저궤도 상용위성의 시스템 수준 FMECA

이창호*, 조영준**

System FMECA for LEO Commercial Satellite

Chang-Ho Lee*, Young-Jun Cho**

Abstract

The purpose of FMECA is to identify parts and design whose damage can effect the mission performance and to improve the spacecraft design using these data. In consequence of this analysis, each failure mode which can be happened during operation and manufacturing period is identified, and their effects on mission performance are reviewed. In this technical report, the FMECA procedures and results for the satellite which is now under development are showed.

초 록

FMECA의 목적은 위성체의 설계 시에 임무 수행에 치명적인 영향을 줄 수 있는 부품이나 구성을 밝혀내어 이를 설계에 이용하기 위한 것이다. 이러한 분석을 통하여 위성체의 운용 또는 생산 중에 예상되는 모든 고장 형태(Failure Mode)를 확인하고, 해당 고장 형태의 임무에 대한 영향을 검토하여 이러한 고장 형태가 허용될 수 있는 것인지를 결정하고 이를 보완하기위한 설계 변경 또는 관리가 이루어지게 된다. 본 기술 논문에는 현재 개발 중인 위성에 대하여 수행된 FMECA의 절차와 결과를 수록하였다.

키워드 : 신뢰성 예측(Reliability Prediction), 고장모드 영향 분석(FMEA), 치명도 분석(Criticality Analysis), 전기전자 부품 (EEE Part), 제품보증 요구조건(Product Assurance Requirement)

1. 개요

FMEA(Failure Mode & Effect Analysis)는 고장의 형태와 그 영향을 밝혀내어 설계상의 취약점을 보완하는데 그 목적이 있다.

FMEA 수행 방식은 크게 하드웨어 접근방식과 기능 접근방식으로 나뉠 수 있다. 하드웨어 접근방식은 세부 부분품에 대한 설계가 수행되어 하드웨어의 각 부분이 규정된 경우에 사용될 수 있다. 이 경우 각 부품의 Failure Mode를 식별한 후 이러한 고장이 하드웨어에 미치는 영향을 분석하는 상향 접근방식의 형태를 띤다. 기능 접근방식은 하드웨어의 설계가 명확히 규정되지 않았거나, 시스템의 복잡성 등으로 인해 하드웨어 접근 방식이 효율적이지 않은 경우 사용된다. 이 경우 상위 시스템에 요구되는 기능을 확인한 후 해당 기능을 위해서 필요한 하위 시스템의 기능을 차례로 정의해 나가는 하향 접근방식의 형태

* 위성본체그룹/chlee@kari.re.kr
** 위성본체그룹/yjcho@kari.re.kr

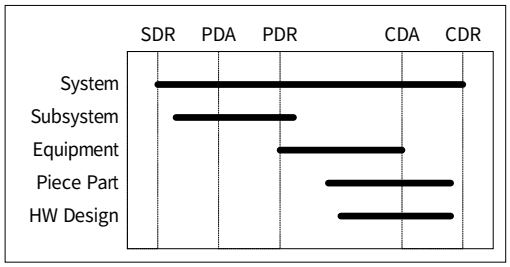

그림 1. Design Phase에 따른 FMEA

를 띤다. 일반적으로 시스템 및 서브시스템 수준의 FMEA는 기능상의 접근방식으로 수행되며, 전장품 수준의 FMEA는 하드웨어 접근방식으로 수행된다.

FMECA(Failure Mode Effect and Criticality Analysis) 란 FMEA에 Criticality Analysis가 더해진 형태로서, 잠재적인 고장 상태가 상위 시스템에 어떠한 영향을 미치는 지를 연역적으로 추론하여 이러한 고장에 대한 Severity를 확인하고 이의 발생 가능성을 예측하여 각각의 고장 상태에 대한 중요도를 평가하는 일련의 과정이다.

이러한 FMECA는 시스템이 잠재적인 고장에 대해 어느 정도의 Tolerance를 갖는지를 확인하고, 이의 개선을 위한 중요도 우선순위를 가늠하기 위하여 사용된다.

일반적으로 상용위성의 경우 시스템 설계 요구조건에 의하여 단일한 고장에 대해서는 Tolerance를 갖도록 규정되어 있으며, 이를 위하여 시스템 설계의 초기단계에서부터 FMEA를 통하여 위성의 Fault Tolerance를 검증하였다.

