Journal of The Korea Society of Computer and Information
Vol. 24 No. 2, pp. 111-118, February 2019
www.ksci.re.kr
https://doi.org/10.9708/jksci.2019.24.02.111

# Implementation of OFP initialization function in IMDC for FA-50 aircraft

Eun-Kyung You*, Chan-Gyu Bae*, Hyeock-Jin Kim**

## Abstract

Recent trends in modern warfare are increasing in importance for air warfare, information warfare, and warfare. The technology of the weapon system software is rapidly developing, and the silent information war to hack it is still going on. Currently, the FA-50 aircraft has a function that can be initialized by a simple switch operation to protect the main military information in the event of an emergency. However, there are limitations in the existing Zeroize function, and this study was carried out to supplement this. First, we compare and analyze the memory structure of aircraft operating in our military, and examined the currently implemented Zeroize function. Second, we reviewed various methods to overcome the limitation of existing Zeroize function. Third, we implement the existing Zeroize function without additional manipulation. In this paper, we propose that the implementation of this feature will enable us to protect our military data more securely and suggest that we should continue to look for ways to enhance security for our technology in the future.

▸Keyword: FA-50 aircraft, IMDC, OFP, Zeroize function, Memory, Security

## I. Introduction

최근 현대전의 양상을 살펴보면 과학기술무기의 수준이 전쟁의 승패를 좌우한다고 해도 과언이 아니다. 최첨단 시스템을 갖춘 장비와 장거리 원격통신이 가능한 지휘·통제체계가 전장 상황을 실시간을 전송하고 있으며, 항법위성 신호를 이용하여 목표물을 정확히 명중시키는 미사일까지 무기체계의 발전은 복잡하고 빠르게 진보하고 있다[1].

그 중 현대전의 핵심인 공중전은 전투기 및 전투기 탑재 장비의 기술력에 따라 그 위력에 차이가 크며, 공중우세를 확보하기 위한 국가 간의 경쟁은 갈수록 치열해지고 있다.

현재 공군은 F-16, F-15 등의 전투기를 운용하고 있으며, 차세대 스텔스 전투기를 확보하기 위한 계획을 추진하고 있다. 특히, 국산 경공격기인 FA-50 전투기는 국내기술로 제작한 최초의 전투기로써 F-16 전투기 기능과 유사한 기능을 제공하며, 최첨단 장비를 탑재하여 그 우수성 또한 뛰어나다[2].

한편, 현대전의 승패를 좌우하는 요인으로 정보전·사이버전 능력의 중요성이 강조되고 있다. 국제안보환경이 급속도로 변화함에 따라 전 세계적으로 사이버전쟁 또는 정보전쟁의 위협이 미치는 영향을 심각하게 받아들이고 있다[3]. 무기체계의 기술력이 발전함에 따라 이러한 군사 기술을 해킹하기 위한 시도가 다수의 공격자들에 의해 끊임없이 발생하고 있다. 실제로 군 내부 인트라넷을 해킹하여 군사기밀이 유출되는 등 해킹당한 정보는 국가안전보장에 치명적인 위험을 초래하게 된다[4].

우리 군은 전투기 및 무기체계 기술력을 꾸준히 발전시키며 국내기술로 전투기를 제작하였고, 무기체계 융합 기술력을 확보해나가고 있다. 이에 따라 우리 군사자료를 해킹하기 위해 국방망을 침투, 각종 군사기밀과 자료를 탈취하기 위한 시도가 지속적으로 포착되고 있다[5].

최신 전투기에는 최첨단 장비가 탑재되어 있으며, 이를 운용하기 위해 주임무컴퓨터가 장착되어 있다. 주임무컴퓨터에 내장된 소프트웨어는 항공기 운용을 위한 알고리즘과 조종사 임

• First Author: Eun-Kyung You, Corresponding Author: Hyeock-Jin Kim
*Eun-Kyung You (yek0444@hanmail.net), Avionics Software Development Center, Republic of Korea Air Force
*Chan-Gyu Bae (ventus@gmail.com), Avionics Software Development Center, Republic of Korea Air Force
**Hyeock-Jin Kim (jin1304@chungwoon.ac.kr), Ph.D, Computer Engineering, Professor, Chungwoon University
• Received: 2019. 01. 16, Revised: 2019. 02. 12, Accepted: 2019. 02. 12.
• This work was supported by an Academic Research Fund of Chungwoon University in 2018

무수행을 위한 다양한 군사정보가 저장되어있다[6]. 이러한 정보를 보호하기 위해 전투기는 Zeroize 기능을 제공하고 있다[7]. Zeroize 기능은 비상상황 발생 시 조종사의 Zeroize 버튼 조작 또는 좌석 사출을 통해 작동이 가능하며, 주요 군사자료를 삭제되도록 구현되어 있다. FA-50 항공기 또한 Zeroize 기능이 작동하면 주임무컴퓨터와 각종 장비에 저장된 군사자료를 삭제하도록 구현되어 있다[8]. 그러나 현재 구현되어 있는 Zeroize 기능은 주임무컴퓨터와 각종 장비의 NVRAM 메모리 영역에 저장된 일부 군사자료만 삭제가 가능하다. 비상상황이 발생하여 전투기가 비상 착륙하거나 불시착 시 주임무컴퓨터가 적에게 노출되어 주임무컴퓨터에 내장된 소프트웨어가 해킹될 수 있는 가능성이 존재한다. 주임무컴퓨터에 내장된 비행운용프로그램은 ROM 영역에 저장되며, Zeroize 기능이 수행되어도 ROM 영역은 제거되지 않기 때문이다.

