SPRi Forum 발제

SW 중심사회에서 SW의 안전

2015.2.24

지 은 경
KAIST 전산학과
ekjee@se.kaist.ac.kr

*본 자료는 이장수 박사(한국원자력연구원), 유준범 교수(건국대학교)와 협력하여 조사 분석한 내용을 기반으로 함

발표자 약력

- Education & Work Experience
  - 2011~현재 KAIST 연구조교수(Research Fellow)
  - 2009~2011 University of Pennsylvania 박사후연구원
  - 2009 KAIST 전산학 박사 (소프트웨어공학 전공)
  - 2003~2004 ㈜이마린로직스 소프트웨어 엔지니어
  - 2001~2002 몽골 울란바타르 대학 컴퓨터학과 전임강사
  - 2001 KAIST 전산학 석사 (소프트웨어공학 전공)
  - 1999 KAIST 전산학 학사
- (SW 안전 관련) Project Experience

기간	프로젝트명 (기관)
2013. 5. ~ 현재	자율지능형 지식/기기 협업 프레임워크 기술 개발 (한국전자통신연구원)
2011. 2. ~ 2013.10.	안전등급 제어기기 엔지니어링 도구 성능개선 기술개발 (한국원자력연구원)
2011. 2. ~ 2012.12.	무기체계(유도조종장치용) 내장형 safety critical S/W 설계기법 및 재사용 지원 시스템 연구 (국방과학연구소)
2011. 5. ~ 2011. 8.	무인항공기 체계 소프트웨어 신뢰도 확보방안 (국방과학연구소)
2009. 9. ~ 2011. 2.	심장박동기 의료SW 안전 보장 개발 기법 (University of Pennsylvania)
2004. 7. ~ 2008. 2.	디지털 보호논리 정형검증 및 자동시험 소프트웨어 검증 (한국원자력연구원)
2005. 5. ~ 2006. 4.	시스템 에어컨 프로토콜 검증 (슈어소프트테크㈜)
2004.10. ~ 2005. 7.	철도소프트웨어 정형개발 및 안전성분석 세부기술 연구 (한국철도기술연구원)
2000. 2. ~ 2000. 8.	다목적 실용위성 위성제어 소프트웨어 안전성 분석 기법 연구 (한국항공우주연구소)

CONTENTS

SW 안전이란?

- SW 안전 (Software Safety) [IEEE Std. 1228-1994]
  - SW 위험요소로부터 자유로운 상태
- SW 위험요소 (Software Hazard)
  - 사고의 필요조건이(prerequisite) 되는 SW 조건
- 사고 (Accident)
  - 사망, 상해, 질병, 환경적 손상 또는 재산적 손실을 일으키는 의도되지 않은 사건(event)

SW 오류로 인한 사고 사례 (1/2)

Softv
NIST A

FOR IM
June 28

BBC NEW

Thursday, 12 December, 2002, 0

Europe's super rocke

The flight lasted barely a few minutes

By Dr David Whitehouse
BBC News Online science editor

The Ariane 5 launcher lost on Wednesday was carrying two satellites: a Hotbird TM7 for the European telecoms consortium Eutelsat, and Stentor, an experimental communications satellite for the French space research institute CNES.

The Eutelsat
250m euros;
380m euros.

9300억

연합뉴스

2012/01/31 15:13

"러'화성 탐사선 사고 원인은 프로그래밍 오류"

포보스 그룬트호를 탑재한 제니트-2SB 로켓이 지난해 11월 9일 카자흐스탄 바이코누르 우주기지에서 발사되는 모습.(AP=연합뉴스, 자료사진)

러시아 정부사고조사위원회 최종보고서서 결론

(모스크바=연합뉴스) 유철종 특파원 = 지난해 11월 발사 후 정상궤도 진입에 실패해 2개월여 만에 추락한 러시아 화성 위성 탐사선 '포보스-그룬트'호의 가장 유력한 사고 원인은 탐사선 컴퓨터의 프로그래밍 오류라고 정부사고조사위원회가 결론 내린 것으로 알려졌다.

