JANT 한국항행학회논문지
Journal of Advanced Navigation Technology

항공 우주 해상

J. Adv. Navig. Technol. 21(2): 155-162, Apr. 2017

항공 안전 필수 시스템에 대한 독립적 검증 및 확인의 효과도 분석

The Effectiveness of Independent Verification and Validation of Safety-critical Aviation Systems

김 영 훈 · 유 병 선 · 강 자 영*
한국항공대학교 항공체계시험인증연구센터

Young-Hoon Kim · Beong-Seon Yoo · Ja-Young Kang*
Korea Aerospace University, 76, Hanggongdaehak-ro, Gyeonggi-do, 10540, Korea

[요 약]

최근 국내에서 항공 관련 안전필수시스템들이 개발되었지만 이들 완성품들은 규정된 요구사항들을 충족시키지 못하여 실용화 또는 상용화 되지 못하였다. 현대 항공 기술의 복잡도가 높아짐에 따라 기존의 검증 및 확인 기술로는 시스템에 잠재된 리스크를 식별하고 줄이는데 어려움이 많다. 이러한 단점들을 극복하기 위해 선진국에서는 독립적 검증 및 확인이라는 새로운 기법에 관심이 모아지고 있다. 이 독립적 검증 및 확인의 효과도에 관한 학술적 연구는 국내에는 전무하고, 국외에서 조차도 매우 희소하게 수행되고 있다. 따라서 본 논문에서는 항공선진기관에서 수행한 항공 안전필수시스템에 대한 독립적 검증 및 확인의 응용 연구들을 조사하여 사업에 미치는 여러 가지 효과들을 분석해 본 결과, IV&V는 조기 오류 검출율을 높이고, 내재된 리스크도 조기에 완화하며, 개발 수명주기 후반에 나타나는 재작업 확률을 줄여서 개발 일정 및 비용의 증가를 획기적으로 막아주는 것으로 나타났다.

[Abstract]

In recent years, aviation-related safety-critical systems have been developed in Korea, but these products have not satisfied the specified requirements and thus have not been commercialized or commercialized. Due to increasing complexity of the modern aviation system, traditional verification and validation techniques are not sufficient to identify and reduce latent risks in the system. To overcome this shortcoming, a new method which is called 'Independent verification and validation (IV&V)' is suggested. However, academic researches on the effectiveness of this independent verification and validation have not been conducted domestically, and it is performed very rarely even overseas. Therefore, in this paper, we investigated the application of independent verification and validation of the safety-critical aviation systems performed by advanced aviation organizations, and analyzed various positive effects on projects. As a result of the analysis, IV&V shows that early error detection rate is increased, potential risk is mitigated early, and the complex reworking probability, which appears later in the development life cycle, is reduced, greatly preventing the development schedule and costs from increasing.

Key word : Systems engineering, Independent verification and validation, System life-cycle, Safety-critical system.

https://doi.org/10.12673/jant.2017.21.2.155

Received 31 March 2017; **Revised** 4 April 2017
Accepted (Publication) 24 April 2017 (30 April 2017)

***Corresponding Author ; Ja-Young Kang**

Tel: +82-2-300-0081
E-mail: jaykang@kau.ac.kr

I. 서 론

최근 국내 안전필수시스템 (SCS; safety-critical system) 연구개발 사업을 통하여 개발된 시스템이 실용화 또는 상용화가 되지 못하는 사례가 발생하고 있다. 이러한 사례들은 명료하지 않은 요구사항 적용으로 인한 설계 오류, 불충분한 개발시험 또는 운용시험, 미흡한 사업 타당성 분석, 객관적이지 못한 검증 및 확인 (V&V; verification and validation) 등 여러 가지 요인에 기인하고 있다.

항공기의 제어감시시스템, 원자력 발전시설, 화학 및 의약품 공장의 제어시스템, 자동제어시스템 및 정보통신망 등 현대산업에서 손쉽게 접할 수 있는 시스템인 SCS는 고장 시 인명에 손상을 주거나 환경에 큰 영향을 주기 때문에 매우 높은 수준의 시스템적 관리가 필요하다[1]. 특히 항행안전시설, 인공위성, 항법유도장치 등과 같이 국가가 법·규정을 통하여 최소한의 안전을 보장하고 있는 SCS의 경우 시스템 개발 초기단계부터 전 수명주기를 통한 V&V활동이 매우 중요하다.

표 1은 Standish 그룹이 2015년 개발된 5만여개의 소프트웨어 개발 사업을 조사하여 발표한 자료이다. 계획된 예산 및 사업 일정 내에 성공적으로 마친 사업은 29 %, 계획된 비용 및 일정을 초과하여 완료된 사업은 52 %, 개발 도중 종료된 사업은 19 %이다. 이와 같이 계획된 사업비용 및 일정 내에서 사업을 성공적으로 완료하는 경우는 많지 않으며 개발 전 수명주기적인 관리를 통하여 개발 초기단계에서 결함을 미리 찾아 제거하는 전략이 필요하다[2].

항공관련 사업의 경우 규모가 커지고 복잡도 또한 증가하고 있기 때문에 종래의 V&V 방식으로는 전수명주기적 V&V를 수행하는데 어려움이 많다. 이를 위해 선진국에서는 V&V의 독립성을 강조하는 새로운 V&V기법이 SCS 개발에 도입되고 있다. IEEE, INCOSE, DoD, NASA 등에서는 표준규격을 제정하여 다양한 시스템 개발에 독립 검증 및 확인 (IV&V; independent verification and validation)을 적용하여 성공적인 사업관리를 하고 있다.

