기술시스템의 리스크분석

권영일(청주대학교), 김종걸(성균관 대학교), 이낙영(충남대학교),
홍연웅(동양대학교), 전영록(경남대학교), 나명환(조선대학교)

요약

국제규격인 IEC 300 신뢰성 경영규격의 3-9절을 중심으로 기술적 시스템(technological systems)의 리스크 분석(risk analysis)에 대해 소개한다. 리스크 분석에 사용되는 용어 및 정의, 리스크 분석 개념과 절차, 제품 수명주기동안 적용되는 리스크 분석과 리스크 경영활동, 그리고 리스크 분석에 사용되는 기법들에 대해 살펴본다.

1. 서론

■ 리스크 경영의 제반 요소들 (그림 1 참조)
- 리스크 규명과 분석
- 리스크 허용수준(tolerability) 평가
- 잠재적 리스크의 감소 방법들 규명
- 적합한 관리/감소 대책의 선택, 실행 및 감시

■ 리스크 분석이란?
- 주어진 활동, 설비, 시스템으로부터 발생하는 불행한 결과(adverse consequences)의 발생확 률 (likelihood)과 크기(extent)를 규명하는 체계 화된 절차이다.
- 불행한 결과란 사람, 재산, 그리고 환경에 대한 물리적 손상(physical harm)을 뜻한다.

■ 리스크 분석에서 다루는 세 가지 기본질문
- 무엇이 잘못될 수 있는가? : 위험요인(hazard) 규명
- 발생 가능성은? : 발생빈도 분석
- 결과는 무엇인가? : 결과분석

