

KSLV-I 상단부에 대한 신뢰성 분석과 신뢰도 모델링

신명호*, 조상연**

Reliability Analysis and Reliability Modeling for KSLV-I Upper Stage

Myoung-Ho Shin*, Sang-Yeon Cho**

Abstract

This paper shows the results of failure mode analysis and the system-level reliability model for the flight test of KSLV-I upper stage. First, the critical 14 functions of KSLV-I upper stage are identified and the mission profile of the flight test is analyzed. Then, based on the functional analysis and the mission profile analysis, we construct a hierarchical structure of failure modes and a system-level reliability model for the flight test of KSLV-I upper stage.

초 록

본 논문은 KSLV-I 상단부에 대한 고장모드 분석 결과와 시스템 수준의 비행시험 신뢰도 모델을 기술한다. 먼저, KSLV-I 상단부의 14개의 주요 기능과 비행시험 임무 프로파일을 분석하고, 기능 분석 결과와 임무 구간별 수행 기능 목록을 바탕으로 시스템 체계에 따른 상단부의 고장모드 계층 구조와 시스템 수준의 비행시험 신뢰도 모델을 구성한다.

키워드 : Failure Mode(고장모드), FMECA(Failure Modes, Effects, and Criticality Analysis ; 고장모드, 효과 및 치명도 분석), Reliability Modeling(신뢰도 모델링)

1. 서 론

시스템의 신뢰성을 보장하기 위한 활동은 크게 정성적인 활동과 정량적인 활동의 두 가지 유형으로 구분된다. MIL-STD-756B에는 신뢰성 프로그램의 세부 활동 사항이 기술되어 있는데, 앞서 언급한 두 유형에 따라 구분하자면, 크게 고장과 관련된 활동과 신뢰도와 관련된 활동으로 나눌 수 있

다. 활동의 특성 상 고장과 관련된 FMECA (Failure Mode, Effect and Criticality Analysis), FRACAS (Failure Reporting, Analysis, and Corrective Action System), FRB (Failure Review Board), 신뢰성 중요 품목 선정, ESS (Environmental Stress Screening) 등은 고장모드를 찾고 분석해서 대책을 수립한 후 설계/제작/운영에 반영하여 신뢰성의 향상을 가져오는 정성적인 작업이다. 반면 신뢰도와 관련된 신뢰도 모

접수일(2007년 12월 14일), 수정일(1차 : 2008년 6월 5일, 2차 : 2008년 6월 17일, 게재확정일 : 2008년 7월 1일)

* 체계종합팀/myshin@kari.re.kr

** 추진기관체계팀/chosangy@kari.re.kr

모델링, 할당, 예측, 성장 곡선, 입증 등의 활동은 주어진 시스템과 컴포넌트의 신뢰성 수준을 평가하는 정량적인 활동에 해당한다. 정성적인 활동이 설계나 제작 과정에 반영되어 제품의 신뢰성 향상을 가져오고 고장의 발생을 방지하는 것을 목표로 한다면, 정량적인 활동은 중요 시험이나 주요 개발 단계, 운영 등에 앞서 현재 제품의 신뢰성 수준을 정확하게 평가하는 것을 목표로 한다. 따라서 두 작업은 상호보완적이며 고장과 관련된 활동은 설계/제작 단계에 집중되고 신뢰도 관련 주요 데이터 분석과 계산은 설계가 거의 완료되는 시점에 주로 수행된다.

본 논문에서는 KSLV-I 상단부의 신뢰성 보증을 위해 수행된 정성적 신뢰성 분석의 결과를 정리하고 신뢰성 평가 활동의 기초 작업으로 수행된 시스템 수준의 신뢰도 모델링 결과를 기술한다.

2. KSLV-I 임무와 상단부의 주요 기능

신뢰성 분석과 신뢰도 모델링을 위해서는 시스템이 운용되는 임무에 대한 분석이 선행되어야 한다 [8,13]. 이 절에서는 KSLV-I 상단부에 대한 신뢰성 분석과 비행시험에 대한 시스템 수준의 신뢰도 모델링을 위해 KSLS의 핵심 임무를 명확하게 정의하고 그 임무로부터 KSLV-I 상단부의 주요 기능을 도출한다.

표 1. KSLS의 4가지 목표

번호	목 표	주요 서브시스템
1	목표한 시간 내에 KSLV-I 발사 준비와 발사를 성공적으로 수행	지상장비
2	위성 투입 단계까지 발사체의 기능을 정상적으로 유지	구조체, 열환경 제어시스템, 전력시스템, 통신시스템
3	발사체의 비행중단을 유발시키는 고장 없이 정확하게 위성출 케도에 투입	제어시스템, 분리장치, 비행중단시스템, 추적시스템
4	위성 케도를 투입하기에 충분한 추력	추진기관

KSLV-I 상단부에 대한 신뢰성 분석과 신뢰도

모델링은 KSLS가 완수해야 할 목표를 명확히 정의하는 것에서부터 시작한다. KSLS의 임무로부터 KSLS의 중요 목표가 설정되고, KSLS의 중요 목표는 다시 KSLV-I 1단, 2단, PLF, AC, LC, 이송 설비, DMAPS (Data Measurement, Acquisition and Processing Set) 등 각 세그먼트가 달성해야 할 세부목표와 기능으로 나누어지고, 각 세그먼트가 필요로 하는 세부 기능은 서브시스템으로 구현된다. KSLS의 4가지 목표를 기술하면 표 1과 같다. KSLS의 4가지 목표 중 발사체와 직접적으로 연관 있는 2, 3, 4의 목표로부터 KSLV-I 2단과 PLF의 세부기능이 정의된다. KSLV-I 2단과 PLF의 주요 세부기능은 14개의 서브시스템으로 구현된다. 각 서브시스템에 해당하는 주요 세부 기능은 표 2와 같다.

