시스템 안전 분석의 시스템 설계와의 통합 데이터베이스 구축 방안

박중용 · 박영원*
에스이테크놀로지(주) · *아주대학교 시스템공학과

1. 서 론

우리나라에는 그 동안 적지 않은 횟수의 대형 참사가 있어 왔으며, 그 때 마다 원인을 분석하고 대책을 세웠지만 사고는 계속되고 있다. 이와 같이 계속되는 사고에 대해 공학적 차원에서 찾아볼 수 있는 주요 원인은 시스템을 개발하는 초기 단계부터 시스템의 안전을 고려해서 규격서를 작성하고 설계를 하는 작업이 이루어지지 않았다는데 있다. 즉, 우리나라의 안전관리가 법률주의적 안전 보건법규에 의한 최소한의 안전성 확보라는 측면을 중요시하면서 실질적 최고수준의 안전성 확보 방안인 시스템 안전 프로그램의 가동에는 관심이 부족했기 때문이다.

이에 반해 미국이나 영국과 같은 선진국에서는 국방분야를 위주로 시스템 안전에 대한 관심이 높고 연구도 활발히 이루어지고 있다. 미국의 MIL-STD-882 시리즈나 영국의 DEF STAN 00-56과 같은 규격은 국방분야의 대표적인 시스템 안전 프로그램 관련 규격이다. 이러한 규격들은 시스템공학을 기반으로 하여 안전 분석과 인간공학을 통합하여 구성되어 있다. 하지만, 내용의 깊이가 일반적인 지침이나 모델을 설명하는 수준에서 그치고 있어 실제로 활용하려면 많은 어려움이 있다. 더구나 시스템이 점점 복잡해지면서 고장이 발생했을 때 사람이나 환경에 막대한 피해를 입히는 안전중시 시스템의 영역이 넓어지면서 종래의 안전 분석법으로는 분석에 어려움이 발생하고 있다.

또한, 시스템 안전 분석을 수행하더라도 분석 결과가 시스템 설계에 즉각적으로 반영되지 않으면 분석과 설계가 융화되지 못해 안전한 시스템 설계라는 목표를 달성하지 못하게 된다. 이에 따라 선진국에서도 현재 안전 분석 과정을 설계 과정과 통합하는 방법론에 대한 연구의 필요성이 제기되고 있는 실정이다.

이러한 문제점들을 해결하는 단서를 제안하기 위해 본 연구는 다음과 같은 목표를 가지고 수행되었다.

1) 안전 분석과 인간공학을 고려한 안전중시 시스템 설계용 통합 모델 개발
2) 상용 전산지원도구를 활용한 모델기반 안전중시 시스템 설계의 수행 방법 개발
3) 지식경영 전략에 부합하는 안전중시 시스템 설계 모델 개발
4) 안전중시 시스템 개발에 필수적인 시스템 설계, 시스템 안전 분석, 인간공학의 지식체계 정리

우리나라가 선진국으로 진입하기 위한 필수적 기술로서 시스템공학 기술 개발이 요구되고 있고, 각종 안전사고의 발생과 갈수록 복잡해지는 시스템의 안전상의 이유로 안전

분석의 필요성이 인식되고 있으며, 지식 경영의 실천 전략으로서 엔지니어링 데이터의 통합이 요구되고 있는 현 상황이 본 연구를 수행하게 된 배경이라 할 수 있다.

본 논문에서는 시스템공학, 안전 분석, 그리고 인간공학을 모두 고려하여 동시공학적으로 안전중시 시스템을 설계할 수 있는 모델에 대해 설명하고 예제를 들어 모델의 활용성을 검증하고자 한다.

2. 이 론

시스템공학은 시스템을 고객의 요구사항에 맞게끔 성공적으로 개발하기 위한 프로세스라고 할 수 있다. 시스템공학의 프로세스는 EIA 632, IEEE 1220과 같은 시스템공학 표준에 서술되어 있듯이 요구사항 분석. 기능 분석 및 할당, 그리고 물리적 아키텍쳐 구축과 같은 시스템 설계를 주요 프로세스로 하고 있다.

