성이 매우 중요하다. 따라서 실제 현장에 도입되어 사용되기 전 소프트웨어 밸리데이션을 통해 의료기

*Corresponding Author : Wonseuk Jang
B1, 20, Eonju-ro 63-gil, Gangnam-gu, Seoul, Republic of Korea, Yonsei University College of Medicine Medical Device Design & Usability Lab
Tel: +82-2-2019-5442
E-mail: WS.JANG@yuhs.ac
본 연구는 2020년 범부처의 연구개발비(202011B26)로 수행되었으며 이에 감사드립니다.

기 소프트웨어의 성능을 점검해야 한다. 또한 기본적으로 의료기기 소프트웨어는 제조업체에서 소프트웨어를 개발 및 유지하기 위한 활동을 수행하는 품질경영과 안전성과 신뢰성을 검증하고 위해요소를 최소화하는 위험관리가 조화를 이루는 범위에서 개발 및 유지되고 사용되어야 한다. 특히, 위험관리와 관련하여 그 위험도의 등급에 따라 밸리데이션의 범위, 시험방법 및 그 정도가 달라진다[3]. 그렇기 때문에 소프트웨어 밸리데이션 활동에 앞서 의료기기 소프트웨어의 고장이나 잠재적인 결함으로 사용자에게 미칠 수 있는 위해(Harm)의 영향에 따라 Class A(부상이나 신체적 피해가 발생할 가능성이 없음), Class B(심각하지 않은 부상이 발생할 가능성이 있음), Class C(심각한 부상 또는 사망이 발생할 가능성이 있음)로 분류하여 안전성 등급을 결정해야 한다[4,5,6].

의료기기에 소프트웨어가 차지하는 부분이 클수록 해킹, 정보 유출 등 사이버보안 위협에 노출될 수 있으므로 보안에 대한 중요성 또한 커진다. 스마트의료 환경에서는 사이버보안이 미흡할 경우 환자 관련 정보 등의 매우 민감한 정보들이 유출되거나 위변조되는 등 막대한 피해가 발생할 수 있다[7,8]. 실제로 2017년 영국의 국가보건서비스가 워너크라이(WannaCry) 랜섬웨어 공격을 받아 환자들의 치료와 수술이 지연되었고, 2020년에는 독일 뒤셀도르프 대학병원 서버 30대가 랜섬웨어에 감염되어 긴급수술이 필요한 환자가 수술을 받지 못해 사망하는 사고가 있었다[9,10]. 일반적으로 의료정보시스템은 별도의 관리 없이 24시간 운영되기 때문에 인터넷에 연결된 상황만으로도 랜섬웨어 감염에 매우 취약했던 것이다[11]. 따라서 이같은 사고가 반복되지 않으려면 사이버보안을 필수적으로 적용하여 데이터의 기밀성, 무결성, 가용성을 실현해야 한다[12]. 기밀성은 전송되는 정보가 허가된 사용자에게만 공개되는 것을 의미하며, 무결성은 데이터가 정상적인 상태를 유지하고 무단으로 변환되거나 파괴되지 않아야 하는 것을 의미하고 가용성은 데이터에 대한 접근과 사용이 적시에 이루어지도록 하는 것을 의미한다. 즉, 데이터의 송수신 과정에서 데이터가 노출되더라도 해독하기 어렵도록 암호화해야 하고 허가받은 사용자만 접근할 수 있도록 해야 하며, 그 로그 및 변경 이력을 관리할 수 있도록 해야 한다[13].

의료기기 소프트웨어 밸리데이션과 사이버보안에 대한 검증이 중요해짐에 따라 국내와 미국, 유럽 등 주요 국가에서는 소프트웨어 요구사항과 위험관리 요구사항을 추가 도입한 IEC 60601-1 의료기기 기본안전 및 필수 성능의 일반적인 요구사항에 대한 표준 3판을 기본적으로 요구하게 되었다[14]. 또한 미국 FDA에서는 2014년과 2016년 의료기기 사이버보안 가이드라인을 발표하였고, 유럽에서는 의료보안정책 수립 및 의료보안을 위한 스마트병원 가이드를 발표하였다. 국내 식품의약품안전평가원에서는 2019년 의료기기 사이버보안 허가·심사 가이드라인을 발표하여 유무선 통신이 가능한 의료기기 대상 허가·심사 시 사이버보안이 요구되는 의료기기의 적용 대상을 정의하고 제품 특성에 따라 보안 요구사항 및 제출되어야 하는 자료 범위를 제시하였는데, 그 중 요구사항을 일부 제외하거나 수정하여 적용하는 경우 의료기기 사이버보안 요구사항 체크리스트를 제출해야 한다[15,16]. 체크리스트는 대상 의료기기 소프트웨어 시스템이 의료기기 사이버보안 요구사항에 대한 적합성을 만족하는지를 그 여부를 확인할 수 있는 자료로 의료기기 소프트웨어의 허가·심사 시에 의료기기의 특성에 맞게 작성되어 제출되어야 한다.

