ISSUE REPORT I 2024.03.27 IS-170

# 소프트웨어 안전 사고 사례로 보는 소프트웨어 안전 체계 필요성

## The Need for a Software Safety System Viewed Through Software Safety Incident Cases

박태형 / 이중엽 / 손효현

SPRi 소프트웨어정책연구소
Software Policy & Research Institute

이 보고서는 「과학기술정보통신부 정보통신진흥기금」에서 지원받아 제작한 것으로
과학기술정보통신부의 공식의견과 다를 수 있습니다.
이 보고서의 내용은 연구진의 개인 견해이며, 본 보고서와 관련한 의문 사항 또는 수정·보완할 필요가 있는 경우에는 아래 연락처로 연락해 주시기 바랍니다.

소프트웨어정책연구소 산업정책연구실
박태형 책임연구원 parkth@spri.kr

# CONTENT

Ⅰ. 논의 배경 P.1

1. 연구 배경 및 목적
2. 연구 내용 및 방법

Ⅱ. 소프트웨어 안전 사고 사례 분석 P.6

1. 분석 개요
2. 소프트웨어 알고리즘 오류 및 품질 결함으로 인한 사고 사례
3. 소프트웨어 안전기능 오작동 사고 사례
4. 소결

Ⅲ. 결론 및 제언 P.21

# 요 약 문

디지털 심화 사회에서 소프트웨어는 점점 더 중추적인 역할을 맡으며 산업 전반에 걸쳐 고부가가치를 창출하고 있다. 특히 모바일 컴퓨팅, 양자컴퓨터, 사물인터넷(IoT), 자율주행차, 빅데이터, 인공지능(AI), 로봇공학, 블록체인 등 4차 산업혁명의 핵심 영역에서 기술 발전을 가속화하는 중요한 요소로 자리 잡고 있다. 디지털 전환 가속은 디지털 사회의 복잡성과 의존성을 심화시키며 잠재적 위협이 되는 한편 디지털 기술을 활용한 안전 고도화의 기반으로도 자리매김한다. 소프트웨어 적용 확대로 인한 잠재적 위험 증가는 신체적 상해뿐만 아니라 사회적, 경제적 손실을 유발하는 사고로 이어질 수 있다. 이제 자연적·사회적 재난 사례의 증가뿐 아니라 디지털 공간에서의 안전 위협 사례가 빈번함에 따라, 소프트웨어 안전 확보는 주요 과제로 더욱 대두된다.

소프트웨어 안전은 외부 침해 없이 소프트웨어로 인해 발생할 수 있는 사고로부터 인간의 생명이나 신체에 대한 위험에 대비하는 상태를 의미한다. 이는 'Safety of Software'와 'Safety through Software' 두 가지 측면으로 좀 더 나누어 볼 수 있다. 'Safety of Software'은 소프트웨어 자체의 무결성을 보증하며, 사용자와 이용자에게 미칠 수 있는 위험으로부터 안전하게 보호하는 소프트웨어 설계를 포함한다. 즉, 소프트웨어로 인한 사고가 발생하지 않도록 소프트웨어 자체 품질 수준을 확보하는 것을 염두에 둔다. 'Safety through Software'은 소프트웨어 안전 기능을 중점으로 하여 발생 가능한 사고를 감소 및 예방하고, 비상 상황에 대응하는 것을 말한다. 이 보고서는 각각의 사례를 분석하여 소프트웨어 안전 관리 관점에서의 미비한 부분과 개선 방향을 조명하고, 추가적으로 보완해야 할 부분을 식별한다. 이를 통해 안전관리 프레임워크 차원에서 체계적으로 살펴 우리 정책의 개선 방안을 제시하고자 한다.

# Executive Summary

In the digitally advanced society, software is becoming increasingly central, driving high-value creation across industries. It's particularly influential in accelerating technological advancements in key areas of the Fourth Industrial Revolution, such as mobile computing, quantum computing, the Internet of Things (IoT), autonomous vehicles, big data, artificial intelligence (AI), robotics, and blockchain. The acceleration of digital transformation deepens the complexity and dependence in digital society, posing potential threats while also serving as a foundation for enhanced safety through digital technology. The rise in natural and social disasters, along with frequent safety threats in digital spaces, has made securing digital safety for citizens a primary concern. The expansion of software applications increases potential risks, leading to accidents causing physical, social, and economic damages, necessitating preventive and management measures.

Software safety refers to the state where there is sufficient preparation against risks to life or physical harm from accidents caused by software, in the absence of external breaches. This can be divided into two concepts. First, 'Safety of Software' ensures the integrity of software itself, maintaining the safety level to prevent accidents caused by the software. Recent examples include autonomous vehicles and smart factories, where embedded software must guarantee integrity and safeguard against potential risks. Software algorithm malfunctions and abnormal operations can lead to human casualties. Second, 'Safety through Software' focuses on utilizing software safety features to reduce and prevent potential accidents, and ensuring safety in emergency situations. This includes incidents where software errors in safety devices fail to prevent, and instead cause, major accidents. This report examines such cases to analyze shortcomings and directions for improvement in software safety management, identifying areas needing further enhancement. Through this, we aim to systematically examine our policy's improvements within the safety management framework.

# I. 논의 배경

## 1. 연구 배경 및 목적

□ 소프트웨어는 디지털 심화 사회에서 점점 더 중추적인 역할로 자리매김하며 산업 전반의 고부가가치 창출에 영향력을 확대 중

○ 특히 모바일 컴퓨팅, 양자컴퓨터, 사물인터넷(IoT), 자율주행차, 빅데이터, 인공지능(AI), 로봇공학, 블록체인 등 4차 산업혁명의 핵심 영역에서 기술 발전을 가속화하는 중요한 구성 요소로 더욱 영향 확대

- 자동차 분야는 과거 기계장치 중심에서, AI기반의 지능형교통시스템(AI Intelligent Transportation Systems)으로 전환하며 소프트웨어의 원가 비중이 52.4%에 달하고 있으며 전기차는 '25년 70% 수준까지 증가 전망

  * BMW 7은 150개 이상 ECU(electronic control unit) 포함, Ford F-150은 1억 5천만 줄의 코드를 포함

- 항공 분야도 기체의 대형화, 속도·기능 향상 등을 위해 다양한 소프트웨어를 적용하여 전체 개발비의 50%, 항공기 가격 40% 수준으로 비중 증가

  * 1960년대 F-4의 SW 비중은 8%였으나, 최신 F-35의 SW 비중은 90% 육박

- 의료 분야는 최근 디지털 기반의 의료기기 비중 증가로 소프트웨어 비중이 46%까지 증가

○ 소프트웨어 및 디지털 콘텐츠 연구개발 투자 비용은 전년 대비 21.7% 증가한 3조 4,549억 원을 기록하며 타 산업에 비해 높은 성장률 기록(IITP, '23.4.)[1)]

- 또한 '16년부터 '21년까지 14.3%의 연평균 성장률을 기록하며 전체 ICT 부문 중 가장 높은 성장을 보이며 산업 전반의 고부가가치 창출에 소프트웨어의 역할과 기대가 급증하고 있음을 강조

1) ICT 기업 R&D 통계, 정보통신기획평가원, 2023.4.

