Journal of the KIMST, Vol. 28, No. 2, pp. 208-216, 2025
ISSN 1598-9127(Print) · 2636-0640(Online)
DOI https://doi.org/10.9766/KIMST.2025.28.2.208

Research Paper 제어·구동 부문

유도무기 발사통제기의 발사절차제어 분산화와 다운타임 구간의 메시지 전송 복원을 통한 고장감내 성능 향상 연구

권기용*,1) · 김현철1) · 정동윤1) · 정휘화1) · 장부철2) · 정광래2) · 고혜승2)

1) LIG넥스원㈜ 미사일시스템교전통제연구소
2) 국방과학연구소 제2기술연구원

Study on Improving Fault Tolerance Performance of Guided Weapon Fire Control Unit Through Decentralization of Fire Sequence Control and Message Transmission Restoration During Downtime Periods

Kiyong Kwon*,1) · Hyunchul Kim1) · Dongyoon Jeong1) · Hwihwa Jung1) · Bucheol Jang2) · Kwangrae Jeong2) · Hyeseung Koh2)

1) *Missile System Engagement and Control R&D, LIG Nex1, Korea*
2) *2nd R&D Institute, Agency for Defense Development, Korea*

(Received 5 November 2024 / Revised 13 January 2025 / Accepted 20 January 2025)

Abstract

This study focuses on improving fault tolerance performance of Guided Weapon Fire Control Unit(FCU) based on decentralizing fire control and improved redundancy. The hot standby redundant FCU converts the spare module into a service module when a service module malfunctions. In the improved system, uninterrupted launch is possible even when above transition occurs because fire sequence control was transferred from FCU to separate Missile Control Unit(MCU), and an additional message recovery process was designed to compensate for the loss of message transmission during the transition time. Through experiments, the fault tolerance performance of the FCU was verified by measuring the role switching performance and message recovery performance.

Key Words : Fire Control System(발사통제시스템), Fault Tolerance System(고장감내시스템), Hot-Standby Sparing Technique(핫 스탠바이 스페어링 기법)

1. 서 론

임베디드 시스템이 적용되는 환경은 아주 엄격한 신뢰성과 가용성을 요구하는 경우가 많다. 특히 항공

* Corresponding author, E-mail: kiyong.kwon1@lignex1.com

및 국방 분야 등 시스템 고장으로 인해 인명 피해 또는 생존률 저하를 야기할 수 있는 미션 크리티컬 시스템(Mission Critical System)의 고장감내 설계는 더 엄격하게 이루어지는 것이 일반적이다[1]. 고장감내 시스템이란 일부 하드웨어 또는 소프트웨어에서 구성 요소에 장애가 발생하더라도 전체적으로 정상적인 동작을 이어나갈 수 있도록 설계된 컴퓨터 시스템을 일컫는다[2]. 최근에는 임베디드 시스템에도 하드웨어 성능 향상 및 소프트웨어 기술의 발전으로 인해 하드웨어 이중화 없이 고장감내 성능을 향상시키는 다양한 연구가 진행 중이다[2,6]. 그러나 미션 크리티컬 시스템에는 여전히 다중화된 하드웨어 기반의 고장감내 설계가 널리 활용되고 있으며 본 연구의 배경이 되는 유도무기 발사통제장비도 마찬가지다.