국내외적으로 의료기기 소프트웨어의 안전성 및 보안이 중시되는 추세에 따라 본 연구에서는 중앙에서 원격으로 다수의 인공호흡기를 통합 모니터링 및 제어할 수 있는 시스템을 개발하고, 소프트웨어 밸리데이션에 따른 성능평가와 위험관리 프로세스, 그리고 스마트의료 분야 사이버보안 요구사항이 개발한 시스템의 특성을 반영하여 적합하게 적용되어 안전성과 신뢰성을 보장하는지 확인하였다.

II. 연구 방법

1. 인공호흡기 원격 통합 모니터링 및 제어 시스템 개발

자가호흡을 할 수 없거나 어려운 이유로 인공호흡기를 적용한 다수의 환자들을 중앙에서 지속적으로 모니터링하고 위해 상황 발생 시 인공호흡기를 원격으로 제어할 수 있는 통합 모니터링 및 제어 시스템을 개발하였다.

2. 국내 품목분류 및 이상사례 조사

국내 식품의약품안전처 고시 제2022-53호 의료기기 품목 및 품목별 등급에 관한 규정을 분석하여 인공호흡기 원격 통합 모니터링 및 제어 시스템의 품목분류 현황을 조사하고 식품의약품안전처 안전성정보를 통해 인공호흡기 원격 통합 모니터링 및 제어 시스템 관련 의료기기 품목에 대한 이상사례를 참고하여 해당 품목에 대해 발생할 수 있는 위해요인(Hazard)을 식별하였다.

3. 의료기기 소프트웨어 밸리데이션 규격 조사 및 밸리데이션 수행

식품의약품안전처고시, 국제전기기술위원회(International Electrotechnical Commission, IEC), 국제표준화기구(International Organization for Standardization) 등 소프트웨어 밸리데이션과 관련된 국내·외 규격들을 조사 및 참고하여 의료기기 소프트웨어의 성능을 점검할 수 있는 주요 항목들을 도출하고 평가하였다. 또한 의료기기 품목에 대한 이상사례들을 통해 식별한 위해요인으로부터 위해(Harm)를 파

악하고, 정상 및 고장상태에서의 위해의 발생 가능성과 심각도를 분석하여 위험을 산정하였다. 산정된 위험은 허용할 수 있는 수준으로 감소시킬 수 있도록 적합한 위험통제 대안들을 식별하여 적용하였다.

4. 의료기기 사이버보안 요구사항 조사 및 평가

본 연구에서는 사이버보안이 개발된 인공호흡기 원격 통합 모니터링 및 제어 시스템에 적용되었는지를 점검하기 위해 스마트의료 사이버보안 가이드, 사물인터넷 보안 시험·인증기준 해설서 등을 참고하여 사이버보안 요구사항을 조사하고 사이버보안 허가·심사 가이드라인에서 제공하는 사이버보안 요구사항 체크리스트를 작성하였다. 사이버보안 요구사항 체크리스트의 기초자료로 사용한 스마트의료 사이버보안 가이드는 스마트의료 서비스의 구성요소를 네트워크 기능을 갖는 의료기기, 게이트웨이, 네트워크, 의료정보시스템 등으로 구분하고 발생할 수 있는 보안 위협과 이에 대한 대응방안을 제시한다. 발생할 수 있는 보안위협에는 데이터 유출, 악성코드 감염, 기기 오작동, 비인가 접근 등이 있으며, 이에 대한 대응방안으로는 사용자 접근 통제 및 인증, 패스워드 및 암호화 키 관리, 네트워크 보안, 망분리, 감시로그 기록 및 관리 등이 있다. 기초자료로 함께 사용한 사물인터넷 보안 시험·인증기준 해설서는 사물인터넷을 기반으로 한 기기에 적용되도록 요구되는 최소 시험기준에 대해 제시한다. 최소 시험기준은 인증유형, 암호유형, 데이터 보호 유형, 플랫폼 보호 유형, 물리적 보호 유형으로 구분된다[17].

사이버보안 요구사항과 시험기준에 대한 체크리스트의 사이버보안 요구사항은 스마트의료 사이버보안 가이드에서 제시하는 대응방안을 참조하여 적용하였고, 시험기준은 사물인터넷 보안 시험·인증기준 해설서에서 제시한 최소 시험기준을 참조하여 적용하였다. 체크리스트에 나타낸 사이버보안 요구사항 항목들은 시험기준에 따라 평가하였다.

III. 연구 결과

1. 인공호흡기 원격 통합 모니터링 및 제어 시스템

인공호흡기 원격 통합 모니터링 및 제어 시스템은 다수의 환자감시장치를 중앙에서 모니터링하는 기존의 환자중앙감시장치 시스템과는 달리 환자감시장치뿐만 아니라 병원 내부 네트워크에 연결된 인공호흡기들을 서버를 통해 중앙에서 원격으로 실시간 모니터링 및 제어할 수 있는 의료기기 소프트웨어이다. 자가호흡이 어려운 이유로 인공호흡기를 적용한 환자의 상태정보를 수집하고, 그 정보를 실시간으로 제공한다. 또한 환자 상태가 제한 수치보다 초과하거나 부족한 경우, 즉시 높은 수준의 알람을 시각적, 청각적 방법으로 발생시킨다.

