한국에너지공학회지(1999), 제8권 제2호
Energy Engg. J(1999), Vol. 8, No. 2, pp. 213~223

기술논문

원자력발전소 안전계통 소프트웨어의 동적시험에 관한 연구

문채주 · 장영학 · 이순성* · 서 영*
목포대학교 전기공학과, *한전기술 원자로설계개발단

A Study on Dynamic Test of Safety System Software on Nuclear Power Plant

Chae Joo Moon, Young Hak Chang, Sun Sung Lee* and Young Suh*
Department of Electrical Engineering, Mokpo National University
**Nuclear Engineering Development Division, KOPEC*

요 약

최근 원자력발전소의 안전계통 소프트웨어는 신뢰성을 향상시키기 위해 ANSI/IEEE-ANS-7-4.3.2-1982 기준에 따라 확인 및 검증이 이루어지고 있다. 이 규정은 안전관련 소프트웨어가 정적 및 동적 환경에서 시험되어야 한다고 요구하고 있다. 부적절노심냉각감시계통의 경우에 정적시험 절차 및 관련기술들은 개발되었으나 동적시험 절차 및 관련기술들은 개발되지 않았다. 따라서, 본 논문에서는 미개발된 기술들을 논의하고, 동적시험 절차와 시험 입력자료 생성 프로그램을 제안한다. 이 프로그램의 성능은 울진 3,4호기 최종 안전성 분석 보고서의 사고해석 결과를 사용하여 확인하였다.

Abstract — In recently, the safety system software of the nuclear power plant has been verified and validated according to ANSI/IEEE-ANS-7-4.3.2-1982 to improve the reliability. This standard requires that safety-related software should be tested in the static and dynamic environments. In case of Inadequate Core Cooling Monitoring System (ICCMS), the static test procedure and related techniques are developed but the dynamic test procedure and related techniques are not developed. Therefore, this paper discusses the undeveloped techniques, and suggests the dynamic test procedure and the program for generation of test input data. The performance of the program was identified using accident analysis report of Ulchin 3&4 Final Safety Analysis Report (FSAR).

1. 서 론

최근 원자력발전소 계측제어시스템은 계통의 신뢰성 향상, 기기의 단종, 관련규정의 변경 및 급속한 전자기술의 발전 등으로 디지털 시스템이 널리 적용되고 있다. 또한, 기존 원자력발전소 아날로그 계측제어시스템의 노후화로 인한 운전 및 유지보수 비용의 증가 그리고 디지털 기술의 우수성 때문에 디지털 시스템의 적용은 더욱 확산 추세에 있으며, 이러한 디지털 시스템의 적용에는 종래의 하드웨어 기능을 향상시킨 소프트웨어가 사용된다. 이 소프트웨어는 유지보수를 하기 위한 보수용 소프트웨어를 개발하여 사용하거나 디지털 설비의 성능개선에서도 유용하게 활용되기도 하나 이는 소프트웨어 공통모드고장 문제와 소프트웨어 신뢰도 문제를 야기하게 되었다. 이러한 문제를 해결하는 소프트웨어의 확인 및 검증기술이 요구되었으나 지금까지 시스템 특성상 안전성 확보에 대한 소프트웨어 개발기준과 규제방법이 정립되지 않았다. 또한, 디지털 계측제어계통의 핵심기술인 고신뢰도 소프트웨어 개발 방법론이 확립되지 못하여 소프트웨어 공통모드 고장문제, 정량적인 소프트웨어 신뢰도 보장문제 등이 논란의 대상이 되어 소프트웨어의 확인 및 검증(V&V: Verification and Validation)이 원자력 산업계의 최대 관심사항으로 부각되었다. 이러한 문제는 신규 설계되는 발전소 뿐만 아니라 기존 원자력발전소 아날로그 계측제어계통에 대한 유지보수 비용증가와 운전편이성의 욕구증대로 디지털 시스템이 설치되는 경우에도 동일한 쟁점이 되고 있다. 일부에서는 확인 및 검증을 위한 시험설비를 개발하여 해결을 시도하

고 있으나 많은 비용과 시간이 요구되어 여전히 관심사항으로 등장하고 있다[1]-[5].

현재 소프트웨어의 확인 및 검증이 적용되고 있는 원자력발전소 안전계통은 경수로의 경우 노심보호계산기계통(CPCS: Core Protection Calculator System)과 부적절노심냉각감시계통(ICCMS: Inadequate Core Cooling Monitoring System) 등이 있고, 중수로의 경우 제1안전계통(SDS1: ShutDown System #1)이 있다. 한국표준형 원자력발전소인 영광 3,4호기 및 울진 3,4호기의 경우 적용된 기준은 ANSI/IEEE 7-4.3.2-1982이며, 이 기준에서는 정적시험 및 동적시험을 요구하고 있다. CPCS의 경우 실제 운전상황을 모사한 시험자료와 시뮬레이터를 이용하여 소프트웨어의 확인 및 검증을 수행하였고, 중수로의 경우 사고 시나리오를 이용한 동적시험 자료 및 자체검증 시험설비를 사용하였다. ICCMS의 경우는 규제요건에서 요구한 동적시험에 대해 실제 운전조건이 고려되지 않고 기능요건의 만족여부만 시험하였다. ICCMS의 경우 자동보호조치를 수행하지 않기 때문에 상대적으로 규제가 완화되었으나 안전관련 계통에 대한 규제가 강화되고 있어 확보된 정적시험 기술을 제외한 동적시험에 대한 연구가 요구되고 있다[6]-[11].

본 연구에서는 안전계통과 관련된 소프트웨어의 동적시험 기준과 CPCS나 SDS에 대한 소프트웨어 확인 및 검증의 적용방법을 검토하여 ICCMS의 동적시험을 위한 시험절차를 개발하고, 또한 동적시험 시나리오에 필요한 입력자료를 만들어주는 소프트웨어를 개발하고자 한다.

2. 동적시험 절차개발

ICCMS에 대한 동적시험 절차를 개발하기 위해 안전계통과 관련된 소프트웨어의 동적시험 기준과 경수로 CPCS 및 중수로 SDS1에서 수행한 동적시험 방법을 검토하고 ICCMS에 적용 가능한 동적시험 절차를 수립한다.

