

# 2016년 국내 SW안전 동향

2016. 11. 29.

SW안전연구팀

선임연구원 박태형

# - 목 차 -

1 개요

2 학계 및 정부 (Governing Sector)

3 SW안전 컨설팅 (Supervising Sector)

4 SW 개발·사용자 (End User Sector)

5 시사점 종합 및 결론

# - 목 차 -

**1** 개요

**2** 학계 및 정부 (Governing Sector)

**3** SW안전 컨설팅 (Supervising Sector)

**4** SW 개발·사용자 (End User Sector)

**5** 시사점 종합 및 결론

# 개요

- 국내 SW안전 산업의 구조적인 특성과 실태를 파악
- 해외 주요국의 SW안전 관련 정책 및 시장현황 조사를 수행
- SW안전성 제고를 위한 신뢰성 있는 정책 기초 자료를 제공

## 목적

SW안전성 제고를 위한 **신뢰성 있는** 정책 기초 자료 제공

## 과제

**1** 국내 SW안전 산업 분야  
수요·공급 기업 실태 파악

**2** 해외 주요국의 SW안전  
관련 정책 및 시장현황 조사

## 수업 행무

- ✓ 기업 현황 분석
- ✓ 기술 / 서비스 분석
- ✓ 비즈니스 특성 분석
- ✓ 기업 환경 분석
- ✓ 시장 활성화 정책 요구 분석

- ✓ 관리체계
- ✓ 시장 활성화 정책
- ✓ 인력양성 정책
- ✓ 표준화 정책

# 개요

## ● SW안전 관련 학계, 공공, 컨설팅, 개발·사용자에 대한 동향 조사

### 공공 (Governing)

- SW 안전성 확보를 위한 정책적/학술적 차원의 역할을 수행하는 주체
  - SW 안전 관련 법/제도 제정 및 기관
  - SW 안전 연구 및 표준 수행 기관

### 컨설팅 (Supervising)

- 테스트, 검사/인증 등의 활동을 통해 SW안전을 점검하는 주체
  - TIC기업 : 테스트, 검사 및 인증 산업 종사 기업
  - SW안전 전문 기업 : 기능 안전 산업 종사 기업

### 개발·사용자 (End User)

- 제품 및 서비스 등에 SW안전을 활용하는 주체
  - SW 안전이 요구되는 제품/서비스/인프라 등을 제공하거나 사용하는 주체

# 주요조사항목 : 학계 및 정부

- 학계 및 공공 기관이 인식하는 SW안전의 개념, 산업 현황 및 문제점, 해결 방안 등 조사

## 조사 대상

### ▪ 학계 및 공공기관 등

- SW 안전 연구 수행 대학
- SW안전 관련 전담기관 등

## 조사 항목

### ▪ SW안전 개념

- 학계 및 기관의 SW 안전(safety)의 정의 및 개념 파악

### ▪ SW 안전 산업 현황 및 문제점

- 국내 SW 인증 및 컨설팅 사업 현황
- 해외 선진국 SW안전 체계 및 국내 시장 차이점
- 개별 기업 및 인프라 측면 요건
- SW 안전 산업 시장 활성화 방안 등

### ▪ 해결방안

- 법/제도/인증
- 표준/절차/가이드 및 프로세스
- 교육 및 業 환경개선 등

# 주요조사항목 : SW안전 컨설팅

- SW안전 관련 기업 현황 및 산업계가 인식하는 SW안전의 개념, SW안전 확보 프로세스 및 인프라, 산업 활성화 지원요청 사항 등 조사

## 조사 대상

- 컨설팅 기업 대상  
: TIC 기업 및 SW 안전 전문 기업 등
  - TIC 기업  
: 테스트, 검사 및 인증 산업 종사 기업
  - SW안전 전문 기업  
: 기능 안전 산업 종사 기업

## 조사 항목

- 기업 현황 및 SW안전 개념
  - SW 안전(Safety) 정의 및 개념
  - 주요 제공 서비스 및 고객 현황
  - SW안전 사업 규모 및 전문가 확보 현황
- 프로세스 측면  
: 예방, 탐지, 대응, 사후 활동
- 인프라 측면
  - 표준/매뉴얼
  - 인력/조직
  - 시스템/툴(Tool)
- 산업 활성화 지원 요청 사항
  - 법/제도, 인력 및 시장 측면