현재 국내에서는 IV&V에 대한 정확한 개념이 정의되어 있지 않고, 또한 기 수행된 대부분의 SCS 개발 사업에서 형성된 관련 자료가 가용하지 않다. 따라서, 본 논문은 항공 선진기관에서 수행한 여러 가지 사업 중 V&V와 IV&V를 적용한 사례를 통하여 V&V의 독립성이 SCS 개발에 어떠한 긍정적인 효과를 나타냈는지를 조사 분석해 보았다.

표 1. S/W 개발 사업 성공률
Table 1. S/W development project success rate, reproduced from [2].

	2011	2012	2013	2014	2015
Successful	29 %	27 %	31 %	28 %	29 %
Challenged	49 %	56 %	50 %	55 %	52 %
Failed	22 %	17 %	19 %	17 %	19 %

II. 검증 및 확인의 독립성

2-1 검증 및 확인

V&V는 SE 요소 중 하나로서 요구사항들이 시스템 수명주기에 걸쳐 올바르게 구현되었는지를 검증하고 그 유효성을 확인하는 프로세스이다. 시스템 또는 각 제품에 대한 V&V의 적용방법은 사업의 특성 및 규모에 따라 다를 수 있으므로 테일러링이 가능하다. 이에 대한 결정은 시스템의 중요도, 제약사항, 복잡도에 의해서 많은 영향을 받는다. 일반적으로 V&V의 목적은 제품이 사용자나 시스템의 요구사항을 만족시키는 지를 보장하기 위한 것이다. 따라서 시스템 요구사항 및 규격에 있는 모든 사항들이 V&V의 대상이 된다.

검증은 선택된 작업 결과물들이 그들의 명시된 요구사항을 만족시킨다는 확증이다. 이는 모든 적용 요구사항에 대한 최종 결과물(시스템, 서비스 또는 운용상의 변경) 및 중간 결과물들의 검증을 포함한다. 검증은 작업 결과물들의 개발 수명주기를 통하여 발생되기 때문에 본질적으로 점진적 프로세스이다. 즉 개발 수명주기는 운용개념 및 초기 요구사항들로 시작되고, 그 다음에는 변경을 통해 진전되며, 최종 결과물의 검증으로 완결된다[3].

유효성 확인은 최종 결과물 또는 최종 결과물의 구성품이 그 예정된 운용환경에 놓였을 때 소기의 목적을 충족시킬 것이라는 보증이다. 확인을 완료하기 위해 도입된 방법들은 선택된 작업 결과물들뿐만 아니라 최종 결과물 및 그 결과물의 구성품들에도 적용된다. 작업 결과물들은 최종결과물 또는 그 최종 결과물의 구성품이 예상된 목적 및 사용자의 필요를 얼마나 잘 만족시키는가에 대한 최고의 예언자라는 것에 근거하여 선택되어야 한다. 확인은 운용, 훈련, 제작, 정비 또는 지원 서비스들과 같은 어떠한 예정된 환경에 있는 모든 측면의 최종 결과물에 적용될 수 있다.

그림 1에 주어진 V모델은 검증 및 확인 활동이 운용개념 및 사용자 요구사항 정의 단계로부터 시스템 유효성 확인단계까지 시스템 또는 서비스 획득을 통하여 수행되는 개념을 보여주고 있다[4]. 검증 및 확인은 획득에 참여하고 있는 여러 실체에 의해서 계속되는 기반 위에서 다양한 수준으로 수행된다. 예를 들어 시스템 엔지니어링 조직은 요구사항의 검증 및 확인에서 중요한 역할을 하는데 반해 시험평가 조직은 시스템 또는 서비스의 통합 및 시험에 대한 검증 및 확인에서 등가의 역할을 한다.

검증 및 확인의 맥락에서 시험평가 전문가들은 획득 프로세스에서 아주 중요한 역할을 한다. 그림에 나타낸 바와 같이 다이어그램 바깥쪽에 있는 화살표들은 시험평가 단계들을 묘사하고 있다.

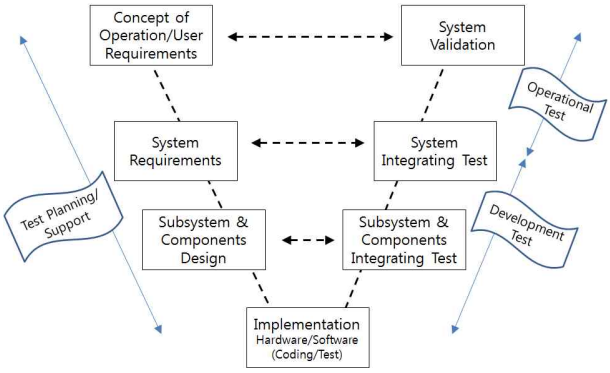

그림 1. 시스템 개발 V 모델
Fig. 1. System development "V model".

V 모델 좌측에 있는 화살표는 시험평가 계획 및 지원 단계를 나타낸다. 이 단계 동안 시험평가의 주요 검증 및 확인 역할은 개념, 요구사항 및 설계의 개발을 지원하는 것이다. V 모델 우측에 있는 화살표는 개발시험 (development test) 및 운용시험 (operational test)을 나타낸다. 이 두 단계 동안의 주된 V&V 역할은 시험평가를 수행하는 것이다.

V 모델 중간에 있는 쇄선 화살표는 V모델 양측의 대응 관계를 나타내기 위한 것이다. 예를 들어, 운용개념 및 사용자 요구사항은 운용시험을 위한 시험 케이스를 구동하고, 운용시험의 개발 및 실행은 향후 사용자 요구사항 정의를 위한 피드백을 제공한다.

