2004 춘계학술발표회 논문집
한국원자력학회

초기사건 및 안전계통이 결합된 사고경위의 고장수목 모델 및 빈도 평가 방법

Development of a Practical Approach to Estimate the Frequency of an Accident Sequence Using a Fault Tree Method

한상훈, 박진희
한국원자력연구소
대전광역시 유성구 덕진동 150

요 약

PSA(Probabilistic Safety Assessment)에서 사고경위(Accident Sequence)는 초기사건(Initiating Event)과 안전계통(Mitigating Safety System)의 곱으로 나타난다.
초기사건은 단순히 하나의 값으로 주어지는 경우도 있지만, 초기사건이 계통의 고장일 경우에는 고장수목(Fault Tree)으로 모델하여 계산되기도 한다. 초기사건을 고장수목으로 모델할 경우 초기사건과 안전계통의 고장수목을 결합하여야 사고경위 발생빈도를 적절히 평가할 수 있다.
같은 계통이 초기사건 및 안전계통에 포함될 경우, 하나의 계통에 대해 초기사건에서는 고장률 모델로, 안전계통에서는 이용불능도 모델로 처리하여야 한다. 특히 초기사건이 보조계통의 고장으로 인한 경우에는 이 보조계통의 고장이 안전계통의 부분으로도 포함되어 분석을 어렵게 할 수 있다.
많은 PSA에서 초기사건에 대한 고장수목을 구성하여 초기사건 고장률을 계산한 후에 초기사건을 단순히 하나의 사건으로 처리하여 안전계통과 통합하는 것이 일반적이다. 따라서 안전계통과의 연관관계가 완전하게 처리되지 않을 수 있다.
본 보고서에서는 초기사건과 안전계통의 고장수목이 결합되는 사고경위의 발생빈도를 평가하는 방법에 대한 연구를 수행하였다.
제안된 방법은 같은 계통이 초기사건과 안전계통에 사용되어도 하나의 고장수목 모델을 양쪽에 사용할 수 있으며, 기존의 PSA에서 개발된 안전계통의 고장수목 모델을 초기사건 모델에도 활용할 수 있는 장점이 있다. 또한, 초기사건과 안전계통의 고장수목 모델이 곱해진 사고경위에 대해 한번에 최소단절집합을 구할 수가 있어 PSA에서 실질적으로 활용할 수 있는 방법이다.

Abstract

An accident sequence in the PSA (Probabilistic Safety Assessment) is expressed in production of an initiating event and a mitigating system.

An initiating event can be expressed either in one value or in a fault tree. To calculate the occurrence rate of the accident sequence in case that the initiating event is modeled using a fault tree, we have to combine two fault tree models for the initiating event and the mitigating system.

Note that the initiating event is modeled in terms of the failure rate and the mitigating system is modeled in terms of the failure probability. Currently, no practical approach is available to combine the two different kinds of fault trees where one is for the failure rate and the other is for the failure probability.

In most PSAs, even if an initiating event is modelled as a fault tree, it is treated as one value and combined with the mitigating systems.

This report presents a practical approach how to model fault trees for the initiating event and mitigating system for the purpose of estimating the occurrence rate of the accident sequence. The basic idea of the approach is to estimate the failure rate from the failure probability during the mission time.

Furthermore, in case that a system is included in both the initiating event and the mitigating system, the fault tree model already developed for the mitigating system in the PSA can be used directly for the initiating event with the proposed approach.

1. 서론

PSA(Probabilistic Safety Assessment)에서 사고경위(Accident Sequence) 모델은 초기사건(Initiating Event)과 사고완화 안전계통(Mitigating Safety System)의 곱으로 나타난다. 초기사건은 시간당 발생빈도로 평가되며, 안전계통은 이용불능도(Unavailability)로 평가되므로 단위가 주어지지 않는다. 따라서 사고경위는 단위 시간당 발생빈도로 평가된다. 초기사건은 단순히 하나의 값으로 주어지는 경우도 있지만, 초기사건이 계통의 고장일 경우에는 고장수목(Fault Tree)으로 모델하여 계산되기도 한다.

초기사건 모델과 관련하여서는 Xing[1]이 2 트레인(Train) 계통의 초기사건 빈도 평가를 위해 고장수목 방법 및 Markov 방법을 비교한 적이 있으며, 몇 가지 참고문헌에서는 주어진 최소단절집합의 발생률을 계산하는 방법이 제시되어 있다 [2, 3].

그러나, 초기사건과 안전계통이 결합된 사고경위 발생빈도와 관련한 방법은 제시된 바 없다. 예로서 초기사건이 계통의 고장인 경우에는 초기사건과 안전계통의 고장수목을 결합하여야 사고경위 발생빈도를 적절히 평가할 수 있다. 이 때, 초기사건의 고장수목과 안전계통의 고장수목은 많은 연관관계를 가질 수 있다. 예를 들면 Essentail Service Water System(ESWS)은 초기사건 고장수목에도 포함되며 안전계통의 고장수목에도 포함된다. 그러나 초기사건에서는 고장률 모델로, 안전계통에서는 이용불능도 모델로 처리된다.

