

우주발사체 개발사업에서 신뢰성공학의 시스템엔지니어링 인터페이스

신명호*, 조상연, 조미옥
한국항공우주연구원 우주발사체사업단

System Engineering Interfaces of Reliability Engineering in Development of Launch Vehicle

Myoung Ho Shin*, Sang Yeon Cho and Miok Joh

*KSLV Systems Division, Korea Aerospace Research Institute, 45 Oun-dong, Yuseong-gu, Daejeon 305-333,
Korea*

Abstract : Development of launch vehicle needs a large-scale and complicated System Engineering discipline interfacing to small-quantity production with special manufacturing processes. In general, the System Engineering discipline of launch vehicle has its relationship with Production, Operations, Product Assurance and Management disciplines and its internal partitions into the functions of System Engineering Integration & Control, Requirements Engineering, Analysis, Design and Configuration and Verification. As a function of Product Assurance, reliability of launch vehicle plays an significant role in risk management, system safety, flight safety and launch certification through design assurance. Moreover, major functions of systems engineering are integrated by means of reliability in the phases of design and verification. Therefore, detailed identification of system engineering interfaces of reliability, and execution of tasks for reliability assurance is required for successful development of launch vehicle. This paper identifies specific pattern and mechanism of the interfaces between reliability and system engineering.

Key Words : Reliability Program, System Engineering Interface, Reliability Assurance, FMEA, FTA, Failure Mechanism

1. 서론

성공적인 제품 개발은 설계, 개발, 생산, 지원 등의 모든 제품 수명 주기와 수준에서 참여 작업자의 재능과 생산성을 요구하는데, 이러한 요소들은 교육, 책임 부여, 신뢰, 팀 등에 의해서 강화

되는 경향이 있다. 최근에는 이러한 요소를 최적화하기 위하여 시스템엔지니어링은 새로운 과학적 관리의 패러다임으로서 전체 과정을 '하나'의 일관된 관점과 기준으로 통합해서 관리하는 방법론을 모색해 왔다. 일반적으로 제품 개발 과정을 설계와 생산의 두 단계로 구분하는 것은 피할 수가 없는데, 신뢰성은 설계 단계에서 품질은 생산 단계에서 통합 관리의 주요 사업 지표와 목표

* 교신저자 : myshin@kari.re.kr

로서 관리되는 것이 최근의 추세이다. 지난 20년 간의 신뢰성과 품질 부문에서의 놀라운 혁신에 힘입어 복잡함에도 불구하고 신뢰할 만한 제품을 생산해 내는 것이 가능하게 되었다. 이는 또한 설계자나 생산자가 자율적이고 책임 있는 판단을 내릴 수 있는 통합적인 관리 체계 수립에 성공한 것에 힘입은 바 크다. [6,8]

우주발사체 개발사업 역시 신뢰성과 품질은 핵심 요소이며, 각 단계에 따라 기술 관리 전체를 통합하는 역할을 수행한다. 실질적으로 우주발사체 개발사업에서 신뢰성은 제품 개발에 있어서 다른 주요 활동들과 독립적인 활동이 아니라 전 개발 프로그램을 통합하는 요소로서 기능한다. 신뢰성은 고장모드, 고장요인, 고장확률에 대한 분석과 평가는 시스템안전, 비행안전, 발사인증, 승인을 위한 전제조건이자, 사업 전체의 비용과 일정을 결정하는 데 있어 주요한 평가 기준이 된다. 따라서 신뢰성 프로그램은 사업관리, 시스템엔지니어링, 제품보증, 제작, 운용 등 개발사업 전체의 구성요소들을 긴밀하게 결합하는 통합/관리 기능을 수행하게 된다. [5,7]

본 논문에서는 신뢰성 프로그램과 시스템엔지니어링과의 연계성에 보다 주목하고, 신뢰성 프로그램의 주요 업무들에서 시스템엔지니어링 인터페이스가 발생하는 업무별로 경험적이고 실용적

인 내용들을 정리/검토하고자 한다.