2-2 독립적인 검증 및 확인의 중요성

IV&V는 개발자에 의한 시스템 개발 활동의 결과물이 고객의 요구사항을 충족시키고 인도품이 의도된 사용 및 사용자 필요를 만족시키고 있는지를 보증하기 위해 개발그룹과 무관한 독립적인 그룹이 수행하는 프로세스이다. 다양한 기관 및 단체에서 IV&V를 정의하고 있지만 IEEE Standard 1012-2012 System and Software Verification and Validation에서는 "IV&V를 수행하는 그룹은 개발 그룹으로부터 분리된 그룹이어야 한다."라고 정의하고 있으며, 사업을 성공적으로 이끌기 위한 IV&V 활동으로 다음과 같이 기술적, 직제관리상 및 재정적 독립성을 강조하고 있다[5].

기술적 독립성 : 개발 그룹과는 무관한 그룹으로 조직되어야 하며, 개발 그룹과는 다른 관점에서 시험 및 분석을 수행하기 위해서는 기술, 시험방법 등을 개발그룹이나 관리그룹의 영향을 받지 않고 자유롭게 선택할 수 있어야 한다.

직제상의 독립성 : 시스템의 시험 및 분석 결과, 이상 상태, 결과물 등을 외부(개발부서, 사업책임 부서 등)의 압력 없이 최고 경영자에게 직접적으로 보고할 수 있는 체계를 말한다.

재정적 독립성 : IV&V 그룹이 시험 및 분석 방법을 자유롭게 선택하는데 있어 개발 그룹이나 관리 그룹으로부터 잠재적인 재정 압박을 받는 것으로부터 자유로운 것을 말한다.

따라서 IV&V는 기술적, 직제 관리상, 재정적으로 이해 당사자 그룹과는 별개로 운영되어 전 수명주기에 걸쳐 요구사항이 올바르게 충족되었는가를 입증하고 확인하는 일련의 활동으로 구성되며 다음과 같은 장점을 가지고 있다[6].

- IV&V를 적용하면 사업적 리스크로 발전될 수 있는 중대한 결함을 개발 수명주기 초기에 발견할 가능성이 높다.
- IV&V는 현재 진행 중인 시스템의 상태 및 성능을 사업 책임자에게 직접 보고한다.
- IV&V는 시스템 개발 활동의 품질 및 진척사항을 이해관계자들에게 투명하게 제공한다.
- IV&V는 개발자의 재작업 필요성을 줄이고 개발 사업의 총 비용을 감소시킨다.
- IV&V는 최종 인도품의 결함을 줄인다.

사업 규모, 기간 및 인원 등 시스템 개발 부서의 내부 사정으로 인하여 기술적, 직제관리상, 재정적 독립성의 3가지의 요소를 모두 충족할 수 없는 경우가 발생하는 경우가 있기 때문에 IEEE에서는 IV&V의 형태를 다음과 같이 분류하고 있다[5].

Classical IV&V : IEEE Standard 1012-2012가 정의하고 있는 IV&V의 기본적 독립성에 기초한 형태이다.

Modified IV&V : 시스템 개발을 통합하는 주계약자가 IV&V를 포함한 전체 시스템 개발에 책임을 지는 비교적 큰 규모의 사업에 사용된다. 주계약자는 시스템 개발을 돕고 IV&V를 수행할 기관을 선정한다. 따라서 고객 또는 최종 산출물의 운영자는 주계약자에게 이 책임을 일임함으로써 획득 시간을 줄일 수 있다. 주계약자는 개발의 전체 또는 부분을 수행하면서 IV&V 결과를 보고받기 때문에, 직제 관리상의 독립성은 절충이 된다. IV&V 활동은 시스템 개발 솔루션에 대해 편견 없는 의견을 표출하고 IV&V를 수행할 독립적인 인적 자원을 활용하기 때문에 기술적인 독립성은 유지된다. 분리된 예산이 IV&V 노력을 위해 따로 확보되어 있기 때문에 재정적 독립성도 유지된다.

Integrated IV&V : 개발 프로세스에서 고객에게 V&V 결과를 신속하게 제공하는데 초점을 두고 있는 형태로 IV&V 그룹은 개발 그룹과 상호의존적으로 V&V 활동을 수행하여 그 결과를 고객에게 신속히 제공할 수 있다는 장점이 있다. V&V 결과의 빠른 피드백을 위해 개발 그룹과 협동 방식으로 함께 V&V를 수행하지만 개발 그룹과는 재정적, 직제관리상 독립성은 유지하고 있는 형태이다. Integrated IV&V는 IV&V 그룹과 개발 그룹간에 기술적 IV&V 활동이 상호의존적으로 기술적 독립성에 대해서는 절충된 형태이지만 직제관리, 재정적 독립성은 보장받고 있는 형태이다

Internal IV&V : 개발과 직접적으로 관련이 없는 시스템 개발 그룹 내부 전문가를 활용하여 V&V 업무를 수행한다. 개발 과정에 직접 영향을 주는 엔지니어는 아니지만 개발 그룹 내 인원이 V&V를 수행하기 때문에 기술적, 직제 관리상, 재정적 독립

성은 모두 절충된 상태이다.

Embedded IV&V : Internal IV&V와 유사하지만 이 경우에는 개발 인력이 V&V 활동을 수행하기 때문에 실질적으로 독립적인 검증 기능을 유지하기가 어려운 환경이다. 하지만 IV&V 그룹을 별도로 운영하는데 드는 비용과 인력 소모가 많기 때문에 소규모의 사업을 시행하는 사업체에서 선호한다.