많은 PSA에서는 초기사건에 대한 고장수목을 구성하여 초기사건 고장률을 계산한 후에 초기사건을 단순히 하나의 사건으로 처리하여 안전계통과 통합한다. 따라서 안전계통과의 연관관계가 완전하게 처리되지 않을 수 있다.

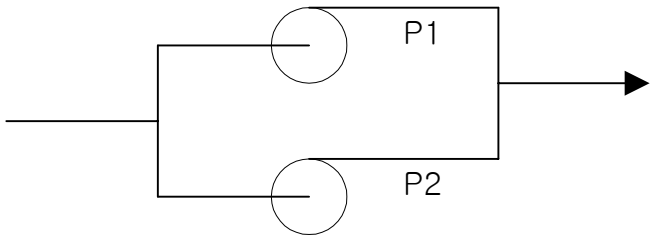
또한 초기사건에 포함되는 보조계통 등에 대해서도 PSA에서 기존의 이용불능도 모델로 개발된 것과는 다른 완전히 새로운 모델을 구성하여야 할 수도 있다.

한국원자력연구소에서는 이와 같은 경우의 분석 방법을 개발하기 위한 연구를[4] 수행하였고, 이 논문은 그 결과 중 분석 방법에 대한 것을 요약한 것이다.

2. 방법론 제안

이 논문에서는 작동요구시간(Mission Time) 동안의 계통 고장확률을 구하고, 이를 이용하여 계통의 고장률을 구하는 방법을 제안한다. 이 방법의 기본적인 개념은 다음에 주어져 있다.

다음과 같이 2개의 펌프로 이루어진 계통을 가정한다. P1 또는 P2 어느 하나만 작동하면 계통의 기능을 수행할 수 있다.



여기서는 문제를 간단히 하기 위하여 Fails to Start, Fails to Run 고장모드만을 고려하며, OOS로 인한 이용불능은 고려하지 않는다.

P1은 운전중이고, P2는 대기중에 있는 경우에 계통의 고장률은 P1이 고장나는 고장률에 P1이 고장나는 경우에 P2의 고장확률을 곱합으로서 계산할 수 있다.

즉, 다음과 같이 계산할 수 있다.

$$\lambda sys = \lambda_1 \cdot (S_2 + \lambda_2 \cdot Tm)$$

여기서 λ_1, λ_2는 각기 펌프 P1, P2의 고장률이고,

S_2는 P2의 기동실패 확률이며, Tm은 작동요구시간이다.

위의 식 양쪽에 Tm을 곱하면,

$\lambda sys \cdot Tm = \lambda_1 \cdot Tm \cdot (S_2 + \lambda_2 \cdot Tm)$

과 같이 된다. 각 항의 의미를 보면

$\lambda_1 \cdot Tm$: P1이 작동요구시간 동안 고장나는 확률

$S_2 + \lambda_2 \cdot Tm$: P1이 고장나는 경우에 P2의 고장확률

$\lambda sys \cdot Tm$: 계통이 작동요구시간 동안 고장나는 확률

$\lambda sys \cdot Tm$을 구하는 것은 작동요구시간 동안의 고장확률을 구하는 것으로서 일반적인 계통의 이용불능도를 구하는 것과 같아진다.

즉, 이용불능도를 구하고 이를 작동요구시간으로 나누어 계통의 고장률을 구할 수 있다.

이 방법에서는 작동요구시간을 적절히 설정하는 것이 중요하다. 위의 계통에서 P1이 고장나는 경우에는 P2가 기동하여 운전한다. P1을 복구할 때까지 P2가 계속하여 운전한다면 이 계통은 원래의 건전한 상태로 돌아가게 된다. 따라서 P2의 작동요구시간은 P1의 복구시간을 사용하는 것이 적절하다. 반면, 울진 3,4 호기 등 국내 표준원전 계열의 PSA에서는 작동요구시간으로서 모두 24시간을 이용하였으며, 이는 일반적인 기기의 복구시간인 20시간에서 40시간 정도와 유사하다.

만일 계통마다 또는 사고경위마다 작동요구시간이 크게 차이나는 경우에는 이 방법을 사용하기 어려울 수 있다.

3. 사고경위 분석 예제

여기서는 간단한 계통을 대상으로 고장수목을 모델하고, 사고경위 발생빈도를 계산하는 예제를 제시한다. 고장수목 모델은 일반적인 고장률 계산 방법과 본 논문에서 제시된 방법의 2가지 방법으로 각기 평가하여 장단점을 검토하였다.

