FTA와 FMECA의 통합 방법의 안전성 분석에 대한 연구 및 유비쿼터스 응급구난 시스템에의 적용

김규아*, 박만곤**
*부경대학교 공과대학 IT융합응용공학과
e-mail : kga1203kr@naver.com, mpark@pknu.ac.kr

A Study in the Safety Analysis Forward and Backward Integration Method of FTA and FMECA and the Application of Ubiquitous Emergency Rescue System

*Gyu-Ah Kim, **Man-Gon Park
*Dept of Information Systems, Pukyong National University

요 약

현재에 시스템의 결함을 분석하는 안전성 분석 기법들이 여러 가지가 있다. 본 논문에서는 많은 결함 분석 기법 중에서 FTA(Fault Tree Analysis)와 FMECA(Failure Modes, Effect and Criticality Analysis)을 통하여 안전성 분석을 하고자 한다. 또한 이 두 가지 기법을 따로 사용하지 않고 전방에서 FTA 분석을 하고 후방에서 FMECA 분석을 수행하는 통합 기법을 제안한다. 이를 통해 각 기법의 단점을 최소화하고 장점을 최대화 하여 안전성 분석의 효율성을 제고하고자 한다.

1. 서론

과거의 인간-기계 시스템(Human-Machine System)은 각종 장치들이 컴퓨터와 반도체 기술의 발달에 힘입어 안전성 확보를 위한 많은 부분에서 감시 및 통제 기능을 수행함으로써 인간을 대신하고 있다. 이에 따라 감시 및 통제 기능을 수행하는 내장 소프트웨어 또는 제어용 탑재 소프트웨어 시스템이 정상적으로 동작을 하는지에 관심 생겨났고, 안전 중심 시스템에서 하드웨어 또는 소프트웨어의 결함으로 재난 또는 사고가 발생하기 시작하자 시스템의 보안 및 안전을 보장해 주기 위한 연구들에 대해 큰 관심을 가지게 되었다. 안전성 분석 작업들은 시스템 안전성을 담당하는 인력과 소프트웨어 품질 보증 인력 그리고 독자적인 안전성 엔지니어에 의해서 수행된다. 따라서 안전성 작업들의 목표는 시스템에 통합되어진 최종 소프트웨어가 안전한가를 보증하는 것이다.

안전성이란 안전하거나 안전을 보장하는 성질로써 사고나 손실로부터 자유로운 상태라고 정의할 수 있다. 시스템의 경우 외부로부터의 잘못된 입력으로부터 시스템을 안전하게 지켜 주고 재난의 발생을 막기 위한 통제를 수행할 수 있을 것인가에 관심을 갖는 것을 말한다. 안전성과 관련하여 많은 컴퓨터 시스템이 사용되어지고 내장된 소프트웨어의 안전성과 보안성에 대하여 사람들의 관심이 높아짐으로써 이러한 기법들이 개발되고 있거나 양도되고, 사용 중인 소프트웨어 시스템의 안전성을 보증하는 증명이 필요하게 되었다. 이를 행하는 과정을 안전성 분석이라고 한다. 즉 안전성 분석이란 소프트웨어 시스템이 가지고 있는 안전성에 관련된 결함을 분석함으로써 소프트웨어의 안전성을 증명하거나, 발견된 결함을 제거하는 기술에 관하여 보다 심도 있는 연구이다.

2. FTA

FTA는 결함 트리 분석으로 위험들을 평가하고 제어하기 위한 표준화된 방식을 제공하고 해당 프로세스는 넓고 다양한 문제들을 해결하는데 사용된다. 이는 효과적인 방법을 제시하며 고장과 위험을 나타내는 논리적 도식 표현의 결함 트리 다이어그램으로 나타낼 수 있다. FTA에 해당하는 기호는 <표 2>에 나타나 있다.

