

철도안전정보 지원시스템의 요구사항 개발을 위한 엔터프라이즈 아키텍처 활용 연구

A Study on the Enterprise Architecture to Develop the Requirements for Railway Safety Support information Systems

이병길* · 이재천*

Byoung-Gil Lee · Jae-Chon Lee

Abstract This paper is concerned with the development of the requirements for railway safety support information systems. The five safety elements at the system level have been modeled based on the enterprise architecture approach. Specifically, the modeling has been carried out as follows. First, the requirements are derived according to EIA-632 process. Also, the possible scenarios on the accident-investigation-support are developed from the help of relevant personnel in the area. The developed scenarios are reflected in modeling the operational and system architectures of DoDAF approach using a CASE tool. From this architecture model, we can easily get the specifications required for the operations. These results can give the improved understanding of the railway safety system to the members of diverse teams and areas working for the system development.

Keywords : Enterprise Architecture, DoDAF, Requirements, Systems Engineering, Railway System

요 지 이 논문은 엔터프라이즈 아키텍처 접근을 기반으로 시스템 수준의 철도안전정보지원시스템의 안전 요소에 대한 요구사항 개발에 관한 내용이다. 모델링은 다음과 같은 절차를 따른다. 첫째로, 요구사항은 EIA-632 프로세스를 따른다. 또한 관련 전문가의 도움을 받아 사고기반 시나리오를 개발한다. 개발된 시나리오는 DoDAF 모델을 지원하는 CASE 도구의 지원을 받아 구현한다. 이 결과는 시스템관련 종사자의 이해를 돕는다.

주 요 어 : 엔터프라이즈 아키텍처, 미국방 아키텍처 프레임워크, 요구사항, 시스템 공학, 철도 시스템

1. 서론

1.1 연구의 배경 및 목적

최근 삼성전자 기흥 반도체 공장에서 정전으로 6개 라인이 동시에 가동 중단되는 초유의 사태가 벌어지고, 현대자동차 울산 엔진 공장 옥상에서는 화재가 발생했다. 미국 미시시피 주에서는 다리가 붕괴해 최소한 4명이 사망하고 20~30명이 실종됐으며 60여명의 부상자가 발생했다. 안전을 제1의 가치로 여기는 우리에게 시사하는 바가 적지 않다. 이들 사

고를 타산지적으로 삼아 유사 사고가 재발하지 않도록 사전 점검 등에 만전을 기해야 할 것이다.

21세기 모든 산업의 커다란 이슈는 안전과 업무 효율화라고 볼 수 있다[1-3].

철도산업에서도 2003년 발생했던 대구 지하철 참사가 시 작점으로 작용하여 대부분의 시스템 개발 및 운용 시 안전에 대한 철저한 관리를 요구하고 있다. 또한 업무 효율화에서는 국내 기업에서 업무프로세스 재설계(BPR: Business Process Re-engineering), 전사적 지원관리(ERP : Enterprise Resource Planning) 등 수 많은 프로세스들을 기업 내부 프로세스로 도입하여 최대의 이윤을 남기려는 노력들을 수행하고 있다. 이와 관련 하여 철도분야에서도 안전과 업무 효율화에 관심을 가져야 할 시점이다. 그러나 각 산업 분야에서는 사고 발생

† 책임저자 : 정회원, 아주대학교, 시스템공학과
E-mail : dfslove@naver.com
TEL : (031)330-7667 FAX : (031)330-7118
* 정회원, 아주대학교 시스템공학과, 정교수

조직에 의해 개별적으로 위험 분석을 진행하기 때문에 사고 발생 위험확률을 도출하기 어렵고, 사고 관련 데이터들이 개별 조직에 의해 산발적으로 분석됨으로써 분석 절차들의 통일성을 유지하기 어렵다.

통일성 유지의 문제를 해결하기 위해서는 통합된 단일 데이터를 구축하고, 관리를 위한 전문 시스템이 개발되고, 개발된 시스템으로 표준화된 분석 절차가 수립되어야 한다. 철도 시스템과 같이 규모가 크고 여러 조직에 의해 운용 관리되는 시스템에 대한 통합된 정보 시스템을 개발할 경우 가장 중요시 되어야 할 사항은 개발된 정보 시스템이 여러 조직의 업무를 효율적으로 지원할 수 있어야 한다는 것이다.