3. 고장모드 분석

FMECA는 설계 초기 단계에서부터 설계 단계에 따라 반복적으로 수행하면서 설계 변경을 통해 시스템 설계에 내재하는 파국적이거나 심각한 고장의 확률을 예측하여 제거하거나 최소화하기 위한 것이다. 따라서 FMECA는 예비설계단계에서 시스템 레벨부터 시작되어야 하며, 설계가 진행됨에 따라 낮은 레벨까지 상세화/구체화된다. 고장모드 분석은 FMECA의 한 활동으로 이러한 목적에 맞게 시스템 설계의 모든 고장을 식별해 내는 것을 목표로 한다. 일반적으로 대규모 시스템은 구조적으로 여러 개의 레벨로 된 구성 체계를 갖는다. 발사체의 경우에도 시스템, 세그먼트, 서브시스템, 유닛, 컴포넌트, 조합체, 서브조합체, 부품 등과 같은 순차적인 구성 체계를 갖고 있다. 이러한 계층적 시스템 구조에서 낮은 레벨에서의 고장은 높은 레벨의 고장을 야기시키는 원인이 된다. 따라서 고장모드 분석은 시스템을 구성하는 각 요소에 대한 고장모드를 식별해야 할 뿐 아니라 시스템의 기능을 구현하는 서브시스템과 유닛, 컴포넌트 레벨에 따라 체계화되는 고장모드 계층 구조를 발견해야 한다.

본 논문에서는 먼저 고장모드 분석의 이론과 그 결과의 구체적인 활용 방안에 대해 정리하고, KSLV-I 상단부 중 임무에 결정적인 영향을 미치는 14개 중요 기능을 수행하는 서브시스템에 대해 고장모드를 식별하여 고장모드 계층 구조를 구성한다. 각 서브시스템에 대한 고장모드 분석은 컴포넌트 레벨까지 수행되며 보편적으로 적용되는 FMECA 분석 항목 중 고장원인, 고장효과, 검증방법 등의 항목만을 고려하여 수행한다.

3.1 고장모드 분석의 원칙과 방법 [6-7]

FMECA는 원칙적으로 설계 초기 단계에 수행된다. 수행 시 필수적으로 포함해야 할 항목은 표 3과 같다. 일반적으로 FMECA는 설계 초기 단계에서부터 치명도 분석을 통해 설계의 약점과 치명도가 높은 고장모드를 확인하고 이를 보완하고 방지하기 위한 설계 변경, 부품 교체, 재료 변경, 시험평가 조정, 공정 개선, 운용/작업 절차 강화 등을 수행하게 된다. KSLV-I 상단부의 경우, 상세 설계가 완료된 이후 고장모드 분석에 착수하였으므로, 고장모드 분석의 범위를 고장모드 식별과 계층 구조 분석을 위한 “고장모드, 고장원인, 효과 및 영향, 검증/점검 방법” 항목으로 한정한다.

표 3. FMECA 기본 항목

번호	항목	설명
1	고장모드	고장 이름
2	고장원인	고장을 발생시키는 원인을 모두 기술
3	효과 및 영향	고장 시 발생할 수 있는 모든 가능한 결과들을 기술
4	검증/점검 방법	고장모드의 발생 여부와 고장이 발생하지 않음을 보장하는 확인/점검 방법(시험평가, 검사, 설계검토, 시뮬레이션과 분석 등)
5	방지대책	고장 방지, 고장으로 인한 부정적 효과 감소, 발생 확률 감소 등을 위한 조치 (설계 변경, 부품 교체, 시험평가 조정, 공정 개선, 절차 강화 등)
6	심각도	고장으로 인한 효과의 심각도
7	발생빈도	고장 발생 확률
8	치명도	심각도 × 발생빈도
9	비고	기타 관련 내용

발사체와 같은 대규모 복합 시스템은 많은 계층 구조를 갖는 다양한 서브시스템과 컴포넌트로 구성되어 있다. 따라서 FMECA 또한 다양한 수준에서 수행되는데, 그 결과 식별된 각각의 고장모드는 상위 수준의 고장모드와 원인과 효과라는 관계로 연결되어 계층 구조를 형성하게 된다. 한 시스템의 고장모드를 분석하는 작업은 각 수준에서 모든 고장모드를 식별해내는 것 뿐 아니라 이러한 FMECA의 계층 구조를 밝혀내는 것을 포함한다. 실질적으로 시스템 체계에 따른 FMECA 계층 구조는 FTA (Fault Tree Analysis)와 FMECA를 결합해서 Bottom-up 방식인 FMECA

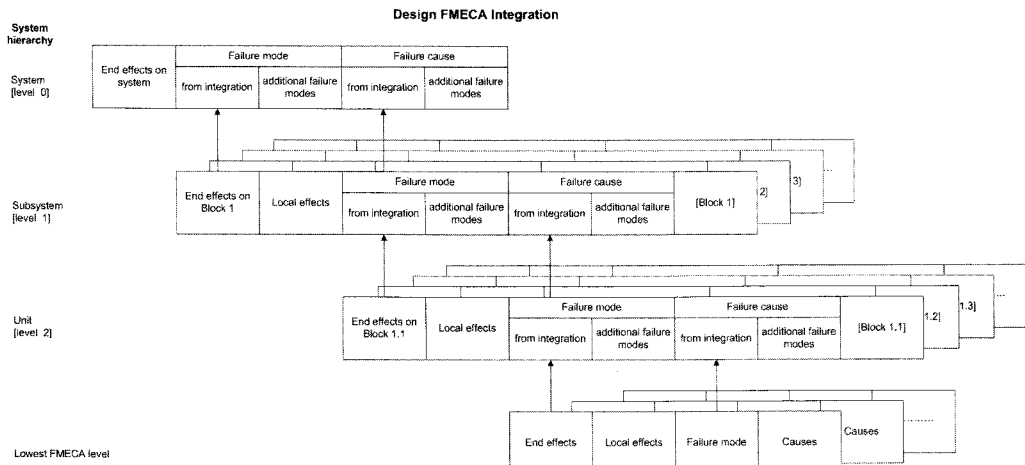


그림 1. 시스템 체계에 따른 FMECA 계층구조 (Figure 5, [6])