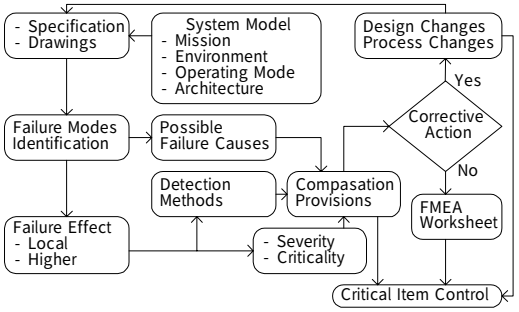

그림 2. FMEA 수행 절차

일반적으로 FMEA는 5가지 수준으로 나뉘어 수행된다. '시스템 FMEA'는 각 서브시스템들 간의 인터페이스를 분석하여 이들의 고장이 전체 시스템에 미치는 영향을 확인한다. '서브시스템 FMEA'는 시스템 FMEA의 수준을 서브시스템 내의 각 전장품 수준으로 확장한 것이다. 마찬가지로 '전장품 FMEA'는 서브시스템 FMEA의 수준을 전장품 내의 각 모듈 및 Board 수준으로 확장한 것이며, 내부 Redundancy가 존재하거나 전원 공급과 관련된 전장품 등에 수행된다. '부품 FMEA'는 상향 접근방식으로 수행되며, 각 부품의 고장 형태를 분석하여 이에 대한 영향을 확인한다. Single Point Failure Mode가 존재하거나 Deployment Phase에서 사용되는 장치 등과 같이 그 임무 중요도가 큰 설계의 검증에는 'Product Design FMEA'가 추가로 적용된다. 이는 하드웨어 형상, 배선, 회로의 Layout, 및 커넥터 핀 배치 등을 고려하여 고장 모드에 의한 영향을 분석한다.

'그림 1'은 Design Phase에 따른 FMEA의 수행 수준을 나타내고 있다. 전장품 수준의 세부 설계가 완료되기 이전에는 시스템 및 서브시스템 요구조건 수준의 해석을 통하여 위성의 설계에 대한 Fault Tolerance를 검증하고, 설계가 구체화되어 각 전장품에 대한 Failure Mode가 확인된 경우 실현 가능한 Failure Mode를 재구성하여 필요한 경우 이에 대한 운용 및 제작상의 대처 방안을 강구하였다. '그림 2'는 이러한 FMEA 수행 절차를 개략적으로 나타내고 있다.

2. Failure Mode의 확인

세부 설계가 수행되지 않은 개발 초기 단계에서는 시스템 및 서브시스템 수준의 설계 요구조건에 대한 Noncompliance 상태를 시스템 Failure Mode로 설정하였다. 일반적으로 위성의 설계 요구조건은 설계가 구체화됨에 따라 Top-Down 방식으로 Flow Down되므로 FMEA를 위한 Failure Mode도 세부 요구조건의 설정

