# 우주 발사체 추진기관 공급시스템의 사전 위험 분석

조상연*† · 오승협*

# Preliminary Hazard Analysis for Propulsion System of Space Launch Vehicle

Sang Yeon Cho*† · Seung Hyub Oh*


## ABSTRACT

KARI is now developing KSLV-II which can insert 1.5ton satellite into the orbit, and system design review is close at hand. As a part of mission assurance for space launch vehicle, reliability and safety management is being performed and to assure the safety, KARI has been doing actions on the basis of the safety assurance plan and system safety program plan. In this study, preliminary hazard analysis is reviewed and the result for the propulsion system will be illustrated. The result will be used as a reference for the safety and risk management.

## 초 록

한국항공우주연구원에서는 현재 1.5톤급 위성 발사체인 한국형 발사체 KSLV-II를 개발중이며 시스템의 설계 리뷰를 앞두고 있다. 또한, 발사체의 개발과정에 있어서 임무 보증 업무의 일환으로 신뢰성과 안전, 품질등을 관리하고 있으며 발사체의 안전 확보를 위해서 기존에 공표된 안전 보장 계획 및 시스템 안전 프로그램 계획에 따라 관련 업무를 수행하고 있다. 본 연구에서는 상기의 계획에 의거하여 수행된 사전 안전 분석의 내용과 방법에 대하여 설명하고 실제 추진기관 시스템에 대하여 도출된 위험요소들을 소개하고자 한다. 도출된 위험 요소들은 향후 개발이 진행되면서 위험 수준을 완화하는 방향으로 관리될 계획이다.


Key Words: KSLV-II (한국형발사체), Propulsion system (추진기관 시스템) Safety (안전), PHA (사전 안전 분석)

## 1. 서 론

한국형 발사체 KSLV-II는 2020년을 발사 목표로 하는 1.5톤 급의 인공위성 발사체로 위성을 태양 동기 궤도를 포함한 지구 저궤도에 올릴 수 있는 발사체이다. KSLV-II는 3단형의 발사체로 1단은 75톤급의 액체 엔진을 4기 클러스터한 300톤 급의 추진기관이 적용될 계획이며 2단은 1단에 사용한 75톤급 엔진 1기에 확장 노즐을

* 정회원, 한국항공우주연구원 발사체추진기관팀
† 교신저자, E-mail: chosangy@kari.re.kr

장착하는 개념으로 개발될 예정이다. 3단 엔진의 경우, 7톤급의 터보펌프 엔진을 사용하는 것으로 결정되었다.

우주 발사체와 같이 사고가 발생할 확률이 높은 대형 시스템의 개발에 있어서는 제품 보증 차원에서의 신뢰성과 안전, 품질 등의 확보가 반드시 필요하며 이에 요구조건 도출 단계부터 관련 제품보증워킹그룹을 구성하여 해당 업무를 수행한 바 있다. 비록 현재는 한국형 발사체 개발 사업단이 새로이 구성되었으나 상기의 개념은 크게 변경되지 않고 유지되고 있다.

우주 발사체의 개발과 같은 대형 시스템의 안전 확보를 위해서는 각종 안전 관련 활동이 지속적으로 수행되어야 하며 이런 차원에서 이미 발사체 시스템 수준의 "안전 보장 계획"이 수립된 바 있다.[1],[2] 본 논문에서는 안전 보장 계획에서 언급된 사전 안전 분석의 내용에 대하여 설명하고 추진기관 추진제 공급 시스템에 대한 적용 결과를 소개하고자 한다.

## 2. 사전 위험 분석

### 2.1 시스템 안전 관리 차원에서의 사전 위험 분석

아래의 그림 1은 미국 FAA에서 규정한 시스템 안전 관리의 흐름도이다.