의 분석 방법을 보완하는 효과를 가져온다. 시스템 체계에 따라 FMECA 계층 구조를 구성하는 것은 다음과 같은 원칙을 따라야 한다.

- 하위 수준 품목의 모든 FMECA는 연관된 상위 수준 품목의 FMECA에 통합되어야 한다.
- 개발 책임자는 참여업체가 개발하거나 제작하는 품목의 고장모드의 심각도를 알려주어야 한다.
- 참여업체는 납품하는 품목의 고장효과가 그 품목을 구성 컴포넌트로 갖는 상위 품목의 고장모드에 해당한다는 사실을 인식하고 있어야 한다.
- 하위 수준 FMECA의 모든 고장 효과는 상위 수준 FMECA의 고장모드가 된다.
- 앞서서와 같이 연결된 계층 구조에서 동일한 고장효과를 발생시키는 하위 수준의 모든 고장모드는 해당 상위 수준 고장모드의 고장원인이 된다.
- 시스템 계층 구조의 모든 수준에서 하위 수준의 FMECA로부터 도출되지 못하는 고장모드들이 추가될 수 있다.
- 상위 수준 고장모드의 고장원인이 되는 하위 수준 고장모드들은 다른 상위 수준 고장모드들의 공통 고장원인이 될 수 있다. 이러한 FMECA 계층 구조에서는 공통 고장원인에 대한 분석이 필요하다.
- 특수 품목의 작동이나 고장이 기계적, 전기적, 열적 인터페이스를 통해 시스템을 구성하는 다른 품목에 미치는 효과가 분석되어야 한다.

3.2 발사체 레벨의 고장모드

발사체는 비행단계에서 정상궤도에서의 비정상 추력종료, 궤도이탈, 발사체 파괴, 발사체 폭발의 4가지 반응모드를 갖는다. 발사체를 구성하는 서브시스템과 유닛의 고장모드는 최종적으로 4가지 반응 중 하나로 귀결된다. 해외 발사체 실패 사례로부터 발사체 반응모드의 주요 원인이 되는 서브시스템 수준의 고장모드를 정리하면 표 4와 같다 ([5,12]).

표 4. 2단형 우주발사체의 비행단계별 반응 모드와 서브시스템 수준의 고장모드

비행 구간 구분	반응모드	고장모드 수준 1	고장모드 수준 2		
1단 추진 구간	정상 궤도에서의 비정상 추력 종료	조기 엔진 중단	-		
		의도하지 않은 FTS 작동	-		
	궤도 이탈	지상으로부터의 FTS 작동	단분리 실패	단분리 실패	
			PLF 분리 실패	PLF 분리 실패	
		위성 조기 분리	위성 조기 분리		
		추적 실패 = TLM 실패 + 레이더 추적 실패 + EOTS 추적 실패	추적 실패 = TLM 실패 + 레이더 추적 실패 + EOTS 추적 실패		
		주 엔진 조기 점화	-		
		제어 실패	TVC 시동 실패 TVC 제어기 고장 CS-1과 TVC 간의 인터페이스 오류		
	발사체 파괴	추력 정렬 실패	-		
		항법 실패	CS-1 하드웨어 고장 CS-1 소프트웨어 고장		
		공력 편 고장	-		
		PLF 파손	-		
발사체 폭발	KM 초기 점화	-			
	PLF 조기 분리	-			
	PLF 분리 후 발사체와 충돌	-			
2단 추진 전 항행 구간	정상 궤도에서의 비정상 추력 종료	의도하지 않은 FTS 작동	위성 조기 분리		
			지상으로부터의 FTS 작동	KM 초기 점화 추적 실패 = TLM 고장 + 레이더 추적 실패	
	발사체 파괴	1/2단 충돌	-	-	
			-	-	
	2단 추진 구간	정상 궤도에서의 비정상 추력 종료	KM 점화 실패	명령 인터페이스 라인 실패	
				점화기 고장	점화기 고장
		궤도 이탈	KM 추력 감쇄	고고도 점화 실패	고고도 점화 실패
				KM 초기 연료 소모	-
			Coasting 구간에서 RCS 고장	-	
			TVC 고장	-	
			추력 정렬 실패 및 CG 읍셋 오류	-	
			항법 실패	INGU 하드웨어 고장 INGU 소프트웨어 고장	
발사체 파괴		명령 인터페이스 고장	-		
		KM 폭발	-		
		상단부 구조물 파손	-		
		위성 조기 분리	-		
궤도 이탈	의도하지 않은 FTS 작동	지상으로부터의 FTS 작동	추적실패 = TLM 실패 + 레이더 추적 실패		
		추적 실패 = TLM 실패 + 레이더 추적 실패	추적실패 = TLM 실패 + 레이더 추적 실패		

3.4 KSLV-I 상단부의 고장모드 목록

표 4에서 조사된 서브시스템 수준의 고장모드를 기준으로 KSLV-I 상단부 서브시스템에 대해 레벨 5까지 고장모드를 식별하고 시스템 구조에 따른 고장모드의 계층 구조를 분석하였다. 본 논문에서는 레벨 2까지의 고장모드를 표 5에서 기술한다. KSLV-I 상단부 전체에 대한 고장모드는 [2]에 상세하게 설명되어 있다.

