KOSHA GUIDE
X - 52 - 2012

생산시스템의 수명주기에 따른 리스크 평가지침

2012. 11.

한국산업안전보건공단

안전보건기술지침의 개요

○ 작성자 : 사단법인 한국안전학회
충북대학교 안전공학과 임현교

○ 제·개정 경과

- 2012년 8월 리스크관리분야 제정위원회 심의(제정)

○ 관련규격 및 자료

- AS/NZS 4360, Risk management, 1999
- ISO 9000, Quality Management Systems, 2000
- KS A 3004, 신뢰성 용어, 1988
- IEC 61511-1, Functional Safety, 2000
- NM 87117-5670, Air Force System Safety Handbook, 2000
- DHB-S-001, SYSTEM SAFETY HANDBOOK, 1999
- KOSHA GUIDE X-1-2011 (리스크 관리의 용어 정의에 관한 지침)
- KOSHA GUIDE X-4-2012 (리스크 평가기법 선정에 관한 지침)
- KOSHA GUIDE X-6-2012 (고장형태와 영향분석(FMEA)기법에 관한 지침)

○ 기술지침의 적용 및 문의

이 기술지침에 대한 의견 또는 문의는 한국산업안전보건공단 홈 페이지 안전보건기술지침 소관 분야별 문의처 안내를 참고하시기 바랍니다.

공표일자 : 2012년 11월 2일
제 정 자 : 한국산업안전보건공단 이사장

KOSHA GUIDE
X - 52 - 2012

생산시스템의 수명주기에 따른 리스크 평가지침

1. 목 적

이 지침은 생산시스템과 관련된 사고의 예방을 위하여, 구상에서부터 폐기에 이르기까지 전 수명주기에 걸쳐 리스크를 관리하는 시스템안전공학적 안목에 입각하여 생산시스템의 리스크 평가 원칙을 제시함을 목적으로 한다.

2. 적용범위

이 지침은 반복적으로 개발되고 생산되는 제품이나 생산시스템 등 생산기술과 관련된 모든 기구 및 시스템에 적용된다.

3. 용어의 정의

(1) 이 지침에서 사용하는 용어의 정의는 다음과 같다.

(가) “생산시스템(이하 “시스템”이라 한다)”이라 함은 여러 요소로 구성된 시스템으로서, 사용자에게 판매 후 제품생산을 위해 이용되는 산업기기 및 설비를 말한다.

(나) “수명 주기 (Life cycle)”라 함은 생산시스템의 구상단계에서 시작하여 완전히 폐기될 때까지의 안전성을 평가함에 있어서 고려되어야 하는 전체 기간(IEC 61511-1: 2003 참조)을 말한다.

(다) “시스템 안전 프로그램 (System safety program)”이라 함은 시스템의 전 수명단계를 통하여 가장 적합할 때에 가장 효율적이고 경제적인 방법으로 시스템 안전요건을 만족시킴으로써 시스템의 효용성을 높이려는 안전관리 활동들의 추진계획을 말한다.

(라) “시스템 안전 우선순위 (System safety precedence)”라 함은 시스템을 개

발함에 있어 안전을 확보하기 위해 순서에 따라 우선적으로 적용되어야 하는 유해위험요인 제거기법들의 적용순서를 말한다. 선행 기법을 적용할 수 없거나, 적용하더라도 잔존 리스크가 허용 기준을 넘을 때에만 후행 기법을 적용하는 것을 원칙으로 한다.

(마) "구상설계심사 (Concept design review, CDR)"라 함은 시스템의 구상 단계에서 실시하는 시스템의 리스크 평가와 검토를 말한다.주1)

(바) "예비설계심사 (Preliminary design review, PDR)"라 함은 기본설계가 끝나고 상세설계가 시작되기 전에 실시하는 시스템의 리스크 평가와 검토를 말한다.

(사) "중요설계심사 (Critical design review, CDR)"라 함은 시스템 상세설계의 기술적 타당성, 완벽성 및 정확성의 평가와 검토를 말한다.주2)

(아) "최종수용심사 (Final acceptance review, FAR)"라 함은 생산 설계가 완성되고 실시하는 시스템의 리스크 평가와 검토를 말한다.