# 주요조사항목 : 개발·사용자

- 개발·사용자 기업의 SW안전 관련 인력/조직 체계, SW안전을 위한 프로세스 및 인프라 등 조사

## 조사 대상

- 개발·사용자 기업 대상  
: SW안전이 요구되는 SW를 개발, 사용하는 제품/서비스/인프라 등을 제공하는 기업
  - 정보통신
  - 자동차
  - 금융
  - 우주항공
  - 기타(댐/상하수도 등)

## 조사 항목

- 인력/조직 체계
  - SW안전 사고 예방/대응관리 조직 및 역할
  - 내부 보유 전문인력/자격요건 현황
- 프로세스 측면  
: 예방, 탐지, 대응, 사후 활동
  - SW 개발/도입/변경 시, SW안전 사전점검 활동
  - SW 안전사고 발생 시, 대응방안 및 사후관리 방안
- 인프라 측면  
: 표준/매뉴얼, 인력/조직, 시스템
  - SW 안전관련 국내/외 매뉴얼 현황
  - SW 안전관련 표준/매뉴얼 지원 요청 사항

# - 목 차 -

1 개요

2 학계 및 정부 (Governing Sector)

3 SW안전 컨설팅 (Supervising Sector)

4 SW 개발·사용자 (End User Sector)

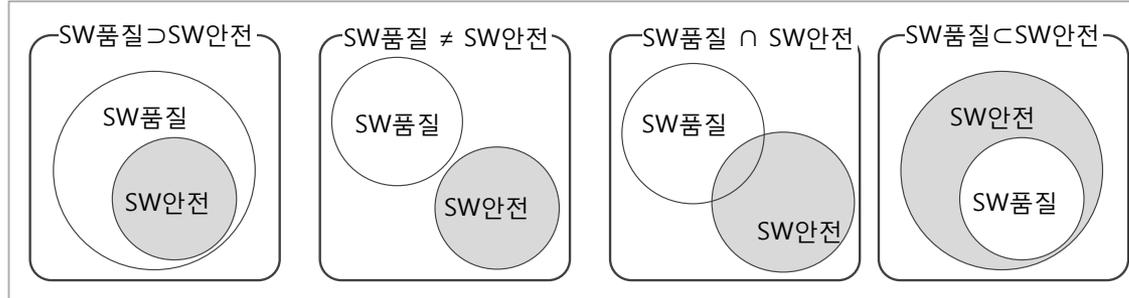
5 시사점 종합 및 결론

# 학계 및 정부 (Governing Sector)

## ● 조사 결과

### ✓ SW안전 개념은 아직 미 정립

- 인터뷰 대상에 따라 SW 안전 개념 및 범위 상이
- 주요 품질 vs. 안전 개념 답변 유형



- 의견 1: 품질이 곧 SW 안전
- 의견 2: 인명/재산 사고를 회피하는 방안(Safety Mechanism)이며, 품질과는 다름
- 의견 3: SW안전은 품질을 포함

### ✓ SW 산업

- 설계/개발보다는 코딩을 중시하는 국내의 개발 문화
- 열악한 SW 개발 환경(단가 등)으로 인한 전반적인 품질 저하

### ✓ SW안전 산업

- SW안전 사업에 대한 법/제도적 기반 미흡
- 전문인력 양성 프로그램, 전문인력의 부족, 산업 중심의 접근전략 미흡 등 시장 여건 미 조성

# 학계 및 정부 (Governing Sector)

## ● 시사점

### 1 SW안전 개념 정의 필요

- SW안전의 개념 명확화를 통한 공감대 형성  
⇒ 법/제도적 접근방법의 시발점
- SW안전  
: 인명이나 재산상 피해를 주는 사고 발생을 회피하기 위한 능동적인 방안(Safety Mechanism /Functional Safety)을 포함한 개념