표 5. KSLV-I 상단부 유닛 레벨까지의 고장모드 목록

서브시스템	레벨 1	레벨 2
2단 구조체 파손	과도한 하중에 의한 구조 파손과 탑재물 오작동	정하중에 의한 구조 파손 동하중에 의한 구조 파손과 탑재물 오작동 1,2단 진동 커플링에 의한 과도 하중
	기계적 체결과 인터페이스 실패	1,2단 기계적 인터페이스 실패 고주파 랜덤 진동에 의한 탑재물/체결류 풀림 Subassy.간 체결류 고장
	복합재료 구조물의 불성치 저하로 인한 파손	제작/조립/운용 작업에서의 오류 단열 실패
	Subassy. 구조물 파손	EB 파손 KMS 파손 SJ 파손
위성 분리 실패	조기 분리	우발적 자동발화 비정상 기록신호 발생 클램프밴드 파손으로 인한 인장볼트 끊어짐
	분리 실패	파워 카트리지의 고공전화 실패 기록 후 인장볼트 절단 실패
	분리 후 비정상 작동	분리 속도 이상 분리 가속도 이상 밴드 캐치 실패
FTS 실패	종단 명령 시 FTS 작동 실패	FTS 신호 수신 실패 기록 실패 KM 케이스 절단 실패
	의도하지 않은 FTS 작동	종단 명령 없이 FTS 자동 기록
KM 실패	KM 점화 실패	점화구동부 결함 진공 점화 실패
	KM 폭발	노즐 파손 케이스 파손
INGU 실패	구성 하드웨어/소프트웨어 고장	하드웨어 고장 관리자 소프트웨어 고장 기능 소프트웨어 고장
	기능고장	정렬 실패 시퀀스 명령 실패 자세제어 명령 실패 심각한 위성 궤도오차 발생
	제어명령 이상	서보제어기 전원공급 이상 INGU로부터의 제어명령 이상
TVC 시동	제어명령 이상	서보제어기 오동작 TVC 변위 측정 실패 Pitch 작동기 고장 Yaw 작동기 고장

및 운영 실패	유압구동 실패	서보제어기 오동작
		TVC 변위 측정 실패
		Pitch 작동기 고장
		Yaw 작동기 고장
동력공급 실패	유압공급 실패	유압공급부 전원공급 실패
		BLDC EMDP 고장
		유압누설
		외부 debris 유입으로 인한 유압펌프 손상
RCS 실패	Nitrogen 충전 실패	지상 충전시스템 고장
		RCS 충전라인 고장
	RCS Enable 실패	추력기 구동 신호 생성 실패
		추력기 Solenoid 밸브 열림 실패
추력 이상	추력 허용 범위를 초과하는 이상 추력 발생	추력 허용 범위에 못미치는 이상 추력 발생
		구동시간 지연으로 인한 자세제어 실패
		지상으로부터의 전력공급 실패
		내부/외부전원 전환 실패
2단 전력공급 실패	정전력 전원공급 실패	SSPC On 실패
		Functional 배터리 고장
		전원공급라인 고장
		기동전력 전원공급 실패
2단 텔레메트리 실패	데이터 획득 실패	RDU 구성 전기전자 부품의 고장
		SCU 구성 전기전자 부품의 고장
		센서 고장
		진동, 진공, 열 등의 환경조건에 대한 SCU의 내구성 결함
데이터 손실 실패	데이터 송신 실패	MDU 고장
		데이터 라인 하니스 결함
		Telemetry 송신부 구성 전기전자 부품 고장
		전력증폭부 진공환경에서 microwave breakdown
2단 추적 시스템 실패	수신 실패	S-band diplexer의 진공기밀 실패
		하니스 체결 오류
		지상 추적레이더의 추적 실패
		수신부 전기전자 부품 고장
PLF 시스템 실패	PLF 파손	하니스 체결 오류
		진공기밀 실패
		송신부 전기전자 부품 고장
		진공기밀 실패
PLF 내 페이로드/탑재물 파손	PLF 내 페이로드/탑재물 파손	급속한 외부 공기 유입
		PLF 내외부 압력 평형 유지 실패
		구조강도가 구조하중을 견디지 못함
		급속한 외부 공기 유입
PLF 초기 분리	PLF 초기 분리	PLF 내부 온도 상승
		Duct 탈착
		음향블랭킷이 탈착되어 떨어짐
		비행 중 음향하중을 견디지 못함
TVC 시동	제어명령 이상	INGU의 비정상 기록명령 송신
		EMI, ESD 등으로 인한 비정상 Trigger 신호 발생
		주변 온도 상승 (160 °C)에 따른
		서보제어기 오동작

	EBW 자동 점화 (페어링 내부에 장착된 EBW 주변온도는 50° C 이내로 유지해야 함)
PLF 분리 실패	PLF 분리 명령 실패 기폭 실패 Near/Far PLF 분리 실패
분리 후 상단부와의 충돌	분리 시의 급격한 PLF 내부 압력강하 분리 속도 비정상