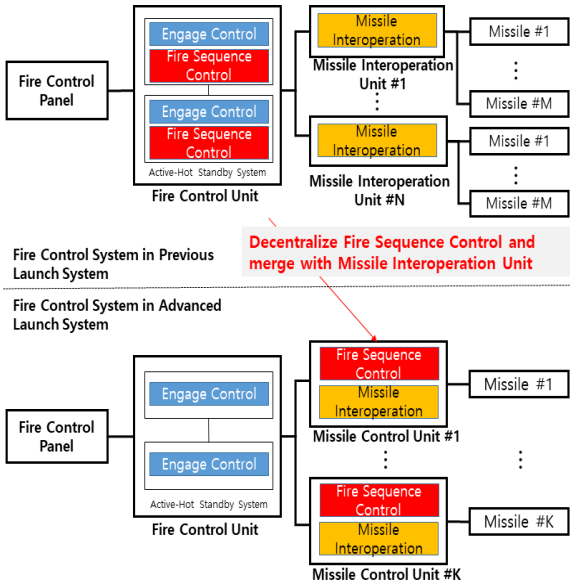


Fig. 1. Comparison of previous and improved fire control system

본 연구의 발사통제시스템은 함정의 발사대에서 동작하는 유도탄을 제어의 대상으로 하며, 분산화 된 발사절차제어와 서비스 모듈 고장 시 발생하는 다운타임 구간의 메시지 전송 복원을 통한 발사통제기의 고장감내 성능 향상을 주제로 한다. Fig. 1은 기존 발사대와 개선된 발사대에서 동작하는 발사통제시스템(Fire Control Systems)의 연동 구성을 비교하여 나타내고 있다. 기존에는 발사통제기(Fire Control Unit)에서 교전제어(Engage Control)와 함께 유도탄(Missile)의 발사절차제어(Fire Sequence Control)를 수행하였다. 발사통제기는 핫 스탠바이 스페어링(Hot Standby Sparing) 방식으로 동작하여 서비스 모듈에 고장이 발생할 경우 여분 모듈로 전환된다. 기존 발사통제시스템의 발사통제기는 모든 유도탄의 발사절차 제어를 중앙집중화(Centralized)하여 처리하며, 서비스 모듈과 여분 모듈은 하나의 장비 내에 배치되었다. 이로 인해 서비스 모듈의 고장 원인이 여분 모듈의 발사절차 진행에 영향을 줄 수 있는 가능성을 고려하여 진행 중인 모든 유도탄의 발사절차가 즉시 중단되고 운용자의 확인 후에 재개가 가능하였다. 이는 특정 초읽기 구간에서 중단 시, 해당 탄을 일정 시간 또는 영구적으로 사용할 수 없게 되어 전투력이나 비용 손실을 발생시킬 수 있다. 개선된 발사통제기는 발사절차 제어를 별도 장비로 분산화(Decentralize)하여 발사통제기의 모듈 간 전환이 일어나더라도 발사절차에 고장이 전파되지 않아 중단 없이 발사절차 진행이 지속 가능하도록 하였다. 또한, 서비스-여분 모듈 역할 전환 간 발생하는 메시지 전송 소실을 보상하는 고장감내 기법을 고안하였다. 기존 발사통제기는 서비스 모듈 고장 시 발생하는 다운타임 구간에서 발생하는 메시지 전송 누락을 고려하지 않았다. 이는 초읽기 구간에서 발사절차제어를 담당하는 장비로 교전정보 전송이 누락될 경우, 발사절차의 비정상 종료 가능성을 내포한다. 이를 메시지 전송 복원을 통해 해결하여 발사통제기 서비스 모듈 고장이 발생하더라도 중단 없는 발사절차가 가능하도록 하였다.

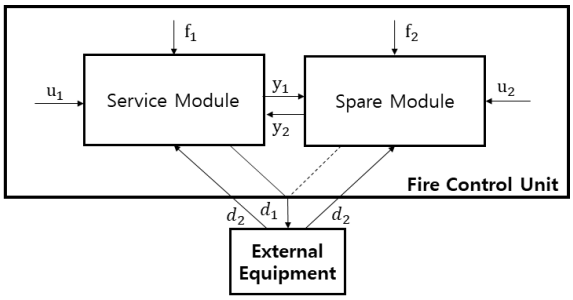
본 논문의 구성은 다음과 같다. 2장에서는 발사통제기의 고장감내 시스템에 대한 기본적인 설계 내용을 소개한다. 3장에서는 본 연구에서 고안한 발사절차 제어의 분산화와 다운타임 구간의 메시지 전송 복원 내용에 대해 상세하게 서술한다. 분산화 된 발사절차 제어 동작, 발사통제기 모듈 별 역할 할당 및 고장탐지 절차, 메시지 전송 복원 프로세스에 대한 상세 설계 내용에 대해 다루었다. 4장에서는 발사통제기 고장감내 시스템에 대한 성능평가를 진행한다. 발사통제기에 부하 상황을 나누어 고장을 주입하고 역할 전환 속도 및 복원된 메시지수를 측정한다. 동시에 개발벤치 내 유도탄제어기에서 무중단으로 발사절차를 수행하는지 확인하였다. 5장에서는 본 연구의 결론에 대해 서술하였다.

2. 발사통제기 고장감내 이중화 시스템 소개

이 장에서는 이중화된 발사통제기의 고장감내 시스템에 대한 일반적인 내용을 소개한다.

2.1 발사통제기 이중화 방식 및 구조

하드웨어 다중화 방식은 서비스를 수행하는 모듈, 서비스 수행 모듈과 동일한 형태의 여분 모듈들로 시스템을 구성하여 서비스 수행중인 모듈에 고장이 발생하면 여분의 모듈이 서비스를 계속 수행할 수 있도록 한 방식이다[3]. 발사통제기의 각 모듈은 제어용 보드, 통신용 보드, 전원공급장치 및 외부 연동 케이블까지 모든 하드웨어가 중복으로 구성된다. 하드웨어의 다중화 방식은 콜드 스탠바이, 웜 스탠바이, 핫 스탠바이 스페어링 기법이 대표적이다[4]. 본 연구의 발사통제기는 핫 스탠바이 방식으로 이중화 설계 되었다. 장비 전원 인가 시, 서비스 모듈과 여분 모듈에 동시에 전원 공급이 되며, 각 모듈에는 동일한 소프트웨어가 탑재되어 동일시간 동일 동작을 수행하며 동기 상태를 유지하는 방식이다.



u_1, u_2: Module Status
f_1, f_2 : Unexpected Fault
y_1, y_2: Heartbeat Message
d_1, d_2: Send/Receive Message

