

시스템 안전 분석

-고장 형태 및 영향 분석

(Failure Mode and Effect Analysis: FMEA)-

-고장 형태, 영향 및 치명도 분석

(Failure Modes, Effects, and Criticality Analysis: FMECA)-

한국교통대학교 안전공학과

박 정 철

FMEA 개요

□ FMEA

- 서브시스템, 구성요소, 기능 등의 잠재적 고장 형태에 따른 효과를 평가하는 기법

□ 목적

- 고장 형태에 따른 영향 평가를 통해 신뢰성, 안전 또는 잠재적 고장 문제로 인한 설계 개선 필요 여부 판단
- 잠재적 고장에 따른 재해 위험 파악
- 각 구성요소 고장 확률에 따른 시스템 신뢰도 파악

□ 역사

- 미군 로켓 개발 MIL-P-1629 (1949년)
- NASA 우주 개발 (1960년대)
- Ford Motors 자동차 가스 탱크 폭발 사고 (1970년대) – 설계 및 생산 개선
- 자동차 제조업계에 확산 (1990년대)

□ 시점

- 상세 설계 단계

□ 대체 기법

- 고장 형태, 영향, 치명도 분석 (Failure Mode, Effects and Criticality Analysis: FMECA)

FMEA 종류

- 기능적(Functional) FMEA
 - 시스템의 기능적 목적에 초점
 - 소프트웨어 평가에 적용 가능
 - 시스템 레벨의 분석
- 구조적(Structural) FMEA
 - 하드웨어 고장 형태의 평가
 - 컴포넌트 레벨의 분석
- 하이브리드(Hybrid) FMEA
 - 기능적 및 구조적 관점의 조합
 - 기능 분석 → 하드웨어 분석
- 제품 FMEA
 - 부품의 고장이나 오류가 제품이나 시스템의 작동에 미치는 영향
- 공정 FMEA
 - 공정의 고장이나 오류가 제품이나 시스템에 미치는 영향

