論文 J. of The Korean Society for Aeronautical and Space Sciences 46(1), 86-94(2018)
DOI:https://doi.org/10.5139/JKSAS.2018.46.1.86
ISSN 1225-1348(print), 2287-6871(online)

항공소프트웨어 안전과 보안을 위한 통합 감항 인증기준 개발 연구

한만군*, 박태규**

A Study on Integrated Airworthiness Certification Criteria for Avionics Software Safety and Security

Man-Goon Han* and Tae-Kyou Park**
Department of Aerospace Software Engineering, Hanseo University*,**

ABSTRACT

As the use of software is increasing in aircraft system, an exposure to the threat of safety and security also continues to grow. Although certification criteria for software safety such as DO-178C have already been established, specific certification criteria for software security have not yet been included. Recently DO-326A, DO-356 and DO-355 have been published separately for aircraft and system airworthiness security certification criteria. However, to comply individual certification criteria and procedures, it requires the additional cost and effort. Therefore, this paper proposes the efficient integrated certification criteria saving cost, effort and time by combining the certification criteria for software safety and security.

초 록

항공기 시스템에서 소프트웨어의 사용이 증가 추세에 있어 안전 및 보안 위협에 대한 노출이 점차 증대되고 있다. 소프트웨어 안전에 관한 인증기준은 DO-178C가 발표되었으나, 소프트웨어 보안을 위한 인증기준은 포함되어 있지 않다. 한편 최근 항공기 및 시스템 감항 보안 인증기준으로 DO-326A, DO-356 및 DO-355가 별도로 발표되었다. 그러나 안전과 보안의 인증을 위해 각각의 기준과 절차를 준수함으로써 별도의 비용과 노력이 요구되는 실정이다. 따라서 본 논문에서는 안전과 보안을 위한 각각의 인증기준을 하나로 통합하여 비용, 노력 및 시간 등을 감소시킬 수 있는 효율적인 통합인증 방안을 제시하고자 한다.

Key Words : Avionics Software(항공소프트웨어), Airworthiness(감항), Safety(안전), Security(보안), Certification(인증)

† Received : September 27, 2017 Revised : December 4, 2017 Accepted : December 4, 2017
* Corresponding author, E-mail : hanmgun@naver.com

Ⅰ. 서 론

항공기의 항공전자 시스템은 각각의 기능으로 분리된 컴퓨터로 구성된 FMA(Federate Modular Assembly) 시스템에서 더욱 작고, 가볍고, 저렴한 시스템으로의 추세와 요구로 인해서 하나의 공통 연산 플랫폼에서 구동되는 통합 시스템(IMA : Integrated Modular Assembly)으로 교체되고 있다. 결과적으로 통합시스템에서 더 작은 크기, 무게 및 전력(SWaP)에 대한 목표를 달성하기 위해서 복잡성이 증가됨에 따라 엔지니어는 이전의 어느 때보다 더 많은 소프트웨어를 개발하고 수정하고 있으며 결과물을 항공전자 시스템에 적용하게 되었다[1]. 이로 인해 항공전자 시스템이 더욱 복잡하고 난해하게 됨에 따라 안전과 보안에 관련된 결함도 증가하게 되었다.

또한, 항공전자 시스템은 운영체제, 미들웨어, 어플리케이션 등으로 대표되는 항공소프트웨어가 운용되고 있다. 더불어 인터넷을 포함한 다양한 다른 시스템과 네트워크로 서로 연결되어 있어서 인터넷 환경에서는 항공기 자체가 하나의 네트워크 노드라고 할 수 있다[2,3]. 항공소프트웨어는 여러 경로를 통한 의도적인 네트워크 공격이나 악성 바이러스와 같은 오염된 자료에 의한 침해 등 위협이 지속 증가하고 있어 보안의 중요성이 더욱 증가되고 있다.

마지막으로 항공전자 시스템에서 중요도가 비교적 낮은 시스템에는 상용(COTS : Commercial Off-The-Shelf) 제품이 많이 사용되는 추세에 있다. 이는 합리적인 가격에 확장된 기능을 제공하여 유용한 반면, 수준이 높은 보안 요구사항을 충족시키지 못하는 경향이 있고 보안 위협에 대한 노출을 가중시키는 하나의 요인이 되기도 한다[4].

이와 같이 증가되는 보안 위험은 종종 항공기 결함이나 임무수행 불가 상황을 초래하여, 군용 항공기의 경우 중요한 임무와 작전의 실패로 이어지기도 하고, 민간 항공기의 경우 회사의 명성과 신뢰도를 저하시키는 결과를 초래하여 막대한 경제적인 손실을 가져오기도 한다.

항공소프트웨어의 안전에 대한 중요성은 이미 오래 전부터 인식되어 1980년 처음으로 DO-178이 발표되어 항공기 설계, 개발 및 검증 등 전 개발과정에 거쳐 항공소프트웨어 안전기준에 대한 지침서로 활용되었으며, 2012년에 DO-178C가 발표되었다.

그러나 항공소프트웨어 보안 관련 인증기준은 비교적 늦은 시기인 1996년부터 IT 제품에 대한 보안 평가 기준인 Common Criteria(CC)를 준용하여 적용해 오다가, 2014년에 이르러 별도의 항공기 및 시스템 감항 보안 인증기준으로 DO-326A(ED-202A), DO-356(ED-203) 및 DO-355(ED-204)가 발표되었다.

