

## 다목적실용위성 2호기 신뢰성 및 FMECA

이창호\*

### Reliability Prediction and FMECA for KOMPSAT-2

Chang-Ho Lee\*

#### Abstract

The purpose of reliability prediction is to estimate the basic reliability and mission reliability of system and to make a determination of whether these reliability requirements can be achieved with the proposed design. Also, potential design weakness can be identified through the FMECA process. This technical memo summarizes the KOMPSAT-2 reliability and FMECA analysis results.

#### 초 록

신뢰성 예측의 목적은 시스템의 임무를 달성하기까지 기대되는 신뢰성을 평가하여 시스템의 설계가 할당된 요구조건을 만족하도록 이루어졌는지를 확인하는 것이다. 또한 FMECA를 통하여는 설계상의 잠재적인 위험요소를 식별하여 설계의 개선 및 공정의 개선을 도모 할 수 있다. 본 기술 논문은 아리랑 위성 2호기에 대해서 수행된 신뢰성 및 FMECA 결과를 요약하고 있다.

키워드 : 신뢰성(reliability), 고장모드해석(FMEA), 중요도 해석(criticality analysis)

#### 1. 서 론

신뢰성 해석의 목적은 임무 말기(End Of Life, EOL)에서의 시스템에 주어진 임무 요구조건을 만족할 수 있는 확률을 평가하고, 시스템에 부여된 하나 이상의 임무 수행에 영향을 줄 수 있는 고장 모드(Failure Mode)를 확인하여 시스템이 고장에 대해 갖는 내성(Tolerance)을 평가하는 것이다. 이러한 해석은 크게 신뢰성 예측(Reliability Prediction), 고장 모드 분석(Failure Mode & Effect Analysis), 중요도 분석(Criticality

Analysis)으로 구분 될 수 있으며, 이에 더하여 부품 스트레스 해석(Part Stress Analysis), 제한 수명 해석(Limited Life Analysis) 및 최악 경우 분석(Worst Case Analysis) 또한 신뢰성 해석의 범주에 포함될 수 있다. 본 기술논문에서는 다목적실용위성 2호의 개발을 위하여 수행된 신뢰성 예측, 고장 모드 분석, 중요도 분석의 결과를 제시하고자 한다.

\* 위성본체 그룹/chlee@kari.re.kr

## 2. 신뢰성 할당(Allocation) 및 예측

본체에 대한 신뢰성 할당 및 예측은 다목적실용위성 2호기 제품보증 요구조건(KOMPSAT-2 Product Assurance Requirement)에서 정의된 바대로 수행되었다. 또한 탑재체인 MSC의 신뢰성 예측은 개발사인 ELOP의 신뢰성 보고서를 바탕으로 하여 이루어 졌다.

신뢰성 예측은 개발 프로그램의 전 기간 중에 수행되며 효율적인 개발 관리를 위해서 Redundancy 및 Fault Management 설계와 밀접한 관계를 맺으며 수행되어야 한다.

### 2.1 부품 수준의 신뢰성 평가

다목적실용위성 2호기와 같은 상용위성의 경우 대부분의 설계에 고 신뢰도 부품(High Reliability Part)을 사용하고 있다. 따라서 이들 위성에 대한 신뢰성 예측은 우선적으로 MIL-HDBK-217F에 준하여 수행된다. 다목적실용위성 2호기 프로그램의 경우에도 MIL-HDBK-217F에 따른 신뢰성 예측의 수행을 제품보증 요구조건으로서 요구하고 있다. 따라서 대부분의 전장품 제조사는 신뢰성 예측 보고서를 제공하였으며 이에 따라 다목적실용위성 2호기의 시스템 신뢰성이 계산되었다. 신뢰성 예측에 사용된 신뢰성 자료는 다음의 Ground Rule에 따라 참조되거나 계산되었다.

