SW WEEK 2017



# SW 안전 사회 구축을 위한 기반 조성 방안

2017-11-23

**송 지 환** 선임연구원

SPRi 소프트웨어정책연구소

# 발표 내용

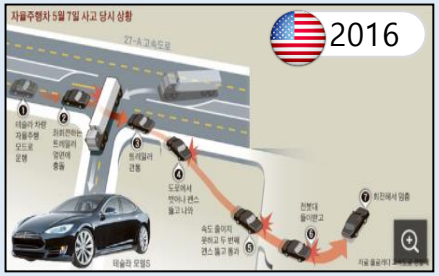
- SW 안전 사회의 정의
- 해외 주요국의 SW 안전 수준
- 우리의 SW 안전 현실은?
- SW 안전 사회 구축을 위한 기반 조성 방안

# SW 안전의 중요성

## SW 안전 결함 시 막대한 **사회 · 경제적 손실**과 **인명피해** 발생

### 테슬라 사망 사고

오토파일럿 시스템
오작동으로 운전자 사망




**오토파일럿 시스템**이 햇빛과 트레일러의 흰색을 구분하지 못함

**운전자 사망**

### 토요타 급발진 사고

자동차 급발진으로
운전자, 동승자 사망 등


Bit-flip으로 인한 **전자 스로틀 제어 SW 문제**

**총 40억 달러**, 미국 법무부에 벌금 12억 달러, 400여 건의 급발진 소송 중 338건 합의 등

### 상왕십리 전동차 추돌 사고

상왕십리역 열차 간
15Km/h로 추돌로 시민 부상


**신호기 고장**으로 자동정지장치 시스템 작동하지 않음

**승객 388명 중경상**
**28억여 원 재산 피해**

### 윈저우 고속철 탈선 사고

중국 윈저우에서 고속열차
추돌사고로 대규모 사망/부상 발생


낙뢰로 인한 **열차제어시스템 오류** 발생, 후속 열차에 대해 잘못된 진입 신호 유도

객차 2량이 선로에서 벗어나 추락
**승객 40명 사망, 192명 부상**

출처 : 뉴욕타임즈, 연합뉴스, 중앙일보

# 안전이란?

## 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)<br>• 우연적(accidental)<br>• 자연적인(natural) 행위(act) 또는 상황 | • 의도적(intentional)<br>• 고의적·계획적(deliberate)<br>• 악의적(malicious) 행위 또는 상황 |
| 적용대상 및 범위 (예시) | • 우발적 사고(accidental events)<br>• 차량 안전(vehicle safety)<br>• 작업장 위험(hazards at work)<br>• 신체적·심리적·사회적·물질적 위해 (physical·psychological·social·material harm) 등 | • 테러(terrorist threat or attach)<br>• 탈취(hijacking)<br>• 반달리즘(vandalism)<br>• 범죄활동(criminal activity)<br>• 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

# SW 안전이란?

## SW 안전

IEEE 표준 1228-1994

전체 시스템의 안전 보장을 위하여 외부에 미치는 **위험 요소**를 **분석**하고 **제거**하여 **SW의 오류로 인한 사고를 예방**하는 것

SW 안전은 품질(quality)과 보안(security)의 상위 개념

### SW 품질

시스템의 효율적 운영을 위해서
기능성, 사용성, 유지보수성,
호환성의 구현을 목적으로 함

### SW 보안

SW가 올바르게 동작하도록
시스템 밖에서의 침입을 방지

## SW 안전성

SW정책연구소

사람의 신체나 생명에 위험을 발생시킬 가능성이 있는
SW에 대해 여러 위험요인의 발생을 방지하거나
이러한 위험요인에 **충분한 대비**가 되어 있는 상태