이러한 거대 조직을 위한 통합 정보 시스템은 흔히 EA (Enterprise Architecture)라는 방법론을 적용하여 연구되고 있으며, 근래 국내 다수의 기업에서 적용하여 연구되고 있으며, 근래 국내 다수의 기업에서 적용하고 있는 실정이다. 그러나 국내 엔터프라이즈 아키텍처 적용 기업은 성공보다는 실패 경험들이 더 많다. 그 이유는 바로 기업의 업무 즉, 비즈니스 프로세스를 제대로 파악하지 못한 상태에서 정보시스템을 개발하여 기업의 환경과 동떨어진 시스템이 개발되어 유용성이 낮아지기 때문이다. 본 논문은 철도안전정보지원시스템에 엔터프라이즈 아키텍처 방법론을 적용하여 비즈니스 프로세스를 정립하고 비즈니스 가치를 극대화 할 수 있는 시스템의 기능을 정의한다.

본 논문에서는 많은 엔터프라이즈 아키텍처 방법론 중 DoDAF (Department of Defense Architecture Framework)를 적용하여 철도안전정보지원시스템을 구축한다.

본 논문의 구성을 보면, 사회 동향 및 문제점을 기술한 서론에 이어서, 본론에서는 엔터프라이즈 아키텍처 프레임워크를 작성하기 위한 프로세스와 엔터프라이즈 아키텍처에 대해 기술하고, 안전정보지원시스템의 각 프로세스 수행 결과를 기술, 결론에서는 본 사례에서 기여하는 바와 추진 방안에 대해 요약하였다.

2. 본 론

2.1 엔터프라이즈 아키텍처 적용을 위한 프로세스

철도안전정보지원시스템에 엔터프라이즈 아키텍처를 적용하기 위해서 EIA-632를 기반으로 프로세스를 설정하고, 아래와 같은 단계를 거쳐 시스템 요구사항 아키텍처 모델을 구축한다[4].

- 요구사항 아키텍처 DB스키마 개발
- 운용 개념 및 요구사항 구축용 템플릿 개발

- 요구사항 아키텍처 모델 구축
- 시스템 개발규격서 자동 출력 체계 구축

Fig. 1은 엔터프라이즈 아키텍처를 통한 철도안전정보지원 시스템의 요구사항 개발을 위한 프로세스를 설명한 것이다. 각 프로세스를 보면 우선 요구사항 사이의 관계를 설정하는 스키마를 개발한다. 스키마는 ERA구조로 이루어져 있다. ERA구조란 Entity, Relation, Attribute사이의 관계를 표현한 것이다. 운용 개념 및 요구사항 아키텍처 구축용 템플릿은 각 개발자와 이해당사자 사이의 발생할 수 있는 하나의 시스템에 대한 각각의 다른 형상을 줄이고 각자가 원하는 요구사항을 다른 관계자에게 이야기할 수 있는 의사소통의 도구로 사용되도록 도와준다. 요구사항 아키텍처 모델은 운용 관점 (Operational View), 시스템 관점(System View), 기술 관점 (Technical View)의 일관성을 통하여 아키텍처의 모델을 구축한다. 본 연구의 범위는 운용 관점(Operational View), 시스템 관점(System View)사이의 일관성을 유지한다. 앞의 결과물을 통하여 시스템 개발 규격서 자동 출력 체계 구축을 통하여 시스템을 개발하는데 고려해야 할 요구사항을 기술한 규격서를 제공한다.

