

SW 안전 분야 선정기준 및 SW 안전 공통기준 도출 연구

A Research on Software Safety Classification and
Software Safety Common Criteria

송지환 / 진회승 / 권영환 / 민상윤 / 김형호 / 김성원 / 이지연 / 박재진

2018. 12.

이 보고서는 2018년도 과학기술정보통신부 정보통신·방송연구
개발사업의 연구결과로서 보고서 내용은 연구자의 견해이며,
과학기술정보통신부의 공식입장과 다를 수 있습니다.

제 출 문

과학기술정보통신부 장관 귀하

이 보고서를 『SW 안전 분야 선정기준 및 SW 안전 공통기준 도출 연구』의 연구결과보고서로 제출합니다.

2018년 12월

연구기관 : 소프트웨어정책연구소

과제책임자 : 송지환 선임연구원

참여연구원 : 진희승 책임연구원

권영환 선임연구원

민상윤 대표이사 (솔루션링크)

김형호 수석 컨설턴트(솔루션링크)

김성원 수석 컨설턴트(솔루션링크)

이지연 수석 컨설턴트(솔루션링크)

박재진 선임 컨설턴트(솔루션링크)

목 차

요 약 문	i
Summary	viii
제1장 서 론	1
제1절 연구의 배경 및 목적	1
1. 연구의 배경	1
2. 연구의 목적	2
제2절 연구의 구성 및 방법	4
1. 연구의 구성	4
2. 연구의 방법	4
제2장 SW 안전 분류 도출 연구	7
제1절 분야 중심 안전 분류 연구 분석	7
1. 산업일반 분야의 안전 표준	7
2. 철도 분야의 안전 표준	10
3. 항공 분야의 안전 표준	12
4. 자동차 분야의 안전 표준	15
5. 의료기기 분야의 안전 표준	18
6. 분야 중심의 안전 분류 연구 고찰	20
제2절 SW 중심 안전 분류 연구 분석	23
1. MIL-STD-882E	24
2. NASA Software Safety Guidebook	28

제3절 SW 안전 분류 모델	31
1. SW 안전 분류 모델 제안	31
2. SW 안전 분류 모델 개선	32
3. 전문가 자문단 검토 및 SW 안전 분류 보완	45
제4절 SW 안전 분류 도출 및 검증	48
1. SW 안전 분류 도출	48
2. SW 안전 분류 정당성 검증	51
제3장 SW 안전 공통기준 도출 연구	66
제1절 SW 안전 공통기준 관련 연구 분석	66
1. MIL-STD-882E 관련 가이드	66
2. NASA Software Safety Guidebook	68
제2절 SW 안전 공통기준 도출	70
1. 안전 활동 및 기법 선정	71
2. SW 안전 공통기준	72
3. SW 안전 분류 및 SW 안전 공통기준 활용 방법	87
제4장 결 론	89

표 목 차

〈표 1-1〉 소프트웨어산업진흥법 전부 개정안에 포함된 SW 안전 관련 조문 일부	3
〈표 2-1〉 안전 무결성 수준 별 안전기능 고장 기준	8
〈표 2-2〉 위험 파라미터 분류	9
〈표 2-3〉 안전 무결성 수준 별 견딜 수 있는 고장 확률	11
〈표 2-4〉 DO-178C의 고장상태 정의	13
〈표 2-5〉 DO-178C의 SW 레벨 정의	14
〈표 2-6〉 DO-178C의 SW 레벨 별 고장률 기준	14
〈표 2-7〉 ISO 26262 위험 파라미터 수준 정의	16
〈표 2-8〉 ISO 26262 자동차 안전 무결성 수준 결정	17
〈표 2-9〉 IEC 62304 클래스별 피해 정도	18
〈표 2-10〉 MIL-STD-882E의 SW 심각도 등급	25
〈표 2-11〉 MIL-STD-882E의 SW 통제 등급	25
〈표 2-12〉 MIL-STD-882E의 SW 안전 중요도 매트릭스	27
〈표 2-13〉 MIL-STD-882E의 안전활동수준 권고사항	27
〈표 2-14〉 NASA Software Safety Guidebook의 SW 심각도 등급	29
〈표 2-15〉 NASA Software Safety Guidebook의 SW 통제 등급	29
〈표 2-16〉 NASA Software Safety Guidebook의 SW 위험 매트릭스	30
〈표 2-17〉 NASA Software Safety Guidebook의 SW 위험 색인	30
〈표 2-18〉 DO-178C의 위험 심각도	33
〈표 2-19〉 EN ISO 14971 위험 심각도 - 3개 수준	34
〈표 2-20〉 EN ISO 14971 위험 심각도 - 5개 수준	34
〈표 2-21〉 EN ISO 14971의 3개 수준과 5개 수준의 위험 심각도 비교	35
〈표 2-22〉 SW 안전 분류 위험 심각도 정의	36

〈표 2-23〉 자율성 수준 결정 요소	41
〈표 2-24〉 자율성 수준 정의	41
〈표 2-25〉 SW 통제 등급 정의	43
〈표 2-26〉 SW 안전 위험 색인 정의	44
〈표 2-27〉 전문가 자문단 주요 검토 의견	46
〈표 2-28〉 SW 안전 통제 등급 정의 보완	47
〈표 2-29〉 위험 심각도 정의 보완	48
〈표 2-30〉 SW 안전 분류	49
〈표 2-31〉 SW 안전 분류의 SW 안전 통제 등급 정의	50
〈표 2-32〉 SW 안전 분류의 위험 심각도 정의	50
〈표 2-33〉 SW안전위험색인(SSRI)	51
〈표 2-34〉 보행자 AEB 시스템 기능 정의	53
〈표 2-35〉 SW 안전 분류의 위험 심각도 결정	56
〈표 2-36〉 SW 안전 분류의 SW 안전 통제 등급 결정	57
〈표 2-37〉 기존 SW 안전분야 예제 시스템 대상 SW 안전 분류 수행 결과	59
〈표 2-38〉 SW 안전 분류의 위험 심각도 결정	62
〈표 2-39〉 SW 안전 분류의 SW 안전 통제 등급 결정	63
〈표 2-40〉 신규 SW 안전분야 예제 시스템 대상 SW 안전 분류 수행 결과	65
〈표 3-1〉 요구되는 SW 안전 노력	70
〈표 3-2〉 SW 안전 위험 색인 등급 별 안전 요구 활동	72
〈표 3-3〉 SW 안전 공통기준	74
〈표 3-4〉 SW 안전 공통기준(SSRI 1)	75
〈표 3-5〉 SW 안전 공통기준(SSRI 2)	76
〈표 3-6〉 SW 안전 공통기준(SSRI 3)	77
〈표 3-7〉 SW 안전 공통기준(SSRI 4)	78
〈표 3-8〉 SW 개발 단계 안전 활동	79

그 립 목 차

[그림 1-1] 제4차 산업혁명 관련 과학·기술과 산업 간 연계도	2
[그림 1-2] 연구 개요	3
[그림 1-3] SW 안전 분류 정당성 검증 대상 시스템	5
[그림 2-1] 위험 그래프 적용 방법	10
[그림 2-2] IEC 62279의 안전 시스템의 안전 무결성 수준 결정 방법	12
[그림 2-3] ISO 26262의 SW 안전 요구사항 명세 요건	16
[그림 2-4] ISO 26262의 SW 안전 요구사항 작성 기법	17
[그림 2-5] IEC 62304의 SW 안전 분류 방법	19
[그림 2-6] 분야 중심의 안전 분류 수준 비교(실패율 기반)	21
[그림 2-7] SW 안전 분류(견본)와 DO-178C, IEC 62304 요건 관계	22
[그림 2-8] DO-178C의 Software Level D와 IEC 62304의 Class A 요건 비교 ...	23
[그림 2-9] SW 안전 분류 모델 제안	32
[그림 2-10] SW 안전 분류의 위험 심각도 비교 및 도출	36
[그림 2-11] 자율등급에 따른 자율주행차 구분 기준	37
[그림 2-12] 자율주행 등급 별 주요 기능	39
[그림 2-13] Autonomous Horizon 내 자율성 수준	40
[그림 2-14] SW 안전 분류의 SW 통제 등급 비교 및 도출	42
[그림 2-15] SW 안전 분류 초안 도출	44
[그림 2-16] 전문가 자문단 검토용 자료	45
[그림 2-17] 보행자 AEB 시스템 구성도	53
[그림 2-18] 보행자 AEB 시스템 예비 아키텍처	54
[그림 2-19] 보행자 AEB 시스템 HARA 수행 결과	55
[그림 2-20] 보행자 AEB 시스템의 SW 안전 분류 수행 결과	58
[그림 2-21] 차상 PSD 무선장치와 지상 PSD 무선장치의	

연동방식을 나타낸 구성도	60
[그림 2-22] 승무원 조작반	61
[그림 2-23] 전동차 출입문과 지상 스크린도어의 동시 개폐 제어 시스템의 SW 안전 분류 수행 결과	64
[그림 3-1] SW 안전 공학 세부 내용	67
[그림 3-2] SW 위험 색인 수준 별 개발 단계 권고 사항	68
[그림 3-3] SW 개발 단계 별 권고 활동 제공 형식	69
[그림 3-4] 요구사항 단계를 위한 SW 안전 노력	70
[그림 3-5] Software fault tree analysis 예시	81
[그림 3-6] Software failure mode and effect analysis 예시	82
[그림 3-7] Generation and analysis of equivalence classes 예시	84
[그림 3-8] Boundary value analysis 예시	84
[그림 3-9] Statement coverage 예시	85
[그림 3-10] Branchh coverage 예시	86
[그림 3-11] Fault injection 예시	87
[그림 3-12] SW 안전 분류 및 SW 안전 공통기준 활용방법	88

요 약 문

1. 제 목 : SW 안전 분야 선정기준 및 SW 안전 공통기준 도출 연구

2. 연구의 추진 배경 및 목적

(1) 추진 배경

- SW가 중심이 되는 제4차 산업혁명 시대가 도래함
 - 첨단 정보통신기술, 특히 SW 중심의 기술이 경제·사회 전반에 융합되면서 혁신적인 변화(例, SW가 핵심인 자율주행차, 스마트 빌딩, 무인항공기 등의 등장)가 일어나고 있음
 - 이러한 혁신적인 변화를 제4차 산업혁명의 시대로 규정하고 있음
- 이처럼 많은 곳에서 SW가 사용됨에 따라 SW의 안전이 더욱 중요시되고 있으나 이와 관련된 안전 기준 연구는 미흡함
 - SW 오류로 인한 사고로부터 국민을 보호하고 안전을 강화하기 위해 SW 안전에 대한 충분한 연구가 필요함
 - 그간의 연구는 철도, 항공, 자동차 분야 등 특정 영역에 한정하여 HW 중심의 시스템 수준 안전을 고려하는 데 집중함
 - 그러나 SW 중심의 안전 등급을 분류하고 이에 대한 SW 안전 기준을 제시하는 연구는 부족하였음
- 이에 국민의 안전을 도모하고 생명을 보호하기 위해 SW 안전 분류 및 SW 안전 공통기준 도출의 필요성이 증대됨
 - 지금까지 철도, 항공, 자동차 등 안전-중요(safety-critical) 분야를 중심으로 시스템 안전의 한 부분으로 SW 안전이 일부 연구되었음
 - 이제는 제4차 산업혁명을 통해 부상하는 자율주행차, 드론과 같은 새로운

분야를 대상으로 [연구 1] SW 중심의 안전 분류 기준과 [연구 2] 분류에 따른 적절한 수준의 안전을 고려하여 SW를 개발할 수 있는 기준을 도출하는 연구가 필요함

(2) 연구 목적

- SW 안전이 필요한 분야에 대해
 - 안전 수준을 구분할 수 있는 선정기준을 마련함
 - 안전 수준별 SW 안전성을 향상 시킬 수 있는 기법 및 활동을 제시함
 - 궁극적으로 전부 개정 중인 소프트웨어산업진흥법의 제29조 소프트웨어 안전 확보를 위한 지침의 기초자료로 활용하고자 함

제29조(소프트웨어안전 확보) ① 정부는 소프트웨어안전 확보를 위한 시책을 마련할 수 있다.

② 과학기술정보통신부장관은 다음 각 호의 사항을 포함하는 소프트웨어안전 확보를 위한 지침을 정하여 고시할 수 있다.

1. 소프트웨어안전 관련 위험 분석
2. 소프트웨어안전 확보를 위한 설계 및 구현 방법
3. 소프트웨어안전 검증 방법
4. 운영 단계의 소프트웨어안전 확보 방안
5. 그 밖에 소프트웨어안전 확보에 필요하다고 인정되는 사항

③ 중앙행정기관의 장은 소관 분야의 기술기준을 수립하는 경우 제2항에 따른 지침 또는 국제표준 등을 고려하여야 한다.

3. 연구의 구성 및 방법

(1) 연구의 구성

- 본 연구의 구성은 총 4장으로 구성됨
 - 제1장은 서론으로 연구의 배경, 필요성, 목적 등을 기술함

- 제2장은 SW 안전 분류를 도출함 [연구 1]
- 제3장은 2장에서 도출된 SW 안전 분류에 따라 SW 안전성을 향상시킬 수 있는 SW 안전 공통기준을 제시함 [연구 2]
- 제4장은 결론으로 지금까지 내용을 정리하고 추후 연구에 대해 논함

(2) 연구의 방법

- 안전과 직결된 철도, 항공, 자동차 등의 기존 분야의 안전 관련 연구, 국제 표준 등을 종합적으로 분석하여 [연구 1] SW 안전 분류 및 [연구 2] SW 안전 공통기준을 도출하는 연구를 수행함
- 도출된 SW 안전 분류를 학계 · 산업계 · 연구소 등의 SW 안전 전문가들의 검토 및 검증을 받고 유효성을 확보함
 - 적절성 및 유효성을 평가하기 위하여 국내 SW 안전 전문가 자문단을 구성 · 운영하여 연구의 품질을 보증함
- 전문가 자문단의 검토를 바탕으로 보완된 SW 안전 분류를 기존 및 신규 분야의 특정 SW에 적용하여 SW 안전 분류의 정당성을 검증함

4. 연구 내용 및 결과

[연구 1] SW 안전 분류 도출 연구

(1) 분야 중심의 안전 분류 연구 분석

- 연구 범위 선정
 - SW 안전 분류를 도출하기 위해 다양한 분야에서 활용되는 안전 분류를 비교 · 분석할 수 있도록 산업 일반, 철도, 항공, 자동차, 의료기기 분야를 연구 범위로 선정함

- 아래 표와 같이 영역별 대표적인 국제 안전 표준을 분석하여 분류 방법의 특징을 뽑아냄

분야	국제 표준	설 명	분류 방법
산업 일반	IEC 61508	시스템 수준에서 8개의 안전무결성수준(SIL*)(저 요구 동작 모드 4개 수준, 고 요구/연속 동작 모드 4단계)으로 안전 분류를 제시	위험 심각도와 발생 확률을 사용
철도	IEC 62279	시스템 수준에서 4단계의 안전무결성수준(SIL)으로 안전 분류를 제시	위험 심각도와 발생 확률을 사용
항공	DO-178C	5단계의 Software Level로 안전 분류를 제시	위험 심각도만 사용
자동차	ISO 26262	시스템 수준에서 5단계의 자동차안전무결성수준(ASIL*)으로 안전 분류를 제시	위험 심각도, 발생 확률, 제어도를 사용
의료 기기	IEC 62304	SW 수준에서 3단계의 클래스(Class)로 안전 분류를 제시	위험 심각도만 사용

* Safety Integrity Level의 약자로 전기·전자기기의 안전무결성수준을 나타냄

** Automotive Safety Integrity Level의 약자로 자동차 분야에서 사용되는 SIL을 말함

○ 연구 결과 정리 및 고찰

- 산업 일반, 철도, 자동차, 의료기기 영역의 대표적인 안전 국제 표준들은 SW 수준이 아닌 시스템 수준의 안전 분류를 제시하고 있음
- 이를 일반화하여 비교 분석하기에는 필요한 정보가 제공되지 않아 연구가 제한적임
- 제한적인 분야 중심의 안전 분류 비교 분석 연구 접근 방법에서 SW 중심의 안전 분류 연구 비교 분석 방법으로 연구 접근 방법 변경 수행함

(2) SW 중심 안전 분류 연구 분석

○ 연구 대상 선정

- SW 중심의 안전 분류를 제시하고 있는 MIL-STD-882E와 NASA Software Safety Guidebook을 SW 안전 분류 도출 연구 대상으로 선정함 (각각에 대한 설명은 아래 표 참조)

구 분	설 명
MIL-STD-882E	- 미 국방부 산하의 모든 군사부서 및 국방기관에서 사용이 승인된 시스템 안전 표준 - 해당 시스템 안전 표준에는 군사용으로 개발/사용되는 SW에 대해 안전 분류 기준이 존재 - 산업 일반, 철도, 자동차 영역의 연구와 다르게 <u>SW 중심의 안전 분류를 수행할 수 있도록 위험 심각도와 SW 통제 등급을 이용하는 매트릭스를 제공</u>
NASA Software Safety Guidebook	- 미 항공우주국에서 안전을 고려하여 SW를 개발할 수 있도록 고안된 표준 - 해당 표준에서는 일반적인 SW 개발이나 안전을 중점적으로 고려해야 하는 SW를 대상으로 모두 적용할 수 있는 SW 안전 분류를 제시 - MIL-STD-882E와 유사하게 <u>SW 중심의 안전 분류를 수행할 수 있도록 위험 심각도와 SW 통제 등급을 이용하는 매트릭스를 제공</u>

○ MIL-STD-882E 기반의 SW 안전 분류 참조 모델 제시

- SW 특성상 SW를 통한 위험 발생 확률을 도출하거나 예측하는 것은 매우 제한됨
- 최악의 경우를 고려하여 SW 안전 분류를 수행해야 함 (즉, 기본적으로 위험 심각도 기반으로 안전 분류를 수행함)
- MIL-STD-882E의 경우, SW 기능 실패율을 도출하기에 어렵다는 특성을 고려하여 SW 통제 등급을 사용하여 안전 분류를 수행하는 특징을 가짐
- MIL-STD-882E에서 제공하고 있는 SW 중심의 안전 분류 모델이 본 연구를 통해 도출해야 하는 모델에 가장 부합한다고 판단하여 SW 안전 분류 모델로 참조함
- MIL-STD-882E 기반의 SW 안전 분류 모델은 4개의 위험 심각도 수준과 5개의 SW 통제 등급을 각 축으로 가지며, 이를 기반으로 총 5개 수준의 SW안전위험색인(SSRI, Software Safety Risk Index)을 결정함

○ SW 안전 분류 참조 모델 개선

- MIL-STD-882E 기반의 SW 안전 분류 참조 모델은 국방 분야를 중심으로 고려된 위험 심각도와 SW 통제 등급을 사용하고 있어, 다양한 도메인에서 SW 안전 분류가 활용될 수 있도록 개선함
- 위험 심각도는 유사한 개념이 활용되고 있는 의료기기, 항공 분야의 관련 연구를 조사 및 분석하여 4단계의 위험 심각도 수준을 5단계로 재정의함
- SW 통제 등급은 유사한 개념이 활용되고 있는 항공, 자동차 분야의 관련 연구를 참고하여 SW 통제 등급 수준을 최종 4단계로 재정의함

○ 전문가 자문단 검토 및 보완

- 학계, 산업계, 연구소 등의 국내 SW 안전 전문가로 자문단으로 구성하여 개선된 SW 안전 분류 모델을 검토함
- 전문가 자문단 검토를 통해 SW 안전 분류 모델의 적절성을 확인하였고 세부적으로 위험 심각도, SW 통제 등급, SW 안전 분류 모델 자체에 대해 검토 의견을 바탕으로 SW 안전 분류 모델을 보완함

(3) SW 안전 분류

○ SW 안전 분류 도출

- SW 안전 분류는 위험 심각도 및 SW 안전 통제 등급을 축으로 가지며 이를 기반으로 SW가 내포한 기능을 평가하여 아래와 같이 SW안전위험 색인(SSRI, Software Safety Risk Index)을 최종 결정함

위험 심각도 Severity SW 안전 통제 등급 SW safety control level	재앙적 Catastrophic	치명적 Critical	심각한 Serious	견딜만한 Tolerable	경미한 Negligible
완전자율 Full autonomy	SSRI 1	SSRI 1	SSRI 3	SSRI 4	SSRI 5
반(半)자율 Semi autonomy	SSRI 1	SSRI 2	SSRI 3	SSRI 4	SSRI 5
지원 Aid	SSRI 2	SSRI 2	SSRI 3	SSRI 4	SSRI 5
안전 제어 없음 No Safety Control	SSRI 5	SSRI 5	SSRI 5	SSRI 5	SSRI 5

SW안전위험색인	설 명
SSRI 1	△SW가 보유하고 있는 위험방지 제어 기능에 대해 반(半)자율 이상의 자율성을 가지고 재앙적(catastrophic) 수준의 위험을 제어하거나 △완전자율 수준의 자율성을 가지고 치명적(critical) 수준의 위험을 제어함
SSRI 2	△SW가 보유하고 있는 위험방지 제어 기능에 대해 지원 수준의 자율성을 가지고 재앙적(catastrophic) 수준의 위험을 제어하거나 △지원 및 반(半)자율 수준의 자율성을 가지고 치명적(critical) 수준의 위험을 제어함
SSRI 3	△SW가 보유하고 있는 위험방지 제어 기능에 대해 자율성 가지며 심각한(serious) 수준의 위험을 제어함
SSRI 4	△SW가 보유하고 있는 위험방지 제어 기능에 대해 자율성 가지며 견딜만한(tolerable) 수준의 위험을 제어함
SSRI 5	△SW가 위험방지 제어 기능을 보유하지 않거나 △경미한(negligible) 수준의 위험을 제어함

○ SW 안전 분류 정당성 검증

- SW 안전 분류를 기존 및 신규 SW 안전 분야를 대상으로 특정 시스템의 SW 기능에 적용하여 유효성과 정당성을 검증함
- 기존 SW 안전 분야의 경우, 자동차 영역에서 사용되는 자동긴급제동(AEB, Autonomous Emergency Braking) 시스템을 대상으로 SW 안전 분류를 적용하여 기존의 자동차 영역에서 부여받은 안전 분류 결과와 비교 분석을 수행하여 유효성 및 정당성을 확인함

- 신규 SW 안전 분야의 경우, 기존의 SW 수준에서 안전을 고려하지 않았던 지하철 슬라이딩 도어와 지하철 개폐 장치의 통합 시스템을 대상으로 SW 안전 분류를 적용해 보았으며, 도출된 SW안전위험색인(SSRI)이 적절한 수준임을 확인함

[연구 2] SW 안전 공통기준 도출 연구

(1) SW 안전 공통기준 관련 연구 분석

○ MIL-STD-882E 가이드라인 분석

- SW 안전 분류 도출을 위해 참조한 MIL-STD-882E를 실질적으로 활용하기 위한 가이드라인이 존재하며, 해당 가이드라인에 안전 분류 수준에 따라 SW 설계, 구현, 단위 검증, 통합 단위 검증, 시스템 통합 검증 단계별로 적용할 수 있는 안전 활동 및 기법이 제시되고 있음
- 특이사항으로 SW 개발 단계 중, SW 요구사항 명세 단계에 대한 활동 및 기법이 별도로 제공되지 않음

○ NASA Software Safety Guidebook 분석

- NASA Software Safety Guidebook에서 SW 안전 분류 수준에 따라 SW 요구사항, 설계, 구현, 검증 단계별로 적용할 수 있는 안전 활동 및 기법이 제시되고 있음
- 특이사항으로 SW의 검증이 IEC 12207과 같이 일반적으로 많이 사용하는 SW 단위 검증, SW 통합 검증, SW 검증 단계를 하나의 단계로 묶어 활동과 기법을 소개함

○ SW 안전 공통기준 도출

- MIL-STD-882E와 NASA Software Safety Guidebook에서 사용되는 활동

과 기법을 병합 및 조정 후 SW 개발 시 요구사항, 설계, 구현, 단계별 검증 단계를 모두 고려함

- 5개의 SW안전위험색인(SSRI)에 따라 아래 그림과 같이 적용 가능한 안전 활동을 정리하고 자동차 분야에서 활용되고 있는 기법들을 선정하여 적용 기법으로 정리함

단계	안전 활동	SSRI1		SSRI2		기타	SSRI5	
		필수 유무	적용 기법	필수 유무	적용 기법		필수 유무	적용 기법
Requirements	Development of software safety requirements	○	• Structured natural language	○	• Structured natural language	○	X	N/A
	Safety analysis of safety requirements	○	• Software Fault Tree analysis • Software Failure mode and effects analysis	○	• Software Fault Tree analysis • Software Failure mode and effects analysis	○	X	N/A
	Review of safety requirements	○	• Inspection	○	• Inspection	○	X	N/A
Design	Development of software safety design	○	• Hierarchical structure of software components	○	• Hierarchical structure of software components	○	X	N/A
	Safety analysis of design	○	• Software Fault Tree analysis • Software Failure mode and effects analysis	○	• Software Fault Tree analysis • Software Failure mode and effects analysis	○	X	N/A
	Review of safety design	○	• Inspection	○	• Inspection	○	X	N/A
Implementation	Safety analysis of code	○	• Safety code analysis	X	N/A	○	X	N/A
	Review of safety code	○	• Inspection	X	N/A	○	X	N/A
Software	Development of safety related unit test case	○	• Analysis of safety requirements • Generation and analysis of equivalence classes • Analysis of boundary values	○	• Analysis of safety requirements • Generation and analysis of equivalence classes • Analysis of boundary values	○	X	N/A
	Review of safety related unit test case	○	• Inspection	○	• Inspection	○	X	N/A
	Analysis of test coverage at software unit	○	• Statement coverage	○	• Statement coverage	○	X	N/A
...								
Integration test	Analysis of test coverage at software architectural level	○	• Function coverage • Call coverage	○	• Function coverage • Call coverage	○	X	N/A
	Safety related software integration test	○	• Requirements based test • Fault injection test	○	• Requirements based test • Fault injection test	○	X	N/A
	Review of safety related software integration test result	○	• Inspection	○	• Inspection	○	X	N/A
Software test	Development of safety related software test case	○	• Analysis of safety requirements • Generation and analysis of equivalence classes • Analysis of boundary values	○	• Analysis of safety requirements • Generation and analysis of equivalence classes • Analysis of boundary values	○	X	N/A
	Review of safety related software test case	○	• Inspection	○	• Inspection	○	X	N/A
	Safety related Software test	○	• Requirements based test • Fault injection test	○	• Requirements based test • Fault injection test	○	X	N/A
	Review of safety related software test result	○	• Inspection	○	• Inspection	○	X	N/A

- SW 안전 공통기준에 포함된 활동 및 기법은 IEC 12207과 같이 SW 개발 과정의 일반적인 활동과 기법이 사용되는 것을 가정하고 있으며, 일반적인 활동 위에 SW 안전에 관련된 활동 및 기법을 추가 수행하면 됨

5. 기대 효과

- 제4차 산업혁명의 도래로 기존의 SW 안전 영역뿐 아니라 융·복합을 통해 새롭게 발굴되는 산업 영역에서 SW 안전을 고려할 수 있도록 SW 안전 분류를 제시하고 분류된 안전등급에 따라 적절한 SW 안전 공통기준을 적용하여 국민의 안전을 도모할 수 있는 SW 개발 산업에 기반을 마련함
- SW 기술이 융합됨에 따라 국민의 신체나 생명에 위해를 발생시킬 가능성이 있는 모든 분야에서 국민 안전 강화를 위한 기술적 방향을 제시하며 소프트웨어산업진흥법 전부 개정안의 제29조 소프트웨어안전 확보를 위한 지침인 SW 일반안전기준 구현에 대한 기초자료로 활용 가능함

Summary

This study deals with the process of developing SW safety classification and SW safety common criteria so that software safety can be taken into account not only in existing software safety considerations but also in the newly created industrial sector following the advent of the 4th Industrial Revolution.

In order to derive the SW safety classification, related studies in various fields where safety is important were analyzed and the safety classification based on software was also analyzed. Although an industrial based safety classification study approach was applied to derive SW safety classification, the research was carried out using a software based safety classification study approach, considering that it was not suitable to derive SW safety classification.