2. 리스크 분석 개념

2.1 리스크 분석의 목적과 기본 개념

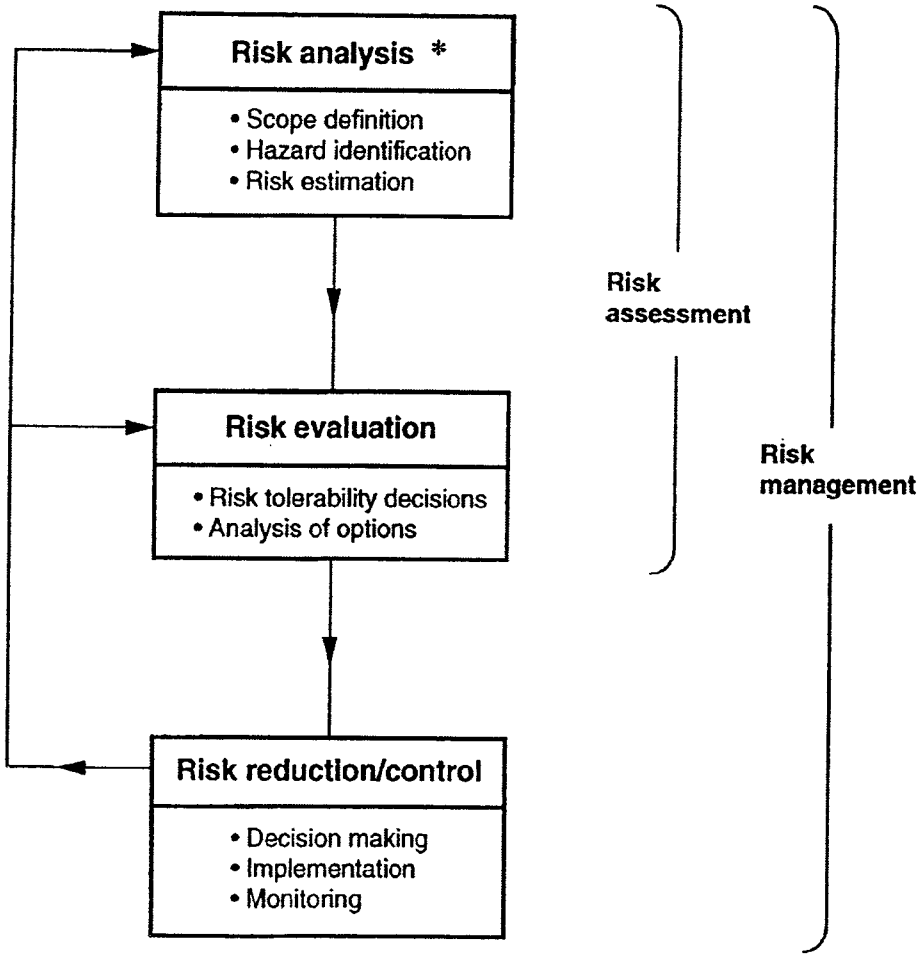
■ 리스크 경영의 목적

인명손실, 질병, 상해, 재산 손실, 환경적 영향을 관리하고, 예방하고, 감소시키기 위한 것이다.

■ 리스크 분석의 용도

■ 리스크 분석의 주요 혜택

■ 리스크 분석에는 다음과 같은 전문분야의 인 원들이 참여한다.



2.2 리스크 경영과 리스크 분류

■ 위험요인에 대한 네 가지 일반적 분류

■ 결과의 성격에 따른 리스크의 분류

■ 리스크 분석의 전반적인 목적은 리스크와 관련된 의사결정을 위해 합리적인 근거를 제공하는 것이다. 이러한 의사결정은 리스크 경영의 한 부분으로서 리스크 분석 결과와 리스크 허용기준의 비교를 통해 이루어진다.

2.3 수명주기동안의 리스크 분석 적용

■ 개념, 정의/설계 및 개발단계

■ 제조, 설치, 운용 및 정비단계

■ 폐기단계

3. 리스크 분석절차

3.1 개요

리스크 분석의 효율성과 객관성을 위해 규정된 절차(그림 2 참조)를 따라야 한다.

