KAERI/CM-1069/2007

디지털 원자로 안전계통 개발

A development of Digital reactor safety system

안전등급 제어기기(PLC) RTOS 고신뢰도화 및 RPS 구조 검증

High-Reliable PLC RTOS Development and RPS Structure Analysis

KAERI

2008. 4

연구기관

(주)에네시스

한국원자력연구원

제 출 문

한국원자력연구원장 귀하

본 보고서를 “안전등급제어기기(PLC) RTOS 고신뢰도화 및 RPS 구조 검증” 과제의 보고서로 제출합니다.

2008. 4. 30.

주관연구기관명 : (주)에네시스

주관연구책임자 : 손 한 성

연 구 원 : 송 덕 용

〃 : 손 대 성

〃 : 김 진 혁

보고서 초록

<table>
<tr><td>과제관리번호</td><td>KAERI/CM-1069/2007</td><td>해당단계 연구기간</td><td>2006. 5. 1 ~2008. 4. 30</td><td>단계 구분</td><td>(4차) / (총2단계)</td></tr>
<tr><td rowspan="2">연구사업명</td><td>중 사 업 명</td><td colspan="4">원자력중장기계획사업</td></tr>
<tr><td>세부사업명</td><td colspan="4">원전기술혁신</td></tr>
<tr><td rowspan="2">연구과제명</td><td>대 과 제 명</td><td colspan="4">디지털 원자로 안전계통 개발</td></tr>
<tr><td>세부과제명</td><td colspan="4">안전등급제어기기(PLC) RTOS 고신뢰도화 및 RPS 구조 검증</td></tr>
<tr><td>연구책임자</td><td>손한성</td><td>해당단계 참여연구원 수</td><td>총 : 4 명
내부 : 4 명
외부 : 0 명</td><td>해당단계 연구비</td><td>정부: 230,000 천원
기업: 0 천원
계: 230,000 천원</td></tr>
<tr><td>연구기관명 및 소속부서명</td><td colspan="2">(주)에네시스 시스템사업부</td><td>참여기업명</td><td colspan="2"></td></tr>
<tr><td>국제공동연구</td><td colspan="5">상대국명 : 상대국연구기관명 :</td></tr>
<tr><td>위 탁 연 구</td><td colspan="5">연구기관명 : 연구책임자 :</td></tr>
<tr><td colspan="5">요약</td><td>보고서 면수</td></tr>
<tr><td colspan="6">안전등급제어기기(PLC) RTOS 고신뢰도화 및 RPS 구조 검증 과제의 최종 목표는 안전계통 중 특히 안전등급 PLC인 POSAFE-Q의 프로세서 모듈 소프트웨어의 고신뢰도화 개발 및 RPS 구조 검증을 통한 계통 및 소프트웨어 설계 지원을 수행하기 위함이다. 이를 위해서 본 연구에서는 POSAFE-Q 및 RPS 개발자에게 안전-필수 소프트웨어 개발 시 필요한 소프트웨어 요구사항 명세서 및 소프트웨어 설계 명세서 작성, 컴포넌트 시험 및 통합 시험 수행을 직접 지원하며, RTOS 고신뢰도화 및 RPS 구조 검증에 필요한 핵심 기술을 지원하였다. 이러한 지원 노력은 고신뢰도화된 소프트웨어를 탑재한 POSAFE-Q 프로세서 모듈로 결실을 맺었으며, KNICS만의 독특한 설계를 가지며 안전성 및 신뢰성이 향상된 RPS 설계로 결실을 맺었다.</td></tr>
<tr><td rowspan="2">색 인 어 (각 5개 이상)</td><td>한 글</td><td colspan="4">안전등급제어기기, 원자로보호계통, 리얼타임 운영체제, 설계명세서, 고신뢰도</td></tr>
<tr><td>영 어</td><td colspan="4">Safety Grade PLC, RPS, RTOS, SDS, High Reliability</td></tr>
</table>

