KOMPSAT-2 Fault and Recovery Management

Myung-Jin Baek*, Na-Young Lee and Jung-Hoon Keum*****
Satellite System Department
Korea Aerospace Research Institute, Daejon City, Korea 305-600

Abstract

In this paper, KOMPSAT-2 on-board fault and ground recovery management design is addressesed in terms of hardware and software components which provide failure detection and spacecraft safing for anomalies which threaten spacecraft survival. It also includes ground real time up-commanding operation to recover the system safely. KOMPSAT-2 spacecraft fault and recovery management is designed such that the subsequent system configuration due to system initialization is initiated and controlled by processors. This paper will show that KOMPSAT-2 has a new design feature of CPU SEU mitigation for the possible upsets in the processor CPUs as a part of on-board fault management design. Recovery management of processor switching has two different ways: gang switching and individual switching. This paper will show that the difficulties of using multiple-processor system can be managed by proper design implementation and flight operation.

Key Word : KOMPSAT-2, Fault Management, Recovery Management

Introduction

Korea Multipurpose Satellite-2 (KOMPSAT-2) is high resolution multi-spectral earth observation satellite system to be launched in 2004. Main mission objective is to provide geo-information products based on the multi-spectral high resolution sensor called Multi-Spectral Camera (MSC) which will provide 1m panchromatic and 4m multi-spectral high resolution images. KOMPSAT-2 spacecraft bus has space-proven KOMPSAT-1 heritage design. KOMPSAT-2 is low earth orbit satellite of altitude of 685km so that it is orbiting the earth about 14 times a day. But, KOMPSAT-2 has only very limited time of ground contact about 8-10 minutes per orbit(total maximum 4 orbits a day) and it spends most of orbiting time without ground communication. Therefore, during the mission, in the event of a failure in any situation, KOMPSAT-2 is required to have on-board autonomous function of safing the spacecraft (called on-board fault management): fault detection, removal of fault effect and system reconfiguration for the safe mode. On the other hand, ground station is required to have the capability of performing fault monitoring and isolation, system reconfiguration to the primary equipment for recovery, and transition to normal operation(called ground recovery management).

In this paper, the KOMPSAT-2 on-board fault and ground recovery management design is addressesed in terms of hardware and software components which provide failure detection and spacecraft safing for anomalies which threaten spacecraft survival. It also includes ground real time up-commanding operation to recover the system safely. Due to inherent multiple processors system of the KOMPSAT-2, on-board fault and ground recovery management schemes for the

* Principal Researcher
E-mail : mjbaek@kari.re.kr, TEL: 042-860-2346, FAX: 042-860-2007
** Researcher
*** Senior Researcher

multiple-processor system is more complex than that of the single processor system. This paper will show that KOMPSAT-2 spacecraft fault and recovery management is designed such that the subsequent system configuration due to system initialization is initiated and controlled by processors. But these events all involve processor reset or power switching. All three processors are required to operate properly in any on-orbit operation state without ground intervention.

KOMPSAT-2 has equipped with Intel 80386 CPU in the on-board processors. In the event of CPU SEU occurrence, without proper treatment, spacecraft operation can be hung-up and result in mission failure at the end. This paper will show that KOMPSAT-2 has a new design feature of CPU SEU mitigation for the possible upsets in the processor CPUs as a part of the on-board fault management design.

Recovery management of processor switching has two different ways: gang switching and individual switching. Individual processor switching management is more complex than gang switching of the processors in terms of recovery management and system reconfiguration. This paper will show that the difficulties of using multiple-processor system can be managed by proper design implementation and flight operation.

On-board Fault and Ground Recovery Management Design

Capability of Subsystem Hardware Redundancy

KOMPSAT-2 has three on-board processors: On-Board Computer (OBC) for command, telemetry and data handling management, Remote Drive Unit (RDU) for attitude and orbit control management including propulsion subsystem, and Electrical power system Control Unit (ECU) for electrical power and thermal control management. These on-board processors are interfaced through MIL-STD-1553B data bus for basic communication and data handling function between them. Also, gyro and star trackers are interfaced through local MIL-STD-1553B data bus. Figure 1 shows KOMPSAT-2 electrical system block diagram and demonstrates how each processor is interfaced with other processors and with its subsidiary dedicated hardware units. Space proven hardware and fully redundant system for critical components maximize robust design and on-orbit performances.

