한국항행학회논문지
Journal of Advanced Navigation Technology

항공 우주 해상

J. Adv. Navig. Technol. 24(3): 163-172, Jun. 2020

# 무인항공기용 비행자료 기록장치 소프트웨어 설계 및 검증 방안

# Software Design and Verification Method of Flight Data Recorder for Unmanned Aerial Vehicle

**양 서 희**
국방과학연구소

**Seo-hee Yang**
Agency for Defense Development, Daejeon, 34060, Korea

**[요 약]**

무인항공기 사고 발생 시 사후 조사를 위한 비행자료 기록장치는 항공기 추락에 따른 극한환경에 노출된 후 비행자료를 정상 복원할 수 있도록 EUROCAE(European Organization for Civil Aviation Equipment)의 ED-112 규격을 준수하여야 한다. ED-112 규격은 유인항공기를 포함한 모든 항공기의 일반적인 요구사항을 규정하고 있기 때문에 특정 플랫폼의 형상 및 운용개념에 따라 적합한 설계 요구사항을 선택적으로 적용하여야 하므로 소프트웨어에 대한 세부 요구사항 분석이 필수적이다. 본 논문에서는 무인항공기에 적합한 소프트웨어 요구사항을 분석하고 이를 고려한 비행자료 기록장치 소프트웨어의 설계 방안을 제안한다. 또한 구현된 소프트웨어가 모든 요구사항을 고려하여 설계되었는지 확인하기 위한 각 요구사항에 대한 소프트웨어 검증 방안을 제시한다.

**[Abstract]**

Flight data recorder (FDR) for accident investigation is required to comply with EUROCAE(ED-112) standard so that flight data can be restored when exposed to extreme conditions due to aircraft crash. Since the ED-112 standard defines the general requirements for all aircraft, it is essential to analyze detailed requirements for FDR software to apply appropriate requirements selectively according to the configuration and operation concept of a specific aircraft. In this paper, the software requirements applicable to unmanned aircraft will be analyzed and the FDR software design will be proposed. Also, a software verification method for each requirement will be presented to verify that the implemented software is designed to satisfy all requirements.

**Key word :** Flight data recorder(FDR), ED-112, Software design, Software verification, Recording algorithm.

**https://doi.org/10.12673/jant.2020.24.3.163**

This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-CommercialLicense(http://creativecommons.org/licenses/by-nc/3.0/) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

**Received** 27 April 2020; **Revised** 27 May 2020
**Accepted (Publication)** 22 June 2020 (30 June 2020)

***Corresponding Author; Seo-hee Yang**

**Tel:** +82-42-821-0964
**E-mail:** ysh@add.re.kr

## Ⅰ. 서 론

비행자료 기록장치는 항공기 운용 시 고도, 자세 및 속도 등 항공기 상태 정보를 기록하여 항공기 사고 발생 시 사후 조사를 가능하게 하는 장비이다. 비행자료 기록장치는 사고 발생 후 비행자료를 정상 복원할 수 있어야 하기 때문에, 타 항공전자장비 대비 가혹한 외부 환경에 대하여 더욱 강건한 설계가 필요하여 EUROCAE, ICAO (International Civil Aviation Organization), FAA(Federal Aviation Administration) TSO (Technical Standard Orders Authorization) 등의 규격을 준수하여야 한다 [1]. 국내 대부분의 무인항공기용 비행자료 기록장치에는 EUROCAE의 ED-112 규격이 요구되며, 이를 만족하기 위한 설계 및 입증이 필요하다 [2], [3]. 비행자료가 저장되는 핵심부품인 충돌 보호 메모리 모듈 (CPM; crash protected memory module)은 충격, 고온, 해수침수 등과 같은 극한환경에서의 시험을 통하여 강건성을 입증하여야 하며 CPM 내 플래시 메모리에 저장된 비행자료는 손실을 최소화하여 복원되어야 한다 [4], [5]. CPM에 기록되는 비행자료의 안정성 확보를 위하여 데이터 기록/삭제, 파일 복원, 비행자료 저장 범위 등에 대한 소프트웨어 요구사항 분석이 필요하며 이를 만족하기 위한 비행자료 기록장치 소프트웨어 설계 및 검증이 필요하다 [6].

EUROCAE의 ED-112 규격은 모든 유형의 항공기에 탑재되는 비행자료 기록장치의 일반적인 요구사항을 정의하고 있기 때문에 플랫폼에 따라 적합한 요구사항을 식별하여야 한다. 또한 ED-112 요구사항뿐만 아니라 적용하고자 하는 항공기의 운용개념에 따라 필요한 세부 요구사항이 달라질 수 있기 때문에 소프트웨어 요구사항에 대한 상세한 분석이 필수적이다. 본 논문에서는 ED-112 규격 요구사항 중 무인항공기 운용개념에 따른 요구사항을 분석하고 이를 만족하기 위한 비행자료 기록장치 소프트웨어 설계 및 검증 방안에 대하여 논하고자 한다.

## Ⅱ. 비행자료 기록장치 소프트웨어 설계

### 2-1 비행자료 기록장치 소프트웨어 요구사항 수립

ED-112 규격은 유인항공기를 포함한 모든 유형의 항공기에 탑재되는 기록장치의 일반적인 요구사항을 정의하고 있기 때문에 적용하고자 하는 플랫폼에 적합한 요구사항을 수립하여야 한다. ED-112 규격에서 식별된 무인항공기를 위한 비행자료 기록장치 소프트웨어 요구사항은 표 1과 같으며, 고장 모니터링, 데이터 간 동기화, 기록매체 분리 기록 등 12개 항목에 대한

**표 1.** 무인항공기 비행자료 기록장치를 위한 ED-112 요구사항
**Table 1.** Requirements of ED-112 for UAV flight data recorder

| ED-112 Requirements | Requirements for UAV flight data recorder |
|---|---|
| 2-1.4.2 Monitoring of proper operation | - Pre-flight checking and in-flight monitoring<br>a. Loss of system electrical power<br>b. Failure of the acquisition and processing equipment<br>c. Failure of the recording medium<br>d. Failure of the recorder to store the information in the recording medium<br>e. The absence of the recorder and/or the acquisition equipment |
| 2-1.5 Start and termination of recording | - Recording start : prior to the aircraft moving under its own power<br>- Recording termination : the aircraft is no longer capable of moving under its own power |
| 2-1.11 Recorder synchronisation | - Synchronised in time with any other required recording to within 1 second. |
| 2-5.3.8 Inadvertent turnoff | - Protection shall be provided to prevent the inadvertent turnoff of the equipment. |
| 2-5.3.11 Recorder operation | - In order to ensure reliable operation, particularly under the abnormal conditions, the means provided to automatically stop the recorder should rely on more than one device. |
| 4-1.2 Funtional segregation | - Where two or more types of flight recording functions are combined, the recorder shall be designed that a failure of one function does not impair the operation of any of the others. |
| 4-1.2.1 Recording medium segregation and partitioning | - The recording mechanism shall be designed such that loss of data from multiple recording functions cannot result from the loss of a single memory device. |
| I-1.3.2 Classes of voice recorder<br>II-1.3.2 Classes of flight data recorder | - Voice recorder : data recorded during the last 2 hours of its operation<br>- Flight data recorder : data recorded during the last 25 hours of its operation |
| II-2.1.4 Recording technology | - The method of retrieval shall not alter, or re-write, the data in the recording medium.<br>- Non-availability of a single memory device does not lead to the loss of more than 16 seconds of contiguous data. |
| II-2.1.7 Erasure of recorded data | - Except for the overwriting of the oldest data by new information, no means for the erasure of the record shall be provided in the recorder. |
| II-3.2.1 Start-up and effects of power interruptions | - Recording within 10 seconds, and built in test shall be completed within 60 seconds<br>- At normal power level, interruptions with a duration of 200 millisecond or less shall have no effect on the recorder. |
| II-3.2.2 Recording delay | - The delay between data acquisition and recording in the recording medium shall not exceed 0.5 seconds. |