3.1. 예제 계통

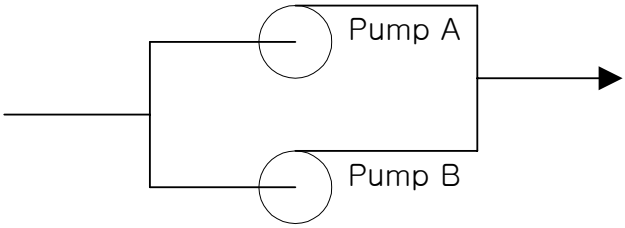
3.1.1. 예제 계통 선정

다음과 같이 Loss of An Essential Service Water Train(LOSW)이 발생하였을 때, Auxiliary Feedwater System(AFWS)가 작동하면 발전소가 안정한 상태로 가고, AFWS가 작동하지 않으면 원하지 않는 상태로 진행하는 사고경위에 대하여 예제 고장수목들을 작성하고, 문제점 및 해결 방안을 모색한다.

LOSW-2는 LOSW가 발생하고 AFWS가 작동하지 않아 사고로 진행되는 사고경위로서 여기서는 LOSW 사고경위로 부르겠다.

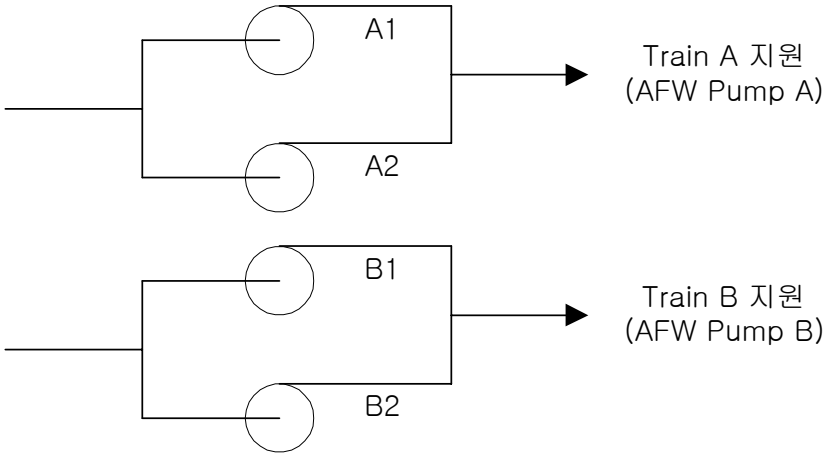
문제를 간단히 하기 위하여 계통은 ESWS, AFWS, Electric Power System(EPS) 3개만을 고려한다. ESWS 및 AFWS는 펌프만 고려한다. 작동신호 고장, 보수로 인한 이용불능 등은 고려하지 않는다. EPS는 2개의 버스(Bus)만을 고려한다.

AFWS는 다음과 같이 2 개의 트레인으로 구성되며, 각 트레인 모두 대기상태에 있다가 LOSW 등의 사건이 발생하면, 자동적으로 작동한다.



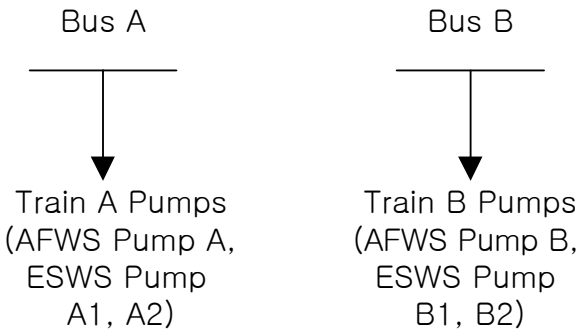
Aux Feedwater System

ESWS는 다음과 같이 2개의 트레인으로 구성되며 각 트레인은 2개의 부트레인(Subtrain)으로 구성된다. 각 트레인에서 A1, B1은 정상시 운전 중이며, A2, B2는 정상시 대기상태에 있다.



Essential Service Water System

EPS는 다음과 같이 2개의 트레인으로 구성된다.



3.1.2. 고장수목에서의 사건이름

본 보고서의 예제 고장수목에서 각 사건의 특징을 명확히 구분하기 위하여 다음과 같이 사건 이름의 양식을 정하여 사용한다.

- 각 사건을 Initiator (고장률로 평가) 또는 Mitigating 기능상실 (이용불능도로 평가) 사건인지를 구분하고, 또한 Mitigating 기능상실 사건은 사고전부터 계속하여 운전중인지, 사고후 작동하는 것인지, 사고후 작동하여 운전하는 지에 따라 사건(Event)을 분류
- Event 분류는 최소단절집합에 나타나는 각 사건의 특징을 쉽게 파악하기 위하여 사용함.
- Event 분류
  - L : Initiator
  - C : Fails to Continue Running
  - R : Fails to Run Once Started
  - S : Fails to Start or Out of Service (Failure at or Before System Demand)
- 고장수목에 나타나는 사건이름을 다음과 같이 처리함
  - SSCCFT-nnnnnn : SS : 계통분류, CC : 기기종류, F : 고장모드, T : Event 분류

3.1.3. 예제 신뢰도 자료

예제 고장수목에서는 다음과 같이 신뢰도 자료를 가정하여 사용한다.

