

## 리스크 정보에 의거한 정지불능예상과도사고 분석

### Analysis of Risk-Informed ATWS

김명기, 오혜철, 이재용, 하상준  
전력연구원  
대전광역시 유성구 문지동 103-16

#### 요약

원자력발전소에서 원자로 정지조건이 발생할 경우, 제어봉이 노심으로 낙하되어 부 반응도를 야기시켜 원자로는 안전하게 정지된다. 그러나 원자로 정지계통 기기 고 장이 발생하면 제어봉 삽입이 안되어 노심손상까지 유발시킬 수 있는 사고로 전개 되며 이런 사고를 정지불능예상과도사고라 불리운다. 정지불능예상과도사고가 발생 하면 순간적으로 1차계통의 압력이 설계압력인 3200psi 이상으로 과압되어 1차계통 이 파단되고 노심이 노출되어 결국은 노심손상이 일어난다. 이런 사고의 리스크는 안전계통의 작동유무와 가압기압력방출밸브 작동여부 및 노심의 핵설계 변수 중 하나인 감속재온도계수에 의존한다. 본 연구에서는 정지불능예상과도 사고가 발생하 였을 때 안전계통의 작동유무와 핵 설계 변수의 조건에 따라 리스크를 분석하는 방 법을 제시하고, 또한 역으로 리스크 정보를 활용하여 안전성이 저해되지 않는 범 위 내에서 핵설계 완화 가능성을 제시하고자 한다.

#### Abstract

Where the conditions of reactor trip occur, the trip signal cause the control rods assemblies to drop into the reactor which adds up the negative reactivity resulting in safely shutdown. But the failure of reactor trip system which does not trip the reactor, causes core damage, which is called as an anticipated transient without scram (ATWS). ATWS immediately increases pressure of the primary system over the Level C pressure 3200psi, breaching the primary system pressure boundary, and finally causing core damage. The risk induced by ATWS depends on safety systems actuation, the number of the pressurizer pressure relief valves, and the parameters of core design. In the paper,

we propose the method of risk-informed ATWS considering the safety systems and the parameters of core design and the possibility of relaxation of core design while maintaining risk neutral.

## 1. 서론

원자력발전소에서 원자로 정지조건이 발생할 경우 원자로 정지계통은 제어봉을 노심으로 낙하시켜 노심에 부반응도를 첨가함으로써 원자로는 안전하게 정지된다. 그러나 원자로 정지계통이 고장이 나고 연이어 다중의 안전계통이 고장이 나면 노심손상까지 유발시킬 수 있는 사고로 전개되며 이런 사고를 정지불능예상과도사고(ATWS)라 불리운다. ATWS 사고는 현재 설계기준사고에 포함되어 있지 않다. ATWS 사고가 발생하면 순간적으로 1차계통의 압력이 1차 계통 설계압력인 3200pai 이상으로 과압되어 1차계통이 파단되고 결국은 노심이 노출되어 노심손상이 일어난다. 이런 ATWS 사고의 심각성을 인식한 미국 원자력위원회는 1984년 10CFR50.62로 정지불능예상과도상태(ATWS)관련 법을 공포하였고 이 법령의 타당성을 SECY-83-293를 통하여 입증하였는데 이 법령에서는 AMSAC의 설치와 발전소 고유의 과도현상을 줄이도록 요구하였다. 이에 따라 미국 원전 사업자는 각 발전소에 AMSAC을 설치하였으며 ATWS 사고의 가능성을 줄이는 데 노력 해왔다. 모든 가압경수로원전에 AMSAC (ATWS Mitigating System Actuation Circuitry) 설치와 CE 및 B&W사 원전의 경우 다중정지계통(Diverse Scram System, DSS) 설치를 의무화하였다. 국내 웨스팅하우스 원전에 대해서는 현재 AMSAC을 설치하였거나 설치 중에 있으며 한국표준형 원전은 DPS(Diverse Protection System)가 설치되어 있다. 그러나 원자로 노심이 장주기로 설계됨에 따라 핵설계의 변화로 정지불능예상과도사고로 인한 노심손상 빈도가 증가함을 보이게 된다.

이런 사고의 리스크는 안전계통의 작동유무와 가압기압력방출밸브 작동여부 및 노심의 핵설계 변수 중 하나인 감속재온도계수에 의존한다. 본 논문에서는 정지불능예상과도 사고가 발생하였을 때 안전계통의 작동유무와 핵 설계 변수의 조건에 따라 리스크를 분석하는 방법으로 사건수목을 작성하여 위험도를 평가하는 방법을 제시하고, 미국의 리스크 정보 활용 규제를 기준으로 안전성이 저해되지 않는 범위 내에서 핵설계 완화 가능성의 판단 여부를 제시하고자 한다.

