J. Astron. Space Sci. 15(2), 499-508 (1998)

동적 고장관리 기법을 이용한 위성운용 서브시스템 설계

김재훈 · 모희숙 · 정원찬

한국전자통신연구원 무선방송기술연구소 위성통신시스템연구부

DESIGN OF SATELLITE OPERATIONS SUBSYSTEM USING DYNAMIC FAULT MANAGEMENT MECHANISM

Jaehoon Kim, Heesook Mo, and Woonchan Jung

Satellite Communications System Department, Radio and Broadcasting Technology Laboratory,ETRI

email: jhkim@etri.re.kr

(Received October 14, 1998; Accepted November 4, 1998)

요 약

다목적 실용위성 관제시스템의 SOS(Satellite Operations Subsystem) 서브시스템은 위성에서 보내온 원격측정 데이터를 처리하여 위성의 상태를 감시하고 위성으로 원격명령을 전송하는 업무를 수행한다. 본 논문에서는 SOS 서브시스템의 신뢰성 및 가용성을 향상시키기 위하여 하드웨어와 소프트웨어를 이중화하여 데이터 손실을 최소화하도록 설계한 SOS의 동적 고장관리(dynamic fault management) 기법에 대하여 기술하였다. 또한 구현의 정당성을 확인하기 위한 성능 시험 방법을 제시하였으며 그에 대한 시험 결과를 분석하였다.

ABSTRACT

Satellite Operations Subsystem in the Mission Control Element provides real-time monitoring of the satellite status and transmits telecommands to control the satellite during the contact time. This paper presents the dynamic fault management strategy of Satellite Operations Subsystem designed to minimize data loss using software and hardware redundancy for upgrade safety and reliability of Satellite Operations Subsystem. Also this paper describes the performance test method to prove justification of implementation and analyzes the results.

1. 서 론

다목적 실용위성(Korea Multi-purpose Satellite: KOMPSAT)은 685Km 상공에서 한반도의 지도 제작, 해양관측 및 우주과학 실험 등의 임무를 수행하는 저궤도 위성이다. KOMPSAT에서 보내온 데

이터를 처리하고 KOMPSAT을 관제하는 다목적 실용위성 지상시스템(KOMPSAT Ground System : KGS)은 KOMPSAT에서 보내온 영상 데이터를 처리하는 영상수신처리시스템(Image Reception and Processing Element : IRPE)과 KOMPSAT을 추적하고 감시 및 제어하는 관제시스템(Mission Control Element : MCE)으로 구성된다.

KGS는 위성을 제어하기 위한 원격명령(TeleCommand : TC)과 위성의 상태를 나타내는 원격측정(TeleMetry : TM) 데이터는 S-밴드를 통하여 KOMPSAT과 송수신하며, 위성에서 수집한 영상 데이터는 X-밴드를 통하여 IRPE로 보낸다. 위성을 제어하기 위하여 위성으로 보내는 원격명령과 위성의 상태를 나타내는 원격측정 데이터는 Consultative Committee for Space Data Systems(CCSDS)에서 권고하는 표준 형식을 따른다(NASA 1987, 1995).

MCE는 위성을 효과적으로 감시 및 제어하기 위하여 크게 4개의 서브시스템으로 구성되며 개략적인 구성도는 그림 1과 같다. TTC(Telemetry, Tracking & Control) 서브시스템은 위성으로부터 원격측정 신호 수신, 위성으로 원격명령 신호 전송 및 위성 추적 기능을 수행하며, SOS(Satellite Operations Subsystem) 서브시스템은 원격측정 데이터의 처리 및 출력, 원격명령 생성 및 원격명령을 TTC 서브시스템과 SIM(SIMulator) 서브시스템으로 전송하는 기능을 수행한다.

MAPS(Mission Analysis and Planning Subsystem) 서브시스템은 다목적 실용위성의 궤도 및 자세를 분석하고 임무일정을 계획하는 기능을 담당하며, SIM 서브시스템은 다목적 실용위성에 대한 수학적 모델링, 원격명령의 검증, 이상상태 분석 및 운용자에 대한 훈련을 지원한다.

