CS492: Formal SW Modeling and Verification

Moonzoo Kim

KAIST

Software Testing Verification (SWTV) Group

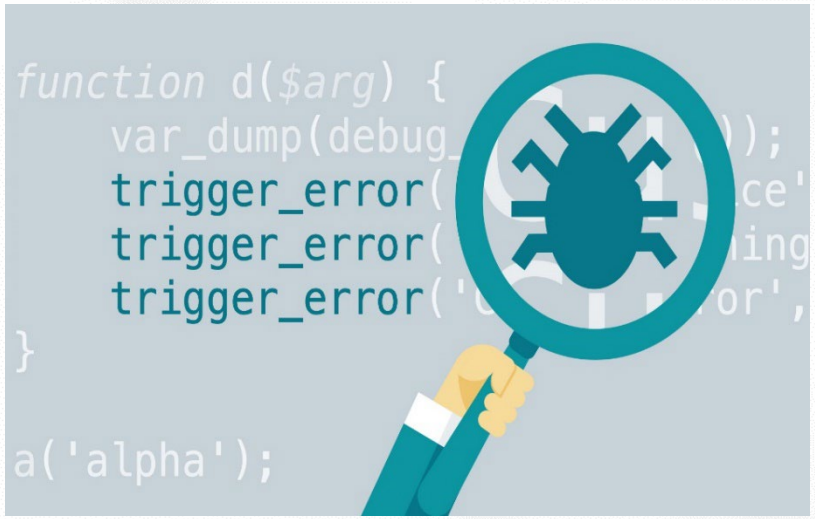
Prof. Moonzoo Kim

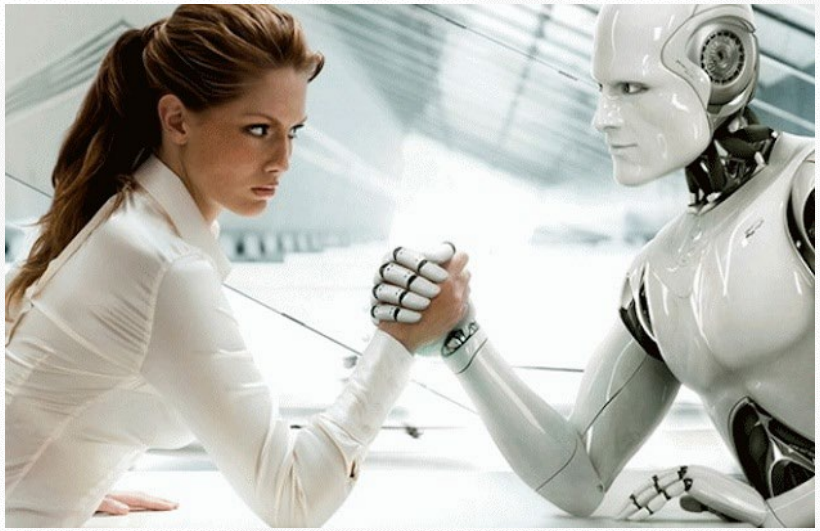
KAIST

E-mail:
moonzoo.kim@gmail.com

https://swtv.kaist.ac.kr/

Necessity of Automated SW Testing



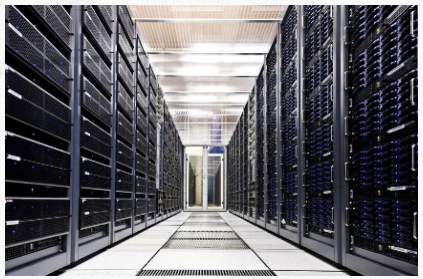


- Safety of SW becomes unreliable due to the high complexity of SW

89 people died caused by Toyota SUA (sudden unintended acceleration)

