기능적 안전성 분석 기법을 적용한 안전성 요구사항 관리 체계 구축 방안 연구

The study of Developement Safety Requirement management system using functional hazard analysis technic

홍선호* **조연옥***

Hong, Seon-Ho **Cho, Yeon-Ok**

ABSTRACT

All the systems can be used properly for the original purpose when they can make the functions required for the users be concrete. Especially in the case that many technical systems are integrated like railroad systems, physically useful systems could be built if requirements analyses applying systems engineering and the process of functional design had to be supported. This paper is intended to review and present the measures and procedures to correctly supply the systems to users by giving systems manufactures and suppliers requirements in order to supply safe systems using safety analysis techniques named FHA(Functional Hazard Analysis) and Hazop Study.

1. 서 론

철도시스템은 승객 또는 화물을 운송하기 위한 주기능과 이를 둘러싼 다양한 환경요소와의 인터페이스를 담당하는 보조기능으로 대별할 수 있다. 따라서, 운송에 요구되는 에너지의 생성과 소비를 기반으로 수송수요를 충족하는 것이 가장 큰 존재의 이유이자 목표라고 할 수 있다. 특히 안전한 시스템의 운영은 이 목표를 달성하기 위한 필수적인 요소라고 할 수 있다. 이를 수행하기 위해서는 운영자, 계약자, 공급자, 분석가, 평가자 간의 관계가 각기 주어진 미션에 따라 수행되어질 때라야만 비로서 충족되어질 수 있다. 따라서 이러한 다양한 분야의 임무 수행자가 어떠한 절차와 방법론을 통해 수행되어야 하는지 검토하므로서 체계적인 접근 방안에 대한 도출이 필요하다.

2.. 운영자 관점의 역할과 임무

시스템을 운영하고 있는 운영자는 운용과 관리의 두가지 측면에서의 역할을 수행하고 있다. 즉, 철도차량 및 운영시설과 같은 특정 장치를 운용하는 운용자와 이들이 잘 운용하도록 하는 시스템 관리자가 있으며, 이때 자기 자신의 시스템을 정의하고 문제점이 관리되어져야 한다. 운영단계에서의 문제점은 PHA와 같은 분석기법이 사용되어 질 수 있으며, 이때 전체 시스템의 현황이 체계적으로 관리되어질 수 있도록 운용목적, 목표과 대비되는 안전성 활동이 수행되고 이를 모니터링하여야 한다.

3. 시스템 엔지니어의 프로젝트 접근과정과 역할

* 한국철도기술연구원 정회원
E-mail : shhong@krri.re.kr, yocho@krri.re.kr
TEL : (031)460-5542, 5429 FAX : (031) 460-5509

3.1 시스템 엔지니어링 요구사항 분석 단계에서의 임무

시스템 엔지니어의 요구사항분석 결과가 시스템에 적합하게 반영되었는지를 보는 활동 중 확인과 검증에 대한 업무가 있다. 검증에는 두가지 형태 즉, 주기검증(life-cycle verification)과 형식 검증(formal verification)이 있는데 주기 검증은 개발 주기의 특정 단계에서 제작된 생산 제품이 그 이전 단계에서 설정한 사양들을 어느 정도 충족시킬 수 있는가를 결정하는 과정이고, 형식 검증은 원시코드가 사양에 맞게 작성되었는가를 수학적으로 엄격하게 증명하는 것이다. 확인은 요구사항 분석결과가 고객의 니드에 맞게 도출되었는지와 시스템 개발과정의 종료시 시스템이 요구사항에 맞게 제작되었는가를 결정하기 위하여 이를 평가하는 과정이라고 할 수 있다.

보햄은 검증은 제품을 올바르게 만들고 있는가로 정의하고, 확인은 올바른 제품을 만들고 있는가로서 검증과 확인을 정의하고 있다.

검증과 확인 활동에는 생산 제품이 사양을 준수하여 제작되었는가를 평가하는 활동도 포함하고 있는데, 평가 대상이 될 사양에는 다음과 같은 것들이 있다.

