Journal of KIIT. Vol. 21, No. 1, pp. 39-48, Jan. 31, 2023. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2023.21.1.39

무인비행체 지상관제시스템 안전성 평가를 적용한 소프트웨어 개발 방안 연구

장 정 훈*

A Study on Software Development Guideline by Applying System Safety Assessment for GCS of UAV

Jeong-Hoon Jang*

국토교통부/국토교통과학기술진흥원의 지원으로 수행되었음(과제번호: 22DPIW-C153651-04,
과제명: 공공혁신조달 무인이동체 통합기술관리 및 시험평가체계 개발)

요 약

본 연구에서는 무인비행체 시스템에 대한 안전성 평가(SSA)를 기반으로 지상제어시스템(GCS)을 개발하는 방안을 제시한다. 보다 안전한 무인비행체 시스템을 개발하기 위해서는 FAA에서 제시하는 SSA와 항공용 소프트웨어 개발 절차(DO-178C) 등의 항공 분야의 시스템 개발 가이드를 활용한다. 무인비행체 시스템에 대한 SSA를 수행하고 그 결과로부터 시스템 안전 요구사항과 안전등급(Safety level)이 정해지며, 시스템 안전 요구사항은 시스템의 각 구성요소에 할당되고, 해당 구성요소의 안전등급이 결정된다. 무인비행체 시스템은 크게 비행체와 GCS로 구성되며, GCS에 할당된 안전 요구사항 안전등급에 적합하게 GCS 소프트웨어를 개발하는 소프트웨어 개발 방안을 제시한다.

Abstract

In this study, we propose a method to develop a ground control system(GCS) based on the safety assessment (SSA) for unmanned aerial vehicle(UAV) systems. In order to develop a safer unmanned aerial vehicle system, use the system development guide in the aviation field, such as the SSA and aviation software development procedure (DO-178C) presented by the FAA. SSA is performed on the unmanned aerial vehicle system, and the system safety requirements and safety level are determined from the results, the system safety requirements are assigned to each component of the system, and the safety level of the component is determined. The unmanned aerial vehicle system is largely composed of the vehicle and the GCS, and suggests a software development plan to develop the GCS software in accordance with the safety requirements and safety grades assigned to the GCS.

Keywords
UAV, SSA, GCS, SDLC, safety

* ㈜모아소프트 핵심기술센터 미래사업본부
- ORCID: https://orcid.org/0000-0003-1031-8226

· Received: Oct. 27, 2022, Revised: Dec. 07, 2022, Accepted: Dec. 10, 2022
· Corresponding Author: Jeong-Hoon Jang
Dept. of Future Business Division, MOASOFT Corp. Korea
Tel.: +82-2-6945-2120, Email: jhjang@moasoftware.co.kr

Ⅰ. 서 론

최근 각 산업분야에서 무인비행체(소형 드론)에 대한 활용이 많아지면서, 이에 대한 관련 기술과 개발 방안이 다각도로 연구되고 있다. 각 분야에서 개발되고 있는 각종 드론에 대한 시험평가 기술 및 방안으로, 일반적인 접근 방법인 MOC(Means of Compliance, 설계 적합성, 제작 합치성) 기준을 적용하고 있으나, 드론에 탑재되는 소프트웨어에 대한 시험 평가 기준으로 적용하는데는 한계가 있다. 드론에 탑재되는 소프트웨어의 역할이 더욱 중요시됨에 따라 제품의 안전성 확보를 위해서는 국제 수준의 소프트웨어 규격을 적용하는 개발 방안이 필요하다. 각 산업에서 요구하는 임무(Mission)에 따라 활용성이 점점 더 높아지고 있는데, 철도 시설물 점검, 하천 조사, 산불 대응, 다중이용시설 사고예방, 우편배송, 해안쓰레기 현장정보수집, 국토 조사 및 지적재조사, 도서산간지역 방범순찰 등 공공 임무뿐만 아니라 최근 세계적으로 유행하고 있는 코로나-19 방역임무에도 활용되고 있다. 또한 중량 200Kg 이상의 대형 비행체를 교통 및 화물 운송수단으로 활용하는 상용화 체계를 위한 도심항공교통(UAM, Urban Air Mobility)이 법적 체계, 인프라, 제도 등 많은 과제를 해결하면서 가까운 미래에 실현될 것으로 전망하고 있다. 이러한 무인비행체를 항공 교통, 물류 및 각종 임무 수단으로 활용하기 위한 기술 발전에서 가장 중요한 점은 안전성(Safety) 확보이다.

