한국에너지공학회지(1998), 제7권 제1호
Energy Engg. J(1998), Vol. 7, No. 1, pp. 96~102

원자력발전소 안전계통 소프트웨어의 확인/검증을 위한 시험장치 개발에 관한 연구

이순성 · 서 영 · *문채주
한국전력기술(주) 원자로설계개발단, *목포대학교 전기공학과

A Study on the Development of Test Facility for Safety System Software V/V in Nuclear Power Plant

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

요 약

원자력 안전계통의 일부분인 컴퓨터의 사용은 일반 산업분야에서 명시되지 않은 부가적인 요건 즉 소프트웨어의 확인 및 검증, 하드웨어의 품질요건이 요구된다. 원자력 발전소에서 사용되는 컴퓨터는 컴퓨터 하드웨어, 소프트웨어, 펌웨어 및 연계장치를 포함하는 시스템이다. 원자력 안전등급을 갖는 컴퓨터 시스템을 개발하기 위해서는 우선적으로 개발환경이 요구되고 개발된 소프트웨어는 원자력 코드 및 표준에 따라 확인 및 검증되어야 한다. 이러한 요건 때문에 원자력 발전소 안전계통의 하나인 부적절노심감시계통에 대한 시험설비가 개발되었다. 시험설비는 입출력 모의설비, 자료수집계통 케비넷 및 감시컴퓨터의 3부분으로 구성된다. 이 시스템의 성능은 수동시험절차에 따라 검증되었다.

Abstract — The use of computers as part of nuclear safety systems elicits additional requirements-software verification and validation (v/v), hardware qualification-not specifically addressed in general industry fields. The computer used in nuclear power plants is a system that includes computer hardware, software, firmware, and interfaces. To develop the computer systems graded with nuclear safety class, the developing environments have to be required in advance and the developed software have to be verified and validated in accordance with nuclear code and standards. With this requirements, the test facility for Inadequate Core Cooling Monitoring System (ICCMS) as one of safety systems in the nuclear power plants was developed. The test facility consists of three(3) parts such as Input/Output (I/O) simulator, Plant Data Acqusition System (PDAS) cabinets and supervisory computer. The performance of the system was validated by manual test procedure.

1. 서 론

최근 원자력발전소 제어계통은 지속적인 전자산업 발전에 따라 기존에 사용되고 있는 설비들이 디지털 기기로 교체되고 신규 설계되는 원전에도 디지털 기술이 적용되고 있다. 이러한 추세에 따라 디지털 기술을 반영한 소프트웨어가 사용되게 되어있으나 이는 공통모드고장, 정량적인 소프트웨어 신뢰도 및 안전성 확보 등의 문제를 야기시키고 있다. 사용자, 개발자와 규제자가 모두 인정하는 소프트웨어의 확인 및 검증절차와 설비들은 계측제어계통 소프트웨어의 품질을 보증할 수 있고 소프트웨어의 신뢰를 높임으로써 전체 디지털시스템의 품질을 높일 수 있다[1-3].

디지털 계측제어계통의 소프트웨어에 대한 품질보장을 위한 규제요건중 가장 기본이 되는 IEEE 7-4.3.2-1993이 제기되어 이 요건을 만족시키기 위한 여러 가지 절차 및 설비가 요구되었다. 원자력발전소의 대표적인 안전계통은 발전소 보호계통, 노심보호연산기, 주요변수

감시계통, 부적절노심냉각감시계통 등이 있으며, 이 계통들은 소프트웨어 규제요건을 만족시켜야 한다. 본 연구에서는 부적절노심냉각감시계통을 그 대상으로 하였으며, 이 계통은 안전등급의 컴퓨터계통으로서 하드웨어는 발전소 자료수집계통에서 제공되고 고품질의 소프트웨어가 요구된다. 지금까지 ICCMS 소프트웨어는 발전소별로 외국사에 의해 개발되고 적용되었으나, 영광 5, 6호기 이후부터 설계되는 모든 원자력발전소에 대해 이 소프트웨어를 국내에서 개발하도록 계획되어 있다[4][5]. 이에 따라 독자적으로 ICCMS 소프트웨어를 개발하여 시험, 확인 및 검증을 수행하여야 하며, 이를 위해서는 시험장비에 대한 설계 및 제작이 우선적이다. 본 연구에서는 실제 발전소에 적용되는 동일한 설비로 개발환경을 갖추기 위해 소프트웨어가 구동되는 CCC(Concurrent Computer Inc.)사의 3205 컴퓨터, 입출력신호가 처리되는 CPI (Computer Product Inc.)사의 입출력카드를 선정하였다. 또한, 입출력신호 처리설비는 siemens사의 PLC (Programmable Logic Controller)를 채택하여 입력신호를 생성시키고, 입출력신호를 감시하고 계산결과를 표시하는 각종 화면은 Citect을 사용하여 구현하였다.

