KOMPSAT-2

저궤도 상용위성 개발을 위한 시스템 신뢰성 엔지니어링 적용사례

항공우주연구원

이창호

2003년 5월 15일

KOMPSAT-2

Contents

KOMPSAT-2

Reliability Tasks for SC Development

Generally Required Work Scope

System and Mission Definitions
- Requirements
- Specifications
- Success & Fail Definition

Product Design
- Part & Material Selection
- Designs
- Design Verification

Manufacturing and Verification
- Process Specification
- Failure Reporting, Review, and Corrective Actions

Design Assurance
- Part & Material Selection Criteria
- Reliable Design Criteria
- Reliability Assessment
- Failure Mode & Effect Analysis
- Criticality Analysis

Subcontractor Control
- Quality Audits
- Design Review
- Test Result & Trend Analysis

Quality Assurance
- Process Control
- Hardware Inspection
- MRB / FRB Coordination

KOMPSAT-2

Reliability Tasks for SC Development

Tasks of MIL-STD-785B

Task	Program Phase			
	CONCEP	VALID	FSED	PROD
Program Surveillance and Control				
Reliability Program Plan	S	S ①②	G ①②	GC ①②
Monitor / Control of Subcontractors and Supplier	S	S	G	G
Program Review	S	S ①	G ①	G ①
Failure Reporting, Analysis, and Corrective Action System (FRACAS)	NA	S	G	G
Failure Review Board (FRB)	NA	S ①	G	G
Design and Evaluation				
Reliability Modeling	S	S ①	G ①	GC ①
Reliability Allocations	S	G	G	GC
Reliability Predictions	S	S ①	G ①	GC ①
Failure Modes, Effects, and Criticality Analysis (FMECA)	S	S ①②	G ①②	GC ①②
Design and Evaluation				
Sneak Circuit Analysis (SCA)	NA	NA	G ②	GC ②
Electronic Parts/Circuits Tolerance Analysis	NA	NA	G	GC
Parts Program	S	S ①②	G ①	G ①

KOMPSAT-2

Reliability Tasks for SC Development

Tasks of MIL-STD-785B (Continued)

Task	Program Phase			
	CONCEP	VALID	FSED	PROD
Design and Evaluation				
Reliability Critical Item	S ①	S ①	G	G
Effects of Functional Testing, Storage, Handling, Packaging, Transportation, and Maintenance	NA	S ①	G	GC
Development and Production Testing				
Environmental Stress Screening (ESS)	NA	S	G	G
Reliability Development/Growth Test(RDGT) Program	NA	S ①	G ①	NA
Reliability Qualification Test(RQT) Program	NA	S ①	G ①	G ①
Development and Production Testing				
Production Reliability Acceptance Test(PRAT) Program	NA	NA	S	G ①③

CONCEP	Conceptual phase	VALID	Demonstration and validation phase
FSED	Full scale engineering development phase	PROD	Production phase
S	Selectively applicable	G	Generally applicable
GC	Generally applicable to design change only	NA	Not applicable
①	Requires considerable interpretation of intent to be cost effective		
②	MIL-STD-785 is not the primary implementation requirements		
③	Partial implementation to cost effectively prepare for future phase		

KOMPSAT-2

Reliability Tasks for SC Development

Tasks of KOMPSAT II

Normally, reliability program requirements are described in Product Assurance Requirements(PAR) and system requirement specification. These requirements will be flowed down to equipment specification.

KOMPSAT II reliability tasks.