요 약 문

Ⅰ. 제 목

안전등급제어기기(PLC) RTOS 고신뢰도화 및 RPS 구조 검증

Ⅱ. 연구개발의 목적 및 필요성

○ 기술적 측면

원자력발전소는 그 특성상 안전성이 매우 강조되는 시스템이다. 발전소보호계통을 포함하는 계측제어계통은 원전에서 인간의 두뇌와 같은 역할을 담당하는 계통으로서 원전 전체의 안전성은 물론 운전에도 매우 중요한 영향을 미친다. 따라서 발전소보호계통과 같은 계측제어계통의 성능을 향상시키고 높은 수준의 신뢰도를 보장하기 위한 기술을 개발하는 것은 원전의 경제성 및 안전성 향상에 결정적인 효과를 가져다 줄 수 있을 것이다.

한편 안전이 중요한 원자력발전소의 보호계통에 소프트웨어 기반의 기기를 사용하려고 할 때 확인 및 검증은 필수적으로 수행되어야 하며, 개발된 보호계통의 신뢰도 향상 및 품질보증의 측면에서 이 기술의 중요성은 아무리 강조해도 지나치지 않을 것이다. 일반적으로 소프트웨어 기반 기기 및 계통의 신뢰성 및 안전성은 하드웨어의 경우와는 다르게 기기의 개발과정 자체를 포함하는 엄격한 품질관리 체계를 가지고 철저하게 관리함으로써 향상될 수 있다고 알려져 있다. 따라서 확인 및 검증이 소프트웨어 기반 기기 및 계통의 안전성을 보장하기 위한 핵심기술이라고 할 수 있으며, 또 이것은 인허가 문제와 직결되어 있기 때문에 기술적으로 매우 중요하다. 전 세계적으로도 확인 및 검증 기술의 중요성을 인식하고, 특히 항공우주, 원자력, 교통, 통신 등 안전성 및 경제성이 매우 중요한 분야에서 확인 및 검증 기술의 확립을 위해 많은 노력을 기울이고 있다. 그런데 소프트웨어 기반 기기 및 계통이 적용되는 분야에 따라 요구되는 확인 및 검증의 수준 등이 바뀔 수 있는 것이어서, 이 기술의 확립은 적용 분야에 대한 철저한 이해를 바탕으로 해야 가능하다.

본 과제에서 개발하고자하는 안전등급제어기기 실시간 운영체제 소프트웨어 기술 및 원자로보호계통 설계 고도화 기술은 원전 계측제어 기술 국산화의 중심 기술에 해당한다. 특히, 원전용 안전등급제어기기의 국산화 개발 자체가 최초로 시도되고 있는 상황에서 제어기기의 핵심 소프트웨어인 실시간 운영체제 개발을 순수 국내 소프트웨어 기술로 수행하면서 원전 규격에 맞는 인허가를 획득한다는 것은 실시간 운영체제 기술 분야에도 큰 파급효과를 가져올 것으로 기대된다.

○ 경제·산업적 측면

원전 계측제어 국산화 개발사업의 성공은 크게 두 가지 경제 및 산업적 의미를 갖는다.

하나는, 국내 원전 계측제어 관련 산업의 기반 확대와 성숙화이다. 원전 계측제어 관련 핵심 기술의 국산화 개발을 통하여 산업체를 중심으로 한 저변이 확대될 것이며, 상대적으로 낙후된 안전성 관련 기술, 소프트웨어 관련 기술 등이 한층 성숙할 수 있을 것으로 기대된다. 또 다른 하나는 해외사의 국내 원전 계측제어 시장에서의 독점적 위치 확보를 견제하여 국부의 지나친 유출을 방지할 수 있다는 것이다. 이러한 측면들은 본 과제에서 개발하고자하는 기술들에도 동일하게 적용된다고 할 수 있다. 참고로, 원전 계측제어 사업단의 연구개발 결과물을 적용하고자 하는 대상 플랜트는 신규 건설 원전과 가동원전으로 구분할 수 있으며, 신규 건설 시장과 가동 원전 업그레이드 시장에서 모두 동일한 효과를 얻을 수 있을 것으로 기대된다.