2. 부적절노심냉각감시계통

ICCMS는 부적절한 노심 냉각상태를 야기하는 사고가 발생했을 때 운전원에게 노심의 정보를 제공하기 위해 설치된 계통이며, 원자로 용기내의 냉각수 수위, 핵연료 출구온도 및 과냉각 여유도를 제공한다. 이러한 정보를 근간으로 설계기준사고와 가상사고시 운전원이 적절한 조치를 취하도록 한다. ICCMS 설비는 발전소 자료수집계통(PDAS: Plant Data Acquisition System)에 포함되어 있다. 이 발전소자료수집계통은 원자력발전소 전 계통의 자료를 수집하는 계통이므로 여러 개의 부속계통으로 구성되어 있으나 본 연구의 목적상 ICCMS와 관련된 계통만을 기술한다. 이 계통은 4개의 안전채널과 3개의 비안전채널로 구성되어 있다. ICCMS는 4개의 안전채널중 A, B채널에서 이중화 개념으로 운전되고 현장신호는 4개의 채널에서 수집된다. 즉, ICCMS 계통은 C채널로 입력된 자료는 광케이블에 의해 A 채널로 보내고, D 채널로 입력된 자료는 B 채널로 보내서 각각 A, B채널에서 처리된다. Fig. 1의 ICCMS 계통구성도에서 나타낸 바와 같이 발전소 자료수집계통은 입출력 신호처리, ICCMS 인터페이스 및 데이터 링크 등의 기능을 갖고 있다.

ICCMS에 관련된 입출력 처리기능을 보면 한 개의 채널당 현장으로부터 2개의 고온배관 온도, 2개의 저온배관 온도, 1개의 가압기 압력, A 채널은 23개 B 채널은

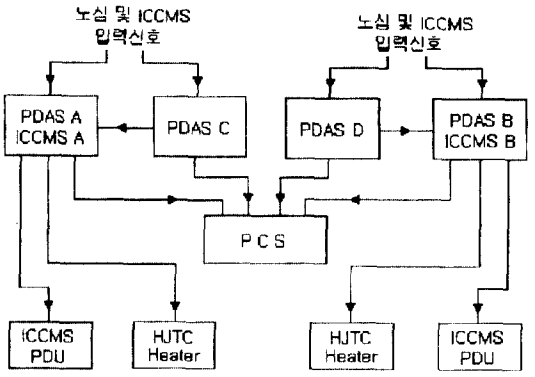

Fig. 1. ICCMS structure.

22개의 노심 출구온도 및 8개의 HJTC(Heated Junction ThermoCouple) 감지기 신호를 입력받는다. 본 연구에서는 이중화된 A, B채널중 A 채널을 대상으로 설계하였다. ICCMS 소프트웨어에서 계산된 값은 각각 1개의 원자로 냉각재 및 상부 포화여유도, 노심출구 포화여유도, 노심출구 온도 대표값, 원자로 용기 헤드(Head)영역 냉각재수위 및 원자로 용기 프레늄(Plenum)영역 냉각재수위 등이 있다. 이 신호들은 독립적인 화면표시설비(PDU: Plasma Display Unit)와 발전소 컴퓨터계통(PCS: Plant Computer System) 그리고 기록계 등으로 보내진다. 또한 4개의 경보출력을 제공하여 운전원이 비정상 운전상태를 인식하도록 한다. 여기서 사용된 미니컴퓨터, PDU, HJTC 가열기 전력제어장치, 입출력카드 등은 안전등급의 규제요건을 적용 받는다.

