안전 요구사항의 추적성 구현을 통한 시험/평가 계획서의 효율적 개발

윤 재 한* · 이 재 천*
*아주대학교 시스템공학과

On an Efficient Development of the Test & Evaluation Plan through the insured Traceability of the Safety Requirements

Jae-Han Yoon* · Jae-Chon Lee*
*Department of Systems Engineering, Ajou University

Abstract

It is well known that the test and evaluation plan (TEP) is very crucial in the successful development of safety-critical systems. As such, this paper discusses an approach to the development of the TEP for a system that should meet safety requirements in the systems development process. It is studied how to incorporate the result of preliminary hazard analysis (PHA) in generating the safety requirements.

It is also discussed how to deal with them when the system requirements (i.e., functions, performance, constraints, components, etc) and the safety requirements are integrated into one model. While doing so, we have constructed the required traceability among them, which is necessary and very useful when the safety requirements need to be corrected or be changed. The use of the traceability makes it possible to easily check out whether and how the safety requirements are properly incorporated in the system design process.

Furthermore, without the verified traceability, the system cannot be changed or upgraded later. In order to implement the model on a computer-aided tool, we have constructed a database (DB) schema. As a result, the implemented model/DB allows to automatically generate TEP which can be used to measure the performance and safety level of the developed system.

Keywords : System Safety, Safety Requirements, Preliminary Hazard Analysis (PHA), Test & Evaluation Plan (TEP), Traceability

1. 서 론

현대의 많은 시스템들은 점점 복잡화, 대형화되어 가는 추세이다. 이런 대형 복합 시스템들은 여러 문제가 있지만, 최근 들어 가장 화두가 되는 문제 중 하나는 시스템의 안전이라고 할 수 있다. 시스템은 주변 환경에 대해 악영향을 최소한으로 미치며, 시스템 사용자에 대한 인적 피해 없이 그리고 시스템의 별다른 고장 없이 운영될 필요성이 있다.

시스템의 안전성 확보 문제는 대형 공공 시스템으로부터 군사용 시스템, 민수용 제품 등 규모 및 용도의 다양한 범위에서 제기되고 있다. 우주 항공 및 고속철도 등의 대형복합시스템 뿐만 아니라 최근의 휴대품 폭발 사고 등 공산품에서도 안전성 문제가 제기되고 있는데, 특히 PL법으로 불리는 생산자 배상책임법도 중요한 이유가 되고 있다.

시스템 안전을 확보하기 위한 다양한 방법론들을 통해 시스템의 위험요소를 식별하고 제거하는 노력이 이루어지고 있다. 시스템 안전을 위한 활동에서 가장 중요한 개념은 초기에 시스템의 위험요소를 판별하는 것이다 [1].

2007년 11월 접수; 2007년 12월 수정본 접수; 2007년 12월 게재확정

시스템을 개념단계에서부터 시스템의 위험원 (Hazard)을 파악하고 시스템이 개발 주기 동안 진화됨에 따라 시스템의 위험이 제거되고 경감되도록 시스템을 개발해야 한다 [1]. 즉, 시스템의 설계 시 요구사항 단계부터 안전 분석을 통해 안전 요구사항들을 수집하고, 안전 요구사항으로부터 시스템 기능 및 물리적 구성품 (Component)에 대한 안전 설계를 해야 한다. 그리고 각 요구사항을 검증하기 위한 검증 요구사항을 작성하고 검증 요구사항을 바탕으로 시스템에 대해 안전 시험/평가를 단계별로 수행함으로써 시스템의 안전을 확보하였음을 확인해야한다.

안전 요구사항은 PHA (Preliminary Hazard Analysis: 예비 위험원 분석)을 통해서 초기본이 구성된다 [3]. 이는 점차 진화하여 검증 요구사항 개발에 사용되고 시스템 기능 및 구성품에 대한 안전 검증 기준으로써 시험/평가에 활용된다. 그리고 시험/평가를 통해 오류가 발생하였을 때 요구사항과 설계를 변경할 수 있도록, 시험/평가는 요구사항과 설계와 추적성을 확보해야만 한다 [2]. 즉, 올바른 안전 확인을 위한 안전 시험/평가는 PHA에서부터 시험/평가까지 추적성을 확보하고 의도된 안전 목표를 누락 없이 검증해야 한다. 본 논문에서는 PHA로부터 안전 시험/평가까지의 추적성 확보 방안을 제시하고, 이를 통해 시험/평가를 계획서 (안전 시험/평가 포함)를 개발함으로써, 시스템의 안전 검증 방안을 제시하고자 한다.

논문은 본 서론에 이어 제 2장에서는 추적성 구현의 중요성, 제 3장에서는 추적성 구현, 제 4장에서는 시험/평가 계획서 개발, 그리고 제 5장에서는 철도시스템의 시험/평가 계획서 개발을 기술한다. 마지막으로 제 6장에서는 본 연구의 결론을 맺는다.

2. 추적성 구현 및 TEP 개발의 중요성

2.1 추적성 구현의 개념

추적성이란 요구사항, 설계, 그리고 최종 시스템의 구현간의 관계를 제공하는 것을 말한다 [3]. 그리고 추적성을 확보한다는 것은 시스템 개발에 있어서 특정 산출물과 해당 산출물이 나오기 위한 근거 자료의 연관성을 기록하고 관리함을 의미한다.

본 논문에서는 추적성의 범위를 PHA에서부터 안전 요구사항, 시스템 기능, 성능, 제약사항, 구성품, 검증 요구사항, 그리고 시험/평가까지로 정한다. 즉, 본 논문에서의 추적성 구현이란, 1) 안전 요구사항이 PHA의 어떤 결과로부터 발생하였는지, 2) 시스템 기능, 성능, 제약사항, 구성품은 어떠한 요구사항 (안전 요구사항 포함)으로부터 발생하였는지, 3) 최종적으로 시험/평가를 통해 시스템의 어떠한 요구사항 (안전 및 검증 요구사항 포함), 기능, 성능, 제약사항, 그리고 구성품을 검증할 것인지 제공함을 의미한다.

