KOSHA GUIDE
X - 35 - 2014

확률론적 리스크 평가 절차에 관한 지침

2014. 11.

한국산업안전보건공단

안전보건기술지침의 개요

○ 작성자 : 사단법인 한국안전학회 리스크관리 연구위원회
충주대학교 안전공학과 박정철
○ 개정자 : 산업안전보건연구원 안전연구실
○ 개정자 : 한국산업안전보건공단 류창환

○ 제·개정 경과

- 2011년 9월 리스크관리분야 제정위원회 심의(제정)
- 2012년 4월 리스크관리분야 제정위원회 심의(개정, 법규개정조항 등 반영)
- 2014년 11월 리스크관리분야 제정위원회 심의(개정)

○ 관련규격 및 자료

- ISO 11231:2010 Space systems – Probabilistic risk assessment (PRA)
- ISO 17666:2003 Space systems – Risk management
- Center for Chemical Process Safety (2008) Guidelines for hazard evaluation procedures, Third edition. John Wiley & Sons, Inc.
- C.A. Ericson II (2005) Hazard Analysis Techniques for System Safety. Wiley-Interscience.
- KOSHA GUIDE P-84-2012(결함수 분석기법)
- KOSHA GUIDE P-84-2012(사건수 분석기법)
- KOSHA GUIDE X-6-2012(고장형태와 영향분석(FMEA)기법에 관한 지침)

○ 기술지침의 적용 및 문의

- 이 기술지침에 대한 의견 또는 문의는 한국산업안전보건공단 홈 페이지 안전보건 기술지침 소관 분야별 문의처 안내를 참고하시기 바랍니다.
- 동 지침 내에서 인용된 관련규격 및 자료 등에 관하여 최근 개정 본이 있을 경우 해당 최근 개정 본을 참고하시기 바랍니다.

공표일자 : 2014년 11월 24일
제 정 자 : 한국산업안전보건공단 이사장

KOSHA GUIDE
X - 35 - 2014

확률론적 리스크 평가 절차에 관한 지침

1. 목 적

이 지침은 리스크를 수반하는 대규모 프로젝트나 복잡한 시스템을 운영하는 사업장에서 불확실성을 고려하여 리스크를 정량적이고 체계적으로 평가하기 위하여 9개의 단계로 구성된 확률론적 리스크 평가의 절차를 제공하는데 그 목적이 있다.

2. 적용범위

이 지침은 리스크를 수반하는 대규모 프로젝트나 복잡한 시스템을 운영하는 사업장에 적용한다.

3. 용어의 정의

(1) 이 지침에서 사용되는 용어의 정의는 다음과 같다.

(가) “마스터 로직 다이어그램(Master logic diagram, MLD)”이라 함은 사고의 일반적 유형을 정상부에, 상세화된 사고에 대한 기술을 아래에 나타내고, 도출된 초기사상을 하단부에 표시하는 계층 구조적인 트리 구조의 다이어그램을 말한다.

(나) “고장형태와 영향분석(Failure modes and effects analysis, FMEA)”이라 함은 구성품의 실패를 체계적으로 고려하고 시스템 성능에 대한 영향을 평가하는 방법론을 말한다. 기타 구체적인 내용은 KOSHA GUIDE X-6-2012를 참조한다.

(다) “시나리오(Scenario)”라 함은 초기의 원인에서 원하지 않는 결과까지 이어지는 사상의 순서 또는 조합을 말한다.

(라) “불확실성(Uncertainty)”이라 함은 입력 파라미터나 분석 과정의 부정확성으로 인한 확신의 결여를 말한다.

(마) “사건수(Event tree)”라 함은 초기사상(사건)에서 출발하여 중간사상(또는 축사상)의 성공과 실패에 따라 종결 상태까지 이어지는 사고 시나리오의 분기를 나무(Tree) 형태로 표현한 것을 말한다. 기타 구체적인 내용은 KOSHA GUIDE P-87-2012을 참조한다.

(바) “사건수 분석(Event tree analysis, ETA)”은 초기사건으로 알려진 특정한 장치의 이상 또는 운전자의 실수에 의해 발생되는 잠재적인 사고결과를 정량적으로 평가·분석하는 방법으로, 이 기법에 관한 자세한 기술적 사항은 KOSHA GUIDE P-87-2012을 참조한다.

(사) “결함수(Fault tree)″라 함은 원하지 않는 사상의 발생원인과 확률을 분석하기 위해 특정 사상의 원인을 그 아래에 있는 다양한 사상들의 논리적 조합으로 표현하는 나무 형태의 그림을 말한다. 기타 구체적인 내용은 KOSHA GUIDE P-84-2012을 참조한다.