- Reliability Program Plan
- EEE Part Derating Criteria

Mission & System Definition

- Reliability Allocation
- Reliability Prediction
- Failure Modes, Effects and Criticality Analysis
- Limited Life Items
- Part Stress Analysis
- Worst Case Analysis

Product Design (System & Equipment)

- Critical Item Control
- Test Results / Trend Analysis
- Failure Reporting, Analysis, and Corrective Actions
- Failure Review Board / Material Review Board

Manufacturing, System Integration, Test

Mission Definition

Overall Mission Requirements

The KOMPSAT II system shall allow the realization of 1m panchromatic and 4m multi-spectral high resolution image for GIS and the composition of printed maps and digitized maps. (SR00100)

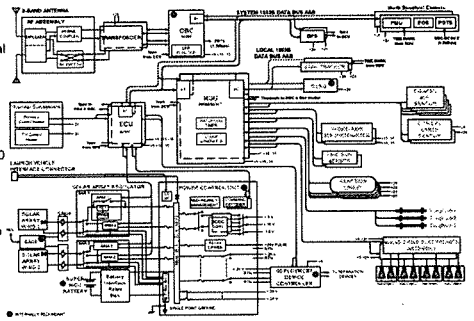
Mission

Mission Orbit Maintenance	Cartography	Communication & Data Processing
• Orbit Insertion • Maintaining Mission Orbit	• Attitude Control Capability • Pointing Capability • MS Image • PAN Image	• Data Processing & Storage • Downlink & Uplink • Command Processing
Environmental Compatibility	**Hardware Interface**	**SC Bus Power**
• LV Env. Compatibility • Orbit Env. compatibility	• SC-LV Interface • MSC-Bus Interface • Bus Internal Interface	• Power Design Life • Energy Balancing

System Definition

Functional Block Diagram Overview

- Modular Design.
- 3 processor / main-local 1553b bus.
- Single fault tolerant.
- Most critical function is redundant.
- Automatic initiation of safe mode transition.
- Automatic safing for 30 days without GS.
- Fuse protect primary power. UVD protect secondary power
- PS design compliant to EWR127-1
- No TCS SPF for over heat.



Reliability Allocation & Prediction

Introduction

General

The purpose of reliability allocation & prediction is to manage system reliability budget and to achieve mission reliability required at end of life.

Allocation & Prediction

- Reliability Allocation : Initially allocate by heritage information or preliminary prediction and update it as design matured. Allocated reliability is part of specification requirements.
- Reliability Prediction : Construct system reliability model and part reliability model (if required). Evaluate part reliability using available data (such as MIL-HDBK-217F Methods).

Reliability Enhancement

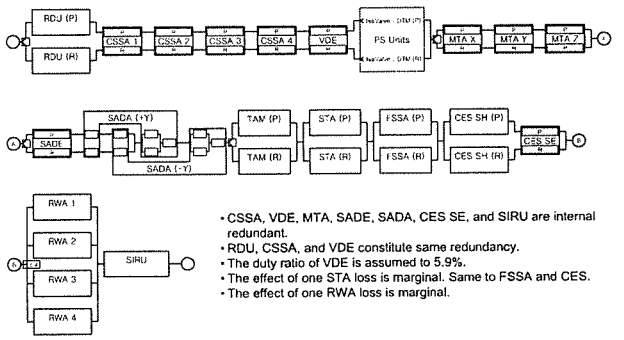
- Additional redundancy path
- Usage of higher level reliability part
- Lower part stress level

Interface with Other Reliability Task

	Reliability Prediction	
Part Stress Analysis	Part Stress Level	-
Criticality Analysis	-	Part Failure Rate
FMEA	-	Reliability Model

Reliability Allocation & Prediction

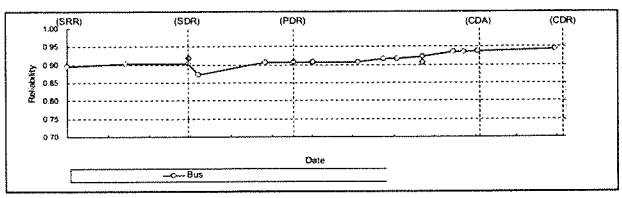
Example : AOCS Reliability Block Diagram



- CSSA, VDE, MTA, SADE, SADA, CES SE, and SIRU are internal redundant.
- RDU, CSSA, and VDE constitute same redundancy.
- The duty ratio of VDE is assumed to 5.9%.
- The effect of one STA loss is marginal. Same to FSSA and CES.
- The effect of one RWA loss is marginal.

