Research Report

RE-083

# 소프트웨어 안전 관리 프레임워크 연구

## A Study on SW Safety Management Framework

권영환 / 진회승 / 송지환

2020. 01.

SPRi 소프트웨어정책연구소

이 보고서는 2019년도 과학기술정보통신부 정보통신·방송연구개발사업의 연구결과로서 보고서 내용은 연구자의 견해이며, 과학기술정보통신부의 공식입장과 다를 수 있습니다.

연 구 기 관 : 소프트웨어정책연구소

과제책임자 : 권영환 선임연구원
참여연구원 : 진회승 책임연구원
송지환 선임연구원

# 목 차

# 표 목 차

# 그 림 목 차

# 요 약 문

## 1. 제 목

소프트웨어 안전 관리 프레임워크 연구

## 2. 연구 목적 및 필요성

자율자동차, 드론, AI 등 소프트웨어 기술 발전에 따라 소프트웨어의 복잡성이 증가하고 소프트웨어 편의성 증가로 많은 분야에서 소프트웨어 의존성이 증가하고 있다. 이로 인해 소프트웨어의 제어를 받는 시스템이 증가하게 되어서 소프트웨어 결함으로 인한 사고의 발생 확률이 증가하고 있다. 결국은 과거와 달리 소프트웨어 문제로 인해 발생하는 사고의 피해의 영향력도 같이 커지고 있기 때문에 소프트웨어 안전관리가 국민의 안전 확보에 중요한 요소가 되고 있다.

IEEE 1228 표준에 의하면 소프트웨어 안전이란 전체 시스템의 안전 보장을 위해 외부에 미치는 위험요소를 분석하고 제거하여 소프트웨어의 오류로 인한 사고를 예방하는 것을 의미한다[1]. 여기서 소프트웨어는 열차, 항공기, 발전소, 안전시설 등 주요 안전 분야에 사용하는 제어용 소프트웨어나 소프트웨어를 포함하는 시스템 뿐만 아니라 안전을 위해 사용하는 관련 소프트웨어를 모두 포함한다. 이러한 소프트웨어가 오류를 발생시키지 않도록 안전 활동을 수행하는 것이 국가적인 소프트웨어 안전 관리 활동이다. 4차 산업혁명으로 의해 소프트웨어가 우리의 삶과 직접적으로 연관될수록 안전관리 활동이 중요해지고 잘 작동되어야 국민의 재산과 신체의 안전을 확보할 수 있다.

따라서 본 연구의 목적은 미래 사회 안전 확보를 위해 소프트웨어 안전과 관련된 활동들을 정의하기 위한 프레임워크를 제시하는데 있다. 이를 위하여 소프트웨어 밀접하게 관련된 안전 관리 활동들을 조사하여 소프트웨어 안전 관리 프레임워크를 도출하고 이를 소프트웨어 안전 주요 분야의 안전 관리 활동들과 비교하여 소프트웨어 안전 관리 프레임워크를 검증하고 보완한다.

---

1) 소프트웨어정책연구소(2016), 『이슈리포트-자동차 산업의 SW안전 이슈와 해결 과제』, 제2016-016호, p7에 나온 내용을 인용한 것으로 표준은 IEEE 1228:1994 'IEEE Standard for Software Safety Plans'을 말함

### 3. 연구 구성과 내용

본 연구는 총 4장으로 구성되어 있다.

제 1장은 서론으로 소프트웨어 안전 관리 프레임워크 연구의 배경과 연구 방법을 설명하고 연구 내용에 대해 요약한다.

제 2장은 기존의 안전 관리에 대한 기본 체계를 분석하고 소프트웨어 관리 요소를 보완함으로써 소프트웨어 안전 관리 프레임워크(안)을 도출한다. 이를 위해 안전 관리의 기본 체계에 해당하는 재난안전법을 분석하여 예방-대비-대응-복구의 단계별로 안전 관리 활동들을 도출하였다. 그리고 대표적 소프트웨어 기반 시스템 관리 법인 정보통신망법과 대표적 데이터 관리 법인 개인정보보호법을 기반으로 소프트웨어 관리 활동들을 도출한다. 그리고 이들 세 가지 법들을 비교 분석하고 전문가 자문을 통해 소프트웨어 안전 관리 프레임워크(안)을 만들었다.

[소프트웨어 안전 관리 프레임워크(안)]


제 3장은 2장에서 만들어진 소프트웨어 안전 관리 프레임워크(안)을 검증한다. 검증을 위해 소프트웨어 안전 관리가 이루어지고 있는 중요 분야를 선정하여 해당 분야의 소프트웨어 안전 관리 활동들을 소프트웨어 안전 관리 프레임워크(안)을 가지고 조사를 수행한다.

프레임워크(안)의 활동들이 개별 분야에서 실행되는지를 조사하여 프레임워크의 보완 사항을 도출한다.

이를 위해 우선적으로 소프트웨어 안전 관리가 활발히 이루어지고 있는 분야 선정을 위해 전문가 설문 조사를 수행하였다. 먼저 SW안전과 관련있는 약 30여개의 안전 관련 법안 도출하고 이를 7개 분야(재난안전, 정보통신, 제품안전, 교통, 시설물, 에너지, 기타)로 분류하였다. 그리고 선정 기준으로 소프트웨어 사고 발생 빈도, 소프트웨어 사고 사회 파급력, 소프트웨어 관련성, 소프트웨어 안전 관리 시급성을 도출하였다. 이 기준들을 가지고 2번에 걸친 전문가 설문으로 소프트웨어 안전 관리 현황 조사를 수행할 세부 분야 선정로 자동차, 철도, 항공 분야가 선정되었다.

선정된 세부 분야들에 대한 소프트웨어 안전 관리 현황 조사를 소프트웨어 안전 관리 프레임워크(안)을 가지고 조사하였다. 조사 결과 대부분의 소프트웨어 안전 관리 활동들이 이루어지고 있었다. 또한 전문가 자문을 통해 소프트웨어 안전 관리 프레임워크(안)의 한계점인 재난안전 관리 체계와 SW안전 관리의 차이점을 도출하고 개별 활동들의 중요 고려 사항들을 파악하였다.

[개선된 SW안전 관리 프레임워크]


제 4장은 3장에서 수행한 소프트웨어 안전 관리 현황 조사 결과와 전문가 의견들을 가지고 소프트웨어 안전 관리 프레임워크(안)을 수정하여 최종적인 소프트웨어 안전 관리 프레임워크를 제시한다. 기본 안전관리 체계의 예방-대응-대비-복구 단계를 소프트웨어 안전관

리 측면에서 ① 인증단계, ② 운영단계, ③ 응급조치, ④ 사후관리로 보완하였다.

- 인증 단계 : 안전관리 대상 및 기준 정의, 안전 검사/인증, 자격 부여를 위한 시험/자격 획득, 위험평가를 수행하는 단계
- 운영 단계 : 안전 기준을 기반으로 안전 점검, 시스템 유지 및 점검 결과 공개, 이용자 보호, 사고 대응 매뉴얼/훈련 등을 수행하는 단계
- 응급 조치 : 사고 발생 시 신고, 사고에 대응
- 사후 관리 : 사고 조사, 사고 재발 방지, 손해 배상, 분쟁 조정 등

그리고 해외 안전 관리 개선 사례로 자율주행차 기술 발전을 위한 안전 기준의 개정 사례인 비엔나 협약 변경과 미국 캘리포니아의 제도 개선 사례를 소개하고 사고 재발 방지를 위한 미국과 호주의 교통안전 사고 조사 체계에 대해 소개한다.

마지막으로 제 4장은 결론으로 연구의 요약, 연구의 한계점 등에 대해 기술한다.

## 4. 정책적 활용 내용

본 연구는 미래 사회 안전 확보를 위해 소프트웨어 안전 관리 프레임워크를 제시한다. 4차 산업혁명 시대에는 소프트웨어 기반 자동화 기술이 널리 활용될 것이기에 안전 확보를 위핸 소프트웨어 안전 관리가 중요해지고 있다. 정부의 소프트웨어 안전 관리 체계 마련을 위한 정책을 개발할 때 본 연구 결과는 활용될 수 있다. 특히 소프트웨어 안전 관련 법 제도 정비와 소프트웨어 안전 관련 세부 정책 과제 도출에 기초 자료로 활용될 수 있다.

## 5. 기대효과

본 연구는 소프트웨어 안전 확보를 위한 정책 마련의 기초 자료로 활용될 것이기에 소프트웨어 중심의 미래 사회의 국가적 안전 역량 강화에 기여를 할 것이다. 이는 곧 국민들이 보다 안전한 미래를 누리를 수 있을 것이며 미래 신산업을 보다 위험 없이 맞이 할 수 있을 것으로 생각된다.

# SUMMARY

## 1. Title

A Study on SW Safety Management Framework

## 2. Study Purpose and Necessity

Software becomes more complicated because of the development of software technologies such as autonomous vehicles, drones, and AI, and many fields increase their software dependency due to increased software convenience. As a result, the number of software controlled systems increases and the probability of accident occurrence increases because of software defects. Eventually, unlike the past, the impact of accidents caused by software problems is also increasing, so software safety management becomes an important factor in securing public safety.

According to the IEEE 1228 standard, software safety means preventing accidents caused by software errors by analyzing and removing external risk factors to ensure the safety of the entire system. Here, the software includes not only a system including controlling software or used software in major safety fields such as trains, aircraft, power plants, and safety facilities, but also all related softwares used for safety. These are national software safety management activities to perform safety activities to ensure that such software does not cause errors. As the software is directly related to our lives by the 4th Industrial Revolution, software safety management activities become important and work well to ensure the safety of people's property and body.

Therefore, the purpose of this study is to present a framework for defining software safety activities to secure future social safety. To this end, a software safety management framework is proposed by examining safety management activities related to software, and the software safety management framework is verified and supplemented by comparing safety management activities in major software safety areas.

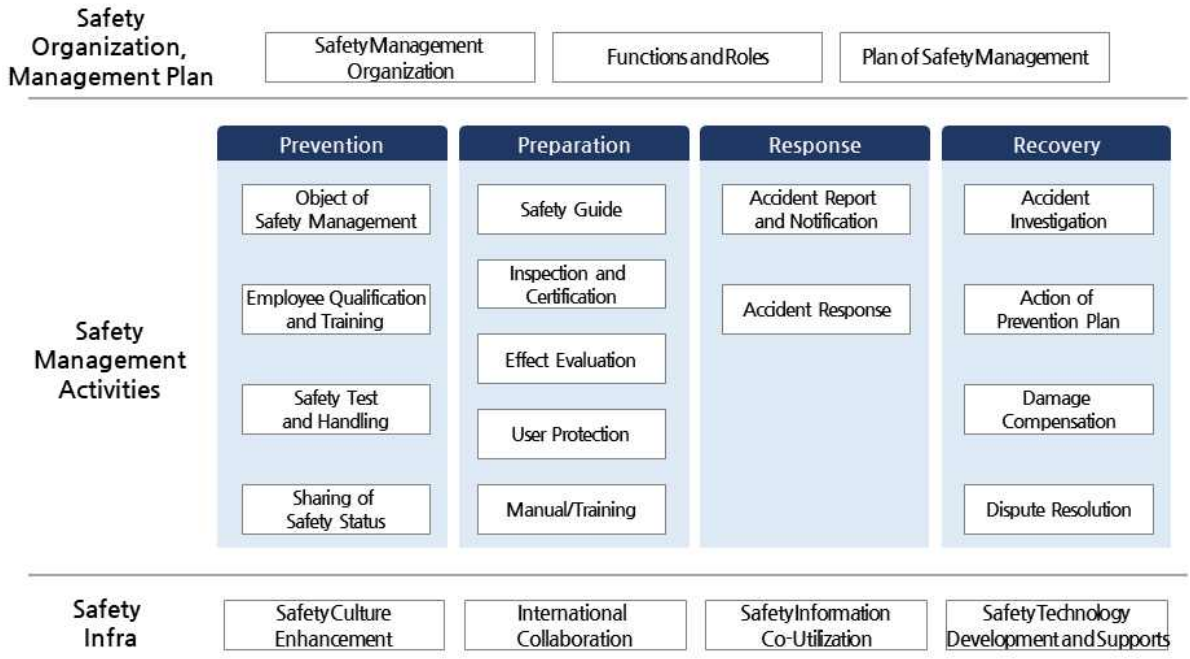
## 3. Study Composition and Contents

This study consists of 4 chapters.

Chapter 1 introduces the background and method of the software safety management framework study and summarizes the research contents.

Chapter 2 derives a software safety management framework proposal by analyzing the basic framework for existing safety management and supplementing software management elements. To do this, the Disaster Safety Law of the Republic of Korea, which is the basic safety management system, was analyzed to derive the safety management activities in each stage of prevention-preparation-response-recovery. In addition, software management activities are derived based on the representative software-based system management law, Information and Communication Network Law, and the representative data management law, Personal Information Protection Law. Then, a comparative analysis of these three laws and expert consultations resulted in a software safety management framework proposal.

[Software Safety Management Framework Proposal]



Chapter 3 verifies the software safety management framework proposal of Chapter 2. For verification, important fields of software safety management are selected, and software safety management activities in the fields are investigated with the software safety management framework proposal. Supplements of the framework are derived by investigating whether each activity of the framework is implemented in individual fields.

To do this, expert surveys were conducted in order to select a field in which software safety management is actively conducted. First, about 30 safety-related laws related to SW safety were drawn and classified into 7 fields (Disaster Safety, Information and Communications, Product Safety, Transportation, Facilities, Energy, Etc.). In addition, the frequency of software accidents, the social impact of software accidents, the software relevance, and the urgency of software safety management were derived as selection criteria. The automotive, rail, and aviation sectors were selected as detailed fields for conducting investigations on the status of software safety management through two expert surveys with these criteria.

The current status of software safety management for selected sub-fields was investigated based on the software safety management framework (proposal). As a result of this investigation, most software safety management activities were conducted. In addition, through the expert consultation, the difference between the disaster safety management system and software safety management, which is the limitation of the the derived software safety management framework proposal and important considerations of individual activities were identified.

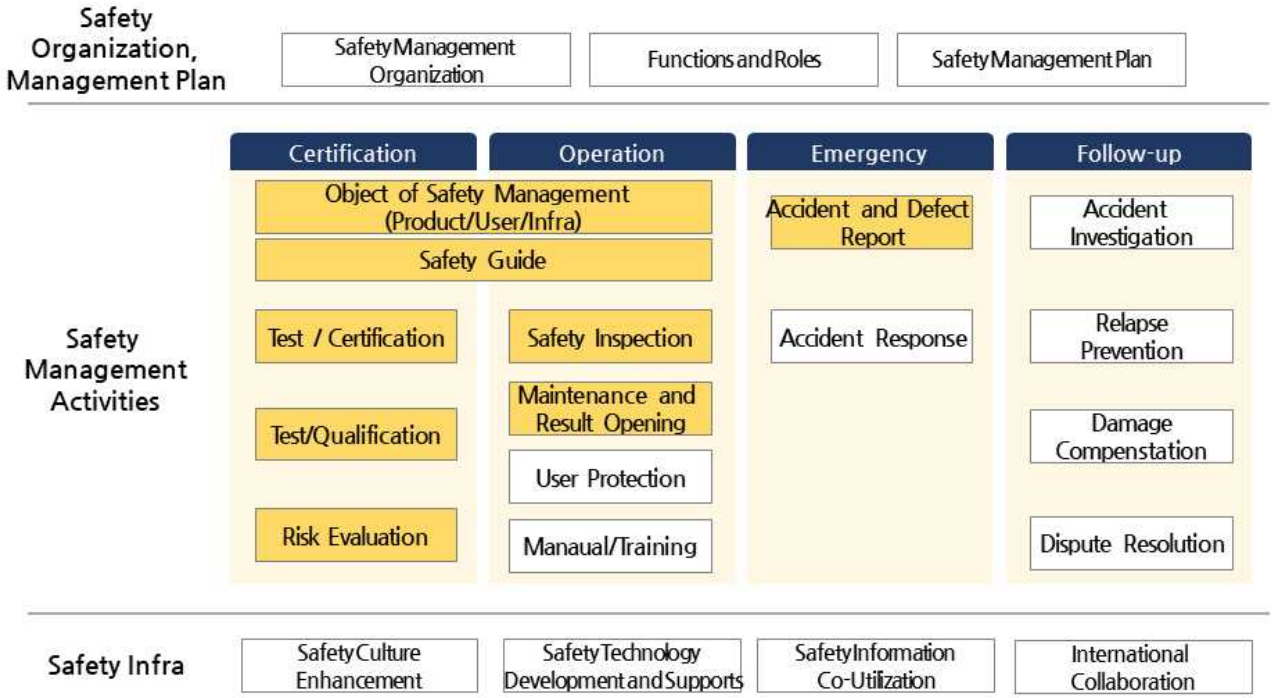
Chapter 4 presents the final software safety management framework by revising the software safety management framework proposal with the investigations of the software safety management conducted in Chapter 3 and expert opinions. The prevention-response-preparation-recovery phase of the basic safety management system was supplemented with ① Certification phase, ② Operation phase, ③ Emergency phase, and ④ Follow-up in terms of software management.

- Certification phase: defining the obejct of safety management, Safety Test/Certification, Test/Qualification, and Risk Evaluation
- Operational phase: Performing Safety Inspection, Safety Maintenance and Resual

Opening, User Protection, and Manual/Training based on Safety Guide

- Emergency: Accident and Damage Report, Accident Response
- Follow-up: Accident Investigation, Relapse Prevention, Damage Compensation, Dispute Resolution, etc.

[Enhanced Software Safety Management Framework]




In addition, as examples of overseas safety management improvement, the Vienna Convention revision and legal system change in California, USA are introduced to enhance the development of autonomous vehicle technology and then the traffic safety accident investigation system in the United States and Australia to prevent accidents from reoccurring do.

Finally, Chapter 4 describes the summary and the limitations of the study.

## 4. Policy utilization

This study proposes a software safety management framework to secure future social safety. In the era of the 4th Industrial Revolution, software-based automation technology will be widely used, so software safety management for securing safety is becoming more and more important. The results of this study can be used when developing policies for the government's software safety management system. In particular, it can be used as a basic reference for the maintenance of software safety-related legal systems and the deduction of detailed policy tasks related to software safety.

## 5. Expected effect

Since this study will be used as the basic reference for policy preparation to secure software safety, it will contribute to strengthening the national safety capacity of the software-oriented future society. It is expected that sooner or later, people will enjoy a safer future and will be able to meet new industries in the future without risk

# 제1장 서 론

## 제1절 연구 배경

소프트웨어(Software, SW)기술 발전으로 인해 SW에 대한 의존성과 복잡성이 점점 증가하고 있고 이에 따라 다양한 분야에서 SW 결함으로 인한 사고 발생 가능성도 같이 증가하고 있다. 또한, SW가 제어하는 분야가 늘어날수록 사고가 발생할 경우 사고의 사회·경제적 피해 규모도 크게 증가할 것으로 예상되고 있다. 예를 들어 과거에는 SW가 주로 사용되던 정보시스템에서 SW 문제가 발생할 경우 단순 데이터 손실에 그쳤지만 최근 등장하고 있는 자율주행차의 경우 인명의 손실까지 발생하고 있다.

더욱이 737 맥스의 추락 사고의 원인으로 MCAS(Maneuvering Characteristics Augmentation System)가 거론되고 있으며 이와 같은 SW 결함은 수백명의 사상자를 발생시킬 정도로 사고 피해가 커지고 있다. SW가 보다 많이 활용되고 확산되는 4차 산업 혁명 시대를 생각하면 SW 결함으로 유발되는 사고의 규모는 더욱 증가될 것으로 예상된다. 따라서 미래 사회는 안전한 SW를 어떻게 확보할 것인가가 국민 안전 확보에 중요한 요소가 되고 있다.

하지만, 아직까지는 특정 분야를 제외하면 SW안전 관리에 대한 고려가 많지 않은 상태이다. 기존 안전 관리 연구는 주로 자연 재해 및 재난 관점의 안전 관리에 대해 주로 연구하였으며 그리고 SW 보다는 하드웨어(Hardware, HW) 중심의 연구가 진행되어 왔다. 국내 최초의 SW안전 관련 정책 연구인 2016년도에 진행된 소프트웨어정책연구소의 소프트웨어 안전 관리 관점에서의 기반시설 보호 법제 개선 연구[2]는 하드웨어 중심의 국가 기반시설에 대한 SW안전 관리를 재난 관점의 안전 관리 프레임워크를 통해 연구를 수행하였다.

하지만 SW안전 관리는 정적인 HW 중심의 안전 관리와 다른 동적인 특성을 가지고 있기 때문에 재난 관점의 안전 관리 체계와 다른 면을 고려해 볼 필요가 있다. 더욱이 SW 확산으로 인하여 향후 예상되는 SW 중심의 안전 관리에 대한 연구의 필요성이 제기됨에 따라 본 보고서는 미래 사회 안전 확보를 위한 SW안전 관리를 위한 범용적인

2) 소프트웨어정책연구소(2016), 『소프트웨어 안전 관리 관점에서의 기반시설 보호 법제 개선 연구』

프레임워크에 대한 연구를 수행하게 되었다. 이를 위해 본 보고서는 우선 국내 주요 안전 관련 분야의 안전 관리 체계와 기존 SW안전 관리 현황을 조사하여 한계점을 분석하고 안전 선진국의 SW안전 관리 사례를 조사하였다. 그리고 조사된 내용을 기반으로 미래 사회 안전 확보를 위한 SW안전 관리 프레임워크를 제시한다.

## 제2절 연구 방법 및 내용

본 연구를 수행하기 위해 연구 방법과 내용은 다음과 같다.

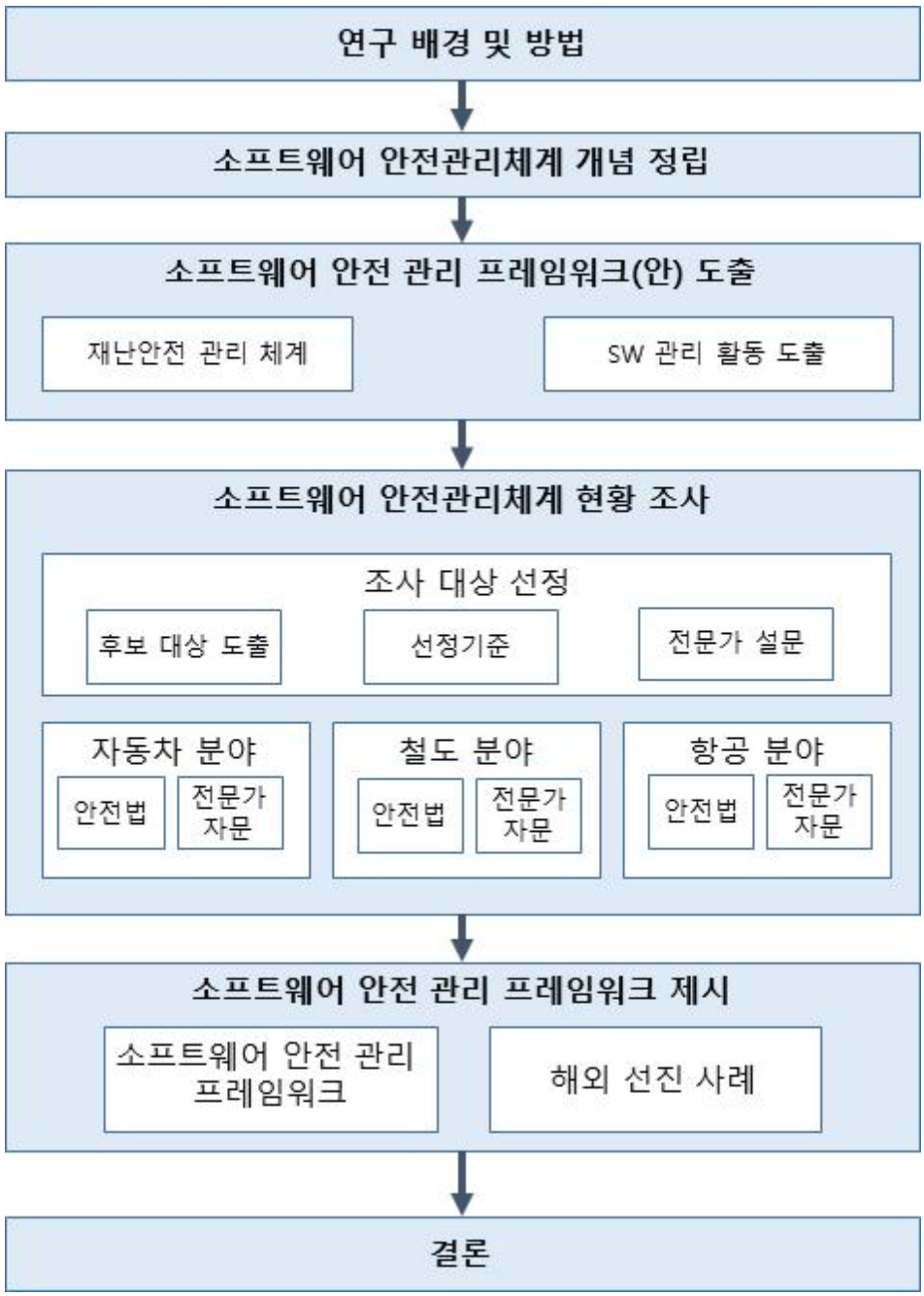
우선 SW안전 관리 프레임워크(안)을 도출한다. 해당 프레임워크(안)은 기존 연구와 같이 안전 관리의 기본 체계라고 할 수 있는 재난안전법의 안전 관리 체계를 기본으로 한다. 그리고 SW 관리 항목들을 추가하기 위해 정보통신망법과 개인정보보호법의 분석한다. 그리고 3가지 법을 비교 분석해서 SW안전 관리 프레임워크(안)을 설계하였다.

그리고 설계된 SW안전 관리 프레임워크를 검증하였다. 이를 위해 SW안전 관리가 수행되고 있는 주요 분야를 선정하여 SW안전 관리 프레임워크(안)을 기반으로 안전 관리 현황을 조사하였다. 주요 분야 선정을 위해서 30여개의 법안들로 대상 후보를 도출하고 4가지 선정 기준을 가지고 전문가 설문을 통해 자동차, 철도, 항공 분야를 선정하여 SW안전 관리 현황을 조사하였다.

조사된 결과를 기반으로 프레임워크(안)을 보완하여 제시할 SW안전 관리 프레임워크(안)의 실용성을 확인하고 개선 사항을 도출하여 최종적인 SW안전 관리 프레임워크를 제시하였다. 그리고 SW안전 관리에 대한 주요 시사점을 도출하기 위해 해외의 SW안전 관리 개선 사례들로 신기술 활성화를 위한 제도 개선과 안전사고 원인 조사 선진 사례들을 조사하였다.

[그림 1]은 본 연구 방법 및 내용에 대한 요약이다.

[그림 1] SW안전 관리 프레임워크 연구 방법 및 내용



# 제2장 소프트웨어 안전 관리 프레임워크(안) 설계

## 제1절 소프트웨어 안전 관리 개요

### 1. 소프트웨어 안전(SW Safety) 개념

소프트웨어 분야의 외연은 지속적으로 확장되면서 더욱 중요해지고 있다. 더욱이 4차 산업혁명의 주요 기술 분야로 떠오른 모바일 컴퓨팅, 슈퍼컴퓨터, 사물인터넷, 자율주행 자동차, 빅데이터, 인공지능, 로봇, 블록체인, 3D프린터 등은 소프트웨어가 핵심 요소가 되어 기술 발전이 가속화되고 있다.

대표 사례로 과거 자동차는 기계장치로 구성되어 사람의 이동과 사람에게 필요한 물품들의 운송을 편하게 해주면서 중요한 산업으로 성장하였다. 전자 기술의 발전으로 인해 자동차는 더 이상 단순 기계 장치에 머물지 않고 전자 기술을 활용한 장치와 제어 장치를 포함하게 되면서 인류의 삶에 없어서는 안 될 물품으로 진화되었다. 최근 인공지능을 포함한 ITS(Information Telematics System) 등의 첨단 IT 시스템의 개발은 자동차 산업에서 SW 영향력이 지속적으로 확장되고 있음을 나타낸다.

결국 자동차에서 SW 원가 비중은 의료기기(40.9%)보다 높아졌으며 스마트폰(54.3%)과 비슷한 52.4%에 이르게 되었다. 최신 최고급 자동차는 70개 이상의 ECU(Electric Control Unit)를 내장하고 있으며 SW 코드가 점점 많아지면서 자동차에 포함된 SW 코드는 1억 라인을 넘어가게 되었다[3]. 이와 같은 SW 코드 증가는 SW 복잡도를 증가시키게 되어 SW 결함으로 자동차 사고 발생 가능성이 커져가고 있다. 자동차의 SW 결함을 해결하기 위한 자동차 리콜이 최근 증가하고 있다. 과거 도요타 급발진 사고는 사소한 SW의 오류로 인한 차량 엔진 오작동으로 인한 사고로 밝혀졌고 이로 인한 전 세계에서의 리콜이 실시되었다.

항공 분야에서도 항공 기술의 발전으로 항공기 속도의 증가와 경제성 확보를 위한 기체 대형화로 인하여 항공기를 제어하기 위한 다양한 항공 소프트웨어가 많이 도입되고 있다. 1960년대 개발된 F-4 팬텀 전투기는 SW 비중은 8%에 불과했지만 최신 전투기인 F-35의 SW 비중은 90%에 이를 정도로 크게 증가하였다. 그 결과 최신 항공기

3) 임베디드소프트웨어협회(2016), 차량용 SW의 현황과 발전 방향

개발비에서 SW가 차지하는 비중은 전체 개발비의 50%, 항공기 가격의 40%를 차지할 정도로 항공 분야에서 SW의 중요성을 크게 증가하였다.[4)]

〈표 1〉 대표 소프트웨어 안전사고 사례

| | |
|---|---|
|  Therac25 사용 환자사망(~ '87) | • 방사선 치료기인 Therac 25가 오류로 방사능 과다 투여<br>• 턴테이블(X-ray 균일 분사기능)을 작동하는 플래그 데이터가 8비트로 변화되며 생기는 오버 플로우 상태에서 작동키를 누를 경우 오작동<br>• 3명 사망, 3명은 심각한 방사능 후유증에 시달림 |
|  Arian5 우주선 폭발( '96) | • 유럽연합의 상용 우주선 Arian5가 발사 후 공중 폭발<br>• 64비트 정수를 16비트 정수로 변환하는 SW 오류가 발생<br>• 5억 달러 피해 금액 발생 |
|  도요타 자동차 급발진( '09) | • 도요타 렉서스 자동차가 ECU 메모리를 SW간 공유하면서 생기는 간섭 현상으로 195km/h 속도로 급발진 발생<br>• 일가족(4명) 사망<br>• 벌금 1조 3천억원 부과, 900만대 리콜 |
|  재해경보시스템 오동작 야영객 사망( '09) | • 북한 황강댐의 급작스런 유량 방출로 임진강 부근 수위 급상승<br>• 경보 방송을 담당하는 경보국과 경보제어 시스템 서버 간 통신 SW 오류발생으로 경보 시스템이 오동작<br>• 부근 야영객·낚시객 6명 급류에 휩쓸려 사망 |
|  서울지하철 추돌사고( '14) | • 신당역에서 상왕십리역으로 들어오던 열차가 상왕십리역을 출발하려던 열차를 추돌<br>• 신호기 고장으로 후속 열차 ATS(자동정지장치) 미작동<br>• 승객 등 250여명 중경상 |
|  신호등 오작동으로 정면충돌( '17) | • 삼천포 대교에 위치한 가변차로 신호등 오작동으로 차량 2대가 정면 충돌<br>• SW 오류로 인해 신호등 제어시스템 문제 발생 추측<br>• 운전자 2명 중상 |
|  열차 신호설비SW 오작동( '17) | • 경의중앙선 시운전 열차 추돌 (양평역과 원덕역 사이)<br>• 신호 설비인 모듈에 잘못된 SW 설치<br>• 기관사 사망, 신호수 등 6명이 중경상<br>• 열차 2대 파손으로 68억 3000만원의 물적 피해 |
|  자율주행차 보행자 사망( '18) | • 우버의 자율주행차가 자율모드로 주행 중 보행자와 충돌하여 보행자 사망<br>• 횡단보도 바깥쪽으로 보행자가 건너는 상황에서 주의를 필요로 하지 않은 구역으로 인식했을 것으로 추정 |

출처 : 정보통산산업진흥원(2019), SW 안전 국제표준화 동향과 시사점

4) https://post.naver.com/viewer/postView.nhn?volumeNo=11275372&memberNo=38486222 (한국방위산업진흥회)

이와 같은 SW 활용의 증가로 인하여 SW가 미치는 영향력은 크게 증가하였으며, SW 복잡도 증가로 인하여 결함 없는 SW 구현은 더욱 어려워지게 되었다. 결과적으로 결함 있는 SW로 인하여 사고 발생 가능성을 증가시키게 되었다. <표 1>은 대표적인 SW 안전 사고 사례를 보여준다. 이와 같이 만약 SW로 인한 사고가 발생할 경우 막대한 생명·재산 피해가 발생할 수 있으며 이를 미리 방지하고 예방하기 위한 안전 이슈가 부각되었고 SW와 관련된 안전 확보를 위한 노력이 필요하게 되었다.

사전적 의미로 안전(Safety)은 "위험이 생기거나 사고가 날 염려가 없이 편안하고 온전한 상태"를 의미하며 안전 교육의 창시자인 호온은 안전은 넓은 의미에서 "삶의 전부"이며, 좁은 의미에서 "사고를 방지하는 것을 포함하는 신체적 삶의 전부"로 정의하였다.[5] 국제 안전 규격을 위한 가이드인 ISO/IEC GUIDE51[6]는 안전을 "수용할 수 없는 위험이 없는 것(freedom from unacceptable risk)"로 정의하였다. 이를 다시 해석하면 "재난이나 사고의 위험으로부터 허용 가능한 수준으로 통제되어 있는 상태"라고 할 수 있다.

그러므로 SW안전은 "소프트웨어로 인하여 위험이 생기거나 사고가 날 염려가 없이 편안하고 안전한 상태"를 의미하며, "소프트웨어로 인한 수용할 수 없는 위험이 없는 것"으로 구체화 할 수 있다. IEEE(미국 전기·전자 통신 학회) STD 1228-1994는 SW안전을 "전체 시스템의 안전 보장을 위해 외부에 미치는 위험요소를 분석하고 제거하여 SW 오류로 인한 사고를 예방하는 것"으로 정의하고 있다. 즉, SW안전은 단순히 오류에 의한 사고를 예방함과 함께 사람의 신체나 생명 사고를 발생시킬 가능성이 있는 SW에 대해 여러 위험 요인을 방지하고 충분한 대비가 되어 있는 상태라고 할 수 있다.