(아) “결함수 분석(Fault tree analysis, FTA)”은 사고를 일으키는 장치의 이상이나 운전자 실수의 조합을 연역적으로 분석하는 방법으로, 이 기법에 관한 자세한 기술적 사항은 KOSHA GUIDE P-84-2012를 참조한다.

(자) “축사상(Pivotal event)”이라 함은 사건수에서 초기사상과 종결 상태 사이의 중간에 위치한 사상들을 말한다.

(차) “마르코프 분석(Markov analysis) 기법”이라 함은 어떤 상태가 시간의 경과에 따라 확률적으로 변화하는 확률과정을 바탕으로 시스템의 현 상태를 분석하여 미래를 예측하는 기법을 말한다.

(카) “신뢰도 블록 다이어그램(Reliability block diagram, RBD)”이라 함은 네트워크 관계를 나타내는 블록 다이어그램을 사용하여 복잡한 시스템의 신뢰도 및 가용성을 분석하는 기법을 말한다.

(타) “몬테카를로 시뮬레이션(Monte-Carlo simulation)”이라 함은 확률적인 조건하에서

의사결정을 목적으로 난수(Random number)를 생성하여 정해진 조건식에 적용하는 절차를 말한다.

(파) “Fussell-Vesely (F-V) 중요도”라 함은 특정 사상을 포함한 컷세트(Cut set)의 발생 확률 합을 정상사상의 발생 확률로 나눈 값을 말한다.

(하) “리스크 감소 가치 (Risk reduction worth, RRW)”라 함은 특정 사상이 발생하지 않는다고 가정할 때 감소하는 재해의 확률을 말한다.

(거) “리스크 달성 가치 (Risk achievement worth, RAW)”라 함은 특정 사상이 반드시 발생한다고 가정할 때 증가하는 재해의 확률을 말한다.

(너) “번버움(Birnbaum) 중요도”라 함은 특정 사상이 반드시 발생할 때의 재해 확률에서 발생하지 않을 때의 재해 확률을 뺀 것으로 리스크 감소 가치와 리스크 달성 가치의 합이다.

(2) 그 밖에 이 지침에서 사용하는 용어의 정의는 이 지침에 특별한 규정이 있는 경우를 제외하고 산업안전보건법, 같은 법 시행령, 같은 법 시행규칙, 산업안전보건기준에 관한 규칙 및 KOSHA GUIDE X-1-2014(리스크 관리의 용어 정의에 관한 지침)에서 정하는 바에 의한다.

4. 확률론적 리스크 평가1

확률론적 리스크 평가(Probabilistic risk assessment)는 확률에 대한 수학적 이론에 기반한 기법들을 활용해 복잡한 공학 기술적 시스템의 리스크를 전 수명주기에 걸쳐 체계적이고 포괄적으로 평가하는 것을 말한다.

확률론적 리스크 평가는 우주 항공, 전력 생산, 석유 화학, 국방 등 다양한 분야에서 복잡성이 큰 시스템이나 프로젝트의 리스크 파악 및 분석에 사용되며, 안전이나 작업의 성공에 관한 최적의 의사 결정을 보조하기 위한 체계적이고 포괄적인 방법론을 제공한다.

4.1. 확률론적 리스크 평가의 목적

(1) 확인된 개별 시나리오 또는 전체 시나리오 집합에 의해 제기되는 리스크를 파악하고 평가

(2) 리스크와 불확실성의 근원을 파악하고 시스템 설계와 운용 상에서 해당하는 리스크 영역을 확인

(3) 리스크와 불확실성의 근원의 중요도 순위 결정

(4) 리스크 감소를 위한 옵션을 파악하고 우선순위 결정

4.2. 확률론적 리스크 평가의 특징

(1) 시스템의 불확실성의 근원에 대한 정보를 제공하고, 각각의 사상과 전체 시스템의 불확실성을 보다 정확하게 정량화한다.

(2) 불확실성을 감소시키기 위한 자원 투자에 관련된 의사결정을 돕는다.

(3) 발생 확률이 낮으나 매우 심각한 결과를 초래하는 사고 시나리오를 분석하는 데 매우 적합하다.