설계가 요구된다. 특히 의도치 않은 전원 차단, 메모리 손상 등의 비정상 상황을 고려한 설계는 항공기 사고 시점의 하드웨어 손상으로 인한 비행자료 손실을 최소화하기 위하여 반드시 요구되는 항목이다.

ED-112 규격뿐만 아니라 적용하고자 하는 항공기의 운용개념에 따라 필요한 세부 요구사항이 달라지기 때문에 이에 대한 분석이 필요하다. ED-112 규격의 2-5.3.11 Recorder operation 요구사항은 항공기 추락 시 전원이 완전히 차단되지 않았을 경우, 추락 이후의 무의미한 데이터가 이미 저장되어 있는 비행자료를 overwrite하는 상황을 방지하기 위한 요구항목이다. 일반적으로 충격 감지용 관성 스위치 등을 사용하여 일정 가속도 이상의 충격 발생 시 자동으로 전원을 차단하도록 하지만 별도의 장치 추가로 인한 중량 및 비용이 증가하는 단점이 있어 이를 적용하지 않는 무인항공기는 비행자료 기록장치에 저장되는 데이터만으로 항공기 추락을 판단하여야 한다. 비행자료 기록장치에 기록되는 센서 정보 중 착륙장치의 WOW(weight-on-wheel) 신호, GPS의 고도 및 속도 정보, 대기센서(ADS; air data senser)의 속도 정보를 사용하여 추락을 판단하도록 세부 요구사항을 도출하였다. 이와 같이 항공기의 형상 또는 운용개념에 따라 필요한 세부 요구사항이 달라지기 때문에 소프트웨어 설계 전 상세한 요구사항 분석이 필수적이다.

### 2-2 비행자료 기록장치 소프트웨어 설계 방안

ED-112 및 자체 세부 요구사항을 만족하기 위한 비행자료 기록장치 소프트웨어는 정상 기록, 기록 중단, 데이터 복원 등 여러 기능을 포함하도록 그림 1과 같이 7개의 모드로 구성된다. ED-112의 2-1.4.2 Monitoring of proper operation, 2-1.5 Start and termination of recording 및 II-3.2.1 Start-up and effects of power interruptions 요구사항을 만족하기 위하여 비행자료 기록장치에 전원 인가 시 전원 초기화 모드로 진입하여 10초 이내에 장비 초기화 및 PBIT(power-up built-in test)을 수행하여 고장 항목을 모니터링한다. PBIT 완료 후 점검용 디스크리트 신호를 확인하여 기록 모드 또는 정비 모드로 진입하고 기록 모드로 진입 시 전원 인가 10초 이내에 MIL-STD-1553B 통신으로 수신되는 비행 데이터 기록을 시작하며 정비 모드로 진입 시 점검장비와 연동하여 점검을 수행한다. 기록 모드에서 정상 기록 중 일시적인 통신 오류로 인한 비행자료 미수신 시 기록 중지 모드로 진입하여 데이터가 정상 수신될 때까지 기다리며, 데이터 정상 수신 시 다시 기록 모드로 진입하여 정상 기록을 수행한다. 무인항공기 추락과 같은 사고 발생 시 전원이 완전하게 차단되지 않아 기록 모드를 유지할 경우 기록된 비행자료가 overwrite될 수 있기 때문에, 항공기 상태에 따른 기록 중단 조건 충족 시 기록 중단 모드로 진입하여 기록을 완전 중단한다. 또한 지상시험 및 점검 시 비행자료 기록장치의 세부 점검을 수행하기 위한 IBIT(initiated built-in test)을 수행할 수 있으며, 비행조종컴퓨터 및 점검장비로부터 IBIT 명령 수신 시 시험 모드로 진입하여 IBIT 수행 후 결과를 송신한다. ED-112의 2-5.3.8

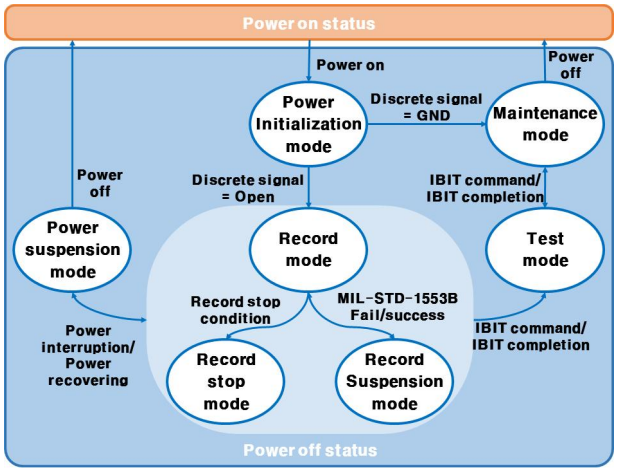


**그림 1.** 비행자료 기록장치 상태 및 모드
**Fig. 1.** Status and mode of flight data recorder

Inadvertent turnoff 요구사항을 만족하기 위하여 전원 차단 시 250 ms 이상 전원을 유지하도록 하드웨어 설계(hold-up 모듈)를 반영하였으므로, 전원 차단 감지 시 전원 중단 모드에 진입하여 200 ms동안 비행자료 정상 저장 수행 후 전원이 복구되지 않으면 마지막으로 수신된 비행자료 및 메모리 주소 값을 저장하고 기록을 중단한다.

이와 같이 비행자료 기록장치 소프트웨어의 모든 요구사항을 만족하기 위하여 각 모드별 세부 설계가 필요하며, 이 중 비행자료 기록을 위하여 가장 핵심이 되는 기록 모드의 비행자료 기록 알고리즘과 무인항공기 추락과 같은 사고 상태를 판단하여 기록을 중단하는 기능에 대한 상세 설계 방안을 제안한다.

