철도시스템 안전성 확보를 위한 시스템 설계와 안전성 활동의 통합에 관한 연구

On the Integration of System Design and Safety Processes to Assure Safety in Rail Systems Design

김창원*†, 이재천*

Chang-Won Kim*†, Jae-Chon Lee*

Abstract A class of systems are called safety-critical systems in which systems failure may result in accidents with serious damage on human being and properties. As such, safety assurance has been a big necessity in large-scale complex systems in a variety of domains such as rail, automotive, aerospace, and defense. Therefore, a successful development of complex systems with safety assured has created a special concern on how to incorporate safety requirements in the system design process. To discuss what are needed to meet such concern is the objective of this study. To do so, the relevant systems design processes and safety processes in a variety of domains are analyzed. The result is then utilized in the development of an integrated process for the rail systems design with safety assured.

Keywords **:** Functional Safety, Integrated Process, Safety Analysis, System Engineering Process, System Safety

초 록 시스템 설계 오류 등 여러 요인으로 사고가 발생했을 때, 인명과 재산상에 막대한 피해를 초래하는 시스템을 안전중시 시스템이라고 하는데, 대표적으로 철도, 자동차, 항공, 국방 분야의 대형복합 시스템들이 해당된다. 시스템의 복잡도가 증가하고 시스템의 무인화 운영 등으로 안전성 위해 요소가 증가하고 있기 때문에 시스템의 안전성 확보는 매우 중요한 설계목표가 되고 있다. 따라서 안전성 분석 활동이 반영된 시스템 설계 프로세스, 방법론 및 도구의 개발이 필요하다. 이것을 위해 본 연구에서는 다양한 산업 분야에서의 시스템 설계 프로세스와 안전 분석 프로세스에 대한 연구들을 분석하고 비교하였다. 이 결과를 기반으로 안전성이 확보된 철도시스템 개발에 필요한 시스템설계 활동과 안전성 분석 활동이 통합된 프로세스를 제시하였다.

주요어 : 기능 안전, 안전성 분석, 시스템 설계, 시스템 안전, 시스템공학 프로세스, 통합 프로세스

1. 서 론

안전사고가 발생했을 때, 인명과 재산상의 막대한 피해를 입히는 시스템을 안전중시 시스템이라 한다. 이러한 안전중시 시스템들은 과거와 비교해서 급격한 운영성능의 발전을 가져왔고, 동시에 기능적으로도 매우 복잡해지게 되었다. 대형화, 복잡화 되어 가고 있는 시스템

† 교신저자: 아주대학교 시스템공학과(zzang00k@ajou.ac.kr)
* 아주대학교 시스템공학과

들은 더욱 커진 사고 및 고장에 대한 위험을 내재하게 된다. 따라서 이와 같은 안전중시 시스템들은 사고나 고장이 인명 피해로 직결되기 때문에 체계적인 안전관리가 필요하다.

미국방부의 시스템 안전 표준[1]과 IEC의 기능 안전 표준[2]은 대표적으로 시스템 설계에 안전성이 반영되도록 하기 위한 표준이다. 국방, 철도, 항공, 해양, 원자력 등의 안전이 중시되는 산업분야에서는 위와 같은 표준규격을 제정하고 이를 준수하도록 권장하고 있다. 특히 철도 분야에서는 철도시스템 설계 시에 안전과 품질을 고려할 수 있도록, EN 50126 표준을 제정하여 RAMS(Reliability, Availability, Maintainability, Safety) process를 프로젝트 초기 및 시스템 개발과 운영 동안에 적용함으로써, 안전과 품질을 고려하도록 하고 있다[3].