전세계 민간 항공기의 안전 운항에 대하여는 미국연방항공국 (FAA, Federal Aviation Administration)에서 각종 규제와 관리 및 승인이 이루어지고 있다. FAA에서 발간된 규격 중에서 항공기 안전을 위한 소프트웨어 개발 절차인 RTCA/DO-178C가 그 중 하나다[1]. DO-178C에서는 항공용 소프트웨어를 안전성 등급으로 분류하고 각 등급에 따라 달성해야 하는 목적(Objective)을 차등적으로 요구하고 있다. 사람을 태우지 않는 소형 무인비행체에 대한 개발 기술로 대형 비행체를 개발하면 사람을 이동시키는 교통 수단 또는 화물 운송 수단으로 활용할 수 있게 되며, 최대이륙중량 25kg 이상인 경우는 비행안전성인증을 받아야만 한다[2].

무인비행체 시스템은 크게 비행체와 지상제어장치로 구성된다. 그림 1과 같이, 비행체에 탑재되는 소프트웨어(SW)는 비행제어 SW, 임무제어 SW, 통신 SW 등이며, 지상제어장치에 설치 운영되는 소프트웨어는 지상제어 SW과 통신 SW로 구성된다.

무인비행체 시스템에 탑재되는 소프트웨어에 대한 요구사항은 비행제어 SW, 임무제어 SW, 지상제어 SW의 소프트웨어에 각각 요구되는 기능 요구사항과 비행체와 지상제어장치 간의 무선통신으로 수행되는 통신 인터페이스 요구사항 및 비행체 내부에서의 비행제어 SW와 임무제어 SW 간의 인터페이스 요구사항으로 구분된다. 비행제어 SW와 지상제어 SW에 대한 소프트웨어 요구사항은 정형화된 수준의 정의되어 있지만, 임무제어 SW에 대한 요구사항은 각 산업에서 요구하는 다양한 임무를 충족시키기 위하여 비정형화 되어 있다.

본 연구에서는 비정형화되어 있는 임무제어 SW를 제외한 비행제어 SW, 통신 SW 및 지상제어 SW에 대하여 요구되는 기능을 정의하고, 무인비행체 시스템 관점에서의 안전성 평가를 수행한다. 다만 안전성 평가 시 임무제어 SW가 영향 분석 대상으로 포함될 수 있다. 시스템 안전성 평가의 결과에 따라 무인비행체 시스템의 각각 SW의 기능에 대하여 안전성 등급을 결정하고, 지상제어장치의 지상제어 SW에 대한 소프트웨어 개발 방안을 제시하고자 한다.

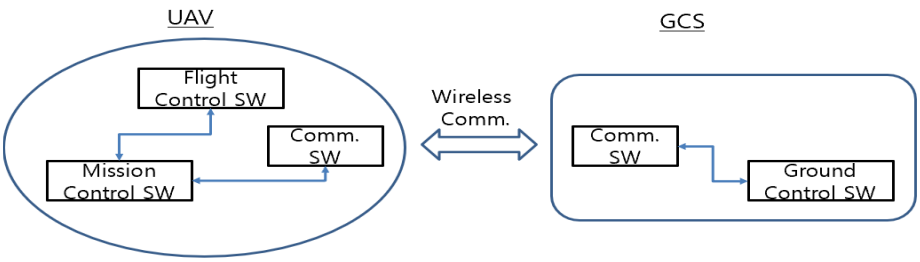

그림 1. UAV 시스템 구성도
Fig. 1. Structure of UAV system

무인비행체 시스템에 대한 시스템 안전성 평가(SSA) 절차는 FAA에서 제시하고 있는 ARP 4561에 따라 수행한다[3]. 무인비행체 시스템의 지상통제장치(GCS)에 탑재되는 지상제어 SW에 대한 개발 절차 방안에는 항공기 SW 개발 절차인 DO-178C와 항공 관제 시스템에 대한 소프트웨어 절차인 DO-278A를 적용한다[1][4].

II. 무인비행체 시스템에 대한 시스템 안전성 평가(SSA)

2.1 시스템 안전성 평가(SSA) 절차

항공기 시스템 개발과 관련된 전체 규격 간의 관계는 그림 2와 같다. 시스템 안전성 평가와 관련되어 시스템 개발, 하드웨어 개발 및 소프트웨어 개발 규격 등과의 연관성을 보여주고 있다. 시스템 수준에 적용되는 규격으로는 ARP 4761, ARP 4754A 등이 있으며, HW와 SW를 개발하고 통합하는데 관련된 규격으로는 DO-254, DO178C, DO-278A 등이 있다[1][3]-[6].

ARP 4761은 민수 항공기 감항 인증(Airworthiness certification)을 받기 위해 고려해야 하는 요건과 안전성 평가 절차(Safety assessment process)를 제공하고 있다[3]. 안전성 평가 절차는 그림 3과 같다.