346 people died due to Boeing 737 MAX crash

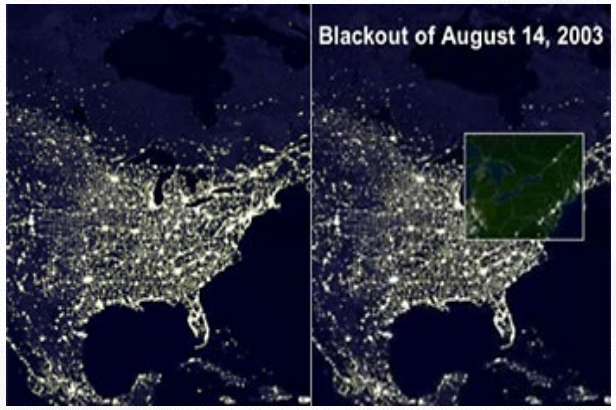
- Modern SW is too large and complex for human engineers to manually test
- Decreased product quality due to the low effectiveness and efficiency of SW bug detection



Scientific modeling and verifying SW is the solution to the problem

Social and Economic Loss due to High Complexity of SW

Although most areas of modern society depend on SW,
reliability of SW is not improved much due to its high complexity



(2003) US & Canada blackout
- 7 states in US and 1 state in Canada suffered 3 days electricity blackout
- Caused by the failures of MISO monitoring SW
- 50 million people suffered and economic loss of 6 billion USD

(2010s) Toyota sudden unintended acceleration
- 89 people died since 2002
- SW bugs detected in 2012
- Fined 1.2 billion USD in 2014

TOYOTA

(2018-2019) Boeing 737 MAX accidents
- 346 people died in 2 accidents
- SW bugs detected in 2019
- Boeing 737 MAX is banned all over the world

BOEING

Boieng 737 MAX Crash due to SW Bugs

참화 부른 보잉의 '늑장대응'…이제 와서 "열흘내 업그레이드"(종합)

송고시간 | 2019-03-16 06:54

NYT "보잉, 작년말까지 업그레이드 약속"…셧다운發 업무지연 연관성도 주목

(뉴욕=연합뉴스) 이준서 특파원 = 미국 항공기 제작업체 보잉이 전 세계적으로 운항중단 조처가 내려진 '보잉 737맥스(Max)' 기종에 대해 10일 이내 '소프트웨어 업그레이드'에 들어갈 예정이라고 AFP통신이 15일(현지시간) 보도했다.

문제로 지목된 소프트웨어는 '조종특성 향상시스템'(MCAS·Maneuvering Characteristics Augmentation System)이다. 난기류 상황에서 항공기의 급하강을 막아주는 일종의 운항정지 방지 시스템이다.

구체적인 원인 분석은 이뤄지지 않았지만, 4개월여 사이에 재발한 '737맥스 8' 기종의 추락 참사는 MCAD와 무관치 않은 것으로 분석된다.

"보잉, 737 맥스 조종제어 소프트웨어 대폭 수정 중"