또한, 철도 신호시스템의 안전관련 표준인 EN 50129[4]에서는 철도 신호시스템의 안전성 분석 프로세스를 제시했다. 먼저 시스템 설계 정보를 기반으로 위험원을 식별하고, 식별된 위험원에 의해서 발생할 수 있는 사고들을 식별한다. 이 사고의 리스트를 기반으로 리스크 평가를 수행하여, 사고의 발생 빈도와 심각도의 곱으로 표현할 수 있는 리스크를 도출한다. 이 리스크 평가결과를 기반으로 안전 요구사항을 도출한다. 요약하자면 EN 50129의 안전성 분석 활동은 위험원 식별, 위험원으로 인한 결과의 분석, 리스크 평가 및 안전 요구사항 도출로 정리 할 수 있다. [Fig. 1]은 EN 50129에서 제시한 안전성 분석 프로세스를 보여준다.

안전중시 시스템의 개발에서 안전 활동과 설계 활동은 각각의 산출물이 상호간의 입력 데이터로 활용되므로, 두 활동들은 항상 상호 의존적으로 수행되어야 한다. 하지만 안전부서와 개발부서는 두 활동들이 개별적으로 수행되고 있다[5]. 또한 시스템 안전과 기능 안전 표준에서 명확한 프로세스를 제시했더라도, 이 프로세스를 활용해서 실제 안전중시 시스템 설계에 어떻게 반영하는지에 대한 가이드나 지침을 찾는 것이 어렵다[6]. 따라서 최근에는 시스템 개발 프로세스의 초기 개념설계 단계부터 안전성 분석 활동을 다양한 방식으로 통합 하려는 연구들이 수행되고 있고, 이 연구 결과들은 안전중시 시스템

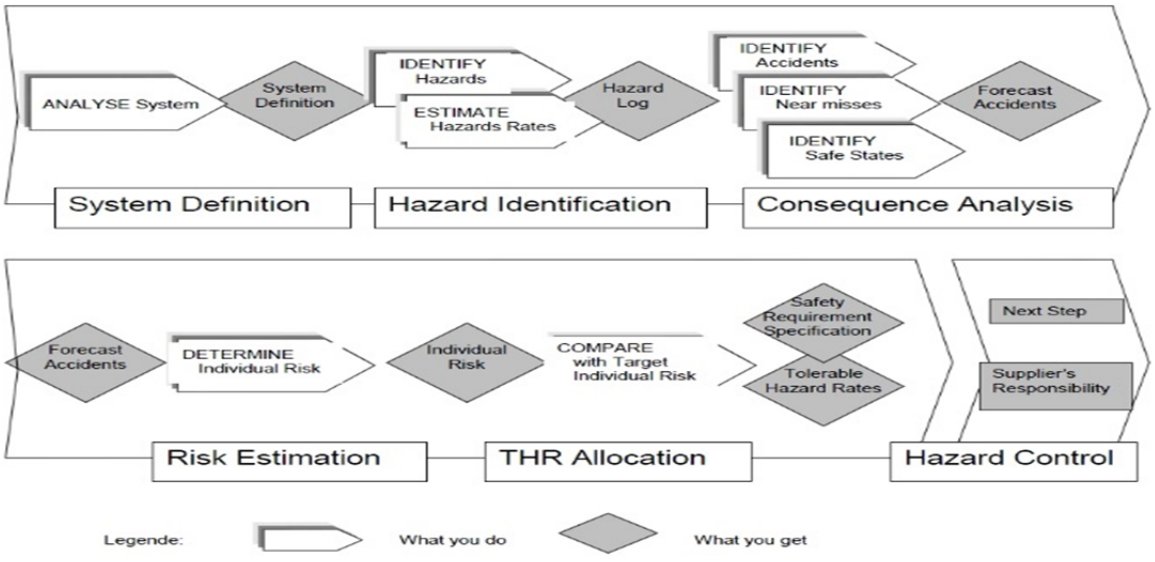

Fig. 1 Risk analysis process of EN 50129[4].

설계의 가이드나 지침으로서 역할을 수행할 것으로 기대되고 있다.