기호	내용
	논리 게이트를 통해 사건들의 결합으로 생겨난 사건을 나타내는 기호
	기본 사상(Basic Event): 더 이상 발달을 요구하지 않는 기본적인 오류 사건을 나타내는 기호
	AND 게이트: 하위의 사건을 모두 만족하는 경우에 사용하는 논리 게이트
	OR 게이트: 하위의 사건 중 하나라도 만족하면 사용하는 논리 게이트

<표 1> FTA에 사용되는 기호들

3. FMECA

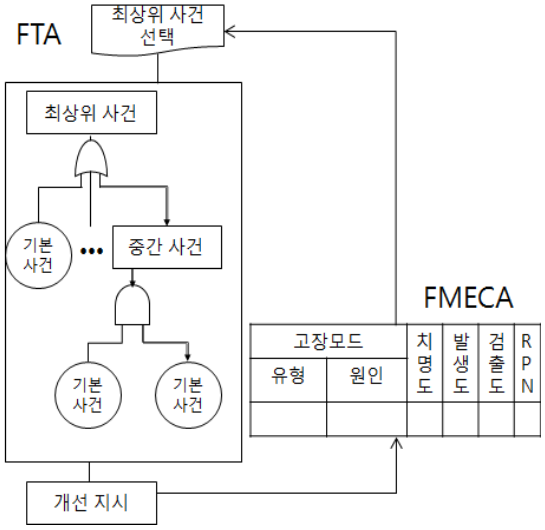
FMEA에서 특히 고장 영향의 치명도에 대한 정도를 중요시 할 때에는 FMECA을 사용한다. 이 분석 기법은 완성된 부품이나 시스템의 안전성을 검토하기 위한 것이 아니라, 앞으로 개발하려고 하는 부품이나 시스템의 설계를 개선하여 시스템의 안전성을 높이는 데에 있다.

	수행 내용
치명도	0≦치명도<1.0 : 아무런 위험 없음 1.0≦치명도<3.0 : 심각하지 않음 3.0≦치명도<6.0 : 중함 6.0≦치명도<9.0 : 심각함 9.0≦치명도<10.0 : 치명적임 치명도=10.0 : 재앙적임
발생도	0≦발생도<1.0 : 발생 가능성 없음 1.0≦발생도<3.0 : 발생 가능성 거의 없음 3.0≦발생도<6.0 : 이따금씩 있음 6.0≦발생도<9.0 : 발생 가능성 높음 9.0≦발생도<10.0 : 발생 가능성 아주 높음 발생도=10.0 : 발생 가능성이 매번 있음
검출도	0≦검출도<1.0 : 고장검출능력 확실함 1.0≦검출도<3.0 : 거의 확실함 3.0≦검출도<6.0 : 고장검출능력 빈번함 6.0≦검출도<9.0 : 고장검출능력 조금 있음 9.0≦검출도<10.0 : 거의 불확실함 검출도=10.0 : 고장검출능력이 없음
RPN	위험 우선순위(Risk Priority Number; RPN) RPN = 치명도×발생도×고검출도

<표 2> FMECA의 용어와 그 정의

4. FTA와 FMECA의 통합

FTA와 FMECA의 통합은 먼저 시스템의 결함 트리를 만들기 위한 최상위 사건을 선택하고 FTA를 분석한다. 이후 FMECA에 의해 치명도 분석이 이루어진 후에 최상위 사건의 발생 정도를 계산 할 수 있다.

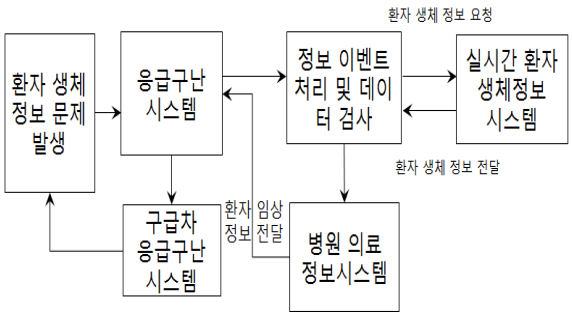


(그림 2) FTA와 FMECA의 통합

5. 유비쿼터스 응급구난 시스템에 통합 FTA와 FMECA의 적용

5.1 유비쿼터스 응급구난 시스템

산업이 다양화되고 고도화됨에 따라 각종 정보의 감지 및 이의 변환 기술을 크게 필요로 하게 되어 각 산업에서 첨단 센서는 매우 중요한 위치를 차지하게 되었다. 유비쿼터스 센서 네트워크(Ubiquitous Sensor Network; USN)란 필요한 모든 곳에 전자 태그를 부착하고 이를 통하여 사물의 인식 정보를 기본으로 주변의 환경 정보(온도, 습도, 오염정보, 균열 정보 등) 까지 탐지하여 이를 실시간으로 네트워크에 연결하여 정보를 관리하는 것을 말하는 것으로 궁극적으로 모든 사물에 컴퓨팅 및 커뮤니케이션 기능을 부여하여 언제 어디서나 언제라도 통신이 가능한 환경에서 원하는 서비스를 제공받기 위한 것이다. 유비쿼터스가 적용된 예기치 못한 급작스러운 응급 상황 및 테러 등 각종 대량 재해 시 사고 예방 및 응급 환자 관리 차원에서 응급 처치 및 구난을 하는 시스템을 유비쿼터스 응급구난 시스템이라고 한다. (그림 2)은 유비쿼터스 응급구난 시스템의 서비스 플랫폼이다. 이를 토대로 FTA를 분석한다.



