안전우선 시스템을 위한 동기식 미들웨어의 검증

발표: 김철기

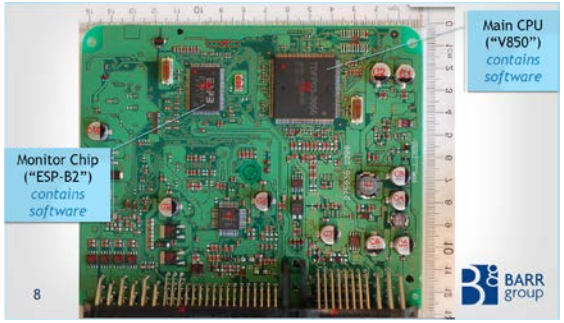
with Min Young Nam, Lui Sha (UIUC)
Sagar Chaki (SEI)

토요타 급발진 문제와 SW

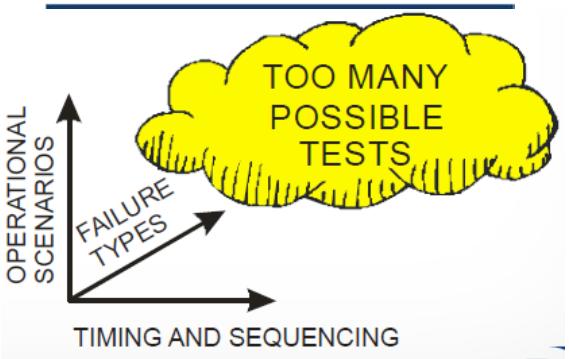
- 토요타 급발진 사건은 SW 문제로 사실상 결론
  - Barr 그룹에 의하여 시연
  - 결함 구속의 실패와 부적절한 다중화가 요인
  - 경쟁조건으로 인하여 테스트를 통한 발견 불가

