J. Korea Saf. Manag. Sci. Vol. 15 No. 1 March 2013
http://dx.doi.org/10.12812/ksms.2013.15.1.1

ISSN : 1229-6783 (Print)
ISSN : 2288-1484 (Online)

상호운용성을 요구하는 복합시스템 개발에서 DoD 아키텍처 프레임워크를 활용한 안전성 확보에 관한 연구

김 영 민* · 이 재 천*
*아주대학교 시스템공학과

A Study on Safety Coordination for a Complex System Comprised of Interoperable Systems Utilizing DoD Architectural Framework

Young-Min Kim* · Jae-Chon Lee*
*Dept. of Systems Engineering, Ajou University

Abstract

The recent trend in the war fields on the globe may be characterized by the network-centric warfare, which would, in turn, make the concept of weapon systems be changed. To this end, the concept of system of systems (SoS) has been introduced in literature. An SoS is a collection of multiple systems, each of which is an independent system and can be interoperable with each other. Thus, in defense domain each SoS is a big weapon system as a whole operated in actual environment and each element of it is also an independent smaller weapon system, but they should be interoperable via network among each other. The safety results studied for each elementary system alone may not be fully applicable to the whole SoS. As such, the objective of this paper is to study how to make the SoS safety requirements be distributed down over the interoperable elementary systems. Since handling the interoperability requires a technique of systems architecture, a standard method called the DoD Architectural Framework (DoDAF) has been used here to derive a solution. Using DoDAF, the safety requirements were first analyzed in the operability environment. The results were then studied to be included in an integrated model of both the systems design and safety processes. A further study of present paper would facilitate ensuring safety in the development of SoS weapon systems in practice.

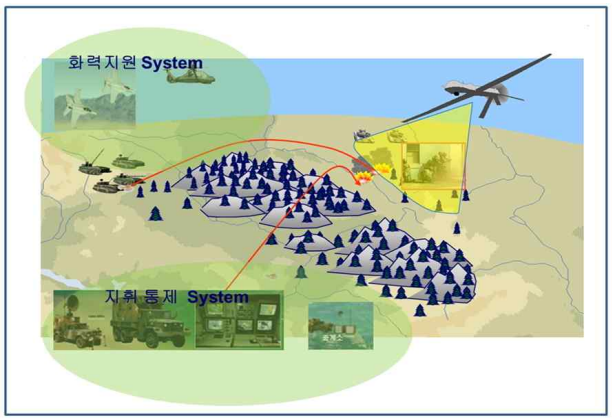
Keywords : System of Systems, Interoperability, Systems Design, Systems Safety, DoDAF(Department of Defense Architecture Framework), NCW(Network-centric warfare)

† 이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No.2012R1A1A2009193)

† Corresponding author: Prof. Jae-Chon Lee, Dept. of Systems Engineering, Ajou University, Wonchon-dong, Youngtong-gu, Suwon, 443-749. Tel: 031-219-3941, E-mail: jaelee@ajou.ac.kr
Received January 18, 2013; Revision Received March 5, 2013; Accepted March 14, 2013.

1. 서 론

오늘날 현대전에서 사용되는 무기체계의 구성은 매우 고도화된 기술의 집약된 결과로서 수많은 하부 체계로 구성되어 있다[1]. 따라서, 개발단계의 통합관점에서 바라본다면, 개별 체계에서 개발에 성공하였다고, 전체 시스템의 개발이 성공 했다고 보기 어려운 시기에 와있다. 또한, <Figure 1>의 국방 분야 무인항공기의 상위단계 운용 개념에서 볼 수 있듯이, 개발단계 이후의 운용 단계에 있어서, 해당 시스템을 운용하는 조직과, 또 다른 조직에서 운용되는 시스템 간에 데이터가 연동되어 운용되는 점을 생각 한다면 오늘날 시스템이 얼마나 대형화되고 복잡화 되었는지 알 수 있다.



<Figure 1> The top-level concept of a unmanned aerial vehicle in the war field

이러한 점에서 시스템 간에 상호 운용성(Interoperability)에 관한 측면은 그 어느 때 보다 중요하게 여겨지고 있다[2]. 따라서, 대형 복합시스템 설계단계의 통합과정에서 인터페이스로 인한 수많은 문제가 야기됨에 따라 시스템을 구성하는 하부 시스템들 간의 상호 운용성에 관한 측면 등 다양한 방안을 통해 체계간 인터페이스로부터 발생되는 문제를 해결하기 위해 다각도로 연구가 활발히 진행되고 있다[3].

현재까지, 시스템 개발 및 운용에 관해, 안전에 관한 수행은 대부분의 활동이 상세 설계단계에서의 기능중심 안전 활동에 초점을 두었다면, 최근 안전성에 대한 패러다임은 전체 시스템 설계 뿐만 아니라 설계이후의 단계인 운용유지 및 폐기 단계까지 고려한 패러다임이라고 할 수 있겠다[4].

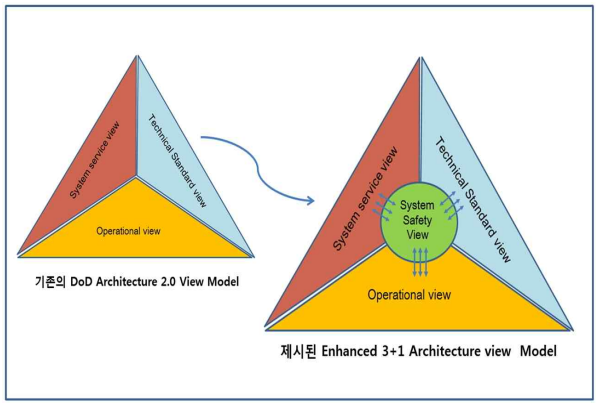
또한, 시스템의 대형화 및 복잡화에 따라, 시스템을 개발하고 운용하는데 있어서 급증하는 상호운용성에 관해 발생하는 문제로 인해 안전에 관한 새로운 패러다임은 단일 시스템의 안전 추구에서 보다 확장된 형태인 대형 복합시스템의 상호 운용으로부터 야기되는 안전 문제를 해결할 수 있는 연구가 필요한 시점에 와있다. 이러한 점에서 또한, 시스템공학의 최근 추세는 대형 시스템의 전 수명 주기적 그리고 전체 시스템을 계층적 관점에서 바라보고 문제를 해결하고자 한다. 미국의 경우, 상호 운용성을 강조한 시스템공학 기반의 DoDAF(Department of Defense Architecture Framework)를 통해서 무기체계의 개발 및 운용에 의무적으로 활용한 다는 점에서 대형 복합시스템을 구성하는 하부 체계간 상호운용으로부터 발생하는 안전에 대한 문제를 해결하는데 있어서 유용하다 말할 수 있겠다.