- 제작사로부터의 부품 목록(Engineering Part List)이나 설계 다이어그램(Schematic Diagram) 등의 설계 자료와 함께 부품의 스트레스 수준에 대한 해석 결과가 제공된 경우에는 MIL-HDBK-217F에 따라 부품 스트레스 신뢰성 해석(Part Stress Reliability Prediction)이 수행되었다.
- 부품 목록(Engineering Part List)이나 설계 다이어그램(Schematic Diagram) 등의 설계 자료는 제공 되었으나 부품의 스트레스 수준을 알 수 없는 경우에는 일반적인 스트레스 수준을 가정하여 MIL-HDBK-217F 또는

ESA PSS-01-302의 부품 계수 신뢰성 해석(Part Count Reliability Prediction)이 수행되었다.

- 부품에 대한 정보가 MIL-HDBK-217F 및 ESA PSS-01-302등에 제시되지 않은 경우에는 유사한 기술이 사용된 부품에 대한 정보를 참조하거나, 과거의 설계예(Heritage) 정보를 이용하여 신뢰성 예측을 수행하였다.
- 새로운 부품으로서 기존에 사용되지 않았고, 또한 MIL-HDBK-217F 및 ESA PSS-01-302등에 제시된 기준으로도 분류가 되지 않은 부품의 경우에는 미국 RAC의 EPRD-97 또는 NPRD-95와 같이 범용적인 운용환경에서 얻어진 부품 수준의 신뢰성 데이터를 참고하였다.

### 2.2 부품 스트레스 신뢰성 해석 (Part Stress Reliability Prediction)

부품 스트레스 신뢰성 해석은 MIL-HDBK-217F에 정의된 방법에 의해 수행되었다. 이에 의하면 전장품에 대한 고장률(Failure Rate)은 각 부품에 대한 고장률의 합으로 표시되며 다음과 같이 나타내어진다.

$$\lambda_{EQ} = \sum_{i=1}^n (\lambda_p)_i$$

$\lambda_{EQ}$ : 전장품의 고장률

$\lambda_p$  : i번째 부품에 대한 고장률

$n$  : 부품의 수

부품에 대한 고장률 모델은 부품에 따라 달라진다. 그 한 예로서 스위칭 다이오드(Switching Diode) 부품의 고장률 모델은 다음의 식으로 표시된다.

$$\lambda_p = \lambda_b \cdot \pi_T \cdot \pi_S \cdot \pi_C \cdot \pi_Q \cdot \pi_E$$