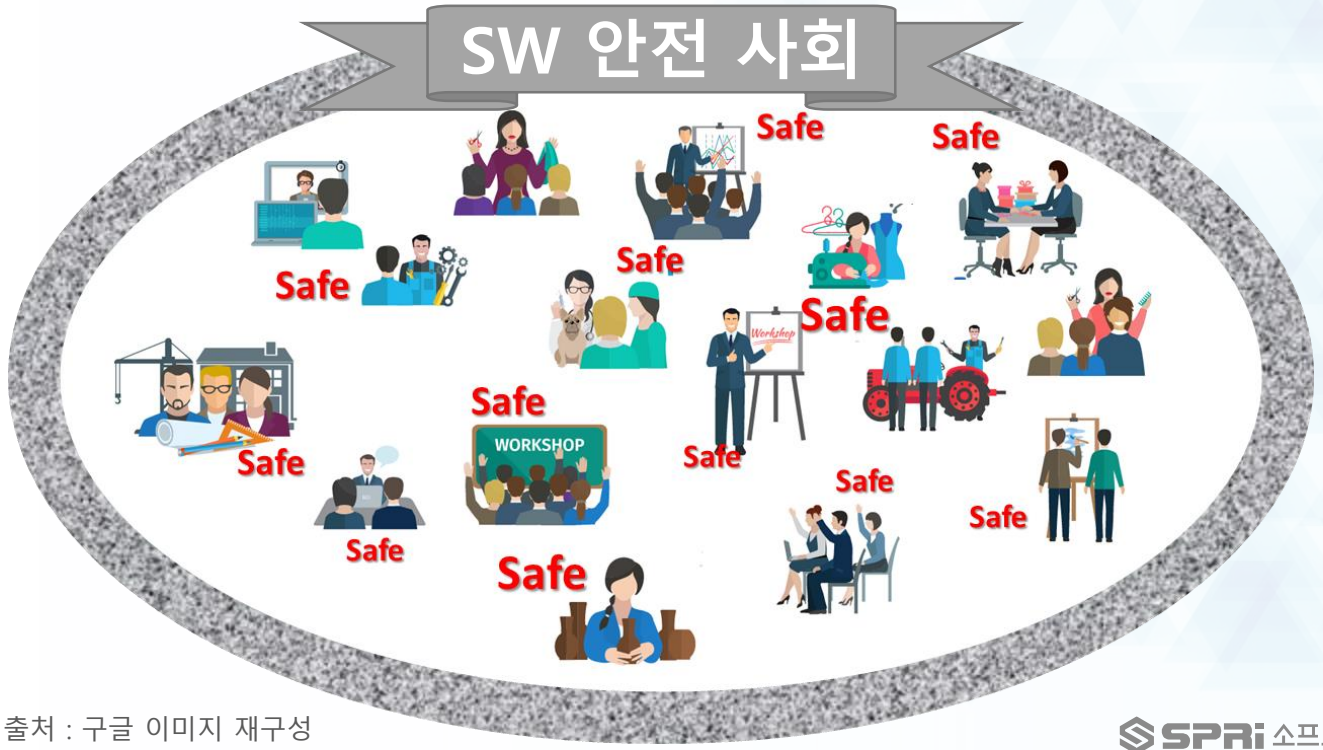
# SW 안전 사회

## SW 안전 사회

SW정책연구소

안전 필수 분야*의 시스템뿐만 아니라 SW 오류 발생 시 안전에 영향을 줄 수 있는 기기까지 **SW 안전성**이 확보되어 국민의 신체나 생명에 위해(危害)를 발생시킬 가능성이 낮은 **사회**

* 안전 필수 (safety critical) 분야 : 원자력, 항공, 철도, 의료 등 사고 발생 시 대규모 피해가 예상되는 분야




출처 : 구글 이미지 재구성

# 해외 주요국의 SW 안전 수준

## 全 산업에 SW 융합으로 SW 안전의 중요성 강화

- 안전 필수 산업에 자율화 기능 도입 증가 (항공 자율 비행, 자율 주행차 등)
- 다양한 산업의 전자시스템 및 SW 적용이 융·복합화 (Smart Factory, Robot, 의료, 조선 등)

## 산업별 주요 법에 국제 표준에 준하는 SW 안전 확보 명시

- 미국·유럽 등 세계 주요국은 민관이 협업하여 자동차·철도·에너지 등 주요 산업분야별 SW 안전 관련 국제표준을 제정
- SW 산업계가 이를 준용할 수 있도록 법·제도적 기반을 조성

## 안전 표준 구체화 및 상세화

- 추상적인 시스템 기능 안전표준이 상세화되고 SW 안전이 부각되는 방향으로 진화

## 국가 차원의 전문기관 설립

- 신뢰할 수 있는 SW 기술 확보 및 산업별 적용을 체계적으로 지원


'신뢰성향상전담기관' 설치운영(2014년까지 8.5억 파운드)


'소프트웨어고신뢰화센터' 개설(2013년)


'고신뢰성소프트웨어/시스템' 프로젝트(2015년 2억 달러)