SW 오류로 인한 사고 사례 (2/2)

2011.12.3(토) 07:32

농협 또

농협 전산망이
다.

농협은 3일 오전
결제 등 일부 서

이에 따라 이 시

MK

종합
NEWS

KTX 또 멈춰섰다…이번엔 열

작년 나흘에 한번꼴 고장…12월엔 15

기사입력 2011.02.25 15:41:55 | 최종수정 2011.02

국토부가 국회 국토해양위 소속 김진애 민주당 의
대책`에 따르면 차량 고장은 제어 소프트웨어 오류
문제로 발생했으며 나머지는 경험 미숙에 따른 취

연합뉴스

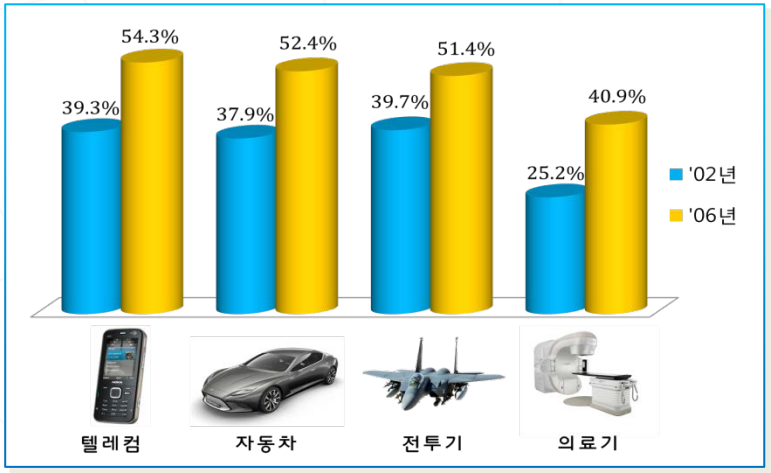
2014/02/12 16:22

도요타 또 리콜…프리우스 190만대 '소프트웨어 결함'

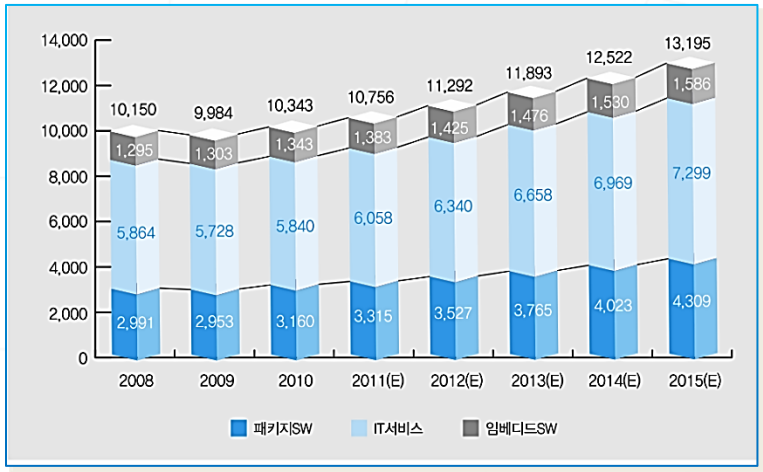
(서울=연합뉴스) 권수현 기자= 미국에서 급발진 문제로 리콜 사태를 겪은 도요타자동차가 이번에는 하이브리드 승용차인 프리우스의 소프트웨어 결함으로 또다시 대규모 리콜을 결정했다.

