공 학 석 사 학 위 논 문

핀테크 결제 시스템의 보안성 평가를 위한 결함 트리 분석 기법에 관한 연구

2017년 2월

부 경 대 학 교 대 학 원

정보시스템협동과정

남 필 식

공 학 석 사 학 위 논 문

핀테크 결제 시스템의 보안성 평가를 위한 결함 트리 분석 기법에 관한 연구

지도교수 박만곤

이 논문을 공학 석사 학위 논문으로 제출함.

2017년 2월

부 경 대 학 교 대 학 원

정보시스템협동과정

남 필 식

남필식의 공학석사 학위논문을 인준함.

2017년 2월 24일

주심 김 창 수 (인)

위원 이 경 현 (인)

위원 박 만 곤 (인)

<차 례>

<표 차례>

<그림 차례>

A Study on the Fault Tree Analysis Methods for the Security Evaluation of Fintech Payment Systems

Nam Pil Shik

Department of Information Systems, Graduate School,
Pukyong National University

Abstract

Recently, it has been changed various patterns related with our consumption because of fast propagation of smart technology in our life. Thus we can buy a necessary products anywhere and anytime. Though the change of patterns in our life, in recent years, Fintech attracts a lot of attention. Therefore the security of Fintech payment system becomes more important and necessary. There are many fault analysis methods to evaluate the security and safety of information systems according to their characteristics and usages. However, the only assessment method to evaluate the security of information systems is not enough to analyses properly on account of the various types and characteristics of information system y the progress of IT convergence and their applications.

In this paper proposes and integrative method of the Fault Tree Analysis (FTA) and Fault Modes and Effect Analysis/Criticality (FMEA/C) based on criticality to evaluate and improve the security of Fintech payment system as an illustration.

I. 서론

1. 연구 배경 및 목적

IT기술의 발달은 통신, 제조, 서비스 등 다양한 분야에 걸쳐 융합되면서 편리한 서비스들이 현실로 구현되어 제공되고 있으며 지속적인 발전 과정에 있다. 이러한 IT 기술 융합을 진행 중인 분야들은 불필요한 비용의 절감에 따른 서비스 수준을 향상시키면서 사용자들의 만족도를 높이고 나아가 생활 방식의 변화에 큰 영향을 주고 있는데 최근 가장 주목을 받고 있는 분야로 금융서비스가 있다.

기존의 금융서비스 형태는 고객과의 직접적인 대면을 통해 금융 업무를 처리하는 방식이었다면IT기술 활용에 따른 PC, ATM 등을 이용한 온라인 서비스를 시작으로 스마트폰을 이용한 모바일 금융서비스 형태로 전환되고 있으며. 스마트폰의 대중화로 언제, 어디서든지 원하는 시간에 금융 서비스를 이용할 수 있는 핀테크가 등장하게 되었다.

핀테크는 IT 기술에 금융 서비스를 접목시켜 모바일 단말기를 이용한 송금 및 결제 등과 같은 서비스의 장점을 극대화하여 보다 편리하고 빠르게 금융 서비스를 이용할 수 있도록 해주는 형태로 대출, 투자 및 자산 관리 등 보다 다양한 영역으로 확대되어가고 있다.

주로 영국, 미국, 중국 등의 나라에서 활발하게 개발 및 제공되고 있으며, 국내에서는 2014년에 핀테크를 집중 육성 산업으로 선정하고 각종 규제 및 법안 등의 완화에 대한 정부의 지속적인 지원과 시장의 확대로 핀테크 시장이 성장해가고 있는 추세이다.

또한 해외 핀테크 기업의 국내 진출도 활발하게 이루어 지고 있는데 2013년 페이팔과 하나은행의 제휴로 해외소액송금서비스를 시작하였고 2014년부터는 중국의 알리바바, 텐센트 등이 은행, PG사(Payment Gateway), 백화점 등과 제휴하여 결제서비스를 제공하고 있다. 이러한

핀테크 산업의 성장은 정부가 4대 핵심 개혁 중의 하나로 금융 개혁을 선정하고 2015년부터 지속적으로 제도 개선을 추진해온 영향으로 볼 수 있지만 지급 결제 방식에만 편향되어 있는 국내 핀테크 사업을 발전시켜 나아가야 하는 필요성을 시사한다.

핀테크는 과거 직접 방문을 통한 점포에서 제공되던 금융서비스에 대한 불편함이 IT 기술과 결합되면서 언제 어디서든지 모바일 단말기 사용자라면 누구나 빠르고 편리하게 금융 서비스를 활용할 수 있다는 장점으로 인해 핀테크 서비스의 보안적인 측면의 우려에도 불구하고 핀테크 시장은 점차 확대되어 가고 있다.

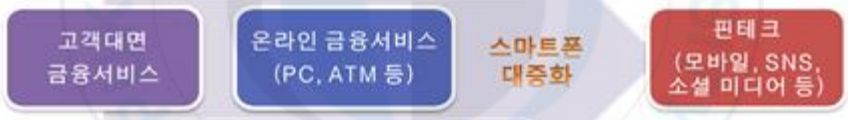
핀테크의 발전에 따른 금융서비스의 변화는 인터넷 은행의 등장을 기점으로 보다 가속화 될 것으로 예상되며 이는 금융 개혁에 따른 제도의 개선에도 많은 영향을 미칠 것이다. 이렇게 핀테크 산업에 대한 관심이 높아지는 만큼 안정적인 서비스를 제공하기 위해서는 핀테크 결제 시스템의 보안성 역시 중요한 이슈로 떠오르고 있다. 핀테크 결제 시스템들과 같은 정보 시스템의 보안성을 평가하기 위해서 사용되는 여러 가지 결함 분석 기법들이 있지만 단지 하나의 시스템 보안성 평가 방법으로는 적절한 분석이 이루어 질 수 없다.

이에 본 논문에서는 핀테크의 개념 및 특징, 국내외 현황을 살펴보고 핀테크 서비스 유형과 서비스 기술, 보안 기술에 대해 알아보고, 핀테크 결제 시스템의 보안성을 평가하기 위해 두 가지 중요 결함 분석 기법인 결함 트리 분석(Fault Tree Analysis; FTA) 기법과 치명도(Criticality)기반의 고장모드별 영향 분석(Fault Modes and Effect Analysis/Criticality; FMEA/C)기법을 통합하여 사용한 후 핀테크 결제 시스템의 결함 분석을 수행하여 보안성을 평가하고 개선하는 방법에 대해 제안하고자 한다.

II. 핀테크

1. 핀테크의 개념

고객과의 직접적인 대면을 통해 금융 업무를 처리하는 기존의 금융서비스 형태가 IT기술이 발달함에 따라 PC, ATM 등을 이용한 온라인 서비스와 스마트폰을 이용한 모바일 금융서비스 형태로 전환되고 있다. 스마트폰의 대중화로 언제, 어디서든지 원하는 시간에 금융 서비스를 활용할 수 있게 되면서IT와 금융의 융합이 촉진되었고 온라인과 오프라인의 경계를 허무는 핀테크가 등장하게 되었고 아래의 <그림 1>과 같다.



<그림 2> 핀테크의 등장

핀테크(Fintech)는 IT기술을 기반으로 한 금융 시스템으로 금융(Finance)과 기술(Technology)의 합성어이다[1]. 비 금융기관인 IT기업들이 금융서비스 프로그램을 개발하고 향상시키기 위한 모든 기술과 서비스를 지칭하며 고객과의 대면 없이 인터넷이나 모바일을 통해 고객 중심의 금융서비스를 제공할 수 있는 차세대 서비스이다.

금융 주도하에 이루어지던 핀테크 사업은 점차 IT의 주도로 발전하게 되었고 이에 모바일, SNS, 소셜 미디어 등과 결합되어 결제, 송금, 대출, 크라우드 펀딩, 개인자산관리 등 많은 분야에 걸쳐 기존 금융기관이 제공하지 못했던 새로운 서비스를 보다 편리하고 저렴한 비용으로 이용할 수

있게 해준다. 이러한 IT와 금융의 융합은 새로운 금융상품 및 서비스를 창출하게 되고 금융 거래의 확산을 촉진 시키게 된다.

2. 핀테크의 특징

디지털 시대의 금융 산업을 이끌고 있는 핀테크의 4가지 특징은 다음과 같다[2].

가. 접근성

핀테크는 고객들이 금융서비스 이용에 있어 시간적 공간적 제약으로부터 자유롭게 접근이 가능하도록 하였다. 과거에는 지점을 내방하여 업무처리가 가능했으나 PC환경을 기반으로 한 온라인 서비스가 출현하고 현재에는 스마트폰과 테블릿PC를 이용한 환경까지 발전하였다.

이러한 기술은 소비자들이 언제 어디에서나 손쉽게 금융 업무를 처리할 수 있게 하였다. 기존 금융기관에서도 핀테크 기술처럼 접근성이 용이한 서비스를 제공하였다. 온라인 뱅킹과 모바일 뱅킹이 대표적인 예이다 하지만 기존 고객에 한해 서비스가 제공되어 신규 고객을 확보하거나 접근성에는 여전히 불편함이 따랐다.

2009년 하반기에 아이폰이 국내에 도입되고 년 안드로이드 기반인 스마트폰과 테블릿PC의 보급이 활발해지면서 PC환경이었던 웹 서핑과 뱅킹 쇼핑 등이 모바일로 점차 이동하였다 현재는 도서 쇼핑몰이나 소셜 커머스 사업자의 모바일 상거래 비중은 이미 50%를 상회하고 있으며 오픈마켓도 30% 정도 차지한다. 모바일 결제가 활발해짐에 따라 스마트폰에 는 결제와 관련된 앱이 출시되고 카드를 등록하여 사용하는 등 결제 방식에 변화를 주었다[3].

과거 온라인에서 카드 결제를 하려고 할 경우 매번 카드번호와 비밀번호

등을 입력하고 개인정보를 등록하여 번거로운 절차를 걸쳐 결제를 했으나 현재는 등록된 카드를 불러와 아이디와 비밀번호나 지문 인식 등을 사용하여 본인 인증을 한 후 결제가 가능하게 되었다. 미국의 스퀘어는 스마트폰을 가지고 있는 고객들을 상대로 카드결제를 가능토록 단말기를 개발하여 2014년에만 약 30조원이 넘는 결제액을 기록하였고 기업 가치는 2009년 설립 이후 약 5조원으로 성장하였다.

나. 자동화 실현

사람의 개입이 없이 자동화를 추구하는 것이 핀테크 기술의 또 다른 특징이다 모든 업무에 대해 알고리즘을 사용하여 자동으로 업무 처리가 가능하도록 되어 있다. 기존 금융기관에서는 일부 영역에 한해 IT기술을 활용하여 반자동화를 사용하였다. 하지만 핀테크는 불가피한 영역만 제외하고 가능한 한 전 영역을 자동화함으로써 사람들은 관리와 감독의 주체만 될 뿐이다 지난 10여 년 동안 IT기술이 발전하고 사람들은 효율적으로 그 기술을 활용하였기 때문에 가능한 일이다.

업무의 자동화는 비용 절감 및 시간 단축의 효과가 있다. 고객을 접견해야 하는 장소 결정의 문제나 서로 만날 시간을 별도로 정할 필요가 없게 되었다. 더불어 자동화를 추구하는 핀테크는 고객과의 거래비용도 줄여준다. 지점을 내방하지 않아도 되고 시간에 쫓겨 금융소비를 결정하는 번거로움을 없애주기 때문이다.

투자자와 대출자를 연결해주는 온라인 투자중개회사인 렌딩 클럽은 대출을 매개로 투자를 중개해주는 역할을 한다. 렌딩 클럽은 대출신청 대출심사 및 지급 투자에 대한 등록 선택 수익배분 등의 절차를 온라인에서 진행하여 기존 은행과는 다른 방식을 제공한다.

이러한 특징으로 고객들에게는 대출이나 투자에 대한 편의성을 제공하고 과거 은행처럼 긴 줄을 서거나 서류를 준비하는데 긴 시간을 소비하지 않아도 된다. 또한 대출담당자를 만나는 절차가 생략되기 때문에 옷이나

태도에 신경 쓰는 일은 사라진다 그만큼 자동화를 추구하는 핀테크에서는 고객 입장에서 최적의 환경을 느낄 수 있다.

다. 정보보안

핀테크는 스마트폰 보급과 모바일 기술의 발전으로 성장된 산업이지만 비대면 방식으로 온라인 금융거래의 보안 및 안정성에 우려를 갖고 있다. 2014년 한국은행이 조사한 자료에 따르면 모바일 결제 미사용에 대한 가장 큰 이유는 정보유출 및 보안(78.3%)에 대한 부분이었다. 개인정보의 유출이 기사를 통해 시시각각 보도되면서 온라인 거래의 편의성에 대해 비관적으로 보는 시선들이 많아지게 되었다. 더욱이 핀테크가 발전할수록 다양한 서비스가 온라인에서 제공되고 새로운 채널이 생겨 더 많은 문제가 발생할 여지가 있다.