Reliability Allocation & Prediction

Example : SC Reliability Requirements & Predictions



	Reliability Allocations	Estimated Reliability
EPS	0.96	All of the subsystem comply to the allocation requirements.
AOCS	0.97	
TC&RS	0.98	
PS	0.99	
TCS	0.98	
SMS	0.99	
BUS Total	*0.90*	

EEE Part Derating & Part Stress Analysis

Introduction

General

Hardware longevity and reliability are increased by derating parts so that applied stresses are well within ratings. All space flight hardware shall employ a comprehensive derating program.

Derating Requirements

KOMPSAT II program has own derating criteria. This criteria is based on the following documents.

- MIL-STD-1547B Electronic Parts, Materials, Processes for Space and Launch Vehicles.
- MIL-STD-975M NASA Standard EEE Parts List.
- ESA PSS-01-301 Derating Requirements applicable to EEE components
- PPL-21
- Military Specifications for EEE Part.

Interface with Other Reliability Task

	Part Stress Analysis	
Reliability Prediction	-	Part Stress Level
Worst Case Analysis	Derating Criteria	Part Stress Level
Critical Item Control	-	High Stressed Part

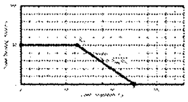
KOMPSAT-2

EEE Part Derating & Part Stress Analysis
Example : PCU DC-DC Converter (Diode)

- Part stress analysis is done for each parameter described in the derating requirements.
- Circuit analysis and thermal analysis results should be available to get reliable stress value

A. General Purpose, Rectifier, Switching, Pin/Schottky, and Thyristor

Parameter	Derating
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]



Desig.	Part No.	Description	Forward Current			Reverse Voltage			Power Dissipation		Rjc °C/W	Rbc °C/W	Board Tmp	Power (W)	Tj (°C)	Allowable Tj (°C)
			Der Max	Appl Max.	Ratio	Der Max	Appl Max.	Ratio	Der Max	Appl Max.						
CR001	JANTXV1N5806	DIODE, 1N5806, RECTIFIER	1.25	0.800	64.00	105.000	15.600	14.86	0.56	0.3077	20	14.06	69.251	0.3077	79.73	125.00
CR002	JANTXV1N5806	DIODE, 1N5806, RECTIFIER	1.25	0.800	64.00	105.000	34.000	32.38	0.56	0.3723	20	14.06	69.251	0.3723	81.93	125.00
CR003	JANTXV1N5811	DIODE, 1N5811, RECTIFIER	62.5	0.000	0.00	150.000	34.000	22.67	1.68	0.0000	10	11.64	74.186	0.0000	74.19	125.00
CR004	JANTXV1N5811	DIODE, 1N5811, RECTIFIER	62.5	0.000	0.00	150.000	34.000	22.67	1.68	0.0000	10	11.64	74.186	0.0000	74.19	125.00
CR005	JANTXV1N4150-1	DIODE, 1N4150-1, SWITCHING	0.1	0.00295	2.95	35.000	N/A	N/A	0.11	0.0023	100	70.9	72.906	0.0023	73.29	125.00
CR006	JANTXV1N5811	DIODE, 1N5811, RECTIFIER	62.5	0.200	0.32	150.000	34.000	22.67	1.68	0.0876	10	11.64	69.501	0.0876	71.40	125.00
CR007	JANTXV1N5816R	DIODE, 1N5816R, RECTIFIER	10	1.280	12.80	105.000	34.000	32.38	6.02	0.6307	1.5	0	70.311	0.6307	71.26	125.00
CR008	JANTXV1N5816R	DIODE, 1N5816R, RECTIFIER	10	1.280	12.80	105.000	15.600	14.86	6.02	0.5213	1.5	0	69.696	0.5213	70.48	125.00
CR009	JANTXV1N5816R	DIODE, 1N5816R, RECTIFIER	10	1.170	11.70	105.000	34.000	32.38	6.02	0.5766	1.5	0	71.379	0.5766	72.24	125.00
CR010	JANTXV1N5816R	DIODE, 1N5816R, RECTIFIER	10	1.170	11.70	105.000	15.600	14.86	6.02	0.4765	1.5	0	70.816	0.4765	71.53	125.00
CR011	JANTXV1N6306R	DIODE, 1N6306R, RECTIFIER	35	9.800	28.00	105.000	34.000	32.38	13.72	4.8290	0.8	0	86.884	4.8290	90.75	125.00
CR012	JANTXV1N6306R	DIODE, 1N6306R, RECTIFIER	35	9.800	28.00	105.000	5.559	5.29	14.70	3.9911	0.8	0	84.410	3.9911	87.60	125.00