2. 우주발사체의 시스템엔지니어링

우주발사체의 시스템엔지니어링은 주요하게 1) 시스템엔지니어링 종합 및 통제, 2) 요구조건 공학, 3) 분석, 4) 설계 및 형상, 5) 검증의 다섯 가지 기능으로 구성되어 있다. 이 다섯 가지 기능은 시스템엔지니어링에서 수행해야할 업무 전체를 포괄하고 있다. Fig. 1은 시스템엔지니어링 내부 기능들 간의 동적 프로세스와 주요 작업의 반복 패턴을 상세하게 보여주고 있다. 고객의 요구조건을 입력으로 하는 시스템엔지니어링 프로세스는 각 기능을 반복적으로 수행해서 최종적으로 인증시험과 요구조건 검증 작업을 완료한 설계형상을 산출물로 생산하면서 종결된다. [2,3]

3. 우주발사체의 신뢰성 프로그램

신뢰성 프로그램은 해당 시스템에 대한 개발 경험과 기술 수준에 기초하여 준비된다. 따라서 시스템에 따라 그리고 개발 경험의 차이와 방식에 따라 조금씩 다른 신뢰성 프로그램을 구축하게 된다. 우주시스템에 대한 일반적인 신뢰성 프로그램 세부 내용은 미국 군사 규격(7)에서 기술하고 있

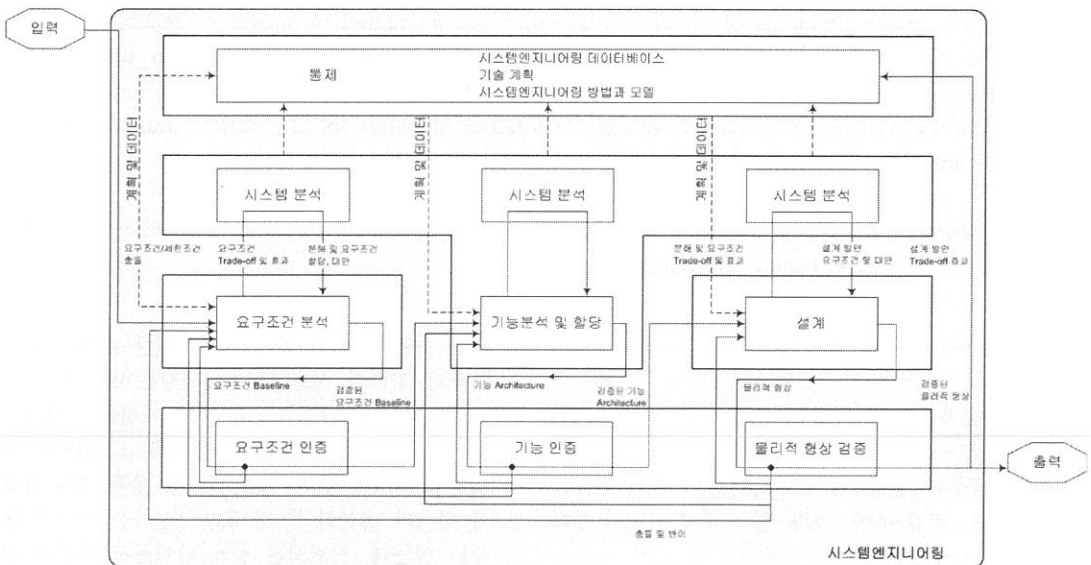


Fig. 1 Internal Process of System Engineering for Launch Vehicle

다. 미국 군사 규격에서 언급하고 있는 우주시스템에 대한 신뢰성 프로그램 업무는 포괄적인 일반 항목들을 나열하고 있으므로, 대상 시스템과 기술 수준에 따라 주요 작업을 선별하여 집중적으로 수행하는 것이 필요하다. 한국형 우주발사체 개발사업에서도 그 특수한 상황에 적절한 신뢰성 프로그램 계획을 수립하는 것이 요구된다. 현재 진행하고 있는 한국형 우주발사체 신뢰성 업무는 Table 1과 같다.