2.2 추적성 구현의 필요성 및 활용

요구사항의 추적성을 확보하면 시스템 구성요소들에 대한 요구사항 간의 추적성 기록은 고객과 기업의 관리진에게 잠재적인 비용에 대한 통찰력을 제공함으로써 개발 팀의 공정을 모니터하는 기회를 제공한다 [4].

또한, 고객의 요구를 만족하기 위한 노력들에 팀의 중점 사항을 관리하는데 도움을 주며 변경사항을 평가할 때도 도움을 준다 [4].

이와 같은 맥락에서, PHA 및 안전 요구사항 추적성 분석은 시스템의 모든 위험원 요소들이 각각의 위험도를 경감시킬 수 있는 요구사항으로 설계되었는지를 제공한다. 또한 시험/평가를 통해 관련된 안전 요구사항을 시스템 및 시스템 요소들이 모두 평가되는지를 제공한다. 이 두 가지 추적성 분석을 통해, 계획한 시험/평가가 시스템이 의도한 안전 목표의 달성을 평가할 수 있는지가 제공된다.

2.3 TEP의 중요성

TEP (Test and Evaluation Plan: 시험/평가 계획서)는 시스템 검증 및 확인 (Verification and Validation)을 위해 작성하고 계획에 따라 시스템을 검증 및 확인한다 [5]. 시험/평가 (Test and Evaluation)는 절충 분석, 위험도 감소, 그리고 요구사항 개선을 지원하는 데이터를 제공하는 의사 결정 절차의 중요한 요소이다 [6]. 신중하고 완벽한 계획은 성공적인 시험 프로그램을 보장하진 않지만, 부적절한 계획은 심각한 시험 문제들, 시스템 성능 저하, 비용 초과를 초래한다 [6].

즉, 시스템의 의도된 안전도를 최대화하고 이와 관련한 비용 초과 및 문제를 최소화하기 위해, 적절한 시험/평가 계획은 중요하다.

