J. Korea Saf. Manag. Sci. Vol. 17 No. 2 June 2015
http://dx.doi.org/10.12812/ksms.2015.17.2.97

ISSN 1229-6783(Print)
ISSN 2288-1484(Online)

린 6시그마 DMADOV를 이용한 시스템 안전설계 표준지침 및 프로세스 구축

김 형 관* · 박 도 현* · 허 형 조* · 성 원 혁*
*삼성탈레스

Development of Standard Guideline and Process for Safety Design using DMADOV of the Lean 6 Sigma.

Hyung-Kwan Kim* · Do-Hyun Park* · Hyoung-Jo Huh* · Won-Hyuk Sung*
*SamsungThales

Abstract

System is the organization of hardware, software, personnel and facilities needed to perform a designated function within a stated environment with specified results. The trend of modern systems is getting more complex and larger. The system is necessary for modern society but the minor malfunction of the system can result the enormous human and material losses. Recently it is being heightened the concern for system safety and required to be built and applied Safety Engineering standard Guideline for safety of complex and large-sized system. This paper describes the System Engineering Process model integrated with Safety Engineering and the establishment of standard safety guidelines for safety of product development using DMADOV Methodology of the Lean 6 Sigma.
Keywords : Safety Engineering, Safety Process, Safety Standard Guideline, Lean 6 Sigma, DMADOV

1. 서 론

안전(Safety)이란 사망, 부상, 직업병, 손상을 유발하거나 장비 및 재산에 대한 손실 또는 환경피해를 일으킬 수 있는 우려가 없는 상태 또는 조건을 의미한다. 현대 안전공학 사고이론 중 하나인 '도미노' 이론의 창시자인 하인리히(H. W. Heinrich)는 "사고나 재난은 발생 전에 여러 가지 징후가 나타나므로 이에 대한 분석과 준비를 통해 미리 예방할 수 있다" 고 주장하였고, 밥 휘렌츠(Bob Firenze)는 사고를 사람, 기계 및 환경이란 시스템 속에서 일어난 현상으로 보았으며 인간이 기계와 환경에 조화되어야 효율적이라고 보았다. 즉, 기계의 설계가 불량하거나 불안전할 때 사고의 원인이 될 수 있고 환경은 인간과 기계에 영향을 주어 사고를 조장하거나 유발한다고 보았다[1][2].

특히 특정 기능을 수행하기 위한 복합체인 시스템에 있어서는 이러한 안전성의 확보는 매우 중요한 문제이다. 현대의 시스템은 사회의 다양한 분야에서 사용되고 있으며 전자 및 정보기술 분야의 비약적인 발전으로 인하여 기존의 아날로그 시스템에 비하여 하드웨어뿐 아니라 소프트웨어적으로도 더욱 복잡한 제어 기능을 수행하고 대형 시스템화가 되어가는 추세이다. 시스템이 복잡화 및 대형화됨에 따라 고장의 예측이 어려워졌으며, 사소한 고장이나 오작동이 대형 사고를 유발할 수 있다는 점에서 시스템의 신뢰성 및 안전성확보 문제가 대두되고 있다. 국가기반시스템, 산업제어시스템, 군사무기체계 등은 고장이 발생할 경우 사회 · 경제적으로 큰 문제를 야기할 수 있는 안전성이 매우 중요한

†Corresponding Author : Hyung-Kwan Kim, Naval/System R&D Center, Samsung Thales. 244 1gongdan-ro, Gumi-City, Gyeongsangbuk-Do 730-904 e-mail: 525v@daum.net
Received October 27, 2015; Revision Received May 07, 2015; Accepted June 14, 2015.

시스템(Safety-Critical System)이다. 이러한 시스템들의 사소한 오류는 천문학적인 경제적 손실과 인명피해를 발생시킬 수 있다[3].

해외 선진업체에서는 이러한 시스템의 안전성을 확보하기 위해서 안전공학에 의거하여 안전설계 기준 및 체계를 구축하고 시스템 설계 초기단계에서부터 적용하고 있으나, 국내 업체의 경우에는 안전에 관한 요구를 설계과정에 반영하기 위한 프로세스 즉, 기준 및 관리체계의 부재로 인하여 개발자의 업무 숙련도에 따라서 시스템 안전성이 좌우되고 있는 실정이다. 이러한 문제점을 해결하기 위해서는 시스템 개발 절차에 체계적으로 적용할 수 있는 시스템 안전 기준체계 구축이 필요하다고 할 수 있겠다.

시스템 요구사항 분석 단계에서부터 설계, 구현, 검증 단계까지 전반적인 체계공학(SE, System Engineering) 프로세스에서의 시스템 안전방법을 사용하여 위험 식별 및 경감이 될 수 있도록 시스템 안전 프로세스 확립과 함께 안전공학을 기반으로 한 각 개발 단계에 따른 세부 위험 분석, 위험 평가 및 관리를 수행하는데 있어서 필요한 작업 및 활동에 대한 안전설계 표준지침이 구축되어야 시스템의 신뢰성 및 안정성을 확보할 수 있을 것이다.

본 논문에서는 S사의 린 6시그마 경영혁신 과제를 통해 연구개발 특성에 맞는 안전설계 요건을 도출하고 체계공학 고유의 특성화된 안전설계 표준지침 및 프로세스를 구축하였다.