모니터링 시스템의 서버는 그림 1에 나타낸 것처럼 모듈(Module)들이 데이터를 송수신하는 구조로 구성되어 있다. Data Agent는 인공호흡기와 연결되어 실시간으로 모니터링 데이터를 수신하고, 수신한 데이터를 Message Broker로 저장하는 모듈이며 Message Broker는 다른 모듈과의 통신을 전담하는 모듈로 데이터 유실이 없도록 고속의 통신을 보장한다. Data Aggregator는 Message Broker에서 순차적으로 데이터를 조회하여 Database에 저장하는 모듈로 실시간 처리와 구분하여 독립적으로 동작하며 Database는 인공호흡기가 전달하는 모니터링 데이터, 인공호흡기 정보와 병실, 환자 정보 등을 저장하고 관리한다. Service Server는 실시간 데이터를 조회하여 시스템 사용자의 브라우저로 전송하는 Backend와 브라우저에 사용자 인터페이스를 제공하는 Frontend로 나누어진다.

서버 모듈들이 데이터를 송수신함으로써 모니터링 시스템 사용자는 그림 2의 기능들을 사용할 수 있다. 그림 2(a)는 산소포화도(SpO2), 흡기압(PI), 맥박 수(PR), 산소포화도 대 흡입산소 비율(S/F ratio), 흡입 산소농도(FiO2), 유량

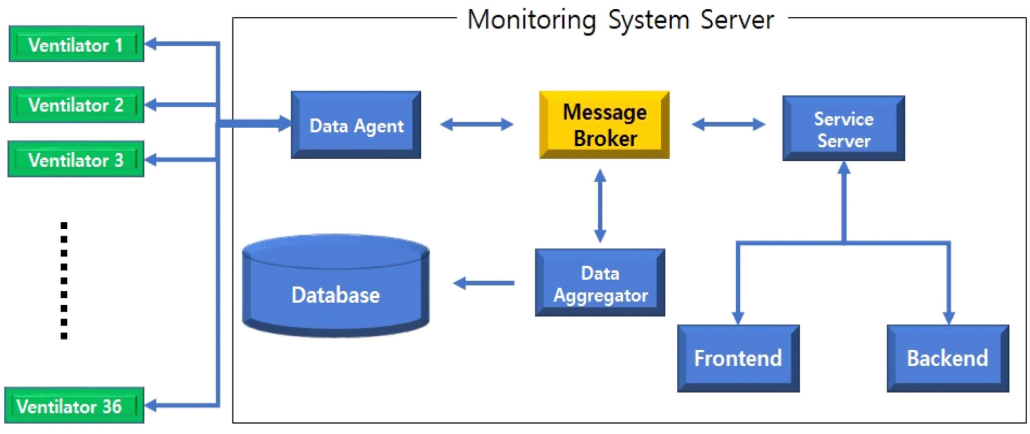

그림 1. 모니터링 시스템의 서버 구성도
Fig. 1. Server Structure of Monitoring System

그림 2. 시스템 기능 (a) 호흡 파라미터 모니터링 (b) 데이터 트랜드 리뷰 (c) 이벤트 알람 리뷰 (d) 파라미터 알람 한도 원격 제어
Fig. 2. System Function (a) Respiratory Parameter Monitoring (b) Data Trend Review (c) Event Alarm Review (d) Parameter Alarm Limit Remote Control

(Flow) 등의 환자 호흡 관련 파라미터들을 모니터링할 수 있는 기능, 그림 2(b)는 각 환자에 대해 최대 7일 동안의 데이터 트랜드, 그림 2(c)는 최대 3개월 동안 발생한 이벤트 및 알람 내역을 저장하거나 열람할 수 있는 기능이다. 또한 그림 2(d)는 모니터링 시스템에서 설정한 호흡 파라미터의 알람 한도를 모니터링 중인 인공호흡기에 원격으로 적용할 수 있는 기능을 나타낸다.

2. 국내 품목분류 및 이상사례 현황을 통한 위험스러운 상황 식별

인공호흡기 원격 통합 모니터링 및 제어 시스템은 의료기기 품목 및 품목별 등급에 관한 규정에 의해 중분류 내장기능 검사용 기기에 속하며 A26100 2등급 환자중앙감시장치로 분류되고, 여러 대의 환자감시장치를 집중하여 감시하는 기구로서 유해한 경우에는 시각 또는 청각 등에 의한 경보를 발생시키는 장치로 정의된다. 식약처 안전성정보에서 공개하고 있는 환자중앙감시장치 이상사례에 대한 표 1에 따르면 스위칭허브 내부소자 불량으로 인한 정보 이상 표시, 인터페이스 오류, 전자의무기록 시스템과의 데이터 호환 불가, 시스템 불능 등의 제품결함을 확인할 수 있었다[18]. 이러한 제품결함 사례들은 인공호흡기 원격 통합 모니터링 및 제어 시스템의 서버를 구성하는 모듈들의 주요 소프트웨어 항목별 위해요인을 식별하고, 그 위해요인으로 인한 위험스러운 상황(Hazardous situation) 식별에 반영되었다. Ventilation Main, Vital Main, Window Main, Ventilation value and

표 1. 식약처 환자중앙감시장치[2] 안전성 정보
Table 1. MFDS Central Monitoring System[2] Safety Information