## 2. 본론

ATWS사고에 따른 리스크를 정량적으로 평가하기 위해서는 발전소의 출력상태에 따라 리스크가 달라지므로 크게 다음과 같은 모드에서 리스크를 분석하여야 한다.

상태 1 : 발전소 기동 (지논 불평형) 출력 < 40% (AMASC 작동안함)

상태 2 : 발전소 기동 (지논 불평형) 출력  $\geq$  40% (AMASC 작동)

상태 3 : 출력운전 (지논 평형) 출력  $\approx$  100% (AMASC 작동)

상태 4 : 정지 (지논 평형) 출력  $\geq$  40% (AMASC 작동)

상태 5 : 정지 (지는 평형)

출력 < 40% (AMASC 작동안함)

그러나 정성적으로 보면 상태 3/4에서의 ATWS 사고의 리스크가 가장 큰 값을 가지므로 본 분석에서는 발전소 상태 3를 분석 대상으로 하며 노심 설계가 Low 노심, High 노심, 경계(Bounding) 노심 세 가지 경우에 대하여 분석한다.

### 사건수목 개발

정지불능사고 초기사고가 발생할 경우 안전계통의 작동여부에 따라 사고 진행 사건수목은 그림 1에서 보는 바와 같으며 사고수목의 각 표제는 다음과 같다.

IE : 정지불능 과도사건

RT : 원자로 정지 신호

OMG : 전원에 의한 제어봉 구동계통의 M-G 세트 전원 차단

CRI : 제어봉 구동계통의 제어봉 삽입

CR : 원자로 정지에 충분한 수의 제어봉 낙하

AMSAC : 원자로 정지불능 완화계통 작동

AFW100 보조급수계통 100% 공급 (AFW100)

AFW50 보조급수계통 50% 공급 (AFW50)

SR : 증기발생기를 통한 증기 방출 (SR)

PR : 1차 계통 압력방출 (PR)

LTS : 비상방산수주입을 통한 장기정지조치 (LTS)

본 사건수목은 자동 원자로 정지가 요구되는 과도사건으로부터 시작한다. 자동 원자로 정지기능이 실패할 때 원자로 노심의 출력은 이차측 열부하에 종속적으로 열출력을 생산하게 된다. 자동 원자로 정지신호가 발생한 이후에 대해 가정된 사건수목이기 때문에 초기사건 발생과 동시에 주급수는 차단된다고 본다.

주급수가 공급되지 않는 상태에서 원자로 정지가 이루어지지 않으면 증기발생기 수위는 급격히 감소한다. 이에 따라 원자로 냉각재계통의 압력과 온도는 급격히 증가하게 된다. 증기발생기의 수위가 더욱 감소하여 증기발생기 세관이 노출될 경우에는 이차측으로의 열전달이 더욱 어렵게 된다. 이로 인해 원자로 냉각재계통의 온도와 압력이 지속적으로 증가하게 되어 결과적으로 가압기 방출밸브와 안전밸브들을 통하여 원자로 냉각재를 방출하게 된다. 가압기가 냉각재로 충전이 되어 증기 대신에 원자로 냉각재가 방출하게 되면 가압기 방출밸브를 통한 방출 기능이 더욱 저하된다.

정지불능 과도사건에 있어 운전원은 원자로를 정지시킬 수 있는 모든 조치를 취하여야 한다. 원자로 냉각재계통의 압력을 ASME Level C 수준 이하로 유지하여 계

통 기기 건전성이 유지되도록 하여 비상봉산수주입을 통해 원자로 정지를 수행한다. 운전원의 조치로 인하여 제어봉이 원자로 노심을 미입계로 유지할 만큼 충분히 삽입이 된 경우를 제외하고는 이차측을 통한 열제거와 함께 비상봉산수주입 과정을 통하여 원자로를 미입계로 안정되게 유지하도록 하여야 한다.

## 사건수목 성공기준

### 1) 과도사건 (IE)

ATWS 사고를 유발시킬 수 있는 초기사고인 과도사건을 말한다. 고리 1호기의 과거 10년간 원자로 정지이력은 2.2/Ry회이나 최근 몇 년간에는 불시정지가 없는 것으로 나타나 있다. 이는 고리 1호기의 원자력발전소가 최근 많은 설비개선으로 발전소가 안정화되어 있음을 말하고 있다. 본 분석에서는 연간 불시정지 빈도를 1회로 간주하여 분석한다.