SW 안전 왜 중요한가? (1/2)

- SW 중심사회에서는 대부분의 국가 기반시설 및 대단위 산업분야에서 SW를 이용한 제어가 이루어짐
- 금융, 자동차, 철도, 항공, 전력, 국방, 의료, 교육 등 대부분 분야에서 SW 의존도가 높아짐에 따라, SW 오류로 인한 사고의 피해 범위와 규모가 확대됨



제품별 SW 비중 증가
(출처: 한국소프트웨어진흥원, 2006)



부문별 세계 SW 시장 규모 (단위: 억 달러)
(출처 : IDC 2011)

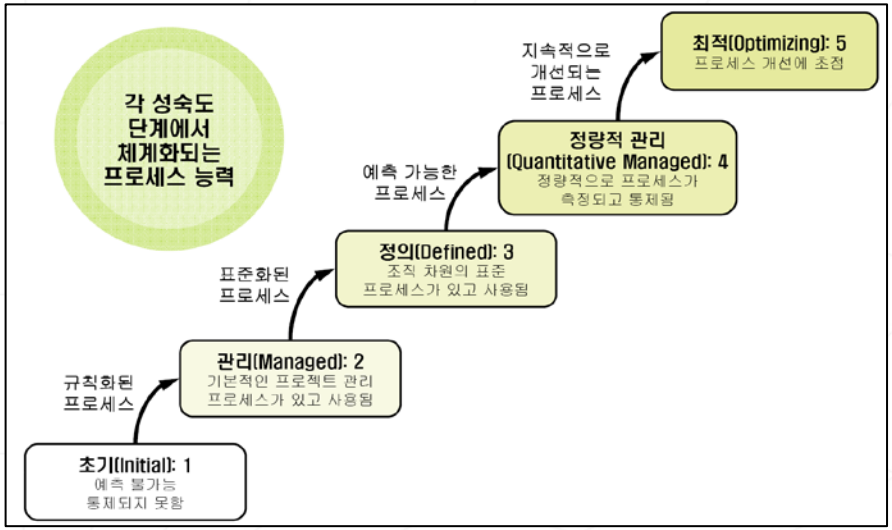
SW 안전 왜 중요한가? (2/2)

- SW 오류로 인한 사고 발생시, 국가 경제 및 사회 전반에 부정적 영향
  - 대형 사고 발생으로 대규모 경제적 손실 야기
  - SW오류에 기인한 국가 기반시설의 안전사고가 빈번히 발생할수록, 국가 및 사회에 대한 상호 신뢰도에 부정적 영향
- SW 안전성 확보는 안전산업의 수출 확대 측면에서도 중요한 과제
  - 국제적으로 자동차, 항공기, 열차, 의료기기, 원자력발전소 등 안전산업에 사용되는 SW에 대한 안전기준을 강화하고 있음
    - 예) EU와 미국 등에 수출할 모든 새로운 자동차 모델들의 전장 제어 SW는 ISO 26262 표준에 준하여 개발해야 하며, 국내 완성차 및 협력업체들은 이 기준을 맞추기 위한 컨소시엄을 구축하는 등 노력 中

SW 안전은 사회안정 유지 및 SW 중심사회로의 신속한 진입을 위한 선결조건임

SW 안전 확보 및 평가 기술

- SW를 통해 제어되는 각종 국가 기간산업에서 SW의 안전을 확보 및 평가하기 위한 기술
  - **소프트웨어공학**의 기술과 도구들을 중심으로 구성됨
  - **기능안전성**이 국제적으로 가장 객관적인 기법으로 인식됨
- 전통적 소프트웨어공학 기법
  - "SW 개발 프로세스를 따라 체계적으로 개발할 경우 일정 수준의 SW 안전성을 확보할 수 있다" 는 전통적인 개념에서 시작
  - 기업의 SW 개발 성숙도(능력)를 평가하는 모델 존재
    - CMMI(Capability Maturity Model Integration), SW프로세스 품질인증 등



<CMMI의 5단계 프로세스 성숙도>

기능 안전성 (Functional Safety)