(자) "결함 위험요인 분석 (Fault hazard analysis, FHA)"이라 함은 복잡한 시스템에 있어 전체 시스템을 몇 개의 서브시스템(Subsystem)으로 나누어 분할 제작하는 경우, 서브시스템이 다른 서브시스템 또는 전체 시스템의 안전성에 미치는 영향을 분석하는 방법을 말한다.

(차) "운용 위험요인 분석 (Operating hazard analysis, OHA)"이라 함은 대상 시스템을 사용하는 도중에 발생할 수 있는 생산, 유지보수, 시험, 운반, 저장, 운전, 구조, 훈련 및 폐기 등에 관련된 인원, 순서, 설비에 관한 유해위험요인을 평가하기 위하여 실시하는 분석 방법을 말한다.

(2) 그 밖에 이 지침에서 사용하는 용어의 정의는 이 지침에 특별한 규정이 있는 경우를 제외하고는 산업안전보건법, 같은 법 시행령, 같은 법 시행규칙, 산업안전보건기준에 관한 규칙 및 KOSHA GUIDE X-1-2011(리스크 관리의 용어 정의에 관한 지침)에서 정하는 바에 의한다.

주1) 중요설계심사와 구분하기 위하여, 통상 같이 쓰는 경우에는 CDR1로 표기함. <표 1> 참조.
주2) 구상설계심사와 구분하기 위하여, 통상 같이 쓰는 경우에는 CDR2로 표기함. <표 1> 참조.

4. 생산시스템의 수명주기에 따른 리스크 평가

4.1 수명주기 단계별 특성

(1) 구상 (Concept) 단계

구상 단계는 시스템을 제작하기 위한 시작 단계로서, 시스템의 사용목적과 기능, 앞으로 생산할 시스템을 개발함에 있어 일반적인 진행과정이 결정된다.

(2) 정의 (Definition) 단계

예비 설계안과 생산 기술과의 비교를 통해 시스템 개발의 가능성과 타당성을 확인하고, 시스템 개발상의 일반적인 설계가 이루어지는 단계이다.

(3) 개발 (Development) 단계

시스템 개발의 공식적인 시작단계이다. 이미 시스템 안전 프로그램에 계획된 대로 개발단계에서 시도되어야 하는 시스템 안전 업무들이 시작된다.

(4) 제조 (Production) 단계

제조 단계에서 수행되는 거의 모든 업무는 주로, 이전 단계에서 획득된 시스템의 안전수준이 생산단계에서도 유지되는가를 확인하기 위한 것이다.

(5) 배치 (Deployment) 단계

운용 단계는 시스템 개발, 생산의 다음 단계로서, 사용자가 최초의 시스템을 사용하기 위해 수용하는 순간부터 시작한다.

(6) 폐기 (Disposal) 단계

폐기 단계는 시스템이 갖는 특정한 설계요인 때문에 매우 중요할 수도 있다. 시스템의 유해위험요인이 있는 부분, 예를 들어 부식성·유해성 물질, 방사능 폐기물, 가연성 물질, 방향성 물질 등을 폐기하는 절차는 시스템 개발 초기에, 주로 개발단계에서 검토되고 결정되어야 한다.

4.2 수명주기 단계별 리스크 평가

(1) 유효하고 적절한 정보는 성공적인 리스크 평가를 위한 필수 조건이며, 리스

크 평가자가 사용할 수 있는 정보는 수명주기 단계에 따라 제한된다.

(2) 생산시스템의 수명주기 단계는 어떤 리스크 평가 기법을 사용하든지 변하지 않으며 리스크 평가자가 변경할 수 없는 조건이다. 리스크 평가자가 수명주기 단계를 변경할 수는 없지만, 각각의 수명주기 단계에서 사용할 수 있는 정보를 바탕으로 적합한 리스크 평가 기법을 선정할 수는 있다.

(3) 각 수명주기 단계에 대한 리스크 평가는 아래와 같다.

