항공전자 SW 위험 분석

Fault injections: Practical enabling technology for risk analysis

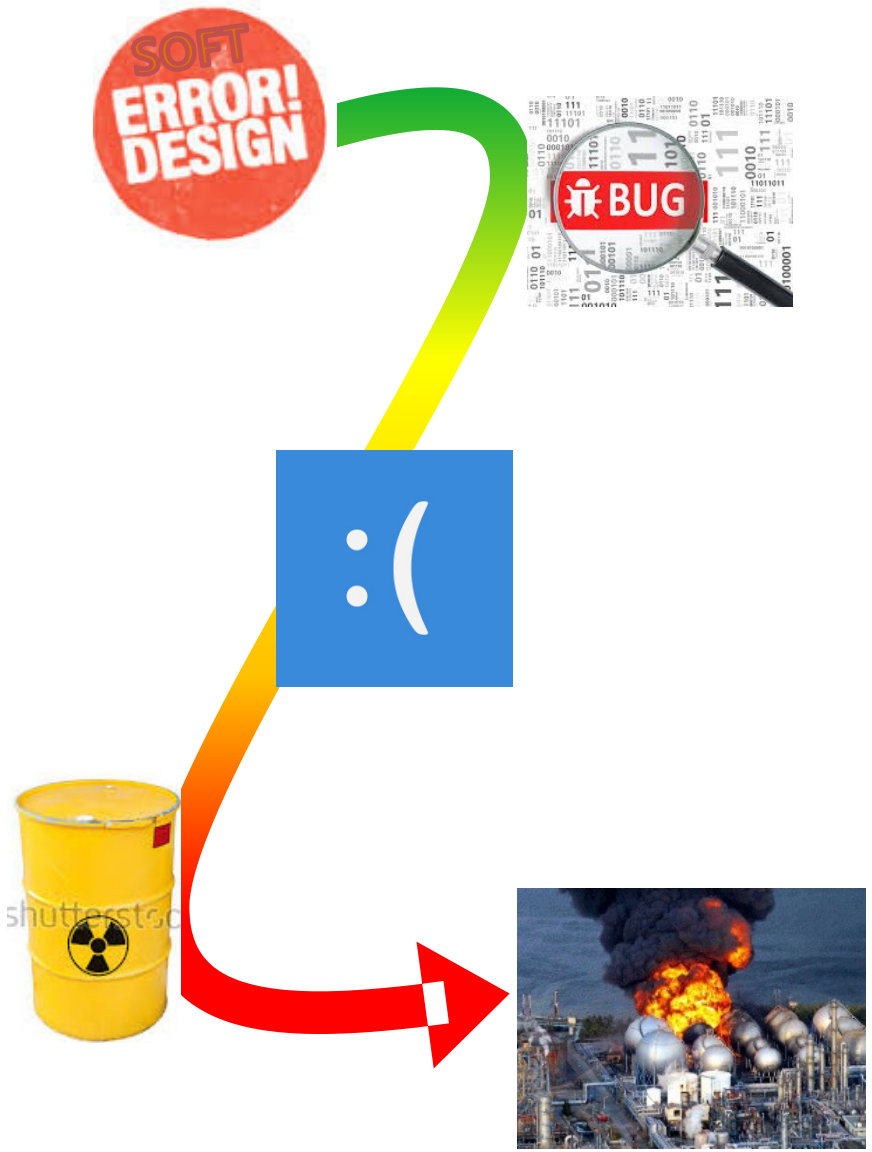
고신뢰성 임베디드 시스템 연구실

한국항공대학교
나종화

Outlines

- Are you safe?
- Hazard & Risk in Avionics
- Fault injection
- Model based Automatic Risk analysis System (MARS)

결함 고장 용어



- **Error, 에러**
  - SW – 설계 오류 Design Error
  - HW – Soft error
- **Fault, 결함**
  - 잠복 에러가 드러남
  - 고장의 원인
- **Failure, 고장**
  - 기능수행 실패
  - 결함의 결과
- **Hazard, 위협 요소**
  - 위험한 조건
  - 고장의 결과
- **Accident**

목표: 안전

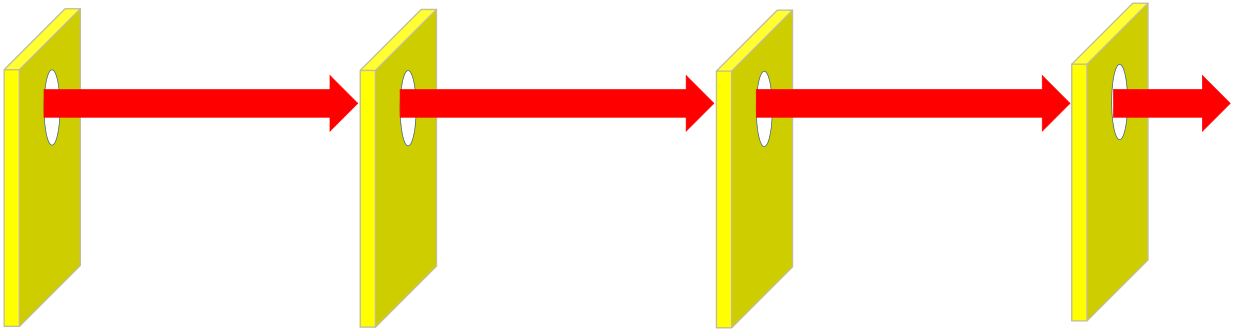
Error

Fault

Failure

Hazard

Accident



에러 검출

결함감내 시스템

Fail-Safe

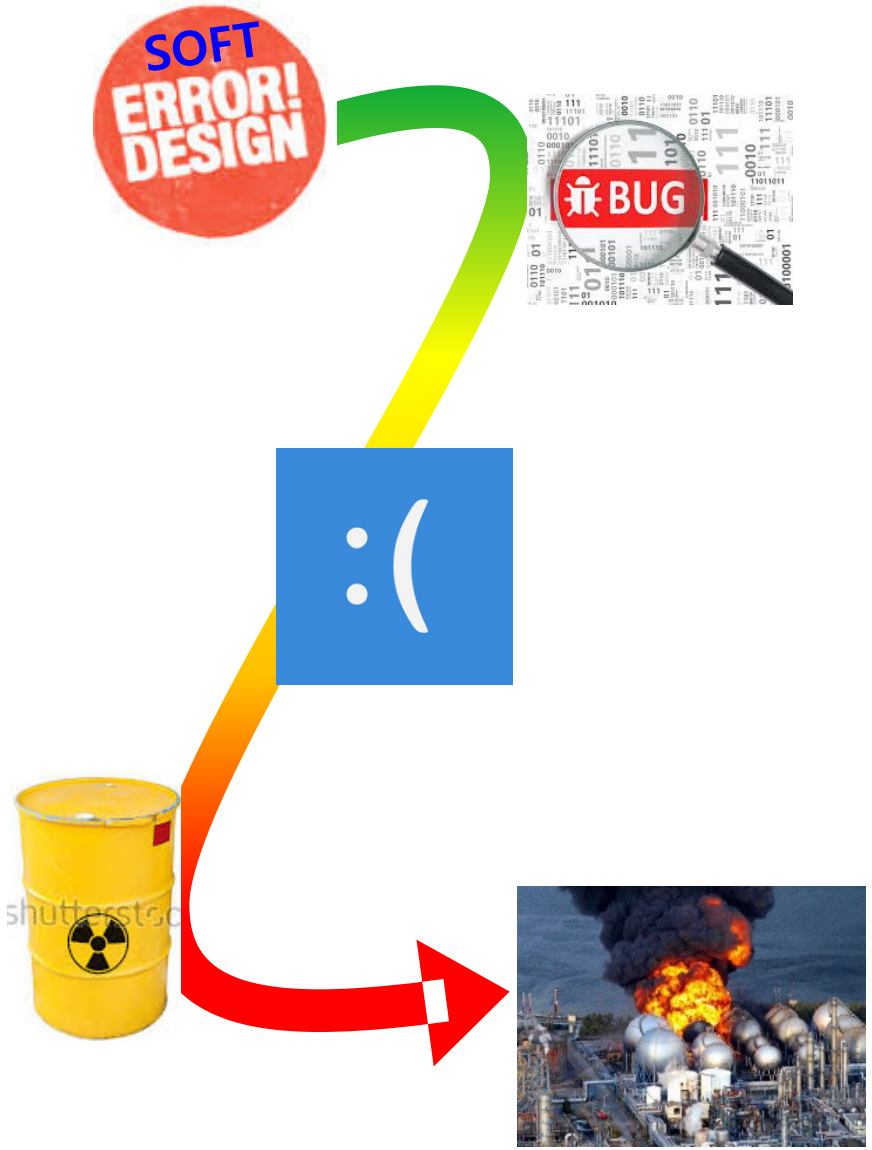
사고 예방 대응

위험은 현실.. 대책이 필요

사고유형	2017	2016	2015	2014	2013
합계	**291,285**	**303,578**	**315,736**	**297,337**	**294,707**
도로교통	216,335	220,917	232,035	223,552	215,354
화재	44,178	43,413	44,435	42,135	40,932
산불	692	391	623	492	296
열차	52	62	85	130	148
지하철	53	61	53	79	84

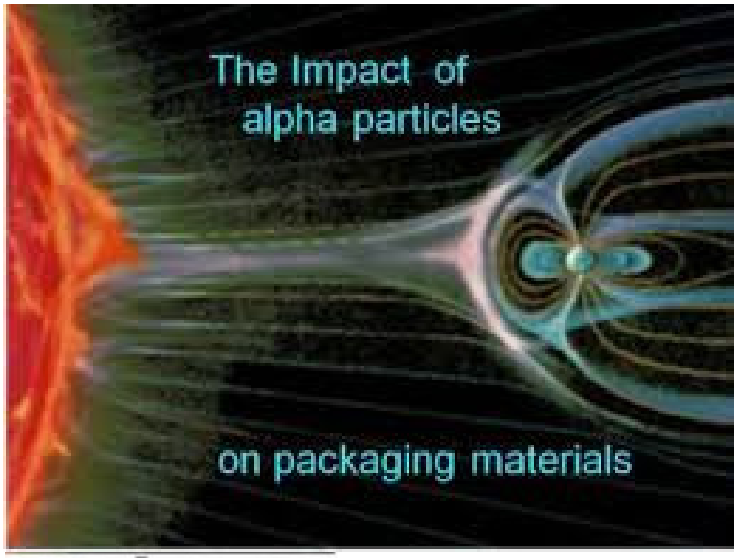
https://www.mpss.go.kr/home/policy/statistics/statisticsOkay/

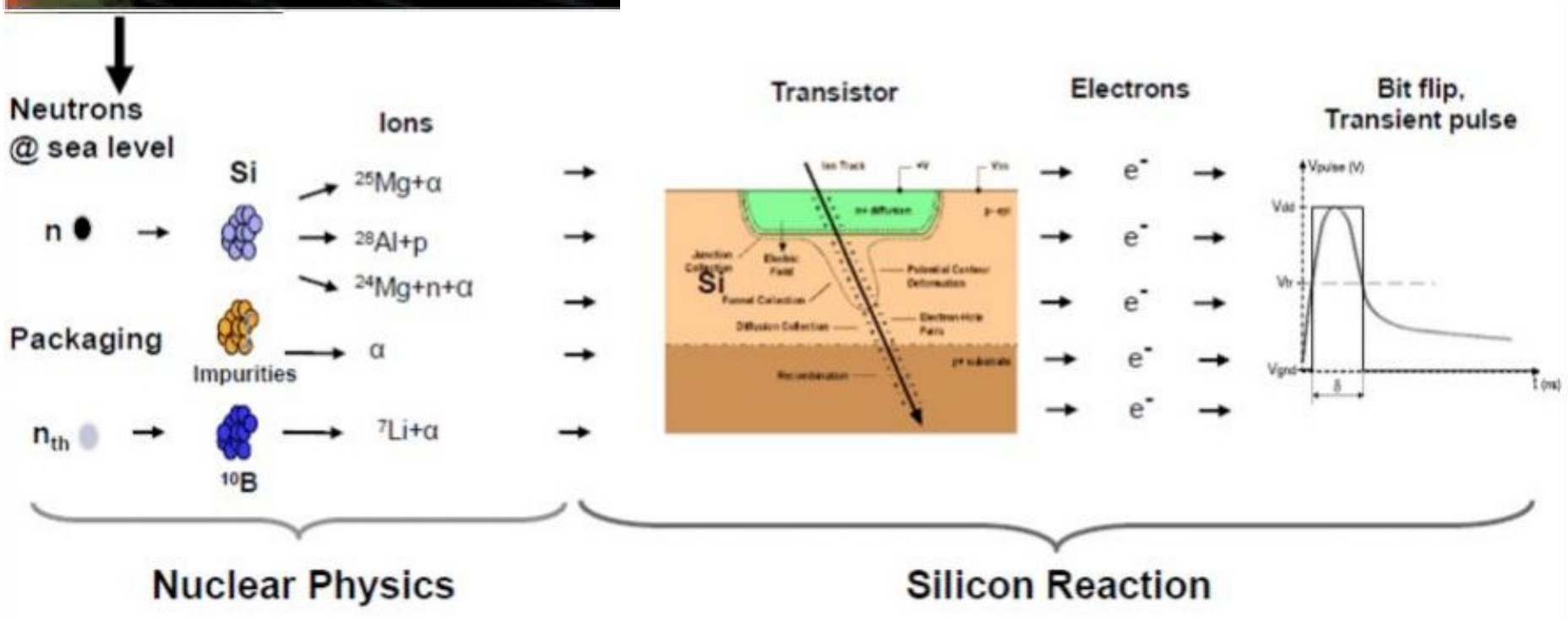
결함 고장 용어 리뷰



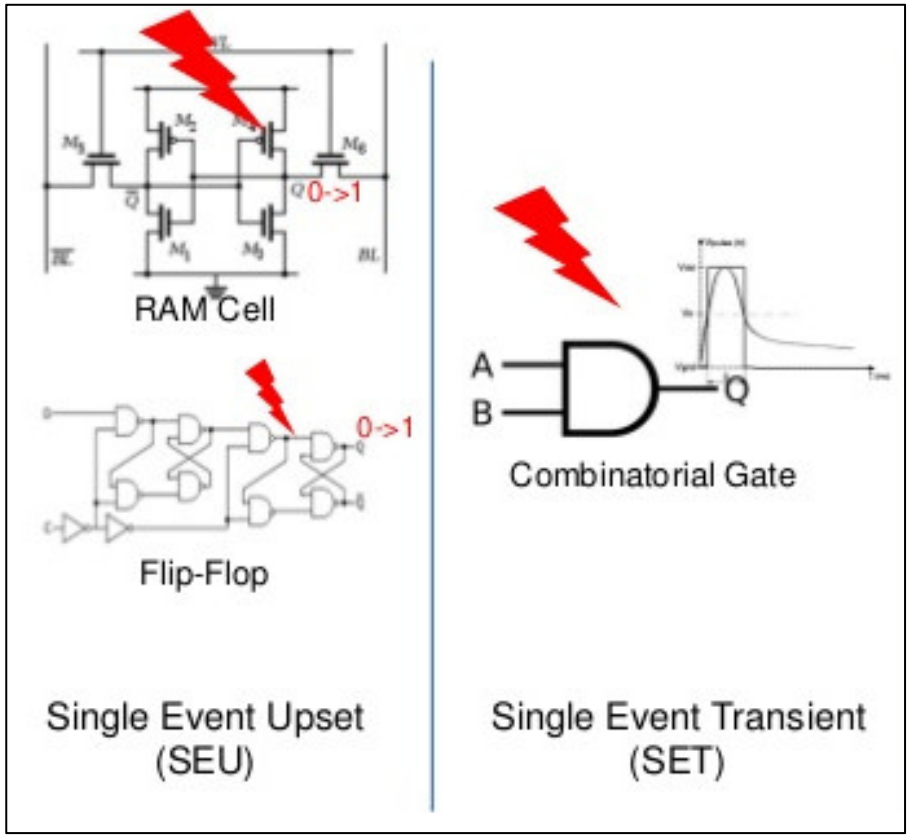
- **Error, 에러**
  - SW – 설계 오류 Design Error
  - **HW – SOFE ERROR**
- **Fault, 결함**
  - 잠복 에러가 드러남
  - 고장의 원인
- **Failure, 고장**
  - 기능수행 실패
  - 결함의 결과
- **Hazard, 위협 요소**
  - 위험한 조건
  - 고장의 결과
- **Accident**

Soft Error ?