4.3. 확률론적 리스크 평가 기법의 대표적 예

(1) 사건수 분석(Event tree analysis, ETA) 기법

(2) 결함수 분석(Fault tree analysis, FTA) 기법

(3) 마스터 로직 다이어그램(Master logic diagram, MLD)

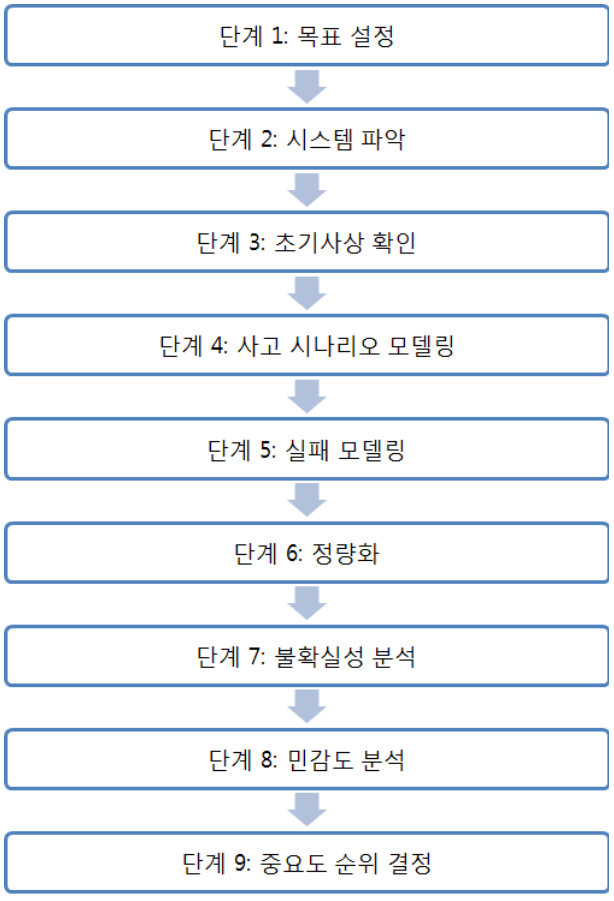
(4) 마르코프 분석(Markov analysis) 기법

(5) 신뢰도 블록 다이어그램(Reliability block diagram, RBD)

(6) 몬테카를로 시뮬레이션(Monte-Carlo simulation)

5. 확률론적 리스크 평가 절차

확률론적 리스크 평가 절차는 9개의 세부 단계로 구성되며, 각 단계의 흐름은 <그림 1>과 같다.



<그림 1> 확률론적 리스크 평가 절차의 9단계

5.1. 단계 1: 목표 설정

이 단계에서는 확률론적 리스크 평가의 목표와 범위를 정한다. 이 단계의 결과물은 분석을 하기 전에 해당 과제의 책임자와 안전 및 사업 담당 조직에 의해 면밀히 검토되어야

한다.

(1) 확률론적 리스크 평가의 목적을 파악하고, 의도한 목적과 결과의 활용 방안을 정의한다.

(2) 작업의 범위, 적용 대상이 되는 시스템의 설계 및 운영 범위, 사고 시나리오와 관련된 분석의 상세화 정도 등을 포함해 분석의 범위와 심도를 결정한다.

(3) 분석의 결과 측정 기준치를 파악한다. 이는 다음의 활동을 포함한다.

(가) 가능한 결과의 유형 파악

(나) 개별 사고 시나리오에 대한 리스크 분석이 필요한지, 특정 결과 유형에 대한 전반적 리스크 분석이 필요한지, 또는 둘 다 필요한지 결정

(다) 결과의 심각도와 사고 시나리오의 개연성 카테고리에 기반해 사용할 리스크 분류 방법(예: 리스크 매트릭스) 결정

(라) 확률 목표 및 특정 결과의 기준에 기반해 전반적 리스크 목표와 수용 기준 결정

(4) 관련된 정보 및 데이터의 출처를 파악한다.

5.2. 단계 2: 시스템 파악

이 단계의 목적은 작업과 시스템에 대해 이해하고, 작업을 완료하기 위한 시스템의 성공 기준을 이해하는 것이다. 이 단계는 다음 사항들에 대한 이해를 포함한다.

(가) 시스템 각 부분의 구성요소, 기능, 작동 원리 및 상호연관관계

(나) 운용 시 시스템 설정

(다) 운용에 있어서의 사람의 역할(명령, 통제, 유지/보수 등)

(라) 작업 중의 가능한 시스템 변경 사항

(마) 운용의 단계

(바) 관련 제도

(2) 관련 설계 및 운용 정보, 도면, 운용 및 비상 절차 등을 활용해 분석 대상 시스템을 파악한다.

(3) 기존에 운영된 적이 있는 시스템의 경우 기존의 시스템에 대한 기술 정보들을 활용한다. 설계 중에 있는 시스템의 경우 현재까지의 설계안을 기준으로 한다.