[7]에서는 시스템공학과 안전 활동의 통합에 관한 연구를 수행했다. 각 활동을 수행함으로써 생성한 결과물들을 하나의 테이블로 나타내어 매칭시켰고, 이러한 방식을 시스템 설계와 안전 활동 사이의 산출물 교환이라고 표현했다. 하지만 시스템공학 활동과 안전성 분석 활동의 순서를 명확하게 파악하지 못했고, 각 활동에서 산출된 데이터들의 교환방식을 제시하지 않았다.

[8]에서는 시스템 설계와 안전 활동을 통합하기 위해서 두 활동들 사이의 상호작용(interaction)을 핵심 요소로 고려한다. 하지만 시스템 설계와 안전 활동 사이에 데이터 교환이 양방향으로 이루어지는 것이 아니라 시스템 설계의 데이터를 안전활동에 제공하는 것만을 나타내고 있기 때문에 두 활동들 사이의 상호작용을 면밀히 고려했다고 볼 수 없다. 시스템 설계와 통합 프로세스를 제시한 연구들은 위와 같은 문제점을 지니며, 자동차나 항공분야에 적용하기 위한 통합 프로세스는 제시되었지만 철도시스템에 적용하기 위해 적합한 통합 프로세스 모델에 관한 연구는 거의 없다.

따라서 시스템 설계 활동과 안전성 분석 활동이 어떤 순서로 이루어지고, 각 활동에서 산출한 데이터들이 어떻게 양방향으로 교환되는지 명확하게 표현할 필요가 있다. 또한 철도시스템 설계에 안전성 분석 활동을 통합시킨 모델이 필요하다. 본 논문에서는 시스템 설계 활동과 안전성 분석 활동을 통합시킨 프로세스를 생성하는 것이 목적이다. 이 프로세스는 시스템 설계와 안전성 분석 활동의 순서와 데이터 교환을 명확하게 기술했기 때문에 안전중시 시스템인 철도시스템 개발의 프레임워크로서 적용시킬 수 있을 것이다.

2. 시스템 설계와 안전성 분석 프로세스의 정의

철도시스템 개발에 적용하기 위한 안전성 분석이 통합된 시스템 설계 프로세스를 생성하기 위해서, 먼저 시스템 설계 프로세스를 정의하고 철도시스템 안전성 분석 활동을 식별해야 한다. 이를 기반으로 두 프로세스가 어떤 정보들을 필요로 하는지 식별하고, 인터페이스를 정의한다. 마지막으로 시스템 설계 프로세스와 철도시스템 안전성 분석