항공소프트웨어 안전과 보안에 대한 인증기준은 상호 중복되는 부분이 많음에도 불구하고 각각 별도의 인증 기준과 절차를 준수함에 따라 비용과 노력이 몇 배로 소요되고 있는 실정이다. 따라서 본 논문에서는 안전(DO-178C)과 보안(CC 또는 DO-326A, DO-356, DO-355)에 대한 인증기준을 분석하여 각각의 공통적인 부분을 식별하고 부족한 부분을 보완하여 하나의 통합된 인증기준을 제시한다. 안전관련 기준인 DO-178C와 보안 관련 기준인 CC를 분석하여 DO-178C에 포함되지 않은 CC의 보안 관련 요구사항은 새로 발표된 보안 인증기준인 DO-326A 및 DO-355의 요구사항을 추출하여 보완 결합함으로써 항공소프트웨어 안전과 보안을 위한 통합 감항 인증기준을 제안하고자 한다. 이를 통해 항공소프트웨어 안전과 보안 관련 인증을 기존의 인증기준과 동일한 수준으로 유지하는 동시에 비용, 노력 및 시간 등을 상당 부분 감소시키는 효과를 기대할 수 있다.

Ⅱ. 항공소프트웨어 안전 및 보안 인증기준 현황

2.1 안전 관련 인증기준(DO-178)

항공기 시스템에서 항공소프트웨어는 1960년부터 사용되기 시작하였으며, 현대 무기체계의 경우는 첨단 전자장비 등의 비중이 높아짐에 따라 소프트웨어의 비중과 역할도 비약적으로 높아지고 있다. 전투기가 수행하는 임무 중 항공소프트웨어가 차지하는 비중은 1960년에 F-4 전투기는 8%에 불과했지만, F-16에서는 45%, F-22는 80%, 한국공군이 도입예정인 F-35는 90% (2007년)에 달해 F-4에 비해 11배가 증가되었다[5]. 이에 따라 하드웨어 위주의 결함만 해결하던 과거와는 달리 이제는 소프트웨어 오류에 대한 문제해결 및 품질보증에 대한 노력이 절실하게 되었다.

1980년에 이러한 시대적인 요구에 의해 RTCA (Radio Technical Commission for Avionics)는 항공소프트웨어 안전에 대한 검증과 인증을 위한 기준인 DO-178을 제정하였다[6]. 유럽에서도 EUROCAE (European Organization for Civil Aviation Equipment)에 의해 ED-12가 발표되었다. 이 두 문서는 여러 번의 개정을 거쳐 1992년에 DO-178B(ED-12B), 그리고 2011년에는 DO-178C(ED-12C)가 승인되었다[7,8].

DO-178B와 비교하여 DO-178C에는 모델-기반 개발

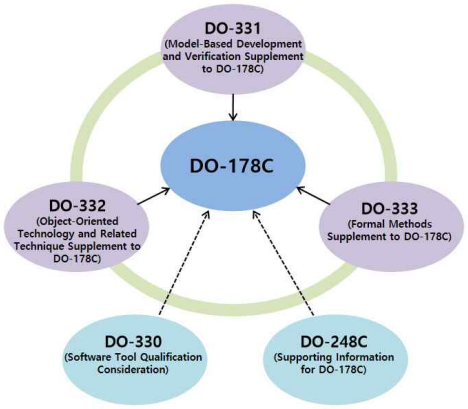

Fig. 1. DO-178C Supplement Documents

및 검증(Model-Based Development and Verification), 정형기법(Formal Method) 그리고 객체지향 기술(Object-Oriented Technology)과 같은 새로운 소프트웨어 개발 기술에 대한 지침이 추가 반영되었다. Fig. 1에서와 같이 새로운 기술을 도입하기 위해 기존의 문서를 확장하기보다는 DO-178C와 함께 부가적으로 사용될 수 있는 새로운 문서들을 추가하였다. 이 문서들을 세부적으로 살펴보면 DO-330(소프트웨어 툴 검증 고려사항), DO-331(모델 기반 개발 및 검증), DO-332(객체지향 기술 및 관련 기술), DO-333(정형 기법), DO-248C(추가 정보) 등이다[9]. DO-178C는 소프트웨어 계획, 개발, 검증, 형상관리 및 품질보증 등 모든 수명주기 프로세스 기간에 거쳐 적용된다.

항공소프트웨어 개발과정에 있어 안전에 대한 검증을 위해서는 위험요소를 결정하는 것이 중요하다. DO-178C는 항공기의 안전을 저해하는 결함과 관련된 항공소프트웨어 위험요소를 Table 1과 같이 다섯 가지 등급으로 분류하고 있다[8].

다섯 가지 등급은 결함이 가장 치명적인 A 등급부터 항공기 안전에 전혀 영향이 없는 E 등급까지이다. A 등급은 항공기에 재난을 초래하는(Catastrophic) 결함을 유발시키는 수준이며, B 등급은 항공기에 매우 위험한(Hazardous) 결함을 초래하고, C 등급은 중대한(Major) 결함을 유발하며, D 등급은 사소한(Minor) 결함을 발생시키는 상태, 그리고 E 등급은 항공기에 아무런 영향이 없는(No Effect) 상태를 나타낸다.

