J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

의료기기 시스템의 해저드 분석 기법 비교☆

Comparison of Hazard Analysis for Medical Device System

최 보 윤[1] 이 병 걸[2*] 한 혁 수[3]
Bo-yoon Choi Byong-gul Lee Hyuk-soo Han

요 약

의료기기 분야의 시스템들은 사고가 발생할 경우 상해 등의 큰 피해를 줄 수 있으므로 사고가 발생할 수 있는 원인을 찾아 사고를 예방하고 피해를 최소화하는 해저드 분석 활동이 필수적이다. 해저드 분석 활동은 분석 목적에 따라 수행 방법이 다르고 적용할 수 있는 개발 단계가 다르기 때문에 분석 대상 시스템에 적합한 기법을 선택하는 것은 매우 어려운 일이다. 개발 단계 중 개념 단계에서 식별된 해저드를 기반으로 해저드를 완화하거나 예방하기 위한 기본 안전 요구사항이 도출되기 때문에 개념 단계에서 적합한 해저드 기법을 선택하는 것은 매우 중요하다. 본 논문에서는 의료기기 분야 시스템들의 해저드 분석 활동에 적합한 기법을 선택할 수 있도록 개발 단계 중 개념 단계에서 PHA 기법과 STPA 기법을 비교하도록 한다. 이 분석을 통해 의료기기 시스템에서 개념 단계의 적합한 해저드 분석 기법을 선정할 수 있을 것이다.

☞ 주제어 : 해저드 분석, PHA, STPA

ABSTRACT

Medical systems incurred accidents may result in significant damage for human being. Therefore, performing hazard analysis is important for medical system which is to identify hazard for preventing the accidents and minimizing the potential harm. Hazard analysis that is applied medical systems are difficult to apposite selected, because difference of analysis methods and applied development lifecycle is caused by objective of hazard analysis. It is required to select appropriate hazard analysis at concept phase during development lifecycle, owing to basic requirement elicitation to mitigate or prevent hazard based on identified hazard at concept phase. In this paper, hazard analysis methods, PHA and STPA, are compared at concept phase in which both methods have been applied on the medical system. As a result of compared methods, hazard analyst can be selected optimized hazard analysis methods for concept phase of the medical systems.

☞ keyword : Hazard analysis, PHA, STPA

1. 서 론

의료기기 분야의 시스템들은 사고가 발생할 경우 인명 상해 등의 큰 피해를 줄 수 있기 때문에 시스템 개발 시 사고가 발생할 수 있는 원인을 찾아 사고를 사전에 예방하고 피해를 최소화하는 활동이 필수적이다. 이와 같은 활동을 해저드 분석 활동이라고 한다. 해저드 분석 활동에 적용되는 기법들은 분석 목적에 따라 수행 방법과 절차가 다르고, 해저드 분석을 적용할 수 있는 단계가 다르기 때문에 시스템 개발 생명주기 동안 수행되는 단계마다 적합한 기법을 적용하여 지속적으로 수행해야 한다. 특히, 시스템 개발 첫 단계인 개념 단계에서의 해저드 분석에 적합한 기법의 선택은 이후 단계의 해저드 분석에 영향을 끼치기 때문에 단계별, 특히 초기 단계인 개념 단계에서의 적합한 기법의 선택은 매우 중요하다. 이는 이후 단계에서 개념 단계에서 식별된 해저드를 기반으로 해저드를 완화하거나 예방하기 위한 기본 안전 요구사항이 도출되기 때문이다. 도출된 기본 안전 요구사항은 설계 과정에 반영되어 구현됨으로써 최종 의료기기 시스템의 안전성을 확보하게 된다.

개념 단계에서의 해저드 분석 기법은 전통적인 해저드 분석 기법과 컴포넌트의 상호작용을 기반으로 하고 있는 STPA[1, 2] 기법으로 구분할 수 있다. 전통적 해저드 분석

1 Sangmyung university industry-Academy cooperation foundation, Sangmyung University, Seoul, 03016, Korea.
2 Department of Information Security, Seoul Wowen's University, 01797, Seoul
3 Department of Computer Science, Sangmyung University, Seoul, 03016, Korea.
* Corresponding author (byongl@swu.ac.kr)
[Received 5 November 2018, Reviewed 11 November 2018, Accepted 20 November 2018]
☆ 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학 ICT연구센터육성지원사업의 연구결과로 수행되었음(2015-0-00445)

기법은 사고의 원인이 컴포넌트의 고장으로 발생함을 가정하여 개별 컴포넌트를 대상으로 해저드를 파악하고 발생 원인을 분석한다. 현재 대부분의 의료기기 분야의 시스템에서는 전통적 해저드 분석 기법을 기반으로 분석 활동이 수행되고 있으며, 대표적인 방법으로는 PHL(Preliminary Hazard List), PHA(Preliminary hazard analysis), SSHA(Subsystem Hazard Analysis) 등이 있다[3]. 반면 STPA 기법은 사고의 원인이 컴포넌트들 간의 예상하지 못한 또는 의도하지 않은 상호작용에 기인한다고 간주한다. 기존의 의료기기 분야의 시스템에서는 STPA 기법을 적용하여 해저드 분석을 수행한 사례가 많지 않다. 하지만 점차 규모가 커지고 복잡해지고 있는 의료기기 시스템의 해저드 분석에 적용 효과가 클 것으로 평가되고 있다[4, 5].

본 논문에서는 의료기기 분야 시스템에서 개념 단계의 해저드 분석 활동에 적합한 기법을 선택할 수 있도록 전통적인 해저드 분석 기법과 STPA 기법을 비교한다. 개념 단계에서 식별된 해저드가 분석 대상 의료기기 시스템의 안전성 요구사항 도출에 기초가 되고, 요구사항의 도출에 적용된 해저드 분석 기법이나 분석 과정에 따라 서로 다른 결과를 도출할 수 있기 때문에 해저드를 식별하는 과정과 결과를 중심으로 두 기법을 비교한다. 분석 과정을 고려하기 위해 해저드 기법들의 분석 과정을 기술 수용 모델(TAM)에서 제시하고 있는 기준을 적용하여 평가하고, 추가적으로 분석의 효율성을 향상시킬 수 있는 분석의 자동화 가능 여부를 비교한다. 또한 분석 결과를 비교하기 위해서 식별된 해저드와 해저드의 발생 원인을 비교함으로써 식별된 해저드들간의 차이를 파악 비교한다.

논문의 구성은 다음과 같다. 2장에서는 STPA 의 해저드 분석 기법과 기존의 해저드 분석 기법들을 설명한다. 3장에서는 해저드 분석 대상 의료기기 시스템에 대해 설명하고, 비교하고자 하는 해저드 분석 기법들을 적용한다. 4장에서는 해저드 분석을 비교하기 위한 비교 기준을 설명하고, 기준에 따른 비교 결과를 기술한다. 마지막으로 5장에서는 비교 결과와 향후 연구 방향을 제시한다.

