KAERI/TR-2548/2003

확률론적안전성평가 (PSA) 수행 절차서

- 1단계 전출력 내부사건분석 -

Procedure for Conducting Probabilistic Safety Assessment

- Level 1 Full Power Internal Event Analysis -

한국원자력연구소

제 출 문

한국원자력연구소장 귀하

본 보고서를 " 위험도 정보 활용 기반 기술 개발" 과제의 PSA 표준 모델 개발에 대한 기술보고서로 제출합니다.

2003년 7월

주 저 자 : 정원대

공 저 자 : 이윤환, 황미정, 한상훈, 장승철, 강대일, 박진희, 양준언, 김태운, 하재주, 진영호

요 약 문

확률론적 안전성평가(Probabilistic Safety Assessment; PSA)는 대상 시스템의 안전성을 확률적으로 평가하는 기법이다. WASH-1400 보고서를 통하여 원자력발전소의 안전성 평가에 처음으로 도입된 후, 지금은 원자력발전소 뿐만 아니라 일반 산업체의 안전성 평가에까지 널리 사용되고 있다. 원자력발전소에 대해 수행되는 PSA는 분석의 범위에 따라, 다음과 같이 1단계 PSA, 2단계 PSA, 3단계 PSA로 구분된다.

- 1단계 PSA : 발전소 내의 사고로 인한 노심 손상빈도를 결정한다.
- 2단계 PSA : 1단계 PSA결과를 이용하여 격납용기의 반응을 평가하고, 궁극적으로는 격납용기 밖으로의 방사능 유출빈도를 결정한다.
- 3단계 PSA : 2단계 PSA결과를 이용하여 발전소 외부에서의 사고 결과를 평가하고, 최종적으로 위험도를 추정한다.

본 기술보고서는 1단계 PSA 내부사건 분석 절차와 방법을 정리한 것이다. 한국원자력연구소에서 한국 표준형 원전의 건설 및 운영 인허가와 관련하여 수행하였던 1단계 PSA의 분석 방법과 절차를 보고서로 만들었다. 1단계 PSA는 원자력발전소에서 발생할 수 있는 노심손상 사고 시나리오를 파악하고 그로 인한 노심손상 빈도를 평가하는 작업으로서, PSA에서 가장 기본적이고 핵심적인 업무이다. 또한 1단계 PSA는 발전소 기계적 설비의 신뢰성을 분석하고, 설계 및 운영에 대한 안전성을 평가하고 개선하는데 직접적으로 활용된다. 따라서 PSA를 활용하는 실무 부서에서는 1단계 PSA가 가장 필요한 내용이며, 또한 최근에 활발히 논의되고 있는 위험도 정보 활용(Risk-Informed Application)에 직접적으로 사용되는 부분이다.

1단계 PSA는 크게 발전소 친숙화, 초기사건 분석, 사건수목 분석, 계통 고장수목 분석, 신뢰도 자료 분석, 그리고 정량 분석의 단계로 수행된다. 본 기술보고서에는 1단계 PSA의 전체적인 개요를 2장에서 소개하고 있으며, 3장에서부터 7장까지 앞에서 언급한 1단계 PSA의 기술적 단계를 차례로 다루고 있다. 각 단계의 기술적 업무에 필요한 방법과 수행 절차 그리고 참고문헌을 체계적으로 정리함으로써 PSA를 활용하고자 하는 실무자들에게 직접적인 도움을 줄 수 있도록 작성하였다.

본 기술보고서는 원자력발전소의 PSA를 직접 수행하거나 다루어야 하는 실무자를 대상으로 만든 것이나 PSA 결과를 검토하는 관리자나 규제 담당자에게도 적절한 지침으로 사용될 수 있다. 또한 본 보고서에서 소개하는 분석 방법과 절차는 화학공장과 같은 일반 산업체의 안전성 평가에도 유용하게 사용될 수 있을 것이다.

SUMMARY

Probabilistic Safety Assessment(PSA) is a conceptual and mathematical tool to evaluate numerical estimates of risk for nuclear power plants (NPPs). After the first comprehensive application of the method, Reactor Safety Study (WASH-1400), PSA has become a standard tool in safety evaluation of not only NPPs but industrial installation. According to the analysis scope, PSA for NPPs consists of Level I, II, and III as follows.

- Level I PSA : The assessment of plant failures leading to the determination of core damage frequency.
- Level Ⅱ PSA : The assessment of containment response leading, together with Level I results, to the determination of containment release frequencies.
- Level Ⅲ PSA : The assessment of off-site consequences leading, together with the results of Level 2 analysis, to estimates of public risks.

This report provides guidance on conducting a Level I PSA for internal events in NPPs, which is based on the method and procedure that was used in the PSA for the design of Korea Standard Nuclear Plants (KSNPs). Level I PSA is to delineate the accident sequences leading to core damage and to estimate their frequencies. It has been directly used for assessing and modifying the system safety and reliability as a key and base part of PSA. Also, Level I PSA provides insights into design weakness and into ways of preventing core damage, which in most cases is the precursor to accidents leading to major accidents. So Level I PSA has been used as the essential technical bases for risk-informed application in NPPs. The report consists six major procedural steps for Level I PSA; familiarization of plant, initiating event analysis, event tree analysis, system fault tree analysis, reliability data analysis, and accident sequence quantification.

The report is intended to assist technical persons performing Level I PSA for NPPs. A particular aim is to promote a standardized framework, terminology and form of documentation for PSAs. On the other hand, this report would be useful for the managers or regulatory persons related to risk-informed regulation, and also for conducting PSA for other industries.

목 차

그 림 목 차

표 목 차

제1장 서 론

확률론적 안전성평가(Probabilistic Safety Assessment; PSA)가 국내에 도입되어 본격적으로 원자력발전소 안전성 평가에 사용된 것도 벌써 15여년이 넘었다. 이제까지는 주로 원전의 건설과 운영을 위한 인허가 과정의 하나로서 PSA가 수행되었으나 최근에 와서는 위험도 정보를 활용하여 규제와 운영 관리를 최적화 하려는 움직임이 활성화되면서 PSA의 활용 범위가 확산되고 이에 따라 PSA를 실무적으로 다루어야 하는 사람들도 많아졌다. 이에 따라 이제까지 국내 일부 기관에서만 수행하였던 PSA의 기술적 방법과 절차를 체계적으로 정리함으로써 새롭게 PSA 기술을 익히고자 하는 사람들을 돕기 위하여 이 보고서를 작성하게 되었다.

본 기술보고서는 1단계 PSA 내부사건 분석 절차와 방법을 정리한 것이다. 한국원자력연구소에서 한국 표준형 원전의 건설 및 운영 인허가와 관련하여 수행하였던 1단계 PSA의 분석 방법과 절차를 보고서로 만들었다. 여기서 소개하는 1단계 PSA 절차서는 원자력발전소를 대상으로 개발된 것이나, 제시된 분석 방법과 절차는 화학공장과 같은 일반 산업설비의 안전성평가에도 적용할 수 있다.

원자력발전소에 대해 수행되는 PSA는 분석의 범위에 따라 다음과 같이 세 단계로 구분된다.

- 1단계 PSA(Level I PSA): 노심손상 사고경위를 분석하고 노심 손상 빈도를 평가한다.
- 2단계 PSA(Level Ⅱ PSA): 1단계 PSA 결과를 이용하여 노심손상 이후 격납건물의 건전성을 평가하고, 격납건물 밖으로의 방사능 유출 빈도를 평가한다.
- 3단계 PSA(Level Ⅲ PSA): 1, 2단계 PSA 결과를 이용하여 격납건물 밖으로 유출된 방사능 물질로 인하여 주민과 환경에 미치는 위험도를 평가한다.

본 기술보고서는 1단계 PSA에 초점을 맞추고 있다. 1단계 PSA는 노심손상 사고경위와 발생 빈도를 분석하는 것으로서, 원전의 안전성을 평가하기 위해 가장 기본적이고 필수적으로 수행되는 부분이다. 1단계 PSA는 발전소 기계적 설비의 신뢰성을 분석하고, 설계 및 운영에 대한 안전성을 평가하고 개선하는데 직접적으로 활용된다. 따라서 PSA를 실제로 활용하는 실무 부서에서는 1단계 PSA가 가장 필요한 내용이며 또한 최근에 활발히 논의되고 있는 위험도 정보 활용(Risk-Informed Application)에 직접적으로 사용되는 부분이기 때문에 본 기술보고서에는 여기에 초점을 맞추어 기술하였다. 1단계 PSA는 원전의 운전 상태에 따라 다시 전출력 PSA와 정지/저출력 PSA로 구분할 수 있고, 사고가 시작되는 사건의 성격에 따라 내부사건 PSA와 외부사건

PSA로 구분할 수 있다. 본 보고서에서는 그 중에서도 PSA에 가장 기본이 되는 전출력 운전의 내부사건에 대한 PSA를 다루고 있다.

1단계 PSA는 발전소 친숙화, 초기사건 분석, 사건수목 분석, 계통 고장수목 분석, 신뢰도 자료 분석, 그리고 정량 분석의 단계로 수행된다. 본 기술보고서에는 1단계 PSA의 전체적인 개요를 2장에서 소개하고 있다. 3장에서는 발전소 친숙화 및 초기사건 분석을, 4장에서는 사건수목 분석을 언급함으로써 노심손상을 유발하는 사고 시나리오를 도출하는 과정을 설명하고 있다. 5장 계통 고장수목 분석에서는 계통의 이용불능도를 평가하기 위하여 개발하는 계통별 고장수목의 구성 방법과 절차를 예제를 곁들여 상세히 기술하였다. 6장에서는 1단계 PSA에 모델되는 인간신뢰도 분석과 공통원인고장 분석을 포함하여 모든 기본사건의 신뢰도를 분석하는 절차와 방법을 소개하고 있으며, 마지막으로 7장에서는 앞에서 분석된 모든 정보를 통합하여 노심손상 사고경위 빈도를 계산하는 정량분석 과정을 상세히 정리하였다.

제2장 1단계 PSA 분석 개요

제1절 개요

1. 목적

본 내부사건 분석 개요에서는 원자력발전소의 확률론적안전성평가(PSA) 중에서 전출력 내부사건 분석의 내용을 간략히 정리하였다. 본 개요에서는 Level 1 PSA 내부사건 분석에 포함된 초기사건 분석, 사건수목 분석, 계통 고장수목 분석 및 정량 분석 내용을 간략히 소개하여 중대사고에 대한 원전의 안전성을 종합적으로 평가할 수 있는 지침을 제공하고자 한다.

2. 적용 범위

본 1단계 PSA 내부사건 분석 절차서는 한국표준원전에 대하여 한국원자력연구소에서 수행하였던 설계 중 원전 PSA 과제에서 적용한 분석 절차와 방법을 정리한 것이다. 따라서 본 절차서에 기술된 분석 방법 및 수준은 이제까지 국내에서 수행한 인허가 원전의 PSA에 준하는 것으로서, 향후 설계 중 원전 PSA에 적용할 수 있을 것이다.

3. 참고문헌

PSA 내부사건 분석에 대한 참고문헌은 분석 분야별로 각 장에서 기술하고 있다.

4. 기본가정 및 용어정의

본 절차서는 설계 중인 원전인 영광 5,6호기 전출력 Level 1 PSA의 내부사건 분석에 적용하기 위해 작성한 절차서로서 그 동안 국내에서 수행되었던 설계 중 원전 PSA 방법에 근거하여 작성한 것이다. 외부사건 분석이나 정지/저출력 PSA는 본 절차서에서 다루고 있지 않다.

내부사건 분석에 사용되는 주요 용어는 분야별 상세 절차서에 기술된 바와 같다.

제2절 분석 절차

1단계 PSA는 노심손상 사고경위와 빈도를 분석하는 것으로서, 발전소 설계와 운영에 대한 안전성을 평가하고 개선하는데 직접적으로 활용되는 부분이다. 1단계 PSA는 그림 1에 정리된 바와 같이 발전소 친숙화, 초기사건 분석, 사건수목 분석, 계통 분석 및 신뢰도 자료 분석, 그리고 정량 분석의 단계로 수행된다.

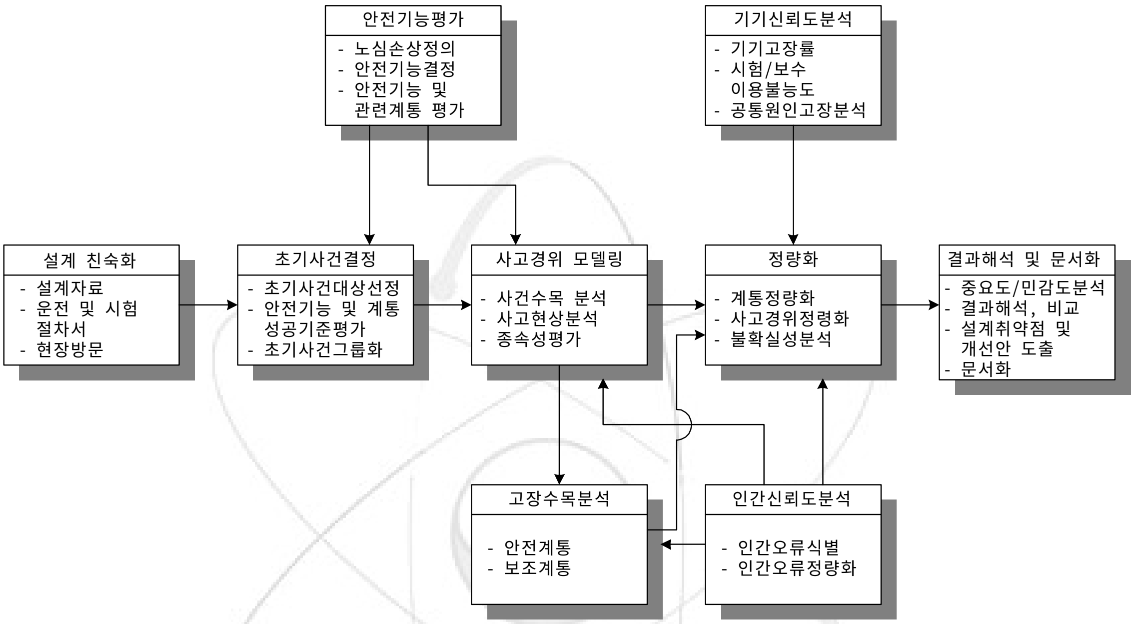


그림 1. 1단계 PSA 내부사건 분석 절차

1. 초기사건 분석

사고경위를 결정하기 위한 첫번째 단계는 원전의 노심손상을 초래할 수 있는 사고 시나리오들에 대한 초기사건을 선정하는 것이다. 초기사건이란 정상 운전 중인 발전소의 불시 원자로 정지를 초래하는 기기 혹은 계통의 이상이나 인간 행위를 의미한다. 원자로 정지란 운전 변수들이 적정 운전 범위를 벗어나는 경우에 취해지는 보호 조치이다. 따라서 초기사건이 발생하면 원자로의 보호 및 사고 방지를 위하여 안전 계통들이 작동하여 원자로를 정지시키고 노심의 잔열을 제거하여 원자로를 안전하게 유지한다.

초기사건에는 원전 내부적 요인에 의한 것과 지진, 홍수 등과 같은 외부적 요인에 의한 것이 있으나 본 내부사건 분석에서는 내부적 요인에 의한 초기사건만을 대상으로 하였다. 내부적 요인에 의한 초기사건은 기본적으로 다음과 같은 2 가지 부류로 구분할 수 있다.

- 원자로냉각재 상실(LOCA) : 원자로냉각재계통의 냉각수 상실을 초래하는 일차 계통의 파손(Rupture) 이나 파단(Break) 사고로서, 파손 부위의 크기나 위치 혹은 방사성 물질의 격납건물 밖으로의 누출 가능성 등에 따라서 원자로냉각재 상실 사고는 다시 몇 가지로 보다 세분화된 초기사건으로 구분된다.
- 과도사건(Transient) : 원자로냉각재 상실 사고가 아니면서 원자로 정지를 초래하고 노심의 건전성을 유지하기 위해 관련 안전계통의 작동을 필요로 하는 사건으로서, 이차측 혹은 보조계통의 사용 여부에 따라 몇 개의 보다 세분화 된 초기사건으로 구분된다.

세부적인 초기사건은 다음과 같은 수행절차에 따라 결정한다. 먼저 발전소의 안전기능(Safety Function)을 저해할 수 있는 가능한 사고 유형들을 논리적으로 추적하기 위해 주 논리도(Master Logic Diagram)를 개발하고, 다음 단계에서는 앞에서 파악된 사고 유형에 대한 구체적 목록을 작성한다. 이 단계에서는 운전 및 사고 경험의 분석, 주요 기기에 대한 고장모드 분석, 타 발전소 PSA의 초기사건 목록 검토 등을 통하여 발생 가능한 모든 초기사건의 목록을 작성한다. 마지막 단계에서는 사고 유형이나 진행 과정이 유사하며, 이들 사고로부터 원자로를 안전하게 정지시키기 위해 필요한 안전계통 및 그 성공 기준이 동일한 초기사건을 그룹화하여 최종 초기사건을 결정한다. 보다 자세한 내용은 3장에 기술하였다.

2. 사건수목 분석

사건수목 분석이란 선정된 초기사건에 대하여 사건수목을 구성하여 노심손상을 초래하는 모든 중요 사고경위를 논리적으로 밝혀내는 과정이다. 이를 위해서 각 초기사건 별로 노심을 건전한 상태로 유지하기 위해 필요한 안전기능을 파악하고 작동이 요구되는 안전계통 및 운전원 조치를 사건수목의 표제로 정의하여 각 표제의 성공 혹은 실패에 따라 이분수목(Binary Tree) 형태로 사고 시나리오를 전개하여 발생 가능한 노심손상 사고경위를 논리적으로 구성한다.

노심을 안전한 상태로 유지하기 위해서는 안전기능이 유지되어야 하는데, 사건수목 개발 시에 고려한 안전기능은 다음과 같다.

- 반응도 조절 (Reactivity Control)
- 원자로냉각재 재고량 유지 (RCS Inventory Control)
- 원자로냉각재 압력 조절 (RCS Pressure Control)
- 노심 및 원자로냉각재 열 제거 (Core and RCS Heat Removal)

다음으로는 위에서 언급한 안전기능을 유지하기 위해 필요한 계통들을 파악하고 이를 사건수목 표제로 정의한다. 또한 초기사건에 따른 각 계통들의 성공기준 및 작동 시점도 결정한다. 표제 배열의 순서는 결과에 큰 영향을 미치지는 않지만 분석의 효율성과 사건전개의 이해 관점에서는 매우 중요하다. 시간, 기능 및 계통 간의 연관성 등이 주요 고려 인자이며, 가능한 관련 계통의 작동 시간 순으로 표제를 배열하는 것이 일반적이다. 각 표제의 성공 기준 및 사고 전개에 따른 시간 정보는 안전성분석보고서의 사고해석 결과 및 열수력 분석 결과 등에 근거하여 결정된다.

각 초기사건에 대한 계통 및 성공기준, 표제 순서 등을 결정한 후, 이들 표제의 성공 혹은 실패에 따라 각 초기사건에 대하여 발생 가능한 모든 사고경위를 논리적으로 도출한다. 모든 사고경위는 최종적으로 노심손상 혹은 원자로 안전 정지와 같은 둘 중 하나의 상태로 종결된다.

보다 자세한 내용은 4장 사건수목 분석 절차서에 기술하였다.

3. 계통 고장수목 분석

사건수목 분석 시에 모델한 계통의 신뢰도를 평가하기 위하여 고장수목 분석 기법을 사용하여 계통 분석을 수행한다. 고장수목이란 계통이 필요한 기능을 수행하지 못하는 상태 즉, 이용 불능한 상태가 되는 모든 경우를 AND, OR 혹은 NOT의 논리 게이트를 사용하여 연역적으로 도식화 한 논리 수목이다. 기기의 기계적 고장, 공통원인고장, 인간오류, 시험 및 보수에 기인한 이용 불능 등을 계통 고장수목 모델에 포함한다.

계통 고장수목 분석을 위해서 먼저 각 계통의 정점사건을 정의한다. 정점사건이란 계통이 필요한 기능을 성공적으로 수행하지 못하는 사건으로, 초기사건 및 사고경위 분석 과정에서 결정된다. 계통의 성공 기준은 초기사건 및 사고 전개 과정에 따라 달라지며, 이에 따라 동일 계통에 대해서도 여러 개의 정점사건이 정의될 수 있다. 다음에는 정의된 각 정점사건의 원인을 연역적으로 추적하여 고장수목을 전개한다. 고장수목의 논리 전개는 유용한 신뢰도 자료가 있는 최소 기기 단위까지 수행되며, 이 최소의 단위를 기본사건(Basic event) 이라 한다. 고장수목 구성 시에 고려되는 계통 고장의 원인에는 기기의 기계적 고장, 공통원인고장, 인간오류 그리고 시험 및 보수로 인한 기기 이용불능과 같은 기본사건이 포함된다:

본 PSA 내부사건 분석 절차서에서는 소형 사건수목/대형 고장수목 방식에 따라 사고경위를 도출하며, 직접적으로 사고 완화에 관련된 전위 계통만을 사건수목 표제로 하고 보조계통의 고장수목은 전위계통 계통 고장수목의 하부 논리로 연결하여 계통 간의 상호 연계성을 모델링 한다.

계통 고장수목 구성 후 정량화 코드를 사용하여 계통 이용불능도를 계산하며, 이 과정을 통하여 계통 모델에 대한 정성, 정량 분석을 수행한다. 정성적 분석 단계에서는 고장수목에 대한 정량화 분석 결과인 최소 단절집합(Minimal Cutset)을 검토함으로써 고장수목의 논리적 타당성을 검토한다. 최소 단절집합이란 계통 정점사건을 초래하는 기본사건 들의 조합으로서, 최소 단절집합 중에서 논리적으로 맞지 않는 것이 있는지 혹은 누락된 최소 단절집합은 없는지 등을 정성적 분석 과정을 통하여 확인하게 된다.

정량적 평가는 계통의 이용불능도를 평가하는 단계로, 이용불능도란 계통의 작동이 요구되는 특정 시점에서 작동하지 않거나 주어진 작동 시간 동안 운전하지 못할 평균 확률 값을 의미한다. 앞에서 구한 정점사건에 대한 모든 최소 단절집합에 기본사건의 확률을 대입하여 계통 이용불능도를 산출한다. 계통분석 절차에 대한 자세한 내용은 내부-04 계통 고장수목 분석 절차서에 기술되었다.

4. 신뢰도 데이터 분석

신뢰도 데이터 분석은 사건수목과 고장수목에 모델링 된 모든 기본사건에 대한 신뢰도 자료를 분석하는 과정이다. PSA 결과의 정확도는 사용 데이터의 신뢰도에 직접적인 영향을 받으므로 데이터 분석 및 데이터베이스 개발은 PSA의 핵심 연구 내용 중 하나이다. PSA를 수행하는데 필요한 신뢰도 데이터는 다음과 같은 것들이 있다.

- 초기사건 빈도
- 기기고장률
- 공통원인고장확률
- 인간오류확률
- 보수/시험 빈도 및 기간

데이터 분석은 PSA 연구의 특성에 따라 분석 범위가 상당히 달라질 수 있다. 운전 중인 발전소에 대한 PSA인 경우에는 발전소 고유 운전 이력을 조사하여 분석에 반영해야 하기에 많은 인원과 시간을 투입하여 운전 데이터 및 고장 데이터를 수집, 분석하여야 한다. 그러나 대부분의 경우에는 직접 이용 가능한 데이터를 생산할 만한 적절한 양의 고장 자료를 찾을 수 없기 때문에 일반 데이터 (Generic Data)와 발전소 고유 데이터 (Plant Specific Data)를 통계적으로 처리하여 사용하고 있다.

이에 비하여 설계 중인 원전에 대한 PSA는 운전 이력이 없으므로 일반데이타원을 근거로 한 데이터베이스 구축 혹은 기 개발된 것을 선택하여 사용하게 된다. 일반데이타원으로는 해외 원전의 데이터를 근거로 개발된 일반 데이터베이스(예, ALWR URD data base , NUCLARR 등)와 국내 타 원전의 운전 이력을 근거로 한 신뢰도 데이터가 있다.

일반 데이터베이스를 개발하기 위해서는 많은 수의 데이타원을 수집, 분석하여야 하며, 특히 다음 사항을 점검하여야 한다.

- 기기의 물리적 경계(Component Boundary) 및 고장모드(Failure Modes)
- 데이터 산출 근거
- 데이터 산출에 사용한 수학적 모델, 절차 및 가정 사항
- 불확실성 분석

자세한 내용은 5장 신뢰도 데이터 분석 절차서에 기술된 바와 같다.

5. 정량 분석

정량화 단계에서는 이전 단계에서 수행된 모든 결과물을 조직적으로 통합하여, 노심손상을 초래하는 모든 기본사건의 조합을 도출하고 그로 인한 노심손상빈도를 정량적으로 평가한다. 정량화 시의 연구 내용은 각 사고경위에 대한 boolean 수식을 구하고, 이를 통하여 해당 사고경위를 일으키는 최소 단절집합 (초기사건과 기본사건의 조합)들을 파악한 후, 초기사건 발생 빈도와 각 기본사건의 발생 확률을 대입하여 사고경위 발생 빈도를 구하는 것이다. 모든 사고경위에 대한 정량화 결과를 합하면 총 노심손상빈도가 계산된다. 또한 각 사고경위에 대한 최소 단절집합을 검토하여 사건수목 및 고장수목 전개논리가 적절히 모델링 되었는지를 확인하는 정성 분석도 이 단계에서 함께 수행한다.

PSA 정량화는 일반적으로 예비 정량화와 최종 정량화 두 단계에 거쳐 수행한다. 설계에 대한 개념적 평가나 주요 영향 인자를 파악하기 위하여 간략한 모델과 보수적 데이터를 사용하여 예비 분석을 수행하며, 예비 정량화 결과를 근거로 사건수목과 고장수목에서 도출된 논리적 혹은 신뢰도 데이터 사용의 문제점을 수정하여 최종 정량화를 수행한다. 최종 정량화 단계에서는 운전원의 복구 조치가 가능한 일부 최소 단절집합에 대한 운전원 회복조치 분석(Recovery Analysis)도 포함된다. 또한 사용 데이터의 불확실성을 고려한 불확실성 분석, 주요 영향 인자 및 설계 개선 항목에 대한 민감도 분석도 정량화 분석의 일부로 수행된다. 자세한 내용은 6장 정량분석 절차서에 기술하였다.

제3장 초기사건 분석

제1절 개요

1. 목적

본 계통분석 절차서는 원자력발전소의 확률론적 안전성평가 (Probabilistic Safety Assessment : 이하 PSA) 시 사용되는 초기사건분석 절차와 기법을 기술하여 PSA 수행 시 노심손상을 초래할 가능성이 있는 모든 초기사건을 일관성 있고 기술적으로 정확하게 선정하는 지침을 제공하고자 한다.

2. 적용 범위

본 초기사건분석 절차서는 설계 중인 원전에 대하여 그 동안 국내에서 수행되었던 PSA의 초기사건분석 절차 및 방법을 기본적으로 정리하였다. 따라서 본 절차서에 기술된 분석 방법 및 수준은 국내의 설계 중 원전 PSA에 적용된 초기사건 분석에 준하는 것으로서, 향후 설계 중 원전 PSA에 적용할 수 있을 것이다.

3. 참고문헌

초기사건 분석에 대한 참고문헌으로는 여러 종류가 있으나, 본 절차서를 작성하기 위해 참고한 대표적인 문헌은 다음과 같다.

[1]"PRA Procedure Guide", NUREG/CR-2300", ANS and IEEE, 1982.

[2]"Probabilistic Safety Analysis Procedures Guide", NUREG/CR-2815, 1984.

[3]"Procedures for Conducting Probabilistic Safety Assessment of NPPs (Level 1)", IAEA, 1992.

[4]"고리 3,4 호기 및 영광 1,2 호기 PSA 수행절차서", 한국전력공사, 1992.

[5]"영광 5, 6 호기 확률론적 안전성 평가 보고서", 한국전력공사, 2001

4. 기본가정 및 용어정의

본 절차서는 설계중인 원전인 영광 5,6호기 전출력 Level 1 PSA에 적용하기 위해 작성한 절차서로서 그 동안 국내에서 수행되었던 설계중인 원전 PSA의 초기사건분석 방법에 근거하여 작성한 것이다. 따라서 만일 운전중인 원전의 초기사건분석이나 전출력 이외의 운전모드에서의 초기사건분석을 위해서는 필요에 따라 일부 내용을 수정하여 사용할 수 있다.

초기사건분석에서 사용되는 주요 용어는 다음과 같다.

PSA	확률론적 안전성 평가
노심손상빈도	노심손상 사고가 발생할 수 있는 빈도로 1년 단위로 계산된다.
사고경위	사건수목에서 계통 작동유무에 따라 전개되는 사고 시나리오. 하나의 사고경위는 어떠한 초기사고가 발생한 후 어떠한 계통들이 작동하였고 어떠한 계통들이 실패하였는지에 따라 정해진다.
초기사건	원전 정상운전 중 이상사태를 발생시킬 수 있는 사고. PSA에서는 유사한 사고들을 그룹화하여 하나의 초기사건으로 처리하며, 대부분의 경우 원자로 정지로 이어지는 사고만을 취급한다.
정점사건	계통이 특정 운전 조건에서 필요한 기능을 성공적으로 수행하지 못하는 사건
과도사건	정상출력 운전 중 기기 혹은 운전원 조치 실수에 의해 계통운전 변수의 변화를 초래하여 원자로 정지를 유발하는 사건
냉각재상실사고	일차계통 압력경계의 파손에 의해 발생되는 냉각재 상실사고 중 충전계통의 냉각재 보충능력을 초과하는 모든 사건

제2절 분석 절차

1. 안전기능의 정의

안전기능 (Safety Function) 이란 발전소내의 에너지원과 방사선 사고를 관리하는데 필요한 기능을 말한다. 안전기능의 개념은 초기사건의 선정과 사고추이 규명의 기준으로서 사용된다. 일반적인 안전기능은 노심용융방지, 격납건물 파괴방지 및 방사성

물질 방출의 최소화 등의 동작을 말한다. 이러한 안전기능은 자동 혹은 수동으로 작동하는 여러 계통들과 원자로 고유의 부반응도 등으로 달성된다.

안전기능은 발전소 형태, 계통 설계, 계통 반응시간 및 분석자의 선호 등에 따라 여러가지 방법으로 정의될 수 있다. 표 1은 전형적인 안전기능들과 그 목적을 보여주고 있다. 특별히 안전기능은 계층적 구조로 생각할 수 있다. 반응도 제어 (Reactivity Control) 는 노심으로부터 제거되어야 할 열량을 결정하는 첫번째 기능이다. 다음의 기능은 노심냉각 기능이다. 노심냉각은 원자로 냉각재계통내의 재고량 유지와 적절한 원자로 냉각재 계통의 압력 유지를 위하여 노심으로부터 유량 공급을 요구한다. 이와 같은 논리를 통하여 발전소에 대한 기본 안전기능의 구조를 수립한다. 안전기능의 정의는 초기사건의 그룹화에 사전 기준을 제공하며, 또한 각 초기사건에 대한 각 계통의 반응과 계통간의 상호작용에 대한 정보를 제공한다. 또한 안전기능은 초기사건에 따라 다르게 정의될 수 있다. 예를 들면 원자로 냉각재계통의 냉각재 유지기능은 대부분의 과도사건(Transient)에서는 원자로 냉각재계통의 건전성 (Intergity) 유지가 필요하나 냉각재 상실사고에서는 보충수의 공급이 필요하다.

표 1. 안전기능과 목적

안 전 기 능	목 적
Reactivity Control	Shut reactor down to reduce heat production
Reactor Coolant System Inventory Control	Maintain a coolant medium around the core
Reactor Coolant System Pressure Control	Maintain the coolant in the proper state
Core Heat Removal	Transfer heat from the core to a coolant
Reactor Coolant System Heat Removal	Transfer heat from the core coolant
Containment Isolation	Close openings in containment to prevent radionuclide releases
Containment Temperature and Pressure Control	Keep from damaging containment and equipment
Combustible Gas Control	Remove and redistribute hydrogen to prevent and explosion inside containment

* From Corcoran et al. (1980)

2. 초기사건의 선정

초기사건이란 사고진행의 시작점을 말하며 사고는 원전에서 원자로보호계통의 작동을 요구하거나 혹은 이상 신호등으로 제어봉이 삽입된 경우등을 말한다. 사고경위 모델링에 있어 중요한 점의 하나는 가능한 한 모든 사고경위를 모델링하고 분석해야 한다는 점이다. 그러나 발전소에서의 발생 가능한 모든 사고경위를 모델링하여 분석하는 것은 현실적으로 불가능한 일이다. 따라서 사고경위 모델링에 있어 가능한 한 모든 사고경위를 분석하고 업무량도 감소시킬수 있도록 다음 초기사건의 정의 및 식별 과정을 통하여 초기사건을 선정한다.

가. 초기사건의 정의 및 식별

초기사건의 정의는 앞에선 언급한 바와같이 원자로보호계통의 작동이 요구되거나 이상 신호등으로 제어봉이 삽입된 경우를 말하는 것으로 이 단계에서는 상기 사고들을 야기시키는 '이차측급수상실' 등과 같이 구체적인 사고경위 상태를 정의하는 것이다. 또한 사고경위 모델링의 완벽성을 기하기 위하여 앞에서 정의된 초기사건 중 발생 가능한 모든 초기사건을 찾아내는 것이 필요하다. 이러한 초기사건의 식별을 위하여 보통 다음 3가지의 방법이 사용되고 있다. 이 세가지 방법들은 서로 독립적으로 사용되는 것이 아니고 서로 보완적으로 사용하여 초기사건 선정에 완벽을 기하는데 그 목적이 있다.

- 경험적 평가 (Comprehensive Engineering Evaluation)
- 논리적 평가 (Logical Evaluation)
- 고장모드효과분석 (Failure Mode and Effect Analysis)

(1) 경험적 평가

이 방법은 과거에 검토대상 발전소나 타 발전소에서 발생하였던 사고 또는 타 발전소 PSA 보고서에 나타난 사고들을 평가하여 검토대상 발전소에서 발생 가능한 초기사건을 도출하는 것이다. 초기사건은 경험에 따라 통상 LOCA와 과도사건(Transient)으로 구분되며 LOCA는 파단크기에 따라 대형, 중형, 혹은 소형 LOCA로 구분한다. 그러나 과도사건(Transient)은 발전소 형태 등 여러 조건에 따라 그 분류가 복잡하다. 원자력 발전소의 대표적인 과도사건 목록이 표 2에 정리되어 있다.

표 2. 발전소 초기사건 목록 (과도사건)

1. Loss of RCS flow (one loop)	21. Feedwater flow instability-operator error
2. Uncontrolled rod withdrawal	22. Feedwater flow instability-miscellaneous mechanical causes
3. Problems with control-rod drive mechanism and/or rod drop	23. Loss of condensater pumps (one loop)
4. Leakage from control rods	24. Loss of condensater pumps (all loops)
5. Leakage in primary system	25. Loss of condenser vacuum
6. Low pressurizer pressure	26. Steam generator leakage
7. Pressurizer leakage	27. Condenser leakage
8. High pressurizer pressure	28. Miscellaneous leakage in secondary system
9. Inadvertent safety injection signal	29. Sudden opening of steam relief Valves
10. Containment pressure problems	30. Loss of circulation water
11. CVCS malfunction-boron dilution	31. Loss of component cooling
12. Pressure, temperature, power imbalance-rod-position error	32. Loss of service-water system
13. Startup of inactive coolant pump	33. Turbine trip, throttle valve closure, EHC problems
14. Total loss of RCS flow	34. Generator trip or generator-caused faults
15. Loss or reduction in feedwater flow (one loop)	35. Loss of all offsite power
16. Total loss of feedwater flow (all loops)	36. Pressurizer spray failure
17. Full or partial closure of MSIV (one loop)	37. Loss of power to necessary plant systems
18. Closure of all MSIVs	38. Spurious trips-cause unknown
19. Increase in feedwater flow (one loop)	39. Automatic trip-no transient condition
20. Increase in feedwater flow (all loops)	40. Manual trip-no transient condition
	41. Fire within plant

* From ATWS: A Reappraisal, Part 3 (EPRI, 1982).

(2) 논리적 평가

이 방법은 사건수목분석시에 사용하는 고장수목의 논리적 모델을 다량의 방사능 누출등과 같은 발전소 안전성 관점에서의 정점사건등에 적용하여 논리적으로 여러 단계를 거쳐 초기사건을 도출하는 방법이다.

PRA Procedure Guide (NUREG/CR-2300) 에서는 정점사건을 "Excessive Offsite Release"로 하여 모델을 세웠으며 이를 "주 논리도 (Master Logic Diagram)" 라 명명하였다. 그림 2에 이를 나타내었다. 그림에서 보는 바와같이 Level 2에서는 방사능 누출 경로를 직접 및 간접으로 분류하였고 Level 3에서는 방사능 장벽을 노심손상, RCS 압력 경계파손 및 격납건물파손 등으로 분류하였다. Level 4에서는 원전의 안전기능으로 분류하였다. Level 5에서는 Level 4의 안전기능으로부터 각각의 초기사건을 도출할 수 있음을 나타내었다. 그러나 초기사건의 도출을 위한 논리적 평가를 수행할 때에 PSA 수행시마다 정점사건과 초기사건 도출까지의 단계가 일정하지 않다. 어떤 경우에는 중간단계를 생략하고 반응도제어, 노심열제거 등과 같은 안전기능을 정점사건으로 취하기도 한다. 또한 정점사건의 종류나 분류방법에 따라 다른 명칭을 부여하고 있다. 예를 들면 Seabrook 발전소 PSA 보고서에서는 "발전소 열평형 고장수목 (Plant Energy Balance Fault Tree)" 이라 하여 발전소에서의 생성열과 제거열간의 불평형을 정점사건으로 하며 논리적 모델을 세워 추가적으로 초기사건을 도출하였고 만산발전소 PSA 보고서에서는 "Hirarchical Structure for Determining Initiating Event"라 하여 "원자로정지"를 정점사건으로하여 논리적 모델을 세워 초기사건을 도출하였다.

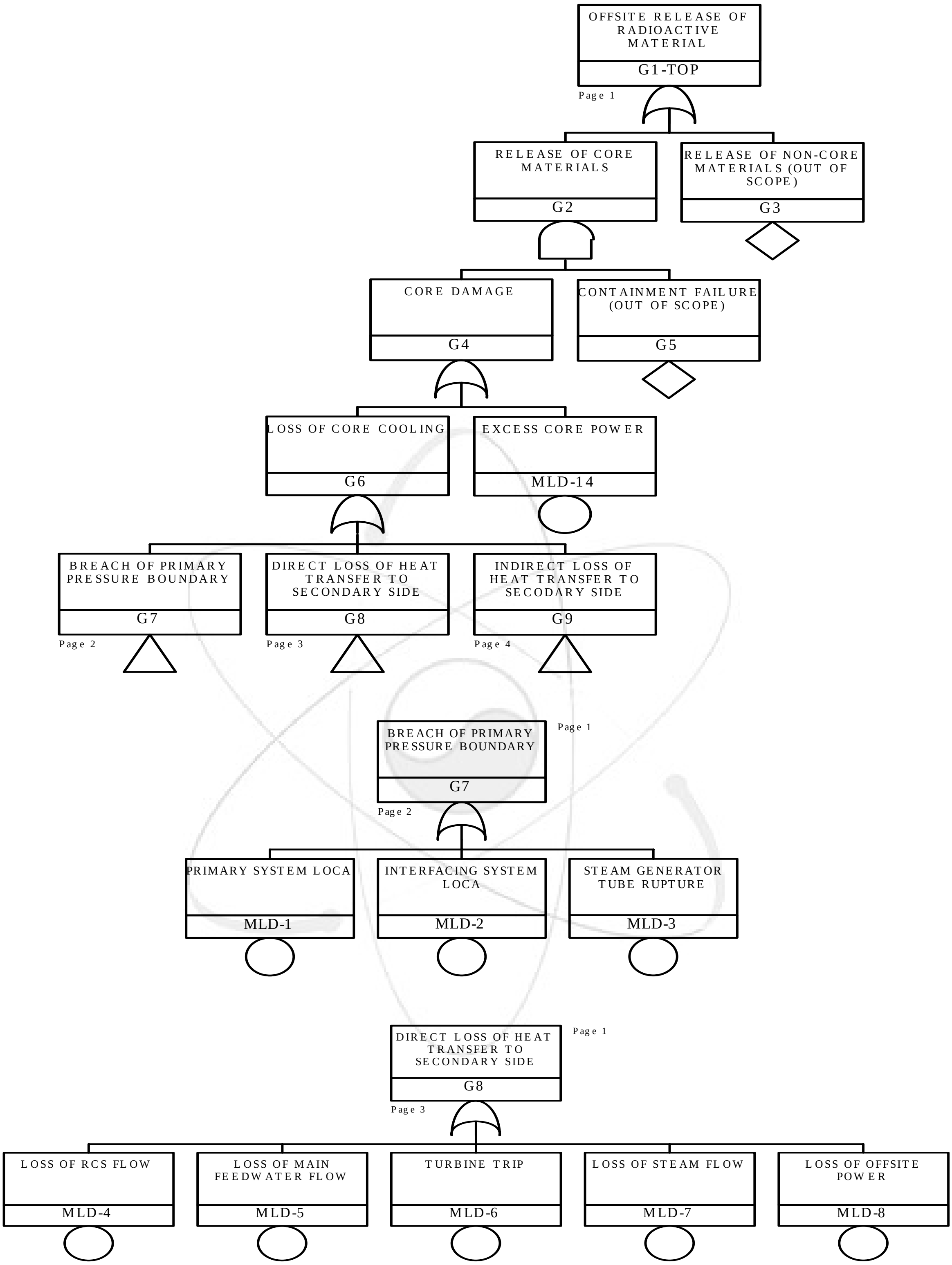

OFFSITE RELEASE OF RADIOACTIVE MATERIAL
G1-TOP
Page 1
RELEASE OF CORE MATERIALS
G2
RELEASE OF NON-CORE MATERIALS (OUT OF SCOPE)
G3
CORE DAMAGE
G4
CONTAINMENT FAILURE (OUT OF SCOPE)
G5
LOSS OF CORE COOLING
G6
EXCESS CORE POWER
MLD-14
BREACH OF PRIMARY PRESSURE BOUNDARY
G7
Page 2
DIRECT LOSS OF HEAT TRANSFER TO SECONDARY SIDE
G8
Page 3
INDIRECT LOSS OF HEAT TRANSFER TO SECODARY SIDE
G9
Page 4
BREACH OF PRIMARY PRESSURE BOUNDARY
G7
Page 1
Page 2
PRIMARY SYSTEM LOCA
MLD-1
INTERFACING SYSTEM LOCA
MLD-2
STEAM GENERATOR TUBE RUPTURE
MLD-3
DIRECT LOSS OF HEAT TRANSFER TO SECONDARY SIDE
G8
Page 1
Page 3
LOSS OF RCS FLOW
MLD-4
LOSS OF MAIN FEEDWATER FLOW
MLD-5
TURBINE TRIP
MLD-6
LOSS OF STEAM FLOW
MLD-7
LOSS OF OFFSITE POWER
MLD-8

그림 2. 주 논리도 예

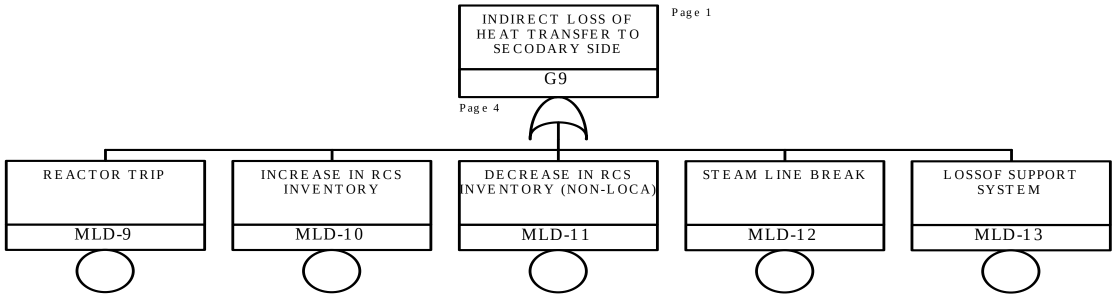


그림 2. 주 논리도 예 (계속)

(3) 고장모드 효과분석

초기사건의 도출을 위한 또 하나의 방법으로 고장모드 효과분석 (FMEA: Failure Mode and Effects Analysis) 이 있다. 앞에서 언급된 초기사건 도출방법은 발전소 사고의 정점사건인 안전기능, 1차안전계통 (Front-Line System) 등에 관심을 두고 경험 혹은 논리적 모델을 통하여 정점하향식 (Top-Down) 으로 초기사건을 도출한다. 그러나 FMEA는 상기방법과는 반대로 발전소 사고의 하부구조 즉 전기공급 계통, 계측설비 등과 같은 보조계통 (Support System)등에 관심을 두고 이들의 고장으로 인한 영향을 정성적으로(필요시 정량적) 분석하여 기정상향식 (Bottom-Up) 으로 초기사건을 도출하는 것이다. FMEA는 초기사건을 도출하는 것 이외에도 주요 계통이나 안전기능간의 상호작용, 쉽게 알기가 어려운 보조계통 (Support System) 들 사이 혹은 보조계통과 1차안전계통 사이의 상호작용 등에 대하여 쉽게 알 수 있도록 한다.

FMEA 방법 적용시에는 대상 계통의 기기별로 기기의 기능, 발생 가능한 고장모드 및 고장원인, 고장 감지 방법, 기기고장으로 인해 계통 또는 발전소에 미치는 영향 등을 검토하게 되고 최종적으로 원자로의 불시정지를 초래하는지 분석하여 초기사건의 대상 여부를 판정한다.

표 3은 초기사건의 도출을 위해 기기냉각수계통(CCWS)을 대상으로 적용한 FMEA의 한 예를 보여준다. 기기냉각수계통의 트레인 A에는 펌프 01A와 펌프 02A가 있는데, 펌프 01A는 평상 시 운전 중이고 펌프 02A는 대기 상태에 있다. 운전 중 펌프 01A가 정지하게 되면 펌프 출구 저압력 신호에 의해 펌프 02A가 자동으로 기동하게 되어 있다. 만일 펌프 02A 마저 고장나면 기기냉각수계통의 트레인 A는 기능을 상실하게 되며, 이로부터 냉각수를 공급받던 모든 원자로냉각재펌프가 정지되고 이로인해 원자로 정지가 발생한다.

표 3. FMEA 예

기기명	기능	고장모드	고장원인	고장징후 및 국부적 영향	고장 감지 방법	고장영향	초기사건 대상 여부
CCWS 펌프 01A	트레인 A 기기냉각수 공급 (운전 중)	Fail to run	기계적고장, 전력공급상실, 펌프룸 냉각상실	펌프01A 출구 모관 저압력 및 저유량	펌프출구 저압력 신호 발생 (MCR)	펌프02A 기동신호 발생	CCWS 펌프 01A/ 02A 동시 고장 (CCWS 트레인 A 상실) 시 초기사건 대상
CCWS 펌프 02A	트레인 A 기기냉각수 공급 (대기 중)	Fail to start Fail to run	기계적고장, 전력공급상실, 기동신호상실 기계적고장, 전력공급상실, 보수오류, 펌프룸 냉각상실	펌프02A 출구 모관 저압력 및 저유량	펌프출구 저압력 신호 발생 (MCR) 열교환기출구온도지시계	CCWS 트레인A 기능상실로 모든 원자로각재펌프 정지 및 원자로 정지	

나. 안전기능과 계통상호 연관성 평가

본 절차에서는 사고 시 각 안전기능을 수행하기 위해 요구되는 각 계통을 확인하여야 한다. 통상적으로 이러한 안전기능을 수행하는 계통을 1차 안전계통 (Front-Line System) 이라 하며, 1차 안전계통을 지원하는 계통을 보조계통 (Support System) 이라 한다. 본 과정에서는 모든 1차 안전계통들이 안전기능을 수행하기 위해 독립적 또는 상호 연관적으로 작동되는가를 확인하여야 하며, 이를 위해서 모든 1차 안전계통의 목록이 작성되어야 한다. 참고로 각 안전기능 수행 시 요구되는 1차 안전계통을 표 4에 나타내었으며, 일반 가압경수로의 1차 안전계통 목록은 표 5에 나타낸 바와 같다.

1차 안전계통과 보조계통 간의 상호 연관성을 평가하기 위해서는 일단 1차 안전계통 및 보조계통 간의 종속성 표를 작성한다. 작성된 종속성 표로부터 보조계통의 목록을 확인하며, 이러한 보조계통의 수행에 필요한 기타 계통들도 보조계통의 목록에 추가시키도록 한다. 최종적으로 이러한 1차 안전계통과 보조계통 간의 종속성을 통해 안전기능을 수행하는 모든 1차 안전계통에 영향을 미치는 모든 계통들이 확인된다. 보조계통 간의 종속성도 상기 설명된 종속성 표에 의해 설명될 수 있다.

상기 과정을 통해 최종적으로 다음과 같은 결과물을 얻을 수 있다.

- 각 초기사건에 따른 안전기능과 1차 안전계통의 안전기능 및 계통상호 연관성
- 1차 안전계통의 목록
- 보조계통의 목록
- 1차 안전계통과 보조계통 간의 종속성 표
- 보조계통 간의 종속성 표

상기 분석과정에서 확인된 계통들은 사고경위 분석 및 계통분석 과정에서 분석되어야 한다.

표 4. 안전기능과 관련 1차 안전계통

Safety Function	Front Line Systems
Control reactivity	(a) Reactor protection system (b) High pressure injection system
Remove core decay heat and stored heat	(a) Power conversion system (b) Emergency feedwater system (c) High pressure injection system and pressure safety relief valves (d) Low pressure injection system (e) Residual heat removal system
Maintain integrity of primary reactor coolant boundary (pressure control)	Pressurizer safety relief valves
Maintain primary reactor coolant inventory	(a) High pressure injection system (b) Low pressure injection system
Protect containment integrity (isolation, overpressure)	(a) Reactor building spray system (b) Reactor building cooling system
Scrub radioactive materials from containment atmosphere	Reactor building spray system

* From NUREG/CR-2728 (1983)

표 5. 1차 안전계통

1. Reactor Protection System
2. Core Flood System
3. High Pressure Injection / Recirculation System
4. Low Pressure Injection / Recirculation System
5. Reactor Building Spray Injection / Recirculation System
6. Reactor Building Cooling System
7. Power Conversion System
8. Emergency Feedwater System
9. Pressure Safety Relief Valves

* From NUREG/CR-2728 (1983)

다. 초기사건의 그룹화

예비목록에 있는 초기사건 중 각 발전소 설계 특성에 비추어 분석대상에서 제외될 수 있는 초기사건들은 삭제하고, 나머지 예비 초기사건에 대하여 발전소의 거동과 원자로를 안전하게 정지시키기 위해 필요한 안전계통의 기능적 대응에 기초하여 유사한 양상을 보이는 초기사건들은 그룹화하는 것이 필요하다. 그 이유는 모든 초기사건에 대하여 각각의 사건수목을 작성하는데 시간과 노력을 절약하기 위함이다. 즉, 필요안전기능이 비슷한 초기사건들을 한 개의 그룹으로 하고 각 그룹에 대하여 하나의 사건수목을 작성하면 적은 수효의 사건수목을 작성하더라도 모든 초기사건에 대하여 사고경위분석이 가능하다.

초기사건은 크게 두 가지 주요사건 범주의 하나로 분류할 수 있다. 즉 원자로 냉각재 상실사고와 과도사건이다. 원자로 냉각재 상실사고는 일차계통 압력경계의 파손에 의해 발생되는 냉각재 상실사고 중 충전계통의 냉각재 보충능력을 초과하는 모든 사건을 포함한다. 냉각재 상실사고는 파단 위치 및 크기에 근거하여 그룹화한다. 과도사건은 기기파손이나 운전원 조치실패에 의해 발생할 수 있고 사고완화를 위해 원자로의 자동 혹은 수동정지를 필요로 하는 사건으로 직접적인 냉각재 상실을 유발하지 않는 사건을 말한다.

표 6은 일반적인 가압 경수로의 경우 예비초기사건을 그룹화하여 선정된 최종 초기사건을 나타낸 것이다.

3. 문서화

초기사건 분석을 수행한 결과로서 다음과 같은 내용을 문서화한다.

- 예비 초기사건의 목록
- 예비 초기사건 그룹화 후 최종 초기사건 목록
- 각 초기사건에 따른 안전기능과 1차 안전계통의 안전기능 및 계통 상호 연관성
- 1차 안전계통 및 보조계통 목록
- 계통간 종속성 표

표 6. 가압경수로의 초기사건

Large LOCA
Medium LOCA
Small LOCA
Interfacing system LOCA
Steam generator tube rupture
Steam break inside containment
Loss of main feedwater
Trip of one MSIV
Loss of flow in reactor coolant system
Core power excursion
Turbine trip
Turbine trip - loss of off-site power
Turbine trip - loss of service water
Reactor trip
Reactor trip - loss of service water
ATWS
Seismic event
Flooding
Fires

제3절 초기사건 상세 분석 방법

1. 초기사건 분석 과정

본 절에서는 표준 원전을 대상으로 노심손상을 초래할 가능성이 있는 모든 초기사건의 선정에 대하여 기술하였다.

초기사건에는 발전소 내부적 요인에 의한 것과 지진, 홍수 등과 같은 외부적 요인에 의한 것이 있으나 본 전출력 내부사건 분석에서는 100% 출력 운전 중 발전소 내부적 요인에 의해 발생하는 초기사건들만을 대상으로 하였다. 내부적 요인에 의한 초기사건들은 기본적으로 원자로냉각재상실 및 과도사건으로 구분할 수 있다.

세부적인 초기사건은 다음과 같은 네단계의 수행 절차에 따라 결정되었다. 첫째, 영광 5, 6 호기 초기사건 분석을 위해 고려한 안전기능 (Safety Function) 을 정의하였으며, 둘째 단계에서는 발전소의 안전기능을 저해할 수 있는 사고 유형을 논리적으로 추적하기 위해 주논리도 (Master Logic Diagram)를 개발하였고, 운전 및 사고 경험의 분석, 주요 기기에 대한 고장모드분석, 혹은 영광 3,4 호기 PSA 및 울진 3, 4 예비 PSA 초기사건 목록의 검토 등을 통하여 발생 가능한 모든 초기사건을 선정하였다. 셋째 단계에서는 본 절차에서는 사고 시 각 안전기능을 수행하기 위해 요구되는 각 계통을 확인하였다. 마지막 단계에서는 사고 유형이나 전개과정이 유사하며, 노심의 건전성을 유지하기 위해 필요한 안전계통 및 그 성공기준이 동일한 초기사건들을 그룹화하여 최종 초기사건을 결정하였다.

가. 안전기능의 정의

노심을 안전한 상태로 유지하기 위해서 안전기능들이 유지되어야 하는데, 영광 5, 6호기 초기사건 분석 시에 고려된 안전기능은 다음과 같다.

- 원자로 미임계 (Subcritical) 유지
- 노심 붕괴열 제거
  - 원자로 냉각재 유지
  - 원자로 냉각재 유량 유지 (강제 혹은 자연순환 유지)
  - 원자로 냉각재계통으로부터 열 제거
- 원자로 냉각재계통 과압 방지

나. 초기사건의 선정

(1) 주 논리도 구성

주 논리도는 초기사건 범주를 정의하고 초기사건의 선정, 그룹화를 도와주며 초기사건 선정 과정에의 누락 가능성을 줄이기 위해 개발하였다. 그림 2 는 영광 5, 6 호기에 대한 주 논리도를 나타내고 있다. 주 논리도는 가상의 사건과 그 잠재적 원인간의 논리적 관계를 연역적으로 표현한 고장수목 모델이다. '방사성물질의 소외 누출' 같이 가상의 정점사건 (Top Event) 을 정의하고 이 정점사건의 발생을 초래할 수 있는 계통의 고장을 논리적으로 표현함으로써 초기사건 그룹을 파악하였다.

그림 2의 주 논리도는 어떻게 방사성 물질의 소외누출이 '노심물질 누출'이나 '비노심 물질의 누출'로부터 초래될 수 있나를 단계적으로 보여주고 있으며, 비노심 물질의 누출은 본 분석의 영역에 포함되지 않는다. 따라서, 노심물질 누출은 '노심 손상' 혹은 '격납건물의 격납기능 실패'에 의해서만 발생할 수 있다. 그러나 격납건물의 실패로 인한 노심물질 유출도 전출력 내부사건의 초기사건 분석의 대상은 아니다.

따라서, '노심 손상'을 유발하는 사건들이 내부사건의 초기사건 대상이 될 수 있다. 만일 원자로냉각재계통의 열을 적절히 제거하지 못하거나 노심의 과도한 출력을 유발시키는 사건이 발생한다면 노심손상이 일어날 수 있으며, 그 사건들이 초기사건의 대상이 된다. 주 논리도의 4번째 단계는 노심냉각상실과 과잉 노심출력에 대한 전개 논리를 보여주고 있다.

과잉노심출력에 의한 노심손상은 냉각재로 전달될 수 있는 에너지의 비율보다 핵연료 내 생성 에너지가 크기 때문에 발생한다. 개념적으로 이와 같은 과잉출력사건은 과도한 감속재 냉각, 제어봉 인출, 영(0) 출력에서 부적절한 제어봉인출, 붕소희석 등에 기인된다.

5번째 단계는 노심냉각상실에 대한 전개 논리를 보여주고 있다. 노심냉각상실 사건에서 노심손상은 핵연료 손상이 시작될 정도의 시간 이상으로 노심이 노출되기 때문에 발생한다. 노심의 노출은 원자로 냉각재상실로 발생하는데, 원자로냉각재는 일차계통 압력 경계에서 발생하는 파단이나 이차측 열제거 기능 상실 시 일차측 압력 증가에 의해 열리는 가압기 안전밸브를 통해 누출되며, 터빈 트립이나 원자로 트립을 유발시키는 사건과 같은 간접적인 원인에 의해 발생 될 수 있다.

그림 2와 같은 주 논리도를 통해 총 14개의 초기사건 범주를 도출하였다.

(2) 경험에 의한 초기사건 목록

주 논리도를 통해 개념적인 내부 초기사건의 범주를 결정하였다. 그러나 사고경위 분석을 위해서는 보다 구체적인 초기사건 목록을 선정해야 한다. 따라서 이들 일반 범주 각각에 대해서 가능한 모든 초기사건들을 도출하여 예비 초기사건 목록을 개발하기 위해서 예비 초기사건 목록 작성시 EPRI/NP-2230, Oconee PRA 보고서, Millstone PSS 보고서, 고리 3,4 호기 PSA 보고서, 영광 5,6 호기 예비 안전성분석보고서의 6장과 15장에 해석된 초기사건 목록 등을 기초 자료로 사용하였다. 이 중 특히 EPRI 일반 과도사건 목록, Oconee PRA 초기사건 예비 목록 및 영광 5, 6 호기 안전성분석 보고서 6장과 15장에 해석된 사건들이 주요 입력 자료로 사용되었다.

(3) 초기사건의 예비목록 결정

주 논리도를 통해 총 14개의 개념적인 내부 초기사건 범주(표 8)를 결정한 후 이를 일반범주 각각에 대해서 가능한 모든 초기사건들을 도출하였다. 모든 기초자료를 사용하여 예비 초기사건의 예비목록을 결정하였으며, 예비 목록에 있는 초기사건 중 영광 5,6호기의 발전소 설계 특성에 비추어 분석 대상에서 제외될 수 있는 초기사건들과 발전소의 거동과 원자로를 안전하게 정지시키기 위해 필요한 안전계통의 기능적 대응에 기초하여 유사한 패턴을 보이는 초기사건들은 초기사건의 그룹화 단계에서 정리하였다.

다. 안전기능과 계통별 상호 연관성 평가

본 단계에서는 사고 시 각 안전기능을 수행하기 위해 요구되는 각 계통을 확인하였다. 통상적으로 이러한 안전기능을 수행하는 계통을 1차 안전계통 (Front-Line System) 이라 하며, 1차 안전계통을 지원하는 계통을 보조계통 (Support System) 이라 한다. 이 단계에서는 모든 1차 안전계통들이 안전기능을 수행하기 위해 독립적 또는 상호 연관적으로 작동되는가를 확인하였으며, 이를 위해서 모든 1차 안전계통의 목록을 작성하였다. 참고로 표 7에 영광 5, 6호기의 1차 안전계통과 보조계통 목록을 나타내었다.

표 7. 영광 5, 6 호기 전위계통 및 보조계통 목록

구 분	계 통 목 록
전 위 계 통 (Front Line Systems)	고압안전주입계통 (High Pressure Safety Injection System)
	안전주입탱크 (Safety Injection Tank)
	저압안전주입계통 (Low Pressure Safety Injection System)
	정지냉각계통 (Shutdown Cooling System)
	격납건물살수계통 (Containment Spray System)
	안전감압계통 (Safety Depressurization System)
	화학 및 체적제어계통 (Chemical and Volume Control System)
	원자로냉각재 압력조절계통 (Reactor Coolant Pressure Control System)
	보조급수계통 (Auxiliary Feedwater System)
	주급수계통 (Main Feedwater System)
	주증기계통 (Main Steam System)
보 조 계 통 (Support Systems)	공학적 안전설비 작동계통 (Engineered Safety Features Actuation System)
	원자로보호계통 (Reactor Protection System)
	증기발생기 취출계통 (Steam Generator Blowdown System)
	전기계통 (Electrical System)
	기기냉각수계통 (Component Cooling Water system)
	필수용수계통 (Essential Service Water System)
	필수냉수계통 (Essential Chilled Water System)
	공기조화계통 (Heating, Ventilation and Air Conditioning System)
	압축공기계통 (Compressed Air System)

라. 초기사건 그룹화

초기사건 그룹화단계에서는 대상 발전소인 영광 5, 6 호기의 초기사건을 최종적으로 선정하였다. 예비 목록에 있는 초기사건 중 영광 5, 6호기의 발전소 설계 특성에 비추어 분석 대상에서 제외될 수 있는 초기사건들은 삭제하고, 나머지 예비 초기사건에 대하여 발전소의 거동과 원자로를 안전하게 정지시키기 위해 필요한 안전계통의 기능적 대응에 기초하여 유사한 패턴을 보이는 초기사건들을 그룹화하였다. 모든 예비

초기사건에 대한 검토 및 그룹화 결과를 표 9에 정리하였으며, 표 10에 영광 5, 6 호기 PSA의 최종 초기사건을 정리하였다.

초기사건은 2가지 주요 사건 범주의 하나로 분류할 수 있다. 즉, 원자로냉각재 상실사고와 과도사건이다. 냉각재상실사고는 일차 계통 압력 경계의 파손에 의해 발생되는 냉각재상실사고 중 충전계통의 냉각재 보충 능력을 초과하는 모든 사건을 포함한다. 냉각재상실사고는 파단 위치 및 크기에 근거하여 그룹화된다. 과도사건은 기기파손이나 운전원 조치 실패에 의해 발생할 수 있고, 사고완화를 위해 원자로의 자동 혹은 수동정지를 필요로 하는 사건으로 직접적인 냉각재상실을 유발하지 않는 사건을 말한다.

