Journal of The Korea Society of Computer and Information
Vol. 21 No. 10, pp. 125-133, October 2016
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2016.21.10.125

The Design of Fault Tolerant Dual System and Real Time Fault Detection for Countdown Time Generating System

Jeong-Seok Kim*, Yoo-Soo Han**

Abstract

In this paper, we propose a real-time fault monitoring and dual system design of the countdown time-generating system, which is the main component of the mission control system. The countdown time-generating system produces a countdown signal that is distributed to mission control system devices. The stability of the countdown signal is essential for the main launch-related devices because they perform reserved functions based on the countdown time information received from the countdown time-generating system.

Therefore, a reliable and fault-tolerant design is required for the countdown time-generating system. To ensure system reliability, component devices should be redundant and faults should be monitored in real time to manage the device changeover from Active mode to Standby mode upon fault detection. In addition, designing different methods for mode changeover based on fault classification is necessary for appropriate changeover.

This study presents a real-time fault monitoring and changeover system, which is based on the dual system design of countdown time-generating devices, as well as experiment on real-time fault monitoring and changeover based on fault inputs.

▸ Keyword : Mission Control System, Changeover Software, Fault Monitoring, Dual System

• First Author: Jeong-Seok Kim, Corresponding Author: Yoo-Soo Han
*Jeong-Seok Kim (ryankim@kari.re.kr), Dept. of Computer Engineering, Chung-Nam National University / Dept. of Flight Safety Technology Team, KARI
**Yoo-Soo Han (yshan@kari.re.kr), Dept. of Electronic Engineering, Kyungpook National University / Dept. of Flight Safety Technology Team, KARI
• Received: 2016. 09. 24, Revised: 2016. 09. 28, Accepted: 2016. 10. 08.
• This Paper("Research on the Changeover Software for Duplicated Countdown Time Generating Device of the Mission Control System") was announced in The 2016 Fall Conference of The Korea Society of Computer and Information and extended for the Journal of The Korea Society of Computer and Information.

I. Introduction

발사통제시스템의 주요 장치 중 하나인 카운트다운 타임 생성 장치는 협정세계시(Universal Time Coordinated, UTC)와 발사예정시간(Predicted Launch Time, H0)을 이용하여 카운트다운 타임(CountDown Time, CT)을 생성하고, 발사 관련 주요 장비에 예정된 스케줄에 따라 임무가 수행될 수 있도록 시간 정보를 제공하는 역할을 한다[1]. 그러나 CT를 생성하는 CT 생성 장치가 단일화되어 있는 경우, CT 생성 장치에 고장이 발생하였을 때 각 발사통제시스템 및 발사 임무 관련 주요 장비에 발사체 발사에 필요한 CT 정보 및 CT 일시 정지 여부, 발사예정시간, 발사체 이륙 시간(Lift-off Time) 등의 정보를 제공할 수 없게 된다. 이로 인해 잘못된 정보를 운용자에게 제공할 수 있다. 또한 발사체 발사 직전 CT 생성 장치의 고장은 임무 실패로 귀결될 수 있는 위험성을 지니고 있다.

이를 방지하기 위한 설계 방법으로 종래의 신호 분배 장치의 경우 각 구성 모듈들을 이중화하여 한 모듈에 고장이 발생하여도, 정상 모듈로의 절체를 통하여 운용성을 높이는 물리적인 설계를 수행하여 왔다[2][3]. 그러나 CT 생성 장치와 같이 시간에 민감한 장치의 경우 각 모듈 간 주기적인 시간 정보 동기화를 하지 않으면, 고장 발생 모듈에서 정상 모듈로의 절체 시에 기준 시간에 대한 신뢰성을 잃게 되는 문제점이 발생한다.

또한 해당 장치에 대한 실시간 고장 감시 또는 내장자체점검 중 CBIT(Continuous Built-In-Test)과 같은 실시간 자체점검 기능을 활용하여 고장을 감시하고[4], 고장 발생 유형에 따른 절체를 수행하지 않으면 타 장치로의 부정확한 시간 정보를 송신할 수 있다[5]. 이와 같이 고장 감지에 따른 신속한 고장 대응을 하고 신뢰성 높은 CT를 생성 및 제공하기 위해 CT 생성 장치와 네트워크 카드, 시리얼 통신 회로 등을 물리적으로 이중화하여야 한다. 또한 각 이중화 장비 간의 데이터 공유 또는 주기적인 동기화를 통해 이중화 장치 간 절체 시 데이터 손실을 방지하고 장치의 일관성을 유지할 수 있도록 설계를 수행하여야 하며, 이중화된 CT 생성 장치 설계에 따라 실시간 고장 감시 및 동기화 기능과 절체 운용을 위한 소프트웨어 설계가 동반되어야 한다.

이를 통해 CT 생성 장치에 발생한 고장을 실시간으로 감시하고 고장 발생 시 CT 신호 손실 허용 범위 안에서 CT 생성 장치를 절체하여 CT 생성 장치의 지속적인 운용이 가능하게 된다[6].

따라서 본 논문에서는 카운트다운 타임을 생성하는 CT 생성 장치를 이중화하고 실시간 고장 감시 및 절체 운용 방법을 제안한다. 2장에서는 실시간 고장 감시 및 이중화 시스템에 대한 관련 연구를 기술하고 3장에서는 CT 생성 시스템의 전체적인 설계 구조 및 인터페이스에 대하여 설명한다. 4장에서는 설계한 CT 생성 장치의 CT 생성 소프트웨어 유닛(Computer Software Unit, CSU), 고장 및 상태 감시 CSU, 절체 관리 CSU의 기능 및 구조에 대하여 설명한다. 5장 시험 평가에서는 설계한 CT 생성 장치의 설계 기능 검증을 위하여 CT 생성 장치에 고장 주입 후 CT 생성 장치가 실시간으로 고장을 감지하는지 시험하고 고장 종류에 따른 절체 수행 여부와 절체 중 CT 신호 손실률을 확인하며 6장에서 결론을 맺는다.