SW safety classification model was defined first before SW safety classification was derived and utilized as reference to MIL-STD-882E. After selecting the SW safety classification model, the SW safety classification draft was completed by improving the SW safety classification model by analyzing relevant research in space, aviation, medical equipment and automotive fields so that SW safety classification can be utilized in various fields. The SW safety classification draft was reviewed by an expert advisory group to confirm the adequacy and appropriateness of the SW safety classification draft, and was supplemented with the draft SW safety classification to derive the SW safety classification.

SW safety classification can be performed using a total of 5 risk severity

and a total of 4 software safety control level and defined to take account of all new industrial sectors derived from the 4th Industrial Revolution.

To justify the derived SW safety classification, verification was carried out on systems used in the existing software safety sector and systems in the new software safety sector, and SW safety classification was verified as appropriate.

Based on the software safety risk index determined through SW safety classification, SW safety common criteria was derived and studied to perform appropriate levels of safety activities and techniques. For safety activities, the U.S. national defense standards and NASA's Guide were analyzed and the applicable techniques for safety activities were derived by analyzing the standards of the automobile domain.

The SW safety common criteria comprises a total of 22 safety activities and 17 techniques, and the recommended safety activities and techniques are defined by differences in the software safety risk index. The applicable techniques for each safety activity and safety activity are defined for the desired utilization of the SW safety common criteria.

In this study, the SW safety classification and SW safety common criteria were derived from the advent of the 4th Industrial Revolution, and the basic data were prepared to present SW general safety criteria based on them.

CONTENTS

Chapter 1. Introduction	1
Chapter 2. Derivation of SW Safety Classification	7
Chapter 3. Derivation of SW Safety Common Criteria	66
Chapter 4. Conclusion	89

제1장 서론

제1절 연구의 배경 및 목적

1. 연구의 배경

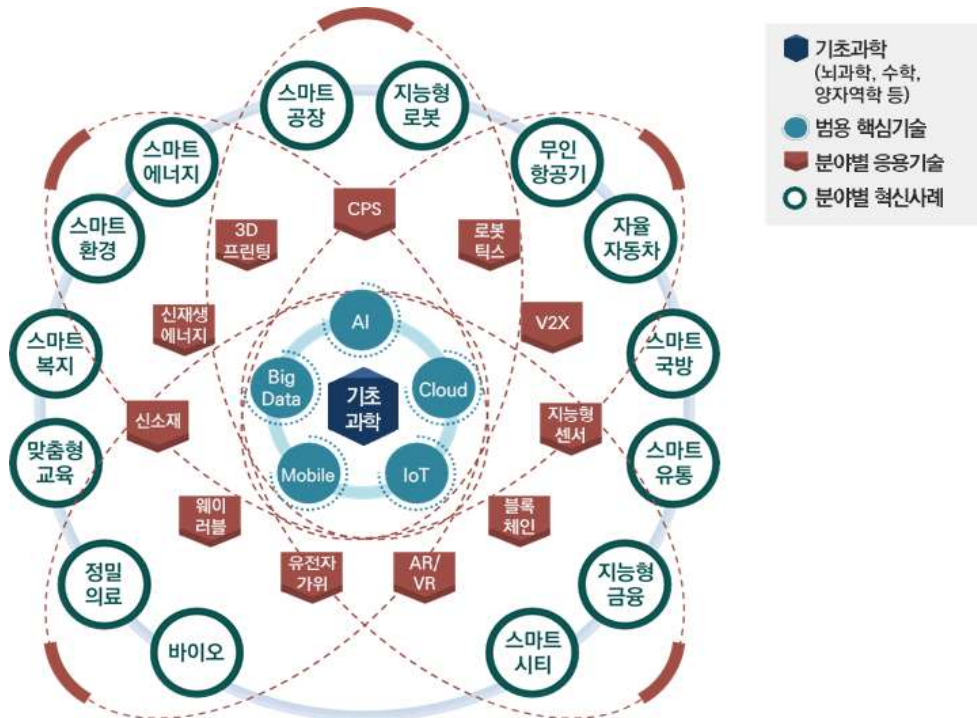
약 20년 전 딥블루(Deep Blue)¹⁾는 인간 체스 챔피언과 대결하여 인간을 최초로 이겼다. 이후 2016년에는 체스보다 훨씬 복잡한 바둑에서 알파고²⁾가 인간을 이겼다. 이처럼 인공지능 기술이 비약적으로 발전하고 있다. 이를 바탕으로 지능화된 로봇이 공장에서 일하고 자율주행차가 도로를 달리고 있다. 새로운 기술의 등장과 발전은 우리 사회를 급격히 변화시키고 있다. 즉, 이러한 변화를 제4차 산업혁명이라 규정하고 있으며, 경제·사회뿐만 아니라 일상의 삶 등 모든 분야에서 새로운 가치를 창출하고 있다.

제4차 산업혁명은 超연결과 超지능의 특징을 갖는다. 이로 인해 [그림 1-1]과 같이 기존에 없었던 스마트 공장, 무인항공기, 자율주행차 등과 같은 융·복합된 새로운 산업이 만들어지고 있다. 이는 인간에게 더욱 편안하고 효율적인 삶을 제공한다. 단, 이러한 이점을 얻기 위해서는 ‘안전’이 반드시 선행되어야 한다. 지능화된 시스템이 제어권을 가지고 있는 상황에서 탑재된 SW가 오작동하게 되면 사람의 생명이나 신체에 위해(危害)를 가할 수 있다. 자동차, 항공, 원자력 등 안전이 중요한(safety critical) 분야는 예전부터 업계 및 학계 전문가가 모여 안전 확보를 위한 연구 및 표준 제정 등의 활동이 활발하다. 반면, 융·복합으로 파생된 신규 산업에 대한 안전 연구는 상대적으로 미비한 실정이다.

1) IBM과 과학자들이 8년여에 걸쳐 개발한 높이 2m, 무게 1.4t의 슈퍼컴퓨터

2) 구글 딥마인드가 개발한 인공지능 바둑 프로그램

[그림 1-1] 제4차 산업혁명 관련 과학·기술과 산업 간 연계도



출처 : 4차 산업혁명 대응을 위한 기본 정책방향, 4차산업혁명위원회, 2017.10.

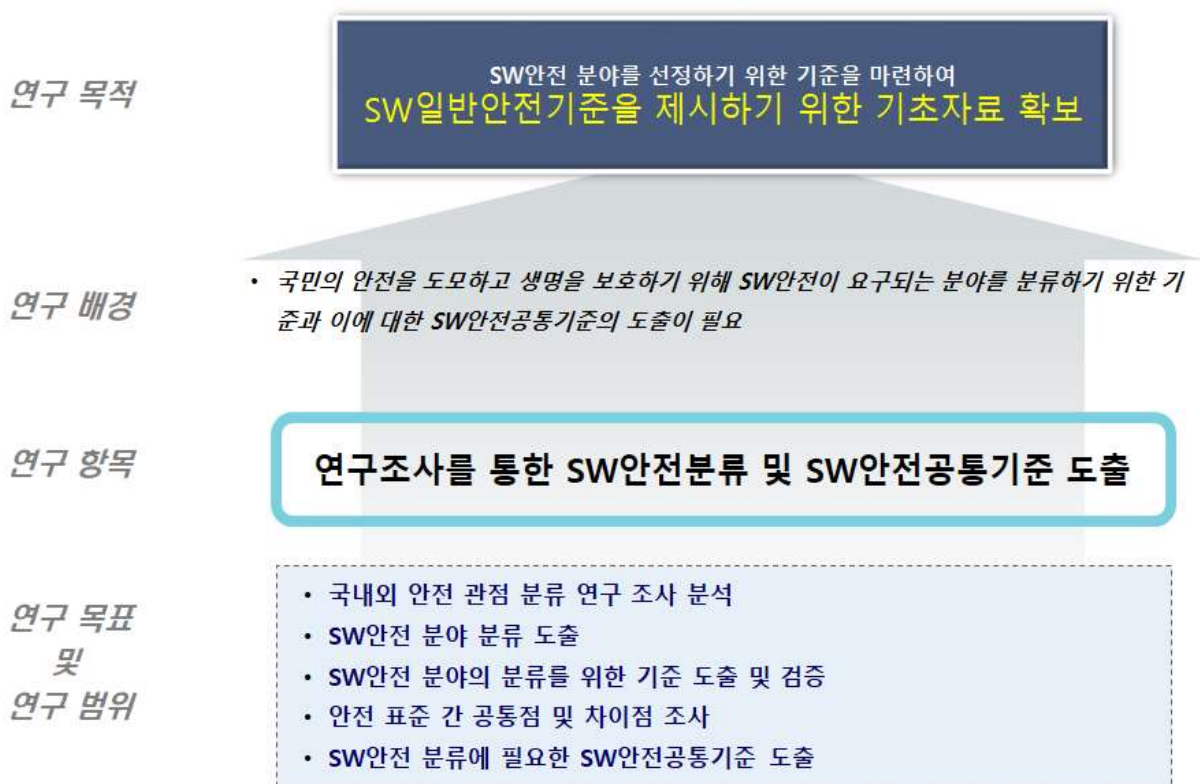
융·복합되는 산업들은 SW가 차지하는 비중이 증대되고 이전보다 많은 기능이 SW로 동작하고 있다. 이러한 SW는 더욱 복잡해질 것이다. 제4차 산업혁명은 우리의 삶을 더욱더 풍요롭고 효율적으로 만들지만, 얻는 이점만큼 국민의 안전에 위해(危害)가 될 수 있는 요인이 증가할 수 있다. 결국 SW의 안전이 그 어느 때보다도 중요하다. 이에 국민의 안전을 도모할 수 있는 SW 중심의 안전 분류를 수행할 수 있는 기준이 필요하다. 안전 기준에 따라 적절한 수준으로 안전을 고려하여 SW를 개발할 수 있도록 필수 활동 및 기법에 대한 기준을 제시하는 연구 역시 필요하다.

2. 연구의 목적

[그림 1-2]와 같이 제4차 산업혁명을 통해 파생되는 신규 산업 분야를 포함하여 SW 안전이 필요한 분야에 대해 안전 수준을 구분할 수 있는 기준을 마련

하고자 한다. 이를 통해 새롭게 개발하고자 하는 SW가 어느 정도의 안전 위험을 내포하고 있는지 인지한다. 이후 분류된 기준에 맞추어 SW로부터 야기될 수 있는 안전 위험을 감하(減下) 시킬 수 있는 공통적인 기법 및 활동을 제시한다. 궁극적으로 전부 개정 중인 소프트웨어산업진흥법의 제29조 소프트웨어 안전 확보를 위한 지침의 기초자료로 활용하고자 한다.

[그림 1-2] 연구 개요



<표 1-1> 소프트웨어산업진흥법 전부 개정안에 포함된 SW 안전 관련 조문 일부

제29조(소프트웨어안전 확보) ① 정부는 소프트웨어안전 확보를 위한 시책을 마련할 수 있다. ② 과학기술정보통신부장관은 다음 각 호의 사항을 포함하는 <u>소프트웨어안전 확보를 위한 지침을 정하여 고시</u>할 수 있다. 1. 소프트웨어안전 관련 위험 분석 2. 소프트웨어안전 확보를 위한 설계 및 구현 방법 3. 소프트웨어안전 검증 방법
--

- 4. 운영 단계의 소프트웨어안전 확보 방안
- 5. 그 밖에 소프트웨어안전 확보에 필요하다고 인정되는 사항
- ③ 중앙행정기관의 장은 소관 분야의 기술기준을 수립하는 경우 제2항에 따른 지침 또는 국제표준 등을 고려하여야 한다.

제2절 연구의 구성 및 방법

1. 연구의 구성

본 연구의 구성은 총 4장으로 구성된다.

제1장은 서론으로 연구의 배경, 필요성, 목적 등을 기술한다.

제2장은 SW 안전 분류를 도출하기 위해 연구 접근 방법 및 도출 과정을 기술한다. 도출된 SW 안전 분류를 전문가 자문단의 검토를 통해 개선하는 내용을 담는다. 이후 기존·신규 SW 안전 분야의 예제 시스템을 대상으로 정당성 검증 수행한 내용을 요약한다.

제3장은 2장에서 도출한 SW 안전 분류 수준에 따라 SW 안전 분류를 도출하는 과정에서 참조한 가이드라인을 활용하여 SW의 안전 위험을 감하(減下)시킬 수 있는 안전 중심의 활동 및 기법을 정리한 SW 안전 공통기준을 제시한다.

제4장에서는 지금까지 기술된 내용을 종합적으로 정리한다.

2. 연구의 방법

제4차 산업혁명의 변화에 대응하여 SW 안전을 고려할 수 있도록 직·간접적으로 연관된 산업 일반, 철도, 항공, 자동차, 의료기기 영역에서 활용되는 안전 표준을 종합적으로 비교 분석하여 SW 중심의 안전 분류 및 SW 안전 공통기준

을 도출한다.

학계(4명)·산업계(1명)·연구기관(3명)에서 SW 안전 관련하여 활동하는 전문가를 자문단으로 구성하여 도출된 SW 안전 분류를 검토하여 연구의 방향성, 품질, 적절성을 확인한다.

[그림 1-3] SW 안전 분류 정당성 검증 대상 시스템

기존 SW 안전분야
자동긴급제동장치



신규 SW 안전분야
스크린 도어+지하철 개폐 장치



전문가 자문단의 검토의견을 반영하여 완성된 SW 안전 분류의 정당성 및 유효성을 검증한다. 이를 위해 [그림 1-3]과 같이 기존 SW 안전분야와 신규 SW 안전분야를 대상으로 시스템을 선정하고 SW 안전 분류를 적용하여 도출되는 결과를 확인한다.

기존 SW 안전분야의 시스템은 자율주행차에 포함되는 여러 서브시스템 중 하나인 자동긴급제동장치(AEB³⁾) 시스템의 SW 기능이며 해당 시스템을 대상으로 자동차 분야에서 안전 분류를 결정하는 방식 중 하나인 위험 분석 및 위험 평가(HARA⁴⁾) 수행 결과와 SW 안전 분류 적용 결과의 차이를 비교 분석한다.

3) Autonomous Emergency Braking

4) Hazard Analysis and Risk Assessment

신규 SW 안전분야의 경우, 기존에 SW 수준에서 안전을 고려하지 않았던 지하철 슬라이딩 도어와 지하철 개폐 장치가 통합된 신규 SW 안전 시스템의 SW 기능을 대상으로 SW 안전 분류를 적용하여 결과 도출 후 분석한다.

제2장 SW 안전 분류 도출 연구

본 장에서는 SW 안전 분류를 도출하기 위해 연구 접근 방법 및 도출 과정을 기술한다. 도출된 SW 안전 분류를 전문가 자문단의 검토를 통해 개선된 결과를 설명한다.

제1절 분야 중심 안전 분류 연구 분석

SW 안전 분류를 도출하기 위해 다양한 분야의 안전 분류를 비교·분석할 수 있도록 산업 일반, 철도, 항공, 자동차, 의료기기 분야를 연구 범위로 선정하여 분야별 안전 표준을 비교 연구 조사한다.

1. 산업 일반 분야의 안전 표준

산업 일반 분야에서 안전 분류를 다루고 있는 IEC 61508을 기준으로 연구 조사를 수행했다. IEC 61508은 일반적인 산업 분야에서 전기/전자/프로그래밍 가능한 전자 장치의 기능 안전성을 고려할 수 있도록 제정된 국제 표준이다.

IEC 61508은 안전 수준을 고려하여 전기/전자/프로그래밍 가능한 전자 장치를 개발 및 관리할 수 있도록 ‘안전무결성수준(SIL)⁵⁾’이라는 분류 체계를 가진다. 안전무결성수준은 전기/전자/프로그래밍 가능한 전자 장치가 주어진 시간 내에 요구되는 안전 기능을 만족스럽게 수행할 수 있는 확률을 의미한다.⁶⁾

<표 2-1>과 같이 안전무결성수준은 총 4개의 수준으로 구분된다. 해당 안전 장치가 사용되는 요율을 고려하여 저(低) 요구 작동 모드 및 고(高) 요구·연속

5) Safety Integrity Level

6) IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems

작동 모드로 구분하여 같은 명칭의 안전무결성수준을 사용하는 특징이 있다. IEC 61508에서 사용하고 있는 저(低) 요구 작동 모드로, 안전 관련 시스템상에서 기능 작동 요구 빈도가 연간 1회 미만인 경우를 의미하며 에어백 시스템이 해당 예시가 될 수 있다. 고(高) 요구·연속 작동 모드는 안전 관련 시스템상에서 기능 작동 요구 빈도가 연간 1회 이상인 경우로 브레이크 시스템이 하나의 예가 될 수 있다.

〈표 2-1〉 안전무결성수준 별 안전기능 고장 기준

안전무결성 수준(SIL)	저(低) 요구 작동모드에서 운영되는 안전기능 고장 기준	고(高) 요구 및 연속 작동모드에서 운영되는 안전기능 고장 기준
4	$\geq 10^{-5}$ 에서 $<10^{-4}$	$\geq 10^{-9}$ 에서 $<10^{-8}$
3	$\geq 10^{-4}$ 에서 $<10^{-3}$	$\geq 10^{-8}$ 에서 $<10^{-7}$
2	$\geq 10^{-3}$ 에서 $<10^{-2}$	$\geq 10^{-7}$ 에서 $<10^{-6}$
1	$\geq 10^{-2}$ 에서 $<10^{-1}$	$\geq 10^{-6}$ 에서 $<10^{-5}$

안전 무결성 수준은 고장률을 기준으로 명확히 구분하는데 고장률을 산술적으로 도출하기 위해서는 긴 시간 동안 고장 발생 횟수를 기록하여 누적된 데이터를 기반으로 산출한다. 결국 고장률을 확보하는 것 자체가 쉽지 않아 고장률 기반으로 안전무결성수준을 결정하기는 어렵다.

이를 위해 〈표 2-2〉와 같이 안전 시스템이 갖는 4개의 위험 파라미터를 기반으로 안전무결성수준을 결정할 방법을 제시한다. 〈표 2-2〉의 4개의 리스크 파라미터는 위험의 피해 결과 정도(C) → 위험 발생 가능한 상황에 노출된 정도(F) → 위험 회피 허용 정도(P) → 위험의 발생 정도(W) 순서로 각각 파라미터 값을 정하고 [그림 2-1]과 같이 위험 그래프를 활용하여 안전무결성수준을 결정한다.

예를 들어, 특정 위험을 통해 발생한 피해가 중상의 피해(C_B)를 일으키고 위험에 노출되는 시간이 짧으며(F_B) 위험의 발생에 대해 피할 수 없는 상황(P_B)이고 1년에 1번 정도 위험이 발생하는 상황(W_2)이라면 그림 2-1의 그래프를 이용하여 SIL 2가 결정된다. 예시와 같은 방식으로 위험이 가지고 있는 특성에 따라 SIL 1에서 SIL 4 사이의 값을 결정한다. 대상 안전 시스템의 안전무결성수준의 결정 후, 결정된 안전무결성수준에 따라 적합한 활동 및 기법을 적용하여 안전성을 고려할 수 있게 된다.

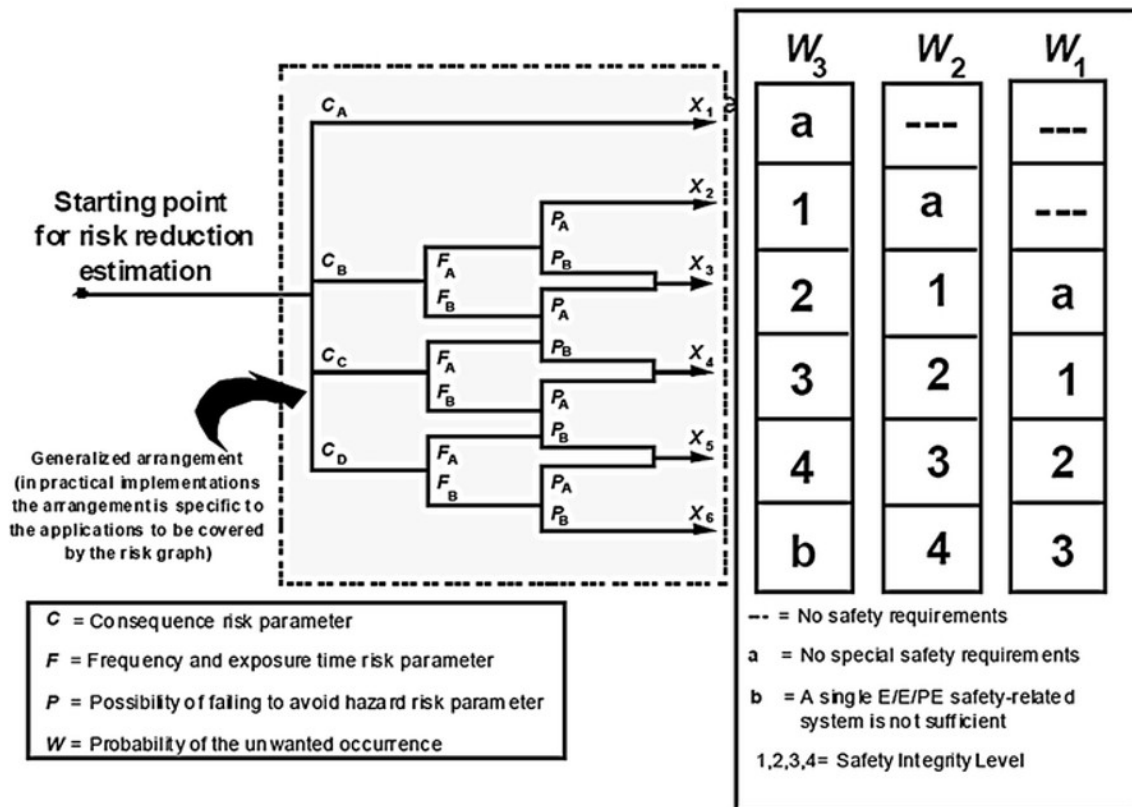
<표 2-2> 위험 파라미터 분류

위험 파라미터	등급 분류	
Consequence risk parameter(C)	C_A	경상
	C_B	다수의 중상 또는 사망 1명
	C_C	사망 2인 이상
	C_D	다수 사망
Frequency and exposure time risk parameter(F)	F_A	매우 희박함
	F_B	빈번함
Possibility of failing to avoid hazard risk parameter(P)	P_A	회피 가능
	P_B	회피 불가능
Probability of the unwanted occurrence(W)	W_1	낮음(연간 0.1건 미만)
	W_2	중간(연간 0.1건 이상 1건 이하)
	W_3	높음(연간 1건 초과 10건 이하)

이처럼 IEC 61508에서는 산업 일반 분야에서 사용되는 다수의 전기/전자/프로그래밍 가능한 전자장치 시스템을 대상으로 안전 분류를 수행할 수 있도록 방법을 제시하고 있다. 해당 안전 분류 방법은 시스템 수준에서 발생할 수 있는 위험을 대상으로 위험의 심각도와 위험의 발생 확률로 안전 분류를 수행하도록 구성되어 있다. 해당 방식을 SW 측면으로 활용 시 SW 수준에서 위험 발생 확률을 예측 및 측정하는 것이 매우 어렵고 설사 측정되더라도 시스템 수준에서

요구되는 안전 분류 등급별 요구되는 허용 고장률과 SW 기능 고장률의 관계를 결정짓기가 어렵기 때문에⁷⁾ SW 안전 분류로 활용하기에는 어려움이 존재한다.

[그림 2-1] 위험 그래프 적용 방법



출처 : IEC 61508, Part 5 Examples of methods for the determination of safety integrity levels

2. 철도 분야의 안전 표준

철도 분야에서 안전 분류를 다루고 있는 IEC 62279를 기준으로 연구 조사를 수행했다. IEC 62279는 철도 분야에서 사용하는 SW를 대상으로 기능 안전성을 고려할 수 있도록 제정된 국제 표준이다.

7) PG Bishop, "SILs and Software", Adelard and Centre for Software Reliability, City University London, 2005.01

IEC 62279는 안전을 위해 철도용 SW 개발 및 관리할 수 있도록 ‘안전무결성수준(SIL)’이라는 분류 체계를 가진다. 안전무결성수준(SIL)은 해당 SW가 주어진 시간 내에 요구되는 기능을 수행하면서 감내할 수 있는 위험 발생 확률을 의미한다.

<표 2-3>과 같이 안전무결성수준은 총 허용 위험요인 발생 빈도(THR)⁸⁾의 범위에 따라 4개의 수준으로 구분된다. [그림 2-2]와 같이 개발해야 하는 시스템을 대상으로 위험원 분석(Hazard Analysis)을 수행하여 발생할 수 있는 위험과 위험별로 요구되는 허용 위험요인 발생 빈도를 식별한다. 이후 <표 2-3>과 같이 위험 별 식별된 허용 위험요인 발생빈도에 맞추어 안전무결성수준을 결정하고 서버 시스템에 상속시켜 서버 시스템 구성요소에 허용 위험요인 발생 빈도와 실패율(FR)⁹⁾을 할당하여 안전한 SW를 개발하도록 하는 방식을 갖는다.

<표 2-3> 안전무결성수준 별 견딜 수 있는 고장 확률

안전무결성수준 (SIL)	THR (Tolerable Hazard Rate per hour and function)
4	$10^{-9} \leq \text{THR} < 10^{-8}$
3	$10^{-8} \leq \text{THR} < 10^{-7}$
2	$10^{-7} \leq \text{THR} < 10^{-6}$
1	$10^{-6} \leq \text{THR} < 10^{-5}$

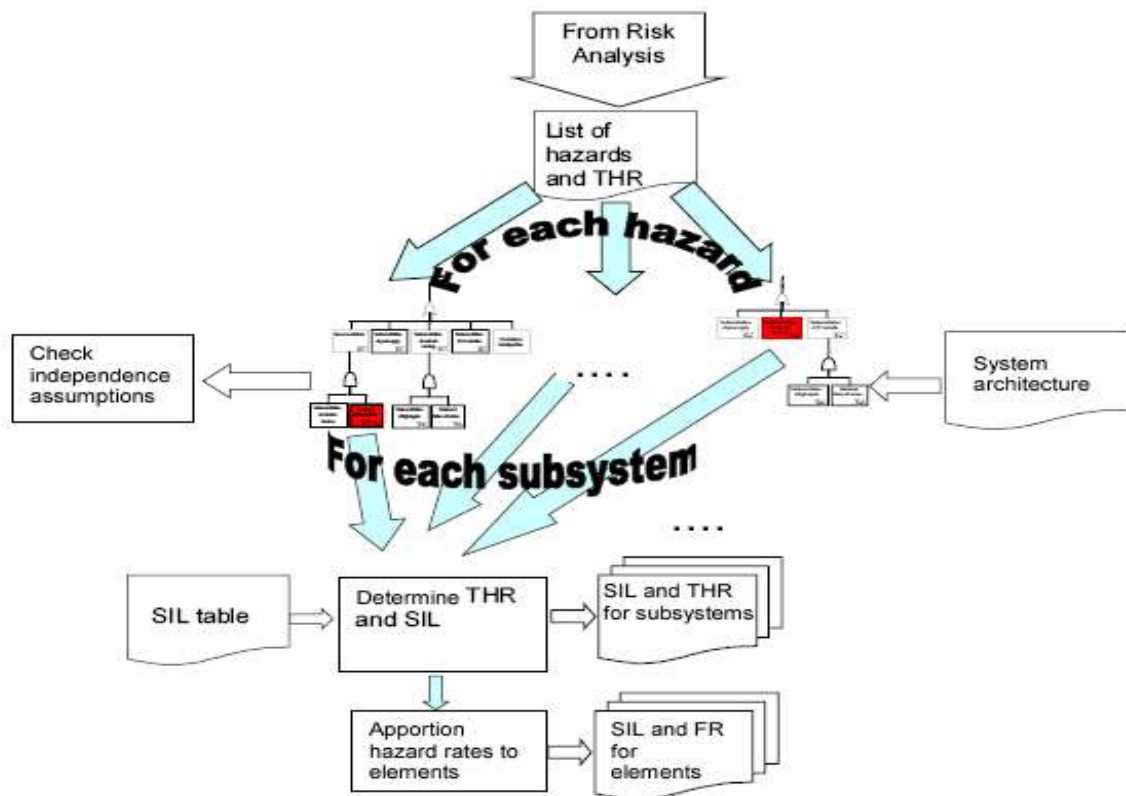
이처럼 IEC 62279에서는 철도 분야에서 사용되는 SW를 대상으로 안전 분류를 도출하는 방법에 대해서 다루고 있는데, 시스템 수준에서의 허용 위험요인 발생 빈도를 기반으로 SW가 안전 분류를 강제적으로 할당받는 방식으로 구성된다. IEC 62279는 SW를 대상으로 안전 분류 결과를 설명하고 있다. 그러나 안전 분류 도출은 시스템 수준에서 수행하여 결과를 상속받기 때문에 우리가 개발하

8) Tolerable hazard rate

9) Failure rate

고자 하는 SW 중심의 안전 분류 수행 방식으로 활용하기에는 분석 분류 대상 수준의 차이가 존재한다.