SBS이혜미 기자

입력 : 2019.03.13 12:54 | 수정 : 2019.03.13 12:54

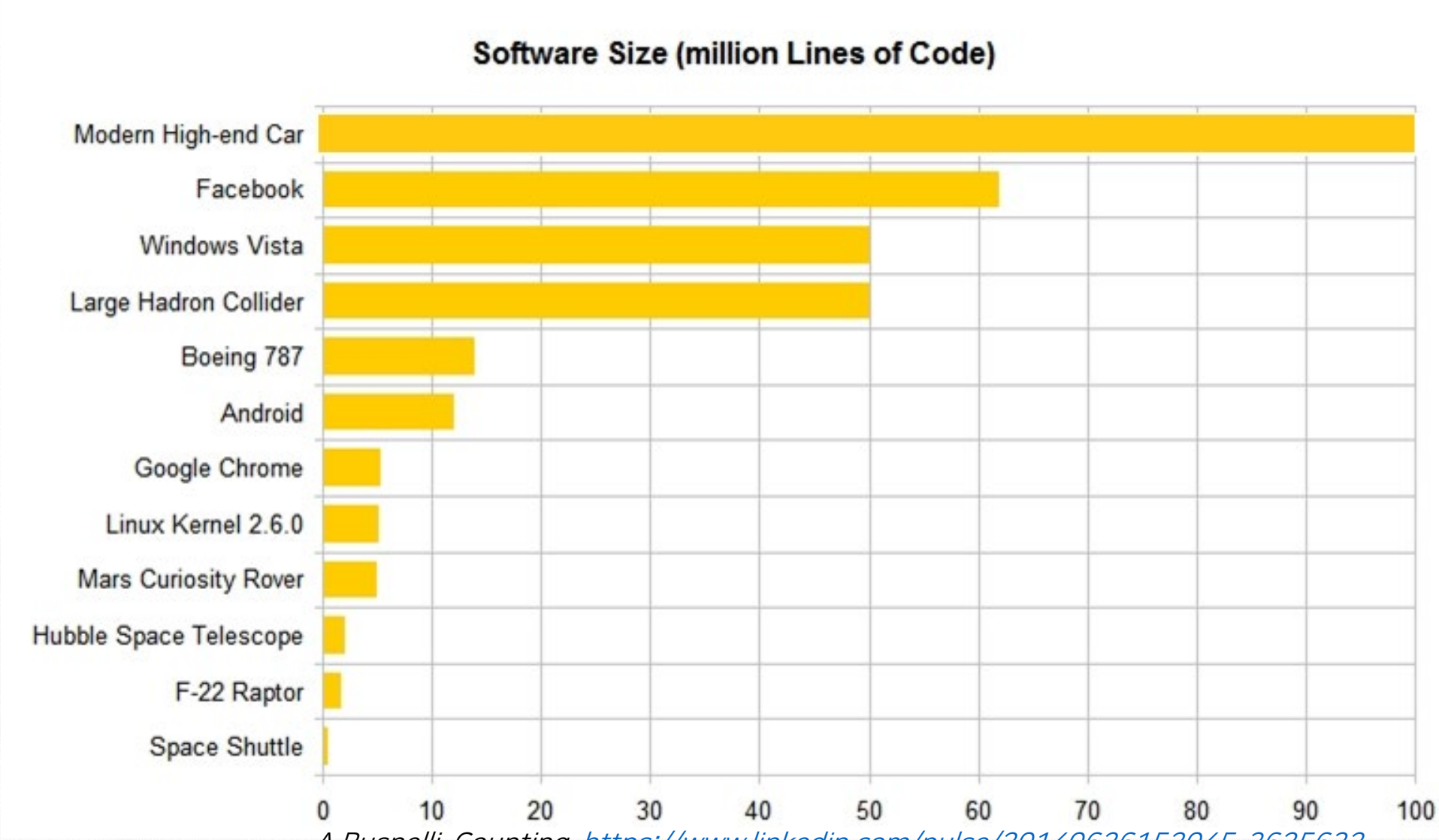
미국 보잉사가 안전성 우려가 불거진 737 맥스 기종 전반에 대해 조종제어 소프트웨어를 대폭 수정하고 있다고 월스트리트저널이 보도했습니다.

소프트웨어 수정은 지난 주말 에티오피아 여객기 추락 사고가 발생하기 전부터 진행해 온 것으로 지난해 10월 같은 기종인 인도네시아 라이언에어 여객기가 추락한 데 따른 것입니다.

미 항공당국은 다음 달 말까지 수정작업이 마무리될 것으로 예상하고 있다고 신문은 전했습니다.

보잉의 최신기종을 둘러싼 안전성 논란이 커지면서 보잉의 주가도 이틀째 추락했습니다.

Size and Complexity of Modern SW



A.Busnelli, Counting, https://www.linkedin.com/pulse/20140626152045-3625632-car-software-100m-lines-of-code-and-counting