- 산업에 적용되는 규칙의 국제표준인 IEC 61508로 대표되는 기준
  - "전기/전자/프로그램 가능한 전자 안전 관련 시스템의 기능 안전"
  - 모든 종류 산업에 적용 가능한 기본적 기능 안전 표준이 될 의도로 작성됨
- 시스템의 안전 관련 기능을 여러 등급으로 나눈 후, 높은 등급일수록 보다 엄격한 개발 및 검증 기법을 적용, SW 안전을 '간접적'으로 확보하려는 기준
  - 높은 등급의 안전성이 요구될수록 보다 고비용의 소프트웨어공학 기술이 필요 (테스팅 및 정형검증 등)
  - 안전성 분석(Hazard Analysis) 및 위험 평가(Risk Assessment)를 시작으로 안전 관련된 기능들을 발견•분석•개발•검증 할 수 있는 안전 수명주기 정의

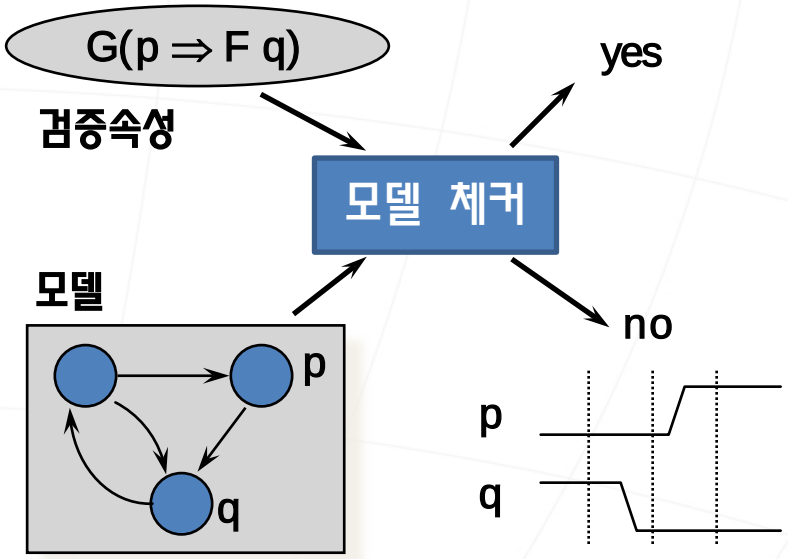
기능 안전성 (계속)

- 기능 안전 표준외에도 소프트웨어(시스템)의 안전을 확보 하기 위해 각 산업 특성에 맞는 국제 표준들이 제정되어 사용되고 있음

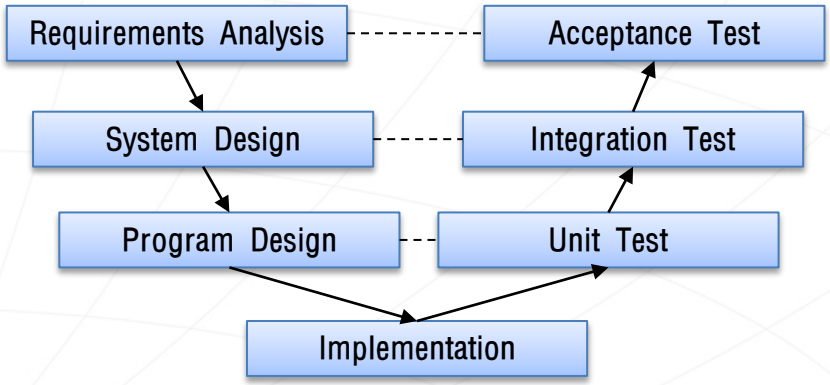
산업분야	공통	자동차	철도	항공	원자력	국방	의료
기능 안전성 관련 표준	IEC 61508	ISO 26262	IEC 62278 IEC 62279	ARP 4761 DO-178C	IEC 60880 IEC 62138 IEEE7-4.3.2 IEC 61513	MIL-STD-498 MIL-STD-882E	IEC 60601 IEC 62304 ISO 13606

SW 안전 관련 SW공학 기술 동향 (1/3)

- 모델 체킹 (Model Checking)
  - 모델이 속성을 만족하는지 자동으로 검사
  - 모든 상태 검사를 통해 강력한 검증 결과를 제공
  - 확장성에 제약이 많아 제한적으로 사용되고 있음