항공기 수준의 FHA(Functional Hazard Analysis), PASA(Preliminary Aircraft Safety Assessment)에서는 항공기 수준의 기능 요구사항으로부터 안전성 요구사항을 도출하기 위하여 기능 고장 조건(Functional failure conditions)을 분석하고 영향 평가를 수행한다. 시스템 수준의 FHA 에서는 항공기 수준의 기능 요구사항으로부터 시스템 수준의 안전성 요구사항을 도출하기 위하여 기능 고장 조건을 분석하고 영향 평가를 수행한다. PSSA에서는 FHA에서 식별한 안전 목표(Safety objectives)를 충족할 수 있는 구조적 안전성 요구사항(Architectural safety requirements)과 HW/SW 요구사항을 도출한다. SSA에서는 안전 목표가 달성되고 HW/SW 요구사항이 구현되었는지를 평가한다.

2.2 무인비행체 시스템의 안전성 평가(SSA) 결과

무인비행체 시스템에 대한 SSA는 TxDOT Flight Service의 UAS Flight Operations and User's Manual에서 제시한 무인비행체에 대한 운용 요구사항은 참조하여 수행하였으며, 그 결과를 요약하면 표 1과 같다[7].

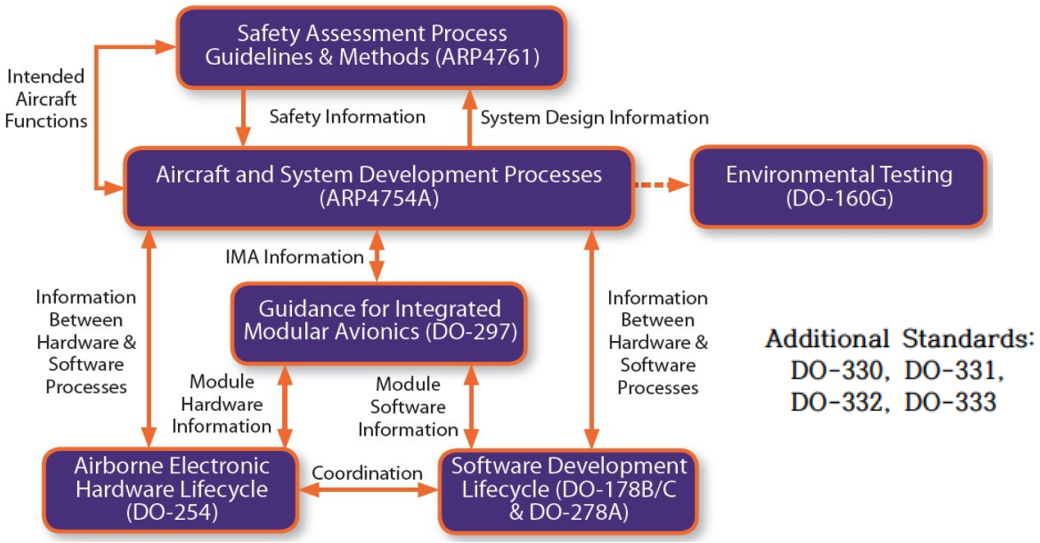

그림 2. 시스템 개발 규격 간의 관계
Fig. 2. Relationship of system development standards

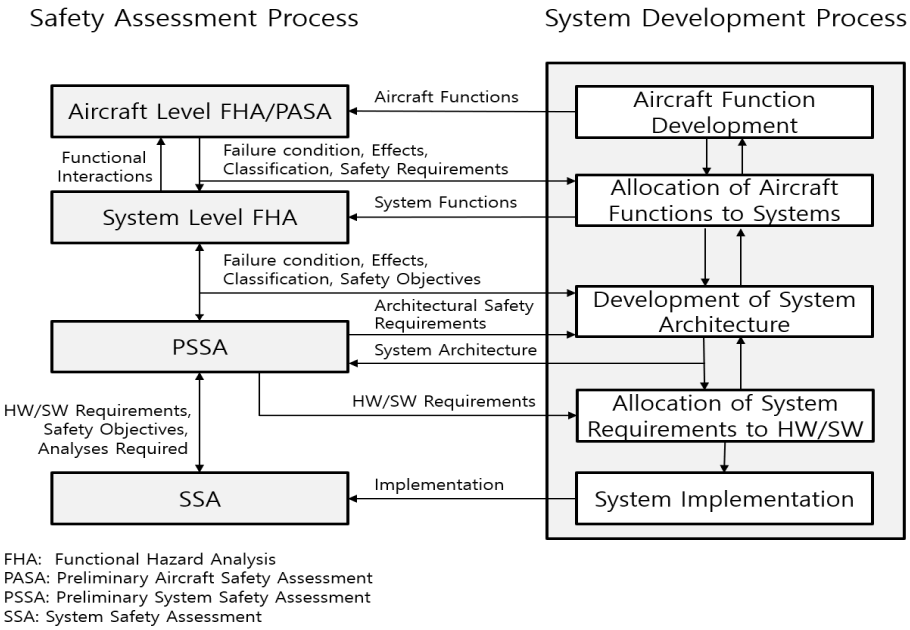

그림 3. SSA 절차
Fig. 3. SSA procedure

표 1. UAV 운영 요구사항과 SSA 결과 요약
Table 1. UAV operation requirements and SSA results summary