- 펌프 Fails to Start : 1.0e-3
- 펌프 Fails to Run : 1.0e-5/h
- 버스 Fails while Operation : 1.0e-6/h

3.2. 고장률 계산을 위한 일반적인 고장수목 모델

본 논문에서 제안된 방법으로 사고경위의 고장수목을 모델하기 전에, 고장률 평가를 위한 일반적인 고장수목 모델 방법을 이용하여 사고경위의 고장률을 평가하여 그 방법을 검토한다.

3.3.1 고장수목 모델

사고경위의 고장수목 모델은 초기사건 모델과 안전계통 모델의 곱으로 표현된다. LOSW에 해당하는 GSW-LA 게이트는 부트레인 A1이 작동 중 고장나는 모델과 A1이 고장나는 경우에 대기중인 부트레인 A2가 작동하지 않는 모델의 곱으로 표현된다. 부트레인 A1에 해당되는 부분은 고장률 모델로, 부트레인 A2에 해당되는 부분은 이용불능도 모델로 표현된다. 반면 안전계통인 AFWS 계통은 이용불능도 모델로 구축되며, 그림에는 안전계통 용으로 모델되는 고장수목이 표시되어 있으며, 이는 PSA에 기본으로 모델되는 것과 동일한 방법으로 모델되었다.

이 방법에서는 같은 기기의 고장이라도 용도에 따라 고장률 또는 이용불능도 용으로 모델된다. 예로서 ESW 펌프 A1이나 EPS 버스 트레인 A가 이에 해당된다.