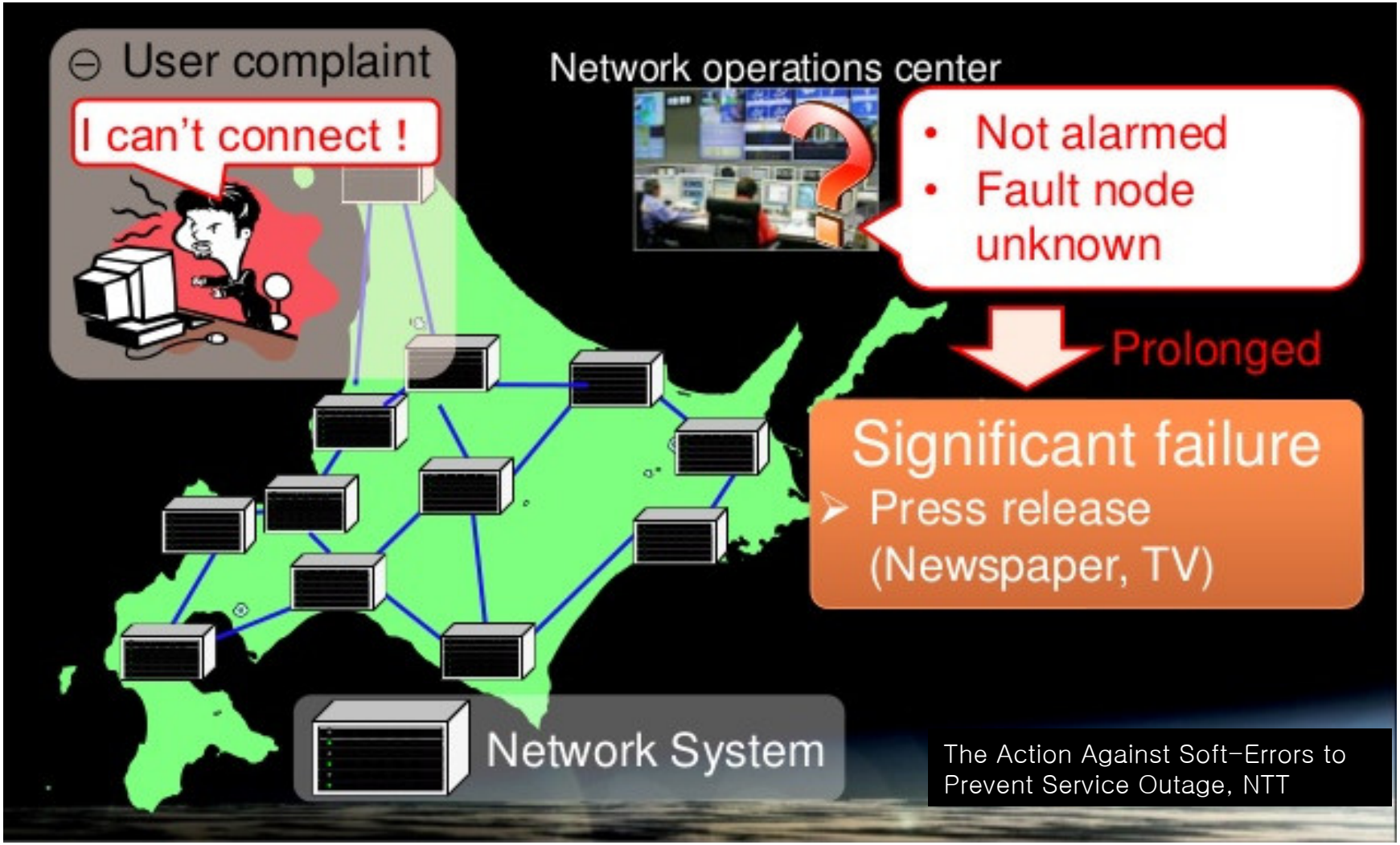

The Impact of
alpha particles
on packaging materials


Neutrons
@ sea level
n
Packaging
Impurities
n_{th}
Si
^{10}B
Ions
$^{25}Mg+\alpha$
$^{28}Al+p$
$^{24}Mg+n+\alpha$
α
$^{7}Li+\alpha$
Transistor
Si
Electrons
e⁻
e⁻
e⁻
e⁻
e⁻
Bit flip,
Transient pulse
Nuclear Physics
Silicon Reaction

Soft error 결과



Soft error 사회적 결과



Soft error

- Soft error 현상
  - Random glitch in semiconductor devices
- Soft error 원인?
  - 고 에너지 우주선(cosmic rays): 양성자 중성자
  - 태양 입자 : 알파 입자, 베타 입자
  - 방사성 동위원소: 알파 입자
- Soft error의 증가 원인 별 분석
  - 기술:고 직접 회로 → 잡음 여유 ↓ 및 간섭현상 ↑
  - 개발:수요자요구사항 ↑→HW&SW 복잡도 ↑ →에러 발생 ↑
  - 환경: 우주, 극지, 고고도, 구글 서버 팜, tera & peta DRAM
- 결과
  - 순간 및 영구 결함 발생 & 사고의 원인

Outlines

- Are you safe?
- Hazard & Risk in Avionics
- Fault injection
- Model based Automatic Risk analysis System (MARS)

System safety process

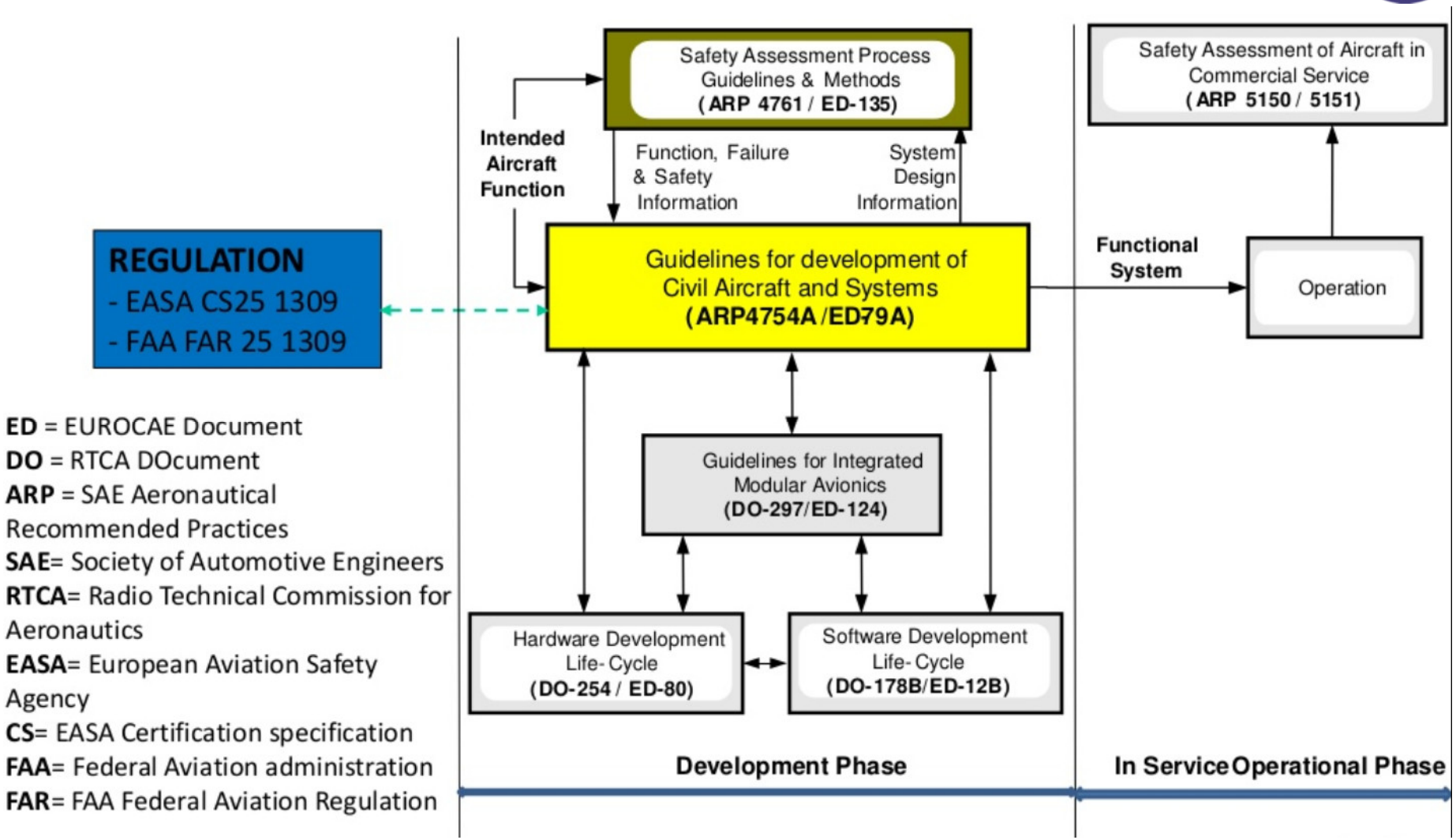
Hazard Analysis Type (HAT)

- Conceptual Design (CD-HAT)
- Preliminary Design (PD-HAT)
- Detailed Design (DD-HAT)
- System Design (SD-HAT)
- Operations Design (OD-HAT)
- Human Design (HD-HAT)

Hazard Analysis Techniques

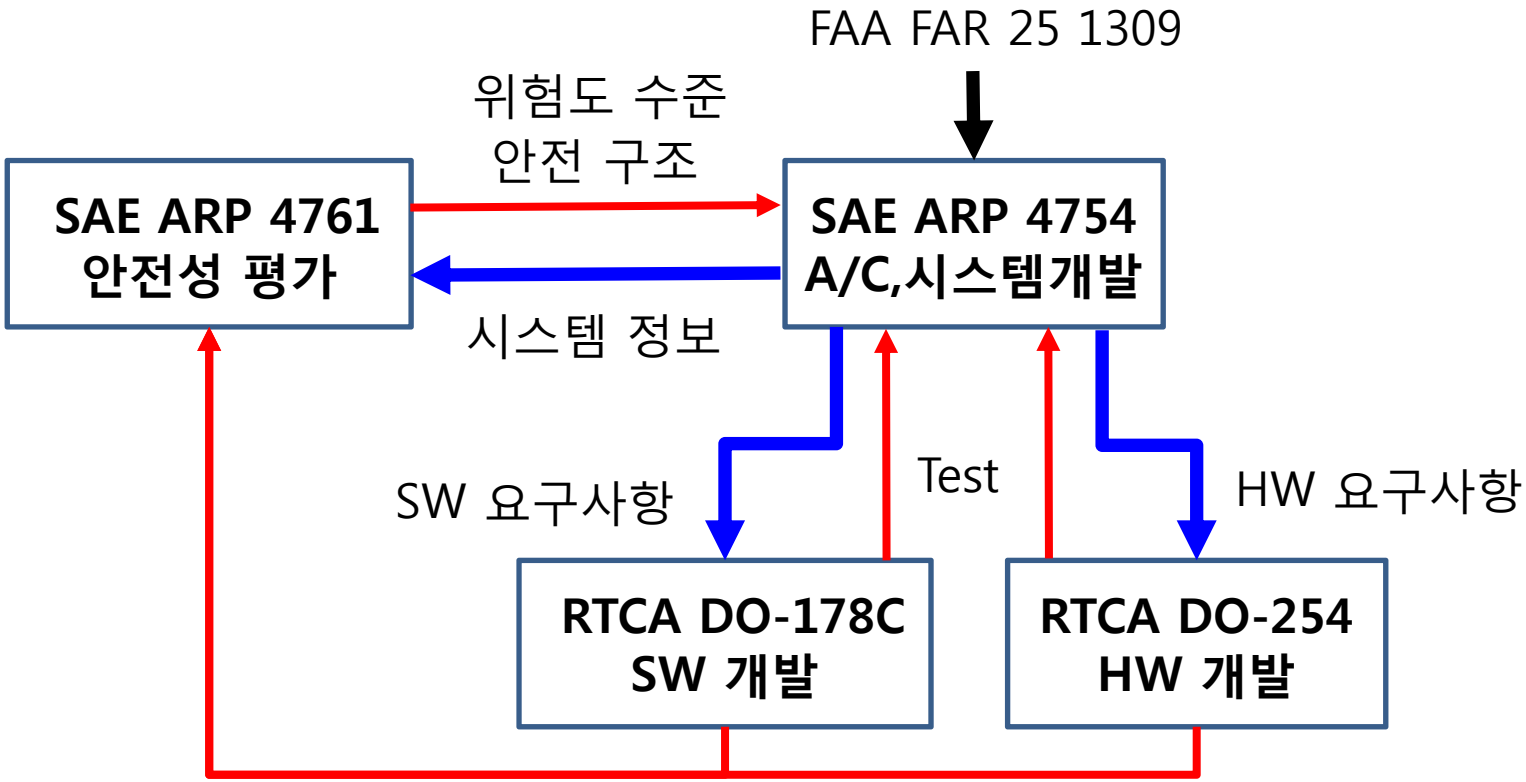
1. Preliminary Hazard List (PHL)
2. Preliminary Hazard Analysis (PHA)
3. Safety Requirements/Criteria Analysis (SRCA)
4. Subsystem Hazard Analysis (SSHA)
5. System Hazard Analysis (SHA)
6. Operations & Support Hazard Analysis (O&SHA)
7. Health Hazard Assessment (HHA)
8. Fault Tree Analysis (FTA)
9. Failure Modes and Effects Analysis (FMEA)
10. Fault Hazard Analysis (FaHA)
11. Functional Hazard Analysis (FuHA)
12. Sneak Circuit Analysis (SCA)
13. Software Sneak Circuit Analysis (SWSCA)
14. Petri Net Analysis (PNA)
15. Markov Analysis (MA)
16. Barrier Analysis (BA)
17. Bent Pin Analysis (BPA)
18. Threat Hazard Assessment (THA)
19. Hazard and Operability Study (HAZOP)
20. Cause Consequence Analysis (CCA)
21. Common Cause Failure Analysis (CCFA)
22. Management Oversight and Risk Tree (MORT)
23. Software Hazard Assessment (SWHA)