Fig. 2. Block diagram of fault tolerance system for engagement control unit

Fig. 2는 본 연구의 발사통제기의 고장감내 설계 내용을 블록다이어그램으로 나타낸 것이다[5]. 각 모듈은 BIT(Built In Test) 및 케이블 연결 상태를 종합한 모듈 상태 정보와(u1, u2)와 고장(f1, f2) 상황을 입력 파라미터로 하여 상대 모듈에 HeartBeat 메시지(y1, y2)의 송신 유무를 결정된다. 모듈에 이상이 발생하거나 역할이 할당되지 않은 경우, 상대 모듈에 HeartBeat 메시지 송신이 중단된다. 각 모듈에서는 일정시간 동안 HeartBeat 메시지가 수신되지 않으면 상대 모듈을 고장으로 판단하고 고장시스템 상태를 변경하게 된다. 각 모듈은 외부장비로부터 동일한 데이터를 수신(d2)하며, 각 모듈의 역할에 따라 외부 메시지 전송(d1) 주체가 결정된다.

2.2 발사통제기 고장감내 시스템 상태

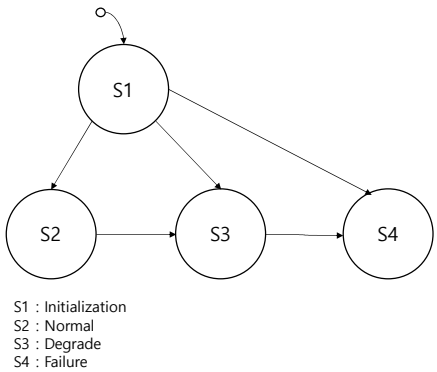


Fig. 3. Transition diagram of fault system state

Table 1. Role definition based on fault system state

	S1 Init	S2. Normal	S3. Degrade		S4. Failure
Service Module Role	No Role	Primary	Primary	No Role	No Role
Spare Module Role	No Role	Secondary	No Role	Primary	No Role

Fig. 3은 발사통제기 고장감내 시스템 상태 천이도를 나타내며, Table 1은 시스템 상태 별 서비스 모듈과 여분 모듈의 역할 할당 케이스를 나타낸다. 각 모듈이 가질 수 있는 역할은 총 세 가지로 역할 없음(No Role), 주(Primary), 부(Secondary)가 있다. 초기화(Initialization) 상태는 최초 전원인가 시 1회만 진입하는 상태로 연동 초기화를 통해 서로의 상태를 확인하고 동작에 필요한 설정파일을 동기화 한다. 또한, 각 모듈은 상호 확인된 모듈 상태를 기반으로 역할 할당을 수행한다. 두 시스템이 모두 정상이라면, 초기화 상태에서 정상(Normal) 상태로 천이하며, 서비스 모듈

이 '주' 로, 여분 모듈이 '부' 로 역할이 할당된다. 이 상태에서는 상호 상태를 주기적으로 감지하여 동일시간 동일 동작을 수행하는 핫 스탠바이 이중화가 수행된다. 성능 저하(Degrade) 상태란 두 시스템 중 하나의 시스템에 고장이 발생해 정상적으로 동작을 하고 있지 않은 상태를 말한다. 만약, 초기화 단계에서 기본 서비스 모듈과 여분 모듈 둘 중 하나에 고장이 발생한 경우, 정상인 모듈에서는 상대방의 고장을 인지하고 성능 저하 상태로 진입한다. 또한, 동작 중 고장이 발생한 경우에도 동일한 형태로 성능 저하 상태로 천이하게 된다. 고장(Failure) 상태란 중복으로 구성된 두 모듈에 모두 고장이 발생한 상태이다. 초기화 단계에서 두 시스템에 모두 고장이 감지되거나, 성능 저하 상태에서 정상인 모듈마저 고장 시 천이하게 된다. 고장 상태에서는 어떠한 상태로도 천이가 불가하며, 운용자의 조치를 대기한다.

3. 발사통제기 발사절차 분산화 및 메시지 전송 복원을 통한 고장감내 성능 향상

이 장에서는 발사절차의 분산화와 메시지 전송 복원을 고안하여 발사통제기의 고장감내 성능을 개선한 내용에 대해 소개한다.

3.1 발사절차 분산화를 통한 고장감내 성능 향상

본 연구에서는 발사통제기에서 발사절차를 분산화하여 발사통제기 내의 서비스 모듈 고장에 의해 스페어 모듈로 전환 시에도 발사절차에 고장이 전파되지 않고 지속 수행되도록 하였다. Fig. 4는 기존 시스템에서 발사절차 도중 발사통제기의 서비스 모듈 고장 시 동작을 흐름도로 나타낸 것이다. 유도탄에 대한 발사절차가 하나의 하드웨어 내에 배치되어 있는 서비스/여분 모듈에서 중앙 집중화되어 처리되므로, 감지 및 전환 시간 동안 발사절차에 이상이 생겼을 가능성을 고려하여 발사절차는 즉시 중단되고 운용자를 확인을 통해서만 재개할 수 있도록 하였다. 결과적으로 발사중지 및 시간 지연은 불가피하며, 특정 초읽기 구간에 발사중지가 되었을 경우, 해당 탄을 일정 시간이나 영구적으로 사용할 수 없게 되어 전투력이나 비용 손실이 발생하게 된다. Fig. 5는 개선된 시스템의 동일한 동작을 흐름도로 나타낸 것이다. 개선된 시스템에서는 발사절차제어 기능을 분산화하고 이를 유도탄

