숲 산업 안전성 확보를 위한 SW의 역할과 과제

2019-04-12

송 지 환 선임연구원

SPRi 소프트웨어정책연구소

숲 산업? 안전성? 소프트웨어?

" ①숲 산업 ②안전성 확보를 위한 ③SW의 역할과 과제 "

①숲 산업 = 안전 중요 산업 ∪ the other 산업

②안전이란?

안전

국가안전관리기본계획, 행정안전부

자연적 혹은 인적·인위적 위험요인이 없거나,

이러한 위험 요인에 대한 **충분한 대비**가 되어 있는 상태

Safety vs. **Security** - 안전의 영문용어 비교

영문표기	Safety	Security
개념	우발적이거나 또는 자연적인 원인에 의해 발생하는 비의도적인 피해(damage) 또는 파괴로부터 인명과 자산의 보호	의도적이거나 또는 악의 있는 행위나 상황에 의한 피해 또는 파괴로부터 인명과 자산을 보호
판단기준 (사고 원인)	• 비의도적(unintentional) • 우연적(accidental) • 자연적인(natural) 행위(act) 또는 상황	• 의도적(intentional) • 고의적·계획적(deliberate) • 악의적(malicious) 행위 또는 상황
적용대상 및 범위 (예시)	• 우발적 사고(accidental events) • 차량 안전(vehicle safety) • 작업장 위험(hazards at work) • 신체적·심리적·사회적·물질적 위해 (physical·psychological·social·material harm) 등	• 테러(terrorist threat or attach) • 탈취(hijacking) • 반달리즘(vandalism) • 범죄활동(criminal activity) • 불법행위(illeagal act) 등
현행 주요 한글표기	안전(安全), 안전성(安全性), 위험방지장치, 안전장치	안전(安全), 보안(保安), 안보(安保), 안전보장(安全保障), 안심, 보호, 방호, 경비부문

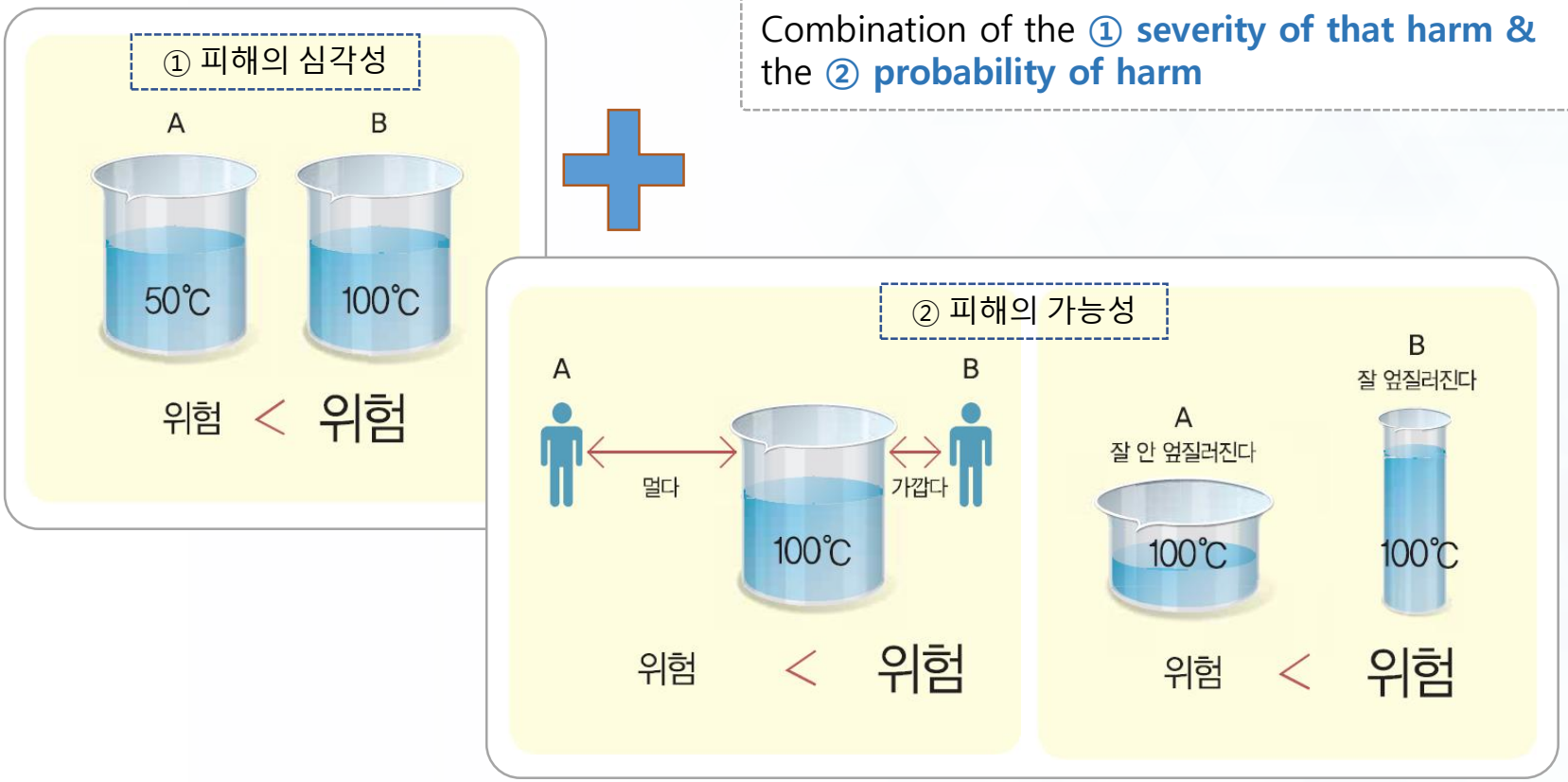
출처 : 배대식 (2009) 대학캠퍼스의 생활안전 위기관리 체계 연구 재인용

위험(risk)이란?

피해의 심각성과 가능성 개념 포함 (정량적 분석 가능)

Risk(위험)

Combination of the ① **severity of that harm** & the ② **probability of harm**



과거 안전중요(관련) 산업의 사고 책임자?

