

# 우주 발사체 체계신뢰도 증진과 비행안전 기술

박 찬 빈 · 한국항공우주연구원 기술경영팀, 책임연구원

\_e-mail : cbpark@kari.re.kr

이 글에서는 미국의 APOLLO 프로그램 사례를 중심으로 우주 비행체 신뢰도 증진 방안을 설명하고 체계 안전 기술은 우주 발사체 비행안전 기술에 국한하여 소개한다.

우주발사체는 수많은 부품들이 통합된 거대 복합체계로서 효율적이고 체계적인 관리를 필요로 하며, 단 한 번의 발사를 성공으로 이끌어야 하는 특성으로 신뢰도와 안전이 개발 초기부터 체계설계에 반영되어야 한다. 우주비행체의 체계 신뢰도는 주어진 목표시간에 임무목표를 성공적으로 달성할 수 있는 확률로, 미국의 아폴로 계획에서는 설계, 제작 및 시험의 전 과정을 통해 신뢰도를 향상시키기 위한 노력과 이를 위한 전용 프로그램을 개발, 적용하였다. 체계안전은 체계운용 중에 발생할 수 있는 사고 피해로부터 장비와 사람을 보호하는 것으로 비행 안전에 대한 통제시스템과 안전 위험도의 계산과 공적 안전 위험도에 대해 기술하였다. 이러한 우주 발사체 체계 신뢰도 증진 방안

및 비행 안전에 대한 검토는 KSLV-I 사업에도 적용되었다.

1957년 10월 구 소련은 인류 사상 최초로 소형 인공 위성을 탑재한 스푸트니크(SPUTNIK) 발사체(SL-1)를 성공적으로 발사하여 위성을 지구 궤도에 진입시

켰다. 그러나 이것은 동서 냉전 속에서 미소간 우주 경쟁의 계기가 되었으며, 미국은 1955년부터 미 해군 연구소(NRL)에서 이미 3단 벵가드(VANGUARD) 발사체를 이용하여 민수 목적의 국제 지구 물리 관측년(IGY; Inter-