원전 계측제어계통 소프트웨어 기반 설비에 대한 확인 및 검증 기술을 확립하는 것은 관련된 산업 분야에도 많은 영향을 미칠 것으로 기대할 수 있다. 확인 및 검증 기술은 소프트웨어 개발 과정과 직접적인 연관성을 가지고 있다. 따라서 원전 계측제어계통 소프트웨어 기반 설비에 대한 확인 및 검증 기술을 확립해 나가는 과정에서 기존 소프트웨어 산업과의 기술적 교류가 이루어질 수 있다. 안전성이 중요한 계통을 위한 소프트웨어 개발 산업의 필요성에 대한 인식이 산업계에 확산될 수 있으며 확인 및 검증에 관한 컨설팅, 벤처기업 창업 등을 통한 경제 및 산업적 측면의 효과도 기대할 수 있을 것이다.

○ 사회·문화적 측면

원자력발전은 타 발전과는 다르게 대기오염 물질을 배출하지 않아 요즈음 많은 사람들의 관심의 대상이 되고 있는 환경문제 해결에 큰 도움을 줄 것으로 기대되고 있다. 이러한 원자력발전소가 사회적으로 더 큰 기대를 모으기 위해서는 원자력발전소가 매우 안전한 시스템임을 입증하는 것이 중요하다. 따라서 국내의 기술을 활용하여 계통의 안전성을 투명하게 입증할 수 있도록 하는 것은 중요한 의미를 갖는다.

Ⅲ. 연구개발의 내용 및 범위

○ 안전등급제어기기 RTOS 소프트웨어 개념문서 개발

○ 안전등급제어기기 RTOS 소프트웨어 계획문서 개발

○ 안전등급제어기기 RTOS 소프트웨어 요구사항 명세서 개발

○ 안전등급제어기기 RTOS 소프트웨어 설계 명세서 개발

○ 안전등급제어기기 RTOS 소프트웨어 컴포넌트 시험계획서 및 절차서 개발

○ 안전등급제어기기 RTOS 소프트웨어 통합 시험계획서 및 절차서 개발

○ 안전등급제어기기 RTOS 소프트웨어 시스템 시험계획서 및 절차서 개발

○ 안전등급제어기기 특정주제기술보고서 작성

○ 안전등급제어기기 프로세서 모듈 PLD 요구사항 명세서 개발

○ 안전등급제어기기 프로세서 모듈 PLD 설계 명세서 개발

○ 안전등급제어기기 프로세서 모듈 PLD 컴포넌트시험, 통합 시험 수행

○ RPS 기능 예비구현 및 기능/성능시험

○ RPS 자동시험 및 수동개시자동시험 논리 분석 및 평가

○ RPS 주기시험절차 개발

○ RPS 기능/성능시험 개발 지원 업무 수행

○ RPS Technical Manual 주기시험 검토

원전 계측제어계통의 소프트웨어는 원자력발전소의 안전에 중요한 역할을 담당하기 때문에 소프트웨어 공학 생명주기 단계에 근거하여 철저한 확인 및 검증 작업이 수행되어져야 한다. 본 연구에서는 원전 계측제어계통의 고신뢰도화 및 RPS 구조 검증을 위해 안전등급제어기기(PLC)의 OS로 사용되는 RTOS의 고신뢰도화를 위해 원전 소프트웨어 개발 단계별로 각종 문서 및 테스트를 수행하였다. 또한 원자로보호계통 구조 검증을 위해 필요한 시험 및 시험주기, 시험 방법에 대한 연구를 수행하였다.

