2002년도 대한전기학회 하계학술대회 논문집 2002.7.10-12

KSR-III 비상엔진중단 상황에 대한 정성적 결함 트리 분석

신명호°, 서진호°, 홍일희°
°한국항공우주연구원 로켓체계개발그룹

A Qualitative Fault Tree Analysis to Emergency Engine Stop of KSR-III

Myoung Ho Shin, Jin Ho Seo, Il Hee Hong
Korea Aerospace Research Institute

Abstract - 본 논문에서는 가압형 액체 추진 로켓인 KSR-III의 위험도 관리에 Fault Tree Analysis (FTA)를 적용한다. 미니멀 컷 set과 같은 FTA 구조 분석 방법을 소개하고, KSR-III 비상엔진중단 상황에 대해 정성적 FTA를 적용한다. 정성적 FTA를 통해서 KSR-III 추진기관 시스템의 구조적 특성을 명확히 하고 비상엔진중단을 야기시키는 컴포넌트 레벨에서의 실패와 작동 시퀀스의 조합에서의 문제 등을 명확히 하였다.

1. 서 론

KSR-III는 가압형 액체 추진 로켓으로 국내에서 처음으로 액체 추진기관을 시도하는 로켓이다. KSR-III의 추진기관은 산화제탱크, 연료탱크, 가압가스 탱크, 밸브 구동용 헬륨 탱크 등으로 구성되어 있다 [2]. 고체 추진기관에 비교해서 높은 추력을 내는 반면에 복잡한 구조를 갖추고 있다. 추진기관은 로켓 시스템에서 가장 중요한 부분으로, 로켓이 계획된 비행을 통해 지정된 작업을 수행할 수 있도록, 충분하고 안정된 추력을 낼 수 있어야 한다. KSR-III의 경우, 엔진 내부에 있는 두 개의 저주파 압력 센서와 하나의 고주파 센서를 통해 엔진 점화 이후 추력이 안정되고 충분하게 생성되는 지 여부를 판단하는 과정을 거친다. 만약, 추력이 충분하지 않거나 불안정하게 될 경우, 엔진을 비상 중단시키게 된다. 이와 같은 로켓 발사 실패를 방지하기 위해서는 이를 야기시킬 수 있는 원인들을 상세하게 확인, 평가, 분석해서, 위험도를 효과적으로 감소시키거나 제거할 필요가 있다. 본 연구에서는 이러한 목적을 위해 추진기관의 비상엔진중단 상황에 대해서 항공·우주 분야에서 신뢰성 해석 및 안정성 해석에 널리 사용되는 FTA를 적용한다.

FTA는 1962년 벨 전화연구소의 Watsonon에 의해 미닛 맨 미사일의 발사 제어 시스템 연구에서 처음으로 고안된 이후, 벨 전화연구소의 Mearns를 비롯한 연구 그룹에 의해 개량되어 미사일의 우발 사고를 예측하는 문제의 해결에 적용되었다. 그 후 보잉사의 Haasl, Schroder, Jackson 등은 FTA를 컴퓨터를 이용해 시뮬레이션 가능하도록 수정하였다. FTA는 주로 보잉사를 중심으로 하는 항공 우주 산업에 의해서 이루어 졌다. 1965년 Koloner나 Recht 등에 의해 FTA의 유효성이 연구되었고, 1974년 미국 원자력위원회가 행한 상업용 원자력 플랜트 재해 위험성의 평가 (일명, 라스므센 보고서)에서 FTA가 대규모로 활용되어 광범위한 재해 예측이 수행되었다. 이후 방면에 FTA는 항공·우주 분야를 비롯해서 원자력 산업, 화학 공정 등에서 신뢰성과 안전성 해석을 위해 널리 이용되었다 [1]. Fault Tree (FT)의 수리적 구조는 신뢰성 이론의 진보와 함께 점차 해명되었다. 최근에까지 복잡한 시스템을 나타내는 대규모 FT의 작성을 위해 컴퓨터 알고리즘이나 객체 지향 방법 등을 이용한 FT 모델링 등이 연구되고 있다 [3, 5, 6].