II. Related works

본 논문에서 제안하는 카운트다운 타임 생성 장치는 실시간 고장 모니터링과 이중 서버 관리 기능으로 나눠진다.

최근에 수행된 실시간 고장 모니터링 연구들로는 자체진단시험[7], 자동 고장진단을 위한 실시간 모니터링[8], Can 통신 기반 고장진단[9] 연구들이 있다.

자체진단시험[7] 연구는 하드웨어, 소프트웨어의 고장 위치를 찾아내고 식별하는 진단 소프트웨어 연구로서 진단 소프트웨어를 통하여 고장 격리를 수행하며, 실시간 고장 발견 시 사용자는 다기능 시현기 화면을 통해 장비 결함을 신속하게 파악할 수 있다는 장점이 있다.

자동 고장진단을 위한 실시간 모니터링[8] 연구는 신경망을 이용한 상태 모니터링 시스템(Condition Monitoring System, CMS) 기반의 자동 고장진단 시스템으로서 실시간 입력 신호 분석을 통하여 분류된 신호 패턴에 따라 정상 상태 및 고장 유형을 진단할 수 있다.

Can 통신 기반 고장진단[9] 연구는 Can을 통해 차량의 기능 테스트를 수행하는 연구로서, 차량용 통신 인터페이스를 통해 테스트 컨트롤러가 동작하므로 추가적인 인터페이스 구축 없이 고장진단을 수행할 수 있으며, 차량 기능 동작에 영향을 미치지 않고 실시간 테스트가 가능하다.

이러한 기존의 고장 모니터링 연구들은 소프트웨어 고장 감시 항목을 소프트웨어 사용 목적에 맞게 선택하여 고장 진단을 할 수 없으며 고장 항목들의 조합을 통한 고장의 심각도를 판단할 수 없다는 한계를 지닌다.

현재까지 연구된 이중 서버 연구들로는 VMEBus를 통한 이중화[10] 지상통제장비 이중화 설계[11] 핫 스탠바이 스페어링 기법[12]이 있다.

VMEBus를 통한 이중화[10] 연구는 핫 스탠바이 스페어링 기법에 해당되는 Master와 Slave 역할로 동작하는 SBC(Single Board Computer) 간에 VMEBus 통신을 통한 이중화 네트워크 연구로서 네트워크 운용 지속성을 향상시킨 장점이 있으나, 백업 기능이 없어 데이터 손실 및 데이터 복구 안정성 취약의 한계점을 가진다.

지상통제장비 이중화 설계[11] 연구는 안정적인 장비 운용을 위하여 비행통제장비를 하드웨어, 소프트웨어적으로 이중화하고 제어권을 가진 장비에서 제어 명령을 수행하고 제어권이 없는 비행통제장비는 백업 운용을 수행하도록 설계되었다. 비

행통제장비의 운용성을 향상시킬 수 있다는 장점이 있지만 다양한 고장 발생 원인에 따른 신속한 제어권 획득이 어렵다는 한계를 가진다.

하드웨어 이중화 방법으로는 콜드 스페어링, 웜 스탠바이 스페어링, 핫 스탠바이 스페어링 기법이 있으며, 핫 스탠바이 스페어링 기법[12] 연구는 수행 또는 대기 중인 하드웨어의 고장을 실시간으로 검출할 수 있으며, 검출된 고장을 바탕으로 절체를 수행하여 장비 또는 시스템의 고가용성을 확보 할 수 있다. 하지만 다중화 된 하드웨어 장치 간의 동기화 및 동일한 정보 자원을 지속적으로 유지해야 한다는 단점을 가지고 있다.

기존 연구들과 다르게 본 연구는 이중 장치 간 공유 메모리와 인터럽트를 통해 데이터 동기화를 하도록 설계하였으며, 고장별 절체 설계를 통해 다양한 고장에 대응하고 고장 발생 시 절체 절차에 따라 데이터 손실을 최소화하기 위한 절체 방안을 설계하였다. 또한 본 연구는 고장 감시항목을 소프트웨어 운용자가 선택하여 필요에 따라 절체 판단 조건을 변경할 수 있도록 하여 절체 조건의 유연성을 높일 수 있다는 장점이 있다.

III. Structure and Interface of CT Generating System

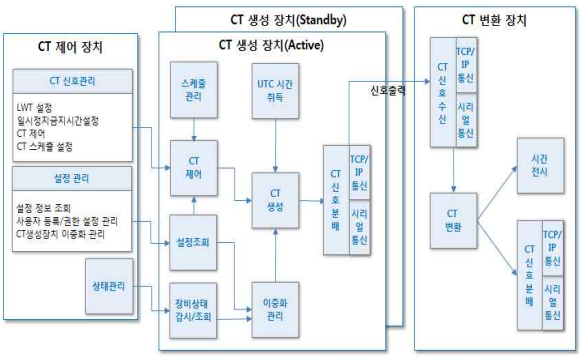

Fig. 1. Configuration of Countdown Time Generating System

카운트다운 타임 신호를 생성하고 분배하는 카운트다운 생성 시스템은 CT 제어 장치, CT 생성 장치, CT 변환 장치로 구성된다.

CT 제어 장치는 CT 신호에 대한 전반적인 제어를 담당하는 장비로서 CT 신호 제어(시작, 일시정지, 재시작, 종료), CT 스케줄 관리 및 발사 가능 시간 설정과 CT 일시정지 금지 시간 설정, CT 변환 설정 기능을 수행한다.

