위험원 분석 결과를 반영한 시스템 안전 요구사항 생성에 관한 연구

김 재 철* · 이 재 천*
*아주대학교 시스템공학과

On the Development of Systems Safety Requirements Using Hazard Analysis Results

Jae-Chul Kim* · Jae-Chon Lee*
*Department of Systems Engineering, Ajou University

Abstract

Modern systems become more complex and the demand for systems safety goes up sharply. Thus, the proper handling of the safety requirements in the systems design is getting greatly increased attention these days. Hazard analysis has been one of the active areas of research in connection with systems safety. In this paper, we study a subject on how the hazard analysis results can be incorporated in the systems design.

To this end we set up a goal on how to systematically generate safety requirements that should reflect hazard analysis results and be implemented in the systems design and development. To do so, we first review the process for systems design and suggest the associated Model. Then the process and results of hazard analysis are analyzed and Modeled particularly with emphasis on the safety data. The resulting data Model incorporating both the hazard analysis and system life cycle is used in the generation of safety requirements.

Based on the developed data Model. the generation of the requirements, the construction of requirements DB, and the change management later on is demonstrated through the use of a computer-aided software tool.

Keywords : System Safety, Safety Requirement, Hazard Analysis, Data Model, System Life Cycle Model

1. 서 론

현대의 대형 시스템의 복잡도는 날로 증가하는 추세이다. 또한 이러한 대형 시스템은 그 사용자로 하여금 안전을 중요하게 생각하게 한다. 이를 위해 안전과 관련한 모든 활동은 시스템 설계 개념 초기부터 상세 설계, 시험, 그리고 시스템 폐기에 이르기까지 전체 시스템 수명주기 전반에서 수행되어야 한다[1].

이러한 관점에서 시스템공학은 안전을 다루기에 적합한 분야라고 할 수 있다. 시스템공학은 전 수명주기별 그리고 시스템의 계층적 관점에서 시스템이 갖추어야 하는 요구사항을 식별하고 이것이 구현되도록 노력하는 다학제적 접근이기 때문이다[2].

이러한 맥락에 따라, 시스템공학과 시스템 안전 활동의

† 교신저자: 이재천, 경기도 수원시 영통구 원천동 산 5번지 아주대학교 시스템공학과
Tel: 031-219-3941, E-mail: jaelee@ajou.ac.kr
2011년 10월 20일 접수; 2011년 12월 22일 수정본 접수; 2011년 12월 23일 게재확정

통합 수행에 대한 연구가 있었다. 시스템공학, 시스템 안전 분석, 그리고 인간 요소를 기반으로 한 통합 시스템 설계 방법을 개발한 연구가 참고문헌 [3]에 발표되어 있다. 또한 참고문헌 [4]에서는 이를 더욱 발전하여 시스템 전 수명주기에 걸쳐 필요한 통합 프로세스를 주장하였다.

이들 선행연구들의 공통적 주장은 시스템 전 수명주기 동안 안전관련 요소를 다루기 위한 방법을 찾고자 했다는 것이다. 그러나 선행연구에서는 수명주기 상의 시점에서 어떤 활동, 또는 어떤 위험원 분석 기법을 활용해야 하는지 만을 언급하고 있다.

시스템 안전을 고려하기 위해서는 시스템 개발에 있어 필요한 안전관련 정보를 식별하고 이를 지속적으로 관리하는 것이 중요하다. 안전관리를 위한 방법 중 하나는 안전 분야의 전문가 활용이 필수적이다. 그러나 이는 개발 비용 증가를 유도한다[5]. 이러한 점을 미루어보아 시스템 안전을 다루기 위해서는 일반 엔지니어들이 다루기 쉬어야 하며, 그 정보의 관계성을 한눈에 알 수 있어야 한다.

본 논문에서는 이를 위해 필수 안전관련 정보를 식별하고 이를 안전요구사항으로 정의하기위한 방법론을 제시하고자 한다. 본 논문에서는 이를 위해 시스템 수명주기 단계에서 고려되어야 할 정보를 식별하기 위한 데이터 모델(Data Model)을 제시한다. 제시되는 데이터 모델은 상위에서 언급한 문제에 활용되고 궁극적으로 대형 시스템의 다양한 정보들을 활용하도록 전산지원도구를 통한 데이터베이스(Data Base)구축의 기초가 된다.

본 논문의 구성은 다음과 같다. 서론에서는 본 연구의 사회 및 연구 동향과 필요성을 제시하였고, 2장에서는 관련 선행연구정리 및 연구 목표를 기술하여 문제정의를 언급하고, 3장에서는 본 연구의 내용인 데이터 모델과 시스템 수명주기 모델(System Life Cycle Model)을 기술한다. 4장은 본 논문에서 언급한 모델1의 적용 사례를 언급 하고, 5장에서 본 논문의 결과를 정리 및 요약 하였다.