이렇듯, 대형복합 시스템의 개발 및 운용에서 상호운용성에 관해 발생될 수 있는 문제를 해결하고자 미국 국방성에서는 DoDAF의 초기 형태인 C4ISR(Concept of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) AF(Architecture Framework)를 1996년 만들어 Version 1.0을 제시하였다. 이를 통해, 효율적인 대형 국방 시스템 개발 사업을 추진하기 위해서 의무적으로 사용되도록 규정하였다. 최근까지 미 국방성(DoD, Department of Defense)은 DoDAF의 Version 2.0까지 공고하였으며, 이러한 DoDAF는 주어진 자원(Resource)을 효율적으로 운용하기 위해, 시스템 개발과 운용에 필요한 산출물을 개발하고, 표현하며 통합하기 위한 공통 접근 방법을 정의한다. 따라서, 시스템의 대형화와 복잡화에 따라 개발단계에 위치한 시스템의 상호운용으로 부터 안전과 직결되는 문제를 시스템공학 기반의 DoDAF을 바탕으로 안전성 측면에서 보다 강화된 아키텍처 프레임워크를 바탕으로 보다 개선된 대형복합 안전중시 시스템 설계의 안전도 향상을 추구할 수 있을 것이다.

본 연구진은 관련 주제에 대한 연구를 최근에 선행연구를 통해 발표하였다[3],[5],[6]. 제시되는 선행연구의 공통점은 시스템 설계활동과 시스템 안전 활동을 통합된 형태로 추구하기 위해 연구되었다. 선행연구 [5]에서는 철도 시스템 개발에서 수명주기에 따른 시스템공학 프로세스와 안전성 평가를 동시에 고려한 통합 프로세스를 제시하였으며, 선행연구 [6]에서는 개념설계단계에서의 시스템 수명주기와 계층 수준에 따른 시스템공학 설계 프로세스와 시스템 안전프로세스의 활동과 활동에 따른 입·출력 데이터 분석을 통해서 통합 설계 프로세스 모델을 제시 하였다. 선행연구[3]을 통해, 시스템공학 설계 프로세스와 시스템 안전 프로세스 수행을 통해 발생되는 산출물에 대해 기존에 제시한 통합 설계프로세스에 대해 데이터 모델 관점에서 접근하여 보다 개선된 통합 프로세스 모델을 제시하였다.

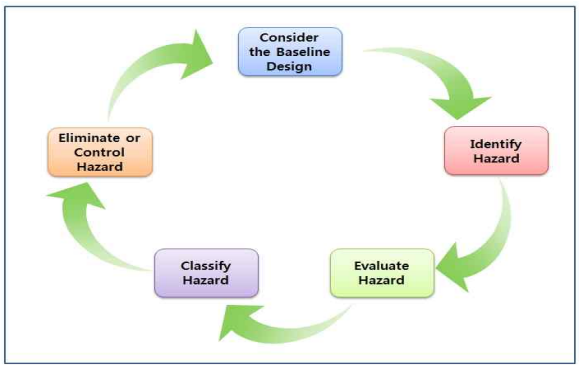
ISSN : 1229-6783 (Print)
ISSN : 2288-1484 (Online)

하지만, 아직 국내에서는 시스템 설계와 시스템 안전을 동시에 고려한 기술이 부족할 뿐만 아니라, 상호 운용성 요소를 반영한 연구 미흡한 실정이다. 또한, 기존 연구를 통해서는, 서두에 언급한대로, 단일시스템이 아닌 대형 복합 시스템의 설계에 있어서 체계 간 상호 운용으로 부터 발생할 수 있는 안전문제를 해결하기에는 한계가 있다. 따라서, <Figure 2>에서 제시되는 것처럼, 기존에 제시된 DoDAF를 설계와 운용 측면에서의 상호운용에 관해 발생할 수 있는 안전 문제 해결에 활용한다면 유용할 것이다. 하지만, 기존 DoDAF의 문제점은 안전에 관한 문제를 중점적으로는 다루지 않았을 뿐더러, 안전과 설계 및 운용과의 상호 유기적인 연계성에 관한 제안을 하지 못하고 있다.

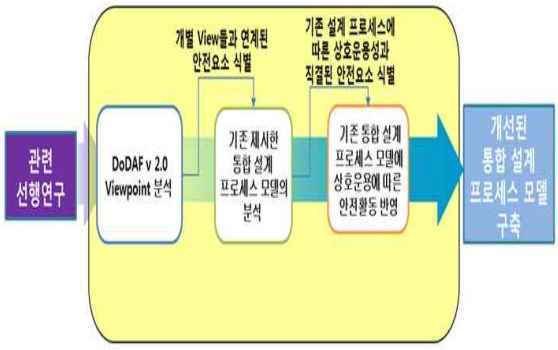


<Figure 2> An enhanced 3+1 model of DoDAF augmented by safety

따라서, <Figure 3>에서 제시되는 일반적인 단일 시스템 안전 확보를 위한 안전 분석 프로세스에 대해서 상호 운용으로 부터 발생되는 안전 문제를 해결하기 위해서 DoDAF를 통해 상호 운용성으로 부터 발생 가능한 상위레벨에서의 안전 문제를 해결하고 설계와 운용단계에 적용 가능한 통합 설계 프로세스 모델을 제시하였다.