3. 하드웨어 구성

3-1. 하드웨어 설계

시험설비는 ICCMS가 구동되는 발전소 자료수집계통과 가상입력신호를 발생시키고 입출력신호를 비교 및 감시하는 입출력 신호처리설비로 구분된다. ICCMS 계통구성에 사용되는 발전소 자료수집계통은 A, C 채널로 구성된다. Fig. 2와 같이 입출력 신호처리설비는 A, C채널로 입력신호를 보내고 실 시스템과 동일하게 C채널은 A채널로 입력신호를 보내 A채널에서 ICCMS 변수를 계산한다. 한편, 프로세싱 컴퓨터로 각종 시험 시나리오를 프로그램 하여 개발된 소프트웨어의 및 검증작업을 손쉽게 수행하도록 설계하였다.

3-2. 시험설비 제작

3-2-1. 발전소 자료수집계통 채널

1) 케비넷: 2중반의 표준형으로 신호보호 및 처리카드를 좌측에, 각종 입출력 접속단자와 프로세싱 컴퓨터를

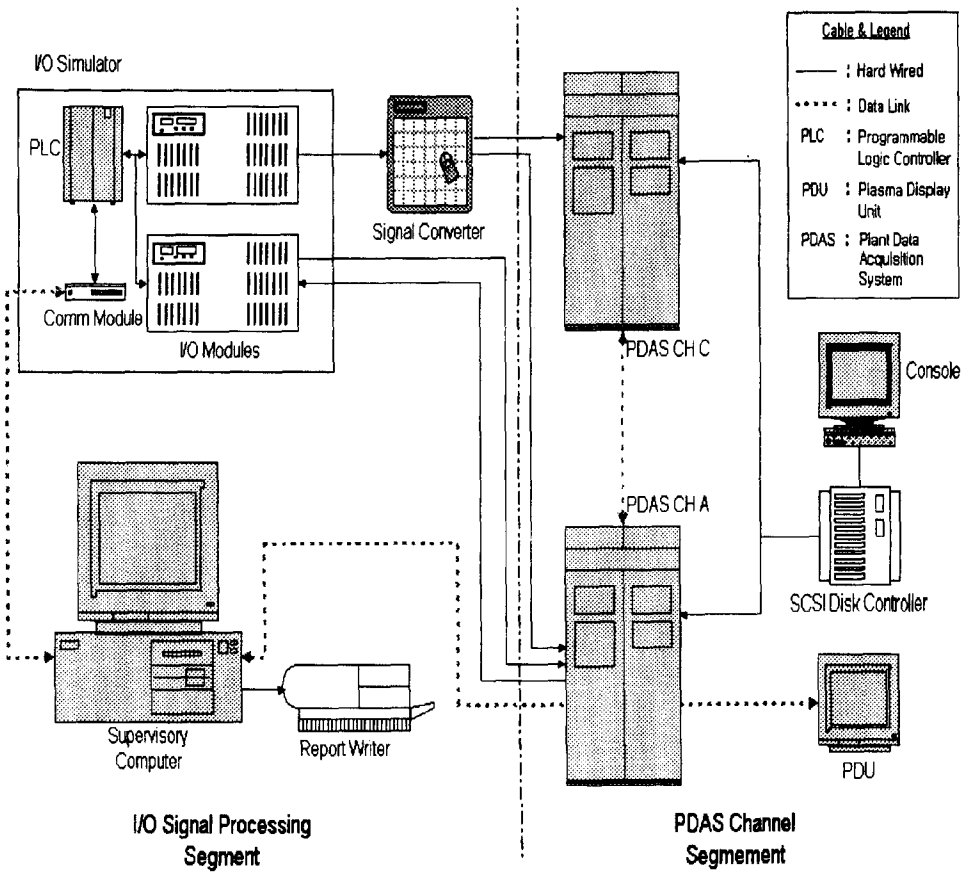

Fig. 2. Hardware configuration for test facility.

우측에 그룹지어 설치하여 케이블 접속 및 연결에 편의성을 주었다.