이를 위해 본 연구는 기업 경영혁신 방법론인 린 6시그마 기법을 기반으로 DMADOV 프로세스에 맞게 구조화시켜 과제 형태로 진행하였다.

2. 이론적 고찰

2.1 린 6시그마 정의

6시그마는 고객관점에서 프로세스의 품질을 향상시키기 위하여 통계적 사고와 과학적 기법들을 사용하여 불량을 제거해 나가는 체계적인 방법과 인프라 체계를 강점으로 하여 이미 많은 기업들이 도입하여 적용을 하고 있다. 린(Lean)은 낭비제거를 통하여 가치흐름을 원활하게 하고 프로세스의 효율을 증가시킴으로써 스피드경영을 가속화하기 위한 방식이다. 린 6시그마는 린 방식과 6시그마의 결합을 통하여 고객만족, 비용, 품질, 공정속도, 자본회수 등에 개선을 가장 빠른 속도로 달성함으로써 기업의 가치를 극대화 해주는 방법론으로 낭비나 비 부가가치 업무를 제거하거나 업무 프로세스를 개선하는 과제를 대상으로 적용하면 효과적이라 할 수 있다[4] [5].

2.2 린 6시그마 추진단계

6시그마의 전형적인 방법론(Methodology)인 DMAIC (Define, Measure, Analyze, Improve, Control)는 5단계로 구성되며 이미 존재하는 제품의 개선과 같은 문제를 해결하는 프로세스이다. 그러나 6시그마가 사무간접부문과 연구개발 부문에 활성화되기 시작하면서 이미 발생된 문제를 해결하는 것뿐만 아니라 신규업무를 추진하는데 있어서 제품의 기능과 성능 또는 프로세스에 향후 발생할 문제까지도 사전에 해결할 수 있는 새로운 방법론인 DFSS(Design For Six Sigma)가 등장하였다. 신제품과 프로세스 개발 시 최적화를 위해 가장 보편적으로 활용하는 대표적 DFSS 프로세스로는 GE에서 개발한 DMADV(Define, Measure, Analyze, Design, Verify)와 IDOV(Identify, Design, Optimize, Validate)가 있으며 과제 특성에 따라 추진단계(phase)를 서로 적절히 혼용하여 사용한다[6].

6시그마 적용 초기에는 개발을 위한 추진방법론으로서의 DMADV에서 실질적인 설계(Design) 단계의 절차가 구체적으로 제시되지 못하여 성과 예측 및 리스크에 대한 확인 등에서 많은 문제가 발생할 수 있음을 추진과제에서 실행자들의 고객들로부터 취합이 되었고, 이를 강화하고자 설계(Design) 단계를 거친 후 최적화(Optimize) 단계를 추가하여 전체 최적화, 강건 설계 개념을 확인하는 과정이 명문화되어 개발과제의 6시그마 방법론으로 사용되고 있다.

따라서 시스템 안전설계 표준지침 및 프로세스를 개발하는 본 연구에서는 설계(Design) 단계를 거친 후 전체성과에 대한 검토, 과제 추진의 리스크를 상세히 검증함으로써 과제 성공률을 올릴 수 있는 DMADOV(Define, Measure, Analyze, Design, Optimize, Verify) 프로세스를 사용하고자 한다. <Table 1>은 DMADOV 프로세스의 단계별 추진항목을 나타내며 3장에서 세부적으로 정의한다.

<Table 1> Action items of each DMADOV phase

Phase	Action Items	Chapter
Define	Projects selected/defined /approved	3.1
Measure	CTQ deployment and Y's current level check and goal set	
Analyze	System design Design elements identification /analysis Preliminary design	3.2
Design	Critical design	3.3
Optimize	Critical design optimization Critical design assessment	
Verify	Pilot verification Management planning/ implementation Documentation/transfer	3.4

3. DMADOV 를 이용한 안전설계 표준지침 개발

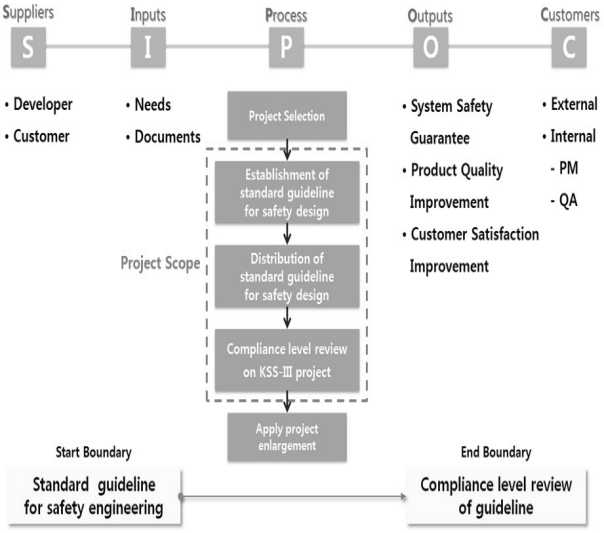
3.1 과제 정의 및 현수준 파악

본 과제에서는 안전공학을 반영한 체계적인 안전설계 적용 절차 및 지침을 확보하고 이를 시스템 설계에 적용함으로써 안전사고 발생요인을 사전에 제거하여 인적/물적 피해를 최소화하는 것에 목적이 있다. 린 6 시그마에서 CTQ(Critical To Quality)란 고객의 요구사항을 대변하는 성과척도로서 프로젝트 목표가 달성될 수 있는 핵심 품질항목이 된다. 시스템 안정성 확보를 위하여 VOC(Voice of Customer)/VOB(Voice of Business)/VOP(Voice of Process) 분석을 통해 다음과 같은 세 가지 잠재 CTQ를 도출하였다.