핀테크는 정보보안 관점에서 살펴보면 이용자의 편리함을 제공하기 위해 간소화된 결제단계 및 인증방식을 채택한다. 과거에는 공인인증서 및 ActiveX, 일회용비밀번호 등을 이용하여 안정성을 중요시 했으나 현재는 해당 도구를 미사용 함으로써 온라인에서 보안 사고를 막기 위한 노력이 필요하다.

서비스 채널 기술 간의 다양한 융복합 현상이 발생하여 접점이 증가하여 새로운 취약점이 발생하고 대응 방법 또한 복잡해진다. 개인정보의 수집 및 이용 의 필요성이 증가하여 고객의 개인정보유출이나 프라이버시 침해를 야기할 수 있어 언제 어디서 누구의 정보가 이용되고 있는지 고객에게 알릴 필요가 있다. 고객은 스스로 자신의 정보 노출 및 폐기 여부를 결정해야 한다.

또한 IT기업들은 핀테크 산업의 성장을 위해 사전규제 및 법안을 완화 또는 폐지를 요구한다. 이는 금융거래의 안정성을 저하하는 결과를 초래할 수 있다. ICT기술과 금융산업의 융화라는 측면에서 핀테크 산업 발전을 위한 불가피한 조치라고 생각되지만 온라인에서의 금융서비스에 대한

신뢰를 구축하고 편의성과 보안성 간의 균형과 조화가 필요해 보인다.

라. 빅데이터 활용

방대한 양의 데이터에서 가치가 있는 정보를 추출하고 그 정보를 이용하여 소비자의 성향을 예측할 수 있는 기술인 빅데이터는 현재 핀테크 산업에 적용되고 있다 비 금융기관인 IT기업들은 이러한 빅데이터를 활용하여 기존 금융기관보다 더 많은 정보를 얻고 정보우위에 있게 된다.

핀테크 기업은 고객이 제공하는 정보 이외에도 기존 금융기관이 가지고 있지 않은 영역의 정보까지 이용하여 금융서비스 개발 및 운영에 오류를 줄여왔다 오류의 감소를 통하여 고객에게 신뢰를 얻고 손실을 줄이며 이로 인해 기업은 수익성을 높일 수 있다.

빅데이터는 다양하고 많은 정보가 공존하는 현 사회에서 꼭 필요한 기술이다. 소비자들은 최적의 의사결정을 내리기 위해서는 복잡한 정보를 스스로 결정하기보다는 정보를 재가공하고 그 정보만을 이용하여 소비자는 간단하게 결정하는 것이 필요하다. 즉 핀테크 기업에게 빅데이터는 소비자의 의사결정에 도움을 주는 중요한 요인이다.

미국의 온라인 전용증권회사인 모티브 인베스팅(Motif Investing)은 최대 30개 종목의 주식과 채권으로 구성된 테마주를 투자자에게 제시한다. 빅데이터를 이용하여 산업별 트렌드와 메가트렌드를 파악함으로써 투자자들에게 원하는 테마의 종목을 선택하도록 도와준다.

국내에서는 은행 증권 카드사에서 신규서비스를 도입하여 제공하고 있지만 핀테크 기업이 활발하지 않다는 점에서 서비스 제공 단계에만 그쳐있다. 향후 핀테크의 발전과 더불어 IT기업들과의 제휴를 통해 빅데이터를 활용한 서비스가 업그레이드 될 전망이다.

3. 핀테크의 국내외 현황

가. 국내 핀테크 동향

한국의 핀테크 시장은 다른 핀테크 사업의 선두국가에 비해 많이 뒤쳐져있는 것이 사실이다. 세계 최초로 휴대폰 결제시스템을 개발하였으며, 오래 전부터 인터넷 은행에 대한 필요성을 인식하고 있었고, 무엇보다 높은 스마트폰 보급률과 통신 인프라가 갖춰져 있음에도 불구하고 각종 규제와 지원정책의 미비로 인해 지난해부터 핀테크에 대한 관심이 집중되고 있다. 국내외 소비자들이 물건을 구매할 때 발생하는 공인인증서나 액티브 엑스 등의 문제점을 해결하는 방안으로 핀테크에 대한 관심이 시작되었으며, 문제점으로 지적되어 오던 규제나 지원정책도 정비되기 시작하였다. 현재는 비금융기업들의 주도하에 다양한 형태의 핀테크 서비스를 제공하거나 준비 중에 있다. 대표적인 서비스로는 카카오톡을 이용한 카카오페이 및 뱅크월렛 카카오, 삼성 스마트폰의 사용자를 대상으로 하는 삼성페이 등이 있다[5].

(1) 카카오페이 및 뱅크월렛 카카오

국내의 대표적인 모바일 메신저인 카카오톡은 카카오톡 안에 사용자의 신용카드를 등록한 후, 다양한 곳에서 결제 시 번거로운 절차없이 간단한 비밀번호만 입력하여 결제할 수 있는 모바일 결제 서비스인 카카오페이를 출시하였다. 카카오페이는 국내 스마트폰 사용자의 약 90%이상이 사용하고 있는 카카오톡 내에 이미 탑재되어 있어 별도의 앱을 필요치 않는다는 특징이 있다. 기존의 결제 서비스를 이용할 경우, 결제가 필요할 때마다 공인인증서를 통한 인증이나 각 카드 별로 다른 비밀번호를 입력해야 하는 불편함이 있었다.

이와 같은 불편함을 해소하기 위해 카카오페이는 최초 1회에 한해 카드 등록 시에 만 인증 및 비밀번호 입력의 단계를 거치면 추후 결제 서비스를 이용할 때에는 간편하게, 설정된 비밀번호만 입력하면 처리가 가능하다.

또한 여러 종류의 카드를 등록하더라도 동일한 비밀번호를 이용할 수 있다. 현재 등록 가맹점을 점차 확대하고 있는 추세이다. 또 다른 서비스인 뱅크월렛 카카오도 송금의 불편함을 해결하기 위해 개발되었다. 금융결제원과 각 금융기업들이 공동으로 개발한 뱅크월렛이라는 서비스에 카카오톡을 결합한 서비스 상품으로 사용자는 본인의 카카오톡에 등록된 사용자에게 메시지를 보내듯이 소액을 메신저를 통해 송금할 수 있는 서비스 형태이다. 따라서 주로 개인 간의 거래에서 불필요한 계좌정보와 같은 개인금융정보를 주고 받을 필요가 없다는 장점이 있다.

(2) 삼성페이

eBay나 알리바바가 기업의 특성인 유통업에 금융서비스를 접목시켜 페이팔이나 알리페이를 서비스한다면, 국내 대표 제조기업인 삼성은 스마트폰을 제조할 때 금융서비스를 사용할 수 있는 기능을 탑재하여 출시함으로써 삼성 스마트폰을 지닌 사용자는 별도의 플라스틱 카드를 가지고 다니지 않아도 결제 및 은행의 ATM을 이용한 인출서비스를 사용할 수 있게 되었다.

삼성페이는 미국의 애플페이와 유사하게 스마트폰을 이용하고, 결제 시 지문인식을 사용하여 보안성을 향상시킨다는 유사점이 있으나, 애플페이가 NFC 형태의 전용 단말기가 필요한 것에 비해, 삼성페이는 기존의 마그네틱 결제단말기를 그대로 사용할 수 있다는 점이 다르다. 기업이나 개인이 삼성페이의 이용을 위해 결제단말기를 새로 구입할 필요가 없다는 점이 장점이 될 것이며, 사용자측면에서는 플라스틱 카드로 결제가 가능한 대부분의 장소에서 그대로 사용할 수 있다는 장점이 있다.

추후 정부의 정책에 따라 기존의 마그네틱 카드 단말기를 IC 카드 형태의 보안성이 향상된 카드 및 결제 단말기의 교체를 주도할 예정이지만 삼성페이의 시장 선점 효과는 높을 것으로 예상되며, 마그네틱 단말기의 교체가 확산된다 하더라도 NFC 방식의 결제서비스를 지원할 수 있는 기능이 동시에 탑재되어 있기 때문에 큰 영향은 없을 것으로 생각된다.

최근 삼성페이는 중국의 유니온페이와 업무협약을 통해 내년부터 중국의

모바일 결제 시장에 진출하게 된다. 현재 중국 시장은 알리페이가 시장 점유율이 높은 가운데, 앱이나 소프트웨어를 통해 결제를 진행하는 것이 아닌 모바일 단말기기 자체를 통해 결제를 처리할 수 있는 삼성페이와 애플페이가 중국시장 내에서 경쟁을 앞두고 있는데, 삼성페이의 중국 시장 진출 시 장점은 역시 마그네틱 보안 전송 기능과 NFC 기능이 동시에 지원 가능하기 때문에, 중국 대부분의 오프라인 상점에서 이용이 가능하다는 점이다. 현재 삼성페이는 미국, 유럽에 진출해 있는 상태이다.

나. 해외 핀테크 동향

(1) 미국

미국은 핀테크 사업이 가장 활발히 이루어지고 있는 국가 중 하나로 미국ICT 기업들은 핀테크 사업을 주도하고 있다. 실리콘밸리와 뉴욕을 기준으로 전 세계의 약 83%에 해당하는 투자규모를 가지고 있으며, 2014년 IDC가 발표한 “2014 핀테크 100대 기업(2014 FinTech Rankings Top 100)”에 따르면 그 중 약 70 ~ 80%가 미국의 ICT 기업으로 나타났다.

미국은 금융위기 이후, 금융 서비스에 IT 기술을 적극 활용하고 있으며, 유럽에 비해 발전이 더딘 측면도 있지만, 투자 규모로는 압도적인 1위를 차지하고 있다. 미국의 핀테크 서비스의 특징은 이메일이나 핸드폰번호 등만 알면 계좌번호와 같은 번거로운 개인금융정보 없이도 개인 간의 송금이나 결제서비스를 신속하고 편리한 처리할 수 있는 결제 서비스가 제공되고 있으며, 많은 호응을 얻고 있다. 대표적인 서비스로는 PayPal과 최근 이슈가 되고 있는 애플페이를 들 수 있다.

미국의 eBay가 1998년에 설립한 PayPal은 금융서비스를 사용하는 개인이나 기업을 대상으로 개인정보에 해당하는 계좌정보나 결제정보를 주고 받지 않고 송금 및 결제를 진행할 수 있는 대표적인 결제서비스이다. 최근에는 애플, 구글, 아마존, PayPal이 FIN(Financial Innovation

Now)라는 연합을 설립하여 핀테크 서비스를 금융기업이 중심이 아닌 IT 기업이 기술로 핀테크 사업을 활성화하기 위해 노력 중이다.

애플이 2014년 10월부터 시작한 모바일 결제 서비스로 플라스틱 신용카드 대신 아이폰을 사용하여 결제를 할 수 있는 서비스 방법이다. 사용 방법은 아이폰에 등록된 신용카드를 선택하고 전용 결제 단말기에 아이폰을 가져다 댄 후, 지문 인식을 하면 결제가 이루어지는 서비스 방법이다. 지문인식 기능을 사용하기 때문에 보안 기능을 향상시킬 수 있다는 장점이 있지만, 애플페이를 사용하기 위해서는 NFC 형태의 전용 단말기가 필요하다는 점과 애플페이가 결제 시장을 장악할지도 모른다는 우려로 인해 대형 유통업체들이 애플페이의 결제를 거부하고 있는 상황이기 때문에 보급에는 시간이 걸릴 것으로 예상되고 있다.

(2) 영국

영국은 미국에 비해 투자 규모에서는 뒤지지만 가장 핀테크 서비스 개발이 활발하게 이루어지고 있는 국가 중 하나이다. 영국은 금융위기 이후 금융기관에 대한 국민들의 신뢰하락 및 불만 증대를 해결하기 위해 대체 금융서비스 개발에 투자하였다. 그로 인해 핀테크 관련 스타트업 기업들이 증가하고 정부에서도 규제 완화 및 벤처 기업 설립에 전폭적인 지원을 하였다. 2014년 영국무역투자청은 핀테크 사업을 핵심 사업으로 선정하고 투자자를 모집하였으며, 그들에게 영국에서의 핀테크 현황 및 지원, 발전 방향에 대해 설명하였다. 이러한 정부의 노력으로 인해 영국의 핀테크 투자는 폭발적으로 증가하였다.

영국의 대표적인 핀테크 기업은 트랜스퍼 와이즈(Transfer Wise)를 들 수 있다. 트랜스퍼 와이즈는 P2P 방식의 해외외화송금서비스를 지원하는 핀테크 기업으로 해외여행이나 해외유학 등에서 불편함 점 중 하나인 송금 및 현금인출이나 카드 거래에서 발생하는 수수료를 낮추기 위해 서비스를 제공하는 기업이다. 트랜스퍼 와이즈의 기본적인 서비스 모델은 타국으로 송금하려는 다수의 건수를 찾아서 마치 자국 내의 송금처럼 변경시키는 서비스 모델을 가지고 있다.

