소프트웨어 분야의 리스크경영시스템과 신뢰성 경영시스템의 통합모델
An Integrated Model of RMS and DMS in Software Industry

김 종 걸*·김 형 만**·김 인 희**
Jong-Gurl Kim*·Hyung-Man Kim**·In-Hee Kim**

Abstract

다양한 리스크 문제가 발생하고 있는 환경 속에서 리스크에 대한 적절한 대응을 하고 안정화를 도모함과 동시에 리스크 문제가 표면화되어 초래하는 영향을 극소화 하기 위한 새로운 패러다임의 경영시스템 도입이 주요 전략과제로 대두되고 있다.

본 연구에서는 소프트웨어 분야에서의 리스크 위험 요소를 줄이고 신뢰성 향상을 목적으로 소프트웨어 분야가 가지고 있는 문제를 효과적으로 관리 할 수 있는 새로운 모델로서 IEC60300 신뢰성경영시스템과 IEC61508 리스크경영시스템의 통합 모델을 제시한다.

Keywords : 신뢰성경영시스템(Dependability Management System), 리스크경영시스템(Risk Management System), 소프트웨어 품질관리(Software Quality Control)

1. 서 론

C&C(Computer & Communication) 혁명 이후 오늘날 사회에서 소프트웨어가 차지하는 비중은 날로 높아져가고 있다. 소프트웨어의 규모나 수행능력, 용량이 날로 복잡화, 대형화되어감에 따라 고신뢰성과 고품질의 소프트웨어를 개발하기 위한 체계적이고 합리적인 소프트웨어개발시스템 구축이 어느 때보다 절실히 요구되고 있다[3]. 이에 따라 "소프트웨어 공학"이라는 학문이 점점 활성화되어가고 있으며, 소프트웨어 품질에 관한 전반적인 관심도 한층 부각되어지고 있다. 이러한 소프트웨어 품질에 대한 체계의 확립과 방법론에 대한 관심은 앞으로도 더욱 높아지리라 예상된다[3].

* 성균관대학교 시스템경영공학과
** 성균관대학교 산업공학과
*** 성균관대학교 산업공학과

국내 실정에 적합한 품질에 관련된 소프트웨어 기초 이론 분야가 보다 발전하기 위해서는 우리 설정에 맞는 소프트웨어 품질평가 방법론과 자동화 도구 개발의 기초 연구가 선행되어야 한다. 그러나 국내에서는 소프트웨어 품질 평가 방법론과 도구의 필요성을 충분히 인식하면서도 실질적인 연구가 활발히 진행되지 못한 실정이며, 현재의 연구 현황은 많은 문제점과 과제를 안고 있는 것이 사실이다[3]. IT융합의 진전으로 소프트웨어 결함으로 인한 열차, 선박, 항공기, 의료장비 등의 사고 발생우려, 석유화학 공장, 철도 자동차, 항공분야 등 고도의 소프트웨어기능 안전성이 필요한 분야 및 하드웨어 분야와 달리 소프트분야는 신뢰성이 정량적 확보 방안이 아직 초보 단계의 문제점들이 그 예이다.

2. 소프트웨어 기술 현황

2.1 소프트웨어 정의

IEC 61508에 의하면 소프트웨어는 프로그램, 절차, 데이터 또는 규칙과 어떤 관련된 문서와 이에 부속되는 시스템을 운영상의 데이터로 구성되는 지각적 창조물로 정의하였다.

한편, Pressman에 의하면 소프트웨어는 원하는 기능을 수행하는 컴퓨터 프로그램과 프로그램이 설계, 이용, 개발, 추진, 보수하는데 필요한 문서 체계라고 정의하였다[1].

이와 같이 소프트웨어는 “실행할 때 원하는 기능과 성능을 제공해 주는 명령어, 프로그램이 정보를 알맞게 조작하도록 해주는 자료구조, 프로그램의 연산과 사용을 설명해주는 문서” 라는 차원에서 정의되어진다.