Classification Name	Central Monitoring System[2]
Summary	It is an instrument that intensively monitors multiple patient monitoring devices, which generates alarms in hazardous situations
	Abnormal case
Product Defect	Information displayed strangely due to defective internal elements of the switching hub
	Interface error
	Data is not compatible with Electronic Health Records system
	Central monitor suddenly shuts down and does not operate

wave Gen. 등 그래프 및 파형, 생체신호 수치를 표시하는 Frontend의 소프트웨어 항목은 그래프 왜곡 및 잘못된 파형이나 부적절한 알람 등 정보 이상 표시를 반영한 위험스러운 상황이 식별되었고, Data Agent 및 Message Broker의 인공호흡기와의 TCP/IP 통신 관련 데이터 전송 및 수신에 대한 항목은 전체 신호 모듈과 통신 이상 등 데이터 호환 불가, 정보 이상 표시 등을 반영한 위험스러운 상황이 식별되었다. 또한 Frontend와 Backend를 포함한 Service Server의 TIMER Main, Screen Main과 같은 간격 조정, 화면 표시 유무 판단 등에 관한 소프트웨어 항목과 Invoke CMD, Menu Main 등 사용자의 설정에 따른 수행과 관련된 항목은 각각 시스템 불능을 반영하여 프로그램의 동작이 멈추는 위험스러운 상황과 사용자 정보 화면의 표시가 이상하거나 잘못된 명령이 전달되는 등 정보 이상 표시, 인터페이스 오류를 반영한 위험스러운 상황이 식별되었다.

3. 의료기기 소프트웨어 밸리데이션

(1) 관련 규격

인공호흡기 원격 통합 모니터링 및 제어 시스템에 적용 가능한 소프트웨어 밸리데이션에 관한 규격은 표 2와 같다. 기본적으로 모든 의료기기 개발은 안전한 기기의 개발을 위한 특별지침을 제공하는 IEC 60601 규격 시리즈와 관련성을 가지고 있다[19]. 특히 3판부터는 의료기기 소프트웨어 요구사항과 위험관리 요구사항이 포함되어 IEC 62304와 관련성을 가지게 되었다. 의료기기 소프트웨어는 모든 가능한 입력에 대해 모든 결함을 찾아낸다고 보장할 수 없기 때문에 수명주기의 모든 절차마다 체계적인 연구개발 프로세스를 수립하고 그에 대한 활동을 문서 산출물로 기록할 것을 요구하는 기준 표준인 IEC 62304를 준수해야 한다. IEC 62304에서는 기본적으로 의료기기 소프트웨어는 ISO 14971에 따른 위험관리 시스템 및 ISO 13485에 따른 품질관리 시스템과 조화를 이루는 범위에서 개발 및 유지되고 사용되어야 하는 것으로 보며, 각각 적용 가이드 규격을 통해 적용할 수 있다. 국내에서는 적용 가이드 규격을 한글 부합화 작업을 거쳐 국가기술표준원으로부터 의료기기가 통합된 IT 네트워크에 대한 위험관리의 적용에 대해 1부(역할, 책임 및 활동), 2-1부(실제적용과 사례), 2-2부(의료기기의 보안 요구사항, 위험, 통제에 대한 공개 및 통신을 위한 지침), 2-3부(무선 네트워크에 대한 지침), 2-4부(적용지침-의료서비스기관에 대한 일반구현지침)로 분리하여 국가표준(KS) 문서로 등록하였으며, 식약처 의료기기 소프트웨어 밸리데이션 가이드라인에 따라 소프트웨어가 내장되어 있거나 단독으로 사용되는 경우 소프트웨어의 모델명, 운영환경, 구조 등을 포함하여 주요기능을 검증할 수 있는 기술문서 작성방법에 대하여 IEC 62304를 바탕으로 기술하고, 허가·심사 시 제출해야 할 첨부자료에 대해 제시하고 있다.

(2) 주요 기능에 대한 성능평가 결과

인공호흡기 원격 통합 모니터링 및 제어 시스템은 식약처 의료기기 품목 및 품목별 등급에 관한 규정에 의해 환자중앙감시장치로 분류되며, 유해한 경우 시각 또는 청각 등에 의한 경보를 발생시키는 장치로 정의되기 때문에, 성능 평가 항목으로 모니터링한 호흡 관련 파라미터들에 대한 알람의 적절한 작동에 대한 항목들과 시스템에 대한 항목들을 도출하였다. 도출된 항목들에 대해 성능평가를 수행한 결과는 표 3과 같다.