Table 1. Reliability Program Plan for KSLV

1. 신뢰성 예측/평가 기준 및 방법론 결정
2. 시스템 레벨 신뢰성 요구조건
3. 제품보증 요구조건
4. 신뢰성보증 계획
5. 규격서 트리 작성
6. FMEA/치명도 분석
7. 세그먼트/서브시스템 레벨 신뢰성 요구조건
8. 요구조건 검증 및 통제 계획서
9. 신뢰성 중요 품목 통제 및 관리
10. 시험평가 프로그램 검증
11. 서브시스템 레벨 시험 프로그램 검증
12. 서브시스템 레벨 시험 실패 분석 및 결과 검증
13. 종합 시험 프로그램 검증
14. 종합 시험 실패 분석 및 결과 검증
15. 고장/불일치 통제 및 공정관리 결과 검증
16. 시험평가 및 검증의 완전성 평가
17. 시험평가 시험결과 및 신뢰성 보증 활동에 대한 최종 기술 평가
18. 비행시험 프로그램 검증
19. 발사인증 신뢰성 항목 평가/검토
20. 종합 신뢰성 평가 및 예측
21. 신뢰성 지표에 대한 정기적 예측

4. 시스템엔지니어링과 신뢰성 프로그램의 연계

신뢰성은 제품 개발에 있어서 다른 주요 활동들과 전 개발 프로그램을 통합하는 요소로서 기능하므로, 신뢰성 프로그램은 품질 관리 프로그램처럼 강제적인 집행력을 갖추어야 한다. 강제적인 집행을 보장하기 위해서는 의무적인 절차로서 신뢰성 프로그램이 공포되어야 하며, 관련된 작업과 책임 등이 명시되어야 한다. 주요 설계 검토와 감사에서 신뢰성 프로그램에 대한 점검 또한 필수적인 부분으로서 포함되어야 한다. 시스템엔지니어

링 각 기능별로 수행되고 있는 주요 신뢰성 업무는 다음과 같다.

4.1 종합 및 통제 기능에서의 신뢰성 프로그램

4.1.1 신뢰성 프로그램 계획과 매뉴얼

개발 사업의 참여자에게 강제적으로 준수하도록 의무화하는 기본 문서에는 신뢰성 프로그램 계획과 매뉴얼이 있다. 신뢰성 프로그램 계획에는 다음의 내용이 포함되어야 한다.

- 신뢰성 요구조건에 대한 요약 설명
- 참여업체의 신뢰성 조직
- 설계분석, 시험, 보고 등 수행되어야 하는 신뢰성 활동
- 프로젝트 개발 주요 마일스톤에 따른 신뢰성 주요 활동의 수행 시점
- 참여업체에 대한 신뢰성 관리
- 안전, 유지보수, 품질보증 등 신뢰성과 연관된 다른 계획들을 상호 참조하는 표준서, 규격서, 내부 절차서 (신뢰성 매뉴얼)

신뢰성 관리 작업 내용과 설계 지침, 조직 구성, 품질 보증 절차 등을 포괄하는 내부 매뉴얼이 필요하다. 신뢰성 매뉴얼에서 갖추어야 할 최소 항목은 다음과 같다.

- 사업단의 신뢰성 관련 정책
- 신뢰성 조직
- 설계 과정에 적용되는 신뢰성 작업과 절차
- 신뢰성 시험 절차
- 시험 결과로부터 얻어지는 데이터를 포함하는, 신뢰성 데이터 취득/분석/조치 시스템.

4.1.2 신뢰성 성장 계획

새로운 기술요소를 갖고 있는 복잡한 시스템의 경우, 개발단계에서 초기 시제품은 신뢰성과 성능에 있어서 많은 결함을 내포하고 있다. 최종 인증 시험에서 모든 신뢰성 요소를 검사하는 작업으로는 신뢰성 요구조건을 만족시키기 어렵다는 사실이 많은 개발 경험을 통해서 밝혀져 있다. 이를 극복하기 위한 방법으로 제기된 것이 신뢰성 성장 관리이다. 신뢰성 성장 활동은 기본적으로

반복적인 시험/재설계의 과정이다. 신뢰성 목표를 달성하기 위해 다음과 같은 다섯 단계를 반복적으로 수행한다.

