소프트웨어안전 확보를 위한 효율적 안전 관리 방안

2020. 12.03

진 회 승
소프트웨어정책연구소 책임연구원

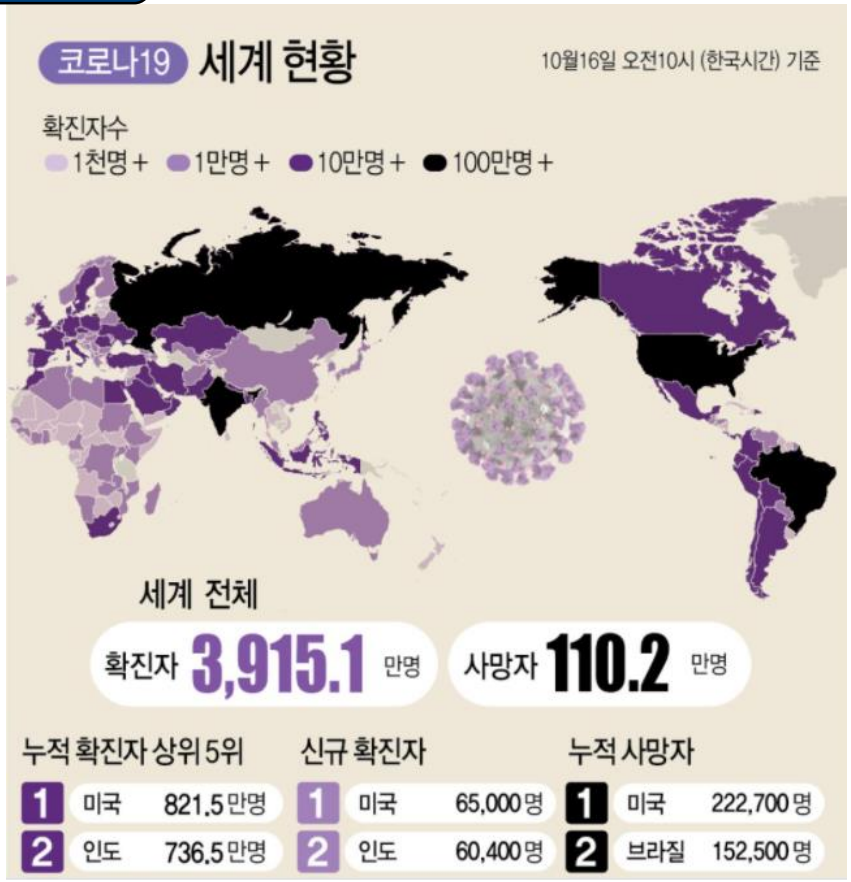
SPRi 소프트웨어정책연구소

목 차

안전과 소프트웨어안전

재난 (코로나 19, 항공기 사고)

10.16.



12.2.

	사망자	발생국가·영토
63,839,014	1,479,999	221
602,219▲	12,014▲	-

보잉 747 MAX 사고

항공기 추락방지 **SW**인 **MCAS**의 오작동으로 인도네시아, 에티오피아 여객기 추락사고

(346명 사망)

* 연합뉴스(2020/10/16) , 세계 코로나19 현황 / 중앙재난안전대책본부(2020.12.2) , 세계현황 / 사진(뉴시스, AP)

위험과 안전

● 위험

- **harm :** injury or damage to the health of people, or damage to property or the environment
- **Hazard :** potential source of **harm**

● 안전

- **Safety** is the state of being "safe", the condition of being protected from harm or other non-desirable outcomes.
- **Safety** can also refer to the control of recognized hazards in order to achieve an acceptable level of risk.

Wikipedia(2020) , safety ISO/IEC Guide 51:2014 , Harm, Hazard

Risk

Categories

- Economic
- Environmental
- Geopolitical
- Societal
- Technological

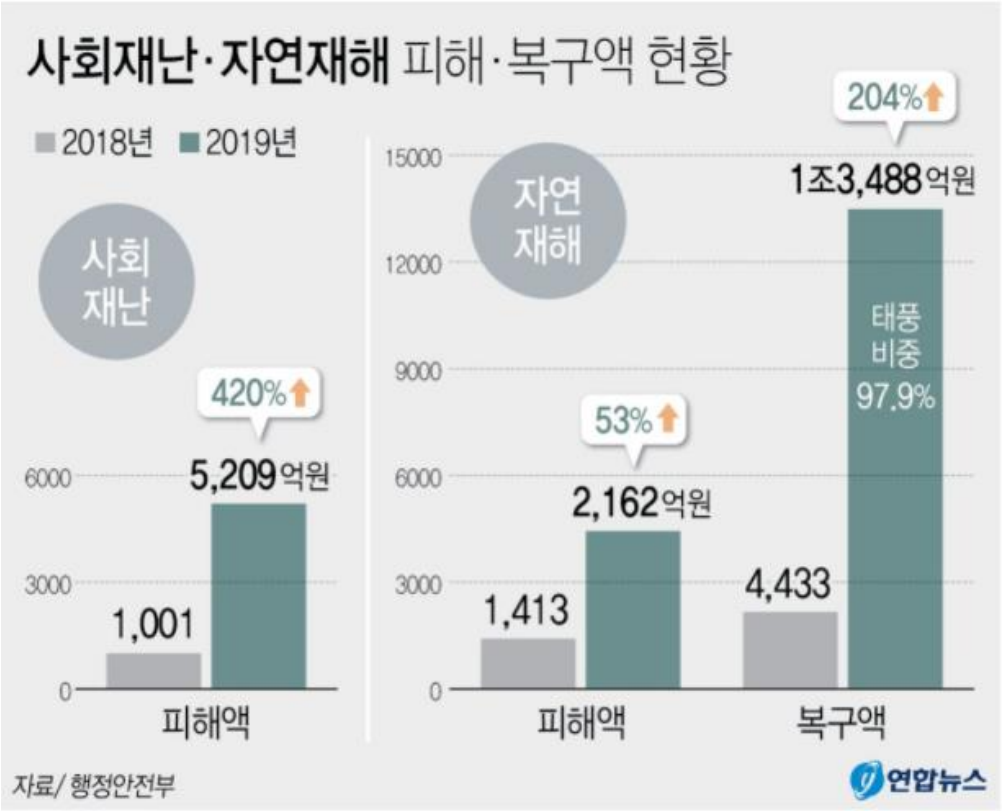
The Global Risks Report 2020(WEF)