(3) 위험관리 프로세스

소프트웨어 의료기기의 안전성 등급은 소프트웨어 시스템을 기능 또는 구성에 따라 분해한 소프트웨어 항목별로 할당되고, 할당된 등급 중 가장 높은 등급이 시스템 전체의 안전성 등급이 된다. 식품의약품안전처에서 발간한 의료기기 소

표 2. 소프트웨어 밸리데이션 관련 규격
Table 2. Software validation relevant standards

Number of Standard/Public Notification	Standard/Public Notification
IEC 60601-1 (2020)	Medical electrical equipment – General requirements for basic safety and essential performance
IEC 62304 (2015)	Medical device software – Software life cycle process
ISO 14971 (2019)	Medical devices – Application of risk management to medical devices
ISO 13485 (2016)	Medical devices – Quality management systems – Requirements for regulatory purposes
IEC 80002-1 (2009)	Medical device software – Part 1 : Guidance on the application of ISO14971 to medical device software
ISO 80002-2 (2017)	Medical device software – Part 2 : Validation of software for medical device quality systems
KS X IEC TR 80001 Series (2020)	Application of Risk Management for IT Network where Medical Devices are Integrated
MFDS Guideline No. 0095-01	Guidelines for Software Validation of Medical devices

표 3. 성능 평가 결과
Table 3. Result of Performance Evaluation

Software Item	Test	Result
VE Tidal Alarm	Alarm is activated when out of setting value High : 5 ~ 2500 ml, Low : 0 ~ 2500 ml	PASS
VE MIN Alarm	Alarm is activated when out of setting value High : 0.1 ~ 50 lpm, Low : 0.0 ~ 49.9 lpm	PASS
Resp. R Alarm	Alarm is activated when out of setting value High : 3 ~ 180 bpm, Low : 2 ~ 179 bpm	PASS
Ppeak Alarm	Alarm is activated when out of setting value High : 1 ~ 120 cmH_2O, Low : 0 ~ 119 cmH_2O	PASS
O2 Alarm	Alarm is activated when out of setting value High : 19 ~ 100 %, Low : 18 ~ 100 %	PASS
Air Leak Alarm	Alarm is activated when out of setting value High : 50 ~ 500 ml	PASS
Apnea Alarm	Alarm is activated when out of setting value High : 2 ~ 60 seconds	PASS
SpO2 Alarm	Alarm is activated when out of setting value High : 52 ~ 100 %, Low : 51 ~ 99 %	PASS
PR Alarm	Alarm is activated when out of setting value High : 30 ~ 250 bpm, Low : 25 ~ 245 bpm	PASS
EtCO2 Alarm	Alarm is activated when out of setting value High : 0.0 ~ 15.0 %, Low : 0.0 ~ 14.9 %	PASS
FiCO2 Alarm	Alarm is activated when out of setting value High : 0.0 ~ 15.0 %, Low : 0.0 ~ 14.9 %	PASS
Respiration Alarm	Alarm is activated when out of setting value High : 2 ~ 180 bpm, Low : 1 ~ 179 bpm	PASS
Allowance System Access	Working system in the PC environment where the firewall is not working	PASS
Network Problems	Operating system under the condition that the MAC address and IP of the ventilator are different	PASS
System Error	Operating the device continuously for at least 30 days	PASS

프트웨어 허가 · 심사 가이드라인에 따르면 인공호흡기 원격 통합 모니터링 및 제어 시스템의 기능 중 모니터링한 호흡 관련 파라미터들에 대한 알람을 발생시키는 기능은 안전성 등급 Class C에 해당하는 기능이므로 전체 시스템 또한 Class C에 해당한다.

환자중앙감시장치 제품결함 사례로부터 식별한 위험스러운 상황을 초래하는 10개의 소프트웨어 항목에 대한 위해의 발생 가능성과 심각도를 분석하여 산정한 위험(Risk)을 정량적으로 평가한 결과는 표 4와 같다. 표 4의 영역은 위험의 허용 판정에 의해 결정된다[20]. Green Zone 영역은 위험을 허용할 수 있는 영역으로 해당하는 위험은 위험통제 조치가 필요하지 않으며, Red Zone 영역은 위험을 허용할 수 없는 영역으로 해당하는 위험은 위험통제 조치가 필요하다. 따라서 표 4는 위험스러운 상황을 초래하는 10개의 소프트웨어 항

표 4. 위험 평가 결과
Table 4. Results of risk assessment

Probability of Failure \ Severity	Negligible (1)	Minor (2)	Marginal (3)	Critical (4)	Catastrophic (5)
Frequent (5)					
Probable (4)					
Occasional (3)					
Remote (2)			7	3	
Rare (1)					

표 5. 소프트웨어 항목별 각 위험스러운 상황 및 위해의 심각도와 발생가능성
Table 5. The Severity and Probability of Failure of each Hazardous Situation by Software Items.

Software Item	Hazardous Situation	Measures of Risk Control	Severity	Probability of Failure
Ventilation Main	Graph distortion and displaying invalid waveforms and figures.	CRC Check	4	2 -> 1
Vital Main	Graph distortion and displaying invalid waveforms and figures.	CRC Check	4	2 -> 1
Ventilation value and wave Gen.	Respiratory signal figures abnormality - Graph distortion - Alarm false	CRC Check	3	2 -> 1
Vital Sign value and wave Gen.	Biological signal figures abnormality - Graph distortion - Alarm false	CRC Check	3	2 -> 1
Comm Main	Communication failure	CRC Check Transmission Invalidity	3	2 -> 1
TIMER Main	Program error	Watch Dog Timer	3	2 -> 1
Invoke CMD	Displaying invalid user information	Comparing Flash Memory and RAM	3	2 -> 1
Menu Main	- Invalid command - Flash memory storage and loading error	Comparing Flash Memory and RAM	3	2 -> 1
Window Main	- Invalid information - Graph distortion and displaying invalid waveforms and figures - Alarm false	Comparing Flash Memory and RAM	4	2 -> 1
Screen Main	Program error	Watch Dog Timer	3	2 -> 1

목 모두 위험통제 조치가 필요함을 의미한다. 특히 그래프 왜곡 및 파형이나 수치 표시 이상이 발생할 수 있는 항목의 경우 심각성이 Critical에 해당하였다.