이에 본 연구에서는 FA-50 항공기 주임무컴퓨터의 메모리 영역을 분석하고, Zeroize 기능 수행 시 ROM 영역에 저장된 비행운용프로그램 접근이 불가능하도록 구현하고자 한다. 이러한 연구를 위하여 첫째, 각 항공기 기종별 메모리 구조 및 Zeroize 기능을 분석하고, 둘째, 기존 Zeroize 기능의 한계점을 보완할 수 있는 방안을 연구하며, 마지막으로 조종사가 기존의 Zeroize 절차와 동일한 절차대로 운용하도록 하여 간단한 조작만으로 기존 Zeroize 기능의 취약점을 보완하고자 하였다.

본 기능의 테스트는 항공기 주임무컴퓨터의 비행운용프로그램 소프트웨어에 적용하고, 단위시험 테스트, 시스템 통합시험을 수행한다. 또한 실제 항공기와 동일한 환경을 갖춘 HILS(Hardware In the Loop Simulation) 장비인 AHB(Avionics Hot Bench)를 활용하여 지상시험을 수행한 후 검증된 소프트웨어를 항공기에 적용할 예정이다.

논문의 구성은 2장에서 FA-50 항공기 항공전자 시스템과 FA-50 항공기 IMDC의 메모리 구조에 대해 설명하고, 기종별 항공기의 Zeroize 기능을 비교 분석한다. 3장에서는 본 기능을 구현하기 위한 소프트웨어 설계 내용을 구체적으로 서술하며, 4장에서는 구현된 기능의 성능을 테스트하고, 5장에서 결론 및 제언을 한다.

## II. Preliminaries

### 1. Related works

#### 1.1 FA-50 aircraft avionics system

FA-50 항공기는 전술입문훈련기인 TA-50 항공기의 공대공과 공대지 작전능력을 향상시켜 공군의 노후화된 전투기를 대체하기 위해 개발된 최초의 국산 전투기이다[9]. FA-50 항공기는 첨단의 디지털 항공전자 시스템이 장착되어 있어 전천후 공격임무에 적합할 뿐 아니라, Link-16 전술데이터 링크를 탑재하여 실시간으로 전장 정보를 공유하는 것이 가능하다[10].

FA-50 항공기 항공전자 시스템에는 화력제어 레이더(FCR, Fire Control Radar), 레이더 고도계(RALT, Radar Altimeter), 통합위성/관성 항법장치(EGI, Embedded GPS/INS), UHF/VHF/Have Quick Radio, 적아식별 장비(IFF, Identification of Friend or Foe), 전자전장비(EWS, Electronic Warfare System), 엔진 상태 점검 시스템(ECMS, Engine Control Monitoring System), 무장 관리 컴퓨터(SMS, Stores Management System), 다기능 정보 분배체계(MIDS, Multi-functional Information Distribution System) 등이 탑재되어 있으며, 이러한 항공전자 시스템은 항공기 주임무컴퓨터인 IMDC(Integrated Mission Display Computer)를 통해 운영 및 통제되고 있다[11]. 항공기는 IMDC를 중심으로 각 시스템으로부터 획득한 데이터를 이용하여 디스플레이, 입·출력 및 화력제어 기능을 제공하고, 항공기 시스템이 정상적으로 작동할 수 있도록 다른 서브시스템들을 제어한다. Fig. 1과 같이 IMDC는 dual-redundant 방식으로 X, Y, V 및 Z의 Multiplex buses를 통해 각 시스템 간의 데이터를 송·수신하며, 여기서 획득한 데이터를 가공하여 전방시현장비(HUD) 또는 스마트 다기능시현장비(SMFD) 등을 통해 임무 수행에 필요한 각종 정보를 제공하고 있다. 또한, 조종사는 비행 전 미리 계획한 비행임무자료를 임무계획컴퓨터(RMM, Removable Memory Module)에 입력한 후 비행대기선에서 항공기에 데이터 전송카트리지(DTC, Data Transfer Cartridge)를 로딩하여 운용하고 있다[12].

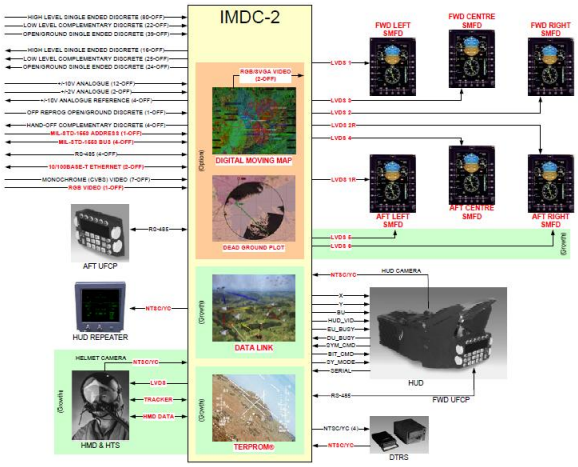



Fig. 1. Typical IMDC-2 System Overview[13]