자연 재난과 사회 재난

● 재난

➢ 국민의 생명 · 신체 · 재산과 국가에 피해를 주거나 줄 수 있는 것

순번	행정안전부와 그 소속기관 직제 시행규칙의 제19조의2 (재난협력실)		
	재난 유형 (42종)		재난유형(42종)
1	감염병 재난	22	사업장 인적사고
2	가축질병	23	고속철도 사고
3	보건의료 사고	24	지하철 사고
4	식용수 사고	25	도로터널 사고
5	지역축제	26	내수면 유도선 사고
6	학교 및 학교시설에서 발생한 사고	27	저수지 사고
7	경기장 발생 사고	28	댐 사고
8	공연장 발생 사고		
9	정보통신 사고	29	원유수급 사고
10	교정시설 재난 및 사고	30	가스 수급 및 누출 사고
11	문화재 시설 사고	31	육상화물운송 사고
12	금융 전산 및 시설사고	32	항공운송 마비
13	위성항법장치(GPS) 전파혼신 재난	33	항행안전시설 장애
14	접경지역 사고	34	항공기 사고
15	인공 우주물체 · 위성 등의 추락 · 충돌	35	유해화학물질 유출 사고
16	정부주요시설 사고	36	위험물 사고
		37	원자력안전 사고
17	다중 밀집시설 화재	38	인접국가 방사능 누출사고
18	해양 선박 사고	39	공동구(公同溝) 재난
19	해양 유도선 등의 수난사고	40	산불
20	다중밀집건축물 붕괴 사고	41	수질분야 환경오염 사고
21	전력 사고	42	해양 분야 환경오염 사고



재난 및 안전관리기본법 , 재난의 정의 / LIG시스템 장대원(2020), 시민 참여형 사회안전 위험 해소 방안

소프트웨어안전

● 소프트웨어 진흥법

"소프트웨어안전"이란 외부로부터의 침해행위가 없는 상태에서 소프트웨어의 내부적인 오작동 및 안전기능(사전 위험분석 등을 통하여 위험발생을 방지하는 기능을 말한다) 미비 등으로 발생할 수 있는 사고로부터 사람의 생명이나 신체에 대한 위험에 충분한 대비가 되어 있는 상태를 말한다.