안전중요(관련)산업

* Safety-critical(related)

개발

- HW 결함이 없도록 설계
  * 위험분석
- 안전한 HW 개발에 집중
  * 이중화 등
- **중요한 제어 기능은 사람이 수행**,
  단순 제어 및 조력 기능은 HW

운영

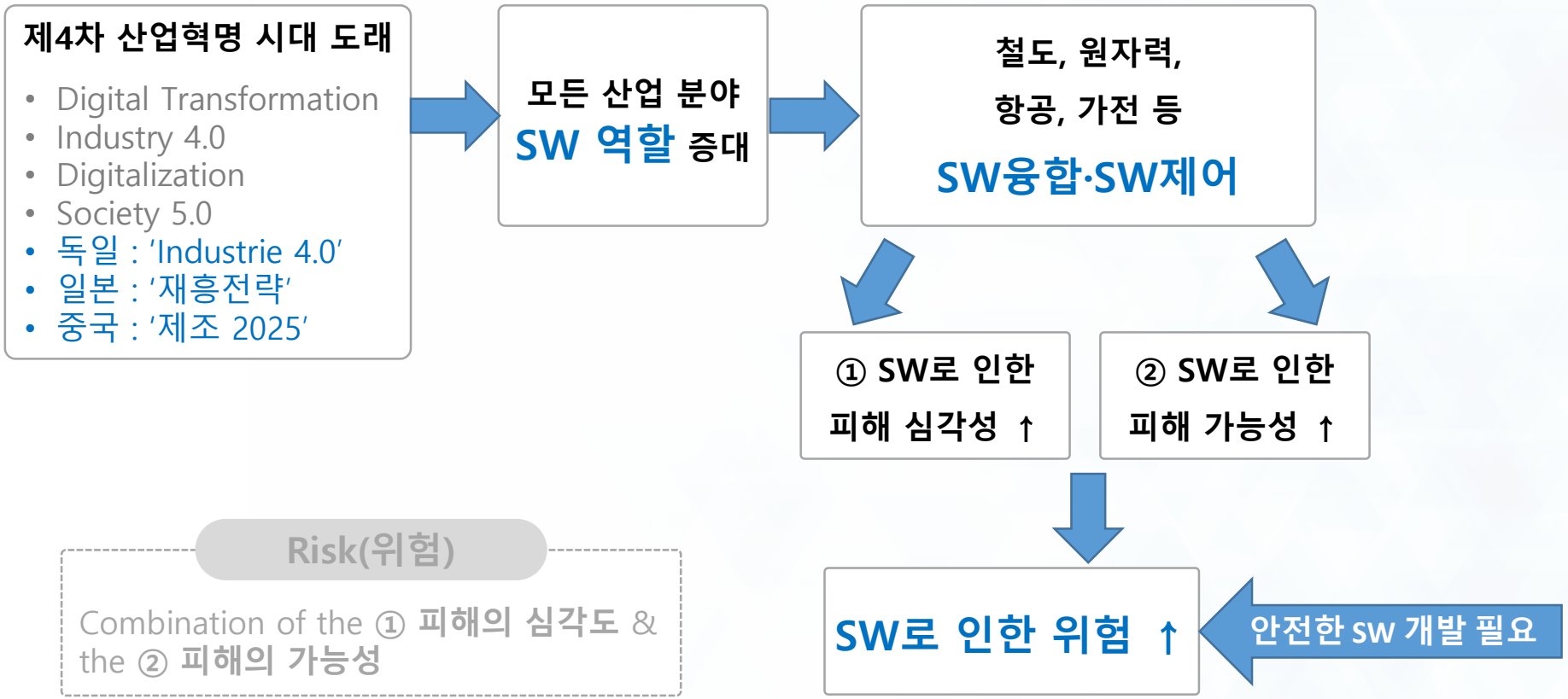
- HW 관리(기름칠, 부품교체 등)
- 안전 관련 절차 마련 및 훈련

사고 책임자

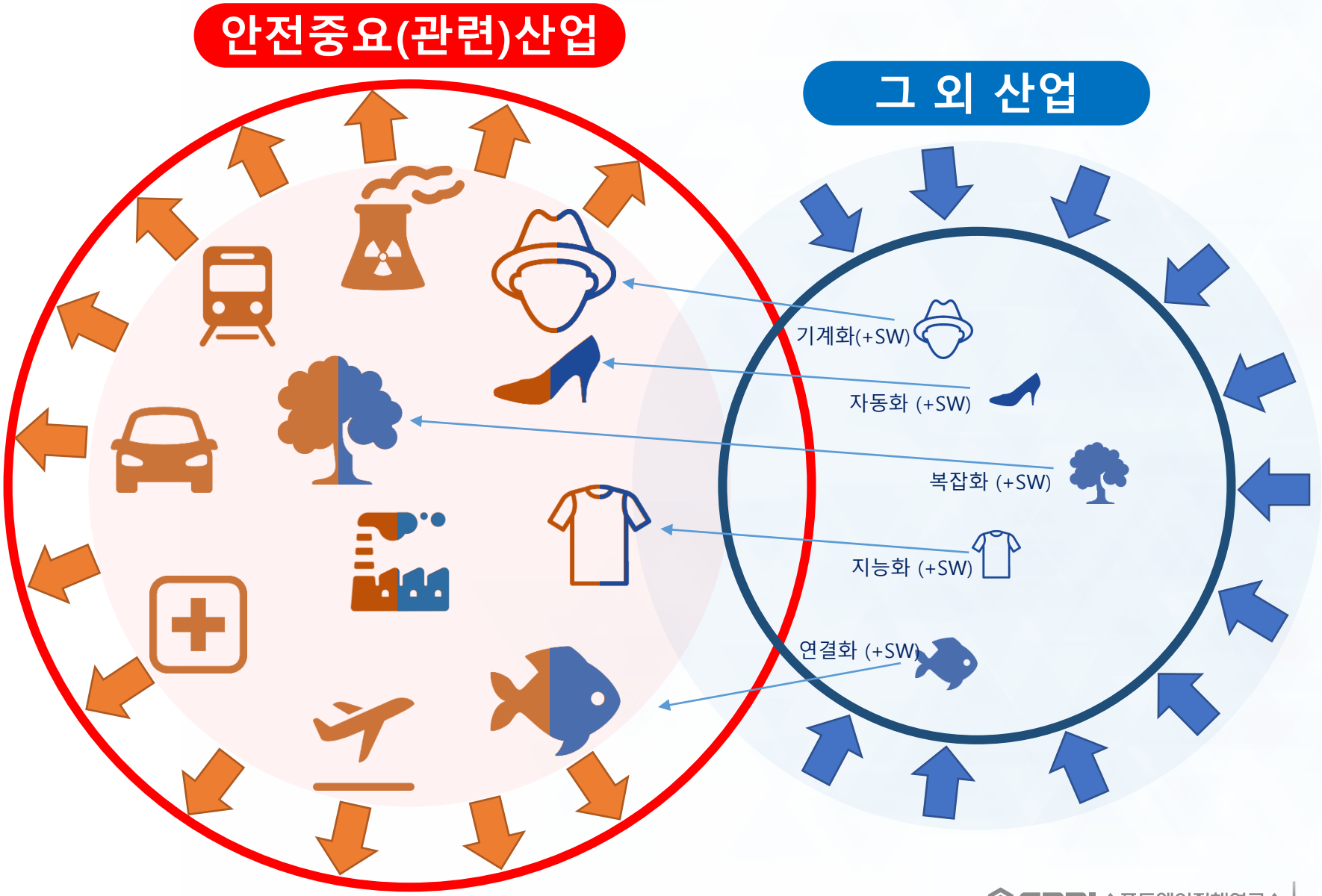
- HW 오류 : 제작(개발)사(제조물책임)
- 운영실수 : 운영자(사용자) (人災)