(4) 작업의 성공기준을 정의하고, 작업을 완수하기 위해 필요한 각 구성요소의 성공기준 및 기여도를 정의한다.

5.3. 단계 3: 초기사상 확인

이 단계에서는 사고로 이어질 수 있는 모든 초기사상들을 파악하고 분석한다. 이 단계는 다음의 활동을 포함한다.

(1) 기존의 시스템이나 유사 시스템에 대한 과거 경험과 체계적 방법(MLD, FMEA 등 기존 시스템의 위험 분석 결과)을 활용해 사고로 이어질 수 있는 초기사상들을 파악하고 평가한다.

(2) 파악된 초기사상들의 발생 확률을 평가하고 매우 낮은 확률(또는 빈도)의 사상들을 제외한다.

(3) 시스템에 유사한 영향을 미치는 초기사상들을 그룹화하고 그룹별 발생 확률(또는 빈도)을 결정한다.

5.4. 단계 4: 사고 시나리오 모델링

이 단계는 사건수를 이용해 초기사상들로부터 사고 시나리오를 도출한다. 이 단계는 다음의 활동을 포함한다.

(1) 각 초기사상(또는 초기사상 그룹)에 대해 초기사상이 잠재적인 결과를 발생시키지 않도록 막는 데 필요한 중간사상들(인간 행동, 구조, 시스템, 구성요소 등)의 조건적 반응(성공 또는 실패)과 대략적인 시간 순서를 도출한다.

(2) 잠재적 결과로 이어지는 사고 순서에 대해, 초기사상의 효과에 대한 시스템의 조건적인 반응을 평가한다. 재해를 예방하기 위한 제어 장치나 통제 활동(인간 행동, 구조, 시스템, 구성요소 등)의 작동에 따라 시스템의 반응은 조건적으로 변화한다.

(3) 시스템에 나타나는 반응(폭발, 산소 부족, 제어 불능 등)의 강도와 특성을 결정한다.

(4) 잠재적 결과로 이어지는 시스템 반응들에 대해, 시스템의 반응이 가져오는 잠재적 결과를 감소시키기 위해 설계되었거나 사용이 가능한 제어(인간 행동, 구조, 시스템, 구성요소)의 조건적 반응(성공 또는 실패)을 도출한다.

5.5. 단계 5: 실패 모델링

이 단계는 마르코프 분석, 신뢰도 블록 다이어그램, 결함수 분석 등의 방법을 사용해 각각의 축사상들의 결함과 실패 원인을 모델링한다.

(1) 각각의 축사상에 대해, 관련된 초기사상과 사고 시나리오 상의 이전 사상을 파악해 기록한다. 이러한 사상들은 그 성공이나 실패, 보완 등을 평가하는데 필요한 초기 조건과 경계 조건을 제공한다.

(2) 축사상의 정상적인 기능에 대한 단계 2의 성공기준을 기록한다.

(3) 각각의 축사상을 정상사상으로 하여, 해당 정상사상을 유발할 수 있는 중간 단계 고장들의 논리 조합인 실패 모델(예를 들면 결함수)을 만든다. 기능이나 시스템에 따라 중간사상의 계층은 여러 개일 수 있다.

(4) 정상사상과 연관된 초기 조건 및 경계 조건에 대해 기본사상(실패 또는 고장)들과 그들의 성공기준을 파악한다.

(5) 정상사상에 대한 결함수 모델을 사건수 모델의 해당 부분에 연결한다.

5.6. 단계 6: 정량화

이 단계는 사고 시나리오 종결 상태에 따른 결과의 크기와 발생 빈도를 추정한다.

(1) 각 초기사상에 대해 연결된 사상모델과 고장모델의 부울 대수 평가를 실시한다. 평가 결과, 사고 상태에 이르는 기본사상의 조합들(최소컷세트)을 도출한다.

(2) 초기사상의 빈도와 연관된 기본사상들의 실패 확률을 논리적으로 결합하여 각 최소컷세트의 발생 빈도를 추정한다. 실패 확률에 대한 데이터는 다음을 포함한다.

(가) 과거의 유사 시스템에 대한 경험(관련 테스트 또는 측정, 관찰의 결과 등)

(나) 다른 시스템이나 프로젝트의 데이터(데이터베이스로부터의 추정, 유사 데이터, 물리적 모델 등)

(다) 전문가 판단(분야 전문가의 직접적인 발생 가능 빈도 추정)

(3) 결과의 유형과 크기를 추정한다.

