확률적 위험분석을 이용한 우주발사체 시스템의 신뢰도 계산 기법

Evaluation of Launch Vehicle Reliability using Probabilistic Risk Assessment

조상연*, 신명호, 김용욱, 오승협 (한국항공우주연구원)

1. 서 론

미국의 우주개발과 함께 고안된 확률적 위험 분석(Probabilistic Risk Assessment; PRA)은 이후 발사체 분야보다 원자력 발전 사업 등에서 더 활발히 적용되어왔으나 챌린저호의 사고이후 다시 미 항공우주국(NASA)의 주목을 받아 현재에 이른 기법이다. 확률적 위험 분석은 위험요소를 인식하고 이를 미션 단계와 운용 시간에 따라 나눈 뒤 최종 상태를 유추하고 이 이벤트들의 발생 가능성을 계산하는 순서로 분석이 이루어진다. 본 논문에서는 현재 항공우주연구연이 개발하고 있는 소형위성발사체(KSLV-I)에서의 확률적 위험 분석을 적용한 신뢰도 분석의 가능성을 확인하고 한다.

2. 역사적 배경

확률적 위험 분석은 복잡한 시스템에서 그 안전성과 성능을 향상시키는데 유용한 분석 기법이다. 고장목 분석(Fault Tree Analysis; FTA)등을 이용한 위험도나 신뢰도의 정량적 분석 수행 방법은 1960년대의 미국 우주 계획이나 미사일 개발 계획으로부터 시작되었다. 하지만, 아폴로 계획의 초기에 우주인을 성공적으로 달에 보냈다가 안전하게 지구로 귀환시키는 확률을 계산한 결과, 그 값이 과도하게 낮게 나타났고 이 때문에 NASA에서는 1986년 챌린저호의 사고 전까지 위험도나 신뢰도의 정량적인 분석보다는 고장모드 및 영향분석(Failure Modes and effects analysis; FMEA)와 같은 정성적인 분석에 더 의존하게 되었다. 반면, 원자력 발전 산업에서는 PRA를 받아들여서 안전 분석을 수행하는 것을 기본으로 삼았다. 수십 년간의 경험을 통해 점차 분석 방법이 향상되고 그 결과의 신뢰성이 높아지게 되었으며 이에 따라 석유화학이나 해상 구조물, 방위 사업 등에서도 이 기법이 적용되게 되었다. 챌린저 호의 사고가 발생하였을 때, PRA는 안전 분석을 위한 유용한 방법으로 다시 NASA에서 적용되게 되었다. 이 기법의 논리적, 체계적 접근 방법은 가장 경험이 많은 안전 전문가들도 빠뜨릴 수 있었던 설계나 운용상의 약점들을 찾아낼 수 있게 해주었다.

1986년 10월 29일, 미 하원 과학 기술위원회의 "챌린저 사고 조사위원회"에서는 우주 왕복선 부품에 대한 고장의 확률을 계산할 방법이 없이는 NASA가 가장 중요한 셔틀 시스템에 최대한 효율적으로 자원을 집중하였음을 확인할 수 없다고 선언하였다.

1988년 1월 Slay 위원회에서는 "챌린저 이후 우주 왕복선 위험 분석과 관리"라는 제목의 보고서에서 PRA 기법을 가능한 개발 초기부터 적용할 것을 제안하였다. 또한, 우주 발사체 시스템의 고장, 부적합, 비행 시험 결과와 관련 분석 등의 database를 체계적으로 확장하여 PRA와 경향 분석 그리고 신뢰성, 안전과 관련된 다른 정량적 분석들의 수행에 적용할 것을 제안 하였다. 이러한 Slay 위원회의 지적에 따라 NASA는 PRA를 수행하기 시작하였고 우주왕복선 주엔진(SSME) 프로그램 등에 적용되었다. 이어서 1996년에는 자체적인 PRA tool을 개발하여 우주왕복선의 위험 분석 등에 적용하게 되었다.[1]

3. PRA의 구성

PRA는 다음의 흐름을 따라 수행된다.