본 논문에서는 로켓 발사 시에 발생할 수 있는 비상엔진중단 상황에 대해 정성적 FTA를 적용해서, 어떠한 기본 사건 또는 조합이 비상엔진중단을 발생시키는 지를 찾는 작업에 이용할 것이다. 이러한 작업은 비상정지 상황에 대한 FT에서 미니멀 컷 set (minimal cut set)을 발견함에 의해서 가능해지는데, 미니멀 컷 set을 이용해서 비상엔진중단이 발생하는 원인을 명확히 하고 그 위험도를 감소시키거나 제거하는 조치를 취할 수 있게 된다.

2. FTA

2.1 FTA의 정의 및 특징

FT는 특정한 시스템 실패를 야기시킬 수 있는 원인을 상세하게 조합해 놓은 논리 모델로서, AND와 OR인 두 종류의 논리 게이트 조합에 의해 대상 플랜트 설비의 위험성이나 불신뢰성의 성립을 표현한다. FT는 각종 사상과 그것을 연결하는 게이트로 구성된다. FT를 작성하기 위해서는 먼저 해석하려는 시스템 실패 (top event, 정상사상)를 쓰고 그 아래 단에 그 실패의 직접 원인이 되는 기계·설비의 불량상태나 작업자의 에러 등 (fault event, 결함사상)을 나열해서 정상사상과의 사이를 게이트로 연결한다. 다음에 제2단 째 각 결함사상의 직접 원인이 되는 결함사상을 각각 제3단 째에 써서, 제2단 째와의 사이를 게이트로 연결한다. 이와 같이 해서 트리 구조로 원인이 되는 사상을 연결시킨다. FT의 최하단은 1)통상상태 (통상 행해지는 작업이나 기계·설비의 통상상태), 2)기본사상 (기본적으로 볼 수 있는 기계 등의 고장이나 인간의 에러), 3) 생략사상 (그것 이하는 정보 부족으로 분석할 수 없거나 또는 분석을 생략해도 좋은 결함 사상), 4)서브 트리 등이 된다.

FTA는 앞에서 설명한 FT를 작성하고 FT로 표현된 논리 모델의 정상사상을 야기시키는 여러 종류의 조합을 찾는 연역적 분석법으로, 그 목적은 시스템의 실패에 해당하는 정상사상을 발생시키는 원인들을 찾아내고 분석·평가하는데 있다. FT의 정상사상을 야기시키는 것은 항상 컴포넌트의 실패로 인해 발생하는 것만은 아니다. 작업자의 실수, 설계에서의 결함, 심각하지 않은 실패들의 조합이나 정상적인 상태를 갖는 컴포넌트의 상호 작용 등이 정상사상을 발생시키기도 한다. 인터페이스에서 발생한 문제가 시스템 레벨에서 실패를 야기하는 경우도 여기에 포함된다. 연역적 분석법인 FTA는 이러한 상황을 분석하는 데 있어 유용한 방법이다. FTA는 다음과 같은 6단계의 과정을 거쳐서 수행된다.

단계 1. 정상사상의 설정
단계 2. 대상 시스템의 특성 파악
단계 3. FT의 작성
단계 4. FT의 구조 분석 (정성적 분석)
단계 5. FT의 정량화
단계 6. FT 분석 결과 평가

2.2 정성적 FTA

FT의 정성적 분석이란 어떠한 사상에도 수치를 할당하지 않거나 또는 사상에 0이나 1의 값을 할당하여 분석

을 수행하는 방식이다. 0이나 1을 할당하는 것은 단지 사상이 발생하는 지의 여부를 판별하는 데 이용될 뿐이다. 따라서 정성적 분석에서 얻어지는 결과는 각 사상의 고유한 빈도 등의 확률적 수치와는 독립적이다. 정성적 분석의 목적은 대상으로 하는 시스템의 구조적 특성을 명확히 하는 것이다. 어느 기본사상의 조합이 정상사상의 발생에 큰 영향을 가지고 있는가를 아는 것은 정상사상에 의한 위험성을 유효하고 경제적으로 감소시키기 위해 아주 중요하다. 이를 위한 방법으로서 미니멀 컷 또는 미니멀 패스가 사용된다. 또 미니멀 컷이나 미니멀 패스는 정상사상과 깊은 관계를 가지고 있으므로 정상사상의 확률 계산이나 FT 특성의 해명 등에 이용할 수 있다.