2-1. 시험기준

안전관련 컴퓨터계통의 소프트웨어에 대한 동적시험 및 동적시험 자료의 작성과 관련된 기준은 ANSI/IEEE-7-4.3.2-1982, "Application Criteria for Programmable Digital Computer Systems in Safety Systems in Nuclear Power Generating Stations"와 ANSI/IEEE-829-1983, "IEEE Standard for Software Test Documentation"이 있다. 각 기준의 내용을 보면, ANSI/IEEE-7-4.3.2-1982의 section 6, Computer System Validation에서는 안전관련 컴퓨터계통의 검증을 위해서 반드시 수행되어야 할 시험범위를 정의하고, ANSI/IEEE-829-1983의 section 5. Test Case Specification에서는 시험자료 작성에 대한 지침을 제공하고 있다.

2-2. 동적시험 사례검토

기존의 안전관련 컴퓨터계통의 소프트웨어 동적시험 현황은 국내원전에 적용된 안전계통인 노심보호 계산기계통 및 제1원자로 정지계통을 기준으로 검토하였다.

2-2-1. 노심보호계산기계통[8][9]

노심보호계산기계통에 대한 확인 및 검증방법은 1986년에 미국 원자력규제위원회로부터 인허가를 받았으며[16] 영광 3,4호기 및 울진3,4호기에서도 그대로 적용하고 있다. 이 방법은 소프트웨어의 수학적, 논리적 측면에서의 성능을 확인하기 위해서 기계어 수준의 명령어 및 코드 가지(Branch) 수준으로 세분화된 모듈들의 입출력을 확인하는 Phase I 시험과, 계통 알고리즘이 소프트웨어와 하드웨어에 적절히 조합되었는지와 계통의 정적 및 동적 반응을 검증하기 위한 Phase II 시험으로 나누어진다. 이 중에서 동적시험과 관련된 Phase II 시험은 입력스윕시험(IST: Input Sweep Test)과 동적소프트웨어 확인시험(DSVT: Dynamic Software Verification Test), 그리고 실입력 단일변수시험(LISPT: Live Input Single Parameter Test) 등의 세 가지 시험으로 구성된다.

2-2-2. 제1원자로정지계통[10][11]

월성 2,3,4호기에서 적용하고 있는 제1원자로 정지계통 소프트웨어의 확인 및 검증방법은 크게 확인 및 검증의 두 작업으로 나누어진다. 확인작업은 소프트웨어가 개발되는 전 과정동안 소프트웨어 모듈들이 설계요건에 부합되는지를 검토, 시험하는 것으로서 설계요건 및 전산코드 확인, 전산코드 위험요소 분석, 단위 시험, 그리고 부속계통 시험등의 정적시험들로 구성된다. 검증 작업은 소프트웨어의 동적 성능을 입증하고 기능 요구사항의 만족 여부를 검사하기 위한 검증 시험과 소프트웨어의 신뢰성을 검사하기 위한 신뢰도 시험으로 구성된다.

2-3. ICCMS 동적시험 절차 설계

안전관련 컴퓨터 계통의 확인 및 검증에 대한 소프트웨어 관련 기준과 기존 안전계통의 동적시험 방법에 대한 검토결과를 토대로 ICCMS에 대해 동적시험을 하기 위한 요건은 다음과 같이 얻어진다. 1) 안전계통의 동적시험에는 그 계통의 설계기준사고 및 운전조건을 모사한 동적시험 자료를 사용해야 한다. 2) 동적시험 자료는 식별번호, 시험항목, 입력 및 출력, 환경조건, 시험절차상 제한사항, 그리고 각 시험자료간의 상관성을 명시한 동적시험 자료 사양서에서 제공되어야 한다. 3) 시험결과의 만족여부를 판단하기 위해서는 계통 시뮬레이터가 필요하다. 4) 최종 시험에 앞서서 시험결과에 대한 허용

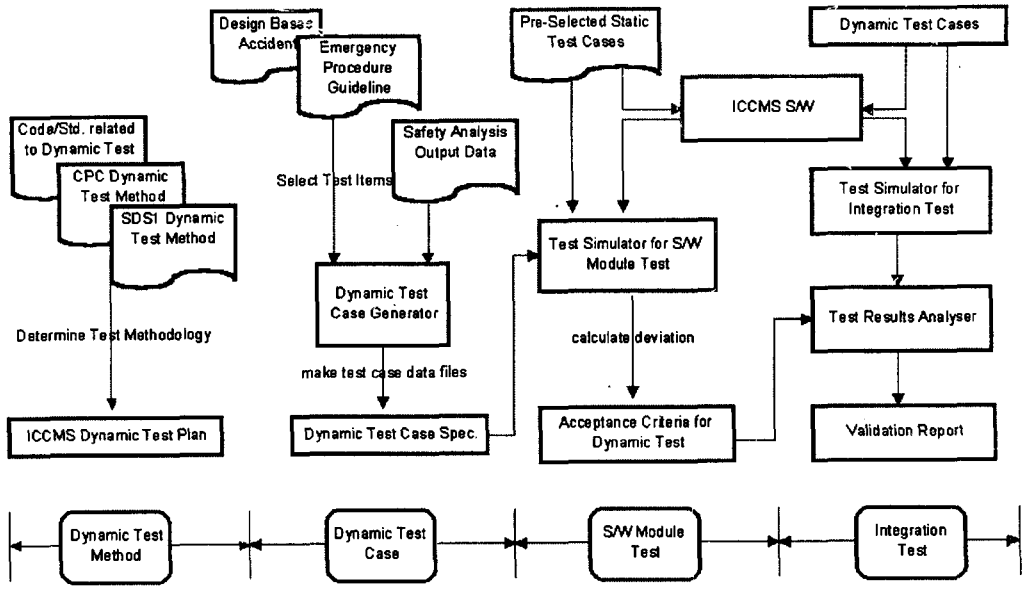


Fig. 1. Dynamic test procedure for ICCMS.

기준을 결정하기 위해 적용된 하드웨어 및 사용 프로그래밍 언어의 차이에 따른 ICCMS 소프트웨어와 시뮬레이터 소프트웨어간의 처리오차를 계산하는 시험이 선행되어야 한다. 이 결과를 정리하면 ICCMS의 동적시험 방법 및 수행절차는 Fig. 1과 같이 수행되어야 한다.

Fig. 1에 나타난 바와 같이 동적시험 자료 작성방법은 ICCMS의 설계기준 사고 및 비상운전지침서를 분석하여, 각 사고 영역별 필수 운전변수들을 정의함으로써 동적시험 항목을 선정하고, 사고해석코드의 모사자료 및 개발된 동적시험 자료 작성용 소프트웨어를 이용하여, 최종적으로 동적시험 자료를 작성한다. 또한 ICCMS 소프트웨어의 알고리즘 요건을 만족하는 시뮬레이터를 개발하고 이에 대한 시험 및 검증을 수행하여 성능을 입증한다. 그리고 정적시험 및 최소한 모듈당 한 개 이상의 동적시험 항목에 대해 소프트웨어 모듈시험을 실시하여 최종 동적시험에 대한 허용기준을 결정하고, 마지막으로 ICCMS 시험장비와 시뮬레이터를 이용하여 동적시험을 수행한다.