Attitude and Orbit Control Subsystem(AOCS) provides the necessary attitude and orbit control, attitude determination, and safing function for the KOMPSAT-2 mission operation phase which is managed by RDU. A three-axis stabilization method with zero momentum bias

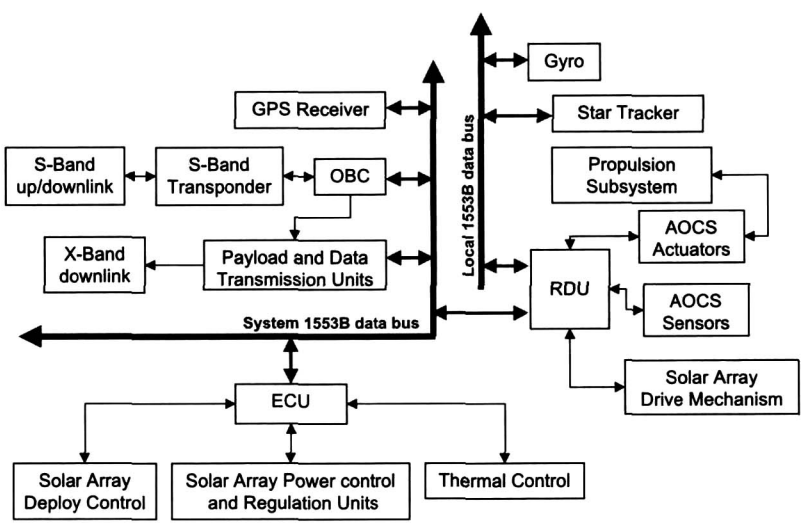

Fig. 1. KOMPSAT-2 Electrical System Block Diagram

Table 1. Subsystem Hardware Redundancy Capabilities

Function	Primary Component		Redundant Component
TC&RS	Processors	Primary (OBC, RDU, ECU)	Redundant (OBC, RDU, ECU)
	GPS Receiver and Antenna	Primary	Redundant
	Transponder	Transponder A	Transponder B
	RF Assembly	Diplexer A	Diplexer B
AOCS	Gyro	Gyro A, B, C (3 of 4)	Redundant Gyro D (internal) (3 of 4)
	Fine Sun Sensor(FSSA)	FSSA-1 (1 of 2)	FSSA-2
	Coarse Sun Sensor(CSSA)	CSSA "A" cell	CSSA "B" cell(internal)
	Earth Sensor(CES)	CES-1 (1 of 2)	CES-2
	Star Tracker(STR)	STR-1 (1 of 2)	STR-2
	Magnetometer	Primary	Redundant
	Reaction Wheel(RWA)	RWA (4 of 4)	RWA (3 of 4)
	Magnetic Torquer	"A" winding	"B" winding
	Valve Drive Electronics	Primary	Redundant
	Solar Array Drive Electronics(SADE)	Primary	Redundant
	Solar Array Drive Assembly(SADA)	"A" Motor Drive	"B" Motor Drive
EPS	Solar Array Regulator	ARM-1	ARM-2(internal)
	Battery	22 cells	21 cells (1 cell redundant)
	Deployment Device Controller	Primary	Redundant(internal)
	Power Control Unit	Primary decoder and DC/DC Converter	Redundant decoder and DC/DC Converter(internal)
	Battery Interface Box	Primary relay	Redundant relay(internal)
Propulsion	Iso-valve	Iso-valve A	Iso-valve B
	Thruster	Thruster Bank A	Thruster Bank B

closed-loop system is used for attitude control of the satellite. Fine earth and sun sensors provide precise pointing knowledge, while gyros perform attitude propagation between updates. Magnetic torquers and magnetometer are used for momentum unloading. Electrical Power Subsystem(EPS) generates, stores, regulates, and distributes electrical power for the payloads and the spacecraft bus. The solar array regulator operates as series regulators in conjunction with ECU to control battery charging. 22-cell, 21Ah super NiCd battery provides electrical energy during eclipse. The power control unit controls and distributes primary and secondary power as required by the various spacecraft bus and instruments loads. The Telemetry, Command and Ranging Subsystem (TC&RS) provides RF communications and ranging capability with S-band omni antennas, an RF assembly, and S-band transponders. Command storage, processing and distribution, telemetry input, formating and storage, data processing for the spacecraft are managed by the OBC. The OBC provides the bus controller for data management using a Mil-Std-1553B data Bus and 1 Gbit mass memory storage for satellite state of health and science data recording. Table 1 describes major subsystem hardware redundancy capabilities.