### 2 SW 안전 공통 산업기반 마련 필요

- SW 산업 자체의 건전한 성장을 위한 인력 수급, 정당한 대가 지급 등 선순환 구조 전환 필요
- 전반적인 SW 산업의 발전과 함께 자연스럽게 SW 안전분야도 발전하는 모습이 바람직함
- 자연과학의 토대 위에 응용과학이 발전한 것처럼 SW 산업 기반의 개선 없이 SW 안전 분야의 성장은 기대하기 어려움
- 법/제도, 인증, 표준, 절차, 조직, 인력, 교육, 업 환경개선, 프로세스 등 전 분야에서의 해결방안을 제시할 필요가 있음

# - 목 차 -

1 개요

2 학계 및 정부 (Governing Sector)

3 **SW안전 컨설팅 (Supervising Sector)**

4 SW 개발·사용자 (End User Sector)

5 시사점 종합 및 결론

# SW안전 컨설팅 (Supervising Sector)

## ● 조사 결과 : 일반 현황 1

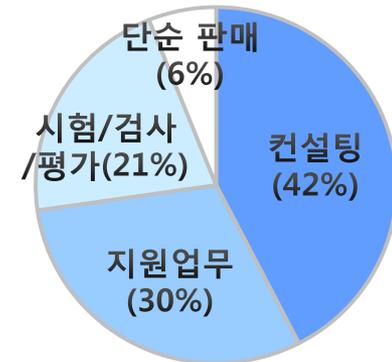
### ✓ SW안전 개념

- 상당수 Safety 관점의 안전 개념 보유 중, Security 관점이 주
  - Security 관점 : 외부의 악의적 공격으로부터 방어
  - Safety 관점 : 사고 발생 원인 회피 메커니즘, 모든 사고발생 가능성 도출/검증 후 분석/설계 수행
  - Quality 관점 : 성능, 기능, 코드의 요구사항/설계내역 부합



### ✓ 주요 수행 업무

- 용역 위주의 컨설팅 중심 사업 구조로 매출 및 수익 확대에 한계
  - 컨설팅 : 품질 및 품질관리체계, 전체 공정 품질 및 안전 점검 등
  - 지원업무 : 인증, 설계 타당성 검증
  - 시험/검사/평가 : 성능, 신뢰성 등
  - 단순 판매 : 도구(Tool), 시스템, 하드웨어
- 단기 매출 위주의 사업 수행으로 사업 영속성 취약



### ✓ 도구(Tool) 사용

- 자동화 도구(Tool) 사용률은 높으나, 주로 사내에서 활용하는 수준

# SW안전 컨설팅 (Supervising Sector)

## ● 시사점

### 1 Safety 중심 SW안전 개념 확산 필요

- Safety 중심에서 Security, Quality를 포함한 SW안전 개념 정립 및 확산 필요

### 2 사업구조 개선 필요

- 용역(인력 투입) 중심의 컨설팅 보다는 제품(솔루션 등) 중심 판매를 통한 수익구조 개선 필요
- 단기 매출 보다 매출 신장을 위한 중장기 전략 수립을 통한 지속적인 사업 구조 개선 필요

### 3 해외 규격을 만족하는 도구(Tool) 국산화

- 국제적으로 통용 가능하도록 규격화된 완성도 높은 도구(Tool) 개발 필요
- 합리적이고 지속적 지원 가능한 국산화 도구(Tool) 개발을 위한 정책적 지원 필요

# SW안전 컨설팅 (Supervising Sector)

## ● 조사 결과 : 일반 현황 2

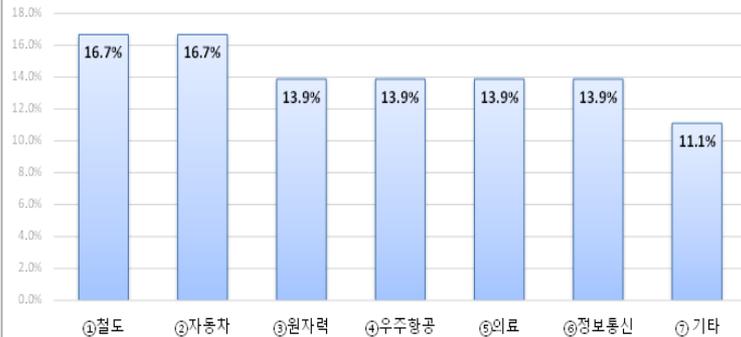
### ✓ 관련 자격 및 특허 보유 현황

- 71%가 SW 검증/인증/안전 업무 수행 관련 자격증 및 자격요건 보유  
⇒ 자격증 보다는 표준/인증 심사경험 등 실 업무경험 중요시
- 코드 자동생성, 도구(Tool) 관련, 인증/검증(또는 SW안전 메커니즘) 특허 등 보유

