다목적실용위성 2호의 On-Board Fault Management

최종욱[0] 천이진, 이재승
한국항공우주연구원
{jwchoi, yjcheon, jslee}@kari.re.kr

On-Board Fault Management for KOMPSAT-2

Jong-Wook Choi0 Yee-Jin Cheon Jae-Seung Lee
Space Division, Korea Aerospace Research Institute

요 약

인공위성 시스템은 기존의 임베디드 시스템과 달리 우주환경에서도 예측가능하며 견고히 수행되어야 하며, 또한 위성의 오류가 발생하게 되면 어떠한 환경에서도 위성의 생존을 위하여 자동적인 오류 검출, 오류 제거, contingency state로 위성을 재구성 하는 과정이 반드시 필요로 한다. 이러한 모든 과정을 On-Board Fault Management라 하며, 본 논문에서는 다목적실용위성 2호의 On-Board Fault Management 구조와 오류 검출방식, 위성을 safing시키는 과정과 테스트 결과에 대해서 설명한다.

1. 서 론

2005년 발사 예정인 다목적실용위성 2호(KOMPSAT-2)는 탑재 프로세서(processor)로 인텔 80386을 채택하고 있으며 각각의 프로세서는 기능에 따라 지상으로부터의 명령 수신 및 라우팅, 원격 측정데이터의 수집 & 송신을 담당하고 있는 탑재 컴퓨터(OBC, On-Board Computer), 위성의 전력 발생 및 분배 그리고 위성체에 대한 열 제어를 담당하는 전력계 제어장치(ECU, Electrical Power subsystem control Unit) 그리고 자세 센서로부터 정보를 받아들이고 위성 자세 및 궤도에 대한 제어를 담당하는 원격 구동 장치(RDU, Remote Drive Unit)로 3개의 프로세서로 구성된 다중 프로세서 구조를 가지고 있으며 primary 프로세어와 redundant 프로세서로 이중화 되어있다. 각각의 프로세서와 탑재체간의 통신을 위해서는 명령-응답 방식의 MIL-STD-1553B 데이터 방식을 사용하고 있으며 OBC는 Bus Controller로 동작하며 RDU와 ECU는 Remote Terminal로 동작한다. 실시간 운영체제(RTOS)인 VRTX와 탑재소프트웨어(Flight Software)에 의하여 위성의 전반적인 운영이 이루어진다. 위성 시스템은 기존의 임베디드 시스템과 달리 우주환경에서도 예측가능하며 견고히 수행되어야 하며, 또한 위성의 오류가 발생하게 되면 어떠한 환경에서도 위성의 생존을 위하여 자동적인 오류 검출, 오류 제거, contingency state로 위성을 재구성 하는 과정이 반드시 필요로 하며, 이러한 모든 과정을 On-Board Fault Management라 한다. On-Board Fault Management를 위하여 각각의 프로세서는 독립적인 Watch Dog Timer(WDT)를 가지고 있으며, 탑재소프트웨어는 매 250ms마다 위성의 오류 발생을 확인하게 되며, 오류가 검출되게 되면, WDT Timeout을 통해 모든 프로세서를 redundant 프로세서로 failover하는 방식을 채택하고 있다. 본 논문에서는 다목적실용위성 2호 On-Board Fault Management 구조와 오류 검출방식, 위성을 safing시키는 과정과 테스트 결과에 대해서 설명한다.

2. 다목적실용위성 2호의 On-Board Fault Management

다목적실용위성 2호의 탑재컴퓨터 시스템 및 소프트웨어 구조는 그림 1에 나타나 있으며 각 서브시스템은 모두 primary와 redundant를 가진 이중화 구조를 가지고 있다.