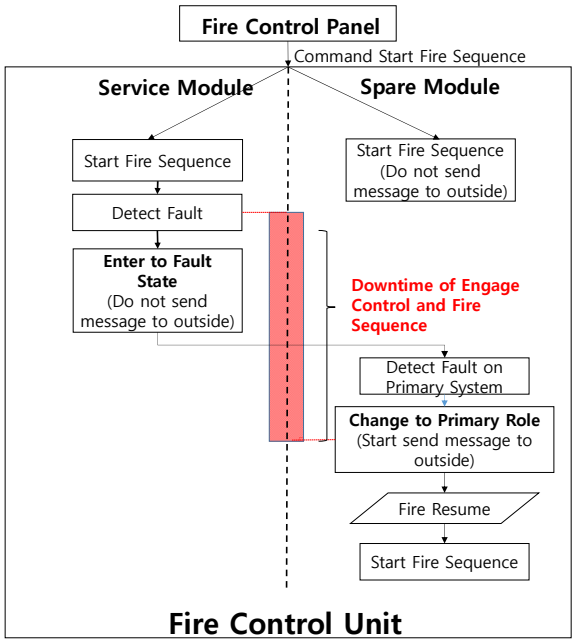


Fig. 4. Flow diagram of fire sequence with main module failure in the previous system

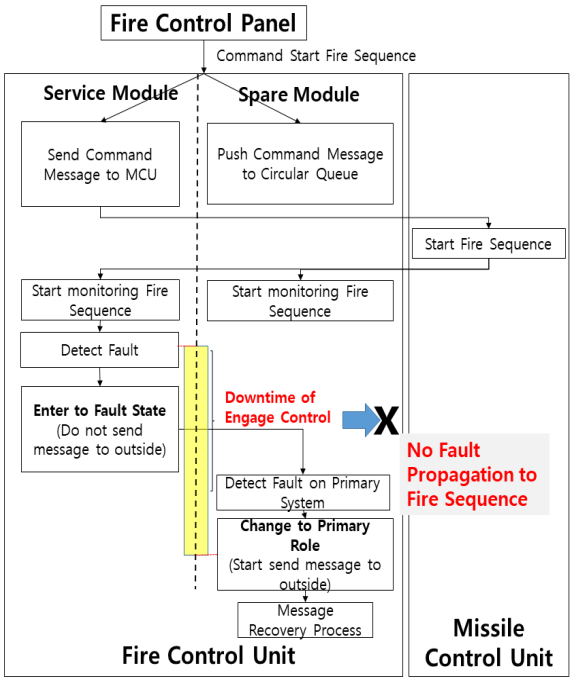


Fig. 5. Flow diagram of fire sequence with main module failure in the advanced system

연동기에 통합하여 별도의 장비인 유도탄제어기를 구성하였다. 발사통제기의 서비스 모듈은 발사통제콘솔로부터의 발사명령 전달 후에는 발사절차에 대한 모니터링 및 임무자료장입만 수행한다. 따라서 발사통제기의 서비스 모듈에 고장이 발생하더라도 발사절차에는 고장이 전파되지 않아 별도 운용자 확인 없이 무중단 발사가 수행 가능한 구조이다.

3.2 발사통제기 스페어 모듈 전환 시 메시지 전송 복원을 통한 고장감내 성능 향상

기존 시스템에서는 발사통제기의 서비스 모듈 고장 시 발생하는 다운타임 구간에서 발생하는 메시지 전송 누락을 고려하지 않았다. 발사절차가 즉시 중단되고, 운용자의 재확인 후에 발사절차 재개가 결정되기 때문에 다운타임 구간의 메시지 전송 누락으로 발생할 수 있는 문제를 운용자의 조치에 맡길 수 있었다. 그러나 본 연구에서 목표로 하는 핵심기능인 중단 없는 발사절차 달성에는 다운타임 구간 메시지 전송 누락이 치명적이었다. 예를 들어 교전정보를 장입하는 초읽기 시점에 다운타임이 발생한다면, 여분 모듈로의 전환이 정상적으로 이루어진다고 하더라도 교전정보 장입 실패로 발사절차가 비정상 종료되게 된다. 이를 해결하기 위해 서비스-여분 모듈 역할 전환 간 발생하는 메시지 전송 복원 기법을 고안하였다.

