GOVP1200512360

최종연구보고서

KAERI/RR-2537/2004

원자력 위험도 관리 기술 개발
Development of Nuclear Risk Management Technology

정지/저출력 및 디지털 계통의 위험도 평가 기술 개발
Development of Risk Assessment Technology for Low Power, Shutdown and Digital I&C Systems

연구기관

한국원자력연구소

과 학 기 술 부

제 출 문

과 학 기 술 부 장 관 귀하

본 보고서를 "원자력 위험도 관리 기술 개발"과제 (세부과제 "정지/저출력 및 디지털 계통의 위험도 평가 기술 개발")의 최종보고서로 제출합니다.

2005. 4.

연 구 기 관 명 : 한국원자력연구소

연 구 책 임 자 : 장 승 철

연 구 원 : 강현국, 임호곤, 박진희,
김태운, 엄흥섭, 하재주

최종연구보고서 초록

<table>
<tr><td>과제관리
번호</td><td></td><td>해당당계
연구기관</td><td colspan="2">한국원자력연구소</td><td>단계구분</td><td colspan="2">2/3</td></tr>
<tr><td rowspan="2">연구사업명</td><td>중 사 업 명</td><td colspan="6">원자력연구개발 중장기계획사업</td></tr>
<tr><td>세부 사업명</td><td colspan="6"></td></tr>
<tr><td rowspan="2">연구과제명</td><td>대과제명</td><td colspan="6">원자력 위험도 관리 기술 개발</td></tr>
<tr><td>세부과제명</td><td colspan="6">정지/저출력 및 디지털 계통의 위험도 평가 기술 개발</td></tr>
<tr><td>연구기관명
(연구책임자)</td><td>한국원자력
연구소
(장승철)</td><td>해당단계
연구인력</td><td>내부 : 11.28M·Y
외부 : 0 M·Y
계 : 11.28M·Y</td><td>연구비</td><td colspan="2">정부: 1,267,000 천원
민간: 0 천원
계: 1,267,000 천원</td></tr>
<tr><td>위탁연구</td><td colspan="7">연구기관: 한국과학기술원 연구책임자: 성풍현</td></tr>
<tr><td>국제공동연구</td><td colspan="5">상대국명: 상대국연구기관명:</td><td>참여기업</td><td></td></tr>
<tr><td>색 인 어
(각 5개
이상)</td><td colspan="7">한글: 위험도, 안전성, 신뢰도, 확률론적 안전성 평가, 정지, 저출력, 디지털 계측제어, 소프트웨어
영어: Risk, Safety, Reliability, PSA (or PRA), Shutdown, Low power, Digital I&C, Software</td></tr>
<tr><td colspan="6">요약(연구결과를 중심으로 개조식 500자 이내)</td><td>면수</td><td>246면</td></tr>
</table>

1. 연구개발목표 및 내용

○ 위험도 정보 활용 의사결정이 가능한 정지/저출력(LPSD) 1단계 내부사건 PSA 표준 모델 개발
○ LPSD 안전성 향상을 위한 위험도 관리 기반 기술 개발
○ 디지털 I&C 안전성 입증을 위한 디지털 계통의 발전소 안전성 영향 평가 모델 개발
○ 디지털 I&C PSA 수행 기술 확보를 위한 안전-필수 요소 평가 기술 개발

2. 연구결과

○ LPSD PSA 표준 모델 개발
  - 표준원전 LPSD PSA 모델 등급 평가 및 개선 방안 도출
  - ANS II 등급 수준의 LPSD PSA 모델 개선 (8개 중 4개 분석 분야)
○ LPSD 위험도 관리 기반 기술 개발
  - LPSD 초기사건 DB 구축 (총 625건) 및 검색/분석 프로그램 (LEDB) 개발
  - LPSD 기기 배열 위험도 관리 (CRM)용 시범 모델 구축 및 평가
○ 디지털 안전 계통의 발전소 안전성 영향 평가 모델 개발
  - 디지털 발전소 보호계통(DPPS) 및 공학적 안전설비 작동계통(DESFAS)의 신뢰도 상세 평가 모델
  - 디지털 원전 안전성 영향 평가용 노심손상빈도(CDF) 및 조기대량방출빈도(LERF) 모델
○ 디지털 안전-필수 요소 평가 기술개발
  - 디지털 기기의 공통원인고장(CCF) 평가 방법론 연구 (디지털 CCF 그룹핑 기법)
  - 안전필수 소프트웨어 신뢰도 분석 방법론 및 원전 시범 적용 연구 (BBN 시범 적용 모델)
  - 고장내구성 기법의 고장 검출 범위 정량화 평가 방법론 개발 (Hybrid 평가 모형)

3. 기대효과 및 활용방안

○ LPSD 위험도 정보 활용 의사결정을 위한 PSA 모델의 기술적 적합성 판단 기준으로 모델 활용
○ 열수력 분석 체계를 비롯한 LPSD PSA 개선 모델은 표준원전 CRM 모델의 입력으로 직접 활용
○ LPSD 운전 중 초기사건 발생 저감을 위한 기초 자료로 LEDB 활용
○ 디지털 계통의 안전성 영향 평가 모델은 설계 개선 및 인허가에 활용
○ 차세대 원전의 디지털 I&C PSA 기술 확립(수행절차서 작성)을 위한 방법론으로 활용

요 약 문

Ⅰ. 제 목

정지/저출력 및 디지털 계통의 위험도 평가 기술 개발

Ⅱ. 연구개발의 목적 및 필요성

최근까지의 원자력 발전소 운전 경험과 PSA 결과에 따르면, 정지/저출력 위험도가 전출력 위험도에 비해 결코 적지 않음을 알 수 있다. 정지/저출력 운전 기간 동안에는 많은 정비 활동으로 인한 다중방어 개념 약화, 위험도 관리 부족 등의 원인으로 안전성 저하가 초래될 수 있으므로 위험도 정보 활용 기술의 이용 확대라는 시대적 흐름에 따라 원전 전 운전주기에 대한 위험도 관리가 필수적이다. 그러나 정지/저출력 운전모드에서는 출력 운전과는 달리 다양한 기기배열로 인해 정지/저출력 PSA는 그 수행 방법이 매우 복잡하여 아직 통일된 방법론이 정립되어 있지 않은 상태에 있다. 특히, 정지/저출력 위험도 평가 결과의 불확실성이 상대적으로 크기 때문에 위험도 정보를 활용한 의사결정을 지원하기 위해서는 불확실성이 저감된 보다 현실적인 위험도 정보를 제공할 수 있도록 기술의 개선이 함께 요구된다.

원전 계측제어 계통은 기존의 아날로그 회로로 구성된 원전 계측제어(I&C) 계통의 노후화로 열화와 품귀 문제가 점차 심각해지고 유지보수의 효율화, 편차(drift) 제거 등 저비용 고효율의 장점을 갖는 디지털 기술의 눈부신 발전에 따라 원전의 안전 기능에서도 디지털 계통이 도입되거나 디지털로의 대체가 고려되고 있는 것이 세계적 추세이다. 이에 따라, 안전기능에 적용되는 디지털 기기/계통에 대한 안전성 입증이 요구되나, 이를 위한 디지털 계통의 위험도 정량 평가 방법론은 초기 개발 단계에 있어 명확한 체계 및 방법론이 정립되어 있지 못한 상태이므로 매우 시급한 세계적 현안 문제가 되고 있는 실정이다. 특히, 국내에서는 최근 상업 운전을 시작한 울진 5,6 호기를 선두로 안전 관련 디지털 I&C 계통이 이미 도입되었으며, 이와 같은 디지털 기술의 조기 도입으로 인해 국내 원전의 안전성 입증이라는 관점에서

디지털 기기/계통의 정량적 안전성 평가 방법론 개발은 더욱 시급한 국내 현안 문제로 다룰 수밖에 없는 상황이다.

이에 따라, 본 과제와 관련한 2단계(2002.4 - 2005.2; 2년 11개월) 및 3단계(2005.3 - 2007.2; 2년)의 최종 연구 목적은 (1) 정지/저출력 위험도 평가 및 관리 기술 개발, (2) 디지털 계측제어 계통의 위험도 평가 기술 개발에 있다. 보다 구체적으로는 전자의 경우 표준원전에 대하여 ANS II 등급[1]을 충족하는 운전모드별 기기 배열 위험도 관리 모델의 개발을 통하여 정지/저출력 운전모드의 정량적 위험도 관리 기술을 확보하는 것을 목적으로 한다. 후자는 차세대 원전의 인허가 및 위험도 정보 활용 설계 개선 지원을 위해 대표적인 3개 계통 - 디지털 발전소 보호 계통(DPPS), 디지털 공학적 안전설비 작동 계통 (DESFAS) 및 공학적 안전설비 기기제어 계통 (ESF-CCS) - 의 상세 신뢰도 평가 모형을 포함한 디지털 안전 계통의 원전 위험도 영향 평가용 통합 모델 및 요소 기술을 개발하고, 이를 통한 디지털 PSA 기반 기술을 확보하는 것을 목적으로 한다.

Ⅲ. 연구개발의 내용 및 범위

본 과제는 크게 정지/저출력 PSA 기술 개발과 디지털 I&C PSA 기술 개발 분야를 다루고 있으며, 각 분야별 수행된 연구 내용 및 범위는 다음과 같다.

정지/저출력 PSA 기술 개발 분야

○ 표준원전 정지/저출력 PSA 모델 품질등급 평가

- ANS Low Power and Shutdown PSA Methodology Standard [ANS, 2002]에 따른 영광 5,6 호기 정지/저출력 1단계 내부사건 PSA 모델 등급 평가를 통한 모델 취약점 및 개선 방안 도출

○ 정지/저출력 PSA 방법론 및 모델 개선 (4개 분야: 발전소 운전상태 분석, 초기사건 분석, 성공기준 결정 및 사고경위 분석 분야)

1) ANS Standard의 218개 세부요건 중 80% 이상의 요건이 II 등급 수준을 만족할 때로 자체 정의함

- 최신 발전소 계획정비 공정자료를 이용한 발전소 운전상태 (POS) 재분석
- 초기사건 분석 방법 개선 연구
- 국내·외 정지/저출력 초기사건 경험 자료의 수집, 분석 및 DB 구축
- 정지/저출력 고유 특성의 초기사건 기인자 분석 (반응도 사건)
- MARS 코드를 이용한 정지/저출력 PSA용 최적 열수력 분석 체계 구축
- 정지/저출력 성공기준 결정을 위한 POS별 기본사고에 대한 열수력 분석
- 정지/저출력 고유 특성의 열수력 상세 거동 분석 (가압기 안전밸브 개방고착 사고, 중력 급수, 저온 과압 사고, 관류 응축 현상)

○ 정지/저출력 위험도 관리 기반 기술 연구

- 정지/저출력 초기사건 발생 저감을 위한 초기사건 DB 검색 및 분석 프로그램 개발
- 정지/저출력 위험도 관리 모델 개발 방향 정립
- 발전소 기기배열 위험도 관리 모델 시범 구축 및 평가 (POS 1&2)

<u>디지털 I&C PSA 기술 개발 분야</u>

○ 안전 관련 디지털 계통의 상세 신뢰도 평가 모델 개발

- 안전 등급 디지털 계통의 설계 현황 분석
- 디지털 발전소 보호계통의 상세 신뢰도 평가 모델 개발
- 디지털 공학적 안전설비 작동계통의 상세 신뢰도 평가 모델 개발

○ 디지털 계통의 원전 위험도 영향 평가 모델 개발

- 노심 손상 빈도 평가 모델 개발
- 대량 조기 방출 빈도 평가 모델 개발
- 정지불능 과도사건 빈도 평가용 상세 모델 개발

- 조건부 인간오류분석 방법론 개발 및 원전 적용 연구

○ 디지털 I&C PSA 요소 기술 연구

- 디지털 기기의 공통원인고장 평가 방법론 기초 연구
- BBN (Bayesian Belief Net) 기법을 이용한 소프트웨어 신뢰도 평가 방법론 개발 및 원자로 보호 계통 소프트웨어 요건 개발 단계로의 적용 연구
- 고장내구성 기법/설비의 고장 검출률 (fault coverage) 정량적 평가 방법론 개발

Ⅳ. 연구 개발 결과

정지/저출력 PSA 분야와 디지털 I&C PSA 분야로 나누어 각 분야의 주요 연구 결과를 요약하면 다음과 같다.

정지/저출력 PSA 기술 개발 분야

○ 표준원전 정지/저출력 PSA 모델 품질등급 평가

- 정지저출력 위험도 정보 활용 의사결정이 가능한 PSA 표준모델 (등급 II 수준)의 개발 기초자료를 마련하기 위하여 ANS (American Nuclear Society) Low Power and Shutdown PSA Methodology Standard [ANS, 2002]에 따른 표준원전(영광 5,6 호기) 정지/저출력 1단계 내부사건 PSA 모델의 품질등급 평가를 수행하였고, 그 결과 전체적으로 1.5 등급 수준으로 판정되었다.
- 표준원전 PSA 모델의 등급평가 결과로 도출된 취약점 및 개선 방안은 상대적으로 인간오류 분야와 데이터분석 분야가 매우 취약한 것으로 나타났으며, 다음으로 초기사건 분야, 발전소 운전상태 분야, 정량화 분야, 성공기준 분야의 순으로 개선이 필요한 것으로 파악되었다.
- 본 과제에서는 아래에 기술된 4개 기술 분야 (발전소 운전상태 분석 분야,

초기사건 분석, 성공기준 결정 및 사고경위 분석 분야)에 대한 등급 개선을 수행하였고 그 결과 이들 분야에서 총 34개의 I 등급 이하 요건들 가운데 16개의 요건이 II 등급 이상으로 개선되었다.

○ 발전소 운전상태 분석 분야의 등급 개선

- 최신 발전소 계획정비 공정자료를 이용한 발전소 운전상태 (POS) 재분석을 수행하였으며, 그 결과 POS는 15개 그룹 17개 POS로 분류되었다 (기존과 동일).

- POS별 지속시간은 최신의 자료를 이용하여 재추정 하였으며, POS #7-#9 (핵연료 교체)를 제외하고 기존 추정치와 큰 차이는 없었다.

○ 초기사건 분석 분야의 등급 개선

- 초기사건 분석 방법을 보다 체계적으로 개선하였다. 개선된 방법론은 논리적 평가 (주논리도 개발), 경험적 평가 (사건 DB 이용), 공학적 평가 (발전소 고유의 기인자 분석) 방법의 결합으로 표준원전에 적용하여 최종적으로 22개의 초기사건을 선정하였다.

- 국내·외 정지/저출력 초기사건 경험 자료 (1973년부터 1999년까지의 운전 경험 자료)를 기술한 문헌들로부터 총 625건의 초기사건 자료 - 가압경수형 원전 422건, 비등 경수로 203건 - 를 수집/분석하고 이들에 대한 데이터베이스를 구축하였다.

- 정지/저출력 초기사건 발생 저감을 목적으로 구축된 초기사건 DB를 바탕으로 초기사건 검색 및 분석 프로그램 (LEDB; Low power and shutdown Event DataBase)을 개발하였다. LEDB 프로그램은 산업체의 향후 정지/저출력 PSA 수행 뿐만 아니라 정지/저출력 운전 중 초기사건 발생 저감을 위한 발전소 스텝의 교육 자료로도 매우 유용할 것이다.

- 또한 정지/저출력 고유 특성의 초기사건 기인자 분석의 일환으로 표준원전에 대해 붕소 희석에 의한 반응도 사고의 발생가능성을 정성적으로 또는 정량적으로 평가하였다. 이를 위해 문헌을 통해 알려진 15개의 붕소희석 반응도

사고 시나리오가 선정하여 표준원전의 POS (15개)에 따라 검토되었으며(총 225 case), 그 결과 현재의 표준원전에서는 붕소희석 반응도 사고가 발생할 가능성이 매우 낮은 것으로 판단되었다.

○ 성공기준 결정 및 사고경위 분석 분야의 등급 개선

- 정지/저출력 PSA 표준모델 개발을 위해 무엇보다도 정지/저출력 고유의 현상학적 사고 거동에 대한 이해가 필요하며, 보수성 및 불확실성이 저감된 열수력 분석 결과가 요구된다. 본 과제에서는 이를 위해 1) 정지/저출력 PSA용 열수력 분석 체계를 MARS V2.1을 이용하여 새롭게 구축하였고 (기술 국산화 및 향후 산업체의 정지/저출력 PSA 수행 시 활용 가능), 2) 성공기준 재결정을 위해 14개 POS에 대한 기본 사고 (정지냉각 상실사고)의 열수력 분석을 재수행 하였으며 (열수력 분석 결과의 불확실성 저감), 3) 기존 PSA에서 미흡한 정지/저출력 고유 특성에 대한 열수력 상세 거동 분석 (PSV 개방고착사고, 중력급수, 저온과압 사고, 관류 냉각)을 수행하였다.

- 특히, PSV 개방고착 사고에 대한 상세 열수력 분석 결과는 PSV 압력 설정치 시험의 개선안 제공으로 이어져 원전 안전성 향상에 기여하였으며, 중력급수와 관련한 분석에서 현장 실험 결과와 일치하도록 개선된 역지 밸브의 모델은 MARS 2.1 이후 버전의 기본 모델로 채택된 바 있다.

○ 정지/저출력 위험도 관리 기반 기술 연구

- 정지/저출력 위험도 관리를 위해 모델 개발 방향을 정립하였으며, 그 결과 위험도 정보 활용 분야로의 확대 적용이 용이한 일주기 (one-cycle) 위험도 감시 모델 형태의 기기 배열 위험도 관리 (CRM) 모델로 개발 방향을 정하였다. CRM 모델은 향후 본 과제의 3단계에서 본격 개발될 예정이다.

<u>디지털 I&C PSA 기술 개발 분야</u>

○ 안전 관련 디지털 계통의 상세 신뢰도 평가 모델 개발

- 울진 5,6 호기의 디지털 발전소 보호 계통 (DPPS)의 15개 정지 신호에 대한 상세 고장수목 모델을 개발하였으며, 정지 변수별 이용 불능도는 디지털 안전 필수 요소에 대한 가정 사항에 따라 5e-5 ~ 9e-4의 범위로 평가되었다.
- 울진 5,6 호기의 디지털 공학적 안전설비 작동 계통 (DESFAS)의 7개 ESF 작동 신호에 대한 상세 고장수목 모델을 개발하였으며, 신호별 이용 불능도는 디지털 안전 필수 요소에 대한 가정 사항에 따라 5e-5 ~ 3e-4의 범위로 평가되었다.
- 이들 디지털 안전 계통에 대한 상세 신뢰도 분석 모델은 총 1607개의 기본 사건과 4579개의 논리 게이트로 구성된 매우 상세한 모델로, 산업체의 설계 개선 및 인허가에 이미 활용되고 있다 (KNICS, KOPEC, 삼창(주)).

○ 디지털 계통의 원전 위험도 영향 평가 모델 개발

- 울진 5,6호기의 DPPS 및 DESFAS 상세 모델과 표준원전 위험도 감시용 PSA 모델을 결합한 노심 손상 빈도 (CDF; Core Damage Frequency) 및 대량 조기 방출 빈도 (LERF; Large Early Release Frequency) 평가 모델을 개발하였다. 결합된 CDF 모델은 3900여개의 기본 사건과 7000여개의 논리 게이트로 이루어진 매우 방대한 고장수목 모델이다. 이들 모델은 산업체 (KNICS, KOPEC, 삼창(주))의 인허가 및 설계 대안 평가를 위해 활용되고 있으며, 한국과학기술원(KAIST)으로의 기술 실시를 통하여 인간-기계 연계 (HMI) 연구에 활용되고 있다.
- 디지털 계통 모델과 원전 위험도 감시 모델의 결합을 위해 연계 기술이 필요하며, 본 과제에서는 1) 열수력 분석 결과를 활용한 정지불능 과도사건 (ATWS; Anticipated Transients Without Scram) 빈도 평가용 상세 모델 개발, 2) 조건부 인간오류분석 (CB-HRA; Condition Based Human Reliability Analysis) 방법론 개발 및 원전 적용 연구가 수행되었다.
- CDF와 LERF 정량화 결과는 디지털 안전-필수 요소에 대한 가정 사항에 따라 각각 7.7e-6 ~ 1e-4, 1.2e-6 ~ 6.7e-5 의 범위를 갖는 것으로 평가되었

다.

○ 디지털 I&C PSA 요소 기술 연구

- 디지털 I&C PSA 분야는 디지털 기기의 특성상 기존 PSA 분야에서는 일반적으로 다루지 않았던 수많은 디지털 안전 필수 요소들에 대한 평가 방법론들의 개발이 선행되어야 한다.

- 탑재된 소프트웨어에 의해 그 기능이 결정되고, 하드웨어는 모듈화된 부품을 사용하여 대량으로 생산하며, 계통차원에서 수많은 기기가 병렬 운전되는 디지털 기술의 특성으로 인해 기존의 공통원인고장 평가 방법론을 그대로 적용할 수 없게 되어, 보다 실용적이면서도 정확한 디지털 기기 공통원인고장 평가 및 모델링 방법론을 정립하기 위한 기초연구를 수행하였다. 울진5,6호기 DPPS에 적용할 수 있도록 실제 모수들을 계산하였다.

- 고전적인 확률모델로는 원자력과 같이 초고신뢰도를 요구하는 분야의 소프트웨어 신뢰도를 추정하기 어려우므로, BBN (Bayesian Belief Net) 기법을 이용하여 한 소프트웨어 신뢰도 평가 방법론 개발 및 원자로 보호 계통 소프트웨어 요건 개발 단계로의 적용 연구를 수행하였다.

- 지능적인 디지털 기기의 특성상 고장을 스스로 검출하여 안전한 방향으로 처리하는 고장내구성 기능을 내재하게 되는데, 이 기능의 유효성 (fault coverage) 정량화가 디지털 기기 안전성 평가에서 매우 중요한 역할을 하므로, 이에 대한 기초연구를 수행하였다. VHDL과 C++을 이용하여 시뮬레이션을 수행하여 다양한 검출 알고리듬의 고장 검출률을 시범적으로 정량화하였다.

V. 연구개발결과의 활용계획

○ 정지/저출력 PSA 분야의 모든 연구 결과물들은 위험도 정보 활용 의사결정이 가능한 수준의 정지/저출력 PSA 품질 향상을 위한 기반기술로서 정량적 위험도 관리 도구 개발의 실용화에 직접 활용될 계획이다.

○ 특히, 위험도 정보 활용 분야 가운데 상위 레벨의 응용 분야 - 차등 품질 보증, 가동 중 정비, 위험도 정보 활용 설계 등 - 에서 필수적으로 요구되는 기술로서 가까운 미래에 유용하게 활용될 전망이다.

○ 디지털 PSA 기술 개발 결과들은 디지털 기술의 원전 도입에 따른 안전성 영향을 종합적으로 정량 평가할 수 있는 기반 기술로 설계 개발자나 규제자로 하여금 계통성능의 관점만이 아닌 원전 전체 위험도의 관점에서 디지털 관련 최적 의사결정에 활용 가능하다.

○ 특히, DPPS와 DESFAS에 대한 상세 신뢰도 분석 모델 및 디지털 계통의 발전소 위험도 영향 평가 모델은 한국 원전 계측제어 시스템 개발단 (KNICS)에 제공되어 계통 설계 영향 평가를 통한 설계 개선 및 인허가에 이미 활용되고 있다.

SUMMARY
(영문요약문)

I. The Project Title

Development of Risk Assessment Technology for Low Power, Shutdown and Digital I&C Systems

II. The Objectives and Importance of the Project

Both the operational experience and the PSA results indicate that the risk from low power, shutdown (LPSD) operations could be comparable with those from power operations. As a result of economic imperatives and risk-informed initiatives related to LPSD operations, this project has initiated with the following objectives;

- ○ To understand and assess LPSD risks that are insufficiently modeled in conventional PSAs
- ○ To develop methods and tools for better management of LPSD risks
- ○ To reduce uncertainty that can affect the estimates of LPSD risks

Meanwhile, the obsolescence and narrow market security of the analog technologies substitute the digital I&C components for the analog ones. For instance, the safety-critical digital systems such as digital plant protection system (DPPS) and digital engineered safety feature actuation system (DESFAS) was adopted in Ulchin 5 & 6 units. As of now, however, the application of the conventional PSA methods to digital I&C systems is inefficient and may yield unrealistic and misleading risk insights regarding safety-critical digital systems. Thus, the project has also initiated with the objectives;

○ To provide PSA platform for evaluating digital I&C risks

○ To develop methods and tools for treating the digital-specific safety-critical problems in digital I&C PSA

○ To feedback risk insights regarding digital systems in the design stage, thus to support licensing activities of regulatory and non-regulatory side.

III. The Scope and Contents of the Project

There are two technical areas to deal with in the project; (1) the low power and shutdown PSA, and (2) the digital I&C PSA. Each of the areas covers the scope and contents as follows.

The LPSD PSA Area

○ Quality assessment of a LPSD PSA model for a Korean Standard Nuclear Power Plant (KSNP)

○ Quality improvement of the KSNP LPSD PSA model in the following four technical areas

- Plant operating status (POS)
- Initiating event analysis
- Determination of success criteria
- Accident sequence analysis

○ Development of the LPSD risk management technologies

- Study on the initiating event reduction techniques and configuration risk management techniques

The Digital I&C PSA Area

○ Unavailability analysis of Digital safety systems such as Digital Plant Protection System (DPPS) and Digital Engineered Safety Feature Actuation System (DESFAS)

○ Impact analysis of the digital safety systems on plant risks throughout of the digital plant risk models for evaluating core damage frequency (CDF) and large early release frequency (LERF)

○ Study on the methodologies for treating digital-specific problems in the digital I&C PSA such as reliability of safety-critical softwares, common cause failure (CCF) of digital components, fault coverage, etc.

IV. The Results of the Study

○ Quality assessment of a KSNP LPSD PSA model

- Based on the ANS Draft Standard (as of 13 Sep. 2002), we have performed a self-assessment of the quality of the KSNP LPSD PSA model. The aim of the self-assessment is to efficiently allocate the limited resources into the technical areas required for improving the LPSD risk model of which the quality will be appropriate for supporting risk-informed decision making.

- The review of the KSNPP LPSD risk model has been accomplished in two steps, (i) internal review and (ii) independent review. Some domestic experts with experiences in LPSD PSA have independently reviewed the results of the internal self-assessment to ensure their objectivity.

- The overall quality of the KSNP LPSD PSA model is estimated to be between Category 1 and Category 2 (1.5 level).

○ Improvement of the KSNP LPSD PSA model

- Re-evaluation of POS throughout the state-of-the-art of refueling outage information

- The systematic methodology for selecting initiating events was developed, which consists of three steps such as selection by logical approach, experience data, engineering design review.

- A database of LPSD initiating events (total 625 records) was developed, based on operational experience during the period of 1993 through 1999 in foreign and domestic plants

- Reactivity accident scenario by the boron dilution classified as the LPSD-specific initiator (total 225 cases = 15 scenario x 15 POS) was assessed in the qualitative and/or quantitative manners.

- A platform for relatively detailed thermal-hydraulic (TH) calculations to LPSD conditions was developed in the study, based on a best-estimate TH analysis code, MARS2.1. It is because both plant response time and recovery time are important attributes to accident sequence analysis in LPSD PSAs.

- To verify the efficient operation of the MARS platform during the LPSD conditions and improve the quality of success criteria area in KSNP LPSD PSA model, many TH analyses were performed for the loss of shutdown cooling events for various POS.

- The detailed TH analyses were performed reflecting the LPSD-specific characteristics in the project. They include PSV (Pressurizer Safety Valve) stuck-open, gravity feed, cold over-pressurization, reflux condensation, etc. Many fruitful risk insights at LPSD conditions were obtained from the results of these TH analyses.

○ Development of the LPSD risk management technologies

- A computer program, LEDB (Low power and shutdown Event DataBase), for searching and analyzing initiating events from database was developed to reduce the occurrence of initiator at LPSD conditions.
- The development and assessment of the demonstration models for managing configuration risks at the limited LPSD conditions such as POS #1 and #2 were performed.

○ Unavailability analysis of digital safety systems

- The detailed unavailability models for digital plant protection system (DPPS) and digital engineered safety feature actuation system (DESFAS) for Ulchin 5&6 units were developed based as-designed information.

○ Impact analysis of the digital safety systems on plant risks

- As the digital plant risk models, the CDF (Core Damage Frequency) and LERF (Large Early Release Frequency) models were developed including reliability models for DPPS and DESFAS. Several sensitivity analyses for digital safety-critical features on plant risks were performed using these models. Many useful risk insights were obtained.
- The interface model and methodology were developed to link digital systems to plant risk model as follows: 1) The detailed model for assessing ATWS (Anticipated Transients Without Scram) frequency, 2) Development of the methodology for CB-HRA (Condition Based Human Reliability Analysis).

○ Study on the methodologies for treating digital-specific problems in the digital I&C PSA

- The development of the technique for selecting and grouping digital equipments to analyze common cause failure (CCF) was performed.
- The methodology for evaluating the reliability of safety-critical softwares

using bayesian belief network (BBN) was developed and it was applied to the KNICS (Korea Nuclear I&C System development center) RPS software which is in its requirement stage.

- The hybrid modeling method for quantitatively evaluating the fault coverage of fault tolerant techniques or equipments, e.g., watchdog timer was developed.

V. The Proposals for the Future Applications

○ The results of the LPSD PSA research project can be directly used for the high level risk-informed applications initiated in the near future, e.g., Graded Quality Assurance (GQA), On-line Maintenance (OLM), risk-informed design (Option 3), and so on. The results were also utilized in various applications such as the improved check valve model adopted to MARS V3.0, the improvement of the PSV popping tests based on TH analysis.

○ The results of digital I&C PSA research project can be used for risk-informed decision-making related to digital I&C system. They will be used to develop the procedure guideline for digital I&C PSA in the near future. In particular, most of them are being also used to improve design of the digital safety systems in KNICS, KOPEC, Samchang Co.

Table of Contents
(영문 목차)

목 차

표 목 차

그 림 목 차

제 1 장 연구 개발 과제의 개요

제 1 절 연구 개발의 배경 및 필요성

위험도 대개의 공학적인 설계나 공공 정책 결정 과정에서는 사고 발생확률 자체가 매우 낮다 하더라도 만약의 사고 발생 시 대형 재난으로 이어질 수 있는 사건에 대해 많은 관심이 집중된다. 예를 들면, 댐의 설계는 평균 저수량보다 100년 만의 최대 홍수 사건을 기반으로 하고 원전 설계의 경우 수명기간 동안 발생 가능한 각종 최대 자연 재해 뿐만 아니라 예측 가능한 모든 사고 가능성에 대해 대비하고 있다.

위험도 분석은 이와 같이 공중의 건강과 안전에 대한 위험 요소들을 선정하고 그 위험 요소들의 발생 확률 및 발생 시 입게 될 손실의 심각성을 추정함으로서 정량적 평가가 가능하다. 이를 위해 원자력 발전소와 같이 복잡한 시스템에서는 확률론적 안전성 평가 (PSA; probabilistic safety assessment) 기법을 사용하며, 이는 파이프, 펌프, 밸브, 제어장비, 운전원과 같이 시스템 구성 요소들에 대해 경험 자료와 설계 및 성능 특성을 종합한 전반적인 정량적 위험도 평가 방법으로 다른 어떤 분석기법에 비해 원자력발전소와 같이 복잡한 시스템의 분석에 적당하다는 인식들이 60년대 후반부터 확산되면서 위험도 평가 및 규제에 대한 의사결정이나 인허가 지원, 안전성 향상 등의 용도로 확장되어 왔었다.

PSA 기술의 발전과 전력 산업계의 환경 변화에 따라 미국 원자력규제위원회 (NRC; Nuclear Regulatory Commission)는 1995년도에 공표한 규제 정책 성명 [NRC, 1995]을 통하여 규제 분야에서 위험도 정보 활용의 확대를 천명하기에 이르렀고, 이 후 미국 뿐 만 아니라 전 세계 원자력 선진국에서 '위험도 정보를 활용한 원전 운영 및 규제' (RIR&A; Risk Informed Regulation & Applications)에 대한 연구 및 적용이 매우 활발하게 진행되고 있는 실정이다. RIR&A의 중심축인 PSA 결과의 적용은 일차적으로 위험도 정보를 활용한 올바른 의사결정에 목적이

있으며, 이에 따라 의사 결정 문제가 무엇인가에 따라 합당한 PSA 수행 범위와 기술적 적합성이 요구된다. 일반적으로 의사 결정에 필요한 정보가 많을수록 요구되는 PSA 모델의 범위는 넓어지고, 중요한 의사 결정일수록 보다 높은 수준의 기술적 적합성이 요구된다.

최근 미국 NRC의 정지/저출력 위험도에 대한 현황분석 보고서[NRC, 2000]에 따르면 정지/저출력 위험도가 전출력 위험도에 비해 결코 적지 않았다는 점이 강조되면서, 많은 정비 활동으로 인한 다중방어 개념 약화, 위험도 관리 부족 등의 원인으로 안전성 저하가 초래될 수 있는 정지/저출력 위험도에 대한 연구 필요성을 주창하고 있다. 즉, 위험도 정보 활용 기술의 이용 확대라는 시대적 흐름에 따라 원전 전 운전주기에 대한 위험도 관리가 필수적이라 하겠다. 그러나, 정지/저출력 운전모드에서는 출력 운전과는 달리 다양한 기기배열로 인해 정지/저출력 PSA 수행 방법이 매우 복잡하고, 아직 통일된 방법론이 정립되어 있지 않은 상태에 있다. 특히, 정지/저출력 위험도 평가 결과의 불확실성이 상대적으로 크기 때문에 올바른 위험도 정보를 활용한 의사결정을 지원하기 위해서는 불확실성이 저감된 보다 현실적인 위험도 정보를 제공할 수 있는 기술의 개선이 함께 요구된다.

원전의 계측제어계통은 기존의 아날로그 회로로 구성된 원전 계측제어(I&C) 계통의 노후화로 열화와 품귀 문제가 점차 심각해지고 유지보수의 효율화, 편차(drift) 제거 등 저비용 고효율의 장점을 갖는 디지털 기술의 눈부신 발전에 따라 원전의 안전 기능에도 디지털 계측제어 계통으로 대체되거나 대체를 고려하고 있는 것이 세계적 추세이다. 이에 따라, 안전기능에 적용되는 디지털 기기/계통에 대한 안전성 입증이 요구되나, 이를 위한 디지털 계통의 위험도 정량 평가 방법론은 초기 개발 단계에 있어 명확한 체계 및 방법론이 정립되어 있지 못한 상태이므로 매우 시급한 세계적 현안 문제가 되고 있는 실정이다. 특히, 국내에서는 최근 상업 운전을 시작한 울진 5,6 호기를 선두로 안전 관련 디지털 I&C 계통이 이미 도입되었으며, 이와 같이 디지털 기술의 조기 도입으로 국내 원전의 안전성 입증이라는 관점에서 안전 관련 디지털 기기/계통에 대한 정량적 안전성 평가 방법

론 개발은 더욱 시급한 국내 현안 문제로 다룰 수밖에 없는 상황이다.

현재까지의 디지털 계통에 대한 안전성 평가는 주로 디지털 안전 계통 설계의 신뢰성 및 안전성 확인 및 검증을 결정론적 방법에 의해 수행하여 왔으나, 규제 및 원전 사업자의 위험도 정보 이용 확대 추세에 따라 디지털 안전 계통의 원전 위험도 전반에 미치는 영향을 종합적으로 평가할 수 있는 정량적 위험도 평가 기술 개발을 서둘러야 할 필요가 있다. 그러나, 이러한 디지털 I&C PSA 분야는 디지털 기기의 특성상 기존 PSA 분야에서는 일반적으로 다루지 않았던 수많은 디지털 요소 - 예를 들면, 소프트웨어 신뢰도, 고장내구성(fault-tolerance) 기법의 고장 검출률, 통신망 신뢰도, 디지털 기기 신뢰도, 등등 - 들에 대한 평가 방법론들의 개발이 선행되어야 한다.

제 2 절 연구 개발의 목적 및 내용

과제 제안 요구서(RFP)에 따라 2 단계 (2002. 4 - 2005. 2 ; 2년 11개월) 및 3 단계 (2005. 3 - 2007. 2; 2년)에 걸친 본 과제의 최종 연구 목표는 (1) 정지/저출력 종합 위험도 평가 및 관리 기술 개발, (2) 디지털 계측제어 계통의 위험도 평가 기술 개발에 있다. 보다 구체적으로 언급하자면, 전자는 표준원전에 대하여 ANS II 등급[1]을 충족하는 운전모드별 기기 배열 위험도 관리 (CRM; Configuration Risk Management) 모델의 개발을 통하여 정지/저출력 운전모드의 정량적 위험도 관리 기술을 확보하는데 있다. 후자는 차세대 원전의 인허가 및 위험도 정보 활용 설계 개선 지원을 위해 대표적인 3개 계통 - 디지털 발전소 보호계통 (DPPS), 디지털 공학적 안전설비 작동 계통 (DESFAS) 및 공학적 안전설비 기기제어 계통 (ESF-CCS) - 의 상세 신뢰도 평가 모형을 포함한 디지털 안전계통의 원전 위험도 영향 평가용 통합 모델 및 요소 기술을 개발하고, 이를 통한

1) ANS Standard의 218개 세부요건 중 80% 이상의 요건이 II 등급 수준을 만족할 때로 자체 정의함

디지털 PSA 기반 기술을 확보하는 데 있다.

상기의 최종 연구 목적을 달성하기 충족시키기 위한 2 단계 연구목표는 1) 정지/저출력 1단계 내부사건 PSA 방법론·모델 개선 및 위험도 관리 기반 기술 연구, 2) 디지털 계통의 안전성 평가 기술 개발이며, 단계 목표별 수행된 연구 내용 및 범위는 다음과 같다.

정지/저출력 1단계 내부사건 PSA 방법론 개선 및 위험도 관리 기반기술 연구

○ 표준원전 정지/저출력 PSA 모델 품질등급 평가

- ANS (American Nuclear Society) Low Power and Shutdown PSA Methodology Standard [ANS, 2002]에 따른 영광 5,6 호기 정지/저출력 1단계 내부사건 PSA 모델 등급 평가를 통한 모델 취약점 및 개선 방안 도출

○ 정지/저출력 PSA 방법론 및 모델 개선 (4개 분야: 발전소 운전상태 분석, 초기사건 분석, 성공기준 결정 및 사고경위 분석 분야)

- 최신 발전소 계획정비 공정자료를 이용한 발전소 운전상태 (POS) 재분석
- 초기사건 분석 방법 개선 연구
- 국내·외 정지/저출력 초기사건 경험 자료의 수집, 분석 및 DB 구축
- 정지/저출력 고유 특성의 초기사건 기인자 분석 (반응도 사건)
- MARS 코드를 이용한 정지/저출력 PSA용 최적 열수력 분석 체계 구축
- 정지/저출력 성공기준 결정을 위한 POS별 기본사고에 대한 열수력 분석
- 정지/저출력 고유 특성의 열수력 상세 거동 분석 (가압기 안전밸브 개방고착 사고, 중력 급수, 저온 과압 사고, 관류 응축 현상)

○ 정지/저출력 위험도 관리 기반 기술 연구

- 정지/저출력 초기사건 발생 저감을 위한 초기사건 DB 검색 및 분석 프로

그램(LEDB; Low power and shutdown Event DataBase) 개발

- 정지/저출력 위험도 관리 모델 개발 방향 정립
- 발전소 기기배열 위험도 관리 모델 시범 구축 및 평가 (POS 1&2)

디지털 계통의 안전성 평가 기술개발

○ 안전 관련 디지털 계통의 상세 신뢰도 평가 모델 개발

- 안전 등급 디지털 계통의 설계 현황 분석
- 디지털 원자로 보호계통의 상세 신뢰도 평가 모델 개발
- 디지털 공학적 안전설비 작동계통의 상세 신뢰도 평가 모델 개발

○ 디지털 계통의 원전 위험도 영향 평가 모델 개발

- 노심 손상 빈도 (CDF; Core Damage Frequency) 평가 모델 개발
- 대량 조기 방출 빈도 (LERF; Large Early Release Frequency) 평가 모델 개발
- 정지불능 과도사건 (ATWS; Anticipated Transients Without Scram) 빈도 평가용 상세 모델 개발
- 조건부 인간오류분석 (CB-HRA; Condition Based Human Reliability Analysis) 방법론 개발 및 원전 적용 연구

○ 디지털 I&C PSA 요소 기술 연구

- 디지털 기기의 공통원인고장 평가 방법론 기초 연구
- BBN (Bayesian Belief Net) 기법을 이용한 소프트웨어 신뢰도 평가 방법론 개발 및 원자로 보호 계통 소프트웨어 요건 개발 단계로의 적용 연구
- 고장내구성 (fault tolerance) 기법/설비의 고장검출률 (fault coverage) 정량적 평가 방법론 개발

본 과제에서 연차별 주요 연구 내용들의 상호 연관 관계는 그림 1-1에 주어져 있다.

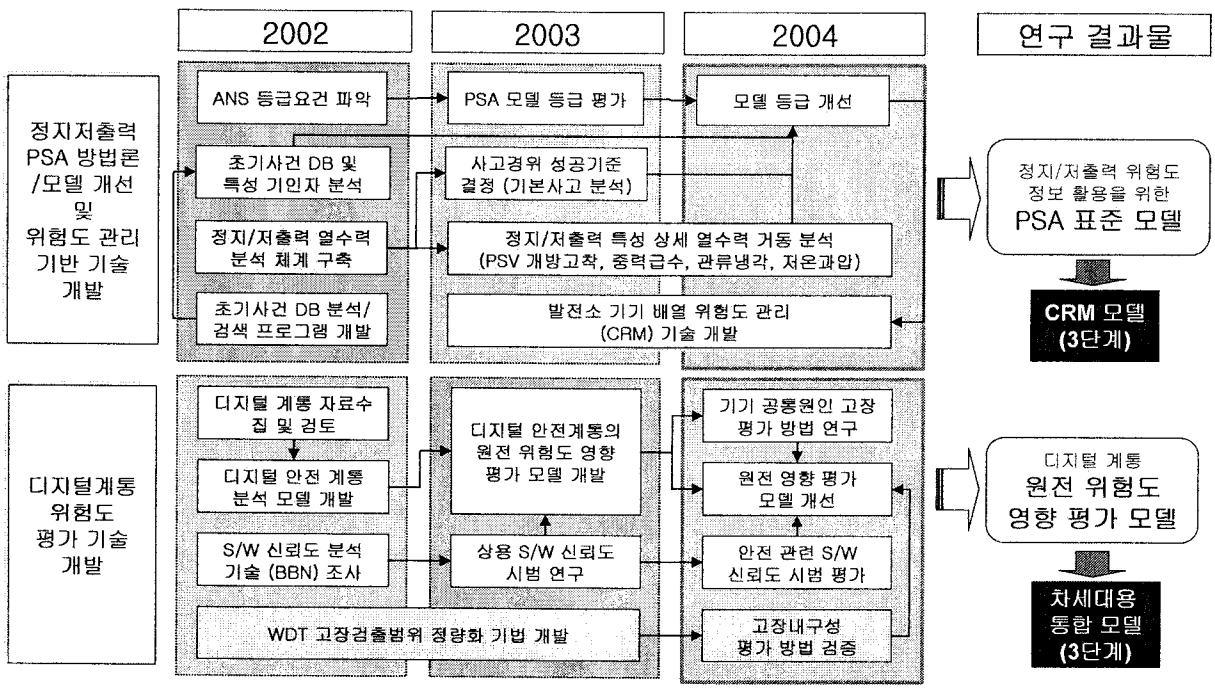


그림 1-1 연차별 연구수행 내용 및 연관도

제 2 장 국내·외 기술개발 현황

제 1 절 정지/저출력 PSA 기술 개발 현황

원자력 발전 초기 단계에서는 고온정지를 포함한 발전소의 정지 상태를 안전한 상태로 간주하였으며, 정지 중 사고발생 후에도 정상 출력 운전에 비하여 노심에서 발생하는 잔열이 낮고 운전원이 조치를 취할 수 있는 시간이 길다는 등의 이유로 출력 운전 중에 발생하는 사고에 비해 위험도가 크지 않다고 판단하였다. 따라서 원자로 정지 이후 발생하는 사고에 대한 안전성에 대한 평가를 간과하여 왔으며, 정지 상태에서 붕괴열이나 잔열을 제거하는 정지냉각계통의 중요성이 제대로 인식되지 않아 정지냉각 기능상실에 대한 위험성이 고려되지 않았다.

그러나 원자력 발전소가 상업운전을 시작한 이후 정지냉각 운전기간에 정지냉각 기능이 상실되는 사고가 빈번히 발생하였고, 노심손상과 같은 중대사고로 진전된 사례는 없었으나, 원자로냉각재계통의 비등을 초래하는 사고가 발생되는 등 정지냉각 기능 상실과 관련된 많은 사고를 경험하였다. 정지 운전 중에 발생한 사고들 중에는 적절한 조치를 취하지 않을 경우에 궁극적으로는 노심손상을 초래할 수 있는 가능성이 있는 사건들이 빈번하게 발생함으로써 정지/저출력 운전 중의 안전성에 대한 연구가 정지냉각 기능상실에 초점을 맞추어 80년대 중반부터 수행되기 시작하였다.

미국의 원자력 규제 위원회(US NRC)는 1987년 4월 미국의 Diablo Canyon에서 발생한 부분충수 운전 중 정지냉각 기능상실 사고에 대한 검토 결과, 가압 경수형(PWR) 원전의 정지 중 부분충수 운전이 발전소 정지 중 안전성에 상당히 취약한 상태라는 것을 인식하게 되었다. 이 사건에 대한 후속조치로 1987년 10월과 1988년 10월에 GL 87-12와 GL 88-17을 각각 발행하여 발전사업자들에게 부분충수 운전 중 안전성을 저해할 수 있는 절차서, 설비, 지침들의 미비점을 파악하고, 이를 개선할 것을 요구하였다. 그리고, 미국 원전의 정지 운전 중에 발생하는 주

요 사건들에 대하여 사건들에 대한 정보를 사업자들에게 알리고 후속 조치 사항의 이행을 지속적으로 촉구하고 있는 실정이다. 미국 원전에서는 GL 88-17의 안전조치요건을 이행한 후 사고의 발생률은 감소하였으나, 정지운전 중 정지냉각 상실사고의 발생 빈도는 감소되었다 하더라도 최근까지 다양한 원인으로 계속 발생하고 있다. 특히, 1990년 3월 미국 Vogtle 원전에서 발생한 발전소 정전으로 인한 부분 충수 운전 중 정지냉각 기능 상실 사고와 1994년 9월 Wolf Creek 원전에서 발생한 작업관리 미흡으로 인한 증기고착(steam binding)으로 인한 냉각재 보충수단의 부재에 대한 잠재적인 위험성을 발견하고 사업자가 이에 대한 조처를 강구하도록 하였으며, 정지 중에 발생하는 주요 사건에 대한 잠재적인 위험도에 대한 평가를 수행하였다[NRC, 1992].

이와 같이 원전 운전 경험 측면에서 보면, 국내에서는 정지 운전 중에 발생하는 사건과 관련한 명확한 보고 규정이 없어 정확히 알 수 없으나, 외국의 운전 경험 사례에 비추어 저출력 및 정지냉각 운전의 안전성을 향상시키기 위하여 1996년 과기부에서 행정명령 원검 71233-78 [과기부, 1996]을 발행하여, 부분충수 운전을 위한 계측장비 개선 작업과 분석을 통한 기술지침서 및 절차서 개정작업을 요구하였다. 또한 원자력안전기술원에서도 저출력 및 정지냉각 운전의 안전조치요건 수행상태를 평가한 규제기술 정보 보고서[김위경, 2001]를 발행한 바 있다.

정지/저출력 운전모드에 대한 PSA는 80년대 후반까지는 특정 토픽별로 제한적인 분석만이 수행되어 왔었다 [Lobner, 1982; Beveridge, 1985; Holderness, 1985; Chu, 1988; Kiper, 1988]. 그러나, 1990년 프랑스에서 900MW [Lanore, 1990]와 1300MW [Montagnon, 1992] 표준원전에 대한 종합적인 정지/저출력 PSA가 수행되었고, 그 결과 연 평균 기준으로 (on calender year basis) 정지/저출력 노심손상빈도 (CDF)가 전출력 CDF의 50%, 225%를 각각 차지하는 것으로 발표되면서 정지/저출력의 높은 위험도에 대한 세계적인 관심을 불러 일으켰다. 영국의 Sizewell B [Ang, 1995], 스위스의 Gosgen [Rao, 1994], 미국의 Surry [Chu, 1994] 및 Grand Gulf [Whitehead, 1995]원전에 대한 정지/저출력 CDF가 전출력 CDF의 150%, 95%, 13%*, 50%* 에 각각 이르는 것으로 발표되었다 (*주: 정지 운전 중

부분 충수운전에 대한 CDF로 국한함). 특히, Sizewell B의 3단계 PSA 결과인 개인 위험도에 대해 정지/저출력의 위험도가 차지하는 부분은 43%인 것으로 밝혀진 바 있다. 이후 세계 각국에서 정지/저출력 운전 모드에 대한 안전성을 평가하기 위하여 많은 노력을 기울이고 있다.

국내에서도 전출력 운전에 대해서만 PSA가 수행되다가 영광 5,6호기의 건설 단계에 이르러 인허가용으로 정지/저출력 1단계 내부사건 PSA가 수행되기 시작했다. 이후 지금까지 울진 5,6 호기와 APR-1400 설계에 대한 정지/저출력 PSA가 완료되었으며, 현재 2001년 과기부가 고시한 중대사고 대책안에 따라 신규 및 가동 중 원전에 대해 한수원(주)는 순차적으로 정지/저출력 PSA를 수행할 계획으로 있다. 지금까지의 국내 정지/저출력 PSA 분석 결과에서도 외국의 경우와 마찬가지로 정지/저출력 위험도를 무시할 수 없는 수준으로 평가되었다. 현재까지의 국내 정지/저출력 PSA는 건설 또는 설계 개발 중인 원전을 대상으로 안전성을 확인할 목적으로 많은 보수성을 고려하여 수행되었고, 따라서 최근 RIR&A로의 확대 적용을 위해서는 방법론 및 모델의 개선이 필요한 상황이다.

살펴본 바와 같이 정지/저출력 운전 경험과 정지/저출력 PSA 결과, 모두로부터 저출력 및 정지 운전 중에 발생되는 사고로 인한 위험도가 정상출력 운전에 비해 무시할 수 없는 수준임이 확인된 이후 사고의 심각성에 대한 인식과 함께 저출력 및 정지 운전 중의 안전성 확보가 주요 관심사로 부각되었다. 특히, SECY-00-0007의 첨부물로서 최근 미국 NRC가 마련한 정지/저출력 위험도에 대한 현황분석 보고서[NRC, 1999]에 따르면, 원전에 따라 1.0e-7/RY ~ 8.5e-5/RY 범위의 노심손상빈도(CDF)로 조사·보고되어 정지/저출력 위험도가 전출력 위험도에 비해 결코 적지 않다는 점을 강조하면서, 위험도 정보 활용 의사결정을 위한 정지/저출력 위험도 연구의 필요성을 주장되고 있다. 이는 PSA의 목적은 궁극적으로 의사 결정 지원에 있고, 의사 결정 문제가 무엇인가에 따라 그에 합당한 PSA 수행 범위와 기술적 적합성이 요구되기 때문이다. 즉, 의사 결정에 필요한 정보가 많을수록 요구되는 PSA 모델의 범위는 넓어지고, 중요한 의사 결정일수록 보다 높은 수준의 기술적 적합성이 요구된다[NRC, 2003]. 예를 들어, Option 2

에 해당하는 차등 품질 보증 (GQA; Graded Quality Assurance) 같은 분야 [NRC, 1998]는 Option 1 분야에 비해 전출력(full-power) 뿐만 아니라 정지/저출력 위험도 정보도 함께 요구되고, 위험도 정보를 제공하는 PSA 모델도 보다 높은 품질 등급 기준을 만족하여야만 가능하다.

그러나, 현재까지 정지/저출력 운전 중 변화되는 공정에 의한 다양한 분석 대상과 초기사건 발생 가능성 등에 의해 PSA 수행 방법이 매우 다양하며 불확실성이 높아 통일된 방법론이 정립되어 있지 않은 상태에 있다. IAEA, OECD/NEA와 같은 국제기구에서 보다 표준화된 방법론을 정립하기 위해 노력 중이며, 특히 미국은 위험도 정보 활용기술의 확대에 따라 ANS에 의뢰하여 표준 지침서를 개발 중에 있다. 또한, NRC 주관의 COOPRA (International Cooperative PRA Research Program) 등을 통해 정지/저출력 PSA 방법론에 대한 국제 협력 연구가 활발히 진행되고 있다.

미국 NRC는 GL 88-17과 같은 규범적인 규정이 의한 정지/저출력 위험도 관리 노력뿐만 아니라 정비규정, ROP (Reactor Oversight Process) 등의 원전 운전, 정비 등 운영 전반에 대한 성능 및 안전성을 평가하기 위한 제도를 통해 위험도를 감시하고 있다. 미국에서는 정지/저출력의 경우 현재 전통적인 PSA 모델을 갖고 있는 원전이 매우 적은 관계로 정량적 위험도 평가 방법 보다는 정성적 위험도 평가 방법이 사용되고 있는 상황이다. 하지만, 최근에는 위험도 정보 활용 규제의 확대와 산업계의 계획예방정비 기간 단축 노력에 따라 Southern Company를 비롯한 여러 원전에서 정량적인 정지/저출력 위험도 평가와 이를 통한 위험도 관리를 수행할 계획이 추진되고 있다.

국내의 경우도 위험도 정보 활용 의사결정 (RIDM; Risk-Informed Decision Making)에 대한 도입이 활발히 논의되고 있는 상황이므로 우선 국내에서 수행된 정지/저출력 PSA 모델이 RIDM에 적합한 수준인지에 대한 평가가 이루어져야 할 필요가 있다. 이를 위해 본 과제에서는 최근 초안이 발간된 ANS 표준에 따른 품질 등급 평가를 통하여 부족한 기술을 찾아 대비하는 보완 연구를 수행하였다. 또한, 이러한 연구개발 결과를 이용하여 RIDM에 적합한 정지/저출력 PSA 표준모

델을 구축하는 것이 필수적이라 하겠다.

제 2 절 디지털 I&C PSA 기술 개발 현황

아날로그 기술의 퇴행과 디지털 기술의 진보로 현재는 원자력, 항공, 철도, 위성 등 안전과 관련한 분야에서도 거의 모든 기기에 디지털 기술이 적용되는 추세에 있다. 새롭게 설계되는 원자력발전소는 물론이고 기존의 원자력발전소에서도 아날로그 설비를 디지털 설비로 교체하고 있다. 이러한 변화에 따라 디지털 계통의 안전성 평가에 대한 필요성이 강조되고 있고, 외국에서도 이와 관련된 많은 연구가 진행 중이다. 그러나 디지털 계통의 정량적 위험도 평가 기술 개발은 국내외를 막론하고 전 세계적으로 아직 명확한 체계 및 방법론이 정립되어 있지 못한 상태에서 디지털 기술의 발전 속도가 빨라짐에 따라 더욱 다양한 현안 문제들이 도출되고 있는 실정이다.

미국 원자력산업계에서 개발한 대표적인 디지털 기기는 Westinghouse의 안전등급 분산제어시스템(DCS)인 Eagle21 시리즈와 지금은 Westinghouse로 합병된 Combustion Engineering이 개발한 안전등급 디지털 컨트롤러(PLC)인 AC160시리즈가 있다. 독일의 Siemens도 안전등급 디지털 계통인 Teleperm XS을 개발하여 판매하고 있다. 그 외에도 국방산업체에서 DY4 등의 계통도 원자력안전계통에 이용이 가능한 것으로 판단된다. 이와 같이 이미 원자력 산업계에서 디지털 기술의 활용이 확대되고 있고, 많은 상용 플랫폼이 개발·판매되고 있는 상황이다.

국내 원전에서의 계측제어 시스템은 표 2-1에서 보는 바와 같이 비안전 계통에서부터 안전계통으로 디지털 기술의 도입이 최근 가속화되고 있어 APR-1400(신고리 3,4 호기)에 이르러 보호 계통을 포함한 모든 계측제어계통이 디지털 기술을 기반으로 설계될 예정이다. 최근, 고리 1호기와 같은 기존 원전에서도 하드웨어 중심의 아날로그 계통들이 마이크로 프로세서 기반의 디지털 계측제어 계통으로 교체된 바 있다. 국내 원전에서 디지털 기기는 현재 외국의 상용 플랫폼을

사용하나 원전 계측제어시스템 개발단(KNICS)에서 이를 국산화하기 위한 과제가 진행 중에 있다.

하지만, 이러한 상용 플랫폼의 안전성에 대해서는 아직도 많은 불확실성이 존재하므로 미국과 유럽 등 기술선진국에서는 안전성 입증을 위한 연구의 중요성이 지속적으로 제기되고 있는 상태이다. 특히, 기존의 디지털 계통에 대한 안전성 연구는 주로 계통 자체의 안전성을 확인·검증에 초점을 두고 있으나, 디지털 계통 자체가 원전 위험도 전반에 미치는 영향 평가는 거의 이루어지고 있지 않고 있어 원전에 디지털 기기가 본격적으로 도입되고 있는 현 시점에서 이에 대한 위험도 평가 기술개발이 시급한 상황이다. 다시 말해서, 위험도 정보 기반 규제나 설계가 추진되는 등 위험도 정보의 활용이 중요해 진 현 상황에서 디지털 기기를 안전계통에 적용한 원자력발전소의 위험도 평가를 확률론적 안전성 평가(PSA) 관점에서 접근할 필요성이 증대되고 있는 것이다. 디지털 I&C PSA 분야에서의 주요 항목별 국제 동향은 다음과 같다.

<u>디지털 I&C 계통 안전성 평가를 위한 기술 지침 개발 현황</u>

국제표준기구인 IEC에서는 디지털 계통의 원자력을 포함한 안전관련 산업에의 적용에 대한 연구를 수행하여 보고서를 출간하고 있으나, 국내에서는 한국원자력안전기술원(KINS)이 현재 설계 개발 과정에 직접 참여하여 디지털 안전 계통의 규제 지침들을 개발 중에 있다. IEC의 대표적인 관련 보고서 및 내용은 다음과 같다.

○ IEC-61838 [IEC, 2001] : 기 출간한 IEC 61226 (Nuclear power plants - I&C systems important for safety - classification)에서 계측제어 계통의 안전 분류(safety category)를 기능(function)에 기초하여 결정론적으로 정의하도록 한 것에 대해 정량적인 분석을 전혀 고려하지 않았다는 지적이 있어, 이를 수용하여 보완 방안을 강구한 내용임. 확률론적 분석을 통해 위험도를 정량적 분석함으로써 궁극적으로는 위험도 기반 분석 및 계통 구분을 수행하여야 한다는 주장함.

○ IEC-61508 [IEC, 1998] : 구체적인 방법론을 제시하기보다는 기본적인 계통 및 소프트웨어의 요구 조건(requirement)을 기술하는데 중점을 두고 있음.

디지털 계통 안전성 평가 방법론 연구 동향

거의 모든 선진국에서 원자력발전소 안전성 검증을 위해 PSA를 수행하였었고, 기존의 결과물을 보유하고 있는 상황이므로 기존 PSA 방법론인 고장수목을 활용하여 디지털계통의 안전성 평가를 수행하는 것이 유리한 점이 많다. 그러나 디지털 계통의 위험요소를 고장수목으로 모델링하기 위한 세부 기술이 개발되어 있지 않고 지침도 확정되어 있지 않으므로 각국에서 각자의 가정을 도입하여 연구를 수행하고 있는 실정이다.

미국 EPRI에서는 디지털 계통을 도입하고자 하는 발전소에서 일반적으로 적용할 수 있는 플랫폼을 만들고자 하는 연구를 수행중이며[Naser, 2004], 독일의 Framatom에서는 디지털 계통의 PSA를 위해 기존 인공지능 방법이나 전문가 판단 기법을 활용하기 위한 연구를 수행 중에 있다[Ciesielski, 2004]. 또한 프랑스 EdF에서도 디지털계통의 PSA를 위한 연구를 유럽공동 프로젝트 형태나 EPRI 공동연구 형태로 수행하고 있다[Nguyen, 2004]. 그러나 전술한 바와 같이 공통원인 고장확률의 평가나 소프트웨어 고장확률의 평가 등 매우 중요한 기술 항목에서 공인된 방법론이 존재하지 않아 많은 어려움을 겪고 있다.

한편 캐나다에서는 시험에 의한 고장확률 상한성 설정 방법을 적용하고 있다. 즉, 소프트웨어를 포함한 디지털 안전 계통 전체의 신뢰도 목표치를 고장률을 기준으로 1E-4로 설정하고 이에 상응하는 수의 시험 입력을 임의로 동작시켜 고장이 없는 경우 1E-4를 소프트웨어의 고장률 값으로 사용하는 평가방법을 택하고 있다. 그러나 이것은 소프트웨어 시험 기술에 지나치게 의존하고 있어 신뢰도 값에 대한 체계적인 확신을 갖는데 문제가 있다고 사료된다. 뿐만 아니라, 시험 입력에 대한 출력이 고장으로 판명되었을 경우에 대한 신뢰도 평가를 위한 체계적인 방법도 미흡하다. 프랑스의 경우에도 캐나다와 비슷한 접근 방법을 N4의 계측제어 계통에 적용한 바 있다.

영국의 국가 기관인 Health and Safety Executive에서도 관련 연구를 수행하였는데, PSA가 꼭 필요하다는 내용을 도출하였을 뿐 구체적인 방법론은 제시하지 못하였다[HSE, 1998]. 영국은 철도 시스템이 발달하여 그 안전성이 중요한 현안이며 원자력 발전소 및 산업시설을 다수 보유하고 있으므로 디지털 기기의 안전계통 적용에 대해 심도있는 검토와 연구를 진행 중에 있으나 주로 소프트웨어의 확인 및 검증에 치우친 연구결과를 내고 있어 안전성의 정량적 평가와 관련한 핵심 현안을 모두 다루고 있지는 않다.

미국 버지니아 대학의 Safety-Critical Systems 센터는 1998년에 설립되었으나 Semi-conductor Integrated Systems 센터의 기존 연구를 이어받아 계속함으로 가장 심도 있는 연구를 지속한 기관이며, 미국의 NRC, 철도국, NASA, 뉴욕 교통국 등으로부터 연구비를 지원받아 디지털 계통의 안전성에 관한 연구를 수행하였다. 원전 디지털 기기의 공통원인 고장에 관한 보고서를 제출하는 등 원자력계의 현안에 관한 연구결과를 다수 생산하고 있으나 주로 반도체와 회로 수준의 미시적 연구를 수행하고 있으므로 시스템에 미치는 영향 평가 등 거시적 연구는 수행하지 않고 있다 [Kaufman, 1999].

미국 방산 업체와 NRC와 같은 국가 기관을 대상으로 안전성 분석 소프트웨어인 MEADEP을 개발·판매하는 회사인 SoHaR사(미국)도 관련 연구를 수행하고 있다. MEADEP은 마코프-모델에 바탕을 둔 알고리듬을 이용하여 계통의 신뢰도를 분석하는 소프트웨어이다. 기술적으로 다루고 있는 분야가 제한적이고, 원전의 경우 사용이력이 부족하여 마코프-모델에 입력할 자료가 전무하다는 것이 문제이다. Westinghouse와 연계하여 현재도 계속 연구를 진행 중이다[Tang, 1998].

독일과 프랑스의 경우 Siemens를 중심으로 연구가 진행되고 있다. Siemens가 안전시스템에 사용할 수 있도록 설계한 디지털 장비인 Teleperm 시리즈를 생산하기 때문이기도 한데, 주요 연구는 하드웨어의 고장에 치중해 있으며 소프트웨어를 포함하는 전 계통의 안전성평가 연구는 아직 미흡한 상황이다.

OECD의 Halden 프로젝트에서는 2003년부터 디지털 계통의 안전성 평가에

대한 연구를 집중적으로 수행해 오고 있어, 많은 성과를 내고 있다[Thunem, 2004]. 그러나 Halden 프로젝트의 성격상 기존에 수행해 오던 소프트웨어 확인 및 검증에 기반한 평가 체계를 지향함으로써 고장내구성 평가 등 하드웨어를 포함한 전 계통에 대한 안전성평가 연구는 아직 미흡한 상황이다.

국내의 경우, 최근 울진 5,6 호기에 디지털 RPS/ESFAS이 도입됨에 따라 이들 계통에 대한 PSA 모델이 인허가 지원을 위하여 건설 단계에서 개발된 적이 있다 [김인석, 2000]. 그러나, 울진 5,6호기의 디지털 안전 계통에 대한 PSA는 기존의 PSA 체계에 디지털 하드웨어만을 대체한 것으로 현실적인 위험도 평가에는 매우 미흡한 상황이다. 또한, 한국원자력연구소(KAERI)에서 원자력 중장기계획사업의 일환으로 수행된 "차세대원자로 설계검증기술 개발"의 세부과제인 "차세대원자로 설계관련 요소기술 개발"에서 주요 요소기술의 한 분야로서 기초 연구를 수행한 바 있고, 이어 본 과제의 수행을 통해 전체 원전 PSA 모델에 결합하여 위험도 분석이 가능하도록 고장수목 기반의 상세 모델을 디지털 안전 계통에 대하여 새롭게 개발하였다. 현재, 소프트웨어의 신뢰도 추정을 위한 BBN 기법의 적용 기법, 고장검출률 계산을 위한 기법, 공통원인고장 처리 기법, 조건부 인간오류확률 모델 기법 등을 개발하여 소프트웨어와 하드웨어를 아우르는 종합적인 방법론 개발을 수행 중에 있다.

디지털 기기 신뢰도 평가 방법 연구 현황

디지털 전자 부품의 신뢰도 평가 기법과 고장률 자료는 영국, 일본, 캐나다, 프랑스, 미국 등의 선진국에서 연구가 상당히 많이 이루어지고 있다. 예를 들면, MIL-HDBK-217F [MIL, 1991], Bellcore [Bellcore, 1997], 미국 RCA사의 EPRD 등이 고장률 자료와 신뢰도 예측 기법을 동시에 제공한다. 또한, 이들 자료들을 바탕으로 군수용이나 일반 디지털 전자 제품의 신뢰도 예측을 편리하게 하기 위한 상용 소프트웨어 도구 - 예를 들면, RELAX, ITEM 등 - 들이 개발되어 RAM (reliability, availability and maintainability) 분야에서 많이 사용되고 있는 실정이다. 원자력 산업계에서는 원전 디지털 계통의 운전 경험을 수집/분석하기

위하여 OECD 주관으로 한국을 포함한 10여 개국의 국제공동연구로 COMPSIS (Computer-based systems important to safety) 프로젝트가 최근 출범하였다.

국내에서는 한국전자통신연구원(ETRI)가 디지털 기기의 신뢰성에 관한 연구를 가장 먼저 시작하여 선도해 온 기관이며 국내에서는 유일하게 전자기기 신뢰성 분석용으로 상용 소프트웨어 팩키지인 ERIS를 개발한 바 있다[전자통신연구원, 1999]. 그러나 그 연구의 대상이 통신관련 기기이므로 안전성 분석보다는 정비보수를 위한 수명평가 및 정비주기 연구에 초점이 맞추어져 있어 원전에 적용할 수 있는 기술이 아니다. 한국원자력연구소에서는 각각 MIL-HDBK-217F를 기반으로 하여 원자력발전소의 특성에 맞는 인자들을 추가하여 각 전자 부품 고장률 예측에 활용할 수 있도록 소프트웨어 팩키지, RPEE (Reliability Prediction for Electronic Equipments),를 개발한 바 있고[장승철, 2000], 한국과학기술원(KAIST)에서도 유사한 일을 수행한 바 있다. 본 과제에서는 월성 원전의 PDC (programmable digital comparator) 에 대해 운전 경험에 의한 고장률, Bellcore와 MIL-HDBK-217F의 신뢰도 예측 기법에 의한 고장률 추정 결과들을 비교 분석한 바 있다[정환성, 2002; 정환성, 2003].

소프트웨어 신뢰도 평가 방법 연구 현황

디지털 I&C 시스템에서는 하드웨어와 소프트웨어를 분리하여 생각하기 어렵다. 일반적인 소프트웨어의 신뢰도에 대한 연구의 역사는 매우 오래되었고 현재까지도 활발히 진행되고 있다. 본 과제에서 연구 대상으로 하는 원자력 발전소의 안전-필수(safety-critical) 소프트웨어는 고-신뢰성 (reliability-mission)만이 강조되는 일반 소프트웨어와는 달리 고-안전성 (safety-mission)이 요구되는 고유한 특성으로 인해 이 들에 대한 정량적 신뢰도 분석 방법론은 기존 소프트웨어 신뢰도 평가 모델의 한계점이 널리 인식되면서 1990년대 중반에서야 본격적으로 연구되기 시작되었다[Butler, 1993; Littlewood, 1993]. 여기서는, 본 과제에서 연구 중인 Bayesian Belief Network (BBN) 기법의 적용과 관련한 국내·외 연구 현황만을 살펴보기로 한다.

유럽의 경우, 영국에서는 London 대학과 Queen Mary 대학에서 디지털시스템/안전소프트웨어의 안전성과 신뢰도에 대한 연구를 Bayesian Belief Networks(BBN)과 Testing 기법을 위주로 수행하였으며[Littlewood, 1993], OECD Halden Project에서는 안전소프트웨어 표준 중의 하나인 RTCA/DO-178B를 기반으로 항공 커뮤니케이션 시스템 소프트웨어의 안전성과 신뢰성 평가를 BBN을 이용하여 수행하였다[Thunem, 2004]. 또한, 프랑스의 EdF와 핀란드의 VTT와 같은 기업에서는 유럽 국제 공동연구의 일환으로 Halden 프로젝트, London 대학 등과 공동으로 외주 개발 디지털 시스템의 소프트웨어 신뢰도 평가에 BBN을 활용한 유사 연구를 수행한 바 있다.

미국의 경우, 국립연구소인 LLNL에서 NUREC-0800을 기반으로 안전소프트웨어 설계문서 승인을 위한 BBN 모델을 구축한 바 있고, Virginia 대학, Maryland 대학 등에서는 Testing, V&V 그리고 신뢰도 성장 (reliability-growth) 모델과 같이 다양한 기법을 결합한 종합적인 방식으로 안전-필수 소프트웨어의 신뢰도와 안전성 평가 방법론 연구를 수행 중에 있다.

국내에서는 한국원자력연구소를 비롯한 일부 대학에서 안전 소프트웨어의 V&V를 위하여 현재 세계적으로 가장 애용되고 있는 정형 기법(formal method)을 중심으로 적용 연구 중에 있지만, 정량적 소프트웨어 신뢰도 평가 방법에 대한 연구는 아직 미흡한 실정이다. 후자의 경우, 본 과제에서 BBN 기법을 사용하여 상용 소프트웨어(COTS)에 대한 방법론을 개발하였고, 이를 KNICS 원자로 보호계통에 사용되는 소프트웨어의 요구명세서 단계에 시범 적용한 상태에 있다.

표 2-1 국내 원전에서 디지털 기술의 도입 현황 (자료출처: KINS)

Systems / Plants	Reactor Trip System	ESFAS Systems	Protection Process	NSSS Control	PCS	Turbine Contro	Main Control Board
Kori No. 1	Relay Logic (W/H)	Relay Logic (W/H)	Foxboro H-line	Foxboro H-line	Foxboro H-line	DCS	Conventional
Kori No. 1 (Upgraded in 1998)	Relay Logic (W/H)	Relay Logic (W/H)	Spec200 Spec200m (Foxboro)	Spec200 Spec200m (Foxboro)	Spec200 Spec200m (Foxboro)	DCS	Conventional
Kori No. 2,3,4 YG No. 1,2	SSPS Relay Logic (W/H)	SSPS Relay Logic (W/H)	7300 Analog	7300 Analog	7300 Analog	Mark V (GE)	Conventional
YGN No. 3,4	Relay Logic (ABB-CE)	Relay Logic (ABB-Œ)	Analog (ABB-CE)	Spec200 Spec200m (Foxboro)	ILS (Forney)	Mark V (GE)	Conventional
Ulchin No. 3,4 YG No. 5,6	Relay Logic (ABB-CE)	Relay Logic (ABB-CE)	Analog (ABB-CE)	Spec200 Spec200m (Foxboro)	PCS (Eaton)	Mark V (GE)	Hybrid
Wolsong No. 1,2,3,4	Relay Logic (AECL)	Relay Logic (AECL)	Analog/PDC (AECL)	DCC X/Y Computers Control	Analog/Relay (AECL)	Mark V (GE)	Hybrid
Ulchin No. 5,6	PLC (W/H)	PLC (W/H)	Analog (W/H)	Spec200 (PLC)	PCS (HFC)	Mark V (GE)	Hybrid
Shin Kori No. 1,2 Shin Wolsong No.1,2	PLC (W/H)	PLC (W/H)	Analog (W/H)	Spec200 (PLC) Ovation(W/H)	Teleperm XP (Siemens)	Mark VI (GE)	Hybrid
Shin Kori No. 3,4 (APR-1400)	PLC (W/H)	PLC (W/H)	Analog/PLC (W/H)	Ovation (W/H)	PLC (W/H)	Mark VI (GE)	Compact Workstation
HANARO Reactor	Relay Logic (AECL)	Not Applicable	Analog (AECL)	Control Computer	Not Applicable	Not Applicable	Hybrid

☐ Digital I&C modules

제 3 장 연구개발 수행 내용 및 결과

제 1 절 정지/저출력 위험도 평가 기술 개발

PSA 기술의 발전과 전력 산업계의 환경 변화는 최근 전 세계적으로 규제자나 원전사업자 모두에게 이익이 되는 위험도 정보 활용 기술에 대하여 연구 및 적용을 가속화되고 있다. 위험도 정보 활용 기술의 중심축인 PSA 기법의 가장 근본적인 목적은 위험도 정보를 활용한 올바른 의사결정의 지원에 있다. 올바른 의사 결정을 위해서는 고품질의 PSA 모델이 필요한 것은 사실이나, 고품질 PSA 모델의 개발에는 많은 시간과 비용이 따르게 되기 마련이고, 또한 모든 의사 결정 문제에 고품질의 위험도 정보가 요구되는 것도 아니다. 따라서, '의사 결정 문제가 무엇이냐?'에 따라 합당한 PSA 수행 범위와 기술적 적합성이 요구된다. 일반적으로 의사 결정에 필요한 정보가 많을수록 요구되는 PSA 모델의 범위는 넓어지고, 중요한 의사 결정일수록 보다 높은 수준의 기술적 적합성이 요구된다. 예를 들어, Option 2에 해당하는 차등 품질 보증 (GQA; Graded Quality Assurance) 같은 적용 분야는 Option 1 적용 분야에 비해 전출력 위험도 정보 뿐만 아니라 정지/저출력 위험도 정보까지도 요구되고, 위험도 정보를 제공하는 PSA 모델도 보다 높은 수준의 품질 등급 기준을 만족하여야만 가능하다.

국내에서는 아직 Option 1 적용 분야에 머무르고 있고 Option 2 를 시작하려는 움직임이 있다는 점에서 정지/저출력 PSA 기술 개발은 가까운 미래를 준비하는 분야라 할 수 있다. 이를 위해 본 과제에서는 그림 3-1에서 보는 바와 같이 과제 제안 요구서(RFP)에 따라 2 단계 (2002.4 - 2005.2) 및 3 단계 (2005.3 - 2007.2)에 걸쳐 기존의 표준원전 정지/저출력 1단계 내부사건 PSA 모델을 ANS II 등급 품질요건을 충족하는 정지/저출력 위험도 평가 모델 - 기기 배열 위험도 관리 (CRM; Configuration Risk Management) 모델 - 을 개발하여 정지/저출력 운전모드의 정량적 위험도 평가 및 관리 기술을 확보하고자 한다.

중장기 2 단계인 본 과제에서는 기존 표준원전 정지/저출력 PSA 모델을 대상으로 ANS standard [ANS, 2002]에 따라 모델 등급 평가를 실시하였고, 여기서 도출된 미비점이나 모델 개선 사항들을 바탕으로 4개 분야 - 즉, 발전소 운전상태 분석 분야 (PS), 초기사건 분석 분야 (IE), 성공기준 결정 분야 (SC) 및 사고경위 분석 분야 (AS) - 에 대한 방법론 및 모델 개선이 수행되었다. 나머지 4개 분야 - 계통 분석 분야 (SY), 인간 오류 분석 분야 (HR), 데이터 분석 분야 (DA), 정량화 분야 (QU) - 에 대한 방법론 및 모델 개선은 3 단계 중장기 과제 (2005.3 - 2007.2)를 통하여 발전소 기기배열 위험도 관리 (CRM) 모델의 본격 개발과 병행하여 수행될 계획이다. (그림 3-1 참조)

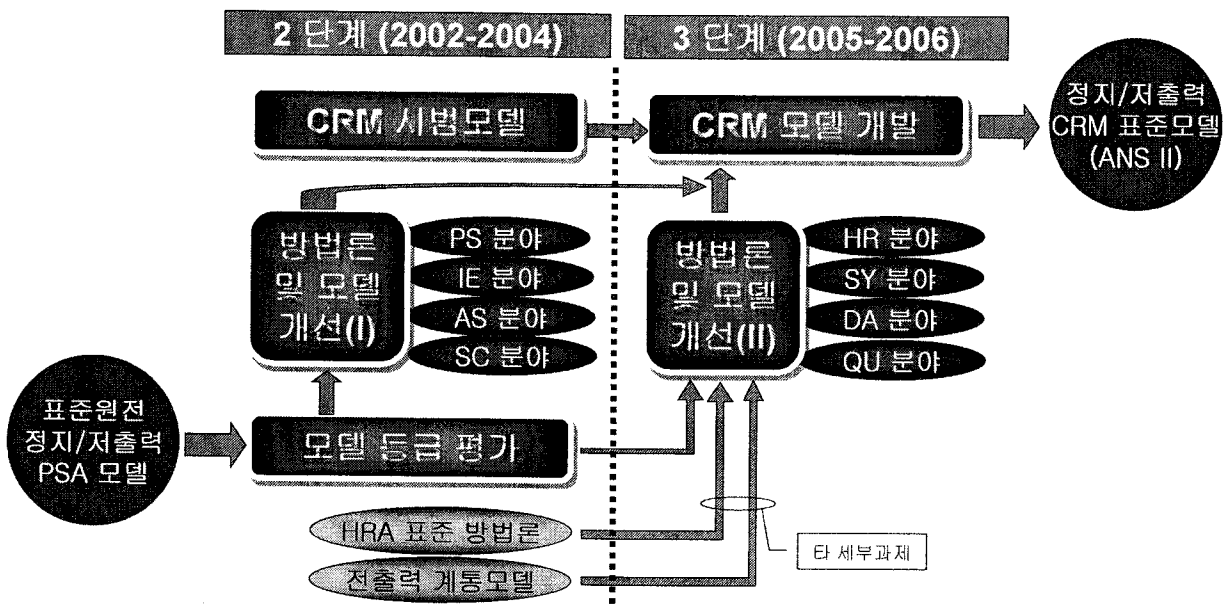


그림 3-1 정지/저출력 PSA 기술 개발 분야의 연구 목표 달성 추진 체계
(PS: 발전소 운전상태 분석, IE: 초기사건 분석, AS: 사고경위 분석, SC: 성공기준 결정, HR: 인간오류분석, SY: 계통분석, DA: 데이터분석, QU: 정량화)

1. 표준원전 정지/저출력 PSA 모델 등급 평가

전 세계적으로 경제성과 안전성을 동시에 추구하는 위험도 정보 활용 의사결정 개념을 원전 운영 및 규제 분야에 도입하고 있다. 이를 위해 무엇보다 정량적 위험도 정보를 제공하는 중심축인 PSA 모델의 품질 (또는 기술적 적합성)이 매우 중요하며, PSA 모델의 품질 평가 기준을 마련하기 위해 IAEA를 비롯한 미국, 일본 등 원전 선진국에서는 각고의 노력을 기울이고 있다. 이러한 노력의 일환으로 현재 미국에서는 전출력 1단계 내부사건 PSA 모델의 품질 평가를 위하여 원전 사업자 대표기구인 NEI (Nuclear Energy Institute)가 작성한 NEI PRA Peer Review Process Guidance와 규제 기관인 NRC가 미국 기계학회(ASME)에 의뢰하여 작성된 ASME PRA Standard이 실제 사용 중에 있다 (그림 3-2 참조). 이와는 별도로 정지/저출력 PSA 모델의 품질 평가를 위하여 최근 미국 원자력 학회(ANS)에서 ANS Low Power and Shutdown Methodology Standard[ANS, 2002]을 발표한 바 있다. 이는 초안(draft) 단계로 ASME PRA Standard와 거의 유사한 방식으로 작성되어 있다.

