Journal of Korea Multimedia Society Vol. 20, No. 11, November 2017(pp. 1793-1802)
https://doi.org/10.9717/kmms.2017.20.11.1793

스마트 러닝 시스템의 보안성 개선을 위한 고장 트리 분석과 고장 유형 영향 및 치명도 분석

천회영†, 박만곤††

Fault Tree Analysis and Failure Mode Effects and Criticality Analysis for Security Improvement of Smart Learning System

Hoe-Young Cheon†, Man-Gon Park††

ABSTRACT

In the recent years, IT and Network Technology has rapidly advanced environment in accordance with the needs of the times, the usage of the smart learning service is increasing. Smart learning is extended from e-learning which is limited concept of space and place. This system can be easily exposed to the various security threats due to characteristic of wireless service system. Therefore, this paper proposes the improvement methods of smart learning system security by use of faults analysis methods such as the FTA(Fault Tree Analysis) and FMECA(Failure Mode Effects and Criticality Analysis) utilizing the consolidated analysis method which maximized advantage and minimized disadvantage of each technique.

Key words: Smart Learning System, Software Security, Fault Tree Analysis(FTA), Failure Modes Effects and Criticality Analysis(FMECA)

1. 서 론

지금은 정보통신기술을 활용하여 새로운 가치들이 창출되면서 우리의 삶의 형태가 바뀌고 있는 스마트(Smart)시대이다. 스마트 디바이스의 확산으로 모바일 멀티미디어 콘텐츠를 누구나 이용할 수 있고 시간과 장소에 제약 없이 언제 어디서든 즐길 수 있는 시대가 된 것이다. Table 1에서는 2016년 10월 기준 스마트폰과 태블릿PC를 통한 인터넷 이용률이 51.3%로 데스크탑을 통한 인터넷 이용률(48.7%)을 추월한 것으로 나타내고 있다. 이제 인터넷 이용 단말로서 PC의 역할은 거의 끝이 난 것으로 판단되며, 업무 시간의 인터넷 검색, PC를 통해서만 가능한 작업, PC에서만 이용 가능한 게임 등을 제외한 인터넷 서비스 이용 단말로의 역할은 스마트폰과 태블릿PC가 담당하고 그 영향력이 더욱 확대될 것으로 전망하고 있다.

Table 1. Percentage of Internet Usage by Device
(Unit:%)

Year / Classification	2011	2012	2013	2014	2015	2016
Desktop	93.5	85.0	76.7	62.8	55.9	48.7
Smartphone +Tablet PC	6.6	15.0	23.3	37.2	44.2	51.3

정보통신 환경의 변화로 교육환경도 급격한 변화

※ Corresponding Author : Man-Gon Park, Address : (48513) Yongso-Ro 45, Nam-Gu. Busan, Rep. of Korea, TEL: +82- 51-629-6240, FAX : +82-51-629-6230, E-mail : mpark@pknu.ac.kr
Receipt date : Sep. 25, 2017, Approval date : Oct. 23, 2017

† Dept. of Information Systems, Pukyong Nat. Univ., Rep. of Korea
(E-mail : hycheun@naver.com)
†† Dept. of IT Convergence and Application Engineering, PuKyong Nat. Univ., Rep. of Korea

를 거듭하며 새로운 미디어를 통한 미디어 간 융합이 활발하게 이루어지고 있다. 이제는 인터넷에 접속하여 온라인 강의를 수강하던 학습형태를 탈피하여 스마트폰과 같은 스마트 디바이스를 사용하여 수강 및 학습활동에 참여하여 자신의 학습에 필요한 정보를 얻는 스마트 러닝이 확산되고 있다[1]. 스마트 러닝은 장소와 공간의 개념이 제한적이었던 이러닝에서 확장된 개념으로 유비쿼터스 학습 환경을 기반으로 시간, 공간, 환경 등에 구애받지 않고 언제, 어디서나 원하는 학습을 가능하게 하는 스마트 디바이스를 활용한 형태로 유선 웹기술을 사용하는 이러닝과는 달리 무선 웹기술 환경 기반에서 서비스된다[2].

언제 어디서나 원하는 학습을 할 수 있는 스마트 러닝 시스템의 편리함 이면에 시스템 내에 존재하는 다양한 보안 위협 또한 함께 수반되고 있다. 보안 위협 (Security Threats)은 주로 사용자 인증 (User Authentication) 단계와 접근 통제 (Access Control) 단계 그리고 바이러스 탐지 및 통제(Virus Detection and Control) 단계에서 가장 많이 발생한다. 그 외에도 스마트 러닝 시스템 내의 운영체제, 데이터베이스, 네트워크 등에서도 보안성이 위협 당하고 있다. 점차 다양하고 고도화된 해킹 기법으로 스마트 러닝 시스템을 위협하여 사용자들에게 피해를 줄 것으로 예상된다[3].

따라서 본 논문에서는 스마트 러닝 시스템이 가지고 있는 보안성에 관련된 결함을 분석함으로써 시스템의 보안성을 개선하고자 한다. 결함 분석을 위해 FTA와 FMECA를 이용하여 시스템의 보안성을 보다 더 개선되고 강화되도록 각 기법의 장점을 최대화하고 단점을 최소화시킨 통합된 결함 분석 기법을 사용한다. 통합 방법으로 FTA에 FMECA를 전방으로 통합하는 방법과 FTA에 FMECA를 후방으로 통합하는 방법을 중심으로 시스템의 실제적인 결함 분석 프로세스를 정의하고 그에 따른 실험적인 결과 분석을 수행한다.