2. 관련 연구

2.1 개념 단계에서의 해저드 분석 연구

의료기기 분야의 시스템들을 포함한 안전 중시 시스템들에서는 개념 단계에서의 해저드 분석 활동이 매우 중요하다[6, 7, 8, 9]. 시스템의 안전성과 관련된 기능들의 대략 70%정도가 개발 초기인 개념 단계에서 결정되기 때문에 시스템의 안전성은 개념 단계에서부터 확보되어야 시스템으로 설계되고 구현될 수 있다.

개념 단계에서의 해저드 분석 활동의 중요성을 인식하고 의료기기 분야의 시스템에 개념 단계의 해저드 분석 기법을 적용한 연구가 수행되고 있다. Yi Zhang[8] 등의 연구에서 인슐린 펌프 시스템에 PHA 기법을 적용하여 해저드를 식별하였고, Paolo Masci[6] 등의 연구에서는 인슐린 펌프 SW의 사용자 인터페이스에 대한 해저드 분석 활동을 PHA 기법을 활용하여 수행하였다.

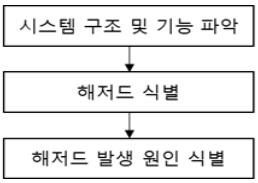
하지만 개념 단계에서의 해저드 분석 활동에 대한 연구들은 PHA 기법 중심의 전통적인 해저드 분석 기법으로 수행되고 있다는 한계점이 있다. 의료기기의 위험 관리 표준인 ISO 14971에서 권장하고 있는 기법은 전통적인 해저드 분석 기법인 PHA, FTA, FMEA, HAZOP, HACCP 등 5개의 기법들이다. 이 기법들 중에서 다른 4개의 기법들은 설계 단계에서부터 적용 가능한 기법들이지만 PHA 기법은 개념 단계에서 적용 가능하다. 하지만 STPA 기법을 적용한 개념 단계의 의료기기 시스템 해저드 분석 연구는 아직 시작 단계로 연구 결과를 찾기 어렵다. 이는 STPA를 이용한 해저드 분석 사례가 많지 않고 관련 정보도 충분하지 않아서 분석 기법 사용자들이 STPA 분석 기법을 선택하고 적용하는 데에 많은 어려움이 따르는 것으로 볼 수 있다.

본 논문은 의료기기 분야 시스템들의 해저드 분석 활동에 있어 분석 활동 참여자들이 PHA 기법과 STPA 분석 기법 중 분석 활동의 목표와 기대하는 결과를 바탕으로 어느 기법을 선택할 것인지에 대한 기법 선택의 판단 기준을 비교하고 결과를 제시한다.

2.2 PHA (Preliminary hazard analysis)

PHA 기법은 개념 단계에서 수행되는 되기 때문에 시스템에 대한 정보가 적고 상세 정보를 활용할 수 없는 시점에서 수행되며, 전통적인 해저드 분석 기법들 중에서 먼저 수행된다. 식별된 해저드 및 관련된 원인 요소, 영향, 위험 수준을 기반으로 설계 측면에서 완화할 수 있는 방안을 제시함으로써 이후 FMEA 등의 분석 기법에서 활용할 수 있다. 요약하면, PHA 기법은 가능한 가장 빠른 시점에 개발하고자 하는 시스템 또는 프로그램의 안전 관련 설계가 반영될 수 있도록 기본 시스템 안전 요구사항을 정의하기 위한 방법을 제공하는 기법이다.

이 기법은 그림 1에서와 같이 3단계로 수행될 수 있다. 첫 번째 단계인 시스템 구조 및 기능 파악 단계에서는 분석 대상 시스템을 정의하고 범위를 정하여 시스템의 개발 목적, 요구사항, 초기 설계 정보 등을 통해 시스템의 이해도를 높인다. 두 번째 단계인 해저드 식별 단계와 세 번째 단계인 해저드 발생원인 식별 단계에서는 해저드 분석을 위한 팀을 구성하여 해저드 체크리스트 등을 기반으로 브레인스토밍을 하여 잠재적인 위험 요소나 이벤트를 식별한다.



(그림 1) PHA 기법 수행 단계
(Figure 1) PHA process

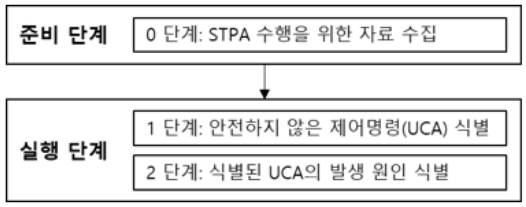
해저드 체크리스트는 알려진 위험 요인이나 잠재적인 위험 설계, 기능, 상황들의 목록이다. 해저드 체크리스트는 분석가들이 고려해야할 사항들을 확인할 수 있도록 제공되며, 에너지 자원, 위험한 기능/운영/컴포넌트, 유사 시스템에서 식별된 해저드, 발생된 안전사고 등을 고려해야 한다. 해저드 체크리스트의 사례는 표 1과 같다.

(표 1) 해저드 체크리스트 예시
(Table 1) Hazard checklist example

구분	체크리스트
에너지원	연료, 압축가스, 점화기, 뇌관, 축전기, 발전기 등
항공기능	승무원 탈출/진입, 비상탈출, 발사 및 분리 단계, 랑데부&도킹 등

2.3 STPA(System Theoretic Process Analysis)

STPA 기법은 사고의 발생 원인을 컴포넌트들이나 시스템들 간의 실패한 상호작용을 기반으로 분석하는 기법이다. STPA 기법도 개념 단계에서부터 해저드를 식별할 수 있는 방법으로, 이후 단계에서도 반복하여 해저드를 식별하고 구체화할 수 있다. 이 기법은 그림 2에서와 같이 준비 단계와 STPA 실행 단계로 구분할 수 있다. 준비 단계에서는 STPA 기법을 수행하기 위한 시스템을 파악하여 제어구조도를 작성하고 제어 명령을 식별하게 되며, 실행 단계에서는 위험을 발생시키는 해저드인 안전하지 않은 제어 명령(Unsafe control action: UCA)과 해저드 발생 원인인 UCA가 수행될 수 있는 시나리오를 식별한다.