3.2.1 역할전환 감지 및 메시지 복원 판단 흐름도

Fig. 6은 개선된 시스템에서 이중화 동작을 수행하는 발사통제기에서 주기적으로 수행되는 상대 모듈 감시 및 메시지 복원 판단 절차를 흐름도로 표현한 것이다. 첫째, 현재 할당된 역할을 확인한다. 만약 '역할 없음' 일 경우, 어떠한 절차도 수행하지 않는다. 둘째, 자기 장비 상태를 확인한다. 비정상으로 판단 시 '역할 없음' 으로 할당하며 정상일 경우 상대방 모듈에 HeartBeat 메시지를 송신한다. 셋째, 상대방 모듈과의 링크 상태를 확인한다. 상대방 모듈이 만약 비정상이라면 HeartBeat 메시지가 송신되지 않으므로 링크가 비정상으로 식별된다. 따라서 여분 모듈이라면 링크가 비정상인 상황에서 자기 자신의 역할을 '부' 에서 '주' 로 전환하게 되어 메시지 복원 프로세스를 수행하게 된다. 서비스 모듈일 경우 기존에 수행중인 '주' 역할을 지속한다. 넷째, 링크가 일시적인 통신 불량으로 인해 여분 모듈의 역할이 '주' 로 전환되어 서로 자기 자신의 역할을 '주' 로 오해하고 동작하는 상황에 대한 예외 처리 단계이다. 두 개의 모듈이 모두 주 시스템으로 동작하면 액티브 핫 스탠바이 형태가 아닌 액티브 액티브 형태로 동작하게 된다. 이를 방지하기 위해 서비스 모듈에서는 여분 모듈의 역할을 주기적으로 확인하여, 여분 모듈에서 한 번이라도 '주' 역할을 주장할 경우, '역할 없음'으로 강등시키도록 하였다. 민수 분야에서 많이 볼 수 있는 방식으로 고장으로부터 복구된 모듈의 역할을 런타임 단계에서 복원하도록 구성할 수도 있지만[7], 기능의 단순화로 얻을 수 있는 장점과 낮은 고장률을 고려하여, 한 번 문제가 생긴 모듈의 경우 운용자 조치를 통해 문제를 해결하는 기존 방식을 고수하였다.

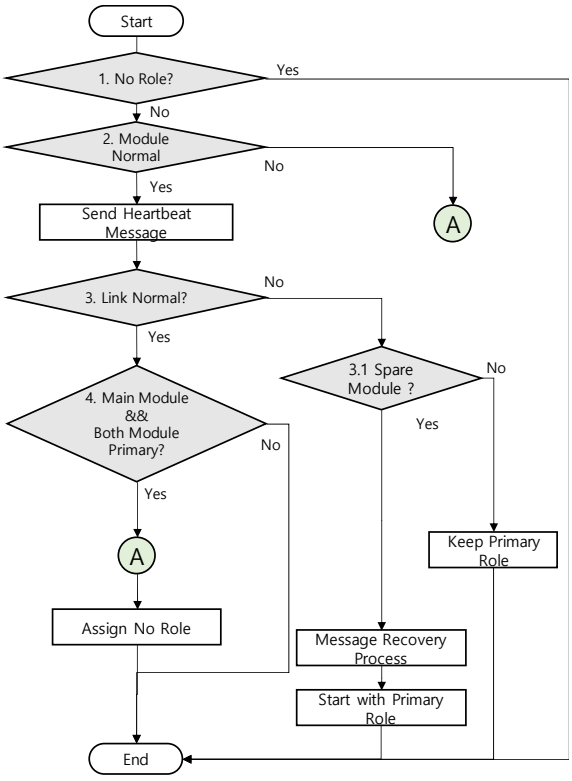


Fig. 6. Periodic fault detect process of the fire control unit

3.2.2 여분 모듈의 메시지 전송 복원

Fig. 7은 개선된 시스템에서의 메시지 전송 복원 기능을 표현한 것이다. 정상 상태에서 발사통제기 여분 모듈은 외부로 메시지를 송신하지 않고 메시지 복원용 원형 큐에 삽입한다. 이는 발사통제기의 역할 전환