4. 비행시험에 대한 시스템 수준의 신뢰도 모델링

4.1 고장모드 분석과 신뢰도 예측

일반적으로 발사체의 신뢰도를 추정하는 데 세 가지 방법이 사용되고 있다. 첫 번째 방법은 PRA (Probabilistic Risk Assessment) 기법을 적용하는 방법으로, 전체 시스템을 수행하는 기능에 따라 서브시스템과 유닛, 컴포넌트 등으로 분해해서 시스템의 고장률을 하부 컴포넌트들의 고장모드의 발생 확률로 모델링하여 계산하는 방법이다. 두 번째 방법은 시스템에 대한 기능적 분해 없이 경험 있는 전문가의 판단을 토대로 전체 시스템의 성공률을 추정하는 방법이다. 세 번째 방법은 시스템의 과거 이력 데이터에 대한 통계적 분석을 통해 고장률을 예측하는 방법이다. 발사체와 같이 복잡한 대규모 시스템의 경우, 개발 초기 단계에서 통계적 분석이 유효할 정도의 데이터를 획득하기 어려우므로 PRA 기법을 활용하여 신뢰도를 계산하게 된다. 이 때 전체 시스템의 고장률은 그 시스템의 고장모드 계층 구조와 사건 발생 트리에 맞추어 고장 확률을 조합한 값으로 계산되므로, 시스템에 대한 고장모드 분석은 PRA 기법을 활용한 신뢰도 계산에 있어 필수적인 작업이 된다.

PRA를 실제 시스템에 적용하기 위해서는 기본 초기 사건 (BIE, Basic Initiating Event)으로부터 최종 사건 (FE, Final Event)으로의 사건 시나리오를 모델링해야 한다. 최종 사건이 발생할 수 있는 사건 시퀀스 확률의 합으로 고장률이나 실패율이 계산된다는 점에서, 이 사건 시나리오 모

델링은 해당 시스템의 운용, 작동, 고장 메커니즘을 표현하고 정량적 분석을 수행하는 데 있어 가장 핵심적인 작업이라 할 수 있다. PRA의 사건 시나리오 모델링은 두 가지 부분에서 한계를 갖고 있는데, 1)PRA 사건 시나리오 모델링이 해당 시스템에서 발생할 수 있는 주요 사건 모두를 포괄하지 못하는 불완전성과 2)기본 초기 사건으로부터 최종 사건으로 연결되는 모든 사건 시나리오를 포괄하지 못하는 불완전성, 두 가지 불완전성 문제가 발생한다. 따라서 전문가들은 이러한 불완전성 문제를 보완하고 해당 시스템의 특수한 메커니즘을 반영하기 위해 기존의 PRA 방법론을 보완하는 것을 목적으로 하는 추가적인 사건 모델링 방법을 활용해왔다. 본 논문에서는 고장모드 분석을 활용한 사건 시나리오 모델링의 대표적인 두 방법으로, Cassini 무인 위성에 적용되었던 사건 시퀀스 모델 구조 (Accident Sequence Model Structure) ([9])와 스페이스 셔틀 오비터의 TPS (Thermal Protection System)에 적용되었던 작용 다이어그램 방법 ([10-11])을 소개한다.

사건 시퀀스 모델링 방법은 기본 초기 사건 이후에 3단계의 pinch-point 사건 계층을 설정하고 각 pinch-point에 해당하는 사건들을 식별한 후 pinch-point 계층 간 사건들의 연결 구조를 찾아내는 방법이다. 사건 시퀀스의 3가지 pinch-point 계층은 다음과 같이 정의된다.

- AIC (Accident Initiating Condition) - 발사체 혹은 위성의 심각한 고장을 발생시키는 시스템 수준의 시작 사건
- AOC (Accident Outcome Condition) - 최종 사건을 발생시키는 시작 사건이 되는 발사체 혹은 위성 수준의 심각한 고장
- FE (Final Event) - 해당 임무의 실패로 인해 인명, 재산, 환경 등에 직접적인 손실과 피해를 가져오는 사건

앞에서 정의한 3단계 pinch-point 사건들로 구성된 사건 시퀀스 모델링은 다음과 같은 절차로 작성된다. 사건 시퀀스 모델은 발사체와 같은 여

러 기능들과 사건들이 복합적으로 작동하는 시스템 수준의 PRA 분석에 적합하다.

[단계 1] 각 pinch-point 계층별 사건의 set을 작성한다. BIE는 FMEA, AIC/AOC/FE는 MLD (Master Logic Diagram)을 통해 사건의 set을 구성한다.

[단계 2] Pinch-point 계층별 사건 간에 연결 구조를 구성한다.

- BIE → AIC : FTA
- AIC → AOC : ETA
- AOC → FE : ETA

기본 초기 사건과 최종 사건 사이를 3단계의 pinch-point 계층을 나누어 각 계층에 대해 사건을 먼저 식별한 후 작동 메커니즘을 분석하여 연결 구조를 발견해내었던 사건 시퀀스 모델링 방법과는 다르게, 해당 시스템의 주요 사건과 작용 관계를 일괄적으로 모델링하여 사건 시나리오를 모델링하는 PRA 모델링 방법을 작용 다이어그램 방법이라고 한다. 작용 다이어그램을 통해서 다양한 사건 시나리오의 초기 사건과 조건 변수, 발생할 가능성이 있는 연계 사건과 최종 결과 등을 구분하고 분석해낼 수 있게 된다. 이 모델링 방법은 기능이 한정적으로 정의되는 서브시스템 수준의 시스템에 대한 PRA 모델링 방법에 적합하다. 작용 다이어그램을 통해 PRA 모델링을 수행하기 위해서는 다음과 같은 단계를 거치게 된다.

[단계 1] 시스템의 기능, 물리적 구조, 작동 특성 등을 분석한다.

[단계 2] 작동 환경과 시스템에 미치는 효과에 대해 분석한다.