본 과제에서는 정지/저출력 위험도 정보 활용 의사결정이 가능한 PSA 표준 모델의 개발 기초 자료를 마련하기 위하여 영광 5,6 호기 정지/저출력 1단계 내부사건 PSA 모델을 대상으로 ANS Standard (Draft)의 품질 요건에 따라 모델 등급 평가를 수행하였다. 수행된 주요 내용을 정리하면 다음과 같다.

○ 영광 5,6 호기 정지/저출력 1단계 내부사건 PSA 보고서와 보조 분석 자료들 - 예를 들면, 설계 및 발전소 운영 자료, 열수력 분석 자료, 정량화 전산 파일 등 - 을 검토하였다.

○ ANS Standard의 요건에 대해 상세 검토하였다. ANS Standard에는 총 10개 분야로 나누어져 있으나 영광 5,6 호기 정지/저출력 PSA 범위를 넘어서는 2개 분야 - 내부 침수 분석 (IF) 및 대량조기방출빈도 분석 (LR) 분야 - 를 제외한 8개 분야의 43개 상위요건(HLR; high level requirement)에 대한 총 218개 세부요건(SR; supporting requirement)를 검토 대상으로 하였

다 (표 3-1 참조).

○ 총 14회의 내부 등급평가회의를 통하여 자체적으로 요건별 등급평가를 수행하였다.

○ 등급평가 결과의 객관성을 확보하기 위하여 국내 관련기관의 정지/저출력 PSA 전문가들로 구성된 2회의 외부 등급평가회의(2003.12.15, 2004.1.15-16)를 개최하여 자체 등급평가 결과들을 상세 재검토하였고, 2004년 7월초에 수행된 국외 전문가의 검토·자문 결과를 반영하여 최종 등급 평가를 완성하였다.

ANS Standard에 따른 영광 5,6 호기 정지/저출력 1단계 내부사건 PSA 모델에 대한 등급 평가로부터 다음과 같은 주요 결과들이 도출되었다. 보다 세부적인 결과는 기술보고서[박진희, 2004]와 발표 논문[장승철, 2004a; 장승철, 2004b]에 기술되어 있으므로 이 들을 참조하여야 한다.

○ 영광 5,6 호기 정지/저출력 PSA 모델의 전반적인 등급은 그림 3-2에서 볼 수 있듯이 II 등급 이상으로 평가된 항목이 50%이므로 1.5 등급 수준으로 판단된다.

○ 기술 분야별 품질등급 평가 결과는 그림 3-3과 표 3-1에 상세 기술되어 있으며, 상대적으로 인간오류 분야와 데이터분석 분야가 매우 취약한 것으로 나타났다. 그 다음으로 초기사건 분야, 발전소 운전상태 분야, 정량화 분야, 성공기준 분야의 순으로 개선이 필요한 것으로 판단된다.

○ 모델 등급 개선을 위한 세부 보완 사항들은 표 3-2에 정리되어 있으며, 보다 자세한 내용은 KAERI/TR-2672/2004[박진희, 2004]에 기술되어 있다. 특히, 문서화와 관련한 총 27개 요건 가운데 22개가 I 등급으로 판정되어 이에 대한 보완이 매우 시급한 것으로 판단되었다.

앞서 언급한 바와 같이 이 들 모델 등급 평가 결과를 바탕으로 본 과제에서는 우선 4개 분야 - 발전소 운전상태 분석 분야 (PS), 초기사건 분석 분야 (IE), 성공기준 결정 분야 (SC) 및 사고 경위 분석 분야 (AS) - 의 등급 개선을 위해 방법론 및 모델 개선이 이루어 졌다. 그림 3-1에서 알 수 있듯이 모든 분야에서의 모델 개선 후 최종적인 등급 재평가는 3 단계 과제 종료 시점에 가능하겠지만, 2 단계에서 수행된 4개 분야의 방법론 및 모델 개선 효과를 파악하기 위해 이 들에 대한 등급 재평가 결과를 보면 82개 중 II 등급 미만으로 판정된 34개(41%) 요건들 가운데 16개(19%) 요건들이 II 등급 이상으로 등급 상향될 것으로 판단된다. 본 과제에서 수행된 4개 기술 분야별 방법론 및 모델 개선 후 등급 재평가 결과는 표 3-3에 요약 정리되어 있으며, 이는 다음과 같은 분야별 등급 개선 노력의 결과로서 보다 자세한 내용은 이후 세션부터 순서대로 소개하도록 하겠다.

○ 발전소 운전 상태 분석 (PS) 분야

- 표준원전의 최신 계획정비 표준 공정 자료를 바탕으로 POS 재분석
- 발전소 고유의 POS 분류 및 POS 기간 추정

○ 초기 사건 분석 (IE) 분야

- 초기사건 분석 방법론 개선 : 논리적 평가 방법, 경험적 평가 방법 및 공학적 평가방법의 체계적 결합
- 초기사건 자료 수집 및 DB 구축 (625건)
- 초기사건 DB 검색 및 분석 프로그램 개발 (LEDB)
- 초기사건 DB 상세 분석 (특히, 정지냉각 상실사고의 원인별 분석 수행)
- 정지/저출력 고유 특성 기인자 분석 (반응도 사고 분석)

○ 성공 기준 결정 (SC) 분야

- 정지/저출력 PSA용 열수력 분석 체계 구축 (MARS 코드 이용)
- 성공기준 결정을 위한 POS별 기본 사고에 대한 열수력 분석 수행 (정지

냉각 상실 사고)

○ 사고 경위 분석 (AS) 분야

- 정지/저출력 고유 특성을 반영한 열수력 상세 거동 분석 (가압기 안전밸브 개방 고착 사고, 중력급수, 저온 과압 사고, 관류 냉각 현상)

표 3-1. ANS 표준 요건별 모델 등급 평가 결과

분야		상위요건 항목	세부 요건수	등급 평가 결과					비고
				등외	I	II	III	N/A	
발전소 운전상태 (PS)		선정	6	0	1	5	0	0	
		기간 결정	2	0	1	1	0	0	
		그룹핑	3	0	1	2	0	0	
		문서화	4	0	4	0	0	0	
		소계 (4)	**15**	**0**	**7**	**8**	**0**	**0**	
초기사건 (IE)		선정	10	0	3	7	0	0	
		그룹핑	4	0	2	2	0	0	
		발생빈도 추정	12	0	6	6	0	0	
		문서화	4	0	4	0	0	0	
		소계 (4)	**30**	**0**	**15**	**15**	**0**	**0**	
사고경위 (AS)		발전소고유 사고경위 선정	11	0	1	10	0	0	
		종속성	6	0	1	5	0	0	
		문서화	4	0	3	1	0	0	
		소계 (3)	**21**	**0**	**5**	**16**	**0**	**0**	
성공기준 (SC)		정의 및 일관성	6	0	2	4	0	0	
		보조 계산 및 정보	6	0	2	4	0	0	
		문서화	4	0	3	1	0	0	
		소계 (3)	**16**	**0**	**7**	**9**	**0**	**0**	
계통분석 (SY)		고장원인 및 모드	23	0	5	16	1	1	
		종속성 분석	16	0	7	9	0	0	
		문서화	3	0	2	1	0	0	
		소계 (3)	**42**	**0**	**14**	**26**	**1**	**1**	
인간 오류 (HR)	사고전	자료 수집 및 검토	3	1	2	0	0	0	
		선별 분석	2	0	2	0	0	0	
		인간오류 선정 및 영향분석	3	2	1	0	0	0	
		인간오류확률 평가	7	1	4	2	0	0	
		소계 (4)	***15***	***4***	***9***	***2***	***0***	***0***	
	사고후	자료 수집 및 검토	4	1	1	2	0	0	
		인간오류 선정 및 영향분석	2	0	0	1	1	0	
		인인오류확률 평가	9	1	5	3	0	0	
		회복조치분석	3	2	1	0	0	0	
		소계 (4)	***18***	***4***	***7***	***6***	***1***	***0***	
	공통	문서화	1	0	1	0	0	0	
		소계 (1)	***1***	***0***	***1***	***0***	***0***	***0***	
	소계 (9)		**34**	**8**	**17**	**8**	**1**	**0**	
데이터분석 (DA)		모수정의 (부품경계, 모델,등)	3	0	1	2	0	0	
		부품 그룹핑	2	0	2	0	0	0	
		일반 모수추정치의 적합성	16	0	9	7	0	0	
		발전소고유 모수 추정	7	0	6	1	0	0	
		문서화	1	0	1	0	0	0	
		소계 (5)	**29**	**0**	**19**	**10**	**0**	**0**	
정량화 (QU)		정량화 과정	4	0	0	4	0	0	
		정량화 모델과 코드의 적절성	9	0	2	5	2	0	
		종속성 처리	3	0	1	2	0	0	
		결과 검토 및 추적성	5	0	4	1	0	0	
		불확실성 분석	4	4	0	0	0	0	
		문서화	6	0	4	2	0	0	
		소계 (6)	**31**	**4**	**11**	**14**	**2**	**0**	
총계 (43)			**218 (%)**	**12 (5.5)**	**95 (43.6)**	**106 (48.6)**	**4 (1.8)**	**1 (0.5)**	

표 3-2. 기술 분야별 미비점 및 개선 사항 요약

분야	보완사항
발전소 운전 상태 (PS)	A2,B1&C2:정지유형별 분석(선정, 지속시간, 그룹핑), D1-4:문서화 및 QA
초기사건 (IE)	A1:선정과정 체계화, A7:선행자(precusor) 분석, A10:다중호기 초기사건 분석, B2:그룹핑과정 체계화, B4:LERF영향 고려, C1:발전소 고유 정보 수집/반영, C2: 베이지안 방법 이용, C3: Calendar year beae 계산, C4:정량적 초기사건 선별기준 적용, C5:추세분석, C10: 자료원간 비교분석, D1-D4:문서화 및 QA
사고경위 (AS)	A7:사고경위별 분석 및 기술, B3:사고경위별 현상학적 조건 및 영향 분석, C2-4: 문서화
성공기준 (SC)	A1:전출력 노심손상 정의와 불일치, A5:사고경위별 임무시간 분석, B1&B6:열수력 입력자료의 보수성 개선 및 영향 분석, C1,C2&C4:문서화
계통분석 (SY)	A13:모델링 기준 및 적용시 일관성 유지, A14:정성적 판단기준 적용, A15:사고전인간오류 분석, A18:T&M영향분석 및 실제와의 일치성, A19:룸냉각 모델 개선, B1:CCF root cause 및 영향분석, B5:보조계통 (사고조건과의 종속성 분석), B6:보조계통 (성공기준과 임무시간), B7:공간 및 환경적 영향 분석, B9:보조계통 (기기작동논리&룸냉각), B11:자동작동논리 상세모델, B15: 다중 SSC의 고장 원인 분석(NPSH, steam binding등), C1&C2: 문서화
인간오류 (HR)	사고전인간오류: A1-3(직무파악), B1-2(선별분석), C1-3(영향분석), D3-7(오류확률 추정), 사고후인간오류: E3-4 (발전소 정보수집), G1 (상세확률분석), G2 (수행오류 및 인지오류 평가), G3 (고유 shaping factor), G7 (종속성 분석), G8 (절삭오류 방지), G9 (추정치의 불확실성 분석), H2 (회복조치 근거), H3 (회복조치사건의 종속성 분석), 공통분야: I1(문서화)
데이터분석 (DA)	A3:모수추정항목 선정 및 자료수집, B1&B2:고유기기 그룹핑, C2-10:고유자료수집, D1&D4: 고유모수추정(베이지안 update), D2: 전문가판단 자료 목록 및 문서화, D3:모수추정(통계적 해석), D6: 발전소고유 CCF 확률 추정 (선별분석 및 mapping분석), D7:PSA update시 고유신뢰도 정보 사용, E1:문서화
정량화 (QU)	B3: truncation error 확인, B4: 희귀사건 근사문제, C2: 인간오류 종속성 처리문제, D2: 결과검토(가정사항의 합리성 검토), D3: 결과 비교 분석, D4: non-dominant cutset 확인, D5:중요도 분석 결과 검토, E1-4: 불확실성분석, F1-3 & F6:문서화

표 3-3. 정지/저출력 PSA 4개 분석 분야 방법론 및 모델 개선 후 등급 재평가

분야	상위요건 항목	세부 요건수	모델 개선 전		모델 개선 후		개선 사항 요약
			I 등급 이하	II 등급 이상	I 등급 이하	II 등급 이상	
발전소 운전상태 (PS)	선정	6	1	5	1	5	- 최신 계획정비 공정 자료에 의한 POS 재분석 및 POS 기간 재추정
	기간 결정	2	1	1	1	1	
	그룹핑	3	1	2	1	2	
	문서화	4	4	0	3	1	
	소계 (4)	**15**	**7**	**8**	**6**	**9**	
초기사건 (IE)	선정	10	3	7	1	9	- IE 분석 방법론 개선 및 상세 재분석 - 초기사건 DB 개발 - 고유 기인자 분석
	그룹핑	4	2	2	1	3	
	발생빈도 추정	12	6	6	3	9	
	문서화	4	4	0	0	4	
	소계 (4)	**30**	**15**	**15**	**5**	**25**	
사고경위 (AS)	발전소고유 사고경위 선정	11	1	10	1	10	- 고유 현상 및 사고 경위에 대한 상세 TH 분석
	종속성	6	1	5	0	6	
	문서화	4	3	1	3	1	
	소계 (3)	**21**	**5**	**16**	**4**	**17**	
성공기준 (SC)	정의 및 일관성	6	2	4	2	4	- TH 분석 체계 구축 - 기본 사고 거동 분석
	보조 계산 및 정보	6	2	4	0	6	
	문서화	4	3	1	1	3	
	소계 (3)	**16**	**7**	**9**	**3**	**13**	
총계 (43)		**82 (100%)**	**34 (41%)**	**48 (59%)**	**18 (22%)**	**64 (78%)**	**16개 항목 등급 개선**

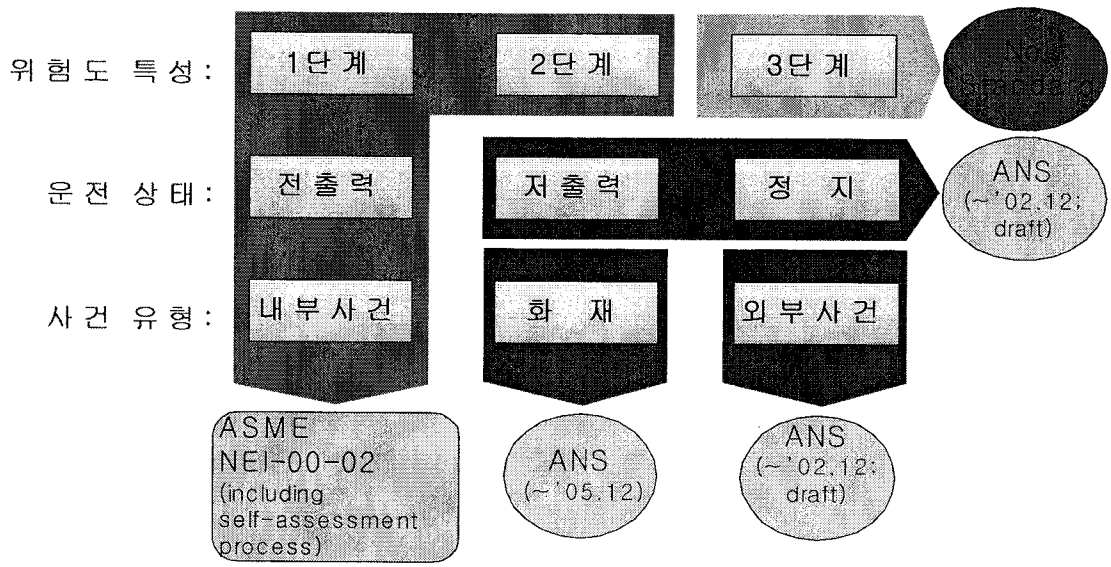


그림 3-2 NRC의 PSA 분야별 모델 등급 평가 지침서 발간/승인 계획
(2002년 10월 기준)

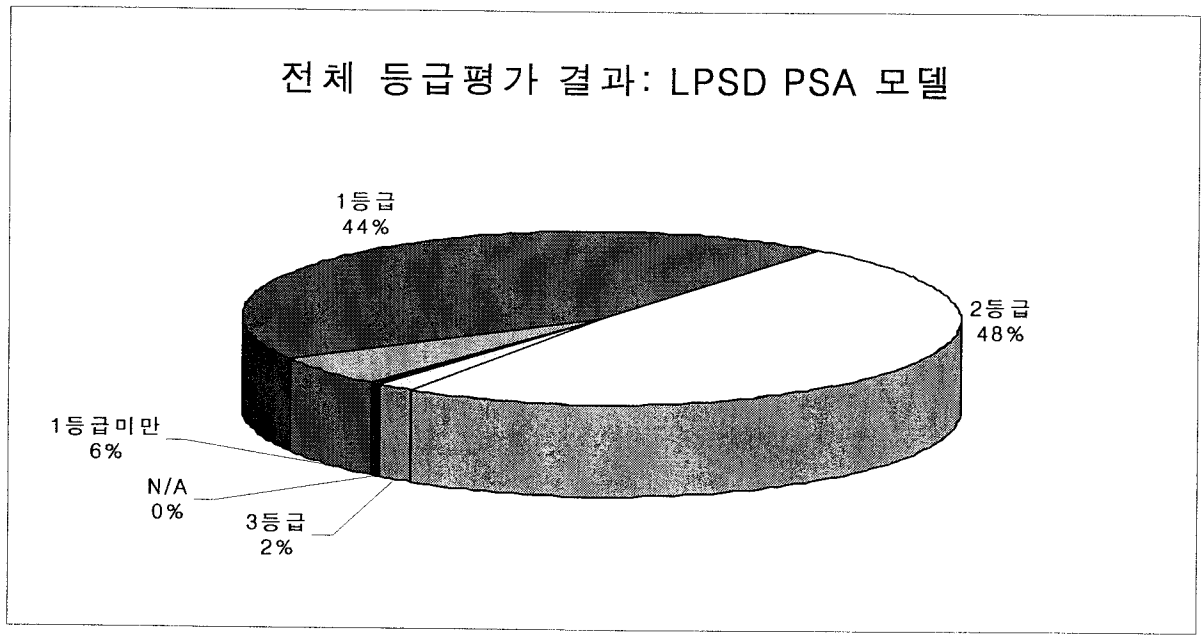


그림 3-3. 표준원전 정지/저출력 PSA 모델의 전체 등급평가 결과

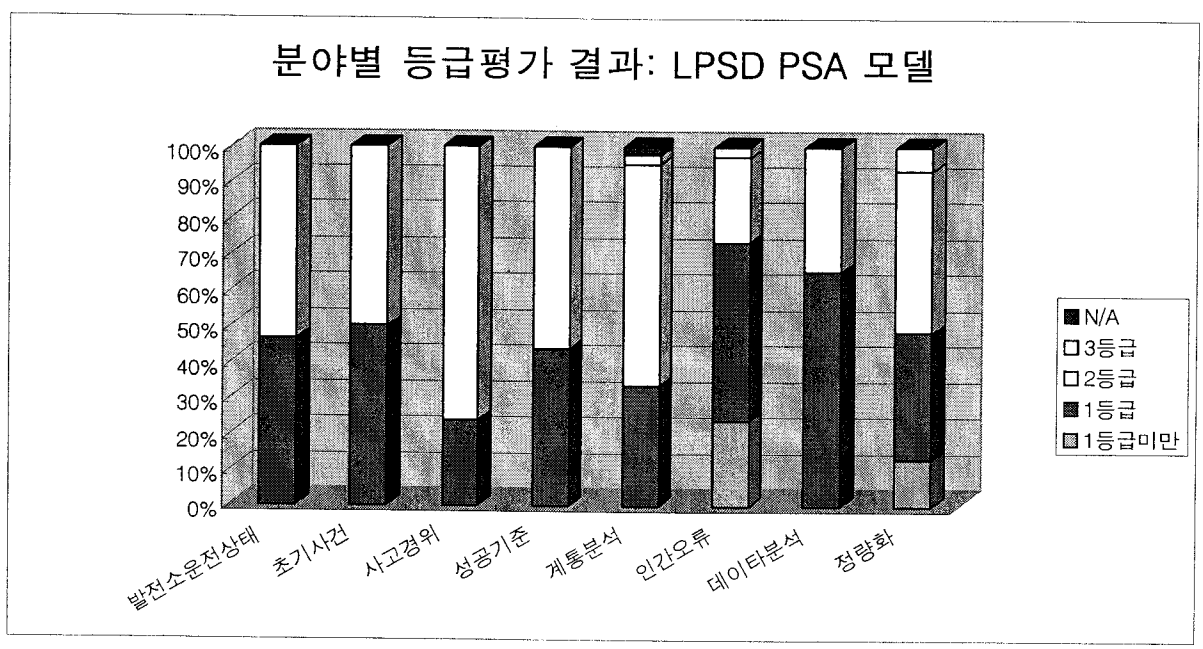


그림 3-4 표준원전 정지/저출력 PSA 모델의 기술 분야별 등급평가 결과

2. 발전소 운전 상태 분석 분야의 등급 개선

앞서 언급된 바와 같이 본 과제에서는 국내 표준원전의 정지/저출력 PSA 모델을 대상으로 ANS Standard (Draft)에 따라 모델 등급 평가를 수행하였고, 그 결과 정지/저출력 PSA의 8개 기술 분야별로 미비점 및 보완 사항들이 도출되었다. 발전소 운전 상태 (POS : Plant Operational States) 분석 분야에서는 총 15개 요건들 중 I 등급 이하가 7개 요건이고, II 등급 이상이 8개 요건인 것으로 판정되었다. POS 분석 분야의 등급 평가 결과로서 파악된 미비점 및 개선 사항들을 정리하면 다음과 같다 (표 3-2 참조).

○ 핵연료 재장전을 위한 계획예방정비를 포함한 모든 정지유형에 대한 POS 분석

○ 최신 국내 발전소 경험자료 반영한 POS 재분석

○ 체계적인 문서화 (분석 근거 기술, 타 PSA 기술 분야와의 연계 사항 기술, 정지 유형별 분석 결과 문서화)및 품질 보증 (QA) 절차 확립

본 과제에서는 RFP에 따라 이들 개선사항 가운데 최신의 국내 표준원전 계획정비 경험 자료를 바탕으로 POS를 재분석 하였고, 이로 인해 1개의 I 등급 요건이 II 등급으로 개선되었다 (표 3-3 참조). 다른 분야에 비해 상대적으로 등급 개선 요건 수가 적은 이유는 대부분의 I 등급 항목들의 판정 사유가 정지 유형별 분석 미흡에 기인하기 때문이다. 국내에서 수행된 모든 기존의 정지/저출력 PSA 수행 범위가 핵연료 재장전을 위한 계획 정지 (refueling outage)로 국한되어 있고, 타 정지 유형에 대한 PSA 수행은 많은 인력, 시간 및 비용이 요구되는 업무로 가까운 미래에 이와 관련된 요건들의 등급 개선은 어려울 것으로 판단된다.

본 과제에서 POS의 등급 개선을 위해 수행된 연구 내용은 아래와 같으며 이어지는 섹션에서 차례로 연구 내용과 결과들을 간단히 소개하기로 하겠다.

○ 기존의 POS 분석 방법론 및 결과 검토

○ 표준원전의 최신 계획정비 표준 공정 자료를 바탕으로 발전소 고유의 POS

분류 및 POS 기간 추정

가. 표준원전 발전소 운전 상태에 대한 기존 분석 결과

정지/저출력(LPSD) PSA에서 분석하는 운전 모드는 전출력 PSA에서는 발전소 전출력 운전 하나만을 분석대상 운전모드로 선택하는 반면에 LPSD PSA에서는 발전소 정지/저출력 운전 전반에 걸쳐 다양하게 변하는 모든 운전모드가 포함되어야 한다. LPSD PSA에서는 이와 같이 발전소 정지 및 저출력 운전 중에 나타날 수 있는 다양한 운전 형태를 발전소 운전 상태(POS)로 정의되며, 다음과 같은 분류 기준을 가지고 결정된다.

○ 원자로 출력(붕괴열 즉, 원자로 정지 후 경과시간)

○ 원자로 냉각재 수위 및 온도

○ 원자로냉각재계통의 개방(가압기 보수용 출입구, 증기발생기 보수용 출입구, 가압기 배기 밸브, 원자로 헤드 배기 밸브, 원자로 헤드 개방 및 노내 핵계측관 개방 여부 등)

○ 노심내 핵연료 장전여부와 각종 전위계통(front line system) 및 보조계통(support system)의 정비

국내 표준원전 LPSD PSA [전력연구원, 2001]는 건설 중인 원전을 대상으로 원전 운전경험이 전혀 없었기 때문에 POS 분류를 위하여 동일 유형인 영광 3,4호기를 참조 발전소로 이 들의 운전경험 자료를 이용하였다. 참조 발전소의 계획예방정비 경험과 국내 원전의 정비이력을 검토한 결과 (영광 3,4 호기 상업운전 초기 4회의 운전이력; 각 호기별 1,2차 계획예방 정비 운전 이력), 총 15개의 POS 그룹에 17개 POS로 다음과 같이 분류되었다 (그림 3-5).

○ POS 1 : 계통병해(turbine trip)에서 발전소 정지

○ POS 2 : 증기우회제어 계통을 이용한 발전소 냉각

○ POS 3 : 정지냉각계통을 이용한 발전소 냉각

○ POS 4 : 1차 부분충수를 위한 배수운전

- POS 4A (가압기 manway 개방 후)

- POS 4B (가압기 manway 개방 후)

○ POS 5 : 1차 부분 충수 운전(증기발생기 노즐댐 설치)

○ POS 6 : 핵연료 인출을 위한 재장전수조 충수 운전

○ POS 7 : 핵연료 인출

○ POS 8 : 핵연료 인출후 정비를 위한 배수 운전

○ POS 9 : 핵연료 재장전

○ POS 10 : 2차 부분충수를 위한 배수 운전

○ POS 11 : 2차 부분충수 운전(증기발생기 노즐댐 제거)

○ POS 12A : 발전소 기동을 위한 충수 운전

- POS 12A (가압기 manway 폐쇄 전)

- POS 12B (가압기 manway 폐쇄 후)

○ POS 13 : 1 단계 가열 운전(정지냉각계통 연결)

○ POS 14 : 2 단계 가열 운전(정지냉각계통 격리)

○ POS 15 : 발전소 기동에서 계통 병입

또한, 참조 발전소의 계획예방정비 공정 자료로부터 최종적으로 발전소 운전 상태별 지속 시간은 표 3-4와 같이 추정되었다.

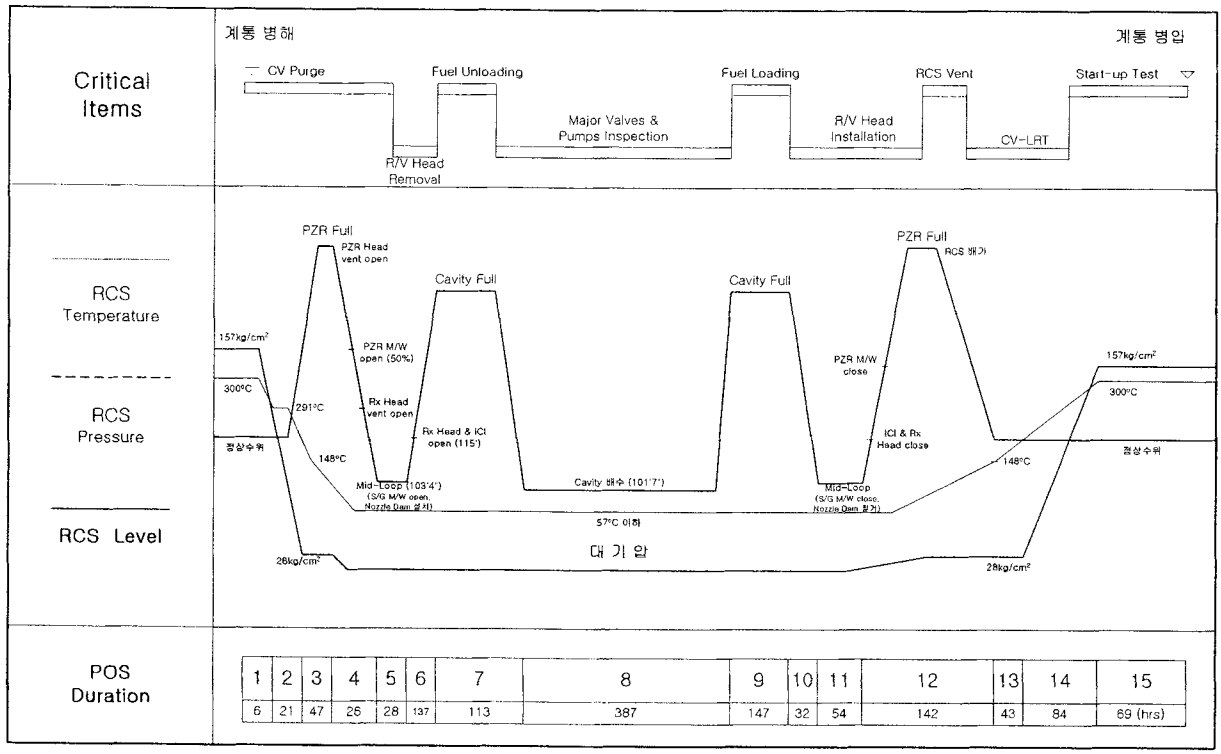


그림 3-5. 표준원전 정지/저출력 PSA에서의 발전소 운전상태 분류

표 3-4. 발전소 운전 상태별 지속시간 추정치

POS 구분		POS 특성	지속 기간(시간)
POS 1		계통병해에서 발전소 정지	6
POS 2		증기발생기를 이용한 발전소 냉각운전	21
POS 3		정지냉각계통을 이용한 발전소 냉각운전	47
POS 4	A	1차 부분충수 운전을 위한 배수운전 (가압기 manway 개방 전)	26
	B	1차 부분충수 운전을 위한 배수운전 (가압기 manway 개방 후)	
POS 5		1차 부분충수 운전	28
POS 6		핵연료 인출을 위한 충수운전	137
POS 7		핵연료 인출	113
POS 8		정비를 위한 배수 및 충수운전	387
POS 9		핵연료 재장전	147
POS 10		2차 부분충수 운전을 위한 배수운전	32
POS 11		2차 부분충수 운전	54
POS 12	A	발전소 기동을 위한 충수운전 (가압기 manway 폐쇄 전)	142
	B	발전소 기동을 위한 충수운전 (가압기 manway 폐쇄 후)	
POS 13		1단계 가열운전 (정지냉각계통 연결)	43
POS 14		2단계 가열운전 (정지냉각계통 격리)	84
POS 15		발전소 기동에서 계통병입	69
합 계			1,336 시간 (55.7일)

나. 국내 표준원전 발전소 운전 상태 재분석

일반적인 가압 경수형 발전소에서 정지 및 저출력 운전은 핵연료 재장전을 위한 계획 예방 정비, 불시정지, 수동정지 및 간이 예방 정비에 의해 발생 가능하다. 이 들 중 불시정지는 정상 운전 중에 기기/계통 혹은 운전원의 실수로 인한 발전정지를 의미하며 전출력 PSA 모델에서 다루어진다. 불시 정지를 제외한 정

지 유형은 발전소 종합운전절차서[한국전력공사, 1997]에 따라 동일한 방법으로 원자로를 정지하고 냉각절차에 해당 정비에 필요한 수준까지 냉각 및 감압 운전을 수행하게 된다. 계획예방정비를 제외한 정지유형을 비계획 정지 (unplanned outage)로 분류하고 여기에는 정비 대상에 따라 배수 정비 (drained maintenance)와 비배수 정비(non-drained maintenance)로 다시 나뉘어 진다. 이들 비계획 정지도 계획 정지와 유사한 절차를 사용하지만 대개 고장 기기/계통의 정비만을 목적으로 수행되므로 정비 부위에 따라 그 특성은 매우 다를 수 있다. 본 과제에서는 핵연료 재장전을 위한 정기 계획 정지 기간을 분석 대상으로 다루었다.

이 기간 중에는 출력 감발 및 증발을 포함한 저출력 운전과 원자로 정지 후에 수행되는 핵연료 교환이나 안전 및 비안전 등급 기기의 정비나 시험 등으로 인한 공정 변화에 따라 다양한 운전형태를 보일 수 있다. 정지/저출력 PSA를 수행하기 위해서는 정지/저출력 운전 중에 나타날 수 있는 다양한 운전 형태를 반영할 수 있는 모든 운전 형태를 PSA 분석대상 운전 모드로 고려하는 것은 현실적으로 불가능하다. 이에 따라, 기존에 적용되었던 것과 동일한 방법으로 발전소의 계획예방정비 경험 자료로부터 POS 재분석을 수행하였다.

먼저 기존의 발전소 운전상태 분석에 사용된 자료는 참조 발전소(영광 3,4 호기)의 상업운전 초기 4회의 운전이력 (각 호기별 1,2차 계획예방 정비 운전 이력)이었으나, 최근 조사된 참조 발전소의 계획예방정비별 수행 기간은 표 3-5와 같다.

표 3-5. 영광 3,4 호기 계획 예방정비 기간 비교

연차 계획 예방 정비	영광 3 호기	영광 4 호기
1 차	92일	65일
2 차	54일	44일
3 차	48일	43일
4 차	44일	53일
5 차	51일	56일
6 차	39일	40일

또한, 국내 표준원전의 최근의 계획예방정비 운전이력과 계획예방정비 공정 편성을 위한 기술행정절차서[한국전력공사, 2003]를 입수하여 현실성 있는 POS 분석을 수행하였다. 아래 표 3-6에는 기술행정 절차서에 기술된 계획예방정비 표준 공기를 나타내고 있다. 표준원전의 경우 대개 30일 정도의 표준 공기가 계획되어 있으나 표 3-5의 실제 원전에서 수행된 계획예방정비 기간과는 괴리가 존재함을 알 수 있다. 따라서 본 분석에서는 표준 공정 자료보다 실제 원전에서 수행된 계획예방정비 경험 자료를 바탕으로 POS를 재분석하였다.

수집된 경험 자료는 발전소 운전원과의 면담을 통한 확인 절차를 거쳐 각종 정지/저출력 운전변수 및 각 계통의 정기 점검 일정 등을 분석하였다. 그 결과, 모든 POS 내의 원자로냉각재계통의 상태나 발전소 배열 상에서 기존 결과에 영향을 미칠 수 있는 주요한 차이점은 발견되지 않았으나, POS별 지속시간 다르게 나타났다. 따라서, POS 분류 결과는 기존 PSA 모델과 동일하게 15개 POS 그룹에 17개 POS로 분류되었고, POS 지속시간은 표준원전 계열의 원전 중에 운전 경험이 가장 많은 영광 3,4호기의 최신 자료인 6차 정기계획예방정비 운전 경험 자료로부터 표 3-7과 같이 추정되었다. 그림 3-6은 국내 최근 운전이력들과 기존의 PSA 모델에서 추정된 POS 지속시간을 비교한 것이다.

결론적으로, POS 재분석 결과 기존의 PSA 모델에서 도출된 POS별로 수행되는 공정상의 상이점은 발견되지 않았으나, 각 POS별 지속시간에는 많은 차이가 발견되었다. 그림 3-8에서 보듯이 전체 공정별 지속시간이 최근 줄어들고 있는 경향을 보이고 있으며, 특히, POS 6, 8, 9와 12에서 공정시간이 많이 줄어들어 계획예방정비 전체 공정에 큰 영향을 주는 것으로 나타났다. 분석으로 LPSD PSA Standard에서 요구하는 최근의 운전이력 반영 및 POS 분류근거 확보 등에 대한 요건은 만족시킬 수 있으나, 정기계획예방정비 외의 정지 유형에 대한 POS 분석은 향후 정지/저출력 PSA 분석 범위의 완전성을 위해서는 보완되어야 할 필요가 있다 하겠다.

표 3-6 국내 PWR 원전별 계획예방정비 표준 공정 기간 (단위: 시간)

단위공정	600MW (W)		950MW (W)		950MW (F)	1,000MW (ABB-CE)		비 고
	고리1	고리2	고리 3,4	영광 1,2	울진 1,2	영광 3,4	울진 3,4	
1. RCS 냉각 및 배수	101	101	120	120	95	-	30	
★ CV Stepping 및 Crane 점검	-	-	-	-	-	40	-	
★ 원자로 부대설비 분해	-	-	-	-	-	74	74	
2. S/G M/W 개방/노즐댐 설치	-	-	-	-	12	-	-	
3. 원자로 분해	64	64	60	60	47	61	56	
4. 연료인출	47	47	76	76	92	99	90	
5. 연료검사	78	78	92	92	134	73	72	
6. 연료장전	56	56	96	96	88	111	106	
7. 원자로조립	131	131	69	69	57	79	54	
8. S/G M/W 조립 / 노즐댐 제거	-	-	-	-	-	-	-	
★ 원자로 부대설비 조립	-	-	-	-	-	-	80	
9. RCS 충수, 배기	35	35	32	32	47	53	-	
10. RCS 가열	47	47	47	47	42	36	38	
11. 원자로 특성시험	38	38	57	57	56	58	58	
12. 터빈/발전기 기동	20	20	22	28	10	24	28	
소 계	612	612	671	677	680	708	686	
	25.5일	25.5일	28.0일	28.2일	28.3일	29.5일	28.6일	

표 3-7 표준원전 POS별 소요시간에 대한 신·구 추정치 비교

POS	설명	표준원전 (기존)	영광 3 호기 6차 O/H	영광 4 호기 6차 O/H
POS 1	계통병해에서 발전소 정지	6시간	3시간	1.8시간
POS 2	증기우회제어계통을 이용한 발전소 냉각	21.3시간	28.4시간	41.3시간
POS 3	정지냉각계통을 이용한 발전소 냉각	46.6시간	60.6시간	49.8시간
POS 4	1차 부분충수 운전을 위한 배수 운전	35.5시간	24시간	24.3시간
POS 5	1차 부분 충수 운전	27.5시간	18.1서간	16.3시간
POS 6	핵연료 인출을 위한 재장전수조 충수 운전	136.9시간	37.8시간	31.6시간
POS 7	핵연료 인출	112.5시간	83.2시간	90시간
POS 8	정비를 위한 배수 및 충수 운전	387.3시간	266.3시간	315.8시간
POS 9	핵연료 재장전	147.3시간	88.5시간	87.6시간
POS 10	2차 부분 충수 운전을 위한 배수 운전	32시간	136시간	118.5시간
POS 11	2차 부분 충수 운전	54시간	27.5시간	40.8시간
POS 12	발전소 기동을 위한 충수 및 배기 운전	154.1시간	14.5시간	31.4시간
POS 13	1 단계 가열 운전(정지냉각계통 연결)	43시간	51.1시간	13.3시간
POS 14	2 단계 가열 운전(정지냉각계통 격리)	84.2시간	1.5시간	56시간
POS 15	발전소 기동에서 계통병입	69.2시간	80.2시간	27.6시간
총 계		1357.4시간	930.7시간	946.1시간

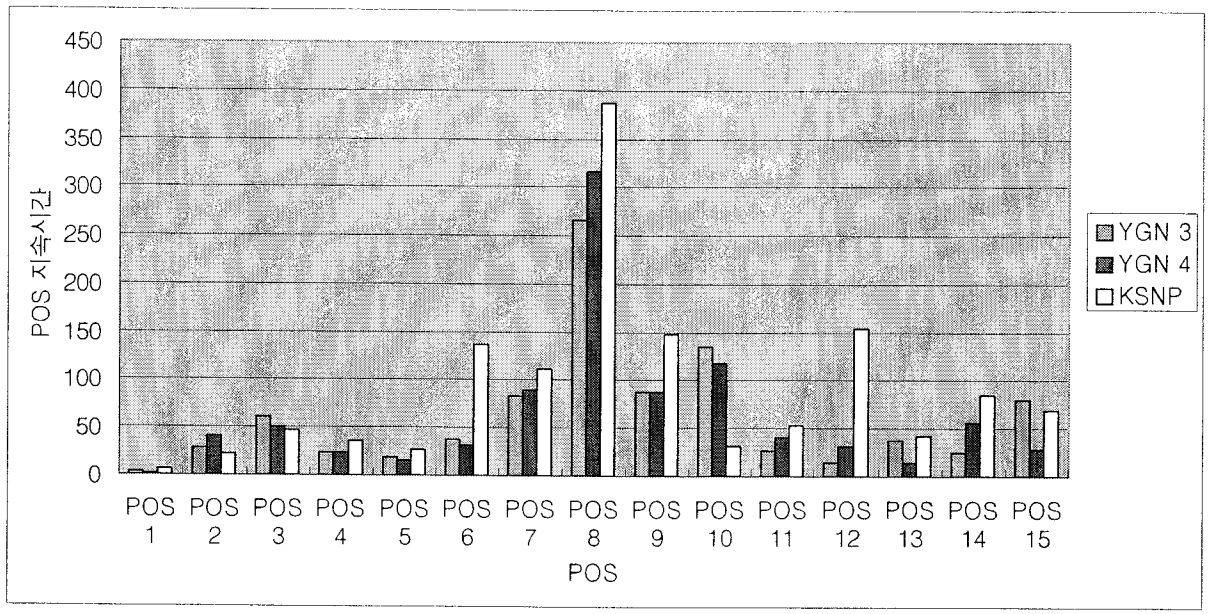


그림 3-6. 표준원전 POS별 소요시간에 대한 신·구 추정치 비교

3. 초기사건 분석 분야의 등급 개선

국내 표준원전의 정지/저출력 PSA 모델을 대상으로 ANS Standard (Draft)에 따라 모델 등급 평가를 수행하였고, 그 결과 초기사건 분석 분야에서는 총 30개 요건들 중 I 등급 이하가 15개 요건이고, II 등급 이상이 15개 요건인 것으로 판정되었다. 초기사건 분석 분야의 등급 평가 결과로서 파악된 미비점 및 개선 사항들을 정리하면 다음과 같다 (표 3-2 참조).

○ 초기사건 선정 시 구조적·체계적인 방법론 적용 및 문서화

○ 국내원전의 운전 경험 반영

○ 초기사건 선정 근거 및 다른 PSA 업무와의 연계성에 대한 문서화

○ 초기사건 그룹화에 대한 체계적이고 구조적인 방법론 적용

○ 초기사건 선행자(Precursor) 분석 결과 반영

○ 다중 호기 초기사건 분석

본 과제에서는 초기사건 분석 분야에서 도출된 미비점을 개선하기 위하여 RFP에 따라 아래와 같은 방법론 및 모델 개선 업무를 수행하였고, 그 결과 10개의 I 등급 요건들이 II 등급으로 개선되었다 (표 3-3 참조).

○ 논리적 평가 방법, 경험적 평가 방법 및 공학적 평가 방법를 체계적으로 결합한 초기사건 분석 방법론을 개선하고, 개선된 방법론에 의한 표준원전 초기사건 재분석

○ 초기사건 자료 수집 및 DB 구축 (625건)

○ 초기사건 DB 상세 분석 (특히, 정지냉각 상실사고의 원인별 분석 수행)

○ 초기사건 DB 검색 및 분석 프로그램 개발 (LEDB)

○ 정지/저출력 고유 특성 기인자 분석 (반응도 사고 분석)

여기서, DB 검색 및 분석 프로그램 - LEDB (Low Power and Shutdown

Event DataBase) - 은 표준원전 초기사건 재분석을 위하여 직접 이용하였음에도 불구하고, 연구 목적상 일차적으로 국내 원전의 초기사건 저감을 통한 정지/저출력 안전성 향상을 위해 개발된 것이므로 보고서 작성의 편의상 초기사건의 수집 자료원, DB 및 상세 분석 결과와 함께 본 보고서의 제 3장 2절에 기술하기로 하겠다. 이들을 제외한 나머지 항목들만 이어지는 섹션에서 순차적으로 연구 내용 및 결과들을 간략하게 소개하기로 하겠다.

가. 초기사건 분석 방법론 개선 및 표준원전 적용

초기사건이란 안정적인 발전소 운전 상태 (plant steady state operation)의 유지를 방해하는 사건으로 이러한 사건의 발생 후 적당한 안전 조치나 사고 완화 기능이 실패할 경우 발전소 안전성에 중대한 위험 (예를 들면, 노심손상)으로 이어질 잠재성이 있는 비정상 사건을 말한다. 이러한 초기사건의 분석을 위해서 전출력 및 정지/저출력 PSA의 구분 없이 일반적으로 다음과 같은 분석 절차가 적용될 수 있다.

○ 안전기능 정의

○ 초기사건 기인자 선정 (initiator identification)

○ 초기사건 선별 (screening) 및 그룹핑 (grouping)

○ 초기사건 빈도 추정

상기의 절차들에 대한 세부적인 접근 방법들에 있어서도 전출력과 정지/저출력 PSA에서 차이는 없으나, 다른 항목과는 달리 정지/저출력 초기사건 기인자 선정을 위한 세부 방법론은 정지/저출력 운전의 특성이 고려되어야 하므로 전출력 운전의 경우와는 매우 다를 수밖에 없다. 이는 정지/저출력 운전 기간 동안 매우 다양한 운전 상태의 전이(transition)가 일어날 뿐만 아니라 많은 정비 활동이 이루어지기 때문이다. 이렇듯 정지/저출력 초기사건 기인자 선정을 위한 구체적이고 체계적인 방법이 요구됨에도 불구하고, 아직 통일된 방법론이 정립되어 있지 않은

실정이다. 이에 따라, 본 과제에서는 정지/저출력 초기사건 기인자 선정 방법에 대한 연구를 수행하였으며, 그 결과로 다음의 세 가지 방법을 결합한 혼합 모델(hybrid model)을 제시하였다 [박진희, 2005].

○ 논리에 의한 기인자 선정 방법

○ 경험에 의한 기인자 선정 방법

○ 공학적 판단에 의한 기인자 선정 방법

제안된 혼합 모델은 각각의 방법에 의해 초기사건 기인자 목록을 작성한 다음 이들 목록의 상호 비교 분석 과정 (선별 및 그룹핑 과정)을 통하여 최종 초기사건 목록을 도출하게 된다. 본 과제에서는 표준원전의 정지/저출력 초기사건 재분석에 혼합 모델을 적용하였으며, 각각의 방법에 의한 주요 적용 과정 및 결과(선정 방법별 기인자 목록 및 최종 초기사건 목록)들을 아래에서 간단히 기술하기로 한다. 특히, 경험에 의한 평가 방법의 적용을 위한 기초자료로 개발된 정지/저출력 운전 중의 사건 DB, 공학적 판단에 의한 평가 방법으로 수행된 반응도 사건에 대한 표준원전 적용 결과는 별도의 세션으로 다루어질 것이다.

(1) 논리에 의한 기인자 선정 방법

논리에 의한 기인자 선정 방법은 일반적으로 전출력 PSA에서 이용하는 주논리도 (MLD; Master Logic Diagram) 작성 기법을 정지/저출력 초기사건 기인자 선정을 위해 적용함을 의미한다. MLD는 PSA 모델에서 최상위 논리로 발전소의 운전으로 인한 공중의 안녕과 건강에 미치는 위험요소(대량의 방사능 방출)를 정의하고 정의한 위험요소가 발생하기위한 조건들을 고장수목을 이용한 top-down 방식으로 연역적 사고에 의해 원인을 도식화한 것으로 초기사건의 도출을 위해 전출력에서 일반적으로 이용하는 방법이다. 본 과제에서는 그림 3-7에 예시된 바와 같이 정지/저출력 운전 모드에 대한 MLD를 개발하였다[한석중, 2003b]. 최종적으로 표준원전의 정지/저출력 운전모드에 대하여 개발된 MLD 기법을 적용한 결과, 선정된 초기사건 기인자 목록은 총 26개로 표 3-8에 기술된

바와 같다.

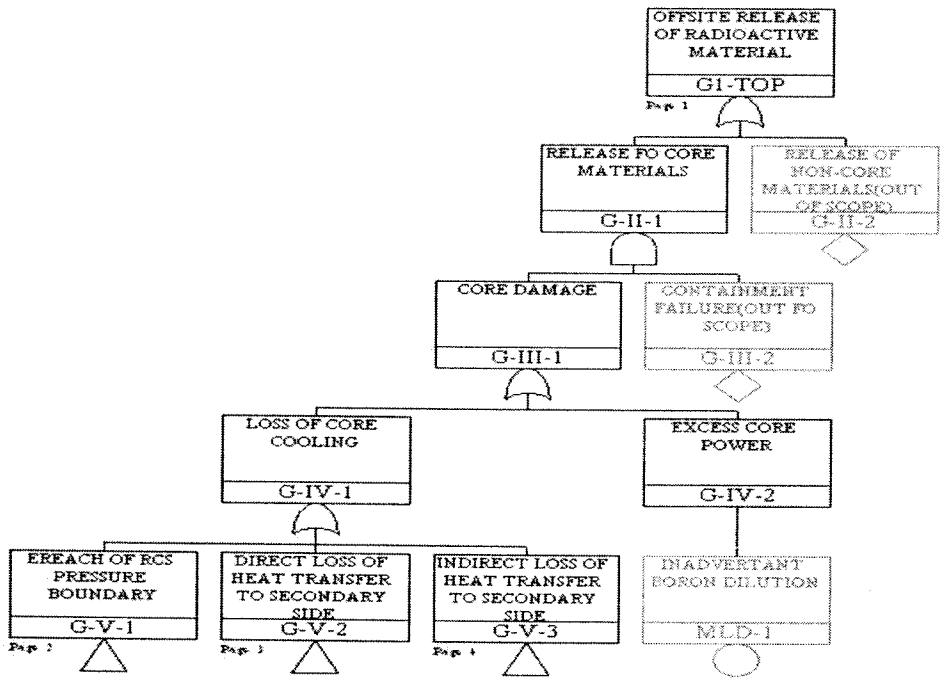


그림 3-7 정지/저출력 운전 모드에 대한 주논리도(MLD) (1/3)

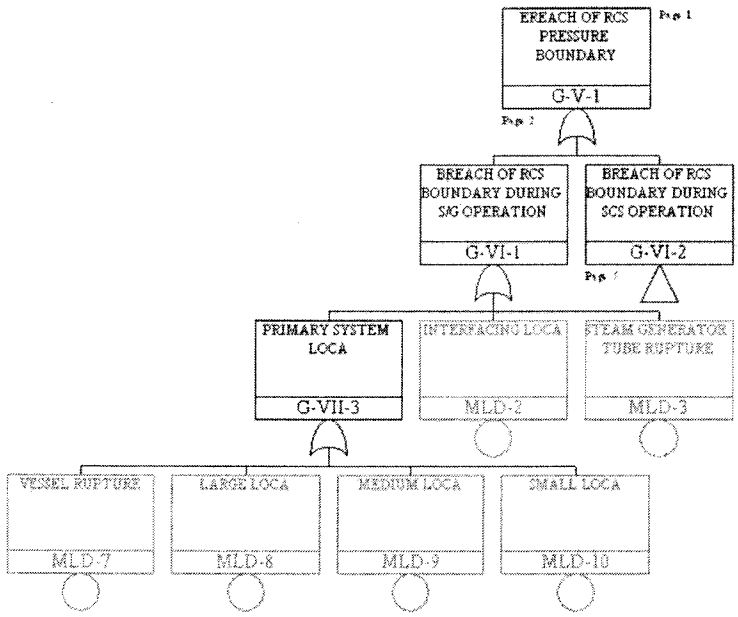


그림 3-7 정지/저출력 운전 모드에 대한 주논리도(MLD) (2/3)

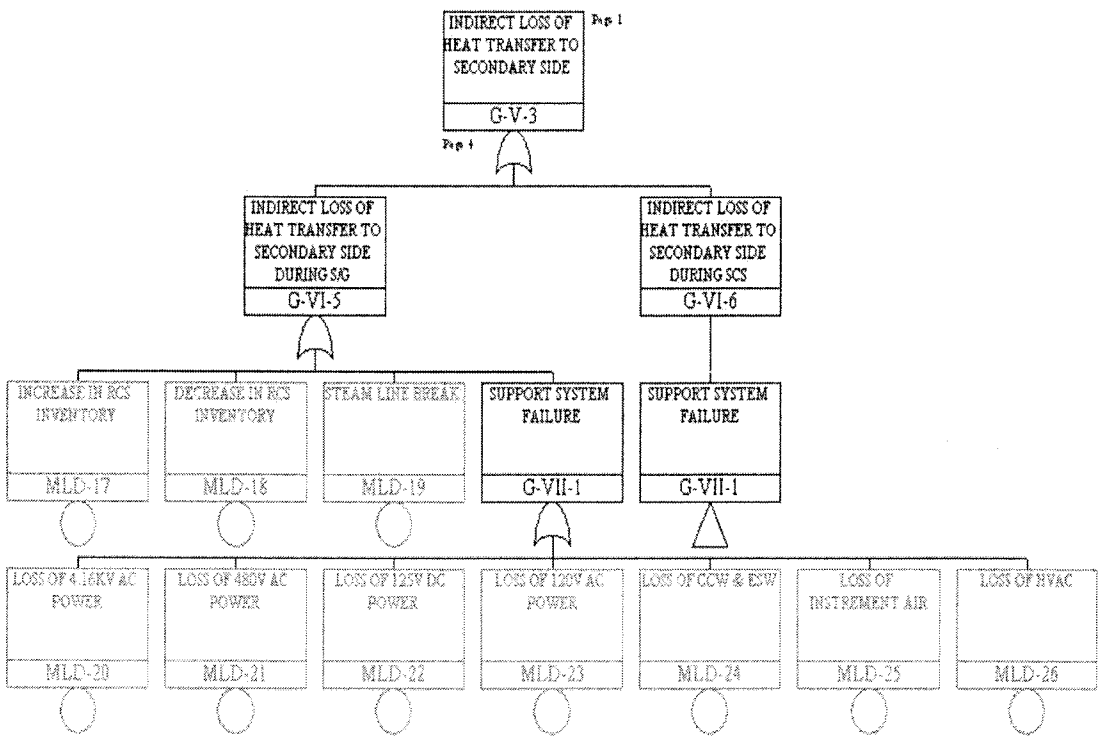


그림 3-7 정지/저출력 운전 모드에 대한 주논리도(MLD) (3/3)

표 3-8 MLD 기법에 의해 선정된 표준원전 초기사건 기인자 목록

	MLD 번호	설명	비고
1	MLD-1	Inadvertant Born Dilution	
2	MLD-2	Interfacing LOCA	
3	MLD-3	Steam Generator Tube Rupture	
4	MLD-4	Maibtenance related LOCA Inside Containment	
5	MLD-5	Maintenance related LOCA Outside Containment	
6	MLD-6	LTOP	
7	MLD-7	Vessel Rupture	
8	MLD-8	Large LOCA	
9	MLD-9	Medium LOCA	
10	MLD-10	Small LOCA	
11	MLD-11	Loss of RCS Flow	
12	MLD-12	Loss of MFWS	
13	MLD-13	Loss of Steam Flow	
14	MLD-14	Loss of Offsite Power	
15	MLD-15	Loss of SCS Flow	
16	MLD-16	Loss of RCS Level during Mid-Loop Operation	
17	MLD-17	Increase in RCS Inventory	
18	MLD-18	Decrease in RCS Inventory(Non-LOCA)	
19	MLD-19	Steam Line Break	
20	MLD-20	Loss of 4.16kV AC Power	
21	MLD-21	Loss of 480V AC Power	
22	MLD-22	Loss of 125V DC Power	
23	MLD-23	Loss of 120V AC Power	
24	MLD-24	Loss of CCW & ESW	
25	MLD-25	Loss of Instrument Air	
26	MLD-26	Loss of HVAC	

(2) 경험에 의한 기인자 선정 방법

경험에 의한 초기사건 기인자 선정을 위해서는 우선 정지/저출력 운전 중에 발생한 사건/사고에 대한 경험 자료가 요구된다. 이는 논리에 의한 기인자 선정 방법인 MLD에서 혹시 누락되었을지도 모를 초기사건 기인자에 대한 정보를 경험 자료를 통해 비교 분석함으로서 초기사건 분석의 완전성을 도모하기 위함이다.

이를 위해 수집된 경험 자료들은 1973년부터 1999년도까지의 외국에서 발생한 총 625건이었으며, 발전소 유형별 국내 원전(2건)을 포함한 가압 경수형(PWR) 422건, 비등 경수형(BWR) 203건으로 분류된다[박진희, 2003a; 박진희, 2003b]. 앞서 언급한 바와 같이 본 연구에서는 국내 원전의 초기사건 저감을 통한 정지/저출력 안전성 향상을 위해 현장에서 손쉽게 이용할 수 있도록 수집된 경험 자료를 DB화하고 자료 검색 및 분석용 프로그램 (LEDB; Low power and shutdown Event DataBase)을 개발한 바 있다. 표준원전에 대한 초기사건 기인자 선정을 위해 LEDB 프로그램을 이용한 것은 당연하나, 보고서 작성의 편의상 경험 자료에 대한 보다 상세한 분석 결과들은 LEDB를 기술하고 있는 본 보고서의 제 3장 제 2절에 함께 기술되어 있다. 여기서는, 간단히 이들을 활용하여 표준원전을 대상으로 경험적 방법에 의한 초기사건 기인자의 선정 결과만을 간단히 기술하기로 한다.

경험에 의한 기인자 선정 결과는 정지냉각상실, 냉각재 상실, 과도사건 및 기타 사건으로 나누어 최종적으로 총 19개의 기인자 목록을 선정하였으며 이는 표 3-10에 기술하였다. 이들 경험에 의해 선정된 기인자들은 논리에 의해 선정된 기인자들과 함께 최종 초기사건 선정을 위한 기본 자료로 이용된다.

표 3-9 PWR 정지/저출력 운전 경험 자료에 의한 원인별 사건 분석 결과

대분류	기인자	원인분류	건수	총계
정지냉각 상실	흡입밸브 닫힘	오신호	36	68
		전기기기고장	16	
		기타	16	
	공기흡입	수위조절실패	38	60
		냉각재상실	10	
		RCS 가압	2	
		정지냉각유량증가	5	
		기타	5	
	정지냉각계통 고장	정지냉각 펌프고장	15	53
		열교환기 고장	3	
		강제정지	7	
		기타 기기 고장	14	
		오신호	5	
		기타	9	
냉각재 상실 (LOCA)	회수가능 냉각재 상실사고		27	28
	증기발생기 세관 파열		0	
	회수불능 냉각재상실사고		1	
과도사건	일반과도사건		33	114
	소외전원 상실사고		12	
	발전소 정전사고		0	
	4.16kV 모선 전원 상실사고		41	
	직류모선 전원상실 사고		3	
	필수모선 전원상실사고		14	
	기기냉각수 및 필수냉각수 상실 사고		4	
	공기조화계통 상실사고		0	
	압축공기 상실사고		0	
기타	반응도 사고		59	95
	저온과압사고		8	
	정지냉각기동실패		12	
	기타		16	

표 3-10 경험에 의한 초기사건 기인자 선정 결과

사건 분류	번호	기인자 분류
정지냉각 상실(Loss of Shutdown Cooling System)	1	흡입밸브 이상닫힘
	2	정지냉각 펌프 공기 흡입
	3	정지냉각 계통 고장
냉각재 상실(Loss of Coolant Accident)	4	회수가능 냉각재 상실사고
	5	증기발생기 세관 파열
	6	회수불능 냉각재상실사고
과도사건(General Transient)	7	일반과도사건
	8	소외전원 상실사고
	9	발전소 정전사고
	10	4.16kV 모선 전원 상실사고
	11	125V DC 전원상실 사고
	12	120V AC 필수모선 전원상실사고
	13	기기냉각수 및 필수냉각수 상실 사고
	14	공기조화계통 상실사고
	15	압축공기 상실사고
	16	480V 모선 및 전동기 제어반 전원 상실사고
기타	17	반응도 사고
	18	저온과압사고
	19	정지냉각기동실패

(3) 공학적 판단에 의한 기인자 선정 방법

정지/저출력 PSA의 초기사건 분석에는 대상 발전소의 정지/저출력 운전 방식과 설계 특성에 따른 발전소 고유의 초기 사건을 선정하는 것이 매우 중요하다. 이러한 발전소 고유의 초기사건은 정지/저출력 운전 전반에 걸친 공학적 분석 없이 논리적 분석 방법이나 경험적 분석 방법에 의해서는 완전히 파악될 수는 없다. 따라서, 공학적 판단에 의한 기인자 선정 방법은 대상 발전소 고유의 초기 사건을 도출하기 위해 논리적 및 경험적 방법의 보완적인 방법이라 할 수 있다.

본 분석에서는 국내 표준형원전에 대한 POS 재분석을 통하여 최신의 정지/저출력 운전 및 설계 특성을 파악하였으며, 이를 바탕으로 다음과 같이 세 가지의 국내 고유 기인자를 공학적 판단에 의해 추가 선정하였다.

○ 가압기 안전밸브(PSV; Pressurizer Safety Valve) 개방시험(Popping Test) 중 개방 고착(Stuck Open) 사고

○ 주증기 안전밸브(MSSV; Main Steam Safety Valve) 개방 시험 중 개방고착 사고

○ 가압기 만수위 운전 중 질량 및 에너지 유입에 의한 저온 과압 사고

(4) 표준원전 최종 초기사건 목록

초기사건 선정을 위해 혼합 모델 - 논리적 선정 방법, 경험적 선정 방법 및 공학적 선정 방법 - 을 표준원전에 적용한 결과, 표 3-11과 같이 정리될 수 있다.

이를 바탕으로 표준원전에서는 발전소 타 계통에 미치는 영향, 발전소 대응, 사고 완화 기능의 차이, 등을 고려하여 4 가지의 초기사건 그룹 - 정지냉각 상실 사고, 냉각재 상실 사고, 과도사건, 및 보조 계통 상실 사고 - 으로 나누어 기인자를 선별하였고, 최종적인 초기사건들은 표 3-12에서 보는 바와 같이 총 22개로 선정되었다. 마지막으로 이들 22개의 초기사건들은 발전소 운전 상태 (POS)별로 사고 발생 가능성 여부를 평가하게 되며 그 결과는 표 3-12에 함께 나타나 있다. 최종적으로 선정된 초기사건별 설명은 다음과 같다.

<u>기계적 고장에 의한 정지냉각 기능 상실사고</u>

정지냉각계통 고장은 펌프, 밸브고장, 배관의 누설로 인한 고장과 열교환기의 고장 등과 같은 다양한 기기의 고장에 의해 정지냉각 기능을 상실시키는 초기사건이다. 이 초기사건은 정지냉각계통이 운전 중인 POS 3에서부터 POS13에서 발생 가능하다. 정지냉각기능 상실은 발생 원인에 따라 계통 운전에 미치는 영향이 다르며 사건 발생이후 사고 완화 방법에 영향을 줄 수 있기 때문에 이들에 대한 상세 분류가 필요하다. 고장 중에는 정지냉각계통의 대기 중인 다른 계열에까지 영향을 미칠 수 있으며 고장의 종류에 따라서는 후속 복구조치를 불가능하게 하는 고장도 있다. 따라서 이들 기계적 고장에 의한 정지냉각 기능 상실 초기사건은 다음과 같이 분류하였다.

○ 정지냉각 기능 상실 (S1)

○ 부분 복구불능 정지냉각 기능 상실 (S2)

저수위에 의한 정지냉각 기능 상실

부분 충수운전 중에 발생하는 사건으로 수위 감소로 인해 정지냉각 펌프에 공동현상이 발생하여 정지냉각 기능이 상실되는 사건이다. 이러한 사건이 발생하면 운전 중인 정지냉각 펌프에 공기가 유입되어 재가동에 어려움이 있으며, 펌프가 손상을 입어 단시간 내에 복구가 불가능하게 된다. 따라서 이 초기사건에서는 운전 중 정지된 계열의 복구가 불가능한 것으로 가정한다. 부분 충수 수위로 배수하는 과정에서 발생하는 과배수 사건과 배수가 완료된 부분 충수 운전 중에 발생하는 저수위 사건으로 구분된다.

○ 과배수 사건 (SO)

○ 저수위 사건 (SL)

냉각재 상실사고

냉각재 상실사고는 충전 용량을 초과하는 원자로 냉각재 누출 사고를 나타내며 이들 사고는 누출량, 즉 파단 크기에 따라 나누어진다. 이들은 원자로냉각재계통이 건전성을 유지하고 있으며, 어느 정도 압력이 유지되는 상태인 POS 1, 2, 3과 13, 14, 15에 대해 적용되었다. 일반 냉각재 상실사고는 소형, 중형, 대형의 파단 범주를 갖는 3개의 초기사건이 선정된다. 본 분석에서는 각 사건의 성공기준은 전출력 사건과 동일하다고 가정하였다.

○ 대형 냉각재 상실사고 (LL)

○ 중형 냉각재 상실사고 (ML)

○ 소형 냉각재 상실사고 (NL)

회수 가능 냉각재 상실사고

여러 원인에 의해 원자로 냉각재가 원자로냉각재계통으로 재이송 될 수 있는 재장전수 탱크나 격납건물 집수조 등으로 누설되는 초기사건을 나타낸다. 본 분석에서는 최소 유량관을 통한 냉각재 상실사건을 대표적인 회수 가능 냉각재 상실사고로 선정하였다. 이 외에 특정 POS에 적용되는 사건으로 POS 2에서 가압기안전밸브 개방고착에 의한 냉각재 상실사건과 POS 3에서 가압기 만수위 운전에서 발생할 수 있는 정지냉각 저온 과압 방지밸브 개방에 의한 냉각재 상실사건을 초기사건으로 선정하였다.

○ 회수 가능 냉각재 상실사고 (HL)

○ 가압기 안전밸브 개방고착 (PL)

○ 정지냉각 저온 과압 방지밸브 개방 (RL)

회수 불능 냉각재 상실사고

회수 불능냉각재 상실사고(JL)는 격납건물 외부 등 재순환 운전이 불가능한 곳으로 원자로 냉각재가 누설되는 사건을 나타낸다. 이 사건은 정비에 의한 냉각재 상실사건을 포함하는 사건으로 정비 및 여러 연결배관의 오조작 등의 원인에 의해 발생한다. 이 외에 특정 POS에 적용되는 사건으로 POS 3에서 저온 과압 사고에 의한 냉각재 상실사건을 제 3장 1절 4항에 기술되어 있는 저온 과압 사고에 대한 열수력 분석 결과에 의거하여 초기사건으로 추가 선정하였다.

○ 회수 불능 냉각재 상실사고 (JL)

○ 저온 과압 사고 (LTOP)

증기발생기 세관파열

증기발생기 세관파열 사건(SG)은 냉각재 상실사고의 한 유형으로 일차측 냉각재가 증기발생기 세관의 파열 부위를 통해 이차측으로 누출되는 초기사건이다. 이 사건은 원자로냉각재계통에 압력이 유지되고 있고 증기발생기 2차측이 격리되어 있지 않은 POS 1, 2, 14와 15에서 발생할 수 있다. 이들 POS에서의 사고경위는 전출력 운전과 유사하다.

소외전원 상실

소외전원 상실(LP)은 발전소로 공급되는 외부 전원이 상실되는 사고이다. 외부 전원이 상실되면 4.16kV 안전모선의 전압상실 신호에 의해 비상 디젤발전기가 기동되어 안전등급 모선에 비상전력을 공급하며, 각 안전등급 기기에는 정해진 순서에 따라 전력이 공급된다. 저출력 운전 시와 증기발생기를 이용한 냉각운전 중 즉, POS 1, 2 와 14, 15에서 소외전원 상실이 발생하면 발전소에 미치는 영향은 전출력 PSA와 거의 유사하다.

발전소 정전 사고

발전소 정전(LX)은 발전소 외부로부터 공급되는 외부 전원이 차단되는 소외전원 상실시 비상 디젤발전기가 이용 불가능하여 발생하는 초기사건이다. 발전소 정전사고가 발생하면 일부 축전지를 통해 전력을 공급받는 제어, 계측기기 등 일부 기기를 제외한 전력을 이용하는 모든 기기가 이용이 불가능하게 되어 초기사건으로 선정한다. POS 1, 2 와 14, 15에서 발전소 정전이 발생하면 발전소에 미치는 영향은 전출력 경우와 거의 유사하다. POS 3부터 13에서 발전소 정전이 발생하면 운전 중인 정지냉각 펌프가 정지되어 정지냉각 기능을 상실하게 되며, 이때 대부분의 기기들은 운전이 불가능하다.

4.16kV 전원 상실

정지냉각을 수행하는 계열에 전력을 공급하는 4.16kV 전원 상실사고(KV)는 정지냉각 기능 상실과 동시에 같은 계열의 사고 완화에 이용되는 계통의 운전에 영향을 주게 된다. 따라서 정지냉각계통이 운전 중인 계열의 안전등급 4.16kV 교류 모선의 전력 상실을 독립된 초기사건으로 선정한다.

기기냉각 상실

기기냉각 기능 상실(CC)은 정지냉각 열교환기에 대한 냉각수 공급 중단으로 정지냉각 기능 상실을 유발하며 같은 계열의 고압안전주입 펌프나 격납건물 살수 펌프의 운전을 불가능하게 하여 초기사건 발생 이후 사고 완화에도 영향을 미친다. 따라서 이를 독립된 초기사건으로 선정한다.

125V 직류 전원 상실

POS 1과 15에서 125V 직류 전원 상실(DC)은 원자로를 정지시키고 기동 급수 펌프와 터빈 우회밸브를 사용한 이차측 냉각 운전을 저해한다. POS 2와 14에서는 원자로가 이미 정지되어 있지만 직류 전원 상실에 의해 기동 급수 펌프와 터빈 우회밸브를 사용한 이차측 냉각 운전을 저해하므로 초기사건으로 선정하며 이는 이후의 사고 완화 시 제어 전력을 공급받는 고압안전주입, 저압안전주입, 보조급수 펌프들의 운전에 영향을 준다. 따라서 125V 직류 전원 상실은 POS 1, 2, 14, 15에 대해서만 적용되며, 사고 경위는 전출력 PSA와 유사하다.

일반 과도사건

일반 과도사건(T1)은 단순한 원자로 정지나, 증기발생기를 이용한 냉각운전 중 발전소 계통에 과도상태가 발생한 경우로 저온정지 상태로 발전소를 냉각하는데 특별한 문제를 발생시키지 않는 과도사건을 나타내며 초기사건으로 선정한다.

주급수 상실 과도사건

주급수 상실 과도사건(T2)은 과도사건 발생으로 기동급수 펌프를 포함한 주급수 계통을 이용할 수 없는 사건을 나타낸다. 기동급수 펌프를 이용한 냉각운전이 불가능한 주급수 상실 과도사건이 발생하면 보조급수계통을 이용해야만 하므로 초기사건으로 선정한다.

터빈 우회 복수기 밸브 상실 과도사건

터빈 우회복수기 밸브 상실 과도사건(T3)은 과도사건 발생으로 터빈을 우회하여 복수기로 증기를 방출하는 밸브를 이용하지 못하게 하여 원자로 냉각에 영향을 주는 사건을 나타낸다. 복수기 진공 상실과 같은 사건이 발생하면 터빈을 우회하여 증기를 방출하는 밸브 8개 중에 복수기로 증기를 방출하는 6개의 밸브의 사용이 불가능하게 되어 증기발생기 대기덤프 밸브나 복수기 우회 밸브를 통하여 대기로 방출하는 2개의 밸브만을 이용하므로 독립적인 초기사건으로 선정한다.

주급수 및 터빈 우회 밸브 상실 과도사건

주급수 및 터빈 우회 밸브 상실 과도사건(T4)은 사건 발생으로 주급수와 터빈을 우회하여 증기를 방출하는 밸브를 동시에 이용하지 못하게 하는 사건을 나타낸다. 이 사건에는 주급수와 주증기 차단 밸브를 동시에 폐쇄시키는 과도사건이 포함되며, 주증기 안전밸브 개방고착 사건도 포함한다. 이와 같은 사건이 발생하면 보조급수 계통을 이용하여 증기발생기에 급수를 공급하며, 증기발생기에서 발생하는 증기는 증기발생기 대기 덤프 밸브를 이용하여 방출하여야 하므로 초기사건으로 선정한다.

표 3-11 정지/저출력 초기사건 기인자별 비교표(1/2)

사건 분류	MLD 분석 결과		경험 분석 결과	공학적 분석 결과	최종 선별 결과	발생가능 POS
정지냉각 상실 사고	MLD-15	Loss of SCS Flow	흡입밸브 이상닫힘		선별 제거	POS 3,4,5,6,7,9,10,11,12,13
	MLD-15	Loss of SCS Flow	정지냉각기동실패		선별 제거	POS 3
	MLD-16	Loss of RCS Level	정지냉각 펌프 공기 흡입		SL과 SO로 분리	POS 4,5,11
	MLD-15	Loss of SCS Flow	정지냉각 계통 고장		S1과 S2로 분리	POS 3,4,5,6,7,9,10,11,12,13
냉각재 상실 사고	MLD-8	Large LOCA			LL	POS 1,2,14,15
	MLD-9	Medium LOCA			ML	POS 1,2,14,15
	MLD-10	Small LOCA			NL	POS 1,2,14,15
	MLD-3	Steam Generator Tube Rupture	증기발생기 세관 파열		SG	POS 1,2,14,15
	MLD-4	Maintenance related LOCA inside Containment	회수가능 냉각재 상실사고		HL	POS 3,4,5,6,7,9,10,11,12,13
	MLD-5	Maintenance related LOCA outside Containment	회수불능 냉각재 상실사고		JL	POS 3,4,5,6,7, 9,10,11,12,13
	MLD-2	Interfacing LOCA			선별 제거	POS 1,2,14,15
	MLD-7	Vessel Rupture			선별 제거	POS 1,2,14,15
				PSV 개방고착사고	PL	POS 2

표 3-11 정지/저출력 초기사건 기인자별 비교표(2/2)

사건 분류	MLD 분석 결과		경험 분석 결과	공학적 분석 결과	최종 선별 결과	발생가능 POS
과도사건	MLD-11	Loss of RCS Flow	일반과도사건		T1	POS 1,2,14,15
	MLD-17	Increase in RCS Inventory			T1	POS 1,2,14,15
	MLD-18	Decrease RCS Inventory			T1	POS 1,2,14,15
	MLD-19	Steam Line Break			T4	POS 1,2,14,15
				MSSV 개방고착사고	T4	POS 2
	MLD-12	Loss of MFWS			T2	POS 1,2,14,15
	MLD-13	Loss of Steam Flow			T3	POS 2
	MLD-14	Loss of Off-site Power	소외전원 상실사고		LP	모든 POS
			발전소 정전사고		LX	모든 POS
	MLD-20	Loss of 4.16kV AC Power	4.16kV 모선 전원 상실사고		KV	모든 POS
	MLD-21	Loss of 480V AC Power	480V 모선 및 전동기 제어반 전원 상실사고		선별 제거	모든 POS
	MLD-22	Loss of 125V DC Power	125V DC 전원 상실사고		DC	모든 POS
	MLD-23	Loss of 120V AC Power	120V AC 필수모선 전원 상실사고		선별 제거	모든 POS
	MLD-24	Loss of CCWS & ESWS	기기냉각수 및 필수냉각수 상실사고		CC	모든 POS
	MLD-26	Loss of HVAC			선별 제거	모든 POS
	MLD-25	Loss of Instrument Air			선별 제거	모든 POS
기타	MLD-1	Inadvertant Boron Dilution	반응도 사고		선별 제거	POS 2,3,4,5,6,7,10,11, 12,13,14
	MLD-6	LTOP	저온 과압 사고	저온 과압 사고	LTOP	POS 3, 13

표 3-12. 표준원전 POS별 초기사건 적용 표

POS / 사고종류*	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
정지냉각 기능 상실															
S1			O	O	O	O	O		O	O	O	O	O		
S2			O	O	O	O	O		O	O	O	O	O		
SO					O						O				
SL					O						O				
냉각재 상실사고															
LL, ML, NL	O	O	O										O	O	O
(회수가능 냉각재 상실사고)															
HL			O	O	O	O	O		O	O	O	O	O		
RL			O												
PL		O													
(회수불능 냉각재 상실사고)															
JL			O	O	O	O	O		O	O	O	O	O		
LTOP			O												
SGTR (SG)	O	O												O	O
소외전원상실 (LP)	O	O	O	O	O	O	O		O	O	O	O	O	O	O
발전소정전 (LX)	O	O	O	O	O	O	O		O	O	O	O	O	O	O
보조계통 기능 상실															
CC	O	O	O	O	O	O	O		O	O	O	O	O	O	O
KV	O	O	O	O	O	O	O		O	O	O	O	O	O	O
DC	O	O												O	O
과도사건															
T1	O	O												O	O
T2	O	O												O	O
T3	O	O												O	O
T4	O	O												O	O

* 정지냉각 기능 상실 (S1), 부분 복구불능 정지냉각 기능 상실 (S2), 과배수 사건 (SO), 저수위 사건 (SL), 대형 냉각재 상실사고 (LL), 중형 냉각재 상실사고 (ML), 소형 냉각재 상실사고 (NL), 회복 가능 냉각재 상실사고 (HL), 가압기 안전밸브 개방고착 (PL), 정지냉각 저온 과압 방지밸브 개방 (RL), 회복 불능 냉각재 상실사고 (JL), 증기발생기 세관파열 (SG), 소외전원 상실 (LP), 발전소 정전 사고 (LX), 저온 과압 사고(LTOP), 4.16kV 전원 상실 (KV), 기기냉각 상실 (CC), 125V 직류 전원 상실 (DC), 일반 과도사건 (T1), 주급수 상실 과도사건 (T2), 터빈 우회 복수기 밸브 상실 과도사건 (T3), 주급수 및 터빈 우회 밸브 상실 과도사건 (T4)

나. 정지/저출력 특성 기인자 분석

본 연구는 정지/저출력 특성 기인자 분석의 일환으로 붕소 희석에 의한 반응도 사고 발생 가능성을 표준원전에 대하여 분석하였다. 이는 기존의 표준원전 정지/저출력 PSA 모델에서 붕소 희석에 의한 반응도 사고의 발생 가능성에 대한 검토가 충분하지 않은 상태에서 선별 제거되었기 때문이다. 붕소 희석 사고란 운전원의 실수 또는 잘못된 계통 운전 등으로 초래된 붕소 농도 감소로 인하여 노심에 정반응도 (positive reactivity)가 삽입되는 초임계 노심손상 사고를 말한다. 먼저, 반응도 사고와 관련한 연구 동향을 간단히 살펴보면 다음과 같다.