2.2 엔터프라이즈 아키텍처

엔터프라이즈 아키텍처의 개발 목적은 비즈니스 프로세스에 적합한 시스템의 아키텍처를 개발하고 미래의 가치를 창출하는 것이다. 즉 엔터프라이즈 아키텍처는 정의된 업무 범위(Scope)와 미션(Mission)을 지원하는 운용 아키텍처와 시스템 아키텍처 그리고 시스템의 기술적 타당성을 고려한 기술 및 표준으로 이루어진 내용이다. 엔터프라이즈 아키텍처에 대한 연구는 1987년 Zachman이 IBM System Journal Magazine에 기재한 정보시스템의 구조를 체계화하려는 시도에서 출발되었다. 이후 엔터프라이즈 아키텍처는 90년대 중반 미 연방정부기관과 미 국방부에서 적용하면서 민간부분으로까지 확산되었다[5].

엔터프라이즈 아키텍처 프레임워크는 조직, 정보, 시스템, 기술이 복잡하게 얽혀져 있는 엔터프라이즈의 실제들을 체계

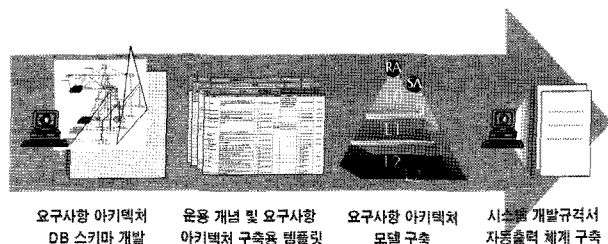


Fig. 1. Requirement Development Process

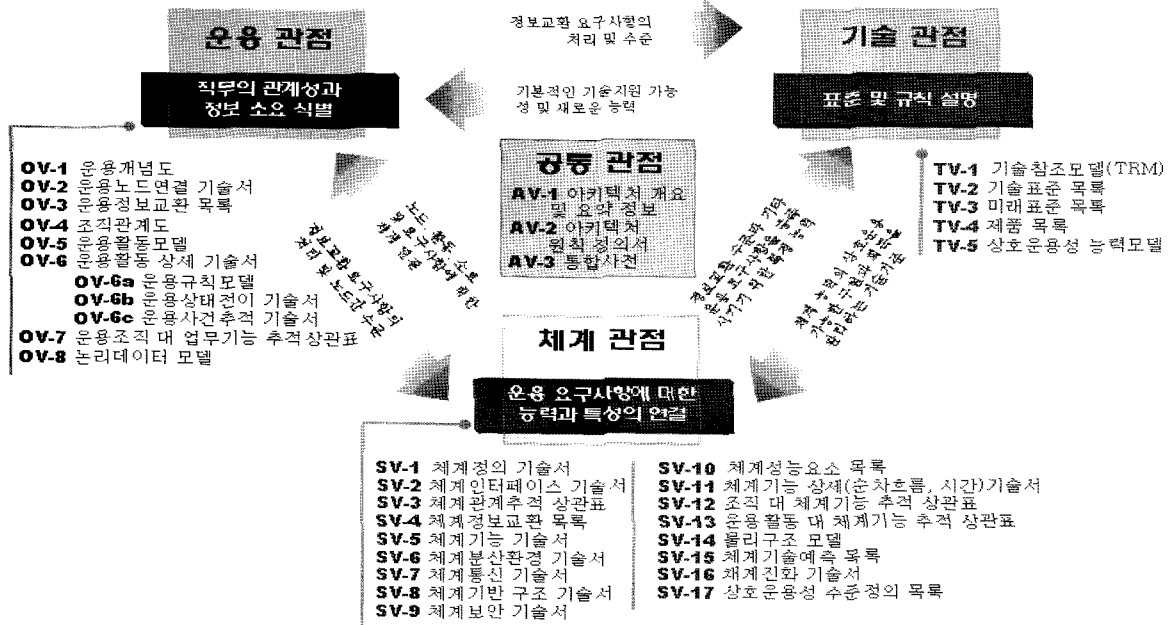


Fig. 2. Architecture View of DoDAF

적으로 접근하기 위한 논리적인 틀을 제공하는 것으로 이해 당사자가 필요한 정보에 대하여 명확하고 상호관계성을 가지는 요소에 대하여 다양한 관점에서 바라볼 수 있는 방법과 지침을 제공한다.