#### 1.2 IMDC memory structure of FA-50 aircraft

FA-50 항공기 주임무컴퓨터인 IMDC는 FC, IUFC, HUD, MFDS 및 SMFD 총 5개의 비행운용프로그램(OFP, Operational Flight Program)으로 구성되어 있다. 먼저 FC OFP는 입/출력 데이터 처리 및 MUX Bus를 제어하며 System Mode, Subsystem 제어 등의 핵심 기능을 수행한다. IUFC OFP는 통신, 항법, 피아식별과 관련된 정보를 입력 및 제어할 수 있는 기능을 수행한다. HUD OFP는 조종석 전방에 위치한 HUD에 다양한 조종사 참조 심벌을 시현하는 기능을 수행한다. MFDS OFP는 임무계획, 항법 또는 무장과 관련된 데이터를 입력하고 각종 심벌을 시현해주는

기능을 수행한다. 마지막으로 SMFD OFP는 IMDC가 작동 불능인 경우 백업 기능을 제공한다.

IMDC의 내부 프로세싱 모듈은 HPM(HSG Processing Module)과 PGM(Processing and Graphics Module)으로 구성되어 있으며, GPM(Generic Processor Module)이라는 동일한 프로세서를 사용한다. 이 프로세서는 BAE Systems사에서 제공하는 BAE Systems Modular Computing GP2인 HPM과 PGM을 사용하기 위한 Board Level 형상에 적용되는 프로세싱이며, GENESYS software architecture를 지원하기 위한 능력을 제공한다. GPM의 메모리 영역에는 Fig. 2와 같이 FLASH, NV-SRAM, RAM 등으로 구성되며, FA-50 항공기는 주임무컴퓨터의 OFP를 운용하기 위해 xxx Mbytes의 Flash EEPROM, xxx Kbytes NV-SRAM, xxx Mbytes DDR SDRAM을 제공한다.

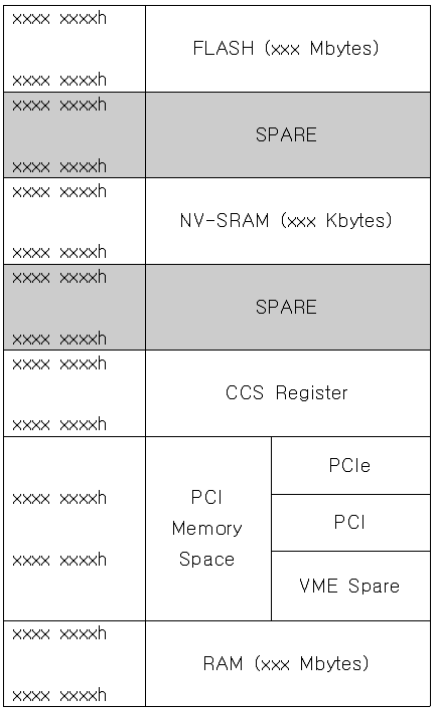



Fig. 2. GPM Address Space Map[14]

Flash 메모리는 시스템을 실행하기 위한 필수적인 Program Image를 저장하며 IMDC가 부팅될 때 이곳에 저장된 OFP Image 파일을 불러오게 된다. NV-SRAM 메모리는 시스템 전원이 공급되지 않아도 주요 정보를 계속 유지할 수 있도록 저장한다. IMDC는 조종사가 다음 비행임무 시에도 재사용되어야 하는 주요 정보를 NV-SRAM 영역에 저장하며, 시스템 전원이 차단되는 즉시 저장된다. 조종사는 항공기 전원이 공급되면 비행운용과 관련된 데이터를 다시 사용할 수 있지만, 임무계획장비를 통해 입력한 자료는 NV-SRAM 영역에 저장되지 않기 때문에 DTC를 재로딩해서 사용해야한다. RAM은 비행운용 시 일시적으로 데이터를 저장하는데 사용되며, 항공기 전원이 공급되는 동안 데이터를 유지한다. 항공기는 단위 시간당 처리할 수 있는 업무 단위량을 최대화하기 위해 ROM에 저장된 OFP Image를 RAM으로 복사해서 RAM 영역에서 OFP를 운용한다.

### 1.3 Zeroize function for aircraft type

현재 공군에서 운용하고 있는 항공기 중 항전 시스템을 통해 운영하는 대표적인 기종으로 KF-16, F-15K, T/TA/FA-50 항공기를 들 수 있다.

먼저, KF-16의 메모리는 부팅 시 Start-up 관련 프로세싱을 수행하는 xxx Kbyte의 Start-up ROM과, OFP 로드모듈이 저장되어있는 xxxKbyte의 RAM으로 구성된다. RAM 영역에 OFP 로드모듈이 저장되어 운용되기 때문에 메모리 보존을 위해 별도의 Battery가 연결되어 있다. KF-16 메모리에 저장된 중요 데이터를 삭제하기 위해 총 3가지 방법으로 Zeroize를 수행할 수 있으며, Zeroize 작동 방법은 항공기 조종석 내에 장착된 Zeroize Switch 또는 항공기에 장착된 주요 장비의 개별 Zeroize Switch를 작동시킴으로써 중요 데이터를 삭제할 수 있다. 또한 비상상황 시 좌석 사출을 하게 되면 Zeroize Switch 동작과 동일한 작동을 수행한다. KF-16의 Zeroize 기능은 동작에 따라 Fig. 3과 같은 자료를 삭제하며, OFP Zeroize 시 OFP 메모리 카드(Ax Card)로 전기 신호를 직접 전송하여 RAM 영역에 저장된 OFP를 직접 삭제하도록 구현되어 있다.