KOMPSAT-2

Worst Case Analysis

General

WCA guaranties the end of life functionalities of the design. This analysis includes drift from initial tolerance, temperatures effects, radiations effects, ageing effects on components and on designs.

WCA is the intentional augmentation of electrical and thermal margin in order to increase the useful lifetime of a component. WCA is done because parameters of a components change with;
- Components dispersion
- Temperature
- Radiations
- End of life, etc.

Generally Used Methods

- Extreme Value Analysis
- Quadratic Analysis
- Monte Carlo Analysis
- Timing Analysis, etc.

Interface with Other Reliability Task

	Worst Case Analysis	
Part Stress Analysis	Derating Criteria	Part Stress Level

KOMPSAT-2

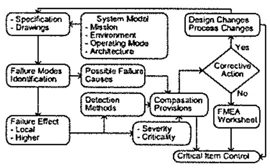
FMEA
Introduction

General

The Purpose of the FMEA is to analyze the results of effects of item failure on system operation and to classify each potential failure according to its severity. Verify fault tolerance design and system reliability model.

Failure Mode Identification

Specific failure mechanisms which could cause system failure modes are identified by FMEA process. Two approaches are used for identifying failure mode. Before PDR, functional FMEA (Top-Down) is performed. And after PDR, Hardware FMEA (Bottom-Up) is performed.



Interface with Other Reliability Task

The FMEA has interface with following tasks. The diagram on the right side shows the FMEA flow / work relationship in the KOMPSAT II program.

	FMEA	
Reliability Prediction	Reliability Model	-
Criticality Analysis	-	FMEA Results
Critical Item Control	-	SPFs

KOMPSAT-2

FMEA
Example : SADA System FMEA

FMEA Work Sheet

The format of KOMPSAT II FMEA sheet is compliant to MIL-STD-1629. Following table is system FMEA result for KOMPSAT II SADA.

- I.D. Number : reference code of failure mode.
- Operation Phase : mission phase code under consideration.
- Failure Effect : the effect of the failure mode on the subsystem or mission.
- Failure Detection Method : telemetries or SC response by which the failure could be detected.
- Compensating Provisions : the method by which the failure could be isolated or prevented.

I.D. Number	Item	Module / Function	Failure Modes and Causes	Operation Phase	Failure Effects		Failure Detection Methods		Compensating Provision	Severity
					System Effects	Mission Effects	Related TLMs	SC Response		
3.5.1	SADA	Provide the actuation necessary to rotate the solar array	Partial loss of motor torque.	D, E	Erratic SA rotation	Temprary SA power reduction No permanent effect on mission due to redundancy. Reliability degradation.	Battery DOD TLM, Battery taper charge TLM, SADA Position	Sun sensor error is increasing	Use redundant actuator	2R
3.5.2			Increased motor drag and power requirements.	D, E	Loss of SADA function	Significant loss of electrical power. Severe degradation of mission performance	Battery DOD TLM, Battery taper charge TLM, SADA Position	Sun sensor error is increasing	Classified as critical item C3.1	2
3.5.3			Erratic output rotation due to gear failure	D, E	Erratic SA rotation	Significant loss of electrical power. Severe degradation of mission performance	Battery DOD TLM, Battery taper charge TLM, SADA Position	Sun sensor error is increasing	Classified as critical item C3.1	2
3.5.4			Incorrect position sensing	D, E	Erratic SA rotation	Temprary SA power reduction No permanent effect on mission due to redundancy. Reliability degradation	SADA Position	Solar array angle will be abruptly jumping at certain time.	Use redundant potentiometer	2R

KOMPSAT-2

Criticality Analysis
Introduction

General

The purpose of the criticality analysis is to rank each potential failure mode identified in FMEA, according to the combined influence of severity classification and its probability of occurrence.