예를 들어, 한국에서 미국으로 돈을 송금하려는 A와 미국에서 그 돈을

받으려는 B의 발생건과 반대로 미국에서 한국으로 돈을 송금하려는 C와 한국에서 그 돈을 받으려는 D의 발생 건을 서로 매칭시켜 한국에 있는 A가 한국에서 돈을 받으려는 D에게 송금하고, 미국에서 한국으로 송금하려는 C가 미국에 있는 B에게 송금한 것처럼 서비스를 제공하는 것이다. 겉으로는 해외송금처럼 보이지만 자국 내에서 발생하는 금융거래처럼 만들게 되는 것이다.

(3) 중국

중국은 금융서비스와 관련해서 과거에는 매우 불편한 국가였다. 결제 시 필요한 신용카드의 보급률이 굉장히 낮은 추세였고, 은행계좌 역시 개설되지 않은 사람이 더 많았으며, 현금 또한 위조지폐의 위험이 항상 존재하고 있었다.

그리고 지리적인 특성상 금융서비스를 이용하기 위한 은행지점을 찾기 힘든 점 등 여러 가지 요인으로 인해 금융서비스의 확산이 매우 어려운 상황이었다. 하지만 전 세계적으로 스마트폰의 보급이 확산되는 시점에서 중국도 예외는 아니었으며, 저가 휴대폰시장의 확산으로 중국 국내 스마트폰 보급률이 2014년에는 약 70%를 초과하는 등 IT 기술의 보급이 확산되고 있었으며, 이러한 스마트폰의 확산과 함께 핀테크 시장도 급속도로 발전하고 있다. 2014년 말 중국의 모바일 결제 규모는 약 1,411조 원 정도를 보이고 있으며, 그 중 8억 명 이상의 가입자를 보유한 알리페이가 약 50% 이상의 시장점유율을 기록하고 있다.

중국의 가장 대표적인 핀테크 서비스로써 중국 최대 전자상거래 업체인 알리바바에서 제공하고 있다. 알리페이는 신용카드를 연결하여 결제서비스를 이용할 수도 있지만, 대부분 사용자들은 알리페이와 연결되어 있는 계좌에 현금을 충전하고 필요 시 결제에 사용하는 방식으로 충전식 결제서비스의 형태를 나타내고 있다. 사용방법은 온라인 결제뿐만 아니라 오프라인에서도 앱을 통하여 바코드를 인식하여 결제를 하는 방식이다. 주로 교통요금이나 쇼핑 등에서 사용되고 있으며, 중국 전역뿐만 아니라 전 세계로 시장 영역을 확대하고 있다.

III. 관련연구

1. 서비스 유형

핀테크 산업은 사업영역을 기준으로 영국무역투자청(UK Trade & Investment)에서 분류한 4가지 영역으로 나눌 수 있는데 지급결제, 금융데이터 분석, 금융 소프트웨어, 플랫폼 영역으로 다음과 같다[6].

가. 지급결제

이용이 간편하면서도 수수료가 저렴한 지급결제서비스를 제공함으로써 지급결제 시장의 진입장벽을 완화한다. 지급결제 부문에는 전자화폐를 이용하거나 카드사와 PG사의 간편결제 원 클릭 서비스 같은 전자결제서비스를 제공한다. 동일한 서비스를 사용한 이용자는 화폐를 가지고 있지 않아도 빠르고 편리하게 결제서비스를 이용할 수 있어 효과적이다. 하드웨어 기반 모바일 간편결제 서비스부터 앱 기반 간편결제 서비스까지 다양한 서비스가 출시되고 있다.

나. 금융데이터 분석

고객의 금융 거래를 바탕으로 신용도를 파악해 적절한 이자율을 계산하는 기존 금융데이터 분석 업무를 개인 및 기업고객과 관련된 다양한 데이터를 수집하여 분석함으로 새롭게 가치를 창출하고 금융 서비스의 효율성을 향상시키고 있다. 이는 대출의 유무와 이자율을 계산하기 위해 직장이나 소득현황 등의 변수를 분석하는 방식에 SNS, 댓글, 기사, 이미지 등의 비정형데이터를 반영하여 신용을 평가하는 하는 방식이다.

미국의 마스터카드와 익스페리안 등에서 신용평가에 도입한

비주얼DNA테스트는 금융 거래 내역이 없어도 15분 동안 40개 정도의 이미지를 보고 사용자의 취향이나 심리 상태에 따라 항목들을 선택하면 신용도를 평가 받을 수 있다. 이는 평소 사용자의 습관이나 성격, 특성을 단시간에 파악하여 신용도를 측정하는 방식이다.

국내의 금융기관은 개인정보유출에 대한 위험성을 고려하여 주로 신용평가기관이 전달한 정보를 바탕으로 고객 신용도를 평가하는 방식을 선호하는데 국외의 사례와 같이 많은 양의 금융데이터를 적극적으로 활용할 수 있는 기술과 인식의 개선이 필요하다.

다. 금융소프트웨어

기존에서 발전된 스마트기술을 사용하여 현재 기술방식보다 더욱 효과적이고 발전적인 금융업무 및 서비스 관련 소프트웨어를 제공한다. 송금의 경우 전자화폐 또는 이메일, 모바일을 통해 온라인상으로 편리하게 서비스를 제공할 수 있다. 자산관리 부문에는 기존의 금융 산업에 기술을 융합하여 보다 쉽게 사용할 수 있는 온라인 전용 펀드 등이 있으며 점포를 방문할 필요 없이 인터넷과 모바일을 통한 서비스 제공이 가능하다. 이는 발전된 금융 소프트웨어가 금융 업무를 효율적으로 만드는 것으로 이상 금융거래 탐지 시스템인 FDS(Fraud Detection System)도 이에 포함된다.

예를 들어 국내에서 사용된 신용카드가 1시간 뒤 미국에서 사용된 경우 기존 거래 패턴에서 어긋난 이상거래로 인식하고 추가 인증을 요구해 사기를 막는 기술을 말한다. 페이팔의 경우에는 초기 20% 정도의 사기 거래 비용들을 기업에서 부담하면서 FDS기술을 구축하였고 비자 혹은 마스터 카드와 같이 국제적 신용카드 회사도 자체 FDS를 사용 중이다.

국내의 금융 환경도 해외처럼 편의성을 우선으로 하게 되면서 핀테크로 대표되는 각종 규제가 완화되고 있고 이에 따라 FDS와 같은 금융 모니터링 시스템 도입에 대한 필요성이 커지고 있다

라. 플랫폼

국내외를 통합한 모든 기업들과 고객들이 금융기관과의 연계 없이 자유롭게 금융 거래서비스를 할 수 있는 다양한 거래기반을 제공하며 보다 더 안정적이고 이용하기 편한 플랫폼과 서비스들이 각광받고 있다.

투자 부문의 경우에는 개인과 기업의 자금을 공급해주는 금융 투자 플랫폼으로 소셜 플랫폼과 크라우드 펀딩 등이 존재하며 개인 혹은 기업이 인터넷 상으로 투자정보를 수집하고 자금을 조달할 수 있게 중개하는 역할을 한다. 또한 소비자가 각각의 금융거래와 온라인 상거래 등을 구분하지 않고 플랫폼서비스에만 가입을 하면 다른 서비스를 이용할 수 있도록 디자인 될 것이다.

예를 들면 소비자의 욕구에 따라 온라인 상거래에서의 결재서비스, 예금의 예치와 인출, 대출과 송금 등 전통적인 은행서비스, 자산운용서비스 등이다. 이외에도 금융시스템의 보안을 담당하거나 결제시스템이 간단해지고 인터넷 기반 금융서비스가 크게 활성화되면서 해킹 사이버 보안 위협 등에 대비한 고도의 금융보안 기술이 필요하다. [6]

2. 서비스 기술

현재 가장 유용하게 사용되는 휴대폰과 같이 센서들과 통신 기술이 구성된 모바일 기계의 발전과 확산으로 인하여 핀테크에 다양한 기술들을 적용하여 융합할 수 있는 환경이 구축되면서 주변 업체는 서비스 시장을 우선 확보하기 위해 여러 기술과 방법을 적용하여 결제 프로세스를 간단하면서 최소화하고 있다. 대표적으로 NFC, Barcode/QR 코드, Beacon, 모바일 단독카드 등이 있다[7].

가. NFC 결재

NFC(Near Field Communication)는 RFID의 하나로 13.56Mhz 주파수 대역을 사용하는 비접촉식 근거리 무선통신 모듈로 10cm의 단거리에서 단말기 간 데이터를 전송하는 기술이다[8]. 이 기술은 현재 데이터 전송뿐만 아니라 결재, 출입통제, 잠금장치 등에서 광범위하게 사용되고 있으며 구조적 특징은 아래의 <그림 2>와 같다. NFC결재는 2014년 'Apple Pay'를 선보이면서 결제에 널리 활용되기 시작했다.

<그림 2> NFC의 등장

나. Barcode/QR 코드

카드의 정보를 PG사에 등록하여 결제할 때 스마트폰으로 바코드(barcode)를 출력하거나 QR코드를 확인하여 결제가 이루어지는 방식이다. 바코드는 이용자가 스마트폰으로 바코드를 출력해 본인 카드의 정보를 제시하면 서비스센터는 바코드 리더기로 확인하여 카드 회사에 지급승인을 요청한다. QR코드방식은 서비스센터가 상품의 정보를 QR코드를 통해 제시하고 소비자는 어플리케이션을 이용하여 QR코드를 읽고 카드사에 지급승인을 요청한다.

다. Beacon

비콘(beacon)은 저전력 블루투스 통신기술을 이용하여 신호를 계속 보내주는 작은 장치이다. 근거리 위치인식을 적용시킨 무선 감지기다. 카드사들은 고객이 매장에 들어서면 스마트폰에 자동으로 쿠폰이나 할인정보 등이 뜨게 해 소비를 유도하는 마케팅기법을 도입·추진하고 있다. 하지만 카드사들의 시범사업 결과 블루투스 연동 등 사용자들의 기술적인 경험과 가맹점 단의 인식 부족이 비콘 확산이 지연되고 있다. 혁신적인 서비스의 사용자 경험이 많지 않아 마케팅 기법으로 서비스되고 있지 않다[9].

라. 모바일 단독카드

모바일 신용카드는 유심형(USIM) 모바일 카드와 앱형 모바일 카드 두 가지가 있다. 유심카드는 NFC 기능이 탑재된 안드로이드 OS 전용 단말기에서만 이용할 수 있고 앱 카드는 안드로이드 OS전용단말기와 애플IOS전용 단말기에서도 모두 사용할 수 있다. 핀테크의 발달로 대부분의 카드사들은 실물카드를 모바일 기기에 앱을 설치 한 후 서비스를 이용하는 앱 카드를 출시하였고. 최근에는 카드사별로 스마트폰으로만 카드결재를 할 수 있는 모바일 단독 카드를 출시하고 있다[10].

3. 보안 기술

금융시장이 온라인으로 확대되면서 보안에 대한 필요성은 강화되고 있고 최근 주목받고 있는 보안 기술인 FIDO, 블록체인, FDS 등에 대해 알아본다. [7].

가. FIDO (Fast Identity Online)

평균적으로 이용자 인증에 사용되는 ID/PW 방식은 지식 활용 인증으로 분류되는데, 다른 하드웨어가 필요하지 않으나, 이용자들이 서비스의 ID/PW를 기억해야 하는 고전적인 지식 활용 인증 방법의 문제점을 가지고 있다. 최근 인증방식은 이용자가 가지고 있는 고유 형태의 신체와 구조 또는 행동 및 결과 기반의 생체 인증 방법이 선호를 받고 있다. 이용자가 다른 토큰을 가지거나 기억해야 할 정보가 없으므로 이용자에게 편리함을 제공한다. 또한, 이용자의 고유정보를 사용함으로 보안성도 강하다.

최근 주목을 받고 있는 FIDO(Fast Identity Online)인증 방식은 스마트폰, 스마트 와치 같은 모바일 기계에서 사용하는 지문인식, 패턴, USIM기반 등의 인증방법을 온라인에 적용하는 것을 기본아이디어로 하고 있다. FIDO인증기술은 패스워드가 아닌 기계 인증을 통해 필요에 따라 다양한 인증기술을 선택할 수 있다는 점에서 간편결제에 가까운 기술이다. FIDO는 개인정보 제공하는 방식보다 더욱 강한 보안성을 가지면서도 쉽게 이용할 수 있는 인증 서비스라 할 수 있다[11].

온라인 환경에서 생체인식기술을 활용한 인증방식인 FIDO 대한 기술표준을 정하기 위해 2012년 7월 FIDO(Fast IDentity Online) 얼라이언스(Alliance)라는 협회가 설립 되었다. 회원사로 성전자, 블랙베리, 크루셜텍, 구글, 레노보, 마스터카드, 마이크로소프트, 페이팔, LG전자 등이 있다[12].