#### 1) 비행자료 기록 알고리즘

비행자료 기록장치에 저장되는 비행자료는 음성통신중계 시스템의 음성 데이터와 조종면, 엔진 등과 같은 항공기 상태를 판단하기 위한 비행 데이터로 분류된다. 음성 데이터는 ED-112 규격의 I-1.3.2 Classes of voice recorder 요구사항에 따라 2시간 이상의 데이터를 저장하여야 하므로 용량이 크지 않아 메모리

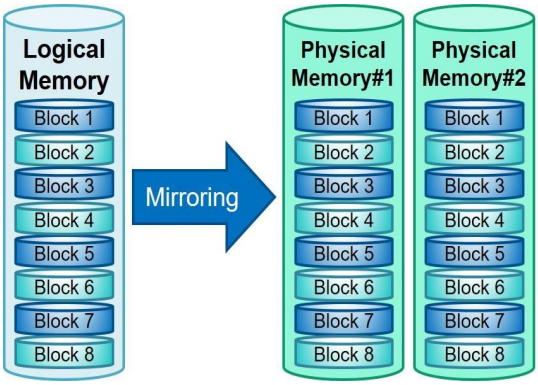


**그림 2.** 메모리 미러링 기법 개념도
**Fig. 2.** Concept of memory mirroring

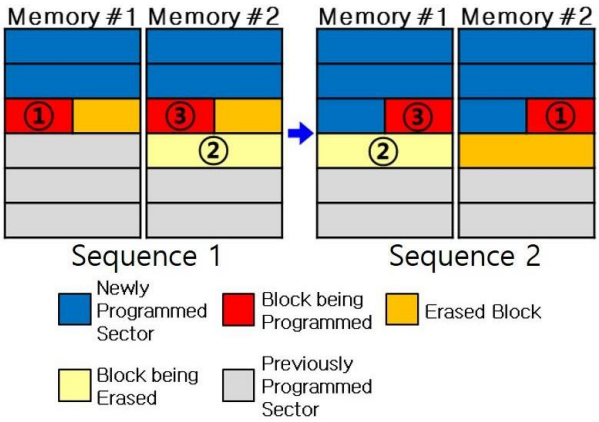


**그림 3.** 저용량 음성 데이터를 위한 기록 알고리즘
**Fig. 3.** Recording algorithm for low volume audio data

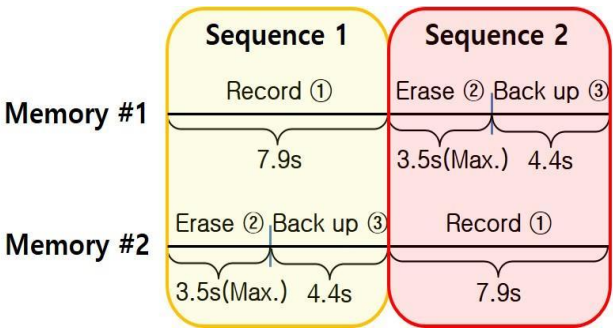


**그림 4.** 저용량 음성 데이터 기록 알고리즘 타이밍도
**Fig. 4.** Timing diagram for low volume audio data

미러링(memory mirroring) 기법을 적용할 수 있다. 메모리 미러링 기법은 그림 2와 같이 표현되며, 데이터 백업을 위한 메모리를 추가하여 두 개 이상의 메모리에 동시에 데이터를 저장하여 데이터 백업을 가능하게 하는 방법이다. ED-112 규격의 4-1.2.1 Recording medium segregation and partitioning 요구사항을 충족하기 위하여 하나의 메모리 고장 시에도 백업 메모리를 통한 완벽한 데이터 복원이 가능한 방법이지만 메모리를 추가하여야 한다는 단점이 있기 때문에 2시간 분량의 음성 데이터와 같은 저용량 데이터에만 제한적으로 적용 가능하다.

음성 데이터를 저장하기 위한 플래시 메모리는 이미 기록된 데이터가 있는 영역에 새로운 데이터를 쓸 경우 기존 데이터를 미리 삭제하여야 하며, 하나의 플래시 메모리에서는 기록과 삭제를 동시에 수행할 수 없다. 따라서 첫 번째 메모리에 수신된 데이터를 저장함과 동시에 두 번째 메모리의 백업하고자 하는 영역을 삭제 후 첫 번째 메모리에 저장된 데이터를 백업하여야 하며, 이를 고려한 저용량 음성 데이터 기록 알고리즘은 그림 3과 같다. 플래시 메모리 구성단위인 sector를 두 개의 logical block 으로 분리하여, memory #1의 logical block(①)에 데이터 기록 시 memory #2의 기록을 수행하고자 하는 sector(②) 데이터를 삭제하고 logical block 백업(③)을 수행한다(sequence 1). 이어서 sequence 2에서도 마찬가지로 memory #2의 logical block(①)에 데이터 기록 시 memory #1의 기록을 수행하고자 하는 sector(②) 데이터를 삭제하고 logical block 백업(③)을 수행한다. 그림 4는 sequence 1, 2 에 대한 기록 및 삭제 시 소요되는 시간을 나타낸다. memory #1에 기록을 수행하는 7.9초 동안 memory #2의 기록 예정 영역을 삭제(최대 3.5초)하고 백업 데이터를 기록(4.4초)한다.

비행 데이터는 ED-112 규격의 II-1.3.2 Classes of flight data recorder 요구사항에 따라 25시간 이상의 데이터를 저장하여야 하므로 용량이 매우 크기 때문에 그림 5와 같은 데이터 스트라이핑(data striping) 기법을 적용한다. 데이터 스트라이핑 기법은 그림 6과 같이 메모리 구성단위인 sector를 네 개의 logical block 단위로 분리하여, 하나의 logical block에 데이터 저장(①) 후 다음 logical block에 저장을 이어가지 않고 다음 메모리(memory #2)에 데이터를 저장(②)한다. ED-112의 II-2.1.4 Recording technology 요구사항을 만족하기 위하여 하나의 logical block에