1) 여러 제품의 사양에 적용될 형식과 표기법에 관한 사양
2) 요구사양(요구사양 명세서)
3) 설계서(설계 명세서)
4) 여러 유형의 지침
5) 구현용 언어의 표준
6) 프로젝트의 표준
7) 조직의 표준
8) 사용자의 기대감

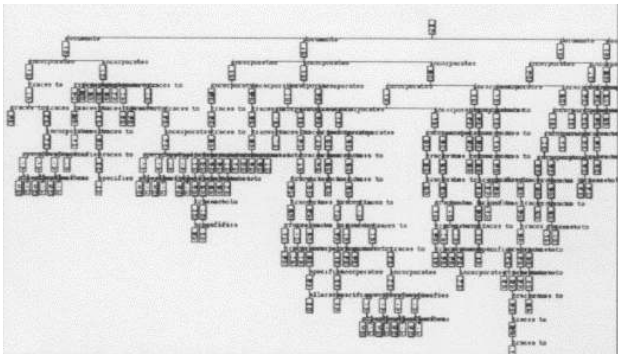

그림 1 요구사항 트리 사례

이상과 같이 시스템의 설계단계에서 수행되는 요구사항의 분석단계에서부터 시스템이 문제가 발생되지 않도록 시스템엔지니어의 활동이 수행되어야 한다.

3.2 시스템 엔지니어링 아키텍쳐 개발 단계에서의 임무

시스템 아키텍쳐 개발 단계는 상위의 요구사항 및 기능분석과정을 통해 물리적인 형상을 구체화하는 과정이다.

이때 요구사항과 기능 및 아키텍쳐 간의 물리적 추적성을 통하여 요구되는 모든 사항이 시스템에 반영되어질 수 있도록 분석되어져야 한다. 아래는 요구사항영역과 기능역을을 기반으로 아키텍쳐로서 반영되어지는 과정을 설명한 것이다.

