

철도 안전성 평가를 위한 운용 아키텍처 개발 방안 연구

A Study On Operational Architecture Development Method for Railway System Safety Assessment

장재덕* · 박영원*

Jae-Deuck Jang · Young-Won Park

Abstract Recently, Architecture Frameworks are used to develop Information Management System (IMS). This paper describes an operational architecture development method for railway system safety assessment, using DoDAF (Department of Defense Architecture Framework). The need of IMS is increasing to perform safety assessment task effectively and efficiently as safety-critical system like railway System. It is necessary that operational architecture based IMS requirements generated for safety assessment. ARP(Aerospace Recommended Practice)4761 are referred to develop safety assessment operational architecture applicable to railway system. Firstly, schema and template was developed to perform the operational architecture development process using a commercial CASysE(Computer-Aided Systems Engineering) tool, CORE. Not only the operational architecture allows building flexible IMS, but also helps business process solving.

Keywords : Operational Architecture, Schema, DoDAF

요 지 최근 아키텍처 프레임워크가 정보 관리 시스템 개발에 사용되고 있다. 본 논문은 미국방 아키텍처 프레임워크를 사용하여 철도 안전성 평가에 대한 운용 아키텍처 개발 방법론에 대해 기술한다. 철도 시스템과 같이 안전에 민감한 시스템의 경우는 안전성 평가 업무를 효과적이고, 효율적으로 수행하기 위해 정보 관리 시스템의 필요성이 증대되고 있다. 운용 아키텍처를 기반으로 안전성 평가에 대한 정보 관리 시스템의 요구사항을 생성하는 것은 필수적이다. 철도 시스템에 적용 가능한 안전성 평가 운용 아키텍처를 개발하기 위해 ARP4761이 참고 되었다. 우선, 상용 시스템엔지니어링 도구인 CORE를 활용한 운용 아키텍처 개발 프로세스를 수행하기 위해 스키마 및 템플릿을 개발하였다. 운용 아키텍처는 유연한 정보 관리 시스템 구축을 가능하게 할 뿐만 아니라 업무 프로세스의 문제도 해결하는데 도움을 준다.

주 요 어 : 운용 아키텍처, 스키마, 미국방 아키텍처 프레임워크

1. 서론

근래 많은 공공기관, 기업 및 조직 등에서 커다란 이슈는 업무 효율화라고 볼 수 있다. 업무 효율화를 달성하기 위해 많은 시스템들이 만들어지고 활용된다. 그러나 다수의 정보 시스템은 사용자 요구사항을 제대로 반영하지 못하여 적극적으로 활용되지 않거나 사용자가 정보 시스템을 사용하기 위해 본연의 업무가 아닌 추가적인 업무를 수행해야 하는 사

례가 많다. 업무 효율화를 달성하기 위해 사용하는 시스템으로 인해 업무가 더 늘어나는 경우라 할 수 있다. 이러한 문제를 해결하기 위해 업무 및 운용 아키텍처를 개발하고 이를 기반으로 시스템을 개발해야 한다. 특히 안전 업무와 같이 분석적 기능을 수행해야 하는 정보 시스템의 경우, 분석 방법론 및 조직의 안전 업무 활동을 시스템이 잘 지원할 수 있어야 최적의 업무 관리가 가능하다. 철도와 같이 안전 요구사항에 민감한 시스템의 경우는 위험 분석 및 안전성 평가 업무를 효과적이고 효율적으로 수행하기 위한 정보 관리 시스템이 필요하고, 시스템을 잘 개발하기 위해서는 운용 아키텍처를 기반으로 시스템의 요구사항을 도출하는 과정이 필수적이다.

† 책임저자 : 정회원, 아주대학교 시스템공학과 박사과정수료

E-mail : bbidak@paran.com

TEL : (02)2071-8483 FAX : (02)2071-8480

* 아주대학교 시스템공학과 교수

MIL-STD-498에서 정의하고 있는 아키텍처는 “시스템 또는 형상항목의 구성품, 그들의 인터페이스, 그리고 이들 간의 수행개념을 식별하는 조직적 구조”이다[1].