컷이란 그 속에 포함되어 있는 모든 기본사상이 일어났을 때 정상사상을 일으키는 기본사상의 집합이다. 컷 중, 그 부분 집합만으로는 정상사상을 일으키는 일이 없는 것, 즉 정상사상을 일으키기 위한 필요 최소한의 컷을 미니멀 컷이라 한다. 한편, 패스란 그 안에 포함되는 모든 기본사상이 일어나지 않을 때, 처음으로 정상사상이 일어나지 않는 기본사상의 집합으로서 미니멀 패스는 그 필요 최소한의 것이다. 이와 같이 미니멀 컷은 어느 고장이나 에러를 일으키면 재해가 일어나는가 하는 것, 즉 시스템의 위험성을 나타내는 것이며, 미니멀 패스는 어느 고장이나 패스를 일으키지 않으면 재해는 일어나지 않는다는 것, 즉 시스템의 신뢰성을 나타내는 것이라고 할 수 있다.

많은 기본 사상과 많은 게이트를 갖는 FT에서는 직관적인 관찰에 의해 미니멀 컷을 구한다는 것은 쉬운 일이 아니다. 그래서 기계적인 방법이 요구되고 1972년 Fussel 등에 의해 FT의 미니멀 컷을 구하는 알고리즘이 개발되었다. 이 알고리즘은, AND 게이트는 항상 컷의 크기를 증가시키고, OR 게이트는 항상 컷의 수를 증가시킨다는 것을 기초로 하고 있다. 즉 정상 사상에서부터 차례로 상단의 사상을 하단의 사상으로 치환하면서 AND 게이트에서는 가로로 나열, OR 게이트에서는 세로로 나열해서 쓰는데 이렇게 모든 기본 사상에 달했을 때 이들의 각 행이 미니멀 컷이 된다.

미니멀 패스를 구하기 위해서는 미니멀 컷과 미니멀 패스의 쌍대성을 이용하는 것이 좋다. 즉, 먼저 대상으로 하는 FT와 쌍대인 FT (dual FT)를 구한다. 쌍대 FT란 원래 FT의 이론곱은 이론합으로, 이론합은 이론곱으로 치환해, 모든 사상은 그것들이 일어나지 않는 경우에 대해 생각한 FT다. 이 쌍대 FT에서 미니멀 컷을 구하면 그것은 원래의 FT의 미니멀 패스가 된다.

2.3 미니멀 컷과 미니멀 패스에 의한 정상사상 표현 [1]

여기서는 미니멀 컷 또는 미니멀 패스를 사용해서 정상사상을 표현하는 방법에 대해 설명한다. 먼저, 다음과 같은 기본 사상 i의 출력을 나타내는 함수 Y_i를 생각한다.

$$Y_i = \begin{cases} 1 & \cdots \text{ 사상 } i \text{ 가 일어나는 경우} \\ 0 & \cdots \text{ 일어나지 않는 경우} \end{cases}$$

$\boldsymbol{Y} = \{Y_1, Y_2, \ldots, Y_n\}$ 라 정의할 때, $\phi(\boldsymbol{Y})$ 를 다음과 같이 정의한다.

$$\phi(\boldsymbol{Y}) = \begin{cases} 1 & \cdots \text{ 정상 사상이 일어나는 경우} \\ 0 & \cdots \text{ 일어나지 않는 경우} \end{cases}$$

즉, $\phi(\boldsymbol{Y})$ 은 기본사상의 발생 상태에 따른 정상사상 발생의 유무를 나타내는 함수로서 정상사상에 대한 불표시 함수라 불리운다.