이러한 시스템공학은 컴퓨터 기술의 발달로 종래의 문서위주의 시스템공학에서 모델기반의 시스템공학으로 전환되었다. 그림 1은 시스템공학 전산지원도구인 CORE를 활용해서 시스템 설계를 수행하는 모델을 보여주고 있다[1].

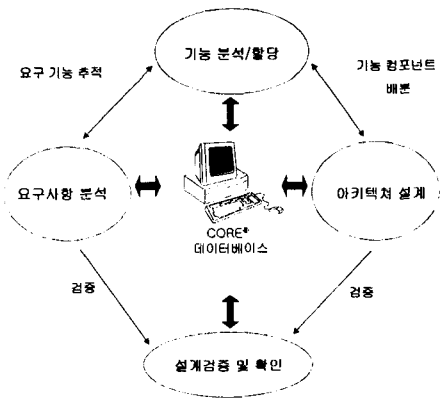


그림 1. 모델기반 시스템 설계의 개념.

시스템 안전 분석은 기능의 식별, 기능에 잠재되어 있는 위험 식별, 위험이 시스템에 미치는 영향 분석, 위험을 제거하는 방법 정의와 같은 업무를 수행하는 것으로 정의된다. 여기서 기능의 식별은 시스템공학의 중요 업무로서 이를 통해 시스템공학과 시스템 안전분석이 통합 수행되어야 하는 당위성을 알 수 있다. 위험 식별의 방법은 알려진 것만 해도 100여가지가 넘으나, 개발 초기에 사용되는 대표적인 방법으로는 FHA (Functional Hazard Assessment)와 HAZOP(Hazard and Operability Study)이 있다.

FHA는 시스템 수명주기의 초기에 위험을 식별하는데 사용되는 방법으로 SAE(Society of Automotive Engineers)가 발간한 ARP4754에서 제안되었다. FHA는 시스템 부분의 기능적 고장이 시스템에 미치는 영향을 발견하는 방법으로 주요 목적은 위

험한 상황을 일으키는 기능을 식별하고 위험의 심각도를 결정하는데 있다. FHA를 수행하기 위해서는 먼저, 분석하고자 하는 기능을 선택한 후 선택된 기능의 목적과 거동을 정의한다. 다음 고장 모드를 가정하고 그 영향을 결정한다. 마지막으로 고장의 심각도나 발생 확률과 같은 리스크 관련 요인들을 결정하고 기록한다.

HAZOP은 통합된 이벤트 기반 분석법의 일종으로 예측적인 분석법이다. 즉, 연역적인 사고와 귀납적인 사고를 동시에 하도록 프로세스가 구성되어 있고, 존재하지 않는 새로운 시스템을 개발할 때 사용됨으로써 알려지지 않은 원인을 대상으로 하기 때문에 예측적인 측면이 있는 것이다. 또한 정량적인 분석이 아닌 정성적인 분석법이다.

FHA와 HAZOP을 수행하여 산출되는 결과는 FMEA(Failure Modes and Effects Analysis)와 비슷한 표 형태로 만들어진다. 또한 두 방법 수행 과정 역시 FMEA와 비슷하되 주로 기능에 대해 분석을 수행한다는 차이점만 가지고 있어서 FMEA에 익숙한 일반 엔지니어들이 쉽게 받아들일 수 있는 장점이 있다. FMEA는 기능보다는 구체적으로 구현된 구성품에 대해 고장 분석을 하는 방법이다.

안전중시 시스템을 설계함에 있어 인간공학적 측면을 고려해야 하는 당위성에 대해서는 인정하면서도 구체적인 통합 방안이나 도구의 제공은 거의 없는 실정이다[2]. 인간공학의 수많은 영역 중에서 안전중시 시스템 설계와 깊은 관련이 있는 분야는 업무 분석과 인간과오 분석이다. 위험 분석에서 기능을 식별하고 그 기능에 잠재되어 있는 위험을 분석했듯이 인간이 수행하는 업무를 식별하고 그 업무를 수행하면서 발생할 가능성이 높은 인간과오를 분석하는 작업이 필요하다.