Ⅳ. 연구개발결과

○ 안전등급제어기기(PLC) RTOS S/W 원전규격화 개발

- 안전등급제어기기 RTOS 소프트웨어 개념문서 개발

- 안전등급제어기기 RTOS 소프트웨어 요구사항 명세서 개발

- 안전등급제어기기 RTOS 소프트웨어 설계 명세서 개발

- 안전등급제어기기 RTOS 소프트웨어 컴포넌트 시험계획서 및 절차서 개발

- 안전등급제어기기 RTOS 소프트웨어 통합 시험계획서 및 절차서 개발

- 안전등급제어기기 RTOS 소프트웨어 시스템 시험계획서 및 절차서 개발

○ 안전등급제어기기 프로세서 모듈 PLD 고신뢰도화 개발 및 PLC 특정주제기술보고서 작성 지원

- 안전등급제어기기 특정주제기술보고서 작성

- 안전등급제어기기 프로세서 모듈 PLD 요구사항 명세서 개발
- 안전등급제어기기 프로세서 모듈 PLD 설계 명세서 개발
- 안전등급제어기기 프로세서 모듈 PLD 컴포넌트 시험 계획서 및 절차서 개발
- 안전등급제어기기 프로세서 모듈 PLD 통합 시험 계획서 및 절차서 개발

○ RPS 구조/기능 분석 및 평가

- RPS 기능 예비구현 및 기능/성능시험
- RPS 자동시험 및 수동개시자동시험 논리 분석 및 평가
- RPS 주기시험절차 개발
- RPS 기능/성능시험 개발 지원 업무 수행
- RPS Technical Manual 주기시험 검토

V. 연구개발결과의 활용계획

○ 경제·산업적 측면

무엇보다도 원전 계측제어사업단이 발족되어 원전 계측제어 기술 국산화의 초석을 다지게 되었다는 점이 경제 및 산업적 측면에서의 가장 큰 의의이다. 한편, 본 과제에서 개발한 안전등급제어기기 실시간 운영체제 소프트웨어 기술 및 원자로보호계통 설계 고도화 기술은 원전 계측제어 기술 국산화의 중심 기술에 해당한다. 특히, 원전용 안전등급제어기기의 국산화 개발 자체가 최초로 시도되고 있는 상황에서 제어기기의 핵심 소프트웨어인 실시간 운영체제 개발을 순수 국내 소프트웨어 기술로 수행하면서 원전 규격에 맞는 인허가를 획득한다는 것은 타 시스템 실시간 운영체제 기술 분야에도 큰 파급효과를 가져올 것으로 기대된다. 발전소보호계통 및 플랫폼 국산화 개발은 직접적으로 보호계통 설계, 시험 등에 소요되는 자원을 줄일 수 있어서 발전단가 절감으로 이어질 수 있다. 또한 현재 전 세계적으로 확인 및 검증 도구의 확립이 제대로 이루어져 있지 않은 상태이고, 검증 체계마저 미흡한 상태에 있는 상황에서 국내 기술력을 통한 확인 및 검증 체계의 확립은 그 자체로도 경제적, 산업적으로 큰 파급 효과를 거둘 수 있을 것이다. 또한, 원자력발전소 필수안전계통의 소프트웨어를 개발함에 있어서 국내 기술만을 이용할 수 있게 되면, 원전 이용률의 향상을 기대할 수 있고, 또한 외국의 소프트웨어에 전적으로 의존하고 있는 안전 소프트웨어 개발을 순수 국내의 기술력을 이용하여 국산화함으로써 수입대체효과를 거둘 수 있다. 이러한 측면에서 본 연구결과는 커다란 경제적 가치가 있다고 사료된다. 아울러 본 연구를 통해 안전이 중요한 계통을 위한 소프트웨어 개발 산업의 필요성에 대한 인식이 산업계에 확산될 수도 있으며 벤처

기업 창업 등을 통한 경제 및 산업적 측면의 효과도 기대할 수 있을 것이다.