2. 문제정의

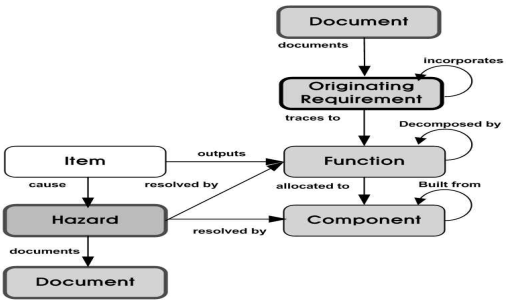
2.1 관련 선행연구

참고문헌 [3]과[4]에서는 공통적으로 시스템공학과 시스템 안전 활동의 통합 수행에 대한 연구를 주제로 하고 있다. 시스템공학, 시스템 안전 분석, 그리고 인간 요소를 기반으로 한 통합 시스템 설계 방법이 연구 결과물이 되고 있다.

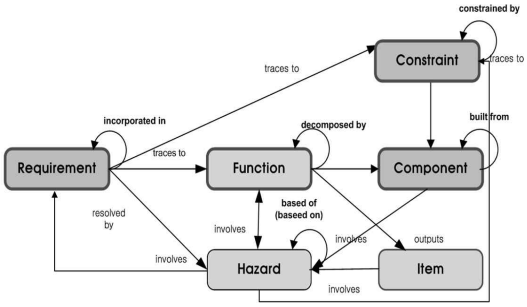
참고문헌 [3]은 시스템공학 프로세스를 요구사항 분석, 기능 분석, 합성, 그리고 시스템 분석 및 최적화로 정의하고 각 시스템 수준에 따른 위험원 분석 기법을 정의하였다. 참고문헌 [3]의 연구는 시스템공학 프로세스를 위험원 분석 기법을 활용하여 추가/개선하였다고 볼 수 있으며, 본 연구는 이를 기반으로 시스템공학과 시스템 안전 활동을 통합한 개발 방법을 제시한다.. 두 분야의 활동을 통합하기 위해서는, 두 분야의 활동 간의 인터페이스 정의가 중요하다. 인터페이스란 두 분야의 활동들이 어떠한 산출물들을 어느 시점에 주거나 받는지 정의한 것이다.

참고문헌 [4]는 안전 요구사항 반영을 위해, 시스템 수명주기와 시스템의 계층구조에 따라 어떠한 위험원 분석 결과를 시스템 설계에 반영해야 하는지 정의하였다.

[그림 1,2]의 데이터 모델은 기존 시스템공학의 활동을 지원하는 데이터 모델에서 “Hazard”라는 클래스를 추가 하여 이야기 하고 있다. 그러나 다양한 현존하는 위험원 분석 기법의 정보를 효과적으로 활용하고 이를 관리하기 위해서는 데이터 모델에서 위험 및 안전에 관한 클래스가 상세하게 기술될 필요가 있다.



[그림 1] 참고문헌[3]의 데이터 모델



[그림 2] 선행연구[4] 의 데이터 모델

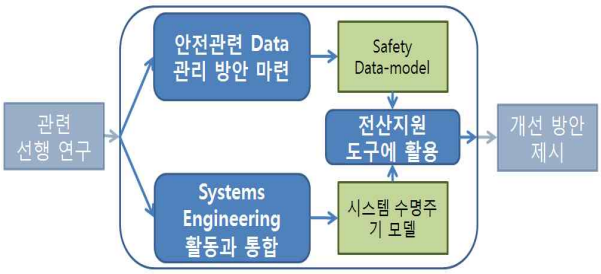
2.2 연구 목표 및 범위

상위의 선행 연구 분석을 통해 안전 이라는 것은 전 수명주기 적으로 다루어 져야 하고, 이제는 더 이상 특수 공학이 아닌 일반 엔지니어들 또한 안전 요소들을 다룰 방안이 필요하다.