DoDAF을 보면 버전 1.0의 C4ISR AF에 기반으로 2003년에 개편한 것으로 전쟁과 임무 수행을 위한 미 국방부 아키텍처 개발, 표현, 통합에 대한 접근 방법으로 프레임워크는 아키텍처 기술이 조직 영역을 통해 비교되고 상호 관계가 될 수 있도록 보장해주는 역할을 수행한다. 프레임워크는 정의, 지침, 관련 사항을 제공하는 부분과 각 산출물에 대해 기술하는 부분 2가지 영역으로 되어 있으며 프레임워크는 운영 관점(Operational View), 시스템 관점(System View), 기술 관점(Technical View)에서 시스템의 산출물을 정의하고 있다. 본 논문에서는 미 국방부의 DoDAF를 철도안전정보지원시스템에 적용하였다.

2.3 프로세스 수행 내용

2.3.1 요구사항 아키텍처 DB 스키마 개발

요구사항 아키텍처 DB스키마를 개발하기위하여 시스템 엔지니어링 프로세스를 기반으로 운영 모델 및 요구사항 정의 방법을 연구하고 요구사항 정의 방법과 시스템엔지니어링 지원 도구(CORE)와의 통합을 위한 DB 스키마를 개발한다[6].

Fig. 3은 SE 도구에서 지원하는 아키텍처 스키마의 구조를 나타낸 것이다. 아키텍처 스키마를 철도안전정보지원시스템의 아키텍처 개발에 적용하였다. 철도안전정보지원시스템의

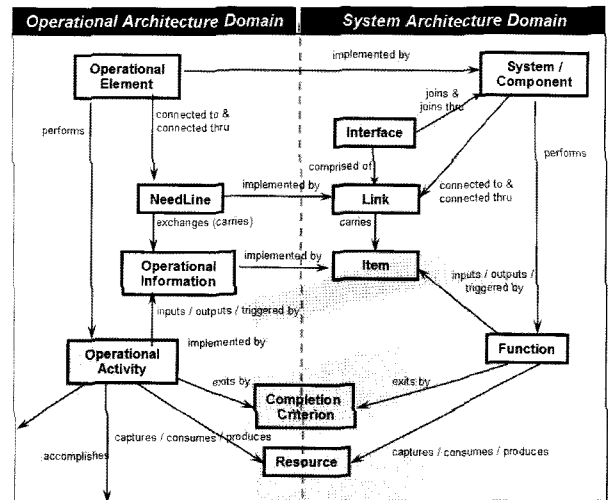


Fig. 3. Architecture Schema Structure of SE Tool

운영 시나리오를 SE 도구에서 제공하는 스키마의 구조로 모델링할 경우 운영 아키텍처와 추적성을 가지는 시스템 아키텍처를 개발할 수 있다. 또한 DoDAF에서 제공하는 다양한 형태의 아키텍처 산출물의 개발이 가능하다.

2.3.2 운영 개념 및 요구사항 아키텍처 구축용 템플릿

철도안전정보지원시스템의 개발자에 정확한 개발 의도를 요구사항에 반영할 수 있도록 요구사항 아키텍처 템플릿을 사용하였다. 요구사항 아키텍처 템플릿은 사용자와 개발자 사이의 아키텍처링 Communication 도구로 사용자의 요구사항

연계	주어	From/To	무엇을	어떻게	동사	거동 소요 시간	정보속성							상호 운용성 요구수준	
							사용 언어	처리 형태	주기	적시성	무결성 확인	보안 등급	보안 유형		배포지침
시간 1	운영사/ 시설관리자는		사고발생을		보고 한다.									지역본부	도메인
시간 1	철안사는		시스템 아키텍처를	(Reengi- neering)	작성 한다.									위험분석 및 평가수행조직	기능적
시간 1	참조자료생성 기관·기상청은		환경관련 Hazard 정보관리를		수행 한다.										기능적
시간 2	운영사/ 시설관리자는	건교부·교통 안전공단에	사고개황을		전달 한다.									시스템 설계조직	기능적
시간 2	철안사는		Conceptual PHA를		수행 한다.									시스템 설계조직	기능적
시간 2	운영사는		사건을		조사 한다.									시스템 설계조직	도메인
시간 3	운영사는	철안사에	HPES· 사건자료를		전달 한다.									지역본부	도메인
시간 3	건교부·철도사 고조사위원회는		사고를		접수 한다.									지역본부	도메인