지금까지 정지/저출력 PSA 및 사고 해석에서 고려되어 온 반응도와 관련한 주요 사고 원인들은 다음과 같다[Jacobson, 1989; Westinghouse, 1992].

○ 제어봉 집합체의 인출

○ 원자로 냉각재 펌프(Reactor Coolant Pump; RCP)의 기동

○ 부적절한 핵연료 집합체의 장전

○ 부적절한 붕소희석

이들 중 보편적으로 제어봉 집합체 인출에 의한 반응도 사고가 주된 반응도 사고로 고려되어 왔으나, 최근 프랑스를 중심으로 미국 및 독일 등지에서 국부적 또는 급속 붕소희석(Local or Rapid Boron Dilution, 이하 단순히 "붕소희석"으로 기술)에 의한 반응도 사고에 대한 연구를 진행된 결과 붕소희석에 의해서도 급격한 반응도 사고가 유발될 가능성이 높고 이로 인한 노심 손상될 확률도 무시될 수 없는 수준이라는 것이 발표된 바 있다. 하지만, 붕소희석으로 인한 반응도 사고에 대한 국내의 연구는 외국에 비해 미비한 실정이다.

본 과제에서는 정지/저출력 PSA 모델 개선을 위해 표준원전에 대하여 붕소희석으로 인한 반응도 사고의 발생 가능성에 대한 검토가 우선적으로 필요하며, 이를 위해 정성적 상세 선별 분석 방법에 의거하여 다음과 같은 분석 절차에 따라 수행하였다.

○ 붕소 희석 사고에 관한 외국의 선행 연구 결과 및 운전 경험 조사 분석

- 정지/저출력 운전 시 발생 가능한 사고 시나리오 선정
- 사고 시나리오별 발생 확률 및 심각성 검토

○ 한국형 표준원전에 대한 시나리오 선별 분석

- 표준원전에 적용 가능한 붕소 희석 사고 시나리오로 변경
- 표준원전 발전소 운전 상태(POS)에 따른 시나리오의 적용 가능성에 대한 선별 분석
- 선별된 붕소희석 사고 시나리오에 대한 정성적 상세 분석 (시나리오별 발생빈도 및 결과의 심각성에 대한 정성적/정량적 비교 분석)

○ 상세 분석 결과를 바탕으로 초기사건 기인자로의 선정 여부 결정

상기의 분석 절차에 따른 자세한 연구 내용 및 결과들은 기술보고서 [박진균, 2003]에 기술되어 있고, 여기서 주요 결과들을 정리하면 다음과 같다.

○ 외국의 붕소 희석 반응도 사고 연구 결과와 운전 경험 자료[Jacobson, 1989; Westinghouse, 1992; Diamond, 1990; Diamond, 1992]들을 조사·분석하여 가압 경수형 원전(PWR)의 정지/저출력 운전 시에 적용 가능한 붕소 희석 사고 시나리오로 6개 관련 계통에서 총 15개를 선정하였다 (표 3-13 참조)

○ 외국의 자료로부터 붕소 희석 사고 시나리오들의 발생 확률 및 심각도 (사고 진행 속도)에 대한 분석 결과들은 표 3-13에 함께 정리된 바와 같다. 이들 중 가장 주목하여야 할 시나리오는 시나리오 5A와 4C로 판명된 반면, 시나리오 1C, 3 및 4A는 외국의 선행 분석에서 더 이상 고려할 필요가 없는 사소한 시나리오로 평가되었다.

○ 상기의 붕소 희석 사고 시나리오를 한국형 표준원전에 알맞은 형태로 변경하였고, 그 결과 시나리오에 대한 설명은 표 3-14에 정리된 바와 같다.

○ 상세 분석에 앞서 15개 붕소희석 시나리오별로 표준원전 POS에 따른 적용 가능성에 대하여 정성적 선별 분석을 먼저 수행하였다. 선별 분석 결과 표 3-15에서 알 수 있듯이 총 225개 (= 15개 시나리오 x 15개 POS) 대상 가운데 67개의 상세 분석 대상을 선별하였다. 상세 분석 대상 가운데 다음과 같은 이유로 시나리오 3, 4A, 4C에 해당하는 17개는 분석 대상에서 제외하였다. 따라서, 최종적으로 상세 분석 대상은 5개 관련 계통의 12개 시나리오에 대해 POS에 따라 총 50개로 선정되었다.

- 시나리오 4C는 작업자의 실수로 인한 증기발생기의 정비실수를 고려해야 하지만, 고려해야 하는 작업자의 실수 형태가 매우 다양할 뿐 아니라 현실적으로 이용 가능한 자료를 얻을 수 없기 때문에 상세 분석 대상에서 제외하였다

- 시나리오 3과 4A는 표 3-13에서 보듯이 외국의 선행 연구에서도 추가적인 검토가 필요하지 않은 시나리오로 판단되었기 때문에 제외하였다. 그러나, 중요하지 않은 시나리오로 평가된 시나리오 1C의 경우는 참조원전이 웨스팅하우스사의 Zion 원전을 대상으로 한 결과로 국내 표준원전의 계통 설계 및 운전 조건들이 다르기 때문에 상세 분석 대상으로 분류되었음에 유의하여야 한다.

○ 최종적으로 선별된 총 50개의 상세 분석 대상에 대하여 외국의 참조원전과 국내 표준원전의 설계 및 운전 방법의 차이를 고려한 정성적/정량적 상세 평가를 수행하였다. 붕소 희석 사고 시나리오와 관련하여 계통의 차이점에 근거한 상세 평가 결과를 정리하면 다음과 같다.

- 시나리오 1A, 1B, 1C 및 1D에 대한 상세 분석 결과 : 표준원전의 경우 외국의 참조원전인 Zion에 비해 RWT의 용량이 약 60% 이상 크고 붕소농도 또한 약 2배 이상 높게 유지되고 있으며, 특히 발전소가 운전모드 5와 6에 있을 경우에는 72시간에 한번씩 RCS와 RWT의 붕소농도를 확인하게 되어 있다 (표 3-16 참조). 이러한 설계 특성 및 기술지침서 요구

사항들을 모두 고려해 볼 때, RWT의 붕소 농도 희석 확률은 참조 발전소에 비해 현저히 낮을 것으로 예측되기 때문에 표준원전에 대한 시나리오 1A, 1B, 1C 및 1D의 발생확률은 매우 낮을 것으로 판단된다.

시나리오 2A, 2B 및 2C에 대한 상세 분석 결과 : 표준원전의 경우 외국의 참조원전인 Zion에 비해 SIT의 용량 및 붕소농도가 약 2배이고, 특히 축압기의 수위 및 압력은 운전조(operating crew)의 교대시마다 확인하도록 되어 있다 (표 3-17 참조). 또한 표준원전 정상 운전 절차서에 따르면 원자로 정지 후 RCS 감압시, RCS 압력의 감소에 따라 SIT의 질소압력을 적절히 조절하여 주입압력을 감소시키다가 RCS 압력이 약 400 psi에 도달하면 SIT를 배기시키면서 SIT 차단밸브를 닫고 동시에 차단밸브의 전원도 차단하도록 명시하고 있다. 따라서, RCS 냉각재의 유입으로 인한 SIT의 붕소농도 희석 확률은 Zion에 비해 현저히 낮을 것으로 예측된다.

시나리오 4B에 대한 상세 분석 결과 : 외국의 참조원전과는 달리 한국형 표준원전 형태의 발전소에 적용되는 비상운전 절차서에는 역보충 냉각 방법이 없고 주증기 덤프를 통한 RCS 냉각이 고려된다. 또한 SGTR 발생 시 적용해야 하는 E-3 비상운전 절차서에서는 증기발생기를 통한 2차측 냉각재의 유입으로 초래될 수 있는 RCS 붕소희석을 방지하기 위해 "RCS 압력이 증기발생기 압력보다 낮을 때, 주기적인 RCS 붕소농도 확인을 수행한다."라는 항목이 명시되어 있기 때문에, 증기발생기를 통한 2차측 냉각재의 유입으로 붕소희석이 발생할 가능성은 매우 낮다고 판단된다.

시나리오 5A에 대한 상세 분석 결과 : 표준원전의 경우는 소외전원상실 사고가 발생하면 RCP로 공급되는 전원이 상실되면 디젤 발전기가 가동되어 충전펌프에 전원은 공급되지만, 운전원이 충전펌프의 기동스위치를 누르기 전에는 기동되지 않도록 설계되어 있다. 그러나 전원이 공급되면 운전 절차서에 따라 운전원은 1차계통의 냉각재 재고량 및 가압기의 수

위조절을 위해 충전펌프의 기동은 가능하므로 외국에 비해 발생확률은 현저히 낮다고 판단되지만 인간오류분석 결과에 따라 추후 판단되어야 한다.

- 시나리오 5B 및 5C에 대한 상세 분석 결과 : 표준원전의 경우, 원자로가 정지상태일 때 RCP는 Stop Seal을 사용한 기계적인 밀봉상태를 유지한다. 외국의 참조원전과는 달리 하기 때문에 RCP에 열 차단벽이 없기 때문에, 열 차단벽을 통한 누출 가능성은 고려할 필요가 없고, 원자로가 정지 상태에서 RCP는 Stop Seal을 사용한 기계적인 밀봉이므로 상당히 낮은 밀봉수 누출 가능성을 가지는 것으로 판단된다.
- 시나리오 6에 대한 상세 분석 결과 : 표준원전의 경우 정지냉각계통을 RCS로 연결하기 전에 두 계통간의 붕소 농도 차이를 측정하도록 계통 운전 절차에 명시되어 있고, 특히 정지냉각계통이 운전 중일 때는 1시간 간격으로 붕소 농도를 감시하도록 명시하고 있다. 따라서, 참조 원전에 비해 보다 훨씬 낮은 발생 확률을 가질 것으로 판단된다.

상기와 같은 상세 분석 결과를 바탕으로 붕소 희석 사고 시나리오에 대한 최종 결론은 다음과 같다.

○ 표준원전의 경우 예상 가능한 모든 붕소 희석 반응도 사고 시나리오들에 대해 대비 설계가 비교적 우수한 원전으로 모든 시나리오의 발생 확률은 현재까지 알려진 외국의 참조 원전들에 비해 충분히 낮은 발생 확률로 예측된다. 이로써, 현재 상태에서 분석된 모든 시나리오에 대해 낮은 발생 확률로 붕소 희석에 의한 반응도 사건은 초기사건에서 선별 제거될 수 있다.

○ 증기발생기의 보수작업을 수행하던 작업자의 실수로 인한 2차측 냉각재 유입을 고려하는 Swedish Scenario (4C)의 경우, 고려해야 하는 작업자의 오류 형태가 다양할 뿐 아니라 현실적으로 이용 가능한 자료가 빈약하기 때문에 인간오류에 대한 상세한 연구가 수행된 후 상세 분석이 가능하다.

○ 현재 우라늄 235의 최대 농축도는 3.5W%이하이다. 따라서, 부적절한 핵연료 집합체 장전으로 인한 노심손상 가능성은 거의 무시 가능하지만, 장주기 운전의 경우 농축도의 증가가 인해 반응도 희석 사고에 대한 재분석이 필요할 뿐만 아니라 부적절한 핵연료 집합체 장전으로 인한 반응도 사고 가능성에 대해서도 검토되어야 할 부분으로 판단된다.

표 3-13 반응도 사고 시나리오에 대한 분석결과

시나리오 관련계통	시나리오	설명	발생확률 (RY^{-1})	사고 진행속도
핵연료 재장전수 탱크	1A	Diluted RWT + Spurious SI	3.7e-8	빠름
	1B	Diluted RWT + Inadvertant Leakage to Reactor	1.5e-8	느림
	1C	Diluted RWT during Reactor Cavity Filling (Cavity Flushing으로 인한 경우 포함)	Not Significant	매우 느림
	1D	LOCA + Diluted RWT	2.7e-8 (최대값)	빠름
안전주입 탱크	2A	Diluted SIT + Inadvertant Opening of MOV	6.9e-10	빠름
	2B	Diluted SIT + Leaking MOV	4.1e-9	느림
	2C	LOCA + Diluted SIT	5.4e-8	빠름
격납건물 배수조	3	LOCA + RAS + Diluted Sump Water	Not Significant	빠름
증기 발생기	4A	LOCA + SGTR	Not Available	빠름
	4B	SGTR + LOOP + Backfill Cooldown	3.0e-7	빠름
	4C	Dilution during SG Maintenance [Swedish Scenario]	1.0e-8 이상	빠름
화학및 체적 제어 계통	5A	LOOP during Startup [French Scenario]	2.8e-5 (최대값)	빠름
	5B	Leaking RCP Seal during Pressurization	~1.0e-8	빠름
	5C	Leaking RCP Thermal Barrier during Pressurization	~1.0e-8	빠름
정지냉각 계통	6	Diluted SCS + SCS Startup	~1.0e-8	빠름

표 3-14 표준원전에 적용 가능한 붕소 희석 사고 시나리오

시나리오 No.	시나리오의 개요
1A	RWT가 희석되어 있고, 안전주입 계통이 동작할 수 있는 상태이며 RCS의 압력이 대기압으로 유지되는 상태에서, 부적절하게 발생된 안전주입 신호에 의해 고압/저압 안전주입 펌프가 기동될 경우 희석수의 노심 유입.
1B	RWT가 희석되어 있고, RCS의 압력이 대기압으로 유지되는 경우, RWT부터 노심으로의 부적절한 밸브 배열로 인한 유로가 형성되면, 핵연료 재장전수 탱크와 노심의 높이 차이에 의해 희석수가 노심으로 유입.
1C	RWT가 희석되어 있고, RWT에서 물을 공급받아 수행하는 cavity 충수나 water flushing을 사용한 cavity 청소 작업 시 희석수가 고온관을 통해 노심으로 유입.
1D	RWT가 희석되어 있고, LOCA로 인해 발생된 안전주입 신호가 발생하고, 이때 기동된 고압/저압 안전주입 펌프를 통해 희석수가 노심으로 유입된다.
2A	SIT가 희석된 상태이고 RCS 압력이 SIT 압력보다 낮게 유지되고 있을 때, SIT 차단밸브의 개방으로 인해 희석수가 노심으로 유입된다.
2B	SIT가 희석된 상태이고 RCS 압력이 SIT 압력보다 낮게 유지되고 있을 때, SIT 차단밸브의 누설로 인해 희석수가 노심으로 유입된다.
2C	SIT가 희석된 상태에서 LOCA 발생으로 인해 RCS의 압력이 SIT 압력 이하로 감소할 경우, 희석수가 노심으로 유입된다.
3	집수조로 붕소농도가 매우 낮거나 순수 유입되어 희석된 경우, RAS가 발생되면 희석된 냉각재가 고압안전주입 펌프에 의해 대규모로 노심에 유입된다.
4A	LOCA 발생으로 인해 RCS 압력이 급격히 떨어지고 있을 때 SGTR이 발생하여 2차측 냉각재가 1차측으로 급격히 유입된다.
4B	SGTR 발생 시 소외전원상실도 발생하여 RCP가 정지된 경우, 운전원이 RCS 후속냉각 방법으로 역보충(backfilling) 방법을 선택하면 2차측 냉각재가 정체구간으로 유입되기 때문에, RCP가 다시 기동될 경우 정체구간에 포함된 희석된 냉각재가 노심으로 급격히 유입된다.
4C	원자로가 정지된 상태이고 SCS가 동작중일 때, SG의 보수나 검사를 수행한 작업자의 실수로 인해 SG 튜브의 누설이 발생할 경우 2차측 냉각재가 정체구간으로 유입되기 때문에, RCP가 다시 기동될 경우 정체구간에 포함된 희석된 냉각재가 노심으로 급격히 유입된다.
5A	발전소 재기동 도중, RCS의 붕소농도 희석을 위해 VCT의 붕소농도를 낮추고 있을 때, 소외전원상실사고가 발생하여 RCP는 정지되고 RCS 내에 정체구간이 생성된다. 그러나 디젤발전기에 의해 전원이 공급되는 충전펌프는 소외전원 상실 시에도 계속 기동되어 VCT에 있던 희석된 냉각재가 모두 정체구간으로 주입되고, 소외전원이 회복되어 RCP가 재기동 될 때 노심으로 급격히 유입된다.
5B	정지냉각계통이 운전 중이고 RCS의 붕소농도 희석을 위해 VCT의 붕소농도를 낮추고 있을 때, RCP 밀봉수가 누출되어 RCS의 정체구간으로 유입된다. 이렇게 정체구간으로 유입된 밀봉수는 RCP 기동시 노심으로 급격히 유입된다.
5C	정지냉각계통이 운전 중일 때, 기기냉각계통의 순수가 RCP 열 차단벽(Thermal Barrier)을 통해 누출되어 RCS의 정체구간으로 유입된다. 이렇게 정체구간으로 유입된 밀봉수는 RCP 기동시 노심으로 급격히 유입된다.
6	노심의 잔열제거를 위해 SCS를 RCS에 연결시킬 때, SCS가 희석된 냉각재를 포함하고 있는 사실을 알 지 못하고 RCS에 연결시킬 경우 희석된 냉각재가 노심으로 급격히 유입된다.

표 3-15. 표준 원전의 POS별 반응도 사건 시나리오 발생가능성 도표

RCP 운전중															
SCS 운전중															
대기압 상태															
시나리오	POS 1	POS 2	POS 3	POS 4	POS 5	POS 6	POS 7	POS 8	POS 9	POS 10	POS 11	POS 12	POS 13	POS 14	POS 15
1A				O	O	O	핵연료 교체 작업 수행			O	O	O			
1B		O	O										O	O	
1C						O					O				
1D	O	O	O										O	O	O
2A	O	O	O										O	O	O
2B				O	O	O				O	O	O			
2C	O	O	O										O	O	O
3	O	O	O										O	O	O
4A	O	O	O										O	O	O
4B	O	O	O										O	O	O
4C				O	O	O				O	O				
5A													O	O	O
5B										O	O				
5C										O	O				
6			O												

표 3-16 참조원전과 표준원전의 RWT에 대한 설계사양 비교

	참조 원전 (Zion)	표준원전 (영광 5·6)
이름	RWST(Refueling Water Storage Tank)	RWT (Refueling Water Tank)
개수	1개	1개
탱크 체적	425,000gal (1.608×10^{6} ℓ)	698,000gal (2.642×10^{6} ℓ)
붕소 농도	1900 ~ 2100 ppm	4000 ~ 4400 ppm
RAS 발생조건	RWST 수위 ≤ 5%	RWT 수위 ≤ 7.6%
충전펌프 Suction	VCT 수위 ≤ 3인치 또는 13% (VCT 체적 = 약 2,900gal)	VCT 수위 ≤ 5% (VCT 체적 = 4,917gal)
기술지침서 (TS) 요구사항	최소 7일에 한번씩 붕소농도 및 저장된 붕산수의 체적을 확인	- 최소 7일에 한번씩 붕소농도 및 저장된 붕산수의 체적을 확인 (운전모드 1, 2, 3, 4) - 최소 72시간에 한번씩 RCS 및 RWT의 붕소농도를 확인(운전모드 5 및 6)
희석 확률	2.8×10^{-5}	$<< 2.8\times10^{-5}$

표 3-17 참조원전과 표준원전의 SIT에 대한 설계사양 비교

	참조 원전 (Zion)	표준원전 (영광 5·6)
이름	Accumulator	SIT (Safety Injection Tank)
개수	4개	4개
탱크 체적	7,000 gal (2.65×104 ℓ)	13,898 gal (5.26×104 ℓ)
N2 압력	625 psig	625 psig
붕소농도	1900 ~ 2100 ppm	4000 ~ 4400 ppm
기술지침서 (TS) 요구사항	- 최소 31일에 한번 씩 붕소농도를 확인 - 탱크 배수 시, 체적의 1% 이상을 초과하는 부피변화가 발생한 경우 6시간 내에 붕소농도를 확인	- 최대 9시간마다 한번씩 탱크 수위 및 압력을 확인 (근무일지 기입사항) - 최소 31일에 한번 씩 붕소농도를 확인 - 탱크 배수시 붕소농도를 확인
희석 확률	9.7×10^{-5}	$<< 9.7\times10^{-5}$

4. 성공기준 분석 분야의 등급 개선

국내 표준원전의 정지/저출력 PSA 모델을 대상으로 ANS Standard (Draft)에 따라 모델 등급 평가를 수행하였고, 그 결과 성공기준 분석 분야에서는 총 16개 요건들 중 I 등급 이하가 7개 요건이고, II 등급 이상이 9개 요건인 것으로 판정되었다. 성공기준 분석 분야의 등급 평가 결과로서 파악된 미비점 및 개선 사항들을 정리하면 다음과 같다 (표 3-2 참조).

○ 전출력 노심손상 정의와 불일치

○ 사고 경위별 임무시간 분석 미흡

○ 열수력 입력 자료의 보수성 개선 및 영향 평가 미흡

○ 문서화 보완

본 과제에서는 성공기준 분석 분야에서 도출된 미비점을 개선하기 위하여 RFP에 따라 아래와 같은 개선 업무를 수행하였고, 그 결과 4개의 I 등급 요건들이 II 등급으로 개선되었다 (표 3-3 참조).

○ 정지/저출력 PSA용 열수력 분석 체계 구축

- 최적 열수력 분석 코드 선정 (MARS V2.1)
- 표준원전 정지/저출력 PSA용 열수력 분석을 위한 코드 입력자료 마련
- 기존 정지/저출력 PSA의 열수력 분석 결과 (RELAP/MOD V3.2 & 3.3)와의 비교 분석을 통한 MARS 코드 체계의 유효성 검증
- 정지/저출력 열수력 분석 체계에 대한 연구 결과를 문서화

○ 정지/저출력 PSA 모델의 성공 기준 결정을 위한 기본사고에 대한 열수력 재분석

- 발전소 운전 상태(POS)에 따라 사고 경위 성공 기준 결정을 위한 기본사고 (정지냉각 상실사고)에 대한 열수력 분석 재수행

- 열수력 분석 결과의 문서화

이들의 연구 내용 및 결과들은 이어지는 섹션에서 순차적으로 간략하게 소개하기로 하겠다.

가. 정지/저출력 PSA용 열수력 분석 체계 구축

정지/저출력 위험도 정보 활용 의사결정이 가능하기 위해서는 보다 정확하고, 보수성 및 불확실성이 저감된 사고 경위 분석과 계통 성공 기준들의 결정이 요구되며, 이를 위해 최적의 품질을 보장할 수 있는 열수력 거동 분석 체계 구축이 필수적이다. 정지/저출력 PSA의 성공 기준 및 사고 경위 파악을 위한 열수력 분석은 PSA의 품질에 많은 영향을 미치고 있다. 본 과제에서는 정지/저출력 PSA 품질 개선을 위하여 최적의 열수력 분석 체계를 확보하기 위해 노력하였다. 이러한 노력의 일환으로 기존의 RELAP4/MOD3.2 코드 보다 한층 해석 능력이 향상된 것으로 알려져 있고 국내 연구진(한국원자력연구소)에 의해 개발된 MARS2.1 코드로 변경하여 검증 계산 등을 통한 정지/저출력 PSA용 최적 열수력 분석 체계를 마련하였다. 또한, RELAP5/MOD3.3 코드도 비교대상에 포함하여 MARS2.1과 RELAP4/MOD3.3의 계산능력도 비교하였다.

비교 대상으로 POS 5의 중력급수 시나리오를 선정하였다. 원자력 발전소 계획 예방정비 기간 동안 부분 충수 운전 시에는 정지냉각기능이 상실될 가능성이 다른 운전 모드에 비하여 상대적으로 높다. 이 운전 중에는 저온관 수위를 중간으로 일정하게 유지하여야 하나 수위의 출렁거림으로 인하여 수위를 중간으로 맞추지 못하고 중간 이하로 내려갈 수도 있다. 이렇게 되면 정지냉각펌프의 흡입구가 대기 중으로 노출되어 정지냉각펌프가 손상을 일으킨다. 저수위운전 중에는 증기발생기를 사용하여 잔열제거를 할 수 없기 때문에 정지냉각기능이 상실되면 노심에서 발생되는 잔열을 제거하기 위하여 안전주입계통을 사용하여 냉각재를 RCS로 주입하여야 한다. 안전주입계통이 작동되지 않으면 노심의 잔열을 제거할 수 없기 때문에 결국에는 노심손상에 이르게 된다. 사고발생 후 운전원이 사고완화를

위하여 어떤 조치를 취한다면 노심이 손상되는 시각이 상당히 지연될 수 있을 것이다. 사고발생 후 운전원이 취할 수 있는 조치중의 하나로 운전원이 수동으로 재장전수 탱크 (refueling water tank, RWT)의 냉각수를 RCS에 주입하는 것이 있다. 즉. 운전원이 RWT와 저온관을 연결하는 밸브를 열어서 중력을 이용하여 냉각수를 RWT로부터 RCS로 보충하는 것이다.

(1) 기하학적 모델링

표준원전 (영광 5, 6호기)는 2개의 11차 냉각재루프 구성된, 정상운전 시 열출력 2815 MWt의 가압경수로이다. 표준원전을 RELAP5/MOD3.2로 모의계산하기 위하여 그림 3-8과 같이 모델링하였다. 그림에서 보여주듯이 원자로용기가 모델되었고, 원자로 노심은 축방향으로 12개의 체적으로 모델 하였다. 각각의 1차 냉각재루프는 고온관, 12개의 체적으로 모델한 U자형 세관을 갖는 증기발생기, 2개의 흡입관, 2개의 원자로 냉각재 펌프, 그리고 2개의 저온관으로 구성되어 있다. 한 쪽 루프의 고온관에는 밀림관(surge line) 및 5개의 체적으로 모델한 가압기가 부착되어 있다. 정지 운전 중 정지냉각계통을 모의하기 위하여 각 루프의 고온관에는 정지냉각계통 흡입 측을, 저온관에는 정지냉각계통 방출 측을 경계 체적 (time dependent volume)으로 부착하였다.

실제 표준원전 정지운전 상황과 동일하게 모의하기 위하여 각 POS 상황에 맞게 다음과 같은 대기로 개방되었거나 폐쇄된 개구부를 고려하였다.

○ 3/4″ 원자로용기 상부 배기관,

○ 3/4″ 가압기 상부 배기관,

○ 수위를 측정하기 위해 각 루프의 고온관에 설치한 1″ tygon tube (설치되었을 경우 가압기 최상부 위치에서 대기로 노출),

○ 16″ 가압기 manway,

○ 16″ 증기발생기 입구 및 출구측 manway,

○ 6″ LTOP 밸브,

○ 가압기 안전밸브.

2차측 증기발생기는 그림에서와 같이 원통형 쉘과 주급수 유입 배관(downcomer), 습분 분리기(separator), 그리고 증기돔(steam dome)으로 모델 되었고, 주급수 및 보조급수는 경계 체적으로 모의하였다. 증기관에는 주증기 차단밸브 및 대기 방출 밸브를 부착하였으며, 사고 시 상황과 동일하게 모의하기 위해 모두 닫혀있도록 모델하였다. 원자로 노심 핵연료봉은 열구조물(heat structure)로 모델하여 이 열구조물이 열원(heat source)을 가지게 함으로써 원하는 수준의 잔열이 생성되도록 모의하였으며, 그 외 증기발생기 세관 등 열전달이 일어나는 기기들의 체적에도 열구조물을 부착하여 열전달이 가능하도록 모의하였다.

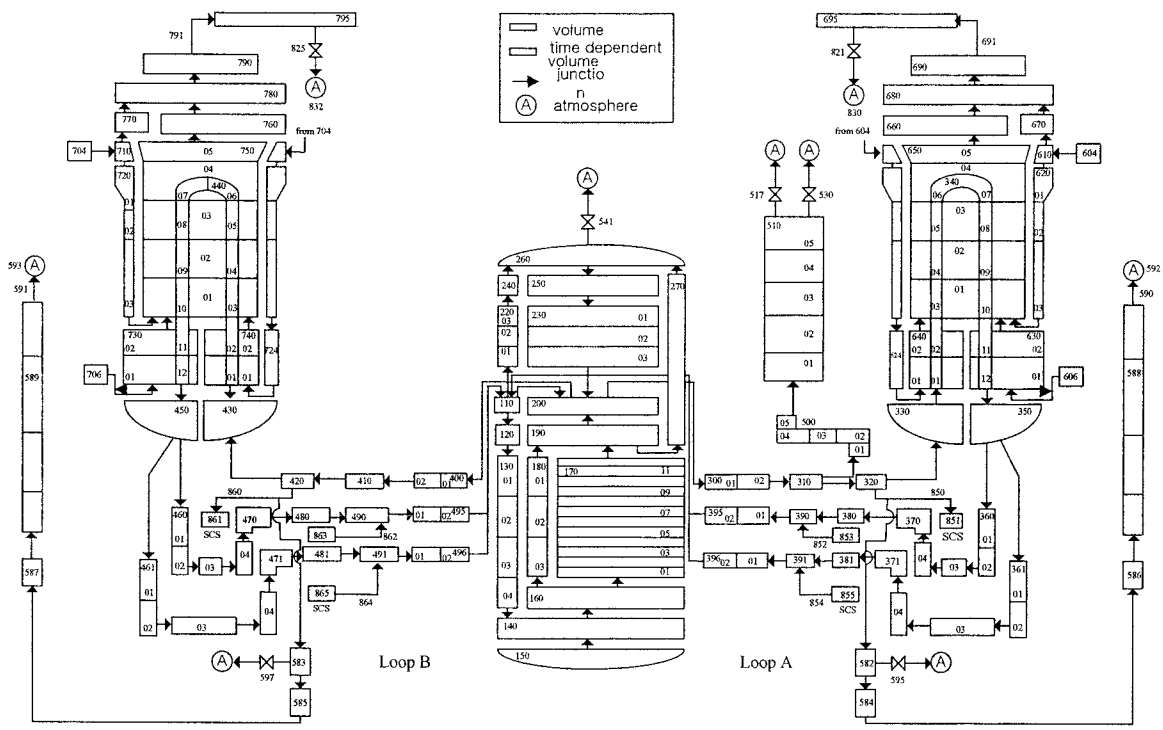


그림 3-8 표준원전에 대한 MARS 계산 체적

(2) 초기조건 및 경계조건

POS 5는 원자로 정지 후 원자로냉각재 수위를 고온관 혹은 저온관 중간수

위로 유지하는 1차 부분 충수 운전 상태이다. 노심 잔열에 의해 발생하는 노심 열출력은 원자로 운전정지 후 72시간이 경과했을 때의 열출력이며, 이는 정상출력의 0.432%에 해당하는 12.161MWt이다. RCS의 압력 및 온도는 각각 1 기압 (101325 Pa), 50 °C (323.15 K)이며, RCS의 수위는 고온관 혹은 저온관 중간수위로 유지되는 상태로 파악되었다. POS 5의 부분 충수 운전 상태 시 RCS에 개방된 배기관은 3/4″ 가압기 상부 배기관, 3/4″ 원자로용기 상부 배기관, 수위를 측정하기 위해 각 루프의 고온관에 설치하여 가압기 최상부 위치에서 대기로 노출된 1″ tygon tube, 16″ 가압기 manway, 2개의 16″ 증기발생기 입구 측 manway이다. 정지 냉각 계통 (SCS)의 흡입배관 상의 6″ 저온 과압 (LTOP) 방지 밸브와 가압기 안전밸브는 자동 모드에 있다.

2대의 증기발생기는 2차측의 냉각수가 완전 배수되어 이용 불가능하므로, 정지냉각 상실사고 시 노심에서 발생하는 잔열의 대체 열제거 원으로서의 역할이 불가능하다. 증기발생기 2차측의 초기 압력 및 온도는 각각 1차측의 압력 및 온도와 동일하며, 2차측 냉각수는 모두 배수되어 수위는 0 (zero)이며 따라서 증기발생기 2차측은 공기로 충진되어 있는 것으로 모의하였다. 주급수 및 보조급수는 증기발생기 2차측으로 공급되지 않으며, 증기발생기 대기 방출 밸브와 주증기 차단 밸브는 사고 후에도 계속 닫혀 있는 것으로 모의하였다.

중력 급수 해석은 정지냉각 상실사고 발생 후 안전주입 실패 시 운전원이 사고 완화를 위하여 RWT와 RCS 루프 A에 있는 두 개의 저온관을 연결하는 밸브를 사고 후 1800초(30분)에 완전 개방하여 중력에 의해 RWT로부터 RCS로 냉각수 보충이 가능한지를 확인하는 것으로 가정하였다. 중력 급수 초기의 RWT 압력과 온도는 각각 대기압, 50°C이며, 수위는 90.8 %이다.

(3) MARS와 RELAP5 계산 결과 비교

RCS내 원자로 노심 상부에서의 사고 후 시간에 따른 압력변화(그림 3-9)를 비교하여 보면, 세 코드가 비교적 일치하나 RELAP5/MOD3.2의 경우 70000초 근처에서 압력이 빨리 감소하는 것으로 예측한다. 이는 RELAP5/MOD3.2가 중력급

수에 의해 RWT로부터 RCS로 유입되는 냉각수량을 MARS2.1 및 RELAP5/MOD3.3 보다 과대하게 예측하기 때문이다 (그림 3-18 참조). 원자로 노심 최상부 냉각재 온도(그림 3-10), 고온관 및 저온관의 냉각재 온도 (그림 3-11, 3-12)는 세 코드 모두 유사하게 예측한다. 고온관 (그림 3-13) 및 저온관 (그림 3-14)의 기포율, 그리고 노심 상부에서의 기포율(그림 3-15)은 전반적으로 RELAP5/MOD3.2가 MARS2.1와 RELAP5/MOD3.3보다 빨리 상승하는 것으로 예측한다. 이는 앞서 언급한 RWT로부터의 중력급수에 의한 냉각수 유입량의 차이와 개방된 배기구를 통한 냉각재 유출량의 차이에서 오는 것으로 판단된다. 원자로 노심에서의 collapsed 수위 변화 (그림 3-20)도 같은 이유로 RELAP5/MOD3.2가 MARS2.1 및 RELAP5/MOD3.3보다 빨리 하강하는 것으로 예측한다.

이와 같이 POS5에서 중력급수를 이용하는 경우 RELAP5/MOD3.3과 MARS2.1은 비교적 잘 일치하나 RELAP5/MOD3.2는 차이가 많이 나는 이유는 다음의 2가지 이유라고 여겨진다.

○ RELAP5/MOD3.3과 MARS2.1은 Henry-Fauske critical flow model을 사용하고 있으며, 이는 RELAP5/MOD3.2에서 사용하던 mechanistic critical flow model보다 더 잘 맞는 것으로 알려져 있기 때문이다.

○ 중력급수 시 RWT의 수위 조절 문제 때문이다. 기존 PSA 열수력 분석 코드인 RELAP5/MOD3.2에서는 RWT의 입력 옵션으로 thermal stratification, level tracking option을 사용하였는데, 이는 이론적으로는 타당하나 현실적으로는 물리적 타당성을 보장할 수 없는 것으로 알려져 있다.

결론적으로 MARS 코드와 RELAP5 코드의 검증을 위하여 중력급수 시나리오에 대한 비교 분석 결과 중력 급수는 가능한 것으로 판단되었다. 가압기 manway 및 증기발생기 입구 측 manway와 같은 큰 배기구가 개방되어 있는 대기압 상태의 부분충수 운전 중 냉각계통 상실사고 발생시 RWT로부터의 중력급수를 시도하는 경우에 대한 열수력 해석을 수행하는데 있어, MARS2.1 과

RELAP5/MOD3.3 은 타당한 예측을 하고 그 결과도 거의 일치하므로 두 코드 모두 신뢰성 있는 열수력 해석을 수행할 수 있음을 알 수 있다. 반면 RELAP5/MOD3.2는 비현실적인 임계 유량 모델과 RWT의 수위를 조절하는데 사용된 thermal stratification/level tracking 옵션의 잘못된 사용으로 다소 다른 예측 결과를 보였다. 본 분석으로부터 MARS2.1은 최적 열수력 해석 코드로써 분석 능력이 이전의 코드보다 향상된 것으로 판단된다.

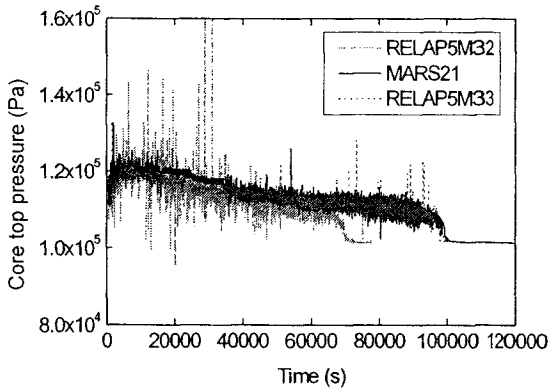


그림 3-9 노심 상부 압력 비교

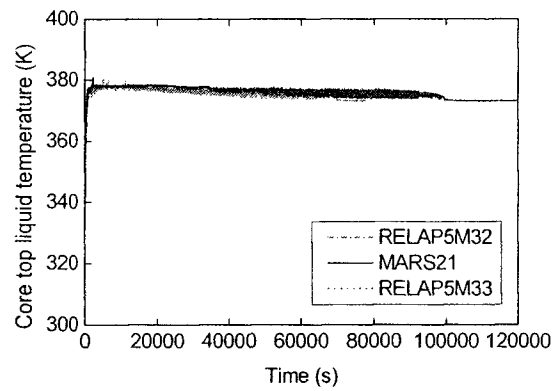


그림 3-10 노심 상부 냉각재 온도 비교

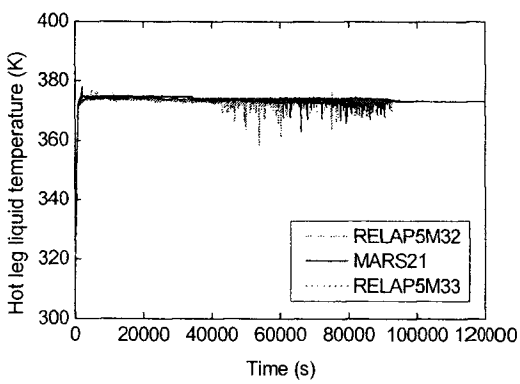


그림 3-11 고온관 냉각재 온도

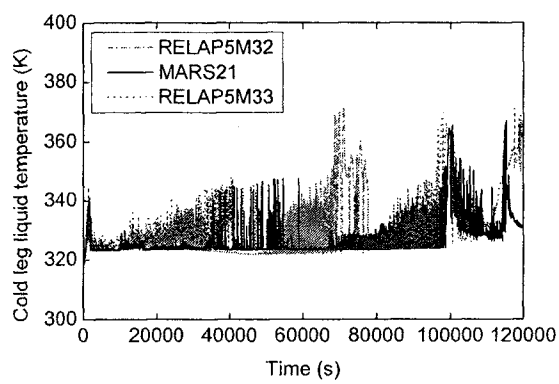


그림 3-12 저온관 냉각재 온도

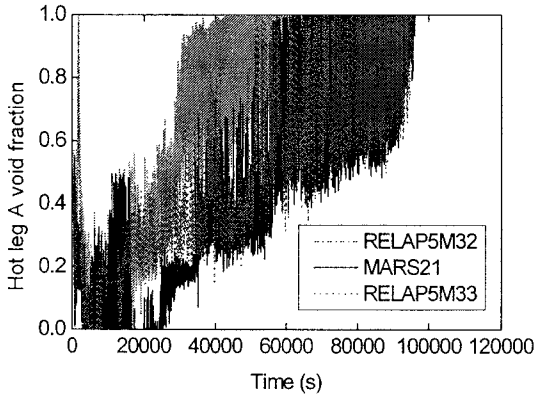


그림 3-13 고온관 기포율

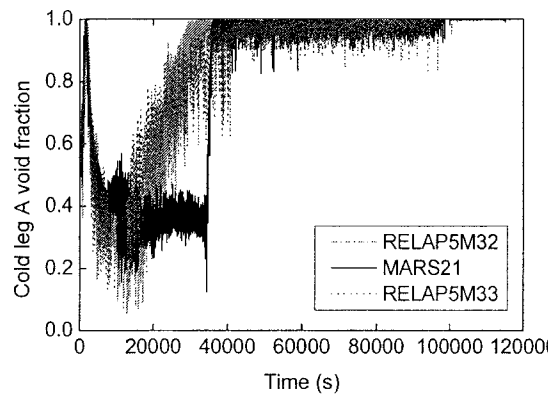


그림 3-14 저온관 기포율

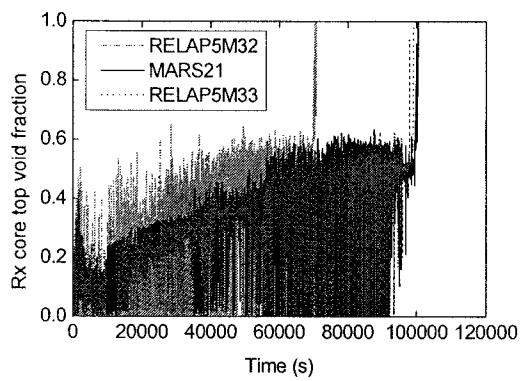


그림 3-15 노심에서의 기포율

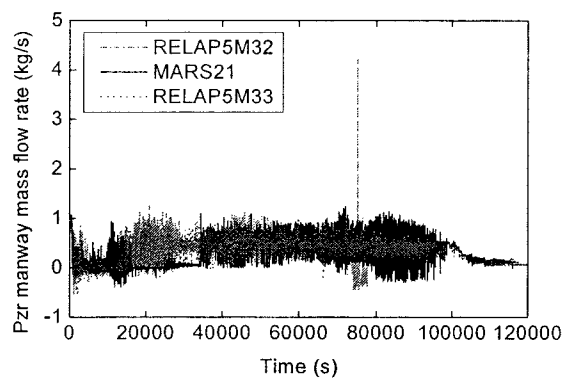


그림 3-16 가압기를 통한 유량

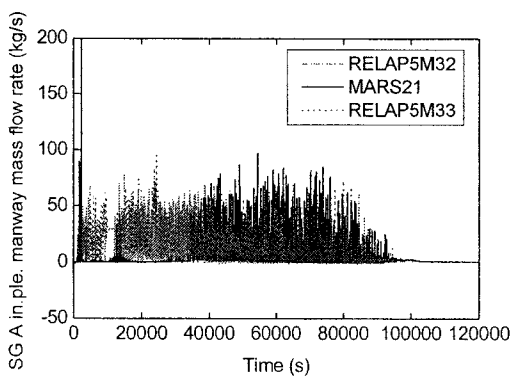


그림 3-17 증기발생기 A를 통한 유량의 변화

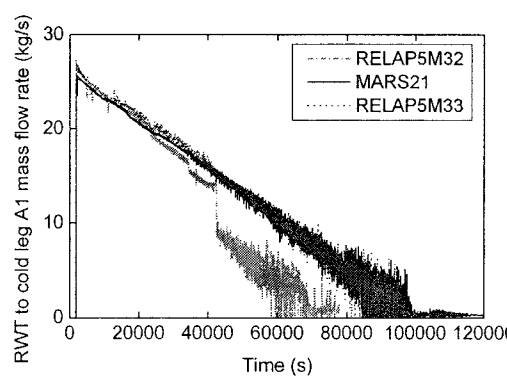


그림 3-18 재장전수 탱크에서 저온관으로의 유량

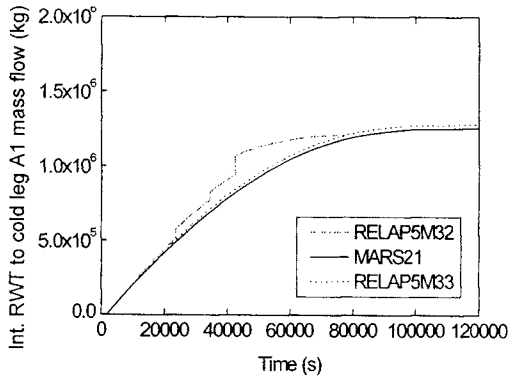


그림 3-19 재장전수 탱크에서 일차계통으로의 누적 유량

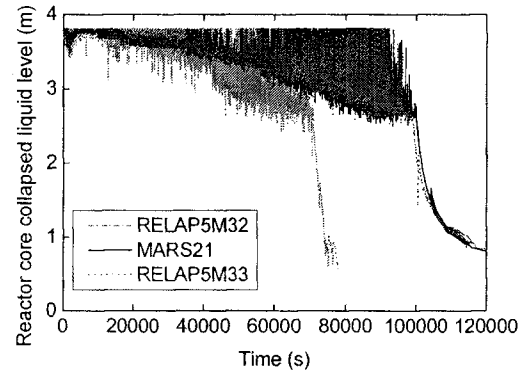


그림 3-20 노심에서의 냉각재 수위 (collapsed level)

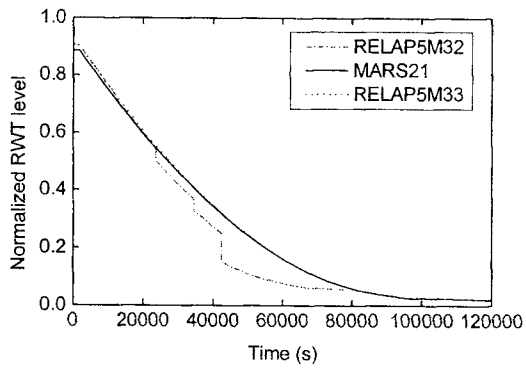


그림 3-21 정규화된 재장전수 탱크의 수위

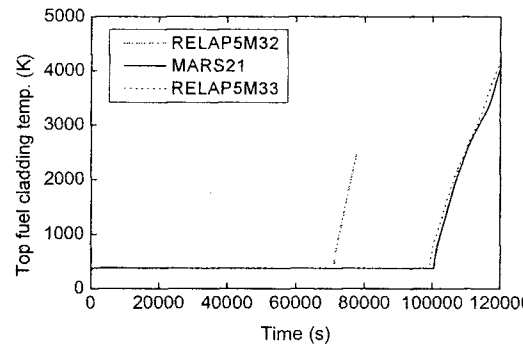


그림 3-22 노심 상부에서의 피복재의 온도변화

나. 정지/저출력 성공기준 결정을 위한 기본사고 분석

정지/저출력 PSA의 품질 개선을 위하여 PSA 모델에서 고려되는 예상 사고에 대한 사고 경위에 대한 보다 현실적인 성공 기준의 결정이 무엇보다도 중요하다. 현실적인 사고 경위 성공 기준의 결정을 위해서는 발전소 거동 분석이 필수적이며, 이를 위해 발전소 고유의 열수력 분석 체계를 이용한 최적 사고 해석 결과에 의존할 수 밖에 없다. 그러나, 정지/저출력 운전 모드에 대해 열수력 분석에 의한 사고 해석 사례들은 전출력 운전에 비해 매우 제한적이고 불충분한 상태에

있다. 또한, 정지/저출력 운전 특성상 다양한 발전소 기기 배열 상태에 따른 열수력 분석이 필요하므로 이는 정지/저출력 PSA용 열수력 분석 자체를 어렵게 만드는 요인이다.

본 연구에서는 한국 표준형 원전 (영광 5, 6호기)을 대상으로 정지/저출력 PSA 모델 개선의 일환으로 현실적인 사고경위 성공기준 결정을 위하여 정지/저출력 PSA의 대표적인 기본사고인 정지냉각 상실사고에 대한 각 발전소 운전 상태(POS)별 발전소 고유의 열수력 분석을 수행하였다. 이를 위해 앞서 언급된 바와 같이 정지/저출력 PSA용 열수력 분석 플랫폼으로 구축된 MARS 2.1 코드 체계를 이용하였다. 이와 관련하여 다음과 같은 연구 내용이 수행되었다.

○ 발전소 운전 상태 파악

○ 열수력 분석을 위한 입력 자료 작성

○ POS별 정지냉각 상실사고에 대한 열수력 거동 분석

○ 결과 해석

이와 관련된 세부적인 연구 내용 및 분석 결과들은 기술보고서 [손영석, 2004]와 논문[손영석, 2005]에 기술되어 있으며, 아래에 이어지는 세션에서 간단히 정리하기로 하겠다.

(1) 발전소 운전상태 분류

정지/저출력 PSA와 관련한 POS 재분석 결과는 본 보고서의 제 3장 1절 세션 2에 기술되어 있다. 따라서, 여기서는 POS별 열수력 분석을 위해 필요한 POS 관련 분류 결과나 가정 사항만을 간단히 기술하면 다음과 같다.

○ 표준원전 정지/저출력 PSA에서는 발전소 운전 상태는 다양한 운전 변수에 따라 그림 3-23과 표 3-18에서 보는 바와 같이 15개로 분류되었다. 특히, POS4와 POS12는 가압기 보수용 출입구의 개방여부에 따라 RCS의 거동이 매우 다를 수 있으므로 각각 2개로 세분되었음에 유의하여야 한다.

○ 각 POS별 지속시간은 해당 POS의 열수력 분석을 위한 노심 붕괴열 설정에 매우 중요하다. 이에 따라, POS 지속시간에 대하여 조사되었고 MARS 2.1 열수력 분석의 입력자료로 사용된 POS별 대표 시간은 표 3-18에 정리된 바와 같다.

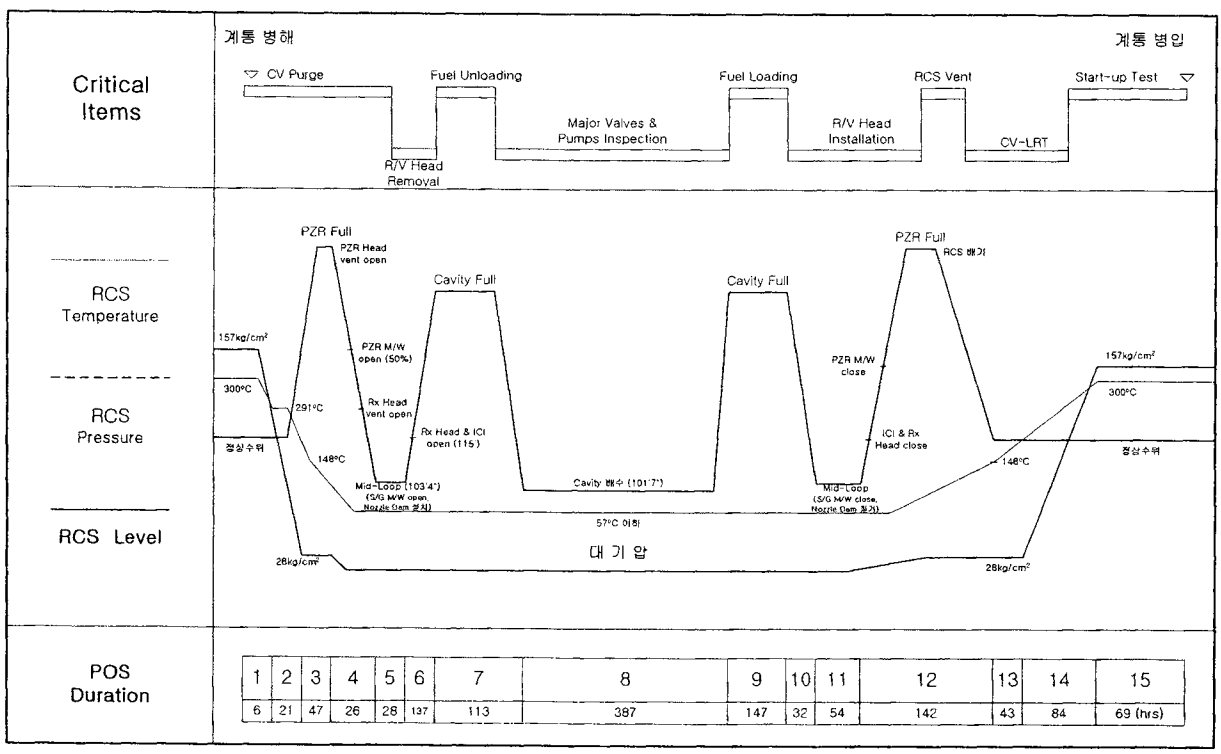


그림 3-23 각 POS 에서의 변수 특성 및 지속 시간

표 3-18 표준원전 정지/저출력 POS 분류 및 특성

POS		POS 특성	지속 시간	누적시간	MARS 적용 시간
POS 1		계통병해에서 발전소 정지	6 hr	0 hr	-
POS 2		증기발생기를 이용한 발전소 냉각운전	21 hr	6 hr	-
POS 3		정지냉각계통을 이용한 발전소 냉각운전	47 hr	27 hr	15 hr
POS 4	A	1차 부분충수 운전을 위한 배수운전 (가압기 manway 개방 전)	26 hr	74 hr	45 hr
	B	1차 부분충수 운전을 위한 배수운전 (가압기 manway 개방 후)			70 hr
POS 5		1차 부분충수 운전	28 hr	100 hr	72 hr
POS 6		핵연료 인출을 위한 충수운전	137 hr	128 hr	96 hr
POS 7		핵연료 인출	113 hr	265 hr (11.0 days)	-
POS 8		정비를 위한 배수 및 충수운전	387 hr	378 hr (15.8 days)	-
POS 9		핵연료 재장전	147 hr	765 hr (31.9 days)	-
POS 10		2차 부분충수 운전을 위한 배수운전	32 hr	912 hr (38.0 days)	25 days
POS 11		2차 부분충수 운전	54 hr	944 hr (39.3 days)	25 days
POS 12	A	발전소 기동을 위한 충수운전 (가압기 manway 폐쇄 전)	142 hr	998 hr (41.6 days)	25 days
	B	발전소 기동을 위한 충수운전 (가압기 manway 폐쇄 후)			25 days
POS 13		1단계 가열운전 (정지냉각계통 연결)	43 hr	1140 hr (47.5 days)	30 days
POS 14		2단계 가열운전 (정지냉각계통 격리)	84 hr	1183 hr (49.3 days)	-
POS 15		발전소 기동에서 계통병입	69 hr	1267 hr (52.8 days)	-

(2) 계산 조건

본 연구에서는 사고 경위에 대한 최적의 해를 찾기 위해 알려진 범위 내에서 최적의 모델을 사용하는 것을 원칙으로 하였으며 기존의 RELAP5/MOD3.2를 이용한 모델과의 분석 차이점은 아래와 같다.

○ 노심 잔열 생성 모델: 기존의 보수적 비상냉각 계통평가 시 사용되었던 ANS73 노심 잔열 생성 모델을 ANS79 노심 잔열 생성 모델로 교체하였다. ANS 79 모델은 ANS73 모델에 비해 보다 최적의 노심 잔열 생성을 모델하며 ANS73 모델과 비교하면 잔열 방생 량이 약간 작은 값을 가진다. 정지 저출력 시의 사고의 특성상 긴 시간의 사고추이를 계산하는 경우는 누적된 노심 잔열 발생량으로 인해 노심 손상시간의 예측시간이 이전의 ANS73모델에 의한 계산보다 길어질 수 있다.

○ 임계유속 모델: RELAP5/MOD3.2에 사용되었던 Trapp-Ransom 임계유속 모델이 MARS2.1 버전 이후부터는 수정된 Henry-Fauske 임계 유속 모델로 변경되었다. 변경된 임계 유속 모델은 이전의 Trapp-Ransom 모델에 비해 임계 유속을 약간 과대 예측하는 경향을 가진다. 정지 저출력 사고 모의 시 임계 열유속 모델이 쓰이는 압력이 높은 상태의 운전모드 사고 모의 시 노심 내의 냉각재 재고량의 빠른 고갈로 인해 원자로 노심의 노출이 빨리 발생할 수 있으며 이로써 보수적으로 계산할 수 있다.

○ 잔열 수준: 기존의 잔열 수준 모델은 여러 발전소의 재장전 일정에 대한 결과를 평균하여 약간 보수적으로 평가한 값으로 노심 잔열 수준을 모델 하였다. 또한 보수성을 위해 일정한 노심 잔열 수준의 값을 상수로 사용하기도 하였다. 그러나 재장전일정이 표준화 되고 있고 좀 더 최적의 계산을 위해서는 사고 발생시점의 잔열 수준을 정확히 모델할 필요가 있다. 본 연구에서는 가급적 실제의 재장전 일정에 맞추어 잔열 수준을 모델하였으며 잔열 발생 값도 잔열 생성모델을 이용하였다.

○ 사고 초기 및 경계 조건: 부분충수 운전의 초기 조건은 일반적으로 사고 전

정상 상태를 맞추기가 상당히 힘들며 변수들이 상당한 진동을 보이는 것이 보통이다. 초기 조건을 가능한 한 일치시키기 위해 정상상태의 계산 시 계산시간을 늘려서 변수들의 변동 폭을 최소화하였다. 또한 일차계통 압력 경계부의 경계조건을 실제와 일치하도록 최적화 하였다. 예를 들면, 저온 과압 사고를 막기 위한 저온 과압 밸브는 약간의 압력차를 두어 순차적으로 열리는데, 사고모의에서도 이를 반영하여 일정한 압력차가 발생하였을 때 순차적으로 열릴 수 있도록 모의하였다. 또한 비 물리적인 압력경계부에서의 질량유입을 막기 위해 압력 경계부의 상태를 입력 자료의 검토 후 수정하였다.

(3) POS별 계산결과

본 연구에서는 정지/저출력 운전 중 대표적인 기본사고로 선정된 정지냉각 상실 사고에 대한 POS별 상세 열수력 거동 분석이 목적이므로, POS 가운데 핵연료가 노심 내에 존재하고, 정지냉각계통 (SCS)이 작동되고 있는 POS만 열수력 분석의 대상이 된다. 즉, 전기 POS (POS3, 4A, 4B, 5 및 6)와 후기 POS (POS10, 11, 12A, 12B 및 13)가 분석 대상 POS에 해당된다. 여기서 각 후기 POS는 전기 POS와 잔열수준과 초기 온도만 다를 뿐 다른 발전소 상태는 거의 동일하다.

열수력 해석 결과는 정지/저출력 PSA 모델의 사고경위 성공기준 결정을 위한 기초 자료로 활용될 뿐만 아니라 정지/저출력 PSA에서 특히 중요한 운전원 오류 확률 계산을 위해 필수적인 운전원 조치 여유 시간에 대한 기초적인 정보도 함께 제공될 수 있다. 본 연구에서 수행된 POS별 정지냉각 상실사고에 대한 주요 열수력 분석 결과들은 다음과 같이 간단히 정리될 수 있겠다.

○ 잔열, RCS 압력 및 온도, 수위, 배기관, 증기발생기 2차 측 상태 등 POS 분류 기준에 따른 정지냉각 상실사고의 주요 열수력 분석 결과들은 표 3-19, 그림 3-24 및 그림 3-25에 정리된 바와 같다. 전기 POS인 POS3, 4A, 4B, 5, 6 및 후기 POS인 POS10, 11, 12A, 12B, 13에 대해 모의계산을 수행하여 RCS 최대 압력 및 온도, 노심비등, 노심노출, 노심손상 시간, 그리고 기타

중요결과들을 구하였다.

○ 전체적인 경향을 보면 사고 발생 후 증기발생기가 노심발생 잔열의 대체 열제거 원으로서 이용 불가능한 경우에는 대체적으로 증기발생기가 이용 가능한 경우보다 노심손상이 빨리 일어남을 알 수 있다(그림 3-24).

- 전기 POS에서 사고 발생 후 증기발생기가 노심발생 잔열의 대체 열제거 원으로서 이용 가능한 경우인 POS3 및 POS4A에서는 노심손상이 각각 21610초 및 49140초에 일어났다.

- 증기발생기가 노심발생 잔열의 대체 열제거 원으로서 이용 불가능한 경우인 POS4B, POS5, POS6에서는 노심손상이 각각 11380초, 9180초, 11220초에 일어났으며, 대체적으로 증기발생기가 이용 가능한 경우인 POS3 및 POS4A보다 노심손상이 빨리 일어남을 알 수 있다.

○ 가압기 및 증기발생기 입구 측 manway, 그리고 ICI tube 등과 같은 큰 면적의 배기관이 열려 있는 경우는, 사고 발생 후 이들 배기관을 통해서 많은 냉각재가 유출되어 노심손상이 빨리 일어났다(그림 3-25).

- POS4B에서는 가압기 manway, POS5에서는 가압기 및 증기발생기 입구 측 manway, 그리고 POS6에서는 가압기 manway 및 ICI tube가 배기관으로 열려 있으므로, 사고 발생 후 이들 배기관을 통해서 많은 냉각재가 유출되어 노심손상이 빨리 일어난다.

- 특히, 부분충수 운전으로 수위가 낮고 가압기 및 증기발생기 입구 측 manway가 모두 열린 경우인 POS5에서 정지냉각계통 상실 사고 시 노심손상 시간이 가장 빨리 일어남을 알 수 있다.

○ 각 후기 POS에서 정지냉각 상실사고에 대한 열수력 해석 결과를 해당 전기 POS 열수력 해석 결과와 비교한 결과, 후기 POS에서는 노심 잔열이 낮아 노심손상 까지의 진행 속도가 상대적으로 매우 느림을 알 수 있었다.

- POS10에 해당하는 전기 POS인 POS6에서는 노심손상이 11220초에 일어나는데 반해, POS10에서는 노심손상이 사고 후 22356초에 발생한다.

- POS11에 해당하는 전기 POS인 POS5의 노심손상 시간이 9180초에 비해, POS11에서는 노심손상까지 이르는 시각을 26620초로 예측되었다.
- POS12A에서는 노심손상이 34160초에 일어나고, 해당하는 전기 POS인 POS4B에서는 노심손상이 11380초에 일어났다.
- POS12B에서는 모의계산 시간인 86400초(24시간)동안 노심손상은 일어나지 않았으나, 해당하는 전기 POS인 POS4A에서는 노심손상이 49410초에 발생하였다.
- POS13에 해당하는 전기 POS인 POS3에서는 노심손상이 21610초에 일어나는데 반해, POS13에서는 86550초에 노심손상이 일어났다.

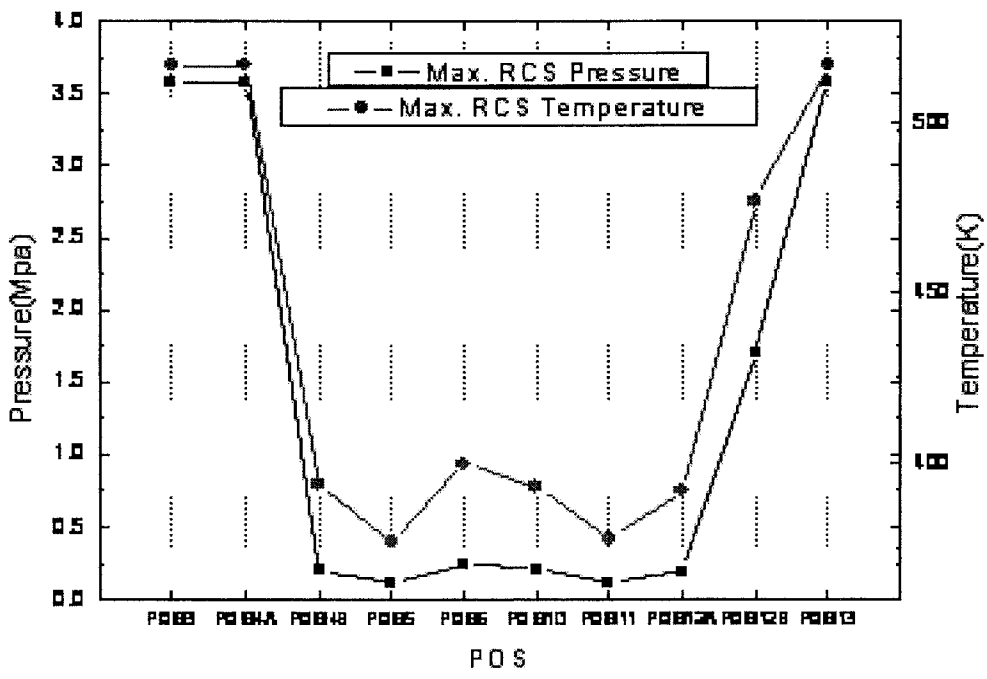


그림 3-24 S/G 이용가능성에 따른 일차계통 압력 및 노심 온도 변화

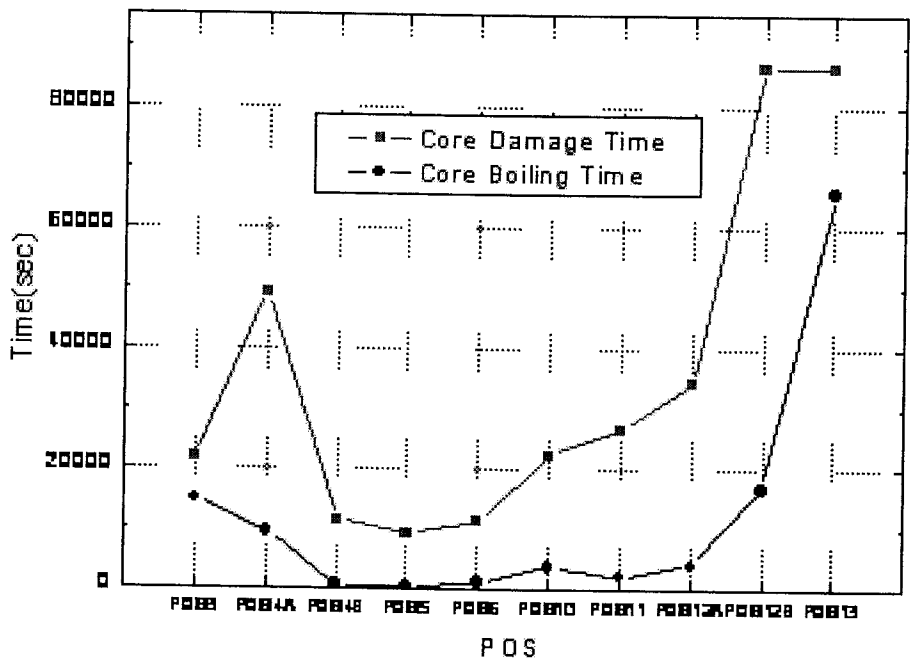


그림 3-25 노심 개구부에 따른 노심 비등 및 손상 시간 변화

표 3-19 표준원전 정지냉각 상실사고에 대한 주요 열수력 분석 결과

POS	Time after Shut-down	RCS Water Level	RCS Pressure and Temp.	RCS and SG Status (LTOP valves and PSV are in automatic mode in all POS's)	Simulation Time	Max. RCS Pressure and Temp.	Time to Core Boiling and Damage
POS3	15 hr	Normal	2.7459 MPa 419.15 K	2 SG's available No vent path	38200 s	3.58 MPa 517 K	14680 s 21610 s
POS4A	45 hr	PZR 50%	0.1013 MPa 323.15 K	2 SG's available PZR head vent open	60000 s	3.58 MPa 517 K	9370 s 49140 s
POS4B	70 hr	Hot leg top	0.1013 MPa 323.15 K	2 SG's unavailable PZR head vent open Rx head vent open Tygon tubes open PZR manway open	17400 s	0.201 MPa 394 K	520 s 11380 s
POS5	72 hr	Midloop	0.1013 MPa 323.15 K	2 SG's unavailable PZR head vent open Rx head vent open Tygon tubes open PZR manway open SG inlet manways open	22000 s	0.122 MPa 377 K	340 s 9180 s
POS6	96 hr	Rx vessel flange	0.1013 MPa 313.15 K	SG nozzle dams installed PZR head vent open Rx head vent open Tygon tubes open PZR manway open ICI tubes Open	17890 s	0.243 MPa 400 K	1000 s 11220 s
POS10 (post POS6)	25 days	Rx vessel flange	0.1013 MPa 303.15 K	SG nozzle dams installed PZR head vent open Rx head vent open Tygon tubes open PZR manway open ICI tubes Open	39377 s	0.214 MPa 393 K	3600 s 22356 s
POS11 (post POS5)	25 days	Midloop	0.1013 MPa 303.15 K	2 SG's unavailable PZR head vent open Rx head vent open Tygon tubes open PZR manway open SG inlet manways open	33200 s	0.12 MPa 378 K	2100 s 26620 s
POS12A (post POS4B)	25 days	Hot leg top	0.1013 MPa 303.15 K	2 SG's unavailable PZR head vent open Rx head vent open Tygon tubes open PZR manway open	41900 s	0.197 MPa 392 K	3960 s 34160 s
POS12B (post POS4A)	25 days	PZR 50%	0.1013 MPa 323.15 K	2 SG's available PZR head vent open	86400 s	1.698 MPa 477 K	16630 s No (possible after 86400s)
POS13 (post POS3)	30 days	Normal	2.7459 MPa 419.15 K	2 SG's available No vent path	100000 s	3.58 MPa 517 K	65700 s 86550 s

5. 사고경위 분석 분야의 등급 개선

국내 표준원전의 정지/저출력 PSA 모델을 대상으로 ANS Standard (Draft)에 따라 모델 등급 평가를 수행하였고, 그 결과 사고경위 분석 분야에서는 총 21개 요건들 중 I 등급 이하가 5개 요건이고, 2등급 이상이 16개 요건인 것으로 판정되었다. 사고경위 분석 분야의 등급 평가 결과로서 파악된 미비점 및 개선 사항들을 정리하면 다음과 같다 (표 3-2 참조).

○ 사고경위별 분석 및 기술보완

○ 사고경위별 현상학적 조건 및 영향 분석 미흡

○ 문서화 보완

본 과제에서는 사고경위 분석 분야에서 도출된 미비점을 개선하기 위하여 RFP에 따라 아래와 같은 개선 업무를 수행하였고, 그 결과 1개의 I 등급 요건이 II 등급으로 개선되었다 (표 3-3 참조).

○ 정지/저출력 고유 특성을 반영한 열수력 상세 거동 분석

- 가압기 안전밸브 개방 고착 사고에 대한 상세 열수력 거동 분석
- 중력급수의 영향분석
- 저온 과압 사고에 대한 상세 열수력 거동 분석
- 관류 냉각 현상의 적용 가능성 상세 분석
- 정지/저출력 열수력 분석 체계에 대한 연구 결과를 문서화

이들의 연구 내용 및 결과들은 이어지는 섹션에서 순차적으로 간략하게 소개하기로 하겠다.

가. PSV 개방 고착 사고에 대한 상세 열수력 거동 분석

(1) 연구개요

한국형 표준원전은 Combustion Engineering (CE)사의 Two-Loop, 1000 Mwe 급의 원전이다 [KHNP, 1996]. 가압기에는 3개의 가압기 안전밸브가 장착되어 있으며 원자로 일차계통의 과압 방지 기능을 수행한다. 이 밸브들은 배압 보상 및 스프링 부하에 의해 닫혀있으며 ASME 코드 기준을 만족 한다 [KHNP, 1996]. 이 밸브들은 핵연료 재장전 기간 중 시험절차에 의해 건전성 시험이 수행된다. 이 시험은 정상운전 상태와 비슷한 조건을 만족할 수 있게 하기 위해 주로 재장전 기간의 초반부에 수행된다. 만약 이러한 시험 중 가압기 안전밸브가 완전히 폐쇄되지 않거나 부분적으로 걸리게 되면 가압기의 증기는 방출라인을 통해 원자로 드레인 탱크에 모이게 된다. 증기의 계속적인 방출로 드레인 탱크가 용량을 초과하면 이 탱크의 물은 파열판을 통하여 격납용기로 방출된다. 이러한 시나리오는 시험에 기인한 냉각재 방출사고로써 정지 저출력 위험도의 가장 큰 기여사고이다 (영광 5,6 정지저출력 안전성평가 [KHNP, 2002]). 이 시나리오에서 노심 손상을 유발할 수 있는 이 사고의 주요한 사고경위로써 고압안전주입계통의 실패 시나리오가 선정된 바 있다. 본 연구의 목적은 이러한 사고 시나리오에 대한 열수력 분석을 수행하여 각 사고 경위의 결과를 예측하고 노심손상 시나리오에 대해 급속 감압 냉각 등의 사고의 완화전략을 찾는데 있다. 급속 감압 냉각은 운전원에 의해 수행되는 일차계통 압력 강하 방법으로 이차측의 증기발생기를 열제거 수단으로 이용한다. 운전원은 보조급수를 증기발생기에 공급하며 대기 방출 밸브를 이용하여 발생한 증기를 제거한다. 원자력발전소에서는 이러한 운전 중 가압 열 충격을 피하기 위해 통상적으로 최대의 냉각률을 제한하고 있다 [NRC, 1987]. CE사의 발전소에서와 동일하게 한국형 표준원전에서도 최대 냉각률로 55°C/hr의 값을 사용하고 있다. 급속 감압냉각의 효과는 세계적으로 실험과 해석적 방법을 통해 널리 연구되어 왔다[Kawanishi et al, 1991; Liu et al; 1998; Liu et al, 2000; Asaka et al, 1998; Han et al, 2003]. 현재 한국 표준형 원전에서는 소형 냉각재 상실사고에

서 급속감압냉각운전을 고압안전주입계통의 실패 시 사용하도록 절차화 되어있다 [KHNP, 1997]. 급속감압 냉각은 일반적으로 일차측의 감압을 급속하게 일어나게 하며 이에 따라 부차적인 안전주입 시점이 앞당겨 진다. 또한 급속감압운전은 파단부위에서의 방출유량을 줄이며 노심에서의 이상 유동에 의한 부풀림(swelling)을 증진시킨다.[Kawanishi, 1991] 본 연구에서는 원자력 연구소에서 개발된 MARS 코드[Jeong, 1999a; Lee, 1998]를 최적 열수력 분석코드로 선정하여 사용하였다. MARS 코드는 RELAP5/MOD3 [ISL, 2003b] 와 COBRA-TF[Thurgood, 1982] 코드를 각각 1차원, 3차원 모듈로 하여 이들 코드의 수치해 구조를 통합하였고, 여러 가지 모델의 및 입출력 구조를 단일화하였다. MARS 코드의 적용성은 RELAP5/MOD3.3의 V&V 결과에 비교에 의해 검증된 바 있다 [Lee, 2003a; Lee, 1998]. 기본계산을 통해 가압기 개방고착 사고는 중형 및 소형 냉각재 상실사고의 특성을 동시에 가짐이 확인되었다. 소형 냉각재 상실사고와 유사하게 일차측의 압력 강하는 느리게 진행되며 파단부위에서의 방출유량을 중형 냉각재 상실사고와 유사하게 빨리 방출됨으로써 사고초기에 노심이 노출되는 경향을 보여주었다. 고압안전주입이 실패하면 일차측의 압력은 서서히 감소하여 축압기나 저압안전 주입이 불가능하게 된다. 이러한 사고 경위에 대해 본 연구에서는 급속 감압운전의 분석을 수행하였다. 또한 몇 가지의 중요한 인자에 대한 민감도 분석을 수행하여 사고 진행에 대한 영향을 분석하였다.

(2). 모의 조건.

일차 냉각재 계통 및 2차측의 초기 및 경계조건은 노심 잔열수준을 제외하고는 정상운전 상태를 가정하였다. 노심 잔열 수준은 원자로 트립 후 1시간을 가정하였다. 표 3-20은 분석에 사용된 중요한 초기 및 경제 조건을 보여준다. 최적해석을 위해 모델 및 가정은 보수성을 줄이는 방향으로 설정되었다.

(가) 사고완화 계통선정

각 사고 경위를 분석하기위해서는 사고 진행시 관련된 사고 완화 계통이 선

정되어야 한다. 다음의 완화 계통 및 기능이 사고완화 계통으로 선정되었다

-고압안전 주입 (HPSI)

- 증기 발생기를 이용한 급속 감압운전

- 안전 주입 탱크 (SIT)

- 저압 안전 주입 (LPSI)

분석에서는 재순환에 의한 노심 잔열 계통은 운전 시작 시점에서 일차측의 냉각재 재고량이 충분하면 항상 성공하는 것으로 가정하였다. 고압안전 주입 및 저압안전주입은 작동압력에 도달하면 자동으로 작동하는 것으로 모델링 하였다. 특히 고압안전 주입계통은 작동압력 도달 시 21.34초의 신호 지연시간을 갖도록 하였다. 또한 안전 주입 탱크는 작동압력에서 자동으로 작동하는 것으로 모델링 하였다. 증기 발생기를 통한 급속감압운전은 자동으로 작동되지 않기 때문에 사고 발생 후 일정 시간이 지난 후 운전원에 의해 작동되는 것으로 모델링 하였다. 급속 감압운전의 세부적인 제어 방식과 모델은 다음 장에서 기술된다.