[그림 2-2] IEC 62279의 안전 시스템의 안전무결성수준 결정 방법



출처:EN50129, Railway applications. Communication, signalling and processing systems. Safety related electronic systems for signalling

3. 항공 분야의 안전 표준

항공 분야에서 안전 분류를 다루고 있는 DO-178C를 기준으로 연구 조사를 수행했다. DO-178C는 항공 분야에서 사용하는 SW를 대상으로 기능 안전성을 고려할 수 있도록 제정된 국제 표준이다.

DO-178C에서는 안전 수준 고려하여 항공용 SW를 개발 및 관리할 수 있도록

SW 레벨(Software level)이라는 분류 체계를 가진다. SW 레벨은 해당 SW가 위험 발생 시, 얼마만큼의 피해를 일으키는 상태인지를 판단하여 구분하고 있다.¹⁰⁾ DO-178C에서 제시하고 있는 실패 상태는 <표 2-4>와 같이 정의된다.

<표 2-4> DO-178C의 고장상태 정의

고장 상태 분류	설 명
Catastrophic	항공기 추락과 같은 고장으로 다수의 사망자 발생
Hazardous	승무원이 비행할 수 없게 되거나 소수의 승객에게 치명적인 부상 발생
Major	승무원이나 승객이 상당한 불편함을 느끼거나 일부 부상을 겪을 수 있음
Minor	승무원과 승객이 불편함을 느낌
No Safety Effect	안전에 영향을 미치지 않으며, 승무원의 업무에도 영향을 미치지 않음

DO-178C 내에서 고장상태 의미는 위험 심각도와 같다. DO-178C는 SW 기능의 실패 확률을 산정하거나 도출하기 어려운 점에 착안하여 확률적인 요소를 사용하지 않는다. DO-178C는 위험 심각도만을 고려하여 SW 안전 분류를 수행하는 특징이 존재한다.¹¹⁾

DO-178C는 <표 2-5>와 같이 SW 레벨은 총 5개의 수준으로 구분되며, 개발하고자 하는 항공용 SW의 기능을 대상으로 시스템 수준에서 할당받은 안전 분류를 상속받아 SW 레벨이 결정된다.

항공기 시스템 수준에서 수행하는 안전 분류는 DO-178C의 상위 표준 문서인 ARP 4754A¹²⁾를 통해 개발 보증 수준(DAL)¹³⁾이라는 명칭으로 안전 분류를

10) DO-178C, Software Considerations in Airborne Systems and Equipment Certification

11) SAFETY-CRITICAL SOFTWARE STANDARDS - SURVEY AND SUMMARY, ASSC, 1996

12) ARP 4754A(Guidelines for development of Civil Aircraft and Systems)는 항공기 시스템 개발을 위한 가이드라인으로, 항공기 시스템의 인증을 위한 Development Assurance level(DAL)의 개념을 설명하고 이를 고려한 개발 프로세스를 설명함

수행한다. ARP 4754A와 DO-178C의 관계를 고려하여 SW 레벨 별 허용되는 기능 실패율에 대해 관계를 정리하면 <표 2-6>과 같이 정의할 수 있다.

<표 2-5> DO-178C의 SW 레벨 정의

SW 레벨	설 명
Level A	SW가 시스템 기능을 실패 또는 실패를 유발하여 항공기의 Catastrophic 고장상태를 초래함
Level B	SW가 시스템 기능을 실패 또는 실패를 유발하여 항공기의 Hazardous 고장상태를 초래함
Level C	SW가 시스템 기능을 실패 또는 실패를 유발하여 항공기의 Major 고장상태를 초래함
Level D	SW가 시스템 기능을 실패 또는 실패를 유발하여 항공기의 Minor 고장상태를 초래함
Level E	SW가 시스템 기능을 실패 또는 실패를 유발하여 항공기의 No effect 고장상태를 초래함

<표 2-6> DO-178C의 SW 레벨 별 고장률 기준

SW 레벨	허용 고장률
Software level A	$<10^{-9}$
Software level B	$\geq 10^{-9}$ 에서 $<10^{-7}$
Software level C	$\geq 10^{-7}$ 에서 $<10^{-5}$
Software level D	해당 없음
Software level E	해당 없음

이처럼 DO-178C는 항공 분야에서 사용되는 SW를 대상으로 안전 분류 개념을 설명하고 있는데, 시스템에서 수행한 안전 분석을 통해 식별된 안전 분류 값을 SW로 상속하여 SW 레벨을 결정하는 특징을 갖는다. DO-178C에서는 SW를 대상으로 안전 분류 결과를 설명하고 있지만, 안전 분류 도출은 시스템 수준에

13) Development assurance level. 항공기 시스템 수준의 안전 분류이며 Software level과 동일하게 5개의 수준으로 구분하여 1:1 상속됨

서 수행하여 결과를 상속받는다. 따라서 우리가 도출하고자 하는 SW 중심의 안전 분류 수행 방식으로 활용하기에는 분석 분류 대상 수준의 차이가 존재한다.

4. 자동차 분야의 안전 표준

자동차 분야에서 안전 분류를 다루고 있는 ISO 26262를 기준으로 연구 조사를 수행했다. ISO 26262는 자동차 분야에서 사용하는 전기/전자/프로그래밍 가능한 전자 장치의 기능 안전성을 고려할 수 있도록 제정된 국제 표준이다.

ISO 26262에서는 안전 수준을 고려하여 차량용 시스템의 개발 및 관리를 위해 ‘자동차 안전무결성수준(ASIL)¹⁴⁾’이라는 분류 체계를 가진다. 자동차 안전무결성수준은 차량에 탑재되는 전기/전자/프로그래밍 가능한 전자 장치가 가지고 있는 위험이 사람에게 미칠 수 있는 영향을 분석하여 안전 분류를 수행한다.

자동차 안전무결성수준은 A ~ D, QM¹⁵⁾까지 총 5개 수준으로 구분하고 있으며 <표 2-7>과 같이 위험의 심각도, 발생 확률, 통제도 수준을 기반으로 <표 2-8>의 기준을 활용하여 자동차 안전무결성수준을 결정한다.¹⁶⁾ 예를 들어, 특정 차량 시스템의 기능 오작동을 통해 유발될 수 있는 피해가 가벼운 상해(S1)를 일으키며 주행 중에 일반적으로 일어나는 상황(E4)이고 사고 발생 시 운전자가 문제 상황을 간단하게 통제하여 회피할 수 있다면(C1) <표 2-8>에 의거하여 자동차 안전무결성수준이 QM로 결정된다.

ISO 26262에서는 결정된 자동차 안전무결성수준에 따라 SW의 개발 과정에서 적용해야 하는 활동 요건 및 기법을 제시하고 있다. 예를 들어, 안전 요구사항을 기술하기 위해 [그림 2-3]과 같이 안전 활동의 세부 요건을 제시하고 해당 활동

14) Automotive safety integrity level

15) Quality Management의 약어이며, 자동차 안전 무결성 수준의 최하위 수준에 해당함

16) ISO26262, Road vehicles -- Functional safety --

을 수행하기 위해 자동차 안전무결성수준에 따라 적합한 기법을 사용할 수 있도록 [그림 2-4]와 같이 제시한다.

<표 2-7> ISO 26262 위험 파라미터 수준 정의

위험 파라미터	등급	설 명
심각도 (Severity)	S0	상해 없음
	S1	가벼운 상해
	S2	생존 가능한 정도의 증상
	S3	생존이 불확실한 정도의 증상
발생 확률 (Exposure)	E0	거의 불가능함
	E1	매우 낮은 확률
	E2	낮은 확률
	E3	중간 확률
	E4	높은 확률
통제도 (Controllability)	C0	대개의 경우 통제 가능
	C1	간단히 통제 가능
	C2	보통의 경우 통제 가능
	C3	통제하기 어렵거나 통제 불가능

[그림 2-3] ISO 26262의 SW 안전 요구사항 명세 요건

6.4.1 Specification of safety requirements 6.4.1.1 To achieve the characteristics of safety requirements listed in 6.4.2.4, safety requirements shall be specified by an appropriate combination of: a) natural language, and b) methods listed in Table 1. NOTE For higher level safety requirements (e.g. functional and technical safety requirements) natural language is more appropriate while for lower level safety requirements (e.g. software and hardware safety requirements) notations listed in Table 1 are more appropriate.

출처 : ISO 26262 Road vehicles -- Functional safety -- Part 8

[그림 2-4] ISO 26262의 SW 안전 요구사항 작성 기법

Table 1 — Specifying safety requirements					
Methods		ASIL			
		A	B	C	D
1a	Informal notations for requirements specification	++	++	+	+
1b	Semi-formal notations for requirements specification	+	+	++	++
1c	Formal notations for requirements specification	+	+	+	+

출처 : ISO 26262 Road vehicles -- Functional safety -- Part 8

<표 2-8> ISO 26262 자동차 안전 무결성 수준 결정

심각도 분류	발생 확률 분류	통제도 분류		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

이처럼 ISO 26262에서는 자동차 분야에서 사용되는 다수의 전기/전자/프로그래밍 가능한 전자 장치 시스템을 대상으로 안전 분류를 수행할 수 있도록 방법을 제시하고 있다. ISO 26262에서는 개발하고자 하는 시스템 수준에서 안전 분류를 수행하는 방식을 제공하며, 제공되는 안전 분류 방법에 위험 발생 확률을 고려하는 부분이 존재하여 SW 중심의 안전 분류 수행 방식으로 활용하기에 어려움이 존재한다.

5. 의료기기 분야의 안전 표준

의료기기 분야에서 안전 분류를 다루고 있는 IEC 62304를 기준으로 연구 조사를 수행했다. IEC 62304는 의료기기 분야에서 사용하는 SW를 대상으로 기능 안전성을 고려할 수 있도록 제정된 국제 표준이다.

IEC 62304는 안전 수준을 고려하여 의료기기용 SW를 개발 및 관리할 수 있도록 클래스(Class)라는 분류 체계를 가진다. 클래스는 해당 SW가 위험 발생 시, 환자에게 얼마만큼의 피해를 일으키는 상태인지를 판단하여 구분하고 있다. IEC 62304에서 제시하고 있는 클래스별 피해 상태는 <표 2-9>와 같이 정의된다. IEC 62304는 SW 기능의 실패 확률을 산정하거나 도출하기 어려운 점을 고려하여 확률적인 요소를 사용하지 않고 위험도만을 사용하여 SW 안전 분류를 수행한다.¹⁷⁾

<표 2-9> IEC 62304 클래스별 피해 정도

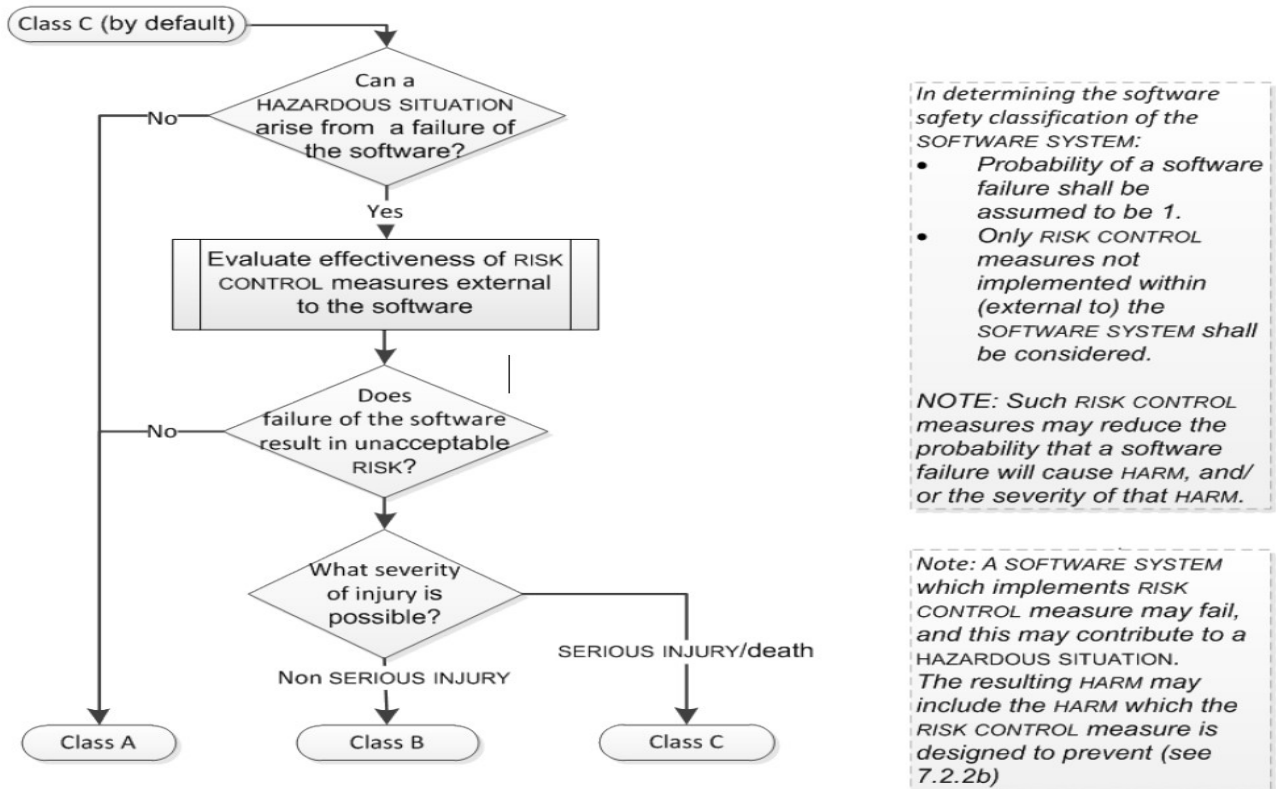
클래스 구분	설 명
Class A	SW 시스템이 위험한 상황을 일으키지 않음
Class B	SW 시스템이 위험한 상황을 일으킬 수 있고 식별된 위험이 수용 불가능한 상태이며, 위험 발생 시 환자에게 경상 발생 가능함
Class C	SW 시스템이 위험한 상황을 일으킬 수 있고 식별된 위험이 수용 불가능한 상태이며, 위험 발생 시 환자에게 중상 또는 환자 사망 발생 가능함

IEC 62304는 [그림 2-5]와 같이 SW 안전 분류를 통해 SW의 클래스를 결정한다. 의료기기용 SW의 안전 분류를 수행하는 과정에서 식별된 위험을 대상으로 안전 분석을 수행하여 제조사의 판단에 따라 수용 가능한 위험인 경우 Class A로 결정한다. 수용 불가능한 위험에 대해서는 환자가 피해를 보는 정도에 따라

17) IEC 62304, Medical device software – Software life-cycle processes

환자에게 경상을 입히는 경우 Class B, 환자에게 중상을 입히는 경우 Class C로 결정한다.

[그림 2-5] IEC 62304의 SW 안전 분류 방법



출처 : IEC 62304, Medical device software – Software life-cycle processes

예를 들어, 환자 모니터링 시스템(PMS)¹⁸⁾에 탑재되는 SW를 대상으로 위험 분석을 해보자. 기능 고장으로 인해 환자의 위급 상황에 알람을 울리지 못할 수 있다고 가정해 보자. 이는 환자에게 위해(危害)를 가할 수 있는 상황으로 수용 불가능한 위험에 해당하며 이를 통해 환자가 적시에 적절한 조치를 받을 수 없게 되어 중상 또는 사망까지 이르게 될 수 있다. 이는 [그림 2-5]의 기준으로 분류하면 Class C로 결정된다.

다른 예를 들어 보면, 디지털 체온계와 같이 단순히 환자의 체온을 측정하는

18) Patient Monitoring System

SW는 해당 기능의 고장으로 잘못된 체온이 측정되어도 환자에게 상해를 입히지 않는다. 또한, 다른 체온계 사용과 같이 별도 수단으로 체온을 측정할 수 있기 때문에 수용 가능한 위험으로 판단하고 Class A로 결정할 수 있다.

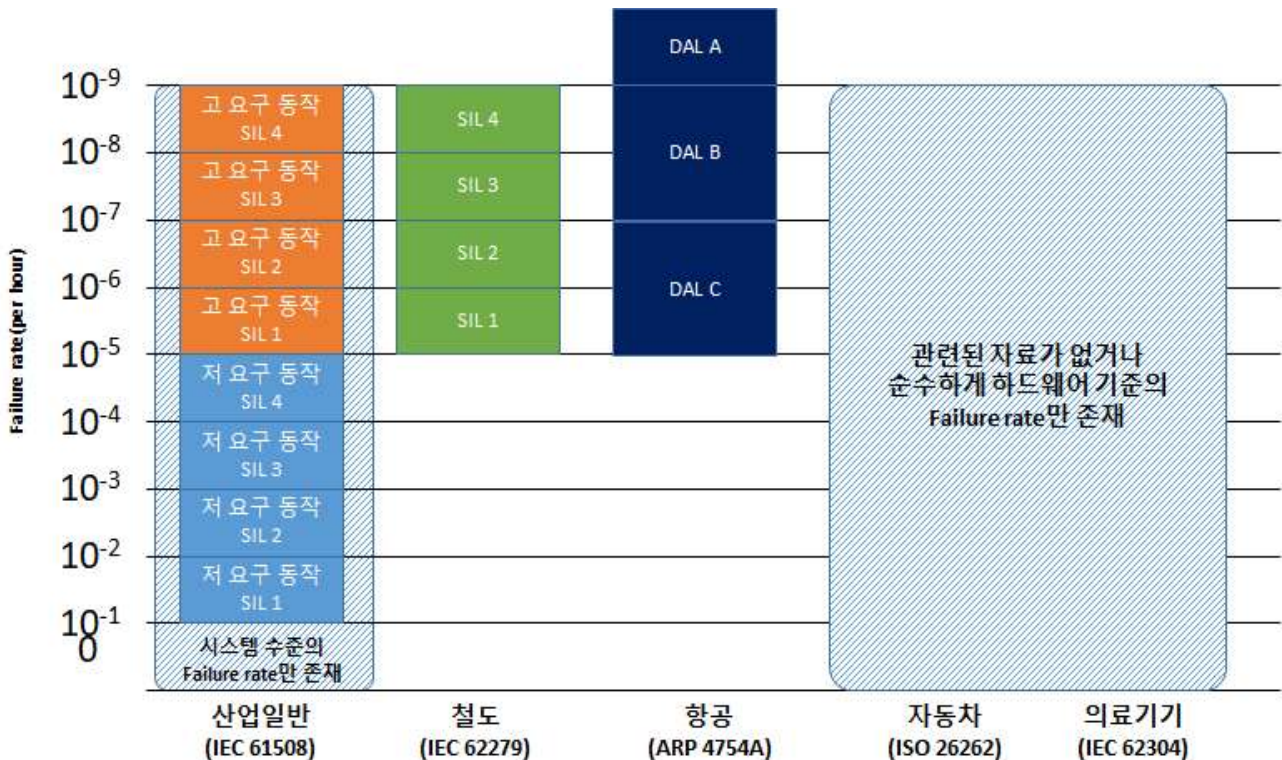
이처럼 IEC 62307에서는 의료기기 분야에서 사용되는 다수의 SW를 대상으로 안전 분류를 수행할 수 있도록 방법을 제시한다. 다만 해당 방법은 결과적으로 환자에게 얼마만큼의 피해를 주는지를 기준으로 안전 분류를 수행하고 있어 해당 안전 분류 방식을 다양한 산업 분야의 SW에 적용한다고 했을 때 세밀한 분류가 이루어지기가 어렵다.

6. 분야 중심의 안전 분류 연구 고찰

분야 중심의 안전 분류 관련 연구는 조사 결과를 기반으로 SW 안전 분류를 도출하기 위해 일반화가 필요하다. 즉, 각기 다른 분야에서 안전을 고려하여 제정된 표준으로 안전 분류를 같은 수준으로 일반화하기 위해 정량적인 지표가 필요하다. 이를 위해 안전 분류 수준별 실패율(Failure rate)을 일반화 지표로 선정하였다. 실패율을 기준으로 산업 일반, 철도, 항공, 자동차, 의료기기 분야의 안전 분류를 비교하면 [그림 2-6]과 같은 결과를 얻을 수 있다.

산업 일반 분야에 해당하는 IEC 61508의 경우 안전 분류 수준별 실패율이 존재하나 시스템 수준에 해당하는 수치만 제공되고 있다. 자동차 분야의 ISO 26262와 의료기기 분야의 IEC 62304는 안전 분류 수준별 실패율이 시스템 수준으로 제공되지 않거나 하드웨어 수준의 실패율만 제공되고 있었다. 이처럼 각기 고유한 분야의 안전 표준의 분류를 실패율을 기반으로 비교 분석하기에는 한계가 있다.

[그림 2-6] 분야 중심의 안전 분류 수준 비교(실패율 기반)

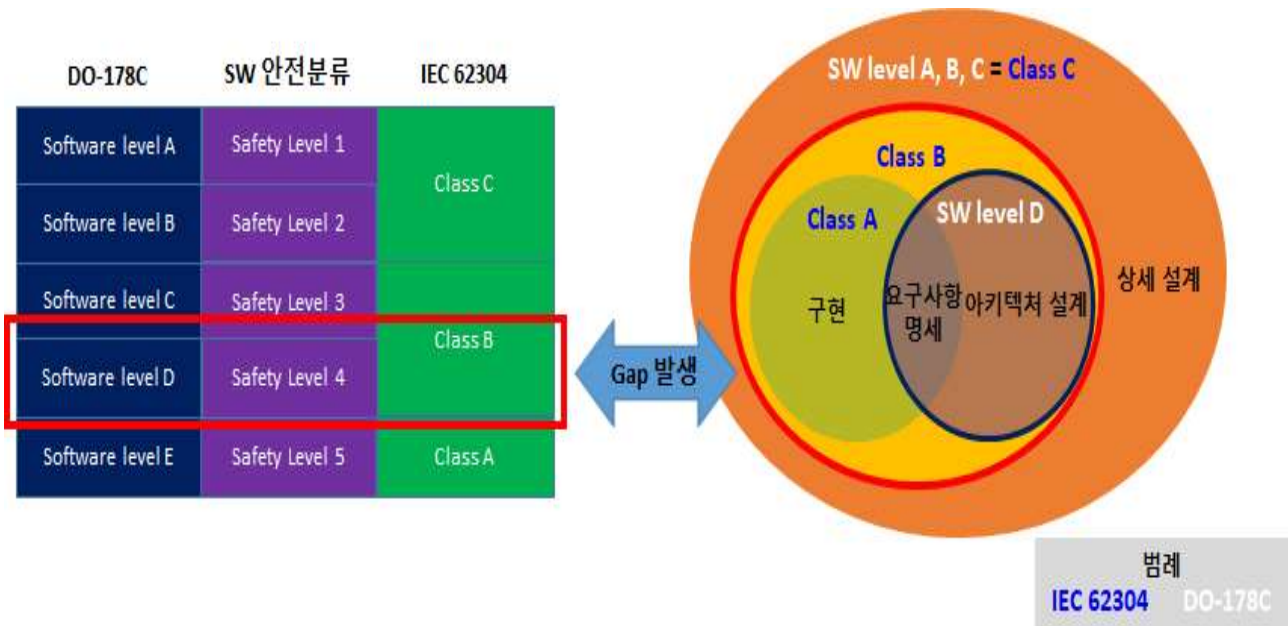


출처 : 항공분야 실패율은 John Rushby의 “New Challenges In Certification For Aircraft Software” (SRI International, 2011) 참조

실패율 기반의 일반화가 적합하지 않다는 판단으로 정성적인 방식으로 안전 분류별 사용된 위험 파라미터를 비교해보고자 하였으나, 분야별 표준에서 SW 측면에서 이를 고려하지 않아 SW 안전 분류 도출에 제한이 있다.

더불어 본 연구 접근 방법에 대해 추가로 고려해야 하는 부분이 존재한다. 정량적·정성적 지표 활용을 통해 SW 안전 분류 도출 시, 수준별 요구되는 활동 및 기법이 연결되지 않는 경우가 발생할 수 있다. 이를 사전에 검증해보기 위해 DO-178C와 IEC 62304의 안전 분류 등급별 세부 요건을 비교하였다. 세부 요건 비교 수행 결과 [그림 2-7]과 같이 수준별 활동 및 기법이 서로 연결되지 않음을 확인하였다.

[그림 2-7] SW 안전 분류(건본)와 DO-178C, IEC 62304 요건 관계



[그림 2-7]에서 명시된 SW 안전 분류(건본)는 DO-178C와 IEC 62304에서 요구하는 안전 분류의 수준을 비교하여 연결하였다. 이후 세밀하게 안전 분류를 구분하기 위해 Safety Level 1 ~ 5와 같이 나눠도록 가정하였다. 이러한 가정 상에서 Safety Level 4에서 요구하는 활동은 DO-178C의 Software Level D와 IEC 62304의 Class B에서 요구하는 활동으로 구성되어야 한다. 이때 해당 수준에서 요구하는 활동의 차이가 존재하여 추후 합리적인 SW 안전 공통기준을 도출하는데 많은 제약이 발생하게 된다.

예를 들어 [그림 2-7]과 같이 SW 안전 분류가 도출된 경우, Safety Level 4는 DO-178C의 Software Level D와 IEC 62304의 Class B에 해당한다. [그림 2-8]과 같이 이때 요구되는 안전 활동은 DO-178C에서는 요구 사항 명세와 아키텍처 설계이고, IEC 62304에서는 요구 사항 명세와 아키텍처 설계, 구현 해당한다. 이처럼 안전 활동에 차이가 발생하여 SW 안전 분류(건본)는 DO-178C와 IEC 62304에서 요구하는 안전 활동을 모두 고려하기는 쉽지 않다.

[그림 2-8] DO-178C의 Software Level D와 IEC 62304의 Class A 요건 비교

DO-178C

IEC 62304

Objective				Activity	Applicability by Software Level				Software development PROCESS			Class A	Class B	Class C
Description	Ref	Ref	A		B	C	D							
1	High-level requirements are developed.	5.1.1.a	5.1.2.a 5.1.2.b 5.1.2.c 5.1.2.d 5.1.2.e 5.1.2.f 5.1.2.g 5.1.2.h	○	○	○	○		5.2. Software requirements analysis					
									5.2.1. Define and document software requirements from SYSTEM requirements					
									5.2.2. Software requirements content	X	X		X	
									5.2.4. Re-EVALUATE MEDICAL DEVICE RISK ANALYSIS					
									5.2.5. Update requirements					
									5.2.6. Verify software requirements					
2	Derived high-level requirements are defined and provided to the system processes, including the system safety assessment process.	5.1.1.b	5.1.2.h 5.1.2.i	○	○	○	○		5.2.3. Include RISK CONTROL measures in software requirements		X		X	
									5.3. Software ARCHITECTURAL design					
3	Software architecture is developed.	5.2.1.a	5.2.2.a 5.2.2.d	○	○	○	○		5.3.1. Transform software requirements into an ARCHITECTURE					
									5.3.2. Develop an ARCHITECTURE for the interfaces of SOFTWARE ITEM S		X		X	
									5.3.3. Specify functional and performance requirements of SOUP item					
									5.3.4. Specify SYSTEM hardware and software required by SOUP item					
									5.3.6. Verify software ARCHITECTURE					
4	Low-level requirements are developed.	5.2.1.a	5.2.2.g 5.2.3.a 5.2.3.b 5.2.4.a 5.2.4.b 5.2.4.c 5.5.b	○	○	○	○		5.3.5. Identify segregation necessary for RISK CONTROL					X
									5.4. Software detailed design					
									5.4.1. Subdivide software into SOFTWARE UNITS		X		X	
									5.4.2. Develop detailed design for each SOFTWARE UNIT					
									5.4.3. Develop detailed design for interfaces				X	
									5.4.4. Verify detailed design					
5	Derived low-level requirements are defined and provided to the system processes, including the system safety assessment process.	5.2.1.b	5.2.2.b 5.2.2.c	○	○	○	○		5.5. SOFTWARE UNIT implementation					
									5.5.1. Implement each SOFTWARE UNIT	X	X		X	
									5.5.2. Establish SOFTWARE UNIT VERIFICATION PROCESS					
									5.5.3. SOFTWARE UNIT acceptance criteria		X		X	
									5.5.5. SOFTWARE UNIT VERIFICATION					
6	Source Code is developed.	5.3.1.a	5.3.2.a 5.3.2.b 5.3.2.c 5.3.2.d 5.5.c	○	○	○	○		5.5.4. Additional SOFTWARE UNIT acceptance criteria					X

이러한 문제 상황을 종합적으로 분석하여, SW 안전 분류 도출을 위한 연구 접근 방식을 분야 중심의 안전 분류 비교 분석이 아닌 SW 중심 안전 분류 비교 분석 방식으로 변경하였다.