3. 동적시험 자료생성 프로그램

3-1. 동적시험 자료작성 절차

3-1-1. 설계기준사고 분석

ICCMS는 TMI 사고 이후, "원자로 운전원에게 부적절한 노심 냉각상태에 대한 명확한 정보를 제공해야 한다"는 미국 원자력규제위원회의 사후 조치사항에 따라 개발된 계통이다[13]. 따라서, ICCMS의 설계기준사고는 부적절한 노심 냉각상태를 만들 수 있는 사고로 제한되며, 이에 대한 분석에는 부적절한 노심냉각 상태에 대한 명확한 정의가 선행되어야 한다. 그러므로 설계기준사고에 대한 분석작업은 먼저 부적절한 노심냉각 상태의 정의 및 진행과정을 파악하고, 검토대상 사고를 선정한 후, 각 사고별 특성을 분석하고, 각 주요변수 별로 사용되는 사고 및 상태를 평가하는 방법으로 수행하였다.

(1) 부적절한 노심 냉각상태 정의[14]

부적절한 노심 냉각상태는 원자로용기 내의 수위 및 핵연료 피복재의 온도에 따라 다음과 같이 5가지로 정의된다.

상태 1 - 최초의 포화 생성

상태 2 - 노심 노출

상태 3 - 핵연료 피복재온도 900°F(482°C)까지 (정상운전 상태로의 회복이 가능한 온도)

상태 4 - 핵연료 피복재온도 1100°F(593°C)까지 (핵연료 피복재의 파단이 발생하지 않는 온도)

상태 5 - 핵연료 피복재온도 2200°F(1204°C)까지 (10 CFR 50.46에서 규제요건으로 요구하고 있는 냉각재 상실사고시의 인허가 제한 온도)

(2) ICCMS 설계기준사고 분석[14][15][17]

ICCMS는 "부적절한 노심 냉각상태"를 지시함으로써 사고를 완화하기 위한 정보를 운전원에게 제공하는 계통이다. 따라서 ICCMS의 설계기준사고는 1) 부적절한 노심냉각 상태는 원자로 냉각재계통의 냉각재가 70% 이

상 상실될 때 발생하므로 냉각재 상실사고 및 냉각재 상실사고 유형의 사고로 악화될 가능성이 있는 사고 2) 운전원이 표시기를 보고 필요한 조치를 취할 수 없을 정도로 급격히 변하지 않는 사고로 제한된다. 따라서 현재 원자력발전소의 설계기준사고 중에서 가장 심각한 "부적절한 노심냉각 상태"를 만드는 사고인 대형파단 냉각재 상실사고는 과도상태의 천이가 너무 급격하여 두 번째 선정기준을 만족하지 못하며, 또한 자동 작동되는 안전설비에 의해 사고 초기에 상황이 완화되므로 고려 대상에서 제외되었다[11]. 설계기준사고 보다 심각한 사고의

Table 1. ICCMS variable names of emergency procedure guideline.

단계	안전기능	사용 ICCMS 변수
표준 원자로 정지 후 조치사항	원자로냉각재계통 재고량제어	원자로냉각재계통 포화여유도
	노심열제거	원자로냉각재계통 포화여유도 노심출구온도
진 단	원자로냉각재계통 압력제어	원자로냉각재계통 포화여유도
원자로정지 회복지침서	원자로냉각재계통 재고량제어	원자로냉각재계통 포화여유도 원자로용기수위
	노심열제거	원자로냉각재계통 포화여유도
냉각재상실사고 복구절차서	원자로냉각재계통 재고량제어	원자로냉각재계통 포화여유도 원자로용기수위
	노심열제거	노심출구온도
증기발생기 전열관 파손사고 복구절차서	원자로냉각재계통 재고량제어	원자로냉각재계통 포화여유도 원자로용기수위
	노심열제거	노심출구온도
과잉증기요구사고 복구절차서	원자로냉각재계통 재고량제어	원자로냉각재계통 포화여유도 원자로용기수위
	노심열제거	노심출구온도 원자로냉각재계통 포화여유도
급수계통완전상실사고 복구절차서	원자로냉각재계통 재고량제어	원자로냉각재계통 포화여유도 원자로용기수위
	노심열제거	노심출구온도
소외전력상실사고 복구절차서	원자로냉각재계통 재고량제어	노심출구온도 포화여유도 원자로용기수위
	노심열제거	노심출구온도 포화여유도
소내전원완전상실사고 복구절차서	원자로냉각재계통 재고량제어	노심출구온도 포화여유도 노심출구온도 원자로용기수위
	원자로냉각재계통 압력제어	노심출구온도 노심출구온도 포화여유도
	노심열제거	노심출구온도 노심출구온도 포화여유도
기능복구절차서	원자로냉각재계통 재고량제어 success path IC-1: CVCS	원자로냉각재계통 포화여유도 원자로용기수위
	원자로냉각재계통 재고량제어 success path IC-2: SIS	원자로용기수위
	노심열제거 success path HR-1	원자로냉각재계통 포화여유도 원자로용기수위
	노심열제거 success path HR-3	노심출구온도

경우에는 다발적인 고장 및 운전원의 부적절한 조치의 가능성 때문에 노심 손상이나 열수력학적 조건을 예상할 수 없으므로 설계기준사고 이상의 심각한 사고도 고려대상에서 제외하였다. 그리고 선정기준으로 고려되어야 하는 또 하나의 중요인자는 사고발생시 원자로 냉각재 펌프의 운전여부이므로 원자로 냉각재 펌프의 운전에 영향을 주는 소외 전원 상실과 같은 사고도 같이 고려되었다. 이러한 기준에 따라 ICCMS에 대한 설계기준사고는 소외 전원 상실사고를 고려한 소형파단 냉각재 상실사고(SBLOCA: Small Break Loss Of Coolant Accident), 증기관 파단사고(SLB: Steam Line Break Accident), 급수계통 상실사고(LOFW: Loss Of FeedWater Accident), 증기발생기 전열관 파단사고(SGTR: Steam Generator Tube Rupture Accident) 등을 선정하였다.