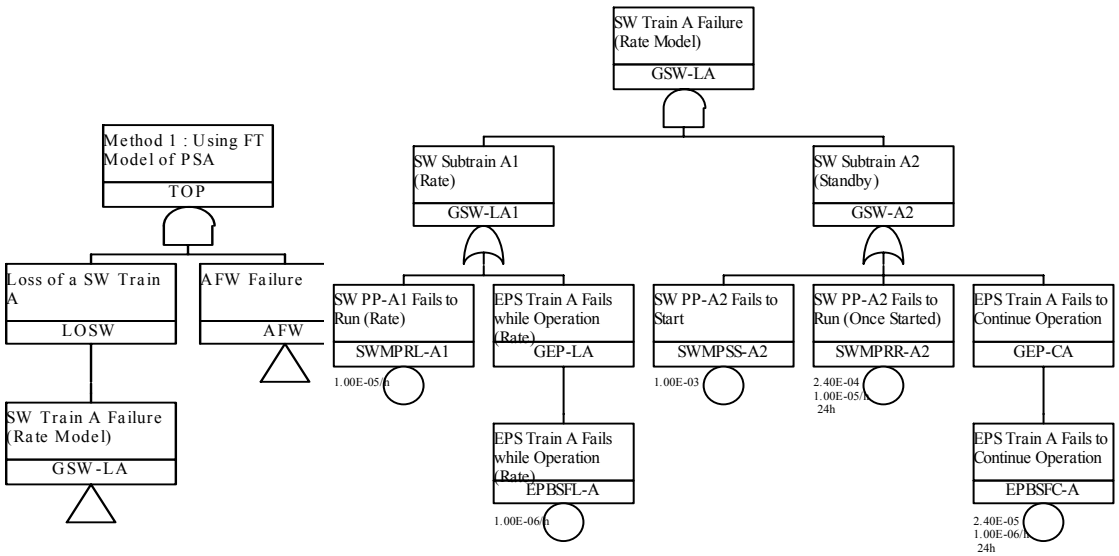


그림 1. 고장률 계산을 위한 일반적인 고장수목 모델

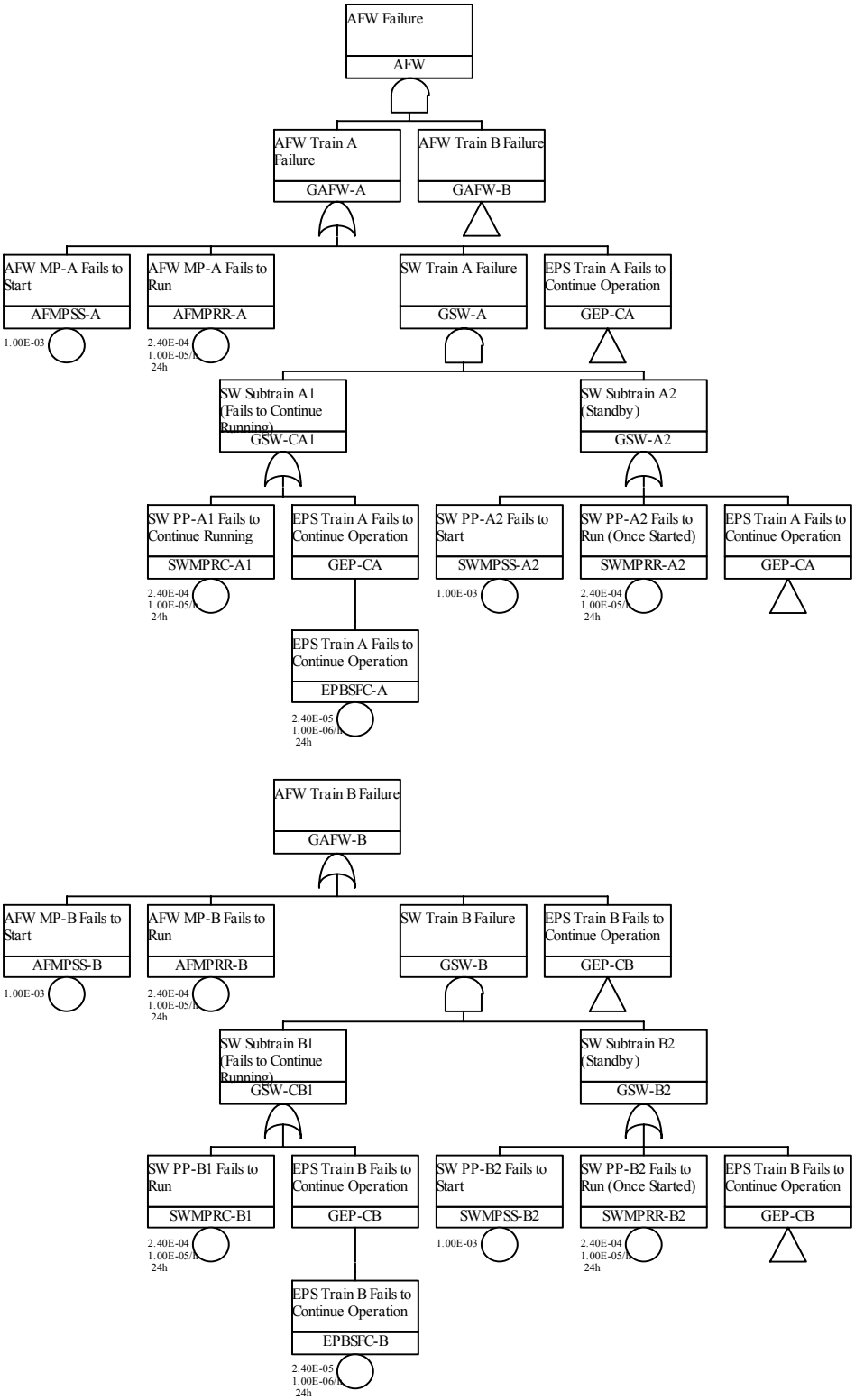


그림 1. 고장률 계산을 위한 일반적인 고장수목 모델 (계속)

3.2.2. LOSW 사고경위 정량화

그림 1의 고장수목을 수정없이 그대로 이용하여 LOSW 사고경위 정량화를 수행할 수 없으며, 다음과 같은 사항을 고려하여 정량화를 수행하여야 한다.

- EPBSFL-A는 정상운전중 버스 A가 상실되는 사건이다. EPBSFC-A는 LOSW 발생시까지는 버스 A가 정상이나, 이후에 사고진행 중에 버스 A가 상실되는 사건이다. EPBSFL-A가 발생하면 버스 A가 고장나서 작동중인 ESWS 펌프 A1이 운전정지되는 것은 물론 대기중인 ESWS 펌프 A2도 기동할 수 없다. 따라서 이용불능도로 모델되는 부분에서도 이를 고려하여 고장수목을 적절히 수정하는 것이 필요하다. 즉, GEP-C에 모델되는 사건을 EPBSFC-A 대신 EPBSFL-A으로 변경하는 것이 필요하다.
  - EPBSFC-A → EPBSFL-A로 처리
- ESWS 트레인 A가 상실되는 경우에는 AFWS 트레인 A 역시 이용불능하여야 하므로, 이를 반영하여 모델을 다시 수정하여 평가하여야 한다. 이 부분은 PSA의 AFWS 모델을 사용하지 않고, 이 초기사건에 맞는 고장수목을 따로 구성한다면 문제가 되지 않는다.
  - AFWS의 트레인 A를 이용불능으로 처리

이와 같이 모델을 수정한 후에 정량화를 수행하면 LOSW 사고경위의 발생빈도는 1.28e-9/h 로 나타나며 다음과 같은 15개의 최소단절집합이 나온다. 표에서 Italic 체는 Initiator 사건을 나타낸다.