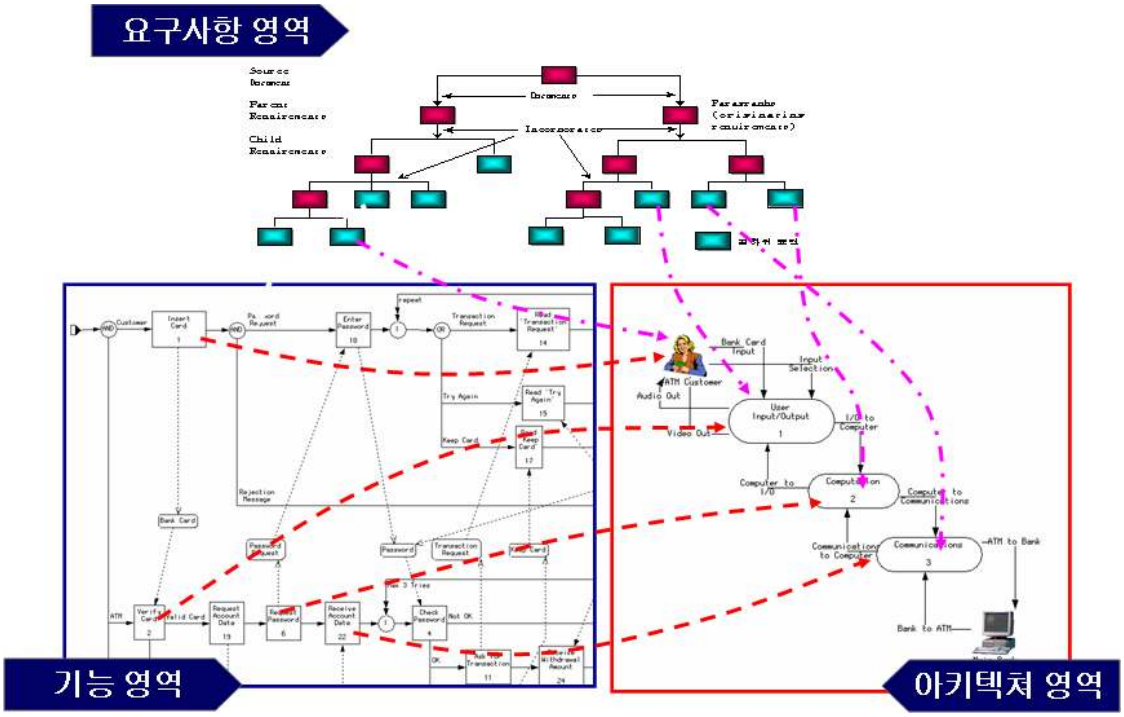

그림 2. 요구사항과 기능 및 아키텍쳐와의 관계

4. 안전 엔지니어의 프로젝트 접근과정과 역할

4.1 요구사항 및 기능적 관점의 안전 엔지니어의 분석

현재의 국내 규격은 국제 규격 부합화에 따른 다양한 분석 방법론이 제시되어지고 있으나 이에 대한 사례 등이 제시되어야만 적용이 가능하다. 이중 유럽 규격인 EN50129의 경우 시스템의 인가 및 수용을 위해 필요한 안전성 요구사항과 그 문서관리에 대한 규정을 제시하고 있다. 단 관련 시스템이 안전성이 요구되는 영역을 독립적인 장치로서 SIL이 할당되어질 수 있으며 안전성을 중시하는 시스템의 무결성 등급을 중심으로 적용할 것을 요구하고 있는 점이 주의하여야 할 사항이다.

여기서는 시스템을 둘러싼 첫 번째 기능이 도출되어지고 이를 기능으로부터의 위험원 식별을 통해 시스템에서 갖춰야할 요구사항을 기능 내에 둘 것인가 아니면 시스템 외부로 정의할 것인가를 정의하고, 또한 무결성 요구의 대상 기능을 정의하는 것이 중요한 분석내용이라고 할 수 있다.

4.2 인터페이스 관점의 안전 엔지니어의 분석

시스템 구축대상의 모든 기능내외의 위험이 식별되어 초기 기능 안전성 요구사항이 도출되어지고, 이들이 반영되어졌다면, 두 번째 서브 시스템 레벨의 아키텍쳐 개발 활동을 통해 서브시스템의 기능간에서 발생되어질 인터페이스 상의 위험을을 도출하여야 한다. 이때 Hazop study 방법이 사용되어 질 수 있으며, 주요 산출된 내용을 다시 기능에 둘 것인지 비기능적인 프로젝트 활동으로 남겨둘 것인지를 결정하게 된다. 즉, 비용분석을 통해 위험이 낮아지는 대안의 채택이 결정되는 과정이라고 할 수 있다.

5. 안전성 요구사항의 검증과 확인

5.1 기능 및 인터페이스 안전성 요구사항의 검증과 확인

이상의 기능 및 인터페이스 관점의 요구사항이 결정되어지면 이들 모든 활동이 적합했음을 증명하는

추적성이 평가자에게 확인되어져야 한다. 아래는 요구사항과 기능간의 추적성 및 연관성이 비교되어져야 한다.