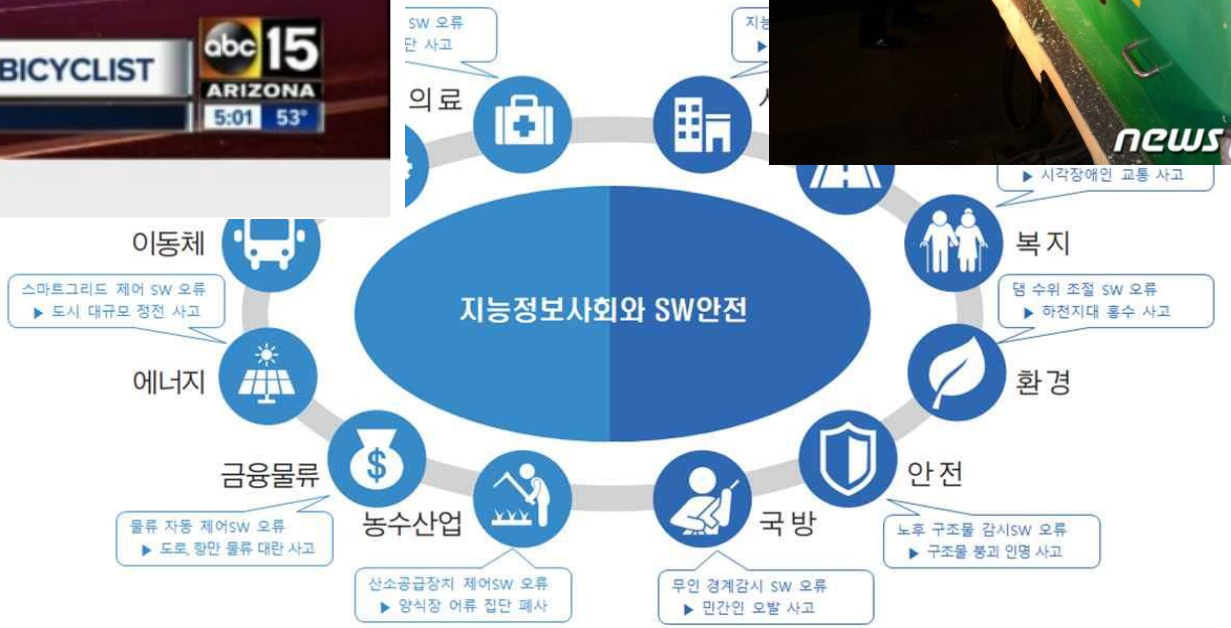
● 소프트웨어로 인한 사고

자동차	도요타 자동차 급발진('09) 	사고내용	도요타 렉서스 자동차가 195km/h 속도로 급발진 발생
		사고원인	ECU 메모리를 SW간 공유하면서 생기는 간섭 현상으로 발생
		피해상황	일가족(4명) 사망 / 벌금 1조 3천억원 부과, 900만대 리콜
	자율주행차 보행자 사망('18) 	사고내용	우버의 자율주행차가 자율모드로 주행 중 보행자와 충돌
		사고원인	SW가 횡단보도 바깥쪽으로 보행자가 건너는 상황에서 주의를 필요로 하지 않은 구역으로 인식했을 것으로 추정
		피해상황	보행자 사망
로봇	경비 로봇 어린아이 폭행('16) 	사고내용	미국의 쇼핑센터에 설치된 자율주행 경비 로봇이 어린아이를 폭
		사고원인	범죄가 의심되는 행동을 감지하고 알리는 시스템 오작동
		피해상황	16개월 아동을 치고 넘어감
의료	Therac25 사용 환자사망(~'87) 	사고내용	방사선 치료기인 Therac 25가 오류로 방사능 과다 투여
		사고원인	턴테이블(X-ray 균일 분사기능)을 작동하는 플래그 데이터가 8비 변화되며 생기는 오버 플로우 상태에서 작동키를 누를 경우 오작
		피해상황	3명 사망, 3명은 심각한 방사능 후유증에 시달림
철도	서울지하철 추돌사고('14) 	사고내용	신당역에서 상왕십리역으로 들어오던 열차가 상왕십리역을 출발하려던 열차를 추돌
		사고원인	신호기 고장으로 후속 열차 ATS(자동정지장치) 미작동
		피해상황	승객 등 250여명 중경상
	열차 신호설비SW 오작동('17) 	사고내용	경의중앙선 시운전 열차 추돌 (양평역과 원덕역 사이)
		사고원인	신호 설비인 모듈에 잘못된 SW 설치
		피해상황	기관사 사망, 신호수 등 6명이 중경상 / 열차 2대 파손으로 68억 3000만원의 물적 피해
항공	보잉737 항공기 추락('19) 	사고내용	보잉 737 Max8 여객기가 이륙 몇 분 뒤 추락함
		사고원인	항공기 추락방지 SW인 MCAS(Maneuvering Characteristics Augmentation System)의 오작동
		피해상황	탑승객 157명 전원 사망

소프트웨어안전을 준비하기 어려운 이유(1)

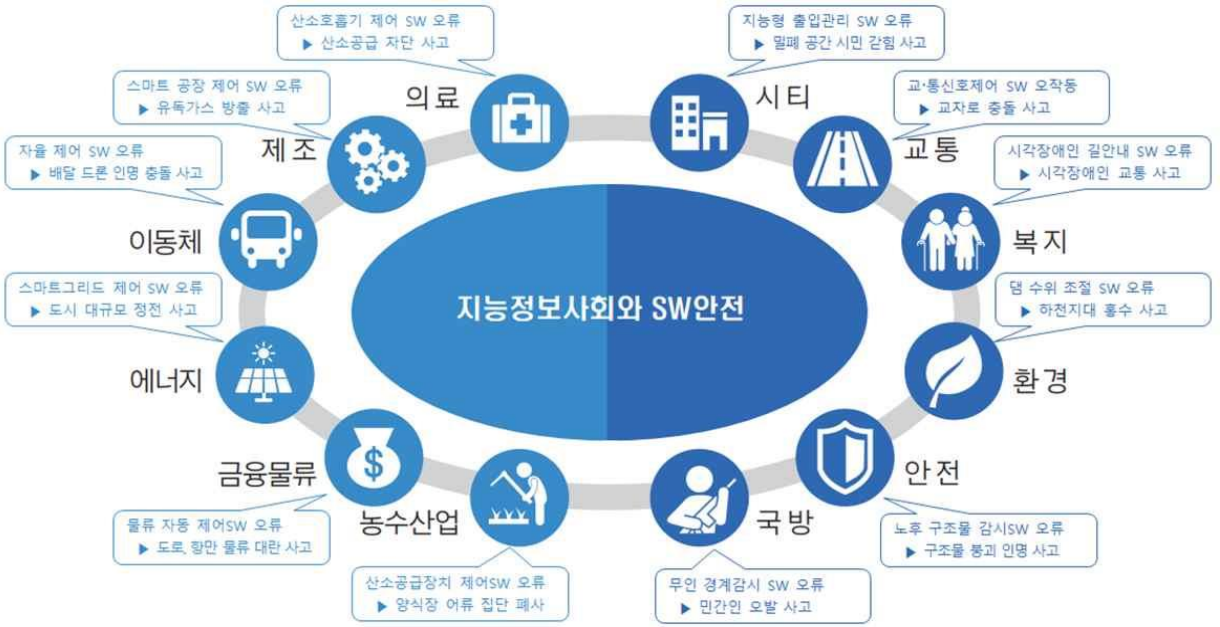
- 소프트웨어 관련 사고 발생 초기
- 소프트웨어안전이 시스템안전의 일부로 포함

우버 자율주행차량 사고 현장/사진=abc 방송화면 캡처



소프트웨어안전을 준비하기 어려운 이유(2)