(나) 노심 잔열 모델

입력 분율로 1.0을 갖는 ANS79 모델이 최적계산을 위해 사용되었다. 통상적인 최적계산에서는 이 모델이 주로 사용되고 있다 [ISL, 2003a]

(다) 임계 유속 모델

수정된 Henry-Fauske 모델이 가압기 안전밸브에서의 방출 유량 계산을 위해 사용되었다. 이 모델은 RELAP5/MOD3.3 및 MARS2.1에서 기본 모델로 사용되고 있다. 이 모델은 Edward 파이프 및 Marveken 실험에서 방출률을 과대 예측하는 경향을 보였다. 한편, RELAP5/MOD3.2의 임계유속모델은 위의 동일한 실험에 대해 과소 예측하는 경향을 보여주었다 [ISL, 2003b]. 또한 위 사고의 예비계산을 통해 이 모델은 RELAP5/MOD3.2의 모델에 비해 가압기 안전밸브에서의 유량을 비교적 과대 예측함을 확인하였다 [ISL, 2003b]. 노심 노출 시점은 방출유량과 밀

접한 상관관계를 갖기 때문에 이 모델은 RELAP5/MOD3.2에 비해 빠른 노심 노출 시간을 예측할 것으로 예상된다.

(라) 방출 유로 면적 결정

방출 유로 면적은 노심노출 시간의 예측에 있어 중요한 인자이다. 한국형 표준원전의 가압기 방출밸브는 일차측 압력이 175.133 Mpa일 때 208,651 kg/hr 에서 285,762 kg/hr 의 방출 유량을 갖도록 설계되었다 [Lee, 2003b]. 평가의 불확실성을 고려하기위해 최대의 방출유량인 285,762 kg/hr이 방출 유로 결정을 위한 값으로 사용되었다. 유로면적 결정을 위해 단상 증기에 대한 Henry-Fauske 임계유속 [ISL, 2003a] 식이 사용된다.

$$G_c^2 = \left[\frac{\gamma P_0}{v_o}\right]\left(\frac{2}{\gamma+1}\right)^{\frac{\gamma+1}{\gamma-1}} \qquad (1)$$

여기서 P_0, v_o, and γ 는 각각 정체 압력, 정체 증기 비체적 및 polytropic 계수를 나타낸다. 주어진 유량에 대해 방출 면적은 다음과 같이 구할 수 있다.

$$A = W/(C_D * G_c) \qquad (2)$$

위의 식에서 방출계수 C_D는 1로 가정하였다. 식(2)로부터 대략 2.26 인치 직경을 갖는 방출유로를 얻었다. 이 값은 가압기의 설계 자료와 잘 일치됨을 확인하였다[KHNP, 2002; Crosby, 1989].

(마) 잔열 모델

다양한 발전소의 정지/저출력 운전기록으로부터 대표적인 잔열 수준은 노심 트립 후 1시간 후로 결정되었다. 잔열 수준은 원자로 정지 후 급격히 감소하는 경향을 가지기 때문에 높은 잔열 수준은 노심 손상시간을 앞당기고 운전원의 여유시간을 줄이는 경향을 갖는다. 이러한 영향을 평가하기위해 민감도 분석에서는 이러한 잔열수준에 대한 분석이 수행되었다.

(바) 기타의 가정 사항

노심 손상의 지표로서 최대 고온 채널의 온도가 2200 °F를 넘는 경우를 사용하였다. 이러한 지표는 확률론적 안전평가 및 기타의 안전해석에서 널리 사용되고 있다. 노심을 나타내는 열 구조에 대해 상향 편중의 Cosine 형태의 선형 열출력 분포를 가정하였다. 이러한 열출력 분포는 노심이 위쪽부터 노출되므로 노심노출 시간을 줄이는 경향을 가지게 된다.

표 3-20 가압기 개방 고착 사고분석을 위한 초기 및 경계조건

변수	값	비고
노심 출력 (MWth)	39.326/2815(1.397%)	
일차측 압력 (MPa)	15.5	
고온관 온도(K)	599.6	
저온관 온도(K)	568.6	
증기 발생기 압력 (MPa)	7.27	
증기 발생기 수위 (m)	11.87	
고압안전주입 시작 압력 (MPa)	12.15 (1762psia)	신호 지연
안전주입탱크 주입 압력 (MPa)	4.11	
저압안전주입 압력 (MPa)	1.58	신호 지연
주증기관 안전밸브 작동압력 (MPa)	9.045	

(바) 계산 체적

그림 3-26에서 보는 바와 같이, 일차측 및 이차측은 221개의 열수력 체적, 222개의 Junction 및 연료 다발, 열교환기를 포함한 열구조물로 나타내어진다. 열수력 체적은 압력용기, 고온관, 저온관, 2개의 증기발생기, 가압기, 및 비상 냉각계통을 포함한다. 기압기는 5개의 열수력 체적으로 나타내어지며 상부에 가압기 안전밸브가 격납용기로 연결되어 진다. 노심은 12개의 열수력 체적으로 구성되며 여기에는 평균연료 집합체 및 고온 연료집합체의 두 가지로 대별된 열구조가 연결된다. 고압안전주입, 저압안전주입, 및 보조급수는 time dependent volumes" 및

"time dependent junctions"으로 모델된다. 안전주입 탱크는 축압기 컴포넌트로 모델된다. 가압기 안전밸브는 트립 밸브로 모델링된다. 증기발생기는 U-튜브 및 일차측의 입, 출구 노즐 등의 일차측과 강수완, 증발기 등의 2차측으로 구성된다. 노심에서 발생한 열은 증기발생기의 U-튜브와 증발기를 연결하는 열구조에서 열교환이 일어난다. 주증기 안전밸브와 대기방출밸브는 증기발생기와 터빈사이의 증기관과 연결된다. 이들 밸브는 서보 밸브로 모델되며 방출 면적은 제어변수에 의해 조절된다. 주증기 안전밸브는 2차측의 압력에 의해 개폐가 조절되며 대기발출밸브는 급속감압 모델에 의해 조절된다.

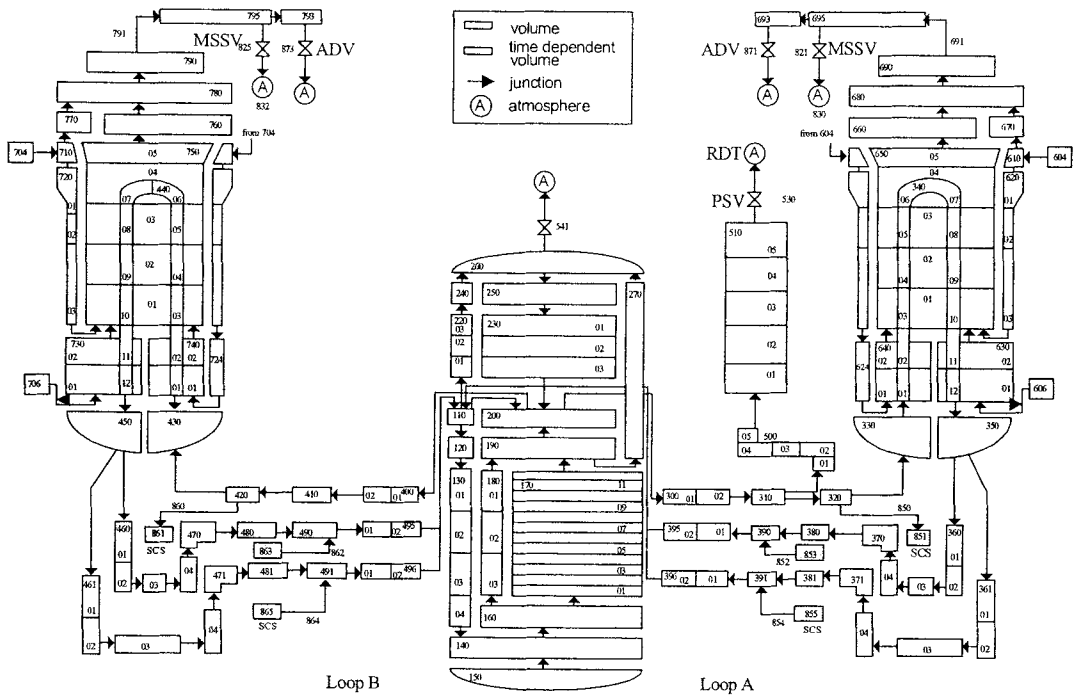


그림 3-26 일차계통 계산 체적

(3) 급속 감압 모델

소형 냉각재 상실 사고 발생 시, 고압안전주입이 실패하면 일차계통은 부가적인 안전주입을 위해 감압이 요구되어 진다 [KHNP, 1997]. 일차측의 감압은 안

전감압계통(SDS) 또는 증기발생기를 이용하여 이루어 질 수 있다. 증기발생기에 의한 감압절차는 일차측의 열을 2차측으로 전달함으로써 이루어진다. 본 분석에서는 안전감압계통은 냉각재 상실사고 시 사용되지 않으므로 증기 발생기를 이용한 급속감압 운전을 모델하였다. 증기발생기를 이용한 일차측 열제거는 증기발생기의 터빈우회밸브나 대기방출밸브를 개방함으로써 이루어진다. 이들 두 밸브는 정해진 냉각률을 충분히 맞출 수 있는 용량을 가지고 있다 [KHNP, 1996]. 발전소의 냉각운전 시 대기방출밸브가 사용되므로 본 분석에서는 대기방출밸브를 이용하였다. 발전소 운전 지침[KHNP, 1995]에 따라, 운전원은 다음의 표준 온도와 일차측의 평균온도차로 밸브를 조작한다.

$$\Delta T = T_{RCS,avg} - T_{ref} \tag{3}$$

일차측의 평균온도란 다음의 저온관과 고온관의 평균온도를 의미한다.

$$T_{RCS,avg} = \frac{1}{2}\left(\frac{1}{2}\left(T_{h1} + T_{c1}\right) + \frac{1}{2}\left(T_{h2} + T_{c2}\right)\right) \tag{4}$$

일차측의 온도와 목표온도가 4°C 이상 차이가 나는 경우는 밸브는 완전 개방되도록 설계되어 있다 [KHNP, 1995]. 우리는 이 자료를 이용하여 밸브의 온도에 대한 변화율을 다음의 식으로 가정하였다.

$$\frac{dA}{dT} = \frac{1}{4}\, normalized \quad area/^{\circ}C \tag{5}$$

코드에서 밸브의 면적변화는 다음의 관계를 이용하여 구할 수 있다

$$\Delta A = \frac{dA}{dT}\Delta T = \frac{1}{4}\Delta T \tag{6}$$

식 (6)으로부터 코드에서의 새로운 면적변화는 다음의 식으로 나타내어진다.

$$A^{n+1} = A^{n} + \frac{dA}{dT}\Delta T^{n} = A^{n} + \frac{1}{4}\Delta T^{n} \tag{7}$$

표준형 발전소 계통 설비 메뉴얼[KHNP,1996]에 의하면 대기 방출 밸브의 개

폐 속도는 초당 0.05 normalized area를 넘지 못한다. 이러한 이유로 밸브의 개폐 속도는 식 (8)에서와 같이 코드의 계산에서 0.05 NA/sec를 넘지 못하도록 제한하였다

$$-0.05 \le \frac{\Delta A}{\Delta t} \le 0.05 \qquad (8)$$

일차계통의 최대 냉각률은 일반적으로 일차측 배관과 압력용기에 대한 가압열 충격[NRC, 1987; Stahlkopf, 1984]에 의해 제한된다. 한국형 표준원전에서는 최대 냉각률이 55 °C/hr (100 °F/hr)로 제한되도록 명시되었다 [KHNP, 1997]. 운전원이 대기방출밸브를 조작할 때 일차측의 온도변화는 즉시 일어나지 않으며 밸브의 조작에 따른 일차측의 온도변화를 운전원이 알기는 매우 어렵다. 발전소에서 운전원은 밸브를 조작한 후에 일차측의 온도변화가 일어날 때까지 밸브의 조작을 하지 않는다. 이러한 형태의 밸브조작은 일차측의 온도변화가 계단식으로 일어남을 의미한다 [Choi, 1998]. 이러한 운전원 조치의 불확실성을 감안하기위해 본 연구에서는 운전원은 2분에 1번꼴로 밸브를 조작하는 것으로 가정하였다. 주어진 최대 냉각률에 대해 운전원이 매 2분마다 밸브를 조작하면 일차계통의 온도는 그림 3-27과 같은 계단식 변화를 따를 것으로 추정된다.

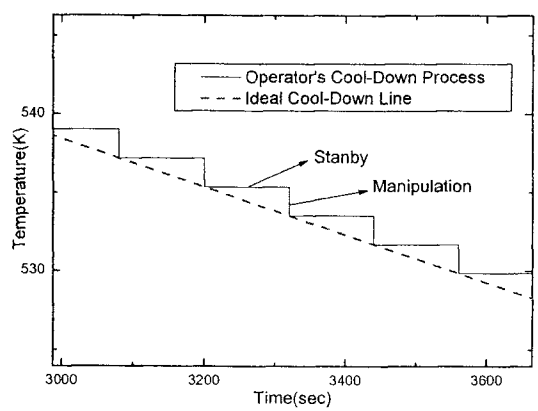


그림 3-27 운전원 밸브 제어 간격에 따른
예상 일차측 온도 변화

(4) 결과 및 고찰

(가) 고압안전 주입 성공 시나리오

고압 안전주입 시나리오가 먼저 모의되었다. 요구되는 사고 완화계통에 대한 최소한의 성공기준을 조사하기 위하여 고압안전주입계통은 1계열만 이용가능하다고 가정하였다. 그림 3-28에서 보는 바와 같이 가압기 안전밸브 개방고착 사고발생 후 일차측의 압력은 급격하게 감소하여 포화압력에 도달한다. 고압안전주입 신호는 가압기 압력, 12.75 Mpa에서 발생하므로 고압안전주입 신호는 1분 이내에 발생한다. 사고의 초기에 가압기 안전밸브로의 유량은 그림 3-31에서 보는바와 같이 고압안전주입 유량을 초과한다. 이러한 초과량은 그림 3-30에서 보는 바와 같이 일차측 냉각재 재고량을 감소시킨다. 약 2000초 후에는 고압안전주입유량은 파단유량과 균형을 이루며 이후 노심 수위는 정상수위를 유지하게 된다. 이러한 결과로부터 본 분석에서는 1계열의 고압안전주입이 성공하면 노심손상을 방지할 수 있는 것으로 확인되었다.

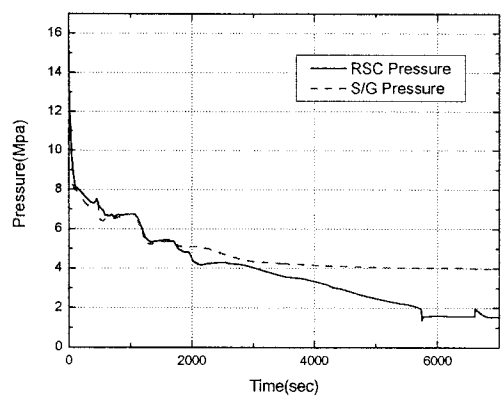


그림 3-28 HPSI 성공 경위(일차측 압력)

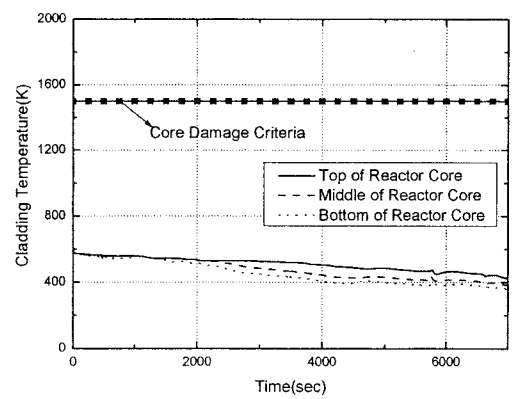


그림 3-29 HPSI 성공 경위(노심 온도)

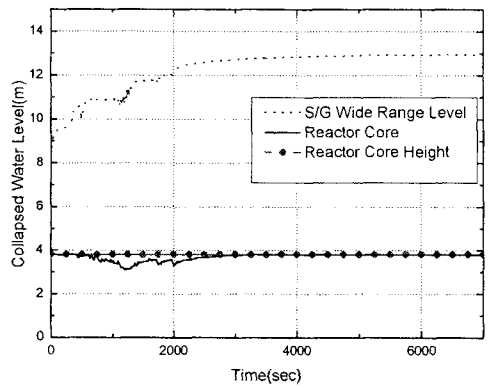


그림 3-30 HPSI 성공 경위(냉각재 수위)

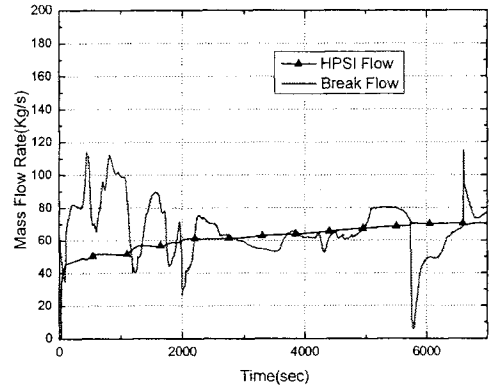


그림 3-31 HPSI 성공 경위(파단 방출유량)

(나) 부가적 완화 전략을 갖지 않는 고압안전주입 실패 시나리오

이 시나리오는 고압안전주입이 실패하고 기타의 완화 조치를 갖는 않는 시나리오이다. 이전의 모의에서와 같이 사고 후 일차측 압력은 급격히 떨어져 포화압력에 도달한다. 고압 안전 주입 후 완화 조치가 없으므로 일차측 압력은 플래싱현상으로 상당한 시간동안 일정한 압력을 유지한다. 이러한 현상은 결국 안전주입 탱크나 저압안전주입과 같은 부차적인 안전주입의 시점을 늦추게 된다. 이후 일차측의 냉각재 재고량이 줄어들게 되며 노심의 온도는 그림 3-33에서와 같이 상승하기 시작한다.

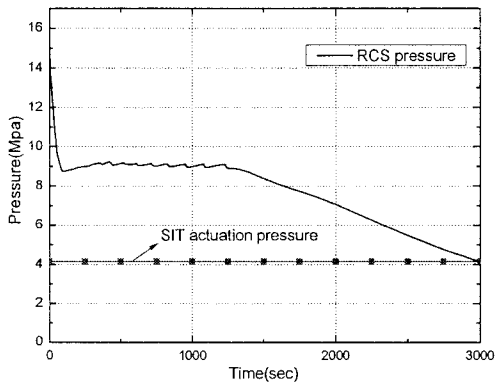


그림 3-32 HPSI 실패 사고 경위 (압력)

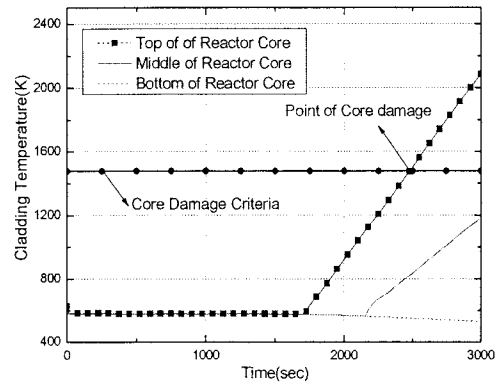


그림 3-33 HPSI 실패 사고 경위 (노심 온도)

(다) 증기발생기 증기 덤프

이전 계산에서 본 바와 같이 고압 안전주입 실패 후 완화 조치가 취해지지 않으면 이는 노심 손상으로 직결된다. 고압 안전주입이 실패하였을 경우 안전주입 탱크나 저압 안전주입을 이용하기 위해서는 적절한 일차계통 감압수단을 필요로 한다. 정상운전 상태에서 증기발생기는 일차측에서 발생한 열을 제거하는 기능을 갖는다. 이차계통이 이러한 사고 상황에서 이용가능하다면 이러한 계통을 이용한 일차계통의 열제거를 통한 감압이 가능할 것이다. 증기발생기의 열제거 능력을 검증하기 위해서 본 절에서는 이차측 밸브를 통한 증기 덤프에 대한 모사가 수행되었다. 본 계산에서는 증기발생기 한대에 대해 한 개의 주 증기관 안전밸브가 개방되고 보조급수가 연속적으로 공급되는 상황을 가정하였다. 그림 3-34부터 그림 3-37은 이 모의 계산의 결과를 보여주고 있다. 주증기관 안전밸브를 개방하면 이차측의 압력은 급속하게 떨어지며 일차측의 압력도 급격하게 감소한다. 그림 3-34에서 보는 바와 같이 안전주입탱크의 주입시점은 사고 후 약 3분에 도달하며 이후 저압안전주입의 시점도 1분 안에 도래한다. 이러한 결과로부터 증기발생기를 이용한 일차측 냉각방법은 안전주입계통의 조기 동장을 위한 좋은 방법이 될 수 있다.

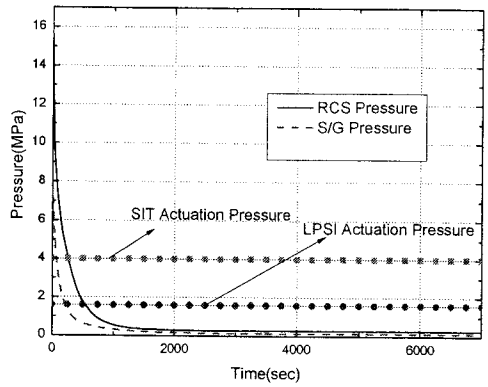


그림 3-34 증기 덤프(압력)

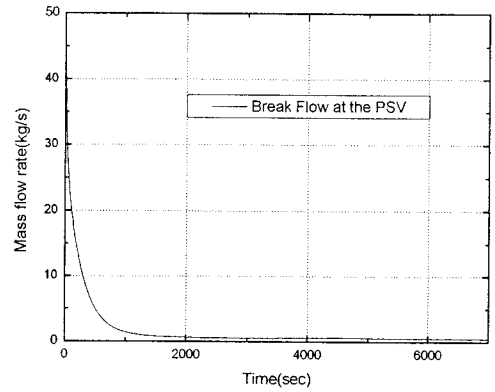


그림 3-35 증기 덤프(유량)

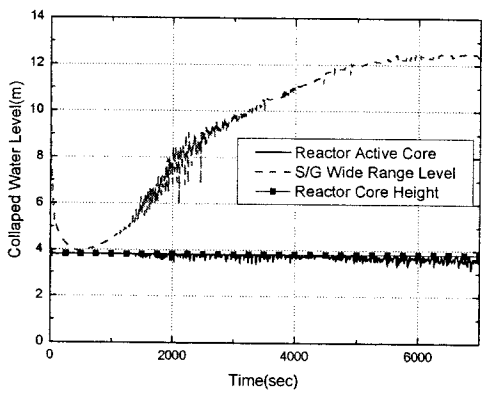


그림 3-36 증기 덤프(수위)

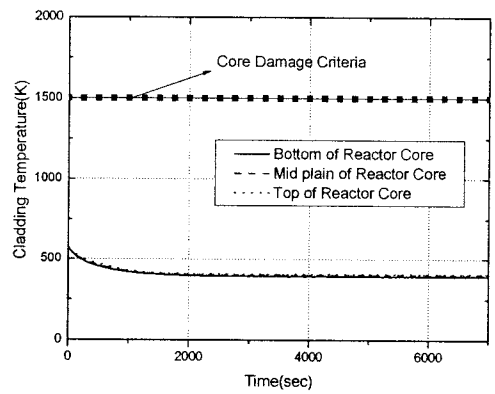


그림 3-37 증기 덤프(온도)

(라) 55°C/hr 냉각률에 의한 일차측 냉각운전

증기 덤프 조치는 일차측 감압의 가장 효과적인 수단임을 알 수 있었다. 이에 따라 저압의 안전 주입계통을 빠르게 동작할 수 있게 할 수 있다. 그러나 이러한 급격한 온도변화는 일차측 배관 및 압력용기에 가압 열충격 문제를 야기할 수 있다 [Stahlkopf, 1984]. 본 절에서는 제한된 냉각률 하에서의 사고 완화 가능성을 분석한다.

① 안전주입 탱크와 저압안전주입이 동반된 일차측 냉각

이 절에서는 안전주입 탱크 및 저압안전주입계통이 작동 가능한 경우의 일차측 냉각운전에 대해서 분석한다. 가압기 안전밸브 고착사고와 같은 경우는 운전원이 빠른 시간 안에 사고를 인지할 수 있는 사고이다. 본 분석에서는 운전원의 급속감압운전 개시 시간은 사고 후 15분으로 가정하였다. 이러한 시간은 전출력 운전에서의 소형냉각재 상실사고 시 가정되었던 시간이다 [KHNP, 1997]. 그림 3-38에서 보이는 바와 같이 대기방출밸브의 제어가 시작된 이후 일차측의 압력은 급속히 떨어진다. 노심은 약 1800초 후에 온도가 상승하기 시작한다(그림 3-40). 그러나 이 시점에서도 안전 주입 탱크의 설정압력까지는 도달하지 못한다. 약 2500초 후에 일차측의 압력은 안전주입탱크의 주입압력인 4.1 Mpa에 도달한다. 안전주입탱크가 주입되면서 피복재온도의 상승은 현격히 떨어진다. 안전주입탱크의 주입량은 고갈된 냉각재 재고량을 충족시키기에는 충분하지 못하므로 안전주입탱크의 주입유량이 줄어드는 4000-5000초에서 다시 피복재의 온도는 재 상승한다. 연속적인 일차측의 냉각운전에 의해 일차측의 압력은 더욱 더 떨어지며 약 5000초에서 저압안전주입 설정압력에 도달한다. 저압안전주입이 개시되면 일차측의 온도는 급격히 감소한다. 그림 3-41는 일차측의 평균온도와 제한 냉각률, 55°C/hr의 비교를 보여준다. 이 그림으로부터 본 분석에서의 계산은 정해진 냉각률에 따라 잘 해석되었음을 알 수 있다. 그림 3-42는 또한 가압기 안전밸브의 파단유량, 안전 주입 유량 및 저압안전주입 유량을 보여주고 있다. 이러한 결과로부터 고압안전주입 실패 시 적절한 급속감압운전이 개시되고 이에 따른 안전 주입 탱크 및 저압안전주입이 성공하면 노심 손상을 막을 수 있을 것으로 예상된다.

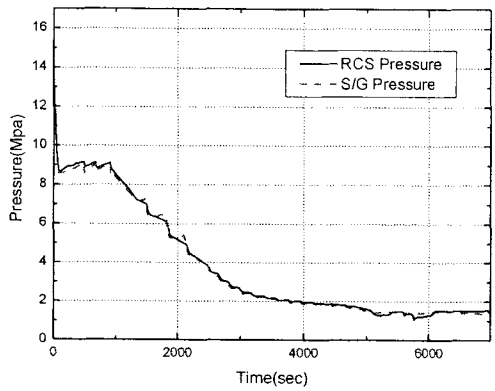


그림 3-38 급속감압운전 시 SIT와 LPSI 성공 경위 (압력)

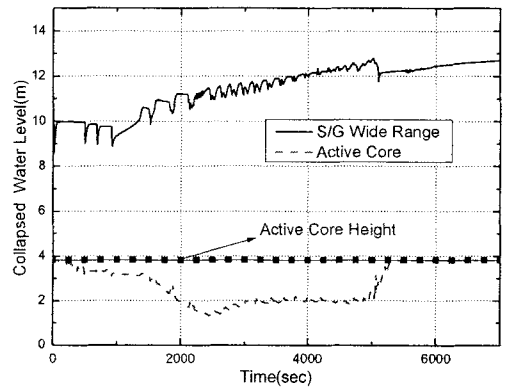


그림 3-39 급속감압운전 시 SIT와 LPSI 성공 경위 (수위)

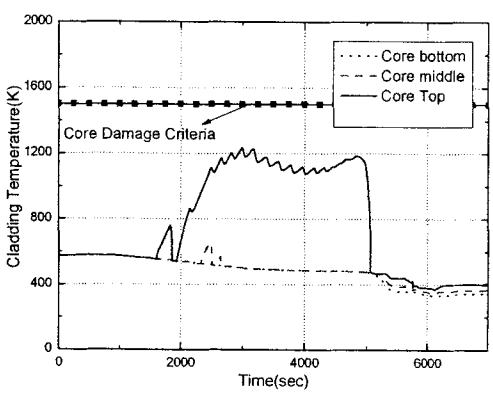


그림 3-40 급속감압운전 시 SIT와 LPSI 성공 경위 (피복재 온도)

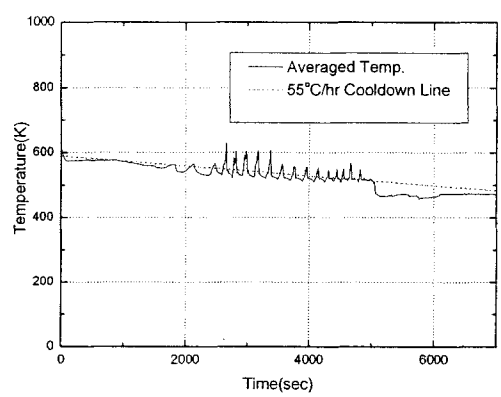


그림 3-41 급속감압운전 시 SIT와 LPSI 성공 경위 (일차측 평균온도)

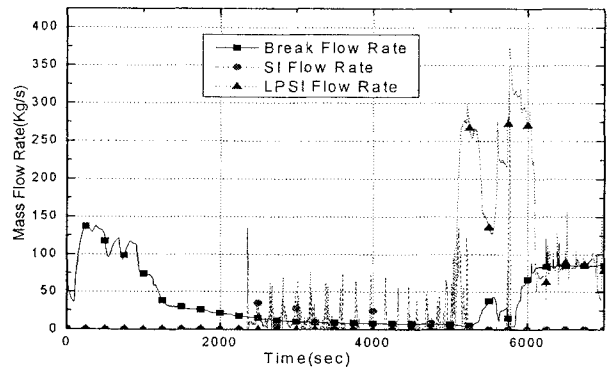


그림 3-42 급속감압운전 시 SIT와 LPSI 성공 경위 (방출유량)

② 안전 주입 탱크 실패시의 시나리오

본 절에서는 급속 감압 운전 시 필요한 최소한의 완화 계통 산정을 위해 안전주입탱크가 실패했을 경우의 사고시나리오에 대해 분석한다. 대기방출밸브에 대한 제어방법은 이전의 경우와 동일하다. 이전의 경우에서와 같이 안전주입탱크의 실패 시는 저압안전주입 시점이전인 약 3000초에서 노심손상이 발생한다. 그림 3-43 및 3-44은 일차측의 압력과 노심은 온도 거동을 보여준다.

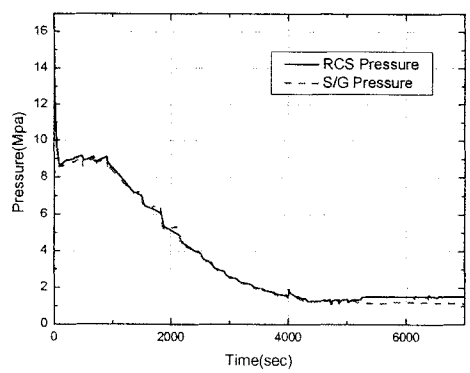


그림 3-43 급속감압운전의 SIT 실패 사고 경위(압력)

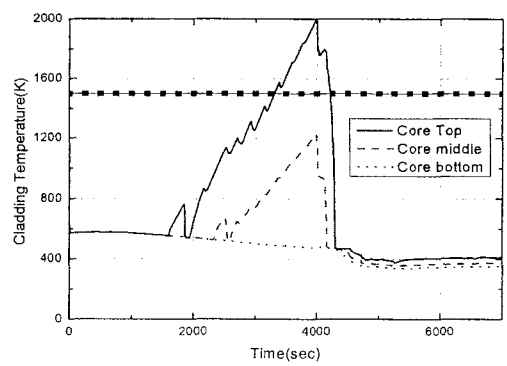


그림 3-44 급속감압운전의 SIT 실패 사고 경위(온도)

(마)민감도 분석

① 노심 잔열 수준의 영향

노심의 잔열 생성량은 시간에 따라 급격하게 감소하기 때문에 가압기 안전밸브의 건전성 테스트는 원자로 정지 후 많은 시간이 흐른 후에 수행하는 것이 안전성에 좋을 것이다. 본 분석에서 사용된 노심 잔열 수준은 원자로 정지 후 1시간의 값을 사용하였다. 또한 현재의 표준형 발전소에서는 이 테스트의 시점을 원자로 정지 후 9시간에 수행할 것을 검토하고 있다. 이러한 노심 잔열 수준의 변화에 따른 영향을 평가하기 위해 (나)절의 시나리오에 대해 9시간의 노심잔열 수준을 사용하여 분석을 수행하였다. 특히 본 분석에서는 급속감압운전 없이 안전 주입탱크에 작동가능성에 초점을 맞추었다. 그림 3-45에 보이는 바와 같이 9시간의 노심 잔열 수준에서의 일차측의 압력은 1시간의 노심잔열 수준보다 빨리 떨어진다. 또한 9시간의 노심잔열수준의 경우에는 피복재의 온도 증가율도 급격히 떨어진다 (그림 3-46). 그러나 일차측의 압력은 (라)절의 급속감압운전의 경우와 비교해보면 높은 편이다. 결과적으로 9시간 노심잔열 수준의 경우에도 이후의 안전주입계통이 보다 빨리 이용가능하기위해서는 급속감압운전이 필요할 것으로 분석되었다.

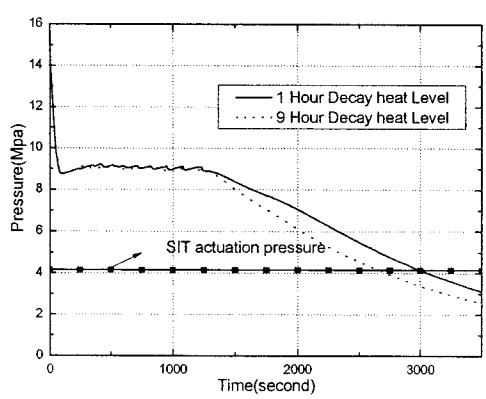


그림 3-45 노심 잔열수준에 따른 압력변화

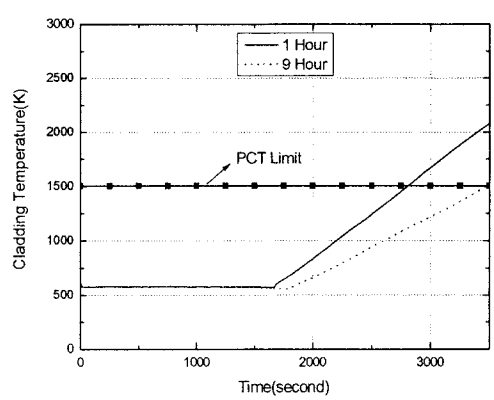


그림 3-46 노심 잔열수준에 따른 온도변화

② 급속감압운전 개시시점에 대한 효과

가압기 안전밸브 개방고착사고는 테스트 도중 발생하는 사고로서, 운전원은 사고를 즉시 인지할 수 있으며 사고 완화를 위한 조치를 빠른 시간 안에 수행할 수 있다. (라)절의 분석을 수행하면서 운전원 조치시간으로서 사고 후 15분을 사용하였다. 본 절의 민감도 분석에서는 운전원은 5분 안에 급속 감압 운전을 수행할 수 있다고 가정하였다. 그림 3-47에서 보는 바와 같이 일차측의 열수력적 거동은 (라)절의 경우와 유사하였다. 그러나 운전원 조치시간이 5분이었을 경우의 일차측 압력이 15분의 경우보다도 높은 결과를 보였다. 이러한 감압의 지연은 5분의 경우가 가압기 안전밸브에서 단상의 증기 임계유량에 늦게 도달하게 되어 발생되는 문제로 밝혀졌다[NRC, 1988; Burchill, 1982]]. 15분 조치시간에서의 파단유량은 5분 조치시간의 경우보다 사고초기에 크게 된다.(그림 3-50) 일차측의 냉각재 재고량이 감소하면서 가압기 안전밸브에서는 증기만 남게 되므로 단상 증기의 임계유속이 발생하게 된다. 단상의 증기에서는 체적 방출율이 2상의 체적 방출율에 비해 현저히 크기 때문에 결과적으로 일차측의 압력은 후반부에서 더욱더 급격히 감소하게 된다. 비록 안전주입탱크의 주입 개시시간은 약간 지연되나 5분의 조치시간을 사용하였을 경우는 피복재의 온도는 15분의 조치시간을 사용하였을 경우보다 낮았다. 이것은 5분의 조치시간을 사용하면 파단부위에서의 파단 유량이 적어지므로 일차측의 냉각재 재고량이 15분의 조치시간보다 많으므로 이러한 냉각재 재고향이 노심온도 상승을 지연시킨 것으로 볼 수 있다. 이러한 분석으로부터 보다 빠른 운전원 조치시간은 피복재의 온도상승을 좀 더 지연시킬 수 있는 것으로 볼 수 있다.

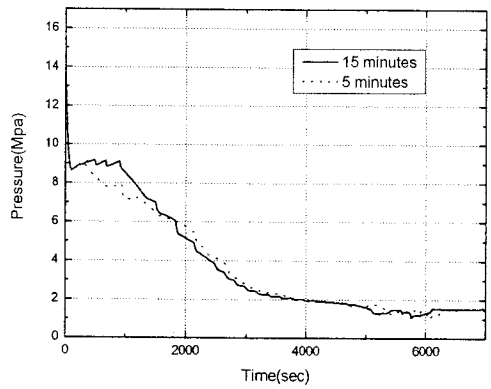


그림 3-47 급속감압운전 개시 시간에 대한 영향(압력)

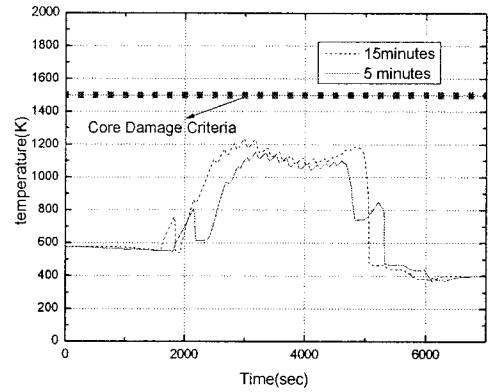


그림 3-48 급속감압운전 개시 시간에 대한 영향(온도)

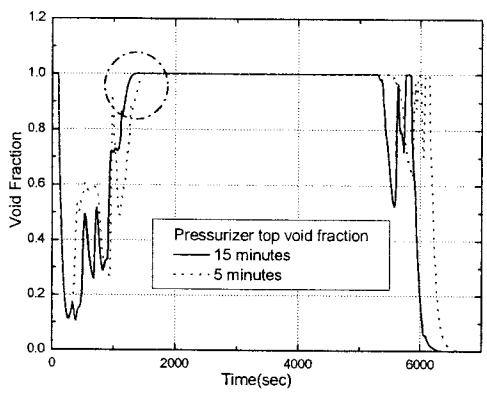


그림 3-49 급속감압운전 개시 시간에 대한 영향(기포계수)

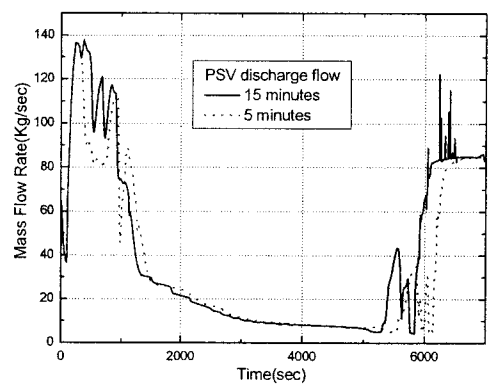


그림 3-50 급속감압운전 개시 시간에 대한 영향(방출유량)

(바) 결론

가압기 안전밸브 개방고착 사고는 정지저출력 위험도의 가장 중요한 기여 인자이다. 이러한 사고 시나리오에 대한 완화 수단을 찾기 위해 정지저출력 기간 중 위 사고에 대한 분석이 수행되었다. 본 분석을 통해 표준형 원전에서의 가압기 안전밸브 개방고착사고는 소형 및 중형 냉각재 상실사고의 특성을 공유하는 사고로 판명되었다. 고압안전주입이 실패하는 사고 시나리오에 대해서는 저압의 안전주입

계통을 작동하기 위해서는 일차측의 감압수단이 필요함을 알 수 있었다. 이러한 감압조치를 수행하기위해 증기발생기를 이용한 급속감압운전 분석이 수행되었다. 이러한 분석으로부터 운전원이 적절한 시간 안에 급속감압운전을 수행하면 안전주입탱크나 저압안전주입 계통과 같은 저압에서는 주입계통을 조기에 이용하여 노심 손상을 방지 할 수 있음을 보였다. 이러한 결과들이 정지/저출력 기간 중의 비정상 대응절차 등에 반영된다면 정지저출력의 위험도를 현저히 감소시킬 수 있을 것으로 예상된다. 또한 이러한 냉각운전은 정상운전시의 가압기 안전밸브 개방 고착사고에서도 적용될 수 있는 것으로 전출력 운전 중의 안전성 및 확률론적 안전성 평가의 품질을 높이는 데도 기여할 수 있을 것으로 기대된다.

나. 중력 급수에 대한 상세 열수력 거동 분석

(1) 연구개요

가압경수로에서 원자로가 재장전이나 유지보수 활동을 위해 정지하는 경우 정지냉각 계통이 작동하여 노심의 잔열을 제거하게 된다. 만일 이러한 정지냉각 계통의 작동이 상실되면 운전원은 냉각재 재고량을 보충하기 위한 절차를 수행해야 한다. 이러한 절차는 펌프를 이용한 안전주입과 중력에 의한 안전주입을 이용한다. 통상적으로 정상운전 상태에서 자동적으로 작동하도록 계획된 비상노심냉각 계통은 정지 저출력 기간 중에는 오동작을 방지하기 위해 비 작동상태에 놓이게 되므로 운전원은 이 기간 중에는 수동으로 이러한 계통들을 작동해야 한다. 이러한 강제 주입은 고압안전주입계통(HPSIS), 저압안전주입계통(LPSIS), 격납용기 살수계통 (CSS) 등이 배관이 이용 가능하도록 배열되어있다면 이용가능하다. 또한 일차계통의 압력이 충분히 낮아서 중력에 의해 유량이 유지될 수 있다면 이러한 계통도 이용가능하다. 이러한 중력급수는 능동계통이 사용되지 않기 때문에 중력에 의한 충분한 유량이 공급될 수 있다면 계통의 신뢰도도 여타의 능동계통에 비해 높다. 한국형 표준원전에서는 정지저출력 기간 중 발전소의 배열이 중력급수

를 이용하기에 용이하다면 중력급수를 최초의 냉각재 재고량 보충 수단으로 고려한다. 강제 급수의 경우처럼 중력급수도 HPSIS, LPSIS 및 CSS의 배관을 이용하여 재장전 수조의 냉각재를 일차 계통으로 공급한다. 이러한 유로에는 몇 개의 역지 밸브(check valve)가 일차 계통으로부터의 역류를 방지하기 위해 설치되어있다. 이러한 역지 밸브는 순방향의 유로가 형성되어 있을 때는 디스크를 열기위한 최소의 속도가 필요하기 때문에 유동 저항으로 작용한다. 중력 급수를 위한 수두가 이러한 역지 밸브의 최소 속도를 만족할 만큼 크지 않을 때는 유량 및 유동장의 예측을 위해서는 역지 밸브의 최소 속도 이하에서의 역지 밸브에 대한 모델이 필요하게 된다. 원자로 안전해석 코드인 MARS나 RELAP5 등의 코드는 이러한 상황에서의 유동저항을 계산할 수 있도록 역지 밸브에 대한 모델을 가지고 있다 [ISL, 2003a; Jeong, 1999]. 역지 밸브의 유동 저항의 계산은 역지 밸브의 디스크의 위치를 예측하여 얻어지며 디스크의 위치 예측을 위해서는 디스크에 대한 각운동량 방정식이 사용된다. 그러나 이들 모델은 각운동량 방정식에서 flow impingement 항을 사용하고 있지 않으며 또한 유동 저항 계산을 위한 유효 유동 면적 계산에 있어 잘못된 가정을 사용함으로써 실험과 많은 차이를 보이고 있다 [Lim, 2004]. 본 연구는 이러한 코드에서의 모델의 부적합성을 개선하기 위해 새로운 각운동량 방정식을 역지 밸브 모델에 도입하고 유효 유동 면적 계산을 적절히 개선하였다. 개발된 새로운 역지 밸브 모델은 단일 역지 밸브에 대한 실험과의 비교를 통해 검증되었으며 또한 발전소에서 수행된 LPSIS을 이용한 중력급수 실용성 검사의 결과와 비교되어 그 적절성을 검증하였다.

(2) 역지 밸브 모델

역지 밸브(그림 3-51)는 유동 경로의 바깥에 설치된 경첩에 연결되어 움직이는 디스크에 의해 유로가 개폐되는 밸브이다. 이 밸브는 역류를 방지하기 위해 역류가 발생할 때 빨리 닫히도록 설계된다. 또한 이 밸브는 유로에서 유동 저항을 줄일 수 있도록 개방 면적이 커지게 만들어 진다. 이런 특성으로 인해 기타의 다른 밸브에 비해 밸브에서 발생되는 압력 강하가 다른 밸브에 비해 상대적으로 작

다.

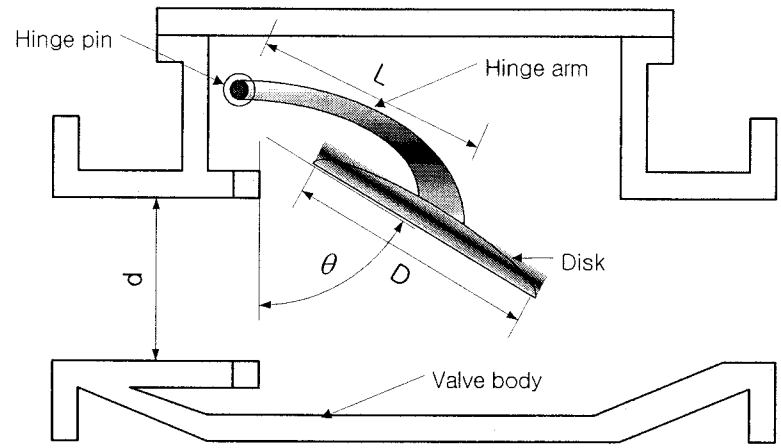


그림 3-51 역지 밸브 개략도

이 밸브는 디스크 및 arm의 무게 때문에 밸브가 완전히 개방되기 위해서는 최소의 유속을 요구한다. 이러한 밸브에 대한 최소 유량에 대한 정보는 잘 알려져 있지 않으며 개개의 밸브의 형태에 따라 달라질 수 있다. 역지 밸브에 대해 적용할 수 있는 최초의 유속에 대한 식은 Crane사 [Crane, 1988]에 의해 발표되었다. 식(1)은 유체의 밀도의 함수로 표시된 Crane사의 방정식을 나타낸다.

$$V_{\min} = 45\sqrt{\rho} \tag{9}$$

위 식에서는 유속을 결정하는 중요한 변수인 디스크의 무게나 크기 등은 배제되어 있다. 다른 종류의 최소 속도 모델로는 EPRI의 모델 [EPRI, 1988]이 제안되었다. 이 식을 유도하기위해서 역지 밸브의 디스크에 작용하는 토크의 균형에 기초하였다. 단순화한 방정식은 식(10)로 표시된다.

$$V_{\min} = \sqrt{\frac{gCW_{eff}\cos\theta}{K\rho_f A_d Sin^2\theta}} \tag{10}$$

이식에서 상수 C는 부력에 대한 상수로 물에 대해서 0.9를 가지며 실험적인 밸브구조에 의한 상수 K는 2.0이 사용된다. 그리고 A는 디스크의 면적을 나타낸

다. 이 모델은 유체의 속도를 50퍼센트 이상 과소평가하는 것으로 알려져 있다.(Kalsi, 1990) 한편 Rahmeyer [Rahmeyer, 1993]는 유체의 impingement를 고려한 보다 근본적인 모델을 개발하였으며 여기에서 쓰인 투영면적은 좀 더 정밀한 기하학적인 형태를 고려하였다. 방정식 (11)은 정적 상태에서의 최소 속도를 나타낸다.

$$V_{\min} = \sqrt{\frac{\frac{1}{\rho} K_{wt}}{K_{vel} + K_{\Delta p}}} \tag{11}$$

K_{wt} : 디스크와 ARM의 무게 영향에 대한 가중치

K_{vel} : 유체의 모멘텀에 대한 속도 영향치

$K_{\Delta p}$: 압력에 의한 가중치

(3) 각운동량 방정식

유체의 속도가 디스크를 충분히 들어 올릴 정도로 충분하지 않을 때, 밸브의 압력, 속도 등의 디스크의 운동과 관련된 변수로부터 디스크의 상태를 기술하는 모델을 가져야한다. 디스크의 운동은 뉴턴의 제 2 운동법칙인 각운동량 방정식으로 기술할 수 있다. RELAP5나 MARS는 이러한 각운동량 방정식에 의해 역지 밸브를 기술하고 있다. 이들 코드에 사용된 각운동량 방정식은 다음과 같다.

$$I\dot{\omega} = \sum T = \Delta p \cdot A_p \cdot L + \Delta p_F A_d L - M_{disk} g L Sin\theta \tag{12}$$

여기서 $A_p = \frac{\pi}{4} L^2$

방정식 (12)는 유체의 Impingement와 관련된 항을 갖고 있지 않다. 또한 압력에 의한 토크 계산을 위해 필요한 투영 면적을 경첩이 디스크의 상단에 붙어 있는 것으로 가정하여 기술함으로써 투영 면적을 과대평가하고 있다. 결과적으로 이 방정식은 역지 밸브를 통과하는 유량을 과소 예측하고 있다(그림3-56). 이러한

역지 밸브 모델을 개선하기 위해 새로운 각운동량 방정식을 도입하였다. 속도 영향을 고려한 각운동량 방정식은 다음과 같다.

$$I\frac{d^2\theta}{dt^2} = \left(T_p + T_v\right) - \left(\frac{1}{2}M_{arm} + M_{disk}\right)gL \cdot BSin\theta + \Delta p_F A_d L - C_d D^5 \frac{d\theta}{dt}\left|\frac{d\theta}{dt}\right| \quad (13)$$

디스크 양단의 압력 차이는 코드의 지배방정식으로부터 구한다.

(4) 수치 해법

사용된 수치 해법은 기존의 MARS에서 사용된 방법과 동일하며 다음과 같다.

$$\dot{\omega}^{n+1} = \left(\sum T\right)^n / I \quad (15)$$

새로운 각속도는 위식으로부터 다음과 같이 구해진다.

$$\omega^{n+1} = \omega^n + \left(\sum T\right)^n / I\,\Delta t \quad (16)$$

새로운 디스크의 각은 위의 식으로부터 다음과 같이 구해진다.

$$\theta^{n+1} = \theta^n + 0.5\left(\omega^{n+1} + \omega^n\right) \quad (17)$$

식 (17) 에 의해 주어진 디스크의 각으로부터 유효 유동면적이 구해진다. 유효 유동면적은 유체의 지배 방정식에서 유동 저항을 구하는데 사용되어 진다.

(5) 회전 관성 모멘트 계산

디스크와 암(arm)의 관성 모멘트는 단순화한 기하학적 가정을 사용하여 계산한다. 디스크는 이상적인 원판으로 가정하며 암은 원기둥으로 가정한다. 아래의 그림은 디스크와 암의 가정된 기하학적인 모양을 보여준다. 이 모양에 대한 관성 모멘트는 다음의 식으로 표현된다.

$$I = \int r^2 dm = \int_0^L r^2 \rho A dr + \int_{L-D/2}^{L+D/2} r^2 \sqrt{\frac{D^2}{4} - (L-r)^2}\, \rho d A dr \tag{18}$$

위의 식을 적분하면 다음의 관성 모멘트 값을 얻는다.

$$I = M_{disk}\left(L^2 + \frac{D^2}{16}\right) + M_{arm}\frac{L^2}{3} \tag{19}$$

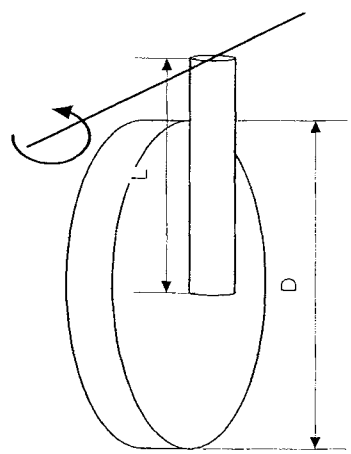


그림 3-52 단순화한 스윙 역지
밸브의 디스크와 암

(6) 결과 및 고찰

(가) 단일 역지 밸브에 대한 실험과의 비교

본 연구에서 개발된 역지 밸브 모델을 검증하기위해 역지 밸브에 대한 실험과 비교하였다. 본 비교에 사용된 역지 밸브의 사양은 표 3-21에 나타나 있다.

표 3-21 역지 밸브 사양

Disk mass (kg)	Arm Mass (kg)	Arm Length (m)	Disk Diameter(m)	Inner Diameter(m)	Max. Open angle (degree)
24.964	5.445	0.189	0.333	0.305	78

그림 3-53은 본 모델을 사용하여 MARS로 계산한 결과와 실험의 비교를 보여준다. 그림 3-53에 보는 바와 같이 이전 모델은 주어진 속도에 비해 실험과 비교하여 디스크의 각을 과대 예측하고 있음을 알 수 있다. 이전 모델은 실험에 비해 낮은 속도에서 밸브가 완전 개방된다. 본 모델은 낮은 속도에서 약간 과대 예측하고 완전히 열리는 각은 과소 예측되는 경향을 보인다. 그러나 전체적인 실험값을 비교적 잘 맞추고 있다.

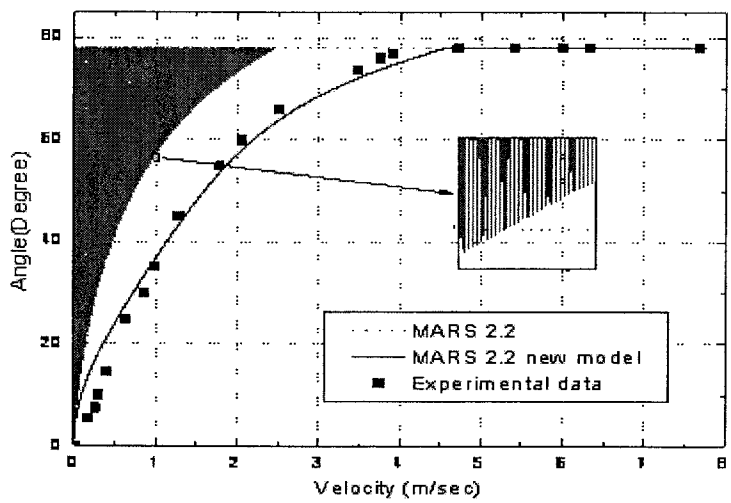


그림 3-53 단일 역지 밸브 모델 결과 비교

(나) 중력 급수 라인 테스트

본 절에서는 LPSIS를 경유하는 중력급수 라인에 대한 테스트를 수행하였다. 그림 3-54 는 LPSIS의 배관 배열을 보여준다.

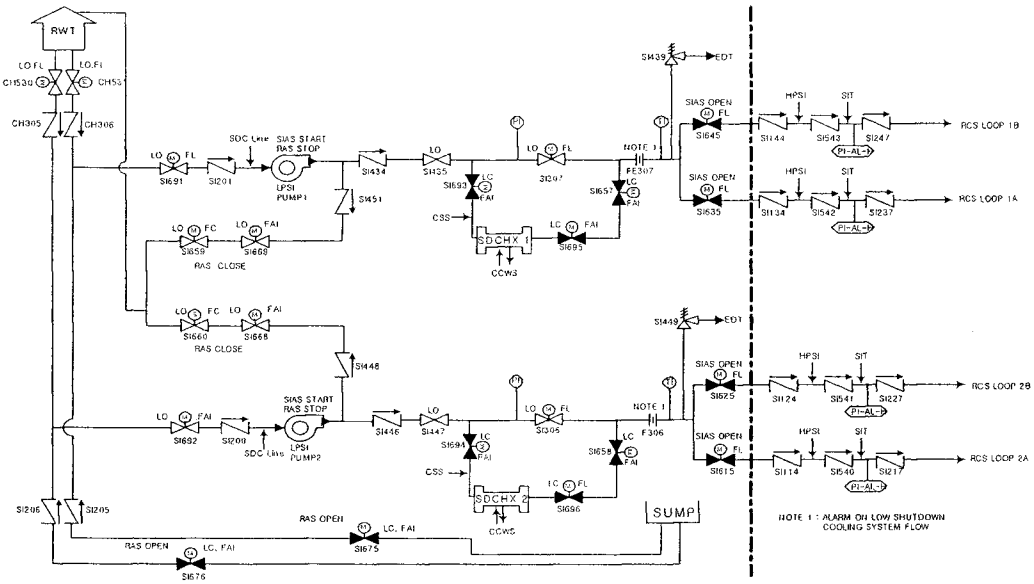


그림 3-54 저압 안전 주입 계통의 단순 계통도

본 분석에서는 한 계열의 중력 급수 라인이 이용되는 것으로 계산하였다. 한 계열을 저압안전주입계통은 5가지 종류의 9개의 역지 밸브를 가지고 있다. 각 각의 밸브에 대한 자세한 사양은 표 3-22 에 나타나 있다.

표 3-22 중력 급수 라인에 있는 역지 밸브의 사양

	20" (150psi)	**10" (900psi)**	**20" (900psi)**	**12" (2500psi)**	**14" (2500psi)**
Flapper Diameter (m)	0.409	0.199	0.385	0.209	0.241
Inlet Diameter (m)	0.350	0.170	0.329	0.179	0.206
Disk arm length(m)	0.258	0.126	0.243	0.132	0.152
Disk mass (kg)	41.640	10.070	62.595	15.150	23.269
Arm Mass(kg)	20.956	4.808	24.675	8.709	11.249
Avg. Mass (kg) (Wdisk+1/2Warm)	52.118	12.474	74.933	19.504	28.894
Moment of Inertia(kgm2)	3.681	0.209	4.769	0.356	0.711
Valve inlet area (m)	0.096	0.023	0.085	0.025	0.033

그림 3-55는 LPSIS를 경유한 중력 급수 라인의 계산 노드를 보여주고 있다.

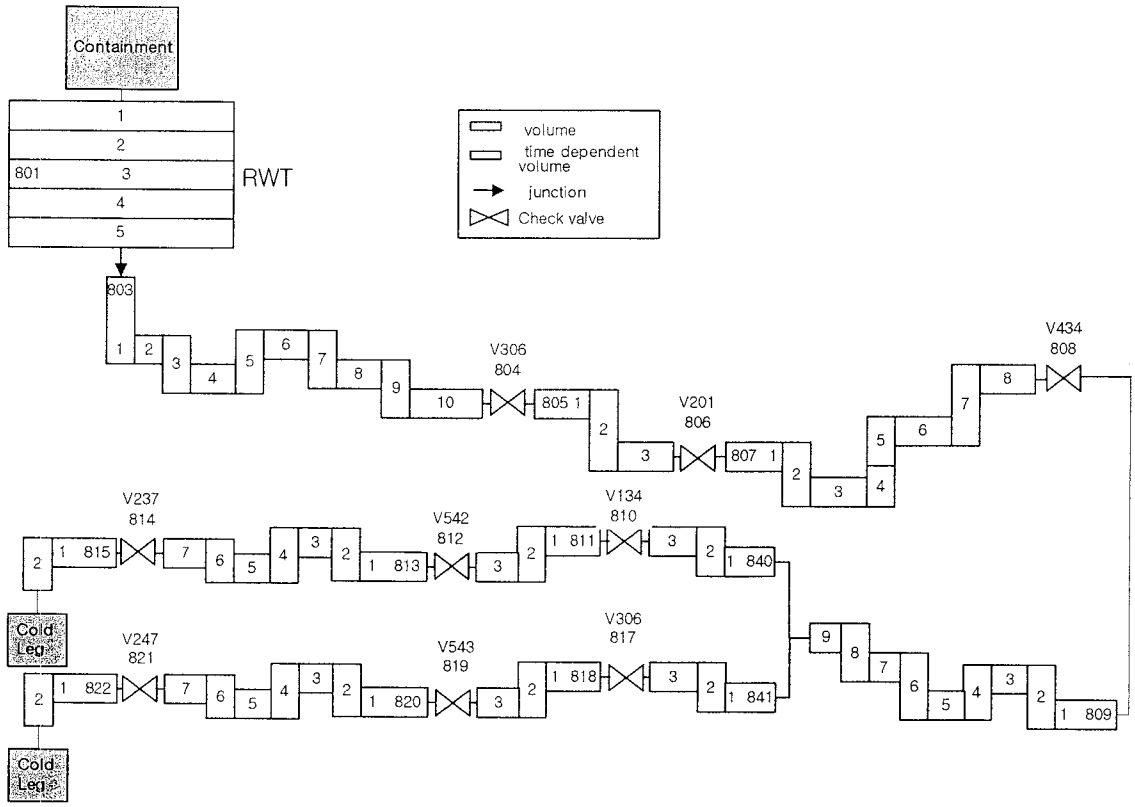


그림 3-55 저압 안전주입 계통을 경유한 중력 급수 라인의 계산 노드

그림 3-56은 MARS를 이용한 계산결과와 표준원전에서 수행한 테스트와의 비교를 보여준다. 테스트 결과는 한국형 표준원전의 부분충수 (mid-loop) 운전 시 비상 대응 절차를 위한 테스트에서 얻어진 결과이다. 이전 모델에 의한 계산은 중력급수 유량을 과소평가하고 있다. 이전 버전의 이와 같은 유량의 과소평가는 flow jet에 대한 모델을 가지고 있지 않으며 또한 밸브의 개방 면적을 과소평가함으로써 과도한 압력 강하가 배관에서 발생했기 때문인 것으로 추정된다. 본 연구에서 개발된 모델은 발전소의 테스트 결과와 비교하여 잘 일치하고 있음을 알 수 있다. 그러나 본 모델도 테스트의 시작과 끝에서 발생하는 진동 현상은 모델하지 못한다.

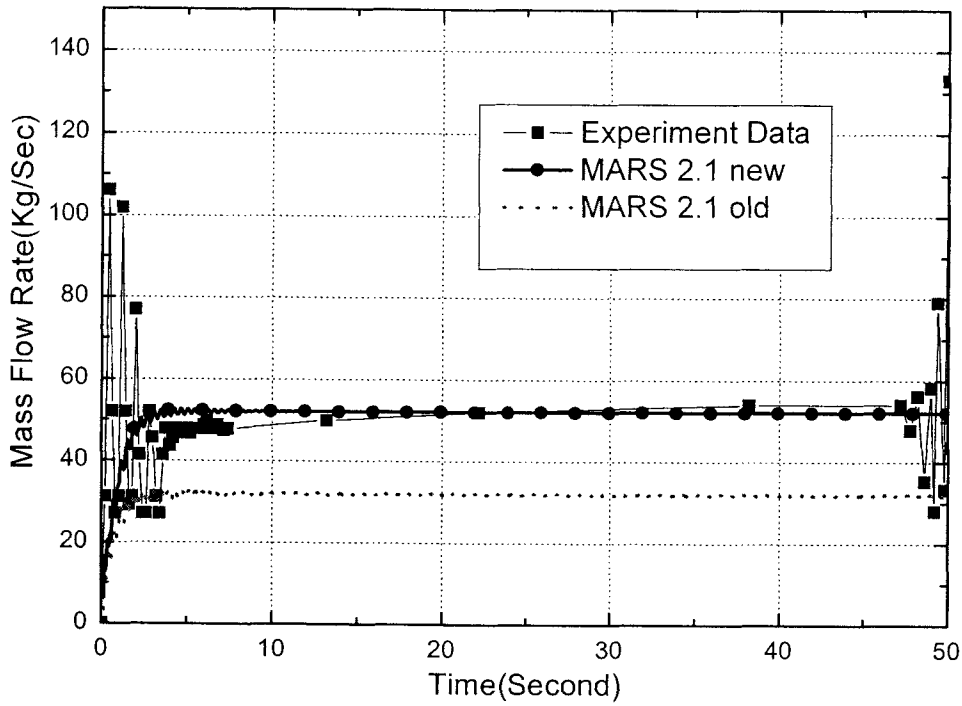


그림 3-56 중력급수 유량비교

(7) 결론

본 연구에서는 새로 개발된 역지 밸브의 각 운동량 방정식을 이용하여 역지 밸브 모델을 개선하였다. 본 모델은 단일 역지 밸브의 실험 치와 비교하여 검증되었다. 또한 중력 급수 라인에서 여러 개의 역지 밸브에 대한 중력급수 효과를 모의하였다. 저압 안전주입 라인이 중력급수 라인으로 선정되었으며 이 파이프라인에 대한 배열을 설계 데이터로부터 구하여 입력 자료를 완성하였다. 모의계산은 중력급수 테스트 데이터와 비교되어 잘 일치됨을 보였다. 본 분석에 근거하여 중력급수는 정지/저출력 기간 중 일차측의 압력이 대기압과 유사한 경우에 노심 냉각재 보충 수단으로 사용가능할 것으로 판단되며 이 후 일차측과의 통합계산을 통하여 그 효용성이 검증되어야 할 것으로 판단된다.

다. 저온 과압 사고에 대한 상세 열수력 분석

(1) 연구개요

기존 PSA 모델에서 저온 과압 사고의 영향은 공학적 판단에 근거하여 선별 제거된 상태로 저온 과압 사고의 현상학적 거동 특성에 대한 이해가 매우 필요한 상황이다. 저온 과압(LTOP; Low Temperature Over-Pressure) 사고는 일차측이 물로 가득 채워진 만수위(solid state) 상태에서 질량이나 에너지 유입에 의해 발생한다. 본 분석에서는 LTOP 사고가 발생할 수 있는 시나리오를 선정하였으며 이 시나리오에 따라 분석을 수행하였다.

(2) 시나리오 선정

본 분석에서는 질량유입에 의한 LTOP 사고의 대표적인 시나리오로 정지저출력 운전 특성인 2번의 만수위 운전 시 "화학 및 체적 제어계통 내 유출밸브의 갑작스런 닫힘" 을 선정하였다. 또한, 에너지유입에 의한 LTOP 사고의 대표적인 시나리오로 만수위 운전 시 "정지냉각기능 상실사고 발생"을 선정하였다. 국내 LTOP 사고 경험자료 수집/검토 (고리원전 2건, 한수원 전문가 초청 세미나), 전반부 만수위 운전 및 정적/동적 배기 운전 시 충전 및 유출 유량 조사, RCS 및 LTOP 방지 밸브 상세 규격 조사. 정지 저출력 기간 중 두 번의 만수위 운전 (POS3, POS 12)이 분석 대상으로 선정되었다.

(3) POS 12 에서의 저온 과압 사고

(가) 사고 개요

일차계통 비응축 가스제거를 위한 만수위 운전 중 부적절한 충수 펌프 기동에 의해 일차측으로 질량이 유입된다.

(나) 분석방법

아래의 그림에 나타난 바와 같이 RCS를 같은 체적과 높이를 갖는 단순한 구조물로 모의하였다. MARS 코드가 분석용 코드로 사용되었다. 사고 시작과 동시에 충전펌프로부터 일차측으로 물이 공급되며 일차측은 물로 가득 차있다. 가압기 상부에는 배기구가 달려있으며 물은 배기구를 통하여 방출된다.

(다) 분석결과

아래의 그림에 나타난 바와 같이, POS 12에서는 비응축 가스제거를 위한 배기 밸브가 열려있기 때문에 충수 펌프가 기동하여 초기 압력이 빠르게 올라가기는 하지만 LTOP 방지 밸브의 설정 치에는 도달하지 않는 것으로 분석되었다. 본 분석에 의해 POS 12에서의 LTOP 사고는 사고 발생이후 더 이상의 사고 전개는 없는 것으로 판단된다.

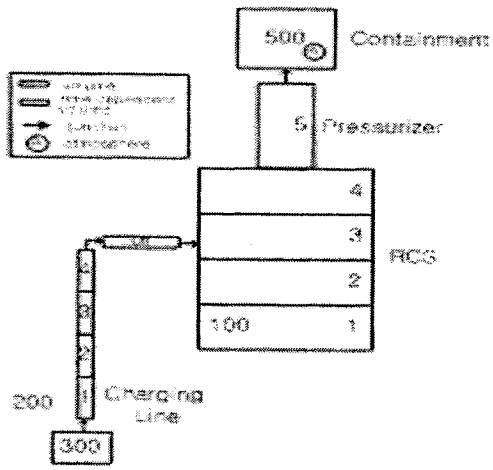


그림 3-57 POS 12 RCS 모델

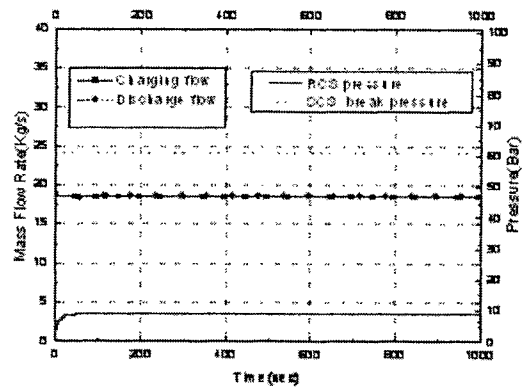


그림 3-58 POS 12 일차계통 압력변화

(4) POS 3 에서의 저온 과압 사고

(가) 사고 개요

가압기 기포 제거를 위한 충수 운전 중 부적절한 충전 펌프 기동에 의해 질량이 유입되거나 또는 동일한 운전 중 정지 냉각 계통 고장으로 인한 열제거 원

상실에 의해 에너지가 유입된다.

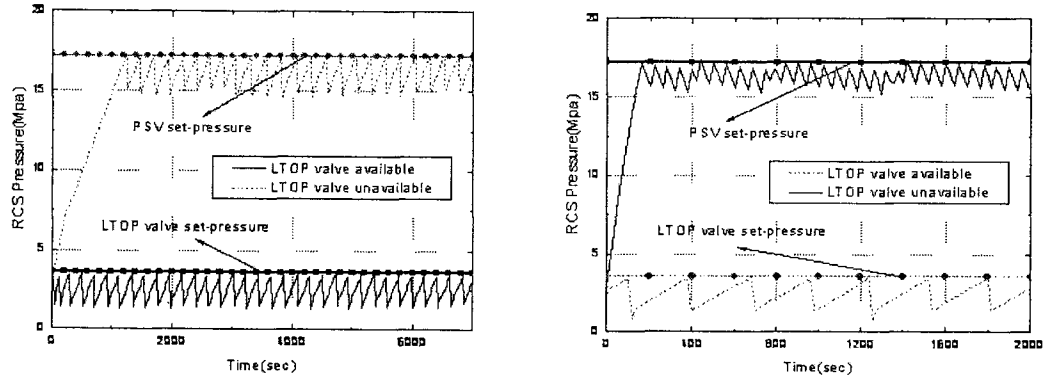
(나) 분석 방법

POS 3 에 대한 정지 냉각 기능 상실 분석용 입력 자료를 수정하여 만수위 운전 상태의 초기 조건 하에서 분석을 수행하였다. 분석용 코드로는 MARS가 사용되었다.

(다) 분석 결과

아래의 그림들에 나타난 바와 같이, POS 3은 격납건물로의 배기계통이 존재하지 않기 때문에 질량 유입 및 에너지 유입 사고 시 압력이 급격히 증가하는 경향을 보였다. 특히, 질량 유입 사고의 압력 증가가 에너지 유입 사고 보다 매우 빨랐다.

LTOP 방지 밸브에 작동 압력까지 수 분만에 도달하였으며 이후 계속적인 압력 증가로 인해 LTOP 방지밸브는 개폐를 반복하게 된다. 또한 LTOP 방지 밸브가 이용 불능인 경우를 고려한 사고 시나리오에서는 가압기 안전밸브(PSV)의 작동 압력 까지 상승한 후 개폐를 반복하게 된다. 이러한 잦은 밸브의 개폐는 밸브의 고장 원인으로 작용하여 밸브를 개방고착 시키거나 개방 실패로 이어질 수 있다. 이러한 개방 고착은 정지/저출력 운전 중의 LOCA의 발생 원인을 제공할 수 있을 것으로 판단된다. 한편, LTOP 밸브가 폐쇄 고착되어지는 경우는 PSV 개방 압력까지 급속하게 가압되므로 정지냉각 계통의 열교환기 파열 가능성이 있으므로 ISLOCA(Interfacing System LOCA)의 발생 원인을 제공하게 된다.



(a) 에너지 유입에 압력증가 (b) 질량 유입에 의한 압력증가
그림 3-59 POS 3 에서의 저온 과압 사고 해석 결과

(5) 결론

POS 12에서의 LTOP 사고는 분석결과 비교적 안전하고 정지/저출력 PSA에 반영할 필요는 없을 것으로 확인되었다. POS 3 에서의 LTOP 사고는 사고 진행 속도도 급격하고 LOCA의 발생 원인을 제공할 것으로 예상된다. 이 사고는 정지 저출력 PSA 모델에 반영하여야 할 것으로 사료된다.

라. 관류 응축 현상에 대한 상세 열수력 분석

(1) 연구개요

관류 냉각 (reflux cooling)은 정지 저출력 운전 중 정지냉각 계통이 상실되고 이차측의 증기발생기가 이용 가능한 상태에서의 2상 유동을 이용한 일차계통 냉각 수단으로써 그 현상의 불확실성으로 인하여 현재의 정지 저출력 PSA 모델에 반영되지 못하였다. 이러한 불확실성을 제거하기 위해서는 관류 응축 (reflux condensation) 현상을 적절히 모사할 수 있는 열수력 코드를 이용하여 해당 사고 경위에 대한 계산을 수행하여야 한다. 정지/저출력 PSA의 성공기준 및 사고 경위 해석용으로 원자력 연구소에서 개발된 MARS코드가 사용되어 왔으나 MARS 코

드는 관류냉각 분석 능력에 대한 검증이 충분히 이루어지지 않았다. 본 연구에서는 MARS 코드를 관류냉각 현상과 관련된 사고 경위에 적용하기 전에 MARS 코드의 관류냉각 현상 모의 능력을 검증하기 위하여 검증계산을 수행하였다.

(2) 검증 계산용 실험 선정

프랑스에서 수행된 BETHSY 실험을 검증용 실험으로 선정하였다. BETHSY 실험 장치는 900MWe 3-Loop PWR 모의 대형 실험 장치로 본 연구에서는 부분 충수 운전 중 잔열제거계통 상실사고 실험에 대한 모의를 수행하였다. BETHSY 실험은 저압, 저출력 하에서 비응축성 기체 존재 시 물리적 현상을 이해하고 비응축성 기체 존재 시 증기발생기를 통한 관류 응측 효과를 고찰하기 위해 수행되었다. 본 분석에서 수행된 실험장치의 초기 조건은 표 3-23에 나타나 있다.

표 3-23 BETHSY 실험 초기 및 경계조건

수위	고온관 중간
노심 상부	비응축성 기체로 충진
증기발생기	1대만 사용 가능
배기	가압기 및 원자로 상부 배기구(d-1.81mm)
노심 출력	143 Kw
2차측 상태	보조 급수 상실 가정

본 실험은 약 33,000초 동안 수행되었으며 시간에 따른 사건의 전개는 표 3-24에 정리되어 있다.

표 3-24 시간에 따른 실험 전개 순서

시간 (second)	사건
0	Loss of RHRS
	Sight Level Indicator (d = 1.2 mm) Broken
	RHR Suction Line 을 통한 CVCS Letdown (d = 4.29 mm) Open
1800	Letdown Close
	증기발생기 ADV (d = 8.86 mm) Open
31668	증기발생기 Aux. feed water 공급
32452	실험종료

(3) 정상 상태 계산

아래의 그림은 BETHSY 실험을 모사하기 위한 계산 노드의 구성을 보여주고 있다. 그림에서 보는 바와 같이 실험 장치는 3개의 주요한 냉각재 루프로 구성된다. 노심은 9개의 계산 체적으로 구성된다. 각 루프는 고온관, 26개의 U-튜브를 모델하는 계산체적을 갖는 증기발생기와 흡입관, 펌프 및 저온관으로 구성된다. 가압기 및 밀림관은 각각 11개, 10개의 계산 체적으로 구성된다. 가압기 및 노심 상부의 배기구는 대기압으로 간주된다. 육안 관측 장치를 나타내는 작은 파열관이 1번 루프에 연결되며 실험 모사 시작과 동시에 개방된다. 화학 및 체적제어 계통의 방출관도 1번 루프에 연결되며 계산 시작과 동시에 개방된다. 그러나 이 라인은 약 30분 후에 닫히게 된다. 2차 계통에서는 1번 증기발생기가 1차 루프에 연결되며 2번 및 3번 증기발생기는 공기로 충진되어 있다. 1번 증기발생기의 2차측은 원형 쉘, 습분분리기, 및 증기돔으로 구성된다. 대기발출밸브는 주증기관에 연결되며 계산 시작 후 30분에 개방된다. 노심 및 증기발생기의 U-튜브는 열구조물로 모델링되며, 노심은 붕괴열을 나타내는 열원을 갖는다.

실험을 정확히 모사하기위해서는 실험 시작 시의 상태를 코드의 계산이 적절하게 맞추어야 한다. 아래의 표는 RELAP5.MOD3.3 과 MARS코드의 정상상태 계산 결과를 보여주고 있다. 표에서 보는 바와 같이 코드에서의 정상상태는 실험과 비교해 비교적 잘 맞추고 있음을 알 수 있다.