제4차 산업혁명 시대의 도래

SW로 인한 위험 증가 ⇒ 사고 발생 가능성 증대



제4차 산업혁명 시대 안전산업의 변화



③(제4차 산업혁명 시대) 사고 책임자는?

개발

- HW, **SW** 결함이 없도록 설계
  * 위험분석
- 안전한 HW 및 **SW** 개발
- **제어기능 : 사람 or SW**

운영

- HW 관리(기름칠, 부품교체 등)
- **SW 운영 관리(업데이트, 데이터무결성 등)**
- 안전 관련 절차 마련 및 훈련

사고 책임자

- HW/**SW** 오류 : 제작(개발)사
  * 제조물 책임
- 운영실수 : 운영자(사용자) (人災)

SW 결함으로 인한 사고사례

Volvo 자동긴급제동장치 기능 오류

* Autonomous Emergency Braking

출처 : Youtube

SW 결함으로 인한 사고사례 (계속)

Tesla Autopilot 기능 오류

출처 : Youtube

SW 결함으로 인한 사고사례 (계속)

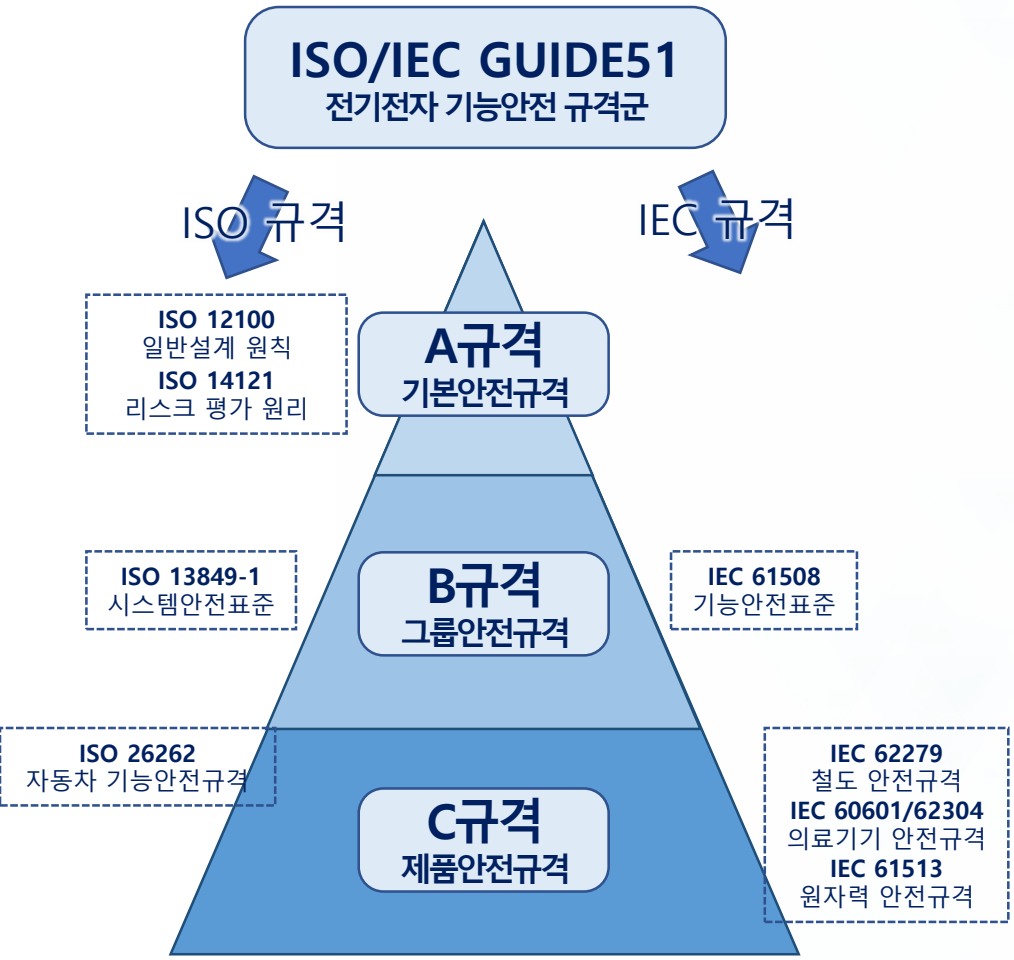
Boeing 737 MAX 8 MCAS 기능 오류

* Maneuvering Characteristics Augmentation System

출처 : Google 검색

국제표준에서 안전이란?