2. 관련연구

2.1 결함 트리 분석(Fault Tree Analysis; FTA)

시스템에 발생하는 중대한 결함이 어떤 원인에 의해서 발생하는가를 이론적으로 분석하고 세분화해서 최종적으로는 1개 부품의 결함 원인까지 규명해 가는 하향성(Top-Down) 방식의 기법으로 결함 원인을 식별하고, 식별된 결함원인을 분석하여 Fault Tree(FT)를 작성하고 이를 기반으로 하여 구성된 Fault Tree에서 정상사상이나 중간사상의 발생 확률들을 계산하여 시스템의 안전성 및 신뢰도 분석 및 평가하는 도구로 사용한다. Fig 1은 FT의 작성을 보여준다[4,5].

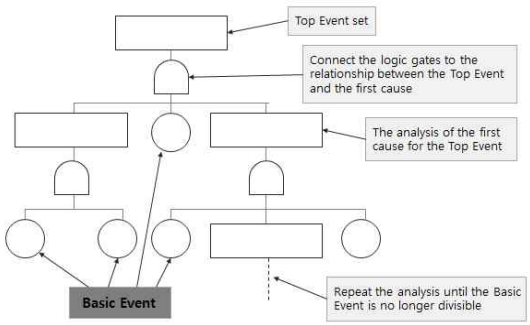


Fig. 1. FT compose.

2.2 고장 유형 영향 및 치명도 분석(Failure Modes Effects and Criticality Analysis; FMECA)

고장 또는 결함으로 인한 결과를 예상하고 부정적인 결과를 제거하기 위한 방법으로 FMECA는 시스템 개발 초기 단계에서 가장 많이 신뢰성 분석 기술에 사용되고 있으며 일반적으로 개념 또는 초기 설계 단계에 수행되는데 가능성 있는 모든 고장 유형을 확인하고 적절한 조치를 취하여 고장을 줄이도록 한다. FMECA기법은 전형적인 귀납적 분석방법이며 상향성(Bottom-Up), 정성적인 위험성 분석기법의 대표라고 할 수 있으며, 특히 결함과 다음 상위 수준의 기능적 시스템에 미치는 영향과 메커니즘을 연구하는 데 적합하다[6,13].

FMECA의 수행은 시스템의 모든 가능한 고장모드를 알아내어 원인과 결과 각각의 고장위험도를 파악하고 고장 모드의 위험 우선순위(RPN)를 계산한다. 계산에 따라 각각의 고장 모드를 평가하고 적절한 개선 수행을 실행한다. 이에 따라 결함은 줄어들며 개선 수행 후 RPN을 다시 계산하여 안정성의 개선 사항을 확인한다. 따라서 FMECA를 통하여 최종적으로 시스템의 안정성을 확보할 수 있다[7,8].

다음 Table 2는 전방 FMECA의 표이다. 고장 모드는 FTA의 중간 사건에 해당하며 원인은 기본 사

건 결과는 최상위 사건에 해당한다. 치명도는 0점에서 10.0점 사이에서 점수화되며 작을수록 치명도가 낮다.

Table 2. As a result of compensating provision forward FMECA

Failure Modes	Causes	Effects	Severity	Compensating Provision

2.3 FTA와 FMECA의 통합적 방법

FTA는 하향성 방식으로 원하지 않은 사건 또는 결함을 발생시키는 원인을 찾는 기법인 반면에 FMECA는 상향성 방식으로 안정성 중심 소프트웨어 시스템에서 가능한 소프트웨어 고장 모드의 결과를 확인하는 기법이다. 두 가지 기법을 각각 따로 사용한다면 통합하여 사용하는 것에 비해 각 기법의 단점 때문에 효율적인 결과를 도출할 수 없다. FMECA는 표 형식의 자료이고 소프트웨어 결함의 원인 사이의 논리 관계를 설명하기 어렵다는 단점이 있고 FTA는 최상위 사건을 선택하는 것이 어렵다. 따라서 FTA와 FMECA를 통합하여 사용하면 각 기법의 단점을 최소화할 수 있다[9].

FTA는 시스템의 원인 규명을 간편히 할 수 있고 결함이 발생하는 모든 원인들 관계들을 알기 쉽고 FMECA는 시스템의 결함에 관련된 치명도 발생도 검출도를 수치적으로 파악할 수 있어 결함율 계산에 용이하다. 따라서 시스템의 결함 원인을 알 수 있는 FTA와 수치적으로 계산할 수 있는 FMECA를 통합하여 실시함으로써 FTA와 FMECA의 장점을 활용할 수 있다.

2.3.1 FTA에 FMECA를 전방으로 통합한 기법

FTA에 FMECA를 전방으로 통합한 기법은 FMECA를 수행 후에 FTA가 이루어지는 기법으로 Fig. 2와 같이 정의한다. FMECA의 결과에 의하여 고장 원인과 결과 및 치명도가 형성되고 치명도의 영향은 FTA의 최상위 사건으로 활용된다. 고장모드는 FMECA로 FTA의 중간 사건으로 사용된다. FMECA의 원인은 FMECA만을 사용한 것보다는 FTA에 FMECA를 전방으로 통합한 기법으로 사용하는 것이 더욱 포괄적으로 형성되어 진다[9].