○ 활용방안

본 연구를 통해 개발된 RTOS, PLD, 이중화 모듈 고신뢰도화 기술은 원전 계측제어 계통 및 플랫폼 국산화 연구의 유용한 입력으로 활용될 수 있다. 또한, 확인 및 검증이 인허가 확보에 매우 중요하다는 관점에서, 본 연구를 통해 개발된 기술은 안전이 중요한 원자력발전소 계측제어계통에 소프트웨어 기반 설비를 적용하고자 할 때, 소프트웨어 개발 공정의 추적 가능성, 완전성 및 일관성 분석과 여러 가지 종류의 시험 등의 확인 및 검증 작업을 효과적으로 수행할 수 있도록 지원함으로써 설비의 안전성 및 신뢰성 향상에 많은 도움을 줄 수 있을 것으로 기대된다. 한편, 이는 가동원전 뿐만 아니라 차후 건설될 원전 계측제어계통에 적용될 소프트웨어 기반 설비에 대한 확인 및 검증 기술을 확립하고 인허가성을 제고하는데 활용할 수 있다.

KAERI

S U M M A R Y

Ⅰ. Project Title

High-Reliable PLC RTOS Development and RPS Structure Analysis

Ⅱ. Objective and Importance of the Project

○ Technical Aspect

One of the KNICS objectives is to develop a platform for Nuclear Power Plant(NPP) I&C(Instrumentation and Control) system, especially plant protection system. The developed platform is POSAFE-Q and this work supports the development of POSAFE-Q with the development of high-reliable real-time operating system(RTOS) and programmable logic device(PLD) software. Another KNICS objective is to develop safety I&C systems, such as Reactor Protection System(RPS) and Engineered Safety Feature-Component Control System(ESF-CCS). This work plays an important role in the structure analysis for RPS.

Validation and verification(V&V) of the safety critical software is an essential work to make digital plant protection system highly reliable and safe. Generally, the reliability and safety of software based system can be improved by strict quality assurance framework including the software development itself. In other words, through V&V, the reliability and safety of a system can be improved and the development activities like software requirement specification, software design specification, component tests, integration tests, and system tests shall be appropriately documented for V&V. This work was performed on this purpose.

○ Economic & Industrial Aspect

The outputs of this work can affect many other related industry. This work is relevant to the software development process, so the technical exchanges with general software development industry can be also expected. As safety critical software industry grows including the software validation and verification consulting and engineering services, the results of this work will be applied more frequently.

○ Social & Cultural Aspect

Nuclear power plants do not discharge noxious fumes, so many people expect it can help the environment problem. Demonstration of the safety of nuclear power plants can softer the social

concerns. The proof of the I&C system with our techniques can demonstrate the safety of NPP more clearly.

Ⅲ. Scope and Contents of Project

- ○ Development of concept phase documents for POSAFE-Q software
- ○ Development of planning phase documents for POSAFE-Q software
- ○ Development of software requirement specification for POSAFE-Q processor module software(RTOS and PLD)
- ○ Development of software design specification for POSAFE-Q processor module software
- ○ Development of component test plan/procedure/report for POSAFE-Q processor module software
- ○ Development of integration test plan/procedure/report for POSAFE-Q processor module software
- ○ Support for the development of topical report for POSAFE-Q
- ○ Pre-development of RPS software and its functional and performance tests
- ○ Evaluation of RPS automatic test functions
- ○ Support for RPS functional and performance tests

Ⅳ. Result of Project

- ○ Concept phase documents, planning phase documents, requirement specifications, design specifications, test documents for POSAFE-Q processor module software
- ○ Evaluation reports and test documents for RPS

Ⅴ. Proposal for Applications

The outputs of this work can be applied to many other related industry. Validation and verification related software development techniques developed in this work can be directly applied

to the development and V&V process in other NPP I&C software systems. These techniques can also help us establish safety critical software development techniques which are adequate to Korean nuclear power plants.