# 해외 주요국의 SW 안전 수준 (계속)

## 주요 산업별 SW 안전 관련 **표준** 및 **법·제도** 현황

| 분야 | 주요 표준 및 법률 |
|---|---|
| **항공** | - (미국) 연방항공국(FAA)은 항공 시스템 개발 시 준수해야 하는 고시(AC) 및 기술표준훈령(TSO)을 지정, **SW 안전 개발 표준을 명시**<br>- (유럽) **DO-178B에 해당하는 ED-12B를 표준으로 적용하며, 관리기관이나 규정이 미국과 유사**하게 운영 |
| **철도** | - (미국) 연방 철도국(FRA)은 연방법 조례 내, **철도 SW의 안전 요구사항** 정의<br>- (유럽) 유럽철도국(ERA)에서 **철도안전 및 상호운용 관련 지침을 제정**하고, 제조사들이 준수해야 할 **기술사양서(TSI)를 제공**<br>* **(독일) 철도 건설 및 운영규정에 철도차량용 안전관련 SW개발 時, EN50128을 준수하도록 강제화** |
| **자동차** | - (미국) **제조물 책임법**에 최신 기술 적용 강제 **(예, SW 안전확보 기준 ISO26262 Part 6)**<br>- (유럽) 자동차 형식 승인 제도 (ISO26262 준용)<br>제조물 책임법 (미국 유사) |

# 해외 주요국의 SW 안전 수준 (계속)

## TIC (Testing, Inspection and Certification) 상위 5개* 기업의 **매출 지속 성장** 中

* 전체 TIC 시장 중 약 25% 차지

### TIC 상위 기업 매출 현황 (단위 : 백만)

| TIC **상위기업** (화폐단위) | 2011년 | 2012년 | 2013년 | 2014년 | 2015년 | CAGR |
|---|---|---|---|---|---|---|
| SGS (CHF) | 4,797.0 | 5,569.0 | 5,830.0 | 5,883.0 | 5,712.0[1)] | 4.5% |
| Bureau Veritas (EUR) | 3,358.6 | 3,902.3 | 3,933.1 | 4,171.5 | 4,634.8 | 8.4% |
| Intertek (GBP) | 1,749 | 2,054 | 2,184 | 2,093 | 2,166 | 5.5% |
| DEKRA (EUR) | 2,006.9 | 2,164.2 | 2,310.9 | 2,509.8 | 2,720.3 | 7.9% |
| DNV-GL (NOK) | 10,156.0 | 12,532.0 | 15,234.0 | 21,623.0[2)] | 23,390.0 | 23.2% |

### TIC 매출 상위 기업의 직원 수 현황 (단위 : 명)

| TIC **상위기업** | 2011년 | 2012년 | 2013년 | 2014년 | 2015년 | CAGR |
|---|---|---|---|---|---|---|
| SGS | 67,633 | 76,790 | 80,510 | 83,515 | 85,903 | 6.2% |
| Bureau Veritas | 52,148 | 58,924 | 61,581 | 66,494 | 65,995 | 6.1% |
| Intertek | 31,712 | 34,882 | 36,864 | 38,407 | 41,434 | 6.9% |
| DEKRA | 27,321 | 28,340 | 32,591 | 35,021 | 36,673 | 7.6% |
| DNV-GL | 8,453 | 10,294 | 16,107[2)] | 15,712 | 14,954 | 15.3% |

1) 2015년 매출감소는 통화가치 고평가 때문이며, **기존 통화기준 적용 시 전년대비 3.6% 매출증가**
2) 2013년 **DNV그룹과 GL그룹의 합병으로 인한 증가**

# 우리의 SW 안전 현실은

## SW 안전 인식 측면

**SW 안전 개념 未 정립 및 중요성 인식 저조**

### SW 안전 개념에 대한 혼동

- SW 안전을 **품질(quality)**이나 **보안(security)**과 혼동

> 보안과 안전을 동일시 또는 품질이 곧 안전 등 잘못된 SW 안전 개념 보유
>
> SW 안전에 대한 ICT 종사자의 인식 설문조사, SW정책연구소, 2016

### SW 안전에 대한 중요성 인식 미흡

- SW 안전을 필수요소로 인식하지 못함
- SW 개발 원가를 상승시키는 추가 **부담 요소**로 인식

# 우리의 SW 안전 현실은?

## 법·제도 측면

### SW 안전 관련 **현행 법령체계의 한계**

#### 재난 및 안전관리 기본법

- 국가는 각종 재난으로부터 국민의 생명, 신체 및 재산을 보호할 의무 가짐

  * 대한민국 헌법 제34조 6항 '국가는 재해를 예방하고 그 위험으로부터 국민을 보호하기 위하여 노력해야 한다'