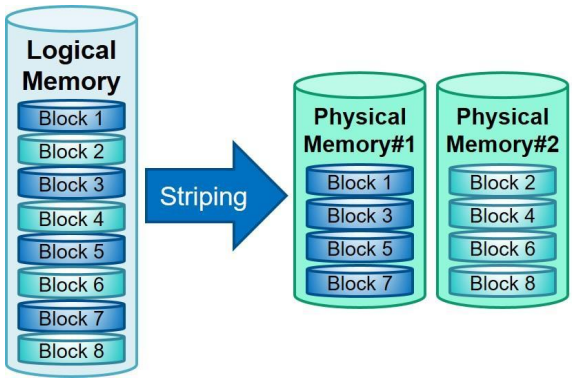


**그림 5.** 데이터 스트라이핑 기법 개념도
**Fig. 5.** Concept of Data Striping

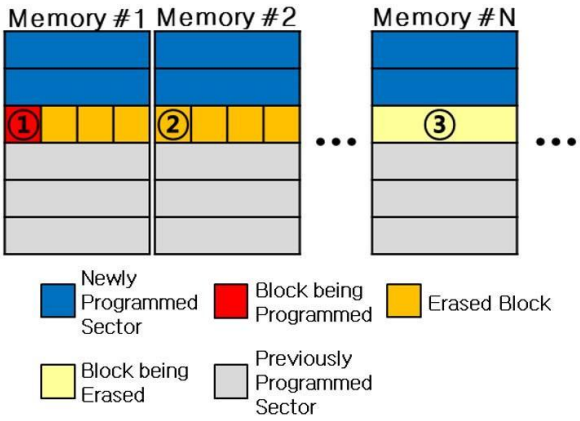


**그림 6.** 대용량 비행 데이터를 위한 기록 알고리즘
**Fig. 6.** Recording algorithm for large volume flight data

**그림 7.** 충격 감지를 위한 관성 스위치
**Fig. 7.** Inertial switch for shock detection

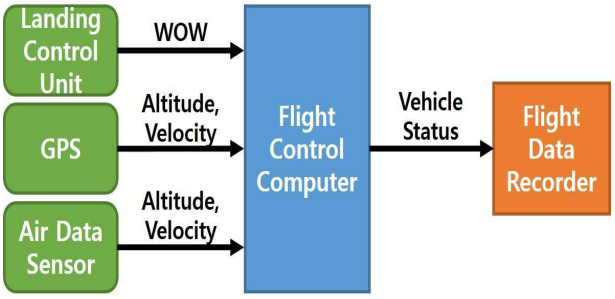


**그림 8.** 기록 중단 판단을 위한 비행자료
**Fig. 8.** Flight data for recording stop condition

는 16초 미만의 비행자료가 저장되도록 설계하여 하나의 메모리 고장 시에도 연속된 16초 이상의 데이터가 손실되지 않도록 한다. 또한 데이터 삭제 도중 장비 재부팅이 발생할 경우 삭제 작업을 다시 시작하게 되어, block ①의 남은 영역에 기록하는 시간이 데이터 삭제 시간보다 짧을 수 있다. 이에 따라, memory #1에 데이터를 기록할 때에는 이웃하지 않은 메모리(memory #N) 영역의 데이터를 미리 삭제(③)하도록 설계하여, 데이터 기록과 삭제 작업이 서로 충돌하지 않도록 하여야 한다.

ED-112의 2-1.11 Recorder synchronisation 요구사항에 따라 플래시 메모리에 저장되는 모든 데이터 헤더에 CPU timer를 이용한 timetag를 포함하여 기록된 데이터 간 동기화가 1초 이내에 가능하도록 설계하여야 한다. 또한 4-1.2 Functional segregation 요구사항에 따라 비행 데이터와 음성 데이터 간 기록 알고리즘이 서로 영향을 주지 않도록 완전하게 독립적인 태스크로 설계되어야 하며 기록되는 메모리도 물리적으로 완전하게 분리되어야 한다. II-2.1.7 Erasure of recorded data 요구사항을 만족하기 위하여 기록 알고리즘에서 가장 오래된 데이터를 삭제하는 기능 이외에 데이터 삭제 또는 overwrite 하는 기능은 없어야 하며, II-3.2.2 Recording delay 요구사항에 따라 데이터 수신 후 즉시 플래시 메모리에 기록을 수행할 수 있도록 비행자료 기록 알고리즘 수행 태스크의 priority가 가장 높아야 한다.

### 2) 비행자료 기록 중단 기능

무인항공기 사고 발생 시 비행자료 기록장치에 공급되는 전원이 완전히 차단되지 않을 경우, 무의미한 데이터를 추가 저장하여 기존에 저장된 데이터를 overwrite하게 된다. 일반적으로 그림 7과 같은 충격 감지 스위치를 설치하여 강한 충격 발생 시 비행자료 기록장치의 전원을 차단하도록 설계하지만, 이는 별도의 장치 추가로 인한 중량, 비용이 증가하는 단점이 있으며 해외 제품의 경우 EL(export license) 승인이 거부되면 사용할 수 없다. 또한 2-5.3.11 Recorder operation 요구사항을 만족하기 위하여 2가지 이상의 장치 정보를 사용하여 무인항공기 추락 상태를 판단할 수 있어야 하므로, 비행자료 기록장치에 기록되는 비행 데이터 중 착륙장치, GPS, 대기센서 정보를 이용하여 무인항공기 상태를 판단할 수 있는 비행자료 기록 중단 기능을 제안한다.

일반적으로 고정익 형상의 무인항공기는 편서풍의 영향을 받지 않는 일정 고도 미만에서는 임계 속도 미만인 상태로 비행을 유지하는 것이 불가능하므로, 이를 활용하여 무인항공기 추락을 판단할 수 있다. 무인항공기의 이동상태 확인을 위하여 GPS 및 대기센서의 속도 정보를 사용하고, 지상에서의 기동 여부를 구분하기 위하여 착륙장치의 WOW 정보를 사용한다. 또한 실제 비행시험 시 편서풍 등의 영향으로 인하여 무인항공기가 일정 시간 이상 한 지점에서 머물러 있어 GPS 속도가 0에 가까운 상태를 유지하는 현상이 발생할 수 있기 때문에, GPS 고도 정보를 사용하여 일정 고도 이하에서만 무인항공기 상태를 추락으로 판단하도록 하여야 한다. 그림 8에서 볼 수 있듯이 비행조종컴퓨터를 통하여 입력 받은 착륙장치, GPS, 대기센서 데이터를 CPM 내 플래시 메모리에 저장함과 동시에 비행자료 기록 중단 여부를 판단할 수 있도록 한다.

비행자료 기록 중단 판단을 위한 순서도는 그림 9와 같으며, 무인항공기가 지상시험을 위한 정지 상태인지 판단하기 위하여 WOW 신호가 off인지 확인한다. WOW 신호가 off이면 무인항공기가 비행 중인 것으로 판단하고, GPS 데이터 정상 여부 확인 후 GPS 데이터가 임계고도(=Alt_th) 및 임계속도(=Vel_th) 미만인지 확인한다. 이 때, Alt_th 값은 고산지대에 추락할 가능성을 고려하여, 무인항공기 운용 지역 중 가장 높은 고도 값 이상으로 설정하여야 한다. 또한 Vel_th 값은 사용하는 GPS 장치의 속도 오차 범위(±σ)를 고려하여, +σ m/s 값으로 설정하여야 한다. 만일 GPS 거부환경이나 GPS 위성 상태가 불량할 경우 무인항공기 추락을 잘못 판단할 가능성이 있으므로, GPS 데이터 비정상인 경우에는 대기센서의 속도 정보를 동일하게 활용한다. 항공기의 WOW 신호 및 고도, 속도가 일정 모니터링 시간(=Time_th) 동안 기록 중단 조건을 만족하면 기록을 중단하여 사고 조사를 위한 비행자료가 overwrite되지 않도록 설계하였다.