사고를 일으킬 수 있는 결함, 고장, 위험원에 영향을 미치는 SW 관련 항목들은 2010년 발간한 NASA(National Aeronautics and Space Administration)의 System Safety Handbook에서 <표 2>같이 정리하였다. 해당 SW 오류나 결함들이 [그림 2]처럼 시스템 결함과 고장으로 이어지고 결국은 위험원으로 작용해 사고를 일으켜 생명과 재산의 손실을 가져오게 된다고 할 수 있다. 따라서 이러한 요인들을 얼마나 잘 관리하여 SW로 인한 결함, 고장, 위험원을 사전에 예방하고 발견시 해결하기 위한 대응 활동들이 중요하다.

---

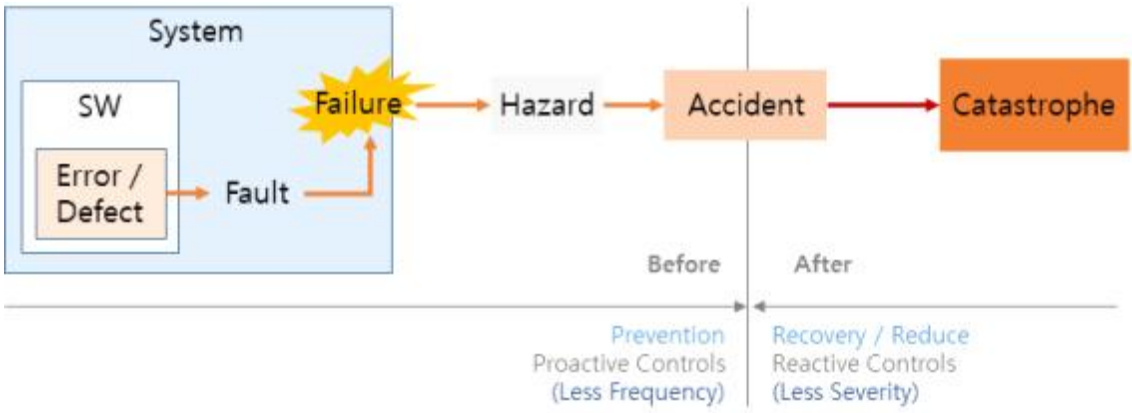
5) 국민안전교육 표준매뉴얼-재난 및 안전사고 이해, 2017, 중앙소방본부
6) ISO/IEC Guide 51 (2014), "Safety aspects - Guidelines for their inclusion in standards"

<표 2> 결함, 고장, 위험원에 대한 SW의 영향(NASA)

| 구분 | 내용(예) |
|---|---|
| I. 이벤트/액션 | 이벤트 미발생/액션 미동작, 잘못된 모드나 상태에서 이벤트발생/액션 실행 의도하지 않은 순서로 이벤트발생/액션 실행, 잘못된 에러 、예외처리 |
| II. 로직/알고리즘 오동작 | Zero로 나누기, 사용하지 않는 코드(Dead Code), 유효 파라미터 및 경계값 체크 누락, 무한 루프, Case/Type 미일치, 잘못된 if then 혹은 else 구문 처리, 외부 입력 데이터 및 파일에 대한 체크 누락 |
| III. 통신 및 입출력 | 통신채널 과부하, 데이터 손상, 명령어 송수신 실패 |
| IV. 타이밍 | 데이터 지연 또는 데이터 경과(Aging), 제한된 시간 내 프로세스 종료/완료, 실패 데이터 경합 |
| V. 사용자 오류/사용자 인터페이스 오류 | 사용자의 잘못된 명령 혹은 명령 누락, 부적절한 순서나 타이밍에 사용자 명령 시스템 상태, 메시지 등 표시 실패, 부정확한 메시지 표시 |
| VI. 그 외 | 시스템 리셋, 메모리 오버로드, 메모리 Deadlock, 메모리 데이터 변질 |

출처 : NASA System Safety Handbook - volume1, 2010

[그림 2] 소프트웨어 오류 및 결함이 사고로 이어지는 과정




## 2. 소프트웨어 안전 관리 개요

앞에서 언급된 SW로 인한 결함, 고장, 위험원을 사전 또는 발견시 해결하여 발생 가능한 사고를 사전에 예방하고 재발을 방지하는 위한 활동들은 SW안전 관리 활동으로

볼 수 있다. 다시 말해 SW가 활용된 기차, 항공기, 발전소 등 사고가 발생했을 때 피해가 예상되는 분야에서 SW 안전성이 확보되어 피해가 발생될 가능성이 낮도록 하기 위한 관리 활동들이 필요하고 이러한 관리 활동들은 결국은 국민의 생명을 보존하고 안전을 확보하기 위해 반드시 수행되어야 하는 활동들이다.[7)]

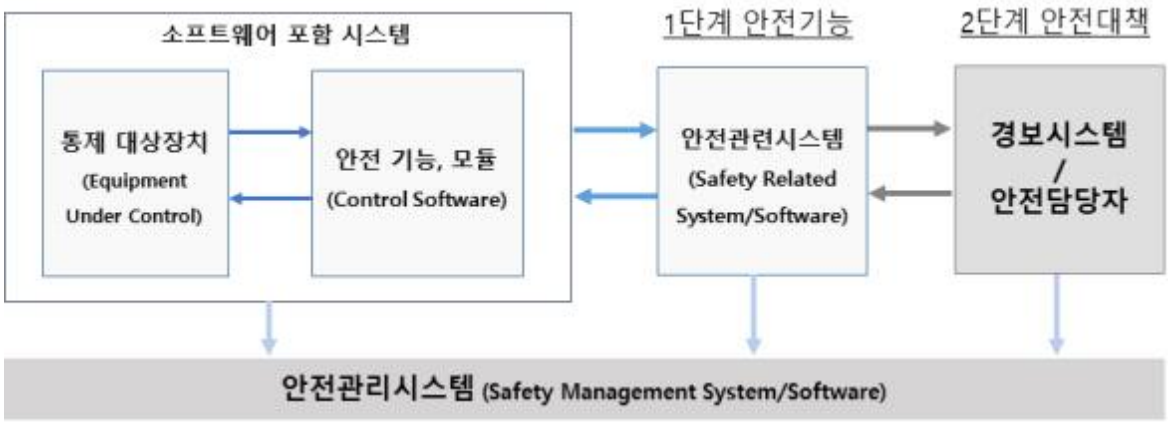
이를 기술적인 관점에서 보면 크게 직접 안전, 기능 안전, 간접 안전으로 구분할 수 있다. 직접 안전은 화재, 감전과 같은 직접 사고를 유발할 수 있는 안전을 의미한다. 기능 안전은 위험성 평가 결과에 따라 시스템 설계 및 구축 과정에 위험원을 미리 제거하기 위해 추가된 기능적인 동작을 말한다. 간접 안전은 데이터베이스 오류 같이 잘못된 데이터로 발생할 수 있는 안전을 의미한다[8)].

[그림 3]에 의하면 직접 안전은 통제 대상 장치에서 직접적으로 사고를 발생시킬 수 있는 것을 의미한다. 통제 대상 장치의 위험성 평가 결과 후에 위험 요인을 기능적으로 해결하기 위한 것을 기능 안전 또는 안전 기능이라고 할 수 있다. 통제 대상 장치에서 관리되는 데이터 값을 오류로 인해서 발생할 수 있는 사고를 간접 안전이라고 할 수 있다. 또한 SW 외부에도 추가적인 안전 관련 시스템을 구축하여 안전을 강화할 수 있으며 안전 관련 시스템 또는 경보 시스템을 통해 인위적인 관리를 추가할 수 있다. 이와 같이 시스템 안전을 확보하기 위해서는 직접 안전, 기능 안전, 간접 안전을 포함한 인위적인 활동들에 대한 종합적인 고려가 있어야 하고 이에 대한 관리가 반드시 필요하다.

7) 재난 및 안전관리 기본법 제 3 조

8) Smith, David J. and Simpson, Kenneth G. L. (2004), “Functional Safety(A Straightforward Guide to Applying IEC 61508 and Related Standards)“, Hutterwirth-Heinemann

[그림 3] 소프트웨어 포함 시스템, 안전기능, 안전대책, 및 안전관리시스템




<표 3>은 SW를 활용한 대표적 안전 기능들을 보여준다.

<표 3> SW를 이용한 대표적 안전 기능들

| 유형 | 설명 |
|---|---|
| 결함 감지 및 진단 | - 내·외부적 수단을 통해 시스템 상태를 체크하여 비정상 상태를 감지 |
| 모니터링 | - Input/Output 데이터, 관련 모듈의 동작 상태, 프로시저 등을 모니터링하여 시스템 이상 상태 감시 |
| 방어적 프로그래밍 | - 프로그램 오류 발생을 대비해 방어코드 추가<br>예: 입출력범위 체크, 제어흐름 체크 |
| 복수의 기능 배치 | - 기능적으로 동일한 복수의 기능을 배치하고 수행결과를 비교하여 오류를 감지 (N-Version Programming) |
| 정지 | - 오류 감시 시 기능을 제한적으로 수행하고 점진적으로 기능을 정지하는 조치 방법 |
| 리셋 | - 시스템 오류 발생 시 시스템을 Reset하여 복구하는 방법<br>예: Watchdog를 이용하여 프로세스 종료, 시스템 무응답 상태 등을 확인하고 Reset을 통해 복구 |
| 정적 복구 | - 오류 발생 시, 사전에 준비된 계획에 따라 복구<br>예:RecoveryBlock,BackwardRecovery,ForwardRecovery등 |
| 동기화 | - 기능적으로 동일한 복수의 기능이 존재하는 경우 오류 방지를 위해 기능 간 데이터 동기화 |
| 타임아웃 | - Watchdog 등을 이용하여 시스템 무응답 또는 무한루프 등 이상 상태를 파악 |

출처 : ISO 26262:2011 Road vehicles - Functional safety

안전 관리는 시스템 안전을 확보하기 위한 노력만이 아니라 이를 제공하기 위한 제반 법규정, 안전 기준, 절차 등을 포함한 전반적인 안전 활동들이 포함하고 이를 안전 관리 체계라고 할 수 있다. 이에 이러한 활동을 위한 조직과 역할. 인력 관리 등을 모두 포함될 수 있다. 그리고 SW 역할이 중요짐에 따라 SW안전 관리의 중요성이 더욱 중요해지고 있다.

## 3. 재난 및 안전 관리 체계

SW안전 관리 연구를 위해서는 기존 안전 관리 활동의 필요성과 당위성에 대한 이해가 필요하다. 그래서 안전 관리의 기본 체계인 재난 및 안전관리 기본법’ 의 주요 용어들을 기반으로 SW안전 관리에 대한 기본 용어를 정의한다.

재난 및 안전관리기본법 제3조에서 재난은 “국민의 생명・신체・재산과 국가에 피해를 주거나 줄 수 있는 것”으로 자연재난과 사회재난으로 구분하고 있다. 자연재난은 태풍, 홍수, 호우, 강풍, 풍랑, 해일, 대설, 낙뢰, 가뭄, 지진, 황사, 조류 대발생, 조수, 및 이에 준하는 자연현상으로 인하여 발생하는 자연 현상으로 인한 재난을 의미하며, 사회재난은 화재・붕괴・폭발・교통사고・화생방사고・환경오염사고 등 인간 활동으로 인해 발생하는 특정 규모 이상의 피해와 에너지・통신・교통・금융・의료・수도 등 국가 기반체계의 마비, 감염병 또는 가축 전염병의 확산 등으로 인한 피해가 발생하는 것을 의미한다.

따라서 재난 관리는 재난의 예방・대비・대응 및 복구를 위하여 하는 모든 활동을 말하며, 안전 관리는 재난이나 그 밖의 각종 사고로부터 사람의 생명・신체 및 재산의 안전을 확보하기 위하여 하는 모든 활동을 말한다. SW안전 관리도 사람의 생명, 신체 또는 재산의 안전을 확보하기 위해 SW를 관리하는 모든 활동으로 정의할 수 있다.

오늘날 많은 나라와 기관들에서 활용되는 재난 안전 관리의 활동과 목표는 총체적 재난 관리 모형(Comprehensive Emergency Management Model, CEM)에 기반하고 있다.[9] 페탁(Willian J. Petak)은 재난 관리 과정을 재난 발생 시점이나 관리시기를 기준으로 ① 완화와 예방(Mitigation and Prevention) ② 대비와 계획(Preparedness and Planning) ③ 대응(Response) ④ 복구(Recovery)의 4단계로 구분하고 있다. 이에 대한

9) Waugh, William L (1994). regionalizing emergency management: Counties as state and Local Government. Public Administration Review, 54(3): 253-258.

요약은 <표 4>로 대체한다.

<표 4> 예방 대비 대응 복구 단계에 대한 설명

| 구분 | 예 방 | 대 비 | 대 응 | 복 구 |
|---|---|---|---|---|
| 개념 | • 재난 발생 요인 제거 및 억제를 위한 장기적 예방 활동 | • 재난에 대한 직접적 대비를 위한 준비 행위 | • 재난 발생에 대한 피해 최소화를 위한 실제적 대응 활동 | • 이전 상태로의 복구를 위한 지속적 활동 |
| 주요 업무 | • 각종 시설 및 재난 유형과 취약 요인 분석<br>• 재난 기준 검토 및 정비<br>• 재난 유발 요인 제거 및 위험 노출 감소를 위한 관리 | • 재난 정보 공유 및 경보 체계 구축<br>• 재난 종류별 사전 대비 교육 및 훈련<br>• 관련 기관 협조 체계 구축 및 조정<br>• 비상 방송 및 근무 태세 유지<br>• 재난 대응 자원 사전 확보 | • 재난 현장 정보 공유<br>• 재난 관리 계획 실행<br>• 대응 기관들의 일원화된 체계 유지<br>• 피해자 대피를 포함한 보호 및 관리<br>• 현장 수습/관리 | • 복구 우선순위 설정, 예산 확보 등의 복구 계획 수립<br>• 단기 및 장기 복구 활동 시행<br>• 피해상황 파악/긴급 지원<br>• 발생원인 분석/평가/개선 |
| 비고 | 완화 (mitigation & prevention) | 준비 (preparedness) | 대응 (response) | 복구 (recovery) |

이와 같이 재난 안전 관리의 모든 단계는 상호 연관되어 있으며 각 단계별 활동이 다음 단계의 활동에 영향을 미치고 있다. 사전에 예방 활동을 얼마나 효율적으로 하였는가가 대비 활동에 영향을 주고, 효과적인 대비 활동은 재난 사고의 규모에 영향을 주기 때문에 바로 재난 대응 활동과 연관이 되며 효과적인 재난 대응은 이후 복구 활동 수행에 지대한 영향을 주게 된다. 이와 같이 SW안전 관리 활동도 하나의 관리 프레임워크 안에서 효율적인 상호 연계가 되어 있다.

## 제2절 소프트웨어 안전 관리 프레임워크(안)

SW안전 관리 현황 조사를 수행함에 앞서 프레임워크(안)을 도출하기 위해 재난 및 안전 관리 기본법(이하, 재난안전법)을 분석하여 안전 관리를 위한 기본 체계를 도출했다. 재난 및 안전관리 기본법은 2004년에 만들어져 지속적인 개정을 통해 안전 관리를 위한 기본 체계를 보완해 오고 있는 검증된 체계이다. 따라서 2016년에 수행하였던 시설물을 대상으로 SW 안전 관리 연구에서도 활용되었다.

하지만, 본 연구에서는 SW 관리 요소를 추가로 고려하기 위해 SW 기반 시스템 관리를 위해 만들어진 정보통신망 이용 촉진 및 정보보호법(이하, 정보통신망법)과 개인정보 관리를 위해 만들어진 개인정보보호법을 재난안전법의 기본 체계 내에서 분석하였다. 그리고 해당 분석 결과를 재난안전법과 비교 분석하여 SW 관리 요소가 추가된 안전 관리 프레임워크(안)를 도출하고자 한다.

[그림 4] 소프트웨어 안전 관리 현황 조사를 위한 프레임워크 도출 방법


### 1. 프레임워크(안) 수립을 위한 관련 법률 분석

프레임워크(안)은 기본 체계 도출을 위해 우선적으로 재난안전법을 분석하였다. 재난안전법은 <표 5>와 같이 구성되어 있고 안전 관리 활동들은 안전 관리의 기본 체계인 예방-대비-대응-복구로 구분되어 있다. 그리고 이들 활동들을 수행하기 위한 안전 관리 기구 및 기능을 정의하고, 관리 계획 수립 절차에 대해 정의하며, 안전 문화 확산을 위한 진흥 및 기금 등의 안전 기반 확보를 위한 활동들로 크게 구분되어 있다. 즉, 재난안전법의 안전 관리 체계는 크게 기구 및 관리계획 분야, 안전 활동 분야, 기반

조성 분야로 나누어져 있다고 할 수 있다.

〈표 5〉 재난 및 안전관리 기본법의 구성

| 분야 | 세부 활동 | 해당 법조항 |
|---|---|---|
| 기구 및 관리 계획 | 안전관리 기구 | 제9조 중앙안전관리위원회 |
| | | 제10조 안전정책조정위원회 |
| | | 제11조 지역위원회 |
| | | 제12조 재난방송협의회 |
| | | 제12조의2 안전관리민관협력위원회 |
| | | 제12조의3 중앙민관협력위원회의 기능 등 |
| | | 제14조 중앙재난안전대책본부 |
| | | 제16조 지역재난안전대책본부 |
| | 조직 역할 정의 | 제25조의2 재난관리책임기관의 장의 재난예방조치 등 |
| | | 제28조 지방자치단체에 대한 지원 등 |
| | | 제32조의2 사법경찰권 |
| | | 제75조 안전관리자문단의 구성·운영 |
| | | 제76조의2 안전책임관 |
| | | 제77조 재난관리 의무 위반에 대한 징계 요구 등 |
| | | 제78조 권한의 위임 및 위탁 |
| | 안전관리 계획 | 제22조 국가안전관리기본계획의 수립 등 |
| | | 제23조 집행계획 |
| | | 제23조의2 국가안전관리기본계획 등과의 연계 |
| | | 제24조 시·도안전관리계획의 수립 |
| | | 제25조 시·군·구안전관리계획의 수립 |
| 안전활동-재난의 예방(4장) | 관리대상지정 | 제26조 국가기반시설의 지정 등 |
| | | 제26조의2 국가기반시설의 관리 등 |
| | | 제27조 특정관리대상지역의 지정 및 관리 등 |
| | | 제29조 재난방지시설의 관리 |
| | 담당자 교육 | 제29조의2 재난안전분야 종사자 교육 |
| | 안전점검 | 제30조 재난예방을 위한 긴급안전점검 등 |
| | | 제32조 정부합동 안전 점검 |
| | | 제33조의2 재난관리체계 등에 대한 평가 등 |
| | 안전조치 | 제31조 재난예방을 위한 안전조치 |
| | 실태조사결과공개 | 제33조 안전관리전문기관에 대한 자료요구 등 |
| | | 제33조의3 재난관리 실태 공시 등 |
| 안전활동-재난의 대비(5장) | 재난 관리자원 비축 | 제34조 재난관리자원의 비축·관리 |
| | | 제34조의2 재난현장 긴급통신수단의 마련 |
| | | 제34조의8 재난안전통신망의 구축·운영 |
| | 관리기준 수립 | 제34조의3 국가재난관리기준의 제정·운용 등 |
| | | 제34조의7 안전기준의 등록 및 심의 등 |
| | 매뉴얼 | 제34조의4 기능별 재난대응 활동계획의 작성·활용 |
| | | 제34조의5 재난분야 위기관리 매뉴얼 작성·운용 |
| | 대비훈련 | 제34조의6 다중이용시설 등의 위기상황 매뉴얼 작성·관리 및 훈련 |
| | | 제34조의9 재난대비훈련 기본계획 수립 |

| | | |
|---|---|---|
| | | 제35조 재난대비훈련 실시 |
| 안전활동-재난의 대응(6장) | 사고인지및전파 | 제36조 재난사태 선포 |
| | | 제38조 위기경보의 발령 등 |
| | | 제38조의2 재난 예보·경보체계 구축·운영 등 |
| | 응급조치, 대피 및 동원 | 제37조 응급조치 |
| | | 제39조 동원명령 등 |
| | | 제40조 대피명령 |
| | | 제41조 위험구역의 설정 |
| | | 제42조 강제대피조치 |
| | | 제43조 통행제한 등 |
| | | 제44조 응원 |
| | | 제45조 응급부담 |
| | | 제46조 시·도지사가 실시하는 응급조치 등 |
| | | 제47조 재난관리책임기관의 장의 응급조치 |
| | | 제48조 지역통제단장의 응급조치 등 |
| | 긴급구조 | 제49조 중앙긴급구조통제단 |
| | | 제50조 지역긴급구조통제단 |
| | | 제51조 긴급구조 |
| | | 제52조 긴급구조 현장지휘 |
| | | 제52조의2 긴급대응협력관 |
| | | 제53조 긴급구조활동에 대한 평가 |
| | | 제54조 긴급구조대응계획의 수립 |
| | | 제54조의2 긴급구조 관련 특수번호 전화서비스의 통합·연계 |
| | | 제55조 재난대비능력 보강 |
| | | 제55조의2 긴급구조지원기관의 능력에 대한 평가 |
| | | 제56조 해상에서의 긴급구조 |
| | | 제57조 항공기 등 조난사고 시의 긴급구조 등 |
| 안전활동-재난의 복구(7장) | 신고및조사 | 제58조 재난피해 신고 및 조사 |
| | | 제69조 재난원인조사 |
| | | 제70조 재난상황의 기록 관리 |
| | 복구계획수립 및 시행 | 제59조 재난복구계획의 수립·시행 |
| | | 제59조의2 재난복구계획에 따라 시행하는 사업의 관리 |
| | 특별 재난지역 | 제60조 특별재난지역의 선포 |
| | | 제61조 특별재난지역에 대한 지원 |
| | 손해 배상 및 포상 | 제62조 비용 부담의 원칙 |
| | | 제63조 응급지원에 필요한 비용 |
| | | 제64조 손실보상 |
| | | 제65조 치료 및 보상 |
| | | 제65조의2 포상 |
| | | 제66조 재난지역에 대한 국고보조 등의 지원 |
| | | 제66조의2 복구비 등의 선지급 |
| | | 제76조 재난 보험등의 가입 등 |
| 기반 조성 | 안전문화 진흥 | 제66조의10 안전지수의 공표 |
| | | 제66조의11 지역축제 개최 시 안전관리조치 |
| | | 제66조의12 안전사업지구의 지정 및 지원 |
| | | 제66조의4 안전문화 진흥을 위한 시책의 추진 |

| | | |
|---|---|---|
| | | 제66조의7 국민안전의 날 등 |
| | | 제66조의8 안전관리헌장 |
| | | 제66조의10 안전지수의 공표 |
| | | 제66조의11 지역축제 개최 시 안전관리조치 |
| | | 제66조의12 안전사업지구의 지정 및 지원 |
| | 재난관리기금 | 제67조 재난관리기금의 적립 |
| | | 제68조 재난관리기금의 운용 등 |
| | 안전기술개발 및 지원 | 제71조 재난 및 안전관리에 필요한 과학기술의 진흥 등 |
| | | 제71조의2 재난 및 안전관리기술개발 종합계획의 수립 등 |
| | | 제72조 연구개발사업 성과의 사업화 지원 |
| | | 제73조 기술료의 징수 및 사용 |
| | | 제73조의2 재난안전기술의 사업화 지원 등 |
| | | 제73조의3 전문기관 지정의 취소 |
| | | 제73조의4 재난안전제품의 인증 |
| | 재난관리정보통신체계 구축 | 제74조 재난관리정보통신체계의 구축·운영 |
| | | 제74조의2 재난관리정보의 공동이용 |
| | | 제66조의9 안전정보의 구축·활용 |

이를 자세하게 보면 기구 및 관리 계획 분야에 안전관리 기구 및 조직, 조직 역할 정의, 안전관리 계획 등으로 분류할 수 있다. 이는 재난 안전관리에 대한 전체적인 조직을 구성하여 역할을 부여하는 것과 안전관리계획을 수립하는 등 전체 틀을 구성하고 방향을 수립하는 것이 주요 내용이다.

안전 관리의 주요 활동들은 재난 안전 관리의 기본 흐름인 예방 - 대비 - 대응 - 복구의 4 단계에 맞추어 재난 예방(제4장), 재난 대비(제5장), 재난 대응(제6장), 재난 복구(제7장)와 같이 4단계로 구분되어 있다. 이를 통해 재난에 대한 준비를 철저히 하고 재난 발생 시 즉각적인 대응을 통해 인명 및 재산 손실을 최소화하기 위한 실질적 활동들을 수행해야 한다. 또한 재난 발생에 따른 특별재난지역 선포 및 손해 배상 및 복구 계획을 수립함으로써 피해에 대한 빠른 복구 활동 등을 체계적으로 수행할 수 있는 체계를 갖추고 있다.

재난 예방(제4장)의 세부 활동으로는 관리대상 지정, 담당자 교육, 안전 점검, 안전조치, 실태조사 결과 공개 등이 있다. 재난 대비(제5장)를 위해 세부 활동에 재난 관리 자원 비축, 관리기준 수립, 매뉴얼, 대비훈련 등을 수행한다. 재난 대응(제6장)의 세부 활동으로는 사고 인지 및 전파, 응급조치 대피 및 동원, 긴급 구조 등이 있다. 재난 복구(제7장)를 위한 세부 활동으로는 신고 및 조사, 복구계획 수립 및 시행, 특별 재난지역, 손해 배상 및 포상, 벌칙 등이 있다.

마지막으로 기반 조성 분야에는 안전문화 진흥, 재난 관리 기금, 안전 기술 개발 및

지원, 재난관리 정보통신 체계 구축 등이 있다. 이는 재난 안전이 단시간에 해결할 수 없는 문제이고 정부 등 어느 일방의 노력이 아니라 전체 구성원이 함께 재난에 대한 예방, 대비, 대응, 복구가 장기적인 관점에서 필요하기 때문에 이에 대한 지속적인 인식 확산과 신기술 개발이 필요하다.

이와 같은 재난 안전 관리를 위한 프레임워크를 그림으로 정리하면 [그림 5]와 같이 정리할 수 있다.

[그림 5] 재난안전법의 안전 관리 기본 프레임워크


정보통신망법은 정보통신망의 이용 촉진과 정보통신 서비스의 사용자 정보를 보호하며 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하기 위해 만들어졌다. 해당 법은 SW 기반의 정보통신 시스템을 관리하기 위한 요소들을 포함하기 때문에 SW안전 관리 프레임워크(안) 도출에 있어 SW 관리 측면을 보완하기 위해 분석하였다. 다만, 안전 관리 측면이 없기 때문에 재난안전법의 4단계 기본 체계를 바탕으로 〈표 6〉 과 같이 재해석할 수 있다.

〈표 6〉 정보통신망법의 안전 관리 관점의 해석

| 대 분류 | 안전관리활동 | 해당 법조항 |
|---|---|---|
| 기구 및 계획 | 기관 및 조직 | 제9조 인증기관의 지정 등 |
| | | 제44조의10 명예훼손 분쟁조정부 |
| | 조직 역할 정의 | 제4조 정보통신망 이용촉진 및 정보보호등에 관한 시책의 마련 |
| | | 제27조 개인정보 보호책임자의 지정 |
| | | 제45조의3 정보보호 최고책임자의 지정 등 |
| | | 제53조 통신과금서비스제공자의 등록 등 |
| 안전활동-예방 | 관리 대상 | 제22조 개인정보의 수집·이용 동의 등 |
| | | 제22조의2 접근권한에 대한 동의 |
| | | 제24조 개인정보의 이용 제한 |
| | | 제25조 개인정보의 처리위탁 |
| | | 제26조 영업의 양수 등에 따른 개인정보의 이전 |
| | | 제23조 개인정보의 수집 제한 등 |
| | | 제27조의2 개인정보 처리방침의 공개 |
| | | 제28조 개인정보의 보호조치 |
| | | 제28조의2 개인정보의 누설금지 |
| | | 제29조 개인정보의 파기 |
| | 사전 점검 | 제45조의2 정보보호 사전점검 |
| 안전활동-대비 | 관리 기준 | 제23조의2 주민등록번호의 사용 제한 |
| | | 제23조의4 본인확인업무의 정지 및 지정취소 |
| | | 제24조의2 개인정보의 제공 동의 등 |
| | | 제28조 개인정보의 보호조치 |
| | | 제28조의2 개인정보의 누설금지 |
| | | 제45조 정보통신망의 안정성 확보 등 |
| | | 제46조 집적된 정보통신시설의 보호 |
| | | 제47조의5 정보보호 관리등급 부여 |
| | | 제48조 정보통신망 침해행위 등의 금지 |
| | | 제49조의2 속이는 행위에 의한 개인정보의 수집금지 등 |
| | | 제50조 영리목적의 광고성 정보 전송 제한 |
| | | 제51조 중요 정보의 국외유출 제한 등 |
| | | 제54조 등록의 결격사유 |
| | | 제55조 등록의 취소명령 |
| | | 제56조 약관의 신고 등 |
| | 표준화 및 인증 | 제8조 정보통신망의 표준화 및 인증 |
| | | 제47조 정보보호 관리체계의 인증 |
| | | 제47조의2 정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관의 지정취소 등 |
| | | 제47조의3 개인정보보호 관리체계의 인증 |
| | | 제66조 비밀유지 등 |
| | 이용자 보호 | 제30조 이용자의 권리 등 |
| | | 제41조 청소년 보호를 위한 시책의 마련 등 |
| | | 제42조 청소년유해매체물의 표시 |
| | | 제42조의2 청소년유해매체물의 광고금지 |

| | | |
|---|---|---|
| | | 제42조의3 청소년 보호 책임자의 지정 등 |
| | | 제43조 영상 또는 음향정보 제공사업자의 보관의무 |
| | | 제44조 정보통신망에서의 권리보호 |
| | | 제44조의2 정보의 삭제요청 등 |
| | | 제44조의3 임의의 임시조치 |
| | | 제44조의4 자율규제 |
| | | 제44조의5 게시판 이용자의 본인 확인 |
| | | 제44조의6 이용자 정보의 제공청구 |
| | | 제44조의7 불법정보의 유통금지 등 |
| | | 제44조의8 대화형정보통신서비스에서의 아동 보호 |
| | | 제47조의4 이용자의 정보보호 |
| 안전활동-대응 | 유출 통지 및 신고 | 제27조의3 개인정보 유출등의 통지·신고 |
| | | 제30조의2 개인정보 이용내역의 통지 |
| | | 제48조의3 침해사고의 신고 등 |
| | 사고 대응 | 제46조의2 집적정보통신시설 사업자의 긴급대응 |
| | | 제48조의2 침해사고의 대응 등 |
| 안전활동-복구 | 사고 원인 분석 | 제48조의4 침해사고의 원인 분석 등 |
| | | 제64조 자료의 제출 등 |
| | | 제64조의2 자료 등의 보호 및 폐기 |
| | | 제65조 권한의 위임·위탁 |
| | | 제69조의2 고발 |
| | 방지 대책 실행 | 제32조의4 노출된 개인정보의 삭제·차단 |
| | | 제64조의4 청문 |
| | 손해배상 | 제32조의2 법정손해배상의 청구 |
| | | 제32조의3 손해배상의 보장 |
| | | 제32조 손해배상 |
| | | 제60조 손해배상 등 |
| | | 제75조 양벌규정 |
| | | 제75조의2 몰수·추징 |
| | | 제76조 과태료 |
| | 분쟁 조정 | 제59조 분쟁 조정 및 해결 등 |
| 기반조성 및 역량강화 | 기술 개발 지원 | 제6조 기술개발의 추진 등 |
| | | 제7조 기술관련 정보의 관리 및 보급 |
| | | 제10조 정보내용물의 개발 지원 |
| | | 제11조 정보통신망 응용서비스의 개발 촉진 등 |
| | 정보 공동 활용 | 제12조 정보의 공동활용체제 구축 |
| | | 제13조 정보통신망의 이용촉진 등에 관한 사업 |
| | | 제14조 인터넷 이용의 확산 |
| | | 제15조 인터넷 서비스의 품질 개선 |
| | | 제29조의2 개인정보보호의 촉진 및 지원 |
| | 국제협력 | 제62조 국제협력 |
| | | 제63조 국외 이전 개인정보의 보호 |
| | | 제63조의2 상호주의 |

SW 기반 시스템을 관리를 위한 법이기 때문에 재난안전법의 안전 관리를 위한 안전 관리 계획, 점검 조치 및 결과 공유, 매뉴얼 및 대비 훈련, 긴급 구조 등은 포함되어

있지 않다. 다만, 개인 정보 관리, 표준화 및 인증, 이용자 보호, 방지 대책 실현, 정보의 공동 활용, 국제협력 등은 소프트웨어 관리를 위한 활동들을 포함하고 있으며 이는 SW안전 관리 관점에서 필요한 관리 항목들이다.

정보통신망법에는 정보 유출을 예방하기 위한 개인 정보 관리를 위한 개인 정보 개인 정보의 수집 및 이용 동의, 접근 권한에 대한 동의, 개인 정보 이용 제한, 개인 정보의 처리 위탁, 개인 정보 처리방침의 공개, 개인 정보의 보호조치, 개인 정보의 누설 금지, 개인 정보의 파기 같은 활동들이 있다. 이와 같은 활동들은 안전 관리의 예방 활동의 관리 대상 선정과 유사하다고 할 수 있다. 또한, 관리 대상을 선정하여 정보보호 사전 점검을 실시하여 정보 유출을 예방할 수 있다.

또한, SW 관점에서 보면 표준화 및 인증 관련하여 정보통신망의 표준화와 인증, 정보 보호 관리 체계의 인증, 인증 및 심사 기관 지정 및 취소, 개인 정보 관리 등급 부여 등은 안전 관리를 위한 대비 활동의 일환으로 볼 수 있다. 이용자 보호 관점에서 이용자 권리보호, 자율규제, 이용자의 본인 확인, 안전 정보의 제공 및 청구, 불법정보의 유통 금지 등의 활동들은 안전 관리 대비 활동으로 볼 수 있다. 그리고 개인 정보 관리를 위한 기준 수립을 위한 활동들도 대비 활동의 일환으로 볼 수 있다.

개인 정보 유출 통지 및 신고 활동 및 사고 대응은 안전 관리 관점에서 보면 대응 측면으로 해석 가능하다. 그리고 사고 원인 분석 및 방지 대책 실행을 위한 노출된 개인정보의 삭제 · 차단, 정보누출 기관에 대한 처리 등의 활동들도 사고 발생 후에 원상 복구 및 재발 방지를 위한 안전 관리 복구 활동으로 해석할 수 있다.