### ✓ 주요 고객군 및 요구사항

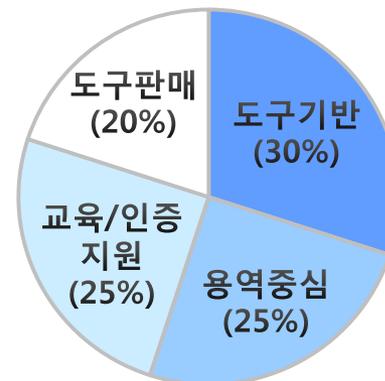
#### 고객군

- 고객은 철도, 자동차, 원자력, 우주항공, 의료 등의 분야에 고루 분포
- 철도, 자동차가 다소 높은 편임



#### 고객요구사항

- 고객 요구 사항은 도구 관련 (도구 기반 서비스 및 판매)가 전체 50% 차지



# SW안전 컨설팅 (Supervising Sector)

## ● 시사점

### 1 SW안전 관련 자격 제도 도입 필요

- 정성적인 업무경험에 대한 객관적 검증 가능한 수준의 자격증 제도 도입 필요
- 자격증 제도의 적극활용을 통한 전문인력 확보 방안 수립 필요

### 2 제공 서비스 분야 세분화 필요

- 기업 자체적으로 제공 가능 서비스, 범위, 역량에 대한 파악 필요 (역량 Self Analysis)
- 고객 및 산업도메인 별 주요 사업 영역을 세분화하고 표준화하여 산업 도메인 및 제공 서비스의 폭 확대 필요

# SW안전 컨설팅 (Supervising Sector)

## ● 조사 결과 : SW안전 프로세스

### ✓ 주요 업무 중 '안전'의 비중 및 중요도 인식 현황

- SW안전 확보를 위해, 'Safety 메카니즘 분석/설계'와 '위험도 분석' 활동이 가장 중요
- 그 외 통합 테스트, 시스템 테스트, 상세설계/구현 등의 순으로 중요도 인식

### ✓ 기존 인증제도 효과성 및 안전 등급 구분

- SW 관련 인증 제도(GS인증, SP인증 등)가 안전성 확보에 효과적이지 않다는 의견 주(57%)
  - 기존인증 보완이나 신규인증 필요하다는 의견이 다수
  - 일부(43%)는 품질 위주의 관련 제도가 SW '안전'을 위한 최소한의 요건이기 때문에 효과적이라고 답변

# SW안전 컨설팅 (Supervising Sector)

## ● 시사점

### 1 SW안전 인식 및 업무 강화

- '안전'에 대한 인식 명확화 및 '안전'업무 비중 확대 필요
- Safety 메카니즘 분석/설계, 위험도 분석 등 '안전'을 위한 핵심 활동 중심으로 업무 재편 필요

### 2 기존 인증제도 보완 / 신규 제도 도입

- '안전'확보를 위한 최소한의 조건으로써의 인증 필요
- 기존제도 보완 또는 신규 인증제도 도입 필요

# SW안전 컨설팅 (Supervising Sector)

## ● 조사 결과 : 인프라 현황 및 Needs

### ✓ 법/제도 측면

- SW 안전 법/제도적 제/개정 필요(86%)
  - 일부는 규제로 인한 산업 침체 우려 의견 존재(14%)
- 법/제도 주요 의견
  - 규제로써 작용하지 않도록, 제3의 독립적인 '안전' 기구 설립
  - 기존 법/제도 내 'SW 안전' 항목 추가 및 점진적 적용

### ✓ 매뉴얼/도구(Tool) 측면

- 품질/테스트/인증 포함한 '안전' 관련 매뉴얼/도구(Tool)가 존재하나, 산업도메인/서비스 별로 상세 정의 되어 있지 않음 ⇒ 업무 수행 중 상황에 맞게 작성/개선하여 활용하는 수준
- 주요 활용 영역 : 개발 및 테스트(산업 도메인 별), SW Life-Cycle 검증, 컨설팅 매뉴얼 제작 등