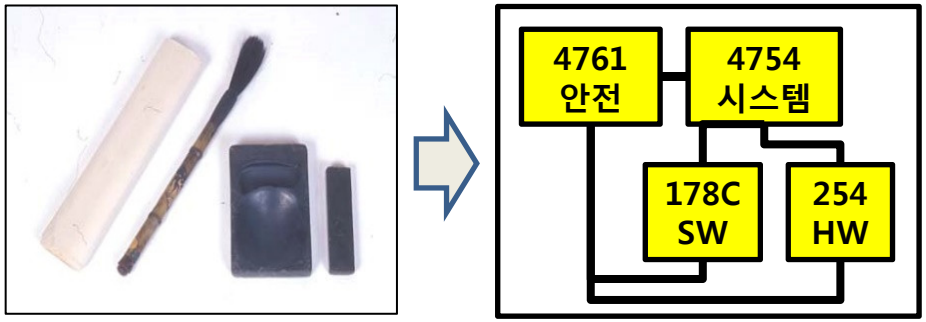
항공 분야의 risk 관리



ED = EUROCAE Document
DO = RTCA DOcument
ARP = SAE Aeronautical Recommended Practices
SAE= Society of Automotive Engineers
RTCA= Radio Technical Commission for Aeronautics
EASA= European Aviation Safety Agency
CS= EASA Certification specification
FAA= Federal Aviation administration
FAR= FAA Federal Aviation Regulation

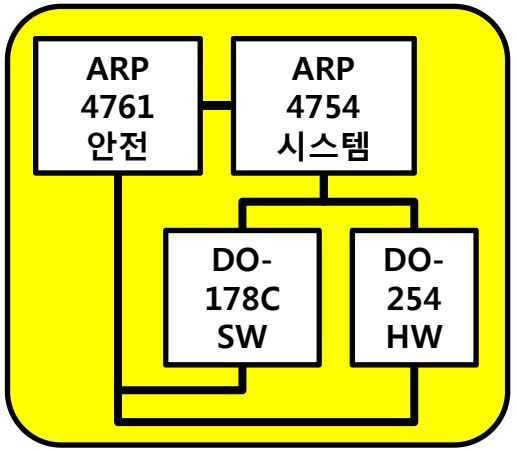
항공4우


FAA FAR 25 1309
위험도 수준
안전 구조
SAE ARP 4761
안전성 평가
SAE ARP 4754
A/C,시스템개발
시스템 정보
SW 요구사항
Test
HW 요구사항
RTCA DO-178C
SW 개발
RTCA DO-254
HW 개발


4761
안전
4754
시스템
178C
SW
254
HW

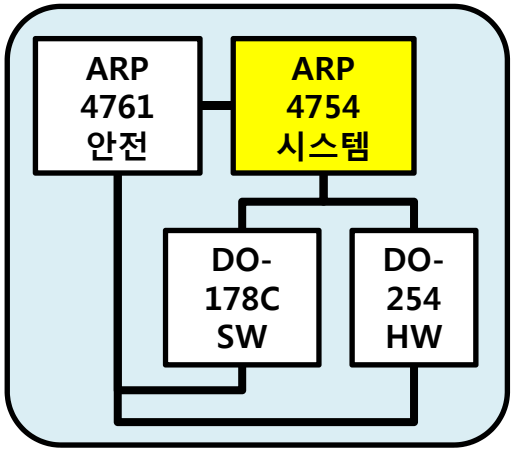
개발보증

- 1단계 : 시스템 개발
  - 항공전자 기능 개발 절차 ← ARP 4754A
    - 항공기 **시스템** 설계
  - 항공전자 안전 개발 절차← ARP **4761**
    - 각 시스템 고장률 계산,
    - if (요구 **안전** 수준 미달),
      then (결함감내기능 추가 → 안전성 개선)
- 2단계 : 아이템 개발
  - 시스템 기능을 HW & SW 에 할당
  - **HW** 설계 ← **DO-254**
  - **SW** 설계 ← **DO-178C**



SAE ARP 4754A

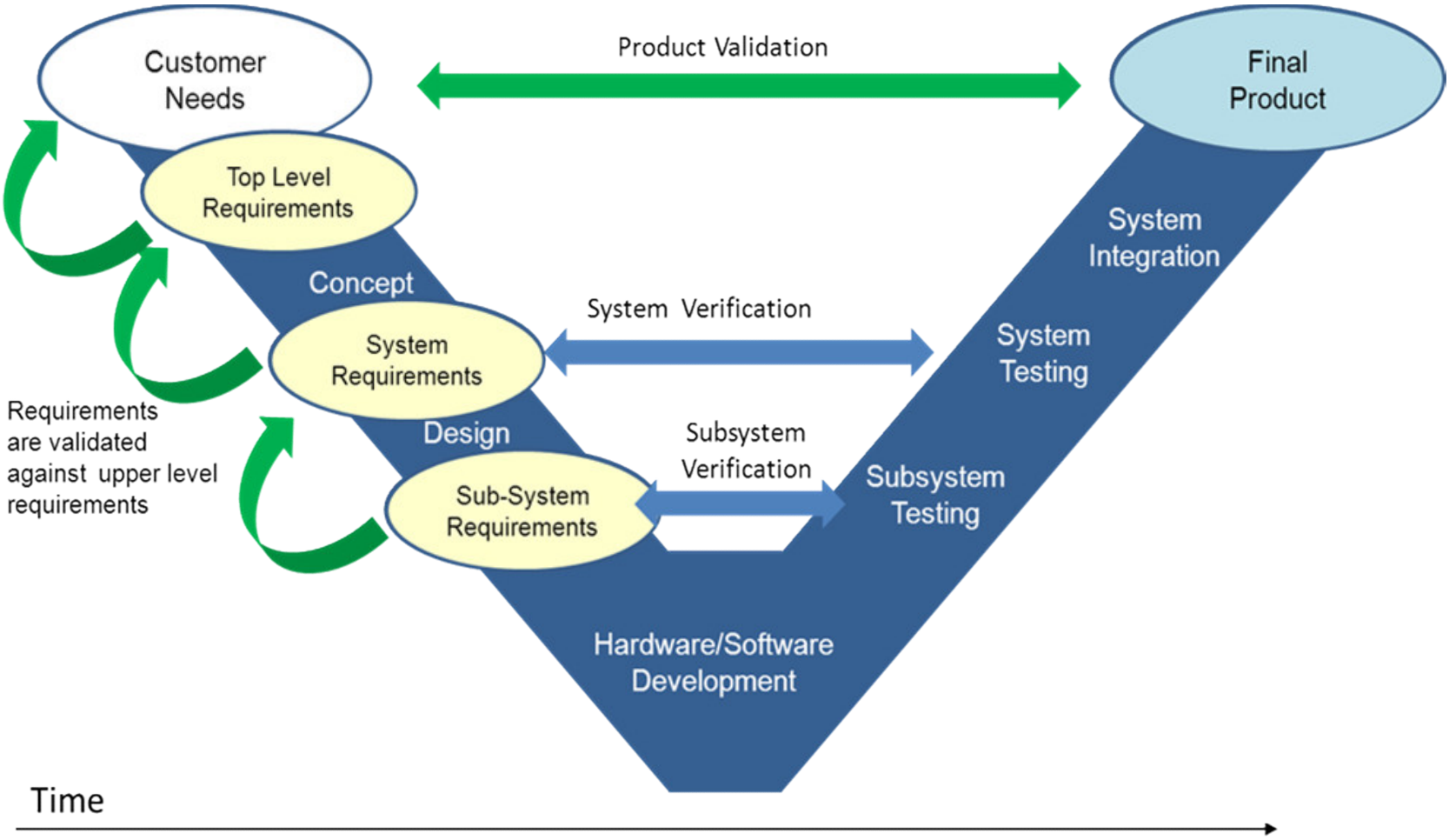
- ARP4754A 이름
  - Guidelines for Development of Civil Aircraft and Systems
- 언제 시작?
  - HW, SW 개발 전에
- 활용 범위
  - 항공기 (Aircraft or A/C)수준의 기능 개발
  - 각 시스템 및 시스템들간의 상호관계
  - 준수 규정은 아님
  - 그러나 인증에 필요?



4754A Scope

- 항공기 기능 및 운영 환경을 고려한 시스템의 개발
- Validation:항공기 및 시스템 요구사항 검증
- Verification:인증 설계 및 보증을 위한 구현 내용 확인
- 개발 계획 및 요구사항, 개발 표준
- 안전 평가, 개발안전보증수준 (DAL) 할당, V&V 확인 및 검증, 형상관리
- 다음 사항과는 무관
  - 항공기 구조 개발
  - 소프트웨어 개발 (DO-178C)
  - 전자부품 개발 (DO-254)
  - 안전성 평가 방법 (ARP 4761)

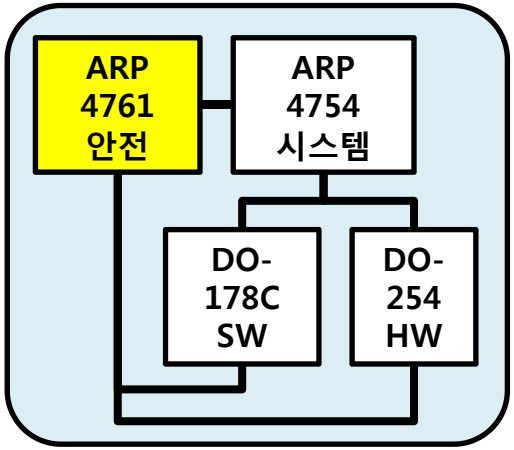
4754A process



http://www.sarel-consult.de/en/consulting.html

SAE ARP 4761

- ARP 4761 이름
  - 민간항공기 시스템 및 장비의 **안전성 평가** 수행 지침 및 방법
- ARP 4761 안전 평가 절차
  - 기능 위험성 평가(Functional Hazard Assessment)
  - 예비 시스템 안전도 평가(Preliminary System Safety Assessment)
  - 시스템 안전도 평가(System Safety Assessment)
- ARP 4761 안전 평가 기법
  - 고장모드 및 영향분석(Failure Mode and Effects analysis)
  - 고장 수목 분석(Fault Tree Analysis)
  - 의존성 다이어그램(Dependence Diagram)
  - 마르코프 분석(Markov Analysis)



ARP 4761 안전 평가 절차

- 기능 해저드 평가 FHA
  - Functional Hazard Assessment (FHA)
  - 기능에 대하여 고장조건을 식별 및 분류하는 체계적인 검토
  - 항공기/시스템 기능 식별 → 기능의 고장조건 식별
  - 고장조건, 영향, 분류, 안전 요구사항을 도출
- 예비 시스템 안전 평가 PSSA
  - Preliminary System Safety Assessment (PSSA)
  - 고장조건을 완성하고 이에 대응하는 안전 요구사항을 개발
  - 안전 요구사항 목표 설정 및 검증
  - 하부 아키텍처 및 아이템으로 할당되는 파생 안전요구사항을 식별
- 예비 시스템 안전 평가 SA
  - System Safety Assessment (SSA)
  - 시스템이 안전요구사항의 충족여부를 **확인**하는 체계적인 평가
  - PSSA 활동과 유사하지만 그 범위가 다르며 FHA 및 PSSA에서 정의된 대로 정성적·정량적 안전요구사항을 모두 충족 하는지 확인

기능 해저드 평가 FHA

- 기능 해저드 평가 FHA
  - 기능에 대하여 고장조건을 식별 및 분류 검토
- 항공기 (A/C) 및 시스템 수준에서 수행
  - Aircraft FHA, System FHA
- 목표
  - 발생 가능한 고장의 환경 및 심각도 **식별 및 분류**
- 수행 내용
  - 각 고장 조건의 식별
  - 각 고장 조건의 분류
  - 각 고장 조건의 영향 식별
  - 상황 (비행 단계, 환경 etc.)