KOMPSAT이 한반도 상공을 지날 때 MCE에서 위성으로 원격명령 송신 및 위성으로부터 원격측정 데이터를 수신할 수 있어야 한다. 이를 위하여 SOS 서브시스템의 원격측정 및 원격명령 처리 등 주요 기능을 이중으로 구성하는 고장허용 한계 시스템(fault tolerant system)의 개념을 적용하여 개발되어야 한다.

이와 같은 고장허용 한계 시스템의 개발을 하드웨어적으로 구현하는 경우 안전성이 뛰어나나 많은 비용이 소요되어 비경제적이며, 소프트웨어적으로 해결하는 경우 구현이 매우 복잡하고 성능이 떨어지는 문제점이 있다(Shieh *et al.* 1990).

현재 사용 중에 있는 대부분의 위성운용 서브시스템은 하드웨어 및 소프트웨어적으로 완전 독립된 이중화 구조로 되어있어, 어느 한 부분에 이상이 발생할 경우 전체 기능을 백업 시스템이 수행하도록 하고있다. 이와 같은 시스템에서는 백업 시스템으로 절체를 하는 중에 데이터의 손실이 발생할 수 있으며, 어느 한 기능의 이상이 전체 시스템의 안정성에 많은 영향을 주는 문제가 발생할 수 있다. 본 논문에서는 SOS 서브시스템의 신뢰성 및 가용성을 향상시키기 위하여 하드웨어와 소프트웨어를 적절히 이중화하여 데이터 손실을 최소화하도록 설계한 SOS의 동적 고장관리(dynamic fault management) 기법에 대하여 기술하였다. 또한 이의 정당성을 확인하기 위한 성능 시험 방법을 제시하였으며 시험 결과에 대하여 분석하였다

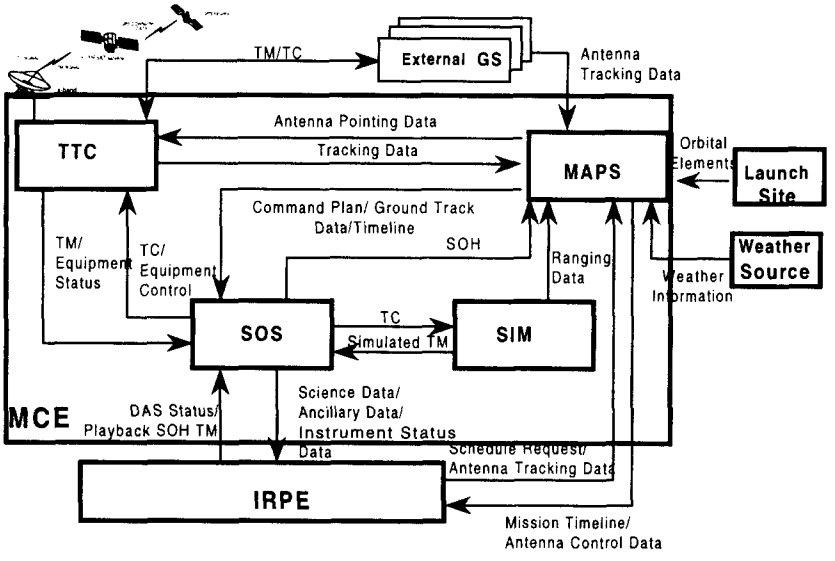

그림 1. 다목적 실용위성 관제시스템 구성도

2. SOS 서브시스템

SOS 서브시스템은 위성으로부터 수신한 원격측정 데이터를 처리하고, 위성을 제어하기 위한 원격명령을 생성하여 TTC 서브시스템을 통해 위성으로 전송하는 업무를 수행한다. SOS 서브시스템의 주요기능으로는 원격측정 데이터 처리(telemetry data processing) 기능, 원격명령 처리(telecommand processing) 기능, 위성 상태 경향 분석(trend analysis) 기능 및 TTC 장비 감시 및 제어(TTC equipments control and monitoring) 기능이 있다. 원격측정 데이터 처리기능은 위성으로부터 위성 상태를 나타내는 원격측정 데이터(TRW 1997)를 수신 및 처리하여 출력하며, 보고서 작성을 위해 저장하는 기능을 수행한다. 원격명령 처리 기능은 위성을 감시하고 제어하기 위해 위성으로 전송할 원격명령을 생성하고 전송하는 기능을 수행한다. 원격명령은 크게 실시간 수행 원격명령(real-time command), 절대시간 수행 원격명령(absolute time command), 상대시간 수행 원격명령(relative time command sequence)으로 구분한다(TRW 1997). 위성 상태 경향 분석 기능은 위성으로부터 수신한 원격측정 데이터 중에서 특정 항목에 대한 일정 기간 동안의 변화를 출력하여 위성의 상태를 분석할 수 있는 기능을 제공한다. TTC 장비 감시 및 제어기능은 TTC 장비들을 원격으로 감시하고 장비 구