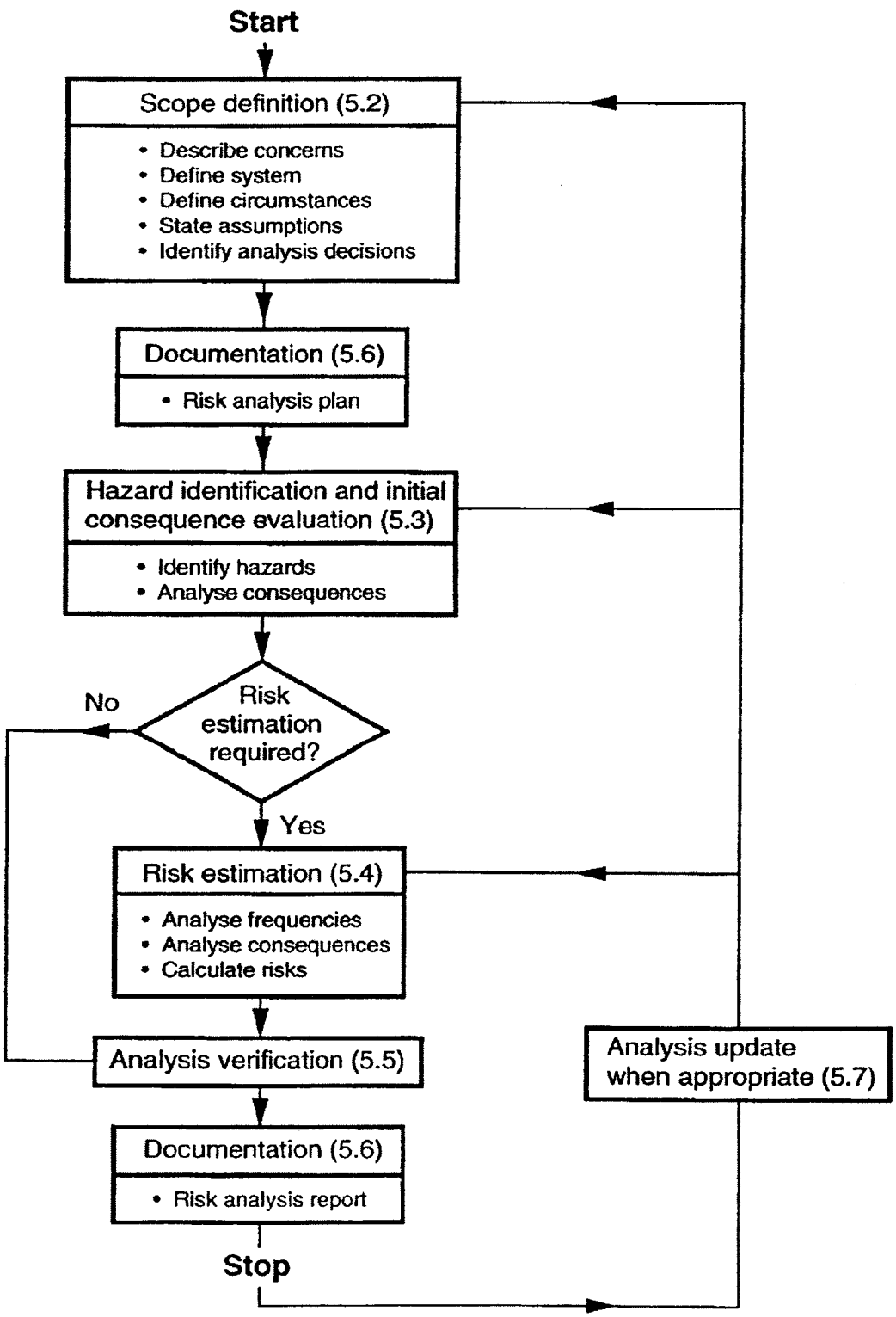

Start
Scope definition (5.2)
• Describe concerns
• Define system
• Define circumstances
• State assumptions
• Identify analysis decisions
Documentation (5.6)
• Risk analysis plan
Hazard identification and initial consequence evaluation (5.3)
• Identify hazards
• Analyse consequences
Risk estimation required?
No
Yes
Risk estimation (5.4)
• Analyse frequencies
• Analyse consequences
• Calculate risks
Analysis verification (5.5)
Analysis update when appropriate (5.7)
Documentation (5.6)
• Risk analysis report
Stop

그림 3. 리스크 분석 절차

3.2 범위 정의

프로젝트 시작과 함께 리스크 분석을 계획하기 위해 리스크 분석의 범위를 정의하고 문서화 해야한다.

1. 리스크 분석을 하게 된 이유나 문제를 기술
2. 분석 대상 시스템을 정의
3. 분석할 활동이나 문제와 관련된 모든 기술적, 환경적, 법적, 조직적, 그리고 인간적 환경에 관해 상세한 정보를 제공하는 자료출처를 정의.
4. 분석에 사용될 가정과 제약들을 기술
5. 결정해야 할 사항들과 요구되는 결과물들을 규명

3.3 위험요인과 초기 결과 평가

시스템에 리스크를 발생시키는 위험요인들 및 그들을 발견할 수 있는 방법을 함께 규명해야 한다. 결과분석에 기초하여 근본원인과 함께 규명된 위험요인의 초기 중요도 평가를 수행해야 한다.

3.4 리스크 추정

첫째, 위험요인의 가능한 원인들을 분석하여 발생빈도, 기간 및 성격을 결정한다. 둘째, 위험요인의 실현에 따른 결과들을 분석한다. 결과분석에서 위험요인과 관련된 결과들의 중요도(severity)를 추정한다. 또한 그 결과들을 초래하는 위험요인의 확률을 추정하고, 위험요인이 그 결과를 초래하게 되는 과정(연속되는 사건들)을 분석한다.