Criticality Evaluation

Criticality is the portion of the criticality number for the item due to one of its failure mode under particular severity classification. Criticality number is the comparative measure of system failure probability.

Criticality Matrix

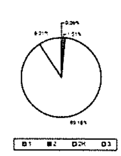
The criticality matrix provides the means of identifying and comparing each failure mode to all other failure modes with respect to severity. The horizontal axis of criticality matrix is the severity and the vertical axis is the criticality level

Interface with Other Reliability Task

	Criticality Analysis	
Reliability Prediction	Part Failure Rate	-
FMEA	FMEA Results	-
Critical Item Control	-	Higher Criticality Item

KOMPSAT-2

Criticality Analysis
Example : SC Bus End Effect List

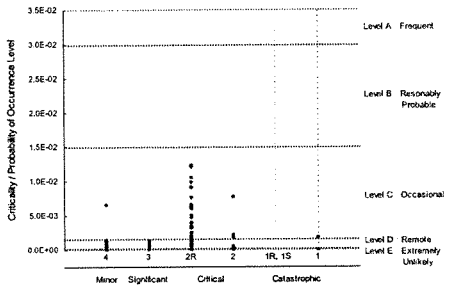


Most of the failure modes are less than severity level 2R.

Severity Class	End Effect		Description	Severity	Contribution
Mission Loss	Loss of Environmental Compatibility	Major	Catastrophic Structure Failure	1	Contribution is evaluated using failure occurrence rate
	Degraded SC Bus Power	Major	- Major Power Reduction - Cannot Deploy SA	2	
	Loss of Communication & Data Processing	Major	- Processor Function Failure S-Band Communication Failure	2	
Major Mission Degradation	Degraded SC Bus Power	Major	- Degraded Power Generation - Power Distribution Failure	2	
	Degraded Mission Orbit Maintenance	Major	- Loss of Propellant (Leak, Saturation)	2	
Reliability Degradation (due to loss of the redundancy)	Degraded SC Bus Power	Temporary	- Degraded Power Generation - Power Distribution Failure - Increased Noise or Increased Stress - Power Status TLM Loss	2R	
	Loss of Hardware Interface	Temporary	- Power Distribution Failure - Hardware Interface Failure - TLM / CMD Decoding / Encoding Failure	2R	
	Degraded of Hardware Interface	Temporary	- Increased Noise or Increased Stress	2R	
	Loss of Communication & Data Processing	Temporary	- Processor Function Failure - Loss of Downlink Function - TLM / CMD Decoding / Encoding Failure	2R	
	Degraded Communication & Data Processing	Temporary	- Loss of GPS Function	2R	
	Loss of Cartography	Temporary	- Loss of Sun Pointing Reference Loss of 3-Axis Reference - Loss of SC Attitude - Loss of Image (PAN, MS)	2R	
	Loss of Mission Orbit Maintenance	Temporary	- Loss of Thruster Control	2R	
	Reduced Functional or Safety Margin	Marginal	Reduced Safety Inhibits - Loss of Contigency Monitoring - Reduced Functional Margin	2R	
Reliability Degradation (due to loss of the margin)	Degraded Cartography	Marginal	- Degraded Attitude Control - Degraded Image	2R	
	Degraded Environmental Compatibility	Marginal	- Degraded Temp Control	2R	
Minor Mission Degradation	Degraded Environmental Compatibility	Significant	- Reduced Contingency Propellant	3	
	Degraded SC Bus Power	Significant	Power Status TLM Loss - Marginal Power Reduction	3	
	Degraded Communication & Data Processing	Significant	- Reduced Link Margin and FOV	3	
	Degraded Cartography	Significant	- Derraded Image	3	
	Degraded Mission Orbit Maintenance	Significant	- OTM or Isolve Malfunction	3	

Criticality Analysis

Example : SC Bus Criticality Matrix



Most of the failure modes are classified as 'Remote' or 'Extremely Unlikely'.