착륙장치의 WOW 신호, GPS 센서의 고도 및 속도 정보, 대기센서의 속도 정보를 이용하여 무인항공기 상태를 추락으로 판단할 경우, CPM 내부 메모리에 마지막 데이터의 메모리 주

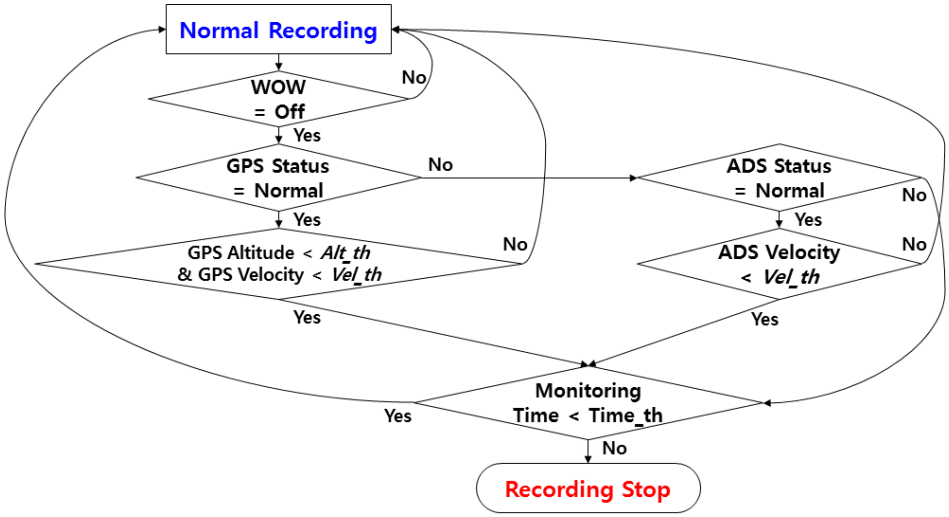


**그림 9.** 기록 중단 판단을 위한 순서도
**Fig. 9.** Flow chart for recording stop

소 값 저장 후 비행자료 기록을 종료한다. 또한 GPS 및 대기센서 데이터 상태가 비정상인 경우에는 정상적인 비행을 수행할 수 없다고 판단되기 때문에 일정 모니터링 시간(=Time_th)동안 정상기록 유지 후 기록 종료 절차를 수행한다.

## Ⅲ. 비행자료 기록장치 소프트웨어 검증 방안

비행자료 기록장치 소프트웨어가 표 1에 식별된 요구사항을 모두 만족하는지 확인하기 위하여 각 요구사항별 검증 방안이 필요하여 이에 대한 방안을 제안하고자 한다. 검증을 위하여 테스트 데이터 모의가 가능한 점검장비가 필요하며, 이는 체계의 연동통제문서에 따른 MIL-STD- 1553B 메시지 및 음성 데이터를 송수신할 수 있어야 한다. 또한 비행자료 복원을 위한 복원 프로그램을 탑재하여야 하며, 28VDC 단전 설계 등을 검증하기 위한 전원공급기 및 타이머 등을 포함하여야 한다. 요구도 검증을 위한 복원 프로그램은 이더넷을 통하여 CPM 메모리에 있는 데이터를 손실 없이 hex 형태로 복원하여야 하며, 사후 분석을 통한 요구도 검증이 가능하여야 한다.

### 3-1 고장 모니터링 기능 검증

표 1의 2-1.4.2 Monitoring of proper operation 요구사항 검증을 위하여, 비행자료 기록장치의 고장 모의 후 점검장비를 연결하여 연동 상태 및 자체진단시험(BIT; built-in test) 세부 항목을 확인하여야 한다. 전원 인가 상태(a) 및 기록장치 연결(e) 확인을 위하여 비행자료 기록장치의 전원 및 신호 케이블 탈거 후 점검장비 화면에서 연동결함 발생 여부를 확인한다. 비행자료 획득 및 처리장치 고장(b) 모의를 위하여 MIL-STD-1553B 통신 컨트롤러를 탈거하여 BIT 세부항목 중 MIL-STD-1553B 통신 항목의 결과를 확인한다. 기록매체 고장(c) 모의 및 정상 기록 여부(d) 확인을 위하여 CPM을 탈거하여 비행 데이터 저장 상태 항목을 확인한다. 비행 데이터 저장 상태 항목은 CPM에 데이터 저장 후 저장된 데이터를 다시 읽어 제대로 저장되었는지 확인하는 항목이므로 장착된 메모리가 없을 경우 고장으로 표시된다. 그림 10은 CPM 고장모의 후 BIT 세부항목을 확인하기 위한 점검장비 화면이며 비행 데이터 저장 상태 항목만 fail로 시현됨을 확인할 수 있다. ED-112에서 요구된 항목뿐만 아니라 BIT에서 정의된 모든 고장 항목들은 이와 같은 고장 모의 후 정상적으로 고장이 탐지되는 것을 확인하여 검증할 수 있다.

### 3-2 비행자료 기록 시작 및 종료 기능 검증

표 1의 2-1.5 Start and termination of recording 요구사항에 따라 항공기 전원 인가 후 항공기가 이동하기 전 비행자료 기록을 시작하여야 하므로, 비행자료 기록장치 전원 인가 후 10초 이내에 비행자료 기록이 시작되는지 확인하여 비행자료 기록 시작 시점을 검증할 수 있다. 비행자료 기록장치 내부 CPU timer를 이용하여 전원 인가 시점부터 데이터 기록 시작 시점까지의 시간을 자동으로 측정하도록 비행자료 기록장치 소프트웨어를 설계한다. 이는 그림 11과 같이 소프트웨어 초기화 완료 후 저장 시작 시점까지 측정된 시간을 시리얼 통신 로그로 출력하여 요구사항대로 10초 이내 부팅이 완료되는 것을 확인할 수 있다.

| 순번 | 점검항목 | 기준값 | 측정값 | 결과 | 에러 발생 횟수 |
|---|---|---|---|---|---|
| 1 | 3.3VDC 출력 전압 상태 | 0 | 0 | Pass | 0 |
| 2 | 28VDC 입력 전압 상태 | 0 | 0 | Pass | 0 |
| 3 | 프로세서 타이머 상태 | 0 | 0 | Pass | 0 |
| 4 | 프로세서 인터럽트 컨트롤러 상태 | 0 | 0 | Pass | 0 |
| 5 | Power Board 상태 | 0 | 0 | Pass | 0 |
| 6 | Control Board 상태 | 0 | 0 | Pass | 0 |
| 7 | 비행 데이터 저장 상태 | 0 | 1 | Fail | 393 |
| 8 | 비행 데이터 저장 상태(channel X) | 0 | 0 | Pass | 0 |