또한 CT 생성 장치의 실시간 상태 감시 기능과 절체 조건 설정 기능, 수동 절체 기능을 통해 CT 생성 장치를 제어할 수 있으며, GUI(Graphic User Interface)를 통해 실시간 고장 정보 또는 절체 정보를 운용자가 시각적으로 확인할 수 있도록 구현하였다. 또한 CT 제어 장치 및 CT 생성 장치의 장애 정보 및 CT 신호의 지연, 손실 등의 정보를 로그로 남기어 장애 관리를 수행할 수 있다.

CT 생성 장치는 카운트다운 타임을 생성하여 분배해 주는 장치로서, Active와 Standby 모드 장치로 이중화되어 있다. 생성 장치는 다수의 CT 제어 장치 또는 CT 변환 장치에 연결될 수 있고, CT 제어 장치의 CT 제어 명령을 통해 CT 생성, 제어 및 분배의 임무를 수행한다. CT 생성 장치는 CT 신호를 시리얼(Serial), 멀티캐스트(Multicast), 유니캐스트(Unicast) 통신 방식으로 발사통제시스템의 각 구성장비에 CT 신호를 분배할 수 있도록 설계하였다. CT 생성 장치의 세부 기능은 그림 1과 같이 UTC 취득, CT 생성, CT 제어, CT 신호 분배, 스케줄 관리, 설정 조회, 장비 상태 감시/조회, 이중화 관리 등으로 나누어진다. CT 생성 장치는 CT 제어 장치의 상태 감시 명령에 따라 주기적으로 생성 장치의 상태를 감시하며 장비 고장 감지 시 신속한 절체를 위해 고장 확인 인터럽트를 발생시키도록 설계하였다.

이중화 관리 기능은 절체 로직에 따라 정상 상태의 장치로 자동 절체, 수동 절체, Heart-Beat 절체를 수행하며 Active 모드 CT 생성 장치와 Standby 모드 CT 생성 장치 간의 주기적인 동기화 수행을 통하여 절체 시에 장비 동작의 일관성 유지와 데이터 누락이 없도록 설계하였다.

CT 변환 장치는 용도에 따라 수신된 CT 신호를 다른 형태의 CT 신호로 변환하는 CT 변환 및 분배 기능과 수신된 CT 신호를 전시하는 시간 전시 기능으로 구성된다. CT 변환 및 분배 기능은 시리얼 CT 신호를 입력받았을 경우 멀티캐스트 또는 유니캐스트 방식으로 이종의 신호로 변환하여 분배함으로써 CT 신호의 호환성을 높였다.

IV. Fault Monitoring and Changeover Software between CT Generating Devices

발사통제시스템의 CT 생성 장치간 고장 감지 및 절체 운용 소프트웨어는 3개의 CSU를 통하여 동작한다.

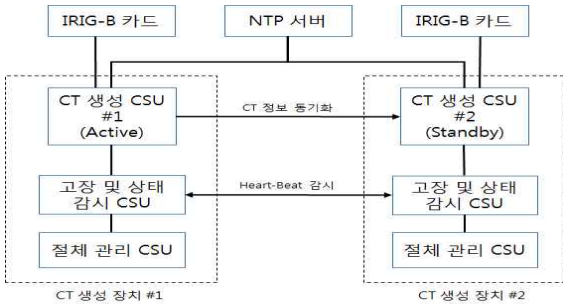

Fig. 2. Configuration Block of Fault Detection for CT Generating Device and Changeover Method

그림 2는 CT 생성 시스템에서 CT 신호 생성과 고장 감시 및 고장에 따른 절체를 수행하는 CT 생성 장치의 구성도이다.

CT 생성 CSU는 IRIG-B(Inter Range Instrumentation Group-B) 신호 수신 카드 또는 NTP(Network Time Protocol) 서버를 통하여 시간 정보를 취득하고 취득한 UTC 시간 정보와 H0를 이용하여 카운트다운 타임을 만들어 각 장치에 제공하는 기능을 수행한다. 또한 CT 생성 CSU는 매 주기마다 CT 신호를 생성하고 CT 생성 CSU #1, 2간 CT 정보를 동기화하는 기능을 수행한다.

고장 및 상태 감시 CSU는 CT 생성 CSU의 정상/비정상 상태를 Heart-beat 수신 여부와 네트워크 카드 상태, CPU 사용률, Memory 사용률, 시리얼 통신의 연결 상태, Process 상태 등의 정보를 실시간으로 감시하여 고장 여부를 확인한다. 또한 식별된 고장 정보를 절체 관리 CSU로 전달하고 에러 로그를 저장하여 사후 분석을 가능하도록 설계하였다.

절체 관리 CSU는 고장 및 상태 감시 CSU를 통해 식별된 고장 내용을 바탕으로 운용자가 설정한 절체 조건에 부합하면 고장 난 CT 생성 CSU를 배제하고 정상 CT 생성 CSU로의 자동 절체를 수행한다. 절체 관리 CSU는 Heart-beat 미갱신에 의한 고장 발생 시 Heart-beat 절체를 수행하며, 운용자의 고장 판단에 의해 강제로 수동 절체가 가능하도록 설계되었다.

1. CT Generation CSU

CT 생성 CSU는 운용자가 설정한 H0와 UTC의 차를 통해 산출한 CT 신호를 100ms 주기로 시리얼과 멀티/유니캐스트 방식을 통해 CT 신호 수신 장치로 송신한다.