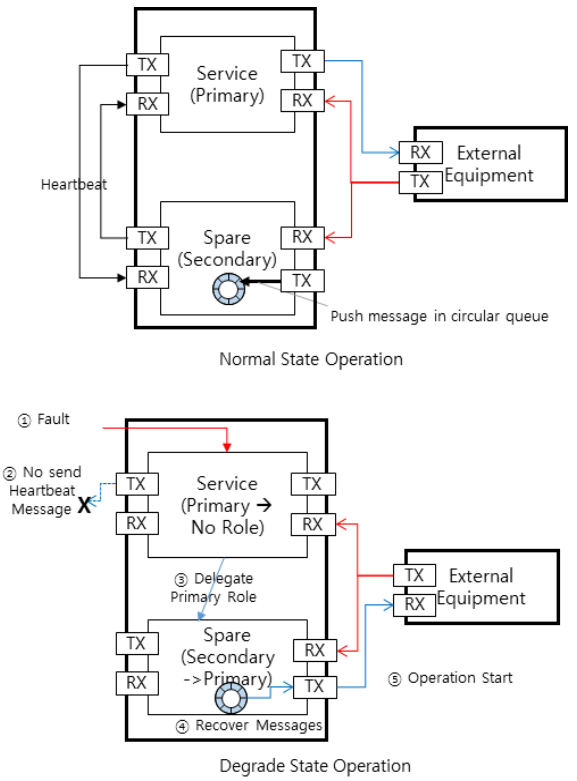


Fig. 7. Operation of fault system state

시 다운타임 간 외부장비들로 메시지 전송을 복원하기 위함이다. 해당 시간 동안 메시지가 소실되면 발사절차 비정상 종료, 전시 및 이력 누락을 야기할 수 있다. 정상 상태에서 서비스 모듈에 고장이 발생한 경우는 아래와 같이 순차적으로 설명이 가능하다. 서비스 모듈에 고장이 발생한다(①), 서비스 모듈에서 HeartBeat 메시지가 전송되지 않는다(②). 여분 모듈은 고장감지 판단 시간인 260 msec 동안 서비스 모듈에서 메시지가 수신되지 않으면 고장을 감지하고, 본인의 역할을 '주'로 전환(③)함과 동시에 성능 저하 상태로 천이한다. 역할이 전환된 즉시 260 msec 내에 삽입된 메시지들을 원형 큐에서 꺼내서 재송신하는 복원 프로세스를 수행한다(④). 이후 정상적인 동작을 진행한다(⑤). 이와 같은 복원 기능은 액티브 핫 스탠바이 시스템에서 다운타임 시간 내의 메시지를 놓치지 않고 전달할 수 있다는 장점이 있지만 같은 메시지가 다른 시스템에 두 번 전달될 수 있어 대비가 없다면 다른 시스템의 비정상 동작을 발생시킬 수 있다. 예를 들어, 외부 연동과 관계없는 영역의 고장이었을 경우에는 전환 중에도 정상적으로 외부 메시지가 전송이 이루어졌을 수 있다. 발사통제시스템 내의 각 장비에는 물리적 이중화 망, 재전송 메시지 등으로 인해 동일한 메시지 수신에 대비한 중복처리 방지 매커니즘이 기본적으로 반영되어있다. 각 장비는 수신된 메시지 종류 별로 시퀀스 번호를 별도로 관리하여 지나간 시퀀스 번호의 데이터는 처리하지 않게 되며, 복원 전송 메시지들에 대해서도 동일하게 동작하여 비정상 동작 방지가 가능하다.

4. 발사통제기 고장감내 설계 성능 평가

4.1 실험구성 및 시나리오

본 연구에서 개선한 발사통제장비의 고장감내 설계 성능 평가를 위해 Fig. 8, 9와 같이 시험구성을 하였다. 먼저 운용자의 인터페이스가 구성되는 화면부는 별도 시뮬레이터로 구성하였다. 발사통제기는 실제 장비와 동일 모델의 SBC(Single Board Computer)로 만들어진 시험치구 2기를 활용하여, 실 장비에 탑재되는 소프트웨어와 동일한 형상을 탑재하여 모의하였다. 유도탄제어기의 경우, 복수의 교전 모의를 위해 개발벤치로 모의하였다. 단, 실제 장비와 동일하게 메시지와 동작을 모의하도록 함으로써 제시된 실험 시나리오를 통한 성능 검증이 가능하도록 하였다. 그 외 발사통제기와 연동하는 타 체계에 대한 모의는 개발벤치 내에 구성하여 시험을 진행하였다. 메시지에 대한 수집/분석 진행 및 복원 성능 측정을 위해 데이터수집장치(Data Acquisition System) 장비를 활용하였다.

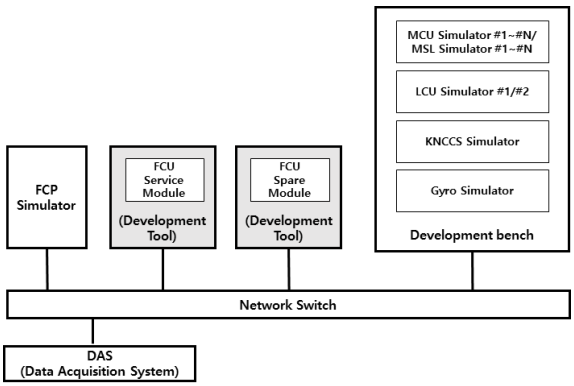


Fig. 8. Interoperation of environment for verification of fault tolerant performance

