제품안전 및 신뢰성기법 체계에 관한 연구

권영일(청주대학교*), 김종걸(성균관대학교), 이낙영(충남대학교)
홍연웅(동양대학교), 전영록(경남대학교), 나명환(성균관대학교)

Abstract

PL시대의 제품안전과 신뢰성을 확보하기 위한 각종 활동 체계와 기법들 및 그 관련성을 알아본다. 제품의 신뢰도, 가용도, 안전성, 그리고 보전성을 종합적으로 다루는 통합 신뢰성 (dependability) 에 관한 예측 및 분석 기법들과 각 기법의 특징, 적용에 대해 소개하고, 이들 기법을 효과적으로 연계, 활용할 수 있는 안전/신뢰성/품질보증 통합경영시스템에 대해 고찰한다.

1. 서론

1.1 제조물책임(PL), 제품안전 과 신뢰성

제조물책임이란 인도된 제품의 결함(defect)에 의한 신체적. 경제적 손실(그 제품을 직접 사용치 않은 제3자도 포함)에 대한 책임을 의미한다. 손실에 대한 책임은 제조, 유통, 판매, 수입 등 사업상 그 제품에 관련된 자가 진다. 단 손실이 결함 제품 그 자체에만 한정되는 경우는 제외한다. 제품안전이란 제품의 수명주기 전 기간에 걸쳐 운영의 효율성, 시간, 비용의 제약 하에서 위험(risk)을 최소화하고 안전성(safety)을 최적화하기 위해 공학적, 경영학적 이론과 기술을 응용하는 것으로 정의된다. 또한 신뢰성(dependability)이란 신뢰도(Reliability), 가용도(Availability), 보전도(Maintainability), 그리고 안전성(Safety) (이를 요약하여 RAMS로 표현) 면에서 시스템이 장기간에 걸쳐 가동하는 행태(behavior)를 종합적으로 표현하는 용어이다. 따라서 제품안전 및 신뢰성은 하나의 제품이 태어나서 폐기되기까지의 수명주기(개념/정의, 설계/개발, 생산, 운용/정비)동안의 모든 업무와 관련된다.

1.2 PL의 기능

제조물 책임법안이 시행됨으로서 제품의 안전성과 신뢰성이 신장되고, 사고 발생 시 충분한 보상을 제공할 수 있게 된다. 생산 및 소비자 양측 모두 제품의 제조. 사용에 있어 안전에 주의를 기울이도록 동기를 부여한다. PL법이 갖는 의미를 함축적으로 나타내면 "과실책임원칙"에서 "결함(defect) 책임원칙"으로 전환된 것이라고 할 수 있다.

1.3 PL법의 주요내용

1) 제조물(제품)의 정의

제조물 = 제조 또는 가공된 동산

(Product = movable property manufactured or processed)

따라서 서비스, 정보, S/W, 전기 등은 법의 대상에서 제외되며, 인위적으로 가공 처리된 제품이 아닌 농.림.수산물, 광산물도 법 적용을 받지 않는다.

2) 결함(defect) 의 정의

결함이란 품질의 결여(lack of quality)가 아니라 생명, 신체, 재산상 손실을 야기할 수 있는 안전의 결여(lack of safety)를 의미한다. 즉 결함이란 제품의 성격, 보통 예측 가능한 사용방법, 제품이 인도된 시점 등을 고려하여 제품이 갖추어야 할 안전의 결여를 말한다. 여기서 제품의 성격(nature of the product)은 제품자체의 환경으로서 제품안내, 사고방지를 위한 경고, 위험에 비한 제품의 유용성, 비용 대 효과 (동일한 비용하에서의 안전기준), 사고발생확률, 통상의 사용기간, 내구년한 등의 요소를 말한다. 일반적으로 예견할 수 있는 사용방법은 제품의 사용환경과 관련된 항목들, 정상적으로 예측 가능한 용도로 사용하는 지와 사용자에 의한 손실 방지 가능성 등의 요소가 고려된다. 제조자에 의해 제품이 인도(유통)된 시점과 관련된 요소에는 제품이 소비자에게 배달된 시점에서의 안전수준, 기술상의 능력 (안전규정, 설계변경 가능성) 등이 포함된다.