성(configuration)을 변경하기 위한 명령을 TTC 장비로 전송하는 기능을 수행한다.

SOS 서브시스템은 우리나라 상공을 하루에 4 5회 통과하는 KOMPSAT으로부터 위성의 각종 상태를 나타내는 원격측정 데이터를 수신하고, 위성 제어를 위한 원격명령을 전송할 수 있어야 한다. 통과 시간(pass time) 동안 원격 측정 데이터를 수신하지 못하는 경우 현재 위성 상태를 정확히 파악할 수 없으며, 만일 위성이 이상상태에 있는 경우라면 이에 대한 적절한 조치를 취할 수 없는 경우가 발생한다. 또한 위성으로 원격명령을 송신할 수 없으므로 위성이 지상에서 원하는 임무를 수행 못하는 문제가 발생한다. 이와 같은 문제들을 사전에 방지하고 시스템의 안정성 및 신뢰성을 향상 시키기 위하여 주요 기능들에 대한 하드웨어 및 소프트웨어 이중화가 요구되며, SOS 서브시스템의 고장으로 인한 원격측정 데이터의 손실을 최소화 할 수 있어야 한다. 또한 이중화가 되어있다 하더라도 백업 기능으로 이동하는 동안 데이터의 손실을 최소화하도록 설계 및 구현되어야 한다

3. 동적 이중화 방법을 이용한 SOS 서브시스템 설계

하드웨어 이중화를 위한 방법으로는 여러 개의 디스크를 이용하여 다중화 파일시스템을 구성하는 방법, 네트워크를 이중화 하는 방법, CPU를 이중화하는 방법 및 메모리를 이중화하는 방법(Huang 1993) 등이 있다.

소프트웨어의 이중화 방법으로는 동일 기능을 중복으로 구성하여 하나의 기능에 이상이 발생할 경우 다른 기능이 이를 대신하도록 하여 고장으로 인한 시스템 중단을 최소화하도록 구성하는 것이다. 주요 소프트웨어에 대하여 이중화하는 경우, 해당 소프트웨어의 이상 유무를 감시하기 위하여 주기적으로 상태를 점검하며 응답이 없을 경우 백업 소프트웨어가 기능을 대신하도록 수행시켜야 한다. 이때 백업 기능을 주(primary) 기능의 고장을 확인한 후 처음부터 백업 소프트웨어를 수행시키는 경우 해당 소프트웨어가 수행을 시작하기 위하여 준비하는 동안 시스템에 필요한 처리를 못하는 경우가 발생한다. 이와 같은 문제점을 해결하고 시스템의 신뢰성을 높이기 위하여 소프트웨어 및 하드웨어 이중화를 혼합한 SOS 서브시스템을 설계하였다. SOS 서브시스템의 주요 기능인 원격 측정 데이터 처리 및 원격명령 처리를 위한 하드웨어 및 소프트웨어의 이중화 구성도는 그림 2와 같다. 시스템의 가용성을 높이기 위하여 동일한 기능을 서로 다른 컴퓨터에서 수행하도록 구성하였으며, 주 TM/TC 처리 워크스테이션(primary TM/TC processing workstation)에는 주 기능들에 관한 클라이언트들이 수행되도록 하였고, 백업 TM/TC 처리 워크스테이션(backup TM/TC processing workstation)에는 주 기능 클라이언트들에 고장이 발생하였을 경우, 동일 기능을 계속적으로 수행할 수 있도록 백업 기능들에 대한 클라이언트들이 위치하도록 하였다.