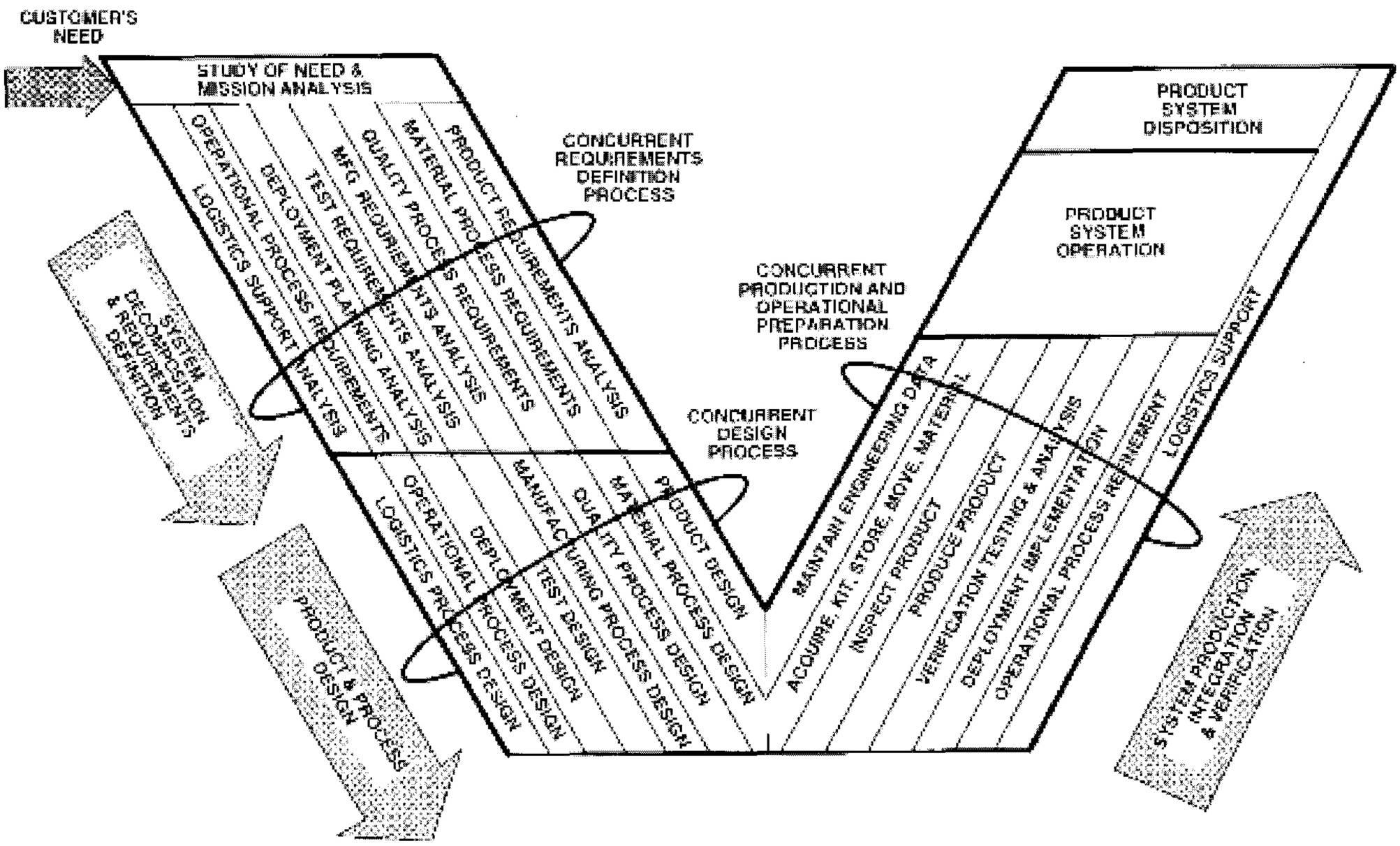
3. 추적성의 구현

3.1 시스템 개발 절차에서의 추적성 구현

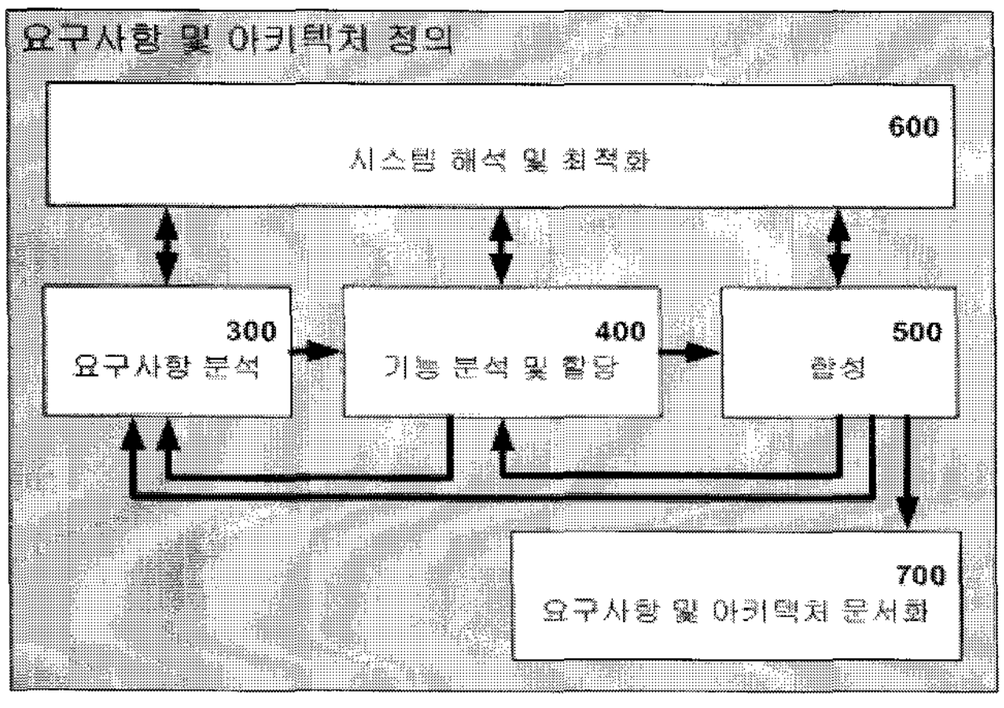
시스템 개발에서는 여러 데이터들을 문서화하게 된다. 이 때, 각종 결과물들과 그 결과물들에 반영된 기

반 데이터들의 관계를 기록/관리하는 것으로 추적성이 기록/관리된다. 즉, 시스템 개발 절차에 따른 각 활동에 따라 기반 데이터와 결과 데이터가 정해지고 이들 간의 추적성 관리가 이루어진다. 본 논문에서는 시스템 개발을 <그림 1>[7]의 Vee Model을 근간으로 수행함을 간주한다. 시스템은 여러 단계 또는 수준으로 요구사항 및 설계가 개발되고, 각 단계에 해당하는 검증 및 확인 절차가 수행된다. 즉, 각 수준에서 요구사항, 설계와 검증 및 확인 데이터들 간에 추적성을 구현한다.

<그림 1>의 각 단계마다 그림 2 [5]의 절차에 따라 시스템을 설계한다. <그림 2>에 따라 시스템 개발 시 발생하는 시스템 설계 요소들은 시스템의 요구사항, 기능, 구성품, 그리고 시스템을 설명하는 각 수준의 규격서가 발생하게 되며, <그림 2>에서 보이는 화살표에 의거하여 각 활동마다 발생하는 산출물들이 다음 활동 데이터와 추적성을 구현한다. 특히, 시스템의 안전을 확보하기 위해, 요구사항 분석 활동에서 PHA (Preliminary Hazard Analysis: 예비 위험원 분석)을 통해 안전 요구사항을 도출하고 이들 사이의 추적성을 구현한다.



<그림 1> 설계 프로세스에 적용한 시스템공학 Vee Model



<그림 2> 추적성 구현을 위한 시스템 설계 프로세스

3.2 데이터들의 추적 관계를 정의하기 위한 DB 스키마 (Schema) 설계

스키마란 데이터를 관리하기 위한 DB의 전체적인 데이터 골격 설계를 나타낸다 [8]. DB 설계는 데이터들을 정의하고 그들의 관계를 정의하는데 이는 본 논문에서추적성 모델과 같은 맥락이다. 추적 관계를 정의하고 차후 전산지원관리를 위하여 DB 스키마를 설계하였다. 스키마는 일반적으로 ER Model [9]을 통해 많이 표현한다. ER Model은 개체 (Entity)와 개체 간의 관계를 표현하는 모델이며, 여기서 관계는 바로 추적성 확보가 필요한 데이터 간의 추적 관계이다.