이제, $K_1, K_2, \cdots, K_k$ 를 어떤 FT의 미니멀 컷이라 할 때, 기호 $\prod$ 를 $\prod_{s=1}^{k} Z_s \equiv 1 - \prod_{s=1}^{k}(1 - Z_s)$ 와 같이 정의하면, 이 FT의 $\phi(\boldsymbol{Y})$ 는 다음과 같은 식으로 표현된다.

$$\phi(\boldsymbol{Y}) = \prod_{s=1}^{k} \prod_{i \in K_s} Y_i$$

또, $P_1, P_2, \cdots, P_l$ 을 이 FT의 미니멀 패스라고 하면 $\phi(\boldsymbol{Y})$ 는 다음 식으로도 표시될 수 있다.

$$\phi(\boldsymbol{Y}) = \prod_{r=1}^{l} \prod_{i \in P_r} Y_i$$

그러나 이들의 $\phi(\boldsymbol{Y})$ 를 표시하는 식에서 어떤 Y_i 에 대해 Y_i^n 의 항이 있을 때는 불 대수 규칙을 사용해서 $Y_i^n = Y_i$ 로 해서 중복을 제외하지 않으면 그 후의 확률 계산 등에 오차가 생기게 된다.

3. FTA의 추진기관 비상엔진중단에의 응용

3.1 추진기관 플로 다이어그램

FTA를 적용할 대상은 그림 1과 같은 KSR-III 가압형 액체 추진기관이다. KSR-III 추진기관은 산화제탱크와 연료탱크에 압력을 가하기 위한 가압 시스템, 엔진 주 공급 라인 밸브를 구동하기 위한 공압 시스템, 추진제 공급 및 배출 시스템, 발사 전 공기와 수분을 제거하기 위한 정화 시스템, 엔진 점화를 위한 점화 시스템, 비상정지를 위한 비상 배출 시스템 등으로 구성되어 있다.

가압 방식은 헬륨 공급방식과 제어방식에 따라 나누어질 수 있는데, KSR-III의 경우 이 중 간단하면서도 신뢰도가 높고 개발 기간이 짧은 대기온도 헬륨-단일 레귤레이터 방식을 채택하고 있다. 대기온도 상태의 헬륨을 헬륨탱크에 4500psia까지 충전하고, 350psia의 추진제 탱크 압력을 맞추기 위해 단일 레귤레이터를 사용한다. 공압 시스템은 로켓 내부의 밸브들 중에 헬륨에 의해 작동되는 추진제 주 공급라인 볼 밸브를 구동하기 위한 시스템이다. 공압탱크의 압력은 4500psia이며 볼밸

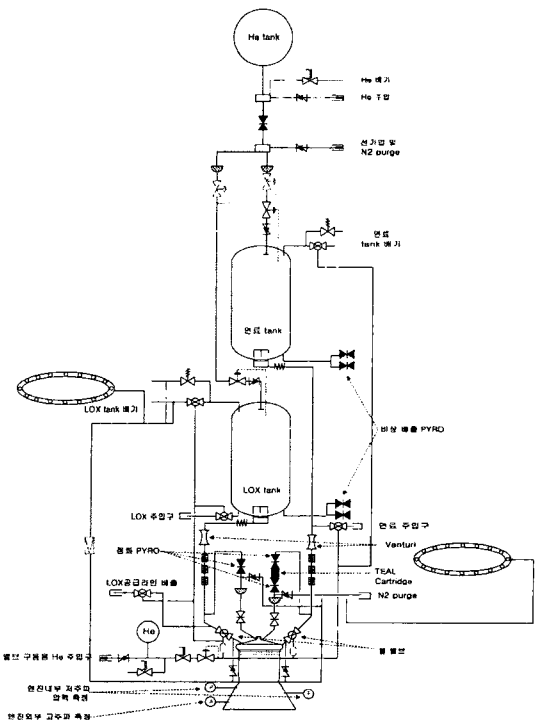

그림 1. KSR-III 추진기관 구성도

브의 구동압은 17kgf/㎠ 이다.