UAV operation requirements (Section in [7])	Failure effect	AL
2. Ground operations		
2.1. Flight crew requirements	No function of GCS	6
2.1.1. Remote pilot in command	No function of GCS	6
2.1.2. Visual Observer(VO)	No function of GCS	6
2.1.3. Secondary Remote Pilot in Command(SRPIC)	No function of GCS	6
2.1.4. Additional Visual Observer (AVO)	No function of GCS	6
2.1.5. Recurrent training	No function of GCS	6
2.2. Project Risk Assessment (PRA)	No function of GCS	6
2.3. Flight planning	Loss of UAS	2
2.3.1. Flight planning general rules	Loss of UAS	2
2.3.2. Flight plan	Loss of UAS	2
2.3.3. Traffic control plan	Loss of UAS	2
2.4. Health and safety plan	Serious injury of crew	2
2.5. In-flight emergency plan	Loss of UAS	1
2.5.1. Total loss of aircraft power	Loss of UAS	1
2.5.2. Partial loss of aircraft power	Higher Increase in crew workload	2
2.5.3. Airspace encroachment	Higher Increase in crew workload	2
2.5.4. Loss of aircraft control	Loss of UAS	1
2.5.5. Erratic aircraft behavior	Higher Increase in crew workload	2
2.5.6. Aircraft fly-away	Loss of UAS	1
2.5.7. Bird strikes	Loss of UAS	1
2.5.8. Fixed object strikes	Loss of UAS	1
2.5.9. Interference with flight crew	Significantly Increase in crew workload	3
2.5.10. Nearby emergency operations	Significantly Increase in crew workload	3
2.6. Downed Aircraft Recovery Plan(DARP)	No safety	6
2.6.1. DARP general rules	No safety	6
2.6.2. The DARP procedures	No safety	6
2.7. Accident reporting	No function of GCS	6
2.7.1. TxDOT reporting requirements	No function of GCS	6
2.7.2. FAA notification requirements	No function of GCS	6
2.7.3. NTSB notification requirements	No function of GCS	6
2.8. Maintenance	Slightly increase in crew workload	5
2.9. Aircraft registration number	No function of GCS	6
2.10. Logs and records	Slightly increase in crew workload	5
2.10.1. Pilot log	Slightly increase in crew workload	5
2.10.2. Aircraft maintenance log	Slightly increase in crew workload	5
2.10.3. Record retention	Slightly increase in crew workload	5

각각의 무인비행체 운용 요구사항에 대하여 고장 영향을 분석하고 DO-278A에서 정의한 안전성 수준(AL: Assurance Level)을 다음과 같이 평가하였다.

AL-1: Loss of UAS(무인비행체 추락)

AL-2: Higher Increase in crew workload or serious injury of crew(파일럿의 업무 부담 매우 증가)

AL-3: Significantly Increase in crew workload(파일럿의 업무 부담 발생)

AL-4: Not Available 적용사항 없음)

AL-5: Slightly increase in crew workload(파일럿의 업무 부담 약간 발생)

AL-6: No safety or no function of GCS(영향 없음)

2.3 DO-178C와 DO-278A 비교

표 2. DO-178C와 DO-278A 비교
Table 2. Comparison with DO-178C and DO-278A

Item	DO-178C	DO-278A	Remark
Scope	Aircraft	Ground system	
Safety level	DAL-A, B, C, D, E	AL-1,2,3,4,5,6	A : AL-1, B : AL-2, C : AL-3, D : AL-5, E : AL-6 AL-4: No mapping
Objectives by level	71-69-62-26-0	71-69-62-(46)-26-0	
Outputs	22	22	Different names of two outputs PSAC : PSAA PDIF : ADIF
SW process	Planning, development (Requirements, Design, Coding, Integration), Integral (Verification, CM, QA, Certification)	Planning, development (Requirements, Design, Coding, Integration), Integral (Verification, CM, QA, Approval)	Difference of certification and approval

DAL: Development Assurance Level
AL: Assurance Level
PSAC: Plan of Software Aspect for Certification
PSAA: Plan of Software Aspect for Approval
PDIF: Parameter Data Item File
ADIF: Adaptation Data Item File
CM: Configuration management
QA: Quality Assurance

본 연구에서는 무인비행체 시스템의 지상통제장치 (GCS)에 탑재되는 소프트웨어에 대한 개발 절차는 FAA의 감항인증 기준인 DO-178C와 DO-278A를 고려한다. DO-178C는 운항하는 비행체에 탑재되는 소프트웨어에 대한 개발 절차이며, DO-278A는 비행체를 지상에서 관제 및 통제하는 시스템에 대한 소프트웨어 개발 절차이다. DO-178C와 DO-278A에서의 소프트웨어 개발 절차를 비교하면 표 2와 같다.