소프트웨어를 이해하기 위해서는 사람들이 다른 분야에서 구축했던 것과 다르게 만들어진 소프트웨어 특성 등을 조사해보는 것이 중요하다. 하드웨어를 구축할 때, 인간의 창조적 과정(분석, 설계, 구축, 검사)이 최종에는 물리적인 형태로 변환된다. 만약에 우리가 새로운 컴퓨터를 구축하려면 초기에 윤곽을 그리고, 공식적인 설계도를 작성하고, 일반적인 원형을 물리적인 제품(VLSI 칩, 회로판, 전력공급 등)으로 발전시켜 나간다.

소프트웨어는 물리적인 시스템 요소라기보다는 논리적인 요소이다. 그러므로 소프트웨어는 하드웨어의 특성에 비해 상당이 다른 특성들을 갖고 있다[3].

2.2 소프트웨어 기술 평가

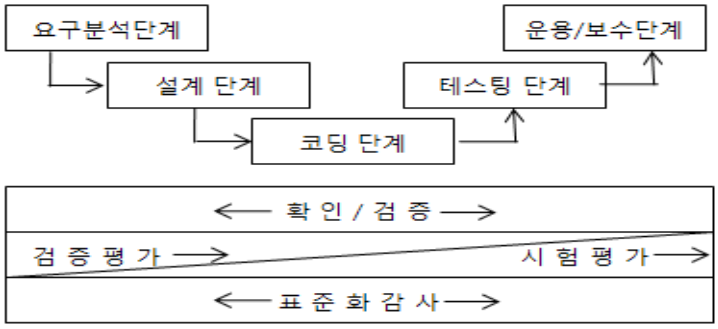
소프트웨어 생명주기의 첫 단계인 요구분석 단계에서부터 마지막 단계인 유지 보수 단계까지의 총비용중 유지보수의 비용은 전체 비용의 약 80%에 이르고 있음을 많은 연구보고서에서 지적해 왔으며, 또한 유지보수 비용을 절감하기 위한 많은 개발 방법론이 연구되어 오고 있다[3].

이러한 유지보수 비용을 절감하기 위해서는 무엇보다도 신뢰성 있는 소프트웨어를 개발하는 것이 중요하며, 이러한 신뢰성 있는 소프트웨어를 개발하기 위한 방법론으로

프로그램 테스팅, 품질평가, 구조적 설계, 객체지향 설계 등 다양한 방법론들이 연구되어져 오고 있다. 이중 소프트웨어 품질평가는 소프트웨어 개발 종료 후, 개발과정에서 생성된 생산물과 최종 생산물인 소프트웨어를 평가함으로써 생명주기 전 과정에서 발생된 오류를 검출할 수 있고, 이를 바탕으로 소프트웨어가 실제 요구자의 요구를 어느 정도 충족시키고 있는지를 평가함으로써 소프트웨어의 신뢰성을 평가하는 평가 방법론이다.

본 연구에서는 평가 기법을 크게 확인/검증과 표준화 감사로 구분하였다. 확인/검증의 주된 관점은 요구사항의 적합성을 입증하기 위한 것이고, 표준화 감사는 개발에 관련된 제반 표준 및 지침에 대한 적합 여부를 판정하기 위한 것이다[3]. 확인이란 어느 단계의 개발 제품이 최초의 사용자 요구 또는 소프트웨어 요구에 적합한지를 입증하기 위한 활동을 의미하며, 검증은 어느 단계의 개발 제품이 이전 단계서 설정된 개발 규격을 충족시키는지의 여부를 판단하기 위한 활동이다[3].

확인/검증은 다시 검증평가와 시험평가로 분류할 수 있다. 검증평가는 요구사항의 정의나 설계와 같이 초기 단계에서 작성되는 개발 규격서의 충분성 평가를 위주로 해왔으며, 시험평가에서는 프로그램자체를 대상으로 하여, 구체적인 시험 사례를 입력한 그 결과를 분석하는 평가 기법이다[3]. 이와 같은 평가기법을 수명주기에 적용시켜 보면 [그림-1]과 같다.



[그림-1] 소프트웨어 품질 평가 기법의 적용 관계[3]

3. 경영시스템 고찰

3.1 신뢰성 경영시스템 (IEC 60300)

IEC 60300의 국제 규격은 신뢰성 경영시스템의 규격으로서 구성은 아래 [표-1]과 같이 되어있다[7][8][9].