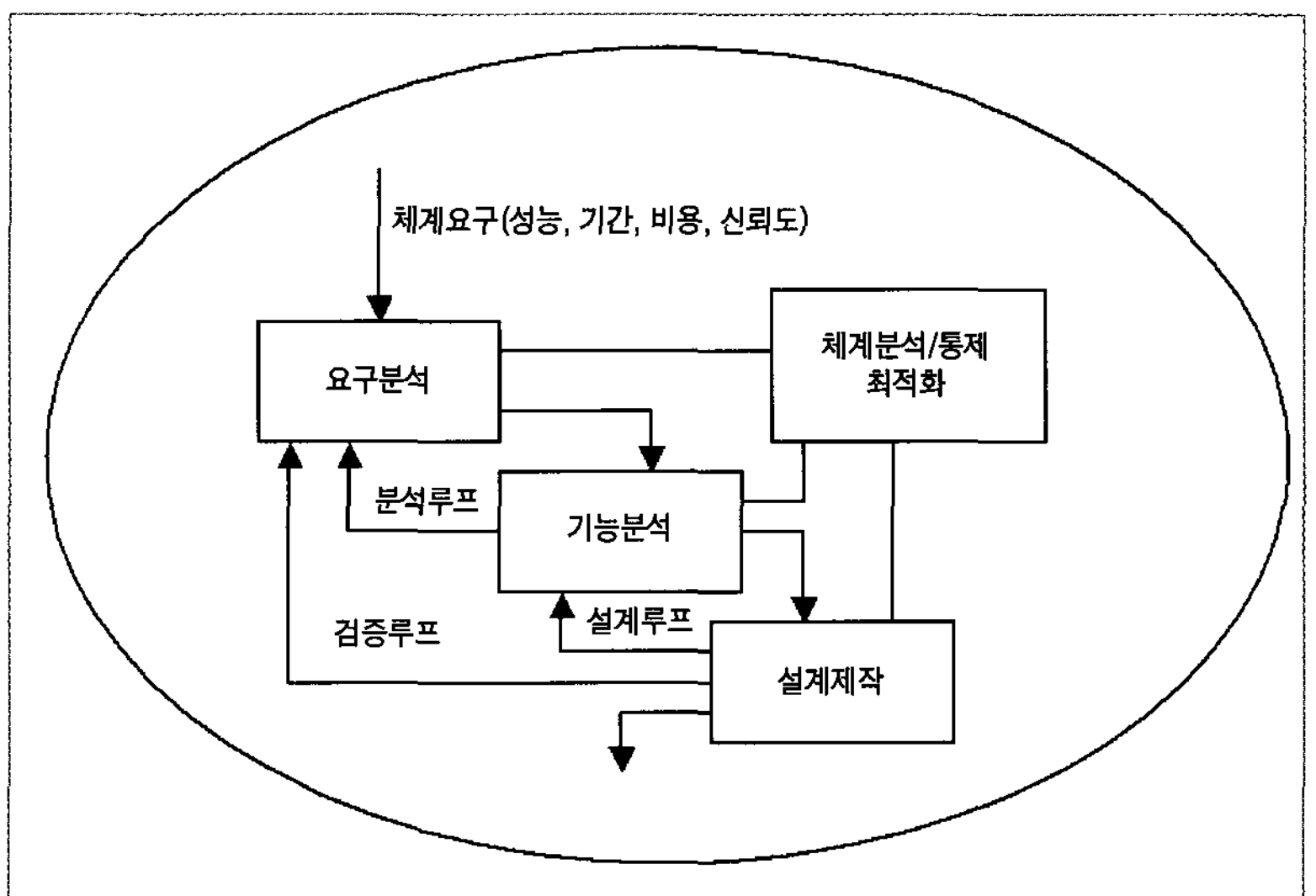


그림 1 체계공학 과정(SEP)

national Geophysical Year) 기념용 인공위성 발사체를 개발 중에 있었다. 미국 정부는 구 소련의 스푸트니크의 위성 발사 성공으로 민수용으로 이미 개발 시험 중에 있었던 벨가드 발사체를 서둘러 발사하였으나 연속 두 번 실패 하였으며, 1957년 12월에야 처음으로 미국은 소형 인공위성 발사에 성공하게 되었다. 그러나 이와 같은 위성 발사 실패는 미국 과학 기술계에 충격을 주었을 뿐만 아니라 위성 발사체의 기존 개발 관리 방법에 대한 자성의 목소리가 높아지게 되었다.

실제로 우주 발사체는 여러 분야의 과학 기술로 개발된 20만 개 이상의 부품으로 통합된 거대 복합체계로서 효율적이고 체계적인 개발 관리를 요구하고 있다. 발사체는 유도탄과 달리 한 개의 생산(one of a kind)과 단 한 번의 허용된 발사(높은 신뢰도 요구)로 고가의 위성체를 안전하게 지구 궤도에 진입시켜야 한다. 따라서 발사체의 이러한 특수성 때문에 발사체는 신뢰도와 안전을 반드시 고려하여 개발 초기부터 체계설계에 반영하여야 한다.

미국은 현재 거대 복합체계의 체계적인 개발 관리 목적으로 체계공학 관리 기법을 활용하고 있으며, 체계공학관리는 체계개발 전순기(요구분석 단계, 체계설계 및 제작단계, 체계검증 단계 및 체계운용 단계)를 통합하여 전순기를 동시 관리하되 기술적인 절충과 통제는 체계공학과정(SEP;

System Engineering Process)을 통하여 관리한다. 체계공학과정은 그림 1에서 체계요구 분석, 체계설계 제작, 체계검증의 세 개 루프로 구성되어 있으며, 발사체 개발의 경우 요구분석 루프를 통하여 발사체 임무를 분석하여 체계기능을 식별하고, 식별된 체계기능은 체계 하부 기능으로 PBS(Product Breakdown Structure)로 분할한다. 설계루프에서는 PBS로 분할된 하부기능을 HW와 SW로 설계 제작하고, 검증 루프에서는 하부 구조로 제작된 HW와 SW를 다시 체계로 종합하고, 종합된 체계 성능이 체계요구를 충족하는지 충분한 환경 시험과 다양한 M&S로 검증하도록 되어 있다. 체계공학과정 기능의 하나인 체계분석/통제/평가 기능은 체계개발 전순기의 체계공학과정의 설계 제작 과정에서 발생할 수 있는 복합적인 HW/SW 항목 상호간에 충돌되는 기술적 문제를 체계 관점에서 분석하고 절충한다. 미 국방부는 1969년에 체계공학과정을 MIL-STD-499로 군사 표준화하고 핵 잠수함과 유도탄 개발에 적용하였다.