* ICT분야 ’16~’21년 연평균 성장률 : (디바이스업) 8.2%, (SW·디콘업) 14.3%, (서비스업) 5.9%, (ICT산업 전체) 8.6%

○ 아직 국내 기업들의 본격적인 디지털 전환이 초기 단계인 것을 고려하면 이러한 소프트웨어의 영향력은 향후에도 지속적으로 확대될 것으로 전망

- 우리 기업들의 디지털 전환 추진이 증가하는 추세이나 여전히 과반 이상의 기업(61.5%)들은 관련 프로젝트 추진 전인 상황[2)]

**[그림 1]국내 기업 디지털전환 추진 여부**




* 자료: 2022년 SW융합 실태조사(SPRi, 2023.6.)

□ 디지털 전환 가속은 디지털 사회의 복잡성과 의존성을 심화시키며 잠재적 위협이 되는 한편 디지털 기술을 활용한 안전 고도화의 기반으로도 자리매김

○ 자연적·사회적 재난 사례의 증가뿐 아니라 디지털 기술과 연계한 안전 위협 사례가 빈번함에 따라, 국민의 디지털 안전 확보가 주요과제로 등장

- 소프트웨어 적용 확대에 따른 잠재적 위험 증가로 상해와 함께 사회·경제적 손실을 유발하는 사고도 발생 되어 이를 예방하고 관리하는 필요성 확대

* ’22년 美 도로교통안전국은 최근 10개월간 자동차 첨단운전자보조시스템(ADAS) 관련 사고 392건 발생하고 6명 사망 발표(’22, 美 도로교통안전국NHTSA)

2) 2022년 SW융합 실태조사, 소프트웨어정책연구소, 2023.6.

* 국내는 ’22년 자동차부문 레벨3 자율주행차 안전기준 강화를 하고, ’20년부터 디지털인프라 진단 및 개선을 위해 SW 안전진단 항목에 대한 무료 진단 및 개선 지원

* 전 세계적으로 자동차 산업에서 전장부품 확대에 따른 소프트웨어 리콜 비중이 증가하는 가운데 국내에서도 관련 리콜 및 무상수리가 확대되는 상황

**[그림 2] 차량 소프트웨어 관련 리콜/무상수리 현황**




**차종별 리콜/무상수리 현황**

| 구분 | 출시 | 조치(건) | SW조치(건) | SW비율 (%) |
|---|---|---|---|---|
| 그랜저(CN7) | ’22.11 | 14 | 10 | 71.4 |
| 아이오닉6(CE) | ’22.9 | 8 | 5 | 62.5 |
| EV6(CV) | ’21.8 | 13 | 9 | 69.2 |
| 아이오닉5(NE) | ’21.4 | 17 | 10 | 58.8 |
| 쏘렌토(MQ4) | ’20.3 | 26 | 15 | 57.7 |

* 자료: 국토교통부 자동차리콜센터

○ AI·IoT등의 기술은 재난 안전이나 생활 안전 등 국민 생활과 밀접한 영역에서 위기 예측, 의사결정지원 등 혁신적인 안전 서비스를 제공하는 기회로도 활용

- 건설분야의 스마트 안전기술은 단순 안전 관제(Monitoring)의 역할을 넘어 센싱을 통한 관리 업무 효율화 및 안전설계·위험확인 등의 분야에도 확대 적용[3)]

3) 스마트 안전기술 동향 분석과 시사점, 대한건설정책연구원, ‘22.09.

- 과기정통부는 주요 안전분야(일터·생활·재난)에 디지털 기술을 융합하여 국민안전 체감성과를 창출하기 위해 '디지털 안전 선도모델 개발' 사업을 진행('23.2.)

□ 디지털 경제를 우리 산업 도약의 기회로 온전히 활용하기 위해서는 동전의 양면과 같은 소프트웨어 기술 적용의 명과 암을 제대로 관리하는 것이 필요

○ 이를 위해 소프트웨어 안전에 대해 다시 한번 주목하여 체계적인 관리를 위한 방향을 제시하고 현 관리 수준에 대한 법제적 보완 수준을 파악하는 것이 필요

## 2. 연구 내용 및 방법

□ 소프트웨어 안전 관련하여 전반의 체계 확립과 함께 산업·분야별 특성을 고려하기 위해 관련 사례 분석을 통한 소프트웨어 안전 체계 보완점을 검토

○ 소프트웨어 진흥법(이하 진흥법)의 전면개정을 통해 기존 SW산업의 내부관점에서 SW가 활용되는 국가의 전영역이 대상으로 포함됨

- 또한, 진흥법의 전면 개정을 통해 "소프트웨어 안전" 개념 도입

[그림 3] 소프트웨어 진흥법 개정방향




* 자료: 과기정통부 "SW진흥법 전면 개정"(2020년)

○ 소프트웨어 안전관련 산업이 발전할 수 있는 계기는 마련되었으나, 보다 명확하게 관련 내용을 적용하기 위해서는 법제 및 체계 적용의 명확화 및 확장 필요

- 현행 진흥법 및 고시의 세부규정 마련, 규정 명확화가 필요하며, 산업 진흥을 위한 인식 제고, 지원 등 구체적 법제 마련 필요
- 산업별 특성을 고려하여 지원, 홍보, 관리 규정 등 법·시행령으로 규정이 필요한 법제도에 대한 입법, 제도적 보완 검토

○ 본 고는 소프트웨어 산업육성 및 활용확산을 목표로 현행 진흥법을 기반으로 소프트웨어 안전체계 확립 및 관련 진흥 정책을 마련하기 위해 주요 사례를 다각도(알고리즘 오류 및 품질 결함, 안전기능 오작동)로 분석하고 이를 통한 시사점을 반영하여 체계 정비를 위한 기반 마련 목적으로 진행