- 소프트웨어안전 전문가 부족
- 소프트웨어안전 관련 기술 미성숙



- 소프트웨어안전 확보 비용 과다

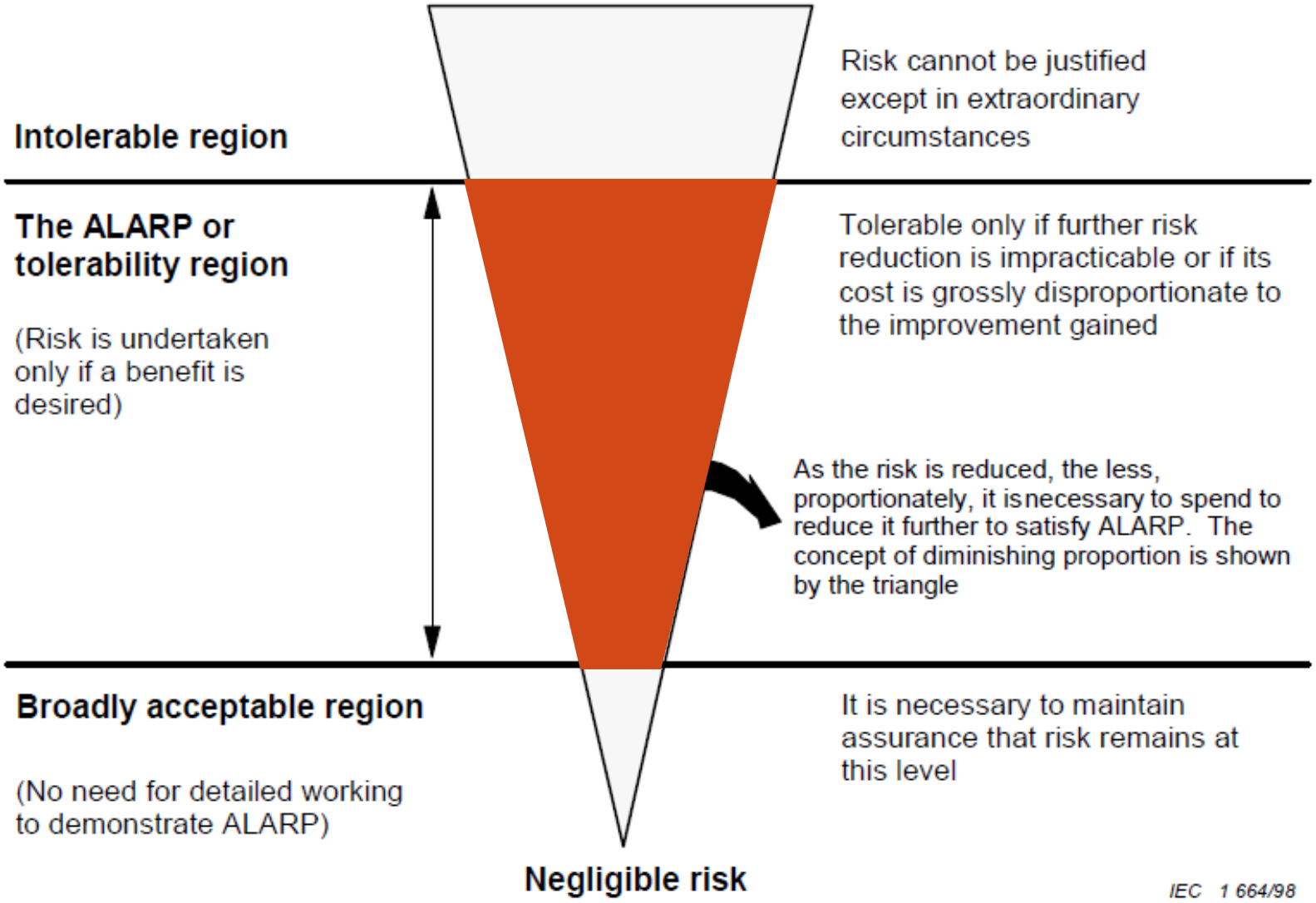
위험 피해와 안전 확보 비용

지난 11일 물에 잠긴 장시성의 한 마을. 연합뉴스

한겨레(2020.7.12.) 중국홍수피해 14조 이재민 3800만명

안전 국제표준과 소프트웨어안전 관리

Tolerable risk and ALARP



안전 표준 (IEC 61508)

Risk Class

Frequency	Consequence			
	Catastrophic	Critical	Marginal	Negligible
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV

SIL	상태
I	받아들이기 어려운 위험
II	위험감소를 구현하기 어렵거나, 사용한 비용에 비하여 개선 결과의 효과가 부족한 경우에만 용인될 수 있는 바람직하지 못한 위험
III	위험감소 비용이 개선 효과를 넘는 경우의 허용 가능한 위험
IV	무시해도 될 정도의 위험

자료: IEC 61508

안전 표준 (IEC 61508)

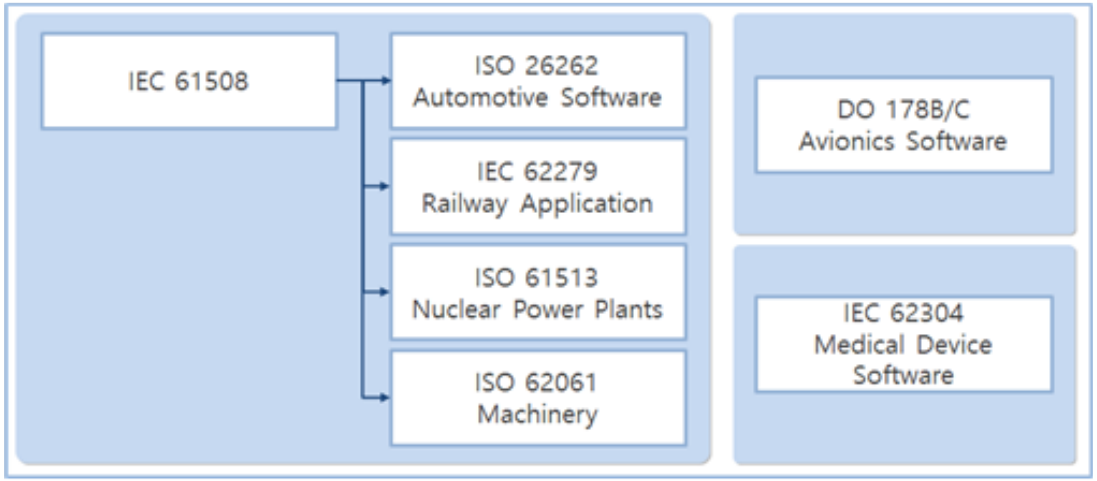
요구 기술

	Technique/Measure *	Ref.	SIL 1	SIL 2	SIL 3	SIL 4
1a	Structured methods **	C.2.1	HR	HR	HR	HR
1b	Semi-formal methods **	Table B.7	R	HR	HR	HR
1c	Formal design and refinement methods **	B.2.2, C.2.4	---	R	R	HR
2	Computer-aided design tools	B.3.5	R	R	HR	HR
3	Defensive programming	C.2.5	---	R	HR	HR
4	Modular approach	Table B.9	HR	HR	HR	HR
5	Design and coding standards	C.2.6 Table B.1	R	HR	HR	HR
6	Structured programming	C.2.7	HR	HR	HR	HR
7	Use of trusted/verified software elements (if available)	C.2.10	R	HR	HR	HR
8	Forward traceability between the software safety requirements specification and software design	C.2.11	R	R	HR	HR