표 8. 주논리도(MLD)에 의한 영광 5,6호기 예비 초기사건 (1/2)

주논리도(MLD)	경험에 의한 방법
MLD-1 : 1차 계통 냉각재상실사고	A-3 제어봉 돌출
	D-1 소형 RCS 배관 파열
	D-2 중형 RCS 배관 파열
	D-3 대형 RCS 배관 파열
	D-4 부적절한 가압기 압력 방출 밸브 개방
	D-5 원자로 냉각재 펌프 밀봉 파손
	D-6 제어봉 밀봉부위 냉각재 누출
	D-7 노심 계측관 파손
	D-10 원자로 본체 파열
MLD-2 : 저압 경계부 냉각재상실사고	D-8 저압 경계부 냉각재상실사고
MLD-3 : 증기발생기 세관파열	D-9 증기발생기 세관파열
MLD-4 : 냉각재계통 유량상실	B-1 한대 또는 그 이상의 원자로 냉각재 펌프 정지
	B-2 원자로 냉각재 펌프 축 고착
	B-3 원자로 냉각재 펌프 축 파단
	B-4 냉각재 유로 막힘
MLD-5 : 주급수 유량상실	C-1 주급수 상실
	C-2 부적절한 주급수 격리밸브 폐쇄
	C-3 부적절한 주급수 공급
	C-4 급수펌프의 정지
	C-6 급수공급의 감소
	C-12 복수기 펌프 정지
MLD-6 : 터빈 정지	C-11 복수기 진공 상실
	C-13 복수기 누설
	C-14 순환수 상실
	C-15 터빈 조절밸브 고장
	C-16 터빈 정지밸브 고장
	C-17 터빈 정지
	C-18 발전기 정지

표 8. 주 논리도(MLD)에 의한 영광 5, 6호기 예비 초기사건 (2/2)

주논리도(MLD)	경험에 의한 방법
MLD-7 : 증기 유량 상실	C-10 부적절한 주증기 격리 밸브의 폐쇄
MLD-8 : 소외 전원상실	E-1 소외전원상실
MLD-9 : 원자로 정지	A-1 제어봉 낙하
	A-4 부적절한 붕소주입
	A-6 원자로정지
	C-5 저온의 급수공급
	C-7 과도한 주급수 유량
	D-14 가압기 가열기 고장
	D-15 가압기 살수고장
MLD-10 : RCS 냉각재량 증가	A-7 정지된 냉각재펌프의 기동
	D-11 유출량을 초과하는 충전
	D-13 부적절한 고압안전주입계통 작동
MLD-11 : RCS 냉각재량 감소 (Non-LOCA)	D-12 충전량을 초과하는 유출
MLD-12 : 증기관 파단	C-8 주급수관 파열 (격납건물 내부)
	C-9 주증기관 파열
	C-19 부적절한 터빈우회밸브 개방
	C-20 부적절한 대기방출밸브 개방
	C-21 부적절한 주증기 안전밸브 개방
MLD-13 : 보조계통상실	E-2 1E급 4.16 KV AC 전력 상실
	E-3 1E급 480 V AC 전력 상실
	E-4 1E급 125 V DC 전력 상실
	E-5 120 V AC 필수 전력 상실
	E-6 기기 냉각수 상실
	E-7 필수 공급수 상실
	E-8 계측용 공기상실
	E-9 공기조화계통상실
MLD-14 : 과도한 노심출력	A-2 부적절한 제어봉 인출
	A-5 부적절한 붕소희석

표 9. 예비 초기사건의 검토 및 분류 (1/4)

예비 초기사건	검 토	최종 초기사건
A-1 제어봉 낙하	제어봉 낙하로 원자로가 정지되며 원자로 정지이후의 조건은 일반 원자로 정지와 동일, 그러나 영광 3,4호기는 CEDMCS의 설계상 다중의 제어봉 낙하가 불가능하게 되어 있다.	N/A
A-2 부적절한 제어봉 인출	급격한 출력 증가에 의해 원자로 정지, 그러나 영광 3,4호기는 정상 운전 시 모든 제어봉을 인출하여 사용한다.	N/A
A-3 제어봉 돌출	PSAR 15.4.8 검토 결과 사고 경위가 원자로 정지 후 소형냉각재 상실사고와 동일	소형 냉각재 상실 사고
A-4 부적절한 붕소주입	붕소에 의한 반응도 감소, 원자로 정지	일반 과도사건
A-5 부적절한 붕소희석	붕소희석에 의해 shutdown margin이 감소한다. 그러나 shutdown margin이 없어질 정도로 희석 되는데는 충분한 보충수량과 시간이 필요하며 발생 확률도 낮다.	일반 과도사건
A-6 원자로정지	일반과도사건 참조	일반 과도사건
A-7 정지된 원자로 냉각재 펌프의 가동	저온수 공급 시 정반응도 부가에 의해 원자로 정지, 그러나 운전모드 3~6에서만 가능한 사건	N/A
B-1 1대 또는 그 이상의 원자로 냉각재 펌프의 고장	냉각재 유량 감소에 의한 원자로 정지 모든 RCP 정지 시에도 노심 내 자연대류에 의한 열제거 가능	일반 과도사건
B-2 원자로 냉각재 펌프 축 고착	축 고착에 의한 유량감소에 의해 원자로 정지, 다중 측,고착에 의한 냉각재 유로 폐쇄 확률은 매우 낮다.	일반 과도사건
B-3 원자로 냉각재 펌프 축 파단	냉각재 유량 감소로 원자로 정지	일반 과도사건
B-4 냉각재 유로 막힘	노심 내에서 전체 냉각재 유로의 차단가능성은 매우 낮다. 영광 5 ,6호기에는 LOOP 격리 밸브가 설치되어 있지 않다.	N/A
C-1 주급수 상실	주급수에 의한 이차측 열제거 기능 상실. 원자로 정지 후 5%의 급수공급이 불가능하여 일반 과도 현상과 다르다.	주급수상실
C-2 부적절한 주급수 격리 밸프 폐쇄	모든 주급수 격리 밸브가 폐쇄되면 주급수 공급이 상실된다. 부분적인 격리밸브의 폐쇄는 급수유량에 감소에 의해 원자로 정지	주급수 상실/ 일반 과도사건

표 9. 예비 초기사건의 검토 및 분류 (2/4)

예비 초기사건	검 토	최종 초기사건
C-3 부적절한 주급수 공급	원인이 급수제어계통에 있을 때 원자로 정지 후 5% 급수 공급이 불가능하다.	주급수 상실
C-4 급수펌프의 정지	모든 급수펌프가 정지되면 주급수 상실 유발. 한대의 급수펌프가 정지되면 노심내열제거 감소에 의해 원자로 정지	주급수 상실/ 일반 과도사건
C-5 저온의 급수 공급	노심의 과도한 냉각에 의해 원자로 정지	일반 과도사건
C-6 급수 공급의 감소	노심내의 열제거 감소에 의해 원자로 정지	일반 과도사건
C-7 과도한 주급수 유량	노심의 과도한 냉각에 의해 원자로 정지	일반 과도사건
C-8 주급수 파열	증기발생기 직전의 체크밸브 후단에서 발생 시에는 증기관 파열과 동일, 전단의 급수관 및 응축수관에서의 발생은 주급수 상실	대형 이차측 파단사고/ 주급수 상실/ 과도 현상
C-9 주증기관 파열	대형 이차측 파단 참조	대형 이차측 파단사고
C-10 부적절한 주증기 격리, 밸브의 폐쇄	모든 주증기 격리밸브의 폐쇄는 영광 5, 6호기에서는 MSIS에 의해 가능하며 모든 주급수 격리밸브도 폐쇄, 부분적인 주증기 격리밸브의 폐쇄는 터빈 트립을 유발	주급수 상실/ 일반 과도사건
C-11 복수기 진공 상실	복수기 진공상실에 의해 터빈 트립. 증기 우회계통 중 복수기로 증기를 우회시키는 밸브의 사용이 불가능	복수기 진공 상실
C-12 복수기 펌프 정지	모든 복수기 펌프가 정지되면 주급수 공급이 상실된다. 그 이외의 복수 펌프의 정지는 급수유량 감소와 동일	주급수 상실/ 일반 복수기 진공 상실
C-13 복수기 누설	복수기 누설에 의해 복수기 진공상실 유발	복수기 진공 상실
C-14 순환수 상실	복수기 진공상실 유발	복수기 진공상실
C-15 터빈조절 밸브고장	터빈정지를 유발	일반과도사건
C-16 터빈 정지 밸브고장	터빈정지를 유발	일반과도사건
C-17 터빈 정지	터빈정지에 의한 원자로 정지	일반과도사건
C-18 발전기 정지	터빈정지를 유발	일반과도사건

표 9. 예비 초기사건의 검토 및 분류 (3/4)

예비 초기사건	검 토	최종 초기사건
C-19 부적절한 터빈 우회 밸브 개방	다중의 터빈 우회밸브의 개방은 주증기관 파열과 동일	대형 이차측 파단 사고/ 일반 과도사건
C-20 부적절한 대기방출 밸브 개방	다중의 대기방출밸브의 개방은 주증기관 파열과 동일	대형 이차측 파단 사고/ 일반 과도사건
C-21 부적절한 주증기 안전 밸브개방	다중의 대기방출밸브의 개방은 주증기관 파열과 동일	대형 이차측 파단 사고/ 일반 과도사건
D-1 소형 RCS 배관 파단	소형 냉각재 상실사고 참조	소형 냉각재 상실사고
D-2 중형 RCS 배관 파단	중형냉각재 상실사고 참조	중형냉각재 상실사고
D-3 대형 RCS 배관 파단	대형냉각재 상실사고 참조	대형냉각재 상실사고
D-4 부적절한 압력방출 밸브 개방	중형 RCS배관 파단과 사고경위가 동일	중형냉각재 상실사고
D-5 원자로 냉각재 펌프밀봉 파손	소외전원 상실사고 경우에만 발생 가능성이 있는 사고이다.	N/A
D-6 제어봉 밀봉 부위 냉각재 누출	상실유량이 소형냉각재 상실사고보다 적으면 기술지침서에 의해 원자로 정지	일반과도사건
D-7 노심계측관 파손	소형냉각재상실 사고와 사고경위 동일	소형냉각재 상실사고
D-8 저압 경계부 냉각재 상실 사고	파단 크기는 대형 냉각재 상실사고와 동일하나 격납건물 외부에서 파단이 발생하여 재순환 운전이 불가능하다.	저압 경계부 냉각재 상실사고
D-9 증기발생기 세관 파열	일차측 냉각재가 직접 이차측으로 누출되며, 그에 따른 운전원의 조치가 소형냉각재 상실사고와 다르다.	증기발생기 세관 파열
D-10 원자로 압력 용기 파열	비상노심냉각계통의 능력을 초과하는 냉각재 상실사고를 원자로 압력용기 파열로 분류	원자로 압력 용기 파열
D-11 유출량을 초과하는 충전	노심 내 압력상승 및 반응도 변화데 의해 원자로 정지	일반 과도사건
D-10 원자로 압력 용기 파열	비상노심냉각계통의 능력을 초과하는 냉각재 상실사고를 원자로 압력용기 파열로 분류	원자로 압력 용기 파열

표 9. 예비 초기사건의 검토 및 분류 (4/4)

예비 초기사건	검 토	최종 초기사건
D-11 유출량을 초과하는 충전	노심 내 압력상승 및 반응도 변화데 의해 원자로 정지	일반 과도사건
D-12 충전량 초과 유출	RCS의 냉각재량 감소에 의해 소형 냉각재 상실사고와 사고 경위 동일	소형 냉각재 상실사고
D-13 부적절한 고압안전주입 계통의 작동	영광 3,4호기의 경우 고압안전주입 펌프의 토출 압력이 정상운전중의 RCS 압력보다 낮기 때문에 영향이 없다.	N/A
D-14 가압기 가열기 고장	가압기 압력변화에 의한 원자로 정지	일반 과도사건
D-15 가압기 상수 고장	가압기 압력변화에 의한 원자로 정지	일반 과도사건
E-1 소외전원상실	모든 사고경위에 영향을 미친다.	소외전원상실
E-1 1E급 4.16KV AC 전력상실	2-01SA 모선 상실 시 원자로 냉각재 펌프 냉각상실에 의해 원자로정지, 모선에서 전력을 공급받는 기기들에 영향을 미친다.	1E급 4.16KV AC 모선 상실
E-1 1E급 480V AC 전력상실	480V AC의 여러 모선들 중 주증기 격리 밸브와 주급수 격리밸브들에 전력을 공급하는 모선의 상실은 원자로 정지를 유발시키지만 4.16KV AC 모선 상실의 일부를 구성하는 사건으로 4.16KV AC 모선 상실의 일부로 분류	
E-4 1E급 125V DC 전력상실	4 - 01EA 모선의 상실 시 주증기 격리 밸브와 주급수 격리 밸브의 폐쇄에 의해 원자로가 정지, 4.16KV AC 2601 SA 모선에 연결된 기기들 및 보조급수계통의 디젤엔진 구동펌프 기능에 영향을 줌	1E급 125V DC 모선 상실
E-5 120V AC 필수 전력상실	1개의 120V AC 필수전력 모선의 상실이 원자로정지를 유발하지 않는다.	N/A
E-6 기기냉각수 상실	기기냉각수 트레인 A의 상실이 원자로 냉각재펌프의 냉각상실, 원자로 정지를 유발하며 트레인 A에서 냉각수를 공급 받는 기기들의 기능이 상실	기기냉각수상실
E-7 필수 공급수 상실	필수 공급수 트레인 A의 상실은 기기냉각수 트레인 A의 상실을 유발한다.	기기냉각수상실
E-8 계측용 공기 상실	계측용 공기의 상실은 원자로 정지를 유발하지 않는다.	N/A
E-9 공기 조화계통 상실	공기조화계통 상실에 의해 원자로정지를 유발하지 않는다.	N/A

표 10. 영광 5, 6 호기 PSA 최종 초기사건

분 류	초 기 사 건 목 록
원자로 냉각재 상실사고	대형 냉각재 상실사고
	중형 냉각재 상실사고
	소형 냉각재 상실사고
	원자로 용기 파손
	증기 발생기 세관 판단
	저압 경계부 냉각재 상실사고
과 도 사 건	대형 이차측 파단
	주급수 상실
	복수기 진공 상실
	기기냉각수 상실
	4.16KV 교류모선 상실
	125V 직류모선 상실
	소외전원 상실
	발전소 정전
	일반 과도사건
	정지불능 과도사건

제4장 사건수목 분석

제1절 개요

1. 목적

본 사건수목분석(Event Tree Analysis) 절차서는 원전의 확률론적 안전성평가(Probabilistic Safety Assessment : 이하 PSA)에서 사고경위분석 기법으로 널리 이용되고 있는 사건수목분석의 절차와 기법을 기술하여 PSA 수행 시 노심손상 사고경위를 일관성 있고 기술적으로 정확하게 분석하는 지침을 제공하고자 한다.

2. 적용 범위

본 사건수목분석 절차서는 설계 중인 원전에 대하여 그 동안 국내에서 수행되었던 PSA의 사건수목분석 절차 및 방법을 정리한 것이다. 따라서 본 절차서에 기술된 사건수목 분석의 방법 및 수준은 국내의 설계 중 원전 PSA에 적용된 방법에 준하는 것으로서, 향후 국내 원전 PSA의 사건수목분석에 적용할 수 있을 것이다.

3. 참고문헌

사고경위 도출 방법에는 여러 가지 방법이 있을 수 있으나, 본 절차서는 사건수목분석 방법을 대상으로 기술하였다. 본 절차서를 작성하기 위해 참고한 대표적인 문헌은 다음과 같다.

[1]"PRA Procedure Guide", NUREG/CR-2300", ANS and IEEE, 1982.

[2]"Probabilistic Safety Analysis Procedures Guide", NUREG/CR-2815, 1984.

[3]"Procedures for Conducting Probabilitic Safety Assessment of NPPs (Level 1)", IAEA, 1992.

[4]"고리 3,4 호기 및 영광 1,2 호기 PSA 수행절차서", 한국전력공사, 1992.

4. 기본가정 및 용어정의

본 절차서는 설계중인 원전인 영광5,6호기 전출력 Level 1 PSA에 적용하기 위해 작성한 절차서로서 그 동안 국내에서 수행되었던 설계중인 원전 PSA의 사건수목분석 방법에 근거하여 작성한 것이다. 사고경위분석에 사용된 기본 가정은 다음과 같다.

- 초기사건은 100 % 출력 운전 중 발생할 수 있는 내부사건만을 대상으로 하였다.
- 노심상부가 노출되면 노심손상이 발생한 것으로 가정하였다. 다만 대형냉각재상실 사고 시 안전주입탱크 물로 노심이 잠길 때까지의 짧은 시간 노심노출은 예외로 하였다.
- 사고경위분석에 사용된 계통의 작동시간(Mission Time) 은 24시간으로 하였다.
- 만일 발전소 상태가 다음 조건 중 하나를 만족하면 사고는 노심손상 없이 성공적으로 종결되었다고 가정하였다.
  - 정지냉각운전조건을 만족하고, 정지냉각계통에 의해서 저온정지 상태가 유지된다.
  - 이차측에 의한 일차측 열제거와 자연순환에 의한 노심잔열 제거를 통해 안정된 고온정지 상태를 유지한다.
  - 주입 및 방출 (Feed and Bleed) 운전 후 재순환 운전으로 노심잔열을 제거한다.
  - 대형 및 중형 냉각재상실 사고 시 재순환 운전으로 노심잔열을 제거한다.

대형 및 중형 냉각재상실 사고 시 파단 부위는 원자로냉각재펌프와 원자로 용기 사이의 원자로냉각재계통 저온관으로 가정하였다.

사건수목분석에서 사용되는 주요 용어는 다음과 같다.

PSA	확률론적 안전성 평가
노심손상빈도	노심손상 사고가 발생할 수 있는 빈도로 1년 단위로 계산된다.
KIRAP	한국원자력연구소에서 개발한 PSA 수행용 전산코드 페키지
기본사건	고장수목 논리 전개에서 최종 하부에 위치하는 사건들로서 신뢰도 자료의 입력이 가능한 기본 단위. 기기의 기계적 고장, 보수 및 시험 이용불능 사건, 인간오류 사건 등이 포함된다.
최소단절집합	계통 실패 또는 노심손상을 발생시킬 수 있는 기본사건들의 조합
고장수목	계통 실패에 대한 원인들을 논리적으로 추적해나가는 도식적 모델

사건수목	사건이 발생한 후 계통 작동유무에 따라 어떠한 사고로 전개되는가를 나타내는 모델
사고경위	사건수목에서 계통 작동유무에 따라 전개되는 사고 시나리오. 하나의 사고경위는 어떠한 초기사고가 발생한 후 어떠한 계통들이 작동하였고 어떠한 계통들이 실패하였는지에 따라 정해진다.
초기사건	원전 정상 운전 중 이상사태를 발생시킬 수 있는 사고. PSA 에서는 유사한 사고들을 그룹화하여 하나의 초기사건으로 처리하며, 대부분의 경우 원자로 정지로 이어지는 사고만을 취급한다.
안전기능	원자로 노심을 건전한 상태로 유지하기 위해 필요한 기능으로서, 반응도, RCS 냉각재량, RCS 압력, 노심 열제거, RCS 열제거, 격납용기 격리, 격납용기 온도 및 압력 제어 등이 있다.

제2절 분석 절차

사건수목분석이란 선정된 초기사건에 대하여 사건수목을 구성하여 노심손상을 초래하는 모든 중요 사고경위를 논리적으로 밝혀내는 과정이다. 이를 위해서 우선 각 초기 사건별로 노심을 건전한 상태로 유지하기 위해 필요한 안전기능을 파악하고 작동이 요구되는 안전계통 및 운전원 조치를 정리하여 사건수목의 표제로 정의한다. 다음에는 각 초기사건 발생시 각 표제의 성공 혹은 실패에 따라 이분수목 (Binary Tree) 형태로 사고 시나리오를 전개하여 발생 가능한 노심손상 사고경위를 논리적으로 구성한다.

사건수목분석은 노심손상 사고경위를 파악하기 위한 사고경위분석의 한 부분으로 수행된다. 사고경위분석에는 안전기능분석, 초기사건분석, 사건수목분석이 포함되며 이들이 각각 별개로 수행되는 것이 아니라 상호 유기적이고 반복적으로 업무가 연계되어 있다. 편의상 이를 초기사건분석과 사건수목분석으로 구분하고 있을 뿐이다.

1. 안전기능 정의

노심을 안전한 상태로 유지하기 위해서 안전기능들이 유지되어야 하는데, 영광 5, 6 호기 사건수목 개발 시에 고려한 안전기능은 다음과 같다.

- 원자로 미임계 (Subcritical) 유지
- 노심 붕괴열 제거
  - RCS 냉각재 유지

– 원자로냉각재 유량 유지 (강제 혹은 자연 순환 유지)
– RCS 열 제거
- RCS 압력 제어
- 격납건물 격리
- 격납건물 온도 및 압력 제어

상기 안전기능들 중 격납건물의 격리와 압력 제어는 노심손상 관점인 내부사건 분석 범위를 벗어나므로 본 사건수목 절차서에서는 고려하지 않았다.

2. 안전기능 관련계통 파악

안전기능이 파악되면 안전기능을 유지하기 위해 필요한 계통들을 파악하고 이를 사건수목 표제로 정의한다. 영광5,6호기 안전기능별 관련 계통은 다음과 같다.

- 반응도제어 : 원자로보호계통, 화학 및 체적제어계통
- RCS 재고량 확보 : 고압안전주입계통, 안전주입탱크, 저압안전주입 계통
- RCS 압력 제어 : 화학 및 체적제어계통, 안전감압계통, 가압기 살수계통
- 노심 열제거 : 강제순환냉각, 자연순환냉각, 정지냉각계통
- RCS 열제거 : 주급수계통, 보조급수계통, 증기방출계통, 정지냉각계통
- 격납건물격리 : 격납건물차단계통
- 격납건물 온도/압력 제어 : 격납건물살수계통

다음은 초기사건에 따른 각 계통들의 성공기준을 결정한다. 이를 위해서는 안전성분석 보고서를 포함한 관련 열수력 분석 보고서 및 참조 원전의 PSA 지원 열수력 분석 보고서 등을 검토한다. 특히 사고경위 결정 및 PSA 분석 결과에 중요한 영향을 미치는 민감한 표제의 선정이나 성공기준은 별도의 열수력 분석을 수행하여 결정한다. 참고로 영광5,6호기 PSA의 LOCA 사건수목에서 사용되었던 표제별 성공기준은 표 11과 같다.

표제 배열의 순서는 결과에 큰 영향을 미치지는 않지만 분석의 효율성과 사건전개의 이해 관점에서는 매우 중요하다. 시간, 기능 및 계통간의 연관성 등이 주요 고려 인자이며, 가능한 관련 계통의 작동 시간 순으로 표제를 배열하는 것이 일반적이다. 각 표제의 성공 기준 및 사고 전개에 따른 시간 정보는 안전성분석보고서의 사고해석 결과, 참조 원전의 PSA보고서 및 열수력 분석 결과에 근거하여 결정되었다.

표 11. LOCA 초기사건별 표제 및 성공조건

초기사건	사건수목 표제	관련 계통 및 성공기준
Large LOCA	SIT(안전주입탱크)	2/3 SITs
	LPI(저압안전주입)	LPSI 1/3 paths, 1/2 pumps
	HPR(고압재순환)	HPSI 1/3 paths, 1/2 pumps
	HPH(고온관/저온관 재순환)	HPSI Hot Leg Rec. 1/2 paths, 1/2 pumps
	CSR(재순환수 냉각)	1/2 CS HX
Medium LOCA	HPI(고압안전주입)	HPSI 2/3 paths, 1/2 pumps
	HPR(고압재순환)	HPSI 1/3 paths, 1/2 pumps
	HPH(고온관/저온관 재순환)	HPSI Hot Leg Rec. 1/2 paths, 1/2 pumps
	CSR(재순환수 냉각)	1/2 CS HX
Small LOCA	RT(원자로정지)	RPS (>= 27/28 SORs)
	HPI/HPR(고압안전주입/재순환)	1/2 HPSI Pump, 1/4 Cold Leg
	AFW(보조급수)	AFWS (1/2 SG, 1/4 pumps)
	SR1(증기방출)	ADV (1/2 SG, 1/4 valves)
	SR2(증기방출)	MSSV (1/2 SG, 1/16 valves)
	DPI/DPR (이차측 감압)	AFW (2/2 SG , 1/2 pumps per SG). ADV (2/2 SG, 1/2 valves per SG), 2/4 SIT
	LPI/LPR(저압안전주입/재순환)	1/2 LPSI
	BD(early)(주입 및 방출)	SDS (1/2 train) and HPSI (1/2 train) 성공 전제
	SDC(정지냉각)	SCS (1/2 train)
	CSR(재순환 냉각)	CSS HX (1/2 train)
	BD(late)(주입 및 방출)	SCS (1/2 train) and 1/2 HPSI

3. 안전기능 사건수목 구성

초기사건별로 필요한 안전기능이 파악되면 안전기능의 성공, 실패 여부에 따른 사고 시나리오의 전개 상황을 분석해 볼 필요가 있다. 이를 안전기능 사건수목이라 하는데, 안전기능 사건수목은 사건수목분석의 최종 결과물이 아니며 초기사건과 상세한 사고경위

및 완화 특성 사이의 복잡한 관계를 밝히는 중간 단계의 작업이다. 안전기능 사건수목의 표제인 각 안전기능은 나중에 해당 안전기능을 수행하는 여러 계통들로 분해되고 이에따라 보다 상세한 사건수목이 구성된다.

안전기능 사건수목을 구성하기 위해서는 우선 초기사건별로 사고 완화 및 중지에 필요한 안전기능을 파악한다. 다음은 유사한 발전소 대응을 갖는 초기사건들을 묶어 이들에 대한 안전기능 사건수목을 구성한다.

안전기능 사건수목의 표제는 앞에서 정의된 안전기능 혹은 초기사건 특성에 따라 한 단계 세분화된 기능으로 정의된다. 예로 대형 혹은 중형 LOCA 에서는 '안전주입', 'RCS 재순환', '재순환수 냉각' 등으로 안전기능 사건수목의 표제를 정의할 수 있다. 영광 5,6 호기에서 대형 및 중형 LOCA가 발생하면 일단 원자로 정지나 RCS 열제거와 같은 안전기능이 사고 완화에 직접적인 영향을 주지는 않는다. 우선 필요한 안전기능은 RCS 냉각재 보충으로, 사고초기에는 '안전주입' 표제로 일정 시점 이 후에는 'RCS 재순환' 표제가 이를 의미한다. RCS 냉각재 보충이 성공하면 장기적으로는 노심 잔열의 제거 즉, RCS 재순환수의 냉각이 이루어져야 된다. 이 안전기능은 '재순환수 냉각'이란 표제로 표현된다.

이와같은 안전기능 사건수목은 계통 사건수목을 개발하기 위한 준비 단계의 하나로서, 초기사건별로 안전기능의 대응이 유사한 것들을 하나의 사건수목으로 표현할 수 있다. 영광5,6 호기 PSA에서는 대형 및 중형 LOCA, 소형 LOCA, 증기발생기 세관파단사고, 일반과도사건, 소외전원상실, 발전소정전사고, ATWS 등이 별도의 안전기능 사건수목 그룹으로 구별된다. 언급되지 않은 초기사건들은 일반과도사건 사건수목을 따른다.

일반적으로 사건수목 개발시에는 복잡한 계통간의 상호작용을 이해하기가 곤란하므로 1차적으로 안전기능 사건수목을 구성하고 다음으로 안전기능을 구성하고 있는 계통을 찾아내어 계통 사건수목을 개발하게 된다. 그러나 계통간의 상호작용, 사고경위 등을 잘 이해하고 있는 경우에는 안전기능 사건수목의 구성없이 직접 계통 사건수목을 구성할 수도 있다.

4. 계통 사건수목 구성

안전기능 사건수목이 구성되면 초기사건에 따라 각 안전기능 표제를 계통 단위로 보다 세분화한 계통 사건수목을 구성한다. 초기사건에 따라 동일한 안전기능도 다른 계통에 의해 수행되기도 한다. 예를 들면 RCS냉각재의 주입은 소형 LOCA시에는 고압 안전주입계통이 수행하고 대형 LOCA시에는 저압 안전주입계통이 수행한다. 안전기능은 일차적으로 공학적 안전설비 계통이 담당하나 이들 안전계통 이외의 타 계통도

안전기능을 담당할 수 있다. 또한 동일한 계통이라도 초기사건에 따라 성공기준이 달라지기도 한다. 예를 들어, 중형과 소형 LOCA에서 고압안전주입계통이 동일하게 사용되지만 중형 LOCA시에는 파단 유로를 고려하지 않음에 따라 소형 LOCA시와는 성공기준이 달라진다. 따라서, 계통 사건수목은 이와같은 계통 단위의 세부적인 차이를 표제로 표현하여 보다 상세한 사고 시나리오를 파악할 수 있게 해준다.

안전기능별 관련 계통의 파악이 끝나면 이들 표제의 배열 순서를 결정한다. 표제 배열의 주요 세가지 인자는 시간, 기능 및 하드웨어적 관련성이다. 표제 배열의 초기단계에서는 시간인자를 고려하는 것이 바람직하다. 즉 1차 안전계통들을 사고경위에 따라 요구되는 시간 순서로 배열하는 것이다. 따라서 즉시 반응하는 계통(원자로보호계통 등)이 가장 먼저 위치하고 시간 순서에 따라 관련 계통을 배치한다. 그러나 반응시간만이 표제 배열의 절대적인 기준은 아니며, 계통의 기능 및 하드웨어적 관련성이 사건수목 표제 순서 결정시 고려되어야 한다.

각 초기사건에 대한 계통 및 성공기준, 표제순서 등이 결정되면, 이들 표제의 성공 혹은 실패에 따라 각 초기사건에 대하여 발생 가능한 모든 사고경위를 논리적으로 도출하게 된다. 모든 사고경위들은 최종적으로 노심손상 혹은 원자로 안전 정지, 둘 중 하나의 상태로 종결된다.

5. 문서화

사건수목분석을 수행한 결과로서 다음과 같은 내용을 문서화한다.

- 사건수목구성 방법론
- 기본 가정사항
- 안전기능 및 관련 계통
- 초기사건별 관련 안전기능
- 초기사건별 안전기능에 관련된 계통 및 성공기준
- 계통 연계성
- 초기사건별 사건수목
- 관련 열수력 분석 자료 및 성공기준 근거 문서

제3절 사건수목 상세 분석 방법

1. 개요

본 장에는 사건수목분석의 방법 및 절차를 보다 상세히 기술하였다. 사건수목분석은 사고경위분석의 한 부분으로서, 정의된 초기사건 각각에 대하여 관련계통들의 성공, 실패 여부를 고려하여 초기사건 발생후 전개될 수 있는 모든 중요한 사고경위를 파악한다. 사고경위분석에는 그림 3에서 보는 바와 같이 안전기능정의, 초기사건분석, 사건수목 분석이 포함된다. 물론 기기 단위의 사고 시나리오를 파악하기 위해서는 계통 고장수목 모델이 함께 취합되어야 한다.

사고경위분석의 첫번째 단계는 분석 목표의 설정이다. 사고경위분석의 첫번째 단계인 분석 목표의 설정은 분석의 깊이와 범위를 정하는데 필요하다. 예를 들면 최적의 설계를 위한 사고경위분석과 최적 시험주기 결정을 위한 사고경위분석은 서로 분석 내용과 범위가 다를 수 있기 때문이다. 분석 목표가 설정되면 분석 대상 발전소에 대한 검토가 필요하다. 발전소 검토의 대상에는 발전소 부지, 건물 배치, 계통 등이 포함된다. 발전소에 대한 전반적인 검토가 완료되면 사고경위 모델링 단계로서 대상 원전에 필요한 안전기능을 정의하고, 발생할 수 있는 초기사건을 선정하며, 정의된 초기사건에 대하여 사건수목을 구성하여 사고 시나리오를 도출한다. 이 후의 작업은 사건수목의 표제(Heading) 및 보조논리에 따라 각 계통의 고장수목을 구성하여 사건수목과 연결하고 각 기본사건에 데이타를 입력하여 사고경위의 정량화를 수행한다.

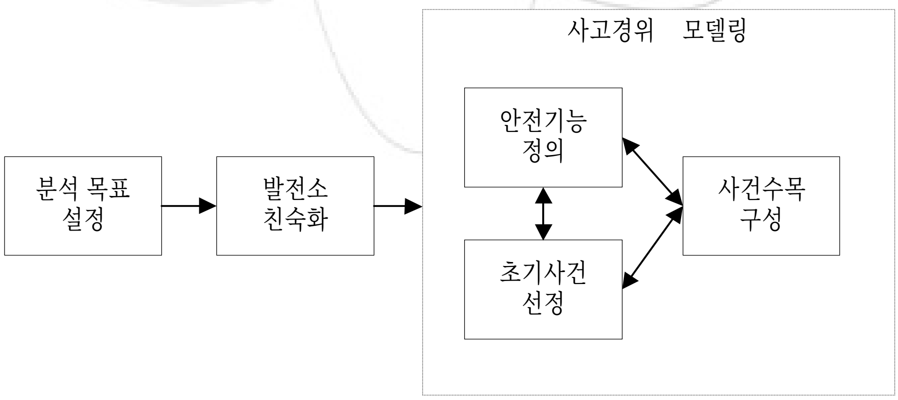


그림 3. 사고경위분석 절차

사고경위분석을 수행하기 위해서 분석자는 발전소의 설계, 운전 및 보수유지 사고발생 및 과정 등을 잘 알고 있어야 하며 또한 발전소 전 계통에 대한 기능과 계통간의 상호작용 등을 알고 있어야 한다. 이와같은 발전소 친숙화를 위하여 우선 발전소에 관한 많은 정보와 자료를 수집하여야 하며 효율적인 검토를 위하여 이들 자료의 조직적이며 체계적인 관리가 필요하고, 필요에 따라서 자료들을 새로 종합, 정리할 필요가 있다. 특별히 발전소 운전에 관한 자료 수집과 운전 경험 뿐만아니라 사고경위분석을 위해서는 발전소 운전원의 참여가 필요하다. 운전원의 참여는 사고경위분석시 필요한 자료, 특히 운전에 관련된 자료를 용이하고 적절하게 얻을 수 있게 하며 사고시 운전원의 대응조치 등 사고경위 파악에 관련된 많은 정보를 제공할 수 있기 때문이다.

업무 초기에는 분석에 필요한 자료들이 어떠한 것이 있는가에 대한 조사가 필요하며 업무가 진행됨에 따라 이들 자료를 수집하고 필요에 따라 새로운 자료들을 조사하여 추가로 수집한다. 정보 및 자료 수집의 방법은 발전소 방문, 운전원과의 면담 등이 있다.

표 12. 발전소 친숙화에 필요한 관련 자료

번호	자 료 명
1	예비/최종 안전성분석보고서
2	발전소 기술지침서 및 기타 규제 문헌
3	계통 설명서
4	계통 도면
5	전기 도면 (전기모선 보호계통에 대한 트립 기준 및 회로도 포함)
6	제어 및 신호 회로도
7	정상, 비상, 시험 및 보수 절차서
8	계통 성공기준 결정에 필요한 열수력 분석 보고서
9	발전소 방문
10	사고분석 보고서 및 유사 발전소 LER 등
11	발전소 배치도, 배관 도면, 전선 배치 도면 등 관련 도면

사고경위분석 및 계통분석에 필요한 대표적 자료들이 표 12에 나타나 있다. 표에 정리된 자료중 발전소에 대한 안전성분석보고서에는 사고경위분석에 필요한 많은 정보가 포함되어 있다. 그러나 이들 정보, 특히 안전기능 수행에 필요한 기기수나 계통 성공기준 등에 대한 최소 요건 설정시에는 과제 목적에 따라 세심한 주의가 요구된다. 이것은 인허가 기준에 따른 요건이 PSA 사고경위분석에 필요한 요건보다 보수적일 수

있기 때문이다. 그러나 현실적인 값(Best Estimate Value)을 사용할 때에도 적절한 문서나 계산 등으로 그 타당성을 입증할 수 있어야 한다. 추가적으로 필요한 자료로서 유사 발전소에 대한 PSA 보고서를 꼽을 수 있다. 이러한 타 발전소 PSA 보고서를 검토할 때에도 보고서의 목적, 범위, 가정사항, 분석방법 등에 대한 세심한 검토가 요구된다. 사고경위 분석자는 표 12에 나타난 자료 등을 통하여 사고경위 모델링에 필요한 안전기능, 발생가능한 사고 및 사고경위, 계통성공기준 등에 대해 전반적으로 이해해야 한다.

2. 사고경위 모델링

원전과 같이 복잡한 계통의 사고경위를 분석하는데 있어서는 체계적이고 논리적인 사고경위의 모델링이 요구된다. 이러한 사고경위 모델링의 한 방법으로서 앞에서 언급한 바와같이 고장수목과 함께 사건수목이 사용된다. 5장 계통분석 절차서에서 상세히 설명되어 있는 고장수목분석은 연역적(Deductive)인 방법으로 계통분석을 수행하며, 사건수목분석은 귀납적(Inductive) 방법으로 계통 수준에서 발생 가능한 사고경위를 모델링하는 방법이다. 그림 4에 사건수목의 간단한 예가 정리되었다.

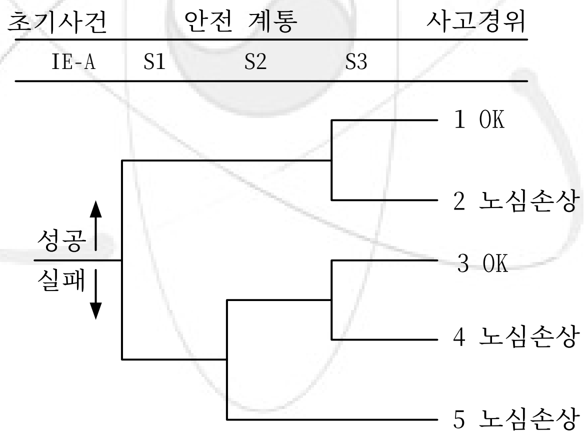


그림 4. 사건수목 구성 예

그림에서 상단에 있는 IE-A는 초기사건 A를 나타내며 S1, S2, S3는 초기사건 A가 발생하였을 경우 이를 완화하는데 필요한 안전기능 혹은 계통을 나타내는 표제(Heading)라 한다. 사건수목에서 표제로 나타난 안전기능 혹은 안전계통의 성공 및

실패에 따라 여러가지의 사고경위를 보여주고 있다. 구성된 사건수목으로 볼때, 초기사건 A는 사고가 발생하면 안전계통 S1이나 S2중 최소한 하나의 계통과 안전계통 S3가 작동해야 발전소가 안전한 것을 알 수 있다. 사건수목 오른쪽에는 각 사고경위 결과를 나타내는데 사고경위 1은 초기사건 A발생후 안전계통 S1과 S2가 정상적으로 작동하여 노심의 손상없이 발전소를 안전하게 정지시킨 경우이며, 사고경위 3은 안전계통 S1은 실패했지만 S2와 S3가 성공하여 발전소가 안전한 경우이다. 사고경위 2, 4, 5는 초기사건 발생후 S3 계통이 실패하거나 S1과 S2가 모두 기능 상실하여 노심손상이 발생한 경우를 보여준다.

사고경위분석을 위한 설계 및 운전과 관련된 많은 정보를 수집, 분석하여야 하는데, 이를 대략적으로 정리하면 다음과 같다.

- 사고경위분석 초기단계에서는 안전계통(Safety System)과 이들 계통을 지원하는 보조계통(Support System)을 구분하는 작업이 필요하다. 사고경위분석 업무에 있어 계통간의 상호작용, 종속성 등에 대한 이해가 중요하므로 안전계통과 보조계통간의 종속관계를 파악한다.
- 초기사건에 대한 정보는 발전소 운전경력과 타 PSA 자료등으로부터 얻을 수 있다. 안전성분석 보고서와 기타 과도사건 분석자료들을 검토하여 사고에 따른 발전소운전 진행 상태를 면밀히 검토한다.
- 추가로 사고를 발생시키거나 사고경위에 영향을 줄 수 있는 계통에 대하여 예비 정성분석을 할 수도 있다. 만일 이들 계통중 사고경위 전개에 중요한 계통이 있다면 대상 계통의 영향에 대한 상세검토를 수행하여 모델링에 포함한다.

설계 및 운전 자료, 사고해석 자료의 분석을 통하여 초기사건의 선정, 사고경위분석 및 모델링, 사건수목의 형태, 주요계통과 이들의 성공기준 등의 정보를 얻는다. 사고경위분석은 안전기능의 분석, 초기사건분석, 사건수목분석이 함께 유기적으로 수행되어야 한다. 비록 각 분석 업무의 내용은 명확히 구별되지만 업무간의 정보 흐름 및 공유가 필수적이고 필요에 따라 반복적으로 수행되기 때문에 분석의 정확성 및 일관성 유지를 위해 하나의 연결된 업무로 수행한다. 이상과 같은 사고경위 모델링을 위한 사건수목의 개발과정이 그림 5에 나타나 있으며 각 과정에 대한 설명은 다음 절에 정리하였다.

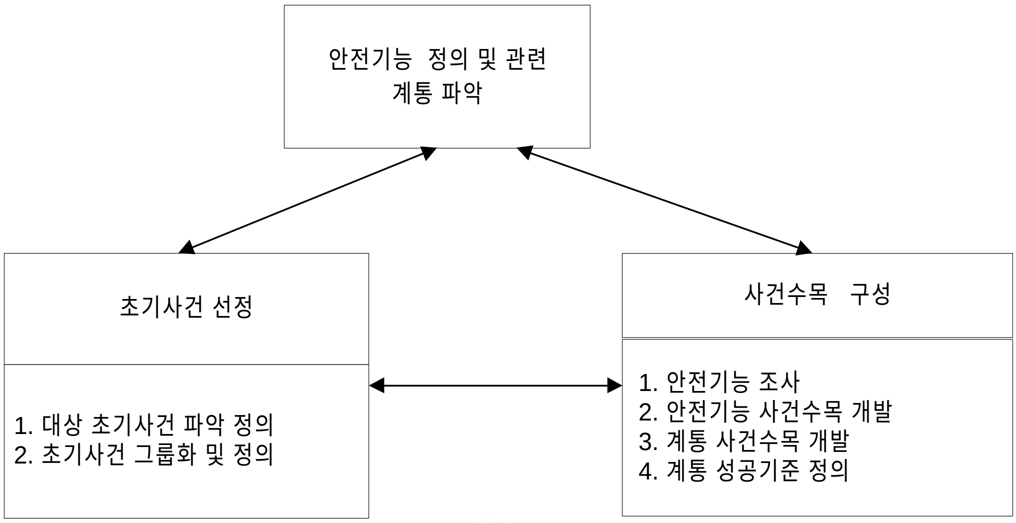


그림 5. 사건수목 개발 과정

가. 안전기능 정의

원전은 화석 연료를 사용하는 화력발전소와는 달리 우라늄 핵반응에서 생성되는 열을 이용하여 증기를 만들고, 이 증기로 터빈을 돌려 전기를 생산한다. 원전의 안전성이 일반 화력발전소에 비해 훨씬 중요한 이유는 사고로 인해 핵물질이 외부로 누출될 경우 막대한 신체적, 경제적 손실을 초래할 가능성이 있기 때문이다. 이런 만일의 사태를 방지하기 위해 원전은 다중방호개념으로 설계되어 방사능 물질의 외부 누출 가능성을 극소화하고 있다.

원전의 연료로 사용하는 우라늄의 특성은 전기를 생산하지 않는 상태(원자로 정지상태) 에서도 계속 약간의 열(정지초기에는 정상출력의 약 4% 정도)을 발생한다는 것이다. 따라서 원전이 안전하기 위해서는 이상 상태 발생시 원자로를 정지(핵반응 중지) 시키고, 약간씩 발생하는 열(잔열)을 계속 제거해야 한다. 잔열을 제거하기 위해서는 핵연료가 물에 잠겨있어야 하고 발생하는 열을 외부로 전달할 수 있어야 한다. 이와 같이 원전의 안전한 상태 유지를 위해 필요한 기능을 보다 명확히 정의한 것을 안전기능(Safety Function)이라 하며, 발전소내의 에너지원과 방사선 사고를 관리하는데 필요한 기능을 말한다. 안전기능의 개념은 초기사건의 선정과 사고경위 규명의 기준으로서 사용된다. 일반적인 안전기능은 노심손상방지, 격납건물 파손방지 및 방사성물질 방출의 최소화 등의 기능을 말한다. 이러한 안전기능은 여러 안전계통 및 운전계통들과 원자로 고유의 부반응도 등에 의해 유지된다.

안전기능은 발전소 형태, 계통설계, 계통 반응시간 및 분석 목적에 따라 여러가지 방법으로 정의할 수 있다. 표 13는 영광3,4호기 비상운전절차서에 명시된 안전기능들과 그 목적을 보여주고 있다. 안전기능은 궁극적으로 방사능 물질의 외부 유출 방지를 목적으로 하고 있기 때문에 노심의 핵연료로부터 사고의 발생 및 확산을 방지하기 위해 필요한 기능을 정의한 것이다.

표 13. 안전기능과 목적

안전기능 (Safety Function)	목　　적
반응도제어	노심 핵분열 반응 중지
RCS 재고량 확보	원자로냉각재계통(RCS)이 냉각재 유지
RCS 압력 제어	RCS 압력 유지
노심 열제거	RCS내의 유로가 형성되어 노심 열제거
RCS 열제거	노심 열제거를 위한 RCS 열제거
격납용기격리	방사능 물질의 외부 누출 방지
격납용기 온도 및 압력 제어	격납건물 건전성 확보 및 방사능 물질의 외부 누출 방지

(`영광3,4호기 비상운전절차서 근거)

반응도 제어(Reactivity Control)는 노심으로부터 제거되어야 할 열량을 결정하는 기능으로 노심이 건전하게 유지되기 위해서는 우선 반응도 제어가 이루어져야 한다. 다음의 기능은 노심냉각기능이다. 노심냉각은 RCS내의 냉각재가 유지되고 노심으로의 적절한 유로가 형성되어 노심의 잔열을 냉각시키는 기능이다. 노심의 열을 제거하기 위해서는 RCS가 적정한 수준의 냉각재가 유지되어야 하고 또한 일정한 수준의 압력 제어가 이루어져야 한다. 따라서, RCS 냉각재 제어와 RCS 압력제어를 각각 하나의 안전기능으로 정의한다. 노심의 열은 궁극적으로 RCS 외부로 제거되어야 하기 때문에 RCS 열제거가 하나의 안전기능이 되며, LOCA 발생시 격납건물의 격리와 온도 및 압력의 제어 기능 역시 안전기능으로 정의한다. 이와같은 논리를 통하여 발전소에 대한 기본 안전기능의 구조를 수립한다. 안전기능의 정의는 초기사건의 그룹화에 사전 기준을 제공한다.

상기 안전기능들은 상호 독립적인 관계는 아니며 일부 안전기능 사이에는 높은 상관관계가 있다. 예를 들면 'RCS압력제어'가 안되면 곧 'RCS재고량 확보' 안전기능이 위협을 받게 된다. 특히 'RCS 재고량 확보'와 'RCS 압력제어', '핵연료 열제거'와 'RCS

열제거' 사이에는 직접적인 상관 관계가 있어 어느 한 계통의 작동이 이들 안전기능을 동시에 만족시키는 경우가 있다.

표 14. 안전기능별 관련 계통 및 사고 유형

안전기능	관련 안전계통	관련 사고 유형
반응도제어	원자로보호계통, 화학 및 체적제어계통	정지불능과도사건(ATWS)
RCS 재고량 확보	고압안전주입계통, 안전주입탱크, 저압안전주입 계통	냉각재상실사고(LOCA), 증기발생기세관파단사고, 이차측 대형파단사고,
RCS 압력 제어	화학 및 체적제어계통, 안전감압계통, 가압기 살수계통	
핵연료 열제거	원자로냉각재 펌프, 자연순환냉각, 정지냉각계통	소외전원상실사고, 급수완전 상실사고, 냉각재상실사고,
RCS 열제거	주급수계통, 보조급수계통, 증기방출계통, 정지냉각계통	증기발생기세관파단사고, 이차측 대형파단사고
격납건물격리	격납건물차단계통	냉각재상실사고(LOCA), 증기발생기세관파단사고,
격납건물 온도/압력 제어	격납건물살수계통	이차측 대형파단사고,

모든 안전기능을 적절한 상태로 유지하는 것이 원전 사고에 대처하는 기본 논리이다. 그러나, 사고의 유형에 따라 위협 받는 안전기능이 다르기 때문에 사고 유형에 따라 대처 방식이 달라진다. 안전기능을 유지하기 위하여 원전에는 여러 종류의 안전계통이 설치되어 있으며, 또한 어떤 사고 유형에서 이들 안전기능이 위협 받는지를 표 14에 정리하였다. 경제적 측면에서 하나의 계통이 여러 기능을 수행하게끔 설계된 것이 많다.

나. 초기사건 선정

발전소 사고에 대비한 안전기능이 정의되면 다음으로 초기사건들이 선정된다. 초기사건이란 PSA에서 사고 시나리오 전개의 시작점을 의미하는 것으로써, 원자로 보호계통의 작동이나 혹은 이상 신호등으로 제어봉 삽입을 필요로 하는 사고를 말한다. 사고경위 모델링에 있어 중요한 점의 하나는 가능한 한 모든 사고경위를 모델링하고 분석해야 한다는 점이다. 그러나 발전소에서의 발생 가능한 모든 사고 사고시나리오를 모델링하여 분석하는 것은 현실적으로 불가능한 일이다. 따라서 사고경위 모델링에 있어

가능한 주요 사고경위를 모델링하고 업무량도 감소시킬수 있도록 다음 2단계 과정을 통하여 초기사건을 선정한다.

첫째 대상 원전에서 발생 가능한 모든 사고 유발 가능한 사건들을 파악하고 정리한다. 주 논리도(Master Logic Diagram)를 구성하여 초기사건의 전형적 그룹 및 대표적 사건을 선정하고 이들 전형적 그룹에 포함되는 모든 대상 사건들을 정의한다. 대상 사건들을 파악하기 위해 필요하면 고장모드 및 효과 분석(Failure Mode and Effect Analysis)을 수행하여 초기사건 대상 목록을 작성한다. 여기에는 유사 발전소의 운전 자료로부터 나온 사건이나 타 PSA 보고서의 전형적 초기사건들도 모두 포함시킨다. 둘째, 파악된 대상 초기사건들을 앞에서 정의한 안전기능과 관련 계통들의 성공기준을 고려하여 사고 전개과정과 발전소 대응이 유사한 것들끼리 그룹핑한다. 즉, 몇 개의 초기사건 대상들이 사건 발생시의 발전소 거동과 필요한 안전계통 및 그 기능적 요구 조건이 동일하다면 이들 대상 사건들을 하나의 초기사건으로 정의한다. 초기사건분석에 대한 보다 자세한 내용은 3장 초기사건분석 절차서에 정리하였다.

다. 사건수목 개발

초기사건의 선정이 완료되면 각 초기사건별로 사건수목을 개발한다. 사건수목의 개발 절차는 그림 5에 이미 정리하였다.

초기사건이 선정되면 각 초기사건 발생에 따른 사고 시나리오를 개발한다. 사고 시나리오 개발에는 사건수목 기법이 사용된다. 사건수목은 표제에 포함되는 계통의 범위와 성격에 따라 대형 사건수목(Large Event Tree)과 소형 사건수목(Small Event Tree)으로 구분할 수 있다. 안전기능에 직접적으로 연관된 주요 안전 관련계통만을 사건수목의 표제로 모델링하는 것이 소형 사건수목이고, 보조계통을 포함하여 사고 완화에 관련된 모든 계통을 표제로 고려하는 방식이 대형 사건수목 기법이다. 따라서, 소형 사건수목에서는 전기, 기기냉각수계통과 같은 보조계통은 각 안전관련계통의 하부 논리로 모델링하여 계통들간의 종속성을 계통 고장수목 구성 단계에서 고려하는 방법이다. 반면 대형 사건수목은 보조계통을 포함한 모든 계통을 독립적으로 모델링한 후 사건수목 구성단계에서 계통간의 종속성을 고려하여 사고 시나리오를 구성하는 방법으로 사건수목이 매우 커지고 복잡해진다. 국내 PSA에서는 사고 시나리오의 구성 및 이해가 쉬운 소형 사건수목 기법을 사용하고 있다.

사건수목 개발을 위해서는 우선 초기사건 발생 후 사고 중지 및 완화를 위해 필요한 안전기능을 조사한다. 초기사건을 분류하기 위한 안전기능정의는 고장수목과 같이 연역적 방법을 사용한 것이나, 여기서는 초기사건 발생후 사고의 진행을 막고 사고의 영향을 완화시키는 안전기능을 귀납적으로 찾는다. 고려하는 안전기능의 순서는 경우에

따라 다르나 일반적으로 안전기능을 필요로하는 시간순으로 배치한다. 안전기능을 조사한 후에는 안전기능 사건수목을 개발하고, 후에 이를 바탕으로 관련 계통 단위의 계통 사건수목을 구성한다.

일반적으로 사건수목 개발시에는 복잡한 계통간의 상호작용을 이해하기가 곤란하므로 1차적으로 안전기능 사건수목을 구성하고 다음으로 안전기능을 구성하고 있는 계통을 찾아내어 계통 사건수목을 개발하게 된다. 그러나 계통간의 상호작용, 사고경위 등을 잘 이해하고 있는 경우에는 안전기능 사건수목의 구성없이 직접 계통 사건수목을 구성할 수도 있다.

(1) 안전기능 사건수목 개발

안전기능 사건수목은 최종 결과물이 아니며 초기사건과 상세한 사고경위 및 완화특성 사이의 복잡한 관계를 밝히는 중간 단계의 작업이다. 안전기능 사건수목의 표제인 각 안전기능은 나중에 해당 안전기능을 수행하는 여러 계통들로 분해되고 이에따라 보다 상세한 사건수목이 구성된다. 이렇게 사건수목 표제에 계통들이 등장하는 사건수목을 계통 사건수목이라 한다. 그림 6은 대형 LOCA에 대한 전형적인 안전기능 사건수목을 보여주고 있다.

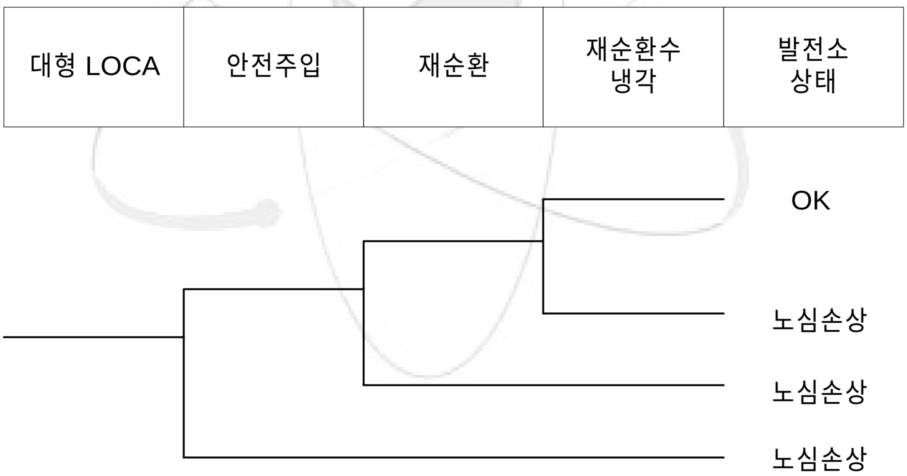


그림 6. 대형 LOCA 안전기능 사건수목

안전기능 사건수목은 계통 사건수목을 개발하기 위한 준비 단계의 하나로 구성한다. 따라서 안전기능 사건수목과 계통 사건수목의 노심손상 과정이 논리적으로 일치하여야 한다. 안전기능 사건수목의 표제인 안전기능은 여러 계통에 의하여 수행되고 어떤

계통은 한 개 이상의 여러 기능을 수행하기도 한다. 또한 초기사건에 따라 안전기능의 성공기준이 다를 수 있다. 표 15은 대형 LOCA에 대한 안전기능과 관련 계통의 성공기준을 보여준다. .

초기사건에 따라 동일한 안전기능도 다른 계통에 의해 수행되기도 한다. 예를 들면 RCS냉각재의 주입은 소형 LOCA시 고압 안전주입계통이 수행하고 대형 LOCA시에는 저압 안전주입계통이 수행한다. 안전기능은 일차적으로 공학적 안전설비 계통이 담당하나 이들 안전계통 이외의 타 계통도 안전기능을 담당할 수 있다. 예를들면 이차측 급수공급 계통이나 증기방출계통은 과도사건이나 소형 LOCA시 RCS 열을 제거하는 안전기능을 수행하므로 이들 계통도 분석 대상에 포함된다. 1차측기기냉각수계통이나 전기계통 등과 같은 보조계통들은 직접 안전기능은 수행하지 않으나 안전기능을 수행하는 주요계통의 운전에 중대한 영향을 미치므로 이들 보조계통도 연계되어 있는 타 계통의 고장수목 모델링에 반드시 포함하여야 한다. 초기사건 및 사건수목 분석 단계에서 각 계통에 대한 성공기준이 결정된다. 계통 성공기준은 유량과 여유시간 등의 성능기준뿐만 아니라 필요 펌프수, 유량 트레인수, 계측 트레인수, 전기부스 등과 같이 구체적 숫자로 표현한다. 이러한 기기의 갯수로 나타낸 성공기준은 각 계통 고장수목 구성의 기본 조건이 된다.

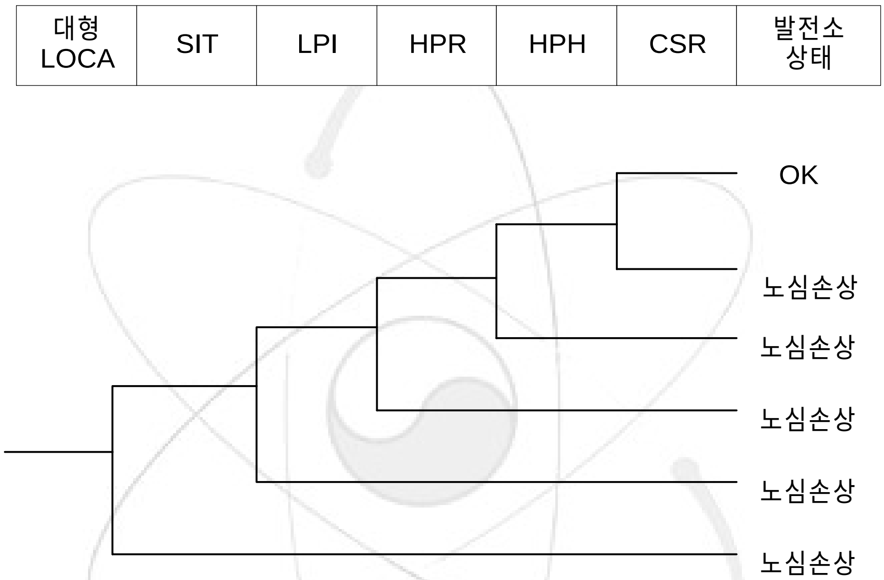
표 15. 대형 LOCA 성공기준

사건수목 표제	성 공 기 준
반응도 제어	원자로 정지 필요 없으나 장기적 반응도 제어를 위해 붕산수 주입
안전 주입 운전	안전주입탱크 (3/3) AND 저압안전주입 (1/3 저온관 + 1/2 저압안전주입 펌프)
재순환 운전	고압안전주입계통을 통한 재순환 (1/3 저온관 + 1/2 고압안전주입 펌프) AND 고압안전주입계통을 통한 고온관 /저온관 재순환 (1/2 고온관 + 1/2 고압안전주입 펌프)
재순환수 냉각	격납건물 살수계통을 통한 재순환수 냉각 (1/2 살수계통 펌프 및 관련 열교환기)

(2) 계통 사건수목 개발

안전기능 사건수목이 구성되면 초기사건에 따라 각 안전기능 표제를 계통 단위로 보다 세분화한 계통 사건수목을 구성한다. 그림 7은 그림 6의 안전기능 사건수목을 계통 사건수목으로 개발한 것이다. 안전기능 사건수목은 대체적인 사고경위를 밝혀주나 계통 사건수목은 더 상세한 계통 단위의 사고 시나리오 전개 상황을 알려준다.

계통 사건수목에는 다음과 같은 자세한 정보가 포함된다. 첫째, 계통 성공기준이 표현된다. 비록 동일한 안전기능이라도 초기사건에 따라 그 기능을 수행하는 계통이 다를 수 있고, 같은 계통이라도 초기사건에 따라 계통내에서 요구되는 성공기준, 즉 필요한 기기수가 달라질 수 있다. 둘째, 초기사건과 계통사이의 연관성이 표현된다. 어떤 초기사건은 안전기능의 일부나 특정 계통에 직접적인 영향을 줄 수 있다. 따라서 초기사건에 따라 이용 가능한 계통이 다를 수 있다. 즉 소외전원상실사고시 RCS 열제거를 위한 동력변환계통의 사용이 불가능한 것이나, 발전소 정전사고시 모든 전기구동 기기가 작동 불가능하게 되는 것이 대표적인 예이다.



여기서, SIT : 안전주입탱크, LPI : 저압안전주입, HPR : 고압 재순환 운전
HPH : 고압 안전주입계통을 이용한 저온관/고온관 동시 주입
CSR : 격납용기 살수계통을 이용한 재순환수 냉각

그림 7. 대형 LOCA 계통 사건수목

계통 사건수목은 안전기능 사건수목에 나타난 여러 안전기능에 대한 정보를 사용한다. 그러나 계통 사건수목상의 사고경위가 안전기능 사건수목의 것과 다소 차이가 있을 수 있다. 이것은 어떤 계통의 고장이 여러 기능을 동시에 불가능하게 할 수도 있기 때문이다.

각 계통 사건수목의 표제로서 계통이나 계통의 그룹들이 나타난다. 정확한 표제 배열의 순서는 결과에 큰 영향을 주지는 않지만 분석의 효율성과 논리의 명확성 관점에서 매우 중요하다. 사고경위의 수는 적절히 표제를 배열함으로써 감소시킬 수 있다. 표제 배열의 주요 세가지 인자는 시간, 기능 및 하드웨어적 관련성이다. 표제 배열의 초기단계에서는 시간인자를 고려하는 것이 바람직하다. 즉 1차 안전계통들을 사고경위에 따라 요구되는 시간 순서로 배열하는 것이다. 따라서 즉시 반응하는 계통(원자로보호계통 등)이 가장 먼저 위치하고 시간 순서에 따라 관련 계통을 배치하는 것이다. 그러나 반응시간만이 표제 배열의 절대적인 기준은 아니다. 계통 사이의 기능 및 하드웨어적 관련성이 사건수목 표제 순서 결정시 또한 고려되어야 한다. 한 계통이 여러 운전모드에 관련있는 것과 같이 하드웨어의 관련성도 순서에 영향을 준다.

계통 사건수목은 사고경위 앞 과정에서의 경계조건에 따라 표제로 모델링된 각 계통의 성공과 실패를 이분 수목으로 표현한다. 사건수목의 각 표제에서의 성공 혹은 실패의 선택은 다음의 모든 질문에 '아니오'라고 대답할 수 있으면 제거될 수 있다. 그러나, 어느 한 질문에라도 '예'라는 대답이 나오면 그 표제에서 성공 혹은 실패의 선택을 하여 사고경위를 모델링하여야 한다.

- 표제의 성공 혹은 실패가 사고경위 결과에 영향을 주는가?
- 표제의 운전이 안전기능에 기여를 하는가?
- 표제의 운전이 타계통의 운전과 필요성에 영향을 주는가?

각 계통 사건수목의 표제는 궁극적으로 기기 단위의 논리 구조로 모델링되고, 정량화하여야 한다. 이를 위하여 각 계통의 고장수목을 구성해야 하며 이러한 고장수목을 구성하기 위하여서는 각 계통의 고장(혹은 기능상실)기준을 정의해야 하는데 이는 해당 계통의 성공기준에 근거하여 정의한다. 또한 계통 고장기준은 사건수목 표제위치에 따라 영향을 받는다. 이러한 영향은 계통 고장수목 구성을 위한 경계조건으로 정의한다. 계통 고장기준은 일반적으로 초기사건 발생후 열유체 계산에 기준하여 결정한다. 예를들면 LOCA후 노심손상을 막기위한 안전주입 유량의 결정 등이다. 계통 성공 혹은 고장기준 결정시에는 여러 자료가 필요하다. 가장 좋은 데이타는 사고발생후 현실적 가정하에서 계산된 열유체 분석결과 데이타이다. 이러한 분석자료가 없을 때에는 최종 안전성분석보고서(FSAR)의 분석 결과를 성공기준으로 사용할 수 있다.

제5장 계통 고장수목 분석

제1절 개요

1. 목적

본 계통분석 절차서는 원자력발전소의 확률론적 안전성평가 (Probabilistic Safety Assessment : 이하 PSA)에서 계통분석 기법으로 널리 이용되고 있는 고장수목 분석의 절차와 기법을 기술하여 PSA 수행 시 대상 계통을 일관성 있고 기술적으로 정확하게 분석하는 지침을 제공하고자 한다.

2. 적용 범위

본 계통분석 절차서는 설계 중인 원전에 대하여 그 동안 국내에서 수행되었던 PSA의 계통분석 절차 및 방법을 기본적으로 정리하였다. 따라서 본 절차서에 기술된 고장수목 분석의 방법 및 수준은 국내의 설계 중인 원전 PSA에 적용된 계통분석에 준하는 것으로서, 향후 설계 중 원전 PSA의 계통분석에 적용할 수 있을 것이다.

3. 참고문헌

계통분석 방법에는 여러 가지가 기법이 있으나, 본 절차서는 특별히 원자력발전소 확률론적 안전성평가(PSA)에서 사용되는 고장수목 분석을 대상으로 기술하였다. 고장수목 분석에 대한 참고문헌으로는 여러 종류가 있으나, 본 절차서를 작성하기 위해 참고한 대표적인 문헌은 다음과 같다.

[1]"PRA Procedure Guide", NUREG/CR-2300", ANS and IEEE, 1982.

[2]"Probabilistic Safety Analysis Procedures Guide", NUREG/CR-2815, 1984.

[3]"Procedures for Conducting Probabilistic Safety Assessment of NPPs (Level 1)", IAEA, 1992.

[4]"고리 3,4 호기 및 영광 1,2 호기 PSA 수행절차서", 한국전력공사, 1992.

[5]"Fault Tree Anlaysis Guidelines", Commonwealth Edison IPE/Accident Management Program, Rev.0, 1990.

4. 기본가정 및 용어정의

본 절차서는 설계중인 원전인 영광5,6호기 전출력 Level 1 PSA에 적용하기 위해 작성한 절차서로서 그 동안 국내에서 수행되었던 설계중인 원전 PSA의 계통분석 방법에 근거하여 작성한 것이다. 따라서 만일 운전 중인 원전의 계통분석이나 전출력 이외의 운전모드에서의 계통분석을 위해서는 필요에 따라 일부 내용을 수정하여 사용할 수 있다.

계통 고장수목 분석에서 사용되는 주요 용어는 다음과 같다.