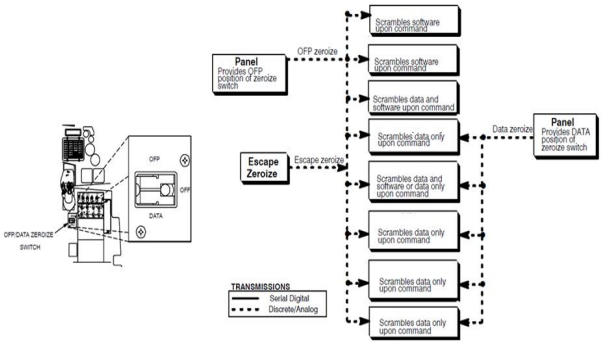



Fig. 3. KF-16 Zeroize Function[15]

F-15K의 메모리는 xxMbyte의 ROM, xxxMbyte의 RAM과 xxMbyte의 NVRAM으로 구성된다. ROM에는 OFP 로드모듈이 저장되며, ROM에 저장된 데이터를 RAM 영역으로 복사해서 항공기 비행운용프로그램을 운용한다. 또한 NVRAM은 시스템 전원이 공급되지 않는 동안에도 데이터를 유지할 수 있도록 해준다. F-15K의 Zeroize 기능은 Zeroize Switch를 작동시키거나, 좌석 사출을 하면 데이터를 삭제할 수 있다. Zeroize 동작 시 주요 장비에 저장된 비밀 자료가 삭제되지만, 주임무컴퓨터인 ADCP로는 Zeroize 신호가 전송되지 않는다. ADCP에 저장된 데이터를 삭제하는 방법으로는 Fig. 4의 항공기 조종석 내에 위치한 ADCP Reset Switch를 이용하여 삭제할 수 있으며, ADCP Reset Switch 동작 시 ADCP 전원이 재부팅되면서 RAM에 저장된 Display & Control Data를 삭제한다. 또한 UFC를 통해 “NVRAM-CLEAR" 절차를 수행하게 되면 ADCP에 저장된 NVRAM 데이터를 삭제할 수 있다.

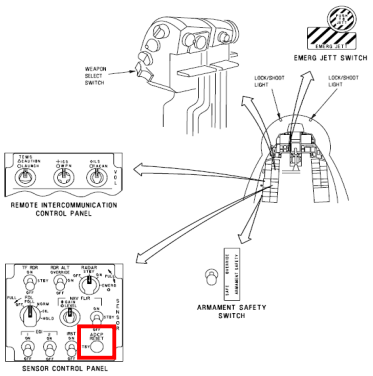



Fig. 4. F-15K Zeroize Function[16]

T/TA-50의 메모리는 xxMbyte의 ROM, xxMbyte의 RAM과 xxKbyte의 NVRAM으로 구성된다. F-15K와 마찬가지로 ROM에 OFP 로드모듈이 저장되며, ROM에 저장된 OFP 이미지를 RAM 영역으로 복사해서 운용한다. 또한 재부팅 시 데이터를 유지하기 위한 NVRAM으로 구성된다. T/TA-50 메모리에 저장된 중요 데이터를 삭제하기 위해 항공기 조종석 내에 장착된 Zeroize Switch 또는 항공기에 장착된 주요 장비의 개별 Zeroize Switch를 작동시킴으로써 중요 데이터를 삭제할 수 있다. 또한 다른 항공기와 마찬가지로 비상상황 시 좌석 사출을 하게 되면 Zeroize Switch 동작과 동일한 작동을 수행한다[17]. Zeroize 동작 시 OFP의 NVRAM에 저장되어 있는 주요 데이터를 삭제하며, ROM에 저장된 비행운용프로그램은 삭제되지 않는다. 이러한 IMDC Zeroize 기능을 보완하기 위해 공군 자체적으로 '07년 ROM 영역 삭제 기능을 구현하였으며, 이는 Zeroize 수행 시 API를 이용하여 플래시 메모리에 접근할 수 있는 저수준의 입출력 접근 함수인 tffsClear(가상명칭) 함수를 사용하여 ROM 영역을 삭제할 수 있도록 구현하였다. IMDC에 Zeroize 신호가 전송되면 tffsClear에서 사용하는 함수 중 TFFS_PHYSICAL_ERASE를 이용하여 ROM 영역에서 비행운용프로그램이 위치하는 유닛을 삭제하도록 명령한다. 유닛이 삭제되면 비행운용프로그램 실행에 오류가 발생하며 OFP의 재부팅이 불가능하게 된다.

FA-50의 메모리는 xxxMbyte의 ROM, xxxMbyte의 RAM과 xxxKbyte의 NVRAM으로 구성된다. 각 메모리의 역할은 T/TA-50과 동일하며, Fig. 5의 Zeroize Switch 작동 또는 좌석 사출 시 주요 장비에 저장된 데이터 및 OFP의 NVRAM에 저장된 데이터만 삭제가 가능하다.