# Ⅱ. 소프트웨어 안전 사고 사례 분석

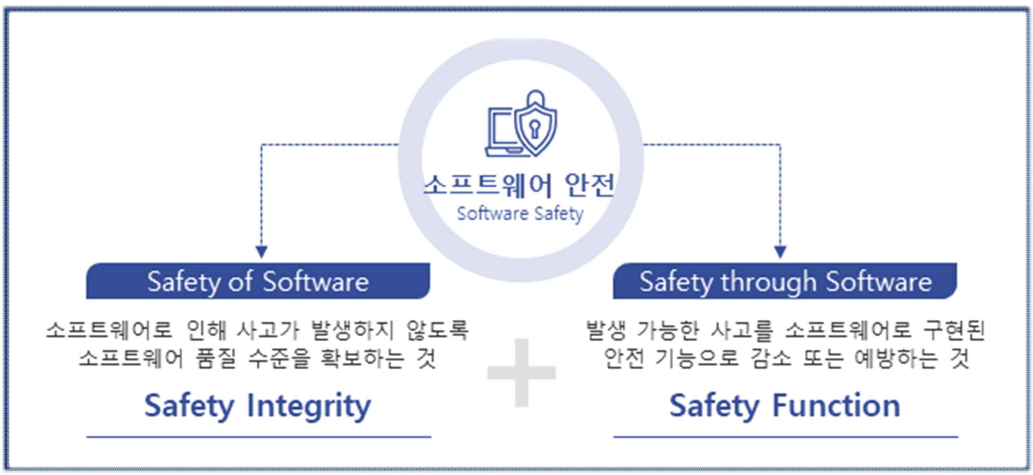
## 1. 분석 개요

□ 소프트웨어 활용 증가에 따라 발생하는 다양한 유형의 사고 사례를 소프트웨어 안전 관점에서 분류하고 분석하여 소프트웨어 안전 대응체계 마련 필요성을 강조

○ 소프트웨어 안전은 외부로부터 침해행위가 없는 상태에서 소프트웨어로 인해 발생할 수 있는 사고로부터 사람의 생명이나 신체에 대한 위험에 충분한 대비가 되어 있는 상태[4)]

- 즉, “대비가 되어 있는 상태”로 정의하여 적극적인 대비가 수행된 상태를 “안전”으로 정의 할 수 있으며, 이는 결국 두가지 의미로 분류 해석 가능함

[그림 4 ] 소프트웨어 안전 분류




○ (Safety of Software) 소프트웨어 자체의 무결성을 보증하며, 소프트웨어의 안전성 즉, 소프트웨어로 인한 사고가 발생하지 않도록 소프트웨어 자체 품질 수준을 확보

4) 소프트웨어 진흥법 제2조에 의거 소프트웨어 안전은 “외부로부터의 침해행위가 없는 상태에서 소프트웨어의 내부적인 오작동 및 안전기능(사전 위험분석 등을 통하여 위험발생을 방지하는 기능을 말한다) 미비 등으로 인하여 발생할 수 있는 사고로부터 사람의 생명이나 신체에 대한 위험에 충분한 대비가 되어 있는 상태를 말한다.”로 정의

- 최근 자율주행차량 및 스마트팩토리 등 일상과 산업에 도입된 다양한 ICT제품들에 내포되어 있는 소프트웨어는 그자체의 무결성이 보증되어야 하며 사용자 및 이용자들에게 미칠 수 있는 위험상황으로부터 안전하게 보호할 수 있는 소프트웨어 설계가 필요

- 이러한 관점에서 소프트웨어 알고리즘 오작동 및 비정상적인 작동 등은 인명피해를 야기하기도 함

○ (Safety through Software) 소프트웨어 안전기능을 중점으로 발생 가능한 사고를 감소 및 예방하고, 비상 상황에 대응 가능한 소프트웨어를 활용하여 안전 보증

- 안전장치로 활용되는 소프트웨어에 오류가 발생하여 사고를 예방하지 못하고 오히려 큰 사고를 야기한 사례 중점 분석

□ 소프트웨어 안전 사고 또한 사람 생명이나 신체에 대한 위협, 나아가 사회 재난에 속하는 결과를 초래하기도 함으로써 안전 관리 체계의 기본적 구성을 바탕으로 분석이 필요

○ 본 고에서는 기존 소프트웨어 안전 관리 방향과 프레임워크 연구를 수행한 자료 중 안전 관리 프레임워크(안)을 기반으로 소프트웨어 안전 사고 사례에서 미비한 부분과 개선된 방향성을 분석하고, 추가로 보완해야할 부분을 식별하고자 함

□ 분석 기준은 소프트웨어 안전 관리 프레임워크[5]에서 '안전 조직 및 관리계획', '안전관리 활동', '안전 기반 조성'을 중점으로 소프트웨어 안전 사고의 원인과 대응, 개선방안에 있어 보완해야 할 부분을 식별

5) SPRi, SW안전관리 프레임워크 연구 내용으로 재난안전법, 정보통신망법, 개인정보보호법의 법체계를 분석하여 소프트웨어 안전 관리 프레임워크를 도출

[그림 5] 소프트웨어 안전 관리 프레임워크(안)




* 출처 : SPRi, 소프트웨어 안전 관리 프레임워크 연구(2020.04.)

○ (안전조직 및 관리 계획) 소프트웨어 안전 관리를 담당하는 조직 구성 및 운영 여부, 산업별 소프트웨어 안전 관리 활동 및 역할, 기능 정의, 소프트웨어 안전 관리 계획 수립 등

- 소프트웨어 안전 사고 발생 당시 산업별 소프트웨어 안전 관리 담당 조직 구성 여부, 소프트웨어 안전 정의 및 관련 대응 계획 여부 등 분석

○ (안전관리 활동) 소프트웨어 안전 관리 측면에서 예방-대비-대응-복구 4단계로 세분화하여 SW안전 관리대상 식별, SW안전 관련 담당자 및 종사자 필요 자격 요건 및 역량 강화를 위한 교육, SW안전 점검실행, SW안전 기준 제시, SW안전사고 발생 시 사고 신고 및 통지, 사고 원인 및 피해상황 파악, 재발 방지 등의 절차 진행 필요

- 소프트웨어 안전 사고 발생 전·후 과정에서 안전관리 활동 4단계가 적절하게 이루어졌는지 분석

○ (안전 기반 조성) SW안전에 대한 사회적 인식 제고를 위해 안전 교육 및 훈련, 행동 요령 개발 및 보급, 안전관련 통계현황 공유 등의 활동, SW안전 확보를 위한 신기술 개발, SW안전 강화를 위한 정보 공유 시스템 구축, SW안전 논의를 위한 국가간 협력 등

- 소프트웨어 안전 사고 사례로 보아 SW안전 기반 조성을 위해 보완되어야 할 부분 중점 분석

## 2. 소프트웨어 알고리즘 오류 및 품질 결함으로 인한 사고 사례

### □ 제너럴모터스(GM) 크루즈 자율주행차량-보행자 사고(2023.11.)[6)]

[그림 6] 크루즈의 자율주행차량 로보 택시




* 출처 : Paul Sancya/AP

○ (개요) 샌프란시스코에서 보행자가 일반차량에 치인 뒤 그 충격으로 크루즈 로보택시가 주행하던 옆 차선으로 튕겨져나갔으나, 로보택시는 이 상황을 측면 충돌로 부정확하게 인식하여 정차 대신 주행하면서 보행자를 약 6미터 가량 끌고가는 사고 발생

○ (SW원인) 크루즈는 자율주행차량이 충돌 후 그 자리에 정지하거나 옆 부분에 정차할 수 있었으나, 소프트웨어 결함에 따라 사고 당시 정지 대신 길 한쪽으로 빠지려고 이동하였다고 설명

- 당시 로보 택시의 브레이크는 보행자가 차량 밑에 깔리자 바로 작동하였으나, 최초 충돌 이후 7초 동안 보행자를 20피트(약 6m) 더 끌고 가는 '풀오버 동작(pull-over maneuver)'이 이루어진 것으로 파악[7)]

6) BLOTER, GM 자율주행차 크루즈, 보행자 사고로 운행 중단 후 950대 리콜, 2023.11.09.