또한 DO-178C 인증기준을 통과하기 위해서 달성해야 하는 속성들이 정의되어 있는데 이를 충족목표(Objectives)라고 한다. 이 충족목표들은 개발 대상 소프트웨어의 등급에 따라 달라진다. DO-178C에서 A 등급의 경우 71개의 충족목표를 달성해야하는 반면, D 등급의 경우 26개의 충족목표만을 달성하면 된다[8].

Table 1. Safety Level of DO-178C

Level	Designation	Interpretation	objectives
A	Catastrophic	Would result in multiple fatalities, typically loss of the airplane	71
B	Hazardous	A large reduction in safety margins or functional capabilities, physical distress or excessive workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely	69
C	Major	A significant reduction in safety margins or functional capabilities, a significant increase in crew workload, or physical distress to passengers or cabin crew	62
D	Minor	A slight increase in crew workload, such as routine flight plan changes, or some physical discomfort to passengers or cabin crew	26
E	No Effect	No effect on safety	0

2.2 안전 인증기준 적용 및 승인

항공소프트웨어에 대한 FAA 인증 프로세스는 항공전자 시스템 프로세스와 이와 연계된 시스템 안전 프로세스와 관련되어 있다. 소프트웨어는 별도로 인증되지 않으므로 인증 대상 구성품 또는 항공기와 같이 보다 넓은 관점에서 고려되어야 하고 시스템 안전 프로세스와 연계하여 검토되어야 한다.

Figure 2는 전체 항공 시스템 개발과 관련된 프로세스와 소프트웨어 프로세스에 대한 관계를 나타내고 있다. 시스템 프로세스(System Process)에서는 안전과 관련된 시스템 요구사항을 식별하고 이 요구사항들은 시스템 안전 평가 프로세스(System Safety Assessment Process)로 전달된다. DO-178C는 소프트웨어 안전에 대한 인증을 A 등급부터 E 등급까지 5개의 등급으로 분류한다. 이러한 분류는 소프트웨어 탑재장비의 안전성 및 신뢰성 수준에 따라 결정되며, 이는 항공기 개발 프로세스 중 시스템 안전성 평가 프로세스에 의해 결정된다[8].

인증 등급이 결정되면 이 등급은 다시 시스템 프로세스로 전달되고, 시스템 프로세스는 다시 소프트웨어 위험 등급, 소프트웨어 관련 시스템 요구사항 및 소프트웨어 안전 관련 요구사항을 결정하여 소프트웨어 프로세스(Software Process)로 전달하는 절차를 수행한다.

DO-178C에서는 수명주기 프로세스(Life Cycle Processes)는 소프트웨어 계획 프로세스와 요구사항, 설계, 코딩 및 통합 단계로 구분되는 소프트웨어 개발 프로세스, 그리고 검증, 형상관리, 품질보증, 인증 프로세스 등으로 구성된다.

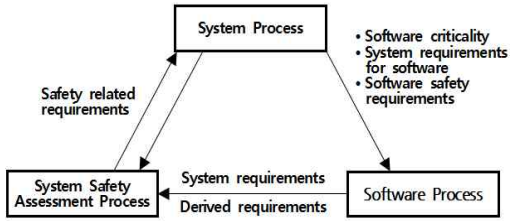

Fig. 2. FAA Certification Overview

항공소프트웨어 인증은 FAA와 FAA의 공식 대리자인 DER(Designated Engineering Representative)에 의해 수행된다. 또한 DER은 현지 안전 담당 요원으로서의 기능을 수행하며 FAA 인증 요구사항이 충족되는지를 확인할 수 있는 적절한 프로세스를 수립한다. FAA는 항공기와 항공기 시스템의 최종 인증에 대한 권한이 있으며 인증을 위해 제출된 자료를 평가하여 인증을 수행한다[8].

2.3 보안 관련 인증기준(CC 및 DO-326A, DO-356, DO-355)

항공기는 다양한 서비스를 제공하기 위하여 외부 시스템과 연결되어 있으며 이중에는 보안에 대한 표준이나 요구조건을 준수하는 시스템 및 서비스도 있지만 인터넷과 같이 허용되지 않은 접근으로 인해 서비스나 시스템에서 보안 위협에 노출되는 위험이 상존하고 있다.

이와 같이 외부의 비인가된 보안 위협에 취약한 항공 시스템은 Airline Network, Airport Terminal Wireless Networks, Public Networks, Portable Electronic Device, Wireless Aircraft Sensors and Sensor Networks, Wireless Ground Support Equipment, USB devices, Maintenance devices 등이 될 수 있다[10]. Fig. 3은 항공기의 전반적인 전자장비 구조 및 설계를 나타내고 있다.

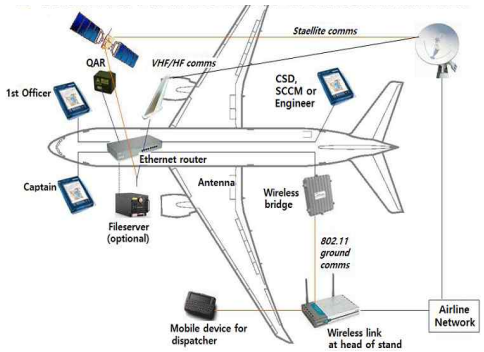

Fig. 3. E-enabled Architecture & Infrastructure

Table 2. EAL of Common Criteria

EAL	Definition	Explanation
1	Functionally tested	Applicable to systems where threats to security are not viewed as serious
2	Structurally tested	Requirements a low to moderate level of independently assured security
3	Methodically tested and checked	Requires a moderate level of independently assured security and thorough investigation of TOE
4	Methodically designed, tested and reviewed	Applicable when moderate to high level of independently assured security is required
5	Semi-formally designed and tested	Applicable where a high level of independently assured security in a planned development and a rigorous development approach is needed
6	Semiformal verified designed and tested	Applicable to the development of security TOEs for application in high risk situations
7	Formally verified designed and tested	Applicable to TOEs with tightly focused security functionality that is amenable to extensive formal analysis