① 문제 발생 요인 확인

시스템에 문제를 일으키는 요인을 확인하는 것은 분석되는 시스템의 중요 기능에 대한 명백한 이해가 요구된다. 정상적인 기능에서 벗어나는 모든 것들은 초기 이벤트(initial events; IE)로 고려되며 이러한 초기 이벤트들은 결국 파국적(catastrophic) 결과로 이어질 가능성을 가진다. 그러므로 PRA의 초기 업무는 시스템에서 고장을 일으킬만한 모든 것들을 체계적으로 인식해내는 것이다. 이것은 시스템에 대한 상하관계를 구조적이거나 기능적으로 분해함으로써 이루어지며 이러한 작업은 Master logic diagram (MLD)라는 형식으로 나타내게 된다. 초기 이벤트 인식은 미션과 시스템의 분석, 사전 안전 분석(Preliminary Hazard Analysis; PHA)이나 FMEA와 같은 신뢰성 활동의 결과를 바탕으로 얻어질 수도 있다.

② 문제 발생 시점의 확인

위의 단계에서 시스템에 문제가 일어날 수 있는 모든 이벤트들을 인식하였다고 해도 그것들은 미션 단계(mission phase)중의 특정 시간대에서 어느 시점에라도 일어날 수 있는 것들이다. 모든 초기 이벤트들이 항상 일어나는 것이 아니라는 것을 가정할 때, 특정 이벤트가 어느 시점에 발생하는 가를 인식하는 것이 중요하게 된다. 또한 한 미션 단계 동안에 이루어지는 초기 이벤트의 영향이 다른 미션 구간에서는 달라질 수 있다. 이러한 문제는 미션 단계와 운용 시간 구간(Operational time intervals; OTI)을 설정함으로써 해결할 수 있다. OTI는 낮은 수준의 미션 단계라고 보면 된다. 각각의 초기 이벤트는 하나 혹은 여러 개의 미션 단계 내에서 하나 혹은 여러 개의 OTI와 연결이 가능하다. 이러한 미션 단계들은 발사체의 준비, 발사, 비행 단계처럼 연속적으로 나타날 수도 있지만 우주정거장의 예(도킹 단계, 외기 행동 단계, 정상 운용 단계, 미중력 단계 등)에서 볼 수 있듯이 불연속적일 수도 있다. [2]

③ 최종 단계에서의 결과 확인

분석자들이 관심 있는 최종 단계(End state)의 결과는 일반적으로 개발자가 피하고 싶은 것들로 이루어진다. 모든 초기 이벤트는 하나 이상의 바람직하지 않은 최종 단계로 이르게 된다. 만약 초기 이벤트가 어떠한 이유에서든 관심 있는 결과로 흘러가지 않는다면 해당 이벤트는 PRA에 적합지 않은 것이 된다. 관심 있는 최종 단계의 발생 가능성은 위험 분석에 의한 의사 결정에서 가장 중요한 변수중 하나가 된다. 이것은 설계의 최적화나 업그레이드 그리고 공정의 관리를 더욱 효율적으로 할 수 있게 도와줄 수 있다.

④ 초기 이벤트에서 최종 단계로의 흐름 확인

PRA에서 가장 중요한 과정은 초기 이벤트가 어떻게 최종 단계로 진행하는 가를 인식하는 것이다. 어떤 초기 이벤트는 발생 즉시 최종 단계에 도달할 수 있다. 그러나 대부분의 경우, 설계자들은 초기 이벤트가 진행하여 최종단계로 가지 않도록 많은 안전장치나 운용 교범 같은 것을 두게 된다. 만약 이러한 대응이 실패로 돌아간다면 초기 이벤트는 바람직하지 않은 최종 단계로 가게 된다. 이렇게 초기 이벤트에서 최종 단계로 가는 진행흐름을 시나리오라고 부른다. 이러한 흐름을 나타내는 도표를 ESD (event sequence diagram)라 하는데 ESD는 시나리오를 도식적으로 나타낸 것이라고 볼 수 있다. 초기 이벤트에 대한 시스템의 반응은 피벗 이벤트(pivotal event; PE)로 나타낼 수 있으며 해당 PE들의 작동 실패가 초기 이벤트를 최종 단계로 진행 시키게 된다.