Fig. 4. Requirement Architecture Template

을 효과적이면서 효율적인 시스템 요구사항으로 도출하는데 유용하다. 요구사항 아키텍처 템플릿의 입력요소로는 정보속성이 있고, 정보속성은 사용언어, 처리형태, 주기, 적시성, 무결성 확인, 보안 등급, 보안 유형, 배포지침, 상호 운용성 요구 수준 등이 있다.

2.3.3 요구사항 아키텍처 모델 구축

철도안전정보지원시스템의 개발 대상 영역을 살펴보면 사고조사지원 및 사고정밀 분석 시나리오, 안전 요구사항 및 대책 개발 시나리오, 철도 안전 종합계획 및 시행 계획 시나리오, 여객 안전 대책 개발 시나리오, 안전 기술 지원 시나리오 등이 시스템 개발의 영역이다. 철도안전정보지원시스템의 전체 거동을 표현하여 시스템과 이해당사자간의 입출력 요소를 확인하고, 전체 운용시나리오를 구축하여 시스템의 운용 요소들을 식별하였다. 이 단계를 통하여 시스템의 경계를 설정한다. 운용 모델의 전체적인 거동을 통하여 개발 기간의 추가 업무를 줄이기 위하여 개발 기간의 전체 시스템의 운용 시나리오를 개발한다. Fig. 5는 철도안전정보지원시스템의 운용모델로 확대한 부분을 보면 위험을 식별하여 처리하는 부분과 위험도 관련 자료조사의 절차를 보여준다.

2.3.4 운영 개념 도출

철도기술연구원에서 제공한 자료를 통하여 사고조사지원의 운영 개념을 작성한다. 이 단계에서 유용한 요구사항 도출

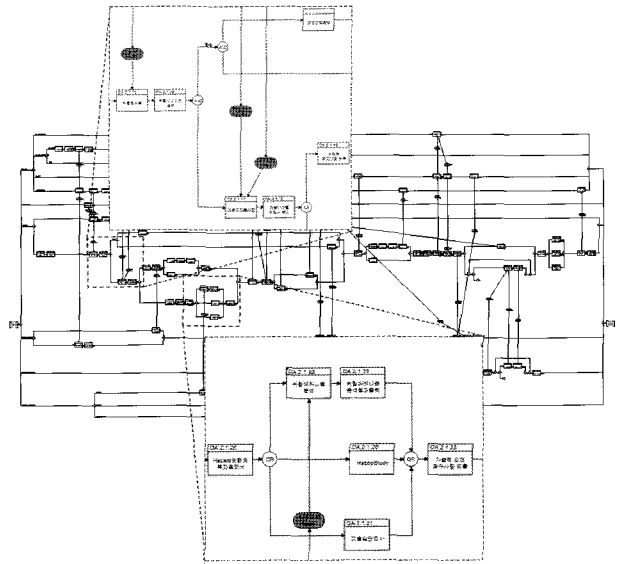


Fig. 5. Operational Scenario Model

을 위해서는 시스템 이해당사자에게 각 단계마다 개발한 내용이 맞는지 확인하는 것이 중요하다. 사고조사지원에 관한 운영 개념을 작성할 때 각 운영의 시간의 순서에 따라서 요구사항을 작성한다.

Fig. 6은 사고조사지원을 담당하는 전문가와 함께 작성한다. 이는 상세 템플릿 작성, 운용 모델을 구축하기위한 기초 작업으로 어느 조직이 어떤 일을 하고, 결과물을 어디에 전달하는지가 잘 나타나야 한다. 이를 통해 시스템이 가져야하는

요구사항이 누락된 것을 확인 할 수 있다.