Limited Life Item Analysis

Introduction

General

Limited Life Items are the hardware subject to degradation due to age, operating time, or cycles that have an expected life of less than twice the mission life, or the hardware which require special ground operation conditions.

Potential Limited Life Items

Items reviewed include the deployment mechanisms, solar arrays, thermal control surfaces, rotating equipment, switches, thermostats, relays, battery, and propulsion time or cycle-sensitive hardware. The effects of thermal cycles, temperature extremes, wear, fatigue, and lubricant degradation were considered.

Limited Life Item Control

The cumulative operation time or cycle of the limited life item should be traced during the development and operation period(if required).

Interface with Other Reliability Task

Limited Life Item Analysis

FMEA	-	Wear Out Effect
Critical Item Control	-	Limited Life Items

Critical Item Control

Introduction

General

Critical item control identifies parts or assemblies that have above average reliability risk and providing special attention procedures to reduce this risk.

Critical Item Control

A critical item is defined as one that requires additional precautions or attention because a failure of the item would significantly affect spacecraft performance (such as SPFs).
Following criteria are used to identify critical items.

- Severity in the system level FMEA or criticality analysis result (which is higher than '2')
- Limited life items
- PMPCB issues
- Subcontractor's critical item list, etc.

Each item appearing herein has been designated as requiring special attention in design, manufacturing, test and/or handling.

Interface with Other Reliability Task

Critical Item Control

FMEA	SPFs	-
Criticality Analysis	Higher Criticality Item	-
Part Stress Analysis	High Stressed Part	-
MRB / FRB	-	Nonconformance to CI Plan

Critical Item Control

Example : SC Critical Items List

No	Critical Item	Implementation Status	Design & Part Procurement	Equipment Manufacturing	AIT & Launch Campaign	Operation
C1.1	On-Orbit ESD Effect of Solar Cell	Closed	✓			
C1.2	Solar Array to BAD A Connector	To be implemented		✓	✓	
C1.3	SAR ARM Selection Relay	Closed	✓			
C1.4	PCU ARM Parallel Fusing	Characterization test remains	✓			
C1.5	PCU ARM Fuse Bus Protection	Closed	✓			
C1.6	PCU Primary Power Bus	ATP activity remains		✓		
C1.7	PCU Secondary Power Bus	ATP activity remains		✓		
C1.8	DC-DC Converter Selection Relay	Closed		✓		
C1.9	Processor Unit Selection Relay	Closed		✓		
C1.10	PCU Decoder Selection Relay	Closed		✓		
C1.11	BRB Relay	Closed	✓			
C1.12	BRB Primary Power Bus	ATP activity remains		✓		
C1.13	Battery Assembly	ATP activity remains		✓		
C1.14	Battery Storage	AIT activity remains			✓	
C1.15	DC Harness between Battery and PCU	ATP & AIT activity remains	✓	✓	✓	
C1.16	DC Harness between SAR and PCU	ATP & AIT activity remains	✓	✓	✓	
C2.1	Nadir S-band Antenna	AIT activity remains			✓	
C2.2	Nadir S-band RF Cable Assy	AIT activity remains			✓	
C2.3	RF Assy Internal RF Connection	AIT activity remains			✓	
C2.4	RF Switch, Diplexer, and Hybrid Coupler	Closed	✓			

Above table is part of the summary of critical item list. The implementation status for each item will be traced through development and mission phase.

Summary

- **KOMPSAT II Part Program guarantees the reliability of EEE parts.**
- **Most of the EEE parts are correctly derated with respect to the program derating criteria.**
- **FMECA has verified the system fault tolerance design and system reliability model.**
- **End of life mission performance is verified by worst case analysis and limited life items analysis.**
- **Potential reliability weaknesses are controlled by critical item control plan.**