

시스템 안전 분석

-미 국방성 시스템 안전 프로그램 (MIL-STD-882)-

한국교통대학교 안전공학과
박 정 철

리스크

- “해를 입는 데 대한 두려움은 해를 입을 위협의 정도뿐만 아니라 사건의 확률에도 비례한다” (Port Royal <La Logique>, 1662)
 - “ 하는 사람들만이 내재된 확률에 아랑곳없이 사안의 중대성에 근거해 선택을 내린다” (Port Royal <La Logique>, 1662)
 - “오직 한 사람들만이 사안의 중대성에 아랑곳없이 확률만으로 결정을 내린다” (Daniel Bernoulli, 1738)
- “신은 존재하거나 존재하지 않는다. 어느쪽으로 마음이 기우는가? 이성만 답할수 없다” (Pascal <Pensées>, 1670)

미국의 시스템 안전 접근방법

- 미국의 시스템 안전 접근방법
 - 미 국방성 (Dept. of Defense: DOD): MIL-STD-882
 - 미 항공우주국 (NASA): NHB 1700.1

MIL-STD-882의 역사

- MIL-STD-882 (1969년 7월) 최초 공표
 - 관리적 측면 강조, 산업체 참여
- MIL-STD-882A(1979년 8월)
 - 위험 확률 및 리스크 수용
- MIL-STD-882B(1984년 3월)
 - 시스템 안전 작업 기술
- MIL-STD-882C(1993년 1월)
 - 하드웨어/소프트웨어 작업 통합
- MIL-STD-882D (2000년 2월)
 - “시스템 안전의 표준 사례 (Standard Practice For System Safety)”
 - 시스템 안전 작업에 대한 기술 제외
- MIL-STD-882E (2012년 5월)
 - 시스템 안전 작업에 대한 기술 재추가

MIL-STD-882E 목차

- Paragraph 1 Scope (목적)
- Paragraph 2 Applicable documents (활용 문서)
- Paragraph 3 Definitions (정의)
- Paragraph 4 General requirements (일반적 요구사항)
- Paragraph 5 Detailed requirements (상세 요구사항)
- Paragraph 6 Notes (참고)

- Task Section 100 Management (관리)
- Task Section 200 Analysis (분석)
- Task Section 300 Evaluation (평가)
- Task Section 400 Verification (확인)

- Appendix A Guidance for the system safety efforts (시스템 안전 노력에 대한 지침)
- Appendix B Software system safety engineering and analysis (소프트웨어 시스템 안전 공학 및 분석)

Task Section (MIL-STD-882E)

□ Task Section 100 Management (관리)

- 101 Hazard identification and mitigation effort using the system safety methodology (시스템 안전 방법론을 이용한 위험 확인 및 감소 노력)
- 102 System safety program plan (시스템 안전 프로그램 계획)
- 103 Hazard management plan (위험 관리 계획)
- 104 Support of government reviews/audits (정부 검토/감사의 지원)
- 105 Integrated product team/working group support (통합된 생산 팀/작업그룹 지원)
- 106 Hazard tracking system (위험 추적 시스템)
- 107 System safety progress report (시스템 안전 진전사항 보고서)
- 108 Hazardous materials management plan (위험 물질 관리 계획)

□ Task Section 200 Analysis (분석)

- 201 Preliminary Hazard List (사전 위험 리스트)
- 202 Preliminary Hazard Analysis (사전 위험 분석)
- 203 Safety Requirements/Criteria Analysis (시스템 요구사항/기준 분석)
- 204 Subsystem Hazard Analysis (서브시스템 위험 분석)
- 205 System Hazard Analysis (시스템 위험 분석)
- 206 Operating and Support Hazard Analysis (작업 및 지원 위험 분석)
- 207 Health Hazard Assessment (보건 위험 평가)
- 208 Functional Hazard Analysis (기능 위험 분석)
- 209 System-of-Systems Hazard Analysis (시스템의 시스템 분석)
- 210 Environmental Hazard Analysis (환경 위험 분석)

Task Section (MIL-STD-882E)