http://www.informationisbeautiful.net/visualizations/million-lines-of-code/

How to Improve the Quality of SW

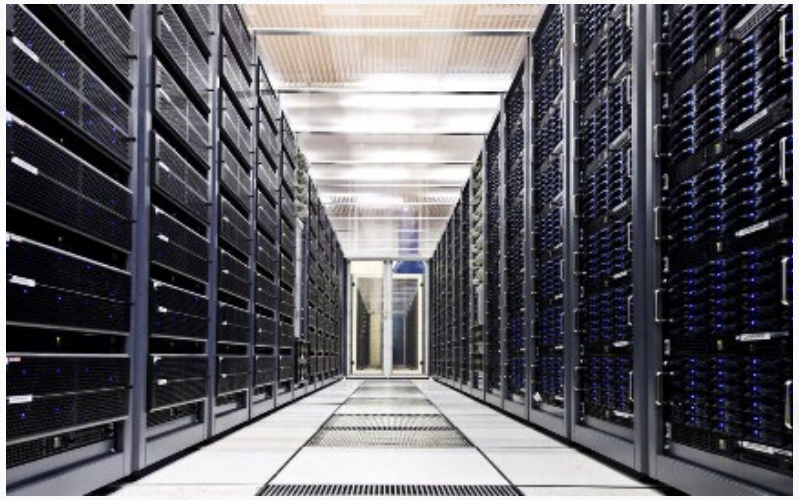
1. Systematic testing (can be still manual)
   - Coverage criteria
   - Mutation analysis
2. Testing through automated analysis tools
   - Generate test inputs to detect bugs
   - Localize detected faults
   - Repairing the fault with patches
3. **Formal verification**
   - **Starting from rigourous modeling of SW**
   - **Guarantee the absence of bugs**