3.4.1 빈도분석

3.4.2 결과분석

3.4.3 리스크 계산

3.4.4 불확실성

모든 추정에는 불확실성이 따른다. 리스크를 규명하고 추정하는데 사용된 데이터, 방법들, 그리고 모델들과 관련된 불확실성 분석은 매우 중요하다. 불확실성 분석에서는 모델을 정의하는데 사용된 모수들 및 가정들의 변동에 의해 발생하는 모델 결과의 변동이나 부정확성을 평가한다. 불확실성 분석과 밀접하게 관련되는 분야가 민감도 분석이다. 민감도 분석에서는 모델 모수들의 변화가 모델 결과의 변화에 미치는 영향을 조사한다.

3.5 분석의 검증

분석의 무결성을 확인하기 위해 분석작업에 참여하지 않은 인원들에 의한 공식적인 검토(review) 과정을 수행한다. 검증에는 다음의 과정이 포함된다:

3.6 문서화

3.7 분석의 갱신

연속적인 리스크 경영과정을 지원하기 위해 리스크 분석이 필요하다면, 리스크 분석 문서를 대상 시스템이나 설비 또는 활동의 수명주기 전반에 걸쳐 유지될 수 있도록 관리한다. 경영상 필요할 때, 그리고 중요한 새로운 정보가 있을 때 리스크 분석은 갱신되어야 한다.

4. 리스크 분석기법

4.1 일반

여기서는 위험요소 규명이나 리스크 추정에 적용할 수 있는 분석 기법들을 그 선택 기준들과 함께 소개한다.

4.2 기법의 선택

그림 3의 요소들에 기초하여 분석기법을 선택한다.