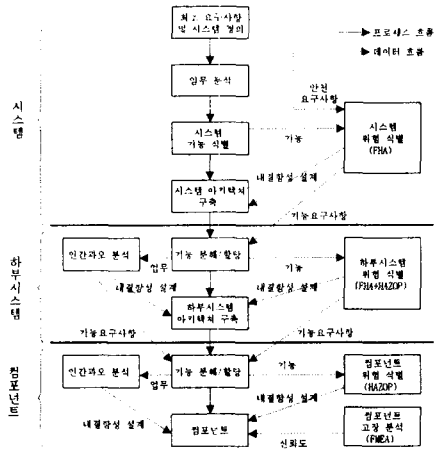
3. 모델 및 예제

본 논문에서 사용하는 통합 모델의 의미는 PMTE(Process, Method, Tool, Environment) 모델을 의미한다. 즉, 안전중시 시스템 설계에 필요한 프로세스, 방법, 그리고 도구를 망라하는 모델을 구축하는 것이다. 환경의 경우는 각 조직마다 다르기 때문에 본 논문에서는 다루지 않았다.

본 절에서는 요구사항 분석, 기능 분석 및 할당, 조합, 그리고 시스템 분석 및 최적화로 이루어져 있는 시스템 설계 프로세스에 FHA, HAZOP, FMEA로 대변되는 안전 분석의 방법들, 그리고 업무분석과 인간과오 분석으로 대표되는 인간공학의 방법들을 통합할 수 있도록 상용 시스템공학 도구인 CORE를 활용해서 모델을 구현하였다. 본 모델이 적용되는 제품의 수명주기는 개념설계, 예비설계 단계와 같은 초기가 되겠다. 그리고, 본 모델을 적용하여 구현한 예제를 소개하였다.

통합 모델을 구축하는데 있어 바탕이 된 원칙 및 필요성으로는 계층적 접근법, 동시공학적 접근, 통합된 모델에서의 데이터베이스 활용, 인간공학 도입, 실용적이고 구체적인 프로세스 구축, 기존의 방법론 수용, 단순한 모델, 주요 분석 과정의 데이터베이스화 등이 있다. 이와 같은 원리를 바탕으로 개발된 안전중시 시스템 설계 프로세스를 그림 2에서

보여주고 있다. 프로세스는 크게 세 가지 영역으로 나뉘어졌다. 즉, 가운데 부분은 시스템 설계 프로세스, 왼쪽은 인간공학의 인간과오 분석 프로세스, 그리고 오른쪽은 안전 분석의 FHA, HAZOP, 그리고 FMEA 프로세스로 구성되어 있다. 본 모델에서는 최상위 시스템에 대해서는 FHA를, 하부시스템에 대해서는 FHA와 HAZOP을 위험 분석 방법으로 채택하였다. 여러 분석 방법 중에서도 두 가지 방법을 택한 이유는 시스템을 설계하는 초기에는 구체적인 컴포넌트가 구현되어 있지 않고 기능만이 식별되기 때문에 기능 분석 결과를 활용할 수 있는 FHA와 HAZOP이 강점을 가지고 있기 때문이다.



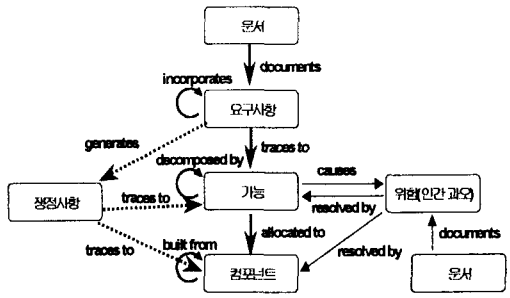


그림 2. 안전중시 시스템 설계 프로세스. 그림 3. FHA, HAZOP, FMEA를 위한 스키마.