1.4 제품 결함의 근거

1) 부적합한 설계 : 통상 소비자가 상해를 방지할 수 있는 설계대안을 제시하도록 요구된다. 설계결함의 경우 관례나 그 분야의 표준사용이 면책요건이 될 수 없다. 예: 전체 제품들이 설계결함일 수도 있다. (state of the art defense 는 예외로 인정)
2) 제품에 대한 시험(test), 검사(inspection) 의 실패
3) 제조.조립상의 하자 : 소비자가 결함이 제조과정에 기인한다는 것을 입증해야 함
4) 위험요소에 대한 경고 실패
5) 과대광고
6) 오용, 남용가능성에 대한 예측 실패

1.5. 제품 수명주기와 제품안전/신뢰성 업무

위에서도 알 수 있듯이 제품의 안전/신뢰성과 관련된 문제에 대처하기 위해서는 하나의 제품이 태어나서 폐기되기까지 수명주기 전 과정에 걸친 공학적, 경영학적 기술과 이론이 필요하다. 정의/개념적 설계, 상세설계/개발, 제조/양산, 판매, 사용/보전 및 폐기에 이르기까지 상호 관련성이 깊은 품질, 안전, 그리고 신뢰성 분야의 업무, 기법, 정보, 각종 표준과 규정을 효율적으로 경영할 수 있는 통합경영시스템을 구축하여 운영하는 것이 바람직하다.

2. RAMS 활동 및 기법

ISO 9001/2/3을 바탕으로 신뢰성 및 안전성을 통합한 경영시스템을 구축. 운영할 수 있다. RAMS 분석은 시스템의 신뢰도, 가용도, 보전도, 그리고 안전성을 검토하고 예측하기 위해 사용되며 시스템의 각 레벨과 세부 항목들에 대하여 주로 개념/정의 단계, 설계/개발 단계, 그리고 운용/정비 단계 동안 수행된다.

2.1 RAMS 분석절차

1단계 : 제품의 안전/신뢰성과 가용도 요구조건, 특성과 특징, 환경조건, 가동조건, 정비조건 목록을 작성(list)한다. 분석할 시스템, 가동 모드, 상위 레벨과 인터페이싱 시스템 또는 공정과의 기능적 관계를 정의한다.

2단계 : 시스템의 기능적 요구조건, 예상되는 작동과 작동 환경에 근거하여 시스템의 결함, 결함 기준과 상태를 정의한다.

3단계 : 수치상의 결과가 필요하면 예비설계에 기초한 배분(allocation)을 수행한다. (시스템의 총 허용 고장률을 각 하위 시스템에 할당한다).

4단계 : 시스템을 분석한다.

4.1) 정성적 분석 (연역적/귀납적 방법)
시스템의 기능적 구조를 분석하고, 시스템/컴포넌트의 결함 모드, 고장 메카니즘, 고장효과와 그 결과를 결정한다. 아이템의 정비성을 고려하고, 신뢰도나 가용도 모델을 설정하며, 가능한 정비, 수리정책을 결정한다.

4.2) 정량적 분석 (해석적 또는 시뮬레이션 방법)
아이템의 신뢰도 데이터(예:고장률)를 규정하고, 수학적 신뢰도/가용도 모델을 설정한다. 수학적 모델을 평가하고 컴포넌트의 중요도와 민감도를 분석한다. 중복구조나 정비정책에 따른 시스템의 성능 개선을 평가한다.

5단계 : 결과의 평가, 요구조건 또는 다른 대안과 비교.

5.1) 시스템 설계 검토, 약점, 불균형, 치명적인 결함 모드와 아이템 파악, 시스템 인터페이스 문제, fail-safe 특성과 매카니즘 등 고려

5.2) 신뢰성을 개선할 수 있는 다른 대안 개발 (예: 중복 구조, 성능 감시, 결함 탐지, 시스템 재구성, 정비성, 부품 교체의 수월성, 수리 절차)

5.3) trade-off 분석을 수행하고 대안 설계들의 비용을 평가한다.

RAMS 분석 활동과 각 기법들간의 관계가 표 1에 주어져 있다.