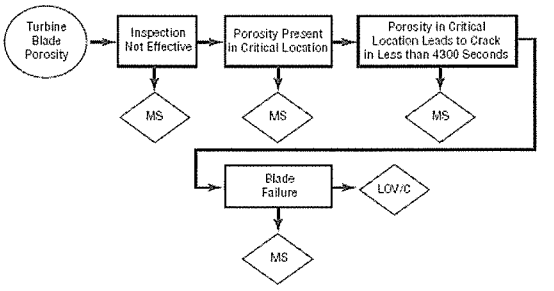

그림 1 Event Sequence Diagram의 예

위의 그림 1은 항공기 엔진에서 사용된 ESD의 예로 이중 원으로 나타낸 "Turbine blade porosity"가 IE이며 사각형으로 구성된 것들이 PE, LOV/C가 최종단계가 된다. [3]

⑤ 이벤트들의 발생 가능성 정량화

상기의 작업들은 위험 모델의 정성적 측면에 대하여 분석한 결과이다. 여기에 정량적 분석을 포함한 것이 확률적 위험 분석이 된다. ESD상의 모든 이벤트들은 발생 확률을 가지고 있거나 fault tree를 이용한 분석을 통해 이 값을 계산해 내어야 한다. 이때 fault tree에서 기본 이벤트 (basic event)들의 고장율은 기존의 시험 결과, 신뢰성 database 등에 Baysian 기법을 적용하여 구하게 된다. Boolean 연산을 이용하여 minimal cut set을 구하고 top event의 발생 가능성을 계산하는 것은 여타의 FTA와 같다. 최종 단계의 발생 가능성은 각각의 최종단계로 가는 모든 위험 시나리오를 종합하여 Event tree 분석으로부터 계산해낸다.

또한 입력 data의 불확실성(uncertainty)을 설명하기 위하여 Monte Carlo simulation과 같은 불확실성 경계 분석을 수행하여야 한다.

아래의 그림 2는 이상과 같은 PRA의 흐름을 정리한 도식이다.

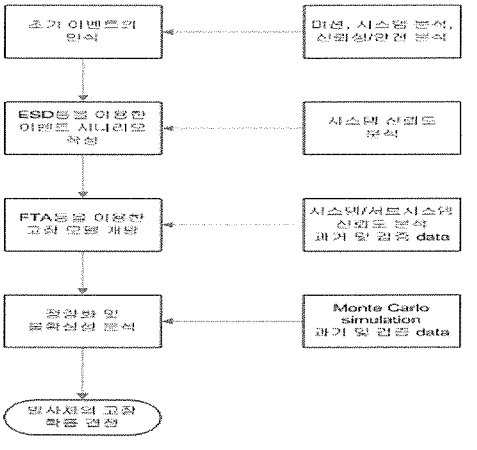

그림 2 PRA의 흐름

4. KSLV-I에의 적용 가능성

위에서 언급한 PRA 기법을 현재 항공우주연구원에서 개발 중인 소형위성발사체(KSLV-I)의 2단에 적용을 시도해 보았다. KSLV-I의 2단부는 추진기관인 킥모터(Kick motor; KM)를 비롯하여 구조체, 추력 벡터 제어 시스템 (Thrust vector control system; TVC), 비행 종단 시스템 (Flight termination system; FTS), 관성 항법 시스템 (Inertial navigation system; INS) 및 RCS(Recative Control System) 등의 복잡한 서브시스템으로 구성되어 있다. 이중 킥모터의 경우, 그 아래를 추진제와 케이스, 노즐과 점화기 등의 하부 유닛들로 나눌 수 있다. 이러한 유닛 수준의 하드웨어에 대하여 수행된 FMEA와 부적합 보고(Nonconformance Report; NCR)에 의한 고장 모드들을 초기 이벤트로 잡게 된다. 아래의 예는 킥모터의 추진제에 대한 초기 이벤트 들로 이중 "연소 불안정"라는 초기 이벤트에 대한 예를 이용하여 PRA의 적용 가능성을 확인하고자 한다.

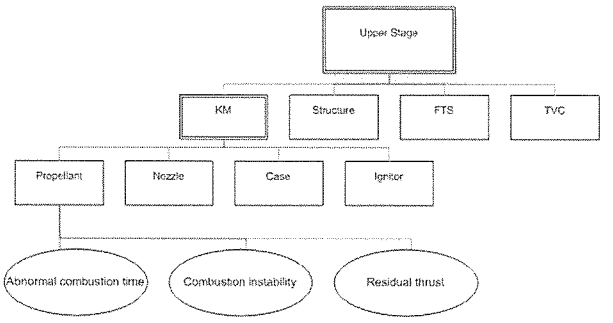

그림 3 Master logic diagram

위 초기 이벤트의 발생 시점을 정의하기 위해 시스템의 미션 단계를 정의하면 크게 준비 단계, 발사대기 단계, 그리고 발사 후로 나뉠 수 있다. 이중 준비 단계는 시스템의 이송, 조립 등의 포함된 단계이다. 발사대기 단계와 발사 후단계는 조금 더 자세히 나눌 수 있으며 이를 OTI로 아래와 같이 나눌 수 있다.