클라이언트들 사이의 통신을 총괄하고 서버 역할을 수행하는 이중화된 ComServer를 중심으로 모든 클라이언트들이 연결되어있으며, 클라이언트들이 어느 워크스테이션에서 수행되든지 상관없이 데이터를 송수신한다. 데이터 손실을 최소화하기 위하여 서로 다른 컴퓨터에 주 클라이언트와 백업 클라이언트가 동시에 수행할 수 있도록 하였으며, 백업 클라이언트는 주 클라이언트와 같이 동일한

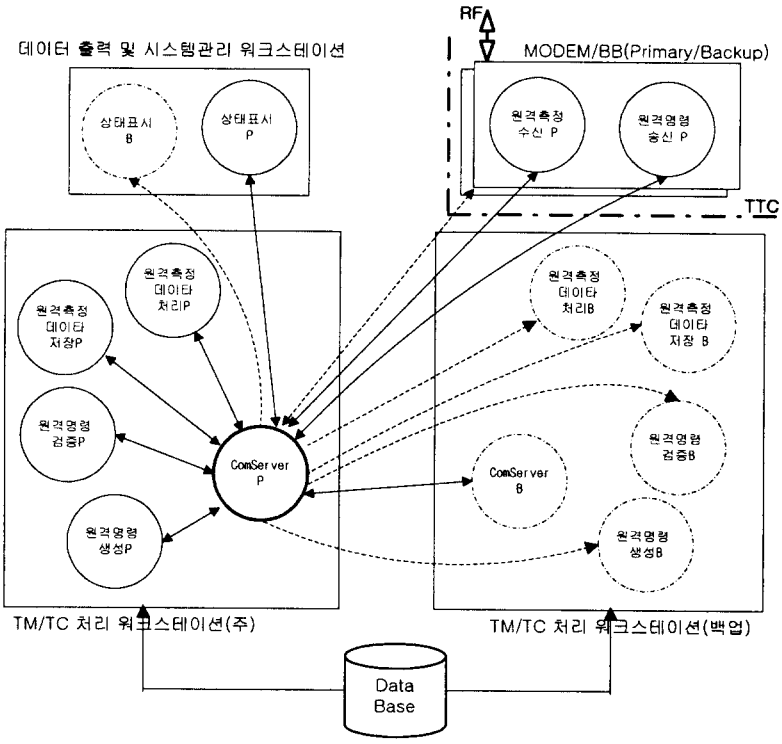

그림 2. SOS 서브시스템의 이중화 구성도

데이터를 수신하여 동일한 처리를 수행하나 다른 클라이언트로 ComServer를 통해 수행 결과를 전송하지 않도록 하였다. 주 클라이언트들이 주어진 시간동안 반응하지 않으면 백업 클라이언트가 주 클라이언트 역할을 대신하며, 주 클라이언트에 대하여 하나 이상의 백업 클라이언트를 두도록 구성할 수 있으나, 동일 기능에 대하여 하나의 백업 클라이언트만 존재하도록 설계하였다.

클라이언트는 ComServer와 통신에 이상이 있는 경우 다른 ComServer를 자동으로 수행시킬 수 있다. 그러나 ComServer의 이상 상태를 확인하고 새로운 ComServer를 수행시키는 동안 전송 중에 있는 메시지는 잃어버릴 수 있다. 이와 같은 문제를 해결하기 위하여 그림 3에서 보는 바와 같이 백업 ComServer를 동시에 수행하도록 하여 클라이언트가 주 ComServer와의 통신에 이상이 발생하는 경우 수행 중에 있는 백업 ComServer로 연결 되어 수행하도록 하여 데이터 손실을 최소화 하였다.

백업 ComServer와 연결하여 통신하고 있는 중에 주 ComServer의 문제를 해결하여 정상적으로 작동하는 상태에서 백업 ComServer에 문제가 발생하면 다시 주 ComServer와 연결하여 수행하도록 하였다. 동시에 주 및 백업 ComServer에 문제가 발생하는 경우를 방지하기 위하여 ComServer를 다