[단계 3] 해당 시스템 혹은 유사 시스템, 구성품 등의 고장 이력과 사고 기록을 분석한다.

[단계 4] 시스템의 주요 고장 메커니즘을 분석한다.

[단계 5] PRA 모델링을 위한 기본 사건과 랜덤

변수를 설정하고 작용 다이어그램을 작성한다.

[단계 6] 기본 사건의 발생 확률에 영향을 미치는 결정과 작업들을 식별한다.

[단계 7] 작용 다이어그램에 바탕을 둔 ETA 모델을 구성하고, 랜덤 변수에 대한 확률 계산을 통해 정량적 분석을 수행한다.

4.2 KSLV-I 상단부의 비행시험 신뢰도 모델링

임무의 성공률과 KSLV-I 상단부의 신뢰도를 예측하기 위해서는, 비행시험 임무 프로파일을 비행시퀀스에 따라 중요 구간을 구획하고 각 구간별로 작동하는 서브시스템과 그 기능을 우선적으로 식별해야 한다. 이 때 해당 구간에서 수행되는 특정한 기능의 조건부 확률을 계산해낼 수 있게 되는데, 전체 임무의 성공률은 이러한 조건부 확률의 곱으로 표현된다. 최종적으로 얻어지는 비행시험 임무 프로파일 구간에 따른 작동 서브시스템 목록으로부터 비행시험에 대한 시스템 수준의 신뢰도 모델이 유추될 수 있다.

표 6. KSLV-I 비행시험 임무 구간 구분

Event	Elapsed Time (s)	Phase Num.	Phase Time (s)
Start inertial navigation	-10.0		
Stage I engine ignition	-3.8	1	6.2
Lift-off	0.0	2	3.8
PLF separation	215.0	3	215.0
Stage I engine cut-off	223.4	4	8.4
Stage I separation	226.4	5	3.0
Stage II KM ignition	395.0	6	168.6
Stage II KM burn-out	453.8	7	58.8
Payload separation	540.0	8	86.2
End CCAM	560.0	9	20.0
Mission End	1100.0		

본 논문에서는 현재까지 확정된 KSLV-I 비행

표 7. KSLV-I 비행시험 임무 구간 별 주요 서브시스템 기능

Mission Phase	KSLV-I Stage II Subsystems											
	Structure	PLA	PSD	FTS	CM	INGU	TVC	RCS	PWS	TLM	TRK	PLF
1	Str Fn.1-3	PLA Fn.1-2	-	FTS Fn.1-2	-	INGU Fn.1-2, 6	TVC Fn.1	-	PWS Fn.3, 5	TLM Fn.1	TRK Fn.1	PLF Fn.1
2	Str Fn.1-3	PLA Fn.1-2	-	FTS Fn.1-2	-	INGU Fn.2, 6	TVC Fn.1	-	PWS Fn.3, 5	TLM Fn.1	TRK Fn.1	PLF Fn.1
3	Str Fn.1-3	PLA Fn.1-2	-	FTS Fn.1-2	-	INGU Fn.2, 5-6	TVC Fn.1	-	PWS Fn.2-5	TLM Fn.1	TRK Fn.1	PLF Fn.1-2
4	Str Fn.1-3	PLA Fn.1-2	-	FTS Fn.1-2	-	INGU Fn.2, 6	TVC Fn.1	-	PWS Fn.3, 5	TLM Fn.1	TRK Fn.1	-
5	Str Fn.1-3	PLA Fn.1-2	-	FTS Fn.1-2	-	INGU Fn.2, 6	TVC Fn.1	-	PWS Fn.3, 5	TLM Fn.1	TRK Fn.1	-
6	Str Fn.1-3	PLA Fn.1-2	-	FTS Fn.1-2	-	INGU Fn.2-6	TVC Fn.1	RCS Fn.1-2	PWS Fn.2-5	TLM Fn.1	TRK Fn.1	-
7	Str Fn.1-3	PLA Fn.1-2	-	FTS Fn.1-2	KM Fn.1	INGU Fn.2-6	TVC Fn.1-3	RCS Fn.1-2	PWS Fn.3-5	TLM Fn.1	TRK Fn.1	-
8	Str Fn.1-3	PLA Fn.1-2	PSD Fn.1	-	-	INGU Fn.2-6	TVC Fn.1	RCS Fn.1-2	PWS Fn.2-5	TLM Fn.1	TRK Fn.1	-
9	Str Fn.1-3	-	-	-	-	INGU Fn.2-7	TVC Fn.1	RCS Fn.1-2	PWS Fn.3-5	TLM Fn.1	TRK Fn.1	-

시퀀스를 토대로, 전체 임무를 표 6과 같이 신뢰도 모델링을 위한 9개의 세부 구간으로 나누고 표 2의 기능 분류에 따라 각 구간 별로 수행되는 기능들을 식별하여 목록을 작성한다. (표 7) 이렇게 해서 얻어진 표 7의 결과와 3절의 고장모드 분석 결과를 바탕으로 KSLV-I 상단부의 시스템 수준 비행시험 신뢰도 모델을 구성한다. (그림 2)

5. 결론 및 추후과제

본 논문에서는 KSLV-I 상단부에 대한 신뢰성 분석과 시스템 수준의 신뢰도 모델링을 수행하였다. 우주발사체의 발사와 비행시험을 성공적으로 수행하기 위해서는 사용되는 모든 시스템에 대한 신뢰성이 보증되어야 한다. 따라서 최종 발사준비 점검에 있어 신뢰성 평가와 입증은 GO/NO-GO의 최종 판단에 결정적 요소가 된다. 본 논문에서 수행한 고장모드 분석과 시스템 수준의 신뢰도 모델링은 발사와 비행시험에 대한 신뢰성 최종 점검 항목 작성과 검증, 최종 임무 수행 신뢰도 예측 등을 위한 예비 작업으로 볼 수 있다. 또한 신뢰성 분석과 신뢰도 모델링이 KSLV-I 상단부에 한정되어 있으므로 발사와 비행시험 전체에 대한 신뢰성 평가와 입증은 수행하기 위해서는 AC, LC, DMAPS, KSLV-I 1단에까지 확장해

야 한다. 따라서 최종 발사준비 점검을 위한 신뢰성 평가와 입증은 위해서는 다음과 같은 작업들이 진행될 필요가 있다.