### 2) 원자로 정지 신호(RT)

이 표제는 원자로보호계통의 고장으로 인해서 원자로 정지신호가 발생되지 않는 경우이다. 고리 1호기 원자로 보호계통은 Foxboro 공정계측계통, 원자로 보호 및 논리계전기 캐비닛, 원자로 정지 스위치기어로 구성되어 있다. 일반적으로 과도사건시에 발전소 조건에 따라 다중 원자로 정지신호가 만들어지며 이 중 하나의 신호만이라도 건전하다면 원자로는 정지하게 된다. 일반적으로 원자로 정지 미발생 이용불능도 분석에 있어서는 다중의 원자로 정지신호 미발생 확률을 구하는 것이 아니라 보수적으로 두개의 정지신호 미 발생 확률을 구한다. 본 분석에서도 이와 같이 두개의 원자로 정지신호 미 발생 확률을 고장수목 분석을 통하여 분석한 NUREG/CR-5500의 분석결과를 사용한다. NUREG/CR-5500 보고서에 의하면 주 제어실에서 운전원에 의한 원자로 수동정지를 모델링하였는데 운전원 인간오류를 0.5로 간주하였을 때 원자로 보호계통의 이용불능도 값은  $5.5E-6/Ry$ 로 나타났다. 전체 이용불능도 중 트레인 및 아날로그 채널에 의한 원자로 정지신호 미 발생 이용불능도는  $2.73E-6$ 으로 나타나있다. 따라서 본 표제인 원자로 정지 신호 이용불능도 값은  $2.73E-6$ 을 사용한다.

### 3) 운전원에 의한 제어봉 구동계통의 M-G 세트 전원 차단 (OMG)

운전원은 전동기-발전기 세트(motor-generator set)로부터 제어봉 구동계통으로 공급되는 480V AC의 XSW-3A 및 XSW-3B 전원을 차단시킴으로써 원자로를 정지시킬 수 있다. 이렇게 제어봉 구동계통의 전원을 차단하여 원자로를 정지시킨다하더라도 적당수의 제어봉이 원자로에 삽입되어야 원자로를 성공적으로 정지시킬 수 있다. 즉 본 표제가 성공이 되면 후속으로 충분한 제어봉이 원자로에 삽입이 되었는지를 물어본다. 만약 본 표제의 확률값은 원자로 정지 신호(RT) 표제에 포함되어

있는 운전원 오류와 연관이 있다. 만약 원자로 정지 신호 미발생 원인이 아날로그 채널이나 로직 상의 고장에 기인한다면 운전원은 원자로 정지 신호가 없는 상황에서 MG세트에서 원자로를 정지하여야 하므로 운전원의 원자로 정지 성공 확률은 매우 적다. 이 경우 본 분석에서는 운전원 실패 확률을 0.5로 간주한다. 그리고 원자로 정지 신호 미발생의 원인이 원자로 정지 차단기에 기인한 것이라면 운전원은 원자로 정지신호를 감지하고 있는 상황에서 MG세트를 사용하여 원자로를 정지하는 행위이므로 이때 운전원의 실패확률은 매우 적다. 본 분석에서는 이때 운전원 오류확률 값을 0.01로 간주한다.

#### 4) 제어봉 구동계통의 제어봉 삽입 (CRI)

정지불능 과도사건 시에 제어봉 구동계통의 운전 모드는 자동 모드 혹은 수동 모드 둘 중의 하나의 운전모드에 있을 수 있다. 만약 제어봉 계통이 수동모드에 있으면 운전원은 수동으로 제어봉을 삽입하여야 하고 자동 모드에 있을 경우에는 제어봉은 자동으로 원자로에 삽입되며 필요에 따라 운전원은 제어봉을 더 삽입할 수도 있다. 초기사건이 발생된 후 이런 운전원의 행위는 매우 짧은 시간에 이루어져야 1차측 과압을 방지할 수 있다. 물론 제어봉이 삽입이 안 될 경우에는 보조급수계통과 냉각재 압력방출에 따라 1차측 냉각재 압력은 좌우된다. 이 표제에서 다루고 있는 제어봉 삽입은 리드뱅크의 72스텝이 삽입되는 것을 다루는 데, 이는 제어봉이 1분 동안 삽입되는 스텝수이다. 이 표제를 고려하는 이유는 제어봉 삽입 여부에 따라 UET의 값이 변하기 때문이다. 제어봉 구동 계통의 제어봉 삽입 (ARI)이 실패하는 경우에는 충분한 제어봉의 삽입 사건(CR)이 포함된 것으로 간주한다. 본 분석에서는 CRI 값을 0.5라 간주하였다. 이는 보수적으로 제어봉 운전모드가 수동으로 되어 있고 이때 운전원이 제어봉 삽입 실패 확률을 0.5라고 평가하여 사용한 값이다.