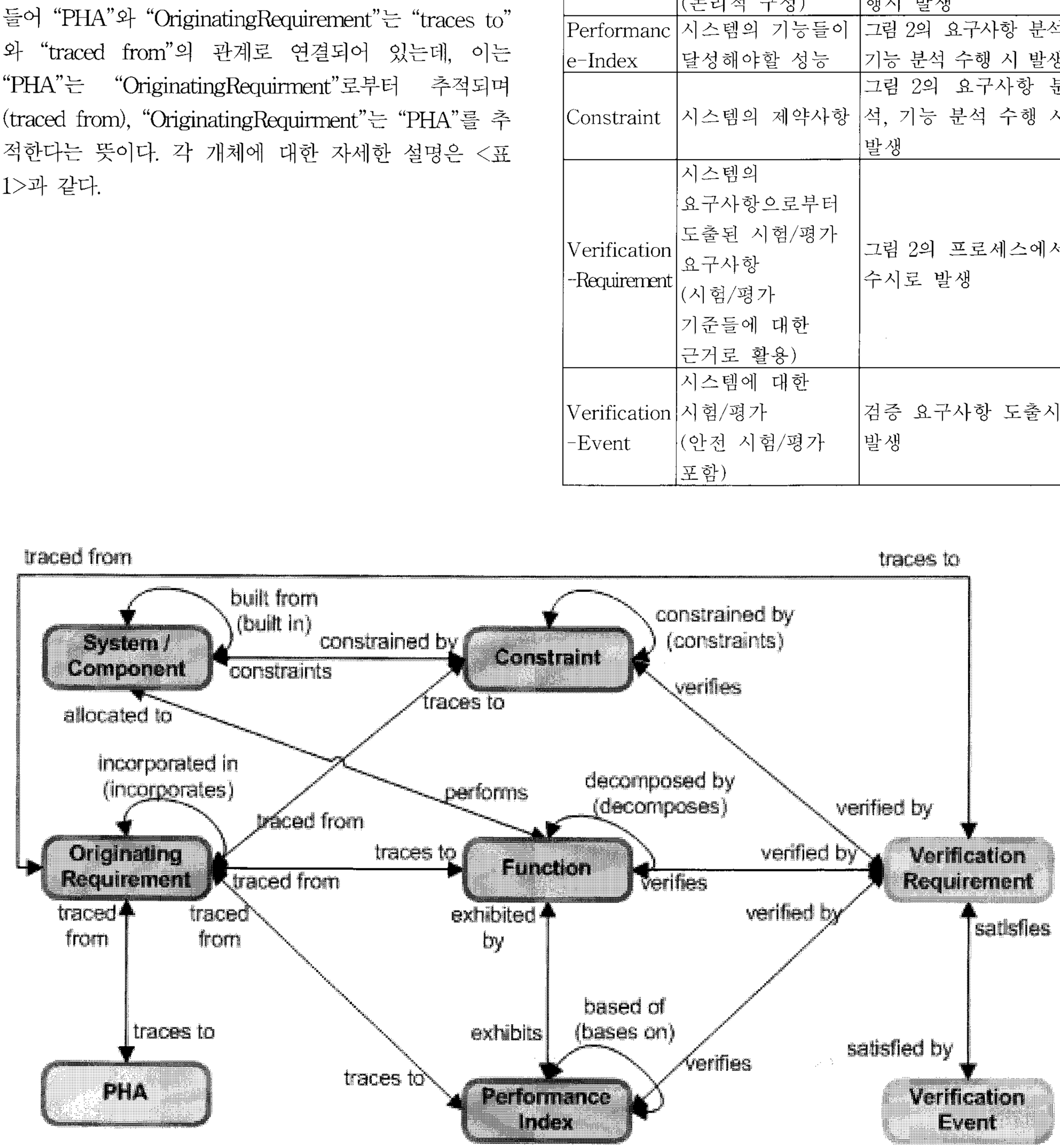
구축한 DB의 스키마는 기존에 시스템공학 데이터들을 관리하기 위해 Vitech 사의 CORE® [10]에서 제시한 기본 스키마를 토대로 <그림 3>과 같이 구성하였다.

<그림 2>의 절차에 따라 발생한 산출물들을 <그림 3>과 같은 관계를 이용하여 추적성을 관리한다. <그림 3>은 전체 DB 스키마를 다 나타낸 것은 아니며, 본 논문에서 제시하는 핵심 내용과 관련된 것만을 나타낸다.

<그림 3>의 스키마를 이루는 각각의 타원형이 개체(Entity)이며 타원들 사이의 화살표는 개체들 간의 관계이다. 그리고 해석은 다음과 같이 할 수 있다. 예를 들어 "PHA"와 "OriginatingRequirement"는 "traces to"와 "traced from"의 관계로 연결되어 있는데, 이는 "PHA"는 "OriginatingRequirment"로부터 추적되며(traced from), "OriginatingRequirment"는 "PHA"를 추적한다는 뜻이다. 각 개체에 대한 자세한 설명은 <표 1>과 같다.

<표 1> 추적성 구현의 핵심 대상인 DB 개체 설명

클래스 명	관련 데이터	데이터 발생 시기
PHA	예비 위험 분석 결과	시스템 개발 초기의 PHA 수행 시 발생
Originating-Requirement	요구사항 Hierarchy (안전 요구사항 포함)	그림 2의 요구사항 분석 시 발생
System/ Component	시스템의 구성품 (물리적 구성)	그림 2의 조합 시 발생
Function	시스템의 기능 (논리적 구성)	그림 2의 기능 분석 수행시 발생
Performance-Index	시스템의 기능들이 달성해야할 성능	그림 2의 요구사항 분석, 기능 분석 수행 시 발생
Constraint	시스템의 제약사항	그림 2의 요구사항 분석, 기능 분석 수행 시 발생
Verification-Requirement	시스템의 요구사항으로부터 도출된 시험/평가 요구사항 (시험/평가 기준들에 대한 근거로 활용)	그림 2의 프로세스에서 수시로 발생
Verification-Event	시스템에 대한 시험/평가 (안전 시험/평가 포함)	검증 요구사항 도출시 발생



<그림 3> 핵심 추적성의 근거가 되는 DB 스키마 개발

3.3 추적성 검증 및 데이터 변경 관리

제시한 추적성 모델을 통해, 구현된 데이터들 간에 추적성을 검증하고 변경 관리가 가능한지 알아보기 위해 두 가지 측면에 접근하였다. 첫째는 PHA와 OriginatingRequirement 사이의 추적성, 두 번째는 OriginatingRequirement와 VerificationRequirement이다.