제2절 SW 중심 안전 분류 연구 분석

SW 중심의 안전 분류를 제시하고 있는 관련 연구를 조사하여 MIL-STD-882E와 NASA Software Safety Guidebook을 SW 안전 분류를 도출하기 위한 기반 연구로 선정하였다. 이를 분석하여 SW 안전 분류를 도출하는 과정을 설명한다.

1. MIL-STD-882E

MIL-STD-882는 미국 국방부 산하의 모든 군사부서 및 국방기관에서 사용이 승인된 안전 표준이다. 본 표준은 위험에 대한 식별, 분류, 회피에 대한 일반적인 방안을 제시하고 있으며, 2012년 5월 11일에 MIL-STD-882D에서 MIL-STD-882E로 개정됨에 따라 SW 안전 기법 및 실무 등이 추가되어 SW 안전 영역이 보강되었다.

MIL-STD-882E는 SW 중심의 위험 평가를 통해 SW 안전 분류를 수행하는 특징을 가진다. SW 및 SW에 의해 운영되거나 SW의 의존도가 높은 시스템에 대한 위험 평가는 위험 심각도와 위험 발생 확률에만 의존해서는 안 된다.¹⁹⁾ 단일 SW 기능 고장 확률을 추정하는 것은 그 자체가 어려우며²⁰⁾ 과거 데이터를 기반으로 할 수 없다. SW는 일반적으로 응용프로그램에 특화되어 있어 이와 관련된 신뢰성 요소는 하드웨어와 같은 방법으로 추정할 수 없다. 따라서 시스템 위험에 대한 SW의 기여도 평가는 기존과 다른 접근법을 사용해야 한다.

이러한 SW의 특성을 고려하기 위해 MIL-STD-882E는 SW 위험 평가를 위해 새로운 방식을 제공한다. MIL-STD-882E에서 SW 안전 분류는 SW 안전 중요도 매트릭스(SSCM)²¹⁾라는 이름으로 수행한다. 해당 매트릭스는 SW 통제 등급(SCC)²²⁾과 SW 심각도 등급을 통해 평가한다.

SW 심각도 등급은 기존의 여러 안전 표준에서 사용되었던 것과 유사한 모습으로 <표 2-10>과 같이 정의된다. MIL-STD-882E에서 해당 SW 심각도 등급은 SW와 시스템 모두 동일한 기준으로 사용되는 특징이 있다.

19) 박태형 외, “소프트웨어 안전(Safety) 산업 동향 조사”, SPRI, 2017.04

20) John McDermid 외, “Software in Safety Critical Systems: Achievement and Prediction, Thomas Telford Journals, June 2006.11

21) Software safety criticality matrix

22) Software control category

〈표 2-10〉 MIL-STD-882E의 SW 심각도 등급

심각도 등급	설 명	사고 결과 수준
1	재앙적 수준 (Catastrophic)	· 다음 중 하나 이상을 유발 가능: 사망, 영구적 완전 장애, 회복 불가능한 중대한 환경 영향 또는 \$10M 이상의 금전적 손실
2	치명적 수준 (Critical)	· 다음 중 하나 이상을 유발 가능: 영구적 부분 장애, 3명 이상의 입원을 유발할 수 있는 직업병이나 상해, 회복 가능한 중대한 환경 영향 또는 \$1M ~ \$10M의 금전적 손실
3	보통 수준 (Marginal)	· 다음 중 하나 이상을 유발 가능: 1일 이상 결근을 유발하는 직업병이나 상해, 회복 가능한 중간 정도의 환경 영향 또는 \$100K ~ \$1M의 금전적 손실
4	낮은 수준 (Negligible)	· 다음 중 하나 이상을 유발 가능: 결근을 유발하지 않는 직업병이나 상해, 최소한의 환경 영향 또는 \$100K 이하의 금전적 손실

SW 통제 등급이란 〈표 2-11〉과 같이 SW가 안전이 중요한 시스템 및 하부 시스템에서 문제 발생 시, SW가 어느 정도까지 자율성을 갖고 제어 권한을 행사하느냐에 따라 총 5개의 등급으로 구분한다.

〈표 2-11〉 MIL-STD-882E의 SW 통제 등급

SW 통제 등급(SCC)		
등급	명 칭	설 명
1	자율 (AT, Autonomous)	· 잠재적으로 안전에 중요한 하드웨어 시스템, 하위시스템 또는 구성 요소의 재난 및 위험 발생을 방지하기 위해 사전 정의된 안전 감지 및 개입 없이 자율적인 통제 권한을 행사하는 SW 기능

2	반-자율 (SAT, Semi-Autonomous)	· 잠재적으로 안전에 중요한 하드웨어 시스템, 하위시스템 또는 구성 요소의 재난 및 위험 발생을 방지하기 위해 사전 정의된 안전 감지 및 개입을 위한 시간을 확보하기 위한 제어 권한을 행사하는 SW 기능 · 사고 발생 또는 위험을 완화하거나 제어하기 위해 운영자가 조속히 사전 정의된 조치를 취하도록 요구하는 안전 관련 정보를 표시하는 SW 항목. SW 예외, 오류, 결함 또는 지연은 사고 발생 또는 예방을 수행하지 못함
3	중복적인 내결함성 (RFT, Redundant Fault Tolerant)	· 안전 기능이 중요한 하드웨어 시스템, 하위 시스템 또는 업무 수행을 위해 지시 기능이 필요한 구성요소에 명령을 지시하는 SW 기능. 시스템 탐지 및 기능적 반응은 기 정의된 각 위험 상태에 대한 중복적이고 독립적인 내결함성 포함 · 중요한 결정을 내리는 데 필요한 안전에 필수적인 정보를 생성하는 SW. 이 시스템은 위험한 조건, 탐지 및 디스플레이에 대한 다수의 중복적이고 독립적인 내결함성 메커니즘 포함
4	영향 있음 (Influential)	· SW는 운영자의 결정을 지원하기 위한 안전 관련 정보를 생성하지만, 사고 회피를 위해 운영자의 조치를 요구하지 않음
5	안전 영향 없음 (NSI, No Safety Impact)	· SW 기능이 안전에 중요한 하드웨어 시스템, 하위 시스템 또는 구성 요소에 대해 명령 또는 제어 권한이 없으며 안전에 중요한 정보를 제공하지 않음 · SW는 안전 관련 또는 시간에 민감한 데이터 또는 제어 기기의 상호 작용에 필요한 정보를 제공하지 않음. SW는 안전에 중대한 또는 시간에 민감한 데이터를 전송하거나 해결하지 않음

앞서 설명한 SW 심각도 및 SW 통제 등급을 이용하여 <표 2-12>와 같이 SW 안전 중요도 매트릭스를 이용하여 SW 심각도 지수(SwCI)²³⁾를 결정한다.

23) Software Criticality Index

〈표 2-12〉 MIL-STD-882E의 SW 안전 중요도 매트릭스

SW 통제 등급	심각도 등급			
	재앙적 수준	치명적 수준	보통 수준	낮은 수준
1	SwCI 1	SwCI 1	SwCI 3	SwCI 4
2	SwCI 1	SwCI 2	SwCI 3	SwCI 4
3	SwCI 2	SwCI 3	SwCI 4	SwCI 4
4	SwCI 3	SwCI 4	SwCI 4	SwCI 4
5	SwCI 5	SwCI 5	SwCI 5	SwCI 5

결정된 SW 심각도 등급에 맞추어 SW 개발 시, 엄격히 준수해야 하는 안전 활동수준(LOR)²⁴⁾이 결정된다. 안전활동수준은 필요에 따라 테일러링이 가능하며, 기본적으로는 〈표 2-13〉과 같이 수행하기를 권고하고 있다.

〈표 2-13〉 MIL-STD-882E의 안전활동수준 권고사항

SW 심각도 지수	필요 업무
SwCI 1	요구 사항, 아키텍처, 설계, 코드를 분석하고 심도 있는 SW 안전 테스트 수행
SwCI 2	요구 사항, 아키텍처, 설계를 분석하고 심도 있는 SW 안전 테스트 수행
SwCI 3	요구 사항, 아키텍처를 분석하고 심도 있는 SW 안전 테스트 수행
SwCI 4	심도 있는 SW 안전 테스트 수행
SwCI 5	안전성 검증을 통해 안전과 무관하다고 판단되면 SW 안전 관련 분석 및 확인 불필요

SW 심각도 지수가 높아질수록 필수 SW 안전 활동이 테스트부터 요구 사항, 아키텍처, 설계, 코드 분석 순으로 추가되는 양상을 갖는다. 상세 활동에 대한 가이드는 군수 관련 연산 시스템의 SW 안전 설계 및 평가 지침(Guidance on software safety design and assessment of munition-related computing systems)

24) Level of Rigor

을 활용하도록 권고하고 있어, 추후 SW 안전 공통기준을 도출하는 데 활용한다.

MIL-STD-882E의 SW 안전 분류는 국방 분야의 시스템 및 SW를 기준으로 활용될 수 있도록 고안된 모델로써 제시하고 있는 위험 심각도, SW 통제 등급, 안전 활동 권고사항이 다양한 산업 분야를 고려하여 개발되었는지는 알 수 없기 때문에 다양한 산업 분야에서 사용하고 있는 위험 심각도, SW 통제 등급, 안전 활동 권고사항과 비교 분석 후 활용하고자 한다.

2. NASA Software Safety Guidebook

NASA Software Safety Guidebook은 미 항공우주국에서 SW 개발 시 안전을 고려하여 개발할 수 있도록 고안한 표준이다. 본 가이드북은 SW가 동작하면서 발생할 수 있는 위험에 대해 사전에 평가하여 SW 안전 분류를 결정한다. 결정된 SW 안전 분류 수준에 따라 SW의 안전성을 향상시킬 수 있도록 SW 개발 시 수행할 수 있는 안전 활동 및 기법을 설명한다.

NASA Software Safety Guidebook은 MIL-STD-882E와 유사하게 SW 특성을 고려하여 위험 평가 시, 위험의 심각도와 발생 확률을 기반으로 SW 안전 분류를 하지 않고 위험의 심각도와 SW 통제 등급을 활용하여 SW 위험 매트릭스(SRM)²⁵⁾라는 이름으로 SW 안전 분류를 수행한다.

SW 위험 매트릭스를 수행하기 위해 사용하는 위험의 심각도와 SW 통제 등급은 <표 2-14>와 <표 2-15>에서 각각 정의하고 있다. 한 가지 특이한 점으로 SW 통제 등급을 정의할 때, 키워드 A와 B를 사용하여 SW 통제 등급이 가지고 있는 특성을 보다 명확하게 설명하고 있다. SW 통제 등급 이름 중 A는 SW가 위험을 통제하는 것을 의미하며 B는 SW가 사용자에게 안전 관련 데이터를 생성

25) Software Risk Matrix

하여 제공하는 것을 의미한다.

<표 2-14> NASA Software Safety Guidebook의 SW 심각도 등급

심각도 등급	사고결과 수준
재앙적 수준 Catastrophic	· 인명 손실 또는 영구적 장애, 전체 시스템 손실, 지상 시설 손실, 심각한 환경 피해
치명적 수준 Critical	· 심각한 부상 또는 일시적 장애, 주요 시스템 또는 환경 손상
적당한 수준 Moderate	· 경미한 부상, 경미한 시스템 손상
미비한 수준 Negligible	· 부상 또는 경미한 부상 없음, 일부 시스템 부하, 시스템 손상 없음

<표 2-15> NASA Software Safety Guidebook의 SW 통제 등급

SW 통제 등급	설 명
IA ²⁶⁾	SW가 안전 중요 기능의 부분 또는 전체를 자동 제어 하는 경우
	복잡한 서브시스템을 가지고 있고 병렬 프로세서로 상호작용을 하거나 다중 인터페이스가 있는 복잡한 시스템이 존재하는 경우
	일부 또는 전체의 안전 중요 기능이 시간에 많은 영향을 받는 경우
IIA & IIB	위험을 감지하고 사용자에게 안전 조치의 필요성을 알리는 경우
	병렬프로세싱은 없지만, 소수의 인터페이스 및 서브시스템으로 다소 복잡한 시스템을 가지는 경우
	사용자나 자동화된 시스템이 위험 통제에 필요한 시간 내에 조치를 수행할 수 있는 경우
IIIA & IIIB	몇 개의 완화 시스템을 통해 위험을 방지할 수 있는 경우
	안전 중요 정보를 제공하는 여분의 방식이 있는 경우
	완화 시스템이 중요한 시간 안에 동작하는 경우
IV	위험을 제어하지 않으며 사용자를 위한 안전 중요데이터를 생성하지 않는 경우
	2~3개의 서브시스템으로 이루어진 단순한 시스템인 경우
	시간이 중요한 요소가 되지 않는 경우

<표 2-16>과 같이 SW 위험 매트릭스를 이용하여 SW 안전 분류를 수행하며, SW 위험 색인(SRI)²⁷⁾이 도출된다. SW 위험 색인은 총 5개의 값으로 구분되면

26) IA 등급의 경우, 사용자에게 안전관련 정보를 생성하여 제공하지 않고 자율적으로 안전 기능을 제어 하므로 B(안전 중요 데이터 생성 및 제공)에 대한 구분이 필요하지 않음

27) Software Risk Index

<표 2-17>과 같은 의미를 갖는다.

<표 2-16> NASA Software Safety Guidebook의 SW 위험 매트릭스

SW 통제 등급	심각도 등급			
	재앙적 수준	치명적 수준	적당한 수준	미비한 수준
IA	1	1	3	4
IIA & IIB	1	2	4	5
IIIA & IIIB	2	3	5	5
IV	3	4	5	5

<표 2-17> NASA Software Safety Guidebook의 SW 위험 색인

SW 위험 색인	위험 정의
1	높은위험: SW가 재앙적이거나 치명적인 위험을 제어
2	중간위험: SW가 감하(減下)된 재앙적이거나 치명적인 위험을 제어하나 여전히 위험이 중요한 상황
3 ~ 4	적정위험: SW가 덜 중요한 위험을 제어
5	낮은위험: SW가 재앙적이거나 치명적인 위험을 제어

본 가이드북은 결정된 SW 위험 색인에 따라 SW 요구사항, 설계, 구현, 검증 단계에서 적용할 수 있는 적절한 수준의 안전 활동을 제공하여 안전성을 고려하여 SW를 개발할 수 있도록 지원한다. 안전 활동 정보는 추후 SW 안전 공통기준을 마련하는데 활용한다.

제3절 SW 안전 분류 모델

SW 안전 분류를 도출하기 위해 SW 중심의 안전 분류를 제시하고 있는 관련 연구를 분석하여 SW 안전 분류 모델을 제안한다. 다양한 분야에서 활용될 수 있도록 SW 안전 분류 모델을 개선 후 전문가 자문단의 검토를 통해 SW 안전 분류 모델의 적절성 및 적합성을 확인한다.

1. SW 안전 분류 모델 제안

일반적으로 다수의 안전 분야 표준들을 살펴본 결과 안전 분류를 수행하기 위해 위험의 심각도와 발생확률을 기반으로 도출하고 있다. 하지만 MIL-STD-882E와 NASA Software Safety Guidebook을 조사·분석한 결과 SW의 위험 발생 확률을 추정하거나 도출하는 것이 매우 어렵기 때문에, 위험 발생 확률은 항상 발생한다는 가정으로 접근하여 SW 안전 분류를 수행해야 한다는 결론을 내릴 수 있다. 즉, 기본적으로 개발하고자 하는 SW의 기능이 가지고 있는 위험의 심각도를 기반으로 안전 분류를 수행하게 된다.

다만 위험의 심각도만을 고려하여 SW 안전 분류를 수행하게 되면 개략적인 수준으로 결과가 도출되는 상황이 발생한다. 이러한 상황을 고려하여 MIL-STD-882E와 NASA Software Safety Guidebook에서는 SW 통제 등급을 SW 안전 분류의 한 축으로 활용하고 있다.

앞서 설명한 상황과 관련 연구를 분석한 결과를 바탕으로 MIL-STD-882E에서 제공하고 있는 SW 중심의 안전 분류 모델인 SW 안전 중요도 매트릭스가 본 연구를 통해 도출해야 하는 모델에 가장 부합한다고 판단하여 이를 참조하여 [그림 2-9]와 같이 SW 안전 분류 초기 모델로 제안했다.

정의된 SW 안전 분류 모델은 MIL-STD-882E와 동일하게 Catastrophic, Critical, Marginal, Negligible의 위험 심각도와 Autonomous, Semi Autonomous, Redundant Fault Tolerant, Influential, No Safety Impact의 SW 통제 등급을 각 축으로 가진다. 이를 기반으로 1 ~ 5까지의 SW 위험 색인(SwCI)을 결정할 수 있고 그 의미가 <표 2-12>와 같이 MIL-STD-882E와 동일하게 정의했다.

[그림 2-9] SW 안전 분류 모델 제안

Severity SW Control Category	Catastrophic	Critical	Marginal	Negligible
AT Autonomous	SwCI 1	SwCI 1	SwCI 3	SwCI 4
SAT Semi Autonomous	SwCI 1	SwCI 2	SwCI 3	SwCI 4
RFT Redundant Fault Tolerant	SwCI 2	SwCI 2	SwCI 4	SwCI 4
Influential	SwCI 3	SwCI 4	SwCI 4	SwCI 4
NSI No Safety Impact	SwCI 5	SwCI 5	SwCI 5	SwCI 5

2. SW 안전 분류 모델 개선

본 연구를 통해 도출하고자 하는 SW 안전 분류 및 SW 안전 공통기준은 특정 분야에 한정하여 사용하는 것이 아니라 SW 안전을 고려해야 하는 모든 분야에 대해서 적용할 수 있어야 한다. 앞서 제안된 SW 안전 분류 모델은 국방 분

야를 중심으로 고려된 위험 심각도와 SW 통제 등급을 사용하고 있다. 다양한 도메인에서 SW 안전 분류가 활용될 수 있도록 관련 연구를 조사·분석하여 위험 심각도 및 SW 통제 등급 개선을 수행했다.

가. 위험 심각도 개선

위험 심각도의 경우 MIL-STD-882E와 NASA Software Safety Guidebook과 유사한 개념이 활용되고 있는 항공, 의료기기 분야의 관련연구를 조사 분석하여 위험 심각도 수준을 재정의했다.

1) 항공 분야

항공 분야에서는 DO-178C를 기준으로 위험 심각도를 참조하여 분석했다. <표 2-18>과 같이 총 5개의 위험 심각도 수준을 가지고 있으며 각 위험 심각도 수준의 정의를 보면 항공기에 탑승한 승무원 및 승객의 피해 규모를 기준으로 정의하고 있다.

<표 2-18> DO-178C의 위험 심각도

위험 심각도	설 명
Catastrophic	항공기 추락과 같은 고장으로 다수의 사망자 발생
Hazardous	승무원이 비행을 할 수 없게 되거나 소수의 승객에게 치명적인 부상 발생
Major	승무원이나 승객이 상당한 불편함을 느끼거나 일부 부상을 겪을 수 있음
Minor	승무원과 승객이 불편함을 느낌
No Safety Effect	안전에 영향을 미치지 않으며, 승무원의 업무에도 영향을 미치지 않음

2) 의료기기 분야

의료기기 분야에서는 EN ISO 14971을 기준으로 위험 심각도를 참조하여 분석했다. EN ISO 14971은 IEC 62304에서 참조하는 위험 관리 절차를 설명하는 국제 표준으로 의료기기 분야에 특화되어 있다. EN ISO 14971에서는 위험 심각도 정의를 2개로 구분하여 예시를 통해 설명하고 있다.

첫 번째 위험 심각도 예시는 <표 2-19>와 같이 3수준으로 구분하여 위험 심각도를 사용하는 경우이다. 두 번째 위험 심각도 예시는 <표 2-20>과 같이 5개 수준으로 구분하여 보다 상세하게 위험 심각도를 판단하는 경우이다.

<표 2-19> EN ISO 14971 위험 심각도 - 3개 수준

위험 심각도	설 명
Significant	사망 또는 신체 기능/구조 유실
Moderate	회복 가능한 수준 또는 작은 부상
Negligible	부상을 야기하지 않거나 아주 작은 부상

<표 2-20> EN ISO 14971 위험 심각도 - 5개 수준

위험 심각도	설 명
Catastrophic	환자 사망
Critical	환자의 생명을 위협하는 부상 또는 영구적인 신체 손상
Serious	전문 의료진의 시술이 필요한 부상
Minor	전문 의료진의 시술이 필요 없는 부상
Negligible	환자가 불편함을 느낌

3개 수준, 5개 수준 위험 심각도 모두 환자의 피해 규모를 기준으로 정의하고 있다.²⁸⁾ <표 2-19>와 <표 2-20>의 관계를 정리하면 <표 2-21>과 같이 관계를 확인 할 수 있다. 의료기기 분야의 위험 심각도 2개 중 위험 심각도 분류가 보

28) EN ISO 14971, Medical devices — Application of risk management to medical devices

다 세밀한 5개 수준의 정의를 기준으로 비교 분석하였다.

〈표 2-21〉 EN ISO 14971의 3개 수준과 5개 수준의 위험 심각도 비교

3개 수준 위험 심각도	5개 수준 위험 심각도
Significant	Catastrophic
	Critical
Moderate	Serious
	Minor
Negligible	Negligible

3) 위험 심각도 비교 및 도출

다양한 분야에서 SW 안전성을 고려할 수 있도록 항공, 우주, 국방, 의료기기 분야의 위험 심각도를 살펴보았다. 분야별 위험 심각도의 의미는 해당 분야에 적합한 용어 또는 대상으로 정의되어 있었다. 이를 일반화시키기 위해 각 분야를 나타내는 용어를 배제하고 피해 규모만을 기준으로 구분되도록 비교 분석을 수행하였다.

분야별 위험 심각도 비교 분석 결과는 [그림 2-10]과 같고, 이를 기반으로 SW 안전 분류에 사용할 위험 심각도를 5개 수준으로 정의했다. MIL-STD-882E와 NASA Software Safety Guidebook의 위험 심각도는 4개 수준으로 구분하고 있지만, 항공 및 의료기기 분야에서는 더 세밀하게 위험의 심각도를 구분할 수 있도록 5개 수준을 사용하고 있다. 이를 반영하여 SW 안전 분류에서 사용할 위험 심각도 수준을 5개로 정의하였고 정의된 심각도 수준 기준은 뒤에서 정당성 검증 및 전문가 그룹의 검토를 통해 유효하게 분류되었는지 확인한다.

[그림 2-10] SW 안전 분류의 위험 심각도 비교 및 도출

IEC 14971	Catastrophic	Critical	Serious	Minor	Negligible
MIL-STD-882E	Catastrophic	Critical	Marginal	Negligible	
SW safety Guide book(NASA)	Catastrophic	Critical	Moderate	Negligible	
DO-178C	Catastrophic		Hazardous	Major	Minor
SW 안전 분류 (위험 심각도)	Catastrophic	Critical	Major	Minor	Negligible

※ DO-178C는 유일하게 안전과 무관한 수준(No Effect)까지 고려하여 있어 분석에서 제외함

SW 안전 분류에서 사용할 위험 심각도의 수준 별 의미는 <표 2-22>와 같이 정의하였다.

<표 2-22> SW 안전 분류 위험 심각도 정의

위험 심각도	설 명
Catastrophic	· 한 명 또는 다수의 인원이 사망 · 시스템 유실
Critical	· 생명에 위협을 줄 수 있는 정도의 상해 · 주요 시스템 손상
Major	· 병원에 내방하여 전문적인 치료를 받아야 하는 부상 · 부가 시스템 손상
Minor	· 간단한 응급처치로 회복할 수 있는 부상 · 일시적인 시스템 기능 상실
Negligible	· 일부 시스템 부하 발생 · 사용자가 불편함을 느낌

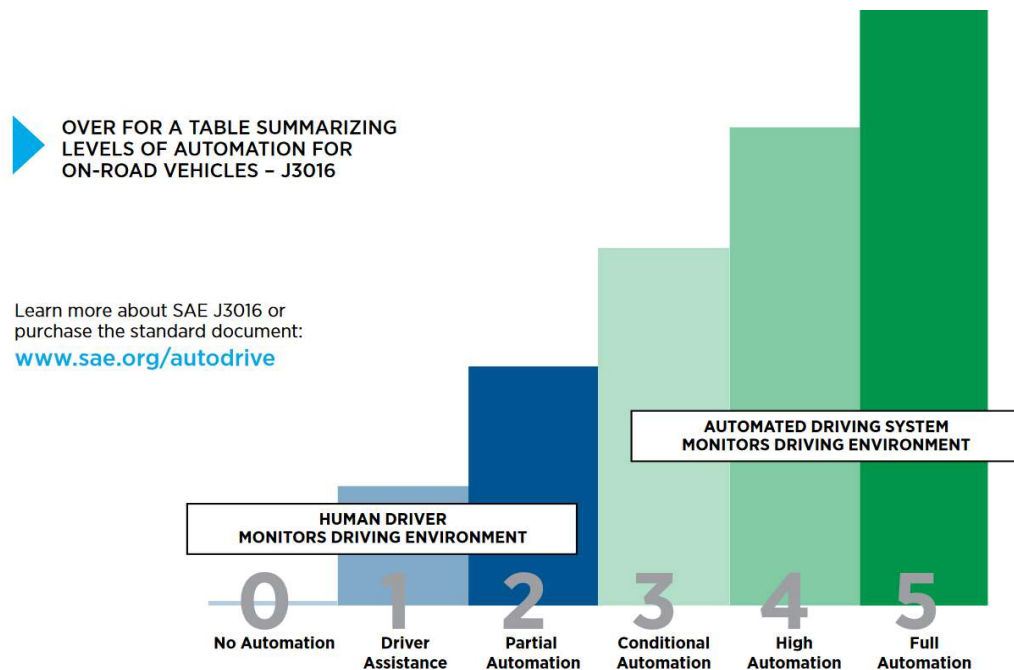
나. SW 통제 등급 개선

SW 통제 등급의 경우 MIL-STD-882E와 NASA Software Safety Guidebook과 유사한 개념이 활용되고 있는 자동차, 항공·국방 분야의 관련 연구를 조사 분석하여 SW 통제 등급을 재정의했다.

1) 자동차 분야

자동차 분야는 미국 자동차기술학회(SAE)²⁹⁾에서 정의한 자율주행 수준 등급을 기준으로 SW 통제 등급을 고려한 부분이 있어 이를 조사 분석하였다. 4차 산업혁명과 더불어 최근 이슈가 되고 있는 자율주행은 SW가 그 중심에 위치하고 있으며 SW의 제어 자율성을 고려한다는 특징이 존재한다.

[그림 2-11] 자율등급에 따른 자율주행차 구분 기준



출처 : SAE international, AUTOMATED DRIVING - LEVELS OF DRIVING AUTOMATION ARE DEFINED IN NEW SAE INTERNATIONAL STANDARD J3016

29) 과거에 미국 자동차 공학회(Society of Automotive Engineers)였으며 현재는 SAE International임

미국 자동차 기술학회(SAE)에서 정의한 자율주행 수준 등급은 [그림 2-11]과 같이 0단계에서 5단계까지 총 6단계가 있으며, 이중 자율주행시스템이라고 함은 자율주행 수준 등급 3단계 이상을 뜻한다. 이는 운전자 또는 자동화된 운전 시스템이 운전 환경에 대해 주시 가능한지에 따라 구분된다.³⁰⁾

미국 자동차기술학회(SAE)에서 제시한 [그림 2-12]와 같이 자율주행 등급별 주요 기능을 살펴보면, SAE Level 0은 운전자가 주행을 위한 모든 작업을 진행하는 것을 의미하며, SAE Level 1은 차량의 주행보조 시스템이 특정 일부 운전 기능을 자동화 하는 것이다. SAE Level 2는 차량의 주행보조 시스템이 실제로 운전 기능 일부를 대신하여 수행하지만 운전자는 주행 환경을 지속해서 주시해야 하고 시스템이 지원하지 않는 모든 운전 기능을 직접 수행해야 한다.