### ✓ 인력 측면

- SW 안전 실무를 보는 인력보다는 인증심사원 등 인증관련 부문으로 인력 쏠림 현상이 있음
- SW 전문가와 도메인 전문가 간 교류가 적고, 이동 어려움

### ✓ 시장 측면

- 공공성이 높은 분야(철도, 원자력, 우주항공, 국방 등)는 정부 주도의 SW안전을 담보할 수 있는 국가차원의 공통 기반 구축 필요

# SW안전 컨설팅 (Supervising Sector)

## ● 시사점

### 1 점진적/단계적 법/제도 적용

- 선행적으로 법/제도 제정 공감대 형성 필요
- 법/제도 적용 시 점진적/단계적 적용
- 법령/시행령 초안, 산업 표준안 개발, 해외 표준 분석, 대가산정 등 전반적인 안전에 대한 기준 마련

### 2 매뉴얼/도구(Tool) 표준화

- 국내 환경에 적합하도록 사업 Domain별 특화된 표준/매뉴얼 필요
- 도구(Tool) 국산화 등을 통한 활용도 제고

### 3 SW 안전분야 전문가 확보 및 육성

- 단기적으로 국가주도의 SW 인력 및 도메인 전문가 대상 교육 제공 필요
- 중장기적으로 고등교육기관에 관련 학과 개설 등을 통한 지속적이고 장기적인 인력 양성 방안 마련

### 4 SW안전 범정부 차원의 공통기반 마련

- SW안전과 관련이 많은 공공 분야에 대한 SW안전 사업 예산 확보 및 발주 필요
- 범정부 차원의 SW안전을 위한 공통기반 (법/제도, 조직, 정책, 예산, 표준, 기술 등) 마련

# - 목 차 -

1 개요

2 학계 및 정부 (Governing Sector)

3 SW안전 컨설팅 (Supervising Sector)

4 **SW 개발·사용자 (End User Sector)**

5 시사점 종합 및 결론

# SW 개발·사용자 (End User Sector)

## ● 조사 결과 : 일반 현황

### ✓ SW안전에 대한 인식

- 소수(32%)의 End User 기업만 SW안전 개념 인지
- SW안전 정의에 대해 다양한 의견이 존재
  - 79%가 품질과 관련이 있다고 생각

### ✓ SW 품질 및 안전 관리체계

- 대부분 SW 품질/안전에 대한 관리체계는 보유하고 있으나 체계적인 활동은 미흡
  - 89%의 기업이 규정과 절차를 보유
  - SW에 대해 구체적인 검증 활동을 수행하는 경우는 58% 정도

### ✓ SW 품질 및 안전 관련 전담조직

- 절반 이상 기업(57.9%)에서 SW 품질/안전 전담 조직이 존재
- 단, 모두 품질 중심의 활동만 수행, SW 안전만을 위한 활동은 전무

# SW 개발·사용자 (End User Sector)

## ● 시사점

### 1 SW안전 개념 정립 및 인식 확산 필요

- SW 안전의 명확한 개념 및 범위 정의 필요  
(생명과 재산의 손실 또는 생명만 포함 등)
- SW 품질과 더불어 안전에 대한 명확한 개념 이해 필요
- 관련 중앙부처, 학계 및 산업계의 의견을 광범위하게 수렴 필요
- SW 안전 인식 확산 필요

### 2 활동내역 구체화 필요

- 품질에서의 활동 내역과 안전에서의 활동 내역 구체화 및 연관 관계 정립 필요

# SW 개발·사용자 (End User Sector)

## ● 조사 결과 : SW안전 예방점검 활동

### ✓ SW안전 사고예방 활동

- 안전사고 예방활동은 대부분 '안전' 보다는 '품질' 관점이 주
- 대부분 기업 내부 인력/전문가 중심의 활동으로 제3자를 통한 객관적 검증은 25.0% 수준
- 단, 솔루션 개발/판매, 제조 기반 IT 기업은 품질/안전 관련 객관적이고 구체적인 활동 수행