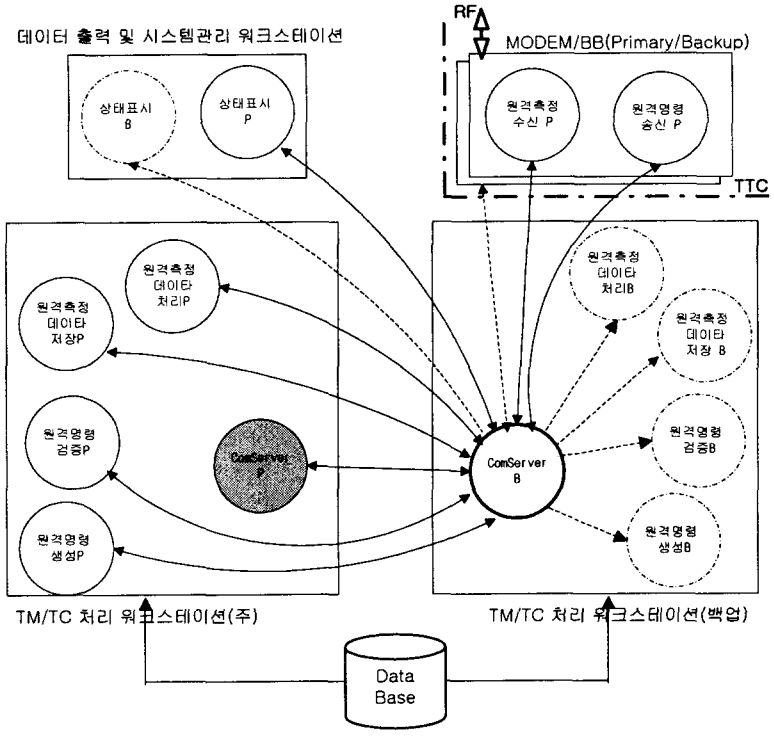

그림 3. Comserver 고장에 대한 백업 처리 구성도

른 워크스테이션에서 수행하도록 구성할 수 있다.

그림 4와 같이 주 TM/TC 처리 워크스테이션 전체에 고장이 발생한 경우 모든 데이터 처리가 백업 TM/TC 처리 워크스테이션에 있는 클라이언트와 ComServer가 수행되도록 하여 시스템의 일부 하드웨어 고장에 대해서도 정상적으로 처리를 할 수 있도록 설계하였다. 특정 주 클라이언트에 고장이 발생하는 경우 그림 5와 같이 백업 클라이언트가 기능 수행을 할 수 있도록 하였다. 백업 클라이언트는 주 클라이언트와 완전 동일한 상태를 유지하므로 백업 클라이언트로 교체가 되어도 다른 클라이언트들에서 이와 같은 상태 변화에 대한 감지를 못하고 기능을 수행하도록 하여 서브시스템에 대한 안정성을 높였다.

4. SOS 서브시스템 구현 및 성능 시험

위에서 기술한 설계 내용 및 개념을 Talarian사의 RTworks와 RtsmartSockets(Talarian 1995)을 이용하여 구현하였으며, 이중화를 고려한 SOS 서브시스템의 하드웨어 구성은 그림 6과 같다.