- 고장 원인의 발견
- 확인한 문제를 피드백
- 확인한 문제 해결을 위한 재설계
- 하드웨어 제작
- 재설계 효과 검증

4.1.3 신뢰성 보증 계획

신뢰성 요구조건을 달성하기 위해 필요한 조직적이거나 기술적인 계획, 활동, 기술, 방법, 규칙, 요구조건, 표준 등을 규정한다. 신뢰성 보증 계획에 최소한 다음 항목들이 포함되어야 한다.

- 적용되는 표준과 지침서
- 시스템 레벨 신뢰성 요구조건
- 임무 달성을 위한 신뢰성 지표와 목표치
- 신뢰성 프로그램에서 작성되는 문서 양식
- 신뢰성 예측과 평가를 위한 방법론, 기법, 절차
- 작업, 일정, 산출물, 담당자 기록표
- 신뢰성 데이터 수집, 분석, 배포, 보고 프로세스와 절차
- 신뢰성 검토 회의와 FRB

4.2 요구조건 기능에서의 신뢰성 프로그램

특별한 신뢰성 요구조건이 명시되지 않은 경우 시제품이 성능 시험을 통과하기만 하면, 어떤 신뢰성 시험도 수행하지 않고 바로 생산으로 들어가는 것이 일반적인 상황이다. 이러한 상황을 극복하고 신뢰성을 확보하기 위해서는 신뢰성 요구조건이 명시될 필요가 있다. 신뢰성 요구조건을 포함하는 신뢰성 규격서의 주요 항목은 다음과 같다.

- 제품의 기능과 관련 있는 모든 고장에 대한 정의
- 제품의 저장, 이송, 작동, 유지보수 등 모든 환경에 대한 충분한 기술
- 신뢰도 요구조건
- 특별히 중요해서 발생 빈도를 아주 낮게

유지해야 하는 고장모드에 대한 정의

일반적으로 'one-shot' 항목들은 성공률이 유일한 신뢰성 척도인데, 우주발사체 역시 대규모의 'one-shot' 품목으로 시스템과 서브시스템 수준의 신뢰성은 고장 없이 작동할 확률을 지표로 활용한다. 보통 우주발사체에서 적용되는 신뢰성 요구조건은 다음 네 가지 신뢰성 지표로 표현된다. 네 가지 신뢰도는 서브시스템과 컴포넌트 수준, 필요할 경우에는 더 낮은 수준까지 할당된다.

1. P_{PRE} - 지정된 시간 내에 발사준비 작업을 성공적으로 준비, 완료할 확률
2. $P_{LV}(\tau_i)$ - 비행시간 τ_i 동안 발사체가 고장 없이 작동할 확률
3. $P_A(\Omega)$ - 발사체의 비행중단 시킴 없이 위성을 지정된 위치에 정확히 투입시킬 수 있는 확률
4. P_{SUF} - 발사체가 위성 투입을 달성할 수 있을 충분한 추력을 가질 확률

4.3 분석 기능에서의 신뢰성 프로그램

4.3.1 FMEA

우주발사체를 구성하는 품목의 모든 가능한 고장모드와 그 고장모드가 임무 성공에 미치는 영향을 파악하고 문서화하는 작업이다. 주요하게 다음 정보와 데이터를 확보해야 한다.

- 가능한 모든 고장모드와 임무 성공에 미치는 영향
- 각 고장모드에 대한 교정 혹은 완화 조치
- 고장모드에 대응하는 조치가 취해지지 않았을 경우의 사업에 미치는 위험

FMEA에서는 각 품목별로 기능, 고장모드, 고장원인, 고장효과, 고장감지 방법 및 증상, 심각도, 빈도, 고장확률, 고장모

드 ratio, 고장모드 치명도, 보완/교정 조치 등이 기록된다. FMEA 결과는 개발 전 단계에서 가장 심각한 고장모드를 선별해 내기 위한 우선순위를 결정하고 중요 항목 리스트와 중요 항목 통제 계획을 수립하고 업데이트하는 데 사용된다.