FIDO에서 가장 인기 있는 인증방식은 바로 바이오 인식이다. 신체가 인증으로 직결되는 바이오 인식은 이용자의 편리함을 추구하려는 국내 상황과 인증을 보강하려는 해외 유행에 적합하기 때문에 FIDO의 중요한 문제로 자리 잡았다. 게다가 FIDO는 다른 인증 방식들도 추가할 수 있기 때문에 다채로운 바이오 인식의 발전에 크게 이바지 할 것으로 보인다.

현재 실로 사용되고 있는 지문인식의 경우 익히 알고 있는 바이오 인식 기술이FIDO를 통해 핀테크와 관련하여 접목되었거나 앞으로 접목될

것이다. 아래의 <그림 3>은 지문인식을 이용한 FIDO 생체인증 과정을 나타낸다.

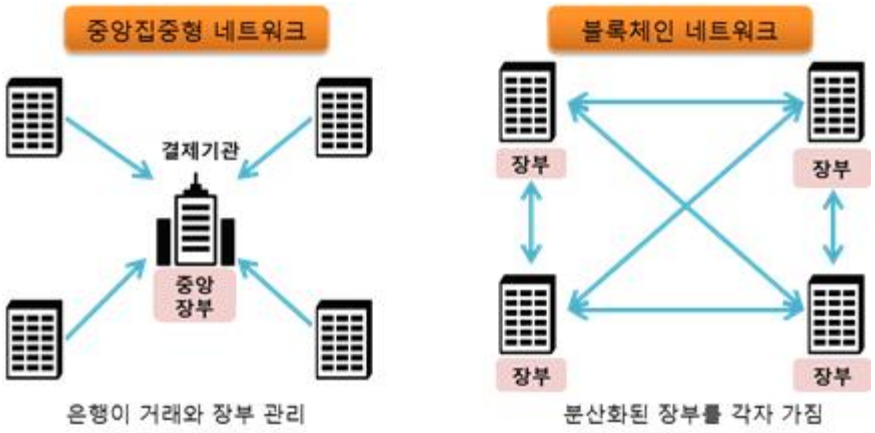
<그림 3> FIDO 생체인증 과정

여기에 뇌파, 음성, 필체, 행위인식 등 다양한 인식이 추가되고 있다. 무엇보다 FIDO는 핀테크의 인증을 포함하여 인터넷 접속 시 로그인, 출입의 제한 등 실생활에서도 간편하게 사용이 가능하므로 크게 주목 받고 있다. 식사 후 스마트폰을 사용해 카드 인증 후 결제하는 것이 가능하고, 신체 한 부분을 여러 사람들이 사용하는 단말기에 인증하는 방식에 대해 불편함을 가지는 사람들에게 FIDO는 희소식이 될 것이다[13].

나. 블록체인

블록체인은 거래 주체가 일정 시간 단위로 거래정보를 동시에 기록하고 보유하는 네트워크를 뜻한다. 기존에는 금융 거래 시 변동 내역을 금융기관이 승인한 후 금융기관 데이터베이스(DB)에 기록했지만, 블록체인에서는 거래주체들이 내역을 서로 교환해 승인하고 대조하는 방식으로 정보를 확인한다.

중앙 데이터베이스에 거래를 저장할 필요가 없기 때문에 처리속도가 빠르고 비용절감이 가능한 것이 장점이다. 또 모든 승인과정이 자동으로 암호화돼 현존하는 최고의 보안기술로 평가된다[14].



<그림 4> 블록체인 네트워크

위의 <그림 4>와 같이 블록체인은 금융거래에서 장부 책임자가 없는 거래 시스템이다. 중앙집권적 은행이 장부를 책임지는 게 아니라 이 거래 시스템에 참여하는 모든 사람들이 같은 장부를 보관하게 된다. 새 거래가 만들어질 때마다 장부는 이 정보를 별도의 '블록'으로 만들고, 이 블록을 기존 장부에 연결한다. 블록이 꼬리에 꼬리를 물게 되니 '블록체인'이 된다.

해커가 디지털 장부를 조작하려 해도 이용자가 수천만 명, 수억 명이라면 흩어져 있는 장부를 한꺼번에 조작할 수 없기 때문에 상대적으로 안전하다. 결국 블록체인 기술이 앞으로 주요 금융시스템으로 자리 잡는다면 은행의 존재가 없어도 개인끼리 스마트폰으로 전자화폐를 주고받는 시대도 상상해볼 수 있다.

이는 금융시스템이 블록체인을 통해 파격적인 비용절감을 얻을 수 있다는 얘기가 된다. 현재의 중앙집중적 시스템에선 모든 거래 기록과 개인정보를 저장하고 있는 중앙의 보안이 매우 중요하다. 금융 범죄자들은 이 보안시스템을 뚫기 위해 온갖 신기술을 끊임없이 개발한다. 금융회사들은 이를 방어할 기술에 막대한 비용을 투자하고 있다. 전자상거래가 더욱 확대되고 사물들까지 거래를 주고받는 사물인터넷 시대가 다가오면 비용은 더 치솟을 수밖에 없다.

다. FDS

FDS는 부정거래탐지 기술로, 카드회사 및 온라인게임에서 이상거래탐지에 빈번하게 사용되었다. 핀테크 분야에서는 모바일 결제방식에서 사용자 인증을 간편하게 만들어 이용자의 편의성을 제공하고, 거래의 안전 확인을 FDS를 이용해 확인한다. 또한 온라인 결제에서 이용자의 이체 혹은 거래내역이 정상거래 혹은 부정거래인지 확인하는 데 사용해 피싱/파밍에 대응하고 있다. 국내 금융사들도 작년부터 FDS를 도입해 오고 있으며, 한 기업은 최근 FDS로 인해 파밍 사기를 탐지해 부정거래를 미리 막을 수 있었다[15]. 아래의 <그림 5>는 FDS 구성요소 및 주요 기능을 나타낸다.

<그림 5> FDS 구성요소 및 주요 기능

하지만 FDS도 좋지 않은 소재들을 가질 수 있다고 확인되고 있다. 예를 들면, FDS의 구성요소인 이용자 스마트폰의 수집정보를 메모리에서 복제해 다른 기기에 재사용해 FDS의 탐지패턴을 우회하거나 피해자가 가해자로 둔갑할 수 있다. FDS의 경우 아직 초기 단계로 운영 및 관리경험이 부족하고 부정거래를 확인하는데 많은 시간이 걸리며 취약성 점검 기준과 프라이버시 문제 및 시험 방식이 구체적으로 개설되지 않았다. [12].

효율적인 FDS 운영에는 '다양한 패턴 축적'과 오탐율 최소화 '분석 및 운영능력'이 필요하다. 금융업계에 따르면 사기범 범죄수법은 갈수록 진화하고 있어 이를 방어하기 위해서는 다양한 패턴을 통해 사전에 인지하고 막는 것과 분석능력을 강화해 오탐율을 최소화하는 노력이 필요하다는 것이다.

많은 경험이 필요한 패턴축적은 일개 회사가 '경우의 수'를 확보하기는 쉽지 않아 업계 공유가 꼭 필요한 부분이다. 또한 단말기를 통한 자동화 차단은 탐지율을 강화하는 측면이 있지만, 100% 오탐율을 막는다고 보장할 수 없다. 거래 패턴이 미묘하고, 복잡한 부분이 있어 사람이 개입돼야 하지만, 24시간 365일 모니터링을 하면서 탐지한다는 것이 그렇게 만만치 만은 않은 작업이다. 고객과 직접 접촉하는 FDS는 오탐에 의한 민원이 발생할 소지가 있어 신중하게 접근해야 하는 부분이다. 업계에서는 FDS가 활성화되기 위해서는 패턴 공유를 통해 서로간의 시너지를 높이고, 오탐율을 최소화 할 수 있는 분석 능력을 강화하는 것이 필요하다고 강조하고 있다.

4. 결함 분석 기법들

가. 기존 결함 분석 기법

보안성 평가를 위한 적절한 분석 및 평가 기법을 적용 대상의 특성 등 여러 가지 요인들에 근거하여 선정되어야 하는 매우 중요한 사항이다.

시스템의 결함은 설계상의 실수, 부품의 오류, 하드웨어의 마모 등과 같은 하드웨어 결함과 소프트웨어 결함 및 운영인력에서 발생하며 그에 따른 통제도 하드웨어, 소프트웨어 및 운영 인력을 중심으로 수행된다[16].

시스템의 분석 기법으로는 먼저 제품을 개발하는 단계와 특성에 따라 분류를 할 수 있으며 예비 위험성 분석 PHA(Preliminary Hazard Analysis), 결함 위험성 분석 FHA(Fault Hazard Analysis), 운용 위험성 분석 OHA(Operating Hazard Analysis), 시스템 위험성 분석SHA(System Hazard Analysis) 등이 있다.

분석을 수행함에 있어서 두 가지로 분류하면 위험성을 언어적 표현으로 판단하는 정성적 분석 (qualitative analysis)과 정량적인 척도에 의하여

판단하는 정량적 분석 (quantitative analysis)이다. 또한 분석을 진행하여 가는 방법에 따라 고장 발생 원인으로부터 그 고장이 제품 전체에 미치는 결과를 시간의 흐름에 따라 분석하는 귀납적 기법 (inductive technique)과 시스템이나 제품의 고장으로부터 시간의 경과를 거슬러 그 원인을 추론해 가는 연역적 기법(deductive technique)이 있다. 대부분의 분석 기법들은 귀납적 기법이며, 결함 트리 분석(Fault Tree Analysis)은 대표적인 연역적 기법(Deductive Techniques)이다.

또한 시스템을 구성하는 최상위 수준에서부터 개별적인 부품 쪽으로 분석수준을 낮추어가면서 분석하는 상향성 접근기법 (Bottom-up approaches)과 개별적인 부품의 고장이 제품 전체에 미치는 영향을 추정하면서 분석수준을 높여 가는 하향성 접근기법(Top-down approaches)으로 분류된다. 대부분의 귀납적 기법은 상향성 접근 방식을 취하고 있으며, 연역적 기법은 하향성 접근 방식을 취하고 있다.

Thomas Maier는 FMEA를 이용하여 내부의 모든 오류를 확인하고, 각각의 소프트웨어 요구사항의 설정에 따라 실패가 치유되어 결함 트리의 구축을 통해 완성될 수 있다고 하였다[17]. James Catmur은 HAZOP와 FMEA를 병합하여 시스템의 사이프 사이클 전반에 걸쳐 위험 분석을 하였다[12]. 최근에는 두 가지 이상의 기법을 결합하여 하나의 시스템을 평가하는 연구가 진행되고 있다[18].

그러나 이와 같은 결함 분석 기법들이 어떤 시스템에서든 그대로 적용되기는 어렵고 안전성과 보안성 관련 부품이나 시스템의 특성에 따라 가장 적절한 기법으로 평가되어야 할 것이다.

나. 결함 위험 분석(Fault Hazard Analysis; FHA)

결함 위험 분석 (Fault Hazard Analysis)은 미국에서 Minute Man미사일을 개발하는 데 처음으로 사용된 기법으로 복잡한 시스템을 몇 개의 서브시스템으로 나누어 제작하는 경우, 서브시스템 인터페이스를

조사하고 각 서브시스템이 다른 서브시스템 또는 전체 시스템의 안전성에 미치는 악영향을 분석하여 보증하는 기법이다.

FHA는 특정한 상황으로부터 일반적인 사항으로 발전시켜 가는 귀납적 분석기법으로 작은 부품이나 사상(event)이 시스템이나 서브시스템의 안전에 미치는 영향이 검토된다.

FHA는 분석을 통하여 시스템 내의 각 시스템에 대해 두 가지 질문을 제기한다.

-해당 시스템은 어떻게 고장 나는가?

-그 고장의 결과가 시스템이나 서브시스템에 어떤 영향을 미치는가?

이 질문들에 답하기 위하여 FHA는 각 시스템은 한 가지 이상의 고장모드를 가질 수 있으며, 각각의 고장모드는 정상적인 시스템 기능에 위험을 초래할 수 있으므로, 시스템의 위험성 모드나, 위험성의 원인, 그리고 시스템이나 서브 시스템에 미치는 영향 등 시스템이나 서브 시스템에 관한 상세한 조사가 필요하다. 이 때 관련된 손상이나 기능저하가 시스템에 미치는 영향은 발생확률과 강도를 이용하여 간략히 서술된다.

이에 아래와 같은 <그림 6>은 결함 위험성 분석표 양식에서 2차 요인이란 시스템의 고장을 확장시키는 요인으로서 운용상의 요인이나 환경적인 요인들의 구체적 기준들을 나열한다. 시스템의 고장이 발전하여 다른 시스템의 고장이나 기능저하 같은 2차 고장을 발생시키는 관리적 요인을 가리킨다.