### ✓ Safety-Critical SW 검수

- Safety-Critical SW 검수에 대하여 기업 내부 표준/지침은 대부분 보유(84.2%)
- 단, 부품공급 업체 등에 이러한 표준/지침 확산/적용은 다소 미흡(68.4%)

### ✓ 안전성(Safety) 강화 제품 개발/판매

- 안전성(Safety)을 강화한 제품을 제조/판매하거나, 양산할 계획이 있는 기업은 절반 이하(47.4%)
- 자동차 제조, IT인프라(서버 등) 제조, 우주항공(드론 등) 등 장치제조 기반의 IT 기업들이 다수
- 고객의 니즈(Needs), 제품 경쟁력 강화/영업 전략, 외부 BMT 통과용 등 외적 요인에 기인

# SW 개발·사용자 (End User Sector)

## ● 시사점

### 1 SW안전 관련 민간기업 인식 변화 시급

- SW안전은 필수적으로 수행해야 한다는 인식 확산 필요
- 제품의 안전성을 위해서는 기업 내부 뿐 아니라 협력사 등, 외부 연계도 함께 고려되어야 한다는 인식 필요

### 2 품질과 안전을 위한 제3자 검증

- SW 품질과 안전에 대한 예방, 검증 시 내부 인력에 의한 자체 진행 뿐 아니라 제3자에 의한 객관적 검증 필요

### 3 기업 상황을 고려한 추진

- 산업 도메인 별 사업 속성 및 기업 별 경영 환경을 고려한 SW안전 추진 필요

### 4 기업의 자발적 안전체계 도입

- SW 품질과 안전을 위한 활동이 기업 매출 확대 및 고객 요구 등과 연계될 수 있는 환경 조성 필요

# SW 개발·사용자 (End User Sector)

## ● 조사 결과 : SW안전 대응관리 활동

### ✓ SW안전 사고 대응 시나리오

- 제품 관련 사고 대응 시나리오를 보유하고 있는 기업은 대기업, 제조 기반 ICT 기업 (자동차, 서버 제작 등)
- 단, 사고 대응 시나리오에 따라 정기적인 대응훈련을 실시하고 있는 기업은 18.2%로 소수
- 시나리오에서 기업 내부의 기본적인 대응 체계는 존재, 기업 외부(정부 또는 협력사 등)와 연계된 대응 체계는 취약

### ✓ 사고 발생 시 문제해결 요소 및 자동화 툴

- SW 관련 사고 발생 시 문제해결을 위한 요소는 '기술과 비용' (인력, 유사해결사례, 예산-비용)
- 안전 사고해결사례는 보안 및 기업 간 이익 논리로 공유 불가
- 기업 중 36.8%만 SW 품질/안전 검증/관리 툴(시스템) 보유, 대부분은 '사업관리/품질관리' 기능

### ✓ SW안전 사고사례 정보 관리

- 기업의 31.6%가 SW 안전 테스트 및 사고사례정보를 수집/축적
- 수집/축적 된 안전 테스트 및 사고사례정보는 주로 '테스트 케이스에 적용', '개발인력의 교육/인식 제고'에 활용(76%), SW 안전기능 개선 활용 사례는 극히 소수(8%)

# SW 개발·사용자 (End User Sector)

## ● 시사점

### 1 종합적인 관리 체계 수립 및 강제화

- 기업 내부와 외부가 연계된 종합적 관점의 SW 사고대응 체계 필요
- 안전을 위한 구체적 지침과 강제화 필요

### 2 민간 추진 불가 사업에 대한 정부 지원

- 기업 간 이익 등 시장논리 때문에 민간 차원에서 추진이 불가능한 사업에 대한 정부 주도의 추진 필요
- 중소기업 중심으로 '기술', '비용(예산)' 부문에 대한 정부의 지원 필요