7) 이데일리, 자율주행車 안전사고 어쩌나…멈춰선 GM 무인 로보택시 '크루즈', 2023.10.25.

○ (피해규모) 보행자 1명 중상

○ (조치사항) 캘리포니아주 차량관리국(DMV[8])은 크루즈 자율주행차량 전면 운행 중단 조치 명령, GM社 크루즈 자율주행차량 950대 대상 자발적 리콜 진행

- 로보택시 서비스 시작 당시에는 DMV로부터 운전자 없는 차량에서의 테스트, 배치, 승객 운송에 요구되는 허가를 받아 운영을 하였지만, 운영 과정에서 발생한 사고사례들로 인하여 DMV는 공공안전에 불합리한 위험이 존재함에 따라 운행허가 중단 진행

- 美 도로교통안전국(NHTSA[9])에 따르면 GM은 자율주행시스템(ADS[10]) 소프트웨어의 충돌 반응과 관련된 결함을 해결하기 위하여 차량 리콜 진행 결정

○ (시사점) 소프트웨어 품질에 대한 안전성이 확보되지 않은 사례로 안전관리 체계에서 예방 및 대비 활동을 얼마나 이행하였는지 점검 및 보완하는 절차가 필요함을 확인 가능

- 크루즈 측은 공식 계정을 통해 당사의 기술에 대한 과정과 시스템, 그리고 공공 안전에 있어 신뢰를 구축할 수 있는 방법들에 대해 검토할 것이라고 밝힌 바 안전성에 대한 점검 및 조치가 이루어질 것으로 보여짐[11]

- 해당 사건으로 인해 최근 GM의 최고경영자(CEO)가 사퇴하였으며, 법률, 정부업무, 상업운영, 안전 및 시스템 팀의 리더 총 9명을 해고하는 추가 결정을 진행

- 사고 경위에 대한 소프트웨어 진단을 통해 필요 부분을 업데이트 하였으며, 향후 운행을 재개하기 위하여 GM은 DMV에 자율주행차량의 안전성을 입증해야함

8) California Department of Motor Vehicles

9) National Highway Traffic Safety Administration

10) Automated Driving System

11) AVING, GM, 美 캘리포니아서 자율주행 실증 전면 중단… “기술 및 안전성 등 전면적 검토”, 2023.10.30.

□ 산업용 로봇發 사고(2023. 11.)[12)]

○ (개요) 경남 고성군 한 파프리카 선별 작업장에서 산업용 로봇의 집게가 로봇 설비 점검업체 직원을 압착한 사고 발생

○ (SW원인) 로봇 센서 이상 유무 확인 및 시운전하는 과정에서 로봇 센서가 작업자를 파프리카가 담긴 박스로 오인하여 작동

- 함께 작업하던 직원이 피해를 줄이고자 로봇 조작을 시도하였으나, 압착이 시작되어 조작이 안되자 전원을 종료 시킴

○ (피해규모) 근로자 1명 사망

○ (조치사항) 현장 안전관리 책임자 등을 상대로 정확한 사고 원인과 과실 여부 수사

- 방호장치 등 설비상 하자나 오작동, 예기치 못한 작동 시 어떤 조치를 취했는지 등 조사할 예정

○ (시사점) 로봇을 작업 현장에서 지속적으로 사용해 왔음에도 불구하고 제품 도입 및 사용 전주기에 대한 안전 기능 점검이 적절했는지 검토하는 것이 필요하며 긴급사항에 보완책 등 발생할 수 있는 위기 상황에 대응할 수 있는 안전 방안의 실제 적용 및 숙달이 요구

- 해당 로봇 센서의 박스 인식 여부에 대해 학습이 적절하게 적용되었는지 사전에 확인할 수 있는 절차의 마련 및 오작동시 비상 조치 등을 통해 추가적인 안전 보완 여부를 검토하는 것이 필요

- 불시에 작동할 수 있는 위험 요소가 있음에도 5년간 작업장에서 사용되어 왔으며, 이에 대한 안전 조치가 마련되지 않은 것으로 보여짐

○ 또한, 로봇 관련 안전 사고의 경우 피해자의 손해배상 측면에서 법적 책임의 모호한 상황이 발생함으로 사고에 대한 책임 및 배상 구체화 필요

- 로봇 관련 사고의 경우 산업재해로 인정되어 근로복지공단의 산업재해보상

12) 중앙일보, "사람 힘으론 꿈쩍도 안해"…'ㄷ' 모양 로봇에 작업자 압착사, 2023.11.08.

보험을 통해 보상 청구 진행, 이외의 경우는 로봇 관리 법인, 책임자 또는 제조사 등의 손해배상 청구 필요

- 이때, 책임의 원리는 기계 자체에 문제가 있을 경우 제조사 또는 판매사가 책임지며, 관리의 잘못일 경우 법인이나 관리자에게 책임
- 그러나, 우리나라의 경우 기계 자체 문제는 제조물 책임법으로 적용되어 피해자가 제조사의 잘못을 입증하는 과정에 어려움 존재

□ 일본 민간 달 착륙선 추락 사고(2023.04.)[13)]

[그림 7] '하쿠토-R 미션1'에 사용된 착륙선



* 출처 : 동아사이언스, http://m.dongascience.com/news.php?idx=60005

○ (개요) 일본 우주기업 아이스페이스(ispace)가 개발한 무인 탐사선 '하쿠토-R 미션1'이 계획된 착륙 순서를 순서대로 완료하고 고도를 낮추며 시속 3.2km의 속도로 감속해 달 표면 고도 5km 지점에 무사히 도달하였으나 직후 시속 320km 속도로 달의 분화구로 추락

○ (SW원인) 원래 평평한 지형인 '꿈의 호수' 평원에 착륙이 예정되어 있었으나, 착륙선의 설계가 완료된 뒤 폭 80km 정도의 충돌구인 '아틀라스 충돌구'

13) 동아사이언스, 일본 민간기업 달 착륙선 실패 원인은 '고도 측정 오류', 2023.05.29.