결함 위험성 분석표

프로젝트 : _____ 제 품 : _____ 계약번호 : _____

부품 명칭	부품 고장모드	제품 운용모드	하부시스템 예외 위험	제품기능 상실위험	환경요인	2차 요인	위험수준	위험관리

<그림 6> FHA 워크시트

FHA는 고장모드 및 영향분석 (FMEA)이나, 영향 및 치명도 분석 (FMECA)과 비슷하지만, 대상요소가 고장발생에 직접적으로 연결되는 것에 한정되며, 2차 고장이나 축차 고장에 관한 검토가 이루어진다는 점에 차이가 있다.

FHA는 고장의 치명적인(Catastrophic)면과 허용범위 밖의 경향들(Out-of-Tolerance Modes)을 고려한다[18]. FHA를 수행하기 위한 시스템의 특성들로는 현실적인 고장 경향과 그들의 측도, 장비의 역할, 운용 제한사항, 성공과 고장의 경계들, 발생 확률 등이 필수적이고 FHA의 수행 순서는 아래의 <표 1>과 같다[19].

<표 1> FHA 수행순서

단계	수행내용
1	해당 시스템의 서브 시스템들을 기능적으로 나눔.
2	시스템과 서브 시스템들을 기능 다이어그램, 약식도면, 그림 사이의 상호관계를 결정하기 위한 검토 수행.
3	분석 작업이 기능적이거나 분할된 수준까지 수행될 때 시스템의 완전한 성분 리스트를 최종 분석 수준까지 준비.
4	운영 및 환경적인 중점사항들은 시스템에 영향을 주게 되므로 시스템 또는 성분들에 미치는 역효과 여부를 검토.
5	중요한 고장을 발생하는데 영향을 주는 메커니즘들을 기능 다이어그램과 엔지니어링 도면을 이용하여 결정하고 서브시스템 고장들의 효과들을 고려.
6	서브시스템의 고장 가능 메커니즘들의 개별 성분 고장 유형들을 확인.
7	특별한 기간에 고장이나 손상의 확률을 증가시키는 하나의 성분, 시스템에 영향을 주는 모든 조작, 압력, 개인 행동들에 대한 조건들을 확인.
8	위험 범주 지정.
9	위험을 제거 및 제어하는 예방 조치들 반영.
10	초기 확률 값들을 지정하고 그 확률이 평가 될 특별한 고장 유형이 나타나고 있는가에 관심.
11	예비 임계 치 분석 수행.

<그림 7>은 고압가스를 저장하는 탱크에 대하여 FHA의 활용방법을 예시하기 위하여 몇 개의 부품을 간단히 분석한 사례이다.

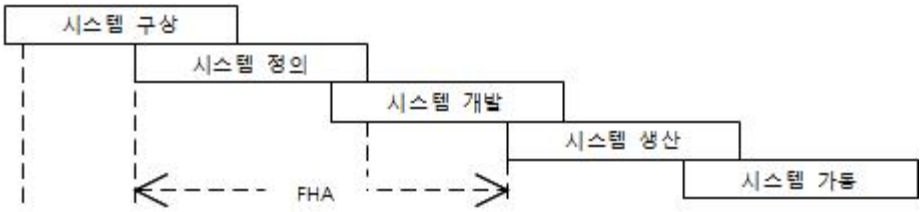
결함 위험성 분석표

계 획 : 제 품 : 고압가스탱크 계약번호 :

부품 명칭	부품 고장모드	제품 운용모드	하부 제품에의 위험	임무에 대한 위험	환경요인	2차 요인	위험수준	위험관리
안전 밸브	닫힌 고장	고압	과압	탱크의 고장	부식	작업자의 근접	강도:근접 작업자에게 파국적 빈도: 드묾	자주 밸브를 검사할 것
	열린 고장	고압	압력 불충분	제품 작동불능	부식	압력의 필요성	강도: 한계적 빈도: 가끔	작업전에 밸브밀폐 상태확인
압력 감지기	압력 과대평가	고압	압력 불충분	압력 불충분	없음	압력의 필요성	강도: 한계적 빈도: 가끔	정기적인 감지기 검사
	압력 과소평가	고압	과압	2차 제품이 정상작동 하면 영향없음 제품전체의 고장	없음	압력배출 부품의 신뢰도	강도:근접 작업자에게 파국적, 장비손상, 빈도: 드묾	정기적인 감지기 검사,압력 배출 제품으 추가설치

<그림 7> FHA의 예

시스템을 개발하는 초기 단계에서는 여러 가지 정보들이 안정되지 못하고, 그 중 어떤 자료들은 시스템의 후기 개발단계에서 정돈되기도 한다. 또한 서브 시스템에 대한 설계가 어느 정도 진행되어야 경계 면의 문제들을 파악할 수 있기 때문에, FHA는 시스템 개발단계에서 수행된다. 이에 FHA는 시스템 정의 및 개발단계에서 수행되는 것이 보통이며, <그림 8>은 이런 점을 보여주고 있다



<그림 8> FHA의 실시 시기

FHA는 어떤 서브시스템은 표시되지 않는 고장들을 가지기도 한다. 시스템 안전 프로그램(System Safety Program; SSP)에서 모든 고장들을 추적해보면 비용이 발생하게 되는데 이로 인해 일반적으로 소프트웨어 고장보다 하드웨어의 고장에 대해 집중하게 된다.

다. 위험 및 운영가능성 분석(HAZOP)

이 기법은 영국의 임페리얼 화학공업주식회사 (Imperial Chemical Industries Ltd.; ICI)에서 개발되어 미국 화공기술자협회 화학공정안전센터(American Institute of Chemical Engineers Center for Chemical Process Safety)에서 정리된 기법으로서, 여러 분야의 구성원들로 이루어진 분석팀이 브레인스토밍을 하는 과정에서 시스템의 위험요소들과 운용상의 문제점을 알아보는 것이다[20].

이는 시스템이 기존에 설계된 대로 작동하는 한 근본적인 위험성이나 운용상의 문제는 없지만 만약에 어떤 이유로 인해 이상요인이 발생하게 되면, 시스템이 그 충격을 감당할 수 있는 유무에 따라 사고가 발생한다. 제품을 생산하고 사용함에 있어서 발생할 수 있는 여러 가지 사건이나 상황을 가정하여 그 결과 초래될 수 있는 위험을 평가하고 개선대안을 모색하고 분석한다. 분석을 연구 절점(study nodes)이라고 하는 특정부분에 집중시켜 지침어(guide words)라는 독특한 분석지침을 도입하기 때문에 좀 더 조직적이고 체계적으로 분석을 할 수 있다.

HAZOP의 분석목적은 다음과 같다.

- 의도된 설계기능이나 조건 등을 포함하여, 제품이나 시스템의 상세한 설명을 제공한다.
- 시스템이나 제품의 모든 부분을 검토하여 설계 의도로부터 일탈이 어떻게 발생하는가를 파악한다.
- 이러한 일탈들이 위험 또는 사용상의 문제들을 초래할 수 있는지 결정한다.

HAZOP에서는 시스템의 기능 특성이 시스템의 상태변수를 통해

표현되어야 한다. 상태변수(process parameters)란 시스템의 기능이나 운용 상태를 나타내기 위한 물리적 변수들을 말한다. 분석을 위한 변수들을 파악하기 위해서는 공정흐름 다이어그램(Process Flow Diagram; PFD), 파이프 및 기기 다이어그램(Pipe and Instrument Diagram; P&ID)이 결정된 단계에서 실행되어야 한다. HAZOP 은 설계단계나 운용단계에서도 수행가능 하지만, 새로운 제품에 대해서는 설계가 거의 완성된 시점에서 실시하고, 기존공정에 대해서는 재설계가 계획되는 단계에서 실시하는 것이 좋다. HAZOP의 수행 순서는 다음 <표 2>와 같다. HAZOP의 수행은 일반적으로 표를 이용하여 정리되는데 일반적인 작성형식의 예는 <그림 9>와 같다.

<표 2> 위험 및 운영가능성 분석(HAZOP)의 수행순서

단계	수행 내용
1	분석 목적과 범위 결정 분석 대상이 너무 많을 때는 보통은 위험성이 높다고 판단되는 부분을 선정하여 분석을 집중한다.
2	분석 팀의 구성 최초 ICI 사에서 규정한 HAZOP의 정의에 의해 분석 팀은 전문가들로 구성된다.
3	예비조사 필요한 자료의 획득, 획득된 자료를 적절한 형태로 전환하거나 분석하기 위한 절차의 수립, 회의 일정의 계획으로 진행된다.
4	브레인 스토밍 실시 팀 구성원들이 함께 모여 다양한 전문지식과 의견 교환을 통한 브레인 스토밍을 한다. 검토대상은 연구 절점(study node)이라고 부르는 제품변수들의 일탈이 조사될 제픔구조 및 기능상의 위치를 말한다. 일탈(deviation)이란 지침어를 적용시킴으로써 발견되는 의도된 기능으로부터 벗어난다.
5	분석 결과 기록 브레인 스토밍을 통하여 발견된 위험요소 또는 사용상의 문제, 안전성 향상을 위해 수행되어야 하는 설계 및 사용절차의 수정사항, 미진한 분석결과를 보완하기 위하여 수행되어야 하는 심층 분석 등의 결과를 얻을 수 있다.

HAZOP

분석팀 : _____ 분석자 : _____

날 짜 : _____ 설계자 : _____

품목번호	일탈	원인	결과	안전장치	조치

<그림 9> HAZOP 워크시트

제품 운용 도중에도 다양한 이유들로 수정을 하게 되는데 이러한 제품의 변경은 제품 기능변화와 동시에 기능장애나 사고의 가능성도 도입되게 되고 제품을 수정하거나 보정을 하는 경우 권장하게 되어 활용되고 있다.

라. 결함 트리 분석 (Fault Tree Analysis; FTA)

이 기법은 미국의 Minute Man 미사일 발사 시스템을 개발하던 도중 1962년 벨(Bell)연구소의 Watson이라는 사람에 의해 고안되었고 결함 수목 분석, 고장 수목 분석 등 여러 가지 용어로 사용되기도 한다. 이 기법의 개발 목적은 아래와 같다.

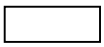
- 정상사상을 초래하는 원인이나 원인들 조합의 구명
- 특정한 제품 신뢰성 척도가 서술된 요구사항을 충족시키는가 여부의 결정
- 제품의 독립성과 고장의 비관련성에 대하여 다른 분석들에서 이루어진 가정들이 위배되지 않는가에 대한 결정
- 특정 신뢰도 척도에 가장 심각한 영향을 미치는 요인들과 그 척도를 개선하기 위하여 필요한 변경들의 결정
- 공통적 사상이나 공통원인고장의 구명 등 이었으며, 이 목적들은 지금도 충실히 충족되고 있다.

FTA의 Tree는 정상사상(top event)이라고 부르는 바람직하지 않은 사상을 시작으로 그 발생원인 또는 발생 원인에 기여하는 조건들을 찾아

시간적 흐름을 거슬러 분석해 가는 연역적 구조이다. 또한, 정성적인 분석 및 정량적인 분석 모두 가능하고, 제품 구성 수준에서는 하향성 분석방법(top-down approach)이라 할 수 있고 수학적 논리는 부울 대수 (Boolean Algebra)에 의해 지원되고 있다.

FTA는 잘 알려진 생산적인 위험 식별 도구이며 위험들을 평가하고 통제하기 위한 표준화된 훈련방식을 제공하고 안전성에서 경영 이슈(issue)들에 이르기까지 다양한 문제들을 해결하고 전문적인 안전성 및 신뢰성 공동체에 의해서 위험과 고장들을 예방하고 분해하는데 모두 사용된다. FTA는 고장과 위험을 나타내는 논리적 도식 표현의 결함 트리 다이어그램으로 결과물을 나타낸다. 결함 트리에 사용되는 기호는 다음 <표 3>과 같다[21].