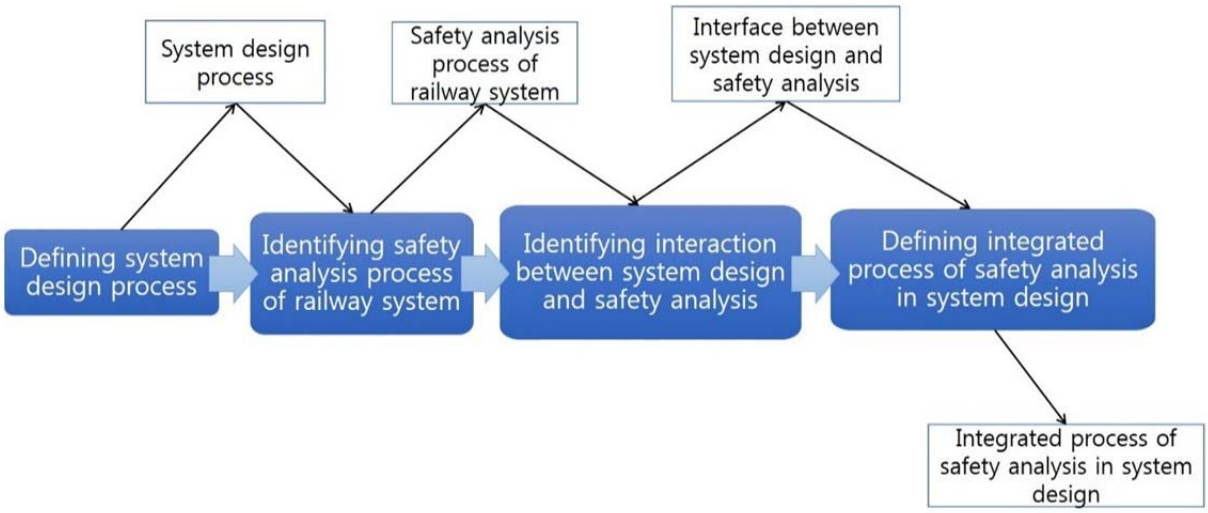

Fig. 2 Integrated procedure for safety analysis in system design.

활동을 제시하고, 인터페이스를 표현하여, 통합 프로세스를 정의하게 된다. [Fig. 2]은 위의 내용을 정리한 것이다.

ISO 15288, IEEE 1220 및 기타 시스템공학과 관련된 문헌에서는 시스템 개념설계의 핵심 활동을 종합하면, 요구사항 정의, 기능 아키텍처 정의 및 물리 아키텍처 정의로 나타날 수 있다. 요구사항을 정의하기 위해서는 니즈(Needs), 운영개념(Concept of Operation)과 같은 문서가 필요하고, 이를 기반으로 이해당사자 요구사항 및 시스템 요구사항을 도출한다. 요구사항 정의에서 도출된 시스템 요구사항을 기반으로 기능 아키텍처를 정의하게 된다. 기능 아키텍처는 시스템이 어떻게 거동하는지, 시스템의 기능 구조는 어떤 것이 있는지 식별할 수 있다. 물리 아키텍처 정의는 기능 아키텍처 정의 활동에서 정의한 기능 아키텍처를 기반으로 시스템의 각 기능이 어떤 물리적 구성요소에 할당되는지, 물리적 구성요소들은 어떤 계층 구조를 갖는지 식별하여 물리 아키텍처를 정의한다. 따라서 시스템 설계 프로세스는 다음의 세가지로 정의할 수 있다. 요구사항 정의, 기능 아키텍처 정의, 물리 아키텍처로 정의.

철도시스템의 안전성 분석을 수행하기 위해서는 반드시 대상시스템은 무엇인지, 시스템은 어떻게 거동하는지, 시스템은 어떤 물리적인 구조를 갖는지에 대한 시스템 설계 데이터를 필요로 한다. 즉, 안전성 분석을 수행하기 위해서는 시스템의 기능 아키텍처와 물리 아키텍처 정보를 활용해야 한다. [Fig. 1]은 안전성 분석을 상세하게 제시하고 있지만 시스템 정의와 위험원 제어(Hazard control) 활동은 실제적으로 시스템 설계에서 수행되는 활동이라고 볼 수 있다. 따라서 본 논문에서는 EN 50129의 안전성 분석 프로세스에서 시스템 설계 활동이라고 판단되는 시스템 정의와 위험원 제어 활동을 제거하여 안전성 분석 활동을 다음과 같이 정의했다. 위험원 식별, 위험원으로 인한 결과 분석, 리스크 평가, 안전 요구사항 정의.

3. 시스템 설계와 안전성 분석 활동의 통합 프로세스 생성

시스템 설계 프로세스와 철도시스템 안전성 분석 프로세스를 통합하기 위해서 두 프로세스를 표현하고, 두 프로세스 사이의 순서와 데이터 교환을 표현해야 한다. 우선 시스템 설계 프로세스를 계층별로 구분하여 표현했다. 시스템 설계 프로세스는 시스템, 서브시스템, 컴포넌트 수준의 요구사항 정의, 기능 아키텍처 정의, 물리 아키텍처 정의 활동이 존재한다. 각 시스템 설계의 산출물로 요구사항, 기능 아키텍처, 물리 아키텍처가 도출된다.