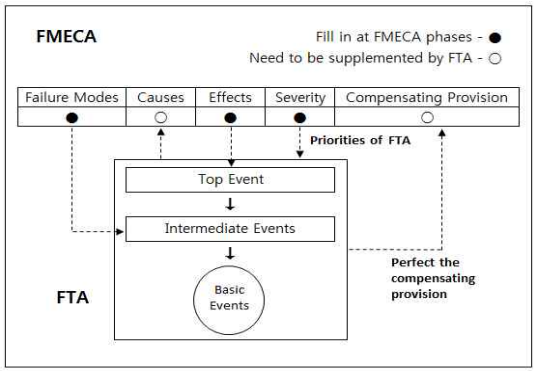


Fig. 2. Technique of forward integration of FMECA in FTA.

2.3.2 FTA에 FMECA를 후방으로 통합한 기법

FTA에 FMECA를 후방으로 통합한 기법은 FTA 수행 후에 FMECA가 이루어지는 기법으로 Fig 3과 같이 정의한다. FTA에 FMECA를 후방으로 통합한 기법은 먼저 결함 트리를 만들기 위한 최상위 사건을 선택한다. 최상위 사건 선택 후 FTA가 수행되어 질적인 분석을 통해 FMECA에 의하여 치명도 발생도 검출도 RPN 개선율을 계산한다. 이후 개선 수행을 통해 새로운 원인이 있으면 FTA가 다시 수행되고 없으면 FMECA를 바로 수행한다. 그리고 고장 영향의 치명도에 따라 새로운 최상위 사건이 나타나면 결함 트리는 수정 가능하다[9].

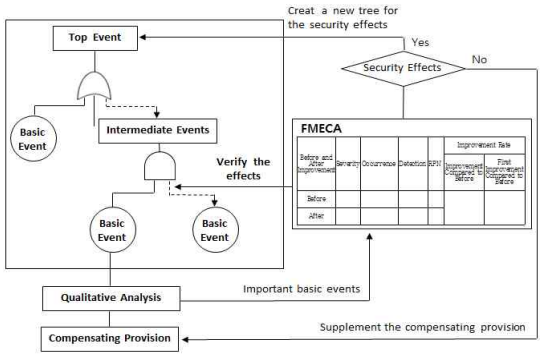


Fig. 3. Technique of backward integration of FMECA in FTA.

2.3.3 FTA와 FMECA를 전·후방으로 통합한 기법

FTA에 FMECA를 전방으로 통합한 기법은 전방

FMECA를 통하여 최상위 사건의 원인이 되는 각 기본 사건들의 치명도를 먼저 구함으로써 우선순위를 구할 수 있는 장점이 있으나 치명도 이외의 수치를 구하지 못함으로 인해 기본 사건들의 개선 수행을 하지 못하는 단점이 있다.

FTA에 FMECA를 후방으로 통합한 기법은 후방 FMECA를 통하여 FTA 분석에 따른 안정성 중심 시스템의 치명도 발생도 검출도 RPN과 개선율을 구함으로 FTA의 최상위 사건의 결함을 개선할 수 있다. 하지만 시스템의 최상위 사건을 일으키는 모든 기본 사건들을 구해야 하므로 특정 시스템의 결함이 발생할 경우 우선순위를 판단하지 못해 결함을 개선하는데 많은 시간이 걸릴 수 있다[9].

따라서 본 논문에서는 FTA와 FMECA를 전·후방으로 통합한 기법을 Fig 4와 같이 제시한다. 먼저 전방 FMECA 수행 후에 중간에서 FTA 분석이 이루어지고 마지막을 후방 FMECA 수행을 하는 기법이다. FTA와 FMECA를 전·후방으로 통합한 기법은 기존 전방과 후방 기법의 단점을 개선할 수 있다. 전방 FMECA에서 치명도를 구함으로 안정성 중심 시스템의 최상위 사건을 일으키는 기본 사건들의 우선순위를 구할 수 있다. 이를 통해 모든 기본 사건들을 순서대로 후방 FMECA 작업을 할 필요 없이 전방 FMECA에 의한 치명도의 우선순위에 의하여 시스템의 결함을 개선할 수 있어 신속하게 대처할 수 있는 장점이 있다.

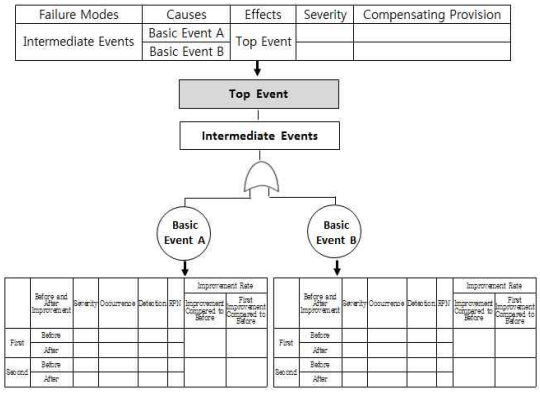


Fig. 4. Technique of backward and forward integration of FMECA in FTA.