첫째는 PHA를 통해 예측되는 모든 위험이 시스템 설계를 위해 요구사항으로 반영되었는지를 검증하고, 두 번째는 모든 시험/평가들이 모든 요구사항을 검증하도록 계획되었는지를 검증한다. 본 논문에서는 이를 위해 전산지원도구 중 CASysE(Computer-Aided Systems Engineering) 도구인 CORE®에서 제공하는 자동 문서 출력 기능을 통해 추적성이 확보되어 있지 않은 데이터들을 수집한 문서를 자동 출력할 수 있도록 문서 작성 Script를 개발하고, 이를 통해 출력된 문서를 통해 누락된 추적성을 분석하고 보완하였다. <그림 4>는 추적성 누락을 확인하기 위해 자동으로 출력한 표의 예이다.

내 용		수 량	비 고
요구사항 개수		263	
시스템 사양 수	Function	30	
	Performance	8	
	Constraint	141	
검증 요구사항 개수		135	
PHA과 연결이 없는 요구사항 개수		0	
시스템 사양과 연결이 없는 요구사항 개수		172	(요구사항 번호 및 요구사항 제목 기술)
요구사항과 연결이 없는 시스템 사양 개수	Function	7	
	Performance	1	
	Constraint	22	
시스템 사양과 연결이 없는 검증 요구사항 개수		0	
검증 요구사항과 연결이 없는 시스템 사양 개수	Function	2	
	Performance	3	
	Constraint	0	

<그림 4> 추적성 누락을 확인할 수 있는 결과표

두 가지 측면의 검증 내용을 포함하는 문서를 자동으로 출력 기능을 통해, 추적성이 누락된 데이터를 파악하고 변경이 필요할 때 변경에 영향을 받는 데이터가 어떤 것들이 있는지 쉽게 확인함으로써 구현된 추적성을 검증하였다.

4. 시험/평가 계획서 개발

4.1 시험/평가 계획서 양식 개발

체계적인 시험/평가 수행을 위해 시험/평가에 대한 전반적인 사항이 시험/평가 계획서 (Test and Evaluation Plan: TEP)에 올바르게 기술되어야 한다. 계획서의 내용을 정하기 위해, 미국방 표준인 DoD5000.2-R [11]을 참고하여 다음과 같은 사항을 시험/평가 계획서의 내용으로 정의하였다.

- 검증 요구사항 (Verification Requirement)
- 검증 이벤트 (Verification Event)
- 검증 책임 조직 (Responsible Organization)
- 시험 장비 (Test Configuration)
- 시험 절차 (Test Procedure)
- 시스템 요구사항 (OriginatingRequirement)
- 시험 대상 (시스템 기능, 성능, 제약사항, 구성품)

TEP 작성 시, PHA를 통해 안전 요구사항을 작성하고, 이러한 안전 요구사항을 만족하기 위한 시스템 요소들에 대해 추적성을 확보하였으므로, 위의 TEP 내용은 안전 시험/평가 계획을 포함한다.

4.2 효율적인 시험/평가 계획서를 위한 자동 문서 출력 Script 개발

시험/평가 계획서의 작성 시간을 줄이고 문서 작성 시 발생하는 인간적인 오류를 최소화하며 문서 변경 시 변경을 용이하게 하기 위하여, 본 논문에서는 CORE®의 자동 문서 출력 기능을 활용하였다. 이를 위하여 개발한 DB 스키마를 기반으로 TEP의 내용이 출력될 수 있도록 TEP Script를 개발하였다.

TEP Script는 검증 요구사항을 시작으로 검증 요구사항과 추적 관계에 있는 시스템 요구사항 시험 대상, 그리고 검증 이벤트를 도출하고 검증 이벤트와 추적 관계에 있는 조직, 장비, 절차를 도출하여 TEP가 작성되도록 하였다.

4.3 시험/평가 계획서 자동 생성

정의한 시험/평가 양식과 그에 대한 자동 출력 Script를 활용하여 구현한 추적성을 기반으로, 시스템 개발 데이터들을 CORE®를 사용하여 자동으로 미국방 표준인 DoD5000.2-R을 준수하는 TEP를 출력하였다.

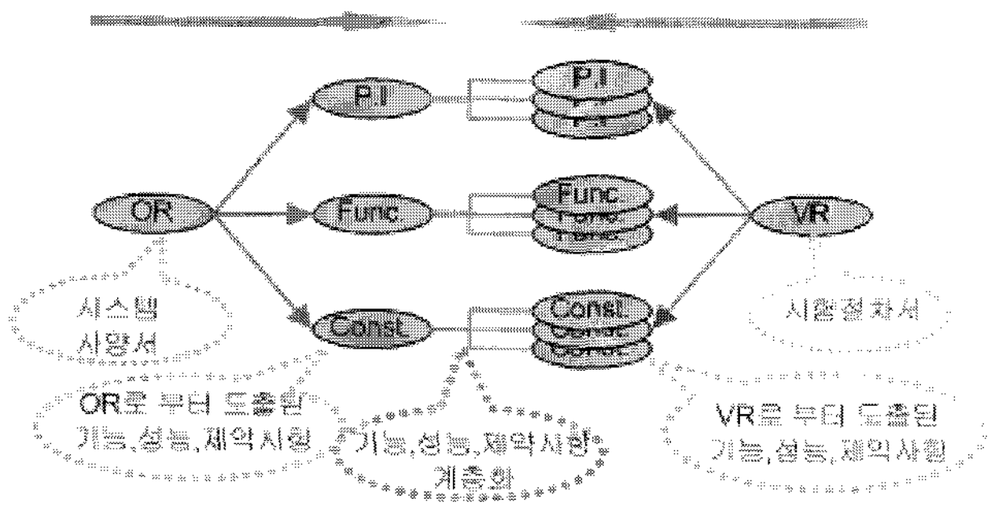
이를 위해, 시스템 개발 데이터들을 CORE® DB에 저장하고 데이터들 간의 추적 관계를 설정하였다. 추적성 검증 과정을 통해, 추적성이 누락된 것은 없는지, 추적 관계인 사항들이 어떤 것들이 있는지 확인하였다.