하지만, 사업 규모, 투입 인력, 장비, 소스 (시스템 개발에 필요한 자재) 등 시스템 개발 예산 측면에 있어 추가적인 IV&V 그룹을 운영하기 어렵다면, 사업 관리자는 표 2에서 명시한대로 IV&V 중요 파라미터와 부분적 절충을 하는 다른 형태의 IV&V 그룹을 구성해야 한다[7]. 결과적으로 IV&V 그룹은 시스템 개발 수명주기 동안에 개발 계획, 품질 평가 방법, 요구사항 및 표준에 대한 의견을 사업 관리자에게 피드백하여 최종 산출물의 품질을 보장할 수 있도록 구성되는 것이 필요하다.

표 2. 다양한 형태의 IV&V
Table 2. Forms of IV&V, reproduced from [5].

	Technical	Management	Financial
Classical IV&V	A	A	A
Modified IV&V	A	B	A
Integrated IV&V	B	A	A
Internal IV&V	B	B	B
Embedded IV&V	C	C	C

A = rigorous independence;
B = conditional independence;
C = minimal independence

III. IV&V 효과도 분석

수명주기란 시스템의 개발 및 운용과 관련된 다양한 제약사항(constraints)과 상호관계를 객관적으로 평가할 수 있도록 해당 개발단계부터 배치 운용단계에 이르기까지의 모든 활동기간을 포함하고 있다[4]. 부연하면, 시스템 개발의 목표 및 타당성 분석, 시스템 개념 및 요구사항 정립, 설계, 제작, 시험 및 평가, 설치, 운용, 유지관리, 배치 이후의 지속 서비스 (in-service) 및 최종 폐기(disposal)까지의 제반 단계를 말한다. 본 연구에서는 수명주기 상에서 오류 유입 및 검출이 가장 많은 단계인 시스템 요구사항 정립 단계부터 시험 및 평가 단계까지 시스템 개발을 주목적으로 수명주기 범위를 설정하였으며[8], 다음과 같이 국내외에서 수행한 IV&V 관련 연구를 조사하여 IV&V의 효과도를 관찰하였다. 불행하게도 국내에는 이 분야에 대한 연구가 전무하였고, IV&V의 효과도를 분석할 수 있는 기본 데이터의 축적이나 공개가 불가능하여 국외의 연구사례에만 의존할 수밖에 없었다.

3-1 오류검출에 대한 IV&V 효과 분석

Virginia Tech과 NASA LaRC(Langley Research Center)는 미육군 유도탄 사령부(AMCOM; US army missile command)가 개발한 소프트웨어 엔지니어링 평가 시스템(SEES; software engineering evaluation system)을 이용하여 IV&V의 가치를 시험하였다[9]. 연구는 2개의 독립된 그룹에 특정문제에 대한 솔루션을 개발하기 위한 동일한 요구사항을 주고, 설계, 코딩, 시험을 독자적으로 수행하도록 하였다. 그룹 1은 개발팀과 독립된 IV&V팀으로 구성하였고, 그룹2는 개발팀으로만 구성함으로써 IV&V기능이 시스템 오류 탐지에 어떠한 영향을 주는가를 조사하였다. 그림 2에서 막대그래프는 그룹1과 그룹2가 각 수명주기 단계에서 검출한 중요한 오류의 수를 보여주고 있다.

그룹 1과 그룹 2에 의해 발견된 중요 오류 수를 비교해보면, 그룹 1이 발견한 오류의 수가 요구사항 단계부터 낮은 수준의 설계(LLD; low level design) 단계까지 점차 증가하고 있는 것을 알 수 있다. 또한, LLD 단계에서 가장 많은 수의 오류가 발견되었으며 다음 두 단계에서는 점차 줄어들고 있음을 알 수 있다. 이는 시스템 개발 수명주기 각 단계에서 고객, 개발팀, IV&V팀 등 이해관계자들로부터 도출된 요구사항이 IV&V 활동을 통하여 올바르게 충족되는 과정으로 수명주기 초기에 발견된 오류를 바로 잡아 구현 및 유닛 시험 단계, 통합 및 시험 단계에서 발견되는 오류의 수가 줄어든 것으로 보인다. 그룹 2의 경우에는 수명주기 초기 단계에서 오류를 거의 발견하지 못하고 수명주기 나중 단계에서 많은 수의 오류가 발견되는 것을 알 수 있다.

또 다른 사례로 그림 3과 같이 NASA에서 개발한 우주왕복선 사업의 CSCI (computer software configuration item)에 IV&V를 적용하여 어떠한 효과가 있는지를 분석해 보았다[10]. 가로축의 DTS (distributed teleconferencing system), DIVDT (the day of launch I-load verification table), SVDS (the space vehicle dynamic simulation) 등은 CSCI로 고객이 요구하는 최종사용기능을 만족하고, 획득기관(고객 또는 운용기관)이 형상관리를 하기 위한 소프트웨어 집합체로 기능, 크기, 지원 개념, 재사용

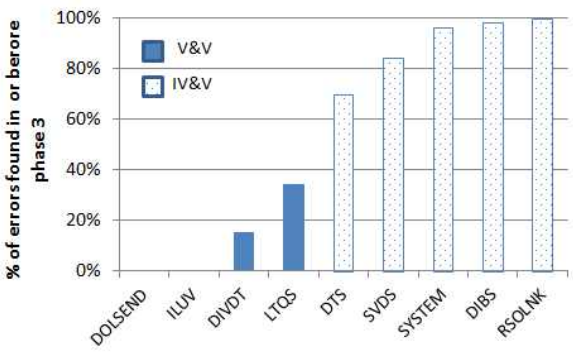

그림 3. 상세설계 또는 이전 단계에서의 오류 발견 확률
Fig. 2. Probability of errors found in or before detailed design, reproduced from [10].