3-1-2. 비상운전지침서 운전요건 분석[16]

TMI 사고 이후 미국 원자력규제위원회의 후속 조치사항에 따라 부적절한 노심냉각 상태를 지시할 수 있는 계기의 설치 및 활용방안으로서 ICCMS 및 비상운전지침서가 작성되었다. 따라서 ICCMS의 운전은 비상운전지침서와 밀접하게 관련되어 있으므로 계통 변수들의 실제 운전조건 및 사용내용을 도출하기 위해 비상운전지침서를 분석하였다. 비상운전지침서는 표준 원자로 정지 후 조치사항, 사고진단, 원자로정지 회복지침서, 사고 최적복구절차서, 그리고 기능회복절차서의 운전지침 및 안전기능상태검사에서 ICCMS 변수들을 사용하고 있으며 분석 내용은 Table 1에 제시되어 있다. 그리고, 사고 진행기간 동안의 각 변수별 사용 시기는 다음절의 사고영역별 변수분석 내용과 거의 일치한다.

3-1-3. 사고영역별 감시변수 분석[14][17]

부적절한 노심 냉각상태를 발생시키는 사고의 진행과정을 감시하기 위하여 각 영역별로 여러 개의 주요변수를 사용할 수 있다. 사고영역은 4개의 영역으로 구분되며, 영역 1에서는 사고가 시작되어 원자로 냉각재계통이 포화에 도달하므로 냉각재의 온도 및 압력 포화여유도가 주요 변수로 사용 가능하다. 영역 2에서는 원자로 용기의 수위가 노심까지 감소하므로 원자로 용기 수위가 주요 변수로 사용 가능하다. 영역 3에서는 핵분열 생성물의 방출 위험에 직접적으로 관련되는 핵연료 피복재 온도가 가장 중요한 변수이며, 원자로 용기 및 노심 출구온도 포화여유도로 노심의 과열정도를 측정함으로써 간접적으로 노심 상황을 감시할 수 있다. 그러나, 핵연료 피복재 온도의 경우, 직접측정이 불가능하므로 노심 출구온도로서 간접적으로 측정한다. 즉, 노심을 나가는 유체의 과열정도가 바로 핵연료 피복재 온도와 핵연료의 노출정도에 관계된다. 그리고 영역 4에서는 원자로 용기의 수위가 증가하고 원자로 냉각재계통이 안정하게 됨에 따라 포화여유도값이 다시 증가하므로, 원자로 용기 수위 및 원자로 냉각재계통 포화여유도가 사용가능하다. 또한 원자로 상부 및 노심 출구온도 포화여유도와의 차를 이용하여 원자로 내부의 온도분포도 감지가 가능하다. ICCMS 주요 변수별로 사용되는 사고영역 및 기능을 요약하면 다음과 같다.

(1) 원자로 냉각재계통 온도 및 압력 포화여유도: 사고영역은 영역 1이고, 기능은 냉각재 상실사고 및 원자로 냉각재 펌프가 운전 가능한 급수계통 상실사고시 최초의 포화발생을 감지한다.

(2) 원자로용기 상부포화여유도: 사고영역은 영역 1, 3 및 4이고, 기능은 원자로 용기 상부의 포화발생을 감지하고 원자로 냉각재계통 및 원자로 용기 상부의 과열정도를 감시함으로써 노심 노출 여부 및 회복을 감시한다.

(3) 노심출구온도 포화여유도: 사고영역은 영역 1, 3 및 4이고, 기능은 노심출구의 포화발생을 감지하고 노심 노출후 노심을 빠져나가는 유체의 과열정도를 감시함으로써 사고의 진행 또는 복구여부를 확인한다.

(4) 원자로용기수위: 사고영역은 영역 2이고, 기능은 이 영역에서 노심 상황을 직접 감시할 수 있는 유일한 수단이며 노심 상부까지의 수위를 감시하고 안전기능 작동 후, 노심의 안정화를 감시한다.

(5) 노심출구온도: 사고영역은 영역 3이고, 기능은 노심 노출 후, 핵연료의 건전성 및 핵분열 생성물의 방출 가능성이 있는 핵연료 피복재 온도의 추이를 감시한다.

3-1-4. 동적시험 항목

공정변수들의 변화량, 변화율, 사고 유지기간, 그리고 "부적절한 노심냉각"의 악화 정도는 사고의 종류 및 원자로 냉각재 펌프의 운전 유무에 따라 다르며, "부적절한 노심냉각 상태"의 영역에 따라 운전이 요구되는 변수 또한 다르다. 따라서 ICCMS 소프트웨어의 성능을 확인하기 위해서는 기능 수행이 요구되는 조건을 고려하여 최소한 한 가지 경우 이상의 동적시험이 수행되어야 한다. 그러므로 ICCMS 소프트웨어의 각 기능 모듈별로 운전되는 요건을 고려하여 성능 확인을 위해 필요한 최소한의 동적시험 항목을 선정한다. 또한 각 동적시험 항목은 시험의 효율성을 위해서 동적시험 자료의 입력으로 사용되는 울진 3, 4호기 최종안전성분석보고서의 사고해석 모사자료를 분석하여 그 기능이 요구되는 시간범위를 고려하여 선정한다. 그러나 최종안전성분석보고서의 사고해석의 경우에 사고마다 해석목적 및 관점이 상이하므로 사고에 따라 이 변수들에 대한 자료가 확보되어 있지 않다. 따라서 비슷한 추이를 갖는 유사변수(예, 가압기 압력은 원자로 용기 압력으로, 원자로 용기 수위는 원자로 냉각재계통의 냉각재 부피로 대체)로서 분석하며, 유사변수도 없는 경우에는 앞절의 설계기준사고

분석결과를 이용한다. 차후 실제 시험에 사용될 최종 동적시험 자료의 작성은 본 연구에서 사용한 자료에 추가하여, ICCMS의 변수가 대부분 포함되어 있는 비상운전 지침서 작성시 수행하는 사고해석 자료를 함께 이용하여야 한다. 그리고 가능하다면 ICCMS의 동적시험 자료 작성을 위한 별도의 사고해석 수행도 고려되어야 한다.

(1) 울진 3, 4호기 최종 안전성 분석보고서

ICCMS의 동적시험자료 작성을 위한 입력변수는 원자로 냉각재계통 온도, 가압기 압력, 원자로 냉각재의 수위, 그리고 핵연료 피복재 온도이다. 최종 안전성 분석보고서의 사고해석에 사용된 전산코드 및 사고종류, 그리고 ICCMS 입력변수들의 사고별 추이를 분석하여 입력데이터 생성 소프트웨어 검증자료로 활용한다.

(2) 동적시험 항목의 선정

Table 2. The dynamic test items for ICCMS software.