(가) 구상 단계 (Concept phase)

① 이 단계의 리스크 평가는 시스템 안전에 관련된 치명적인 요소, 위험 형태 및 영향, 위험수준에 대해 검토하는 것을 목적으로 한다.

② 다양한 설계사양에 대하여 시스템 안전 측면에서 기술적 시도들이 이루어진다.

③ 서브시스템들간의 잠재적인 인터페이스 문제들 중 안전에 관한 문제들을 구명한다.

④ 새로운 사양이거나 최신의 기능을 가졌기 때문에 안전측면에서 조사한다.

⑤ 허용 최대고장률 또는 허용가능한 최대 사고횟수 등의 시스템 안전성능 변수가 정의된다.

⑥ 시스템에 대한 새로운 평가의 필요성, 시스템 운용 등의 제한, 시스템 검사 중 수용될 수 있는 유해위험요인 형태 등의 특별한 이유로 주의하지 않으면 안 되는 분야도 구명한다.

⑦ 일반적으로 예비 위험요인 분석(Preliminary hazard analysis, PHA) 기법을 통해 리스크를 평가한다.

(나) 정의 단계 (Definition phase)

① 이 단계의 리스크 평가는 예비 설계와 생산 기술을 확인하는 것을 목적으로 한다.

② 생산시스템 안전 활동의 핵심이라 할 수 있는 유해위험요인 분석이 시작된다.

③ 보다 상위의 생산시스템 사양에 포함될 필요가 있는 안전 요구사양이나 제한조건들이 결정된다.

④ 생산시스템 안전 조직에 관련되는 모든 정보원으로부터 요구되는 자료들이 무엇인지 결정된다.

⑤ 고장형태와 영향분석(Failure mode and effect analysis, FMEA) 기법을 통해 신뢰도공학과의 연계검토가 필요하다.

(다) 개발 단계 (Development phase)

① 이 단계의 리스크 평가는 완성된 안전성 설계기준의 최종검토를 목적으로 한다.

② 시스템의 다양한 구성요소들의 안전목표를 설정하고, 또 그것이 충족되었는가를 판단하는 데 필요한 설계기준을 설정한다.

③ 여러 가지 설계 단계를 거치는 동안, 시스템과 그 구성요소들에 대하여 안전성을 평가한다.

④ 생산시스템 사용자에게 교육시키기 위한 다양한 훈련과정에 관계자료들을 제공한다.

⑤ 시스템 안전과 관련된 설계 사양들이 적절히 검사되었는지 확인하기 위한 검사계획을 심사한다.

⑥ 시스템 이상이나 고장에 대한 보고체계도 이 단계에서 준비되어야 한다.

⑦ 통상 이 개발단계의 종료시점에서 설계완료된 시스템을 대상으로, 계획대로 생산을 추진할 것인가 말 것인가 최종적인 결정을 하게 된다.

⑧ 고장형태와 영향분석(FMEA) 기법을 통해 신뢰도공학과의 연계검토가 필요하다.

(라) 제조 단계 (Production phase)

① 이 단계의 리스크 평가는 품질관리 부서와의 긴밀한 협력을 통해 정의단계와 개발단계에서 수행되었던 분석을 검토하며, 필요시 설계를 변경하고 그 영향을 검토하는 것을 목적으로 한다.

② 이 단계에서 안전교육이 시작된다.

③ 시스템의 안전 수준을 훼손시킬 수 있는 중요한 생산과정, 검사, 심사를 검토한다.

④ 이미 확보된 안전수준이 훼손되었는가를 판단하기 위하여, 품질보증 활동에 의해 감시되어야 하는 시스템특성을 결정한다.

⑤ 최종적인 시스템 설계의 안전수준이 이미 획득된 수준 이상인가를 결정하기 위하여, 공학적・기술적인 수정을 감사(Audit)한다.

⑥ 일반적인 평가기법으로는 고장형태와 영향분석(FMEA) 기법이나 결함수분석(Fault tree analysis, FTA) 기법 등을 통해 리스크를 평가한다.