- SW 테스팅
  - SW 오류 탐지를 위해 일반적으로 널리 쓰이고 있는 기법
  - 다수 상용 도구 존재, 자동화 지원 우수
  - 오류가 없음을 보일 수는 없음



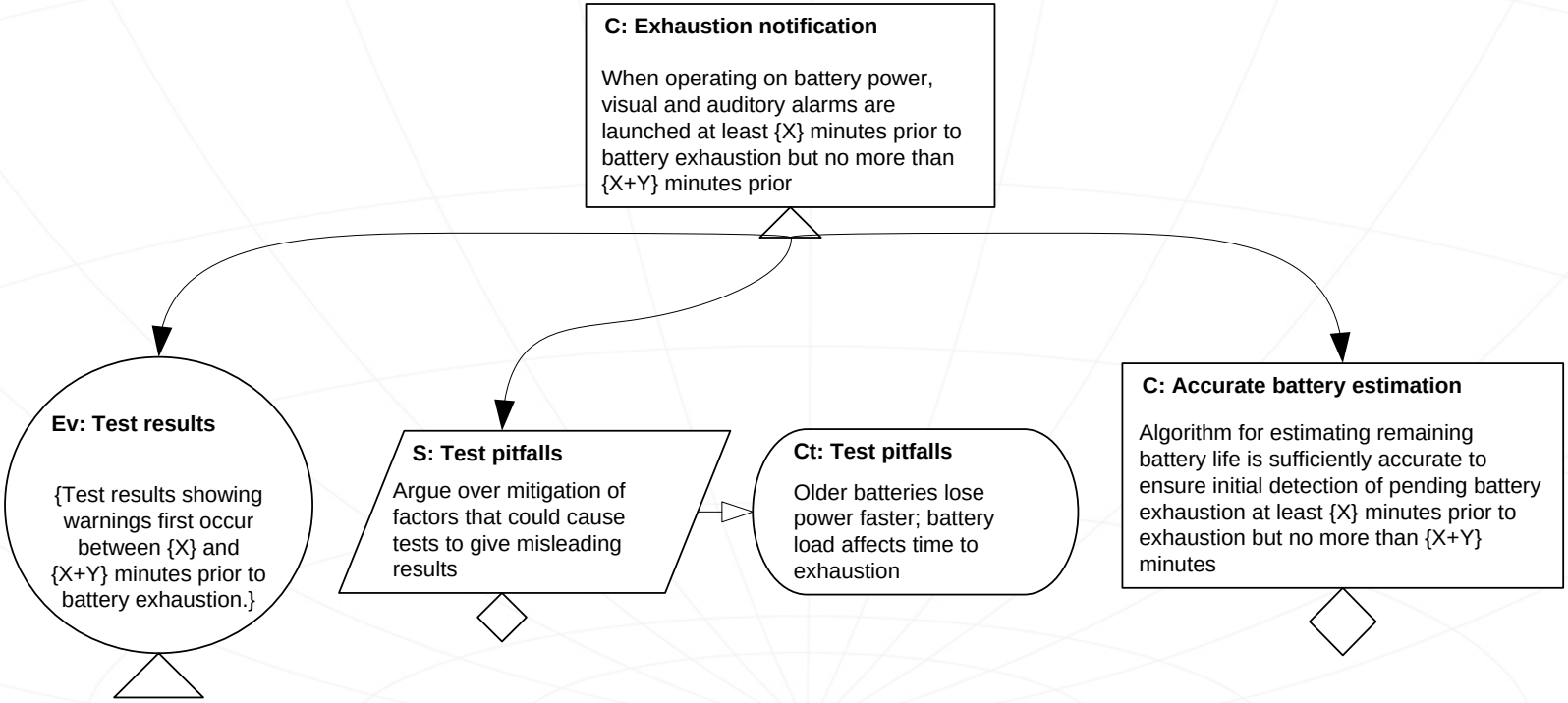
SW 안전 관련 SW공학 기술 동향 (2/3)