- KSLV-I 상단부에 대한 SPF (single point failure)와 critical 컴포넌트 분석
- KSLV-I 상단부의 비행시험 신뢰도 모델 수정/보완
- KSLV-I 상단부에 대한 신뢰성 요구조건/대책/점검 목록 작성
- KSLV-I 상단부 구성 컴포넌트 시험평가 결과에 대한 통계적 분석과 확률 계산
- 발사 시퀀스 시간 구분과 신뢰도 모델링
- KSLV-I 각 구성 컴포넌트의 시험평가 결과에 대한 통계적 분석과 확률 계산

참고 문헌

1. DR61400PA00000-0008, KSLV-I 상단부 주요 서브시스템 기능분석.
2. DR61400PA00000-0012, KSLV-I 상단부 주요 고장모드 정의와 분석.
3. DR61400PA00000-0013, KSLV-I 비정상 및 비정상상태 정의와 대책.
4. DR61400PA00000-0014, KSLV-I 비행시험에

대한 시스템 수준 상단부 신뢰도 모델링.

5. RV41000PA00000-0005, 해외발사체 사례분석을 통한 2단형 발사체의 비행실패 확률 및 실패모드 추정.
6. ECSS-Q-30-02A, Failure modes, effects and criticality analysis (FMECA).
7. MIL-STD-1629A, Procedures for performing a FMECA.
8. NASA-TM-X-66741, Apollo-Saturn 201 Mission Reliability Analysis.
9. Sergio Guarro, Bruce Bream, L. Kevin Rudolph, Robert J. Mulvihill, "The Cassini mission risk assessment framework and application techniques", Reliability Engineering and System Safety, vol. 49, pp. 293-302, 1995.
10. Elisabeth Paté-Cornell, Paul S. Fischbeck, "PRA as a management tool: organizational factors and risk-based priorities for the maintenance of the tiles of the space shuttle orbiter," Reliability Engineering and System Safety, vol. 40, pp. 239-257, 1993.
11. Elisabeth Paté-Cornell, Paul S. Fischbeck, "Probabilistic risk analysis and risk-based priority scale for the tiles of the space shuttle," Reliability Engineering and System Safety, vol. 40, pp. 221-238, 1993.
12. I-Shih Chang, "Investigation of space launch vehicle catastrophic failure," Journal of Spacecraft and Rockets, vol. 33, no. 2, pp. 198-205, 1996.
13. Frank J. Groen, Carol Smidts, Ali Mosleh, "QRAS - the quantitative risk assessment system," Reliability Engineering and System Safety, vol. 91, pp. 292-304, 2006.