3. 스마트 러닝 시스템의 보안성 개선을 위한 FTA와 FMECA의 통합

FTA와 FMECA의 통합 기법인 FTA에 FMECA를 전방으로 통합한 기법과 FTA와 FMECA를 후방으로 통합한 기법을 모두 통합하여 하나의 통합 기법을 수행하여 스마트 러닝 시스템의 보안성을 개선하여 향후에 발생하는 잠재적인 결함을 예방할 수 있도록 한다. 먼저 시스템의 보안성을 개선하기 위해서는 각각의 기능별 보안 취약점을 파악해야 하며 이를 위해서는 기능 블록 다이어그램이 정의되어야 한다. P대학교의 스마트러닝 시스템의 2016년 9월 1일부터 2017년 6월 30일까지 실험적 결과 분석을 토대로 Fig 5는 스마트 러닝 시스템의 기능 블록 다이어그램을 Table 5는 시스템 내에 존재하는 보안 취약점을 Table 6은 보안 취약점을 바탕으로 결함 리스트를 작성하였다.

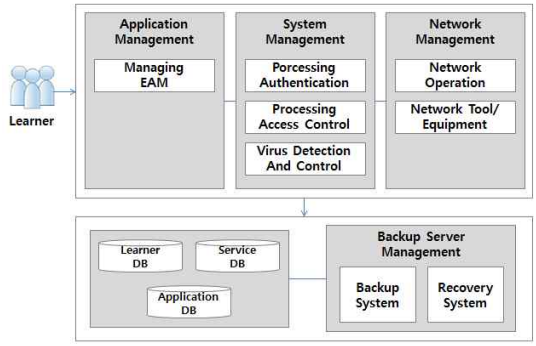


Fig. 5. Security functional block diagram of smart learning system.

3.1 Application Management 부분의 FTA와 FMECA의 전·후방 통합적 분석

Fig. 6은 스마트 러닝 시스템의 Application Management 부분의 FTA와 FMECA의 전·후방 통합적 분석으로 전방에서 FMECA에 의하여 EAM (Extranet Access Management)의 오류를 분석하고 이를 토대로 FTA를 수행하여 후방에서 FMECA를 통하여 치명도(S), 발생도(O), 검출도(D), RPN 그리고 개선율을 구한다. 이후 보안 위협 탐지하기 위한 모듈을 추가하여 개선 수행을 한 후 전방 FMECA, FTA을 거쳐 후방 FMECA를 통해 1차 개선 값을 구한다. 본 논문에서는 2차 개선까지의 값을 구해보았다.

치명도 결정(Determination of Severity)은 오류가 발생했을 때 단지 시스템 성능 감소인지 아니면

시스템의 파과나 인명 피해가 있는지 특정 오류로 인한 영향이나 충돌의 중요성을 참조하여 오류 결과 범위를 정할 수 있다. 이러한 오류 영향을 실례를 통해 표현하기 위해서 치명도를 0에서 10까지 정량적으로 Table 3과 같이 표시 한다.

Table 3. Severity

Severity	Miner	Major	Critical	Catastrophic
Rating	0-2	3-6	7-8	9-10

발생도(Occurrence)는 각 시스템별로 기능블록 다이어그램과 결함 목록 리스트에 의한 정상사상이나 중간사상, 즉 구하고자 하는 결함 발생 빈도를 계산한 것이다. 검출도(Detection)는 시스템이 사용자에게 양도하기 이전에 오류를 검출할 수 있는 능력을 표현하기 위해서 0에서 10까지 정량적으로 table 4와 같이 표시 한다.

Table 4 Detection

Detection	Very high	High	Moderate	Low	Very low	Nondetection
Rating	0-2	3-4	5-6	7-8	9	10

고장 모드의 우선순위 (Risk Priority Number; RPN)는 각각 치명도(Severity), 발생도(Occurrence), 검출도(Detection)의 곱으로 계산하고, 개선율은 (개선 전 RPN - 개선 후 RPN) / (개선 전 RPN)을 이용하여 구할 수 있다.

3.2 System Management 부분의 FTA와 FMECA의 전 · 후방 통합적 분석

Fig. 7은 전방에서 FMECA에 의하여 접근 통제 단계에서 발생하는 결함들을 제거하고 위험을 최소화하기 위해서 잠재적 결함 요인과 실제 결함 요인을 접근 통제 시스템의 핵심인 운영체제 시스템, 미들웨어 시스템, 하드웨어 시스템에 따라 분석하였다. 이를 기반으로 치명도(S), 발생도(O), 검출도(D)를 사용하여 위험우선순위(RPN)를 매긴 결과 운영체제 시스템에서 가장 높게 기록되었다. 이후 파일 시스템 암호화, 보안 샌드 박스 시스템 작동 원격 제어, 데이터베이스 시스템 암호화, 보안 업데이트 수행, 스마트 디바이스 암호화 개선 수행을 한 후 전방 FMECA, FTA을 거쳐 후방 FMECA를 통해 1차 개선 값을 구하고 2차 개선 값을 동일하게 구한다. 운영체제 시스템 오류에 대한 개선율은 최대 64.8%를 나타내고 있다. 특히 접근 통제 단계의 보안이 중요시 되는 만큼 주기적으로 FTA, FMECA 통합 분석을 수행하여 스마트 러닝 시스템의 보안성이 개선될 수 있도록 해야 할 것이다[10].