- 재난 및 안전에 관한 최상위 법률이나, **SW 안전에 대한 세부 내용 없음**

#### 정보통신기반보호법

- 전자적 침해행위로부터 주요정보통신기반시설의 보호에 관한 대책 수립·시행

  정보통신기반시설을 안정적으로 운용하여 최종적으로 국가의 안전과 국민 생활 보장

- 정보보호(security)에 대한 내용 위주, **SW 안전에 대한 세부 내용 없음**

# 우리의 SW 안전 현실은? (계속)

## 법·제도 측면

**안전 필수 산업 분야 조차도 SW 안전 관련 법령이 아직은 미흡**

| 분야 | 주요법률 |
|---|---|
| **항공** | - 항공안전법 (SW 인증, 안전수준 명시)<br>- 군용항공기 비행안전성 인증에 관한 법률 (SW 안전에 대한 사항 명시)<br>- 항공, 철도사고조사에 관한 법률 등 **(SW에 대한 명시 없음)** |
| **철도** | - 철도안전법<br>(철도차량) '철도차량기술기준'에 고속철·일반철의 SW 안전 강화 규정이 마련<br>(철도시설) **SW 안전성 분석의 명확한 근거 규정 부재** |
| **자동차** | - 자동차관리법<br>안전기준이 HW 측면의 구조와 안전 상태에 그쳐, **SW 안전성 명시하지 않음**<br>* 국내 제조사는 글로벌 경쟁력 확보를 위해 **국제인증을 받은 외산 구성품 활용** |

# 우리의 SW 안전 현실은? (계속)

## 법·제도 측면

**안전 필수 분야 이외 SW 안전 관련 규정과 SW 안전 요구 사항 부재**

### 안전 필수 분야 이외 산업에 명확한 SW 안전 기준 부재

- 철도안전법, 공항시설법 등에 최근 SW의 안전요구 수준이 일부 명시
- **이외 분야에 대해서는 명확한 SW 안전 기준 없음**

### SW 안전 요구 사항 부재

- 국가기반시설, 정보통신기반시설 등의 경우 국민 신체 및 생명과 관련된 SW*가 많으나 별도의 안전 요구사항 부재

* 지진감시·조기경보시스템, 혈액관리시스템, 산불상황관제시스템, 국가대기오염측정망시스템, 긴급구조표준시스템 등

외부 침입으로부터 시설을 보호하기 위한 **보안취약점 점검은 요구***

시스템 내부 오류, 운영 실수 등을 대비한 **안전 요구사항은 부재****

* 정보통신기반보호법 제9조에 따라 매년 보안취약점 분석·평가 실시

** 공공SW구매·구축 사업 35,000여 건 중 SW 안전 요구사항 포함 사업 전무 (2011~2013.06)

# 우리의 SW 안전 현실은?

거버넌스 측면

## SW 안전 관련 담당부처 및 수행기관 **산재**

| 분 야 | 담당부처 | 수행기관 | 역 할 |
|---|---|---|---|
| **철도 분야** | 국토교통부 | 한국철도기술연구원 | 철도시험인증,<br>철도표준지정 |
| **항공 분야** | 국토교통부 | 항공안전기술원 | 항공기 및 항행안전시설<br>안전인증 |
| **원자력 분야** | 과기정통부,<br>원자력안전위원회,<br>산업통상자원부 | 한국원자력연구원,<br>한국원자력안전기술원 | 원자력 SW안전지원 |
| **의료 분야** | 식품의약품안전처 | 식품의약품안전평가원 | 의료기기 안전평가·인증 |
| **국방 분야** | 방위사업청 | 국방기술품질원 | 군수품 품질보증 |
| **승강기 분야** | 행정안전부 | 한국승강기안전기술원 | 승강기 안전평가 |