2) 입출력 접속단자(BTSCA: Barrier Terminal Strip Cable Assembly): 입출력 신호처리 설비에서 제공하는 0~10 V 및 0~100 mV용 단자와 같은 모델의 아날로그 단자를 사용한다. 외부에서 인입되는 과전압/전류로부터 프로세싱 카드를 보호하기 위해 보호카드를 사용하며, 모든 입출력신호가 이 카드를 통하여 프로세싱 카드로 입력된다.

3) UIOC(Universal Input Output Controller) 카드: 16개의 프로세싱 카드를 내장할 수 있으며 각 프로세싱 카드의 데이터를 backplane을 통해 제어한다.

4) 3205 컴퓨터: 컴퓨터는 원자력 발전소와 동일한 CCC사의 3205 컴퓨터를 두채널에 각각 1대씩 설치하였다. 이 채널 컴퓨터는 CPU/memory 보드, 입출력제어 보드, EPROM 보드, 디스크/테이프 드라이브 인터페이스 보드 등으로 구성된다.

5) 프로세싱 카드: 아날로그 입력 프로세싱 카드는 gate 카드와 A/D 변환카드로 구성되고 gate 카드는 8개의 차동입력을 처리하며 A/D 변환카드는 gate 카드로부터 받은 신호를 14비트 디지털 값으로 변환시킨다. 아날로그 출력 프로세싱 카드는 4채널 D/A 변환카드이며, 12비트의 레지스터를 갖는다. 이외도 접점입력, 주파수입력, 상태변환감지, 접점출력, 펄스입력, 전원접점 감지 및 감시, 고정형 노내검출기 입력 등의 프로세싱 카드를 시험설비의 범용성을 위해 설치하였다.

6) PDU: PDU는 touch screen 제어방식의 화면표시기이며, 시험관리 소프트웨어의 시험 화면과 동일한 출력을 제공함으로서 시험결과의 교차검사(cross check)가 가능하도록 구성되었다.

3-2-2. 입출력 신호처리설비

입출력 신호처리설비는 Fig. 2와 같이 발전소 자료수집 채널 A, C와의 연계부분(interface)을 담당하는 입출력설비와, 시험입력자료 작성 및 시험결과 처리를 담당하는 프로세싱 컴퓨터의 두 부분으로 구성된다.

1) 신호제어기: 신호제어기의 입력 처리부분은 프로세싱 컴퓨터로부터 제공되는 On/Off 시험입력값을 I/O 모듈로 전달하거나, 0~32000의 시험입력값을 받아 0~

10 V 값으로 변환한 후, I/O 모듈로 전달하고, 출력 처리부분은 발전소 자료수집 채널로부터 제공되는 데이터를 프로세싱 컴퓨터로 전달하는 기능을 수행하며 siemens사의 TI545 PLC를 사용하였다.

2) I/O 모듈: I/O 모듈은 신호제어기나 발전소 자료수집 채널로부터 On/Off 및 0~10 V 값을 받아 외부로 실제 입, 출력하는 기능을 수행하며 siemens사의 TI505 아날로그/디지털 입출력 카드들로 구성되었다.

3) 통신모듈: 통신모듈은 프로세싱 컴퓨터와 신호제어기간의 양 방향 통신을 제어하며, siemens 사의 TI505 통신(network interface)카드로 구성되었다.

4) 신호변환기: 신호변환기는 0~10 V의 아날로그 출력카드의 시험입력값을 0~60 mV의 열전대 신호로 변환하기 위해 사용되며 신우정밀사의 DPSI-4B1-Y 신호분리기(signal isolator)들로 구성되었고, 또한 미세전압 사용에 따른 잡음제거를 위해 필터 및 차폐(shield) 부분이 추가되었다.

5) 프로세싱 컴퓨터: 종합 시험관리, 시험자료 작성, 그리고 모의 소프트웨어가 실행되는 주 컴퓨터로서 intel pentium 프로세서와 두 개의 직렬통신 모듈, 그리고 프린터로 구성되었다. 프로세서는 여러 가지의 시험입력 생성 및 시험출력 분석, 그리고 화면 표시를 수행하는 종합 시험관리 소프트웨어를 실행시키며, 필요시 시험자료 작성 및 모의 소프트웨어를 수행시킬 수 있다. 직렬 통신모듈은 신호제어기와의 인터페이스를 제어하는 모듈과 발전소 자료수집 채널과의 인터페이스를 제어하는 모듈의 두 부분으로 구성되었고 시험 결과를 출력하기 위해 프린터가 연결되어 있다.