Table 5. Functional security vulnerability of smart learning system

System	Detailed Function	Functional Security Vulnerability
Application Management	Managing EAM	Occurring a great risk once one hacking and connection failure generated
System Management	Processing Authentication	An increase in cyber crime such as hacker attacks
		None of additional certification on the internal network
	Processing Access Control	Threat of data availability, confidentiality and integrity by new cyber security attacks
		Robbery of file records about learners intrusion from open API environment
		Hacking of file managing database intrusion
		Error of smart device operation, unawareness of instructions, robbery, loss of devices
	Virus Detection and Control	A lack of prevention once new cyber security attacks such as intelligent APT attack occurred
		Automatic installation of undesired applications
		Operational errors caused by malware intrusion
		Not taking measures for preventing hackers
Network Management	Network Operation	Diversification of cyber attacks over the wireless network (Rouge AP, Phishing AP, WEP/WPA Crack, MAC Spoof, Mis-Config AP)
	Network tool/ Equipment	Leakage of personal information, Loss and robby of network tool/ equipment
Backup Server Management	Backup System	Location in the same disaster area of Main Data Center and Disaster Recovery Center
	Recovery System	

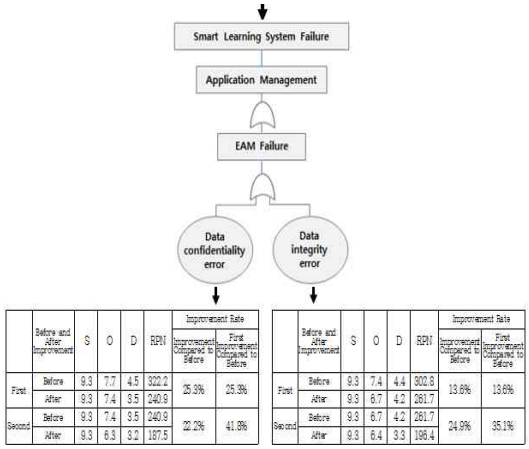
Fig. 8은 전방에서 FMECA에 의하여 바이러스 통제 및 탐지 단계에서 발생하는 결함들을 제거하고 위험을 최소화하기 위해서 잠재적 결함 요인과 실제 결함 요인을 접근 경로에 따라 웹 사이트 방문, 모바

Table 6. Function fault list of smart learning system

System	Detailed Function	Functional Fault List
Application Management	Managing EAM	ID & PW identification & Authentification Failure ⇒ Data Confidentiality error
		ID & PW identification & Authentification Failure ⇒ Data integrity error
System Management	Processing Authentication	Users Authentication error
	Processing Access Control	Robbery of file records about learners intrusion from open API environment
		Hacking of file managing database intrusion
		Error of smart device operation
		Malicious code and malware
	Virus Detection and Control	Automatic installation of undesired applications
		Operational errors caused by malware intrusion
		No installed of security program
		Not taking measures for preventing hackers
Network Management	Network Operation	Error of Network system device operation
		Malicious code and malware
		Not taking measures for preventing hackers
	Network tool/ Equipment	Error of Network security tool/ equipment
		Malfunction from users
Backup Server Management	Backup System	Data confidentiality error
		Data integrity error
	Recovery System	Error of Recovery System device operation

일 디바이스 간의 연결 그리고 SMS, E-Mail을 통한 어플리케이션 설치로 분류하여 분석하였다. 이를 기반으로 치명도(S), 발생도(O), 검출도(D)를 사용하여 위험우선순위(RPN)를 매긴 결과 모바일 디바이스 간의 연결에서 가장 높게 기록되었다. 이후 IP 탐지 시스템, 주기적인 백신 프로그램 업데이트, 보안 프로그램 설치, 스팸 메일 필터링, 어플리케이션 검증센터 구축 개선 수행을 한 후 전방 FMECA, FTA을 거쳐 후방 FMECA를 통해 1차 개선 값을 구하고 2차 개선 값을 동일하게 구한다[11]. 모바일 디바이스 간의 연결 시스템 오류에 대한 개선율은 최대 67.1%를 나타내고 있다.

Failure Modes	Causes	Effects	Severity	Compensating Provision
EAM Failure	Data confidentiality error due to ID password exposing and hacking	Smart Learning System Failure	9.3	Adding security modules to detect security threats such as hacking access failures
	Data integrity error due to ID password exposing and hacking		9.3	



	Before and After Improvement	S	O	D	RPN	Improvement Rate: Improvement Compared to Before	Improvement Rate: First Improvement Compared to Before
First	Before	9.3	7.7	4.5	322.2	25.3%	25.3%
	After	9.3	7.4	3.5	240.9		
Second	Before	9.3	7.4	3.5	240.9	22.2%	41.9%
	After	9.3	6.3	3.2	187.5		

	Before and After Improvement	S	O	D	RPN	Improvement Rate: Improvement Compared to Before	Improvement Rate: First Improvement Compared to Before
First	Before	9.3	7.4	4.4	302.8	13.8%	13.8%
	After	9.3	6.7	4.2	261.7		
Second	Before	9.3	6.7	4.2	261.7	24.9%	35.1%
	After	9.3	6.4	3.3	196.4		

Fig. 6. Application management part of smart learning system.