수용할 수 없는 위험에서 벗어난 것



ISO/IEC GUIDE51

- 안전 : 수용할 수 없는 **위험**에서 벗어난 것
  3.1 safety: freedom from unacceptable **risk**

IEC 61508

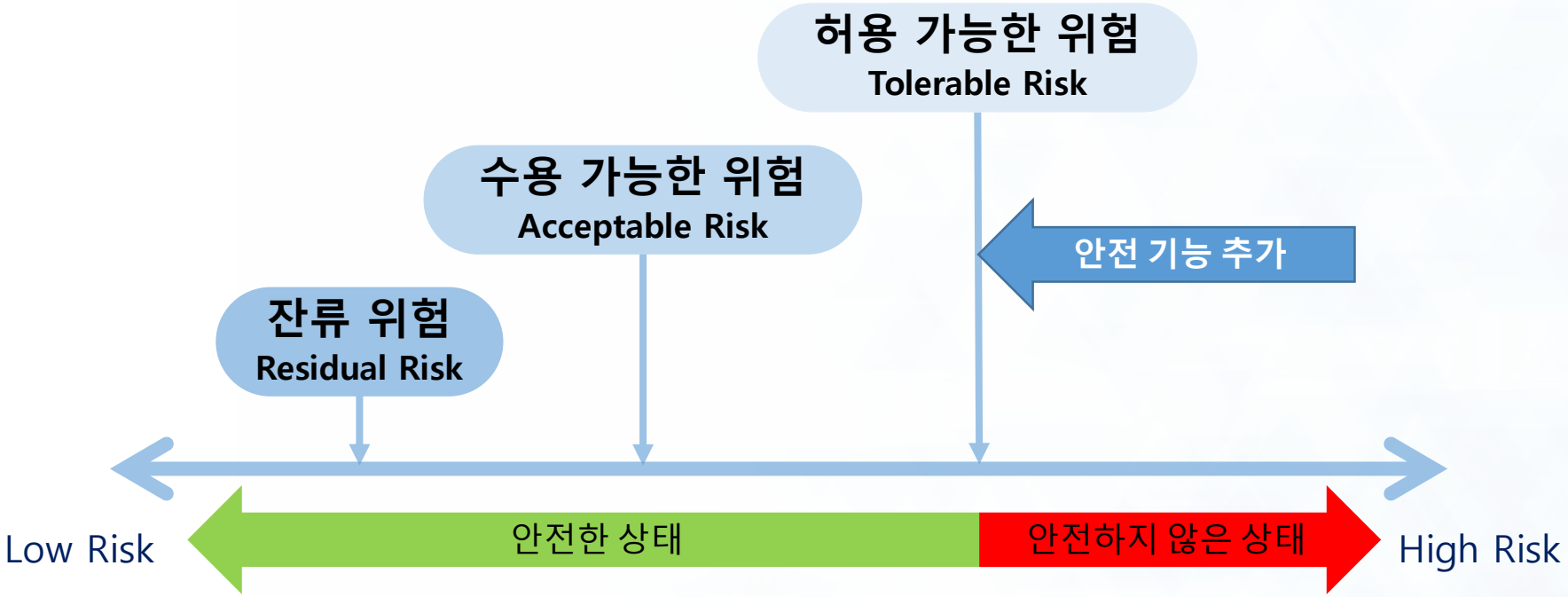
- ISO/IEC GUIDE51의 안전 정의 차용
  Part4 > 3.1.11 safety : freedom from unacceptable **risk**

ISO 26262

- 안전 : 불합리한 **위험**의 부재
  Part 1 > 1.103 safety: absence of unreasonable **risk**

기능 안전 (functional safety)

시스템 / HW / SW 안전 확보 방법



기능 안전? No

- 전선에 고온에 견딜 수 있도록 특수한 피복을 입힘 → 화재 예방

기능 안전? Yes

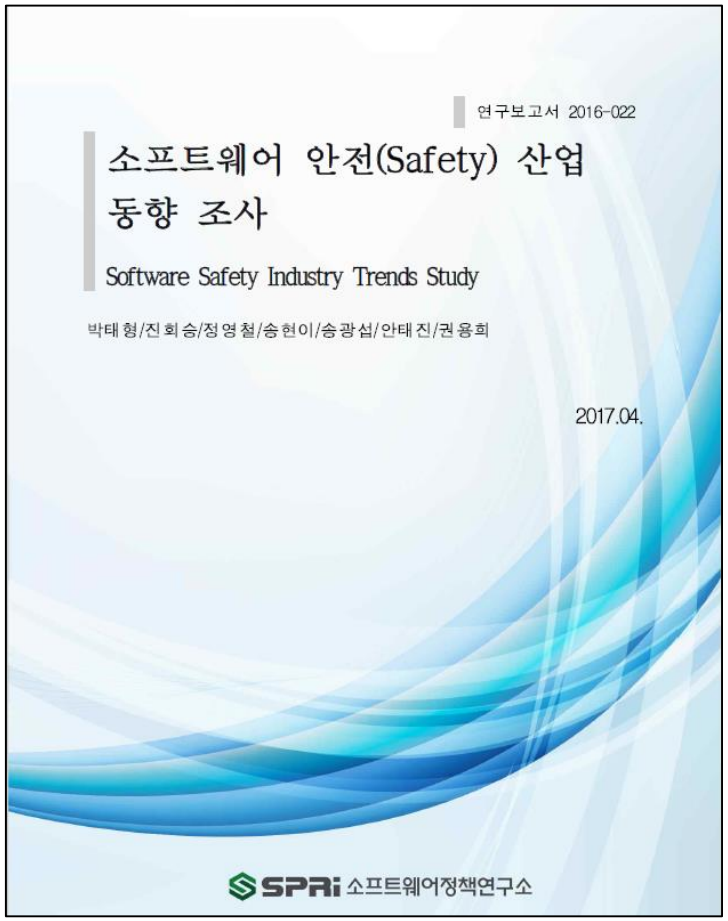
- 전선의 온도가 일정 수준 이상 올라가는 것을 **감지**하여 전기를 **차단** → 화재 예방