5. 철도시스템의 시험/평가 계획서 개발

철도 시스템을 대상으로 한 시험/평가 계획서 개발 결과이다. 기존의 모델링 자료와 시험&평가 자료들을 통합하고 일관성을 유지하기 위해 본 논문의 추적성 확보 방안을 적용하였다.

먼저 PHA를 수행하여 시스템의 위험 요소를 도출하였다. 다음 시스템의 요구사항을 분석하였으며, 요구사항을 분석하면서 PHA의 결과를 이용하여 시스템의 안전 요구사항을 같이 도출하였다. (PHA의 경우 타 기관에서 수행한 자료를 인용하였다.)

요구사항이 개발되고 시스템의 기능, 성능, 제약사항을 도출하였다. 기능, 성능, 제약사항의 경우 대상 시스템의 시험 절차서를 바탕으로 도출되었다. 이때 본래 요구사항으로부터 도출되어야할 기능, 성능, 제약사항 등 시스템 사양들의 일관성 및 추적성을 확보하기 위해 다음 <그림 5>와 같은 작업을 수행하였다. <그림 5>를 자세히 설명하자면 다음과 같다.



<그림 5> 요구사항과 기능, 성능, 제약사항 계층 간의 일관성 및 추적성 확보 개념

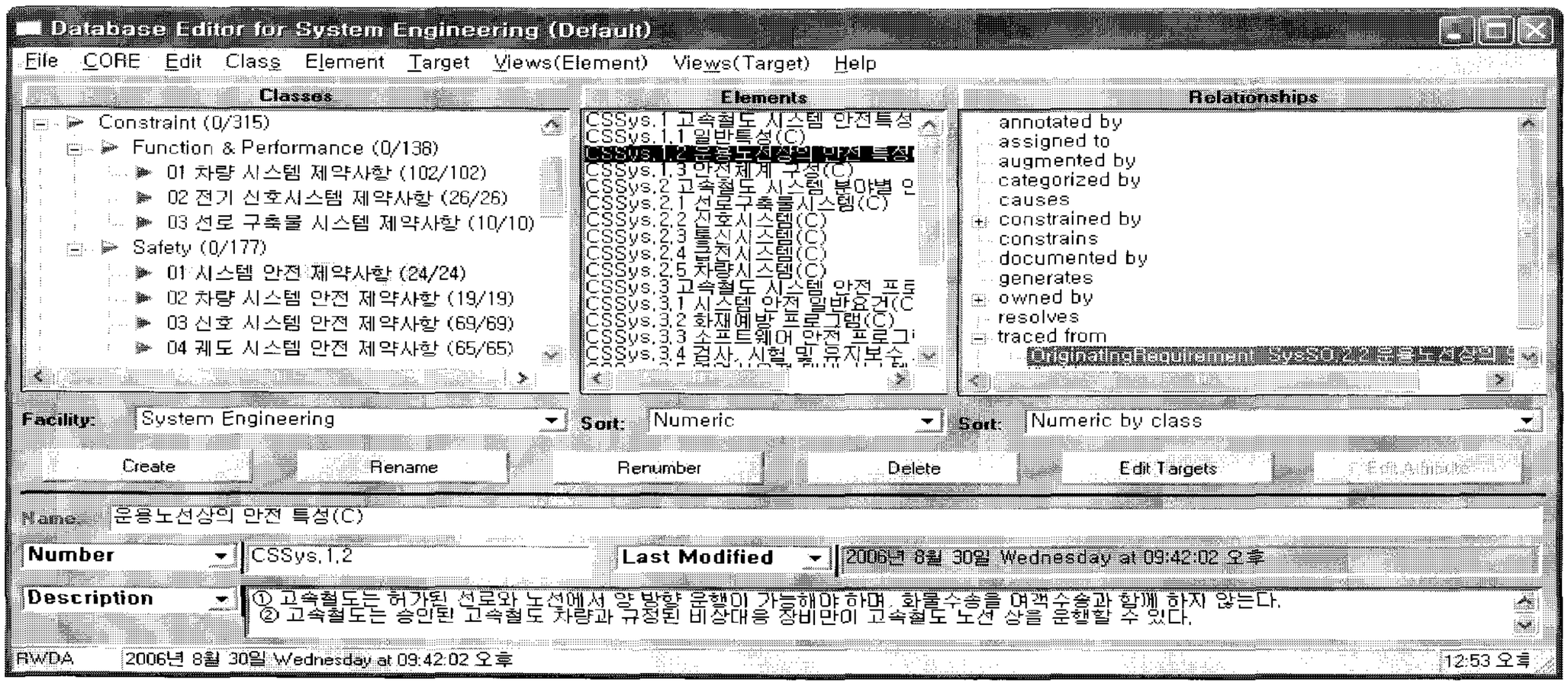
① 최초 요구사항(고속철도시스템의 기본 사양 분석 자료 기반)으로부터 도출된 시스템 수준의 기능/성능 및 제약사항을 최상위에 둔다.

② 시험절차서로부터 도출된 기능/성능 및 제약사항은 같은 수준의 유사항목으로 그룹화한다. 즉 시험절차서로부터 도출된 기능/성능 및 제약사항은 최초요구사항으로 도출된 기능 및 성능의 하부 기능 및 성능으로 둠으로써 계층화를 한다.

시스템의 기능, 성능, 제약사항이 도출되면 다음에는 시스템 물리 아키텍처를 구축하였다. 시스템 물리 아키텍처는 이미 구축된 해당 시스템의 물리적 구조를 반영하고, 각 구성품에 기능, 성능, 제약사항을 할당하였다.