Failure Modes	Causes	Effects	Severity	Compensating Provision
Processing Authentication Failure	Data confidentiality error Data integrity error	Smart Learning System Failure	9.3	ID/ password periodic inspection and security check. Initialization of local device virtual apply keyboard
Operating System Failure	Robbery of file records about learners intrusion from open API environment		9.0	Encrypting File System. Security sandbox system operation remote control
Hardware Failure	Malicious code and malware		8.5	Conducting security updates.
	Error of smart device operation		8.3	Smart device encryption.
Middleware Failure	Hacking of file managing database intrusion		4.5	Database system encryption, remote control

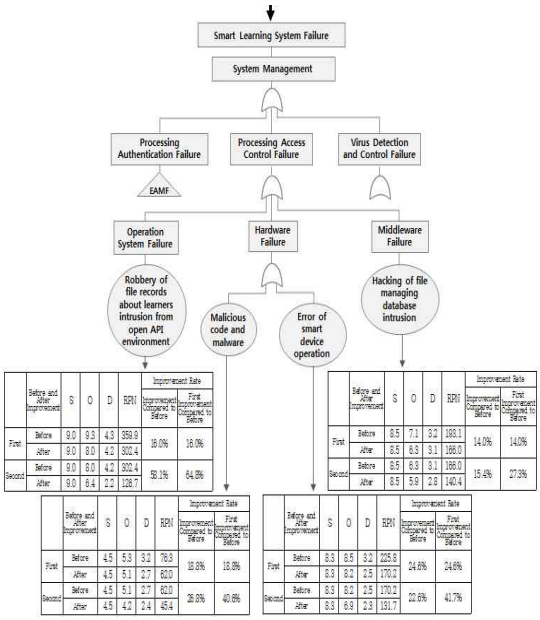


Fig. 7. System management part of smart learning system ①.

3.3 Network Management 부분의 FTA와 FMECA의 전 · 후방 통합적 분석

Fig. 9는 전방에서 FMECA에 의하여 네트워크 단계에서 발생하는 결함들을 제거하고 위험을 최소화하기 위하서 잠재적 결함 요인과 실제 결함 요인을 네트워크 시스템 구성 형태에 따라 네트워크 운영관리와 네트워크 장비관리로 분류하여 분석하였다. 이를 기반으로 치명도(S), 발생도(O), 검출도(D)를 사용하여 위험우선순위(RPN)를 매긴 결과 네트워크 장비관리에서 네트워크 운영관리의 RPN보다 높게 기록되었다. 이후 무선랜 침입 탐지 시스템 구축, 백신 프로그램 업데이트, IP 탐지 시스템, 트래픽 상시 감시, 방화벽 적용, 네트워크 장비 사용 교육, FMC관련 장비 구축 개선 수행을 한 후 전방 FMECA, FTA을 거쳐 후방 FMECA를 통해 1차 개선 값을 구하고 2차 개선 값을 동일하게 구한다. 네트워트 장비 시스템 오류에 대한 개선율은 최대 56.9%를 나타내고 있다. 네트워크 시스템의 보안성을 향상시키기 위한 대책으로 다양한 암호 알고리즘들, 해쉬 함수 등을 사용하고 있다. 향후 스마트 러닝 시스템 네트워크 보안을 위한 대책을 지속적으로 개발해야 할 것이다 [11,12].

Failure Modes	Causes	Effects	Severity	Compensating Provision
Website visits Failure	Automatic installation of undesired applications	Smart Learning System Failure	7.2	Build of IP detection system
	Operational errors caused by malware intrusion		7.2	Update periodic vaccine program
Link between devices Failure	Malware intrusion		9.0	Update periodic vaccine program
	No installed of security program		9.0	Installed of security program
Application installation through SMS, E-mail	Not taking measures for preventing hackers		4.2	Update periodic vaccine program Spam mail filtering Build Application Verification Center

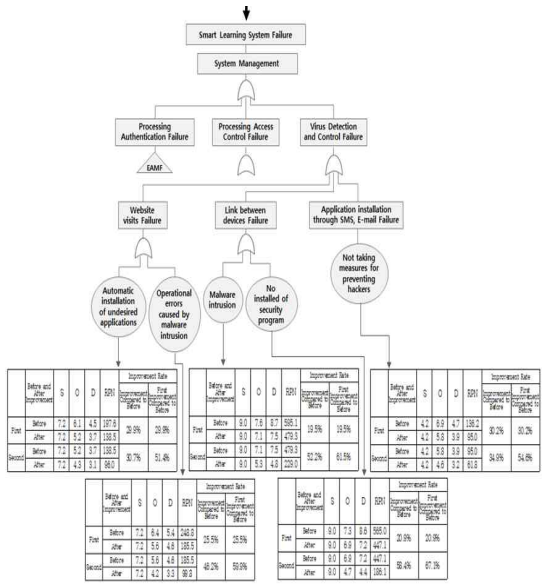


Fig. 8. System management part of smart learning system ②.

3.4 Backup Server Management 부분의 FTA와 FMECA의 전 · 후방 통합적 분석

Fig. 10은 전방에서 FMECA에 의하여 백업 서버 단계에서 발생하는 결함들을 제거하고 위험을 최소화하기 위하서 잠재적 결함 요인과 실제 결함 요인을 백업 서버 시스템 구성 형태에 따라 백업 시스템과 복구 시스템으로 분류하여 분석하였다. 이를 기반으로 치명도(S), 발생도(O), 검출도(D)를 사용하여 위험우선순위(RPN)를 매긴 결과 백업 시스템에서 복구 시스템의 RPN보다 높게 기록되었다. 이후 백신

Failure Modes	Causes	Effects	Severity	Compensating Provision
Network Operation Failure	Not taking measures for preventing hackers	Smart Learning System Failure	8.0	Build a wireless LAN intrusion detection system
	Malicious code and malware		8.5	Update periodic vaccine program
	Error of Network system device operation		8.2	IP detection system, apply VPN, monitor traffic regularly
Network Tool/ Equipment Failure	malfunction from users		7.0	Training on network equipment usage
	Error of Network security tool/equipment		7.5	Build tools about FMC. Build a wireless LAN intrusion detection system.