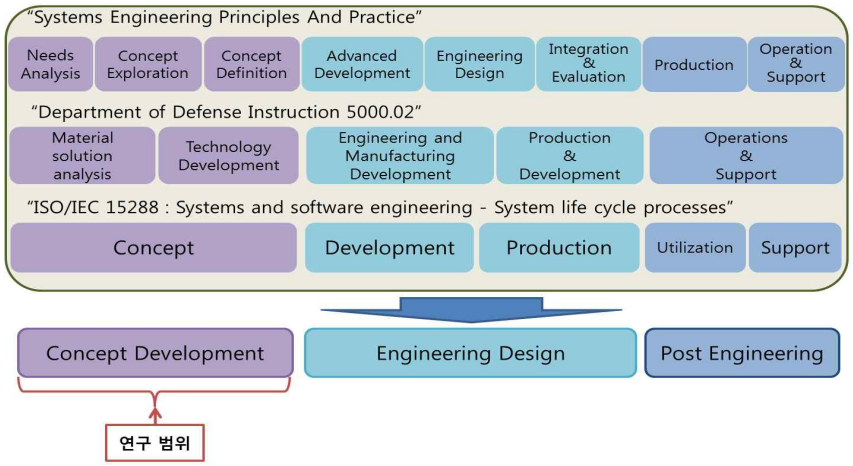
본 연구는 이를 위해 안전 관리를 위한 상세한 데이터 모델을 제시하도록 한다. 상위의 문제를 해결하기 위해서 제시된 연구 내용은 시스템 공학 관점에서 안전을 다루어야 하고, 일반 엔지니어들 또한 다룰 만한 수준이어야 한다.

이를 위해 안전 관리를 위한 데이터 모델과 시스템 수명주기 모델을 제안한다. 데이터 모델은 안전 관리를 위해 필요한 정보들을 정의하고 이들 간의 관계를 도식화 한다. 또한 시스템 수명주기 모델은 이들 정보들이 언제 어떤 활동에 활용되어야 하는지를 명시하도록 한다.

이러한 모델의 필요성은 전산도구를 활용하여 데이터베이스를 구축하는데 있다. 안전을 위해 다루어야 할 데이터가 다양하고 시스템의 구조가 복잡할수록 그들 간의 관계식별은 매우 중요하다. 따라서 본 연구에서 제시되는 모델들은 시스템개발 시 필요한 데이터베이스 구축의 스키마(Schema)로 활용되어 질 것이다. [그림 3]은 본 연구의 방법을 도식화하였다.



[그림 3] 연구 목표 개념도



[그림 4] 시스템 수명주기 및 연구 범위

<표 1> 위험원 분석의 Data[1]

Hazard analysis	Output		Hazard analysis	Output	
Preliminary Hazard List analysis (PHL)	-(위험,재해)핵심 안전요소 및 원인요소 - 위험 - 영향 - 시스템 항목	-수정 조치 제안(위험 감소/제거를 위한 안전 가이드라인 및 제안) - 결론	HAZard and OPerability analysis (HAZOP)	- 기능 /목적 - 파라미터 - 가이드워드 - 결과	- 원인 - 위험 - 리스크 - 조치
Functional Hazard Analysis (FHA)	- 고장형태 - 고장률 - 원인 - 영향	- 검지방법 - 조치 - 위험 - 리스크	Sub-System Hazard analysis (SSHA)	- 위험 - 원인 - 영향	- 모드 - 초기리스크 - 조치 - 조치후 리스크
Preliminary Hazard analysis (PHA)	- 시스템 안전 요구사항 (SSR) - 위험 - 원인	- 모드 - 초기리스크 - 조치 - 조치후 리스크	System Hazard Analysis (SHA)	- 위험 - 원인 - 영향	- 재해 - 리스크 - 원인 요소 - 시스템 안전 요구사항

또한 본 연구는 범위 영역을 [그림 4]와 같이 설정하였다. 일반적으로 시스템공학에서 시스템의 수명주기는 여러 모습으로 제시되고 있다. 그러나 이들을 크게 3가지 단계로 구분할 수 있으며 각 단계의 정의는 다음과 같다.

- Concept Development : 시스템의 요구를 정의 하고 이를 해결할 수 있는 여러 대안에 대한 검토 및 근거를 바탕으로 하나의 대안을 선택하는 과정.
- Engineering Design : 선택된 대안을 바탕으로 물리적 설계가 이루어지는 단계.
- Post Engineering : 시스템의 설계완료 후 사용자의 사용에 대하여 지원 및 폐기에 관련한 단계.

본 논문은 시스템 안전 요구사항의 정의를 다룬 것으로 Concept Development가 해당 단계가 될 것이다. 따라서 시스템 개발에 있어서 요구사항을 도출하는 과정에서 발생 및 요구되는 안전 관련 정보들을 정의하고 이들의 관계를 고려하는 것은 본 논문이 범위로 설정하였다. 이를 [그림 4]와 같이 표현 할 수 있다 [6][7][8].