다음에는 기존의 시험 절차서를 바탕으로 요구사항을 이용하여 시스템의 시험/평가 기준을 정리하였다. 기능, 성능, 제약사항등이 시험 절차서를 이미 고려하여 기록하였기에, 시험/평가 기준과는 일관성을 유지하였다.

이렇게 작성된 DB로 시스템의 사양서 및 TEP를 제공함으로써 시스템을 올바르게 시험/평가할 수 있는 방안을 제시하였다. 작성된 DB는 <그림 6>과 같이 요구사항으로부터 안전 제약사항이 발생됐다는 것을 확인할 수 있다. 이렇게 PHA가 요구사항으로 요구사항이 다시 시스템 사양으로 마지막으로 사양이 시험/평가로 추적성을 이루도록 DB를 구축하였다. 최종적으로 TEP를 <그림 7>과 같이 자동으로 작성하였다. 본 연구에서 제시하는 관리 방안을 통해 해당 사례에서는 PHA에서 의도했던 몇몇 안전 목표들을 시험/평가 계획에서 누락되었음을 확인하고, 시험/평가를 개선하고 안전 요구사항과의 추적성을 확보하여 TEP를 자동출력함으로써 의도된 모든 시스템 안전을 확보할 수 있는 시험/평가 계획을 얻을 수 있었다.



<그림 6> 추적성 확보 예

2006년 9월 6일 Wednesday

1 계획된 시험

1.1 보조전원장치 시험

* 본 절차서는 G7 기술개발 사업을 통하여 개발되고 있는 차량의 객차 단차시험 및 Power Unit 시험이 완료된 후, 7량 편성 상태에서의 보조전원장치 시험에 대하여 규정한다.

a) 측정항목

* 1)670V Converter 동작 시험
* 2)동력차 No1. Battery Charger 동작 시험
* 3)동력차 No2. Battery Charger 동작 시험
* 4)동력객차 Battery Charger 동작 시험
* 5)객차 Battery Charger 동작 시험
* 6)객차 CVCF Inverter 동작 시험
* 7)670V 연장급전 시험 (TCN 정상조건시)
* 8)670V 연장급전 시험 (TCN 고장조건시)

b) 시험조건

* 1)본 시험은 정지 상태에서 시행한다.
* 2)가선 전압은 가압한다.
* 3)모든 NFB 및 스위치는 정상상태로 한다.
* 4)운전실 선택스위치(SB-01)를 ON 후, 밧데리 투입상태로 한다.
* 5)Panto. 상승 및 VCB 투입상태로 한다.
* 6)TCN 정상동작 조건에서 시험한다.

c) 현황

* Not Yet Planned

d) 검증되어야 할 요구사항

* [Constraint] CC.48 보조동력
* [Constraint] CST.13 비상장비(C)
* [Function] F.16 보조 전원 공급 기능

2006년 9월 6일 Wednesday

e) 요구사항 vs. 시험품목

검증되어야 할 요구사항	시험 품목
CC.48 보조동력	CC.1.2.1.7.8 보조 전원 설비
CST.13 비상장비(C)	
F.16 보조 전원 공급 기능	CC.1.2.1.7.8 보조 전원 설비

f) 검증 유형

방법	Level
Test	HWCI

g) 이벤트 일정

이벤트	예상기간	시작 날짜	종료 날짜
1.11 보조전원장치 시험	3.0 시간	2006년 10월 2일 Monday at 10:00:00 오전	2006년 10월 2일 Monday at 01:00:00 오후

1.1.1 보조전원장치 시험

a) 일정

예상기간	시작 날짜	완료 날짜
3.0 시간	2006년 10월 2일 Monday at 10:00:00 오전	2006년 10월 2일 Monday at 01:00:00 오후