<Figure 3> A typical view of safety analysis process



<Figure 4> A conceptual diagram representing the objectives of the paper

본 논문의 구성은 다음과 같다. 서론에서는 사회 및 연구의 연구동향과 필요성을 제시하였고, 2장에서는 관련 선행연구 및 연구 목표를 기술하여 문제정의를 언급하였다. 3장에서는 기존의 DoDAF를 안전관점에서 재분석하기 위한 활동들을 명시하고 수행결과를 바탕으로 안전관점에서 DoDAF를 재정립 하였다. 4장에서는 분석된 DoDAF를 바탕으로 기존에 제시한 통합 설계 프로세스 모델과의 연동 모델을 제시하였다. 또한, 5장에서는 상호운용 기반의 안전성 기반의 통합 설계 프로세스 모델에 대한 검증을 수행하였으며, 마지막 6장에서는 본 논문의 결과를 정리 및 요약 하였다.

2. 문제의 정의

2.1 설계활동에서 개념설계 단계의 안전 활동 및 DoDAF 기법 반영의 중요성

모든 시스템 설계의 첫 단추 역할을 하는 개념설계 단계는 시스템을 개발하는데 있어서 상세설계 단계로 진입하기 위한 토대를 마련하기 위해서 상위 수준에서의 설계 활동을 통한 산출물을 제공한다. 이러한 정보는 안전 활동에 있어서도 마찬가지로 개념설계 단계에서부터 안전 활동을 통한 중요한 산출 결과물을 제공함으로써 개념설계 단계의 중요성을 인지할 수 있겠다. DoDAF 수행에 따른 산출물은 시스템의 설계 및 운용에 있어서 대형복합 시스템을 개발하고 운용하는데 있어서 필수적인 정보를 제공한다. 이러한 정보들은 시스템 설계 단계 및 운용단계에 관여하는 다양한 이해당사자간의 의사결정에 있어서 필요한 정보를 제공하는데 DoDAF는 중요한 기준 틀을 제공하고 있다. 따라서, 아키텍처 프레임워크를 통해서 개발에 참여하는 이해

당사자간에 동일한 관점에서 개발에 참여 할 수 있게 되어, DoDAF에 따른 시스템 개발에 있어서 성공적 수행이 될 것으로 기대된다.

공통(All Viewpoint)	모든 뷰포인트들과 연관된 아키텍처 컨텍스트의 대단히 중요한 측면에 대해서 설명
운용(Operational Viewpoint)	운용적 측면에서 목적을 달성하기 위해 필요한 것과 누가 그것을 수행하는지를 식별 (능력을 지원하기 위한 운용시나리오, 활동, 요구사항을 포함)
체계(System Viewpoint)	체계관점에서 운용에 필요한 것과 연관된 시스템, 특성에 대해 기술
기술(Technical Standards Viewpoint)	기술관점에서 표준과 관례를 규정

<Figure 5> The four principal viewpoints of DoDAF

2.2 안전관점에서 DoDAF 개별 뷰(View) 분석의 필요성

DoDAF는 <Figure 5>을 통해서 제시되는 것처럼 크게 4가지 관점인 공통 관점(All Viewpoint), 운용 관점(Operational Viewpoint), 시스템 관점(System Viewpoint), 기술 관점(Technical Viewpoint)을 통해서 시스템 설계와 운용에 필요한 정보를 산출물로 정의하고 있어, 설계과정에 있어서 중요한 정보를 제공한다. 하지만, 개별 관점(View)이 지니고 있는 시스템 안전관점에서의 특성을 정의하고 있지 못하고 있다. 그로인해, 오늘날 개발되는 대형화 시스템 개발의 추세에서 안전 문제에 관해 대응하는데 있어서 어려운 점이 많다. 따라서, 기존에 제시된 DoDAF를 안전관점에서의 재분석을 통해 DoDAF에서 지원하는 상호 운용성 기반의 발생 가능한 안전 문제를 본 연구 수행을 통해 해결하고자 한다.

2.3 연구 목표 및 범위

본 연구에서는 <Figure 8>을 통해 제시되는 것처럼, 기존 연구 활동을 통해 제시한 시스템공학 프로세스와 시스템안전 프로세스의 통합 프로세스 모델을 바탕으로 DoDAF의 안전 관점에서 재분석한 결과의 적용을 통해 상호 연동성 분석에 따른 보다 개선된 통합 프로세스 모델을 제안한다. 그밖에, 상호 운용성 측면의 안전성에 대해 개선된 통합 설계 프로세스 모델을 전산 지원 도구를 활용해 모델의 구축 및 검증에 관한 연구를 수행 하였다. <Figure 4>을 통해 상호운용 기반의 안전성 문제에 관해 개선 통합 프로세스 모델 구축에 대한 연구 수행 방법을 도식화 하였다.

일반적으로 시스템공학에서 시스템 수명주기는 참고문헌 [7],[8],[9]에서 제시되는 것처럼 여러 형태로 제시되고 있지만, 큰 맥락에서, 개념 설계단계, 상세 설계단계, 양산 및 운용단계로 정의 할 수 있다. 따라서, 상위 수준의 설계단계에서 적용 가능한 연구를 수행하기 위해서, 본 연구의 범위는 개념설계 단계로 범위를 한정 및 설정 하였다.

3. 시스템 안전관점에서 DoDAF 분석

3.1 Viewpoints 따른 아키텍처 산출물 분석활동

DoDAF에서 말하는 Viewpoint는 모델 또는 View의 집합이다. 반대로, View는 목적에 맞는 데이터가 수집되고 더해진 모델을 지칭한다. 따라서, Viewpoint는 특정 목적을 위한 데이터가 더해진 모델인 View들의 집합이라고 할 수 있다.

본 단계에서는 <Figure 5>에서 제시된 DoDAF의 핵심 4가지 기본 뷰포인트를 중심으로 안전 관점에서 분석을 수행한 결과를 설계단계에 반영하기 위한 연구를 수행하였다. 따라서, DoDAF에 대한 안전관점에서의 분석 결과를 설계단계에 적용하기 위해 아래와 같이 4가지 관점의 기준을 바탕으로 수행하였다.

Step 1. DoDAF에서 제시되는 뷰 포인트(Viewpoints)의 개별 산출물과 속성을 분석 및 정의 한다.

Step 2. 개별 뷰(View)로부터 생성된 산출물 분석을 통해서 관련 안전관리 요소를 정의한다.