#### 5) 원자로 정지에 충분한 수의 제어봉 낙하 (CR)

운전원이 수동으로 제어봉 구동계통으로의 전원을 M-G 세트를 이용해 차단했다고 하더라도, 원자로의 미임계 상태 유지에 필요한 충분한 수의 제어봉이 낙하하는 데는 실패할 확률이 존재한다. 이에 CR은 원자로 정지 상태를 유지할 만큼의 충분한 수의 제어봉 낙하 확률을 성공 모드로 가정한다. NUREG/CR-5500 보고서에 의하면 10개 이상의 제어봉이 낙하되면 원자로가 정지되어지는 것으로 분석하고 있다. 따라서 본 분석에서는 CR의 값을 NUREG/CR-5500 보고서에서 제시한 확률 값인  $1.2E-06/d$ 의 값을 사용한다. 그러나 본 표제인 CR이 실패일 경우는 충분한 수의 제어봉이 삽입이 되지 않은 경우이기 때문에 리드뱅크가 72스텝 삽입되었다고 가정한다. 이는 UET의 계산에 영향을 준다.

#### 6) 원자로 정지불능 완화계통 작동 (AMSAC)

정지불능 완화계통인 AMSAC은 터빈정지신호와 보조급수펌프 기동신호를 원자로

정지계통과 별도로 생성한다. 성공 모드는 정지불능 완화계통인 AMSAC의 정상 작동 사건을 나타내면 계통 고장확률은 보수적으로 0.01로 간주한다.

#### 7) 보조급수계통 100% 공급 (AFW)

UET(Unfavorable Exposure Time, 핵연료 1주기 운전 기간동안 ATWS 사고가 발생하였을 경우 1차계통의 압력이 ASME Service Level C를 초과하는 시간)를 계산하는 데 있어 보조급수계통의 용량이 100%일 때와 50%가 공급되었을 때를 별도로 분석한다. 이에 대응하기 위하여 보조급수계통의 표제를 100% 공급과 50% 공급으로 나누어 사건수목을 작성한다. 본 표제는 보조급수계통의 100% 용량을 공급하는 표제이다. 고리 1호기의 경우에는 100% 용량의 터빈 구동 보조급수펌프와 50%의 용량을 가지고 있는 전동기구동 보조급수펌프 2대가 설치되어있다. 본 표제의 성공기준은 2대의 전동기구동 보조급수펌프를 사용하여 보조급수를 공급하거나 혹은 1대의 터빈구동 보조급수펌프를 사용하여 보조급수를 공급하는 경우이다.

#### 8) 보조급수계통 50% 공급 (AFW50)

본 표제는 보조급수계통의 50% 용량을 공급하는 표제이다. 고리 1호기의 경우에는 100% 용량의 터빈 구동 보조급수펌프와 50%의 용량을 가지고 있는 전동기구동 보조급수펌프 2대가 설치되어있다. 본 표제의 성공기준은 1대의 전동기구동 보조급수펌프를 사용하여 보조급수를 공급하는 경우이다.

#### 9) 증기발생기를 통한 증기 방출 (SR)

증기발생기로 급수가 공급되면 원자로 냉각재계통의 핵분열로 인한 원자로 노심 잔열이 증기발생기 세관을 통해 이차측 급수로 전달된다. 이렇게 전달된 열은 증기발생기에서 증기로 바뀌어 대기방출 혹은 복수기방출로 이어져 열을 제거하게 된다. 열제거를 위해 증기방출에 이용되는 증기방출밸브는 증기발생기의 대기증기방출밸브, 복수기증기방출밸브 및 주증기 안전밸브가 있다.

따라서, SR의 성공기준은 임의의 1/2 증기발생기의 대기증기방출밸브, 복수기증기방출밸브 및 주증기안전밸브를 통하여 증기를 방출해 이차측 계통 열제거에 성공하는 것이다.