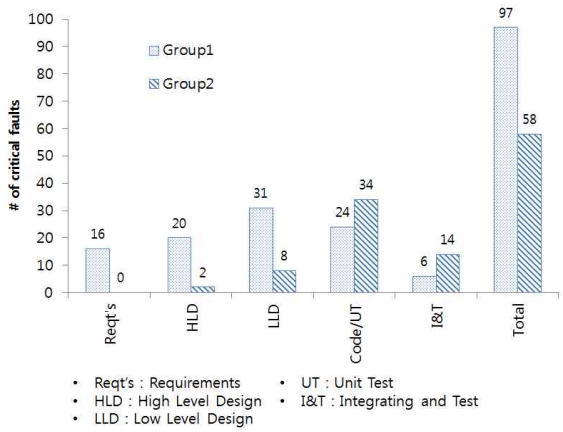

그림 2. V&V 그룹과 IV&V 그룹간의 주요 오류탐지 비교
Fig. 3. Comparison of groups' error detection, reproduced from [9].

계획, 중요도, 상호 운용성, 별도 통제 및 문서화 필요성 등의 요소를 고려하고 절충하여 선정한 컴퓨터 소프트웨어로 우주왕복선 개발에 매우 중요한 형상품목들이다[11].

이 사업에서는 우주왕복선 CSCI에 IV&V를 적용했을 때 소프트웨어 개발 수명주기상의 코딩단계 이전, 즉 상세설계 단계까지 오류를 얼마만큼 발견하게 되는가에 초점이 맞춰져 있다.

이 사업의 수명주기는 요구사항, 예비설계, 상세설계, 코딩 및 유닛 시험, 통합 및 시스템 시험, 운용 및 유지관리 등 6단계로 구분하였다. 9개의 CSCI 요소 중 IV&V 수행 여부에 따라서 요구사항, 예비설계, 상세설계에 이르는 수명주기 초기 단계에서 오류 발견 비율을 그림 3과 같이 나타내 보았다.

수평축에는 9개의 CSCI가 나열되어 있는데 처음 4개의 CSCI에는 IV&V가 적용되지 않았고 나머지 5개에는 IV&V가 적용되었다. 수직축은 각 CSCI의 전체 오류 대비 발견된 오류의 비율을 나타내고 있다. 그림에서 알 수 있듯이 IV&V를 적용한 CSCI의 경우 수명주기 초기, 즉 요구사항, 예비설계, 상세설계에서 발견된 오류가 전 수명주기에서 발견된 오류의 대부분을 차지하고 있으며, IV&V를 미적용한 CSCI의 경우 수명주기 초기에 오류 발견 비율은 매우 낮다.

그림 3의 수직축 값을 수평축으로 놓고 표를 변형해보면 그림 4와 같이 양분화 되는 것을 알 수 있다. 전 수명주기에서 발견된 오류 중 상세설계 단계까지 오류 발견 비율이 0~20%사이에 있는 CSCI수는 3개, 21~40 %사이에 있는 CSCI수는 1개, 61~80 %사이에 있는 CSCI수는 1개, 81~100 %구간에 있는 CSCI수는 4개로 전 수명주기를 통해 IV&V를 수행하였을 때 수명주기 초기에 나타나는 오류의 비율이 앞선 AMCOM사례와 유사한 양상을 보이고 있음을 알 수 있다.

이는 개발 그룹이 만든 산출물을 개발 그룹 스스로가 V&V를 수행함으로써 IV&V가 내포하고 있는 독립적이고 객관적인 관점에서 피드백을 갖지 못하여 수명주기 초기에 오류를 발견하지 못하고 수명주기 나중 단계에서 많이 발견되는 이유로 판단된다.

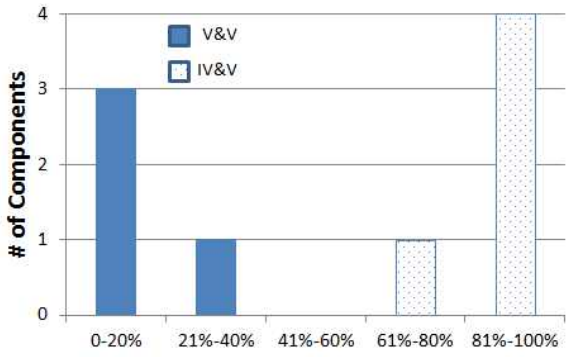

그림 4. 상세설계 또는 이전 단계에서 오류 발견 비율
Fig. 4. Probability errors found in detailed design or earlier, reproduced from [10].

3-2 비용절감에 대한 IV&V 효과 분석

NASA에서는 2007년 초부터 종래의 V&V에 independent 개념을 추가한 새로운 접근방법에 초점을 맞추기 시작하였고 그동안에 NASA에서 수행하여 온 16개 사업들을 모델링한 사례 중 IV&V 효과 중 하나인 재작업(reworks)에 대한 것을 분석해 보았다[6].

전체 사업에서 비용증가에 가장 많은 기여를 하는 요인은 결함(defects)의 발생이다. 실수에 의한 결함 (defects slipped)을 수명주기 각 단계별로 수행한 연구결과를 보면 결함이 발생한 단계 이후에 결함을 고치는 것이 결함 발생 단계에 고치는 것 보다 2.5배의 비용이 더 든다. 개발 수명 주기 후반에 실수에 의한 결함을 바로잡기 위해 증가하는 비용은 그림 5와 같다. 그림에서 알 수 있듯이 개념 또는 요구사항 단계인 수명주기 초기에 발생한 결함을 구현이나 시험 단계인 나중 단계에서 결함을 수정하게 되면 많은 비용이 발생되는 것을 알 수 있다. 따라서 수명주기 초기에 결함들을 발견하여 이를 수정하거나 바로잡지 못한다면 인력, 원자재(materials), 비용, 시간 등을 재투자하여

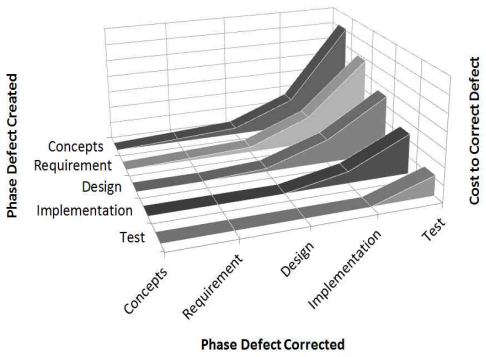

그림 5. 각 단계별 결함 및 오류 수정 비용
Fig. 5. Cost of correcting faults and errors in each phase, reproduced from [6].