비상정지 상황이 발생할 경우 추진제를 비상 배출할

수 있도록, 로켓 발사와 동시에 분리되는 밸브를 이용해서 추진탱크를 충전한다. 추진탱크로부터 엔진으로의 공급라인에는, 유량제어를 위해 공급라인의 직선부에 VENTURI가 설치되어 있고, 최종부에는 ON/OFF 볼밸브가 설치되어 있다. LOX 라인에 수분이 존재하는 경우 수분이 얼어 엔진으로 들어가서 문제를 야기할 수 있고, 점화 라인에 있을 경우에는 TEAL과 반응하여 화재가 발생할 위험이 있다. 따라서, 이를 방지하기 위해 추진기관 내부의 공기 및 수분을 제거하기 위해 발사 직전 질소 퍼지를 수행한다. 점화를 하기 위해서 KSR-III는 접촉발화성 물질인 TEAL을 사용한다. TEAL로만 채워진 cartridge를 연료 점화 라인에 설치하여 점화시 TEAL을 연료가 밀고 나가면서 점화시킨다. 엔진점화는 주 추진제 라인의 볼밸브 구동전에 점화 PYRO가 구동되면서 이루어진다. 먼저 점화 및 라인 냉각을 위해 LOX가 먼저 분사되어진 후 TEAL이 분사되고, 마지막으로 주 추진제가 분사되면서 엔진이 점화된다. 충전된 TEAL이 모두 소모되면, TEAL을 따라서 연료가 점화라인으로 분사된다.

발사대기 상태에서 비상엔진중단은 엔진 내부의 저주파 압력 센서로부터 측정한 압력값이 요구되는 레벨보다 낮거나, 엔진외피에 부착된 고주파 가속도 센서의 측정값이 크면, 추력이 불충분하거나 엔진이 불안정한 것으로 판단해서 엔진을 중단시키고 발사작업을 멈추게 된다. 다음 단락에서 이러한 비상엔진중단 상황에 대해서 정성적인 FTA를 수행할 것이다.

3.2 FT 작성 및 미니멀 컷 set

KSR-III에서 비상엔진중단이 발생하는 경우에 대한 FT는 그림 2와 같다. 비상엔진중단은 크게 추진제 공급이상, 주밸브 오동작, 엔진점화 실패의 세 가지 원인에 의해서 발생한다. 추진제 공급 이상과 주밸브 오동작이라는 결함사상은 주로 각 컴포넌트 레벨에서의 실패에 기인한다는 것이 그림 2의 FT를 통해서 확인된다. 엔진점화 실패와 같은 경우는 점화 PYRO 실패와 같은 부품레벨에서의 실패와 점화 시퀀스 진행 작업간의 타이밍 문제에서 기인한다. 점화 시퀀스 타이밍 문제는 컴포넌트 레벨에서의 발생하는 결함으로 인한 것이 아니라, 정상적으로 동작하는 각 부분이 타이밍을 맞추는데 실패함으로 인해 엔진점화가 불완전하게 이루어지거나 연소가 불안정하게 되는 상황으로 진전되는 경우이다. 엔진점화 타이밍 문제는 엔진점화시 로켓 내부의 연료 PYRO가 열린 후 연료 주 공급라인 볼밸브가 열리는 데 걸리는 실제 시간과 연료 주 공급라인 볼밸브가 열리고 난 후 산화제 주 공급라인 볼밸브가 열리는 실제 시간이 엄밀하게 지켜져야 하기 때문에 발생하는 것이다. 로켓 시스템과 지상장비의 변화, 온도, 습도 등의 환경의 변화 등이 있을 때, 실제 작동이 일어나는 데 걸리는 time delay를 측정해야 한다. 그림 2에서 볼 수 있는 것처럼 time delay의 변화는 엔진점화 실패의 직접적인 원인으로서 작용하고 있다.