(마) 배치 단계 (Deployment phase)

① 이 단계의 리스크 평가는 사고, 사건, 고장 등 사용중 발생하는 모든 문제들에 대한 추적 처리의 실시와 안전교육을 목적으로 한다.

② 이미 달성된 시스템 안전수준이 훼손되지 않았는가를 확인하기 위하여, 기계・절차 등의 변경사항들을 대상으로 평가를 실시한다.

③ 이 단계 동안 수행되는 유지보수절차 자체가 위험을 초래하지 않으며, 동시에 시스템의 안전수준을 훼손하지 않는다는 것을 보증하기 위하여 사용상황을 평가한다.

④ 긴급조치와 훈련 프로그램들이 적절히 수행되었는가 보증하기 위하여, 프로그램의 절차들을 평가한다.

⑤ 사용단계 중에 발생할 수 있는 사건 및 사고에 대하여 조사한다.

⑥ 일반적인 평가기법으로는 운용 위험요인 분석(Operating hazard analysis, OHA) 기법이 적절하다.

(바) 폐기 단계 (Disposal phase)

① 이 단계의 리스크 평가는 사전에 결정된 시스템의 폐기처리 절차대로 처리되는가를 검토하고, 그 방법이 신중하게 감시되고 있는가를 점검하는 것을 목적으로 한다.

② 시스템의 유해위험요인이 있는 부분 등을 폐기하는 절차는 시스템개발 초기에, 주로 개발단계에서 검토되고 결정되어야 한다.

③ 정상적인 제품 수명 후의 폐기절차를 고려해야 한다.

④ 시스템 수명주기 중 어느 때라도 발생할 수 있는 긴급 폐기절차를 고려해야 한다.

⑤ 이 과정들이 적절히 수행되는가를 보증하기 위하여, 시스템의 위험 물질들의 폐기절차를 신중히 감시하고, 필요시 감사업무를 수행하여 시스템으로 인한 유해위험요인이 확산되지 않도록 끝까지 노력하는 것이 시스템 안전의 최종업무이다.

⑥ 일반적인 평가기법으로는 고장형태와 영향분석(FMEA) 기법이나 운용 위험요인 분석(OHA) 기법이 적절하다.

5. 시스템 안전 프로그램 (System safety program, SSP)

5.1 시스템 안전 프로그램의 목적

(1) 시스템 안전 프로그램은 시스템의 수명주기 단계에 따라서 공학적, 과학적, 관리적 적용을 통해서 안전을 확보하는 것을 목적으로 한다.

(2) 주어진 시스템의 개발이나 프로젝트에 있어서 구체적인 시스템 안전 요구사항 (Safety requirements)을 정의하기 위한 것이다.

(3) 시스템 안전 업무활동, 리스크 평가 방법 및 수용 기준, 시스템 안전의 문서 양식, 시스템 개발과정에서의 주요 안전업무활동 시기 및 방법, 시스템 안전조직 등이 포함되어야 한다.