본 연구의 대상 영역은 철도에 대한 위험 분석 및 안전성 평가를 수행하는 조직 및 이해당사자와 조직이 수행하는 운영 및 업무 활동을 정의하는 것이며, 조직들 사이의 인터페이스인 니드라인(Needline)의 정의와 운영 정보를 정의하는 운용 아키텍처를 작성하는 것이다.

본 논문은 운용 아키텍처 개발 방안 제시가 주요 목적이고, 사례로 안전 요구사항에 민감한 철도 안전성 평가 프로세스를 제시하고자 한다. 이를 위해 미항공기 관련 안전성 평가 자료를 근거하여 운용 아키텍처 작성을 위한 요구사항을 수집하였고, 방법론으로 미국방 아키텍처 프레임워크(DoDAF)를 적용하였다.

2. 운용 아키텍처 개발 범위 및 개발 전략

2.1 운용 아키텍처 개발 범위

철도 관련 안전성 평가의 운용 아키텍처를 만들기 위해 SAE(Society of Automotive Engineers)에서 발간한 ARP4761을 참조하였다. 이 자료는 시스템 안전공학 및 관리에 대한 수행 방법 및 최적 사례를 제시하고 있으며, 시스템 라이프사이클 전반에 걸쳐 수행되어야 할 시스템 안전성 평가 프로세스를 보여준다. 본 논문에서는 ARP4761에서 제시하는 안전성 평가 프로세스를 DoDAF 기반으로 모델링하여 운용 아키텍처를 개발하는 과정과 산출물에 대해 제시하고자 한다.

2.2 운용 아키텍처 개발 전략

본 논문에서는 운용 아키텍처 개발을 위해 PMTE(Process, Methods, Tools, Environment) 패러다임을 전략으로 적용한다[2]. 본 연구에 적용하는 프로세스는 미국방 시스템엔지니어링의 표준인 MIL-STD-499 및 미국 민수분야 시스템엔지니어링 표준인 EIA-632(EIA-Electronic Industries Alliance)의 시스템설계 프로세스를 따라, 철도 안전성 평가에 대한 요구사항 분석, 기능 분석 및 해석을 통한 합성을 수행한다. 이와 같이 시스템엔지니어링의 특징인 총체적 또는 체계적 접근법을 통해 철도 안전성 평가를 위한 요구사항을 충실히 분석한 후 운용 요구사항을 만족하는 운용 아키텍처를 개발할 수 있었다.

본 연구에 적용하는 방법론은 DoDAF로써 조직 간에 지리적/기능적으로 통합된 운용, 시스템, 기술관점의 아키텍처를 구축할 수 있도록 제시된 프레임워크이다. DoDAF는 시스템 엔지니어링을 정보 관리 시스템 분야에 적용하기 위하여 방

법론 수준으로 상세화하여 제시한 설계수단이다. DoDAF는 임무 및 기능 효과도 측면에서 정보 시스템을 기술하는데 통일된 방법론을 제시하며 DoDAF의 운용관점, 시스템관점, 기술관점과 관련한 각 산출물과 시스템엔지니어링 산출물인 운용개념서 및 시스템규격서는 밀접한 연관성을 가진다. 따라서 본 연구에서는, 철도안전정보지원시스템의 아키텍처 개발의 구체적인 방법론으로써 DoDAF를 시스템엔지니어링 프로세스와 일관되게 사용하였다.

도구는 시스템엔지니어링 개발 프로세스와 DoDAF를 지원할 수 있는 CORE를 사용하였다.

환경은 운용 아키텍처를 개발하는 환경에 대한 문제로 본 논문에서는 생략한다.

위에서 언급한 운용 아키텍처를 개발하기 위한 전략은 다음 내용에 적용되어 구체화 된다.