표 1. 고장률 계산을 위한 일반적인 고장수목 모델 방법의 최소단절집합

No	Value	Cut Set			
1	1.00E-09	*EPBSFL-A*	AFMPSS-B		
2	2.40E-10	*EPBSFL-A*	AFMPRR-B		
3	2.40E-11	*EPBSFL-A*	EPBSFC-B		
4	1.00E-11	*SWMPRL-A1*	SWMPSS-A2	AFMPSS-B	
5	2.40E-12	*SWMPRL-A1*	SWMPRR-A2	AFMPSS-B	
6	2.40E-12	*SWMPRL-A1*	SWMPSS-A2	AFMPRR-B	
7	5.76E-13	*SWMPRL-A1*	SWMPRR-A2	AFMPRR-B	
8	2.40E-13	*SWMPRL-A1*	SWMPSS-A2	EPBSFC-B	
9	2.40E-13	*EPBSFL-A*	SWMPRC-B1	SWMPSS-B2	
10	5.76E-14	*SWMPRL-A1*	SWMPRR-A2	EPBSFC-B	
11	5.76E-14	*EPBSFL-A*	SWMPRC-B1	SWMPRR-B2	
12	2.40E-15	*SWMPRL-A1*	SWMPSS-A2	SWMPRC-B1	SWMPSS-B2
13	5.76E-16	*SWMPRL-A1*	SWMPRR-A2	SWMPRC-B1	SWMPSS-B2
14	5.76E-16	*SWMPRL-A1*	SWMPSS-A2	SWMPRC-B1	SWMPRR-B2
15	1.38E-16	*SWMPRL-A1*	SWMPRR-A2	SWMPRC-B1	SWMPRR-B2

3.3. 작동요구시간 동안의 고장수목 모델

2절에서는 작동요구시간 동안의 고장확률을 구하고, 이를 작동요구시간으로 나누어 고장률을 계산하는 방법을 제안하였다. 여기서는 이에 따라 고장수목을 구성하고 분석하는 방법을 검토한다.

3.3.1 고장수목 모델

작동요구시간 동안의 계통 고장확률을 구하는 것은 기존의 PSA에서 항상 행해지던 일이다. 작동요구시간 동안의 계통 이용불능도를 구하는 고장수목을 작성하면 그림 2와 같다. AFWS의 고장수목은 일반적으로 PSA에서 안전계통 용으로 모델되는 것을 그대로 사용할 수 있다.

여기서 Event 분류가 C인 사건은 항시 운전중인 기기에 대한 고장을 나타내는 것으로서, Initiator 사건 및 초기사건 발생후 계속 운전을 실패하는 경우를 모두 포함한다. 즉, 3.2절에서의 Event 분류 L 및 C를 통합하여 포함한다.