SAE Level 3은 차량의 주행 자동화 시스템이 실제 일부 운전 기능을 수행하지만 운전자가 주행 환경을 틈틈이 주시해야 하며, 자동화 시스템이 운전자에게 주행을 요청할 때 필히 주행을 직접 할 수 있어야 한다. SAE Level 4는 차량의 자동화 시스템이 운전 기능 수행 및 운전 환경을 주시하며, 운전자는 자동화 시스템의 요청 시 차량을 제어할 준비를 하지 않아도 되나, 자동화 시스템은 특정 환경 및 조건하에서만 차량 운영이 가능하다. SAE Level 5는 차량의 자동화 시스템이 모든 주행 상황에서 모든 운전 기능을 수행할 수 있는 것으로 정의한다.

30) J3016, Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems, 2016

[그림 2-12] 자율주행 등급 별 주요 기능

SAE level	Name	Narrative Definition	Execution of Steering and Acceleration/Deceleration	Monitoring of Driving Environment	Fallback Performance of Dynamic Driving Task	System Capability (Driving Modes)
Human driver monitors the driving environment						
0	No Automation	the full-time performance by the <i>human driver</i> of all aspects of the <i>dynamic driving task</i> , even when enhanced by warning or intervention systems	Human driver	Human driver	Human driver	n/a
1	Driver Assistance	the <i>driving mode</i> -specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the <i>human driver</i> perform all remaining aspects of the <i>dynamic driving task</i>	Human driver and system	Human driver	Human driver	Some driving modes
2	Partial Automation	the <i>driving mode</i> -specific execution by one or more driver assistance systems of both steering and acceleration/deceleration using information about the driving environment and with the expectation that the <i>human driver</i> perform all remaining aspects of the <i>dynamic driving task</i>	System	Human driver	Human driver	Some driving modes
Automated driving system ("system") monitors the driving environment						
3	Conditional Automation	the <i>driving mode</i> -specific performance by an <i>automated driving system</i> of all aspects of the <i>dynamic driving task</i> with the expectation that the <i>human driver</i> will respond appropriately to a <i>request to intervene</i>	System	System	Human driver	Some driving modes
4	High Automation	the <i>driving mode</i> -specific performance by an automated driving system of all aspects of the <i>dynamic driving task</i> , even if a <i>human driver</i> does not respond appropriately to a <i>request to intervene</i>	System	System	System	Some driving modes
5	Full Automation	the full-time performance by an <i>automated driving system</i> of all aspects of the <i>dynamic driving task</i> under all roadway and environmental conditions that can be managed by a <i>human driver</i>	System	System	System	All driving modes

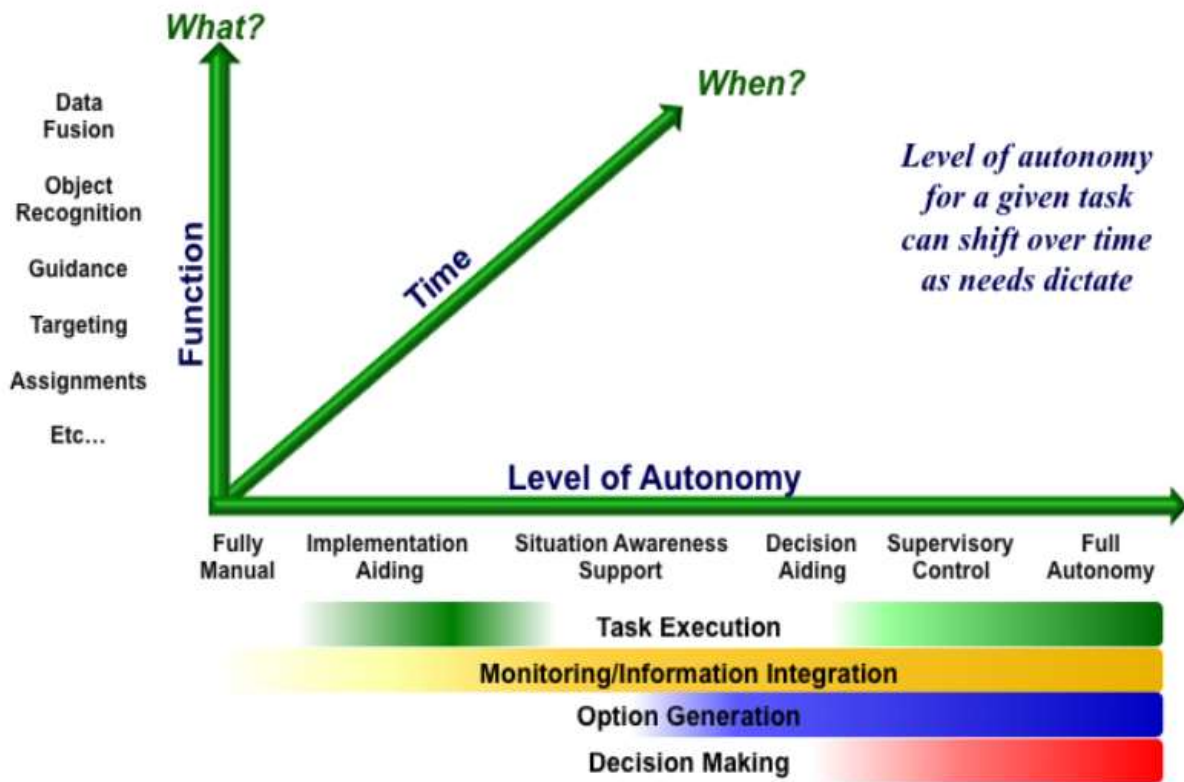
출처 : SAE international, AUTOMATED DRIVING - LEVELS OF DRIVING AUTOMATION ARE DEFINED IN NEW SAE INTERNATIONAL STANDARD J3016

2) 항공 · 국방 분야

항공 · 국방 분야에서는 미국 공군에서 시스템 자율성을 고려한 개발을 수행할 수 있도록 약 40년간의 경험과 연구를 기초로 하여 Autonomous Horizon이라는 지침을 제정하였다. 해당 지침을 통해 미국 공군은 자율 시스템을 개발하여 불필요한 조작 비용을 줄이고, 운영 범위를 늘려 가까운 미래의 미국 공군을 강화할 기회를 얻고자 하는 목표를 갖는다.

Autonomous Horizon에서는 비행사와 자동화 시스템 사이의 상호 작용을 매우 중요하게 생각한다. 이를 테면 주어진 동일한 기능을 놓고도 해당 기능을 사용하는 비행사가 다르거나, 해당 기능을 사용하는 시점에 따라 요구되는 자율성은 달라질 수 있기 때문이다. [그림 2-13]은 주어진 기능이 필요에 따라 다른 자율성을 가져야 한다는 원칙과 자율성 수준으로 6개로 구분하여 설명하고 있다.

[그림 2-13] Autonomous Horizon 내 자율성 수준



출처:Autonomous horizon Volume I: Human-Autonomy Teaming, U.S. AirForce, 2015.06

자율성 수준은 주어진 기능이 수행해야 해야 하는 능력이 증대됨에 따라 증가한다. 이때 자율성 수준을 결정하기 위한 요소로 Task Execution, Monitoring/Information Integration, Option Generation, Decision Making을 이용한다. 이러한 요소별 정의는 <표 2-23>과 같다.

〈표 2-23〉 자율성 수준 결정 요소

요 소	설 명
Task Execution	· 업무를 수행하는 능력
Monitoring/Information Integration	· 주어진 상황과 시스템 상태를 인지하는 능력 · 주어진 상황을 인지하기 위해 다른 데이터를 통합하는 능력
Option Generation	· 의사결정을 위한 잠재적 옵션을 생성하는 능력
Decision Making	· 옵션을 선택하여 적용할 작업을 결정할 수 있는 능력

자율성 수준 결정 요소를 기반으로 6개의 자율성 수준으로 구분하며 각각의 자율성 수준 정의는 〈표 2-24〉와 같다.

〈표 2-24〉 자율성 수준 정의

자율성 수준	설 명
Fully manual	모든 작업 수행이 사용자에게 의해 완료됨
Implementation aiding	비행 관리 시스템 또는 표적 설정을 지원하는 스마트 무기 같은 사용자 작업을 지원함(단, 사용자가 모든 결정을 내림)
Situation awareness support	사용자의 의사결정과 주어진 상황을 인지하기 위한 통합된 정보를 제공하기 위해 상이한 데이터가 병합되어야 하는 경우
Decision aiding	시스템이 잠재적 옵션을 제공하거나 옵션의 순위를 매길 수 있음(단, 사용자가 최적의 옵션을 선택하거나 선택하지 않을 수 있음)
Supervisory control	시스템이 정보 수집하며 올바른 조치를 결정하고 조치를 수행하는 것을 포함하여 기능의 모든 측면을 자동으로 제어하지만, 사용자가 필요에 따라 목표를 설정하고 개입할 수 있음
Full autonomy	사용자의 지침이나 개입 없이도 주어진 기능의 모든 측면을 완벽하게 제어할 수 있음

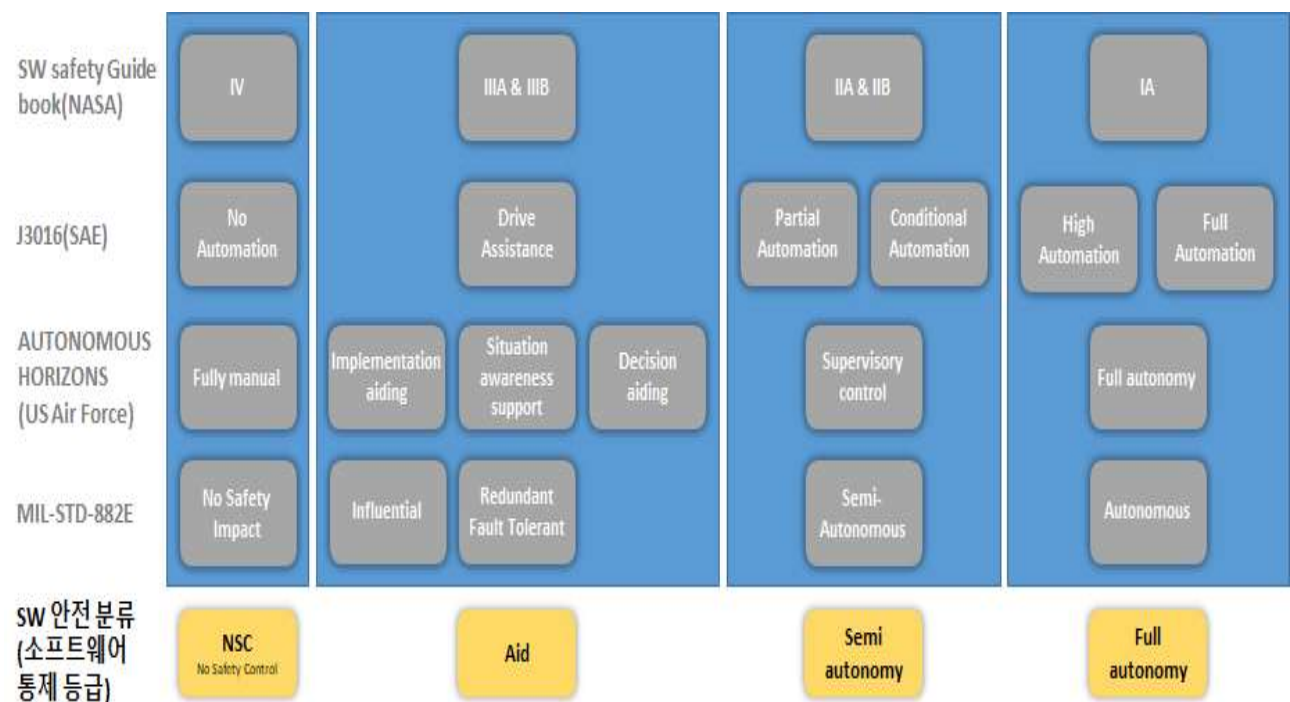
3) SW 통제 등급 비교 및 도출

다양한 분야에서 SW 안전 분류를 활용할 수 있도록 항공, 우주, 국방 분야에

서 사용하는 자율성에 대해 살펴보았다. 분야별 자율성에 대한 기준은 자율성 수준 범위와 요소에 따라 다른 특징을 가진다. 이를 일반화하여 SW 통제 등급을 재정의하고자 한다.

분야별로 제시하고 있는 SW 통제 등급의 개념을 일반화하기 위해 안전 관련 정보 제공에 대한 여부와 안전 기능 제어 주체가 사용자인지 시스템인지를 구분하여 분류하였다. 해당 일반화 요소에 맞추어 SW 통제 등급을 정의하면 [그림 2-14]와 같이 도출할 수 있다.

[그림 2-14] SW 안전 분류의 SW 통제 등급 비교 및 도출



재정의된 SW 통제 등급은 총 4개로 구성되며, NSC부터 Full autonomy 순으로 SW의 자율적인 통제 수준이 높아진다. 재정의된 SW 통제 등급의 특징은 <표 2-25>와 같이 정리할 수 있으며 등급별 의미는 다음 같다.

NSC의 경우, No safety Control의 약자로서 SW가 안전 관련된 기능의 제어

가 없음을 의미하고 Aid는 SW가 일부 기능을 수행하는데 지원하는 부분이 있는 경우를 의미한다. Semi autonomy는 일반적으로 SW가 안전 관련 기능의 자율성을 가지고 있지만, 위급상황에 사용자가 개입할 수 있는 여지가 있는 경우이며 Full autonomy는 SW가 사용자의 개입 없이 안전기능을 제어하고 위급상황에 대응하는 수준을 의미한다.

<표 2-25> SW 통제 등급 정의

SW 안전 통제 등급	설 명
NSC (No safety control)	· 안전 관련 정보 제공 (X) · 안전 기능 제어 주체 (N/A)
Aid	· 안전 관련 정보 제공 (O) · 안전 기능 제어 주체 (N/A)
Semi autonomy	· 안전 관련 정보 제공 (O) · 안전 기능 제어 주체 (Operator/SW)
Full autonomy	· 안전 관련 정보 제공 (X) · 안전 기능 제어 주체 (SW)

다. SW 안전 분류 초안 도출

SW 안전 분류 모델을 대상으로 다양한 분야의 관련 연구를 조사 분석하여 넓은 분야에서 활용될 수 있도록 위험 심각도와 SW 통제 등급을 개선했다. 이를 기반으로 SW 안전 분류 초안을 도출할 수 있었으며, 해당 결과는 [그림 2-15]와 같다.

SW 안전 분류 모델과 비교하여 위험 심각도 및 SW 통제 등급 이외에 보완된 부분이 존재한다. 첫 번째로 기존 MIL-STD-882E에서 사용하던 SW 위험 색인(SwCI)이라는 표현을 ‘SW안전위험색인(SSRI, Software Safety Risk Index)’으로 변경하고 그 의미를 <표 2-26>과 같이 정의하였다. 두 번째로 SW 통제 등급으로 표현되는 용어를 명확하게 의미를 나타낼 수 있도록 ‘SW안전통제등급

(SSCL, Software Safety Control Level)’ 로 변경하였다.

[그림 2-15] SW 안전 분류 초안 도출

		MIL-STD-822E + IEC 14971 + DO-178C + NASA(SW safety guidebook)				
		Severity				
		SW safety control level				
		Catastrophic	Critical	Major	Minor	Negligible
US Air Force (AUTONOMOUS HORIZONS) + MIL-STD-822E + SAE(J3016) + NASA(SW safety guidebook)	Full autonomy	SSRI 1	SSRI 1	SSRI 3	SSRI 4	SSRI 5
	Semi autonomy	SSRI 1	SSRI 2	SSRI 3	SSRI 4	SSRI 5
	Aid	SSRI 2	SSRI 2	SSRI 3	SSRI 4	SSRI 5
	No safety control	SSRI 5	SSRI 5	SSRI 5	SSRI 5	SSRI 5

<표 2-26> SW 안전 위험 색인 정의

SW 안전 위험 색인	설 명
SSRI 1	SW가 보유하고 있는 위험방지 제어 기능에 대해 반자율 이상의 자율성을 가지고 Catastrophic 수준의 위험을 제어하거나 완전자율 수준의 자율성을 가지고 Critical 수준의 위험을 제어함
SSRI 2	SW가 보유하고 있는 위험방지 제어 기능에 대해 지원 수준의 자율성을 가지고 Catastrophic 위험을 제어하거나 지원 및 반자율 수준의 자율성을 가지고 Critical 수준의 위험을 제어함
SSRI 3	SW가 보유하고 있는 위험방지 제어 기능에 대해 자율성 가지며 Serious 수준의 위험을 제어함
SSRI 4	SW가 보유하고 있는 위험방지 제어 기능에 대해 자율성 가지며 Tolerable 수준의 위험을 제어함
SSRI 5	SW가 위험방지 제어 기능을 보유하지 않거나 Negligible 수준의 위험을 제어함

SSRI 5에서 SSRI 1로 이동 할수록 안전 노력(Safety effort)이 증가한다. 여기서 안전 노력이란 SW의 안전성을 향상 시킬 수 있도록 투입되는 노력의 수준을 의미한다.

3. 전문가 자문단 검토 및 SW 안전 분류 보완

SW 안전 분류 모델 선정 후 다양한 분야의 연구 조사를 통해 SW 안전 분류 모델을 개선하고 SW 안전 분류 초안까지 도출하였다. 현재까지 정리된 내용을 기반으로 [그림 2-16]과 같이 SW 안전 분류 도출 과정 및 결과를 정리한 자료를 전문가 자문단에 공유하여 검토를 수행했다. 전문가 자문단은 학계(4명)·산업계(1명)·연구기관(3명)에서 활발히 활동하는 SW 안전 전문가들로 구성하였다.

[그림 2-16] 전문가 자문단 검토용 자료



전문가 자문단의 검토 의견을 살펴본 결과, 주로 SW 안전 분류의 위험 심각

도, SW 안전 제어 등급에 대한 의견이 주를 이루었다. 주요한 검토 의견을 <표 2-27과 같이 정리할 수 있고, 검토 의견 중 SW 안전 분류의 위험 심각도, SW 안전 제어 등급에 대한 의견은 전반적으로 반영하여 SW 안전 분류 초안을 보완하고 원자력과 같이 오래전부터 안전을 고려해오던 분야의 안전 표준과의 관계성을 확인하는 것과 같은 상당한 노력이 많이 요구되는 의견들은 현재 진행하기에 매우 큰 제약이 되므로 추후 연구할 내용으로 관리한다.

<표 2-27> 전문가 자문단 주요 검토 의견

위험 심각도 관련 검토 의견
· 분류 별 기술된 속성 내용이 “or 관계”인지 “and 관계”인지 불분명함 · 속성값 추가 정보 제안 - Catastrophic : 완전한 미션 실패, 시스템 보안 및 안전 손상, 대규모의 재정적/사회적 손실 - Critical : 주요 재정적/사회적 손실 - Major : 심각한 부상 또는 질병, 2차 업무의 악화, 재정적/사회적 손실 - Minor : 일시적인 기능 상실 - Negligible : 시스템 성능에 약간의 영향, 운영진의 불편함 · 분류명을 Catastrophic, Critical, Serious, Tolerable, negligible로 표현하는 것을 고려 필요
SW 안전 통제 등급 관련 검토 의견
· 철도 분야의 안전표준과 비교 분석하여 관계성 확인 필요 · MIL-STD-882E의 Software control categories의 중요한 구분척도가 “위험감지 및 위험방지 제어기능의 유무” 이므로 이를 해당 척도로 포함하는 것에 대해 검토 필요
SW 안전 분류 자체 검토 의견
· 추후 HARA에 대한 내용을 포함하여 SSRI를 어떻게 도출할 것인지에 대한 내용이 포함되어야 함 · Safety effort 용어의 정의를 “SW의 안전성(레벨)을 향상시킬 수 있도록 투입되는 노력의 수준임” 으로 수정검토 필요 · SSRI의 각 수준과 기타 기준(타 표준)과의 구체적인 대응 관계가 있으면 더욱 도움이 될 것으로 판단됨

상기 검토 의견 중, 위험 심각도와 SW 안전 통제 등급과 관련한 검토 의견을 반영하여 SW 안전 분류의 보완을 수행하였다. 위험 심각도 정의와 SW 안전

통제 등급의 정의는 <표 2-28>과 <표 2-29> 같이 개선하였다.

<표 2-28> SW 안전 통제 등급 정의 보완

SW 안전 통제 등급	설 명
NSC (No safety control)	· [추가] 위험감지 기능 보유 (X) · 안전 관련 정보 제공 (X) · [추가] 위험방지 제어 기능 보유 (X) · 안전 기능 제어 주체 (N/A*)
Aid	· [추가] 위험감지 기능 보유 (O) · 안전 관련 정보 제공 (O) · [추가] 위험방지 제어 기능 보유 (X) · 안전 기능 제어 주체 (N/A*)
Semi autonomy	· [추가] 위험감지 기능 보유 (O) · 안전 관련 정보 제공 (O) · [추가] 위험방지 제어 기능 보유 (O) · 안전 기능 제어 주체 (Operator/SW)
Full autonomy	· [추가] 위험감지 기능 보유 (O) · 안전 관련 정보 제공 (X) · [추가] 위험방지 제어 기능 보유 (O) · 안전 기능 제어 주체 (SW)

* 위험방지 제어 기능을 보유하지 않았기 때문에 안전 기능 제어 주체가 없음

<표 2-29>의 Catastrophic, Critical, Serious에 추가된 대규모/중규모/소규모의 재정적/사회적 손실에서 규모의 경우는 산업 분야, 사용 기관/기업에 따라 각기 다른 기준을 가지고 있기 때문에 대규모/중규모/소규모에 대해 구체적인 수치를 제시하지는 않고 구분만 하여 기준을 제공한다. SW 안전 분류를 활용 시 사용하는 기업 및 기관에서 사용하고 있는 재정 피해 규모의 기준을 반영하여 활용하면 된다. 규모에 대한 기준이 없는 경우 참조할 수 있는 기준으로 대규모는 100억 원을 초과하는 재정 피해, 중규모는 10억 ~ 100억 원의 재정 피해, 소규모는 10억 원 미만의 재정 피해를 기준으로 활용한다.

〈표 2-29〉 위험 심각도 정의 보완

위험 심각도	설 명
Catastrophic	· 한 명 또는 다수의 인원이 사망 · 시스템 유실 · [추가] 대규모 재정 손실
Critical	· 생명에 위협을 줄 수 있는 정도의 상해 · 주요 시스템 손상 · [추가] 중규모 재정 손실
[변경] Serious	· 병원을 찾아 전문적인 치료를 받아야 하는 부상 · 부가 시스템 손상 · [추가] 소규모 재정 손실
[변경] Tolerable	· 간단한 응급처치로 회복할 수 있는 부상 · [추가] 일시적인 시스템 기능 상실
Negligible	· 일부 시스템 부하 발생 · [추가] 사용자가 불편함을 느낌

* [추가] 속성 값은 모두 OR 관계를 가짐

제4절 SW 안전 분류 도출 및 검증

SW 중심의 안전 분류 연구 분석과 SW 안전 분류 모델 선정, SW 안전 분류 모델 개선, 전문가 자문단의 검토를 통해 도출된 SW 안전 분류를 소개하고 신규 및 기존 SW 안전 분야의 예시(例示) 시스템을 대상으로 SW 안전 분류를 적용하여 정당성 검증을 수행한 결과를 설명한다.

1. SW 안전 분류 도출

SW 중심의 안전 분류 연구 분석과 다양한 분야에서 활용되고 있는 위험 심각도 및 SW 안전 통제 등급의 개념을 분석하여 SW 안전 분류 초안을 만들었다. 이를 기반으로 전문가 자문단의 검토를 통해 유효성 및 적절성을 확인 할 수 있었다. 현재까지 진행한 모든 연구 내용을 종합하여 〈표 2-30〉과 같은 SW 안전 분류를 도출한다.

〈표 2-30〉 SW 안전 분류

위험 심각도 Severity SW 안전 통제 등급 SW safety control level	재앙적 Catastrophic	치명적 Critical	심각한 Serious	견딜만한 Tolerable	경미한 Negligible
완전자율 Full autonomy	SSRI 1	SSRI 1	SSRI 3	SSRI 4	SSRI 5
반(半)자율 Semi autonomy	SSRI 1	SSRI 2	SSRI 3	SSRI 4	SSRI 5
지원 Aid	SSRI 2	SSRI 2	SSRI 3	SSRI 4	SSRI 5
안전 제어 없음 No Safety Control	SSRI 5	SSRI 5	SSRI 5	SSRI 5	SSRI 5

도출된 SW 안전 분류는 SW 특성을 고려하여 SW 기능으로부터 야기될 수 있는 위험의 심각도와 SW가 안전 기능을 얼마만큼 자율성을 가지고 제어하는지를 판단하여 SW 안전 위험 색인을 결정하는 구조를 갖는다. 각축에 해당하는 위험 심각도와 SW 안전 통제 등급은 〈표 2-31〉과 〈표 2-32〉 같이 정의한다.

SW 안전 분류의 위험 심각도와 SW 안전 통제 등급은 MIL-STD-882E에서 제시한 안전 분류 모델과 다르게 특정 분야에 한정하지 않았다. 다양한 산업 분야에서 안전한 SW를 개발할 때 활용될 수 있도록 항공, 의료, 자동차, 국방 분야에서 주요하게 활용되고 연구들을 비교 분석하여 새롭게 구분 및 정의하였다. 더불어 SW 안전 분류를 통해 도출되는 분류 값 또한 SW안전위험색인이라는 용어로 새로 정의하고 SW안전위험색인에 따라 권고하는 안전 활동 및 적용 기법을 정의한다.

〈표 2-31〉 SW 안전 분류의 SW 안전 통제 등급 정의

SW 안전 통제 등급	설 명
안전 제어 없음 NSC(No safety control)	· 위험감지 기능 보유 (無) · 안전 관련 정보 제공 (無) · 위험방지 제어 기능 보유 (無) · 안전 기능 제어 주체 (해당 없음)
지원 Aid	· 위험감지 기능 보유 (有) · 안전 관련 정보 제공 (有) · 위험방지 제어 기능 보유 (無) · 안전 기능 제어 주체 (해당 없음)
반자율 Semi autonomy	· 위험감지 기능 보유 (有) · 안전 관련 정보 제공 (有) · 위험방지 제어 기능 보유 (有) · 안전 기능 제어 주체 (Operator/SW)
완전자율 Full autonomy	· 위험감지 기능 보유 (有) · 안전 관련 정보 제공 (無) · 위험방지 제어 기능 보유 (有) · 안전 기능 제어 주체 (SW)

〈표 2-32〉 SW 안전 분류의 위험 심각도 정의

위험 심각도	설 명
재앙적 Catastrophic	· 한 명 또는 다수의 인원이 사망 · 시스템 유실 · 대규모 재정 손실
치명적 Critical	· 생명에 위협을 줄 수 있는 정도의 상해 · 주요 시스템 손상 · 중규모 재정 손실
심각한 Serious	· 병원을 찾아 전문적인 치료를 받아야 하는 부상 · 부가 시스템 손상 · 소규모 재정 손실
견딜만한 Tolerable	· 간단한 응급처치로 회복할 수 있는 부상 · 일시적인 시스템 기능 상실
경미한 Negligible	· 일부 시스템 부하 발생 · 사용자가 불편함을 느낌

* 속성 값은 모두 OR 관계를 가짐

SW 안전 분류를 통해 결정된 SW안전위험색인은 〈표 2-33〉와 같이 정의하며, 해당 수준에 따라 권고하는 안전 활동 및 기법이 차이를 가진다. 한 가지 특

이사항으로 SW 안전 분류를 통해 권고하는 안전 관련 활동들은 IEC 12207에서 요구하는 SW 개발 및 관리의 기본적인 활동들이 기본적으로 수행하고 있다는 가정하에 안전에 특화된 활동들만 권고한다. 안전 관련 활동과 관련하여 세부 활동 및 기법에 대해서는 추후 SW 안전 공통기준에서 다룬다.