- 운용 아키텍처 스키마 개발
- 모델링을 위한 템플릿 개발 및 활용
- 템플릿 기반 운용 아키텍처 구축

3. 안전성 평가 운용 아키텍처 개발

3.1 운용 아키텍처 스키마 개발 및 적용

아키텍처를 개발하는 가장 큰 이유 중 하나는 이해관계자의 관점에서 통합 및 비교, 의사결정 등을 지원할 수 있는 지침이 필요하고, 일관성을 유지하기 위함이다. 운용 아키텍처를 일관성 있게 개발하고 프로세스에 따라 효과적으로 수행하기 위해서는 아키텍처의 기본 골격이 되는 스키마가 필요하다. 이러한 스키마는 시스템엔지니어링 도구에서 운용 아키텍처 개발을 잘 지원할 수 있도록 내장되어야 한다. DoDAF에는 각 산출물에 따른 CADM(Core Architecture Data Model)을 제공하여 아키텍처 데이터 모델을 제시하고 있지만 이를 모두 적용하는 것은 아키텍처의 복잡성을 증가시킨다. 따라서 본 논문에서는 그림 1과 같이 DoDAF의 CADM을 수정하고, 간략화하여 운용 아키텍처 작성을 보다 쉽게 할 수 있도록 하였다. 그림 1의 스키마는 국방부 “합동 C4ISR 체계 종합구조 설계” 사업 시 개발하여 사용하였고, 이를 본 논문에서도 적용하였다. DoDAF에서 권고하는 운용 관점의 아키텍처와 이를 통해 도출되는 산출물 7종(운영개념서, 운용노드연결기술서, 운용정보교환목록, 조직관계도, 운용활동모델, 운용활동상세기술서, 논리데이터모델)은 그림 1의 스키마를 통해 달성될 수 있다.

우선 아키텍처 구성요소는 이해관계자가 요구하는 관점, 아키텍처의 목적, 아키텍처의 용도에 따라 종류를 달리한다. DoDAF에서는 관점을 크게 운용 관점, 시스템 관점, 기술 관

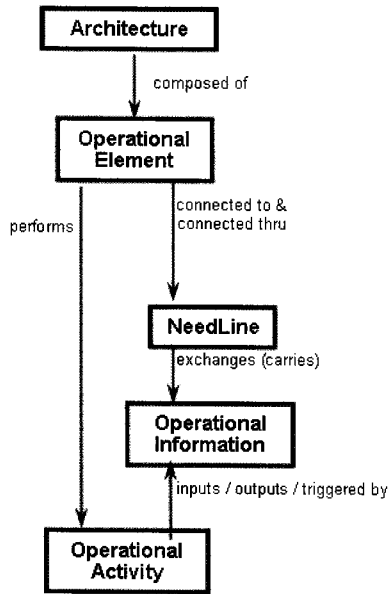


Fig. 1. Operational Architecture Schema[3]

점으로 구분한다. 본 논문에서는 운용 아키텍처 작성이 주요 관심 분야이므로 운용과 관련된 구성요소를 스키마로 개발하여 활용 하였다. 운용구성요소로 표기된 운용노드는 운용 아키텍처에서 정보의 생성, 소비 또는 처리를 위한 핵심요체로 정의한다. 노드는 역할중심, 조직중심, 논리 혹은 기능 중심으로 나누어 노드를 정하는 것이다[4]. 니드라인은 노드 사이의 정보 교환이 존재하고 있음을 나타내는 선을 나타낸다. 운용 활동은 노드가 수행하는 업무 및 활동을 나타내며, 운용 활동 사이의 정보의 흐름을 표현할 수 있는 구성요소로 운용 정보가 존재한다. 이와 같은 운용 아키텍처의 핵심 스키마를 사용하여, DoDAF의 운용 아키텍처 관련 산출물을 작성 한다.

3.2 템플릿 개발 및 활용

운용 아키텍처를 개발하기 위해서 운용 노드, 운용 활동, 운용 정보를 파악하고, 이들의 속성을 잘 도출하기 위해서 모델링을 위한 템플릿을 개발하여 활용하는 것이 필수적이다.

템플릿은 아키텍처를 구축하는 동안 철도 안전성 평가와 관련된 프로세스를 이해관계자들이 모두 이해하고, 개념의 일관성을 확보할 수 있도록 도와준다. 현재 철도 안전성 평가에 대한 프로세스를 이해하기 위해 ARP4761을 참고하여 아키텍처를 작성하지만 참고 된 내용이 획득자, 사용자, 개발자 등의 이해관계자에게 공통적인 이해를 주는 것은 어려운 문제이다. 또한 참고 내용이 현재 철도 관련 안전성 평가 프로세스에서 적용할 수 있는 것인지를 판단하고, 수정 및 개선을 위한 업무를 수행하기 위해서도 템플릿의 사용은 중요하다. 이처럼 이해관계자 사이의 일관된 개념을 유도하고, 명확한 요구사항을 도출하기 위해 그림 2와 같은 아키텍처 템플릿을 개발하였다.