Redundancy and fault containment are key

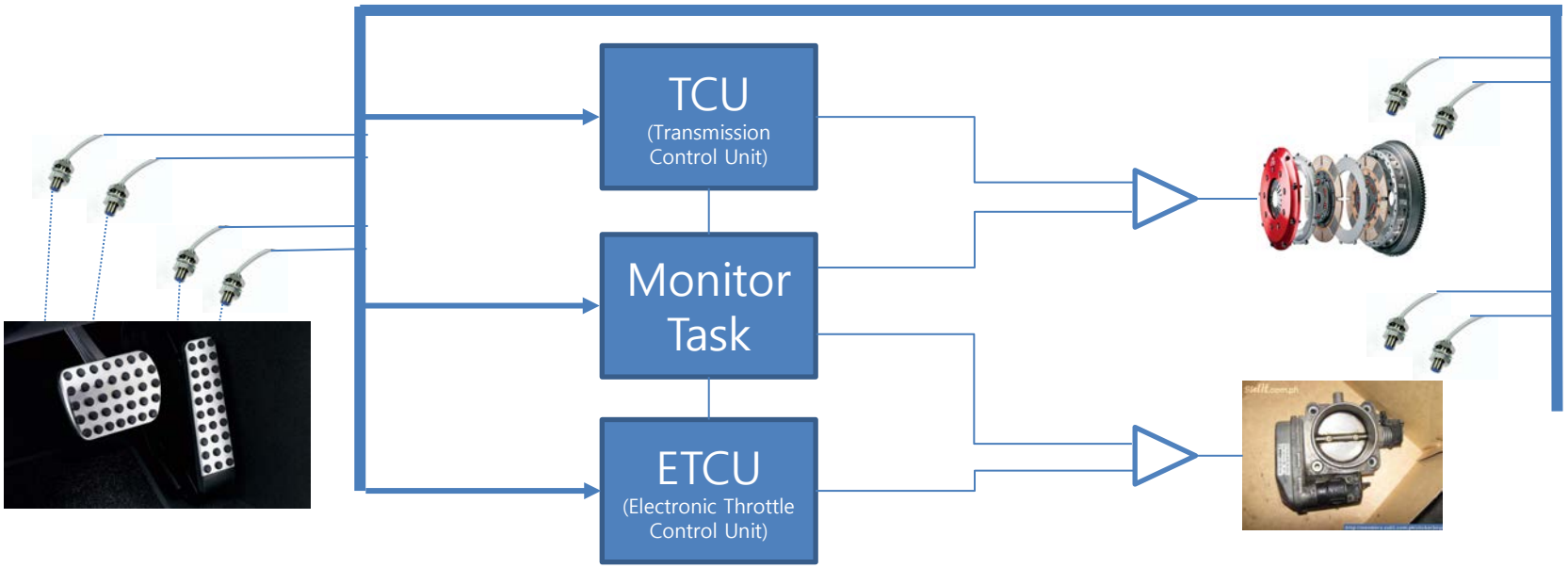
- 부적절한 다중화

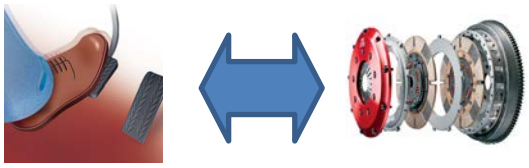


- 사실상 무한대의 테스트 공간



분산 SW와 급발진





깊은 제동 > 1초
⇒ 클러치 분리

가속 X > 1초
⇒ 쓰로틀 최소개방

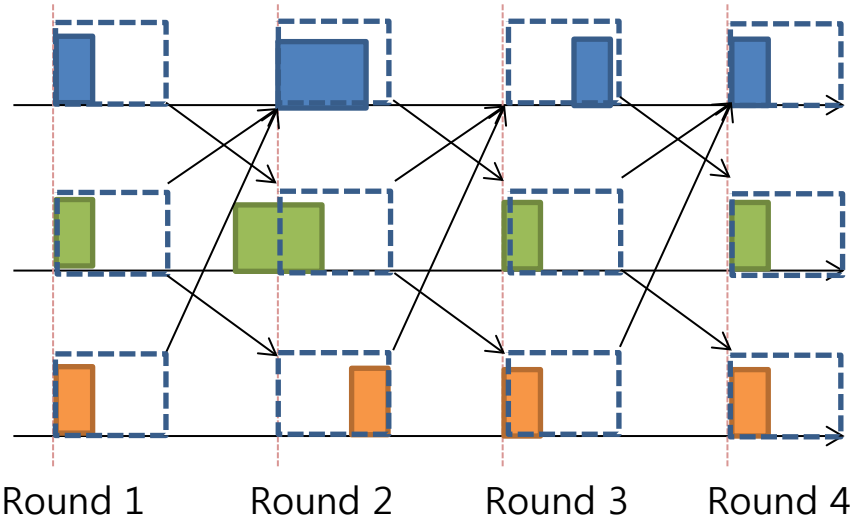