Step 3. 정의된 안전관리 요소와 시스템 안전 확보를 위한 관련 안전 활동 및 산출물과의 연동성에 관한 분석 및 정의한다.

Step 4. Step 3. 수행에 따른 정의된 산출물과 기존 개념 설계 단계의 시스템 설계 산출물과의 연동성 분석 및 정의

3.2 DoDAF 수행에 따른 개별 Viewpoints 산출물의 안전 속성 분석

<Figure 5>에서 제시하는 기본 뷰포인트를 바탕으로 <Figure 6>와 같이, 최근 버전 2.0을 통해 보다 다양화된 뷰 포인트까지 제시하여 많은 요소들을 설계 및 운용단계에 반영하였다. <Figure 6>은 DoDAF의 개별 뷰(Virew) 수행을 통한 산출물을 정리한 것 이며,

산출물에 대해서 안전관점에서의 분석을 통해, 최종적으로, 산출물과 직결하는 안전관리 항목을 도출하였다. 도출된 안전관리 항목은 이후 연구 활동인, 설계단계의 산출물과의 연동성 구축에 중요한 요소로 활용되었다. 또한, 개발된 안전관리 항목은 개별 항목에 관한 안전 활동 산출물과의 연동성 분석을 통해 <Table 1>과 <Figure 7> 처럼 제시하였다. 따라서, 안전관리 항목과 연관되어 발생할 수 있는 대형복합 시스템의 안전 문제를 해결하고 성공적인 개발이 되기 위해서 개별 뷰(View)와 안전 활동 및 산출물 그리고 설계활동과 관련해 상호관계를 정립하는 발판을 마련하여 이후, 설계 및 안전 활동에 있어서 활용적 가치를 높였다.

관 점		세부 관점	명 칭	구성 및 설 명	안전관리 항목
v 1.5	v 2.0				
All Viewpoint (AV)	All Viewpoint (AV)	AV-1	아키텍처 개요 및 요약	범위, 목적, 사용자, 환경 및 분석결과	운용, 프로젝트, 제약
		AV-2	통합사전	AF에 사용되는 용어의 정리	운용, 조직, 규칙, 프로젝트, 데이터
Systems View (SV)	Systems Viewpoint (SV)	SV-1	시스템 인터페이스 기술서	시스템, 서브-시스템 식별 및 연동성 식별	시스템, 인터페이스
		SV-2	시스템 자원(리소스) 흐름 기술서	시스템간에 교환된 자원의 흐름를 기술	시스템, 자원
		SV-3	시스템-시스템 메트릭스	시스템 사이의 관계를 기술	시스템
		SV-4	시스템 기능 기술서	시스템에 의해 수행되는 기능과 시스템 기능 사이의 데이트 흐름 제시	시스템, 기능, 데이터
		SV-5	시스템과 운용활동과의 추적성 메트릭스	시스템 기능-운용적 활동 사이의 연동성 제시	시스템, 기능, 활동, 추적성
		SV-6	시스템 자원(리소스) 흐름 메트릭스	상세한 자원(리소스) 흐름를 정의	시스템, 자원
		SV-7	시스템 측정 메트릭스	시스템 모델 요소들의 측정 척도 기술	시스템, 성능, 측정 비기능, 요구사항
	Service Viewpoint (SvcV) *[New Viewpoints]*	SvcV-1~2	1: 서비스 컨텍스트 기술서 2: 서비스 자원(리소스) 흐름 기술서	1: 서비스 식별 2: 서비스 사이의 교환된 자원의 흐름 기술	서비스, 자원
		SvcV-3a~3b	3A: 시스템-서비스 메트릭스 3B: 서비스-서비스 메트릭스	3A:시스템과 서비스 사이의 관계 3B:기술된 아키텍처 기술서에서 서비스 사이의 관계	시스템, 서비스
		SvcV-4	서비스 기능 기술서	서비스 기능사이의 서비스와 서비스 데이터 흐름에 의해 수행된 기능	기능, 서비스, 데이터
Operational Viewpoint (OV)	Operational Viewpoint (OV)	OV-1	운용개념도	상위 수준의 조직, 임무, 배치, 연결의 운용개념 표현	운용
		OV-2	운용노드 연결 기술서	운용노드에서 수행되는 활동 및 노드간의 정보 흐름 표현	운용, 활동, 정보
		OV-3	운용 자원(리소스) 흐름 메트릭스	노드간 교환되는 정보의 속성표	자원, 정보
		OV-4	조직관계도	조직간의 지휘,통제,조정의 관계도	운용, 조직
		OV-5a	운용 활동 분해모델	업무활동의 계층화 흐름도	운용,능력, 활동,
		OV-5b	운용적 활동 모델	활동, 입출력물 사이의 운용적 활동과 능력의 컨텍스트	운용, 능력, 활동
		OV-6a	운용규칙모델	운용적 활동을 기술하기 위해서 사용된 모델(운용규칙과 제약조건)	운용,활동,규칙,제약
		OV-6b	상태전이 기술서	운용사건에 대한 프로세스 반응 정의도(거동분석, 제약 식별 등)	운용, 상태, 제약
		OV-6c	운용사건추적 기술서	운용시나리오, 사건의 순서에 대한 결과 추적도	운용, 이벤트
Technical View (TV)	Standards Viewpoint(StdV) *[Renamed]*	StdV-1	기술표준 목록	해결 요소들에 적용하기위한 표준 리스트	제약
		StdV-2	미래표준 목록	새로운 표준과 현재의 솔루션 요소에 대한 잠재적인 영향에 대한 설명	제약
	Project Viewpoint (PV) *[New Viewpoints]*	PV-1	프로젝트 포트폴리오 관계	프로그램,프로젝트,포트폴리오에 대해 조직 관점에서 나타냄	프로젝트,조직, 서비스
		PV-2	프로젝트 일정	프로젝트 운용 및 조정	프로젝트, 운용, 시간
		PV-3	프로젝트-능력 맵핑	프로젝트에 능력 요구사항을 추적	능력, 요구사항, 프로젝트
	Data & Information Viewpoint (DIV) *[New Viewpoints]*	DIV-1	개념적 데이터 모델	요구되는 상위 레벨 데이터 개념과 그들의 관계를 기술	정보, 데이터, 요구사항
		DIV-2	논리적 데이터 모델	데이터 요구사항과 구조적 업무 프로세스 규정에 관한 문서화	정보, 요구사항, 활동, 요구사항, 제약, 데이터, 검증
		DIV-3	물리적 데이터 모델	논리적 데이터 모델 객체의 물리적 이행 양식	데이터
	Capability Viewpoint (CV) *[New Viewpoints]*	CV-1	비전	프로젝트의 비전, 목표, 계획, 활동, 척도, 조건 등을 기술	운용, 활동, 제약, 프로젝트
		CV-2	능력 분류	사용된 모든 용어 기록 능력 요구사항의 식별	능력, 요구사항, 데이터, 프로젝트
		CV-3	능력 단계	특정 시점에 달성되어야 하는 계획된 능력을 기술(활동, 조건, 표과, 규칙 등)	활동, 능력, 제약
		CV-4	능력 독립성	계획된 능력과 능력의 논리적 그룹의 정의 사이의 독립성	능력
		CV-5	능력-운용 개발 연동	능력 요구사항의 이행	능력, 요구사항
		CV-6	능력-운용적 활동 연동	능력을 지원하는 운용적 활동과 요구되는 능력과의 연동	운용, 활동, 능력
		CV-7	능력-서비스 연동	능력을 구현 가능하게 하는 서비스와의 연동	운용, 서비스