로 착륙 지점을 변경하면서 고도를 측정하는 소프트웨어에 오류가 발생. 이 때문에 주변 지형보다 3km 정도 높은 달 표면의 분화구 가장자리를 지날 때 착륙선의 고도를 측정하는 센서와 불일치. 하쿠토-R의 컴퓨터는 센서 측정치가 입력된 예상 고도에서 크게 벗어나면, 센서 값을 '비정상'으로 간주해 무시하도록 프로그램[14]되어 있었으며 착륙선에 장착된 레이저 센서가 측정한 고도 사이에 편차가 너무 크자, 컴퓨터는 실제 측정치를 오류로 판단해 거부. 로켓의 연료가 다 떨어진 시점에서, 착륙선은 여전히 달 표면에서 5㎞ 상공에 위치해 있었고 이 거리를 자유 낙하하면서 달표면에 충돌된 것으로 추정

○ (피해규모) 아이스페이스 주가는 기업공개(IPO) 시 주가의 9배가 넘는 2,373엔(약 2만2330 원)까지 올랐으나 사고 후 800엔(약 7530 원) 이하로 떨어졌다 회복 중. 착륙선을 위한 보험에 가입된 덕분에 회사에 미치는 재정적 피해는 최소화할 수 있다고 밝혔으며 매출 손실로 약 1억엔 추정

○ (조치사항) 제작사는 소프트웨어 오류 문제를 해결하여 후속 달 착륙 프로젝트에 진행할 것이라고 밝혀 2024년과 2025년을 목표로 하는 미션2와 미션3는 계획대로 진행할 예정

○ (시사점) 소프트웨어 품질에 대한 안전성 확보를 위해 수 차례 시뮬레이션이 진행된 것으로 알려졌으나 사고의 주된 원인은 착륙 지점이 바뀌었는데 착륙 관련 소프트웨어에 변경 사항이 제대로 반영되지 않은 것으로 판단.

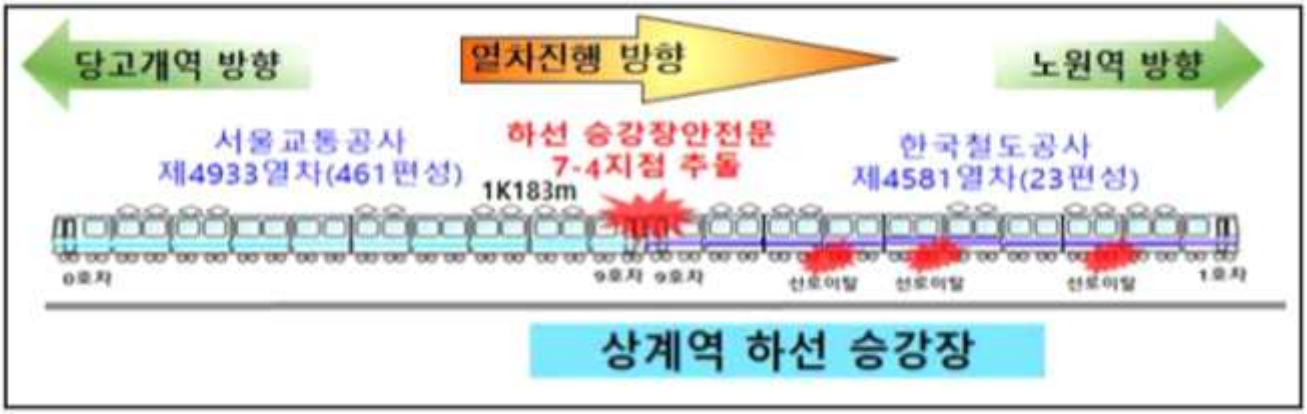
- 또한, 긴급 상황에서의 대응 단계에서도 센서의 측정값과 입력된 기존 값과의 편차 시 센서값 ‘무시’라고 프로그래밍 되어 있던 부분에 대한 추가적인 보완책 등 대응 단계의 신속하고 보다 안전한 보완책 마련이 필요한 사례

14) Cosmos Times, 일본 '달의 야심' 하쿠토-R 왜 추락했나, 2023.05.29.

## 3. 소프트웨어 안전기능 오작동 사고 사례

□ 서울 4호선 상계역 구내 전동열차 간 추돌사고(2020. 06.)[15]

[그림 8] 상계역 구내 열차 추돌사고 상황도




* 출처 : 철도사고조사보고서(ARAIB/R 2021 - 4), 항공·철도사고조사위원회

○ (개요) 4호선에서 창동차량기지로 입고 중인 열차 기관사의 전방주시 소홀 및 차내 신호 상태 미확인 등 관계 규정을 위반하여, 상계역 구내에 정차 중인 다른 열차를 추돌

○ (SW원인) 자동열차제어장치(ATC[16])의 문제 발생으로, '무코드'상황 발생에도 15km/h로 자동 운행되어 추돌 발생

- 무코드가 발생할 경우 ATC의 차상장치[17]가 맘춰야하나 소프트웨어 결함으로 인하여 15km/h모드가 활성화되며 정차하지 못함

○ (피해규모) 전동차 및 승강장 안전문 등 시설물 피해, 승객 80명 긴급대피 및 경상자 일부 발생, 당고개-노원 구간 운행 중단(약 6시간), 서울교통고사 및 한국철도공사 합계 약 3억2천만원 피해 금액 발생

○ (조치사항) 열차 운행 중 차량, 신호, 시설물 등 이상 발견 시 다음 사항을 관계규정에 따라 준수하고 시행할 것을 권고

15) 항공철도사고조사위원회, "(제2021-4호)서울4호선 상계역 구내 전동열차 충돌사고('20.6.11.) 최종보고서"

16) Automatic Train Control

17) 지상의 열차운행 조건을 차상에서 수신하여 차량의 허용속도를 연속으로 표시하고 열차가 허용속도를 초과할 경우 자동으로 열차를 정지 또는 감속시키는 장치

- ATC ‘15km/h’ 스위치 취급 시 승인 내용 또는 이상 발견 시 보고 및 기록 후 관계부서에 통보하여 조치 진행
- ATC 회로개선과 같이 운영 중 설비 개선 시 변경사항에 적합한 검사항목 및 기준 마련 조치

○ (시사점) 안전 사고에 대한 예방 및 대응 장치가 설계되어있으나 소프트웨어의 내부적 오류로 사고 예방은 못하였지만, 사고 이후 대응 및 복구 과정을 통해 동일 사고가 재발하지 않도록 개선하는 방향의 선례

- 안전 장치로 소프트웨어가 작동되었어야 했음에도 불구하고 무코드 모드 대응 오작동으로 인하여 사고가 발생하였으나 철도사고 조사위원회를 통해 사고 원인을 식별하였으며, 해당 부분에 대한 추가 조치 방안 및 기준 마련 수행

□ 에티오피아 보잉 737 추락사고(2019.03.)[18)]

[그림 9] 추락한 보잉 737 사고 잔해



* 출처 : MICHAEL TEWELDE/AFP/Getty Images

18) Ethiopian Civil Aviation Authority - Aircraft Accident Investigation Report B737- MAX 8, ET-AVJ, 2022.12.