표 3-25 초기조건 계산 결과 비교

Parameters	Experiment	RELAP5 /MOD3.2	REALP5 /MOD3.3	MARS2.1
Upper plenum pressure (MPa)	0.10±0.008	0.10	0.10	0.10
Total primary mass (kg)	1135±30	1110	1068	1111
Hot leg void fraction	0.5	0.49	0.5	0.5
Temperatures (℃)				
Core inlet/outlet	63.6±2/63.6±2	62.2/65.2	62.5/66.2	64.6/67.7
Hot leg	62.8±2	63.7	66.8	67.5
Cold leg	52.4±2	53.8	53.6	54.5
Nitrogen mass fraction				
Upper plenum	0.88	0.83	0.81	0.81
Pressurizer	0.85	0.85	0.85	0.85
Hot leg	0.89	0.83	0.81	0.80
SG inlet plenum	0.84	0.84	0.82	0.81
SG 1 secondary side				
Pressure (MPa)	0.122±0.004	0.122	0.122	0.122
Average temperature (℃)	65.0±2	65.6	65.7	65.9
Total mass (kg)	1134±25	1134	1134	1134

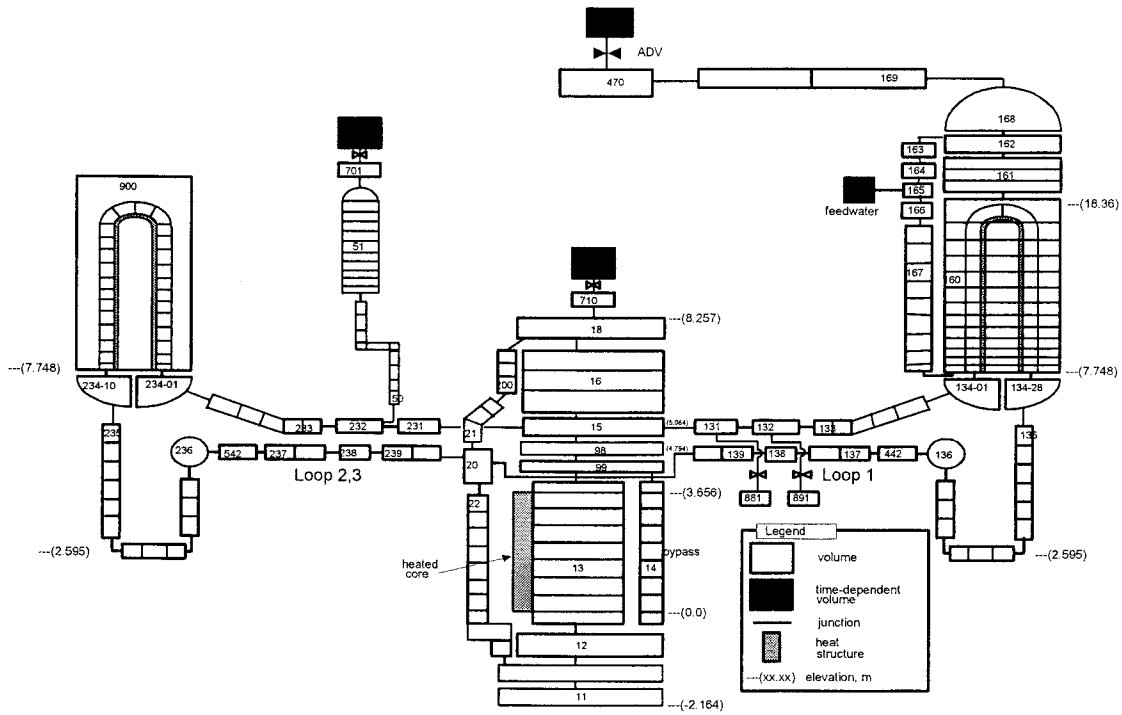


그림 3-60 전산 계산 체적

(4) 결과 분석

표 3-26는 RELAP5/MOD3.3 및 MARS2.1 코드의 실험 결과와의 사고 진행 시간의 비교를 보여주고 있다. MARS 및 RELAP5는 실험과 비교해 사고 진행 과정을 적절히 맞추지 못하고 있으며 사건 진행이 지연되어 나타나고 있음을 알 수 있다. 그림 3-61에서 보는 바와 같이 사고 진행 초기에서 일차측의 압력이 실험에 비해 급격히 증가하는 것을 알 수 있다. 또한 그림 3-62에서 보는 바와 같이 2차측의 압력은 약 5000초의 지연 시간을 두고 증가하는 것을 알 수 있다. 이러한 일차측 및 2차측의 압력 추이는 RELAP5/MOD3.3 이나 MARS 의 계산에서 일차측에서 발생한 열이 2차측의 증기발생기로 잘 전달되지 않고 있음을 나타낸다. 이러한 1차측 및 2차측의 열전달 감소 효과는 RELAP5/MOD3.3 및 MARS 코드의

계면 마찰 계산의 부적절성에 기인한다. 증기발생기의 U-튜브에서는 응축된 물과 증기의 흐름이 반대의 방향을 갖는다. 응축된 물은 중력에 의해 고온관 쪽의 노즐로 흘러내리며 반대로 증기는 부력에 의해 U-튜브의 상부로 향하게 된다. 이 때 각 상의 계면 마찰이 과대평가되면 응축된 물은 고온관으로 흘러내리지 못하고 U-튜브에서 관을 막아 열전달을 현격히 떨어뜨리게 된다.

본 분석은 운전원 조치시간의 관점에서 증기발생기의 고갈시간이 지연됨으로 인해 RELAP5/MOD3.3 이나 MARS2.1 코드의 예측은 낙관적이다. 현재의 RELAP5/MOD3.3 및 MARS 코드는 관류냉각 모의를 위해 계면 마찰 모델 개선의 개선이 필요하며 사고 경위 분석 및 성공 기준 설정을 위한 계산 코드로 부적절한 것으로 사료된다.

표 3-26 시간별 발전소의 주요 거동

Events	Experiment (s)	RELAP5 /MOD3.2 (s)	RELAP5 /MOD3.3 (s)	MARS2.1 (s)
Letdown via RHRS opening	0	0	0	0
Sight level indicator opening	0	0	0	0
Core power build-up	0	0	0	0
Core power stabilized at 143kW	14	14	14	14
Upper plenum saturated	519	500	*	*
Upper head vent steaming	1120	1200	3870	3570
Reflux cooling starts	1207	1300	1250	1290
Pressurizer vent steaming	1792	2800	4770	4230
Letdown closed	1800	1800	1800	1800
SG1 ADV opening	1800	1800	1800	1800
SG1 riser fluid saturated	4454	9500	*	*
Cold leg empty	25000	9000	10500	10200
Hot leg empty	28000	28000	24150	26400
Aux. Feedwater supply starts	31668	32800	34890	34745
End of test/calculation	32452	35000	35000	35000

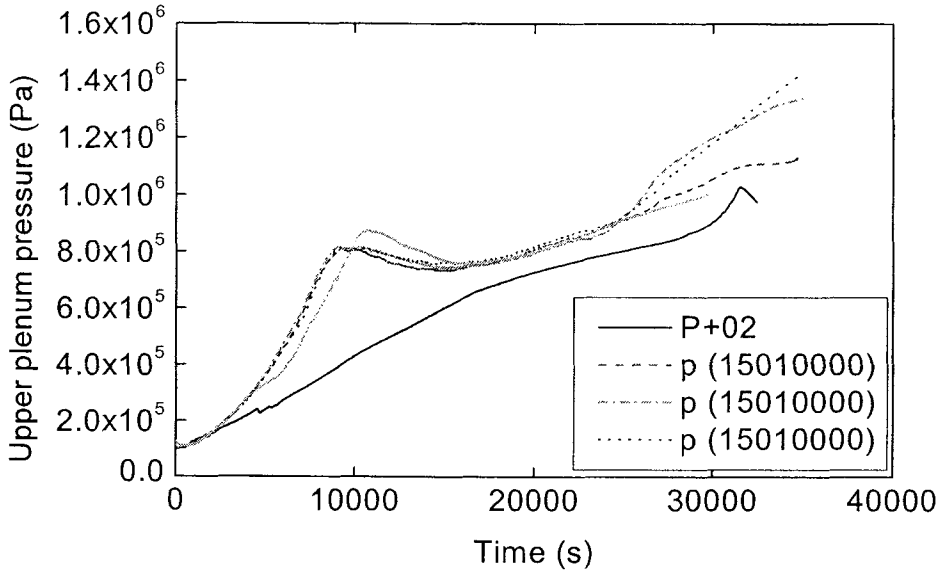


그림 3-61 일차측 압력 거동

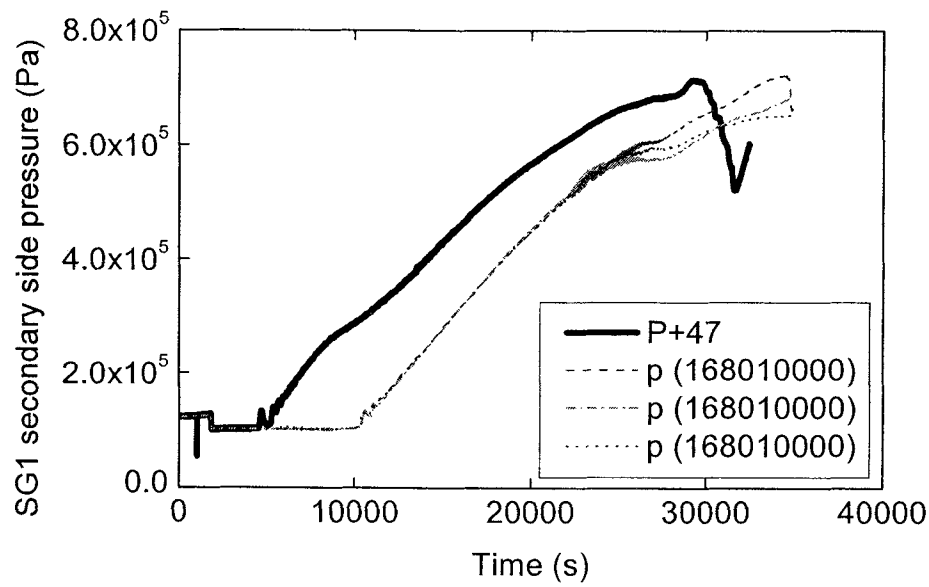


그림 3-62 2차측 압력거동

제 2 절 정지/저출력 위험도 관리 기술 기반 구축

1. 정지/저출력 초기사건 DB 검색 및 분석 프로그램 개발

원자력 발전소가 상업운전을 시작한 이후 세계적으로 정지/저출력 운전 기간 동안 노심손상과 같은 중대사고로 진전된 사례는 없었다 하더라도 RCS 비등과 같이 잠재적인 정지/저출력 위험성을 갖는 많은 사건/사고들을 경험한 바 있다. 정지/저출력 운전 모드에서의 사건/사고 자료는 정지/저출력 PSA의 초기사건 분석을 위한 기초 자료일 뿐만 아니라 사건/사고 사례 분석을 통한 정지/출력 위험도에 대한 이해의 폭을 넓히고 자료 분석을 통한 정지/저출력 안전성 저해 요인을 파악하는데 필수적이다. 또한, 이러한 자료들은 발전소 스텝들에게 발전소의 안전한 운전을 위한 유용한 교육 자료로 활용될 수 있으며, 이를 통해 궁극적으로 정지/저출력 초기사건 발생의 저감을 기대할 수 있다.

본 과제에서는 정지/저출력 PSA 초기사건 분석 분야의 품질 개선과 국내 원전의 정지/저출력 운전 중 초기사건 발생 저감을 통한 안전성 향상을 위하여 국내외 원전에서 정지/저출력 운전 기간 동안 경험한 다양한 사건/사고들에 대한 연구를 수행하였으며, 연구내용을 간단히 정리하면 다음과 같다.

○ 국내·외 각종 문헌을 통하여 정지/저출력 운전 기간 중에 경험한 사건/사고 자료를 수집하였다 (총 625건).

○ 수집된 자료를 여러 가지 기준에 따라 분류하고 이를 데이터베이스(DB)화 하였다.

○ 발전소 스텝들을 손쉬운 DB 접근과 궁극적인 국내 원전의 정지/저출력 초기사건 저감을 위한 DB 검색 및 분석 프로그램(LEDB; Low power and shutdown Events DataBase)을 개발하였다.

○ 또한, 초기사건 분석 분야의 등급 개선을 위해 개발된 LEDB 프로그램을 이용하여 경험 자료에 의한 정지/저출력 초기사건 상세 분석을 수행하였다.

이 들에 대한 자세한 연구 내용 및 결과들은 기술보고서 및 논문[박진희, 2003a; 박진희, 2003b; 김태운, 2003]에 기술되어 있으며, 본 보고서에서는 이어지는 세션에서 순서에 따라 간단히 정리하도록 하겠다.

가. 정지/저출력 초기사건 경험 자료 수집 및 DB 구축

다양한 자료원으로부터 국내·외 정지/저출력 운전 중에 경험한 사건/사고 자료들을 수집하였다 (표 3-27 참조). 각 자료원은 사건 DB 개발을 목표로 자료의 형태 및 내용, 자료원의 성격, 자료의 상세정도, 분석내용 등을 고려하여 직접적으로 사건자체의 정보만을 다룬 자료원을 1차 자료원으로, 개별사건에 대한 상세분석을 포함한 자료원은 2차 자료원으로 분류하였다. 또한 각 사건의 유사성을 분석하고 사고의 원인 및 종류에 따른 분석 자료를 포함하고 있는 자료원을 3차 자료원으로 분류하였다.

표 3-27에서 알 수 있듯이 정지/저출력 사건/사고 경험 자료는 주로 미국과 일본에서 발간된 참고 문헌과 미국 원전에서 보고된 LER (Licensee Event Report)에 기초하고 있으며, 수집된 자료 가운데 중복된 사건/사고들을 제거하고 최종적으로 총 625건의 자료가 수집되었다. 자료 수집 대상 기간은 1973년부터 1999년도까지로 미국 원전에서 발생한 정지/저출력 운전 중 사건/사고 이력이 대부분을 차지하며, 국내 2개 원전에서 발생한 2 건의 사건과 유럽 8개 원전에서 발생한 11 건이 포함되어 있다. 표 3-28은 각 원전별 정지/저출력 사건/사고 건수를 나타낸다. 여기서, 국내 자료의 경우 IAEA 등에 보고된 자료로 국내 원전에서 독자적으로 수집 분석된 자료가 아님에 유의하여야 한다. 국내 자료의 경우는 미국의 LER과 같은 정지/저출력 운전 중에 발생되는 사건/사고의 보고 및 관리 체계가 확립되어 있지 않기 때문에 보고된 정지/저출력 초기사건/사고 자료 건수가 거의 없는 실정이다. 따라서 현재로서는 국내 원전 고유의 정지/저출력 사건/사고 경험 자료를 확보하기는 매우 어려운 상황이다.

최종적으로 수집된 총 625건의 정지/저출력 사건 및 사고 경험 자료에 대해

다음과 같은 분류기준으로 개별 자료를 상세 분류하였고, 그 결과를 바탕으로 마이크로소프트(MS)사의 Access 프로그램을 이용한 DB를 구축하였다. 그림 3-63은 정지/저출력 DB 화면을 예시하고 있다.

○ 발전소명

○ 발생일

○ 사건분류정보

○ 사건 상보

○ 사고시 운전모드

○ 정지냉각계통의 정지시간

○ 자료원에 대한 정보

○ 발전소 유형

표 3-27. 정지/저출력 초기사건 자료원

자료유형	자료성격	출처	자료원	자료명	수집기간	수록내용	자료형태	비고
직접자료	1차	USNRC	LER DB		1975-1996	사건	CD-ROM	NRC 전산DB
		ONL		NUREG/CR-2000	1985-1990	RHR	보고서	개요만 수록; 매년 정기 간행
		USNRC		Information Notice			보고서	사고조사 보고서
		USNRC		NUREG-1410	1976-1990		보고서	
		국내		원자력발전연보	1978-	사건		사고조사 보고서
	2차			AEOD-C503	1976-1984	RHR	보고서	개별 사건 상세 분석
				AEOD-C702	1977-1987	배수운전	보고서	개별 사건 상세 분석
		ONL		NUREG/CR-2799	1976.6-1981	RHR	보고서	개별 사건 상세 분석
				OECD/NEA-IRS				
				NUREG/CR-5015				
		Seabrook						
	3차	EPRI	EPRI	NSAC-52	1976-1981	RHR	보고서	개별 사건 분석 및 통계분석
		EPRI		NSAC-156		RHR	보고서	개별 사건 분석 및 통계분석
		일본	JAERI	JAERI-M91-143	1976-1990	RHR	보고서	개별 사건 분석 및 원인분석
		일본			1990.하-1992	RHR	보고서	개별 사건 분석 및 원인분석
간접자료	개선대책	USNRC		NUREG/CR-4005		RHR	보고서	개선대책 종합정리
	PSA	EPRI		NSAC-84		PSA	보고서	Zion 발전소 정지저출력 PSA 보고서
	PSA	BNL		NUREG/CR-6144		PSA	보고서	Surry 발전소 정지저출력 PSA 보고서

표 3-28 발전소별 정지/저출력 운전 중 초기사건 발생 현황(1/2)

발전소명	발생 건수	발전소 Type	발전소명	발생 건수	발전소 Type	발전소명	발생 건수	발전소 Type
고리 2	1	PWR	Oconee 2	2	PWR	ARNOLD	3	BWR
고리 3	1	PWR	Oconee 3	5	PWR	BIG ROCK POINT	1	BWR
ANO 1	5	PWR	Palisades	5	PWR	Brunswick 1	3	BWR
ANO 2	10	PWR	Palo Verde 2	2	PWR	Brunswick 1 & 2	1	BWR
Beaver Valley 1	11	PWR	Palo Verde 3	1	PWR	Brunswick 2	3	BWR
Blayais 1	1	프랑스, PWR	Point Beach 1	2	PWR	Clinton	7	BWR
Blayais 4	2	프랑스, PWR	Point Beach 2	1	PWR	COOPER	10	BWR
Braidwood 1	5	PWR	Prairie Island 2	1	PWR	DRESDEN 2	5	BWR
Braidwood 2	3	PWR	Rancho Seco	12	PWR	DRESDEN 3	2	BWR
Millstone 2	5	PWR	Ringhals 4	1	스웨덴, PWR	Fermi 2	11	BWR
Millstone 3	1	PWR	Robinson 2	3	PWR	FITZPATRIC K	13	BWR
Bugey 2	2	프랑스, PWR	Salem 1	13	PWR	Grand Gulf 1	8	BWR
Bugey 3	2	프랑스, PWR	Salem 2	14	PWR	Hatch 1	5	BWR
Byron 1	4	PWR	San Onofre 1	7	PWR	Hatch 2	4	BWR
Calvert Cliffs 1	10	PWR	San Onofre 2	7	PWR	Hope Creek 1	6	BWR
Calvert Cliffs 2	13	PWR	San Onofre 3	1	PWR	LaSalle 1	3	BWR
Catawba 1	8	PWR	Seabrook 1	1	PWR	LaSalle 2	5	BWR
Catawba 2	3	PWR	Sequoyah 1	12	PWR	Limerick 1	3	BWR
Comanche Peak 1	2	PWR	Sequoyah 2	3	PWR	Limerick 2	4	BWR
Connecticut Yankee	1	PWR	Shearon Harris 1	3	PWR	Millstone 1	3	BWR
Cook 1	4	PWR	South Texas 1	1	PWR	Browns Ferry 1	1	BWR

표 3-28 발전소별 정지/저출력 운전 중 초기사건 발생 현황(2/2)

발전소명	발생 건수	발전소 Type	발전소명	발생 건수	발전소 Type	발전소명	발생 건수	발전소 Type
Cook 2	6	PWR	St. Lucie 1	4	PWR	Browns Ferry 2	1	BWR
Crystal River 3	17	PWR	Summer	5	PWR	Monticello	2	BWR
Davis Besse 1	17	PWR	Surry 1	21	PWR	Nine Mile Point 1	2	BWR
Diablo Canyon 1	4	PWR	Surry 2	14	PWR	Nine Mile Point 2	6	BWR
Diablo Canyon 2	4	PWR	Three Mile Island 1	2	PWR	Oskarshamn 3	1	스웨덴, BWR
Farley 1	8	PWR	Three Mile Island 2	1	PWR	Oyster Creek	3	BWR
Farley 2	3	PWR	Trojan	9	PWR	Peach Bottom 2	9	BWR
Foreign Reactor	1	PWR	Turkey Point 3	8	PWR	Peach Bottom 3	4	BWR
Ft.Calhoun 1	7	PWR	Turkey Point 4	5	PWR	Perry	7	BWR
Ginna	6	PWR	Vogtle 1	3	PWR	Pilgrim	11	BWR
Haddam Neck	2	PWR	Vogtle 2	1	PWR	Quad Cities 1	3	BWR
Indian Point 2	4	PWR	Waterford 3	5	PWR	Quad Cities 2	2	BWR
Indian Point 3	3	PWR	Wolf Creek	4	PWR	River Bend	19	BWR
Maine Yankee	5	PWR	Yankee Rowe	3	PWR	Shoreham	2	BWR
McGuire 1	14	PWR	Zion 1	8	PWR	Susquehanna 1	5	BWR
McGuire 2	5	PWR	Zion 2	4	PWR	Susquehanna 2	4	BWR
North Anna 1	12	PWR	Doel 1	1	벨기에, PWR	Vermont Yankee	6	BWR
North Anna 2	13	PWR	Golfech 1	1	프랑스, PWR	WNP 2	16	BWR
Oconee 1	1	PWR						
	PWR		BWR	총 계				
발전소 수	79		39	118				
총 발생건수	422		203	625				

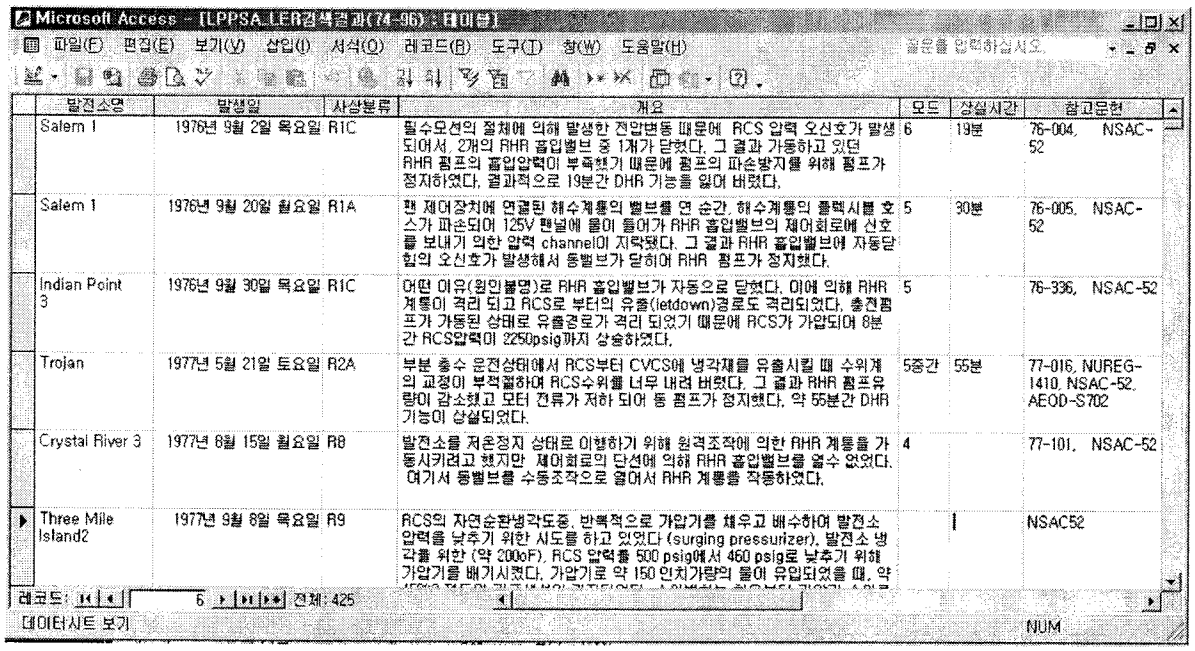


그림 3-63 정지/저출력 경험 자료의 DB 예시 화면

나. 정지/저출력 초기사건 DB 검색 및 분석 프로그램 개발

구축된 정지/저출력 초기사건 DB를 바탕으로 사용자의 다양한 사건/사고의 검색 및 분석 요구 조건들을 고려하여 DB 검색 및 분석 프로그램, LEDB (Low power and shutdown Events DataBase), 을 개발하였다. LEDB 프로그램은 MS 사의 Visual Basic 프로그램을 이용하여 Windows 환경에서 작동하는 전산프로그램으로, 정지/저출력 운전 중 발생한 사건/사고 경험 자료를 추가 입력 가능하고 사용자의 요구 조건에 따른 자료의 검색 및 분석을 지원한다. LEDB 프로그램의 개략적인 구조는 그림 3-64과 같으며, 정지/저출력 사건 정보는 그림 3-63의 MS Access 데이터베이스와 연결된다.

LEDB 프로그램의 개발 과정에서의 주요 결과물은 다음과 같다.

○ LEDB 프로그램 개발을 위해 사용자 및 프로그램의 기능에 대한 요건을 먼저 작성하였다 (표 3-29 참조).

○ LEDB 프로그램의 구조 설계는 간단히 2단계 구조의 모듈로 구성되며, 상위 모듈의 구성항목은 발전소 일반정보와 사건 정보, 사고 분석용 정보, 사용자 및 데이터 관리 정보로 구성하였고, 하위 모듈의 구성 내용은 다음과 같다 (그림 3-65 참조).

- 발전소 일반 정보 : 발전소 개요, 핵연료 주기정보, 정지/저출력 운전 정보
- 사건 정보: 사고 이력에 대한 상보와 사고 이력 출처에 대한 정보
- 사고 분석 정보 : 분석된 정보로 POS에 대한 분류정보, 사고 원인에 대한 분류 정보, 초기사건 유형에 대한 분석 정보, 사고분류체계 정보
- 사용자 및 데이터 관리 정보: DB 관리를 위한 모듈

○ LEDB 프로그램은 미리 저장된 사고정보에 따라 사용자가 필요한 분석 결과를 얻기 위하여 기본적으로 입력되어 있는 검색 조건의 조합을 사용할 수 있게 하였으며 이러한 검색 조건에 대한 내용은 표 3-30과 같이 발생호

기, 발생일, 발전소 유형, 제작사, 발전소 Type, 초기사건을 분류용 상세 분류 코드 (대, 중, 소분류별 코드), 근본 원인, 사고 개요, 운전 모드, 발전소 운전 상태 (POS), 정지 냉각 상실 시간, RCS 온도 상승, 자료 수집에 이용된 자료원 및 기타 항목으로 구성된다.

표 3-29 LEDB 프로그램의 개발 요건

상위요건	구현 내용	하위 요건	내 용
사용자 요건	전문가로 한정		
기능 요건	주요 사건의 상세 분석 지원 및 이해증진	사건원인 파악	사건에 대한 분석으로 파악된 사건원인 Index 지정
		사고원인 추적	검색기능 구현
		사고원인 분석	사고 원인별 분류 기능 구현
		사건유형 분류	사고 유형별 분류 기능 구현
		사건방지 대책 수립	사고 유형별 핵심적인 방지 대책 검토 기능(상세 자료 검색기능)
		사건방지 대책 추적	사고 방지 대책의 요약 및 검색 기능
	정지/저출력 위험도 분석에 이용	효율적인 정지/저출력 위험도 분석 지원	위험도 분석용 GUI 구현
		POS 분석 지원	POS 분류 체계 수록
		다양한 운전유형의 분류 및 통합	발전소별 운전 유형의 통합
		초기사건 분석 지원	초기사건 기인자에 대한 분류 기능
		초기사건 기인자 추적	초기사건 기인자에 대한 검색 기능
		초기사건 유형 분류	초기사건 유형 분류 기능 구현
		사고진행과정 분석 지원	Option
		사고경위 분석 지원	Option
	종합적인 위험도 분석 지원 (Option)	위험도 분석 및 위험도 정보 활용	
		대표적인 사건을 지정 기능 구현	

표 3-30 LEDB 프로그램에서의 자료 검색 조건

검색키워드	의미
일련번호	데이터베이스에 저장된 사건정보의 일련번호
발전소명	사건 발생 원전 명
발생일	사건 발생일
발전소형태	원전 유형 (PWR, BWR, etc)
NSSS제작사	원전 설계 회사
대분류	사건 유형 대분류 기호
중분류	사건 유형 중분류 기호
소분류	사건 유형 소분류 기호
근본원인	사건 근본 원인 분류 기호
개요	사고 개요
모드	사고 발생시 운전 모드
POS	사고 발생시 발전소 운전 상태
정지냉각상실시간	정지냉각 기능 상실 시간 (option)
RCS온도상승(F)	냉각 기능 상실시 RCS 온도 상승 (F) (option)
RCS온도상승	냉각 기능 상실시 RCS 온도 상승 (C) (option)
참고문헌	사건 정보의 출처
기타	기타의 특이 사항 수록 (option)
비고	
첨부	첨부 파일 (option)

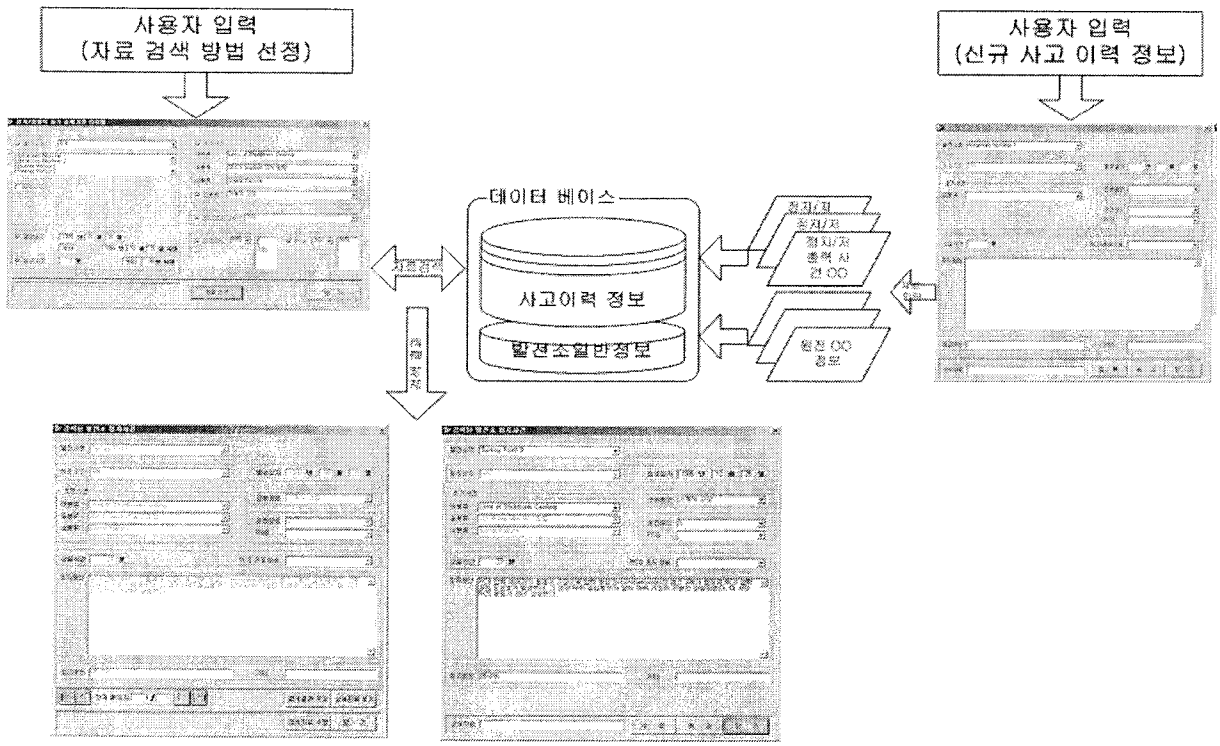


그림 3-64 LEDB 프로그램의 개요

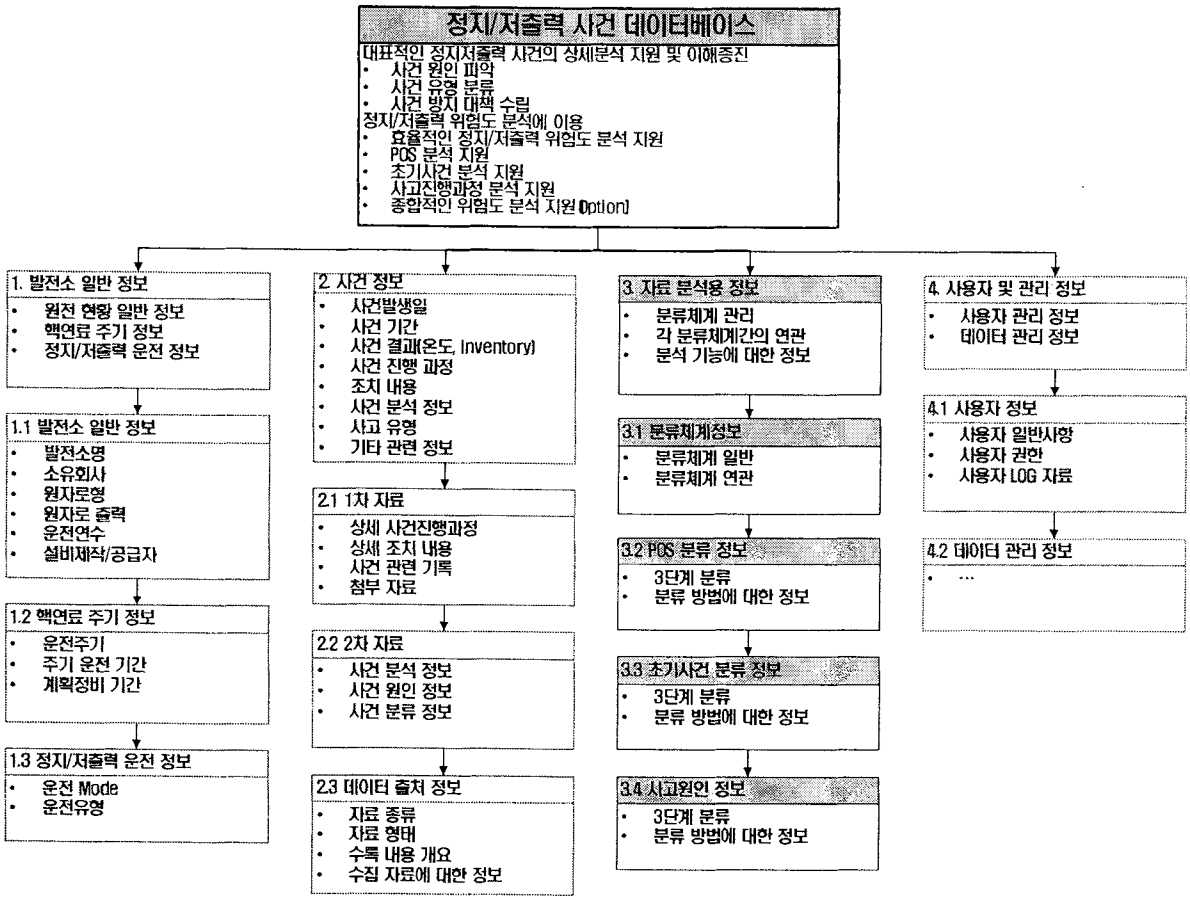


그림 3-65 LEDB 프로그램의 상세 구성도

다. 정지/저출력 초기사건 DB 상세 분석

정지/저출력 PSA 초기사건 분석 분야의 등급 개선과 정지/저출력 운전 중 유사 사건 발생을 막기 위한 목적으로 구축된 DB 검색 및 분석 프로그램(LEDB)을 이용하여 정지/저출력 초기사건 경험 자료에 대한 상세 분석을 수행하였다. 1973년부터 1999년까지 정지/저출력 운전 중 발생한 사건/사고 자료를 보면, 가압 경수형 원전(PWR)의 경우 79개 호기에서 422건, 비등 경수형 원전(BWR)의 경우 39개 호기에서 203건으로 총 625건의 자료가 데이터베이스에 수록되어 있으며, 여기에는 국내 자료 2건과 유럽 원전의 11개 사건 발생 건수가 포함되어 있다. 일부 자료들의 경우 자료원에서 사건 설명이 충분하지 않아 모든 검색 조건에 대한 자료의 분류가 이루어 질 수 없기 때문에 관심의 조건에 따라서는 해당 자료의 개수가 달라짐에 유의하여야 한다. 특히 각 원전의 운전 년수 및 계획 정비 이력에 관한 자료가 없어 초기사건 발생 빈도 평가는 불가능 하였다.

먼저, PWR과 BWR과의 발전소 수와 사건수를 상호 비교해 볼 때 유사한 사고발생 분포를 보이고 있어 발전소 형태에 따른 사건 발생 빈도 차이는 없는 것으로 판단된다. 각 초기사건별 사고이력은 표 3-31에 나타낸 것처럼 PWR과 BWR 모두 정지냉각 상실 사고가 가장 많이 발생했으며 발생 건수별로는 과도사건, 기타 및 LOCA 순으로 나타났다. 보다 세부적인 초기사건 분류 항목별로 경험한 사건/사고 건수를 PWR과 BWR로 나누어 표 3-32에 정리되어 있다.

표 3-31 노형별 초기사건 그룹의 발생 현황 비교

	정지냉각 상실 (LOSC)	냉각재 상실 (LOCA)	과도사건 (GTRN)	기타사건 (ETC)	총계
PWR	183 (43.4%)	28 (6.6%)	114 (27.0%)	97 (23.0%)	422 (100%)
BWR	119 (58.6%)	16 (7.9%)	46 (22.7%)	22 (10.8%)	203 (100%)
총계	302 (48.3%)	44 (7.0%)	160 (25.6%)	119 (19.1%)	625 (100%)

표 3-32 노형별 초기사건 분류 및 발생 현황

대분류	중분류	소분류	PWR		BWR	
			건수	총계	건수	총계
정지냉각 상실 사건	흡입밸브 닫힘	오신호	36	68	57	92
		전기기기고장	16		26	
		기타	16		9	
	공기흡입	수위조절실패	38	60	0	2
		냉각재상실	10		0	
		RCS 가압	2		0	
		정지냉각유량증가	5		2	
		기타	5		0	
	정지냉각계통 고장	정지냉각 펌프고장	15	55	1	25
		열교환기 고장	3		0	
		강제정지	7		0	
		기타 기기 고장	14		3	
		오신호	5		10	
		기타	11		11	
냉각재 상실 (LOCA)	냉각재 상실		27	28	15	16
	증기발생기 세관 파열		0		0	
	저압경계부 냉각재상실사고		1		1	
과도사건 (GTRN)	일반과도사건		33	114	9	46
	소외전원 상실사고		12		6	
	발전소 정전사고		0		0	
	4.16kV 모선 전원 상실사고		41		10	
	직류모선 전원상실 사고		3		1	
	필수모선 전원상실사고		14		11	
	기기냉각수 및 필수냉각수 상실 사고		4		1	
	공기조화계통 상실사고		0		2	
	압축공기 상실사고		0		0	
	480V 모선 및 전동기 제어반 전원 상실사고		7		6	
기타	반응도 사고		59	97	9	22
	저온과압사고		8		0	
	정지냉각기동실패		12		7	
	기타		18		6	
총계			625		203	

PWR에서의 정지냉각 상실 사건은 발생건수로는 흡입밸브 닫힘, 공기흡입 및 흡입밸브를 제외한 정지냉각 계통의 고장 순으로 나타났다. 흡입밸브 닫힘으로 인한 정지냉각 상실 사건은 흡입밸브와 관련된 LTOP 방지 기능과 저압 재순환 관련 신호들의 오동작이나 발전소 정비 중에 각종 신호관련 시험이나 정비 등을 수행하던 중에 운전원의 오류로 인한 사건 발생이 주요 원인인 것으로 나타났다. 공기흡입으로 인한 정지냉각 상실 사건은 원자로냉각재 저수위이나 부분 충수 운전

중에 수위조절 실패로 인하여 운전 중인 펌프가 공기를 흡입하는 사건이 주요원인으로 나타났다. 그 외 정지냉각계통의 고장은 정지냉각 펌프의 고장과 흡입밸브를 제외한 유량조절 밸브 등의 고장이 주요원인으로 나타났다.

BWR에서의 정지냉각 상실 사건은 발생건수로는 흡입밸브 닫힘, 정지냉각 계통의 고장 및 공기흡입 순으로 나타났다. 흡입밸브 닫힘으로 인한 정지냉각 상실 사건은 PWR과 동일하게 흡입밸브와 관련된 재순환 관련 신호들의 오동작이나 발전소 정비 중에 각종 신호관련 시험이나 정비 등을 수행하던 중에 운전원의 오류로 인한 사건 발생이 주요 원인으로 나타났으며, 특히 격납용기의 격리신호 오동작으로 인한 사건이 많았다. 그 외의 사건들은 PWR과 비교하여 발생 건수가 적었다.

그리고 냉각재 상실사건, 과도사건 및 기타 사건에 대한 분류 결과는 표 3-32에 나타난 것과 같이 출력 운전 중에 발생하는 고전적인 개념의 냉각재 상실 사건이 아닌 정지운전 중에 각종 보수 작업 중에 운전원 오류나 절차서의 미비 등으로 인하여 원자로 냉각재가 재장전수 탱크(RWT) 혹은 격납건물 집수구(sump)로 전이되는 되는 사건 등이 대부분이었다. 본 분석에서는 냉각재 상실사건을 LOCA, 증기발생기 세관파열 및 저압 경계부 냉각재상실(Interfacing LOCA) 세 가지의 중분류 항목으로 나누어 분석을 수행하였다.

PWR 자료의 검토 결과 총 28건의 LOCA 사고 중에 27건은 정비수행 중에 원자로 냉각재가 상실되거나 타 계통으로 전이되는 사고로 이 항목으로 분류된 사건들은 상실된 냉각재를 안전주입계통 등을 이용하여 회수가 가능한 사고들이었다. 저압 경계부 상실로 분류된 LOCA 사고는 정지 중 RCS에 연결되어 운전 중인 정지냉각계통(SCS)이나 화학 및 체적제어계통 (CVCS)의 배관 파열 등으로 인한 사고로 격납건물 밖으로 상실된 냉각재를 회수할 수 없는 경우였다. BWR 경우 PWR과는 유사하게 15건은 LOCA로 분류하였고 1건은 저압경계부 상실로 분류되었다. 발전소 저출력 및 정지 운전 중에 발생한 증기발생기 세관파단 사고는 본 보고서를 위한 수집 자료에서 없었으나 최근 국내 표준원전(울진 2발)에서 경험한 바 있다.

과도사건은 PWR이 BWR보다 사건 발생 건수 면에서 많은 이력을 보이고 있으며 발전소 정지 중 각종 정비 작업 중에 전기 공급 계통의 상실로 4.16kV 모선과 120V 필수 안전 모선의 상실 사건이 많이 발생 한 것으로 판단된다. PWR 이력에서는 공기 조화 계통의 상실과 압축공기계통의 상실로 인한 과도사건 발생은 없었으며 BWR 이력에서는 압축 공기 상실로 인한 과도사건 발생은 없었다.

수집된 자료들을 이용하여 사고 발생 시점을 국내 표준에 대한 정지/저출력 PSA에서 분석된 발전소 운전 상태(POS)를 기준으로 정리하였으며 결과는 표 3-33에 정리된 바와 같다. 앞서 언급된 바와 같이 수집된 자료들의 사건 내용에 관한 기술이 부족하여 모든 자료에 대한 POS 분류는 불가능하였으며, PWR 120건과 BWR 17건 만이 POS 분류가 가능하였다. 여기서는 편의상 BWR 자료를 제외한 PWR에 대한 POS별 사건 발생 건수 분석 결과를 보여주며, 부분 충수 운전 상태인 POS 5에서의 정지 냉각 상실 사건이 가장 많은 것으로 판단되었다.

표 3-33 발전소 운전상태(POS)별 사건발생 건수

POS	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	**총 계**
정지냉각 상실사건	N/A	N/A	4	4	47	3	0	2	0	3	2	2	1	N/A	N/A	68
냉각재 상실사건	0	0	0	1	0	0	0	0	0	0	0	0	1	2	0	4
과도사건	4	5	2	2	5	2	1	1	0	0	0	0	1	1	3	27
기 타	2	9	6	1	0	0	0	0	0	0	0	0	0	3	0	21
총계	6	14	12	8	52	5	1	3	0	3	2	2	3	6	3	120

수집된 자료에 대한 원인별 분석은 정지/저출력 초기사건의 재발 방지 및 위험도 저감을 위해 매우 중요하다. 수집된 625건의 자료에 대해 표 3-34와 같이 DB 검색의 편의성을 고려하여 미리 정한 사건/사고의 원인별 분류체계에 따라 원인별 분석을 수행하였다. 분류가 가능한 경험 자료만을 대상으로 수행한 전반적인 사건/사고의 근본 원인별 분석 결과는 표 3-35에 주어져 있다. 그 결과 운전원 오류 (절차서 오류 및 미흡 포함)로 인한 사고 발생 건수가 가장 많은 것으로 나타났다.

표 3-34 사고원인별 분류 체계

종류	대분류	중분류	소분류
직접원인	공기흡입 (와류)	수위저하	
		유량 증가	
		RCS 가압	
		냉각재 상실	
		기타	
	흡인밸브 막힘	오신호	
		기타	
		미확인	
		펌프 고장	
		전기기기의 이상	
		기타	
	열교환기 고장		
	흡입라인열림고장		
	강제 정지		
	흡입밸브외 고장		
	기타		
근본원인	인적요인	절차서 미비	
		운전원/작업자 오류	
		절차서 미비 + 운전원/작업자 오류	
	기기고장	수위계 이상	
		타 기기 이상	
	인적요인+ 기기고장		
	미확인		
	기타		

표 3-35 사고 원인별 사건 발생 건수

발전소 유형	PWR		BWR		총 계	
	사건 수	백분율	사건 수	백분율	사건 수	백분율
수위계고장	34	10.46%	-	0%	34	7.07%
기계적고장	79	24.31%	33	21.15%	112	23.29%
운전절차오류	155	47.69%	81	51.93%	236	49.06%
기타 건수	57	17.54%	42	26.92%	99	20.58%
SUM	325	100%	156	100%	481	100%

특히, 비교적 자료의 정확성이 높다고 판단되는 미국의 LER 자료를 기준으로 미국 원전에 대한 잔열 제거 계통 (표준원전의 경우 정지냉각계통에 해당됨)의 이상 사건 (1976~1990; 197건)에 대하여 기능 상실의 원인별 분석을 상세히 수행하였다. 그 결과, 직접적인 원인으로는 흡입밸브의 닫힘 (35%), 와류(28%), 기계적 고장 (18%)의 순으로 나타났으며, 근본원인으로는 운전원/작업원 오류, 절차서 부족 또는 이 둘의 결합된 원인이 전체의 60%이상을 차지하는 것으로 나타났다 (그림 3-66 및 그림 3-67참조). 이에 대한 보다 자세한 정보는 표 3-36에 기술되어 있다.

표 3-36 미국의 정지냉각 상실사고에 대한 사고원인별 분석

근본원인		인적요인				장치고장			인적요인 + 기기고장	원인 불명	기타	합계
장치원인		절차서 부족	운전원/작업원 오류	절차서부족 +인적오류	소계	수위계 고장	타 기기 고장	소계				
공기 흡입 (와류)	수위 저하	6	6	4	16	15		15		1		32
		0(6)	0(6)	0(4)	0(16)	0(15)		0(15)		0(1)		0(32)
	정지냉각 유량	4		1	5			0				5
		0(4)		0(1)	0(5)			0(0)				0(5)
	RCS 가압	3	1		4			0				4
		0(3)	0(1)		0(4)			0(0)				0(4)
	RCS 재고량 상실	2	4		6			0	1			7
		0(2)	1(5)		1(7)			0(0)	0(1)			1(8)
	기타	1			1		0	0				1
		1(2)			1(2)		1(1)	1(1)				2(3)
	소계	16	11	5	32	15	0	15	1	1	0	49
		1(17)	1(12)	0(5)	2(34)	0(15)	1(1)	1(16)	1(1)	1(2)	0(0)	3(52)
흡입밸브 닫힘	오신호의 발신	1	0	0	1	0	0	0		1	0	2
		19(20)	23(23)	4(4)	46(47)	1(1)	10(10)	11(11)		2(3)	5(5)	64(66)
	기타				0			0				0
					0(0)			0(0)				0(0)
	원인 불명				0			0		0		0
					0(0)			0(0)		2(2)		2(2)
	소계	1	0	0	1	0	0	0	0	1	0	2
		19(20)	23(23)	4(4)	46(47)	1(1)	10(10)	11(11)	0(0)	4(5)	5(5)	66(68)
기계적 고장	펌프 고장				0		1	1	0			1
					0(0)		1(2)	1(2)	1(1)			2(3)
	기기 고장	0	4		4		0	0		0		4
		5(5)	8(12)		13(17)		1(1)	1(1)		2(2)		16(20)
	기타	1	0	0	1		0	0	0			1
		2(3)	1(1)	3(3)	6(7)		2(2)	2(2)	1(1)			9(10)
	소계	1	4	0	5	0	1	1	0	0	0	6
		7(8)	9(13)	3(3)	19(24)	0(0)	4(5)	4(5)	2(2)	2(2)	0(0)	27(33)
정지냉각 열교환기 고장		0	0		0		0	0		0		0
		1(1)	2(2)		3(3)		3(3)	3(3)		3(3)		9(9)
정지냉각 흡입밸브 개방실패					0		0	0		0		0
					0(0)		6(6)	6(6)		1(1)		7(7)
정지냉각계통 강제정지		0	1		1		1	1		0	0	2
		2(2)	8(9)		10(11)		2(3)	2(3)		1(1)	1(1)	14(16)
흡입밸브외 밸브고장		0	1		1		0	0		0		1
		2(2)	3(4)		3(4)		3(3)	3(3)		1(1)		7(8)
기타		0	0	0	0		1	1				1
		2(2)	1(1)	1(1)	2(2)		1(2)	1(2)				3(4)
합계		18	17	5	40	15	3	18	1	2	0	61
		30(48)	47(64)	8(13)	85(125)	1(16)	50(33)	31(49)	2(3)	12(14)	6(6)	136(197)

※ 각 셀의 상단 : 부분충수 운전시의 사건수, 하단 : 만수위 운전시의 사건수, ( ) : 총사건수

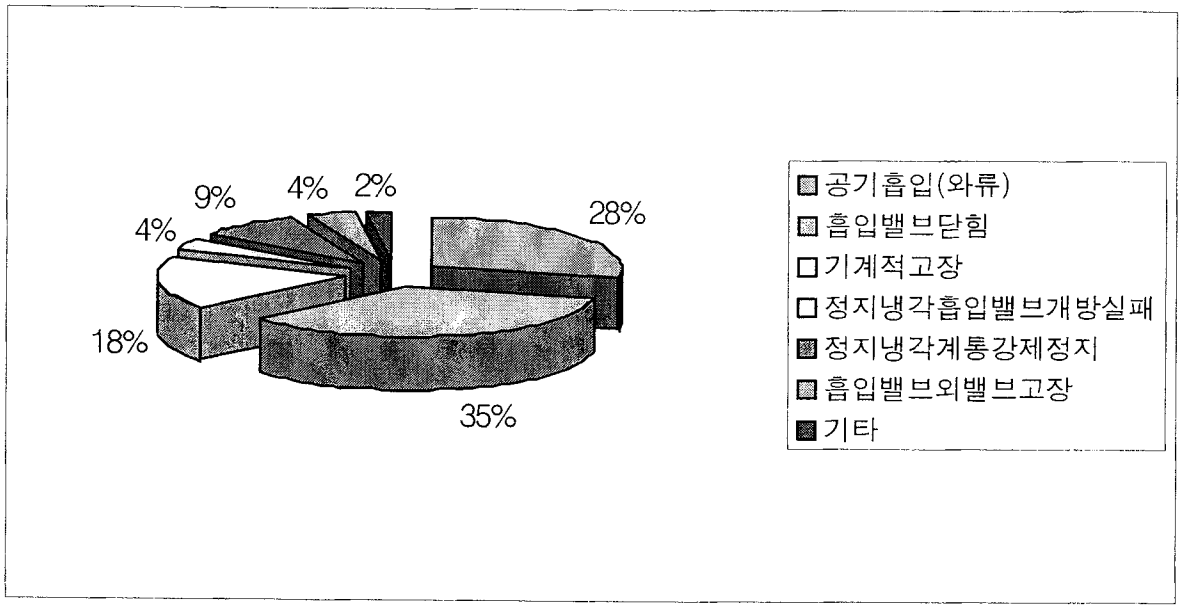


그림 3-66 미국의 정지냉각 기능상실 사건에 대한 직접 원인별 분석

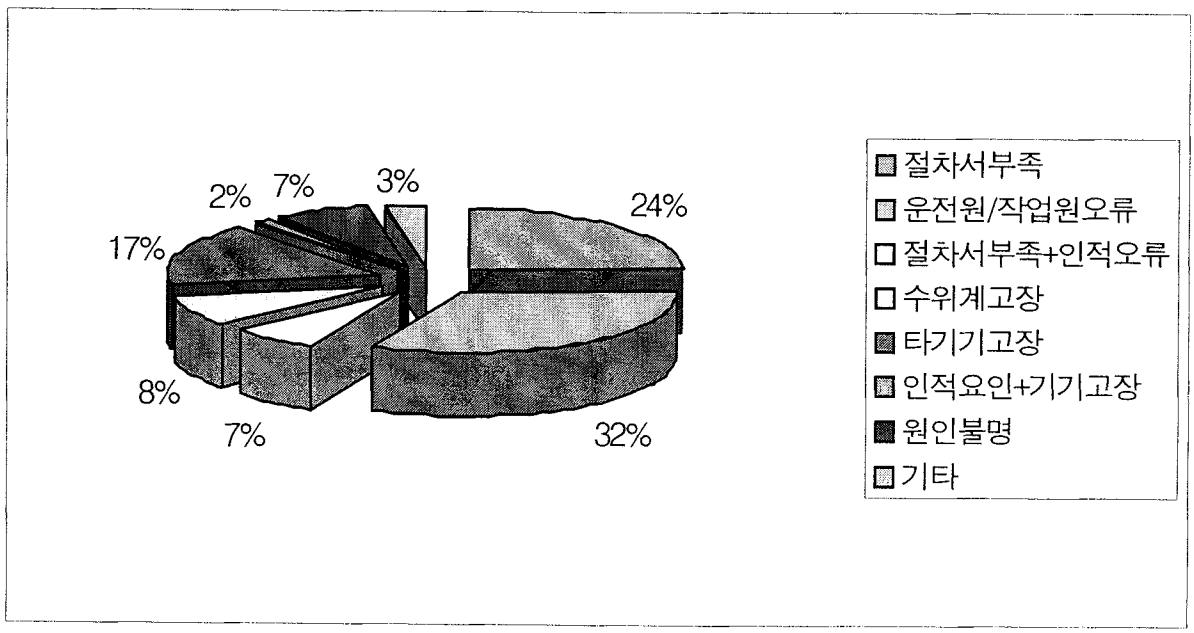


그림 3-67 미국의 정지냉각 기능상실 사건에 대한 근본 원인별 분석

수집된 자료 가운데 정확한 연도 추적이 가능한 444건의 정지/저출력 운전 중 발생한 초기사건에 대하여 발전소 호기당 연도별 발생 건수는 그림 3-68과 같다. 대개 80년대 초반에는 2년에 1회, 80년대 후반 들어서는 3년에 1회 정도의 정지냉각계통의 기능상실을 경험하는 것으로 나타났으며, 이는 80년대 후반부터 부분 충수 운전에 대해 세계 각국의 규제기관들이 취한 안전 강화 조치 (미국의 경우 GL 88-17; 1988년초 발간)에 의해 동일 사고 유형의 발생이 줄어든 효과로 판단된다.

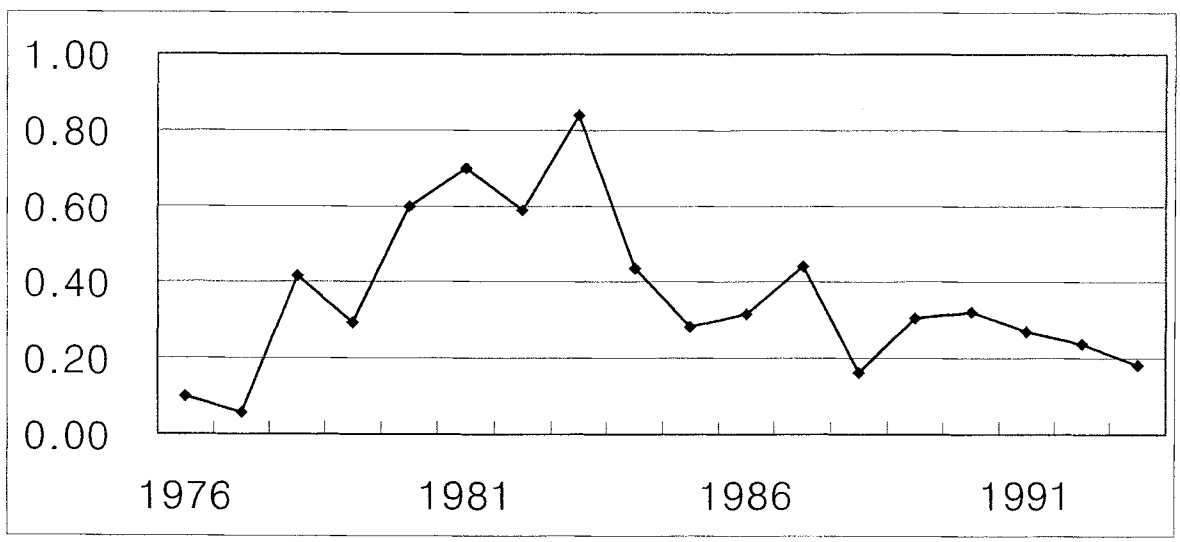


그림 3-68 연도별 원전 호기당 평균 정지냉각계통의 기능상실 사건 발생 횟수

본 과제에서 개발한 정지/저출력 초기사건 DB 및 DB 검색/분석 프로그램 (LEDB)는 정지/저출력 운전의 안전성 확보를 위해 유용한 도구로 사용될 수 있으며, 향후 국내 원전의 정지/저출력 PSA 수행 시 초기사건 도출에 많은 도움을 줄 수 있을 것으로 판단된다. 하지만, 경험 자료에 의한 초기사건 발생빈도 평가를 위해서는 외국 원전의 운전 및 정지 이력과 같은 자료가 보강되어야 할 필요가 있다. 또한, 국내 원전에서 발생한 정지/저출력 운전모드에서의 이상 사건/사고로 DB에 포함된 공식적인 사건은 단 2건 뿐이다. 이는 현재의 국내 실정상 정지/

저출력 이상 사건에 대한 보고 체계의 확립되어 있지 않아 원전 사업자가 보고해야할 법적 의무를 가지고 있지 않은 결과로서 국내 원전에 대한 정지/저출력 운전에서의 이상 사건/사고 분석은 현재 상태로서는 불가능한 상태에 있다. 따라서, 향후 국내 발전소 고유의 경험 자료에 초기사건 분석이 이루어 지기 위해서는 미국의 LER과 같은 법적 보고 또는 관리 체계를 갖추는 것이 매우 시급한 것으로 판단된다.

2. 정지/저출력 위험도 관리 모델 시범 개발

일반적으로 원자력 발전소에서의 위험도 관리라 함은 기기 배열의 변화에 따른 위험도 프로파일 (risk profile)의 관리를 의미하며, 정지/저출력 PSA 분야에서는 이를 일반적으로 기기 배열 위험도 관리 (CRM; Configuration Risk Management)라고 부른다. CRM 모델의 개발 목적은 정지/저출력 운전 중 특정 기간 내에 위험도가 집중되는 것을 사전에 피하기 위함이다. 특히, 핵연료 재장전을 위한 계획 정비 기간에는 다양한 발전소 운전 상태(POS)와 수많은 정비활동으로 인하여 기기 배열 상태도 매우 다양하게 변화하므로 정지/저출력 위험도 저감을 위해서는 CRM 모델의 개발이 매우 중요하다.

본 단계에서 효율적인 CRM 모델 개발을 위하여 필요한 기반 기술을 확보하는데 주력하였으며, 이에 따라 수행된 내용은 1) 정지/저출력 기기배열 위험도 관리 모델의 개발방향을 결정하고, 2) 결정된 개발 방향에 따라 발전소 운전 상태(POS) #1 (계통 병해에서 원자로 정지)을 포함하는 운전모드 #1 (출력운전) 과 운전모드 #2 (기동)에 대한 CRM 모델을 시범 구축하였다. 본격적인 CRM 모델 개발은 대과제내 세부과제들 간의 연계 사항으로 인하여 3단계 (2005.3 - 2007.2) 중장기 연구에서 계통 모델 개선과 함께 이루어질 계획이다.

가. 정지/저출력 위험도 관리 모델 개발 방향 정립

효율적인 정지/저출력 위험도 관리를 위해 가장 먼저 결정해야할 사항은 "어떠한 형태의 모델이 CRM에 바람직한가?"에 대한 질문에 답하는 일이다. 이와 같은 정지/저출력 CRM 모델의 개발 방향을 결정하기 위해서 본 과제에서는 수행한 내용은 다음과 같다.

○ 현존하는 정지/저출력 위험도 평가 모델 유형 조사

○ CRM 모델로의 적합성 검토 및 모델 선정

현재까지 사용되고 있는 정지/저출력 위험도 평가 방법에는 정성적 방법과 정량적 방법으로 크게 나눌 수 있으며, 다시 각 방법에서 2개씩의 모델로 구분되어 다음과 같이 총 4가지 평가 모델로 압축될 수 있었다 (표 3-37 참조).

○ DID (defence-in-depth) 모델

○ 단순 위험도 정량 평가 방법이 추가된 DID 모델

○ 위험도 감시 모델

○ 전통적인 PSA 모델

이들 모델의 장·단점 비교 분석을 통하여 다음과 같은 기준으로 CRM에 가장 적합한 모형을 선정하였다.

○ 적용 대상 발전소에 대한 전통적인 정지/저출력 PSA 모델의 유무 및 모델의 상세 정도

○ CRM 이외에 다른 위험도 정보 활용 분야로의 확장성

○ 모델별 현재의 기술 수준

○ 개발 비용 대비 효과

이로써, 최종적인 CRM 모델 개발 방향 설정 결과는 현재 전통적인 정지/저출력 PSA 모델이 있는 표준원전을 대상으로 할 경우, ① 정량적 CRM 모델, ② 일주기(one-cycle) 위험도 감시 모델 형태로 향후 위험도 정보 활용 분야로의 확대 적용이 가능한 다목적용 모델을 개발하는 것으로 결정하였다 (표 3-37 참조). 또한, 일주기 위험도 감시 모델 형태의 CRM 모델은 향후 발전소 현장 사용자의 편의성, 실시간 계산 능력, 모델의 유지 및 보수의 편리성 등을 고려하여 전통적인 표준원전 PSA 모델의 POS (17개)별 개발이 아니라 발전소 운전모드 - 예를 들면, 출력, 기동, 고온 대기, 고온 정지, 상온 정지, 핵연료 재장전 - 에 따라 총 6개의 통합 CRM 모델로 개발되는 것이 가장 바람직할 것으로 판단되었다.

표 3-37 기기 배열 위험도 관리 모델 개발 방향

접근방법	적용가능 모델 종류	특징	개발 현황
정성적 CRM	DID 모델 (예: ORAM)	1) LPSD PSA 모델이 없는 원전에 적용 가능 2) Opt. 2 (예: 차등품질보증(GQA))와 같은 타 응용분야에 적용불가 3) LPSD PSA 기술 개발 불필요	Diablo Canyon (1998), Calvert Cliffs(1998), **국내 중수로(현재 개발중)**
	DID+단순 위험도평가 모델 (예:ORAM-Sentinel)		
정량적 CRM	**주기별 위험도 감시 모델** (예: EOOS, SM 등) (국내의 경우 **DynaRM** (한원연), **RIMS**(한기))	1) **LPSD PSA 모델이 있는 원전** 2) PSA 모델 품질에 따라 가동중정비 (OLM), GQA와 같은 **다른 위험도 정보 활용 분야로 확대 적용 가능** 3) **LPSD PSA 기술 개발 병행 필요**	**정량적 CRM 적용사례 거의 없음**. 단, 위험도 감시 모델 및 **전통적 PSA 모델 개발 사례는 다수 (국내 표준원전 포함).**
	전통적 LPSD PSA 모델		

나. 발전소 기기배열 위험도 관리 (CRM) 모델 시범 구축

CRM 모델 개발 방향을 운전 모드별 일주기 발전소 기기배열 위험도 감시 모델로 결정함에 따라 본 과제에서는 운전모드 1과 2에 대한 CRM 모델을 시범 구축 및 평가를 통하여 3 단계 (2005.3-2007.2)에서 본격 개발될 CRM 모델의 기초 기술을 확보하고자 하였다. 이와 관련한 주요 연구 내용 및 결과는 다음과 같다.

○ 기존 표준원전 정지/저출력 PSA 모델에서의 발전소 운전 상태 (POS)와 발전소 운전 모드 간 연계성을 파악하였고, 그 결과는 다음과 같다.

- 운전모드 1 (출력운전) : 전출력 및 저출력 ,
- 운전모드 2 (기동) : POS #1 및 #15,
- 운전모드 3 (고온대기) : POS #2 및 #14,
- 운전모드 4 (고온정지) : POS #3 및 #13,

- 운전모드 5 (상온정지) : POS #4-#6 및 #10-#12 ,

- 운전모드 6 (핵연료 재장전) : POS #7-#9.

○ 시범 모델 구축 대상 범위인 운전모드 1 과 운전모드 2 에 대한 기기배열 상태를 표준정비계획에 따라 파악하였고, 그 결과 다음과 같이 8 가지 주요 기기 배열 상태를 분석 대상으로 선정하였다.

① 출력 급감발 계통 (RPCS; Reactor Power Cut-back System) 정지 (@60%출력),

② 주급수 펌프 1대 정지(@50%),

③ 복수펌프 정지(@30%),

④ 다중보호계통 (DPS; Diverse Protection System)의 터빈 트립 우회 (@25%),

⑤ 급수 밸브 전환 및 급수 차단 밸브 닫힘(@20%),

⑥ 주증기 복수기 우회 운전(@10%),

⑦ 터빈 정지 및 발전기 차단기 수동 개방(@5%-10%),

⑧ 기동 급수 펌프 기동 및 주급수 펌프 정지(@5%).

○ 표준원전 전출력 위험도 감시 모델로부터 수정하여 운전모드 1과 운전모드 2(POS#1)에 대한 기기 배열 위험도 평가용 시범 모델을 구축하였고, 이들로부터 운전모드 1과 2에 대한 주요 기기 배열 상태 변화에 따른 년평균 노심손상빈도(CDF) 및 대량조기방출빈도(LERF) 평가하였다. 평가 결과는 표 3-38에 주어져 있다.

표 3-38 운전모드 1 & 2에서의 기본 기기배열 위험도 평가 결과

운전 모드	기기배열 상태	위험도(/RY)		비고
		CDF	LERF	
모드 1	Base: 전출력운전 (@100%출력)	7.47e-6	1.26e-6	
	출력급감발계통 정지 (@60%)	7.52e-6	1.26e-6	
	주급수펌프 1대 정지 (@50%)	7.52e-6	1.26e-6	
	복수펌프 정지 (@30%)	7.52e-6	1.26e-6	
	다중보호계통 터빈 트립 우회 (@20%)	7.52e-6	1.26e-6	
	급수전환 및 차단밸브 닫힘 (@20%)	7.52e-6	1.26e-6	
	주증기 복수기 우회 운전 (@10%)	7.52e-6	1.26e-6	
모드 2	터빈정지 및 발전기 차단기 개방 (@5%-10%)	7.42e-6	1.26e-6	
	기동급수펌프 기동 및 주급수 펌프 정지(@5%)	7.41e-6	1.26e-6	

제 3 절 디지털 계통의 위험도 평가 기술 개발

원전의 계측제어 계통은 기존의 아날로그 회로로 구성된 원전 계측제어(I&C) 계통의 노후화로 열화와 품귀 문제가 점차 심각해지고 유지보수의 효율화, 편차(drift) 제거 등 저비용 고효율의 장점을 갖는 디지털 기술의 눈부신 발전에 따라 원전의 안전 기능에도 디지털 계측제어 계통으로 대체되거나 대체를 고려하고 있는 것이 세계적 추세이다. 이에 따라, 안전 기능에 적용되는 디지털 기기/계통에 대한 안전성 입증이 요구되나, 이를 위한 디지털 계통의 위험도 정량 평가 방법론은 국내외를 막론하고 초기 개발 단계에 있어 명확한 체계 및 방법론이 정립되어 있지 못한 상태이므로 매우 시급한 세계적 현안 문제가 되고 있는 실정이다. 특히, 국내에서는 울진 5,6 호기를 선두로 안전 관련 디지털 I&C 계통이 이미 도입되었으며, 이에 따라 안전 관련 디지털 기기/계통에 대한 정량적 안전성 평가 방법론 개발은 더욱 시급한 국내 현안 문제로 다룰 수밖에 없는 상황이다.

현재까지의 디지털 계통에 대한 안전성 평가는 계통 수준의 신뢰성 확인 및 검증을 위한 결정론적 방법에 의존하고 있으나, 규제 및 원전 사업자의 위험도 정보 이용 확대 추세에 따라 디지털 안전 계통의 원전 위험도 전반에 미치는 영향을 종합적으로 평가할 수 있는 정량적 위험도 평가 기술 개발을 서둘러야 한다. 하지만, 이러한 디지털 I&C PSA 분야는 디지털 기기의 특성상 기존 PSA 분야에서는 일반적으로 다루지 않았던 수많은 디지털 요소 - 예를 들면, 소프트웨어 신뢰도, 고장내구성(fault-tolerance) 기법의 고장 검출률, 통신망 신뢰도, 디지털 기기 신뢰도, 등등 - 들에 대한 평가 방법론들의 개발이 선행되어야 한다.

본 과제의 최종 연구 목표는 과제 제안 요구서(RFP)에 따라 2 단계 (2002. 4 - 2005. 2 ; 2년 11개월) 및 3 단계 (2005. 3 - 2007. 2; 2년)에 걸쳐 디지털 계측제어 계통의 위험도 평가 기술 개발에 있다. 이는 차세대 원전의 인허가 및 위험도 정보 활용 설계 개선 지원을 위해 대표적인 3개 계통 - 디지털 발전소 보호

계통 (DPPS), 디지털 공학적 안전설비 작동 계통 (DESFAS) 및 공학적 안전설비 기기제어 계통 (ESF-CCS) - 의 상세 신뢰도 평가 모형을 포함한 디지털 안전계통의 원전 위험도 영향 평가용 통합 모델 및 요소 기술의 개발하고, 이를 통한 디지털 PSA 기반 기술을 확보하는 것을 의미한다.

그림 3-69는 전반적인 디지털 I&C PSA의 연구 업무 범위 (2단계 및 차기 단계 수행 내용 포함)를 나타내는 것으로 디지털 계통의 위험도 평가기술 개발을 위한 연구는 크게 3가지 부분으로 구성될 수 있다. 디지털 안전계통 신뢰도 분석 모델 개발, 원전 위험도 평가를 위한 PSA 모델과의 결합을 통한 위험도 영향 평가, 개발된 모델이 보다 현실적인 표현력을 가질 수 있도록 하기 위한 디지털 안전-필수 (safety-critical) 요소 평가 기술 개발이다.

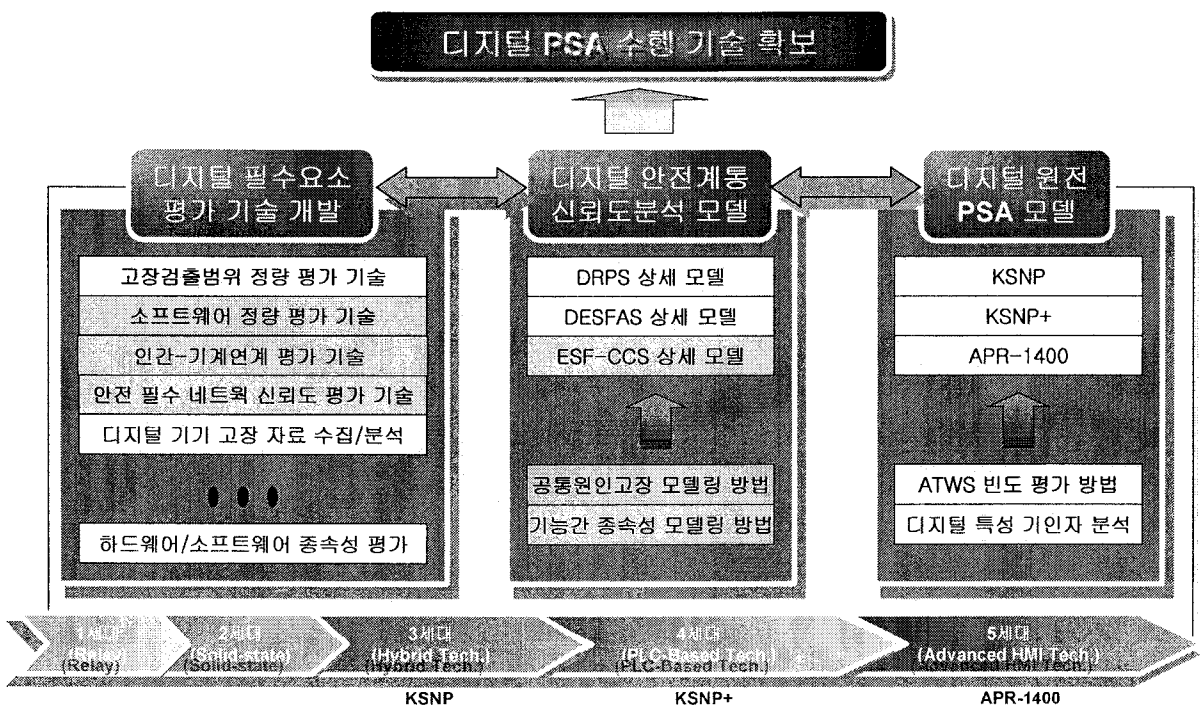


그림 3-69 디지털 I&C PSA 분야의 연구 방향 및 범위

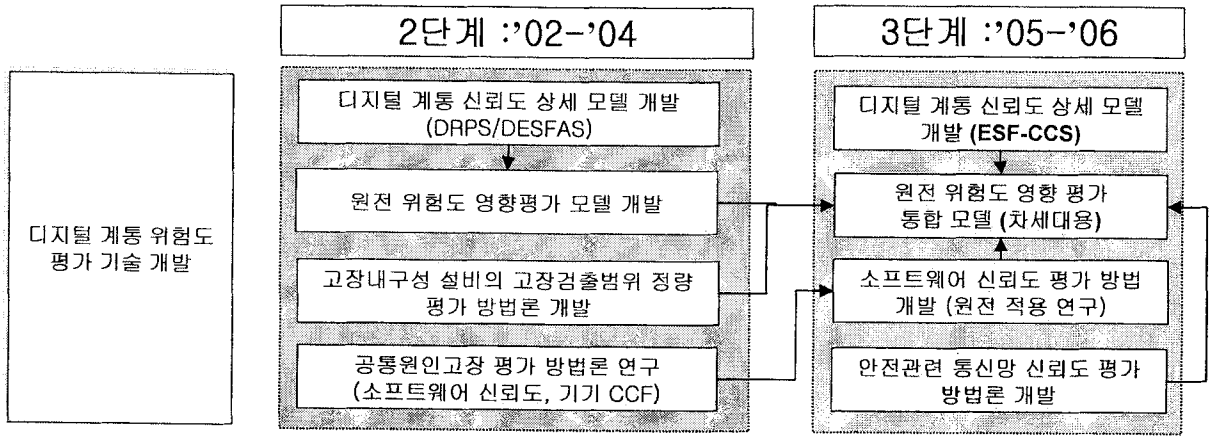


그림 3-70 디지털 I&C PSA 분야의 2단계 및 3단계 연구 흐름도

디지털 계통의 안전성 평가를 위한 기술의 개발이 기존에 거의 이루어져 있지 않았으므로 이를 고려하여 단계적으로 수행하는 것이 바람직하다. 그림 3-70에서 보듯이 본 과제에서는 먼저 디지털 안전계통의 신뢰도 평가 모델 개발을 위한 방법론 연구에서 출발한다. 디지털 계통의 경우 소프트웨어에 의한 다기능 구현, 기기간의 정보 공유, 고장내구성 기법의 활발한 채용, 몇 가지 기기로의 위험도 집중, 공통원인 고장의 중요성 부각 등에서 기존 아날로그 시스템 모델과 많은 차이점을 가진다. 또한 인간 운전원의 오류확률 산정에 정보 제공을 담당하는 디지털 기기의 건전성이 중요한 요인이 된다는 점을 고려하여 조건부 인간오류확률 평가 방법론을 개발하였다. 이러한 방법론에 따라 한국형 표준원전인 울진 5,6호기의 DPPS와 DESFAS의 고장수목을 작성하였다.

이렇게 개발된 고장수목 모델을 한국형 표준원전 플랜트 위험도 평가모델과 결합하여 발전소 전체의 안전성에 디지털 계통이 미치는 영향을 평가하고, 주요 인자에 대한 민감도 분석도 수행하였다. 평가결과 디지털 계통이 작동불능 상태에 빠지는 경우 플랜트의 안전관련 기능이 수행되지 못하여 플랜트 위험도에 큰 영향을 미치는 것으로 나타났다.

플랜트 위험도에 디지털 계통이 미치는 영향이 큰 것으로 평가됨에 따라 보

다 상세하고 정확한 분석이 필요하게 된다. 상세 분석을 수행하기 위해서는 주요 요소기술의 개발이 선행되어야 한다. 본 과제에서는 디지털 계통의 평가에서 가장 어려운 이슈로 부각되는 부분인 소프트웨어 결함의 정량적 평가를 위하여 BBN (Bayesian Belief Net) 기법을 이용한 신뢰도 평가 방법론을 개발하였으며, 디지털 기기에 적용되는 고장내구성 기법의 유효성 정량화를 위하여 우선 감시타이머의 고장 검출률 추정 모델을 개발하였다. 한편, 최대 16개까지의 다중성을 가지는 디지털 계통의 특성상 공통원인 고장의 평가가 매우 중요한 역할을 한다는 점을 고려하여, 공통원인고장 확률 추정을 현실적으로 수행하기 위한 방법론을 개발하였다.

1. 안전 관련 디지털 계통의 상세 신뢰도 모델 개발

디지털화로 인한 위험도의 집중을 고려하여 상세하고 현실적인 분석방법을 개발하고 이를 바탕으로 한국형 표준원전(KSNP)에 적용되는 디지털 계통의 모델을 개발하는 하는 것이 이 연구의 목표이다. 특히 가장 중요한 현안인 안전계통 디지털 시스템을 대상으로 연구를 수행하였다.