1) 시스템설계분야 안전설계 표준지침 수립 및 적용
2) 안전설계 지침 적용을 통한 제품 경쟁력 강화
3) 새로운 방식의 개발절차 및 적용

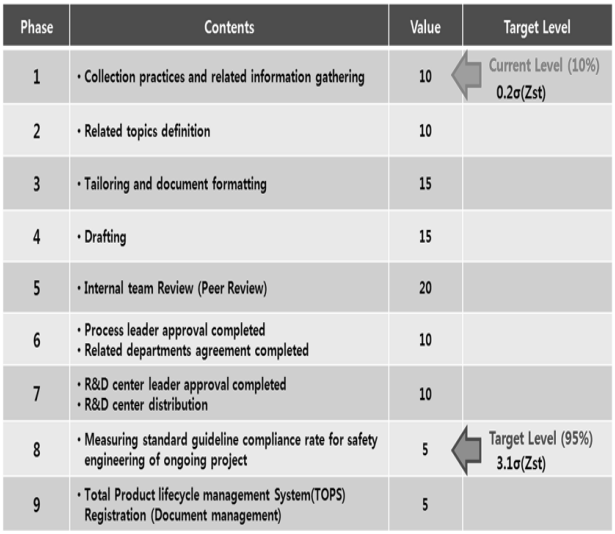
그리고 위의 세 가지 잠재 CTQ를 종합하여 프로젝트 CTQ로 “안전설계 표준지침 수립 및 적용을 통한 시스템 안전성 향상” 을 설정하였다.

과제 목표 달성을 위해 체계공학/소프트웨어/하드웨어의 3가지 분야별 Sub 프로젝트를 추진하였으며 안전설계 표준지침 개발에 있어서 위험요소에 대한 안전공학 적용방안을 수립하고, 시스템 개발 초기에 잠재적인 유해성을 식별하기 위한 분야별 안전설계 체크리스트를 포함하는 것을 목표로 하였다. 상위프로세스맵(SIPOC)을 이용한 프로젝트의 범위 설정은 [Figure 1]과 같이 안전설계 표준지침 수립부터 진행 중인 시스템개발 과제의 산출물에 대한 안전설계 표준지침 준수수준 검토까지로 정의하였다.



[Figure 1] Process configuration using SIPOC

프로젝트의 CTQ인 안전설계 표준지침 수립 및 적용을 통한 시스템 안전성 향상을 대변하는 성과지표 Y's로서 “지침수립단계” 를 도출하였다. 여기서 지침수립단계는 안전설계 표준지침 수립에 있어서 사내 품질표준 문서 수립절차에 따라 진행단계를 세분화하였고, 최종 성과기준은 사내 그룹웨어상의 전자결재 합의 및 승인 상태를 확인하는 것으로 데이터의 신뢰성을 확보하였다. [Figure 2]는 현수준 파악 및 목표수준 설정을 위해 지침수립을 단계별로 구분하고 시스템전문가 회의를 통하여 중요도를 고려한 가중치를 적용하는 것을 나타낸다. 이때, 현 수준은 사례수집 및 관련 내용 수집 단계로서 공정능력분석(Process Capability Analysis) 값이 0.2σ(Zst)로 측정되었으며, 목표수준은 작성된 안전설계 지침서를 기준으로 진행 개발 과제의 안전설계 준수 평가를 통한 검증단계로서 3.1σ(Zst)가 되도록 설정하였다.



[Figure 2] Identification of the current level and the target level set

3.2 설계안 도출 및 기본설계

본 연구에서는 안전설계 표준지침 수립을 위해체계공학, 소프트웨어, 하드웨어의 각 분야별로 안전공학 세부 적용방안을 제시하였으며 분야별 설계 방안은 <Table 2>와 같다.

<Table 2> Sectoral Design Methodology

Sector	Design Methodology
System Engineering (SE)	Safety requirements derivation Safety design procedures and methods Establish action plans in accordance with safety procedures Hardware/Software integration
Software (S/W)	Software safety regulatory requirements derivation Software risk identification and assessment
Hardware (H/W)	Hardware safety regulatory requirements derivation Hardware safety design for components

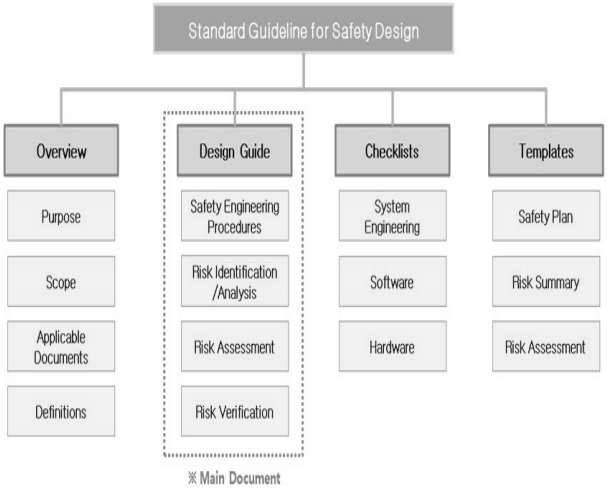
설계안 도출을 위해 당사 과거 수행사업 및 현재 진행중인 시스템 개발 과제에 대해 개발 사양서 및 체계공학 관리계획서를 기준으로 안전관련 요구사항을 분석하였다. 분석결과로부터 체계 설계 및 제작에 관하여 설계 안전검토, 안전기준, 위험수준, 안전분석, 인지된 위험에 대한 조치 및 안전시험을 이행하여야 하며, 이를 위해 체계안전계획을 수립하여 위험관리를 하도록 요구함을 알 수 있었다. 위와 같은 안전체계 수립과 이행에 관한 요건을 규정한 표준지침으로는 <Table 3>과 같으며, 본 과제의 안전설계 지침서 작성에 분야별로 참고하였다.