한편, 1980년대 초에 IT 제품의 보안성을 평가하기 위해 미국은 NSA(National Security Agency)에서 TCSEC(Trusted Computer Evaluation Criteria)를 개발하였고, 이를 바탕으로 1990년에 ISO에서 국제적 표준인 공통평가기준(Common Criteria)을 개발하기 시작하여 1996년에 CC V1을 발표하였으며 1999년에 CC V2.1을 발표하였다[11].

CC 요구사항은 감사(Audit), 통신(Communication), 암호(Cryptography), 데이터 보호(Data Protection), 인증(Authentication), 보안관리(Security Management), 프라이버시(Privacy), 평가목표(TOE : Target Of Evaluation)의 보호, 자원 활용(Resource Utilization), 평가목표 접근(Access), 신뢰 경로(Trust Path)를 포함한다[12]. 인증 요구사항은 여러 개의 클래스로 구성되고 각각의 클래스는 여러 개의 패밀리를 포함하고 있으며, 패밀리는 요구사항을 명시하는 컴포넌트로 구성된다. 인증 관련 클래스는 형상관리, 배포 및 운영, 개발, 지침 문서, 수명주기 지원, 테스트, 취약성 평가 등으로 구성된다. IT 보안 제품에 대한 인증 요구사항이 구현된 것이 보호프로파일(PP : Protection Profile)이며 보안목표(ST : Security Target)는 보호 프로파일과 유사하나 제품에 대한 세부적이며 구체적인 정보를 포함하고 있어 제품에 대한 보안 요구사항을 충족시키기 위한 구체적

인 수단을 정의한다[13].

CC에서는 항공소프트웨어 보안에 대한 평가인증 등급을 7가지로 구분하며 EAL(Evaluation Assurance Level) 1이 가장 낮은 보안 등급을 의미하며, EAL 7은 가장 높은 등급에 해당된다. Table 2는 CC의 평가인증 등급을 나타내고 있다[1,14].

항공소프트웨어 구성품이나 시스템의 CC 인증을 위한 첫 번째 단계는 평가 제품에 대한 EAL 등급을 결정하는 것이다. CC 인증을 위해 요구되는 노력과 비용은 EAL 등급에 따라 달라진다[14]. EAL 등급이 결정되고 나면, 제품의 보안 요구사항을 충족시킬 수 있는 보호프로파일(PP)을 확인하고 요구사항에 맞게 약간 조정하거나, 만일 아직 PP가 없는 경우, 결정된 EAL 등급에 맞는 보안 기능 요구사항과 보안 인증 요구사항을 준수하여 PP를 만들어야 한다.

다음은 개발자가 보안 요구사항을 충족시키기 위해 보안목표(ST)를 준비하고 제조자는 평가를 위해 제품과 ST와 관련 문서를 인증된 시험소에 제출한다. 시험소는 ST와 대조하여 제품을 평가하고, 평가가 통과되면 그 결과를 평가 기관에 제출한다. 미국의 경우 평가기관이 NSA와 NIST (National Institute of Standards and Technology)가 제품의 확인을 통해 CC 인증을 발행하고 제품은 공식적으로 인증된 제품 목록에 추가되는 절차를 거치게 된다[11,15].

2014년에 RTCA와 EUROCAE의 두 단체는 항공 시스템에 대한 감항 보안에 관한 기준 문서를 발표하였다. RTCA의 SC-216이라는 특별단체(Special Committee)는 항공기 시스템 정보보안 인증부분을 담당하였고, EUROCAE의 WG-72라는 작업그룹(Working Group)은 지상 시스템과 관련된 항공기 시스템의 항공정보 시스템 보안(AISS : Aeronautical Information System Security) 부분을 담당하여 보안 관련 기준을 제정하였다. 각각의 기관은 항공기 및 시스템에 대한 보안 위험을 평가하고 보호하기 위한 감항 보안 프로세스(AWSP : Airworthiness Security Process) 기준 문서인 DO-326A와 ED-202A를 제정하였으며, DO-326A (ED-202A)에 기술된 프로세스와 활동을 지원하기 위한 기준 문서로 DO-356과 ED-203을 발표하였고, 감항 보안을 유지하기 위한 정보보안 지침서로 DO-355와 ED-204를 발표하였다[10,16,17].

감항 보안 프로세스(AWSP)의 목적은 비인가 상호작용(unauthorized interaction)에 대해 항공기가 안전한 작동 상태를 유지하도록 하는 것이다. 이를 위해 감항 보안 위험평가(Airworthiness Security Risk Assessment)를 수행해야 하며, 평가 결과로 도출된 보안위험이 감항 보안 프로세스를 통해 정해진 기준 범위를 충족해야 한다. 보안 공격에 의해 항공기 시스템(자산)의 상태가 변경될 경우 안전에 대해서도 영향을 미치게 되는데 이러한 상태를 위협상태로 정의한다. Table 3은 위협상태에 대한 등급을 나타내고 있다[16].