자료: IEC 61508

안전 표준

안전 표준



관리 규정 / 미국

- **철도 : 49 CFR Part 236 Subpart H & I**
  - ✓ FRA (Federal Railroad Administration)
  - ✓ EN50128/IEC62279, AREMA C&S Manual 권고
- **항공 : 14 CFR 25.1309**
  - ✓ FAA (Federal Aviation Administration)
  - ✓ DO-178 사용 권고
- **원자력 : 10 CFR Part 50**
  - ✓ NRC(Nuclear Regulatory Commission)

관리 규정 / 유럽

- **철도 : Directive 2004/49/EC, 2008/57/EC**
  - ✓ 유럽연합지침
  - ✓ 각 회원국은 관련 지침에 의거 자국의 철도관련 법/제도 개정
- **항공 : Commission Reg. No 482/2008**
  - ✓ EASA (유럽항공안전기구)
  - ✓ ED-12B 권고(DO-178 과 내용 동일)

안전 표준 SIL(Safety Integrity Level) 비교

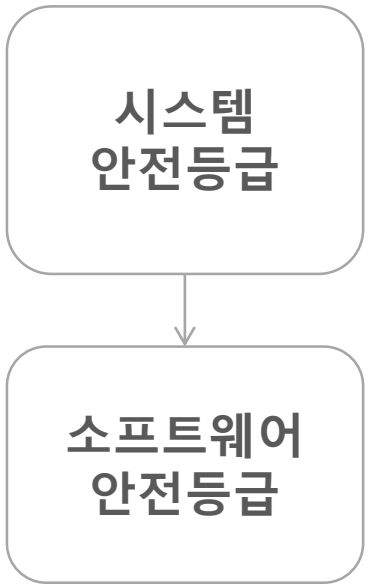
- 안전등급을 통하여 각 도메인에서 정의한 허용가능한 위험 수준과 관리 방안(위험경감방안의 필요 수준) 제공

Generic (IEC 61508)	**(SIL 0)**	**SIL 1**	**SIL 2**	**SIL 3**	SIL 4
Automotive (ISO 26262)	QM	ASIL A	ASIL B / ASIL C	ASIL D	--
Medical (IEC 62304)	Class A	Class B		Class C	
Machinery (ISO 13849)	PL a	PL b / PL c	PL d	PL e	--
Rail (EN 50128)	SIL 0	SIL 1	SIL 2	SIL 3	SIL 4
Household (IEC 60730)	Class A	Class B		Class C	--
Civil Aerospace (DO-178C)	Level E	Level D	Level C	Level B	Level A

자료: SafeTTy System Ltd/ SIL(Safety Integrity Level) 안전무결성 수준

안전표준에서 소프트웨어안전 등급 결정 방법(1)

● 시스템 수준에서 평가된 안전등급을 관련 소프트웨어가 상속



1. 시스템 수준의 위험원 분석 및 위험 평가

2. 소프트웨어에 안전등급 할당

(시스템 위험에 대한 SW의 기여도 고려)

소프트웨어 안전등급
= 시스템 안전등급
(소프트웨어가 시스템 위험에 영향을 주는 경우)

유사한 결정 방법을 사용하는 표준

- IEC 61508 (산업일반)
- IEC 62278, 62279 (철도 분야)
- DO-178C (항공 분야)
- ISO 26262 (자동차 분야)
- ISO 13482 (개인지원로봇 분야)
- NUREG/CR-6430, (원자력)

안전표준에서 소프트웨어안전 등급 결정 방법(2)

● 시스템 수준 안전등급에 소프트웨어 평가요소 추가

- 시스템 위험에 대한 심각도(Severity) 평가
- 소프트웨어가 해당 심각도에 기여하는 정도(Software Control Category) 평가

SW Control Category		Description
1	Autonomous	Software functionality that exercises autonomous control authority over potentially safety-significant hardware systems, subsystems, or components without the possibility of predetermined safe detection and intervention by a control entity to preclude the occurrence of a mishap or hazard.
2	Semi-autonomous	Software functionality that exercises control authority over potentially safety-significant hardware systems, subsystems, or components, allowing time for predetermined safe detection and intervention by independent safety mechanisms to mitigate or control the mishap or hazard. Software item that displays safety-significant information requiring immediate operator entity to execute a predetermined action for mitigation or control over a mishap or hazard. Software exception, failure, fault, or delay will allow, or fail to prevent, mishap occurrence.
3	Redundant fault tolerant	Software functionality that issues commands over safety-significant hardware systems, subsystems, or components requiring a control entity to complete the command function. The system detection and functional reaction includes redundant, independent fault tolerant mechanisms for each defined hazardous condition Software that generates information of a safety-critical nature used to make critical decisions. The system includes several redundant, independent fault tolerant mechanisms for each hazardous condition, detection and display.
4	Influential	Software generates information of a safety-related nature used to make decisions by the operator, but does not require operator action to avoid a mishap
5	No safety impact	Software functionality that does not possess command or control authority over safety-significant hardware systems, subsystems, or components and does not provide safety-significant information. Software does not provide safety-significant or time sensitive data or information that requires control entity interaction. Software does not transport or resolve communication of safety-significant or time sensitive data

SOFTWARE SAFETY CRITICALITY MATRIX				
	SEVERITY CATEGORY			
SOFTWARE CONTROL CATEGORY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
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

자료: MIL-STD-882E

미국 국방 표준 MIL-STD-882E

● 소프트웨어안전 등급과 안전활동

시스템 안전에 대한 SW 영향

SW컨트롤 등급	심각도 등급			
	치명적	매우위험	위험	낮음
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