- Concolic Testing
  - 하이브리드 소프트웨어 테스팅 기법 (Concolic = Concrete + Symbolic)
  - 새로운 테스트 케이스를 만들 때, 기존 테스트 케이스가 거치지 않은 프로그램 실행 경로를 실행할 수 있는 테스트 케이스를 생성
  - 프로그램 내 모든 경로를 커버하는 테스트 케이스 자동 생성 가능

- 모델 기반 개발 (Model-Based Development) 방법론
  - 모델을 중심으로 체계적인 합성 단계를 거쳐 최종 구현 프로그램을 (자동) 생성하는 개발 방법론
  - 각종 모델링, 합성, 검증, 테스트 도구들이 통합적이고 체계적으로 사용됨 (예, SCADE, Simulink 등)

SW 안전 관련 SW공학 기술 동향 (3/3)

- Safety (Assurance) Case
  - 중요한 안전 항목이나 속성이 만족됨을 논리적으로 주장하는 기법
  - 일부 기능안전성 표준(예, ISO 26262)은 Safety Case의 사용을 요구
  - Safety Case의 주요 구성요소
    - 요구사항/주장(Claim): 안전 보장을 위해 다루어져야 하는 안전 목표들
    - 논거(Argument): 근거들이 어떻게 요구사항에 부합하는지 보이는 논리
    - 근거(Evidence): 주장을 뒷받침할 수 있는 시스템 분석, 테스트, 검증 결과 등의 가용한 정보들



SW 안전 관련 국내외 기술현황

KAIST 한국과학기술원 Korea Advanced Institute of Science and Technology

안전성 SW 표준 대응 추진 중

- 국제 표준화 활동 참여 미흡
- 항공SW관련 DO-178B 인증 획득 기업 확대 중
- 자동차업계 ISO 26262 표준 대응 추진

안전 SW 기술 초기단계

- 국방 무기체계 SW
- 현대자동차 전장 SW
- 원자력 발전소 통제 SW

모델기반 방법론 지원 취약

- 국내 지원도구 부재
- 해외 도구 사용에 고가의 라이선스 비용 지출

국내 수준 해외 수준

안전성 SW 관련 표준 제정

- NASA-STD-8719.13
- 미국 DoD, 영국&호주 DEF
- IEEE Std. 1633, IEC 61508
- ISO 26262, DO-178B/C

안전 SW 플랫폼 아키텍처 연구

- Europe Commission, $4.6M 투자 (AirTraffic Management, 2012.5)

모델기반 방법론 지원도구 출시

- SCADE
- Matlab/Simulink
- LabView

SW 안전 평가 및 인증 기술 현황

- 각 인허가 기관이 안전산업별 국제표준의 준수 여부를 확인함
- 해외 컨설팅 업체(SGS, TUV, Lloyd 등)로부터 사설 인증을 받거나, 해당 정부기관의 인허가를 획득

산업분야	자동차	철도	항공	원자력	국방	의료
표준/ 인증기준	ISO 26262	IEC 62280 IEC 62279	ARP 4761 DO-178C	IEC 60880 IEC 62138 IEEE7-4.3.2 IEC 61513	MIL-STD-498 MIL-STD-882E	IEC 60601 IEC 62304 ISO 13606
국내 인허가 기관	국토교통부 교통안전공단	국토교통부 철도연구원	국토교통부 항공우주연구원	미래부/산업부 /원자력안전위 KINS/KAERI	방위사업청 ADD, 국방기술품질원	KFDA
해외 인증/허가 기관	SGS, TUV-Sud, Lloyd, 미국 NTSB	UL, Lloyd, TUV, SGS, 미국 NTSB	UL, FAA, EASA, Transport Canada, 미국 NTSB	미국 US NRC 영국 HSE ONR	미국 DoD 영국 MoD	미국 FDA