5.2 시스템 안전 프로그램의 요건

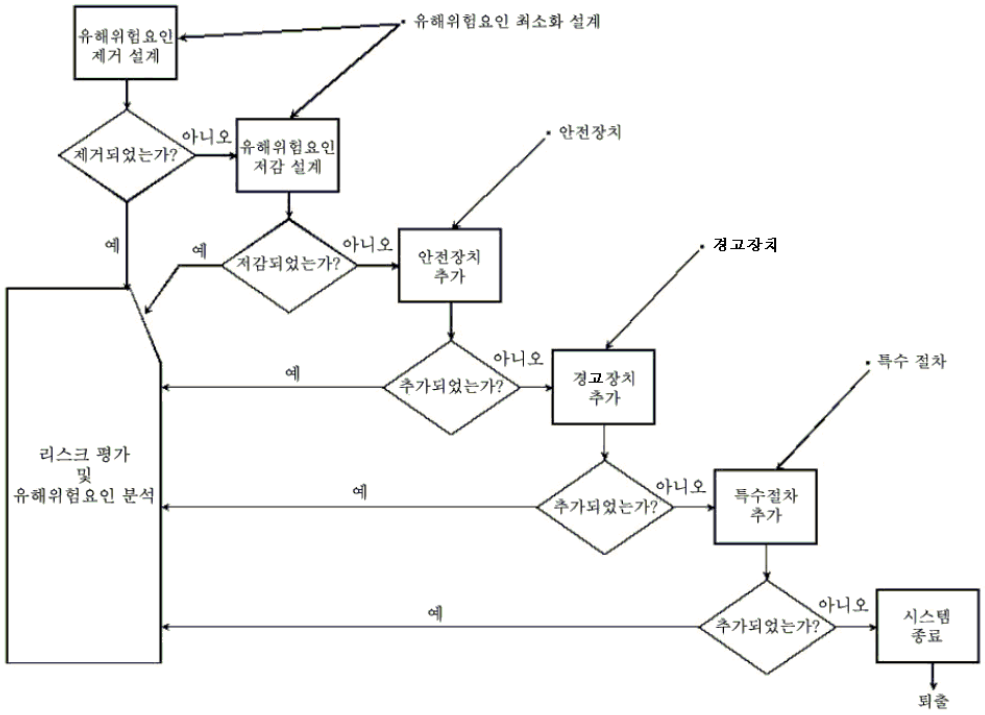
(1) 안전을 위한 설계 범위와 공학적 요구사항을 기술해야 한다. 구상부터 폐기까지의 모든 수명주기 단계에 적절한 안전 요구사항과 보조 장비에 관한 사항을 기술해야 한다.

(2) 리스크 평가 절차를 기술해야 한다. 위험의 강도와 빈도 수준, 안전 요건에 만족하는 시스템 안전 절차를 기술해야 한다.

(3) 리스크 평가에 사용되는 정량적 또는 정성적 척도와 허용 가능한 리스크 수준을 설명해야 한다.

5.3 시스템 안전 우선순위

시스템을 개발함에 있어 안전을 확보하기 위해 순서에 따라 우선적으로 적용되어야 하는 유해위험요인 제거기법들의 적용순서를 말한다. 즉, 시스템과 관련된 사고를 예방하기 위하여 설계자는 <그림 1>과 같은 안전설계의 절차를 반드시 순서대로 준수해야 한다. 선행기법을 적용할 수 없거나, 적용하더라도 잔존 리스크가 허용 기준을 넘을 때에만 후행 기법을 적용하는 것을 원칙으로 한다.



<그림 1> 시스템 안전 우선순위 (Roland, 1983)

(1) 유해위험요인 최소화 설계(Design for minimum hazard)는 시스템의 설계 사항이나 구조 자체가 유해위험요인을 지니지 않도록 구상단계에서부터 신중히 고려하여 설계하는 것을 말한다.

(2) 안전장치(Safety devices)는 작업자나 사용자에게 직접 위해를 가하지 않도록 시스템에 구조적으로 또는 기능적으로 추가되는 장치를 말한다.

(3) 경고장치(Warning devices)는 시스템이 통제상태를 벗어난 경우 사용자로 하여금 신속한 대응조치나 대피가 가능하도록 경보를 발하는 장치를 말한다. 경보장치, 사용 설명서, 표지, 라벨 등이 모두 여기에 포함된다.

(4) 특수 절차(Special procedures)는 이상의 모든 수단이 강구되었음에도 불구하고 유해위험요인이 남아 사용자에게 위협이 된다면, 사용자에게 위험회피 기술이나 능력을 부여하기 위한 관리적 기법을 말한다. 개인 보호구의 활용, 교육 및 훈련은 여기에 해당한다.

5.4 시스템 리스크 평가 활동

(1) 시스템 수명주기 리스크 평가의 활동 계획을 나타내면 <표 1>과 같다.