# 우리의 SW 안전 현실은? (계속) 거버넌스 측면

## SW 안전 관련 기관별로 **개별 연구 추진** 및 **정보공유체계 미비**

- 위험분석 기술이나 SW 안전 메커니즘 설계 등은
  SW로 인한 사고 예방을 위한 **공통기술로 연구 가능**

  원자력, 자동차 항공 분야 등에서 **개별 연구 수행 시 비용 낭비 발생 가능**

- SW 안전 관련 사고사례 데이터베이스 및 사고원인 분석 공유시스템 미비

  정보보안 관련 정보공유시스템(ISAC)에 비해 SW 안전 ISAC 구축 미비

# SW 안전 사회인가?

- SW 안전 개념 **未 정립** 및 중요성 **인식 저조**
- SW 안전 관련 **현행 법령체계의 한계**
- 안전 필수 산업분야 조차도 **SW 안전 관련 법령이 아직은 미흡**
- 안전 필수 분야 이외 SW 안전 관련 규정과 SW 안전 요구 사항 **부재**
- SW 안전 관련 담당부처 및 수행기관 **산재**
- SW 안전 관련 기관별로 **개별 연구 추진** 및 **정보공유체계 미비**

# SW 안전 사회 기반 조성 우선 필요

- SW 안전 중점 관리 대상 선정 및 요구 등급 부여
- 국제 수준 SW 안전 관리 기준 마련
- SW 안전을 위한 법제도 개선
- 공정한 상시 점검 체계 구축
- 전문가 자문단 운영
- SW 안전 자격 제도
- ⋮

## SW 안전 사회


- 공공투자와 민간확산을 통한 시장기반 확충
- 수준별 SW 안전 전문인재 관리 및 풀 구축
- SW 안전 전문기업의 기술역량 강화
- 실무중심 인력 육성
- 마스터급 고급 인력 육성
- 글로벌 SW 안전 기업 육성
- 매뉴얼에 입각한 사고대응
- 범부처 SW 안전 실행체계 마련
- 원인조사 전문성 강화
- 사고사례 데이터베이스 및 분석공유시스템 구축
- ⋮

1 SW 안전 인식 제고

2 법·제도 마련

3 컨트롤타워 설립

출처 : 구글 이미지 재구성

# 1 SW 안전 인식 제고

## SW 안전 인식 제고를 위한 **컨퍼런스, 학회, 교육 지원**

### SW 안전 확보를 위해 산·학·연을 대표할 학회 설립 등

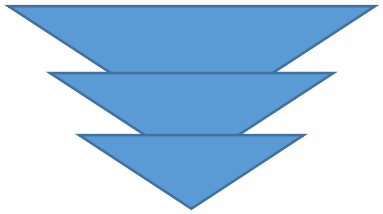
- 컨퍼런스, 교육 등을 통해 SW 안전 정책자료를 비롯한 국민 생활에 밀접한 공공 인프라 분야별 가이드라인 제공
- '(가칭)SW안전학회'를 통해 SW 안전성 확보 기술을 연구, 인력을 양성하고, 산업 현장에 확산

### SW 안전 인식 및 경각심 제고를 위한 SW 안전 개선 캠페인 전개 등

- 웹사이트를 통해 다양한 분야에 걸쳐 SW 안전 위협 요인을 제시하고, 사고 및 피해 예방책 안내
- 지속해서 SW 안전 실태 및 국민들의 의식 현황을 조사하고, 조사 결과를 공개하는 한편, SW 안전 관련 정책 반영에 활용

# 1 SW 안전 인식 제고 (계속)

**SW 안전 인식 제고**



## SW 안전 문화 정착

- SW 안전은 비용이 아니라, 투자라는 인식의 변화

  SW 안전 사고를 예방하여 기업의 신뢰도 보장 및 리콜 등으로 인한 금전적 손실 방지

- 시스템 안전, 크게는 사회 안전을 위해서는 SW 안전이 필수라는 인식 전환

# 2 SW 안전 법·제도 마련

## SW 안전 확보를 위한 법·제도의 제·개정 필요 (86%)

- SW정책연구소의 SW 안전 실태조사 보고서(2016)에 의하면,
  - 일부는 규제로 인한 산업 침체 우려 의견 존재(14%)
  - 규제로 작용하지 않도록 제3의 독립적인 '안전' 기구 설립 필요
  - 기존 법·제도 내 'SW 안전' 항목 추가 및 점진적 적용 필요

## SW 안전 기본법 없이 산업별 SW 안전 법제화 추진의 어려움

- 산업별로 관련 정책을 마련, 기술을 개발하고 법·제화하기에는 엄청난 시간과 비용이 소요
  - 원자력·철도 등 국가기반시설 중 안전 필수 분야에서도 SW 안전 확보를 위해 오랜 기간 기술개발 및 법제화(**원자력:20여 년, 철도:10여 년**)를 추진
  - 아직도 부분적으로 취약