표1 RAMS 분석 활동과 각 기법들간의 대응관계

일반적 절차	분석 기법				
분석활동	FMEA FMECA 고장모드 및 영향해석	FTA 결함나무분석	RBD 신뢰도 블럭도	MA 마코브 분석	PC 부품수계산 신뢰도예측
요구사항과 시스템 정의	컴포넌트 규격과 작동	시스템의 기능적 구조	시스템과 서브시스템 작동	컴포넌트 기능 시스템 기능구조	컴포넌트 규격과 고장 데이터
시스템 결함정의	1차(최하위) 기능 수준의 고장	원치않는 정상사건	시스템 작동 (실패) 기준	시스템성공/실패 기준	1차(최하위) 기능 수준의 고장
신뢰도 배분	컴포넌트에 적용 가능한 경우	서브시스템에 적용가능한 경우	서브시스템에 적용가능한 경우	서브시스템에 적용가능한 경우	컴포넌트에 적용 가능한 경우
정성적 분석 정비전략	귀납적(표)	연역적(결함나무)	연역적(블럭도)	귀납적/연역적 (상태전이도)	직렬구조가정 컴포넌트 열거, 평가
정량적 분석 (수치적 평가)	결함 치명도 확률 분석	시스템신뢰도 가용도 계산	시스템신뢰도 가용도 계산	시스템신뢰도 가용도 계산	시스템/컴포넌트 고장율 계산
요구사항 충족? (절차종료기준)	고장치명도와 발생확률이 기준 이내인가?	정상사건 발생확률이 기준 이내인가?	신뢰도/가용도 요구조건이 만족 되는가?	신뢰도/가용도 요구조건이 만족 되는가?	추정된 시스템고 장율이 요구조건 을 만족하는가?
설계검토 약점파악	컴포넌트 고장모 드, 고장율 등	서브시스템/컴포 넌트 고장모드 고장율, 구조 등	서브시스템,컴포 넌트,신뢰도/가용 도/고장율 시스템구조	시스템/서브시스 템/컴포넌트,신뢰 도/가용도, 정비/ 수리정책 시스템구조	고장율이 가장높 은 부품 결정
설계대안개발	컴포넌트선택과 정비 등	시스템구조 중복배치, 결함 탐지, 정비 등	시스템구조 중복배치, 정비 컴포넌트선택	시스템구조 중복배치 컴포넌트선택 수리정책 시스템 재구성	가장 약한 부품 선택기준 재심의
trade-off 분석과 비용평가 수행	가장 경제적인 안을 결정	가장 경제적인 안을 결정	가장 경제적인 안을 결정	가장 경제적인 안을 결정	비용추정

2.2 기능적 구조분석

연역적 분석

연역적 방법의 요체는 원치 않는 시스템의 작동을 파악하기 위해 최 상위 레벨(시스템)에서 최 하위 레벨(서브 시스템, 컴포넌트)까지 차례로 전개해 나가는 것이다. 이 방법은 사건발생에 초점을 맞춘 방법으로 시스템의 상세한 사양이 결정되기 이전인 개념적 시스템의 설계단계에 적합하다.

모든 경우, 원치 않는 사건이나 시스템의 작동(성공)이 최 상위 사건(top event)에 와야 한다. 그 사건의 원인을 모든 레벨에서 파악하고 분석한다.

귀납적 분석

이 방법의 특징은 컴포넌트 레벨에서 결함모드를 규정하는 것이다. 각 결함모드가 다음 상위 시스템레벨의 성능에 미치는 효과를 추측한다. 이 결함의 효과가 상위 시스템의 결함모드가 되고, 다시 이 수준에서 각 결함모드의 효과를 분석한다. 이와 같이 반복하여 최 상위 시스템에 이르기까지 계속한다. 이 방법은 컴포넌트의 결함모드가 모두 밝혀져야 하므로 장비가 어느정도 성숙된 설계의 후반부에서 주로 사용된다.

2.3 정비 및 수리 분석과 고려사항

수리가능한 시스템의 장기적 가동행태는 수리/정비 정책 뿐 아니라 시스템의 정비성(maintainability)에도 많은 영향을 받는다. 정비/수리가 시스템의 의존성에 미치는 영향을 평가하는 척도로는 가용성 성능척도가 적합하다. 중복(redundant) 시스템의 경우는 시스템 작동에 영향을 주지않고 시스템을 수리할 수 있다. 그러한 경우 수리나 교체는 시스템의 신뢰도 성능과 가용도 성능을 향상 시킨다.