<표 2-33> SW안전위험색인(SSRI)

SW안전위험색인	설 명
SSRI 1	△SW가 보유하고 있는 위험방지 제어 기능에 대해 반(半)자율 이상의 자율성을 가지고 재앙적(catastrophic) 수준의 위험을 제어하거나 △완전자율 수준의 자율성을 가지고 치명적(critical) 수준의 위험을 제어함
SSRI 2	△SW가 보유하고 있는 위험방지 제어 기능에 대해 지원 수준의 자율성을 가지고 재앙적(catastrophic) 수준의 위험을 제어하거나 △지원 및 반(半)자율 수준의 자율성을 가지고 치명적(critical) 수준의 위험을 제어함
SSRI 3	△SW가 보유하고 있는 위험방지 제어 기능에 대해 자율성 가지며 심각한(serious) 수준의 위험을 제어함
SSRI 4	△SW가 보유하고 있는 위험방지 제어 기능에 대해 자율성 가지며 견딜 만한(tolerable) 수준의 위험을 제어함
SSRI 5	△SW가 위험방지 제어 기능을 보유하지 않거나 △경미한(negligible) 수준의 위험을 제어함

2. SW 안전 분류 정당성 검증

SW 안전 분류를 대상으로 기존 SW 안전 분야에 해당하는 시스템과 신규 SW 안전 분야에 해당하는 시스템을 각각 선정하여 SW 안전 분류를 적용해 봄으로써 도출된 SW 안전 분류의 정당성을 확인한다.

가. 기존 SW 안전 분야 검증

1) 검증 대상 시스템 선정

최근 제4차 산업혁명과 더불어 부상하고 있는 영역 중 하나는 자율주행차이다. 차량이 자율주행을 하기 위해 다수의 자동화 또는 운행을 지원하는 시스템

이 필요하다. 그중 자율주행차의 기초기술이 되는 자동긴급제동장치(AEB, Autonomous Emergency Braking)를 기존 SW 안전 분야 검증의 대상으로 선정하였다.

2) 시스템 설명

자동긴급제동장치는 차량이 주행 중에, 전방의 차량 또는 보행자와 충돌이 발생할 수 있는 상황에서 능동적인 브레이크 작동을 수행하여 피해를 경감시키는 안전 시스템이다.

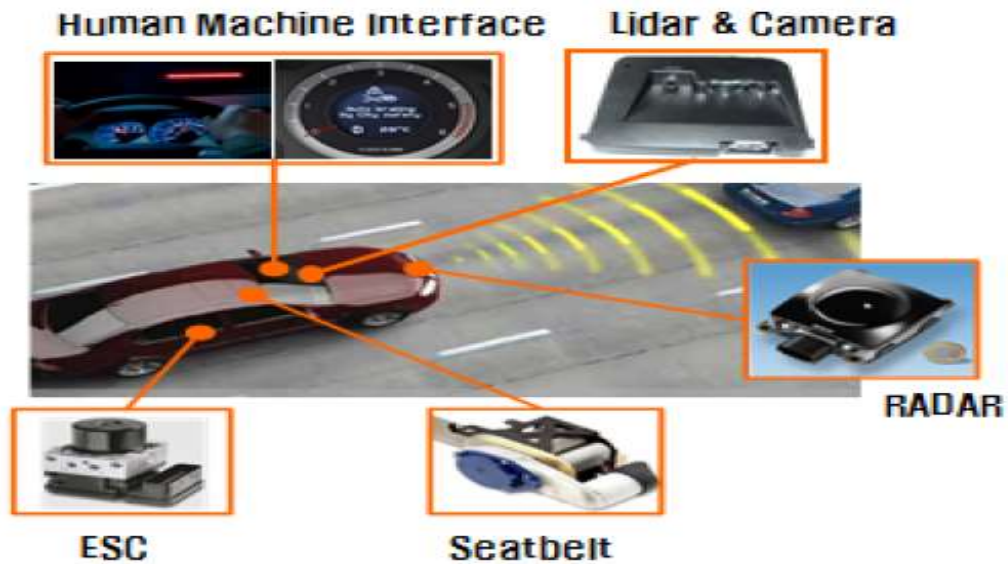
자동긴급제동장치는 기능에 따라 도심 AEB, 교외 AEB, 보행자 AEB 등 3가지로 구분한다. 도심 AEB는 차속이 50km/h보다 낮은 상태에서 60m 이내의 거리를 기준으로 차량을 식별하여 충돌 위험시 긴급제동을 수행하는 시스템이다. 교외 AEB는 차속이 200km/h보다 낮은 상태에서 200m 이내의 거리를 기준으로 차량을 식별하여 충돌 위험 시 긴급제동을 수행한다. 도심 AEB와 교외 AEB는 차량을 대상으로만 검지(檢知)하는 특징을 갖는다.

본 검증에서 사용하는 시스템은 보행자를 검지하여 충돌 직전 자동제동을 하는 보행자 AEB에 해당한다. 보행자 AEB 시스템은 차량을 감지하는 도심 AEB 시스템이나 교외 AEB 시스템과는 다르게 주요 검지 대상이 차량이 아닌 사람을 검지하는 특징이 있다. 차속과 관계없이 40m 이내의 거리를 기준으로 충돌 위험을 판단하여 긴급제동을 수행한다.

보행자 AEB 시스템은 [그림 2-17]과 같이 전방 검지를 위한 카메라 및 레이더, 급제동 수행을 위한 전자식 주행안정 장치(ESC), 급제동 시 운전자의 안전을 확보하기 위한 안전벨트, 전방 위험 상황에 대한 경고를 수행하는 인간-기계 인터페이스(HMI)³¹⁾ 장치로 구성된다.

31) Human-Machine Interface

[그림 2-17] 보행자 AEB 시스템 구성도



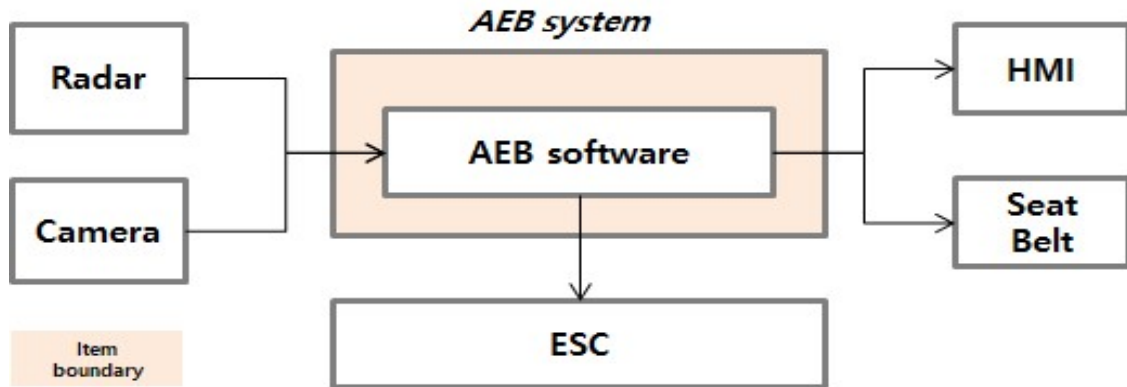
출처 : 이혁기 외, “보행자 AEBS” 의 기능안전 컨셉 분석, 한국자동차공학회, 2014.05

보행자 AEB 시스템이 가질 수 있는 기능은 <표 2-34>과 같이 정의될 수 있다. 보행자 AEB 시스템을 구성하는 요소들 사이의 관계를 도식화하여 [그림 2-18]와 같은 예비 아키텍처는 그릴 수 있다. 예비 아키텍처란 시스템 개발에 들어가기에 앞서 개발하고자 하는 아이템의 개념을 이해하기 위해 그리는 블록도로 개발 대상 아이টে을 중심으로 관계가 있는 외부 요소와 아이টে을 구성하기 위해 필요한 요소들을 표현하는 특징이 존재한다.

<표 2-34> 보행자 AEB 시스템 기능 정의

번호	기능 정의
1	전방 횡단 보행자를 감지한다.
2	충돌 가능성을 판단한다.
3	충돌 위험 시 경고를 수행한다.
4	충돌 직전 자동 급제동을 수행한다.

[그림 2-18] 보행자 AEB 시스템 예비 아키텍처



3) 위험요인 분석 및 위험 평가 수행

보행자 AEB 시스템의 정의된 기능과 구조를 기반으로 위험요인 분석 및 위험 평가(HARA, Hazard analysis and Risk assessment)를 통해 자동차 안전 무결성 수준(ASIL)을 결정한다. ISO 26262에서 요구하는 HARA는 비합리적인 위험을 방지하기 위해 대상 아이템이 오동작을 유발할 수 있는 위험요소를 식별하고 분류한다. 이로써 위험이 발생하는 것을 예방하거나 완화할 수 있는 안전 목표를 수립하는 것을 지원한다. [그림 2-20]과 같이 주어진 보행자 AEB 시스템은 기능 오작동으로 인해 주행 중에 의도하지 않은 제동 발생으로 후방에 위치한 차량과 충돌할 수 있는 위험이 존재한다. 해당 위험은 정상 노면에서 흔히 일어날 수 있으며(E4) 차량이 중속 이상으로 주행하다 급작스러운 브레이크 작동으로 후방 차량과 충돌하면 운전자는 중상을 입을 수(S2) 있다. 또한 사고 당시 브레이크 작동으로 인해 차량의 진행 방향을 조정하는 것이 불가(C3)하다. 이러한 분석을 바탕으로 보행자 AEB는 ASIL C로 자동차 안전 무결성 수준이 결정된다.

[그림 2-19] 보행자 AEB 시스템 HARA 수행 결과

Hazard	Operational Situations	Possible Accident	E	Rationale (E)	S	Rationale (S)	C	Rationale (C)	ASIL	Safety Goal
주행 중 의도하지 않은 제동으로 후방 차량과 충돌 가능	30km/h 이상 속력; 정상 노면;	후방 차량과 충돌	4	- 정상 노면에서 일반적으로 일어나는 상황	2	- 중속 이상 주행 상황에서 후방 차량과 충돌 시 운전자 증상 발생	3	- 중속 이상 주행 중 brake 체결로 인해 차량 제어가 안됨	C	주행 중 의도하지 않은 AEB 기능 작동 방지
주행 중 의도하지 않은 제동으로 후방 차량과 충돌 가능	30km/h 이상 속력; 빙결 노면;	후방 차량과 충돌	2	- 얼은 도로는 1년에 몇번 발생하는 상황	2	- 중속 이상 주행 상황에서 후방 차량과 충돌 시 운전자 증상 발생	3	- 중속 이상 주행 중 brake 체결로 인해 차량 제어가 안됨	A	주행 중 의도하지 않은 AEB 기능 작동 방지

4) SW 안전 분류 적용

① 위험 심각도 결정

기존의 위험요인 분석 및 위험 평가(HARA)와 비교를 명확하게 할 수 있도록 가능한 유사한 값으로 이용하여 SW 안전 분류가 수행할 수 있도록 했다. 즉, HARA에서 사용했던 [그림 2-19]의 심각도(S)³²⁾와 동일한 값을 이용하여 SW 안전 분류에 적용하였다.

중속 이상으로 차량이 주행하는 상황에서 의도하지 않은 브레이크 체결로 후방 차량과 충돌 할 수 있는 위험에 대해, 위험 발생 시 운전자에게 중상 이상의 피해가 발생할 수 있고, 또한 후방 차량도 중속 이상일 가능성이 높기 때문에 충돌 시 차량이 크게 파손될 가능성이 있음을 예측할 수 있다. 이러한 위험에 대해 야기되는 피해 규모를 SW 안전 분류의 위험 심각도에 기준으로 분석하면 <표 2-35>와 같이 위험 심각도가 Critical로 결정된다.

32) Severity

〈표 2-35〉 SW 안전 분류의 위험 심각도 결정

위험 심각도	설 명
재앙적 Catastrophic	· 한 명 또는 다수의 인원이 사망 · 시스템 유실 · 대규모 재정 손실
치명적 Critical	· 생명에 위협을 줄 수 있는 정도의 상해 · 주요 시스템 손상 · 중규모 재정 손실
심각한 Serious	· 병원에 내방하여 전문적인 치료를 받아야 하는 부상 · 부가 시스템 손상 · 소규모 재정 손실
견딜만한 Tolerable	· 간단한 응급처치로 회복할 수 있는 부상 · 일시적인 시스템 기능 상실
경미한 Negligible	· 일부 시스템 부하 발생 · 사용자가 불편함을 느낌
※ 속성 값은 모두 OR 관계를 가짐	

② SW 안전 통제 등급 결정

보행자 AEB 시스템에 포함될 SW가 가져야 하는 기능을 살펴보면, 전방 횡단 보행자를 대상으로 감지하고 충돌 가능성을 판단하여 운전자에게 충돌 위험 시 경고 메시지를 전달하고 충돌 직전 제동 명령을 내보낸다. 즉, 위험 상황에 대해 운전자에게 안전 정보를 제공하고 위험방지 제어 기능을 통해 브레이크를 체결하며 위험을 피하고자 운전자의 개입이 가능한 상황을 제공한다. 이러한 내용을 고려하여 〈표 2-36〉와 같이 SW 안전 분류에서 제공하고 있는 SW 안전 통제 등급에 연결하면 Semi autonomy로 결정된다.

〈표 2-36〉 SW 안전 분류의 SW 안전 통제 등급 결정

SW 안전 통제 등급	설 명
안전 제어 없음 NSC(No safety control)	· 위험감지 기능 보유 (X) · 안전 관련 정보 제공 (X) · 위험방지 제어 기능 보유 (X) · 안전 기능 제어 주체 (N/A)
지원 Aid	· 위험감지 기능 보유 (O) · 안전 관련 정보 제공 (O) · 위험방지 제어 기능 보유 (X) · 안전 기능 제어 주체 (N/A)
반자율 Semi autonomy	· 위험감지 기능 보유 (O) · 안전 관련 정보 제공 (O) · 위험방지 제어 기능 보유 (O) · 안전 기능 제어 주체 (Operator/SW)
완전자율 Full autonomy	· 위험감지 기능 보유 (O) · 안전 관련 정보 제공 (X) · 위험방지 제어 기능 보유 (O) · 안전 기능 제어 주체 (SW)

5) SW 안전 분류 결과 도출 및 결과 고찰

위험 심각도 및 SW 안전 통제 등급을 결정하여 [그림 2-20]과 같이 SSRI 1로 결과가 도출되었다.

[그림 2-20] 보행자 AEB 시스템의 SW 안전 분류 수행 결과

Severity SW safety control level	Catastrophic	Critical	Serious	Tolerable	Negligible
Full autonomy	SSRI 1	SSRI 1	SSRI 3	SSRI 4	SSRI 5
Semi autonomy	SSRI 1	SSRI 2	SSRI 3	SSRI 4	SSRI 5
Aid	SSRI 2	SSRI 2	SSRI 3	SSRI 4	SSRI 5
NSC No Safety Control	SSRI 5	SSRI 5	SSRI 5	SSRI 5	SSRI 5

이를 기반으로 기존에 사용했던 위험요인 분석 및 위험 평가 결과와 비교하면 다음의 고찰 결과를 얻을 수 있다.

- ① ASIL C는 ISO 26262에서 제시하고 있는 안전 무결성 수준 중에 두 번째에 위치하고 있을 정도로 높은 수준을 의미한다. 즉, SW 개발 전반에 걸쳐 안전을 고려할 수 있도록 강도 높은 안전 활동 요건 및 기법을 제시하고 있다.
- ② SW 안전 분류는 SW 측면으로만 안전 분류를 수행할 수 있도록 ISO 26262에서 사용하는 위험 발생도와 통제도를 배제하고 그동안 고려하지 않았던 SW 안전 통제 등급을 이용하여 차별성 확보 후 안전 분류를 수행한 결과 <표 2-37>과 같이 ASIL C와 유사하게 높은 수준의 SSRI 2로 결정되었다. 이를 통해 SW 개발 시, 보행자 AEB 시스템 수준에서 할당된 안전 분류 수준과 기초가 유사하게 많은 안전

노력을 투입할 수 있도록 지원하는 것을 확인하였다.

<표 2-37> 기존 SW 안전분야 예제 시스템 대상 SW 안전 분류 수행 결과

SW 안전 위험 색인	설 명
SSRI 1	SW가 보유하고 있는 위험방지 제어 기능에 대해 반자율 이상의 자율성을 가지고 Catastrophic 위험을 제어하거나 보유하고 있는 위험방지 제어 기능에 대해 완전자율 이상의 자율성을 가지고 Critical 수준의 위험을 제어함
SSRI 2	SW가 보유하고 있는 위험방지 제어 기능에 대해 지원 수준의 자율성을 가지고 Catastrophic 위험을 제어하거나 보유하고 있는 위험방지 제어 기능에 대해 지원 및 반자율 수준의 자율성을 가지고 Critical 수준의 위험을 제어함
SSRI 3	SW가 보유하고 있는 위험방지 제어 기능에 대해 일부 자율성 가지며 Serious 수준의 위험을 제어함
SSRI 4	SW가 보유하고 있는 위험방지 제어 기능에 대해 일부 자율성 가지며 Tolerable 수준의 위험을 제어함
SSRI 5	SW가 위험방지 제어 기능을 보유하지 않거나 Negligible 수준의 위험을 제어함

나. 신규 SW 안전 분야 검증

1) 검증 대상 시스템 선정

해마다 지하철 플랫폼 스크린 도어(PSD)³³⁾와 관련하여 사건·사고가 끊이지 않고 있다.³⁴⁾ 앞서 설명한 것과 같이 플랫폼 스크린 도어는 현재 안전기준이 마련되지 않아 안전에 대해 고려가 미비한 상황이다. 철도 분야의 안전기준은 크게 철도차량, 철도시설, 철도용품으로 구분하여 철도차량 기술기준³⁵⁾, 철도시설 기술기준³⁶⁾, 철도용품 기술기준³⁷⁾을 통해 안전 관련 기준을 관리하고 있다. 하지

33) Platform Screen Door

34) 민경욱 “3년간 서울지하철 사고 1574건…끼임 사고 최다“, News1, 2018.09.09

35) 철도차량 기술기준, 국토교통부

36) 철도시설 기술기준, 국토교통부

37) 철도용품 기술기준, 국토교통부

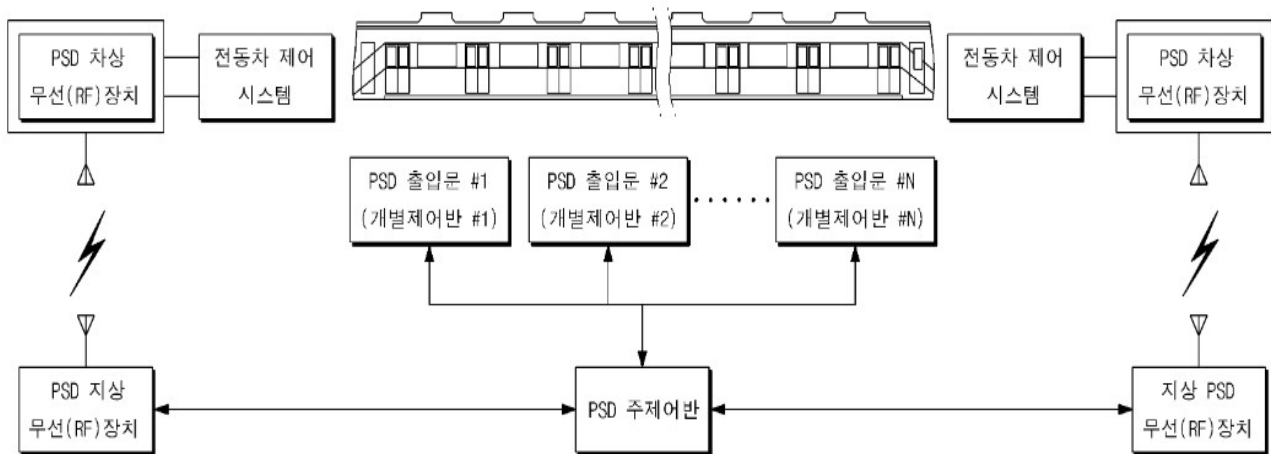
만 이 세 가지 기준 어느 곳에도 지하철 플랫폼 스크린 도어 자체에 대한 안전 기준이 존재하지 않는다.

플랫폼 스크린 도어는 지하철과 연동하여 시스템을 제어하는 특성이 존재하기 때문에 기존에는 SW 측면으로 안전성을 고려하지 않았으나, 추후에는 SW 측면으로 안전성을 고려하도록 요구될 수 있다. 이러한 상황을 고려하여 신규 SW 안전 분야 검증 대상 시스템은 전동차 출입문과 지상 스크린도어의 동시 개폐 제어 시스템³⁸⁾으로 선정했다.

2) 시스템 설명

전동차 출입문과 지상 스크린도어의 동시 개폐 제어 시스템은 [그림 2-21]와 같이 전동차 출입문과 지상 PSD와 무선통신하여 전동차 출입문의 개폐에 따라 지상 PSD도 개폐되도록 제어하는 시스템이다.

[그림 2-21] 차상 PSD 무선장치와 지상 PSD 무선장치의 연동방식을 나타낸 구성도



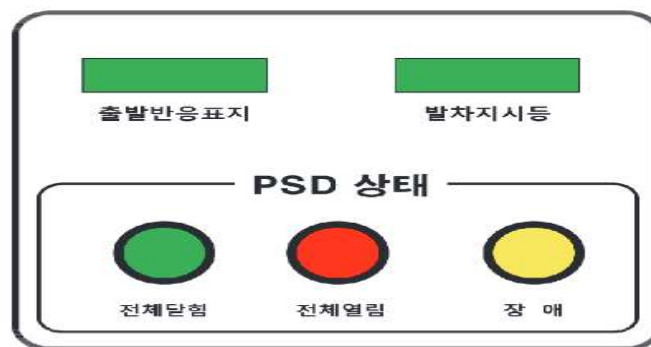
출처 : 등록특허, “전동차 출입문과 지상 스크린도어의 동시 개폐 장치”, 서울메트로, 2012.08.07

38) 등록특허, “전동차 출입문과 지상 스크린도어의 동시 개폐 장치”, 서울메트로, 2012.08.07

지하철 출입문과 승강장에 설치된 스크린 도어는 각각 독립된 시스템이며 동시에 작동해야 한다는 특징을 갖는다. 지하철이 승강장에 위치하고 출입문을 개폐하면서 승강장에 설치된 스크린 도어 또한 함께 개폐되어야 하는 기능이 필요하다. 본 예제 시스템이 무선 장치를 통해 전동차 제어 시스템과 플랫폼 스크린 주제어반을 연동하여 해당 기능을 수행한다. 본 예제 시스템은 지하철과 같이 SW 안전을 고려하고 있는 시스템과 플랫폼 스크린 도어와 같이 SW 안전을 아직 고려하지 않는 시스템이 통합된 시스템으로 기존 시스템 간의 통합을 통해 SW 안전을 고려해야 하는 신규 분야가 된다.

전동차 출입문과 지상 스크린도어의 동시 개폐 제어 시스템은 전동차 출입문 및 지상 PSD를 개폐하는 기능을 가지고 있다. [그림 2-22]과 같이 전동차의 출입문과 PSD의 출입문의 개폐상태, 정위치 차이와 같은 장애 상황을 경고하는 기능을 갖는다.

[그림 2-22] 승무원 조작반



출처 : 류경신, “출입문 검지 센서(Sensor)방식 승강장 안전문(PSD) 안전운용에 관한 연구” , 한국철도학회, 2014

3) SW 안전 분류 적용

① 위험 심각도 결정

지상 PSD와 지하철 출입문의 무선연동 기능이 작동하지 않거나 오작동하여 승객이 선로로 낙상할 수 있고 심한 경우 출입문에 끼인 상태로 전동차가 출발하게 될 수 있다. 이때 승객은 중상 이상의 피해를 당할 가능성이 존재한다. 이러한 위험 발생으로 야기되는 피해 규모를 <표 2-38>과 같이 SW 안전 분류에서 제공하고 있는 위험 심각도 수준에 연결하면 Catastrophic으로 결정된다.

<표 2-38> SW 안전 분류의 위험 심각도 결정

위험 심각도	설 명
재앙적 Catastrophic	· 한 명 또는 다수의 인원이 사망 · 시스템 유실 · 대규모 재정 손실
치명적 Critical	· 생명에 위협을 줄 수 있는 정도의 상해 · 주요 시스템 손상 · 중규모 재정 손실
심각한 Serious	· 병원을 찾아 전문적인 치료를 받아야 하는 부상 · 부가 시스템 손상 · 소규모 재정 손실
견딜만한 Tolerable	· 간단한 응급처치로 회복할 수 있는 부상 · 일시적인 시스템 기능 상실
경미한 Negligible	· 일부 시스템 부하 발생 · 사용자가 불편함을 느낌

* 속성 값은 모두 OR 관계를 가짐

② SW 안전 통제 등급 결정

전동차 출입문과 지상 스크린도어의 동시 개폐 제어 시스템은 발차 지시와 PSD의 개폐 상태 및 장애 상태를 승무원에게 알리는 기능을 가지고 있으나, 위험방지를 위한 제어 기능을 보유하고 있지는 않다. 이러한 특징을 반영하여 <표 2-39>과 같이 SW 안전 분류에서 제공하고 있는 SW 안전 통제 등급에 연결하면 Aid로 결정된다.

<표 2-39> SW 안전 분류의 SW 안전 통제 등급 결정

SW 안전 통제 등급	설 명
안전 제어 없음 NSC(No safety control)	· 위험감지 기능 보유 (X) · 안전 관련 정보 제공 (X) · 위험방지 제어 기능 보유 (X) · 안전 기능 제어 주체 (N/A)
지원 Aid	· 위험감지 기능 보유 (O) · 안전 관련 정보 제공 (O) · 위험방지 제어 기능 보유 (X) · 안전 기능 제어 주체 (N/A)
반자율 Semi autonomy	· 위험감지 기능 보유 (O) · 안전 관련 정보 제공 (O) · 위험방지 제어 기능 보유 (O) · 안전 기능 제어 주체 (Operator/SW)
완전자율 Full autonomy	· 위험감지 기능 보유 (O) · 안전 관련 정보 제공 (X) · 위험방지 제어 기능 보유 (O) · 안전 기능 제어 주체 (SW)

4) SW 안전 분류 결과 도출 및 결과 고찰

위험 심각도 및 SW 안전 통제 등급을 결정하여 [그림 2-23]와 같이 SSRI 2로 결과가 도출되었다.

[그림 2-23] 전동차 출입문과 지상 스크린도어의 동시 개폐 제어 시스템의 SW 안전 분류 수행 결과

Severity SW safety control level	Catastrophic	Critical	Serious	Tolerable	Negligible
Full autonomy	SSRI 1	SSRI 1	SSRI 3	SSRI 4	SSRI 5
Semi autonomy	SSRI 1	SSRI 2	SSRI 3	SSRI 4	SSRI 5
Aid	SSRI 2	SSRI 2	SSRI 3	SSRI 4	SSRI 5
NSC No Safety Control	SSRI 5	SSRI 5	SSRI 5	SSRI 5	SSRI 5

신규 SW 안전 분야 대상으로 SW 안전 분류를 적용하여 다음의 고찰 결과를 얻을 수 있다.

- ① 기존에 SW 안전과 관련하여 국내에서 고려되지 않았던 분야를 대상으로 SW 안전 분류를 적용하여 SW안전위험색인을 도출하였다.
- ② 전동차 출입문과 지상 스크린도어의 동시 개폐 제어 시스템의 경우 다수의 인원이 사용하며 위험 발생 시 큰 인명 피해가 발생하는 점을 미루어 봤을 때, <표 2-40>와 같이 SSRI 2와 같이 적절한 수준으로 SW안전위험색인이 결정된 것으로 판단된다.