시스템을 분석할 때는 FHA를 사용하고 하부시스템의 경우는 각 기능 간에 오고 가는 데이터가 구체화되고 그 만큼 종류가 많아져서 FHA에서 제시하고 있는 고장 모드로는 다 수용할 수 없기 때문에 HAZOP이 분석 방법으로 적절하다. 마지막으로 최하위의 컴포넌트는 고장 분석의 차원에서 FMEA를 수행할 수 있도록 하였다. FHA, HAZOP, FMEA는 결과로 나타나는 속성들이 유사하기 때문에 계층에 따라 별도의 요소를 만들 필요가 없다는 장점이 있다. 개발한 시스템 설계 프로세스를 수행할 수 있도록 CORE에 새로운 스키마를 구축했다. 그림 3은 FHA, HAZOP, FMEA를 수행할 수 있도록 개발된 새로운 스키마를 보여주고 있다.

본 모델의 가장 큰 장점은 기능 분석의 결과를 그대로 이용하여 위험 분석을 할 수 있다는 것이다. 특히, 갈수록 소프트웨어가 차지하는 비중이 높아지고 있는 현 시스템의 경우는 거동분석의 중요성이 큰데, 제안된 모델에서 채택한 EFFBD(Enhanced Functional Flow Block Diagram)는 이 면에서 가장 적당한 방법이다. 기존의 방법들은 구체적인 기능 분석의 방법을 제시하지 않은 경우가 많았고 제시한 경우에도 그 구체성이 떨어지거나 위험 분석 방법과 함께 하나의 모델에서 구현되지 않았다. 그러나, 본 모델은 한 모델에서 기능 분석과 위험 분석을 함께 수행함으로써 식별된 기능에 대해 위험 분석이 누락

되는 경우를 막을 수 있고 추적성을 확보할 수 있게 된 것이다. 특히, 요구사항부터 기능, 컴포넌트까지 추적성을 갖는 기능과 인간공학의 고려는 본 모델만이 제공하고 있음을 알 수 있다.

제안한 안전중시 시스템 설계 모델의 유용성을 검증하기 위해 예제로서 민수용 여객기를 채택하여 실제로 설계를 수행한 결과를 간단히 소개한다. SAE에서 발간한 ARP4761 부록 L에는 제시한 위험 분석 모델을 검증하기 위해 가상의 300-350인승 민수용 여객기 예제가 실려있다[3]. 이 예제를 이용하여 모델의 활용성을 검증하였다. 개발하고자 하는 항공기 시스템의 영역을 정의하는 물리적 정황은 그림 4로 표현된다.

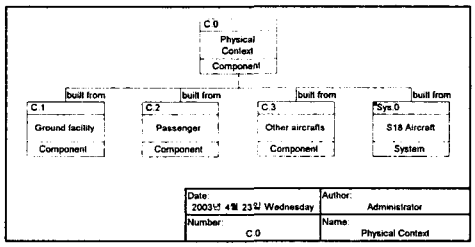


그림 4. 항공기 시스템의 물리적 정황.

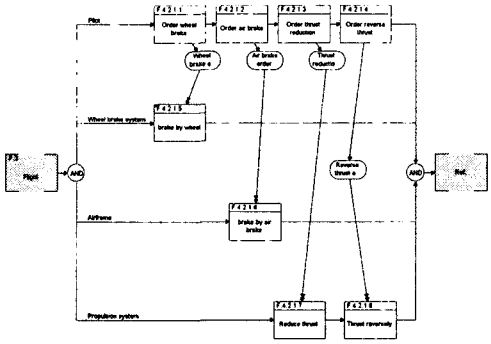


그림 5. 지상에서의 항공기 감속 기능 EFFBD.

그림 5는 항공기가 착륙해서 지상에서 감속할 때 어떤 기능이 필요한지 분석한 EFFBD이다. 그림 6은 지상에서의 항공기 감속 기능에 잠재되어 있는 위험 요소를 해결하기 위해 제안된 새로운 하부 기능을 추적성을 갖도록 연결한 ER(Element Relationship) 다이아그램이다. 그림 7은 위험에 대비하기 위해 중복 설계된 바퀴 브레이크 시스템의 물리적 블록 다이어그램이다.

