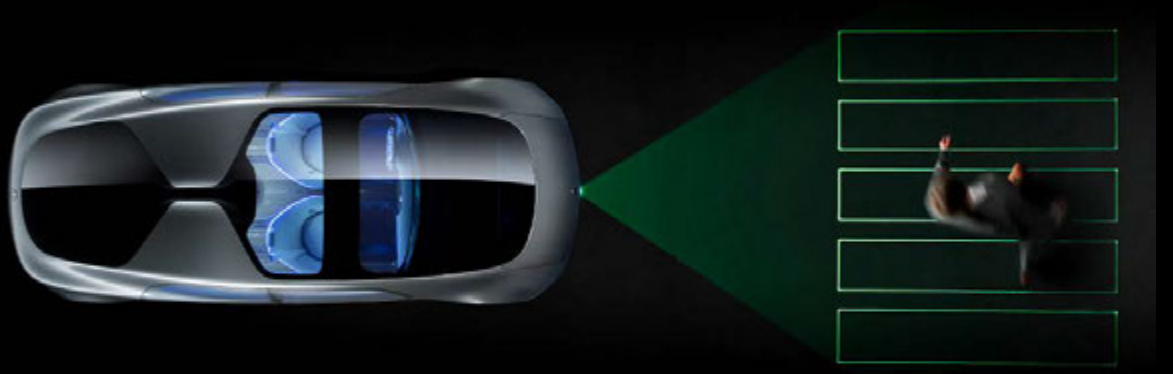
Image from www.mercedes-benz.com



SW Safety for
The Era of ICT Fusion

April 2015, SPRi Conference

Sang Yoon Min

CEO at SOLUTIONLINK Co, Adjunct Professor at KAIST

Topics

- ICT Era, Our Dependency on SW
- Concept of Functional Safety
- Ecosystem for ICT Software
- Safety vs. Conventional Quality Improvement
- Closing,..FS is not just for Safety but,..

ICT Era and Dependency on Software:

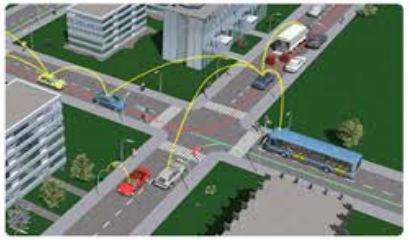
A Pedestrian Protection System Experiment

Extracted from the original clips at

https://m.youtube.com/watch?v=w2pwxv8rFkU

ICT Era and Dependency on Software

Images from www.google.com



ITS의 예: vehicle-to-vehicle communication (사진출처: BMW)

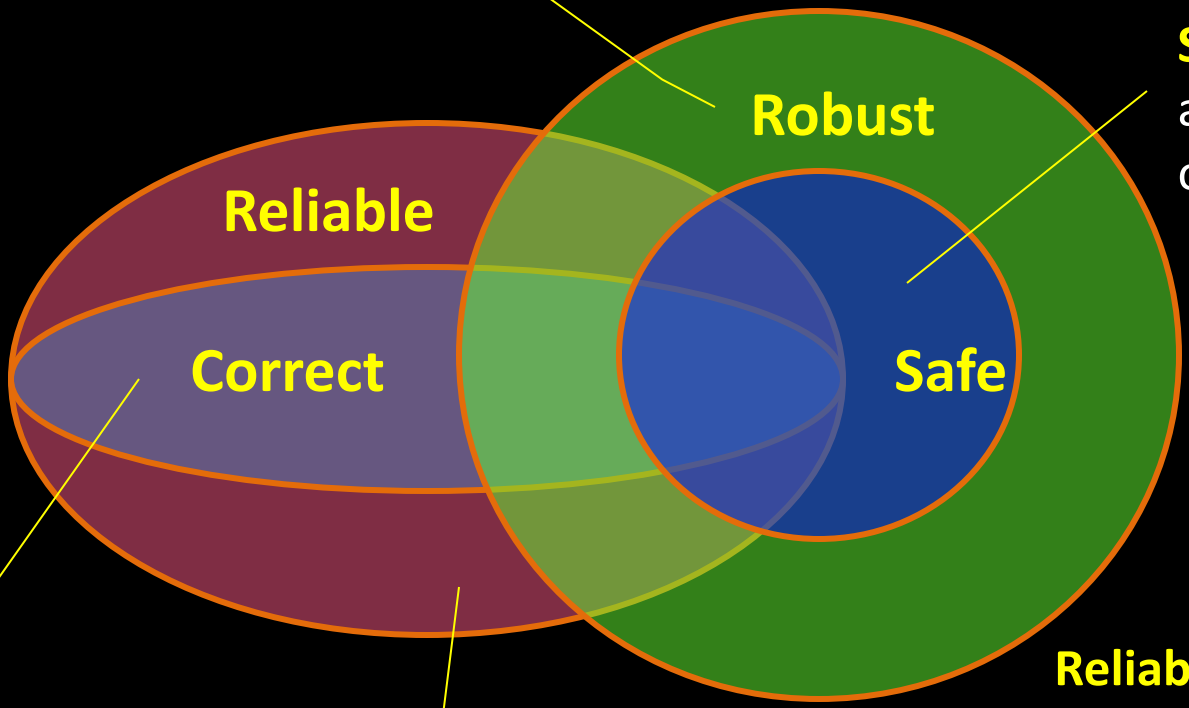
Concept of Functional Safety

Functional safety is….