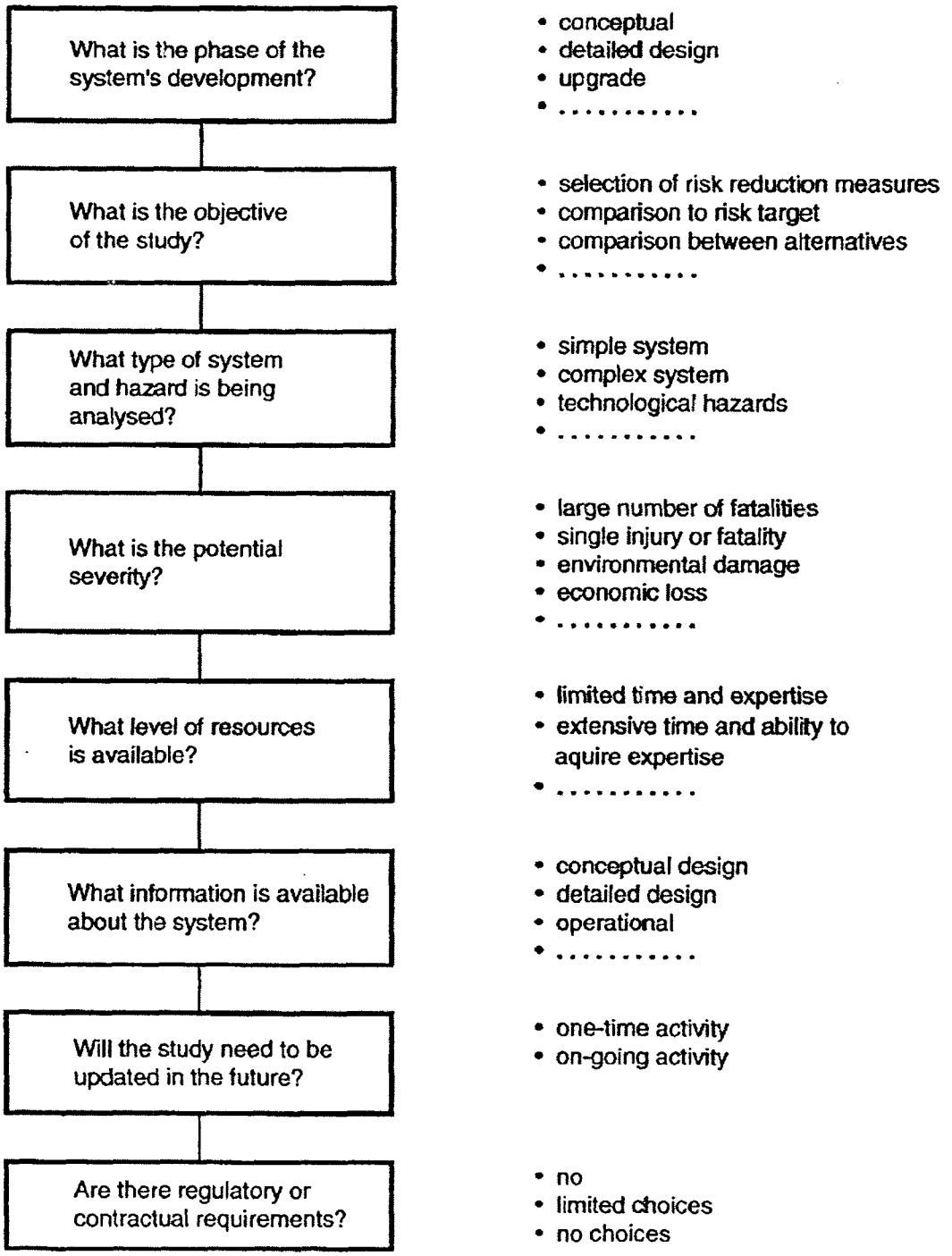


그림 3. 분석유형과 깊이를 선택하기 위한 일반적 고려사항들

4.3 분석 기법들

가장 흔히 사용되는 기법들이 표 1에 주어져 있다.

표 1. 리스크 분석에 사용되는 기법들

Method	Description and usage	Reference
Event Tree Analysis	A hazard identification and frquency analysis technique which employs inductive reasoning to translate different initiating events into possible outcomes	A.4
Fault Modes and Effects Analysis & Fault Modes, Effect and Criticality Analysis	A fundamental hazard identification and frequency analysis technique which analyses all the fault modes of a given equipment item for their effects both on other components and the system	IEC 812 A.2
Fault Tree Analysis	A hazard identification and frequency analysis technique which starts with the undesired event and determines all the ways in which it could occur. These are displayed graphically	IEC 1025 A.3
Hazard & Operability Study	A fundamental hazard identification technique which systematically evaluates each part of the system to see how deviations from the design intent can occur and whether they can cause problems	A.1
Human Reliability Analysis	A frequency analysis technique which deals with the impact of people on system performance and evaluates the influence of human errors on reliability	A.6
Preliminary Hazard Analysis	A hazard identification and frequency analysis technique that can be used early in the design stage to identify hazards and assess their criticality	A.5
Reliability Block Diagram	A frequency analysis technique that creates a model of the system and its redundancies to evaluate the overall system reliability	IEC 1078

4.3.1 위험요소(hazard) 규명

현존하는 고유한 위험요소들의 유형과 그 위험요소들이 실현될 수 있는 방법들을 규명하기 위해 체계적으로 시스템을 검토하는 것이다. 과거의 사고기록이나 위험분석 결과로부터 유용한 정보를 얻을 수 있다.

4.3.2 리스크 추정

잠재적 사고에 대해 발생빈도나 결과를 정량적으로 상세히 구하기가 어려울 수도 있다. 이러한 경우 사고의 시나리오를 정성적으로 평가한 등급을 사용하는 리스크 매트릭스를 사용할 수 있다. 그림 4는 리스크 매트릭스의 한 예를 나타낸다. 정량적 리스크 분석을 위해서는 원치 않는 사건의 발생 확률과 결과의 중요도(severity)에 대한 추정치가 필요하다.

4.3.2.1 빈도 분석

빈도분석의 목적은 위험요인 규명단계에서 밝혀진 원치 않는 사건이나 사고의 빈도를 결정하기 위한 것이다.