SW 안전 확보 기술적 현안

KAIST 한국과학기술원 Korea Advanced Institute of Science and Technology

- 분야 공통적으로 사용할 수 있는 SW 공학 기술이 다수 존재하나 산업별 실질적 적용 가이드 부족
  - 테스팅 기술 및 도구, 정형검증 기술 및 도구, 안전성 분석 기술 등
  - 도메인 별로 독립적으로 SW 안전 확보 및 평가 기술을 연구해왔고, 관련 연구 및 평가 조직도 독립적으로 운영해 옴
- SW 안전 확보 기술들이 다수 제시되고 있으나, 기술적 한계와 적용 경험 부족으로 SW 안전 인증을 위한 국제적인 합의가 어려움
  - 정형검증, 안전성분석 기술, SW 신뢰도 분석 기술, SW 보안-안전 최적화 기술 등
- SW 안전확보 기술관련 국제 표준화 노력 및 표준 대응이 미흡
- SW 안전을 위한 방법론 확립과 SW 안전 분석 도구 개발 미흡
  - 안전 확보를 위해서는 대상 시스템/도메인 지식과 SW 공학 기술이 모두 필요, SW+HW+인적 요소 등을 통합 고려할 수 있는 복합 기술 필요
- SW 안전 확보 및 평가 기술 교육과 전문가 양성 노력 시급

SW 안전 확보 사회적 현안

- 전산학 전공자의 SW 전문인력 및 SW공학전문가 진출 기피 현상
  - SW공학전문가는 지원 조직으로서, 기업 이윤을 창출하는 직접적인 개발 조직이 아니며, 많은 경우 개발조직 보다 경시되는 경향이 있음
- 안전산업 생태계에서 SW전문인력이 절대적으로 부족
  - 안전산업에서 SW공학 전문 인력 상황은 더욱 심각
    - 도메인 전문가가 SW 공학기술을 공부하여 부분적으로 도입해 실행하는 상황
  - 도메인 지식+SW공학기술을 겸비한 SW공학 전문가 필요
- 안전산업의 SW 시장이 협소하여 기업들이 장기적이고 집중적인 투자를 주저함
  - MATLAB을 개발한 MathWorks 社, SCADE를 개발한 Esterel Technologies 社의 경우 기반기술 개발에 30여년 가까이 투자한 결과, 현재 안전 SW 개발, 시뮬레이션 및 검증 도구 분야에서 독보적 위치
  - 국내에서는 해외에 수출하고 있는 SW공학 전문 도구를 찾아보기 어려움

SW 안전체계

- SW 안전을 확보하기 위한 기술을 지원하고, SW 안전 수준을 평가하며, 특정 표준 및 규약에 맞게 개발되었는지 확인하는 인증 기술을 지원하는 프레임워크
- 세 단계의 기술(기술지원, 평가 및 인증)이 모두 유기적인 체계(Framework)를 이루어 작동

국내 SW 안전체계 현황 (1/3)

- 산업분야 별 안전 및 인허가를 전담하는 국가 기관 및 정부 규제기관이 독립적으로 운영되고 있음
  - 산업분야 별로 다루어야 하는 SW 안전 이슈는 상이하나, SW공학적 접근방법은 동일
  - 공통 기술이 많이 있지만 분야별 교류는 드문 상황, 분야별로 고군분투하고 있고 중복투자의 문제도 발생
  - 분야간에 효과적인 정보 교류 및 상호 협력이 필요
    - 예) 기능안전성에서 중요시 되는 Hazard Analysis 기술은 원자력 분야에서는 기본적으로 사용되는 기술이나, 다른 분야에서는 매우 생소한 기술

	자동차	철도	항공/우주	원자력	의료	국방
정부기관	국토교통부	국토교통부	국토교통부	미래부/원안위/산업부	식약청	방위사업청
공공기관	교통안전공단	철도기술연구원	한국항공우주연구원	한국원자력연구원, 원자력안전기술원	식품의약품안전처	국방기술품질원, 국방과학연구소
역할	자동차 안전평가	철도 시험 인증	항공우주 안전인증	원자력 SW 안전 지원	식품 및 의약품 안전성 검증	국방IT 품질 전담