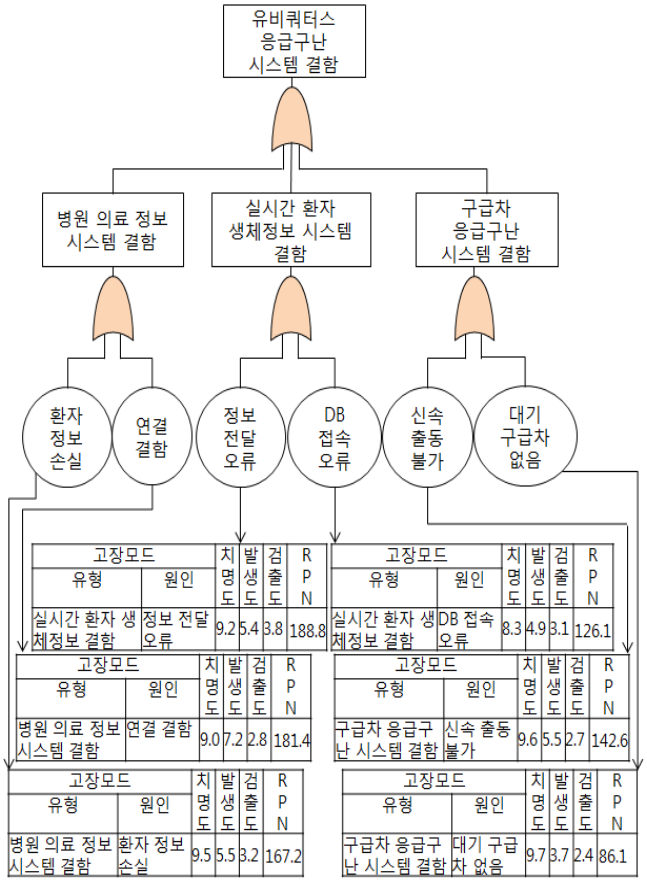
(그림 2) 유비쿼터스 응급구난 시스템의 서비스 플랫폼

5.2 통합 FTA와 FMECA의 적용

FTA와 FMECA의 통합은 각 결함 분석의 장점을 살려 효과적인 결과를 가져다준다. FTA는 사고원인 규명의 간편화를 가져오고 결함 발생의 모든 원인들의 연쇄를 한눈에 알기 쉽게 결함 원인을 분석해서 일반화할 수 있다. 또 다른 기법인 FMECA는 수치적으로 치명도, 발생도, 검출도를 통하여 RPN값을 도출 할 수 있다.

FTA는 탑다운 결함 분석 방식으로 시각적으로 이해가 쉽다. 최상위의 사건이 각 기본 사건에 의해 발생되어지는 원인과 결과의 규명이 용이하다. (그림 3)을 보면 유비쿼터스 응급구난 시스템의 결함이 OR 게이트로 연결되어진 각 중간 사건과 기본 사건에 의해 연결되어 있는 것을 알 수 있다. 예로 병원 의료 정보 시스템의 결함은 환자 정보 손실 또는 연결 결함에 의해 발생하여 유비쿼터스 응급구난 시스템의 결함을 발생 시킨다.

FMECA는 수치적 분석이 장점이다. 고장모드의 유형은 FTA의 중간 사건과 연결되고 원인은 기본 사건과 연결된다. FMECA의 치명도, 발생도, 검출도 그리고RPN은 <표 2>에서 다루었다. (그림 3)의 여섯 가지 기본 사건의 FMECA의 결과는 실시간 환자 생체정보 시스템의 결함 원인 중의 하나인 정보 전달 오류가 RPN이 가장 높다. 이처럼 RPN에 의해 결함 원인들의 우선순위를 정할 수도 있다.