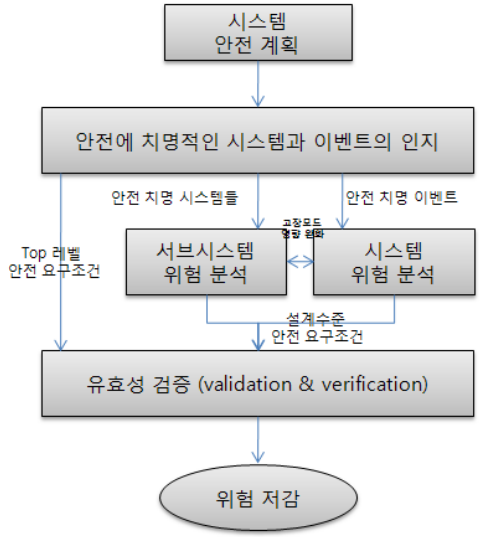


그림 1 시스템 안전 관리 흐름도 [3]

상기의 규정에 따르면 개발 초반에 시스템 안전 계획을 수립하고 안전에 치명적인 시스템과 이벤트의 인지 (Safety critical systems and events identification)하는 작업을 수행한 뒤 이어서 시스템 수준의 위험 분석과 서브 시스템 수준의 위험 분석을 동시에 수행하고 top level의 요구조건에 따른 유효성 검증 (V&V)을 수행하는 순서로 안전 관리가 이루어지게 된다. 이중 안전 치명 시스템 및 이벤트 분석은 시스템 개발 초기에 수행되어야 하며 이단계에서 사용되는 분석 방법들은 사전 위험 분석 (Preliminary hazard analysis; PHA)이나 이벤트 트리 분석 (Event tree analysis; ETA), 고장목 분석 (Fault tree analysis; FTA) 등을 들 수 있다. 이중 PHA는 설계 작업이 시작되자마자 수행되어서 설계상의 trade-off study 적용이 될 수 있어야 하며 미래의 분석을 위한 baseline으로 사용된다.

한국형 발사체의 경우, 전체 시스템에 대한 PHA는 SDR 단계에 시작되어 PDR 단계에서 보고될 것이다.

### 2.2 PHA의 내용과 장단점

PHA는 잠재적인 장애 요소에 대한 가장 일반적이고 정성적인 식별 및 목록화 기법으로 설계의 가이드로 사용되거나 장애 요소들에 대한 절차상 보호 방법을 정의하는데 사용된다. 또한, 사고의 인과 관계나 위험 회피 방안, 혹은 위험의 제어 방법의 식별에 적합하다. [4] 이때, 회피하거나 제어해야하는 장애 이벤트의 목록은 서브 이벤트 수준까지 작성될 수 있다.

PHA는 일반적으로 비용 효율을 높이기 위해 설계나 운용 계획 수립의 초기 단계에 수행된다. 아래의 표 1은 PHA를 통해 확인할 수 있는 일반적인 고장/장애의 일반적인 예를 보여준다. 이러한 고장/장애 상태나 그 결과는 안전 치명 요소 (safety critical item)의 식별과 위험 관리에 사용될 수 있다.

PHA는 성격상 귀납적인 방법이지만 고장의 시스템 계통 구조 목록이나 잠재적 대형 사고로 이르는 사건을 분석한다는 측면에서는 연역적 분석 방법이라고 볼 수도 있다.

표.1 고장 및 장애의 예

| Possible Effects | Possible Cause |
|---|---|
| 기계적 고장 | |
| 1. 장비가 작동 안함<br>2. 진동과 소음<br>3. 베어링의 문제 발생 | 1. 부품의 파손<br>2. 커플링의 분리<br>3. 파스너의 분리<br>4. 지지대나 인터록의 고장<br>5. 심한 녹이나 오염에 의한 협착<br>6. 부품의 정열 실패 |
| 동력원의 고장 | |
| 1. 동력에 의존하는 시스템의 완전한 작동불능<br>2. 치명적인 순간 추진력의 상실<br>3. 움직이는 물체의 유도 제어 실패<br>4. 비행체의 비행 구간에서의 고장<br>5. 타 시스템 가동 불능<br>6. 생명 유지 장치의 고장<br>7. 안전 모니터링 및 경고 시스템의 고장<br>8. 비상 구조 시스템의 고장 | 1. 회전/왕복 부품의 파손, 비정열, 유격<br>2. 진동 차단재나 충격 흡수재의 파손/마모<br>3. 과부하에 의한 베어링 손상<br>4. 베어링이 너무 조이거나 헐거움<br>5. 윤활 부족<br>6. 주요 부속 고장<br>7. 터빈 구동에 사용되는 스팀이나 기체, 물등의 진로 방해<br>8. 동력 관련 장비의 과도한 마모<br>9. 동력 관련 장비의 기계적 파손<br>10. 치명적 장치의 비정상적 조정<br>11. 발전기와의 연결 불량<br>12. 제어 불능에 의한 과도한 속도<br>13. 전지의 전해물질 손실 |
| 전기 시스템의 고장 | |
| 1. 전체 시스템 작동 불능<br>2. 특정 장치의 작동 불능<br>3. 통신 방해<br>4. 계측, 경고 장치의 불능<br>5. 피뢰시스템의 고장<br>6. 지지 장치의 고장 | 1. 전기 연결 불량<br>2. 연결시의 고장<br>3. 컨덕터 잘림<br>4. 퓨즈나 회로의 파손 혹은 오픈<br>5. 컨덕터 전소<br>6. 스위치나 다른 장치의 오픈 혹은 파손<br>7. 단락<br>8. 과부하 |