더불어 정보 공동 활용 관점에서 정보의 공동 활용 체제 구축, 이용촉진 등에 관한 사업, 서비스의 품질 개선 등과 기술 개발 지원 관점의 기술 개발의 추진, 기술 관련 정보의 관리 및 보급 등은 안전 문화 진흥과 연계된 기반 조성으로 볼 수 있다.

이와 같은 분석을 토대로 안전 관리 관점에서 정보통신망법을 분석하면 [그림 6]처럼 단계별 주요 활동을 정리할 수 있다.

[그림 6] 정보통신망법의 관리 단계별 주요 활동


개인정보보호법은 개인정보의 처리 및 보호에 관한 사항을 규정하여 개인의 자유와 권리를 보호함으로써 개인의 존엄과 가치를 구현하는데 있다.[10] 개인정보란 살아 있는 개인에 관한 모든 정보를 의미하며 성명, 주민등록번호 및 영상 등을 통하여 개인을 식별할 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함)로 SW와 관련된 데이터 관리 관점에서 SW 안전 관리를 위한 프레임워크 도출에 시사점을 제공해 줄 수 있다.

특히 개인정보 탈취, 오용으로 인한 피해 방지를 위한 관리 항목들은 재난안전법과 유사성 있지만 개인정보에 한정된 관리이어서 안전관리 매뉴얼 및 대비 훈련, 응급조치 대피 및 동원, 긴급 구조 등의 관련 사항들은 없다. 하지만, 영향 평가, 인증, 분쟁조정 및 단체소송, 국제협력 등은 SW안전 관리 프레임워크에 고려해야할 항목이다. 이 법 체계도 정보통신망법과 마찬가지로 안전 관리에 대한 고려가 없기 때문에 재난안전법에서 안전 관리 4단계를 고려하여 <표 7>처럼 해석하였다.

10) 개인정보 보호법 제 1 조

<표 7> 개인정보보호법의 안전 관리 관점의 해석

| 대 분류 | 안전관리활동 | 해당 법조문 |
|---|---|---|
| 기구 및 계획 | 개인정보 기구 | 제7조 개인정보 보호위원회 |
| | | 제8조 보호위원회의 기능 등 |
| | 조직 역할 정의 | 제4조 정보주체의 권리 |
| | | 제5조 국가 등의 책무 |
| | | 제31조 개인정보 보호책임자의 지정 |
| | 관리계획 | 제9조 기본계획 |
| | | 제10조 시행계획 |
| 예방 | 관리 대상 | 제11조 자료제출 요구 등 |
| | | 제15조 개인정보의 수집·이용 |
| | | 제16조 개인정보의 수집 제한 |
| | | 제17조 개인정보의 제공 |
| | | 제26조 업무위탁에 따른 개인정보의 처리 제한 |
| | | 제32조 개인정보파일의 등록 및 공개 |
| | 개선권고 | 제61조 의견제시 및 개선권고 |
| 대비 | 관리 기준 | 제3조 개인정보 보호 원칙 |
| | | 제12조 개인정보 보호지침 |
| | | 제18조 개인정보의 목적 외 이용·제공 제한 |
| | | 제19조 개인정보를 제공받은 자의 이용·제공 제한 |
| | | 제20조 정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지 |
| | | 제21조 개인정보의 파기 |
| | | 제22조 동의를 받는 방법 |
| | | 제23조 민감정보의 처리 제한 |
| | | 제24조 고유식별정보의 처리 제한 |
| | | 제24조의2 주민등록번호 처리의 제한 |
| | | 제25조 영상정보처리기기의 설치·운영 제한 |
| | | 제27조 영업양도 등에 따른 개인정보의 이전 제한 |
| | | 제28조 개인정보취급자에 대한 감독 |
| | | 제29조 안전조치의무 |
| | | 제30조 개인정보 처리방침의 수립 및 공개 |
| | | 제35조 개인정보의 열람 |
| | | 제36조 개인정보의 정정·삭제 |
| | | 제37조 개인정보의 처리정지 등 |
| | | 제38조 권리행사의 방법 및 절차 |
| | | 제59조 금지행위 |
| | | 제60조 비밀유지 등 |
| | 인증 | 제32조의2 개인정보 보호 인증 |
| | 영향평가 | 제33조 개인정보 영향평가 |
| | | 제8조의2 개인정보 침해요인 평가 |
| 대응 | 유출 통지 및 신고 | 제34조 개인정보 유출 통지 등 |
| | | 제62조 침해 사실의 신고 등 |
| 복구 | 사고 조사 | 제63조 자료제출 요구 및 검사 |
| | 방지대책 실행 | 제64조 시정조치 등 |

| | | |
|---|---|---|
| | | 제65조 고발 및 징계권고 |
| | | 제66조 결과의 공표 |
| | | 제67조 연차보고 |
| | 손해 배상 | 제34조의2 과징금의 부과 등 |
| | | 제39조 손해배상책임 |
| | | 제39조의2 법정손해배상의 청구 |
| | 분쟁 조정 | 제40조 설치 및 구성 |
| | | 제41조 위원의 신분보장 |
| | | 제42조 위원의 제척·기피·회피 |
| | | 제43조 조정의 신청 등 |
| | | 제44조 처리기간 |
| | | 제45조 자료의 요청 등 |
| | | 제46조 조정 전 합의 권고 |
| | | 제47조 분쟁의 조정 |
| | | 제48조 조정의 거부 및 중지 |
| | | 제49조 집단분쟁조정 |
| | | 제50조 조정절차 등 |
| | 단체 소송 | 제51조 단체소송의 대상 등 |
| | | 제52조 전속관할 |
| | | 제53조 소송대리인의 선임 |
| | | 제54조 소송허가신청 |
| | | 제55조 소송허가요건 등 |
| | | 제56조 확정판결의 효력 |
| | | 제57조 「민사소송법」의 적용 등 |
| 기반조성 | 안전문화 진흥 | 제13조 자율규제의 촉진 및 지원 |
| | 국제협력 | 제14조 국제협력 |

개인정보보호법도 개인 정보 관리를 위한 개인정보 보호위원회, 개인정보 보호책임자의 지정 같은 기구 및 역할을 정의하고 있고 기본 계획 수립과 시행 계획 수립 같은 관리 계획 수립을 정하고 있다. 이는 재난안전법의 기구 및 관리 계획 수립과 유사하다고 할 수 있다.

그리고 예방 차원에서 관리 대상 지정을 위한 자료 제출 요구, 개인 정보의 수집 및 이용 및 개인 정보의 제공, 업무 위탁에 따른 개인정보의 처리 제한 관련 규정을 정의하고 있다. 그리고 필요한 경우에 한하여 개선 권고하기 위한 의견 제시 및 개선을 권고함으로써 개인정보 유출을 예방할 수 있는 법적 관리 절차를 규정하고 있다.

개인정보 관리를 위한 대비로서 개인 정보 보호 원칙, 개인정보 보호 지침, 개인 정보의 목적 외 이용 제공 제한 같은 관리 대상의 지정 및 기준을 마련하고 있다. 이 외에 개인정보 보호 인증 활동 및 개인정보 영향 평가와 개인정보 침해요인 평가 같은 개인정보로 인한 여러 평가를 마련하고 있다.

대응 차원으로 개인 정보 보호 활동으로는 유출 통지 및 신고에 해당되는 개인정보 유출 통지 관련 활동과 침해 사실의 신고 활동들이 있다. 이는 개인 정보 유출 사고와 침해 사실에 대한 신고를 통해 사고의 존재를 인식하기 위한 활동들이다.

사고 발생에 따른 복구를 위한 활동들로는 우선 사고 인지 후 사고 조사를 위한 자료 요구 및 검사 활동이 있고, 재발 방지를 위한 방지 대책의 일환으로 시정 조치, 고발 및 징계 권고, 결과의 공표 같은 개선 및 징벌적 활동들이 포함되어 있다. 그리고 발생한 손해에 대한 배상을 위한 과징금 부과 및 손해 배상 책임을 명확히 하고 있다. 이러한 손해 배상 활동 후에도 분쟁이 발생할 경우에는 분쟁을 해결하기 위한 활동들과 필요시 단체 소송에 대한 활동까지 포괄하고 있다.

마지막으로 개인 정보 보호에 관련되어 자율 규제의 촉진을 통한 개인정보 보호 문화 진흥 및 국제 협력을 통해 개인정보의 국가간 이동시에 따른 침해 대비 시책의 필요성을 정의하고 있다.

이러한 개인정보보호법의 안전 관리 관점에서의 각 단계별 활동을 구분하면 [그림 7]과 같이 정리할 수 있다.

[그림 7] 개인정보보호법의 관리 단계별 활동 영역

## 2. 소프트웨어 안전 관리 현황 프레임워크(안) 도출

앞에서 재난안전법, 정보통신망법, 개인정보보호법의 법 체계를 분석하여 기존 HW와 시설물 관점의 안전 관리 체계에 소프트웨어 관리 활동들을 고려한 SW안전 관리 현황 프레임워크(안)를 수립하기 위한 기초 정보들을 <표 8>과 같이 정리하였다.

<표 8> 재난안전법과 정보통신망법, 개인정보보호법을 비교한 SW안전 관리 활동들

| 구분 | | 재난안전법 | SW 관점 추가 요소 도출 | | SW 안전관리 활동 |
|---|---|---|---|---|---|
| | | | 정보통신망법 | 개인정보보호법 | |
| 안전 관리 기구 및 관리 계획 | | 안전 관리 기구 | 기관 및 조직 | 개인정보 기구 | 안전관리 조직 |
| | | 조직 역할 정의 | 조직 역할 정의 | 조직 역할 정의 | 기능 및 역할 정의 |
| | | 안전 관리 계획 | | 관리 계획 | 안전 관리 계획 |
| 안전 관리 활동 | 예방 단계 | 관리대상 지정 | 관리대상 지정 | 관리대상 지정 | 안전관리 대상 |
| | | 담당자 교육 | | | 자격 및 교육 |
| | | 안전 점검 | 사전 점검 | | 안전 점검 |
| | | 안전 조치 | | 개선 권고 | |
| | | 정보 공유 및 공개 | | | 안전현황 공개 |
| | 대비 단계 | 안전 기준 | 관리 기준 | 관리 기준 | 안전 기준 |
| | | | 표준화 및 인증** | 개인정보보호인증** | 인증 |
| | | | | 영향 평가** | 위험 평가 |
| | | | 이용자 보호** | | 이용자 보호 |
| | | 매뉴얼 | | | 대비 매뉴얼/훈련 |
| | | 대비훈련 | | | |
| | | 재난 관리자원 비축* | | | |
| | 대응 단계 | 사고 인지 및 전파 | 유출 통지 및 신고 | 유출 통지 및 신고 | 사고 신고 및 통지 |
| | | 응급조치, 대피 및 동원 | 사고 대응 | | 사고 대응 |
| | | 긴급 구조* | | | |
| | 복구 단계 | 사고 조사 | 사고 원인 분석 | 사고 조사 | 사고 조사 |
| | | 복구 계획 수립 및 시행 | 방지대책 실행** | 방지대책 실행** | 재발 방지 |
| | | 특별 재난 지역* | | | |
| | | 손해 배상 및 보상 | 손해배상 | 손해배상 | 손해배상 |
| | | | 분쟁조정** | 분쟁조정** | 분쟁조정 |
| | | | | 단체소송 | |

| | | | | |
|---|---|---|---|---|
| 안전 기반 조성 | 안전문화 진흥 | | 개인정보 보호 문화 진흥 | 안전 문화 진흥 |
| | 재난관리기금* | | | |
| | 안전기술 개발 및 지원 | 기술개발지원 | | 안전기술 개발 |
| | 재난관리정보통신 체계 구축* | | | |
| | | 정보 공동 활용** | | 안전정보 공동 활용 |
| | | 국제협력** | 국제협력** | 국제협력 |

* 재난안전법의 안전 관리 체계에는 있으나 SW안전 관리 관점에서 불필요한 활동

** 재난안전법의 안전 관리 체계에는 없으나 SW안전 관리를 위해 필요한 활동

다음은 재난안전법의 안전 관리 체계에는 없으나 SW안전 관리 관점에서 필요한 활동들이다.

- 표준화 및 인증, 개인정보보호 인증 --> **인증**: SW안전 확보를 위한 SW, 또는 관련 기술의 검사 및 확인을 같은 인증 활동
- 영향 평가 --> **위험평가**: 들어나지 않은 SW 위험을 평가하기 위한 활동
- 이용자 보호: SW를 활용하는 이용자를 보호하기 위한 활동
- 방지 대책 실행 --> **재발 방지**: SW로 인한 사고 재발을 방지하기 위한 활동
- 분쟁조정, 단체소송 -->**분쟁조정**: 들어나지 않은 SW사고에 대한 분쟁을 조정하기 위한 활동
- **정보 공동 활용**: SW사고에 대한 원인, 대응 등의 정보를 공유함으로써 사고 확산을 방지하기 위한 활동
- **국제 협력**: 국제적으로 활용되는 SW 또는 SW를 포함한 제품의 공동 대응을 위한 활동

그리고 재난안전법의 안전 관리 체계에는 포함되나 SW안전 관리 관점에서 불필요한 활동들은 다음과 같다. 이들 활동들은 재난 안전 관리 측면에서는 반드시 필요한 활동들이지만 SW안전 사고를 예방하고 대비하고 대응하고 복구와는 직접적인 연관성을 찾기가 어려웠다. 하지만 향후에 SW 영향력이 커질 경우 아래의 항목들에 대한 추가 고려가 필요할 수 있다.

- 재난자원 관리 및 비축:

- 긴급 구조
- 특별 재난 지역 선포
- 재난 관리 기금
- 재난관리 정보통신 체계 구축

이러한 SW안전 관리를 위한 활동들을 재난안전법의 안전 관리 체계와 같이 크게 안전조직 및 관리 계획, 안전 관리 활동, 안전 기반 조성 등 3개 분야로 구분할 수 있다. 그리고 SW안전 활동들도 예방 - 대비 - 대응 - 복구의 4단계로 세분화할 수 있다. 각 분야별 활동들을 설명하면 다음과 같다.

### 1) 소프트웨어 안전조직 및 관리 계획

- 안전관리 조직 : SW안전 관리를 담당하는 조직의 구성 및 운영에 관한 내용을 정의하며 안전한 SW 환경을 제공하기 위해 안전 정책을 만들어 안전 관리 계획을 수립하고 실제 안전 관리 활동에 참여하는 각 기관(예를 들어 안전관련 위원회, 대책본부 등) 및 조직 구성을 정하는 활동
- 기능 및 역할 정의 : SW안전 관리 조직이 수행하는 안전 관리 활동 및 각 조직의 세부 구성, 구성원의 자격, 역할, 권한 및 책임을 정의하기 위한 활동으로 관련 기관/기업 지원, 안전관리 책임자 및 자문단 같은 안전 활동을 수행할 주체들을 정하는 활동
- 안전 관리 계획 : SW안전 관리에 대한 국가, 해당 분야별, 해당 조직 단위의 전략, 세부 관리 계획 등을 수립하기 위한 활동

### 2) 소프트웨어 안전관리 예방 활동

- 안전 관리 대상: SW안전이 중요한 분야 및 시스템 등을 정의할 수 있으며 안전 기준 또는 분야에 따라 관리 방법이 달라질 수 있기 때문에 체계적인 대상 선정하는 활동
- 자격 및 교육: SW안전 관련 담당자 및 종사자의 필요 자격 요건 및 역량 강화를

위한 교육 등을 포괄하는 활동

- 안전 점검: SW안전 기준에 따라 정해진 시점에서 행해지는 안전 점검을 통해 SW안전에 위배될 경우 시정 조치 등을 통해 안전을 확보하기 위한 활동
- 안전 관리 현황 공개: SW안전 관리 조사 결과를 투명하게 공개함으로써 안전 에 대한 경각심을 유발하거나 조치 결과를 투명하게 확인할 수 있는 활동으로 필요 시 담당 기관 및 담당자에게 이행 현황에 대한 자료를 요구할 수도 있음

### 3) 소프트웨어 안전 관리 대비 활동

- 안전 기준: SW안전 관리 대상에 대해 관리 기준 등을 제시하기 위한 활동으로 산업 및 SW 제품에 따라 달라질 수 있으며 안전 중요 분야는 안전 기준을 수립해서 지속적으로 관리가 필요함
- 위험 평가: SW안전 관리 대상의 발생 가능한 위험 요인을 도출하고 해당 위험에 대한 영향도를 산정하여 평가하고 해당 위험을 제거, 완화하기 위한 지속적인 관리 활동
- 인증: SW안전 관리 대상이 안전 기준에 적합한지 여부를 검사하고 검사 결과가 적합하다는 확인할 수 있는 활동으로 전체 시스템, 단위 시스템, 구성 부품 등에 따라 수행될 수 있음
- 이용자 보호: SW안전 관리 대상을 이용하는 이용자에 대한 안전보호 조치를 수행하는 활동
- 대응 매뉴얼/훈련: 실제 안전사고가 발생할 경우를 가정한 훈련을 실시하고 행동 요령에 대한 안전관리 대응 매뉴얼을 작성하여 기능별 안전관리 활동계획을 실시해야 함

### 4) 소프트웨어 안전 관리 대응 활동

- 사고신고 및 통지: SW안전사고 발생 시 사전에 정해진 매뉴얼에 따라 신고하고 해당 제품에 대해서는 관련 제품을 사용자에게 통지하여 안전사고 및 향후 발생 가능성을 대응할 수 있게 하는 활동

- 사고 대응: 사고 발생 시 피해를 최소화하기 위하여 사상자에 대한 응급조치 같은 즉각적인 대응 조치를 수행하기 위한 활동

### 5) 소프트웨어 안전 관리 복구 활동

- 사고 조사: 사고 원인 및 사고 피해 상황을 파악하기 위하여 사고 관련 자료의 보존 및 자료 분석 등 사고 원인을 파악하기 위한 일련의 활동
- 재발 방지: SW안전사고가 재발하지 않도록 발생 위험 요인을 제거하거나 위험을 완화하기 위한 활동
- 손해 배상: SW안전사고로 발생한 피해를 구제하기 위하여 응급 대응 비용 부담, 사고 파손된 장비 등에 대한 보상 등을 국가적으로 지원하기 위한 활동
- 분쟁 조정: SW안전사고 당사자 간의 보상 및 배상에 대한 분쟁을 조정을 위한 분쟁조정위원회 등 기구 설치, 위원회 구성원의 자격 등을 정의 같은 분쟁을 조정하는 활동

### 6) 소프트웨어 안전 기반 조성

- 안전 문화 진흥: SW안전에 대한 사회적인 인식을 높이기 위한 안전 교육 및 훈련, 캠페인 및 홍보, 안전 행동 요령의 개발 및 보급, 안전관리 우수사례에 대한 발굴 및 확산, 안전관련 통계 현황 관리 및 공개, 안전관련 각종 조사 및 분석 같은 일련의 활동
- 안전 기술 개발: SW안전 확보를 위한 신기술 개발을 위한 전문 기관 지정 등을 포함한 활동
- 안전 정보 공동 활용: SW안전 강화를 위해 정보를 공유하고 공개함으로써 안전에 위험이 되거나 강화할 수 있는 정보 교류를 원활하게 하기 위한 활동
- 국제 협력: SW안전 기술 논의 및 국가간 협력을 위한 활동들로 대표적 사례로 SW안전 분야의 표준화 활동이 있음

위의 내용들을 기반으로 수립한 SW안전 관리 현황 프레임워크(안)은 [그림 8]과 같다. 이 프레임워크(안)는 SW안전 분야의 안전 관리 활동들을 조사하기 위한 프레임워크로 현황 조사를 통해 해당 프레임워크에 대한 검증을 통해 보완이 필요하다.

[그림 8] 소프트웨어 안전 관리 프레임워크(안)


해당 프레임워크에 대한 다양한 분야의 전문가 의견을 수렴한 결과 다음과 같은 의견들이 있었다.

- 재난안전법은 모든 재난 안전을 다룬 것은 아니지만, 안전 관리 체계의 기본적 구성을 다루고 있기 때문에 안전관리의 기반을 마련하였고, 피해 감소를 위한 응급조치를 중요하게 생각하여 이에 대한 체계를 잘 갖추고 있음.
- SW안전 관리 체계는 발생한 문제에 대한 고려가 필요하며 *철도*/항공/자동차 등의 일부에서는 안전법을 기초로 SW에 대한 고려가 있지만, 대부분의 분야는 이에 대한 고려가 없기 때문에 SW안전 관리의 기반 마련이 필요함
- 분야별로 안전 관리를 위한 체계가 갖추어져 있지만 SW에 대한 종합적인 관리는 부족하므로 SW 통합적인 입장에서 안전 관리에 대한 체계를 연구하는 것은 타 분야에서 참고모델로써 좋은 시도임
- SW는 제품과 사람과의 관계(관제 시스템 - 관제사/항공기 - 조종사 등)가 더 중

요할 수 있기 때문에 SW 시스템을 운영하는 사람의 역량을 검증하고 향상시키기 위한 교육이 중요함

# 제3장 소프트웨어 안전 관리 프레임워크(안) 검증

## 제1절 프레임워크(안) 검증을 위한 현황 조사 대상 선정

SW과 확산되면서 SW와 관련된 안전 분야가 많아지고 있다. <표 9>는 대표적인 SW 안전 분야를 선정하기 위해 전문가 자문을 통해 조사한 안전 관련 법안의 목록들을 주요 분야별로 정리한 내용이다. 이와 같이 SW가 이미 다양한 안전 분야로 확산되고 있으며 관련 법안 중에 일부는 복수의 분야와 연관되어 있다.

하지만, 이들 모든 분야에 대한 현황 조사를 수행하기에는 제한된 연구 기간 때문에 어려움이 있기 때문에 SW와 밀접한 주요 분야를 우선적으로 살펴 볼 필요가 있다. 따라서 SW와 안전의 관련성 및 SW가 안전사고에 미치는 영향에 대해 전문가 설문 조사를 수행하여 SW안전 관리 현황 조사가 중요한 분야를 선정하고자 한다. 선정 분야를 중심으로 앞에서 설계된 SW안전 관리 프레임워크(안)을 기반으로 실제 현장에서 SW 안전 관리 현황에 대해 조사하여 설계된 프레임워크(안)을 검증하고 보완하고자 한다.

<표 9> 안전 관련 법안 목록

| 분야 | 관련 법안 |
|---|---|
| 재난안전 | 재난 및 안전관리 기본법, 정보통신기반 보호법, 국가정보화 기본법, 국가통합교통체계효율화법, 도로교통법, 철도안전법, 도시철도법, 교통안전법, 항공안전법, 항공·철도 사고조사에 관한 법률, 해사안전법, 선박안전법, 시설물의 안전 및 유지관리에 관한 특별법, 송유관 안전관리법, 액화석유가스의 안전관리 및 사업법, 승강기 시설안전법, 위험물안전관리법, 지하안전관리에 관한 특별법, 원자력안전법, 한국원자력안전기술원법, 국민 안전교육 진흥 기본법 등 |
| 정보통신 | 정보통신기반 보호법, 국가정보화 기본법, 소프트웨어산업진흥법, 제품안전기본법, 전기용품 및 생활용품 안전관리법, 국가통합교통체계효율화법 등 |
| 제품안전(전기용품, 공산품 등) | 제품안전기본법, 전기용품 및 생활용품 안전관리법, 품질경영 및 공산품 안전관리법, 제조물책임법, 소비자기본법, 식품안전기본법 등 |
| 교통(자동차, 철도, 선박, 항공 등) | 국가통합교통체계효율화법, 자동차관리법, 도로교통법, 철도안전법, 도시철도법, 교통안전법, 항공안전법, 항공·철도 사고조사에 관한 법률, 군용항공기 비행안전성 인증에 관한 법률, 해사안전법, 선박안전법, 국민 안전교육 진흥 기본법 등 |

| | |
|---|---|
| 시설물 (승강기, 공공시설 등) | 국가통합교통체계효율화법, 도로교통법, 철도안전법, 도시철도법, 교통안전법, 해사안전법, 시설물의 안전 및 유지관리에 관한 특별법, 송유관 안전관리법, 액화석유가스의 안전관리 및 사업법, 승강기 시설안전법, 위험물안전관리법, 지하안전관리에 관한 특별법, 원자력안전법, 소규모 공공시설 안전 관리 등에 관한 법률 등 |
| 에너지(원자력, 유류 등) | 송유관 안전관리법, 액화석유가스의 안전관리 및 사업법, 위험물안전관리법, 지하안전관리에 관한 특별법, 원자력안전법, 한국원자력안전기술원법 등 |
| 기타 (산업안전, 식품안전 등) | 산업안전보건법, 한국산업안전보건공단법, 식품안전기본법, 국민 안전교육 진흥 기본법 등 |

## 1. 현황 조사 분야 선정 방법

전문가 설문에 앞서 <표 9>에서 언급된 30여개의 다양한 안전 관련 법안들이 적용되는 주요 분야들을 재난안전, 정보통신, 제품 안전, 교통, 시설물, 에너지 및 기타 분야로 구분하였다. 이는 개별 전문가들이 모든 분야를 포괄하기 어렵고 설문 조사 수행을 원활하게 하기 위함이다. 선정된 전문가들은 다양한 분야에 걸쳐 최대한 폭 넓게 선정하여 교통 분야 3명, 재난안전 분야 2명, 정보통신 분야 2명, 시설물 분야 2명, 에너지 분야1 명, 제품안전 분야 3명, 기타 분야 2명 등 총 15명의 안전 전문가로 구성하였다. 이들은 <표 10> 같이 해당 분야에서 SW 관련 업무를 10년 이상 수행한 경력이 있고 기술사 또는 박사 학위를 가진 안전 분야 전문가들이다.

<표 10> 조사대상 선정 참여 전문가 목록

| 전문가 | 자격 | 경력(년) | 분야 | 주요 경력 |
|---|---|---|---|---|
| 전문가1 | 박사 | 25 | 정보통신분야 | • 연구 교수<br>• 정보보호및SW품질/안전성 |
| 전문가2 | 기술사 | 20 | 제품안전 분야 | • SW개발 업무<br>• 임베디드시스템개발 |
| 전문가3 | 박사 | 18 | 재난 안전 분야 | • 재난 안전 분야, 안전 법제도 |
| 전문가4 | 기술사 | 17 | 교통 분야 | • 자동차 SW 품질 및 안전 |
| 전문가5 | 기술사 | 15 | 기타 분야 | • 제어장치 SW안전 분야 |
| 전문가6 | 기술사 | 17 | 기타 분야 | • 의료기기 SW개발, 안전 분야 |

| | | | | |
|---|---|---|---|---|
| 전문가7 | 박사 | 12 | 시설물 분야 | • 정보보안, 시설물 관리 |
| 전문가8 | 기술사 | 22 | 정보통신분야 | • SW개발, 사업관리, SW품질 관리 |
| 전문가9 | 박사 | 12 | 재난안전 분야 | • 공공기관 안전 분야<br>• 개발기획및수행 |
| 전문가10 | 기술사 | 16 | 제품안전 분야 | • 제품 개발,안전/품질 관리 |
| 전문가11 | 기술사 | 20 | 시설물 분야 | • GIS 분야 개발 및 감리 |
| 전문가12 | 박사 | 12 | 에너지 분야 | • SW기획, 내부 관리, 발전소 안전 관리 |
| 전문가13 | 박사 | 20 | 교통 분야 | • 자동차, 철도 관련 SW 안전 |
| 전문가14 | 기술사 | 18 | 교통 분야 | • 선박, 쉽야드, 항공 분야 안전 |
| 전문가15 | 기술사 | 18 | 제품안전 분야 | • SW개발, SW품질 및 안전 |

그리고 SW안전 관리 현황 조사 대상을 선정에 앞서 <표 11>에서 정의된 4가지의 선정 기준을 전문가들과 같이 논의하여 도출하였다. 이 기준들을 가지고 우선 SW안전 현황 조사를 수행할 주요 분야를 선정하고, 선정된 주요 분야에서 세부 분야를 추가로 선정한다. 그 이유는 하나의 주요 분야 역시 다양한 산업 분야들이기 때문에 제한된 연구 기간을 고려하여 효율적인 조사를 위해서이다.

<표 11> 현황조사 대상 선정 기준

| 선정 기준 | 기준 설명 |
|---|---|
| SW 사고<br>발생 빈도 | • SW안전 사고의 자주 발생하면 그만큼 피해가 반복되기 때문에 발생 빈도가 높은 분야에 대한 SW안전 관리 현황 조사가 필요 |
| SW 사고<br>사회 파급력 | • 안전사고 발생 시 사고 규모가 크거나, 인명 피해 및 재산상 손실이 커서 사회적 파급력이 높은 분야에 대해 SW안전 관리 현황 조사가 중요 |
| SW 관련성 | • 全산업에서 SW에 대한 활용·의존도가 높아짐에 따라 안전과 관련된 SW 관련성이 높은 경우 SW안전사고 우려가 높기 때문에 해당 분야의 관리 현황 조사가 필요 |
| SW안전 관리<br>시급성 | • SW 적용 비율 증가로 인하여 사고 발생 가능성이 높은 분야일수록 SW안전관리 조사가 필요함 |

설문 문항별 답변은 5점 척도로 구성하여 각 설문 별로 매우 낮음(1)에서 매우 높음(5)로 응답을 받았다. 응답결과를 100점으로 환산하기 위해 각 점수 간 간격을 15점으로 하여 매우 낮음은 40점, 낮음 55점, 보통 70점, 높음 85점, 매우 높음은 100점으로 환산하였다. 이를 위해 아래와 같이 응답 결과를 변환하였다.

$$P = Min + \{ A \times (X - 1) \}$$
$$A = (Max - Min) / (k - 1)$$

Min : 최소값 (= 40)
A : 각 점수간 간격(= 15)
X : 전문가가 판정한 값 (= {1, 2, 3, 4, 5})
P : 환산 점수
X : 설문 결과 (해당 항목을 선택한 인원수)

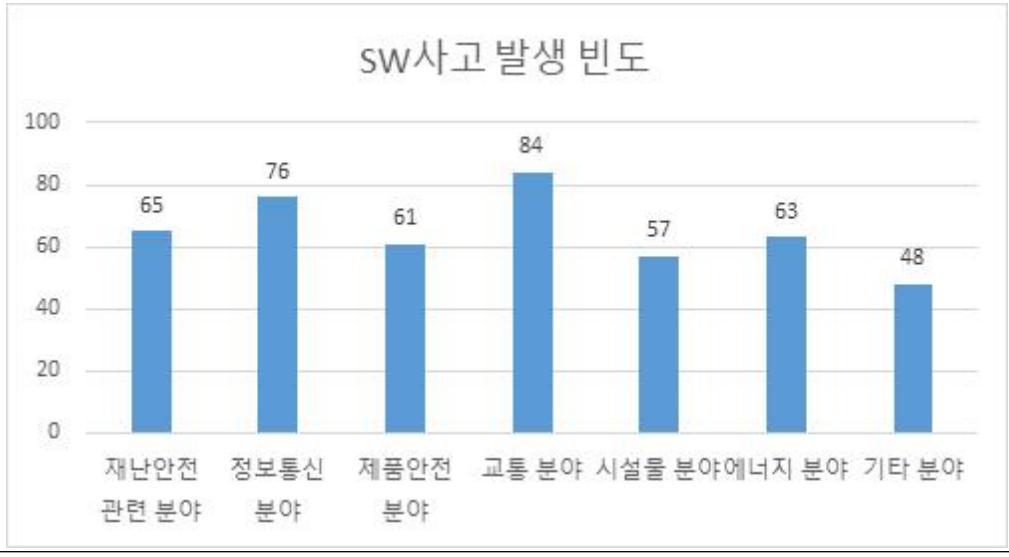
## 2. 현황 조사 수행을 위한 주요 분야 선정 결과

선정된 4가지 기준들(SW 사고 발생 빈도, SW사고 사회 파급력, SW 관련성, SW안전관리 시급성)을 중심으로 다양한 분야의 안전 전문가들의 설문을 실시하여 자동차, 선박, 철도, 항공 등이 포함된 교통 분야의 소프트웨어 안전관리 현황 조사가 중요하다는 다음과 같은 결과를 얻었다.

### ○ 주요 분야의 SW 사고 발생 빈도 설문 결과

SW 사고 발생 빈도에 대한 전문가 설문 결과에서 “교통 분야”가 84.0점으로 1위를 차지했고 이어서 “정보통신 분야”가 76.0 점으로 2위를 차지하며 SW안전사고의 발생 빈도가 높을 것으로 전문가들은 응답하였다.

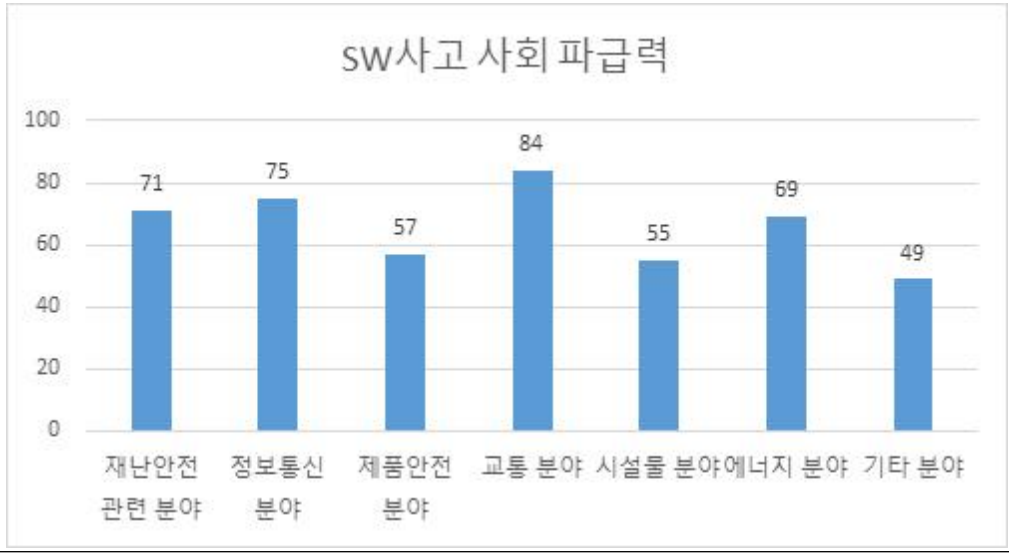
[그림 9] 주요 분야의 SW사고 발생 빈도 설문 결과




○ 주요 분야의 SW 사고 사회 파급력 설문 결과

주요 분야의 SW 사고 사회 파급력에 대한 전문가 설문 결과에서 “교통 분야”가 84점으로 1위를 차지했고 이어서 “정보통신 분야”가 75점으로 2위를 차지하며 안전 사고 발생 시 사회에 주는 영향도가 높을 것으로 응답하였다.