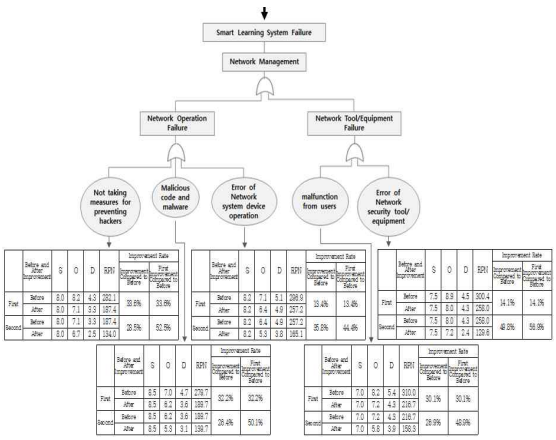


Fig. 9. Network management part of smart learning system.

프로그램 업데이트, IP 탐지 시스템, 트래픽 상시 감시, 방화벽 적용, 내부 서버 직접 연결 차단, 호스트 기반 방화벽 작동, 불필요한 포트 차단 및 제어, 내부 및 외부 네트워크 분리 개선 수행을 한 후 전방 FMECA, FTA을 거쳐 후방 FMECA를 통해 1차 개선 값을 구하고 2차 개선 값을 동일하게 구한다. 백업 시스템 오류에 대한 개선율은 최대 56.3%를 나타내고 있다.

FTA와 FMECA의 전·후방 통합적 분석을 통해 개선 수행을 수행하였을 때 훨씬 치명도, 발생도, 검출도 및 위험우선순위(RPN) 수치가 줄어들고 개선율이 향상된 것으로 나타난다. 따라서 향후에는 스마트 러닝 시스템 보안성이 향상된 스마트 러닝 시스템을 요구하기 때문에 이러한 분석기법들을 사용하여 잠재적인 결함 및 위험요소 발생을 예방하는 것이 반드시 필요하다.

Failure Modes	Causes	Effects	Severity	Compensating Provision
Backup System Failure	Data confidentiality error	Smart Learning System Failure	8.5	IP detection system, apply VPN, monitor traffic regularly.
	Data integrity error		8.5	IP detection system, apply VPN, monitor traffic regularly.
Recovery System Failure	Malicious code and malware		8.3	Update periodic vaccine program Block direct connections to internal servers
	Error of Recovery Sysem device operation		8.5	Host-based firewall operation, unnecessary port blocking and control, internal and external network separation

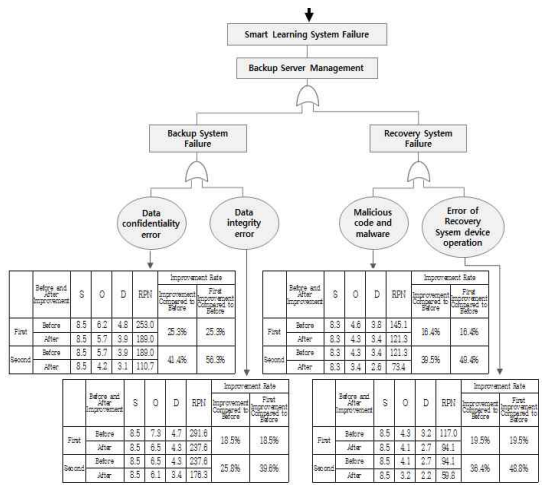


Fig. 10. Backup server management part of smart learning system.

4. 결 론

최근 IT기술과 네트워크 기술이 빠르게 진화하는 환경에서 시대적 흐름에 부합하는 스마트 러닝 서비스의 이용이 증가하고 있다. 스마트 러닝은 스마트폰, 태블릿PC, e-Book 단말기 등 스마트 디바이스와 e-러닝 신기술이 융합된 개념으로 인터넷 접속은 물론 위치기반서비스·증강현실 등 다양한 기술을 적용할 수 있는 스마트 디바이스의 장점을 활용해 기존 e-러닝과 차별화된 서비스를 제공하고 있다. '지능형 단말기'라는 의미의 '스마트폰'의 확산으로 소셜네트워크 서비스(SNS)를 이용한 악성코드의 유포 및 빠

른 전파 등도 새로운 보안 위협으로 나타나고 있다. 그 밖에 스마트 디바이스를 대상으로 한 해킹 및 악성코드 감염 등 위협이 증가하고 있는 상황이다. 스마트 러닝 시스템은 다양한 보안 취약점을 포함하고 있어 이를 해결하고 보안성을 확보하기 위한 연구가 중요시되고 있다.

따라서 본 논문에서는 스마트 러닝 시스템의 보안성 개선을 위하여 시스템의 보안 기능별 취약점과 관련 문제점을 분석한 후, 분석 내용을 바탕으로 결함 트리 분석(FTA)과 고장 유형 영향 및 치명도 분석(FMECA)을 전·후방으로 통합한 기법을 수행하여 스마트 러닝 시스템의 보안성을 개선할 수 있도록 하였다. Any Network, Any Device를 통한 시간과 공간의 제약 없이 지식과 정보에 접근 가능한 유비쿼터스 환경에서의 온라인 학습의 편리함 이면에 사용자들을 위협하는 위협요소들이 점점 많아지고 그 피해수준도 점점 심각해지고 있기 때문에 이를 충분히 고려한 보안 솔루션에 대한 연구가 향후 과제로 남아 있다.