**그림 10.** CPM 고장 모의 후 BIT 결과
**Fig. 10.** BIT result after fault injection(CPM)

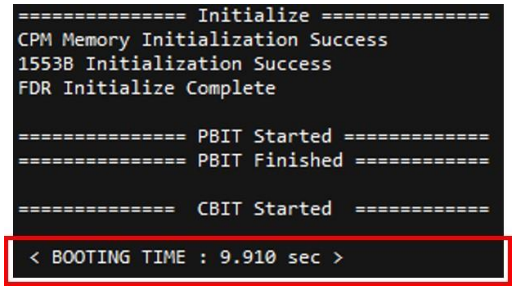


**그림 11.** 기록 시작 시간 검증
**Fig. 11.** Verification of recording start

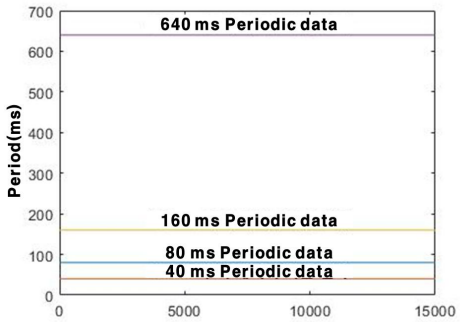


**그림 12.** 저장 주기 확인 결과
**Fig. 12.** Confirmation of recording period

비행자료 기록 종료 검증을 위하여 전원 차단 시점까지 수신된 모든 데이터들의 정상 저장 여부를 확인하여야 한다. 비행자료 기록장치의 전원 차단 후 복원된 데이터와 점검장비의 테스트 데이터가 일치하는지 확인하여 기록 종료 조건 검증이 가능하며, 데이터 일치 여부는 II-1.3.2 Classes of flight data recorder 요구사항의 검증과 동일하게 수행된다.

### 3-3 복원 데이터 동기화 검증

표 1의 2-1.11 Recorder synchronisation 요구사항에 따라 기록된 데이터 복원 시 동기화를 위하여 각 데이터 간 기록된 시간 오차가 1초 이내인지 확인하여야 한다. 비행자료 기록장치에 저장되는 모든 메시지는 timetag이 포함된 헤더 정보를 가지고 있으므로, timetag 시간 기준에 맞춰서 데이터를 분석할 수 있다. 데이터 간 동기 확인을 위하여 점검장비의 시간 정보를 포함하는 테스트 데이터를 기록하여 데이터 간 기록되는 시간 오차가 1초 이내인지 확인할 수 있다. 그림 12와 같이 모든 데이터의 local time이 설계된 주기에 맞춰서 저장되는지 확인할 수 있으며 테스트 데이터의 시간 정보와 local time간 시차가 1초 이내인지 확인한다.

### 3-4 의도치 않은 전원 차단 보호설계 검증

표 1의 2-5.3.8 Inadvertent turnoff 요구사항에 따라 항공기 사고 또는 전원 계통 이상으로 인한 의도치 않은 전원 차단 시에도 마지막까지 수신된 데이터가 정상 저장되어야 한다. 이에 대한 검증은 II-1.3.2 Classes of flight data recorder 요구사항 검증과 동일하게 수행되며, 비행자료 기록장치의 28VDC 전원 차단 후 복원된 데이터와 점검장비에서 송신한 테스트 데이터가 일치하는지 확인하여 검증한다.

### 3-5 비행자료 기록 중단 기능 검증

표 1의 2-5.3.11 Recorder operation 요구사항에 따라 항공기 추락 등의 비정상 상황 발생 시 무의미한 데이터가 기존에 저장된 유의미한 데이터를 overwrite하는 현상을 방지하기 위하여 설계된 기록 중단 기능 검증이 필요하다. 기록 중단 여부 판단을 위하여 착륙장치의 WOW 정보, GPS 센서의 고도 및 속도 정보, 대기센서의 속도 정보를 사용하기 때문에, 표 2와 같이 센서 값들을 모의하여 기록 중단 수행 여부를 확인한다. WOW 정보는 좌측/우측/노즈 랜딩기어 중 하나라도 off인 경우 기록 중단 조건을 만족하므로 총 8가지 경우의 수가 존재한다. GPS 센서는 정상 여부, 고도, 속도 정보를 판단하며 센서 이중화에 따라 64가지의 경우의 수가 존재한다. 대기센서는 정상 여부 및 속도 정보를 판단하며 센서 이중화에 따라 16가지의 경우의 수가 존재한다. 각 데이터들이 기록 중단 조건을 만족한 상태를 일정 시간 이상 유지하는지 확인하기 위한 모니터링 시간은 총 2가지 경우의 수가 존재하며, 이 모든 경우의 수를 조합하여 식별된 테스트 케이스는 총 16,384 가지이다. 테스트 케이스가 매

**표 2.** 기록 중단 기능 검증을 위한 테스트 케이스
**Table 2.** Test case for verification of recording stop

| Data | Test case |
|---|---|
| Weight-on-wheel | Left landing gear = on or off<br>Right landing gear = on or off<br>Nose landing gear = on or off<br>→ $2^3$ = 8 cases |
| GPS sensor | Normal or abnormal<br>→2 x 2 CH = 4 cases |
| | Altitude < Alt_th or Altitude ≥ Alt_th<br>→2 x 2 CH = 4 cases |
| | Velocity < Vel_th or Velocity ≥ Vel_th<br>→2 x 2 CH = 4 cases |
| Air data sensor | Normal or abnormal<br>→2 x 2 CH = 4 cases |
| | Velocity < Vel_th or Velocity ≥ Vel_th<br>→2 x 2 CH = 4 cases |
| Monitoring time | Elapsed time < Time_th or<br>Elapsed time ≥ Time_th<br>→2 cases |
| **Total** | $2^{14}$ **= 16,384 cases** |

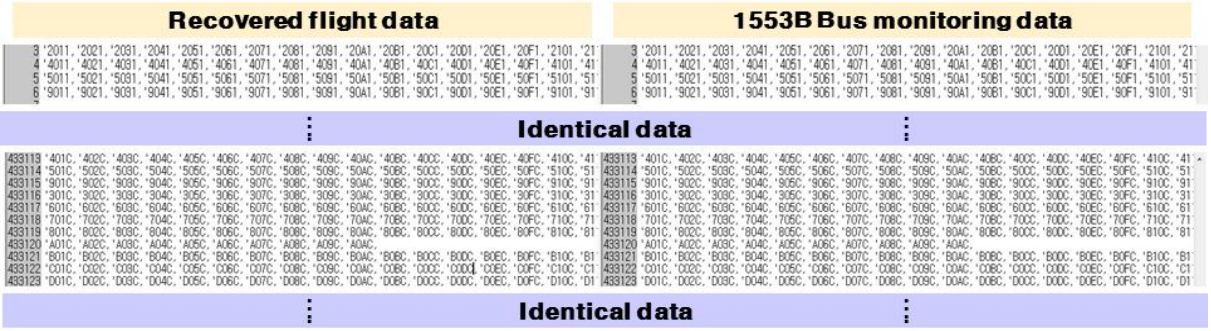


**그림 13.** 비행자료 복원 데이터 검증 결과
**Fig. 13.** Verification of flight data restoration

우 많기 때문에 충분히 검증 가능한 케이스들만 선별하여 검증이 가능하며 그림 10의 비행 데이터 저장 상태 항목을 확인하여 기록 중단 여부를 확인한다.