4. 소프트웨어 구성

본 시험설비를 개발하는 목적은 Fig. 3과 같이 ICCMS 소프트웨어를 시험하기 위한 것이며, 본 설비에서 사용되는 소프트웨어는 기존 계통에서 사용되는 소프트웨어 모듈과 설비개발용 소프트웨어 모듈 및 통신 소프트웨어 모듈로 나누어진다.

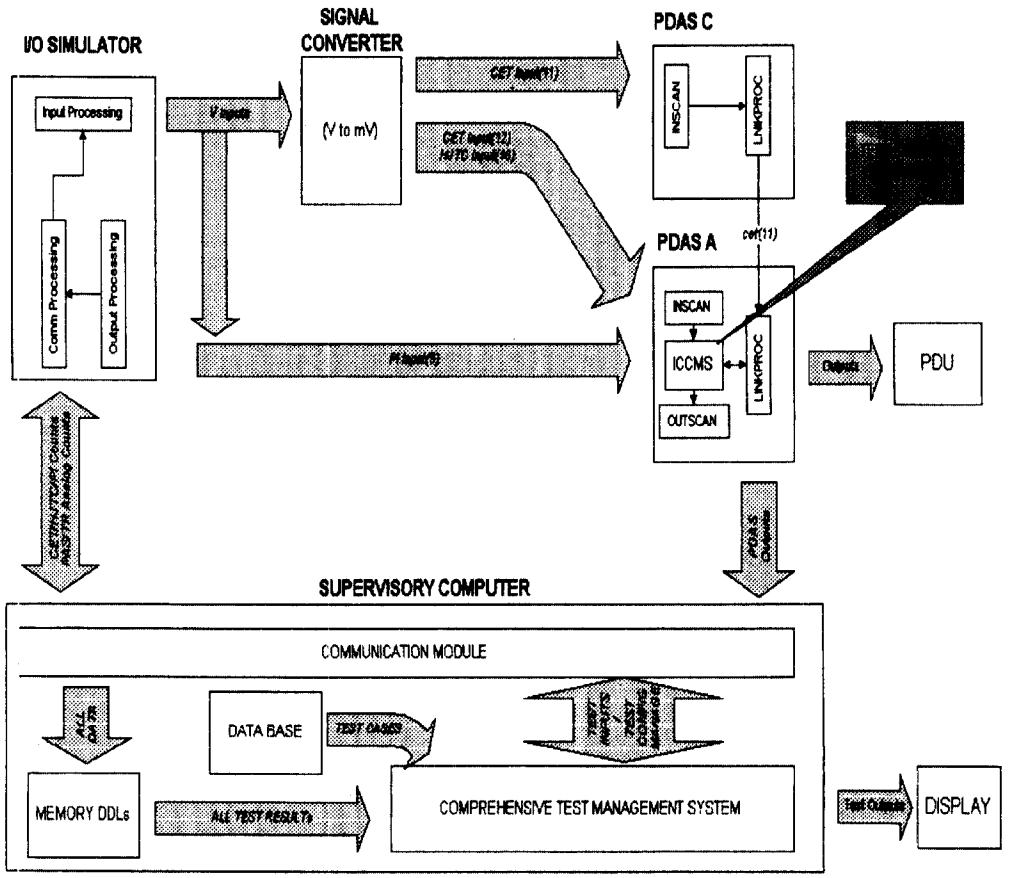

Fig. 3. Software configuration for test facility.

4-1. 계통 소프트웨어 모듈

계통 소프트웨어 모듈은 PDAS에서 사용되는 소프트웨어 및 시험하고자 하는 ICCMS 소프트웨어가 있다. 이 소프트웨어는 본 연구에서 개발한 것이 아니기 때문에 간략하게 기술한다.

1) PDAS 소프트웨어 모듈에는 Fig. 3에 표시된 바와 같이 입력데이터를 처리하는 INSCAN 모듈, 데이터통신을 관장하는 LINKPROC 모듈 그리고 처리된 데이터를 출력시키는 OUTSCAN 모듈이 있다.