[그림 10] 주요 분야의 SW 사고 사회 파급력 설문 결과



○ **주요 분야 SW 관련성 설문 결과**

주요 분야의 안전사고 발생시 SW와의 관련성를 묻는 설문에서 전문가들은 “교통 분야”가 85점으로 1위를 차지했고 이어서 “정보통신 분야”가 76점으로 2위를 차지하는 것으로 응답하였다.

[그림 11] 주요 분야 SW 관련성에 대한 설문 결과


○ **주요 분야의 SW안전 관리 시급성 설문 결과**

주요 분야의 SW안전 관리가 얼마나 시급한지 묻는 설문에 대해 전문가들은 “교통 분야”가 84점으로 1위를 차지했고, 이어서 “정보통신 분야”가 71점으로 2위를 차지하여서 SW안전 관리가 시급한 분야들을 응답하였다.

[그림 12] 주요 분야 SW안전 관리 시급성에 대한 설문 결과


4가지 선정 기준에 대한 전문가 설문 조사 결과 4가지 모두 교통 분야가 1위를 차지하여 SW안전 관리 현황 조사를 위한 주요 분야로 교통 분야를 선정하였다. 실질적으로 교통 분야는 SW안전 개념을 산업적으로 활용하고 있는 자동차, 철도, 항공, 선박해양 분야를 포괄하고 있는 매우 광범위한 분야이다. 그리고 각 분야별로 SW안전과 관련된 국제 표준을 제정하여 SW안전 확보하기 위한 개발 절차를 정의하고 있기 때문에 타 주요 분야에 비교해 SW안전 관리가 수행되고 있는 분야라고 할 수 있다.

## 3. 현황 조사 수행을 위한 세부 분야 선정 결과

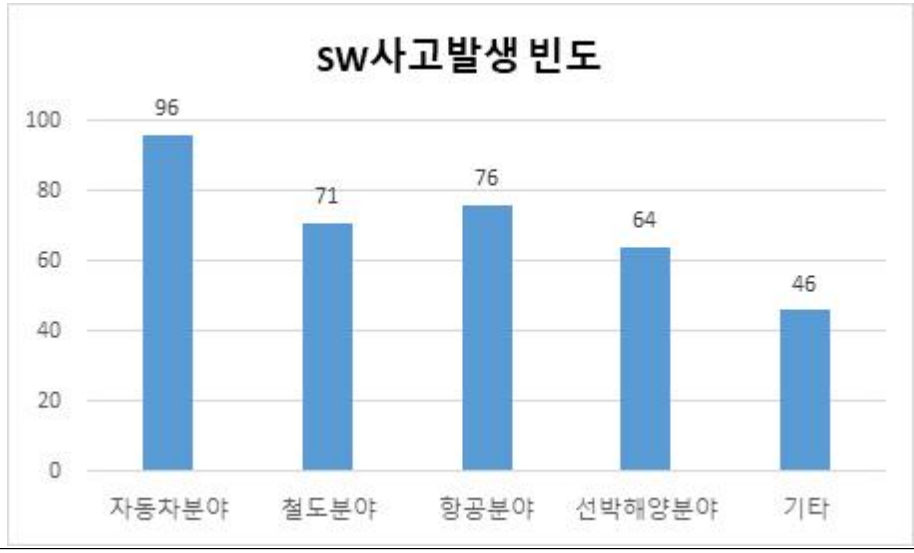
SW안전 관리 조사 수행을 위해 교통 분야도 광범위하기 때문에 제한된 연구 기간의 고려하여 세부 분야 선정을 위해 자동차, 철도, 항공, 선박/해양, 기타로 구분하여 앞서 정의한 4가지 기준들(SW사고 발생 빈도, SW사고 사회 파급력, SW 관련성, SW안전 관리 시급성)을 가지고 2차 전문가 설문 조사를 수행하였다.

### ○ 세부 분야 SW 사고 발생 빈도 설문 결과

교통 분야 중 SW사고 발생 빈도에 대한 전문가 설문 결과에서 “자동차 분야”가

96점으로 1위를 차지하고 이어서 “항공 분야”가 76점으로 2위였고 “철도 분야”가 71점으로로 높은 사고 발생 빈도가 예상된다고 전문가들이 응답하였다.

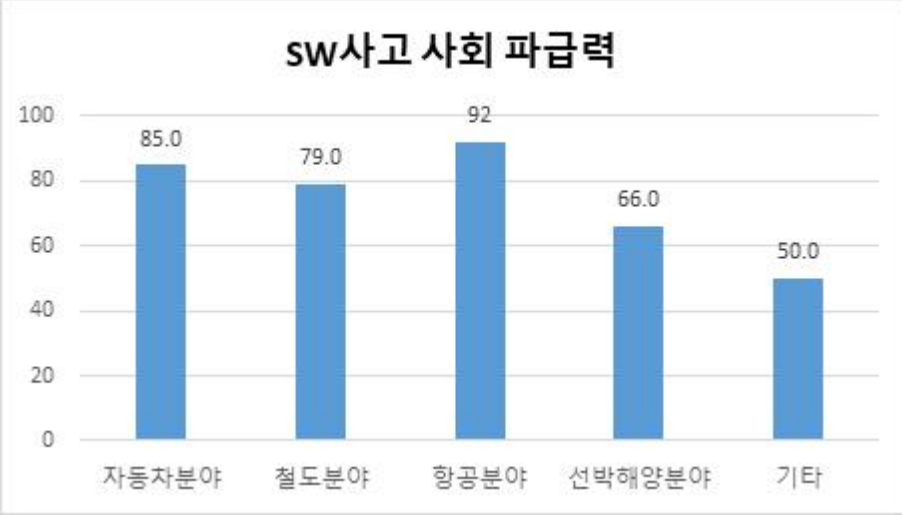
[그림 13] 세부 분야의 SW사고 발생 빈도에 대한 설문 결과




### ○ 세부 분야의 SW사고 사회적 파급력 설문 결과

교통 분야 중 SW사고 발생할 경우에 사회에 미치는 파급력에 대한 전문가 설문 결과 “항공 분야”가 92점으로 1위를 차지했고 이어서 “자동차 분야”가 85점으로 2위였으며 3위는 “철도 분야”로 79점 이었다. 이는 사고 발생에 따른 인명 손상 및 교통 분야의 사고에 대한 사람들의 인식을 알 수 있는 설문 결과이었다.

[그림 14] 세부 분야의 SWtk고 사회 파급력에 대한 설문 결과




○ 세부 분야의 SW 관련성 설문 결과

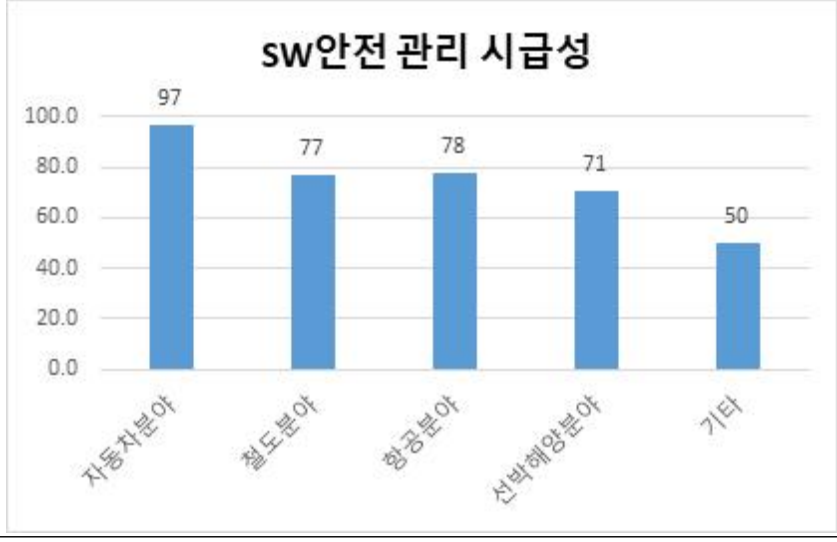
교통 분야 중 안전사고 발생시 SW 관련성에 대한 전문가 설문 결과 “자동차 분야”가 92점으로 1위를 차지했고 이어서 “항공 분야”가 88점으로 2위였으며 “철도 분야”가 81점으로 3위를 차지했다. 이는 최근 자율주행차로 인한 자동차 분야의 SW 활용의 증가와 보잉 737 맥스의 추락 사고로 인한 항공 분야의 SW에 대한 전문가들의 인식이 증가된 것으로 보인다.

[그림 15] 세부 분야의 SW 관련성에 대한 설문 결과


○ **세부 분야의 SW안전 관리 시급성 설문 결과**

교통 분야 중 SW안전 관리 시급성에 대한 전문가 설문 결과 “자동차 분야”가 97점으로 1위를 차지했고 이어서 “항공 분야”가 78점으로 2위였으며 “철도 분야”가 77점으로 3위를 차지했다. 이는 최근 자동차 분야의 자율주행 기술 발전으로 인해 조만간 우리의 일상생활에서 활용될 수 있기 때문으로 생각된다.

[그림 16] 세부 분야의 SW안전 관리 시급성에 대한 설문 결과



교통 분야의 SW안전 관리 조사를 위한 세부 분야 선정을 위한 전문가 설문 결과를 보면 4가지 선정 기준 모두 자동차, 항공, 철도 분야를 상위 3분야로 선정하였다. 이는 이들 세부 분야들이 평상시 사람들이 이용하는 주로 이용하는 교통수단이기 때문이라고 생각된다. 반면에 선박 분야 및 기타 교통수단은 우리의 삶과 밀접하지 않기 때문에 SW안전에 대한 인식이 상대적으로 부족하기 때문이라 생각된다.

# 제2절 프레임워크(안) 검증을 위한 SW안전 관리 현황 조사

앞에서 설계한 SW안전 관리 프레임워크(안)를 검증하기 위해 선정된 3가지 세부 분야에 대한 SW안전 관리 현황 조사를 수행하였다. 해당 현황 조사 범위가 매우 넓기 때문에 우선적으로 관련 분야의 안전 관련 법(자동차 분야 – 교통안전법, 자동차 관리법, 철도 분야 – 철도안전법, 항공 분야 – 항공안전법, 그리고 항공・철도 사고 조사법)을 위주로 현황 조사를 수행하고 전문가 자문을 통해 SW안전 관리 세부 사례를 고려하면서 실질적인 SW안전 관리 프레임워크(안)의 현실성을 검증하고 보완하였다.

## 1. 자동차 분야 소프트웨어 안전 관리 현황 조사

교통안전 연차보고서(2018)에 의하면 2017년에 216,335건의 교통사고가 발생하여 4,185명이 사망하고 322,829명이 부상을 당했으며, 2016년 대비 교통사고 수는 – 2.1%, 사망자 수는 – 2.5%, 부상자 수는 – 2.7%가 감소하였다. 도로에서 발생한 교통사고가 전체 교통사고의 98.8%, 전체 사망자의 95.4%, 전체 부상의 99.9%를 차지하고 있을 정도로 2017년 발생한 대부분의 교통사고는 도로에서 발생하였다. 사망 사고의 경우 대부분이 교통법규 위반(69.1%)이었다[11].

아직까지는 자동차 사고의 대부분이 SW와 무관한 원인으로 판별되며 실제로 SW가 원인인 사고는 별도로 통계가 잡히지 않고 있다. 하지만, 최근 팰리세이드 전복 사고[12] 같이 개인의 실수와 SW 구현 상의 이슈(일부 차종은 동일한 문제 발생시 시동이 꺼지지 않음)와 결합되어 있는 경우도 통계에 잡히고 있지 않다. 지속적으로 자동차의 작동에 SW 활용의 높아지고 있지만, 아직까지는 SW에 대한 관리가 고려되지 않는 현실을 반영한다고 할 수 있다.

이러한 현실에서 SW안전 관리 프레임워크(안) 검증 및 보완을 위해 자동차 분야의 안전 관리 현황 파악을 위해서 우선적으로 교통안전법, 자동차관리법을 중심으로 안전 관리 체계를 조사할 수밖에 없었다. <표 12>와 <표 13>는 해당 법들의 기본 체계로 이를 기반으로 SW안전 관리 프레임워크(안)을 활용하여 SW안전 관리 관점에서 조직 및

11) 2018년도 교통안전연차보고서, 2018, 국토교통부
12) 비상식적인 운전과 부주의가 초래한 팰리세이드 전복 사고, 2020.01.20.,, AutoHerald.

계획, 안전관리 활동, 안전관리 기반 조성에 대해 조사하였다.

<표 12> 교통안전법 기본 체계

| |
|---|
| 제1장 총칙 |
| 제2장 교통안전정책심의기구 |
| 제3장 국가교통안전기본계획 등 |
| 제4장 교통안전에 관한 기본시책 |
| 제5장 교통안전에 관한 세부시책 |
| 제6장 보칙 |
| 제7장 벌칙 |

<표 13> 자동차 관리법 체계

| |
|---|
| 제1장 총칙 |
| 제2장 자동차의 등록 |
| 제3장 자동차의 안전기준 및 자기인증 |
| 제3장의2 저속전기자동차에 대한 특례 |
| 제3장의3 내압용기의 안전관리 |
| 제4장 자동차의 점검 및 정비 |
| 제5장 자동차의 검사 |
| 제5장의2 자동차의 교환 또는 환불 |
| 제6장 이륜자동차의 관리 |
| 제7장 자동차관리사업 등 |
| 제7장의2 자동차안전기준 등의 국제조화 |
| 제7장의3 자동차서비스복합단지의 조성 등 |
| 제8장 보칙 |
| 제9장 벌칙 |
| 제10장 범칙행위에 관한 처리의 특례 |

### 1) 자동차 분야 SW안전 관련 조직 및 관리 계획

자동차 분야 안전 관련 기관/협회, 안전관리 조직(운송사업자) 등에 대해 먼저 알아보면 <표 14>와 같다. 자동차 분야는 도로, 차량, 부품, 정비 등의 다양한 분야에서 자동차 안전을 위한 조직들을 갖추고 있다.

그리고 이러한 조직들은 교통 안전에 관한 주요 정책 등을 심의 같은 업무를 수행하고 있다. 명시적인 SW안전 관리 업무가 들어나지 않았으나 전자식 변속 장치, 안전

운전 보조 기능, 첨단 스마트 운전자 보조 기능 등의 최근 SW가 포함된 자동차 부품의 증가 및 자동차의 SW 비중 증가에 따라 자연스럽게 SW안전 관리에 대응하고 있는 것으로 판단된다. 예를 들어 2016년 영동고속도로에서 발생한 봉평터널 사고 이후에 버스의 자동제동장치 차량 의무화는 SW를 활용하여 자동차 안전을 강화하는 대표적 사례라고 할 수 있다. 그리고 도로 상의 SW를 기반으로 한 다양한 인프라(구간 과속 단속 장치 등)를 활용한 안전 강화 정책들이 실행되고 있기 때문에 이들 조직들은 이미 SW안전 관리 조직이라고 할 수 있다.

<표 14> 자동차 안전 관리 기관 및 조직

| | |
|---|---|
| **안전 관련 기관/협회** | 한국도로공사, 한국교통안전공단, 한국자동차안전연구원, 한국자동차협회, 한국자동차부품협회, 전국고속버스운송사업조합, 전국택시운송사업조합연합회, 한국자동차정비사업조합연합회, 전국자동차검사정비사업조합연합회 등[13] |
| **안전관리조직 구성(운송사업자)** | 교통안전위원회, 교통안전관리 총괄책임자, 교통안전관리 부총괄책임자, 교통안전관리책임자, 교육홍보 담당, 지도단속담당, 교통사고담당, 운영정비담당, 배차업무담당 등 [14] |

또한, 이러한 관리 계획에 따라 조직간 역할 정의가 되어 있다. 기본적으로 안전관리 조직의 기능 및 역할은 교통시설설치 · 관리자의 의무, 교통수단 제조사업자의 의무, 교통수단운영자의 의무, 교통시설설치 · 관리자등의 교통안전관리규정, 교통안전진단기관의 등록, 변경사항의 신고, 결격사유 관리, 기관등록 등록의 취소, 행정처분 후의 업무수행, 교통시설안전진단 실시결과의 평가, 교통안전진단기관에 대한 지도 · 감독 등의 다양한 업무가 정의되어 있다. 이들의 역할 중에는 버스의 자동제어장치의 관리 역할 및 구간 과속 단속 장치 관리 등의 업무도 당연히 포함되어 있기 때문에 조직의 기능 및 역할 부분에 SW안전 관리가 행해지고 있다고 볼 수 있다.

자동차 분야의 안전관리 계획은 별도로 있지 않고 교통 분야에 포함되어 안전관리를 위해 국가교통안전기본계획, 국가교통안전시행계획, 지역교통안전기본계획, 지역교통안전시행계획, 교통시설의 정비, 교통안전지식의 보급, 교통수단의 안전운행의 확보, 교통안전에 관한 정보의 수집 · 전파, 교통수단의 안전성 향상, 교통질서의 유지, 위험물의 안전운송, 긴급 시의 구조체제의 정비, 손해배상의 적정화, 과학기술의 진흥, 교통

13) http://www.molit.go.kr/USR/WPGE0201/m_19475/DTL.jsp (국토교통부 관련 사이트)
14) 교통안전관리규정 포준모델 국토해양부 교통안전과

안전에 관한 시책 강구 상의 배려 등의 계획을 수립하고 있다.

제8차 국가교통안전기본계획[15]에 따르면, 자동차 분야는 도로부문 안전대책에 제시되어 있고 그 중 차량 및 안전관리체계 등에 관한 계획이 제시되어 있는데 이중에 SW와 관련된 안전 계획으로 첨단안전장치를 통한 능동적 사고예방 강화가 있다. 대형 차량 차선이탈경고장치, 비상제동장치 장착 의무화 및 차량 내 블랙박스, 후방감지 카메라 장착 유도하고, 졸음운전 등 운전자 부주의 모니터링 장치 및 S/W 기술 개발 등이 포함되어 있끼 때문에 자동차 안전 관리 측면에서 SW 역할이 중요해지고 있기 때문에 이들은 SW안전 관리 계획으로 볼 수 있다.

### 2) 자동차 분야 SW안전 관리 예방 활동

일반적으로 자동차 분야의 안전관리 활동은 주로 자동차, 버스, 화물차 등이 하드웨어 작동 위주로 SW로 통제되는 장치가 많지 않았다. 최근 발생한 대형 교통사고로 인하여 여객버스, 화물차 등은 SW로 제어되는 자동 제동 장치, 첨단 운전자 보조 장치(ADAS, Advanced Driver Assistance Systems) 등의 설치를 의무화하였다. 이는 사람이 야기할 수 있는 교통사고 가능성을 낮추게 함으로써 교통사고를 감소시킬 수 있다.

이외에도 <표 15>처럼 다양한 SW가 활용되는 자동차 안전장치 및 기능들이 있다. 국토교통부는 SW가 포함된 안전장비의 사고 예방을 위해 자동차 내 첨단전자식 안전장치에 대한 안전성 평가 확대, 자동차 내 첨단전자식 안전장치 개발 현황을 반영하여 지속적으로 평가 대상 장치를 확대하고 있다. 이러한 활동은 교통사고 예방을 위한 SW안전 관리 대상을 지정하고 있기 때문에 SW안전 관리 대상 활동이라고 할 수 있다.

<표 15> 자동차 관련 SW 활용 안전 장치 및 기능들

| | |
|---|---|
| **자동차 통제 대상장치** | 동력발생장치 및 동력전달장치, 주행장치, 조종장치, 조향장치, 제동장치, 완충장치, 연료장치 및 전기.전자 장치, 소음방지장치, 경음기 및 경보장치, 방향지시등 기타 지시장치, 후사경·창닦이기 기타 시야를 확보하는 장치, 속도계·주행거리계 기타 계기, 기타 자동차의 안전운행에 필요한 장치 등 |

15) 국토교통부(2016), 제8차 국가교통안전기본계획(2017_2021)

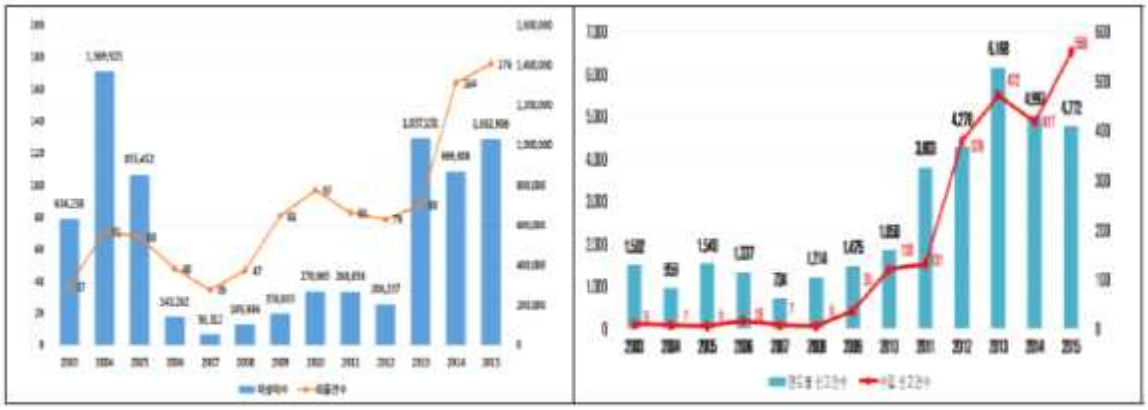
| | |
|---|---|
| **자동차 안전 기능** | 자동차안정성제어장치(ESC : Electric Stability Control), 제동 보조장치(BAS : Brake Assistant System), 비상자동제동장치(AEBS, Advanced Emergency Braking System), 타이어압력감지장치(TPMS : Tire Pressure Monitoring System), 차선이탈경고장치(LDWS : Lane Departure Warining System), 졸음방지장치(DDS : Drowsiness Detection System) 등 |
| **자율주행 관련 자동차 안전 기능** | 운전모니터링시스템(DMS, Driver Monitoring System), HMI-ADAS(지능형 주행보조 시스템), 운전자지원시스템(ADAS, Advances Driver Assistance System) 기술, 고속도로 자율주행 시스템(HDA, Highway Driving Assist), 혼잡구간 운행 지원 시스템(TJA, Traffic Jam Assist), 자동 긴급 제동 시스템(AEB, Autonomous Emergency Braking System), 자율주차(APS, Auto Parking System), 동적 맵, 3차원 정밀지도, 사용자 모니터링, 휴먼 팩터 기술, 차량과 차량과의 통신(V2V, Vehicle-to-Vehicle), 차량과 인프라와의 통신(V2I, Vehicle to Infra), 차량과 보행자간 통신(V2P, Vehicle to Pedestrian) 등 V2X(Vehicle to Everything) 기술 등 |

사업용자동차 운전자의 취약운전자를 대상으로 3D 기반 운전정밀 특별 검사를 시행하기 위해 추진하고 있으며, 교통안전공단은 개인별 맞춤형 교정교육 강화(실제 도로 환경이 반영된 첨단검사기법 적용)를 위해 3D 시뮬레이터를 7개소 24대 설치하여 안전관리를 강화하고 있다. 그리고 첨단 운전자 보조 장치 및 자동 제어 장치를 활용하는 차량의 운전자에게 해당 기능에 대한 설명과 유의사항을 위한 안내 및 교육도 진행하고 있다. 이러한 활동들은 사용자 역량 강화 활동의 일환이라고 할 수 있다.

SW안전 관리를 위한 안전 점검 및 조치 활동과 연계된 활동으로는 교통수단안전점검, 교통안전 특별실태조사, 교통시설안전진단, 교통시설안전진단 결과의 처리, 교통시설안전진단지침 수립 등이 있다. 실제로 여객버스 화물차에 포함되는 SW안전장치에 대한 안전 점검, 실태조사, 결과 처리, 안전진단지침 등이 SW 관련한 직접적인 안전 점검 및 조치 활동이다.

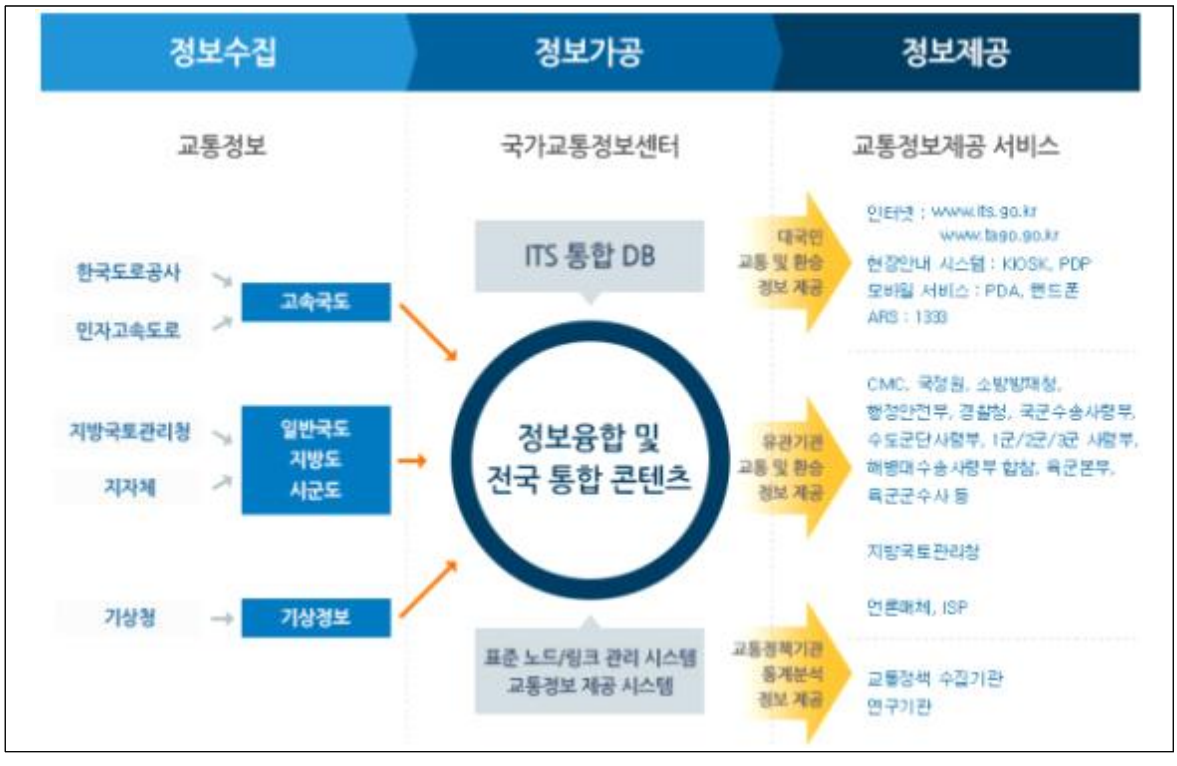
그리고 자동차의 제작결함시정(리콜) 제도를 운영하면서 자동차가 안전기준에 부적합하거나 안전운행에 지장을 주는 결함으로 인하여 소비자의 피해가 생기거나 또는 발생할 가능성이 있는 경우에 자동차 제작자 등이 결함과 관련된 사항을 소비자에게 통보하고 해당 자동차에 대한 수리, 교환, 환불 등의 적절한 조치를 취하도록 하고 있다. 이 제도는 [그림 17] 같이 많이 활성화 되어 있는 대표적인 자동차 분야의 조치 활동이다. 그리고 이 제도에는 SW 관련된 자동차 기능들이 포함되어 있기 때문에 SW 안전 관리 활동이라고 할 수 있다.

[그림 17] 연도별 자동차 리콜대수 및 소비자 결함 신고 건수



출처 : 국토교통부(2017), 제2차 자동차 정책 기본계획

[그림 18] ITS 국가교통정보센터(http://www.its.go.kr/) 서비스 예시




ITS 국가교통정보센터는 돌발사고 정보, 통제·공사 정보를 제공하여 운전자가 불의의 상황을 사전에 대비할 수 있도록 도움을 주어서 교통사고 예방에 기여를 하고

있다. 그리고 ITS와 연계한 자율주행기술 개발을 통해 교통 감소를 위한 예방 활동도 진행하고 있다. 이러한 활동은 대표적인 안전 예방 활동이라고 할 수 있다. 그리고 자동차 제작결함시정 조치를 운영함에 있어 소비자에게 원할한 정보 제공을 위해 국토교통부는 자동차리콜센터(https://www.car.go.kr/)를 운영하면서 소비자의 안전을 강화하기 위한 대비 활동으로 리콜 정보를 제공해 주고 있다. 이는 SW안전 현황 공개 활동이라고 할 수 있다.

### 3) 자동차 분야 SW안전 관리 대비 활동

자동차관리법에 의하면 자동차의 구조 및 장치, 사고기록장치의 장착 및 정보제공, 저속전기자동차의 안전기준, 신기술 등이 적용된 자동차 등의 관리, 자동차 안전기준 적합 여부에 대한 조사 등의 활동들이 있다. 현행 자동차 안전 기준의 주요 구성은 <표 16>과 같다. 이러한 안전 기준은 현행 자동차 자기인증제도를 통해 정부가 자동차의 안전에 대한 최소한의 가이드라인인 안전기준을 규정하고 제작자가 안전 기준에 적합하게 제작하여 자동차의 성능 및 안전을 확보하기 위한 제도이다. 이러한 안전 기준에 앞의 <표 15>에서 언급한 SW가 활용되는 안전장치와 기능에 대한 안전 기준들도 포함되어 있다.

<표 16> 자동차 안전기준 주요 구성

| |
|---|
| 제1장 총칙 |
| 제2장 자동차 및 이륜자동차의 안전기준 |
| 제1절 자동차의 안전기준 |
| 제2절 이륜자동차의 안전기준 |
| 제3장 제작자동차등의 안전기준 <개정 1997.1.17> |
| 제1절 총칙 <신설 2019.12.31> |
| 제2절 장치 등의 안전기준 <신설 2019.12.31> |
| 제4절 부품 등의 성능시험기준 <신설 2019.12.31> |
| 제3장의2 부품의 안전기준 <신설 2011.12.23> |
| 제4장 보칙 |

출처 : 자동차 및 자동차부품의 성능과 기준에 관한 규칙(2010.01)

자동차 분야 검사 및 인증 활동에는 자동차의 자기인증, 자동차부품의 자기인증, 자동차 자기인증의 면제, 대체부품의 성능·품질 인증, 대체부품인증기관의 지정 취소, 제작 결함의 시정, 자체 시정한 자동차 소유자에 대한 보상, 자기인증 자동차에 대한 사후관리, 자동차 또는 자동차부품의 자료 제공, 자동차의 안전도 평가, 자동차의 정비, 점검 및 정비 명령, 기계·기구의 정밀도검사, 자동차검사, 자동차 종합검사 등의 활동이 있다. <표 17>은 자동차 안전도 평가를 위한 분야별 평가 항목으로 해당 평가 항목에 전방 추돌 경고 장치, 차로 이탈 경고 장치, 좌석 안전띠 경고 장치 등 SW가 많이 활용되는 장치들에 대한 평가를 수행하고 있다. 이들 이외에도 자기 인증을 위한 검사 및 오류 점검을 위한 검사 등의 제도들이 갖추어져 있어 SW 안전 관리를 위한 대비 활동을 수행하고 있다.

<표 17> 자동차안전도평가 분야별 평가항목 (2018년)

| 분야 | '18년 평가항목 | 비고 | 분야 | '18년 평가항목 | 비고 |
|---|---|---|---|---|---|
| 충돌 안전성 | 정면충돌 | 여성운전자 평가 | 사고 예방 안전성 | 제동 | - |
| | | | | 주행전복 | - |
| | 부분정면충돌 | - | | 전방충돌경고장치 | - |
| | | | | 차로이탈경고장치 | - |
| | 측면충돌 | - | | 좌석안전띠경고장치 | - |
| | 기둥측면충돌 | - | | 비상자동제동장치 | 고속, 시가지, 보행자 평가 |
| | | | | 최고속도제한장치 | 조절형, 지능형 평가 |
| | 어린이 | 부분정면, 측면, 2열 착석 평가 | | 적응순항제어장치 | - |
| | 좌석 | - | | 사각지대 감시장치 | - |
| | | | | 차로유지 지원장치 | - |
| 보행자 안전성 | 보행자 | - | | 후측방접근 경고장치 | - |
| | | | | 첨단에어백 | - |

출처: 자동차안전연구원(2019), 2018년도 자동차안전연구원 연차보고서

자동차 이용자 보호를 위해 발전되는 SW가 포함된 안전 기능 활용이 증가되고 있다. 예를 들어 첨단기술 기반의 보행자친화형 횡단보도 설치 확대가 추진되고 있는데 이는 야간 및 보행자 교통사고 발생위험을 높은 환경에 이용자 안전을 위한 노력의

일환이다. 특히 스쿨존에서 자동차 속도를 측정하여 안내하는 전광판 역시 안전 운전을 유도하여 어린이의 안전을 확보하기 위한 이용자 보호를 위한 대비 활동이라고 할 수 있다.

특히 자동차에 사용되는 안전 중요 SW는 ISO 26262를 기반으로 자동차 관련 기업에서 적극적으로 활용되고 있기 때문에 SW 관련 기능을 개발함에 있어 위험 평가를 일부 수행하고 있다. 하지만, 이는 안전한 SW 개발을 위한 절차이지 SW안전 관리를 위한 절차라고 할 수 없다. 또한 현재 자동차 분야의 경우 명확한 SW안전 대응 매뉴얼과 훈련 활동을 가지고 있지 않은 것으로 알고 있다.

### 4) 자동차 분야 SW안전 관리 대응 활동

교통안전법과 자동차관리법에는 사고 발생 시 대응에 대한 직접적인 안전 활동이 포함되어 있지 않고 있다. 그 이유는 재난급 사고가 발생할 경우에는 재난안전법에 의해 대응이 이루어지고 교통사고의 경우 경찰 또는 보험사에 신고 절차가 있지만 이러한 절차들은 SW안전과 무관하다. 그리고 사고 초기에 SW안전 사고인지 확인이 불가능한 상황에서 SW안전사고 신고 및 통지 및 사고 대응 활동을 수행하기 어렵기 때문이다. 따라서 이에 대한 활동을 없는 것으로 간주한다.

### 5) 자동차 분야 SW안전 관리 복구 활동

교통사고 유발요인을 심층적으로 조사·분석하고 효과적인 교통사고 예방 대책을 제시하기 위해 1998년 12월 도로교통공단 내에 교통사고종합분석센터를 설치 운영하고 있다. 그리고 교통사고조사 기술지원, 대형교통사고 요인별 조사·분석 및 개선대책 수립, 도로 교통사고에 관한 교통안전정보관리체계 구축(GIS기반 도로교통사고 통합DB 구축) 등을 지원하고 있다. 하지만, 교통안전연차보고서에 의하면 SW로 인한 사고의 통계는 갖추어져 있지 않다. 이는 교통사고에 대해 조사 항목들이 원인분석과 개선대책보다는 가해자와 피해자 정의 및 행정처리가 주목적이기 때문이다. 따라서 SW안전 관리 복구 단계의 SW 사고 조사에 대한 국가적인 명확한 활동이 없다고 볼 수 있다.