#### 10) 1차계통 압력방출 (PR)

본 표제는 1차계통의 과압을 방지한 1차측 압력방출을 나타낸다. 1차측 압력 방출 결정은 보조급수계통 급수용량(100%, 50%)과 제어봉 삽입여부(리드뱅크 72스텝 삽입 혹은 실패)에 좌우된다. PR은 UET와 가용한 가압기 PORV 수 그리고 안전밸브의 고장에 따라 확률값을 결정지을 수 있다. 본 표제의 값을 정하기 위하여 고장수목을 작성하여 계산하였다. 고장수목은 총 4개로 각 고장수목의 정점사건은 다음과 같은 조건에서의 1차측 계통 압력방출이 실패할 경우이다.

- PRA 조건: 제어봉 삽입 성공, 100% 보조급수 공급
- PRB 조건: 제어봉 삽입 성공, 50% 보조급수 공급
- PRC 조건: 제어봉 삽입 실패, 100% 보조급수 공급
- PRD 조건: 제어봉 삽입 실패, 50% 보조급수 공급

상기 고장수목의 정점사건 PR 값은 UET기간을 다음과 같이 구분하여 고장수목을 통하여 분석한다.

- UET 기간 1: 2개 PORV 밸브와 2개 안전밸브가 작동해도 압력방출 실패
- UET 기간 2: 압력방출을 위해서는 2개 PORV 밸브와 2개 안전밸브 필요
- UET 기간 3: 압력방출을 위해서는 1개 PORV 밸브와 2개 안전밸브 필요
- UET 기간 4: 압력방출을 위해서는 0개 PORV 밸브와 2개 안전밸브 필요

상기 분석을 위한 핵설계 자료는 웨스팅하우스 일반 원전의 자료를 사용하였으며 분석결과 PRA, PRB, PRC3, PRD는 Low 노심일 경우  $3.67E-2$ ,  $4.33E-2$ ,  $1.45E-1$ ,  $2.32E-1$ 로, High 노심 경우  $5.29E-2$ ,  $1.67E-1$ ,  $2.82E-1$ ,  $3.2E-1$ 로, 경계노심 경우는  $2.61E-1$ ,  $2.88E-1$ ,  $3.36E-1$ ,  $3.65E-1$ 로 분석되었다.

#### 11) 비상방산수주입을 통한 장기정지조치 (LTS)

제어봉 구동계통이 수동 모드로 설정되어 있거나 혹은 제어봉이 충분히 낮아지지 못하여 미임계를 보장하지 못할 경우에는 비상방산수주입을 시작으로 장기정지냉각을 위한 운전 과정을 발전소 운전원이 수행하여야 한다. 이 표제는 CR, CRI가 성공하였을 경우에는 필요가 없는 것으로 모델링하였는데 이는 CRI이 성공을 한다면 운전원은 계속해서 제어봉을 원자료에 삽입하는 것으로 간주하기 때문이다. 이 표제의 값은 방산수 주입계통의 이용불능도와 운전원의 행위에 좌우하게 된다. 본 분석에서는 운전원 행위를 포함한 계통이용불능도 값인 LTS 이용불능을 0.144 값을 사용한다.

### 3. 분석 결과

ATWS 사건수목과 각 표제의 고장수목 및 룰 값을 사용하여 Low 노심, High 노심, 경계노심에 대하여 KIRAP 전산코드를 사용하여 노심손상빈도를 분석하였다. 그림 1의 사건수목 최종 발전소 상태 중 ATWS사고로 인한 정지불능예상사고에 대해서만 노심손상으로 간주하였으며 노심은 정지된 후 다른 계통의 가용여부에 따라 노심손상을 유발시킬 수 있는 사고추이(1, 11, 22, 30)는 더 이상 ATWS 사고의 범주로 간주하지 않았다. 분석결과 각 노심손상빈도는  $4.02E-7/Ry$ ,  $5.48E-7/Ry$ , 그리고  $1.13E-6/Ry$ 로 나타났다. 분석결과 중 가장 보수적인 노심인 경계노심의 경우를 보면 정지불능예상과도사건에 의한 노심손상빈도는 다른 모든 초기사건(냉각제 상실사고들 및 과도사건들)에 의한 전체 노심손상빈도의 1% 미만으로 나타났다.