On-board Fault Management

In the event of a failure, KOMPSAT-2 is required to have on-board autonomous function of safing the spacecraft (called on-board fault management): fault detection, removal of fault effect

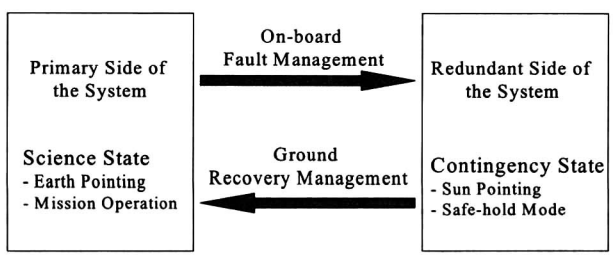

Fig. 2. KOMPSAT-2 Fault and Recovery Management

Table 2. Hardware and Software Fault Management Functions

Failure Mode	Fault Detection	Fault Management Action	Fault Management Effects
GPS Receiver	Loss of earth pointing	WDT Timeout by FSW	Fail safe to Safe-Hold Mode - GPS Receivers off
OBC, RDU, ECU (primary)	SEU Occurrence	WDT Timeout by FSW	Fail safe to Backup Mode - Redundant processors on
	WDT can not reset the timeout	WDT Timeout by FSW	Fail safe to Safe-Hold Mode - Redundant processors on
	Heartbeat failure	WDT Timeout by FSW	Fail safe to Safe-Hold Mode - Redundant processors on
1553B Data Bus	1553B error	WDT Timeout by FSW	Fail safe to Safe-Hold Mode - Redundant processors on
Solar Array Regulator (primary)	No taper charge, Excessive Battery DOD	WDT Timeout by FSW	Fail safe to Safe-Hold Mode - Redundant ARM used
Power Control Unit	Secondary power undervoltage	UV detector	Fail safe to Safe-Hold Mode - Redundant users on
CSSA (primary)	Loss of sun pointing	WDT Timeout by FSW	Fail safe to Safe-Hold Mode - Redundant RDU on
Valve Drive Electroncs (VDE)	Excessive Attitude Rate	WDT Timeout by FSW	Fail safe to Safe-Hold Mode - Redundant VDE on
Thrusters (primary)	Excessive Attitude Rate	WDT Timeout by FSW	Fail safe to Safe-Hold Mode - Redundant DTM on
SADE (primary)	Excessive attitude rate	WDT Timeout by FSW	Fail safe to Safe-Hold Mode - Redundant SADE on
SADA (primary)	Excessive attitude rate	WDT Timeout by FSW	Fail safe to Safe-Hold Mode - Redundant SADA used
RWA	Anomalous wheel speed	WDT Timeout by FSW	Fail safe to Safe-Hold Mode - RWAs off
Magnetic Torquer	Anomalous wheel speed	WDT Timeout by FSW	Fail safe to Safe-Hold Mode - Magnetic Torquer off
FSSA	Loss of earth pointing	WDT Timeout by FSW	Fail safe to Safe-Hold Mode
Magnetometer	Anomalous wheel speed	WDT Timeout by FSW	Fail safe to Safe-Hold Mode
CES	Loss of earth pointing	WDT Timeout by FSW	Fail safe to Safe-Hold Mode - CESs off
Gyro	Excessive attitude rate	WDT Timeout by FSW	Fail safe to Safe-Hold Mode - new gyro combination