<Table 3> Features of system safety management standards and Applications

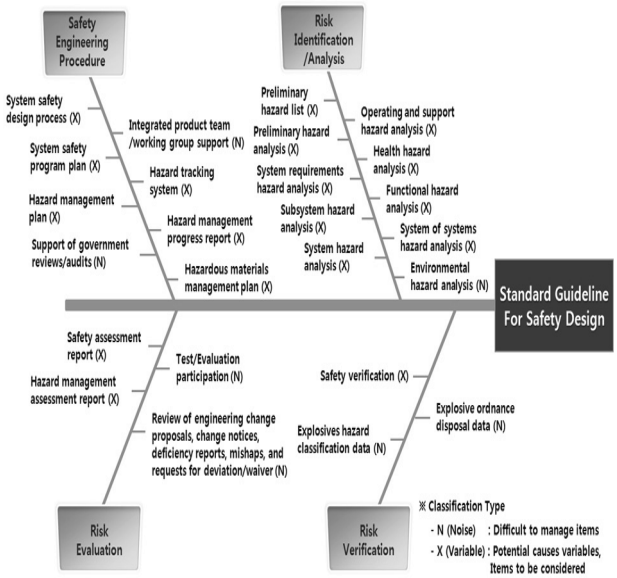
Standard	Contents	Applications
MIL-STD-882D/E	Identifies the Department of Defense(DoD) Systems Engineering(SE) approach to eliminating hazards, and minimizing risks	SE
FAA System Safety Handbook	Provides instructions on how to perform system safety engineering and management	SE
NASA/SP-2010-580 NASA-STD-8719.13A	Provides requirements to implement a systematic approach to software safety and software assurance processes	S/W
JSSSC Software System Safety Handbook	Provides management and engineering guidelines to achieve a reasonable level of assurance that software will execute within the system context with an acceptable level of safety risk	S/W
MIL-HDBK-454B	Provides General Guidelines for electronic equipment	H/W
MIL-STD-1576	Electro-explosive subsystem safety requirements and test methods for space systems	H/W

본 연구에서는 제품 설계 및 제작에 관한 안전공학 설계 요구를 충족시키기 위해 시스템안전 절차 및 관리기법으로 MIL-STD-882E를 적용하였다. MIL-STD-882E는 2012년에 개정된 미국방부 시스템 안전표준으로서 기본적인 시스템 안전관리 기법과 환경, 안전 및 직업건강, 자연환경에 관한 법규 및 공공에 대한 요구/충족을 포함한 안전공학에 대한 전반적인 사항을 다루고 있다.

ISSN 1229-6783(Print)
ISSN 2288-1484(Online)



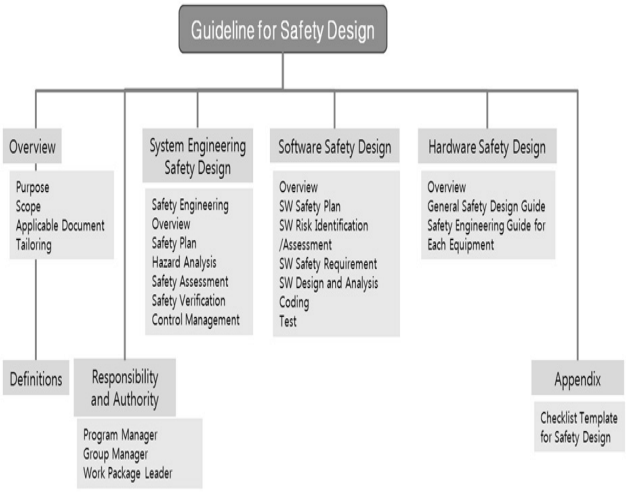
[Figure 3] The main writing topics classification using Logic Tree



[Figure 4] Details of potential X's classification using the C & E diagram

안전설계 지침서 작성에 대한 작성항목을 도출하기 위해 [Figure 3]과 같이 논리구조(Logic Tree)를 활용하여 단계적 분류를 진행하였다. 이로부터 분류된 안전설계 지침서의 주요 작성항목인 안전공학절차, 위험식별/분석, 위험평가, 위험검증에 대해 [Figure 4]와 같이 C&E 다이어그램을 적용하여 하위 카테고리 인자(잠재 X's)를 도출하였다.