1 심각도 등급: 사고 발생시, 결과의 심각도 수준
(사례)치명적: 사망, 영구장애, 영구 환경 피해, 100억 이상의 피해

SW안전 위험도 등급에 따른 안전활동 수준

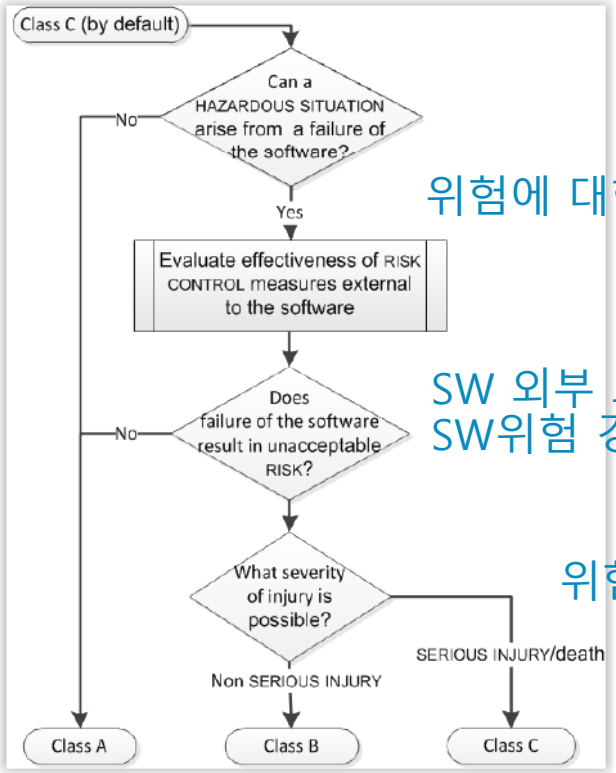
SW안전 위험도 등급	SW안전 활동 수준
SwCI 1	요구사항, 아키텍처, 설계, 코드를 분석하고, 심도 있는 SW안전 테스트 수행
SwCI 2	요구사항, 아키텍처, 설계를 분석하고, 심도 있는 SW안전 테스트 수행
SwCI 3	요구사항, 아키텍처를 분석하고, 심도 있는 SW안전 테스트 수행
SwCI 4	SW안전 테스트 수행
SwCI 5	안전성 검증을 통해, 안전과 무관하다고 판단되면, SW안전 관련 분석 및 확인 불필요

자료: MIL-STD-882E Standard Practice System Safety, Department of Defense, SwCI : Software Criticality Index

안전표준에서 소프트웨어안전 등급 결정 방법(3)

● 소프트웨어 위험 심각도에 기반한 소프트웨어의 안전등급 평가

- 시스템 수준의 위험평가에 대한 고려 없이 소프트웨어 수준에서 평가 가능
- 소프트웨어 외부요소에 의한 위험 감소도 고려함



위험에 대한 SW영향 여부

SW 외부 요소에 의한 SW위험 경감

위험의 심각도

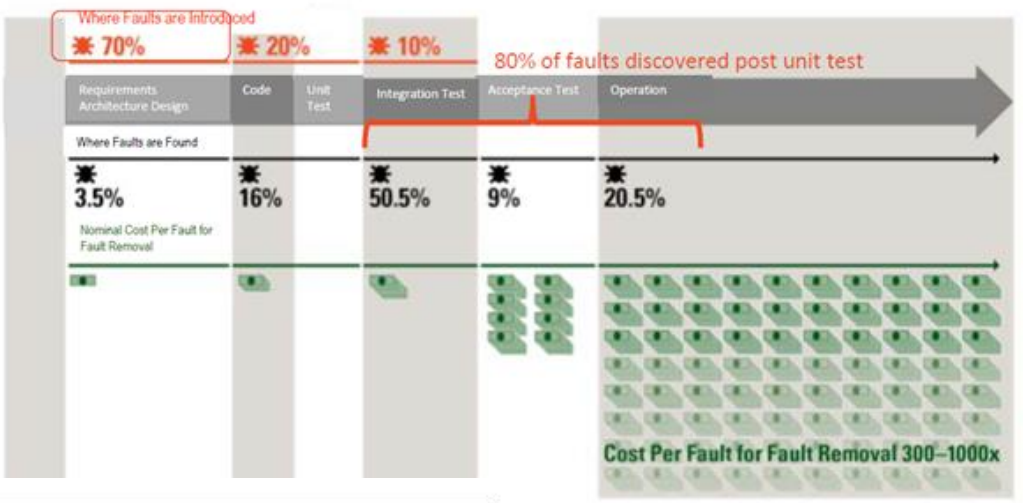
유사한 결정방법을 사용하는 표준

- IEC 62304 (의료)
- IEC 60730 (자동전자제어장치)