잘 수행된 PHA란 흔히 위험이라고 번역되는 hazard와 그 잠재 영향을 정확히 식별하고 위험 상황의 심각도와 가능성을 분석하여 비용 효율적 자원 배분을 돕는데 기여할 수 있다.

PHA는 매우 직설적이고 용이한 분석 방법이지만 동시에 다중의 원인에 의한 비정상 상태는 분석되지 않고 개발 후반부에 수행되면 큰 효과를 보기 어렵다는 단점이 있다.

2.3 PHA의 형식

PHA를 수행하기위해 우선 위험 분석 행렬의 개념을 사용하여 위험도를 지표화한다. 파스칼의 원리에 의해 위험도는 심각도(severity)와 확률(probability)의 곱으로 표현이 가능하다.

MIL-STD-882에 따르면 위험 분석 행렬은 아래 그림 2와 같이 심각도와 확률을 축으로 하여 구성한다. 이때 심각도는 4단계로 구분하고 발생 확률은 5단계로 구분하여 정성적으로 평가한다.

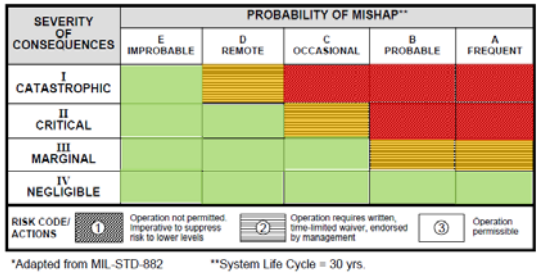


그림 2 위험 분석 행렬

이 경우 I/A, I/B, I/C, II/A, II/B는 Risk Code 1로 I/D, II/C, III/B, III/A는 Risk Code 2로, 나머지는 Risk Code 3으로 표시하고 Risk

tolerance limit을 지정하여 이를 넘는 항목들을 해결하기 위한 작업을 지시한다. 일반적으로 risk code 1,2에 대하여 이러한 작업을 하게되는데 그 내용은 ①포기, ②위험 전가 (보험 등), ③ 예외 (waiver) 선언, ④위험 완화 방법 개발 등이 있을 수 있다.

PHA는 기관별, 회사별로 차이가 있으나 일반적으로 다음의 내용이 포함되는 것이 바람직하다.

① 위험명 (근원(source) -> 메카니즘 -> 결과)
② 임무 단계 (mission phase)
③ 타겟 (일명 hazard의 희생자)
④ 노출 기간
⑤ 심각도 분석
⑥ 확률 분석
⑦ 위험 분석 행렬을 이용한 위험 분석
⑧ 위험 완화 방안
⑨ 기타 (날짜, 평가자, ID 등)

2.4 추진기관 시스템에 대한 PHA 수행 결과

위에서 언급한 내용에 따라 한국형 발사체의 WBS 3레벨 기준으로 수행한 추진기관 공급 시스템의 사전 위험 분석 결과는 다음 그림3과 같다.

KARI **Preliminary Hazard Analysis Worksheet** Date: Page: Part Analyzed: 추진기관시스템