표 2. KSLV-I 상단부의 주요 기능

상단부 시스템	구분	번호	기능
2단 구조체	STR Fn.1		위성체와 PLA로부터의 관성 하중을 지지하고 2단 내부구조를 1단 구조 및 페어링과 연결하는 기능
	STR Fn.2		전자/제어/항법장치 등의 탑재물을 안정적으로 장착하는 기능
	STR Fn.3		TVC와 RCS의 각종 부품을 장착하고 2단 추진기관을 지지하는 기능
TPS	TPS Fn.1		2단 구조와 내부의 작동기기/계측기기에 대한 열안정성 유지
TCCS	TCCS Fn.1		위성 및 탑재물의 열정정 환경 제어
위성 어댑터	PLA Fn.1		위성분리장치 장착, 위성체를 지지하는 기능
	PLA Fn.2		위성분리 전까지 위성과 2단 구조체 사이를 기계적으로 연결하는 기능
위성 분리장치	PSD Fn.1		분리명령에 따라 2단 구조체와 위성을 분리하는 기능
FTS	FTS Fn.1		중단 명령 수행 (GFTS에서 중단 명령이 송신되었을 때, 정확히 FTS가 작동)
	FTS Fn.2		비정상 비행중단 방지 (GFTS에서 중단 명령이 송신되지 않았을 때, FTS가 작동하지 않음)
KM	KM Fn.1		2단 비행구간 동안 충분한 추력을 안정적으로 공급하는 기능
INGU	INGU Fn.1		관성항법유도장치는 관성센서 출력, 초기 위치정보, Theodolite 건물을 이용하여 측정된 방위각 정보를 통해 초기 자세 각(pitch, yaw, roll 각)을 결정하는 기능 (정렬)
	INGU Fn.2		자이로와 가속도계 출력을 적분하여 초기 자세 각, 속도, 그리고 위치로부터 현재의 자세 각, 속도, 그리고 위치를 계산하는 기능 (관성항법)
	INGU Fn.3		비행 중 발생한 외란 및 성능 오차에 의해 최종 궤도 투입 오차가 커지는 것을 막기 위해 비행 중 필요한 자세 명령 및 시퀀스 변경을 계산하는 기능 (유도)
	INGU Fn.4		비행 중 안정성을 유지하고, 발사체가 Open-loop로 미리 계산된 자세명령을 잘 유지하도록 하는 추력 벡터명령과 추력기 명령을 계산하는 기능 (자세제어)
	INGU Fn.5		비행 중 요구되는 점화, 페어링 분리, 위성분리 등 발사체의 비행에 필요한 시점에 디스크릿 명령 신호를 전달하는 기능 (시퀀스)
	INGU Fn.6		2단 ML-STD-1553B 데이터 버스에서 버스 컨트롤러 기능을 수행, 2단 제어시스템으로부터 데이터를 수집하여 MDU로 전송 (데이터 버스 컨트롤러 기능)
	INGU Fn.7		위성분리 후 CCAM (충돌 회피 기능)
TVC	TVC Fn.1		구동장치를 가동노즐과 KM 후방스커트에 연결시키는 인터페이스 역할
	TVC Fn.2		관성항법 유도장치로부터 온 제어신호 따라 구동장치를 제어하는 기능
	TVC Fn.3		유압동력을 발생시키고 구동장치로 전달해서 가동노즐을 구동하는 기능
RCS	RCS Fn.1		자세제어를 위한 추력을 발생시키는 기능
	RCS Fn.2		추력기의 On/Off 제어 및 시스템 상태확인을 수행하는 기능
2단 전력공급 시스템	PWS Fn.1		지상으로부터 전력을 공급받아 배터리를 충전방전하고 내외부 전원전환을 수행하는 기능
	PWS Fn.2		KM 점화안전장치, PLF 분리, 위성분리에 대한 지상시스템으로부터의 Arming 명령과 INGU로부터의 기폭 명령을 릴레이 및 기폭 장치에 전달하는 기능
	PWS Fn.3		비행 중 연속적으로 일정한 정전력을 소모하는 전자장치에 전력을 공급하는 기능
	PWS Fn.4		비행 중 불연속적으로 가변 전력을 소모하는 부하 (롤 추력기, KM 점화안전장치, PLF EBW 구동장치, 위성분리장치)에 전력을 공급하는 기능
	PWS Fn.5		2단 전력부하의 전력을 제어/감시/보호하고 전력 상태 데이터를 지상 및 텔레메트리로 전송하는 기능
2단 텔레메트리	TLM Fn.1		발사체 데이터의 획득/처리/송신 기능
2단 추적시스템	TRK Fn.1		지상 레이더의 추적용 펄스 신호를 수신하고 그에 따른 응답 신호를 지상으로 전송해서 발사체의 비행 궤적을 실시간으로 추적가능하게 하는 기능
PLF	PLF Fn.1		열, 전기, 음향하중 등 외부환경으로부터 위성체와 탑재체를 보호하는 기능
	PLF Fn.2		PLF 분리 및 분리 후 충돌회피 기능

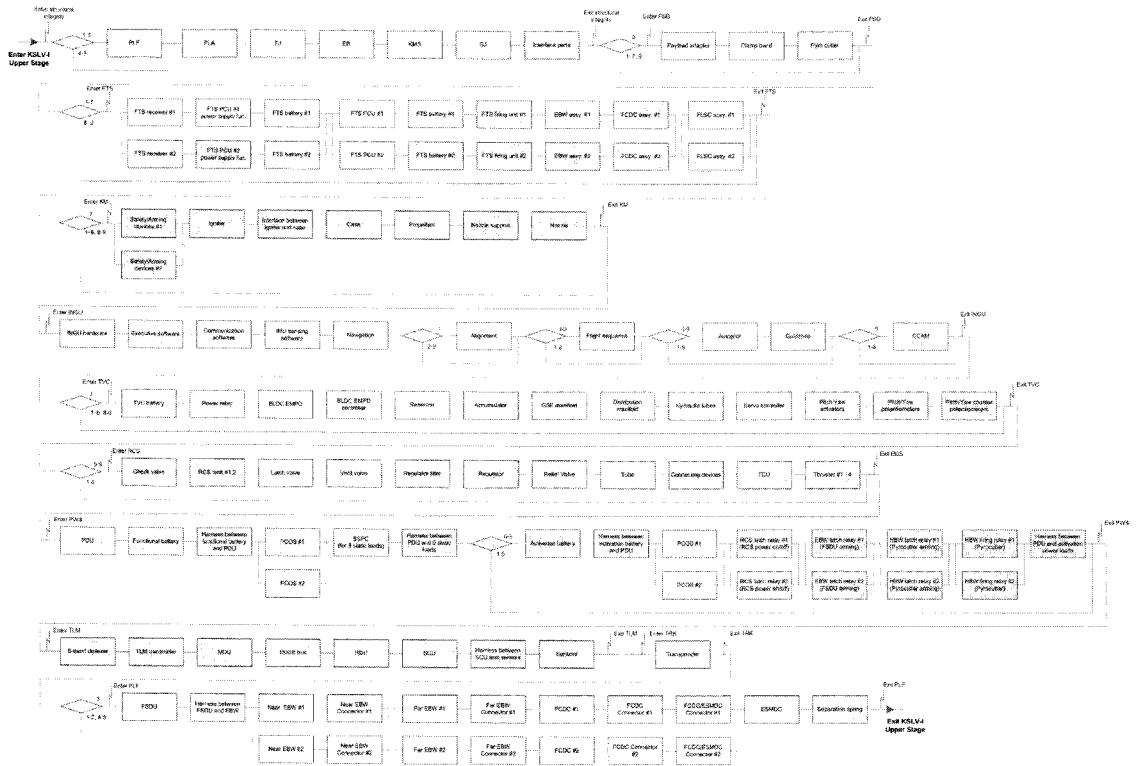


그림 2. KSLV-I 상단부의 시스템 수준의 비행시험 신뢰도 모델