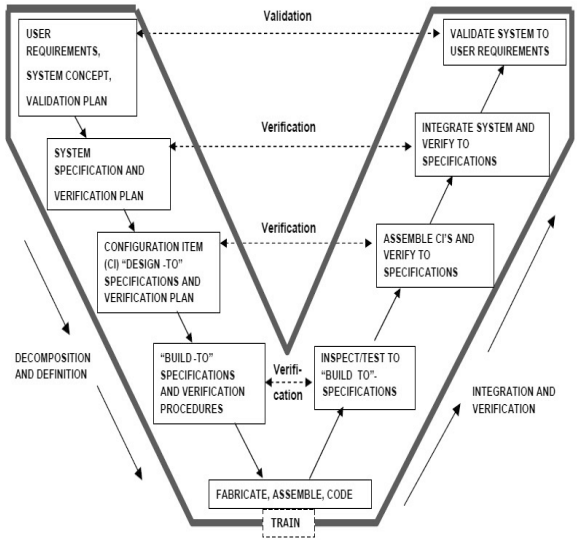
도출된 잠재 X's 인자를 업무의 필요성, 지침의 완성도, 설계적용 가능성 항목으로 평가하고 컨트롤이 가능한 인자를 최종 핵심인자(Vital Few X)로 확정하여 설계된 안전설계 지침서의 기본설계는 [Figure 5]와 같다.



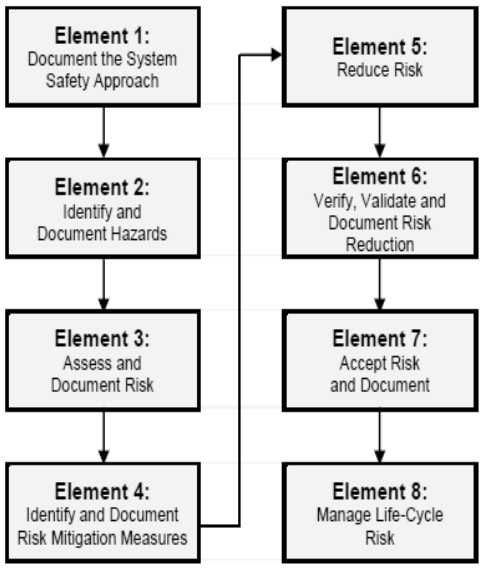
[Figure 5] Safety design guidance document based on Vital Few X

3.3 상세설계 및 최적화

[Figure 6]은 일반적인 시스템 개발 생명주기 V모델로서 좌측은 요구사항 분석, 시스템 사양설계이며 우측은 통합과 요구사항 검증/입증을 의미한다. 대형 시스템을 개발하는 다수의 국내기업에서는 위와 같은 V모델에 준하는 내부 개발절차를 따르고 있지만 시스템 개발 사이클에 걸친 체계적인 시스템 안전성 확보절차 즉, 안전에 관한 요구를 설계과정에 반영하기 위한 시스템안전 프로세스를 갖추고 있지 못한 실정이다.



[Figure 6] Systems development life cycle V models



[Figure 7] System Safety Process

[Figure 7]은 MIL-STD-882E에서 제시한 시스템 안전 프로세스이다. [Figure 7]에서 보여주는 바와 같이 시스템 안전 프로세스는 위험을 관리하기 위한 시스템 안전 접근방식을 문서화하면서 구체화된다. 안전계획(Plan)을 수립하고, 유해성을 식별(Identify)하며, 위험 평가(Assess)을 통해 중요도와 우선순위를 정하고, 위험을 분석(Analyze)하여 그에 따른 대책을 수립/실행하며, 실행결과를 추적/관리하기위해 통제(Control)하는 반복적인 행위의 연속으로 볼 수 있다.

본 연구에서는 시스템 요구사항 분석 단계에서부터 설계, 구현, 검증 단계까지 전반적인 체계공학 프로세스 상에서 시스템 안전방법을 사용하여 위험 식별 및 경감이 될 수 있도록 시스템 안전설계 프로세스를 확립하고 각 단계에 따른 세부 위험 분석, 위험 평가 및 관리를 수행하는 방법들을 개발 업무에 맞게 적용하는데 있다.

이를 위해 본 연구에서는 아래와 같은 주요 항목에 대해 최적평가 및 대안인자를 선정하여 반영하였다.

1) 시스템 안전설계 프로세스
: 시스템안전 설계기법을 사용하여 체계공학 프로세스에서의 위험 식별 및 경감 절차 수립
2) 안전계획서 작성
: 시스템 엔지니어링 관리계획(SEMP)의 일부로 포함
3) 유해성 추적 시스템 구축
: 식별된 위험상태를 추적하고 모니터링을 수행하는 유해성 추적 시스템 구축 및 유지보수 방안 반영(안전통제문서를 활용한 식별된 위험요인 추적 및 모니터링 수행절차 수립)
4) 안전설계 체크리스트
: 시스템통제 분야에 대한 유해성 식별 및 위험 감소 방안 체크리스트 작성(제품 개발단계별로 구분하여 안전설계 항목의 중점 관리)

최적화 단계를 완료한 제품 개발 프로세스 즉, 체계공학 프로세스에서 안전공학을 적용한 통합모델은 [Figure 8]과 같다.

최적화 단계를 거친 개선된 시스템 안전공학 절차는 안전계획 수립, 유해성 식별/평가, 위험 완화조치 방안, 위험감소, 위험감소 검증, 통제의 6단계로 구분되며 시스템 유해성 제거 또는 관련 위험을 완화하기 위한 시스템 설계 요구사항을 결정하고 해당 시스템 개발문서에 요구사항이 반영되었는지, 시스템이 요구사항을 준수하는지를 평가한다. 이후 식별된 유해성을 분석하고, 적절한 정책, 규정, 표준 등의 식별을 통해 유해성을 제거하거나 완화하기 위한 시스템설계 요구사항을 결정하여 시스템 개발절차에 따른 설계 산출 문서에 반영되어 관리된다.