무인비행체 시스템의 지상통제장치(GCS)에 탑재되는 소프트웨어에 대한 개발 절차로 GCS가 지상통제장치의 소프트웨어이므로 지상 관제 시스템에 대한 감항인증 규격인 DO-278A를 적용하는 것이 당연하다고 판단할 수 있으나, 비행체를 직접 제어하는 기능을 수행하는 GCS의 일부 모듈 또는 컴포넌트는 DO-178C를 적용하여야 한다.

- 무인비행체의 비행에 대한 직접적인 제어 기능
- 무인비행체 내의 임무 수행에 대한 제어 기능
- 무인비행체의 고장진단 및 고장 발생에 대한 즉시적인 대처 기능
- 무인비행체와의 직접적인 실시간 통신 기능

2.4 GCS 소프트웨어 모듈 구성 및 안전성 수준

무인비행체 시스템의 지상통제장치 (GCS) 중에서는 QGroundControl(QGC)를 전세계적으로 가장 많이 사용하고 있다[8]. 본 연구에서는 QGC의 최상위 메뉴 수준의 GCS의 기능을 기준으로 무인비행체 개발자가 GCS를 개발한다고 할 경우를 가정하여 GCS 소프트웨어 개발 절차 방안을 제시한다.

QGC의 최상위 메뉴 수준에서 제공되는 5개의 GCS 기능은 5개 기능은 다음과 같다.

- Setting : 기본 구성 설정
- Setup : 옵션 설정
- Plan : 비행 계획
- Fly : 비행 통제
- Analyze : 비행 로그, 임무 결과 관리

GCS의 5개 기능을 SW모듈로 구성하고, 앞서 2.2절에서 수행한 SSA 결과를 표 3과 같이 각 SW 모듈에 할당하여 AL을 결정하였다.

표 3. QGroundControl SW 모듈별 AL 할당
Table 3. AL allocations for QGroundControl SW modules

SW module	Module description	AL
Setting	Configure the QGroundControl application. - General - Comm links - Office maps - MAVLink - Console	3
Setup	Configure and tune your vehicle. - Firmware, Airframe, Radio, Sensors, Flight Modes, Power, Motors, Safety, Tuning, Camera, Parameters	2
Plan	Create autonomous missions. - Map - Plan toolbar - Plan tool - Mission command list/overlay	2
Fly	Monitor your vehicle(s) while flying, including streaming video. - Run an automated pre-flight checklist. Control missions: start, continue, pause, and resume. - Guide the vehicle to arm/disarm/emergency stop, takeoff/land, change altitude, go to or orbit a particular location, and return/RTL. - Switch a map view/a video view - Display information.	1
Analyze	Download logs, geotag images from a survey mission, access the MAVLink console. - Download logs - GeoTag images(PX4) - MAVLink console(PX4) - MAVLink inspector	5

2.5 GCS 소프트웨어 개발 방안

GCS의 5개 모듈에 할당된 AL에 따라 DO-178C와 DO-278A에서 요구하는 소프트웨어 개발 절차를 적용하여 GCS SW 개발 방안을 제시한다.

SW 모듈별로 소프트웨어 안전성 등급이 다를 경우에는 각각의 SW 모듈에 적용할 SW 개발 활동이 달라진다. 앞서 2.3절에서 분석한 결과와 같이, DO-178C와 DO-278A의 SW 개발 단계 (SW Process)는 동일하지만, 안전성 수준(SW Level: DAL, AL)과 SW 산출물(Outputs)에서 약간의 차이를 보이고 있다.

본 논문에서 제시하는, GCS의 5개의 SW 모듈에 대한 SW 개발 절차 방안을 요약하면 표 4와 같다.

표 4. GCS SW 모듈별 SW 개발 절차 방안
Table 4. SW development procedure for GCS SW module

SW module	Standards	DAL/AL	Partition	# of objectives
Setting	DO-278A	AL-3	Partition C	62
Setup	DO-278A	AL-2	Partition B	69
Plan	DO-278A	AL-2	Partition B	69
Fly	DO-178C	DAL-A	Partition A	71
Analyze	DO-278A	AL-5	Partition D	26

5가지 SW 모듈에 대한 개발 절차는 각각의 SW 모듈에 대하여 안전성 수준(SW Level: DAL, AL)이 정의되면, DO-178C와 DO-278A에서 요구하고 있는 각 SW Level에 해당하는 SW 개발 절차 및 활동을 적용하면 된다. 예를 들어, SW Module Setting의 경우 AL-3, 62개 Objective를 달성하기 위한 SW 개발 활동을 수행해야 한다. DAL-A, AL-1 수준의 71개 Objective에 해당하는 SW 개발 활동과 비교해서 9개의 Objective를 달성하는데 필요한 SW 개발 활동을 수행하지 않게 된다. 최하위 SW Level(DAL-D, AL-5)에 대하여 상위 SW Level에 추가되는 주요 활동은 다음과 같다.