(그림 2) STPA 기법 수행 단계
(Figure 2) STPA process

2.4 PHA와 STPA 기법의 비교

PHA와 STPA 기법은 시스템 개발 단계 중 개념 단계에서 적용 가능한 기법으로, 상위 수준의 해저드를 분석하는 것을 목표로 하고 있다. PHA 기법은 대상 시스템의 기본 정보와 유사 시스템의 사고 정보를 통해 사고의 원인인 컴포넌트의 고장을 해저드로 식별할 수 있다. 하지만 분석가의 시스템에 대한 이해나 경험이 해저드 식별에 높은 영향을 미친다는 단점이 있다. STPA 기법은 기존의 전통적인 해저드 분석 기법들과 달리 컴포넌트들 간의 상호작용에 중점을 두어 해저드를 식별한다. 이 기법으로 해저드를 식별하기 위해서는 제어구조도가 반드시 작성되어야 하는데, 이 활동은 해저드 분석만을 위한 추가 활동이 수행된다. 두 기법의 장단점을 요약하면 표 2와 같다.

(표 2) PHA와 STPA 기법 비교
(Table 2) Comparison of PHA and STPA

	PHA	STPA
장점	상세 정보 없이 컴포넌트의 해저드를 식별함	컴포넌트들 간의 상호작용을 분석하여 해저드를 식별함
단점	분석가의 역량이 중요함	분석 활동을 위한 제어구조도를 작성해야 함

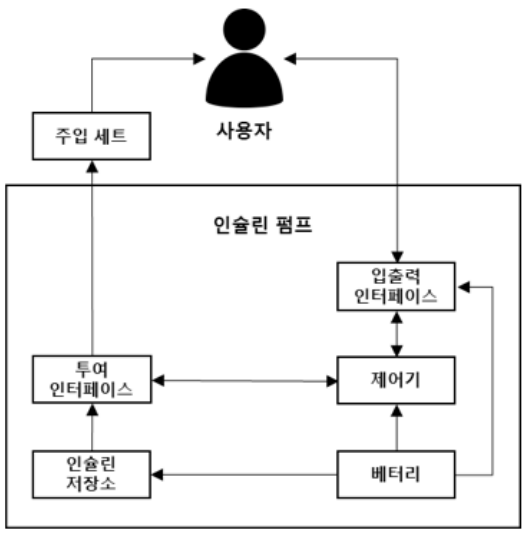
3. 인슐린 펌프 시스템의 해저드 분석

3.1 분석 대상

본 연구에서는 의료기기 시스템의 해저드 분석을 수행하기 위해 당뇨병 환자들을 위한 인슐린 투여 기기인 인슐린 펌프를 분석 대상으로 한다. 인슐린 펌프는 당뇨병 환자들이 당 분해 호르몬인 인슐린을 스스로 만들 수 없기 때문에 인슐린을 효과적으로 투여하기 위해 개발된 의료기기이다. 인슐린 펌프 시스템은 기기마다 기능의 차이가 있지만 펌프의 공통적인 기능은 다음과 같다.

- 사용자가 입력한 정보 및 명령을 기반으로 작동함
- 인슐린을 투여하는 방법은 기초 주입과 식사 주입으로 구분됨
- 인슐린 투여 기록을 저장함
- 인슐린 투여 상황 및 기록을 모니터링 할 수 있음

일반화한 인슐린 펌프 시스템의 구조를 표현하면 그림 3과 같고, 각 컴포넌트들의 역할은 표 3과 같다.



(그림 3) 인슐린 펌프 시스템의 구조도
(Figure 3) System architecture of insulin pump

(표 3) 인슐린 펌프 시스템의 컴포넌트별 역할
(Table 3) Function of component in insulin pump

컴포넌트	역할
주입 세트	● 인슐린이 환자에게 직접 투여되는 주사임
입출력 인터페이스	● 환자의 정보 및 투여 정보를 입력 받고 진행상황 및 이력을 확인할 수 있도록 함
제어기	● 인슐린을 환자에게 일정 시간동안 일정 속도로 투여되도록 인슐린 투여와 관련된 전반적인 제어를 수행함
투여 인터페이스	● 제어기를 통해 전달된 인슐린 투여량과 시간에 따라 인슐린이 투여될 수 있도록 함 ● 투여량과 시간 정보를 제어기에 전달함
인슐린 저장소	● 인슐린이 저장되어 있음
베터리	● 인슐린 펌프가 작동할 수 있도록 함

해당 인슐린 펌프 시스템은 인슐린을 투여하는 방법을 2가지로 정의하였다. 첫 번째 방법인 기초 주입 방법은 정상 혈당을 유지할 수 있도록 정기적인 간격으로 인슐린이 자동 투여가 될 수 있도록 한다. 두 번째 방법은 식사 주입 방법으로 식사 전 필요한 인슐린을 투여하도록 한다. 각 방법에 따라 투여 절차에 차이가 있으며, 투여 유형에 따라 이용하는 방법은 표 4와 같다.

(표 4) 투입 유형에 따른 이용 방법
(Table 4) Usage of infusion mode

투여 유형	이용 방법
기초 주입	● 기초 주입 설정 버튼을 선택함 → 투여 시간과 투여할 인슐린의 양에 대한 정보를 입력함 ● 설정된 내용에 따라 자동으로 투여함 ● 주입 중 정지할 수 있음
식사 주입	● 식사 주입 설정 버튼을 선택함 → 식사 시간마다 투여할 인슐린의 양에 대한 정보를 입력함 ● 식사 주입 버튼을 누르면 해당 식사 시간에 맞는 투여 정보를 제공함 ● 투여 정보를 확인 후 시작하며 필요에 따라 투여량을 변경할 수 있음 ● 주입 중 정지할 수 있음

인슐린 펌프 시스템의 위험 요소는 요구되는 인슐린

의 양이 정확하게 투여되지 않을 경우 발생한다. 설정된 양보다 많이 투여될 경우 저혈당이 발생하게 되고, 적게 투여될 경우는 고혈당이 발생하게 된다. 따라서 인슐린 펌프의 위험 상황은 표 5와 같이 정의한다.

(표 5) 인슐린 펌프 시스템의 식별된 위험 상황
(Table 5) Hazardous situation of insulin pump

분류	위험 상황
투여량	다량 투여: 요구되는 인슐린 양보다 많이 투여됨
	소량 투여: 요구되는 인슐린 양보다 적게 투여됨

인슐린 펌프 시스템의 해저드 분석 활동은 다량 투여 또는 소량 투여가 되는 위험 상황에 대한 해저드를 식별해야 한다.

3.2 PHA 분석

유사한 사례 연구로 특정 인슐린 펌프 시스템을 PHA 기법으로 분석한 연구[8]가 이미 수행된 바 있는데, 본 논문에서는 3.1의 인슐린 펌프의 공통 기능만을 대상으로 해저드 분석을 수행하였다. 먼저 3.1에서 시스템 구조도를 통해 식별한 컴포넌트가 수행해야 하는 역할이나 기능 등을 파악하고, 해저드 체크리스트를 기반으로 시스템이 표 5에서 식별한 위험상황을 발생할 수 있는지를 식별하며, 표 6과 같이 식별할 수 있다. 표 6에서는 상태 관련 해저드 체크리스트를 통해 투여량에 문제가 발생하는 해저드를 식별할 경우이다. 해저드 체크리스트는 의도하지 않은 활성화, 상태 전이 실패 등을 포함할 수 있다.