[표-1] IEC 60300의 구성

구 성	내 용
300-1(2003)	제1부 : 신뢰성 경영시스템 (Dependability management systems)
300-2(2003)	제2부 : 신뢰성 경영지침 (Guidelines for dependability management)
300-3	제3부 : 응용지침 표준 (Application guide)
300-3-1(2003)	신뢰성 분석기법 (Analysis techniques for dependability)
300-3-2(2004)	신뢰성 현장자료의 수집 (Collection of dependability data from the field)
300-3-3(2004)	수명주기 비용 (Life cycle costing)
300-3-4(2007)	신뢰성 요구사항 명세화 (Guide to the specification of dependability requirements)
300-3-5(2001)	신뢰성 시험조건과 통계적 시험원리 (Reliability test conditions and statistical test principles)
300-3-6(2009)	소프트웨어의 신뢰성 방향 (Software aspects of dependability)
300-3-7(2009)	전자장치의 신뢰성 스트레스 스크리닝 (Reliability stress screening of electronic hardware)
300-3-9(1995)	기술적 시스템의 리스크분석 (Risk analysis of technological systems)
300-3-10(2001)	보전성 (Maintainability)
300-3-11(1999)	신뢰성기반 보전 (Reliability centered maintenance)
300-3-12(2001)	통합병참지원 (Integrated logistics support)
300-3-14(2004)	보전과 보전지원 (Maintenance and maintenance support)
300-3-15(2009)	시스템 신뢰성 공학 (Guidance to engineering of system dependability)
300-3-16(2008)	보전지원 서비스의 명세화 (guidelines for specification of maintenance support services)

제 1부는 경영시스템의 전반적인 내용을 다루고, 제 2부는 신뢰성 경영시스템의 요소와 업무별 지침으로서 인증 시 요구사항의 역할을 수행하며, 제3부는 각 요소와 업무에 필요한 응용지침들을 설명하고 있다.

본 국제표준은 대부분의 조직이나 프로젝트 요구를 충족시키는 신뢰성 경영시스템을 구성하는데 일반적인 지침을 제공한다. 신뢰성 표준의 구조는 “tool box"의 개념을 따른다[4]. IEC 60300-1은 적용지침과 방법에 기준을 제시하는 IEC 60300-2에 의해 지원된다[4]. IEC 60300 표준의 특징으로는 신뢰성 활동의 구체화를 촉진하기 위해 ISO 9001:2000 품질경영시스템(QMS) 구조와 방향을 같이한다[4]. 따라서 요구사항에 해당하는 IEC 60300의 요구사항은 ISO 9001의 요구사항과 제목이 정확히 일치하진 않지만 그 구성은 일치한다[4]. 이는 신뢰성 수준으로 제품 신뢰도, 보전도, 보전지원성 등의 달성을 위해 품질경영시스템(QMS)를 보완하고 있음을 나타낸다[4]. [표-2]는 60300-1의 구성을 나타낸다.

[표-2] 60300-1의 구성

조항	세부조항
1. 범위	1.1 일반사항 1.2 적용
2. 인용규격	
3. 용어 및 정의	
4. 시간종속성 경영시스템	4.1 일반 요구사항 4.2 문서화 요구사항
5. 경영책임	5.1 시간종속성 경영 기능 및 의지
	5.2 고객중심 시간종속성
	5.3 시간종속성 방침
	5.4 시간종속성 기획
	5.5 책임, 권한 및 의사소통
	5.6 경영검토
6. 자원관리	6.1 자원확보
	6.2 인적자원
	6.3 기반구조
	6.4 업무환경
7. 제품실현	7.1 제품 실현 기획
	7.2 고객 관련 프로세스
	7.3 설계 및 개발
	7.4 구매 및 계약
	7.5 생산 및 서비스 제공
	7.6 모니터링 장치 및 측정장치의 관리
8. 측정, 분석 및 개선	8.1 일반사항
	8.2 모니터링 및 측정
	8.3 부적합제품의 관리
	8.4 데이터 분석
	8.5 개선