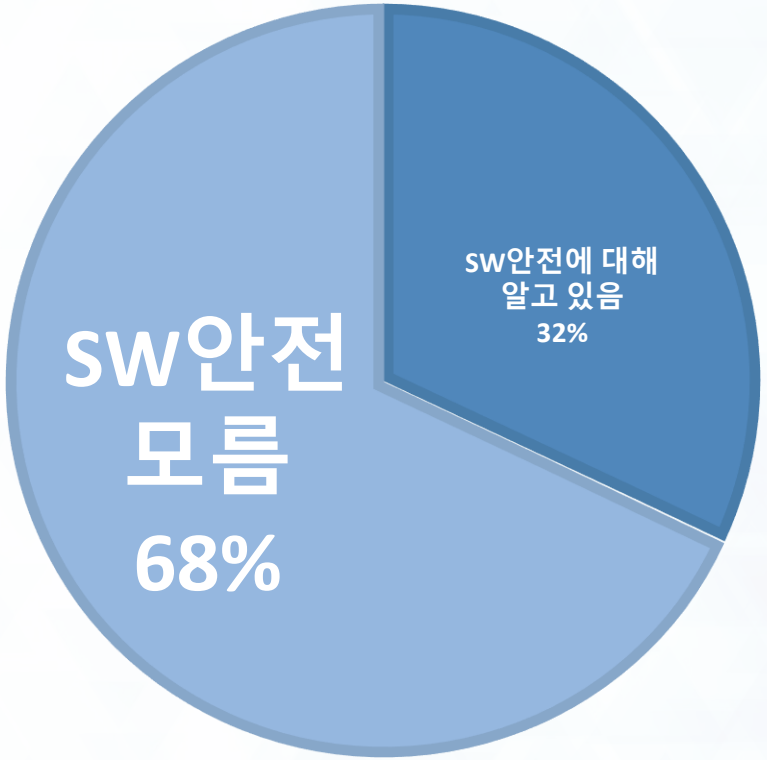
안전한 SW 개발이란?


요구사항 분석
Requirement Analysis
• 위험분석 수행
위험원 식별
위험 평가
위험 제거/저감
위험 확인
• 안전요구사항(SRS) 도출
* Safety Requirement Specification
• SRS를 설계 반영 및 확인
설계
Design
구현
Implementation
• SW안전 코딩 규칙
검증
Testing
• 정적/동적 검증
운영
Operating
• 훈련, 데이터 무결성
폐기
Disposal
위험 추적/관리

SW안전에 대한 인식은? (2016년 기준)

SW품질, 정보보안 대비 SW안전에 대한 인식이 낮음





19개 개발기업 심층인터뷰
(2016 소프트웨어 안전(safety) 산업 동향 조사, SPRi, 2016)

SW안전 vs. SW품질 vs. 정보보안

	SW안전	SW품질	정보보안
목 적	시스템 내부적인 위험으로부터 사람 신체, 생명을 보호하는 것	주문자(사용자) 요구사항의 정상동작 보장	시스템 외부적인 위험으로부터 내부 정보를 보호하는 것
원 인	시스템 내부측면의 위험 - HW 오류 - SW 오류 - 환경적 위험	요구사항 미달(미충족) - 기능적 요구사항 미달 - 비기능적 요구사항 미달	외부로부터의 침입(공격) - 인적 침입 - 물리적 침입 - SW적 침입
미충족 결과	- 사람의 신체 상해 - 사망	- 시스템 미동작 - 기능 오류 - 사용불편	- 정보 유출, 손실 - 정보접근 제한 - 제어권 상실
국제표준	- (산업전반) IEC 61508 - (철도) IEC 62279 - (의료) IEC 62304 등	- ISO/IEC 9126-2	- IEC 27000 시리즈 - IEC 15408

SW안전 인식 제고 활동 수행

SW안전 국제 컨퍼런스 매년 개최 (2015-2018)