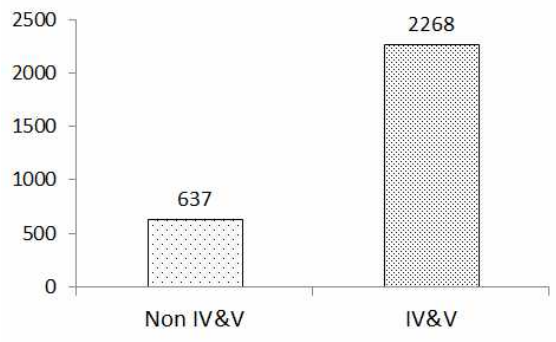

그림 6. 발견된 전체 요구사항 결함
Fig. 6. Total requirement defects detected, reproduced from [6].

야하며 일정 지연, 비용 증가의 부정적인 효과가 나타나게 된다. 재작업은 개발자 측면에서 시간 및 노력이 추가적으로 필요하기 때문에 개발 사업의 전체비용이 증가하게 된다. 추가적인 비용은 전체 사업 비용 중 30~50 %의 재작업 비용이 발생된다.

그림 6은 시스템임무부서(SMD)와 탐사시스템임무부서(ESMD)에서 발견된 전체 요구사항 결함을 나타낸 것으로 Non-IV&V와 IV&V를 비교하면 요구사항간 결함 차이는 1,631개이다.

수명주기 각 단계마다 요구사항 결함으로 인하여 발생한 결함을 수정하는데 드는 비용은 그림 7과 같다. 6단계의 수명주기 중 2단계 요구사항 단계에서 175 USD, 3단계 설계 단계에서 572 USD, 4단계 구현 단계에서 1,227 USD, 5단계 시험 단계에서 8,963 USD, 마지막 운영 단계에서 17,713 USD의 비용이 소모된다.

IV&V의 사업적용으로 인하여 수명주기 초기에 발견한 결함을 고치는데 소요된 비용은 2,800만 USD가 넘는다. 그러나 이는 요구사항에서의 결함만 고려한 것이지 전 수명주기를 고려한 것은 아니다.

그림 8의 꺾은선 그래프는 3-1 오류 검출에 대한 IV&V 관계 분석에서 전 수명주기 단계에서 검출된 오류를 수정하는데 드는 비용에 관한 그래프이다[9]. 앞서 설명한 것처럼 그룹 1의 경

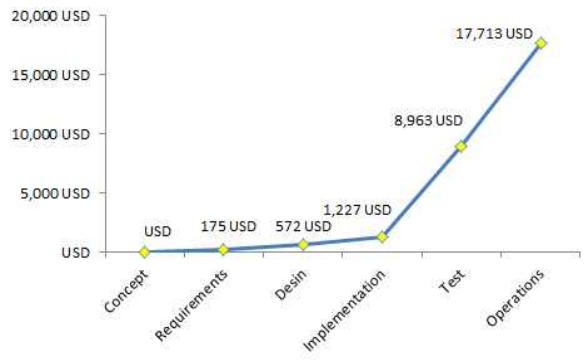

그림 7. 결함 수정 비용
Fig. 7. Cost of correcting defects, reproduced from [6].

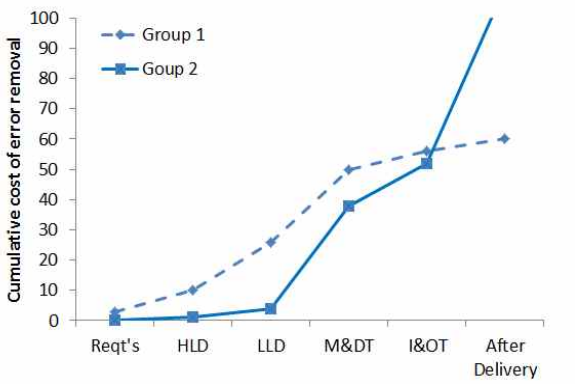

그림 8. IV&V 오류 탐지 및 관련 비용
Fig. 8. IV&V Error detection and associated cost, reproduced from [6].

우가 그룹 2의 경우보다 발견된 오류의 수는 많지만 이해관계자들 간의 빠른 피드백으로 인하여 초기단계에서 발견된 오류를 수정하는 비용이 나중 단계에서 수정하는 비용보다 적게 드는 것을 알 수 있다.

앞선 두 사례와 마찬가지로 NASA에서 개발한 우주왕복선 CSCI에 IV&V를 적용한 사례 또한 시스템 개발 수명주기 초기 단계에서 IV&V를 통하여 오류 및 결함을 발견하여 수정하면 전체 사업 비용이 절감되고 잠재적 오류의 가능성도 줄일 수 있다. 마찬가지로 전 수명주기에서 IV&V를 적용해야 비용 및 일정이 줄어드는 이득을 볼 수 있으며, IV&V를 적용하지 않는다면 수명주기 초기에 오류 및 결함을 발견할 수 없고 나중 단계에서 발견하여 이를 수정하는데 들어가는 비용은 비약적으로 상승할 것이며, 추가 일정 또한 필요할 것으로 예상된다.