○ (개요) 에티오피아 아디스아바바 볼레 국제공항에서 이륙한 에티오피아 항공 ET302편이 이륙한 지 약 6분만에 아디스아바바 동쪽 외곽 상공에서 추락

○ (SW원인) 받음각 센서 이상으로 MCAS[19] 오작동 추락으로 잠정 결정

[그림 10] MCAS 작동 원리




- 다른 이유로 자동운항(Autopilot)장치의 소프트웨어 결함 발생도 예상

  * 항공기 사고 조사국 예비보고서에 따르면 이륙 후 약 1분만에 자동운항장치가 꺼졌다는 교신 기록

○ (피해규모) 탑승인원 157명 전원 사망(승객 149명, 승무원 8명), 항공기 완전 파괴

○ (조치사항) 보잉사 MCAS 재설계 및 MAX 기종 생산 일시중단, 미국 연방항공청(FAA)은 운항 재개 전 새로운 파일럿 교육과 소프트웨어 업그레이드 요청, 40개국에서 MAX 기종 운항 중단 및 9개국에서는 영공통과 금지 조치

○ 이후 2020년 11월 18일 미국 FAA는 운항 중지 약 1년 8개월만에 B737 MAX 항공기 비행 재개를 승인[20]하였으며, 이후 12월에 브라질 골(Gol) 공항에서 첫 운항 재개

○ (시사점) 항공분야의 경우 항공 소프트웨어에 대한 기능안전 표준이

19) MCAS(Maneuvering Characteristics Augmentation System)은 조종특성향상시스템으로 자동실속방지시스템이라고도 불리며, 비행 상태가 비정상적일 때 기수를 일방적으로 내리는 방향으로 조작되는 시스템

20) FAA, Statement on Boeing 737 Max Return to Service, 2020.11.

존재하며 항공기에 대한 유지보수가 주기적으로 이루어지는 체계지만, 본 사고의 MCAS 오작동과 같은 상황은 비정상적인 상황에 대응 하기 위한 안전 조치가 위험 상황을 초래한 결과로 안전장치에 대한 추가적 대비 체계 및 소프트웨어 정밀점검 등 보완 필요

- 해당 항공기의 경우 사고 발생 이전에 비행중 수차례 이상 현상이 발생하여 오류점검 및 유지보수 조치를 수행하였으나 재발된 사례는 없었으며, 정기점검 시에도 문제사항이 없어 운행한 것으로 밝혀짐
- 사고 이전 소프트웨어 문제가 지속적으로 발생했다는 것은 새로운 위협이 될 수 있는 요소가 있다는 가능성을 배제할 수 없으며 기존의 점검 방법외에 추가 안전 기준 및 기술 대응이 필요했을 것으로 보이며 재발 방지 대책이 요구되는 사례
- 항공기 사고 조사국은 예비보고서를 통해 안전 권장사항 조치로 반복적으로 비정상적 항공기 기수 조정 상황이 확인되었음에 따라 비행 통제 가능성과 관련된 항공기 비행 통제 시스템을 제조사에서 검토할 것을 권장함

□ 인도 오디샤주 열차 사고('2023.06.)

○ (개요) 인도 코로만델 익스프레스(Coromandel Express) 소속 12841번 열차가 본선이 아닌 화물열차 선로로 진입해 정차해 있던 화물열차와 충돌하여 객차가 탈선하였으며, 반대편에서 진입하던 SMVT 벵갈루루-하우라 수퍼패스트 익스프레스 (Howrah-SMVT Bengaluru Superfast Express)의 12864번 열차가 탈선해 있던 객차 더미에 충돌하면서 2차 사고가 발생. 열차 사고로 인해 사망자 288명, 부상자 1,175명 총 1,463명의 피해자가 발생

○ (SW원인) 역에 진입하는 열차의 선로 전환과 신호 전달을 책임지는 연동장치에 문제가 발생

- 열차 충돌 방지 시스템 '카바치(Kavach)[21]'가 사고 노선에 미도입된 것도

21) Kavach('Armour')는 인도 철도부 연구설계 표준기구 RDSO(Research Designs & Standards Organization)를 통해 자체 개발한 자동 열차 보호 (ATP, Automation train protection) 시스템. 카바치의 초기 개발은 2012년 열차 충돌 방지 시스템(TCAS, Train Collision Avoidance System)이라는 이름으로

주요한 원인으로 확인. ‘카바치’는 사고 시점 인도 철도 전체 노선의 2%에서만 운영되고 있던 상황

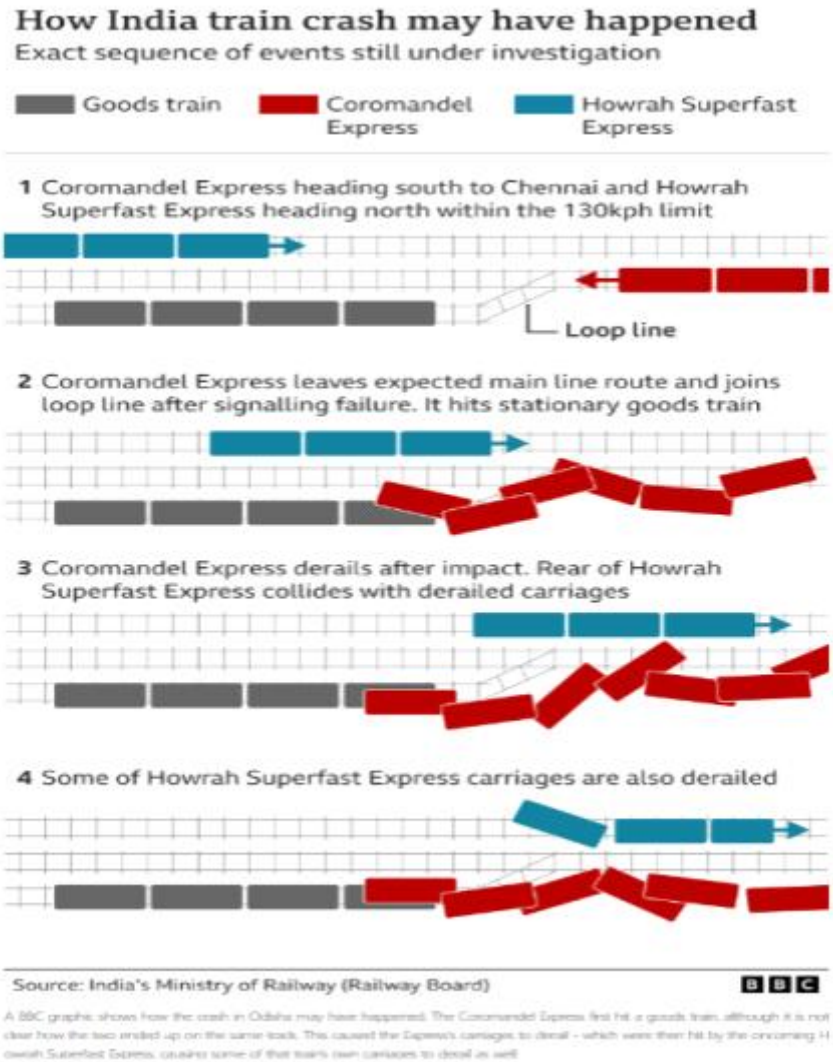
- 인도 민간항공부 산하 철도안전위원회(CRS)는 보고서에서 인부들이 주변의 철도건널목 차단기에서 자주 일어나는 문제를 해결하기 위해 신호 회로 작동을 멈추게 하려다가 자동 신호시스템 내 선을 잘못 연결했다고 설명