Table 3. System Reconfiguration of Normal and Contingency Operation

Function	Normal Operation	Contingency Operation	
Control Mode	Wheel Based	Thruster Based	Wheel Based
Spacecraft Flight Configuration	Earth Pointing	Sun Pointing	Sun Pointing
Payload Operation	Used	Not Used	Not Used
On-board Processors	Primary	Redundant	Redundant
1553B Data Bus	Primary Bus	Redudant Bus	Redudant Bus
Earth Sensor	Used	Not Used	Not Used
Fine Sun Sensor	Used	Not Used	Not Used
Coarse Sun Sensor	Not Used	Used	Used
Star Trackers	Used	Not Used	Not Used
Gyros	Used	Used	Used
Reaction Wheels	Used	Not Used	Used
Magnetometer	Used	Not Used	Not Used
Magnetic Torquer	Used	Not Used	Used
Thrusters	Not Used	Used	Not Used
Solar Array Drive Mechanism	Rotating	Fixed	Fixed
GPS Receiver	Used	Not Used	Not Used
Solar Array Regulator	Primary Used	Redudant Used	Redudant Used
Heaters	Nominal Heaters	Survial Heaters	Survial Heaters

and system reconfiguration for contingency state operations, turn off active equipment, reconfigure the system in the redundant equipment, and maintain solar array sun pointing with minimum power consumption until ground intervention. All autonomous safing procedures are one-way, from the primary to the redundant equipment. On the other hand, ground station is required to have the capability of performing fault monitoring and isolation, system reconfiguration to the primary equipment for recovery, and transition to mission operational state(called recovery management). Figure 2 describes the basic concept of KOMPSAT-2 fault and recovery management.

Table 2 describes hardware failure mode, fault detection, fault management action taken by fault detection, and end effect by fault management. All fault detections and fault management actions are controlled and governed by flight software except power control unit secondary power undervoltage which is detected and actioned by undervoltage detector. Please note that safe-hold mode is thruster based control and backup mode is reaction wheel based control which is related to the Table 3.

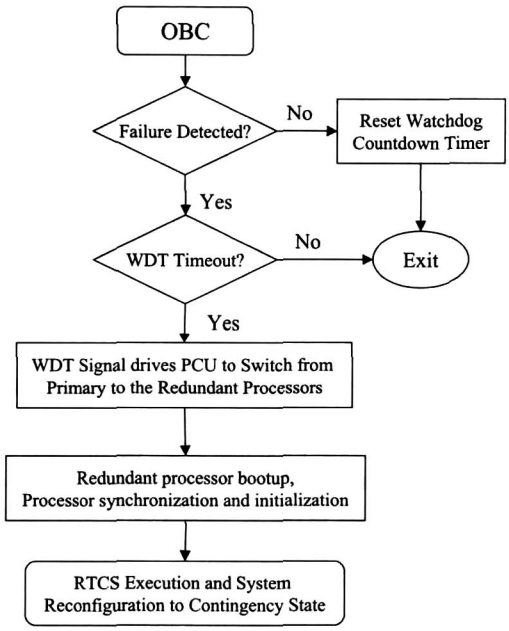

Fig. 3. On-board Fault Management Flow caused by WDT Timeout

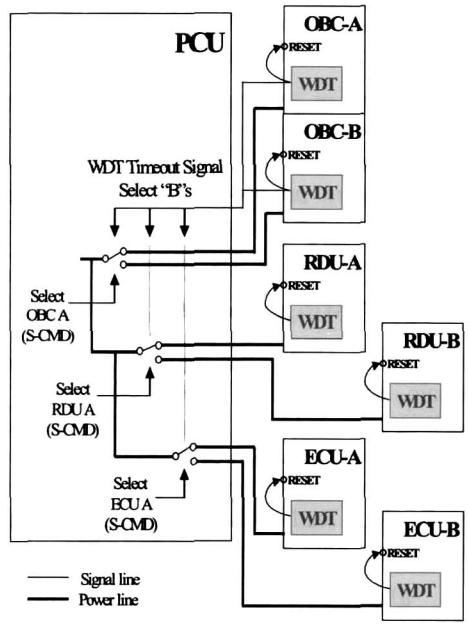

Fig. 4. Processor Power Management

Table 3 describes major hardware utilization of normal and contingency operation. Functions of normal operation explain the system configuration before fault management action occurs. Contingency operation explains system configuration after fault management actions occurred. As shown in the Figure 2 and Table 3, the system reconfiguration includes processors reconfiguration both from the primary to the redundant side (performed as part of an on-orbit autonomous fault management action) and from the redundant to the primary side (performed as part of a recovery management action from the ground). Processor reconfiguration and its switching mechanism design is the main part of the system reconfiguration because it finally selects key hardware and software configuration, such as attitude control mode, attitude control sensors and actuators, battery discharge and charge mode and thermal control mode, by pre-defined stored command sequences called Relative Timed Command Sequences (RTCS) embedded in the processor EEPROM before launch. An RTCS consists of a sequence of spacecraft commands with relative time delay between each command. Upon RTCS execution, the commands are sequentially executed with the specified inter-command delays.