기능 해저드 평가 FHA 종류

Aircraft FHA

Funct Failure Ref	Function	Phase	Failure Condition	Failure Effect	Classification
1.1.1	Decelerate aircraft on ground	Landing / RTO	Loss of deceleration capability on the ground	Crew is unable to stop the aircraft on runway.	Catastrophic
1.1.2	Decelerate aircraft on ground	Landing	Unannunciated loss of all Automatic Stopping functions.	Crew must use manual procedures to stop the aircraft.	Major

Brake System FHA

Funct Failure Ref	Function	Phase	Failure Condition	Failure Effect	Classification
36-40 1.1	Wheel Braking	Landing / RTO	Loss of all wheel braking.	Crew's ability to stop the aircraft on runway is significantly reduced.	Hazardous
36-40 1.2	Auto-Braking	Landing / RTO	Unannunciated loss of Autobraking	Crew must use manual procedures to stop the aircraft.	Major

예비 시스템 안전 평가 PSSA

- 예비 시스템 안전 평가 PSSA?
  - FHA 고장 조건에 대응하는 안전 요구사항 개발
  - 제안된 시스템이 식별된 위협요소들에 대응하는 안전 요구사항들을 충족함을 증명
- 제안된 구조의 분석
  - 항공기 구조와 항공기의 고장 조건, 그리고 고장들 간의 연관관계를 분석
- Design tradeoff 검토
  - 기본 설계 및 대체 설계 정보를 설계 단계에 제공하여 design tradeoff 등 다양한 분석 기회 제공

예비 시스템 안전 평가 PSSA 입출력

- Inputs / Analyses
  - Functional Hazard Analysis (고장 식별 및 분류)
  - 블록도, 회로도, 설계도, 부품 재료 목록 등
  - 설계 회의, 계획
  - 고장모드영향분석 FMEA (Single point failures)
  - 고장수목분석 FTA
  - 공통모드분석 Common Mode Analysis
- Outputs
  - 파생 안전요구사항 (Derived Safety Requirements)
  - 고장률 할당 (Failure rate allocations)
  - 안전 분석 (FTA & CMA) of alternative design
  - Design tradeoff 제시

시스템 안전 평가 SSA

- 시스템 안전 평가 SSA?
  - 시스템이 안전요구사항의 충족여부를 확인하는 체계적인 평가
- 수행 내역
  - PSSA와 활동 내역은 유사
  - PSSA는 시스템과 아이템의 안전 요구사항을 제작하는 활동
  - SSA는 구현된 설계 결과물이 안전 요구사항을 충족하는지 확인하는 활동

SSA 보고서 목차

- 보고서 요약 Compliance Summary
  - 시스템 안전 결론 System Safety Conclusions
  - 승무원 안전 수칙
  - 주요 잠재(latent) 고장 검토
  - 정비 절차
  - 안전 요구사항 및 준수
- System 및 안전설계 개요
- 기능위협요소분석 (Functional Hazard Assessment)
- 고장모드 및 영향분석 (Failure Mode & Effects Analysis)
- 설계 보증 평가
- 결함수목분석 (Fault Tree Analysis)
- 공통 원인 분석 (Common Cause Analysis)

ARP 4761 안전 평가 기법

- 고장모드 및 영향분석(Failure Mode and Effects analysis)
- 고장 수목 분석(Fault Tree Analysis)
- 의존성 다이어그램(Dependence Diagram)
- 마르코프 분석(Markov Analysis)

고장모드 및 영향분석 FMEA

- 시스템의 안전성 평가의 최적 기준을 달성하기 위한, 경험적 관점에서 분석
- 60년대 항공우주 분야(아폴로 프로젝트) 시작
- 원자력, 자동차, 플랜트 등 안전 필수 (safety critical) 산업 전반에서 활용
- FMEA Table 예시

FMEA Worksheet

Filter

	Function Name (Mo...	Failure Mode (Mo...	Failure Rate (M...	Mission Phase (M...	Failure Effect (Mo...	DetectionMethod (Mode)	Comments (Mode)
1	+5 Volt	+5V out of spec.	0.214300	All Phases	Possible P/S shutdown	Power Supply Monitor tri... shuts down supply and passes "invalid power supply(P/S)" to other BSCU system	BSCU channel fails
2		+5V short to ground	0.285700	All Phases	P/S shutdown	Power supply monitor passes invalid P/S to other BSCU system	BSCU channel fails

FMEA Table

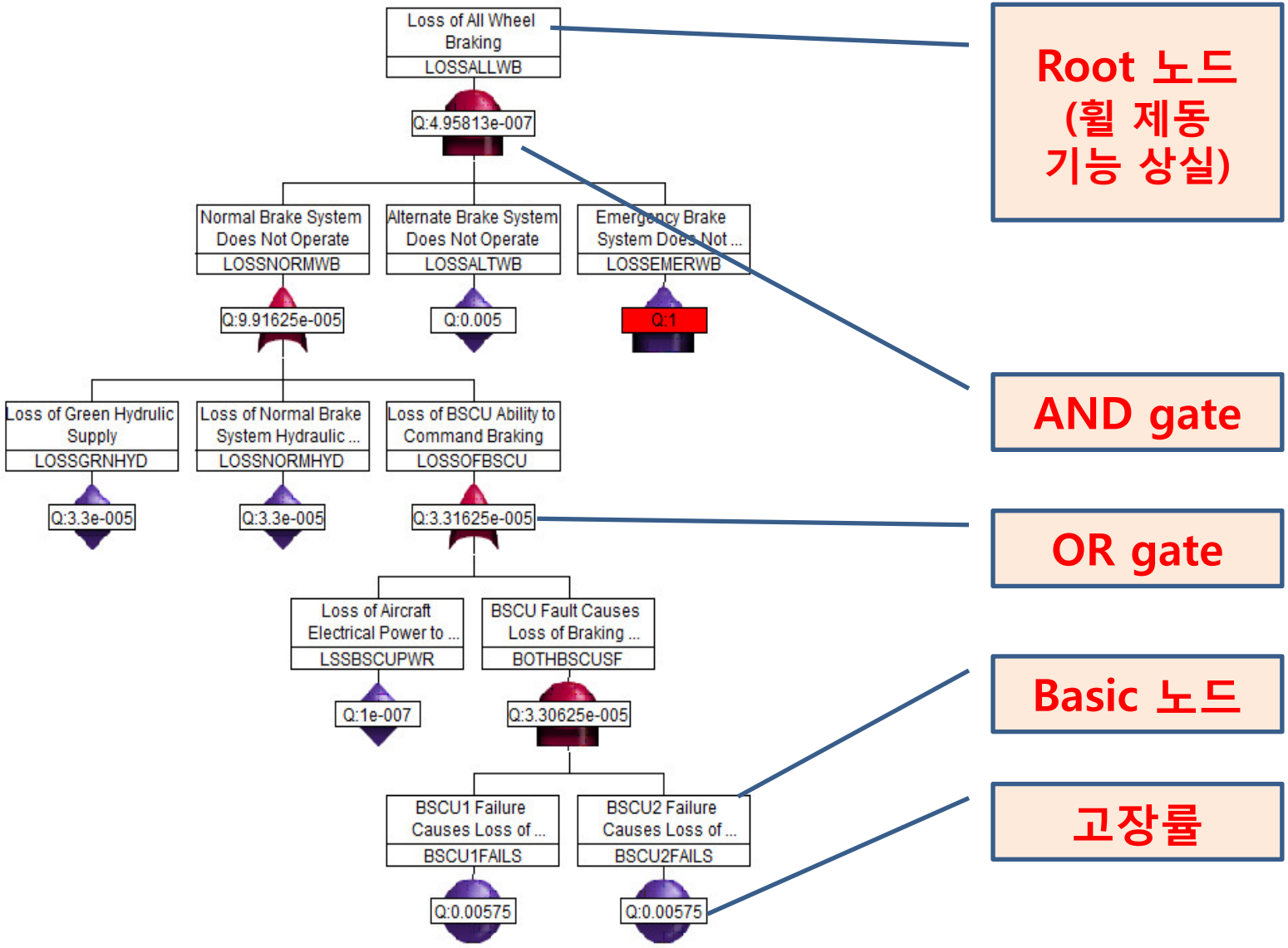
- FMEA Table
  - 잠재고장모드 영향분석 및 심각도 식별,
  - 고장 회피 기능 제시
- FMEA worksheet
  - 고장 식별, 원인 설명, 대응 방법 제시
  - 위험도 Risk Priority Number (RPN) = severity x occurrence x detection
    - Severity: Importance of the effect on customer requirements
    - Occurrence : Frequency with which a given cause occurs
    - Detection: Ability of the control scheme to detect a given cause

id	고장 모드	고장 영향	심각도	원인분석	발생도	검출도	Risk Priority #

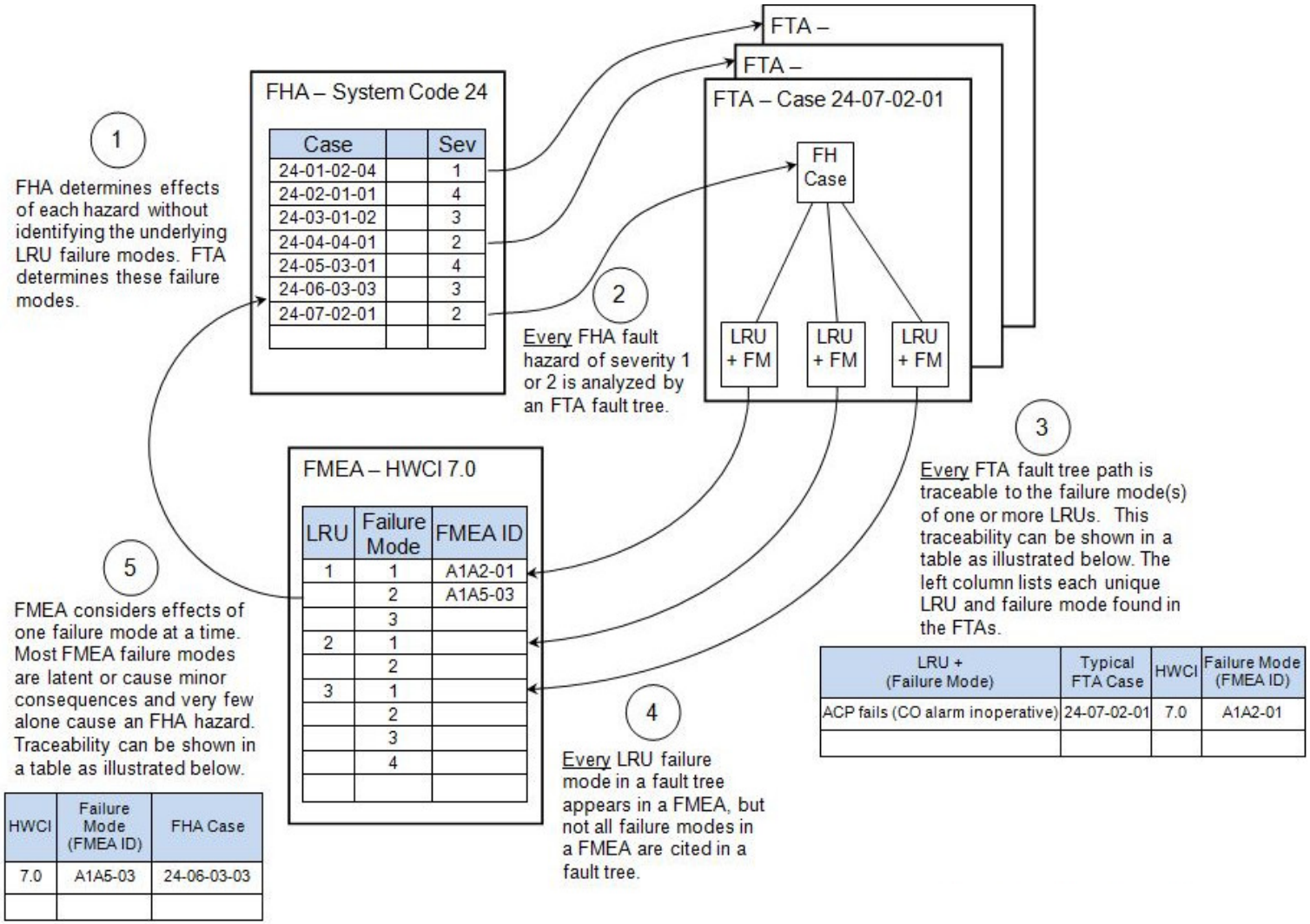
고장 수목 분석(Fault Tree Analysis, FTA)

- 분석대상
  - 잠재 고장 사건 (top event)의 원인 및 확률
- 분석 방법
  - AND/OR 논리를 이용
  - Top-down 방식으로 분석
- 사용법
  - 위험분석에서 원인분석에 활용
  - FMEA수행 후 고장 사건 확률 추정에 활용