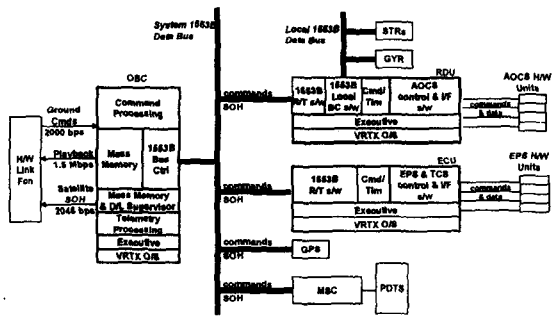

그림 1. 다목적실용위성 2호의 시스템 및 S/W 구조

다목적실용위성 2호의 기본적인 On-Board Fault Management 개념은 위성의 오류가 검출되면 위성의 안전을 위하여 프로세서와 모든 서브시스템을 redundant로 전환하며, 활성화 되어 있는 모든 유닛의 전원을 차단한다. 또한 태양 전지판을 태양을 향하도록 위성의 자

세를 조정하며 최소 전력 소비 모드 상태에서 위성의 생존을 책임지게 된다. 그림 2는 다목적실용위성 2호의 기본 개념을 나타내며, 위성이 Contingency 상태에 있는 동안 지상에서는 위성을 정상상태로 복귀하기 위하여 오류 발생 원인과 오류의 제거를 통해 정상적인 위성운용이 되도록 Ground Recovery Management를 수행하게 된다.

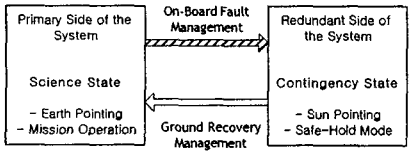

그림 2. KOMPSAT-2 On-Board Fault Management

다목적실용위성 2호에서 On-Board Fault Management를 위하여 각각의 프로세서는 독립적인 Watch Dog Timer를 가지고 있으며, 탑재 소프트웨어에서는 매 250ms마다 오류를 발생 유무를 확인하게 된다. 위성이 정상적인 운용 중에는 탑재소프트웨어는 매 250ms마다 WDT를 리셋하여 failover를 방지하며, 실시간으로 위성의 health정보와 프로세서 정보를 Mass Memory에 저장하게 된다. 탑재소프트에 의해 오류가 검출되면, 지상의 Ground Recovery Management를 위하여 모든 오류 정보를 Mass Memory에 저장하고 WDT Timeout이 발생하도록 WDT reset을 멈추게 된다. WDT Timeout이 발생하게 되면 모든 프로세서는 redundant side로 전환되어 위성을 safing하게 된다.

2-1. Fault Detection

탑재소프트웨어에서는 오류 검출을 위하여 CP(Critical Parameter)를 구성하여 위성의 운용 모드에 따라 오류를 검사하게 된다. OBC는 RDU와 ECU의 health 정보를 관리하며 1553B 통신의 상태를 체크한다. ECU와 RDU는 하드웨어 유닛의 오류를 검사하며 OBC와의 정상적인 통신이 이루어지는지를 검사한다. 아래의 표 1은 OBC와 ECU의 Critical Parameter Table 보여준다. 탑재소프트웨어에서는 검출된 오류가 Threshold Count보다 많이 발생하게 되면, Failover 조건이 발생한 것으로 판단하여 WDT Timeout에 의한 프로세서 전환을 유도하게 된다.

OBC					
Index	GDA Address	Submode	Limit Type	Threshold Count	Description
0	KFS_oabc_error	KFS_CP_ALL_MODES	KFS_UPPER_LIM_SET	1	Double-bit EDAC Error
1	KFS_rdu_hb_failed	KFS_CP_ALL_MODES	KFS_UPPER_LIM_SET	2	RDU Heartbeat Failure Flag
2	KFS_ecu_hb_failed	KFS_CP_ALL_MODES	KFS_UPPER_LIM_SET	2	ECU Heartbeat Failure Flag
3	KFS_rtcs_finished	KFS_CP_ALL_MODES	KFS_BOTH_LIMS_SET	1	RTCS finished flag
4	KFS_1553_mem_critical_err_cnt	KFS_CP_ALL_MODES	KFS_UPPER_LIM_SET	2	System 1553B Non-Critical Message Errors
5	KFS_1553_critical_err_cnt	KFS_CP_ALL_MODES	KFS_UPPER_LIM_SET	2	System 1553B Critical Message Errors
ECU					
Index	GDA Address	Submode	Limit Type	Threshold Count	Description
0	KFS_oabc_error	KFS_CP_ALL_MODES	KFS_UPPER_LIM_SET	1	Double-bit EDAC Error
1	KFS_obc_msg_missed	KFS_CP_ALL_MODES	KFS_UPPER_LIM_SET	2	OBC satellite status message missing
2	KFS_a_d_conv_fault	KFS_CP_ALL_MODES	KFS_BOTH_LIMS_SET	4	A/D Converter Fault
3	KFS_rtcs_finished	KFS_CP_ALL_MODES	KFS_BOTH_LIMS_SET	1	RTCS finished flag
4	KFS_ecu_code_dpen_flag	KFS_CP_ALL_MODES	KFS_UPPER_LIM_SET	1	Excess battery depth of discharge/Anomalous depth of discharge in Sun/Failure to reach taper discharge/Battery temperature out of limit