- DAL-D, AL-5: SW 요구사항 추적 및 검증, Partitioning 구조 및 검증
- AL-4: SW 시험절차 및 결과 검토, Data Coupling/Control Coupling(DC/CC) 달성
- DAL-C, AL-3: SW 설계 추적 및 검증, 코드 검증, Statement Coverage(SC) 달성
- DAL-B, AL-4: Decision Coverage(DC) 달성
- DAL-A, AL-4: Modified Condition/Decision Coverage(MC/DC) 달성, 컴파일러가 추가한 코드 검증

SW 모듈 Fly는 무인비행체를 직접 제어하기 때문에 실질적으로 비행체에 탑재된 SW와 동일한 안전성 수준을 갖게 되므로, DO-178C를 적용한다. 또한 DO-178C와 DO-278A에서 SW Level이 다른 경우에는 기본적으로 Partitioning 구조를 가져야 한다.

Partitioning은 낮은 SW Level의 SW 모듈이 높은 SW Level 모듈에 미치는 영향을 최소화하기 위함이며, 동일한 SW Level을 가지는 SW 모듈일지라도 상호간의 인터페이스를 최소화함으로써 각각의 SW 모듈이 SW level에 해당하는 안전성을 유지하게 되기 때문이다.

GCS의 5개 모듈에 대한 전체적인 구성도는 그림 4와 같다. GCS 시스템은 서버장비에 어플리케이션을 실행하게 되는데, SW 모듈 Fly는 서버 장비를 분리해서 Partitioning을 확보하는 것도 한가지 방안이다. 일반적인 서버 장비에서 실행되는 OS(예를 들어, Linux)는 DO-178C 인증(Certification)을 받아야 한다.

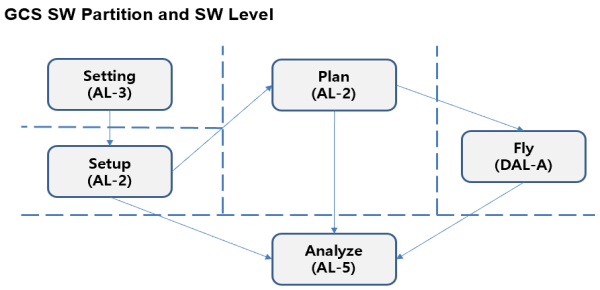

그림 4. GCS SW 구조도
Fig. 4. Structure of GCS SW

서버 장비에 탑재된 OS가 DO-178C DAL-A를 인증받지 못하면 SW 모듈 Fly을 DO-178C DAL-A 수준으로 개발한다 하더라도 결국 서버장비까지 포함한 시스템 수준의 DAL-A를 달성할 수 없다.

SW 개발 단계는 5 단계로 정의한다.

- [P] Planning: SW 개발 계획 수립
- [R] Requirements: SW 요구사항 정의
- [D] Design: SW 설계
- [C] Coding: 소스코드 구현
- [T] Test: SW 시험

각 SW 모듈에 적용되는 SW 개발 단계에 대한 DO-178C/DO-278A와의 적합성(Compliance) 매핑 및 각 단계별산출물은 표 5와 같다.

DO-178C와 DO-278A에서 SW 개발 단계별 활동과 산출물 이외에 전체 단계에 공통으로 수행하는 활동에는 검증(Verification), 형상관리(Configuration management), 품질보증(Quality assurance), 인증(Certification)이 있다.

표 5. GCS SW 개발 단계 및 산출물
Table 5. GCS SW development phases and outputs

SW development phase	DO-178C/ DO-278A	Outputs	Ref.	Remarks
Planning [P]	Planning	SDP	11.2	
		SVP	11.3	
		SCMP	11.4	
		SQAP	11.5	
		SDevStd	11.6	SRStd
			11.7	SDStd
			11.8	SCStd
Requirements [R]	Requirements	SRS	11.9	
Design[D]	Design	SDD	11.10	
Coding[C]	Coding	Source code	11.11	
Test[T]	Integration/ Verification	EOC	11.12	
		ADIF	11.22	PDIF
		STCP	11.13	SVCP
		STR	11.14	SVR

SDP: SW Development Plan
SVP: SW Verification Plan
SCMP: SW Configuration Management Plan
SQAP: SW Quality Assurance Plan
SDevStd: SW Development Standards
SRStd: SW Requirements Standards
SDStd: SW Design Standards
SCStd: SW Code Standards
SRS: SW Requirements Specification
SDD: SW Design Description
EOC: Executable Object Code
ADIF: Adaptation Data Item File (in DO-278A)
PDIF: Parameter Data Item File (in DO-178C)
STCP: SW Test Cases and Procedures
SVCP: SW Verification Cases and Procedures
STR: SW Test Results
SVR: SW Verification Results

- [VV] Review: SW 검토 활동
- [CM] Configuration Management: 형상관리 활동
- [QA] Quality Assurance: 품질보증 활동
- [CC] Certification: 인증 활동

이러한 활동은 모든 SW 개발 시 적용되어야 한다. DO-178C/DO-278A에서 4개의 공통 활동에 대한 산출물은 표 6과 같이 정의한다.