Table 3. Level of Threat Condition

Level	Term	Definition
V	No Safety Effect	Would not affect the operational capability of the airplane, and Would not increase crew workload
IV	Minor	Slight reduction in safety margins or functional capabilities, or Slight increase in crew workload, or Some physical discomfort to passengers or cabin crew
III	Major	Significant reduction in safety margins or functional capabilities, or Significant increase in crew workload, or Discomfort or physical distress to passengers or cabin crew, possibly including injuries
II	Hazardo-us	Large reduction in safety margins or functional capabilities, or Physical distress or higher workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely, or Serious or fatal injury to an occupant other than the flight crew
I	Catastro-phic	Occurrence of multiple fatalities, usually with the loss of the airplane

2.4 감항 보안 인증기준 적용 및 승인

항공기 및 시스템 감항 보안 인증기준인 DO-326A, DO-356, DO-355에 명시된 감항 보안 프로세스(AWSP)는 크게 세 가지로, 첫째 인증 프로세스에 해당하는 인증 활동(Certification Activities), 둘째는 위협 시나리오를 토대로 하여 위험을 평가하고 구현된 보안에 대한 평가를 통해 수락여부를 결정하는 보안위험 평가활동(Security Risk Assessment Related Activities), 마지막으로 필요한 보안대책을 구현하기 위한 보안 개발활동(Security Development Related Activities)이다. 여기서 위협 시나리오는 항공기 안전에 부정적인 영향을 미칠 수 있는 인가되지 않은 어떠한 작용이 발생되는 것을 말한다[10]. Fig. 4는 감항 보안 프로세스에 대한 흐름도를 나타내고 있다.

첫 번째 단계는 보안인증 계획(Plan for Security Aspects of Certification)으로 인증 신청자가 계획하고 인증기관에서 동의한다. 두 번째로는 보안영역 정의(Security Scope Definition)로 보안위험 평가를 위한 보안영역을 설정하며, 세 번째는 보안위험 평가(Security Risk Assessment)로 보안위험을 식

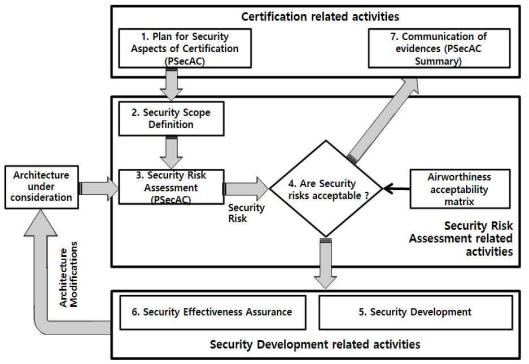

Fig. 4. Airworthiness Security Process

별하여 평가하고, 네 번째는 보안위험 평가 결과에 대한 수락 가능 여부를 판단한다. 다섯 번째는 보안대책이 필요한 경우 보안 개발(Security Development)을 수행한다. 보안 개발은 보안 위험을 포함하고 있는 위협 시나리오에 대응하기 위하여 보안대책이라 할 수 있는 보안 아키텍처를 설계하는 과정이다. 여섯 번째는 보안효율 인증(Security Effectiveness Assurance)으로 보안위험이 수락 가능함을 보증하기 위한 활동이다. 여기서 보안효율이란 항공기가 인가되지 않은 상호작용에 대해 얼마나 잘 보호되어 있는지를 나타내며 보안위협 평가 과정에서 위협 시나리오에 대해 자산을 보호하기 위한 보안대책의 능력으로 정의될 수 있다. 마지막 단계는 결과 종합으로 위험이 수락 가능한 경우, 감항 보안 활동결과를 보고서(PSecAC Summary)로 종합하는 것이다.

Table 4에서 정의된 바와 같이 보안위험 평가 과정에서 수락 가능여부를 결정하기 위해서 감항 보안 수락 매트릭스(Airworthiness Security Acceptability Matrix)라는 보안위험 평가 도구가 사용된다. 감항 보안 수락 매트릭스를 이용하여 위협 시나리오 영향(위협 상태 등급)과 위협 등급의 조합에 의해 수락 가능여부를 결정할 수 있다. 위협 상태 등급은 Table 3에서 설명된 바와 같이 No Effect부터 Catastrophic의 다섯 단계로 구분되며, 위협 등급은 위협 시나리오에서 보안 공격의 성공 가능성(likelihood)에 의해 결정되는데, 이 가능성은 공격이 성공하는 빈도에 대한 정성적인 평가로 측정된다. 위협 시나리오 보안 공격 성공 가능성은 pV부터 pI까지 다섯 등급으로 구분되며 각각은 “Frequent”, “Probable”, “Remote”, “Extremely Remote”, “Extremely Improbable”에 해당된다[16].

보안위험에 대한 수락 가능여부는 감항 보안 수락 매트릭스를 활용하여 인증 신청자가 판단하고 감항 인증 기관이 동의하는 절차를 따르게 된다. 이때 수락 가능한 위험은 추가적인 보안대책이 불필요하지만, 수락 불가능한 위험에 대해서는 수락을 위해 위험을 완화할 수 있는 보안대책이 구현되어야 한다.