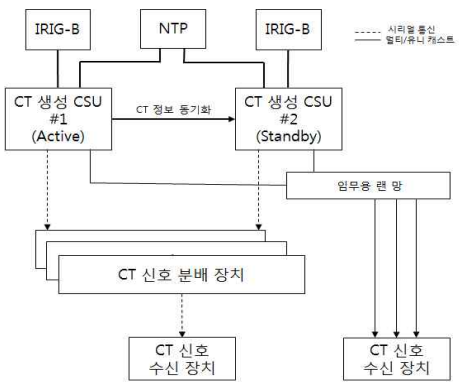

Fig. 3. Connection Diagram of CT Generating CSU

또한 CT 관련 정보인 CT 일시 정지 여부와 Lift-off 발생 여부, H0 설정값 등은 Active 모드인 CT 생성 CSU로만 송신되므로 매 주기마다 Standby 모드인 CT 생성 CSU에 해당 CT 정보를 동기화하여야 한다. 공유 메모리 내의 정보를 100ms 단위로 동기화하는 방법과 설정값 변경에 따른 인터럽트 처리 방법으로 동기화를 수행한다.

공유 메모리 내에 CT 신호 정보인 H0, CT 값, CT 신호 상태, 초기화 여부, Lift-off 여부, 일시정지 시간, 마지막 CT 신호 프레임, 마지막 CT 신호 생성 시간의 정보를 저장한다. 또한 CT 신호 분배 정보인 시리얼 CT 신호 분배 여부, 멀티캐스트 CT 신호 분배 여부, 유니캐스트 신호 분배 여부 그리고 스케줄 정보를 100ms 주기로 업데이트하여 동기화한다. 이를 통해 고장 발생에 의해 CT 생성 장치가 절체되었을 때 주기적으로 동기화된 CT 정보를 바탕으로 타 장비로 정확한 CT 신호를 생성, 복원하여 송신할 수 있으며, CT 신호 손실 프레임을 최소화할 수 있게 된다.

2. Fault & Status Monitoring CSU

고장 및 상태 감시 CSU는 생성 장치의 각 상태 정보를 감시하여 CT 생성 장치의 정상/비정상 여부를 판단한다. 감시 항목은 운영자의 절체 조건에 따라 달라지며, 현재 시스템에 적용되어 있는 감시 항목은 그림 4와 같다.

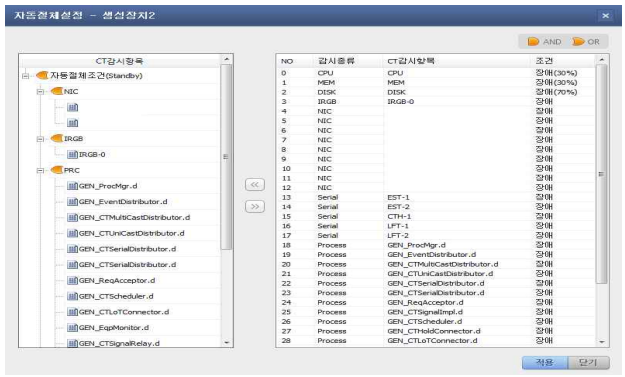

Fig. 4. Fault Monitoring List of CT Generating Device

현재 CT 생성 장치에 설정된 감시 항목 중 CPU, Memory 사용률은 1초 주기, DISK 사용률은 1분 주기로 이상 여부를 감시하도록 설계하였다. 신호 분배를 위한 시리얼 통신의 연결 여부, 네트워크 카드의 연결 여부, CT 생성 관련 프로세스의 구동 여부도 1초 주기로 감시한다. 그리고 UTC 시간을 취득하는 IRIG-B 신호 수신 카드는 시간의 신뢰성 보장을 위해 25ms 주기로 카드의 UTC 시간 취득 여부를 감시하도록 설계하였다.

또한 고장 및 상태 감시 CSU는 CT 생성 CSU #1, 2간 Heart-beat 카운트 값의 갱신 여부를 20ms 주기로 감시하도록 설계하였으며, 20ms 주기로 Heart-beat 값이 연속 3 주기 이상 카운트 갱신이 되지 않으면 Heart-beat 값을 송신하지 않는 CT 생성 CSU를 고장으로 판단하도록 설계하였다.

감시 항목 중 비정상 항목이 발생하면 고장 및 상태 감시 CSU에 해당 고장 정보를 공유 메모리에 기록하여 절체 관리 CSU가 고장 정보를 확인하고 절체 여부를 결정할 수 있도록 한다. 또한 고장 및 상태 감시 CSU를 통해 운용자가 실시간 고장 정보를 쉽게 인식하고 수동 절체 또는 장비 교체, 시스템 리부팅 등의 판단을 할 수 있도록 그림 5와 같이 GUI를 구성하였다.

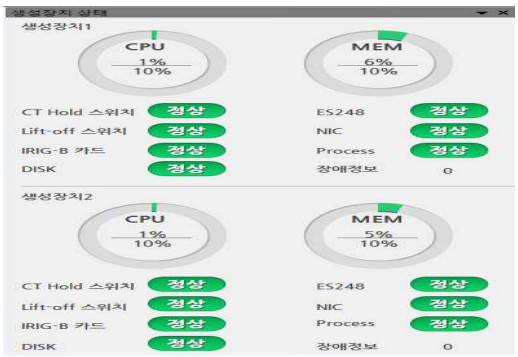

Fig. 5. Status Information of CT Generating Devices #1,2

3. Changeover Management CSU

절체 관리 CSU는 고장 및 상태 감시 CSU를 통하여 획득한 고장 정보를 바탕으로 절체 여부를 판단한다.

절체는 절체 조건에 따라 자동 절체와 운용자에 의한 강제 수동 절체, Heart-beat 미갱신에 따른 Heart-beat 절체로 나누어진다.