Significance of Formal SW Modeling and Verification

- Software has become more ubiquitous and more complex at the same time

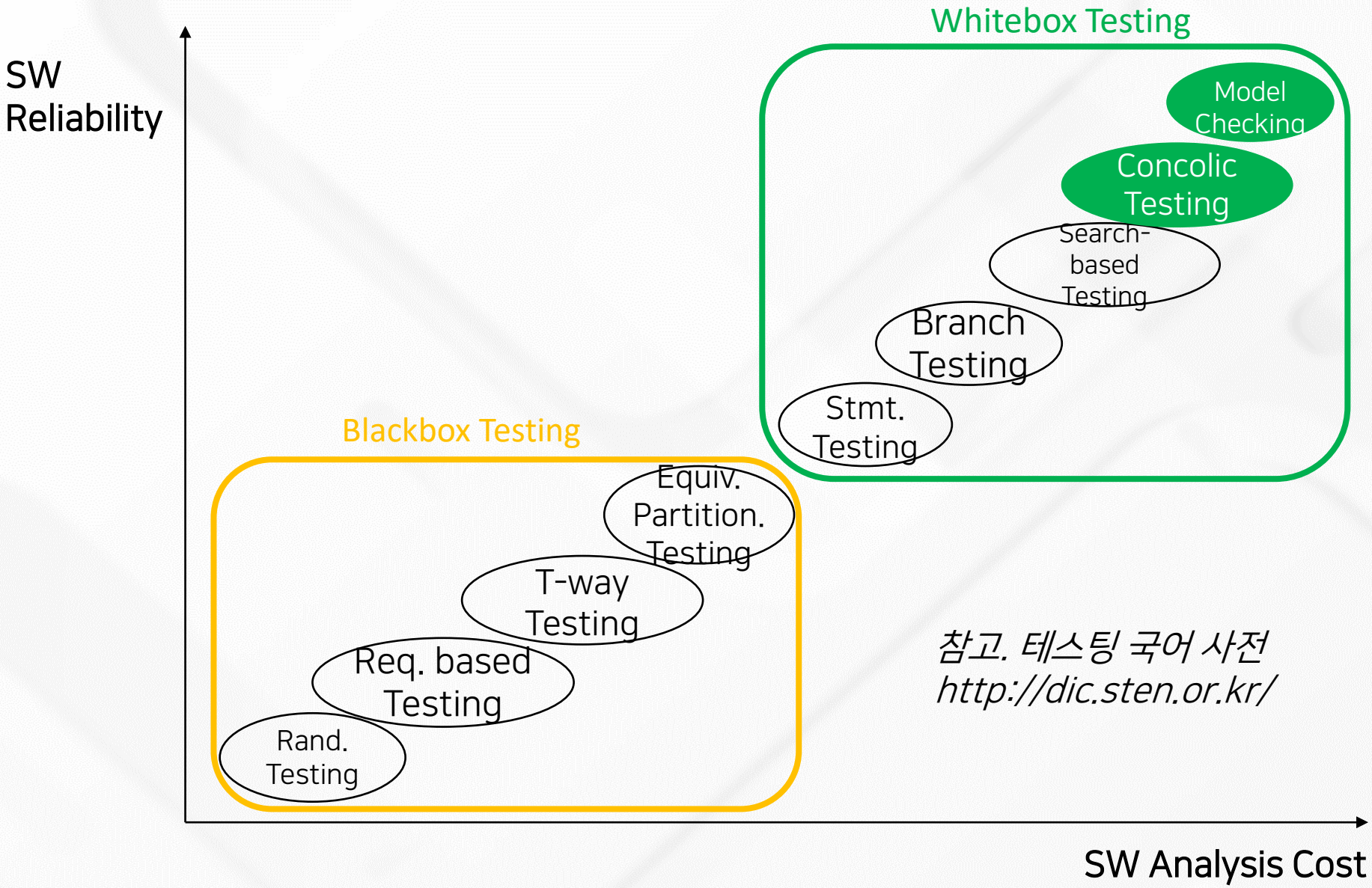
Human resources are becoming **less reliable and more expensive** for highly complex software