본 논문에서 제시된 템플릿은 이해관계자들이 운용 개념 및 정보 요구사항을 동일한 형식을 통해 일관된 개념으로 작성할 수 있도록 유도한다. 아키텍처의 일관성의 달성은 모든 이해관계자들 간의 개념의 일관성을 유지할 수 있을 경우에도 그 결과물으로써 산출물의 내용이 일관성을 달성할 수 있게 된다.

아키텍처를 구축하는 동안 이해관계자들의 개념이 일관성을 확보할 수 있게 되며, 이해관계자들의 일관된 개념을 담은 아키텍처 산출물을 통하여 이해관계자들 또한 일관된 개념을 확보하는 순환적 개념일치를 이루게 된다. 이러한 순환적 과정을 통해 아키텍처는 상세화되고 성숙된다. 템플릿을 작성을 통해 운용노드의 내용이 '주어', 'From/To'의 내용으로 작성되고, '동사'를 통해 운용활동이 식별된다. 또한 운용활동 사이의 정보는 '무엇을'을 통해 식별되며, 운용활동의 흐름은 '언제'를 통해 식별되고, '어떻게'를 통해 방법 및 수단을 식별한다. 운용 아키텍처 대안들의 시간적 효과성을 확인하기 위해 각 활동별 거동 시간을 기입함으로써 시뮬레이션을 통해 대안 선택의 의사결정을 지원할 수 있도록 하였다. 정보 속성은 향후 안전성 평가를 위한 시스템 구축 시 시스템에서 다루어야 할 정보를 압축력하기 위한 제약 및 성능 요구사항으로 활용 될 내용이다. 이와 같은 내용으로 작성된 템플릿은 시스템엔지니어링 도구에 기입함으로써 데이터베이스를 유

언제	주어	From/To	무엇을	어떻게	동사	거동 소요시간 (sec)	정보 속성									
							시용언어	처리 형태	주기	적시성	무결성 확인	보안 등급	보안 유형	배포지침	상호운용성 요구수준	

Fig. 2. Operational Architecture Template

이름:	위험원(하부시스템FHA+HAZAP)
작성자:	DEW@krdc.co.kr
최초 작성날짜:	4월 23일 09:53:57 AM (KST)
번호:	SDPI.18
약어:	
상세설명:	위험분석및안전성평가수행조직은 FHA와 HAZOP을 통해 하부시스템의 위험을 식별한다.
Fields:	<div style="border: 1px solid black; padding: 2px;"> <input type="text"/> </div> <div style="display: flex; justify-content: flex-end; gap: 5px;"> <input type="button" value="Add"/> <input type="button" value="Change"/> <input type="button" value="Remove"/> <input type="button" value="Sort"/> </div>
Priority:	
사용언어:	한국어/영어
대상언어:	nil
크기:	
단위:	
정확도:	
지리형태:	Direct
주제:	Real-Time
작성권:	
무결성검사:	Necessity
보안등급:	
보안등급:	
실용성요구수준:	기능적
관련조직:	위험분석및안전성평가수행조직

Fig. 3. Operational Information Attribute

지할 수 있다. 그림 3은 CORE를 통해 표현한 운용 정보의 속성을 나타낸다.

3.3 운용 아키텍처 구축

아키텍처 템플릿을 활용하여 어느 정도 개념의 일관성을 확보하게 되면 이를 기반으로 운용 아키텍처를 구축한다. DoDAF에서는 각 산출물 별로 작성해야 하는 주요 내용을 제시한다. 그러나 결과적 내용만 제시할 뿐 구체적 수행 방법을 제시하지 않는다. 따라서 본 절에서는 DoDAF의 지침 및 권고 사항을 바탕으로 아키텍처 구축 방법을 제시한다.