제1회 2015.12.01 COEX

- 해외석학 : 3명
- 국내전문가 : 4명

제2회 2016.11.29 COEX

- 해외석학 : 4명
- 국내전문가 : 4명

제3회 2017.11.23 COEX

- 해외석학 : 5명
- 국내전문가 : 4명

제4회 2018.11.29 COEX

- 해외석학 : 3명
- 국내전문가 : 8명

해외 석학 15명

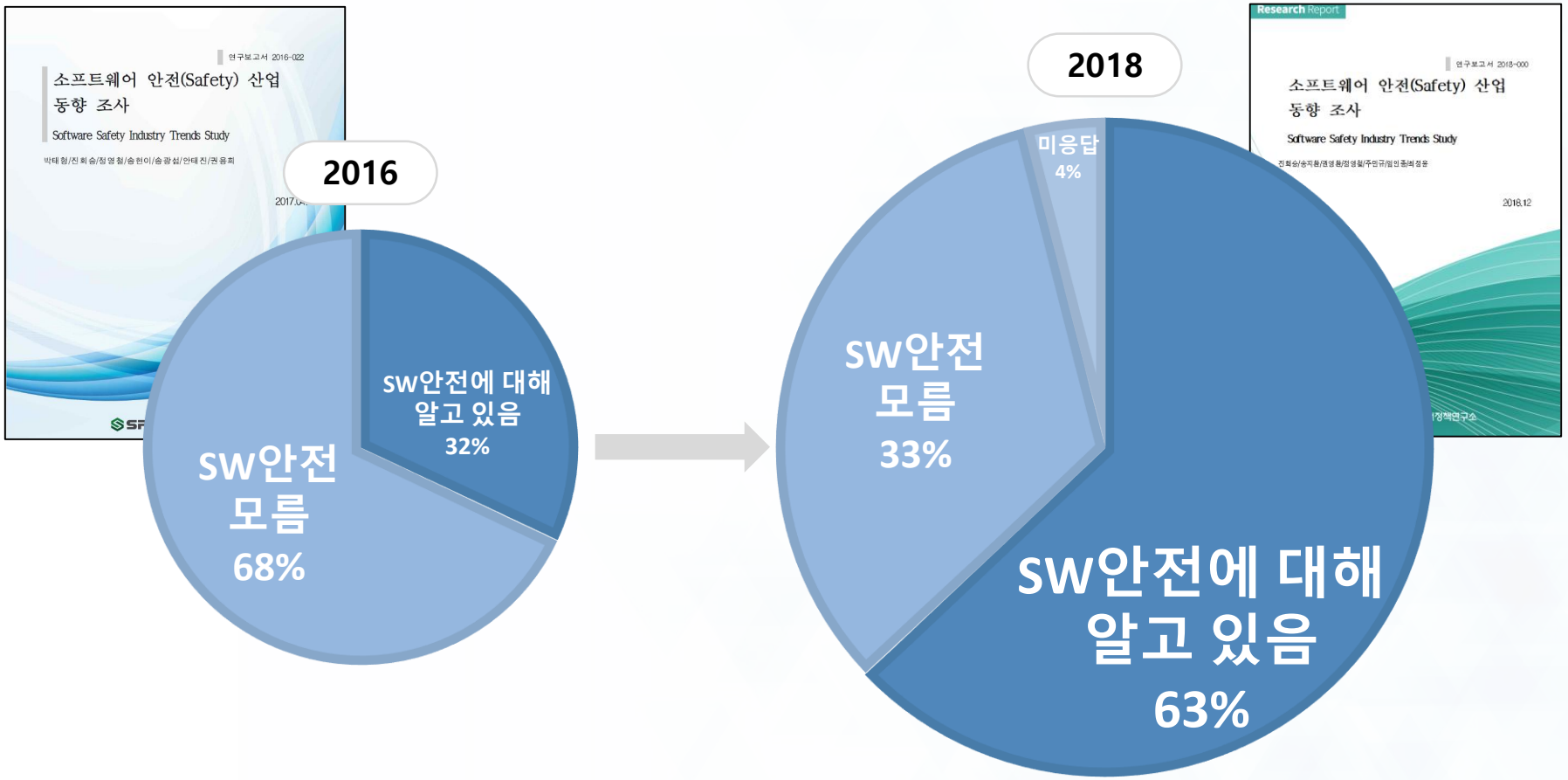
국내 전문가 20명

SW안전 인식 제고 활동 수행 (계속)

SW안전 관련 포럼, 정책 토론회, 전문가 간담회, 세미나 등 개최

SW안전에 대한 인식 재조사 (2018년 기준)

(SPRi의 노력으로?) SW안전에 대한 인식이 높아짐



19개 개발기업 심층인터뷰
(2016 소프트웨어 안전(safety) 산업 동향 조사, SPRi, 2016)

72개 개발기업 심층인터뷰
(2018년 국내 SW안전 산업 동향조사, SPRi, 2018)

법·제도 관점에서 SW안전, SW 품질, 보안 비교

정보보안 및 SW품질 법령으로 규정, SW안전 관련 법령은 無

정보보안

- 정보통신기반 보호법
- 정보통신망법
  정보통신망 이용촉진 및 정보보호 등에 관한 법률
- 정보보호산업법
  정보보호산업의 진흥에 관한 법률
- 개인정보 보호법

SW품질

- 소프트웨어산업 진흥법

  제13조(품질인증) ① 과학기술정보통신부장관은 소프트웨어의 품질확보 및 유통 촉진을 위하여 소프트웨어에 관한 품질인증을 실시할 수 있다.

SW안전

- **법령 없음**
- 철도시설의 기술기준
  국토교통부고시 제2019-132호, 2019. 3. 21.

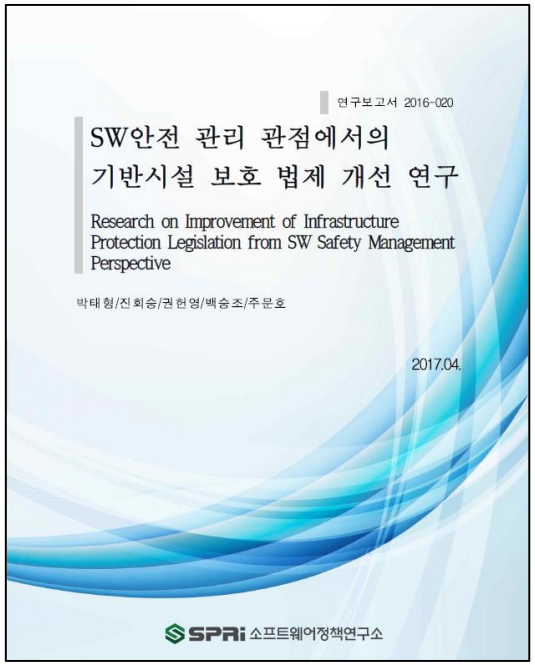
  제96조(철도신호제어설비의 구조)
  철도신호제어설비의 주요 장치를 제작·설치할 때에는 다음 각 호의 사항을 준수하여야 한다.
  … 2. 장치를 설계·개발하는 과정에서 오류 등이 발생되지 않도록 **소프트웨어의 분석·시험 및 검증을 수행**할 것 …
- 항공기 기술기준
  국토교통부고시 제2018-452호, 2018. 7. 23.

  Part1(총칙) 1.7.3 소프트웨어 인증
  모든 시스템 소프트웨어 본 기술기준에서 요구하는 안전수준에 적합하고, 계통 내에서 의도하는 기능으로 작동되도록 설계되고, 검증되어야 한다. **소프트웨어의 설계 및 시험은 RTCA/ DO-178 또는 EUROCAE ED12에 따른다.**

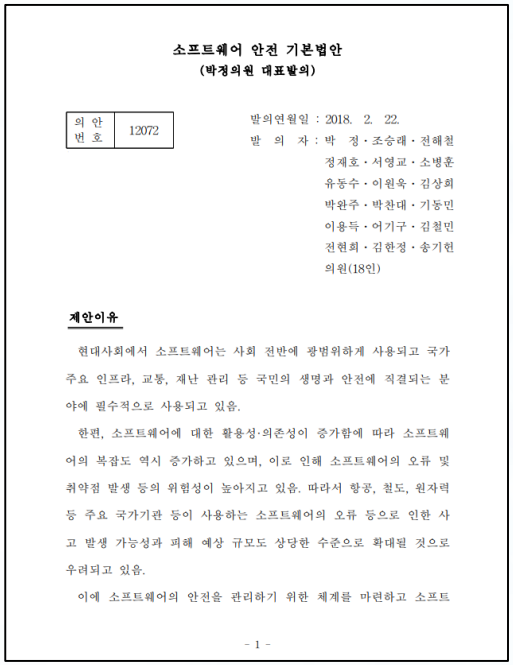
SW안전 관련 법제화 노력

기반 시설 보호를 위한 SW안전 법제 개선 연구 → 법안발의로

2016년 SPRi 연구결과



소프트웨어 안전 기본법안



소프트웨어 안전 기본법안
(박정의원 대표발의)

의안 번호	12072

발의연월일 : 2018. 2. 22.
발 의 자 : 박 정·조승래·전해철 정재호·서영교·소병훈 유동수·이원욱·김상희 박완주·박찬대·기동민 이용득·어기구·김철민 전현희·김한정·송기헌 의원(18인)

제안이유

현대사회에서 소프트웨어는 사회 전반에 광범위하게 사용되고 국가 주요 인프라, 교통, 재난 관리 등 국민의 생명과 안전에 직결되는 분야에 필수적으로 사용되고 있음.