기능적 FMEA와 구조적 FMEA

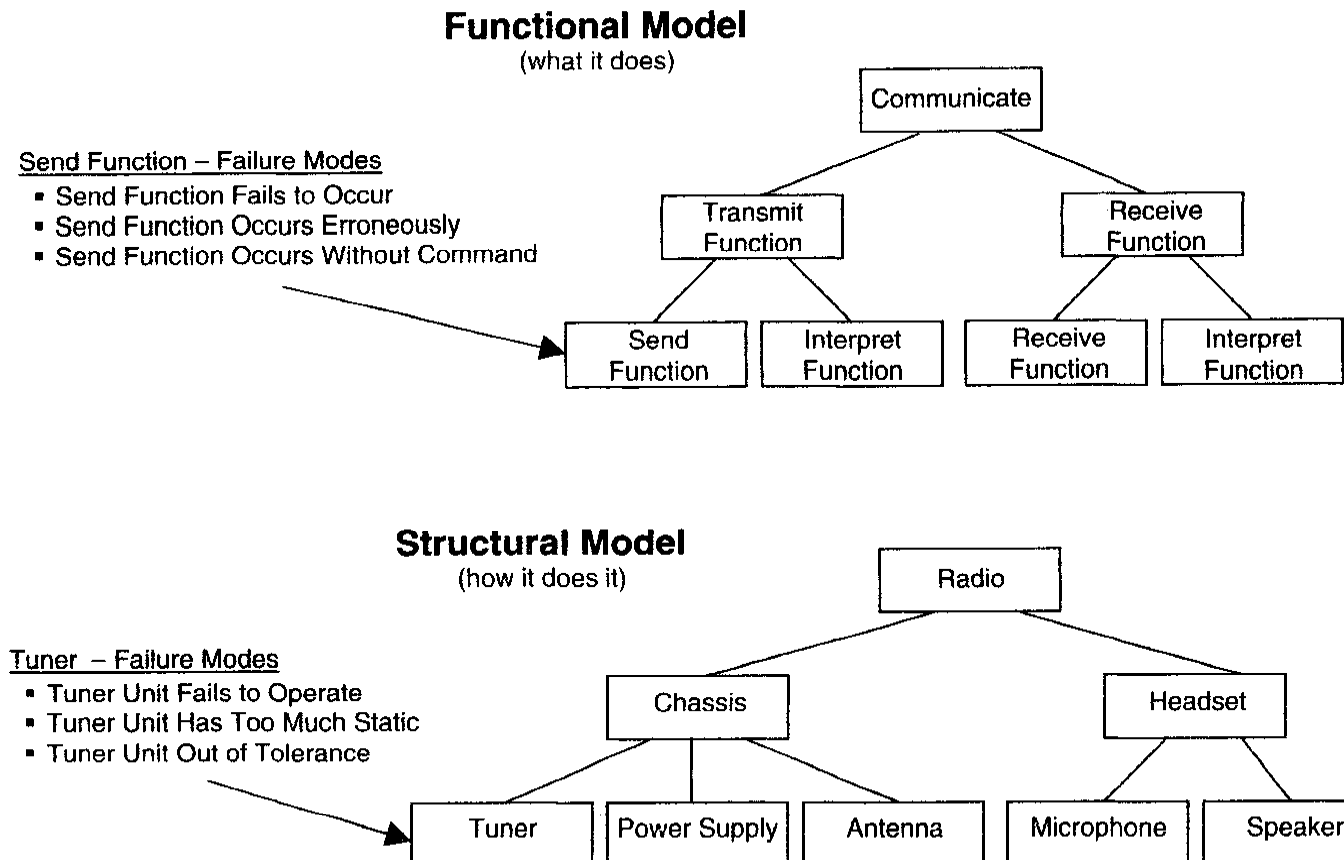


Figure 13.3 Functional and structural models.

고장 형태

□ 하드웨어 고장 형태

- 전체 고장: 기능이 작동하지 않음
- 부분 고장: 기능이 작동은 하되 의도된 대로 작동하지 않음
- 단속성 고장: 기능이 작동되었다가 작동되지 않았다가 함
- 예: 회로 개방, 쇼트, 허용범위 이탈, 누출, 구부러짐, 과열, 깨짐, 부식, ...

□ 소프트웨어 고장 형태

- 소프트웨어의 비정상적인 작동
- 예: 작동 실패, 잘못된 결과 산출, 메시지 표시 안됨, 충돌, ...

신뢰도 예측 모델

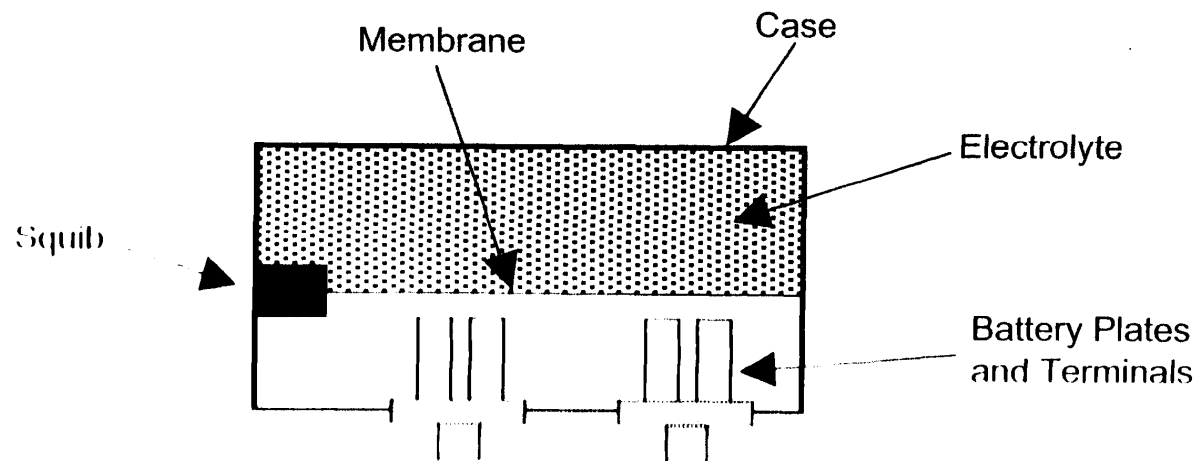
- ❑ MIL-HDBK-217, The Military Handbook for the Reliability Prediction of Electronic Equipment
- ❑ Telcordia (Bellcore), Reliability Prediction Procedure for electronic Equipment, AT&T Bell Labs
- ❑ The Handbook of Reliability Prediction Procedures for Mechanical Equipment (NSWC-98/LE1), Navy
- ❑ HRD5, The Handbook for Reliability Data for Electronic Components Used in Telecommunication Systems
- ❑ PRISM, System Reliability Assessment Methodology developed by the Reliability Analysis Center (RAC)
- ❑ NPRD/EPRD, Nonelectronics Parts Reliability (NPRD) and Electronics Parts Reliability (EPRD) databases by RAC