3. Modeling

3.1 안전 요구사항 데이터 모델

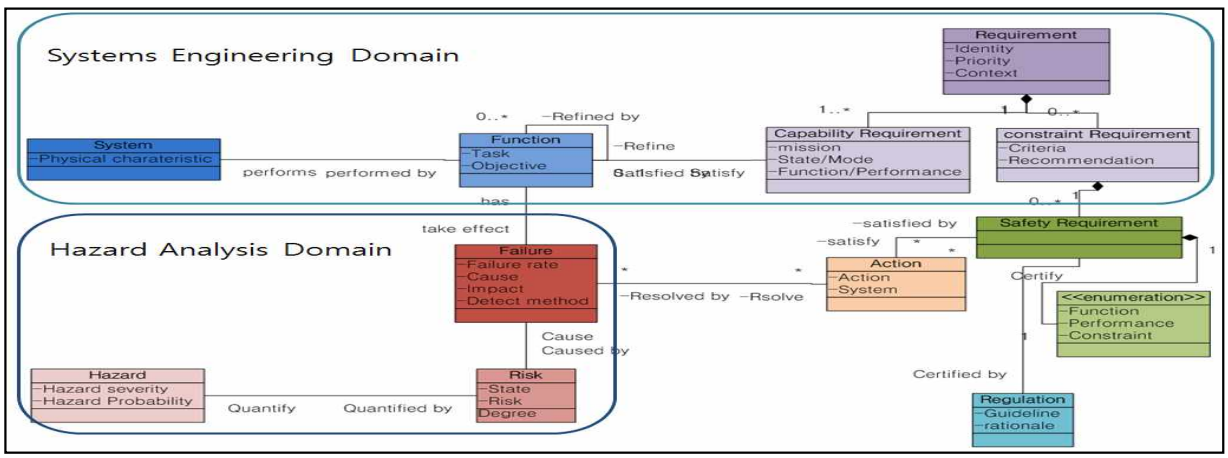
2.1장에서 선행연구에 제시된 위험원 분석을 고려한 시스템 설계의 데이터 모델을 언급하였다. 그러나 선행연구 모두에서 시스템 설계 요소에 “Hazard”라는 하나의 요소만 추가하였다. 이를 통해서 위험원 분석 활동과 시스템 설계와 연관을 짓기가 쉽지 않다.

본 논문에서 모델을 개발하기 위해, 우리는 다음과 같은 절차를 수립하였다. 각각의 활동을 통한 결과들이 모델에 반영되었다.

1) 각 위험원 분석 활동을 통해 얻어지는 정보를 식별한다.
2) 각 공통된 입출력을 클래스로 정의한다.
3) 각 클래스 별 속성을 정의한다.
4) 클래스 간의 상관관계를 정의한다.
5) 기존의 SE 데이터 모델과 통합하여 정리한다.

<표 1>는 각 위험원 분석 활동을 통해 얻어지는 정보를 식별한 것이다. 각 위험원 분석 기법에 의해 얻어지는 정보들은 각 활동에 고유한 정보가 있지만, 공통된 정보들이 많았다. 이는 각 정보들은 지속적으로 변경 관리 되어야 한다는 의미이다. 이러한 정보들을 클래스로 식별하여 UML(Unified Modeling Language)[10]의 Class Diagram으로 표현 하였다. <표 2>에 정리된 것과 같이 핵심 정보인 위험원, 리스크, 결함을 위험원 분석 정보의 핵심 클래스로 정의하였다.

또한 이와 시스템공학 분야의 클래스와 통합한 데이터 모델은 [그림 5]과 같다. 각 데이터의 속성을 정의하였고, 이들 간의 관계를 도식화 한 데이터 모델은 상위 수준에서 일반화 된 것으로 이를 기반으로 각 시스템에 맞는 상세화해 나아가는 방식으로 활용한다.



[그림 5] 시스템 공학 분야와 위험원 관리 분야의 통합 데이터 모델

<표 2> 데이터 모델의 클래스와 속성

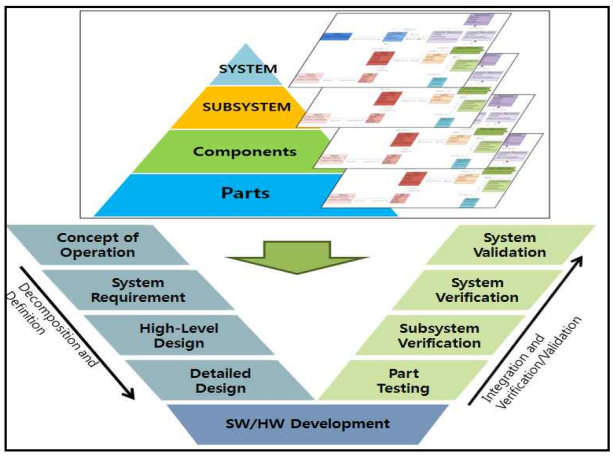
Class	Definition	Attribute
위험원 (Hazard)	관련 개념이 존재하여 발생했던 위험이나, 상위 수준에서 예상되는 위험상황	- 예상 피해 정도 - 예상 발생 빈도
리스크 (Risk)	위험원(Hazard)의 발생빈도 및 확률을 수치적으로 표현한 것	- 위험도 - 상태
결함 (Failure)	기능의 목표달성 실패, 고장 또는 결함	- 발생확률 - 원인 - 탐지 방법