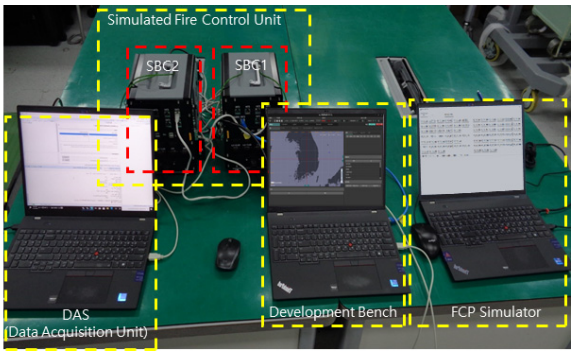


Fig. 9. Test environment for verification of fault tolerant performance

실험 시나리오는 Table 2와 같이 동시 교전하는 유도탄의 개수(Number of Engaged MSL : 4, 8, 16)를 통해 발사통제기에 걸리는 부하에 차이를 두었다. 그리고 유도탄 발사 초읽기 진행 중 특정 시간에 서비스 모듈에 고장을 주입하여 외부로 송신되는 모든 메시지를 즉시 차단하였다. 여분 모듈에서는 이를 감지하여 역할 전환을 수행하게 되며, 비교를 위해 서비스 모듈과 여분 모듈이 모두 정상인 상태에서의 동일한 동작으로 벤치마크 모델을 설정하였다. 측정 데이터로는 초읽기 중 6초 정도 시간을 추출하여 발사통제기가 송신한 메시지의 수, 역할 전환 과정에서의 메시지 복원에 소요되는 시간 및 복원된 메시지 수 및 외부로 메시지 전송이 차단되는 다운타임 시간을 측정하였다. 발사절차 제어를 수행하는 유도탄제어기는 발사통제기로부터 500 msec 동안 Heartbeat 메시지 미 수신 시, 발사절차를 비정상 종료하도록 설계하였다. 발사통제기의 서비스/여분 모듈은 고장 발생 시점부터 260 msec 시간을 기준으로 역할 전환이 진행되지만, 발사통제기와 유도탄제어기와의 통신단절에는 240 msec의 마진을 더 고려하여 500 msec로 결정한 것이다. 실험에서는 다운타임 시간이 500 msec 이내로 측정되어 유도탄제어기에서 중단 없이 발사절차를 수행함을 확인하는 것을 목표로 하였다. 각 케이스별로 실험은 5회씩 실시하고 평균을 측정하였다.

4.2 실험결과 및 분석

실험결과 Table 2와 같이 유도탄제어기에서 통신단절을 판단하는 기준시간인 500 msec 이내에 역할 전환과 메시지 복원이 수행되며, 개발벤치 내 유도탄제어기에서 무중단으로 발사절차를 수행함을 확인하였다. 또한 발사통제기가 외부와 통신이 단절되는 다운타임 시간이나 메시지 복원에 소요되는 시간도 교전 진행 중인 유도탄 수에 영향이 없음을 확인하였다. 이는 역할 전환 프로세스를 담당하는 태스크의 우선순위를 높게 설정하여 가장 우선적으로 메시지 복원 및 역할전환을 수행하도록 한 것에 기인하였다. 송신 메시지나 복원 메시지의 수는 교전 유도탄 수와 특별한 상관관계가 없는 것을 알 수 있었다. 이는 교전 유도탄 정보를 몇 개씩 묶어서 메시지를 구성하기 때문이며, UDP 통신의 패킷소실 및 데이터수집장치의 메시지 수집 누락 가능성도 영향을 미칠 수 있다.

메시지 복원에 대한 효과 및 실제 측정한 다운타임 시간은 Fig. 10의 그래프로 나타내었다. 그래프가 계단식으로 보이는 이유는 여러 통신 태스크가 통합된 하나의 타이머를 통해 메시지를 주기적으로 송신하는 것이 그 이유이다. 역할 전환이 일어나면, 통신을 수행하는 각 태스크에서 메시지 복원을 수행을 최우선을 수

Table 2. Test case for verification of fault tolerant performance

Number of Engaged MSL	Normal Case		Main Module Fault Case				
	Number of Sending Message within Count Down (Only 6 sec)	Lift Off	Number of Sending Message within Count Down (Only 6 sec)	DownTime	Number of Recovered Message	Message Recovery Time	Lift Off
4	3236	Success	3221	263 msec	100	32 msec	Success
8	3381	Success	3318	263 msec	100	33 msec	Success
16	3524	Success	3460	263 msec	102	33 msec	Success

행하는 것을 그래프에서 급격하게 송신 패킷 수량이 올라가는 추이를 통해 알 수 있다. 또한 모듈 간 전환이 일어나지 않는 정상발사와 비교하여 다운타임 기간 내에 소실될 수 있는 메시지 송신 소실을 대부분 보상함을 확인할 수 있다. 단, 실제로 측정된 다운타임 시간의 평균은 263 msec로 모듈 간 고장을 판단하는 기준 시간이자 메시지 복원하는 시간인 260 msec 보다 평균적으로 3 msec 더 길다. 이 오차는 Heartbeat 메시지의 송/수신 주기 타이머와 고장 판단의 기준이 되는 통신 단절 확인 타이머가 별도로 동작한다는 점, 역할 전환 소요시간 및 메시지 송/수신 소요시간 등에 기인함을 확인할 수 있었다. 이를 통해 이 오차시간 동안 메시지 송신 이벤트가 발생한다면 해당 메시지는 소실될 가능성이 있음을 확인할 수 있었다.