FMEA 양식

Failure Mode and Effects Analysis										
시스템 : ①			서브시스템: ②				모드/상태: ③			
항목	고장 형태	고장률	원인	즉각적 영향	시스템 영향	검지 방법	현 통제 방법	위험	리스크	조치
④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭

- 항목: 분석 대상 구성요소나 기능
- 고장 형태: 해당 항목의 가능한 모든 고장 형태
 - 과거 데이터, 생산자 데이터, 경험, 테스트 결과로부터 도출
- 고장률
 - 설계 진행에 따라 수정
 - 참고문헌 명시
- 시스템 영향: 시스템 전반에 미치는 궁극적 효과
- 검지 방법: 발생 이후, 심각한 문제를 일으키기 이전에 특정 고장 상태를 감지하는 방법 (육안, 계기, 센서, 안전장치 작동 등)
- 현 통제 방법: 발생 방지 또는 발생 후 안전 확보를 위해 취하고 있는 방법
- 위험: 해당 고장 상태로 인해 발생할 수 있는 구체적 위험
- 리스크: 재해 심각도와 확률로 나타낸 재해 리스크

하드웨어 FMEA 예 - 미사일 배터리 시스템



하드웨어 FMEA 예 – 미사일 배터리 시스템

Failure Mode and Effects Analysis										
System: Missile			Subsystem: Missile Battery			Mode/Phase: Operation				
Component	Failure Mode	Failure Rate	Causal Factors	Immediate Effect	System Effect	Method of Detection	Current Controls	Hazard	Risk	Recommended Action
Case	Cracks	3.5×10^{-5} Manuf. data	Manufacturing defect	Electrolyte leakage	No power output from battery	Inspection	QA	Fire source	2D	Add system sensor
	Pinholes	1.1×10^{-9} Manuf. data	Material defect	Electrolyte leakage	No power output from battery	Inspection	QA	Fire source	2E	Add system sensor
	Leaks out of case	4.1×10^{-6} Manuf. data	Case defect; pinholes	Electrolyte leakage	No power output from battery	Inspection	QA	Fire source	2D	Add system sensor
	Wrong electrolyte used	1.0×10^{-5} Manuf. data	Human error	Does not react with battery plates	No power output from battery	Inspection	QA	Unsafe battery reaction	2D	
Battery plates and terminals	Cracks	2.2×10^{-6} Manuf. data	Material defect	Inadequate battery reaction	Insufficient power output from battery	None	None	None	4D	
	Breaks	1.0×10^{-9} Manuf. data	Material defect	Inadequate battery reaction	No power output from battery	None	None	None	4E	
Analyst:				Date:			Page: 1/2			