3.2 시스템 수명주기 모델

시스템 수명주기 모델은 데이터 모델에서 식별된 정보들이 시스템이 개발되는 수명주기 동안 언제 활용되어야 하는지를 나타낸 모델이다. 명확히 따라야 하는 것은 아니지만, 일반 엔지니어들이 안전과 관련된 활동을 하고 이를 활용하는 데에 필요한 정보들로 구성하였다.

이에 대한 접근은 3.1에서 언급한 데이터 모델을 시스템의 계층적으로 적용하는 것으로 시작하였다. [그림 6]에서 상단의 표현은 이를 보여주는 것으로, 개발된 데이터 모델은 시스템의 상세화가 진행되면서 그 정보 또한 상세화가 되어간다. 이는 하단에 표현된 Vee-Model에 그대로 적용할 수 있다.

Vee-Model은 시스템공학의 개념을 계층적, 그리고 시간적 개념으로 표현한 모델이다. 본 연구에서는 데이터 모델을 반복적으로 활용한다.

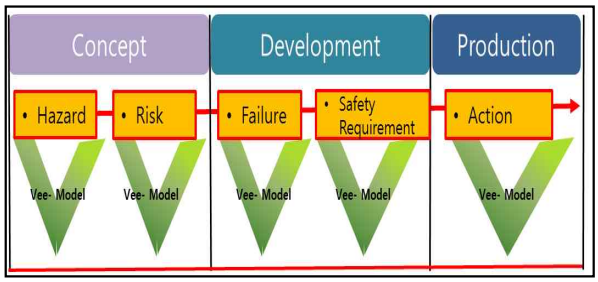


[그림 6] 계층적 데이터 모델 활용과 Vee-Model

시스템 수명주기 모델에 이를 적용하기 위해 Vee-Model을 적용한 전체적인 내용은 [그림 7]과 같으며, 본 논문의 연구 범위 설정에 따라 요구사항 분석 부분까지만 정의하였다.

Model은 가장 상단에 시스템 수명주기를 도식화 하였다. 두 번째로는 각 수명주기 단계별 활동을 언급하고, 각 활동별로 Vee-Model이 적용되는 것이다. 각 활동에서 중요하게 식별되어야 하는 정보를 중간에 표시하였다.

본 Model은 초반에 언급한 연구 범위 내에서 표현되어졌고, 일반 엔지니어들이 쉽게 활용할 수 있도록 상위 수준의 개념을 표현하였다. 추후에 연구 범위를 확대하여 더 개발되어야 하고 각 활동 별 상세화가 더 진행되어야 한다.



[그림 7] 시스템 수명주기 모델

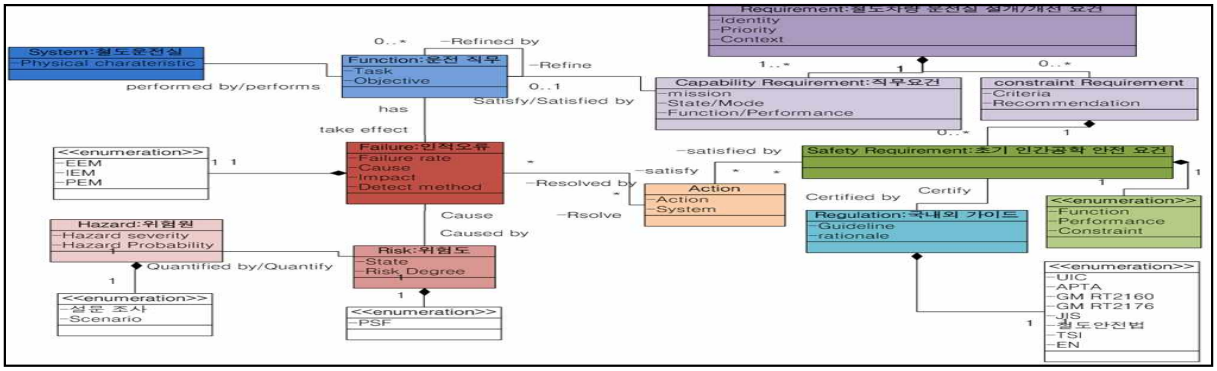
4. 안전요구사항 생성 사례 연구

4.1 철도차량 운전실

우리나라 열차사고 요인 별 현황을 살펴보면 기기취급 불량, 시설 및 장비의 점검, 보수소홀, 운전취급 불량 등 취급부주의로 인한 인적 과실이 42.9%를 차지하며, 그 중 기관사의 취급부주의 사고가 66.7%로 상당한 비중을 차지하고 있다[11].