기능 수행의 복잡도와 안전성 분석 기술 미비를 고려하여, 모델링 기법 개발과 모델 개발을 병행하여 수행하면서 시급한 기술을 우선적으로 개발함으로서 모델을 보완하는 체계를 정립하였다[강현국, 2002c; 강현국, 2002e]. 디지털 기기에 대한 분석과 원전 안전성 분석을 결합하여 3,900여개의 기본사건과 7,000여개의 논리사건으로 구성된 상세 모델을 개발하고, 디지털의 특성에 맞는 분석 방법론들(운전원-기기 상호작용, 기기간 고장감시, 다중성 및 다기능성, 소프트웨어 오류, 초기사건별 종속성)을 개발하여 실제 적용하였다[강현국, 2002d].

상세한 표현력을 가지면서도 실용적인 모델을 개발하여 국내의 안전현안 문제 해결에 기여하고, 한국 전력 기술 주식회사(KOPEC) 및 한국 원자력 계측제어 시스템 개발단(KNICS)의 설계에도 반영되고 있으며, 국제적인 주목을 받고 있다[강현국, 2002b; 강현국, 2002g; 강현국, 2002f].

가. 안전 등급 디지털 계통의 설계 현황 분석

먼저 국내에서 진행 중인 여러 가지 디지털 안전 계통에 대한 설계 동향과 현황을 파악하였다. 현재 국내에서 진행 중인 설계 동향은 표 3-39와 같이 정리될 수 있다.

표 3-39 국내의 디지털 안전계통 설계 동향

설계안	특징	PSA기술개발요소
KSNPP DPPS/DESFAS	- 국내 최초의 원전 안전계통 디지털화 - 다수의 변수를 하나의 프로세서가 처리 - 다중 프로세서 구성 (동일 소프트웨어 탑재 동일 하드웨어) - 입력 모듈 및 메모리 공유 - 감시타이머 활용	- 소프트웨어 고장확률 평가 - 감시타이머 고장검출률 정량화 - 공통원인 고장 평가
APR1400 DPPS/ESF-CCS	- DESFAS와 PCS의 통합 - 안전기능 수행에 네트웍 활용	- 네트웍 안전성 평가
KNICS DPPS/ESF-CCS	- 프로세서 수 저감 (계통 단순화, 다중성은 감소) - 입출력 모듈 완전 2중화 - DESFAS와 PCS의 통합 - 안전기능 수행에 네트웍 활용 - 자동주기시험 기능 도입	- 자동주기시험 고장검출률 정량화
KOPEC DRPS Lab. ADRPS	- 다중성 및 다양성 극대화 (이기종 하드웨어, 이기종 OS, 이기종 소프트웨어) - 개방형 설계 (VME버스 기반)	- 이기종간의 종속성 평가

고장수목 작성을 위해서는 먼저 대상 계통에 대한 체계적인 설계 검토가 선행되어야 한다. 분석 대상인 한국형 표준원전의 DPPS와 DESFAS에 대한 상세 설계 분석을 수행하여 기능 구현을 위한 필수 요건 및 계통 구성을 파악하였다. DPPS는 측정 채널 또는 노심 보호 연산기(CPC)로부터 발생한 신호에 대하여 입력 모듈을 거쳐 정지 논리 프로세서 모듈에서 각 정지 변수별로 설정치에 도달하

였는지의 비교를 수행한 후, 다중 채널의 비교 결과를 동시 논리 프로세서에서 최종적인 정지 신호를 생성한다. 이 신호가 개시 회로로 전송되어 및 정지 회로 차단기 개방을 통하여 제어봉 구동 장치(CEDM)의 코일을 비여자(de-energized)시킴으로써 모든 제어봉들을 노심 하부로 떨어지게 함으로서 원자로 정지 기능을 수행하는데, 계측기부터 작동기(actuator)까지를 고려한 개념도는 그림 3-71과 같다 [강현국, 2003e].

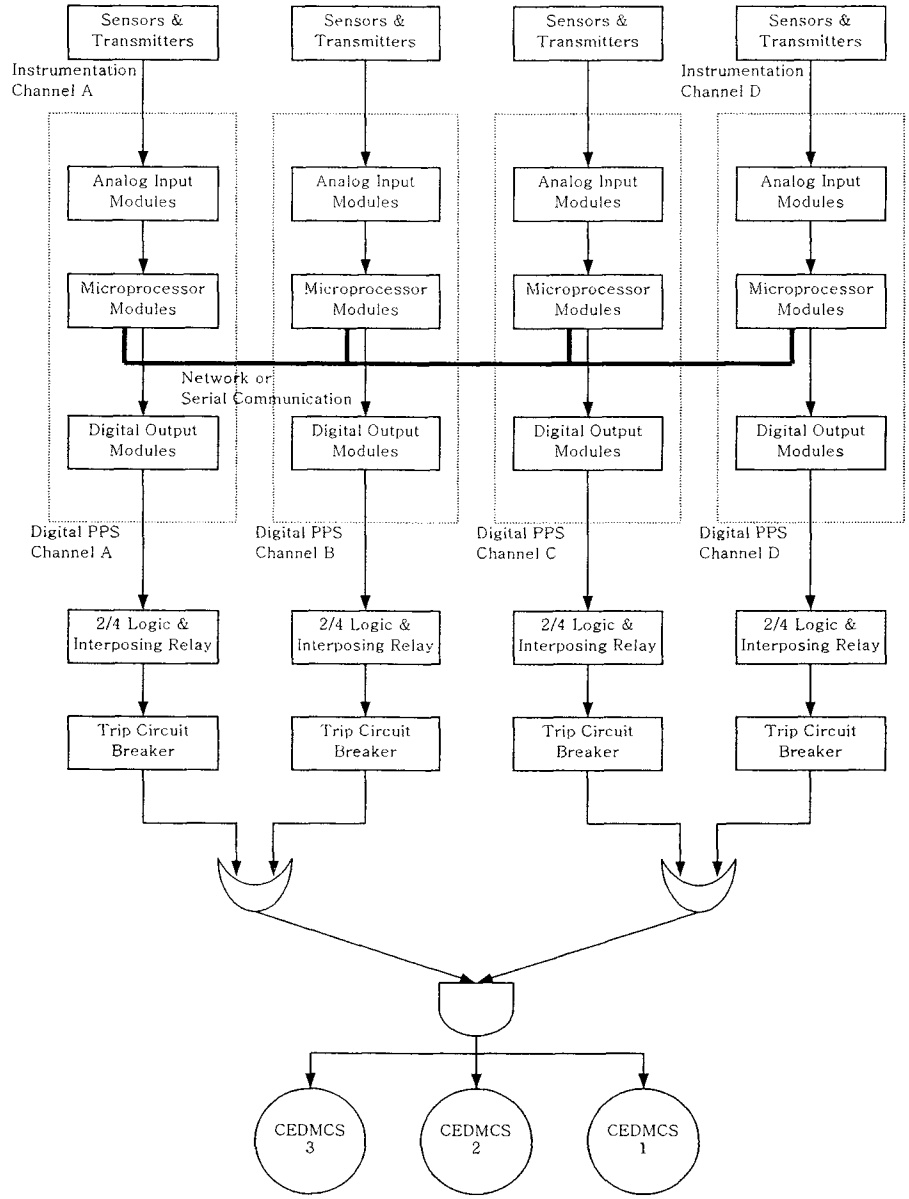


그림 3-71 한국형 표준원전 DPPS 구조 개념도

아래의 그림 3-72는 DPPS의 결선 및 내부 신호흐름을 개념적으로 도시한 것이다. 이러한 신호 흐름은 결국 계통의 고장 수목에 그대로 반영되게 되며 결선 내역까지 파악하는 이유는 공통 원인 고장에 의한 시스템 영향의 파급범위 산정을 위해 필요하기 때문이다.

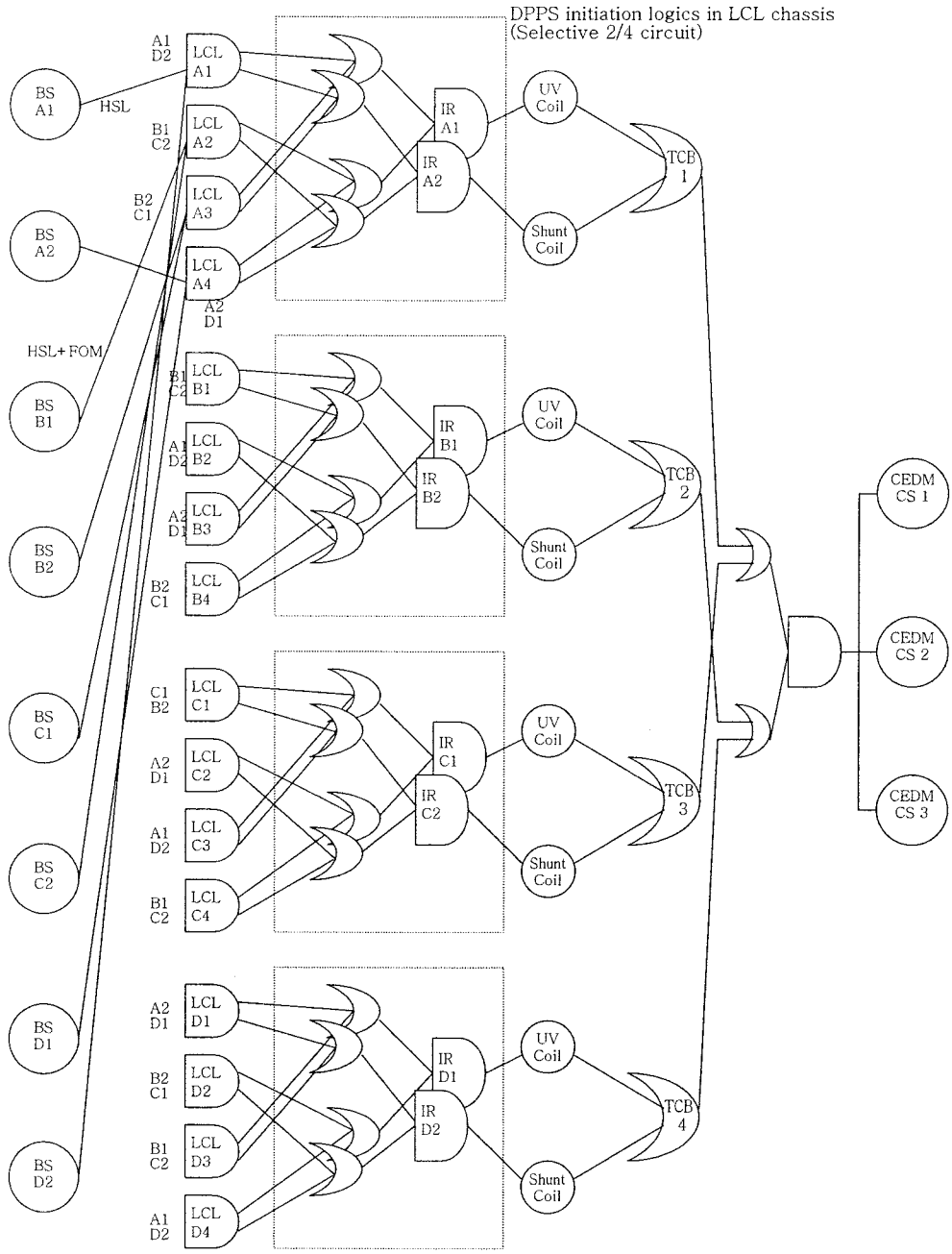


그림 3-72 한국형 표준 원전 DPPS 신호 흐름 및 결선 개념도

나. 디지털 원자로 보호계통의 상세 신뢰도 모델 개발

원전 PSA 모델에 직접 접목 가능한 디지털 안전 계통의 모델 개발을 목표로

하여 울진 5,6 호기 DPPS 고장수목을 개발하였다. 계통의 이용불능도(unavailability)를 평가하기 위해 몇 가지 참조 변수에 대해서만 모델을 구축하여 분석하여도 충분하지만, 실제 원전 PSA 모델에 접목하기 위해서는 모든 정지 변수에 대해 계측기와 입력모듈을 고려한 모델을 구축하여야 한다.

한국형 표준 원전인 울진 5,6호기의 원자로 정지 변수 15개에 대하여 각각 모델을 개발하였다. 각각의 변수는 표 3-40에 기술된 바와 같으며, 한 가지 정지 변수에 영향을 미치는 계측제어 계통이 여러 개일 경우에 대해서는 각 계측계통을 따로 고려하여 모델을 작성하였다 [강현국, 2003f].

표 3-40 한국형 표준원전의 정지변수

번호	약어	정지변수명	목적	계측기 입력 특징
1	VOP	Variable Overpower	Single CEA accident 방지	중성자계측기
2	HPL	High Logarithmic Power Level	CEA, Boron투입 계통 이상시 작동	중성자계측기
3	HLD	High Local Power Density	사고시 cladding 손상방지	CPC디지털입력
4	DNB	Low Departure from Nucleate Boiling Ratio	사고시 boiling 방지, 기타 보조 정지	CPC디지털입력
5	HPP	High Pressurizer Pressure	과압방지	협대역
6	LPP	Low Pressurizer Pressure	감압시 및 LOCA시 작동	광대역
7	LSL1	Low Steam Generator1 Water Level	잔열제거 보조급수 기동시간 확보	광대역
8	LSL2	Low Steam Generator2 Water Level	잔열제거 보조급수 기동시간 확보	광대역
9	HSL1	High Steam Generator1 Water Level	주증기 격립 및 ESF보조	협대역
10	HSL2	High Steam Generator2 Water Level	주증기 격립 및 ESF보조	협대역
11	LSP1	Low Steam Generator1 Pressure	SLB시 검출	증기압
12	LSP2	Low Steam Generator2 Pressure	SLB시 검출	증기압
13	HCP	High Containment Pressure	SI개시 및 ESF보조	격납건물 감시계통
14	LSF1	Low Steam Generator1 Reactor Coolant Flow	RCP shaft 고착사고시 작동	SG 1차측 양단압력차
15	LSF2	Low Steam Generator2 Reactor Coolant Flow	RCP shaft 고착사고시 작동	SG 1차측 양단압력차

디지털 기기들로 이루어진 DPPS 캐비넷 내부의 구성과 데이터 흐름을 파악하기 위해 각 모듈을 단위로 한 기능 블록도를 구성하면 다음의 그림 3-73과 같다.

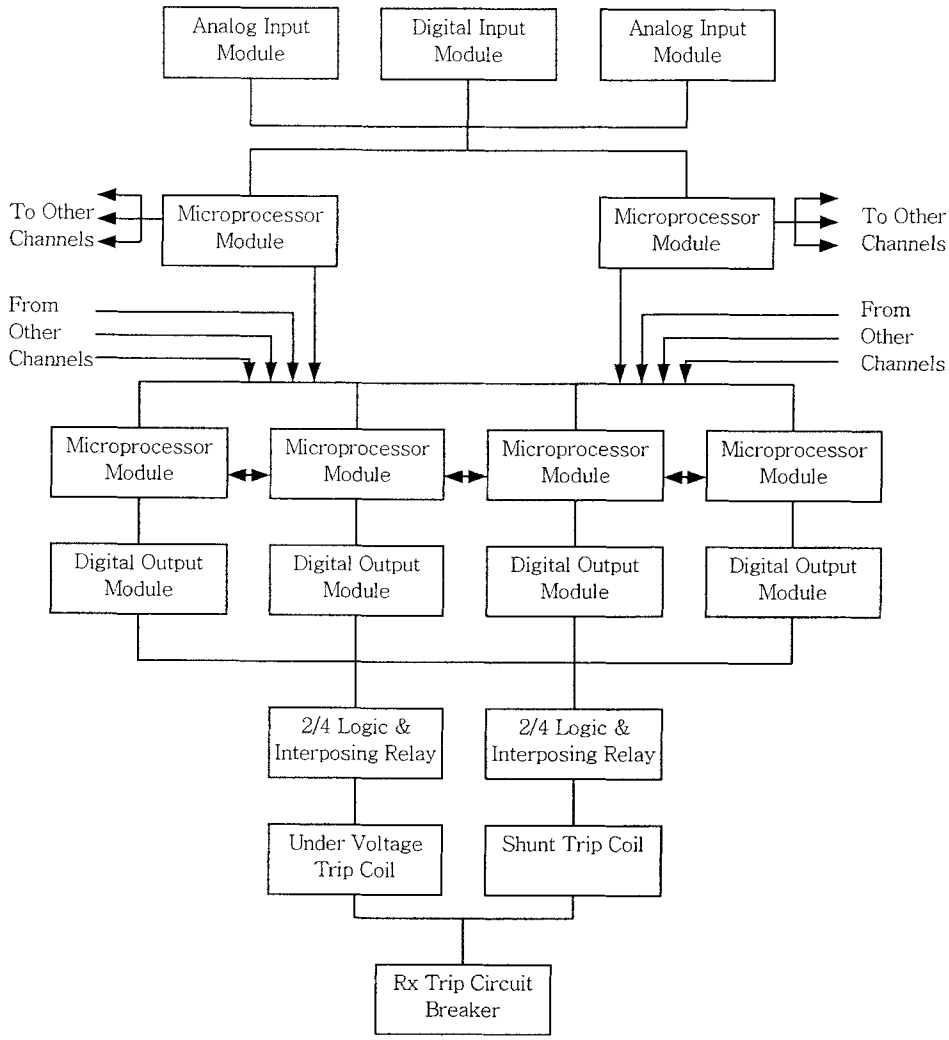


그림 3-73 울진 5,6 호기 DPPS 채널별 구성도

여러 가지 정비변수들 중 그림 3-74 에 증기발생기 저수위로 인한 원자로 정지계통의 이용불능도 계산을 위해 개발된 고장수목 모델의 최상위 부분에 대해 예시하였다 [강현국, 2002g].

본 보고서에서 수행된 분석의 목적은 특정 정지요구 상황이 발생 시 제어봉 구동장치(CEDM)의 전원을 차단하지 못할 확률을 정량적으로 평가하는 것으로 고장수목의 정점사건은 DPPS가 원자로를 정지시켜야 하는 상황에서 정지신호 발

생에 실패하는 사건이다. 따라서 interposing relay, trip circuit breaker등의 기기까지를 모두 포함하여 정량 평가를 수행하였다.

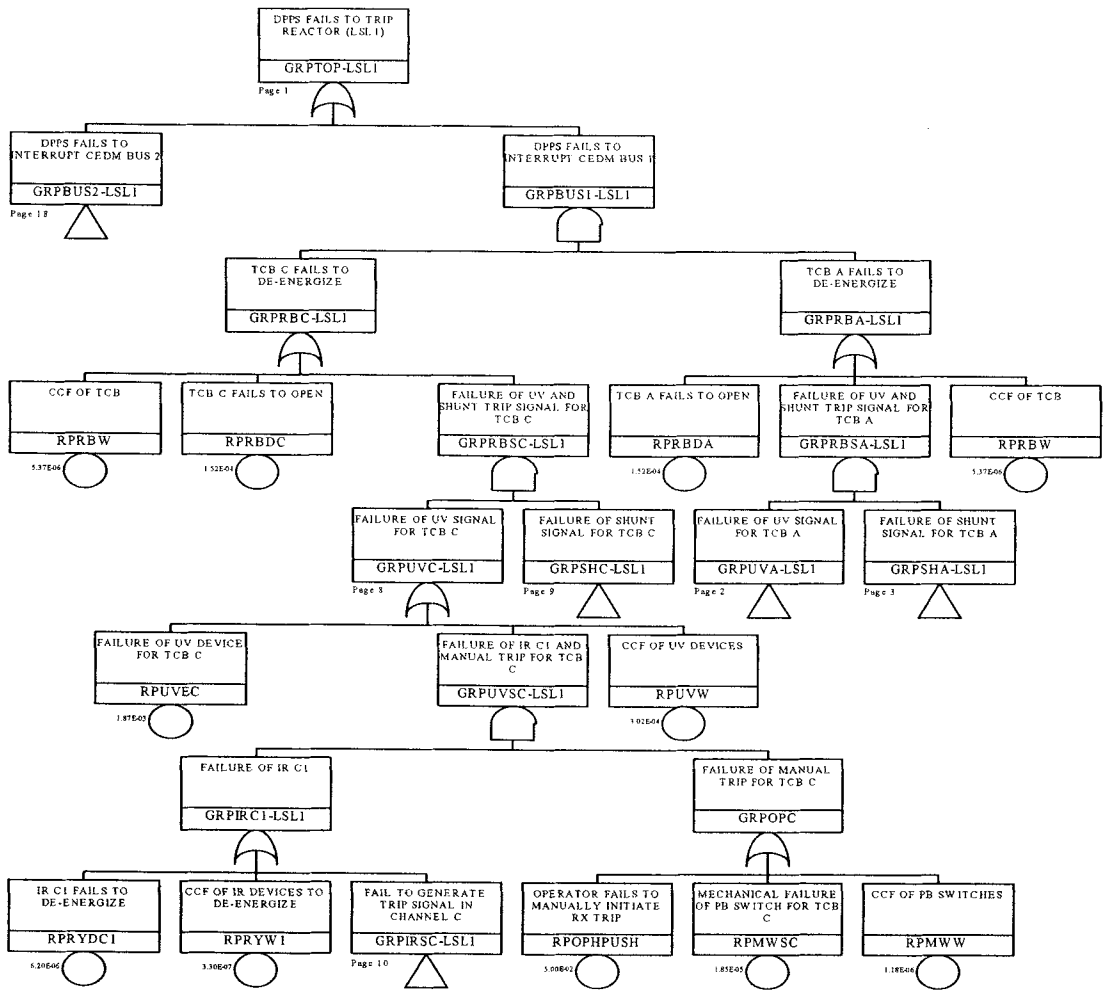


그림 3-74 증기발생기 저수위로 인한 원자로 정지계통 고장수목의 일부

이러한 고장수목 모델을 위한 작성 소프트웨어 패키지는 자체 개발된 PSA 분석용 코드인 KIRAP-KwTREE V3.1을 이용하였다. 이러한 PSA tool을 이용하면 기본사건과 논리조합을 그래픽인터페이스를 통해 쉽게 구성할 수 있을 뿐 아니라 최소 단절 집합에 대한 분석과 입력 고장 데이터 관리도 일괄 수행할 수 있

다. 한편, 정량화를 위해서는 각종 고장률 자료가 필요한데 디지털 기기의 경우 동종의 가압경수로 사용이력이 없으므로 기기 공급자가 제공하는 고장확률을 인용하여 사용하였다. 디지털 기기를 제외한 나머지 정지 회로 차단기 및 릴레이 등의 기기에 대해서는 기존 중장기 연구의 결과물인 KAERI/TR-2164/2002에서 사용한 고유 운전 경험 자료를 활용하였다.

표 3-41 증기발생기 저수위로 인한 원자로 정지계통 이용불능도 분석 결과 (최소단절집합)

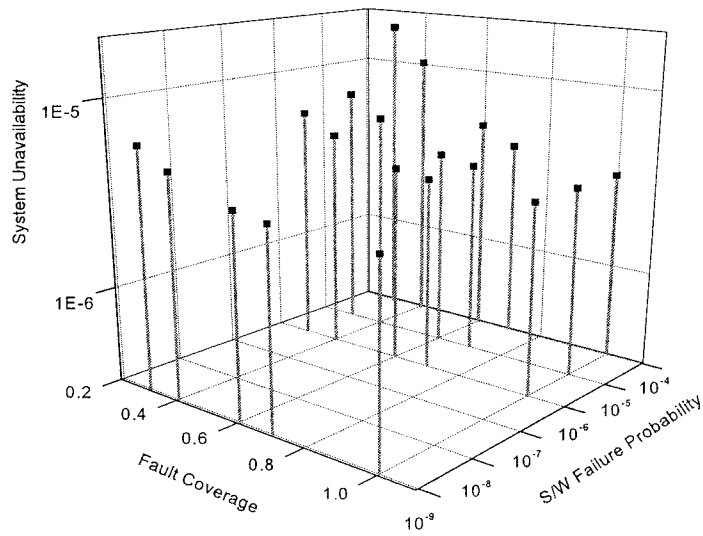
No	Prob.	Events				
1	3.66E-05	RPOPHPUSH	MFLTK-LSL1			
2	5.37E-06	RPRBW				
3	9.30E-07	RPOPHPUSH	RPIMW			
4	8.85E-07	RPOMW	RPOPHPUSH			
5	2.88E-08	RPOPHPUSH	MFLTYA-LSL1	MFLTYC-LSL1	MFLTYD-LSL1	
6	2.88E-08	RPOPHPUSH	MFLTYB-LSL1	MFLTYC-LSL1	MFLTYD-LSL1	
7	2.88E-08	RPOPHPUSH	MFLTYA-LSL1	MFLTYB-LSL1	MFLTYD-LSL1	
8	2.88E-08	RPOPHPUSH	MFLTYA-LSL1	MFLTYB-LSL1	MFLTYC-LSL1	
9	2.31E-08	RPRBDA	RPRBDC			
10	2.31E-08	RPRBDB	RPRBDD			
11	1.32E-08	RPOPHPUSH	RPPMWBI			
12	1.07E-08	RPPMWLL	RPOPHPUSH	RPWDJB2	RPWDJB4	RPWDJD2	RPWDJD4
13	1.07E-08	RPPMWLL	RPOPHPUSH	RPWDJA2	RPWDJA4	RPWDJC3	RPWDJC1
14	1.07E-08	RPPMWLL	RPOPHPUSH	RPWDJB1	RPWDJB3	RPWDJD2	RPWDJD4
15	1.07E-08	RPPMWLL	RPOPHPUSH	RPWDJB2	RPWDJB4	RPWDJD1	RPWDJD3
16	1.07E-08	RPPMWLL	RPOPHPUSH	RPWDJA2	RPWDJA4	RPWDJC2	RPWDJC4
17	1.07E-08	RPPMWLL	RPOPHPUSH	RPWDJB1	RPWDJB3	RPWDJD1	RPWDJD3
18	1.07E-08	RPPMWLL	RPWDJA1	RPOPHPUSH	RPWDJA3	RPWDJC2	RPWDJC4
19	1.07E-08	RPPMWLL	RPWDJA1	RPOPHPUSH	RPWDJA3	RPWDJC3	RPWDJC1
20	6.95E-09	RPUVW	RPSHW				
21	2.50E-09	RPOPHPUSH	RPIMRD1	MFLTYA-LSL1	MFLTYC-LSL1		
22	2.50E-09	RPOPHPUSH	RPIMRA1	MFLTYB-LSL1	MFLTYC-LSL1		
23	2.50E-09	RPOPHPUSH	RPIMRD1	MFLTYA-LSL1	MFLTYB-LSL1		
24	2.50E-09	RPOPHPUSH	RPIMRC1	MFLTYB-LSL1	MFLTYD-LSL1		
25	2.50E-09	RPOPHPUSH	RPIMRA1	MFLTYC-LSL1	MFLTYD-LSL1		
26	2.50E-09	RPOPHPUSH	RPIMRB1	MFLTYA-LSL1	MFLTYD-LSL1		
27	2.50E-09	RPOPHPUSH	RPIMRA1	MFLTYB-LSL1	MFLTYD-LSL1		
28	2.50E-09	RPOPHPUSH	RPIMRD1	MFLTYB-LSL1	MFLTYC-LSL1		
29	2.50E-09	RPOPHPUSH	RPIMRB1	MFLTYA-LSL1	MFLTYC-LSL1		
30	2.50E-09	RPOPHPUSH	RPIMRB1	MFLTYC-LSL1	MFLTYD-LSL1		

그림 3-74에서 예시한 증기발생기 저수위로 인한 원자로 정지계통의 이용불능도에 대한 최초단절집합 분석을 수행한 결과는 표 3-41와 같이 정리된다. 상위 30개의 최소 단절 집합만을 예시하였는데, 계측기의 공통 원인 고장과 운전원 수동 정지 실패가 동시에 발생하는 것이 이용불능도의 가장 중요한 원인이었다.

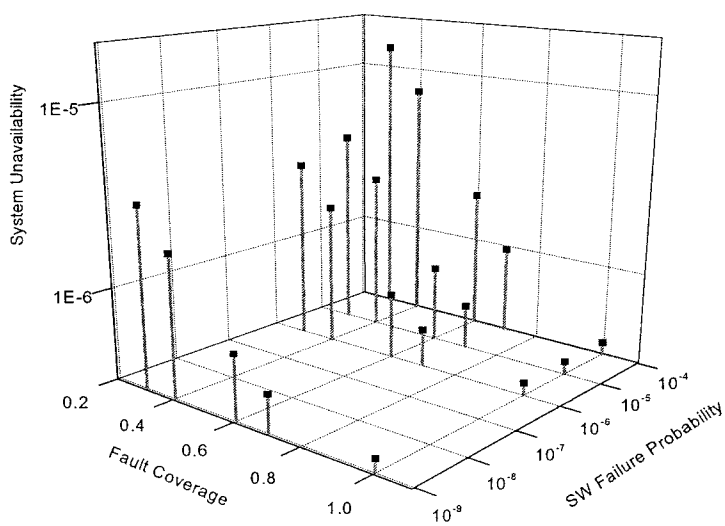
또한 작성된 모델을 기초로 계통 내부 변수의 변화에 따른 계통 전체 이용불능도의 변화를 알아보는 민감도 분석을 수행하였다. 분석결과 중 일부를 그림 3-75 에 그래프로 예시하였다. 공통원인 고장을 회피할 수 있는 설계(즉, 동일기종 모듈 사용 회피 설계)에서는 전체적으로 이용불능도가 낮게 나타나며, 잘 설계된 고장 감시타이머를 이용하거나 소프트웨어의 신뢰도가 높은 경우에는 이용불능도가 낮아지는 것을 확인할 수 있다. [강현국, 2002a; 강현국, 2003g]

15가지 정지변수에 대한 DPPS 이용불능도를 각각 정량화하였다. 결과는 다음 그림 3-76에 주어진 그래프와 같다. HLD (고-국부 출력 밀도)와 DNB(저-핵비등 이탈율) 원자로 정지의 계통 이용불능도가 다른 변수에서의 경우보다 높은 이유는 입력 변수가 계측기로부터 직접 오는 것이 아니라 CPC를 거쳐서 오기 때문에 입력 변수가 오계측될 확률이 높은 것으로 분석하였기 때문이다. 그리고 기존 분석의 결과보다 불가용도가 높은 이유는 주로 운전원 오류확률 산정의 방법론 차이와 입력변수를 개별적으로 고려한 것에 기인한다.

실제 원전 PSA 모델에 접목할 경우, 특정 사고 상황시의 입력변수는 다중이 되므로 각 정지변수의 이용불능도가 그대로 적용되지는 않을 것으로 예상되나, DPPS 디지털 기기의 경우 여러 가지 입력변수를 고려한다 하여도 다중성이 향상되지 않으므로, 결국 플랜트 전체로 볼 때는 DPPS 디지털 기기에 위험도가 집중되는 현상이 나타날 수 있을 것으로 예상된다.



(a) 동일 기종의 입력 모듈 사용 시



(b) 이기종의 입력 모듈 사용 시

그림 3-75 계통 이용불능도 모델을 이용한 민감도 분석

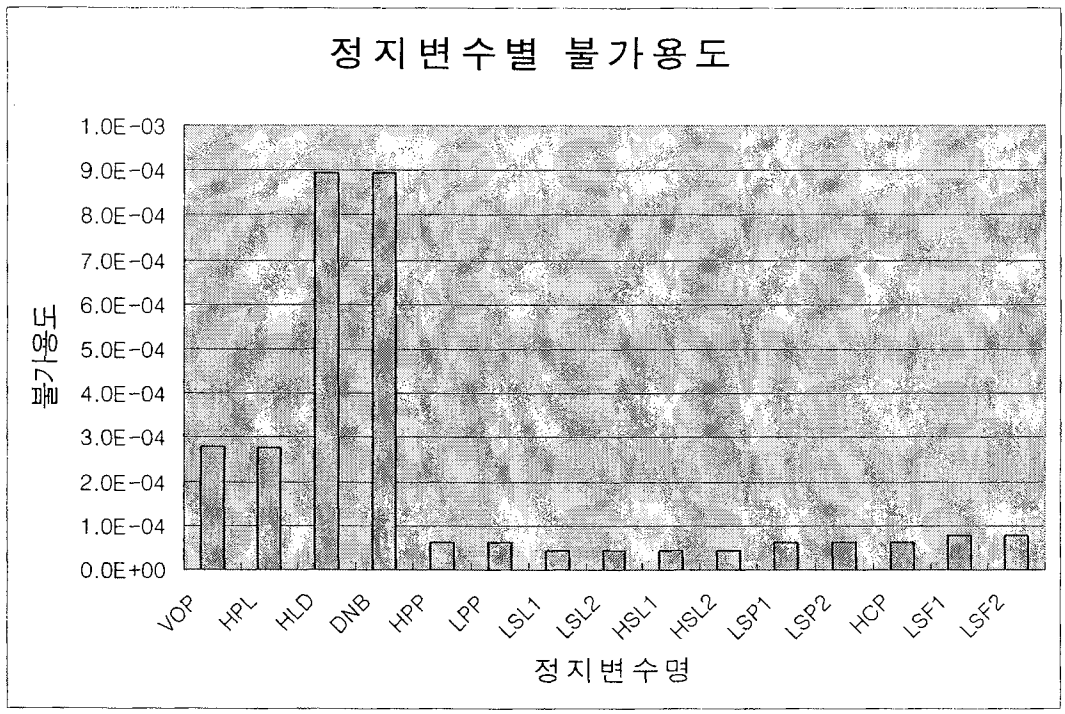


그림 3-76 정지 변수별 DPPS 계통 이용불능도 분석 결과

다. 디지털 공학적 안전설비 작동계통의 상세 신뢰도 모델 개발

한국형 표준원전인 울진 5,6호기의 디지털 공학적 안전 설비 작동 계통(DESFAS)의 계통 이용불능도 분석을 위해 고장수목 작성하였다. DPPS에서 생성한 신호를 DESFAS에서 실제 작동 계통에 해당하는 PCS (Plant Control System)에 전달하게 되는데 이러한 연결은 다음 그림 3-77과 같이 개념적으로 도시할 수 있다.

PCS는 실제 현장의 기기(예를 들면, 밸브와 펌프)를 구동하고 제어하는 제어기의 역할을 하므로 작동기의 일부로 간주하여 모델의 대상에서 제외하였다. DESFAS 고장수목 모델링은 현장 계측기에서 시작하여 DPPS를 포함한 디지털 신호 처리 기기, DESFAS의 디지털 기기를 포함하며 최종적으로는 출력 신호를 생성하는 Opto-coupler까지를 대상으로 한다. 물론 운전원의 수동 작동 실패로 인한 위험도도 모델에 포함되었다.

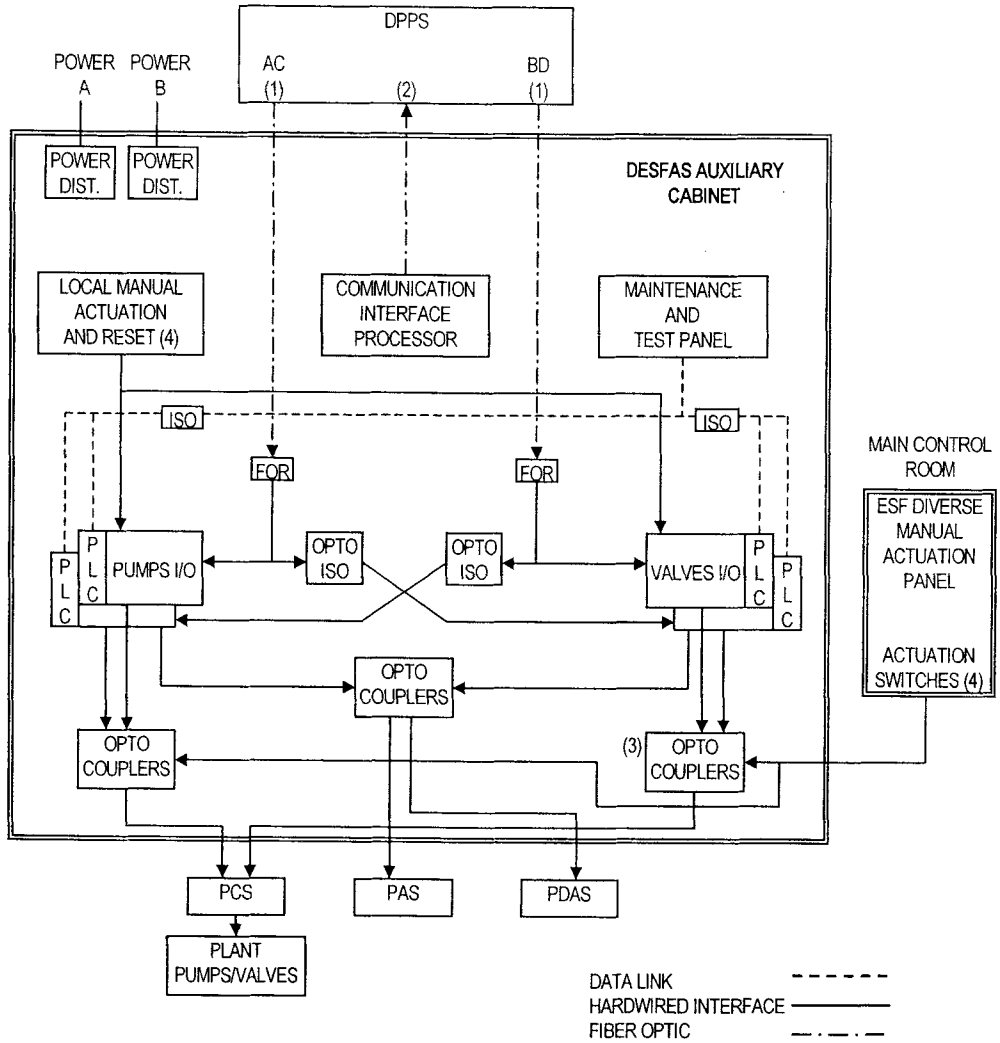
전체적인 신호처리 과정 중 초기의 계측 및 설정치 비교 부분은 DPPS에서 원자로 정지신호를 발생시키기 위한 과정과 동일하며, ESF 작동 신호를 생성하기 위한 변수는 DPPS에서 DESFAS로 전송된다. DPPS의 4개 채널로부터 각각 출력이 전달되며 하나의 DESFAS 프로세서는 두개의 입력(A와C 또는 B와D)을 받아 이를 OR 논리로 처리하고 이것을 출력모듈을 통해 신호를 생성한다. 두개의 프로세서의 출력 신호는 Opto-coupler를 통해 AND 논리 처리가 이루어져서, 결과적으로 선택적 2/4논리를 수행하게 된다.

DESFAS 내에는 총 4개의 프로세서 모듈이 있으며, 펌프와 밸브의 제어를 위해 각각 2개씩의 모듈이 할당된다. 즉, 단일 작동기의 입장에서는 2개의 프로세서를 통해 처리된 신호를 Opto-coupler를 통해 전달받게 되는 것이다.

DPPS의 경우와 마찬가지로, 계통의 이용불능도도만을 분석하는 것이 아니고 실제 원전 PSA 모델에 접목하여 원전 위험도를 평가하고 분석하여야 하므로 모든 작동 변수에 대해 계측기와 입력모듈 및 신호 경로 (DPPS를 거쳐 DESFAS로 입력됨)을 고려한 모델을 구축하여야 한다. 한국형 표준 원전인 울진 5,6호기의 공학적 안전 설비 작동 변수 모두에 대해 각각 모델을 개발하였다. 한 가지 작동 변수에 영향을 미치는 계측계통이 여러 개일 경우에 대해서는 각 계측 계통을 따로 고려하여 모델을 작성하였다 [Sudarno, 2003].

DESFAS의 최종 출력은 Opto-coupler를 통해 전달되는데, 이 과정에서 2가지 유형으로 운전원이 수동으로 개시를 조작할 수 있다. 다음의 그림 3-78은 하나의 서브그룹에 대한 운전원의 수동 개시를 개념적으로 도시한 것이다.

DESFAS 모델의 경우 신호입력을 DPPS로부터 입력받고 작동시켜야 할 actuator가 많으므로 DPPS보다 더 방대한 모델이 된다. 특정 작동 신호를 생성시키는 조건은 몇 가지 변수 중 하나가 설정치를 초과하는 것이므로, 사고 시나리오별 열수력 분석을 수행하여 해당 변수들을 정리하지 못한 상태이므로 보수적으로 다수의 변수 계측기 중 한 가지라도 고장 상태이면 해당 작동 신호가 발생하지 못하는 것으로 가정하였다.



NOTES:

1. ESFAS FIBER OPTIC INITIATION SIGNALS
2. ESFAS FIBER OPTIC STATUS/TEST FEEDBACK DATA LINK SIGNALS.
3. INCLUDES ISOLATED REDUNDANT CHANNEL OUTPUTS.
4. TWO MANUAL SWITCHES FOR EACH ESF FUNCTION.
5. FOR = FIBER OPTIC RECIEVER, ISO = ISOLATION DEVICE

그림 3-77 DPPS와 DESFAS의 연결 및 출력 신호 생성 블럭도

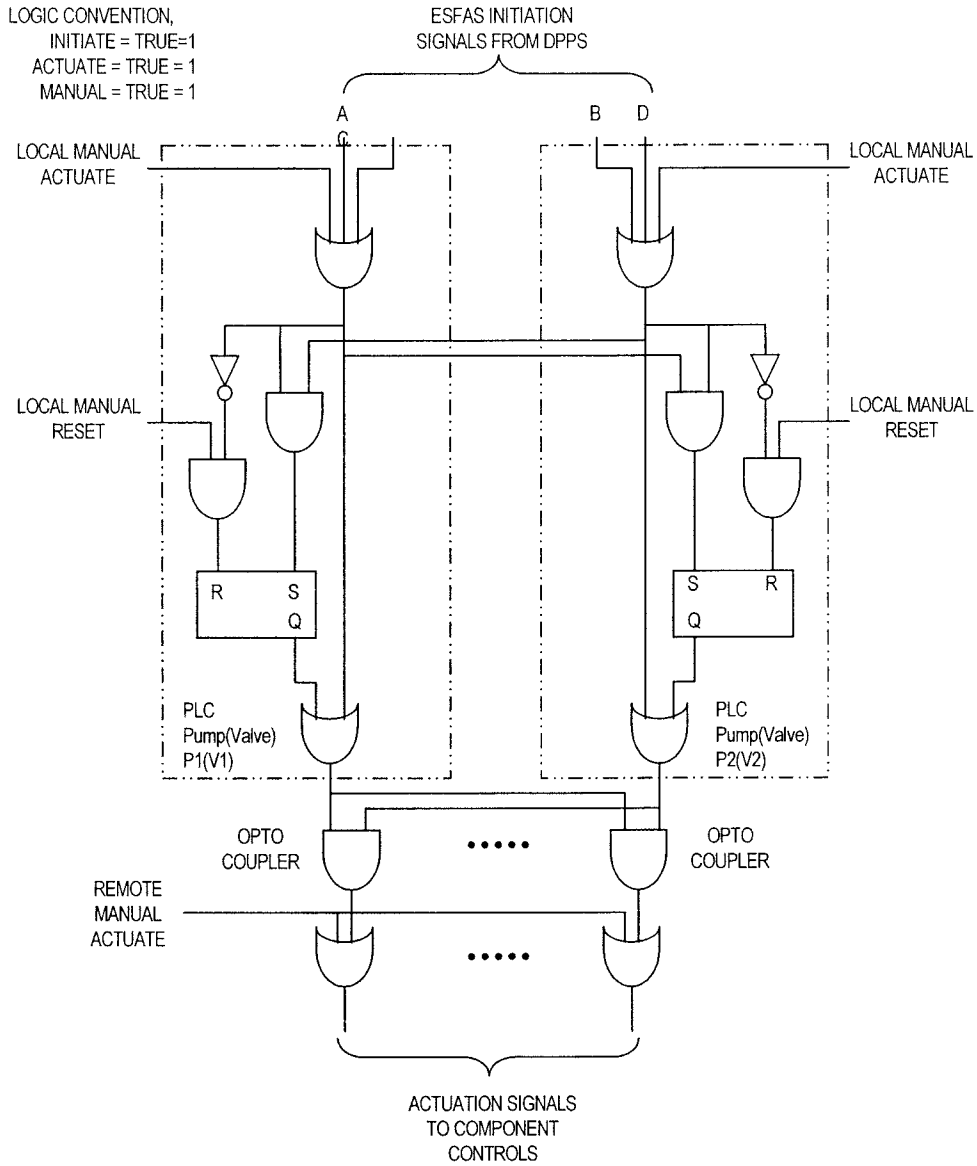


그림 3-78 DESFAS의 Opto-coupler 출력 및 운전원 수동 개시

전술한 바와 같이 공학적 안전설비 작동계통은 한 가지 작동변수에 대해 여러 개의 계측 변수가 영향을 미치므로 이에 대한 분석이 필수적이다. 작동변수 7개에 대하여 각각 모델을 개발하였으며, 한 가지 작동변수의 입력이 되는 계측 계통이 여러 개일 경우 각 계측 계통별로 별도로 모델을 개발하였다. DESFAS의 작동변수 7가지는 다음과 같다.

. Safety Injection Actuation System (SIAS)

. Containment Isolation Actuation System (CIAS)

. Containment Spray Actuation System (CSAS)

. Recirculation Actuation System (RAS)

. Main Steam Isolation System (MSIS)

. Auxiliary Feedwater Actuation System 1 (AFAS-1)

. Auxiliary Feedwater Actuation System 2 (AFAS-2)

고장수목 모델을 위해 사용된 계측 변수는 다음의 표 3-42에 보이는 것과 같다. 모든 변수에 대해 계측기와 입/출력모듈을 상세히 고려한 고장수목을 바탕으로 울진 5,6 호기 DESFAS 고장수목을 개발하였다.

표 3-42 공학적 안전설비 작동계통에서 고려된 계측변수

번호	약어	설명
1	LPP	Low Pressurizer Pressure
2	LSL1	Low Steam Generator1 Water Level
3	LSL2	Low Steam Generator2 Water Level
4	HSL1	High Steam Generator1 Water Level
5	HSL2	High Steam Generator2 Water Level
6	LSP1	Low Steam Generator1 Pressure
7	LSP2	Low Steam Generator2 Pressure
8	HCP	High Containment Pressure
9	HHCP	Hi Hi CNT pressure
10	LRL	Low Refueling water tank level
11	HDP1	SG2 Pr > SG1 Pr
12	HDP2	SG2 Pr < SG1 Pr

이러한 분석 과정을 거쳐, DESFAS 각각의 작동 신호에 대한 고장 수목을 작성하였는데, 그림 3-79는 AFAS-1 신호 작동 계통에 대한 고장수목 일부를 예

시한 것이다. 그림 3-80는 작동변수의 종류에 따른 DESFAS 이용불능도의 변화를 도시한 것이며, 입/출력 변수가 많고 입/출력 모듈을 많이 사용하는 MSIS가 가장 높은 이용불능도를 보이고 있다 [강현국, 2003a].

분석을 위한 가정과 이용된 자료는 DPPS의 경우와 동일하다. 즉, 디지털 기기의 경우 기기 공급자가 제공하는 고장 확률을 인용하여 사용하였고, 디지털 기기를 제외한 나머지 정지 회로 차단기 및 릴레이 등의 기기에 대해서는 KAERI/TR-2164/2002에서 사용한 고유 운전 경험 자료를 활용하였다.

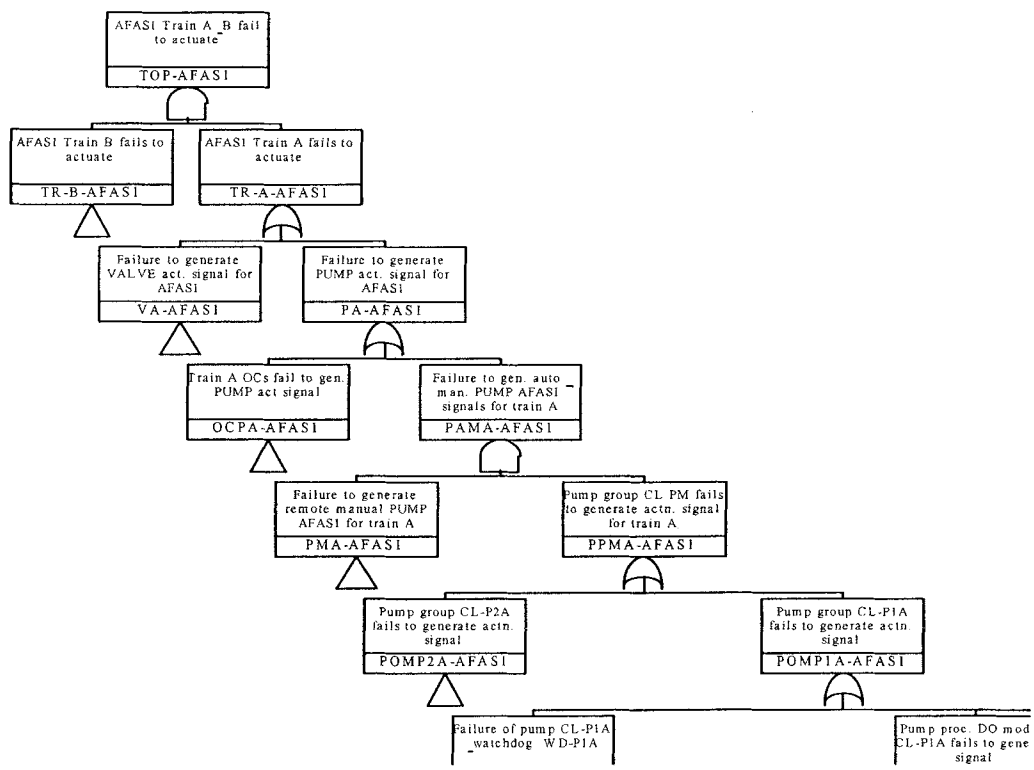


그림 3-79 AFAS-1 신호 작동 계통 고장수목의 일부 예시

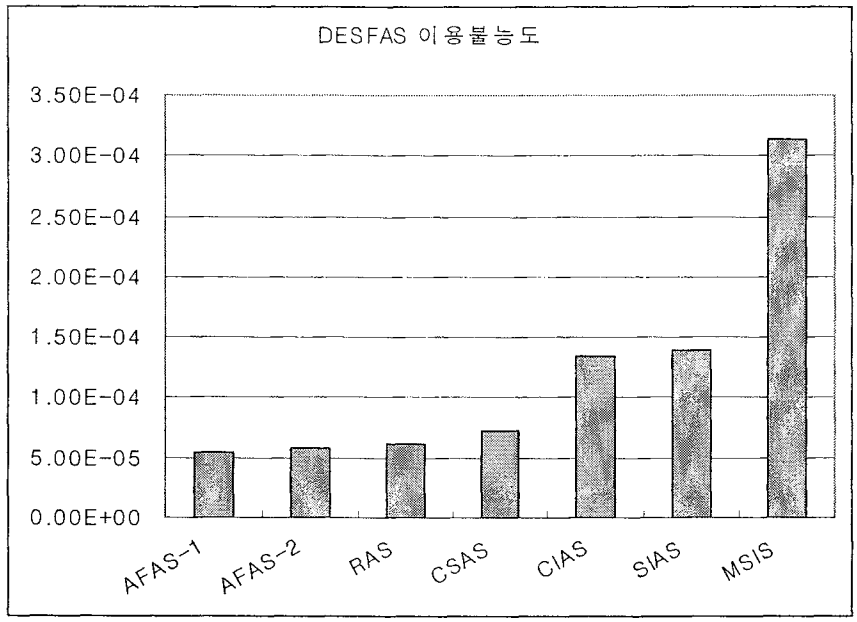


그림 3-80 ESF 신호별 이용불능도의 변화

2. 디지털 계통의 원전 위험도 영향 평가 모델 개발

작성된 DPPS와 DESFAS 고장수목 모델을 원전 위험도 감시용 PSA 모델(RM)에 결합하여 한국형 표준원전의 위험도 분석 모델을 작성함으로서 디지털 계통의 원전 위험도 영향 평가를 수행하였다.

대표적인 위험도 평가 척도인 노심 손상 빈도(CDF)와 대량 조기 방출 빈도(LERF)를 계산할 수 있는 모델을 개발하였다. 디지털 안전 계통인 DPPS와 DESFAS를 포함하는 CDF모델의 경우 3,900여개의 기본사건과 7,000여개의 게이트 사건으로 구성된 매우 방대한 모델이며, LERF는 이보다 더 방대한 모델이다.

한편, 디지털 계통의 역할은 안전 관련 신호를 생성하는 것이므로, 운전원의 수동 신호 생성과 밀접한 관계를 가진다. 즉, 자동과 수동의 결합으로 최종 신호가 생성되는 것이다. 운전원에게 제공되는 정보가 디지털 계통에서 처리되는 경우, 기존의 경우와는 달리 복잡하기 유기적인 상호 의존성이 존재하게 된다. 이러

한 상황을 효과적으로 고장수목으로 모델하기 위한 조건부 인간 오류 분석 방법론을 개발하였다.

가. 노심 손상 빈도(CDF) 평가 모델 개발

원전 위험도 감시용 PSA 모델 (RM)은 기존 원전의 PSA가 사건수목과 고장수목으로 구분되었던 것을 하나의 정점사건을 가지는 고장수목으로 변경한 모델이므로, 그 구성상 최상위 사건은 모두 초기사건의 발생과 그 완화의 실패로 구성되어 있으며, 이중 초기사건 완화 실패의 원인은 안전기기 작동 실패와 작동신호 생성 실패의 2 가지로 정리할 수 있는데, 작동신호 생성 실패가 본 연구의 대상인 DPPS/DESFAS 및 운전원 수동 조작에 해당한다. 운전원 수동 조작의 경우, 기존의 아날로그형 계측제어 시스템과는 달리 디지털화된 기기의 실패는 곧 운전원을 위한 주요 경보의 상실을 의미하므로, 수동 작동 신호 개시의 적절한 가동 확률이 현저히 저하되는 것이 당연하다.

그림 3-81에 디지털계통의 발전소 위험도 영향 평가용 CDF 모델의 최상위 고장수목을 예시하였다. 여기에는 여러 가지 초기사건들로 인한 노심 손상 가능성을 계산하기 위한 모델이 포함되는데, 전술한 바와 같이 디지털 계통은 안전신호 생성실패를 유발함으로써 원전 위험도에 영향을 미친다 [강현국, 2004a].

한편, CDF를 계산하기 위해서는 정지 불능 과도사건(ATWS)을 포함하여야 하므로, 이에 따른 분석을 별도로 수행하였다. DPPS의 작동 불능은 ATWS를 유발하여 결과적으로 CDF 계산에 반영된다[강현국, 2004b].

표 3-43에 개발된 영향 평가 모델의 정량화 결과를 보였다. 이 결과는 울진 3,4호기의 RM 모델에 울진 5,6호기의 디지털 신호 생성 계통을 결합시킨 모델로부터 얻은 것이므로 실제 울진 5,6호기의 기타 기기 설계 변경에 의해 변동될 수 있는 값을 유의해야 하며, 분석의 목적은 아날로그 계통의 포함한 경우와 디지털 계통을 포함한 경우를 비교하기 위한 것으로 한정한다. ATWS는 CDF를 계산하기 위한 세부 항목이므로 이 표에도 나타내었으며, ATWS 확률 정량화를 위한

모델 개발 및 열수력 분석 수행은 아래의 제3장 3절 다항에서 상세히 다루었다.

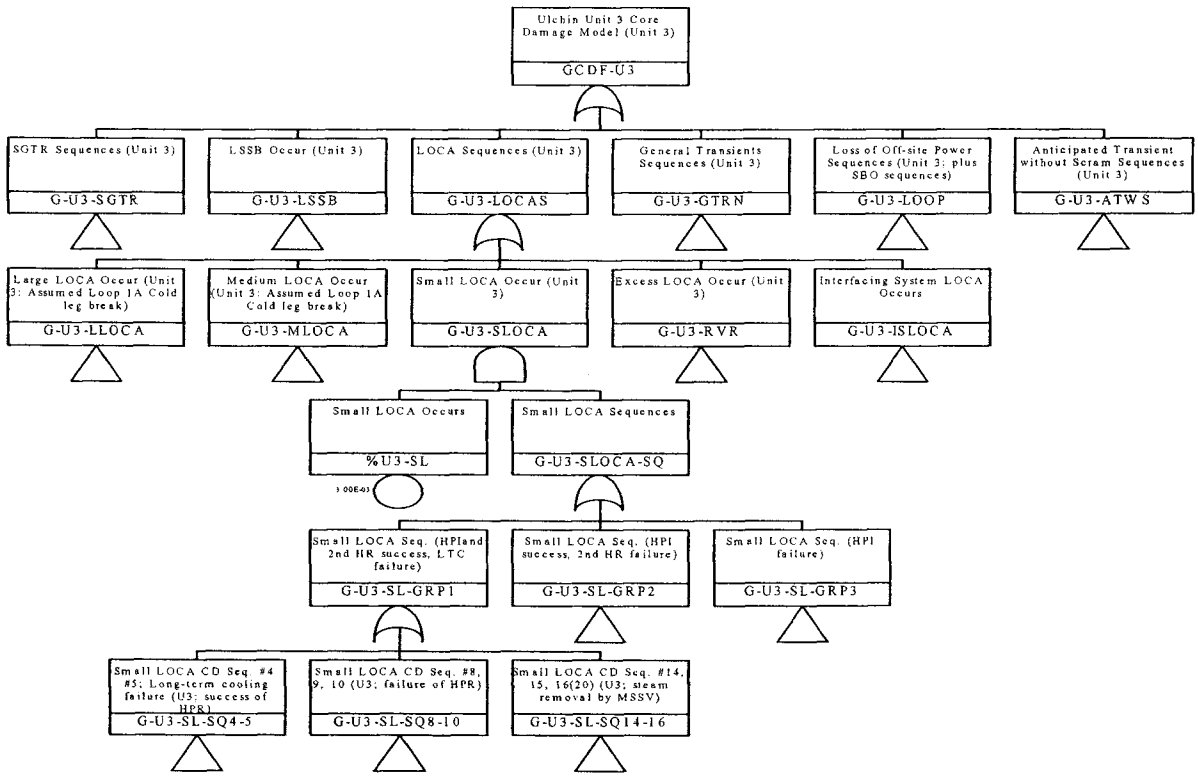


그림 3-81 디지털 계통의 발전소 위험도 영향평가를 위한 CDF 모델의 최상위 논리 예시

한편, 선행 연구를 통해 규명된 디지털 계통 모델의 주요 인자에 대한 원전 CDF의 민감도를 분석하였으며, 그 결과 중 고장 검출 확률 0.7로 고정한 경우에 대해 그림 3-82에 도시하였다. 운전원이 어떠한 경우에도 운전원이 수동으로 원자로를 정지시킬 수 있고 필요한 ESF 작동 신호를 수동으로 개시시킬 수 있는 경우, 소프트웨어의 오류나 고장 감시 타이머의 고장 검출 실패는 CDF에 영향을 미치지 못한다. 수동 개시 실패 확률을 보다 현실적인 값으로 가정을 하면 결과는 달라진다. 소프트웨어의 오류 확률이나 고장 감시 타이머의 고장 검출 확률에 영향을 받아 CDF는 약 13배까지 상승하는 것으로 나타났다. 최악의 경우는 운전원

의 수동 신호 생성을 무시하고 (수동개시 실패확률 1), 소프트웨어의 오류 확률이 높으며 (1E-3), 고장 감시 타이머의 고장 검출률이 낮은(0.3) 경우이다. 이때는 CDF가 1E-4까지 상승하는 것으로 나타났다 [강현국, 2003d; 강현국 2004c].

표 3-43 디지털 계통의 발전소 영향평가용 모델 정량화 결과 (CDF)

초기사건 그룹	초기사건	아날로그 I&C 포함 모델			디지털 I&C 포함 시범 모델*			비고
		IE빈도 (/RY)	CDF		IE빈도 (/RY)	CDF		
			평균	백분율		평균	백분율	
LOCA그룹	LLOCA	1.70E-04	6.80E-07	8.76	1.70E-04	7.20E-07	7.51	
	MLOCA	1.70E-04	5.96E-07	7.67	1.70E-04	6.37E-07	6.64	
	SLOCA	3.00E-03	1.13E-06	14.56	3.00E-03	1.78E-06	18.54	
	SGTR	4.50E-03	1.16E-06	14.99	4.51E-03	1.99E-06	20.78	
	ISLOCA	1.77E-09	1.77E-09	< 0.1	1.77E-09	1.77E-09	< 0.1	
	RVR	2.66E-07	2.66E-07	3.43	2.66E-07	2.66E-07	2.77	
	소계		**3.84E-06**	**49.43**		**5.40E-06**	**56.26**	
과도사건 그룹	LSSB	1.50E-03	1.72E-07	2.21	1.50E-03	1.74E-07	1.81	
	LOFW	1.75E-01	3.91E-07	5.03	1.75E-01	5.28E-07	5.51	
	LOCV	1.01E-01	1.80E-08	0.23	1.01E-01	2.17E-08	0.23	
	LOOP	3.13E-02	2.21E-06	28.46	3.13E-02	2.24E-06	23.34	SBO포함
	LOCCW	4.28E-01	5.57E-07	7.17	4.28E-01	5.74E-07	5.98	
	LOKV	1.31E-03	4.07E-10	< 0.1	1.31E-03	4.07E-10	< 0.1	
	LODC	2.62E-03	2.94E-07	3.78	2.62E-03	2.98E-07	3.11	
	GTRN	7.79E-01	1.59E-07	2.05	7.79E-01	1.89E-07	1.97	
	ATWS	8.40E-06	1.27E-07	1.63	1.13E-05	1.72E-07	1.79	
	소계		**3.93E-06**	**50.57**		**4.19E-06**	**43.74**	
총 노심손상빈도			**7.77E-06**	**100.00**		**9.59E-06**	**100.00**	

*) 수동개시 실패확률 0.05, S/W 고장확률 0.001, 고장검출확률 0.7로 가정함.

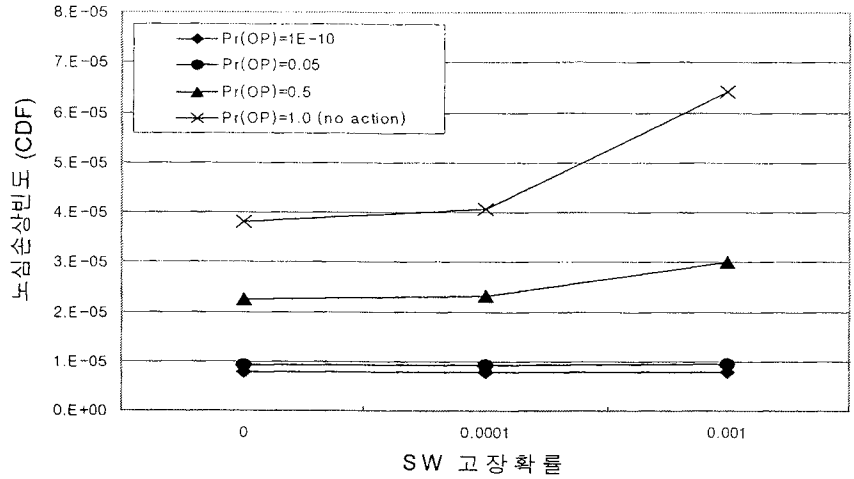


그림 3-82 CDF에 대한 민감도 분석 결과

나. 대량 조기 방출 빈도 평가 모델 개발

대량 조기 방출 빈도(LERF) 모델의 경우, CDF 모델과 계통에 대한 논리 및 기본사건 구성은 완전히 동일하며, 노심 손상 이후 대량 조기 방출이 발생할 가능성에 대한 분석이 추가되는 형태이다. 표 3-44에 분석 결과를 기술하였다. CDF의 경우와 마찬가지로 디지털 계통 모델의 주요 인자에 대한 LERF의 민감도를 분석하였으며, 그 결과 중 일부를 그림 3-83에 도시하였다 [강현국, 2003d].

어떠한 경우에도 운전원이 수동으로 원자로를 정지시킬 수 있고 필요한 ESF를 수동으로 개시시킬 수 있는 경우, 소프트웨어의 오류나 고장감시타이머의 고장 검출 실패는 LERF에 영향을 미치지 못한다. 수동 개시 실패 확률을 현실적인 값으로 가정을 하면 소프트웨어의 오류 확률이나 고장 감시타이머의 고장 검출 확률에 영향을 받아 LERF는 약 54배까지 상승하는 것으로 나타났다. 최악의 경우는 운전원의 수동 신호 생성을 무시하고 (수동개시 실패확률 1), 소프트웨어의 오류확률이 높으며 (1E-3), 고장감시타이머의 고장 검출률이 낮은(0.3) 경우이다. 이 때는 LERF가 6.7E-5까지 상승하는 것으로 나타났다.

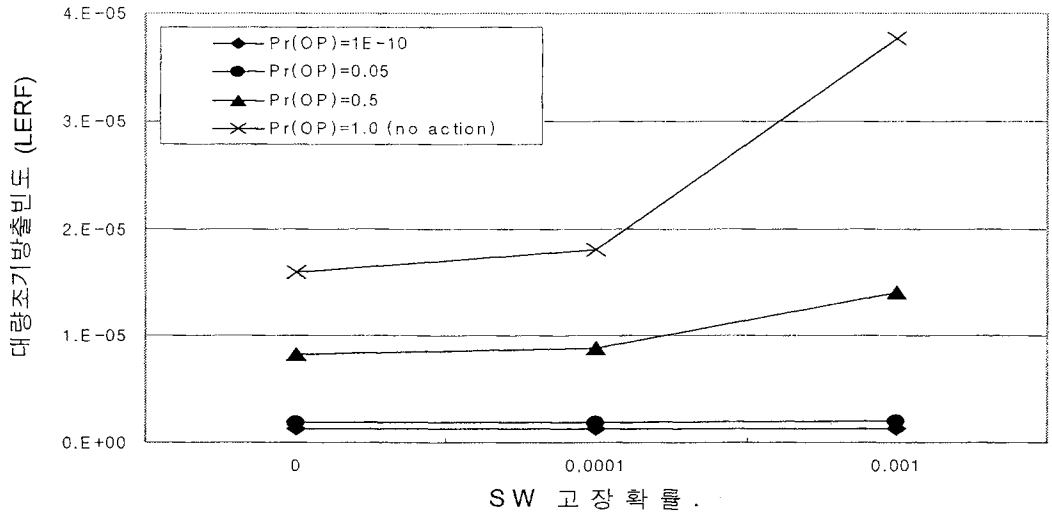


그림 3-83 LERF에 대한 민감도 분석 결과 (CDF의 경우와 동일 조건)

표 3-44 디지털 계통의 발전소 영향평가용 모델 정량화 결과 (LERF)

LERF 경위	아날로그 I&C 포함 모델		디지털 I&C 포함 시범 모델*		비고
	CDF (/RY)	LERF (/RY)	CDF (/RY)	LERF (/RY)	
LERF-SQ#4	7.77E-06	1.09E-08	9.59E-06	1.34E-08	
LERF-SQ#8		1.16E-08		1.20E-08	
LERF-SQ#10		7.17E-08		7.48E-08	
LERF-SQ#12		1.17E-06		1.93E-06	
소계		1.26E-06		2.03E-06	

*) 수동개시 실패확률 0.05, S/W 고장확률 0.001, 고장검출확률 0.7로 가정함.

다. 정지불능 과도사건(ATWS) 빈도 평가 모델 개발

전체 초기 사건(IE)중 DPPS의 원자로 정지 신호 발생 여부에 영향을 받아 사건의 전개 경로가 달라지는 10가지를 선정하여 분석을 수행하였다. 즉, ATWS가 발생할 수 있는 초기사건 10가지를 추출한 것이다.

특정 초기사건이 발생할 경우 복수의 원자로 정지 신호가 설정치를 초과하게 되며 다중 보호 계통의 작동도 고려하여야 한다. 이러한 다중 기능의 종속성 분석을 위하여 10개의 초기사건에 대한 15개의 원자로 정지 신호와 다중 보호 계통

(DPS)에 의한 원자로 정지 신호를 분석하였다. 이러한 분석의 결과는 초기사건별 정지신호 분석(ATWS 빈도)에 대한 상세 모델링에 반영하였다. 최종 안전성 분석 보고서 등 관련 문서를 검토하고 전문가의 자문을 받아 표 3-45의 결과를 얻었다.

이 결과를 검증하기 위해 MARS 2.1 코드를 이용한 열수력 분석을 일부 실행하였다. 그림 3-84는 소형 냉각재 상실 사고 발생 시 DPPS/DESFAS가 작동하지 않고 운전원 수동 신호도 없을 경우에 대한 가압기 압력의 변화를 도시한 것이다 [강현국, 2003b].

ATWS 빈도에 대한 상세 고장수목 모델은 초기사건별 정지신호 분석의 결과를 반영하여 KIRAP 전산코드를 이용하여 개발하였다 [강현국, 2003b; 강현국, 2003c]. CDF 및 LERF의 경우와 마찬가지로 디지털 계통 모델의 주요 인자에 대한 ATWS 빈도의 민감도를 분석하였다. [강현국, 2004g].

어떠한 경우에도 운전원이 수동으로 원자로를 정지시킬 수 있는 경우, 소프트웨어의 오류나 고장 감시타이머의 고장 검출 실패는 ATWS빈도에 영향을 미치지 못한다. 수동개시 실패 확률을 현실적인 값으로 가정을 하면 소프트웨어의 오류 확률이나 고장 감시타이머의 고장 검출 확률에 영향을 받아 ATWS빈도는 약 15배까지 상승하는 것으로 나타났다. 최악의 경우는 운전원의 수동 신호 생성을 무시하고 (수동개시 실패확률 1), 소프트웨어의 오류 확률이 높으며 (1E-3), 고장 감시타이머의 고장 검출률이 낮은(0.3) 경우이며, 이때는 ATWS빈도가 1.3E-4까지 상승하는 것으로 나타났다.

표 3-45 초기사건별 정지신호 분석 결과

초기사건	DPPS정지신호	DPS적용여부
소형LOCA (SLOCA)	DNB, LPP, HCP	X
증기발생기 세관 파단사고 (SGTR)	HSL, DNB	X
대형 이차측 파단 사고 (LSSB)	LSP, VOP, LSL, LPP, DNB	X
주급수 상실사고 (LOFW)	LSL, HPP	O
복수기 상실 사고 (LOCV)	HPP	O
기기냉각수 상실사고 (LOCCW)	LSF, DNB	O
4.16KV 교류전원 상실사고 (LOKV)	LSF, DNB	O
125V 직류전원 상실사고 (LODC)	HPP, DNB, HSL	O
소외전원 상실사고 (LOOP)	LSF, DNB	O
일반과도사건 (GTRN)	HPP, DNB	O

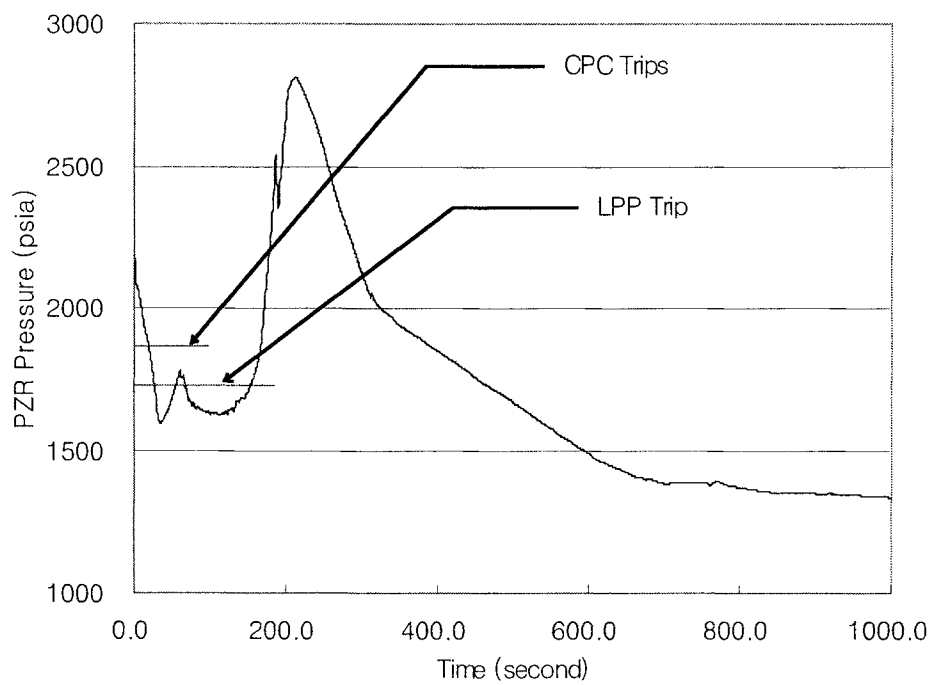


그림 3-84 소형 LOCA 원자로 정지 불능 시 가압기 압력 변화
(MARS2.1 열수력 분석 결과)

라. 조건부 인간오류 분석 (CBHRA) 방법론 개발

자동과 수동의 결합으로 최종적으로 안전 신호가 생성되어 개별 기기로 전달된다. 디지털 계통의 역할은 안전관련 신호를 생성하는 것이므로, 운전원의 수동 신호 생성과 밀접한 관계를 가진다. 즉, 운전원에게 제공되는 정보가 디지털 계통에서 처리되는 경우, 기존의 경우와는 달리 복잡하기 유기적인 상호 의존성이 존재하게 된다. 이러한 상황을 효과적으로 고장수목으로 모델하기 위한 조건부 인간오류 분석 방법론을 개발하였다.

그러나 기존의 분석에서는 운전원에게 모든 정보가 정상적으로 제공된다는 가정 하에 단일 사건으로 고장수목을 작성하였으나, 분석결과 이것은 매우 불합리한 결과를 모델링 초래하는 것으로 밝혀졌으며[강현국, 2004d], 디지털 기기와 운전원은 그림 3-85에 주어진 것과 같이 서로 밀접한 상호 작용이 있다 [강현국, 2004e]. 운전원의 수동 신호 발생이 필요한 상황은 어떤 이유로든 자동신호가 생성되지 못한 때뿐이다. 자동신호가 생성되지 않은 원인을 분석해 보면 현장 계측기가 고장 상태이거나 신호 처리기가 고장 상태에 있기 때문이다. 따라서 수동 신호 발생이 필요할 때 운전원이 필요한 정보를 충분히 제공받지 못할 가능성이 있다. 즉, 운전원 오류 확률은 주어지는 상황에 따라 달라지며 그것이 '신호생성 실패'의 주요 원인 중의 하나이므로 모델에 적절히 다루어져야만 보다 합리적인 원전 위험도 평가가 가능하다.

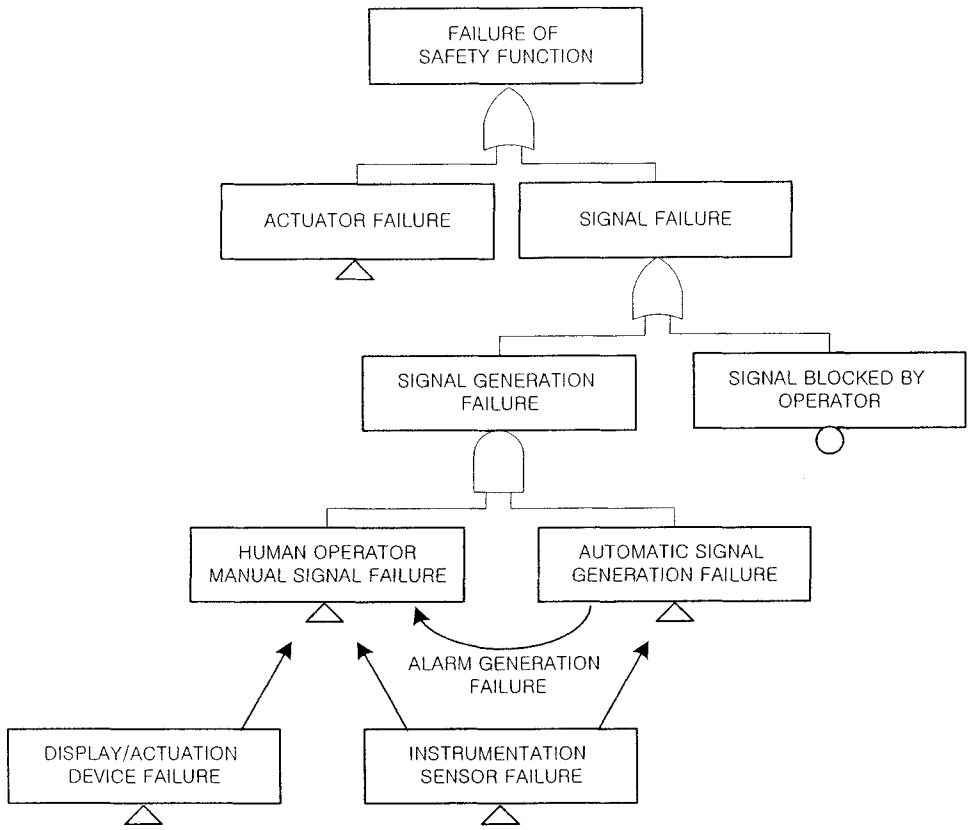


그림 3-85 디지털 계통 고장과 운전원 오류의 상호 작용 개념도

따라서 본 연구에서는 디지털기기 및 입력 센서의 고장 조건에 따른 조건부 인간 오류 확률 모델링(CBHRA)에 대한 연구를 수행하였다. 조건부 확률로 표현한 기능상실(인간 운전원의 오류 포함) 확률은 아래와 같다.

$$F = H = \sum_i \sum_j P(UA \mid A_i, S_j) P(A_i \mid S_j) P(S_j)$$

모든 경우의 수를 고장수목에 개별적으로 반영하는 것은 현실적으로는 불가능하므로, 현실적인 고장수목 모델 개발을 위한 방법론을 제시하였으며, 이를 위해 단일변수 안전기능과 다중변수 안전기능을 나누어 조건별 분류를 수행하고, 몇 개의 그룹으로 묶어 각 조건 그룹에 대한 모델링을 수행하였다. 표 3-46은 단일변수 안전 기능의 경우에 대한 분류표의 예시이다.