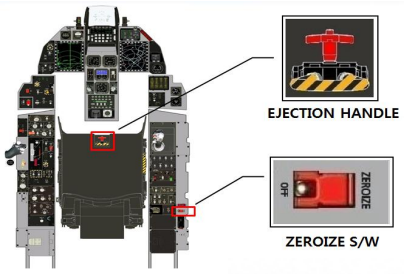



Fig. 5. FA-50 Zeroize Function[18]

# III. Software Design

## 1. CSCI Function

CSCI(Computer Software Configuration Item)는 최종적인 기능을 충족하기 위한 소프트웨어 프로그램의 집합체로써, 다양한 기능을 수행하기 위한 컴퓨터 소프트웨어의 구성품인 CSC(Computer Software Component)로 구성된다. FA-50 항공기 IMDC의 CSCI는 각각의 OFP가 이에 해당하며, CSC는 각각의 OFP 별로 다양한 기능을 수행하기 위한 단위모듈들의 집합이다[19].

FA-50 항공기 임무컴퓨터의 Zeroize 작동 시 보완기능을 구현하기 위해 개조되는 OFP는 FC OFP이며, 조종사 기재취급(PVI, Pilot Vehicle Interface)과 관련된 변경 사항은 없다. 즉, 조종사는 추가적인 조작 절차 없이 현재 Zeroize 조작 절차와 동일하게 작동시키면 기존 Zeroize 기능이 작동되면서 동시에 추가적으로 보완된 기능을 수행하도록 구현하였다.

## 2. Software Design of FC OFP

FC OFP는 Targeting을 위한 Sensor, Cursor 데이터 결정 및 계산, 무장 투하 알고리즘, HUD 및 MFDS 시현 심벌 위치 및 시현여부 결정, 통신 항법, Smart Weapon 무장 투하 기능 제공, Datalink 기능 제공 등 기능별로 구분된 총 24개의 Component로 구성된다[20]. 본 기능을 구현하기 위해 A(Point Management), B(Data Transfer) Component가 수정되었으며, 관련된 Component는 C(Smart Weapon), D(Data Management) Component이다.

FC OFP는 Zeroize System으로부터 IMDC Zeroize discrete 신호를 수신하며, FC OFP 내부 CSC의 역할은 Table 1과 같다.

Table 1. Flow chart of CEI frequency operation function of FC OFP

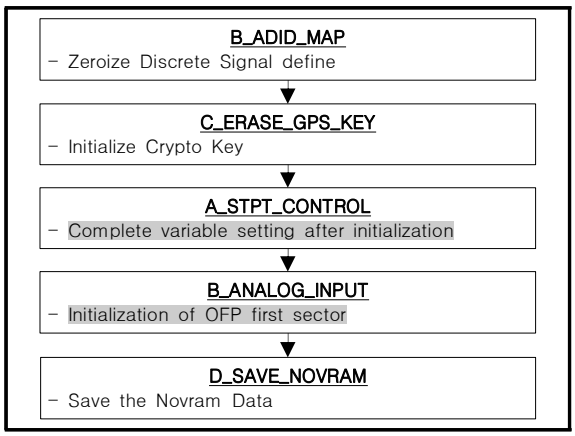
| Zeroize System |
|---|
| ↓ IMDC Zeroize(discrete) |
| **FC OFP** |
| **C Component**<br>- Smart Weapon related logic control<br>- Initialize SMS Data when Zeroize signal is received |
| **A Component**<br>- Steerpoint related logic control<br>- Initialize steerpoint and various reference point data when receiving zero signal<br>- Complete variable setting after initialization |
| **B Component**<br>- Perform discrete and analog signal input<br>- Zeroize signal reception and initialization Perform initialization of OFP first sector after receiving completion signal |
| **D Component**<br>- Saving and recalling data stored in NVRAM |

각 Component의 주요 기능을 살펴보면, 먼저 C Component는 Smart Weapon과 관련된 로직을 제어하는 역할을 수행하며, Zeroize 기능 작동 시 Smart Weapon과 관련된 주요 정보를 초기화 시킨다. A Component는 조종사 참조점과 관련된 로직을 제어하는 역할을 수행하며, Zeroize 기능 작동 시 참조점 관련 정보를 초기화 한다. B Component는 FC OFP에서 사용되는 In/Out 데이터를 정의된 주기에 따라 처리하는 기능을 수행한다. In/Out 데이터로는 1553B MUX Bus Data, Packet Data, Discrete/Analog Data가 있으며, 데이터의 유효성을 검사하고 입출력 처리를 수행한다. 마지막으로 D Component는 다른 OFP로부터 전송된 Change Request를 처리하는 역할을 수행하며, IMDC의 Power Cycle 발생 시 중요 데이터를 NVRAM에 저장하고 불러오는 기능을 수행한다 [21][22].