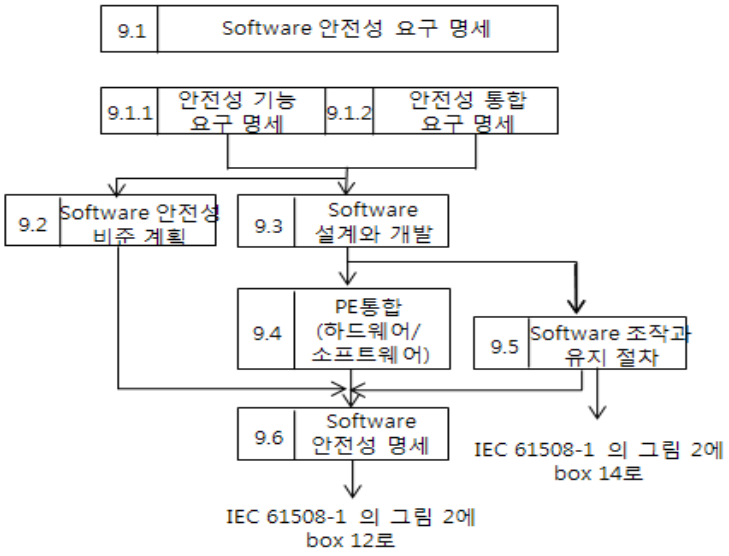
3.2 리스크 경영시스템 (IEC 61508)

이 국제표준은 전기, 전자, 프로그램화 할 수 있는 전자제품(E/E/PES)으로 구성된 시스템이 안전기능을 수행하기 위한 모든 안전 수명주기 활동을 위한 일반적 접근방법을 강조한다. 이 통합화된 접근은 전자에 기반을 둔 안전에 관련된 모든 시스템이 개발되기 위해 채택되어 지고 있다. 주된 목적은 표준 적용의 활성화를 수행하는 것이다. [표-3]는 전체적인 구성을 보여준다.

[표-3]. 국제적인 표준[5]

구 분	개 념
61508-1	- 1998, E/E/PE안전관련 시스템의 기능적 안전성 - PART1 : 일반적 요구사항
61508-2	- 2000, E/E/PES안전관련 시스템의 기능적 안전성 - PART2 : 전기/전자/프로그램 할 수 있는 전자 시스템의 요구사항들
61508-3	- 1998, E/E/PES안전관련 시스템의 기능적 안전성 - PART3 : 소프트웨어 요구사항들
61508-4	- 1998, E/E/PES안전관련 시스템의 기능적 안전성 - PART4 : 정의와 약어
61508-5	- 1998, E/E/PES안전관련 시스템의 기능적 안전성 - PART5:안전도 수준의 정의를 위한 방법의 예시들
61508-6	- 2000, E/E/PES안전관련 시스템의 기능적 안전성 - PART6 : PART2와 3의 적용에대한 가이드라인
61508-7	- 2000, E/E/PES안전관련 시스템의 기능적 안전성 - PART7 : 기법과 척도에 대한 개관

전체 리스크 경영시스템 가운데 중간 시스템으로써 IEC 61508에서 다루는 소프트웨어 수명주기는 다음과 같다.



[그림-2] 소프트웨어 안전 수명주기[6]

IEC61508-3의 국제 규격은 소프트웨어 요구사항으로 구성은 아래 [표-4]와 같이 되어있다.

[표-4]. 61508-3의 구성[6]

조 항	세 부 조 항
1. 범위	
2. 표준을 정하는 참고문	
3. 정의와 생략	
4. 표준에의 순응	
5. 문서화	5.1 목적 5.2 요구사항
6. 소프트웨어 품질경영 시스템	6.1 목표 6.2 요구사항
7. 소프트웨어 안전 수명주기 요구사항	7.1 개요
	7.2 소프트웨어 안전도 요구사항 설명
	7.3 소프트웨어 안전 검정 계획
	7.4 소프트웨어 설계 및 개발
	7.5 프로그램 할 수 있는 전자부품의 통합
	7.6 소프트웨어 운영과 절차 수정
	7.7 소프트웨어 안전 검증
	7.8 소프트웨어 수정
	7.9 소프트웨어 검사
8. 기능적 안전성 평가	8.1 목적 8.2 요구사항

4. 통합경영시스템 모델

4.1 통합시스템의 일반적인 고려사항

통합경영시스템을 구축하기 위해 일반적인 연구논문에서 제시하는 장점과 단점은 고려해야 할 사항은 다음과 같다[10].