$\lambda_b$  : 부품의 기준 고장률

$$\pi_T = e^{-3091 \cdot \left( \frac{1}{T_j + 273} - \frac{1}{298} \right)}$$

: 온도 요인

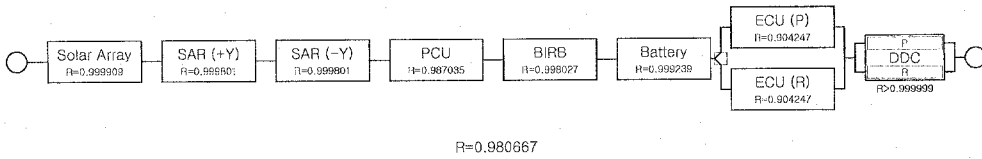


그림 1. 전력계에 대한 Reliability Block Diagram

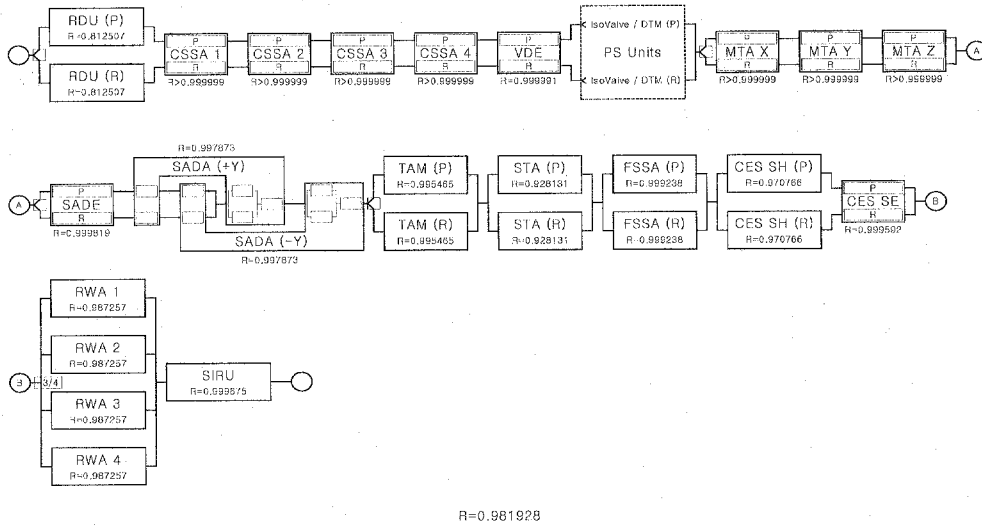


그림 2. 자세제어계에 대한 Reliability Block Diagram

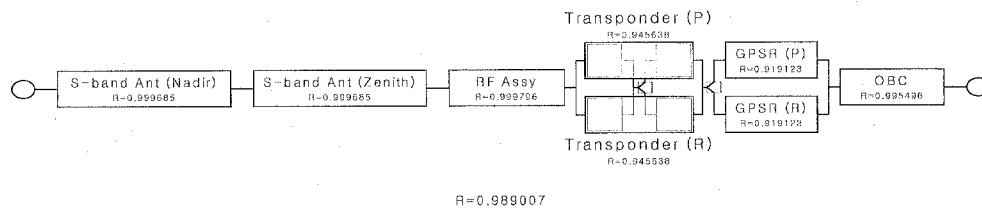


그림 3. 원격측정명령계에 대한 Reliability Block Diagram

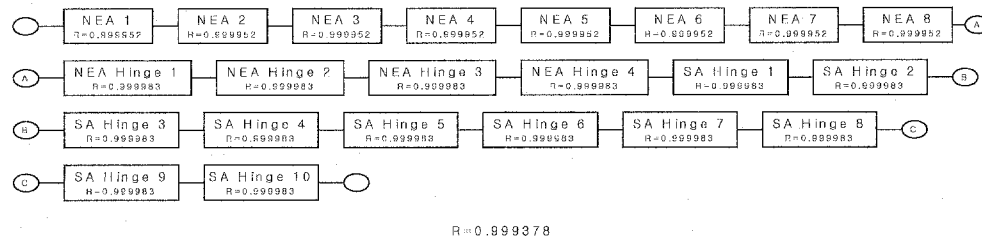


그림 4. 구조계에 대한 Reliability Block Diagram

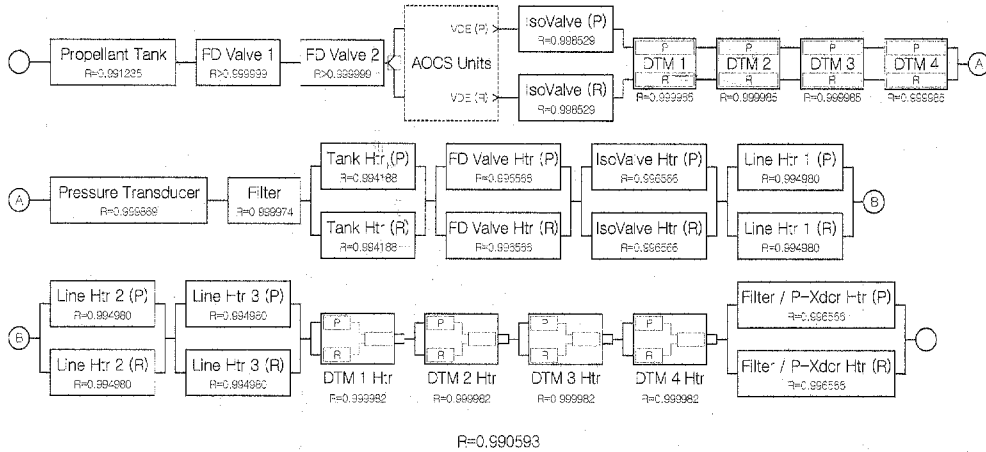


그림 5. 추진계에 대한 Reliability Block Diagram

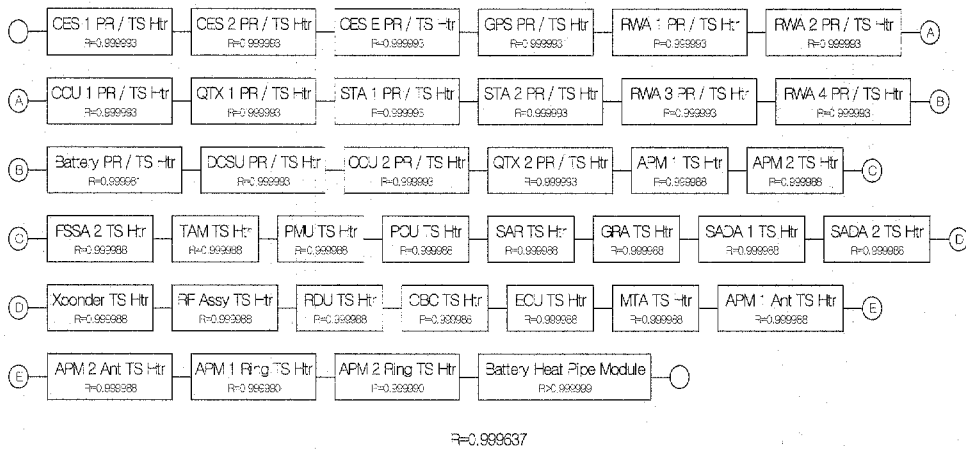


그림 6. 열제어계에 대한 Reliability Block Diagram

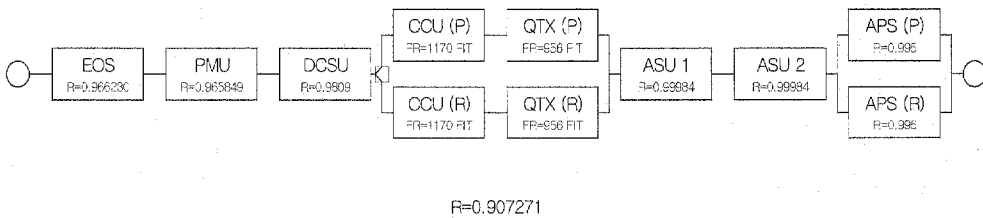


그림 7. MSC에 대한 Reliability Block Diagram

$$\pi_S = \left( \frac{V_{Applied}}{V_{Rated}} \right)^{2.43} : \text{전기적 스트레스 요인}$$