Table 4. Airworthiness Security Acceptability Matrix

Risk Level		Threat Scenario Impact				
Threat Scenario Likelihood		V	IV	III	II	I
		No Effect	Minor	Major	Hazar-dous	Catast-rophic
pV (1)	Frequent	Accep-table	Unacc-eptable	Unacc-eptable	Unacc-eptable	Unacc-eptable
pIV (10^{-3})	Probable	Accep-table	Accep-table	Unacc-eptable	Unacc-eptable	Unacc-eptable
pIII (10^{-5})	Remote	Accep-table	Accep-table	Accep-table	Unacc-eptable	Unacc-eptable
pII (10^{-7})	Extremely Remote	Accep-table	Accep-table	Accep-table	Accep-table	Unacc-eptable
pI (10^{-9})	Extremely Improbable	Accep-table	Accep-table	Accep-table	Accep-table	Accep-table

한편, DO-178C와 항공기 및 시스템 감항 보안 인증 기준인 DO-326A, DO-356, DO-355를 활용하여 하나의 통합된 인증기준을 작성하여 안전과 보안에 대한 인증을 동시에 수행할 수 있다. 또한 최근 발표된 감항 보안 인증을 위해서는 상기에 제시된 감항 인증 프로세스를 준수하는 검증 과정을 통해 항공소프트웨어 보안에 대한 인증을 확보할 수 있다.

2.5 안전 및 보안 관련 인증기준 비교

본 논문에서는 안전 관련 인증기준인 DO-178C와 보안 관련 인증기준인 CC 및 DO-326A의 요구사항을 분석하여 서로 일치하는 부분과 상이한 부분을 식별하였으며 이를 Table 5에 제시하였다.

CC의 ACM 클래스는 형상관리와 관련된 내용으로 DO-178C의 소프트웨어 형상관리 프로세스와 동일하고 CC의 ADV 클래스는 소프트웨어 개발 프로세스와 내용이 일치한다. 그리고 CC의 ALC 클래스와 ATE 클래스는 각각 DO-178C의 소프트웨어 계획 프로세스와 소프트웨어 검증 프로세스와 일치하고 있다. 하지만 CC의 ADO, AGD 및 AVA 클래스는 DO-178C의 어떠한 프로세스와도 일치하지 않는다. DO-178C의 프로세스와 일치하지 않는 세 개의 CC의 클래스는 감항 보안 인증기준인 DO-326A와 DO-355의 감항 보안 활동과 내용이 각각 일치하는 것을 확인할 수 있으며 또한

Table 5. Comparison between CC, DO-178C and Airworthiness Security Activities

CC Class(EAL 5)	DO-178C Processes	Airworthiness Security Activities
ACM Configuration Management	7. Software Configuration Management Process	
ADO Delivery and Operation	Not applicable	**DO-355**
ADV Development	5. Software Development Process	
AGD Guidance Documents	Not applicable	**DO-326A** ASOG, SSIG
ALC Life Cycle Support	4. Software Planning Process	
ATE Tests	6. Software Verification Process	
AVA Vulnerability Assessment	Not applicable	**DO-326A** PSecAC, PSecAC Summary, ASSD, PASRA, ASRA, SSSD, PSSRA, SSRA, ASAM, ASV, SSAM, SSV

대체가 가능하다. 결론적으로 CC를 DO-178C와 비교해보면 CC의 7개 클래스 중에서 4개는 공통부분이 존재하나, 3개의 클래스는 불일치하고 있다[15].

따라서 DO-178C와 일치하지 않는 3개의 CC 클래스는 ADO(배포 및 가동), AGD(지침서) 및 AVA(취약성 평가)이며, 감항 보안 관련 최신 인증 기준인 DO-326A와 DO-355의 감항 보안 활동으로 대체가 가능함을 확인하였다. 따라서 DO-178C와 일치하지 않는 3개의 CC 클래스와 대체가 가능한 감항 보안 인증기준을 통합하여 안전과 보안을 위한 통합 감항 인증기준을 개발할 수 있다.

III. 안전 및 보안 관련 통합 인증기준

현재는 항공소프트웨어를 개발함에 있어서 안전 및 보안 관련 인증기준을 통과하기 위해서 각각의 인증에 필요한 프로세스를 별도로 거쳐야하기 때문에 각각의 인증기준을 충족시키기 위해서 두 배 이상의 시간과 비용이 요구되고 있는 실정이다. 따라서 안전 및 보안에 대한 인증기준은 상호 중복되는 내용을 포함하고 있어 통합 인증기준 마련이 필요하다[18].

소프트웨어 보안 관련 인증기준인 CC는 안전 관련 인증기준인 DO-178C와 비교하여 4개의 공통적인 요구사항이 존재하고 3개는 일치하지 않음을 확인하였다. 따라서 CC의 일치하지 않는 3개의 인증 요구사항 클래스는 최신 인증기준인 DO-326A 및 DO-355의 인증 요구사항으로 대체하고 이를 DO-178C와 결합함으로써 항공소프트웨어 안전과 보안을 위한 하나의 통합 감항 인증기준을 도출할 수 있다. 불일치한 CC의 인증 클래스와 대체 가능한 DO-326A 및 DO-355 인증 활동과 목표(objectives)에 대한 요약은 Table 6에 제시하였다.