따라서 이러한 사고 방지를 위해서 철도차량 운전실에 대한 구조개선 및 인간공학적 설계에 대한 연구 필요성을 언급하였다[12][13].

따라서 철도차량 운전사의 인적 오류를 발생시킬 수 있는 요인을 파악하고 이를 개설할 수 있는 요구사항을 도출하여 설계에 반영해야 한다.



[그림 8] 철도차량 운전실 개선을 위한 안전요구사항 데이터 모델

4.2 철도차량 운전실 데이터 모델

이를 위해 3장에서 언급한 데이터 모델을 바탕으로 철도차량 운전실 개선에 대한 요구사항 도출에 활용하여 보았다. 다음 [그림 8]은 철도차량 운전실의 예를 포함한 데이터 모델이다. 이를 통해 초기에 필요한 데이터a를 식별하였고 이를 수정 보완 하며, 전체적인 흐름을 파악 할 수 있었다.

철도차량 운전실에서 발생하는 운전 직무를 바탕으로 발생할 수 있는 인적오류를 설정하고 이들의 위험원과 발생빈도를 도출하여 안전 요구사항의 개발과정에 활용하였다.

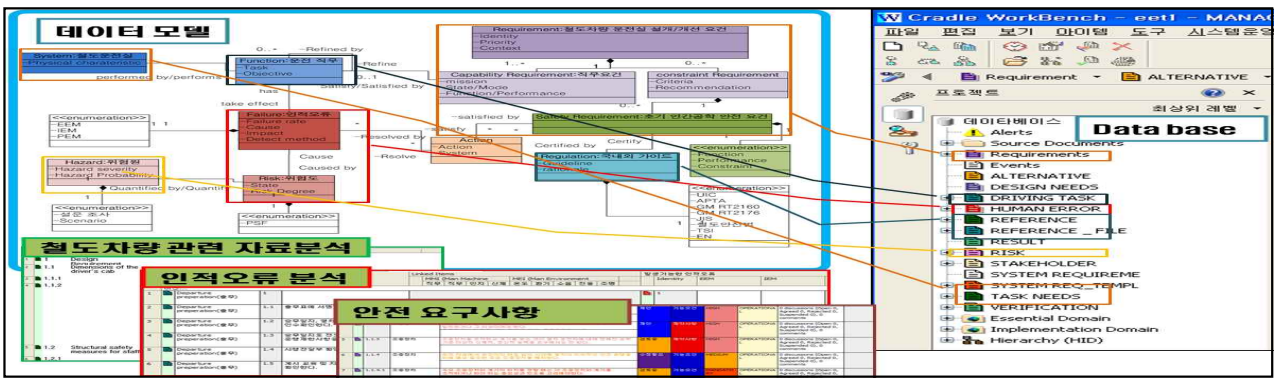
4.3 개발된 데이터 모델을 활용한 Data Base 구축

상위의 결과를 시스템공학 전산지원 도구인 Cradle을 활용하여 안전 요구사항을 관리하는 데이터베이스를 구축하였다. 본 연구에서 언급한 데이터 모델은 전산지원도구의 스키마를 이루는 기초가 되었고, 본 사례 연구에서도 적용하였다.

이를 바탕으로 구축한 데이터베이스는 그림9와 같다. 각 데이터 모델의 클래스를 데이터베이스에 반영하였으며 이들은 각 정보를 확인하는데 활용된다.

<표 3>는 데이터 모델의 클래스들이 반영된 데이터베이스의 Item에 대한 명칭과 속성 및 설명을 정리한 것이다. 또한 이를 활용 및 관리 하기위한 프로세스 또한 개발하여 적용하였다. 구축된 데이터베이스는 각 정보의 기록과 변경관리를 용이하게 할 수 있다 또한 가장 중요한 역할인 각 정보의 상호 관계를 링크 기능을 통해 관리할 수 있도록 하였다. 궁극적으로 이들을 활용하여 관련 사항의 도식화 및 문서 자동출력 하도록 구축하였다.

본 데이터베이스의 활용을 통해 요구사항의 변경 및 수정 보완 관리가 용이하고, 또한 인과관계에 있는 정보들 간의 추적성 확인에도 용이하다.