(표 6) 해저드 체크리스트 활용 예시
(Table 6) Sample hazard checklist

해저드 체크리스트 항목	해저드	투여량
의도하지 않은 활성화	예기치 못한 상황으로 사용자에게 안내 없이 초기 상태로 복원됨	투여량 정보 변경 (다량/소량 투여)
상태 전이 실패	심각한 오류 상황에서 정지가 되지 않음	다량 투여 가능

PHA 기법을 통해 식별된 해저드는 표 7과 같다.

(표 7) PHA 분석 결과
(Table 7) PHA analysis results

ID	해저드	해저드 발생 원인
1	예기치 못한 상황으로 사용자에게 안내 없이 초기 상태로 복원됨	사용자의 부주의로 인하여 초기화가 선택되어 복원됨
		사용 중에 축적된 정전기로 인하여 초기 상태로 복원됨
		부주의로 베터리가 펌프에서 분리되어 초기 상태로 복원됨
		하드웨어 오류로 인해 초기 상태로 복원됨
2	제어기가 투여 상태를 모니터링하지 못함	센서 문제
		SW오류
3	SW가 적절한 값으로 초기화되지 않음	기기가 처음 실행될 때SW가 적절한 값으로 초기화되지 않음
4	심각한 오류 상황에서 정지가 되지 않음	센서 문제
		SW오류
5	예상하지 못한 SW 실행	SW 오류
		운영체제 and/or런타임 지원이 손상되거나 실패 또는 업데이트됨
		기기고장
6	투여 정보가 맞지 않음	승인되지 않은 사람에 의한 데이터가 변조됨
		메모리 손상으로 인해 데이터가 손상됨
		사용자가 잘못된 정보를 입력함
		기기 중지 과정에서 사용자에게 투여된 인슐린이 기록되지 않음
		인슐린이 누출되어 이전에 투여된 인슐린 기록이 정확하지 않음
7	투여 명령이 변경됨 (오류 발생)	승인되지 않은 사람에 의한 데이터가 변조됨
		메모리 오류 또는 손상
		SW 오류
8	입력이 잘못됨	사용자가 사용자 인터페이스를 잘 다루지 못 함
		사용자가 잘못된 정보를 입력함
9	잘못 설정된 식사 주입 모드의 정보가 이용됨	다른 식사 주입 모드를 선택함
10	인슐린이 부족함	인슐린 교체 시기에 교체하지 않음

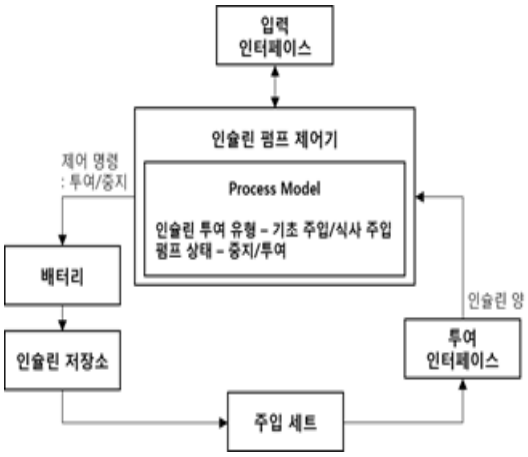
ID	해저드	해저드 발생 원인
11	인슐린 투여 정보를 임의로 변경함	사용자가 잘못된 정보 변경을 함
12	인슐린 투여 설정을 임의로 변경함	사용자가 잘못된 설정 변경을 함
13	펌프가 물리적으로 손상됨	기기 고장
14	인슐린 펌프가 과열됨	기기 고장
		SW 결함
15	기기 내부의 구성요소 또는 전기 회로가 정상적으로 작동하지 않음	센서 또는 감지 장치에 문제가 있음
16	배터리 문제	배터리 교체시기를 놓침
17	전달 경로의 침전 물질이 있음	펌프 청소 또는 교체 과정에서 문제가 있음
18	펌프가 주입 세트와 분리됨	사용자가 펌프 연결을 잘못함
19	인슐린이 잘못 투여됨	배터리 교체 후 SW가 배터리 교체 전 상태에서 시작됨
		SW가 중단 후 다시 실행할 때 중지되었던 기초 투여를 완료하도록 명령하여 다량 투여됨
		투여 명령에 따라 인슐린을 중지하지 못하였고, 사용자가 이를 인식하지 못함
		장치 고장으로 인슐린 투여가 잘못됨

3.3 SPTA 분석

STPA 기법은 준비 단계를 포함한 3단계의 프로세스로 이루어져 있다. 준비 단계에서는 분석을 위해 필요한 자료를 수집하고, 1 단계에서는 안전하지 않은 제어 명령(UCA)을 식별한다. 마지막 단계인 2단계에서는 식별된 UCA가 발생되는 원인을 파악한다.

3.3.1 준비 단계

STPA의 준비 단계에서는 인슐린 펌프 시스템의 제어구조도를 정의하는 단계이다. 인슐린 펌프 시스템은 인슐린 펌프 제어기가 투입된 인슐린 양에 대한 정보를 수집해서 프로세스 상태에 대한 정보를 얻고, 이 정보를 활용하여 제어 명령(투여/중지)을 조작하여 운영한다. 그림 3의 시스템 구조도를 기반으로 제어구조도를 정의하면 그림 4와 같다.



(그림 4) 인슐린 펌프 시스템의 제어구조도
(Figure 4) control structure of insulin pump

3.3.2 안전하지 않은 제어 명령 식별

준비 단계에서 제어구조도가 정의된 후, 1단계에서는 UCA를 식별하게 되며, 제어 명령을 기반으로 4개의 가이드워드에 따라 식별된다. 가이드워드는 시스템의 오류를 발생시킬 수 있는 제어 명령을 제공하거나 제공하지 않아 사고를 발생시킬 수 있는 시스템 상태를 파악할 수 있도록 하며, 표 8과 같다.

(표 8) UCA의 유형
(Table 8) Type of UCA

구분	의미
Not Provide	수행되어야 하는 제어 명령이 수행되지 않음
Provide	부정확하거나 불완전한 제어 명령이 수행됨
Too Late or Early	제어 명령이 수행되어야 할 시점보다 이르거나 늦게 수행됨
Too Soon or Long	제어 명령이 예정 기간보다 빨리 멈추거나 늦게까지 지속됨

4개의 가이드워드를 통해 파악된 시스템의 부적절한 제어 상황은 표 9와 같다.