<주요 산업분야별 안전 전담 기관>

국내 SW 안전체계 현황 (2/3)

- SW 안전 평가 및 인증과 관련 해외 기술과 기업에 의존
  - SW 안전체계를 지원하는 각종 지원 SW 산업이 미흡
    - 안전 SW 개발 방법론
      - MATLAB, SCADE, Rhapsody 등 고가의 외산 도구에 의존
    - SW 테스팅/정적 분석 도구
      - 국내회사들이 테스팅/정적 분석 도구를 개발하였으나, 국제 시장 점유율은 확보하지 못함.
      - 안전 필수 SW 분야는 국산 상용도구의 운용이력이 짧고 적용사례가 많지 않음
    - SW 안전성 분석 도구
      - 국산 상용 도구 없음
    - SW 안전 관련 컨설팅
      - 국내 중소업체들이 자동차 산업 SW 기능 안전성(ISO 26262) 관련 컨설팅을 제공하고 있음
  - 국내에 경쟁 대상이 없어 각종 개발도구를 고가에 구입하고 있음
  - 국내 전문가 집단 부족으로 고가의 도구에 합당한 기술적인 서비스를 제대로 받지 못함

국내 SW 안전체계 현황 (3/3)

- 국내에 권위 있는 평가 및 인증 기관 부재
  - 국내에도 일부 SW 품질 관련 평가 및 인증 제도가 운영되고 있으나, 국제적으로 인정받지 못함
    - 아직 국내에서도 제도의 정착 단계에 있음
  - 국내에 권위 있는 교육/인증/평가기관이 없어 해외기관 (TUV, SGS, Lloyd 등)에 의뢰하여 검증(컨설팅) 받고 있음
    - 국내 기술이 해외로 유출될 가능성이 높음
    - 많은 인증/평가 비용이 해외로 유출됨

SW 안전체계 구축을 위한 전략적 접근

KAIST 한국과학기술원 Korea Advanced Institute of Science and Technology

- SW 중심사회에서의 SW안전 확보를 위한 방안
  - 핵심방안
    - SW 안전기술의 선순환 구조 정착 (산.학.연.관 협력)
      - SW로 인한 대형사고를 예방할 수 있는 기술을 연구/개발하고, SW 안전 산업이 제자리를 갖출 때까지 국가의 적극적 지원 필요
    - SW 안전 확보 및 평가 기술의 산업화
      - SW 안전 산업의 국내 생태계 형성 및 글로벌 시장 대응
  - 장단기 발전 방향
    - 단기: 국가 주도 SW 안전체계 확립
      - SW 안전 control tower 역할을 할 수 있는 국가 기반시설 SW 안전 평가센터 설립
      - 민간(산 · 학 · 연)이 충분한 역할을 수행할 수 있도록 국가가 지원하는 SW 안전기술 지원센터 및 지식허브 구축 (교육, 평가 및 인증을 통합적으로 지원)
    - 장기: 민간 주도 선진 창조경제 실현
      - 기업주도 SW 안전산업의 생태계 활성화
      - SW 안전산업의 선순화 고리 활성화
      - 민간 전문가 양성 및 기술 개발을 통한 전문성 확보

SW 안전 산업 발전 방향

KAIST 한국과학기술원 Korea Advanced Institute of Science and Technology

- IT 융합으로 조선, 자동차, 원자력 등 국가 기반 주력 산업의 고도화
- SW 안전 기술 적용으로 국가기반 SW 산업 高부가가치 창출

- 안전 산업용 SW 수요 증대
- SW 안전 산업 고부가 이익 창출
- 고부가가치 안전SW용 패키지 SW 수요창출 및 수출

- 고급 SW 일자리 창출
- 고부가가치 SW 산업 생태계 조성
- 4D SW산업 악순환 고리 탈출

- 잘 갖추어진 IT 인프라와 인적자원을 기반으로 SW 안전 확보 기술 선제적 개발

감사합니다.