○ (조치사항) 구조 및 수습을 위해 115대의 구급차량과 화재 진압 차량을 투입하였고 철도회사는 유족 100만 루피(약 1,600만 원), 중상을 입은 사람 20만 루피(약 320만 원), 경미한 부상자 5만 루피(약 80만 원) 상당의 보상. 인도중앙수사국(CBI)은 신호 엔지니어 2명과 일반 엔지니어 1명을 과실치사, 증거인멸, 철도 여행객 안전을 위험하게 하는 업무태만 등의 혐의로 체포

○ (시사점) 인도의 ‘카바치’ 시스템은 운전자가 속도 제한에 따라 열차를 제어하지 못하는 경우 열차의 제동 시스템이 자동으로 활성화되며 이를 탑재한 두 기관차 사이의 충돌을 방지. 또한 긴급 상황 발생 시에도 SoS 메시지를 전달하며 네트워크 모니터 시스템을 통해 열차 이동을 중앙 집중식으로 실시간 모니터링. '카바치'가 획득한 SIL-4는 오류 확률이 10,000분의 1인 최고 등급. 안전 사고에 대한 예방 및 대응 장치가 개발되어 있으나 예산 및 정책 집행과정에서 전체 노선의 일부에만 적용되고 있으므로 사고 재발 방지를 위해 관련 기관의 집중적인 지원 노력을 통한 개선 필요

시작돼 2022년 개발을 완료했으며 안전 무결성 레벨 4(SIL-4, System Integrity Model) 인증 획득

## [그림 11] 인도 오디샤주 열차 사고 발생 상황




* 출처 : BBC NEWS 코리아, https://v.daum.net/v/VSSU7Dlffz

## 4. 소결

□ 본 고에서는 최근에 발생한 사고사례를 중점으로 대표적인 사건을 기술하였으나, 이와 관련한 사고는 이전에도 지속 발생하였으며 산업별 사고 조사 절차에 따른 조사 및 결론이 나왔을 뿐 소프트웨어 안전 자체에 대한 근본적 대응 방안 제시 미비

○ 크루즈 자율주행차량의 경우 2022년에도 샌프란시스코 내 교차로에서 좌회선하는 도중 갑작스런 급정차로 뒷 차량과 충돌한 사례[22] 등 여러 차례 논란 끝에 운행 중단 및 대대적 시스템 점검 및 기술 검증 수행

○ 로봇의 활용 증가에 따른 사고 사례는 러시아 모스크바 체스 대회에서 로봇이 상대 선수가 규칙을 위반하자 손가락을 잡아 골절되는 상황 발생[23], 설비 청소 작업 중 로봇 팔에 부딪혀 근로자가 사망한 사례[24]등 다수 사례 발생

□ 분야별 산재된 소프트웨어에 대한 위험을 대응하기 위해서는 소프트웨어 안전 관리 체계가 구축되어 적재적소에 관련 매뉴얼과 대응인력이 투입되어 문제 해결 및 사고 분석이 진행되어야 함

○ 특히, 산업용 로봇 및 자율주행차량의 경우 기술력이 발전함에 따라 활용 분야 및 범위가 지속적으로 증가하고 있는 추세인데 이에 대한 안전성 보장 방안은 마련되지 않은 것으로 보여짐

- 산업로봇의 경우 한국산업안전보건공단에서 산업용 로봇 재해예방을 위한 지침을 통해 안전인식을 제고하고 있지만, 현재 예방 단계로는 작업자 내 로봇반경 접근 위험 표시, 로봇 이용 안전 매뉴얼 등 기본적 안전 지침에 대한 접근 시도

- 로봇 제조물을 검증하는 체계에서 작업자에 대한 인지 알고리즘, 비정상적 물질 및 상황에 대한 중단 시스템, 기타 위험 상황에 대한 대응 방안을 마련하였는지 검토할 필요성이 있음

22) Reuters, U.S. agency probing self-driving Cruise car crash in California, 2022.07.08.
23) AI TIMES, “로봇이 뿔났다”…체스 경기 도중 어린아이 손가락 부러뜨려, 2022.07.25.
24) 서울경제, 공장 설비 청소하던 60대 근로자, 로봇 팔에 맞아 숨져, 2023.05.31.

# Ⅲ. 결론 및 제언

□ 앞서 살펴본 SW안전 사고와 같이, SW 자체에 대한 오류 뿐만 아니라 안전을 담보하기 위한 SW의 오류로 인해 발생되는 사고 사례도 갈수록 증가 하고 있음

○ 디지털 사회의 안전은 이러한 다양한 지점에서 발생되는 안전사고를 예방하고 수습하는 것이 또 하나의 정책과제로 부상하고 있음

□ SW안전 확보는 디지털 심화시대에서 국민의 재산과 생명의 안전을 확보하는 국가의 책무를 실현하는 것임

○ 사고 예방과 피해 최소화는 국가와 지방자치단체의 법적 의무로, 적극적 대응의 타당성은 이미 확보

* 헌법 제34조 제6항[25], 재난 및 안전관리 기본법 제4조(국가 등의 책무) 제2항 등

○ 따라서, 디지털 사회의 안전을 확보하기 위해 SW의 안전을 확보하는 정책적 노력이 필요

□ 한편, SW안전을 확보하는 데 가장 효과적이고 확실한 방법은 예방에 있음

○ 사고발생 이후에 사고의 원인을 분석하고 수습하는 일련의 과정은 책임소재 논의로 귀결되어 다양한 형태의 정책자원 낭비와 논란을 유발

○ 같은 맥락에서 SW안전 사고를 예방하는 것은 국민의 안전 신뢰성을 높이고, 불필요한 사회적 비용을 아끼는 데 가장 핵심적인 출발점

□ 안전관리의 관점에서 사고관리는 사고발생의 방지(예방)에서 출발하고, 사고 발생 이후에는 피해최소화를 위해 얼마나 신속하게 대응·복구하는냐가 관건임