PSA	확률론적 안전성 평가
노심손상빈도	노심손상 사고가 발생할 수 있는 빈도로 1년 단위로 계산된다.
KIRAP	한국원자력연구소에서 개발한 PSA 수행용 전산코드 패키지
기본사건	고장수목 논리 전개에서 최종 하부에 위치하는 사건들로서 신뢰도 자료의 입력이 가능한 기본 단위. 기기의 기계적 고장, 보수 및 시험 이용불능 사건, 인간오류 사건 등이 포함된다.
최소단절집합	계통 실패 또는 노심손상을 발생시킬 수 있는 기본사건들의 조합
고장수목	계통 실패에 대한 원인들을 논리적으로 추적해나가는 도식적 모델
사건수목	사건이 발생한 후 계통 작동 유무에 따라 어떠한 사고로 전개되는가를 나타내는 모델
사고경위	사건수목에서 계통 작동 유무에 따라 전개되는 사고 시나리오. 하나의 사고경위는 어떠한 초기사고가 발생한 후 어떠한 계통들이 작동하였고 어떠한 계통들이 실패하였는지에 따라 정해진다.
초기사건	원전 정상운전 중 이상사태를 발생시킬 수 있는 사고. PSA 에서는 유사한 사고들을 그룹화하여 하나의 초기사건으로 처리하며, 대부분의 경우 원자로 정지로 이어지는 사고만을 취급한다.

제2절 분석 절차

계통 고장수목 분석의 절차는 크게 계통분석 기본 준비단계와 개별 계통에 대한 고장수목 분석으로 구분할 수 있다. 계통분석 기본 준비는 여러 계통에 공통적으로 적용되는 지침이나 정보, 계통분석의 범위, 분석 수준, 기본 가정, 계통간 연관관계,

고장수목 명명법 등 전체 계통분석 방법의 통일성이나 효율성을 얻기 위해 필요한 사전 준비 작업이다. 반면 개별 계통에 대한 고장수목 분석 절차는 앞에서 정리한 기본 지침을 바탕으로 단위별 계통에 대한 구체적 고장수목의 구성 및 정량화 순서 및 방법을 의미한다.

1. 계통분석 기본 준비 절차

원자력발전소의 계통분석에는 모든 안전계통과 관련 보조계통들이 포함된다. 또한 계통분석에는 일반적으로 여러 분석자가 참여한다. 따라서, 여러 분석자가 여러 계통을 분담하여 고장수목을 구성하고 분석하기 위해서는 사전에 세부적인 방법 및 절차에 대한 통일된 지침이 필요하다. 계통 고장수목 분석을 위해 기본적으로 준비해야 되는 내용은 다음과 같다.

- 고장수목 분석 지침
- 고장수목 기본사건 및 게이트 명명법
- 대상 계통 선정 및 계통 경계 구분
- 계통간 연계성 및 종속성

가. 고장수목분석 지침 작성

분석의 통일성을 갖는 계통 고장수목 분석을 위해서는 기본적으로 본 절차서와 같이 고장수목 구성과 정량화 과정에 대한 구체적인 지침 및 대강의 순서를 정하여야 한다. 물론 분석 초기 단계에서부터 완전한 절차서가 준비되어야 하는 것은 아니며, 분석 과정을 거치면서 세부적인 지침이나 수행 절차가 수정되고 보강된다.

고장수목 분석의 기본적인 성격은 대상 PSA의 목적과 범위, 분석 수준에 의해 결정된다. 대상 계통, 사용되는 기기 신뢰도 자료, 발전소 운전 상태 등이 PSA 성격에 의해 좌우되며, 이에 따라 계통 고장수목의 내용 및 수준, 기본적인 가정사항 등이 결정된다.

나. 고장수목 기본사건 및 게이트 명명법

여러 계통의 고장수목이 동시에 모델링 되기 위해서는 관련된 계통, 기기, 고장원인 등이 체계적으로 분류되어 사용될 수 있는 코드가 사전에 개발되어야 한다. 이 코드는 고장수목 구성시 기본사건 및 게이트 이름에 사용되어 전산코드 사용 시 효율적인 자료 관리를 가능하게 하고, 또한 정량화 결과로 얻는 최소단절집합의 의미를 쉽게 파악할 수 있게 한다.

다. 대상 계통 선정 및 계통 경계 구분

계통분석을 위해서는 사전에 분석 대상 계통이 선정되며 서로 연계되어 있는 계통들 간의 물리적 구분이 결정되어야 한다. 대상 계통의 선정 및 정점사건(Top Event)의 결정은 초기사건 분석 및 사건수목 분석을 통해 결정된다. 계통분석 단계에서는 선정된 대상 계통의 고장수목 구성을 위해서 정점사건으로 정의된 계통의 기능을 검토하여 계통 내의 분석 대상이 되는 부분을 파악하고, 타 계통과의 연계부분이 있는 경우에는 이들 계통과의 물리적 경계를 결정하여 계통별 고장수목의 대상을 명확히 한다.

라. 계통간 연계성 및 종속성

위에서 언급하였듯이 계통분석을 위해서는 타 계통과의 기능적, 물질적 연관 관계를 파악해야 한다. 계통별 고장수목을 구성하기 위해서는 앞 절에서 정의한 계통 경계에 따라서 계통별 고장수목이 구성되고, 이들 정보가 관련된 연계 계통의 고장수목에 명확히 모델링 되어야 계통간 기능적, 물질적 연계성 및 종속성을 정확히 고려할 수 있다. 따라서, 개별 계통 단위의 고장수목 구성에 앞서 계통간 연계성이 파악되고 이들 연계성이 고장수목 명명법에 의해 정의되어 타 계통 고장수목 구성 시 입력으로 사용될 수 있도록 준비되어야 한다.

2. 단위별 계통분석 절차

계통분석을 위한 자료 조사 및 기본 준비가 완료되면 개별 계통에 대한 구체적이고 상세한 계통 고장수목 분석이 시작된다. 단위별 계통 고장수목 분석은 초기사건 분석 및 사건수목 분석 단계에서 결정된 각 계통 고장수목의 정점사건(Top Event)과 이에 대한 성공기준을 이해하는 것에서부터 시작한다. 해당 계통의 설계 및 운전 정보, 기술지침, 타 계통과의 연계성 등 대상 계통에 대하여 충분히 숙지한 다음 정점사건을 유발하는 사건들의 조합을 고장수목 구성 기법에 따라 연역적으로 추적하여 고장수목을 구성한다. 마지막으로 각 기본사건들에 대한 고장률이나 작동시간 등 기본사건 이용불능도 계산을 위한 자료를 입력하고, 정점사건의 발생 확률을 정량화 한다. 고장수목의 구성 및 자료 입력, 정량화 과정에는 이를 지원하는 소프트웨어가 사용된다. 계통 고장수목 분석의 일반적인 수행 절차는 다음과 같다. 항목별로 세부적인 내용은 본 절차서 부록에 상세히 기술하였다.

가. 계통분석 기본 지침 이해

단위별 계통 고장수목 분석이 시작되면 우선 모든 분석자들이 이전 단계에서 준비한 계통분석 기본 지침 및 절차를 숙지한다. 세미나 혹은 교육 프로그램을 통하여 기본

지침을 이해하고, 계통 고장수목 구성 시 유의할 점을 확인한다. 기본 지침에는 본 절차서에서 언급하는 모든 내용이 포함된다.

나. 계통 설계 및 운전 정보 이해

담당 계통에 대하여 필요한 모든 설계 및 운전 정보를 이해한다. 계통분석을 위해서는 최소한 대상 계통의 기능 및 운전, 주요 기기의 특성을 잘 알고 있어야 하며, 기술지침서의 제한 사항, 시험 및 보수 방법 등에 대한 이해도 필요하다. 이를 위해 설계 및 운전에 관련된 대표적인 참고문헌을 검토, 정리한다. 주요 참고문헌으로는 계통설명서 및 P&ID(Piping & Instrument Diagram), 예비 및 최종 안전성분석보고서의 계통 설명 및 기술지침서, 운전지침서 등이 있으며, 만일 유사한 발전소가 운전 중에 있으면 관련 계통에 대한 운전절차서 및 교육 자료를 참고한다.

다. 정점사건의 정의 및 성공기준 이해

계통의 기능 및 운전을 어느 정도 이해하면 구성해야 할 계통 고장수목의 정점사건을 이해한다. 정점사건 및 관련 성공기준은 사건수목 분석 단계에서 결정되는데, 관련 사고경위와 계통 정점사건이 결정된 배경을 간단히 이해하고, 여러 개의 정점사건이 정의된 경우에는 정점사건 간의 성공기준 차이를 명확히 숙지한다.

라. 단순계통도 작성

정의된 정점사건과 관련된 계통 기능을 수행하기 위해 필요한 계통 내 배관 및 기기를 확인한다. 다음은 P&ID를 근거로 고장수목 구성을 위한 단순 계통도를 작성한다. 이 과정을 거치면서 계통 내 각 배관의 기능 및 계통 내 기기간의 상호 연계성을 파악한다. 단순계통도 작성 요령은 부록에 상세히 기술하고 있다.

마. 타 계통과의 연계성 파악

타 계통과의 대략적인 연계성은 고장수목 분석 기본 준비 과정에서 정리되었다. 본 절차에서는 관련 기기, 연계된 타 계통의 기기 이름 및 기능, 전이 게이트 명칭 등 구체적인 연계 정보를 표로 정리한다. 이 정보는 관련 기기의 하부 고장수목 구성 시 사용된다.

바. 고장수목의 구성

위의 단계가 어느 정도 완료되면 고장수목 구성을 시작한다. 고장수목 구성의 기본 원칙과 기본사건 명명법에 따라 정점사건에 대한 고장논리를 전개한다. 계통은 편의에 따라 몇 개의 단락(Segment)으로 구분하고, 이를 다시 기기 단위로 나누는 Top-Down

방식으로 고장수목을 구성한다. 기본사건이나 게이트에 대한 설명문도 가능한 통일된 방법에 따라 작성한다. 특히 주요 기기에 대해서는 기본적인 표준 고장수목 논리를 따르므로 가능한 통일된 고장수목을 구성한다. 인간오류, 공통원인고장, 시험/보수로 인한 요인 등도 미리 정해진 방식에 따라 모델링 한다.

사. 고장수목 정량화

고장수목 정량화를 위해 필요한 신뢰도 자료나 시험 및 보수에 대한 정보를 입력해야 한다. 우선 기기의 운전 형태에 따른 이용불능도 계산 방식을 이해하고, 기기별로 이용불능도를 계산에 필요한 입력 자료를 수집, 정리한다. 계통단위에서는 주요 기기의 시험 혹은 보수 주기, 기기 타입에 따른 고장률, 평균 보수시간, 예방정비 빈도 및 기간 등이 정리되어야 한다.

계통 이용불능도 계산 및 중요도 정량화는 관련 전산코드를 이용하므로 절차에 따라 정량화 한다. 정량화 과정에서 얻어진 정점사건에 대한 최소단절집합을 검토하여 고장수목 논리에 문제점이 없는지 확인한다. 또한 이 과정에서 고장수목 상에는 모델링하지 못했지만, 기술지침서의 내용을 위배하거나 논리적으로 일어날 수 없는 최소단절집합은 삭제한 후 최종 정량화 계산을 한다.

3. 문서화

계통 고장수목분석을 수행한 결과로서 다음과 같은 내용을 문서화한다.

- 계통 고장수목 방법론
- 기본 가정사항
- 계통설명 및 운전
- 시험/보수 방법 및 기술지침
- 정점사건 및 성공기준
- 계통 연계성
- 정량화 결과 및 해석

제3절 계통 고장수목 상세 분석 방법

1. 계통분석 방법론

계통의 기능 상실을 초래하는 모든 사건 조합을 체계적으로 분석하고 그 발생 가능성을 평가하는 작업을 계통분석(System Analysis)이라 한다.

PSA 최종 목표 중 하나는 초기사건 및 사건수목 분석을 통해 파악된 노심손상 사고경위들의 발생빈도를 추정하는 것이다. 노심손상 사고경위란 초기사건발생 후 관련 안전계통들이 기능 상실하여 노심손상을 초래하는 사건 조합을 의미하며, 노심손상 빈도는 초기사건 발생빈도 및 관련된 계통들의 고장 조합 확률로부터 계산된다. PSA에서의 계통분석 목적은 계통의 기능 상실을 유발하는 사건 조합을 파악하고 그 발생 확률을 계산하여 노심손상빈도 계산의 입력 자료를 제공하는 것이다. 이 과정은 결국 계통 단위의 신뢰도분석을 의미하는 것으로서, 계통의 설계, 운전, 시험 및 보수 등 계통에 대한 체계적인 정성분석과 계통의 이용불능도를 추정하는 정량분석 단계로 구성된다.

계통분석 방법에는 수행 목적 및 수준에 따라 적용 가능한 여러 가지 분석 기법이 있다. 대표적 기법으로는 고장모드 및 영향분석(Failure Mode and Effect Analysis), 주논리도(Logic Diagram), 성공수목(Success Tree), 고장수목(Fault Tree) 등이 있다. 본 절차서에는 PSA에서 사용되는 고장수목(Fault Tree) 분석 방법에 대하여 기술한다.

가. 고장수목 분석

(1) 배경

이 기법은 1962년에 미국의 Bell 전화연구소 (BTL, Bell Telephone Laboratories) 의 H. A. Watson 에 의해서 개발되었다. 이 후 Minuteman Missile 의 발사 제어 계통을 평가하는데 사용되었으며 항공우주 분야에 적용되었다. 그러다 1975년 상업용 원자력발전소의 확률론적 안전성평가에 대한 최초 보고서인 WASH-1400이 나온 이 후 원자력분야에서 널이 이용되기 시작하였으며, 근래에 와서 모든 산업 분야의 신뢰도 및 안전성 평가의 대표적인 방법으로 사용되고 있다.

고장수목 분석은 계통의 기능상실을 초래하는 사건의 원인을 논리적으로 해명해 가는 분석 방법이다. 이 방법은 계통의 기능상실 논리를 연역적으로 전개하는 해석기법으로서, 복잡한 계통에 대한 상세한 분석이 가능하고 정량적 해석, 시각적

표현 등의 특징을 지녔다. 또한 고장모드 및 영향 분석에 비하여 인적요인, 공통원인고장 등 복합요인을 다룰 수 있다.

고장수목분석은 되도록 이면 설계 초기단계부터 적용하는 것이 바람직하다. 계통구성의 상세한 설계가 없는 상태에서도 계통의 기능상실을 초래하는 바람직하지 못한 사건들을 고장수목 분석을 통해 파악할 수 있으며, 이를 통해 상세 설계단계에서 보다 안전하고 개선된 계통을 설계할 수 있다.

(2) 고장수목 분석 방법론

고장수목분석은 분석대상 계통이 이용불능 상태가 되는 모든 경우를 논리적인 도형으로 표현하는 방법이다. 계통의 기능 실패 상태를 확인하고, 계통의 환경 및 운전 등을 고려하여 계통의 기능 상실을 초래하는 모든 사건 및 그 발생 논리를 도식적으로 분석한다. 일단 계통의 기능 상실을 정점사건(Top Event)으로 정의하고 그러한 정점사건이 발생할 수 있는 경로를 연역적으로 추적하는 분석 방법이다.

본 방법을 수행하기 위해서는 발전소의 계통이 어떻게 작용하는가를 완전히 이해해야 하고 고장모드 및 영향분석 또는 고장모드, 영향 및 위험성 분석(Failure Modes, Effects & Criticality Analysis)을 통하여 그것을 구성하는 기기의 고장모드와 계통에 미치는 영향을 파악하는 것이 무엇보다 중요하다. 그리고 분석자는 계통 및 기기에 경험이 있는 기술자, 운전자와 다른 전문가 등의 자문을 얻어 고장수목을 구성해야 하고 사고의 원인이 되는 결함들과 고장들을 결정하기 위해 필요한 정보들을 확인하여야 한다. 만약 매우 복잡한 계통분석을 위한 고장수목 구성 시에는 팀에 의한 접근이 바람직하다. 즉 고장수목 구성에 참여하는 팀원들과 기타의 경험을 갖는 개개인의 의견교환은 계통분석을 수행하기 위해 절대적으로 필요하다. 그리고 고장수목 구성 시 소요되는 시간과 노력은 사고사건과 분석결과의 수준을 포함한 계통의 복잡성에 따라서 차이가 있다. 즉, 경험을 갖고 있는 팀이 단순한 공정 단위를 모델링 하는 데에는 비교적 짧은 시간을 요구하지만 많은 위험을 갖고 있는 복잡한 공정에 대한 모델링은 상대적으로 많은 시간을 필요로 한다.

Fussel 은 고장수목 분석을 통하여 다음과 같은 가치를 파악할 수 있다고 한다.

- 직접적으로 사고의 원인이 되는 결함과 고장을 예측할 수 있다.
- 주어진 결함에 대한 중요도를 계통의 관점에서 지적할 수 있다.
- 분석 계통을 정성적이고, 정량적으로 해석할 수 있다.
- 계통의 거동에 대한 사항을 알 수 있다.

확률론적 안전성 평가에서 사건수목 및 고장수목은 예상되는 초기사건으로 인해 발생할 수 있는 결과를 구체화하기 위하여 사용된다. 중요한 계통의 성공 및 실패 여부는 사건수목에서 결정되며, 계통모델을 통하여 계통 실패의 원인을 확인할 수 있다. 계통 모델은 기기 고장뿐만 아니라 계통 수행에 영향을 미치는 검사, 보수, 인간오류, 공통원인고장 등을 포함한다.

고장수목은 관련 계통에서 발생할 수 있는 모든 기기의 고장을 포함하지는 않는다. 이것은 계통의 정점사건, 즉 사건수목에서 정의된 계통의 기능에 좌우된다. 정의된 계통 기능의 상실을 초래하는 모든 기기의 고장이 고장수목 구성의 대상이 된다. 기기별 고장모드의 선택은 상세 고장수목 절차, 계통설계에 관한 정보 및 계통 운전, 운전 이력, 유용한 기초자료의 상세 정도 및 분석자의 경험 등을 바탕으로 결정한다.

각 분석대상계통의 고장수목 분석 결과는 사건수목에 입력되어 각 사고추이 사건들이 실패가 되는 모든 조합들을 밝혀내고 정량화 하게 된다. 이로부터 각 사고추이의 발생 빈도를 구하여 발전소 노심손상 빈도를 계산하게 된다. 그림 8은 고장수목 분석을 수행하기 위한 일반적인 절차를 보여주며, 표 16은 일반적으로 사용되는 고장수목의 기호를 나타낸다.

(3) **기본사건 및 게이트 명명법** (Naming Convention)

복잡한 계통의 고장수목 분석을 위해서 사전에 준비해야 되는 것 중의 하나가 기본사건 및 게이트 명명법이다. 원자력이나 석유화학과 같은 대형 시스템들의 계통들은 대부분 대형 고장수목으로 표현된다. 이와 같은 대형 고장수목을 구성하고 분석하기 위해서는 기본사건 및 게이트에 대한 체계적인 명명법이 준비되어야 한다. 이름을 통해 해당 기본사건이 어떤 계통, 어떤 기기의 어떤 종류 고장인지를 쉽게 파악할 수 있도록 통일된 명명법을 준비한다. 최소한 계통명, 기기명, 고장모드명, 트레인 구분 등이 기본사건 이름에 포함되도록 한다. 본 장 3절에 영광5,6호기 PSA에서 사용하였던 기본사건 및 게이트 명명법을 수록하였다.

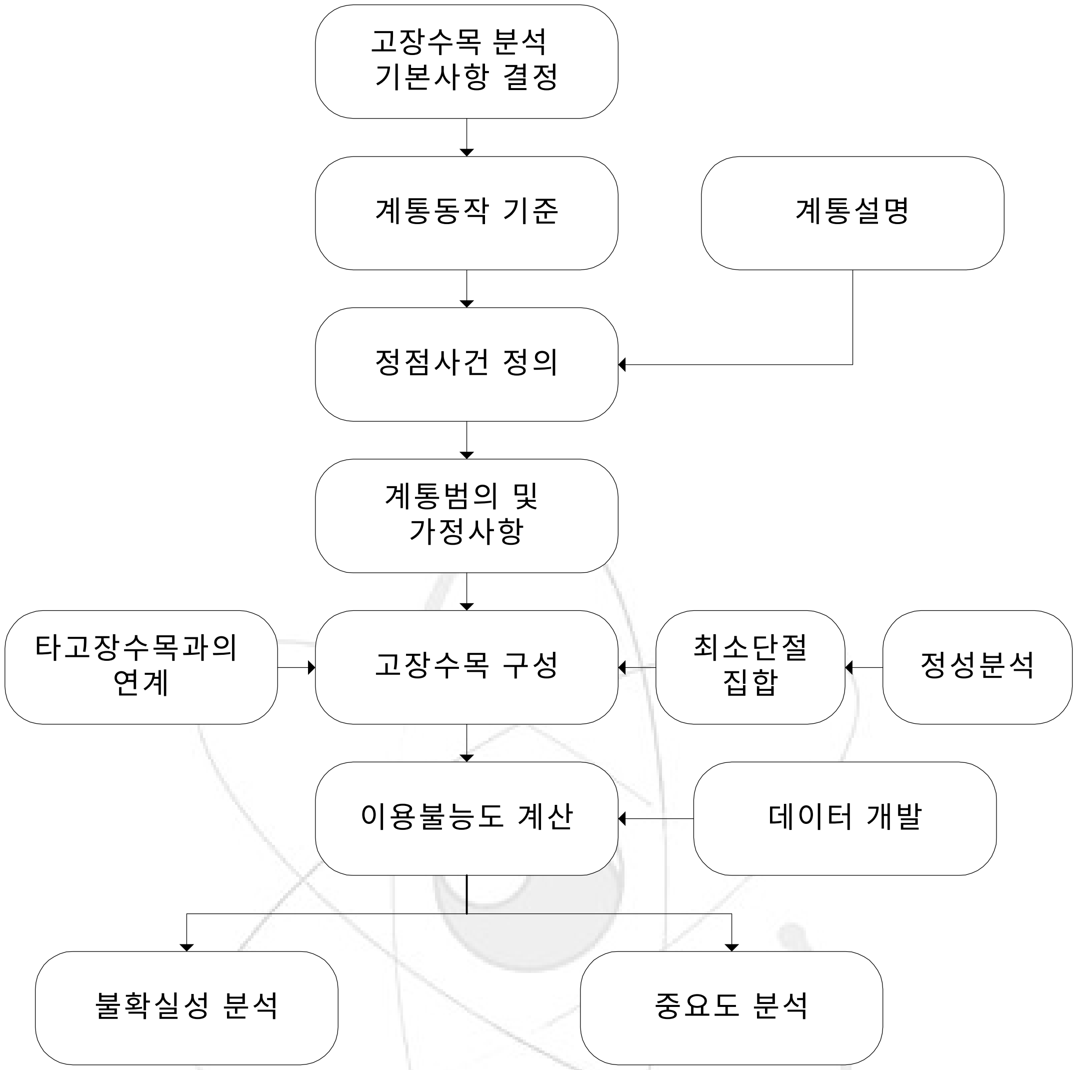
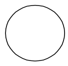
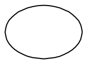
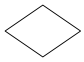
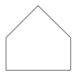
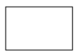
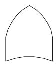
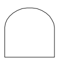
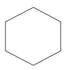
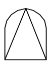
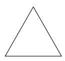


그림 8. 고장수목 분석 절차

표 16. 고장수목에서 사용되는 일반적인 기호

기 호	명 명	기 호 설 명
	기본사건 (Basic Event)	더 이상 개발되지 않는 원인 사건
	조건부사건 (Conditional Event)	논리 게이트에 연결되어 사용되며, 논리에 적용되는 조건이나 제약 등을 명시함. (Priority, Inhibit 게이트에 우선적으로 적용)
	미개발사건 (Undeveloped Event)	사고결과나 관련정보가 미비하여 계속 개발될 수 없는 특정 초기사건
	외부사건 (External Event)	유동계통의 층 변화와 같이 일반적으로 발생이 예상되는 사건
	중간사건 (Intermediate Event)	한 개 이상의 입력사건에 의해 발생된 고장사건으로서 주로 고장에 대한 설명이 서술된다.
	OR gate	한 개 이상의 입력사건이 발생하면 출력사건이 발생하는 논리 게이트
	AND gate	입력사건이 전부 발생하는 경우에만 출력사건이 발생하는 논리 게이트
	Inhibit gate	AND 게이트의 특별한 경우로서 이 게이트의 출력사건은 한개의 입력사건에 의해 발생하는데, 입력사건이 출력사건을 생성하기 전에 특정조건을 만족하여야 한다.
	Exclusive OR gate	OR 게이트의 특별한 경우로서 입력사건 중 오직 한 개의 발생으로만 출력사건이 생성되는 논리 게이트
	Priority AND gate	AND 게이트의 특별한 경우로서 입력사건이 특정 순서별로 발생한 경우에만 출력사건이 발생하는 논리 게이트
	전이기호 (Transfer Symbol)	다른 부분에 있는 (예:다른 페이지) 게이트와의 연결관계를 나타내기 위한 기호로서 Transfer In 과 Transfer Out 이 있다.

나. 고장수목분석 기본준비

(1) 대상 계통의 선정 및 분류

PSA에서 가장 중요한 업무 중 하나는 노심손상을 초래하는 사고경위들을 파악하는 것이다. 노심손상 사고경위의 파악은 초기사건 분석 및 사건수목 분석을 통하여 이루어진다. 이 과정에서 초기사건이 발생한 후 노심을 건전하게 유지하고 사고를 종료시키기 위해 필요한 계통들이 파악되며, 해당 계통들이 기능을 수행하기 위해 필요한 보조계통들이 결정된다.

영광5,6 호기의 경우 사고경위를 파악하기 위해 소형 사건수목/대형 고장수목(Small Event Tree/Large Fault Tree) 방법을 사용하였다. 이 방법은 초기사건 발생 후 노심을 건전하게 유지하는데 직접적으로 필요한 계통들을 사건수목 표제로 모델링 하는 방법으로, 표제로 등장하는 계통들을 편의상 전위계통(Front-Line System)이라 명한다. 반면 동력공급, 기기 및 기기실 냉각과 같이 계통 운전에 필요한 계통들은 전위계통 고장수목에 연결하여 모델링 함으로써 계통간 상호 연관성을 반영한다. 전위계통을 지원하는 계통들은 보조계통(Support System)이라 칭한다.

예를 들면 사건수목에 나타나는 계통 중에 저압안전주입계통이 있다. 이 저압안전주입계통의 분석범위에는 저압안전주입펌프가 포함되는데, 저압안전주입펌프의 고장모드에는 일차측 기기냉각수계통의 실패로 인한 펌프 기능상실이 포함된다. 따라서 일차측 기기냉각수계통은 사건수목의 표제로서 나타나지 않지만 계통의 기능상 저압안전주입계통의 분석에 필요한 계통으로서 고장수목 분석 대상 계통에 포함된다. 또한 사건수목에 나타나는 계통 중에 잔열제거계통이 있다면 이 잔열제거계통의 분석 범위에는 잔열제거 열교환기가 포함되며, 잔열제거 열교환기의 고장모드에는 일차측 기기냉각수계통의 실패에 의한 열교환기 기능 상실이 포함된다. 따라서 일차측 기기냉각수계통은 사건수목의 표제로서 나타나지 않지만 계통의 기능상 잔열제거계통의 분석에 필요한 계통으로서 고장수목 분석 대상계통에 포함된다. 그리고 노심 손상을 예방하는데 중요한 역할을 하지는 못하나 방사선원항(Source Term)의 크기를 결정할 수 있는 계통도 고장수목 분석에 포함된다. 이렇게 볼 때 사건수목에 나타나는 모든 전위계통을 분석하다 보면 거의 모든 안전계통 및 보조계통이 분석대상에 포함된다.

따라서, PSA를 위해 선정된 계통들은 편의에 따라 사건수목의 표제(Heading)로 모델링 되는 전위계통(Front-Line System)들과 표제에 나타나지는 않지만 전위계통의 기능 수행에 필요한 보조계통(Support System)으로 분류한다. 예로써, 영광5,6호기 PSA에서 선정된 분석 대상 계통들을 표 17에 정리하였다.

표 17. 영광5,6호기 전위계통 및 보조계통 목록

구　　　분	계　통　목　록
전 위 계 통 (Front Line Systems)	고압안전주입계통 (High Pressure Safety Injection System)
	안전주입탱크 (Safety Injection Tank)
	저압안전주입계통 (Low Pressure Safety Injection System)
	정지냉각계통 (Shutdown Cooling System)
	격납건물살수계통 (Containment Spray System)
	안전감압계통 (Safety Depressurization System)
	화학 및 체적제어계통 (Chemical and Volume Control System)
	원자로냉각재 압력조절계통 (RCS Pressure Control System)
	보조급수계통 (Auxiliary Feedwater System)
	주급수계통 (Main Feedwater System)
	주증기계통 (Main Steam System)
보 조 계 통 (Support Systems)	공학적 안전설비작동계통(Engineered Safety Features Actuation System)
	원자로보호계통 (Reactor Protection System)
	증기발생기 취출계통 (Steam Generator Blowdown System)
	전력공급계통 (Electrical Power System)
	기기냉각수계통 (Component Cooling Water System)
	필수용수계통 (Essential Service Water System)
	필수냉수계통 (Essential Chilled Water System)
	공기조화계통 (Heating, Ventilation and Air Conditioning System)
	압축공기계통 (Instrument Air System)

(2) 계통분석을 위한 자료 수집 및 검토

계통 고장수목 분석을 위해 분석자는 대상계통과 관련된 정보를 수집하고 확인해야 한다. 이러한 정보의 대부분은 발전소 친숙화 과정에서 수집되며, 일반적으로 아래와 같은 정보들이 포함된다.

- 계통운전 (System Operation)
- 계통설계 (System Design)
- 계통기능 (System Function)

- 연계성 및 종속성 (Interfaces and Dependencies)
- 시험 및 보수 (Test and Maintenance)

상기 정보는 다음과 같은 자료 및 문서로부터 얻을 수 있다.

- 최종 안전성 분석보고서(FSAR)
- 설계문서 및 도면
- 발전소 매뉴얼(Station Manual)
- 전기 단선도(Electrical Single Line Diagram)
- 제어 및 작동회로도(Control and Actuation Circuit Diagram)
- 각종 절차서
  - 종합운전절차서(General Operating Procedure)
  - 계통운전절차서(System Operating Procedure)
  - 비상운전절차서(Emergency Operating Procedure)
  - 비정상 운전절차서(Abnormal Operating Procedure)
  - 정기점검 절차서
  - 시험 및 보수절차서
- 기술운영지침서(Technical Specification)
- 타 발전소 PSA 보고서
- 안전성 관련 각종 연구보고서

위의 자료 외에도 유사한 발전소의 주 제어실 운전원, 보수담당자 및 계통설계자와의 면담 결과, 발전소 방문을 통한 계통 숙지, 고장자료 등도 계통분석에 긴요한 자료가 된다.

계통 검토과정을 통해 기기의 위치, 운전 모드, 계통 구성, 운전조건 뿐만 아니라 대상계통이 발전소의 안전성에 미치는 영향을 개략적으로 판단하게 된다. 또한 상세분석에서 요구되는 각 대상계통에 대한 분석범위도 규정한다.

(3) 계통경계 (System Boundary) 의 구분

앞에서도 언급하였듯이 계통의 모든 부분이 고장수목 구성의 대상이 되는 것은 아니다. PSA에서 정의된 계통의 기능과 관련된 부분만이 계통분석의 대상이 되며, 이에 따라 고장수목 분석의 대상이 되는 계통의 영역이 정의된다. 또한 상호 연관된 여러 개의 계통을 동시에 모델링하기 위해서도 계통간의 물리적 구분이 필요하다. 특히 전위계통과

보조계통 사이 또는 보조계통들 간에는 물리적인 상호 연계(Interface) 부분이 있으므로, 계통간의 체계적인 모델링을 위해 계통경계는 명확히 정의되어야 한다.

보조계통의 고장수목은 보조계통이 영향을 미치는 모든 전위계통의 연계 부분까지 모델링 하여야 하며, 전위계통의 고장수목 모델은 일반적으로 연계된 보조계통과의 연결부분을 포함해서 모델링 한다. 예를 들어 잔열제거계통 열교환기의 고장수목에 기기냉각수계통이 보조계통으로 모델링 된다면, 기기냉각수계통으로부터 공통 모관을 통하여 잔열제거계통 열교환기까지의 냉각수 흐름은 기기냉각수계통의 고장수목에서 모델링 되어야 한다. 그러나 잔열제거계통의 열교환기로의 연결 배관에 설치된 차단 밸브는 잔열제거계통의 고장수목에서 모델링 한다. 일반적으로 이런 계통 경계는 해당 기기의 계통명에 의해 구분되나, 고장수목 모델링의 편의성에 의해 계통 경계가 결정되기도 한다.

고장수목 분석 시 전위계통간의 공통부분 역시 고려해야 할 대상 중 하나이다. 예를 들어 두 개의 계통이 같은 탱크로부터 냉각수를 공급 받거나 두 개의 계통이 같은 배관을 통하여 냉각수를 공급한다면, 고장수목 구성 시 이러한 공통부분의 조건을 반영하여야 한다.

(4) 계통 연계성 및 종속성 (System Interfaces & Dependency) 분석

보조계통은 일반적으로 어느 한 전위계통만을 지원하는 것이 아니라 여러 전위계통 및 다른 보조계통에 전기나 작동 신호, 냉각수 등을 공급한다. 다시 말하면, 한 계통의 기능 상실은 계통 자체 내의 기기 고장에 의해서 발생할 수도 있고, 전기공급 계통과 같은 보조계통의 기능 상실에 의해서도 발생할 수 있다. 이러한 계통간의 상관성을 종속성 혹은 공용성으로 표현한다. 계통 종속성은 두 계통간의 배타적 의존, 지원, 작동 또는 격리의 형태로 존재할 수 있다. 공용성은 한 계통이 다른 계통의 전체 또는 일부를 공유할 때, 또는 한가지 특정 기능의 수행에 두 계통 (또는 두 부품, 또는 한 계통과 다른 계통의 부품들) 이 관여할 경우에 생긴다. 예를 들어 고압안전 주입계통은 저압안전 주입계통, 정지냉각계통 및 관련 배관 및 기타 부품들을 공유한다.

계통 종속성은 두 계통이 서로 상관 관계를 가질 때 생긴다. 이러한 계통 종속성은 다음과 같은 조건에서 존재한다.

- 한 계통이 전원 또는 밸브 운전용 공기를 다른 계통에 의존할 경우
- 한 계통이 다른 계통을 작동시킬 경우, 예를 들면 안전주입 작동신호는 고압안전 주입펌프를 작동시킨다.
- 한 계통이 다른 계통의 기능을 지원할 경우, 예를 들면 기기냉각수계통은

정지냉각계통을 지원하여 기능을 수행할 수 있도록 해 준다.

따라서, 계통 고장수목 구성 시 자체 기기의 고장 논리뿐만 아니라 보조계통의 이상에 의한 기능 상실이 논리적으로 포함되어야 한다. 이런 경우 보조계통들의 고장수목을 별도로 구성하고, 보조계통 고장수목 혹은 그 일부를 다른 계통 고장수목의 전이(Transfer) 게이트로 모델링 함으로써 계통간의 종속성을 표현한다.

이렇게 계통간의 연관 관계를 정확히 모델링하기 위해서는 계통의 경계 및 타 계통과의 연관 관계를 상세히 조사해야 한다. 예를 들어 4.16kV AC 전력계통에 대한 고장수목은 그 4.16kV AC 모선에 연결된 모든 펌프의 고장수목에 전이 게이트로 모델링 된다. 계측 및 제어계통, 공기조화계통, 냉각수계통 등의 보조계통도 동일한 방식으로 그 연계성이 모델링 된다. 이러한 계통간 상호 연계성 및 종속성을 쉽게 확인하고 정의하기 위하여 고장수목 간의 연계 사항을 미리 조사하여 정리한 후 고장수목을 구성하는 것이 바람직하다.

표 18은 여러 계통간의 종속성과 공용성을 정리한 예이다. 이 표는 각 계통이 발전소의 다른 계통들과 연계하는 방식을 확인하기 위하여 작성된 것으로써, 수직축 (참조계통) 과 수평축 (연계계통) 모두 동일한 계통 목록을 갖는다. 참조계통과 연계계통 간의 관계를 나타내는 코드의 의미는 다음과 같다.

- 공통부품을 연계계통과 공유하는 계통 (CE)
- 연계계통에 의존하는 계통 (D)
- 연계계통을 지원하는 계통 (S)
- 연계계통을 작동시키는 계통 (A)
- 연계계통에 의해 작동되는 계통 (AB)
- 해당계통과 관련이 없는 계통 (공란)

표 18. 영광 5,6 호기 계통 연계성 및 종속성 (1/3)

Reference* Interfacing	HPSIS	LPSIS	SCS	CSS	SDS	AFWS
HPSIS	**	CE	CE	CE		
LPSIS	CE	**	CE	CE		
SCS	CE	CE	**	CE		
CSS	CE	CE	CE	**		
SDS					**	
AFWS						**
MFWS						CE
MSS						D
CVCS	CE	CE		CE		
EPS(Vital)	D	D	D	D	D	D
DG	D	D	D	D	D	D
CCWS	D	D	D	D		D
ESWS	D	D	D	D		D
ECWS	D	D	D	D		D
HVAC	D	D	D	D		D
IAS						D
ESFAS	AB	AB		AB		AB
RPS						AB

CE - Common Element

D - Dependent

S - Supports

A - Actuates

AB - Actuated By

* 표 19 참고

표 18. 영광 5,6 호기 계통 연계성 및 종속성 (2/3)

Reference* Interfacing	MFWS	MSS	CVCS	EPS (Vital)	DG	CCWS
HPSIS			CE	S	S	S
LPSIS			CE	S	S	S
SCS				S	S	S
CSS			CE	S	S	S
SDS				S	S	S
AFWS	CE	S		S	S	S
MFWS				S	S	S
MSS				S	S	S
CVCS				S	S	S
EPS(Vital)	D	D	D	**	S/D	S/D
DG	D	D	D	S/D	**	S/D
CCWS	D	D	D	S/D	S/D	**
ESWS	D	D	D	S/D	S/D	D
ECWS	D	D	D	S/D	S/D	S/D
HVAC	D	D	D	S/D	S/D	D
IAS	D	D	D			
ESFAS						
RPS						

CE - Common Element

D - Dependent

S - Supports

A - Actuates

AB - Actuated By

* 표 19 참고

표 18. 영광 5,6 호기 계통 연계성 및 종속성 (3/3)

Reference* Interfacing	ESWS	ECWS	HVAC	IAS	ESFAS	RPS
HPSIS	S	S	S		A	
LPSIS	S	S	S		A	
SCS	S	S	S			
CSS	S	S	S		A	
SDS	S	S	S			
AFWS	S	S	S	S	A	A
MFWS	S	S	S	S		
MSS	S	S	S	S		
CVCS	S	S	S	S		
EPS(Vital)	D	D	S/D			
DG	D	D	S/D			
CCWS	D	D	S/D			
ESWS	**	D	S/D			
ECWS	D	**	S/D			
HVAC	D	S/D	**			
IAS				**		
ESFAS					**	
RPS						**

CE - Common Element

D - Dependent

S - Supports

A - Actuates

AB - Actuated By

* 표 19 참고

표 19. 영광 5,6 호기 계통코드

계 통 코 드	계 통 이 름
HPSIS	고압안전주입계통 (High Pressure Safety Injection System)
SIT	안전주입탱크 (Safety Injection Tank)
LPSIS	저압안전주입계통 (Low Pressure Safety Injection System)
SCS	정지냉각계통 (Shutdown Cooling System)
CSS	격납건물 살수계통 (Containment Spray System)
SDS	안전감압계통 (Safety Depressurization System)
CVCS	화학 및 체적 제어계통 (Chemical and Volume Control System)
RCSPCS	원자로냉각재계통 압력제어계통 (RCS Pressure Control System)
AFWS	보조급수계통 (Auxiliary Feedwater System)
MFWS	주급수계통 (Main Feedwater System)
MSS	주증기계통 (Main Steam System)
SGBS	증기발생기 취출계통 (Steam Generator Blowdown System)
EPS	전력공급계통 (Electric Power System)
DG	디젤발전기 (Diesel Generator)
CCWS	기기냉각수계통 (Component Cooling Water System)
ESWS	필수용수계통 (Essential Service Water System)
ECWS	필수냉수계통 (Essential Chilled Water System)
HVAC	공기조화계통 (Heating, Ventilation and Air Conditioning)
IAS	압축공기계통 (Instrument Air System)
ESFAS	공학적 안전설비계통 (Engineered Safety Features Actuation System)
RPS	원자로 보호계통 (Reactor Protection System)

(5) 고장수목 분석 기본 고려사항 및 가정

(가) 고장수목 구성 시 고려사항

- 일관성 있는 고장수목 분석을 수행하기 위해서는 분석 방법 및 수준, 절차에 관하여 통일된 지침이 필요하며, 분석자는 정해진 지침에 따라 분석을 수행함으로써 분석의 일관성을 유지한다. 주로 분석 대상 계통의 범위, 논리기호, 기본사건 코드 및 인간오류와 공통원인고장의 표현방법 등이 여기에 해당한다.
- 고장수목 구성에 사용한 모든 가정 사항은 설계정보와 함께 문서화한다.
- 계통이 상세하게 모델링 되지 않고 계통 단위의 신뢰도 데이타를 사용할 경우 다른 계통과 공통된 실패 사건은 분리하여 모델링 한다.
- 고장수목 정량화 시에는 정량화 결과의 정확성, 효율성 등을 위하여 전산코드를 사용한다.
- 분석을 수행하기 전 계통분석 범위를 명확하게 정의한다. 전위계통과 기타 보조계통과 연관된 부분, 즉 전력공급계통, 구동신호계통, 물, 오일, 공기 등을 공급하는 보조계통 등의 장치나 배관은 여러 계통에 공통되므로 계통범위를 결정하는 것은 매우 중요한 일이다. 따라서, 계통 설명 및 도면 작성시 누락이나 중복이 없도록 주의한다.
- 고장수목의 기본사건은 통일된 명명법에 의해 코드화한다. 체계적인 고장수목 명명법을 사용하여 전산코드를 사용한 자료 입력의 효율성을 얻으며, 정량화 결과로 도출되는 최소단절집합에 대한 정성적 이해를 돕도록 한다. 기본사건의 이름에는 최소한 아래와 같은 사항을 포함할 수 있도록 한다.
  - 기기의 고장모드
  - 고장기기의 계통 이름
  - 고장기기의 이름
- 고장수목에는 계통의 이용불능도에 영향을 미칠 수 있는 모든 가능한 고장모드가 포함되어야 한다. 여기에는 물론 시험 및 보수정지도 포함되며, 시험 및 보수 후 기기를 제 위치로 환원시키지 못하는 인간오류와 사고대응과 관련한 인간오류도 포함된다.
- 종속고장(Dependent Failure)에 관하여는 다음과 같은 사항을 반영한다.
  - 초기사건과 계통과의 사고 대응에 있어서의 상호관계
  - 공통 보조계통의 고장이나 실패로 인해 한 개 이상의 전위계통이나 기능 종속관계(Functional Dependence)에 있는 기기가 영향을 받을 경우
  - 공통 시험 및 보수(Common Test and Maintenance Activities) 에 관련한 인간 오류

– 전위계통 간에 공유된 기기

- 다중실패사건(Multiple Failure Events)에 대한 정확한 원인-영향관계를 계통분석 시 분명하게 모델링 하여야 한다. 특히 기기의 기계적 요인으로 인한 다중 실패인 공통원인고장(Common Cause Failure)과 여러 계통을 동시에 이용 불가능하게 만드는 인간오류에 의한 다중실패 등이 고려되어야 한다.
- 고장수목을 단순화하기 위해서는 다른 사건과 비교하여 발생확률이 상대적으로 작은 사건은 고장수목에서 생략할 수 있다. 단 타당한 근거에 의한 명확한 기준을 일관성 있게 적용한다.
- 발전소에서 사용되는 시험절차서는 시험동안 발생 가능한 모든 고장모드의 내용을 포함할 수 있도록 면밀하게 검토되어야 하며, 확인된 모든 사항은 문서화하여야 한다. 예를 들면 시험과 관련된 고장원인으로는 운전원이 시험 완료 후 시험을 위해 폐쇄했던 유로의 밸브를 원 상태로 개방하여야 하나 운전원 오류에 의해 원 상태로 개방하지 않는 인간오류가 있을 수 있다.
- 어떤 특정 기기를 보호하기 위해 관련 펌프와 안전장치를 정지시키는 것은 공통모드고장(Common Mode Failure)이 발생할 수 있으므로 신중하게 검토한다. 예를 들어 낮은 흡입압력 문제로 보조급수펌프를 이상 정지시키면 계통실패를 초래할 수 있다.
- 계속적인 운전을 수행하는 계통 중 두 개 이상의 다중 계열(Multiple Trains)로 구성되어 있으며, 정상 운전 중에는 한 개의 계열만으로 교대 운전하는 계통이 있다. 이런 계통의 분석에서 만약 두 개의 계열 중 한 개의 계열이 정상운전 상태로 모델링 된다면 나머지 한 개의 계열은 대기 중인 상태로 모델링 하게 된다. 그러나 비정상 조건 하에서 어떤 계열이 운전 가능하고 어떤 계열이 대기 상태인가를 결정하는 것은 불가능하므로 계통의 다중 계열이 다음과 같은 사항을 만족하는가를 결정함으로써 운전 및 대기 상태의 계열을 가정, 계통 모델을 단순화할 수 있다. 만약 상기 조건을 만족하지 않는다면 각 계열은 운전 및 대기 상태의 두 가지 경우로 분리하여 모델링 되어야 하며, 두 개 모델은 해당 계열이 수행 가능한 시간을 기준으로 평가되어야 한다.

– 각 계열은 대략적으로 거의 같은 시간 동안 운전된다.

– 각 계열에 구성된 기기 식별 번호(Identical Number)와 기기의 사양이 같지 않다면 유사한 기기로 구성한다.

– 각 계열의 운전 실패는 비슷한 결과와 상황을 발생한다.

(나) 분석의 상세 정도 (Level of Detail)

고장수목의 상세 정도 즉, 기본사건의 분해 정도는 설계 수준, 고장 데이타 유무, 모델에 대한 이해 범위 및 처리 능력, 분석 결과에 대한 해독 및 유용성 등에 의해

좌우된다. 이런 결정 기준은 특정 계통에만 적용되어서는 안되며, 전체 계통 고장수목 분석의 일관성 확보 차원에서 결정되어야 한다.

특히 분석 수준을 결정하는 결정적 기준은 고장 데이타의 유무로, 예를 들어 고장수목의 어느 단계에서 한 밸브가 작동 요구 시 열림 실패 되는 사건이 정의되었지만, 열림 실패의 원인들(즉 밸브축의 고장 또는 전선의 결함 등)에 대한 의한 고장률 정보가 없다면 작동 요구 시 열림 실패의 수준보다 더 확장 시켜 분석할 수 없다. 또한 펌프에 대한 신뢰도 자료가 펌프와 제어회로(Control Circuit)등의 고장을 모두 포함한다면, 펌프 베어링으로 인한 펌프의 고장, 제어회로의 고장 등을 분리하여 모델링 할 필요가 없게 된다. 일반적으로 고장수목은 분석에 사용하는 기기신뢰도 데이타베이스에 의해 그 분석 수준이 결정된다.

고장수목 구성의 상세 정도를 결정할 수 있는 다른 기준은 상대적으로 낮은 발생 확률을 지닌 기본사건을 결정하여 고장수목에서 제외한다. 예를 들면 배관, 열림 상태로 잠긴 밸브(Locked Open Valve)와 같은 수동기기(Passive Component)나 낮은 발생 확률을 지닌 고장은 고장수목에서 제외할 수 있다.

위에서 언급하였듯이 이와 같은 분석 수준을 결정하는 지침은 계통의 고장수목 구성 시 전 과정에 걸쳐서 일관성이 있게 적용되어야 한다. 즉, 고장수목의 한 쪽에서는 밸브의 작동 요구 시 열림 실패만 모델링하고, 다른 한 쪽에서는 열림 실패의 원인까지 모델링해서는 안된다.

(다) 고장수목 구성 시 기본 가정

다음은 영광 5,6 호기 사고경위 분석에 사용된 기본가정으로서 아래 사항을 계통 분석에 적용하여 고장수목을 구성한다.

- 계통의 작동시간(Mission Time)은 특별한 상황이 아닌 한 24시간으로 한다.
- 운전 중인 펌프는 기동실패를 고려하지 않는다. 단지 소외전원 상실과 같이 펌프에 전원을 공급할 수 없는 경우는 제외한다.
- 계통 기능에 영향을 거의 주지 않는 오리피스, 압력 및 온도 지시계의 고장은 고려하지 않는다.
- 전기계통의 고장수목에서 기기 이상으로 인한 사고의 시작은 초기사건 선정 시 고려되므로 고장수목 분석 시에는 회로 차단기 이상 열림이나 모선 혹은 회로의 단락 (Short) 등만을 모델링 한다.
- 펌프, 밸브 고장수목 구성 시 관련 회로차단기(Circuit Breaker)는 기기경계 내에 포함된다고 가정하여 별도로 모델링하지 않는다.

다. 단위 계통별 고장수목분석

계통분석을 위한 자료 조사 및 기본 준비가 완료되면 개별 계통에 대한 구체적이고 상세한 계통 고장수목 분석이 시작된다. 고장수목 분석에는 일반적으로 여러 사람이 참여하게 되므로 분석자간의 통일성을 유지하는 것이 매우 중요하다. 이를 위해서는 기본 준비 단계에서 확정된 방법론, 자료 및 지침을 일관성 있게 적용하도록 체계적인 관리 기법 및 품질 보증 프로그램을 활용해야 한다.

단위별 계통 고장수목 분석은 초기사건 분석 및 사건수목 분석 단계에서 결정된 각 계통 고장수목의 정점사건(Top Event)과 이에 대한 성공기준을 이해하는 것에서부터 시작한다. 해당 계통의 설계 및 운전 정보, 기술지침, 타 계통과의 연계성 등 대상 계통에 대하여 충분히 숙지한 다음 정점사건을 유발하는 사건들의 조합을 고장수목 구성 기법에 따라 연역적으로 추적하여 고장수목을 구성한다. 마지막으로 각 기본사건들에 대한 고장률이나 작동시간 등 기본사건 이용불능도 계산을 위한 자료를 입력하고, 정점사건의 발생 확률을 정량화 한다. 고장수목의 구성 및 자료 입력, 정량화 과정에는 이를 지원하는 소프트웨어가 사용된다.

계통 고장수목 분석의 일반적인 수행 절차는 다음과 같다.

- 계통분석 기본 지침 이해
- 계통 설계 및 운전 정보 이해
- 정점사건의 정의 및 성공기준 이해
- 단순계통도 작성
- 타 계통과의 연계성 파악
- 고장수목의 구성
  - 고장수목 구성 기본 원칙 및 명명법 숙지
  - 계통수준 (System-Level) 모듈 구성
  - 노드수준 (Node-Level) 모듈 구성
  - 단락수준 (Segment-Level) 모듈 구성
  - 기기수준 (Component-Level) 모듈 구성
  - 인간오류 및 공통원인고장 기본사건의 구성
  - 기기별 표준 고장수목 논리
- 고장수목 정량화
  - 기본사건 이용불능도 계산
    - ✓ 기계적 고장으로 인한 이용불능도
    - ✓ 보수정지로 인한 이용불능도

- ✓ 시험정지로 인한 이용불능도
- ✓ 인간오류 확률
- ✓ 공통원인고장 확률
- – 정점사건 이용불능도 및 중요도 분석

(1) 계통분석 기본 지침 이해

계통 고장수목 분석 기본 지침은 고장수목 모델을 구성하고 기본사건 고장 자료를 입력하는데 대한 기본적인 방법 및 가정사항을 제공한다. 여기에는 일반적으로 고장수목 분석 방법론, 분석 대상 계통, 계통 경계(System Boundary), 계통간 연계성, 고장수목 게이트 및 기본사건 명명법, 대표적 기기에 대한 표준 고장수목 논리 및 고장 모드 등 본 계통분석 절차서에 언급되는 주요 내용 전반이 포함된다. 분석자는 기본 지침을 통하여 계통분석의 기술적 방법, 분석 범위 및 기본 가정사항, 계통간 연계 정보 등에 대한 전반적인 기준을 이해한다. 기술적으로는 전기 및 유체 계통에 대한 주요 기기의 고장 유형, 검사 및 보수로 인한 운전 정지, 인간오류 및 공통원인 고장 등에 해당하는 고장 형태 등에 대한 정보를 기본 지침을 통해 습득한다.

앞에서 언급한데로 고장수목분석에는 일반적으로 여러 사람이 참여하므로 여기에서 언급하는 기본 지침을 준비하고 체계적으로 적용하여 분석의 일관성을 유지하는 일이 매우 중요하다.

(2) 계통 설계 및 운전 정보 이해

계통 고장수목 분석을 위해서는 사전에 최소한 대상 계통의 기능 및 운전, 기기 특성에 대한 이해가 필요하다. 이를 위해 설계 문서 및 도면, 계통 운전 교육 자료 등의 문서를 수집하여 검토하며, 필요 시에는 설계자나 운전원과의 면담을 통해 관련 계통의 기능 및 운전에 대하여 충분히 이해한다. 일반적으로 참조하는 대표적인 설계 및 운전 관련 참고 문헌은 다음과 같다.

- 예비 및 최종 안전성분석보고서 (PSAR, FSAR)의 계통 설명 및 기술지침서
- 계통별 설계문서
  - 설계요구서 (Design Requirement)
  - 설계시방서 (Design Specification)
  - 연계요구서 (Interface Requirement)
  - 계통설명서 (System Description)
  - 배관 및 계장도 (P&ID)

- 운전지침서 (Operation Guideline)

(3) 정점사건의 정의 및 성공기준 이해

고장수목의 구성은 대상 계통의 정점사건을 정의하는 것으로부터 시작한다. 정점사건이란 계통이 특정 운전 조건에서 필요한 기능을 성공적으로 수행하지 못하는 사건으로, 초기사건 분석 및 사건수목 분석 단계에서 결정된다. 특정 운전 조건 및 필요한 기능은 초기사건별로 사고경위를 개발하는 과정에서 결정된다. 초기사건별 사건수목은 초기사건으로부터 발전될 수 있는 대표적 사고 시나리오들을 표현한 것으로서, 사고 완화 및 종결을 위해 필요한 계통과 그 성공기준이 사건수목의 표제로 정의된다. 따라서 계통의 성공기준은 초기사건 및 사고 전개에 따라 달라질 수 있으며, 이에 따라 동일 계통에 대해서도 사고경위별로 여러 개의 정점사건이 정의될 수 있다.

고장수목의 정점사건을 결정할 때 기본 가정사항, 간단한 계산의 수행, 열수력 사고해석 결과 등을 충분히 검토한 후 가능한 범위 내에서 현실적인 방향으로 정의한다. 그러나 자료 또는 정보가 부족하여 정점사건을 명확히 규정할 수 없을 경우에는 보수적인 관점에서 결정한다.

정점사건 정의 시 고려해야 할 사항은 다음과 같다.

- 초기사건별 요구 안전기능(Safety Function) 및 특성
- 대상계통에 영향을 줄 수 있는 타 계통의 상태
- 계통의 기능 손실을 초래하는 운전설비의 고장
- 계통의 운전형태 및 운전요구시간
- 고장수목 구성에 영향을 줄 수 있는 여러 제한조건

예로써, 영광5,6호기 PSA에서 고압안전주입계통의 경우는 3개의 운전모드 (안전주입 모드, 재순환모드, 고온관 및 저온관 재순환 모드)에 모두 5개의 정점사건이 정의되었다. 안전주입모드 및 재순환 모드에서 각각 2개의 정점사건을 정의하였으며, 대형냉각재상실사고 분석을 위해 고온관/저온관 재순환 모드의 정점사건을 정의하였다. 표 20에 고압 안전주입계통의 운전 모드 및 정점사건에 대한 정보를 정리하였다.

표 20. 고압안전주입계통 고장수목 정점사건 및 관련 정보

운전모드	계통 정점사건명	정점사건 설명	관련 사건수목
안전주입 모드	GHSIETOP	Failure to inject water from RWT to RCS through 2 of 3 cold legs using 1 of 2 HPSI pumps	중형LOCA
	GHSIGTOP	Failure to inject water from RWT to RCS through 1 of 4 cold legs using 1 of 2 HPSI pumps	소형LOCA, 모든 과도사건
재순환 모드	GHSRDTOP	Failure to inject water from Sump to RCS through 1 of 3 cold legs using 1 of 2 HPSI pumps	대형LOCA, 중형LOCA
	GHSRGTOP	Failure to inject water from Sump to RCS through 1 of 4 cold legs using 1 of 2 HPSI pumps	소형LOCA, 모든 과도사건
고온/저온관 재순환 모드	GHSHBTOP	Failure to inject water from Sump to RCS through 1 of 3 cold legs and 1 of 2 hot legs using HPSI pumps : LOCA	대형LOCA

(4) **단순계통도 작성**

단순계통도는 PSA 측면에서 분석 대상계통의 기능 수행에 관련된 모든 기기 및 배관을 표현한다. 일반적으로 계통 설계 도면은 계통분석에서 요구되는 것보다 훨씬 많은 정보들을 매우 자세하게 표시한다. 그러나 PSA에서 수행되는 계통 고장수목 분석에는 계통 설계 도면 내용 중 일부 부분 혹은 정보만을 필요로 한다. 따라서 고장수목 구성 및 이해의 편리성을 높이기 위해서 PSA에서 정의된 계통 기능의 수행에 필요한 배관이나 기기만을 명확히 표시하고 불필요한 부분을 삭제한 단순계통도를 구성한다. 이 과정을 통하여 분석자는 계통의 성공적인 운전에 필요한 주요 기기들을 파악하고 고장수목 논리 구성의 기본 아이디어을 도출한다. 일반적으로 적용되는 단순계통도 작성 내용 및 순서는 다음과 같다.

단순계통도 작성 내용

단순계통도에는 다음과 같은 내용이 포함되어야 한다.

- 안전관련 유체계통 (Front-line Fluid System)

- 주배관 반경의 1/3보다 큰 우회배관
- 모든 주요기기 (예, 펌프, 구동밸브, 열교환기, 탱크)
- 최소우회유로 (Minimum Recirculation Lines)
- 정상 유로에 있는 수동 및 체크밸브 (소규모 시험관에 있는 것은 제외)
- 격납건물 경계 표시 (사고 시 접근 불가능한 기기들을 나타내기 위함)

● 보조 유체계통 (Support Fluid System)

- 냉각수 공급 계통의 주요기기 (열교환기, 펌프, 주요 밸브)
- 안전계통의 성공을 위해 격리되는 부하나 냉각이 요구되는 부하의 냉각 기능을 상실케 하는 고장

● 전기공급계통 (Electric Power System)

- 주요기기(예, 디젤, 모선, 축전지, 축전기, 변환기, 차단기 등)를 포함한 전기계통 단선도 (Single-Line Diagram)

● 계기 및 제어계통 (Instrumentation and Control System)

- 계기 및 제어 계통의 단순계통도는 필요하지 않지만 중요한 작동신호에 대한 정보는 명시한다.

● 공기조화 계통 (HVAC System)

- 계통분석에서 고려하는 공기조화계통 부하 표시
- 각 공기조화계통 부하에 영향을 주는 주요기기 (Damper, Fan)
- 공기조화계통 운전에 영향을 주는 주요기기(Compressor, Damper)
- 격납건물 경계

● 이차측 동력변환계통 (Power Conversion System)

- 증기 발생기
- 주증기 배관 및 증기방출밸브(ADV, MSSV)
- 터빈우회 증기방출유로(TBV)
- 복수기
- 주급수 및 보조급수 계통

● 일차측 감압계통 (Primary Pressure Relief System)

- 안전감압계통(SDS), 가압기 안전밸브(PSV) 및 차단밸브

● 압축공기계통(Instrument Air)

- 압축공기공급계통의 주요 기기와 압축공기를 공급 받는 주요 부하

<u>단순계통도 작성 절차</u>

단순계통도를 작성하는 절차는 다음과 같다.

- 계통별 상세 P&ID, 전기계통 단선도 및 부하목록(Load List), 관련 보조 도면 및 기기별 도면 등을 확보한다.
- 확보한 자료를 검토하여 계통 내에서 주요한 유체 흐름 및 전기 배열을 확인한다. 또한 도면 상에서 유체나 동력의 흐름이 합쳐지고, 나뉘어지고, 다른 유로로 전환되는 사항 등을 확인하며, 주요 공정과 직접 관련되지 않은 부분 등을 점검한다. 그리고 안전계통과 보조계통과의 연계성을 파악한다.
- 상세 계통 설계 도면을 단순계통도 형태로 재구성한다. 단순화는 상세 도면의 모든 배관 및 기기 중에서 PSA관점에서 정의된 계통 정점사건의 기능 수행에 관련된 배관 및 기기를 제외한 나머지 배관 및 기기를 생략함으로써 가능하다. 이 과정에서는 계통 운전이나 기기 운전 특성을 충분히 고려하여 필요한 배관 및 기기를 누락하는 일이 없어야 한다. 예로 펌프에 연결된 시험 유로나 최소우회유로 등이 기기 운전 기능에 영향을 준다면 고장수목 구성 시 모델링 해야 할 사항이므로 생략해서는 안된다. 기기의 기능 수행에 직접적인 관련이 없을지라도 운전 및 보수에 대한 이해에 필요한 것이면 단순계통도에 포함시킬 수 있다.
- 우회유로의 횡단 면적이 주 유로의 10 % 이하일 경우에는 생략하여도 무방하다. 일반적으로 우회유로의 직경이 주요배관의 직경의 1/3 이상이면 계통분석에 포함한다.
- 단순계통도 상에 기기를 나타내는 기호는 가능한 원래의 상세 도면에서 사용한 부호를 따르도록 하며, 단순계통도에 나타낸 모든 기기는 적절한 기기 번호를 부여하여 확인할 수 있도록 한다. 일반적으로 원래의 상세 도면에 나타난 번호를 확인번호로 사용한다.
- 안전주입작동신호(SIAS)나 공학적안전설비작동신호(ESFAS)에 의해 작동되는 격리밸브, 펌프 및 회로 차단기 등과 같은 능동 기기(Active Component)는 단순계통도 상에 꼭 표기되어야 한다.
- 격납건물과 다른 건물사이에 설치된 방호벽의 위치는 단순계통도상에 점선으로 표시한다. 이 경계를 더욱 확실하게 하기 위하여 "Inside Containment" 와 "Outside Containment" 라고 명시하기도 한다.
- 단순계통도에는 계통의 운전 모드를 표시하여 계통도에 나타난 기기배열이 어떤 운전 상태를 의미하는지를 명확히 한다.
- 작성된 단순계통도상에는 원래 상세 도면을 참고문헌으로 명시한다.

(5) 타 계통과의 연계성 파악

고장수목 기본 준비 단계에서 이미 파악된 계통간 연계성 정보를 바탕으로 해당 계통과 기능적, 물리적 연관 관계를 갖는 계통들을 파악하고 관련된 정점사건을 정리한다. 표 18에 영광5,6호기의 전체 계통별 연계 정보가 정리되었다. 개별 고장수목 구성을 위해서는 보다 구체적인 정보, 즉 연계되는 타 계통의 고장수목 정점사건 정보가 필요하다. 표 21은 영광5,6호기 고압안전주입계통의 타 계통과의 구체적인 연계 정보를 예로 보여주고 있다. 이 표는 고압안전주입계통 고장수목 구성 시 각 기기의 하부 고장수목에 전이 게이트(Transfer Gate)로 모델링 된 연계 계통 정보의 일부를 정리한 것이다.

표 21. 고압안전주입(HPSI)계통 연계 정보

기 기	기기 보조계통	전이 게이트 이름	비 고
HPSI 펌프1	4.16KV 5-SW01A 125V DC 12-DC01A 공기조화계통 트레인 A 안전주입 작동신호-A	GEK01A GED01A GHCHPSIP1 GFSSIASA	구동전력 제어전력 펌프실 냉각 SIAS로 작동
HPSI 펌프 2	4.16KV 5-SW01A 125V DC 12-DC01B 공기조화계통 트레인 B 안전주입 작동신호-B	GEK01A GED01B GHCHPSIP2 GFSSIASB	구동전력 제어전력 펌프실 냉각 SIAS로 작동
모관 격리밸브 SI- 617, 627, 637, 647 SI- 616, 626, 636, 646	480V MCC 8-MC08A 안전주입작동신호-A 480V MCC 8-MC08B 안전주입 작동신호-B	GEM08A GFSSIASA GEM08B GFSSIASB	Motive power Open on SIAS Motive power Open on SIAS
고온관 격리밸브 SI-603* SI-604* SI-321* SI-331*	480V MCC 8-MC05A 480V MCC 8-MC05B 125V DC 12-DC01C 125V DC 12-DC01D	GEM05A GEM05B GED01C GED01D	구동전력 구동전력 구동전력 구동전력
펌프Orifice 우회밸브 SI-699** SI-698**	480V MCC 8-MC05A 480V MCC 8-MC05B	GEM05A GEM05B	구동전력 구동전력

(6) 고장수목 구성

고장수목 분석을 위한 사전 준비가 완료되면 계통별 고장수목을 구성한다. PSA 대상 계통들은 모두 흐름(Flow)을 갖고 있으며, 계통 기능도 그 흐름을 발생 혹은 중지, 조절하는 것이다. 계통에 따라 흐름의 대상이 액체, 기체 또는 전기적인 것으로 구분될 뿐이다. 따라서 계통의 기능 상실로 표현되는 정점사건은 어느 지점으로의 흐름의 상실, 발생 또는 조절 실패 등으로 표현된다. 고장수목의 구성은 정점사건의 발생을 초래하는 흐름의 이상을 최종 흐름 도달 지점으로부터 흐름의 시작 지점까지 연역적으로 추적하는 방식으로 논리를 전개한다.