안전계획 수립(System Safety Approach) 단계에서는 안전 위험의 식별, 분류 및 전반적인 체계공학 프로세스의 일부로서 위험완화에 대한 시스템 안전 방법을 문서화하며, 세부 위험 분석, 위험 평가 및 위험 관리의 체계적인 접근 방법을 구현하는 데 필요한 작업 및 활동을 정의한다.

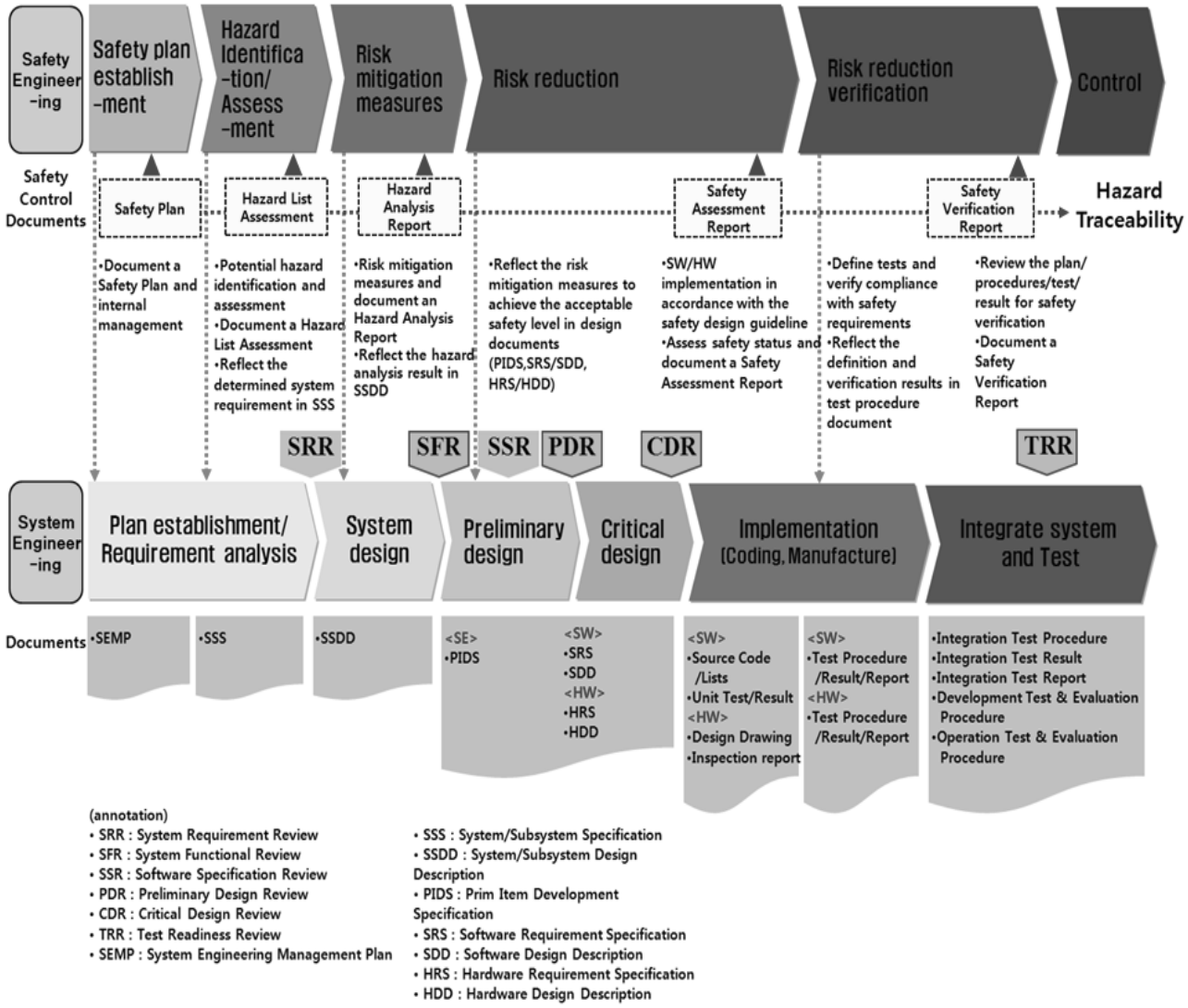
유해성 식별/평가(Identify/Assess Hazard) 단계에서는 설계단계(요구사항분석, 기본설계)에서 시스템을 분석하고 설계개념(또는 요구사항)에 내재 된 잠재적 위험을 식별한다. 식별된 유해성에 대해 위험 평가를 수행하여 유해성 목록 평가서를 작성한다.

위험 완화조치 방안(Risk Mitigation Measure) 단계에서는 식별/평가된 위험에 대한 완화조치를 확인하며 예상 위험감소 대안을 식별하고 유해성 분석 보고서를 작성한다. 위험을 제거할 수 없는 경우에는 관련된 위험 우선순위를 기준으로 시스템 안전설계 절차를 준수하여 비용, 일정, 성능의 제약 내에서 가장 낮은 허용 가능한 수준으로 감소시킨다.