<표 2-40> 신규 SW 안전분야 예제 시스템 대상 SW 안전 분류 수행 결과

SW 안전 위험 색인	설 명
SSRI 1	SW가 보유하고 있는 위험방지 제어 기능에 대해 반자율 이상의 자율성을 가지고 Catastrophic 위험을 제어하거나 보유하고 있는 위험방지 제어 기능에 대해 완전자율 이상의 자율성을 가지고 Critical 수준의 위험을 제어함
SSRI 2	SW가 보유하고 있는 위험방지 제어 기능에 대해 지원 수준의 자율성을 가지고 Catastrophic 위험을 제어하거나 보유하고 있는 위험방지 제어 기능에 대해 지원 및 반자율 수준의 자율성을 가지고 Critical 수준의 위험을 제어함
SSRI 3	SW가 보유하고 있는 위험방지 제어 기능에 대해 일부 자율성 가지며 Serious 수준의 위험을 제어함
SSRI 4	SW가 보유하고 있는 위험방지 제어 기능에 대해 일부 자율성 가지며 Tolerable 수준의 위험을 제어함
SSRI 5	SW가 위험방지 제어 기능을 보유하지 않거나 Negligible 수준의 위험을 제어함

제3장 SW 안전 공통기준 도출 연구

본 장에서는 SW 안전 공통기준을 도출하기 위해 관련 연구를 조사·분석한 결과를 설명하고 이를 정리하여 SW 안전 공통기준을 제시한다.

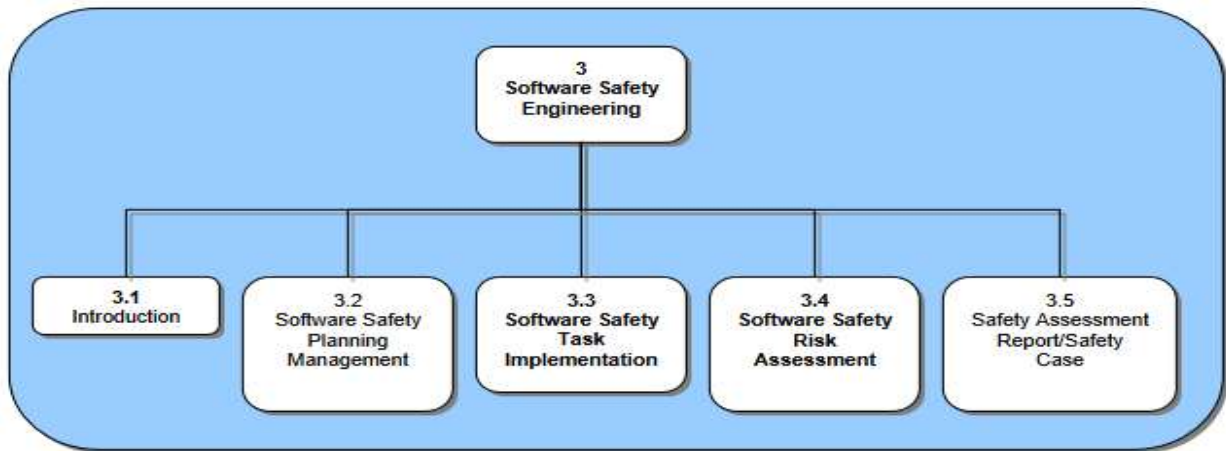
제1절 SW 안전 공통기준 관련 연구 분석

SW 안전 분류를 도출하기 위해 활용한 MIL-STD-882E와 NASA Software Safety Guidebook을 기준으로 SW 안전 공통기준을 도출할 수 있도록 연구를 수행하였다. MIL-STD-882E의 경우, SW 안전 공통기준을 도출하기 위한 자료가 별도로 존재하여 이를 기반으로 분석을 수행하였다.

1. MIL-STD-882E 관련 가이드

SW 안전 분류를 도출하기 위해 중심으로 활용한 MIL-STD-882E를 실제로 활용하기 위한 별도의 가이드가 존재한다. 해당 가이드는 군수 관련 연산 시스템의 SW 안전 설계 및 평가 지침(Guidance on software safety design and assessment of munition-related computing systems)이다. 이는 북대서양 조약 기구(NATO)에서 안전을 고려한 SW 시스템 개발 가이드로 활용되도록 제정되었다.

[그림 3-1] SW 안전 공학 세부 내용



출처 : Guidance on software safety design and assessment of munition-related computing systems, NATO, 2008.12.09.

본 가이드는 [그림 3-1]과 같은 구조로 SW 안전 공학에 대해 상세하게 설명하고 있다. MIL-STD-882E에서 SW 안전 중요도 매트릭스 기반의 안전 분류를 고려하여 각 SW 위험 색인 별 적용해야 하는 활동을 제시하고 있다. [그림 3-2]와 같이 SW 개발단계를 설계, 구현, 단위 검증, 통합 단위 검증, 시스템 통합 검증으로 구분하고 있으며 단계별로 적용할 수 있는 안전 활동을 소개한다.

[그림 3-2] SW 위험 색인 수준 별 개발 단계 권고 사항

PHASE SSCI	DESIGN	CODE	UNIT TEST	INTEGRATING UNIT TEST	SYSTEM INTEGRATION
1 High Risk	• Design Team Review • Safety Review • SCF Linked to SW Rqmts • SCF Linked to Design Architecture • Safety Fault Tolerant Design	• Design Code Walkthrough • Independent Code Review • Safety Code Analysis • SCF Code Review • Safety Fault Detection, Fault Tolerance	• Test Case Review • Independent Test Review • Failure Mode Effect Testing • Safety Test Result Review	• Test Case Review • Independent Test Review • Failure Mode Effect Testing • 100% Regression Testing • Safety Test Result Review	• Test Case Review • Independent Test Review • Failure Mode Effect Testing • 100% Regression Testing • Safety Test Result Review
2 Serious Risk	• Design Team Review • Prioritizing Safety Review • SCF Linked to SW Rqmts • SCF Linked to Design Architecture	• Design Code Walkthrough • Safety Code Analysis for Prioritized Modules • SCF Code Review • Safety Fault Detection, Fault Tolerance	• Test Case Review • Independent Test Review • Failure Mode Effect Testing • 100% Thread Testing • Safety Test Result Review	• Test Case Review • Independent Test Review • Failure Mode Effect Testing • 100% Regression Testing • Safety Test Result Review	• Test Case Review • Independent Test Review • Failure Mode Effect Testing • 100% Regression Testing • Safety Test Result Review
3 Moderate Risk	• Design Team Review • Minimal Safety Review • SCF Linked to SW Rqmts • SCF Linked to Design Architecture	• SCF Code Review • Safety Fault Detection, Fault Tolerance	• Test Case Review • Independent Test Review • Failure Mode Effect Testing • Safety Test Result Review	• Test Case Review • Independent Test Review • Failure Mode Effect Testing • Safety Test Result Review	• Test Case Review • Independent Test Review • Failure Mode Effect Testing • Safety Test Result Review
4 Low Risk	• Design Team Review • Minimal Safety Review • Normal Software Design Process IAW SDP	No specific tasks	• Test Case Review • Independent Test Review • Safety Test Result Review	• Test Case Review • Independent Test Review • Safety Test Result Review	• Test Case Review • Independent Test Review • Safety Test Result Review
5 No Safety Risk	• Normal Software Design Activity IAW the Software Development Plan	• Normal Software Code Activity IAW the Software Development Plan	• Normal Software Unit Test Activity IAW the Software Development Plan	• Normal Software Unit Integration Test Activity IAW the Software Development Plan	• Normal Software System Integration Test Activity IAW the Software Development Plan

출처 : Guidance on software safety design and assessment of munition-related computing systems, NATO, 2008.12.09.

2. NASA Software Safety Guidebook

NASA Software Safety Guidebook은 NASA에서 SW 개발 시 안전을 고려하여 개발할 수 있도록 고안한 정규 표준으로 SW 안전 분류 도출을 위해 위험 심각도 및 SW 통제 등급 정보를 활용한 바 있다. 해당 가이드는 SW의 안전 분류에

관한 지침만 있는 것이 아니라 안전 분류에 따라 적절한 수준으로 이루어져야 하는 안전 활동에 대한 내용도 포함하고 있다. SW 개발단계를 요구사항, 설계, 구현, 검증으로 구분하고 있으며 단계별로 적용할 수 있는 일반적인 SW 개발 활동, 시스템 및 SW 안전 활동, SW 보증 활동을 [그림 3-3]과 같은 형식으로 소개한다. 특이사항으로 SW 검증에 대해 ISO/IEC 12207³⁹⁾과 같이 일반적으로 많이 사용하는 SW 단계별 검증이 아닌 통합된 검증단계로 안전 활동을 소개하고 있다.

[그림 3-3] SW 개발 단계 별 권고 활동 제공 형식

Software Engineering Tasks	System and Software Safety Tasks	Software Assurance or IV&V Tasks
Software requirements development [Sections 6.4.2 and 6.5]	Development of software safety requirements [Section 6.5]	Formal methods for verification [Sections 4.2.2.3 and 6.6.4]
Requirements management [Section 6.4]	Safety Requirements Flow-down Analysis [Section 6.6.1]	Model checking [Section 6.6.5]
Formal methods for specification [Sections 4.2.2.3 and 6.6.4]	Requirements Criticality Analysis [Section 6.6.2]	Formal inspections of software requirements [Section 6.5.5]
Formal inspections of software requirements [Section 6.5.5]	Specification Analysis of Safety-critical Requirements [Section 6.6.3]	Specification analysis [Section 6.6.3]
System test planning [Section 6.5.6]	Software Fault Tree Analysis [Section 6.6.7 and Appendix C]	Timing, throughput and sizing analysis [Section 6.6.6]
Timing, throughput and sizing considerations [Section 6.5.4]	Software Failure Modes and Effects Analysis [Section 6.6.8 and Appendix D]	
	Formal inspections of Software requirements [Section 6.5.5]	
	Develop Safety Package for Phase 0/1 Safety Review or other external safety review.	

출처 : Software Safety Guidebook, NASA, 2004.03.31.

SW 개발 단계별로 권고하고 있는 안전 활동을 모두 수행하기에 제한이 될 수 있다. 이때 결정된 안전 분류 값이 의미하는 안전 노력 수준을 <표 3-1>과 같이 확인하고 안전 노력(Safety effort)의 수준에 따라 [그림 3-4]와 같이 필수

39) ISO에서 제정한 표준으로 SW 생명주기 프로세스에 관해 설명하고 있다.

적용을 조절하여 사용할 수 있다.

<표 3-1> 요구되는 SW 안전 노력

SW 통제 등급	심각도 등급			
	재앙적 수준	치명적 수준	적당한 수준	미비한 수준
IA	Full	Full	Moderate	Minimum
IIA & IIB	Full	Moderate	Minimum	Minimum
IIIA & IIIB	Moderate	Moderate	Minimum	None
IV	Minimum	Minimum	None	None

[그림 3-4] 요구사항 단계를 위한 SW 안전 노력

Technique or Analysis	Safety Effort Level		
	MIN	MOD	FULL
2.3.1 Preliminary Hazard Analysis (PHA) (if not previously performed)	★	★	★
2.3.4 Software Subsystem Hazard Analysis (if not previously performed)	★	★	★
Software safety requirements development			
6.5.1 Generic requirements	✓	✓✓	✓✓
6.5.2 Fault and Failure Tolerance	✓	✓✓	★
6.5.3 Hazardous Commands	★	★	★
6.4 Requirements Management	★	★	★
6.5.5 Formal Inspections	✓	★	★
6.6.1 Software Safety Requirements Flow-down Analysis	✓✓	★	★
6.6.2 Requirements Criticality Analysis	✓	✓✓	★
6.6.3 Specification Analysis	⊖	✓	✓✓
4.2.2.3 and 6.6.4 Formal Methods	⊖	✓✓ (Specification)	✓✓ (Specification & Verification)
6.6.5 Model Checking	⊖	✓✓	✓✓
Timing, Throughput, and Sizing			
6.5.4 Development Considerations	✓✓	★	★
6.6.6 Analysis	✓✓	★	★
6.6.7 Software Fault Tree Analysis	✓	✓✓	★
6.6.8 Software Failure Modes and Effects Analysis	⊖	✓	✓✓

Recommendation Codes			
★	Mandatory	✓✓	Highly Recommended
✓	Recommended	⊖	Not Recommended

출처 : Software Safety Guidebook, NASA, 2004.03.31.

제2절 SW 안전 공통기준 도출

MIL-STD-882E의 적용 가이드와 NASA Software Safety Guidebook을 분석하고 이를 기반으로 SW 안전 공통기준 도출하는 과정을 설명한다.

1. 안전 활동 및 기법 선정

군수 관련 연산 시스템의 SW 안전 설계 및 평가 지침(Guidance on software safety design and assessment of munition-related computing systems)과 미 항공우주국 SW 안전 가이드(NASA Software Safety Guidebook)에서 사용하고 있는 안전 활동 및 기법을 활용하여 SW 안전 공통기준을 도출한다.

군수 관련 연산 시스템의 SW 안전 설계 및 평가 지침의 경우, SW 요구사항 개발과 관련된 안전 활동 및 기법이 별도 제공되지 않는다. 미 항공우주국 SW 안전 가이드에서는 SW 검증 단계가 하나로 통합되어 안전 활동 및 기법을 소개하고 있다. 이러한 차이를 모두 고려하고 SW 공학적인 체계성을 가질 수 있도록 SW 개발 단계를 SW 요구사항, 설계, 구현, 단위 검증, 통합 단위 검증, SW 검증으로 구성하여 SW 안전 공통기준을 도출하고자 한다.

SW 안전 공통기준을 도출하기 위해 활용한 연구를 살펴보면 안전 분류 수준별 권고하는 안전 활동의 차이가 존재하는데, 의미상 공통으로 요구하는 활동을 추출하고 더 쉽게 이해할 수 있도록 활동명을 수정하였다. 특이사항으로 미 항공우주국 SW 안전 가이드(NASA Software Safety Guidebook)에서 권고하는 활동은 일부 기법을 포함하고 있어 이를 재분석하여 안전 활동이 명확히 구분되도록 하였다.

SW 안전 공통기준은 SW 안전 분류를 통해 결정된 SW안전위험색인(SSRI)에 따라 필수적으로 권고하는 안전 활동의 차이가 존재하며, 해당 차이는 <표 3-2>와 같다. SSRI 4에서부터 SSRI 1로 SW 안전 분류 수준이 높아질수록 전반적인 SW 개발 과정에서 안전을 고려하도록 안내한다.

〈표 3-2〉 SW 안전 위험 색인 등급 별 안전 요구 활동

SW 안전 위험 색인	설 명
SSRI 1	안전 측면으로 SW 요구사항 도출 및 분석, 설계, 코드 분석, SW 단위 검증, SW 통합 검증, SW 검증을 수행해야 함
SSRI 2	안전 측면으로 SW 요구사항 도출 및 분석, 설계, SW 단위 검증, SW 통합 검증, SW 검증을 수행해야 함
SSRI 3	안전 측면으로 SW 요구사항 도출 및 분석, 설계, SW 통합 검증, SW 검증을 수행해야 함
SSRI 4	안전 측면으로 SW 요구사항 도출 및 분석, SW 검증 활동을 수행해야 함
SSRI 5	별도 안전 관련 분석 또는 검증 활동이 요구되지 않음

SW 개발 단계별 적용할 수 있는 안전 활동은 앞서 살펴본 군수 관련 연산 시스템의 SW 안전 설계 및 평가 지침(Guidance on software safety design and assessment of munition-related computing systems)과 미 항공우주국 SW 안전 가이드(NASA Software Safety Guidebook)에서 상세히 설명하고 있지만, 해당 안전 활동을 수행하면서 적용할 수 있는 기법에 대한 설명은 다소 부족하다. 이를 위해, 각 안전 활동 별로 적용할 수 있는 기법이 상세히 설명되고 있는 자동차 분야의 안전 표준⁴⁰⁾을 참조하여 SW 안전 위험 색인(SSRI)에 따라 적용할 수 있는 기법을 도출하였다.

2. SW 안전 공통기준

SW 안전 공통기준 관련 연구 분석을 통해 SW 안전 공통기준을 도출하면 〈표 3-3〉과 같이 SW 안전 공통기준을 도출할 수 있다. SW 안전 공통기준은 총 22개의 안전 활동과 17개의 기법으로 이루어져 있으며, SW안전위험색인(SSRI)에

40) ISO26262, Road vehicles -- Functional safety --

따라 필수적용 여부와 적용 시 활용할 수 있는 기법을 제시한다. SW 안전 공통 기준은 SW 개발 시, ISO/IEC 12207에서 요구하는 SW 개발 활동을 모두 수행하는 것을 가정으로 하며 안전에 관련된 활동과 기법만을 고려한다.

〈표 3-3〉 SW 안전 공통기준

단계	안전 활동	SSR1		SSR2		SSR3	
		필수 유무	적용 기법	필수 유무	적용 기법	필수 유무	적용 기법
Requirements	Development of software safety requirements	O	• Structured natural language	O	• Structured natural language	O	• Structured natural language
	Safety analysis of safety requirements	O	• Software Fault Tree analysis • Software Failure mode and effects analysis	O	• Software Fault Tree analysis • Software Failure mode and effects analysis	O	• either Software Fault Tree analysis or Software Failure mode and effects analysis
	Review of safety requirements	O	• Inspection	O	• Inspection	O	• Walkthrough
Design	Development of software safety design	O	• Hierarchical structure of software components	O	• Hierarchical structure of software components	O	• Hierarchical structure of software components
	Safety analysis of design	O	• Software Fault Tree analysis • Software Failure mode and effects analysis	O	• Software Fault Tree analysis • Software Failure mode and effects analysis	O	• either Software Fault Tree analysis or Software Failure mode and effects analysis
	Review of safety design	O	• Inspection	O	• Inspection	O	• Walkthrough
Implementation	Safety analysis of code	O	• Safety code analysis	X	N/A	X	N/A
	Review of safety code	O	• Inspection	X	N/A	X	N/A
Software unit test	Development of safety related unit test case	O	• Analysis of safety requirements • Generation and analysis of equivalence classes • Analysis of boundary values	O	• Analysis of safety requirements • Generation and analysis of equivalence classes • Analysis of boundary values	X	N/A
	Review of safety related unit test case	O	• Inspection	O	• Inspection	X	N/A
	Analysis of test coverage at software unit level	O	• Statement coverage • Branch coverage • Condition coverage	O	• Statement coverage • Branch coverage	X	N/A
	Safety related unit test	O	• Requirements based test • Fault injection test	O	• Requirements based test • Fault injection test	X	N/A
	Review of safety related unit test result	O	• Inspection	O	• Inspection	X	N/A
Software integration test	Development of safety related software integration test case	O	• Analysis of safety requirements • Generation and analysis of equivalence classes • Analysis of boundary values	O	• Analysis of safety requirements • Generation and analysis of equivalence classes • Analysis of boundary values	O	• Analysis of safety requirements
	Review of safety related software integration test case	O	• Inspection	O	• Inspection	O	• Walkthrough
	Analysis of test coverage at software architectural level	O	• Function coverage • Call coverage	O	• Function coverage • Call coverage	O	• Function coverage
	Safety related software integration test	O	• Requirements based test • Fault injection test	O	• Requirements based test • Fault injection test	O	• Requirements based test
	Review of safety related software integration test result	O	• Inspection	O	• Inspection	O	• Walkthrough
Software test	Development of safety related software test case	O	• Analysis of safety requirements • Generation and analysis of equivalence classes • Analysis of boundary values	O	• Analysis of safety requirements • Generation and analysis of equivalence classes • Analysis of boundary values	O	• Analysis of safety requirements • Generation and analysis of equivalence classes • Analysis of boundary values
	Review of safety related software test case	O	• Inspection	O	• Inspection	O	• Walkthrough
	Safety related Software test	O	• Requirements based test • Fault injection test	O	• Requirements based test • Fault injection test	O	• Requirements based test • Fault injection test
	Review of safety related software test result	O	• Inspection	O	• Inspection	O	• Walkthrough

SSRI 1은 <표 3-4>와 같이 SW 안전 분류로 도출될 수 있는 최상위 수준으로 모든 SW 개발 단계에서 안전 활동 및 안전 기법을 모두 수행하도록 명시한다.

<표 3-4> SW 안전 공통기준(SSRI 1)

단계	안전 활동	SSRI 1	
		필수 유무	적용 기법
Requirements	Development of software safety requirements	O	• Structured natural language
	Safety analysis of safety requirements	O	• Software Fault Tree analysis • Software Failure mode and effects analysis
	Review of safety requirements	O	• Inspection
Design	Development of software safety design	O	• Hierarchical structure of software components
	Safety analysis of design	O	• Software Fault Tree analysis • Software Failure mode and effects analysis
	Review of safety design	O	• Inspection
Implementation	Safety analysis of code	O	• Safety code analysis
	Review of safety code	O	• Inspection
Software unit test	Development of safety related unit test case	O	• Analysis of safety requirements • Generation and analysis of equivalence classes • Analysis of boundary values
	Review of safety related unit test case	O	• Inspection
	Analysis of test coverage at software unit level	O	• Statement coverage • Branch coverage • Condition coverage
	Safety related unit test	O	• Requirements based test • Fault injection test
	Review of safety related unit test result	O	• Inspection
Software integration test	Development of safety related software integration test case	O	• Analysis of safety requirements • Generation and analysis of equivalence classes • Analysis of boundary values
	Review of safety related software integration test case	O	• Inspection
	Analysis of test coverage at software architectural level	O	• Function coverage • Call coverage
	Safety related software integration test	O	• Requirements based test • Fault injection test
	Review of safety related software integration test result	O	• Inspection
Software test	Development of safety related software test case	O	• Analysis of safety requirements • Generation and analysis of equivalence classes • Analysis of boundary values
	Review of safety related software test case	O	• Inspection
	Safety related Software test	O	• Requirements based test • Fault injection test
	Review of safety related software test result	O	• Inspection

SSRI 2는 <표 3-5>와 같이 구현 단계를 제외한 SW 요구사항, 설계, 단계별 테스트에서 안전 활동 및 안전 기법을 모두 수행하도록 명시한다.

<표 3-5> SW 안전 공통기준(SSRI 2)

단계	안전 활동	SSRI 2	
		필수 유무	적용 기법
Requirements	Development of software safety requirements	O	• Structured natural language
	Safety analysis of safety requirements	O	• Software Fault Tree analysis • Software Failure mode and effects analysis
	Review of safety requirements	O	• Inspection
Design	Development of software safety design	O	• Hierarchical structure of software components
	Safety analysis of design	O	• Software Fault Tree analysis • Software Failure mode and effects analysis
	Review of safety design	O	• Inspection
Implementation	Safety analysis of code	X	N/A
	Review of safety code	X	N/A
Software unit test	Development of safety related unit test case	O	• Analysis of safety requirements • Generation and analysis of equivalence classes • Analysis of boundary values
	Review of safety related unit test case	O	• Inspection
	Analysis of test coverage at software unit level	O	• Statement coverage • Branch coverage
	Safety related unit test	O	• Requirements based test • Fault injection test
	Review of safety related unit test result	O	• Inspection
Software integration test	Development of safety related software integration test case	O	• Analysis of safety requirements • Generation and analysis of equivalence classes • Analysis of boundary values
	Review of safety related software integration test case	O	• Inspection
	Analysis of test coverage at software architectural level	O	• Function coverage • Call coverage
	Safety related software integration test	O	• Requirements based test • Fault injection test
	Review of safety related software integration test result	O	• Inspection
Software test	Development of safety related software test case	O	• Analysis of safety requirements • Generation and analysis of equivalence classes • Analysis of boundary values
	Review of safety related software test case	O	• Inspection
	Safety related Software test	O	• Requirements based test • Fault injection test
	Review of safety related software test result	O	• Inspection

SSRI 3은 <표 3-6>과 같이 SW 요구사항, SW 설계, SW 통합 테스트, SW 테스트 단계에서 안전 활동 및 안전 기법을 수행하도록 명시하며 안전 기능과 관련된 단계별 산출물을 검토하는 활동의 기법은 Inspection에서 모두 Walkthrough로 바뀌며, 안전 분석을 수행하는 기법은 Software Fault Tree Analysis와 Software Failure Mode Effect Analysis 중 하나를 선택하여 수행하도록 권고한다.

<표 3-6> SW 안전 공통기준(SSRI 3)

단계	안전 활동	SSRI 3	
		필수 유무	적용 기법
Requirements	Development of software safety requirements	O	• Structured natural language
	Safety analysis of safety requirements	O	• either Software Fault Tree analysis or Software Failure mode and effects analysis
	Review of safety requirements	O	• Walkthrough
Design	Development of software safety design	O	• Hierarchical structure of software components
	Safety analysis of design	O	• either Software Fault Tree analysis or Software Failure mode and effects analysis
	Review of safety design	O	• Walkthrough
Implementation	Safety analysis of code	X	N/A
	Review of safety code	X	N/A
Software unit test	Development of safety related unit test case	X	N/A
	Review of safety related unit test case	X	N/A
	Analysis of test coverage at software unit level	X	N/A
	Safety related unit test	X	N/A
	Review of safety related unit test result	X	N/A
Software integration test	Development of safety related software integration test case	O	• Analysis of safety requirements
	Review of safety related software integration test case	O	• Walkthrough
	Analysis of test coverage at software architectural level	O	• Function coverage
	Safety related software integration test	O	• Requirements based test
	Review of safety related software integration test result	O	• Walkthrough
Software test	Development of safety related software test case	O	• Analysis of safety requirements • Generation and analysis of equivalence classes • Analysis of boundary values
	Review of safety related software test case	O	• Walkthrough
	Safety related Software test	O	• Requirements based test • Fault injection test
	Review of safety related software test result	O	• Walkthrough

SSRI 4는 <표 3-7>와 같이 SW 요구사항, SW 테스트 단계에서만 안전 활동 및 안전 기법을 수행할 수 있도록 명시한다.

<표 3-7> SW 안전 공통기준(SSRI 4)

단계	안전 활동	SSRI 4	
		필수 유무	적용 기법
Requirements	Development of software safety requirements	O	• Structured natural language
	Safety analysis of safety requirements	O	• either Software Fault Tree analysis or Software Failure mode and effects analysis
	Review of safety requirements	O	• Walkthrough
Design	Development of software safety design	X	N/A
	Safety analysis of design	X	N/A
	Review of safety design	X	N/A
Implementation	Safety analysis of code	X	N/A
	Review of safety code	X	N/A
Software unit test	Development of safety related unit test case	X	N/A
	Review of safety related unit test case	X	N/A
	Analysis of test coverage at software unit level	X	N/A
	Safety related unit test	X	N/A
	Review of safety related unit test result	X	N/A
Software integration test	Development of safety related software integration test case	X	N/A
	Review of safety related software integration test case	X	N/A
	Analysis of test coverage at software architectural level	X	N/A
	Safety related software integration test	X	N/A
	Review of safety related software integration test result	X	N/A
Software test	Development of safety related software test case	O	• Analysis of safety requirements • Generation and analysis of equivalence classes • Analysis of boundary values
	Review of safety related software test case	O	• Walkthrough
	Safety related Software test	O	• Requirements based test • Fault injection test
	Review of safety related software test result	O	• Walkthrough

SSRI 5는 안전과 관련된 위험이 없는 SW로 분류가 되었기 때문에 필수적으로 적용해야 하는 안전활동 및 적용기법은 존재하지 않는다. 필요에 따라 SW

안전 공통기준에 명시된 안전활동 및 적용기법을 활용할 수 있다.

가. 안전 활동

SW 안전 공통기준에서 권고하는 안전 활동은 SW 요구사항, SW 설계, 소프트웨어 구현, SW 단위 검증, SW 통합 검증, SW 검증 단계에 맞추어 구성되어 있으며 각각의 <표 3-8>과 같다.