절체 관리 CSU는 수신한 CT 생성 시스템의 각 상태 정보를 통해 고장 발생 시 운용자가 설정한 자동 절체 조건에 부합되면 자동 절체를 수행한다. 각각의 조건은 AND 또는 OR 게이트 조합을 통해 이루어지며, 현 시스템에서는 CT 신호 분배를 위한 네트워크 카드 상태와 IRIG-B 수신 카드 상태 그리고 CT 신호 생성 관련 프로세스들의 상태 및 리소스 사용률을 OR 게이트로 묶어서 그중 하나라도 이상 동작이 발생할 경우 자동 절체를 수행하도록 설정하였다. 자동 절체 절차는 그림 6과 같다.

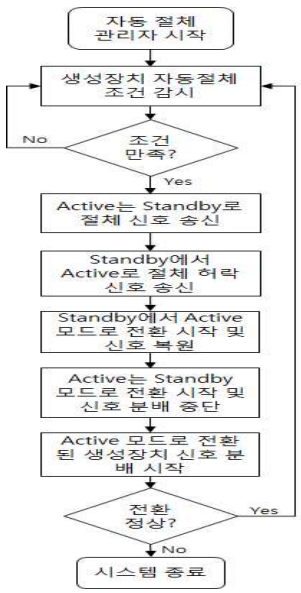

Fig. 6. Flowchart for Automatic Changeover of CT Generating devices

자동 절체 조건 검사는 절체 관리 CSU의 최소 주기인 25ms 주기에 맞추어 검사 및 판단하도록 설계되었으며, 자동 절체 시 Active 모드인 CT 생성 장치 #1은 Standby 모드인 CT 생성 장치 #2로 절체 신호를 보낸다. Standby 모드인 CT 생성 장치 #2에서 절체 신호 수신 시 절체 조건 검사를 수행하고 검사 결과에 따라 Active 모드인 CT 생성 장치 #1으로 절체 허락 신호를 송신한다. Standby 모드인 CT 생성 장치 #2는 Active 모드로 전환 및 CT 신호 복원을 시작한다. Active 모드인 CT 생성 장치 #1은 절체 허락 신호 수신 시 Standby 모드로 전환을 수행하며 CT 신호 생성/송신 임무를 중단한다. Active 모드로 전환된 CT 생성 장치 #2는 CT 신호 분배 장치를 통해 CT 신호 분배를 시작한다.

수동 절체는 자동 절체 조건 이외의 고장이 발생하였다고 판단되었을 경우 운용자 명령에 의해 수행된다. 수행 절차는 자동 절체 조건 검사를 제외하고 자동 절체와 동일하게 수행된다.

Heart-beat 절체는 Heart-beat 카운트가 연속하여 미갱신될 경우에 수행된다. Heart-beat은 20ms 주기로 Active 모드인 CT 생성 장치와 Standby 모드인 CT 생성 장치 간 Heart-beat 송수신을 하도록 설계되었으며, 3주기 이상 Heart-beat 송수신이 없으면 고장으로 판단하여 절체를 수행한다. Active 모드인 CT 생성 장치에서 Heart-beat을 못 받았을 경우, Standby 모드인 CT 생성 장치를 고장으로 판단하여 CT 정보 동기화를 중단하고 해당 장치를 배제시킨다. Standby 모드인 CT 생성 장치에서 Heart-beat을 못 받았을 경우, 동기화된 CT 정보를 바탕으로 모든 프로세스에 Active 모드 전환 신호를 송신하여 절체를 수행한다.

V. Evaluation

본 장에서는 설계한 CT 생성 시스템의 실시간 고장 감시 기능과 고장 종류에 따른 절체 수행 및 절체 시의 CT 신호 손실 여부를 확인하기 위해 3가지 실험을 수행하였다.

첫 번째 시험은 CT 생성 장치에 고장을 모의하여 고장 및 상태 감시 CSU가 실시간으로 고장을 감지하고 고장 정보를 절체 관리 CSU와 운용자에게 알리는지 확인하는 시험이다.

두 번째 시험은 CT 생성 장치의 자동 절체 조건에 따라 Active 모드인 CT 생성 장치에 고장을 주입한 후, CT 신호 손실 없이 비정상 CT 생성 장치에서 Standby 모드인 정상 CT 생성 장치로 절체하는지 확인하였다.

세 번째 시험은 Active 모드인 CT 생성 장치의 Heart-Beat 프로세스를 강제로 종료시켜, Heart-beat 절체 수행 여부와 CT 신호 손실을 확인하였다.

또한 Active 및 Standby 모드 CT 생성 장치의 Heart-beat 프로세스를 모두 종료하였을 경우 CT 생성 장치가 CT 생성 관련 프로세스들을 종료시키고 운용자와 CT 제어 장치에 종료 결과를 알리는지 확인하였다.

1. Test Environment

CT 생성 시스템은 CT 생성 장치 구성 형태에 따라 하드웨어 이중화 모드 또는 단독 모드로 구성할 수 있다. 본 논문에서는 이중화 모드로 장비를 구성하여 시험을 진행하였다. 아래 그림 7과 같이 2대의 CT 생성 장치 중 1대는 Active 모드 장치로 다른 1대는 Standby 모드 장치로 설정하였다. CT 생성 장치 간에는 Heart-beat 송수신 및 CT 관련 정보를 실시간 동기화하기 위해 HA(High Availability)망을 구성하였다. 또한 CT 생성 장치에 CT 제어 장치 1대와 CT 변환 장치 1대를 연결하여 CT 신호 제어 및 변환/ 분배를 할 수 있도록 환경을 구성하였다. 각 CT 생성 장치, CT 제어 장치, CT 변환 장치는 시간 정보를 수신하기 위해 IRIG-B 신호 분배 장치와 동축케이블로 연결된다. 생성한 CT 신호를 발사통제시스템의 각 구성장비에 분배하기 위해 CT 신호 분배 장치와 시리얼 통신으로 연결되고, 나로우주센터 임무용 랜망을 통하여 각 장치들과 통신되도록 환경을 구성하였다.