휠 브레이크 시스템 FTA

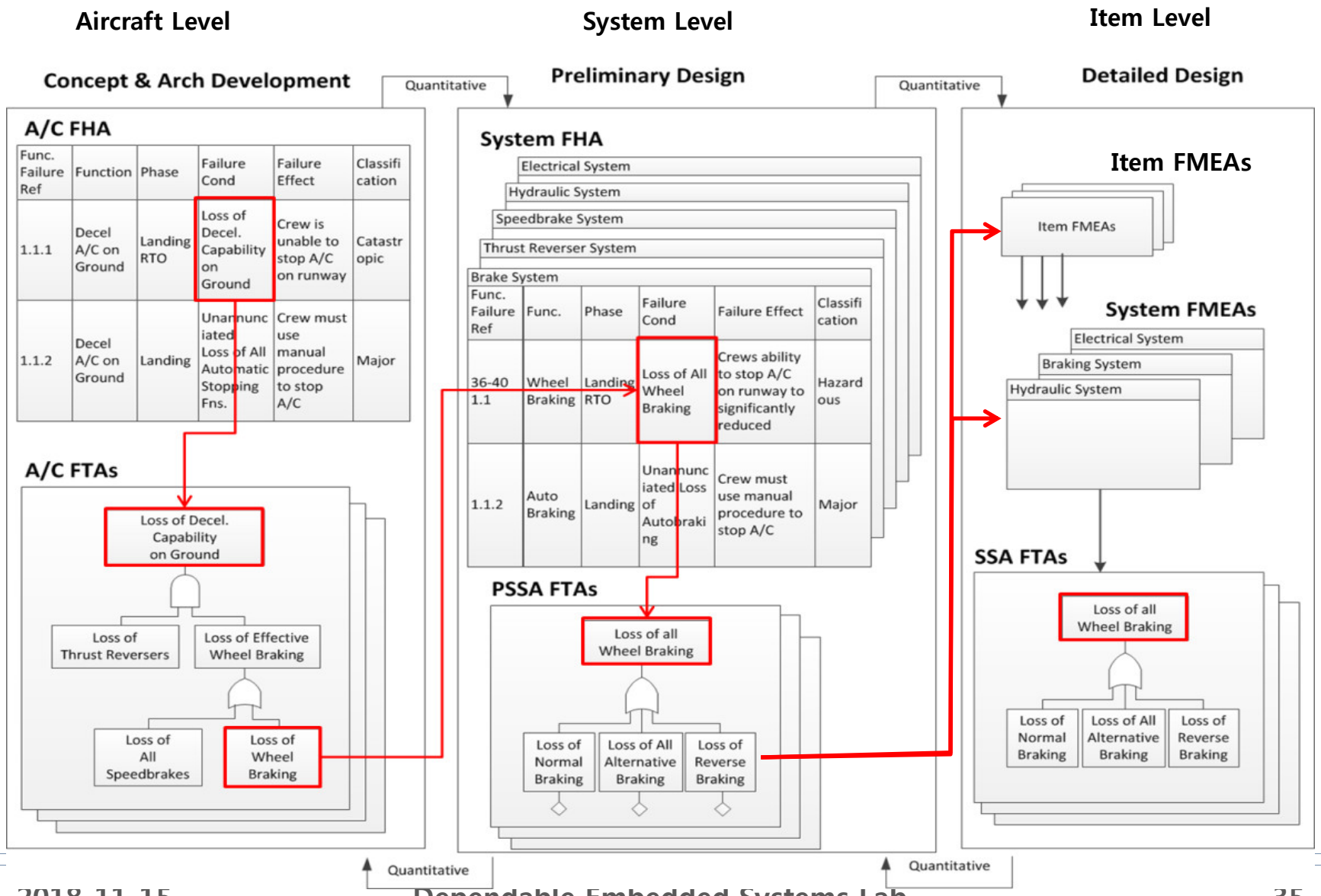


FHA, FMEA, FTA 관계

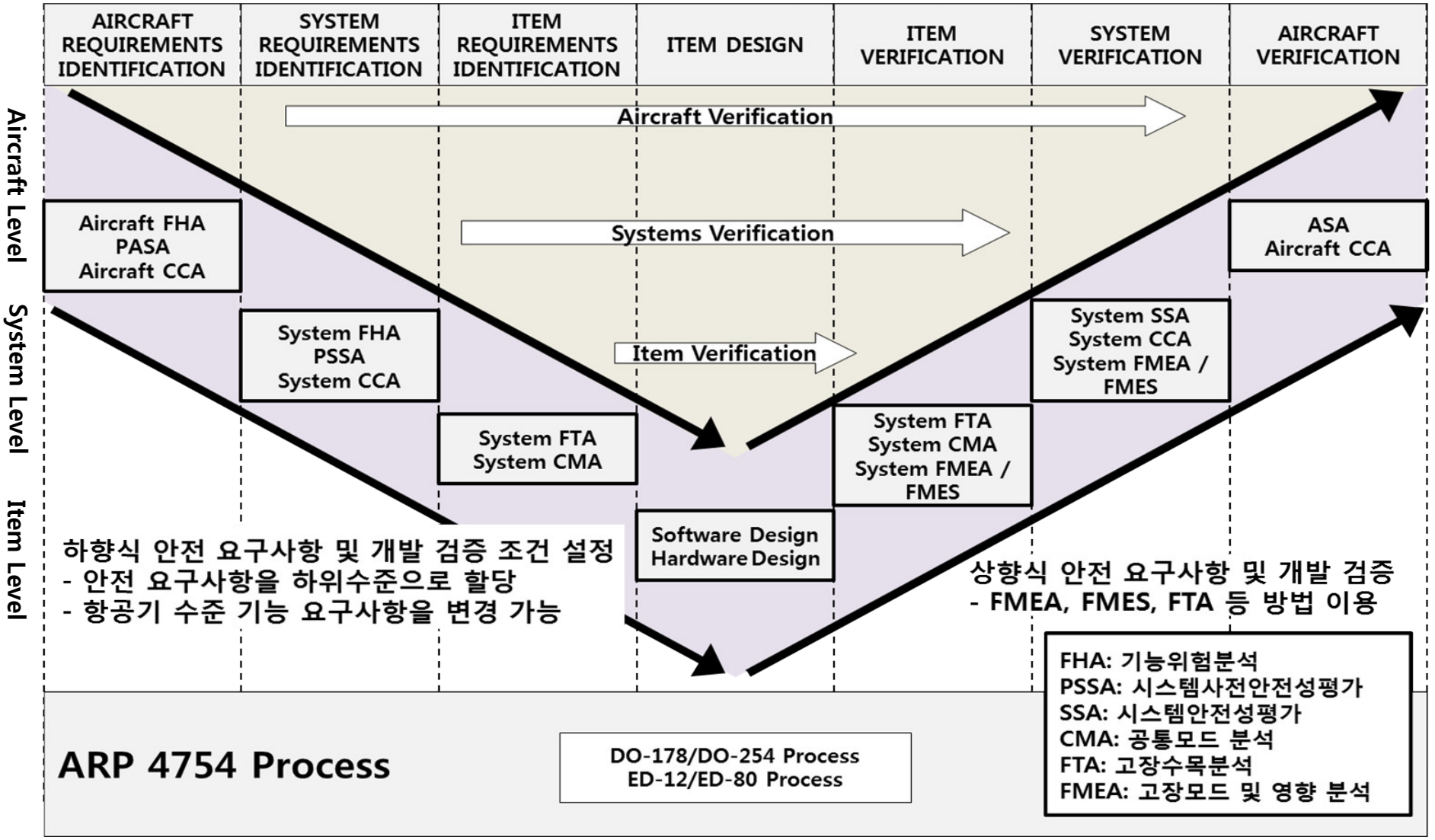


https://www.omnicongroup.com/blog/443-march-2017-fmea-vs-fta

4761 절차 및 기법


Aircraft Level
System Level
Item Level
Concept & Arch Development
Quantitative
Preliminary Design
Quantitative
Detailed Design
A/C FHA
Func. Failure Ref
Function
Phase
Failure Cond
Failure Effect
Classification
1.1.1
Decel A/C on Ground
Landing RTO
Loss of Decel. Capability on Ground
Crew is unable to stop A/C on runway
Catastropic
1.1.2
Decel A/C on Ground
Landing
Unannunciated Loss of All Automatic Stopping Fns.
Crew must use manual procedure to stop A/C
Major
A/C FTAs
Loss of Decel. Capability on Ground
Loss of Thrust Reversers
Loss of Effective Wheel Braking
Loss of All Speedbrakes
Loss of Wheel Braking
System FHA
Electrical System
Hydraulic System
Speedbrake System
Thrust Reverser System
Brake System
Func. Failure Ref
Func.
Phase
Failure Cond
Failure Effect
Classification
36-40 1.1
Wheel Braking
Landing RTO
Loss of All Wheel Braking
Crews ability to stop A/C on runway to significantly reduced
Hazardous
1.1.2
Auto Braking
Landing
Unannunciated Loss of Autobraking
Crew must use manual procedure to stop A/C
Major
PSSA FTAs
Loss of all Wheel Braking
Loss of Normal Braking
Loss of All Alternative Braking
Loss of Reverse Braking
Item FMEAs
Item FMEAs
System FMEAs
Electrical System
Braking System
Hydraulic System
SSA FTAs
Loss of all Wheel Braking
Loss of Normal Braking
Loss of All Alternative Braking
Loss of Reverse Braking
Quantitative
Quantitative

4754 + 4761


AIRCRAFT REQUIREMENTS IDENTIFICATION
SYSTEM REQUIREMENTS IDENTIFICATION
ITEM REQUIREMENTS IDENTIFICATION
ITEM DESIGN
ITEM VERIFICATION
SYSTEM VERIFICATION
AIRCRAFT VERIFICATION
Aircraft Level
System Level
Item Level
Aircraft Verification
Systems Verification
Item Verification
Aircraft FHA
PASA
Aircraft CCA
System FHA
PSSA
System CCA
System FTA
System CMA
Software Design
Hardware Design
System FTA
System CMA
System FMEA / FMES
System SSA
System CCA
System FMEA / FMES
ASA
Aircraft CCA
하향식 안전 요구사항 및 개발 검증 조건 설정
- 안전 요구사항을 하위수준으로 할당
- 항공기 수준 기능 요구사항을 변경 가능
상향식 안전 요구사항 및 개발 검증
- FMEA, FMES, FTA 등 방법 이용
FHA: 기능위험분석
PSSA: 시스템사전안전성평가
SSA: 시스템안전성평가
CMA: 공통모드 분석
FTA: 고장수목분석
FMEA: 고장모드 및 영향 분석
ARP 4754 Process
DO-178/DO-254 Process
ED-12/ED-80 Process

FMEA 장단점

장점: 고장 식별 및 평가

- Single Failure Analysis
- Hardware/Software Interfaces
- Requirements
- Design
- Detailed Design

단점:

- 여러 분야의 인원 필요
- 긴 회의 시간
- 경험 의존
- 문서 기록 의존
- 단일 고장 상황만 체크
- 복합 고장 판단 불가능
- 신 제품 고장 판단 어려움
- 미확인 고장

Outlines

- Are you safe?
- Hazard & Risk in Avionics
- Fault injection
- Model based Automatic Risk analysis System (MARS)

결함 주입Fault Injection overview

- FI?
  - 결함을 타겟 시스템/보드/칩/SW에 주입
  - 정상 상태 → 고장 상태 상태변화 유도
  - 고장 결과 분석
- 목표
  - 고장률
  - 인증 자료
  - 취약점 (Vulnerability) 식별
  - 결함 고장 감내 시스템 성능 평가
- 종류
  - HW, SW, Simulation, Physical, hybrid tools
- 장점
  - Dynamic & complex 시스템/칩/보드/SW 분석
  - Observability, controllability 최상급 결과
  - 시험결과를 통계적으로 분석

Fault injection Types

1. Physical fault injection
   - Electronic/electrical, mechanical, hydraulic targets
2. Software fault injection
   - Software
3. Simulated fault injection
   - RTL/ESL simulation design model
   - Hybrid design model

Physical fault injection

- 정의
  - 실제 하드웨어에 특정 장비를 사용하여 결함을 주입
  - Ex) Pin-level, Protons, neutrons, alpha particles, heavy ions.
- 장점
  - 실제 고장상황과 밀접한 결함주입 시험을 실시할 수 있음.
  - 결함주입 시험속도가 빠르다.
- 단점
  - 실험을 수행하기 위해 최소한 prototype 제작이 필요
  - 초기 설계 단계에서 평가 어려움
  - 결함 관측 제어와 시스템 내부 상태 분석이 어려움
  - 시험 장비 구축, 시험대상의 파손위험 등을 많은 비용이 필요
- Example tools
  - RIFLE, FIST, MESSALINE, FOCUS

Software fault injection

- 정의
  - 소프트웨어 코드 또는 바이너리 파일을 대상으로 주입
  - Compile-time injection(code modification)
  - Runtime injection(JTAG, time trigger)
- 장점
  - 어플리케이션 수준에서의 결함주입 시험이 가능.
  - 운영체제와 같은 kernel 수준의 소프트웨어를 대상으로 결함주입 시험을 수행 할 수 있음.
- 단점
  - 결함주입 루틴의 시스템 간섭.
  - 코드 수정과 컴파일의 반복적인 과정.
- 사례
  - FIAT, FERRARI, XCEPTION, EXFI, GOOFI

Simulated fault injection

- 정의
  - 시뮬레이션 모델을 대상으로 결함을 주입
- 종류
  - 툴 지원: Fault injection system task, Tool commands
  - 모델 수정:Simulation model modification(Saboteur, Mutant)
  - 툴 수정: Simulation kernel modification
- 장점
  - 시스템 설계초기에 결함주입 시험이 가능
  - 시험결과 분석에 따른 설계변경이 용이
  - 결함에 대한 제어와 추적이 용이
- 단점
  - 모델의 복잡도 증가에 따른 결함주입 공간의 폭발적 증가.
  - 실제 시스템에 비해 매우 느린 시뮬레이션 속도
  - 시뮬레이션 수행결과 정보 증가에 따른 분석에 어려움.
- 사례
  - SystemC fault injection, Verilog fault injection, Simulink model fault injection

Fault injection tools classification

Fault Injection Types		Access-ibility	Observ-ability	Intrusi-veness	Repeat-ability	Cost	Types	Tools
HW-Based Fault Injection	Direct Injection	high	low	none	low	high	Pin Level FI	RIFLE3, MESSALINE
							Bus Level FI	Y-CAN Platform
							Power Supply FI	MARS
	Indirect Injection	high	low	none	low	high	Heavy Ion Radiation FI	FIST, Cf-252,
SW-Based Fault Injection	SW during Runtime	low	low	low	high	low	Non Automated SW FI	FIAT, Xception, DOCTOR, EXFI, GOOFI, DEFINE
							Fully Automated SW FI	
Simulated Fault Injection	Tool	high	high	high	high	high	Command	MEFISTO
	Model-modified						Saboteur	REACT
							Mutant	VERIFY
	Simulator-modified	high	high	none	high	low	SystemC model	SystemC fault injection
							Verilog model	Verilog fault injection
							Simulink model	Simulink fault injection

Simulated fault injection

Kernel modified simulated fault injection

1. SystemC-FI fault injection
2. Verilog-FI fault injection

Commercial tools

1. VPI- VFI fault injection

Hybrid fault injection

1. JTAG fault injection
2. HILSFI fault injection

Simulated fault injection summary

	SystemC FI	Verilog FI	Verilog Procedure Interface-VFI
Simulation Level	Electronic System Level (SystemC)	Gate Level, Register-Transfer Level (Verilog)	
Injection Mechanism	Kernel Modification		Verilog Procedure Interface (VPI)
RTL/ESL tools	SystemC (open source)	ICARUS-Verilog (open source)	ModelSim, NCVerilog (commercial)
Fault model	Fault type : Transient, Permanent, Intermittent Fault time : User / Random Fault location : User / Random Fault value : Stuck-at-1/0, Multibit-1/0		