$\pi_C$  : 접촉 형태 요인

$\pi_Q$  : 품질 요인

$\pi_E$  : 환경 요인

이와 같이 부품의 고장률은 부품의 종류, 스트레스 수준, 품질 수준, 동작 환경 등이 고려되어 계산된다.

### 2.3 신뢰성 모델

각 서브시스템에 대한 신뢰성 모델이 개발되었다. 이러한 모델은 임무 달성을 위한 요구조건 및 기능상의 블록다이어그램(Block Diagram)을 바탕으로 하여 개발되며, 주로 신뢰성 블록다이어그램의 형태로 표시된다. 다목적 실용위성 2호의 신뢰성 해석을 위한 신뢰성 모델은 MIL-STD-756B Notice 1에 준하여 개발되었다. 각 서브시스템에 대한 신뢰성 모델은 각각 그림 1에서 그림 7에 나타내었다.

### 2.4 Ground Rule 및 가정

다목적 실용위성 2호의 신뢰성 해석을 위해 다음의 Ground Rule 및 가정이 적용되었다.

- 운용 환경은 MIL-HDBK-217F에 규정된 우주 비행 조건이다.
- 전기 전자 부품이나 동작을 수반하는 기계류 부품만을 대상으로 한다. 따라서 별도의 규정이 없는 한, 고정된 구조물이나 소프트웨어는 해석에서 제외된다.
- 위성의 모든 설계는 충분히 검증되어, 예상치 못한 과도한 스트레스나 Worst Case 조건은 발생하지 않는다.
- Common Cause Failure는 존재하지 않는다.
- 발사, 발사체 분리, 또는 태양전지판 전개 등에만 사용되는 장치는 1개월간의 임무 기간을 갖는다.