4.3.2.2. 결과분석

결과분석은 원치 않는 사건 발생 시 사람, 재산 또는 환경에 미치는 영향을 추정하는 것

이다.원치 않는 사건이란 독극물질의 유출, 화재, 폭발, 붕괴된 장비로부터의 돌출물 등을 말한다. 사상이나 영향의 크기를 추정할 수 있는 모델이 필요하다. 간단한 분석 방법에서부터 복잡한 컴퓨터 모델에 이르기까지 많은 방법들이 있다. 현재의 문제에 적합한 모델의 선택에 주의를 기울여야 한다.

표 1(계속). 리스크 분석에 사용되는 기법들 - 추가적인 기법들

Method	Description and usage
Category Rating	A means of rating risks by the categories in which they fall in order to create prioritized groups of risks
Checklists	A hazard identification technique which provides a listing of typical hazardous substances and/or potential accident sources which need to be considered. Can evaluate conformance with codes and standards
Common Mode Failure Analysis	A method for assessing whether the coincidental failure of a number of different parts or components within a system is possible and its likely overall effect
Consequence Models	The estimation of the impact of an event on people, property or the environment. Both simplified analytical approaches and complex computer models are available
Delphi Technique	A means of combining expert opinions that may support frequency analysis, consequence modelling and/or risk estimation
Hazard Indices	A hazard identification/evaluation technique which can be used to rank different system options and identify the less hazardous options
Monte-Carlo Simulation and other simulation techniques	A frequency analysis technique which uses a model of the system to evaluate variations in input conditions and assumptions
Paired Comparisons	A means of estimation and ranking a set of risks by looking at pairs of risks and evaluating just one pair at a time
Review of Historical Data	A hazard identification technique that can be used to identify potential problem areas and also provide an input into frequency analysis based on accident and reliability data *et al*
Sneak Analysis	A method of identifying latent paths that could cause the occurrence of unforeseen events

부록

IEC-300-3-9의 부록 A에 다음의 기법들이 소개되어 있다.

1. Hazard and Operability study (HAZOP)
2. Fault Mode and Effects Analysis (FMEA)
3. Fault Tree Analysis (FTA)
4. Event Tree Analysis (ETA)
5. Preliminary Hazard Analysis (PHA)
6. Human Reliability Assessment (HRA)

Frequency of occurrence	Indicative frequency (per year)	Severity of consequence			
		Catastrophic	Major	Severe	Minor
Frequent	> 1	H	H	H	I
Probable	$1 - 10^{-1}$	H	H	I	L
Occasional	$10^{-1} - 10^{-2}$	H	H	L	L
Remote	$10^{-2} - 10^{-4}$	H	H	L	L
Improbable	$10^{-4} - 10^{-6}$	H	I	L	T
Incredible	$< 10^{-6}$	I	I	T	T

NOTE - The category definitions and values used within this matrix are illustrative only

Where the risk classes are:

H = High risk
I = Intermediate risk
L = Low risk
T = Trivial risk

For this example the severity of the consequence categories are defined as:

Catastrophic	Virtually complete loss of plant or system. Many fatalities
Major	Extensive damage to plant or system. Few fatalities
Severe	Severe injury, severe occupational illness, significant damage to the plant or system
Minor	Minor injury, minor occupational illness or minor system damage

그림 4. 리스크 매트릭스

참고문헌

1. IEC 300-3-9 : 1995, Dependability Management - Risk Analysis of technical systems
2. IEC 50(191) : 1990, International Electronical Vocabulary(IEV) - Chapter191: Dependability and quality of service
3. IEC 812 : 1985, Analysis tecniques for system reliability - Procedure for failure mode and effects analysis (FMEA)
4. IEC 1025 : 1990, Fault tree analysis (FTA)
5. IEC 1078 : 1991, Analysis techniques for dependability - Reliability block diagram method (RBD)
6. MIL-STD-882D : 2000, Standard practice for system safety