#### 4. 결론

본 논문에서는 ATWS 사고 위험도를 평가하기 위해 UET 개념을 사용하여 고장수목과 사건수목을 작성하여 분석하였다. 분석결과 ATWS로 인한 노심손상빈도는 전체 노심손상빈도의 1% 미만으로 평가되었다. 이는 미국의 위험도 정보 활용 규제 지침인 RG-1.174를 판단 지침으로 사용할 경우, 현재 고리 1호기에서 진행 중인 설비개선 사항을 감안할 때 ATWS에 의한 위험도는 허용 가능한 범위에 들어와 현재 설치된 ANMSAC으로 정지불능예상과도사건에 의한 안전성은 확보되었다고 말할 수 있다.

#### 참고문헌

1. “WOG Risk-Informed ATWS,” WCAP-15831, Westinghouse, 2002, 7.
2. “고리 1호기 확률론적 안전성 보고서(내부사건),” 한수원(주), 2002. 11,

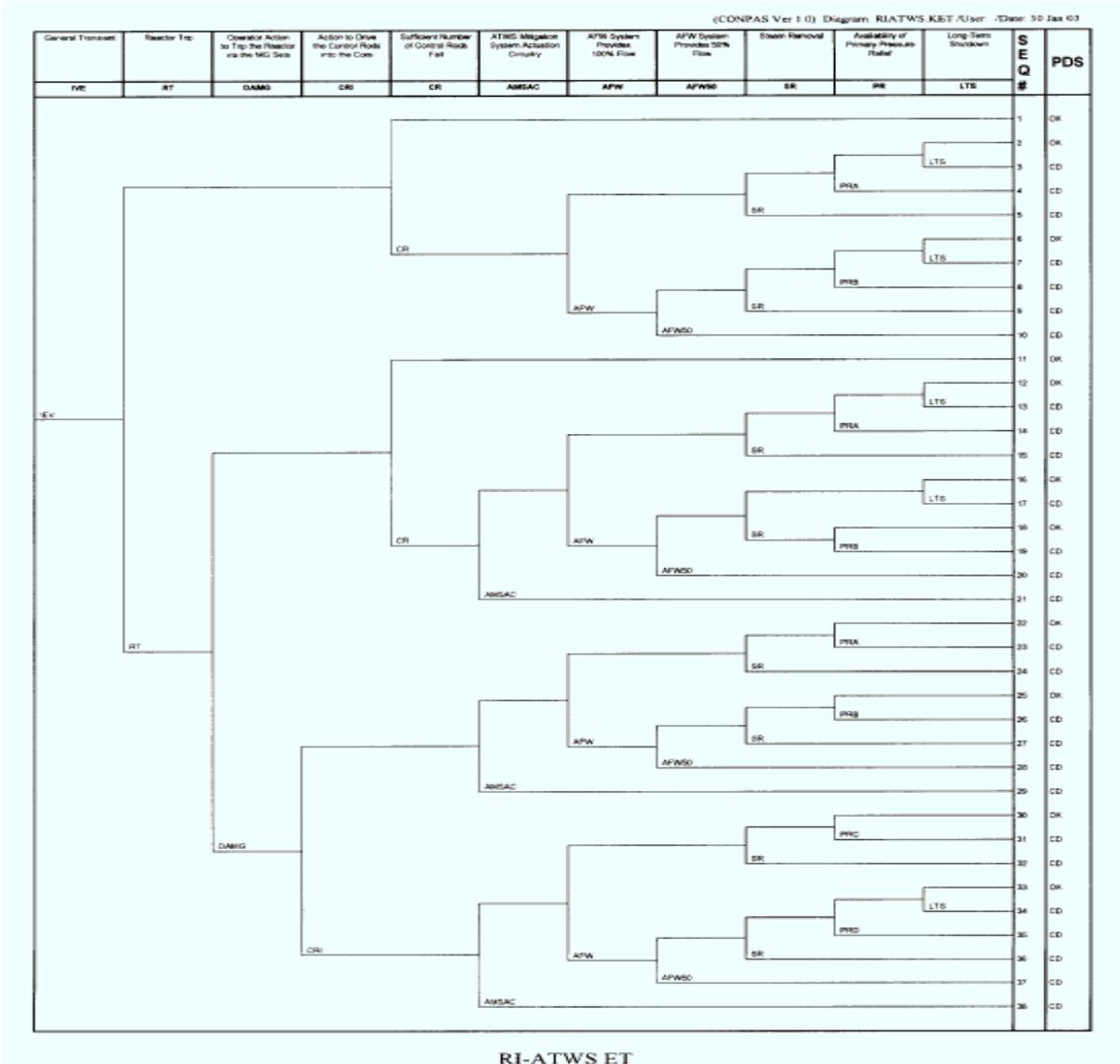


그림 1 정지불능예상과도사건 사건수목