시험종류	기능모듈	시험항목	최소시험기간 (초)	최소시험항목
모듈시험	포화여유도	1. 0.5 ft^2 SBLOCA	0~20	5, 6
		2. 0.35 ft^2 SBLOCA	0~30	
		3. 0.2 ft^2 SBLOCA	0~50	
		4. 0.05 ft^2 SBLOCA	0~200	
		5. 0.02 ft^2 SBLOCA	0~200	
		6. SLB+LOOP at 100% power	0~50	
		7. SLB at 100% power	0~50	
		8. SLB+LOOP at 0% power	0~50	
		9. SLB at 0% power	0~50	
		10. LOFA	0~400	
		11. SGTR+LOOP	0~80	
		12. SGTR	0~80	
	원자로용기 수위	1. 0.5 ft^2 SBLOCA	0~140	4
		2. 0.35 ft^2 SBLOCA	0~200	
		3. 0.2 ft^2 SBLOCA	0~380	
		4. 0.05 ft^2 SBLOCA	0~1000	
		5. 0.02 ft^2 SBLOCA	0~1500	
		6. SLB+LOOP at 100% power	0~500	
		7. SLB at 100% power	0~250	
		8. SLB+LOOP at 0% power	0~500	
		9. SLB at 0% power	0~250	
		10. LOFA	2500~5000	
		11. SGTR+LOOP	0~1500	
		12. SGTR	0~1500	
	노심출구온도	1. 0.5 ft^2 SBLOCA	60~140	1
		2. 0.35 ft^2 SBLOCA	90~200	
		3. 0.2 ft^2 SBLOCA	125~320	
		4. 0.05 ft^2 SBLOCA	180~220	
		5. 0.02 ft^2 SBLOCA	200~240	
		6. SLB+LOOP at 100% power	0~500	
		7. SLB at 100% power	0~500	
		8. SLB+LOOP at 0% power	0~500	
		9. SLB at 0% power	0~500	
		10. LOFA	4600~6000	
		11. SGTR+LOOP	0~500	
		12. SGTR	0~500	
종합시험		1. 0.5 ft^2 SBLOCA	0~200	1, 4
		2. 0.35 ft^2 SBLOCA	0~300	
		3. 0.2 ft^2 SBLOCA	0~500	
		4. 0.05 ft^2 SBLOCA	0~3000	
		5. 0.02 ft^2 SBLOCA	0~6000	
		6. SLB+LOOP at 100% power	0~700	
		7. SLB at 100% power	0~600	
		8. SLB+LOOP at 0% power	0~600	
		9. SLB at 0% power	0~600	
		10. LOFA	0~1800	
		11. SGTR+LOOP	0~1800	
		12. SGTR	0~1800	

ICCMS의 충분한 기능 확인을 위해서는 기본적으로 모든 설계기준사고 및 전체 사고진행 기간을 시험대상으로 하여야 한다. 그러나 각 기능 모듈별로 반드시 필요한 사고 및 기간을 파악하므로써 효과적인 시험을 수행할 수 있으며, 소프트웨어 모듈의 사소한 수정시에도 불필요한 노력을 줄일 수 있다. 따라서 동적시험 항목의 선정은 각 사고별로 사고의 악화정도 및 추이를 고려하여 ICCMS의 기능모듈의 성능확인에 필요한 최소 시험기간 및 항목을 결정하였다. 최소 시험기간은 포화여유도 모듈의 경우는 사고 시작부터 원자로 냉각재계통의 온도 및 압력이 안정될 때까지, 원자로 용기 수위 모듈의 경우는 수위가 감소하기 시작할 때부터 회복할 때까지, 그리고 노심 출구 열전대 모듈의 경우는 원자로 용기 수위가 노심 상부에 도달할 때부터 노심 출구 온도의 증가가 끝날 때까지의 시간을 고려하여 결정하였다. 또한 소프트웨어 모듈별 최소 시험항목은 사고별 각 기능모듈의 필요 정도와 대표적인 진행추이를 갖는 사고 등을 고려하여 결정하였다. 설계기준사고 및 비상운전지침서 분석에서 나타나듯이 포화여유도모듈의 경우는 모든 사고의 초기 감지에 사용되므로 모든 고려대상 사고가 시험대상이 되지만 0.2 ft^2 이상의 소형파단 냉각재 상실사고의 경우, 사고의 초기 진행이 너무 급격하여 동적시험대상으로 부적합하다. 그리고 원자로 용기 수위모듈의 경우도 모든 사고시 수위가 감소되므로 모든 고려대상 사고가 시험대상이 되어야 하지만 소외전원 상실사고의 경우와 냉각재의 감소율 또는 원자로 용기의 냉각재 수축율이 적은 사고의 경우에는 정확도의 감소로 인해 동적시험대상으로 부적합하다. 또한 원자로용기 수위의 사고추이를 잘 나타내는 0.05 ft^2 소형파단 냉각재 상실사고가 원자로 용기 수위모듈의 기능확인에 가장 적합하다. 노심 출구 열전대 모듈의 경우는 노심이 노출되는 경우에 주로 사용되므로 소형파단 냉각재 상실사고와 급수계통 상실사고가 시험대상이 된다. 종합시험의 경우는 ICCMS의 전체적인 기능 확인이 필요하므로 앞의 각 모듈별 선정사고에 모두 포함되는 0.05 ft^2 소형파단 냉각재 상실사고가 가장 적합하지만, 이 사고의 경우에는 노심이 완전히 노출되지 않으므로 이 영역에 대한 시험을 보완하기 위하여 0.5 ft^2 소형파단 냉각재 상실사고가 추가되었다. 따라서 ICCMS 소프트웨어의 모듈시험 및 종합시험의 동적시험 항목은 표 2와 같이 선정되었다.

3-2. 동적시험 자료생성 프로그램 설계

ICCMS의 입력변수는 노심 출구온도 모듈의 경우에 노심의 반경방향으로 45개 위치에 분포되어 있는 노심 출구 열전대 신호, 원자로 용기 수위 모듈의 경우에 원자로 용기의 축방향으로 8개 위치에 분포되어 있는 가열접점 열전대 및 비가열접점 열전대 신호, 그리고 포화여유도 모듈의 경우에 가압기 압력과 원자로 냉각재계통 고온관 및 저온관 온도이다. 현재 동적시험 자료의 입력으로 사용하는 사고해석 코드의 경우 포화여유도의 입력변수에 대한 모사는 가능하지만, 노심의 반경방향으로 45개 위치 및 원자로 용기의 축방향으로 8군개 위치의 온도 분포에 대한 모사는 불가능하다. 따라서 사고해석 모사자료에서 입수 가능한 핵연료 피복재의 온도를 이용하여 노심 출구 열전대 자료들을 구하고 그리고 냉각재 수위 및 원자로 냉각재계통 온도를 이용하여 가열접점 열전대 및 비가열접점 열전대 자료들을 생산하는 알고리즘을 개발하여 이를 C 언어로 구현하였다. 이 프로그램은 노심 출구 열전대 자료를 생산하기 위한 CET 모듈과 가열 및 비가열접점 열전대 자료를 생산하기 위한 HJTC 모듈로 이루어진다.