계통은 일반적으로 몇 개의 하부 계통 또는 흐름 노드(Flow Node)에 의해 구분되고, 그것은 다시 몇 개의 단락(Segments) 으로 구분할 수 있다. 여기서 노드라 함은 유체가 다른 유로와 합쳐지는 지점, 나뉘어지는 지점, 전환되는 지점을 의미하며, 단락은 두 개의 노드를 연결하는 배관 및 기기 부분을 의미한다. 단락은 다시 몇 개의 기기와 배관으로 표현된다. 따라서 고장수목의 논리 전개도 이와 같은 물리적 구분에 따라 Top-Down 방식으로 구성하게 된다. 분석자는 고장수목의 하부 수목에 각 단락의 특정 사항을 표현하여 각 단락에 대한 상세한 실패 논리를 구성한다. 펌프나 밸브와 같은 공통 기기들은 기기 형태(Type) 및 운전 방식에 따라 분류되어 각 기기의 특성에 맞는 하부 수목을 구성한다. 이상과 같은 모듈 고장수목 구성 방법은 고장수목 개발의 일관성을 제공한다.

(가) 고장수목 구성 원칙

기본원칙 1 : 기본사건의 내용을 기술하되 고장의 유형 및 내용을 정확히 기술한다.

이 원칙에 따라 고장의 원인 및 내용을 기술하면 상당히 긴 문장이 될 수도 있다. 참고로 고장수목분석 코드인 KIRAP코드에서는 최대 82자까지 내용을 기술할 수 있다. 그러므로 고장수목분석코드에 따라 다르겠지만 기술할 수 있는 범위가 제한되어 있기 때문에 간략하면서도 다른 분석자나 검토자가 알 수 있도록 주요 내용을 기술해야 한다. 현재 KIRAP 코드의 데이타베이스에서는 대부분의 주요 기기에 대한 기본사건 설명문을 제공하고 있다. 이를 이용하면 기기 번호등과 같이 기본사건 고유 정보만을 추가로 입력하면 기본사건 설명문을 완성할 수 있다. 필요 시에는 사용자가 직접 모든 설명문을 입력할 수 있다.

기본원칙 2 : 고장 원인이 기기고장인지 혹은 시스템, 노드, 단락 단위의 고장인지를 분류한다.

고장의 유형을 판단하여 기기고장이면 OR 게이트를 사용하여 기기고장의 원인을 차례로 나열한다. 만일 기기 단위 이상의 고장이면 성공기준에 따라 AND 혹은 OR

게이트를 사용하여 논리를 전개한다. 모든 게이트가 기기 단위 혹은 타 계통 연결 논리까지 이 과정을 반복한다.

<u>기본원칙 3</u> : 한 기기의 고장으로 인해 다른 고장의 진행을 우연히 차단시킬 수 있다고 보면 안된다(기적 불발생의 원칙).

예를 들어 어떤 계통이 성공적으로 작동하기 위하여 반드시 열려 있어야 하는 밸브가 오류에 의해 밸브가 닫히려는 순간, 밸브의 작동계전기가 고장나 있었기 때문에 밸브가 닫히지 않아서 계통이 성공하는 것을 고려하지 않는 것이 이 원칙에 해당된다. 더욱이 고장수목은 고장에 관한 모델이기 때문에 이러한 성공에 관한 논리는 부적절하다.

<u>기본원칙 4</u> : 대상 게이트의 모든 입력은 그 입력들 중 어느 하나에 대한 하부 논리를 확장하기 전에 완전히 정의한다(게이트 완결의 원칙).

고장수목의 구성은 단계별로 전개하여야 하며, 한 단계를 완전히 구성한 후에 다음 단계에 대한 분석을 수행한다.

<u>기본원칙 5</u> : 게이트의 입력은 고장 사건이 기술된 것이어야 하며, 한 게이트는 다른 게이트와 직접 연결되지 않는다(게이트 불연결의 원칙).

게이트 대 게이트의 직접 연결은 바람직하지 못하다. 물론 완성된 고장수목에 대하여 최소단절집합을 구하거나 정량화 할 때는 관계없으나, 실제로 고장수목을 구성할 때 게이트와 게이트를 연결하게 되면 혼란이 발생할 수 있다.

<u>기본원칙 6</u> : 고장수목의 구성은 분석 대상 계통의 이용불능을 직접 초래하는 기기 및 하부 계통에서부터 시작한다.

예로서 보조급수계통의 경우, 증기발생기에 보조급수를 공급하지 못하는 것부터 시작하여 증기발생기에 연결된 보조급수 공급 유로를 역으로 추적하면서 고장수목을 구성한다.

<u>기본원칙 7</u> : 여러 기기에 동시에 기능을 제공하는 보조계통은 공통 부분만 보조계통 고장수목에서 고려하고, 기능을 제공받는 계통에 관련된 부분(밸브, 열교환기 등)은 관련계통 고장수목에 포함시킨다.

예를 들어 일차측 기기냉각해수계통(NSCWS)이 냉각수를 공급하는 기기가 일차측 기기냉각수 열교환기, 필수냉각수 열교환기 등이 있다고 하자. 일차측 기기냉각 해수계통의 고장수목은 공통 부분인 해수유입부분과 방출부분만 대상으로 분석하고, 나머지 기기들은 해당 열교환기 기능 실패에 관한 고장 논리에 포함시켜 해당 계통 고장수목에서 직접 모델링 한다.

(나) 고장수목 명명법

앞에서 이미 언급하였듯이 복잡한 계통의 고장수목 분석을 위해서 사전에 준비해야 되는 것 중의 하나가 기본사건 및 게이트 명명법이다. 이름을 통해 해당 기본사건이 어떤 계통, 어떤 기기의 어떤 종류 고장인지를 쉽게 파악할 수 있어야 하며, 전산코드를 이용할 시 자료 관리나 처리가 효율적으로 되도록 통일된 명명법을 준비하여 사용한다. 최소한 계통명, 기기명, 고장모드명, 트레인 구분 등이 기본사건 이름에 포함되도록 한다.

(다) 고장수목 구성 절차

계통은 일반적으로 몇 개의 하부 계통 또는 흐름 노드(Flow Node)에 의해 구분되고 그것은 다시 몇 개의 단락(Segments)으로 구분할 수 있다. 단락은 다시 몇 개의 기기와 배관으로 구성된다. 고장수목의 논리 전개도 이와 같은 물리적 구분에 따라 계통 내 유체 흐름의 최종 도달 지점에서부터 초기 흐름의 시작 지점까지 Top-Down 방식으로 구성한다. 고장수목 구성에는 노드(Node)나 단락(Segment) 구분을 단순계통도에 명시적으로 표시하고 이를 사용하여 고장수목 논리를 전개하는 방법이 있고, 노드나 단락을 명시적으로 표시하지 않고 게이트 설명을 통해서 묵시적으로 표현하면서 고장수목을 구성하는 방법이 있다. 일반적으로 고장수목분석 경험이 있는 경우에는 노드나 단락을 명시적으로 표현하지 않으면서 고장수목을 구성하는 후자의 방법을 많이 사용한다. 영광5,6호기 계통분석에서도 후자의 방법을 사용하여 고장수목을 구성하였다. 그러나, 본 절차서에서는 초보자의 고장수목 구성을 지원하기 위해 노드나 단락을 명시적으로 표현하는 방식을 사용하여 고장수목 구성 절차를 설명한다.

그림 9의 계통A를 예로 고장수목 구성 순서를 살펴본다.

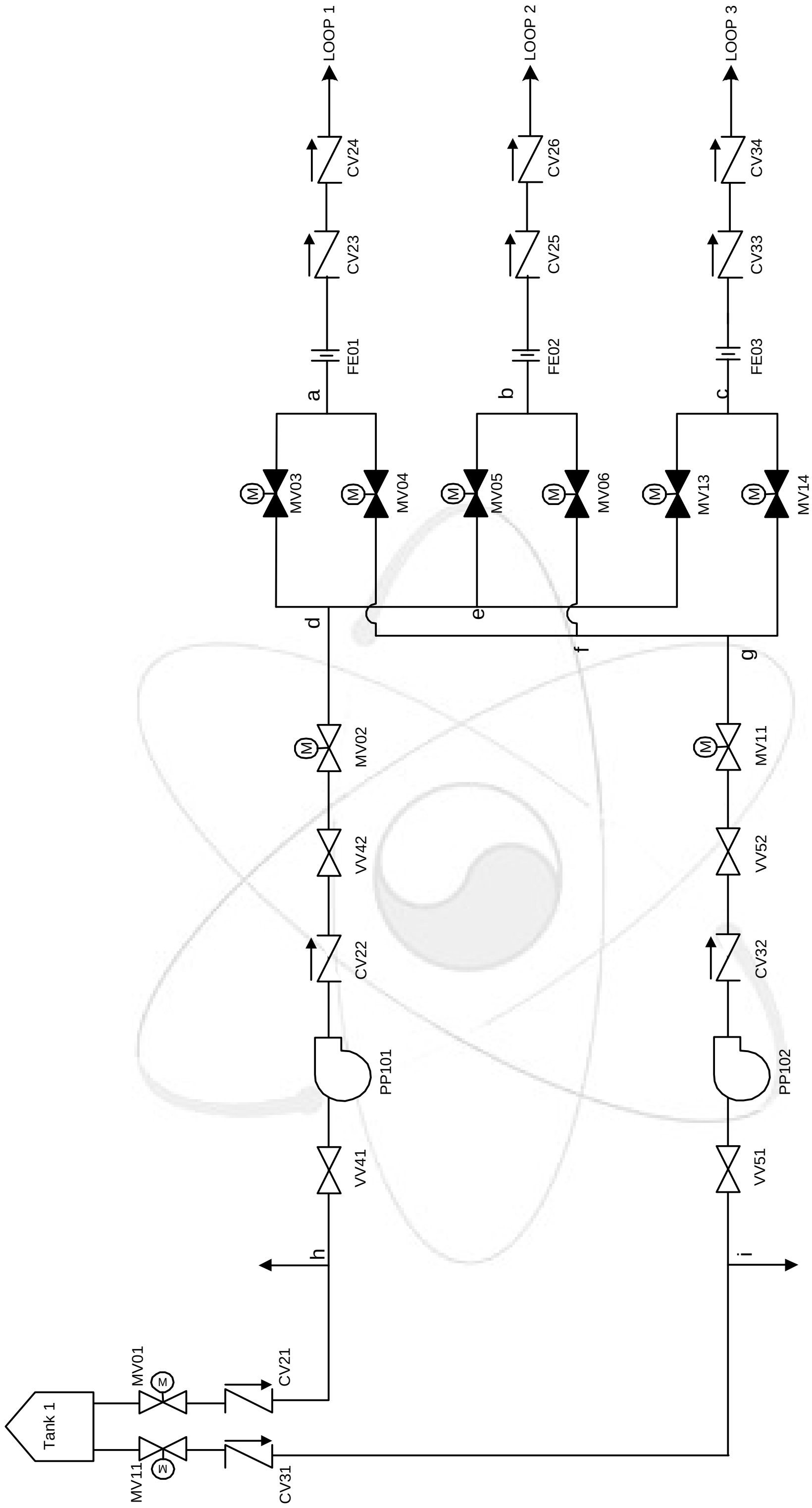


그림 9. 계통 A 단순계통도

① 계통수준 모듈

계통수준의 모듈이란 계통 정점사건 수준의 고장수목을 의미한다. 앞에서 언급한 것처럼 동일 계통이라도 계통 운전모드 및 사고경위에 따라 성공기준이 달라질 수 있다. 이에 따라 계통 고장수목 상위 수준에서의 논리 전개가 다른 고장수목이 구성된다. 그러나 정점사건과 직접적으로 연결된 상위 수준의 논리를 제외하고는 하부 고장수목은 동일한 게이트가 여러 정점사건 고장수목에서 동시에 사용된다.

이런 계통수준의 고장수목을 구성하는 방법에는 크게 두 가지 방법이 있다. 계통 고장수목 구성 시 모든 조건들을 하나의 정점사건의 하부 논리로 모두 입력하는 방식이 있고, 각 조건 마다 별도의 정점사건의 정의하여 여러 개의 고장수목으로 구성하는 방법이 있다. 전자는 'House Event' 혹은 'Conditional Event'를 사용하여 사고경위별로 계통 이용불능 사건조합을 표현하는 방식으로, 계통별로 하나 씩의 대형 고장수목을 관리하는 방식이다. 후자는 사고경위별로 필요한 모든 정점사건을 정의하고 정점사건별로 별도의 고장수목을 구성하는 방법이다. 그러나, 여러 개의 고장수목에 동시에 사용되는 하부 고장수목 논리는 어느 한 정점사건 고장수목에 한번만 모델링 한다. 어느 방법을 사용해도 문제는 없으며, 두 방법 모두 장단점이 있으므로 이를 검토하여 선택한다. 본 절차서에서는 후자를 사용하여 고장수목 구성을 설명한다.

만일 계통A의 성공기준이 초기사건 IE-1과 IE-2에서 서로 다르다면 각 경우 정점사건이 달리 정의된다. 계통A 정점사건이 다음과 같이 정의되었다고 가정하자.

- GSYS-A-IE1 : No Flow to One of Three Loops (Loop 1, 2 or 3) from System A
- GSYS-A-IE2 : No Flow to One of Two Loops (Loops 2 or 3) from System A

정점사건 GSYS-A-IE2는 Loop 1의 파손 등으로 Loop 1으로 주입되는 유량은 효과가 없는 경우로 Loop 2 혹은 3 중 최소한 어느 하나로 유로가 형성되어야 하는 것을 의미한다. 그림 10과 그림 11에 두 정점사건에 대한 논리가 정리되어 있다. 정점사건의 하부 논리 중 B와 C는 두 정점사건 모두에서 동일하게 사용된다. 이렇듯 계통수준의 모듈은 계통 성공기준과 관련된 상위수준의 고장수목 모듈이다.

② 노드(Node) 수준 모듈

노드수준의 모듈은 계통수준 모듈의 하부 논리로서, 전체 계통을 몇 부분으로 구분하여 구분된 각 부분의 고장수목을 말한다. 일반적으로 유체 계통의 단순계통도는 배관의 분기나 접목 부분인 노드에 의해 몇 개의 부분으로 나뉠 수 있으며, 노드에 의해 구분된다.

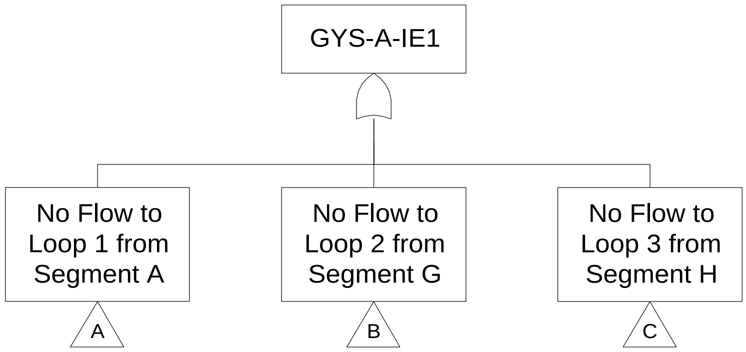


그림 10. 정점사건 GSYS-A-IE1에 대한 계통수준 모듈

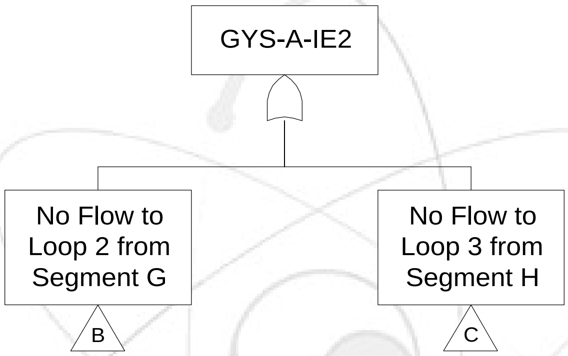


그림 11. 정점사건 GSYS-A-IE2에 대한 계통수준 모듈

이렇게 구분된 부분의 고장수목을 노드수준 모듈이라 한다. 다음과 같은 경우가 노드수준 모듈의 대상이 될 수 있다.

- 두 개 이상의 배관이 하나로 되는 경우
- 한 개의 배관이 두개이상으로 나뉘어지는 경우
- 유체 전환 (diversion) 유로가 있는 경우
- 2개 이상의 배관이 교차 연결될 경우

그림 12는 계통A 단순계통도에 주요 배관 분기점마다 영문 소문자로 노드를 표시하고, 노드를 기준으로 구분되는 단락(Segment)을 표시한 예를 보여주고 있다. 계통수준의 고장수목은 이 노드를 기점으로 하부 논리가 전개된다. 성공기준에 따라 노드를 기점으로 AND나 OR 논리가 결정되며, 게이트 설명문도 노드를 기준으로 작성할 수 있다. 그림 13은 계통A의 Loop 1과 관련된 노드수준의 고장수목 일부를 보여준다.

③ 단락(Segment) 수준 모듈

노드수준의 고장수목은 편의에 따라 적절한 크기의 단락(Segment)으로 나누어서 단락 단위의 고장수목으로 구성된다. 단락 수준의 고장수목에는 단락내의 유체 흐름을 중단하는 기기 단위의 기능 상실 논리들이 "OR" 게이트로 연결된다. 기기 없이 단지 배관만으로 이루어진 노드간의 단락은 별도로 모델링하지 않는다. 계통A 단락D 부분에 대한 단락수준 고장수목 예를 그림 14에 정리하였다.

④ 기기 (Component) 수준 모듈

단락수준의 고장수목 논리는 다시 각 단락내의 구성 기기에 대한 고장수목으로 세분화된다. 단락내의 유체 유동을 상실 시키는 기기 단위의 고장 유형 및 보조계통의 기능 상실이 기기수준의 고장수목 논리에 구체적으로 표현된다. 기기수준의 고장수목에는 다음과 같은 기기 이용불능 원인들이 포함된다.

- 기기의 기계적, 전기적 독립 고장 (Independent Component Failure)
- 다중 설치된 동일 기기의 공통원인고장 (Common Cause Failure)
- 시험 및 보수로 인한 이용불능 (Outages due to Test and Maintenance)
- 보수원 혹은 운전원의 인간 오류 (Human Error related Test and Maintenance Activity)
- 기기의 작동 불능을 초래하는 보조계통의 기능 상실 (Loss of Function of Support System)
  - 제어 및 신호 계통(Control & Actuation Signal System)의 기능 상실
  - 전기계통(Electric System)의 기능 상실
  - 기기냉각수계통(Component Cooling Water System)의 기능 상실
  - 기기 룸 공기조화계통(HVAC System)의 기능 상실
  - 압축공기계통(Instrument Air System)의 기능 상실
  - 기기수준의 고장수목을 구성할 때에는 해당 기기와 보조계통과의 연계성, 구동(Actuation) 및 제어(Control) 계통과의 연관 관계들을 일관성 있게 고려한다. 유체계통 고장수목 구성에는 일반적으로 다음과 같은 기기 및 고장 모드가 포함된다.
- 펌프 (Motor-Driven Pump, Turbine-Driven Pump, Diesel-Driven Pump)
  - 기동실패 혹은 재기동 실패 (Fail to Start or Fail to Restart)
  - 동작 중 고장 (Fail to Run)
- 밸브 (Check Valve, Manual Valve, Safety/Relief Valve, Motor-Operated Valve, Pneumatic/ Hydraulic-Operated Valve)
  - 열림/닫힘 실패 (Fail to Open/Close)

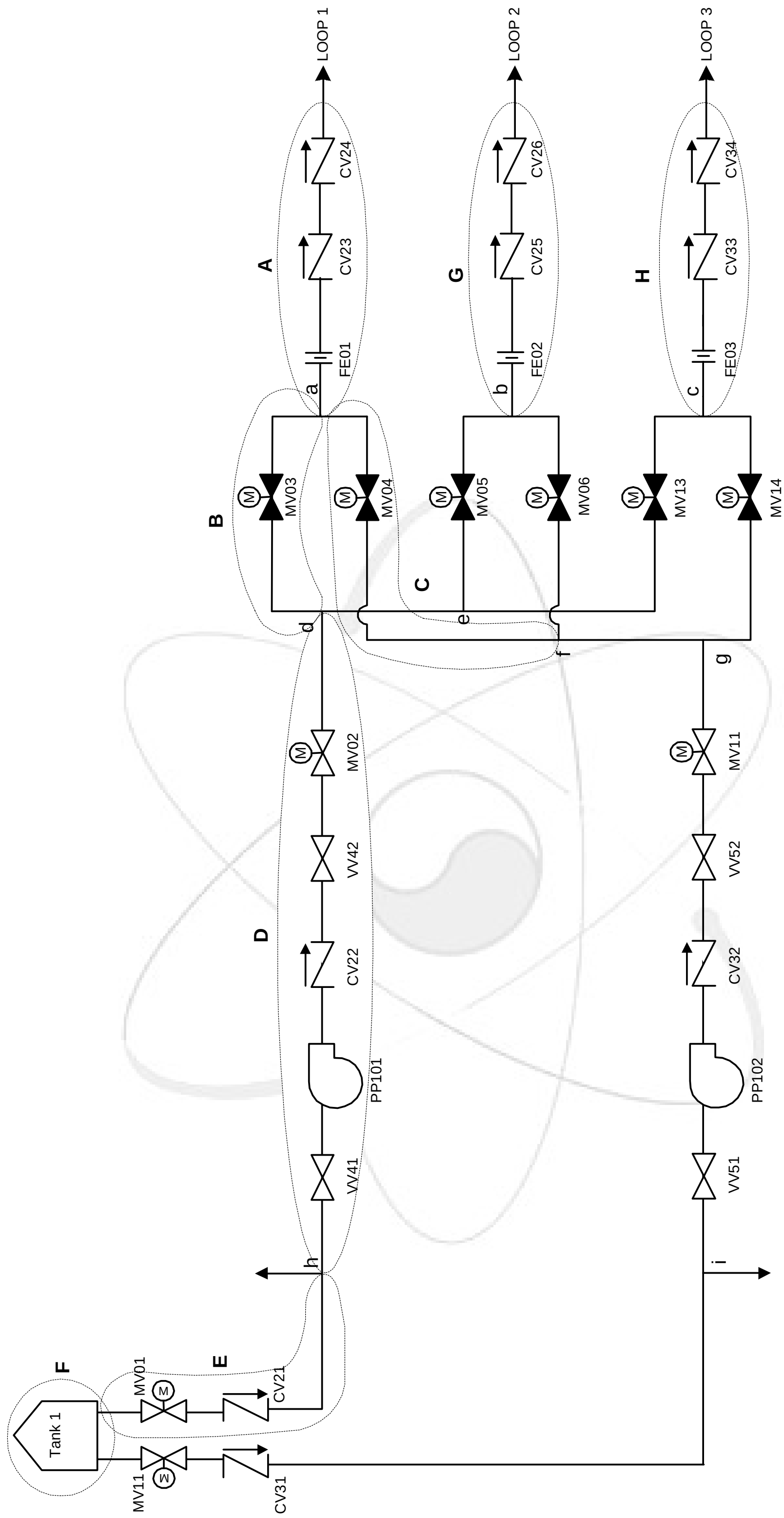


그림 12. 단락 구분된 계통 A 단순계통도

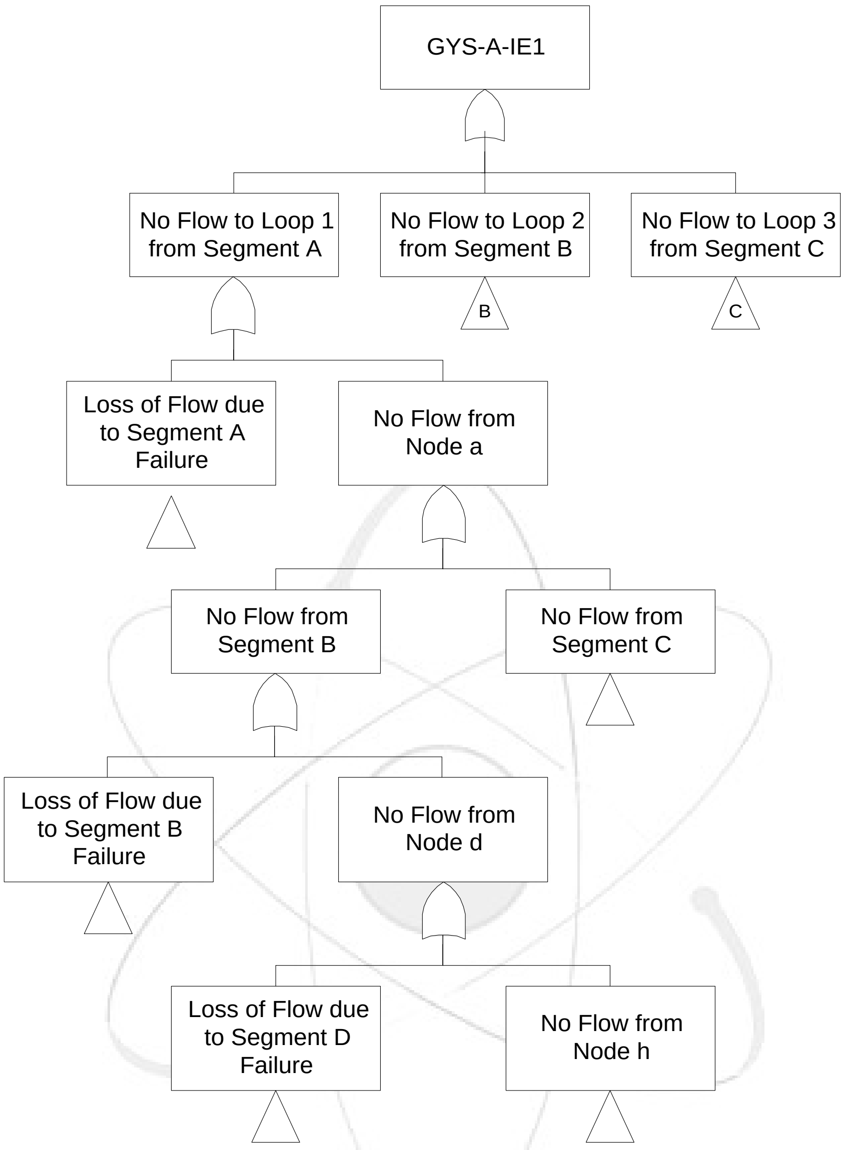


그림 13. LOOP 1 Flow 상실에 대한 노드수준 모듈

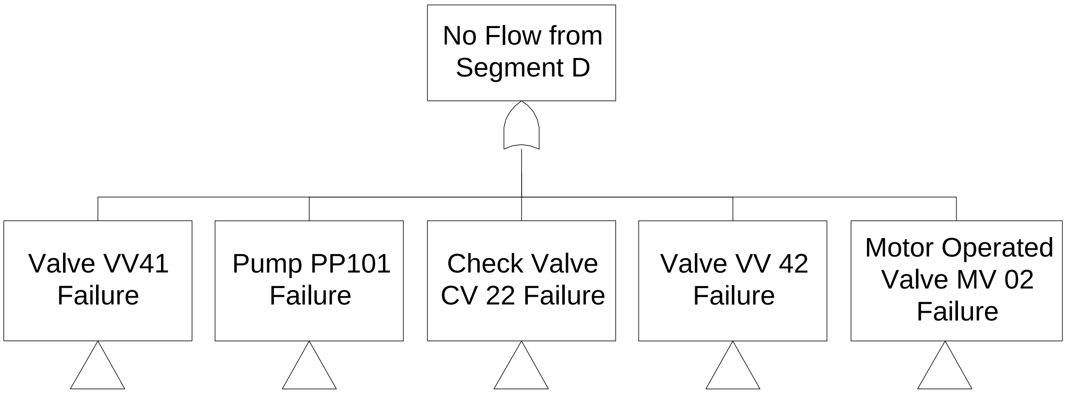


그림 14. 단락 D에 대한 단락수준 모듈

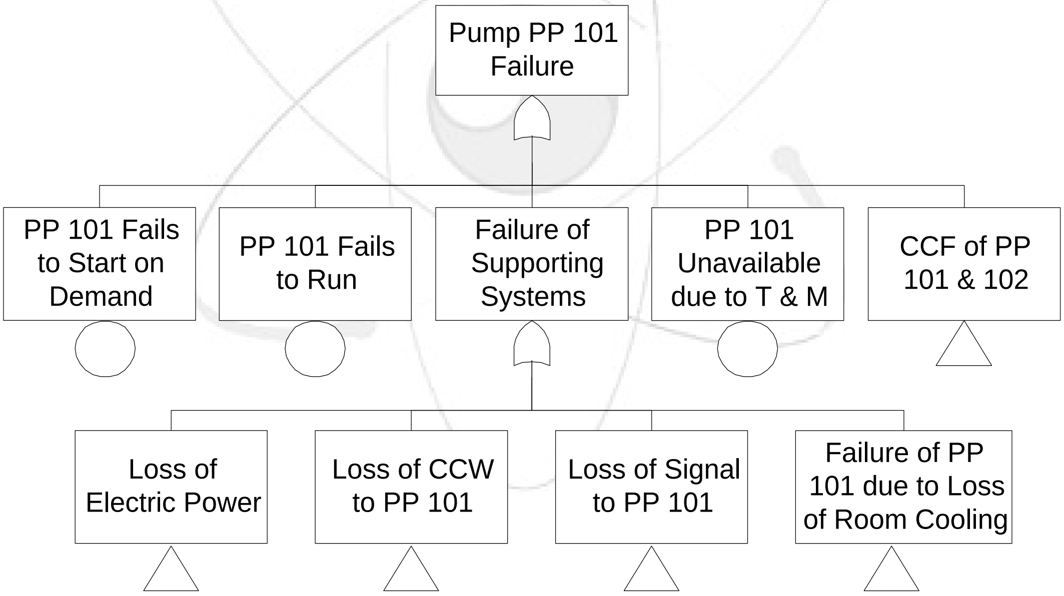


그림 15. 펌프에 대한 기기수준 모듈

- 열림 상태 유지 실패 (Fail to Remain Open/Transfer Closed : Manual Valve or Check Valve는 모델링에서 제외)

- 열 교환기 (Heat Exchanger)
- 탱크 (Tank)
- 압축기 (Compressor) 및 펜 (Fan)

기기수준 고장수목의 예로 대기중인 모터구동 펌프에 대한 고장수목 논리를 그림 15에 정리하였다.

⑤ 인간오류 및 공통원인고장 모델링

계통 고장수목 구성에서 일관성 유지를 위해 주의를 기울여야 하는 것 중의 하나가 인간오류 및 공통원인고장 사건의 모델링이다. 이것은 계통분석 전체 관점에서 구체적 지침이 결정되어 모든 계통 고장수목 구성에 일관성 있게 적용되어야 한다.

인간오류사건

사고 발생 및 전개와 관련된 모든 인간행위는 기본적으로 PSA 인간신뢰도분석의 대상이 되며, 이에는 주 제어실에서 수행되는 운전원 행위 및 비상운전절차서(EOP), 비정상운전절차서(AOP), 계통운전안내서(Systems Operations Manuals)에 명시된 운전원 행위 등이 포함된다.

PSA에서 고려되는 인간오류는 크게 사고 발생 전에 일어난 인간오류와 사고 발생 후 비상운전절차서 수행 단계에서 일어나는 인간오류로 구분한다. 사고 후 발생하는 인간오류는 주로 사건분석 단계에서 모델링 되고, 계통분석 단계에서는 사고 전 인간오류가 고장수목에 모델링 된다. 사고 후 발생하는 인간오류는 일반적으로 사건수목 표제의 하부 논리에서 모델링 한다. 필요에 따라 계통 고장수목의 상위 수준에서 모델링하기도 하는데, 이 경우에는 운전원 행위와 직접적으로 관련된 계통 수준의 게이트와 동등한 수준에 인간오류를 모델링 한다. 제어실 밖에서 수행되어야 하는 운전원 행위, 절차화 되어 있지 않은 운전원 행위 그리고 고장기기의 운전원 복구조치 등은 원칙적으로 사건수목이나 고장수목분석 단계에서 고려하지 않는다.

계통 고장수목 구성에서 고려되는 사고 전 인간오류에는 계통의 이용불능을 초래하는 운전원의 조치 실패들로 안전계통의 시험/보수 후 밸브 원위치 실패와 계기 보정 실패가 있다. 고장수목 구성에서 고려되는 인간오류 중 시험/보수 후 밸브 원위치 실패는 안전계통의 정기적 작동점검 혹은 보수를 위해 차단했던 밸브를 작업 후 원위치로 환원하지 않아 기능을 상실하는 인간오류로 관련 밸브의 기기 하부 논리에 모델링 한다. 운전원이 밸브, 펌프 및 기타 안전계통 기기의 시험 및 보수후 원래의 정상적인 위치로

환원시키지 못하는 인간오류들 중 일부는 다중 점검 등으로 발생 가능성이 매우 작기 때문에 모델링에서 제외시키기도 한다. 모든 대기중 기기에 대하여 시험/보수 후 밸브 원위치 실패나 계기 보정 실패를 고려하는 것을 원칙으로하되 다음과 같은 선별 기준에 해당되면 모델링하지 않는다.

- 보수나 시험 후 기기가 작동 가능상태(Operable State)에 있음을 독립적으로 확인하는 Tagging System 이 적용되는 경우
- 기기 상태가 작동 가능상태에 있지 않으면 주 제어반에 경보(Annunciation)가 발생하는 경우
- 기기 상태가 주 제어반에 표시되고 점검표(Check List) 등을 사용 매일 혹은 교대조 별로 점검하는 경우
- 기기 상태를 현장에서 점검표(Check List) 등을 사용하여 주기적으로(교대조별, 일별 혹은 주간별) 점검하는 경우
- 부주의로 작동 가능상태에 있지 않더라도 비상시 작동 가능상태로의 자동 작동 신호를 받는 밸브
- 보수나 시험 후 원위치 작업의 일환으로 유량 시험(Flow Test)을 수행하는 밸브

<u>공통원인고장</u>

계통의 신뢰도를 높이기 위한 방법 중의 하나가 중복 설계 개념이다. 그러나 이런 중복 설계의 효과를 없애는 고장이 바로 공통원인고장이다. 원칙적으로는 유사한 환경에서 운전하는 동일 기기는 모두 공통원인고장의 대상이 될 수 있으나, 모델링의 어려움으로 인하여 중복 트레인의 속한 동일에 한해 기기간 공통원인고장을 고려하는 것이 일반적이다.

공통원인고장의 모델링은 트레인(혹은 단락) 수준의 게이트와 동일한 상위 수준에 모델링 하는 방법과 해당 기기의 하부 고장수목에 모델링 하는 방식이 있다. 그림 16과 그림 17은 각각 두 방식에 대한 예를 보여주고 있다. 영광5,6호기 PSA에서는 고장수목 구성 원칙에 입각하여 어떤 기기의 기능 상실을 초래하는 모든 원인들을 그 기기의 하부 논리에 포함시키는 방식을 택하였다.

보조계통의 기능 상실을 의미하는 전이 계통의 모델링 방법도 위에서 언급한 것처럼 두 가지 방식이 있을 수 있으나, 영광5,6호기 PSA에서는 그림 17에서 처럼 관련 기기의 하부 논리에 포함시키는 방식을 따른다.

⑥ 기기별 표준 고장수목 논리

본 절에서는 계통 분석에서 사용되는 대표적 기기에 대한 표준 고장수목 논리를 언급한다. 동일 유형의 펌프나 밸브의 경우 기기 고장수목 논리는 거의 유사하거나 동일한 형태를 갖게 된다. 따라서, 이들 주요 기기에 대한 표준 고장수목 논리의 사용은 계통별 고장수목 사이의 일관성 유지에 큰 도움이 된다.

<u>펌프</u>

펌프는 구동 방식에 따라 모터구동펌프, 증기구동펌프, 디젤구동펌프가 있으며, 펌프의 타입에 따라 원심형(Centrifugal) 타입과 왕복동(Replacement) 타입이 있다. 그러나, 이런 구동 방식이나 펌프 타입에 따른 차이로 고장수목 논리가 달라지는 것은 아니고 다만 펌프 구동방식이나 타입에 따라 다른 기기 고장률을 사용한다. 펌프의 고장수목 논리는 운전 방식에 따라 차이를 보인다.

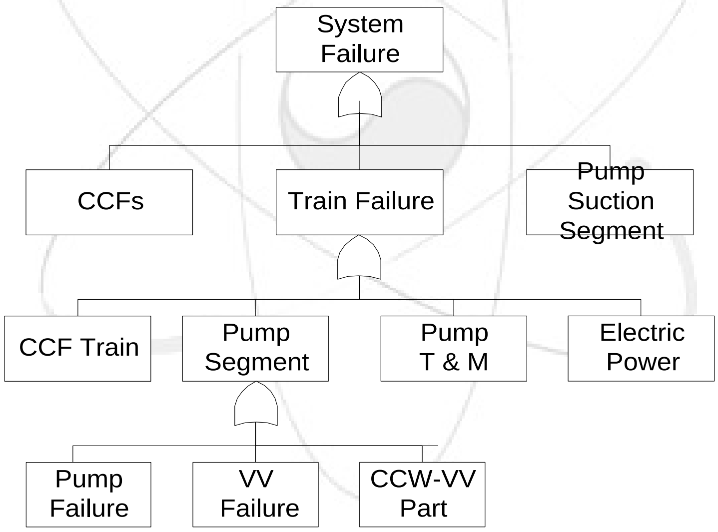


그림 16. 공통원인고장을 트레인 수준에서 모델하는 방식(System 80+)

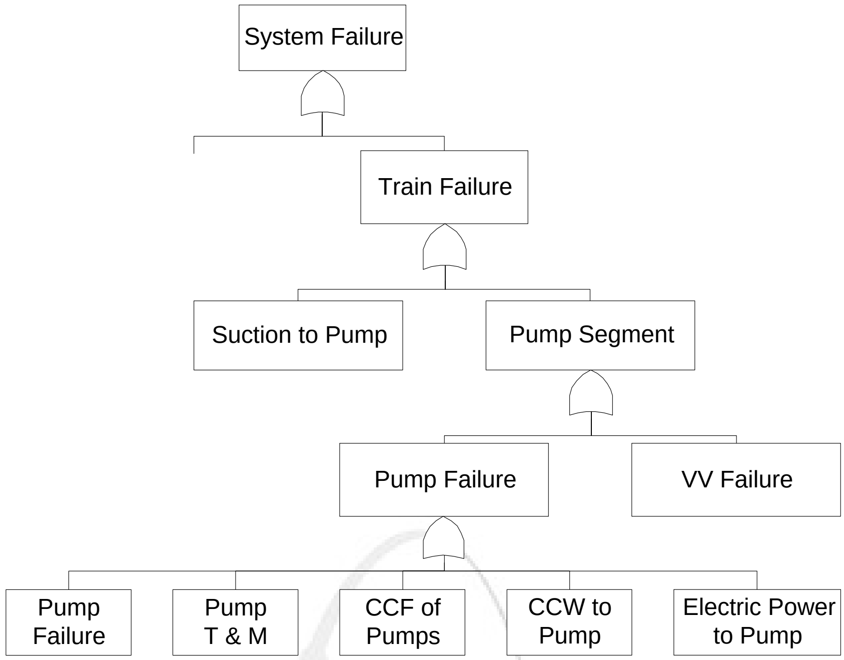


그림 17. 공통원인고장을 트레인 수준에서 모델하는 방식

예로 평상시 운전 중인 펌프와 대기 중인 펌프의 고장수목 논리는 일부분이 틀리게 된다. 평상시 운전 중인 펌프는 펌프 작동 중 실패(Fail to Run) 사건이 없는데 반해 대기 중인 펌프는 기동 실패 사건이 고장수목에 포함된다.

펌프 기능 상실에는 아래와 같은 고장원인들이 포함된다. 이들 중 운전 방식에 따라 불필요한 고장 유형과 관련 없는 보조계통 부분을 삭제하여 해당 펌프의 표준 고장수목을 구성한다. 앞서 언급한 그림 15는 대기중인 모터구동펌프에 대한 표준 고장수목을 보여준다.

- 펌프 기동실패
- 펌프 작동실패
- 펌프 시험 혹은 보수로 인한 이용불능
- 펌프간의 공통원인고장
- 보조계통 기능상실
  - 펌프 구동전기 상실
  - 펌프 구동 증기공급계통 상실
  - 펌프 작동신호 상실
  - 펌프 냉각 상실

– 펌프 룸 냉각 상실

<u>밸브</u>

밸브도 펌프와 유사한 방식으로 표준 고장수목을 구성한다. 구동 방식 및 밸브 타입에 따른 차이는 신뢰도 자료에서 반영하며, 표준 고장수목에는 밸브의 운전 방식에 따른 차이를 표현한다. 다만 일부 타입의 밸브에서 특정 고장 유형은 영향이 미미하다는 판단 하에 모델링하지 않는다. 예로 밸브의 기능상실 원인 중 열림/닫힘 실패(Fail to Open/Close)와 'Transfer Closed'가 모두 고려될 수 있는 경우, 'Transfer Closed' 항목으로 인한 영향이 상대적으로 충분히 작다고 판단되면 이를 모델링에서 제외한다.

밸브 기능 상실에는 아래와 같은 고장원인들이 포함된다. 이들 중 운전 방식에 따라 불필요한 고장 유형과 관련 없는 보조계통 부분을 삭제하여 해당 밸브의 표준 고장수목을 구성한다.

- 밸브 열림 혹은 닫힘 실패
- 밸브 열림 유지 실패 (Transfer Closed during Mission Time)
- 밸브 시험 혹은 보수로 인한 이용불능
- 밸브간의 공통원인고장
- 시험 혹은 보수 후 밸브 원위치 실패 인간오류
- 보조계통 기능상실
  – 밸브 구동전기 상실
  – 밸브 작동신호 상실
  – 밸브 냉각 상실
  – 밸브 룸 냉각 상실

그림 18은 닫힘 상태로 대기중인 모터구동밸브가 사고 시 열림 신호를 받을 때, 이에 대한 표준 고장수목을 예로 정리한 것이다.

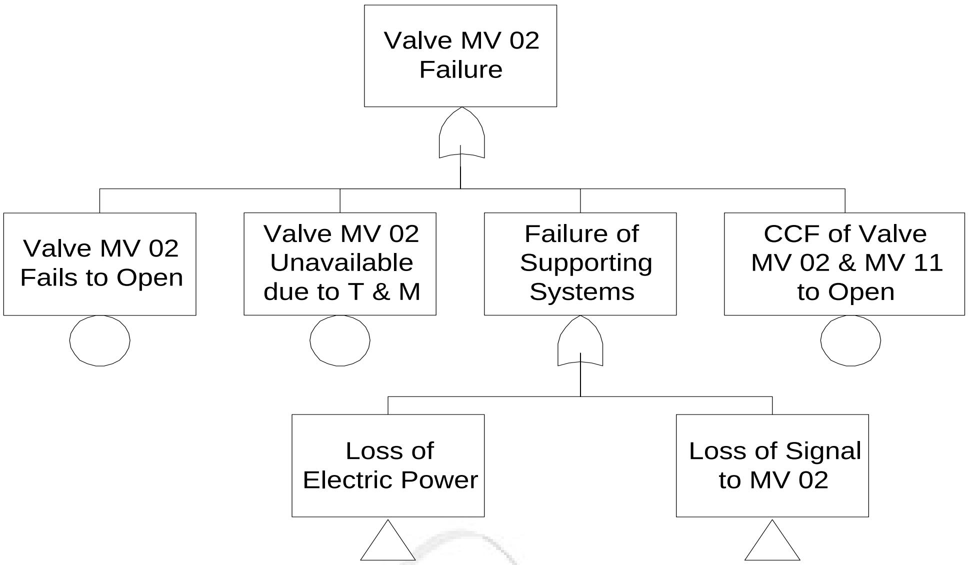


그림 18. 밸브에 대한 표준 고장수목 예

라. 고장수목 정량화

계통 고장수목의 정량화 단계는 입력된 모든 기본사건들의 이용불능도 계산에 필요한 고장률, 작동시간 등 관련 정보를 입력하는 것과 정점사건 이용불능도 계산, 결과 해석 등이 수행된다. 계통 정량화가 별도로 수행되는 것은 아니며 PSA 정량화 과정 중의 하나로 수행된다. 다만, 본 절에서는 계통의 이용불능도 계산과 고장수목의 논리 점검이 계통분석의 범위에 포함되기에 기본사건의 이용불능도 계산 과정을 중심으로 간략히 기술한다. 고장수목의 구성 및 정량화에는 KIRAP코드를 사용하는데, 보다 상세한 신뢰도 자료 입력과 정량화 방법은 코드 메뉴얼에 기술되었다.

(1) 기본사건 이용불능도 계산

계통 고장수목을 정량화 하기 위하여 기계적인 고장, 시험 및 보수를 위한 정지, 시험 및 보수 관련 또는 사고 대응에 관련한 인간오류 그리고 공통원인고장 등 기본사건에 대한 이용불능도를 입력해야 한다. 상기 항목과 같은 기본사건에 이용 불능도값을 부여하여 고장수목을 정량화 하는 방법은 NUREG/CR-2728 "Interim Reliability Evaluation Program Procedures Guide," 에 상세히 설명되어 있다.

<u>기계적 고장으로 인한 이용불능도</u>

고장수목 구성 시 기기의 이용불능도는 일반적으로 아래 두 가지에 기인한다.

- 기계적 고장 (Hardware Failures)

– 기동실패 (Standby Failure : Fail to Start, Fail to Open/Close)
– 일정 기간 작동실패 (Running Failure : Fail to Run, Transfer Closed)

- 시험 혹은 보수로 인한 정지 (Hardware Outages)

기계적 고장은 기기의 구동 실패나 운전 중 고장을 의미하며, 시험 혹은 보수로 인한 정지는 기기의 시험, 예방보수 및 수리 등으로 인하여 기기가 이용불능인 상태를 의미한다.

기기의 기계적 고장은 기본적으로 기기의 기능 및 운전 형태에 따라 달라진다. 기기의 기능면에서 보면, 임의 시점에서 작동 요구가 올 때 그 시점에서만 성공적으로 작동하면 되는 것과 어느 기간 동안 기능을 계속 유지해야 되는 것이 있다. 운전 형태 측면에서 보면 어떤 기기든지 운전 혹은 대기상태 중 하나의 상태에 있게 된다. 만약 대기상태에 있는 기기가 작동 요구 시 일정 기간동안 동작해야 되는 것이라면, 기기의 이용불능도는 작동 요구 시 기능 실패하는 부분과 성공적으로 작동은 했지만 요구하는 기간동안 지속적으로 기능 수행을 못하는 부분으로 구성된다. 이 두 부분의 이용불능도는 기기의 시간당 고장률이나 작동 요구 시 고장 확률(Demand Failure Probability)을 근거로 계산한다.

시간당 고장률로 표현되는 기기고장은 고장을 일으키는 요인으로 인해서 전후 기기시험 시간사이 기기운전 중에 발생하므로 이러한 기기의 시험주기는 고장모드별 이용불능도 계산에 매우 중요하다. 요구 시 고장확률로 표현되는 기기고장은 기기의 시험주기에 좌우되지 않으며, 기기의 운전요구횟수에 의해 결정된다. 시간당 고장률로 표현되는 대기중인 기기의 기동실패(Standby Failure) 확률은 아래 식으로부터 얻는다.

$$q_c = 1/2\ \lambda_s T_T \qquad (1)$$

여기서 q_c 는 기기의 평균 이용불능도, λ_s는 시간당 고장률(Failures/hour), T_T는 시험주기(Hours) 이다. 이 식은 기기의 고장률이 지수함수분포를 가지며, $\lambda_s T_T$ 가 0.1 보다 작을 경우 매우 적당하다.

대기중인 기기의 기동실패 확률은 아래와 같이 주어진 기기 고장률 자료로부터 직접 구할 수 있다.

$$q_c = q_d \qquad (2)$$

여기서 q_c 는 기기의 평균 이용불능도, q_d 는 요구 시 고장확률이다.

해당 기기가 시간당 고장률과 요구 시 고장확률을 모두 포함할 경우에는 아래 수식을 통하여 대기상태의 기기 이용불능도를 좀 더 상세하게 계산할 수 있다.

$$q_c = q_d + 1/2\ \lambda_s T_T \quad (3)$$

여기서 q_c, q_d, λ_s, T_T 는 상기 정의한 내용과 같다. 그러나 일반적으로 제공되는 기기의 고장률 자료는 해당 기기의 시간당 고장이나 요구 시 고장확률 중 하나의 형태로 제공되기 때문에 이 두 부분이 동시에 포함된 이용불능도를 실제로 계산하기는 어렵다.

기기의 시험주기가 약 3 개월보다 작을 경우 식 (1) 과 (2) 는 고장수목 정량화 시 큰 오차나 오류 없이 대기상태의 기기 이용불능도를 예측할 수 있다.

운전중인 기기가 일정시간 동안 계속 작동하지 못하는 동작 중 실패(Running Failure) 확률을 계산하기 위한 모델은 아래와 같다.

$$q_c = \lambda_o T_M \quad (4)$$

여기서 q_c 는 작동실패 확률, λ_o 는 운전 중 시간당 고장률 (Failures/hour), T_M 은 작동시간 (Mission Time) 이다. 이 식은 기기의 고장률이 지수함수분포를 가지며, $\lambda_o T_M$ 가 0.1 보다 작을 경우 매우 적당하다.

따라서 대기중인 기기가 작동 신호에 반응하여 작동시간동안 기능을 수행하지 못하는 확률은, 아래와 같이 기동실패(Standby Failure) 확률과 작동실패(Running Failure) 확률을 더하여 기기의 이용불능도를 계산한다.

$$q_c = q_d + \lambda_o T_M \quad (5)$$

or

$$q_c = 1/2\ \lambda_s T_T + \lambda_o T_M \quad (6)$$

식 (5) 및 (6) 은 주어진 고장률 자료에 따라 선택하도록 한다.

보수정지로 인한 이용불능도 (Maintenance Outage Unavailability)

앞에서 기술한 바와 같이 기기의 보수정지로 인한 이용불능도는 시험, 예방 보수, 수리 등으로 인해 사용할 수 없는 상황을 의미하며, 아래와 같이 구분된다.

- 주기적인 시험 (Periodic Test) 과 계획 예방보수 (Scheduled Preventive Maintenance) 로 인한 계획 보수정지 (Scheduled Outages)
- 고장기기의 수리로 인한 비계획 보수정지 (Unscheduled Outages)

계획 예방보수는 정상적인 발전소 운전 중에 중요한 안전장치에 대해 수행되므로 계획 보수정지로 인한 기기의 이용불능도가 발생한다. 발전소에 따라 계획 예방보수 전략이 다르지만 경험상 계획 예방보수로 인한 기기 이용불능도는 무시할 수 없는 경우가 많다. 계획예방 보수정지(Scheduled Preventive Maintenance Outage)로 인해 발생하는 기기의 이용불능도는 다음 식에 의해 표현된다.

$$q_{SM} = f_M (\tau_M / T_T) \qquad (7)$$

여기서 q_{SM} 은 계획 보수로 인한 기기의 이용불능도, f_M 은 시험주기동안에 발생 가능한 보수 빈도, τ_M 은 평균 기기보수 정지 시간(hours), T_T 는 시험주기(test period)이다.

비계획 보수 정지란 불시적인 기기의 고장으로 인해 기기 보수를 하는 경우를 말한다. 대기상태 기기의 경우에도 주기적인 정기 시험에서 기기의 이상 상태가 확인되므로 비계획 보수정지가 발생할 수 있다. 시험 중 감지된 기기의 실패에 의한 비계획 보수정지로 인해 발생하는 기기의 이용불능도는 다음 식에 의해 표현된다.

$$q_{RM} = f_R (\tau_R / T_T) \qquad (8)$$

여기서 q_{RM} 은 비계획 보수로 인한 기기의 이용불능도, f_R 은 시험주기동안에 발생 가능한 보수 빈도, τ_R은 평균 기기보수시간, T_T 는 시험주기이다.

식 (7) 과 (8) 에서 q_{SM}과 q_{RM} 은 오른쪽 식에서 모든 차원이 상쇄되므로 무차원이다. 예를 들어 T_T 가 시간/달(hours/month), τ_R 이 시간(hours), f_R 이 횟수/달(frequency/test period) 이므로 q_{RM} 은 무차원이 된다.

시험으로 인한 이용불능도 (Test Outage Unavailability)

발전소의 정상운전 중에 대부분의 안전장치나 기기를 기술지침서에 따라 시험할 경우 만약 사고가 발생한다 해도 안전기능을 수행하는 데에는 문제가 없다. 그러나 특정 기기의 시험절차로 인해 기기의 기능을 수행하지 못 할 경우에는 시험으로 인한 보수정지가 발생한다. 시험으로 인한 기기의 이용불능도는 다음 식에 의해 구할 수 있다.

$$q_t = \tau_t / T_T \qquad (9)$$

여기서 q_t 는 시험보수정지로 인한 평균 이용불능도, τ_t 는 평균 시험시간 (hours), T_T 는 시험 주기 (hours) 이다. 시험보수정지로 인한 이용불능도를 계산하기 위해서는 발전소 고유의 데이타를 사용하여 사례별로 처리하여야 하며, 평균 시험시간은 실제 발전소 경험을 근거로 산출한다.

인간오류 확률 (Human Error Probability)

인간신뢰도분석은 사고경위 전개과정에서 발생 가능한 모든 인간오류들을 파악하여 이를 모델링하고 정량화 하는 것이다. 인간신뢰도분석 방법으로는 여러 가지가 있으나 영광 5,6 호기 PSA에서는 ASEP(Accident Sequence Evaluation Program) HRA방법을 기본으로 하였다. 인간신뢰도분석은 데이터 분석 절차서에서 상세히 기술하고 있으므로 본 절에서는 언급을 생략한다.

공통원인고장 확률 (Common Cause Failure Probability)

영광5,6호기 PSA에서 공통원인고장분석은 기본적으로 MGL(Multiple Greek Letter) 기법을 사용하였다. MGL 기법에 의한 공통원인고장 확률 계산 방법은 데이터 분석 절차서에서 상세히 기술하고 있으므로 본 절에서는 언급을 생략한다.

(2) 정점사건 이용불능도 및 중요도 계산

계통분석 정량화는 정점사건에 대하여 구성된 고장수목을 정량적으로 분석하여 계통 이용불능도를 계산하는 단계이다. 고장수목은 정점사건을 유발하는 사건들의 조합을 도식적으로 나타낸 것으로서, 정점사건은 기본사건들의 Boolean 수식으로 표현된다. 이 Boolean 수식을 Boolean 대수로 풀어 정점사건을 유발하는 기본사건들의 조합을 구하며,

이런 기본사건들의 조합을 최소단절집합(Minimal Cut Set)이라 한다. 각 최소단절집합에 포함된 기본사건에 확률값을 대입하여 최소단절집합에 대한 확률값을 구하며, 정점사건을 유발하는 모든 최소단절집합에 대한 발생 확률값을 더하여 계통 정점사건에 대한 확률, 즉 계통 이용불능도를 산출한다. 또한 이 과정에서 기본사건에 대한 중요도분석이 수행되어 각 기본사건이 정점사건에 미치는 중요도를 계산한다. 계통분석 정량화 과정에는 PSA용 전산코드가 사용되는데, 영광5,6호기 PSA에서는 KIRAP(KAERI Integrated Reliability Assessment code Package) 코드를 사용한다.

각 계통 정점사건 및 사고경위에 대한 정량화 단계에서 적절한 시간 내에 계산되면서도 의미있는 모든 최소단절집합을 도출하기 위하여, 전체 결과에 영향이 극히 미미한 일부 최소단절집합을 제외하기 위한 절단값(Cut-off Value)을 적용한다. 영광5,6호기 PSA 에서는 계통 정점사건 및 사고경위 정량화에 대한 절단기준으로 모두 1.0E-11을 적용한다. 이는 통상 계통이용불능도인 1.0E-3 ~ 1.0E-5 보다 1.0E-6 이상 낮은 값이며, 최종 노심손상빈도 추정치에 비해 거의 1.0E-6 이나 낮은 값으로 모든 의미있는 최소단절집합을 고려할 수 있는 절단값이다.

한 계통에서 사고경위에 따라 여러 개의 정점사건이 정의되는 경우, 이용불능도는 정점사건들에 따라 달라진다. 사고경위 정량화를 위해서는 모든 정점사건에 대한 정량화가 수행되지만, 계통분석 단계에서는 대표적인 정점사건에 대하여 정량분석을 수행하여 계통 이용불능도를 확인하고 고장수목 논리를 확인한다.

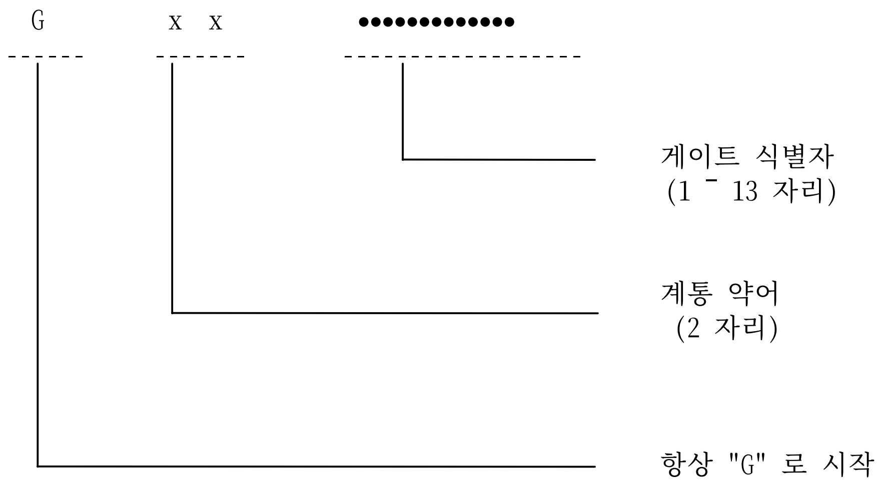
정량화 과정이나 KIRAP 코드 사용 절차는 정량분석 절차서나 KIRAP 코드 메뉴얼에 상세히 기술하고 있다.

2. 고장수목 기본사건 및 게이트 명명법

본 절은 영광5,6호기 PSA에서 사용하는 고장수목 명명법을 기술하고 있다. 이름을 통해 해당 기본사건이 어떤 계통, 어떤 기기의 어떤 종류 고장인지를 쉽게 파악할 수 있어야 하며, 전산코드를 이용하여 자료 관리나 처리가 효율적으로 되도록 다음과 같은 명명법을 준비하여 사용한다. 이 명명법은 게이트 명명법과 기본사건 명명법으로 구성되어 있다.

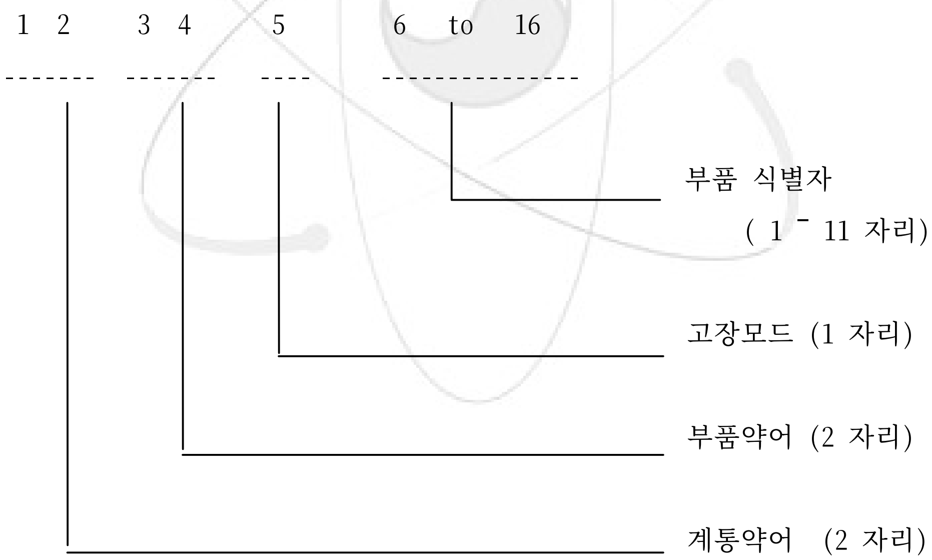
가. 게이트 명명법

게이트 이름은 최대 16자로 만들 수 있다. 첫번째 자리는 항상 "G" 로 시작한다. 두번째와 세번째 자리에는 각 계통을 가리키는 계통 약어를 쓴다. 계통 약어는 계통 약어표를 참조하여 사용한다. 4번째부터 16번째 자리는 다른 게이트 이름과 구별할 수 있는 이름을 부여한다.



나. 기본사건 명명법

다음과 같은 방법으로 기본사건의 이름을 만들 수 있다.



(1) 계통 약어 (System Designator)

첫번째와 두번째 자리에 계통을 가리키는 계통 약어를 쓴다. 각 계통에 대한 약어는 표 22를 따라 표기한다.

(2) **부품 약어** (Component Designator)

세 번째와 네 번째 자리에는 부품을 가리키는 부품 약어를 쓴다. 각 부품의 약어는 표 23에 따른다.

(3) **고장모드** (Failure Mode)

다섯번째 자리는 고장모드를 나타낸다. 각 고장모드의 표시는 표 24에 따라 표기한다.

(4) **부품 식별자** (Component Identifier)

6번째부터 16번째 자리는 각각의 다른 부품의 기본사건들과의 구별을 위해 사용된다. 그러나 11자리를 모두 사용할 필요는 없다. 다음과 같은 사항을 표기함으로써 다른 기본사건들과 구별을 한다.