Figure 3 shows on-board fault management flow caused by WDT timeout. KOMPSAT-2 on-board fault management design employs on-board software logic, hardware circuits, and hardware redundancy. Each processor is equipped with a Watch Dog Timer (WDT) countdown circuit. Under normal conditions the flight software executing on the respective processor outputs a command to reset the WDT circuit prior to time-out. A time-out event is caused by either CPU fault (hard processor failure) or WDT circuit fault (A failure in the WDT circuitry causes an inadvertent WDT time-out). Also, the OBC flight software monitors the health of the ECU and RDU. Periodically the OBC reads a status message from each processor (ECU and RDU) which includes state-of-health information such as battery state of charge or attitude control. If either of these units fails, or an OBC internal error is detected, the OBC flight software performs a processor reconfiguration procedure as shown in the Figure 3.

⇒ It allows its WDT circuit to time-out. The OBC WDT circuit output is sent to the Power Control Unit (PCU). On receipt of this signal the PCU reconfigures the processors by applying power to the redundant processors.

⇒ All redundant processors boot up, go through synchronization and initialization process.
⇒ Pre-defined RTCSs executed for system reconfiguration to contingency state as described in the Table 3.

Processor switching is controlled by power switching relays in the PCU as depicted in Figure 4. Processor reconfiguration from the primary to the redundant side is quite straightforward. WDT timeout signal drives the PCU to turn active primary processors off and turn redundant processors on all at a time, so called gang switching. All of processors boot up in the redundant side at the same time and performs processor synchronization and initialization process including 1553B data bus configuration.

CPU SEU Mitigation Management

KOMPSAT-2 has equipped with Intel 80386 CPU in the on-board processors. In the public domain, 80386 CPU is known sensitive to space radiation. Based on the space radiation analysis [5], it is expected to experience CPU SEU during mission operation. Frequent SEU occurrence can cause excessive usage of propellant and result in mission failure at the end if proper mitigation design is not implemented. But, significant design change in the existing CPU board may cause design risk. Rather than, minimizing design change and utilizing existing hardware and software capabilities, new on-board CPU SEU mitigation management has been designed as follow:

a) Detection of SEU occurrence using software function based on existing fault management design method - usage of fault management information in contingency operation data area
b) Selection of mitigation design for CPU hardware hang-up
c) Utilization of wheel based sun pointing control algorithm in the event of fault management action caused by CPU SEU fault
d) Ground command override capability of SEU mitigation logic enable and disable.

CPU SEU mitigation management has mainly 6 control gates(CG) to determine autonomously whether the system must be reconfigured either thruster based control or reaction wheel based control as shown in the Figure 5.