<표 3> FTA에 사용되는 결함 트리의 기호

기호		내용
	Event	개개의 사상으로 보통 결함사상을 표시 논리 기호의 입력 또는 출력
	Basic Event	기본적 사상 논리기호의 입력 논리기호의 출력은 되지 않음
	undeveloped event	정보부족에 의해 분석되지 않거나 또는 분석의 필요가 없는 생략현상을 나타내는 기호
	In	동일한 결함 트리 속에서 내용이 같은 다른 부분과의 사이에 전이를 나타내는 기호 삼각형의 상부에 선이 나오는 경우는 다른 부분에서의 전입을 의미하고 측면에서 나오는 경우는 다른 부분으로의 전출을 의미
	Out	
	AND gate	하위의 사건을 모두 만족하는 경우에 사용하는 논리 게이트
	OR gate	하위의 사건 중 하나라도 만족하면 사용하는 논리 게이트

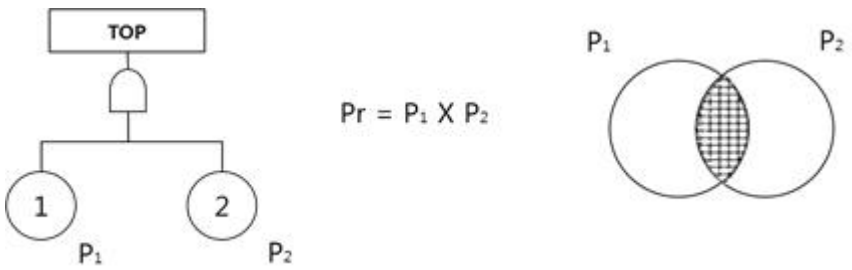
구성된 FTA에서 정상사상이나 중간사상의 발생 확률을 계산하여

예측하는 것도 중요하지만 정상사상 발생에 영향을 미치는 요소를 파악하는 것도 중요하다.

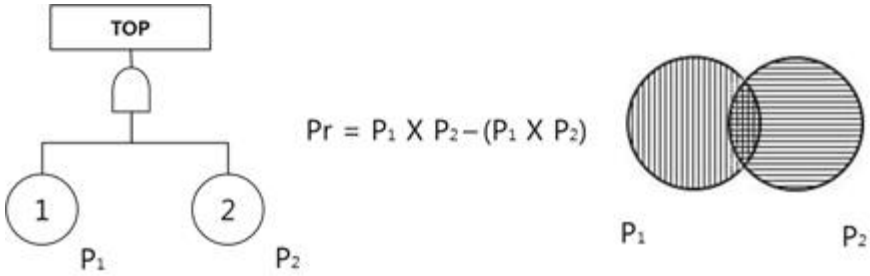
정상사상의 위험성을 효과적으로 감소시키기 위하여 사용되는 방법이 최소절단집합(Minimal Cut Sets)과 최소경로집합(Minimal Path Sets)이다. Minimal Cut Sets과 Minimal Path Sets은 개개의 기본사상 발생확률과 무관하며 AND와 OR로 구성되는 논리조합의 영향을 받아 현실적으로 유용하고 즉각적인 FTA가 가능할 수 있는 것이다. 즉, FTA를 이용하여 재해발생 확률을 계산하자면 각각의 기본 사상 발생 확률 확보가 전제되어야 하고, 또한 고장율의 신뢰도에 따라 결과의 차이는 클 수 있지만 Minimal Cut Sets과 Minimal Path Sets은 논리조합의 지배를 받기 때문에 분석의 오차를 최소화할 수 있는 장점이 있다.

한편 Minimal Path Sets이란 여기에 포함되어 있는 기본 사상이 일어나지 않으면 정상사상이 발생하지 않는 기본사상의 집합이라고 정의할 수 있다. FT를 수식으로 표현하거나 간소화하기 위하여 부울 대수(Boolean Algebra)를 사용하는데 이 방법은 논리계산의 한 수단으로서 어느 집합을 구성하는 부분집합들의 논리곱과 논리합을 사용하여 표현하고, 이들의 확률을 계산식을 사용함으로써 FT의 정상 사상이나 중간 사상, 즉 구하고자 하는 재해 발생확률을 계산하는 방법을 말한다.

이와 같은 방법으로 구성된 FT는 AND게이트 <그림 10>과 OR게이트 <그림 11>로 이루어지며 이들의 해석적 방법에 의한 사상발생 확률을 다음과 같이 표시할 수 있고 기본사상이 서로 통계적으로 독립되어 있다고 가정한 접근 방법이다.



<그림 10> AND 게이트

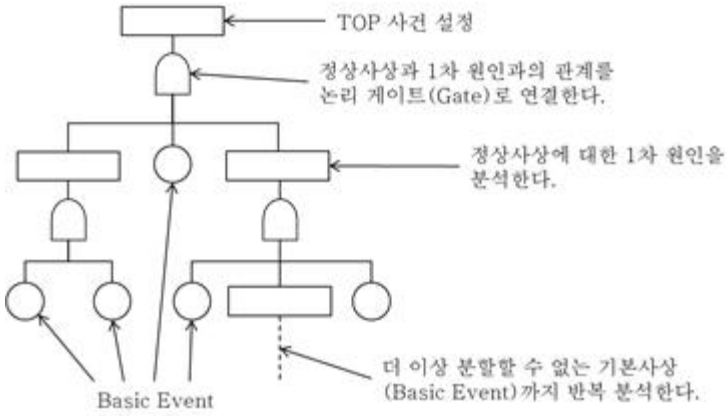


<그림 11> PR 게이트

결함 트리 분석(FTA)의 일반적인 수행 절차는 <표 4>와 같고 <그림 12>는 FT의 작성을 보여준다[21-25].

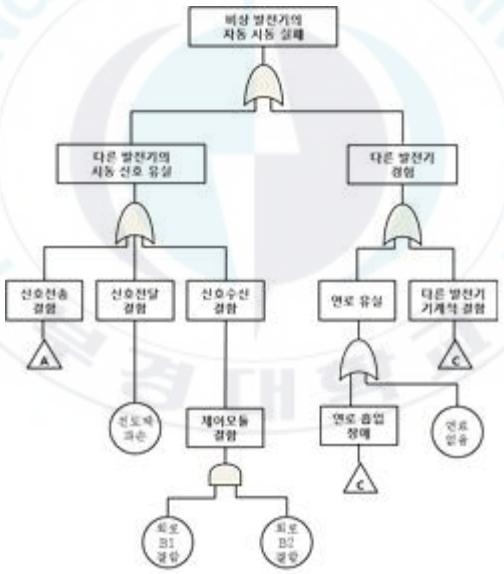
<표 4> 결함 트리 분석(FTA)의 수행순서

단계	수행 내용
1	정상사상(Top Event) 설정 작업자의 과오나 대책을 설정할 문제점들에 대해 중요도나 우선순위를 결정하여 분석할 대상이 되는 사항을 정상사상으로 선정한다.
2	대상 플랜트, 프로세스의 특성을 파악 해석하려는 시스템의 공정과 작업내용을 파악한다. 시스템의 완전한 이해와 정의, 그리고 이들의 상호관계가 있는 것이 FTA에 있는 모든 단계들을 위해 필요하다. 예상되는 재해에 대하여 과거의 재해사례나 재해통계 등을 활용하여 가급적 폭넓게 조사한다.
3	FT 작성<그림 12> 1) 정상사상에 대한 1차 원인을 분석한다. 2) 정상사상과 1차 원인과의 관계를 논리 게이트(GATE)로 연결한다. 3) 1차 원인에 대한 2차 원인(결함사상)을 분석한다. 4) 1차, 2차 원인에 대한 관계를 논리 게이트로 연결한다. 5) 더 이상 분할 할 수 없는 기본사상(Basic Event)까지 반복 분석한다.
4	FT 구조해석 작성된 FT를 부울 방정식(Boolean Algebra)에 의해 간소화한다. Minimal Cut Sets, Minimal Path Sets를 구한다. 정상사상에 영향을 미치는 중요한 중간 및 기본 사상을 파악한다.
5	FT 정량화 기본사상의 발생빈도나, 고장률, 에러 데이터 등을 정리하여 중간사상 및 정상사상의 발생확률을 계산한다. 재해발생 확률 계산 결과는 과거의 재해 또는 유사한 재해의 발생률과 비교하는 현격한 차이가 날 경우는 작성된 FT에 대하여 재검토를 한다.
6	해석 결과의 평가 재해 발생의 확률이 허용할 수 있는 위험수준을 초과할 경우 이것을 감소시키기 위한 대책을 수립한다.



<그림 12> FT 작성

<그림 13>은 비상발전기의 자동시동이 실패한 경우를 분석하기 위하여 구성된 결함 트리 (FT) 의 예이다.



<그림 13> FTA의 예

분석은 이와 같은 FT를 근거로 중복 사상의 제거, Minimal Cut Sets의 획득, 각 사상들의 발생확률 도출 등의 순서로 진행되지만, 계산상의 과정은 상당히 복잡하여 사실상 조금만 복잡한 제품을 분석하려 해도 지원도구가 필수적이다.

FTA를 이용하여 시각적으로 사고원인을 분석하여 재해 발생확률이

높은 인적, 물적 환경상의 위험 및 위험사항에 대한 안전대책을 강구함으로써 재해발생확률의 지속적인 감소를 통한 재해예방활동을 체계적이고 과학적으로 수행할 수 있다. 그러나 FTA를 실천하기 위해서는 현 분야에 전문적인 지식을 갖춘 인재가 필요하고 정성 평가에 비하여 막대한 시간과 경비가 소요된다. 따라서 정성적 평가를 거친 후 위험도가 높은 시설이나 공정 등을 대상으로 수행함이 바람직하다.

성공적인 FTA를 위하여 동일한 기기, 부품이라도 사업장, 취급물질, 운전조건 및 작업자의 숙련도에 따라 고장율은 다르므로 가능한 해당 공정 및 시스템에서 발생한 정비자료를 기초로 통계처리를 하여야 높은 신뢰도를 유지할 수 있다. 이에 AND게이트 선택 시에는 논리적으로 타당한가를 신중히 검토하여야 정확한 FTA 결과를 도출할 수 있다.

마. 고장 유형 영향 및 치명도 분석

고장 유형 영향 및 치명도 분석(FMECA)은 고장 분석을 위해 수행하는 체계적인 기술 중에 하나로 미 항공우주국(NASA)에 의해 우주 프로그램 하드웨어의 신뢰성을 향상시키고 검증하기 위해 개발되었다[26].

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[27].

초기 FMECA는 FMEA (Failure Mode sand Effect Analysis)라 불렸으며 지금은 FMEA의 확장된 개념으로 FMEA와 치명도 분석(CA; Criticality Analysis)으로 구성된다. FMECA에서 “C”가 CA를 의미하며

이는 다양한 고장으로 인한 영향의 치명도 또는 심각성(Criticality또는 Severity)을 고려하고 그 정도를 레벨로 표현한다. FMEA는 CA를 수행하기 전에 완료되어야 하며 FMEA는 시스템과 하부시스템의 고장유형의 정량적 순위를 분석하여 보여주고 CA는 컴포넌트와 시스템과 연관된 신뢰성과 심각성을 분석한다[28-30]. FMECA의 수행 순서는 다음 <표 5>와 같다[31]

<표 5> 고장 유형 영향 및 치명도 분석(FMECA)의 수행순서

단계	수행내용
1	시스템 요구사항을 정의하고 핵심 기술적 목표를 기술.
2	시스템의 기능적 분석 시스템을 기능별로 분류하고 다이어그램을 작성. 시스템은 개발 생명 주기 초반에 기능 요소로 분해되고 이후에 물리적인 패키지 형태로 구성.
3	시스템의 최상위 단계에서 중간단계, 최하위까지 하향식 방법으로 기능별 요구 조건 분석.
4	시스템의 구성요소 별 주어진 기능이 결함을 일으키는 고장 모드를 식별.
5	부정확한 재료, 부적당한 보수유지, 피로, 마모 등과 같은 고장의 잠재적인 원인과 고장 메커니즘을 평가.
6	고장으로 인한 영향(Effects of Failure)을 결정. 시스템 내 같은 레벨, 상위 시스템 레벨, 전체 시스템 순으로 확대.
7	고장 식별성 평가(Failure Detection Means). 시스템 내에 특정 결함의 식별 가능성이 어느 정보 되는지 확인.
8	고장 모드의 심각도 결정(Determination of Failure Mode Severity). 시스템 성능 감소, 시스템의 파괴나 인명 피해가 있는지 특정 고장으로 인한 영향이나 충돌의 중요성을 참조하여 고장 결과 범위 설정.
9	특정 고장 유형이 얼마나 자주 발생하는가에 대한 고장 모드 발견 확률 평가. 발견 확률 순위 1부터 10까지의 수를 사용하여 정량화 표기.
10	위험 우선순위 (Risk Priority Number; RPN) 를 계산. RPN = 고장효과의 심각도(Severity) x 발생 가능성(Occurrence) x 고장 검출 능력(Detecting)
11	영역으로 식별되는 반복적인 프로세스나 그 원인에 대한 평가, 시스템 향상을 위한 제언으로 후속 조치를 하는 것이다.

FMECA의 수행은 일반적으로 표를 이용하여 정리되는데 일반적인 작성형식의 예는 <그림 14>와 같다.