우주 발사체 체계기술의 핵심은 체계공학과정 기술이며, 체계공학과정의 목표는 높은 신뢰도를 보유한 발사체를 개발하여 안전하게 위성을 지구 궤도에 진입하도록 하는 것이다. 체계목표를 체계적으로 달성하기 위하여 발사체의 개념 정립 단계부터 체계신뢰도와 체계안전이 고려되어

체계설계 되어야 한다.

이 글에서는 미국의 APOLLO 프로그램 사례 중심으로 우주 비행체 신뢰도 증진 방안을 설명하고 체계 안전 기술은 우주 발사체 비행안전 기술에 국한하여 기술한다.

체계 신뢰도  $R(T)$ 는 주어진 임무 운용기간  $T$ 에 목표된 체계임무를 성공적으로 달성할 수 있는 확률로 정의한다. 수학적으로 체계고장 확률을 프와송 분포 모델로 표시할 때, 체계 신뢰도는 주어진 임무 운용 기간( $T$ )에 체계고장이 없는 경우의 확률  $R(T) = \text{EXP}(-Fr \times T)$ 로 표시되며 여기서  $Fr$ 은 체계 운용 기간의 고장률로 표시된다. 따라서 신뢰도는 고장률과 운용시간의 함수로 표시되며 체계 운용 시간과 고장률이 클 경우는 당연히 신뢰도가 감소된다. 또한 신뢰도가 0.9인 장비를 두 개 병렬로 중복 운용할 때의 신뢰도는 0.99가 되어 장비를 하나 사용하였을 경우 보다 신뢰도가 크게 향상 된다.

CROSSLINK(WINTER 2003) 자료에 의하면 1957부터 1999년까지 세계 우주 발사체의 체계신뢰도는 91.9%이며, 4,378회 발사에서 390회가 임무 목표 달성에 실패하였다. 더욱이 발사체를 민수 주도로 처음 개발하여 발사할 경우 임무 성공 확률은 67.7%에 불과하다.

1961년 4월 구 소련은 세계 최초로 유인 인공위성 발사에 성공함으로써 미국을 다시 한 번 놀라게 하였다. 미국 케네디 대통령

은 1961년 5월 미의회 특별 연설에서 “LANDING A MAN ON THE MOON AND RETURNING HIM SAFELY TO THE EARTH WITHIN THE DECADE OF 1960s”라는 국가 사업 목표를 발표하였으며, 이에 따라 NASA는 APOLLO 계획을 수립하여 국가과제로 추진하게 되었다. 이 APOLLO 계획은 1969년 7월에 APOLLO-11로 세계 최초로 미국인을 달에 착륙시키고 지구에 안전하게 귀환함으로써 그 체계 목표를 달성하였다. 당시 APOLLO우주선 사업 책임자인 LOW 박사는 그의 기고문에서 APOLLO 사업의 성공은 전적으로 비행체의 높은 신뢰도에 기인하였다고 술회하였다.

LOW 박사는 성공적인 APOLLO 사업에 적용하였던 신뢰도 증진 기술에 대하여 다음 몇 가지로 요약하였다. 첫째로 설계 측면에서 되도록 단순 설계와 중복 설계(redundancy design) 기술을 도입하여 장비 설계 신뢰도를 증진시켰으며, 둘째로 거대 복합 체계인 APOLLO 사업 진행 과정에서 흔히 발생하는 HW와 SW 설계 변경에 대한 효과적 통제로 체계 신뢰도와 체계설계의 효율적 관리를 도모하였다. 셋째로 충분한 시험으로 비행체 성능을 입증하되, 먼저 설계 제작 단계에서 성능 시험으로(DT; Development Test) 비행체 설계 성능을 입증하였으며, 또한 설계의 비행 환경 인증 단계