3-2-1. CET 모듈

노심 출구 온도 모듈은 노심의 축방향으로 분포되어 있는 45개의 노심 출구 열전대 신호를 입력받아 노심 출구 온도를 계산한다. 따라서 노심 출구 온도 모듈의 계산기능을 검증하기 위해서는 45개의 노심 출구 열전대 신호가 필요하다. 사고해석 모사자료 중에는 이러한 변수가 없으므로 노심 출구 온도를 간접적으로 감시할 수 있는 핵연료 피복재의 온도를 이용하여 45개의 분포 자료를 만든다. 이 45개의 자료들의 확률모델로는 물리학의 각종실험을 행할 때 수반되는 측정오차에 대한 확률분포로서 도입된 이후, 모든 학문분야에서 일반적인 근사적 확률모형으로 적용되는 대표적인 연속확률분포인 정규분포[17]를 사용하였으며, 실제로 ICCMS 소프트웨어에서도 대표노심 출구 온도의 계산시 정규분포를 가정하고 있다. 한 개의 데이터로 정규분포를 갖는 45개의 데이터를 만들기 위해서는 우선 해당 모집단의 확률 변량, 즉 난수를 발생시켜야 한다. 모든 확률변량의 기간은 일양난수이므로 일양난수를 발생하기 위해 표준 ANSI C의 내장함수인 rand()를 이용하여 일양분포를 만들고, 이 일양난수를 사용하여 정규분포를 갖는 난수를 발생시키는 방법을 사용하였다. 정규분포를 갖는 난수의 발생방법은 중심극한정리를 이용한 방법, Box-Muller 방법, Marsaglia 방법 등이 있으나 본 연구에서는 Marsaglia 방법을 사용하였다[20].

CET 모듈은 사고해석코드의 핵연료 피복재 온도 모사자료를 시간 이력별로 입력받아 $N(\mu, \sigma^2)$, 즉 입력값을 평균으로 하고 분산이 20의 정규분포를 갖는 45개씩의 노심 출구 온도 입력 자료를 생산하며, 알고리즘은 다음과 같다.

(1) 입력값을 읽어 들인다.

(2) randomize() 함수를 호출하여 난수표를 초기화시킨다.

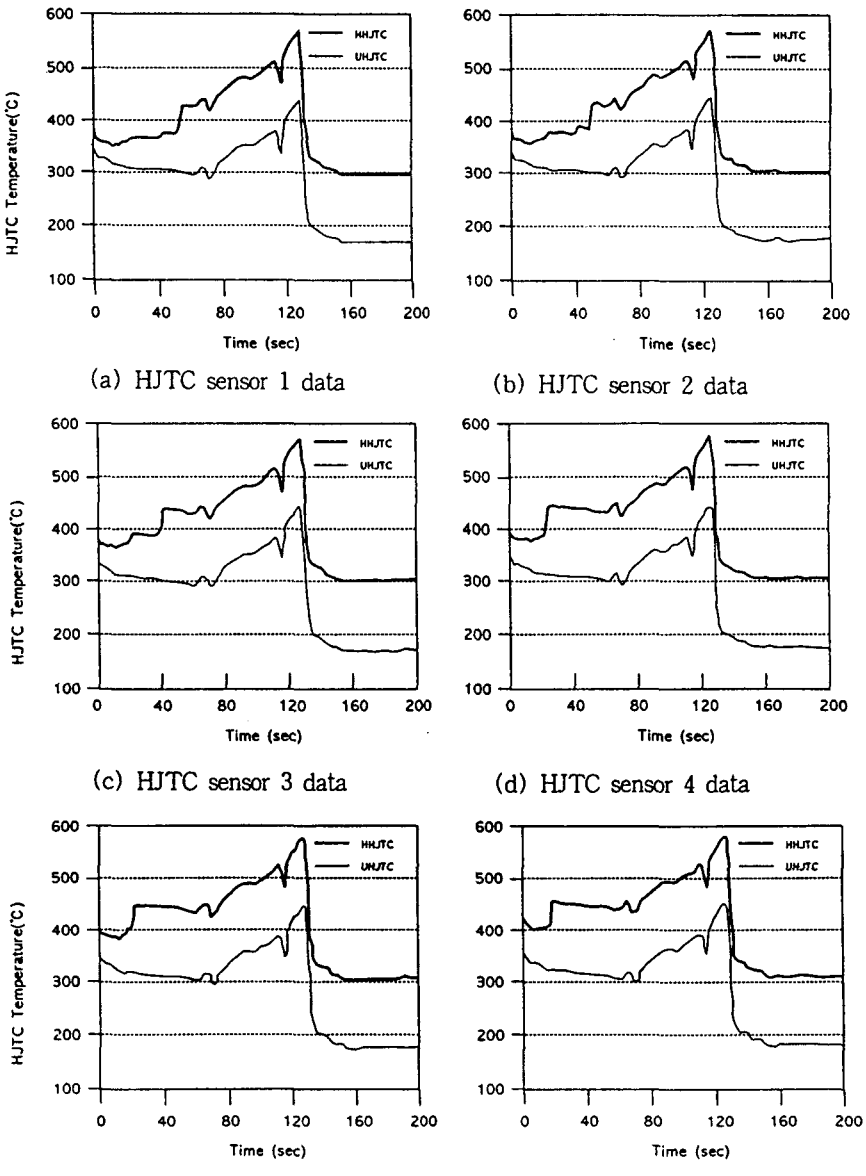
(3) U=(1.0/(RANDM_MAX+1.0)) * (rand()+0.5)의 공식으로 일양난수를 발생시킨다. 여기서 발생하는 난수는 구간(0, 1) 사이의 수이다.