- 다목적실용위성 1호기의 운용 이력에 근거하여 Contingency State 대 Normal State의 임무기간 비는 3대75로 설정하며, Fine Science Mode, Coarse Science Mode, Earth Search Mode, Attitude Hold Mode 그리고 Delta V Mode의 구성비는 각각 90, 7, 1, 1, 그리고 1로 한다.
- 대기(Standby) 상태의 부품은 해당 부품의 고장률의 10%에 해당하는 고장률을 갖는다.

### 2.5 신뢰성 예측 결과

본체의 신뢰성 예측 결과는 임무기간 말기에 0.942471이며 이는 요구조건인 0.9를 만족한다. 그림 8은 임무기간 중의 본체 신뢰성의 감소 곡선이다. 탑재체인 MSC에 대한 신뢰성 예측은 제작사인 ELOP에 의해 수행되었다. 신뢰성 예측 결과는 임무기간 말기에 0.90729이며 이 또한 요구조건인 0.9를 만족한다.

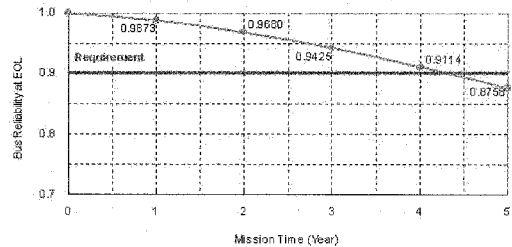


그림 8. 임무기간 중의 Bus Reliability

### 2.6 개발 기간 중의 신뢰성 변화 경향

개발 프로그램의 초기에는 신뢰성 할당치 및 과거의 설계에(Heritage) 정보 등을 바탕으로 신뢰성 예측이 수행되었다. 대부분의 전장품이 초기에 할당된 신뢰성 요구조건을 만족하였다. 이에 따라 그림 9에서 볼 수 있듯이 시스템 수준에서 평가된 신뢰성 예측치는 설계가 확정됨에 따라 일부 증가하였다. SDR 부근에서 발생한 신뢰성 감소는 자세제어계의 운용개념 재정립에 따른 신뢰성 모델의 변경에 의한 것이다.

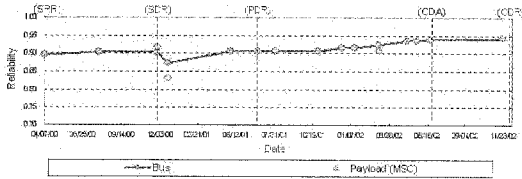


그림 9. 프로그램 기간 중의 신뢰성 경향

### 3. 고장 모드 및 중요도 해석 (Failure Mode Effect and Criticality Analysis, FMECA)

다목적 실용위성 2호기 본체에 대한 시스템 수준의 고장 모드 및 중요도 해석 (Failure Mode Effect and Criticality Analysis, 이하 FMECA)은 각 서브시스템 및 제작사로부터의 설계정보 및 전장품 수준의 FMEA를 바탕으로 하여 이루어 졌다. 탑재체인 MSC에 대한 FMECA는 ELOP의 FMEA 보고서를 바탕으로 수행하였다.

#### 3.1 Ground Rule 및 가정

다목적 실용위성 2호기에 대한 FMECA는 제품보증 요구조건에서 요구하고 있는 방법에 준하여 수행되었다. 여기에 더하여 다음과 같은 Ground rule 및 가정이 사용되었다.

- 각 고장 모드(Failure Mode)는 기능상의 접근법(Functional Approach)에 의해 확인된 Functional Block에 대해 정의 되었다.
- 고장에 대한 전과 자체가 고장 모드가 아닌 경우에는 각각의 고장은 적절히 고립(Isolation)되어 있고 또 제한된 상태에서 작용한다.
- 단일한 고장에 대한 영향에 의해 심각도(Severity)를 부여한다.
- 지역 효과(Local Effect)는 고장 모드가 발생한 전장품 수준에서의 임무 또는 기능상의 영향을 고려하여 기술한다.
- 최종 효과(End Effect)는 위성 전체에 대한 임무 및 기능의 영향을 고려하여 기술한다.

#### 3.2 운용 단계(Operational Phase)의 정의

다목적 실용위성 2호기에 대한 FMECA를 위하여, 임무 운용 단계(Operational Phase)는 표 1과 같이 정의되었다. 고장 모드에 대한 영향은 각 단계에 대해 확인되었다.