(표 9) 1차 식별된 UCA
(Table 9) Primary identified UCA

	투여	중지
Not Provide	a. 투여되어야 할 인슐린이 투여되지 않음	f. 투여되어야 할 인슐린이 투여되었지만 중지되지 않음
Provide	b. 투여되어야 할 인슐린 양이 투여되었지만 계속 투여함	g. 인슐린이 투여되어야 하나 중지됨
Too late or early	c. 투여 정보가 확인 전에 투여가 시작됨 d. 설정된 투여시간보다 빠르게/늦게 투여함	h. 설정된 투여시간보다 빠르게/늦게 중지됨
Soon or long	e. 설정된 투여량보다 더 많이/적게 투여함	해당 없음

식별된 UCA중에서 a와 g UCA, b와 f UCA, d와 h UCA의 경우는 유사 UCA이므로 f, g, h의 UCA는 삭제한다. 따라서 투여 제어명령을 기반으로 식별된 5개의 UCA를 대상으로 식별된 인슐린 투여 유형(기초주입, 식사주입)을 적용하여 최종적으로 식별된 UCA는 표 10과 같다.

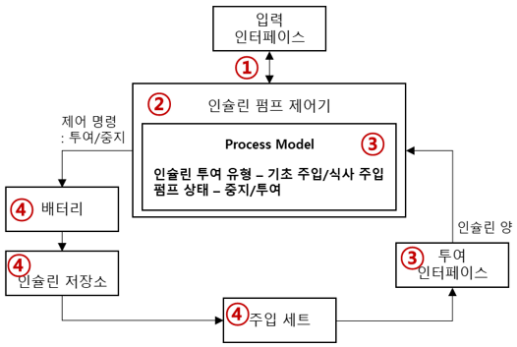
(표 10) 최종 식별된 UCA
(Table 10) final identified UCA

제어 명령	투여
Not provide	a-1. 기초 주입 시 투여되어야 할 인슐린이 투여되지 않음 a-2. 식사 주입 시 투여되어야 할 인슐린이 투여되지 않음
Provide	b-1. 기초 주입 시 투여가 중지된 후에도 계속 투여됨 b-2. 식사 주입 시 투여가 중지된 후에도 계속 투여됨
Too late or early	d-1 기초 주입 시 시작되어야 할 투여시간보다 빠르게 투여됨 c-1 식사 주입 시 투여 정보가 확인되기 전에 투여가 시작됨
Soon or long	e-1 기초 주입 시 설정된 투여량보다 더 많이 투여됨 e-2 기초 주입 시 설정된 투여량보다 더 적게 투여됨 e-3 식사 주입 시 설정된 투여량보다 더 많이 투여됨 e-4 식사 주입 시 설정된 투여량보다 더 적게 투여됨

3.2.3 발생 원인 파악

2단계에서는 식별된 UCA의 발생 원인을 4개의 가이드에 따라 파악하게 되며, 기준은 다음과 같다.

① 외부입력 제어나 정보가 잘못되거나 없어짐
② 제어 알고리즘이 올바르지 않음
③ 정보를 제공하는 시스템/센서가 잘못된 경우
④ 수행 대상이 실패하는 경우



(그림 5) 발생 원인 식별 기준
(Figure 5) Criteria of identified casual factor

UCA의 발생 원인은 그림 5에서와 같이 컴포넌트 각각에 대한 인과 관계 분석을 통해 UCA가 생성되는 시나리오 또는 제어 동작을 실행하지 않거나 적절하게 실행하지 않는 시나리오를 파악한다. 외부에서 제어기로 입력되는 제어나 정보를 감지하지 못 하거나 전달되지 않은 경우(①), 제어기의 문제로 제어 명령이 잘못 제공되는 경우(②), 제어기로 잘못된 피드백을 제공하는 경우(③), 제어기에서 제어 명령을 다른 컴포넌트로 전달하지만 감지하지 못하거나 수행되지 못 하는 경우(④) 등의 시나리오가 파악될 수 있다.

기준별로 상호작용이 실패한 컴포넌트는 식별된 UCA의 발생 원인은 다음 표 11과 같고, 각 발생 원인에 해당하는 UCA의 번호를 표기하였다. 인슐린 펌프 제어기는 입력 인터페이스로부터 제공받은 입력 정보가 잘못 전달되거나 전달되지 않아 두 컴포넌트 간의 상호작용에 문제가 발생할 수 있다(①). 입력 인터페이스로부터 투여 유형이 잘못 입력되는 시나리오는 식사 주입 실행 버튼이 잘못 눌린 경우로 파악할 수 있다.

(표 11) UCA의 발생 원인
(Table 11) List of casual factors of UCA

구분	기준	발생 원인
인슐린 펌프 제어기	①	• 투여 정보를 잘못 입력함(a-1, a-2) • 투여 중지 명령이 입력되지 않음 (b-1, b-2) • 식사 주입 시 투여 명령이 입력되지 않음(a-2) • 식사 주입 실행 버튼을 잘못 누름(c-1) • 식사 주입 시 투여 정보를 잘못 변경함(b-2, e-3, e-4) • 투여 시간 정보를 잘못 입력함(d-1)
	②	• 제어 SW의 오류로 투여가 중단되지 않음(b-1, b-2) • 제어 SW의 오류로 투여 시간보다 빨리 투여됨(d-1) • 제어 SW의 오류로 실제 투여되어야 할 투여량과 일치하지 않음 (e-1, e-2, e-3, e-4)
	③	• 투입 실행 명령이 전달되지 않음 (a-1, a-2) • 투입 중지 명령이 전달되지 않음 (b-1, b-2) • 투입 중지 명령의 전달이 지연됨 (e-1, e-3)
투여 인터페이스	③	• 투여량에 대한 정보가 잘못 제공됨 (b-1, b-2, d-1, e-1, e-2, e-3, e-4) • 투여량에 대한 정보가 전달되지 않음(c-1, e-1, e-3) • 투여량에 대한 정보가 지연됨 (c-1, e-1, e-3) • 투여량을 정확하게 파악하지 못 함 (b-1, b-2, e-1, e-2, e-3, e-4)
배터리, 인슐린 저장소	④	• 배터리가 없어 수행되지 못함(a-1, a-2) • 인슐린이 없어 수행되지 못함(a-1, a-2) • 배터리가 부족하여 수행이 중단됨 (e-2, e-4) • 인슐린이 부족하여 수행이 중단됨 (e-2, e-4)
주입 세트	④	• 인슐린이 투여되지 않음(a-1, a-2) • 인슐린이 투여되는 과정에서 일부 누출됨(e-2, e-4)

4. 해저드 분석 기법들의 비교

4.1 분석 방법

의료기기 시스템에 적합한 해저드 분석 기법을 비교하기 위한 기준 수립은 분석 과정 측면과 분석 결과 측면을 고려하여 비교 기준을 설정하였다. 먼저 해저드 분석 기법들의 분석 과정을 고려하기 위해서는 기존 기법들의 분석 과정을 평가할 수 있는 방법이 마련되어야 한다. 이를 위해 기술 수용 모델(TAM)이라는 기법을 적용하였다. 이 기법은 새로운 기술을 채택하는 방법을 평가하기 위해 사용되는 방법으로, 지각된 유용성(Perceived Usefulness)과 지각된 용이성(Perceived Ease of Use)이라는 2가지 측면에서 분석 기술을 파악한다. 이 기법은 해저드 분석 기법을 비교하는 유사 연구[10]에서도 적용되었으며, 본 논문에서도 해당 연구에서 사용되었던 기술수용모델의 분석 항목인 분석의 용이성, 용이성의 근거, 지원방법, 결과의 신뢰성, 적합성을 비교 기준으로 정의하였다. 또한 분석 과정의 효율성을 향상시킬 수 있는 자동화 가능 여부를 비교 기준에 추가하였다.