2) ICCMS 모듈은 ICCMS의 모든 기능을 처리하는 모듈로서 PDAS 모듈과 연계하여 운영된다.

4-2. 개발 소프트웨어 모듈

개발 소프트웨어는 시험설비를 운영하기 위해 개발된 소프트웨어 모듈로서 다음과 같이 구성된다.

1) 종합 시험관리 소프트웨어

종합 시험관리 소프트웨어의 전체 구조 및 화면은 Ci사의 monitoring and control system 개발 환경인 Citect에서 제공하는 라이브러리를 이용하였으며, 시험결과 분석 및 처리는 Citect에서 제공하는 프로그래밍 개발 도구인 Cicode라는 Script 언어를 사용하여 개발하였다. 종합 시험관리 소프트웨어의 구성은 Fig. 4와 같이 일반시험 부분, 응용시험 부분, 시험구성 부분, 보안 부분, 그리고 보조도구/유틸리티 부분으로 이루어지며, 각 부분별 기능 및 구성은 아래와 같다.

(1) 일반시험: 부적절노심냉각감시계통의 입력처리 기능을 검사하기 위한 초기시험 부분과 포화여유도, 원자로용기수위, 그리고 노심출구온도의 세 계산모듈의 기능을 검사하기 위한 기능시험 부분으로 구성된다. 이 중에서 원자로용기수위에 대한 계산모듈의 수행화면은 Fig. 5와 같다. (2) 응용시험: 일반시험에서 수행되는 세 계산모듈에 대한 자동시험을 수행하는 자동시험 부분과 시간 이력별로 연속 입력시험 자료를 제공하여 동적 환경에서의 성능을 검사하는 동적 시험 부분, 그리고 발전소 자료수집 채널에 탑재되어 시험되는 원본 소프트웨어와 동일한 알고리즘의 이종언어로 작성된 시뮬레이션 소프트웨어에 동일한 입력 시험자료를 제공하여 시험 소프트웨어의 성능을 검증하는 신뢰도 시험부분으로 구성된다. 각 시험은 Fig. 6과 같은 추이감시화면을 포함하여 진행과정을 온라인으로 확인할 수 있다.

(3) 시험구성: 일반시험에서 사용되는 시험 입력자료를 작성하기 위한 편집기 부분 및 시험 수행결과를 보여주고 분석할 수 있는 시험분석기 부분으로 구성된다.

(4) 보안: 사용자 로그인 및 로그아웃을 검사하는 부분으로 접근 가능한 사용자를 3 종류로 구분하여 모든 시험화면 및 편집기 화면 등을 사용자별로 접근 권한을 제한함으로써 시험시 발생 가능한 인적오류를 대비하였다.

(5) 보조도구/유틸리티: 사용자 등록 및 접근권한을 편집하는 부분과 시스템을 정지하는 부분, 그리고 입출

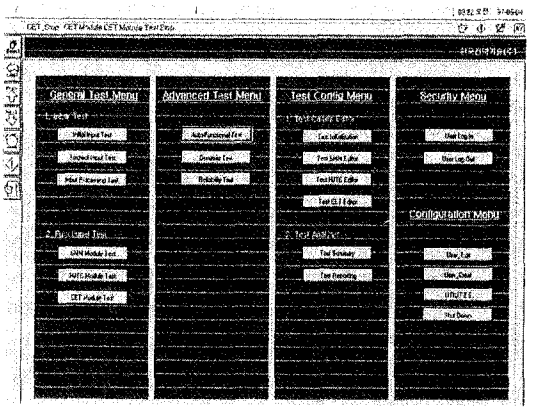

Fig. 5. Display of calculation module for reactor vessel water level.

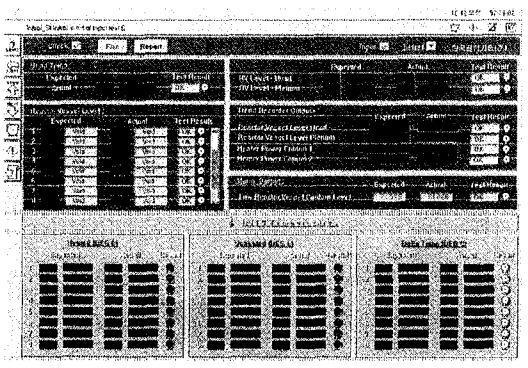

Fig. 4. Main display structure for overall test management.