기존의 보안 인증기준으로 활용 중이던 CC의 인증 클래스는 DO-178C 인증 프로세스와 공통적인 부분이 존재하며, DO-178C 프로세스에 포함되어 있지 않은 CC 클래스는 최근 2014년 발표된 보안 인증기준인 DO-326A 및 DO-355로 완벽하게 대체될 수 있다. 따라서 기존의 안전과 보안에 대한 인증기준과 동일 수준으로 검증이 가능하므로 인증에 대한 신뢰성을 동일하게 유지할 수 있는 동시에 인증을 위한 효율성은 증대될 수 있다. 또한 두 개의 절차를 통합함으로써 인증을 위한 절차를 간소화하고 소요되는 비용과 시간이 절감될 수 있다. 뿐만 아니라 항공기 시스템 내에서 운용되는 항공소프트웨어는 소프트웨어 보안 위협으로부터 발생되는 문제가 곧바로 소프트웨어의 결함으로 이어지는 경향이 있다. 따라서 항공소프트웨어 안전과 보안은 상호 유기적으로 연관성을 가지고 있으므로 항공소프트웨어 안전과 보안에 대한 통합된 인증기준에 의해 안전이라는 범주 내에서 보안에 대한 인증절차가 수행되는 것이 훨씬 더 신뢰성과 효율성을 증가시키는 방법이 될 것이다.

따라서 Table 6에서와 같이 DO-178C에 포함되어 있지 않은 CC의 인증 요구사항은 DO-326A와 DO-355의 인증 요구사항으로 각각 대체가 가능하며 이를 DO-178C와 결합하여 항공소프트웨어 안전과 보안에 대한 인증을 위해 통합된 인증기준으로 활용이 가능할 것이다.

IV. 결 론

최근 항공기 시스템의 기능이 대부분 소프트웨어로 구현됨에 따라 항공소프트웨어의 안전과 보안에 대한 대책과 이에 대한 평가와 인증이 필수적이다. 현재 항공소프트웨어 인증체계는 안전과 보안의 인증 요구사항이 중복되는 부분이 많음에도 불구하고 안전과 보안에 대한 인증을 위해 별도의 인증기준과 절차를 준수하는 불편함이 있다. 또한 각각의 기준과 절차를 따로따로 준수

Table 6. DO-326A and DO-355 Activities consistent with CC Classes which are not matched with DO-178C Processes

CC Classes	Airworthiness Security Activities
ADO Delivery and Operation	DO-355
	• Airborne Software • Aircraft Components • Aircraft Network Access Points • Ground Support Equipment(GSE) • Ground Support Information Systems • Digital Certificates • Aircraft Information Security Incident Management • Operator Aircraft Information Security Program • Operator Organization Risk Assessment • Operator Personnel Roles and Responsibilities • Operator Personnel Training
AGD Guidance Documents	DO-326A
	• **ASOG**(Aircraft Security Operator Guidance) – ASOG is correct, complete and validated – ASOG is consistent and complete with respect to aircraft security scope – ASOG is consistent and complete with respect to aircraft requirements and implementation – ASOG is consistent and complete with respect to System Security Integrator Guidances(SSIG) • **SSIG**(System Security Integrator Guidance) – SSIG is correct and complete – SSIG is consistent and complete with respect to system – SSIG is consistent and complete with respect to system security scope
AVA Vulnerability Assessment	• **PSecAC**(Plan for Security Aspects of Certification) – PSecAC is correct and complete • **PSecAC Summary** – PSecAC Summary is consistent and complete with respect to PSecAC – PSecAC Summary is consistent to aircraft security verification and test results and analysis – Deviations are acceptable • **ASSD**(Aircraft Security Scope Definition) – ASSD(security perimeter, security environment) is identified, correct and complete • **PASRA**(Preliminary Aircraft Security Risk Assessment) – PASRA is consistent with Aircraft Functional Hazard Assessment – PASRA is consistent and complete with respect to aircraft security scope, aircraft requirements, and aircraft security architecture – Preliminary aircraft security risks are acceptable – PASRA is consistent and complete with respect to PASA • **ASRA**(Aircraft Security Risk Assessment) – ASRA is correct, complete, and consistent with aircraft requirements, and aircraft safety assessment – ASRA is consistent and complete with respect to aircraft & system security scope, security architecture, operator guidance, and vulnerability dossier – ASRA is consistent and complete with respect to SSRA • **SSSD**(System Security Scope Definition) – System requirements are identified, correct, and complete for security concerns – System security scope is identified, correct and complete – System security scope is consistent and complete with respect to aircraft security scope and adjacent system security environments – System security scope is consistent and complete with respect to aircraft security architecture and aircraft requirements for security concerns