SystemC FI fault injection

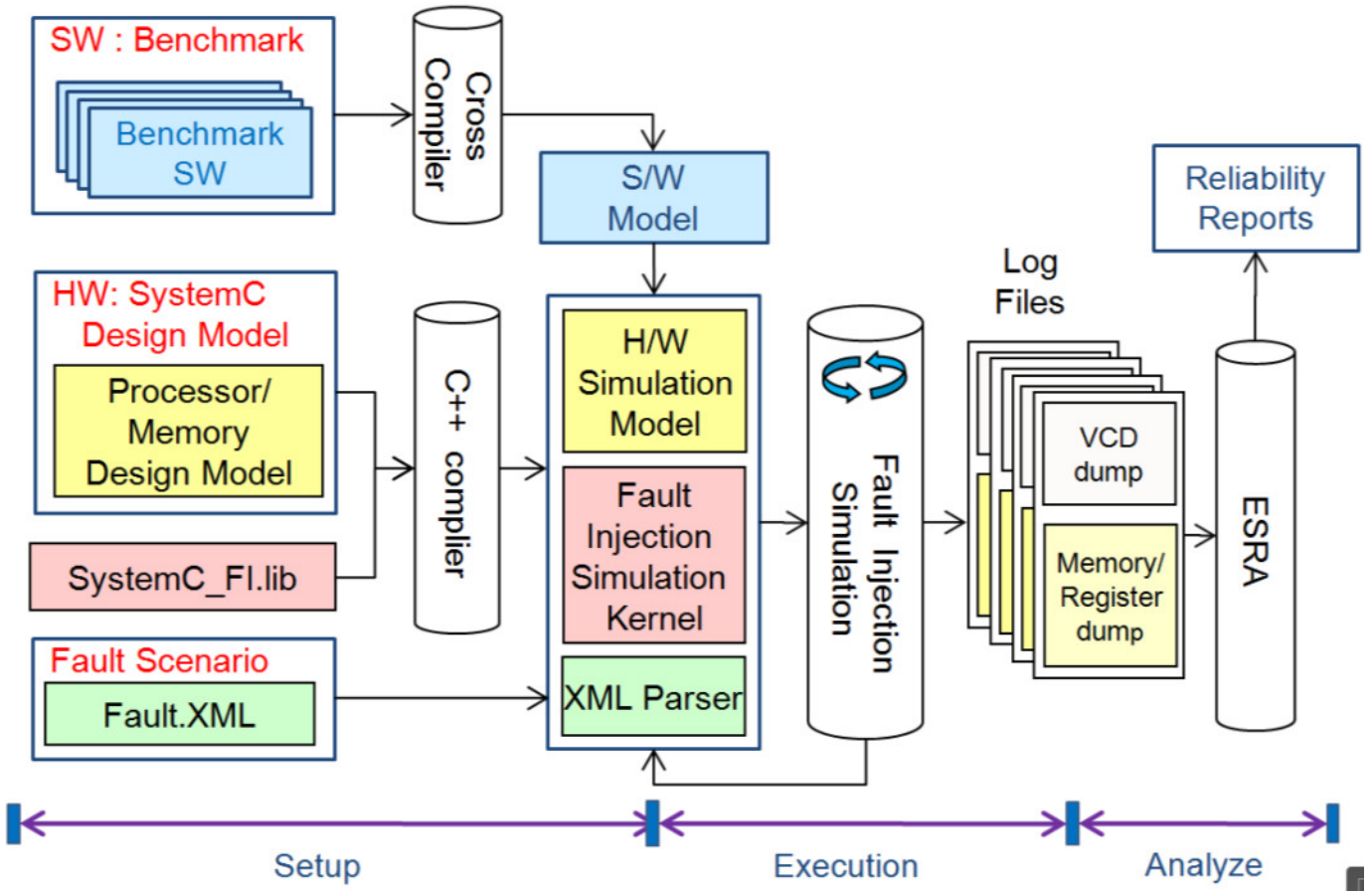
- SystemC FI overview
- SystemC FI procedure
- SystemC FI mechanism
- SystemC FI fault models
- SystemC FI failure results

SystemC FI overview

- SystemC FI
  - **SystemC** simulation model 기반 결함주입 환경
  - Simulation kernel modification 기반 결함주입 방법론
  - Systemc_FI.lib
    - SystemC kernel library + **Fault injection mechanism**
    - 기본적 SystemC 시뮬레이션 수행;
    - 동시에 결함 주입 계획에 따라 결함주입 동작 수행
- SystemC FI 결함모델

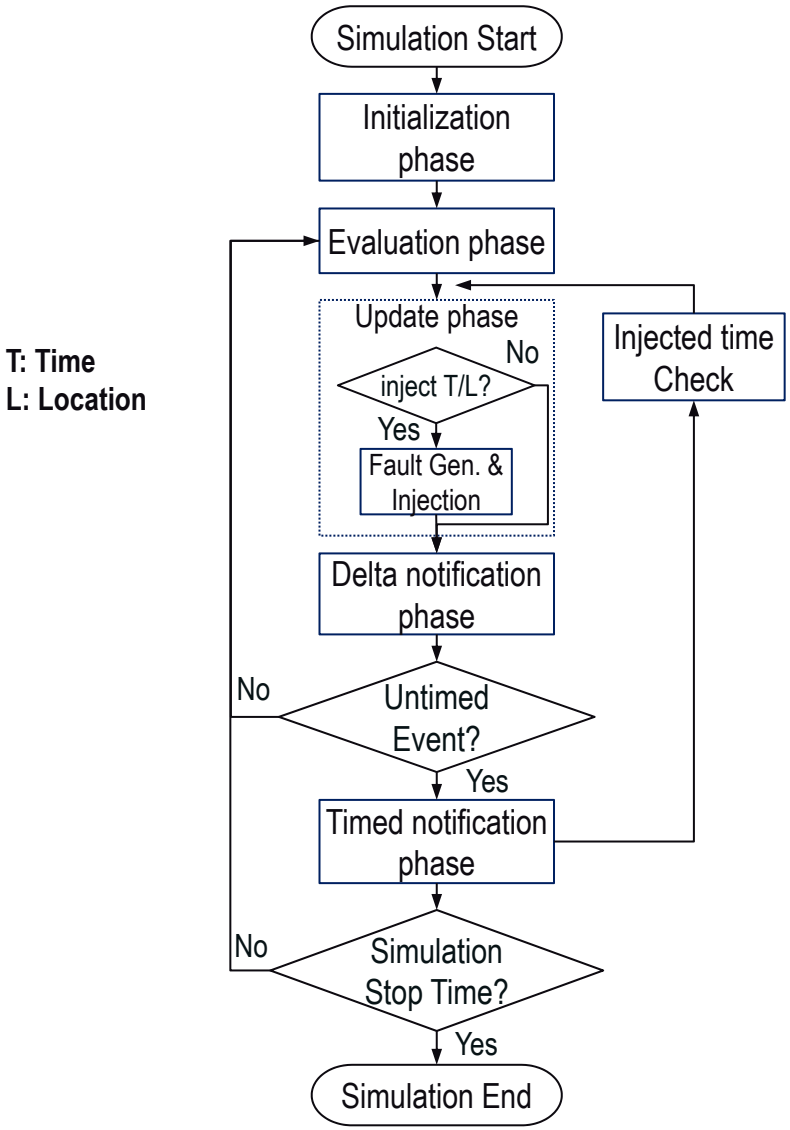
결함 종류	Transient, Permanent, Intermittent
결함 시간	Random / Deterministic
결함 위치	Random / Deterministic (SystemC sc_signal 객체)
결함 값	Stuck-at-1(0), Single-bit/multi-bit

SystemC FI procedure



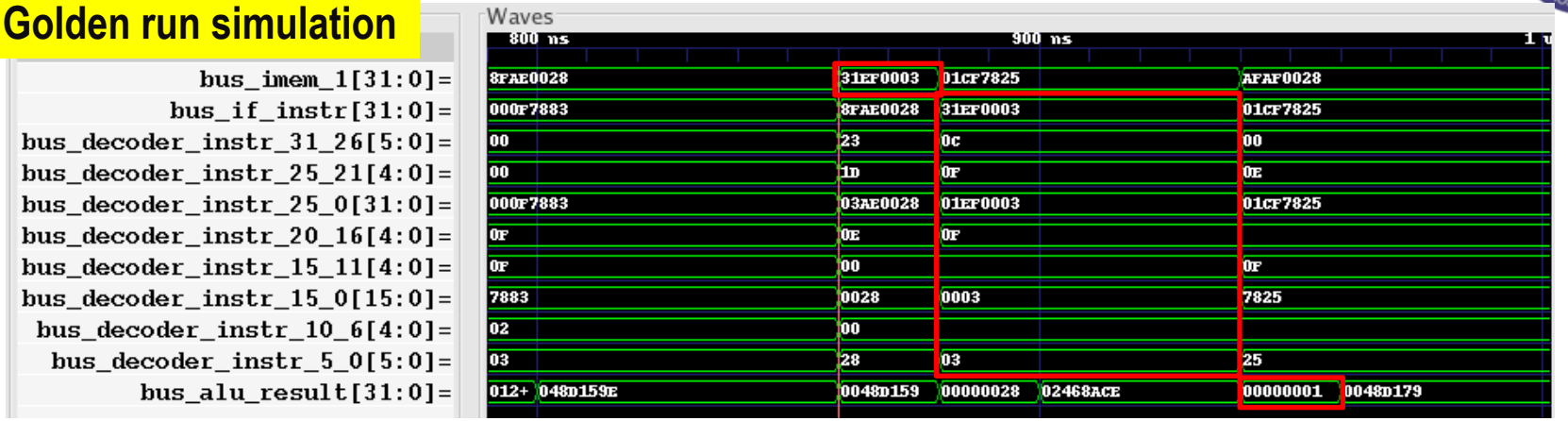
- SystemC open source simulator
  - SystemC_FI.lib → SystemC kernel library + Fault injection mechanism
- 3-stage operation: Setup → Execution(injection) → Analyze

SystemC FI mechanism

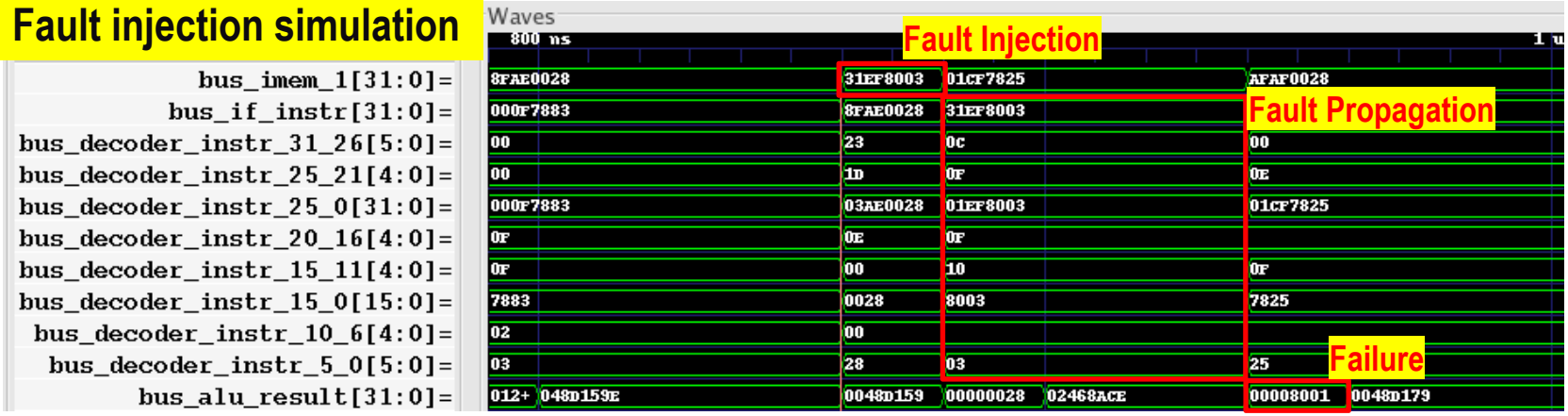


SystemC FI failure results

Golden run simulation

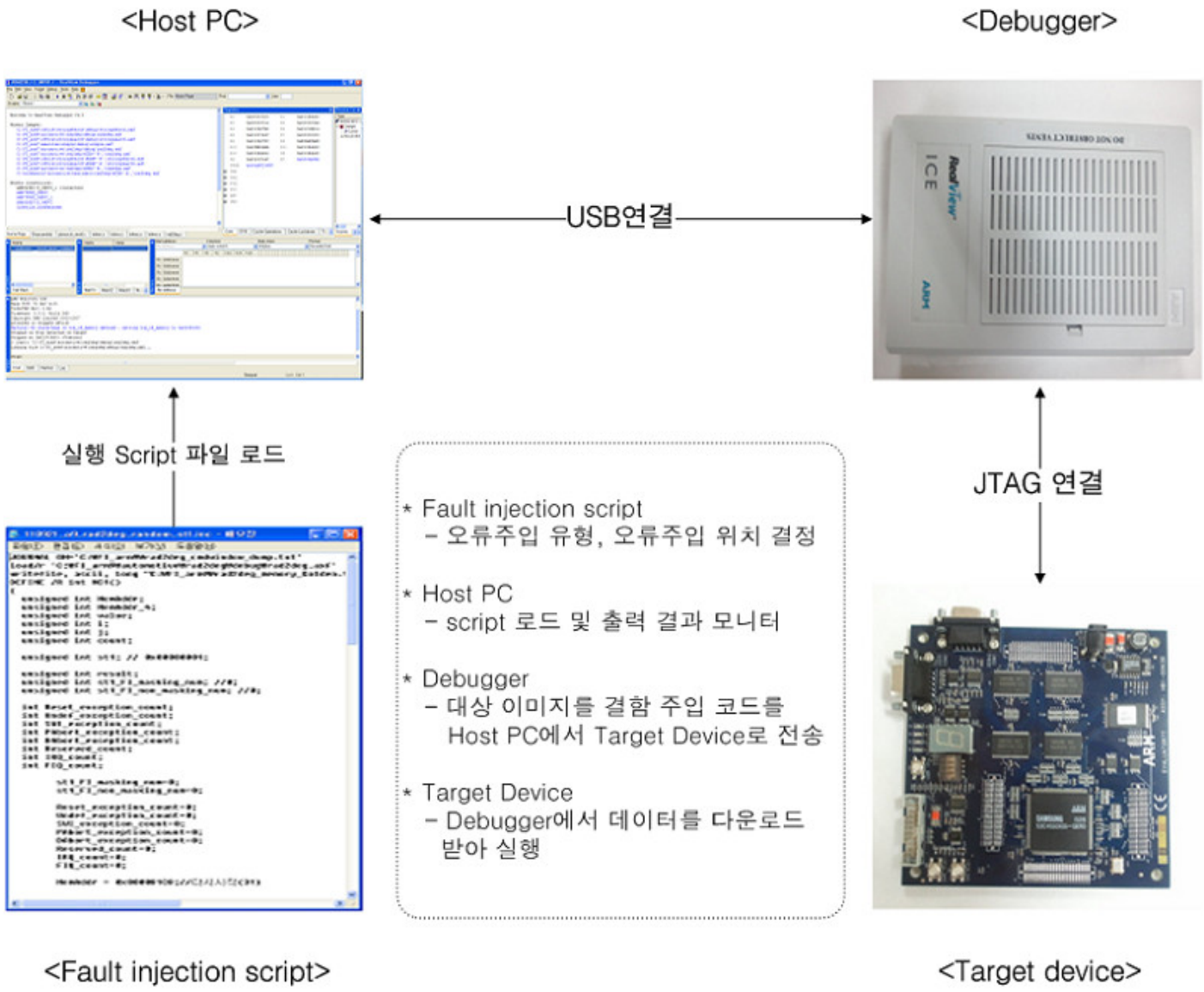


Fault injection simulation



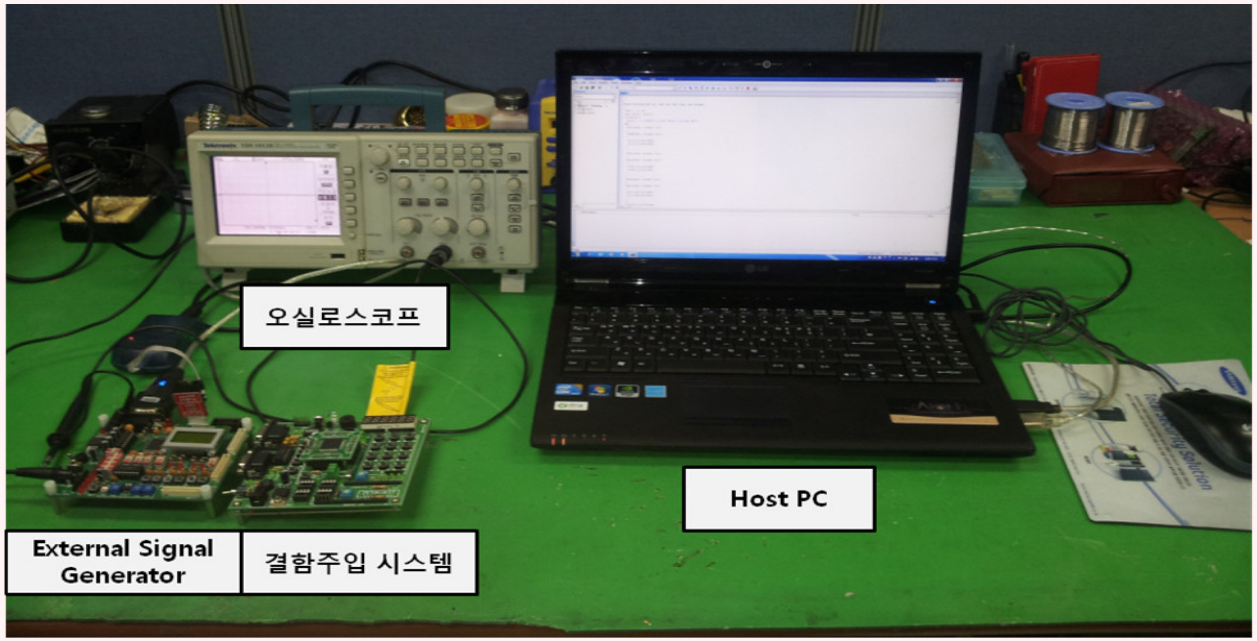
- Bus_imem_1(Instruction memory output signal): 0x31EF0003→0x31EF8003
  - Golden Run : andi $16 $16 #3 --Fault injection Run: andi $16 $16 #8003
- And operation failure
  - 연산결과: 1(normal) → 0x8001(failure)