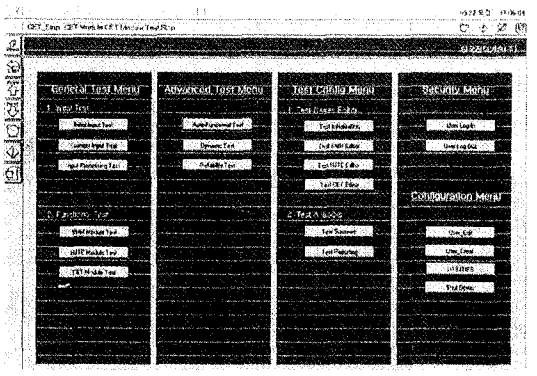

Fig. 6. Trend display for dynamic and reliability test.

력신호처리 설비에 포함되는 각 하드웨어들의 상태 검사 및 보정, 그리고 계산기나 데이터베이스 편집기 등의 각종 유틸리티를 실행하는 부분으로 구성된다.

4-3. 통신 소프트웨어 모듈

통신 소프트웨어는 발전소 자료수집 채널에 탑재된 시험 소프트웨어의 계산 변수들을 프로세싱 컴퓨터로 직접 받기 위해, 19.2 kbauds의 RS-232 링크라인을 이용한 직렬 데이터 통신방법을 Boland사의 C/C++ 4.5를 사용하여 개발하였다. 통신 소프트웨어는 종합 시험관리 소프트웨어의 실행 초기에 구동되나, 별도로 메모리에 상주하며 500 msec 주기로 발전소 자료수집 채널로부터 오는 데이터를 받아 처리한다.

5. 시험 및 검증

5-1. 데이터 전송시험

데이터의 흐름은 Fig. 3과 같이 먼저 입출력모의설비에서 생성한 아날로그 신호를 PDAS에 입력하고 이를 디지털 값으로 변환시킨다. 이 디지털 값은 ICCMS로 보내지고 여기서 공학단위로 다시 변환하여 PDU에 표시한다. 한편, 이 공학단위 값은 전송라인(data link)을 통해 다시 입출력모의설비로 보내 감시화면에 표시한다. 따라서, 데이터 전송에 대한 시험은 입출력모의설비의 감시화면에 표시된 값과 PDU에 표시된 값을 비교하여 동일한 값을 가질 경우 데이터 전송은 이상이 없는 것으로 판정하였다. Table 1은 데이터의 전송시험 결과를 표시한 것이며, PLC 출력값과 신호변환기의 출력값은 오실로스코프로 확인하였다. 또한, 입출력모의설비의 감시화면에 표시된 값과 PDU에 표시된 값이 동일함을 확인하였으며, 데이터의 전송은 적합한 것으로 판정하였다.

5-2. 입출력모의설비 성능시험

입출력모의설비의 성능은 입출력모의설비가 생성한 열전대 아날로그 신호를 전송라인을 통해 PDAS에서 받은 공학단위 값과 입력된 동일한 열전대 아날로그 신호에 대해 예상되는 공학단위 값을 계산하여 비교하므로 써 그 성능을 판정한다. 입력된 열전대 아날로그 신호에 대한 공학단위 값은 열전대(K형) 참조표[6]를 사용하여 예상치를 계산하였다. 또한, 입출력모의설비가 생성한 동일한 아날로그 신호는 PDAS가 읽어들인 디지털 값(PDAS buffer에 위치)으로 확인하였다. 아날로그 입력 값은 mV 단위이며, 실 시스템에서 정상운전값은

Table 1. Test results for data transmission.

Supervisory Computer Input Value	PLC Output (V)		Signal Converter Output (mV)		PDU Display	Suprvisory Computer Actual Value Display
	Expected Value	Actual Value	Expected Value	Actual value		
20	2	2	20	20	485	485
10	1	1	10	10	243	243

Table 2. Performance test results.