표 5에는 소프트웨어 항목별 각 위험스러운 상황 및 위해의 심각도와 발생 가능성, 위험통제대안 및 위험통제 후의 발생 가능성에 대해 나타내었다. 그래프 왜곡 및 잘못된 파형, 부적절한 알람을 표시하는 위험스러운 상황일 경우 수신된 데이터의 정확도를 높이기 위해 순환 중복 검사(CRC, Cyclic Redundacny Check)를 수행한 다음 그래프 모듈로 전송하게 하였다[21]. 전체 신호 모듈과 통신 이상이 발생하는 위험스러운 상황일 경우에는 전송된 수치 데이터의 값이 유효한 값인지를 CRC를 통해 검증하고, 유효하지 않은 값일 경우에는 전송오류로 무효화 처리하도록 하였다. 프로그램이 동작하지 않는 위험스러운 상황일 경우에는 각 루틴별로 정해진 시간 안에 실행이 되는지를 검사하였고, 프로그램 오류로 인하여 제품의 일부 기능이 작동 불능 상태가 되는 것을 대비하여 소프트웨어적인 수단으로 Watch Dog Timer를 도입하여, 일정시간 동안 응답이 없을 때 프로그램을 재동작하도록 하여, 만약에 발생할 제품 전체 동작 불능을 대비하게 하였다[22]. 마지막으로 사용자 정보 화면 표시가 이상하거나 잘못된 명령이 전달되는 등의 위험스러운 상황일 경우에는 메뉴 전체 항목의 정확한 동작을 검증하거나 Flash Memory와 RAM 상의 데이터를 비교검증하여 일치할 때에 저장을 실시하게 하였다. 설정한 위험 통제 대안을 반영함으로써 모든 소프트웨어 항목별 위해상황의 발생가능성이 Remote에서 Rare로, 즉 2에서 1로 감소하는 효과가 나타났다. 그 결과 표 4의 Red Zone 영역에 해당하는 위험들이 Green Zone 영역에 해당하게 되었고 모두 허용 가능한 수준임을 확인하였다.

4. 의료기기 소프트웨어 사이버보안 요구사항 및 성능 평가

스마트의료 사이버보안 가이드와 사물인터넷 보안 시험 · 인증기준 해설서를 기반으로 체크리스트에 작성한 사이버보안 요구사항을 시험기준에 따라 검토한 결과는 표 6에 나타내었다. 인공호흡기 원격 통합 모니터링 및 제어 시스템에 적용되어야 하는 모든 사이버보안 요구사항들을 시스템을 실제 동작시켜 검토하였고 적합 판정을 받았다. 한편, 해당 의료기기에 적용되지 않은 사이버보안 요구사항 항목으로는 표 6에서 결과를 EXCL(Exclude)로 나타낸 항목인 다중접속금지와 개인의료정보 저장관리로 본 연구의 의료기기는 환자중앙감시장치로써 기본적으로 클라이언트로 일대일 접속만 허용되고, 의료기관 외부에서 사용되는 게이트웨이를

표 6. 의료기기 사이버보안 요구사항 체크리스트 검토 결과
Table 6. Result of the Reviewing Medical Device Cybersecurity Requirements Checklist

Cybersecurity Requirements	Test	Result
Access control and authentication	• Verify it does not switch to the setup screen when the administrator password does not match • Verify that the administrator password appears masked when entered • Verify that English, numbers, or special characters are not displayed when inputting password • Verify that at least two types of English, numbers, and special characters are combined to enter at least 10 digits when inputting password	PASS
Recognizing users access	• Verify it does not switch to the setup screen when the administrator password does not match • Verify that you can set up a user account when you enter the correct administrator password	PASS
Limiting the access of unauthorized users	• Verify it does not switch to the setup screen when the administrator password does not match • Verify that you can set up a user account when you enter the correct administrator password	PASS
Blocking unauthorized network communication	• Verify that the general purpose ventilator and the patient monitoring device are connected when connecting to the IP and port allowed by the central monitoring system • Verify that the general purpose ventilator and the patient monitoring device are not connected when connecting to the IP and port not allowed by the central monitoring system	PASS
Blocking remote access	• Verify that the central monitoring system is connected to a registered account • Verify that the central monitoring system is connected to a not registered account	PASS
Authentication management of users	• Verify that a valid user account is connected to the central monitoring system • Verify that an expired user account is not connected to the central monitoring system	PASS
Auto session close	• Connect the general purpose ventilator and the patient monitoring device to the central monitoring system • After the general purpose ventilator and the patient monitoring device operating, verify that status of operation is displayed on central monitoring system • After the general purpose ventilator and the patient monitoring device stoped, verify that session connection close on central monitoring system after 30 minutes	PASS
Strengthening rules on creating passwords	• Verify that at least two types of English, numbers, and special characters are combined to enter at least 10 digits when inputting password • Verify that changing display into software update screen when inputting administrator password at least two types of English, numbers, and special characters are combined to enter less than 10 digits	PASS
Prohibiting password hardcoding	• Verify that at least two types of English, numbers, and special characters are combined to enter at least 10 digits when inputting password • Verify that changing display into software update screen when inputting administrator password at least two types of English, numbers, and special characters are combined to enter less than 10 digits	PASS
Prohibiting password exposure	• Verify that password are displayed as **** when input administrator password • Verify that English, numbers, or special characters are not displayed when inputting password	PASS
Approval for firmware or software update	• Verify that switch to the software update screen after inputting the certification number • Verify that not switch to the software update screen when inputting certification number at least two types of English, numbers, and special characters are combined to enter less than 10 digits	PASS
Ensuring the integrity of firmware or software update	• Verify that the software to update has the correct identification code • Verify that the device is operating normally after updating the software • Verify that software updates do not proceed when the identification code is incorrect	PASS