1) 장점

- 경영시스템 표준과 요구사항의 간결화
- 심사와 등록비의 절감
- 심사의 원스톱 접근
- 조직 스스로 선호하는 개선 단위 선택
- 표준의 실행에서 발생되는 비용 감소
- 경영시스템 문서의 조화
- 기능적으로 다른 분야에서 목표, 프로세스, 자원 등의 조율

- 중소기업은 통합적 접근으로 이익창출의 효과가 큼
- 문서작업의 감소
- 다른 시스템들이 통합 시 시너지의 효과 발생
- 중복된 시간, 노력, 비용의 절감
- 시스템의 효율, 효과적인 개선

2) 고려사항

- 통합 시 기업에서 발생되는 이익
- 시스템이 통합되어도 감사의 내·외부 수행 여부
- 잘못된 정보로 인한 중간 의사결정자들의 혼란
- 관리자와 작업자 사이의 충분한 의사소통 여부
- 기존의 경영시스템 구축 실패사례에 대한 걱정
- 통합경영의 실행에 대한 내·외부 타당성 부족
- 근본적 지향점이 다름
- 통합적 전문 인력 양성과 확보에 대한 어려움

4.2 통합시스템의 요구사항

통합경영시스템이란 모든 서브시스템과 경영요소를 포함하는 하나의 포괄적 시스템을 말한다[2]. 이 두 규격의 통합에 있어서 가장 중요하게 고려해야 할 부분은 규격구성의 차이에 따르는 통합적 모델과 가장 합리적이고 효율적인 평가측정을 통한 자원배분이라고 할 수 있다[2]. 즉 조직내의 상호 모순될 수도 있는 각종 목표와 관련된 서브시스템과 구성요소들이 경영의 기본목적 하에서 유기적으로 결합하고 그에 따라 외부의 환경 변화에 능동적으로 대처할 수 있으며 나아가 조직의 지속적 발전을 도모하는 시스템이다[2].

소프트웨어 리스크 및 신뢰성에 공통적으로 적용 가능한 점을 도출하고, 불필요한 중복이나 모순이 있는 부분을 제외 하여야 한다[2]. 또한 IEC61508 과 IEC60300의 공통감사 규격이 확립되어야 한다. 즉 통합경영시스템을 효과적으로 이루기 위해서는 첫째 각 규격의 공통적인 요구사항을 정리, 파악하고, 둘째 공통적으로 요구되는 사항에 대한 통합문서화를 제시하는 등 통합에 대비한 구성체제를 갖추는 것이 중요하다[2].

특히 통합시스템은 장기적인 관점에서 소프트웨어 프로그램의 안전성을 위해 단계적인 통합전략을 세워 추진하는 것이 중요하며, 통합은 단순한 조직이나 업무 기능의 축소가 아니라 시스템 능력을 높이는 것이다.

통합경영시스템은 신뢰성경영시스템 60300-1을 기반으로 소프트분야의 리스크경영시스템 61508-3을 통합한 것으로서 통합경영시스템 구축을 위한 측정항목은 [표-5]과 같다.

[표-5] 통합경영시스템

조항	세부조항
1. 범위	1.1 일반사항 1.2 적용
2. 인용규격	
3. 용어 및 정의	
4. 통합 경영시스템	4.1 일반 요구사항 4.2 문서화 요구사항
5. 경영책임	5.1 경영기능
	5.2 요구 충족
	5.3 방침
	5.4 기획
	5.5 책임, 권한 및 의사소통
	5.6 경영검토
6. 자원관리	6.1 자원확보
	6.2 인적자원
	6.3 기반구조
	6.4 업무환경
7. 제품실현	7.1 안전도 요구사항 설명
	7.2 안전 검정 계획
	7.3 고객 관련 프로세스
	7.4 설계 및 개발
	7.5 운영과 절차수정
	7.6 생산 및 서비스 제공
	7.7 모니터링 장치 및 측정장치의 관리
8. 측정, 분석 및 개선	8.1 일반사항
	8.2 모니터링 및 측정
	8.3 안전검증
	8.4 수정
	8.5 검사
	8.6 부적합제품의 관리
	8.7 데이터 분석
	8.8 개선