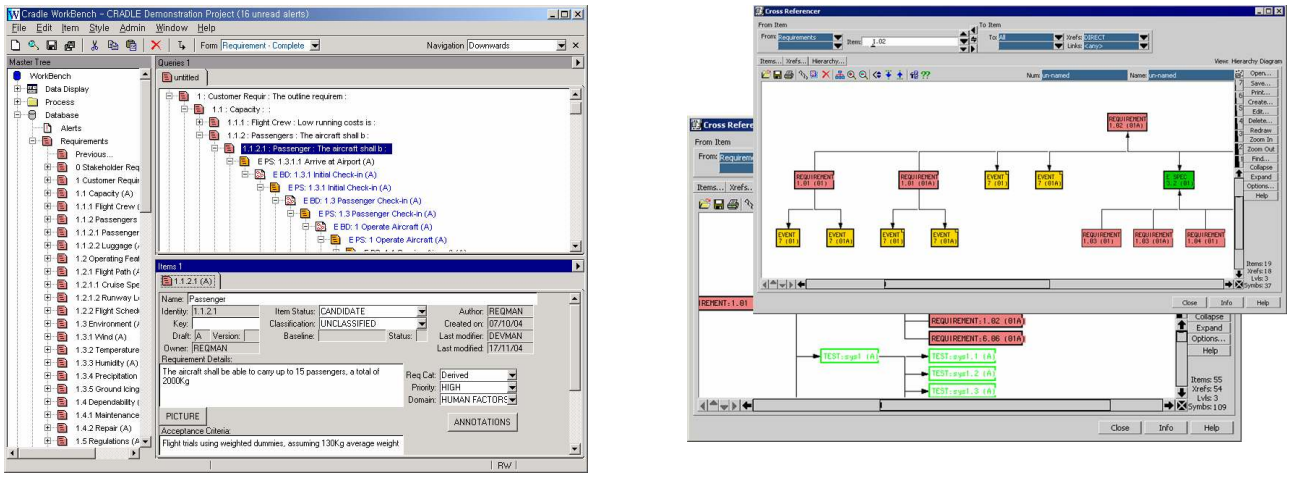

그림 3 추적성 및 연관성 분석 예시

5.2 안전성 요구사항의 검증과 확인 문서화

상기 정의된 바를 기반으로 시스템의 모든 정형화 과정에 대한 결과가 적합했음을 입증하는 문서화 활동이 요구되어진다. 이때 시스템의 개요를 기반으로 안전성 활동에 대한 증거들이 체계적으로 제시되어질 수 있다. 또한 이들 문서는 프로젝트 과정중 지속적으로 변경 및 관리되어짐으로서 마지막 사용자에게 인도할 때 까지 유지되어질 수 있어야 한다.