Test Input (mV)	Expected Raw Data	Expected Engineering Data	Actual Raw Data	Actual Engineering Data	Error	Test Evaluation
1.00	000 0110 0110	25°C	000 0101 1100	22°C	-3°C	OK
2.00	000 1100 1101	50°C	000 1100 1000	48°C	-2°C	OK
3.02	001 0011 0101	74°C	001 0010 1001	71°C	-3°C	OK
4.01	001 1001 1010	98°C	001 0010 1001	95°C	-3°C	OK
5.00	010 0000 0000	122°C	001 1111 0110	119°C	-3°C	OK
6.02	010 0110 1000	147°C	010 0101 1101	144°C	-3°C	OK
7.02	010 1100 1110	172°C	010 1100 1000	170°C	-2°C	OK
8.02	011 0011 0101	197°C	011 0010 1001	194°C	-3°C	OK
9.02	011 1001 1011	222°C	011 1001 0000	219°C	-3°C	OK
10.02	100 0000 0010	247°C	011 1111 0110	244°C	-3°C	OK
11.01	100 0110 0111	271°C	100 0101 1101	268°C	-3°C	OK
12.00	100 0110 1001	295°C	100 1100 0011	292°C	-3°C	OK
13.03	101 0011 0110	320°C	101 0010 1100	317°C	-3°C	OK
14.04	101 1001 1101	344°C	101 1001 0010	341°C	-3°C	OK
15.00	110 0000 0000	367°C	101 1111 0111	365°C	-2°C	OK
16.01	110 0110 0111	391°C	110 010 1101	388°C	-3°C	OK

285℃에서 305℃ 범위이므로 약 400℃ 까지 시험하였다. 총 44개의 입력신호중 1개의 입력에 대한 시험결과는 Table 2와 같이 온도오차가 ±3℃ 이내에 있으며, 이 경우 A/D 변환오차 및 보정오차 등을 포함하므로 그 결과는 설계요건[7]에 적합한 것으로 판정하였다. 나머지 43개의 입력신호도 Table 2와 같이 유사한 결과를 얻었다. 기대값보다 실제값이 모두 적게 나오는 것은 오차보정시 일정한 조정값으로 조절하였기 때문에 나타난 것으로 생각된다.

6. 결 론

원자력발전소 부적절노심냉각감시계통의 시험설비가 개발되었다. 성능시험을 거친 본 시험설비를 이용하여 안전등급의 소프트웨어인 부적절노심냉각감시계통 소프트웨어에 대한 시험 및 검증절차를 수행할 수 있으며, 후속 설계되는 동일계통에 대한 소프트웨어의 개발에 활용 및 다른 안전계통 시험설비 개발에 응용될 수 있을 것이다. 또한, 본 연구를 기반으로 차세대 원자로개발 업무수행시 안전계통의 시험설비 개발에도 활용할 수 있을 것으로 판단된다.

참고문헌

1. 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).
2. 이장수, 권기춘, 동인숙, "원전 계측제어 고신뢰도 소프트웨어 확인/검증 기술현황", 한국원자력학 회지, 26(4), pp. 600-610, (1994).
3. 권기춘, "원전 개량형 계측제어계통 기술개발 동향", 제어. 자동화. 시스템 공학회지, 2(5), pp. 34-42, (1996).
4. 문채주 외 4인, "원자력발전소 부적절노심감시계통의 시험장치 설계 및 제작", '97 대한전기학회 창 립 50주년 하계학술대회 논문집, pp. 2453-2455, (1997).
5. IEEE, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations", IEEE Std 7-4.3.2-1993, (1994).
6. "Temperature Measurements Thermocouples", ANSI/MC96.1-1982, pp. 25-27, ISA.
7. KOPEC, "Design Specification for ICCMS for YGN 5&6", (1997).
8. Concurrent Computer Corporation (CCC), "OS/32 Supervisor Call (SVC) Reference Manual", 48-038 F00 R03.
9. Concurrent Computer Corporation (CCC), "OS/32 System Support Run-Time-Library Reference Manual", 48-152, F00 R02.
10. Ci Technologies, "Citect Programmer's Reference", (1995).
11. Siemens, "Sigmatic TI505 Programming Reference User Manual", (1995).
12. Siemens, "Sigmatic TI545 System and I/O Manual Set", (1994).
13. Siemens, "Sigmatic TI505/TI500 TISOF2 5.0", (1995).