- 계통도에 표기된 부품의 이름
- 간략한 사건설명

표 22. 계통 약어 (1/2)

계 통 약 어	계 통 이 름
RC	원자로냉각재계통 (Reactor Coolant System)
ST	안전주입탱크 (Safety Injection Tank)
HS	고압안전주입 (High Pressure Safety Injection System)
LS	저압안전주입계통 (Low Pressure Safety Injection System)
SC	정지냉각계통 (Shutdown Cooling System)
(SC 와 LS가 공유하는 부품에 대해서는 "LS" 를 사용한다.)	
CV	화학 및 체적 제어계통 (Chemical and Volume Control System)
CS	격납건물살수계통 (Containment Spray System)
CF	격납건물 환풍 냉각기계통 (Containment Fan Cooler System)
PS	가압기 살수계통 (Pressurizer Spray System - Main, Aux)
PG	가압기 가스 방출계통 (Pressurizer Gas Vent System)
PZ	가압기 안전밸브 (Pressrizer Safety Valve)
MS	주증기계통 (Main Steam System)
CD	복수기계통 (Condensate System)
MF	주급수계통 (Main Feedwater System)
AF	보조급수계통 (Auxiliary Feedwater System)
BD	증기발생기 취출수계통 (Steam Gnerator Blowdown System)
CC	기기냉각수계통 (Component Cooling Water System)
CW	필수냉수계통 (Essential Chilled Water System)
SW	필수용수계통 (Essential Service Water System)
PW	발전소 냉수계통 (Plant Chilled Water System)
TO	터빈건물 개방 냉각수계통 (Turbine Building Open Cooling Water System)
TC	터빈건물 폐쇄 냉각수계통 (Turbine Building Closed Cooling Water System)
RW	원수계통 (Raw Water System)
HC	비상노심냉각계통 기기실 공기조화계통 (ECCS Equipment Room HVAC)

표 22. 계통 약어 (2/2)

계 통 약 어	계 통 이 름
HA	보조건물 공기조화계통 (Auxiliary Building HVAC)
HE	공학적 안전설비 스위치 기어실 공기조화계통 (ESF Switch Gear Room HVAC)
HD	디젤 발전기실 공기조화계통 (Diesel Generator Room HVAC)
HH	취수구 구조물 및 펌프 건물 배기계통 (Intake Structure / Pump House Ventilation System)
IA	압축공기계통 (Instrument Air)
FS	공학적 안전설비작동계통 (Engineering Safety Feature Actuation System)
RP	원자로보호계통 (Reactor Protection System)
1E급 전기	
EO	4.16KV보다 높은 전력
EK	4.16KV 버스
EL	480V 교류전원 부하 센터
EM	480V 교류전원 모터제어센터
EA	120V 교류전원
ED	125V 직류 전원
EG	비상 디젤발전기계통 (Emergency Diesel Generator System)
비 1E급 전기	
NH	13.8KV보다 큰 전력
NO	13.8KV 버스
NK	4.16KV 버스
NL	480V 교류전원 부하 센터
NM	480V 교류전원 모터제어센터
NA	120V 교류전원
ND	125V 직류전원
NG	비 1E급 디젤발전기

표 22. 계통 약어 (3/3)

계 통 약 어	계 통 이 름
NO	13.8KV 버스
NK	4.16KV 버스
NL	480V 교류전원 부하 센터
NM	480V 교류전원 모터제어센터
NA	120V 교류전원
ND	125V 직류전원
NG	비 1E급 디젤발전기
FS	공학적 안전설비작동계통 (Engineering Safety Feature Actuation System)
RP	원자로보호계통 (Reactor Protection System)

표 23. 부품 약어 (1/3)

부 품 약 어	부 품 이 름
MV	Motor Operated Valve
AV	Air Operated Valve
CV	Check Valve
VV	Manual Valve
LV	Solenoid Valve
RV	Relief Valve
SV	Safety Valve
EV	Electro Hydraulic Operated Valve
XV	Other Valves
MP	Motor Driven Pump
DP	Diesel Driven Pump
DG	Diesel Generator
AC	Air Compressor
AB	Blower / Ventilation Fan
AU	Air Handling Unit / Air Cleaning Unit
AD	Air Dryer
AS	Air Separator
CQ	Cubicle Cooler
CU	Chiller Unit
FL	Filter / Strainer
FE	Flow Element / Orifice
NZ	Nozzles
DM	Dampers
TK	Tanks
PI	Piping
HX	Heat Exchanger (Including Steam Generator)
CD	Condenser
TB	Turbine
HT	Heater

표 23. 부품 약어 (2/3)

부 품 약 어	부 품 이 름
HR	Heat Tracing
BY	Battery
BC	Battery Charger
HB	Circuit Breaker (around 4 KV)
LB	Circuit Breaker (around 600V)
RB	Reactor Trip Breaker
FS	Fuse
XH	Transformer (High Voltage)
XM	Transformer (4 KV to 600 / 408V)
XL	Transformer (Low Voltage)
SP	Sump
GD	Grid
SY	Switchyard
BS	Bus
LC	Load Center
MC	Motor Control Center
PN	Distribution Panel
CR	Converter
IR	Inverter
VR	Voltage Regulator
FT	Flow Transmitter
PT	Pressure Transmitter
TT	Temperature Transmitter
LT	Level Transmitter
PW	Pressure Switch
VW	Level Switch
MW	Manual Switch
QW	Torque Switch

표 23. 부품 약어 (3/3)

부 품 약 어	부 품 이 름
LW	Limit Switch
TW	Temperature Switch
SW	Other Switch
CA	Cable
CO	Coil
AL	Alarm
AN	Annunciator
ID	Indicator
BI	Bistable
RY	Relay
SQ	Sequencer
CP	Capacitor
DI	Diode
RS	Resistor
IK	Interlock
CK	Control Circuit
SK	Actuation Signal Generating Circuitry
FW	Flow Switch
OP	Operator Action

표 24. 고장모드 약어

약 어	고 장 모 드
S	Fails to Start
R	Fail to Run / Continue Operating
O	Fail to Open
C	Fail to Close
T	Transfer Closed
G	Fail to Reclose / Reseat
P	Plugged
L	Leakage (Reverse / Internal)
B	Leakage (External) / Rupture / Break
Y	Fails While Operating / Fails to Maintain Output
A	Fails to Provide Output / Fail to Actuate / Generate Actuation Signal
I	Spurious Operation
M	Unavailable Due to Test / Maintenance
H	Operator Error to Perform a Task / Operator Inadvertent Action
V	Operator Recovery Action Failure
U	Operator Fails to Restore After T&M
X	Electrical Short
N	Open Circuit
E	Fails to Energize
D	Fails to Deenergize
F	Failure (General)
W	Common Cause Failure (Demand)
K	Common Cause Failure (Operating)
Z	Modularized Event

제6장 신뢰도 데이터 분석

제4절 개요

1. 목 적

고장수목에 나타난 모든 기본 사건의 발생확률을 입력함으로써, 정량분석의 토대를 제공한다. 기본사건의 데이터는 고장수목 구성 시 임의대로 입력하거나, 이미 만들어진 데이터베이스로부터 추출하여 사용하게 된다. 그러나 계통이용불능도의 계산을 위해 일반 데이터베이스를 사용하거나 발전소 고유 데이터를 수집, 분석하여 사용한다. 그러므로 평가된 데이터의 질과 데이터 평가에 사용된 방법론은 PSA 정량화 결과에 직접적인 영향을 준다. 따라서 신뢰도 데이터베이스의 개발은 확률론적 안전성평가 (Probabilistic Safety Assessment : 이하 PSA) 수행에 있어서 중요한 부분의 하나이다. 그러므로 본 데이터분석 절차서에서는 원자력발전소의 PSA 수행 시 데이터분석의 절차와 기법을 기술하여 정확한 데이터 분석 지침을 제공하고자 한다.

신뢰도 데이터 분석에서는 계통 모델링 시와 사고경위 개발 시에 정의된 초기사건 빈도, 기본사건에 대한 고장확률 그리고 오차 인자를 추정하여 사고경위 정량화를 위한 데이터베이스를 구축한다.

2. 적용 범위

본 데이터분석 절차서에서는 그 동안 국내에서 설계 중인 원전에 대하여 수행되었던 PSA의 데이터분석 절차 및 방법을 기본적으로 정리하였다. 따라서 본 절차서에 기술된 데이터 분석의 방법 및 수준은 국내의 설계 중인 원전 PSA에 적용된 데이터분석에 준하는 것으로서, 향후 설계 중 원전 PSA의 데이터분석에 적용할 수 있을 것이다.

기기 고장율 데이터, 시험 및 보수 데이터와 인간오류 데이터는 계통분석의 결과를 정량화할 때 입력 자료로 사용되며 초기사건 빈도 데이터는 사고추이분석의 정량화 시 입력자료로 사용되고 공통원인 고장 데이터는 계통분석 및 사고 추이 분석에 모두 필요하다.

개발되는 데이터베이스는 사고경위 정량화를 위해 모델하는 각 기본사건에 대해 점 추정치와 불확실성 추정치를 포함해야 한다.

PSA 수행 시 필요한 데이터는 다음과 같다:

- 초기사건 데이터
- 기기 고장율 데이터
- 기기 공통원인 고장 데이터
- 인간 오류 데이터
- 보수 및 시험 데이터

3. 참고문헌

데이터 분석 방법에는 여러 가지 기법이 있으나, 본 절차서는 특별히 한국원자력발전소에서 수행한 PSA에서 사용되는 데이터 분석을 대상으로 기술하였다. 데이터 분석에 대한 참고문헌으로는 여러 종류가 있으나, 본 절차서를 작성하기 위해 참고한 대표적인 문헌은 다음과 같다.

[1] "PRA Procedure Guide", NUREG/CR-2300", ANS and IEEE, 1982.

[2] "Probabilistic Safety Analysis Procedures Guide", NUREG/CR-2815, 1984.

[3] "Procedures for Conducting Probabilitic Safety Assessment of NPPs (Level 1)", IAEA, 1992.

[4] "고리 3,4 호기 및 영광 1,2 호기 PSA 수행절차서", 한국전력공사, 1992.

[5] "Fault Tree Anlaysis Guidelines", Commonwealth Edison IPE/Accident Management Program, Rev.0, 1990.

[6] EPRI-URD

[7] 울진 3,4호기 PSA

[8] Swain, "Accident Sequence Evaluation Program Human Reliability Analysis Procedure", NUREG/CR-4772, 1987.

[9] Dougherty, J.R. Fragola, "Human Reliability Analysis", John Willy & Son, 1987.

[10] Swain, H.E. Guttmann, "Handbook of HRA with Emphasis on NPP Application", NUREG/CR-1278, 1983.

[11] Hannaman, J.R. Fragola, "Systematic Human Action Reliability Procedure", Interim Report, NP 3583, EPRI, 1984.

[12] 한국전력공사, "Ulchin Unit 3,4 Final PSA Report", Rev.0, 1997.

[13] 한국전력공사, "영광 5,6 호기 확률론적 안전성평가 보고서", 2000.

[14] Bell, A.D. Swain, "A Procedure for Conducting a HRA for NPPs", NUREG/CR-2254, 1983.

[15] Hannaman, A.J. Spurgin, Y.D. Lukic, "Human Cognitive Reliability Model for PRA", NUS-4531, Draft, 1984.

4. 기본가정 및 용어정의

본 절차서는 설계 중인 원전인 영광5,6호기 전출력 Level 1 PSA에 적용하기 위해 작성한 절차서로서, 그 동안 국내에서 수행되었던 설계 중인 원전 PSA의 데이터분석 방법에 근거하여 작성한 것이다. 따라서, 운전 중인 원전의 데이터분석이나 전출력 이외의 운전모드에 대한 데이터 분석을 위해서는 필요에 따라 일부 내용을 수정하여 사용할 수 있다.

데이터분석에서 사용되는 주요 용어는 다음과 같다.

PSA	확률론적 안전성 평가
노심손상빈도	노심손상 사고가 발생할 수 있는 빈도로 1년 단위로 계산된다.
사고경위	사건수목에서 계통 작동유무에 따라 전개되는 사고 시나리오. 하나의 사고경위는 어떠한 초기사고가 발생한 후 어떠한 계통들이 작동하였고 어떠한 계통들이 실패하였는지에 따라 정해진다.
초기사건	원전 정상 운전 중 이상사태를 발생시킬 수 있는 사고. PSA 에서는 유사한 사고들을 그룹화하여 하나의 초기사건으로 처리하며, 대부분의 경우 원자로 정지로 이어지는 사고만을 취급한다.
정점사건	계통이 특정 운전 조건에서 필요한 기능을 성공적으로 수행하지 못하는 사건
기본사건	고장수목 논리 전개에서 최종 하부에 위치하는 사건들로서 신뢰도 자료의 입력이 가능한 기본 단위. 기기의 기계적 고장, 보수 및 시험 이용불능 사건, 인간오류 사건 등이 포함된다.
과도사건	정상출력 운전중 기기 혹은 운전원 조치 실수에 의해 계통운전 변수의 변화를 초래하여 원자로 정지를 유발하는 사건
냉각재 상실사고	일차계통 압력경계의 파손에 의해 발생되는 냉각재 상실사고 중 충전계통의 냉각재 보충능력을 초과하는 모든 사건

회복조치	기능이 상실된 기기를 운전원이 복구하는 조치

제5절 분석 절차

데이터 분석 시 분석되어야 할 데이터의 종류는 초기사건 빈도, 기기 신뢰도 데이터, 공통원인고장 데이터, 인간오류 데이터, 시험 및 보수 데이터 등의 5가지로 구분된다.

데이터 분석 절차는 크게 데이터 분석 기본 준비 단계와 5가지 분류된 각각의 데이터에 대한 분석으로 구분할 수 있다. 데이터 분석을 위한 기본 준비는 여러 데이터에 공통적으로 적용되는 지침이나 정보, 데이터 분석의 범위, 분석 수준, 기본 가정 등 전체 데이터 분석 방법의 통일성이나 효율성을 얻기 위해 필요한 사전 준비 작업이다. 반면, 개별 데이터에 대한 데이터 분석 절차는 앞에서 설명한 5종류의 데이터들에 대한 분석 절차를 의미한다.

사고 경위 정량화를 위한 데이터 베이스 개발을 위해서는 데이터 수집, 분석 그리고 적절한 신뢰도 모델을 사용한 평가 등의 다단계 과정이 필요하다. PSA 목적 및 특성에 따라 관련 분석 단계 중 일부는 간략히 수행하거나 생략할 수 있다. 예를 들어, 설계 중인 원전의 PSA인 경우, raw data를 수집하고 분석하는 대신 이전에 수행된 PSA 보고서의 데이터를 사용할 수 있다.

본 절차서는 설계 중인 원전 PSA에서 수행된 데이터분석 절차를 정리한 것으로서, 기본적으로 일반 데이터원을 사용한 신뢰도 데이터 분석 과정을 설명하고 있다. 신뢰도 데이터 분석에는 다음과 같은 5가지 종류가 있다.

- 초기사건 빈도 분석
- 기기 신뢰도 데이터 분석
- 공통원인고장 분석
- 인간 신뢰도 분석
- 시험 및 보수 이용불능도 분석

1. 초기 사건 빈도 분석

가. 개요

설계 중인 원전의 PSA에서 초기사건 빈도는 일반 자료원에 근거하여 계산한다. 다만 소외전원상실과 같이 발전소 스위치야드의 설계 특성이나 소외 전력망의 안전성에 크게

영향을 받는 경우에는 국내 운전이력을 반영하여 초기사건 빈도를 결정하였다. 일반 자료원을 사용한 초기사건 빈도 계산 방법도 여러 가지가 있다. 즉, 초기사건 빈도 값을 그대로 인용하는 경우, 계통의 특성을 반영한 고장수목을 구성하여 초기사건 빈도를 계산하는 경우와 수리적 방법을 사용해서 빈도를 계산하는 경우가 있다. 영광 5,6호기 내부사건 분석의 초기사건 빈도 분석에서 사용된 분석 방법을 표 25에 정리하였다.

표 25. 영광 5,6호기 내부사건 분석에서의 초기사건 및 빈도 분석 방법

초기사건	비고
Large LOCA	Generic data (ALWR KAG) 이용하였으나 기본 가정 재해석
Medium LOCA	Generic data (ALWR KAG) 이용하였으나 기본 가정 재해석
Small LOCA	Generic data (ALWR KAG) 사용
Steam Generator Tube Rupture	Generic data (ALWR KAG) 사용
Large Secondary Side break	Generic data (ALWR KAG) 사용
General Transients	발전소 특성에 따른 초기사건 그룹핑 및 ALWR KAG 자료 사용
Loss of Feedwater	Generic data (NUREG/CR-3862) 사용
Loss of Condenser Vacuum	Generic data (NUREG/CR-3862) 사용
Loss of a 125V DC Bus	Generic data (ALWR KAG) Bus 고장율에 기초하여 계산
Loss of a 4.16 KV Bus	Generic data (ALWR KAG) Bus 고장율에 기초하여 계산.
Loss of a CCW Train	계통 고장수목 모델 이용하여 계산.
Loss of Offsite Power	국내 소외전원상실 발생빈도 사용
Station Blackout	계통 고장수목 모델 이용하여 계산.
Anticipated Transients without Scram	고장수목 모델 이용하여 계산.
Interfacing Systems LOCA	수리적 모형 사용 (압력경계마다 LOCA 가능성을 조건부 확률모델로 평가)
Reactor Vessel Rupture	Generic Data (WASH-1400) 사용

나. 분석 절차

(1) 일반 데이터를 사용한 경우

일/이차측 파단 사건의 빈도는 일반 데이터원인 ALWR URD KAG의 자료를 가공하지 않고 사용하였다. 단, 대형 및 중형 LOCA빈도는 일반 데이터의 LOCA 사이즈 정의를 참고하여 재계산 하였다. ALWR KAG에 의하면 현 PSA의 중형 LOCA 이상의 파단 사고의 발생 빈도를 보수적으로 대형 및 중형 LOCA 빈도에 각각 적용하고 있다. 그러나, 영광 5,6호기 PSA에서는 이를 보다 현실적으로 적용해서, 대형 및 중형 LOCA의 발생 가능성이 동일하다는 가정 하에 ALWR KAG 발생 빈도를 1/2 하여 각각 사용하였다.

일반 데이터를 사용한 초기사건은 대형, 중형 및 소형 LOCA, 증기발생기 세관 파단, 원자로 용기 파손, 이차측 대형 파단, 4.16KV 교류모선상실, 125V 직류모선상실, 급수상실, 복수기 진공상실 등이다.

(2) 계통 고장수목을 구성한 경우

일부 초기사건은 계통의 설계 특성을 보다 정확히 반영하기 위해서 계통 고장수목을 구성하여 초기사건 발생 빈도를 계산한다. 기기냉각수상실, 발전소 정전, 정지불능 과도사건 등에 대한 초기사건빈도를 고장수목을 통해 계산하였으며, 일반 과도사건의 경우는 고장수목은 별도로 구성하지 않았지만, EPRI 과도사건 목록에서 일반 과도사건으로 그룹핑된 대상 과도사건의 빈도를 취합해서 초기사건 빈도를 도출하였다.

(3) 기타

기타 방법으로는 국내 원전의 운전 이력을 사용하는 경우와 수리적 방법을 사용해서 초기사건 빈도를 계산하는 방법이 있다. 소외전원상실 사건은 국내 전력망의 안전성이나 환경적인 특수성이 중요한 영향 인자이기 때문에 국내 원전의 불시정지 이력을 조사/분석하여 초기사건 빈도를 계산하였다. 저압 경계부 LOCA 사건은 대상 파손 부위를 결정한 후 수리적 모형을 사용해서 초기사건 발생 빈도를 계산하였다.

2. 기기 신뢰도 데이터 분석

가. 개요

영광 5,6 발전소와 같이 설계 중인 발전소에 대한 고유 발전소 자료는 없다. 그러므로 영광 5,6호기 PSA에 사용한 기기 신뢰도 데이터는 일반 기기 고장율을 바탕으로 하여

개발되었다. 주로 사용한 일반 자료원은 "ALWR PRA Key Assumptions and Groundrules (KAG) of revision 7, 12/95 " 이며, 그 외 NUREG/CR-4639 등의 자료원이 사용되었다.

나. 분석 절차

(1) 데이터 수집 대상 기기 목록 작성과 고장모드 정의

발전소의 여러 기기들 중 분석 대상기기를 파악하여 목록을 작성한다. 그러나 완벽한 기기 목록은 계통 분석이 완결된 후에 얻을 수 있으므로 유사 발전소의 PSA 결과를 검토하여 발전소의 일반 기기 목록을 작성한다. 이 단계에서는 분석 대상 계통을 선정하여 데이터 수집 대상 기기 목록을 작성하고, 각 기기에 대한 고장모드를 정의하여야 한다.

고장모드는 일반적으로 세 가지 즉, 대기상태 고장, 운전 중 고장 그리고 작동 요구 시 고장으로 나누어진다. 이러한 정의는 일반 데이터에 반영되어 있는 고장 데이터의 형태와 계통 모델링에서 고려되는 기기의 고장 모드를 동시에 표현하고 있다.

(2) 기기 경계 정의

기기의 물리적 경계를 결정하여 기기 고장을 정의한다. 이 물리적 경계는 분석 수준에 따라 보조 기기, 제어 기기, 전기 기기 등의 연결장치 (coupling mechanism)와 관련하여 결정되며, 데이터의 이용 가능성에 의해서도 결정된다. 물리적 경계의 결정은 주요 밸브, 펌프 및 디젤발전기에 대해서 뿐만 아니라 제어계통 분석 대상 블랙박스 주위에 대해서도 설정해야 한다.

(3) 기기 고장확률 분류 및 평가 방법 선정

계통 고장수목과 사고경위 정량화를 위해서는 다음과 같은 두 가지 종류의 기기 고장확률이 필요하다.

- 이용불능도 (unavailability) - 어떤 계통이나 기기가 작동 요구 시 작동하지 못할 확률
- 신뢰도 (reliability or unreliability) - 어떤 계통이나 기기가 성공적으로 작동한 후 주어진 시간 동안 운전되지 못할 확률

기기 이용불능도(unavailability)는 작동 실패율을 가지고 계산할 수 있다. 작동 실패는 기기가 어떤 상태를 바꾸거나 기동 요구에 대한 기동 실패를 의미한다. 고장 데이터가 작동 요구에 대한 실패 확률이라면, 그 값은 기기의 이용불능도이다. 그러나 어떤 경우에는 기기의 대기 기간 동안의 단위시간에 대한 실패로 고장 데이터가 주어진다. 이런 경우에는 다음의 계산식으로 기기의 이용불능도를 추정한다.

$$U = \lambda_s \cdot T_s / 2$$

여기서, U는 기기의 이용불능도, λ_s는 기기의 대기 중 고장률(Standby Failure Rate), T_s는 평균 시험 간격(Test Interval)을 의미한다. 대기 중 고장률 λ_s는 기기가 관찰된 시간과 고장 횟수에 의해 다음과 같이 추정된다.

$$\lambda s = \frac{X}{T}$$

여기서, X는 고장 횟수이고, T는 관측된 총 운전 시간을 나타낸다.

반면에 '작동 중 고장'은 기기가 운전 중에 고장난 경우로서, 고장이 발생하는 즉시 관련 계통에 영향을 주어 기기의 고장이 발견될 수 있다. 작동 중 고장으로 인한 기기의 이용불능도는 다음 식에 의해 계산된다.

$$U = \lambda_r \cdot T_r$$

여기서, λ_r은 작동중 고장률(Running Failure Rate), T_r은 작동요구시간이다.

만일 센서와 같이 기기의 상태가 주제어실에서 항상 감시되는 경우에도 위의 '작동 중 고장' 이용불능도 계산식을 사용해서 기기의 이용불능도를 구할 수 있다. 이때 Tr은 기기가 고장나 있는 시간으로 평균수리시간(Mean Time to Repair: MTTR)이 된다.

일반적으로 원자력 발전소의 안전 관련 계통의 기기들은 매우 높은 신뢰도를 갖기 때문에 고장 경험 자료가 매우 적다. 해당 기기의 운전 경험 자료가 충분하지 않아서 그것만으로 고장률 또는 고장 확률을 추정하기 어려운 경우, 베이지안 통계 처리 기법에 의해 고장률 또는 고장확률을 계산한다. 베이지안 기법이란 간단히 말해서 일반 자료원에 있는 기기 고장률을 해당 기기의 운전 경험 자료를 반영해서 기기 고장률을 추정하는 통계적 방법이다.

(4) 일반 기기 신뢰도 데이터 베이스 개발

일반 데이터원들은 각각 유사 기기 및 고장 모드에 대해 서로 다른 추정치를 가지는 경우가 많다. 또한 데이터원들은 각각 다른 기기 경계를 가지는 경우도 있다. 따라서 적절한 일반 데이터 추정치를 결정하기 위해서는 각각의 데이터원에 대한 분석과 분석가의 판단이 필요하다. 영광 5,6 호기와 같이 설계 중인 발전소는 운전이력이 없으므로 PSA 정량화를 위해 일반 고장율을 바탕으로 하여 일반 기기 신뢰도 데이터 베이스를 개발한다. 일반 기기 신뢰도 데이터의 주된 일반 자료원은 "ALWR PRA Key Assumptions and Groundrules (KAG)"와 NUREG/CR-4639이다. 그러나 선정된 기기의 각 고장 모드에 대한 데이터가 적절하지 않은 경우에는 두 자료원 이외의 자료원을 참고로 하여 일반 기기 신뢰도 데이터 베이스를 개발하였고, 다음의 분석 단계를 거쳐 평가하였다.

- 1 단계 : 일반 기기 신뢰도 데이터 베이스 구축을 위해 다음과 같은 고장 데이터 자료를 검토한다. 검토된 자료는 이전의 PSA 보고서, LER (License Event Report) 자료 등의 자료로 구한 데이터 베이스이다.
  - "RKS 85-25 Reliability Data Book for Components in Swedish Nuclear Power Plants," Nuclear Safety Board of the Swedish Utilities, 1985.
  - "Advanced Light Water Reactor Requirement Document Vol II: Utility Requirements for Evaluatory Plants Appendix A to Chapter 1 ; PRA Key Assumptions and Ground Rules," Rev. 7, EPRI, 1995.
  - "System 80+™ Probabilistic Risk Assessment," LD-92-106, CE-ABB, 1992.
  - T. W. Kim, et. al., "Survey and Analysis of the Loss of Off-site Power Events on Korean Nuclear Power Plants and the Reliability/Unavailability of Emergency Diesel Generators of Kori Units 3 and 4," KAERI/TR-363/93, KAERI, 1993.
  - "Base Line Level 1 Probabilistic Risk Assessment for the System 80® NSSS Design," LD-88-008, CE-ABB, 1988.
  - T. J. Lim, et. al., "Survey and Comparison of Generic Component Reliability Data and Establishment of Preliminary Generic Database for Use in PSA", KAERI/TR-364/93, KAERI, 1993.
- 2단계 : 각 데이터 베이스의 고장율에 포함된 기기 경계를 확인한다.
- 3단계 : 모든 일반 데이터원 중에서 가장 대표적이라고 판단되는 값을 선정한다. ALWR PRA KAG 자료는 일반 자료원과 특정 발전소 자료도 포함하고 있는 대표적인 자료원이다.

ALWR PRA KAG 자료에서 값을 제시하고 있지 않거나 인용하기 곤란한 몇몇 기기들에 대해서는 다른 일반 자료원으로 부터 값을 인용하였다. 이런 과정을 거쳐 얻은 일반 기기 신뢰도 데이터는 영광 5,6호기 PSA 보고서에 정리되어 있다.

3. 공통원인고장 데이터 분석

공통원인고장 사건은 MGL (Multiple Greek Letter) 방법을 사용하여 모델하였다. MGL 방법은 기기고장 사건을 하나의 독립적 사건과 여러가지 공통원인고장 사건으로 나눈다. 각 공통원인고장 사건은 크기 m인 공통원인 기기 군에 대하여 다음과 같이 표현될 수 있다.

m : 독립사건 수

${}_mC_2$: 2 개의 특정 기기를 포함하는 공통원인고장 사건 (double CCF)

.

${}_mC_k$: k 개의 특정 기기를 포함하는 공통원인고장 사건 (k-tuple CCF)

.

${}_mC_m$: 모든 m 개의 기기를 포함하는 공통원인고장 사건 (m-tuple CCF)

고장수목과 사고경위의 정량화를 위해서 위 공통원인고장 사건의 확률을 평가해야 한다. MGL 방법에서는 평가의 단순화를 위해서 대칭(symmetry) 가정이 적용된다. 대칭 가정에 의하면 유사한 유형의 기기가 포함된 유사한 기본사건의 확률은 같다. 공통원인 기기군 내의 어떠한 주어진 기본사건의 고장확률은 그 기본 사건의 특정기기에 의존하는 것이 아니라 조합의 수에만 의존한다.

따라서 모든 k-tuple 공통원인고장사건은 다음과 같은 동일 확률을 가질 것이다.

$Q^{(m)}{}_k$:크기 m인 공통원인 기기군에서 k (k = 1, 2, ..., m) 개의 특정 기기가 포함된 기본 사건 확률.

만약 m이 n과 같지 않다면 일반적으로 $Q^{(m)}{}_k$ 는 $Q^{(n)}{}_k$ 와 같지 않기 때문에 공통원인 기기군의 크기에 의존하는 기기 유형에 대하여 $Q^{(m)}{}_k$ 의 여러 가지 다른 집합이 존재할 수 있다. MGL 방법은 총 (m-1)개의 변수를 정의하고 추가로 크기 m인 공통원인기기 그룹의 $Q^{(m)}{}_k$ 를 평가하기 위해서 총 기기실패확률 Q_t에 대한 확률을 정의한다. MGL 변수는 같은 기기군 내의 다른 기기들과 공유할 수 있는 기기의 모든 가능한 공통원인고장확률 경로에 대한 조건 확률이다. 예를 들어, 크기 3인 기기군의 MGL 변수는:

β = 한 특정기기가 실패했을 때, 기기고장의 원인이 하나 이상의 추가 기기에 공유될 수 있을 조건 확률이다. 그리고,

γ = 2 개의 특정 기기가 실패했을 때, 하나 이상의 기기에 공유된 기기 고장의 원인이 두개 이상의 추가 기기에 공유될 수 있을 조건 확률이다.

$Q^{(m)}{}_k$ 의 확률은 Q_t 및 MGL 변수를 사용하여 다음 식으로 계산한다:

$$Q^{(m)}{}_k = \frac{1}{{}_{m-1}C_{k-1}} \prod_{i=1}^{k} \theta_i (1-\theta_{k+1}) Q_t \qquad (1)$$

이 때, k = 1, 2, ..., m

여기서,

θ_i (i = 1, 2, ..., m+1)

= MGL변수 (θ_1=1, θ_2=β, θ_3=γ, ..., θ_{m+1}=0)

Q_t : 전체 기기 고장확률

m : 공통원인고장 군에서 특정기기가 포함된 기본사건 확률

$Q^{(m)}_k$ 의 평가를 위해서 Q_t 및 MGL변수를 평가해야 한다. 공통원인고장 경험 데이터에 기초하여 MGL 변수를 평가하는데 영광 5,6호기 PSA에서는 참조 원전 PSA에서 사용한 MGL 변수 값을 사용하였다. 일반적인 값은 NUREG/CR-4780 의 0.1로 가정하였다. β와 다른 MGL 변수는 대부분의 경우 0.5 와 0.99 사이로 평가한다. β와 다른 값이 1.0에 근접하면 모든 기기를 포함하는 공통원인고장사건의 확률은 극히 일부 기기를 포함하는 공통원인고장 사건의 확률에 좌우된다.

4. 인간신뢰도 데이터 분석

가. 개요

본 절차서는 ASEP(Accident Sequence Evaluation Program) 인간신뢰도분석(Human Reliability Analysis : 이하 HRA) 및 THERP(Technique for Human Error Rate Prediction) 방법을 기본으로 하고 있으며, 설계 중 원전 PSA의 HRA 수행 절차서로 만들어졌다. 분석 방법 및 절차는 전체적으로 ASEP 방법을 따랐으나 그간의 HRA 수행 경험을 바탕으로 일부 정량화 규칙을 세분화 하였다. PSA 예비분석 단계를 위한 선별분석(Screening Analysis)은 실제 PSA 수행 절차에 맞추어 보다 간단한 방법을 적용하였으며, 과거 PSA 수행 경험 및 데이터 베이스를 바탕으로 가능한 상세분석(Nominal Analysis)을 직접 수행하기 위한 절차를 만들었다. 본 절차서는 설계 중 원전 PSA 전출력 내부사건분석에서 고려하는 인간오류를 분석하기 위하여 작성하여 영광 5,6 호기 PSA의 HRA에 적용하였다.

나. 분석 절차

HRA 수행 절차로는 A.D. Swain 에 의하여 개발된 THERP (Technique of Human Error Rate Prediction) 기법과 Hannaman이 개발한 SHARP (Systematic Human Action Reliability Procedure) 방법이 있다. 두 방법 모두 원전운전과 관련된 인간의 작업성능 평가를 PSA 수행과 연계하여 체계적인 방법으로 수행할 수 있도록

개발되었으며 두 방법 모두 유사한 분석 절차를 포함하고 있다. 실제 HRA 분석 절차는 선별분석과 상세분석으로 구분할 수 있다.

(1) 선별분석

사고 후 인간오류에는 절차서 수행상 필요한 직무를 수행하지 못하는 경우와, 자동 작동 실패한 기기를 수동으로 작동하지 못하는 경우, 그리고 고장 난 기기를 현장에서 수동으로 조작하는 경우 등이 포함된다. 선별분석 단계에서는 고장 난 기기의 현장 조작은 고려하지 않는다. 이 부분은 최종 정량화 단계인 최소단절집합에 대한 Recovery Analysis에서 고려한다. 선별분석에서는 다음 규칙에 의거하여 오류 확률 값을 선정한다.

다음 경우 인간오류 확률 값으로 1.0 사용한다.

- 주제어실 밖에서 수행되는 중요 작업
- 수행절차서가 없는 경우
- 필요 계기가 고장이거나 잘 못 읽힌 경우

나머지 사고 후 인간오류는 다음과 같이 사고 발생 후 시간에 따른 HEP를 사용한다.

- 초기사건 발생으로부터 15 분 이내의 인간오류 : HEP = 1.0
- 초기사건 발생으로부터 30 분 이내의 인간오류 : HEP = 0.2
- 초기사건 발생으로부터 30분 이상 60 분 이내의 인간오류 : HEP = 0.1
- 초기사건 발생으로부터 60 분 이후의 인간오류 : HEP = 0.01

(2) 상세분석

사고 후 인간오류는 크게 다음 진단오류와 수행오류 두 단계로 구분하여 분석한다.

<u>**진단오류 분석**</u>

진단과정의 오류는 주로 허용시간에 영향을 받는다는 가정 하에, 최대 진단 허용시간에 대한 THERP (NUREG/CR-1278) 진단오류 표를 사용하여 분석한다. 분석 절차는 다음과 같다.

(1) 최대 허용시간(Tm) 추정 : 사고해석, FSAR, 작업분석(task analysis), 타 PSA보고서 및 전문가 판단에 근거하여 주어진 작업이 수행되어져야 하는 최대 허용시간을 추정한다.

(2) 작업예상 시간(Ta) 추정 : 진단이 완료된 후 작업 위치로 이동하여 적절한 작업을 완료하는 데 필요한 시간으로 발전소 walk-through를 통한 실측 시간이나 시뮬레이터에서 측정한 작업 시간을 사용한다.

(3) 추정된 시간들을 근거로 진단허용시간 (Td) 결정 : Td = Tm - Ta

(4) THERP (NUREG/CR-1278) 진단오류 표나 그림에 근거하여 진단오류 확률 값을 산출한다.

(5) 동일한 진단허용시간(Td)에도 불구하고 운전원의 업무 수행도는 달라질 수 있으므로 여러 영향인자를 고려하여 기본 진단오류 값을 보정한다.

(6) 짧은 시간 내에 하나 이상의 이상상태(abnormal event)가 발생하는 경우, ASEP Table 8-2 이용하여 두 번째나 세 번째 진단오류를 평가한다. 하나 이상의 이상상태를 평가할 것이냐는 아래 기준을 사용하여 결정한다.

<u>행위오류 평가</u>

진단 후 조치 행위에 대한 평가는 THERP를 기본으로 작성된 아래 절차를 따라 수행한다. 행위오류 분석은 ASEP HRA 방법을 근거로 하는데, 오류 가능성은 크게 작업유형 (task type) 및 스트레스 수준에 의해 결정되며, 얻어진 오류 확률 값은 다른 운전원에 의한 복구 가능성이나 정보 feedback 수준에 의해 보정 된다.

(7) 작업분석을 통해 사고경위 및 사고 상황 (이용불능인 안전관련 계통), 작업 내용, 작업 위치 및 환경, 작업소요 시간, 적용 절차서, Information feedback 수준, 여러 가지 작업 영향 인자 등에 대한 정보 수집한다.

(8) 작업유형 (task type) 결정 : 진단 후 조치행위의 특성이 dynamic인지 step-by-step인지 결정한다.

(9) Stress level 결정 : 다음 규칙에 따라 스트레스 수준을 결정한다.

(10) Basic HEP 결정 : 작업유형과 스트레스 수준에 따라 기본 인간 오류 값을 선정한다. 이것은 ASEP HRA 방법에서 제시한 것으로 중앙값이며, 실제 적용 시에는 평균값을 산출하여 사용한다.

- moderately high stress 상황에서 step-by-step(critical procedural) action 수행 : HEP = 0.02 (EF = 5)
- moderately high stress 상황에서 dynamic action 수행 혹은 extremely high stress 상황에서 step-by-step action 수행 : HEP = 0.05 (EF = 5)
- extremely high stress 상황에서 dynamic action 수행 : HEP = 0.25 (EF =5)

(11) Time Stress 하에서의 Doubling Rule : moderately high or extremely high stress 하에서 매우 제한된 시간 내에 작업이 동일 운전자에 의해 진행되어야 할 경우, 만일 첫번째 action이 ineffective하면 후속 actions을 실패할 확률은 정상 평가치를 배(double)하여 사용한다.

(12) 다른 운전원(감독자)에 의한 Recovery 가능성 고려 : 이상상태 발생 후 초기 과도기간이 지나면 급박한 상황 전개는 줄어들게 되며, 이 경우 한 운전원에 의한 조치 행위의 오류는 다른 운전자나 감독자에 의해 확인되고 바르게 수정될 수 있다. 이런 복구 가능성을 다음 규칙에 따라 고려한다.

- 기본적으로 basic HEP 의 10% 고려
- moderately high stress 상황에서 step-by-step (critical procedural) 인 경우 : HEP = 0.2 (EF = 5)
- moderately high stress 상황에서 dynamic action 혹은 extremely high stress 상황에서 step-by-step 인 경우 : HEP = 0.5 (EF = 5)
- extremely high stress 상황에서 dynamic action 인 경우 : HEP = 0.5 (EF =5)
- extremely high stress 상황에서 dynamic action인 경우 time stress를 받는 경우 많은데, 시간이 30분 이내로 짧은 경우 감독자에 의한 Recovery 가능성은 고려하지 않는다.
- human redundency 이외에 다른 Recovery 인자가 있다면 이를 별도로 고려할 수 있다.

(13) 정보 feedback 에 의한 오류 복구 가능성 고려 : 발생한 조치단계의 인간오류를 복구할 수 있는 가능성을 고려하여 수행오류 확률 값을 보정해 준다.

(14) 최종 인간오류확률 값 HEP 산출

- 진단오류 확률 값과 행위오류 확률 값을 더하여 최종 인간오류 확률 값을 산출한다.

(15) 오차인자(error factor)는 다음 규칙을 사용하여 결정한다. 그러나, 인간오류의 95% 값이 1 보다 크면, 95%값이 1을 넘지 않도록 오차인자를 적절히 수정한다.

- 인간오류 확률 값이 0.01 보다 작으면 (HEP < 0.01) EF = 10
- 인간오류 확률 값이 0.1 보다 작으면 (0.01 < HEP < 0.1) EF = 5
- 인간오류 확률 값이 0.1 보다 크면 (HEP > 0.1) EF = 3

5. 시험 및 보수 데이터 분석

시험 및 보수 데이터 역시 일반 데이터원에 근거하여 결정하였다. 일반적으로 기기 고장율에 대한 데이터는 많지만, 보수 또는 시험으로 인한 이용불능 데이터는 거의 없다.

가. 시험 및 보수 데이터 분석 대상 계통 선정

작동 요구 시 계통이 작동할 수 있도록, 대기 모드에 있는 계통을 대상으로 시험을 수행한다. 그러나 영광 5,6 호기의 안전관련 계통은 시험 시라도 실제 운전 조건이 되면 작동하는 override 기능을 가지고 있으므로 시험으로 인한 기기의 이용불능도는 분석하지 않았다.

보수에 의한 기기 이용불능도는 대기 모드에 있는 기기에 대하여 계산한다. 이러한 계통은 대개 과도 상태 또는 냉각재 상실 사고와 같이 발전소가 이상이 있을 때만 작동하는 공학적 안전설비 계통과 관련이 있는 기기들이다. 이런 기기들의 사용 가능성은 영광 5,6 기술 지침서 (Technical Specification)를 근거로 판단한다. 기술 지침서의 운전 제한 조건에서는 동시에 다중 트레인의 기기들을 보수하지 못하도록 규제한다. 정상 출력 운전하는 동안에는 운전 제한 조건 범주 밖의 기기나 시험 중에 있는 기기 혹은 고장이 발견된 기기에 한해서만 보수를 한다. 그러므로 비규칙적인 보수만이 계통 이용불능도에 영향을 준다.

보수 데이터 분석이 필요한 일반적인 계통과 기기들은 다음과 같다.

<u>분석 대상 계통</u>

- 보조 급수 계통
- 안전 주입 계통
- 화학 및 체적 제어 계통
- 전기 계통
- 격납건물 살수 계통
- 기기 냉각수 계통
- 필수 냉수 계통
- 필수 해수 계통
- 정지 냉각 계통
- 공기 조화 계통
- 계기용 공기 계통
- 비상 디젤 발전기 계통

<u>분석 대상 기기</u>

- 펌프
- 열 교환기
- 디젤 발전기
- 공기 압축기
- 공기 건조기
- 팬 (Fan)
- 건전지 충전기 (Battery Charger)

나. 보수에 의한 이용불능도 계산 방법

보수로 인한 기기의 이용불능도는 PSA Procedures Guide에서 사용한 방법을 이용하여 계산한다. 사용한 계산식은 다음과 같다.

$$Q_m = \frac{MTTR}{MTTF + MTTR} = M_f \cdot T_m$$

여기서,

Q_m = 보수에 의한 이용불능도,

MTTF = Mean time to failure,

MTTR = Mean time to Repair,

M_f = 1/(MTTF+MTTR) : Unscheduled maintenance frequency,

T_m = MTTR : Outage time due to maintenance.

위의 식을 사용해서 보수에 의한 이용불능도를 계산하기 위해서는 비규칙적인 보수 빈도와 MTTR을 알아야 한다.

다. 일반 자료원 선정

영광 5,6호기 발전소는 설계 단계에 있으므로 비규칙적인 보수 빈도와 outage time에 대한 발전소 자료가 없다. 그러므로 이에 관련된 데이터는 일반 자료원으로부터 인용하여 사용한다.

영광 5,6 호기의 비규칙적인 보수 빈도 분포로는 Oconee PRA (Table B-38 through B-42)의 보수 빈도 분포를 사용하였다. MTTRs 또한 Oconee PRA (Table B-43 through B-47)에서 유도된 MTTRs의 사전 분포를 통하여 도출하였다.

6. 문서화

신뢰도 데이터 분석 방법론, 개발 절차, 참고 문헌 및 가정 사항 등의 내용을 수록한다. 또한 데이터 베이스의 개정 기준, 관련된 불확실성 처리 등의 절차도 이 서류에 포함한다. 일반적으로 이 패키지는 각각의 업무에 따른 내용들을 이해하고 필요시 이를 검증할 수 있도록 충분한 정보를 포함하도록 작성해야 한다.

데이터분석을 수행한 결과로서 다음과 같은 내용을 문서화한다:

- 데이터 베이스 분석 방법론
- 개발 절차
- 기본 가정사항
- 참고 문헌

제6절 신뢰도 데이터 상세 분석 방법

1. 기기 신뢰도 데이터 분석

가. 개요

영광 5,6 발전소와 같이 설계 중인 발전소에 대한 고유 발전소 자료는 없다. 그러므로 영광 5,6호기 PSA에 사용한 기기 신뢰도 데이터는 일반 기기 고장율을 바탕으로 하여 개발하였다. 주로 사용한 일반 자료원은 "ALWR PRA Key Assumptions and Groundrules (KAG) of revision 7, 12/95 " 이다. 그러나 일반 기기 신뢰도 데이터는 데이터베이스 구축 시 여러 개의 자료원들과 비교 분석된다.

나. 분석 절차

(1) 대상 기기 목록 작성과 고장모드 정의

발전소의 여러 기기들 중 분석 대상기기를 파악하여 목록을 작성한다. 그러나 완벽한 기기 목록은 계통 분석이 완결된 후에 얻을 수 있으므로 다른 이용 가능한 유사 발전소의 PSA 결과를 검토하여 발전소의 일반 기기 목록을 작성한다.

이 단계에서 수행해야 할 일은 분석 대상 계통을 선정하여 대상 기기 목록을 작성하고 각 기기에 대한 고장모드를 정의하는 것이다.

분석 대상 계통

PSA 정량화를 위해 분석이 필요한 일반적인 계통은 표 26과 같다.

표 26. 영광 5,6호기 PSA에서 모델된 계통 명

계통 코드	계 통 이 름
HPSIS	고압안전주입계통 (High Pressure Safety Injection System)
SIT	안전주입탱크 (Safety Injection Tank)
LPSIS	저압안전주입계통 (Low Pressure Safety Injection System)
SCS	정지냉각계통 (Shutdown Cooling System)
CSS	격납건물살수계통 (Contament Spray System)
SDS	안전감압계통 (Safety Depressurization System)
CVCS	화학 및 체적제어계통 (Chemical and Volume Control

계통 코드	계 통 이 름
	System)
RCSPCS	원자로냉각재계통 압력제어계통 (RCS Pressure Control System)
AFWS	보조급수계통 (Auxiliary Feedwater System)
MFWS	주급수계통 (Main Feedwater System)
MSS	주증기계통 (Main Steam System)
SGBS	증기발생기취출계통 (Steam Generator Blowdown System)
EPS	전력공급계통 (Electric Power System)
DG	디젤발전기 (Diesel Generator)
CCWS	기기냉각수계통 (Component Cooling Water System)
ESWS	필수용수계통 (Essential Service Water System)
ECWS	필수냉수계통 (Essential Chilled Water System)
HVAC	공기조화계통 (Heating, Ventiation and Air Conditioning)
IAS	압축공기계통 (Instrurmnt Air System)
ESFAS	공학적안전설비계통 (Engineered Safety Features Actuation System)
RPS	원자로보호계통 (Reactor Protection System)

<u>분석 대상 기기</u>

분석 대상 계통이 결정되면 이에 대한 계통 고장수목을 구성하게 되며 이 과정에서 필요한 분석 대상 기기를 선정하고 필요한 부품 약어를 결정하게 된다. 영광 5,6호기 PSA에서 사용한 대상 기기 및 부품 약어는 표 27과 같다.

표 27. 영광 5,6호기 PSA에서 사용된 부품 명

부 품 약 어	부 품 이 름
MV	Motor Operated Valve
AV	Air Operated Valve
CV	Check Valve
VV	Manual Valve
LV	Solenoid Valve
RV	Relief Valve
SV	Safety Valve
EV	Electro Hydrulic Operated Valve

부 품 약 어	부　　품　　이　　름
XV	Other Valves
MP	Motor Driven Pump
DP	Diesel Driven Pump
DG	Diesel Generator
AC	Air Compressor
AB	Blower / Ventilation Fan
AU	Air Handling Unit / Air Cleaning Unit
AD	Air Dryer
AS	Air Separator
CQ	Cubicle Cooler
CU	Chiller Unit
FL	Filter / Strainer
FE	Flow Element / Orifice
NZ	Nozzles
DM	Dampers
TK	Tanks
PI	Piping
HX	Heat Exchanger (Including Steam Generator)
CD	Condenser
TB	Turbine
HT	Heater
HR	Heat Tracing
BY	Battery
BC	Battery Charger
HB	Circuit Breaker (around 4 KV)
LB	Circuit Breaker (around 600V)
RB	Reactor Trip Breaker
FS	Fuse
XH	Transformer (High Voltage)
XM	Transformer (4 KV to 600 / 408V)
XL	Transformer (Low Voltage)
SP	Sump

부 품 약 어	부　품　이　름
GD	Grid
SY	Switchyard
BS	Bus
LC	Load Center
MC	Motor Control Center
PN	Distrbution Panel
CR	Converter
IR	Inverter
VR	Voltage Regulator
FT	Flow Transmitter
PT	Pressure Transmitter
TT	Temperature Transmitter
LT	Level Transmitter
PW	Pressure Switch
VW	Level Switch
MW	Manual Switch
QW	Torque Switch
LW	Limit Switch
TW	Temeprature Switch
SW	Other Switch
CA	Cable
CO	Coil
AL	Alarm
AN	Annunciator
ID	Indicator
BI	Bistable
RY	Relay
SQ	Sequencer
CP	Capacitor
DI	Diode
RS	Resistor
IK	Interlock

부 품 약 어	부　품　이　름
CK	Control Circuit
SK	Actuation Signal Generating Circuitry
FW	Flow Switch
OP	Operator Action

<u>고장 모드 정의</u>

고장 모드는 일반적으로 세 가지 즉, 대기 중 고장, 운전 중 고장 그리고 작동 요구 시 고장으로 나누어진다. 이러한 정의는 일반 데이터에 반영되어 있는 고장 데이터의 형태와 계통 모델링에서 고려되는 기기의 고장 모드를 동시에 표현하고 있다. 영광 5,6호기 고장 수목 분석 시 사용한 고장 모드는 표 28과 같다.

표 28. 영광 5,6호기 PSA에서 사용된 기기 고장 모드

약　　어	고　장　모　드
S	Fails to Start
R	Fail to Run / Continue Operating
O	Fail to Open
C	Fail to Close
T	Transfer Closed
G	Fail to Reclose / Reseat
P	Plugged
L	Leakage (Reverse / Internal)
B	Leakage (External) / Rupture / Break
Y	Fails While Operating / Fails to Maintain Output
A	Fails to Provide Output / Fail to Actuate / Generate Actuation Signal
I	Spurious Operation
M	Unavailable Due to Test / Maintenance
H	Operator Error to Perform a Task / Operator Inadvertant Action
V	Operator Recovery Action Failure
U	Operator Fails to Restore After T&M
X	Eletrical Short

약 어	고 장 모 드
N	Open Circuit
E	Fails to Energize
D	Fails to Deenergize
F	Failure (General)
W	Common Cause Failure (Demand)
K	Common Cause Failure (Operating)
Z	Modularized Event

(2) 기기 경계 정의

기기의 물리적 경계를 결정하여 기기 고장을 정의한다. 이 물리적 경계는 분석 수준에 따라 보조 기기, 제어 기기, 전기 기기 등과의 상관관계 (coupling mechanism)와 관련하여 결정되며 어느 정도는 데이터의 이용 가능성에 의해서도 결정된다. 물리적 경계의 결정은 주요 밸브, 펌프 및 디젤발전기에 대해서 뿐만 아니라 제어계통 분석 대상 블랙박스 주위에 대해서도 명확히 설정한다. 기기 경계의 예는 표 29와 같다.

표 29. 기기경계의 예

기기	기 기 경 계
Motor Operated Valve	Includes the valve body, all its internal parts, valve operator(motor), attached functional accessories such as limit and torque switches and exclusive of external support systems. (DC, AC power, and control signal)
Solenoid Operated Valve	Includes the valve body, all its internal parts, valve operator(solenoid), attached functional accessories, and exclusive of external support systems (DC power, and control signal)
Air Operated Valve	Includes the valve body, all its internal parts, valve operator, internal solenoid valve, attached functional accessories, and exclusive of external support systems (Instrument Air, DC power and control signal)
Check Valve (other than stop check)	Includes the valve body and all its internal parts
Stop Check Valve	Includes the valve body, all its internal parts, and valve operator
Manual Valve	Includes the valve body, all its internal parts, and valve operator (human errors not included)
Pressurizer Safety Valve	Includes the valve body and all internal parts
Electro-Hydraulic Operated Valve	Include the valve body, all its internal parts, valve operator, attached functional accessories, system systems relating hydraulic pressure such as hydraulic pressure generation pump, reservoir, accumulator, and

기기	기 기 경 계
	exclusive of external support systems (AC or DC Power, Instrument Air, and control signal)
Motor Driven Pump	Includes the motor, pump, circuit breaker, self-contained lubricating system, and exclusive of external support systems (AC, DC power, HVAC, and control signal)
Turbine Driven AFW Pump	Includes the turbine, circuit breaker, turbine control system, pump internals and exclusive of external support systems (DC power and control signal)
Air Compressor	Includes compressor, and motor exclusive of external support systems (AC, DC power, and cooling, control signal)
Blower or ventilation fan	Include fan and motor, exclusive of external support systems (AC,DC Power)
Room Chiller Unit (Essential Chiller)	Includes compressor, evaporator, condenser, internal cooling system, and exclusive of external support system (AC, DC power, cooling water, control signal)
Diesel Generator	Includes the diesel engine, generator, air start motor air receiver tanks, output breaker, internal cooling system, fuel oil system, and associated control circuitry exclusive of external support systems (Cooling water, DC power, HVAC)
Circuit Breaker (4KV)	Includes breaker mechanism, charging motor and controls local breaker open/close contact and exclusive of external support systems (DC or AC control power, HVAC, etc.)
Circuit Breaker (600V)	Includes the breaker mechanism, local open/close contact, and exclusive of external support systems (DC or AC control power, HVAC, etc.)

(3) 기기 고장확률 분류 및 평가 방법 선정

계통 고장수목과 사고경위 정량화를 위해서는 다음과 같이 두 가지 종류의 기기 고장확률이 필요하다.

- 이용불능도 (unavailability) - 기기가 대기 상태에서 작동이 요구될 때 작동을 하지 못할 확률
- 신뢰도 (Unreliability or reliability) - 기기가 성공적으로 작동한 후 주어진 시간 동안 지속적으로 운전되지 못할 확률

기기 이용불능도는 작동 실패율을 가지고 계산할 수 있다. 작동 실패는 기기가 어떤 상태를 바꾸거나 기동 요구에 대한 작동 실패를 의미한다. 일반적인 작동실패의 예를 들어보면 다음과 같다 ;

- 펌프 작동 요구 시 펌프의 기동 실패

- 필요 시 공기구동 밸브의 개방 실패

고장 데이터가 작동 요구에 대한 실패 확률이라면, 그 값은 기기의 이용불능도이다. 그러나 일반 데이터원 중에는 단위시간에 대한 기기 고장율로 데이터가 주어진다. 이런 경우에는 다음의 계산식으로 기기의 이용불능도를 추정한다.

$$U = \frac{1}{2}\lambda T$$

여기서,

U: 작동 요구에 대한 기기의 고장확률 (이용불능도)

λ: 단위 시간당 고장율

T: 대기시간 (hours)

반면 기기의 unreliability는 기기의 가동 중 고장율을 바탕으로 계산된다. 가동 중 고장이란 기기가 성공적으로 작동한 후 주어진 기간 동안 가동하는데 실패하는 고장으로서, 일반적인 예는 다음과 같다.

- 펌프가 임무 수행 시간 (mission time) 동안 성공적으로 운전하는데 실패

이런 종류의 고장모드에 대한 고장 데이터는 단위 시간당 고장 확률에 근거하여 계산한다. 기기 unreliability 는 운전 중 고장율과 임무 수행 시간을 이용하여 다음 식으로 계산한다.

$$P = \lambda T$$

여기서,

P: 임무 수행 시간 동안의 기기 고장 확률

λ: 단위 시간 당 기기 가동 고장율

T: 임무 수행 시간

(4) 일반 기기 신뢰도 데이터 베이스 개발

다양한 일반 데이터원은 유사 기기 및 고장 모드에 대해 서로 다른 추정치를 가지는 경우가 많다. 또한 데이터원들은 각각 다른 기기 경계를 가지는 경우도 있다. 따라서 적절한 일반 데이터 추정치를 결정하기 위해서는 각각의 데이터원에 대한 분석과 분석가의 판단이 필요하다. 설계 중인 발전소는 운전이력이 없으므로 PSA 정량화를 위해 일반 고장율을 바탕으로 하여 일반 기기 신뢰도 데이터 베이스를 개발해야 한다. 영광 5,6

호기 PSA 수행을 위해 개발된 일반 기기 신뢰도 데이터의 주된 일반 자료원은 "ALWR PRA Key Assumptions and Groundrules (KAG) of revision 7, 12/95"와 NUREG/CR-4639이다. 그러나 선정된 기기의 각 고장 모드에 대한 데이터가 적절하지 않은 경우에는 두 자료원 이외의 자료원을 참고로 하여 일반 기기 신뢰도 데이터 베이스를 개발하였고, 다음의 분석 단계를 거쳐 평가하였다.

- 1 단계 : 일반 기기 신뢰도 데이터 베이스 구축을 위해 여러 개의 고장 데이터 자료를 검토한다. 검토된 자료는 이전의 PSA 보고서, LER (License Event Report) 자료 등의 자료로 구한 데이터 베이스들이다.
- 2단계 : 각 데이터 베이스의 고장율에 포함된 기기 경계를 확인한다.
- 3단계 : 모든 일반 데이터원 중에서 가장 대표적이라고 판단되는 값을 선정한다. ALWR PRA KAG 자료는 일반 자료원과 특정 발전소 자료도 포함하고 있는 대표적인 자료원이다.

ALWR PRA KAG 자료에서 값을 제시하고 있지 않거나 인용하기 곤란한 몇몇 기기들에 대해서는 다른 일반 자료원으로 부터 값을 인용하였다. 경우에 따라서는 간단한 기하 평균 기법을 이용하여 여러 개의 자료원을 결합하였다. 이런 일련의 과정을 거쳐 얻은 일반 기기 신뢰도 데이터는 각 기기의 고장모드에 대한 Data worksheet로 정리한다. Data worksheet의 예제 형태는 다음과 같다.

PSA DATA WORKSHEET

Event ID: AVO

System: ______, N/A

Component: AV, air operated valve

Failure Mode: O, fails to open

❑ **Description:**

Air operated valve ##### fails to open (generic component)

❑ **Event Type *(Check One)*:**

___	Random-operating;	X	Random-demand;
___	CCF-operating;	___	CCF-demand;
___	Diamond Event-operating;	___	Diamond Event-demand;
___	Initiating Event;	___	Human Error;
___	Test/Maintenance Unavailability;	___	Special Event;
___	Other (describe below);		

❑ **Event Boundary *(if necessary)*:**

❑ **Calculation Summary:**

	Value Selected	*Prominent Sources*
Mean:	2.0E-3/d	EPRI ALWR KAG(Ref.1)
Error Factor:	15.38	NUREG/CR-4639 (Ref.2)
5th Quantile:		
50th Quantile:		
95th Quantile:		

❑ **Source References:**

1. EPRI ALWR URD PRA KAG, Vol.2, Chapter. 1, App.A, Rev.7, 12/95.
2. NUREG/CR-4639, Vol.5, Part 3, Rev.3, 12/90 (NUCLARR).

PSA DATA WORKSHEET

❑ **Calculation** ***(use additional sheets if needed)*:**

The mean failure rate (per demand) was taken directly from the EPRI ALWR KAG (Reference 1). The original failure mode was "air operated valve fails to operate (open or close)". The EPRI ALWR KAG reflected generic data sources (e.g., NUREG/CR-4550, NUREG/CR-1363, Oconee PRA, Seabrook PSS) as well as five plant specific evidences (total 6,762 demands; 42 failures).

The EPRI ALWR KAG does not provide error factors. Therefore, the error factor was calculated using the data for "air operated valves, fails to operate group" in NUREG/CR-4639 (Reference 2) as follows.

Error Factor = 95th quantile / Median

= (6.0e-3/d) / (3.9e-4/d)

= 15.38

2. 공통원인고장 데이터 분석

공통원인고장 사건은 MGL (Multiple Greek Letter) 방법을 사용하여 모델 한다. MGL 방법은 기기고장 사건을 하나의 독립적 사건과 여러가지 공통원인고장 사건으로 나눈다. 각 공통원인고장 사건은 크기 m인 공통원인 기기 군에 대하여 다음과 같이 표현될 수 있다.

m : 독립사건 수

$_mC_2$: 2 개의 특정 기기를 포함하는 공통원인고장 사건 (double CCF)

.

$_mC_k$: k 개의 특정 기기를 포함하는 공통원인고장 사건 (k-tuple CCF)

.

$_mC_m$: 모든 m 개의 기기를 포함하는 공통원인고장 사건 (m-tuple CCF)

고장수목과 사고경위의 정량화를 위해서 위 공통원인고장 사건의 확률을 평가해야 한다. MGL 방법에서는 평가의 단순화를 위해서 대칭(symmetry) 가정이 적용된다. 대칭 가정에 의하면 유사한 유형의 기기가 포함된 유사한 기본사건의 확률은 같다. 공통원인 기기군 내의 어떠한 주어진 기본사건의 고장확률은 그 기본 사건의 특정기기에 의존하는 것이 아니라 조합의 수에만 의존한다.

따라서 모든 k-tuple 공통원인고장사건은 다음과 같은 동일 확률을 가질 것이다.

$Q^{(m)}_k$:크기 m인 공통원인 기기군에서 k (k = 1, 2, ..., m) 개의 특정 기기가 포함된 기본 사건 확률.

만약 m이 n과 같지 않다면 일반적으로 $Q^{(m)}_k$ 는 $Q^{(n)}_k$ 와 같지 않기 때문에 공통원인 기기군의 크기에 의존하는 기기 유형에 대하여 $Q^{(m)}_k$ 의 여러 가지 다른 집합이 존재할 수 있다. MGL 방법은 총 (m-1)개의 변수를 정의하고 추가로 크기 m인 공통원인기기 그룹의 $Q^{(m)}_k$ 를 평가하기 위해서 총 기기실패확률 Q_t에 대한 확률을 정의한다. MGL 변수는 같은 기기군 내의 다른 기기들과 공유할 수 있는 기기의 모든 가능한 공통원인고장확률 경로에 대한 조건 확률이다. 예를 들어, 크기 3인 기기군의 MGL 변수는:

β = 한 특정기기가 실패했을 때, 기기고장의 원인이 하나 이상의 추가 기기에 공유될 수 있을 조건 확률이다. 그리고,

γ = 2 개의 특정 기기가 실패했을 때, 하나 이상의 기기에 공유된 기기 고장의 원인이 두개 이상의 추가 기기에 공유될 수 있을 조건 확률이다.

$Q^{(m)}{}_k$ 의 확률은 Q_t 및 MGL 변수를 사용하여 다음 식으로 계산한다:

$$Q^{(m)}{}_k = \frac{1}{{}_{m-1}C_{k-1}} \prod_{i=1}^{k} \theta_i (1-\theta_{k+1}) Q_t \qquad (1)$$

이 때 k = 1, 2, ..., m

여기서

θ_i (i = 1, 2, ..., m+1)

= MGL변수 (θ_1=1, θ_2=β, θ_3=γ, ..., θ_{m+1}=0)

Q_t : 전체 기기 고장확률

m : 공통원인고장 군에서 특정기기가 포함된 기본사건 확률

$Q^{(m)}{}_k$ 의 평가를 위해서 Q_t 및 MGL변수를 평가해야 한다.

공통원인고장 경험 데이터에 기초하여 MGL 변수를 평가한다. MGL 변수를 계산하기 위한 식은 다음과 같다.

$$\theta_i = \sum_{k=i}^{m} k \cdot n_k \Big/ \sum_{k=i-1}^{m} k \cdot n_k \quad ,\text{for } i = 2, 3, ..., m \qquad (2)$$

여기서

θ_i for i = 2, ..., m : MGL변수 (θ_1=1, θ_{m+1}=0)

n_k : k개 기기가 포함된 고장 사건의 수

n_k에 대한 값은 공통원인고장 경험자료에 기초하여 평가된다. EPRI-NP-3967과 NUREG/CR-1363 은 경험자료의 주요 자료원이다. 모든 공통원인고장의 적용성을 결정하고 기기에 대한 영향을 식별하기 위해서 위 참고문헌의 모든 사건을 검토하여야 한다. 공통원인 기기군의 크기는 참고문헌의 대상 발전소마다 다르기 때문에 특정군 크기에 대한 적절한 경험자료 집합을 만들기 위해서 매핑(mapping) 과정을 수행한다.

공통원인고장 분석을 위해 평가된 MGL 변수를 표 30에 요약하였다. 식 (2)을 사용하여 얻은 MGL 변수값으로서 공통원인고장사건의 확률을 계산하는데 사용한다. 경험자료를

이용할 수 없는 기기에 대해서는 NUREG/CR-4780에 기술되어 있는 일반적인 값에 기초하고, 해석 중에 식별된 다른 기기에 대해서는 MGL 변수의 경향에 기초하여 가정하였다. 일반적인 값은 NUREG/CR-4780 의 0.1로 가정하였다. β와 다른 MGL 변수는 대부분의 경우 0.5 와 0.99 사이로 평가한다. β와 다른 값이 1.0에 근접하면 모든 기기를 포함하는 공통원인고장사건의 확률은 극히 일부 기기를 포함하는 공통원인고장 사건의 확률에 좌우된다.

따라서 β와 다른 MGL 변수에 대해서 높은 값을 가정하면 고장수목 정량화 결과는 보다 더 보수적이 될 것이다. 본 해석에서는 MGL 변수 평가에 대해서 이용할 만한 경험자료가 없을 경우, β와 다른 모든 MGL 변수는 위의 논의에 기초하여 보수적으로 0.9로 가정하였다. 제 2 장에서 언급한 바와 같이 상위계통 고장수목에서와 보조계통 고장수목에 있어서 4대의 기기들 보다 많은 기기군들에 대해서만 계통수준 공통원인고장사건 접근법을 사용한다. 직접적으로 계통실패를 초래하는 공통원인 고장사건의 확률을 합함으로써 계통수준 공통원인고장 사건의 확률을 계산한다.

예를 들어, 고압안전주입계통 주입관에는 8 개의 유동 격리 전동구동밸브가 있다. 만약 중형 냉각재상실사고가 4개의 저온관 중의 하나에서 발생한다면 고압안전주입계통은 저온관에 연결된 3개의 주입관 중에서 적어도 2개의 주입관으로 재장전수를 주입해야만 한다.

파손된 저온관으로의 유동은 가능하지 않은 것으로 간주한다. 공통원인 기기군 크기는 요구 시 개방해야 하는 격리밸브가 8개이므로 계통수준 공통원인고장 사건 접근법을 사용하고, 또한 격리밸브의 계통수준 공통원인고장의 확률은 아래에서 설명한 방법으로 계산하게 된다. 각 주입관에는 2개의 격리밸브가 있다. 하나는 펌프 트레인 A에 있고 다른 하나는 펌프 트레인 B에 있다. 주입을 위해 격리밸브를 열어야 한다. 파손된 저온관으로의 주입은 파손된 부위로 배출된다고 가정하기 때문에 파손된 저온관에 관계된 2개의 밸브 상태는 계통 성공에 영향을 주지 않는다. 성공기준에 따르면 주입시 최소한 2개의 주입관은 이용 가능해야만 한다.

계통 성공기준에 부합하기 위해서 주입관에 있는 2개의 밸브라인 중에서 하나는 관련된 주입라인에서 요구하는 충분한 유량이 형성할 수 있어야 하기 때문에 파손된 저온관과 관련이 없고 다른 주입관에 위치한 최소한 2 개의 격리밸브를 열어야 한다. 따라서 8개의 밸브가 동시에 고장을 일으키는 공통원인고장 사건과 7개의 밸브가 동시에 고장을 일으키는 공통원인고장 사건은 직접적으로 계통 실패를 초래한다.

그러나 6개, 5개 또는 4개의 밸브가 동시에 고장을 일으키는 공통원인고장 사건은 단지 기기 실패의 특정 조합이 발생할 수 있는 경우에만 직접적으로 계통실패를

초래할 수 있다. 3개 및 2개의 밸브가 동시에 고장을 일으키는 공통원인고장 사건은 직접적으로 계통 실패를 초래할 수 없다. 공통원인고장 사건의 조합과 최소한 하나의 독립사건을 무시할 수 있음으로써 저온관에서의 중형 냉각재상실사고의 경우에는 고압안전주입 격리밸브의 계통수준 공통원인고장 사건의 확률은 다음 식으로 계산한다.

$$Q_{ccf} = 3Q^{(8)}_4 + 12Q^{(8)}_5 + 16Q^{(8)}_6 + 8Q^{(8)}_7 + Q^{(8)}_8 \qquad (3)$$

여기서

Q_{ccf} : 고압안전주입 격리밸브의 계통수준 공통원인고장 확률.

$Q^{(8)}_k$: k-tuple 공통원인고장 확률.

$Q^{(8)}_k$ 의 계수는 직접적으로 계통 실패를 초래하는 기기의 특정 조합의 숫자인 점을 주의해야 한다.