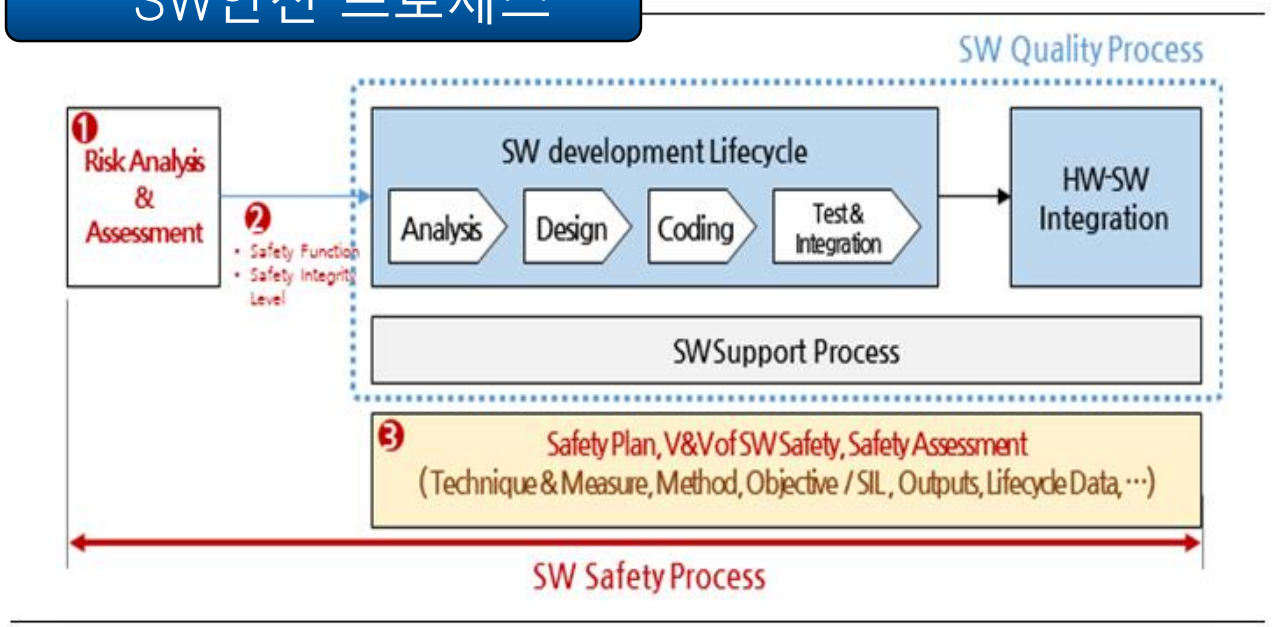
자료: IEC 62304

소프트웨어안전 확보 활동

- **SW안전 확보를 위한 활동**
  - 안전 개발 프로세스에 따른 제품 개발
  - 안전 등급에 따른 무결성 보장



SW안전 프로세스



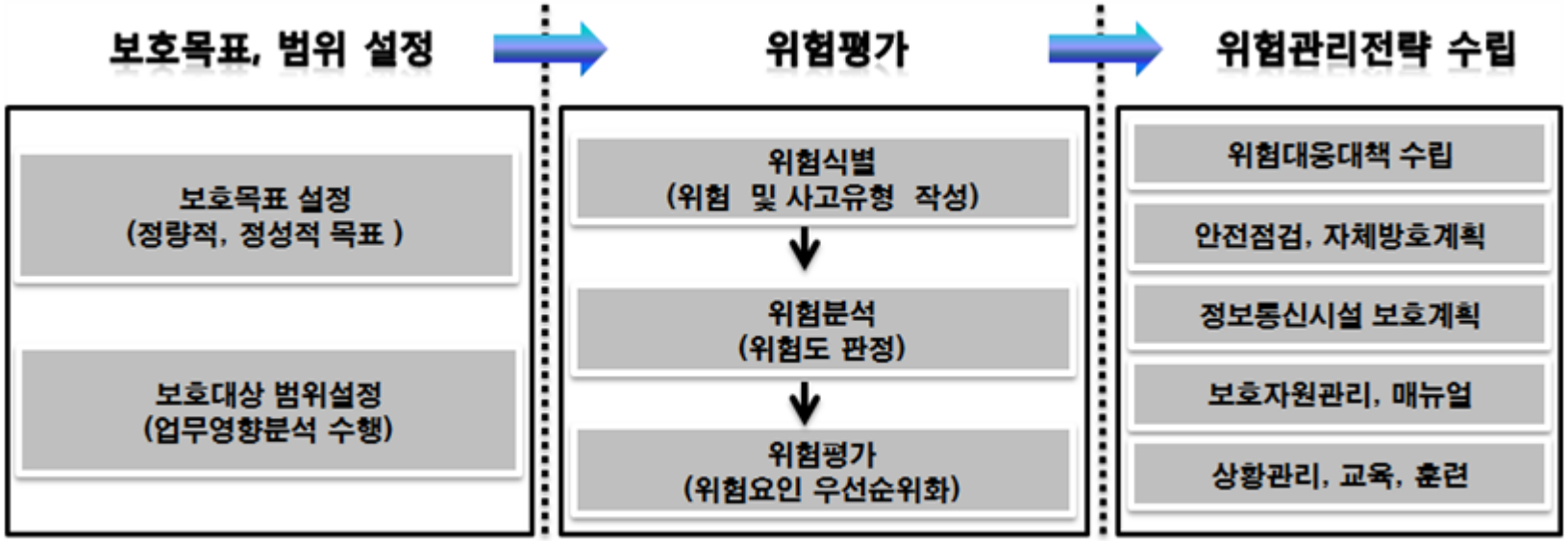
출처 : Peter Feiler, Challenges in Existing System Safety Practices, CMU, Software Solutions Symposium 2017

국내 소프트웨어안전 관리방안

국가기반시설 관리

- 재난 및 안전관리 기본법 제26조 (국가핵심기반의의 지정 등), 제26조의 2(국가핵심기반의의 관리 등)