### 3-6 이종 데이터 간 분리 설계 검증

표 1의 4-1.2 Functional segregation 요구사항을 만족하기 위하여 비행자료 기록장치는 MIL-STD-1553B 통신으로 수신되는 비행 데이터와 음성통신중계 시스템에서 수신되는 음성 데이터를 저장하기 위한 각 기록 기능이 서로 영향을 주지 않도록 메모리 및 기록 알고리즘이 분리되어 동작한다. 이를 검증하기 위하여 각 데이터 유형에 대한 고장 주입 후 나머지 데이터 유형의 기록 알고리즘에 영향성이 있는지 확인하여야 한다. 이를 위하여 점검장비에서 음성 데이터와 비행 데이터 중 한 가지 데이터를 고장 모의(데이터 미전송)하여, 정상 기록된 데이터가 테스트 데이터와 일치하는지 확인하여야 한다. 데이터 일치 여부는 II-1.3.2 Classes of flight data recorder 요구사항의 검증과 동일하게 수행된다.

### 3-7 기록매체 분리 기능 검증

표 1의 4-1.2.1 Recording medium segregation and partitioning 요구사항을 만족하기 위하여 비행자료 기록장치는 하나의 메모리 손상 시에도 모든 데이터가 손실되지 않도록 비행자료를 여러 개의 플래시 메모리에 나누어 저장하도록 설계된다. 이를 검증하기 위하여 모든 메모리에 저장된 데이터를 덤프한 후 각 데이터의 timetag을 비교하여 모든 메모리에 순서대로 저장되었는지 확인한다.

### 3-8 저장 용량 검증

표 1의 II-1.3.2 Classes of flight data recorder 요구사항의 비행자료 기록장치의 저장 용량 검증을 위하여 두 가지 검증 시나리오가 필요하다. 한 가지는 25시간 동안 연속된 데이터가 정상 저장되는지 확인하여야 하며, 나머지는 여러 소티의 데이터를 25시간 분량으로 저장하여 정상 저장되는지 확인하여야 한다. 각 시나리오에 맞는 점검장비 테스트 데이터를 생성하여 시험을 수행하여야 하며, 모든 테스트 데이터는 시간에 따라 변화는 값이고 모든 bit가 0과 1을 모두 표현하여야 한다. 점검장비와 연동하여 각 시나리오에 대한 테스트 데이터 저장 후 그림 13과 같이 복원된 데이터와 동일한지 확인하여 요구사항을 검증하도록 한다.

### 3-9 데이터 기록 및 복원 기능 검증

표 1의 II-2.1.4 Recording technology 요구사항에 따라 기록된 비행자료 복원 시 기록매체에 저장되어있는 데이터를 변경하지 않아야 하며, 이를 검증하기 위하여 두 가지 검증 시나리오가 필요하다. 한 가지는 CPM에 저장된 모든 소티의 데이터를 복원할 경우 영향성이 있는지 확인하여야 하며, 나머지는 1개 이상의 일부 소티 데이터만 복원 시 영향성이 있는지 확인하여야 한다. 검증 방안은 각 시나리오 별로 데이터 복원을 수행하고 CPM에 저장된 모든 데이터를 한 번 더 복원하도록 한다. 복원된 모든 데이터들이 테스트 데이터와 일치하는지 확인하여 비행자료 기록장치의 복원 기능이 기록매체(CPM)에 영향을 미치는지 확인한다.

하나의 메모리 손상 시, 16초 이상의 연속된 데이터가 손실되지 않도록 비행자료 기록장치의 기록 알고리즘에서는 memory mirroring 및 data striping 기법을 사용한다. 이를 검증하기 위하여 비행자료 복원 프로그램에서 CPM의 특정 메모리의 데이터를 읽지 않도록 수정하여 복원된 데이터의 시간 축을 분석할 수 있다. 복원된 데이터의 주기를 분석하여 16초 이상의 연속된 데이터가 손실되는지 확인하여 기록 알고리즘을 검증한다.

### 3-10 덮어쓰기 기능 검증

표 1의 II-2.1.7 Erasure of recorded data 요구사항을 만족하기 위하여 비행자료 기록장치는 가장 오래된 데이터부터 덮어쓰는 기능을 가지고 있다. 사고 발생 시 가장 최근의 데이터가 중요하므로 덮어쓰기 기능으로 인하여 손실되지 않는지 확인하는 것은 매우 중요하며, 이를 검증하기 위하여 두 가지 검증 시

**표 3.** 덮어쓰기 기능 검증 결과
**Table 3.** Verification of overwrite

| Before recording | After recording |
|---|---|
| S_0_X.fdr | Deleted |
| S_1_X.fdr | |
| S_2_X.fdr | |
| S_3_X.fdr | |
| S_4_X.fdr | |
| S_5_X.fdr | |
| S_6_X.fdr | S_6_X.fdr |
| S_7_X.fdr | S_7_X.fdr |
| S_8_X.fdr | S_8_X.fdr |
| S_9_X.fdr | S_9_X.fdr |
| S_10_X.fdr | S_10_X.fdr |
| S_11_X.fdr | S_11_X.fdr |
| S_12_X.fdr | S_12_X.fdr |
| S_13_X.fdr | S_13_X.fdr |
| S_14_X.fdr | S_14_X.fdr |
| S_15_X.fdr | S_15_X.fdr |
| S_16_X.fdr | S_16_X.fdr |
| N/A | S_17_X.fdr |
| | S_18_X.fdr |
| | S_19_X.fdr |
| | S_20_X.fdr |
| | S_21_X.fdr |
| | S_22_X.fdr |

나리오가 필요하다. 한 가지는 플래시 메모리 최대 용량 이상을 차지하는 비행 소티 1개의 데이터를 덮어쓸 경우 비행 소티 초반의 데이터가 삭제되는지 확인하여야 하며, 나머지는 여러 비행 소티의 데이터를 덮어쓸 경우 가장 오래된 비행 소티들만 삭제되는지 확인하여야 한다. 두 번째 시나리오는 표 3과 같이 플래시 메모리 최대 용량만큼의 여러 비행 소티 데이터를 기록 및 복원한 후 추가 비행 소티 데이터를 저장하여 가장 먼저 저장된 비행 소티의 데이터부터 삭제되고 추가 소티의 데이터가 저장되는지 확인한다. 표 3은 CPM에서 복원된 자료의 파일명을 비교한 결과이며, 이 때 삭제된 데이터의 용량과 추가 저장된 데이터의 용량이 일치하는지 확인하여야 한다.