표 30. 공통원인고장 분석에서 사용된 MGL 변수 (1/3)

Component	Failure mode	Redundancy	Parameters		Remark
SI Pump	Fail to start	2	β	0.0890	High head pumps (HPSI and CVCS charging pumps)
		3	β	0.0782	
			γ	0.5826	
		4	β	0.0710	
			γ	0.8503	
			δ	0.3622	
	Fail to run	2	β	0.0710	
		3	β	0.0695	
			γ	0.9534	
		4	β	0.0688	
			γ	0.9965	
			δ	0.9042	
CS Pump	Fail to start	2	β	0.0917	
	Fail to run	2	β	0.0917	
AFW Pump (MDP)	Fail to start	2	β	0.0797	
	Fail to run	2	β	0.0030	
AFW Pump (TDP)	Fail to start	2	β	0.0797	
	Fail to run	2	β	0.0030	
ESW/CCW Pump	Fail to start	2	β	0.1201	including ECW pump
		4	β	0.1749	
			γ	0.9974	
			δ	0.9306	
	Fail to run	2	β	0.0470	
		4	β	0.0480	
			γ	0.9625	
			δ	0.9896	
LPSI Pumps	Fail to start	2	β	0.0593	
	Fail to run	2	β	0.0800	

표 30. 공통원인고장 분석에서 사용된 MGL 변수 (2/3)

Component	Failure mode	Redundancy	Parameters		Remark
Motor Operated valve	Fail to operate (open or close)	2	β	0.0736	CCF of AFWS isolation MOVs(4); a) Between AC motor drivers(2), or Between DC ones(2) β=0.0752 b) CCF between valve body 1) For three redundancy β=0.0710, γ=0.977 2) For four redundancy β=0.0705, γ=0.998, δ=0.947
		3	β	0.0734	
			γ	0.9712	
		4	β	0.0731	
			γ	0.9980	
			δ	0.9477	
		6	β	0.0732	
			γ	0.9930	
			δ	0.9962	
			ε	0.9839	
			ζ	0.9201	
		8	β	0.0701	
			γ	0.9925	
			δ	0.9974	
			ε	0.9970	
			ζ	0.9926	
			η	0.9737	
			θ	0.8971	
Solenoid Operated Valve	Fail to operate (open or close)	2	β	0.0594	
		3	β	0.0579	
			γ	0.9429	
		4	β	0.0571	
			γ	0.9957	
			δ	0.8821	
Air Operated Valve	Fail to operate (open or close)	2	β	0.0653	
		3	β	0.0720	
			γ	0.7778	

표 30. 공통원인고장 분석에서 사용된 MGL 변수 (3/3)

Component	Failure mode	Redundancy	Parameters		Remark
Air Operated Valve	Fail to operate (open or close)	4	β	0.0740	
			γ	0.8892	
			δ	0.7356	
		8	β	0.0712	
			γ	0.9965	
			δ	0.9735	
			ε	0.9271	
			ζ	0.8964	
			η	0.8829	
			θ	0.7373	
Check Valve	Fail to operate (open or close)	2	β	0.0104	Applicable for swing check v/v
DG (between Emergency DGs)	Fail to start	2	β	0.0170	
	FTR	2	β	0.0500	
DG (between Emergency DGs and AAC DG)	Fail to start	3	β	0.0097	
			γ	0.9944	
	FTR	3	β	0.0883	
			γ	0.9423	
Batteries	Fail to provide output	2	β	0.0427	
		3	β	0.0533	
			γ	0.6000	
		4	β	0.0640	
			γ	0.5000	
			δ	1.0000	
		5	β	0.0640	
			γ	0.5000	
			δ	1.0000	
			ε	1.0000	
Others	all modes		β	0.1000	Higher parameters assume to be 1.0 if needed

3. 인간신뢰도 데이터 분석

본 절차서는 ASEP(Accident Sequence Evaluation Program) 인간신뢰도분석(Human Reliability Analysis : 이하 HRA) 및 THERP(Technique for Human Error Rate Prediction) 방법을 기본으로 하고 있으며, 설계중 원전 PSA의 HRA 수행 절차서로 만들어졌다. 분석 방법 및 절차는 전체적으로 ASEP 방법을 따랐으나 그간의 HRA 수행 경험을 바탕으로 일부 정량화 규칙을 세분화 하였다. PSA 예비분석 단계를 위한 선별분석(Screening Analysis)은 실제 PSA 수행 절차에 맞추어 보다 간단한 방법을 적용하였으며, 과거 PSA 수행 경험 및 데이타베이스를 바탕으로 가능한 상세분석(Nominal Analysis)을 직접 수행하기 위한 절차를 만들었다. 본 절차서는 설계 중인 원전의 PSA 전출력 내부사건분석에서 고려하는 인간오류를 분석하기 위하여 작성하였으며, 영광 5,6 호기 PSA의 HRA에 적용하였다.

PSA는 그 수행 목적 및 대상 발전소의 상태에 따라 분석의 초점과 수준, 그리고 분석 범위가 달라진다. 이런 관점에서 설계나 건설 중인 발전소에 대한 PSA는 운전 중인 발전소의 PSA와 같지 않으며, 인허가 및 규제 만족을 위한 PSA가 발전소의 설비 개선이나 관리 최적화를 위한 PSA와 같을 수 없다. 따라서, HRA 역시 대상 PSA의 목적과 수준에 따라 분석 방법이나 범위가 달라진다. 설계나 건설중인 원전 PSA는 대상 원전의 안전성 수준을 입증하고 발전소가 균형적으로 설계되었는지를 평가하는 것이 주 목적이며, 설계 단계에서 안전성을 종합적으로 평가하여 설계 취약점을 발견하고 이를 개선하기 위하여 수행한다. 따라서, PSA가 Best-Estimation Approach이지만 설계 중 PSA에서는 보다 보수적인 접근 방법이 적용된다. 본 절차서는 설계나 건설 중 원전 PSA에 대한 HRA 수행 절차서로서, PSA 수행 목적과 분석 수준을 고려하여 ASEP HRA 방법을 기본 분석 방법으로 채택하였다.

ASEP HRA 방법은 THERP 방법을 간략히 개정한 것으로서, THERP 방법론에 대해 그 동안 제기되었던 많은 의견을 고려하여 만들어졌다. THERP에 대해 제기된 의견중 ASEP 방법 개발시 주로 고려한 것들은 다음과 같다. 첫째, 방법이 너무 복잡하고 적절한 지침이 없어 분석 결과가 분석자에 따라 너무 다를 수 있다. 둘째, HRA 수행에 많은 경험을 필요로 하고 분석에 시간이 많이 소요된다. 따라서, ASEP HRA 방법은 보다 간단한 framework과 절차를 만드는데 초점을 맞추었으며, HRA자가 아닌 계통분석자가 이용할 수 있을 정도로 단순한 적용 규칙을 기본으로 하고 있다. 단순화하는 대신 기본적으로 사용하는 데이타는 상당히 보수적으로 설정하였다.

THERP를 간략화한 ASEP HRA 방법은 THERP을 원칙적으로 적용할 때 보다는 결과가 보수적으로 나올 수 있다. 그러나, THERP 자체도 적용하는 수준이 분석자나 과제 목적에

따라 상당한 차이가 있을 수 있으므로, ASEP 방법이 항상 보수적이라 말할 수는 없다. 또한 본 절차서가 ASEP HRA 방법을 기본으로 하고 있지만, 일부 분석 절차 및 적용 규칙을 개정하고 세분화하여 너무 보수적인 결과 도출을 지양하고 있다.

가. 직무 구분 및 오류 분류

PSA에서 고려하는 인간오류는 원전에서 수행되는 인간직무(human task)를 대상으로 한다. PSA 대상이 되는 인간직무에는 시험 및 보수 작업, 운전을 위한 직무, 사고 시 운전원의 대응 조치나 복구 조치가 포함된다. 즉, 사고 발생 시점 이전에 정상 운전 상태에서 운전이나 시험, 보수를 위해 수행되는 직무와 사고 발생 후 사고를 종결 또는 완화시키기 위해 수행하는 직무로 구분할 수 있다.

인간이 작업을 수행하는 과정은 사고 발생 시냐 평상 운전 중이냐에 따라 다를 수 있다. 평상 운전중의 작업인 경우는 사전 계획에 의하여 작업을 시작하며, 대부분의 경우 절차서를 사용하여 구체적인 작업을 수행하게 된다. 이때는 운전원이나 작업원이 사전에 작업의 목적, 방법 및 필요한 조건이 무엇인지를 알고 있는 상태이고, 수행 경험이 많은 작업이므로 인식/진단단계에서의 오류는 거의 발생하지 않는다. 반면 작업이 사고 발생시 복구조치와 관련된 작업이라면 평소에 익숙치 않은 사고 상황을 판단하고 경험과 지식에 근거하여 대응 조치를 결정해야 된다. 이런 작업에서는 인식/진단단계가 특별히 중요하며 경우에 따라 많은 시간을 필요로 하게 된다. 복구조치와 관련된 작업에서의 실패 중의 많은 경우는 사고 상황에 대한 인식/진단의 실패에 기인하는 것으로 분석되고 있다. 또한 행위에 영향을 미치는 여러 환경 인자가 사고 시와 평상시가 다르기 때문에 인간오류를 평가하는 절차가 구분되어져야 한다.

본 HRA 절차서에서는 상기 기술한 배경에 의해 인간오류를 사고 발생 시점을 기준으로 구분하는 방식에 따라 다음과 같이 분류하고 각각에 대한 분석 절차를 수립하였다.

- 사고 전 인간오류 (pre-accident human error) : 검사, 보수 및 보정 작업 수행단계에서 발생하는 인간오류
- 사고 후 인간오류 (post-accident human error) : 사고 발생 후 운전원 조치 단계에서 발생하는 인간오류

사고 전 인간오류는 주로 검사, 보수, 검침 작업시 발생하는 인간오류로 원자로 정지를 직접 유발하거나 초기사건을 유발시키지는 않지만 관련 계통이나 트레인이 이용불능 상태로 만든다. 이 중 원자로 정지를 유발하는 인간오류는 초기사건 빈도에 포함되므로 HRA에서는 별도로 분석하지 않는다. 사고 전 인간오류의 전형적인 예로는 검사나 보수작업 후에 밸브를 원래 위치로 환원시키지 않아 관련 계통을 이용불능

상태로 만드는 인간오류가 있다. 사고 후 인간오류는 사고가 발생한 후 절차서에 따라 발전소를 안전한 상태로 유도하는데 필요한 운전원 직무 수행 중 발생하는 오류로서, 필요한 절차를 누락하거나 자동 작동 실패한 안전계통을 수동으로 작동시키는데 실패하는 오류 또는 고장 난 기기를 제한 시간 내에 복구하지 못하는 사건 등이 대표적 사건들이다.

두 인간오류 유형에 따라 분석 절차가 달라지는 것은 위에서 언급한 것처럼 상황을 인식/진단하는 과정이 작업의 성패에 미치는 영향이 다르다는 점이다. 검사 및 보수작업은 계획된 작업을 수행하는 것이며 경험이 많은 작업이므로, 사고 전 인간오류는 인식/진단과정에서의 오류 가능성이 무시할 만하다 가정하여 이 단계에 대한 평가는 생략하고 반응단계에서의 오류만 평가한다. 반응단계인 수행오류에 대한 평가는 세분화된 동작 평가에 알맞은 THERP를 이용하였다. 반면 사고 후 인간오류는 이상사태 발생 후 복구조치 단계에서 일어나는 인간오류로서, 많은 정보를 처리하여 상황을 판단하고 대응 방법을 선택하는 인식/진단하는 과정이 상대적으로 매우 중요하다. 따라서, 사고 후 인간오류는 진단과정에 대한 평가와 수행단계에 대한 평가를 각각 수행하여 오류 가능성을 분석한다.

나. HRA 분석 과정 및 수행 절차

HRA는 PSA 수행 과정에 맞추어 반복적으로 수행된다. HRA에는 소요 되는 자원은 분석 수준에 따라 상당히 달라진다. 따라서 모든 인간오류를 필요 이상으로 상세히 분석하지는 않는다. PSA 업무 과정에 맞추어 여러 단계의 HRA가 수행되며 초기에는 보수적인 인간오류 값을 간단히 사용하여 분석한 후, 어떤 인간오류가 PSA 전체 결과에 큰 영향을 주는지를 근거로 상세 분석 대상을 선정한다. 본 절차서에서는 이런 HRA 수행과정을 편의에 따라 선별분석과 상세분석으로 구분하였다. 일반적으로 선별분석은 PSA 초기분석단계에서 제한된 정보를 바탕으로 간단히 보수적으로 인간오류를 평가하는 것이며, 상세분석은 선별분석에서 선정된 인간오류에 대해 최종 설계단계의 상세한 정보를 근거로 분석하는 것이다.

선별분석에도 다양한 수준이 있을 수 있으나, 본 절차서에서 언급하는 선별분석은 사용하는 인간오류 값이 매우 보수적이어서 계통이나 사고경위에 대한 의미 있는 분석결과를 얻는 데는 부적절하다. 본 절차서에서 언급하는 선별 분석은 계통이나 사고경위에 대한 의미 있는 분석결과를 얻기 위한 것이 아니라, 사고경위 정량화의 절차 확인 및 HRA 상세 분석을 필요로 하는 인간오류 사건을 파악하는 목적으로만 사용한다. PSA 예비분석에 사용할 정도의 HRA 결과는 상세 분석 절차를 따르되, 분석시점까지 이용 가능하지 않은 자료는 기 수행된 PSA의 분석 자료나 전문가 판단 중 보수적 데이타를

사용한다. 예비 PSA 분석이 완료되면 이를 근거로 보다 상세한 분석이 수행될 인간오류를 선정하고, 동일한 KAERI 상세 분석 절차를 따르되 대상 작업 및 사고경위에 대한 보다 구체적 정보를 사용하여 정량화한다. 필요에 따라서는 이 단계에서 THERP 상세분석 절차를 따라 분석을 수행할 수 있다.

HRA 수행 절차로는 A.D. Swain 에 의하여 개발된 THERP (Technique of Human Error Rate Prediction) 기법과 Hannaman 이 개발한 SHARP (Systematic Human Action Reliability Procedure) 방법이 있다. 두 방법 모두 원전운전과 관련된 인간의 작업성능 평가를 PSA 수행과 연계하여 체계적인 방법으로 수행할 수 있도록 개발되었으며 두 방법 모두 비슷한 절차를 포함하고 있다. 일반적인 HRA 수행 절차는 그림 19와 같으며, 주요 업무 수행 단계는 다음과 같으며, PSA와 연계하여 반복적으로 수행한다.

- 인간오류 정의 (Definition) : 관련자료 수집과 PSA모델과의 연계 분석을 통하여 운전 및 보수, 사고시 직무와 관련된 인간 직무의 파악 및 주요 인간오류 선정
- 직무분석 (Task Analysis) : 선정된 인간오류에 대한 직무분석을 통하여 대상 직무에 대한 상세 정보수집 및 분석
- 표현 (Representation) : 직무분석 결과를 적용하고자 하는 모델에 알맞는 형태로 표현
- 정량화 (Quantification) : 알맞는 자료나 정량화 방법을 이용하여 기본 오류 확률을 산출, 수행 특성인자(Performance Shaping Factor : PSF), 종속성(Dependency), 복구인자(Recovery Factor) 등을 고려하여 수정된 오류 확률 값 산출
- 불확실성분석 (Uncertainty Analysis) : 인간오류값의 불확실성 분석
- 문서화 (Documentation) : PSA에 결과 반영 및 문서화

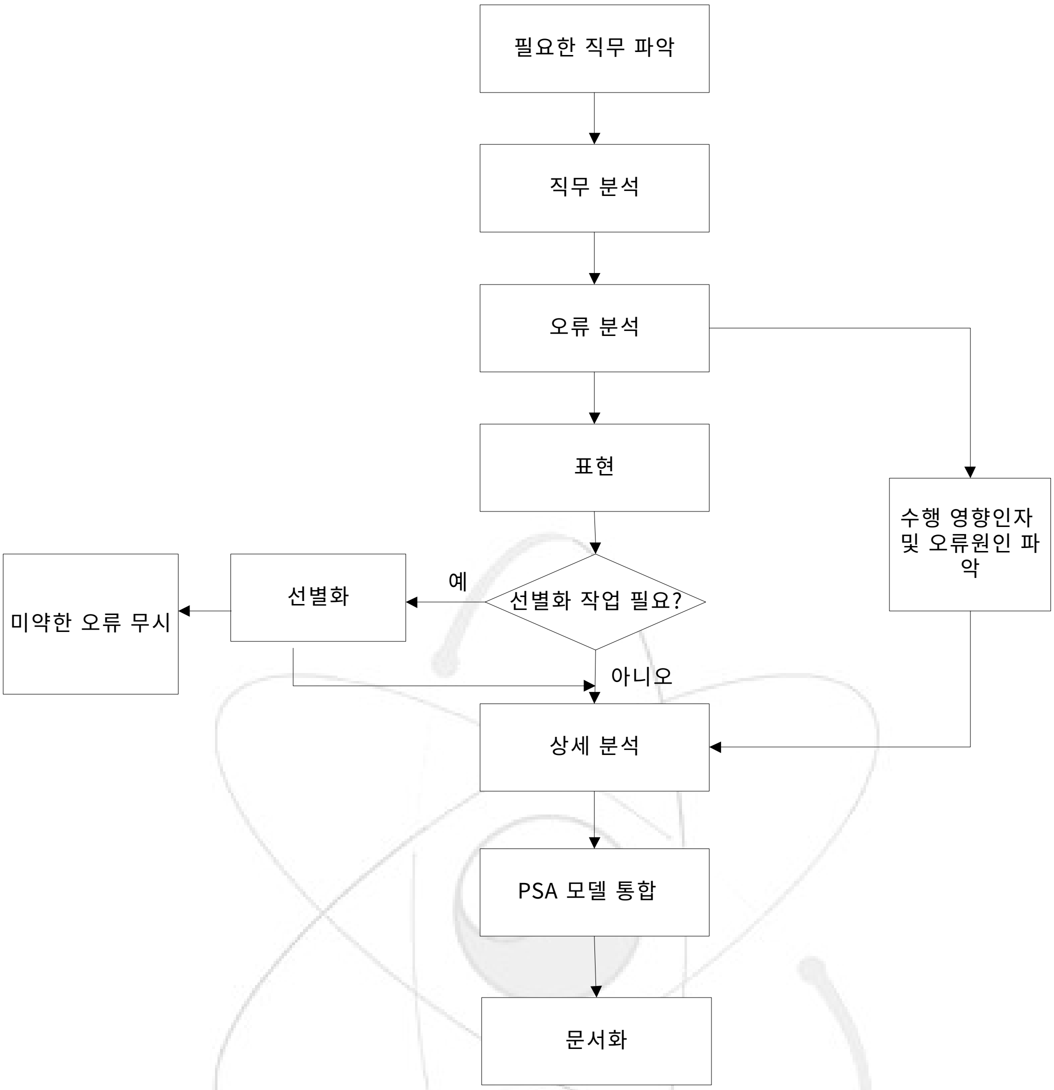


그림 19. 인간신뢰도분석 절차

다. 기본 가정 (Ground Assumptions)

본 절차서에 따라 HRA를 수행할 때 적용한 기본 가정은 다음과 같다.

1) 원자로 정지 시 운전원은 비상운전절차서(EOP) 및 회복절차서(FRP)를 따라 운전한다.

2) ESFAS는 간단한 FT 모델로 구성되는데, 신호발생 논리 회로 작동 실패를 하나의 undeveloped event로 처리한다. 따라서, 보정오류(miscalibration error)는 이 undeveloped event의 확률 값에 이미 고려된 것으로 처리한다(CEN-327 근거).

3) 동일 계통의 여러 트레인에 대한 시험 및 보수(T&M)가 동일 작업자에 의해 같은 교대조 내에서 진행된다면, 트레인간의 작업 사이에는 완전한 종속성(completely

dependence)이 있다는 가정 하에 'restoration error after T&M'나 'miscalibration error'는 여러 트레인에 동일한 basic event를 사용한다.

4) 발전소 MCR에는 어느 상황에서든지 최소한 발전과장, 안전과장, RO, TO, DB가 각 1명씩 근무하며, 발전과장 및 안전과장은 최소한 5년 이상의 운전 경험이 있다.

5) 발전과장은 원자로 정지 시 EOP를 따라 각 운전원의 조치를 명령하고, 각 운전원은 이에 따라 행동한다.

6) 안전과장은 주요 안전기능(critical safety functions)의 해당 안전변수의 추이를 관찰하고, 적정 수준을 만족하지 못할 때는 회복절차서로 진입한다.

7) 발전부장은 원자로 정지 시 10분 이내에 주제어반에 도착, 발전과장 및 안전과장의 결정 및 조치를 지원한다.

8) 주제어반 밖에서 수행되는 모든 운전원 조치는 최소한 10분 이상의 이동 시간을 갖는다. 만일 필요한 정보를 얻기 어려운 경우는 최소 이동 시간을 30분 이상으로 가정한다.

9) 계통 안전 점검 및 보수 작업장에는 최소한 2명 이상의 운전원이 참관하며, 이 경우 밸브 조작자가 아닌 사람에 의하여 밸브 위치 점검(점검표나 독립적 절차서 없이 어깨 너머로 확인하는 정도도 포함)이 가능하다.

10) 본 절차서에서 조치 단계의 인간오류 평가 중 commission error가 명시적으로 취급되지는 않는다.

11) ASEP이나 THERP HRA 절차서에 주어진 인간오류 확률 값은 중앙값(median)이며, 이로부터 아래 수식을 통하여 평균값(mean)을 산출하여 인간오류 확률 값으로 사용한다. 그러나, 중앙값 (median) 자체가 상당히 큰 경우(0.1 이상)에는 이를 평균값으로 취급한다.

$$\text{Mean} = \text{Median} * \text{Exp}\ [\ (\ln \text{EF}/1.645)^2\ /\ 2\ ]$$

12) 오차인자(error factor)는 다음 규칙을 사용하여 결정한다. 그러나, 인간오류의 95% 값이 1 보다 크면, EF를 수정한다.

- 인간오류 확률 값이 0.01 보다 작으면 (HEP < 0.01) EF = 10
- 인간오류 확률 값이 0.1 보다 작으면 (0.01 < HEP < 0.1) EF = 5
- 인간오류 확률 값이 0.1 보다 크면 (HEP > 0.1) EF = 3

라. HRA 상세 절차

(1) 사고 전 인간오류 분석 절차

(가) 선별분석

모든 대기(standby)중 기기 대하여 'restoration error after T&M(overhaul 포함)'를 고려함을 원칙으로 하되 아래 선별 규칙(screen out rules)을 적용, 해당되면 모델링 하지 않는다.

- 보수나 시험 후 기기가 운전가능상태(operable state)에 있음을 독립적으로 확인하는 tagging system (보수나 시험에 직접 참여하지 않은 담당자가 check list를 가지고 기기 상태를 확인한 후 MCR에 연락 in service 하는 경우)이 적용되는 경우
- 기기 상태가 운전가능상태에 있지 않으면 주제어반에 경보(annunciation)가 발생하는 경우
- 기기 상태가 주제어반에 표시되고 check list 사용하여 교대별(shiftly) 혹은 일별(daily)로 기기 상태를 점검하는 경우
- 기기 상태를 현장에서 check list 사용 주기적으로(교대별, 일별 또는 주간별) 점검하는 경우
- 부주의로 운전 가능한 상태에 있지 않더라도 비상시 필요한 상태(required state)로 전환되도록 auto 작동 신호를 받는 밸브인 경우
- 보수나 시험 후 기기 원위치의 일환으로 기능 시험(functional test)을 수행하는 밸브인 경우

위의 선별규칙을 적용한 후 남은 사고 전 인간오류는 HEP = 0.03 (EF = 5)을 선별값(screening value)으로 사용. 만일 동일한 인간오류에 대해 이전 PSA의 상세분석 결과가 있다면 이를 직접 사용 할 수 있다. 영광5,6호기 PSA에서 고려한 사고 전 인간오류로는 "not restored after T&M" 와 "miscalibration error" 2가지가 있다.

(나) 상세분석

상세분석은 앞에서 언급한 것처럼 선별된 사고 전 인간오류에 대하여 실제 상황을 반영하여 보다 구체적으로 분석한다. 그러나, 이제까지의 PSA 결과 사고 전 인간오류는 상대적으로 전체 결과에 큰 영향을 미치지 않는다. 따라서, 본 절차서에서는 개개의 사고 전 인간오류를 상세분석하지 않고 두 가지 사고 전 인간오류 유형 각각에 대해 가장 대표적이며 보수적인 인간오류를 선택하여 상세 분석한 후 이를 각 유형의 대표 오류값으로 사용한다.

기본조건으로는 모든 시험, 보수 및 보정 작업은 절차서에 근거하여 수행되며, 작업장에는 최소한 2명 이상이 있어 주 작업자의 오류가 다른 사람에 의해 점검 (독립적 점검이 아닌 어깨 너머로 확인하는 것도 포함) 가능하다고 가정한다. 사고 전 인간오류 분석 과정은 다음과 같다.

1) 'restoration error after T&M'는 절차서 상의 해당 step을 누락하고, 이를 작업장에 함께 있는 다른 운전원이 감지 못하여 복구 조치가 실패하는 사건으로 이에 대한 확률 값을 다음 자료를 근거로 산출

- 시험/보수 절차서상의 밸브 원위치 항목(step)을 누락하는 것으로 NUREG/CR-1278 Table 20-7 item 2를 적용하여 HEP = 0.003 (EF=3)으로 평가
- 담당 운전원이 상기 오류를 범했을 경우, 이를 작업장에 함께 있는 다른 운전원 혹은 작업자가 이를 감지하지 못하여 복구 조치가 실패할 확률 : 0.1 (Table 20-22 item 1)
- HEP = 3.0E-3 * 0.1 = 3.0E-4 (median)   EF = 3.0
- 중앙값을 평균값으로 환산하면 HEP = 3.75E-4 (mean)   EF = 3

2) 만일 (1)항의 기본조건이 맞지 않는 경우는 다음 규칙을 따른다.

- 절차서가 없으면 ASEP 절차서의 basic HEP = 0.03 (EF = 5) 사용
- 절차서는 있지만 격리 밸브 열림 및 닫힘에 대한 명시적 조작 단계가 없는 경우 전문가 판단에 근거하여 HEP = 0.03 (EF = 5) 사용
- 절차서는 있지만 주 운전원의 오류를 점검해줄 사람이 없는 경우 HEP = 0.003 (EF=5) 사용

3) 기본전제조건 이외에 check list를 갖고 정기적으로 기기 상태를 확인하는 경우 이를 고려할 수 있음

- 일정 주기로 check list를 갖고 기기(밸브) 상태를 육안으로 점검하는 경우 'restoration error after T&M(overhaul 포함)' 인간오류 확률은 다음 수식에 의해 계산한다.

$$Uv = (fm/fv) [(1- HP^{r}) / (1 - HP)] HEP$$

Uv : check list에 의해 시각 점검을 할 때 'not restored after T&M' 인간오류 확률
fm : 기기 조작 빈도 (즉, 관련 밸브가 시험이나 보수를 위해 close되는 빈도)
fv : 시각 점검 빈도
r : 시각 점검 빈도 와 기기 조작 빈도의 비 (= fv/fm)
HP : 시각 점검을 통해 잘못된 밸브 배열을 바로 잡지 못 할 확률

HEP : 시각 점검을 고려하기 전의 'not restored after T&M' 인간오류 확률

- 예로 3달에 1번씩 surveillance test를 하는 보조급수계통이 1달에 1번 check list를 갖고 기기 상태 점검을 실시하는 경우 펌프 전, 후단의 차단 밸브의 'not restored after T&M' 인간오류 확률은 다음과 같이 계산한다.
- - 기기 조작 빈도 계산 : 18 개월에 1번씩 년차 보수를 하며, 3개월에 1번씩 기능시험을 한다. 이 이외에 펌프의 보수를 위해 관련 밸브가 조작될 수 있는데, 이 경우 보수 빈도는 펌프 고장율의 10 배라 가정한다.

  fm = [6(기능시험)+1(년차 보수)+3.0E-3 * 10 * 6 (비정기 보수)]/18 = 0.399
- 시각 점검 빈도 계산

  fv = 1 (매달 check list 에 의해 시각점검)
- HP (시각 점검을 통해 잘못된 밸브 배열을 바로 잡지 못 할 확률)

  HP = 0.1 (Table 20-22 item 1)
- HEP (시각 점검을 고려하기 전의 'not restored after T&M' 인간오류 확률)

  HEP = 3.0E-4 (2항 : 3.0E-3 * 0.1 = 3.0E-4)
- Uv (check list에 의해 시각 점검을 할 때 'not restored after T&M' 인간오류 확률)

  Uv = (0.399/1.0)*[(1- $0.1^{2.506}$)/(1- 0.1)] * 3.0E-4 = 1.33E-4 (median)
- 중앙값을 평균값으로 환산하면 HEP = 2.15E-4 (mean), EF = 5.0

4) 'miscalibration error'는 'not restored after T&M' 보다는 복잡한 오류 발생 구조를 갖는다. 절차 누락뿐만 아니라 수행상 오류(commission error)도 포함하고 있다. 모든 종류의 수행상 오류를 정확히 고려하지는 못하지만 계기치를 잘 못 읽어서 발생할 수 있는 오류 가능성을 고려한다.

- 'miscalibration error'는 절차서 상의 해당 항목을 누락하는 것과 calibration시 계기치를 잘 못 읽어서 발생한다. 따라서, 절차서 해당 항목의 누락은 NUREG/CR-1278 Table 20-7 item 2를 적용하여 HEP = 0.003 (EF=3)으로 평가하고, calibration시 계기치를 잘 못 읽어서 발생할 수 있는 오류는 Table 20-10 item 1을 적용하여 HEP = 0.003 (EF = 3)으로 평가하였다. 즉, 'miscalibration error' HEP = 0.006 (EF = 5) 를 사용한다.
- 담당 운전원이 상기 오류를 범했을 경우, 이를 작업장에 함께 있는 다른 운전원 혹은 작업자가 이를 감지 못하여 복구 조치가 실패할 확률 : 0.1 (Table 20-22 item 1)
- HEP = 6.0E-3 * 0.1 = 6.0E-4 (median) EF = 5.0
- 평균값으로 환산하면, HEP = 9.7E-4 (mean), EF = 5.0

(2) 사고 후 인간오류 분석 절차

(가) 선별분석

사고 후 인간오류에는 절차서 수행상 필요한 직무를 수행하지 못하는 경우와, 자동작동 실패한 기기를 수동으로 작동하지 못하는 경우, 그리고 고장난 기기를 현장에서 수동으로 조작하는 경우 등이 포함된다. 선별분석 단계에서는 고장난 기기의 현장 조작은 고려하지 않는다. 이 부분은 최종 정량화 단계인 최소단절집합에 대한 Recovery Analysis에서 고려한다. 선별분석에서는 다음 규칙에 의거하여 오류 확률 값을 선정한다.

다음 경우 인간오류 확률 값으로 1.0 사용한다.

- 주제어실 밖에서 수행되는 중요 작업
- 수행절차서가 없는 경우
- 필요 계기가 고장이거나 잘 못 읽힌 경우

나머지 사고 후 인간오류는 다음과 같이 사고 발생 후 시간에 따른 HEP를 사용한다.

- 초기사건 발생으로부터 15 분 이내의 인간오류 : HEP = 1.0
- 초기사건 발생으로부터 30 분 이내의 인간오류 : HEP = 0.2
- 초기사건 발생으로부터 30분 이상 60 분 이내의 인간오류 : HEP = 0.1
- 초기사건 발생으로부터 60 분 이후의 인간오류 : HEP = 0.01

(나) 상세분석

사고 후 인간오류는 크게 다음 두 단계로 구분하여 분석을 수행한다. 사고 발생 후의 운전원 행위는 사고 종류 파악 및 관련 절차서를 선정하는 사고 진단(Accident Diagnosis) 과정과 사고 상황을 판단한 후 절차서 혹은 기억 속에 있는 내용대로 실제 조치를 취하는 진단 후 작업 수행 과정으로 구분할 수 있다. 이와 같이 두 단계로 구분하는 것은 각 과정에서 발생하는 오류 유형 및 특성이 다르기 때문에 분석 방법 역시 달라지기 때문이다. 현실적으로 진단과정에 대한 오류분석은 아직 초보적인 단계로 아주 간단한 모델을 사용하고 있다.

<u>진단오류 분석</u>

진단과정의 오류는 주로 허용시간에 영향을 받는다는 가정 하에, 최대 진단 허용시간에 대한 THERP (NUREG/CR-1278) 진단오류 표를 사용하여 분석한다. 분석 절차는 다음과 같다.

1) 최대 허용시간(Tm) 추정 : 사고해석, FSAR, 작업분석(task analysis), 타 PSA보고서 및 전문가 판단에 근거하여 주어진 작업이 수행되어져야 하는 최대 허용시간을 추정한다. 최대 허용시간 계산 시 기준 시점은 운전원에게 관련작업의 필요를 알리는 정보(경보 혹은 지시계 이상)가 최초로 제시된 시점으로 한다.

2) 작업예상 시간(Ta) 추정 : 진단이 완료된 후 작업 위치로 이동하여 적절한 작업을 완료하는 데 필요한 시간으로 발전소 walk-through를 통한 실측 시간이나 시뮬레이터에서 측정한 작업 시간을 사용한다. 만일 실제 자료가 이용 불가능한 경우는 다음 규칙을 사용한다.

- 절차서를 사용해야 되면, 사고 진단이 성공적으로 된 후 실제 조치 행위 시작까지 5분의 시간지연이 있다고 가정
- 주제어반의 주제어 판넬에 있는 기기 조작을 위한 시간 (이동 및 조작 시간)은 1분으로 평가
- 주제어반 안에 있지만 주제어 판넬이 아닌 경우, 기기 조작 시간은 2 분으로 평가
- 주제어반 밖에서 수행되는 작업인 경우, 필요한 이동 및 작업시간 정보를 운전원들로부터 얻는다면 이를 2배 하여 사용

3) 추정된 시간들을 근거로 진단허용시간 (Td) 결정 : Td = Tm - Ta

4) THERP (NUREG/CR-1278) 진단오류 표나 그림에 근거하여 진단오류 확률 값을 산출한다.

5) 동일한 진단허용시간(Td)에도 불구하고 운전원의 업무 수행도는 달라질 수 있으며, 이에는 여러 가지 영향 인자들이 있을 수 있다. 시간적 압박감(time stress), 절차서 구성 및 기술 수준(quality of procedure), 직무에 대한 거부감(hesitation), 직무 및 상황에 대한 숙련도(familiarity) 등을 업무 수행도에 영향인자로 선정하였다. 동일한 Td인 경우에도 Tm, Tm에 대한 Td와 Ta 비 등에 따라 운전원이 받는 스트레스는 달라진다. 상황에 따라 사고 에 대한 운전원의 인지가 충분하다고 판단되던지 혹은 최근 동일한 사건에 대한 직, 간접 경험 및 훈련이 있었던 사건인 경우에는 이를 고려하여 진단오류 확률 값을 보정해 줄 수 있다. 또한 만일 절차서가 없거나 내용이 불충분한 경우에는 이를 적절히 고려하여 기본 진단오류 확률 값을 보정해 준다.

- 진단 오류에 영향을 미치는 인자에는 time stress (허용시간 30분 이내), hesitation, 절차서 대응 조치 기술 수준, 운전원의 사고에 대한 인지도 및 훈련 정도 등이 있으며, 진단 오류 확률 값은 이런 영향 인자를 정성적으로

평가하여 기본 진단오류값 (ASEP, Table 8-2 혹은 Figure 8-1)의 상한치, 3배, 2배 혹은 1/2배, 1/3배, 하한치를 사용한다.

- 복구조치 (자동 작동 기기가 자동 기동에 실패한 경우 이를 인지하여 수동 기동시키는 행위와 같이 기동 실패나 작동 중 고장난 것을 회복시키는 행위) 중 보조계통에 대한 복구조치나 사고 전개과정으로 볼 때 운전원의 주 관심 대상에서 벗어난 기기에 대한 복구조치의 진단 오류 확률 값은 기본값 (ASEP, Figure 8-1)의 상한치를 사용한다.

6) 짧은 시간 내에 하나 이상의 이상상태(abnormal event)가 발생하는 경우, ASEP Table 8-2 이용하여 두 번째나 세 번째 진단오류를 평가한다. 하나 이상의 이상상태를 평가할 것이냐는 아래 기준을 사용하여 결정한다.

- EOP에 초기 사건 상황변화를 포함하여 추가 전개 사건 (any additional event)에 대해 명확히 기술되지 않았다면, nominal diagnosis model을 재 적용
- 만일 두 번째 혹은 그 다음의 abnormal event 가 초기 사건에 이어 아주 짧은 시간 내(10분 이내) 발생한다면, Table 8-2의 두 번째 혹은 세 번째 행(column)을 적용함. 만일 그 시간 후에 두 번째 혹은 세 번째 사건이 발생한다면 표의 첫번째 행을 적용
- 네 번째 이상의 사건이 짧은 시간 내에 발생한다면, 세 번째 행(column)을 적용
- Table 8-2의 기준시점 To 는 이상 사태의 시작을 알리는 compelling signal 작동시점을 의미하며 어떤 이상이 발행했는지를 100% 감지할 수 있다고 가정. 만일 두 개 이상의 compelling signal 이 사고 시나리오 내에 발생한다면 annunciator response model (Table 8-4) 사용 signal 감지 실패 확률 추정

<u>행위오류 평가</u>

진단 후 조치 행위에 대한 평가는 THERP를 기본으로 작성된 아래 절차를 따라 수행한다. 행위오류 분석은 ASEP HRA 방법을 근거로 하는데, 오류 가능성은 크게 작업유형 (task type) 및 스트레스 수준에 의해 결정되며, 얻어진 오류 확률 값은 다른 운전원에 의한 복구 가능성이나 Information feedback 수준에 의해 보정된다.

1) 작업분석을 통해 사고경위 및 사고 상황 (이용불능인 안전관련 계통), 작업 내용, 작업 위치 및 환경, 작업소요 시간, 적용 절차서, Information feedback 수준, 여러 가지 작업 영향 인자 등에 대한 정보 수집한다.

2) 작업유형 (task type) 결정 : 진단 후 조치행위의 특성이 dynamic인지 step-by-step인지를 다음 규칙에 의거하여 결정한다(그림 20).

- 비상운전절차서(EOP)사용 중 안전관련 계통이 고장 나는 경우 step-by-step을 dynamic으로 재 분류
- 만일 절차서가 있더라도 증상 중심(symptom oriented)으로 잘 설계되지 못하거나, 이를 근거로 적절한 훈련이 되지 못한 경우, 또한 회복절차서를 적용해야 되는 경우에는 관련 작업을 dynamic으로 분류
- 한 운전원이 한 작업에서 다른 작업으로 전환해야 할 때 적절한 신호(good cues)없이 두 개 이상의 작업을 동시에 수행해야 한다면 각 작업은 각기 step-by-step에 해당될지라도 각 작업을 dynamic 으로 분류

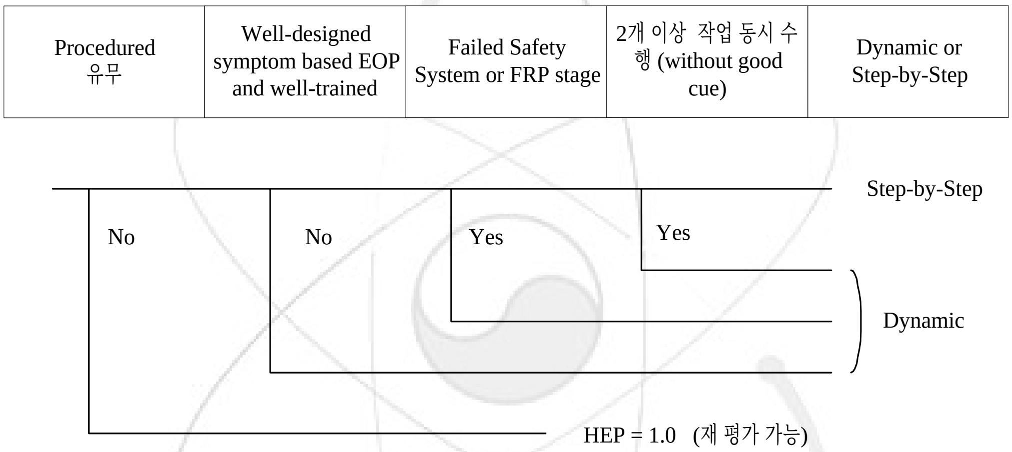


그림 20. 작업 유형 (task type) 결정 수목

3) Stress level 결정 : 다음 규칙에 따라 스트레스 수준을 결정한다.

- abnormal event가 시작된 후 2 시간까지는 최소한 moderately high level
- LOCAs 경우 재순환 운전 시작 전까지는 extremely high level
- 두 개 이상의 안전관련 계통이 기능 상실이면 extremely high level, 그러나 만일 해당 사고 시나리오에 대한 훈련이 충분하다 판단되면 low bound 값 사용 가능
- 이 이외에 time stress, 사고경위 및 작업에 대한 인지도, 작업 수행에 대한 부담감 등이 stress level 결정에 영향을 준다고 판단하여 표 31의 규칙에 따라 이들 인자를 평가

- LOCA 사고지만 표 31의 3가지 stress 영향 인자가 모두 Positive(+)인 경우는 moderately high stress로 평가 할 수 있다.
- 사고 발생 후 충분한 시간이 지나 사고가 거의 종결 상황에 이르렀고, 위의 stress 영향 인자가 모두 Positive(+)인 경우는 normal stress로 평가 할 수 있다.

표 31. Stress Level 결정 규칙

Time Stress (초기사건 1시간 이내 혹은 진단허용 시간 30분 이내)	Familiar with seq. (상황을 잘 이해하고 조치 행위를 숙지하고 있는가?)	Hesistance (행위에 대한 거부 감이 있는가?)	Stress Level
Yes (-), No (+)	Yes (+), No (-)	Yes (-), No (+)	Negative effect (-)가 (즉stress를 높이는 쪽이) 2개 이상이면 extremely high, 1개 이하이면 moderately high

4) Basic HEP 결정 : 작업유형과 스트레스 수준에 따라 기본 인간 오류값을 선정한다. 이것은 ASEP HRA 방법에서 제시한 것으로 중앙값이며, 실제 적용 시에는 평균값을 산출하여 사용한다.

- moderately high stress 상황에서 step-by-step(critical procedural) action 수행 : HEP = 0.02 (EF = 5)
- moderately high stress 상황에서 dynamic action 수행 혹은 extremely high stress 상황에서 step-by-step action 수행 : HEP = 0.05 (EF = 5)
- extremely high stress 상황에서 dynamic action 수행 : HEP = 0.25 (EF =5)

5) Time Stress 하에서의 Doubling Rule : moderately high or extremely high stress 하에서 매우 제한된 시간 내에 작업이 동일 운전자에 의해 진행되어야 할 경우, 만일 첫번째 action이 ineffective하면 후속 actions을 실패할 확률은 정상 평가치를 배(double) 하여 사용한다.

6) 다른 운전원(감독자)에 의한 Recovery 가능성 고려 : 이상상태 발생 후 초기 과도기간이 지나면 급박한 상황 전개는 줄어들게 되며, 이 경우 한 운전원에 의한 조치 행위의 오류는 다른 운전자나 감독자에 의해 확인되고 바르게 수정될 수 있다. 이런 복구 가능성을 다음 규칙에 따라 고려한다.

- 기본적으로 basic HEP 의 10% 고려
- moderately high stress 상황에서 step-by-step (critical procedural) 인 경우 : HEP = 0.2 (EF = 5)
- moderately high stress 상황에서 dynamic action 혹은 extremely high stress 상황에서 step-by-step 인 경우 : HEP = 0.5 (EF = 5)
- extremely high stress 상황에서 dynamic action 인 경우 : HEP = 0.5 (EF =5)
- extremely high stress 상황에서 dynamic action인 경우 time stress를 받는 경우 많은데, 시간이 30분 이내로 짧은 경우 감독자에 의한 Recovery 가능성은 고려하지 않는다.
- human redundency 이외에 다른 Recovery 인자가 있다면 이를 별도로 고려할 수 있다.

7) Information Feedback 에 의한 Recovery 가능성 고려 : 발생한 조치단계의 인간오류를 복구할 수 있는 인자로 본 절차서에서는 타 운전원에 의한 복구 가능성과 함께 조치행위의 결과를 곧바로 확인할 수 있는 계기의 존재 유무(이를 information feedback이라 지칭)를 선정하였다.

- 인간의 행위는 목적지향성(goal oriented)을 갖고 있어, 수행하고자 하는 목적을 달성하기까지 조치, 결과 확인, 오차 보정 등 정보의 feedback을 통한 운전을 반복한다. 예를 들어 운전원이 밸브 개폐 혹은 펌프 작동을 시키면, 이로 인한 유량 및 유압의 변화를 어떤 식으로든 확인하고 싶어한다. 이때 제어 판넬에 조치 결과를 직접적으로 확인할 수 있는 유량계 혹은 압력계가 존재한다면, 자신의 조치결과를 쉽게 확인할 수 있으며 이로 인해 세부 조치수행 단계에서의 오류를 수정할 수 있게 된다. 따라서 운전원이 수행 조치를 확인할 수 있는 직접적인 계기 및 지시계가 주제어반에 설치되어 있다면 이를 통한 오류 복구 가능성을 고려한다.

- 운전원이 조치한 행위를 담당 판넬 상의 계기를 통하여 직접적이며 즉각적으로 확인할 수 있는 계기나 경보가 있는 경우 운전원 자신이나 감독자에 의해 조치가 제대로 되었는지를 확인할 수 있으며, 이런 확인 과정이 누락되거나 실패할 오류 확률은 HEP = 0.1 이다

8) 기타 스트레스 영향 인자 고려

- 표 31의 Stress Level 결정 규칙에서 고려하는 3가지 Stress Factor가 모두 Positive 이면 Basic HEP와 감독자에 의한 Recovery HEP를 1/2 할 수 있다.

9) 최종 인간오류확률 값 HEP 산출

- 진단오류 확률 값과 행위오류 확률 값을 더하여 최종 인간오류 확률 값을 산출한다.

10) 오차인자(error factor)는 다음 규칙을 사용하여 결정한다. 그러나, 인간오류의 95% 값이 1 보다 크면, 95%값이 1을 넘지 않도록 오차인자를 적절히 수정한다.

- 인간오류 확률 값이 0.01 보다 작으면 (HEP < 0.01) EF = 10
- 인간오류 확률 값이 0.1 보다 작으면 (0.01 < HEP < 0.1) EF = 5
- 인간오류 확률 값이 0.1 보다 크면 (HEP > 0.1) EF = 3

마. 인간 오류간의 종속성 분석 (dependency analysis)

인간오류 종속성 분석에는 두 가지 대상이 있다. 첫째는 한 직무를 수행하는 세부 조치 행위들 사이의 종속성으로서, THERP와 같이 인간의 행위를 미세한 단위동작으로 세분화하여 평가할 때 단위 동작들 사이의 관계성을 말한다. 둘째는 보다 상위수준의 종속성으로 직무들 사이의 종속성을 말한다. 즉, 사고 전개과정에서 이전 직무의 성공, 실패가 후속 직무의 수행도에 영향을 줄 수 있는데 이런 종속성을 인간 오류간 종속성이라 한다. 본 절차서에서는 두 번째 종속성, 인간 오류간 종속성 평가에 대하여 기술하고 있다.

인간 오류들 사이의 종속성이란 노심손상을 초래하는 사건 조합(즉, 최소단절집합)에 두 가지 이상의 인간오류가 나타나는 경우 이들 인간 오류들 사이에 존재할 수 있는 상호 연관성을 말한다. 예를 들어 두 개의 인간오류가 하나의 최소단절집합에 나타나는 경우, 첫번째 인간오류가 발생한 상황에서 두 번째 인간오류가 발생할 가능성이 높아진다면 이들간의 종속성을 평가하여 두 번째 인간오류의 확률 값을 보정해야 한다. 만일 이런 평가 과정이 누락되면 실제보다 낙관적인 평과 결과를 얻게 될 것이다.

여기서 언급하는 종속성은 THERP에서 말하는 세부 단위 동작들간의 종속성을 의미하는 것은 아니다. THERP에서의 종속성은 하나의 인간오류를 평가하는 과정에서 운전원 조치를 구성하는 세부 단위 동작들간의 상호 연관성을 말하는 것이고, 여기서 언급하고 있는 종속성은 두 인간 오류들 사이의 상호 연관성을 뜻하는 것이다.

두 인간오류 사이의 종속성을 고려하는 방법에는 여러 가지 수준이 있을 수 있다. 현재 인간오류는 진단(인지)과정과 세부작업 수행 과정을 구별하여 평가하는데, 진단과정 및 세부작업 수행 과정 전부를 포함하여 인간 오류들간에 종속성을 평가하는 방법과 종속성은 상황 진단과정 사이에만 강하게 작용한다고 보고 이들 사이의 종속성을 평가하는 방법이 있다. 본 절차서에서는 두 인간오류 사이의 존재하는 종속성의 대부분은 상황 진단과정 사이에서 발생한다고 판단하여 이들간의 종속성을 평가하였다.

인간 오류들 사이의 종속성이 상황 진단과정에서 주로 발생한다고 판단하기 때문에 종속성 분석 대상 인간 오류들은 사건수목분석 단계에서 고려되는 인간 오류들이 된다. 즉, 사고 후 인간오류가 분석 대상이 된다. 그러나, 사고 후 인간오류 모두가 분석 대상이 되는 것은 아니며, 상호 종속성이 결과에 크게 영향을 미친다고 판단되는 것들에 대해서만 상세 분석을 수행한다. 예로 공학적 안전 계통의 자동작동신호 발생 실패 시 고려한 운전원 수동신호발생 실패 사건과 다른 사고 후 인간오류와의 종속성은 분석 대상에서 제외하였다. 이는 수동신호발생 실패 사건은 항상 자동신호발생 실패 사건과 AND 조건으로 발생하게 되며 이들의 발생 확률이 매우 낮기 때문에, 결과적으로 수동신호발생 실패 인간오류와 다른 사고 후 인간오류가 동시에 나타나는 최소단절집합은 발생 빈도가 매우 낮게 되며 따라서 이들의 상호 연관성이 전체 결과에 미치는 영향은 무시할 수 있다고 판단하였다.

종속성에는 어떤 사건의 발생이 다음 사건 발생을 촉진시키는 경우와 억제 시키는 두 가지 방향이 있다. 앞에서 언급한 것처럼 첫번째 인간오류 발생이 두 번째 인간오류의 발생 가능성을 높이는 경우와 반대로 첫번째 인간오류 발생이 두 번째 인간오류가 발생할 가능성을 낮추는 경우가 있을 수 있다. 그러나 사고경위에서 나타나는 인간오류의 조합을 살펴보면 대부분의 경우 두 번째 발생 가능성을 높이는 것들이며 또한 보수적 관점에서 두 번째 인간오류 발생 가능성을 낮추는 경우는 본 분석에서 고려하지 않았다.

인간 오류간의 종속성 분석은 분석 대상 인간오류 선정, 종속성 수준 결정, 종속성 평가 등으로 구분할 수 있다.

(1) 분석 대상 인간오류 선정

종속성 분석 대상 인간오류를 선정하기 위해서는 우선 어떤 인자가 두 인간 행위 사이에 동시에 영향을 미치는지 살펴보아야 한다. 모든 사건수목 표제에 대한 검토를 바탕으로, 본 분석에서는 다음과 같은 두 가지 인자를 기준으로 대상 인간오류를 선정하였다.

- 동일 혹은 유사한 기능(Function)과 관련된 운전원 행위 중 시간적으로 많은 차이가 없는 경우 (2시간 이내)
  - 안전주입 (Safety Injection)과 관련된 행위
  - 재순환 (Recirculation)과 관련된 행위
  - 이차측을 통한 열제거와 관련된 행위 (급수 공급과 증기 방출 운전)
  - 이차측을 통한 열제거와 주입 및 방출 (F&B) 운전
  - 이차측을 통한 열제거와 증기발생기 격리
  - 정지냉각(Shutdown Cooling) 운전과 관련된 행위

- 손상된 증기발생기 격리와 관련된 행위
- 시간상으로 연속되거나 혹은 짧은 시간 (1시간 이내) 범위 내에서 수행되는 운전원 행위

대상 인간오류를 선정하기 위해 우선 각 초기사건에 대한 사건수목 표제를 검토한다. 위의 두 가지 인자를 기준으로 상호 연관성이 있다고 판단되는 사건수목 표제를 우선 파악한 후, 각 사건수목 표제에 모델링된 인간오류 사건들을 대상으로 최종 분석 대상 인간오류를 선정한다.

(2) 종속성 수준 결정

대상 인간 오류들이 파악되면 인간 오류들 사이의 종속성 수준을 결정한다. 종속성 수준에는 완전(complete), 고(high), 중(medium), 저(low) 및 무(zero) 종속성이 존재하며, 이들 종속성에 대한 평가 방법은 THERP에서 제시하고 있다. 종속성 수준의 결정하는 것은 매우 어려운 작업이며 전문가의 판단에 전적으로 의존하게 되는 경우가 많다. 따라서 본 절차서에서는 보수적 관점에서 대상 인간 오류들 사이에는 고 종속성이 존재한다고 가정한다.

(3) 종속성 평가

인간오류 사이의 종속성 평가에는 THERP Ch.10의 종속성 평가 수식을 사용하였다. 인간오류는 진단부분과 진단 후 세부동작 부분으로 나누어 평가하며, 앞에서 언급하였듯이 인간오류 사이의 주된 종속성은 진단부분 사이에서만 발생한다고 가정하였다. 따라서, 다음과 같은 수식에 따라 두 인간오류 사이의 종속성을 평가하였다.

인간오류는 진단부분의 오류와 진단 후 세부동작 부분에서의 오류로 나뉜다. 즉,

HE1(2) = HE1(2)c + HE1(2)a

여기서, HE1(2) : 인간오류 HE1(2)의 확률 값

HE1(2)c : 인간오류 HE1(2)의 진단부분 오류 확률 값

HE1(2)a : 인간오류 HE1(2)의 진단 후 세부동작 수행 오류 확률 값

두 인간오류 HE1과 HE2가 하나의 최소단절집합에 나타나고 두 사건 사이에 상호 종속성이 없다면 두 인간오류의 영향은 다음과 같이 두 오류 확률 값을 곱(product)하는 것으로 평가된다.

HE1 * HE2 = (HE1c + HE1a) * (HE2c + HE2a)

= HE1c * HE2c + HE1a * HE2c + HE1c * HE2a + HE1a * HE2a (1)

그러나 두 인간오류 HE1과 HE2 사이에 고 종속성(high dependence)이 존재한다면 HE1이 발생한 상황에서 HE2의 확률 값은 높아진다. 앞에서 가정한데로 두 사건의 진단부분 사이에서만 상호 종속성이 존재하므로, 수식 (1)의 4가지 사건 조합 중 HE1c * HE2c 사이의 종속성을 평가하면 된다. 종속성 수준이 고 종속성이므로 THERP Ch.10의 고 종속성 평가 수식을 사용하면 위 수식은 다음과 같이 정리된다.

HE1 * HE2(dep) = <u>HE1c * HE2c(dep)</u> + HE1a * HE2c + HE1c * HE2a + HE1a * HE2a

= HE1c * (1 + HE2c)/2 + HE1c * HE2a + HE1a * (HE2c + HE2a)

= HE1c * ((1 + HE2c)/2 + HE2a) + HE1a * (HE2c + HE2a) (2)

여기서,HE2(dep) : 종속성이 고려된 HE2 확률

HE2c(dep) : 종속성이 고려된 HE2의 진단오류 확률

결과적으로, 종속성이 고려된 HE2(dep) 는 다음과 같이 계산된다.

HE2(dep) = 수식 (2) / HE1 (3)

수식 (2)와 (3)을 사용하여 표2에 정리된 대상 인간오류 조합 사이의 종속성을 평가하였다.

바. 복구분석(recovery analysis)에서의 인간신뢰도분석

PSA 사고경위 정량화 단계에서는 최소단절집합에 대한 복구분석이 있다. 각 사고 시나리오에 대한 최소단절집합들 중에는 운전원의 간단한 현장 조작만으로 고장 난 기기를 기능 회복시켜 사고를 종결 시킬 수 있는 사건 조합들이 있다. 복구분석이란 이런 최소단절집합을 파악하여 운전원의 복구 가능성을 고려하는 업무이다. 이런 복구조치분석을 통해 보다 현실적인 PSA 결과를 얻을 수 있다. 그러나, 그 대상의 선정 기준 및 복구 가능성 평가에는 세심한 주의가 필요하며, 너무 낙관적인 분석 결과를 얻지 않도록 제한된 범위 내에서의 복구분석을 한다.

본 절차서의 대상인 울진3,4와 영광5,6 PSA에서는 영광3,4 PSA에 대한 독립검토에서 제기되었던 의견들을 반영하여 가능한 보수적인 복구분석을 수행한다. 복구분석 대상은 모두 3가지 유형으로 '소외전원상실 시 소외전원복구', '모터구동밸브의 수동 개방', '고장 난 interlock card를 수동 제거 또는 우회'가 있다. 이중 소외전원복구 확률은 실제 발생 사건을 분석한 참고 자료를 사용하므로 HRA 대상에서 제외된다. 복구분석 대상의 선정에는 최소한 60분 이상의 여유시간이 있는 경우만을 대상으로 하였으며, 고장난 모터구동밸브의 복구는 밸브 구동(actuator) 부분의 고장인 경우에만 가능한

것으로 분석하였다. 밸브 구동부분의 고장은 전체 고장의 10%[EPRI/NP-3967]에 해당하므로, '모터구동밸브의 수동 열음' 가능성은 밸브 고장확률의 10%에 해당하는 부분에만 고려한다.

'모터구동밸브의 수동 개방 실패' 와 '고장 난 interlock card를 수동 제거 또는 우회 실패' 인간 오류값은 다음과 같은 계산하였다.

- 최소한 60분 이상의 여유시간이 있으나, 보수적 60분의 운전원 여유시간이 있다고 가정
- 현장으로 이동하고 밸브 개폐 핸들을 조작하거나 interlock card를 제거하는데 필요한 시간은 20분으로 산정
- 그러므로, 고장 난 밸브나 interlock card의 복구 필요성을 인식하고 현장 수동 복구를 결정하는데 필요한 진단여유시간은 40분
- ASEP HRA 그림8-1의 진단오류 확률 분포로부터 진단오류 확률을 계산한다. 고장 난 밸브의 이상 상태의 파악이 운전원의 주 관심사에서 벗어났다는 판단 하에 40분 진단여유시간의 상한치 값인 0.008을 진단오류 확률로 계산
- 작업유형은 step-by-step, 스트레스는 사고 시 현장에서의 작업이므로 extremely high로 판정하여 행위오류 확률 값 0.08 계산
- 인간오류 확률 값은 진단오류와 행위오류 값을 합하여 0.088 이나, 보수적 관점에서 0.1을 사용

4. 시험 및 보수 데이터 분석 절차

일반 데이터원 파악 및 고유 데이터원 파악 등의 단계는 기기 신뢰도 데이터 분석 절차와 같다. 한편 고장율에 대한 데이터는 많지만 보수 또는 시험으로 인한 이용불능 데이터는 거의 없다. 또한 이용 가능한 보수 데이터에도 예방보수 활동에 관한 것은 거의 없으며 계통의 배열, 보수관습 및 행정적 제한에 따라 분석대상 발전소에 대해 재해석하는 것이 필요하다.

가. 분석 대상 기기 결정

분석 대상 발전소의 특성에 따라 시험 및 보수 데이터가 필요한 기기를 결정한다. 일반적으로 선별되는 분석 대상 기기는 앞에서 설명된 것과 같다.

나. 보수 데이터 수집

분석 대상으로 결정된 기기에 대한 보수 관련 데이터를 수집한다.

- 모든 관련된 일차적 및 이차적인 데이터원을 검토한다.

- 이용 가능한 정보가 충분하지 않을 때는 발전소 요원과 면담하여 가능한 모든 정보를 수집한다.
- 대부분의 시험들은 Override 특성을 갖는다. 따라서 이러한 시험은 이용불능도에 영향을 끼치지 않으므로 데이터에 포함하지 않는다.
- 보수 데이터에 포함되는 것은 기기가 그 기능을 수행할 수 없도록 격리되거나 제거되었을 경우이다. 대부분의 밸브 보수는 밸브 구동체(Operator)에 대한 것으로 보통 매우 짧은 시간이 소요된다. 밸브의 분해를 요하는 기계적 수리는 일반적으로 발전소 정지 시에 수행하므로 보수로 인한 이용불능도에는 영향을 끼치지 않는다. 또한 펌프를 격리시켜야 하는 보조 기기의 보수는 펌프 데이터에 포함된다. 발전소의 저온정지기간 중의 보수는 저온정지시의 보수 절차가 운전 시와 매우 다르고 기술운영지침서의 운전제한시간이 적용되지 않으므로 데이터베이스에는 포함되지 않는다.
- 각각의 발전소 기기에 대해 'MAINTENANCE RAW DATA BOOK'을 작성한다.

다. 성공데이터의 결정

성공데이터의 결정은 일반 기기 신뢰도 데이터에서 설명된 바와 같이 수행한다.

- 교정보수 - 기능상의 고장이 일어나 보수가 수행될 때마다 완전한 기능상의 점검이 수행된다. 따라서 이를 작동 요구 수에 포함시켜야 한다.
- 연계보수(Interfacing Maintenance) - 대상 기기 및 병행 기기의 기능 점검이 수행된다
- 발전소 요원과 면담하여 계산에 사용된 절차 및 결과를 검증한다.
- 주기적인 시험기간 중에만 운전되는 기기는 각각의 시험운전 시간을 합한다.
- 실제 주기시험 기록을 검토하여 시험되었던 모든 운전시간을 합한다.
- 실제 주기시험 기록이 이용 가능하지 않을 때는 한번의 시험에서의 운전 시간을 결정하기 위하여 시험절차를 검토한다.
- 비주기적인 시험시간을 포함시키기 위하여 운전절차, 특수시험 절차 및 운전일지를 검토하여 비주기적인 시험에 의한 운전시간을 계산한다.
- 성공데이터에 대한 검증 : 발전소 고유 데이터원에 포함된 정보의 변화가능성(Variability) 때문에 성공데이터의 수집에는 발전소 운전에 대한 철저한 이해가 필요하다. 따라서 성공데이터의 수집 시에는 발전소 운전원과 수시로 접촉하여 발전소 및 기기에 대한 가정의 적합성을 검토하는 게 큰 도움이 된다.

라. 발전소 고유데이터의 검토, 평가 및 처리

수집된 발전소 고유 데이터의 검토 및 평가는 이 데이터를 사용할 계통분석가 또는 사고추이 분석가와 긴밀한 협의를 통해 수행되어야 한다. 이 단계에서의 주된

목적은 데이터분석가가 처리하기에 적합한 형태로 데이터를 요약하고 그 수를 감소시키는데 있다.

- 시험 및 보수 데이터의 처리
  - 시험 데이터 : 시험빈도 및 시험기간의 파악에 대해서는 절차 6에서 설명하였다. 여기서는 시험 기간 중에 발생한 고장을 파악하는 것이 주 목적이다. 이들 고장은 나중에 분포의 변수들을 계산하는데 사용한다.
  - 보수데이터 : 각각의 보수기기에 대해 'MAINTENANCE RAW DATA BOOK'을 검토한다.
    - ✓ 가동중인 기기를 분해하거나 격리시켜야 하는 보수활동을 파악하여 분류한다.
    - ✓ 각 보수시간을 계산하거나 또는 직접 데이터에서 얻는다.
    - ✓ 기기고장의 결과로 인한 보수활동을 파악하여 기기고장 데이터에 포함되어 있는가를 확인한다.
- 보수 빈도는 일반적으로 다음의 요인에 의하여 결정된다.
  - 기기의 정상적인 기능과 관련 고장율
  - 발전소 예방보수 활동과 주기검사 및 정기점검 프로그램
  - 기술운영지침서의 작동불능 허용시간
- 보수지속 시간은 일반적으로 다음 요인에 의하여 결정된다.
  - 고장의 규모
  - 보수요원의 투입가능성
  - 일반 보수계획 및 보수 우선순위
  - 기술운영지침서의 작동불능 허용시간

마. 최종 발전소 고유데이터베이스 개발

- 기기 보수 데이터
  - 발전소 고유데이터가 없는 경우는 일반분포를 사용한다.
  - 발전소 고유데이터가 있는 경우
    - ✓ 보수 시간에 대한 분포를 개발한다.
    - ✓ 보수 빈도에 대한 분포를 개발한다.
- 일반적으로 발전소의 고유 고장정보는 기기수준에서의 이용불능도를 구할 수 있을 정도로 충분한 데이터를 제공하지 못한다. 또한 적합한 일반 보수 데이터가 없을 경우, 간접적으로 각 계열에 대한 이용불능도를 구한다.

바. 발전소 고유 데이터 베이스 전산화

발전소 고유 데이터 베이스는 사용하기 편리하게 하고 새로운 정보를 계속해서 반영할 수 있도록 하며 수집된 정보를 신속히 처리하고 기록의 정확성을 얻기 위하여 전산화할 필요가 있다. 이 전산화는 데이터의 자동 처리, 일차적 데이터에의 접근성 용이 등의 특성을 가져야 하며 포함시켜야 할 내용은 다음과 같다.