CC Classes	Airworthiness Security Activities
AVA Vulnerability Assessment	DO-326A
	• **PSSRA**(Preliminary System Security Risk Assessment) – Preliminary System Security Assessment is correct and complete – Preliminary System Security Assessment is consistent and complete with respect to system security scope, system requirements, and system security architecture – Preliminary Aircraft Security Assessment is consistent and complete with respect to system security requirement and Preliminary System Safety Assessment – Preliminary system security risks are acceptable • **SSRA**(System Security Risk Assessment) – System Security Assessment is correct, complete and consistent with system requirements and System Safety Assessment – System Security Assessment is consistent and complete with respect to system security scope, system security architecture, System Security Integrator Guidance, system requirements and system verification – System security risks are acceptable • **ASAM**(Aircraft Security Architecture and Measures) – Aircraft security architecture and requirements are correct, complete and consistent with aircraft safety architecture – Aircraft security architecture and requirements are consistent with aircraft requirements – Aircraft security architecture is consistent and complete with respect to aircraft security scope – Aircraft security effectiveness requirements are correct, complete and consistent with Preliminary Aircraft Security Risk Assessment – Assurance actions are consistent with threat conditions for security measures • **ASV**(Aircraft Security Verification) – Security elements of aircraft verification and test plans are correct, complete, and approved – Aircraft verification is correct and complete for security concerns – Aircraft verification is consistent and complete with respect to aircraft requirements and aircraft security architecture – Aircraft vulnerability assessment and test results and analysis is consistent and complete with respect to aircraft security scope, aircraft requirements, PASRA, and ASOG – Remaining vulnerabilities in aircraft vulnerability dossier are acceptable – Aircraft vulnerability dossier is correct and complete • **SSAM**(System Security Architecture and Measures) – System security architecture and requirements are correct, complete and consistent with system safety architecture and ASAM – System security effectiveness requirements are correct, complete and consistent with PSSRA – Assurance actions are consistent with threat conditions for security measures • **SSV**(System Security Verification) – Security elements of system verification and test plans are correct, complete, and approved – System verification is correct and complete for security concerns – System verification is consistent and complete with respect to aircraft security scope – System verification is consistent and complete with respect to system requirements and system security architecture – System vulnerability dossier is correct and complete – System vulnerability assessment and test results and analysis is consistent and complete with respect to system security scope, system requirements, and SSIG – System vulnerability assessment and test results and analysis is consistent and complete with respect to PSSRA

해야 하기 때문에 중복된 노력과 비용 및 시간 등을 할애해야 하는 어려움을 겪고 있다.

본 논문에서는 안전과 보안에 적용되는 각각의 인증기준을 하나로 결합한 통합 인증기준을 제시하였다. 먼저 안전과 보안에 관련된 인증 기준을 분석하여 상호 공통적인 요구사항과 일치하지 않는 요구사항을 식별하였다. 안전 관련 인증기준인 DO-178C에 포함되지 않는 보안 관련 인증기준인 CC의 요구사항을 식별하여 최신 보안 인증기준인 DO-326A와 DO-355에서 해당되는 요구사항으로 보완하여 안전과 보안을 위한 통합 감항 인증기준을 제시하였다. 따라서 하나의 인증기준을 활용하여 안전과 보안 관련 인증을 동시에 수행할 수 있으므로 인증에 필요한 시간 및 비용과 노력을 절감할 수 있을 것이다.

현재 항공분야의 안전 인증업무는 국토해양부에서 주관하고 있으며, 보안 관련 인증업무는 과학기술정보통신부 산하 국가보안기술연구소에서 담당하고 있다. 따라서 국토해양부에서 안전과 보안을 위한 통합 감항 인증에 대한 전반적인 업무를 주관하되, 국가보안기술연구소의 보안 인증 지원을 받아 인증업무를 수행하는 것이 바람직한 형태가 될 것이다. 이는 항공분야 특성상 보안은 안전에 포함되는 것이 바람직하기 때문이다.

References

1) Paul Skentzos, DornerWorks, Ltd., "Software safety and security best practices : a case study from aerospace," *2014 NDIA Ground Vehicle Systems Engineering and Technology Symposium*, August 12-14, 2014.

2) Thompson Aerospace, "Aircraft Information Technology made Straightforward and Secure," Thompson Aerospace, 2017.

3) Laurent Fabre and Jeff Joyce, Critical Systems Labs, "Integration of Security and Airworthiness in the Context of Certification and Standardization," *SafeComp 2014-ISSE workshop*, Sep. 8, 2014.

4) Youssef Laarouchi, Yves Deswarte, David Powell, Jean Arlat, Eric De Nadai, "Ensuring safety and security for avionics: a case study," *DASIA 2009 Conference, Data Systems in Aerospace*, May 26-29, 2009, pp.1.

5) Unite States Airforce Scientific Board, "Report on sustaining air force aging aircraft into the 21st century," 2011.

6) Johnson, L. A. "DO-178B, Software considerations in airborne systems and equipment certification," 1998,

7) RTCA. *DO-178B, Software Considerations in Airborne Systems and Equipment Certification*, RTCA, 1992.

8) RTCA. *DO-178C, Software Considerations in Airborne Systems and Equipment Certification*, RTCA, 2011.

9) Youn, Won-Keun, Yi, Baek-Jun, "Development trend of software certification technology for the safety of avionic system", *Current Industrial and Technological Trends in Aerospace*, Vol. 11, 2013, pp.192~193.

10) RTCA, *DO-326A, Airworthiness Security Process Specification*, Aug. 6, 2014, pp.35~36.

11) Troy, E. F., "Common Criteria: Launching the International Standards," NIST, 1998.

12) Joe Wlad, LynuxWorks, "DO-178B and the Common Criteria: Future Security Levels," *COTS Journal*, 2009, pp.4.

13) NIST, *Common Criteria for Information Security Evaluation. Parts 1, 2, 3*, NIST, 1999.

14) NIST, *Common Criteria User Guide*, NIST, 1999.

15) Carol Taylor, Jim Alves-Foss, and Bob Rinker, "Merging safety and assurance: the process of dual certification for software," *High Integrity Software*, 2002, pp.8.

16) RTCA, *DO-356, Airworthiness Security Methods and Considerations*, Sep. 23, 2014.

17) RTCA, *DO-355, Information Security Guidance for Continuing Airworthiness*, June 17, 2014.

18) Stephane Paul et al, "Recommendations for security and safety co-engineering(release n°3)," 2016.