# 2 SW 안전 법·제도 마련 (계속)

## SW 안전 확보를 위한 **기본법** 제정

- 국가 차원의 SW 안전 확보를 위한 **기본법**을 마련하고 필요 산업에 점진적으로 적용
- 국가기반시설에 대한 SW 안전성 점검 제도화의 근거 마련
- 산업별 법률 및 규정 재정비의 근거 마련

### 주요 내용

- SW 안전성에 대한 정의 추가
- 안전한 SW 개발과 운영을 위한 SW 생애주기 全 단계 안전 기준 포함
- 사고조사 및 대응에 SW 안전 전문가 참여
- SW 안전 관련 컨트롤타워 설립 혹은 전문기관 지정 등

# 2 SW 안전 법·제도 마련 (계속)

## 글로벌 요구 수준과의 간극을 좁히기 위한 **견인차 역할 수행**

### 국내 법제도 성숙 분야

NRC(美원자력규제위원회)
FDA(美식품의약국), MDD(유럽의료기기규정)
철도 안전 및 상호운용 관련 지침
(Directive 2004/49/EC, 2008/57/EC)
자동차 안전기준 국제조화

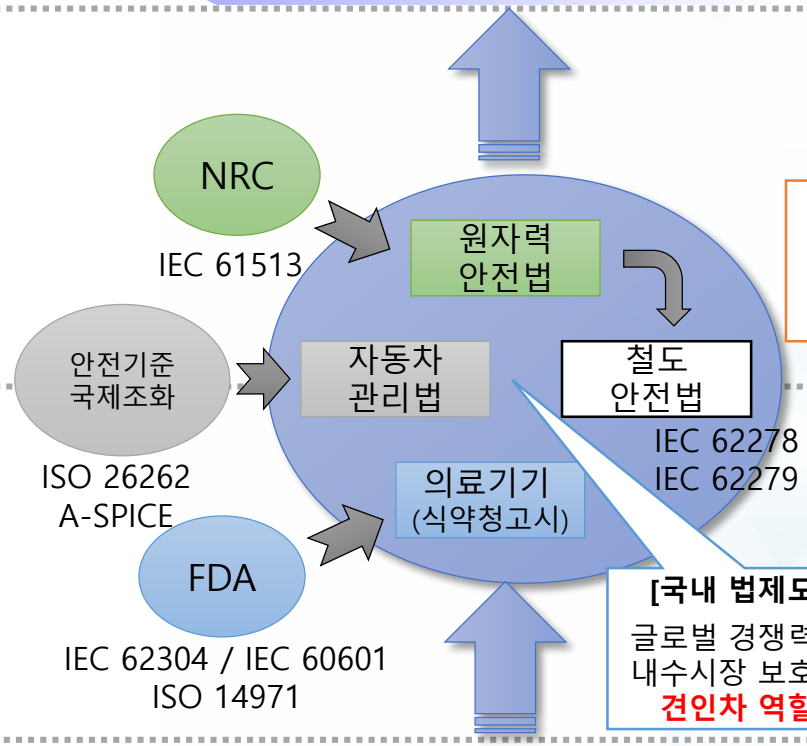
### 국내 법제도 미비 분야

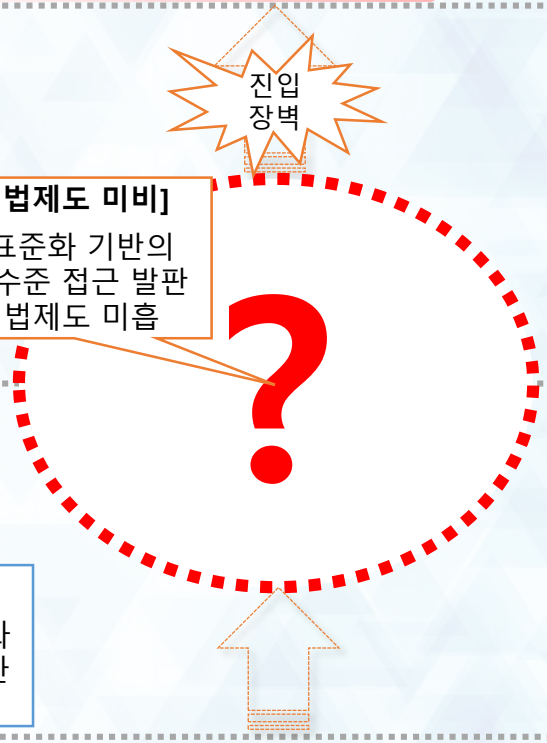
미/유럽의 전기전자분야 국내기업 61508인증 요구
EU의 로봇법(RoboLaw) 프로젝트
조선/해사 분야의 국제 표준화 움직임
무인항공기의 국제민간항공조약(ICAO)