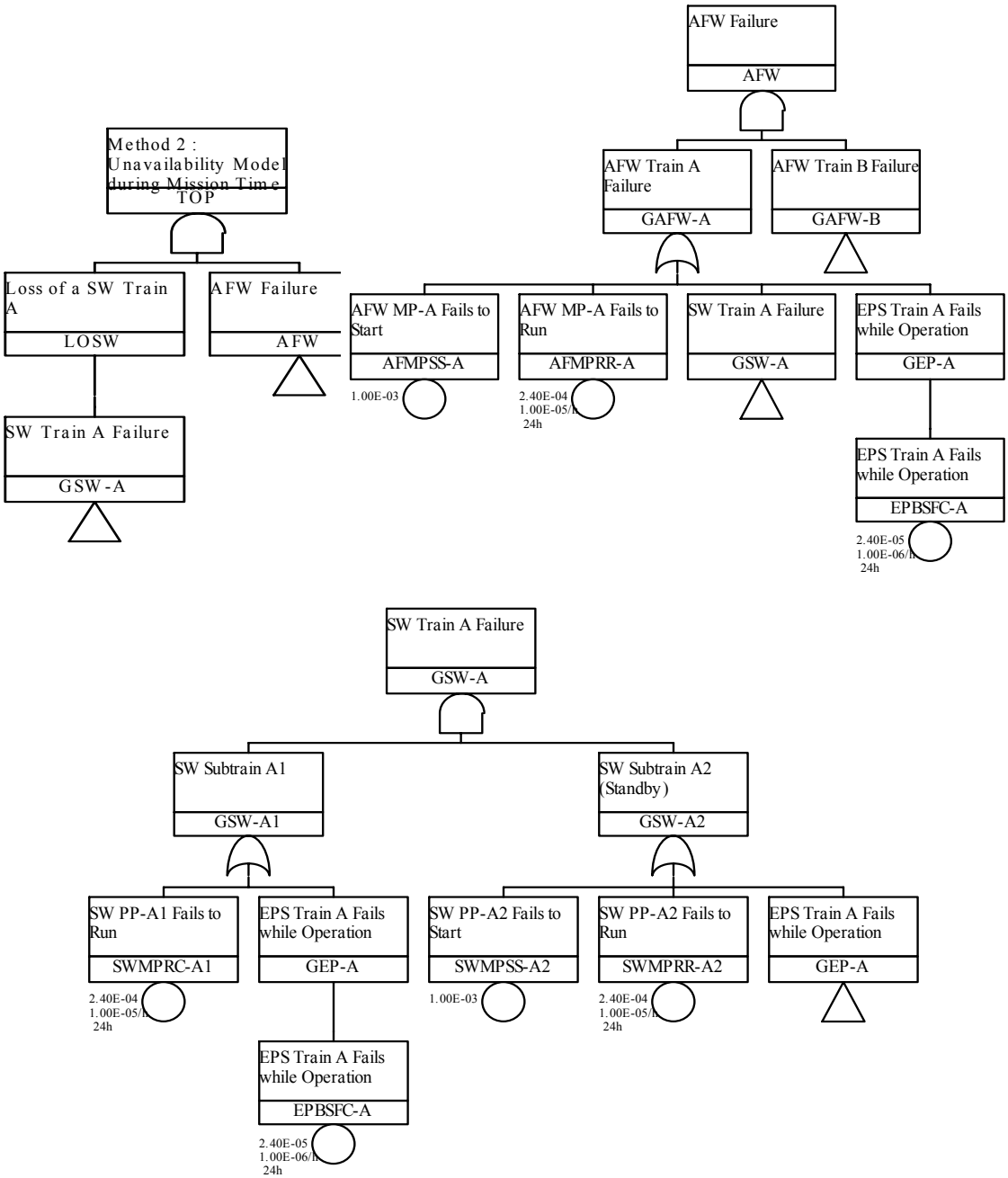


그림 2. 작동요구시간 동안의 고장확률로부터 추정하는 방법에 의한 고장수목

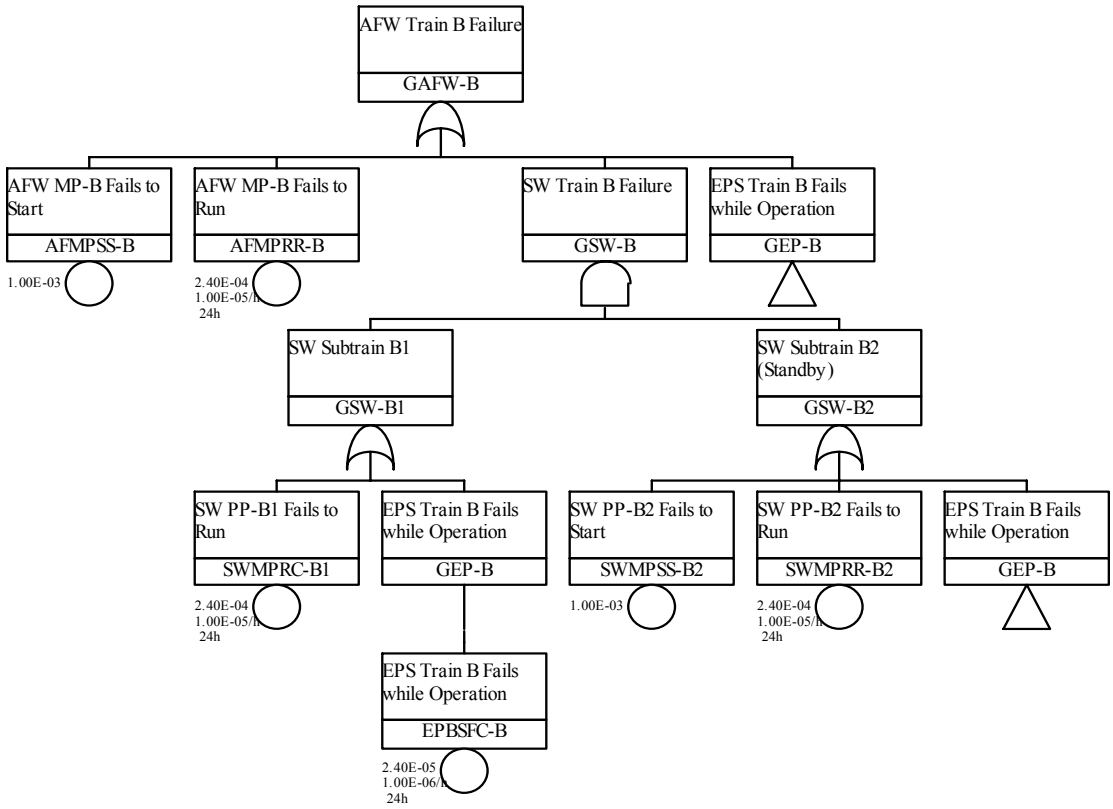


그림 2. 작동요구시간 동안의 고장확률로부터 추정하는 방법에 의한 고장수목 (계속)

3.3.2. LOSW 사고경위 정량화

LOSW 사고경위 정량화는 그림 2에 주어진 고장수목으로부터 바로 수행될 수 있으며, 그 결과는 다음과 같다.