#### 3.3 심각도(Severity)에 대한 정의

심각도(Severity)는 고장 모드에 대한 영향을 정량적으로 평가할 수 있도록 해준다. 이는 각 고장 모드에 대한 영향 중 가장 심각한 영향을 기준으로 평가되었다. 표 2는 이러한 심각도에 대한 정의이다.

#### 3.4 중요도 해석(Criticality Analysis)

FMEA를 통하여 확인된 모든 고장 모드에 대해 중요도 해석(Criticality Analysis)이 수행되었다. 중요도(Criticality)란 각 고장 모드(Failure Mode)에 대한 심각도(Severity) 및 그 발생 확률을 고려하여 평가되는 일종의 임무 실패 확률로서 심각도(Severity) 및 고장 모드의 발생확률이 클수록 중요도 또한 커진다.

MIL-STD-1629A에 의하면 각 고장 모드에 대한 중요도를 계산하기 위하여 다음의 관계식이 사용된다.

$$C_r = \sum C_m$$

$$C_m = \alpha \cdot \beta \cdot \lambda_p \cdot t$$

$C_m$  : 고장 모드에 대한 중요도 값

$C_r$  : 전장품에 대한 중요도 값

$\alpha$  : 해당 고장 모드와 관련된 부품의 전체고장률에 대한 구성비

$\beta$  : 해당 고장 모드에 의해 임무 실패가 일어날 수 있는 기여 확률. 이는 표 3에 제시되었다.

$\lambda_p$  : 부품에 대한 고장률

$t$  : 임무 기간

Criticality Matrix는 각 고장 모드(Failure Mode)에 대한 발생 확률을 고려한 중요도(Criticality)와 심각도(Severity)를 비교 확인할 수 있도록 해준다. Criticality Matrix의 수직 축

은 중요도의 수준을 나타내며 수평축은 심각도를 나타낸다. 중요도 수준은 MIL-STD-1629A에 정의된 바와 같이 시스템의 고장 확률에 의해 표 4와 같이 구분될 수 있다.

표 1. Operational Phase 구분

Operation Phase	Definition
The Pre-launch Phase	Begins at the launch site and includes launch site processing activities.
The Launch and Ascent Phase	Begins during the final launch countdown and encompasses lift-off and period until separation.
The Deployment Phase	Occurs immediately following separation from the launch vehicle and encompasses the activities of solar array deployment, attitude stabilization, and sun acquisition.
The On-Orbit Checkout Phase	Begins after completion of sun acquisition and encompasses and the activities of earth acquisition and satellite checkout. The phase ends with completion of checkout and hand over of the satellite for mission operations.
The Mission Operations Phase	Begins with hand over of the satellite from completion of checkout. This phase is the normal operations phase for the satellite.

표 2. Severity 구분

Severity	Definition
Catastrophic	1 Failure modes that could result in serious injury or loss life (flight or ground personnel) or loss of launch vehicle.
	1R Failure modes of identical or equivalent redundant hardware item that, all of which if failed, could result in Severity 1 effects.
	1S Failure in a safety or hazard monitoring system that could cause the system to fail to detect a hazardous condition or fail to operate during such condition and leads to Severity 1 consequences.
Critical	2 Failure modes that could result in loss of one or more mission objectives.
	2R Failure modes of identical or equivalent redundant hardware item that, all of which if failed, could result in Severity 2 effects.
Significant	3 Failure modes that could cause degradation to mission objectives.
Minor	4 Failure modes that could result in insignificant or no loss to mission objectives.