한 지점이 실패 하더라도 안전조건 보장 필요

접근 방법

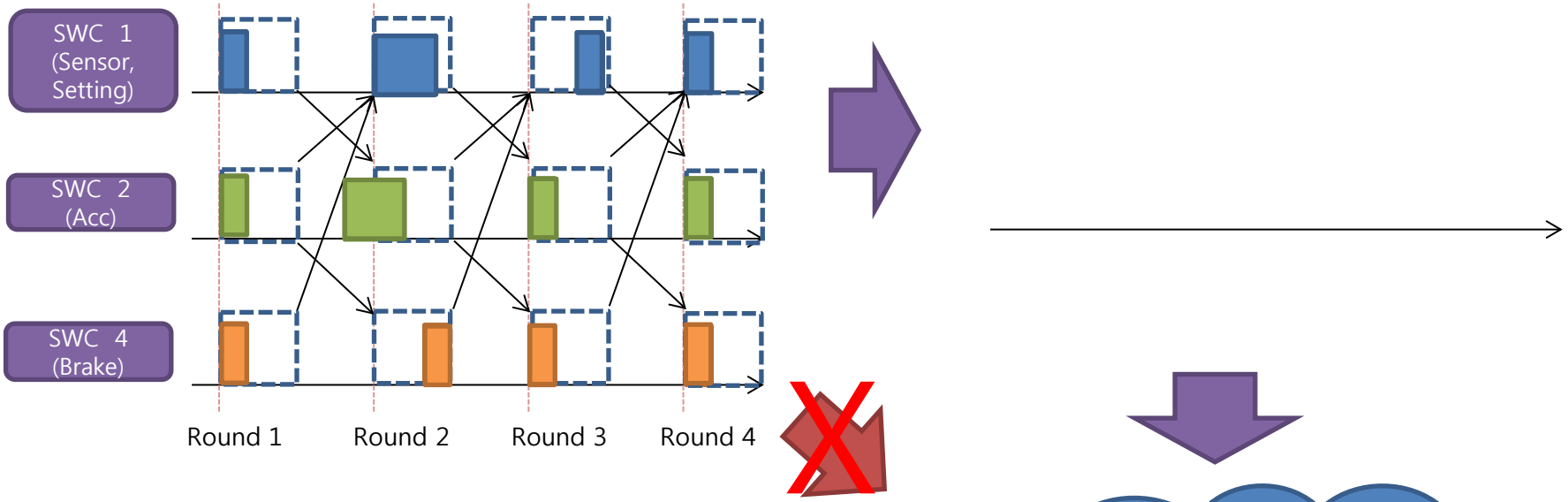
- SW 대상과 구현 방식을 통제하여 검증성 향상

- 대상 시스템: 실시간 제어 시스템
  - 동적 메모리 할당 금지
  - 실시간 수행의 무한 루프 (단순한 분기)

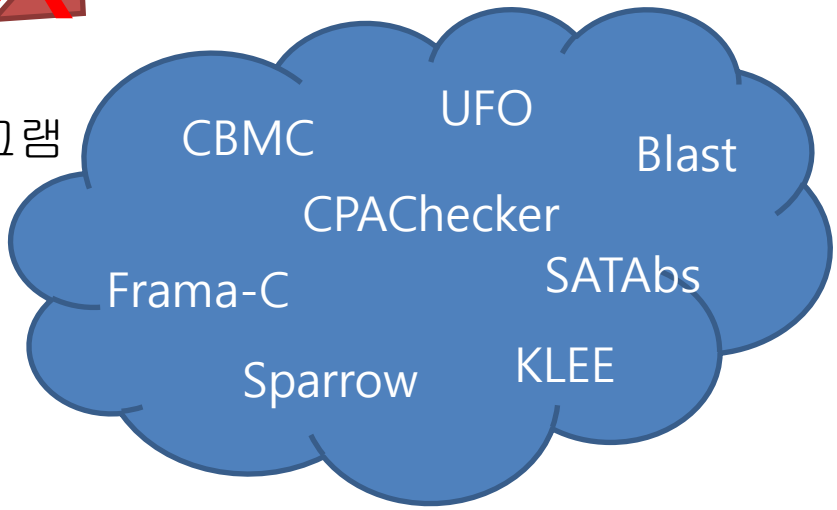
- 통신 방식 제한: 동기식 통신
  - 동기식 미들웨어 이용의 강제
  - 경쟁 조건의 제거