<Figure 6> Generation of safety-related items by analyzing DoDAF (v2.0) from a safety viewpoint

<Table 1> Analysis of the possible linkages between each of the safety management item and the artifacts obtained from its associated safety activity

안전관리 항목	정의 및 설명	관련 안전 활동 산출물
프로젝트	설계 및 운용단계 보다 상위 단계 개념인 관리적 측면에서 관련한 안전사항	Safety Plan Safety Design Plan Prelim. Safety Doc.
운용	개발된 시스템을 운용하는데 있어서 수반되는 안전사항	Hazard Analysis Data Monitored Performance Data PHL(Preliminary Hazard List)
제약	프로젝트 운용 및 개발단계에서 조직 또는 대상 시스템이 준수해야하는 표준 및 관련 규정	International Standard Handbook Safety Requirement
조직	시스템을 개발 또는 운용관점에서 관련한 조직관점에서의 안전사항	International Standard Safety Plan
시스템	설계 및 운용단계의 시스템과 관련해 발생 가능한 안전사항	Prelim. Hazard Analysis Data Safety Design Plan
인터페이스	시스템을 구성하는 하부 체계간 상호 연동성과 관련한 안전사항	Specified Safety Function Safety Design Plan Hazard Analysis
기능	개발 및 운용되는 대상시스템이 지원하는 기능과 관련되어 수반되는 안전사항	Monitored Performance Data Specified Safety Function Updated Safety Function Safety Requirement
시간	개발 프로젝트의 관리적 측면에서 관리되어져야 할 사항	Safety Plan Safety Design Plan Updated Safety Design Plan
능력	개발되는 시스템이 운용단계에서 지녀야 할 능력	Monitored Performance Data Safety Requirement
데이터	시스템을 구성하는 하부 컴포넌트 또는 개발 및 운용 단계의 조직에서 상호 교환되어지는 데이터와 관련한 안전사항	International Standard Detailed Hazard Analysis Data Monitored Performance Data
요구사항	설계 및 운용단계에서 요구되는 요구사항과 관련되어 수반한 안전관리 사항	Safety Requirement Ordinance
활동	설계 및 운용단계에서 요구되는 활동수행에 따라 관리가 요구되어지는 안전관리 요소	Safety Plan Safety Design Plan PHL(Preliminary Hazard List) Pre-Conceptual Hazards Detailed Hazard Analysis