(그림 3) 유비쿼터스 응급구난 시스템에 통합 FTA와 FMECA의 적용

6. 결론

현재에 안전성 개선을 위한 여러 가지 결함 분석들이 있다. 하지만 IT 기술과 멀티미디어 처리 기술이 발전하면서 시스템의 종류와 그 특성이 다양해져 하나만의 결함 분석 기법으로는 정확한 결함 분석을 할 수 없게 되었다. 따라서 본 논문에서는 결함 트리 분석인 FTA와 고장 유형과 영향 분석인 FMECA 기법을 통합하여 유비쿼터스 응급구난 시스템의 안전성을 평가해보았다.

본 논문에서 제안한 통합 분석 기법은 전방에서 FTA를 통한 탑다운 방식의 다이어그램 분석을 하고 후방에서 표를 이용한 수치적 분석을 하는 FMECA를 이용하는 통합 방법이다. 이는 단 한가지의 결함 분석에 의한 결과 보다 더욱 효율적인 결과를 가져온다. FTA의 시각적 효과와 FMECA의 수치적 효과가 그 결과이다.

참고문헌

[1] 김두현, 이종호, “FMEA를 이용한 건설현장 전력설비의 위험성에 대한 정성적 평가,” 한국안전학회지, 제 19권, 제 14호, pp.36-41, 2004,

[2] 김상연, 윤원영, 김호균, “가전용 모터의 FMEA 실시 과정에서의 RPN 평가방법 재정립,” 품질경영학회지, 제 35권, 제 1호, pp.1-9, 2007.

[3] 김은미, “FTA를 이용한 안전성 검증에 대한 고찰,” 한국정보과학회지, 제 25권, 제 2호, pp.582-584, 1998.

[4] 김홍규, 문승진, “u-EMS:바이오 센서 네트워크 기반의 응급 구조 시스템,” 정보과학회논문지, 제 13권, 제 7호, pp.433-441, 2007.

[5] 김효영, 한혁수, “SW-FMEA 기반의 결함 예방 모델,” 정보과학회논문지, 제 33권, 제 7호, pp.605-614, 2006.

[6] 김명희, 박만곤, “소프트웨어 안정성 평가를 위한 소프트웨어 고장 유형과 영향 분석에 관한 연구,” 멀티미디어학회논문지, 제 15권, 제 1호, pp.113-130, 2012.

[7] 박현기, “전자 교수학습 시스템의 보안성 개선을 위한 결함분석과 고장영향분석의 통합방법에 관한 연구”, 부경대학교 박사학위논문, pp.1-80, 2012.

[8] 오암석, “효율적인 응급의료서비스를 위한 HL7 기반 응급의료시스템 설계 및 구현,” 동명대학교 박사학위논문, pp.1-84, 2011.

[9] 이익성, “고장모드 영향분석(FMEA)을 통한 컨벤션산업 품질개선 연구,” 한국컨벤션학회, 제 5권, 제 1호, pp.101-107, 2005.

[10] 장중순, “효과적인 FMEA 실시 절차에 관한 연구,” 대한설비관리학회지, 제 4권, 제 4호, pp.69-77, 1999.

[11] 장중순, 안동근, “효과적인 FMEA 실시,” 품질경영학회지 제 25권, 제 1호, pp.156-172, 1997.

[12] Adem Sabic, jasmin Azemovic, “Model of Efficient Assessment System with Accent on Privacy, Security and Integration with e-University Components,” Second International Conference on

Education Technology and Computer(ICETC), Vol. 3, pp.128-131, 2010.

[13] M. Ben-Daya, Abdul Raouf, “A Revised Failure Mode and Effects Analysis Model,” International Journal of Quality & Reliability Management, Vol. 13, No. 1, pp.43-47, 1996.

[14] N. Snooke, C. Price, “Model-driven automated software FMEA,” Proceedings of Reliability and Maintainability Symposium (RAMS), pp.1-6, 2011.

[15] Rodrigo de Queiroz Souza, Alberto José Álvares, “FMEA and FTA Analysis for Application of the Reliability Centered Maintenance Methodology: Case Study on Hydraulic Turbines,” ABCM Symposium Series in Mechatronic, Vol. 3, pp.803-812, 2008.

[16] Thomas Maier, “FMEA and FTA to Support Safety Design of Embedded Software in Safety-Critical Systems,” Proceedings of CSR 12th Annual Workshop on Safety and Reliability of Software Based Systems, pp. 351-367, 1997.

[17] Zhang Hong, Liu Binbin, "Integrated Analysis of Software FMEA and FTA," Proceedings of International Conference on Information Technology and Computer Science, pp.184-187, 2009.