한편, 소프트웨어에 대한 활용성·의존성이 증가함에 따라 소프트웨어의 복잡도 역시 증가하고 있으며, 이로 인해 소프트웨어의 오류 및 취약점 발생 등의 위험성이 높아지고 있음. 따라서 항공, 철도, 원자력 등 주요 국가기관 등이 사용하는 소프트웨어의 오류 등으로 인한 사고 발생 가능성과 피해 예상 규모도 상당한 수준으로 확대될 것으로 우려되고 있음.

이에 소프트웨어의 안전을 관리하기 위한 체계를 마련하고 소프트

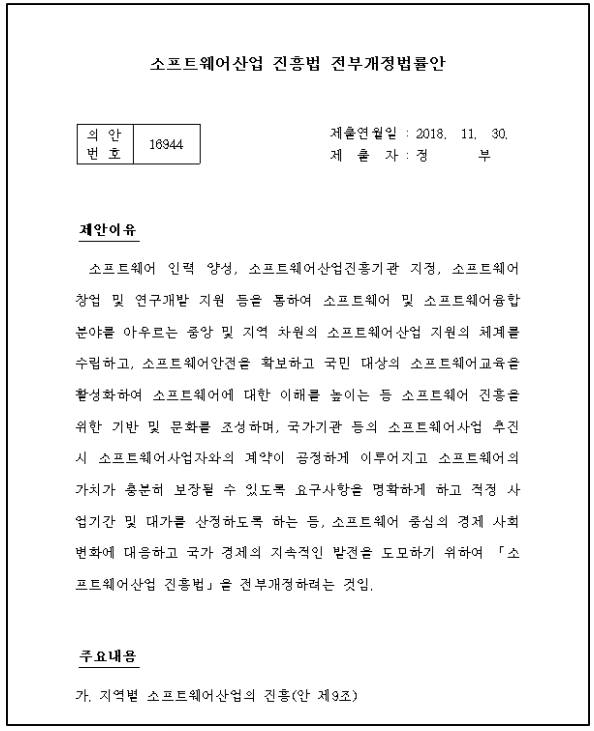
- 1 -

- 의안번호 : 2012072 (2018-02-22)
- 제안자 : 박정의원 대표발의(참여의원 18인)
- 소위회부 (2018-09-19)

SW안전 관련 법제화 노력 (계속)

소프트웨어산업 진흥법 전부개정안에 SW안전 조문 추가

소프트웨어산업 진흥법 전부개정법률안



소프트웨어산업 진흥법 전부개정법률안

의안 번호	16944

제출연월일 : 2018. 11. 30.
제 출 자 : 정 부

제안이유

소프트웨어 인력 양성, 소프트웨어산업진흥기관 지정, 소프트웨어 창업 및 연구개발 지원 등을 통하여 소프트웨어 및 소프트웨어융합 분야를 아우르는 중앙 및 지역 차원의 소프트웨어산업 지원의 체계를 수립하고, 소프트웨어안전을 확보하고 국민 대상의 소프트웨어교육을 활성화하여 소프트웨어에 대한 이해를 높이는 등 소프트웨어 진흥을 위한 기반 및 문화를 조성하며, 국가기관 등의 소프트웨어사업 추진 시 소프트웨어사업자와의 계약이 공정하게 이루어지고 소프트웨어의 가치가 충분히 보장될 수 있도록 요구사항을 명확하게 하고 적정 사업기간 및 대가를 산정하도록 하는 등, 소프트웨어 중심의 경제 사회 변화에 대응하고 국가 경제의 지속적인 발전을 도모하기 위하여 「소프트웨어산업 진흥법」을 전부개정하려는 것임.

주요내용

가. 지역별 소프트웨어산업의 진흥(안 제9조)

- 의안번호 : 2016944 (2018-11-30)
- 제출자 : 정부(과기부)
- 과방위 상정 (2019-03-14)

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

8. "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.

SW안전 관련 법제화 노력 (계속)

소프트웨어산업 진흥법 전부개정안에 SW안전 조문 추가

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

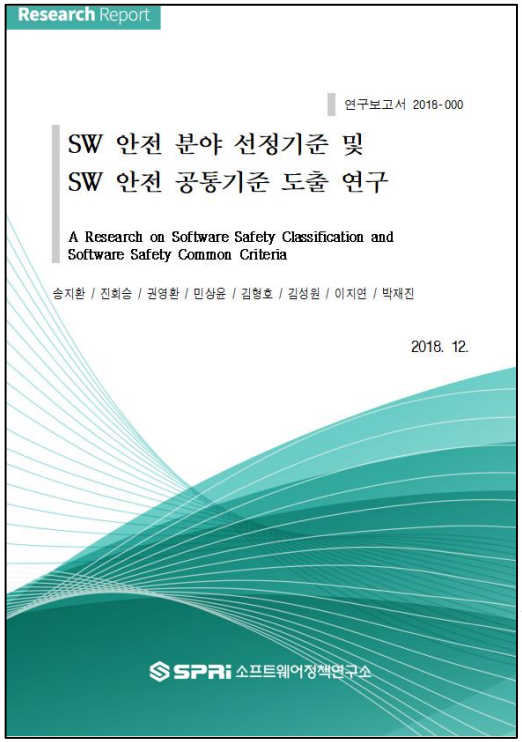
③ 중앙행정기관의 장은 소관 분야의 기술기준을 수립하는 경우 제2항에 따른 지침 또는 국제표준 등을 고려하여야 한다.