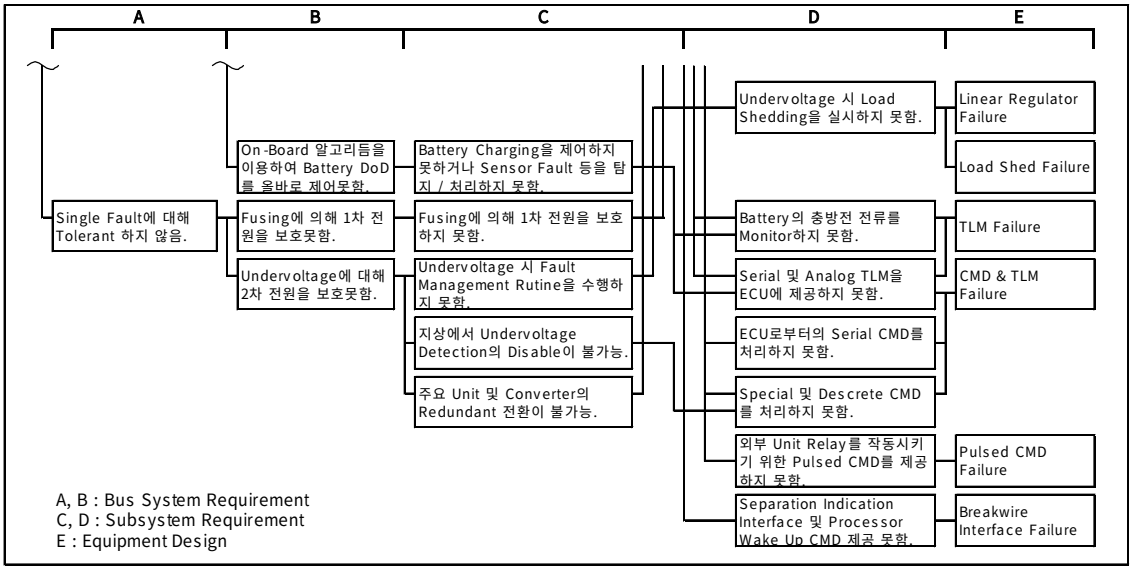

그림 3. 저궤도 상용위성 전력계 관련 Failure Mode의 Flow Down (부분예)

과 함께 구체화된다. '그림 3'은 이러한 예로서 저궤도 상용위성의 전력계에 일반적으로 사용되는 전력 분배 장치에 대한 시스템 Failure Mode의 Flow Down 일부를 개략적으로 나타내고 있다. 여기에서 Column A와 B는 시스템 설계 단계의 Failure Mode이며, C와 D는 서브시스템 설계 단계의 Failure Mode이다. Column E는 이러한 요구 조건들을 반영하는 전장품 설계이다.

표 1. Film Resistor의 Failure Mode [4]

Failure Mode	Failure Mode Ratio(α)
Open	37.5%
Short	5.0%
Drift	30.0%
Contamination	7.4%
Fracture	5.2%

전장품에 대한 세부 설계가 진행되는 단계에서는 이를 구성하는 각 부품 및 Hardware에 대한 물리적인 설계 요인 등을 고려하여 Failure Mode를 설정한다. 그 일례로서 '표 1'은 전장품에 주로 사용되는 Film Type Resistor에 대한 Failure Mode이다.

3. Mission Phase의 구분

표 2. Mission Phase 당의 Duty Ratio [2]

Mission Phase		Duration/Ratio
Pre-Launch		3 Month
Launch & Ascent		52 Min
Deployment		40 Min
On Orbit Checkout, Mission Operation	Normal	97 %
	Contingency	3%

위성의 Hardware 구성, 운용 및 환경 요건은 Mission Phase에 따라 달라지므로, Failure Mode에 대한 영향도 이에 따라 달리 평가되어야한다. 일반적으로 전개부를 갖는 저궤도 상용위성의 경우에는 'Pre-launch', 'Launch & Ascent', 'Deployment', 'On Orbit Checkout', 'Mission Operation'의 5 단계의 Mission Phase로 구분하여 Failure Mode에 대한 영향을 분석한다.

표 3. Failure Mode에 대한 Severity의 정의 [1]

Severity	시스템 수준의 Severity 정의	β
1	발사체 또는 인명의 손상을 야기할 수 있는 Failure Mode.	1.00
1 R	Severity 1 Effect를 야기할 수 있는 HW / Function에 대한 Redundant HW / Function의 Failure Mode.	0.70
1 S	Severity 1 Effect를 야기할 수 있는 상황을 Monitor 하는 HW / Function의 Failure Mode.	0.70
2	System 요구조건에 기술된 Mission Objective를 달성하지 못하게 할 수 있는 Failure Mode.	1.00
2 R	Severity 2 Effect를 야기할 수 있는 HW / Function에 대한 Redundant HW / Function의 Failure Mode.	0.40
3	System 요구조건에 기술된 Mission Performance를 저하시킬 수 있는 Failure Mode.	0.10
4	Mission Performance등에 영향을 주지 않는 Failure Mode	0.05

Severity	Equipment 수준의 Severity 정의	β
1	Unit 내부의 Failure로 인해 이와 Interfacing하고 있는 외부 Unit을 손상시킬 수 있는 Failure Mode.	1.00
1 R	Severity 1 Effect를 야기할 수 있는 Part / Function에 대한 Redundant Part / Function의 Failure Mode.	0.70
2	임무의 수행에 필요한 Unit의 기능을 상실 시킬 수 있는 Failure Mode.	1.00
2 R	Severity 2 Effect를 야기할 수 있는 Part / Function에 대한 Redundant Part / Function의 Failure Mode.	0.40
3	임무의 수행에 필요한 Unit의 Performance를 저하시킬 수 있는 Failure Mode.	0.10
4	임무의 수행에 필요한 Unit의 Performance등에 영향을 주지 않는 Failure Mode	0.05

Criticality 계산 시에 있어서 해당 Failure Mode를 야기하는 부품의 사용 시간을 평가하는 것이 필요하므로 위성에 예정된 임무 시나리오 및 유사 위성의 운용 이력 등을 참고하여 각각의 Mission Phase 당의 지속 기간을 예측한다. '표 2'는 이러한 사항을 참조하여 구성된 Mission Phase 구분의 예이다.