(QT; Qualification Test)에서 비행체의 비행환경 부하(load)를 예측하고, 예측된 환경을 지상에서 모사하여 모사된 환경으로 지상에서 충분한 시험을 수행함으로써 비행체의 설계 실용성을 입증하였다. 실용성이 입증된 설계로 제작된 발사용 비행체 장비/부품을 모두 검수하여 총 조립하되, 수락검사 단계(AT; Acceptance Test)에서 모든 장비에 대하여 환경 수락시험(EAT; Environment Acceptance Test) 강화로 비행 중에 있을 장비 결함을 지상 시험에서 미리 발견하도록 하였다. 넷째로 시험 기간 중에 발생하는 시험 불일치 항목에 대하여 철저한 원인 분석과 대책을 강구하되 관련 기술자(체계설계 종합자, 장비 설계 제작자, 시험 담당자)간에 정직하게 문제가 제기되고 투명하게 토의함으로써 최적으로 문제가 해결하도록 유도하였다. 또한 APOLLO 사업 관련 전 연구원은 APOLLO 사업을 국가 사업으로 긴급성과 중요도를 인식하고 스스로 한 팀이 되어 일하는 단체정신(team spirit; 애국정신)이 APOLLO 사업을 성공하게 한 원동력이 되었다고 LOW 박사는 술회하였다.

여기서 환경수락시험은 APOLLO 비행체의 높은 신뢰도 확보의 핵심 수단으로서 비행용으로 제작하여 조립된 장비의 제작 조립 결함(workmanship faults)을 시험을 통하여 발견하는 장비수락 보증시험의 일환이다. 우주비행용으로

로 제작되고 조립되는 모든 부품(parts), 모든 기능품(component), 모든 부분체(subsystems), 조합체(system)를 시험 대상으로 전수 검사하였으며, 제품 보증 활동에 소요되는 총비용은 프로그램 전체 비용의 25%가 되었다. APOLLO 전용 환경 수락시험은 진동 수락 시험과 열주기 수락시험으로 구성되어 있으며, 환경 수락시험 레벨과 주기는 그 동안 유사 비행체 시험으로 확보된 데이터베이스와 경험적 요소로 결정하였다.

열주기 수락 시험과 진동주기 수락시험 통계에 의하면 수락 시험 중 고장률이 각각 10.3%와 5.0%로 열주기 수락 시험이 진동 시험에 비하여 고장률이 약 2배로 관찰된다. 이것은 기계와 전자 요소로 제작 조립된 장비가 기계적 진동보다는 열 주기 환경에 더 취약함을 나타낸다. 만약 APOLLO 수락 시험에서 환경 수락 시험을 철저히 수행하지 않았으면 인류 최초의 미국 우주인의 지구 귀환은 장담할 수 없었을 것이다.

또한 환경 수락시험 고장 내용을 살펴보면 장비 조립과정에서 발생할 수 있는 기능공 일솜씨(workmanship)에 의한 고장이 설계 결함에 의한 고장의 약 2배가 되어 일솜씨에 의한 고장이 환경 수락시험 전체 고장의 66%나 됨을 알 수 있다. 따라서 우주 비행체에 사용되는 모든 부품은 높은 신뢰도 기준으로 선별(screen)되어야 하며 또한 선별된 부품으

로 장비를 제작하고 비행체를 조립하는 모든 과정의 일순씨를 체계적으로 관리하여야 한다.

NASA는 이를 위하여 APOLLO 전용 환경 수락시험 프로그램을 개발하였으며, 이러한 노력으로 NASA는 APOLLO 임무를 높은 신뢰도를 가지고 달성할 수 있었다. 환경 수락시험의 설계 고장에 대하여는 부품 수를 줄이는 단순 설계 원칙을 고수하고 체계고장 위험이 큰 장비에 대하여 특별히 중복 설계 개념을 도입하여 설계에 의한 고장을 최소화하였다. NASA는 또한 환경 수락시험 중에 발견된 장비 고장에 대하여 고장 위치를 쉽게 찾고 쉽게 고칠 수 있도록 장비 설계에 반영하였으며 고치는 시간을 단축함으로써 개발 비용을 절감하도록 하였다.

체계안전은 체계운용 중에 발생할 수 있는 사고 피해로부터 장비와 사람을 보호하는 것으로서 1962년 미 공군은 대륙간 탄도탄 MINUTEMAN 사업에 최초로 체계안전 프로그램을 적용하였으며 미 국방성은 1969년에 체계안전 프로그램을 MIL-STD-882로 표준화하였다. 같은 해에 미국 NASA는 우주 발사체 사업에 체계안전 프로그램을 포함하여 관리하기 시작하였다.