5. 결론

본 논문에서는 리스크관리 부재 시 대형사고가 수반될 수 있는 소프트웨어 분야의 전략 중 하나인 리스크경영시스템과 신뢰성, 보전성 및 가용성을 기반으로 한 신뢰성 경영시스템 통합에 대한 기초자료를 제시하기 위해 리스크경영시스템인 IEC 61508과 신뢰성경영시스템 IEC60300을 분석하였다. 리스크경영시스템인 IEC61508 요구사항, 신뢰성경영시스템인 IEC60300 요구사항을 기반으로 통합경영시스템을 수립하였다. 신뢰성 경영은 고장률을 최소화하고 리스크경영은 기대손실을 최소화하를 목적으로 하기 때문에 항목의 범위가 다를 수 있으나 통합된 기준항목을 개발 할 수 있다. 본 연구에서 리스크경영시스템과 신뢰성경영시스템 통합을 위한 요구사항을 분석하였지만 통합경영시스템 도입 방법에 대한 대안과 시간, 비용 등의 자원을 고려하여 단계적으로 구

축하는 자원배분 방법이 필요하며, 이것을 차후 연구과제로 제안한다.

이 자료를 토대로 한국의 소프트웨어 분야의 안전수준이 세계수준으로 발전하고, 국가 경쟁력을 강화하기 위해서는 향후 소프트웨어 분야에서의 리스크관리와 신뢰성관리의 통합연구가 계속 지속되어야 할 것이다.

6. 참 고 문 헌

[1] 권오탁, " 소프트웨어 품질관리를 위한 품질평가 기술", The Journal of Information Systems Review, pp.1-16, 1994

[2] 김종걸, 김창수, "품질경영시스템과 리스크경영시스템의 통합" 대한산업공학회/한국경영과학회 2002년도 춘계공동학술대회, pp.817-824, 2002

[3] 김종걸, 소프트웨어 품질관리, 성균관대학교, 2007

[4] 김종걸, 고재규, 김창수, "신뢰성경영시스템(IEC 60300)의 효과적 도입 방안에 관한 연구" 대한안전경영과학회 2009년도 춘계학술대회, pp.153-165, 2009

[5] IEC, IEC 61508-1, General Requirements, 1998

[6] IEC, IEC 61508-3, Software Requirements, 1998

[7] IEC/TC 56, IEC 60300-1 ; Dependability management system, 2003

[8] IEC/TC 56, IEC 60300-2 ; Guidelines for dependability management, 2003

[9] IEC/TC 56, IEC 60300-3 ; Application Guide, 2003

[10] S. V. Karapetrovic, W. O. Willborn, "Integration of management systems: focus on safety in the nuclear industry", International Journal of Quality & Reliability Management, Vol. 20, No. 2, pp. 210~228, 2003

저 자 소 개

김 종 걸
서울대학교 계산통계학에서 석사
한국과학기술원 산업공학과에서 박사학위
현재 한국품질보증/PL 연구회 회장으로 활동
성균관대학교 시스템경영공학과 교수로 재직
주 소 : 경기도 수원시 장안구 천천동 300번지 성균관대학교 시스템경영공학과 27416호실

김 형 만
상지대학교 산업공학과를 졸업, 성균관대학교 산업공학과 석사, 성균관대학교 산업공학과 박사수료, 현 에틱스아카데미 e-Learning 강사로 활동, 상지대학교 시스템경영공학과 외래교수 관심분야: 신뢰성공학, 품질공학, TRIZ, 제품개발
주 소 : 경기도 수원시 장안구 천천동 300번지 성균관대학교 시스템경영공학과 26418B호실

김 인 희
남서울대학교 산업공학과를 졸업
현 성균관대학교 산업공학과 석사재학
관심분야: 신뢰성공학, 품질공학, 소프트웨어 품질관리, 리스크 경영공학, SPC
주 소 : 경기도 수원시 장안구 천천동 300번지 성균관대학교 시스템경영공학과 26418B호실