그림 2의 FT에 대한 정성적 평가를 위해서 미니멀 컷 set을 구한다. 미니멀 컷 set은 그 집합에 포함되는 기본사상이 발생하면 반드시 정상사상이 발생하는 최소 기본사상들의 집합이므로, 어떠한 요소 고장 또는 조합에 의해서 시스템에 문제가 발생하는 지를 명확히 할 수 있다. 그림 2의 FT의 미니멀 컷 set은 Fussell의 알고리즘({1})을 적용해서 구해진다. 다음의 3가지 조합을 제외하면 그림 2의 FT의 최하단에 해당하는 컴포넌트 레벨에서의 결함들은 모두 비상엔진중단 상황에 대한 미니멀 컷이 된다.

1. (Time delay 측정 및 테스트 작업 불충분) + (연료 PYRO open 신호가 발사통제 시스템에서 나간 후, 실제 open되는 데 걸리는 time delay 변화)
2. (Time delay 측정 및 테스트 작업 불충분) + (연료 주 볼밸브 open 신호가 발사통제 시스템에서 나간 후, 실제 open되는 데 걸리는 time delay 변화)
3. (Time delay 측정 및 테스트 작업 불충분) + (산화제 주 볼밸브 open 신호가 발사통제 시스템에서 나간 후, 실제 open되는 데 걸리는 time delay 변화)

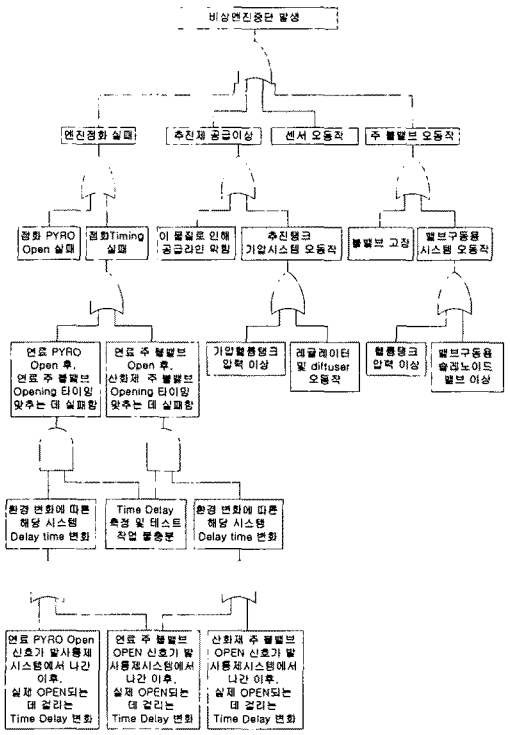

그림 2. KSR-III 비상엔진중단 상황에 대한 FT

4. 결 론

FTA는 로켓 시스템의 신뢰성 확보를 위한 위험도 관리에서 top-down 방식의 분석법으로 이용될 수 있다. FT를 이용해서 시스템에서 문제가 되는 실패의 원인들을 찾아내고, 이를 바탕으로 위험도를 감소시키거나 제거하여 허용할 수 있는 정도 이하로 위험도를 낮추기 위해서는, 대상으로 하는 실패에 대해서 위험도 및 신뢰성을 정량적으로 수치화에 하는 것에 대한 추가적인 연구가 필요하다.

[참 고 문 헌]

[1] 이근철, *FTA 안전공학*, 기전연구사, 1990.

[2] 한국항공우주연구원, *3단형 과학로켓 개발사업 (IV)*, 2001.

[3] M. Cepin and B. Mavko, "Fault tree developed by an object-based method improves requirements specification for safety-related systems", *Reliability Engineering and Systems Safety*, vol. 63, pp. 111-125, 1999.

[4] W. E. Hammond, *Design Methodologies for Space Transportation Systems*, Reston:AIAA Inc., 2001.

[5] D. H. Kuo, D. S. Hsu, and C. T. Chang, "A prototype for integrating automatic fault tree/event tree/HAZOP analysis," *Computers Chem. Eng.*, vol. 21, pp.S923-S928, 1997.

[6] Y. Wang, T. Teague, H. West, and S. Mannan, "A new algorithm for computer-aided fault tree synthesis," Preprint, 2002.