우주 발사 체계는 발사체와 위성체, 발사장, 발사 지원 지상장비/시설 그리고 운용 인력과 운용문서 등으로 구성되어 있다. 우주발사 안전 목표는 우주발사 체계 각 구성 요소에 대하여 사고

위험요소(HAZARDS)를 미리 식별하고 식별된 각 위험 요소에 대하여 안전 위험도(Risk = 고장 확률 x 피해결과)를 분석하고 통제하여 발사체 발사와 비행 중에 발생할 수 있는 인명 손상과 재산 피해를 수용 가능한 수준으로 안전을 확보하는 것이다.

우주발사는 발사체의 발사준비 단계와 발사 이륙의 발사단계 그리고 임무비행으로 인공위성의 지구 궤도 진입의 비행단계로 크게 구분되어 있으며, 우주발사 체계안전은 우주발사 단계별로 분석되고 통제되어야 한다. 그러나 이 글에서는 우주발사 체계안전 가운데서 발사체 비행 단계 안전에 국한하기로 한다.

비행 중에 있는 발사체(LV; Launch Vehicle)의 안전 통제는 첫째로 비행 중에 있는 LV의 비행 상태를 실시간으로 모니터링하고, 둘째로 LV 비행궤적이 안전 구역 내에 있는지 확인하고, 셋째로 LV의 비행궤적이 안전 구역을 벗어날 경우 비행종료 시스템(FTS)을 이용하여 강제로 LV를 비행종료(FT) 시킴으로 안전 목표를 달성하고 예상되는 피해를 피할 수 있다.

비행안전 통제 시스템에는 LV의 비행상태를 실시간으로 모니터링하는 장비로 레이더 추적장비와 원격 측정장비, 전자 광학 추적장비 등이 있으며 이들 장비를 이용하여 실시간으로 LV의 비행위치와 비행 속도를 추적하고 동시에 LV와 LV 부속물(분리된 추진 단이나 페어링, 강제로 비행중단 되

었을 때 잔해물 등)이 지상에 충돌하는 위치(IIP; Instantaneous Impact Point)를 컴퓨터 모니터 상에 표시된 지도상에 시현한다. 실시간으로 예측된 LV와 LV 부속물의 IIP 궤적이 안전 저지선인 ILL(Impact Limit Line) 범위를 초과할 때 FTS를 이용하여 LV 비행을 강제 중단 시킴으로 예상되는 피해를 보호할 수 있게 된다.

비행종료 시스템은 LV 탑재 장비와 지상장비로 구성되어 있으며, 탑재장비로는 수신 안테나, 수신기, 복호기, 안전 및 장전장치, 화약 등이며, 지상장비로는 인코더, 송신기, 송신 안테나 등으로 구성되어 있다. 신뢰도를 높이기 위하여 FTS 주요 장비는 중복 설계되어 있으며 신뢰도는 신뢰도 수준 0.95에서 0.999 수준이다. 전자 장비 신뢰도는 고장을 분석과 계산 그리고 시험으로 입증되며 신뢰도 계산의 경우 MIL HAND BOOK 217을 이용하여 예측하며 임무 운용시간(T)은 예정된 임무비행 시간의 1.5 배 외에 발사 준비기간의 시험시간 그리고 추가로 30분을 더 추가하여 계산하고 계산된 임무 시간으로 신뢰도를 계산한다. 미 공군 통계에 의하면 1988~1999년 간 공군 발사장에서 발사된 발사체 602 발 발사에서 비행 안전을 위하여 실제로 FTS를 이용한 비행중단 명령은 22회로 약 3.6 %이다.

우주발사 임무성공을 위한 종래의 모든 위험도를 제거(risk avoidance)하는 방식의 안전

요구는 발사비용 측면에서 특히 상용 우주발사 비용을 사기업이 부담하기는 어려울 것으로 판단된다. 따라서 미국정부는 상용 우주발사에 대하여 정부가 수락 가능한 비행 위험도를 정량적으로 표준화할 필요성을 제기하였다.