본 논문은 DoDAF의 산출물 의도와 목적을 반영하여 CORE에서 활용 가능한 다이어그램을 산출물의 핵심 결과물로 제시한다. 다이어그램에 사용된 데이터는 스키마를 통해 추적성이 확보되어 기록되며, 이는 향후 아키텍처의 변경 관리를 용이하게 하고, 재활용성을 높일 수 있다.

DoDAF에서 제시하는 아키텍처 산출물 중 제일 먼저 작성하는 것은 운용개념서(OV-1)이다. 이 산출물은 임무수행, 핵심운용노드(조직), 운용능력 등에 대한 총체적인 모습을 표현한 산출물로서 아키텍처 혹은 체계의 개념을 빠르게 포착 가능하게 한다[4]. 그림 4는 철도 안전성 평가를 위한 운용개념서의 핵심 내용이다. 운용개념서의 개념도가 형성되면 운용 활동모델(OV-5) 구축을 시작으로 본격적인 운용아키텍처 모델 구축을 시작한다.

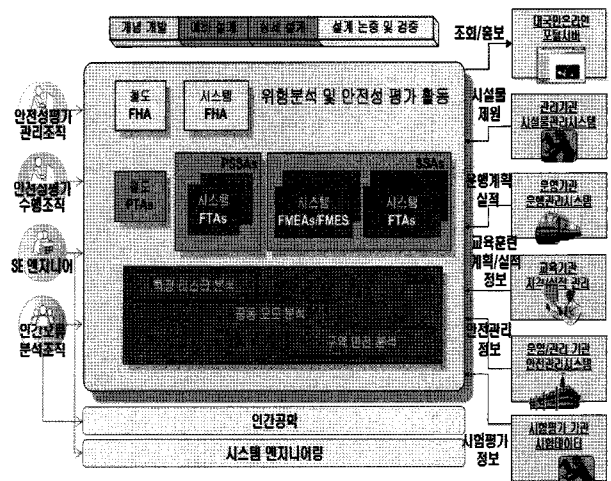


Fig. 4. Operational Concept Diagram (OV-1)

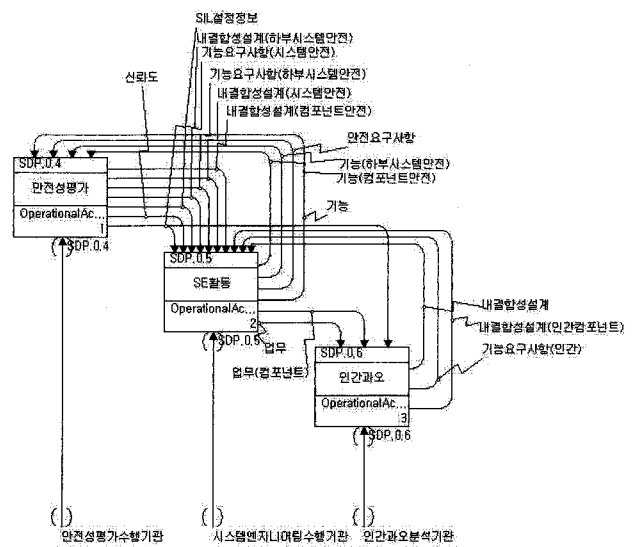


Fig. 5. Top Level Behavior Model (IDEF0)

모델링 템플릿에서 6하원칙에 의거하여 기술된 문장의 각 요소를 아키텍처 요소로 식별하여 운용활동에 대한 흐름을 거동모델로 구축한다. ARP4761에서 참고된 안전성평가 활동, 시스템엔지니어링 활동, 인간요류 분석에 대한 활동으로 상위 조직 수준에서 영역을 구분하였다. 그림 5는 도구에서 표현한 상위 조직 수준의 거동모델을 IDEF0(IDEF-Integrated Definition)로 표현한 것이다. 상위 조직 수준에서 식별된 3가지 운용활동은 분할되어 영역별 거동모델로 나타난다.