4.3.2 FTA

우주발사체 개발에서 FTA는 아주 심각한 결과를 초래하는 문제나 비용이 많이 드는 변경 사항 등을 검토할 때, 특정한 시스템 실패를 발생시키는 고장들의 조합을 찾는데 사용된다. FMEA와 같은 하향식 방식으로는 찾아내기 어려운 작업자의 실수, 설계에서의 결함, 심각하지 않은 실패들의 조합이나 정상적인 상태간의 상호작용 등을 고려해서 시스템 레벨에서의 고장을 규명한다. FTA 수행의 첫 단계에서는 숙련된 분석가가 문제가 되는 시스템 고장을 최상위 사건인 root로 하고 중간단계의 결합 사건으로 구성된 결합트리로 연역적인 방법을 통해 구성하고, 다음 단계로 설계, 운영, 관리 담당자와 분석가는 결합트리를 검토하고, 검토를 통해서 나타난 그 모델의 약점이나 문제점에 대한 해결책을 제안하게 된다.

4.4 설계 및 형상 기능에서의 신뢰성 프로그램

우주발사체는 복잡한 대규모 시스템으로 여러 가지 종류의 기계 및 전기전자 컴포넌트와 시스템, 소프트웨어로 구성되어 있다. 설계 및 형상 기능에서는 각 부문별로 특징적인 고장모드와 주요 원인을 판별하는 것이 중요하다.

4.4.1 기계적 고장 원인

기계적 고장은 크게 두 가지 주요 원인에 의해서 발생한다.

1. 과부하 - 파손을 발생시킨다. 하중은 장력, 압축, 전단응력 등으로 구성된다.
2. 내구성 약화 - 작용 하중이 파열을 일으킬 수 있다.

위의 두 가지 외에도 기계적 고장을 일으키는 원인들을 기술하면 다음과 같다.

1. 구동부, 연결부, 기어 등에서의 백래쉬

2. 밸브나 측정 장치 등의 잘못된 조절
3. 베어링이나 슬라이드 등과 같은 접촉부 운동부품의 끼임
4. 누출
5. 느슨한 체결
6. 과도한 진동이나 잡음

4.4.2 전기전자 고장 원인

대부분의 전기전자 컴포넌트와 시스템에 있어서 많은 신뢰성 요소가 생산 공정에서의 품질 관리에 의해서 결정된다. 따라서 전기전자 컴포넌트와 시스템 설계 담당자에게는 기술적인 영역 뿐 아니라, 생산, 품질 통제, 시험 계획, 신뢰성 공학 등의 전기전자 컴포넌트와 시스템의 신뢰성 요소에 영향을 미치는 다양한 분야에 대한 지식과 경험이 요구되고 있다. 전기전자 컴포넌트와 시스템에서 주요한 고장 메커니즘은 다음과 같다.

1. 전자 장치의 약한 본딩
2. 마모와 스트레스 등으로 인한 결함 있는 소자의 고장
3. 과부하로 인한 고장
4. 그 외 - 컴포넌트의 파라미터 특성 변화, 납땜 불량으로 인한 단락, 릴레이의 과도한 저항 값, 커넥터 접촉 불량, 허용 한계의 불일치, EMI 등

4.4.3 소프트웨어 고장 원인

스펙을 점검하고 프로그램 구조를 계획하고 스펙에 따른 설계를 평가하는 기본 작업을 주의 깊게 수행하는 것이 가장 핵심적인 소프트웨어 신뢰성 보장 방법이다. 소프트웨어 신뢰성 작업은 항상 초기 단계 여러 가능성을 최소화 하는 것과 다음 단계로 넘어가기 전에 에러를 모두 제거하는 것에 초점을 맞추어야 한다.

4.5 검증 기능에서의 신뢰성 프로그램

우주발사체의 기능과 신뢰성을 보증하기 위해서는, 우주발사체를 구성하고 있는 모든 컴포넌트와 시스템이 요구되고 있는 특성을 만족시키는 지 여부를 검증하고 입증하는 작업이 필요하다. 일반적으로 신뢰성 조직이 요구조건에 대한 최종 검증 작업을 수행하는 데, 시험계획서, 시험절차서, 시험결과서 등을 토대로 시험의 결과가 제품의 성능

과 신뢰성 요구조건을 만족시키는 지를 확인한다. 설계 규격, 시험 규격, 시험 매트릭스, 검증 매트릭스, 종합 시험평가 계획, 검증 통제 계획 등은 신뢰성 조직이 검증 업무를 수행하는 데 있어 핵심적으로 검토해야 하는 문서이다. 신뢰성 평가의 목적과 유형에 따라 품목별 시험을 구분하면, 컴포넌트 시험과 시스템 시험의 두 가지 종류로 나누어서 생각할 수 있다. 컴포넌트 시험과 시스템 시험은 시험의 목적과 시험을 통해 획득하고자 하는 정보의 종류, 내용에서 큰 차이가 있다.