[그림 9] 데이터 모델을 활용하여 구축한 전산지원 데이터베이스

<표 3> 데이터베이스의 Item

Item 명	속성	속성 설명
Reference (참고문헌)	이름	참고문헌의 이름 또는 문단 이름
	설명	참고문헌의 내용
Requirement (요구사항)	이름	요구사항 이름
	설명	요구사항 설명
	상태	요구사항 분석 진행 상태
	타입	요구사항 구분
Task Need (직무 요건)	이름	직무 요건 이름
	설명	검증 이벤트 설명
	가중치	직무 부하 가중치
	인터페이스	직무 인터페이스
Reference _file (참고문헌 파일)	이름	참고문헌 이름
	설명	파일에 대한 설명
Driving Task (운전 직무)	이름	운전 직무 이름
	설명	직무의 설명
	기기 구조	해당직무가 시행되는 기기
	문서 번호	문서 번호
Human Error (인적오류)	이름	인적오류 이름
	내/외적 요인	내/외부 요인 영향
	심리적 요인	심리적 요인 영향
	인적오류 영향인자	영향을 미치는 인자

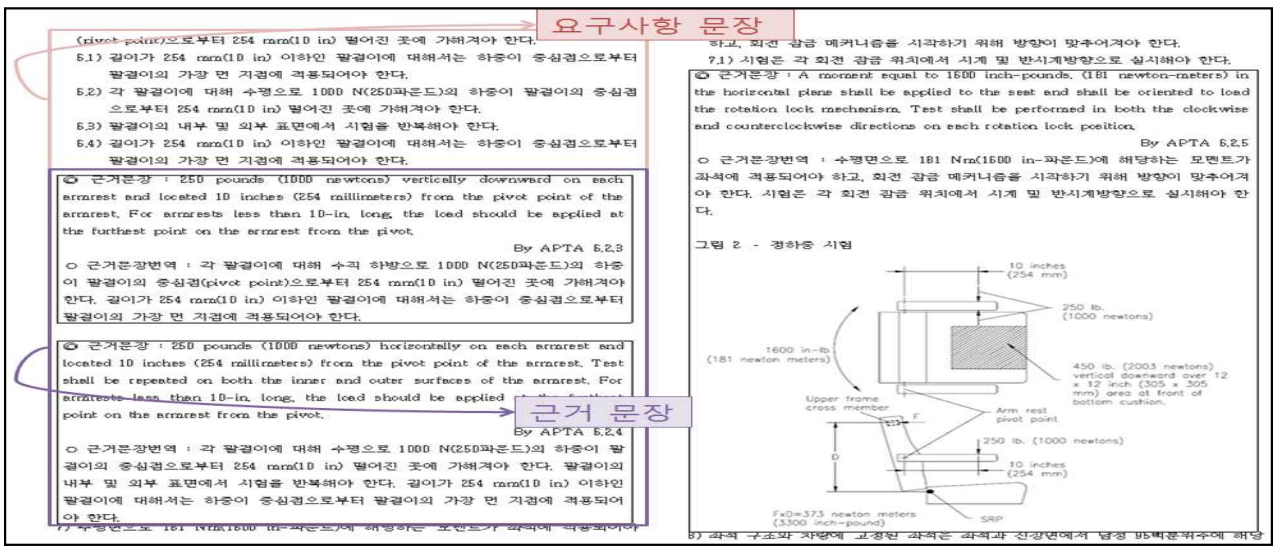
4.4 철도차량 운전실 개선을 위한 안전 요구사항

4.3.의 데이터베이스에서 설문과 자료조사를 통한 직무 분석 및 인적오류의 결과를 현존하는 권장사항 및 가이드와의 추적성을 식별하여 약 240여개의 초기 안전 요구사항을 개발 할 수 있었다.

그 양식은 [그림 10]과 같다. 이들의 구조화를 위하여 4계층으로 분류하였다. 상세한 분류 계층의 내용은 <표 4>와 같다. 상위 수준에서는 운전실의 구조와 작업환경으로 항목화 하였고 이들을 각각 세분화하여 구조화하였다. 각 요구사항 문서는 해당 요구사항 문장별 가이드 및 법령의 근거 문장이 기술되도록 구성되어 있다.