지금까지의 동향과 비슷하게 앞으로도 계속 스마트 러닝 시스템의 사용자는 증가할 것으로 예상되지만, 아직 해결하지 못한 보안 취약점과 새롭게 등장하는 사이버 범죄 유형의 증가로 인하여 스마트 러닝 시스템의 보안성 확보에 관한 문제는 더욱 중요시될 것이다. 따라서 스마트 러닝 시스템의 보안성을 개선하기 위해서는 효율적인 결함 분석 기법들과 그 상호 보완적인 결함 분석 기법들의 조합을 연구하고 분석하여 더욱 포괄적이고 효율적인 방법을 제안하여 스마트 러닝 시스템의 보안성을 개선할 수 있는 지속적인 개발과 연구가 필요할 것이다.

REFERENCES

[1] K.H. Park and Y.M. Kim, "A Study on the Influence of Smartphone Utilization on Learning Satisfaction in e-Learning," *International Journal of E-Business Research*, Vol. 14, No. 2, pp. 25-45, 2013.

[2] Y.A. Kim and H.G. Sin, "A Study on the Influencing Factors of Smart Learning," *Journal of the Korea Industrial Information System Society*," Vol 16, No. 5, pp. 93-105, 2011.

[3] J.S. Seong, "A Study on the Prevention of Security Incident," *Journal of Security Engineering*, Vol. 9, No. 6, pp. 503-510, 2012.

[4] M.H. Kim, W. Toyib, and M.G. Park, "An Integrative Method of FTA and FMEA for Software Security Analysis of a Smart Phone," *Korean Information Processing Society Transactions on Computer and Communication Systems*, Vol. 2, No. 12, pp. 541-552, 2013.

[5] S.M. Jang and M.G. Park, "A Study on the Fault Analysis and Security Assessment for Smart Card Management System," *Journal of the Korea Multimedia Society*, Vol. 17, No. 1, pp. 52-59, 2014.

[6] N. Snooke and C. Price, "Model-driven Automated Software FMEA," *Proceeding of Reliability and Maintain Ability Symposium*, pp. 1-6, 2010.

[7] Rodrigo de Queiroz Souza and Alberto Jose lvares, "FMEA and FTA Analysis for Application of the Reliability Centered Maintenance Methodology: Case Study on Hydraulic Turbines," *Proceeding of ABCM Symposium Series in Mechatronic*, Vol. 3, pp. 803-812, 2008

[8] S.G. Teng and S.M. Ho, "Failure Mode and Effects Analysis: An Integrated Approach for Product Design and Process Control," *International Journal of Quality & Reliability Management*, Vol. 13, No. 5, pp. 8-26, 1996.

[9] Z. Hong and L. Binbin, "Integrated Analysis of Software FMECA and FTA," *Proceedings of Internatinal Conference on Information Technology and Computer Science*, pp. 184-187, 2009.

[10] Chrysler LLC, Ford Motor Company, and General Motors Corporation, *Potential Failure Mode and Effects Analysis (FMEA)*, 4th Edition of Reference Manual, 2008.

[11] J.S. Seong, "A Research on Preventing for Security Threats," *Journal of Security Engin-*

eering, Vol. 9, pp. 503-509, 2012.

[12] S.W. Na, Y.H. Lee, and S.J. Ji, *The Security Issue and Strategies of Smartphone an Mobile office*, CIO Report of National Information Society Agency, Vol. 26, pp. 10-27, 2010.

[13] M.H. Kim and M.G. Park, "A Study on thd Fault Modes and Effect Analysis for Software Safe Evaluation," *Journal of Korea the Multimedia Society*, Vol. 15, No. 1, pp. 113-130, 2012.

천 회 영

1989년 2월 동아대 응용통계학과 (경영학사)
1991년 8월 동아대 경영대학원 (경영학석사-마케팅관리 전공)
2016년 2월 부경대 대학원 정보시스템학과 박사학위과정수료
2000년～현재 동의과학대학교 강사
2016년～현재 경성대학교 강사
관심분야 : Smart Learning and E-Learning, 소프트웨어 신뢰성 공학, 멀티미디어 정보처리기술, 정보시스템 성능평가

박 만 곤

경북대학교 수학교육(이학사)
경북대학교 전산통계학(이학박사)
Philippine Women's University (국제행정학석사)
University of Rizal System, Philippines(명예 기술학박사)
Dept. of Electrical and Computer Engineering, University of Kansas (Post Doc.)
1981년～현재 부경대학교 IT융합응용공학과 교수
1997년～현재 한국멀티미디어학회(KMMS), 초대 총무이사, 수석부회장, 회장 및 명예회장
2002년～2007년 정부간 국제기구 CPSC (콜롬보플랜기술교육대학교) 사무총장 (Director General and CEO)
2004년～2007년 Asia-Pacific Accreditation and Certification Commission (아태지역 인증검증위원회) 위원장
2005년～2007년 유네스코 (UNESCO-UNEVOC) 자문위원, 아시아개발은행(ADB) 자문관
관심분야 : 소프트웨어 공학 및 재공학, 소프트웨어 신뢰성공학, 소프트웨어 안전성 공학, 비즈니스 프로세스 재공학 (BPR), ICT-기반 HRD, 전자정부 및 전자교수학습 시스템 구축