표 3. Failure Effect Probability

End Effect	Severity		Failure Effect Probability
Actual Loss	1	Catastrophic	1.0
	2	Critical	1.0
Probable Loss	1R, 1S	Loss of Catastrophic Redundancy	0.7
	2R	Loss of Critical Redundancy	0.4
Possible Loss	3	Significant	0.1
No Effect	4	Minor	0.0

표 4. Criticality Classification Categories

Criticality Level		Criticality Number
Level A	Frequent	$2.899 \times 10^{-2} \sim 1.449 \times 10^{-1}$
Level B	Reasonably Probable	$1.449 \times 10^{-2} \sim 2.899 \times 10^{-2}$
Level C	Occasional	$1.449 \times 10^{-3} \sim 1.449 \times 10^{-2}$
Level D	Remote	$1.449 \times 10^{-4} \sim 1.449 \times 10^{-3}$
Level E	Extremely Unlikely	$0 \sim 1.449 \times 10^{-4}$

### 3.5 FMECA 결과

다목적 실용위성 2호기의 시스템 설계의 기본 개념은 1호기의 설계에서 많은 부분을 인용하였다. 이러한 이유로 대부분의 Single Point Failure는 다목적 실용위성 1호기의 설계로부터 기인한다. 다음은 Single Point Failure의 요약이다.

- 전력계통 및 Processor의 Relay Arm의 Open 또는 Ground로의 Short.
- RF Assy의 스위치 고장으로 인한 Nadir 방향의 S-Band Antenna로의 RF 경로의 단절.
- SADA Bearing의 기계적인 Failure.
- 추진계 Equipment의 누설 또는 파손.
- Cold Welding 등으로 인한 전개장치의 일부 기계류 부품의 Failure.

위에서 나열된 대부분의 Single Point Failure 수동적인 요인에 발생될 수 있는 고장 모드에 의해 발생하며, 그 발생확률도 매우 낮을 것으로 예상된다. 이 들에 대해서는 Critical Item Control Plan에 정의된 바에 따라 제작 및 시험 운용 기간 중의 위험 관리를 수행하며, 이를 통하여 관련 고장의 발생 요인을 최대한 억제하고 있다.

다목적실용위성 2호의 시스템의 대부분의 기능 및 하드웨어는 충분한 Redundancy를 갖추고 있으며, 정상적인 운용 모드 이외에 다양한 시나리오를 가정한 운용 모드가 존재한다. 따라서 실제 운용 중에 발생하는 부품의 고장에 대한 영향은 대부분 Redundancy를 상실하게 되는데서 그치게 된다.

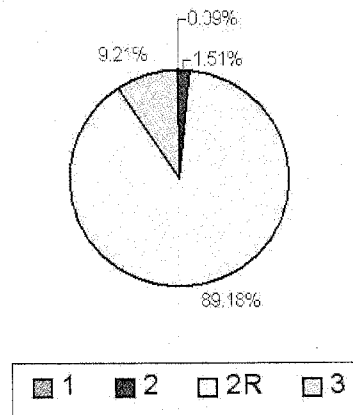


그림 10. Severity 분포



표 5. End Effect 목록

Severity Class	End Effect		Description	Severity	Contribution
Mission Loss	Loss of Environmental Compatibility	Major	• Catastrophic Structure Failure	1	0.09%
	Degraded SC Bus Power	Major	• Major Power Reduction • Cannot Deploy SA	2	0.72%
	Loss of Communication & Data Processing	Major	• Processor Function Failure • S-Band Communication Failure	2	0.18%
Major Mission Degradation	Degraded SC Bus Power	Major	• Degraded Power Generation • Power Distribution Failure	2	0.31%
	Degraded Mission Orbit Maintenance	Major	• Loss of Propellant(Leak, Saturation)	2	0.30%
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	7.15%
	Loss of Hardware Interface	Temporary	• Power Distribution Failure • Hardware Interface Failure • TLM/CMD Decoding/Encoding Failure	2R	6.34%
	Degraded of Hardware Interface	Temporary	• Increased Noise or Increased Stress	2R	0.17%
	Loss of Communication & Data Processing	Temporary	• Processor Function Failure • Loss of Downlink Function • TLM/CMD Decoding/Encoding Failure	2R	7.12%
	Degraded Communication & Data Processing	Temporary	• Loss of GPS Function	2R	3.79%
	Loss of Cartography	Temporary	• Loss of Sun Pointing Reference • Loss of 3-Axis Reference • Loss of SC Attitude • Loss of Image (PAN, MS)	2R	41.87%
	Loss of Mission Orbit Maintenance	Temporary	• Loss of Thruster Control	2R	0.61%
	Reduced Functional or Safety Margin	Marginal	• Reduced Safety Inhibits • Loss of Contingency Monitoring • Reduced Functional Margin	2R	5.59%
Reliability Degradation (due to loss of the margin)	Degraded Cartography	Marginal	• Degraded Attitude Control • Degraded Image	2R	13.08%
	Degraded Environmental Compatibility	Marginal	• Degraded Temp Control	2R	3.47%
Minor Mission Degradation	Degraded Environmental Compatibility	Significant	• Reduced Contingency Propellant	3	0.02%
	Degraded SC Bus Power	Significant	• Power Status TLM Loss • Marginal Power Reduction	3	2.42%
	Degraded Communication & Data Processing	Significant	• Reduced Link Margin and FOV	3	0.02%
	Degraded Cartography	Significant	• Degraded Image	3	6.45%
	Degraded Mission Orbit Maintenance	Significant	• DTM or Isoalve Malfunction	3	0.30%