표 3-46 단일변수 안전 기능 수행을 위한 인간 오류의 조건별 분류표

Status of the automated system / Status of instrumentation	Normal	Abnormal
3 or more channels available	Auto. signal: O Indication: O Alarm: O <*Condition 1*>	Auto. signal: X Indication: O Alarm: X <*Condition 2*>
2 channels available	Auto. signal: O Indication: X Alarm: O → < *Condition 1*>	Auto. signal: X Indication: X Alarm: X <*Condition 3*>
1 or less channel failures	Auto. signal: X Indication: X Alarm: X <*Condition 3*>	Auto. signal: X Indication: X Alarm: X <*Condition 3*>

그림 3-86과 그림 3-87은 개발된 CBHRA방법론을 이용하여 분석한 안전기능의 실패 확률 비교를 위한 예시이다. 그림 3-86은 단일 변수 안전기능인 보조급수 작동 신호 생성 실패 확률에 대하여 기존의 방법론의 결과와 CBHRA 방법론의 결과를 비교하여 도시한 것이다. 기존 단일사건 분석방법 적용 시와 비교하면 수백 배에 달하는 이용불능도 차이를 보이는 것을 확인할 수 있다 [강현국, 2005a, 강현국, 2005b].

그림 3-87은 다중 변수 안전기능인 소형 냉각재 상실사고 시의 원자로 정지 신호 생성 실패에 대하여 비교한 결과를 도시한 것이다 [강현국, 2004f]. 다중변수 안전기능의 경우에는 '신호처리장치 실패로 인한 경보 부재' 및 '개별 신호 표시 가능' 상태가 차지하는 비중이 절대적이므로, 이 한 가지 경우만을 고려하여 단일 사건으로 모델하여도 결과에 큰 차이가 없으므로, 적용성을 높이기 위하여 인적오류를 단일 사건으로 모델링하는 방법도 적용 가능하다고 판단된다.

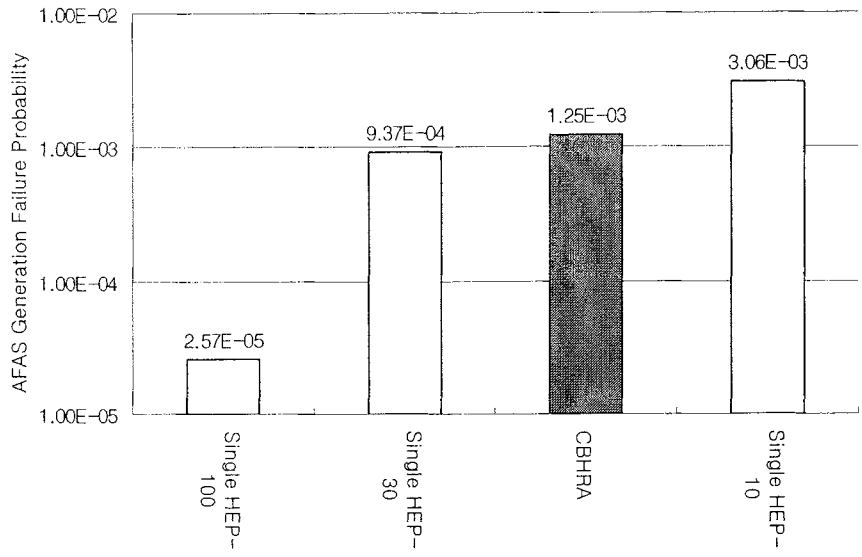


그림 3-86 단일변수 안전기능인 보조급수 작동신호 생성 실패 확률의 비교

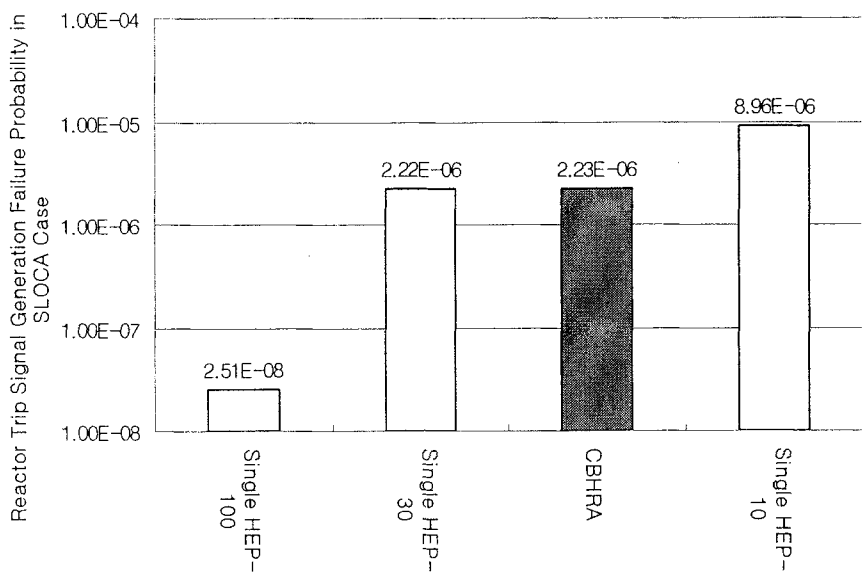


그림 3-87 다중변수 안전 기능인 소형 LOCA 시의 원자로 정지신호 생성 실패 확률의 비교

3. 디지털 I&C PSA 요소 기술 개발

기존의 연구 결과에 의하면 디지털 계통이 원전 위험도에 미치는 영향이 상당히 큰 것으로 평가되었다. 따라서 디지털 계통의 특유의 기능들을 보다 상세하고 정확하게 분석하여 고장수목 모델에 반영할 필요성이 높아졌다. 디지털 계통의 위험도 평가에 대해서는 세계적으로도 아직 정립된 방법론이 존재하지 않는 상황이므로, 상세 분석을 수행하기 위해서는 주요 요소기술의 개발이 병행되어야만 한다.

본 과제에서는 최대 16개까지의 다중성을 가지는 디지털 계통의 특성상 공통원인 고장의 평가가 매우 중요한 역할을 한다는 점을 고려하여, 공통 원인 고장 확률 추정을 현실적으로 수행하기 위한 방법론을 개발하였다. 또한 디지털 계통의 평가에서 가장 어려운 이슈로 부각되는 부분인 소프트웨어 결함 확률의 정량적 평가를 위하여 BBN (Bayesian Belief Net) 기법을 이용한 신뢰도 평가 방법론을 개발하였으며, 디지털 기기에 적용되는 고장 내구성 기법의 유효성 정량화를 위하여 우선 감시타이머의 고장 검출률 추정 모델을 개발하였다.

이러한 요소기술 개발을 통해 디지털계통의 안전성 분석이 보다 정교해지고 현실적이 될 수 있을 것으로 기대되며, 기존의 고장수목 기반의 PSA를 그대로 활용할 수 있으므로 위험도 정보기반 규제나 설계에 보다 편리하게 많은 정보를 제공할 수 있게 될 것으로 판단된다.

가. 디지털 기기 공통원인고장 (CCF) 분석 방법론 기초 연구

디지털 계통 중 안전기능을 수행하는 계통은 그 기능수행을 보장하기 위하여 다중의 기기를 설치하는 것이 일반적이며, 현재 한국형 표준원전에 설치된 디지털 안전계통에서는 4중 채널이 그 내부에서 다시 4중화되어 총 16중의 설비를 갖추는 등 매우 높은 수준의 다중성을 가지도록 설계되어 있다. 이렇게 높은 수준의 다중성 설계를 채택함으로 인하여 개별 기기의 고장으로 인한 기능상실 확률은

매우 낮은데 비해 공통 원인 고장(CCF)에 대한 분석의 중요성은 매우 증대된다.

기존의 확률론적 안전성 평가(PSA) 방법에서 이용하던 CCF 분석 방법론을 활용하여 고장수목을 작성하기 위하여 각 계통에 대한 기능 요구사항 및 물리적 배치 등을 체계적으로 분석하고 이를 이용하여 현실적으로 구현 가능한 모델을 개발하기 위한 기초 연구를 수행하였다.

최대한 이론적인 값에 가까운 결과를 얻으면서도 현실적으로 모델링이 가능하도록 단순화 알파-펙터 방법을 도입하여 16중 다중 트레인의 CCF를 65,519개의 기본사건으로 모델하는 대신 축약된 단일 초기사건으로 표현할 수 있도록 하였다. 한국형 표준원전인 울진 5,6호기의 DPPS에 대하여 출력모듈, 동시 논리 프로세서, 비교 논리 프로세서, 입력 모듈을 구분하여 단순화된 단일 초기사건 계수를 산출하였다. 표 3-47에 출력 모듈 분석의 예제를 보였다.

표 3-47 한국형 표준원전 DPPS 출력모듈 공통원인고장 중 계통 기능상실을 초래하는 고장조합

공통원인고장 기기 수 (k)	가능한 고장조합의 수 ($_{16}C_k$)	계통 기능상실을 초래하는 고장조합의 수 (F_k)	비율 ($p_k=F_k/_{16}C_k$)
1	16	0	0.000
2	120	0	0.000
3	560	0	0.000
4	1820	8	0.004
5	4368	96	0.022
6	8008	520	0.065
7	11440	1680	0.147
8	12870	3584	0.278
9	11440	5264	0.460
10	8008	5352	0.668
11	4368	3728	0.853
12	1820	1756	0.965
13	560	560	1.000
14	120	120	1.000
15	16	16	1.000
16	1	1	1.000

이렇게 계산한 고장조합 중 계통 기능 상실을 초래하는 조합의 비율(pk)을 이용하여 다음의 식과 같이 단일 공통 원인 고장 사건의 확률을 계산할 수 있다.

$$Q_{CCF} = \sum_{k=2}^{m} ({}_{m}C_{k} \times p_{k} Q_{k}^{m})$$

또한 기존의 아날로그 회로와는 달리 디지털 기기의 경우 안전기능 수행에 필수적인 부품은 기기 내에서도 한정되어 있음을 고려하여, 이러한 부품의 용도에 맞는 고장률을 계산하여 CCF 확률 산정에 이용할 수 있도록 방법론을 제시하였다 [강현국, 2005c]. 즉, 소프트웨어 중의 안전기능 부분이 정상적으로 작동하는 상태에서 호출하는 부품만이 안전기능 수행에 필수적인 부품이므로 이러한 분석을 바탕으로 보다 현실적인 위험도를 계산할 수 있도록 하였다. 그림 3-88은 하드웨어 부품의 고장이 소프트웨어를 통해 시스템 고장으로 전파되는 개념을 도시한 것이다.

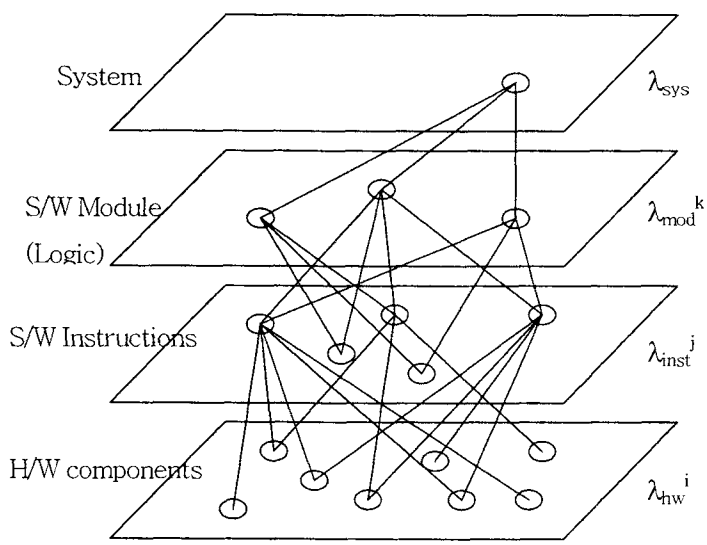


그림 3-88 소프트웨어를 탑재한 디지털 계통의 기능 수행 개념도

디지털의 특성에 따라 이기종의 기기에서도 CCF 노출 가능성이 있으므로,

이기종의 하드웨어 모듈을 이용하여 구성된 시스템에서 동일 기능을 수행하는 이기종의 하드웨어 모듈간의 공통원인 고장을 추정하기 위해 이러한 개념이 유용하게 이용된다. MIL-HDBK- 217F의 기기 고장율 계산식에 따라 공유한 부품은 x, 전체부품을 y 로 표현하면 다음의 식에서 계산된 δ의 분율만큼 알파 factor 방법론으로 계산한 공통원인고장 확률을 분배하여 각 모듈의 CCF 분율을 다음과 같이 계산한다.

$$\delta_{CCF} = \frac{\sum_{x=1}^{m} N_x (\lambda_g \pi_Q)_x}{\sum_{y=1}^{n} N_y (\lambda_g \pi_Q)_y}$$

나. 소프트웨어 신뢰도 분석 방법론 연구

안전 계통에 사용되는 소프트웨어의 정량화된 신뢰도는 시간과 자원의 제약이 따르는 현실적 상황 하에서는 구하기 어렵다는 것이 밝혀짐에 따라 [Littlewood, 1993] [Butler, 1993] 그 동안 이 분야에 대한 연구는 이루어지지 않고 있었다. 그러나 원자력 발전소를 비롯한 여러 산업 분야에서 디지털 시스템이 안전 계통에 사용되는 것이 필연적인 추세가 되고 또 이들 디지털 안전 계통을 포함하는 전체 시스템에 대한 확률론적 안전성 평가(PSA)와 같은 현실적 필요성이 대두됨에 따라 안전 소프트웨어에 대한 정량적인 신뢰도 연구가 필요하게 되었다. 이러한 필요성에 의하여 근래에 시작된 동 분야의 연구는 Testing이나 Reliability Growth Model과 같은 기존 방법들의 확장 연구, 기존에 있는 수 개의 방법들을 종합적으로 결합해서 사용하는 연구 그리고 Bayesian Belief Net (BBN)와 같은 새로운 기술의 활용 등이 진행 중이다. 본 과제에서는 이들 방법들 중에서 가장 유망한 기술 중의 하나로 인정되고 있는 BBN을 이용하여 안전 소프트웨어의 신뢰도를 정량적으로 분석하는 연구를 수행하였다.

국내와 미국, 영국, 캐나다, 프랑스의 원자력규제기관에서 현재 시행 중인 규제 내용들과 IEC, IEEE와 같은 국제표준 중에서 안전 소프트웨어의 신뢰도와 관

련된 항목들을 조사 분석하였다. 조사 결과를 보면, 기존의 정량적 평가 방법은 한계가 있어서 이들 방법으로 구해낸 결과만으로는 원전 안전 소프트웨어의 신뢰성을 보장할 수 없다는 것이 규제와 표준의 기본 입장으로 나타났다. 그러나 최근 건설되었거나 계획 중인 원전들에서 디지털 시스템의 사용이 증가하는 추세에 맞추어 규제 및 표준도 소프트웨어의 정량적 평가에 대한 필요성을 인식하고 이를 위한 준비 작업들이 진행 중인 것으로 나타났다.

안전 소프트웨어의 정량적인 신뢰도 평가와 관련하여 기존 기술들은 모두 이론과 실용적 측면에 있어서 한계성을 지니고 있는데 이들이 가진 한계성을 극복할 가능성이 있는 방법들 중에서 BBN 기법이 가장 유망한 것으로 검토되어 본 연구에서는 이 BBN을 사용하여 안전 소프트웨어의 신뢰도를 평가하는 방안을 연구하였다. 안전 소프트웨어의 정량적인 신뢰도 평가에 있어서 BBN의 장점은 다음과 같다 [Littlewood, 1998].

○ 기존의 방법으로는 구현하기 어려운 복잡한 모델을 표현하고 처리할 수 있는 능력

○ 부분적 자료, 불확실한 자료를 근거로 목표 사건들을 예측(추론) 가능함

○ 수학적 엄밀성을 가지고 있어 해석/계산이 가능한 소프트웨어 도구가 존재

○ 복잡한 관계를 조건부 확률로 명세화 가능

○ 그래프 형태를 통하여 복잡한 연결과 외견 상반되는 추론들을 쉽게 이해

○ 불확실성을 명시적으로 모델링

○ 내재된 가정들을 명시적으로 모델링

○ 주관적 또는 객관적으로 도출된 자료들을 하나의 틀(framework)에서 통합하여 사용이 가능

○ 여러 가지 의사결정의 지원도구로 활용이 가능

안전 소프트웨어의 신뢰도 평가 분야에 BBN을 적용하기 위하여 상용 소프트

웨어(COTS)의 평가 기술에 대한 기반 연구를 수행하였다. 한국 원자력 연구소에서 작성한 상용 소프트웨어의 평가 방안을 토대로 BBN 모델을 구축하였다. 사용된 평가 방안은 상용 등급 조사방법에 따른 인정(approval) 프로세스이며, 이를 근거로 COTS 평가용 BBN 그래프, 노드 확률 테이블을 작성하였고 가상 시나리오를 작성하여 시나리오별 주요 변수를 계산하고 분석하였다. 또한 현실적으로 COTS의 평가에는 여러 가지 다른 상황이 존재하므로 이런 실정을 고려하여 3가지 서로 다른 평가 방안을 작성하였다 [엄흥섭, 2003a].

COTS 평가용 BBN을 구축하는데 필요한 모든 증거들을 작성하기 위하여 문서화된 COTS 평가 방안으로부터 80여개의 주요 변수를 도출하였다. 이들 변수들은 다음 단계에서 보는 바와 같이 BBN 모델의 구성 요소(노드)들이 되며, 평가에 영향을 미치는 실체, 특성, 속성들로 구성되어 있다.

전 단계에서 작성된 변수들을 가지고 BBN 그래프와 노드 확률 테이블을 작성하였다. 그래프는 각 변수들의 연결 관계를 나타내고 노드 확률 테이블은 변수들 간의 연결 강도(조건부 확률)를 나타낸다. 표 3-48은 목표 노드인 "COTS acceptance"의 노드 확률 테이블이다.

표 3-48 목표노드 "COTS acceptance"의 노드 확률 테이블

operation_history_record		good							
development_process		good				bad			
support_quality		good		bad		good		bad	
integration_validation		good	bad	good	bad	good	bad	good	bad
COTS_ acceptance	<0, 0.00001]	0.7	0.1	0.1	0.0	0.1	0.0	0.0	0.0
	<0.00001, 0.0001]	0.25	0.45	0.45	0.2	0.45	0.2	0.2	0.0
	<0.0001, 0.001]	0.04	0.35	0.35	0.25	0.35	0.25	0.25	0.1
	<0.001, 0.01]	0.01	0.1	0.1	0.4	0.1	0.4	0.4	0.2
	<0.01, 0.1]	0.0	0.0	0.0	0.15	0.0	0.15	0.15	0.6
	<0.1, 1]	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.1

operation_history_record		bad							
development_process		good				bad			
support_quality		good		bad		good		bad	
integration_validation		good	bad	good	bad	good	bad	good	bad
COTS_ acceptance	<0, 0.00001]	0.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0
	<0.00001, 0.0001]	0.45	0.2	0.2	0.0	0.2	0.0	0.0	0.0
	<0.0001, 0.001]	0.35	0.25	0.25	0.1	0.25	0.1	0.1	0.0
	<0.001, 0.01]	0.1	0.4	0.4	0.2	0.4	0.2	0.2	0.0
	<0.01, 0.1]	0.0	0.15	0.15	0.6	0.15	0.6	0.6	0.1
	<0.1, 1]	0.0	0.0	0.0	0.1	0.0	0.1	0.1	0.9

그림 3-89는 COTS 평가를 위한 최상위 BBN 그래프이고 그림 3-90은 노드 "design_review"의 서브 그래프, 그림 3-91은 최종적으로 완성된 COTS 평가용 BBN 전체 그래프이다.

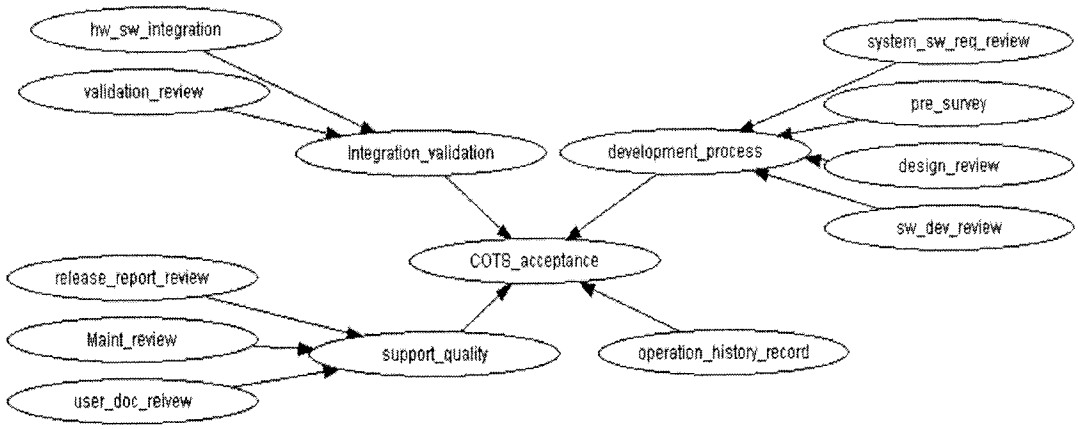


그림 3-89 COTS 평가를 위한 BBN 모델의 최상위 레벨 그래프

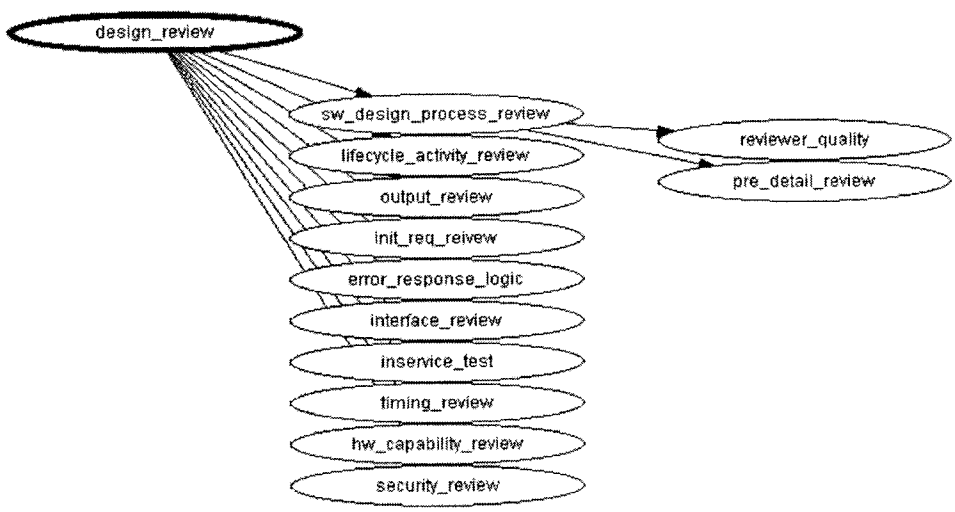


그림 3-90. COTS 평가를 위한 BBN 모델의 하위 레벨 그래프 일부("설계 검토" 노드)

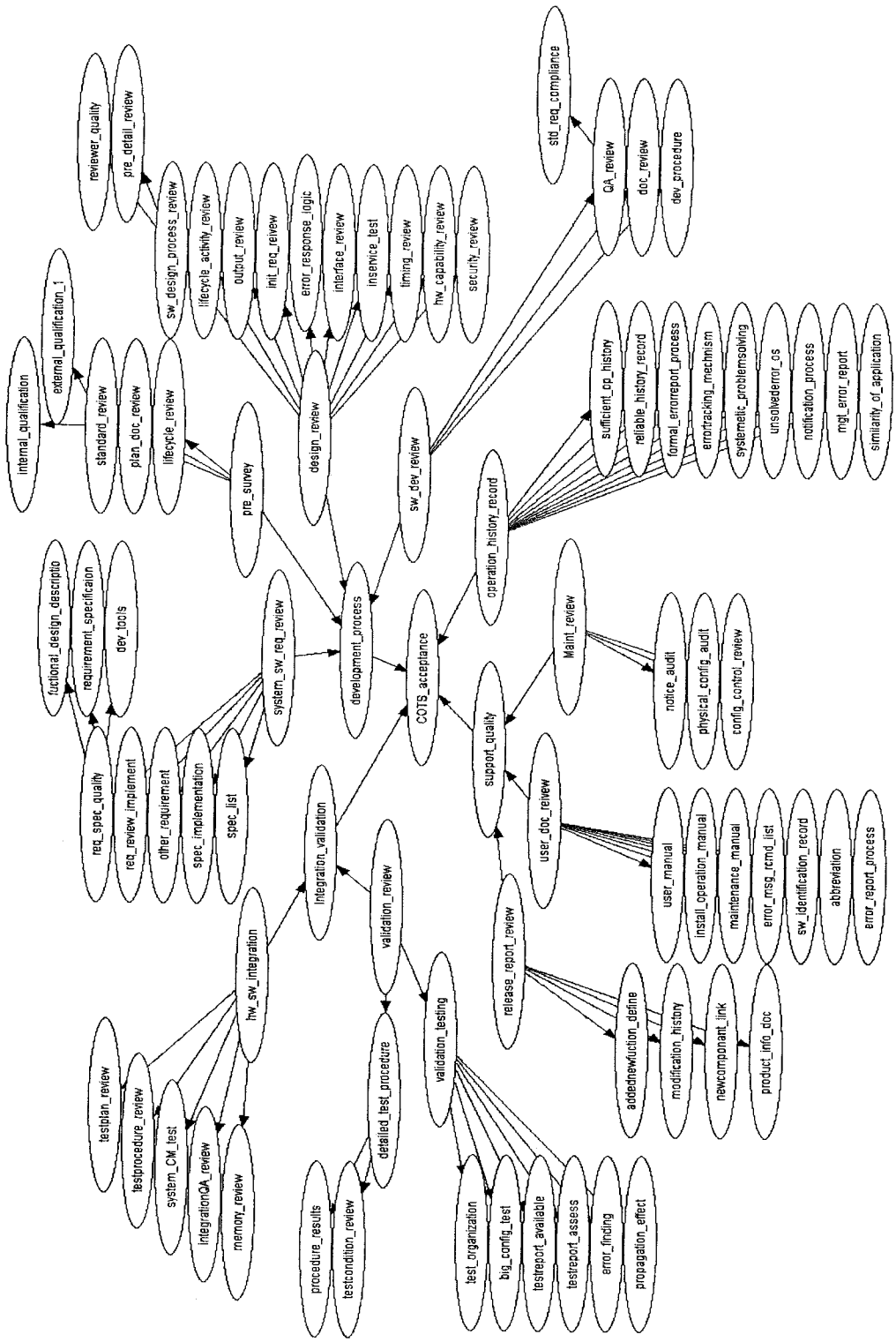


그림 3-91. COTS 평가용 전체 BBN 그래프

표 3-49와 같은 시나리오를 작성하고 각 시나리오에 대한 계산 및 주요 변수를 분석하였다.

표 3-49 COTS 평가용 BBN 분석을 위한 시나리오

시나리오		시나리오 내용	BBN 모델에서 증거 입력 상태
A		초기 상태	어떠한 관찰 값도 입력되지 않은 초기 상태의 BBN
B		최적 경우	모든 측정 가능 노드의 "yes" 상태를 100%로 설정
C		최악 경우	모든 측정 가능 노드의 "no" 상태를 100%로 설정
D	D-1	측정 가능 노드에 관찰된 값을 사용한 경우	1개의 측정 가능 노드에만 부정적 값(no 상태가 100%)이 사용된 경우
	D-2	D-1과 동일	2개의 측정 가능 노드에만 부정적 값(no 상태가 100%)이 사용된 경우
	D-3	D-1과 동일	3개의 측정 가능 노드에만 부정적 값(no 상태가 100%)이 사용된 경우
	D-4	D-1과 동일	4개의 측정 가능 노드에만 부정적 값(no 상태가 100%)이 사용된 경우
	D-5	D-1과 동일	5개의 측정 가능 노드에만 부정적 값(no 상태가 100%)이 사용된 경우
	D-6	D-1과 동일	6개의 측정 가능 노드에만 부정적 값(no 상태가 100%)이 사용된 경우

작성된 모델에 대하여 시나리오들의 값을 적용하여 계산을 수행한 결과, 일반적으로 기본 레벨에 속한 자노드(child node)의 수가 목표노드의 계산 결과에 영향을 미치는 것으로 나타났고, 부정적 관찰 결과를 한 개의 기본 레벨 노드에 적용한 결과와 여러 개의 기본 레벨 노드에 분산하여 적용한 계산 결과는 서로 다르게 나타났으며, 각 기본 레벨에 속한 세부 검토 항목의 일부에 부정적 결과를 적용한 경우에는 목표 노드의 긍정적 상태 "accept" 값이 best case와 차이가 없는 것으로 나타났다.

시나리오별 계산 결과들을 종합적으로 분석해 보면 정성적 평가 방안의 체제를 BBN 모델로 변환할 때에는 자노드의 개수에 대한 조정이 필요한 것으로 나타났고, 모델의 계산 결과들은 실제의 정성적 평가 절차와 기준을 사용하여 전문가가 최종 판단을 내리는 것과 유사하게 나타난 것을 보면(표 3-50 참조) BBN을

이용한 COTS 평가 방안은 현실적인 목적으로도 충분히 사용될 가능성이 있는 것으로 나타났다.

표 3-50 시나리오 "일부 노드에 부정적 값 입력"에 대한 계산 결과

목표 노드: COTS_acceptance		시나리오 D의 경우 목표노드 값					
		D-1	D-2	D-3	D-4	D-5	D-6
상태	<0, 0.00001]	0.6919	0.6908	0.6854	0.5257	0.4718	0.4578
	<0.00001, 0.0001]	0.2527	0.2530	0.2548	0.3072	0.3249	0.3294
	<0.0001, 0.001]	0.0442	0.0447	0.0475	0.1295	0.1573	0.1644
	<0.001, 0.01]	0.0112	0.0114	0.0122	0.0371	0.0455	0.0476
	<0.01, 0.1]	0.0000	0.0000	0.0000	0.0005	0.0007	0.0007
	<0.1, 1]	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000

현실적으로 COTS의 형태는 다양하므로 한 가지 방법으로는 이런 다양한 형태의 제품들을 평가하기가 어려운 실정이다. 본 연구에서는 COTS의 여러 형태를 고려하여 3가지 형태의 COTS 평가 방안을 작성하였다 [엄홍섭, 2003b].

BBN 모델링에서는 전문가의 정성적인 지식/판단을 추출하고 이를 정량화하는 작업이 많이 필요한데 그래프 작성, 노드 확률 테이블 작성, 각 노드의 평가값 작성 등이 그것이다. 현재 안전 SW의 특성상 규칙기반의 정성적 평가가 주류(기존의 규제/표준)이므로 이들 평가 결과를 BBN의 입력 값으로 사용하기 위해서는 확률 값으로 변환하는 작업이 필수적이다. 그러나 이 과정에서 많은 오류나 바이어스가 나올 수 있으므로 이를 사전에 방지하거나 발견/제거하기 위한 기법의 도입이 필요하게 되는데 이에 대한 기본 연구로 지식 추출 기법에 관련된 자료들을 조사 정리하였고, 1) 오류와 바이어스의 사례 수집과 형태/종류별 분류 2) 지식 추출 절차에 대한 가이드를 작성하였다[엄홍섭, 2004c]. 본 연구 결과는 KNICS 원자로 보호 계통 소프트웨어의 요구 명세서 평가용 BBN 모델 구축 작업에 활용되었으며 추후 안전 소프트웨어의 신뢰도나 또는 안전성 평가 등 여러 가지의 BBN 구축에 활용 예정이다.

확률 판단에 영향을 미치는 공통적 문제점(바이어스와 오류)은 다양하며 이

러한 문제점에 대해 충분히 주의를 기울이는 것이 전문가로부터 확률 값을 추출하거나 또는 추출된 확률을 조정하는데 중요하다. 본 연구에서는 지식 공학과 심리학 등 여러 학문 분야에서 확률과 관련된 오류와 바이어스의 사례를 수집하였고 이들을 표 3-51과 같이 분류하였다.

표 3-51 오류/바이어스 분류표

오류/바이어스 형태 구분	대분류	소분류
인지적 오류와 바이어스	대표성	결과의 사전확률에 대한 무감각
		표본 크기에 대하 무감각
		가능성에 대한 오인
		예측성에 대한 무감각
		타당성에 대한 착각
		회귀에 대한 오인
	이용의 용이성	사례의 검색 용이성에 따른 바이어스
		검색 집합의 효율성에 따른 바이어스
		상상의 용이성에 의한 바이어스
		상호 관계의 착각
	조정과 고착	불충분한 조정
		결합사건과 분리사건의 평가에서 나타나는 편중
		주관적인 확률분산의 평가에서 나타나는 고착
	기타	- 결합 오류 - 분산, 공분산, 상관성을 평가할 때의 어려움 - 보수적 경향 - 과신 - 원인과 진단상의 추론에 관련된 오류들 - 확실성의 부인
동기적 오류와 바이어스	사회적 압력	
	잘못된 해석	
	잘못된 설명/진술	
	희망적 사고	
	집단 사고	

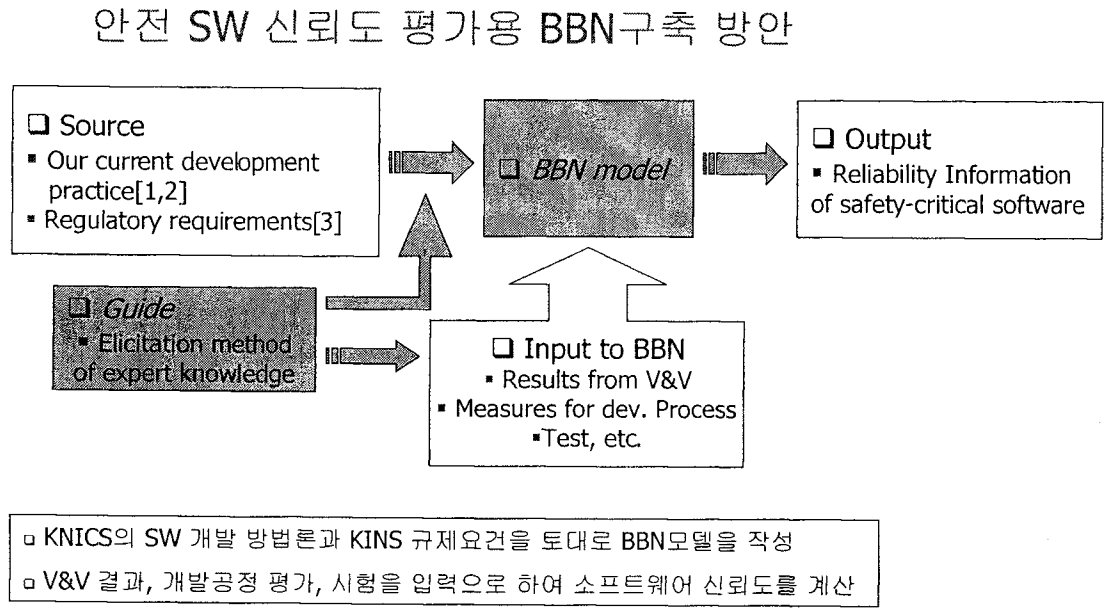
앞에서 나타난 오류와 바이어스를 완전하게 방지하는 체계적인 기법이나 방법론은 아직 개발된 적이 없으며, 다만 케이스별로 적용 가능한 기법이나 지침이 나와 있는 실정이다. 본 연구에서는 안전 소프트웨어 평가용 BBN을 구축하기 위하여 전문가의 지식을 추출할 때 도움이 되는 절차를 가이드 형태로 작성하였다.

이 가이드는 7개의 작업으로 구성되어 있고 각 작업은 수 개의 단계를 포함하고 있는데 각 단계별로 해야 할 일들을 체크리스트 형태로 정리하였고 발생 가능한 문제점들과 그 해결 방안들을 제시하였다.

안전 소프트웨어의 신뢰도/안전성 평가와 같이 높은 불확실성 하에서의 평가에는 필연적으로 전문가의 지식과 판단이 중요한 역할을 하므로, 본 연구에서 작성된 지식/판단의 추출과 관련된 절차 및 기법들은 안전 소프트웨어의 신뢰도 평가용 BBN 모델 작성을 비롯한 다양한 소프트웨어의 평가 업무에 활용할 수 있을 것으로 보인다.

또한, KNICS에서 개발 중인 원전 안전 소프트웨어 요구명세서에 대한 평가를 BBN을 이용하여 수행하였다[엄흥섭, 2004a; 엄흥섭, 2004b; 엄흥섭, 2004d]. 연구 목적은 안전 소프트웨어의 신뢰도 정량 평가를 위한 BBN 모델의 실용성 검증이다. 연구 수행 방안은 다음 그림 3-92와 같고 수행된 연구 범위는 그림의 초록색 부분이다.

종합적이고 실용적인 안전 소프트웨어의 정량적 신뢰도 평가방안을 개발하기 위한 첫 단계로 소프트웨어의 생명주기(life-cycle)를 기반으로 한 상위 레벨 BBN 모델을 구축하였다. 소프트웨어의 생명주기 걸친 품질의 평가는 기존 규제 및 개발방법론의 주류이다. 그림 3-93은 소프트웨어 개발 단계 전체를 포함하는 최상위 레벨 BBN 모델이다. 그리고 그림 3-94는 소프트웨어의 각각의 개발 단계 기본 모델이다. 이들 두 가지의 그래프를 적용하여 작성된 소프트웨어 개발 전체 단계를 포함하는 상위 레벨 BBN 그래프는 그림 3-95와 같다.



[1] V&V Procedure for Software Requirement Specification for Reactor Protection System, KNICS-RPS-(SRS)-SVP121, KAERI KNICS, 2003.
[2] Software Development Plan for Engineering Safety Features, KNICS-ESF-SDP101, KAERI KNICS,
[3] Safety Inspection Guide for KNICS Design, Korea Institute of Nuclear Safety(KINS), Korea

그림 3-92 안전 소프트웨어 신뢰도 평가용 BBN 구축 방안

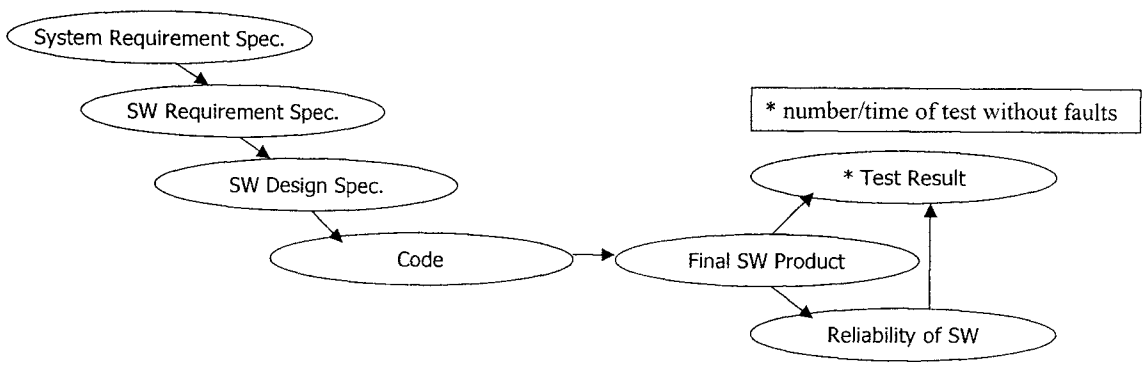


그림 3-93 안전 소프트웨어 신뢰도 평가용 최상위 레벨 BBN 그래프

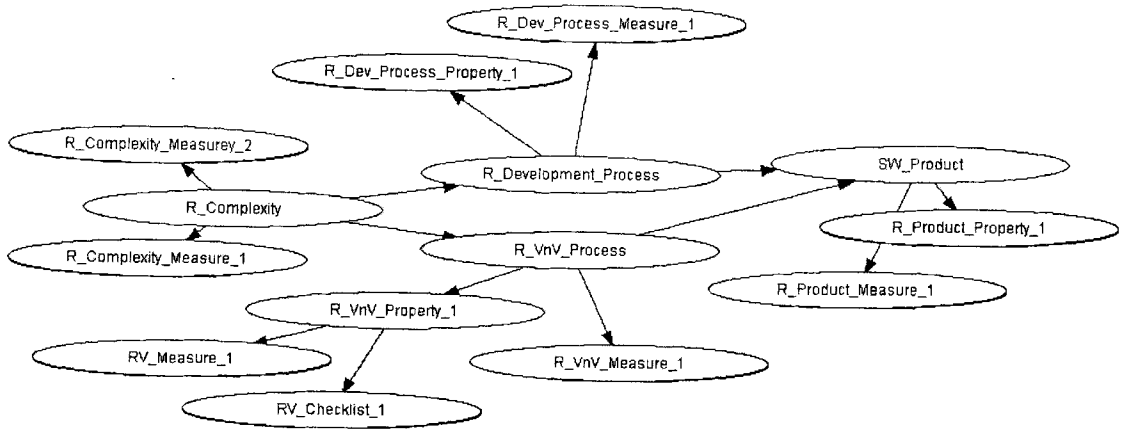


그림 3-94 소프트웨어 개발 주기 중 한 개의 단계에 대한 BBN 그래프

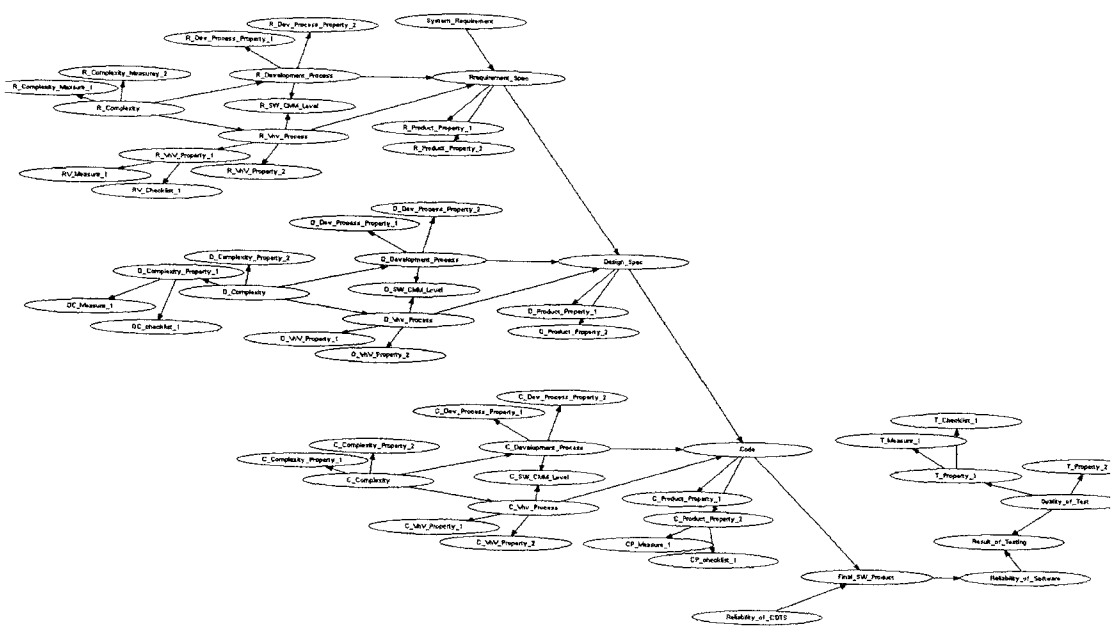


그림 3-95 소프트웨어 개발 전체 단계를 포함하는 상위 레벨 BBN 그래프

KNICS에서 개발 중인 원자로 보호 계통 소프트웨어의 요구사항 명세서에 대한 검증 절차서 및 보고서, 기기 제어 계통 소프트웨어 개발 계획서를 검토하였

고 이로부터 평가에 필요한 120여개의 변수들과 14개 특성(표 3-52 참조)을 도출하였다.

표 3-52 원자로보호계통 소프트웨어의 요구명세서 특성 분류

Properties related to function	Properties related to process
Accuracy	Completeness
Functionality	Consistency
Reliability	Correctness
Robustness	Style
Safety	Traceability
Security	Unambiguity
Timing	Verifiability

전 단계에서 작성된 변수들을 이용하여 요구명세서 평가를 위한 BBN 모델을 구축하였다. 그림 3-96은 상위 레벨 그래프이고 그림 3-97은 일부 특성 노드(Consistency, Correctness, Style)의 서브 그래프이며 그림 3-98은 전체 그래프이다.

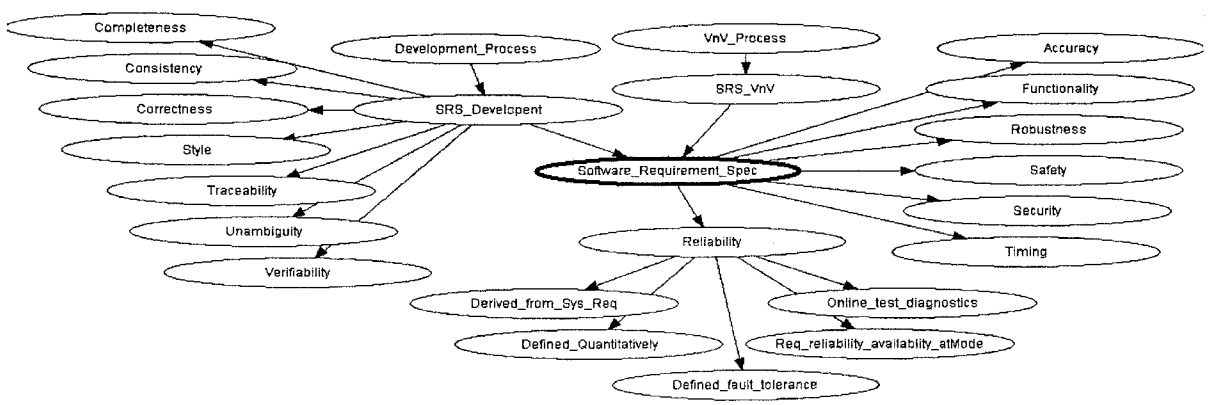


그림 3-96 원자로보호계통 SW에 대한 최상위 BBN Graph: 요구명세 단계

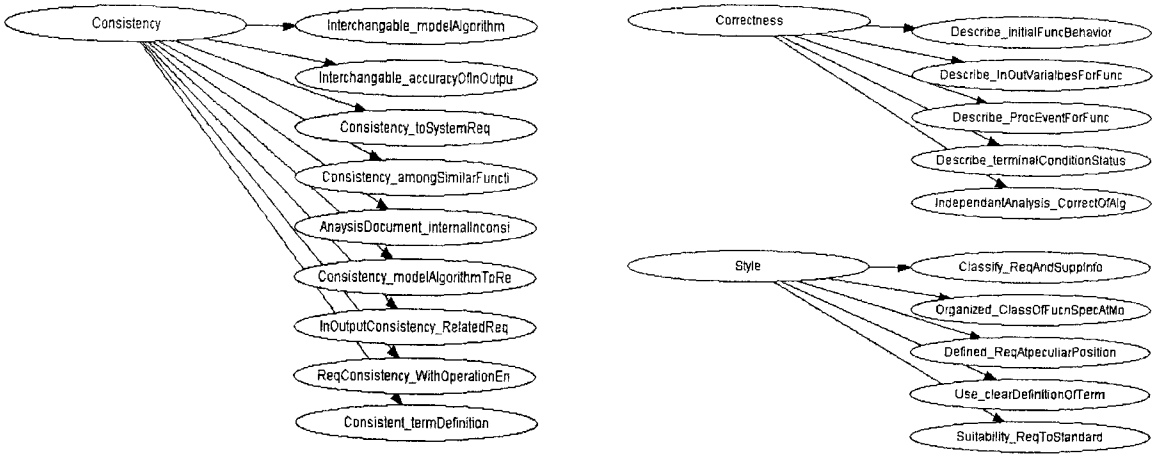


그림 3-97 원자로보호계통 SW에대한 하위 레벨 BBN 모델 중 일부: "Consistency" "Correctness" "Style" 노드

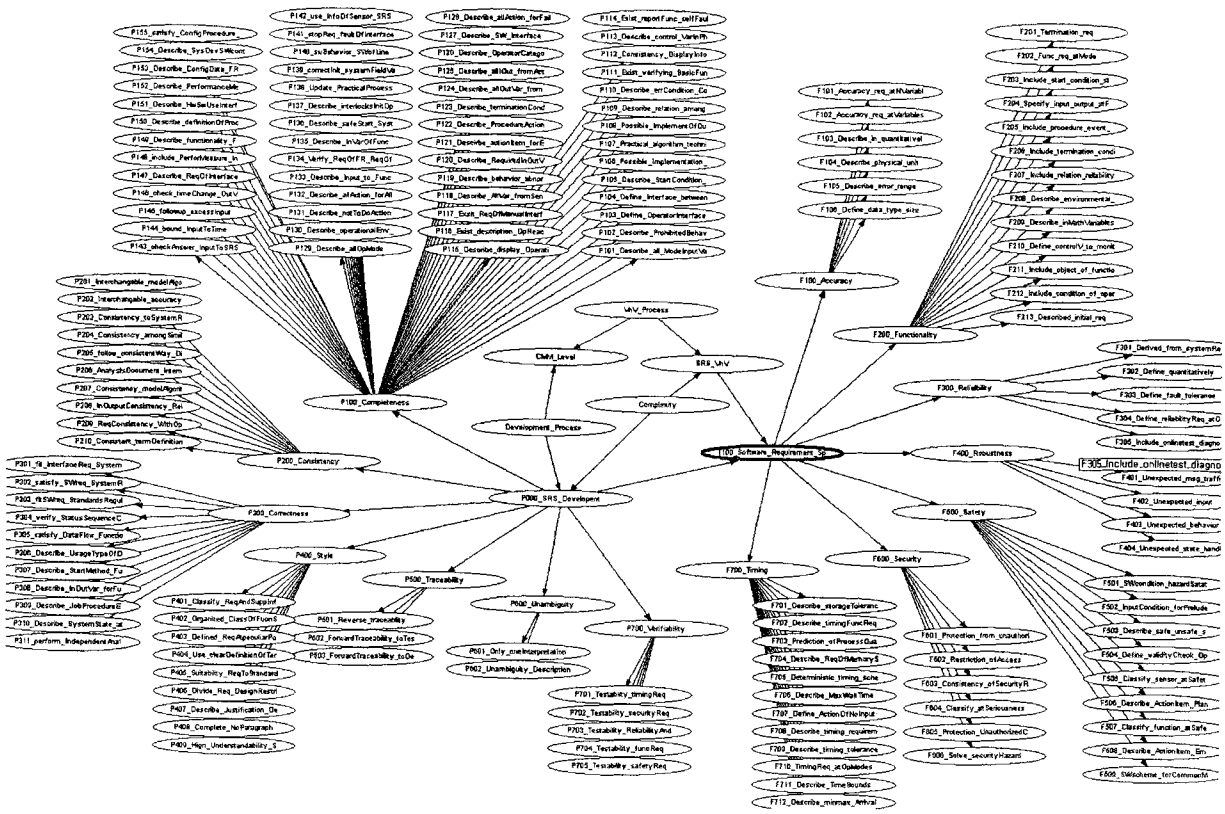
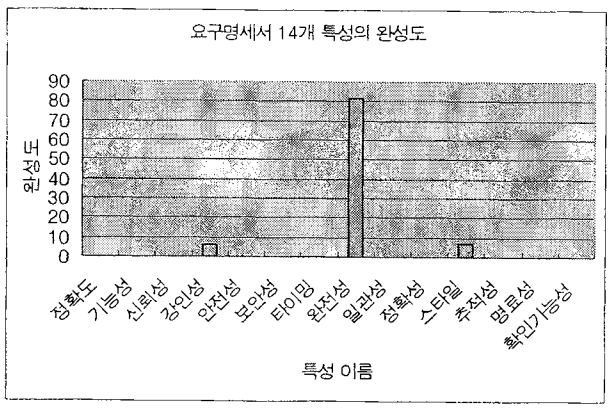


그림 3-98 안전 소프트웨어 요구명세서 평가용 BBN 그래프 전체

V&V 검증보고서의 체크 리스트(150여개 항목)에 대한 전문가의 평가치를 입력으로 하여 모델을 계산하고 분석을 수행하였다. 입력 자료는 체크리스트의 정성적 평가 결과를 정량화하여 사용하였다. 이들 입력 자료를 사용하여 모델을 계산한 결과는 별도로 수행된 V&V 전문가의 정성석인 판단과 유사하게 나타났다. 한편 추후의 개발 및 V&V 관련 의사 결정을 위하여 다양한 "What If" 분석을 수행하였는데 그림 3-99와 그림 3-100은 그 중의 하나로 요구명세서가 목표 수준에 도달하기 위한 각 특성들의 완성도 확률을 보여주고 있다.

Case Study(SW 요구명세서 평가) 결과 정량분석 예

❖ 요구명세서 14개 주요 특성 완성도



특성	상태 값(%)
완전성	81.56
스타일	6.89
강인성	6.61
확인가능성	0.26
신뢰성	0.09
일관성	0.08
정확도	0.06
명료성	0.05
기능성	0.04
안전성	0
보안성	0
타이밍	0
정확성	0
추적성	0

그림 3-99 요구명세서 14대 주요 특성의 완성도

Case Study(SW 요구명세서 평가) 시나리오 분석 예

* 목표 값(95%) 달성을 위한 요구명세서 14개 주요 특성의 예상 값

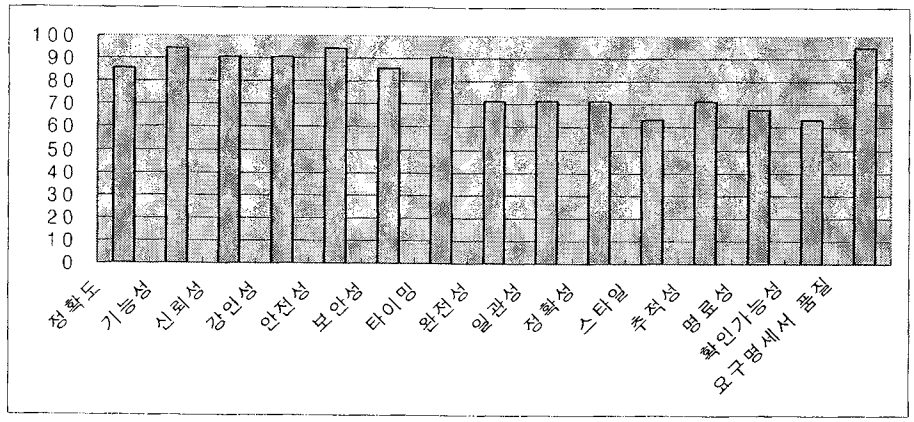


그림 3-100 요구명세서의 완료를 위한 14개 주요특성의 예상 값

다. 고장내구성 기법의 고장 검출률 정량 평가 방법론 개발

원자력 발전소의 디지털 계통은 안전성에 중요한 계통이기 때문에 안전 설계 개념에 따라 다중성과 다양성, 독립성을 가지고 있다. 특히 소프트웨어나 하드웨어에서도 다중성을 가지며 자기 감시 기능 등 여러 가지 고장 내구성 기법들이 적용된다. 이러한 기법들은 고장 시 안전(fail-safe) 설계 개념으로 높은 계통 신뢰도를 기대할 수 있다.

현재 원자력 발전소 디지털 계통에서는 감시타이머를 이용하여 디지털 기기 내의 소프트웨어 등으로 인한 공통 원인 고장에도 효과적으로 대처하고 있다. 그러나 감시타이머를 고장 내구성 향상을 위해 적용하였을 경우, 감시타이머 자체의 신뢰도와 고장 감지 확률이 전체 시스템의 신뢰도에 결정적인 영향을 미치므로 이에 대한 상세한 분석이 요구된다. 이와 함께 감시타이머 이외의 고장내구성 기법을 적용하였을 때 전체 시스템의 신뢰도에 어떤 영향을 미치는지에 대한 상세한 분석이 요구된다.

원자력 발전소 환경에서 디지털 시스템의 노후화(aging) 현상은 방사선 및 습도, 온도 및 오염과 같은 다양한 운영 환경의 조합에 의해 발생한다. 방사선이 전기 및 전자 부품을 통과할 때, 부품 내부에는 내부 전리화(internal ionization)현상이 발생한다. 이러한 현상 중에 가장 대표적인 것은 단일 사건 효과(single event upset, SEU)라고 일컬어지는 현상이다. 습도, 온도 및 오염 등은 전자부품 내부의 절연효과를 내는 물질을 부식시키거나 전도체의 저항을 감소시키거나 증가시킬 수 있다. 이러한 현상에 의해 전자 부품들은 본래의 기능을 서서히 그리고 완전히 상실하거나 일시적으로 그 기능을 상실할 수 있다 [성풍현, 2001].

원자력 발전소 운전 중에 디지털 시스템에서 발생할 수 있는 고장은 다음과 같이 5가지로 분류할 수 있다 [NEA, 1997; Hassan, 1998].

○ 심각한 고장 (Critically Failure)

○ 잠재적 불안전 고장 (Potentially Unsafe Failure)

○ 조건부 안전 고장 (Conditionally Safe Failure)

○ 잠재 고장 (Latent Failure)

○ 안전 고장 (Fail-Safe Failure)

디지털 시스템 부품에서 발생 가능한 고장은 계층별, 기능별, 시간별로 분류가 가능하다 [DBench, 2002; Siewiorek, 1998].

○ 계층별 분류

계층	표현
시스템(System)	프로세서 고장 혹은 불통, 메모리 고장
레지스터(Register)	잘못된 명령어
게이트(Gate)	Stuck at 0 or 1
회로(Circuit)	부품 손실, 단락 혹은 개방, 교차

○ 기능별 분류

이름	부품	신호
기능별	프로세서, 메모리, 스위치, 입출력	데이터 블록
레지스터	레지스터, 조합 회로, 직렬 회로	워드(Word)
게이트(Gate)	논리 게이트, 플립플롭	0, 1
스위치	트랜지스터 스위칭 작용	0, 1, U, Z
전기	트랜지스터, 저항, 축전기	아날로그

○ 지속시간별 분류

이름	부품
영구적 고장 (Permanent Fault)	계속 지속되는 고장
단속적 고장 (Intermittent Fault)	일정하지 않고 주기적이지도 않는 고장,
일시적 고장 (Transient Fault)	짧은 순간에 나타났다가 사라지는 고장

본 연구에서는 조사된 고장 검출률 정량화 방법론 중에서 복합(hybrid) 방법론을 사용하였다. 이 방법은 해석적 방법과 시뮬레이션의 큰 두 축을 가지고 있다. 디지털 계통에서의 고장은 크게 하드웨어 고장과 소프트웨어 고장으로 구분할 수 있는데, 하드웨어 고장의 경우에 대해서는 그 동작이 정적인 구조를 가지고 수학적 모델링이 가능할 경우 이론적 분석을 적용하며, 동작이 동적인 구조를 가질 경우 시뮬레이션을 통한 고장 검출률 정량화를 적용할 수 있다. MIL-HDBK-217F를 이용한 고장률 산출 방법론 및 시뮬레이션을 이용한 방법론은 범용성을 고려하여 하드웨어 묘사(hardware description)를 이용한 고장주입실험 방법론을 선정하였다. 시스템 고장 검출률 개념은 다음과 같다.

$$\text{시스템고장검출률} = \frac{\text{고장률이 가중된 각 부품 고장검출률의 합}}{\text{시스템 고장률}}$$

이는 각 부품의 고장 검출률은 부품 고장률로 가중되어야 한다는 것을 의미한다. 시스템 고장 검출률 산출에 있어서는 각 부품의 고장 특성이 반영이 될 필요가 있기 때문이다. 각 부품 고장률이 서로 독립적이라는 가정 하에 시스템 고장률은 다음과 같이 계산되어질 수 있다. 고장률은 MIL-HDBK-217F를 이용해서 구할 수 있다 [MIL, 1991].

$$\lambda_{system} = \sum_{comp} \lambda_{comp} = \lambda_{CPU} + \lambda_{RAM} + \lambda_{ROM} + \cdots$$

여기서, λcomp : 부품 고장률

λsystem : 시스템 고장률

부품당 고장 검출률은 다음과 같이 구해질 수 있다.

$$C_{comp} = \frac{N_{detected}}{N_{activated,comp}}$$

여기서, Nactivated,comp : 부품내에서 활성화된 고장 개수

Ndetected : 검출된 고장 개수

고장 검출률이 서로 겹치지 않는다는 가정 하에서 가중 고장 검출률은 다음과 같이 나타내어진다.

$$\sum_{comp} C_{comp}\lambda_{comp} = C_{CPU}\lambda_{CPU} + C_{RAM}\lambda_{RAM} + C_{ROM}\lambda_{ROM} + \cdots$$

그러므로 위의 식들을 조합하면 다음과 같은 일반화된 수식을 얻을 수 있다.

$$C_{system} = \frac{\sum_{comp} C_{comp}\lambda_{comp}}{\sum_{comp} \lambda_{comp}}$$

고장 검출률 정량화 방법론을 검증하기 위해 DPPS의 동시논리 프로세서(local coincidence logic processor)를 대상 시스템으로 선정하였다. 그림 3-101은 동시논리 프로세서 내에 있는 2/4 동시논리를 나타내고 있다. 이 프로세서는 AND, OR, NOT 등과 같은 기본적인 논리 연산자로 구성되어 있다. 동시논리 프로세서는 쌍안정 프로세서에서 나오는 여러 신호들을 입력받아 2/4 선택 논리를 수행한다. 만약 2채널 이상이 트립 상태이면 동시논리 프로세서는 트립 신호를 출력한다. 각 동시논리 프로세서에는 기능 손실을 방지하기 위해 감시타이머(watchdog timer)가 부착되어 있다. 각 감시타이머는 시간초과(time-out)설정이

가능하고 프로그램이 수행되는 도중에 주기적으로 재설정이 된다. 동시논리 프로세서는 CPU, PROM, SRAM, I/O로 구성되어 있다. 이 중에서 동시논리 처리 관련 프로그램은 PROM에 저장되어 있다.

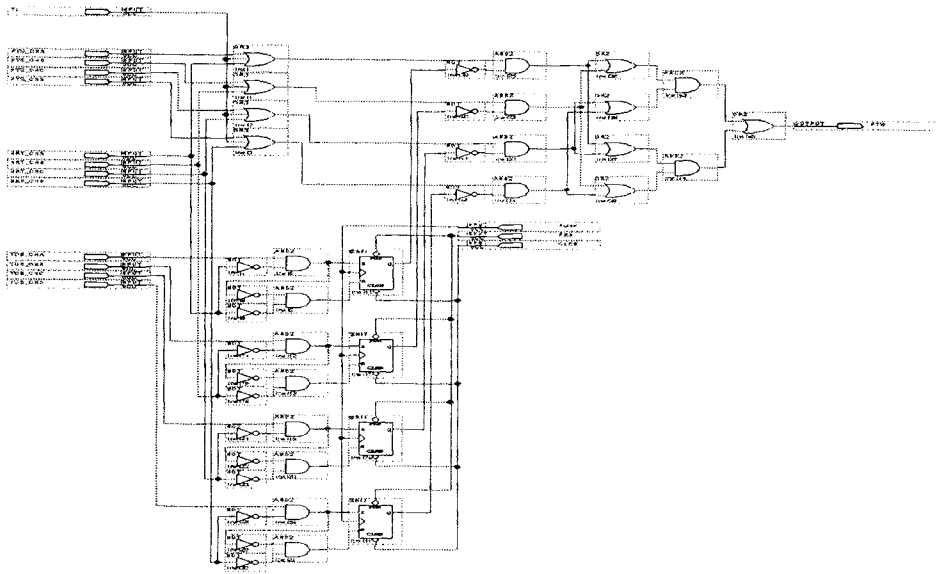


그림 3-101 2/4 동시 논리 회로도 [Westinghouse, 2002]

동시 논리 프로세서를 하드웨어 묘사(hardware description)를 이용하여 구현하였다. 동시논리와 고장검출 프로그램은 ROM에 저장하였다. 동시논리 처리와 고장 검출 신호는 입/출력으로 보내어진다.

앞에서 언급한 듯이 대상 시스템으로 사용된 동시논리 프로세서는 CPU, RAM, ROM, I/O로 구성되어 있다. 그런데 동시논리 프로세서를 하드웨어 묘사법으로 구성하기는 매우 어렵다. 프로세서 내에 들어있는 저항, 콘덴서 등과 같은 것은 아날로그 신호용이기 때문에, 이들은 디지털 신호용으로 사용되는 하드웨어 묘사법을 적용하기 어렵다. 그래서 본 연구에서는 시스템을 CPU, RAM, ROM, I/O로 간략화 하여 하드웨어 묘사를 하였다. 그림 3-102는 단순화된 컴퓨터 구조를 나타내고 있다.

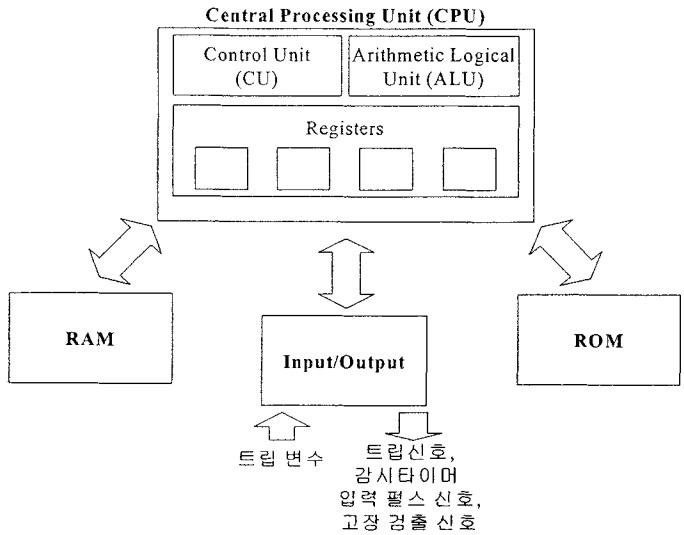


그림 3-102 단순화된 컴퓨터 구조

본 연구에서는 Intel 8051을 CPU로 사용하였다. 2/4동시논리를 수행하기 위해서는 최소 8비트가 필요한데 8051은 이를 충분히 만족하고 또한 현재 원자력 발전소 계측제어 시스템에서 많이 도입되고 있으므로 선택을 하게 된 것이다.

그림 3-103은 8051의 블록선도이다. 8051은 불리언 프로세서(boolean processor), 5~6 인터럽트, 2~3개의 16bit 타이머/카운터, 32개 입출력으로 구성되어 있다. 프로세서 내에는 연산·논리부(arithmetic logical unit, ALU), 제어부(control unit, CU), 레지스터(register)로 구성된다 [ATMEL, 1997]. 단순화된 하드웨어 묘사는 다음의 순서대로 기능이 수행된다 [Tanenbaum, 1984].

○ 다음에 수행될 명령어를 기억장소로부터 불러서 명령어 레지스터(instruction register, IR)에 넣는다.

○ 다음 명령어를 지시하도록 프로그램 계수기를 변화시킨다.

○ 불러낸 명령어의 종류를 결정한다.

○ 명령어에서 데이터를 필요로 하면 그 데이터의 위치를 결정한다.

○ 데이터가 있다면 그 데이터를 채취하여 내부 CPU레지스터로 옮긴다.

○ 명령어를 수행한다.

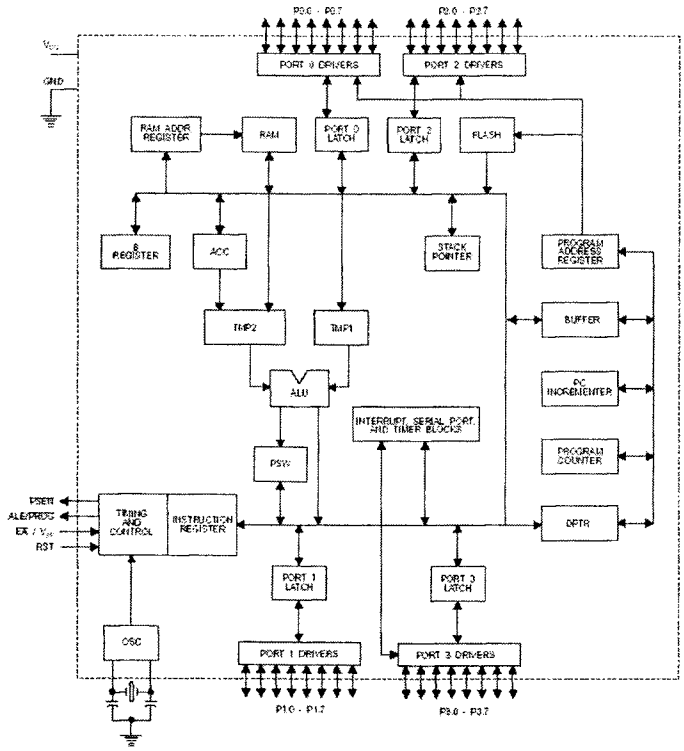


그림 3-103 8051 블록선도 [ATMEL, 1997]

8051을 묘사하기 위해 사용한 언어는 Visual C++이다. Visual C++로 구현된 하드웨어 묘사는 다음과 같다.

○ 헤더 파일(I8051.h)의 구조 : 헤더파일에서는 8051의 내부를 정의하는 부분이다. 여기서는 명령어, 레지스터, 메모리 크기, 입/출력, 비트 함수 등을 정의하였다.

○ 사용한 소스파일(i8051.cc)의 구조 : 이 파일에서는 8051의 대부분의 기능을 수행하는 곳이다. 여기서 Simulate 함수가 8051 대부분 기능을 담당하는 곳이다.

○ 소스 파일 내에서 핵심적인 기능을 수행하는 함수 구조 : 이 함수에서는 8051의 기능을 수행하도록 하였다. 몇몇 기능은 별도의 함수로 구성하여 서로 간에 데이터 교환이 이루어지도록 하였다.

본 연구에서는 영구 고착(stuck-at) 고장이 시스템에서 발생할 수 있는 고장으로 선택하였다. 앞장 고장 분류내 고장 지속성에 따른 종류에서 고장은 영구 고장, 일시 고장, 단속 고장으로 분류될 수 있다고 하였다. 그런데 원자력 발전소에서 사용되고 있는 안전 관련 디지털 시스템은 중복성(redundancy)을 갖도록 설계되므로 일시 혹은 단속고장의 영향은 무시될 수 있다 [강현국, 2002a]. Stuck-at 고장은 한 개의 핀이 0 혹은 1 논리로 고정되는 것을 말한다. 이 고장 모델은 상대적으로 간단하므로 많이 사용되고 있다. 본 연구에서는 stuck-at 고장을 주입하기 위해 고장 주입법(fault injection)을 사용하였다. 그림 3-104와 3-105는 stuck-at 고장 주입의 예를 보여주고 있다. 이 그림에서 1바이트의 원본 데이터를 AND 혹은 OR 연산을 통해 비트 하나가 0 혹은 1로 고정되어지는 것을 볼 수 있다. 이러한 연산이 하드웨어 묘사 프로그램 실행 중에 계속 수행되게 하여 영구 고장의 효과가 나도록 하였다.

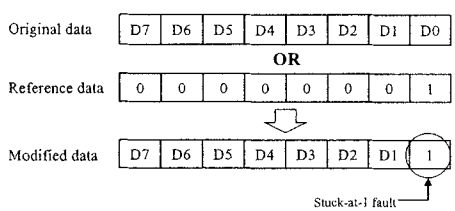


그림 3-104 Stuck-at 1 고장

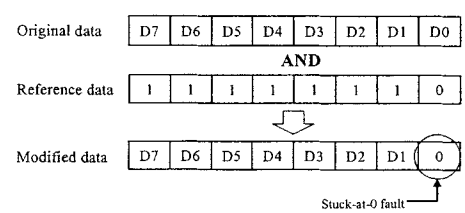


그림 3-105 Stuck-at 0 고장

본 연구에서 사용한 고장 검출 방법은 감시타이머(heartbeat-watchdog timer), ROM 검사합(ROM checksum), RAM 데이터 검증(RAM data verification), 패리티 비트(parity bit), 레지스터 쓰고 읽기(register write and read) 및 이들을 통합하는 방법이다 [Iyer, 2004; Siewiorek, 1998]. 각각의 방법들은 다음과 같이 요약할 수 있다.

○ 감시타이머(heartbeat-watchdog timer) : 감시타이머는 고장 검출하는 방법 중에서는 그다지 비싸지 않아서 오래전부터 사용되어져왔다. 시스템에서 나오는 신호가 프로세서와는 별도로 부착된 타이머에 의해 계수되어 시스템을 감시한다. 만약 프로세서로부터의 펄스 응답이 없으면 감시타이머는 시스템에 고장이 난 것으로 판단하고 정지시킨다.

○ ROM 검사합(ROM checksum) : 그림 3-106은 ROM 검사합 개념도를 나타낸다. ROM 검사합은 ROM내의 데이터들을 모두 더한 값을 이용한다. ROM내의 데이터를 모두 더해서 데이터의 가장 끝에 위치한 검사합 코드와 비교해 그 결과가 상이하면 고장이 발생한 것으로 판단한다.

○ RAM 데이터 검증(RAM data verification) : 그림 3-107은 RAM 데이터 검증의 개념을 나타내고 있다. RAM 데이터 검증은 메모리 쓰고 읽기가 무결한지 검사하기 위한 것이다. 여기에서는 가장 낮은 비트부터 높은 비트까지 1비트씩 쓰고 읽기를 수행하여 결함의 유무를 검사하였다. 이 방법을 사용하면 stuck-at 고장은 물론 다른 유형의 고장도 검사해낼 수 있다.

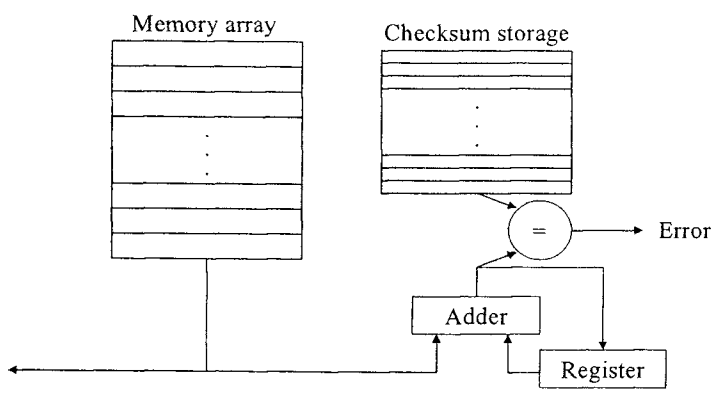


그림 3-106 ROM 검사합 [Siewiorek, 1998]

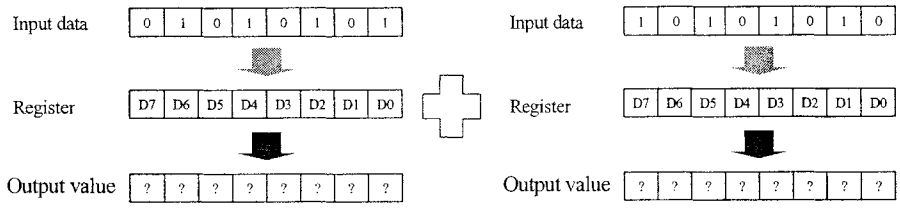


그림 3-107 RAM 데이터 검증

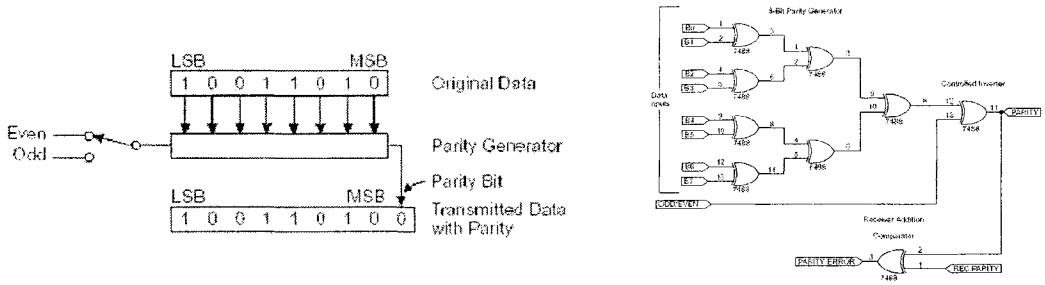


그림 3-108 패리티 비트 [Siewiorek, 1998]

○ 패리티 비트(parity bit) : 그림 3-108은 패리티 비트의 개념을 나타내고 있다. 패리티 비트는 부가적인 2진 비트로 2진 데이터가 요구되어지는 패리티를 만족하는지 검사하여 0 혹은 1의 값을 출력한다. 만약 주어진 데이터 집합에서 1의 개수가 짝수이면 짝수 패리티라고 정의한다. 만약에 1의 개수가 홀수이면 홀수 패리티라고 정의한다. 8051의 경우 내부 프로그램 상황(program status word, PSW)을 나타내는 모듈이 있는데 여기에서 누산기(accumulator, ACC)의 패리티를 제공한다. 만약 누산기의 계산에 문제가 발생하면 패리티 비트가 서로 일치하지 않으므로 고장을 검출해낼 수 있다.

○ 레지스터 쓰고 읽기(register write and read) : 레지스터는 CPU내에 있는 용량은 작으나 고속처리가 가능한 기억장치이다. 레지스터 읽고 쓰기는 각 비트를 0 혹은 1을 쓰고 출력한 값이 일치하는지를 검사하는 방법으로 RAM 데이터 검증과 유사하다. 만약 비트에 쓴 값과 읽은 값이 서로 같지 않으면 고장이 발생한 것으로 시스템이 판단하여 고장을 검출해낼 수 있다.

○ 통합 방법 (integration) : 몇 가지의 고장 검출 방법들을 통합시키면 단일 고장 검출 방법과 비교하여 고장 검출률을 높일 수 있다. 여기에서는 감시 타이머, ROM 검사합, RAM 데이터 검증을 통합시켜 고장 검출률이 얼마나 높아지는지 알아보았다.

표 3-53은 고장 주입 실험에 사용한 실험 변수를 정리한 것이다. 이 실험에서는 CPU에 336개, RAM에 1,050,608개, ROM에 1,048,576개, I/O에 64개 고장이 주입되었다. 고장 검출 방법은 앞에서 소개한 6개의 방법이 사용되었고, 결과는 고장 활성화율, 고장 검출률, 고장 내구성 서술 블록선도도 나타내었다.

그림 3-109는 ROM에 저장되어 있는 프로그램의 흐름도이다. 프로그램이 시작되면 먼저 초기화가 되고 다음에 시스템 고장 유무를 검사한다. 여기에서 고장이 검출되면 바로 시스템이 정지가 된다. 고장 유무 조사에서는 감시타이머 이외의 고장 검출 방법이 사용된다. 시스템에 고장이 없다고 판단되면 2/4 동시논리가 수행된다. 만약 감시타이머 방법이 적용되는 경우 2/4동시논리가 수행되고 나면 heartbeat신호가 시스템으로부터 출력되어 감시타이머로 전달된다.