(4) 45개의 정규난수 발생: 다음의 방법을 45번 수행한다. 두 개의 독립된 일양난수 u1, u2를 이용하여 두 개의 난수 x_1과 x_2를 다음의 방법으로 구한다.

$$v_1=2u_1-1$$
$$v_2=2u_2-1$$
$$s=v_1^2+v_2^2$$

If $s^2 \geq 1$이면, Then 처음부터 다시 시작하고, Else 다음식을 이용하여 난수를 얻는다.

$$x_1=v_1\sqrt{-2\log(s^2)/s^2}$$
$$x_2=v_2\sqrt{-2\log(s^2)/s^2}$$

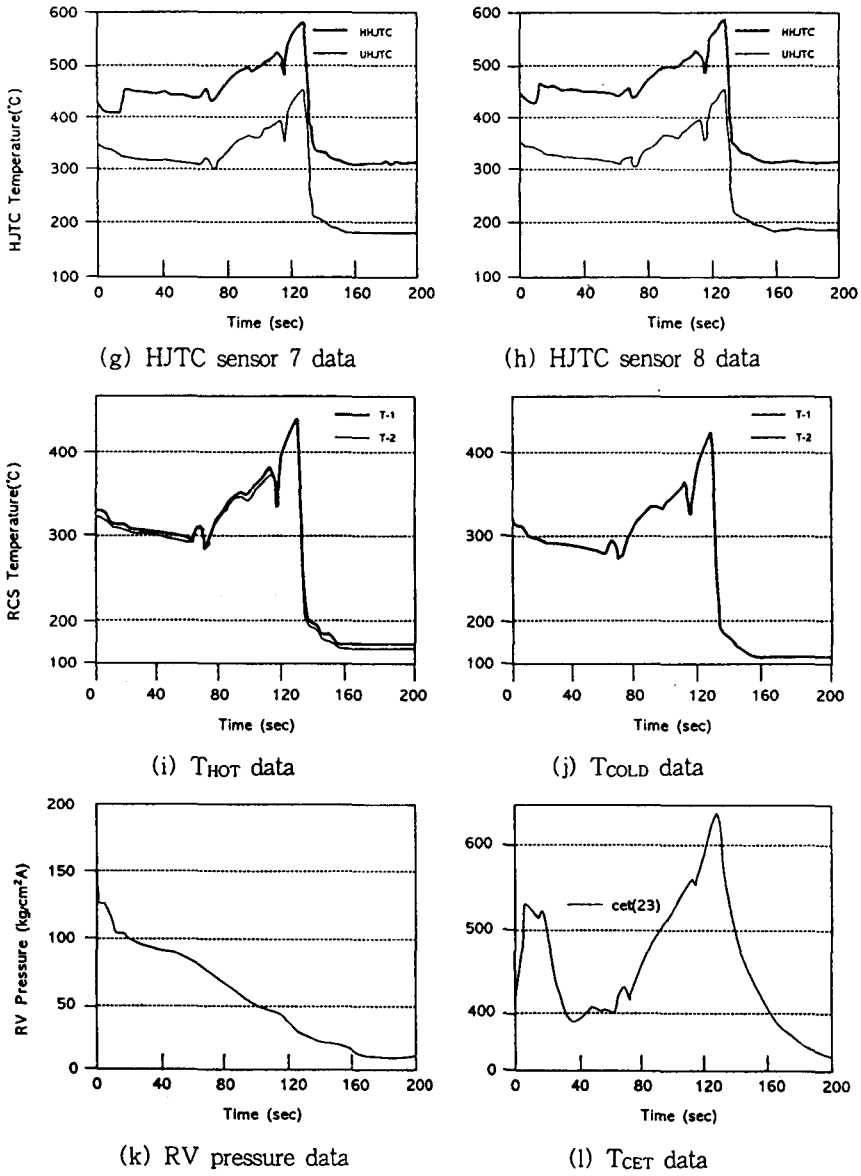


(a) HJTC sensor 1 data (b) HJTC sensor 2 data

(c) HJTC sensor 3 data (d) HJTC sensor 4 data

(e) HJTC sensor 5 data (f) HJTC sensor 6 data

Fig. 2. Dynamic test data for 0.5 ft² SBLOCA.



(g) HJTC sensor 7 data (h) HJTC sensor 8 data

(i) T_{HOT} data (j) T_{COLD} data

(k) RV pressure data (l) T_{CET} data

Fig. 2. Continued.

(5) 45개의 출력값 발생: 다음의 방법을 45번 수행한다.

표준편차(σ)=sqrt(분산)

출력=입력(μ)+표준편차(σ) * x(난수)

(6) 입력값이 없을 때까지 반복한다.

3-2-2. HJTC 모듈

원자로 용기 수위 모듈은 원자로 용기의 축방향으로 위치되어 있는 8개의 가열접점 열전대계통 센서의 가열접점 열전대 및 비가열접점 열전대 신호를 입력받아 수위를 계산하므로 이 모듈의 계산기능을 검증하기 위해서는 각 위치별 가열접점 열전대 및 비가열접점 열전대 신호가 필요하다. 따라서 사고해석 모사자료 중의 냉각재 수위 및 원자로 냉각재계통 온도변수를 이용하여 각 위치별 가열 및 비가열접점의 온도분포를 만들어야 하는데 이를 위하여 ICCMS의 수위계산 알고리즘을 사용하였다. 원자로 용기 수위의 계산 알고리즘에 의하면 원자로 용기 수위는 임의의 위치에서의 가열접점과 비가열접점의 온도차가 설정치 이상일 경우, 해당 센서가 위

치한 부분에 냉각재가 존재하지 않는다고 판단하므로 사고해석자료 중에서 냉각재 수위정보를 이용하여 각 센서 위치별 가열접점과 비가열접점 열전대간의 온도차를 계산할 수 있다. 그리고 사고시 상하위 비가열접점간의 온도차는 가열접점 열전대계통의 개발 당시 수행한 HJTC Phase III 시험 결과를 이용하였다. 계산된 온도차를 이용하여 각 열전대의 온도를 구하기 위해서는 기준온도가 필요하므로, 센서중 제일 하부의 비가열접점 열전대 온도를 원자로 냉각재계통 온도로 가정하였다. 또한 계산된 각 열전대 온도 값에 대한 가중치로 $N(\mu, \sigma^2)$의 정규난수값을 합산하여 데이터의 가변성을 고려하였다. 그리고 울진 3, 4호기 설계에 사용된 가열기의 제어논리에 따른 가열접점 열전대 제한온도 및 비가열접점 열전대 제한온도, 최소 상하위 비가열접점 열전대 온도차 설정치 등을 고려하였다.

HJTC 모듈은 사고해석코드의 냉각재 수위 및 원자로 냉각재계통 온도 모사자료를 시간 이력별로 입력받아서 각 8개씩의 가열접점 열전대 및 비가열접점 열전대 온도 입력 자료를 생산하며, 알고리즘은 다음과 같다.

(1) 입력값들을 읽어 들인다: 냉각재 수위, 원자로 냉각재계통 온도.

(2) 각 위치별 온도차 결정: 입력값이 어느 위치에 존재하는지 판단한다. 각 위치별 온도차를 구한다.