본 기능 구현을 위해 FC OFP는 Zeroize System으로부터 Zeroize Discrete 신호를 수신한다. FC OFP의 B Component에서는 Zeroize Discrete 신호를 수신하고 Time Scheduling의 처리 주기에 따라 Zeroize 기능을 수행한다. 먼저 50Hz 주기로 수행되는 C Component에서는 SMS의 버퍼에 남아있는 SMS 관련 Data를 지우기 위한 로직을 수행한다. SMS는 선택된 무장의 GPS를 운용하기 위해 DTRS로부터 SMS 관련 Data를 수신받으며, IMDC가 지정한 무장 Station으로 SMS 관련 Data를 전송해야한다. 이때 SMS Memory와 Input/Output 버퍼에 SMS 관련 Data가 남아있을 수 있으며, IMDC가 Zeroize 신호를 수신하면 SMS의 버퍼에 있는 SMS 관련 Data를 지우라는 명령을 전송한다. 25Hz 주기에서는 A Component에서 관리하는 Steerpoint와 각종 참조점을 초기화하는 로직을 수행한다.

A와 C Component에서 기존 Zeroize 기능이 먼저 수행된 후, 다음 50Hz 주기에서 비행운용프로그램을 초기화하기 위한 로직을 수행한다. Component 내부 모듈 간의 CSU (Computer Software Unit) 흐름도는 Table 2와 같다.

Table 2. Flow chart of CSU




비행운용프로그램을 초기화하기 위해서는 BAE사에서 제공한 API 상의 FlashClear() 함수를 사용하여야하며, ROM에 저장된 OFP 영역을 초기화할 수 있다. OFP Image가 저장된 ROM은 Sector 단위로 구성되어 있으며, 각 Sector는 xxx Kbytes이고 ROM 전체 영역 xxx Mbytes는 xxx Sector로 구성된다. 한 Sector를 초기화하는 시간은 1초 이내이며, 전체 메모리 영역을 초기화할 경우 약 16분 30초가 소요된다. 전체 메모리 영역을 초기화할 경우 장시간 소요되어 Zeroize 상황 발생 시 대처방안으로 부적합하며, OFP 부팅과 관련된 BIFI(Boot Image for IMDC2) Sector를 초기화하도록 구현하였다. OFP의 BIFI Sector는 OFP Image의 첫 번째 Sector에 포함되며, OFP Zeroize 명령 즉시 1초 이내로 초기화가 가능하다. FlashClear() 함수를 수행하기 위해서는 메모리에 접근하기 위한 FlashLockUnlock() 함수를 호출하여 Unlock 명령어인 U_Operation을 전송하여야 한다. 메모리 접근이 허용된 후 FlashClear() 함수를 호출하여 OFP Image의 Start_Address와 End_Address를 전송한다. OFP Image의 첫 Sector가 삭제된 후 메모리 접근을 해제하기 위해 FlashLockUnlock() 함수를 호출하여 Lock 명령어인 L_Operation을 전송한다. 다음은 메모리를 초기화하기 위한 함수의 구조를 나타낸다.

```
flashLockUnlock(Start_Address, End_Address, U_Operation);
flashClear(Start_Address, End_Address);
flashLockUnlock(Start_Address, End_Address, L_Operation);
```

메모리 초기화 명령을 수행하면 IMDC는 정해진 시간 내에 수행되어야 하는 Run time을 초과하여 Time-slice Timeout에 의한 Fatal Fault를 발생시키고 IMDC를 중단시킨다. IMDC 전원이 차단되면서 RAM에 저장된 OFP Image가 삭제되고, IMDC 재부팅 시 ROM에 저장된 OFP Image의 BIFI Sector가 초기화되었으므로 부팅이 불가능하게 된다. 즉, 본 개조를 통하여 ROM에 저장된 OFP Image의 일부분을 초기화시키고, 의도적인 Time Out 에러를 발생시켜 IMDC의 전원 공급을 강제적으로 중단시킴으로써 RAM에 저장된 OFP Image가 삭제되도록 구현하였다.

## IV. Experiment Result

본 개발 소프트웨어의 검증을 위해 기존 Zeroize 기능 작동 상태를 테스트하고, 추가적으로 구현된 OFP 초기화 기능이 정상적으로 작동하는지를 검증하였다. FA-50 항공기는 IMDC의 동작 불능 시 조종사가 최소한의 임무를 수행하기 위해 SMFD를 통한 백업모드를 제공한다. 이에 대한 검증을 위해 OFP 초기화로 인한 IMDC 전원 공급 중단 시 SMFD를 통한 백업 모드가 제공되는지를 검증하였다.

본 기능의 검증을 위한 시험 범주는 아래 Table 3과 같으며 소프트웨어 요구사항에 대한 PVI(Pilot Vehicle Interface) 구현 여부를 검증하였다.

Table 3. Test Category

| Test Category | Checklist |
|---|---|
| Functional | Functional review required during software development review |
| Performance | Check that the software is functioning properly within its intended operation range |
| Stress | Repeat the same procedure or check whether it works at the limit |

Zeroize 신호 전송 시 OFP를 초기화하기 위해 기존 기능이 먼저 수행되는지를 확인하였다. 아래 Table 4와 같이 SMS 버퍼에 SMS 관련 Data가 존재하지 않거나, 존재할 경우 Erase 명령을 보냈으나 오류가 발생한 경우에는 OFP를 초기화한다. 아래 Case 4번과 같이 오류가 발생하지 않았고 SMS 관련 Data가 존재할 경우에는 OFP를 초기화시키지 않고 32초(Erase 재 명령 및 확인 시간)간 대기하며, 32초 후에는 Case 5번과 같이 오류가 발생했더라도 OFP를 초기화하도록 수행한다.