표 6. Continued
Table 6. Continued

Cybersecurity Requirements	Test	Result
Using authentication method upon firmware or software update	• Verify that the software to update has checked correct CRC check • Verify that device is operating normally after updating the software • Verify that software updates do not proceed when the CRC check is incorrect	PASS
Ensuring the confidentiality and integrity for transferring medical device control information on network	• Verify that the receive data cannot be viewed without the TLS decryption algorithm • Verify that the transmitted data cannot be viewed without the TLS decryption algorithm • Verify that users are being provided for use only in the hospital network	PASS
Ensuring the confidentiality and integrity for transferring personal health records on network	• Verify that the receive data cannot be viewed without the TLS decryption algorithm • Verify that the transmitted data cannot be viewed without the TLS decryption algorithm • Verify that users are being provided for use only in the hospital network	PASS
Using safe encryption algorithm	• Verify that the receive data cannot be viewed without the TLS decryption algorithm • Verify that the transmitted data cannot be viewed without the TLS decryption algorithm	PASS
Minimizing physical infringement on communication port	• Verify that users are being provided for use only in the hospital network	PASS
Removing or inactivating unnecessary services	• Verify that the general purpose ventilator and the patient monitoring device are connected when connecting to the IP and port allowed by the central monitoring system • Verify that the general purpose ventilator and the patient monitoring device are not connected when connecting to the IP and port not allowed by the central monitoring system	PASS
Recording system log for data audit	• Verify that external access log information • Verify that there are recorded user accounts, connection times, data generation, changes, and deletion record	PASS
Verifying integrity of major execution and setting files and taking actions	• Verify that the software related to key executable and setup files has checked correct CRC check • Verify that device is operating normally after checking digital signature for the software	PASS
Providing information on countermeasures to be taken when cybersecurity threat is detected	• Verify that information about cybersecurity is provided for users	PASS
Protection against DDoS attack	• Verify that users are being provided for use only in the hospital network	PASS
Prohibiting multiple access	• Excluded because Central Monitoring System allows only one-to-one client connections by default	EXCL
Managing personal health records storage	• Excluded because personal medical information is sent directly through the device without using a gateway used outside the medical institution	EXCL

사용하지 않고 기기에 개인의료정보를 직접 전송하기 때문에 해당되지 않아 적용되지 않았다.

IV. 고찰 및 결론

인공호흡기를 중앙에서 원격으로 모니터링하고 제어할 수 있는 시스템은 COVID-19와 같은 대규모 호흡기 감염병 유행에서 의료인력의 공백을 보충할 수 있는 효과적인 방안이며 사회적 거리를 두는 언택트(Untact) 사회에 적합한 시스템이다[23]. 하지만 의료기기 소프트웨어는 사람의 생명과 밀접하게 연관되어 있어서 안전성이 매우 중요하기 때문에 실제 현장에 도입되어 사용되기 전에 소프트웨어 밸리데이션 과정을 통해 성능을 점검하고 안전성과 신뢰성을 검증해야 한다. 또한 해킹, 정보 유출 등 사이버보안 위협에 노출되기 쉬운 의료기기 소프트웨어 특성상 사이버보안의 적용은 필수적이다.

본 연구는 인공호흡기 원격 통합 모니터링 및 제어 시스템을 개발하고, 개발한 시스템의 관련 국내 품목분류 및 의료기기 소프트웨어 밸리데이션 규격을 조사하여 해당 품목의 성능을 점검할 수 있는 주요 항목들을 도출하고 위험관리가 필요한 위해를 소프트웨어 항목별로 식별하였다. 모니터링한 호흡관련 파라미터들에 대한 알람 및 시스템에 대한 항목을 도출하여 성능을 점검하였으며, 식별된 위해는 소프트웨어 밸리데이션 규격인 IEC 62304를 바탕으로 한 소프트웨어 밸리데이션 가이드라인 및 소프트웨어 위험관리 가이드라인 등에 따라 심각도와 발생가능성을 분석하여 위험통제조치가 필요한 위험을 산정하였다. 최종적으로 산정된 위험은 적절한 위험통제 대안을 설정함으로써 위해의 발생가능성을 감소시켜 허용 가능한 수준으로 통제함으로써 시스템의 안전성과 신뢰성을 검증하였다. 또한 스마트의료 사이버보안 가이드, 사물인터넷 보안시험 · 인증기준 해설서를 참고하여 인공호흡기 원격 통합 모니터링 및 제어 시스템의 사이버보안 요구사항들을 도출하여 체크리스트를 작성하였고, 체크리스트의 항목들을 시험기준을 준수하여 검토함으로써 시스템이 사이버보안 요구사항을 충족하여 보안위협으로부터 민감하고 중요한 정보들을 안전하게 보호할 수 있음을 확인하였다.