그림 3-110은 결과를 평가하기 위한 흐름도이다. 시스템의 출력신호 중에서 고장 검출신호가 출력되면 고장이 검출된 것으로 판단한다. 만약 검출이 되지 않으면 시스템 트립 신호에 문제가 발생하였는지 여부를 조사하여 발생하였으면 고장 검출 실패로 판단한다. 트립 신호에도 문제가 발생하지 않으면 프로그램 흐름을 분석하여 이 부분이 문제가 발생하면 고장은 내구화된 것으로, 여기에서도 아무런 문제가 발생하지 않았으면 고장은 비활성화된 것으로 판단한다.

표 3-53 고장 검출률 정량화를 위한 실험 변수

고장종류	영구고장	
프로그램	2/4 동시논리 + 고장검출 알고리즘	
고장모델	stuck-at (0, 1) 고장	
고장위치	CPU	336
	RAM	1,050,608
	ROM	1,048,576
	I/O	64
고장검출방법	감시타이머, ROM 검사합, RAM 데이터 검증, 레지스터 쓰기 읽기, 패리티비트, 통합화 방법	
결과분석	고장 활성화율, 고장검출률, 고장내구성 서술 블록선도	

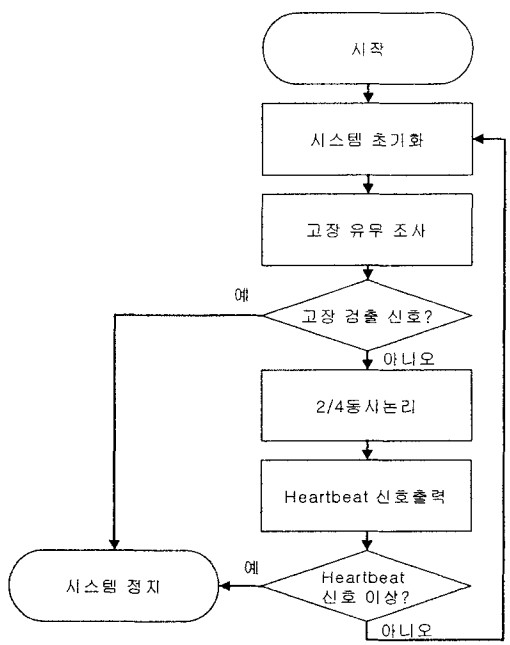


그림 3-109 프로그램 흐름도

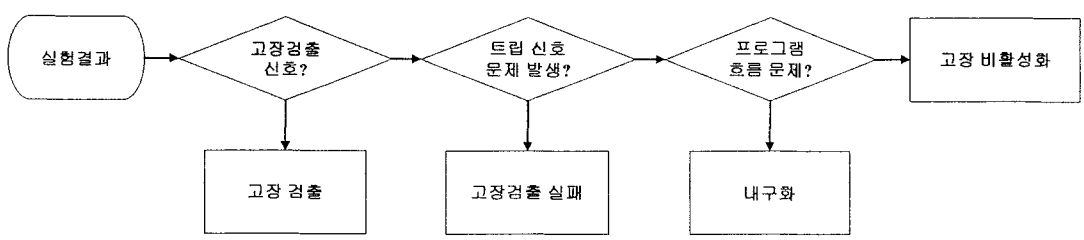


그림 3-110 실험 결과 평가 흐름도

MIL-HDBK-217F를 사용하기 위해 다음과 같은 환경에서 시스템이 동작하고 있다고 가정하였다. 이로부터 계산되어진 각 부품 고장률은 표 3-54에 나타내었다.

○ 시스템은 ground benign(GB)에서 동작하고 있다.

○ 시스템에서 사용되고 있는 부품은 JANTX에 의해 선택되었다.

○ 시스템 주변 온도는 35도이다.

○ 유지, 보수 작업은 없다.

표 3-54 각 부품 고장률

	CPU	RAM	ROM	I/O
Failure Rate (failures/10^6Hours)	0.0356408	0.0108750	0.0073163	0.0549125

실험결과로부터 시스템의 고장 내구 특성을 나타내기 위해 몇 개의 서술 블록으로 구성된 고장 내구성 서술 블록선도를 도입하였다. 그림 3-111은 고장 내구성 서술 블록선도를 나타낸다. 각 서술 블록의 내용은 다음과 같다 [Amendola, 1997; Arlat, 1993].

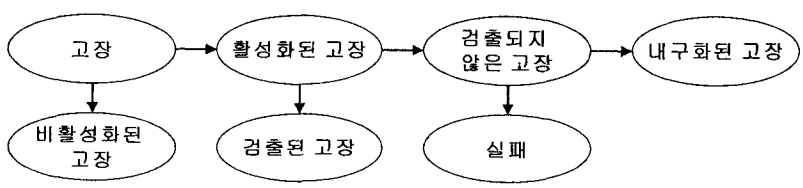


그림 3-111 고장 내구성 서술 블록선도

○ 비활성화 고장 : 고장이 쓰이지 않는 부분에 주입이 되면 그 고장은 활성화

되지 못하고 시스템 기능 수행에 아무런 영향을 미치지 않는다.

○ 활성화된 고장 : 고장이 시스템 기능 수행에 어떤 영향을 미쳤을 때 이를 활성화된 고장으로 보았다. 활성화된 고장은 검출된 고장과 비검출 고장으로 나누어진다.

○ 검출된 고장 : 고장이 검출 방법들에 의해 검출된 경우이다. 여기서는 감시타이머 시간초과와 고장 검출 신호 출력을 고장이 검출된 경우로 보았다.

○ 비검출된 고장 : 고장이 검출방법에 의해 검출되지 못한 경우이다. 이 경우는 내구화 고장과 실패로 나누어진다.

○ 내구화 고장 : 고장이 활성화되었는데 검출이 되지 않았고 출력에도 아무런 영향을 미치지 않은 경우이다. 본 연구에서는 고장에 의해 프로그램 흐름이 감시타이머 혹은 고장 검출 신호 출력에 아무런 영향을 미치지 않을 정도로 바뀐 경우를 내구화되었다고 판단하였다.

○ 실패 : 고장이 활성화되었는데 검출이 되지 않았고 그 출력도 정상적인 경우와 다른 경우이다. 본 연구에서는 고장이 주입되었을 때 트립신호 출력이 정상적인 시스템의 트립신호 출력과 다른 경우 실패로 보았다.

고장 주입 실험에 앞서 동시논리가 저장되어 있는 시스템의 입력에 대한 출력을 Quartus를 이용해서 확인하였다. 그림 3-112는 Quartus를 이용해서 동시논리의 신호를 검사한 결과이다.

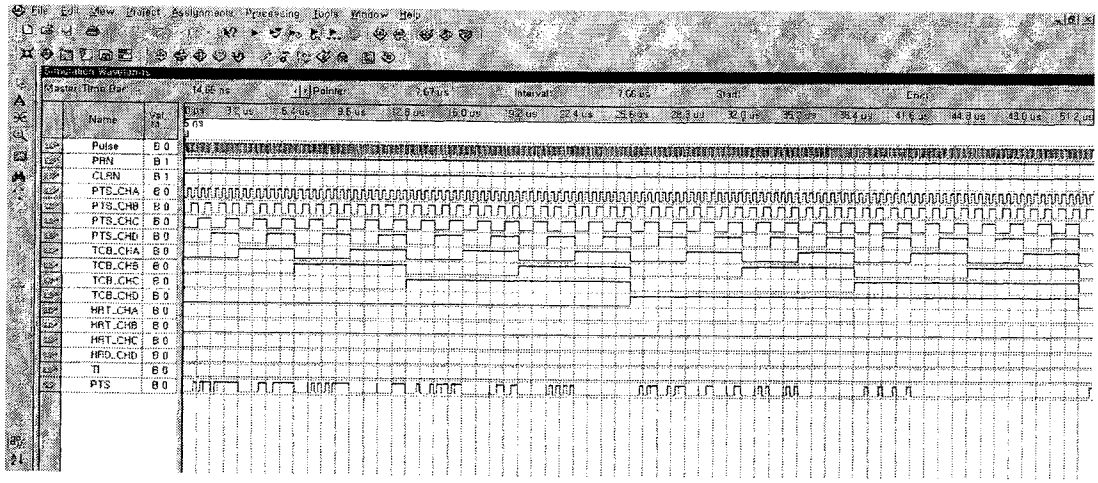
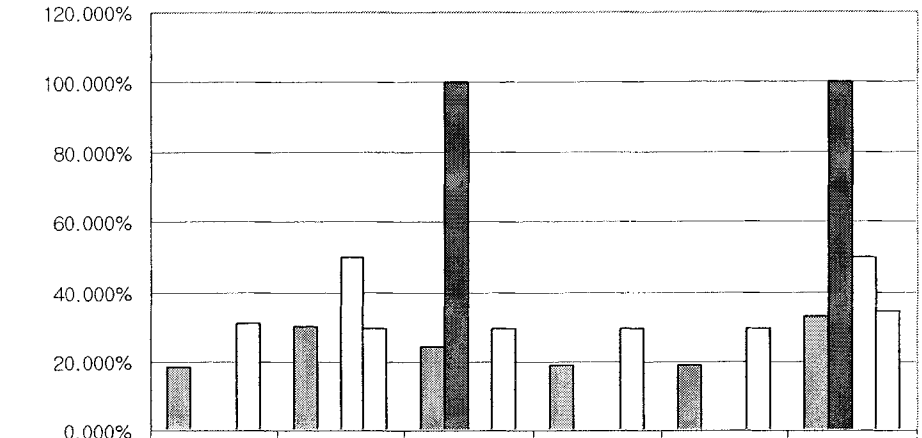


그림 3-112 Quartus를 이용한 동시 논리 신호 검사 결과

그림 3-113과 그림 3-114는 활성화된 고장의 비율을 부품, 시스템별로 나타낸 것이다. 통합화 방법이 다른 방법에 비해 높은 활성화된 고장 비율을 나타내고 있다. 감시타이머, 패리티비트, 레지스터 쓰고 읽기는 21%정도이다. 앞에서 설명하였듯이 통합화된 방법은 감시타이머, ROM 검사합, RAM 데이터 검증의 조합이므로 각각의 고장 활성화 특성이 복합적으로 나타나게 되어서 고장 활성화 비율이 높게 나온 것으로 생각된다.



	감시타이머	ROM 검사합	RAM 데이터 검증	패리티 비트	레지스터 쓰고 읽기	통합화
CPU Fault	18.452%	30.060%	24.405%	18.750%	19.048%	33.036%
RAM Fault	0.017%	0.015%	100.000%	0.012%	0.017%	99.962%
ROM Fault	0.204%	49.998%	0.195%	0.144%	0.204%	49.995%
I/O Fault	31.250%	29.688%	29.688%	29.688%	29.688%	34.375%

그림 3-113 고장 활성화율 (부품별)

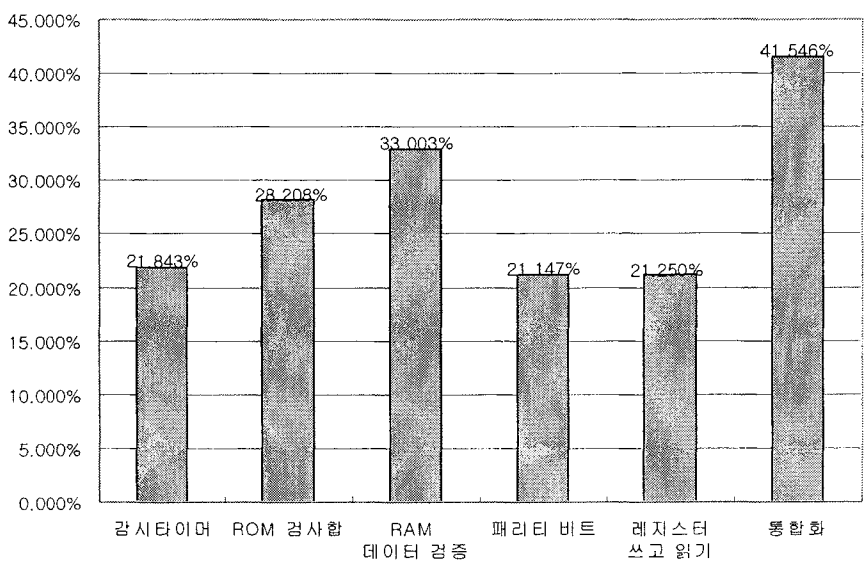


그림 3-114 고장 활성화율 (시스템)

RAM 데이터검증을 사용하는 경우 RAM에 주입된 대부분의 고장은 대부분 활성화가 되었다. 이는 RAM 데이터 검증이 각 비트를 검사하기 때문에 고장이

시스템 동작에 영향을 미치지 않더라도 그것을 검사할 수 있기 때문이다.

ROM 검사합을 사용하는 경우 ROM의 고장 활성화율은 약 50%이다. 이는 Stuck-at 0 고장이 ROM의 쓰이지 않은 부분에 발생하는 경우 검사합 결과에는 아무런 영향을 미치지 않으므로 고장이 활성화되지 못한다.

감시타이머나 패리티비트, 레지스터 쓰고 읽기는 ROM과 RAM의 고장이 그다지 영향을 미치지 못한다. 감시타이머는 프로그램 수행 이상을 감지해내므로 ROM이나 RAM의 쓰이지 않는 부분에 고장이 주입되면 프로그램 수행에는 아무런 문제가 없으므로 낮게 나온 것이다.

그림 3-115는 각 부품의 고장 검출률 그림 3-116은 시스템 고장 검출률을 보여준다. 통합화 방법이 다른 방법에 비해 가장 높은 고장 검출률을 보여준다. 위에서 설명한 바와 같이 통합화 방법은 3개의 고장 검출 방법이 조합된 것이므로 3개의 특성이 모두 다 나타나기 때문에 높게 나온다.

감시타이머는 다른 방법에 비해 CPU 고장 검출률이 높게 나온다. CPU에서 발생한 고장은 수치 혹은 논리 연산 수행 이상 등으로 인해 시스템이 무한 루프에 빠져 시스템 시간 초과의 원인이 되므로 감시타이머에 의해 고장이 검출된다.

ROM 검사합은 감시타이머 다음으로 고장 검출률이 높다. 검사합은 ROM에서의 고장이 시스템에 영향을 미치지 않더라도 그 고장을 검출할 수 있다. 이 방법은 ROM을 주로 검사하는 방법인데도 불구하고 다른 부품 고장 즉 CPU나 RAM 고장의 경우에도 상당히 검출률이 상당히 높다. 이는 CPU나 RAM의 고장이 ROM 검사합 결과에 영향을 미친다는 것을 의미한다.

RAM 데이터 검증은 RAM고장에만 효과가 있음을 알 수 있다. RAM내 프로그램 실행에 쓰이지 않는 고장이 주입된다고 하더라도 그 고장은 검출될 수 있다. 그러나 이 방법은 다른 부품 특히 ROM의 고장은 검출하지 못한다. 이로 인해 RAM의 고장을 거의 100%검출한다고 하더라도 시스템 고장 검출률은 검사합이나 감시타이머에 비해 낮게 나온다.

레지스터 쓰고 읽기는 RAM고장에 약간 효과적이다. 이는 레지스터가 CPU

와 RAM사이에 위치하고 있고 RAM과의 데이터 통신을 많이 하기 때문이다. 그러므로 RAM의 고장은 레지스터 쓰고 읽기 검사에 상당한 영향을 미치게 되므로 이의 고장 검출률이 높게 나온다.

패리티 비트는 다른 방법에 비해 비효율적이다. CPU, RAM 고장 검출률은 15%대이나 다른 부품은 10%도 되지 않는다. 그러므로 이 방법은 고장 검출 방법으로는 부적합하다고 볼 수 있겠다.

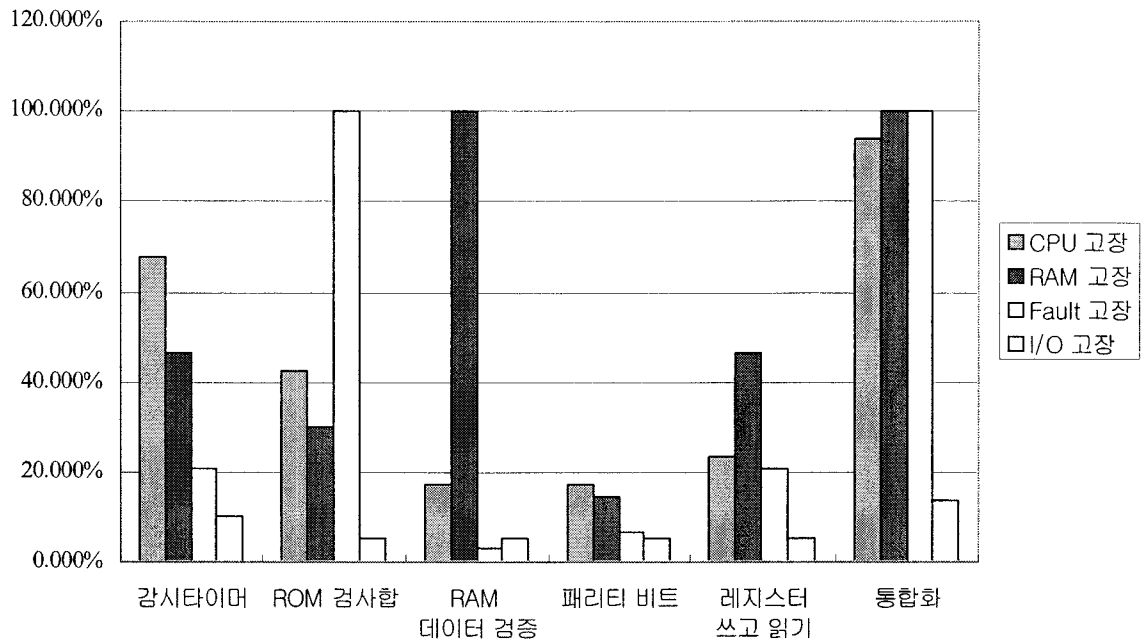


그림 3-115 고장 검출률 (부품별)

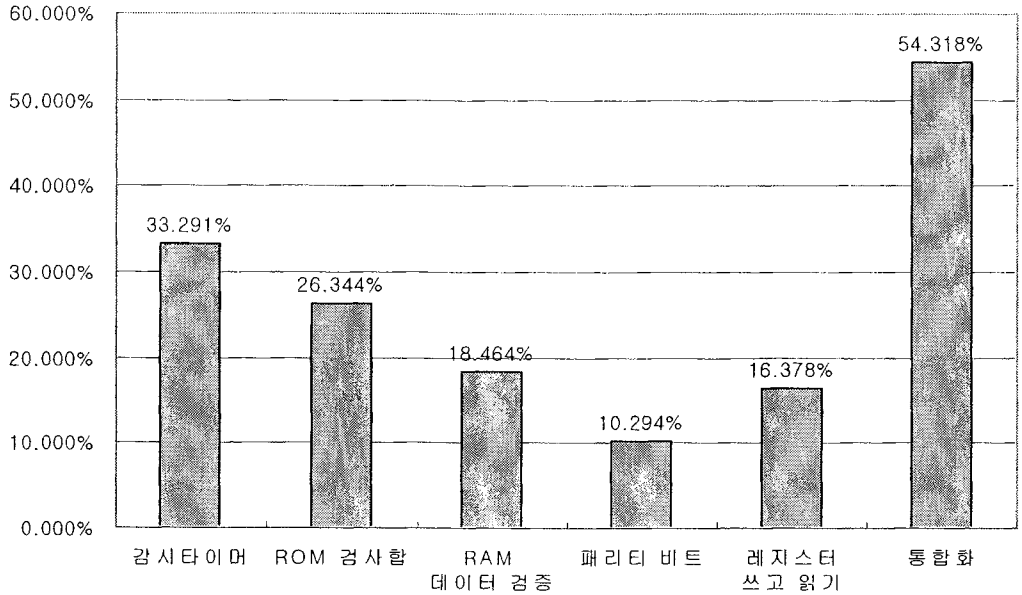
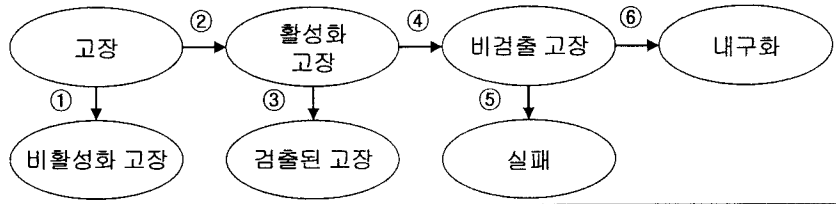


그림 3-116 고장 검출률 (시스템)

고장내구성 서술 블록선도는 시스템의 고장내구성 특성을 한눈에 알아볼 수 있도록 하기 위해 고안된 것이다. 이 블록선도로부터 고장으로부터 실패까지의 과정을 보다 쉽게 파악할 수 있다. 표 3-55는 실험으로 나온 자료를 분석하여 고장내구성 서술 블록선도로 나타낸 것이다. 비활성화 고장 서술 블록에서는 감시타이머, 패리티 비트, 레지스터 쓰고 읽기 검사가 높은 값을 가진다. 통합화 방법의 비활성화 고장 비율은 낮다.

검출된 고장에서는 통합화 방법이 6개의 방법 중에서 가장 높은 반면에 패리티 방법은 매우 낮다. 앞에서 설명하였듯이 통합화된 방법은 고장 검출 방법들을 통합한 것으로서 그 특성들이 복합적으로 나타나기 때문에 이와 같이 높게 나온다. 이에 반해 패리티 비트는 CPU, ROM, RAM의 대부분의 고장을 검출해내지 못한다.

표 3-55 고장내구성 서술 블록선도



	①	②	③	④	⑤	⑥
감시타이머	78.157%	21.843%	33.291%	66.709%	97.094%	2.906%
ROM 검사합	71.792%	28.208%	26.344%	73.656%	98.311%	1.689%
RAM 데이터 검증	66.997%	33.003%	18.464%	81.536%	97.680%	2.320%
패리티 비트	78.853%	21.147%	10.294%	89.706%	97.934%	2.066%
레지스터 쓰고 읽기	78.750%	21.250%	16.378%	83.622%	98.733%	1.267%
통합화	58.454%	41.546%	54.318%	45.682%	72.267%	27.733%

고장활성화율과 고장 검출률의 비교는 시스템 평가에 있어서 중요하다. 감시타이머와 통합화 방법은 고장 활성화율에 비해 고장 검출률이 높게 나온다. 그러나 다른 방법들은 활성화 고장 비율이 고장 검출률 보다 높게 나온다. 특히 RAM 데이터 검증은 활성화 고장 비율이 33.003%인데 비해 고장 검출률은 18.464%로 상당히 낮다. 이는 RAM 데이터 검증 방법이 고장을 많이 활성화시키나 그것의 검출은 그다지 높지 않다는 것을 의미한다. 그런데 고장검출 방법에 있어서 통합화 방법은 고장 검출률을 높이는 데는 효과적이나 통합화를 하기 위해서는 관련 프로그램이 더 추가되어야 하기 때문에 이로 인해 고장 활성화율이 높아진다. 그런데 감시타이머는 상대적으로 간단한 구조로 인해 고장 활성화율은 낮으면서 고장 검출률이 높게 나온다. 따라서 감시타이머는 다른 방법에 비해 효율적인 방법인 것을 알 수 있다. 여기서 효율적으로 보다 적은 고장 활성화로 더 많은 고장을 검출하는 것은 신뢰성 있는 고장 내구 시스템 설계에서 중요한 요소임을 알 수 있다.

만약 고장이 고장 검출방법에 의해 검출되지 않으면 대부분의 경우 시스템은 실패가 된다. 즉, 검출되지 않은 고장은 시스템을 잘못된 기능을 수행하게 한다. 6개의 고장 방법 중 통합화된 방법이 약 72% 실패율을 가지지만 나머지는 약 97%이상의 실패율을 가진다. 이 결과로부터 고장을 효율적으로 가능한 많이 검출해야 시스템 실패를 방지할 수 있다는 것을 알 수 있다.

제 4 장 연구개발 목표 달성도 및 대외 기여도

제 1 절 연구개발 목표 달성도

본 과제는 PSA 현안 기술 문제의 해결을 위한 중.장기 연구로서 원자력 연구개발 사업 제 2단계 (2002.4 - 2005.2; 2년 11개월간) 연구기획 결과에 따라 요구된 RFP 연구개발 목표와 내용에 충실한 연구를 수행하였고, 표 4-1에 기술된 바와 같이 분야별 단계 연구 목표는 충실히 달성되었다.

공개 발표된 연구 성과로는 국외 SCI 저널 논문은 7편 (2편은 투고 중), 국내 저널 4편 (2편은 투고 중)을 게재하였으며, 20편의 국제 컨퍼런스 논문발표, 23편의 국내 학술 논문 발표, 기술 보고서 16편 발간, 프로그램 1건 등록 등 활발한 학술활동을 수행하였고. 대과제 차원에서 추진된 PSA 연구회 개최(2003.10, 용평), PSA 실무 교육(2003.9, 2004.7 각 2주간, 한수원 직원 대상), PSA 관련 저술(1건) 및 원자력연수원 교재 작성(1건) 등에서 타 세부과제와 역할 분담하여 참여하였다. 또한, 2건의 기술이전 실시 계약(RPS/ESFAS 상세모델을 한국과학기술원과 한기(주)로 각각 기술 실시)을 체결하였으며, 특히 디지털 계통의 원전 위험도 영향 평가 모델은 원전 계측제어 시스템 개발단 (KNICS), 한기(주), 삼창(주)에서 디지털 계통/기기 설계 평가 및 개선과 관련 직접 이용되었거나 기술자문을 시행한 바 있다.

표 4-1 주요 연구 개발 실적 및 목표 달성도

세부연구목표	주요 연구개발 실적	가중치 (%)	연구목표 달성도 (%)	비고
o 정지/저출력 (LPSD) 1단계 내부사건 PSA 방법론 개선 및 위험도 관리 기반 기술 개발	o 표준원전 LPSD PSA 모델 등급평가 - 영광 5,6호기 대상 LPSD PSA 모델 등급 평가 (국내외 전문가 참여, 8개 분야 218개 ANS 요건 기준) o LPSD PSA 기반기술 개선 - LPSD PSA용 최적 열수력 거동분석 체계 (MARS V2.1 체계, 모든 POS에 대한 정지냉각상실사고 분석 체계) - LPSD 초기사건 자료 분석 및 DB 개발 (국내외 총 625건) - 초기사건분석 방법 개선 o 표준원전 LPSD PSA 표준모델 시범 개발 - 모델 개선(10여개의 1등급 항목의 개선: LPSD 특성 기인자 분석, 사건수목 개정, 표준 공정 재분석, 등) - LPSD 고유의 열수력 상세 분석 (중력급수, 저온 과압 사고, PSV 개방고착사고, 관류 냉각 현상) o LPSD 위험도 관리 기반 기술 개발 - 운전모드별 기기배열 위험도관리용 시범 모델 (POS 1,2) - 초기사건 DB 검색 프로그램 (LEDB)	50	100	정지/저출력 1단계 PSA 모델의 품질 등급 향상을 위한 기반기술 개선 및 시범 적용을 통하여 정량적 위험도 관리에 필요한 기술 확보
o 디지털 계통의 위험도 평가 기술 개발	o 발전소 위험도 영향평가 모델 개발 - 울진 5,6호기 디지털 RPS 상세 신뢰도 분석 모델 (총 15종의 정지변수) - 울진 5,6호기 디지털 ESFAS 상세 신뢰도 분석 모델 (총 7종의 ESF 작동신호) - 디지털 계통의 CDF 및 LERF 영향 평가 시범 모델 - 디지털 ATWS 빈도 평가 상세 모델 - 디지털 주요 인자에 대한 민감도 분석 - 디지털 특성 조건기반 HRA 평가 방법 o 공통원인고장(CCF) 분석 방법론 개발 - 소프트웨어 신뢰도 평가 방법 기초 연구 (BBN 기법의 타당성 연구) - 디지털 기기의 CCF 그룹핑 기법 o 고장내구성기법의 고장범위 정량화 방법론 연구 - Hybrid 방법 개발 및 검증 (시뮬레이션 결과와 기기 고장률 가중치의 결합 모형)	50	100	디지털 계통의 원전 위험도 영향 평가 모델 및 현안 요소기술의 성공적 개발을 통하여 후속기의 디지털 설계 및 인허가 지원 기반 확충
총 계		100	100	

제 2 절 대외 기여도

본 연구는 한국 표준형 원전을 대상으로 위험도 정보 활용 의사결정을 위한 PSA 수행 기술상 현안 문제로 대두된 두 개의 분야인 정지/저출력 PSA와 디지털 안전계통 위험도 평가 기술 분야를 다루었고, 본 연구를 통하여 **국내 환경에 적합한 고유 PSA 수행기술을 확립**하는 것은 물론 **국제적인 선도 연구**를 수행하였다.

정지/저출력 운전모드에서는 많은 정비 활동으로 인하여 다중방어 개념이 약화되고 위험도 관리 기술의 부족으로 원전 안전성이 저하되는 것을 방지하여야 한다. 특히, 국내 가동원전의 증가와 원전 운영자의 경제성 제고를 위한 정지 기간 단축 노력에 따라 정지 공정 최적화를 통한 효율적인 위험도 평가 및 관리가 절실히 요구되는 시기로, 본 과제에서 연구 개발된 결과물들은 정지/저출력 PSA 표준 모델과 정지/저출력 위험도 정보 활용 기반 기술로서 차등 품질 보증 (GQA; Graded Quality Assurance), 가동 중 정비 (OLM; On-line Maintenance) 등 가까운 미래에 요구될 고난도의 PSA 응용 분야에 직접 기여할 것으로 판단된다. 다음은 정지/저출력 PSA 기술 개발 분야에서 도출된 세부 연구 결과물들 가운데 이미 활용되고 있거나 현재 예상되는 주요 대외 기여도를 기술한 것이다.

- ○ 정지/저출력 PSA 품질 등급 평가로 국내 정지/저출력 PSA 기술의 기준점 역할과 기술 개발의 방향 제시
- ○ 정지/저출력 PSA의 4 개 분야 - 발전소 운전 상태(POS; Plant Operation Status) 분석, 초기 사건 분석, 사고 경위 분석, 성공 기준 분석 분야 - 에서의 모델 개선 결과는 PSA 모델의 품질 등급 향상으로 위험도 정보 활용 의사결정에 활용 가능
- ○ 정지/저출력 운전 중에 발생한 초기 사건 자료들의 DB화 (625건) 및 DB 검색/분석 프로그램 (LEDB)의 개발로 초기사건 저감을 위한 기반을 마련함으로서 원전 안전성 향상에 기여

○ MARS2.1을 이용한 순수 국내 기술 기반의 정지/저출력 PSA용 최적 열수력 분석 모델 구축함으로서 기술 국산화 및 정지/저출력 운전모드에 대한 MARS 코드 검증용으로도 활용 가능.

○ 정지/저출력 고유 특성을 반영한 상세 열수력 분석 모델 및 결과들은 향후 정지/저출력 PSA 수행 시 사고경위별 성공 기준 결정에 직접 활용 가능함으로서 PSA 품질 개선에 기여

○ 계획 정비 기간 중에 예상되는 가압기 안전밸브 (PSV; Pressurizer Safety Valve) 개방 고착 사고에 대한 상세 열수력 분석 결과를 이용하여 제안된 PSV 설정 압력 시험 방식 개선안은 원전 안전성 향상에 기여

○ 부분 충수 운전 (mid-loop operation)에서의 정지 냉각 상실 사고 발생 시 중력 급수 능력에 대한 상세 열수력 분석 과정에서 새롭게 개발된 역지밸브의 유량 모델은 실험 결과와 비교 분석을 통한 우수성이 인정되어 기존 MARS 코드의 보수성 개선을 위해 버전 3.0부터 기본 모델로 채택될 예정임.

본 연구에서 개발된 디지털 계측 제어 위험도 평가 기술 및 모델은 인허가 등 산업체 및 규제기관의 요구가 많은 기술 분야이다. 동시에 디지털 기기의 관련 기술은 매우 빠른 속도로 발달되고 있기 때문에 새로운 기기·설계·알고리듬의 안전성을 체계적으로 보다 정확히 평가할 수 있는 기법의 개발은 원전에서의 디지털 기술 도입을 촉진하여 궁극적으로 원전 안전성 및 경제성 향상에 크게 기여할 것으로 기대된다. 또한, 디지털 기술의 원전 도입에 대해서도 본 과제에서 개발된 디지털 PSA 기술을 이용한 보다 체계적인 정량적 안전성 검증은 원전에 대한 국민 수용성 증진에 기여할 것으로 판단된다. 다음은 디지털 PSA 기술 개발 분야에서 도출된 세부 연구 결과물들 가운데 이미 활용되고 있거나 현재 예상되는 주요 대외 기여도를 기술한 것이다.

○ 본 과제의 디지털 PSA 기술 개발 결과들은 디지털 기술의 원전 도입에

따른 안전성 영향을 종합적으로 정량 평가할 수 있는 기반 기술로 설계개발자나 규제자로 하여금 계통 성능의 관점만이 아닌 원전 전체 위험도의 관점에서 디지털 관련 최적 의사결정을 가능하게 함으로서 원자력 안전성 향상에 기여.

○ 본 과제에서 시범 구축된 울진 5,6호기 DPPS/DESFAS 상세 신뢰도 모델과 관련한 기술들은 타 산업계에서 많이 수행되지만 원자력 발전소와 같이 위험도 관점에서의 평가 사례는 없으므로 우주항공, 고속철도, 군수산업 등과 같은 고-신뢰도 뿐 만 아니라 안전성도 강조되는 산업 분야에서 활용성이 클 것으로 예상되어 이로 인한 산업 파급효과 및 관련 기술 인프라 구축에 기여

○ 디지털 계통의 발전소 위험도 영향 평가 모델 개발로 원전 계측제어 시스템 개발단 (KNICS)의 디지털 기기 국산화, 후속호기와 차세대 원전에 도입되는 디지털 계통의 설계 최적화 및 인허가 지원에 기여

○ 원자력 디지털 안전 기기의 대부분이 채택하고 있는 고장내구성 설비/기법에 대하여 본 과제에서 개발된 고장 검출 범위 정량화 방법은 고-신뢰도 디지털 안전기기의 설계에 직접 활용 가능하며, 나아가 타 산업체로의 기술 파급 효과가 클 것으로 판단됨

○ BBN (Bayesian Belief Net) 기법을 이용한 소프트웨어 신뢰도 평가 방법은 현재 KNICS 원자로 보호 계통의 소프트웨어 요건 단계에 대해 적용 평가하였으며, 평가 결과는 안전 필수 소프트웨어에 대한 인허가에 기여

제 5 장 연구 개발 결과의 활용 계획

제 1 절 정지/저출력 PSA 기술 개발 결과의 활용

정지/저출력 PSA 분야의 모든 연구 결과물들은 위험도 정보 활용 의사결정이 가능한 수준의 정지/저출력 PSA 품질 향상을 위한 기반기술로서 정량적 위험도 관리 도구 개발의 실용화에 직접 활용될 계획으로 차기 단계 (2005.3 - 2007.2; 2년간)에서 개발될 기기 배열 위험도 관리모델을 통하여 구체화될 것이다 (**원자력 안전성 향상에 기여**). 특히, 위험도 정보 활용 분야 가운데 국내에서 가까운 미래에 적용될 계획인 하이 레벨의 응용 분야 - 예를 들면, 차등 품질 보증, 가동 중 정비, 위험도 정보 활용 설계, 등등 - 에서는 필수적으로 요구되는 기술로서 활발히 활용될 전망이다. 정지/저출력 PSA 기술 개발 분야에서 보다 구체적인 연구 결과들의 세부 활용 계획은 다음과 같다.

o 한국 표준형 원전 정지/저출력 PSA 품질 등급 평가 및 모델 개선

한국 표준형 원전인 영광 5,6 호기의 정지/저출력 PSA 모델에 대한 품질 등급 평가 결과는 국내 유관 기관들의 정지/저출력 PSA 기술 기준점으로 활용되고 있으며, 향후 산업체의 PSA 수행과 관련하여 보완 기술 개발의 방향타 역할을 할 수 있을 것으로 판단된다. 또한, 품질 등급 평가 결과에 따라 본 과제에서 수행된 4개 분야 - 발전소 운전 상태 (POS) 분석, 초기 사건 분석, 사고 경위 분석 및 성공 기준 분야 - 에서의 PSA 모델 개선 결과는 향후 차기 단계에서 본격 개발 예정인 기기배열 위험도 관리 모델의 입력 자료로 직접 활용될 계획이다.

o 정지/저출력 PSA용 최적 열수력 거동 분석 체계

원자력 중장기 연구 사업을 통해 한국원자력연구소에서 개발된 MARS 2.1 코드를 이용하여 순수 국내 기술기반의 정지/저출력 PSA용 최적 열수력 거동 분석 체계를 구축함으로써 기반 기술의 인프라 확충 및 국산화에 기여하였고, 체계를 구성하는 입력 자료 및 해석 결과는 기존 원전 및 후속기 정지/저출력 PSA

수행 시 산업체에서 직접 활용이 가능하다. 부수적으로 정지/저출력 운전모드에 대한 최적 열수력 분석 체계 구축 과정에서 MARS 코드의 오류를 코드 개발팀으로 피드백 하였을 뿐만 아니라 향후 MARS 코드의 정지/저출력 열수력 분석 능력 검증용으로 활용함으로써 기초 기술의 국제 경쟁력 향상에 기여할 것이다.

o 고유의 정지/저출력 운전 특성에 대한 상세 열수력 거동 분석

정지/저출력 고유의 현상학적 불확실성을 저감하기 위해 본 과제에서 수행된 상세 열수력 분석 결과 - 가압기 안전밸브 (PSV) 개방 고착 사고, 중력 급수 능력 해석, 관류냉각 현상, 저온 과압 (LTOP) 사고 - 들은 차기 단계의 기기배열 위험도 관리 모델의 개발과 향후 산업체에서 기존 원전 및 후속기 정지/저출력 PSA 수행 시 사고 경위 분석의 불확실성 저감을 위해 직접 활용될 것이다. 특히, 한국 표준형 원전 정지/저출력 PSV 개방 고착 사고에 대한 상세 열수력 분석 결과를 통하여 제안된 PSV 설정 압력치 시험 방식 개선안은 한수원에서 현재 검토 중에 있으며, 중력 급수 능력 해석 과정에서 개발된 역지 밸브의 모델은 MARS 코드 버전 3.0 의 기본 모델로 이용될 예정이다.

o 정지/저출력 초기사건 DB 검색/분석 프로그램

본 과제에서는 세계 각국의 가압 경수로 (PWR)와 비등 경수로 (BWR)의 정지/저출력 운전 경험 자료로부터 총 625 건의 초기 사건들을 데이터베이스화 하였고, 이를 검색/분석할 수 있도록 전산 프로그램 (LEDB; Low power and shutdown Event DataBase)을 개발하였다. 이 결과들은 산업체의 가동 중 원전 및 후속기의 초기사건 저감을 위한 연구 토대가 될 것이다.

제 2 절 디지털 I&C PSA 기술 개발 결과의 활용

본 과제의 디지털 PSA 기술 개발 결과들은 디지털 기술의 원전 도입에 따른 안전성 영향을 종합적으로 정량 평가할 수 있는 기반 기술로 설계개발자나 규제자로 하여금 계통성능의 관점만이 아닌 원전 전체 위험도의 관점에서 디지털 관련 최적 의사결정을 가능하게 한다(**원자력 안전성 향상에 기여**). 디지털 PSA

기술 개발 분야에서 보다 세부적인 연구 결과들의 활용 계획은 다음과 같다.

o 디지털 안전 계통 (DRPS 및 DESFAS)의 상세 신뢰도 분석

국내에서 최초로 디지털 기술이 안전 계통에 적용된 울진 5,6 호기의 디지털 원자로 보호계통 (DRPS; Digital Reactor Protection System)과 디지털 공학적 안전설비 작동 계통 (DESFAS; Digital Engineered Safety Feature Actuation System)에 대한 상세 신뢰도 분석 모델은 한국 원전 계측제어 시스템 개발단 (KNICS)에 제공되어 디지털 기기별 계통 설계 영향 평가와 설계 개선에 활용되고 있는 중이며, 울진 5,6 호기의 디지털 계통 운영 개선 및 후속기의 디지털 계측제어 계통의 설계 최적화 및 인허가 지원에도 활용될 것이다. 또한, 디지털 계통의 성능/신뢰도 평가들은 타 산업계에서도 수행한 경험이 있긴 하지만 원자력 발전소와 같이 위험도 관점에서의 평가 사례는 발견되지 않으므로 우주 항공, 고속 철도, 군수 산업 등과 같은 고(high)-신뢰도 뿐 만 아니라 고-안전성도 강조되어야 하는 산업분야에서 디지털 PSA 기술의 적용이 확대될 것이다 (산업 파급효과 및 인프라 구축에 기여).

o 디지털 계통의 원전 위험도 영향 평가 모델

상기의 울진 5,6 호기 DRPS/SESFAS 계통 신뢰도 분석 모델과 표준 원전 위험도 감시용 PSA 모델과 결합하여 개발된 디지털 계통의 발전소 위험도 영향 평가 모델 (노심 손상 빈도 및 대량 조기 방출 빈도 모델)은 KNICS의 디지털 기기 국산화, 후속기와 차세대 원전에 도입되는 디지털 계통의 설계 최적화 및 인허가 지원에 활용 가능하다 (최적 설계 및 인허가 지원에 활용). 또한, 세계 최초로 디지털 안전 관련 계측제어 계통을 포함한 PSA 모델을 구축한 결과로 2004년 6월 OECD CSNI의 디지털 계측제어 관련 회의에서 연사로 초청 받은 바 있듯이, 향후 디지털 PSA 분야의 세계 기술 선도 역할에 적극 활용할 계획이다.

o 소프트웨어 신뢰도 평가 방법론 연구

본 과제에서 개발된 BBN (Bayesian Belief Net) 기법을 이용한 소프트웨어 신뢰도 평가 방법은 현재 KNICS의 소프트웨어 요건 단계에 대하여 적용 평가를

완료하였고, 평가 결과는 KNICS 안전 필수 소프트웨어에 대한 인허가에 직접 활용될 것이다. 또한 향후 차기 단계에서 KNICS의 안전 필수 소프트웨어 개발 전 주기에 따라 - 예를 들면, 설계 단계, 코딩 단계, 통합 단계, 등 - BBN 기법의 적용 연구가 계속될 계획이며, 이 때 개발된 방법론 및 절차들은 분석의 기본 토대로서 활용 될 것이다(기반기술 확충).

o 고장내구성 기법의 고장 검출 범위 정량화 방법 연구

원자력 디지털 계측제어 기기/계통에 채택된 고장내구성(fault tolerance) 설비 또는 기법에 대하여 본 과제에서 개발된 고장검출범위 (fault coverage) 정량화 방법은 고-신뢰도 디지털 안전 관련 계측제어 기기의 설계 평가 및 개선에 직접 활용 가능하며, 나아가 타 산업체의 고품질 디지털 기기 개발을 위한 설계 검증 기술로 활용될 것이다.

제 6 장 연구개발 과정에서 수집한 과학 기술 정보

제 1 절 해외 과학 기술 정보

[Amendola, 1997] Amendola, L. Impagliazzo, P. Marmo, and F. Poli, "Experimental Evaluation of Computer-Based Railway Control Systems", in Proceeding 27th Int. Symposium on Fault-Tolerant Computing (FTCS-27) Seattle, WA, USA, June 1997, pp. 380-384.

[Ang, 1995] M.L. Ang, et al., A Shutdown Probabilistic Safety Assessment for Sizewell B Nuclear Power Plant, SUV Futher Education Course on Safety of Nuclear Power Plants during Shutdown, 1995

[ANS, 2002] "Low-Power and shutdown PRA Methodology standard" Draft, 2002. ANS

[Arlat, 1993] J. Arlat, A. Costes, Y. Crouzet, J. Laprie, and D. Powell, "Fault Injection and Dependability Evaluation of Fault-Tolerant Systems", IEEE Transactions on Computers, Volume 42, Number 8, August 1993, pp. 913-923.

[Asaka, 1998] H. Asaka, Y. Anoda, Y.Kukita, and I.Ohtsu, Secondary-Side Depressurization During PWR Cold Leg Small Break LOCAs Based on ROSA-V/LSTF Experiments and Analyses, J. Nuclear Science and Technology, Vol. 35, pp.905 1998

[ATMEL, 1997] "AT89C51 Datasheet", ATMEL, 1997.

[Bellcore, 1997] Bellcore Standard TR-332, Issue 5, Reliability prediction procedure for electronic equipment, 1997.

[Beveridge, 1985] R.L. Beveridge, et al., A Probabilistic Safety Analysis of Boron Dilution Events at Millstone Unit 3, Proc. International Topical

Meeting on Probabilistic Safety Methods and Applications, EPRI NP-3912-SR, Vol. 3, 1985, pp.1661-1669.

[Butler, 1993] R. W. Butler and G. B. Finelli, The Infeasibility of Quantifying the Reliability of Life-Critical Real-Time Software, R.W. Butler, IEEE Transactions on Software Engineering, 19(1), 1993

[Burchill, 1982] W. E. Burchill, Physical Phenomena of a Small-Break Loss-of-Coolant Accident in a PWR, Nuclear Safety, Vol. 23 1982

[Choi , 1998] S. S. Choi, S. H. Chang, D. H. Lee, "Automating Stragegies of Emergency Operation for Optimal Shutdown in Pressurized Water Reactors", IEEE Transactions on Nuclear Science, Vol. 45 1998

[Chu, 1988] T.L. Chu, et al., Improved Reliability of Residual Heat Removal Capability in PWRs as Related to Resolution of Generic Issue 99, NUREG/CR-5015, BNL-NUREG-52121, Brookhaven National Lab., 1988.

[Chu, 1994] T.L. Chu, et al., Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Surry Unit-1, NUREG/CR-6144, BNL-NUREG-52399, Vols. 1-6, Brookhaven National Lab., 1994.

[Ciesielski, 2004] Dave Ciesielski, Phil Liddle, "Qualified Software Tools For Safety I&C Applications", NPIC&HMIT 2004, Columbus, USA, 2004.

[CRANE, 1988] CRANE, "Flow of Fluids through Valves, Fittings, and Pipe", Chicago, St , 1988

[Crosby, 1989] Crosby, "Pressurizer Safety Valve Design Drawing, C-N95471". 1989

[DBench, 2002] Fault Representativeness, "Deliverble ETDI2 of Dependability Benchmarking Project(DBENCH)", IST-2000-25245, 2002.

[Diamond, 1990] D. J. Diamond, C. J. Hsu, R. Fitzpatrick, "Reactivity

Accidents-A Reassessment of Design-Basis Events," NUREG/CR-5368, U.S. Nuclear Regulatory Commission, January 1990.

[Diamond, 1992] D. J. Diamond, P. Kohut, H. Nourbakhsh, K. Valtonen, P. Secker, "Probability and Consequences of Rapid Boron Dilution in a PWR," NUREG/CR-5819, U.S. Nuclear Regulatory Commission, June 1992.

[EPRI, 1988] Electrical Producers Research Institute, "Application Guidelines for Check Valves in Nuclear Power Plants", EPRI NP 5479 Project 2233-20, Palo Alto, California., 1988

[Han, 2003] S. J. Han, H. G. Lim, J. E. Yang, Thermal Hydraulic Analysis of Aggressive Secondary Cooldown in Small Break Loss of Coolant Accident with Total Loss of High Pressure Injection, 2003, NURETH-10 2003

[Hassan, 1998] M. Hassan, W.E. Vesely, "Digital I&C Systems in Nuclear Power Plants-Risk-Screening of Environment Stressors and a Comparison of Hardware Unavailability With an Existing Analog System", NUREG/CR-6579, 1998.

[Holderness, 1985] J.H. Holderness, et al., Brunswick Decay Heat Removal Probabilistic Safety Study, NSAC-83, Nuclear Safety Analysis Center, 1985.

[HSE, 1998] Health and Safety Executive, The use of computers in safety-critical applications, London, HSE books, 1998.

[IEC, 1998] Functional safety of electrical / electronic / programmable electronic safety-related systems, IEC-61508, IEC, 1998

[IEC, 2001] Nuclear power plants - Use of probabilistic safety assessment for the classification of instrumentation and control function, IEC -61838 TR, Ed. 1, IEC, 2001

[ISL, 2003a] Information Systems Laboratories, "RELAP5/MOD3.3 Code Manual Vol. I, Code Structure, System Models, and Solution Method", Rockville, Maryland/Idaho Falls, Idaho 2003

[ISL, 2003b] Information Systems Laboratories, "RELAP5/MOD3.3 Code Manual Vol. I, Code Structure, System Models, and Solution Method", Rockville, Maryland/Idaho Falls, Idaho 2003

[Iyer, 2004] Ravishankar K. Iyer, Zbigniew Kalbarczyk, "Hardware and software error detection", http://citeseer.ist.psu.edu/585103.html

[Jacobson, 1989] S. Jacobson, "Some Local Dilution Transients in a Pressurized Water Reactor," Thesis, No. 171, Linköping Studies in Science and Technology, November 1989.

[Jeong, 1999a] Jeong, J. -J., Ha, K. S., Chung, B. D., Lee, W. J., "Development of A Multi-dimensional Thermal-Hydraulic System Code, MARS 1.3.1,"Annals of Nuclear Energy 26(18), 1161-1642 1999

[Kaufman, 1999] Lori M. Kaufman, Barry W. Johnson, "Embedded Digital System Reliability and Safety Analysis", NUREG/GR-0020, U.S. NRC, 1999.

[Kawanishi, 1991] K. Kawanishi, A. Tsuge, M. Fujiware, T. Kohriyama, and H. Nagumo, Experimental Study on Heat Removal during Cold Leg Small Break LOCAs in PWRs, J. Nucl. Sci. Technol., Vol. 28, pp.555 1991

[KHNP, 1995] KHNP, "Yong-Gwang Second Nuclear Power Plant Operation Manual", Vol. 2 1995

[KHNP, 1996] KHNP, "System Description Manual for Korea Standard Nuclear Power Plant", Vol. 1, Yong-Gwang Nuclear Power Plant Training Center, 1996.

[KHNP, 1997] KHNP, Ul-Chin Unit 3&4 Emergency Operate Procedure, Korea Hydraulic and Nuclear Power Co. 1997

[KHNP, 2002] KHNP, "Probabilistic Safety Assessment for Young Gwang 5&6: Low Power and Shutdown Analysis", 2002

[Kiper, 1988] K.L. Kiper, et al., Seabrook Station Probabilistic Safety Study (Shutdown Mode 4, 5 and 6), New Hampshire Yankee, 1988.

[Lanore, 1990] J.M. Lanore, The French 900MWe PWR PSA Results and Specificities, Proceedings of the CSNI Workshop on PSA Applications and Limitations (Sep. 4-6, 1990, Santa Fe, NM), NUREG/CP-0115, SAND90-2797, U.S. NRC, 1991. pp.75-80.

[Lee, 1998] W. J. Lee, B. D. Chung, J. -J. Jeong, K. S. Ha, "Development of a Multi-Dimensional Realistic Thermal-Hydraulic System Analysis Code, MARS 1.3 and Its Validation" KAERI/TR-1108/98 Daejeon, Korea 1998

[Lee, 2003a] Y. J. Lee, S. W. Bae, B. D. Chung, "Validation of One-Dimensional Module of MARS 2.1 Computer Code by Comparing with The RELAP5/MOD3.3 Developmental Assessment Results.", KAERI/TR-2411/2003, Daejeon, KAERI 2003

[Lee, 2003b] S. I. Lee, Private Communications 2003

[Lim, 2004] Lim H. G., Park J. H., Jang S. C., "Improvement of the check valve model for the prediction of gravity feed flow" The 6th International Conference on Nuclear Thermal Hydraulics, Operations and Safety(NUTHOS6), Nara, Japan, 2004

[Littlewood, 1993] B. Littlewood and L. Strigini, Validation of Ultrahigh Dependability for Software-Based Systems, B. Littlewood, Communication of the ACM, 36(11), 1993

[Littlewood, 1998] B. Littlewood and L. Strigini, Examination of BBN for Safety Assessment of Nuclear Computer-Based Systems, ESPRIT DeVa Project 20072, 1998

[Lobner, 1982] P. Lobner, et al., A Preliminary Assessment of Core Melt Probability in Cold Shutdown Following a Postulated LOCA at the Sequoyah Nuclear Plant, ASI01382-147LJ, Science Application International, 1982.

[Liu, 1998] T. J. Liu, C. H. Lee, C. Y. Chang, "Power-Operated Relief Valve Stuck-OpenAccident and Recovery Scenarios in the Institute of Nuclear Energy Research Integral System Test Facility, Nuclear Engineering & Design 186, 149-176pp 1998

[Liu, 2000] Liu, Tay-Jian, Chan, Yea-Kuang, Ferng, Yuh-Ming, and Chang, Chien-Yeh, Experimental Investigation of Early Initiation of Primary Cooldown by Secondary-Side Depressurization in a PWR Inadequate Core-Cooling Accident, Nuclear Technology, American Nuclear Society, Vol. 129, No. 2, pp.187 2000

[MIL, 1991] MIL-HDBK-217F, Military Handbook Reliability Prediction of Electronic Equipment, United States Department of Defence, Dec 2 1991.

[Montagnon, 1992] F. Montagon, Probabilistic Evaluation of Risk at Shutdown, Proceedings of an IAEA Technical Committee Meeting of Accident Sequences during Shutdown and Low Power Conditions, (Nov.30-Dec.3, 1992, Stockholm, Sweden), IAEA-TECDOC-751, IAEA, 1994, pp.51-55.

[Naser, 2004] Joseph Naser, "Generic Pre-Qualification of Digital Platforms for Safety Applications: A Success Story for Instrumentation and Control Modernization in Nuclear Power Plants," NPIC&HMIT 2004, Columbus, USA, 2004.

[NEA, 1997] "Operating and Maintenance Experience with Computer-based Systems in Nuclear Power Plants-A report by the PWG Task Group on Computer-based Systems Important to Safety", NEA/CSNI/R(97)23, 1997.

[Nguyen, 2004] Thuy Nguyen, Dave Blanchard, Robert Fink, Glenn Lang, Ray Torok, "Simplified Risk-Informed Assessment of Defense-in-Depth and Diversity for Digital I&C Upgrades in Nuclear Power Plants", NPIC&HMIT 2004, Columbus, USA, 2004.

[NRC, 1987] "Format and Content of Plant-Specific Pressurized Thermal Shock Safety Analysis Reports for Pressurized Water Reactor,"Regulatory Guide 1.154, U.S. Nuclear Regulatory Commission 1987

[NRC, 1988] Compendium of ECCS (Emergency Core Cooling Systems) Research for Realistic LOCA (Loss-Of-Coolant Accidents) Analysis, NUREG-1230, U.S. Nuclear Regulatory Commission. 1988

[NRC, 1992] Shutdown and Low-Power Operation at Commercial Nuclear Plants in the United States, NUREG-1449, U.S. NRC, 1992.

[NRC, 1995] Final Policy Statement on the Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities, SECY-95-126, U.S. NRC, 1995.

[NRC, 1998] Regulatory guide 1.176 An Approach for Plant-Specific, Risk-Informed, Decision Making: Graded Quality Assurance, US NRC, 1998.

[NRC, 1999] Low Power and Shutdown Risk : a Perspectives Report, US NRC, 1999.

[NRC, 2000] Proposed Staff Plan for Low Power and Shutdown Risk Analysis Research to Support Risk-Informed Regulatory Decision Making, SECY-00-0007, U.S. NRC, 2000.

[NRC, 2003] Status Report on Draft Regulatory Guide DG-1122 and Draft Standard Review Plan Chapter 19.1, SECY-03-0122, U.S. NRC, 2003.

[Rahmeyer, 1993] W.J. Rahmeyer, "Sizing Swing Check Valves for Stability and Minimum Velocity Limits", Journal of Pressure Vessel Technology, Volume 115, pp.406-410, 1993

[Rao, 1994] S.B. Rao and J. Landolt, A Results of the Gosgen Level 1 PSA for Non-full-Power Conditions, Technical Committee Meeting, IAEA, Arnhem, Netherlands, Nov. 8-11, 1994.

[Siewiorek, 1998] D. P. Siewiorek, R. S. Swarz, "Reliable Computer Systems-Design and Evaluation", A. K. Peters, 1998.

[Stahlkopf, 1984] K. E. Stahlkopf, "Pressure Vessel Integrity under Pressurized Thermal Shock Conditions," Nuclear Engineering and Design, Vol. 80, Pages 171-180 1984

[Sudarno, 2003] Sudarno 외 4인, Reliability Study: Digital Engineered Safety Feature Actuation System of Korean Standard Nuclear Power Plant, KAERI/TR-2467/2003, 한국원자력연구소, 2003.4

[Tanenbaum, 1984] Andrew S. Tanenbaum, "Structured computer organization 2/e", Prentice/Hall international, 1984.

[Tang, 1998] D. Tang, M. Hecht, X. An & R. Brill, "MEADEP and its application in dependability analysis for a nuclear power plant safety system," IEEE Tr. on Nuclear Science, Vol., 45, No. 3, p. 1014-1021, June 1998.

[Thurgood, 1982] M. J. Thurgood, J. M. Kelly, T. E. Guidotti, R. J. Kohrt, K. R. Crowell, " COBRA/TRAC A Thermal-Hydraulics Code for Transient Analysis of Nuclear Reactor Vessels and Primary Coolant Systems", NUREG/CR-3046, Vol. 1 1982

[Thunem, 2004] Atoosa P.J. Thunem, "Computerized Systems' Availability, Safety And Security Research At The OECD Halden Reactor Project", NPIC&HMIT 2004, Columbus, USA, 2004.

[Westinghouse, 1992] Westinghouse Electric Corporation, "Risk of PWR Inadvertant Criticality During Shutdown and Refueling," NSAC-183, December 1992.

[Westinghouse, 2002] Technical Manual for Digital Plant Protection System (DPPS) for Ulchin 5&6, Westinghouse electric company LLC, 2002

[Whitehead, 1995] D.W. Whitehead, et al., Evaluation of Potential Severe Accidents During Low Power and shutdown Operations at Grand Gulf, Unit 1: Summary of Results, NUREG/CR-6143, SAND93-2440, Vol. 1, Sandia National Lab., 1995.

제 2 절 국내 과학 기술 정보

[강현국, 2002a] 강현국, 성태용, An Analysis of Safety-Critical Digital Systems for Risk-Informed Design, RESS, Vol.78, 2002. pp.307-314.

[강현국, 2002b] 강현국 외 2인, A Sensitivity Study on the Factors of the PSA for Digital Equipment, PSAM6, 2002.4.

[강현국, 2002c] 강현국 외 2인, A Systematic Approach for the Quantitative Safety Assessment of Digital Safety Systems, 한국원자력학회 2002년 춘계 학술발표회, 2002.5.

[강현국, 2002d] 강현국 외 1인, The Research Activities and Plan on The Risk Assessment of Digital I&C Systems in KAERI , 7th KJ PSA Workshop, 2002.5.

[강현국, 2002e] 강현국 외 2인, A Simplified Risk Effect Analysis of Digital Reactor Protection System, 한국원자력학회 2002년 추계학술발표회 2002.10.

[강현국, 2002f] 강현국 외 2인, Evaluation of the Impact of the Digital Safety-Critical I&C Systems on the Plant Risk, ISOFIC2002, 2002.11.

[강현국, 2002g] 강현국 외 2인, Korean Activities in Safety Assessment of Digital Safety System, OECD Halden Workshop, 2002.11.

[강현국, 2003a] 강현국 외 2인, Unavailability Analysis of Digital ESFAS, 한국원자력학회 2003년 춘계학술발표회, 2003.5.

[강현국, 2003b] 강현국 외 2인, ATWS Probability Quantification Considering the Effect of Digital Equipment, 한국원자력학회 2003년 추계학술발표회 2003.10.

[강현국, 2003c] 강현국 외 2인, The Status and Applications of the Methodology of Digital Safety System PSA, 제 3차 원자력학회-전기학회 공동주최 계측제어기술 웍샵, 2003.11.

[강현국, 2003d] 강현국 외 1인, Interim Findings from the PSA of Digital Safety Critical Systems, KORAS2003, 2003.12.

[강현국, 2003e] 강현국 외 4인, PSA관점에서의 디지털 안전계통의 최근 설계동향 분석, KAERI/AR-669/2003, 한국원자력연구소, 2003.3

[강현국, 2003f] 강현국 외 3인, 신뢰도 상세분석 : 표준원전 디지털 원자로 보호 계통, KAERI/TR-2419/2003, 한국원자력연구소, 2003.3

[강현국, 2004a] 강현국, 장승철, Plant Risk Effect Analysis Focusing on Digital I&C Systems, IIE Trans. Quality and Reliability ('04.1 submitted)

[강현국, 2004b] 강현국 외 3인, 디지털보호계통에 의한 표준원전 안전성 영향분석, KAERI/TR-2669/2004, 한국원자력연구소, 2004.3

[강현국, 2004c] 강현국 외 3인, Coupled Failure of Vital Areas in Nuclear Plants, IYNC2004, 2004.5.

[강현국, 2004d] 강현국 외 2인, The Risk Effect Analysis of the Digital Safety-Critical Systems a in Nuclear Power Plant , PSAM7, 2004.6.

[강현국, 2004e] 강현국 외 2인, Analysis on Manual Actuation Failure and Risk Effect, NPIC&HMIT2004, 2004.9.

[강현국, 2004f] 강현국 외 2인, Fault Tree Model of Human Error Based on Error-Forcing Contexts, 원자력학회 2004 추계학술발표회, 2004.10.

[강현국, 2004g] 강현국 외 2인, Fault Tree Based Risk Assessment of Safety-Critical Digital Systems and Its Effect on Plant Risk, 제 7차 KJ-PSA Workshop, 일본 도쿄, 2004.10.

*[2)][강현국, 2004h] 강현국 외 2인, ATWS Frequency Quantification Focusing on Digital I&C Failures, J.KNS, V36, No.2, 2004. pp.184-195.

[강현국, 2005a] 강현국, 장승철, Application of Condition-Based HRA Method to

2) * 표시는 본문 중 인용되지 않은 자료이지만 본 과제의 단계 결과물의 일부임을 의미함.

a Manual Actuation of the Safety Features in a Nuclear Power Plant, RESS ('05.2 sumitted)

[강현국, 2005b] 강현국 외 2인, 디지털 특성을 반영한 조건 기반 인간 신뢰도 분석 방법론 연구, KAERI/TR-2907/2005, 한국원자력연구소, 2005. (to be published)

[강현국, 2005c] 강현국 외 2인, 한국형 표준원전 디지털 보호 계통 공통원인고장 모델링에 관한 연구, KAERI/TR-2908/2005, 한국원자력연구소, 2005. (to be published)

[과기부, 1996] 과기부, 가압경수형 원전 부분충수 운전 안전조치요건, 원검 71233-78, 과기부, 1996.

*[김석준, 2003a] 김석준 외 2인, A Quantitative Method for the Fault Coverage of Watchdog Timers in NPP Digital Systems, 한국원자력학회 2003년 춘계 학술발표회, 2003.5.

*[김석준, 2003b] 김석준 외 2인, Evaluation of Fault Coverage for Digitalized System in NPPs using VHDL , 한국원자력학회 2003년 추계학술발표회, 2003.10.

*[김석준, 2003c] 김석준 외 2인, Evaluation of Fault Coverage for Digitalized System in NPPs using VHDL, 4th IEEE-ISSRE, 2003.12.

*[김석준, 2004a] 김석준 외 2인, Quantitative Evaluation of Fault coverage for Digitalized Systems in NPPs, NPIC & HMIT 2004, 2004.9.

*[김석준, 2004b] 김석준, 이준석, 성풍현, 강현국, 장승철, Quantitative Evaluation of Fault coverage for Digitalized Systems, RESS ('05.1 accepted)

[김위경, 2001] 김위경 외, 저출력 및 정지냉각운전 관련 규제 동향 및 사건 사례 분석보고서, KIN/AR-771, 한국원자력안전기술원, 2001.

[김인석, 2000] I.S. Kim, et al., Suitability Review of FMEA and Reliability

Analysis for Digital Plant Protection System and Digital Engineered Safety Features Actuation System, KINS/HR-327, 한국원자력안전기술원, 2000.

*[김종기, 2003] 김종기, "유비쿼터스(Ubiquitous) 철도시대를 대비한 전자기기의 신뢰성 기술", 철도와 전기기술, Volume 14, Number 5, 2003.

[김태운, 2003] 김태운 외 4인, 원전의 정지/저출력 운전 중 발생사건 자료 수집 및 데이터베이스 구축, 한국원자력학회 2003년 춘계학술발표회, 2003.5.

[박진균, 2003] 박진균 외 4인, 표준원전에서의 붕소희석 반응도 사건에 대한 정성적 분석, KAERI/TR-2436/2003, 한국원자력연구소, 2003.3

[박진희, 2003a] 박진희 외 4인, 원전의 정지/저출력 운전 중 발생사건 자료 수집 및 데이터베이스 구축, KAERI/TR-2471/2003, 한국원자력연구소, 2003.4

*[박진희, 2003b] 박진희, 한석중, 장승철, 김태운, 정지/저출력 사건 검색 및 분석 프로그램(LEDB), 프로그램No. 2003-01-12-3596, 2003.7

[박진희, 2004] 박진희 외 5인, ANS LPSD PSA Standard 기반 국내 표준원전 정지/저출력 PSA 모델 검토, KAERI/TR-2672/2004, 한국원자력연구소, 2004.5

[박진희, 2005] 박진희, 임호곤, 장승철, 한국 표준형 원전 정지/저출력 PSA 초기사건 분석 개선, KAERI/TR-2986/2005, 한국원자력연구소, 2005.

[성풍현, 2001] 성풍현 외, "차세대 원전 디지털 계측제어 부품의 신뢰도 정량적 평가기술 개발", 한국과학기술원, 대전, 2001.

[손영석, 2004] 손영석 외 4인, 국내 표준형 원자력발전소 정지/저출력 운전중 상세 열수력 분석, KAERI/TR-2680/2004, 한국원자력연구소, 2004.5

[손영석, 2005] 손영석, 서지영, 임호곤, 박진희, 장승철, Thermal-Hydraulic Calculations Applied to Low Power and Shutdown PSA, J. Nuclear Engineering and Design, ('05.1 accepted)

[엄흥섭, 2003a] 엄흥섭 외 3인, BBN을 이용한 안전 소프트웨어의 정량적 신뢰도

평가 방안 연구, KAERI/TR-2437/2003, 한국원자력연구소, 2003.5

[엄흥섭, 2003b] 엄흥섭 외 2인, A Study on the Quantitative Evaluation of the Reliability for Safety Critical Software Using BBN, 한국원자력학회 2003년 춘계학술발표회, 2003.5

*[엄흥섭, 2003c] 엄흥섭 외 4인, 안전소프트웨어의 정량적 V&V 방안 연구, KAERI/TR-2668/2004, 한국원자력연구소, 2003.6

[엄흥섭, 2004a] 엄흥섭 외 2인, A Study on the Quantitaive V&V for Safety-Critical Software , 원자력학회 2004 추계학술발표회, 2004.10.

[엄흥섭, 2004b] 엄흥섭 외 3인, A Study on Quantitative Reliability Estimation of Safety-critical Software for PSA, NPIC&HMIT2004, 2004.9.

[엄흥섭, 2004c] 엄흥섭 외 3인, 안전 소프트웨어의 신뢰도 정량 평가 BBN을 위한 전문가 지식추출 지침, KAERI/TR-2662/2004, 한국원자력연구소, 2004.2

[엄흥섭, 2004d] 엄흥섭 외 3인, 안전소프트웨어의 정량 V&V 방안 연구, KAERI/TR-2668/2004, 한국원자력연구소, 2004

*[이준석, 2004] 이준석 외 2인, Estimation of reliability on digital plant protection system in nuclear power plant using fault simulation with self-checking, NUTHOS 6, 2004.10.

*[임호곤, 2003a] 임호곤 외 4인, Analysis of the Feasibility for Boron Dilution Accident in KSNP, 한국원자력학회 2003년 춘계학술발표회, 2003.5.

*[임호곤, 2003b] 임호곤 외 1인, Analysis of Virtual Mass Force Effects on the Numerical Stability of Three-Fluid Model, 한국원자력학회 2003년 춘계학술발표회, 2003.5.

*[임호곤, 2004a] 임호곤 외 3인, Simulation of Pressurizer Stuck-Open Accident for the Development of Accident Aequences in the Low Power/Shutdown PSA, ICONE12, 2004.5.

*[임호곤, 2004b] 임호곤 외 4인, 정지/저출력 PSA 열수력 분석 플랫폼 개발, 제 2회 안전해석 심포지엄, KINS, 2004.6.

*[임호곤, 2004c] 임호곤 외 2인, The Impacts of Check valves on the Gravity feed Flow , 원자력학회 2004 추계학술발표회, 2004.10.

*[임호곤, 2004d] 임호곤 외 3인, Improvement of Check Valve Model for Gravity Feed Flow Prediction, NUTHOS-6, 2004.10.

*[임호곤, 2004e] 임호곤 외 2인, The Effect of an Aggressive Cool-down Following a Refueling Outage Accident in which a Pressurizer Safety Valve is Stuck Open, J.KNS, Vol.36, No.6, Dec. 2004, pp.497-511.

*[임호곤, 2005a] 임호곤 외 3인, The Analysis of Pressurizer Safety Valve Stuck Open Accident for Low Power and Shutdown PSA, KAERI/TR-2670/2004, 한국원자력연구소, 2005.1.

*[임호곤, 2005b] 임호곤 외 3인, The Analysis of Gravity Feed in KSNP for the Development of Shutdown PSA, KAERI/TR-2671/2004, 한국원자력연구소, 2005.2.

*[임호곤, 2005c] 임호곤, 박진희, 장승철, Calulation of Low Velocity Pipe Flow Including Swing Check Valve, J. Nuclear Engineering and Design ('05.2 sumitted)

[장승철, 2000] 장승철 외, "RPEE", 프로그램 등록번호 2000-01-12-4182, 한국원자력연구소, 2000.

*[장승철, 2002] 장승철 외 2인, Performance and Unavailability Analysis of RPS/ESFAS in Korean Standard Nuclear Power Plant(KSNPP), ICONE-10, 2002.4.

[장승철, 2004a] 장승철 외 4인, Self-Assessment of the Low Power and Shutdown PSA Quality for the Korea Standard Nuclear Power Plant

(KSNPP), IAEA Workshop on PSA Quality for Decision Making, 2004.2.

[장승철, 2004b] 장승철 외 3인, Quality of the Current Low Power and Shutdown PSA Prectice , 원자력학회 2004 추계학술발표회, 2004.10.

*[장승철, 2004c] 장승철 외 4인, 울진 3,4호기 RPS/ESFAS 신뢰도 상세분석 모델, 기술실시 No. 2004-009, 대상기관(KAIST), 2004.3

*[장승철, 2004d] 장승철 외 1인, 설정치 드리프트 관리를 위한 통계적 분석 방법 개발, KAERI/TR-2167/02, 한국원자력연구소, 2004.8

*[장승철, 2004e] 장승철 외 2인, Statistical Drift Control Methods Using Plant specific As-Found/As-Left Data, NPIC&HMIT2004, 2004.9.

*[장승철, 2004f] 장승철 외 2인, A New Approach to the Statistical Setpoint Drift Management , 원자력학회 2004 추계학술발표회, 2004.10.

[전력연구원, 2001] 전력연구원, '00전력연 단612, Technical Memo, TM.94ZJ15.T2000.607-1, 영광 5,6호기 확률론적 안전성 평가 [정지/저출력 분석 보고서: 별책 2권], 전력연구원, 2000.11

[전자통신연구원, 1999] ERIS Frame v3.0 사용자 메뉴얼, 전자통신연구원(ETRI), 1999.

[정환성, 2002] 정환성 외 3인, 디지털 계측제어 계통의 확률론적 안전성 평가를 위한 주요인자 선정 및 민감도 분석, KAERI/TR-2026/02, 한국원자력연구소, 2002.

[정환성, 2003] 정환성 외 4인, Analysis of Hardware Reliabilities for NPP Digital I&C Equipment Predicted by Various Methods, ICAPP'03, 2003.5

*[진영호, 2003a] 진영호 외 1인, MARS 코드의 정지/저출력 운전중 사고해석 능력 검증, KAERI/TR-2442/2003, 한국원자력연구소, 2003.3

*[진영호, 2003b] 진영호 외 2인, The Effect of Gravity Feed into RCS for the Loss of Shutdown Cooling Accident during Mid-loop Operation, 한국원자

력학회 2003년 춘계학술발표회, 2003.5

*[진영호, 2003c] 진영호 외 3인, 정지/저출력 PSA 에서의 열수력 분석, 제 1회 원자력 안전해석 심포지엄, 2003.6.

[한국전력공사, 1997] 한국전력공사 울진원자력본부, "울진 제2 발전소 운영절차서 (종합운전)," 1997.

[한국전력공사, 2003] 한국전력공사 영광원자력본부, "표준 기술행정 절차서, 표준기행-03"

*[한석중, 2002a] 한석중 외 3인, Simplified Method of Estimating Large Early Release Frequency for Risk-informed Applications , 한국원자력학회 2002년 추계학술발표회, 2002.10.

*[한석중, 2003a] 한석중 외 3인, 정지/저출력 PSA에서 주논리도를 이용한 초기사건 선정, 한국원자력학회 2003년 춘계학술발표회, 2003.5.

[한석중, 2003b] 한석중 외 2인, 정지저출력 PSA에서 주논리도를 이용한 초기사건 선정, KAERI/TR-2497/2003, 한국원자력연구소, 2003.6

서 지 정 보 양 식

수행기관보고서번호	위탁기관보고서번호	표준보고서번호	INIS 주제코드
KAERI/RR-2537/2004			

제목 / 부제	정지/저출력 및 디지털 계통의 위험도 평가 기술 개발
연구책임자 및 부서명	장승철 (종합안전평가부)
연 구 자 및 부 서 명	강현국, 임호곤, 박진희, 엄홍섭, 김태운, 하재주 (종합안전평가부)

출 판 지	대전	발행기관	한국원자력연구소	발행년	2005. 4
페 이 지	246 p.	도 표	있음(O), 없음( )	크 기	21×29.7Cm.
참고사항					
비밀여부	공개(O), 대외비( ), __ 급비밀		보고서종류	RR	
연구위탁기관	한국원자력연구소		계약 번호		

초록 (15-20줄 내외)

본과제는 정지/저출력 PSA와 디지털 기기 PSA의 두 분야로 구성되어 있다. 각 분야별 연구 목적과 수행된 연구 내용 및 범위는 다음과 같다.

<정지/저출력 PSA 기술 개발 분야>

정지/저출력 운전모드에서는 출력 운전과는 달리 다양한 기기배열로 인해 정지/저출력 PSA는 그 수행 방법이 매우 복잡하여 아직 통일된 방법론이 정립되어 있지 않은 상태에 있고 분석의 불확실성이 크기 때문에, 위험도 정보를 활용한 의사결정을 지원하기 위해서 불확실성이 저감된 보다 현실적인 위험도 정보를 제공할 수 있도록 하기위한 기술의 개발을 목적으로 한다.

○ 표준원전 정지/저출력 PSA 모델 품질등급 평가
○ 정지/저출력 PSA 방법론 및 모델 개선 (4개 분야: 발전소 운전상태 분석, 초기사건 분석, 성공기준 결정 및 사고경위 분석 분야)
○ 정지/저출력 위험도 관리 기반 기술 연구

<디지털 I&C PSA 기술 개발 분야>

세계적으로 원전의 안전기능에도 디지털 기기가 적용되기 시작하고 국내 원전에도 디지털 안전기기가 본격적으로 활용되기 시작했음에도 불구하고 그 안전성 입증을 위한 위험도 정량 평가 방법론은 초기 개발 단계에 있으므로, 활용성이 높고 정확한 디지털 계측제어 계통의 위험도 평가 기술 개발을 목적으로 한다.

○ 안전 관련 디지털 계통의 상세 신뢰도 평가 모델 개발
○ 디지털 계통의 원전 위험도 영향 평가 모델 개발
○ 디지털 I&C PSA 요소 기술 연구

주제명키워드 (10단어내외)	위험도, 안전성, 신뢰도, 확률론적 안전성 평가, 정지, 저출력, 디지털 계측제어, 소프트웨어

BIBLIOGRAPHIC INFORMATION SHEET

Performing Org. Report No.	Sponsoring Org. Report No.	Stamdard Report No.	INIS Subject Code
KAERI/RR-2537/2004			

Title / Subtitle
Development of Risk Assessment Technology for Low Power, Shutdown and Digital I&C Systems

Project Manager and Department	Seungcheol Jang (Integrated Safety Assessment Team)
Researcher and Department	Hyungook Kang, Hogon Lim, Jinhee Park, Heungsub Eom, Taewoon Kim, Jaejoo Ha, (Integrated Safety Assessment Team)

Publication Place	Daejeon	Publisher	KAERI	Publication Date	2005. 4
Page	246 p.	Ill. & Tab.	Yes(O), No ( )	Size	21×29.7Cm.
Note					
Classified	Open(O), Restricted( ), ___ Class Document		Report Type	RR	
Sponsoring Org.			Contract No.		

Abstract (15-20 Lines)

There are two technical areas to deal with in the project; (1) the low power and shutdown probabilistic safety assessment (PSA), and (2) the digital I&C PSA. The scope and contents of each area could be summarized as follows:

<The LPSD PSA Area>

○ Quality assessment of a LPSD PSA model for a Korean Standard Nuclear Power Plant (KSNP)

○ Quality improvement of the KSNP LPSD PSA model in the following four technical areas; plant operating status (POS), initiating event analysis, determination of success criteria, accident sequence analysis

○ Development of the LPSD risk management technologies

<The Digital I&C PSA Area>

○ Unavailability analysis of Digital safety systems such as Digital Plant Protection System (DPPS) and Digital Engineered Safety Feature Actuation System (DESFAS)

○ Impact analysis of the digital safety systems on plant risks throughout of the digital plant risk models for evaluating core damage frequency (CDF) and large early release frequency (LERF)

○ Study on the methodologies for treating digital-specific problems in the digital I&C PSA such as reliability of safety-critical softwares, common cause failure (CCF) of digital components, fault coverage, etc.

Subject Keywords (About 10 words)	Risk, Safety, Reliability, PSA (or PRA), Shutdown, Low power, Digital I&C, Software