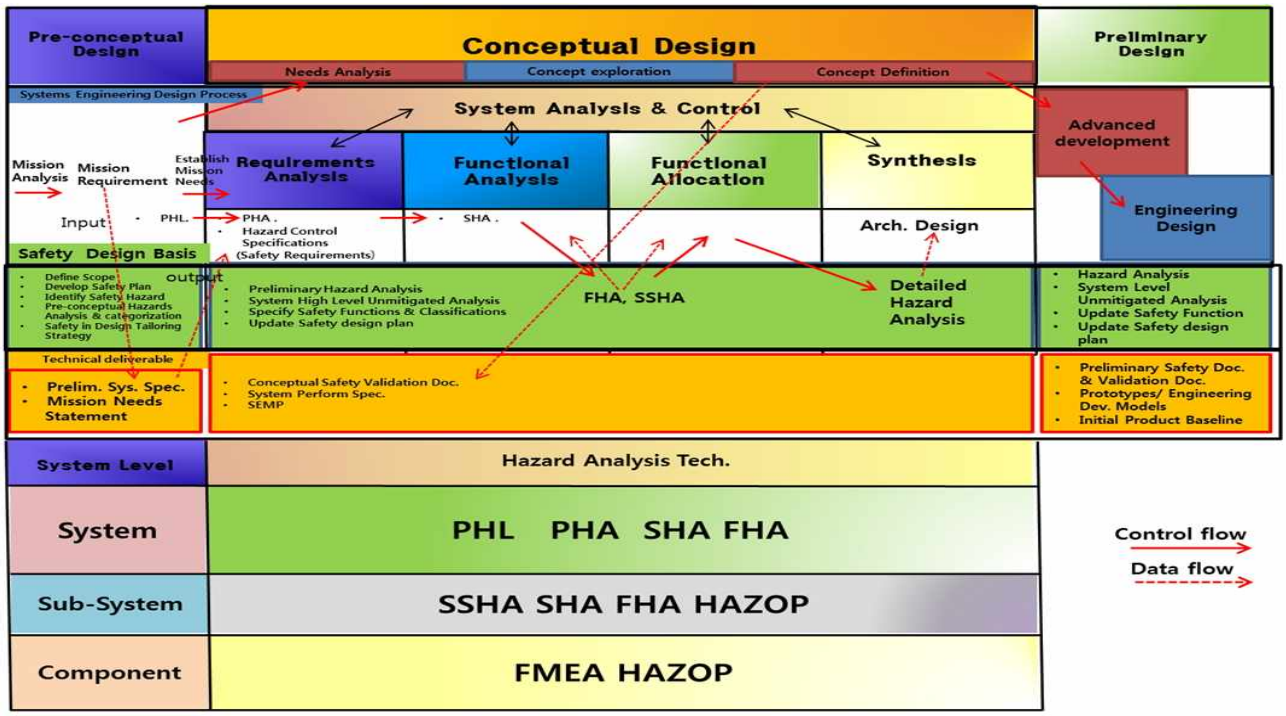
4. 통합 설계 환경의 구축

4.1 안전관점에서 재분석된 DoDAF와 통합 설계 프로세스 모델의 상호 연동성 분석

설계 프로세스와 안전 프로세스 수행에 따른 공통점은 프로세스 수행에 따른 입·출력물이 존재한다는 것이다. 특히, 설계 프로세스 수행에 따른 결과와 안전 활동에 따른 수행 결과를 독립적으로 바라본다면 오늘날과 같은 대형복합 시스템 개발 추세에 효과적인 대응을 하지 못할 것이다. 따라서, 본 연구 수행을 통해서 대형복합시스템 설계로부터 발생가능한 안전성 문제를 해결하기 위해서 상호운용 기반의 설계 및 운용활동을 지원하는 DoDAF의 산출물을 안전관점에서 분석하였다. 따라서 <Figure 6>에서 제시하는 안전관리 항목을 도출하였다. 도출된 안전관리 항목은 설계활동과 안전활동과의 연동성 측면에서 중요한 역할을 한다. 하지만, 안전관리 항목만으로 설계 프로세스와의 상호 연동성을 찾기 어렵기 때문에, <Figure 8>에서 제시되는 기존에 제시한 설계활동과 안전 활동의 통합 설계 프로세스 모델을 활용하여 <Figure 9>과 같이 보다 개선된 상호운용 안전성 기반의 통합 설계 프로세스 모델을 구축 할 수 있었다.

관점		안전관리 항목															
		프로젝트	운용	제약	조직	시스템	인터페이스	기능	시간	능력	데이터	요구사항	활동	자원	정보	이벤트	서비스
All Viewpoint (AV)	AV-1	O	O	O													
	AV-2	O	O		O						O						
Systems Viewpoint (SV)	SV-1					O	O										
	SV-2					O								O			
	SV-3					O											
	SV-4					O		O			O						
	SV-5					O		O					O				
	SV-6					O								O			
	SV-7					O		O					O				
Service Viewpoint (SvcV)	SvcV-1				O									O			O
	SvcV-2				O									O			O
	SvcV-3a					O											O
	SvcV-3b					O											O
	SvcV-4							O			O						O
Operational Viewpoint (OV)	OV-1		O														
	OV-2		O										O		O		
	OV-3		O		O									O	O		
	OV-4		O		O												
	OV-5a		O							O			O				
	OV-5b		O							O			O				
	OV-6a		O	O									O				
	OV-6b		O	O													
	OV-6c		O													O	
Standards Viewpoint(StdV)	StdV-1			O													
	StdV-2			O													
Project Viewpoint (PV)	PV-1	O			O												O
	PV-2	O	O						O								
	PV-3	O								O		O					
Data & Information Viewpoint (DIV)	DIV-1										O	O			O		
	DIV-2			O							O	O	O		O		
	DIV-3										O						
Capability Viewpoint (CV)	CV-1	O	O	O									O				
	CV-2	O								O	O	O					
	CV-3			O						O			O				
	CV-4									O							
	CV-5									O		O					
	CV-6	O								O			O				
	CV-7	O															O

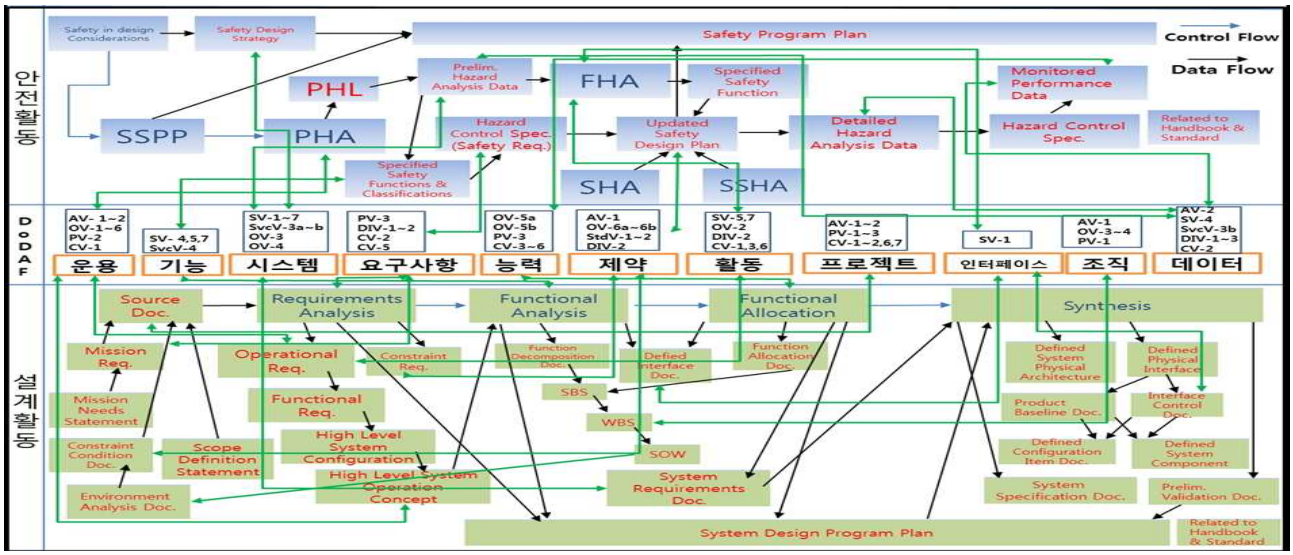
<Figure 7> An interlinkage/interoperability matrix generated from the individual views of DoDAF and the items of safety management