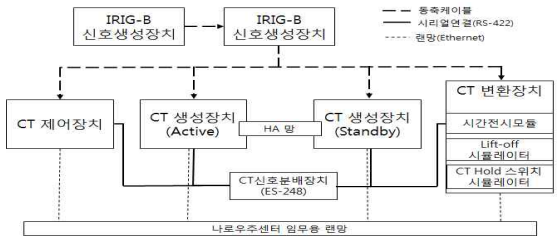

Fig. 7. Configuration of Test Environment

2. Real-time Fault Detection Test

CT 생성 시스템의 실시간 고장 감시 기능을 확인하기 위하여 2가지 시험을 수행하였다. 첫 번째, CT 생성 장치에 장착된 네트워크 카드의 IP를 변경하여 네트워크 고장을 주입하였으며, 두 번째는 연동 장비인 Lift-off 신호 수신 장치의 연결을 CT 생성 시스템 운용 중 강제로 해제하여 연결 해제 고장을 주입하였다.

먼저 CT 생성 장치 #1의 UTC 05:16:18.000에 네트워크 카드 IP를 변경하여 고장을 주입하였다. CT 생성 장치의 고장 감지 및 상태 감시 CSU는 1초 주기로 네트워크 카드 고장을 감시하므로, 그림 8번과 같이 고장 발생 후 700ms 뒤인 UTC 05:16:18.700에 CT 생성 장치 #1의 네트워크 고장을 감지하여 장애 알림 창을 통하여 네트워크에 대한 고장 정보를 운용자에게 알리는 것을 확인할 수 있다.

UTC	장애분류	장 치	위 치	장애내용
000 05:13:28.000	SYSTEM	MSDS	SYS-Socket / 10.20.10.43	The process(10.20.10.43) is no response
000 05:13:32.100	SYSTEM	DSP1	SYS-Socket / 10.20.23.51	The process(10.20.23.51) is no response
000 05:16:18.700	NETWORK	GEN1	NIC-p1p3 / 10.20.13.113#1	The interface(name=p1p3,ip=10.20.13.113#1) is down

Fig. 8. Detection of Network Fault

두 번째로 발사체 준비제어시스템 또는 발사체 이륙 신호(Lift-off) 시뮬레이터로부터 Lift-off 신호를 수신하는 Lift-off 신호 수신 장치와의 CT 생성 장치 연결을 강제로 해제하여 고장을 주입하였다. UTC 02:09:22.000에 Lift-off 신호 수신 장치 연동을 해제하여 1초 주기로 연동 고장을 감시하는 고장 및 상태 감시 CSU에서 아래의 그림과 같이 고장 발생 후 300ms 뒤인 UTC 02:09:22.300에 CT 생성 장치와 Lift-off 신호 수신 장치의 연동 고장을 감지하고 장애 알림 창을 통해 고장 정보를 운용자에게 알리는 것을 확인할 수 있다.

UTC	장애분류	장 치	위 치	장애내용
000 02:27:53.500	NETWORK	GEN1	NIC-p1p1 / 10.20.1.113#1	The interface(name=p1p1,ip=10.20.1.113#1) is down
000 02:09:22.300	SERIAL	GEN1	SER-3 / LFT-1	Serial port(LiftOff#1) is disconnected
000 02:09:22.300	SERIAL	GEN1	SER-4 / LFT-2	Serial port(LiftOff#2) is disconnected
000 02:09:22.300	SERIAL	GEN2	SER-3 / LFT-1	Serial port(LiftOff#1) is disconnected
000 02:09:22.300	SERIAL	GEN2	SER-4 / LFT-2	Serial port(LiftOff#2) is disconnected
000 02:09:11.900	SERIAL	CON1	SER-0 / CTH-1	serial port(CTH-1) is disconnected
000 02:09:11.400	SERIAL	GEN2	SER-2 / CTH-1	Serial port(CT Hold Controller) is disconnected
000 02:09:11.400	SERIAL	GEN1	SER-2 / CTH-1	Serial port(CT Hold Controller) is disconnected

Fig. 9. Detection of Lift-off Interlocking Fault

위 두 시험을 통하여 고장 및 상태 감시 CSU가 1초 안에 고장을 감지하고 CT 생성 시스템의 운용자와 절체 관리 CSU에게 고장 정보를 알리는 것을 확인할 수 있다.

3. Changeover Test

CT 생성 장치의 절체 기능 중 자동 절체 기능을 확인하기 위해 자동 절체 조건에 부합하는 고장을 CT 생성 장치 #1에 주입하였다. 주입한 고장을 통해 CT 생성 장치의 자동 절체 실행 및 절체에 따른 데이터 손실 유무를 확인하였다.

자동 절체 시험은 실시간 고장 감시 시험과 동일하게 CT 생성 장치에 네트워크 고장을 주입하였으며, 자동 절체 조건인 네트워크 고장으로 아래의 그림 10 및 11과 같이 CT 생성 장치 #1에서 Standby 모드로 동작 중이던 CT 생성 장치 #2로 절체된 것을 확인할 수 있다.