해저드 분석 기법 평가의 분석 결과 측면에서는, 식별한 해저드와 발생 원인을 비교하여 식별된 해저드의 차이를 파악하고, 결과를 비교하였다. 본 논문에서 적용할 분석 기준은 다음과 같이 6가지 항목으로 요약된다.

1) 해저드 분석 기법의 프로세스 평가 비교 (TAM 모델의 용이성, 용이성 근거, 지원방법, 결과의 신뢰성, 적합성)
2) 식별된 해저드의 비교
3) 식별된 해저드의 원인 비교
4) 자동화 가능성
5) 제약사항
6) 표준 준수 여부 비교

4.2 분석 결과

4.2.1 해저드 분석 기법의 프로세스 평가 비교

기존 분석 기법들의 프로세스를 평가하기 위해 적용된 프로세스 평가 항목은 아래와 같이 5개로 정의하였다.

1) 분석의 용이성

분석 프로세스의 특정 단계를 수행함에 있어, 분석의 난이도 수준에 따라 1-5 사이의 값으로 표현한다. 분석 난이도가 높을수록 높은 값을 부여한다.

2) 용이성의 근거
특정 단계를 수행하는 난이도의 근거를 설명한다.

3) 지원 방법
특정 단계를 수행하는데 도움이 되는 지침, 도구들의 유무를 판단하고 지원 방법을 설명한다.

4) 결과의 신뢰성
특정 단계를 수행한 결과물을 신뢰할 수 있는 수준에 따라 매우 높음, 높음, 보통, 낮음, 매우 낮음 등으로 값을 표현한다.

5) 적합성
특정 단계의 활동과 결과물이 시스템의 해저드를 식별하는데 필수 여부를 설명한다.

표 12과 표 13는 앞서 언급한 프로세스 평가 기준을 기반하여 기존 기법들의 해저드 분석 프로세스에 대한 평가 결과를 보여준다. 기존 기법들의 해저드 분석 프로세스는 그림 1과 그림 2에 기술하였다.

PHA 기법의 2단계와 STPA 기법의 1단계의 경우는 해저드(UCA)를 식별하는 단계로 유사하며, 각 기법의 필수적인 단계이다. PHA 기법의 경우 체크리스트가 제공되나 알려진 해저드 목록으로 분석가가 잠재적인 해저드를 식별할 수 있도록 돕기 위해 제공된다. 분석가의 경험이나 유사 시스템에서의 사고 발생 자료를 통해 해저드를 식별하기 때문에 수행하기 어렵고, 분석가의 역량이나 수집된 정보에 따라 다른 결과가 나올 수 있기 때문에 분석 결과의 신뢰성이 낮다. 또한 STPA 기법은 제공되는 4개의 가이드워드를 통해 해저드를 식별하기 때문에 수행하기가 매우 쉬우며, 분석가에 상관없이 유사한 결과가 나오기 때문에 분석 결과를 신뢰할 수 있다.

표 12과 표 13의 분석 결과를 살펴보면 PHA 기법의 1단계와 STPA 기법의 0 단계에서는 분석 대상 시스템을 분석가가 얼마나 잘 이해했는지에 따라 분석 목적 및 범위가 결정되기 때문에 분석가의 역량이 중요하다. PHA 기법의 2단계와 3단계는 분석 방법으로 브레인스토밍이 권장되기 때문에 분석가에 따라 분석 결과가 달라질 수 있음을 확인할 수 있다. 하지만 STPA 기법의 경우는 1단계와 2단계에서 가이드를 제공하고 있기 때문에 분석가의 경험이 다르더라도 유사한 분석 결과를 도출할 수 있다.

(표 12) PHA 기법의 프로세스 평가 결과
(Table 12) Assesment result of PHA process

	분석의 용이성	용이성의 근거	지원 방법	결과의 신뢰성	적합성
1 단계	3	시스템의 기능 및 구조에 대해 제공되는 정보에 따라 달라짐	없음	보통 - 분석가의 역량에 따라 시스템 이해도가 달라질 수 있음	분석 대상을 파악하는 단계이기 때문에 적합함
2 단계	4	유사 사고의 발생 자료를 검토하거나 사고로 이어질 수 있는 요소나 사건을 조사하여 해저드를 식별해야하기 때문에 어려움	체크리스트 제공	낮음 - 분석가의 역량에 의존됨	해저드 식별 단계이기 때문에 적합함
3 단계	5	잠재적인 위험 원인을 파악하기 위한 가이드나 기준이 없어 매우 어려움	없음	낮음 - 분석가의 역량에 의존됨	인과 관계를 파악할 수 있기 때문에 적합함

(표 13) STPA 기법의 프로세스 평가 결과
(Table 13) Assessment result of STPA process

	분석의 용이성	용이성의 근거	지원 방법	결과의 신뢰성	적합성
0 단계	3	시스템의 기능 및 구조에 대해 제공되는 정보에 따라 달라짐	없음	낮음 - 분석가의 시스템에 대한 이해도에 따라 결과가 달라질 수 있음	분석 대상을 파악하는 단계이기 때문에 적합함
1 단계	1	가이드워드에 따라 식별하기 때문에 식별이 용이함	4개의 가이드 워드 제공	높음 - 가이드워드에 따른 위험 상황을 식별하기 때문임	해저드를 식별할 수 있기 때문에 적합함
2 단계	4	가이드가 제공되지만 동적인 상황을 고려하여 원인을 식별하는 것이 어려움	4개의 상황에 대한 가이드 제공	높음 - 가이드에 따른 분석 결과를 식별하기 때문임	인과 관계를 파악할 수 있기 때문에 적합함

4.2 식별된 해저드의 비교

기존 분석 기법을 통해 식별된 해저드 개수는 PHA 기법은 19개(표 4), SPTA 분석 기법은 10개(표 5)의 해저드가 식별되었다. 두 기법에서 식별된 해저드는 유사 항목을 1:1로 맵핑하여 구분할 수는 없지만 PHA 분석 기법의 해저드 중 4, 5, 6, 7, 19번 해저드는 STPA의 10개 해저드와 밀접한 연관 관계가 있는 해저드임을 확인할 수 있다.