### 3 안전 사고 해결사례 공유 체계 구축

- 정부 주도의 SW안전 사고 해결사례 공유 체계 구축 필요

# SW 개발·사용자 (End User Sector)

## ● 조사 결과 : SW안전 관련 정책 요구사항

### ✓ 품질 및 안전 관련 정부 지원 경험

- 극히 소수의 기업(11%)만이 SW안전과 관련하여 정부의 정책적인 지원을 받은 경험 有
  - SP인증 등 SW 품질을 포함

### ✓ 기업의 SW안전 관련 요구사항

- '규제'와 '지원'의 균형
- 구체적이고 현실적인 지원
- 시장 환경을 고려한 단계적 SW안전 관련 제도 도입 및 추진
- 범정부 SW 안전 플랫폼 구성
  - 정부 지원/관리 공통 서비스와 민간의 산업 도메인 별 특화서비스로 구성된 SW 안전 산업 생태계 활성화 구조를 요구

# SW 개발·사용자 (End User Sector)

## ● 시사점

### 1 품질/안전 인증에 대한 정부 지원 강화

- 품질과 안전 관련 해외 인증에 대한 정부의 지원(소요 비용 또는 컨설팅 지원 등)이 필요

### 2 민·관 융합 범정부 지원체계

- SW안전은 다수의 중앙부처가 연관되어, 범정부적 고려가 필요
- 정부가 잘하는 부분과 민간이 잘하는 부분을 구분하여 각 분야별 장점을 살리는 전략 필요

### 3 SW안전 관련 단계적인 정책 도입 필요



# - 목 차 -

**1** 개 요

**2** 학계 및 정부 (Governing Sector)

**3** SW안전 컨설팅 (Supervising Sector)

**4** SW 개발·사용자 (End User Sector)

**5** 시사점 종합 및 결론

# 시사점 종합 및 결론

- 정부/학계 : SW안전 생태계 조성을 위한 법/제도적 기반 및 지원 체계를 마련
- 산업계 : SW안전 컨설팅 업계는 SW안전 기술 및 문화를 주도
- 사용자 : 개발사용자는 SW안전 문화 정착 필요

## 현황분석 및 시사점 종합 및 결론

### Governing

- ◆ SW 안전 개념 정의 필요
- ◆ SW 안전 공통 산업기반 마련 필요

### Supervising

- ◆ Safety 중심의 SW안전 개념 확산 필요
- ◆ SW 안전 관련 자격 제도 도입 필요
- ◆ 점진적/단계적 법/제도 적용 방안 필요
- ...

### End User

- ◆ SW 안전 개념 정립 및 인식 확산 필요
- ◆ SW 안전 관련 민간기업 인식 변화 시급
- ◆ 품질과 안전을 위한 제3자 검증 필요
- ◆ 종합적인 관리 체계 수립 및 강제화 필요
- ◆ 안전 사고 해결사례 공유 체계 구축
- ...