<Figure 8> The integrated process model quoted from the previous study [6]

4.2 구축된 상호운용 안전성 기반 통합 설계 프로세스 모델

<Figure 9>를 통해 제시한 것처럼 통합 설계프로세스에 안전관점에서 재분석된 DoDAF를 반영하기 위해서 시스템공학 설계 프로세스와 시스템 안전 프로세스에 대해 동일한 수명주기 기준을 가지고 개별 프로세스 분석을 통해, 활동에 따른 산출물을 분석·정리하였다. 상호 운용성 기반 안전성을 확보를 위해, DoDAF 수행에 따른 산출물을 안전관점에서 분석하여 안전관리 항목을 도출하였다. <Figure 6>에서 제시되는 안전관리 항목을 활용적 측면에서 예를 들어 설명하자면, 오늘날 시스템을 개발하는데 있어서 대상인 시스템에 대해서만 안전관리가 중요한 것이 아니라, 최상위 수준인, 개발이 진행되는 '프로젝트'라는 관리적 측면에서도 안전과 관련하여 수반되어 관리되어져야 할 요소들이 많다. 따라서, 제시된 안전관리 항목을 통해서 관련되어진 DoDAF 개별 뷰(View)의 수행을 통해 생성되는 산출물을 활용한다면, 서두에 우려한 대형복합 시스템의 상호 운용성 기반으로부터 발생 가능한 안전문제를 해결할 수 있을 것이다.

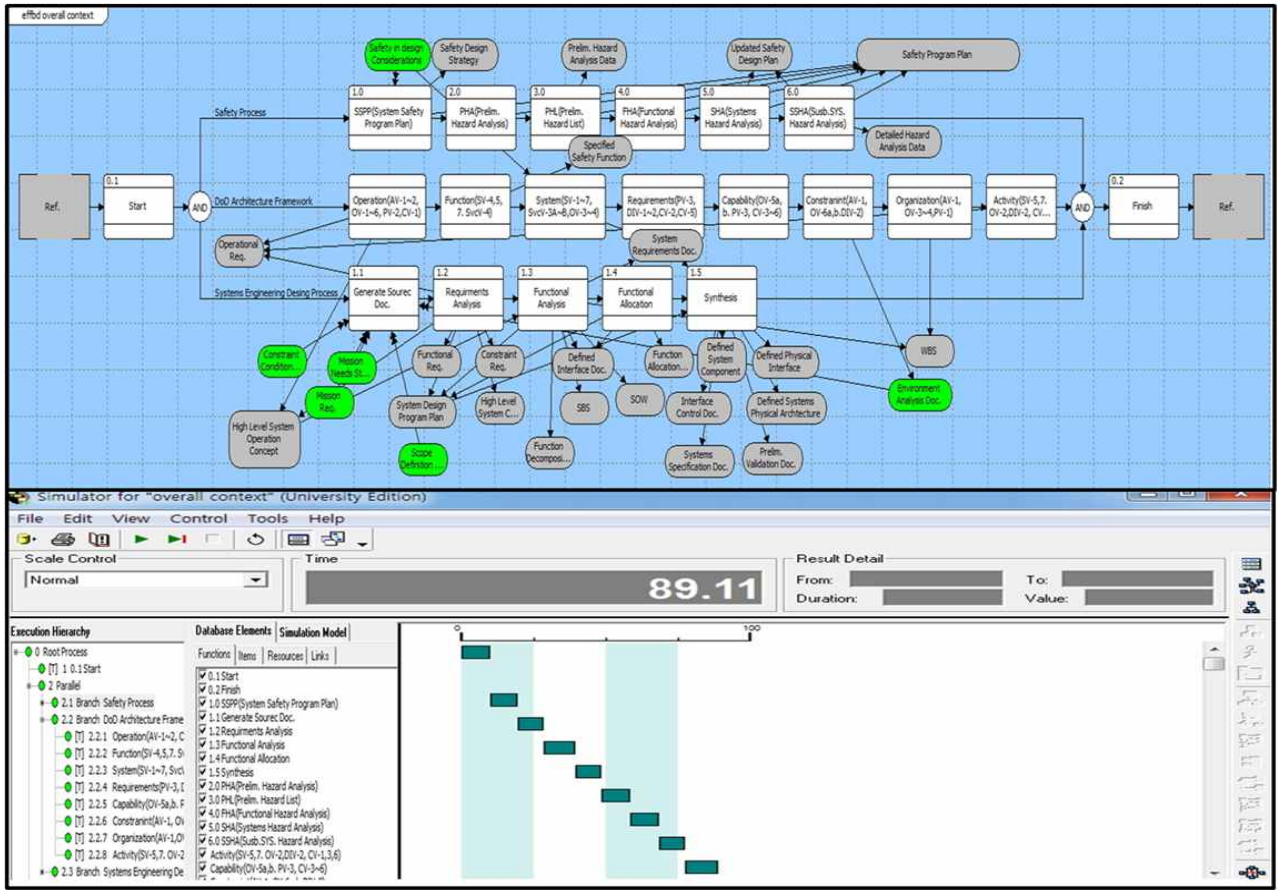


<Figure 9> An improved and integrated process model exploiting the design and safety processes under interoperability environment