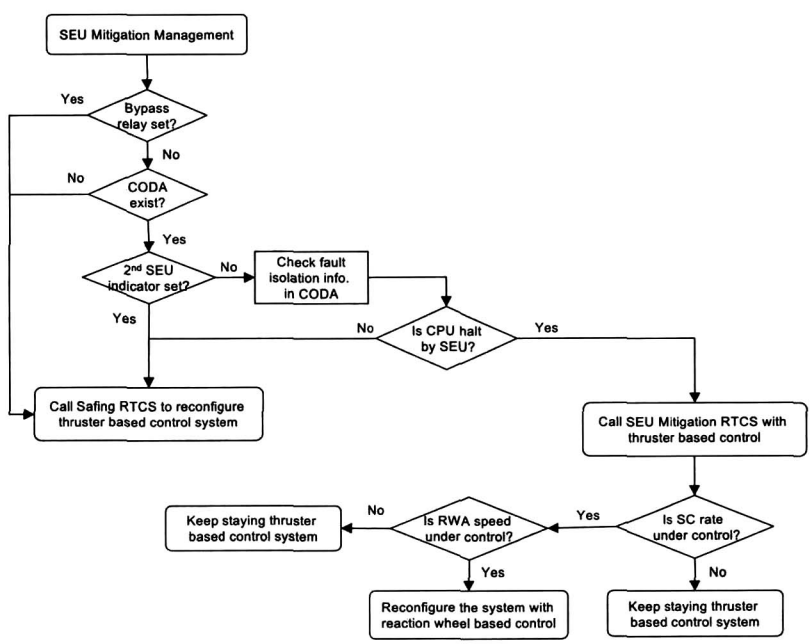

Fig. 5. CPU SEU Mitigation Flow

1) SEU Mitigation Bypass CG: In case CPU has many SEUs in space, ground enables SEU mitigation module by not setting bypass relay.
2) CODA CG: In case CODA(Contingency Operation Data Area) does not exist, the system is reconfigured with thruster based control, even if SEU bypass relay is not set.
3) 2nd SEU Indicator CG: In case this indicator is set, the system is reconfigured with thruster based control. And exit.
4) Cause of CPU halt CG: If CPU was hung-up by SEU, then the system is reconfigured with thruster based control and proceed with Spacecraft Rate CG. Otherwise, the system is reconfigured with thruster based control. And exit.
5) Spacecraft Rate CG: If spacecraft rate is under control, then the system proceed with Reaction Wheel Speed CG. Otherwise, the system is reconfigured with thruster based control. And exit.
6) Reaction Wheel Speed CG: If reaction wheel speed is under control, then the system is reconfigured with reaction wheel based control. Otherwise, the system is reconfigured with thruster based control.

Ground Recovery Management

After ground isolates the cause of the failure, spacecraft recovery concept is to switch back good ones to the primary side. Unlike on-board fault management, the recovery action must be initiated by ground command. The first action is to switch good processors back to primary side. In the event that one processor is the cause of the failure, the all of three processors can not be switched back to the primary side. In this case processor switching must be followed by individual switching recovery procedure. Otherwise, all processors can be switched back to the primary side by gang switching recovery procedure. In the Table 4, the first three columns describe the combination of processors that can be recoverable and the last column describes required ground recovery action and its type of commands to be used. In the table, P stands for primary side and R for redundant side. The last row explains there will be no ground action required if ground wants to run the spacecraft in the redundant side. Therefore, from the ground operation point of view, the recovery management of the processors is more complex than that of fault management in the following aspects:

1) Ground must have the capability of switching processors either all at a time or individually one at a time (called individual switching) depending on the failure scenario of the processors.
2) Individual recovery procedure must be designed such that one processor switching should not cause unnecessary safing action or total system reconfiguration.

Gang switching recovery procedure is designed to use hardware special command only. Hardware special command process is from ground via on-board link function to the PCU directly without software command processing. The advantage of using hardware special command is to

Table 4. Acceptable Recovery Combination

Combination of Processors			Required Ground Recovery Action (Type of Command)
OBC	RDU	ECU	
P	P	P	Gang switching (Hardware Special Command)
P	P	R	Individual switching (Both Software and Hardware Special Commands)
P	R	P	
P	R	R	
R	P	P	
R	P	R	
R	R	P	
R	R	R	No Action Required

make sure command reception and execution without software command processing. As shown in the Figure 4, a hardware special command for the selection of primary processor had been allocated to each processor. In the figure, S-CMD stands for hardware special command. Therefore, utilizing reliable hardware special command and existing autonomous system configuration function, the recovery could be guaranteed with minimum ground operations. Please note that the safing action results in the system reconfiguration in the redundant side.

Individual switching recovery procedure is quite different from that of gang switching recovery. Simply switching a processor will break the rule described in the fault management design. That is because, as described in the Figure 3, the switching processor can not provide its status to the OBC while it is booting up. In that case the OBC will interpret as processor fault and initiate the safing action as designed. Therefore, individual switching recovery procedure must be designed to avoid unnecessary fault management action when switching one processor back to the primary side while other two processors are running. The following procedures describe the individual switching recovery procedures. Since the OBC acts as bus controller and the other processors act as remote terminal of 1553B data bus, the recovery procedure of the OBC and RDU/ECU are different. Recovery procedure for the OBC is as following:

a. Disable processor response to critical fault.
b. Change 1553B data bus communication mode into SPARSE mode.
c. Reconfigure OBC.
d. Wait for the three-processor synchronization.
e. Enable processor response to critical fault.
f. Change 1553B data bus communication mode to NORMAL mode.