Table 4. FA-50 IMDC OFP Test environment

| Case | SMS 관련 Data | Error occurred :"1" | OFP initialization |
|---|---|---|---|
| 1 | 0 (none) | 0 (normal) | Perform |
| 2 | 0 (none) | 1 (error occurred) | Perform |
| 3 | 1 (exist) | 1 (error occurred) | Perform |
| 4 | 1 (exist) | 0 (normal) | Can not perform |
| 5 | 1 (exist) | 32 seconds elapsed after Erase command | Perform |

C Component에서 수행하는 Steerpoint 및 각종 참조점 관련된 데이터가 초기화되었는지 여부를 확인하기 위해 *'STPT_ZERO_COMPLETE'* 변수를 조건으로 추가하였다. 위 두 가지 기존 기능이 수행된 후에 OFP 초기화를 수행하는지 여부를 Table 5와 같이 검증하였다.

Table 5. Result According to Test Case

| Case | STPT_ZERO_COMPLETE | OFP initialization | | Result |
|---|---|---|---|---|
| | | Expected value | Result value | |
| 1 | True | Perform | Perform | PASS |
| 2 | True | Perform | Perform | PASS |
| 3 | True | Perform | Perform | PASS |
| 4 | True | Can not perform | Can not perform | PASS |
| 5 | True | Perform | Perform | PASS |

또한, Table 6과 같이 OFP Zeroize를 수행하면 ROM 메모리에 저장된 OFP Image의 첫 번째 Sector가 정상적으로 초기화되었는지를 검증하였다.

Table 6. First Sector initialization result of OFP Image

| Command | Result value | Result |
|---|---|---|
| Start address of the first Sector | ffff ffff ffff ffff ffff ffff ffff<br>…<br>ffff ffff ffff ffff ffff ffff ffff | PASS |
| Last address of the first Sector | ffff ffff ffff ffff ffff ffff ffff<br>…<br>ffff ffff ffff ffff ffff ffff ffff | PASS |

※ The address of the sector is not provided for security purposes, and the default value is 'f'.

마지막으로 Time-slice Timeout으로 인한 Fatal Fault가 발생함으로써 IMDC가 중단되는지 확인하였다. 이를 검증하기 위해 실제 항공기와 동일한 환경으로 구성된 시험 장비인 AHB(Avionics Hot Bench)를 이용하여 각 Frame의 시간을 측정하였다. 그 결과 Zeroize 버튼을 누르는 순간 Idle Time 없이 각 Frame에 할당된 시간을 모두 사용하였으며, Clock Interrupt를 발생시킨 후 Time-slice Timeout이 발생하였다. Timeout 에러 발생으로 인해 SMFD의 Test 페이지에 IMDC022(SW Timeslice Timeout) Fault를 시현하였으며, IMDC 작동이 중단되었음을 확인하였다.

FA-50 항공기는 IMDC의 오류로 인해 중단되더라도 SMFD를 이용한 백업모드를 운용할 수 있다. 백업모드 운용을 위해 Avionics Power Panel에 위치한 AV FUNC S/W를 IMDC에서 MFD로 변경하면 백업모드로 전환된다.

또한 IMDC Zeroize 수행 후 IMDC 재운용을 위해 ORP(OFP Reprogramming) 프로그래머를 이용하여 새로운 OFP를 재로딩하면 정상적으로 운용이 가능하다.

## V. Conclusion

본 연구의 결론은 다음과 같다.

첫째, 본 연구를 통하여 각 항공기 기종별 메모리 구조를 비교 분석하였고, 특히 FA-50 항공기 주임무컴퓨터의 메모리 내부 구조를 파악함으로써 소프트웨어 개발 가능 영역을 확장하였다. 항공기 임무컴퓨터의 메모리 구조와 관련된 자료가 한정되어 있어 이를 연구하는데 한계가 있었으나, 메모리에 접근 가능한 함수들을 유추함으로써 향후 메모리 분석 및 개발에 유용하게 활용될 것이다.

둘째, 기존에 구현되어 있는 Zeroize 기능의 한계점을 보완함으로써 항공기에 내장된 군사자료의 보안성을 더욱 강화하였다. 무기체계 소프트웨어의 기술력이 전투력의 핵심자원으로 주목되고 있는 시점에서 항공기 주임무컴퓨터 소프트웨어에 내장된 자료의 중요성은 갈수록 증대되고 있다. 이에 따라 본 기능으로 항공기 주임무컴퓨터 소프트웨어에 접근할 수 없도록 구현함으로써 군사자료의 노출을 방지할 수 있게 하였다.

셋째, 비상상황 발생 시 Zeroize 버튼을 조작하거나 좌석 사

출만으로 신속하게 항공기에 내장된 군사자료를 제거함으로써, 군사자료 보호와 동시에 조종사의 생존성을 향상시키고자 하였다. 조종사의 군사자료 보호에 대한 임무부담을 경감시키고 안전하게 군사자료를 보호할 수 있도록 기존 Zeroize 절차에서 추가적인 조작이 불필요하도록 구현하였다. 조종사의 판단으로 Zeroize 기능을 동작시키더라도 FA-50 항공기는 백업모드를 통해 최소한의 임무를 지속해서 수행할 수 있다. 또한 하드웨어 손상 없이 ORP 프로그래머를 이용하여 비행운용프로그램을 재로딩하면 주임무컴퓨터의 재사용이 가능하다.