컴포넌트 시험에서 신뢰성 관련하여 두 가지 심각한 문제가 발생한다. 하나는 파라미터 입력과 컴포넌트의 변이 특성 등을 포함한 실제적인 시스템 환경을 시뮬레이션하기 힘들다는 점이고, 다른 하나는 단일 컴포넌트에 대한 신뢰성 요구조건이 과도하게 높아서 개발 단계에서 그러한 신뢰도를 달성하기 위해서는 상당한 횟수의 시험을 수행해야 한다는 점이다. 따라서 컴포넌트 시험은 절대적인 신뢰도 값을 결정하고서 이를 만족시키려 하기보다는 최적의 선택을 통해 신뢰성을 향상시키는 것을 시험의 목표로 설정하는 것이 필요하다.

시스템 시험은 컴포넌트가 스펙을 만족시키느냐 여부보다는 컴포넌트가 시스템 내에서 요구되는 신뢰성을 확보하고 있는지에 집중해야 한다. 스펙은 시스템의 성능과 신뢰성 확보라는 목적을 위한 수단으로 활용되어야 한다. 시스템 시험은 컴포넌트 시험을 대체하거나 배제하지 못한다. 시스템 시험은 단지 고장이 있는 컴포넌트를 정확하게 짚어 내어서 보다 품질이 우수한 제품으로 대체하거나 수정할 수 있도록 하는 데 활용될 수 있다.

5. 결론

본 논문에서는 우주발사체의 신뢰성 프로그램을 전체 개발사업의 시스템 엔지니어링 기능에 따라 정리하고 그 인터페이스를 구체화하였다. 신뢰성공학은 대상 시스템에 따라 그 주요 강조점과 특성이 달라지며, 축적된 방대한 양의 데이터베이스를 토대로 해야만 실질적으로 의미 있는 결과를 가져올 수 있다.

한국형 우주발사체 개발은 아직 초기 단계로 신뢰성 확보에 필요한 충분한 데이터가 부족한 것

이 현실이다. 그로 인하여 더욱 더 시스템 엔지니어링 업무와의 통합 적용이 요구되고 있다. 현재 FMEA 결과를 바탕으로 중요 품목 목록을 선정하고 통제 계획을 준비하고 있다. 다음 단계로 FMEA와 FTA를 통합하는 확률적 위험도평가(PRA, Probabilistic Risk Assessment)를 적용하여 전체 시험평가와 검증 작업을 통합하고 신뢰도 예측과 평가를 수행하는 것, 그리고 그 결과를 통해 개발사업의 의사결정에 적용할 수 있는 절차를 개발하는 것이 신뢰성 연구의 추후 과제이다.

참고문헌

1. 이창호, 한동인, 다목적 실용위성 2호기 신뢰성 프로그램, KARI-SB0TN-2004-001, 2004.
2. 조미옥, 조병규, 오범석, 박정주, 조광래, "우주발사체 시스템 개발에 있어서의 SE 관리기법 적용," 2004 시스템엔지니어링 추계 심포지엄 논문집, pp. 90-94, 2004.
3. ECSS-E-10A, Space Engineering: System Engineering, 1996.
4. ECSS-Q-30A, Space Product Assurance: Dependability, 1996.
5. Walter E. Hammond, Design Methodologies for Space Transportation Systems, AIAA, 2001.
6. David K. Lloyd and Myron Lipow, Reliability: Management, Methods, and Mathematics, Prentice-Hall, 1989.
7. MIL-STD-1543B, Reliability Program Requirements for Space and Launch Vehicles, 1988.
8. Patrick D. T. O'conner, Practical Reliability Engineering, John Wiley & Sons, 1991.