철도시스템의 안전성 분석 활동도 시스템 설계의 계층적인 관점을 적용하여 시스템, 서브시스템, 컴포넌트 수준의 설계 데이터를 활용하여 수행된다. 시스템 수준의 설계 데이터를 기반으로 안전성 분석 활동을 수행할 때, PHL(Preliminary Hazards Lists) 분석을 먼저 수행하게 된다. PHL은 가장 초기의 니즈와 운영개념을 기반으로 최상위 수준의 위험원을 식별하기 때문에 다음 단계의 위험원 분석을 수행하기 위한 사전 분석 기법으로 활용한다. 시스템 수준에서 PHL 분석이 먼저 수행되는 것을 제외하고, 모든 안전성 분석 활동은 위험원을 식별, 리스크 평가, 안전 요구사항 도출이 반복적으로 수행된다.

본 논문에서 제시한 시스템 설계와 안전성 분석 활동의 상호작용은 다음과 같다. 먼저, 니즈와 운영개념을 입력으로 받아 시스템 수준의 요구사항 분석과 PHL 분석을 동시에 수행한다. 두 번째, 시스템 수준의 시스템 설계 프로세스는 시스템 요구사항을 정의하고, 이를 기반으로 기능 아키텍처 정의, 기능 아키텍처를 기반으로 물리 아키텍처를 정의하게 된다. 세 번째, 시스템 수준의 안전성 분석 프로세스는 시스템 설계 프로세스가 진행됨과 동시에 PHL 분석을 수행한다. 네 번째, PHL과 시스템 기능 아키텍처, 물리 아키텍처를 기반으로 위험원을 식별하고, 위험원의 리스크를 평가하며, 리스크 평가 결과를 기반으로 안전 요구사항을 식별한다. 마지막으로 안전 요구사항은 다시 시스템 요구사항 정의 활동에 반영되어 처음에 나온 시스템 요구사항에 추가되거나 시스템 요구사항을 수정하게 된다. 위와 같은 활동은 시스템이 안전하다고 판단될 때까지 지속된다.

시스템 수준의 안전성이 보장되면, 다음으로 시스템 수준의 물리 아키텍처 관련 정보와 위험원 정보를 입력으로 하여 서브시스템 수준의 시스템 설계와 안전성 분석 활동이 수행된다. 서브시스템 수준에서 적용되는 활동도 시스템 수준에서 진행되는 활동과 같다. 서브시스템 수준에서 안전성이 보장되면, 같은 방식으로 컴포넌트 수준의 통합 프로세스 활동이 수행된다. [Fig. 3]은 본 논문에서 정의한 시스템 설계 프로세스와 안전성 분석 프로세스 및 두 프로세스 사이의 상호작용을 종합하여 표현한 통합 프로세스이다.