본 연구에서 제시된 인공호흡기 원격 통합 모니터링 및 제어 시스템을 개발하는 과정에서 소프트웨어 밸리데이션 및 사이버보안을 적용한 방법은 향후 의료기기 제조업체에서 원격 제어가 가능한 의료기기 소프트웨어 개발 및 인허가 시에 밸리데이션 수행 및 제출해야 하는 기술문서들을 개발하기 위한 기초자료로 활용할 수 있을 것으로 기대한다.

References

[1] Choi BY, Lee BG. A Safety Process Guideline of Medical Device System Based on STPA. Journal of Internet Computing and Services. 2021;22(6):59-69.

[2] Lee JH. The Recent in Telemedicine in the era of COVID-19 and Policy Recommendations for the Balanced growth of Healthcare Service Industry in Korea. Journal of the Convergence on Culture Technology. 2020;6(4):591-598.

[3] Kim DY, Park YS, Lee JW. Development Life Cycle-Based Association Analysis of Requirements for Risk Management of Medical Device Software. Korea Information Processing Society Transactions on Software and Data Engineering. 2017;6(12):543-548.

[4] MFDS. Guideline for Software Validation of Medical Devices. Cheongju: Ministry of Food and Drug Safety; 2007.

[5] MFDS. Guideline on Review and Approval of Medical Device Software. Cheongju: Ministry of Food and Drug Safety; 2019.

[6] IEC. IEC 62304, Medical Device Software-Software Life-Cycle Processes. Geneva: International Electrotechnical Commission; 2006.

[7] KISA. Cyber Security Guide for Smart Medical Service. Seoul: Korea Internet & Secuirty Agency; 2018.

[8] Noh SW, Park YH, Rhee KH K. An Enhanced Secure Health Data Transmission Protocol using Key Insulation in Remote Healthcare Monitoring System. Journal of Korea Multimedia Society. 2016;19(12):1981-1991.

[9] Oh JM, Kang SJ. Policy Research on Smart Medical and ICT Convergence Security. Proceedings of the Korea Technology Innovation Society. 2020;607-624.

[10] Shin SM, Kim SR, Youn BC, Hur U, Kim DE, Kim KM, Kim JS. Analysis of Encryption Processes of 5ss5c and Immuni Ransomware, and Their Data Recovery. Journal of Digital Contents Society. 2020;21(10):1895-1903.

[11] Jeon IS, Kim DW, Han KH. How to Cope with Ransomware in the Healthcare Industry. Journal of The Korea Institute of Information Security & Cryptology. 2018;28(1):155-165.

[12] Kim KH, Choi SS, Kim IH, Shin YT. A Study on the Establishment of a Digital Healthcare Next-Generation Information Protection System. Journal of The Korea Society of Computer and Information. 2022;27(7):57-64.

[13] Thomasian NM, Adashi EY. Cybersecurity in the Internet of Medical Things. Health Policy and Technology. 2021;10(3).

[14] Kim YR, Lee SJ, Jang HJ, Chang HJ, Song SY, Han TH. A Study on the Regulation of Medical Devices Software and the Demand of Medical Device Developers. Proceeding of the Institute of Electronics and Information Engineers. 2019; 1005-1008.

[15] Han SH, Woo JH, Kim SM. A Study on Postmarket Management Method for Cybersecurity in Medical Devices. Regulatory Research on Food, Drug, and Cosmetic. 2021;16(1):27-35.

[16] MFDS. Guideline on Review and Approval for Cybersecurity of Medical Devices. Cheongju: Ministry of Food and Drug Safety; 2020.

[17] KISA. KISA-GD-2019-0007. Seoul: Korea Internet & Security Agency; 2019.

[18] https://udiportal.mfds.go.kr. Accessed on 3 Jan 2023.

[19] Park HJ, Jang JS, Proposal of a Risk Management Methodology in Accordance with the IEC 60601-1 Medical Electrical Equipment. Journal of the Korean Institute of Industrial Engineers. 2018;44(3):215-225.

[20] MFDS. Guidelines for Risk Management of Medical devices. Cheongju: Ministry of Food and Drug Safety; 2007.

[21] Lim JC, Lee JM. Protocol Design for Fire Receiver-based Fire Detection Robots. Journal of Korea Information Electron Communication Technology. 2018;11(4):452-259.

[22] Lee YS. Automatic Recovery and Reset Algorithms for System Controller Errors. Journal of The Korea Society of Computer and Information. 2020;25(3):89-96.

[23] Chung YJ. Untact Technology Trends Due to the Diffusion of Covid19 – A Study on the Service Robot. The Journal of the Korea Contents Association. 2020;18(2):18-23.