재발 방지를 위한 안전 관리 활동으로 기존에는 위반행위에 대한 금지 조치, 위반

시 등록 취소, 지정취소, 중지명령, 인증 취소 등을 위한 청문 등이 있다. 그리고 제작결함시정(리콜) 제도를 통해 밝혀진 문제에 대해서는 시정하도록 하는 제도가 있기 때문에 원인이 밝혀진 문제에 대해서는 충분히 복구가 가능하기에 현 제도상에서 SW안전 관리를 위한 재발 방지 활동은 있는 것으로 볼 수 있다.

손해배상 관련한 안전관리 활동에는 자동차의 교환 또는 환불 요건, 하자의 추정, 과징금의 부과, 손해배상 수수료 등의 활동이 있다. 그리고 분쟁 조정을 위한 활동으로 제품 교환 또는 환불을 위한 중재 신청, 중재 판정에 따른 교환 또는 환불 방법, 자동차안전 · 하자심의위원회의 설치, 자동차안전 · 하자심의위원회 구성 및 운영, 중재부의 구성 및 운영 등의 활동들이 있다. 비록 이러한 활동들이 SW안전을 위한 활동들이 아니지만, 손해 배상의 원인 또는 분쟁 조정의 원인이 SW일 경우에는 충분히 활용이 가능하리라 본다. 따라서 SW안전 관리를 위한 복구 활동으로 볼 수 있다.

### 6) 자동차 분야 SW안전 기반 조성

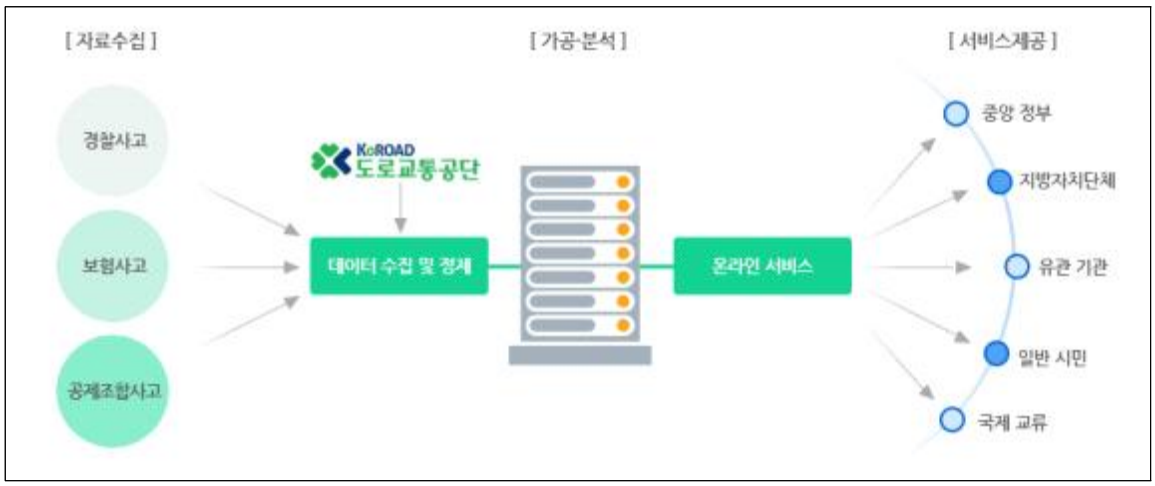
자동차 분야의 안전 문화 진흥 활동으로 교통안전 체험에 관한 연구 · 교육시설의 설치, 중대 교통 사고자에 대한 교육실시, 교통 문화 지수의 조사 및 활용, 교통안전 시범도시의 지정 및 지원 등의 활동이 있다. 그리고 최근 자율주행 관련한 시범 지구 지정 등의 수행되고 있기 때문에 SW안전 문화 진흥을 위한 활동이 있다고 할 수 있다.

자동차 분야의 SW안전 기술 개발 활동에는 안전기준 관련 연구 · 개발 등의 활동이 있다. 자율주행자동차 등 미래형 자동차 안전성 평가기술 개발 및 환경 구축, 안전도 검사기준(V2X 제어장치 등) 표준화 등에 대한 기술 개발을 지원하고 있다. 또한 인공지능 SW를 활용하여 졸음운전 방지장치 개발, 졸음운전 등 운전자 부주의 모니터링 장치 및 SW 개발 등 자율주행 및 스마트교통을 위한 다양한 연구들이 수행되고 있다.

자동차 안전 관리를 위한 안전정보 공통 활용 활동으로는 교통사고 관련자료 등의 보관 및 관리, 교통안전 정보 관리체계의 구축, 자동차 관리 업무의 전산 처리, 자동차 이력관리 정보의 제공 등이 [그림 19]처럼 수행되고 있다. 이 정보 중에는 손해보험사들의 자동차 보험요율 조정에 활용되는 첨단안전장치 보유 정보와 교통사고 통계 분석에 활용된다. 이와 같은 분석으로 첨단안전 장치가 교통사고를 줄이는데 효과적이라는 분석이 있었다. 비록  SW안전 관점에서 교통사고 관련 자료의 관리가 되고 있지 않지만, SW안전 관련 정보 관리 시스템이 구축은 일부 이루어지고 있다고 할 수 있

다.

[그림 19] 교통사고DB 구성체계 (TAAS)




출처 : 교통사고분석시스템(http://taas.koroad.or.kr), TAAS소개 / 주요서비스

### 7) 자동차 분야 소프트웨어 안전 관리 현황 및 한계점

자동차의 전자화 및 첨단화로 인하여 자동차에서 SW 비중이 지속적으로 증가하고 있다. 이로 인한 SW 결함이 많아지고 있으며 대표적으로 급발진 사고의 원인으로 SW 결함이 의심받고 있다. 하지만, 아직까지 자동차 사고의 다수는 SW 결함을 원인으로 보고 있지 않기때문에 자동차 분야에서 SW를 직접적으로 관리하는 법 제도 체계는 마련되어 있지 않다. 따라서 본 현황 조사에서도 SW안전 관리 프레임워크(안)을 만들어 이를 기반으로 자동차 분야의 SW안전 관리 현황 조사를 수행하여 [그림 20] 같은 자동차 분야 SW안전 관리 현황을 얻을 수 있었다.

안전 조직 및 관리 계획 분야에 SW안전 관리를 위한 조직(교통안전관리 기관, 교통안전관리 조직 등) 수립, 조직 및 담당자(관리자, 사업자, 운영자, 대행자 등)의 기능 및 역할 정의, 안전 관리 계획(국가차원/지역차원 안전 기본 계획, 안전성 향상, 안전 정보 수집, 등) 부분에 대한 구성 및 활동이 교통안전법, 자동차관리법, 도로교통법 등에 제시가 되어 있다. 그리고 현 체계 내에서 명시적이지 않지만 SW안전에 대한 대응이 이루어지고 있었다.

[그림 20] 자동차 분야 SW안전 관리 현황


안전관리 활동 분야는 예방활동 단계로 정의한 안전 관리 대상으로 여러 자동차 중에 여객버스, 화물차 등은 소프트웨어가 포함된 안전장치를 의무화하고 그 내용을 운행회사에서 보고하게 되어 있는 등의 SW안전 관리 대상이 있었다. 그리고 이에 대한 종사자 자격 및 교육 과정이 있고, 이에 대한 안전 점검도 수행되고 있었다. 특히 자동차 제작결함시정(리콜) 제도로 인하여 많은 SW 문제들이 리콜 형태로 개선되고 있음을 알 수 있었다. 또한 안전 현황 공개에 대해서는 ITS 시스템을 구축하여 안전 정보를 공유하고 자동차리콜센터를 운영하면서 SW관련 리콜 정보도 공유되고 있었다.

대비 단계에서는 이미 다양한 첨단 기능에 대한 안전 기준이 정립되고 있으며 이에 대한 검사를 수행을 통한 자체 인증 제도가 마련되어 있었다. 그리고 이용자 보호를 위한 다양한 SW 기능 안전 시스템들이 구축되어 있었다. 하지만, 위험 평가가 대응 매뉴얼 및 훈련에 대한 명확한 노력에 대해서는 확인하지 못하였다. 그리고 대응 단계에서 이루어지는 사고 신고 및 통지와 사고 대응에 관련해서는 자동차 안전 측면에서는 있었으나 SW안전과 관련되어 있다고는 볼 수 없었다.

복구 단계에서는 교통 고에 대한 조사가 이루어지고 있지만 SW안전 관련된 사고조사는 명시적으로 이루어지고 있다고 보기 어려웠다. 하지만, SW 문제에 대한 재발 방

지는 손해 배상, 분쟁 조정을 기존 절차에 의해 이루어지고 있다고 할 수 있다. 실제로 급발진 같은 SW로 인한 사고로 의심되는 경우에 대해서도 제대로 된 원인 분석이 이루어지지 않는다는 의견이 있지만, 이에 대한 손해 배상 및 분쟁 조정 절차는 이루어지고 있기 때문이다. 그리고 급발진 관련된 문제에 대해서는 최근에는 이슈화되지 않는 것으로 보면 일정 부분 재발 방지가 이루어진 것으로 볼 수 있다.

안전 기반 조성 분야는 자율주행 같은 새로운 SW안전과 연관된 교육과 홍보가 꾸준히 이루어지고 있고 관련 기술 개발도 정부의 투자로 원활하게 이루어지고 있다. 이에 관련한 국제 협력도 추진되고 있었다. 또한 첨단안전장치에 대한 정보를 활용하여 버스 같은 대형차량의 경우 자동제동장치 의무화 같은 절차도 실행되고 있었다.

본 보고서에서 처음 개발된 SW안전 관리 프레임워크(안)을 기반으로 자동차 분야의 SW안전 관리에 대한 전반적인 조사를 수행하였지만, 이에 대한 한계점도 명확히 존재한다. 우선 자동차 분야의 전체적인 상세 조사를 하지 못한 한계가 존재한다. 이는 자동차 산업이라는 거대 산업에 대한 상세 조사가 필요한데 예산과 연구 기간의 한계와 SW안전 관리 프레임워크라는 매우 넓은 범위의 조사 수행으로 인하여 개별 활동별 명확한 상세 조사의 어려움이 있었다. 하지만 이러한 문제로 인하여 프레임워크(안)을 먼저 설계하고 SW안전 관리 활동에 대한 Top-Down 방식의 조사를 수행하여 SW안전 관리 프레임워크 제시를 위한 목적은 달성하였다.

자동차 분야의 SW안전 관리는 재난안전법의 예방-대비-대응(응급조치)-복구(사후관리) 관점과는 달리 예방과 대비를 명확히 구분하기 어려웠으며 사고 전에는 주로 안전한 자동차 및 부품을 개발하고 이를 얼마나 효율적으로 인증하는지가 중요한 요소이었다. 그리고 사고발생 후에는 피해를 최소화하기 위한 빨리 부상자를 의료체계에 넘기는 절차가 필요하다는 의견이 제기되었으며, SW안전사고 원인 조사에 대한 명확한 절차 마련이 필요하다는 의견도 있었다. 그리고 자동차 분야에서 SW안전 관리 현황 조사가 필요한 분야로 공용 운송 수단(버스, 트럭 등)으로 제기되었다.

다음은 자동차 분야 SW안전 관리 현황 조사를 수행함에 있어 전문가 자문 및 심층 인터뷰를 수행한 결과 자동차 분야의 SW안전 관리에 대해 다음과 같은 다양한 의견들이다.

- 자동차 분야에서 SW안전 관리가 중요한 분야는 우선적으로 버스, 트럭 등 공용 운송 수단으로 이들은 이미  차선이탈, 앞차 경보, 속도 제어 등 SW가 포함된 장치가 장착되어 있으며 운행 기록을 운송사업자가 관리하고 있고 도로 위의 상황을 ITS으로 파악할 수 있기 때문에 SW안전 관리를 공용 운송 수단을 중심으로 구축할 필요가 있음
- 반면에 SW안전 관리 측면에서 자주 언급되는 자율주행차의 경우 상용화 시기에 대해서는 다양한 의견들이 있으며 자율주행 4-5 단계가 되기 위해서는 인프라와 상호 연동이 필요하므로 SW 중요성이 강조됨에도 아직까지는 불완전한 자율주행 수준(3레벨)를 벗어나지 못하고 있음
- 테슬라가 5레벨을 조기에 적용한다고 하지만, 미국처럼 국토가 넓고 차량 통행이 적은 경우에 가능하며, 한국 같이 차량이 밀집된 환경에서는 5단계 자율주행 구현이 매우 어려울 것이기에 맹목적인 환상을 갖기보다는 안전에 대한 지속적인 관심과 연구가 필요함
- 항공 분야의 안전 기술이 다른 분야 보다 앞서 있기 때문에 항공 분야의 검증된 기술이 도로교통 분야로 내려오고 있으며 SW 관련 분야도 유사함
- 제한된 운영 방식의 항공과 철도 분야와 달리 자동차 분야는 고려해야 할 요소들이 많기 때문에 SW안전 관련 기술이 더 많이 발전되어야 하며 따라서 이에 대한 많은 연구가 필요함
- 유럽은 자동차(버스)는 사고가 발생하면 관리자(버스회사)에 연결해주는 이콜이라는 시스템을 의무화하고 있기 때문에 사고시 응급 대응을 빠르게 할 수 있도록 하고 있지만 국내는 승용차에서 비상 상황에서 쉽게 신고할 수 있는 기능을 옵션으로 선택해야 함
- 사고 데이터 관리에 있어서 개인정보 차원에서 접근에 대한 권한을 강하게 통제해야 하지만. 비행기의 블랙박스와 같이 사고 원인 분석을 위한 장치들은 의무화 할 필요가 있음

## 2. 철도 분야 소프트웨어 안전 관리 현황 조사

교통안전연차보고서(2018)에 의하면 2017년에 발생한 철도 관련 사고는 87건으로 51명이 사망하고 30명이 부상을 당했으며, 2016년 대비 철도사고 수는 - 9.46%, 사망자 수는 - 12.1%, 부상자 수는 - 23.1%가 감소하였다. 주요 사고 원인은 열차 충돌, 탈선, 화재, 위험물 누출 등으로 인한 운행 중단이었지만, 건널목에서의 열차 사고 같은 인명의 손상을 가져오는 사고도 있었다. 2018년에 발생한 강릉선 탈선 사고의 경우 신호기계실의 잘못된 케이블 연결로 인한 선로 전환시스템 오작동으로 열차 탈선이 발생하였고 16명이 부상을 당하였다.

철도 운행의 효율화를 위해 도입된 SW 기반 다양한 시스템들로 인하여 철도 안전에 미치는 SW의 영향력은 갈수록 커지고 있다. 2011년 신분당선을 개통하면서 도입된 철도 무인 차량은 점차적으로 확대되고 있다. 이와 같이 과거 사람이 관리하던 안전이 SW가 관리하는 체계로 변화되기 때문에 철도 분야의 SW안전은 더욱 중요해지고 있다.

SW안전 관리 프레임워크(안)의 검증과 보완을 위해 철도 분야의 현황 조사를 우선적으로 철도안전법과 항공·철도 사고조사에 관한 법을 중심으로 SW안전 관리 현황을 조사하였다. <표 18>과 <표 19>는 해당 법들의 기본 체계이며 이를 기반으로 SW안전 관리 프레임워크(안)을 활용하여 SW안전 관리 관점에서 조직 및 계획, 안전관리 활동, 안전관리 기반 조성에 대해 조사하였다.

<표 18> 철도안전법 체계

| |
|---|
| 제1장 총칙 |
| 제2장 철도안전 관리체계 |
| 제3장 철도종사자의 안전관리 |
| 제4장 철도시설 및 철도차량의 안전관리 |
| 제5장 철도차량 운행안전 및 철도 보호 |
| 제6장 철도사고조사·처리 |
| 제7장 철도안전기반 구축 |
| 제8장 보칙 |
| 제9장 벌칙 |

<표 19> 항공 · 철도 사고조사에 관한 법 체계

| |
|---|
| 제1장 총칙<br>제2장 항공 · 철도사고조사위원회<br>제3장 사고조사<br>제4장 보칙<br>제5장 벌칙 |

### 1) 철도 분야 SW안전 관련 조직 및 관리 계획

철도 분야 SW안전 관리 현황 조사에 앞서 철도 분야의 SW 중요성 및 관련성을 알아보기 위해 철도안전 관련 기관 및 철도 관련 종사 업무를 알아보면 <표 20>과 같다. 관련 기관들을 보면 국토교통부를 포함하여 많은 기관들이 참여하고 있을 정도로 안전 관련한 다양한 업무들이 있다. 대부분 시스템이 SW 기반으로 동작(모니터링, 제어, 통제 등)하고 있기 때문에  열차 운전, 정비, 운전관리, 철로, 관제 등 많은 종사자들의 업무에서 SW와 연관되고 있다.

비록 철도 분야의 법 제도 체계에서 SW안전 관리가 명시적으로 들어나지 않지만 SW 기반 시스템 및 제어가 많기 때문에 SW안전 관리가 중요하다고 할 수 있다. 대표적으로 2018년 철도안전 시행계획에는 SW를 적극 활용하여 철도 사고의 주요 원인인 사람의 실수를 예방하기 위한 안전 설비인 ATP(Automatic Train Protection)[16], 안전측선[17] 등의 설치를 확대하는 계획을 담고 있다.

<표 20> 철도 안전 관련 기관 및 관련 종사 업무

| | |
|---|---|
| **철도 안전관련 기관** | 국토교통부, 항공철도조사위원회, 교통안전공단, 철도기술연구원, 안전업무지정기관(신체검사/적성검사/교육훈련/자격인증/철도용품인증/차량성능시험/차량제작검사/차량정밀진단), 철도시설공단, 철도운영기관, 철도시설/차량제작사[18], 등 |
| **철도 종사자** | 운전업무종사자, 관제업무 종사자, 승무원, 역무원, 시스템 작업책임자, 철도운행 안전관리자, 등 |

16) ATP(Automatic Train Protection, 열차자동방호장치), 열차가 일정속도 이상을 초과하여 운행 시 자동으로 감속·제어하는 장치
17) 안전측선 : 단선구간에서 열차가 교행할 경우 열차가 대기할 수 있는 측선
18) http://www.molit.go.kr/USR/policyData/m_34681/dtl?id=438 (국토교통부 철도안전관리체계) 참조

철도 분야 안전 관리를 수행하는 조직들의 체계는 [그림 21]과 같다. 국토교통부를 중심으로 하여 철도 안전 시책 마련, 안전 계획 및 관련 규정 승인을 위한 목표 설정, 철도안전 시설의 확충, 개량 및 점검관련 사항, 철도차량 정비 및 점검 관련 사항, 철도안전 관련 제도개선 사항, 철도안전 관련 종사자의 교육 훈련 사항, 철도안전관련 연구 및 기술개발 관련 사항 등을 수행하고 있다. 이들 안전 관련 업무에는 당연히 SW안전 관련 업무를 포괄하여 계획을 세우고 수행하고 있기 때문에 철도 관련 SW안전 관리 조직, 관련 기능 및 역할 정의, 안전 관리 계획 등이 실행되고 있다고 판단할 수 있다.

[그림 21] 철도 안전관리체계 조직도


출처 : http://www.molit.go.kr/USR/policyData/m_34681/dtl?id=438 (국토교통부)

### 2) 철도 분야 SW안전 관리 예방 활동

철도 분야는 안전관리를 위해서 다양한 시스템들을 구축해서 운영하고 있다. 예를 들어 철도차량 운전면허 관리시스템, 철도자격 관리 시스템, 철도사고 통계분석 관리 시스템, 종합 안전심사 업무관리 시스템, 철도안전 종합계획 실적관리 시스템, 철도안전 정책지원 분석시스템 등이 있다. 이러한 시스템들을 구축하여 철도 차량 운전면허를 관리하고 철도 자격을 관리한다는 의미는 그 자체로 이미 안전 관리 대상을 지정하고 체계적으로 관리하고 있다는 것으로 해석 가능하다. 이들 업무 이외에도 신호 제어 시스템, 선로 관리 시스템 같은 운영에 관련된 시스템들도 구축되어 있고 이들 시스템들이 SW 기반으로 동작한다는 것을 감안하면 SW안전 관리 대상이 지정되어 있다고 볼 수 있다.

그리고 철도 분야의 다양한 시스템들은 안전과 매우 밀접하며 실제로 사고 발생시 인명 손상 및 재산상 피해가 크기 때문에 평상시 철도 시스템을 운영하는 종사자들에 대한 엄격한 교육과 자격 제도를 유지하고 있다. 대표적으로 철도차량 운전면허를 획득하지 않고서는 철도 차량을 운행할 수 없다. 철도 차량을 운전하는 사람에 대해 철도차량 운전면허를 발급하고 운전면허를 발급할 수 없는 사람에 대한 결격 사유를 제시하고 있다. 면허를 받기 위해서는 신체검사를 합격해야 하는데 이를 위한 의료기관을 지정하고 있다. 운전 적성 검사를 실시하기 위해 운전적성검사 기관을 지정하고 위반 시 정지 및 취소 사항을 제시하고 있다.

또한 종사자의 기본안전 수칙 준수를 의무화하고 전사적 안전모니터링 도입(서울도시철도 사례)하고, 우수 사례(Best Practice) 워크숍 및 경진 대회 등을 통해 철도 분야의 안전을 위한 노력을 하고 있다. 특히 철도운영자는 고용하고 있는 철도종사자에 대한 정기적인 안전 교육을 실시해야 하고 철도차량 정비 기술자는 인정 기준을 만족해야 하며, 정비교육훈련을 주기적으로 이수해야 한다. 이와 같이 철도 분야는 종사자 자격 및 교육에 대한 관리 활동을 철저히 하고 있다.

철도 분야는 다양한 SW 기반 안전 시스템들을 관리하기 위해 주기적인 안전 점검 활동을 하고 있다. 그리고 철도운영자등에 대한 안전관리 수준평가, 점검 결과에 따라 수준 미달 시 우수운영자 지정의 취소 등의 조치 활동을 병행하고 있다. 이러한 활동들은 우리가 안전하게 철도를 이용할 수 있는 근간이 되고 있다. 또한 활동의 수행 결과에 대한 현황 공개와 함께 철도안전 우수운영자를 지정하여 혜택을 제공하고 있다.

철도 분야는 철도 사고가 발생하면 운행 중단 및 인명 사고가 발생하기 때문에 쉽게 사회 문제화 되므로 사고 정보를 숨기기 어려우며 사회적 영향을 고려해서 많은 정보를 공개하고 있다. 대표적으로 철도안전 정보 포탈과 철도안전 정보 통합DB를 통해 정보를 관리 공개하고 있다.

이와 같은 사례들로 종합해 보면 기존의 철도 분야에서 SW안전에 대한 예방 활동들을 위한 안전 관리 대상 지정, 종사자 자격 및 교육, 안전 점검, 안전 현황 공개가 수행되고 있다고 볼 수 있다.

### 3) 철도 분야 SW안전 관리 대비 활동

국가 차원의 철도 안전관리 기준은 국토교통부에서 제시하고 이에 따른 세부 안전관리 기준은 철도운영자가 수립하여 시행하고 있다. 이를 위해 철도운영자가 수립한 안전관리 체계는 교통안전공단(권한위탁)의 검토 후 국토교통부에서 최종 승인한다. 이 과정에서 철도차량 및 용품 구매 시 형식승인을 받도록 하고 있고, 형식승인 검사는 철도기술연구원(권한위탁)이 수행하고 형식승인증명서는 국토교통부가 발행하게 되어 있다. 그리고 철도차량 운전면허 관련 기준은 교통안전공단(권한위탁)이 수립하고 면허교육 및 시험기관은 국토교통부가 지정(서울교통공사, 코레일 인재개발원, 우송대 등)하여 수행하고 있다.

이러한 시스템, 차량, 부품에 SW가 포함되어 있기 때문에 형식 승인을 위해서는 SW 안전 관련된 기준들이 철도차량 형식승인, 철도차량 제작자승인, 철도차량 완성 검사, 철도용품 형식승인, 철도용품 제작자승인, 형식승인 등의 사후관리, 종합시험 운행, 철도차량의 개조, 철도차량의 이력관리, 철도차량정비, 철도차량 정밀안전진단, 철도 교통관제, 영상 기록 장치의 장착 등을 위해 일부 포함되어 있다.

예를 들어 철도 차량 기술 기준에 <표 21>처럼 SW 인증 관련 기준이 포함되어 있으며 이를 가지고 형식 승인이라는 인증 제도를 운영되고 있다. 그리고 2016년에 한국철도기술연구원이 철도 안전 분야 국제공인 제품 인증기관으로 인정받아 IEC 62279를 기반으로 철도 부품에 대한 SW 안전성에 대한 국제 수준의 인증이 시작되었다.

<표 21> 철도차량 기술기준 Part 31 - 소프트웨어 인증 기준

| |
|---|
| 3.2.7.1 소프트웨어 안전<br>8) 신청자는 소프트웨어 안전확보를 위해 철도소프트웨어에 대한 국제표준 IEC 62279를 기반으로 안전활동을 하여야 한다. |

출처 : 철도차량 기술기준 - Part 31_고속철도차량 기술기준

이용자 보호를 위해 기존 철도 안전 관리 활동으로 여객 열차에서의 금지 행위, 여객 등의 안전 및 보안, 보안 검색 장비의 성능 인증, 시험기관의 지정, 직무 장비의 휴대 및 사용 등이 마련되어 있다. 그리고 이러한 활동들의 효과적인 지원을 위해 SW를 활용한 직무 장비, 안전관리 시스템, 안전경고 시스템 등이 마련되어 있기 때문에 SW를 활용한 이용자 보호 관리가 실행되고 있다.

철도안전 관리 체계 내에서 위험 관리 수행이 정의되어 있지만 이러한 활동들이 안전 관리의 대비 단계의 주요 활동인 SW안전 위험 평가와는 같은 활동이라고 할 수 있는 구체적인 철도 분야의 SW안전 위험 평가 활동들을 찾을 수 없었다.

철도 분야 SW안전을 위한 대응 매뉴얼과 훈련과 관련된 활동들로는 운전 교육 훈련 기관의 지정 정지 및 취소 절차가 있다. 또한 철도 교통 관제사들의 관제 교육 및 훈련을 통한 관제 자격 증명시험 제도가 있고 철도차량 정비 기술자는 주기적인 정비 교육 훈련을 받아야 하며 차량 운전자를 포함한 철도 종사자들에 대한 정기적인 안전 교육이 있다 따라서 차량 운행 및 철도 운영 시스템의 갑작스런 오류에 대한 대응 매뉴얼과 훈련이 진행되고 있다고 볼 수 있다.

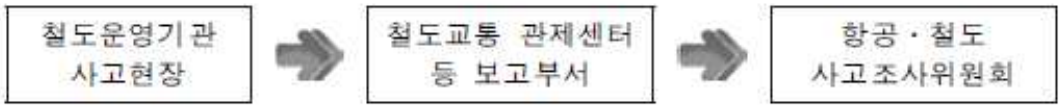
이와 같은 사례들로 종합해 보면 기존의 철도 분야에서 SW안전에 대한 대비 활동으로 안전 기준 지정, 차량 및 부품 인증, 이용자 보호, 대응 매뉴얼 및 훈련 등의 활동 등이 수행되고 있지만, 위험 평가에 대해서는 명확한 활동이 없는 것으로 판단된다.

### 4) 철도 분야 SW안전 관리 대응 활동

철도 분야는 항공 분야와 같이 사고 조사를 위한 법인 항공·철도 사고 조사를 위한 법이 제정되고 있다. 해당 법에 의하면 철도 사고의 경우 사상자가 많은 대형사고의 경우 철도운영자가 즉시 국토교통부 장관에게 보고하도록 되어 있으며 철도운영자 또

는 종사자는 사고 사실을 지체 없이 사고조사위원회에 통보해야 한다고 규정되어 있다.

[그림 22] 철도사고 보고 체계




출처: 국토교통부(2019), 2019년도 교통안전연차보고서

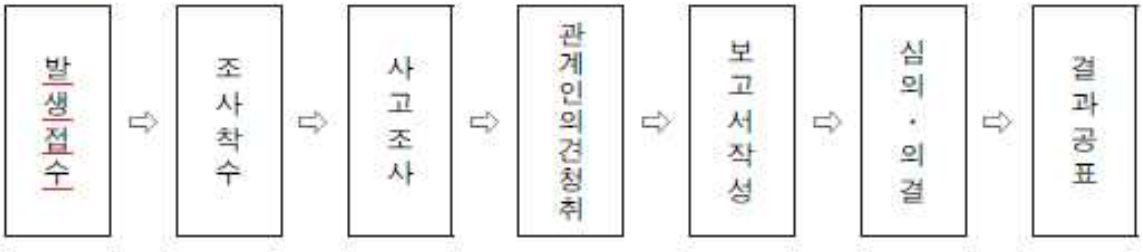
그리고 재난 및 안전 관리 체계에 의해서 비상 대응 계획에 따라 철도운영자가 사고 조치, 유관기관과의 협조 등 필요한 조치를 수행하도록 되어 있기 때문에 비상 대응 활동은 재난안전법 체계에서 수행된다고 할 수 있다.

비록 항공·철도 사고 조사를 위한 법이 SW안전을 위한 법은 아니지만 SW 오류로 발생한 사고의 경우도 동일한 절차에 따른 대응이 필요하기에 SW안전사고 신고 및 통지 활동도 동일하게 적용된다고 볼 수 있다. 다만, 사고 대응 관련한 부분은 SW안전 보다는 재난안전 관점에서 수행되기 때문에 SW안전 관리와 무관하다고 할 수 있다.

### 5) 철도 분야 SW안전 관리 복구 활동

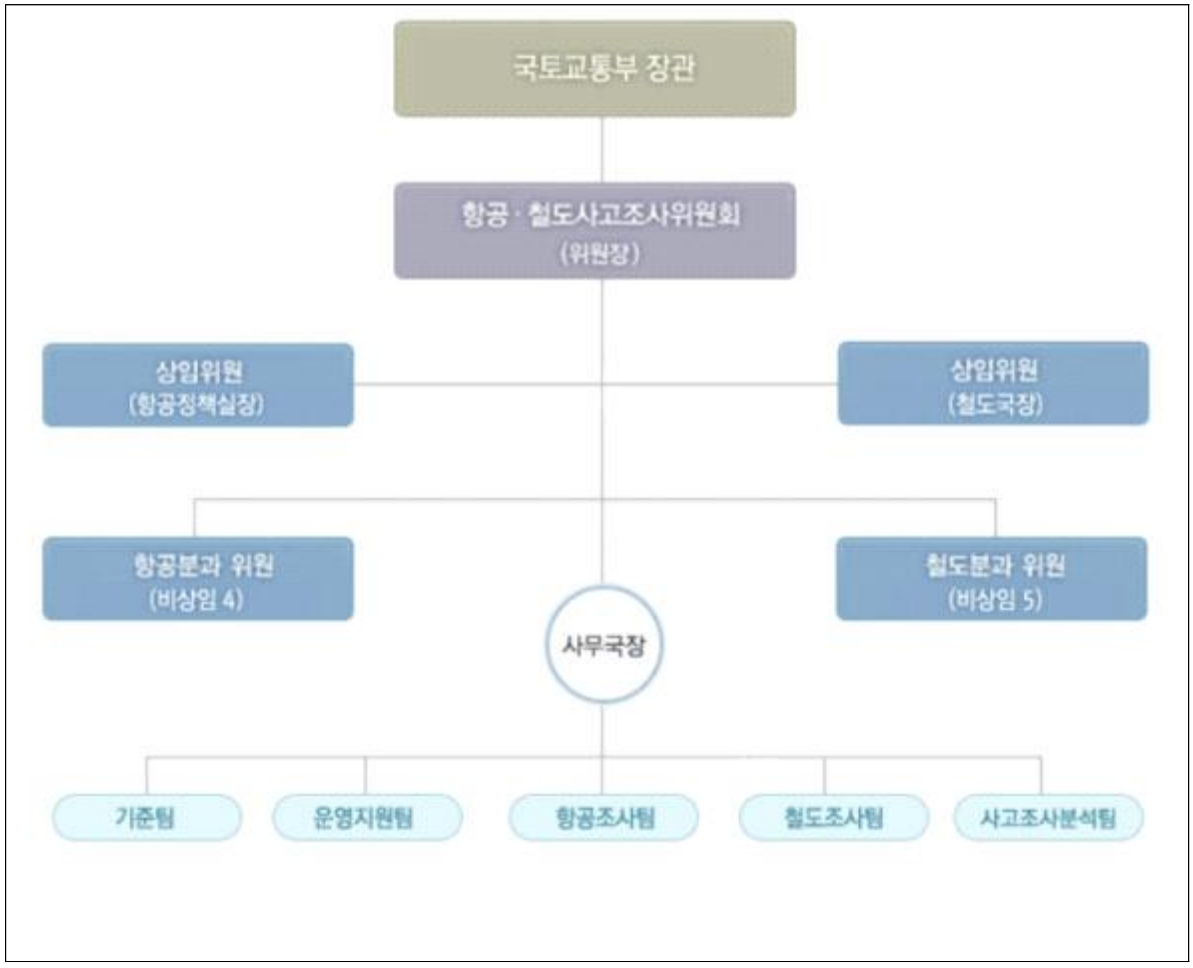
철도 분야 SW안전 관리 대응 활동에서 철도 분야는 사고 발생시 항공·철도 사고조사를 위한 법에 의해 철도운영자가 국토교통부에 보고하게 되고 3명 이상의 사상자가 발생하거나 5천만원 이상 재산 피해가 발생할 경우에는 국토교통부 항공철도조사위원회에서 사고 원인 규명을 위해 조사가 수행된다.(사고원인 규명, 유사 철도사고 예방 및 안전 확보 방안[안전권고 등]) 항공·철도 사고조사를 위한 법에 의한 사고 조사 절차는 [그림 23]과 같은 절차에 따라 수행된다.

[그림 23] 항공철도사고조사위원회 사고조사 절차




출처: 국토교통부(2019), 2019년도 교통안전연차보고서

[그림 24] 항공철도사고조사위원회 조직도




출처: 철도항공사고조사위원회(https://araib.molit.go.kr/) 조직도

항공·철도 사고조사에 관한 법에 의하면 사고조사위원회[19]는 [그림 24]와 같이 구

19) 위원회는 위원장 1명과 위원 11명으로 구성하되, 위원장은 비상임으로 하고, 위원 중 2명은 상임으로 한다. 상임위원은 항공정책실장과 철도국장이 겸직한다. (국토교통부와그소속기관직제 제 47 조)

성되어 필요하다고 인정되는 경우에 지체 없이 사고 조사를 실시할 수 있고 철도사고 관계인은 요구가 있으면 사고 관련 보고 및 자료를 제출해야 하고 관련 물건의 검사, 관계인 출석요구, 물건의 유치, 출입통제를 사고조사 위원에게 제공해야 한다.