4. Failure Effect에 대한 평가

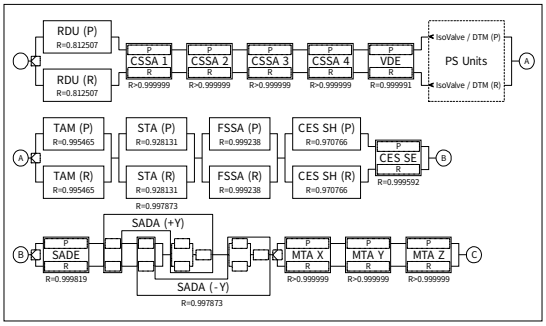

그림 4. 자세제어계의 시스템 RBD (부분예) [2]

확인된 Failure Mode에 대한 Effect는 해당 Failure에 의해 나타날 수 있는 1차 적인 효과인 'Local Effect'와, 이로 인해 궁극적으로 발생할 수 있는 효과인 'End Effect'로 구분되어 평가된다. FMEA가 여러 수준으로 나뉘어 수행 될 경우, 하위 시스템의 End Effect는 상위 시스템의 Failure Mode로서 고려 될 수 있다. FMEA의 각 Failure Mode는 서로 연관성이 없음을 전재로 하므로 Failure Mode에 대한 Effect는 단일한 Failure 발생을 가정하여 평가된다.

각각의 Failure Mode는 End Effect의 Severity에 따라 그 경중이 평가된다. Severity에 대한 기준은 프로그램의 성격에 따라서 여러 가지가 있을 수 있으나 저궤도 무인 상용 위성의 경우에는 일반적으로 '표 3'과 같은 기준이 FMEA 기준으로서 사용된다. 전장품의 경우에는 내부의 고장이 외부로 확산되지 않는다면 비록 그 기능이 상실되어도 시스템 Redundancy를 이용하여 임무 수행이 가능 할 수 있으므로 Severity의 기준이 시스템의 그것과는 차이가 있다.

Failure Mode의 Severity는 그 End Effect가 대상이 되는 요구조건 또는 기능이 임무의 성공

표 4. 저궤도 상용위성의 FMEA를 통한 End Effect 목록의 예

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 Contigency 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	- Deraded Image	3	6.46%
	Degraded Mission Orbit Maintenance	Significant	- DTM or Isoalve Malfunction	3	0.30%

에 어떠한 영향을 미치는지에 따라 결정된다. 일반적으로 설계 요구조건을 설정하기 위해서는 여러 형태의 임무 해석이 이루어지므로 이를 이용하여 관련 기능의 중요도를 판단하며 또한 시스템의 Reliability Model 을 통하여 관련 기능의 Redundancy 여부를 확인하게 된다. '표 4'는 현재개발중인 위성에 대한 FMEA를 통하여 확인된 End Effect 목록이다. '그림 4'는 자세제어계에 대한 시스템 Reliability Block Diagram의 예이다.

5. Criticality Analysis

전장품에 대한 설계가 진행되어 시스템 Failure Mode를 각 부품에 대한 Failure와 연관시킬 수 있는 경우에는 Failure Mode의 발생 확률을 이용하여 Criticality를 계산할 수 있다. 일

표 5 전력계 UV Function에 대한 시스템 수준의 FMECA Worksheet (부분예) [2, 3]