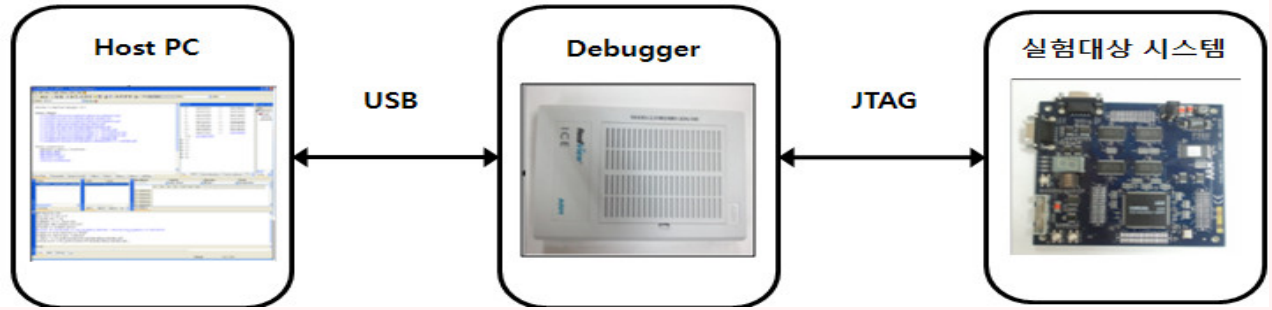
임베디드 타겟 고장분석 : JTAG FI 환경



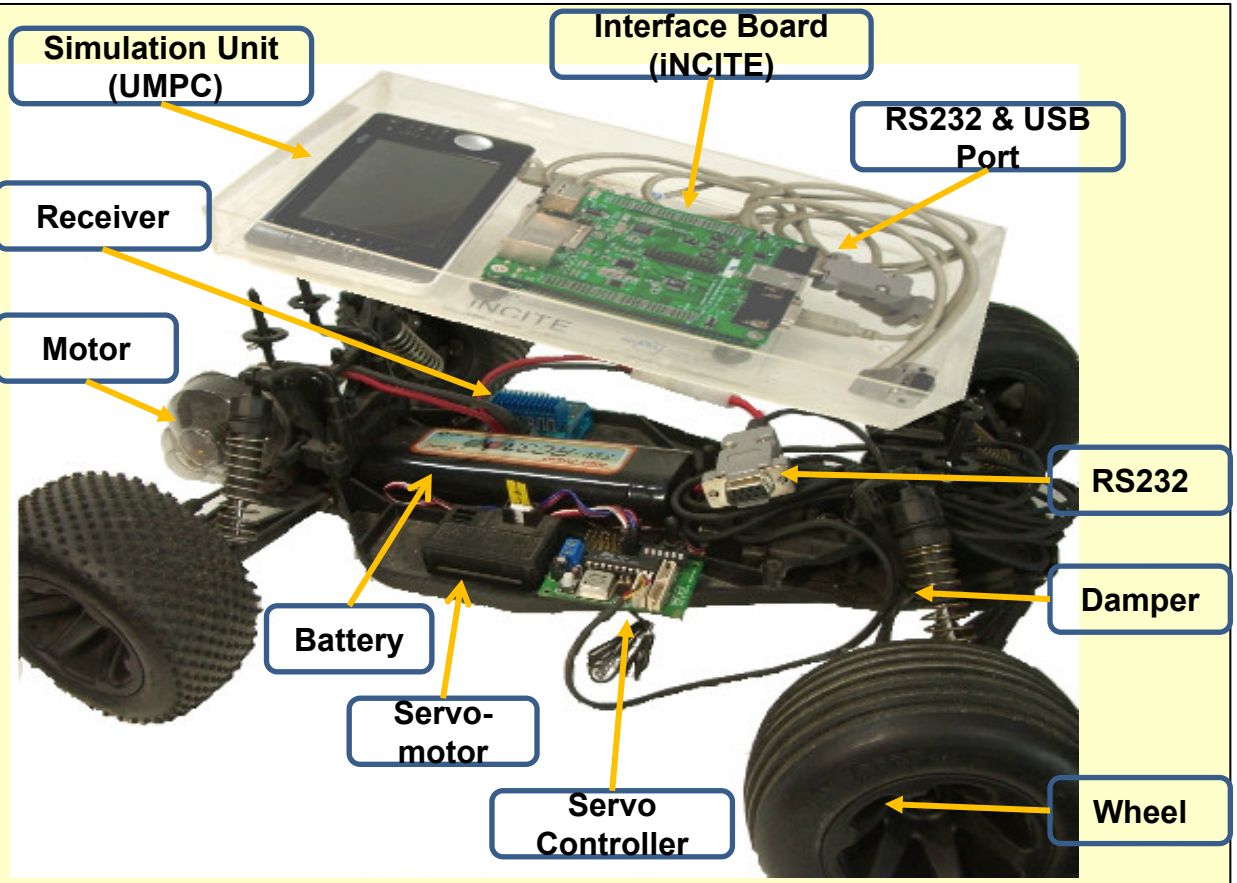
JTAG FI overview

DES Embedded Board 개발



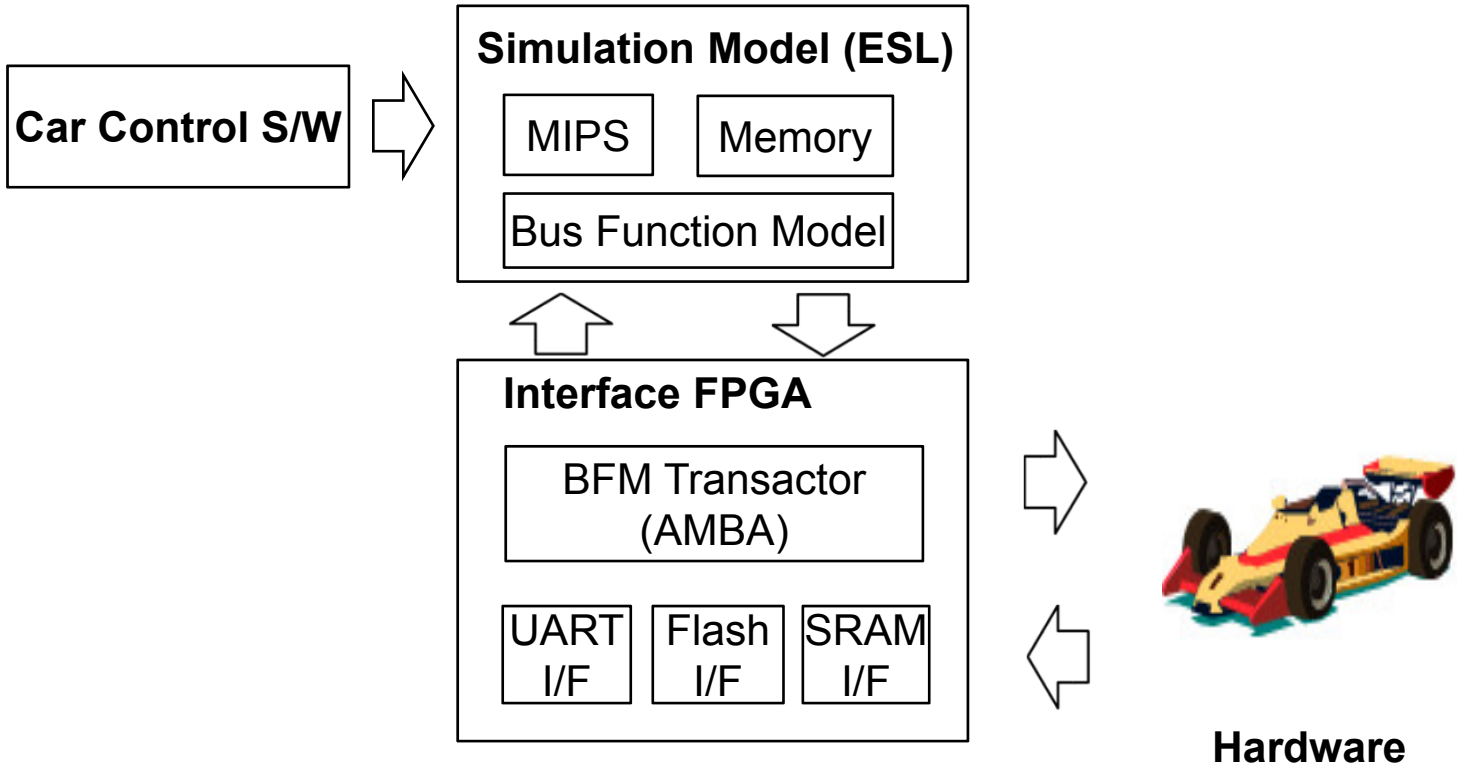


HILS 타겟 고장 분석: HILSFI

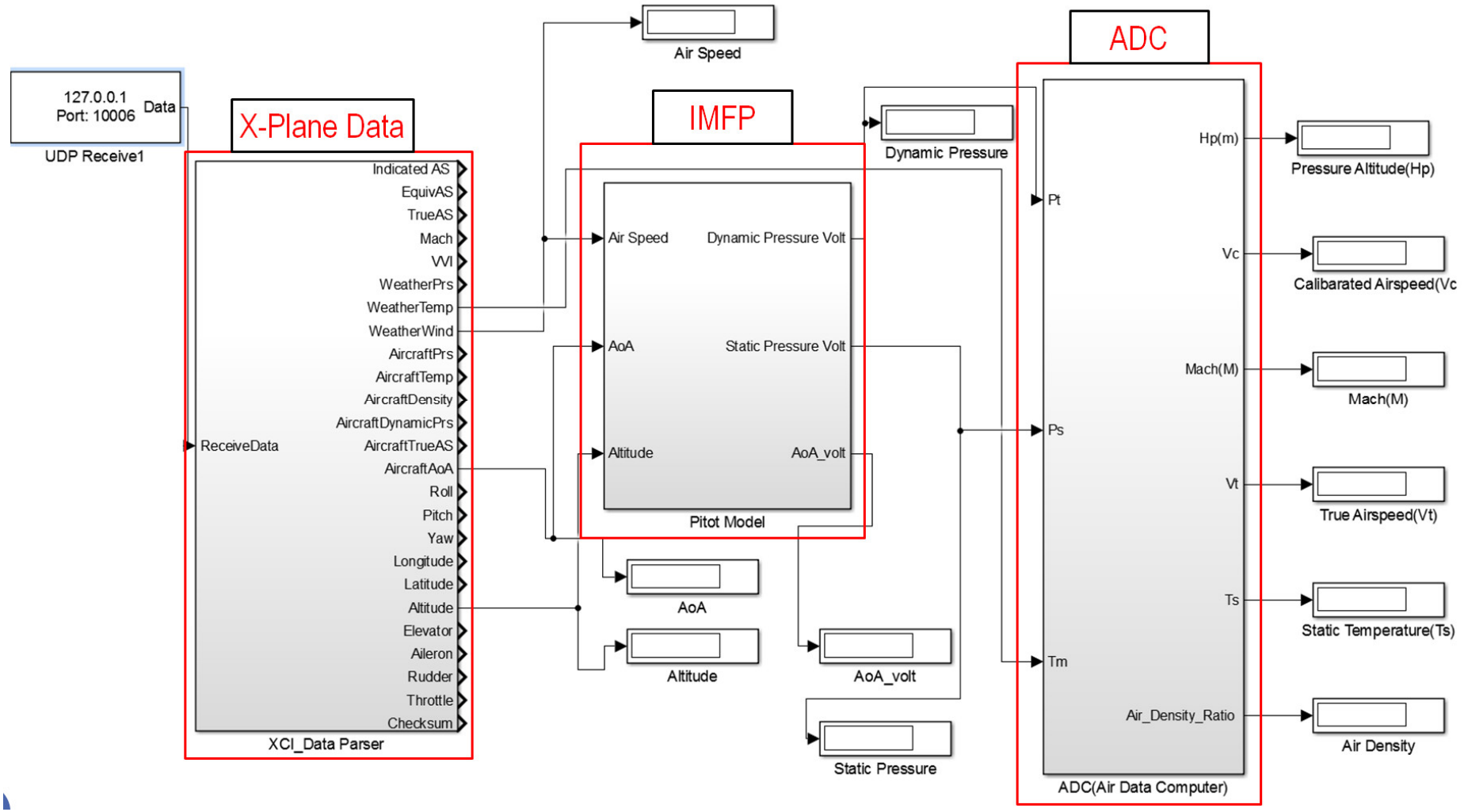


HILS prototype system
= Simulation model + FPGA board + Servo controller + RC Car