항공철도조사위원회는 조사대상에 대한 사고 조사단 구성하여 분야별(안전 운전・관제, 시설, 차량, 전기・신호) 철도 사고 조사관(항공철도조사위원회 소속조사관)을 현장에 출동시켜 조사를 수행하게 한다. 사고조사단은 필요 시 국토교통부장관에게 사고조사 지원을 요청할 수 있고 관계기관이 장은 필요한 협조에 응해야 한다. 사고로 수집된 자료는 정보관리체계를 구축하여 필요한 정보를 제공하여야 한다.

사고조사 위원회는 사고조사결과에 의해 도출된 정보를 기반으로 재발 방지를 위해 긴요하다고 판단되는 안전권고 사항에 대해서는 서면으로 작성하여 위원장에게 보고하도록 되어 있다. 그리고 최종보고서에서 안전권고에 대한 이행실태를 점검하며, 부적절할 경우 국토교통부나 운영기관 등에 시정을 요구하도록 하고 있다. 항공・철도 사고조사에 관한 법에는 안전권고를 항공・철도 사고에 대한 비난 및 책임 추정을 위한 목적으로 사용할 수 없다고 명시되어 있다. 따라서 이 조사 결과를 활용해서 손해배상과 분쟁 조정을 위한 자료로 활용될 수 없다. 다만, 안전을 위한 연구 목적으로 활용될 수 있다고 되어 있다.

이와 같은 사례들로 종합해 보면 철도 분야에서 SW안전을 위한 복구 활동으로는 사고 조사와 재발 방지를 위한 활동들은 정의되어 있으나 손해 배상과 분쟁 조정을 위한 활동을 명확하게 정의되어 있지 않다.

### 6) 철도 분야 SW안전 기반 조성

철도안전법에는 국토교통부가 철도안전 기술 진흥을 위한 기술개발, 관련 전문기관 등을 지정 및 육성하도록 되어 있다. 철도안전 전문 인력(철도운행 안전관리자, 철도안전 전문기술자 등)의 자격을 국토교통부가 관리하며 한국철도시설공단에 위탁하여 시행 중이며, 5년마다 수립하는 철도안전 종합계획을 통해 안전관련 지식의 보급, 안전기술의 개발 및 지원 계획, 철도안전 산업 활성화 방안 등을 수립 및 시행하고 있다. 이 내용 중에는 철도 차량 결함 초기 검출 모듈, 레일 결함 검측 장비와 같은 최신 철도 기술 개발이 되고 있으며 이들 기술들은 철도 안전을 강화하기 위한 기술들이 포함되어 있다.

또한 철도 안전에 관한 지식 보급과 안전의식 고취, 각 기관 및 단체(운전적성 검사기관, 관제적성 검사기관 또는 정밀안전 진단 기관, 운전교육 훈련 기관, 관제교육 훈련 기관 또는 정비교육 훈련 기관, 인증기관, 시험 기관, 안전 전문기관 및 철도안전에 관한 단체)에 재정지원을 할 수 있도록 되어 있다. 이러한 진흥 활동들 중 일부는 SW 기반의 시스템 운영과 밀접하게 관련되어 있으므로 SW안전 문화 진흥 활동이라고 할 수 있다.

철도안전법에 국토교통부가 철도안전정보를 종합관리 및 제공할 수 있도록 하고 있고 권한위탁을 위해 철도산업정보센터(한국철도시설공단 소속)에 각 철도운영기관은 철도산업(안전포함) 데이터를 제출하고, 철도산업정보센터에서는 인터넷으로 공개하고 있다. 철도안전시책을 효율적으로 추진하기 위하여 철도안전에 관한 정보를 종합관리하고, 관계 지방자치단체의 장 또는 철도운영자, 운전적성검사기관, 관제적성검사기관, 운전교육훈련기관, 관제교육훈련기관, 인증기관, 시험기관, 안전전문기관 등 철도관계기관에 그 정보를 제공할 수 있기 때문에 철도 분야에서는 SW관련 정보도 공동 활용할 수 있는 체계가 마련되고 있다고 할 수 있다.

그리고 국토교통부는 철도안전 관련 국제 표준화 활동 지원하고 있다. 철도산업 및 철도안전 관련 기준들의 대부분은 유럽 중심으로 개발되고 있기 때문에 우리나라는 이 유럽제도의 벤치마킹을 통해 철도차량/용품의 형식승인제도가 도입하고 있다. 그리고, 철도 기술의 해외 수출을 위해서 국토교통부는 해외 기관들과 협력을 하면서 국내의 형식승인을 유럽의 TSI인증과 상호인증까지 계획하고 있으므로 국제협력이 활발하게 이루어지고 있다.

이와 같은 사례들을 보면 철도 분야의 SW안전 기반 조성을 위해 SW안전 문화 진흥, SW안전 기술 개발, SW안전 정보 공동 활용, SW안전 국제 협력이 추진되고 있음을 알 수 있다.

### 7) 철도 분야 SW안전 관리 현황과 한계점

철도 분야는 철도 차량 운행 및 선로 운영을 위한 관제 시스템에서 SW를 많이 활용하고 있기 때문에 ISO/IEC 62279를 기반으로 SW안전을 확보하기 위한 많은 노력을 기울여 왔다. 특히 철도 분야는 큰 사고가 발생하면 다수의 사상자가 발생할 수 있는 가능성이 높기 때문에 안전 확보가 전통적으로 중요했으며 철도 시스템에 SW가 많이

사용되기 때문에 다른 분야에 비해 상대적으로 SW안전 관리가 잘 수행되고 있다. 철도 분야 역시 명확한 SW안전 관리 체계가 없지만 앞서 설계된 SW안전 관리 프레임워크(안)을 기반으로 체계를 조사하고 사례를 기반으로 [그림 25]같이 철도 분야의 SW안전 관리 현황 조사 결과를 얻었다.

[그림 25] 철도 분야 SW안전 관리 현황


철도 분야의 안전관리 조직 및 관리계획 분야는 국토교통부를 중심으로 관련 조직, 역할, 안전관리 계획 수립 및 실행에 대한 체계가 잘 갖추어져 있다. 이는 기존의 철도안전을 위한 조직이지만 내부적으로 스마트화 되어가는 철도 차량 및 인프라 운영을 위한 안전 관리 필요성으로 인하여 SW에 대한 안전관리 역할, 조직의 기능과 역할 정의, 안전 관리 계획이 일정 부분 체계적으로 수행되고 있다.

철도 분야 안전관리 활동 분야는 예방 단계에서는 다양한 SW 기반 시스템을 기반으로 SW와 관련된 안전 관리를 수행하고 있으며 안전 확보를 위해 철도차량 운전면허, 철도 관제 면허 및 교육을 수행하고 있다. 또한, 철도 관련 시스템에 대한 안전 점검을 수행하면서 항시 안전 확보를 위해 노력하고 있다. 그리고 철도 안전과 관련된 정보를 철도 안전 포털 및 철도안전 정보 통합 DB를 통해 정보를 관리하고 공개하고 있었다.

대비 단계 활동으로 철도 차량 및 철도 부품을 위한 다양한 형식 인증 제도를 갖추어 있으면서 준수해야 할 안전 기준을 정의하고 있으며 이를 기반으로 형식 승인이라는 인증 제도를 통해 안전이 제공되는 부품을 사용하거나 시스템을 운영하고 있다. 또한 이미 다양한 첨단 기능에 대한 안전 기준이 정립되고 있으며 이에 대한 검사를 수행을 통한 자체 인증 제도가 마련되어 있다. 그리고 이용자 보호를 위해 보안 검색 장비 성능 인증, 시험 기관 지정 같은 활동들이 있다. 그리고 철도 종사자들은 정기적인 안전 교육을 통해 비상시 대응할 수 있는 훈련을 받고 있다.

대응 단계 활동으로 항공·철도 사고 조사를 위한 법에 의해서 사고가 발생하고 3인 이상의 부상 또는 5000만원 이상의 피해가 발생하면 바로 신고를 할 수 있게 되어 있으며, 이는 복구 단계의 사고 조사로 자연스럽게 연결이 되어 있다. 그리고 사고조사위원회가 구성되어 사고 조사를 수행하고 재발 방지를 위한 안전 권고 활동을 할 수 있게 되어 있다. 다만, 대응 단계의 사고 대응과 복구 단계의 손해 배상과 분쟁 조정에 대해서는 명확한 사례를 찾을 수가 없었다.

철도 분야 안전 기반 조성 분야에는 SW안전 문화 진흥을 위해 차량 운전 교육 기관, 관제 적성 검사 기관 및 훈련 기관 등을 지원하고 있으며, 철도의 스마트화 및 첨단 기술을 활용한 안전 확보를 위한 최신 기술 개발을 지원하고 있다. 그리고 철도 산업의 수출 전략을 위한 국제 협력을 추진하고 있고 안전 관련 정보에 대해서는 기관별 공동 활용을 위한 체계를 이미 갖추고 있다.

본 현황 조사는 본 보고서에서 개발된 SW안전 관리 프레임워크(안)을 기반으로 철도안전법과 항공·철도 사고 조사를 위한 법을 중심으로 주요 활동들을 도출하고 해당 활동들에 대한 사례가 있는지에 대해 조사하는 Top-Down 방식으로 조사가 되어 있기 때문에 철도 분야의 전체적인 상세 조사를 수행하지 못한 한계가 존재한다. 따라서 철도 산업의 전반적인 SW안전 관리 현황을 조사하기 위해서는 이에 대한 충분한 예산과 기간을 가지고 수행되어야 할 필요가 있다. 다만, 본 보고서의 목적인 SW안전 관리 프레임워크(안)을 검증하기 위한 목적으로는 충분한 효과가 있다고 볼 수 있다.

그리고 철도 분야의 SW안전 관리 조사를 수행하면서 제기되었던 현안 중 가장 중요한 것은 바로 철도 사고 조사위원회에 SW 전문가가 없다는 것이다. 이는 사고조사위원회의 철도 분과는 6명(상임 1명, 비상임 5명)으로 구성되어 있는데 철도 분과 위원 중에 SW 전문가가 없기 때문이다. 하지만 이는 실제 조사단 구성할 때 SW 전문가를 반드시 포함하고, SW 문제를 분석할 수 있는 도구를 확보하게 되면 충분히 극복할 수

있다고 생각한다.

다음은 철도 분야 SW안전 관리 조사를 수행하면서 전문가 자문 및 심층 인터뷰를 수행한 결과로 철도 분야의 SW안전 관리를 위해 다양한 의견들이 수렴되었다.

- 철도시설 및 철도차량의 안전관리는 철도시설(철도선로 등)은 국토교통부가 제시한 기준에 따라 시설관리자(한국철도공단, 한국철도교통공사 등)가 설치 및 유지보수하도록 하고 있으며, 철도 차량은 구매 시 필요한 형식승인을 국토교통부가 지정하고 이를 활용한 검사업무는 철도연구원에 위탁 받아 수행하고 있음
- 종합 시험 운행은 새로운 노선을 개통하거나 기존 철도선을 개량할 경우 종합시험운행 후 국토교통부에 적합여부(국토교통부 제시 기준에 적합여부, 철도시설 및 운행체계의 안전성 여부, 정상운행 가능 여부 등) 필수적으로 보고하여야 하며, 종합시험 결과의 검토는 교통안전공단에 위탁하여 수행하고 있음.
- 안전 점검은 권한을 위임받은 교통안전공단을 통해 안전 관리 체계의 정기 및 수시 점검이 이루어지고 있으며 필요시 국토교통부가 직접 점검(국토교통부의 안전감독관들이 있음)을 할 수도 있음
- TSI 승인 기준에 철도차량의 SW안전 관련 기준이 제시되어 있으며(IEC 62278), 철도의 안전성 인증(IEC 62278, IEC 62279, IEC 62280 인증)은 ISA(Independent Safety Assessor, 독립안전성 평가기관)에서 수행해야 함

## 3. 항공 분야 소프트웨어 안전 관리 현황 조사

교통안전연차보고서(2018)에 의하면 2017년에 발생한 항공 관련 사고는 10건으로 4명이 사망하고 7명이 부상을 당하였다. 2016년 대비 항공사고 수는 - 44.4%, 사망자수는 - 76.5% 감소하고 부상자 수는 133.3% 증가하였다. 2008년부터 2017년까지의 10년간 항공사고를 분석한 결과를 보면, 인적 요인(Human Error)으로 인한 사고는 전체의 63%를 차지할 정도가 가장 큰 요인이었으며 각 분야별로 보면 항공기 사고의 25%, 항공기 준사고의 31%, 경량/초경량비행장치 사고의 44%이었다.

이미 SW가 항공기 구성요소의 90%를 차지할 정도로 거의 모든 항공 안전 업무 및 시설들에서 SW 연관성이 높기 때문에 항공안전법에는 SW와 직접적으로 연관되어 있는 항공기기술 기준과 형식 승인이 포함되어 있을 정도로 SW안전 관리가 중요하다. 특히 최근 발생한 737 MAX의 추락 사고도 잘못된 SW 동작과 조종사들의 대응 미숙으로 기체 추락 사고가 발생했다는 이야기가 있다. 이와 같이 SW 오동작 예방 및 인적 요인 사고를 줄여주기 위해 SW 기능안전이 항공 분야에서 중요하게 다루어지고 있다.

<표 22> 항공안전법 체계

| |
|---|
| 제1장 총칙 |
| 제2장 항공기 등록 |
| 제3장 항공기기술기준 및 형식증명 등 |
| 제4장 항공종사자 등 |
| 제5장 항공기의 운항 |
| 제6장 공역 및 항공교통업무 등 |
| 제7장 항공운송사업자 등에 대한 안전관리 |
| 제8장 외국항공기 |
| 제9장 경량항공기 |
| 제10장 초경량비행장치 |
| 제11장 보칙 |
| 제12장 벌칙 |

SW안전 관리 프레임워크(안)의 검증과 보완을 위한 항공 분야의 현황 조사를 항공안전법과 항공 · 철도 사고조사에 관한 법을 중심으로 조사하였다. <표 22>는 항공안전법

의 기본 체계이며 항공·철도 사고조사에 관한 법의 체계는 철도 분야에서 이미 설명하였다. 이러한 법 체계를 SW안전 관리 프레임워크(안)을 활용하여 SW안전 관리 관점에서 조직 및 계획, 안전관리 활동, 안전관리 기반 조성에 대해 조사하였다.

### 1) 소프트웨어 안전 조직 및 관리 계획

항공 분야 SW안전 관리 현황 조사에 앞서 항공 분야의 SW 중요성 및 관련성을 알기 위해 <표 23> 같이 항공 안전 관련 체계, 항공 안전 관련 기관, 항공 안전 관련 역할 및 관련 업무들을 정리하였다. 항공 운항 체계에 포함된 항공기 운항 통제 및 안전 관련 체계 등은 SW 기반으로 동작하는 시스템이기 때문에 SW안전이 매우 중요하다.

<표 23> 항공 분야 관련 주요 체계 및 관련 기관들

| | |
|---|---|
| **항공 안전 관련 체계**[20] | 항공기 운항 체계(항공기/운항관리/항공공역/항행안전시설/공항및항공교통업무/비행계획/운항통제), 안전 증명 제도(항공운송사업운항증명/감항증명/자격증명/운영기준), 항공안전 관리 시스템(사전 예방적 안전관리) |
| **항공 안전 관련 기관** | 국토교통부 항공정책관, 항공 안전 정책관 및 공항항행정책관, 서울지방항공청, 부산지방항공청, 제주지방항공청, 항공교통센터(본부), 항공철도 사고 조사 위원회 등[21] |
| **항공 안전 역할** | 공항, 국내항공 운송 사업자, 국제항공 운송 사업자, 소형항공운송 사업자, 항공기 사용 사업자, 항공기 정비업자, 항공기 취급업자, 항공기 대여 업자, 초경량 비행 장치 사용 사업자, 항공교통 사업자, 외국인 국제항공운송사업자 등 (항공사업법 참조) |
| **항공 안전 관련 업무** | 비행정보, 항공교통관제(지역관제/접근관제/비행장관제), 경보시스템, 항공교통센터, 접근관제소, 공항관제탑 등 [22] |

항공 분야의 안전 관련 조직은 [그림 26]과 같이 국토교통부의 항공정책실장을 중심으로 국가 항공안전 프로그램이 운영되고 있다. 그리고 항공정책실장이 항공정책관·

20) 항공안전관리체계 진단(최종보고서) 국토교통부, 2015
항공안전관리체계는 국제민간항공기구(ICAO, 회원국이 법적으로 효력 있는 국가 민간 항공 규제를 만들 시 참고가 되는 국제적인 표준 및 권고(SARPs, Standards and Recommended Practices)를 개발하는 범세계적 기구)의 표준 및 권고에 맞게 체약국(우리나라)은 안전관리체계를 만들고 이를 ICAO의 평가를 받아야 함

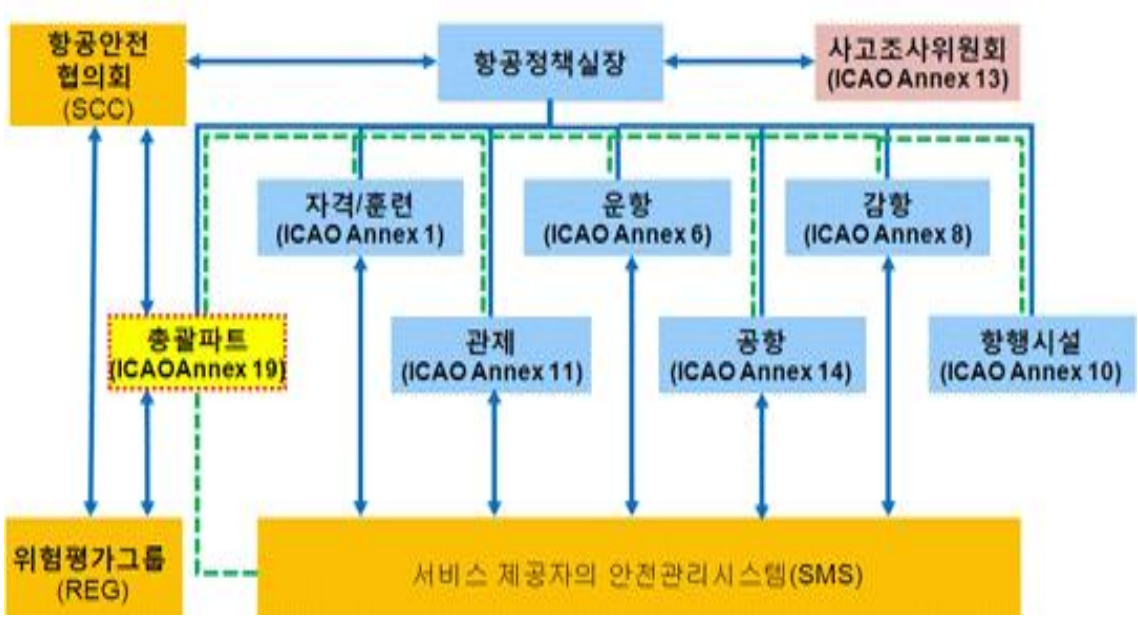
21) 2015년 국토교통부 “항공안전관리체계 진단” 보고서의 국내 항공 안전관련 조직 현황 참조

22) 항공안전백서 국토교통부 항공정책실, 2018

항공안전정책관 및 공항항행정책관을 거닐고 다음과 같은 업무를 수행하는 것으로 되어 있다.

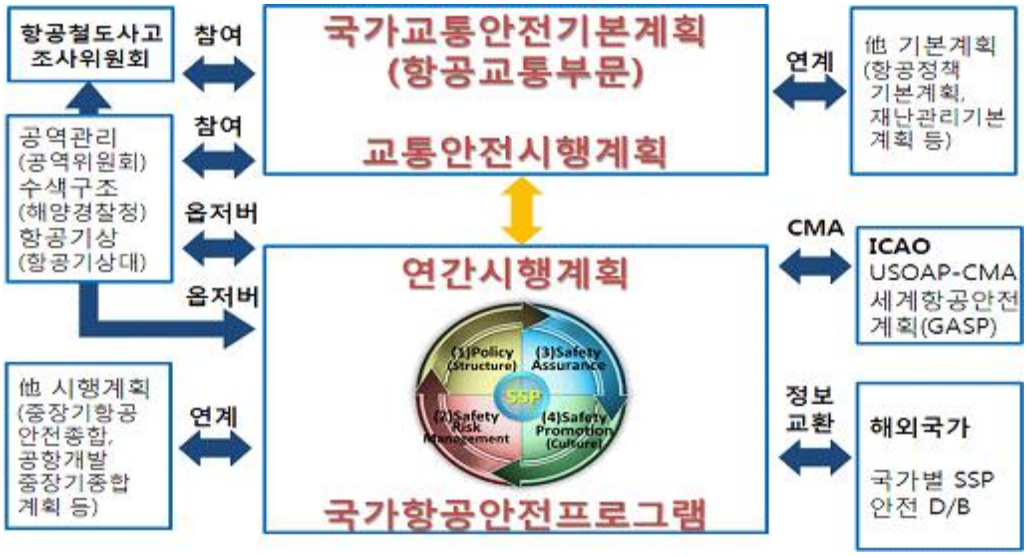
- 항공정보화계획의 수립·시행 및 항공물류 정보화사업에 관한 사항
- 항공보안에 관한 기본계획·국가항공보안계획·우발계획 수립 및 항공보안 관련 협의회 운영에 관한 사항
- 항행 분야(항공교통·정보·지도·비행절차·고정통신 및 이동통신 분야만 해당한다) 안전감독 및 항공교통관제 안전조사 등에 관한 사항
- 항공안전에 관한 법령·기준·정책 등의 연구 발전과 국가항공안전프로그램의 수립·시행
- 항공기 안전운항과 항공위험물의 안전운송을 위한 기술기준·안전대책 수립과 행정처분에 관한 사항
- 항공운송사업자에 대한 연도별 안전감독 종합계획의 수립 및 시행

[그림 26] 항공안전 관련 운영 체계




출처 : 행정규칙 - 국가항공안전프로그램 [시행 2017. 8. 25.]

[그림 27] 국가항공안전프로그램과 연관 조직/법제 간의 관계




출처 : 행정규칙 - 국가항공안전프로그램 [시행 2017. 8. 25.]

이러한 국가항공안전 프로그램은 항공 안전을 위한 국내외 조직과 역할이 정의하며 항공안전법에 의해 국내 조직과 역할도 정의하고 있다. 그리고 이에 따라 항공안전 기본계획을 수립해야 하며 이 계획에는 항공안전정책의 목표 및 전략, 항공기사고 · 경량항공기사고 · 초경량비행장치사고 예방 및 운항 안전 사항, 항공기 · 경량항공기 · 초경량비행장치의 제작 · 정비 및 안전성 인증체계, 비행정보구역 · 항공로 관리 및 항공교통체계 개선, 항공종사자의 양성 및 자격관리, 그 외 항공안전 개선 사항 등이 포함되어야 한다.

이와 같은 항공 분야의 안전 조직 및 관리 계획의 안전 관리 조직, 조직의 기능 및 역할 정의, 안전 관리 계획에는 SW 기반의 시스템과 연계되어 있기 때문에 SW 안전 관리 조직, 기능 및 역할 정의, SW안전 관리 계획들을 포함하고 있다.

### 2) 항공 분야 SW안전 관리 예방 활동

비행 속도의 증가와 기체의 대형화로 인하여 이륙, 비행, 착륙을 위한 기체의 다양한 부품들을 효과적으로 제어하기 위해 SW를 보편적으로 활용하고 있다. 더욱이 넓은 공

역을 관제하기 위한 레이더 기술과 통신 기술의 활용은 SW 역할 없이는 불가능하다. 따라서 항공 분야의 SW안전 활동의 역사는 다른 분야와 달리 전통적으로 오래되었다.

<표 24>는 항공 분야의 다양한 인프라들과 관련 기술들을 정리하였다. 이러한 인프라와 기술들 중에 SW와 연관되지 않은 부분이 없으며, SW안전 관리는 안전한 항공 운항을 위해 매우 중요하다. 따라서 항공안전법은 SW와 직접적으로 관련된 부분을 제3장 항공기기술기준 및 형식승인 부분에서 정의하고 있다. 이를 통해 SW안전과 관련된 대상을 정의하고 관리하고 있다.

<표 24> 항공 안전 관련 인프라와 기술

| | |
|---|---|
| **항공 안전관련 인프라** | 관제용 : 레이더접근관제소, 관제레이더, 지상레이더(ASDE), 다변측정감시시설(MLAT), 정밀접근레이더(PAR)<br>착륙용 : 계기착륙시설(ILS), 준계기착륙시설(ILS), 전방향표지시설(VOR/DME) |
| **항공 안전관련 기술(고정익 기준)** | 체계종합기술(체계공학/체계설계/M&S기술/시험평가기술), 기체기술(기체구조해석기술/기체구조부품제작기술/세부계통장비), 추진기술(엔진구성품제작/이차동력장치/비상동력장치/엔진장치), 비행조종기술(광성항법/전파항법/복합항법), 비행조종기술(비행제어장치/항법장치/감지장치), 항공전자기술(통신장치/임무 무장 장비/항전장비-레이더) |

출처: 통합항공안전정보시스템(https://www.esky.go.kr/)

운송용 항공기 사고의 70%는 조종 과실에서 발생될 만큼 항공기 조종 능력은 항공기 운항 안전의 중요한 요소이다. 항공기 조정은 기체 제어를 위한 SW 운영과 유사하다고 볼 수 있으며 조종사의 능력 향상을 위해 엄격한 자격 제도 및 양성 프로그램을 가지고 있다. 특히 대형기체의 경우 단계별 자격과 비형 경력을 통한 기체 교육 훈련 프로그램을 이수해야 하는 등 자격 획득을 위한 복잡한 면허 제도를 가지고 있다. 이뿐만 아니라 항공관제 시스템을 운영하는 관제사들도 실제 시스템 운영을 위한 자격을 획득해야 하고 항공 분야 시스템 정비를 위해서도 다양한 자격증들을 필요로 한다. 이와 같이 항공 분야에서는 다양한 종사자 자격을 규정하고 다양한 교육 프로그램을 갖추고 있다.

항공 분야는 안전 확보를 위해 항공기, 경량항공기 또는 초경량비행장치, 항행안전시설 등을 주기적으로 검사하고, 항공운송사업자가 취항하는 공항도 정기적인 안전성 검

사를 실시하고 안전운항에 중대한 위험을 초래할 수 있는 사항이 발견되었을 경우 항공기, 관련 시설 또는 관련자의 업무를 일시 정지하게 할 수 있고, 검사 결과 안전운항에 위험을 초래할 우려가 있을 경우에는 시정조치를 명령한다. 이러한 검사 과정에 당연히 SW 관련 시스템에 대한 점검도 포함되어 있다.

항공기 운항의 안전성 및 효율성을 확보하기 위한 항공정보, 항공지도 등을 비행정보구역에서 비행하는 사람 등에게 제공하며, 국민이 항공기를 안전하게 이용할 수 있도록 항공운송사업자의 항공기 사고 정보 등을 공개하고 있다. 또한 항공 사고 예방을 위해 항공사 · 공항 · 관제기관 등과 거버넌스 구성 및 '위험데이터 통합분석플랫폼'을 공동운영하고 있는데, 국내에서 수집 가능한 위험데이터의 소유기관, 종류, 특성, 공개범위 및 활용도 등을 고려한 위험 데이터의 통합운영계획 마련중이다.

이와 같이 항공 분야는 타 분야보다 체계적인 SW안전 관리 예방 활동들이 이루어지고 있으며 이는 타 분야에서 SW안전 관리 예방 활동을 정의할 때 충분히 참고할 수 있는 분야라고 생각된다.

### 3) 항공 분야 SW안전 관리 대비 활동

앞에서 언급하였듯이 항공 분야는 항공안전법에서 SW와 직접 관련된 부분에 대한 항공기기술기준을 마련하고 제작증명/감항증명 등을 위한 안전 기준을 정의하고 있다. 이 기술 기준에는 항공기 감항 기준/환경 기준/감항성 유지기준, 항공기 장비품 또는 부품의 인증 절차, 형식 증명 등이 포함되어 있다.

항공 분야 SW는 제작증명 전 제출되어야 하며 산출물을 통한 개발 프로세스 적합성을 평가하고 전문 심사원에 의해 필요한 경우 소소 코드까지 검사하여 인증과 유사한 체계를 갖추고 있다. 항공기 운항을 위해서 필요한 형식증명, 제작증명, 감항증명 과정에 SW가 직접적으로 해당 증명을 받진 않지만 해당 증명을 받기 위해서는 해당 SW가 신뢰할 수 있고 정합하게 만들어졌는지를 개발 단계에서 관리가 되어야 하며 DO-178C에 규정된 산출물(Outputs)을 반드시 제공해야 한다. 이러한 절차를 위해 항공기 기술 기준에는 <표 25> 같은 항공 분야 SW인증 기준을 정의하고 있다.

<표 25> 항공 분야의 SW인증 기준

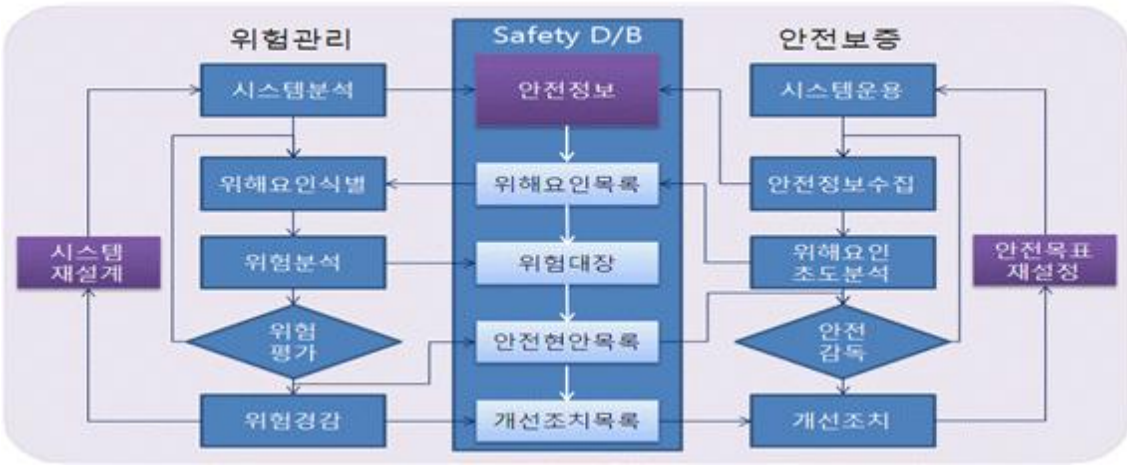
| |
|---|
| 1.7.3 소프트웨어 인증<br>모든 시스템 소프트웨어 본 기술기준에서 요구하는 안전수준에 적합하고, 계통 내에서 의도하는 기능으로 작동되도록 설계되고, 검증되어야 한다. 소프트웨어의 설계 및 시험은 RTCA/ DO-178 또는 EUROCAE ED12에 따른다. |

출처 : 01 항공기기술기준 Part 1 총칙

항공 분야의 인증 활동에 대해 추가로 알아보면 SW를 포함한 모든 항공기, 기술 표준품, 부품 등의 인증을 위한 형식증명, 형식증명승인, 제작증명, 감항증명 및 감항성 유지, 감항승인, 항공기기술기준 변경에 따른 요구, 기술 표준품 형식승인, 부품등 제작자증명, 항공운송 사업자의 운항 증명, 항공운송 사업자의 운항증명 취소, 항공운송 사업자에 대한 안전 개선명령, 항공기 사용 사업자의 운항증명 취소 등의 다양한 인증 활동들이 있다.

[그림 28]은 국가 항공안전 프로그램에 포함된 위험 관리 프로세스이다. 항공 분야는 이와 같인 안전 정보를 기반으로 시스템의 위험을 분석하여 재설계를 하고 시스템 운영의 안전을 보증하기 위해 위험 분석을 하고 안전 목표 재설정 활동을 하고 있다. 다른 분야와 다르게 항공 분야는 제대로 된 위험 평가를 통해 SW안전 확보를 위한 활동을 하고 있다.

[그림 28] 국가항공안전 프로그램에 포함된 위험관리 프로세스




출처 : 행정규칙 - 국가항공안전프로그램 [시행 2017. 8. 25.]

DO-178 기준에 맞춰 제작되었다고 하더라도 연계된 시스템들과의 동작 중에 예상하지 못했던 문제가 발생할 수도 있고 SW가 포함한 시스템을 운영하는 사람(조종사, 정비사 등)에 의해 문제가 발생할 수 있다. 이러한 경우 적절한 대응 매뉴얼을 갖추고 평상시 훈련을 통해 문제를 빨리 해결하여 피해를 최소화하기 위한 노력이 필요하다.

따라서 조종사들의 개인별·그룹별 훈련 이력을 관리하고 데이터 기반 기종별 맞춤형 훈련 프로그램이 도입되어 있으며 비정상 상황에 대한 훈련 프로그램들이 있을 정도로 SW안전 대비 활동으로 잘 갖추어져 있다. 특히 운송용 항공기 사고의 70%가 비행기 조종 과실에서 발생할 정도로 비상 상황에서의 조종사의 대응 능력은 매우 중요하다. 특히 737 맥스의 추락 과정에서도 조종사들이 비행 매뉴얼을 보고 있었다고 할 정도로 비상 매뉴얼과 비상 상황에 대한 훈련은 매우 중요한 활동이다.

### 4) 항공 분야 SW안전 관리 대응 활동

항공 분야는 항공기사고, 항공기준사고 또는 항공안전장애가 발생하거나 이와 같은 문제가 발생한 것을 알게 된 항공종사자 등의 관계인은 즉시 국토교통부에게 보고하도록 되어 있다. 이 보고 체계는 사고가 아니어도 사고로 이어질 가능성이 있는 경우(제작하거나 인증을 받은 항공기, 장비품 또는 부품이 설계 또는 제작의 결함으로 인한 고장, 결함 또는 기능장애가 발생한 것을 알게 된 경우)를 포함하고 있을 정도로 강력하다.

항공 분야는 사고로 인한 피해를 최소화하기 위해 항공기가 조난되는 경우 항공기 수색이나 인명구조를 위하여 국토교통부 및 관계 행정기관은 역할 등을 정한 항공기 수색 · 구조 지원에 관한 계획을 수립 · 시행하도록 되어 있다. 이는 항공 분야의 사고의 경우 대형 사고로 이어질 수 있는 가능성이 매우 높기 때문이다.