비행시험 후 비행자료 확인이 필요하거나 사고가 발생하여 비행자료 복원이 필요할 경우, 기록된 비행자료를 덮어쓰지 않도록 다운로드 케이블 연결 및 데이터 추출을 안전하게 수행하기 위한 절차가 필요하다. 비행자료 기록장치는 다운로드 케이블 연결 시 점검용 디스크리트 신호 값에 따라 기록 모드 또는 정비 모드로 진입하며, 정비 모드 진입 시 플래시 메모리의 쓰기 기능을 사용하지 않도록 한다. 이를 검증하기 위하여 우선 비행자료 기록장치에 점검장비 테스트 데이터를 저장한 뒤 점검용 디스크리트 입력 값을 변경하여 정비 모드 진입 여부를 시리얼 통신 로그를 통하여 확인한다. 정비 모드에서 CPM에 저장된 비행자료를 복원하여 점검장비의 테스트 데이터와 일치하는지 확인하여 데이터 손실 여부를 확인하여야 한다.

### 3-11 초기화 및 단전 설계 검증

표 1의 II-3.2.1 Start-up and effects of power interruptions 요구사항에 따라 비행자료 기록장치는 항공기 전원이 인가되면 10초 이내에 비행자료 저장을 시작하며, 이에 대한 검증은 2-1.5 Start and termination of recording 요구사항 검증 방안과 동일하게 수행한다. 60초 이내 자가진단 여부를 확인하기 위해서는 비행자료 기록장치 전원 인가 시점부터 PBIT 결과 수신 시점까지의 시간을 측정한 결과가 60초 이내인지 확인한다.

비행자료 기록장치는 200 ms 이하의 단전 시에도 정상적으로 비행자료를 저장하여야 하기 때문에 점검장비에 내장된 전원공급기의 전원을 200 ms 동안 자동으로 차단하도록 점검 환경을 구성하여야 한다. 점검장비를 이용하여 자동으로 200 ms 단전 수행 후 점검장비에서 송신하는 테스트 데이터와 비행자료 기록장치에서 복원된 비행자료를 비교하여 일치 여부를 확인한다. 데이터 일치 여부는 II-1.3.2 Classes of flight data recorder 요구사항의 검증과 동일하게 수행된다.

### 3-12 데이터 저장 시간 검증

표 1의 II-3.2.2 Recording delay 요구사항에 따라 사고 발생 시 가장 마지막으로 수신되는 데이터까지 손실없이 저장하기 위하여 비행자료 기록장비가 데이터를 획득하는 시점부터 CPM의 플래시 메모리에 저장되는 시점까지 0.5초 이하의 시간이 소요되어야 한다. 이를 검증하기 위하여 MIL-STD-1553B 데이터 수신 시 인터럽트 시점부터 플래시 메모리에 데이터 저장까지의 CPU timer 시간을 측정하여 0.5초 이하인지 확인한다. 이러한 검증 방안은 비행자료 기록장치의 스케줄러에 따라 다른 태스크의 영향을 받을 수 있기 때문에 장시간동안 BIT 등 다른 기능 시험을 수행하면서 함께 검증을 수행하여야 한다.

## Ⅳ. 결 론

무인항공기 사고 발생 시 사후 분석을 위한 비행자료 기록장치는 극한환경에서도 메모리에 기록된 비행자료 보존 및 복원하기 위하여 EUROCAE의 ED-112 규격을 준수하여야 한다. ED-112 규격은 유인항공기를 포함한 모든 항공기의 일반적인 요구사항을 규정하고 있기 때문에 적용하고자 하는 플랫폼의 형상 및 운용개념에 적합한 요구사항을 선택적으로 적용하여야 한다. 본 논문에서는 ED-112 규격의 요구사항 중 무인항공기에 대한 요구사항을 식별하였고, 적용하고자 하는 무인항공기의 형상 및 운용개념에 따른 요구사항을 추가로 식별하였다. 또한 이를 만족하기 위한 비행자료 기록 알고리즘 및 비행자료 기록 중단 기능에 대하여 상세하게 서술하였다. 비행 데이터 및 음성 데이터의 기록 알고리즘 간 서로 영향을 주지 않도록 독립적인 태스크로 설계하였으며, 하나의 메모리가 물리적으로 손상이 발생하더라도 16초 이상의 연속된 데이터가 손실되지 않도록 설계하였다. 또한 항공기 추락과 같은 사고 발생 시 전원

이 완전히 차단되지 않을 경우를 대비하여 착륙장치의 WOW 정보, GPS 센서의 고도 및 속도 정보, 대기센서의 속도 정보를 이용하여 유사시 비행자료 기록을 중단하는 기능을 설계에 반영하였다.

제안된 소프트웨어 설계 검증을 위하여 각 요구사항별 검증 방안을 제시하였으며 이에 따라 비행자료 기록장치 소프트웨어가 정상적으로 설계되었음을 확인할 수 있다. 기록된 데이터의 헤더에 저장된 timetag을 비교하여 복원된 비행자료 간 동기화 여부를 확인할 수 있으며, 16,384 가지의 테스트 케이스를 식별하여 항공기 추락 감지 및 자동 기록 중단 기능을 검증할 수 있도록 하였다. 25시간 이상 저장된 데이터를 점검장비의 테스트 데이터와 비교하여 저장 용량, 덮어쓰기, 복원 기능 및 단전 설계 검증이 가능하며, CPU timer로 소프트웨어 동작 시간을 측정하여 데이터 수신 시점부터 CPM 저장 시점까지의 소요 시간 검증이 가능하였다.

## References


[1] J. S. Roh and J. H. Kim, “A study on development trends of flight data recorder and certification methods,” in *Proceeding of The Korean Society for Aeronautical and Space Sciences Spring Conference,* Seorak: Korea, pp. 450-451, Apr. 2018.

[2] Minimum Operational Performance Specification for Crash Protected Airborne Recorder Systems, EUROCAE ED-112, 2003

[3] B. Y. Kim, J. S. Jang, H. J. Lee, and B. G. Kim, “Voice/flight data recorder hardware and test equipment,” in *Proceeding of The Korean Society for Aeronautical and Space Sciences Fall Conference,* Pyeongchang: Korea, pp. 1676-1680, Nov. 2011.

[4] J. H. Kim, J. P. Kim, J. Y. Kim, and T. W. Kim, “Design and verification of housing and memory board for downsizing for crash protected memory module,” *The Journal of The Korean Society for Aeronautical and Space Sciences*, Vol. 48, No. 1, pp. 81-88, Jan. 2020.

[5] S. K. Lee, B. H. Lee, and J. H. Choi, “The study of analysis and test for crash survival about the crash protected module in black box used at aircraft,” *The Journal of The Korean Society for Aeronautical and Space Sciences*, Vol. 40, No. 1, pp. 61-68, Jan. 2012.

[6] S. H. Yang, J. P. Han, J. S. Huh, and J. C. Shin, “Development of voice and flight data recorder software for aerial vehicle,” in *Proceeding of The Korean Society for Aeronautical and Space Sciences Fall Conference,* Jeju: Korea, pp. 1128-1129, Nov. 2017.

**양 서 희** (Seo-Hee Yang)
2013년 2월 : 이화여자대학교 전자공학과 (공학사)
2015년 2월 : 이화여자대학교 전자공학과 (공학석사)
2015년 3월 ~ 현재 : 국방과학연구소 연구원
※관심분야 : 항공전자장비, 임베디드 S/W