2.3.5 상세 템플릿 작성

운영개념 자료 수집을 통해 작성된 운영개념을 상세 템플릿에 적용하여 철도안전정보지원 시스템의 정보속성을 식별하여 시스템 운용 개념의 요소를 기능적인 요소와 비 기능적인 요소로 구별하였다. 상세 템플릿을 작성할 때 From/To에 내용이 있으면 정보 속성을 작성해야 한다.

Fig. 7은 사고조사지원에 관한 운용요소의 정보속성을 통하여 시스템의 기능을 식별하고, EIA-632에서 제시하는 요구사항이 가져야하는 목표를 만족시킨다. 또한 이는 시스템 관점의 기능으로 전환하는데 사용된다.

2.3.6 운용 모델 구축

철도안전정보지원시스템의 사고조사지원시스템의 운용 모

운영사/시설관리자는 사고발생을 보고한다.
철안사는 시스템아키텍처를 작성(Reengineering)한다.
운영사/시설관리자는 사고개황을 건교부 교통안전공단에 전달한다.
철안사는 Conceptual PHA를 수행한다.
운영사는 사건을 조사한다.
운영사는 철안사에 HPES 사건자료를 전달한다.
건교부 철도사고조사위원회는 사고를 접수한다.
건교부 교통안전공단은 사고보고를 접수한다.
소방방재청은 철안사에 현장실태조사를 의뢰한다.
건교부 철도사고조사위원회는 대상 위험원 관련 정보를 출력한다.
건교부 교통안전공단은 안전자료를 수집한다.
건교부 교통안전공단은 철안사에 안전자료를 전달한다.
건교부 철도사고조사위원회는 사고조사관을 출동시킨다.

Fig. 6. Operational Concept

델을 개발하기위하여 철도기술연구원의 자료를 통하여 사고조사지원에 관한 개념 및 데이터를 수집하여 Fig. 8과 같은 운용모델을 개발한다. 운용 모델은 운영개념을 도출한 문서를 기반으로 최초 사고발생에서부터 지침작성까지의 시간순서별 정보제공기관, 사고조사지원 수행기관, 자료 수집하는 기관 사이의 업무흐름을 나타낸다.

2.3.7 아키텍처 산출물 개발

운용 모델을 구축하여 SE지원 도구인 CORE에서는 스키마라는 데이터베이스의 관계를 통하여 의사결정에 필요한 여러 산출물을 출력할 수 있다. DoDAF의 산출물을 출력하기위해 Table. 1과 같은 산출물의 관계를 설정한다.

철도안전정보지원시스템의 사고조사지원시스템의 운용활동이 할당된 운용노드(Node)들은 조직구성과 대부분 일치하나 현재 작성된 운용활동 모델과 같이 임시조직인 경우 기본구성과 일치하지 않을 수도 있으며, 한 재대가 여러 시스템을 다루는 경우 등 재대의 계층구조가 한 운영개념에서 동일한 계층을 유지하지 못할 수도 있다. 원칙은 동일계층을 유지하는 것이지만 운영개념의 표현의 편의상 상이한 계층구조를 사용하는 것도 허용된다. 이것을 보다 쉽게 파악하기 위해서 운용노드연결기술서(OV-2)에 물리적 블록 다이어그램(PBD: Physical Block Diagram)을 제시한다. Fig. 9는 운용활동상세 기술서(OV-2)에 제시되는 노드의 할당을 나타낸다.

Fig. 3에 SE지원 도구의 아키텍처 스키마 구조 참조하여 Fig. 8의 항목을 정리하면, DoDAF에서 산출물인 Fig. 2에 기술된, 운영관점(OV)의 산출물(운영개념도, 운용노드연결기술서, 운용정보노드 목록, 운용활동 모델, 운용활동 상세 기술

연계	주어	From/To	무엇을	어떻게	동사	가동 소요 시간	정보속성							상호 운용성 요구수준	
							사용 언어	처리 형태	주기	적시성	무결성 확인	보안 등급	보안 유형		배포지침
시간 1	운영사/ 시설관리자는		사고발생을		보고 한다.										
시간 1	철안사는		시스템 아키텍처를	(Reengi- neering)	작성 한다.										
시간 2	운영사/ 시설관리자는	건교부·교통 안전공단에	사고개황을		전달 한다.		한글	승인	1/2	0	0	0		건교부 교통안전공단	
시간 2	철안사는		Conceptual PHA를		수행 한다.										
시간 2	운영사는		사건을		조사 한다.										
시간 3	운영사는	철안사에	HPES 사건자료를		전달 한다.										