Recovery procedure for RDU or ECU is as follow:

a. Disable processor response to critical fault.
b. Change 1553B data bus communication mode into SPARSE mode.
c. Reconfigure RDU or ECU.
d. Wait for the three-processor synchronization.
e. Command to transmit contingency operation data and on-board time to reconfigured processor waiting for the message from OBC.
f. Enable processor response to critical fault.
g. Change 1553B data bus communication mode to the NORMAL mode.
h. Select key subsystem hardware and software configuration.

As described in the above, compared to gang switching recovery operation, individual switching recovery operation demands many commands to be uploaded. Processor recovery operation is the most critical ground operation. Real time ground operation can be exposed to unexpected space to ground communication failure, such as ground antenna tracking malfunction or ground facility power down in the middle of real time recovery operation. To minimize the number of real time ground commanding operation, the KOMPSAT-2 design utilizes autonomous function such that just one ground command can activate a processor switching procedure and proceed with minimum system configuration to achieve attitude control or battery charging autonomously:

1) Make the recovery procedure RTCS and embed it in the OBC processor. That design provides the capability of achieving the processor switching procedure with a single ground command.
2) Make one processor be able to switch other processor using processor on-board software command, and vise versa. This is because hardware special command can not be embedded in the stored command for the future use. That design provides the capability of switching processors by themselves without direct ground command.
3) Make multiple-pass ground operation concept one processor recovery per one orbit.

Conclusions

In this paper, KOMPSAT-2 on-board fault and ground recovery management design is addressesed in terms of hardware and software components which provide failure detection and spacecraft safing for anomalies which threaten spacecraft survival. Subsystem hardware redundancy capabilities and fault management functions in terms of hardware and software have been identified. It was shown that processor reconfiguration and its switching mechanism design is the main part of the system reconfiguration of fault management because it finally selects key hardware and software configuration. New on-board CPU SEU mitigation management has been described utilizing existing hardware and software functions to minimize design risk. It was shown that individual processor switching management is more complex than gang switching of the processors in terms of recovery management and system reconfiguration. But, this paper shows that the difficulties of using multiple-processor system can be managed by proper design implementation, ground operational procedure and flight operation.

Acknowledgement

This paper has been supported in part by the KOMPSAT-2 System Design and Development Project of the Korean Ministry of Science and Technology.

References

1. Baek, M. J.and Lee, J. I., 2002, "On-board Management of Multiple Processor Spacecraft System," IEEE Transaction on Aerospace and Electronic Systems, submitted

2. Korea Aerospace Research Institute, 2002, "KOMPSAT-2 Preliminary Fault Management Design," KOMPSAT-2 document

3. Korea Aerospace Research Institute, 2001, "KOMPSAT-2 Spacecraft Bus Preliminary Design Audit", KOMPSAT-2 document

4. Korea Aerospace Research Institute, 2001, "KOMPSAT-2 Preliminary Fault Management Design Report", KOMPSAT-2 design report

5. Baek, M. J., Kim, D. Y., and Kim, H. J., 2001, "The Analysis on Space Radiation Environment and Effect on KOMPSAT-2 Spacecraft(II): Single Event Effect," J. of KSSS, Vol. 18, No 2, pp 163-173

6. Baek, M. J., Lee, J. I., and Kim, H. J., 2001, "KOMPSAT-2 CPU SEU Mitigation Design," Proceedings of the KSAS Fall Annual Meeting 2001, pp 41-44

7. Baek, M. J., 1999, "A Study on KOMPSAT Fault Management and Test," J. of KSAS, Vol. 27, No 8, pp 158-169

8. Korea Aerospace Research Institute, 1999, "KOMPSAT-1 Fault Management Test Plan and Procedure", KOMPSAT-2 Test Plan and Procedure