- 작동요구시간 동안의 계통 고장확률은 3.072e-8로 계산된다.
- 3.072e-8을 작동요구시간인 24시간으로 나누면 사고경위 발생빈도는 1.28e-9/h로 고장률 계산을 위한 일반적인 고장수목 모델 방법의 결과와 같다.
- 표에서 Italic체는 LOSW로 인한 Initiator 사건에 해당한다. 각 최소단절집합은 고장률로 표시되는 Initiator과 고장확률로 표시되는 다른 사건의 곱으로 나타나야 한다. 각 최소단절집합을 검토하면 ESWS에서 운전중인 기기들의 고장이 각 최소단절집합에 하나씩 나타난다. 이들의 고장이 LOSW를 유발할 수 있는 Initiator 사건이 된다. 만일 이들 사건들을 고장률 사건으로 대치한다면, 최소단절집합 역시 고장률 계산을 위한 일반적인 고장수목 모델 방법의 결과와 동일하게 된다.

표 2. LOSW 사고경위 최소단절집합

No	Value	Cut Set			
1	2.40E-08	*EPBSFC-A*	AFMPSS-B		
2	5.76E-09	*EPBSFC-A*	AFMPRR-B		
3	5.76E-10	*EPBSFC-A*	EPBSFC-B		
4	2.40E-10	*SWMPRC-A1*	SWMPSS-A2	AFMPSS-B	
5	5.76E-11	*SWMPRC-A1*	SWMPRR-A2	AFMPSS-B	
6	5.76E-11	*SWMPRC-A1*	SWMPSS-A2	AFMPRR-B	
7	1.38E-11	*SWMPRC-A1*	SWMPRR-A2	AFMPRR-B	
8	5.76E-12	*SWMPRC-A1*	SWMPSS-A2	EPBSFC-B	
9	5.76E-12	*EPBSFC-A*	SWMPRC-B1	SWMPSS-B2	
10	1.38E-12	*SWMPRC-A1*	SWMPRR-A2	EPBSFC-B	
11	1.38E-12	*EPBSFC-A*	SWMPRC-B1	SWMPRR-B2	
12	5.76E-14	*SWMPRC-A1*	SWMPSS-A2	SWMPRC-B1	SWMPSS-B2
13	1.38E-14	*SWMPRC-A1*	SWMPRR-A2	SWMPRC-B1	SWMPSS-B2
14	1.38E-14	*SWMPRC-A1*	SWMPSS-A2	SWMPRC-B1	SWMPRR-B2
15	3.32E-15	*SWMPRC-A1*	SWMPRR-A2	SWMPRC-B1	SWMPRR-B2

4. 결론 및 고찰

본 논문에서는 초기사건과 안전계통이 결합되는 사고경위에 대해 고장수목을 모델하고 발생빈도를 평가하는 방법에 대한 연구를 수행하였다. 본 논문에서 제안된 방법은 작동요구시간 동안의 실패확률을 평가하는 고장수목 모델을 구성하고, 이로부터 발생빈도를 추정하는 방법이다.

이 방법의 장점은 다음과 같다.

- 계통이 복잡하게 연계된 경우도 모델 및 정량화가 간단하다.
- 작동요구시간에 대해 모델함으로써 초기사건과 안전계통에 같은 기기/계통이 포함된 경우에 초기사건과 안전계통에 대해 하나의 고장수목을 구성하여 처리 가능하며, 기존의 PSA에서 안전계통용으로 구성된 모델을 초기사건 모델에도 사용이 가능하다.
- 초기사건 빈도 모델과 안전계통 모델이 곱해진 것도 서로간의 의존성이 자동적으로 처리되므로 한번에 최소단절집합을 구할 수 있다.

울진 3,4호기 및 영광 5,6호기 PSA 등에서는 Loss of ESWS Train A와 같은 경우에 초기사건에 대해서 고장수목 모델을 구성하여 초기사건 빈도를 산출하고, 사고경위의 빈도 산출을 위해서는 초기사건을 단순히 하나의 값을 처리하였다. 지금까지의 PSA에서는 이러한 방법이 노심손상빈도를 계산하는 데는 별 문제가 없으나, 추후 활성화되는 Risk

Monitor에서는 초기사건 빈도와 계통 모델을 따로 취급하여 평가하여야 하는 문제가 발생할 수 있다. 본 논문에서 제안한 방법은 Risk Monitor 등에서 필수적인 기기의 이용불능(Out of Service) 등을 포함하여 초기사건 모델과 계통 모델을 한번에 처리할 수 있는 기반을 제공하여 PSA 및 Risk Monitor의 모델 및 분석 방법을 용이하게 할 것으로 기대된다.

5. 참고 문헌

[1] L. Xing, et.al., Comparison of Markov Model and Fault Tree Approach in Determining Initiating Event Frequency for Systems with Two Train Configulations, Reliability Engineering and Systems Safetym Vol. 53, pp 17-30, 1996

[2] Reliability Engineering and Risk Assessment, p331, E. Henley, Prentice-Hall Inc., 1981

[3] Reliability Analysis and Prediction : A Methodology Oriented Treatment, p729, Krishna B. MISRA, Elsevier Science Publishers B.V., 1992

[4] 고장수목을 이용한 계통 고장률 평가 방법 개발, 한상훈, 박진희, 한국원자력연구소, KAERI/TR-2712/2004, 2004