<표 3-8> SW 개발 단계 안전 활동

안전 활동	설 명
Development of software safety requirements	SW 안전 요구사항을 정의하는 활동으로 일반적인 SW 요구사항 정의 시 적용 가능하며, 활동 수행 시 Structured natural language 기법을 사용함
Safety analysis of safety requirements	식별된 SW의 안전 요구사항을 대상으로 Software Fault Tree Analysis 및 Software Failure mode and effects analysis 기법을 통해 안전 분석을 수행하여 위험 요소가 없는지 확인하는 활동
Review of safety requirements	SW 안전 요구사항을 대상으로 Inspection 및 Walkthrough를 사용하여 완전성, 정확성, 일관성 및 테스트 가능성을 검토하는 활동
Development of software safety design	SW 안전 요구사항을 대상으로 Hierarchical structure of software components 기법을 이용하여 SW 설계를 수행하는 활동
Safety analysis of design	안전이 고려된 SW 설계 정보를 대상으로 Software Fault Tree Analysis 및 Software Failure mode and effects analysis 기법을 통해 안전 분석을 수행하여 위험 요소가 없는지 확인하는 활동
Review of safety design	안전이 고려된 SW 설계 정보를 대상으로 Inspection 및 Walkthrough를 사용하여 완전성, 정확성, 일관성 및 테스트 가능성을 검토하는 활동
Safety analysis of code	SW 설계 정보를 기반으로 작성된 소스 코드를 대상으로 Safety code analysis 기법을 통해 안전 분석을 수행하여 기능 오작동을 일으킬 수 있는 요소가 존재하는지 분석하는 활동
Review of safety code	안전 기능과 관련된 소스 코드를 대상으로 Inspection 및 Walkthrough를 사용하여 완전성, 정확성, 일관성 및 테스트 가능성을 검토하는 활동
Development of safety related unit test case	안전 기능과 관련된 소스 코드를 대상으로 단위 검증을 수행하기 위해 Analysis of safety requirements, Generation and analysis of equivalence classes, Analysis of boundary values 기법을 사용하여 테스트 케이스를 개발하는 활동

안전 활동	설 명
Review of safety related unit test case	안전 기능과 관련된 테스트 케이스를 대상으로 Inspection 및 Walkthrough를 사용하여 완전성, 정확성, 일관성 및 테스트 가능성을 검토하는 활동
Analysis of test coverage at software unit level	안전 기능과 관련된 소스 코드를 대상으로 SW 단위 수준에서 달성해야 하는 Statement coverage, Branch coverage, Condition coverage에 대해 분석하는 활동
Safety related unit test	안전 기능과 관련된 테스트 케이스 기반으로 Requirements based test, Fault injection test를 통해 SW 단위 검증을 수행하는 활동
Review of safety related unit test result	안전 기능과 관련된 SW 단위 검증 결과에 대해 Inspection 및 Walkthrough를 사용하여 적절성 및 적합성을 검토하는 활동
Development of safety related software integration test case	안전과 관련된 SW 설계 정보를 기반으로 SW 통합 검증을 수행하기 위해 Analysis of safety requirements, Generation and analysis of equivalence classes, Analysis of boundary values 기법을 사용하여 테스트 케이스를 개발하는 활동
Review of safety related software integration test case	안전 기능과 관련된 SW 통합 테스트 케이스를 대상으로 Inspection 및 Walkthrough를 사용하여 완전성, 정확성, 일관성 및 테스트 가능성을 검토하는 활동
Analysis of test coverage at software architectural level	안전 기능과 관련된 통합 SW를 대상으로 SW 설계 수준에서 달성해야 하는 Function coverage, Call coverage에 대해 분석하는 활동
Safety related software integration test	안전 기능과 관련된 SW 통합 테스트 케이스를 대상으로 Requirements based test, Fault injection test를 통해 SW 통합 검증을 수행하는 활동
Review of safety related software integration test result	안전 기능과 관련된 SW 통합 검증 결과에 대해 Inspection 및 Walkthrough를 사용하여 적절성 및 적합성을 검토하는 활동
Development of safety related software test case	SW 안전 요구사항을 기반으로 SW 검증을 수행하기 위해 Analysis of safety requirements, Generation and analysis of equivalence classes, Analysis of boundary values 기법을 사용하여 테스트 케이스를 개발하는 활동
Review of safety related software test case	SW 안전 요구사항과 관련된 테스트 케이스를 대상으로 Inspection 및 Walkthrough를 사용하여 완전성, 정확성, 일관성 및 테스트 가능성을 검토하는 활동
Safety related Software test	SW 안전 요구사항과 관련된 테스트 케이스 기반으로 Requirements based test, Fault injection test를 통해 SW 검증을 수행하는 활동
Review of safety related software test result	SW 안전 기능과 관련된 SW 검증 결과를 대상으로 Inspection 및 Walkthrough를 사용하여 적절성 및 적합성을 검토하는 활동

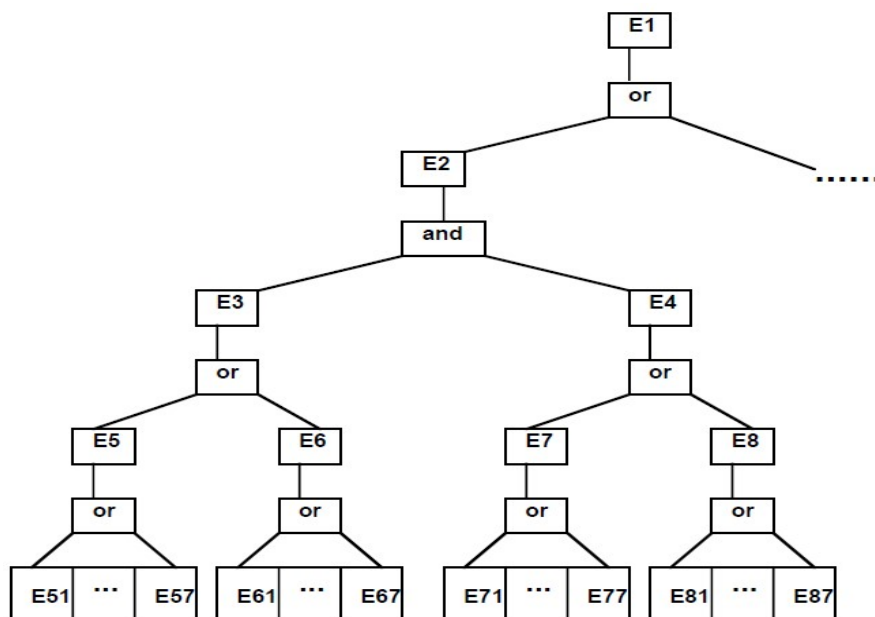
나. 적용 기법

SW 안전 공통기준에서 제시하고 있는 것과 같이, 각 안전 활동 별로 적용할 수 있는 기법이 존재한다. 해당 기법들에 대해 아래와 같이 소개한다.

1) Structured natural language

요구사항을 일반적인 자연어로 기술하였을 때, 그 의미가 모호해질 수 있고 요구사항 간의 균일성이 맞지 않을 수 있다. 이를 해결할 수 있도록 구조화된 자연어를 사용하여 SW 요구사항의 품질을 향상할 수 있다.

[그림 3-5] Software fault tree analysis 예시



출처 : J. Dennis Lawrence, “Software Reliability and Safety in Nuclear Reactor Protection Systems” , U.S. Nuclear Regulatory Commission, 1993.06.11.

2) Software fault tree analysis

본 기법은 [그림 3-5]와 같이 SW의 기능 또는 설계상에서 발생할 수 있는 최상위 고장 이벤트에 대한 근본적인 원인을 식별하고 각각의 원인이 발생할 수

있는 확률을 정의하기 위해 사용되는 논리적인 연역적 안전 분석 방법이다.

3) Software failure mode and effect analysis

본 기법은 [그림 3-6]과 같이 SW의 기능 또는 설계상에서 발생할 수 있는 고장모드의 위험도를 평가하고, 원인과 위험이 미치는 영향을 분석하는 기법이다. 고장 모드의 발생 가능성을 낮추거나 회피하는 방안을 정의하기 위해 사용되며 경험 기반의 정보를 사용하는 안전분석 방법이다.

[그림 3-6] Software failure mode and effects analysis 예시

Module	Failure modes	Failure causes	Failure effects			Severity	Corrective actions
			Local	Higher	System		
The redundancy management of the input signal	No voting result of the input signal produced	The input signal of the module cannot be identified.	-----	No input signal for the calculation of the control law.	The fight control system produce no command to the actuator and thus the airplane may lose control .	1	Implement the mornitoring of the signal to find the failure in time.
							
	The voting result of the input signal is incorrect	Invalid channels are judged to be valid.	-----	May lead to a fault in the calculation of the control law.	The flight control computer system may produce wrong command to the actuator and thus may lead to a dangerous state of the airplane.	2	Strengthen the unit test.
		Valid channels are judged to be invalid.					Strengthen the unit test.
		The algorithm does not re-configure after the fault recovery.					Improve the fault management to update the state and revise the algorithm.
		Deviation in the input signal when only one valid channel left.					When there is only one vaid channel, the voting result should be the average value of the previous-cycle signal and the current signal.
		The “hardware failure” and “the flag of the channel switches from 0 to 1” occur simultaneously.					The flag of the channel should contain two or more bits, e.g. 01 represents the invalid state and 10 represents the valid state.
							

출처 : Xu Lili 외, “An Improved SFMEA Method Integrated with Assistive Techniques” , ISSREW, 2013

4) Inspection

검토를 수행하는 정형화된 방법으로 검토 대상의 결함 발견 및 결함 데이터를 수집하며 검토 대상에 대한 전문지식을 교환한다. 수행 조직은 검토 대상에 대해 전문지식을 가진 인원으로 구성하며 계획, 사전검토, 검토 회의, 수정/개선,

검증의 단계로 진행한다.

5) Walkthrough

검토를 수행하는 비정형화된 방법으로 검토 대상의 결함을 발견하기 위해 수행한다. 수행 조직은 검토 대상 개발에 참여한 팀원으로 구성하고 계획, 검토 회의, 수정/개선의 단계로 진행한다.

6) Hierarchical structure of software components

SW 설계 중 SW 컴포넌트를 식별 및 구성하기 위해 적용할 수 있는 기법으로, SW 컴포넌트를 계층적 구조로 설계하여 SW의 복잡도를 적절하게 관리할 수 있도록 한다.

7) Safety code analysis

안전과 관련된 기능을 구현한 소스 코드 대상으로 주어진 안전 요구사항을 적절하게 구현하는지를 확인하며 소스 코드 내부에 에러를 유발할 수 있는 코드가 존재하는지 확인하다.⁴¹⁾⁴²⁾

8) Generation and analysis of equivalence classes

안전과 관련된 기능에 대한 테스트 케이스 설계 시 적용할 수 있는 기법의 하나로써 [그림 3-7]과 같이 검증해야 하는 기능의 입력값이 동일하게 여겨질 수 있는 구간을 식별하여 테스트 케이스를 최소한으로 설계한다.

41) David J. Shampine 외, “Introduction to System & Software Safety – Class 1-1”, International System Safety Society Wahington DC Chapter, 2015.05.12

42) Peggy Rogers 외, “Software Safety Tutorial”, International System Safety Training Symposium, 2014.08.05

[그림 3-7] Generation and analysis of equivalence classes
예시

[블랙박스 시스템의 충격 관련 기능 명세]

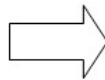
충격 정보는 다음과 같은 가속도 센서의 값에 따라 4단계로 구분하여 출력된다.

- 가속도 센서 값(1 - 5) : 1단계
- 가속도 센서 값(6 - 10) : 2단계
- 가속도 센서 값(11 - 15) : 3단계
- 가속도 센서 값(16이상) : 4단계

[동치 분할]

입력 영역 분할

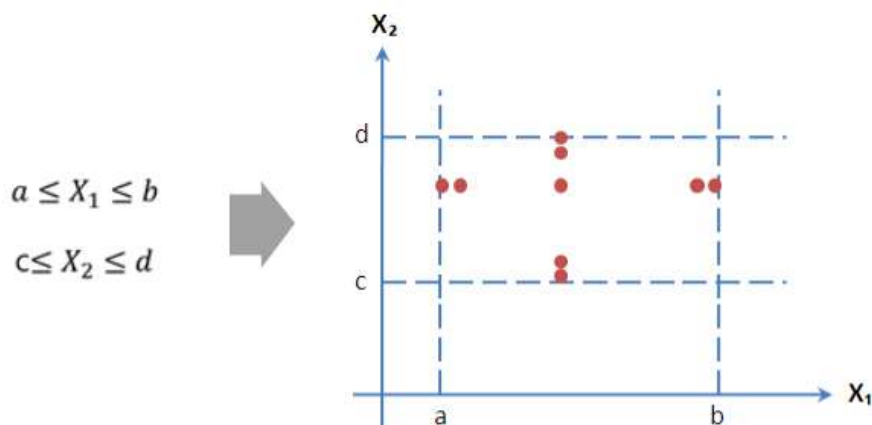
- [1..5] : 1단계
- [6..10] : 2단계
- [11..15] : 3단계
- [16..255] : 4단계



9) Analysis of safety requirements

안전과 관련된 기능에 대한 테스트 케이스 설계 시 적용할 수 있는 기법으로, 안전과 관련된 SW 요구사항 및 설계 정보를 분석하여 테스트 수행 시 안전 기능을 검증할 수 있도록 테스트 케이스를 설계한다.

[그림 3-8] Boundary value analysis 예시



출처 : <웹진 167호 : 공학 트렌드> 프로젝트 수행 - 테스트 설계 편, NIPA, 2016.03.14

10) Analysis of boundary values

안전과 관련된 기능에 대한 테스트 케이스 설계 시 적용할 수 있는 기법의 하나로써 검증해야 하는 기능에 대해 입력 구간이 정해진 상황에서 사용할 수 있다. [그림 3-8]과 같이 입력 구간의 경계값을 기준으로 작거나 큰 값을 이용하여 테스트 케이스를 설계한다.

11) Statement Coverage

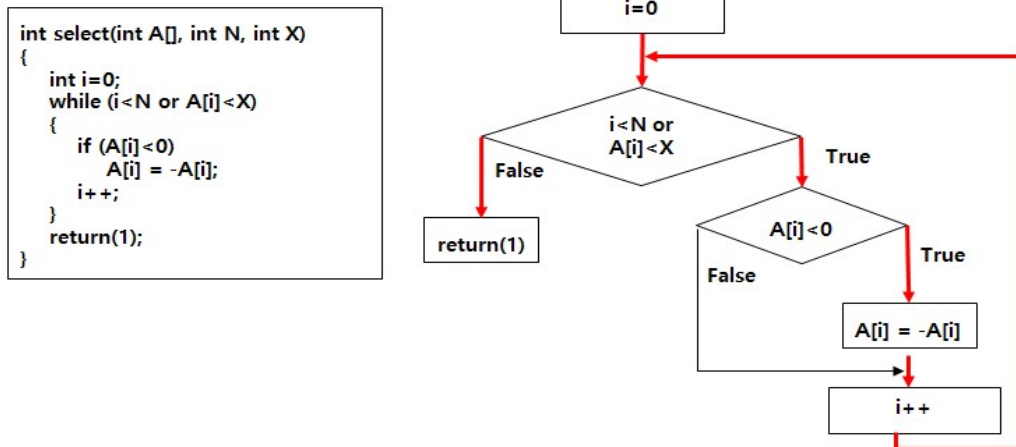
안전과 관련된 SW 단위를 대상으로 검증 범위를 확인 할 수 있는 기법의 하나로써 [그림 3-9]와 같이 SW 단위 검증 중에 소스 코드가 얼마만큼 실행되었는지 정도를 의미한다.

[그림 3-9] Statement coverage 예시

테스트 입력 하나로 스테이트먼트 커버리지를 달성할 수 있다. (흐름 그래프 상의 빨간 경로)

- Test cases = { (N=1, A[0]=-7, X=9) }

If 문의 '거짓' 경로(흐름 그래프 상의 검정 경로)에 결함이 있을 경우 발견되지 않는다.



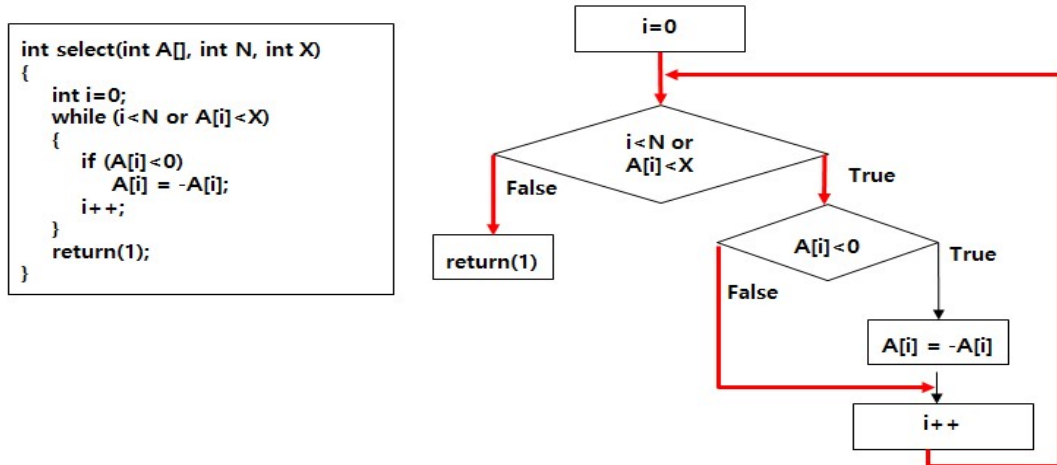
12) Branch coverage

안전과 관련된 SW 단위를 대상으로 검증 범위를 확인할 수 있는 기법의 하나로써 [그림 3-10]과 같이 SW 단위 검증 중에 소스 코드 내 모든 결정의 분기가 얼마만큼 실행되었는지 정도를 의미한다.

[그림 3-10] Branch coverage 예시

Statement coverage 테스트 입력에 If 문의 '거짓' 경로를 포함함으로써, 분기 커버리지를 달성할 수 있다.

- Test cases = { (N=1, A[0]=-7, X=9), (N=1, A[0]=7, X=9) }
 하지만, while의 조건문 내부의 결함은 발견되지 않을 수 있다.



13) Condition coverage

안전과 관련된 SW 단위를 대상으로 검증 범위를 확인할 수 있는 기법의 하나로써 SW 단위 검증 중에 소스 코드 내 모든 결정을 구성하는 조건에 대해 얼마만큼 실행되었는지 정도를 의미한다.

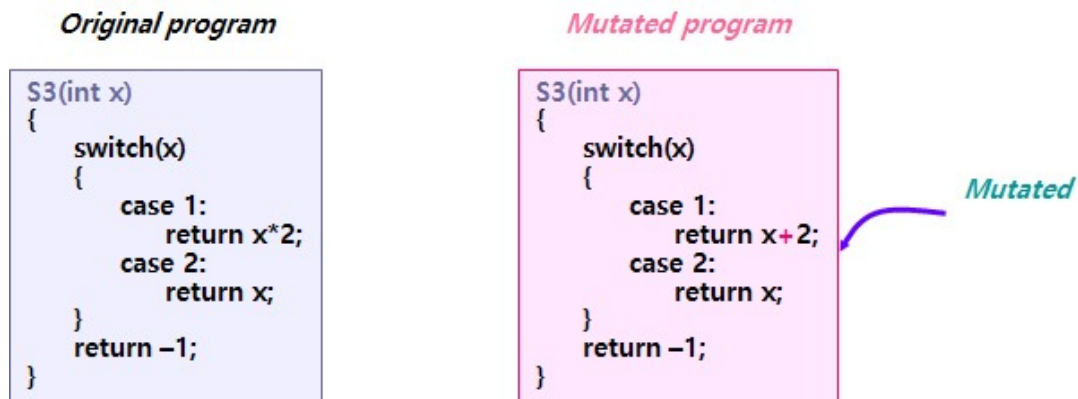
14) Requirements based test

안전과 관련된 SW 요구사항 및 설계 정보로부터 테스트 케이스를 설계하여 테스트를 수행하는 방법으로, SW의 주요 명세 정보에 대해 입력 및 출력을 설계하고 테스트를 수행한다.

15) Fault injection test

SW가 정상적으로 동작하는 동안에 비정상적인 상태로 전환될 수 있도록 [그림 3-11]과 같이 강제로 결함을 주입(Mutated)하여 발생 되는 예외 상황에 대한 SW 반응을 테스트하는 방법이다.

[그림 3-11] Fault injection 예시



16) Function coverage

안전과 관련하여 통합된 SW를 대상으로 검증 범위를 확인할 수 있는 기법의 하나로써 SW 통합 검증 중에 SW가 가지고 있는 모든 함수를 기준으로 얼마만큼 호출되었는지 정도를 의미한다.

17) Call coverage

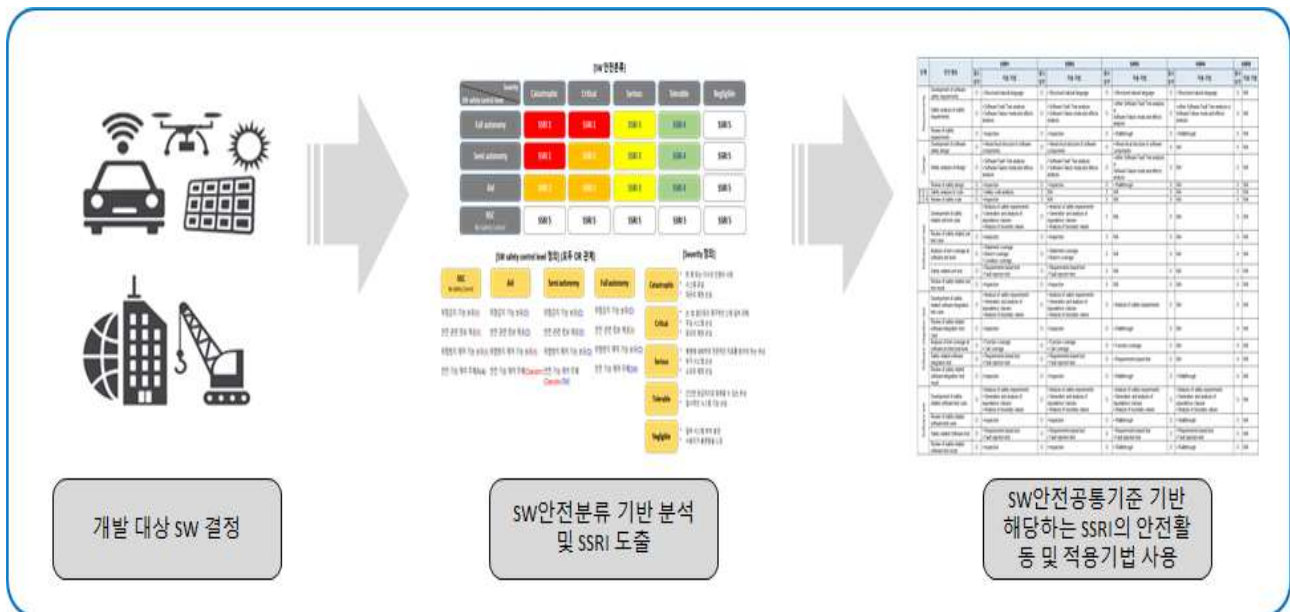
안전과 관련하여 통합된 SW를 대상으로 검증 범위를 확인할 수 있는 기법의 하나로써 SW 통합 검증 중에 SW가 가지고 있는 모든 함수 호출 수를 기준으로 얼마만큼 호출되었는지 정도를 의미한다.

3. SW 안전 분류 및 SW 안전 공통기준 활용 방법

아래의 [그림 3-12]와 같이 SW 안전 분류 및 SW 안전 공통기준을 활용할 수 있다. 개발하고자 하는 SW를 대상으로 SW 안전 분류에 따라 위험 심각도 및 SW 안전 제어 통제 등급을 결정하여 SSRI를 도출 후, SW 안전 공통기준에 따라 도출된 SSRI에 부합하는 안전활동과 적용기법을 식별한다. 이후 식별된 안전활

동 및 적용기법을 SW 개발 단계별로 적용하여 적정한 수준으로 안전을 고려하여 SW를 개발할 수 있다.

[그림 3-12] SW 안전 분류 및 SW 안전 공통기준 활용방법



제4장 결 론

이 연구에서는 기존의 SW 안전성을 고려하는 분야뿐 아니라 제4차 산업혁명의 도래로 새롭게 만들어진 산업 분야에서도 SW의 안전성을 고려할 수 있도록 SW 안전 분류 및 SW 안전 공통기준을 도출하는 과정을 다루었다.

SW 안전 분류를 도출하기 위해 기존에 안전을 중요하시는 다양한 분야의 관련 연구들을 분석하였고, SW 중심의 안전 분류를 하는 연구도 함께 분석하였다. 최초 SW 안전 분류를 도출하기 위해 분야 중심 안전 분류 연구 접근 방식을 적용하였으나, SW 안전 분류를 도출하기에 적합하지 않다고 판단하여 SW 중심의 안전 분류 연구 접근방식으로 연구를 진행하였다.

SW 안전 분류 도출에 앞서 MIL-STD-882E를 기준으로 활용하여 SW 안전 분류 모델을 먼저 정의하였다. SW 안전 분류 모델을 선정 후 다양한 분야에서 SW 안전 분류가 활용될 수 있도록 항공·우주, 의료기기, 자동차 분야의 관련 연구를 분석하여 SW 안전 분류 모델을 개선하여 SW 안전 분류 초안을 완성했다. SW 안전 분류 초안의 적절성 및 적합성을 확인하기 위해 전문가 자문단의 검토를 받았고, 검토 의견을 반영하여 SW 안전 분류 초안을 보완 후 SW 안전 분류를 도출했다.

5개의 위험 심각도와 4개의 SW 안전 통제 등급을 이용하여 SW 안전 분류를 수행할 수 있도록 구성하였으며 제4차 산업혁명으로 파생되는 신규 산업 분야까지 모두 고려할 수 있도록 정의하였다.

도출된 SW 안전 분류의 정당성을 확인하기 위해 기존의 SW 안전분야에서 사용되는 시스템과 신규 SW 안전 분야의 시스템을 대상으로 검증을 수행하였으며, 적합하게 SW 안전 분류를 수행하고 있는 것으로 검증 결과가 확인되었다.

SW 안전 분류를 통해 결정된 SW 안전 위험 색인을 바탕으로 적절한 수준의 안전 활동과 기법을 수행할 수 있도록 SW 안전 공통기준을 도출 연구를 진행하였다. 안전 활동의 경우, SW 안전 공통기준 도출을 위해 활용한 미 국방 표준과 미 항공우주국 가이드를 분석하여 도출하였고, 안전 활동 별 적용 가능한 기법은 자동차 도메인의 표준을 분석하여 도출하였다.

SW 안전 공통기준은 22개의 안전 활동과 17개의 기법으로 구성되어 있으며, SW 안전 위험 색인에 따라 권고하는 안전 활동과 기법의 차이를 두어 정의하였다. SW 안전 공통기준의 원활한 활용을 위해 안전 활동과 안전 활동 별 적용할 수 있는 기법에 대해 정의했다.

본 연구를 통해 제4차 산업혁명의 도래로 파생되는 산업 분야와 안전에 대한 고려가 증대하는 것을 고려하여 SW 안전 분류 및 SW 안전 공통기준을 도출하였다. 궁극적으로 전부 개정 중인 소프트웨어산업진흥법의 제29조 소프트웨어안전 확보를 위한 지침의 기초자료로 활용하고자 한다.

참고문헌

< 국내 문헌 >

등록특허, “전동차 출입문과 지상 스크린도어의 동시 개폐 장치”, 서울메트로, 2012.08.07

박태형 외, “소프트웨어 안전(Safety) 산업 동향 조사”, SPRi, 2017.04

철도시설 기술기준, 국토교통부

철도용품 기술기준, 국토교통부

철도차량 기술기준, 국토교통부

< 해외 문헌 >

David J. Shampine 외, “Introduction to System & Software Safety – Class 1-1”, International System Safety Society Wahington DC Chapter, 2015.05.12

DO-178B Software level 별 Failure rate 출처 John Rushby, “New Challenges In Certification For Aircraft Software”, SRI International, 2011

DO-178C, Software Considerations in Airborne Systems and Equipment Certification

EN ISO 14971, Medical devices — Application of risk management to medical devices

IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems

IEC 62304, Medical device software – Software life-cycle processes

ISO26262, Road vehicles -- Functional safety --

J3016, Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems, 2016

John McDermid 외, “Software in Safety Critical Systems: Achievement and Prediction, Thomas Telford Journals, June 2006.11

Peggy Rogers 외, “Software Safety Tutorial” , International System Safety Training Symposium, 2014.08.05

PG Bishop, “SILs and Software” , Adelard and Centre for Software Reliability, City University London, 2005.01

SAFETY-CRITICAL SOFTWARE STANDARDS – SURVEY AND SUMMARY, ASSC, 1996

< 기 타 >

민경욱 “3년간 서울지하철 사고 1574건…끼임 사고 최다“, News1, 2018.09.09

주 의

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



[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.)