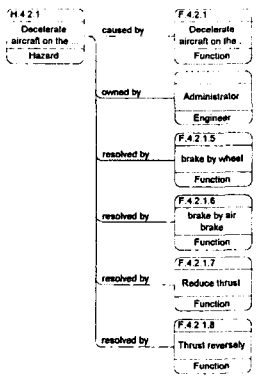


그림 6. 지상에서의 항공기 감속 위험 요소의 해결책.

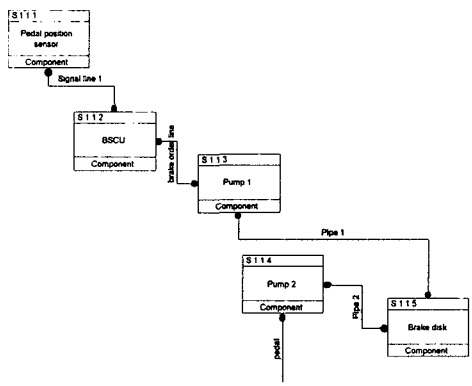


그림 7. 바퀴 브레이크 시스템의 물리적 블록 다이어그램.

4. 결 론

본 논문에서는 갈수록 영역이 확장되면서 복잡해지고 있는 안전중시 시스템을 설계하는데 필요한 동시공학적 모델을 제시하였다. 모델은 시스템공학의 핵심 프로세스인 시스템 설계 프로세스를 기본으로 하고 여기에 시스템 안전 분석 방법인 FHA, HAZOP, FMEA와 인간공학의 방법인 업무 분석법과 인간과오 분석법을 통합하여 구성되었다. 기존의 안전중시 시스템 설계 방법론들은 구체적인 기능 분석 방법을 제시하지 못하거나 식별된 기능들이 빠짐없이 위험 분석의 대상이 되었는지 확인할 수 없다는 한계를 가지고 있었다. 또한, 인간공학의 측면을 고려 대상으로 선정만 했을 뿐 실질적으로 다른 분야와 통합해서 구현하는 방법을 제시하지 못했다. 이에 본 논문에서는 잘 알려진 CASysE 도구를 활용해서 동시공학적으로 시스템 설계를 할 수 있는 프로세스, 방법, 그리고 도구를 제시하였다. 즉, 기능 분석의 방법으로 EFFBD를 채택하고 시스템 수준에서부터 분해를 통해 하부 시스템의 기능을 분석하도록 했으며, 이 과정에서 자연스럽게 업무 분석을 수행할 수 있게 하였다. 식별된 기능과 업무에 대해 잠재되어 있는 위험을 FHA, HAZOP을 통해 분석하여 이를 다음 단계의 기능 분석이나 물리적 아키텍쳐 구축에 반영함으로써 안전 분석 결과가 시스템 설계에 효과적으로 활용될 수 있도록 하였다. 본 연구의 주요 성과는 시스템 설계를 손쉽게 구현할 수 있는 모델기반 시스템 설계 기법을 통해 동시공학적으로 안전중시 시스템의 규격을 창출할 수 있는 가능성을 선보였다는 데 있다. 또한, 이 과정에서 구축된 통합 데이터베이스는 비슷한 시스템을 개발할 때 재사용될 수 있어 지식경영의 큰 틀에도 적합함을 알 수 있다.

참고문헌

[1] J.Y. Park and Y.W. Park, "Application of Computer-Aided Systems Engineering to Develop Automated Guided Transit(AGT) System Architecture", Proceedings of the 11th Annual INCOSE Symposium, 2001

[2] Y. Papadopoulos, J. McDermid, R. Sasse, and G. Heiner, "Analysis and synthesis of the behaviour of complex programmable electronic systems in conditions of failure", Reliability Engineering and System Safety, Vol. 71, No. 3, pp. 229~247, 2001

[3] SAE, SAE ARP4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, Society of Automotive Engineers, Inc., USA, pp. 12~39, 168~331, 1996