① 발사대기 단계

시스템의 정상 운영 상태 점검 - 광학 정렬 - 추진제 충진 - 탑재기기 활성화 - 카운트다운 - 1단 엔진 점화 - 1단 엔진 추력 상승

② 발사 후

이륙 - 가속비행 중 킥턴 - 가속비행 중 중력 턴 - 1단 엔진 종료모드 진입 - 페어링 분리 - 1단 엔진 종료 - 단분리 - 역추진 고체모터 점화 - 2단 무추력 비행 및 자세제어 - 2단 킥모터 점화 - 2단 가속 비행 및 자세제어 - 2단 킥모터 연소종료 - 2단 무추력 비행 및 자세제어 - 위성분리 - 충돌회피기동(CCAM) [4]

여기서 "연소 불안정"이라는 초기 이벤트는 발사 후 단계의 2단 킥모터 점화에서 2단 킥모터 연소종료 사이에 위치하게 된다.

최종 이벤트는 발사체 손실(Loss of vehicle; LOV)과 미션 성공(Mission success; MS)을 들 수 있을 것이다. 이제 상기의 초기 이벤트중 하나에 대하여 간단한 ESD(Event sequence diagram)를 작성하면 다음과 같다.

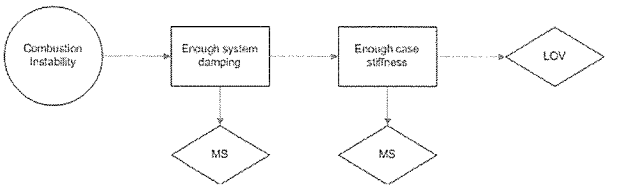

그림 4 Event sequence diagram의 작성 예

여기서 만들어진 PE들은 "충분한 시스템 댐핑이 존재할 경우"와 "case의 강성이 충분할 경우"로 예를 들었다. 이 경우에는 ESD가 단순하게 작성되어 LOV로의 시나리오가 하나만 존재하지만 실제의 경우는 여러 개의 시나리오가 나타날 수 있다.

다음으로 수행할 작업은 위 ESD를 정량화 하는 작업이다. 위에서 언급된 초기 이벤트와 피벗 이벤트들의 발생 가능성을 계산하는 것이다. 위의 예에서 "연소 불안정"현상은 하나의 기본 이벤트이므로 따로 FTA를 수행하지 않고 해당 고장율을 과거의 data에서 구해야 한다. 각 PE들에 대하여는 FTA를 수행하거나 시험을 통해 얻어진 결과를 이용하여 고장 분포 함수를 구한다. 고장 분포 함수로 가장 흔하게 이용되는 모델은 binominal, 지수, Weibull, Lognormal, Normal 분포 등이며 그 선택은 해당 data의 특성을 고려하여 가장 적절한 것으로 이루어져야 한다. 이렇게 구해진 이벤트 발생 확률에 대하여 최종 단계의 발생 가능성을 구하고 불확실성 분석(uncertainty analysis)를 수행하여 신뢰 수준을 확인한다.

최종적으로는 이렇게 계산된 값들에 대하여 중요도 분석이나 민감도 분석 등을 수행하여 시나리오상의 주된 위험 기여 항목을 확인하고 업데이트에 따른 변화를 예측하게 된다.

5. 결 론

이상과 같이 PRA 기법의 역사와 내용, 수행 방법 등을 살펴보고 우주 발사체의 신뢰도 분석에 적용 가능성을 살펴보았다. KSLV-I에 대한 현재까지의 진행 수준은 적용 타당성을 확인하기 위하여 전체 시스템에

대한 정성적 분석이 이루어지는 단계이며 추후 정량적 분석이 이루어져 위험 요소들을 관리하고 decision making에 기여할 수 있을 것으로 기대된다.

6. 참고 문헌

[1] Probabilistic risk assessment-procedures guide for NASA managers and practitioners, NASA headquarters, Washington, 2002

[2] Quantitative risk assessment system (QRAS) version 1.6 user's guide, NASA headquarters, Washington, 2001

[3] Safie, F. M., An overview of quantitative risk assessment of space shuttle propulsion elements, PSAM 4, IAPSAM, 1998

[4] SP10000 PA00000-0001, KSLV-I 시스템 규격서 (안), 한국항공우주연구원, 2005