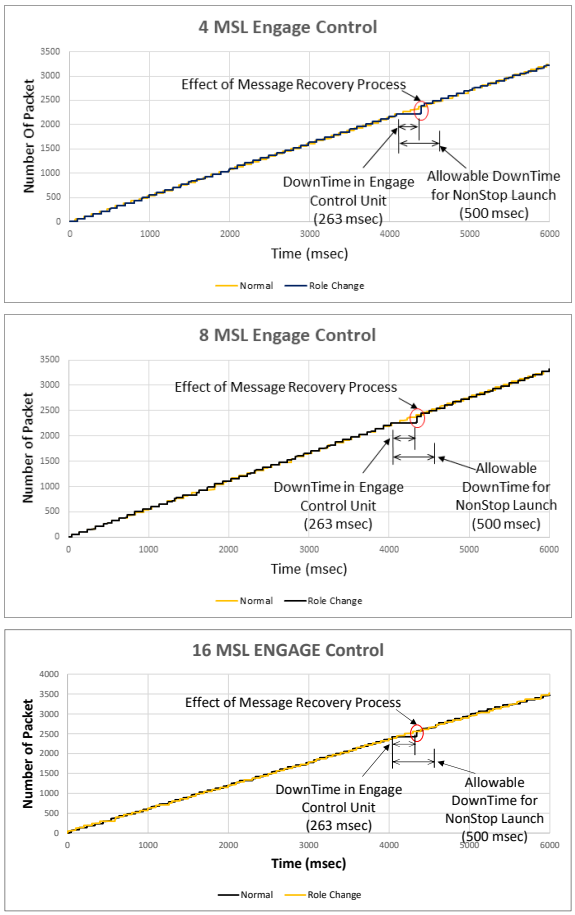


Fig. 10. Number of sending message during missile countdown in fire control unit

5. 결론

본 연구를 통해 핫 스탠바이 방식으로 이중화된 발사통제기에서의 고장 발생 시에도 유도탄의 무중단 발사절차 달성을 위한 개선된 고장감내 설계를 수행하였다. 기존시스템은 발사통제기의 서비스 모듈과 여분 모듈 간 전환이 일어나더라도 발사절차는 즉시 중단되게 되며, 운용자 확인을 통해 발사재개가 가능한 구조였다. 개선된 시스템에서는 발사통제기 내의 발사절차의 분산화와 다운타임 시간 동안의 메시지 전송 복원을 통해 발사통제기에서 역할 전환이 일어나더라도 발사절차는 중단 없이 진행이 가능하도록 하였다. 특정 초읽기 구간에서 발사절차가 중단될 경우, 해당 탄을 다시 사용하지 못하거나 일정 시간 대기해야만 하는데, 유도탄의 고도화로 인한 비싼 가격과 급박한 현대전 양상을 고려하면, 운용자가 의도하지 않은 발사중단 가능성을 최소화 하였다는 것에 의미가 있다. 또한, 다운타임 시간 동안의 메시지 전송 복원은 발사절차 수행 중이 아닐 시에도 타 체계로의 메시지 송신이 누락될 가능성을 감소시키는 효과가 있다.

개선된 발사통제기의 고장감내 성능을 확인하기 위해 실험을 통해 정상적인 초읽기 수행과 역할 전환이 발생한 초읽기 수행 간의 메시지 전송 추이 비교를 수행하였다. 이중화된 발사통제기가 기준시간 이내에 서비스 모듈과 여분 모듈의 역할 전환이 수행되어 초읽기가 정상적으로 수행됨을 확인하였으며 목표한 성능을 달성함을 확인하였다. 단, 메시지 복원 기준 시간에서 오류 탐지 및 역할 전환에 걸리는 실제적인 소요시간을 추가적으로 고려한다면 복원 성능이 향상 가능함을 유추할 수 있었다.

후 기

이 논문은 2024년 정부(방위사업청)의 재원으로 국방과학연구소의 지원을 받아 수행된 연구임.

References

[1] Victor P. Nelson, “Faut-Tolerant Computing: Fundamental Concepts,” Computer, Vol. 23, No. 7, pp. 19-25, 25, 1990.

[2] S. Son, “Improving Availability of Embedded Systems Using Memory Virtualization,” Journal of The Korea Society of Computer and Information Vol. 27, No. 5, pp. 11-19, 2022.
[3] J. Shin, D. Park, “The Implementation of Fault-Tolerant Dual System Using the Hot-Standby Sparing Technique,” Korea Institute of Communication Sciences, Vol. 29, No. 10A, pp. 1113-1122, 2004.
[4] Dhiraj K. Pradhan, “Fault-Tolerant Computer System Design,” PRENTICE HALL, 1996.
[5] Hassan Noura, Didier Theilliol, Jean-Christophe Ponsart, Abbas Chamseddine, “Fault-tolerant Control Systems: Design and Practical Applications,” Springer Science and Bussiness Media, 2009.
[6] S. Kwon, S Jung, “Virtualization based high efficiency naval combat management system design and performance analysis,” Journal of The Korea Society of Computer and Information, Vol. 23, No. 11, pp. 9-15, 2018.
[7] D. Kim, D. Kim, J. Lee, J. Namgung, “A Study on Arbitration Control Method of Steer-by-Wire System in Dual Redundancy Environments,” Journal of Transaction of Korean Society of Automotive Engineers, Vol. 31, pp. 143-151, 2021.