위험감소(Reduce Risk) 단계에서는 수용 가능한 안전 수준을 달성하기 위해 적합한 완화조치를 결정하고 수행한다. 비용, 타당성, 그리고 체계공학 프로세스의 일부로 제시된 완화 방법의 효율성을 고려하여 평가하며, 현재 위험에 관련된 심각도, 확률 평가 및 기술 검토에서 위험 감소에 대한 대처 상황을 제시한다. 유해성 안전상태 및 관련위험에 대한 종합적인 평가를 수행하고 안전평가 보고서를 작성한다.

위험감소 검증(Verify Risk Reduction) 단계에서는 안전 요구 사항의 준수여부를 검증하기 위해 안전에

ISSN 1229-6783(Print)
ISSN 2288-1484(Online)



[Figure 8] System engineering process model integrated with safety engineering

중요한 하드웨어, 소프트웨어 및 절차에 대한 추가 검증 방법을 사용하거나 시연, 테스트를 정의하고 수행한다. 안전요구사항 준수 검증을 위한 계획, 절차, 시험/검사 결과를 검토하고 안전검증 보고서를 작성한다.

통제(Control) 단계에서는 현재 식별된 유해성 상태를 추적하고 모니터링 함으로써, 위험을 완화시키기 위한 효과적인 의사 결정을 수행한다. 또한 안전통제 문서를 관리하며 각 위험에 대한 의견수렴, 협업관리, 새로운 위험과 수정된 위험을 관리 유지한다. 만약 새로운 위험이 발견되거나 알려진 위험이 이전 평가보다 높은 수준을 결정하는 경우에는 위험 우선순위를 기준으로 시스템 안전절차를 준수하여 적절한 대응전략을 수립한다. 안전절차에 따른 안전통제 산출문서는 <Table 4>와 같다.

<Table 4> Safety control documents in accordance with the safety design process

Phase	Document
Safety plan establishment	Safety Plan
Hazard identification/ assessment	Hazard List Assessment
Risk mitigation measures	Hazard Analysis Report
Risk reduction	Safety Assessment Report
Risk reduction verification	Safety Verification Report

3.4 검증

검증 단계는 최적화 단계를 거쳐 확정된 설계안이 현장에 실제로 적용되더라도 문제가 없는지를 파일럿 테스트를 통해 확인하고, 설계 결과를 문서화·표준화하며, 향후에도 성과가 지속적으로 유지될 수 있도록 관리 계획을 수립하는 단계이다.

본 연구에서는 앞서 수행한 최적화 단계를 통하여 도출된 체계공학 프로세스에서 안전공학을 적용한 통합모델 및 안전설계 체크리스트를 진행 중인 시스템 개발 과제에 대해 파일럿 검증을 통하여 적용가능성을 평가하였다.

현재 상세설계 단계인 시스템 개발 과제에 [Figure 8]의 통합모델 적용 및 안전설계 체크리스트 기준으로 개발산출물에 대한 준수 수준을 검토하였다. [Figure 9]는 개발산출물(SSS, SSDD, PIDS, SRS/SDD, HRS/HDD)에 대해 개발 단계별로 작성된 안전설계 체크리스트를 기준으로 안전 요구사항 준수 및 반영률을 측정한 결과이다. 또한, 현 개발단계에 따른 안전통제문서를 [Figure 10]에서와 같이 설계를 수행하는 실무담당자가 작성함으로써 안전설계 지침서의 실무적용 가능성을 평가하였다.

No	Category	Data Collection Methods				Type	Note
		What	How	Tool	Period		
Y1	Safety Design Compliance Level	Output Documents of OOO project	Measurement of requirement compliance and reflects	Checklist	20xx.xx	DV	-

Subcategory	Results	Compliance Rate(%)	Expert Comments
XXX	29 / 29	100 %	Hazard identification and risk mitigation measures about OOO are reflected in the design document. The activities to remove/reduce the risk should be continued after CDR.
XXX	29 / 29	100 %	
XXX	13 / 13	100 %	
XXX	33 / 33	100 %	
XXX	33 / 33	100 %	
XXX	33 / 33	100 %	

[Figure 9] Safety design requirements compliance and measure reflected through the pilot verification

Hazard Analysis Report

Program: xxxx		**Issued by:** xxx	**Date:**	20xx.xx.xx
Hazard No/Sector: 1, System Engineering(SE)		**Owner:** xxx		
System Requirement No: SSS. 132				
Hazard Classification: Equipment(A) abnormal termination due to undefined message				
Related Content / Impact Message Definition Check System Degradation				
Hazard Assessment				
Severity	**Probability Level**	**Risk Assessment**		
3 (Marginal)	D (Remote)	Medium		
Risk Mitigation Measures				
Contents			Note	
Equipment(A) Interface/Linking Function Equipment(A) provides defined messages in case of training mode - ooo: ooo - ooo: ooo - ooo: ooo			SSDD [Function 532]	

[Figure 10] Hazard Analysis Report

객관적인 결과 검증을 위해 시스템 전문가평가를 실시하였으며 그 결과, 시스템 유해성 제거 또는 관련 위험을 완화하기 위한 시스템 설계 요구사항이 시스템 설계가 진행됨에 따라 체계/부체계 규격서(SSS), 주장비 개발 사양서(PIDS), 소프트웨어 요구사항 명세서/설계서(SRS/SDD), 하드웨어 요구사항 명세서/설계서(HRS/HDD) 등의 설계 문서에 요구사항으로 반영되어 안전통제문서를 통해 추적관리될 수 있음을 확인할 수 있었다.