FMECA 작성표

제 품 : _____ 분석자 : _____

날 짜 : _____ 설계자 : _____

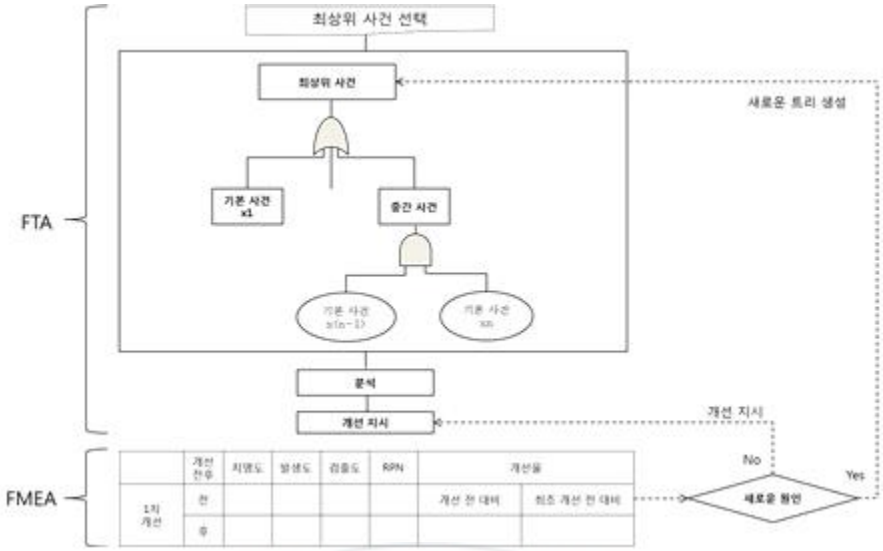
구성요소	기능	구분 번호	고장양식	고장원인	고장의 영향		검출방법	중요성 및 대책	고장발생 확률	치명도 순위	비고
					부분적 영향	제품 전체					

<그림 14> FMECA의 워크시트

IV. 핀테크 결제 시스템의 보안성 개선을 위한 결함 트리 분석

1. FTA와 소프트웨어 FMEA/C의 통합

FMEA/C는 bottom-up 분석 기법으로 소프트웨어 시스템에서 가능한 소프트웨어 실패 모드의 결과를 확인하는 기능이다. FMEA/C는 표 형식의 자료이기 때문에 소프트웨어 결함의 원인 사이의 논리 관계를 설명하기 어렵다는 단점이 있다. FTA는 top-down 분석 기법으로 원하지 않은 사건을 유발하는 요소를 찾아내는 기법이다. FTA는 최상의 사건의 선택을 고려하는 것이 어렵다. 이에 두 가지 기법을 통합하여서 분석한다면 포괄적이고 효과적인 방법이 될 것이다. FTA와 FMEA/C를 통합하는 방법은 아래의 <그림 15>와 같다[36-43].



<그림 15> FTA기준 FMEA/C 통합 기법

우선 소프트웨어 결함 트리를 만들기 위한 최상위 사건을 선택하여 결함 트리에서 부정확성이 나타나거나 고장 영향의 치명도에 따라 새로운 최상위 사건이 나타난다면 결함 트리를 수정할 수 있다. FMEA/C에 의해 치명도 분석이 이루어진 후에 최상위 사건의 발생 확률은 계산될 수 있다.

FTA 기준 FMEA/C의 통합 기법 수행 순서는 다음과 같다. 소프트웨어 보안 요건이나 위험 분석에 따른 최상위 사건 선택과 결함 트리 제작, 해당 사건들의 질적인 분석을 통한 확인, 고장 모드에 의한 해당 사건의 FMEA/C 형성, 결함트리와 개선 지시 수정 또는 새로운 결함 트리를 만들어 다음의 분석을 수행하기 위한 최상위 사건의 결함 모드 선택이다[35,42-43].

2. 핀테크 결제 시스템의 FTA와 FMEA/C 보안성 평가 및 개선

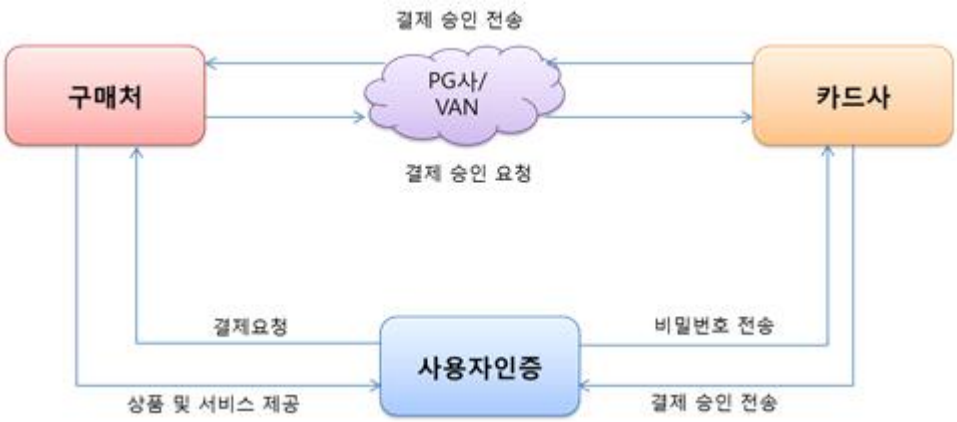
가. 핀테크 결제 시스템의 기능블록 다이어그램

핀테크 결제 시스템의 보안성을 분석하기 위해서는 기능 영역이 정의되어야 한다. 아래의 <그림 16>은 핀테크 결제 시스템의 기능 블록 다이어그램이다.

핀테크 결제 시스템은 사용자 인증, 관리 시스템으로 이루어져 있고 관리 시스템은 키 관리 서버, 어플리케이션 관리 서버, 카드 관리 서버로 구성되어 있다.

키 관리 서버는 어플리케이션 관리 서버와 카드관리 서버를 운영하기 위하여 요구되는 키들에 대한 프로파일 생성, 관리하는 서버로써 키값의 정의와 키 프로세스 관리 등을 수행한다. 어플리케이션 관리 서버는 어플리케이션의 전체적 프로세스를 관리하는 서버로 어플리케이션의 정의, 어플리케이션 추가 및 제거, 어플리케이션 발급정보 조회, 발급 요구처리 등의 기능을 수행한다.

카드 관리 서버는 전체적인 주기인 프로세스를 관리하는 서버로써 카드 발급 프로세스, 데이터의 입력과 출력, 카드 형식, 종류의 정의 등의 기능을 처리하기도 한다. 어플리케이션 다운로드 서버는 다양한 네트워크인 인터넷이나 무선 랜을 통하여 요청되는 후 발급 처리에 대해서 키 관리 서버, 어플리케이션 관리 서버, 카드 관리 서버와 연동하여 사용자에게 다양한 어플리케이션을 동적으로 다운로드 시켜주는 역할을 수행한다.



<그림 16> 핀테크 결제 시스템 다이어그램

나. 핀테크 결제 시스템의 결함 리스트

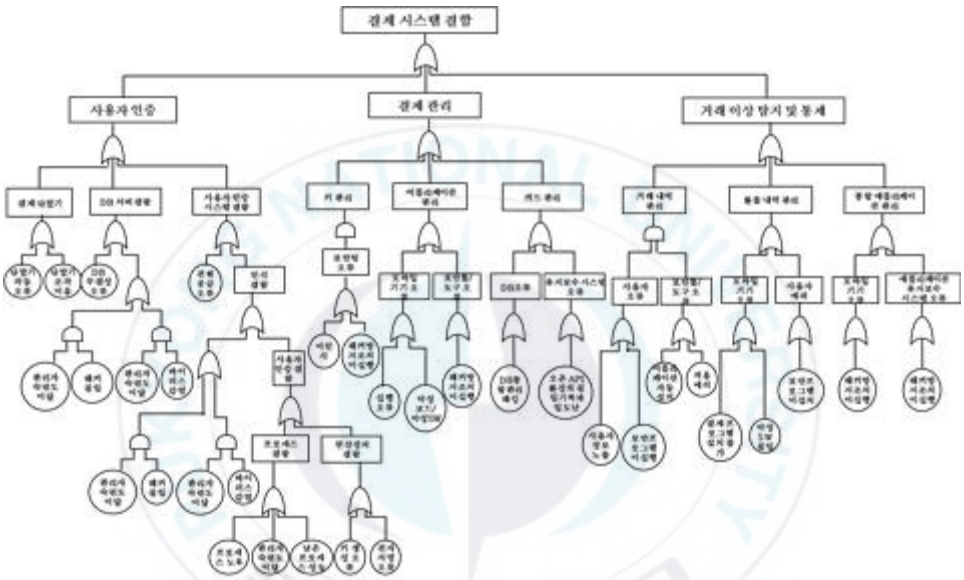
핀테크 결제 시스템의 기능 블록 다이어그램을 사용하여 기능별 결함들을 추출한다. 초반부에는 기능별 예상 결함을 리스트로 작성하여 사용하지만 시험과 운영을 거치면서 보다 자세하고 실제적인 결함 리스트들을 <표 7>과 같이 구할 수가 있다.

<표 6> 핀테크 결제 시스템의 기능별 결함리스트

시스템		기능	기능별 결함
사용자 인증	결제 단말기	결제 카드 인식	단말기 작동 오류
	DB 서버	사용자 정보 저장	DB 서버 오류
	사용자인증 시스템	사용자 정보 식별	사용자 인증 오류
결제 관리	키 관리	키 값의 정의	사용자 거래 불가, 사용자 거래내역 오류, 사용자 인증 오류
		키 프로세스 관리	사용자 거래 불가, 사용자 거래내역 오류, 사용자 인증 오류
	어플리케이션 관리	어플리케이션 정의	카드 결제 오류
		어플리케이션 추가 및 제거	카드 결제 오류
		어플리케이션 발급정보 조회	카드 결제 오류, 사용자 거래 불가
		발급 요구처리	카드 결제 오류, 사용자 거래 불가
	카드 관리	카드 발급 프로세스	사용자 발급 오류
		데이터의 입력과 출력	사용자 데이터 오류
		카드 형식 및 종류의 정의	카드 결제 오류
이상거래탐지 및 통제	거래 내역 관리	거래 자료 수집	사용자 거래내역 오류
		분배 정산 처리	사용자 거래내역 오류
	환불 내역 관리	환불 내역 자료 수집	사용자 거래내역 오류
		수수료 지불 내역 정산 처리	사용자 거래내역 오류
	통합 어플리케이션 관리	보안 툴 오류	사용자 거래내역 오류
		유지 보수 시스템 오류	사용자 거래내역 오류

다. FTA에 의한 결함 분석

FTA는 결함 발생의 원인들을 한눈에 알기 쉽게 표현한 순차적인 그래프 모형으로 모바일 결제 시스템과 모바일 결제 시스템의 결함 목록 리스트에 의하여 <그림 17>과 같이 모바일 결제 시스템의 FTA를 정의할 수 있다. 이를 통해 모바일 결제 시스템 결함 원인이 파악되어 설계된 시스템을 정성적, 정략적으로 분석 가능하다.



<그림 17> 결제 시스템의 최상이 수준에 따른 결함 트리

라. FMEA/C에 의한 핀테크 보안위험 우선순위계산과 개선지시

FMEA/C에 의한 핀테크 결제 시스템의 보안 위험 분석을 위해서는 적당한 워크시트가 필요하다. 아래의 <표 7>은 기존의 FMEA/C를 위한 워크시트를 축약 및 변경하여 나타내었다. 고장에 대한 위험 우선순위(RPN, Risk Priority Number)를 계산하여 RPN을 높은 고장부터 개선지시(Corrective Action)를 수행한다. 결함에 대한 개선 지시(Corrective Action)에 의해서 결함은 줄어든다.

<표 7> 개선 지시에 따라 수정 계산된 RPN 값

개선 차수	개선 전후	치명도	발생도	검출도	RPN
1차	개선 전	7.0	9.4	10.0	658.0
	개선 후	7.0	8.2	9.3	533.8
2차	개선 전	7.0	8.2	9.3	533.8
	개선 후	7.0	6.5	6.4	291.2
3차	개선 전	7.0	6.5	6.4	291.2
	개선 후	7.0	4.3	4.5	135.5

치명도(Criticality)는 고장 유형의 치명성의 정도 ($0 \leq C \leq 10$), 발생도(Occurrence)는 고장 유형의 발생 가능성의 정도($0 \leq O \leq 10$), 검출도(Detection)는 시스템이 사용자에게 양도하기 이전에 고장이 검출될 수 있는 가능성의 정도($0 \leq D \leq 10$)를 말한다. RPN의 값은 RPN=치명도(Criticality) x 발생도(Occurrence) x 검출도(Detection)로서 구할 수 있다.