- 발전소 명칭
- 계통명
- 기기명
- 기기 설명
- 원인 설명 등

제7장 정량 분석

제1절 개요

1. 목적

본 사고경위 정량분석 절차서는 원자력발전소의 확률론적 안전성평가(Probabilistic Safety Assessment : 이하 PSA)에서 노심손상빈도를 계산하는 정량화 방법과 수행 절차에 대한 정확한 지침을 제공하기 위하여 기술하였다.

2. 적용범위

본 절차서는 영광 5,6호기 1단계 확률론적 안전성 평가의 사고경위 정량화를 위한 것으로서, 설계 중인 원전에 대하여 그 동안 국내에서 수행되었던 PSA의 사고경위 정량분석 절차 및 방법을 기본적으로 정리하였다. 따라서 본 절차서에 기술된 정량화 방법 및 수준은 국내의 설계 중 원전 PSA에 적용된 정량분석에 준하는 것으로서, 향후 설계 중인 원전 PSA에 적용할 수 있을 것이다.

3. 참고문헌

사고경위 정량화에서는 PSA 모델 전반을 이해하는데 필요한 자료와 계산을 수행하는데 필수적인 최소단절집합 계산 논리에 대한 자료가 필수적이다. 이외에 최소단절집합 계산방법, 순환논리를 가진 고장수목 처리 방법, 회복조치 처리 방법, 사고경위 정량화 방법, 고장수목 및 사건수목 구성에 관한 방법등에 관한 자료가 필요하다. 본 절차서를 작성하기 위해 참고한 대표적인 문헌은 다음과 같다.

[1]"KIRAP Release 2.0 사용자 설명서," 한상훈 외, KAERI/TR-361/93, KAERI, 1993

[2]"CONPAS 1.0 Code Package 사용자 설명서," 안광일 외, KAERI/TR-651/96, KAERI, 1996

[3]"An Analytic Method to Solve the Logical Loop between the Support Systems in the Fault Tree Model," Yang, Joon-Eon et al., Proceeding of PSA '95: International Topical Meeting Probability, Reliability, and Safety Assessment, pp.579-582, Seoul, Korea, 1995

[4]"해석적 방법에 의한 고장 수목 순환 논리의 분석: 실제 PSA에의 적용 예," '96 추계학술발표회 논문집, 한국원자력학회, 1996

[5]"원자력 안전성 향상 연구 - 1단계 PSA 전산체제 개선," 박창규외, KAERI/RR-1487/94, KAERI, 1995

[6]"PSA Workstation KIRAP 개발," 김태운 외, KAERI, 추후 발간 예정

[7]"Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1), " Safety Series No. 50-P-4, IAEA, 1992

[8]"Probabilistic Safety Analysis Procedures Guide," NUREG/CR-2815, USNRC, 1984

[9]"PRA Procedures Guide," NUREG/CR-2300, USNRC, 1982

4. 기본 가정 및 용어 정의

사고경위 정량화에 사용되는 주요 용어는 다음과 같다.

PSA	확률론적 안전성 평가
노심손상빈도	PSA 분석에서 도출된 노심손상이 발생할 수 있는 빈도. 1년 단위로 계산됨.
KIRAP	한국원자력연구소에서 개발한 PSA 수행용 전산코드들
최소단절집합	계통 실패 또는 노심손상을 발생시킬 수 있는 기본사건들의 조합
고장수목	계통 실패에 대한 원인들을 논리적으로 추적해나가는 모델
사건수목	사건이 발생한 후 계통 작동유무에 따라 어떠한 사고로 전개되는 가를 나타내는 모델
Branch 모델	사건수목에서 계통의 작동유무에 사고경위가 나누어진다. 여기서 계통 실패를 나타내는 모델을 branch 모델이라 한다.
HRA	인간신뢰도 분석
사고경위	사건수목에서 계통 작동유무에 따라 전개되는 사고를 지칭. 하나의 사고경위는 어떠한 초기사고가 발생한 후 어떠한 계통들이 작동하였고 어떠한 계통들이 실패하였는지에 따라 정해짐
초기사건	원전 정상운전중 이상사태를 발생시킬 수 있는 사고. PSA 에서는 유사한 사고들을 그룹화하여 하나의 초기사건으로 처리하며, 대부분의 경우 원자로 정지로 이어지는 사고만을 취급함.
회복조치	실패한 사건 (기기 고장) 을 운전원이 복구하는 행위
회복조치분석	본문 참조

중요도분석	본문 참조
불확실성 분석	본문 참조
운전원 행위 의존성	본문 참조
Double Initiator 삭제	본문 참조
Rule-Based Recovery	회복조치분석을 규칙 기반으로 처리하여 전산화하는 방법
고장수목의 순환논리	고장수목중 한 게이트의 하부논리중에 그 게이트의 논리가 다시 나타나는 것
Nonsense 최소단절집합	PSA 모델중 원전의 설계 또는운전특성상 현실적으로 나타날 수 없는 최소단절집합
절삭치	최소단절집합을 계산할 때 주어진 절삭치보다 값이 적은 최소단절집합은 삭제한다.

제2절 사고경위 정량화 절차

1. 개요

사고경위 정량화의 기본적인 목적은 1단계 PSA 에서 노심손상빈도를 계산하는 것이다. PSA 는 그림 21과 같이 원전 정보수집, 초기사건 분류, 각 초기사건에 대한 사건수목 구성, 사건수목 분석에 필요한 고장수목 구성, 필요한 신뢰도 자료 분석후에 사고경위 정량화를 수행하게 된다. 사고경위 정량화에서는 노심손상빈도 계산, 중요도 분석 및 불확실성 분석등이 수행된다.

사고경위 정량화에서 핵심이 되는 부분은 각 사고경위에 대한 최소단절집합을 계산하는 것이다. 하나의 사고경위일지라도 PSA 에서 모델되는 거의 모든 고장수목을 연결하여 최소단절집합을 계산하여야 하므로, 사고경위 최소단절집합 계산은 모든 PSA 모델에 대한 이해가 필요하다. 또한 PSA 에서 계산시간이 가장 많이 걸리는 분야로서 기능이 뛰어난 최소단절집합 계산기가 필수적이다.

본 절차서에서는 사고경위 정량화 절차를 간략히 기술하고, 뒷 부분에 PSA 정량화용 Kcut 전산코드의 간단한 사용법과 이를 이용한 사고경위 정량화 방법을 간단한 예제와 함께 기술하였다.

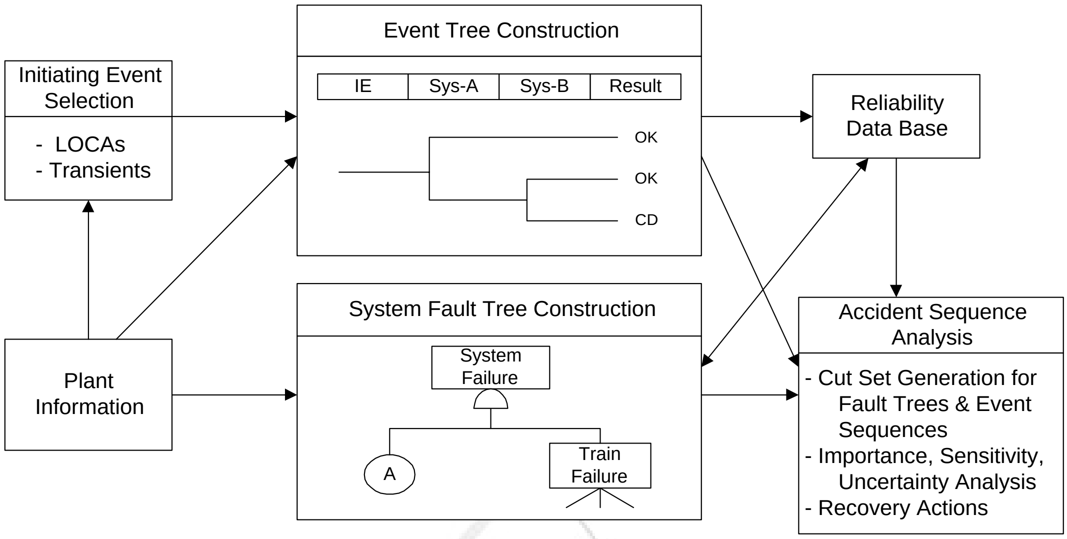


그림 21. PSA 수행 절차

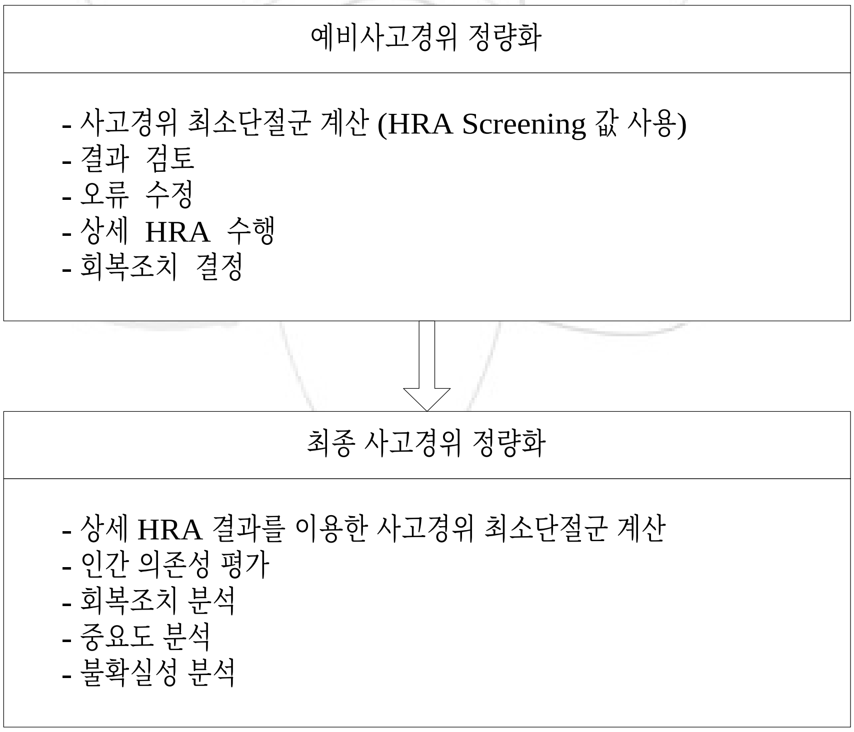


그림 22. 사고경위 정량화 절차

PSA 정량화 절차는 PSA 마다 차이가 있을 수 있으며, 또는 같은 PSA 라도 분석자에 따라 약간의 차이가 있을 수 있다. 따라서 여기서 기술되는 절차외에도 다른 절차가 있을 수 있으므로 기본적인 방법론을 이해하여야 한다.

본 절차서에서는 영광 5,6 호기 PSA 에서의 사고경위 정량화 절차를 기본으로 기술하였으며, 이는 그림 22에서와 같이 두번의 정량화 과정을 거친다. 이중 예비 사고경위 정량화는 전체 PSA 모델 및 신뢰도자료에 대한 점검 및 최종 정량화를 위한 자료 도출을 목적으로 수행된다.

예비 사고경위 정량화의 수행 과정 및 결과 최소단절집합을 검토함으로서, 고장수목과 사건수목등의 PSA 모델이 적절히 구성되었는지 또는 오류가 없는지등을 파악할 수 있으며, 사용된 신뢰도 자료의 오류도 점검할 수 있다. 또한 결과 최소단절집합을 검토하여, 상세 HRA 에 포함될 주요한 인간행위등을 파악할 수 있으며 또한 회복조치 분석에 포함되어야할 회복조치들을 도출할 수 있다.

상세 HRA 분석은 예비 사고경위 정량화와 최종 사고경위 정량화 사이에 수행된다. 여기서는 편의상 예비 사고경위 정량화에 포함시켰다. 예비 사고경위 정량화가 끝나면, PSA 모델의 오류도 수정되며, 최종 정량화에 필요한 HRA 항목, 회복조치 등이 준비된다. 이로부터 사고경위 최소단절집합을 구하고, 인간 의존성 평가 및 회복조치 분석을 수행하면, 이 결과가 최종적인 사고경위별, 초기사건별, 전체 노심손상 최소단절집합 및 노심손상 빈도가 된다. 최종 사고경위 최소단절집합 및 노심손상 빈도가 구해진 후에는, 일반적으로 중요도 분석 및 불확실성 분석이 수행되고, 분석자의 필요에 따라 민감도 분석등이 수행되게 된다.

다음에서는 예비 사고경위 정량화 및 최종 사고경위 정량화의 개념 및 절차를 간단히 기술한다.

2. 예비 사고경위 정량화

앞에서 설명하였듯이 예비 사고경위 정량화는 전체 PSA 모델에 대한 점검 및 최종 정량화를 위한 자료 도출을 목적으로 수행된다. 여기서 중점을 둘 사항은 노심손상 최소단절집합을 구하는 절차를 확립하는 것과 PSA 모델 및 신뢰도자료의 오류 점검, 그리고 상세 HRA 분석 항목 및 회복조치 항목의 도출이다. 이중 노심손상 최소단절집합 계산은 최종사고경위 정량화에서도 같은 방법으로 반복된다.

다음은 예비 사고경위 정량화 절차를 나타낸 것이다. 이중 사고경위 최소단절집합 계산은 모든 PSA 모델 및 신뢰도 자료를 종합하여야 함으로 가장 복잡하며 그 분석 절차가 여러 단계에 걸쳐 확립되게 된다. 일단 분석절차가 확립되면 사고경위

최소단절집합 계산을 수행하는 Kcut 사용자 프로그램 화일들이 작성되므로 그 다음 분석부터는 상당히 간단하게 수행될 수 있다.

- 사고경위 최소단절집합 계산
  - 분류된 초기사건 검토
  - 사건수목 및 고장수목의 연결
    - ✓ 사건수목 및 사건수목에서 사용된 각 branch 검토
    - ✓ 각 branch 에 대한 논리 (기본사건 또는 고장수목) 검토
    - ✓ 사건수목의 특성에 따른 conditioning event 검토
  - 사고경위 정량화를 위한 Kcut 사용자 프로그램 작성
  - 사고경위에 대한 최소단절집합 계산
- 최소단절집합 검토 및 오류 수정
- 상세 HRA 항목 도출 및 분석
- 회복조치 항목 도출 및 분석

가. 사고경위 최소단절집합 계산

사고경위 최소단절집합 계산은 각 초기사건에 대한 사건수목의 노심손상 사고경위에 대한 최소단절집합을 계산하는 것이다. 이 과정은 PSA 모델의 핵심인 사건수목 및 고장수목을 모두 종합하여 분석을 수행하기 때문에 상당히 방대한 작업이며, 대체로 계산시간도 많이 소요된다.

사고경위 최소단절집합 계산을 하기전에 가장 먼저 할 일은 PSA 에서 어떠한 초기사건이 있는가를 파악하는 것이다. 예를 들면 영광 5,6 호기 PSA 의 경우 16 개의 초기사건이 선정되었으며, 이중 2 개의 초기사건은 초기사건이 발생하면 항시 노심손상이 발생하므로 따로 사건수목이 구성되지 않았다. 그 외 14 개 초기사건 각각에 대해 사건수목이 구성되었다.

초기사건을 검토하고 나면, 다음은 사건수목이 각 초기사건에 대해 어떻게 모델되었는가를 파악하여야 한다. 각 사건수목에 대해서는 초기사건은 무엇이며, 그후 사고전개가 어떻게 진행되는지, 초기사건의 특성에 따른 사건수목 및 계통 고장수목의 특성등을 검토하여야 한다.

다음은 이에 따라 사건수목의 분석을 위해 어떠한 모델이 사용되는 가를 파악하여야 하는데, 이 과정은 PSA 의 전체 모델의 연결 상황을 파악하여야 함으로 상당한 주의를 요한다.

현재 국내에서 사용되는 PSA 방법은 Small Event Tree / Large Fault Tree 방법을 사용한다. 노심손상 사고경위는 여러 branch 의 곱 (AND logic) 으로서 표현되며, 각 branch 는 대부분 고장수목으로서 모델 되며 특별한 경우에 기본사건으로 모델 되기도 한다. 따라서 하나의 사고경위에 대한 최소단절집합을 구하기 위해서는 여러 계통 고장수목을 연결하여야 한다. 사고경위 정량화에서 가장 중요한 것은 각 사건수목의 branch 에 대한 논리가 어떠한 고장수목들을 이용하여 모델 되었는가를 파악하는 것이다.

여기서 주의할 점은 각 branch 가 어떠한 고장수목의 정점사건이 사용되었다는 것 이외에도, 초기사건 및 사고경위에 따라 어떠한 조건이 사용되었는지를 파악하는 것이다. PSA 에 따라서는 모델을 간단히 하기 위해 conditioning event 를 사용하며, 이러한 경우는 하나의 정점사건이 여러 개의 논리를 나타낼 경우도 있다.

HRA 방법론에 따라 사고경위 정량화 방법이 변할 수 있다. 영광 5,6호기 PSA 에서는 예비 사고경위 정량화 수행 시 HRA 확률 값은 screening 값을 사용한다. HRA screening 값을 사용하면 그 값들이 상당히 높기 때문에 사고경위 최소단절집합 계산 시 계산시간이 상당히 많이 걸리게 된다.

다음은 파악된 정보를 이용하여 사고경위 정량화를 위한 Kcut 사용자 프로그램을 작성하고, Kcut 을 수행하여 최소단절집합을 구하는 작업이다.

위에서 설명한 과정에 따라 최소단절집합을 구하다 보면, 사건수목 모델 및 고장수목 모델이 제대로 연결되지 않은 경우도 발생할 수 있으며, 필요한 신뢰도 자료가 없는 경우도 발생한다. 이러한 오류를 모두 수정한 후에야, 예비적인 사고경위 최소단절집합을 구할 수 있다.

사건수목에서 각 branch 에 대한 정보를 파악하는 과정 및 사용자 프로그램을 작성하는 방법은 사고경위 정량화 방법에서 상세히 설명된다.

나. 최소단절집합 검토 및 오류 수정

예비적인 사고경위 최소단절집합이 구해지면, 다음은 각 사고경위별로 최소단절집합을 검토하여야 한다. 여기서는 각 최소단절집합이 각 사고경위의 의미에 맞게 나타나 있는지를 검토하고, 잘못되었으면 어떠한 모델 (사건수목 또는 고장수목 등) 이 잘못되었는지를 찾아야 한다. 또한 나타나야 할 최소단절집합이 나타나지 않는 경우도 모두 찾아내야 한다.

최소단절집합을 검토한 후 필요하다면 PSA 모델을 수정하여 최소단절집합을 재계산하여야 한다.

이 작업을 수행하기 위해서는 반드시 사건수목 및 계통 고장수목 등의 전체적인 PSA 모델을 파악하고 있어야 한다. 그렇지 않은 경우 최소단절집합만을 보고 모델의 오류를 찾아내기가 거의 불가능하다.

다. 상세 HRA 항목 도출 및 분석

예비 사고경위 최소단절집합 계산 후에 최소단절집합 등을 검토하여 상세 인간신뢰도 분석을 수행하여야 할 사건을 모두 도출하여야 한다. 이러한 인간오류 사건에 대해서는 상세 인간신뢰도 분석을 수행하여야 한다. 상세한 내용은 인간신뢰도 분석 절차에 따른다.

라. 회복조치 항목 도출

예비 사고경위 최소단절집합 계산 후에 최소단절집합을 검토하면서 어떠한 실패 사건을 운전원이 복구할 수 있는지를 검토한다. 회복조치 항목 도출에서 주요한 사항은 운전원이 실패한 사건을 복구할 수 있는지의 여부와 복구에 필요한 시간, 그리고 운전원에게 이용 가능한 시간 등의 파악이다. 대부분의 회복조치는 운전원 관련이므로 회복조치 확률은 인간신뢰도 분석가로부터 받아야 한다.

복구조치분석에 대해서는 뒤의 사고경위 정량화 방법에서 기본적인 방법론이 설명되어 있다.

3. 최종 사고경위 정량화

예비 사고경위 정량화가 끝나면 최종 정량화를 수행한다. 상세 HRA 분석을 반영하여 사고경위 최소단절집합을 구하고, 인간 의존성 평가 및 회복조치 분석을 수행하면, 이 결과가 최종적인 사고경위별, 초기사건별, 전체 노심손상 최소단절집합 및 노심손상 빈도가 된다.

그 후에 중요도 분석 및 불확실성 분석을 수행하게 된다.

가. 상세 HRA 결과를 이용한 사고경위 최소단절집합 계산

최종 사고경위 정량화에서 최소단절집합 계산 과정은 예비 사고경위 최소단절집합 계산 과정과 기본적으로 동일하다. 단, PSA 모델 및 신뢰도 자료를 종합, 오류 수정 등 많은 작업이 예비 사고경위 최소단절집합 계산 과정에서 확립되므로 최종 사고경위 정량화에서의 최소단절집합 계산은 비교적 단순하다. PSA 모델 검토 및 Kcut 사용자 프로그램 작성 등은 예비 정량화에서 확립된 것을 그대로 사용할 수 있으므로, 대부분의 경우 최종 단계에서는 단순히 상세 HRA 값만을 반영하여 계산을 수행하면 된다.

나. 인간 의존성 평가

운전원 행위 의존성은 하나의 최소단절집합에 두개 이상의 운전원 행위가 나타나는 경우에 적용된다. 첫번째 운전원 행위가 실패하면, 다음 운전원 행위의 실패 확률이 커질 수가 있다. 최소단절집합에서 두 개의 운전원 행위가 나타날 경우 두 번째 운전원 행위의 실패 확률이 커지게 되는 경우를 도출하고, 커지는 비율을 인간신뢰도 분석 방법론에 따라 계산하여야 한다.

이를 처리하는 방법은 PSA 방법론 및 사용하는 전산코드에 따라 변할 수 있다. 영광 5,6 PSA 에서는 한 최소단절집합에서 두 번째 운전원 행위에 해당하는 기본사건을 찾아 보다 높은 확률을 가지는 다른 기본사건으로 대치하는 방법을 사용하였다. Kcut 의 Rule-based recovery 기능을 이용하여 사고경위 최소단절집합을 수정함으로써 수행된다. 인간 의존성 평가의 예가 사고경위 정량화 방법에 주어져 있다.

다. 회복조치 분석

사고경위에 대한 최소단절집합이 구해지면 고장수목이나 사건수목에서 모델 되지 않은 운전원이 고장 난 기기를 복구하는 행위를 고려하여야 한다. 사고 전 또는 사고진행동안 고장 나거나 작동하지 않은 부품 또는 계통들을 사고진행동안 운전원이 이를 복구할 수가 있으므로 이를 고려하여야 한다.

회복조치 분석에서 주로 고려되는 사항은 상실된 소외전원 복구, 작동하지 않은 모터구동밸브의 수동 조작 등이다. 회복조치 분석 시 주요한 사항은, 기기의 복구 가능성과 운전원에게 이용 가능한 시간 등이다. 같은 기기에 대한 복구라 할지라도 사고진행에 따라 운전원에게 이용 가능한 시간이 달라진다. 또한 LOCA 등이 발생하여 격납용기가 오염되면, 격납용기내의 기기는 복구가 불가능하다.

사고경위 최소단절집합에서 원전의 설계 또는 운전 방법에 따라 현실적으로 나타날 수 없는 최소단절집합이 있다. 예를 들면 고압안전주입 펌프 두 대의 동시 보수가 최소단절집합에 나타나는데, 이는 기술사양서에 위배되므로 현실적으로 나타나지 않는다. 이러한 최소단절집합들을 Nonsense 최소단절집합이라고 부르며, 최종 최소단절집합에서 삭제되어야 한다. 이 작업은 Kcut 의 Delete Term 기능이나 Rule-Based Recovery 기능을 이용하여 수행될 수 있다. 여기서는 Nonsense 최소단절집합 삭제를 편의상 회복조치분석에 포함시켜 설명하였다.

라. 중요도 분석

회복조치분석까지 완료되어 최종적인 사고경위 최소단절집합이 구해지면 중요도분석 및 불확실성 분석이 수행된다. 중요도분석은 노심손상빈도에 어떠한 인자가 중요한

영향을 미치는 것인지를 파악하는 것으로서, 사고경위별 노심손상빈도, 초기사건별 노심손상빈도, 또는 전체 노심손상빈도등에서 어떠한 기본사건이나 또는 계통 등이 중요한 영향을 미치는 가를 평가한다.

기본사건에 대한 중요도 평가는 Kcut 에서 기본적으로 제공하며, 평가 척도로는 Fussell-Vesely 중요도, Risk Reduction Worth (RRW), Risk Achievement Worth (RAW), 세가지의 척도가 사용된다. 반면 계통에 대한 중요도 계산은 Kcut 에서 기본적으로 제공하지는 않으며, 사용자가 사용자 프로그램을 작성하여 계산을 수행하여야 한다.

중요도 평가 방법 및 그 척도에 대한 설명은 사고경위 정량화 방법에 설명되어 있다.

마. 불확실성 분석

불확실성 분석은 신뢰도 자료의 불확실성이 각 사고경위 노심손상빈도, 각 초기사건별 노심손상빈도 또는 전체노심손상빈도에 대해 어떠한 영향을 미치는 가를 평가하는 것이다.

신뢰도 자료의 불확실성이나 노심손상빈도의 불확실성 모두 확률 분포를 이용하여 표현된다. 현재 KIRAP 에서 각 기본사건에 대한 신뢰도 자료의 불확실성 분포함수로서는 Lognormal 분포만을 사용할 수 있다.

KIRAP 을 이용한 불확실성 분석에서는 크게 두 단계로 구분할 수 있다. 하나는 각 기본사건에 대한 분포함수를 입력하는 것이다. 이 과정은 PSA 모델링 단계에서 고장수목 구성 시 기본사건에 대한 자료를 입력하는 과정에서 수행되는 것이 일반적이나, PSA 에 따라서는 불확실성 분석 단계에서 수행되기도 한다.

신뢰도 자료가 확립되며 다음은 사고경위 또는 전체 노심손상빈도등에 대한 확률 분포를 계산하는 것이다. 노심손상 최소단절집합과 기본사건에 대한 확률분포함수가 주어지면, KIRAP 은 Monte Carlo 방법을 이용하여 노심손상빈도에 대한 확률 분포를 계산한다.

4. 문서화

사고경위 정량화를 수행한 결과로서 다음과 같은 내용이 문서화되는 것이 바람직하다.

- 전체 노심손상빈도
- 초기사건별 발생빈도 및 노심손상빈도

- 전체 노심손상빈도에 미치는 초기사건별 노심손상빈도 비율
- 최소단절집합 계산에 사용된 절삭치
- 초기사건별 주요 최소단절집합
- 주요 사고경위에 대한 주요 최소단절집합
- 각 기본사건의 중요도
- 각 주요계통의 중요도
- 불확실성 분석 결과

제3절 사고 경위 정량분석 소프트웨어 사용 방법

1. Kcut 사용법 개요

가. Kcut 기능 개요

Kcut 은 KIRAP 의 부 프로그램의 하나로서 주 기능이 최소단절집합 계산이다. Kcut 은 단순히 주어진 고장수목에 대한 최소단절집합 계산만이 아니라, 최소단절집합 출력, Logical Loop 를 가진 고장수목 분석, 고장수목 모듈화, 고장수목 들의 조합, Delete Term 등 매우 다양한 기능을 가지고 있다. 따라서 Kcut 의 기능을 이해할수록 사고경위 정량화를 쉽고 효율적으로 수행할 수 있다. 또한 사고경위 정량화 방법에 따라 고장수목 및 사건수목 모델링 방법이 변할 수 있으므로, PSA 수행 전에 Kcut 의 기본기능을 이해할 필요가 있다.

Kcut 의 주요기능은 다음과 같다.

- C 언어로 작성되었으며, DOS, Windows 95, Unix Workstation 에서 수행 가능
- 사용자 프로그램에 의해 수행
- 최소단절집합 계산
  - 기본적으로 Bottom-up 전개 방법을 개선하여 사용
  - Shannon decomposition 을 응용한 고장수목 단순화 기능
  - 고장수목 모듈화 기능
- Rule-Based Recovery 기능
- Logical Loop 를 가진 고장수목 분석
- Double Initiator 삭제 기능
- Complement event 를 사용 가능
- 최소단절집합 결과를 저장하였다가 재사용 가능
- SETS 코드와 같이 STOP, OMEGA, PHI, EXCEPT (EXCEPTNONCMP) option 사용 가능
- Delete term 기능
- 중요도 계산 기능
- 여러 개의 file 로부터 명령어들 읽을 수 있음

Kcut 을 사용할 때 다음과 같은 점을 주의하여야 한다.

- 다음과 같은 문자는 operator 로 인식되므로 사건 이름으로 사용할 수 없다

+ * , / ( ) . = $

- 각 명령어는 점 (.) 으로 마쳐야 한다.

Kcut 은 사용자 프로그램 화일에 들어있는 명령어들을 하나씩 읽어 들여 이를 수행한다. 명령어는 Boolean 식 (고장수목, 사고경위 논리, 최소단절집합) 을 읽는 것, 식들을 하나로 합치는 것, 최소단절집합을 계산하는 것, 최소단절집합을 출력하는 것, 회복조치 수행, Delete Term 수행, 최소단절집합을 file 에 저장하는 등이 있다. Kcut 의 명령어는 표 32에 주어져 있다.

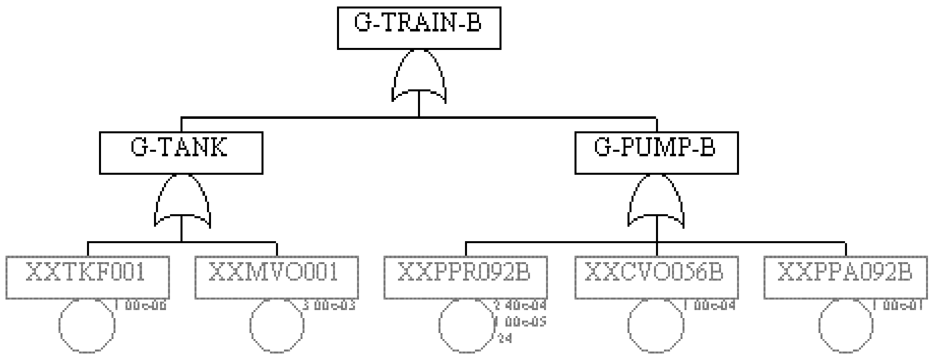
표 32. Kcut 명령어

명령어	설명
RdEqn	Read Equations
Equation	Read a equation
Value	Read probabilities for basic events
Deltrm	Delete cut sets
Prteqn	Report a equation in Boolean form
Wrteqn	Report a equation in Boolean form on a file to use the equation in another run
Comment	' Included between two symbols is a Comment ' ; Characters in a line after the symbol is a Comment
Read	Read commands from another file
Savetsv	Save all equations in a file, which can be reloaded
Loadtsv	Reload equations which are saved by Savetsv
Loadndb	Read probabilities of basic events from a NDB file
Genprg	Merge, Expand and Reduce a top event. It generates a set of commands which consists of Merge and Reduce, and Execute the set of commands.
Cutoff	Delete cut sets below the given cutoff value
RecoveryRule	Read Recovery Rules
Recovery	Process Rule-based Recovery
Merge	Build one equation from several equations
Reduce	Generate minimal cut sets
Import	Report minimal cut sets
Level	Determine the output quality
Uncert	Perform uncertainty analysis (Only available in Kcut - Uncertainty Analysis Version)

Kcut 의 각 명령어에 대한 사용법 및 설명은 Kcut 사용자 설명서[1] 에 주어져 있으므로, 여기서는 기본적인 개념에 대해 설명하도록 한다.

나. Boolean 식

Kcut 에서 고장수목, 사고경위 논리, 최소단절집합 등은 모두 Boolean 식으로 표현된다. 예로서 다음과 같은 고장수목이 있다고 하자.



이 고장수목에 있는 각 게이트는 다음과 같은 Boolean 식으로 표현될 수 있다.

```
G-TRAIN-B = G-TANK + G-PUMP-B.
G-TANK = XXTKF001 + XXMV0001.
G-PUMP-B = XXPPR092B + XXCV0056B + XXPPA092B.
```

또한 IE1사건발생 후에 계통 A 및 B 가 실패하면 노심손상에 이르는 사고경위가 있다고 하자.

이 사고경위는 다음과 같은 Boolean 식으로 표현될 수 있다. 여기서 SA 및 SB 는 계통 A, B 가 실패하는 사건을 나타낸다.

```
IE1-SEQ = IE1 * SA * SB.
```

이와 같이 Kcut 에서는 기본적으로 Boolean 식을 가지고 작업을 한다. 또한 고장수목, 사고경위는 물론 최소단절집합도 모두 Boolean 식으로 표현될 수 있기 때문에 Kcut 은 이들을 모두 처리할 수 있다.

다. 사용자 프로그램

원하는 결과를 얻기 위해서는 Kcut 의 명령어들을 적절하게 조합하여 Kcut 을 수행하여야 한다. Kcut 에서 이러한 명령어들의 집합을 사용자 프로그램이라고 부른다.

가장 기본적인 작업은 고장수목의 논리 및 신뢰도 자료를 읽어 들이고, 이에 대해 최소단절집합을 구하는 것이다. 다음은 Kcut 명령어의 예로서 Ex.Usr file 에 그 내용이 들어 있다고 하자. 처음은 고장수목의 논리를 Boolean 식의 형태로 읽어 들이는 것이고, 다음은 신뢰도 자료를 읽는 것이다. 다음 Merge 명령어는 TOP 이라는 정점사건에 대해 식들을 대치하여 하나의 식을 구하라는 것이며, Reduce 명령어는 절삭치 1.0e-6 으로 TOP 에 대해 최소단절집합을 계산하고 그 결과를 출력하라는 것이다.

```
File : EX.USR
TOP = GA * GB * GC. ; Boolean equation
GA = A + B + C + D + E.
GB = B + C + D + E + F.
GC = C + D + E + F + G.

VALUE.     ; Data
  0.01,  A, B, C.
  0.05,  D, E, F.
  0.001, G.
END.
```

```
MERGE (TOP).     ; Merge a Top Gate
REDUCE (TOP /PROBA * 1.0E-06 /REPORT).       ; Generate Cut Set
```

위와 같이 Kcut 사용자 프로그램에 해당하는 Ex.Usr 이라는 file 이 만들어지면, 다음과 같이 DOS prompt (Windows 95 의 DOS Box 도 무방함) 에서 Kcut 을 수행시킨다. 먼저 Kcut 에 대한 option 을 넣고 다음은 입력 file, 출력 file 이름들을 넣고 수행한다.

```
c:> Kcut -p  Ex.Usr  Ex.Coo
```

일반적으로 고장수목 논리 및 신뢰도 자료는 다른 file 에 저장되어 있다. 이러한 경우 Kcut 의 Read 명령어를 이용할 수 있다. 먼저 Ex.Cut 이라는 file 에 고장수목 논리 및 신뢰도 자료가 들어 있다고 하자.

```
File : EX.CUT
-----------------------------------------
TOP = GA * GB * GC.; Boolean equation
GA = A + B + C + D + E.
GB = B + C + D + E + F.
GC = C + D + E + F + G.

VALUE.     ; Data
  0.01,  A, B, C.
  0.05,  D, E, F.
  0.001, G.
END.
```

다음과 같이 사용자 프로그램을 작성하고 Kcut 을 수행시키면 된다.

```
File : EX.USR
-----------------------------------------
READ ("EX.CUT").    ; Read a Fault Tree Logic File
MERGE (TOP).     ; Merge a Top Gate
REDUCE (TOP /PROBA * 1.0E-06 /REPORT).       ; Generate Cut Set
```

위의 예제에서는 TOP 에 대한 최소단절집합을 구하기 위하여 Merge 및 Reduce 명령어를 사용하였다. 이들을 사용하는 대신 Genprg 명령어를 사용하는 것이 대부분의

경우 바람직하다. Genprg 명령어는 Bottom-Up Algorithm 에 따라 여러 개의 Merge 및 Reduce 들로 이루어지는 사용자 프로그램을 생성하고 이를 수행시켜 TOP 에 대한 최소단절집합을 구한다. 또한 Genprg 명령어는 Logical Loop 를 풀어야 할 경우나, 고장수목 모듈화 기능 등을 이용하려면 반드시 사용하여야 하는 명령어이다.

Genprg 명령어를 사용할 경우 다음과 같이 사용자 프로그램을 작성한다.

```
File : EX.USR
READ ("EX.CUT").    ; Read a Fault Tree Logic File
GENPRG  (TOP /PROBA * 1.0E-06 /REPORT).      ; Generate Cut Set
```

라. Double Initiator 삭제 기능

Kcut 은 Double initiator 삭제 기능을 가지고 있다. Double initiator 삭제란 초기사건이 두개 이상 곱해져 나오는 최소단절집합을 삭제하는 것이다.

많은 PSA 에서 하나의 계통 고장수목이 초기사건에 따라 논리가 변경되는 경우 각 초기사건마다 계통에 대한 고장수목을 따로 구성하는 대신에, 하나의 고장수목만을 구성하고 conditioning event (house event) 를 이용하여 각 초기사건에 따른 논리 변경을 처리한다.

예로서 A 라는 계통의 경우 초기사건 1 에 대해서는 Ta 와 같은 논리가 필요하고, 초기사건 2에 대해서는 Tb 와 같은 논리가 필요하다고 하자. 이러한 경우 그림 23과 같이 각 초기사건에 대해 고장수목을 각각 구성할 수가 있다. 예제 그림에서 보면 초기사건에 따라 G3a 또는 G3b 라는 논리가 사용되며 나머지 논리는 같다.

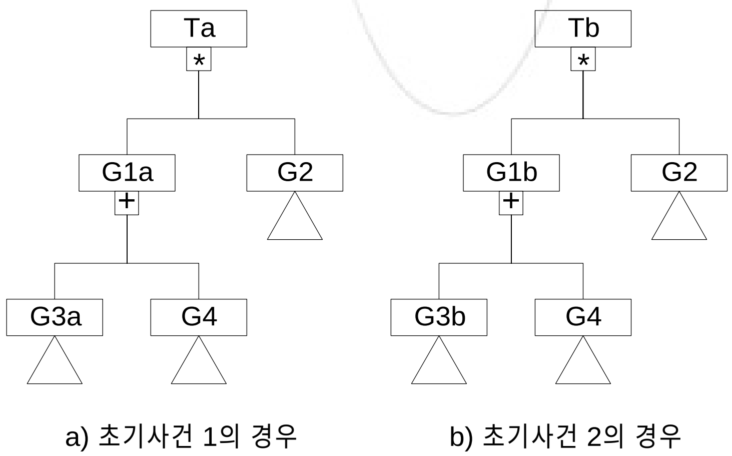


그림 23. 초기사건별 고장수목 논리

이러한 경우 G3a 및 G3b 외의 나머지 논리는 같기 때문에 각 초기사건마다 따로 고장수목을 구성하는 대신에 그림 24와 같이 conditioning event 를 사용하여 하나의 고장수목을 구성하는 방법을 사용할 수 있다.

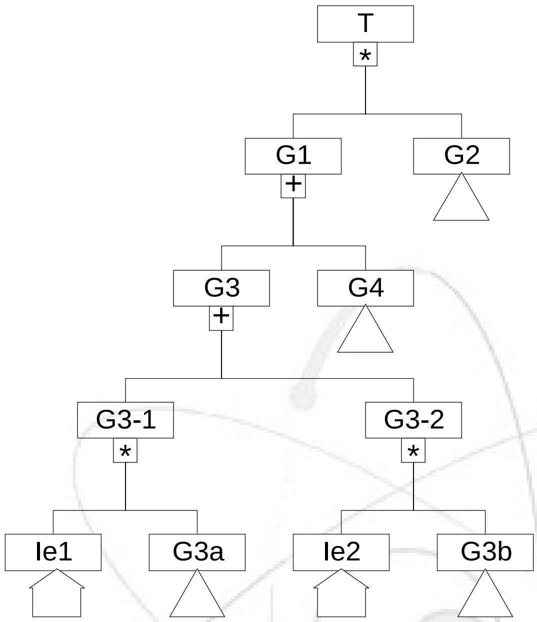


그림 24. 초기사건별 고장수목 논리

위의 고장수목에서 Ie1 을 True, Ie2 를 False 로 지정하면 게이트 G3 는 G3a 가 된다. 이 경우 고장수목 T 는 초기사건 1의 경우에 해당하는 고장수목 Ta 와 같게 된다. 마찬가지로 Ie2 를 True, Ie1 을 False 로 지정하면 게이트 G3 는 G3b 가 되어 고장수목 T 는 초기사건 2 에 필요한 고장수목 Tb 와 같게 된다.

많은 PSA 에서 위와 같이 conditioning event 를 이용하여 고장수목을 구성하는 노력을 줄이고 있다. 또한 이에 따라 각 초기사건마다 conditioning event 들을 적절하게 True 또는 False 로 지정하여 고장수목을 분석하고 있으므로, 하나의 고장수목에 대해 원칙적으로는 초기사건 수만큼 최소단절집합 계산을 수행하여야 할 수도 있다.

리스크 모니터용 PSA 모델의 경우 모든 초기사건에 대한 사건수목을 하나의 큰 고장수목으로 구성하는 것이 일반적이다. 이러한 경우 한 계통이 초기사건에 따라

약간씩 고장수목의 논리가 달라진다면 지금까지의 방법으로는 각기 다른 고장수목을 작성하여야 하며 리스크 모니터용 고장수목의 크기도 매우 커질 것이다.

Double initiator 삭제 기능은 이러한 경우에 유용하게 사용될 수 있다. 다음과 같은 예를 들어보자. 먼저 고장수목 Ta, Tb, T 를 Boolean 식으로 표현하면

Ta = G2 * (G3a + G4)

Tb = G2 * (G3b + G4)

T = G2 * (G4 + Ie1 * G3a + Ie2 * G3b)

가 된다. 여기서 초기사건 1을 Ie1, 초기사건 2 를 Ie2 로 각기 지정한다. 초기사건 1에 대해 Ie1-3, 초기사건 2에 대해 Ie2-3 과 같은 사고경위들을 가정하자.

Ie1-3 = Ie1 * T * SysB

Ie2-3 = Ie2 * T * SysB

Ie1-3 에서 T 는 게이트 Ta, Ie2-3 에서 T 는 게이트 Tb 를 사용한다면 Ie1-3 및 Ie2-3 은 다음과 같이 표현될 것이다.

Ie1-3 = Ie1 * (G2 * (G3a + G4)) * SysB

Ie2-3 = Ie2 * (G2 * (G3b + G4)) * SysB

이번에는 그대로 T 를 사용하여 보면 다음과 같이 된다.

Ie1-3 = Ie1 * (G2 * (G4 + Ie1 * G3a + Ie2 * G3b)) * SysB

Ie2-3 = Ie2 * (G2 * (G4 + Ie1 * G3a + Ie2 * G3b)) * SysB

이들을 각기 Ie1-3 는 Ie1 을 중심으로, Ie2-3 는 Ie2 를 중심으로 정리하여 보면 다음과 같이 된다.

Ie1-3 = Ie1 * (G2 * (G4 + G3a)) * SysB + Ie1 * (Ie2 * G3b) * SysB

Ie2-3 = Ie2 * (G2 * (G4 + G3b)) * SysB + Ie2 * (Ie1 * G3a) * SysB

위의 식에서 Ie1 과 Ie2 가 곱해진 항을 삭제하면 다음과 같이 된다.

Ie1-3 = Ie1 * (G2 * (G4 + G3a)) * SysB

Ie2-3 = Ie2 * (G2 * (G4 + G3b)) * SysB

이 결과는 Ie1-3 에 대해 Ta, Ie2-3 에 대해 Tb 를 사용한 결과와 같음을 알 수 있다. 따라서 여기서와 같은 방식으로 conditioning event 를 초기사건과 같은 이름으로 사용하고 double initiator 삭제 기능을 이용하면, 각 초기사건에 대해 계통고장수목을 재구성할 필요가 없으며, 하나의 계통 고장수목에서 conditioning event 를 사용한 경우 이를 각 초기사건마다 재분석할 필요 없이 한 번만 분석하여 여러 사건수목 분석에 사용할 수가 있다.

Genprg 명령어에서 주어진 정점사건에 대한 최소단절집합을 구하면서 double initiator 삭제 기능을 이용하고자 할 경우는 아래와 같이 Initiator option 다음에 Initiator 들을 나열하면 된다.

```
Genprg (TOP  /Proba * 1.0e-10  /Initiator * IE1, IE2 . . . . ).
```

마. 순환논리를 가진 고장수목 분석

Logical loop 를 형성하는 고장수목은 일반적인 PSA 에서 흔히 발생하는 일이다. 예로서 디젤발전기는 4.16 KV 버스에 전원을 공급하며, 4.16 KV 버스는 기기냉각수펌프등과 같은 주요 기기에 전원을 공급한다. 반면 디젤발전기의 냉각은 기기냉각수 펌프에 의해 이루어진다. 이와 같은 경우 고장수목의 모델이 logical loop 를 형성하게 된다. 이런 순환 논리는 최소 단절군을 구하기 위하여 반드시 해결 되어야만 한다.

순환논리는 다음과 같은 세가지 방법 중 하나를 사용하여 처리가 가능하다.

- 고장수목에서 순환논리를 삭제

  많은 PSA 에서 사용되는 방법으로서 순환 논리를 유발하는 부분을 갖지 않는 별도의 보조계통 고장 수목을 다시 작성하는 것이다. 그러나, 이 방법은 보조계통 간의 관계 검토, 이에 따른 별도 고장 수목의 재작성 등 추가적인 작업이 필요하며 또한 일부 최소 단절군이 생성되지 않는 약점을 갖고 있다.

- Iteration 방법

  Iteration 방법은 순환논리상에 있는 게이트들의 논리를 초기치를 가정한 후, iteration 방법에 의해 계속하여 이 들 게이트들의 해들 구해 나가는 것으로서 결과가 수렴할 때까지 반복한다. 이 방법은 한국원자력연구소에서 개발한 logical loop 를 가진 고장수목을 분석할 수 있는 방법론을 이용하여 올바른 해를

제공한다는 것이 검증되었다. 그러나 결과가 수렴할 때까지 여러 번의 반복 계산이 필요하다는 단점이 있다.

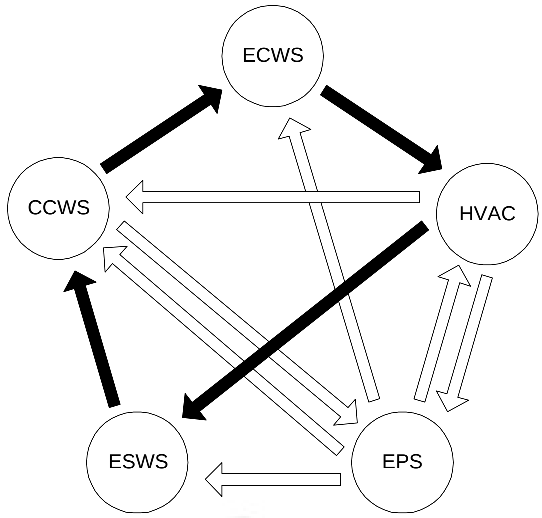
- Kcut 의 순환논리 해석 기능 이용

  Kcut 은 한국 원자력 연구소 (KAERI)에서 개발한 해석적으로 순환 논리를 푸는 방법 [3, 4] 에 따라 최소단절집합을 정확하게 계산하여 준다. 이 방법을 간단히 요약하면 고장수목을 전개하여 나가면서 무한 loop 를 형성하는 path 를 찾아 이를 삭제하는 방법으로서, 변환된 고장수목은 순환논리가 삭제되면서도 원래의 고장수목과는 같은 논리를 가지게 된다. 이 방법은 기존 방법의 약점을 극복하고 보조계통 고장 수목간의 순환 논리를 자동으로 풀 수 있다. 여기서 주의할 점은 이 방법론을 사용할 경우 변환된 고장수목의 크기가 커짐에 따라 계산시간이 크게 늘어나는 경향이 있다.

PSA 분석자는 위의 세가지 방법중 어느 하나를 선택할 수 있다. 단 방법론의 선택에 따라 PSA 모델링 방법이 결정된다는 것이 주의하여야 한다. 방법론에 따라 순환논리가 있는 경우와 그렇지 않은 경우에 고장수목 구성방법이 변하게 된다.

영광 5,6 호기 PSA 에서는 Kcut 의 순환논리 분석 기능을 이용하였다.

가압 경수로 보조계통의 고장 수목간에 나타나는 전형적인 순환 논리가 다음 그림에 나와 있다. 그림에서 검은 화살표로 표시된 바와 같이 ECWS는 HVAC을 보조하며, HVAC은 ESWS를, ESWS는 CCWS를, CCWS는 다시 ECWS를 보조하는 관계가 형성된다. 이와 같은 관계를 보조계통 간의 순환 논리라고 부른다.



ECWS: Essential Cooling Water System CCWS: Component Cooling Water System
ESWS: Essential Service Water System EPS: Electrical Power Distribution Syst.
HVAC: Heating, Ventilation and Air Conditioning System

그림 25. 계통간 순환논리의 예

기존의 방법에서는 이들 관계 중 가장 상관 관계가 적은 부분을 찾아 이를 무시하는 방법을 사용하여 왔다. 예를 들어, 위 그림에서 HVAC과 ESWS의 상관관계가 가장 적다면, 이를 무시하고 HVAC과 관계가 없는 것으로 가정한 상태에서 ESWS의 고장 수목을 다시 작성하여 이를 이용하여 순환 논리를 풀어왔다. 이와 같은 방법은 앞에서 언급한 바와 같이 보조계통 간의 관계를 검토하여 가장 관련이 적은 부분을 찾아 내야 하며, 이에 따른 별도의 고장 수목을 작성하여야 하는 등 추가적 작업을 필요로 하였다. 또한, 일부 최소 단절군이 생성되지 않는 약점을 갖고 있다. 즉, 위의 예에 따르면 HVAC과 ESWS의 관계가 무시되었으므로, HVAC의 고장에 의하여 유발되는 ECWS의 고장을 나타내는 최소 단절군은 이 경우에 나타나지 않게 된다.

KIRAP 코드에서는 어떤 정점사건 (Top Event)에 대하여 푼다고 할 때 그 정점사건을 하나의 출발 노드로 보고 이로부터 Top-Down/Depth-First 탐색 방법을 이용하여 모든 경로를 찾아내도록 하고 있다. 이와 같은 해석적 방법을 이용할 때 고장 수목이 어떻게 변하는 지가 다음의 그림 26와 그림 27에 나와 있다.

그림 26는 서로가 서로를 보조하는 세 개의 보조 계통 A, B 및 C가 있다고 할 때, 계통 A에 대한 고장 수목이다. 그림에서 사각 노드는 각 보조계통의 정점 사건을, 원형 노드는 기본 사건이나 게이트를 의미하며 네모들 중 빗금 쳐진 노드는 순환 논리를

유발하는 부분을 표시한다. 즉, 그림의 예에서는 A, B 및 C 3개의 계통이 상호간에 순환 논리를 유발한다. 따라서 기존의 방법에서는 A, B 및 C 모든 계통에 대하여 별도의 고장 수목을 작성하여야 했다. 그러나 개발된 방법에서는 코드가 이와 같은 순환 논리를 유발하는 부분을 자동으로 점검하여 그 부분을 삭제한다.

그림 26와 같은 순환 논리를 갖는 고장 수목을 해석적 방법으로 풀면 그림 27와 같이 순환 논리를 갖지 않는 고장 수목이 나타나게 된다. 이 고장 수목을 풀음으로써 A 계통에 대한 최소 단절군을 구하게 된다.

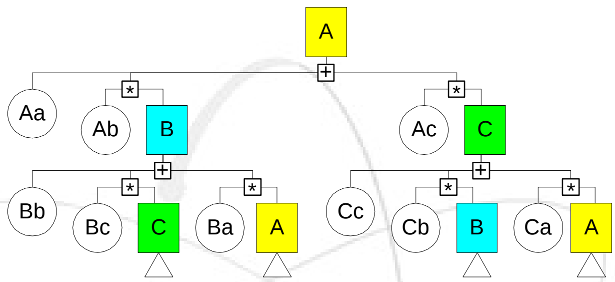


그림 26. 순환논리를 가진 고장수목

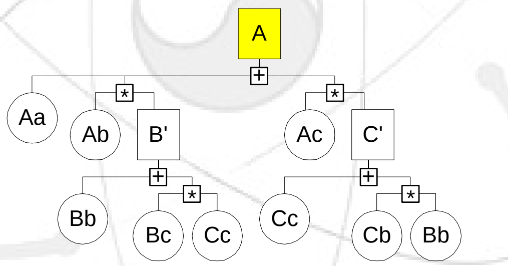


그림 27. 순환논리가 삭제된 고장수목

Genprg 명령어에서 주어진 정점사건이 Logical Loop 를 포함하고 있을 경우는 아래와 같이 LogicalLoop option 을 추가한다.

```
Genprg (TOP  /Proba * 1.0e-10  /LogicalLoop ).
```

바. 회복조치 분석

회복조치분석에서는 각 최소단절집합을 검토하고 이에 회복조치에 해당하는 기본사건을 추가하는 작업으로 이루어진다. 다시 말해 하나의 최소단절집합에 포함된 사건, 즉 어떤 기기의 고장을 사고 진행 중에 복구할 수 있다면 이를 복구하는 운전원 조치에 해당하는 기본사건을 이 최소단절집합에 추가하는 것이다.

예로서 (A, B) 라는 최소단절집합이 있을 때, A 는 'Pump A fails to start' 에, B 는 'Valve B fails to open' 에 해당한다고 하자. 어떤 사고경위에서 Valve B가 밸브 구동기의 문제로 작동되지 않았을 때 충분한 시간여유가 있다면 운전원이 현장에서 이를 수작업으로 열 수 있다. 이 운전원 조작 실패 사건을 R 이라 할 때 회복조치분석을 (A, B) 최소단절집합에 R 를 더해 (A, B, R) 로 수정한다.

이와 같은 회복조치분석은 계산된 각 최소단절집합을 수정하는 기능을 필요로 한다. Kcut에서는 Rule-Based Recovery 라는 기능을 가지고 있으며, 여러 가지 방법으로 최소단절집합들을 수정할 수 있도록 하고 있다.

Kcut 에서 회복조치 처리는 회복조치규칙 작성과 이를 적용한 회복조치분석 명령으로 이루어진다.

먼저 회복조치규칙을 다음과 같은 예와 같이 구성한다.

```
RecoveryRule.
   A, B + R1.
   A, C + R2 / CON2.
End.
CON2 = E + F.
```

여기서 회복조치규칙은 RecoveryRule. 과 End. 사이에 놓이게 된다. 각 회복조치규칙은 각기 한 줄을 차지하게 되며 각 항은 (,) 에 의해 구분되며 각 회복조치규칙은 (.) 으로 마친다. 하나의 회복조치 규칙에는 기본사건들의 조합과 회복조치를 합쳐 6개 이하의 항을 사용할 수 있다.

예로서 'A, B + R1.' 에서 A, B 는 기본사건들의 조합을 나타내며, + 다음의 R1 은 회복조치이다. 즉 A, B 를 포함하는 모든 최소단절집합들에 R1 이라는 회복조치를 추가하라는 것이다.

각 회복조치를 적용할 때 조건을 추가하고자 할 경우 (/) 다음에 Boolean 식의 이름을 추가한다. 'A, C, R2 / CON2.' 예에서 보면 A, C 를 포함하는 최소단절집합

중에서 식 CON2 에 포함된 최소단절집합들을 포함하지 않는 것에 대해 회복조치 R2 를 추가하라는 것이다.

다음의 회복조치 규칙들을 이용한 분석 예제는 아래와 같이 수행된다.

A, B + R1.
A, C + R2 / CON2.

먼저 회복조치 분석전의 최소단절집합들이 다음과 같다고 하자.

A B D
A B F
A C E G
A B C H
A C I

회복조치 분석후의 결과는 다음과 같이 된다.

A B D R1	A, B 를 포함 -> R1 추가
A B F R1	A, B 를 포함 -> R1 추가
A C E G	A, C 를 포함. 그러나 E 를 포함. 회복조치 없음.
A B C H R1 R2	A, B 를 포함 -> R1 추가 A, C 를 포함 -> R2 추가
A C I R2	A, C 를 포함 -> R2 추가

Kcut 에서 회복조치분석 수행 명령어는 다음과 같다.

```
Recovery (E1  [, E2]   /01  /02 .... ).
   0 =  REPORT * noset
      EVENT * noevent
      PROBA *  cutoff
```

Recovery 명령어에서는 식 E1 을 전개하여 각 최소단절집합에 대해 앞서 주어진 Recovery Rule 에 따라 회복조치 분석을 수행한다. 명령어에서 E2 가 주어지면 결과식은 E2 에 저장되며 그렇지 않을 경우에는 E1 에 다시 저장된다. 여기서 REPORT option 이 사용되면 회복조치분석후의 최소단절집합을 출력하며, EVENT option 이 사용되면 각

기본사건 중요도를 출력한다. 이때 noset 이나 noevent 가 주어지면 최소단절집합을 noset 개만큼만, 기본사건 중요도를 noevent 개만큼 출력하라는 것이다.

표 33은 Kcut 에서 사용할 수 있는 Recovery Rule의 종류와 방법을 정리한 것이다.

표 33. Recovery Rule 의 종류

Rule 종류	Rule 입력 양식 예제	예제 설명
Add Type	A , B + R1 .	A, B 를 포함하는 cut set 을 찾아 R1 을 추가. 즉, + 다음에 들어가는 사건들을 추가.
Replace Type	C , D / C1, D1 .	C, D를 포함하는 cut set 을 찾아 C, D를 C1, D1 으로 대체. 즉, / 전의 사건들을 / 다음의 사건들로 대체.
Equation Type	Eqn1 * R1 .	Eqn1 에 포함된 cut set 을 포함하는 cut set 을 찾아 R1 을 추가. 예로서 (A, B), (A, C), (B, D), (E, F) 등을 포함하는 cut set 에는 모두 R1 을 더하고자 한다면, 4 개의 Add Type Rule 이 필요하다. 이러한 경우 4 개 cut set 을 Equation 으로 만들면 간단히 처리할 수 있다.
Add Type with Condition	A , B + R1 / ConEqn1 .	기본적으로는 Add Type 과 같다. 단, A, B 를 포함하더라도 ConEqn1 에 포함된 cut set 을 포함하면 이 rule 을 적용하지 않는다. 초기사건 I1, I2 등에 대해서는 이 rule 을 적용하고 싶지 않은 경우 필요.
Replace Type with Condition	C , D / C1, D1 / ConEqn2 .	기본적으로 Replace Type 과 같다. 단 ConEqn2 에 포함된 cut set 을 포함하면 이 rule 을 적용하지 않는다.
Equation Type with Condition	E , F * Eqn1 / ConEqn3 .	기본적으로 Equation Type 과 같다. 단 ConEqn3 에 포함된 cut set 을 포함하면 이 rule 을 적용하지 않는다.

2. 사고경위 정량화 예제

가. 사고경위 정량화 개요

사고경위 정량화는 여러 가지 작업으로 이루어진다. 여기서는 사고경위 정량화에 필수적인 다음과 같은 방법들에 대해 간단한 예제 및 Kcut 사용자 프로그램 작성법을 함께 기술하였다.

- 초기사건 및 사건수목 검토
- 사건수목과 고장수목의 연결
  - 초기사건별 사건수목 및 사건수목에서 사용된 각 branch 검토
  - 각 branch 에 대한 논리 (기본사건 또는 고장수목) 검토
  - 사건수목의 특성에 따른 conditioning event 검토
- 사고경위에 대한 최소단절집합 계산
- 회복조치 방법
  - 운전원 의존성 평가
  - 회복조치 분석
  - Nonsense 최소단절집합 삭제
- 중요도 분석
- 불확실성 분석

나. 초기사건 및 사건수목 검토

사고경위 정량화를 시작하기 전에 분석가는 고려되는 초기사건들, 어떠한 초기사건에 대해 사건수목이 구성되었는지, 초기사건 발생빈도, 초기사건 특성들을 검토한다. 그리고 각 사건수목에 대해 사건수목 구성 논리 및 계통 고장수목과의 연관관계를 검토하여야 한다.

영광 5,6 호기 PSA 의 경우 표 34의 16 개 초기사건이 선정되었으며, 이중 2 개의 초기사건은 초기사건이 발생하면 안전계통의 작동유무에 관계없이 노심손상이 발생하므로 따로 사건수목이 구성되지 않는다. 그 외 14 개 초기사건 각각에 대해 사건수목이 구성된다.

표 34. 영광 5,6 호기 PSA 의 초기사건들

LL (Large LOCA)
ML (Medium LOCA)
SL (Small LOCA)
SGTR (Steam Generator Tube Rupture)
LSSB (Large Secondary Side break)
TRSN (General Transients)
LOFW (Loss of Feedwater)
LOCV (Loss of Condenser Vacuum)
LODC (Loss of a 125V DC Bus)

LOKV (Loss of a 4.16 KV Bus)
LOCCW (Loss of a CCW Train)
LOOP (Loss of Offsite Power)
SBO (Station Blackout)
ATWS (Anticipated Transients without Scram)
ISLOCA (Interfacinf Systems LOCA)
RV (Reactor Vessel Rupture)

초기사건이 선정되면 다음은 각 사건수목을 검토하여야 한다. 이 과정을 통하여 사건수목에서 사고경위가 개발된 기술적 근거를 파악하여야 한다. 특히 각 branch 에 대해 어떠한 계통, 운전원 행위 등이 모델 되었는지, 성공조건은 무엇인지를 검토하여야 한다.

다음은 영광 5,6 PSA 의 과도상태 (TRSN : General Transients) 에 대한 사건수목이다.

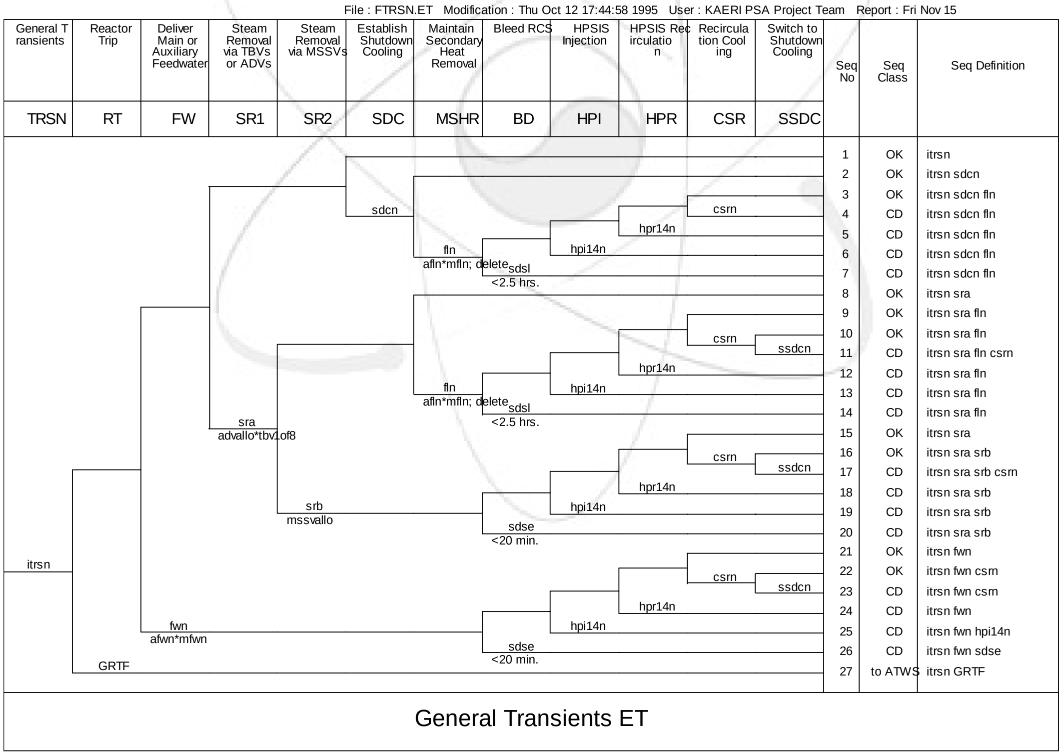


그림 28. 영광 5,6 호기 PSA 의 General Transients 사건수목

다. 사건수목과 고장수목의 연결

사건수목의 검토가 완료되면 각 branch 는 어떠한 모델을 사용하는 것인지를 정확하게 파악하여야 한다. 계통 고장수목은 사건수목의 각 branch를 통하여 사건수목과 연결된다. 하나의 사건수목 분석을 위해서도 거의 모든 계통 고장수목이 연결되어 분석되어야 하므로 분석자는 PSA 모델 전반에 대한 이해가 필요하다.

사건수목의 각 branch 에 대한 모델은 다음중 하나로 표현된다.

- 기본사건으로 표현 : Heading 이 운전원 조작이나 또는 어떠한 조건을 나타낼 때는 각 branch 는 대부분 기본사건이 된다. 이 경우 각 기본사건의 확률은 간단한 고장수목이나 인간신뢰도 분석 등을 통하여 계산된다.
- 고장수목으로 표현
  - 계통 고장수목으로 표현 : 각 branch 가 계통 실패 자체가 되는 경우이며, 이 때는 branch 논리가 계통 고장수목 분석에 포함된 정점사건을 바로 가리킨다.
  - 사건수목 보조논리로 표현 : 하나의 branch 에 대한 논리를 여러 계통 고장수목 및 운전원 조작 등이 조합으로 표현하여야 하는 경우이다. 이 때는 사건수목 보조논리라는 또 하나의 고장수목을 구성하여야 한다. 사건수목 보조논리의 경우 KIRAP 의 특성상 고장수목 대신 간단한 Boolean 식을 사용하기도 한다. 참고로 모든 고장수목은 Boolean 식으로 표현될 수 있다.
  - 여기서 계통 고장수목으로 표현하는 것이나, 사건수목 보조논리로 표현하는 것에 실제적으로 차이는 없다. 일부 PSA 에서는 사건수목 보조논리도 특수 기능에 대한 고장수목으로 나타내기도 한다.