## 개선 방향

SW안전  
개발·사용자

자동차, 우주항공, 원자력 등  
주요 산업도메인 별 적용환경 조성



SW안전 산업 활성화를 위한 전문기업  
육성 정책 적용 및 문화 확산 기반 마련

SW안전  
컨설팅업계

SW안전 문화 ⇒ 매뉴얼 작성  
도구(Tool) 개발 ⇒ 사례공유



법/제도 및 정책기반 위에 SW안전  
전문 업체의 활동을 적극적으로 지원

정부  
및 학계

개념 정립 ⇒ 법/제도 ⇒ 정책수립  
⇒ 정부지원 ⇒ 자격/인증 제도  
⇒ 인력 ⇒ 공통기반 ⇒ 운영

# 시사점 종합 및 결론

SW안전  
개발·  
사용자

## SW 안전 문화 정착

기업의 자발적 안전체계 도입

제3자 검증

업종별 적용

SW안전  
컨설팅  
업계

## SW 안전 기술 및 문화 주도

SW안전 관련 도구(Tool) 개선

SW안전 사고 해결사례 공유

SW안전 문화 민간분야 정착 주도

SW안전 표준 매뉴얼/가이드 작성

정부  
및  
학계

## SW 안전 생태계 조성을 위한 법/제도적 기반 및 지원 체계 마련

전문인력 양성

SW안전 공통 산업기반

전문가 자문단 운영

범정부 차원 지원체계 수립

SW 안전 자격 제도

SW안전 인증제도 개선

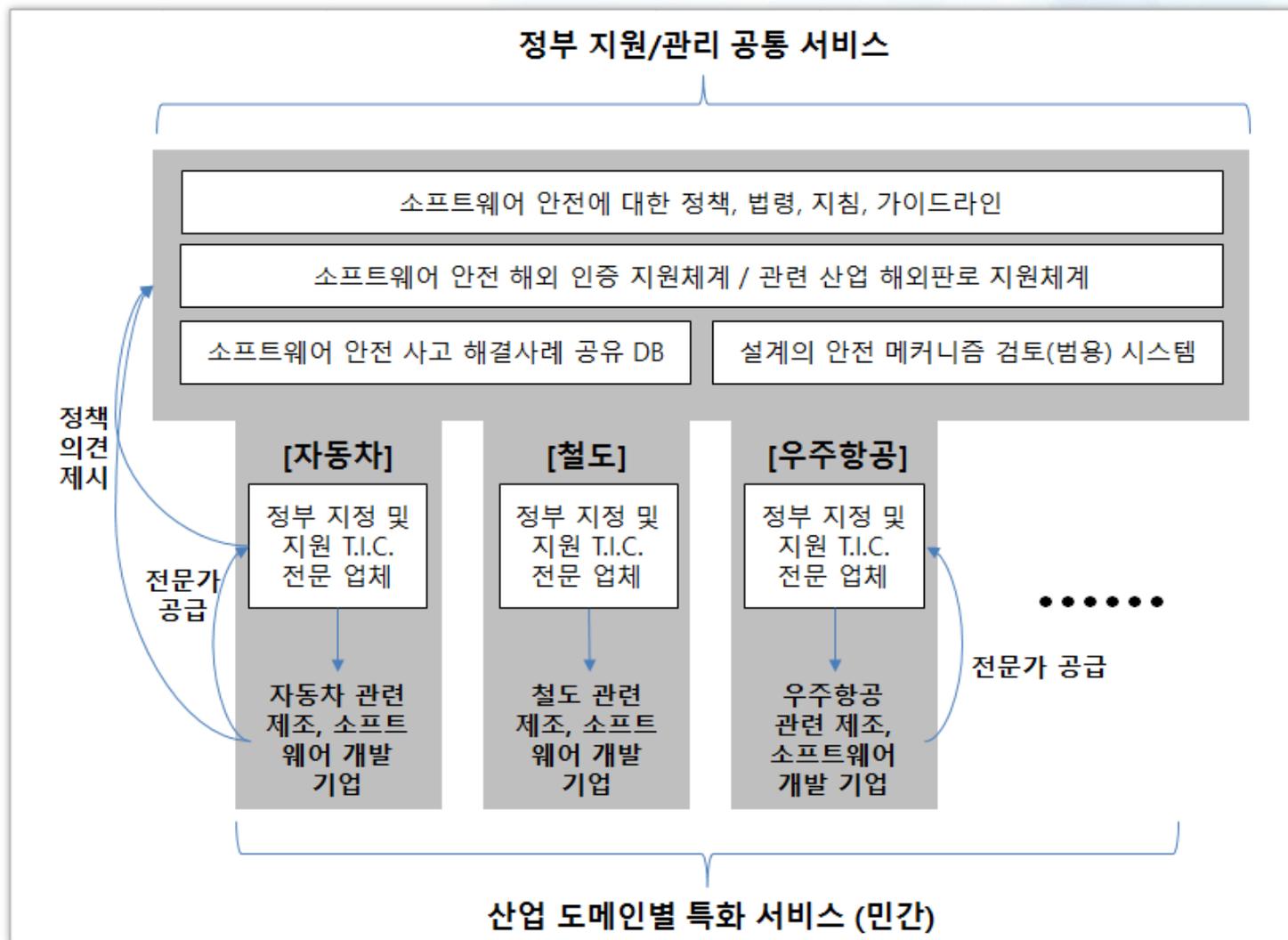
SW안전 관련 법/제도 제정

SW안전 관련 정책 수립

SW 안전 개념 정립 및 인식 확산

# 시사점 종합 및 결론

## ● 범정부 SW안전 플랫폼 개념도



# 산업과 사회의 **변화**를 선도하는 정책 개발

소프트웨어 중심사회의 Think Tank



**SPRI**

소프트웨어정책연구소  
SOFTWARE POLICY & RESEARCH INSTITUTE