PHA 분석 기법은 분석 가이드를 제공하고 있지 않기 때문에 운영/SW/HW/사용자/환경/에너지/물리적 관점 등의 다양한 관점에서 해저드를 식별할 수 있었다. 반면 STPA 분석 기법은 제어구조도를 기반으로 4개의 정해진 가이드워드를 사용하여 분석되기 때문에 PHA보다 제한된 관점에서 해저드가 분석되었다. 하지만 STPA로 식별된 해저드는 위험의 발생 원인을 PHA 보다 상세하게 설명하고 있다. 다음 표 14는 각 기법으로 식별한 해저드 중 유사 해저드로 분류된 PHA 기법의 4번 해저드와 STPA 기법의 b-1번 해저드이다.

(표 14) PHA 기법과 STPA 기법으로 식별된 해저드 비교
(Table 14) Comparison of hazards identified by PHA and STPA

	PHA	STPA
해저드	• 심각한 오류 상황에서 정지가 되지 않음	• 기초 주입 시 투여가 중지된 후에도 계속 투여됨

예를 들어, 2개의 기법 모두 인슐린이 계속 투여가 되는 상황을 동일하게 해저드로 식별하였다. 하지만 PHA 기법의 경우 그 조건이 심각한 오류가 발생한 경우로만 (심각한 오류 상황에서 정지가 되지 않음) 파악하였고, STPA 기법의 경우 위험 상황이 되는 구체적인 조건 (기초주입 시 투여가 중지된 후에도 계속 투여)까지 설명하였다. 따라서 PHA 분석 기법은 분석가의 경험과 역량에 따라 다양한 관점에서 분석이 가능하지만, 동일한 수준의 해저드가 식별되기 어려워서 해저드의 수준이 분석가의 역량에 따라 서로 다를 수 있다, STPA 기법은 주어진 가이드워드에 따라 한정된 관점에서 분석이 되지만 동일한 수준의 비교적 상세한 해저드를 파악할 수 있다.

4.3 식별된 해저드의 원인 비교

두 개의 분석 기법에 의해 식별된 위험 원인은 명확한 차이가 있다. STPA 기법은 원인 분석을 위한 가이드를 제공하고 있기 때문에 가이드에 따라 많은 요소들이 상세하게 파악된다. 하지만 PHA 기법은 해저드 발생의 잠재적인 원인을 상세하게 식별하지 못하였다. STPA와 비교하여 모든 위험 요소에 대해 식별되지 않으며 상세한 원인도 파악되지 않았다. 표 15는 PHA 기법과 STPA 기법으로 각각 식별한 해저드와 해저드 발생 원인이다. 인슐린 투여가 계속 되는 해저드에 대한 발생 원인은 PHA 기법에서는 센서와 SW 문제로 파악되었다. 하지만 STPA에서는 센서와 SW가 어떻게 컴포넌트들과의 상호작용 중 해저드를 발생하게 되었는지를 5개의 조건으로 상세하게 파악하였다.

(표 15) PHA 기법과 STPA 기법으로 식별된 발생 원인 비교
(Table 15) Comparison of casual factors of identified each hazards

	PHA	STPA
해저드	• 심각한 오류 상황에서 정지가 되지 않음	• 기초 주입 시 투여가 중지된 후에도 계속 투여됨
발생 원인	• 센서 문제 • SW 오류	• 투여 중지 명령이 입력되지 않은 경우 • 제어 SW의 오류로 투여가 중단되지 않은 경우 • 투입 중지 명령이 전달되지 않은 경우 • 투여량에 대한 정보가 잘못 제공된 경우 • 투여량을 정확하게 파악하지 못한 경우

이를 통해 STPA 기법을 활용하여 해저드의 발생 원인을 식별하는 것이 더 상세한 해저드 원인을 파악하는데 효과적임을 확인할 수 있으며, STPA가 보다 많은 컴포넌트들의 상호작용으로 인한 발생 원인을 다루고 있음을 확인할 수 있다.

4.4 자동화 가능성

해저드 분석 기법은 많은 노력과 비용이 요구되는 활동이다. 해저드 분석 기법의 비용을 줄이고 효과를 향상시키기 위해서는 분석 과정을 자동화하는 것이 필요하다. PHA 기법의 경우 해저드 식별을 위해 체크리스트를 활용하나 브레인스토밍 방법에 의존하기 때문에 자동화

하는 것이 어렵다. 하지만 STPA 기법의 경우 준비 단계에서 시스템을 파악하고 제어구조도를 작성하는 부분까지는 자동화를 할 수 없지만 이후 단계는 가이드워드에 따라 해저드를 식별하고 발생 원인을 식별하는 과정에서도 가이드가 사용되기 때문에 부분적으로 자동화가 가능하다. 또한 STPA 기법의 경우 개발 단계가 달라져도 해저드 식별 가이드워드와 발생 원인을 식별하는 가이드가 변하지 않기 때문에 이 후 단계에서도 분석 기법의 재사용이 가능하다.

4.5 제약사항

PHA 기법과 STPA 기법은 개념 단계에서 해저드를 식별하는데 적합한 기법이지만 몇 가지 한계를 포함하고 있다. 먼저 PHA 기법은 시스템의 개별 컴포넌트를 중점으로 해저드를 식별하기 때문에 복잡한 소프트웨어 오류, 구성 요소들간의 상호작용에 따른 사고, 분석가의 오류나 실수, 복잡한 의사 결정 및 설계의 결함 관리와 같은 요소들에 대한 해저드를 식별하는데 제한이 있다. STPA 기법은 제어 명령과 피드백에 중점을 두어 제어 명령과 관련된 해저드는 쉽게 식별되지만 이외의 컴포턴트 자체에서 발생할 수 있는 위험과 위험 원인들을 식별하는데는 제한이 있다.

4.6 표준 준수 여부 비교

의료기기 분야의 시스템에서 해저드 분석 기법으로 사용되기 위해서는 의료기기 안전성 표준을 준수해야 한다. PHA 기법은 의료기기 위험 관리 표준인 ISO 14971에서 사용을 권장하는 개념 단계의 기법이다. STPA 기법의 경우 의료기기의 안전성 표준에서 권장 기법으로 명시되어 있지는 않지만 최근 적용 가능함을 증명하는 연구가 발표되고 있다. 따라서 두 기법 모두 의료기기 표준을 준수하여 적용 가능하다.

5. 결론 및 향후 연구

본 논문에서는 의료기기 분야의 시스템에서 해저드 분석 활동을 수행할 때 적합한 해저드 분석 기법을 선택할 수 있도록 전통적인 해저드 분석 기법과 STPA 분석 기법을 비교하였다. 6개의 분석 기준에 따른 비교 결과를 요약하면 다음 표 16과 같다.