Computing resources are becoming **ubiquitous and cheap**
Amazon AWS price: you can use thousands of CPUs @ 0.03$/hr for 2.5Ghz Quad-core CPU



› To-do: Develop **scientific SW modeling and verification tools** to utilize computing resource effectively and efficiently

Various SW Analysis Techniques w/ Different Cost and Effectiveness



참고. 테스팅 국어 사전
http://dic.sten.or.kr/

Roadmap for Improving Quality of SW Product and Service

Problem: Huge Economic & Social Cost **due to Software Bugs**

Labor-intensive Manual Testing
Large SW Testing Cost and Time
Low Bug Detection Abilty
Low Product Quality

Solution: AI-based Highly Effective and
Low Cost **Automated SW Verification Technique**

movie link https://bit.ly/3NS6RrQ

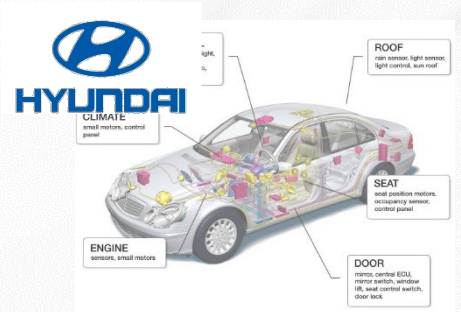
Existing Problems → Developed Solutions

'10-14 Project w/ Samsung Electronics

Detected dozens of crash bugs in the comm. firmware

'18 Project w/ LIGnex1

Detected several SW bugs in the 10 programs in the battleships



'15~20 Project w/ Hyundai/Mobis

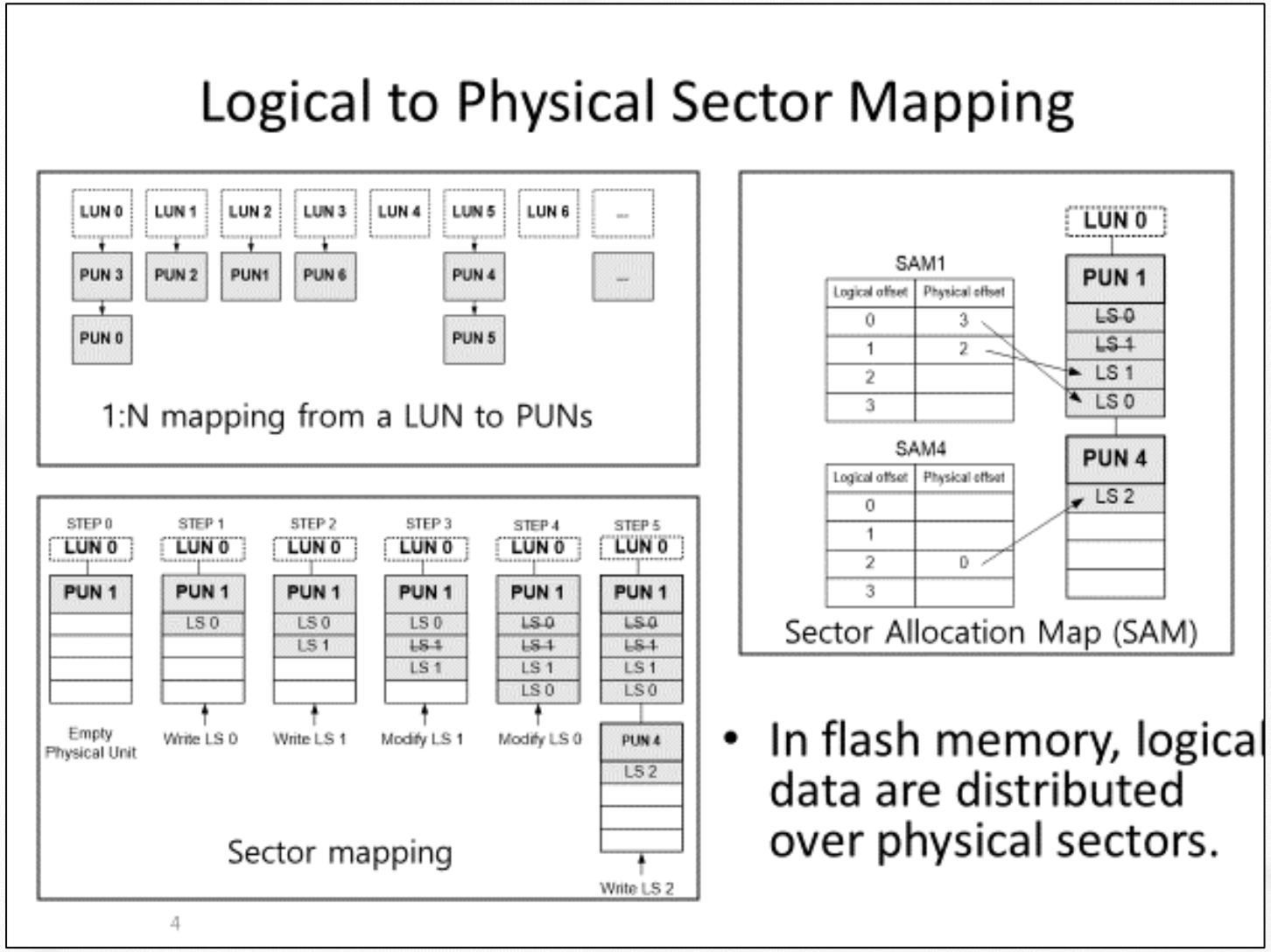
Acheived 90% branch cov. and reduced 80% of labor cost by using auto. testing tech.

'20 Project w/ Natl. Security Research Inst.