| ITEM NO. | Hazard Cause(s) | Hazardous Condition | Hazard Effects | Hazard Severity | Hazard Frequency | Hazard Risk index | Hazard Controls |
|---|---|---|---|---|---|---|---|
| 1 | 산화제 충전/배출/공급 시스템에서의 누설 | 유기물질과 에너지 소스 결합에 의한 화재 발생 | 화재/폭발에 의한 기체 파손 | II | C | 2 | |
| 2 | 연료 공급/충전/배출 시스템에서의 누설 | 국부적 에너지 소스에 의한 화재발생 | 화재/폭발에 의한 기체 파손 | II | C | 2 | |
| 3 | 산화제 탱크 벤트 시스템 고장 | 산화제 탱크 과압 | 탱크 파손 | II | C | 2 | |
| 4 | 연료 탱크 벤트 시스템 고장 | 연료 탱크 과압 | 탱크 손상 | II | D | 3 | |
| 5 | PSD 작동 실패 | POGO현상 발생시 제어 불능 | 기체 파손 | I | C | 1 | 작동부 2중화 sol. Valve를 pyro valve 같은 고신뢰성 부속으로 교체 |
| 6 | 추진기관 제어기의 고장 | 밸브 오작동에 따른 추진제 가압 실패 | 엔진 운용 실패에 따른 미션 실패 | II | C | 2 | |
| 7 | 추진제 가압시스템 작동 불량 | 추진제 가압 실패 | 엔진 운용 실패에 따른 미션 실패 | II | D | 3 | |
| 8 | 산화제 라인 냉각 시스템 고장 | 선냉각 실패 | 추진기관 시동 실패 | II | D | 3 | |
| 9 | 탱크나 배관으로 이물질 유입 | 엔진 시스템으로 이물질 유입 | 기체 파손 | I | D | 2 | |
| 10 | 레벨센서의 고장 발생 | 충전량 확인 실패 | 추진기관 운용시간 확인실패로 레도진입 실패 | II | D | 3 | |
| 11 | 추진제 소진 감지 센서의 고장 | 추진기관 비정상 종료 | 레도진입 실패 | II | C | 2 | |
| 12 | 추진제 소진 감지 센서의 고장 | 추진기관 종료 실패 | 기체 파손 | I | C | 1 | redundancy를 적용하여 신뢰도 향상 |
| 13 | | | | | | | |

그림 3 추진기관 공급 시스템 수준의 PHA 결과

상기의 분석은 개발자와의 면담과 당사자 및 제3자의 평가를 거쳐 수행되었다. 분석의 대상이 된 추진기관 공급계 시스템의 경우, 1,2,3단으로 구별한 것이 아니라 전체를 산화제 공급 시스템, 연료 공급 시스템, 가압/순환 시스템으로 구분하여 수행되었다.

PHA의 수행 결과 대략 12개의 위험 요소가 파악되었는데 이중 Risk code 1에 해당되는 항목은 2개로 이는 각각 “POGO 현상을 억제하는 PSD의 작동 실패”와 “추진제 소진 감지 장치의 고장”으로 분석되었다. 이 내용이 흥미로운 점은 해당 하드웨어가 공급 시스템의 운용상으로는 다른 것에 비해 특별히 중요하다고 할 수 없으나 위의 위험이 현실화되었을 경우는 가장 치명적인 사고로 이어진다고 분석된 점이다.

이외에 6개의 Risk Code 2 위험 요소와 4개의 Code 3 위험 요소가 식별되었으며 상기의 위험 요소들 중 Code 1의 경우는 해당 컴포넌트의 개발시 설계에서 위험도를 낮추기 위하여 적용될 개념이 표에서 언급되었다. 현재, 엔진 시스템에 대한 PHA가 수행된 상태이며 전체 발사체 시스템에 대한 분석도 조만간 이루어질 예정이다.

PHA의 분석 결과는 이후 한국형 사업단의 위험 관리 업무가 본격적으로 수행되었을 때 기초 자료로 검토되고 위험을 낮추는 방향으로 관리될 계획이다.

## 3. 결 론

이상과 같이 현 단계에서 수행되어야 할 사전 안전관리의 내용을 설명하고 추진기관 공급 시스템에 대하여 수행한 결과를 나타내었다. 본 연구를 통해 얻어진 결과는 추후 한국형 발사체의 위험관리 활동의 근거 자료와 이후에 수행될 고장목 분석을 위한 기초 분석 자료의 역할을 할 수 있을 것으로 기대된다.

## 참 고 문 헌


1. 조상연, 신명호, 김성룡, 오승협, “우주발사체 개발시의 안전 보장 계획 수립”, 한국항공우주학회 추계학술대회 발표자료, 2011
2. 조상연, 시스템 안전 프로그램 계획 (안), PN0PSG0K0003, 한국항공우주연구원, 2011
3. AC 431.35-2A, Reusable launch and reentry vehicle safety process, FAA, 2005
4. IASS E-07-00403, PHA, APT Research, 2007