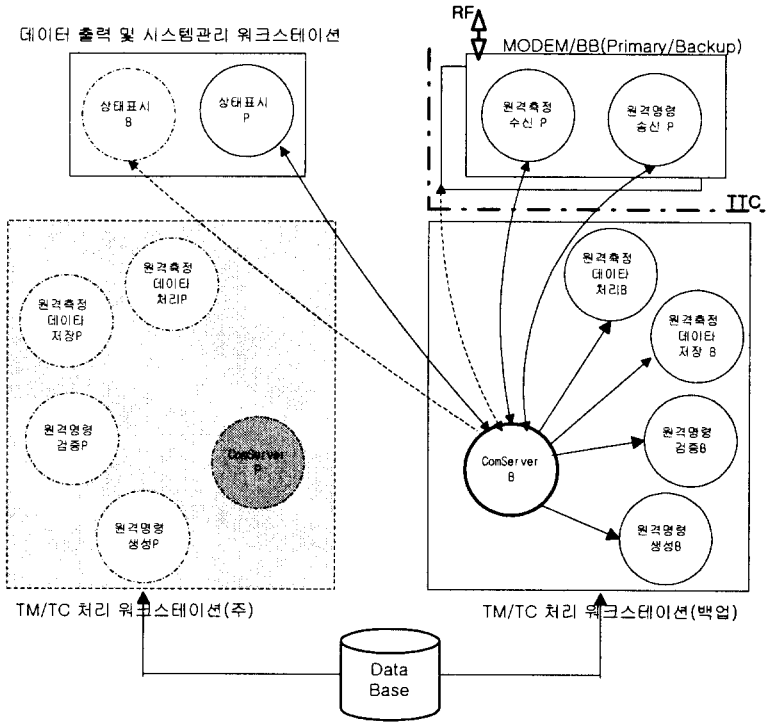

그림 4. 주 TM/TC 처리 워크스테이션 고장에 대한 백업 처리 구성도

표 1. 이중화에 대한 시험 결과.

시험	시험시 이용한 프레임 수	정상 처리 프레임 수	비정상 처리 프레임 수	비고
정상적인 이중화 구조	320(minor 프레임)	320	0	
주 ComServer 고장	640	640	0	
주 TM/TC 처리 워크스테이션	19,200	19,200	0	
주 클라이언트 고장	640	640	0	

RTworks 및 RTsmartSockets에서 고장 허용한계 시스템 구현을 위하여 제공하는 주요 기능으로는 시스템 운용 중 ComServer가 고장이 발생하면, 자동으로 ComServer를 재수행 시키는 ComServer 자동 수행 및 재수행 기능, ComServer의 이상 상태를 확인하고 새로운 ComServer를 수행시키는 동안 전송 중에 있는 메시지 손실 문제를 해결하기 위하여 백업 ComServer를 동시에 수행하도록 하여 클라이언트가 주 ComServer와의 통신에 이상이 발생하는 경우 이미 수행중인 백업 ComServer로 연결 되어 수행하도록 하는 ComServer 긴급 백업(hot backup) 기능, 동일한 기능을 처리하는 두개의 클라이

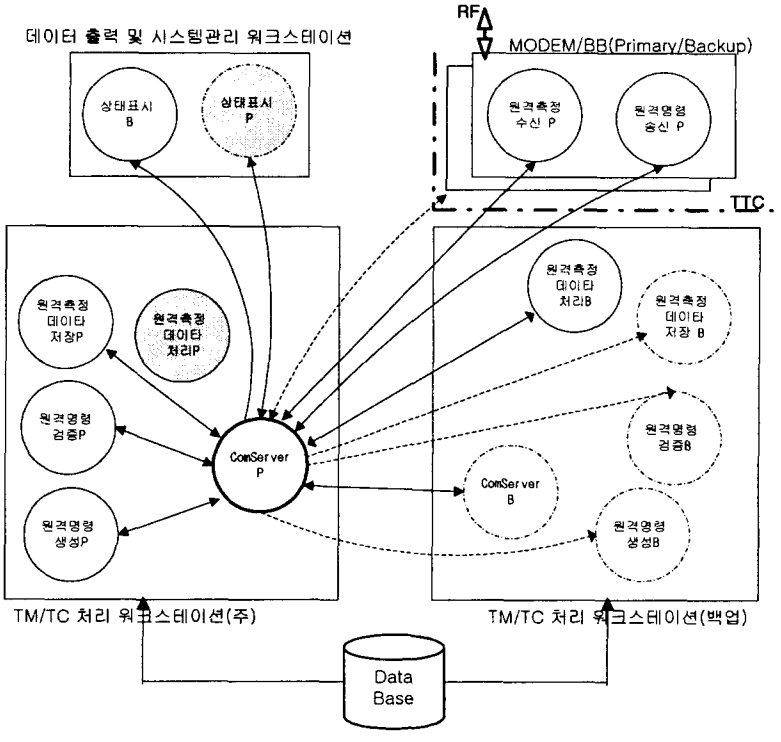

그림 5. 주 클라이언트 고장에 대한 백업 클라이언트 처리 구성도

언트를 수행시키며, 주 클라이언트에 이상이 있으면 백업 클라이언트가 기능을 대신하여 수행하도록 하는 클라이언트 긴급 백업 기능이 있다.