b) 시험 설비 및 장치

시험 설비/장치	내 용
온도계	
출력전압 측정용 Power scope	
Tester	

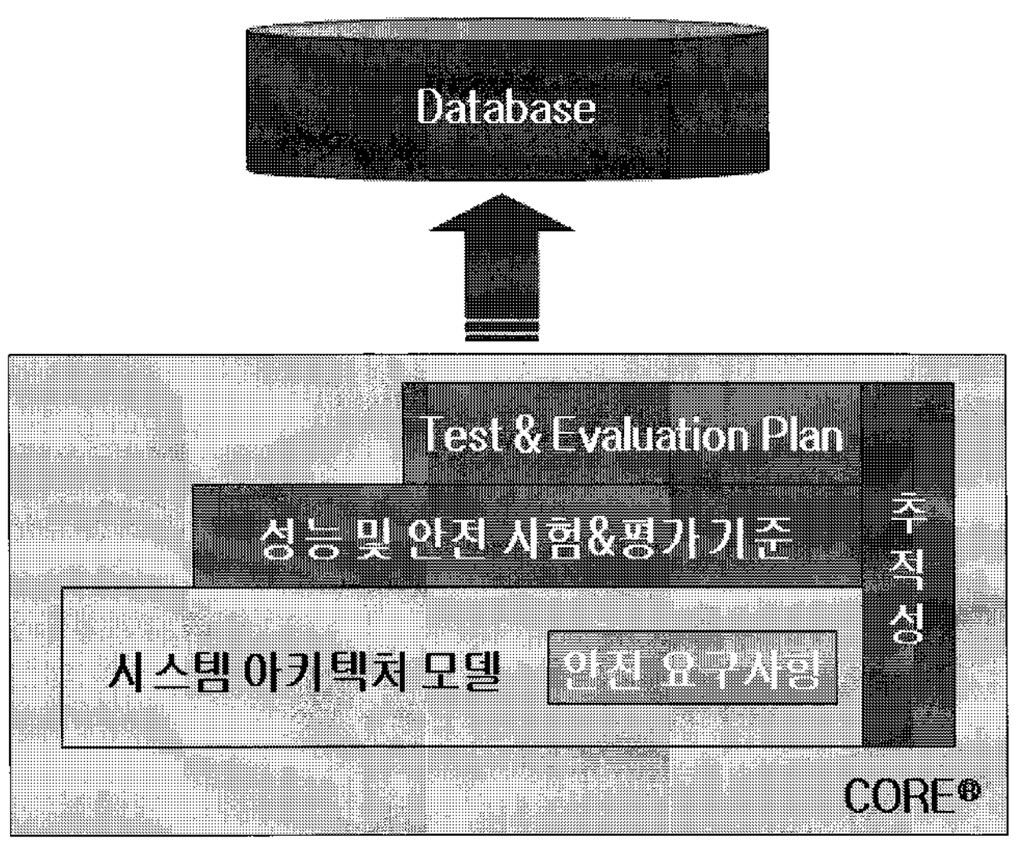
<그림 7> TEP 예

6. 결 론

안전 요구사항의 추적성을 구현하고, 구현된 추적성을 바탕으로 시스템의 시험/평가 계획서를 자동 출력함으로써 효율적인 시험/평가 계획서를 작성하는 방안에 대해 연구하였다. 이를 위해 CASysE 도구 중 하나인 CORE®의 DB를 다음 <그림 8>과 같이 구성하여 활용하였다. 시스템의 요구사항, 기능, 성능, 제약사항 등을 기술하고 표현한 모델이 DB의 기본 내용이다.

그러한 모델 중 시스템의 요구사항은 안전 요구사항을 포함하게 된다. 안전 요구사항은 시스템 초기의 위험 분석 내용 (PHA)을 바탕으로 도출하므로 안전 요구사항은 위험 분석의 결과와 추적성을 가지도록 구성하였다.

시스템 초기부터 시스템 개발 시 발생하는 모든 산출물들간의 추적성을 구현하고 결과적으로 TEP를 출력함으로써 시스템이 안전 요구사항을 만족하는지 시험/평가 할 수 있도록 제시하였다. 추적성이 누락없이 모두 확보되었는지 확인하기 위하여 CORE에서 추적성이 누락된 데이터를 출력하도록 자동 문서 출력 Script를 사용하여 보완하였다.



<그림 8> 효율적인 시험/평가 계획서 개발을 위해 구현된 추적성과 데이터 구조

시스템의 요구사항, 기능, 성능, 제약사항, 물리 구조 등을 기록하고 이들 간에 관계를 통해 추적성을 확보함으로써 변경에 대한 Impact Analysis를 용이하게 하였다. 또한 국제 규격에 맞는 TEP를 제시함으로써 시험/평가가 올바르게 수행될 수 있도록 하였다. 마지막으로 전산지원도구를 통해 차후 유사 프로젝트 수행 시 데이터의 재사용이 용이하게 하였다.

현재까지는 다양한 안전 분석 기법들을 고려하지 못하였으나, 향후 다양한 안전 분석 기법들에 대해 연구하여 해당 기법을 통한 안전 요소들이 시스템에 반영할 수 있도록 추적성 확보 대상들의 확장 연구가 필요하다.

7. 참 고 문 헌

[1] Clifton A. Ericson, II, Hazard Analysis Techniques for System Safety, John Wiley & Sons, INC., 2005

[2] Bradley J. Brown, "Assurance of Software Quality," Carnegie Mellon University, Software Engineering Institute 1987

[3] Edwards, M. and S. Howell, A Methodology for Requirements Specification and Traceability for Large Real-Time Complex Systems, Naval Surface Warfare Center, 1992

[4] Jeffery O. Grady, System Requirements Analysis, Academic Press, p61, 2005

[5] James N. Martin, Systems Engineering Guidebook, CRC Press, p. 119, 1997

[6] John D. Claxton, Test and Evaluation Management Guide, The Defense Acquisition University Press, 2005

[7] Jeffery O. Grady, System Integration, CRC Press, INC., p. 11, 1999

[8] Silberschatz, Database System Concepts, Mc Graw Hill, p. 131, 2002

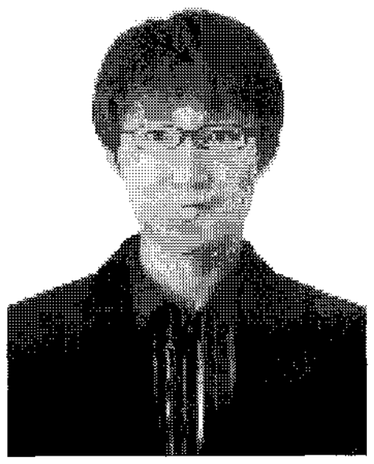
[9] Peter Pin-Shan, Chen, The entity-relationship model-toward a unified view of data, ACM Transactions on Database Systems, p. 9-36, 1976

[10] http://www.vitechcorp.com/

[11] Department of Defense (DoD), Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs, DoD, DoD 5000.2-R, 2002

저 자 소 개

윤 재 한



현 아주대학교 시스템공학과 박사과정, 철도안전 SE 표준 스키마 과제, 주요 관심분야는 모델기반 시스템공학, Systems Safety, Modeling & Simulation, 기술관리 등.

주소: 경기도 수원시 영통구 원천동 산5번지 아주대학교 팔달관 117-1호

이 재 천

현 아주대학교 시스템공학과 정교수 및 학과장. 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, 최근 미국 Stanford Univ. 방문교수 역임. 현재 연구 및 교육 관심분야는 시스템공학 (Systems Engineering: SE) 분야에서 Model-based SE, Modeling & Simulation 및 Systems Architecting. 그리고 Safety-Critical Systems에서 SE의 응용 등.

주소: 경기도 수원시 영통구 원천동 산5번지 아주대학교 서관 309호