SW 개발 단계와 공통 활동을 도식화하면 그림 5와 같다.

표 6. SW 개발 공통 활동 및 산출물
Table 6. SW Development integral processes and outputs

SW process	DO-178C/ DO-278A	Outputs	Ref.	Remarks
Review [VV]	Verification	SVR	11.14	
		RTM	11.21	TD
		PR	11.17	
Configuration Management [CM]	CM	SCI	11.15	SECI
			11.16	SCI
		SCMR	11.18	
Quality Assurance[QA]	QA	SQAR	11.19	
Certification [CC]	Certification	PSAC	11.1	PSAA
		SAS	11.20	

RTM: Requirements Traceability Matrix
TD: Trace Data
PR: Problem Report
SCI: SW Configuration Index
SECI: SW Life Cycle Environment Configuration Index
SCMR: SW Configuration Management Records
SQAR: SW Quality Assurance Records
PSAC: Plan for SW Aspect of Certification (in DO-178C)
PSAA: Plan for SW Aspect of Assurance (in DO-278A)
SAS: SW Accomplishment Summary

표 5와 표 6에 정의된 SW 개발 단계 및 공통 활동의 주요 산출물은 다음과 같다.

- SDP: 소프트웨어 개발 계획서
- SVP: 소프트웨어 검증 계획서
- SCMP: 소프트웨어 형상관리 계획서
- SQAP: 소프트웨어 품질보증 계획서
- SDevStd: 소프트웨어 개발 표준서
- SRStd: 소프트웨어 요구사항 표준서
- SDStd: 소프트웨어 설계표준서
- SCStd: 소프트웨어 코드 표준서
- SRS: 소프트웨어 요구사항 명세서
- SDD: 소프트웨어 설계 기술서
- EOC: (소프트웨어) 실행코드
- ADIF: 적용 데이터 항목 파일
- PDIF: 파라미터 데이터 항목 파일
- STCP: 소프트웨어 시험 항목 및 절차서
- SVCP: 소프트웨어 검증 항목 및 절차서
- STR: 소프트웨어 시험 결과서
- SVR: 소프트웨어 검증 결과서
- RTM: (소프트웨어) 요구사항 추적표
- TD: (소프트웨어 요구사항) 추적 데이터
- PR: 문제 보고서
- SCI: 소프트웨어 형상 목록
- SECI: 소프트웨어 환경 형상 목록
- SCMR: 소프트웨어 형상관리 기록
- SQAR: 소프트웨어 품질보증 기록
- PSAC: 소프트웨어 인증 계획서
- PSAA: 소프트웨어 보증 계획서
- SAS: 소프트웨어 완료 요약서

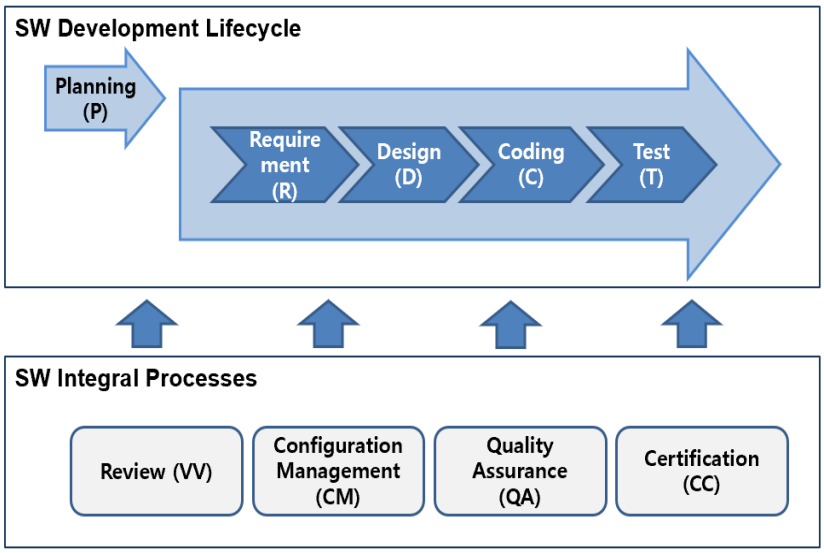

그림 5. SW 개발 단계 및 공통 활동
Fig. 5. SW development life cycle and integral processes

본 연구의 결과에 대한 우수성을 요약하면 다음과 같다.