본 논문에서는 핀테크 결제 시스템의 FMEA/C는 치명도, 발생도, 검출도, RPN의 이해를 돕기 위한 개선 지시의 1차, 2차, 3차에 따른 RPN이 개선되는 가상적인 예를 나타낸 것이다. RPN이 개선된 것은 결함에 대한 치명도, 발생도, 검출도 등을 최대한 감지하여 개선한 것으로 차구가 높아짐에 따라 결함이 감소되어 3차 개선에서는 RPN 개선율이 최고 83.4%까지 도달됨을 보여주고 있다. <표 7>에서 치명도의 값이 1차, 2차, 3차에 있어서 동일한 이유는 치명도라는 것은 그 보안성의 위험은 시스템이나 소프트웨어가 개선됨에 있어서도 동일하기 때문에 본 논문에서는 각 소프트웨어 보안성 결함에 있어서 동일한 수치를 사용했다. 또한 <표 7>의 예에서는 개선 지시를 3차까지 수행하였지만 안전성을 보장해야 하는 사용자의 요구사항이 있다면 그 조건을 만족 시킬 수 있을 때까지 수차에 걸쳐서 개선노력을 수행해야 할 것이다.

V. 결론 및 향후 과제

핀테크는 모바일 단말기 사용자라면 누구나 빠르고 편리하게 금융 서비스를 활용할 수 있다는 장점으로 인해 개인정보 및 금융 정보 등에 대한 보안적인 측면의 우려에도 불구하고 핀테크 시장은 점차 확대되어 가고 있다.

그러나 핀테크에 대한 국내외 관심과 개발 단계는 이제 초기 단계를 벗어나는 시점으로 볼 수 있으며 핀테크를 대상으로 집중적으로 다루어진 연구는 크게 많지 않은 실정이다. 주로 핀테크 초기 형태인 모바일 간편 결제에 대한 연구가 국내외에서 실시되고 있으며, 핀테크 관련 연구로는 개념 정리하는 형태의 연구나 보안과 같은 기술적인 측면을 다루는 연구가 주로 이루어지고 있다.

특히 국내의 핀테크 수용에 대한 연구가 매우 미흡한 실정이며, 정부규제가 완화되고 지원 정책이 발표되고 있는 시점에서 사용자들을 대상으로 하는 핀테크 수용에 관한 지속적인 연구가 필요하다.

본 논문에서는 FTA를 기준으로 FMEA/C와 통합하여 핀테크 결제 시스템의 보안성을 평가하고 개선하는 상호 보완적인 결함 분석 기법 제안하였다. 핀테크 결제 시스템들과 같은 정보 시스템의 보안성을 평가하기 위해서는 단지 하나의 시스템 보안성 평가 방법으로는 적절한 분석이 이루어 질 수 없다. 시스템의 결함들을 FTA를 기준으로 FMEA/C와 통합하는 것은 핀테크 결제 시스템의 보안성을 평가하고 개선하는데 상호 보완적인 최적의 결함 분석 기법이라고 할 수 있다.

이에 핀테크 결제 시스템의 보안성을 평가하기 위해서는 효율적인 결함 분석 기법들과 그 상호 보완적인 결함 분석 기법들의 조합을 연구하고 분석하여 앞으로 핀테크 활성화를 위한 시스템의 안전성과 무결성을 확보할 수 있는 방안에 대해 연구해나갈 것이다.

참고문헌

[1] 이기송, “국내외 핀테크 동향과 전망,” KB지식비타민, Vol. 14, No 60, 2014.

[2] 강병진, “국내 핀테크 활성화 방안 연구_해외 사례를 중심으로,” 석사학위논문, 고려대학교, 2015.

[3] 성기윤, “핀테크 결제의 편리성과 안정성: 토큰화 관점,” 정보과학회지, Vol. 33, No. 5, pp. 13-16, 2015.

[4] 한동균, “핀테크 수용 및 활성화에 영향을 미치는 요인에 관한 연구,” 박사학위논문, 연세대학교, 2015.

[5] 김병우, “국내 핀테크 산업 활성화에 관한 연구,” 경영교육저널, Vol. 26, No. 1, pp. 47-73, 2015.

[6] 구은희, “핀테크의 모바일 결제 기술 및 보안 동향,” 정보처리학회지, Vol. 22, No. 6, pp. 15-22, 2015.

[7] 문성태, 김기남, “핀테크 서비스 기술과 보안동향 분석,” 인터넷정보학회지, Vol. 16, No. 2, pp. 23-32. 2015.

[8] 강준영, 손준혁, 곽경섭, “QR코드, NFC를 활용한 모바일 소셜 커머스 쿠폰 결제 시스템에 관한 연구,” 한국컴퓨터정보학회, Vol. 23, No. 1, pp. 325-328, 2015.

[9] 조해룡, 이양규, 최민, “Beacon을 이용한 위치기반 인증 시스템 설계,” 한국컴퓨터정보학회, Vol. 23, No. 1, pp. 67-70, 2015.

[10] 이지호, “모바일 카드의 주요 기술 및 표준화 동향,” 한국정보보호학회, Vol. 21, No. 4, pp. 57-61, 2011.

[11] 김수형, “FIDO 기반 핀테크 인증 기술,” 정보와 통신, Vol. 33, No. 2, pp. 59-65, 2016.

[12] 조상래, 조영섭, 김수형, “FIDO 2.0 범용인증기술 소개,” 한국정보보호학회, Vol. 26, No. 2, pp. 14-19, 2016.

[13] 문현준, 이민형, 정강훈, “스마트폰 환경의 인증 성능 최적화를 위한 다중 생체인식 융합 기법 연구,” 한국디지털정책학회, Vol. 13, No. 6, pp. 151-156, 2015.

[14] 박수민, 강희정, 정윤정, 홍승필, “블록체인 기반의 안전한 핀테크 서비스 정책 제언,” 한국인터넷정보학회, Vol. 17, No. 1, pp. 117-118, 2016.

[15] 이성훈, 박준범, 김대엽, 최대선, 진승헌, “핀테크 기술 및 보안동향,” 전자통신동향분석, vol. 3, no.4, pp. 110-119, 2015.

[16] Harold W. Lawson, “An Assessment Methodology for Safety Critical Computer Based Systems,” *Proceeding of CSR 12th Annual Workshop on Safety and Reliability of Software Based Systems*, pp. 183-200, 1995.

[17] Maier T., “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, 1995.

[18] Rodrigo de Queiroz Souza, Alberto José lvares, “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.

[19] Myong hee Kim and Man-Gon Park,”A Study on the Software Fault Modes and Effect Analysis for Software Safety Evaluation,” *Journal of Korean Multimedia Society*, Vol. 15, No. 1, pp.113-130. 2012.

[20] Andrew Hussey, “HAZOP Analysis of Formal Models of Safety-Critical Interactive Systems,“ *Computer Safety, Reliability and Security, Lecture Notes in Computer Science*, Vol. 1943, pp. 371-381, 2000.
[21] Myong hee Kim, Eun-Ji Jin and Man-Gon Park,“Fault Tree Analysis and Fault Modes and Effect Analysis for Security Evaluation of IC Card Payment Systems,” *Journal of the Korean Multimedia Society*, Vol. 16, No. 1, pp. 87-99. 2013.
[22] R. E. Barlow, P. Chatter jee “Introduction to fault tree analysis,” ORC 73-30, *Operations Research Center, Univ. of California*, 1973.
[23] Knight, John C. and Luis G. Nakano, “Software Test Techniques for System Fault-Tree Analysis,” *Press of University of York*, Vol. 16, pp. 369-380. 1997.
[24] Youn ju Oh, Jun beom Yoo, Sung deok Cha, and Han Seong Son, “Software Safety Analysis of Function Block Diagrams using Fault Trees,”*Reliability Engineering and System Safety*, Vol. 88, No. 3, pp. 215-228, 2005.
[25] Maier T. “FMEA and FTA to support safe design of embedded software in safety critical systems,” *Proceeding of CRS 12th annual work shop on safety and reliability of software based systems*, pp. 351-367, 1997.
[26] Mil-std-1629a, military standard: *Procedures for Performing a Failure Mode Effects, and Criticality Analysis*, 1980.
[27] N. Snooke, C. Price, “Model-driven automated software FMEA,” *Proceeding of Reliability and Maintain ability Symposium (RAMS)*, pp. 1-6, 2011.
[28] G. Cassanelli, G. Mura, F. Fantini, M. Vanzi, B. Plano, "Failure Analysis-assisted FMEA," *Microelectronics Reliability*, Vol. 46, pp.1795-1799, 2006.
[29] SAE J1739, “Potential Failure Mode and Effects Analysis in Design (Design FMEA) and Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA) and Effects Analysis for Machinery (Machinery FMEA),” 2002.
[30] Kai Xu, Meilin Zhu, Maji Luo, “Turbo charger's Failure Mode Criticality Analysis Using Fuzzy Logic," *Society Automotive Engineers International*, 2000-01-1350, 2000.
[31] Benjamin S. Blanchard, Wolter J. Fabrycky, “Systems Engineering and Analysis (5th Edition),” *Prentice Hall*, pp. 386-390, 2010.
[32] Rajiv Kumar Sharma and Pooja Sharma, "System Failure Behavior and Maintenance Decision Making using, RCA, FMEA and FM," *Journal of Quality in Maintenance Engineering*, Vol. 16, No. 1, pp. 64-88, 2010.
[33] Hyo Young Kim and Hyuk Soo Han, "A Defect Prevention Model based on SW-FMEA," *Journal of the Korean Information Science Society*, Vol. 33, No. 7, pp. 605-614, 2006.
[34] Hyun Ki Park, "A study on methods of Fault Analysis and the Failure Effect Analysis for Security Improvement of e-Teaching and Learning System," *Ph.D. Dissertation, Pukyong National University*, 2012.
[35] Ik-Sung Lee, "A Study for Quality Improvement of Convention by Failure Mode and Effects Analysis," *Journal of the Korean Convention Society*, Vol. 5, No. 1, pp. 101-107, 2005.

[36] Joong-Soon Jang, "A Study on Performing FMEA Effectively," *Journal of the Korean Institute of Plant Engineering*, Vol. 4, No. 4, pp. 69-77, 1999.
[37] Joong-Soon Jang and Dong-Geun An, "How to Perform FMEA Effectively," *Journal of the Korean Society of Quality Management*, Vol. 25, No. 1, pp. 156-172, 1997.
[38] Adem Sabic, jasmin Azemovie, "Model 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.
[39] M. Ben-Daya and Abdul Raouf, "A Revised Failure Mode and Effects Analysis Model," *International Journal of Quality & Reliability Management*, Vol. 13, No. 1, pp. 43-47, 1996.
[40] N. Snooke and C. Price, "Model-driven Automated Software FMEA," *Proceedings of Reliability and Maintainability Symposium (RAMS)*, pp. 1-6, 2011.
[41] Rodrigo de Queiroz Souza and Alberto Jose Alvares, "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.
[42] Thomas Mailer, "FMEA and FTA to Support Safety Design of Embedded Software in Safety-Critical System," *Proceedings of CSR 12th Annual Workshop on Safety and Reliability of Software Based System*, pp. 351-367, 1997.
[43] Zhang Hong and Liu Binbin, "Integrated Analysis of Software FMEA and FTA," *Proceedings of International Conference on Information Technology and Computer Science*, pp. 184-187, 2009.
[44] 이용희, "기술경영의 관점에서 살펴본 모바일 지급결제의 의미와 금융기관의 대응전략," 금융결제원 지급결제와 정보기술, No. 48, pp. 84-112, 2012.
[45] 한국산업표준(KS), "모바일 지급결제 - 모바일 신용카드 - 제1부: 일반," 지식경제부 기술표준원, KSX6928-1, 2012.

감사의 글

2010년도 학부 동서대 경영정보학과로 편입을 하여 열심히 공부하여 제가 꿈에 그리던 부경대학교 대학원 정보처리시스템협동과정에 입학하여 훌륭하신 교수님들의 은덕으로 오늘에 이르렀습니다.

이런 영광을 있게 해주신 박만곤 지도교수님께 깊은 감사를 드립니다. 박만곤 교수님을 만난 것은 저에게 큰 행운이었습니다. 직장과 학업을 병행하다보니 부족한 점이 많이 있지만, 손수 자료를 찾아주시고 많은 도움과 격려 그리고 열정적으로 지도해 주신 지도교수 박만곤 교수님께 감사의 말씀을 전합니다. 공사다망하신 가운데도 저의 논문을 심사해 주신 김창수 교수님, 이경현 교수님 감사합니다.

그리고 포기하려고 할 때 옆에서 이끌어 주고 격려해주며 많은 도움과 조언을 해주셨던 서진호 선생님, 그리고 항상 든든하고 세세하게 문제를 짚어주며 도움을 주시고 항상 랩을 든든하게 지켜주시는 김민지 랩장님에게도 감사의 말씀을 드리고 싶습니다.

“꿈을 향하여”

저는 꼭 이루고 싶은 꿈이 있습니다. 지금 그 꿈을 이루기 위해 한발 한발 걸어가고 있습니다. 고지가 얼마 남지 않았습니다. 꼭 꿈을 이루어 부경대학교의 이름을 빛낼 것입니다.

마지막으로 저의 삶의 근원이자 항상 저의 그늘이 되어주시는 사랑하는 주귀분 어머니와 남택양 아버지에게 이 논문을 바칩니다.

2017. 2.

남 필 식