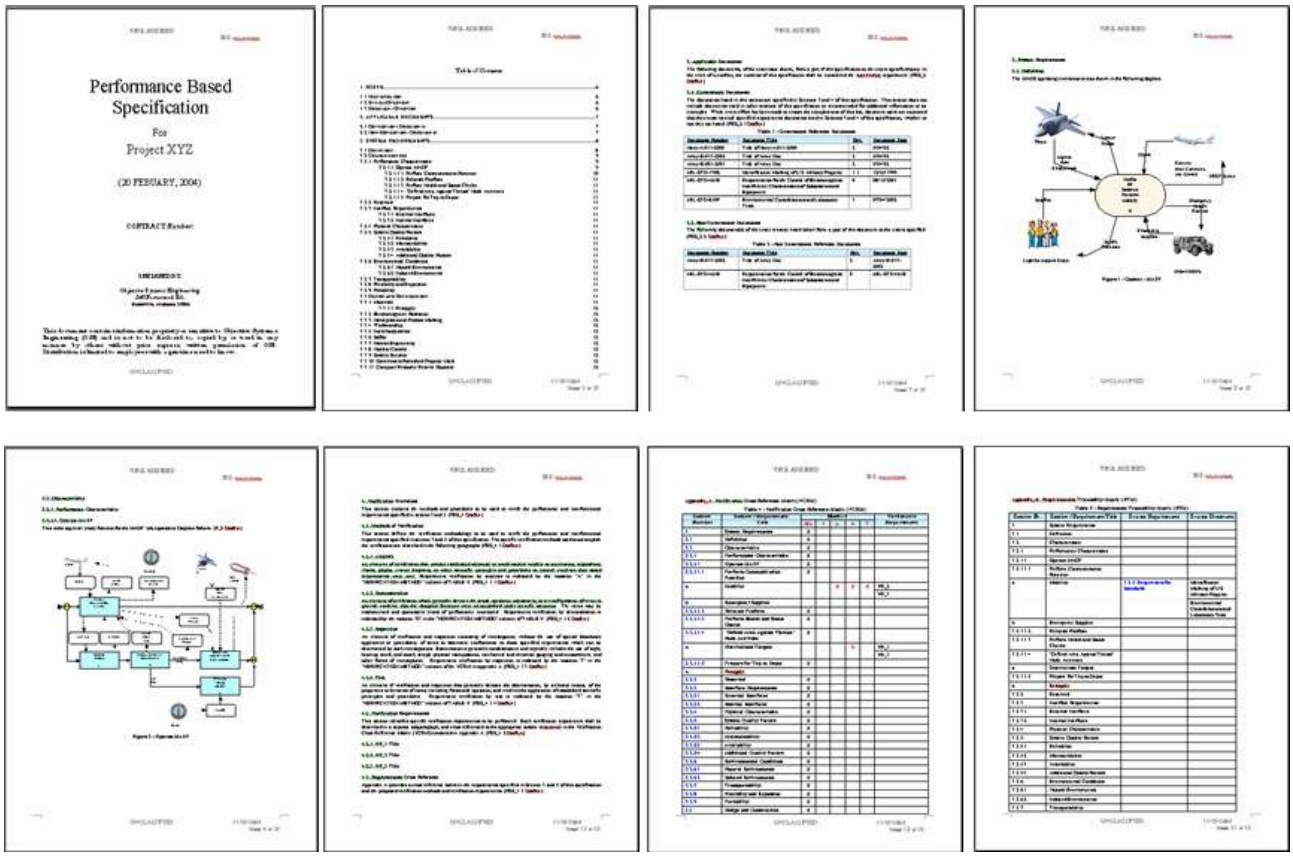

그림 4 문서화 사례

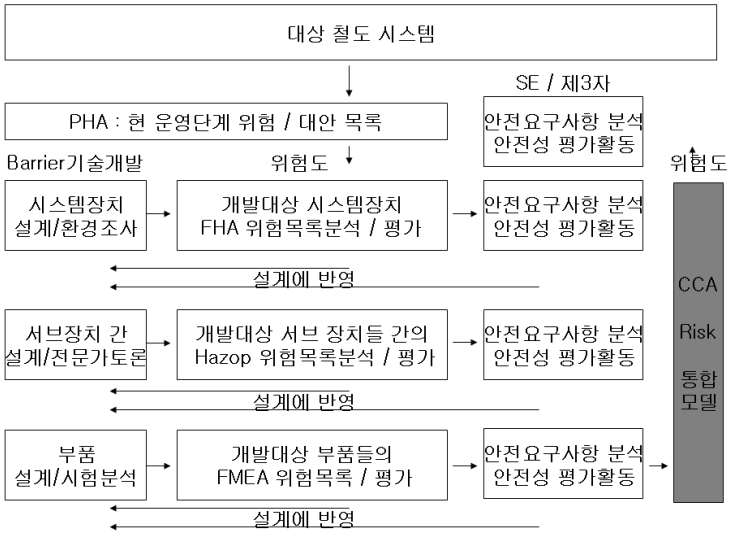

그림 5 통합 시스템 안전성 요구사항 분석 및 관리 체계

6. 결언

이상에서 살펴본 바와 같이 새로운 또는 변경되어지는 시스템에 대한 안전성 요구사항의 분석과 관리 절차와 필요한 분석과정을 살펴보았다. 이 과정은 기능적 관점의 시스템 분석과 이를 기반으로 하는 안전성 분석 및 관리 방안으로서 다음과 같은 결론을 도출하였다.

- 운영자 관점에서의 역할과 프로젝트내에서의 시스템엔지니어와 안전 엔지니어의 역할을 정의하였다.
- 각 단계별 적용대상 분석방법을 검토하였으며, 이 방법은 다시 시스템에 반영되어지는 추적성을 유지하여야 함을 제시하였다.
- 모든 활동의 단계별로 검증과 확인의 중요성을 제시하였으며, 이는 새로운 철도시스템의 채택으로 인한 사고 저감에 기여할 수 있는 방안인 것으로 판단된다.

참고문헌

1. 김종기, 철도와 전기기술 (2003년), “신호시스템 안전성 규격의 국제화”, 논문집, Vol 14