(3) 최하부 가열 및 비가열접점 열전대 온도 결정:

최하부 비가열접점 열전대 온도=원자로 냉각재계통 온도 입력값

최하부 가열접점 열전대 온도=최하부 비가열접점 열전대 온도+온도차

(4) 나머지 위치별 가열 및 비가열접점 열전대 온도 결정: 다음을 7번 수행한다.

비가열 온도차=상하위 열전대간의 최소온도차+정규난수

상위 비가열접점 열전대 온도=현 비가열접점 열전대 온도+비가열 온도차

상위 가열접점 열전대 온도=현 가열접점 열전대 온도+온도차+정규난수

(5) 계산된 8개 가열 및 비가열접점 열전대 온도의 수정: 다음을 8번 수행한다.

If 비가열접점 열전대 온도>비가열접점 열전대 상한 온도이면,

Then 비가열접점 열전대 온도=비가열접점 열전대 상한 온도+온도차

If 가열접점 열전대 온도>가열접점 열전대 상한 온도이면,

Then 가열접점 열전대 온도=가열접점 열전대 상한온도+온도차

(6) 입력값이 없을 때까지 반복한다.

3-2-3. 동적시험 자료 생성 프로그램의 검증

본 연구에서 개발된 동적시험 자료 생성 프로그램의 성능을 검증하기 위해 울진 3, 4호기의 ICCMS 설계기준 사고 중에서 제일 심각한 사고인 0.5 ft^2 소형파단 냉각재 상실사고에 대한 동적시험 자료를 생성시켰다. 가열접점(HHJTC)과 비가열접점(UHJTC)의 HJTC 온도, 각각 2개의 고온 및 저온 배관 온도, 원자로 용기 압력, 45개의 CET 중 A채널에 할당되는 23개의 CET 평균온도에 대한 추이가 그림 2에 나타나 있다.

프로그램의 성능을 확인하기 위해서 그림 2의 결과를 울진 3, 4호기 최종 안전성 분석보고서의 사고해석 결과와 비교하면 보고서 6장 및 15장에 기술된 사고해석 결과와 정확하게 일치한다. 따라서, 개발된 이 프로그램은 다른 발전소 ICCMS 소프트웨어 동적검증에 충분히 활용할 수 있을 것이다.

4. 결 론

원자력발전소 안전계통 소프트웨어는 시험절차를 개발하고 그 시험절차에 따라 소프트웨어가 개발되도록 규정되어 있다. 본 연구에서는 ICCMS 소프트웨어에 대한 동적시험 절차를 개발하였으며, 또한 절차의 1단계인 시험 수행에 필요한 동적시험 자료 작성용 프로그램을 개발하였다. 개발된 프로그램의 성능은 비교기준인 울진 3, 4호기 최종 안정성 분석보고서와 동일한 결과를 보인 것으로 입증되었다. 따라서, 본 연구에서 개발된 동적시험 절차 및 소프트웨어는 ICCMS 설계과정의 단계인 개발설비에서 수행되는 소프트웨어 모듈시험 뿐만 아니라 발전소에 설치되는 설비에 대한 최종 검증시험 수행에도 유용하게 사용될 수 있을 것으로 판단된다. 또한 본 연구에서 개발된 절차의 2단계인 소프트웨어 모듈시험 및 통합시험에 대한 연구가 지속되고 완성되어야 실질적인 활용이 이루어질 것이다. 그리고 개발된 절차에 따른 소프트웨어 개발이 이루어지면 후속으로 이어지는 울진 5, 6호기를 비롯한 북한경수로, 차세대 원자력발전소 등의 설계시 지속적으로 활용할 수 있어 개발효과가 매우 클 것으로 판단된다.

참고문헌

1. 이장수, 권기춘, 동인숙, "원전 계측제어 고신뢰도 소프트웨어 확인/검증 기술현황", 한국원자력학회지, 제26권 제4호, pp. 600-610, (1994).
2. Gideon Ben-Yaacov, et. al: "Advanced Sequence of Event Monitoring Facility at the Connecticut Yankee Nuclear Power Plant", Proceedings of the Thirties

Power Instrumentation Symposium, pp. 63-69, (1987).
3. 문채주, 이병채, 서영, "단일 처리기를 사용한 원자력 발전소 SOE 계통의 성능개선에 관한 연구", 한국에너지공학회논문지, 제5권 제2호, pp. 153-159, (1996).
4. 문채주, 서 영, 이 진, "원자력발전소 자료수집계통에 대한 보수용 소프트웨어 구현에 관한 연구", 대한전기학회논문지, 제46권 제9호, pp. 1402-1408, (1997).
5. 문채주, 이순성, 서 영, "원자력발전소 안전계통 소프트웨어 확인/검증을 위한 시험장치 개발에 관한 연구", 한국에너지공학회논문지, 제7권 제1호, pp. 96-102, (1998).
6. ANSI/IEEE-7-4.3.2, "Application Criteria for Programmable Digital Computer Systems in Safety Systems in Nuclear Power Generating Stations", (1982).
7. ANSI/IEEE-829, "Software Test Documentation", Aug. 19, (1982).
8. 00000-ICE-3514, "CPC/CEAC Phase I Test Procedure", Rev. 02, Jan. 13, (1988).
9. 00000-TS-051, "Core Protection Calculator System Phase II Test Procedure", Rev. 00, July 8, (1987).
10. 86-68200-TP-001, "SDS1 Validation Test Procedure", Rev. 00, Feb. (1994).
11. 86-68200-TP-002, SDS1 PDC Reliability Test Procedure, Rev. 00, Dec. (1994).
12. Taylor, R.P., Mills, S., Chen, S. and El-Saadany, S.: "Reliability Assessment for Safety Critical Systems", AECB paper.
13. CE NSPD-430, "Special Report on ICCMS Licensability for the KNU 11 and 12 Plants", December (1987).
14. CEN-158-P, "Evaluation of Instrumentation for Detection of Inadequate Core Cooling", (1981).
15. CEN-117, "Inadequate Core Cooling - A Response to NRC IE Bulletin 79-06C, Item 5", Oct. (1979).
16. CEN-152, "Emergency Procedure Guideline", Rev. 03, May 1987.
17. CE-NPSD-232, "Analysis of HJTC/RVLMS Performance during Accident Conditions", July (1983).
18. CA-AA-UC3-94014, "UCN 3,4 FSAR Small Break LOCA Analysis Summary Report Book", Rev.00, Sep. 29, (1995).
19. KEPCO, "UCN 3,4 Final Safety Analysis Report", Chapter 6 and 15.
20. 류충현, "C로 배우는 통계학", PC Advance, Sep. 20, (1994).