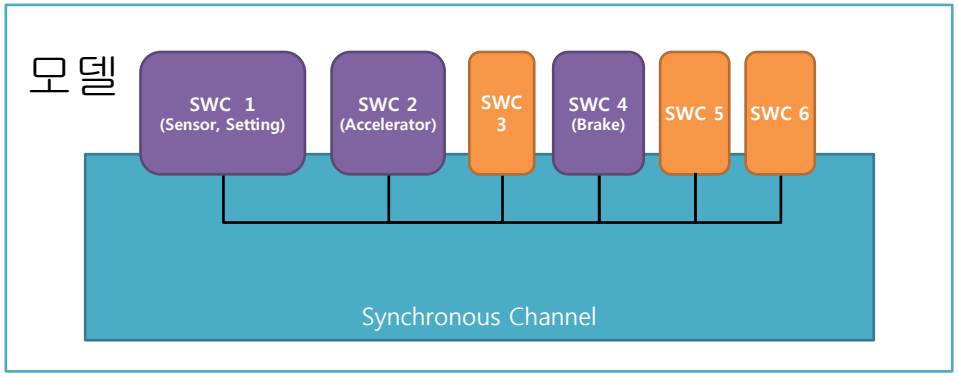
검증 방법

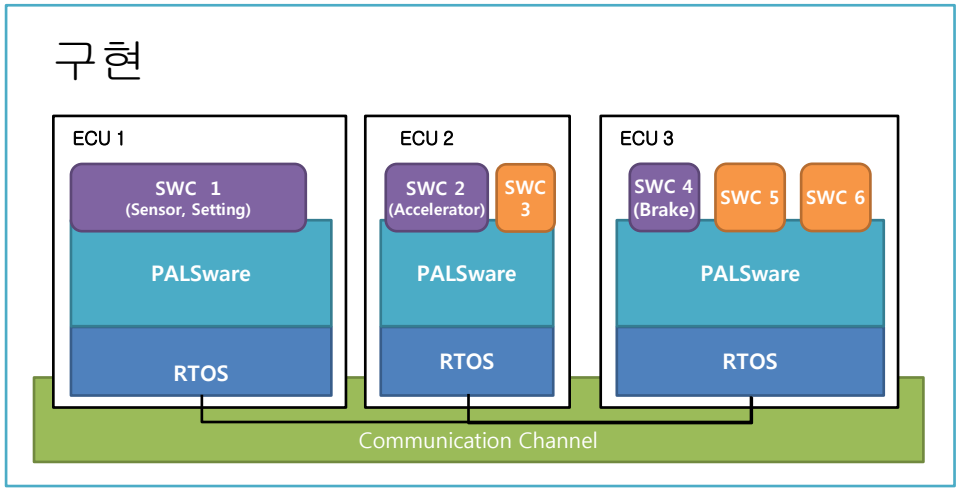


순차적 프로그램 검증도구



동등성 검증





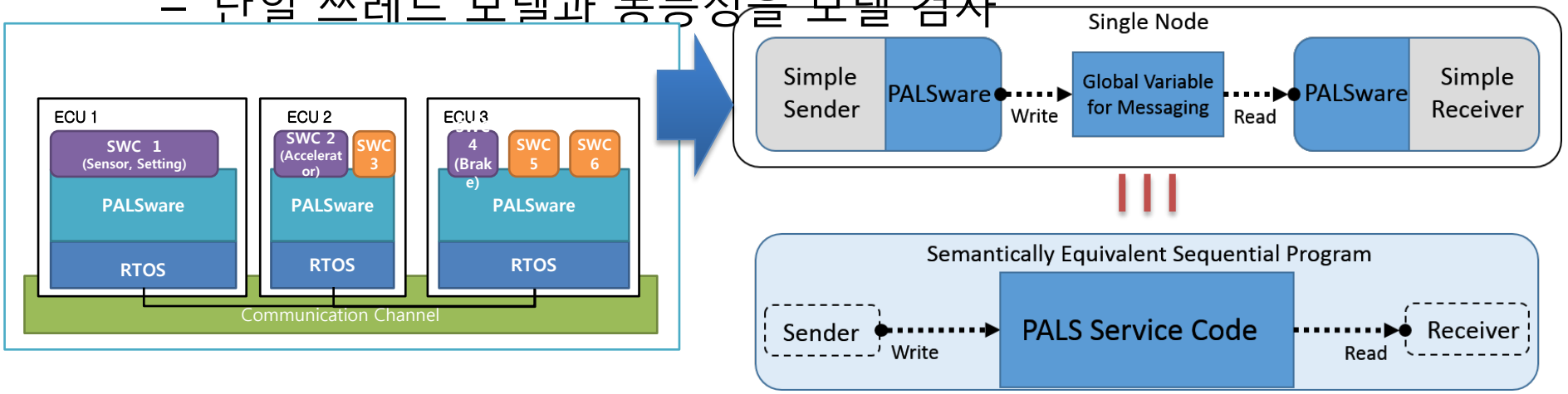
- 가정: RTOS와 네트워크는 비동기식 시스템을 성실히 구현한다

- 목적: 미들웨어는 동기식 모델과 동등한 의미론의 구현을 보장한다

  어떤 응용이 올라가더라도…

CBMC를 이용한 현재의 검증 전략

- 비동기 분산 시스템을 다중 쓰레드 환경으로 모델링
  - 하나의 Sender와 하나의 Receiver를 가지는 형상에 대하여 검증
  - Sender와 Receiver를 다중 쓰레드로 모델링하여 비동기 현상 재연
  - 네트워크는 전역변수 버퍼로 모델링
  - 단일 쓰레드 모델과 동등성을 모델 검사



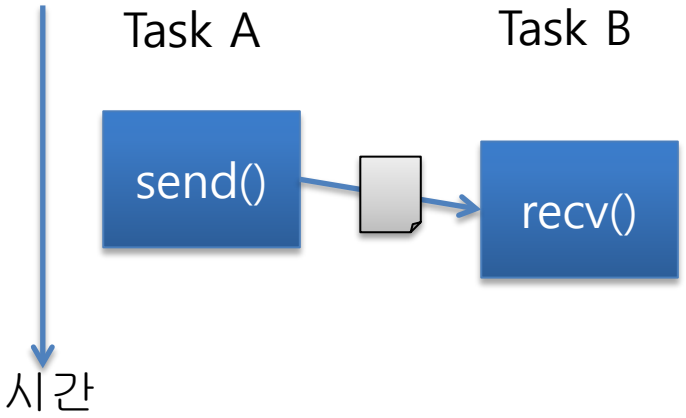
현재 검증 전략의 문제와 우회 방법 (1)

- 문제 1: 응용의 매개변수화
  - 미들웨어 사용 규약만 만족한다면 어떤 응용이 어떠한 미들웨어 API 호출 패턴을 가지더라도 모델 동등성이 보장되어야 한다
  - 1 Sender – 1 Receiver pair의 예에 한하여 검증
    - sender는 send(), receiver는 recv() 함수만 호출한다.

- 문제 2: CBMC는 무한 수행 프로그램 검증이 불가능