### 5) 항공 분야 SW안전 관리 복구 활동

최근 발생하는 항공 분야 사고는 SW와 많이 관련되며 인명 사고 발생, 항공기에 손상 또는 결함 발생, 항공기의 행방불명 또는 완전히 접근이 불가능한 경우에 국토교통부와 항공철도 조사위원회에 보고하도록 되어 있다. 이러한 제도는 항공기 사고, 항공

기 준사고 또는 의무보고 대상 항공 안전 장애가 발생 시 사실 여부와 이 법의 위반 사항 등을 파악하기 위함이다. 사고 조사 관련 내용은 항공철도 조사위원회에서 수행하며 철도 분야의 SW사고 조사 활동과 유사한 체계를 갖추고 있다.

사고 조사위원회 항공분과 위원은 현재 5명으로 구성되어 있으며 항공기 사고 원인 조사를 위해 사고 현장에서의 초동조치, 잔해 조사, 운항 분야 조사, 비행기록장치 조사, 구조물 조사, 동력장치 조사, 시스템 조사 등의 업무를 수행한다.

그리고 철도 분야와 마찬가지로 사고조사결과에 의해 도출된 정보를 기반으로 재발 방지를 위해 긴요하다고 판단되는 안전권고 사항에 대해서는 서면으로 작성하여 위원장에게 보고하고 안전권고를 요구할 수 있도록 되어 있다.  이와 같은 조사와 재발 방지를 위해서 SW안전 관련 사항들이 포함될 수 있다.

항공안전법에는 손해 배상 및 분쟁 조정에 관한 제도적 체계는 존재하지 않지만, 국토교통부는 형식증명, 제한형식증명, 부가형식증명, 제작증명, 기술표준품형식승인 또는 부품등제작자증명의 효력정지를 명하는 경우로서 그 증명이나 승인의 효력정지처분을 갈음하여 추가로 과징금을 부과할 수 있는 벌칙 조항을 포함하고 있다.

### 6) 소프트웨어 안전 기반 조성

항공안전법에는 산업 진흥을 위한 내용이 없지만, 항공정책 기본 계획 수립, 항공정책위원회의 설치, 항공기술개발 계획의 수립, 항공사업의 정보화 같은 진흥 사업들은 항공사업법에서 따로 규정하고 있다.

항공 분야의 국제 협력은 해외 제작자들이 만든 항공기, 외국 항공기의 국내 취항, 국적기의 해외 취항을 고려할 때 필수적인 요소이다. 외국인 국제 항공 운송 사업자의 운항 증명 및 항공기 운항 정지 그리고 외국 항공기의 운항 안전성 검사 조항들이 있으며, 항공 사고 발생시 해외 제작자와 함께 사고 조사를 할 수 있는 체계들이 마련되어 있다.

항공 분야는 [그림 29]처럼 통합 항공안전 정보 시스템을 구축하여 운영하고 있다. 해당 시스템은 항공안전 의무 자율보고 시스템, 안전 감독 정보 시스템, 운항 자격 심사 관리 시스템, 항공종사자 신체 검사 시스템, 항공기 인증 이력 관리 시스템, 비행검사 관리 시스템 등을 운영하면서 항공 안전을 위한 다양한 정보들을 통합 관리하면

서 항공 분야 조직간의 효율적인 현황을 공유하고 있다.

[그림 29] 통합항공안전정보시스템


출처: 통합항공안전정보시스템(https://www.esky.go.kr/)

이와 같이 항공 분야의 안전 기반 조성을 위한 다양한 활동들이 있으며 이 활동들에는 SW와 연관된 활동들이 포함된다.

### 7) 항공 분야 SW안전 관리 현황과 한계점

항공 분야 SW는 항공기 제어와 운항 관리를 위한 많은 시스템에서 폭 넓게 활용되고 있기 때문에 DO-178C를 기준으로 안전한 SW 개발을 위한 프로세스를 갖추고 있다. 그리고 형식승인 제도를 통해 안전한 항공기, 시스템, 부품 등의 안전을 확인하고 있으며, 다양한 점검 제도를 통해 안전한 항공기 운항을 위한 체계도 갖추어져 있다. 그리고 실제 SW기반 시스템이라고 할 수 있는 항공기와 관제 시스템을 제어하기 위한 종사자들의 자격, 교육 등의 프로그램들도 잘 갖추어져 있다. 이러한 항공 분야의 SW안전 관리 현황을 개발된 SW안전 관리 프레임워크(안)을 기반으로 조사하여 [그림 3]과 같이 항공 분야 SW안전 관리 현황 조사 결과를 얻었다.

항공 분야의 안전관리 조직 및 안전계획 분야는 국토교통부 항공정책실을 중심으로

체계적으로 조직 및 역할이 구성되어 있으며 항공기/항공기술/항공종사자/항공기운항/공역/운항사업자 등의 자격, 역할, 유지, 취소에 대한 부분이 잘 정리되어 있다. 이러한 조직과 조직의 역할들에는 당연히 SW안전을 포괄하여 구성되어 있다. 항공 분야 안전 관리 계획을 수립하기 위한 체계가 갖추어져 있어서 항공 분야 SW안전 관리 계획도 포함되어 있다.

안전관리 예방 활동 분야에서 SW안전 관리 대상은 항공기/경량항공기/초경량비행체/무인비행체, 교통체계, 공항시설 등이 포함되고 모두 안전에 매우 중요한 역할을 담당하고 있다. 그리고 항공 분야의 종사자들을 위한 엄격한 자격 조건과 교육 프로그램들을 통해 해당 분야의 종사자들의 역량 검증 및 강화를 통해 SW안전사고를 예방할 수 있는 체계가 갖추어져 있다. 안전 확보를 위한 점검 활동들도 체계적으로 수행함으로써 SW 오류로 인한 문제를 사전에 예방할 수 있도록 하며 안전 현황 공개를 통해 공개되지 않은 정보로 인한 사고 발생을 예방할 수 있는 체계도 갖추어져 있다.

[그림 30] 항공 분야 SW안전 관리 현황


SW안전 관리를 위한 대비 활동으로 항공기의 안전 기준을 통해 형식증명/제작증명 같은 인증 방안들을 정의하고 있다. SW는 형식증명을 위해 제시된 안전기준을 통과해

야하므로 안전한 SW개발을 확인하는 소스코드 검사를 포괄한 인증 활동이 시행되고 있다. 또한 안전을 위한 위험 요인을 찾아내고 분석, 평가하는 활동과 매뉴얼/대비훈련(ERP)은 국가항공안전프로그램 행정 규칙 포함되어 있을 정도로 활동들이 명확하게 되어 있다. 그리고 이용자 보호를 위한 SW 기능안전을 기반으로 한 다양한 활동들도 활성화되어 있었다.

SW안전 관리를 위한 대응 활동으로 항공 분야 종사자들은 항공기 사고, 항공기 준사고, 항공안전 장애들이 일어나면 이를 국토교통부에 신고해야 하며 매뉴얼이나 기타 정해진 절차에 따른 대응을 신속하게 수행해야 한다. 이는 SW가 유발하는 문제들도 포함하고 있다.

SW안전 관리를 위한 복구 활동으로 항공 분야의 사고 관련 보고가 이루어졌을 경우에는 사고조사위원회 중심의 사고 조사를 위한 사고조사단 구성, 자료제출 요구/검사/출석요구/질문/현장통제/물건유치와 더불어 원인 분석의 위한 시험/검사 및 관계인 의견청취를 통한 사고조사 보고서 작성이 이루어진다. 그리고 조사 결과는 안전권고 형태로 재발 방지를 위해 활용될 수 있다.

항공 분야의 SW안전 기반 조성을 위한 활동을 항공안전법에서 정의하고 있지는 않지만 SW를 포함한 항공안전 기술 개발, 항공 사업의 정보화, 항공사업 진흥, 국제민간항공기구 활동 등이 항공사업법에 의해 진흥되고 있다. 또한 항공 사고 조사를 위한 국제 협력은 국제민간항공기구(ICAO, International Civil Aviation Orgaminzation)을 중심으로 체계가 갖추어져 있다. 그리고 국제적으로 안전과 관련된 정보를 공동으로 활용될 수 있는 체계가 갖추어져 있고 국내에서도 통합 항공안전 정보시스템이 구축되어 효율적으로 정보 공유가 이루어지고 있다.

다음은 항공 분야 SW안전 관리 조사를 수행하면서 전문가 자문 및 심층 인터뷰를 통해 항공 분야의 SW안전 관리와 관련된 다양한 의견들이 수렴하였다.

- 항공 분야는 SW가 모든 계통의 핵심을 이루는 매우 중요한 부분으로 항공안전법에서 SW와 직접 관련된 부분은 제3장 항공기기술기준 및 형식승인 부분으로 제19조에서 제33조까지의 조문이며 나머지는 SW와 간접적으로 관련되거나 사용하는 부분에 관한 것으로 확장된 안전관리 관점에서 연관성이 있음
- 항공관련 내용은 우리나라 독자적으로 하지 않고 국제민간항공기구(ICAO)의 표

준과 권고를 반드시 준수해야 하며, 만약 자체적인 기준을 만들게 되면 우리나라 비행기의 해외 운항은 불가능하기 때문에 국제적 표준 준수가 중요함

- 항공기 사고와 관련하여 국제 협약에 의해 사고 발생 시 만약 외국 제작 항공기의 경우는 제조국의 제조사(형식증명소자자)와 감항당국, 사고조사위원회의 협조를 통해 사고 원인을 공동 조사하고 필요한 경우에 전문조사원을 파견하게 되어 있음
- 보잉 항공기에 사용할 SW를 개발하여 납품한다면 반드시 설계국(미국, FAA)의 기술 기준(국가 안전 기준, 감항성 기준)에 대해 동등한 수준의 안전성에 대한 인증을 받아야 함.
- 무인항공기 같이 새로운 기술들이 도입되면 기술 기준도 새로이 정의되어야 하는데 현행법 상 제품 적합성에 대한 기술 기준이 없어서 새로운 기기의 감항성 확인이 불가능한 경우에 신청자와 감항당국이 함께 특수 기술기준을 정하여 해당 요건을 모두 인증해야 하기 때문에 많은 어려움이 있음
- 우리나라는 SW가 쉽다고 생각해서 쉽게 고칠 수 있다고 하는데 실제로는 복잡한 SW가 많고 지속적으로 복잡해지고 있기 때문에 이에 대한 인식 전환이 필요

# 제4장 소프트웨어 안전 관리를 위한 제언

## 제1절 소프트웨어 안전 관리 프레임워크

3장에서 개발된 SW안전 관리 프레임워크(안)을 검증하기 위해 해당 프레임워크(안) 기반으로 자동차, 철도, 항공 분야의 SW안전 관리 현황을 조사하였다. 제한된 시간과 예산을 고려하여 프레임워크(안)의 주요 활동들을 가지고 관련 분야의 주요 법 체계를 우선적으로 분석하고 SW와 관련된 사례들을 추가로 조사하였다. 그리고 분야별 전문가 자문으로 수립한 SW안전 관리 프레임워크(안)에 대한 아래와 같은 주요 한계점들이 파악되었다.

- SW안전 관리 활동을 다가오는 위험에 대응하기 위한 재난안전 관점의 예방-대비-대응-복구 관점으로 해석하기 어려운 점이 있었고 자동차, 철도, 항공 등 SW안전이 활성화된 분야는 오히려 SW시스템을 안전하게 제작하고 운행(SW 운용)하는 관점이 필요
- 일부 교통 분야는 SW 관리 활동들이 명확화하지 않았는데 이는 해당 분야에서 시스템 중심으로 안전 관리가 충분히 이루어지기 때문이지만 새로이 등장하는 자율주행차, 무인 철도 차량, 무인항공기 같은 SW 중심으로 작동하는 새로운 시스템의 경우 기존의 관리 체계로 관리하기 어려울 수 있다는 우려가 있음
- 관리대상(제품/사용자/인프라) 지정에 따른 안전 기준 마련이 매우 중요하고 이를 토대로 인증, 운영 등의 다양한 관리 활동들과 연계되어야 하므로 사전에 위험 평가를 통해 모든 위험 요인을 고려한 대상 지정과 안전 기준 마련이 필요하고 새로이 등장하는 SW 제품의 경우 충분한 연구가 선행되어야 함
- 기존의 SW안전 관리는 응급조치에 대한 고려가 크지 않았지만, 다수의 전문가들은 기능 안전 측면에서 SW를 활용한 응급조치 자동화로 SW안전 관리를 강화할 수 있을 것으로 봄
- 교통 분야는 시스템 관점의 관리가 주로 이루어지기 때문에 SW 관련 안전 점검이 상시적으로 이루어지지 않지만, 향후 스마트시티 같은 SW 중심의 제어 시스템 환경에서는 SW 관점의 점검 및 결과 공개가 더욱 중요해질 것으로 예상

- 미래 사회에서 SW가 보다 확산될 경우 안전 조직 및 관리 계획 측면에서도 SW에 대한 고려가 더 많이 필요하며 스마트시티, 자율주행차 등의 신기술 발전에 따른 조직과 역할의 변화가 발생할 수 있음

위의 한계점들을 고려한 개선된 SW안전 관리 프레임워크는 [그림 31]과 같다. 우선적으로 재난안전 관점의 예방-대비-대응-복구 프레임을 인증-운영-응급 조치-사후 관리로 변경하였다. 그 이유는 대부분의 SW안전 관리의 시작이 SW가 들어간 해당 제품의 개발로부터 시작되기 때문이다. 자동차, 철도, 항공 분야들도 SW 제품을 안전하게 개발하기 위한 다양한 표준들을 제정하고 있다. 그리고 개발 결과물에 대한 인증 제도로 제품의 안전성을 보장하기 때문에 예방이라는 단어보다는 SW 개발과 좀 더 밀접한 인증이라는 용어를 사용하였다.

[그림 31] 개선된 SW안전 관리 프레임워크


첫 번째 단계인 인증 단계는 재난안전의 경우 다가오는 위험(사회 재난, 자연 재난) 등을 대비하기 위한 활동들이 필요하지만 SW안전의 경우 SW 개발을 통해 구현되기 때문에 개발 과정이 포함한 인증이라는 단계 속에서 안전한 SW 확보가 이루어져야 한다. 따라서 SW안전에 영향을 미치는 대상을 정의하고 이에 대한 안전 기준 마련함

으로써 SW안전 관리가 시작해야 한다. 그리고 SW안전 관리 대상과 안전 기준은 운영 단계와도 연계가 되어야 한다. 그 이유는 인증 단계에서 중요한 안전 관리 대상은 운영 단계에서도 지속적인 안전 점검을 통해 안전성에 대한 관리가 이루어져야 하기 때문에 이를 위한 안전 기준도 동시에 마련되어야 한다.

그리고 관리 대상은 제품/사용자/인프라 등 SW와 관련된 다양한 대상들을 지정할 필요가 있다. 제품 또는 인프라 그리고 이와 관련된 부품에 대해서는 검사를 통해 인증하여 안전성에 대한 확인 절차가 필요하다. SW와 관련된 사람(설계자, 개발자, 운영자, 검사자 등)들도 일정한 자격 조건에 대한 시험을 통해 검증이 필요할 수 있다. 마지막으로 위험에 대한 평가를 통해 어떠한 위험 요인이 있는지 확인을 하고 이에 대한 대비가 충분히 이루어져 개발, 인증, 운영이 되어야 한다.

다음 단계는 운영 단계이다. 이 단계에서는 언제 발생할지 모르는 사고에 대비하기 위해 SW를 운영하는 과정에서 상시 또는 주기적인 점검을 통해 안전 관리를 수행해야 하고 그 결과를 공개하여 최대한 SW안전에 대한 정보를 공유하고 위험을 대비해야 한다. 충분한 이용자 보호 조치를 통해 SW 시스템 운영자가 안전하게 시스템을 운영하고 관리할 수 있게 하고 SW 시스템의 영향을 받는 사용자들의 안전도 확보해야 한다. 그리고 737 맥스의 추락사건 같이 발생할지 모르는 비상 상황에 대한 매뉴얼을 갖추어야 하고 훈련을 통해 사전에 SW가 야기할 수 있는 위험에 대한 대비도 필요하다.

세 번째 단계는 응급 조치이다. 철도와 항공 분야의 경우 사고가 발생하면 기존 체계 내에서 빠르게 신고(보고)를 하게 되어 있고 그 이후 대응 절차에 따른 응급 조치를 수행하게 되어 있다. 하지만 자동차 분야의 경우 자연 재난 또는 사회 재난이 아닌 경우 자체적으로 경찰에 신고하게 되어 있다. 하지만, 보편적인 SW 제품의 경우 이러한 신고 절차가 포함되어 있지 않다. 특히 사람의 생명이나 인체에 손상이 올 수 있는 SW안전 사고가 발생할 수 있는 SW가 포함된 제품 및 서비스는 사고가 발생하게 되면 명확한 원인 조사를 위해서 엄격한 신고 절차가 마련되어야 한다. 그리고 사고를 유발할 수 있는 SW 결함에 대한 신고 및 보고 절차도 마련되어야 한다. 또한 불가피하게 사고가 발생할 경우 사람의 생명과 인체 손상 같은 피해를 최소화하기 위해 응급 구조 활동 같은 사고 대응 활동에 대해서도 미리 정의되어야 한다.

마지막 단계인 사후 관리 분야는 발생한 SW안전사고에 대한 철저한 원인 조사와 이를 통한 재발 방지 활동이 필요하다. 가장 좋은 것은 인증 단계에서 충분한 위험 평가

를 통해 안전성이 확보되고 운영 단계에서 엄격한 점검으로 사고가 발생하지 않는 것이지만 어쩔 수 없이 발생한 사고나 결함에 대해서는 철저한 사고 조사가 수행되어야 한다. 그리고 조사 결과에 따라 재발 방지를 위한 활동들이 반드시 수행되어야 한다. 만약 사고로 인한 피해나 손해가 발생할 경우에는 이에 대한 손해 배상 및 분쟁 조정 활동들을 통해 피해 및 손해 보상에 대한 조정 기능도 마련되어야 한다.

이러한 단계별 안전 관리 활동들 이외에 안전 조직 및 관리 계획과 안전 기반 조성은 앞에서 충분히 설명하였기에 여기에서는 생략한다.

[그림 31]은 현재 교통 분야의 SW안전 관리 현황을 기반으로 보완한 것으로 미래 사회에서 SW 역할의 변화에 따라 변경될 수 있다. 지금 당장 미래 사회에서의 SW 역할을 정의하기는 어렵지만 이러한 변화에 따른 SW안전 관리 체계의 개선에 대한 예를 알아보기 위해 다음 절에서는 해외를 중심으로 안전 관리 개선 사례들을 살펴보도록 한다.

## 제2절 신기술 활성화를 위한 법제도 개선 사례

사회의 디지털화와 인공지능의 발전으로 다양한 분야에서 SW 활용이 확산되어 가고 있다. 특히 자동차 분야에서 운전자 중심 자동차에서 SW 중심의 자율주행차로의 진화가 진행되고 있다. 자율주행차는 자동차와 인프라가 유기적으로 연결되어 사람의 조작 없이 자동차가 주변 환경을 인식하고 위험을 판단하여 주행이 가능한 경로를 스스로 설정하여 운행이 가능한 자동차를 의미한다.[23] 현행 「자동차관리법」 제2조 제1의3호도 자율주행자동차를 ‘운전자 또는 승객의 조작 없이 자동차 스스로 운행이 가능한 자동차’로 정의하고 있다.

이러한 자율주행차를 개발하기 위해서는 인공지능, 빅데이터, 클라우드, IoT 같은 SW 신기술들을 기반으로 여러 센서와 전자장치가 지능적으로 작용해야 하므로 SW 역할이 중요해지고 있다. 그리고 전 세계 많은 국가들은 자율주행 기술 개발에 앞장서고 있으며 기술 신뢰성을 얻기 위해 다양한 시험 주행을 하고 있다.

과거 UN 도로교통에 관한 비엔나 협약은 자율주행자동차에 의한 주행을 허용하지 않았으나 2016년 12월에 발효된 비엔나 협약의 개정은 운전자가 언제든지 차량시스템에 개입할 수 있다는 조건하에서 자율주행시스템에 의한 주행이 허용되는 것으로 개정되었다. 비엔나 협약에 서명하지 않았거나 비준하지 않은 국가들은 비엔나 협약을 준수할 필요가 없는데 그 대표적 국가가 미국이다. 따라서 본 절은 자율주행차 관련된 비엔나 협약의 변경 내용과 미국의 캘리포니아의 사례를 중심으로 자동차 분야의 SW 안전 관리 개선 사례들을 검토한다.

전통적으로 도로교통법은 인간 운전자를 가정하고 제정되었기 때문에 인간이 아닌 다른 운전 주체가 차량을 제어하는 것을 고려하지 않았었다. 이러한 제도로 인간이 직접 운전하지 않는 자율주행차는 도로운행 자격을 제도적으로 충족하지 못하였다. 이는 각국의 법만이 아니라 UN 유럽경제이사회(UNECE)의 내륙교통위원회(Inland Transport Committe) 소속의 도로교통 안전을 위한 국제 포럼(Global Forum for Road Traffic Safety; 이하 WP.1)에서 다루고 있는 1949년의 도로교통 협약(이하 제네바 협약)과 1968년의 도로교통 협약(이하 비엔나 협약)에서도 역시 동일한 문제를 내포하고 있었

23) 자율주행차동차 상용화 대비 도로교통법 개정 방안 연구, 2016, 아주대

다. 이들 협약의 가입국들은 협약 내용에 의해 국내에서 자율주행차 운행을 제약할 수 밖에 없었다. 하지만 비엔나 협약의 변경으로 협약 상의 운전자는 항상 차량을 제어하고 있어야 한다는 조항이 운전자가 제어할 수 있는 범위로 변경되면서 도로에서 자율행차의 운행이 가능하게 되었다.

비엔나 협약의 개정으로 해당 협약 가입국의 대부분인 유럽 국가들은 상용화를 위한 운전자가 탑승한 상태에서 자율주행차 시험주행이 가능해졌다. 이 비엔나 협약의 개정의 주요 내용은 “차량의 운행에 영향을 주는 차량시스템이 앞에서 언급한 국제법 기준에 따른 설계, 장착 및 이용을 위한 조건에 부합하지 않지만 당해 차량시스템이 운전자에 의해 제어 또는 차단될 수 있는 경우에는 본조 제5항 및 제13조 제1항에 부합하는 것으로 본다.” 는 것으로 운전자의 판단에 의해 차량시스템(자율주행 기능)이 정지될 수 있는 것으로 수정한 것이다.

미국은 교통부문 중·장기 계획에서 자율자동차 시험주행 기술 개발을 활성화하기 위해 국가적으로 노력하고 있다. 백악관은 2015년 Strategy for American Innovation을 발표하면서 자율주행차 활성화를 위한 연방 정보 지원 계획을 발표하였고 교통부도 2015년 ITS Strategic Plan 2015-2019을 발표하면서 C-ITS 계획에 자율주행차 기술 개발 계획을 포함한 자동차 안전 강화 방향을 밝혔다. 이어서 2016년에는 자율주행차 성능요건, 주정부 정책수립 방향, 제도개선 방향을 포괄하는 가이드라인을 발표하였다.

자율주행차 개발·판매를 위한 성능요건으로 운행구역, 인식·제어 기능, 고장 안전, 데이터 기록 및 공유, 인증·등록, 사고 시 거동, 정보보호·보안, 충돌 안전성 같은 15개 안전 관련 사항의 기준이 제시되었고 이에 대한 준수 여부를 연방 도로교통안전청에 보고하도록 하였다. 주 정책 방향에 관련되어 연방정부와 주정부간 업무의 명확화 및 주정부의 자율차 관련 조직 및 업무에 대한 표준안 제시되었다. 기술 개발이 필요한 자율주행차(4-5단계) 성능 및 기술 관련 제도화는 연방정부에서 담당하고 주정부는 법제화 추진할 때는 연방정부와 협의하도록 되었다.

〈표 26〉 캘리포니아 자율차 규정 개정작업 진행경과

| 일자 | 진행 사항 |
|---|---|
| 2015년 12월 16일 | 자율차 보급 규정 초안 공개 / 이해관계자 의견수렴(public workshop) |
| 2016년 09월 30일 | 수정 초안 공개 및 이해관계자 의견수렴 |
| 2017년 03월 10일 | 자율차 시험운행 및 보급 규정 입법예고 및 공청회(public hearing) |
| 2017년 10월 11일 | 자율차 시험운행 및 보급 규정 수정안 입법예고 및 의견제출 절차 |
| 2017년 11월 30일 | 자율차 시험운행 및 보급 규정 수정안 2차 입법예고 및 의견제출 절차 |
| 2018년 01월 11일 | 최종 규정안 법제처(OAL: Office of Administrative Law)에 제출 |
| 2018년 03월 02일 | 법제처 승인을 얻은 최종 규정안 공고 |

※ 출처 : https://www.dmv.ca.gov/portal/dmv/detail/vr/autonomous/milestones_regulations

특히 미국의 주정부 중에서 구글, 테슬라 등의 많은 IT 기업들이 있는 캘리포니아주는 〈표 26〉 같이 자율주행자동차 관련 입법이 활발히 이루어지고 있다. 과거 캘리포니아 자동차법 에 의하면 자율주행차를 운행할 수 없었다. 하지만 캘리포니아는 2012년에 자율주행규정의 도입을 위하여 시험운행규정 제정하게 되었다. 그리고 2018년 3월 자율주행자동차 시험 운행 규정 개정안 및 보급 규정 제정안을 최종 확정하여 공포하면서 운전자가 탑승하지 않은 상태의 시험운행을 허용하고 사고기록장치 장착을 의무화하였다.

이에 관련해서 캘리포니아 차량국은 세부 규정으로 운전자가 있는 시험운행(Testing with a Driver), 운전자가 없는 시험운행(Testing without a Driver), (3) 보급 - 공중 사용(Deployment - Public Use)으로 3가지 자율주행차 허가 프로그램을 운영하고 있다. 2019년 11월 기준 캘리포니아 주에서 운전자가 있는 시험주행(Testing with a Driver)의 허가를 받은 업체들은 〈표 27〉 같이 64개의 회사들이 있다[24].

캘리포니아는 자율주행차의 무인 주행시험 및 공중 사용(driverless testing and public use) 관한 규정을 제정하고 무인 시험 운행에 대한 승인 절차를 진행하여 2018년 10월 기준 구글의 웨이모(Waymo LLC)가 승인을 받게 되었다. 그리고 2019년 12월에는

24) 캘리포니아 차량국, 모빌리티 변화에 대응하기 위한 법과 제도, 2019.10.

10,000파운드 미만의 경량 자율주행 트럭의 운행을 허용하기로 하였고 이를 위한 허가 절차를 요약한 제안서를 발표하였다[25].

이와 같이 미국의 자율주행 기술 발전을 촉진하기 위한 법 제도 개선 노력에는 우선 자율주행차 및 기능에 대한 개념 정립, 자율주행차의 시범 운행 조건 (보험 가입 포함), 자율주행 운행 신청을 위한 조건(자율주행 제어 방법, 안전 기준 만족 여부, 자율주행 감지 데이터 저장, 위험 경보 시스템 등) 등을 정의하였다.

<표 27> 운전자가 있는 시험주행의 허가를 받은 업체(2019년 11월 기준)

| | | |
|---|---|---|
| • Almotive Inc | • Gatik AI. Inc. | • Qualcomm Technologies, Inc. |
| • Ambarella Corporation | • GM Cruise LLC | • Renovo.auto |
| • Apex.AI | • Helm.AI Inc | • Ridecell Inc. |
| • Apple Inc. | • Honda | • Roadstar.Ai |
| • Argo AI, LLC | • Imagry Inc. | • SAIC Innovation Center, LLC |
| • Atlas Robotic, Inc. | • Intel Corp | • Samsung Electronics |
| • Aurora Innovation | • Jingchi Corp | • SF Motors Inc. |
| • AutoX Technologies Inc | • Kaizr, Inc | • Subaru |
| • Baidu USA LLC | • Lyft, Inc. | • Telenav, Inc. |
| • BMW | • Mando America Corporation | • Tesla Motors |
| • Bosch | • Mercedes Benz | • ThorDrive Inc |
| • Boxbot Inc | • Navya Inc. | • TORC Robotics Inc |
| • CarOne LLC | • NIO USA, Inc. | • Toyota Research Institute |
| • Changan Automobile | • Nissan | • TuSimple |
| • Continental Automotive Systems Inc | • Nullmax | • Udacity, Inc |
| • CYNGN, Inc | • Nuro, Inc | • Valeo North America, Inc. |
| • Deeproute.ai Ltd | • NVIDIA Corporation | • Volk소프트웨어agen Group of America |
| • Delphi Automotive | • Phantom AI | • Voyage |
| • DiDi Research America LLC | • PlusAi Inc | • Waymo LLC |
| • EasyMile | • Pony.AI | • Xmotors.ai, Inc. |
| • Faraday & Future Inc. | • Qcraft.ai | • Zoox, Inc. |
| • Ford | | |

※ 출처 : https://www.dmv.ca.gov/portal/dmv/detail/vr/autonomous/permit. 2019/11/21기준

25) automotive, 미 캘리포니아, 경량 자율주행 트럭 운행 허용, 2019.12.20.

비엔나 협약 변경 및 캘리포니아의 자율주행 관련 제도 개선 같은 자율주행 기술 개발을 촉진을 위한 국내 법제도 개선 노력도 이루어지고 있다. 기존 국내 도로교통법에는 지방경찰청장으로부터 운전면허를 받지 아니하거나 운전면허의 효력이 정지된 경우에는 자동차 등을 운전하여서는 안된다고 정의되어 있었다. 하지만 최근 운전주체에 대한 다양한 규정을 마련되었고 자율주행 기술 개발을 촉진하기 위해 특별법 형태로 관련 법제도를 개선함으로써 국내에서도 자율주행의 시범 운행을 통한 기술 발전을 위해 노력하고 있다[26].

이와 더불어 일반 자동차와 구분하기 위한 표식 부과 의무 부여, 특별 등록 번호판 부착 의무 같은 등록 제도를 변경하고, 자율주행차 관련 새로운 안전 기준을 제시하고 있으며 자율주행차 사고 발생시의 손해 배상 책임 및 운행자에 대한 의무와 책임, 시스템 관리자의 의무와 책임 같은 자율주행차 시범 운행에서 발생할 수 있는 문제에 대한 합리적 해결 방안들이 제시되고 있다[27].

이와 같은 국내외의 자율주행차 관련한 법제도의 변화를 보면 SW안전 관리 프레임워크 관점에서 시범 운행을 통해 위험 평가를 통해 새로운 관리 대상 지정, 새로운 안전 기준 마련, 새로운 종사자 자격 및 교육, 새로운 안전 점검 등의 관리 활동들이 개선되고 있다. 미국 캘리포니아 주 정부는 국내 보다 진일보한 규정으로 빠르게 상용화하고 있다. 이와 같이 새로운 SW 기술의 등장은 SW안전 관리를 위한 제도적 개선을 요구하고 있으며 이를 위해 본 연구에서 도출한 SW안전 관리 프레임워크가 효율적으로 활용될 수 있다.

26) 교통안전연구원, 모빌리티 변화에 대응하기 위한 법과 제도, 2019.10.
27) 한국과학기술기획평가원, 자율주행자동차 활성화를 위한 법제 개선방안 및 입법(안) 제안, 2017.09.

## 제3절 안전사고 조사 선진 사례

해외 교통 분야 사고 조사는 원인 분석을 위한 조사와 처벌을 위한 사고 조사를 분리해서 실행하고 있다. 대표적 사례인 미연방 교통안전 위원회(NTSB, National Transportation Safety Board)는 자동차, 항공, 철도, 선박 등의 교통 분야 사고 조사를 담당하는 기구로 보잉 737 맥스의 추락 같은 항공기 사고만이 아니라 최근 발생하는 자율자동차 사고에서 자주 등장한다. 이와 유사하게 호주에는 호주 교통안전 위원회가 있다. 두 조사 기관 모두 사고 조사 과정에 SW에 대한 사고 원인을 알아내기 위한 별도의 전문가 조직을 운영하고 있다. 이러한 사례들은 원인 분석을 통한 재발 방지 측면에서 중요한 의미가 있으므로 두 조직에 대한 사례들을 조사하였다.

미연방 교통안전 위원회는 1967년 미국 교통부(DOT) 설립할 때 독립 행정기관으로 설립되었고 1975년 독립 안전위원회 법(The Independent Safety Board Act)으로 교통부에서 완전하게 독립하였다.[28] 그 이유는 교통안전 위원회의 역할을 수행함에 있어 여러 정부 조직에서 규제하는 사고(항공, 철도, 해양, 고속도로, 송유관, 위험물 운송 등)에 대한 엄격한 조사를 수행하고 정부 조직 및 관련 공무원들에게 비판적일 수 있는 조사 결과와 안전 권고에 대한 완전한 독립성을 유지하기 위해서이다.

현재는 미국 내 모든 민간항공 사고 및 도로, 철도, 해양 등 다양한 교통 분야의 대형사고 조사를 수행하는 독립적인 기구로 교통사고에 대한 심도 있는 조사를 통해 원인을 분석하고 사고 재발 방지를 위해 안전 권고를 집행함에 있어 관련 연구를 수행하고 사고 후 희생자와 유가족을 위해 조정 및 지원 기능을 갖추고 있다.

이러한 업무를 수행함에 있어 객관성을 유지하기 위해 2년 임기의 위원장은 상원의 권고와 동의를 받아 대통령이 임명하며 상임위원은 상원의 권고와 동의를 받아 대통령에 의해 5년 임기의 상임위원 5명이 임명된다. 상임위원은 같은 정당에서 3명 이상의 임명할 수 없으며 최소 3명은 사고재현, 안전공학, 인적 요인, 교통안전, 교통법규와 관련하여 자격, 직업적 지위, 공인된 지식 등을 갖춘 사람으로 임명하게 되어 있다. 구성은 약 400명의 인력을 가지고 5개의 이사회와 8개의 부서로 이루어져 있으며, 5개의 이사회는 자금관리이사회(Chief Financial Officer), 법무자문이사회(General

28) https://www.ntsb.gov/about/history/Pages/default.aspx

Counsel), 상무이사회(Managing Director), 안전권고 및 정보담당 이사회(Safety Recommendations & Communications), 고용기회균등담당이사회(Equal Employment Opportunity, Diversity, and Inclusion)로 이루어져 있다. 그리고 항공안전, 철도·송유관·위험물 안전, 고속도로 안전, 해양안전, 행정 심판, 연구 및 기술, 정보통신 관리 등의 업무를 수행하고 있다.

철저한 사고 조사와 빠른 재발 방지 대책 마련을 위한 목적으로 조사를 수행하기 때문에 조사 결과를 가지고 책임을 추궁하지 않도록 되어 있다. 따라서 원칙적으로 미국 내의 모든 법정에서 안전위원회의 사고조사 보고서가 증거로 채택될 수 없다. 항공 분야의 사고 조사 역시 독립적인 조사 수행을 통해 안전 개선을 위한 원인 분석을 위한 조사를 수행한다. [그림 32]는 미국 교통안전 위원회의 사고 조사의 예이다.