(4) 종결 상태가 같은 사고 시나리오들을 그룹화하고, 확률의 논리적 합을 구함으로써 각각의 대표적인 종결 상태가 일어날 전체 확률을 추정한다.

5.7. 단계 7: 불확실성 분석

이 단계는 의사결정자가 이해하기 쉬운 형태로 분석 결과의 불확실성을 정량화한다. 일반적으로 불확실성 분석에는 몬테카를로 시뮬레이션 방법을 사용한다.

(1) 각 최소컷세트의 발생 빈도를 추정할 때, 데이터의 불확실성이 포함되어야 한다. 최소컷세트에 있는 기본사상들에 대해 적합한 불확실성 분포를 만든다.

(2) 분석적 방법이나 몬테카를로 시뮬레이션 방법을 사용하여 초기사상의 불확실성 분포를 연관된 기본사상의 실패 확률에 대한 불확실성 분포와 논리적으로 합한다.

(3) 종결 상태(결과)의 크기의 불확실성을 결정한다.

(4) 개별 기본사상들의 전체 결과의 불확실성에 대한 기여도를 평가한다.

(5) 시사점들을 정리하고, 결과를 불확실성의 범위와 함께 기록한다.

5.8. 단계 8: 민감도(Sensitivity) 분석

이 단계는 분석 결과에 큰 영향을 미칠 수 있는 입력이나 요소를 파악하기 위해 수행하여야 한다.

(1) 작업, 구조, 시스템, 구성요소들의 성공기준, 모델링, 물리적 파라미터에 관련된 가정들을 열거한다.

(2) 최소컷세트 내에 포함된 구조, 시스템, 구성요소 중 실패에 노출되기 쉬운 공통의 특성을 갖는 것들을 찾아낸다.

(3) 열거된 가정들에 대해, 성공기준, 모델링, 파라미터 값들을 각각 독립적이고 체계적인 방법으로 변화시킨다.

(4) 성공기준, 모델링, 파라미터 값들의 변화에 따라 사상모델과 고장모델을 조정함으로써 확률론적 리스크 평가 모델을 변화시킨다.

(5) 확률론적 리스크 평가 모델을 사고 순서, 중요도 순위, 정량적 리스크 결과의 변화 관점에서 전반적으로 재평가한다.

(6) 단일 컷세트 내에 있는 잠재적으로 상호의존적인 구조, 시스템, 구성요소에 대해, 그들을 단일 기본사상으로 합치고 연관된 사상들 중 가장 높은 확률을 부여한다.

(7) 각각의 조정된 컷세트에 대해 사고 순서, 중요도 순위, 정량적 리스크 결과에 생기는 변화들을 재평가한다.

5.9. 단계 9: 중요도 순위 결정

이 단계는 사고 시나리오에 미치는 영향력이 큰 요소들을 파악하기 위해 중요도를 정량적으로 평가하고 순위를 부여한다.

(1) 리스크에 기여하는 주요 요소를 파악한다.

(2) 중요도 측정방법을 활용해 전반적인 리스크 모델을 평가하고 개별 사고 시나리오와 기본사상에 순위를 부여한다. 중요도 측정 방법으로는 Fussell-Vesely (F-V) 중요도, 리스크 감소 가치 (RRW), 리스크 달성 가치 (RAW), 번버움 중요도 등이 사용될 수 있다.

(3) 사고 시나리오와 기본사상들의 전반적 리스크와 불확실성에 대한 기여도를 결정한다.

6. 데이터 수집 및 분석

확률론적 리스크 평가의 수행 시 다양한 데이터를 수집하고 분석하는 활동은 주로 데이터베이스를 통해 이루어진다. 데이터 수집 및 분석은 위의 9개 단계와 병행하여 또는 결합하여 수행되며 다음과 같은 활동을 포함한다.

(1) 확률론적 리스크 평가 모델의 초기사상과 기본사상들로부터 데이터를 확인한다.

(2) 객관적 데이터(측정되거나 관련 테스트 또는 경험을 통해 직접 관찰된 데이터), 반객관적 데이터(일반적 데이터, 유사 데이터, 물리적 모델 등을 통한 유추), 주관적 데이터(해당 분야 전문가의 판단)를 활용해 사상들의 확률 및 빈도 정보를 수집한다.

(3) 통계적 방법을 활용해 사상의 발생 확률을 추정하고 불확실성 분포를 도출한다.

(4) 수집된 정보, 데이터, 파라미터 추정치, 불확실성을 포함하여 확률 정보를 데이터베이스에 입력한다.