4. 결론

본 논문에서는 철도시스템 개발을 위해서 적용 가능한 시스템 설계 프로세스와 철도시스

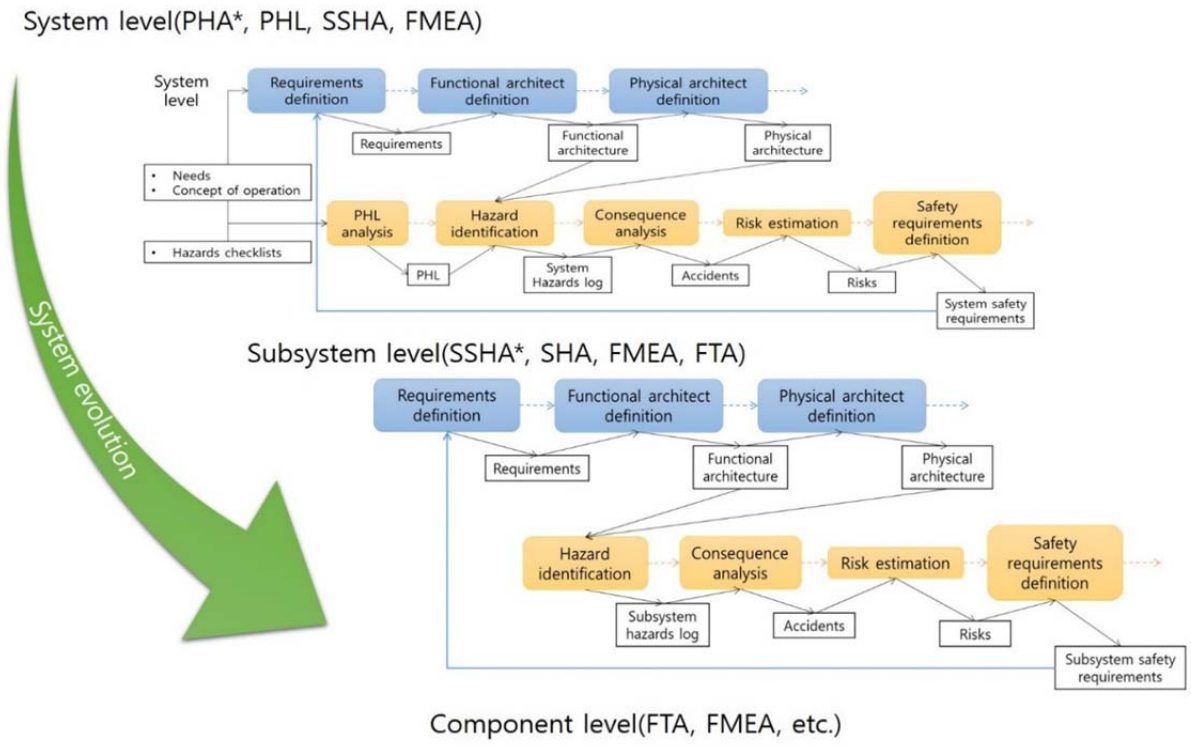

Fig. 3 Integrated process of safety analysis in system design.

템 안전성 분석 활동이 통합된 프로세스를 생성했다. 기존의 연구들에서 제시한 통합 프로세스는 두 프로세스 사이의 양방향 데이터 교환과 시스템의 각 계층수준에서 생성된 데이터를 명확하게 제시하지 못했다. 또한 철도분야에 적용 가능한 통합 프로세스 연구가 거의 없었다. 본 저자가 생성한 통합 프로세스는 위에서 언급한 문제들을 해결하고, 실제적으로 철도시스템 개발에서 안전성 분석과 시스템 설계 활동이 어떻게 수행되어야 하는지에 대한 프레임워크로 역할을 할 수 있을 것이다.

참고문헌

[1] Department of Defense Standard (2012) Department of Defense Practice: System Safety, MIL-STD-882E.

[2] IEC (2010) Functional safety of electrical/electronic/programmable electronic safety-related systems, IEC Standard, 61508.

[3] BSI (1999) Railway application – The specification and demonstration of reliability, availability, maintainability and safety (RAMS), BSI standard, BS EN 50126-1:1999.

[4] CENELEC (2003) Railway application – Communication, signaling and processing systems – Safety related electronic systems for signaling, CENELEC Standard, EN 50129:2003.

[5] O. El Ariss, D. Xu, and W. E. Wong (2011) Integrating safety analysis with functional modeling, *IEEE Transactions on Systems, Man and Cybernetics: Systems,* 41(4), pp. 610-624.

[6] Y. Papadopoulos and C. Grante (2005) Evolving car designs using model-based automated safety analysis and optimisation techniques, *The Jounal of Systems and Software,* 76(1), pp. 77-89.

[7] E. Denney, G. Pai, C. Ippolito, and R. Lee (2012) An integrated safety and systems engineering methodology for small unmanned aircraft systems, *in Proc. Infotech@Aerospace 2012,* Garden Grove, CA.

[8] H. Aboutaleb, M. Bouali, M. Adedjouma, and E. Suomalainen (2012) An integrated approach to implement system engineering and safety engineering processes: SASHA Project, *in Proc. European congress on Embedded Real Time Software and Systems(ERTS 2012),* Toulouse, France.