3. SR&QA 통합경영시스템 (AHB 5300.1)

여기서는 앞에서 소개한 각종 RAMS 활동 및 기법들을 효과적으로 적용하기 위한 안전, 신뢰성 및 품질보증 (Safety, Reliability and Quality Assurance : SR&QA) 통합경영시스템 AHB 5300.1에 대해 소개한다.

3.1 구성

이 매뉴얼은 안전, 신뢰성, 품질 면에서 고객의 기대를 충족시키기 위한 NASA의 요구사항과 국제규격인 ISO 9001의 조건을 만족하도록 작성되었으며, 적시(timely)에 효과적으로(cost-effective) 내부 및 외부 고객을 만족시킬 수 있는 방안을 제공하고 있다. 매뉴얼의 구성은 다음 그림 1과 같다.

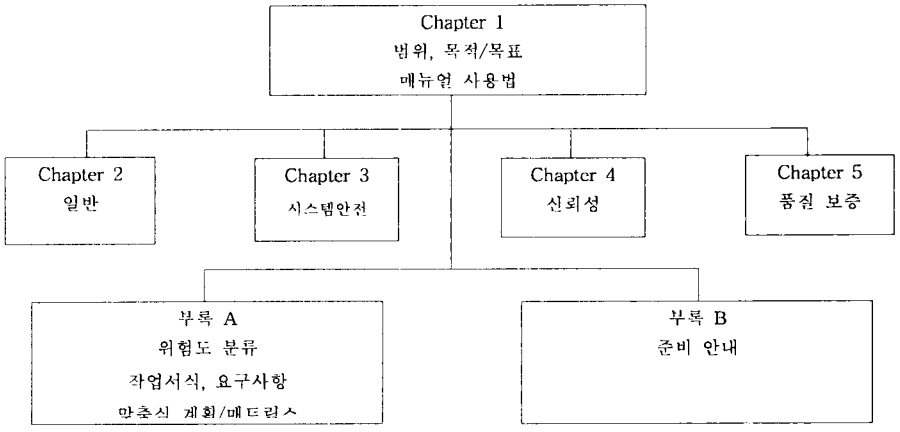

그림 1. SR&QA 경영 매뉴얼

3.2 특징

1) 위험도 분류(risk classification)

대상이 되는 장비, 프로젝트, 작업영역에 대해 그림 2와 같이 risk를 평가, 분류하여 SR&QA 요구사항들에 대해 맞춤형식으로 적용할 수 있는 표준화된 기준을 제공한다.
: Risk의 분류 : Minimal / Low / Medium / High

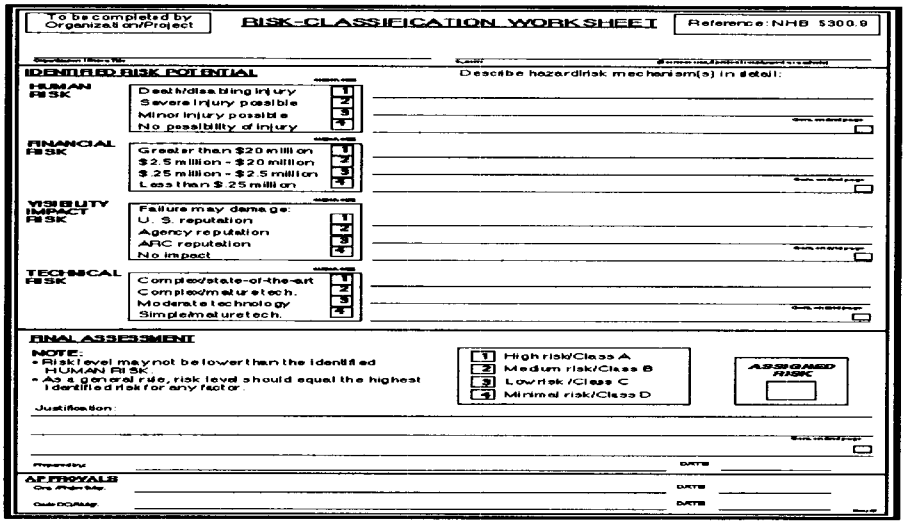

그림 2. 위험도 분류 서식

2) 맞춤형 SR&QA 경영시스템

수명주기동안의 리스크(life-cycle risk)를 최소화 하면서 고객의 요구조건을 달성할 수 있는 유연성 있는 방법을 제공한다(그림 3 참조).