- 무인이동체 소프트웨어 개발 시 안전성 수준(SW level)을 정의하기 위해서 무인이동체 시스템에 대한 안전성 평가 절차(SSA)를 적용함
- 무인이동체 소프트웨어 개발에 항공 분야 국제 기준의 소프트웨어 개발 규격(DO-178C, DO-278A)을 적용함
- 무인이동체 소프트웨어 모듈의 특성에 따라 항공기 탑재용(DO-178C), 항공 관제용(DO-278A)으로 구분하여 선택적으로 적용하는 방안을 제시함
- DO-178C, DO-278A를 통합하여 적용하는 SW 개발 절차 및 방안을 제시하
- SW 개발자들이 쉽게 이해하고 활용할 수 있는 SW 개발 단계 및 산출물을 제시함
- 제안된 SW 개발 절차 및 방안이 DO-178C, DO-278A에 적합(Compliance)한 근거를 제시함

III. 결 론

본 연구에서는 무인이동체 시스템의 지상장비에 탑재되는 GCS SW에 대한 개발 절차 방안을 연구하였다. 먼저, 항공 시스템의 전체적인 시스템 수준의 안전성 분석절차인 ARP 4761를 적용하여 시스템 안전성 평가(SSA)를 수행하고 지상통제장비(GCS)의 SW 수준의 안전성 수준(SW level)을 할당하였다. 항공용 SW와 지상관제시스템의 안전성을 보장하기 위한 SW 규격서인 DO-178C와 DO278A를 적용하여 SW를 개발하는 절차와 방안을 제시하였다.

본 논문에서 제시한 SW 개발 단계는 일반적인 SW 개발 생명 주기와 유사하지만 DO-178C와 DO278A에 적합하게 정의하였다. GCS SW 구성에서는 항공용 SW의 안전성을 보장하기 위해서는 GCS SW를 5개 모듈로 분할하여 각각에 대하여 안전성 수준(SW level)을 할당하고 파티션 하는 SW 구성도를 제시하였다. SW 개발 단계와 SW 공통 활동의 산출물도 DO-178C와 DO278A에 적합하게 정의하였다.

무인이동체는 향후 UAM 분야의 핵심 수단이며, 안전성이 보장되는 이동수단으로 개발되어야 한다. SSA, DO-178C, DO-278A 등 국제 항공분야의 안전성 인증 규격을 적용을 요구하게 되면, 본 연구에서 이러한 규격들이 요구하는 기준에 적합하게 제시한 SW에 대한 개발 절차 방안이 적용하면 된다.

공공 임무용 드론 등 무인이동체 시스템 개발에서 GCS SW를 오픈소스로 제공되는 소스를 활용하여 개발한다 하더라도 각 SW 모듈에 대한 안정성 수준을 정의하고 각 수준에 적합한 활동과 산출물을 작성함으로써 보다 안전한 SW를 개발할 수 있을 것이다.

후속 연구에서는 본 연구에서 제시한 GCS SW 개발절차와 방안을 이용하여 실제로 개발한 SW를 적용하여 실험과 검증을 하고자 한다. GCS를 개발할 경우에 각 SW 모듈에 대한 안전성 수준을 정의하고, 각 수준에 적합한 DO-178C와 DO-278A에서 요구하는 활동과 산출물을 적용한 후에, 본 연구 결과에서 제시하는 개발 방안을 적용한 결과와 비교분석함으로써 GCS SW 모듈의 특성에 적합하고 효율적으로 적용됨을 확인하고자 한다.

References

[1] DO-178C, Software Considerations in Airborne Systems and Equipment Certification, RTCA, 2011.

[2] https://www.safeflying.kr, Safety Certification of Light Aircraft and Ultra Light Flying System(KIAST). [accessed: Nov. 01, 2022]

[3] ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, SAE, 1996.

[4] DO-278A, Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems, RTCA, 2011.

[5] ARP 4754A, Guidelines for Development of Civil Aircraft and Systems, SAE, 2010.

[6] DO-254, Design Assurance Guidance for Airborne Electronic Hardware, RTCA, 2000.

[7] Unmanned Aircraft System (UAS) Flight Operations and User's Manual, TxDOT Flight Service, 2019.

[8] QGroundControl User's Manual, v4.2.3, //qgroundcontrol.com, 2017. [accessed: Nov. 01, 2022]

저자소개

장 정 훈 (Jeong-Hoon Jang)

2004년 2월 : 동국대학교 전산학과(학사)

2005년 9월 ~ 현재 : ㈜모아소프트 이사

관심분야 : 제어, 시스템, Software, Safety, DO-178C