표 1. OBC/ECU Critical Parameter Table

2-2. Processor Failover Flow

위성이 정상적으로 운영될 경우 OBC는 RDU/ECU로부터 CODA 메시지와 프로세서의 상태를 알려주는 PSM 메시지 주기적으로 받아 모니터링하게 되며, RDU/ECU는 또한 OBC로부터 OBT(On-Board Time)와 OBC의 상태정보인 SSM 메시지를 받아 OBC의 상태를 모니터링 하게 된다. 아래의 그림3은 RDU에서 오류가 검출되어 전체 프로세서가 redundant side로 전환되는 과정을 보여준다.

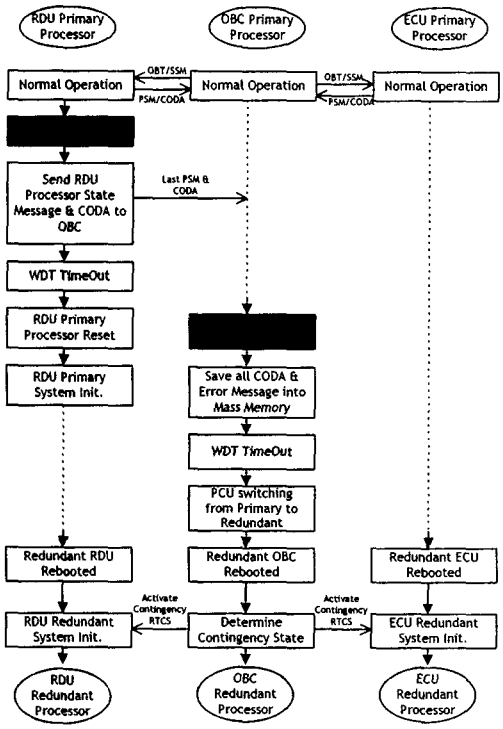

그림 3. On-Board Fault Management Flow

OBC가 WDT Timeout이 발생하게 되면, PCU(Power Control Unit)에 의하여 모든 전원이 primary에서 redundant로 전환되게 되게 구성되어 있어, 동시에 모든 프로세서가 redundant로 전환되게 된다.

2-3. Failure Response

프로세서가 On-Board Fault Management에 의하여 Redundant 프로세서로 깨어나게 되면, OBC는 위성 초기 데이터(Wake-Up Clues)를 이용하여 위성의 상태를 Redundant Contingency State로 결정하며, 위성을 safing시키는 RTCS(Relative Timed Command Sequence)를 구동하게 된다. RTCS는 위성운용에 필요한 명령을 시간순서대로 시나리오별로 구성한 것으로 Mass Memory에 저장되어 있다. 최초 Initial RTCS가

구동되면 아래 그림 4와 같이 시간 순서대로 위성을 safing하는 RTCS들이 구동되게 된다. 위성이 안정화 된 이후 지상국에서는 위성의 Mass Memory에 저장되어 있는 오류정보를 추적하여 위성의 오류를 제거하고 위성을 정상적으로 전환하게 된다.