Detected SW bugs in the software in the security equipments

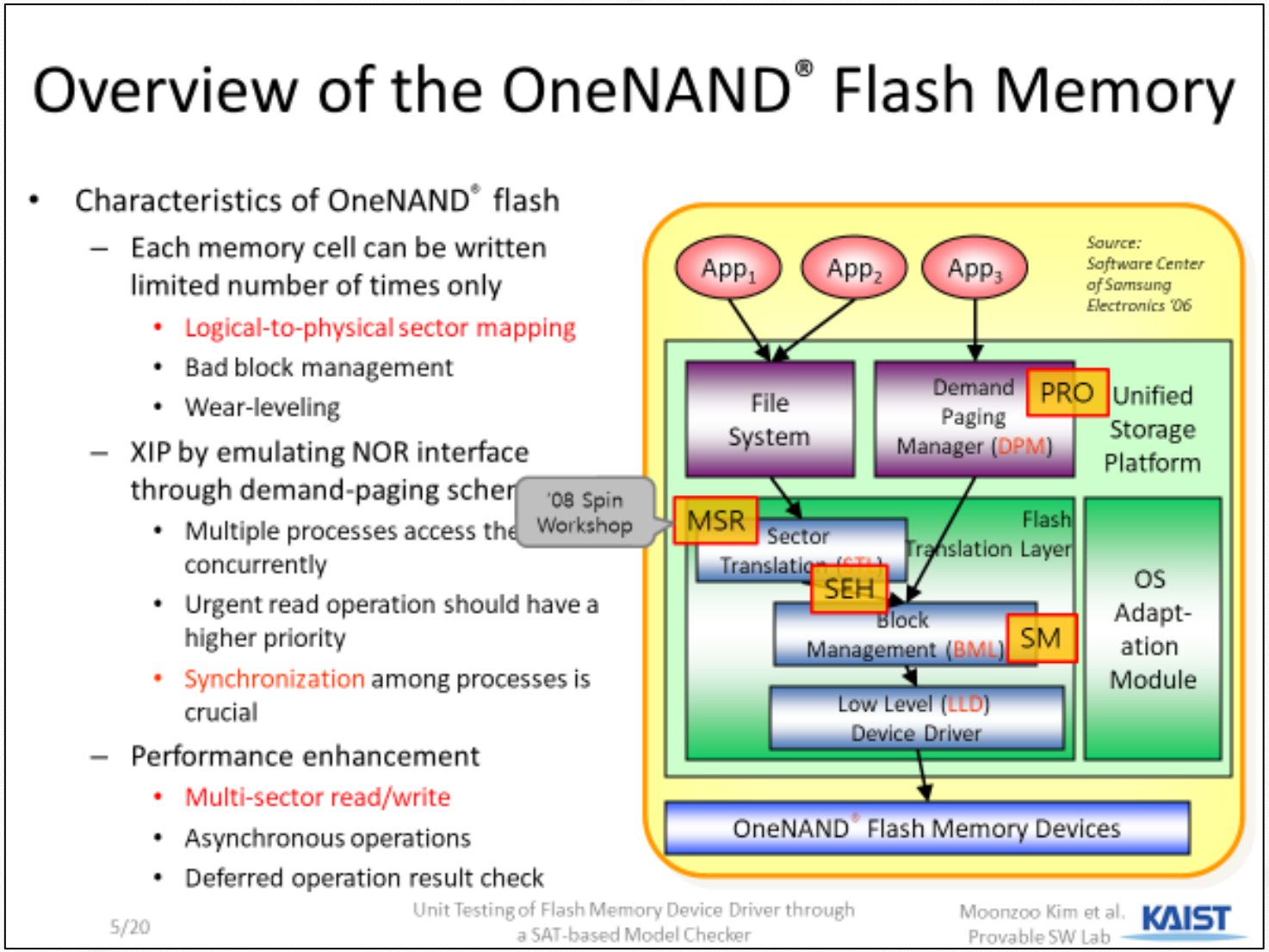
Model Checking of Samsung OneNAND Unified Storage Platform (USP)

- Samsung requested to debug the device driver for the OneNAND™ flash memory
- We reviewed the requirement specifications, the design documents, and C code to identify code-level properties to check.
- Then, we applied model checking to check the properties
  - Provided high confidence in multi-sector read operation through exhaustive exploration



SAT-based Model Checking of Samsung OneNAND USP

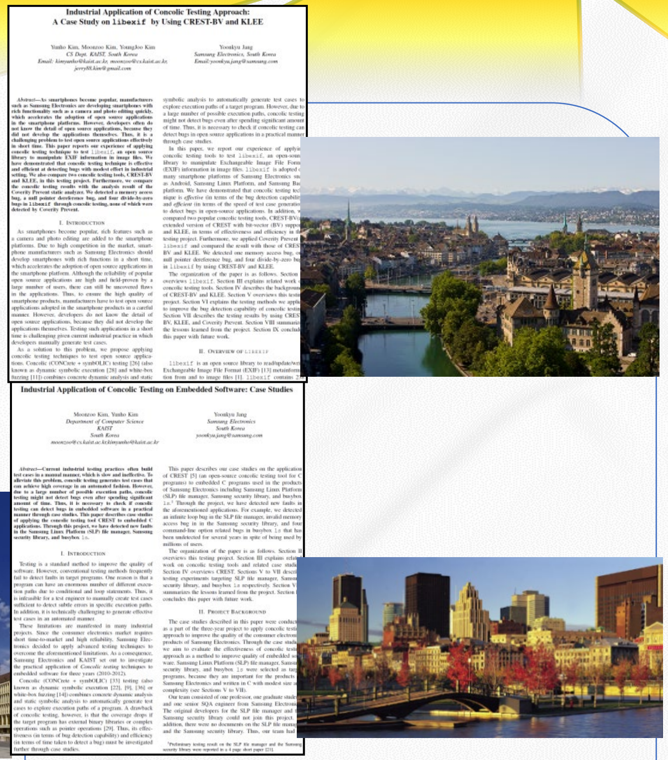
- Prioritized read operation
  - Detected a bug of not saving the status of suspended erase operation
- Concurrency handling
  - Confirmed that the BML semaphore was used correctly
  - Detected a bug of ignoring BML semaphore exceptions