향후 안전설계 체크리스트의 지속적인 업데이트를 통한 안전설계 항목의 중점 관리와 유해성 식별 및 위험완화에 대한 설계가 반영이 되어 상세설계 이후에도 단계별로 위험을 제거/감소 할 수 있도록 지속적으로 관리하여야 될 것으로 판단한다.

4. 결론

본 논문에서는 대형 시스템을 개발하는 업체에서 설계단계에 적용 가능한 안전설계 표준지침 및 프로세스를 구축하는 과제를 린 6시그마 프로젝트로 수행하였다. 신제품과 프로세스 개발 시 최적화를 위한 DFSS 프로세스의 DMADOV를 이용하여 시스템 안전설계 프로세스를 개발하고 표준화함으로써 고객중심의 가치흐름(value stream)과 프로세스의 효율을 증가시키는 혁신기법으로 활용됨을 알 수 있었다.

현대의 시스템은 전자 및 정보기술 분야의 비약적인 발전으로 인하여 자동화 된 복잡한 제어기능을 수행하고 있으며, 이러한 시스템은 국가기반시스템, 산업제어시스템, 군사무기체계에서부터 일반생활에 이르기까지

ISSN 1229-6783(Print)
ISSN 2288-1484(Online)

사회의 다양한 분야에 사용되고 있다. 이러한 기술의 발달은 사람에게 편리함을 제공하지만 시스템의 아주 사소한 오류로 인하여 인명사고가 발생되지 않도록 안전기준 및 체계를 구축하여 안전성을 확보하기 위한 활동이 필요하다.

더욱이 복잡화되고 자동화된 시스템의 안전성을 확보하기위하여 설계단계에서부터 개발 기법, 기준 및 체계를 구축함으로써 안정성을 확보해야 한다. 따라서 시스템 전 생명주기에 대한 위험 식별, 분석, 평가 및 검증 등 체계적인 위험 관리를 위해선 시스템 안전공학 방법을 사용하여 체계공학 프로세스에서의 유해성 식별하고 이를 경감시키기 위한 활동이 지속적으로 수행되어야 할 것이다.

5. References

[1] Sim-jae Ko(2012), “Changes in Military System Safety Standard and Analysis for Airworthiness Certification Impact”, The Korean Society for Aeronautical and Space Sciences, Vol.2012 No.11[2012], 421-429.

[2] Jong-kwon Kang(1986), “Changes of approachs for the Safety Engineering”, The Korean Society of Safety, 1(1):65-70.

[3] Korea Railroad Research Institute(2008), “A Research Report of Rail Software Safety Standards and System to Build”

[4] Moon-bak Choi(2008), “A Guideline for Implementing Lean Six Sigma for Management Innovation”, Korean Institute of Industrial Engineers, 32(4): 298-313.

[5] Seon-woo You, Young-jin Ahn(2009), “An Empirical Study on the Integrated Method of Lean and Six Sigma”, Korean Production & Operations Management Society, 20(3):23-42.

[6] Kang-gun Lee(2006), “A Study of Lean DFSS through the 4th Generation R&D Strategy ”, SeoKyeong University.

[7] DoD MIL-STD-882E(2012), "DEPARTMENT OF DEFENSE STANDARD PRACTICE SYSTEM SAFETY".

[8] Won-hyuk Sung, Hyung-kwan Kim(2014), “ A Study on the Hazard Identification and Analysis for System Safety Design”, The Koean Institute of Military Science and Technology, General Conference, 1:101-102.

[9] Jae-beom Noh(2005), “Service Enovation Engine Six sigma”, Samsung Economic Research Institute.

[10] Jong-ho Kim(2008), “Information Strategy Planning based on Six-Sigma DMADOV Methodology”, The Korean Operations Research and Management Science Society, 25(1):75-91.

[11] INCOSE(2000), "SYSTEMS ENGINEERING HANDBOOK”, ver 2.

[12] Young-min Kim, Jae-chon Lee(2012), “A Study on the Integration of Systems Engineering Process and Systems Safety Process in the Conceptual Design Stage to Improve Systems Safety”, Korea Safety Management & Science, 14(3):1-10.

저 자 소 개

김 형 관

금오공과대학교 대학원 소프트공학과 석사취득, 경영학과 박사 수료. 현재 삼성탈레스 해양/시스템 연구소에서 시스템설계 전문연구원으로 재직 중.
관심분야 : System Engineering, Safety Engineering, Lean 6 Sigma 등

박 도 현

경북대학교 대학원 전자공학과 박사 취득. 현재 삼성탈레스 해양/시스템연구소에서 시스템설계 분야 수석연구원으로 재직 중.
관심분야 : Combat Management System design, Sonar System design, System Engineering, Safety Engineering 등

허 형 조

한양대학교 대학원 전자통신공학과 석사취득, 덕성여대 통계학과 강사(07~08년), SSMI(식스시그마경제연구소) 수석위원(08~09년), 현재 삼성탈레스 경영기획팀에서 혁신사무국 담당부장 재직중, DQS(국방품질연구회)아카데미분과 전문위원 겸.
관심분야 : Lean 6 Sigma, TRIZ, VE(가치공학) 등

성 원 혁

경북대학교 컴퓨터공학과 학사 취득. 현재 삼성탈레스 해양/시스템 연구소에서 시스템설계 전문연구원으로 재직 중.
관심분야 : System Engineering, Safety Engineering, Network Analysis 등