Ec는 공적 안전 위험도로서 LV 비행임무 수행 중에 발생할 수 있는 모든 위험도의 총합으로 정의된다. 미국 FAA는 상용 우주발사 면허 기준으로 발사 임무당 Ec(Expected Casualty)가  $30 \times 10E-6$ 를 넘지 않도록 하였다. 이 수치는 미 3-군 우주발사 시험 주관기관으로 지정받은 미 공군 관할 미국 내 발사장에서 수용 가능한 비행안전 위험도 수치와 일치한다. 상기 Ec의  $30 \times 10E-6$ 는 미국 RCC(Range Commander Council) 표준치와 일치하며, RCC는 미국방성(DOD) 소속 모든 시험장에 적용하도록 추천하였다. LV 임무당 Ec 값을 항공기 사고 사례와 비교하여 보자. 1982년부터 1998년까지 미국 민간 항공기 사고에 의한 사상자 통계에 의하면 1억 3,100만 회 항공기 출발에서 2,868명 사상자 발생하였으며 이것은 항공기 1회 출발에서  $22 \times E-6$ 명 사상자 발생한 것으로 Ec의  $30 \times 10E-6$  값과 유사함을 알 수 있다.

비행 안전 위험도 계산에는 정상비행 경우와 고장에 의한 비정상 비행으로 FT(비행중단) 조치가 취해진 경우의 두 가지를 고려할 수 있다. 2단 추진 LV의 정상

비행 경우 위험도 대상 이벤트로 1단 분리, 페어링 분리, 그리고 2단 낙하 3-가지 이벤트를 고려할 수 있으며 비행 중 고장에 의한 비정상 비행 경우는 비행 중 FT에 의한 LV 파편 총 개수가 총 이벤트 개수가 될 것이다.

고장에 의한 LV의 비정상 비행 경우 비행안전 위험도 계산절차는 다음과 같다. 첫째로 비행 중 특정 시간에 발생할 수 있는 LV 고장 모드와 그의 고장률을 정의하고 FT에 의한 LV의 분산 역학을 모델하되 바람, 폭발에 의한 LV 부속물 속도, 공기 저항의 탄도 계수 등을 충분히 고려되어야 한다. 둘째로 LV의 FT에 의한 LV의 부속물이 지상에 충돌하는 확률을 추정하고 그 부속물로 인한 인명 손상 면적을 모델링 한다. 셋째로 충돌 지역의 인구 밀도 정보를 활용하여 부속물의 Ec를 계산한다. 넷째로 특정 고장모드의 LV 모든 부속물에 대한 Ec를 계산하여 합산한다. 다섯째로 비행 중에 발생할 수 있는 다른 고장 모드 전부에 대하여 같은 방법으로 Ec를 계산하고 최종 합산 한다.

궁극적으로 Ec는 비행 중 LV 고장 확률( $1 - \text{신뢰도}$ )과 LV의 임무 비행 계획에 크게 좌우된다. 만약 임무 비행 계획을 LV가 무인도 상공으로만 비행할 수 있게 설계한다면 Ec 값은 이론적으로 제로가 된다.

우주 발사체 체계기술의 목표는 체계 신뢰도를 만족하는 발사

체를 체계적으로 설계 제작하고 시험 평가하여 탑재 위성을 정해진 지구 궤도에 안전하게 진입하도록 하는 것이다. 성공적인 APOLLO 신뢰도 증진 프로그램처럼 비행환경 시험으로 실용성이 이미 입증된 발사체의 모든 부품과 장비에 대하여 수락시험 단계에서 다시 한번 진동과 열주기로 구성된 환경수락시험(EAT)을 강화함으로써 발사체 제작 조립 과정에서 발생할 수 있는 일손씨에 의한 고장을 최소화하여 우주 발사체 발사 신뢰도를 크게 증진시킬 수 있다. 발사체 임무비행 궤도 설계와 비행 안전구역(ILL) 설정은 체계 신뢰도와 비행 안전 위험도의 최적 절충에 의하여 결정되며 비행 안전 위험도(Ec)는 미국 FAA의 상용우주 발사 면허 기준 수치인  $30 \times 10 E-6$ 를 넘지 않도록 설계한다.

금년도 2008년 12월에 발사 예정되어 있는 한국형 위성 발사체 KSLV-I은 우리 손으로 만든 위성을 우리 기술자가 설계한 발사체에 탑재하여 우리나라 발사장에서 우리 손으로 최초로 발사하는 데 의의가 있다. 우리나라에서 최초로 발사되는 KSLV-I의 발사 신뢰도를 증진하기 위하여 우리나라는 KSLV-I 고유 환경 수락시험 프로그램을 개발하였고 철저한 수락 시험을 진행 중인 것으로 알고 있으며 KSLV-I 비행궤도 설계와 ILL 구역 설정도 FAA 상용우주 발사 면허 기준치인 Ec를 충족하도록 설계하였을 것으로 판단된다.