안전성 평가 영역의 주요 운용활동은 위험 분석 및 안전성 평가 관리 조직에서 시스템 안전성 계획을 작성하여, SIL(Safety Integrity Level)을 설정한 후 위험 분석 및 안전성 평가 수행 조직으로 전달한다. 위험 분석 및 안전성 평가 수행 조직은 시스템, 하부시스템, 컴포넌트에 대한 단계별 Hazard 분석을

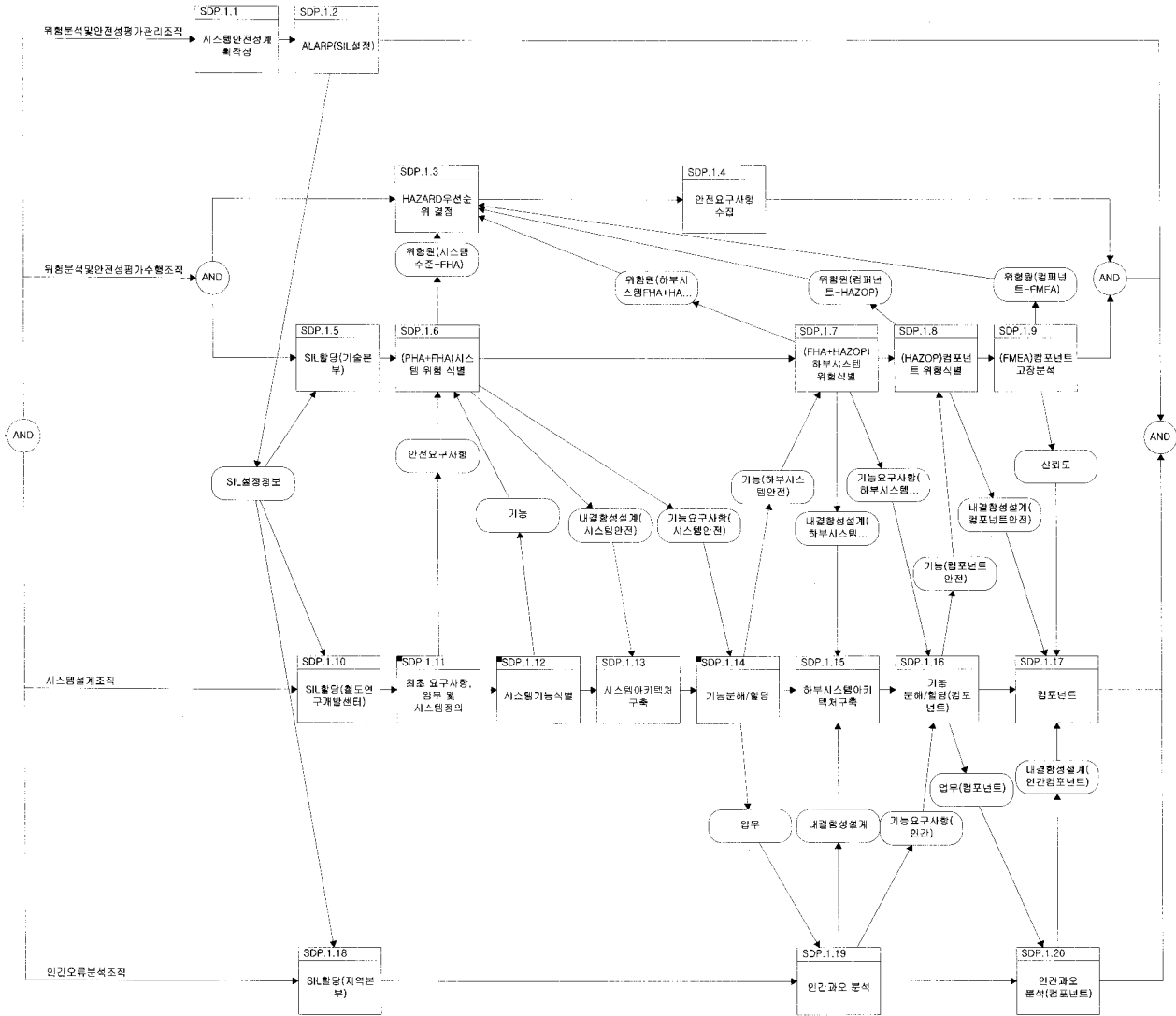


Fig. 6. Safety Assessment Operational Activity Diagram (eFFBD)

수행하고 분석결과로 도출되는 위험에 대한 우선순위를 결정하여 다시 안전요구사항으로 전환하는 거동모델로 나타난다[5].