<표 4> 철도차량운전실 안전요구사항 분류체계

대분류	중분류	소분류
운전실 구조 및 장치	제어대	제어장치
		디스플레이
		안전 및 경보장치
		입력장치
		대화식 설계
		자동화
		음성 커뮤니케이션
	운전실 배치	접근 및 진입
		운전실 전방시야
		좌석
		창문, 바닥, 문
운전실 작업환경	조명과 밝기	
	난방	
	환기	
	냉방	
	소음	
	진동	
	색상과 표면 코팅	



[그림 10] 정리된 철도차량 운전실 안전요구사항 문서

5. 결 론

시스템의 안전을 위한 연구는 활발히 이루어져 왔다. 그것의 일환으로 위험원 분석이라는 분야가 활발해 졌다. 이러한 여러 분석활동의 결과들이 시스템 개발의 시작에서부터 끝까지 활용이 되어야 하고, 이러한 활동이 특수 분야로서가 아니라 필수 분야로 적용되어야 할 필요가 있다. 본 연구에서는 데이터 모델을 제시함으로써, 위험원 분석의 결과를 안전 요구사항을 반영하기 위한 방안을 마련하였다. 또한 이들의 활동과 정보가 언제 필요하고 활용되어야 하는 지를 시스템 수명주기 모델을 통해 주장하였다. 그리고 이러한 결과를 사례를 통해 안전 요구사항이 도출 되는 과정을 나타내었다.

이 모델을 통한 안전 관리의 원칙은 시스템공학 적용과 동일하다. 1) 계층적 접근 2) 반복적 활동 3) 피드백 설계가 그것이다.

본 논문에서는 초반에 언급하였듯이 안전 요구사항 도출과정에서 위험원 분석 결과의 반영에 대하여 정리하였다. 추후에는 이 요구사항을 바탕으로 시스템 설계 상황에서 정보들을 지속적 관리 및 적용을 위한 방법론이 필요하다. 설계 단계에서는 단순한 관리 모델 이상의 것이 필요할 것이다.

6. 참 고 문 헌

[1] I. Clifton A. Ericson, “Hazard analysis techniques for system safety.”, Hoboken, New Jersey: John Wiley & Sons, Inc., (2005)

[2] “A guide for system life cycle processes and activities INCOSE”, handbook, v3.2, (2010)

[3] J. Y. Park and Y. W. Park, “Model-based concurrent systems design for safety.”, Concurrent Engineering-Research and Applications, vol. 12, pp. 287-294, Dec (2004)

[4] 윤재한, 이재천, "안전중시 시스템의 설계 환경 구축에 관한 연구", 대한안전경영과학회지, 대한안전경영과학회, 11권 3호, (2009), 19-26

[5] D.D. Black, M.E.C. Hull, and K. Jackson, "Systems engineering and safety - a framework," The Institution of Engineering and Technology, vol. 5, no. 1, (2010), 43-53

[6] A. Kossiakoff and W. N. Sweet, “Systems engineering principles and practice”, Hoboken, N.J.: Wiley-Interscience, (2003)

[7] “Operation of the Defense Acquisition System", US DoD Instruction Number 5000.2 (DoD I 5000.1), 12 May (2003)

[8] “Systems engineering — System life cycle processes, in ISO/IEC 15288:2002(E)”: International Organization for Standardization, (2002)

[9] “Practice for System Safety: ESOH Risk Management Methodology for Systems Engineering”, MIL-STD-882D, (2000)

[10] UML (Unified Modeling Language)2.4". Omg.org. Retrieved (2011)

[11] “고속철도 안전기술 개발을 위한 조사연구," 한국기계연구원, (1997)

[12] 최은미, 김영국, 김종봉, “철도차량 운전실 승차감에 관한 연구", 한국철도학회 학술발표대회논문집, 한국철도학회, (2008), 1389-1396

[13] 임재은, 정도원, 김치태, “철도차량 운전실제어대 설계기준 마련 연구", 한국철도학회 학술발표대회 논문집, 한국철도학회, (2008), 2119-2124

저 자 소 개

김 재 철

현 아주대학교 시스템공학과 박사과정, 시스템 개발 시 활용을 위한 Model 및 시스템공학 프로세스 관리 관련 과제 수행, 관심분야는 모델기반 시스템공학, Systems Safety, Modeling & Simulation 등

주소: 수원시 영통구 원천동 산5번지 아주대학교 성호관 243호

이 재 천

현 아주대학교 시스템공학과 정교수. 서울대학교 전자공학과에서 공학사, KAIST 전기 및 전자공학과에서 공학석사 및 박사 학위를 취득. 미국 MIT에서 Post-Doc을 수행하였으며, Univ. of California (Santa Barbara)에서 초빙연구원, 캐나다 Univ. of Victoria (BC)에서 방문교수, KIST에서 책임연구원 재직. 이 후 미국 Stanford Univ. 방문교수 역임. 현재 연구 및 교육 관심분야는 시스템공학 및 Systems Safety에의 응용 등.

주소: 수원시 영통구 원천동 산5번지 아주대학교 서관 309호