- Task Section 300 Evaluation (평가)
 - 301 Safety assessment report (안전평가보고서)
 - 302 Hazard management assessment report (위험관리평가보고서)
 - 303 Test and evaluation participation (테스트 및 평가 참여)
 - 304 Review of engineering change proposals, change notices, deficiency reports, mishaps, and requests for deviation/waiver (공학 변경 제안서, 변경 공지, 결함 보고, 사고, 변경/기권 요청의 검토)

- Task Section 400 Verification (확인)
 - 401 Safety verification (안전확인)
 - 402 Explosive hazard classification data (폭발 위험 분류 데이터)
 - 403 Explosive ordnance disposal data (폭발 병기 처분 데이터)

재해 심각도 분류 (MIL-STD-882E)

분 류	범 주	환경, 안전, 보건 결과 기준
파국 (catastrophic)	I	사망, 영구 전신 장애, 1,000만 달러를 상회하는 손실, 또는 법이나 규정을 위반하는 복구 불가능한 환경 파괴
중대재해 (critical)	II	최소 3인 이상의 영구 부분 장애, 부상, 또는 직업병으로 인한 입원, 100만 달러 초과 1,000만 달러 이하의 손실, 또는 법이나 규정을 위반하는 복구 가능한 환경 파괴
경미재해 (marginal)	III	1일 이상의 휴업이 필요한 부상이나 직업병. 10만 달러 초과 100만 달러 이하의 손실, 또는 법이나 규정을 위반하지 않는, 복구 활동 수행으로 완화 가능한 환경 파괴
무시재해 (negligible)	IV	1일 이상의 휴업이 필요하지 않은 부상이나 질병. 10만 달러 이하의 손실, 또는 법이나 규정을 위반하지 않는 최소한의 환경 파괴

재해 확률 수준 (MIL-STD-882E)

분 류	수 준	발 생 상 황	
		개 별 항 목	전 체 항 목(시 스템)
자주 발생 (Frequent)	A	한 항목의 수명 중 발생확률 10^{-1} 이 상의 확률로 자주 일어남,	계속적 경험
보통 발생 (Probable)	B	한 항목의 수명 중 발생확률 10^{-2} 이 상 10^{-1} 미만의 확률로 수 회 일어남,	자주 일어남
가끔 발생 (Occasional)	C	한 항목의 수명 중 발생확률 10^{-3} 이 상 10^{-2} 미만의 확률로 가끔 일어남,	수회 일어남
거의 발생하지 않음 (Remote)	D	한 항목의 수명 중 발생확률 10^{-6} 이 상 10^{-3} 미만의 확률로 일어남, 일어 날 것 같지 않지만 일어날 가능성이 있음.	일어날 것 같지는 않으나 일어날 수 있어 보임
극히 발생하지 않음 (Improbable)	E	한 항목의 수명 중 발생확률 10^{-6} 미 만의 확률로 일어남, 거의 일어날 것 같지 않음.	일어나지 않을 것으로 보이지만 가능함
제거됨 (Eliminated)	F	발생 불가능. 잠재 위험이 확인되고 이후에 제거되었을 때 사용됨.	발생 불가능. 잠재 위험이 확인되고 이후에 제거되었을 때 사용됨.

재해 리스크 매트릭스 (MIL-STD-882C)

HAZARD CATEGORY FREQUENCY	(1) CATASTROPHIC	(2) CRITICAL	(3) MARGINAL	(4) NEGLIGIBLE
(A) FREQUENT ($X > 10^{-1}$)*	1A	2A	3A	4A
(B) PROBABLE ($10^{-1} > X > 10^{-2}$)*	1B	2B	3B	4B
(C) OCCASIONAL ($10^{-2} > X > 10^{-3}$)*	1C	2C	3C	4C
(D) REMOTE ($10^{-3} > X > 10^{-6}$)*	1D	2D	3D	4D
(E) IMPROBABLE ($10^{-6} > X$)*	1E	2E	3E	4E

* Example of quantitative criteria

재해 리스크 매트릭스 (MIL-STD-882E)

TABLE III. Risk assessment matrix

RISK ASSESSMENT MATRIX				
SEVERITY PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			