시스템 엔지니어링 영역의 활동은 최초 요구사항 수집 및 시스템 정의, 시스템 기능 식별, 시스템 아키텍처 구축, 기능 분해 및 할당, 하부시스템 아키텍처 구축, 기능 분해 및 할당 (컴포넌트), 컴포넌트의 활동을 수행함으로써 각 단계에 생성되는 결과물을 출력하여 위험 분석 및 안전성 평가 영역으로 전달하는 거동모델로 나타나고, 인간오류 분석 영역은 시스템 및 하부 시스템에 대한 인간오류 분석 과 컴포넌트 수준의 인간오류 분석으로 활동이 나누어져 거동모델로 표현된다[6].

그림 5의 상위 수준 거동모델을 eFFBD(enhanced Function Flow Block Diagram)를 통해 상세 활동 흐름도로 작성할 수 있다. 다음 그림 6은 안전성 평가를 위한 각 조직별 상세 활동 흐름을 보여준다. 상세 활동 흐름도에 나타나는 모델은 운용

활동상세기술서(OV-6)의 내용으로 포함된다. 운용활동모델이 완성되면 이를 각 활동별로 활동의 주체를 표현하여 향후 운용노드에 할당하게 된다. 상세 활동 흐름도에서 운용노드를 기반으로 운용활동의 시간적인 순서와 운용정보인 입력력 정보를 파악할 수 있다. 운용활동모델과 운용활동상세기술서는 서로 동기화되어 모델의 전환이 가능하게 구성 되었다. 운용활동을 필요한 수준까지 상세화하는 과정은 모델 성숙도를 높여가는 과정이다. 아키텍처 개발 프로세스에 관한 설명에서 모델 성숙도의 한계는 아키텍처 구축 목적에 적합하도록 설정하여야 한다. 본 연구에서는 조직들이 안전성 평가를 수행하는 프로세스를 운용 아키텍처를 통해 보여준다. 상세수준이 잘 정의 되면 운용노드들 사이에 입출력되는 정보를 통해 어떠한 산출물이 있어야 하는지도 명확하게 정의 될 수 있다. 그림 6의 프로세스는 크게 세 가지 영역으로 나누어진다.

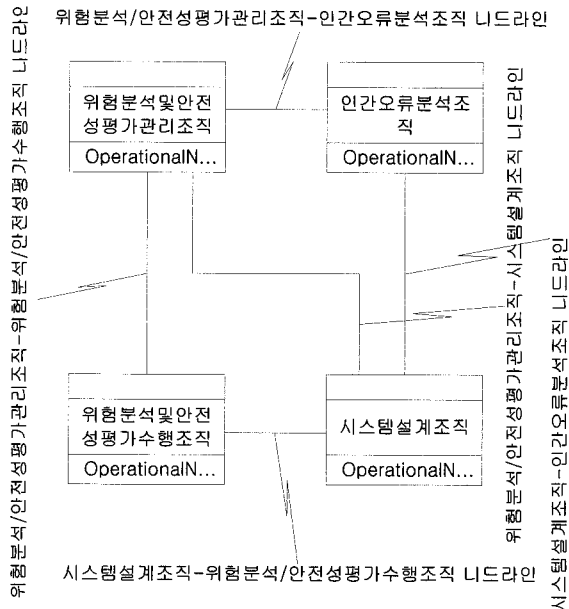


Fig. 7. Operational Node Connectivity Diagram(PBD)

시스템 설계 프로세스, 인간공학의 인간오류 분석 프로세스, 안전 분석의 FHA(Functional Hazard Analysis), HAZOP(Hazard and Operability), 그리고 FMEA(Failure Mode and Effect Analysis) 프로세스로 구성되어 있다. 수명주기가 흘러감에 따라 시스템에서 컴포넌트로 설계의 대상이 상세화 되는 것을 나타낸다. 본 모델에서는 최상위 시스템에 대해서는 FHA를, 하부시스템에 대해서는 FHA와 HAZOP을 위험 분석 방법으로 채택하였다. 여러 분석 방법 중에서도 두 가지 방법을 택한 이유는 시스템을 설계하는 초기에는 구체적인 컴포넌트가 구현되어 있지 않고 기능만이 식별되기 때문에 기능 분석 결과를 활용할 수 있는 FHA와 HAZOP 이 강점을 가지고 있기 때문이다.