<표 1> 시스템 안전 프로그램의 운용 (Roland)

관리포인트 / 시스템안전활동	구상	CDR_1	정의	PDR	개발	CDR_2	생산	FAR	운용 배치	폐기
1 안전 업무활동 작성										
2 안전 설계기준 발										
3 유해위험요인 분석 실행	PHA	PHA/FHA/FTA		FHA/OHA			OHA			
4 안전설계사양 결정	초기		최종							
5 설계검토 실시										
6 사용설명서에 안전관련 사항 제공				제출 및 검토						
7 고장분석에 참여	기록 자료 심사			검사 결과						
8 리스크 분석 실시		필요시								
9 서류심사										
10 안전장치 확인 및 정의	초기		예비 설계							
11 안전검사 계획 및 준비	초기			수정 및 증명						
12 안전검사 실시			모형	증명			수용			
13 안전훈련 실시					지원		감시			
14 사고조사에 참여										

PHA : 예비 위험요인 분석
FHA : 결함 위험요인 분석
OHA : 운용 위험요인 분석
FTA : 결함수 분석

CDR_1 : 구상설계 심사
PDR : 예비설계 심사
CDR_2 : 중요설계 심사
FAR : 최종 수용여부 심사

(2) 표에서 리스크 평가의 관리 포인트로 제시된 CDR_1, PDR, CDR_2, FAR은 각각 구상설계심사 (Concept design review), 예비설계심사 (Preliminary design review), 중요설계심사 (Critical design review), 최종수용심사 (Final acceptance review)를 나타낸다. 이는 시스템을 개발하고 생산함에 있어 필요한 시스템의 리스크 평가와 검토가 요구되는 중요한 관리 포인트를 가리킨다.

(3) 시스템 안전 활동은 안전기준의 설정, 유해위험요인 분석, 안전수준의 측정

과 평가, 안전추진 업무활동, 검사절차, 사용방법 및 지침의 개발, 산업재해의 조사, 그리고 구매 및 판매 연구까지 해당된다.

(4) 시스템 개발의 구상 및 기획을 의미하는 구상단계(Concept phase)에서부터 폐기단계(Disposal phase)까지 지속적으로 이루어진다.

5.4 시스템 안전 프로그램의 내용

(1) 일반개요

(가) 서문

(나) 범위와 목적

(다) 적용과 시행

(라) 적용 문서

(2) 안전조직, 책임 및 권한

(가) 전체 조직과의 관계

(나) 조직계열

(다) 책임과 권한

(라) 관련부문

(마) 시스템 안전 담당 그룹의 조직 계열, 책임 및 권한

(3) 시스템안전기준

(가) 정의

(나) 유해위험요인 수준의 종류

(다) 시스템 안전의 우선순위

(라) 특별한 계약조건

(마) 분석 기술의 확정

(4) 수행해야 하는 시스템 안전 업무활동

(가) 정성적 분석

(나) 정량적 분석

(다) 운용 위험요인 분석 (OHA)

(라) 업무활동 심사의 참가

(마) 설계 심사에의 참가

(5) 시스템 안전문서

(가) 시스템 안전과 관련하여 제출하여야 하는 보고서의 수, 서식 및 예정시기

(나) 시스템 안전과 관련하여 수령되어야 하는 보고서의 수, 서식 및 예정시기

(다) 유해위험요인의 보고를 위한 서식

(라) 사고 조사의 순서

(마) 안전의 홍보

(바) 안전관련 자료은행

(사) 계약업자와 하청업자간에 안전자료를 보급시키기 위한 순서

(아) 진료보고

(6) 안전업무활동의 관리

(가) 관리하는 작업의 중간 및 최종과정

(나) 하청업자의 안전감사를 위한 절차 및 예정

(다) 부서내 안전감사를 위한 절차 및 예정

(7) 안전훈련

(가) 위험한 활동에 대한 직원의 자격

(나) 제조, 검사, 유지보수, 품질관리 작업자, 시스템 운전자, 사용자에 대한 훈련 및 면허 업무활동

(다) 긴급시에 대응한 훈련

(8) 설비 및 지원기능

(가) 위험한 재료의 취급 및 저장을 위한 필요사항과 절차

(나) 위험한 재료의 공급과 수송에 필요한 필요사항과 절차

(다) 취급, 저장, 공급 또는 수송 중에 따라야 하는 평상시 및 긴급시의 절차