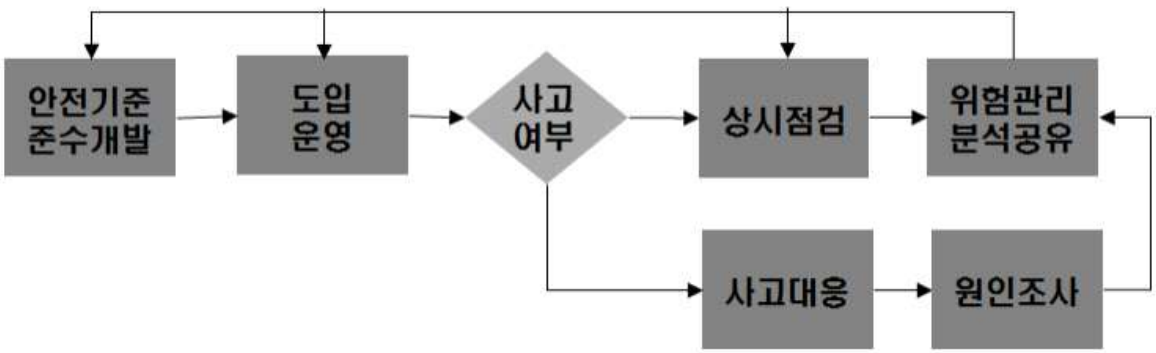
○ 이는 예방체계와 대응체계의 선순환 구조의 확립과 각 체계 간 환류가

25) 헌법 제34조 6항 : 국가는 재해를 예방하고 그 위험으로부터 국민을 보호하기 위하여 노력하여야 한다.

제대로 이루어질 때 가능

- 일상적 예방활동과 사고발생 시 대응활동의 결과가 환류체계 내에서 공유·활용되어야 함을 의미

[그림 12] 사고관리 선순환 체계




□ (SW안전 사고관리 선순환 체계) SW안전 사고관리를 위한 선순환 체계는 예방-대비-대응-복구의 안전관리 전 프로세스에서 유기적으로 활동이 이루어져야 함

○ (예방단계) 안전과 직결된 SW의 개발 및 발주에 있어서 위험원 분석 등 SW안전 개발 요구사항을 철저히 분석·반영하고, 국제표준 등에서 요구하는 기준에 부합하는지 면밀한 검토가 필요

○ (대비단계) 안전 중요 SW의 개발 또는 발주를 통해 도입하여 운영하는 경우에는 SW안전관리계획을 수립하여 시행할 필요가 있으며, 이를 토대로 주기적이고 상시적인 SW안전 진단·점검 체계 구축, 사고대응 매뉴얼의 개발 및 적용, 사고대응 훈련, SW안전 사고 시 비상연락망 구축 등 대비 필요

○ (대응단계) SW안전 사고 발생 시 피해최소화를 위해 신속한 사고원인 분석 및 조치가 필요한데, 이를 위해서 SW안전 전문가가 포함된 사고조사위원회가 가동되어야 하며 평상시 SW안전 사고 조사를 위한 전문가 풀을 구축할 필요

○ (복구단계) SW안전 사고조사 위원회의 결과를 중심으로 신속한 피해복구가 이루어지되, SW안전 사고를 초래한 위험원들에 대한 빠른 후

속 조치 및 정보의 공유·확산 체계 마련이 필요

○ (환류단계) 안전관리의 관점에서 사고를 중심으로 어느 단계에서 취약점이 있는지 식별하고 이에 대한 개선사항을 도출하여 각 단계별로 예방활동 강화, SW안전 관리계획 개선, SW안전 기준 및 매뉴얼 개정 등 후속 조치를 시행할 필요

□ 우리가 최근 경험한 코로나19로 대표되는 물리적 공간에서의 글로벌 팬데믹 현상은 디지털 공간에서 발생할 수 있는 '디지털 팬데믹'에 대한 철저하고 신속한 대응을 요구

○ 디지털 심화시대의 SW는 과거 어느 때보다 복잡성이 높고, 시스템의 SW 의존성은 높아지고 있음

○ 이는 예상하지 않은 사고의 발생 가능성을 높일 뿐만 아니라 그 피해의 규모 또한 광범위해지는 SW안전사고에 대한 정책적 노력이 필요

# 참고문헌

## 1. 참고문헌


- 2022년 SW융합 실태조사, 소프트웨어정책연구소, 2023.6.
- ICT 기업 R&D 통계, 정보통신기획평가원, 2023.6.
- 권영환, 진회승, 송지환, ‘SW안전관리 프레임워크 연구’, 소프트웨어정책연구소, 2020.04.
- 항공철도사고조사위원회, “(제2021-4호)서울4호선 상계역 구내 전동열차 충돌사고(’20.6.11.) 최종보고서”
- 홍성호, 조재용, ‘스마트 안전기술 동향 분석과 시사점’, 대한건설정책연구원, 2022.09.
- Ethiopian Civil Aviation Authority, ‘Aircraft Accident Investigation Report B737-MAX 8, ET-AVJ’, 2022.12.


## 2. 기 타


- 동아사이언스, 일본 민간기업 달 착륙선 실패 원인은 '고도 측정 오류', 2023.05.29.
- 블로터, GM 자율주행차 크루즈, 보행자 사고로 운행 중단 후 950대 리콜, 2023.11.09.
- 서울경제, 공장 설비 청소하던 60대 근로자, 로봇 팔에 맞아 숨져, 2023.05.31.
- 이데일리, 자율주행車 안전사고 어쩌나…멈춰선 GM 무인 로보택시 ‘크루즈’, 2023.10.25.
- 에이빙, GM, 美 캘리포니아서 자율주행 실증 전면 중단… “기술 및 안전성 등 전면적 검토”, 2023.10.30.
- 중앙일보, "사람 힘으론 꿈쩍도 안해"…'ㄷ' 모양 로봇에 작업자 압착사, 2023.11.08.
- AI TIMES, “로봇이 뿔났다”…체스 경기 도중 어린아이 손가락 부러뜨려, 2022.07.25.
- BBC News Korea, 인도 열차 참사 '신호 오류'가 원인인가, 2023.06.05.
- Reuters, U.S. agency probing self-driving Cruise car crash in California, 2022.07.08.
- Cosmos Times, 일본 '달의 야심' 하쿠토-R 왜 추락했나, 2023.05.29.

## 주 의

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

OPEN 공공누리 공공저작물 자유이용허락

**[소프트웨어정책연구소]**에 의해 작성된 **[SPRI 보고서]**는 공공저작물 자유이용허락 표시기준 제4유형**(출처표시-상업적이용금지-변경금지)**에 따라 이용할 수 있습니다.

# 소프트웨어 안전 사고 사례로 보는 소프트웨어 안전 체계 필요성

## The Need for a Software Safety System Viewed Through Software Safety Incident Cases

경기도 성남시 분당구 대왕판교로 712번길 22 글로벌 R&D 연구동(A)
Global R&D Center 4F 22 Daewangpangyo-ro 712beon-gil, Bundang-gu, Seongnam-si, Gyeonggi-do

www.spri.kr

ISSN 2733-6336