기능 FMEA 예 - 비행기 랜딩 기어 시스템

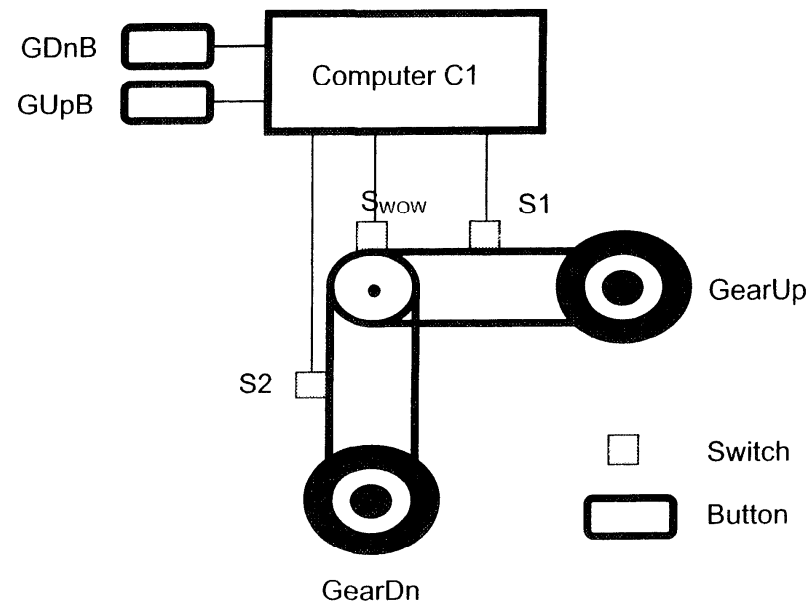


Figure 13.10 FMEA example 2—aircraft landing gear system.

기능 FMEA 예 – 비행기 랜딩 기어 시스템

Failure Mode and Effects Analysis										
System: Aircraft			Subsystem: Landing Gear				Mode/Phase: Flight			
Function	Failure Mode	Failure Rate	Causal Factors	Immediate Effect	System Effect	Method of Detection	Current Controls	Hazard	Risk	Recommended Action
Gear up	Fails to issue	N/A	Computer; software; wiring	Landing gear	Aircraft flight with gear down	Sensor		Damage from drag	4C	
	Issues prematurely	N/A	Computer; software	If down, landing gear raises prematurely	Gear raises during taxi or takeoff	Sensor		Aircraft damage during taxi	2C	
Gear down	Fails to issue	N/A	Computer; software; wiring	Unable to lower landing gear	Aircraft must land with landing gear up	Sensor		Damage or injury during landing	2C	
	Issues prematurely	N/A	Computer; software	If up, landing gear lowers prematurely	Aircraft flight with gear down	Sensor		Damage from drag	2C	
Gear self-test (BIT = built-in-test)	Fails to occur	N/A	Computer; software; electronic faults	Landing gear fault not detected	Unable to raise or lower gear when desired, no warning	None		Possible unsafe state	4C	
	Occurs erroneously	N/A	Computer; software; electronic faults	Landing gear fault self-test data incorrect	No warning or incorrect warning regarding landing gear status	None		Possible unsafe state	4C	
Analyst:				Date:			Page: 1/2			

FMECA

- 특징
 - 기본적으로 FMEA와 동일
 - FMEA 보다 실패 확률 강조
- Failure effect probability (β): 특정 형태의 고장이 일어났다고 가정했을 때, 그 효과가 명시된 치명도 분류에 해당하는 결과를 가져올 확률
- 고장 형태 비율 (α): 명시된 형태의 고장이 발생하는 비율
- Part failure rate (λ_n): 개별 부품, 파트, 컴포넌트의 고장 확률
- Operating time (t): 아이템의 작업 시간 또는 운용 사이클 횟수
- 고장 형태 치명도 $C_m = \beta\alpha\lambda_pt$