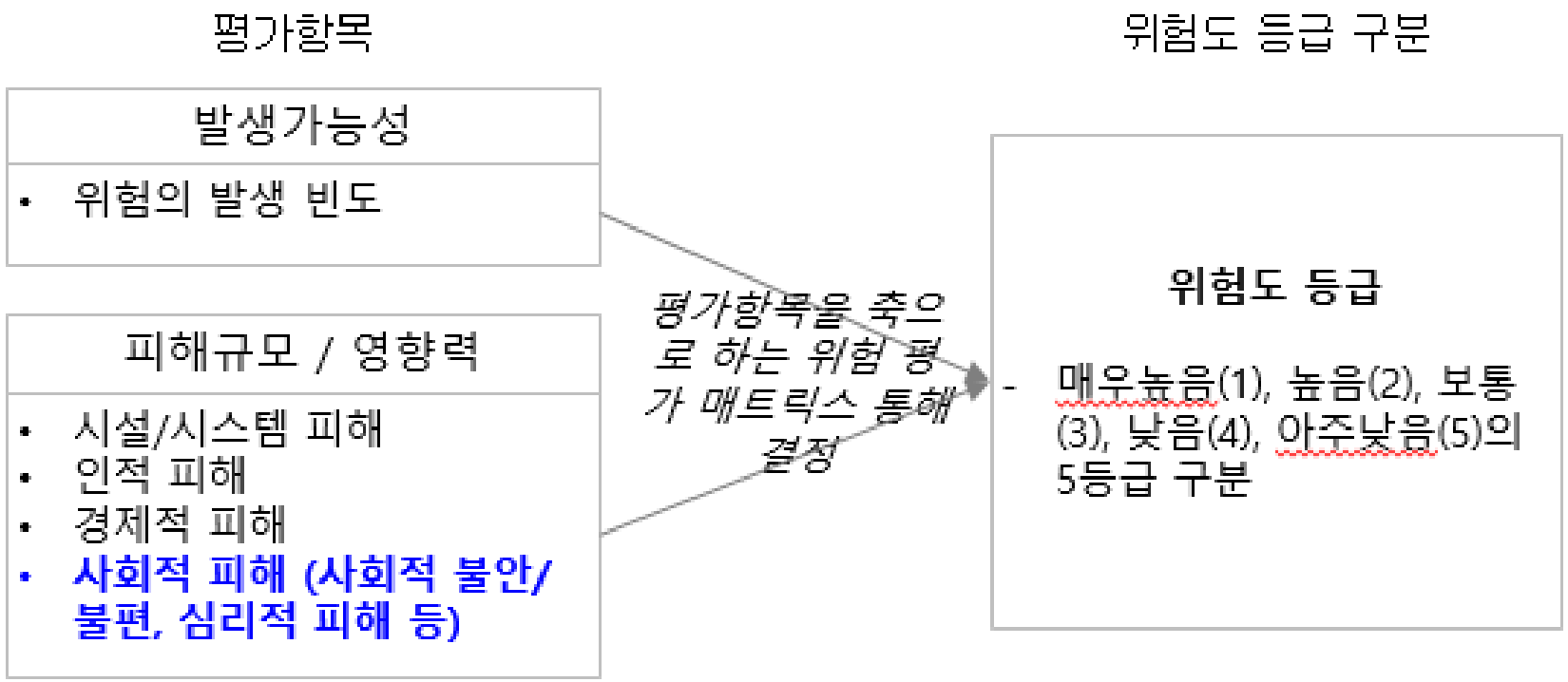
분야별	지 정 기 준
에너지	전력·석유·가스 공급에 필요한 생산·공급시설과 비축시설
정보통신	교환기 등 주요 통신장비가 집중된 시설 및 정보통신 서비스의 전국 상황 감시시설 국가행정을 운영·관리하는 데에 필요한 기간망과 주요 전산시스템
교통수송	인력 수송과 물류 기능을 담당하는 체계와 실제 운용하는 데에 필요한 교통·운송시설 및 이를 통제하는 시설
금융	은행 및 투자매매업·투자중개업을 운영하는 데에 필요한 시설이나 체계
보건의료	응급의료서비스를 제공하는 시설과 이를 지원하는 혈액관리 업무를 담당하는 시설
원자력	원자력시설의 안정적 운영에 필요한 주제어장치(主制御裝置)가 집중된 시
환경	「폐
정부중요시설	중앙행
식용수	식용수
문화재	「문화 재청
공동구	「국토 행정안 인정하



자료 : 국가기반체계 보호계획 수립지침(2017)

국가기반시설 관리 (위험평가 기준)

● 재난 및 안전관리 기본법 제26조의 2(국가핵심기반의의 관리 등)



자료 : 국가기반체계 보호계획 수립지침(2017), 해양수산부 국가기반시설 보호 계획 (2018)

소프트웨어 진흥법

"소프트웨어안전"이란 외부로부터의 침해행위가 없는 상태에서 소프트웨어의 내부적인 오작동 및 안전기능(사전 위험분석 등을 통하여 위험발생을 방지하는 기능을 말한다) 미비 등으로 발생할 수 있는 사고로부터 사람의 생명이나 신체에 대한 위험에 충분한 대비가 되어 있는 상태를 말한다.

제30조(소프트웨어안전 확보) ① 정부는 소프트웨어안전 확보를 위한 시책을 마련할 수 있다.
② 과학기술정보통신부장관은 다음 각 호의 사항을 포함하는 소프트웨어안전 확보를 위한 지침을 정하여 고시하여야 한다.
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 소프트웨어안전에 관한 기술기준을 수립하는 경우 제2항에 따른 지침 또는 국제표준 등을 고려하여야 한다.

제31조(소프트웨어안전 산업 진흥 등) 과학기술정보통신부장관은 소프트웨어안전 산업을 진흥하고 국가 전반의 소프트웨어안전을 확보하기 위하여 다음 각 호의 사업을 추진할 수 있다.
1. 소프트웨어안전 기술 연구
2. 소프트웨어안전 인력 양성
3. 소프트웨어안전 산업 기반 조성
4. 소프트웨어안전 관리 지원 및 안전사고 대응 지원
5. 소프트웨어안전 정보 축적 및 활용
6. 그 밖에 대통령령으로 정하는 사업

소프트웨어안전 증진 방안

소프트웨어안전 증진 방안

- **소프트웨어 관련 사고 발생 초기**
  - 소프트웨어안전 문화 강화

- **소프트웨어안전이 시스템안전의 일부로 포함**
  - 소프트웨어안전 산업 독립

- **소프트웨어안전 전문가 부족**
- **소프트웨어안전 관련 기술 미성숙**
  - 소프트웨어안전 산업 활성화

- **소프트웨어안전 확보 비용 과다**
  - 위험 평가 및 위험 수준에 따른 안전 활동

감사합니다