the part of the overall safety of a system or piece of equipment that depends on the system or equipment, operating correctly in response to its inputs, including the safe management of likely operator errors, hardware failures and environmental changes. [from Wikipedia]

Concept of Functional Safety :

Dependability Properties of ICT System Software



Robust but not safe: catastrophic failures can occur

Safe but not correct: annoying failures can occur

Reliable but not correct: error conditions occur rarely

Correct but not safe or robust: the specification is inadequate

Ecosystem : Number of Parts, HW vs. SW

Source of Faults : SW > HW, SW is not a single part

Hardware		Software
30,000개 전후 **(볼트, 너트15,000개 포함)**		**100,000,000 LOC 전후**
수백~수천여개		**10,000,000 LOC 전후**
수천여개		**2,000,000 LOC 전후**
수백개		**500,000 LOC 전후**

Ecosystem : Quality Ecosystem, Suppliers

하드웨어는 부품의 품질 안정성에 비하여 소프트웨어는 비 규격화 및 비 표준화, 지식 축적 미흡 등 품질의 안정화 측면에서 훨씬 열악

Hardware

부품 1
부품 2
부품 3
부품 N

부품의 표준화

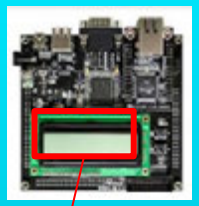
부품의 규격화

납품업체

납품 전 규격에 따른 품질검증

납품업체의 해당 부품전문성

Software

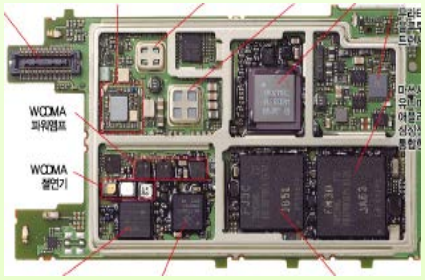


- 소프트웨어 부품화는 아직도 연구 단계임
- 지속적 기술 진화로 표준화 어려움
- 부품화 불가로 인하여 부품 중심의 납품업체 생태계 존속 불가능
- 동일 분야에 대한 개발사의 지속적 기술 축적이 어려움

Ecosystem : Delegation of Changes

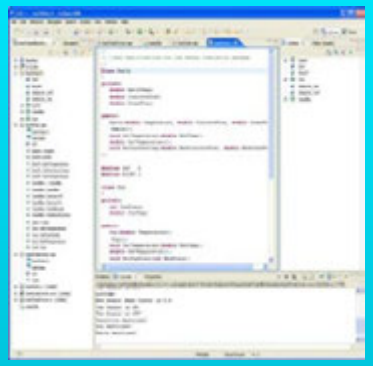
소프트웨어는 intangible한 특성상 변경이 용이하다고 인식됨
빈번한 경우, 제품의 개발 후반 단계의 기능 변경은 소프트웨어로 반영하는 경우가 많음

Hardware



- 설계, 부품 확정 후 조립
- 양산 준비에 돌입 하게 되면 부품에 대한 변경이 매우 어려움
- 또한 부품의 단가 자체가 중요한 의사결정 요소라 고단가 부품으로의 변경을 기피함

Software

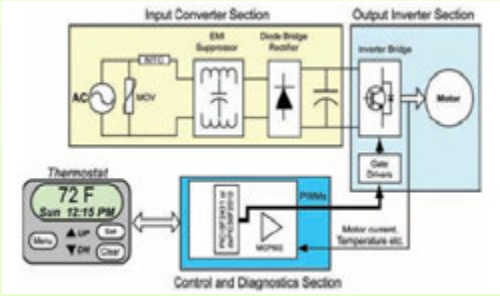


- 소프트웨어라는 특성으로 인하여 쉽게 변경을 가할 수는 있으나,
- 실제 안정적 변경 작업이 절대적으로 용이하지는 않음

Ecosystems : Side-effect of Changes

제품의 구성 요소간 의존성이 하드웨어 대비 소프트웨어는 매우 복잡하며, 높다.

Hardware



- 부품간의 의존도가 명확하며 가시성이 높음
- 특정 부품 설계안에 대한 다양한 실험과 효과 분석이 용이함

Software

- 모듈간의 의존도가 매우 복잡하며, N:M /Loop 관계를 가지는 경우가 많음
- 복잡한 Control Flow와 Data Dependency 가 존재함.
- 하나의 모듈 변경 시 Side-effect의 분석이 중요하며, 어려움

F-22 Raptor Crash Landing

Elevator Shoots Up 30 Floors

Safety v.s. Conventional Quality Improvement

Are process and procedure followed ?

Are the developed contents good enough ?

Can we start improving with testing ?

Are the hazard identified and analyzed ?

Is you domain knowledge good enough ?

Quality is business issue

Safety is legislative issue

Quality is optional issue

Safety is mandatory requirements

Closing : Functional Safety is not just for safety, but for Industry Evolution

Collaborative Robotics and Functional Safety

Thanks,

April 2015, SPRi Conference

Sang Yoon Min
SOLUTIONLINK Co.