5. 구축된 상호운용 안전성 기반의 통합 설계 프로세스 모델의 검증

5.1 시뮬레이션 대상 및 범위

본 연구를 통한, 연구결과의 적용대상은 서두에 언급한대로 대형복합 시스템이 되겠다. 이러한, 대형복합 시스템에는 철도, 국방, 우주항공 등 다양한 산업분야에서의 시스템이 해당되겠다. 또한, 본 연구를 통해 국내에서는 아직 활발히 연구되지 않은 동시공학적인 측면에서 시스템설계와 시스템 안전을 동시에 수행하기 위한 시스템 상위 수준에서 연구를 제한하고 있기에 아직 특정 시스템에 적용을 통한, 본 연구결과에 대한 검증 수행은 이르다고 본다. 하지만, 본 연구를 통해 구축된 상호운용성 기반의 통합설계프로세 모델에 대한 검증을 수행하기 위해서 시스템공학 전산지원 도구를 통해서 개선된 통합 설계 프로세스에 대해 시뮬레이션을 수행하였다. 이를 통해 프로세스의 흐름과 활동에 따른 입·출력물이 원활이 진행되는지에 대한 검증하기 위해서 시뮬레이션이 가능한 EFFBD(Enhanced Functional Flow Diagram)이라는 모델링 기법을 활용하여 시간선 분석(Time-Line Analysis)을 통해 수행하였다. 따라서, 수행 결과를 통해 잘못된 프로세스 수행 시기와 흐름에 관한 논리적 오류를 확인하고 수정하여, 개선된 통합 설계 프로세스에 대해 전체적 흐름이 올바르게 수행되고 있는지에 대한 확인을 수행할 수 있었다. 시뮬레이션 범위 또한, 본 연구범위와 일치하는 개념설계 단계로 한정하였으며, 개념설계 단계에서 통합 구축된 시스템공학 설계 프로세스와 시스템 안전 프로세스 그리고 DoDAF의 수행에 있어서 산출되는 데이터를 모두 고려하였다.



<Figure 10> Verification of the resultant integrated process model by computer simulation

5.2 시뮬레이션 결과 및 해석

<Figure 10>을 통해서 제시되듯이, 개념설계 단계에서 통합된 3가지 프로세스의 서브-프로세스 총 19개와 각각의 개별 프로세스의 입·출력 요소에 대해 시뮬레이션에 반영하여 수행하였다. <Figure 10>의 그림 오른쪽 하단을 통해서 같은 녹색으로 구성된 바 형태의 막대기가 89.11이라는 시간선 분석 지표를 나타내는 것을 알 수 있다. <Figure 10>의 왼쪽 하단의 그림을 통해서 가지마다의 흐름에서 녹색표시를 볼 수 있다. 이는 프로세스의 구성에 오류가 없고 프로세스 흐름이 원활히 진행하고 있다는 것을 나타낸다. 따라서 본 연구를 통해 개선된 통합 프로세스 모델이 시뮬레이션 시간선 분석에 따라 가장 작은 값을 나타낸 89.11에서 개선된 통합 프로세스 모델에 대한 최적화를 마쳤다.

6. 결론 및 요약

오늘날 개발되는 시스템의 추세가 대형화, 복합 화, 고도화 되다 보니, 기존의 단일 시스템 중심의 안전관리 프로세스로는 대형 복합 시스템의 안전성 확보에 큰 어려움이 발생하게 되었다. 따라서, 본 논문에서는 대형복합 시스템의 상호 운용성 기반의 설계 및 운용을 지원하는 DoDAF를 안전성 측면에서 재분석하였다. DoDAF의 개별 뷰 수행에 따른 산출물의 특성을 분석하여 관련 안전관리 항목을 도출하여 제시하였다. 도출된 안전관리항목은 대형복합 안전중시 시스템 개발 사업에 있어 활용 가능한 시스템공학 설계프로세스와 시스템안전 프로세스 수행에 따른 산출물과의 연동성을 분석하여 최종적으로, 상호운용 기반 안전성이 개선된 통합 프로세스 모델을 제시하였다. 따라서, 제안된 안전관리 항목을 바탕으로 관련 요소에 대한 상호운용 기반 안전성확보를 위한 발판을 마련하였다. 이번에 제안한 상호 운용성 기반 안전성 확보를 위해 개선된 통합 설계 프로세스 모델을 상위 수준의 설계 단계 및 운용단계에서 활용한다면 대형복합 시스템의 안전성 확보에 기여할 수 있다고 본다. 후속 연구 활동 또한 활발히 진행되었으면 한다. 추후 연구에서는 연구범위를 확장시켜 안전중시 시스템 설계에서 보다 개선된 대형복합 시스템 안전 확보를 위한 모델을 제시하는 연구가 필요할 것이다.

7. 참 고 문 헌

[1] S. I. Kim, W. J. Jang, C. W. Joo, K. W. Lee, and H. C. Kim, "Technical trend of electrical IC for defense," Electronics and Telecommunications Trends, vol. 24, no. 6, pp. 77-85, 2009.

[2] M. Sadraey, "A Systems Engineering Approach to Unmanned Aerial Vehicle Design, " in Proc. 2010 ATIO, Texas, United States, pp.3-15,(2010)

[3] Y. M. Kim and J. C. Lee, "On the Integration of Systems Design and Systems Safety Process from an Integrated Data Model Viewpoint," Korea Safety Management & Science, vol. 14, pp. 107-116, (2012)

[4] A. E. Clifton, "Hazard analysis techniques for system safety.", Hoboken, New Jersey: John Wiley & Sons, Inc., (2005)

[5] J. H. Yoon, J. C. Lee and S. H. Hong, "A Study on Integrated SE Process for the Development of the Railway Systems with Safety Assessment Included," Korean Society for Rail, vol. 10, pp. 438-443, (2007)

[6] Y. M. Kim and J. C. Lee, "A Study on the Integration of Systems Engineering Process and Systems Safety Process in the Conceptual Design Stage to Improve Systems Safety," Korea Safety Management & Science, vol. 14, pp. 1-10, (2012)

[7] A. Kossiakoff and W. N. Sweet, Systems Engineering Principles and Practice. New Jersey: Wiley, 2003, pp. 117-138.

[8] DoD, "Operation of the Defense Acquisition System," Department of Defense, INSTRUCTION, 5000.02, pp. 1-80, (2008)

[9] Systems Engineering - System life cycle process, in ISO/IEC 15288:2002(E): International Organization for Standardization, (2002)

저 자 소 개

김 영 민

현 아주대학교 시스템공학과 석·박사통합과정. 관심분야는 시스템 안전설계, 요구사항 관리, 모델기반 시스템공학, Modeling & Simulation 등.

주소: 경기도 수원시 영통구 원천동 산5번지 아주대학교 성호관 243호

이 재 천

현 아주대학교 시스템공학과 정교수. 서울대학교 전자공학과에서 공학사, KAIST 전기 및 전자공학과에서 공학석사 및 박사학위를 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: 경기도 수원시 영통구 원천동 산5번지 아주대학교 서관 309호