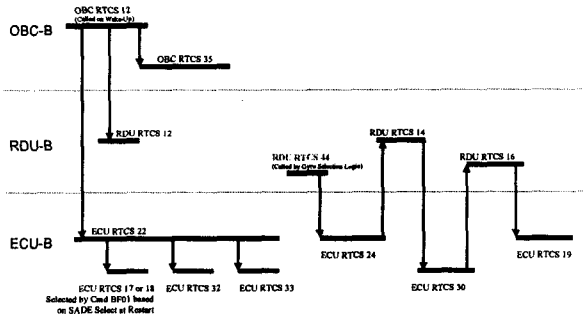

그림 4. Safing RTCS for KOMPSAT-2

3. Fault Management Test

다목적실용위성 2호의 전체적인 시스템 통합 시험과 함께 2년간 3단계에 걸쳐 Fault Management Test가 수행되었다. 1단계 테스트에서는 위성의 오류에 대한 trigger조건을 ETB(Electrical Test Bed)에서 ICE를 이용하여 수행되었으며, 2단계에서는 실제 CPU를 장착한 ETB에서 Failure trigger와 Failure response인 RTCS에 대한 테스트가 수행되어졌으며, 3단계에서는 실제 발사될 Flight Model(FM)에 대해서 Fault Management Test가 수행되었다. 아래의 그림 5는 Fault Management Test중의 하나인 SEU Mitigation에 대한 테스트 절차를 보여준다.

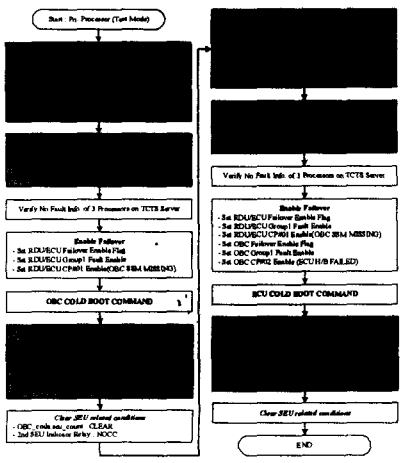

그림 5. CPU SEU Mitigation Test Procedures

위성의 recovery를 위하여 위성이 redundant로 전환되면, Mass Memory에 저장되어 있는 오류정보를 가지고 위성의 failover 원인을 분석하는 테스트도 동시에 이루어 졌다. 아래의 그림 6은 ECU 프로세서의 오류에 의하여 전체 시스템의 전환을 알려주는 OBC Startup CODA의 일부분이다. Startup CODA에는 위성의 마지막 정보를 저장하고 있으며 위성의 오류분석에 반드시 필요한 정보이다. 이러한 오류정보를 가지고 오류를 분석하여 위성을 정상적인 상태로 recovery 할 수 있게 된다.

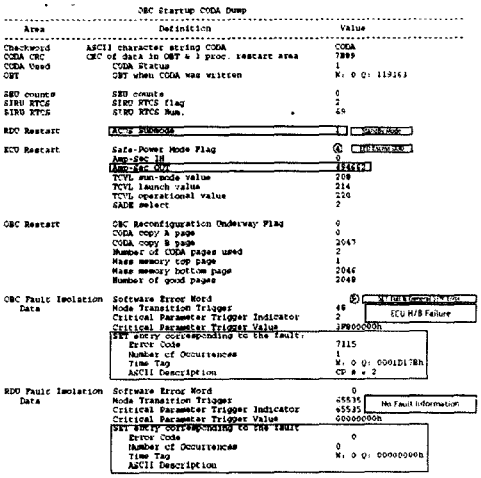

그림 6. OBC StartUp CODA

4. 결론

본 논문에서는 다목적실용위성 2호의 On-Board Fault Management에 대하여 설명하였다. On-Board Fault Management는 다른 테스트와 달리 위성의 안전과 임무에 직접적으로 연관되어 있으며, 어떠한 환경 하에서도 위성을 safing시켜야하는 중요한 역할을 담당하고 있다. 추후 계속적인 Fault Management 테스트가 수행될 되어 예정이며, 실제 위성운영에도 테스트한 절차를 그대로 적용할 예정이다.

5. 참고문헌

[1] KOMPSAT-2 Fault Management Design Report, 2001
[2] KOMPSAT-2 Fault Management Level-1 Test Procedures & Reports, 2002
[3] KOMPSAT-2 Fault Management Level-2 Test Procedures & Reports, 2003
[4] KOMPSAT-2 Fault Management Level-3 Test Procedures & Reports, 2003