HILSFI target block diagram

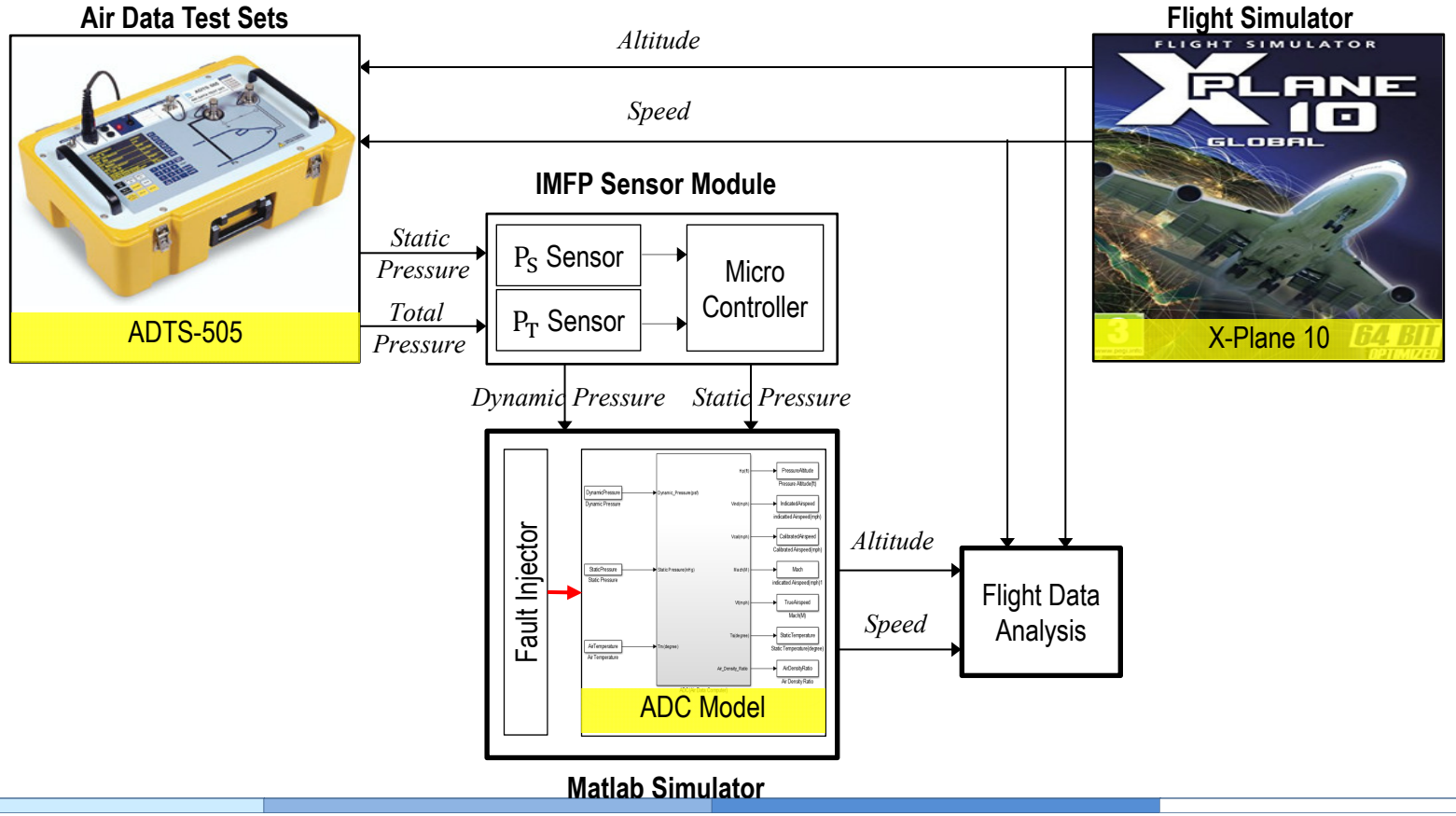


Simulink 모델: 대기자료컴퓨터 + 센서



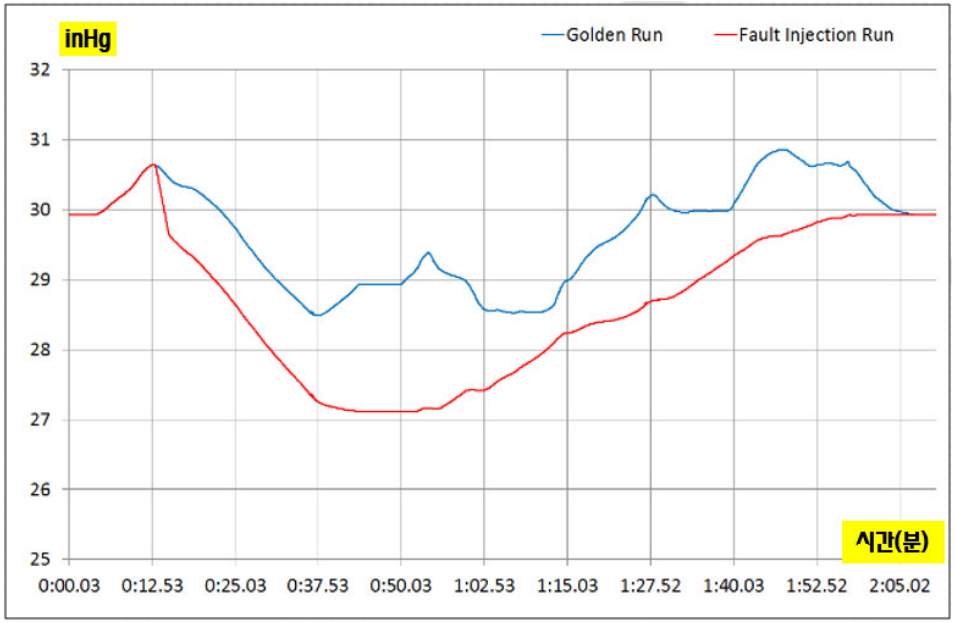
시뮬링크 결함주입 환경

- Hardware in the loop 결함주입 시험 환경
  - Simulink: IMFP, ADC 모델 실행
  - Flight Simulator: 비행 임무 설정 및 관리
  - Air data test sets and sensor : 압력 값 생성 및 측정



시뮬링크 결함주입 시뮬레이션 결과

- 고장 영향 사례
  - 결빙 결함 주입
  - 전압 피토관 막힘
    - 배수관 유입된 공기 흐름 측정 불능
  - 전압센서에서 결함 발생
    - 오 동작 관측



결함주입 응용

1. Safety analysis
   - FMEA, FTA requires fault injection evidence
2. Functional safety evidences
   - ISO26262 requires fault injection evidences
3. Reliability measure
   - Power, area, cost, timing, temperature, …
   - What about lifetime?
4. Model-based safety analysis
   - Simulink fault injection & reliability analysis

Outlines

- Are you safe?
- Hazard & Risk in Avionics
- Fault injection
- Model based Automatic Risk & Safety (MARS)

FMEA/FMECA 연구 동향

- Applicability
  - Anticipate the analysis
  - Automation Info management
  - Guideline
  - Complex systems
  - User interface
  - New criteria
- Cause and effects representation
  - New methods for Failure Modes identification
  - New methods for Failure Effects:
  - Combine multiple Failures Effects
  - New methods for Failure Causes
- Risk analysis
  - Statistical methods
  - Requirements-based criteria
  - Economic criteria
  - Historical data:
  - Qualitative criteria:
- Problem solving
  - Results representation:
  - New methods to be integrated into FMEA
  - Use FMEA for other purposes

FMEA/FMECA Methods & Tools

- **Databases**
  - Physical effects
  - Historical data
  - Costs
  - Others
- **Mathematical, logic and statistical**
  - Fuzzy
  - Bayesian network
  - Petri net
  - Statistical (analysis of mean and variance)
- **Problem solving**
  - QFD
  - TRIZ
  - Methods for maintenance planning
  - Brainstorming
- **Prototyping**
  - Simulation
  - Test
- **Others**
  - Infographics
  - Functional Analysis
  - Ontologies
  - FTA (Fault Tree Analysis)
  - Scenario

C. Spreafico et al. / Computer Science Review 25 (2017) 19–28

FMEA 장단점 Review

장점: 고장 식별 및 평가

- Single Failure Analysis
- Multiple Failure Analysis
- Hardware/Software Interfaces
- Requirements
- Design
- Detailed Design

단점:

- 여러 분야의 인원
- 긴 회의 시간
- 경험 의존
- 문서 기록 의존
- 단일 고장 상황만 체크
- 복합 고장 판단 불가능
- 신 제품 고장 판단 어려움
- 미확인 고장

Future FMEA/FMECA 목표

AS IS

- 여러 분야의 많은 요원
- 긴 회의 시간
- 경험 의존
- 문서 기록 의존
- 단일 고장 상황만 체크
- 복합 고장 판단 불가능
- 신 제품 고장 판단 어려움
- 미확인 고장

TO BE

- 소수의 점검 인력
- 짧은 회의 시간
- 이론적 타당성 추가
- 문서 기록은 참고만
- 복합 고장 체크
- 다중 고장 판단 기능
- 신 제품 고장 판단 가능
- 가능한 모든 고장 확인

New FMEA

- 해결방법
  - FMEA를 자동화
  - 계층 연동 분석: 상위 개념설계~ 하위 부품수준
  - 모델 기반 설계 도입
  - 결함 주입 기술 융합
- **Model based Automatic Risk & Safety (MARS)**
  - 시스템 prototype simulation model 제작
  - Fault injection 기반 FMEA & FTA
    - 각 고장 별 고장률 심각도 검출도 계산 및 기록
  - 안전요구사항 충족 여부 판정
  - 결함/고장 감내 기능 추가 여부 판정
  - 최종 계층?
  - 개발 중

MARS impact

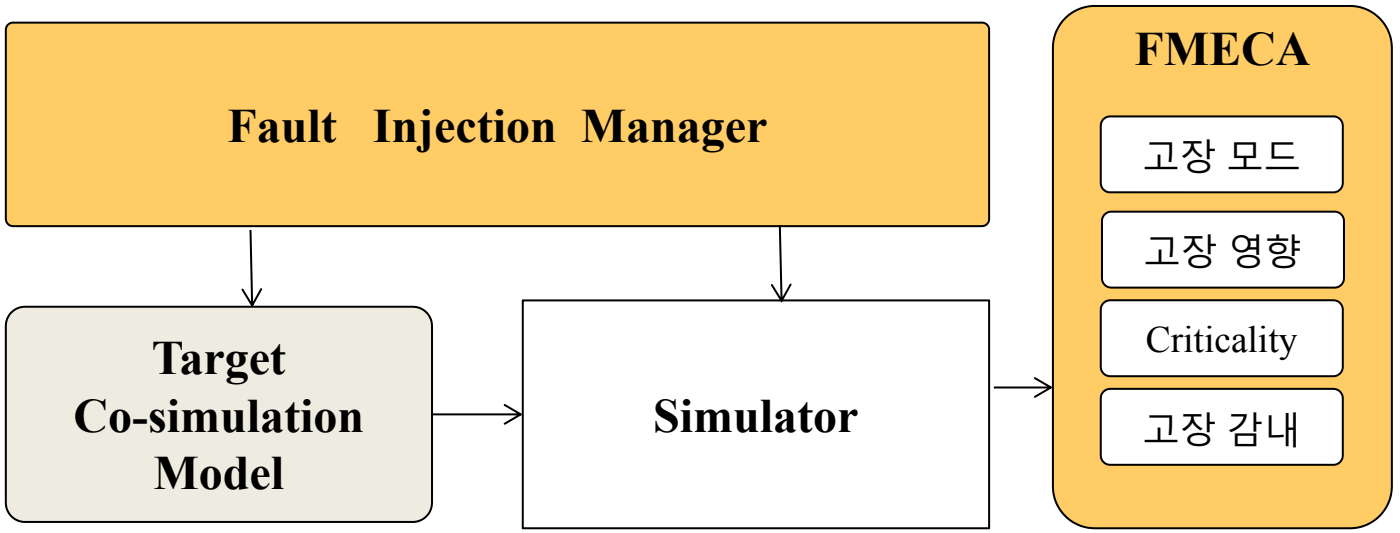
Traditional FMEA

- 방법
  - ∑ engineering meeting
  - Checklist 확인
- Problems:
  - 여러 분야 인원 소집
  - 장시간 회의
  - multiple component failures,
  - latent faults, …

Model based Automatic Risk & Safety (MARS)

- 방법
  - 환경 설정 + 클릭 'run'
  - 테이블 데이터 자동생성
- 장점
  - 인원 소집 없음 – 결과 확인만
  - 단시간 회의 - 결과 확인
  - Single and multiple failure 확인가능
  - Latent fault 확인가능

모델 결함주입기반 FMEA 분석 환경



- Fault Injection Manager → 요구사항 결함 생성 및 주입 시험
- Simulator → 모델 시뮬레이션 수행하고, 결과 생성
- Target Co-simulation Model
  - 알고리즘 수준 (Simulink)
  - 시스템 수준 (SystemC, AADL, SysML)
  - HW (Verilog, VHDL)

FMEA (failure mode & effect analysis)

- FMEA worksheet
  - **Failure Mode:** *Light doesn't turn on*

Possible Effect	**Root Cause**	**S**	**O**	**D**	*RPN*
Car inoperable at night	Battery dead	**10**	**8**	**2**	*160*
	Broken wire	**8**	**3**		*60*
	Headlight out	**6**	**10**		*120*
	Switch corroded	**8**	**2**		*40*
	Switch broken	**8**	**3**		*60*

Conclusions

- Soft Error → fault, failure, hazard, accident
  - Reliability of embedded systems is ‘unknown'
- Avionics uses law
  - ARP4754, ARP4761, DO-178C, DO-254
  - FMEA very expensive & difficult & not efficient
- Fault injection: key technology for Risk analysis
- Model based Automatic Risk & Safety (MARS)
  - Fault injection + Model based safety engineering

고신뢰성 임베디드 시스템 연구실

- 한국항공대 항공전자공학과
- jwna@kau.ac.kr
- 연구분야
  - 결함 주입을 이용한 임베디드 시스템 신뢰성 연구
  - 안전성, 신뢰성 평가 분석, 결함감내 시스템 개발
  - 고신뢰성 시스템 관련 저서, 논문 및 특허 다수
- 교육분야
  - Fault tolerant systems
  - System reliability
  - DO-178C certified SW development
  - DO-254 certified avionics development
- 연구현황
  - New 신뢰성 평가지표
  - 유무인기항공SW개발 가이드
  - 항공전자 장비 (IMFP, RDC)
  - 드론 지상통제SW
  - HW, SW 인증 도구
  - FMEA, FTA 자동화 도구