  - 우회 방법: 수학적 귀납법을 통하여 시간을 무한대로 확장
  - 매 주기마다 시스템이 도달할 수 있는 상태를 정의하고, Assume-guarantee를 통하여 모든 주기에 도달할 수 있는 상태를 조사
  - 수학적 귀납법의 엄밀함의 결여가 존재함

현재 검증 전략의 문제와 우회 방법 (2)

- 문제 3: 분산된 API 수행의 병렬성
  - 검증시에는 분산 API 호출을 Mutex로 보호 (상태 폭발 방지 목적)
  - 실제로는 Task A가 send() 명령을 수행하는 동안 Task B는 recv() 명령을 수행할 수 있다.
  - 두 API 수행은 단일성을 가지는가?
  - 각 API가 네트워크로 write() 또는 read()만 한다면 분산 환경에서의 API 단일성은 보장된다고 선언



- 문제 4: 임의의 topology로 증명된 특성이 확장되는가?
  - 각 Sender와 Receiver 포트는 disjoint한 메모리 영역을 사용하므로 임의의 topology에서도 검증된 특성이 확장된다고 선언

우리의 고민

- 실제 코드와 검증 코드간의 간극
  - CBMC를 이용한 검증을 수행하기 위하여 미들웨어 코드의 상당량 단순화
- 항전 인증 전문가의 의견
  - DO-178C 인증 수준에 미흡하다
- 분산 응용 검증의 자동화는 필요함
- 미들웨어 검증을 위하여 고려 중인 사항
  - 대화형 정리 증명기의 사용
  - 함수형 언어의 도입