**제4차 산업혁명 發 全 분야 SW 비중 확대 및 안전 강화 움직임**

글로벌 수준

국내 수준



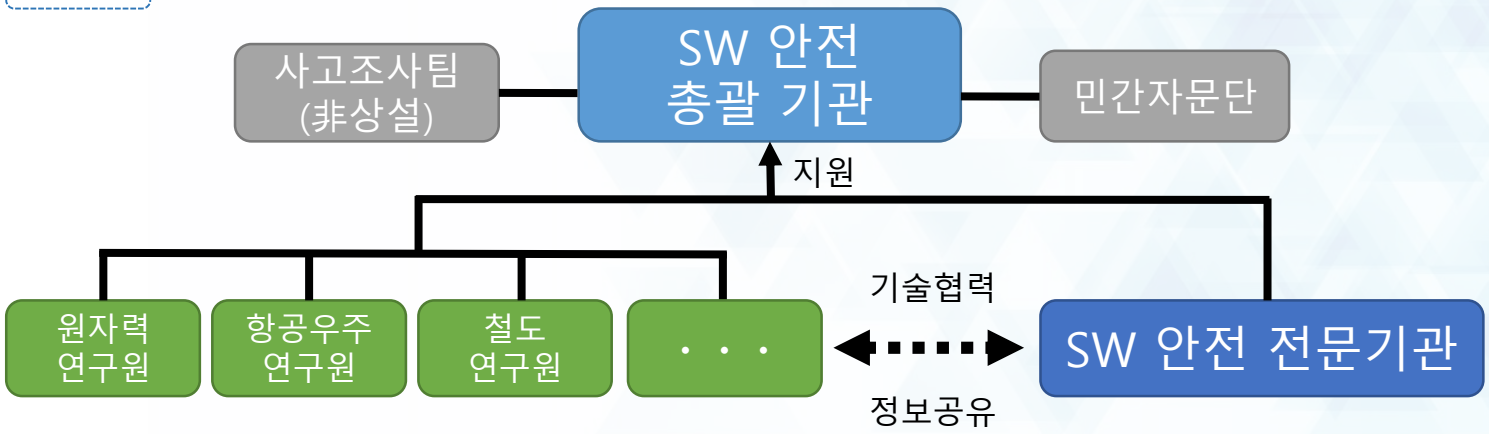
# 3 SW 안전 컨트롤타워 설립

## 범부처 SW 안전 실행체계 마련

- 산업별 정부부처 및 전문기관과 연계하여 범부처 차원의 SW 안전체계 수립
- SW 안전 확보를 지원하는 **컨트롤타워 설립**

  - 각 부처에서 분산 추진하는 안전 정책, 지원방안 등을 통합하여 예방부터 사후복구까지 범부처 차원의 SW 안전 체계 구축
  - SW로 인한 안전사고 재발 방지를 위한 SW 안전 전문가 풀 운영·지원

**예시**



# 3 SW 안전 컨트롤타워 설립 (계속)

## SW 안전 전문기관 지정(설립)

- SW 안전 확보를 위한 **SW 안전 전문기관**을 지정하거나 설립
- SW 안전 분야는 적용 초기임을 고려하여 초기 연구, 운용역량 확보, 산업체 교육 등 단계별 시행계획을 수립하여 효율적인 SW 안전 확보체계 구축