[그림 32] SW 오류를 찾아낸 미국 교통안전 위원회 사고 조사의 예


On Oct. 15, the Lufthansa Group subsidiary SWISS International Airlines grounded its A220 fleet for more than a day after the third flight was forced to divert or return to the departure airport with engine damage.

The NTSB-led investigation focused on a recently updated engine **software that may have caused** vibrations that tore the engine parts. The engine problems with the SWISS A220s arose following a software upgrade, experts who are close to the matter told Reuters news agency.

※ 출처 :
https://thewofa.com/2019/10/ntsb-investigates-recent-airbus-a220-engine-failures

Radar in Uber's self-driving vehicle detected pedestrian Elaine Herzberg more than five seconds before the SUV crashed into her, according to a new report from the National Safety Transportation Board. Unfortunately, a series of **poor software design decisions prevented the software** from taking any action until 0.2 seconds before the deadly crash in Tempe, Arizona.

※ 출처 :
https://arstechnica.com/cars/2019/11/how-terrible-software-design-decisions-led-to-ubers-deadly-2018-crash/

조사를 수행함에 있어 정확성을 확보를 위한 사고 조사 기술을 가진 3~4명의 전문가들을 사고 현장에 파견하고 파견 전문가들은 현장의 정보들을 바탕으로 사고 관련 기록들을 확보하고 산업체, 정부 관계자들과 함께 확보된 내용을 분석한다. 분석된 내용

에서 결함이 밝혀지면 재발 방지를 위해 조사 완전 이전이라도 안전 권고 명령을 내려 문제점을 개선하도록 할 수 있다. 조사가 완료되면 상임위원의 주재로 공청회를 개최하여 조사 결과의 사실을 명확하게 하고 조사 내용에 대한 실효성을 확보함으로써 교통안전 위원회의 투명성을 담보한다.

호주의 교통안전 위원회(ATSB, Australian Transport Safety Bureau)는 호주 연방 정부의 독립 기관으로 교통 안전조사법에 의해 교통 규제 기관, 정책 입안자 및 서비스 제공 업체로 부터 완전히 독립되어 있다. 호주 교통안전 위원회의 기능은 다음과 같은 역할을 수행하고 있다.

- 항공/철도/해양 교통사고 및 기타 안전보고 발생시 독립적인 사고조사 수행
- 사고 및 안전데이터 기록/분석/연구 수행
- 안전의식 향상, 안전지식 공유 및 안전 이행 도모

이외에도 교통안전 문제 및 규정에서 제시된 안전 정보를 평가하고 사고 조사 결과에 따라 안전에 영향을 미치거나 미칠 수 있는 요인들을 안전권고 및 안전조치 성명을 통해 대중들에게 전달하고, 사고조사 결과를 공개적으로 보고하여 안전 향상에 노력하고 있다.

항공사고 발생 시 호주의 교통안전 위원회는 사고 원인을 밝히기 위한 비처벌(No punishment, No blame) 사고 조사를 수행하는데 반하여 행정처분을 위한 사고 조사는 항공안전 규제 당국인 CASA(Civil Aviation Safety Authority)에서 수행한다. 이와 같이 서로 다른 목적을 가지고 두 기관은 사고를 조사한다.

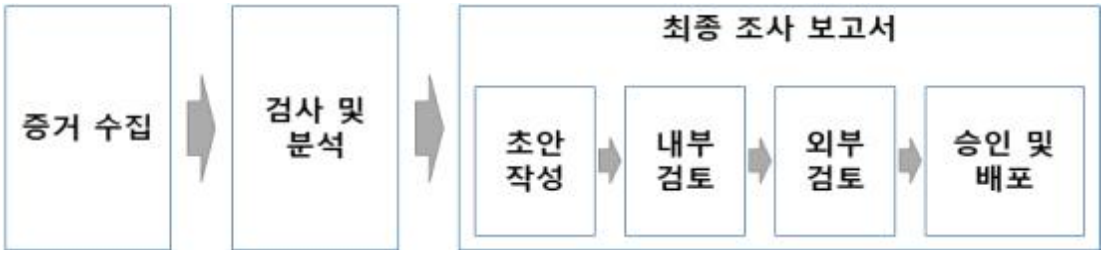
호주의 교통안전 위원회는 위원장과 2명이상의 위원을 중심으로 약 100명의 인원으로 구성되어 있다. 그리고 위원회 직속으로 전략국(Strategic Capability), 항공국(Aviation), 철도국(Rail), 해양국(Marine), 연구분석국(Research & Lab)으로 나뉘어져 있다. 호주 교통안전 위원회는 호주 내에서 발생하는 사고와 호주 소속의 교통수단에서 발생한 사고에 대해 조사를 수행한다. 조사가 시행되면 호주 교통안전 위원회가 단독으로 해당 조사에 대한 권한을 가지게 된다.

사고에 따라 즉시 보고 사항(Immediately reportable matter)과 일반 보고 사항

(routine reportable matter)을 구분되어 있다. 즉시 보고 사항은 사고로 인하여 재산 또는 교통수단이 심각하게 손상되거나 파괴되거나 심각한 부상 및 사망 사고가 발생하게 된 경우를 의미하며 이러한 사고가 발생하면 즉시 호주 교통안전 위원회에게 보고되어야 한다. 일반 보고 사항은 심각한 사고나 즉각적인 보고가 필요하지 않지만 교통안전에 영향을 미칠 수 있는 사안에 대해 72시간 이내에 호주 교통안전 위원회에게 서면으로 보고하게 된다.

사고에 대한 보고를 받게 되면 호주 교통안전 위원회는 조사를 시행할지 여부를 결정하고 사고 조사를 시작한다. 사고 조사를 위해서는 우선 사고 정보에 대한 사고 현장에 대한 정보, 운영 기록 및 기술 문서 같은 기록 정보, 관련자 정보 같은 증거들을 수집한다. 그리고 수집된 증거들을 바탕으로 검사 및 분석을 통해 수행하여 사고의 원인을 밝히고 최종보고서를 작성하게 된다. 작성된 최종보고서는 내부 검토와 외부 검토를 거쳐 최종 승인 후 배포하게 된다. 그리고 2003년 7월 1일 이후 호주 교통안전 위원회에 보고된 사고에 대한 조사 결과를 검색할 수 있는 데이터베이스를 구축하였다.

[그림 33] 호주 교통안전 위원회의 사고 조사에 따른 보고서 작성 절차




미국과 호주의 교통안전 위원회를 보면 재발 방지를 위해 엄격하고 객관적이며 공정한 조사를 수행해야 하므로 민간 기구로부터 분리된 독립적인 법적 단체로 설립되어 있다. 이는 우선적으로 정치적 또는 기타 간섭과 외압을 견뎌내도록 해야 하기 때문이다. 다음은 처벌에 따른 두려움으로 인한 정확한 조사 방해를 미연에 방지하기 위해 행정적 또는 사법적 처벌과는 독립적인 조사 수행을 위해서이다. 이는 정확하고 빠르게 사고 원인을 밝히고 문제 요인을 제거함으로써 동일한 사고가 다시 발생하는 것을 예방하기 위한 목적이다. 하지만 우리나라는 국토교통부 소속의 사고조사 기관으로 설립되어 사고의 재발 방지를 위한 독립성에 대한 일부 우려가 있다. 이는 조사 기관이

책임 규명에 치중한 조사 진행할 수 있지만 정확한 사고 원인 규명 과정에서 외부의 영향을 받을 수 있는 우려가 있기 때문이다.

미국과 호주의 교통안전 위원회는 비처벌 사고조사를 수행하도록 되어 있다. 미국의 경우 항공 사고에 대한 행정 처분을 위한 사고 조사는 FAA에서 담당하며 두 기관에서 획득한 증거를 서로 공유하지 않고 교통안전 위원회에서 조사한 자료를 FAA를 위한 증거로 제출할 수 없게 되어 있다. 호주도 이와 마찬가지로 교통안전 위원회가 사고원인을 밝히기 위해 비처벌 사고조사를 수행하고 항공안전규제당국인 CASA는 행정처분을 위한 사고 조사를 담당한다. 우리나라도 항공·철도 사고조사를 위한 법률에 민형사상 책임과 관련된 사법절차, 행정처분 절차 또는 행정쟁송 절차와 분리 수행되어야 한다라고 정의되어 있지만 독립적인 기관이 아니기에 엄격하게 분리될 수 있는지에 대한 우려가 있다.

# 제5장 결 론

본 연구는 미래 사회의 SW안전 관리 체계 마련을 위해 SW안전 관리 프레임워크에 대한 연구를 수행하였다. 이를 위해 우선 재난안전법의 안전 관리 기본 체계에 정보통신망법과 개인정보보호법에서 도출한 SW 관리 활동을 추가한 SW안전 관리 프레임워크(안)을 도출하였다. 그리고 이 프레임워크(안)을 검증하고 보완하기 위해 자동차, 철도, 항공 분야의 SW안전 관리 현황을 조사하였다. 교통 분야의 SW안전 관리 현황을 조사해보니 기존 재난안전 분야의 체계는 다가오는 위험인 재난에 대한 예방-대비-대응-복구라는 관점이 명확하였으나 SW 관점에서는 다소 해석에 무리가 있었다.

그래서 전문가 자문을 토대로 인증-운영-응급-사후라는 새로운 체계를 바탕으로 SW안전 관리 프레임워크를 제시한다. 이는 SW 관리 측면을 고려하여 SW와 연관된 용어를 직접 사용하여 SW안전 관리에 대한 이해도를 높이기 위해서이다.  첫 번째 인증 단계는 SW안전에 영향을 미치는 대상을 정의하고 이에 대한 안전 기준 마련하여 충분한 시험을 거쳐 인증을 통해 안전 위험을 예방해야 한다. 운영 단계는 SW를 운영중 상시 또는 주기적인 점검을 통해 발생할지 모르는 사고를 대비해야 한다. 혹시 예상치 못한 사고가 발생한 응급 단계는 사람의 생명과 인체 손상 같은 피해를 최소화하기 위해 빠른 사고 대응이 필요하다. 마지막 사후 관리 단계에서는 발생한 SW안전사고에 대한 철저한 원인 조사와 이를 통한 재발 방지 활동이 필요하다.

이번 연구를 수행함에 있어 SW안전 관리 활동에 대한 조사에 대한 일부 한계점으로는 아직까지 SW안전 활동에 대한 명확 개념이 부족하다는 것이다. 기존의 안전 관리가 하드웨어 중심으로 되어있어서 SW는 이에 포함되는 개념으로 보고 명확한 안전 관리가 수행되고 있지 않다. 하지만 SW 기능이 강력해질수록 SW 특성을 고려한 안전 관리를 더욱 중요해진다고 많은 전문가들이 이야기하였다. 그래서 일부 분야는 응급조치 단계의 사고 신고 자동화 같은 더 많은 SW안전 관리 활동이 필요하다는 의견이었다.

이러한 SW안전 관리 프레임워크에서 가장 중요한 활동은 안전 관리 대상 지정과 이에 관련된 안전 기준으로 생각된다. 그 이유는 이 활동들이 SW안전 확보를 위한 중심이기 때문이다. 관리 대상 지정과 안전 기준 수립을 위해서 우선적으로 관리 대상에 대한 철저한 위험 평가가 이루어져야 하고 이를 기반으로 엄격한 안전 기준이 마련되면 이를 만족하기 위한 인증 제도와 자격 제도가 마련되어야 한다. 그리고 정기적인

안전 점검을 통해 안전성을 확보하고 관리해야 하기 때문이다.

그리고 신기술 분야의 SW안전 관리 활동에 따른 개선은 지속적으로 필요하다는 의견이다. 실제로 자율주행차의 상용화를 위한 시범 운행을 위한 제도 개선이 이루어졌으며 기술 발전에 따라 새로운 안전 관리 대상 지정 및 안전 기준 수립 등은 SW와 밀접하게 연결되어 있다. 그리고 이에 따른 새로운 SW 시험 및 인증, 자율주행차 운전자 교육 및 자격, 안전 점검, 이용자 보호, 사고 및 결함 신고, 사고 조사, 재발 방지 등의 다양한 SW안전 관리 활동에 대한 지속적인 개선 노력이 필요하고 이에 대한 상세 연구가 필요하다.

해외의 안전 선진국들은 교통 분야의 사고 조사 체계를 이원화하는데 그치지 않고 재발 방지의 효율성을 강화하기 위해 독립성을 강화하고 있다. HW와 달리 들어나지 않는 속성을 가진 SW를 고려하면 이 같은 조치는 매우 합리적이다. 들어나지 않기 때문에 문제 원인에 대한 은폐, 왜곡이 상대적으로 쉬우므로 정확하고 빠른 조사와 엄격한 재발 방지를 위해서는 비처벌 조사의 독립성 보장은 향후 4차 산업혁명 시대의 SW안전 관리에 있어 매우 중요하다.

본 연구는 안전 관련된 재난안전법, 정보통신망법, 개인정보보호법, 교통안전법, 자동차 관리법, 철도안전법, 항공안전법, 항공 및 철도 사고조사를 위한 법 등의 다양한 법률들을 중심으로 연구되었다는 한계점이 있다. 물론 현황 조사에서 다양한 사례들을 조사하여 이 한계점을 보강하기 위해 노력을 하였지만 다양한 분야들에 대한 철저하게 조사했다고 보기에는 일부 어려움이 있다. 하지만, 한정된 시간 속에서 SW안전 관리 체계에 대한 연구를 수행함에 있어 시작점으로써 충분히 가치 있다고 본다.

따라서 후속 연구로 분야별 또는 단계별 SW안전 관리에 대한 상세 실태 조사가 필요하고 이를 기반으로 본 연구 결과물인 SW안전 관리 프레임워크를 보완할 수 있다고 본다. 더불어 기존에 SW안전 관리가 수행되지 않는 분야는 본 연구 결과물을 가지고 해당 분야에 맞는 개선된 SW안전 관리 체계를 마련할 수 있다고 본다.

결국 본 연구 결과물은 미래 사회 안전 확보를 위한 SW안전 관리 체계 마련을 위한 기초 자료이자 시작점으로써 충분한 가치가 있으며 이를 토대로 분야별 후속 연구를 통해 4차 산업혁명 시대에 안전 확보를 위해 노력해야 한다.

# 부 록

## 1. 조사대상 선정 설문지 - 주요분야

통계법 제 33 조(비밀의 보호)에 의해 본 조사에서 개인의 비밀에 속하는 사항은 엄격히 보호됩니다.

### 국내외 SW 안전 관리 현황 조사에 대한 대상 선정 설문지

소프트웨어정책연구소(SPRI)는 안전 관련 분야 중 SW 안전과 밀접한 분야 선정하기 위해 30 여개의 안전 관련 법안들을 기반으로 안전 관리 대상 및 분야 파악하고자 합니다.
안전 관련 법안으로는 재난 및 안전관리 기본법, 정보통신 관련 법령, 제품안전(전기용품, 공산품 등) 법령, 교통(자동차, 철도, 선박, 항공 등) 법령, 시설물 (승강기, 공공시설 등) 법령, 에너지(원자력, 유류 등) 관련 법령, 기타 (산업안전, 식품안전 등) 법령 등 7 개 그룹으로 구분하였습니다.
모든 법안에 SW안전 관리 현황을 조사하면 좋겠지만 여러가지 한계점으로 그렇게 하지 못합니다. 그래서, 7 개 그룹 중 **"SW 사고 발생 빈도, SW 사고 사회 파급력, SW 관련성, SW 안전관리 시급성"**에 대한 조사를 주요 대상을 선정하고자 하오니 성심껏 설문에 응답해 주시면 고맙겠습니다.

응답해 주신 내용이 소중한 정책 자료로 반영될 수 있도록 바쁘시더라도 잠시 시간을 내서 협조해 주실 것을 부탁드립니다.

귀하의 성의 있는 답변은 SW안전관리 현황 조사에 중요한 기초자료로 활용될 것입니다. 본 조사 결과는 통계법 제 33 조에 의거하여 비밀이 보장되며, 설문에 대한 모든 응답과 개인적인 내용은 철저히 비밀과 무기명으로 처리되고 통계 및 연구 분석 목적 외에 절대 사용하지 않습니다.

주관 기관 : 소프트웨어정책연구소
조사 책임 : 권영환 선임연구원
조사 담당 : 나이스컨설팅 양회석(hsyang@nicelab.co.kr)

※ 1) SW 안전이란 소프트웨어로 인한 사람의 생명이나 신체에 대한 위험의 발생을 방지하거나 이에 대한 충분한 대비가 되어 있는 상태

| 이름 | | 연락처 | |
|---|---|---|---|
| 업무경력(년) | | 이메일 | |

※ 안전 관련 법안으로는 재난 및 안전관리 기본법, 정보통신 관련 법령, 제품안전(전기용품, 공산품 등) 법령, 교통(자동차, 철도, 선박, 항공 등) 법령, 시설물 (승강기, 공공시설 등) 법령, 에너지(원자력, 유류 등) 관련 법령, 기타 (산업안전, 식품안전 등) 법령 등 7개 그룹

| 분야(그룹) | 분야(상세) | 관련 법안 |
|---|---|---|
| 재난 안전 관련 분야 | 재난, 국민안전, 송유관, 위험물 등 | 재난 및 안전관리 기본법, 정보통신기반 보호법, 국가정보화 기본법, 국가통합교통체계효율화법, 도로교통법, 철도안전법, 도시철도법, 교통안전법, 항공안전법, 항공·철도 사고조사에 관한 법률, 해사안전법, 선박안전법, 시설물의 안전 및 유지관리에 관한 특별법, 송유관 안전관리법, 액화석유가스의 안전관리 및 사업법, 승강기 시설안전법, 위험물안전관리법, 지하안전관리에 관한 특별법, 원자력안전법, 한국원자력안전기술원법, 국민 안전교육 진흥 기본법 등 |
| 정보통신 분야 | 보안, 제품안전, 생활용품 등 | 정보통신기반 보호법, 국가정보화 기본법, 소프트웨어산업진흥법, 제품안전기본법, 전기용품 및 생활용품 안전관리법, 국가통합교통체계효율화법 등 |
| 제품안전 분야 | 전기용품, 공산품 등 | 제품안전기본법, 전기용품 및 생활용품 안전관리법, 품질경영 및 공산품 안전관리법, 제조물책임법, 소비자기본법, 식품안전기본법 등 |
| 교통 분야 | 자동차, 철도, 선박, 항공 등 | 국가통합교통체계효율화법, 자동차관리법, 도로교통법, 철도안전법, 도시철도법, 교통안전법, 항공안전법, 항공·철도 사고조사에 관한 법률, 군용항공기 비행안전성 인증에 관한 법률, 해사안전법, 선박안전법, 국민 안전교육 진흥 기본법 등 |
| 시설물 분야 | 승강기, 공공시설,시설 등 | 국가통합교통체계효율화법, 도로교통법, 철도안전법, 도시철도법, 교통안전법, 해사안전법, 시설물의 안전 및 유지관리에 관한 특별법, 송유관 안전관리법, 액화석유가스의 안전관리 및 사업법, 승강기 시설안전법, 위험물안전관리법, 지하안전관리에 관한 특별법, 원자력안전법, 소규모 공공시설 안전 관리 등에 관한 법률 등 |
| 에너지 분야 | 원자력, 유류, 가스 등 | 송유관 안전관리법, 액화석유가스의 안전관리 및 사업법, 위험물안전관리법, 지하안전관리에 관한 특별법, 원자력안전법, 한국원자력안전기술원법 등 |
| 기타 분야 | 산업안전, 식품안전 등 | 산업안전보건법, 한국산업안전보건공단법, 식품안전기본법, 국민 안전교육 진흥 기본법 등 |

## SW안전 관리 관리 분야 대상 선정 조사

1. 다음 중 분야별 "SW사고 발생 빈도"에 대해 아래 숫자를 선택해주세요.

| 분야(그룹) | 매우낮음 | 낮음 | 보통 | 높음 | 매우높음 |
|---|---|---|---|---|---|
| 재난안전 관련 분야 | 1 | 2 | 3 | 4 | 5 |
| 정보통신 분야 | 1 | 2 | 3 | 4 | 5 |
| 제품안전(전기용품, 공산품 등) 분야 | 1 | 2 | 3 | 4 | 5 |
| 교통(자동차, 철도, 선박, 항공 등) 분야 | 1 | 2 | 3 | 4 | 5 |
| 시설물 (승강기, 공공시설 등) 분야 | 1 | 2 | 3 | 4 | 5 |
| 에너지(원자력, 유류 등) 분야 | 1 | 2 | 3 | 4 | 5 |
| 기타 (산업안전, 식품안전 등) 분야 | 1 | 2 | 3 | 4 | 5 |

2. 다음 중 분야별 "SW사고 사회 파급력"에 대해 아래 숫자를 선택해주세요.

| 분야(그룹) | 매우낮음 | 낮음 | 보통 | 높음 | 매우높음 |
|---|---|---|---|---|---|
| 재난안전 관련 분야 | 1 | 2 | 3 | 4 | 5 |
| 정보통신 분야 | 1 | 2 | 3 | 4 | 5 |
| 제품안전(전기용품, 공산품 등) 분야 | 1 | 2 | 3 | 4 | 5 |
| 교통(자동차, 철도, 선박, 항공 등) 분야 | 1 | 2 | 3 | 4 | 5 |
| 시설물 (승강기, 공공시설 등) 분야 | 1 | 2 | 3 | 4 | 5 |
| 에너지(원자력, 유류 등) 분야 | 1 | 2 | 3 | 4 | 5 |
| 기타 (산업안전, 식품안전 등) 분야 | 1 | 2 | 3 | 4 | 5 |

3. 다음 중 분야별 "SW 관련성"에 대해 아래 숫자를 선택해주세요.

| 분야(그룹) | 매우낮음 | 낮음 | 보통 | 높음 | 매우높음 |
|---|---|---|---|---|---|
| 재난안전 관련 분야 | 1 | 2 | 3 | 4 | 5 |
| 정보통신 분야 | 1 | 2 | 3 | 4 | 5 |
| 제품안전(전기용품, 공산품 등) 분야 | 1 | 2 | 3 | 4 | 5 |
| 교통(자동차, 철도, 선박, 항공 등) 분야 | 1 | 2 | 3 | 4 | 5 |
| 시설물 (승강기, 공공시설 등) 분야 | 1 | 2 | 3 | 4 | 5 |
| 에너지(원자력, 유류 등) 분야 | 1 | 2 | 3 | 4 | 5 |
| 기타 (산업안전, 식품안전 등) 분야 | 1 | 2 | 3 | 4 | 5 |

4. 다음 중 분야별 "SW 안전관리 시급성"에 대해 아래 숫자를 선택해주세요.

| 분야(그룹) | 매우낮음 | 낮음 | 보통 | 높음 | 매우높음 |
|---|---|---|---|---|---|
| 재난안전 관련 분야 | 1 | 2 | 3 | 4 | 5 |
| 정보통신 분야 | 1 | 2 | 3 | 4 | 5 |
| 제품안전(전기용품, 공산품 등) 분야 | 1 | 2 | 3 | 4 | 5 |
| 교통(자동차, 철도, 선박, 항공 등) 분야 | 1 | 2 | 3 | 4 | 5 |
| 시설물 (승강기, 공공시설 등) 분야 | 1 | 2 | 3 | 4 | 5 |
| 에너지(원자력, 유류 등) 분야 | 1 | 2 | 3 | 4 | 5 |
| 기타 (산업안전, 식품안전 등) 분야 | 1 | 2 | 3 | 4 | 5 |

## 2. 조사대상 선정 설문지 - 세부분야

통계법 제 33 조(비밀의 보호)에 의해 본 조사에서 개인의 비밀에 속하는 사항은 엄격히 보호됩니다.

### 국내외 SW 안전 관리 현황 조사 세부 분야 선정 설문지

소프트웨어정책연구소(SPRI)는 안전 관련 분야 중 SW 안전과 밀접한 분야 선정하기 위해 30 여개의 안전 관련 법안들을 기반으로 안전 관리 대상 및 분야 파악하고자 합니다.
30 개 법안 중 전문가에게 "SW 사고 발생 빈도", "SW 사고 사회 파급력", "SW 관련성", "SW 안전관리 시급성"에 대한 설문 조사 결과 "교통 분야"가 높은 점수를 받았습니다.

중요 그룹으로 선정된 교통 분야 중 세분야로 "자동차, 철도, 선박, 항공" 분야이 있기 때문에 세분야에서 대해 "SW 사고 발생 빈도", "SW 사고 사회 파급력", "SW 관련성", "SW 안전관리 시급성"에 대한 조사를 통해 상세 분야를 선정하고자 하니 설문에 성심껏 응답해 주시면 고맙겠습니다.

응답해주신 내용이 소중한 정책 자료로 반영될 수 있도록 바쁘시더라도 잠시 시간을 내서 협조해 주실 것을 부탁드립니다.

귀하의 성의 있는 답변은 SW 안전관리 현황 조사에 중요한 기초자료로 활용될 것입니다. 본 조사 결과는 통계법 제 33 조에 의거하여 비밀이 보장되며, 설문에 대한 모든 응답과 개인적인 내용은 철저히 비밀과 무기명으로 처리되고 통계 및 연구 분석 목적외에 절대 사용하지 않습니다.

주관 기관 : 소프트웨어정책연구소
조사 책임 : 권영환 선임연구원
조사 담당 : 나이스컨설팅 양희석 이사(hsyang@nicelab.co.kr)

| 이름 | | 연락처 | |
|---|---|---|---|
| 업무경력(년) | | 이메일 | |

※ SW 안전이란 소프트웨어로 인한 사람의 생명이나 신체에 대한 위험의 발생을 방지하거나 이에 대한 충분한 대비가 되어 있는 상태

※ 교통에 대한 자동차, 철도, 선박, 항공 등에 대한 법령 상세입니다.

| 분야(그룹) | 분야(상세) | 관련 법안 |
|---|---|---|
| 교통 분야 | 자동차 분야 | 국가통합교통체계효율화법, 자동차관리법, 도로교통법 |
| | 철도 분야 | 철도안전법, 도시철도법 |
| | 선박/해양분야 | 항공안전법, 항공·철도 사고조사에 관한 법률, 군용항공기 비행안전성 인증에 관한 법률, |
| | 항공 분야 | 해사안전법, 선박안전법 |
| | 기타 | 교통안전법, 국민 안전교육 진흥 기본법 등 |

## SW 안전 관리 관리 분야 대상 선정 조사

**1. 다음 중 분야별 "SW사고 발생 빈도"에 대해 아래 숫자를 선택해주세요.**
**(매우낮음-1, 낮음-2, 보통-3, 높은-4, 매우높음-5)**

| 상세 분야 | 매우낮음 | 낮음 | 보통 | 높음 | 매우높음 |
|---|---|---|---|---|---|
| 자동차 분야 | 1 | 2 | 3 | 4 | 5 |
| 철도 분야 | 1 | 2 | 3 | 4 | 5 |
| 선박/해양분야 | 1 | 2 | 3 | 4 | 5 |
| 항공 분야 | 1 | 2 | 3 | 4 | 5 |
| 기타 | 1 | 2 | 3 | 4 | 5 |

선정의견 :

**2. 다음 중 분야별 "SW사고 사회 파급력"에 대해 아래 숫자를 선택해주세요.**

| 상세 분야 | 매우낮음 | 낮음 | 보통 | 높음 | 매우높음 |
|---|---|---|---|---|---|
| 자동차 분야 | 1 | 2 | 3 | 4 | 5 |
| 철도 분야 | 1 | 2 | 3 | 4 | 5 |
| 선박/해양분야 | 1 | 2 | 3 | 4 | 5 |
| 항공 분야 | 1 | 2 | 3 | 4 | 5 |
| 기타 | 1 | 2 | 3 | 4 | 5 |

선정의견 :

3. 다음 중 분야별 "SW 관련성"에 대해 아래 숫자를 선택해주세요.

| 상세 분야 | 매우낮음 | 낮음 | 보통 | 높음 | 매우높음 |
|---|---|---|---|---|---|
| 자동차 분야 | 1 | 2 | 3 | 4 | 5 |
| 철도 분야 | 1 | 2 | 3 | 4 | 5 |
| 선박/해양분야 | 1 | 2 | 3 | 4 | 5 |
| 항공 분야 | 1 | 2 | 3 | 4 | 5 |
| 기타 | 1 | 2 | 3 | 4 | 5 |

선정의견 :

4. 다음 중 분야별 "SW 안전관리 시급성"에 대해 아래 숫자를 선택해주세요.

| 상세 분야 | 매우낮음 | 낮음 | 보통 | 높음 | 매우높음 |
|---|---|---|---|---|---|
| 자동차 분야 | 1 | 2 | 3 | 4 | 5 |
| 철도 분야 | 1 | 2 | 3 | 4 | 5 |
| 선박/해양분야 | 1 | 2 | 3 | 4 | 5 |
| 항공 분야 | 1 | 2 | 3 | 4 | 5 |
| 기타 | 1 | 2 | 3 | 4 | 5 |

선정의견 :

# 참 고 문 헌


**[참조 법률]**

재난 및 안전관리 기본법
정보통신망 이용촉진 및 정보보호법
개인정보보호법
국토교통부와 그 소속기관 직제(대통령령)
교통안전법
자동차관리법
도로교통법
철도안전법
도시철도법
항공안전법
항공·철도 사고조사에 관한 법률
군용항공기 비행안전성 인증에 관한 법률
항공안전 및 보안에 관한 법률
드론 활용의 촉진 및 기반조성에 관한 법률

**[국내 문헌]**

소프트웨어정책연구소(2016), 『소프트웨어 안전 관리 관점에서의 기반시설 보호 법제 개선 연구』
소프트웨어정책연구소(2016), 『이슈리포트-자동차 산업의 SW안전 이슈와 해결 과제』
소프트웨어정책연구소(2017), 『이슈리포트-SW안전 체계 확보와 중점 추진과제』
소프트웨어정책연구소(2017), 『지능정보사회를 대비한 안전관리체계 리모델링에 관한 연구』
소프트웨어정책연구소(2018), 『소프트웨어 안전 확보를 위한 개발 프로세스 적용 확산 방안 연구』
정보통신산업진흥원 (2017), 『공통 분야(IEC 61508) 소프트웨어신뢰·안전성 확보를 위한 가이드』
정보통신산업진흥원 (2017), 『자동차 분야(ISO26262) 소프트웨어신뢰·안전성 확보를 위한 가이드』
정보통신산업진흥원 (2017), 『철도 분야(IEC62279) 소프트웨어신뢰·안전성 확보를 위한 가이드』
국토교통부(2015), 『항공안전관리체계 진단』
국토교통부(2018), 『2018년도 교통안전연차보고서』, 교통안전공단
국토교통부(2018), 『항공안전백서』, 국토교통부 항공정책실
국토해양부(2009), 『교통안전관리규정 표준모델』, 국토해양부 교통안전과
국토교통부(2018), 『교통안전연차보고서』
국토교통부(2016), 『제3차 철도안전 종합계획(안)
교통안전공단(2016), 『철도안전백서』
자동차안전연구원(2018), 『연차보고서』
한국교통연구원(2015), 『국토교통부 항공안전관리체계 진단(최종보고서)』
한국교통연구원(2014), 『항공철도사고조사위원회 중장기발전계획 연구』
한국교통연구원(2017), 『ATSB(호주교통안전위원회) 사고조사체계 조사분석을 위한 국외출장보고서』
한국교통연구원(2017), 『NTSB(미연방교통안전위원회) 사고조사체계에 대한 조사분석을 위한 국외출장보고서』
한국교통연구원(2017), 『미래 도로교통체계 관련 법제 동향 및 기초 입법평가 연구』

한국교통연구원(2017), 『자율주행자동차 도입의 교통부문 파급효과와 과제』
한국교통연구원(2018), 『국가 사고조사 체계 및 항공기사용사업 비행훈련 관리방안』
한국인터넷진흥원(2019), 『ISMS-P_인증기준_안내서』
행정안전부(2018), 『180228 (사고조사담당관실) 국민이 신뢰하는 독립적 재난조사기구 설립 추진(외부)』
법제연구원(2018), 『재난 및 안전관리 기본법 체계 정비를 위한 연구』
KISTEP(2017), 『자율주행자동차 활성화를 위한 법제 개선방안 및 입법제안』
한국정보화진흥원(2015), 『SW중심 안전사회 실현 추진전략 수립을 위한 정책연구』
김상암,조연옥(2009), 『철도종합안전기술개발사업의 추진과 안전관리체계(SMS) 구축 방안』, 한국철도학회
오인택,팽정광,장성용(2008), 『안전관리규정과 철도종합안전심사결과 분석을 통한 국내 철도안전관리체계 개선에 관한 연구』, 한국철도학회
최진석, 안효솔(2019), 『철도부문 형식승인제도 개선 연구』, 한국교통연구원
손영삼,이지하(2018), 『철도형식승인 제도의 현황과 발전방향』, 한국철도학회
배영훈,신덕호,엄주환,고태환(2018), 『철도 시험・인증제도 현황 및 동향』, 한국철도학회

**[해외 문헌]**

Smith, David J. and Simpson, Kenneth G. L. (2004), "Functional Safety(A Straightforward Guide to Applying IEC 61508 and Related Standards)", Hutterwirth-Heinemann

**[참조 사이트]**

개인정보보호 종합 포털 (https://www.privacy.go.kr/)
소프트웨어 정책연구소 산업동향 (https://spri.kr/posts/view/22690?code=industry_trend)
교통안전공단 철도안전정보종합관리시스템 (https://www.railsafety.or.kr/)
국토교통부 관련 사이트 (http://www.molit.go.kr/USR/WPGE0201/m_19475/DTL.jsp)
국토교통부 철도안전관리체계 (http://www.molit.go.kr/USR/policyData/m_34681/dtl?id=438)
국토교통부 철도안전정보종합관리 (http://www.molit.go.kr/USR/policyData/m_34681/dtl?id=444)

## 주 의

1. 이 보고서는 소프트웨어정책연구소에서 수행한 연구보고서입니다.
2. 이 보고서의 내용을 발표할 때에는 반드시 소프트웨어정책연구소에서 수행한 연구결과임을 밝혀야 합니다.

비매품/무료
93500
9 788961 084611
ISBN 978-89-6108-461-1

**[소프트웨어정책연구소]**에 의해 작성된 **[SPRI 보고서]**는 공공저작물 자유이용허락 표시기준 제 4유형**(출처표시-상업적이용금지-변경금지)**에 따라 이용할 수 있습니다.
(출처를 밝히면 자유로운 이용이 가능하지만, 영리목적으로 이용할 수 없고, 변경 없이 그대로 이용해야 합니다.)