3-3 개발일정에 대한 IV&V 효과 분석

NASA 소프트웨어 시스템 개발 사업에 IV&V를 적용하여 경제적 이익을 정량적으로 평가하고 이러한 이익을 낼 수 있는 방안을 모색하기 위한 연구 사례를 활용하였다[12]. 모델은 프로세스 구현, 시스템 및 소프트웨어 요구사항 분석, 소프트웨어 아키텍처 및 상세 설계, 소프트웨어 코딩 및 유닛 시험, 하드웨어 시스템 통합 계획, 소프트웨어 통합 계획, 전체 통합 및 품격(qualification) 시험, 설치 및 수락 지원 등 8 단계의 수명주기로 구성되어 있다. IV&V 활동은 요구사항 검증, 설계 검증, 코드 검증 및 확인의 4단계로 이루어져 있는데, 이 중 요구사항 추적 IV&V 기법을 이용하여 수행하였다. 표 3 및 표 4는 각 성능 측정을 통해 IV&V를 수행하지 않은 기준(baseline)과 수명주기 각 단계 및 개발인원과 QA인원 변화에 따른 IV&V 활동을 비교한 데이터이다. Table에서 음의 값은 기준이 되는 값보다 더 많은 재작업 노력 (rework effort), 일정 지연을 나타낸다.

표 3에서 확인(validation) 단계는 요구사항 추적성 분석이 늦게 적용된 단계로 V&V를 수행한 기준보다 개발 기간이 2.6 % 증가하는 것을 알 수 있는데, 나중 단계 (확인 또는 시험 단계)

표 3. 베이스라인 및 각 단계 대비 재작업 노력 및 개발기간 향상(%)
Table 3. Percent improvement compared to the baseline and each phase, reproduced from [12].

	Baseline	Reqt's	Design	Coding	Validation
Rework Effort	(201.65)	9.64%	9.09%	6.01%	-4.51%
Duration	(58.42)	3.46%	3.18%	1.78%	-2.62%

표 4. 베이스라인 및 개발 인력수 대비 재작업 노력 및 개발기간 향상(%)
Table 4. Percent improvement compared to the baseline and development staff, reproduced from [12].

	Baseline	Dev. Staff to 20	Dev. Staff to 30	Dev. Staff to 40
Rework Effort	(201.65)	0%	0%	0%
Duration	(58.42)	4.71%	7.34%	7.26%

에서 IV&V를 수행하여 많은 결함이 뒤늦게 발견되어 이로 인해 재작업 시간이 증가한 것이 주된 이유로 생각된다.

코딩 단계에서 요구사항 추적성 분석(표 3)을 하였을 때 재작업 및 개발기간은 각각 6.01 %, 1.78 %로 확인 단계에서 IV&V를 수행한 것보다 적은 노력이 들고 개발 기간 또한 줄어든 것을 알 수 있다.

마찬가지로 수명주기 초기 단계인 요구사항과 설계 단계에서 IV&V를 적용하면 코딩, 확인의 나중 단계 보다 전체 노력, 재작업 노력, 개발 기간이 감소함을 알 수 있다.

또한, 이 사례에서 구성원을 살펴보면 개발 그룹의 인원은 16명으로 구성되어 있는데, 표 4와 같이 개발 인원을 20명, 30명, 40명까지 추가한 경우 개발 기간은 각각 4.71 %, 7.34 %, 7.26 % 감소하였다. 그러나 개발 그룹의 인원을 충원하여도 재작업 노력에는 아무런 영향을 미치지 않고 순수하게 개발 기간 감소에만 영향을 미치는 것을 알 수 있다.

IV. 결론 및 제언

일반적으로 개발 시스템에 대한 검증 및 확인을 개발 조직과 분리된 독립적인 조직이 수행해야 한다는 논리는 검증의 객관성 확보 측면에서 막연하지만 그 타당성은 인정되어 왔다. 그러나 IV&V가 실제적으로 사업에 어떠한 이익을 가져다주며, 그로 인해 사업의 리스크가 얼마나 완화되고 배치된 제품에 운용 중 결함이 발생할 확률이 얼마가 되는지를 계량화하고 이를 바탕으로 객관화된 데이터를 확보하는 일은 우리나라 R&D 여건상 거의 불가능하다고 볼 수 있다. 따라서 본 연구는 이러한 어려움을 인식하고 문제를 해결하기 위한 방법으로 항공 선진기관에서 수행한 관련 연구사례 조사를 통해서 항공 안전 필수 시스템 개발 사업에 IV&V를 적용했을 때 IV&V가 오류 검출, 개발 비용 및 개발 일정 등에 미치는 효과를 분석했다. 조사 분석을 수행한 결과 IV&V는 매우 긍정적인 효과를 가져다주며, 다음의 3가지로 집약될 수 있다. 첫째, IV&V 프로세스는 종래의 V&V 프로세스에 비해 수명주기 초반에 오류 검출율을 높여준다. 즉, 조기 오류 검출율이 높아진다. 둘째, 내재된 리스크를 조기에 완화시켜 개발 비용이 획기적으로 줄어든다. 셋째, 개발 수명주기 후반에 나타나는 복잡한 재작업 확률이 줄어들어 개발 일정의 지연을 막아준다. 위에서 얻은 분석 결과를 바탕으로 IV&V 적용에 대한 효과를 부연설명하면 다음과 같다:

- IV&V는 개발 수명주기 초반에 리스크가 높은 결함의 탐지 가능성을 높여 주기 때문에 설계 그룹은 마감 시간에 쫓겨서 임시방편에 매달리지 않고 좀 더 포괄적인 시스템 솔루션 개발에 집중할 수 있다.
- IV&V는 진행 중인 개발사업의 상황과 성능보고를 사업 수준의 책임자에게 제공하고, 고객(사용자)에게도 시스템 성능에 대한 점진적인 프리뷰(preview)를 제공하여 조기에 시스템 성능을 조정할 수 있는 기회를 마련한다.
- IV&V는 모든 이해 관계자에게 시스템 개발 진도와 품질에 대한 가시성뿐만 아니라 시스템 개발 노력의 진도와 품질에 대한 가시성을 제공한다.
- IV&V는 개발 계약자에 의한 재작업의 필요성을 감소시켜서 개발사업의 총비용을 줄여준다.
- IV&V는 제품의 신뢰성을 높여 운용 중 결함이 적게 나타나고 유지보수 관리 비용이 적게 드는 효과를 가져 온다.
- IV&V는 궁극적으로 사업에 내재된 리스크를 조기에 완화시켜서 개발 사업을 성공으로 이끄는 요인이 되고, 무엇보다도 안전필수시스템의 안전성을 강화하여 귀중한 생명이나 재산 또는 환경의 손실을 방지한다.

이러한 장점이 있음에도 불구하고 현재 국내 대다수의 SCS 개발 사업에서는 IV&V 개념이 제도적으로 도입되어 있지 않아서 개발 사업의 실패율이 높거나 개발 결과물의 성능 및 품질의 저하로 나타나고 있다. 최근 선진국에서 IV&V는 품질 및 안전성을 확보하기 위하여 안전필수 항공/우주/의료 시스템 등에 적용되는 보편적 방법으로 정착되어 가고 있으며, NASA, ESA 및 JAXA는 공동으로 전략적 IV&V 연구에 착수했다. 따라서 국내 항공 R&D사업에서도 예산의 일정부분을 IV&V 전략수립 연구에 투자하여 개발된 항공안전필수시스템의 안전성과 성능을 제고시키는 전략이 필요하다.

Acknowledgments

본 연구는 국토교통부 항공안전기술개발사업의 연구비지원(15ATRP-C109149-01)에 의해 수행되었습니다.

References

[1] I. Sommerville, *Software Engineering*, 9th ed. Boston, MA: Pearson, 2010.

[2] J. Y. Kang, M. G. Kim, Y. H. Kim, and I. G. Lim, "T&E process for safety-critical CNS/ATM systems," *The Korea Navigation Institute*, Vol. 21, No. 1, pp. 50-57, Feb. 2017.

[3] FAA, Test and Evaluation Handbook, ver3, VVSPT-A2-PDD-013, 2013.

[4] FAA, NAS System Engineering Manual, ver3.1, 2006.

[5] IEEE, IEEE Standard for System and Software Verification and Validation, IEEE Std 1012 − 2012, pp. 165-167, 2012.

[6] NASA, "NASA Independent Verification & Validation Program Value Report 2008 & 2009", 2009.

[7] J. Kasser and V. R. Williams, "What do you mean you can't tell me if my project is in trouble?," in *First European Conference on Software Metrics*, Antwerp: Belgium, pp. 1-11, 1998.

[8] J. Frederick (2014, April). Evolving T&E in the FAA [Internet]. Available: http://www.incose.org/docs/default-source/enchantment/140409frederick-evolvingtandeinthefaaF92D0915726F.pdf?sfvrsn=2

[9] J. D. Arthur, M. K. Groner, K. J. Hayhurst and C. M. Holloway, "Evaluating the effectiveness of IV&V," *Computer*, Vol. 32, No. 10, pp. 79-83, 1999.

[10] R. D. Neal, D. McCaugherty, T. Joshi and J. Callahan, "A case study of IV&V cost effectiveness," NASA/WVU Software IV & V Facility, *Software Research Laboratory Technical Report Series*, Vol. 1, No. 9, 1997.

[11] U.S. Department of Defense, Software Development and Documentation, MIL-STD-498, 1998.

[12] D. M. Raffo, U. Nayak, S. Setamanit, P. Sullivan and W. Wakeland, "Using software process simulation to assess the impact of IV&V activities," in *Proceedings of the 5th International Workshop on Software Process Simulation and Modeling*, Edinburgh: UK, pp. 197-205, 2004.

김 영 훈 (Young-Hoon Kim)
2016년 08월 : 한국항공대학교 항공운항관리학과 (이학석사)
2016년 09월 ~ 현 재 : 한국항공대학교 부설 항공체계시험인증연구소(연구원)
※관심분야 : 항공체계공학

유 병 선 (Beong-Seon Yoo)
1990년 03월~1992.11월 : 미국 Aviation Atlanta Flight Instructor,
1993년 03월 ~ 현재 : 한국항공대학교 항공운항학과 교수,
2008년 11월 ~ 현재 : 해군발전 자문위원
2011년 11월 ~ 현재 : 소방방재청 정책협의회 항공분야 자문위원
1994년 08월 : 고려대학교 대학원 지구과학전공 (교육학석사)
1999년 04월 ~ 현재 : 국토교통부 항공종사자 자격시험위원
※관심분야 : 기초 비행교육 프로그램 개발, 항공종사자(조종사) 자격제도 개선, 산학연계 교육 프로그램 개발

강 자 영 (Ja-Young Kang)
1992년 06월 : 미국 Auburn Univ, AE/Ph.D.
1979년 03월 ~ 1984년 08월 : 국방과학연구소 연구원
1992년 06월 ~ 2002년 03월 : ETRI 책임연구원/팀장
2002년 03월 ~ 현 재 : 한국항공대학교 항공운항학과 교수
2011년 12월 ~ 2015년 12월 : 한국항공대학교 부설 항공체계시험인증연구센터장
※관심분야 : CNS/ATM, 항공체계공학, 위성시스템 응용