SOS 서브시스템 구현 후 시스템의 안정성 및 처리 데이터 손실에 대한 검증을 위하여 정상적인 이중화 구조, 주 ComServer 고장 발생, 고의로 주 TM/TC 처리 워크스테이션 고장 발생 및 주 클라이언트 고장 발생 등 다양한 상황에서 원격측정 데이터를 정상적으로 처리하는지를 시험하였으며, 정상적인 원격측정 데이터 뿐만 아니라 에러가 포함된 원격측정 데이터 프레임, 정해진 속도 보다 빠른 원격측정 데이터 수신 및 처리, 손상된 원격측정 데이터 프레임에 대한 처리 등을 동일한 환경에서 수행하였다. 이에 대한 결과는 표 1과 같다

위의 시험 결과에서 보는 바와 같이 SOS 서브시스템의 이중화 구조하에서 어느 하나의 고장이 발생하여도 데이터 손실 없이 처리하고 있음을 볼 수 있다. 시험 수행 시 SOS 서브시스템에 치명적

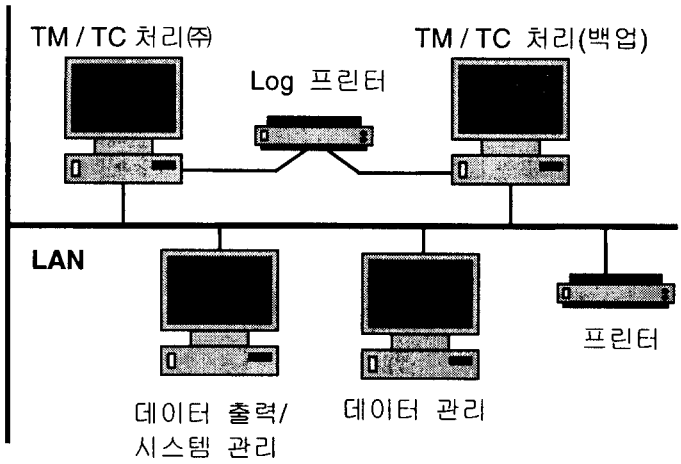

그림 6. SOS 서브시스템의 하드웨어 구성도

인 영향을 줄 것으로 예상되는 경우에 대하여 좀 더 많은 데이터를 가지고 시험을 수행하여 데이터 손실 발생 여부를 시험하였다.

6. 결 론

SOS 서브시스템은 우리나라 상공을 하루에 4 5회 통과하는 다목적 실용위성과 매 통과 시 약 15분 동안 위성으로부터 위성의 각종 상태를 나타내는 원격측정 데이터를 수신하고, 위성을 제어하기 위한 원격명령을 전송할 수 있어야 한다. 통과 시간 동안 원격 측정 데이터와 원격명령에 대한 송수신을 못하는 경우를 최대한 방지하고 시스템의 안정성 및 신뢰성을 향상 시키기 위하여 원격측정 및 원격명령처리 관련 기능들에 대한 하드웨어 및 소프트웨어 이중화를 동적 고장관리 기법을 적용하여 구현하므로 SOS 서브시스템의 고장으로 인한 원격측정 데이터 손실 및 원격명령을 위성으로 송신을 못하므로 발생하는 문제를 최소화하였다. 시스템의 안정성 및 데이터 손실에 대한 검증을 위하여 다양한 환경을 설정하여 시험을 수행하였으며, 시험 결과는 SOS 서브시스템의 규격을 만족시키는 것으로 확인이 되었다.

감사의 글: 본 연구는 정보통신부 출연금의 지원에 의한 것입니다..

참고문헌

Shieh, Y., Ghosal, D., Chintamaneni, P. R., & Tripathi, S. K. 1990, IEEE Transactions on Software Engineering, 16-4, pp444-457

Huang, Y. & Tripathi, S. K. 1993, IEEE Transactions on Software Engineering, 19-2, pp108-119

Talarian Corp 1995, RtsmartSockets Tutorial Version 3.5, pp6-1 ~ 6-14 TRW Space & Electronics Group 1997, KOMPSAT Command Allocation Document

TRW Space & Electronics Group 1997, KOMPSAT Telemetry Allocation Document

NASA CCSDS 1987, Telecommand Summary of Concept and Rationale, CCSDS 200.0-G-6

NASA CCSDS 1995, Packet Telemetry, CCSDS 102.0-B-4