System Level FMEA with Functional Requirement: PCU UV Function

Function	Failure Modes and Causes	Mission Phase	Failure Effects		Failure Detection Methods	Compensating Provision	Severity
			Local Effects	End Effects			
Detect UV & perfrom Load shedding	No output from UV detector in anormaly state	D, E	Cannot detect secondary power anomaly. If one of the secondary load short, DC-DC converter will shut off the power to protect converter.	If one of the secondary load short, Secondary power bus will be lost.	None	None	2R
	False output from UV detector	D, E	Cannot detect secondary power anomaly. SC will go to safe hold mode.	If continuous false signal is out, SC cannot operated in primary side. If redundant side is working properly, operate SC in redundant side,	PCU converter status TLM	Switch to redundant side	2R
	Load shedding process failure	D, E	Cannot perform safing function in anomaly state.	If UV condition is occurred, SC cannot awake in redundant side. Loss of critical redundancy.	None	None	2R

FMEA with Hardware Failure Mode : Linear Regulator (UV function Related)

Module	Failure Modes and Causes	Mission Phase	Failure Effects		Failure Detection Related TLMs	Compensating Provision	Severity	Criticality
			System Effects	Mission Effects				
Linear regulator	Abnormal +5VR1 output	D, E	No loadshed power	Loss of safety inhibits	Bilevel TLM	Use redundant linear regulator	2R	1.52E-04
	Over voltage affect U9 & U1	D, E	U9 & U1 function degraded	Loss of safety inhibits	None	Use redundant linear regulator	2R	6.90E-06
	Linear regulator inoperative	D, E	Loss of linear regulator function	No permanent effect on mission due to redundant linear regulator.	Bilevel TLM	Use redundant linear regulator	2R	2.99E-06
	Bilevel TLM failure	D, E	Loss of bilevel TLM function	No critical effect on mission	Bilevel TLM	Use redundant linear regulator	3	3.82E-05

반적으로 Criticality 값(Cr)은 다음과 같은 관계식을 이용하여 계산한다.

$$Cr = \beta \cdot t \cdot \sum(\alpha \cdot \lambda)$$

β : Mission Loss Probability
α : Failure Mode Ratio
λ : Hadware Failure Rate
t : Duration of Mission

현재 개발 중인 위성의 경우 Failure Mode의 Criticality에 대한 절대적인 판단 기준은 존재하지 않으나, 상대적인 비교를 통하여 설계 개선의 우선순위 등을 결정하기 위한 Trade Off의 참고 자료로서 이용하고 있다.

FMEA 결과와 Criticality Analysis를 결과를 바탕으로 하여 FMECA를 수행할 수 있다.

이와 같은 FMECA의 결과는 MIL-STD -1629의 형식에 따라 정리되었다. '표 5'는 그 예로서 PCU의 Under Voltage Detection 기능과 관련된 FMECA의 Worksheet의 일부이다

6. Observability

운용 중 Failure가 발생하였을 경우 위성은 계획된 Fault Management Logic에 따라 Configuration을 전환하게 된다. 이는 일반적으로 자동적으로 이루어지나 때로는 지상국의 판단에 의해 이루어 질 수도 있으며 필요한 경우 위성의 상태를 고려하여 운용 형태를 바꾸어야 하는 경우도 있을 수 있다. 이를 위하여 FMEA를 통하여 확인된 각 Failure의 발생 여부를 지상에서 식별할 수 있도록 각 Failure Mode에 대한 Detection 방법 및 관련 Telemetry를 함께 확인하였다.

7. Critical Failure Mode에 대한 방안

Failure Mode에 대한 영향이 하나 이상의 Mission을 상실시키거나 성능을 크게 저하시켜 요구되는 Mission 목표를 달성시킬 수 없는 경우, 즉 Severity가 2보다 심각한 경우에는 이를 완화하기 위해 설계 변경을 고려하게 된다. 이러