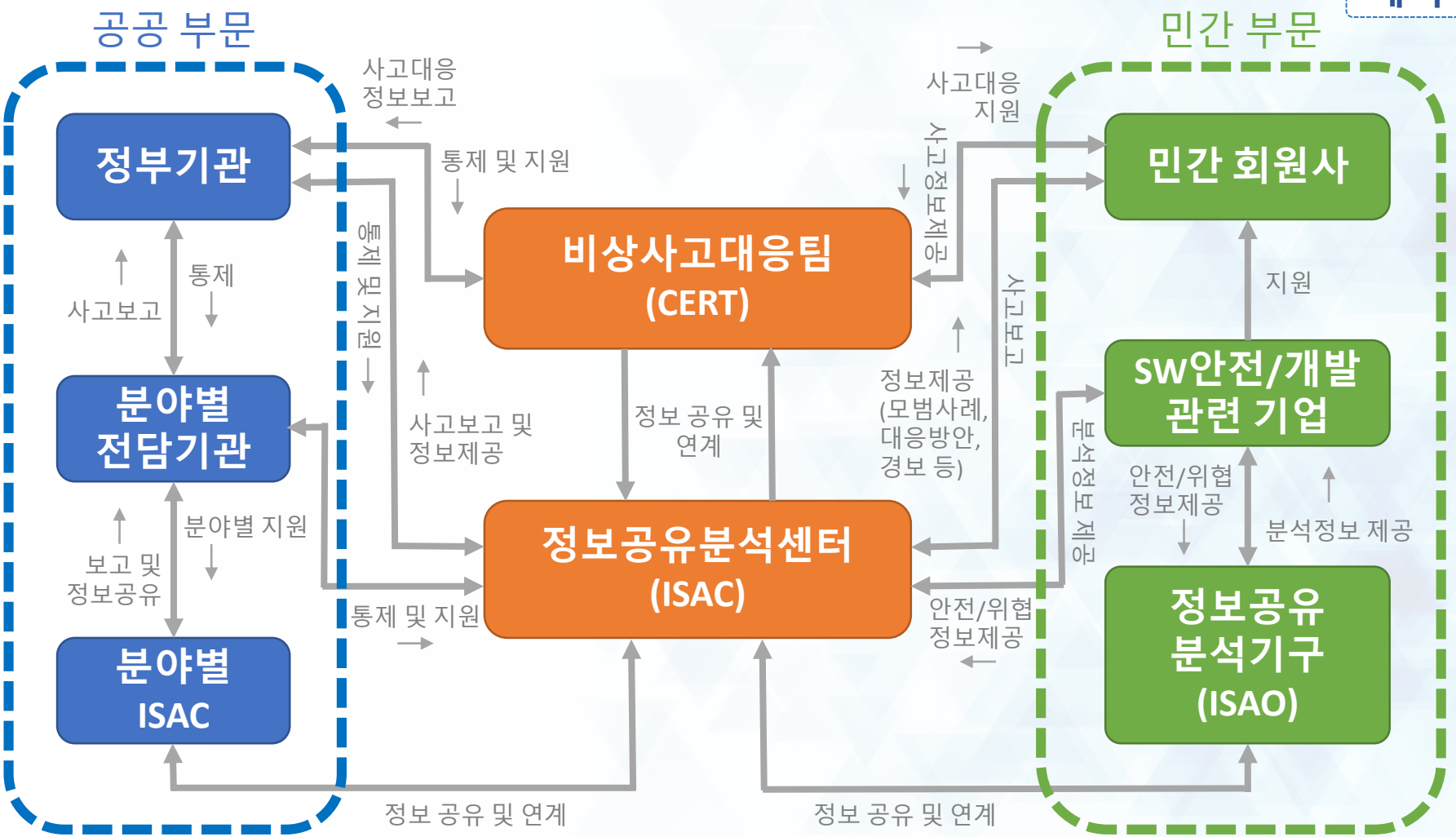
### SW 안전 전문기관 업무 예시

- **(SW 안전 연구)** SW 안전기술 연구 및 컨설팅, SW 안전 인증체계 연구 등
- **(SW 안전 조사)** SW 안전 통계, 정보분석·제공, SW 안전사고 정보축적·활용 등
- **(SW 안전 지원)** SW 운영안전 확보 지원, SW 안전사고 대응·복구 지원 등
- **(SW 안전 진흥)** SW 안전 산업진흥, 국제 협력 등

# 3 SW 안전 컨트롤타워 설립 (계속)

## SW 안전 사고사례/분석 공유시스템 구축 및 데이터베이스 공유

예시



# 결론


SW 안전 사회
Safe
WORKSHOP
검인증
기술/연구개발
R&D
기업
인력/교육
안전관리
SW 안전 인식
법·제도
거버넌스

# 감사합니다
# Q & A

# 소프트웨어 정책 연구를 통한 국가의 미래전략 선도

국가 소프트웨어 정책 Think Tank

SPRi 소프트웨어정책연구소
SOFTWARE POLICY & RESEARCH INSTITUTE