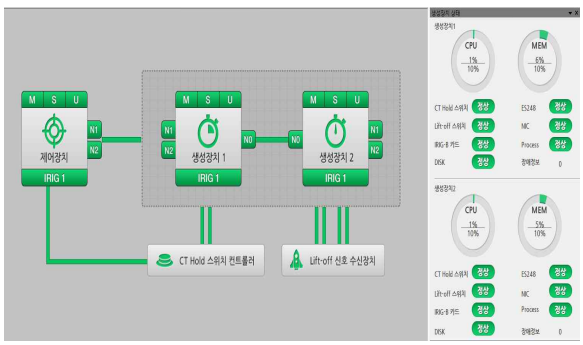

Fig. 10. Execution Screen for CT Generaing Device #1 of Active Mode

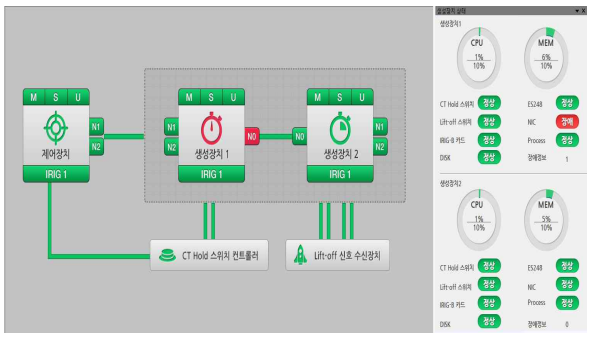

Fig. 11. Execution Screen for Completion of Automatic Changeover

또한 자동 절체 중 CT 생성 및 분배 기능의 일시적인 중단으로 발생하는 데이터 손실 유무를 확인하기 위해 CT 생성 장치 절체 전후의 CT 신호를 감시하였다. 아래 그림 12는 절체 전후의 CT 신호 감시창이다.

자동 절체는 UTC 05:22:30.000에 수행되었으며, 그림 12와 같이 절체 시간을 기준으로 전후에 손실된 CT 신호가 없는 것을 확인하였다. 반복 시험을 통하여 CT 신호 분배 시점과 절체 시점이 일치하지 않는 경우에는 CT 신호 손실 없이 절체가 수행됨을 확인하였다.

반복 시험을 통해서 CT 신호 최대 손실 허용 범위인 1 프레임 내에서 절체가 만족되는 것을 확인하였으며, 자동 절체 시험을 20회 수행하였을 때의 절체 평균 시간은 55ms로 설계 의도대로 CT 신호 분배 주기인 100ms 보다 시간이 적게 걸리는 것을 확인할 수 있었다.

위 시험을 통해 CT 생성 장치 간 절체 시 CT 신호 손실을 방지하기 위해 설계한 동기화 및 신호 복원 기능이 정상 동작함을 알 수 있었다.

Fig. 12. Monitoring Screen for Distribution of CT Signal while Automatic Changeover

4. Heart-beat Changeover Test

HA 망을 통해 각 CT 생성 장치 간 Heart-beat을 송수신하는 Heart-beat 관리 프로세스를 제어하여 두 가지 Heart-beat 절체 시험을 수행하였다.

첫 번째, CT 생성 장치 #1에서 CT 생성 장치 #2로 송신되는 Heart-beat을 일정 시간 미송신하도록 하여 CT 생성 장치 #2가 CT 생성 장치 #1을 고장으로 인식하고 Heart-beat 절체를 수행하도록 하였다.

두 번째, 각 CT 생성 장치의 Heart-beat 관리 프로세스를 강제 종료시켜 고장 및 상태 감시 CSU가 CT 생성 장치 간 Heart-beat 송수신이 불가능한 상태를 감지하고 CT 생성 장치의 Heart-beat 고장 알림이 정확히 실행되는지 확인하는 시험을 수행하였다.

먼저 CT 생성 장치 #1의 Heart-beat 프로세스를 강제 종료하여 CT 생성 장치 #2로 Heart-beat이 미송신 되도록 만들었다. 아래 그림 13번과 같이 Heart-beat 송신이 종료되면, Heart-beat을 수신하는 생성 장치에서 Heart-beat 미수신에 의한 이벤트 알림을 발생시킨다.

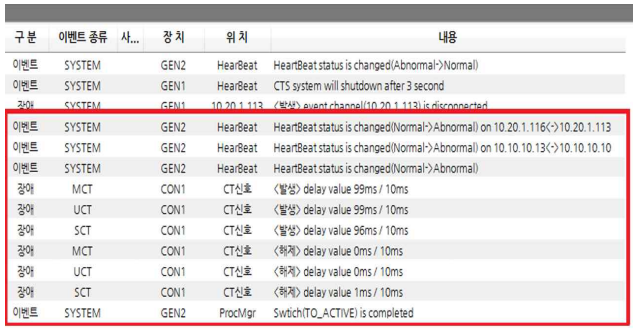

Fig. 13. Event Screen of Heart-beat Changeover

위 그림에서처럼 발생된 이벤트를 보면 3회 간 Heart-beat 신호 수신을 대기하였다가 3회 이후에도 Heart-beat 신호의 수신이 없음을 인지하고 송신 쪽 생성 장치를 고장으로 판단하였다. 그 후 CT 생성 장치 #2는 Standby 모드에서 Active 모드로 전환하는 것을 확인할 수 있다. 또한 100ms 단위로 신호를 분배하기 위하여 10ms 범위 안에서 CT 신호를 생성한 후 송신하는 CT 생성 장치에서 약 99ms, 96ms의 CT 신호 생성 지연이 발생하여 실제 분배되는 CT 신호에서 최대 1개의 CT 신호가 손실되는 것을 확인할 수 있었다.

두 번째 실험은 앞서 수행한 시험 환경에서 CT 생성 장치 #2의 Heart-beat 프로세스를 아래 그림 14번과 같이 강제 종료하여 CT 생성 장치 간 Heart-beat 송수신이 불가능하도록 만들었다.

Fig. 14. Forced Termination of Heart-beat Process

고장 및 상태 감시 CSU는 Standby 모드로 동작하는 CT 생성 장치 #1에 송신되는 Heart-beat 신호를 3회 기다린 후 Heart-beat 신호 연속 미응답에 따라 CT 생성 장치 #2를 고장으로 판단한다.