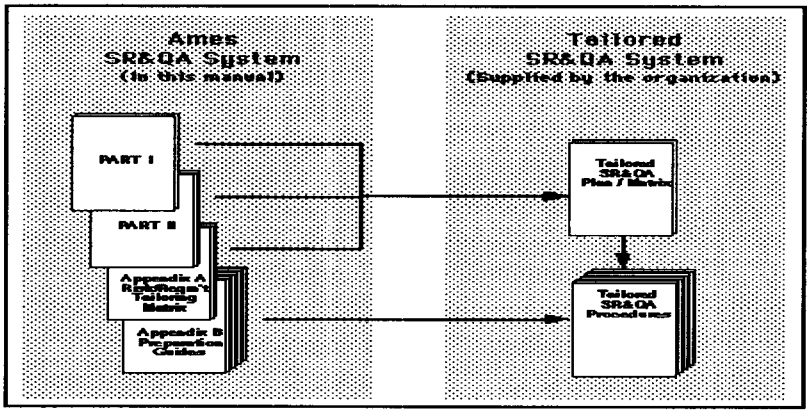

Figure 2. Tailored SR&QA system development flow.

그림 3. 맞춤형 SR&QA 시스템 개발

3.3 맞춤형 SR&QA 계획/매트릭스

앞에서 분류된 4가지 위험도(risk level)와 요구사항들(requirements)의 관계가 아래의 매트릭스에 표현된다. 각 기업은 맞춤형 SR&QA 계획을 수립하고 이들 요구사항들을 실행하기 위한 지침으로서 이 매트릭스를 사용할 수 있다. 예로서 설계심사(design review) 업무에 관한 매트릭스가 표 2에 주어져 있다.

4. 결론

통합신뢰성 분석은 시스템이나 설비의 통합신뢰성 척도(신뢰도, 가용도, 정비도, 그리고 안전성 등)를 평가하고 결정하기 위해, 시스템의 각 레벨과 세부 항목들에 대하여 주로 개념/정의 단계, 설계/개발 단계, 그리고 운용/정비 단계 동안 수행된다. 본 연구에서는 PL 시대를 맞이하여 기업이 필수적으로 갖추어야 할 제품안전 및 신뢰성 확보를 위한 각종 활동과 기법들을 소개하고 그 특징, 연관성 및 적용범위에 대해 살펴보았다. 또한 이들 기법과 연계하여 안전, 신뢰성 및 품질보증을 통합하여 경영하는 SR&QA 통합경영시스템의 구현에 대해 알아보았다. 이들 기법과 활동을 효과적으로 조합, 운영하는 통합경영시스템을 구축함으로써 제품안전/신뢰성 확보 및 고취에 의한 부품, 제품, 그리고 시스템의 경쟁력 강화라는 궁극적 목표를 달성할 수 있을 것이다.

표 2. 설계심사 맞춤형 SR&QA 계획/매트릭스

요구사항 (Requirement)	안내번호 (Guide number)	위험도(Risk Level)			
		Minimal	Low	Medium	High
Design review elements and responsibility	부록 B-1	O	R	M	M
Concept design review	부록 B-1	O	O	R	M
Preliminary design review	부록 B-1	O	R	M	M
Critical design review	부록 B-1	R	M	M	M
Integrated system review	부록 B-1	O	O	R	M
Human occupancy review	부록 B-1	M	M	M	M
Operational readiness review	부록 B-1	M	M	M	M

O - Optional (선택사항), R - Recommended (권장사항), M - Mandatory (의무사항)

[참고문헌]

[1] Ames Directives Management System (1996), System Safety, Reliability And Quality Assurance Manual AHB 5300.1, NASA

[2] International Electrotechnical Commission (1991), International Standard IEC 300-3-1 / 300-3-2.

[3] International Electrotechnical Commission (1990), IEC 50(191): International Electrotechnical Vocabulary, Chapter 191: Dependability and quality of service.

[4] International Electrotechnical Commission (1985), IEC 812: Analysis techniques for system reliability - Procedure for failure mode and effect analysis (FMEA).

[5] International Electrotechnical Commission (1990), IEC 1025: Fault tree analysis (FTA).

[6] International Electrotechnical Commission (1991), IEC 1078: Analysis techniques for dependability - Reliability block diagram method.