운용활동이 할당된 운용노드(Node)들은 조직구성과 대부분 일치하나 현재 작성된 운용활동 모델과 같이 임시조직인 경우 기본 구성과 일치하지 않을 수도 있으며, 한 조직이 여러 시스템을 다루는 경우 등 조직의 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 PBD(Physical Block Diagram)를 제시한다. 운용노드연결기술서에는 조직과 조직 사이에 운용활동을 통해 주고 받는 정보를 개념적 선인 니드라인을 활용하여 표현해준다. 그림 7은 운용노드연결기술서의 핵심적인 다이어그램을 보여준다. 운용노드연결기술서에 나타난 니드라인을 통해 유통되는 정보는 운용정보교환목록(OV-3)을 통해 표로써 나타날 수 있다. 니드라인을 기반으로

정보의 명칭과 앞서 템플릿에서 기록된 정보의 속성, 그리고 정보의 생산자 및 소비자를 구분하여 표로써 제시할 수 있다.

4. 결론

본 논문의 연구 결과는 철도 안전성 평가 프로세스를 사례로 하여 운용 아키텍처로 개발하는 방법을 제시한 것이다. 본 논문에서는 크게 세 가지 내용을 다루었다. 첫째, 운용 아키텍처를 구성하는 데이터들을 스키마를 통해 정의하였다. 스키마는 시스템엔지니어링 도구에 내재되어 운용 아키텍처 데이터들 사이에 추적성을 확보할 수 있도록 한다. 추적성 확보는 변경된 내용을 쉽게 파악할 수 있도록 도와주며, 데이터 관리를 용이하게 한다. 둘째, 운용 요구사항을 효과적으로 수집하기 위해 템플릿을 개발하였다. 템플릿을 통해 바르게 정의된 운용 요구사항은 운용 아키텍처를 구축하는 기반이 된다. 셋째, 운용 아키텍처 구축을 위해 DoDAF 산출물의 목적과 의도에 적합하도록 다이어그램을 작성하고 활용하는 내용을 제시하였다.

본 논문에는 운용 아키텍처를 개발하는 핵심 내용들만 다루었다. 아키텍처 대안 분석, 활용 등의 내용은 제외되었다. 향후 이러한 내용을 더 보완해야 할 것이다. 운용 아키텍처를 개발한 이후의 프로세스는 시스템 및 체계 아키텍처를 개발하는 것이다. 현행(As-Is) 운용 아키텍처를 잘 개발해야만 운용을 올바르게 지원하는 시스템을 개발할 수 있다. 운용 아키텍처 개발은 운용 및 업무 정의에서 시스템 개발 단계까지 일관성을 확보할 수 있는 수단으로 사용되고, 향후 시스템의 진화를 관리 할 수 있는 지침이 될 수 있다.

참고문헌

1. Department of Defense (DoD) (1994), "Software Development and Documentation", Mil-Std-498, USA, pp. ii.
2. Martin, J. N. (1997), "Systems Engineering Guidebook: A Process for Developing Systems and Products," CRC Press, USA, pp.51.
3. 국방부(2004), "합동C4ISR 체계 종합구조설계(작성) 결과 보고서", 과제 수행 결과 보고서, pp.5-41.
4. DoD Architecture Framework Working Group (2003), "DoD Architecture Framework Version 1.0," pp.4-1, 4-7.
5. SAE (1996), "SAE ARP4761 : Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment", Society of Automotive engineers, Inc., USA, pp.13.
6. 박종용(2003), "안전중시 시스템을 위한 동시공학적 설계 모델", 아주대학교 시스템공학과 박사학위논문, pp.68-84.

(2007년 12월 27일 논문접수, 2008년 2월 20일 심사완료)