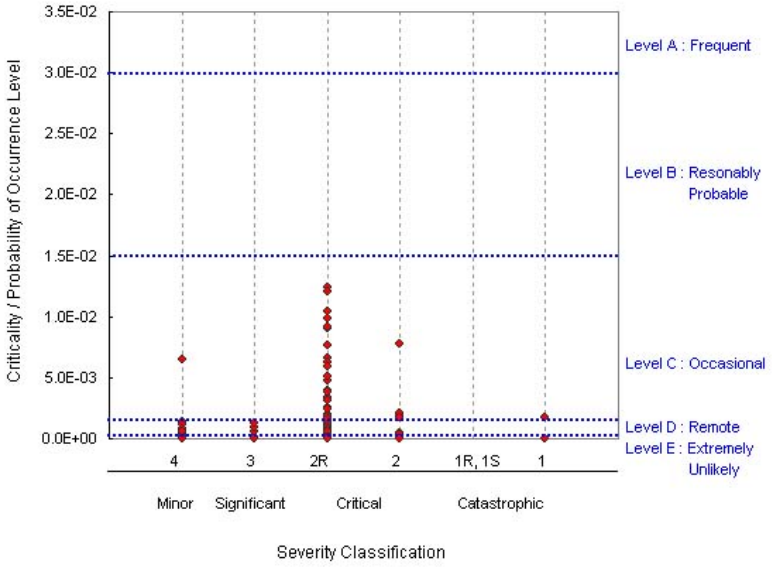

그림 5. Criticality Matrix

한 설계 변경으로는 Redundancy를 추가하여 Severity를 2R로 완화하거나 주변 설계를 개선하여 Failure의 발생 가능성을 낮추는 방법 등이 있다.

일반적으로 상용위성의 경우에는 대부분의 중요 Unit에 대해서는 Redundant 설계가 이루어진다. 그러나 특정 설계의 경우 현실성을 고려하여 Redundancy를 적용하지 않는 부분이 있는데, 예를 들어 현재 개발 중인 위성의 경우에는, 전력계 1-2차 전원 계통의 일부, S-Band Antenna 및 RF 경로, 그리고 추진계의 Tank 등이 이의 예이다. 이들은 잠재적인 Single Point Failure를 야기할 수는 있으나, 대부분의 경우 Failure 가능성이 극히 낮고, 또한 필요한 경우 주변 설계를 개선하여 설계상의 위험요소를 최소화하였다. 설계의 개선이 실질적으로 불가능한 경우에는 이를 Critical Item으로 분류하여 해당 Failure Mode의 발생 가능성을 최소화하였다. Critical Item에 대해 이루어진 별도의 관리는 일반적으로 부품의 추가적인 Screening 및 Evaluation, 제작 공정의 수정, 관련 설계에 대한 추가적인 Verification 등이 있다.

8. Criticality Matrix

'그림 5'는 현재 개발 중인 위성의 Criticality Matrix를 나타낸다. 여기에서 볼 수 있듯이 대부분의 고장 모드는 'Remote' 또는 'Extremely Unlikely'에 분포되어있다. 이러한 해석 결과들로 비추어볼 때 당 위성의 설계는 프로그램 요구조건에서 규정한 Single Fault Tolerant 요구조건을 실제적으로 만족한다고 결론지을 수 있다

9. 그 밖의 Fault Tolerance 검증 해석

현재 개발 중인 위성의 설계는 미국의 East West 발사장 안전 요구조건(EWR 127-1)에 준한다. 따라서 발사체 또는 인명의 손상을 야기할 수 있는 Failure Mode에 대해서는 추가적으로 Double Tolerance를 요구하고 있다. 이 경우에는 Independent한 Failure에 대한 영향만을 확인할 수 있는 FMECA 대신 Fault Tree Analysis 등의 방법을 부분적으로 이용하여 기 개발된 위성과 비교해 변경된 설계의 안전성을 확인하였다.

10. 결 론

본 기술 논문에서는 저궤도 상용 위성의 개발 시 수행된 FMECA 과정을 개략적으로 소개하였으며, 그 예로서 현재 개발 중인 위성의 수행결과를 부분적으로 예를 들었다.

전술한 바와 같이 이러한 FMECA를 통하여 위성 시스템 전반에 대한 Fault Tolerance 및 신뢰성을 검증하고 필요한 경우 일부 설계를 개선하는데 중요한 Guideline을 제공할 수 있다.

현재 개발 중인 위성의 경우에도 이러한 원칙에 준하여 FMECA가 수행되었으며, 이를 통하여 Fault에 대한 Tolerance 및 신뢰성을 검증하였다. 단, 금번의 경우에는 Software Fault 및 Ground Support Equipment 등에 대한 고려가 이루어지지 않은 점은 추후 개선되어야할 점으로 생각된다.

참 고 문 헌

1. KOMPSAT-2 PA Program Plan, KARI, 2001.
2. KOMPSAT-2 Reliability & FMECA Report, KARI, 2002.
3. KOMPSAT-2 PCU FMEA, KAI, 2002.
4. Failure Mode / Mechanism Distributions, RAC, 1997.