(표 16) 비교 평가 결과
(Table 16) Summarizing assessment results

	PHA	STPA
해저드 분석 기법의 프로세스 평가 비교	프로세스 단계 별 활동 수행을 지원 도구가 부족함	프로세스 단계 별 활동 수행을 위한 가이드가 제공됨
식별된 해저드의 비교	다양한 관점에서 분석이 가능함	가이드워드에 한정된 관점에서 분석이 가능함
식별된 해저드의 원인 비교	원인의 범위와 수준이 상세하지 않음	상세한 원인 식별이 가능함
자동화 가능성	어려움	일부 용이함
제약사항	컴포넌트 고장 이외의 해저드 식별이 어려움	컴포넌트 고장에 대한 해저드 식별에 제한이 있음
표준 준수 여부 비교	표준 준수 (ISO14971)	표준 준수 (ISO14971)

첫 번째로, PHA 기법의 경우에는 브레인스토밍 기법에 의존하기 때문에 분석가의 역량이 중요함을 확인할 수 있었다. 반면에 STPA는 가이드워드를 적용하므로 분석의 자동화와 상세한 원인 분석이 가능했다. 두 번째로 PHA 기법의 프로세스 단계별 활동을 지원할 방법이 부족하여 분석 활동이 용이하지 않지만 STPA 기법은 프로세스 단계 별로 가이드가 제공되어 상대적으로 분석 활동이 용이하였다. 세 번째로, 두 기법으로 식별된 해저드를 비교한 결과, 일부 유사한 해저드가 식별되기는 했으나, 대부분의 해저드 및 해저드의 원인들이 상당 부분 상이하기 때문에 특정 기법이 상대적으로 분석에 유용하다는 결론을 내릴 수는 없다. 이러한 차이는 각 기법에서 적용하는 가이드워드의 사용과 브레인스토밍의 차이에서 기인하고 있기 때문이다. 따라서 분석의 목표와 의료기기의 특성에 따라 두 기법을 상호 보완 적용하는 것이 필요하다.

본 연구에서는 계념 단계에서의 해저드 분석 활동에 대해서만 비교하였으므로 이후 개발 단계에서 다른 전통적인 해저드 분석 기법들과 STPA 기법을 비교하는 연구가 필요하다. 또한 인슐린 펌프 시스템 외의 다양한 의료분야의 시스템들에도 분석을 적용할 필요가 있다.

참고문헌(Reference)

[1] Young, William, Nancy Leveson. "Systems thinking for safety and security", Proceedings of the 29th Annual Computer Security Applications Conference. ACM, 2013.
http://dx.doi.org/10.1145/2523649.2530277

[2] Leveson, Nancy, "Engineering a safer world: Systems thinking applied to safety," MIT press, 2011.
https://mitpress.mit.edu/books/engineering-safer-world

[3] Clifton A. Ericson II, "Hazard Analysis Techniques for System Safety," WILEY, 2015
https://www.wiley.com/en-us/Hazard+Analysis+Techniques+for+System+Safety%2C+2nd+Edition-p-9781118940389

[4] Helga Einarsdottir, "Comparison of the application of risk management to medical devices guided by ISO 14971 and STAMP," Reykjavik University, 2017
http://hdl.handle.net/1946/28776

[5] Homa Alemzadeh, Daniel Chen, Andrew Lewis, Zbigniew Kalbarczyk, Jaishankar Raman, Nancy Leveson, Ravishankar Iyer, "Systems-Theoretic Safety Assessment of Robotic Telesurgical Systems", SAFECOMP 2014: Computer Safety, Reliability, and Securitypp pp.213-227, 2015
https://doi.org/10.1007/978-3-319-24255-2_16

[6] Masci P, Zhang Y, Jones P and Campos JC, "Extending STPA to Improve the Analysis of User Interface Software in Medical Devices," STAMP Workshop 2018, 2018
https://doi.org/10.1007/978-3-319-66197-1_18

[7] Kadupukotla Satish Kumar and Panchumarthy Seetha Ramaiah "Hazard Analysis and Metrics Identification for Software Safety in Medical Cyber-Physical Systems," International Journal of Applied Engineering Research, Volume 11, Number 10, pp 7188-7195, 2016
https://pdfs.semanticscholar.org/3f52/6e88894eb2d70dae3f43f55e44ef3756b909.pdf

[8] Yi Zhang, Paul L. Jones, M.S.C.E, and Raoul Jetley, "A Hazard Analysis for a Generic Insulin Infusion Pump," Journal of Diabetes Science and Technology, Volume 4, Issue 2, pp.263-283, March 2010
https://doi.org/10.1177/193229681000400207

[9] Masci P, Zhang Y, Jones P, Thimbleby H and Curzon P. "A generic user interface architecture for analyzing use hazards in infusion pump software" Proceedings of Medical Cyber Physical Systems Workshop (MedCPS2014), 2014
https://doi.org/10.4230/OASIcs.MCPS.2014.1

[10] Sardar Muhammad Sulaman, Armin Beer, Michael Felderer and Martin H¨ost, "Comparison of the FMEA and STPA safety analysis methods: a case study" Software quality journal, pp. 1-39, 2017
https://doi.org/10.1007/s11219-017-9396-0

◐ 저 자 소 개 ◑

최 보 윤(Bo-yoon Choi)
2007년 서울여자대학교 컴퓨터학과(공학사)
2009년 서울여자대학교 대학원 컴퓨터학과(이학석사)
2017년 서울여자대학교 대학원 컴퓨터학과(이학박사)
2017년~현재 상명대학교 산학협력단 산학협력교수
관심분야 : 소프트웨어 안전성, 소프트웨어 프로세스, 소프트웨어 테스팅 etc.
E-mail : choiby@ssarc.re.kr

이 병 걸(Byong-gul Lee)
1988년 University of Bridgeport 물리학과(이학사)
1996년 Auburn University 대학원 전산학과(공학석사)
1998년 Auburn University 대학원 전산학과(공학박사)
1998년~현재 서울여자대학교 미래산업융합대학 정보보호학과 교수
관심분야 : 소프트웨어 보안, 소프트웨어 안전성, 소프트웨어 아키텍처, 소프트웨어 프로세스 etc.
E-mail : byongl@swu.ac.kr

한 혁 수(Hyuk-soo Han)
1985년 서울대학교 계산통계학과(공학사)
1987년 서울대학교 대학원 계산통계학과(공학석사)
1992년 South Florida 주립대학교 대학원 컴퓨터공학과(공학박사)
1993년~현재 상명대학 전기전자컴퓨터학부 컴퓨터과학과 교수
관심분야 : 소프트웨어 프로세스, 소프트웨어 품질, 소프트웨어 안전성 etc.
E-mail : hshan@smu.ac.kr