본 연구는 항공기 주임무컴퓨터의 메모리 구조를 분석하고 기존 Zeroize 기능의 한계점을 보완하여 더욱 강력한 보안체계를 마련하였다. 그러나 아직까지 우리 공군이 보유하고 있는 기술 자료에 한계가 있어 주임무컴퓨터의 메모리를 일부 분석하였으나, 전체적인 메모리 구조를 파악하는 데는 어려움이 있었다. 향후 본 연구를 바탕으로 전체적인 메모리 구조를 파악하고 주임무컴퓨터 소프트웨어를 통해 보안성을 더욱 강화시킬 수 있는 방안을 마련하기 위한 연구가 필요할 것이다.

현재 국내 항공 산업의 수준은 선진국 대비 매우 열악한 상태이다. 그러나 국내 항공 산업의 기술력 차이에도 불구하고 이를 발전시키고자 지속적으로 노력하고 있으며 이에 따라 국내 항공 산업은 빠르게 성장하고 있다. 이와 더불어 항공 산업이 발전하는 만큼 우리 기술력에 대한 보안성을 향상시키기 위한 방안이 모색되어야 할 것이다.

## REFERENCES


[1] Electronics and Telecommunications Research Institute, Technical Trends of Monitoring GPS Jamming, Electronic Telecommunications Trend Analysis, Vol. 26, No. 4, pp.115-122, 1 August 2011.

[2] Eun-Kyung You, and Hyeock-Jin Kim, “Implementation of CEI frequency operation function in IMDC for FA-50 aircraft”, Journal of the Korea Society of Computer and Information, Vol. 23, No. 1, pp. 1-7, 23 January 2018.

[3] Bae, Dal Hyeoung, “Direction for Development of Structure Centering around Cyber Warfare and Cyber-Psychological Warfare in the View-Point of Asymmetric Threats and 4th Generation of War”, The Journal of Strategic Studies, Vol. 22, No. 1, pp. 141-172, March 2015.

[4] Tae-Hee Heo, Noh-Soon Chang, and Sang-Ho Lee, “The 21C Information Warfare and Korea's Stragegic Choices”, Sejong Institute, Vol. 10, No. 2, pp. 73-100, June 2004.

[5] The Korea Times, “North Korea's information warfare capability issue is “North Korea's ability to hack in the advanced countries level””, 15 February 2000.

[6] Eun-Kyung You, TA-50 Implementation of air-to-ground fire protection software function. Journal of Air Force Academy Article, Vol. 67, No. 2. Dec 2016.

[7] Kyung-Hwan Heo, Sang-Myun Shin and Jeong-Ho Choi, Mission Computer Zeroize Function Software Design for the Korean Military Helicopter. The Society for Aerospace System Engineering, Vol. 2018, No 1, 25 April 2018.

[8] KAI, Avionics System User Manual for the FA-50 Program, 14 Dec 2012.

[9] Editorial Office, “Korean-American Fighter FA-50 Wired”, Defense & Technology, No. 430, pp. 28-31, 2014.

[10] Daily Economy, “Up to 4.5 tons of armbandable all-rounder... First Korean Fighter FA-50 Practice Placement”, No. 51, December 2014.

[11] KAI, Avionics System Introduction, Jul 2006.

[12] KIDA, FA-50 Mission Planning System Software User's Manual, 10 Jul 2012.

[13] KIDA, T/TA-50 Mission Planning System Software design specification, 10 Jul 2012.

[14] KAI, Integrated Mission/Display Computer Interface Description Document for the FA-50 Program, 31 Mar 2010.

[15] Lockheed Martin, Avionic System Manual for F16, 1 Nov 1993.

[16] Boeing, Familiarization Training for F-15K, 29 Nov 2004.

[17] Air Force, Operation Command Manual 3-1-2, FA-50 Basic Tactical Training.

[18] KAI, KTO 1A-50A-34-1-1, 30 Oct 2011.

[19] KAI, Electrical Signal Interface Control Document for the FA-50 program, 1 Aug 2010.

[20] KAI, Computer Program Product Specification for the FA-50 FC OFP, 1 Jun 2011.

[21] KAI, Avionics System Requirements Specification for the FA-50 Program, 30 Nov 2009.

[22] KAI, Computer Program Development Specification for the FA-50 FC OFP, 31 Aug 2010.

## Authors

Eun-Kyung You received the master's degree in department of Computer Engineering at Chungwoon University, Incheon, Korea, in 2018. She is responsible for T/TA/FA-50 aircraft mission computer programming at the Avionics Software Development Center, Republic of Korea Air Force. She is interested in embedded system, software engineering, software security, etc.

Chan-Gyu Bae received in master's degree in department of computer science at Korea National Open University Graduate School, Korea, in 2009. He is responsible for T/TA/FA-50 aircraft mission computer programming at the Avionics Software Development Center, Republic of Korea Air Force. He is interested in software engineering especially for the military division and studying data analysis and optimizing using perl and python.

Hyeock-Jin Kim Ph.D. degree in department of Computer Engineering, AJou University, Korea, in 1999. He is currently a professor in department of Computer Engineering, Chungwoon University. His research interests include CG, CAGD, embedded system, web technology, etc.