Path-based Model Checking (a.k.a. Concolic Testing) Project w/ Samsung DMC

- Goal: To detect bugs in Samsung smartphones
- Project period: ‘10~’14
- Project funding: 400,000 USD
- Results:
- Developed Concolic unit-testing tool **CONBOL**
- Detected **hundreds crashes** in 4 MLOC smartphone SW

- FSE '2011



- ICSE 2012, ICST 2012

- ASE 2013

Successful Industrial Case: Concolic Testing Automotive SW

현대모비스, AI 기반 소프트웨어 검증시스템 도입..."효율 2배로"

2018-07-22 10:00

댓글 ••• 가- 가+

'마이스트' 적용...대화형 검색 로봇 '마이봇'도 도입

(서울=연합뉴스) 윤보람 기자 = 현대모비스[012330]가 인공지능(AI)을 활용해 자율주행, 커넥티비티(연결성) 등 미래 자동차 소프트웨어(SW) 개발에 속도를 낸다.

현대모비스는 AI를 기반으로 하는 소프트웨어 검증시스템 '마이스트'(MAIST: Mobis Artificial Intelligence Software Testing)를 최근 도입했다고 22일 밝혔다.

Google에 의해 종료된 광고입니다.
이 광고 그만 보기
이 광고가 표시된 이유

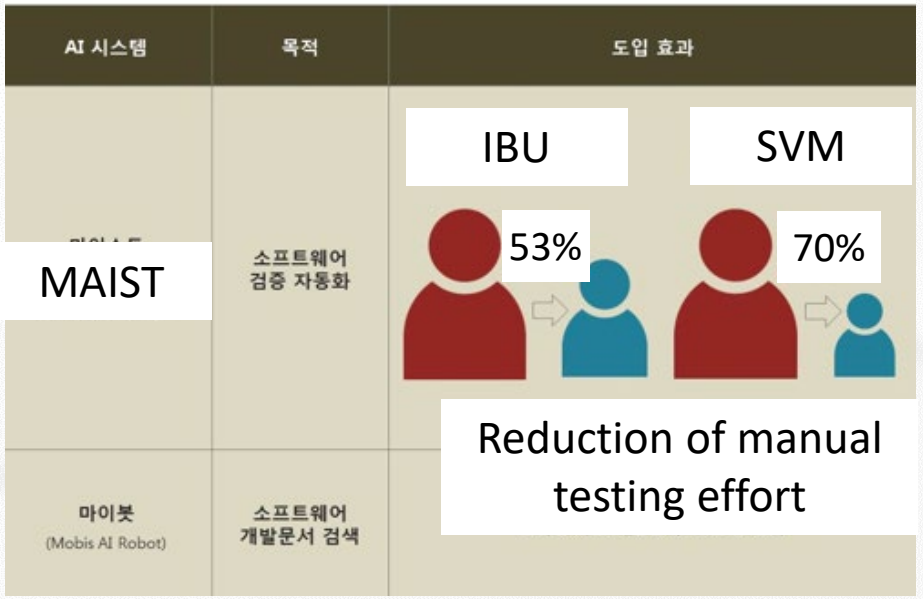
Hyundai Mobis and a research team lead by Prof. Moonzoo Kim at KAIST jointly developed MAIST for automated testing

MAIST automates unit coverage testing performed by human engineers by applying concolic unit testing

MAIST can reduce 53% and 70% of manual testing effort for IBU(Integrated Body Unit) and SVM(Surround View Monitoring)

현대모비스는 하반기부터 소프트웨어가 탑재되는 제동, 조향 등 모든 전장부품으로 마이스트를 확대 적용할 계획이다. 글로벌 소프트웨어 연구기지인 인도연구소에도 적용한다.

■ 현대모비스 인공지능 도입 사례



http://m.yna.co.kr/kr/contents/?cid=AKR20180720158800003&mobile

Final Remarks

- For undergraduate students:
  - Highly recommend URP studies or independent studies
    - 이아청 detected several crash bugs in Hyundai Mobis SW during 2018 summer interns
- For graduate students:
  - Welcome research discussions to apply formal SW analysis techniques
    - Systematically modeling and verifying complex SW

15

16