Fig. 15. Termination of CT Generating Device According to Quit the Heart-beat Process

기존 연구들과는 다르게 본 시험을 통하여 다양한 고장에 대응 할 수 있도록 설계한 고장별 절체 설계의 유효성과 데이터 손실을 최소화하기 위한 절체 방안에 대한 검증을 수행하였다.

VI. Conclusions

본 논문은 발사통제시스템의 구성장치인 CT 생성 장치의 이중화 설계 및 고장 감지에 따른 절체 운용 소프트웨어와 실시간 고장 감지 및 절체 시험 결과에 대하여 기술하였다.

CT 생성 장치는 발사통제시스템의 각 구성장치 및 발사 임무 관련 주요 장비에 CT 신호를 생성하여 분배해 주는 장치로서 발사 임무 성공 여부에 직접적인 영향을 주는 장치이다. 위와 같이 운용 신뢰성을 보장하기 위해 이중화 설계가 적용되어야 하는 시스템의 경우, 본 논문에서 설계한 실시간 고장 감시 및 절체 운용 소프트웨어에 대한 설계 내용을 확장 적용할 수 있을 것으로 판단된다.

본 논문에서 설계한 이중화된 CT 생성 장치의 고장 감시 및 절체 운용 소프트웨어는 장치 운용 요구도를 바탕으로 설계되었으며, 실시간 고장 감지 및 고장에 따른 절체 시험을 통하여 CT 생성 장치의 설계 기능에 대한 요구도 충족을 확인하였다. 개발한 CT 생성 장치 및 소프트웨어는 차기 발사체 발사 시에 CT 신호 생성을 위하여 적용될 예정이다.

REFERENCES

[1] Jong-Ho Kim, Seok-Young Youn, “Description of Lauch Control System in Space Center”, Current Industrial and Technological Trends in Aerospace, Vol. 3, No. 1, pp.108-120, July 2005.

[2] Yoo-Soo Han, Yong-Tae Choi, “Technical Trend of Time Syncronization Equipment in Naro Space Center”, Current Industrial and Technological Trends in Aerospace, Vol. 6, No. 1, pp.114-121, July 2008.

[3] Yoo-Soo Han, Yong-Tae Choi, Hyo-Keun Lee, "An Introduction to the Launch Vehicle Lift-off Signal Processing Equipment at Naro Space Center," The Korean Society For Aeronautical and Space Science, Vol. 85, No. 2, pp. 1112-1115, November 2008.

[4] Jeong-Seok Kim, Seung-Yul Yang, Jong-Pyo Han, “The BIT Design for Identifying Malfunction in Avionics”, The Korea Society For Aeronautical And Space Sciences, pp. 1711-1714, November 2014.

[5] Hae-Dong Park, Jong-Hyun Ha, Hun-Chang Park, Se-Hoon Lee, “Design and Implementation of Embedded Based DCS Terminal Remote Monitoring System”, The Korean Society of Computer and Information, pp. 219-223, June 2007.

[6] Jeong-Seok Kim, Yoo-Soo Han, “Research on the Changeover Software for Duplicated Countdown Time Generating Device of the Mission Control System”, The Korea Society of Computer and Information, Vol. 24, No. 2, pp. 33-36, July 2016.

[7] Sung-Woo Kim, Byung-Hwa Lee, Won-Hong Chang, Woo-Seop Oh, “Design and Verification of Built In Test For KUH”, Journal of The Korea Society for Aeronautical and Space Sciences, Vol. 40, No. 7, pp. 623-628, July 2012.

[8] Sang-June Park, Dae-Seong Kang, “Implementation of Real-time Monitoring System using the Neural Network for Automatic Failure Diagnosis of Offshore Wind Turbine”, Journal of Korean Institute of Information Technology, Vol. 10, No. 7, pp. 193-198, July 2012.

[9] Do-Yeon Hwang, Doo-Young Kim, Sung-Ju Park, “Design of Defect Diagnosis Platform based on CAN Network for Reliability Improvement of Vehicle SoC”, Journal of the Institute of Electronics and Information Engineers, Vol 52, No. 10, pp. 47-55, October 2015.

[10] Jeong-Won Park, Seong-Jin Park, “Implementation of a redundant network protocol based on VMEbus”, The Korea Institute of Information and Communication Enginerring, Vol. 15, No. 3. pp. 753-758, March 2011.

[11] Young-Mi Jeon, Jeong-Hui Jo, Ji-Hoon Kim, “Ground Control Equipment Redundancy for Reliable Operation

of UAV", The Korean Society For Aeronautical And Space Sciences, pp. 716-719, April 2014.
[12] Jin-Wook Shin, Dong-Sun Park, "The Implementation of Fault-Tolerant Dual System Using the Hot-Standby Sparing Technique", Korea Institute of Communication Sciences, Vol. 29, No. 10, pp. 1113-1122, October 2004.

Authors

Jeong Seok Kim received his B.S. and M.S. degrees in Computer engineering from Chung-nam National University, Daejeon, Rep. of Korea, in 2011 and 2013, respectively

Since 2013, he joined Korea Agency for Defense Development (ADD) and Since 2016, he Joined Korea Aerospace Research Institute (KARI). His research Interests include embedded system, software testing and avionic system.

Yoo Soo Han received the B.S. and M.S. degrees in Electronic Engineering from Kyungpook National University, Korea, in 1996 and 1998 respectively.
He joined Korea Aerospace Research Institute (KARI) in 2005.
He is currently a senior researcher in the Flight Safety Technology Team, Naro Space Center. He is interested in tracking filter, flight safety and software testing.