제30조(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

SW안전 분류 및 공통 기준 도출 연구 수행

2018년 SPRi 연구결과



SW안전 분류 도출

SW안전통제등급 SW safety control level \ 위험 심각도 Severity	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

SW안전 공통 기준 도출

단계	안전 활동	SSRI1		SSRI2		SSRI3		SSRI4		SSRI5	
		필수 유무	적용 기법	필수 유무	적용 기법	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	O	• Structured natural language	X	N/A
	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	O	• either Software Fault Tree analysis or Software Failure mode and effects analysis	X	N/A
	Review of safety requirements	O	• Inspection	O	• Inspection	O	• Walkthrough	O	• Walkthrough	X	N/A
Design	Development of software safety design	O	• Hierarchical structure of software components	O	• Hierarchical structure of software components	O	• Hierarchical structure of software components	X	N/A	X	N/A
	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	X	N/A	X	N/A
	Review of safety design	O	• Inspection	O	• Inspection	O	• Walkthrough	X	N/A	X	N/A
Implementation	Safety analysis of code	O	• Safety code analysis	X	N/A	X	N/A	X	N/A	X	N/A
	Review of safety code	O	• Inspection	X	N/A	X	N/A	X	N/A	X	N/A
Software unit test	Development of safety related unit test case	O	·nalysis of safety requirements ·eneration and analysis of uivalence classes • Analysis of boundary values	O	• Analysis of safety requirements • Generation and analysis of equivalence classes • Analysis of boundary values	X	N/A	X	N/A	X	N/A
	Review of safety related unit test case	O	• Inspection	O	• Inspection	X	N/A	X	N/A	X	N/A
	Analysis of test coverage at software unit level	O	• Statement coverage • Branch coverage • Condition coverage				`A	X	N/A	X	N/A
	Safety related unit test	O	• Requirements based test • Fault injection test				`A	X	N/A	X	N/A
	Review of safety related unit test result	O	• Inspection	O	• Inspection	X	N/A	X	N/A	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	X	N/A	X	N/A
	Review of safety related software integration test case	O	• Inspection	O	• Inspection	O	• Walkthro			X	N/A
	Analysis of test coverage at software architectural level	O	• Function coverage • Call coverage	O	• Function coverage • Call coverage	O	• Function coverage	X	N/A	X	N/A
	Safety related software integration test	O	• Requirements based test • Fault injection test	O	• Requirements based test • Fault injection test	O	• Requirements based test	X	N/A	X	N/A
	Review of safety related software integration test result	O	• Inspection	O	• Inspection	O	• Walkthrough	O	• Walkthrough	X	N/A
ware 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	O	• Analysis of safety requirements • Generation and analysis of equivalence classes • Analysis of boundary values	X	N/A
	Review of safety related software test case	O	• Inspection	O	• Inspection	O	• Walkthrough	O	• Walkthrough	X	N/A

안전활동 목록 제공

수행 해야 하는 안전 활동에 대해 적용 가능한 기법

SSRI 별 필수적으로 적용 해야하는 안전활동 구분

(과제) SW안전 저변 확대를 위한 강소기업 육성

AS-IS

SW안전 관련 전문기업 부족

SW안전 관련 인프라 부족

⇒ 글로벌 경쟁력이 낮음

- **SW안전 전문 기업 극소수**
  - ✓ SW공학 기반 품질 컨설팅 기업이 SW안전 분야를 병행하는 경우가 대부분임
- **국내 중소기업의 SW안전 역량 부족**
  - ✓ 국내 SW개발 기업 및 안전 관련 국가기반 시설 종사자 중 SW안전 전문가는 극소수
  - ✓ SW안전 관련 인프라 역시 부족하여 중소기업이 SW안전 역량을 확보하기 힘든 상황
- **해외 기업의 국내 SW안전 시장 독점**

TO-BE

SW안전 분야에 대한 포괄적·집중적 지원

⇒ SW안전 강소기업을

글로벌 히든챔피언으로 육성

- **SW안전 관련 기술·인적·인프라 균형적 지원**
  - ✓ 국내 중소기업이 성장에 필요한 역량 및 자원이 균형적으로 확보될 수 있도록 포괄적·중장기적 지원 추진
  - ✓ 기술개발 R&D, 교육 및 글로벌 기업 교류를 통한 인력양성, SW검증체계·인프라 구축, 실증사업 등 통합지원체계를 마련하여 집중 육성
- **SW안전 검증·평가·개발 기업 선정 및 육성**
  - ✓ 산업공통분야에 대해 검증·평가 기업과 의료·제조·가전 등 글로벌 시장이 확보된 분야에 대해 개발 기업을 시범 육성

(과제) SW안전 확보로 안전한 대한민국 실현

AS-IS

SW안전 선진국 대비
국가 SW안전 기반 및 역량 부족
⇒ SW안전 사고로 인한 공공 안전 위협

- **안전중요 시설의 SW안전 관리 체계 부실**
  - ✓ 철도, 항공, 원자력 등 일부 분야에 국한되어 SW안전을 관리
  - ✓ 공공정보시스템 전반에 대한 SW안전 관리 체계 부재
- **SW안전 관련 인력 및 기술 부족**
  - ✓ SW안전 검증 전문 기업 및 인력 부족
  - ✓ 국내SW 안전 기술 경쟁력 및 표준인지도 열악

TO-BE

예방중심의 SW안전 능동적 관리
全 산업 SW안전 확보체계 구축
⇒ 디지털전환시대의 안전 확보

- **SW안전 관련 조직 및 법·제도 정비**
  - ✓ 공공시스템의 SW안전 확보를 위해 범 부처 협의 기관을 설립
  - ✓ 부처간 업무협의를 통해 SW안전 관련 법·제도 정비
- **국가기반시설 SW를 선정하여 집중관리**
  - ✓ 철도, 항공, 의료 등 국민생명에 큰 영향을 주는 분야의 SW에 대해 안전 대진단 실시
- **생애주기 관점의 SW안전 확보 체계 구축**
  - ✓ SW안전 요구사항이 명확히 정의/관리될 수 있도록 SW안전관리시스템 구축
- **SW안전 최소 확보 방안 마련 및 확산**

감사합니다
Q & A