보조논리를 사용하던, 계통 고장수목을 바로 사용 하던 간에 각 사건수목에 대한 사고경위 정량화를 들어가지 전에 점검해야 할 가장 중요한 사항은 각 branch 를 어떠한 논리로 표현하는 가를 파악하는 것이다. 경우에 따라서는 고장수목에서도 초기사건에 따른 조건 (conditioning event) 이 사용될 수 있으며, 이러한 경우는 단순히 고장수목의 정점사건 이름만을 파악하는 것 이외에도 conditioning event 등에 대한 정보도 파악하여야 한다.

결국 최종적으로 필요로 하는 것은 각 branch 에 대한 최소단절집합이라는 것은 명심하여야 한다.

다음은 영광 5,6 호기 PSA 의 General Transients 를 예제로 하여 각 branch 에 대한 논리를 점검하여 보았다.

표 35. 각 Branch 에 대한 논리

Branch ID	설명	논리
GRTF	Reactor Trip 실패	
FWN	이차측 급수 실패	AFWN * MFWN
SRA	TBV, ADV 를 이용한 Steam Removal 실패	ADVALLO * TBV1OF8
SRB	MSSV 를 이용한 Steam Removal 실패	MSSVALLO * TBV1OF8
SDCN	정지냉각계통 실패	SDCN
FLN	장기간동안 이차측 열제거 실패	AFLN * MFLN
SDSL	RCS 냉각수 방출 실패 (운전원 시간 여유 충분)	SDSL
SDSE	RCS 냉각수 방출 실패 (운전원 시간 여유 부족)	SDSE
HPI14N	안전주입 실패 (성공조건 : 1 of 4)	HPI14N
HPR14N	안전주입 재순환 모드 실패 (성공조건 : 1of 4)	HPR14N
CSRN	재순환시 살수계통을 이용한 잔열제거	CSRN
SSDCN	정지냉각계통 실패	SSDCN

위의 표에서 보면, FWN, SRA, SRB, FLN, 4 개의 branch 에 대해서는 보조논리가 사용되었으며, 다른 branch 들에 대해서는 계통 고장수목이 사용되었다. 다시 반복하지만 보조논리도 계통 고장수목의 형태로 모델될 수 있으므로 보조논리나 계통 고장수목에 차이를 둘 필요가 없다. 단지 PSA 모델링 시 분석자의 취향에 따라 모든 고장수목을 계통 단위로 구성하는가 또는 사건수목 branch 단위로 구성하는가 등이 결정된다.

다음은 표에 주어진 각 항목에 대해 이러한 논리가 어떠한 계통 고장수목으로부터 나왔는지를 점검한다. 각 branch 에 대해 계통 고장수목의 정점사건이 바로 사용되었다 하더라도, 이 논리, 즉 최소단절집합이 어떻게 생성되는 가를 파악하여야 한다.

PSA 에 따라서는 계통 고장수목의 정점사건이 바로 사건수목의 branch 의 논리를 그대로 나타낼 수도 있으나, 영광 5,6 PSA 경우에는 계통 고장수목의 정점사건이 사건수목의 branch 를 바로 표현하지는 않는다. 그 이유는 고장수목의 하나의 정점사건이 초기사건에 따라 다른 논리를 나타내는 경우가 있기 때문이다. 예로서 격납용기 살수계통 (CSS) 고장수목을 보면 GCSRCTOP 이라는 정점사건이 있다. GCSRCTOP

으로부터는 다음 표에 주어진 것과 같이 여러 가지의 다른 종류의 논리가 생성된다. 즉, General Transients 등의 초기사건에 대해서는 고장수목의 논리를 변경하지 않고 그대로 GCSRCTOP 를 사용하나, 소외전원상실, 4.16 Bus 실패 등으로 인한 초기사건의 경우에는 고장수목의 일부 사건을 True/False 로 하여 고장수목의 논리를 변경하여 사용한다.

표 36. 다수의 논리를 가지는 하나의 정점사건의 예

입력 정점사건	출력 정점사건	설명
GCSRCTOP	CSRN	일반적인 경우 사용
GCSRCTOP	CSRLOP	LOOP 의 경우 사용 PHI * GEOLOOP OMEGA * GNOAPRE, GNOBPRE, GNOPRE2M, GNOPRE2N, GNKPRE2M, GNKPRE2N option 을 사용하여 고장수목 논리 수정
GCSRCTOP	CSRAC	SBO 발생하고 AC power 복구 후에 사용 PHI * GEOLOOP, OMEGA * gekdgaaca, gekdgaacb option 사용
GCSRCTOP	CSRKV	Loss 4.16KV 경우 OMEGA * EKBSYSW01A option 을 사용
GCSRCTOP	CSRCCW	Loss of a CCW Train 경우 OMEGA * GCCTRA option 을 사용
GCSRCTOP	CSRDC	Loss of a 125 V DC 경우 OMEGA * EDBSYDC01A option 을 사용

이와 같이 하나의 정점사건으로부터도 여러 가지 다른 논리 (최소단절집합) 가 나타날 수 있다. 따라서 사건수목의 branch 에 대해 어떠한 고장수목이 사용되었는가를 파악하는 것 이외에도 궁극적으로는 최소단절집합이 어떻게 계산되었는가를 파악하는 것이 중요하다.

다음은 표 35에 나타난 항목들이 어떠한 고장수목의 정점사건으로부터 어떻게 최소단절집합이 계산되었는지를 파악한 것이다. General Transients 에서는 특정사건을 True 또는 False 로 대치하여 고장수목의 논리를 변경하는 경우는 없었으나, 다른 초기사건에 대해서는 특정사건을 True 또는 False 로 처리하는 경우가 발생할 수 있으므로 해당되는 사항들을 같이 점검하여야 한다.

표 37. 각 정점사건 설명

출력 사건 이름	설명	입력 정점사건
AFWN	AFWS	GAFTOP-N
AFLN	AFWS : Long Term Cooling	GMHTOP-N
CSRN	살수계통 재순환 모드	GCSRCTOP
HPI14N	HPIS Inejction Mode	GHSIGTOP
HPR14N	HPIS Recirculation Mode	GHSRGTOP
LPI14NS	LPIS Injection Mode	GLSIG104
LPR14N	LPIS Recirculation Mode	GLSRG104
MFWN	MFWS	GMFTOP
MFLN	MFWS : Long term	GMFTOPL
ADVALLO	ADV (1 of 4)	GMSADV1OF4
TBV1OF8	TBV (1 of 8)	GMSTBV1OF8
MSSVALLO	MSSV	GMSMSSVALLO
SDCN	Normal Shutdown Cooling	GSCGTOP
SDCDMDN	Shutdown Cooling (Only Demand Failure)	GSDCDMD
SDSE	SDS - Early Phase	GSDOE
SDSL	SDS - Late Phase	GSDOL
SSDCN	Shutdown Cooling after F&B	GMXSSDC

여기서 SDCDMDN 는 사건수목의 branch 를 나타내는 것은 아니며, 이 것은 특정 branch 의 논리에서 SDCDMDN 에 해당하는 경우를 제외하기 위해 사용된다.

라. 사고경위 정량화를 위한 Kcut 사용자 프로그램 작성

사건수목의 branch 에 대해 모든 논리가 파악되면 최소단절집합 계산을 시작할 수 있다. 각 사건수목에 대해 최소단절집합을 계산할 때 분석은 여러 단계로 나뉘어 수행될 수 있다. 영광 5,6 호기 PSA 에서는 이 분석이 다음과 같이 3 단계로 나뉘었다.

- 보조계통 정점사건에 대한 최소단절집합 계산, 그 결과를 저장
- Branch (front-line 계통 정점사건) 에 대한 최소단절집합 계산, 그 결과를 저장
- 각 사고경위에 대한 최소단절집합 계산

영광 5,6 호기 PSA 에서 위와 같이 3 단계로 나뉜 이유는 보조계통들간 순환논리 (Logical Loop) 를 먼저 처리하기 위해서 이다. 먼저 보조계통들에 대해 최소단절집합을 계산한 후 이 결과를 다음 branch 분석에 이용하였다.

PSA 에 따라서는 보조계통 분석을 따로 하지 않고 branch 분석, 각 사고경위에 대한 분석 2 단계로 나뉘기도 한다. 특이한 경우에는 branch 분석까지도 생략하고, 사건수목 분석 한 단계만을 수행하기도 한다.

중요한 것은 몇 단계를 이용하던 간에 분석 과정 자체는 변함이 없다는 것이다. 주요한 차이는 전산코드의 특성 및 PSA 모델링의 특성에 따라 중간 결과를 저장하여 두는 것이 전체적인 계산에 편리한가 아닌가 이다. 일부 전산코드의 경우에는 무조건 하나의 단계에서 분석을 수행하여야 하기도 하나, KIRAP 의 경우는 어떠한 방법을 선택하여도 모두 처리할 수 있다.

이러한 분석 단계를 나누는 것은 각 PSA 의 특성, 사용할 전산코드, 분석 방법, 분석자의 취향에 의해 결정된다.

분석자가 또 한가지 결정할 사항은 각 단계마다 어떠한 결과를 출력할 것인가 이다. 일반적으로 보조계통은 분석을 수행하더라도 결과를 따로 정리하지 않는다. Branch 에 대해서는 대부분 분석 결과가 정리되나, 극히 일부에서는 분석 결과를 정리하지 않을 경우도 있다. 사고경위 분석의 경우에는 예외 없이 결과가 정리된다.

다음은 branch 분석과 사고경위 분석의 두 단계로 나누었을 경우에 대해 사용자 프로그램을 작성하여 보았다. 이 과정은 다음과 같이 수행된다.

- 필요한 file 들을 읽는다.
- 각 branch 에 대한 최소단절집합 계산
- 각 사고경위에 대한 최소단절집합 계산 및 nonsense 최소단절집합 삭제

- 각 사고경위에 대한 최소단절집합 출력

(1) 필요한 file

필요한 file 들은 고장수목 논리를 저장하는 file 들, 신뢰도 자료 file 들, 그리고 기타 file 들로 이루어진다.

KIRAP 에서 고장수목의 논리는 대부분 Cut file 에 저장된다. 따라서 계산에 사용되는 모든 고장수목 file 들을 정리하여 Kcut 의 read 문으로 읽어 들여야 한다.

신뢰도 자료 file 들은 여러 가지 형태로 저장될 수 있다. 가장 기본적으로는 각 고장수목의 논리를 저장하는 Cut file 에 각 고장수목에 나타나는 기본사건에 대한 신뢰도 자료가 같이 저장된다. PSA 모델링을 하다 보면 하나의 기본사건이 여러 고장수목에 나타나는 경우가 있다. 만일 고장수목 논리 저장용 Cut file 만을 가지고 작업을 하면 이러한 기본사건의 경우 하나의 고장수목의 자료가 잘못되면 PSA 정량화가 잘못될 가능성이 있다.

또한 사고경위 정량화에는 고장수목에 나타나지 않는 사건 (회복조치 등의 사건) 도 많이 있으므로 이들에 대한 신뢰도 자료가 따로 정리될 필요가 있다.

따라서 대부분의 경우 모든 고장수목의 기본사건에 대한 자료를 하나의 file 로 모으고, 고장수목에 나타나지 않는 기본사건들을 추가하여 정리하고 관리하는 것이 바람직하다.

이와 같은 기본사건 신뢰도 자료 관리는 KIRAP 의 TDBEDIT 를 사용하면 된다. 단, 아직까지 TDBEDIT 는 DOS 용 KIRAP-TREE 의 고장수목 file 로부터만 기본사건 자료를 가져올 수 있으므로, Windows 용 고장수목 편집기인 KwTree 를 사용하여 고장수목을 구성할 경우에는 DOS 용으로 변환하여 사용하여야 한다.

TDBEDIT 는 필요한 신뢰도 자료를 두 가지 형태로 Kcut 에 제공할 수 있다. 하나는 TDBEDIT 의 데이터 베이스 file 인 NDB file 자체이며, 다른 하나는 TDBEDIT 내에서 출력하는 VAL file 이다. NDB file 은 기본사건의 이름, 설명, 신뢰도 자료 등 상세한 정보를 저장하며, VAL file 은 단지 신뢰도 자료 중 평균값만을 저장한다.

기타정보로는 PSA 마다 분석자가 추가하고 싶은 자료들이 있다. 영광 5,6 호기 PSA 에서는 주요 펌프실에 공조기의 고장을 모델 하였는데, 민감도 분석을 위하여 공조기 고장에 다른 기본사건들을 곱하였다. 즉, 이 모델은 공조기 고장 시 펌프 실패가 일어날 가능성을 곱한 것이다. PSA 기본 정량화에서는 공조기 실패가 바로 펌프 실패로 연결된다고 가정하여 분석을 수행하였으므로, 이를 공조기 고장에 곱해지는

사건들을 True 로 처리하였다. 이들 정보에 대한 file 을 고장수목 논리, 신뢰도 자료에 추가로 읽어 들였다.

다음은 필요한 file 들을 읽는 Kcut 의 명령어들이다.

```
read ("ft.usr"). ; Load Fault Tree Files
read("u34f.val").  ; Load Reliability Data
read("dyna-rm.dat").  ; Change HVAC Model
```

이중 ft.usr file 은 필요한 계통 고장수목 file 들을 읽는 명령어들을 포함하며 다음에 예제가 주어져 있다.

```
Read ( "cvcs.cut" ) .      ; CVCS
Read ( "ccws.cut" ) .      ; CCWS
Read ( "css.cut" ) .       ; CSS
Read ( "afws.cut" ) .      ; AFWS
Read ( "ecws.cut" ) .      ; ECWS
Read ( "eps.cut" ) .       ; Electrical Power System
Read ( "fs.cut" ) .        ; ESFAS, AFAS, ..
Read ( "hpsi.cut" ) .      ; High Pressure Injection System
Read ( "hvac.cut" ) .      ; HVAC
Read ( "ias.cut" ) .       ; Instrument Air System
Read ( "lpsi.cut" ) .      ; Low Pressure Injection System
Read ( "mfws.cut" ) .      ; Main Feedwater System
Read ( "mixft.cut" ) .     ; Branch Logics, etc.
Read ( "mss.cut" ) .       ; Main Steam System
Read ( "rcs.cut" ) .       ; RCS Pressure Control
Read ( "scs.cut" ) .       ; Shutdown Cooling System
Read ( "sds.cut" ) .       ; Safety Depressurization System
Read                       ; Steam Generator Blowdown System
                           ; SIT
                           ; special events
                           ; Service Water System
```

```
( "sgbds.cut" ) .
Read ( "sit.cut" ) .
Read
( "special.cut" ) .
Read ( "sws.cut" ) .
```

위에서 dyna-rm.dat 은 민감도 분석용으로 추가된 HVAC model 을 PSA 수행자체를 위한 모델로 수정하기 위한 것으로 그 내용은 다음과 같다.

```
AFMPR01AARM = omega.
AFMPR02BBRM = omega.
CCMPR01PA-RM = omega.
CCMPR02PA-RM = omega.
CCMPR01PB-RM = omega.
CCMPR02PB-RM = omega.
CSMPRCSSPA-RM = omega.
CSMPRCSSPB-RM = omega.
CVMPRCHGP1RM = omega.
CVMPRCHGP2RM = omega.
CVMPRCHGP3RM = omega.
CVMPRCHGP4RM = omega.
EGDGR01A-RM = omega.
EGDGR01E-RM = omega.
EGDGR01B-RM = omega.
HSMPR02BRM = omega.
HSMPR01ARM = omega.
LSMPRLPSI1RM = omega.
LSMPRLPSI2RM = omega.
SWMPR01PA-RM = omega.
SWMPR02PA-RM = omega.
SWMPR01PB-RM = omega.
SWMPR02PB-RM = omega.
```

(2) 각 branch 에 대한 최소단절집합 계산

사고경위 정량화에서 각 사고경위에 대한 최소단절집합을 구하기 위해서는 실패 branch 만이 아니라 성공 branch 에 대한 정보도 필요하다. 따라서 사건수목에 나타나는 모든 branch 에 대해 최소단절집합을 미리 구하는 것이 편리하다. 다음은 각 branch 에 대해 최소단절집합을 구하기 위한 Kcut 명령어의 예제이다.

```
; System & ET Support Logic
AFWN = GAFTOP-N.                ; AFWS
AFLN = GMHTOP-N.                ; AFWS : Long Term Cooling
CSRN = GCSRCTOP.                ; 살수계통 재순환 모드
HPI14N = GHSIGTOP.              ; HPIS Inejction Mode
HPR14N = GHSRGTOP.              ; HPIS Recirculation Mode
LPI14NS = GLSIG104.             ; LPIS Injection Mode
LPR14N = GLSRG104.              ; LPIS Recirculation Mode
MFWN = GMFTOP.                  ; MFWS
MFLN = GMFTOPL.                 ; MFWS :  Long term
ADVALLO = GMSADV1OF4.           ; ADV (1 of 4)
TBV1OF8 = GMSTBV1OF8.           ; TBV (1 of 8)
MSSVALLO = GMSMSSVALLO.         ; MSSV
SDCN = GSCGTOP.                 ; Normal Shutdown Cooling
SDCDMDN = GSDCDMD.              ; Shutdown Cooling (Only Demand
                                Failure)
SDSE = GSDOE.                   ; SDS  - Early Phase
SDSL = GSDOL.                   ; SDS - Late Phase
SSDCN = GMXSSDC.                ; Shutdown Cooling after F&B

FWN = AFWN * MFWN.              ; FW Supply
SRA = ADVALLO * TBV1OF8.        ; Steam Removal
SRB = MSSVALLO * TBV1OF8.       ; Steam Removal
FLN = AFLN * MFLN.              ; Long Term FW Supply

; Generate Cut Sets for each
Branch
genprg (FWN /opt0$).
genprg (SRA /opt0$).
```

```
genprg (SRB /opt0$ /Phi *
MSOPHSR).
genprg (FLN /opt0$).
genprg (SDCN /opt0$).
genprg (SDSL /opt0$).
genprg (SDSE /opt0$).
genprg (HPI14N /opt0$).
genprg (HPR14N /opt0$).
genprg (CSRN /opt0$).
genprg (SSDCN /opt0$).
```

(3) 각 사고경위에 대한 최소단절집합 계산 및 nonsense 최소단절집합 삭제

각 branch 에 대한 최소단절집합이 구해지면, 각 사고경위에 대해 최소단절집합 계산을 수행하게 된다.

사고경위별 최소단절집합 계산방법을 먼저 간단한 사건수목에 대해 설명한 후에 영광 5,6 P호기 PSA 의 General Transients 에 대한 계산방법을 제시하였다.

다음에 주어진 사건수목은 General Transients 사건수목을 단순화한 것이다. 이 사건수목을 가지고 실패 branch 들의 곱에 대한 최소단절집합 계산 및 성공 branch 들에 나타나는 최소단절집합을 삭제에 대해 살펴보겠다.

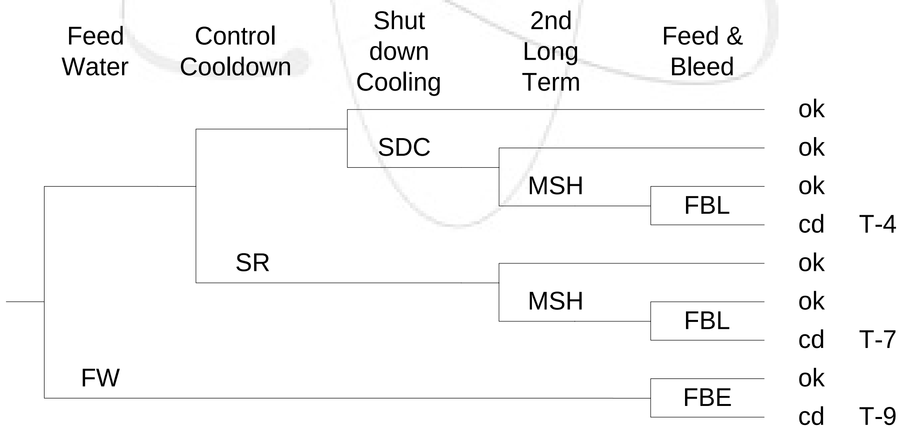


그림 29. 단순화된 사건수목 예제

위의 사건수목에서 노심손상이 발생하는 사고경위는 T-4, T-7, T-9 이 있다. 먼저 각 노심손상 사고경위에 대한 논리를 정확히 구성하면 다음과 같다.

```
T-4 = T * /FW * /SR * SDC * MSH * FBL.
T-7 = T * /FW * SR * MSH * FBL.
T-9 = T * FW * FBE.
```

여기서는 단순히 Boolean 식을 사용하여 사고경위에 대한 논리를 표현하였다. 사용자에 따라서는 사고경위 논리를 고장수목을 이용하여 표현하여도 무방하다. 위 식에서 /FW 와 같이 / 가 붙은 경우는 complement event 를 나타내며, 이들은 그 사고경위에서 성공 branch 에 해당한다. 반면 T-4 의 SDC, MSH, FBL 과 같은 경우는 실패 branch 에 해당한다.

각 사고경위에 대해 정확한 최소단절집합을 구하기 위해서는 위에 주어진 식에 각 branch 에 대한 최소단절집합을 대입하여 계산하여야 한다. 즉, complement 식에 대해서도 정확히 처리하여야 한다. 그러나 현실적으로 complement 식을 정확히 처리하여 계산하는 것은 현재 전산코드의 기능으로는 거의 불가능하다.

여기서 T-4 사고경위를 살펴보자. T-4 사고경위는 T 가 발생 후에 SDC, MSH, FBL 이 실패한 경우이다. 반면 FW 가 실패하면 T-4 사고경위로 진행되지 않고 T-8 또는 T-9 로 진행하게 되며, SR 이 실패하면 역시 T-4 사고경위로 진행되지 않고 T-5, T-6, 또는 T-7 사고경위로 진행하게 된다. 이로부터 다음과 같이 T-4 에 대해 최소단절집합을 구한다. 먼저 T-4 가 발생하는 실패 branch 들을 모델 한다. 다음, FW 및 SR 에 포함된 최소단절집합이 나타나면, 이들은 다른 사고경위로 진행하게 되므로 T-4 에서 삭제한다.

이 방법이 수학적으로 정확한 해를 제공하는 것은 아니지만 논리적으로 상당한 근사치를 제공하며, 많은 PSA 에서 사용하는 방법이다. 이 방법을 이용하면 다음과 같이 두 단계로 나뉘어 계산된다.

- 실패 blanch 들의 곱에 대한 최소단절집합 계산
- 위의 최소단절집합으로부터 성공 branch 들에 나타나는 최소단절집합을 삭제

성공 branch 를 삭제한 실패 branch 들의 곱은 다음과 같이 된다.

```
T-4 = T *  SDC * MSH * FBL.
T-7 = T * SR * MSH * FBL.
T-9 = T * FW * FBE.
```

성공 branch 들에 나타나는 최소단절집합을 삭제하는 방법은 Delete Term 이라는 방법을 이용하며 Kcut 명령어는 다음과 같이 된다.

```
Deltrm (T-4, FW, T-4).
Deltrm (T-4, SR, T-4).
Deltrm (T-7, FW, T-7).
```

위의 Deltrm (T-4, FW, T-4) 은 T-4 에서 FW 에 포함된 최소단절집합을 삭제하고, 그 결과를 T-4 에 다시 저장하라는 명령어이다.

CONPAS 의 ConEdit 에서는 실패 branch 들의 곱에 대한 최소단절집합 계산 및 성공 branch 에 나타나는 최소단절집합을 삭제하는 Kcut 명령어들을 생성하여 KSQ file 에 저장한다. 이 내용은 위에서 설명된 기본적인 방법에 따라 Kcut 명령어를 생성된 것이며, 경우에 따라서는 수정되어야 할 필요가 있다. 예를 들어 branch 가 기본사건으로 표현되는 경우에 이 것이 성공 branch 일지라도 이 것을 Deltrm 명령어를 사용할 필요가 없다. 참고로 ConEdit 에서는 PDS 가 ok 가 아닌 경우는 모두 노심손상 사고경위로 간주하고, 이에 대해 Kcut 명령어들을 생성한다.

다음은 영광 5,6 PSA 의 General Transients 의 사고경위들에 대해 ConEdit [2] 에 의해 생성된 KSQ file 을 수정한 것이며 수정한 부분은 ; 를 사용하여 주석처리가 되어 있다.

```
; <<  SEQUENCE SOLVER >> : TRSN-KSQ.USR File

ITRSN-4  =   ITRSN * SDCN * FLN * CSRN.
merge  (ITRSN-4 /opt0 $).  reduce (ITRSN-4  /opt0 $).
;Deltrm (ITRSN-4, GRTF, ITRSN-4).   ; Delete
Deltrm (ITRSN-4, FWN, ITRSN-4).
Deltrm (ITRSN-4, SRA, ITRSN-4).
Deltrm (ITRSN-4, SDSL, ITRSN-4).
Deltrm (ITRSN-4, HPI14N, ITRSN-4).
```

```
Deltrm (ITRSN-4, HPR14N, ITRSN-4).
Deltrm (ITRSN-4, SDCDMDN, ITRSN-4). ; Add
Import (ITRSN-4  /opt1 $).

ITRSN-5  =   ITRSN * SDCN * FLN * HPR14N.
merge  (ITRSN-5 /opt0 $).  reduce (ITRSN-5  /opt0 $).
;Deltrm (ITRSN-5, GRTF, ITRSN-5).
Deltrm (ITRSN-5, FWN, ITRSN-5).
Deltrm (ITRSN-5, SRA, ITRSN-5).
Deltrm (ITRSN-5, SDSL, ITRSN-5).
Deltrm (ITRSN-5, HPI14N, ITRSN-5).
Deltrm (ITRSN-5, SDCDMDN, ITRSN-5). ; Add
Import (ITRSN-5  /opt1 $).

ITRSN-6  =   ITRSN * SDCN * FLN * HPI14N.
merge  (ITRSN-6 /opt0 $).  reduce (ITRSN-6  /opt0 $).
;Deltrm (ITRSN-6, GRTF, ITRSN-6).
Deltrm (ITRSN-6, FWN, ITRSN-6).
Deltrm (ITRSN-6, SRA, ITRSN-6).
Deltrm (ITRSN-6, SDSL, ITRSN-6).
Deltrm (ITRSN-6, SDCDMDN, ITRSN-6). ; Add
Import (ITRSN-6  /opt1 $).

ITRSN-7  =   ITRSN * SDCN * FLN * SDSL.
merge  (ITRSN-7 /opt0 $).  reduce (ITRSN-7  /opt0 $).
;Deltrm (ITRSN-7, GRTF, ITRSN-7).
Deltrm (ITRSN-7, FWN, ITRSN-7).
Deltrm (ITRSN-7, SRA, ITRSN-7).
Deltrm (ITRSN-7, SDCDMDN, ITRSN-7). ; Add
Import (ITRSN-7  /opt1 $).

ITRSN-11  =   ITRSN * SRA * FLN * CSRN * SSDCN.
merge  (ITRSN-11 /opt0 $ /Phi * AFOPHPPSTART).  reduce (ITRSN-11  /opt0 $).
  ; Modify
;Deltrm (ITRSN-11, GRTF, ITRSN-11).
```

```
Deltrm (ITRSN-11, FWN, ITRSN-11).
Deltrm (ITRSN-11, SRB, ITRSN-11).
Deltrm (ITRSN-11, SDSL, ITRSN-11).
Deltrm (ITRSN-11, HPI14N, ITRSN-11).
Deltrm (ITRSN-11, HPR14N, ITRSN-11).
Import (ITRSN-11  /opt1 $).

ITRSN-12  =   ITRSN * SRA * FLN * HPR14N.
merge  (ITRSN-12 /opt0 $ /Phi * AFOPHPPSTART).  reduce (ITRSN-12  /opt0 $).
  ; Modify
;Deltrm (ITRSN-12, GRTF, ITRSN-12).
Deltrm (ITRSN-12, FWN, ITRSN-12).
Deltrm (ITRSN-12, SRB, ITRSN-12).
Deltrm (ITRSN-12, SDSL, ITRSN-12).
Deltrm (ITRSN-12, HPI14N, ITRSN-12).
Import (ITRSN-12  /opt1 $).

ITRSN-13  =   ITRSN * SRA * FLN * HPI14N.
merge  (ITRSN-13 /opt0 $ /Phi * AFOPHPPSTART).  reduce (ITRSN-13  /opt0 $).
  ; Modify
;Deltrm (ITRSN-13, GRTF, ITRSN-13).
Deltrm (ITRSN-13, FWN, ITRSN-13).
Deltrm (ITRSN-13, SRB, ITRSN-13).
Deltrm (ITRSN-13, SDSL, ITRSN-13).
Import (ITRSN-13  /opt1 $).

ITRSN-14  =   ITRSN * SRA * FLN * SDSL.
merge  (ITRSN-14 /opt0 $ /Phi * AFOPHPPSTART).  reduce (ITRSN-14  /opt0 $).
  ; Modify
;Deltrm (ITRSN-14, GRTF, ITRSN-14).
Deltrm (ITRSN-14, FWN, ITRSN-14).
Deltrm (ITRSN-14, SRB, ITRSN-14).
Import (ITRSN-14  /opt1 $).

ITRSN-17  =   ITRSN * SRA * SRB * CSRN * SSDCN.
```

```
merge  (ITRSN-17 /opt0 $).  reduce (ITRSN-17  /opt0 $).
;Deltrm (ITRSN-17, GRTF, ITRSN-17).
Deltrm (ITRSN-17, FWN, ITRSN-17).
Deltrm (ITRSN-17, SDSE, ITRSN-17).
Deltrm (ITRSN-17, HPI14N, ITRSN-17).
Deltrm (ITRSN-17, HPR14N, ITRSN-17).
Import (ITRSN-17  /opt1 $).

ITRSN-18  =   ITRSN * SRA * SRB * HPR14N.
merge  (ITRSN-18 /opt0 $).  reduce (ITRSN-18  /opt0 $).
;Deltrm (ITRSN-18, GRTF, ITRSN-18).
Deltrm (ITRSN-18, FWN, ITRSN-18).
Deltrm (ITRSN-18, SDSE, ITRSN-18).
Deltrm (ITRSN-18, HPI14N, ITRSN-18).
Import (ITRSN-18  /opt1 $).

ITRSN-19  =   ITRSN * SRA * SRB * HPI14N.
merge  (ITRSN-19 /opt0 $).  reduce (ITRSN-19  /opt0 $).
;Deltrm (ITRSN-19, GRTF, ITRSN-19).
Deltrm (ITRSN-19, FWN, ITRSN-19).
Deltrm (ITRSN-19, SDSE, ITRSN-19).
Import (ITRSN-19  /opt1 $).

ITRSN-20  =   ITRSN * SRA * SRB * SDSE.
merge  (ITRSN-20 /opt0 $).  reduce (ITRSN-20  /opt0 $).
;Deltrm (ITRSN-20, GRTF, ITRSN-20).
Deltrm (ITRSN-20, FWN, ITRSN-20).
Import (ITRSN-20  /opt1 $).

ITRSN-23  =   ITRSN * FWN * CSRN * SSDCN.
merge  (ITRSN-23 /opt0 $).  reduce (ITRSN-23  /opt0 $).
;Deltrm (ITRSN-23, GRTF, ITRSN-23).
Deltrm (ITRSN-23, SDSE, ITRSN-23).
Deltrm (ITRSN-23, HPI14N, ITRSN-23).
```

```
Deltrm (ITRSN-23, HPR14N, ITRSN-23).
Import (ITRSN-23  /opt1 $).

ITRSN-24  =   ITRSN * FWN * HPR14N.
merge  (ITRSN-24 /opt0 $).  reduce (ITRSN-24  /opt0 $).
;Deltrm (ITRSN-24, GRTF, ITRSN-24).
Deltrm (ITRSN-24, SDSE, ITRSN-24).
Deltrm (ITRSN-24, HPI14N, ITRSN-24).
Import (ITRSN-24  /opt1 $).

ITRSN-25  =   ITRSN * FWN * HPI14N.
merge  (ITRSN-25 /opt0 $).  reduce (ITRSN-25  /opt0 $).
;Deltrm (ITRSN-25, GRTF, ITRSN-25).
Deltrm (ITRSN-25, SDSE, ITRSN-25).
Import (ITRSN-25  /opt1 $).

ITRSN-26  =   ITRSN * FWN * SDSE.
merge  (ITRSN-26 /opt0 $).  reduce (ITRSN-26  /opt0 $).
;Deltrm (ITRSN-26, GRTF, ITRSN-26).
Import (ITRSN-26  /opt1 $).

;ITRSN-27  =   ITRSN * GRTF.
;merge  (ITRSN-27 /opt0 $).  reduce (ITRSN-27  /opt0 $).
;Import (ITRSN-27  /opt1 $).
```

여기서 주의할 점은 ConEdit 에서는 Opt0 및 Opt1 두 개의 macro 를 분석자가 입력할 수 있도록 Kcut 사용자 프로그램을 작성한다는 것이다. 이들 macro 로 대한 정의는 분석자가 추가하여야 한다. 분석에서 사용된 예는 다음과 같다.

```
Opt0$ = Proba * 1.0e-10 /LogicalLoop.
Opt1$ = Proba * 1.0e-10 /Report * 100 /Event * 10.
```

본 예제 계산에서는 1e-10 의 절삭치를 사용하였으며, 영광 5,6 PSA 에서는 1e-10 의 절삭치를 사용하였다. 절삭치를 선택하는 기준은 PSA 마다 다르다. 이 값은 최종 노심손상빈도의 값 및 최소단절집합 계산기 등의 능력을 고려하여 결정되어야 한다.

(4) **각 사고경위에 대한 최소단절집합 출력**

각 사고경위에 대한 최소단절집합이 구해지면 일반적으로 다음과 같은 작업이 필요하다.

- 각 사고경위에 대한 최소단절집합을 출력
- 초기사건 전체에 대한 최소단절집합 계산
- 계산된 최소단절집합을 추후 사용할 때를 대비하여 LNK file 에 저장

여기서 각 사고경위에 대한 최소단절집합 출력은 ConEdit 에서 생성되는 KSQ File 에 이미 포함되어 있다. 따라서 각 분석자는 다음과 같이 초기사건 전체에 대한 최소단절집합 계산 및 최소단절집합을 LNK file 에 저장하는 Kcut 명령어를 작성하면 된다.

```
; CDF for General Transient & Save Cut Sets on LNK File
Trsn = Itrsn-4 +  Itrsn-5 +  Itrsn-6 +  Itrsn-7 +  Itrsn-11 +
   Itrsn-12 + Itrsn-13 + Itrsn-14 + Itrsn-17 + Itrsn-18 +
   Itrsn-19 + Itrsn-20 + Itrsn-23 + Itrsn-24 + Itrsn-25 +
   Itrsn-26.
Merge (Trsn).
reduce (Trsn /Opt1$).

;write cutsets
wrteqn(Itrsn-4,  Itrsn-5,  Itrsn-6,  Itrsn-7,  Itrsn-11).
Wrteqn(Itrsn-12, Itrsn-13, Itrsn-14, Itrsn-17, Itrsn-18).
Wrteqn(Itrsn-19, Itrsn-20, Itrsn-23, Itrsn-24, Itrsn-25).
Wrteqn(Itrsn-26).
Wrteqn(TRSN).
```

(5) **최종 Kcut 사용자 프로그램**

위에서 설명한 바에 따라 최종적으로 작성된 Kcut 사용자 프로그램은 다음과 같다. 이중 각 사고경위에 대한 최소단절집합 계산 및 성공 branch 삭제는 Trsn-Ksq.Usr

이라는 file 에 포함시켰으며, 그 file 을 읽어서 명령어를 수행하게 된다. Trsn-Ksq.Usr file 의 내용은 앞에 주어져 있다.

```
;  General Transients

;  KSQ File 및 다른 곳에 사용되는 Macro
Opt0$ = Proba * 1.0e-10 /LogicalLoop.
Opt1$ = Proba * 1.0e-10 /Report * 100 /Event * 10.

; 필요한 File 을 읽음
read ("LoadFt.usr").  ; Load Fault Tree Files
read("Db\u34f.val").  ; Load Reliability Data
read("Db\dyna-rm.dat").  ; Change HVAC Model

; System & ET Support Logic
AFWN  = GAFTOP-N.   ; AFWS
AFLN  = GMHTOP-N.   ; AFWS : Long Term Cooling
CSRN  = GCSRCTOP.   ; 살수계통 재순환 모드
HPI14N = GHSIGTOP.    ; HPIS Inejction Mode
HPR14N = GHSRGTOP.    ; HPIS Recirculation Mode
LPI14NS = GLSIG104.   ; LPIS Injection Mode
LPR14N = GLSRG104.    ; LPIS Recirculation Mode
MFWN  = GMFTOP.       ; MFWS
MFLN  = GMFTOPL.    ; MFWS :  Long term
ADVALLO = GMSADV1OF4. ; ADV (1 of 4)
TBV1OF8 = GMSTBV1OF8. ; TBV (1 of 8)
MSSVALLO = GMSMSSVALLO.  ; MSSV
SDCN  = GSCGTOP.    ; Normal Shutdown Cooling
SDCDMDN = GSDCDMD.    ; Shutdown Cooling (Only Demand Failure)
SDSE  = GSDOE.      ; SDS  - Early Phase
SDSL  = GSDOL.      ; SDS - Late Phase
SSDCN = GMXSSDC.    ; Shutdown Cooling after F&B

FWN = AFWN * MFWN.       ; FW Supply
SRA = ADVALLO * TBV1OF8.    ; Steam Removal
```

```
SRB = MSSVALLO * TBV1OF8.   ; Steam Removal
FLN = AFLN * MFLN.        ; Long Term FW Supply

; Generate Cut Sets for each Branch
genprg (FWN /Opt0$).
genprg (SRA /Opt0$).
genprg (SRB /Opt0$ /Phi * MSOPHSR).
genprg (FLN /Opt0$).
genprg (SDCN /Opt0$).
genprg (SDSL /Opt0$).
genprg (SDSE /Opt0$).
genprg (HPI14N /Opt0$).
genprg (HPR14N /Opt0$).
genprg (CSRN /Opt0$).
genprg (SSDCN /Opt0$).

; Generate Minimal Cut Sets & Delete Success Logic
read ("Trsn-ksq.usr").

; CDF for General Transient & Save Cut Sets on LNK File
Trsn = Itrsn-4 +  Itrsn-5 +  Itrsn-6 +  Itrsn-7 +  Itrsn-11 +
   Itrsn-12 + Itrsn-13 + Itrsn-14 + Itrsn-17 + Itrsn-18 +
   Itrsn-19 + Itrsn-20 + Itrsn-23 + Itrsn-24 + Itrsn-25 +
   Itrsn-26.
merge (Trsn).
reduce (Trsn /Opt1$).

;write cutsets
wrteqn(Itrsn-4,  Itrsn-5,  Itrsn-6,  Itrsn-7,  Itrsn-11).
wrteqn(Itrsn-12, Itrsn-13, Itrsn-14, Itrsn-17, Itrsn-18).
wrteqn(Itrsn-19, Itrsn-20, Itrsn-23, Itrsn-24, Itrsn-25).
wrteqn(Itrsn-26).
wrteqn(TRSN).
```

마. 회복조치 분석

예비적인 사고경위에 대한 최소단절집합이 계산되면 사건수목이나 고장수목에서 모델하지 못한 사항들을 반영하여 이들 최소단절집합을 수정하여야 한다. 이러한 사항들로는 운전원의 실패사건 복구, 운전원 행위간의 의존성 평가, Nonsence 최소단절집합 삭제 등이 있다.

- 첫째는 일반적인 의미로서의 회복조치로서 어떠한 기기가 제대로 작동하지 않을 경우 운전원이 이 기기를 수동으로 작동시키는 행위, 소외전원 상실을 복구하는 행위 등을 포함한다.

- 두 번째는 운전원 행위의 의존성을 고려하는 것이다.예로서 두 개의 운전원 행위가 하나의 최소단절집합에 나타날 경우, 두 운전원 행위사이에는 의존성이 있을 수 있다. 이러한 경우 두개의 운전원 행위를 다른 사건으로 대치하여 정량화를 수행할 필요가 있는데 이러한 것이 회복조치 분석에서 처리될 수 있다. 물론 인간신뢰도 분석 방법론에 따라 이러한 처리방법의 필요성이 결정된다.

- 세 번째는 필요 없는 최소단절집합 삭제이다. 사고경위 최소단절집합에서 원전의 설계 또는 운전 방법에 따라 현실적으로 나타날 수 없는 최소단절집합이 있다. 이러한 최소단절집합들을 Nonsense 최소단절집합이라고 부르며, 최종 최소단절집합에서 삭제되어야 한다. 이 작업은 Kcut 의 Delete Term 기능이나 Rule-Based Recovery 기능을 이용하여 수행될 수 있다.

위의 세가지 사항은 PSA 마다 또는 분석가 및 사용하는 전산코드등에 따라 여러가지 방법으로 수행한다. Kcut 을 사용할 경우는 이들 세가지를 Kcut 의 rule-based recovery 기능에 의해 모두 처리될 수 있으므로, 이들을 모두 회복조치분석에서 설명하였다.

(1) 운전원 행위 의존성 평가

운전원 행위 의존성은 하나의 최소단절집합에 두개 이상의 운전원 행위가 나타나는 경우에 적용된다. 이들 운전원 행위에는 의존성이 있게 된다. 다시 말해 첫번째 운전원 행위가 실패하면, 다음 운전원 행위의 실패 확률이 커질수가 있다. 이러한 경우에는 Rule-Based Recovery 방법을 이용한다면, 최소단절집합에서 두 개의 운전원 행위가 나타나면 이 운전원 행위에 해당하는 기본사건들을 다른 기본사건들로 대치하고, 대치된 기본사건들의 확률을 높게 지정함으로써 처리될 수 있다.

운전원 행위 의존성 평가 방법 및 수정되는 인간오류 확률 등은 기본적으로 인간신뢰도 분석 방법론에 따라 수행되므로, 이 사항은 반드시 인간신뢰도 분석가가 방법론을 참조하여 수행하여야 한다.

다음은 영광 5,6 PSA 에서 사용된 운전원 행위 의존성 평가의 일부로서 Recovery Rule 의 형태로 주어져 있다.

```
; hra dependency rule
RecoveryRule /New.
AFOPHALTWT, SDOPHLATE / AFOPHALTWT, SDOPHLATE-HD1.
   ; AFW 수원 CST 고갈후에 운전원이 Alternate 수원을 연결하지 못하고, 다음 Feed & Bleed 운전을 실패하는 경우
AFOPHPPSTART, SDOPHLATE / AFOPHPPSTART, SDOPHLATE-HD2.
MSOPHSR, SDOPHEARLY, ITRSN / MSOPHSR-T, SDOPHEARLY-HD1T, ITRSN.
MSOPHSR, ITRSN / MSOPHSR-T, ITRSN /cond1.
end.

; Conditions
cond1 = MSOPHSR * SDOPHEARLY.
```

위의 예에 주어진 운전원 행위간의 의존성에 대한 설명이 표 38에 주어져 있다. 이 최소단절집합들을 사건수목과 같이 살펴보면, 그 행위들간에 의존성이 있다는 것을 쉽게 파악할 수 있다.

표 38. 운전원 행위 의존성

운전원 행위 최소단절집합	설명
AFOPHALTWT, SDOPHLATE	AFW 수원 CST 고갈 후에 운전원이 Alternate 수원을 연결하지 못하고, 다음 Feed & Bleed 운전을 실패하는 경우
AFOPHPPSTART, SDOPHLATE	Shutdown Cooling 실패 후 운전원이 AFW 를 재기동하지 못하고, 또한 Feed & Bleed 운전을 실패하는 경우
MSOPHSR, SDOPHEARLY, ITRSN	General Transients 발생 후에 운전원이 이차측을 통한 냉각을 적절히 시행하지 못하고, 또한 Feed & Bleed 운전을 실패하는 경우
MSOPHSR, ITRSN /cond1.	General Transients 발생 후에 운전원이 이차측을 통한 냉각을 적절히 시행하지 못한 경우. 단 운전원의 Feed & Bleed 운전 수행 실패를 포함하지 않는 경우

예비 사고경위 정량화 후에 분석자는 사건수목과 각 사고경위에 대한 최소단절집합을 검토하여 하나의 최소단절집합 내에 두개 이상의 운전원 행위가 나타날 경우 각 운전원 행위간의 의존성을 검토하여 이를 처리할 수 있는 규칙을 구성하여야 한다.

(2) 실패사건 회복조치 분석

실패사건에 대한 회복조치는 사고진행 도중에 운전원이 고장 난 기기 등을 수동으로 복구하는 작업을 나타낸다. 대부분의 PSA 에서는 이러한 사고 후 운전원의 행위 또는 계통 작동을 고장수목이나 사건수목에서 모델 하는 대신 회복조치로 고려하고 있다. 특히 운전원의 회복조치행위는 각 사고경위마다, 각 기기마다 다를 수 있기 때문에 고장수목에서 모델하기가 상당히 어려우며, 같은 기기에 대한 복구일지라고 사고경위마다 운전원 조치에 필요한 여유시간의 차이로 인해 이를 복구할 수 있는 가능성 및 방법이 다를 수 있다. 그러므로 이와 같은 사항은 회복조치 분석에서 별도로 취급하는 것이 편리하다.

회복조치 분석단계에서는 예비적인 사고경위 정량화가 완료된 후 사고경위 최소단절집합을 검토하고, 이로부터 어떠한 회복조치를 고려할 것인가를 분석자가 결정하고 이에 대한 회복조치 규칙을 구성하게 된다. 물론 사고경위 정량화 이전에 사건수목, 고장수목, 기기 및 계통의 운전 등을 파악하여 어느 정도 회복조치에 대한 개요는 파악할 수 있으나, 사고경위 최소단절집합을 검토하기 전에는 완벽한 규칙을 생성할 수 없다.

각 최소단절집합을 점검하면서 회복조치 규칙을 도출하다 보면 어떠한 기본사건들의 조합을 포함하는 최소단절집합에는 일정한 회복조치가 추가되는 경향을 발견할 수 있다. Rule-Based 회복조치분석에서는 어떠한 사건들의 조합에 어떠한 회복조치가 추가될 것인지를 나타내는 규칙을 정리하고 이를 표 형태로 작성하여 이로부터 분석을 수행하는 것이다.

일반적인 PSA 에서는 이상과 같은 대표적인 규칙의 유형을 찾아내고, 이에 따라 분석을 수행한다. 이 후 몇몇 특수한 경우에 대한 회복조치를 추가하는 것으로서 회복조치분석은 완료된다. 대부분의 경우 몇몇 대표적인 유형이 회복조치분석의 90 % 이상을 차지할 수 있다.

회복조치규칙을 구성할 때 규칙을 각 사고경위별로 구성하거나 또는 전체에 대해 규칙을 구성하여도 된다. 각 사고경위 별로 규칙을 작성하면, 초기사건에 따른 차이점을 고려할 필요가 없으며 해당 사고경위에 대한 규칙만을 고려하면 된다는 장점이 있으나, 수많은 사고경위에 대해 각기 규칙을 작성하여야 한다는 단점이 있다.

반면 전체에 대해 규칙을 작성하면, 초기사건에 따른 차이점을 명확하게 고려해야 한다는 단점이 있으나, 회복조치 규칙을 전체적인 관점에서 파악하여 규칙을 작성하고 이를 이용하여 모든 사고경위에 대한 회복조치 분석을 수행할 수 있다는 장점이 있다.

분석자는 각자의 판단에 따라 적절한 방법을 선택하면 된다. 참고로 영광 5,6 호기 PSA 에서는 기본적으로 각 사고경위별로 회복조치 규칙을 구성하고 분석을 수행하였다.

일반적으로 회복조치에는 다음과 같은 사항들이 주로 고려된다. 소외전원상실이 발생하였을 경우, 대부분의 경우 소외전원은 약 30분 이내에 복구되며 길어도 몇 시간 이내에 복구가 되는 것이 보통이다. 이 경우 운전원은 소외전원이 안전계통에 연결될 수 있도록 조치를 취하게 된다. 또한 다른 예로서 모터구동밸브의 모터고장이나 전원 상실로 인해 밸브가 작동하지 않은 경우에 운전원이 현장에서 수동으로 이 밸브를 조작할 수가 있다. 이러한 행위는 사고진행동안 노심손상 전까지 어느 정도 시간이 있는가, 또는 운전원이 이를 인식하는가, 실제로 이를 쉽게 복구할 수 있는 고장인가등에 따라 좌우된다. 이러한 가능성을 모두 반영하는 것이 회복조치 분석이다. 또 다른 예로서는 자동신호 고장 시 운전원이 수동으로 기동 시키는 행위 등이 있다.

실패사건에 대한 회복조치 평가 시 중요한 것은 운전원이 기기를 복구하는데 필요한 여유시간과 기기가 그 시간 내에 복구될 수가 있는가 이다. 이에 따라 회복조치가 추가되기도 하며, 그 실패확률이 인간신뢰도분석에 의해 결정된다.

표 39는 영광 5,6 호기 PSA 에서 사용된 회복조치 규칙을 검토하고 이를 단순화하여 전체에 대한 회복조치를 구성한 예이다. 각 회복조치 규칙에 대한 설명은 영광 5,6 호기 PSA 를 참고하기 바라며 여기서는 설명하지 않는다.

표 39. 사고경위 정량화를 위한 Kcut 사용자 프로그램

```
; Rule for Recovery of MOVs ------------------------------------

MV-LIST =     ; 모든 IE 에 적용
   AFMVW0043456Q + AFMVC0043AA + AFMVC0044BA +  AFMVW004344 +
   AFMV00046BB + AFMVW004446 + ;  AFWS
   CCMV00073A + CCMV00074B + CCMV00141A + CCMV00142B +
   CCMVWCSHX + CCMVWSDCHX + ; CCWS
   CSMV00035A + CSMV00036B +
   CSMVW3536 +       ; CSS V0035, V0036 Contt' Spray Isolation Valve

   HSMV00675A + HSMV00676B +       ; Sump Isolation Valves
```

```
; HSMVW67576 +  ; No recovery for Simultaneous failure of Sump Valves
  HSMV00321A + HSMV00331B + HSMVW32131 +  ; Hot Leg Injection Isolation VV
  HSMVW60304 + HSMV00604B + HSMV00603A + ; Hot Leg Injection Isolation VV

  MFMV0093 + MFMV0058 +    ; Startup Feedwater

  SCMVC0689A + SCMVC0690B + SCMVW68990 +
  SCMV00655A + SCMV00656B + SCMVW65556 +  ; SDC LOOP 1/2 from RCS
  SCMV00657A + SCMV00658B + SCMVW65758 +
  SCMV00693A + SCMV00694B + SCMVW69394 +
  SCMV00695A + SCMV00696B + SCMVW69596 .    Shutdown Cooling

MV-LIST-LPSI =     ; LPSI 관련으로 LL 에서 제외
  LSMVWG6123450 + LSMV06152A + LSMV06252B + LSMVWB6125 .

MV-LIST-HPSI =     ; HPSI 관련으로 ML 에서 제외
  HSMVW69899 + HSMVC0698B + HSMVC0699A . ; HPSI Pump Discharge

GIML = IML.     ; Conditioning
GILL = ILL.        ; Conditioning
GSDOPHEARLY =
  SDOPHEARLY + SDOPHLATE-HD1 + SDOPHEARLY-HD2 + SDOPHEARLY-HD1T.

MV-LIST-AFTK =     ; Pump - Tank Level interlock
  AFPTK005678 + AFPTK00678 +  AFPTY008BB + AFPTK00708 +
  AFPTY007AB + AFPTK00608 + AFPTY006BA .

RecoveryRule.
  MV-LIST * nr-mv.               ; MOV Recovery - 모든 경우에 적용
  MV-LIST-LPSI * nr-mv / GILL.   ; MOV Recovery - Large LOCA 이외에 적용
  MV-LIST-HPSI * nr-mv / GIML.   ; MOV Recovery - Medium LOCA 이외에 적용
  MV-LIST-AFTK * nr-afik .       ; AFW Pump/Tank Interlock 고장 Recovery
end.

; Rule for Recovery in case of LOOP ------------------------------
```

```
; AFTk Makeup => 18 hr
ILOOP-AFTK = ILOOP * (AFOPHALTWT + CDCV002186 + CDVV002187) .

; Initial => 1 hr
ILOOP-EP1HR-REC = ILOOP * EDBYW125DC.

RecoveryRule.
   ILOOP-AFTK * nr-ac18hr.
   ILOOP-EP1HR-REC * nr-ac1hr.
End.

; Rule for delete non SBO sequences ------------------------------
NonSbo = ILOOP * (NR-AC11HR + NR-AC7HR)
   * (EGDGK01ABET + EGDGR01A + EGDGR01B + EGDGR01E + EGDGK01ABD
      + EGDGK01AED + EGDGK01BED
      + HCCQKCCP + HDABKEXFAN + HDABKSUFAN).

recoveryrule.
   NonSbo * Phi.    ;  Non SBO cut sets 들을 삭제
end.
```

바. 중요도 분석

중요도분석은 계통 또는 노심손상빈도에 어떠한 인자가 중요한 영향을 미치는 것인지를 파악하는 것으로서, 계통 신뢰도, 사고경위별 노심손상빈도, 초기사건별 노심손상빈도, 또는 전체 노심손상 빈도등에서 어떠한 기본사건이나 또는 계통 등이 중요한 영향을 미치는 가를 평가하는 것이다.

Kcut 에서는 주어진 식 (최소단절집합으로서 계통 신뢰도, 사고경위별 노심손상빈도, 초기사건별 노심손상빈도, 또는 전체 노심손상 빈도 등을 표현하고 있음)에 대한 기본사건의 중요도 분석 기능을 기본적으로 제공한다.

Kcut 에서 사용되는 평가 척도로는 Fussell-Vesely (F-V) 중요도, Risk Reduction Worth (RRW), Risk Achievement Worth (RAW), 세가지가 있다.

먼저 각각에 대한 계산식은 다음과 같다.

```
F-V = (dPt / dEi) / (Pt / Ei)
RRW = Pt / (Pt | P (Ei) = 0)
RAW = (Pt | P (Ei) = 1) / Pt
```

위 식에서 Pt 는 주어진 식이며, Ei 는 i 번째 기본사건이 된다.

RRW 의 의미를 보면 주어진 기본사건의 고장확률이 0, 즉 이에 해당하는 기기의 고장이 없다고 가정하였을 때에 전체 값이 줄어드는 비이다. RRW 가 높을수록 개선효과가 크다는 것을 뜻하며, 어떠한 기기나 운전 절차 등이 개선되었을 때 큰 효과가 있는지를 파악할 때 사용될 수 있다.

RAW 는 주어진 기본사건의 고장확률이 1, 즉 이에 해당하는 기기가 고장 났다고 가정하였을 때에 전체 값이 늘어나는 비이다. RAW 가 높을수록 해당 기기의 고장이 큰 영향을 미친다는 것을 뜻하며, 해당 기기 등이 고장 나지 않도록 감시해야 하는 우선 순위 등을 파악할 때 사용될 수 있다.

F-V 는 주어진 기본사건이 주어진 식에 기여하는 정도를 나타내는 것으로서, 현재의 식에서 어떠한 기본사건이 크게 기여하는 가를 파악할 때 사용될 수 있다. F-V 가 큰 기본사건은 RRW 역시 크다.

기본사건에 대한 중요도 분석은 다음과 같이 Kcut 의 Import 명령어를 사용하면 된다.

```
; 필요한 file 들 (최소단절집합, 신뢰도 자료) 을 읽는다
Import (ITRSN-5 /Report * 100 /Event * 20).
  ; ITRSN-5 에 대해 중요도 분석결과를 출력. 단 기본사건에 대해서는 20
개까지만
  ; 중요도 분석 결과, 출력하고, 최소단절집합은 100 개까지 출력.
```

많은 PSA 에서 사고경위 노심손상빈도나 전체 노심손상빈도에 대해 계통의 중요도 분석이 수행된다. 계통 중요도 계산은 여러 기본사건들의 집합에 대해 계산을 수행하여야 함으로 단순하게 하나의 명령어로 수행할 수 없다.

계통중요도 분석을 수행할 때, 가장 먼저 하여야 할 일은 각 계통에 포함되는 기본사건들을 분류하는 일이다. 예로서 A 라는 계통에 포함되는 모든 기본사건들을 정리하고, B 라는 계통에 포함되는 모든 기본사건들을 정리하여야 한다. 영광 5,6 PSA 에서는 기본사건의 이름에 계통 코드가 포함되어 있으므로 계통별로 기본사건을 정리하는 것은 어렵지 않다.

다음은 하나의 계통에 포함된 모든 기본사건의 값을 0 으로 하여 원하는 대상에 대해 노심손상빈도를 재계산한다. 다음 그 계통에 포함된 모든 기본사건의 값을 1로 하여 노심손상빈도를 재계산한다. 이로부터 위에 주어진 식을 이용하여 그 계통에 대한 RRW 및 RAW 값을 계산할 수 있다.

사. 불확실성 분석

각 고장수목, 각 사고경위, 각 사건수목 및 전체 노심손상에 대한 최소단절집합이 구해지면 이들에 대한 (이를 모두 합쳐 간단히 노심손상이라고 하겠다) 정량분석을 수행하게 된다. 이 때 사용된 각 기본사건 자료의 불확실성 (Uncertainty) 때문에 노심손상 빈도에는 불확실성이 존재하므로 이들을 평가할 필요가 있다.

기본사건의 불확실성에는 여러 가지 원인이 있을 수 있는데 자료의 부족에서 오는 불확실성, 실제 자료를 analytic한 모델로 표현하면서 발생하는 불확실성, 자료 자체의 Random성 등이 있을 수 있다.

기본사건에서의 불확실성을 정량화 하는 실제적인 방법은 확률함수 (Probability Function) 나 확률밀도함수 (Probability Density Function : PDF) 를 사용하는 것이다. 예로서 많은 고장자료가 주어지면 이를 수학적으로 처리하여 Lognormal, Gamma, Weibull, Beta등의 PDF으로 나타낼 수도 있다.

일반적으로 PDF로서는 Lognormal 분포가 가장 널리 사용되고 있는데 그 이유로는 발생확률이 극히 낮고 분포가 넓을 때는 Lognormal 분포가 이를 취급하기 적절하다는 것과 WASH-1400 이후 대부분의 자료가 Lognormal로 주어졌다는 것이다.

노심손상에 대한 최소단절집합과 각 기본사건에 대한 분포함수가 주어지면 Monte Carlo 방법, DPD 방법, Moments 방법 등을 사용하여 노심손상 빈도의 분포함수를 구할 수 있으며 이를 불확실성의 정량화라고 흔히 이야기한다. 위의 방법 중 가장 널리 사용되는 방법은 Monte Carlo 방법이다.

Monte Carlo 방법을 이용한 불확실성 분석의 상세한 방법에 대해서는 KIRAP Release 2.0 사용자 설명서를 참고하면 된다.

KIRAP 을 이용하여 불확실성 분석을 사용할 때는 Kcut 중 Uncertainty Version 을 사용하면 된다.

이를 수행하기 전에 먼저 불확실성 분포를 포함하는 신뢰도 자료를 준비하여야 한다. 이 자료는 TDBEDIT 를 이용하여 준비될 수 있다. TDBEDIT 의 자료 file 인 NDB file 이나 임시로 생성하는 VAL file 에는 기본사건의 평균고장율과 Lognormal 분포의 error factor 가 같이 주어져 있다.

Kcut Uncertainty Version 을 이용할 경우 사용자 프로그램은 다음과 같은 식으로 준비한다. 여기서 Uncert 명령어가 불확실성 분석을 수행하라는 명령어이다.

```
;  Read Cut Sets for Core Damage Frequence
Read ("cdf.lnk").        ; 노심손상에 대한 최소단절집합을 저장하는 file
LoadNdb ("cdf.ndb").  ; 신뢰도 자료 file
Uncert (CDF /Sample * 1200).     ; 불확실성 분석을 수행
```

계산이 끝나면 Kcut 의 출력 file 에 Monte Carlo 계산의 결과인 5%, 50%, mean, 95% 값, Cumulative Distribution Function와 Probability Distribution Function 에 대한 자료가 저장된다.

서 지 정 보 양 식

수행기관보고서번호	위탁기관보고서번호	표준보고서번호	INIS 주제코드
KAERI/TR-2548/2003			

제목 / 부제	확률론적안전성평가(PSA) 수행절차서 / - 1단계 전출력 내부사건분석 -
연구책임자 및 부서명	정원대 (종합안전평가부)
연 구 자 및 부 서 명	이윤환, 황미정, 한상훈, 장승철, 강대일, 박진희, 양준언 김태운, 하재주, 진영호 (종합안전평가부)

출 판 지	대전	발행기관	한국원자력연구소	발행년	2003
페 이 지	225 p	도 표	있음(O), 없음( )	크 기	26 Cm.
참고사항	원자력 연구개발 중장기 과제				
공개여부	공개(O), 비공개( )		보고서종류	기술보고서	
비밀여부	대외비( ), __ 급비밀				
연구위탁기관			계약번호		

초록 (15-20줄내외)

본 기술보고서는 1단계 PSA 내부사건 분석 절차와 방법을 정리한 것이다. 한국원자력 연구소에서 한국 표준형 원전의 건설 및 운영 인허가와 관련하여 수행하였던 1단계 PSA의 분석 방법과 절차를 보고서로 만들었다. 1단계 PSA는 원자력발전소에서 발생할 수 있는 노심손상 사고 시나리오를 파악하고 그로 인한 노심손상 빈도를 평가하는 작업으로서, PSA에서 가장 기본적이고 핵심적인 업무이다. 따라서 PSA를 활용하는 실무 부서에서는 1단계 PSA가 가장 필요한 내용이며, 또한 최근에 활발히 논의되고 있는 위험도 정보 활용(Risk-Informed Application)에 직접적으로 사용되는 부분이다. 1단계 PSA는 크게 발전소 친숙화, 초기사건 분석, 사건수목 분석, 계통 고장수목 분석, 신뢰도 자료 분석, 그리고 정량 분석의 단계로 수행된다. 본 기술보고서에는 1단계 PSA의 전체적인 개요를 2장에서 소개하고 있으며, 3장에서부터 7장까지 앞에서 언급한 1단계 PSA의 기술적 단계를 차례로 다루고 있다. 각 단계의 기술적 업무에 필요한 방법과 수행 절차 그리고 참고문헌을 체계적으로 정리함으로써 PSA를 활용하고자 하는 실무자들에게 직접적인 도움을 줄 수 있도록 작성하였다. 본 기술보고서는 원자력발전소의 PSA를 직접 수행하거나 다루어야 하는 실무자를 대상으로 만든 것이나 PSA 결과를 검토하는 관리자나 규제 담당자에게도 적절한 지침으로 사용될 수 있다. 또한 본 보고서에서 소개하는 분석 방법과 절차는 화학공장과 같은 일반 산업체의 안전성 평가에도 유용하게 사용될 수 있을 것이다.

주제명키워드 (10단어내외)	확률론전안전성평가(PSA), PRA, PSA 절차서, 내부사건분석

BIBLIOGRAPHIC INFORMATION SHEET

Performing Org. Report No.	Sponsoring Org. Report No.	Stamdard Report No.	INIS Subject Code
KAERI/TR-2548/2003			

Title / Subtitle	Procedure for Conducting Probabilistic Safety Assessment / - Level I Full Power Internal Event Analysis -
Main Author and Dept.	Won-Dea Jung (Integrated Safety Assessment Division)
Researcher and Department	Y.H.Lee, M.J.Hwang, S.H.Han, S.C.Jang, D.I.Kang, J.H.Park, J.E.Yang, T.W.Kim, J.J.Ha, Y.H.Jin (Integrated Safety Assessment Division)

Publication Place	Daejeon	Publisher	KAERI	Publication Date	2003
Page	225 p.	Ill. & Tab.	Yes(O), No ( )	Size	26 Cm.
Note					
Open	Open(O), Closed( )	Report Type	Technical Report		
Classified	Restricted( ), ___Class Document				
Sponsoring Org.		Contract No.			

Abstract (15-20 Lines)

This report provides guidance on conducting a Level I PSA for internal events in NPPs, which is based on the method and procedure that was used in the PSA for the design of Korea Standard Nuclear Plants (KSNPs). Level I PSA is to delineate the accident sequences leading to core damage and to estimate their frequencies. It has been directly used for assessing and modifying the system safety and reliability as a key and base part of PSA. Also, Level I PSA provides insights into design weakness and into ways of preventing core damage, which in most cases is the precursor to accidents leading to major accidents. So Level I PSA has been used as the essential technical bases for risk-informed application in NPPs. The report consists six major procedural steps for Level I PSA; familiarization of plant, initiating event analysis, event tree analysis, system fault tree analysis, reliability data analysis, and accident sequence quantification.

The report is intended to assist technical persons performing Level I PSA for NPPs. A particular aim is to promote a standardized framework, terminology and form of documentation for PSAs. On the other hand, this report would be useful for the managers or regulatory persons related to risk-informed regulation, and also for conducting PSA for other industries.

Subject Keywords (About 10 words)	Probabilistic Safety Assessment, PSA, PRA, PSA Procedure, Level I Internal Event Analysis