Fig. 7. Detail Template of Operation Concept

Table 2. Operation Activity Detail Description

번호	운용활동 명칭	입력정보	출력정보
SOP.1.1	시스템안전성 계획작성		
SOP.1.2	ALARP (SIL설정)		SIL 설정정보
SOP.1.3	HAZARD 우선순위 결정	위험원(시스템수준-FHA) 위험원(컴포넌트-FMEA) 위험원(컴포넌트-HAZOP) 위험원(하부시스템- -PHA-HAZOP)	
SOP.1.4	안전요구사항 수집		
SOP.1.5	SIL 명령	SIL설정정보	
SOP.1.6	위험원식별	기능 안전요구사항	기능요구사항 내적용성 위험원
SOP.1.7	하부시스템 위험식별	기능 (하부시스템)	

젝트 초기에 프로젝트와 관련된 정황을 분석하고 시스템 수준의 요구사항을 하부시스템의 전문가들의 시스템의 이해도 향상을 향상시켰다.

기대효과

1. 효과적이고 일관된 시스템 구현을 지원 및 관리
2. 시스템 이해도 향상
3. 엔터프라이즈 아키텍처 이해를 위한 상세 비즈니스 프로세스 절차 수립

본 사례를 통하여 구축된 통합아키텍처 모델로부터 설계 데이터의 일관성을 유지할 수 있음은 물론, 설계변동사항의 해석, 일관성 검사 그리고 효과성 분석 등에 사용함으로써 효과적이고 일관되게 시스템구현을 지원 및 관리할 수 있고, 시스템공학 도구에 구현된 통합아키텍처 모델로부터 이해가 복잡한 철도안전정보지원시스템을 통합된 하나의 모델로 일관

되게 가시화할 수 있으며, 상위 의사결정자를 포함한 여러 이해당사자들의 시스템에 대한 이해를 증가시킨다.

안전정보지원시스템 설계 및 개발기술의 전형적 프로세스, 방법 그리고 도구 등에 대해서 선진국들이 복잡한 시스템 개발에 이용하는 Know-how를 안전정보지원시스템 요구사항의 아키텍처 정의개념에 적용함으로써 시행착오를 방지하고 기술경쟁력을 제고할 수 있다. 이를 바탕으로 시스템 상부구조 설계 생산성을 지원하는 임무 또는 시나리오 분석, 요구사항 분석, 기능 및 거동분석, 인터페이스 및 아키텍처 정의 방법 등은 시스템개발 기술 자립을 촉진하며 전산보조 시스템공학의 실용화를 추구할 수 있다.

향후 추진 방향

향후 철도안전정보지원시스템의 요구사항 아키텍처를 통하여 DB전문가와 팀을 구성하여 상세 시스템을 개발하고, 시스템 관점을 모델링을 해야 한다. 엔터프라이즈 아키텍처를 구축하기 위해서는 표준 및 기술 동향을 고려한 단기, 장기간의 발전계획을 수립하여야 한다.

참고문헌

1. 산업자원부, “전기설비 검사(점검)제도 개선방향에 관한 연구”, 2004. 10.
2. 한국전기안전공사, “전기안전관리제도 연구”, 1992. 12.
3. 한국전기안전공사, “전기재해통계분석”, 2005. 11.
4. EIA, EIA-632: Processes for Engineering a System, Electronic Industries Alliance, 1998.
5. Maier W. and Rechtin E, The Art of Systems Architecting 2nd Ed., CRC Press, USA, pp.19, 2000.
6. Joseph Maley, James Long, Pat Macdonald, Systems Engineering and CORE®: A Natural Approach to C4ISR/DoDAF, Vitech, 2003.

(2007년 7월 12일 논문접수, 2007년 11월 20일 심사완료)