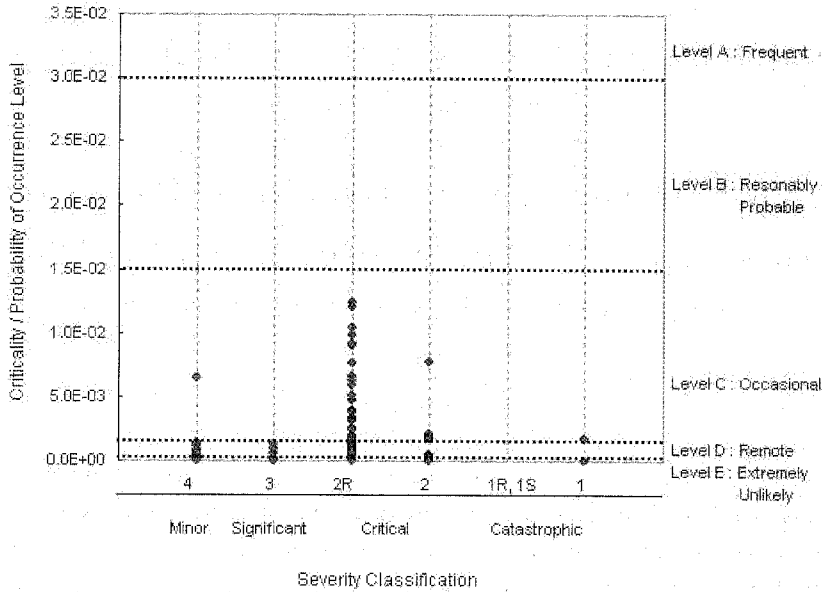


그림 11. Criticality Matrix

표 5는 FMEA를 통하여 확인된 End Effect 목록이다. 이와 함께 이들 고장 모드의 분포 비는 그림 10에 나타내었는데, 대부분의 고장 모드가 심각도(Severity) '2R' 또는 '3'의 고장 모드이다.

그림11은 다목적 실용위성 2호기의 Criticality Matrix를 나타낸다. 여기에서 볼 수 있듯이 대부분의 고장 모드는 'Remote' 또는 'Extremely Unlikely'에 분포되어있다. 이러한 해석 결과들로 비추어볼 때 다목적 실용위성 2호의 설계는 프로그램 요구조건에서 규정한 Single Fault Tolerant 요구조건을 실제적으로 만족한다고 결론지을 수 있다.

### 참 고 문 헌

1. DOD-HDBK-343, Design, Construction, and Testing Requirements for One of a Kind Space Equipment.

2. MIL-HDBK-217F, Reliability Prediction of Electronic Equipment.
3. MIL-STD-1543B, Reliability Program Requirements for Space and Launch Vehicles.
4. MIL-STD-756B, Reliability Modelling and Prediction.
5. MIL-STD-781D, Reliability Testing for Engineering Development, Qualification, and Production.
6. MIL-STD-1629A, Procedures for Performing a Failure Mode Effects and Criticality Analysis.
7. NPRD-95, Non-electronic Parts Reliability and Life-testing Models.
8. Lee J. Bain and Max Engelhardt, Statistical Analysis of Reliability and Life-Testing Models, Marcel Dekker Inc.
9. B. S. Dhillon and Chanan Singh, Engineering Reliability, John Wiley & Sons.