CONTENTS

KAERI

목 차

표 목 차

KAERI

그 림 목 차

제 1 장 연구개발과제의 개요

제 1 절 연구개발의 목적

1. 안전등급제어기기 (PLC) 프로세서 모듈 S/W 고신뢰도화 개발

   - 안전등급제어기기 (PLC) 프로세서 모듈 RTOS 고신뢰도화 개발
   - 안전등급제어기기 (PLC) 프로세서 모듈 PLD 고신뢰도화 개발
   - 안전등급제어기기(PLC) 이중화 모듈(HED) 고신뢰도화 개발
   - PLC 특정주제기술보고서(TR) 작성 지원

2. RPS 개발 지원

   - RPS 구조 검증
   - RPS 개발 및 시험지원

제 2 절 연구개발의 범위 및 내용

1. 범위

안전등급제어기기(PLC) RTOS 고신뢰도화 및 RPS 구조 검증 과제에서는 안전계통 중 특히 안전등급 PLC 및 RPS 개발자에게 안전-필수 소프트웨어 개발 시 필요한 소프트웨어 요구사항 명세서 및 소프트웨어 설계 명세서 작성을 직접 지원하며, RTOS 고신뢰도화 및 RPS 구조 검증에 필요한 핵심 기술을 지원한다.

안전등급 PLC 프로세서모듈 운영체제는 안전등급 PLC 시스템의 중심에서 외부장치들을 제어하고 통제하는 역할을 수행한다. 프로세서모듈 운영체제는 외부장치들과 서로 명령신호와 데이터를 주고받음으로써 안전등급 PLC 시스템이 정상적으로 동작할 수 있도록 한다.

RTOS 고신뢰도화는 다양한 소프트웨어 공학적 방법론의 도입과 프로토타입을 통한 신뢰성 있는 설계를 그 골자로 하고 있으며, RPS 구조 검증 또한 프로토타입 개발을 통한 검증이 그 핵심이다.

IEEE의 표준 특히 IEEE STD 830-1998 "IEEE Recommended Practice for Software Requirement Specification"과 IEEE 1016-1998 "IEEE Recommended Practice for Software Design Description"을 통해 각각 소프트웨어 요구 사항 및 설계 사항의 요구 조건을 분석하여 이를 근거로 요구 사항 및 설계 사항의 작성 절차를 수립하였으며, 이러한 절차에 따라 요구사항 및 설계 명세서를 작성한다.

더불어 RPS 개발 지원 분야에서는 KNICS 과제에서 수행하고 디지털안전계통 개발에서 개발해 오고 있는 원자로보호계통 중 자동시험 및 연계프로세서(ATIP : Auto Test and Integrate Test Processor), BP(Bistable Processor), CP(Coincidence Processor)의 구조 및 성능이 제대로 수행되는지 시험하기 위해 각종 시험을 수행하고 추가적으로 보완될 사항에 대해서는 예비구현 및 선행 시험을 통해 원자로보호계통이 원활하게 수행될 수 있도록 하는 것이다. 또한 특정주제기술보고서(TR) 작성에 필요한 사항 및 기술적 지원을 수행하는 것이 당사가 수행한 위탁연구 업무이다. 원자로보호계통 예비구현 및 기능/성능시험에서는 전 단계에서 구현된 원자로보호계통의 알고리즘 및 구조가 성능을 원활히 수행 가능한지에 대한 기능/성능 시험을 수행하는 업무를 수행하였다. 원자로보호계통 중 자동시험 및 연계프로세서는 BP, CP의 건전성을 위해 시험 수행 및 그 결과를 판단하여 COM, QIAS로 전송하는 역할을 수행하였다.

원자로보호계통 자동시험 및 수동개시 자동시험 논리분석 연구에서는 자동시험이 가지고 있는 시험 기능이 적절하게 수행되며 자동시험 수행 시 원자로 트립 유발, 원자로보호계통 문제가 발생하는 경우, 적절한 시점에 자동시험이 중지되는지 여부를 확인하는 업무가 필수적이다. 또한 수동개시 자동시험 시 중요하게 대두되는 채널우회, 전채널 우회 수행으로 유발될 수 있는 문제점에 대해서 파악하고 그 논리가 적절한지 시험하고 문제 발생 시 보완 사항을 제시하는 업무를 수행한다.

마지막으로 원자로보호계통 시험절차서 작성 업무는 주로 자동시험 및 연계프로세서 시험에 대한 시험절차서 및 시험보고서 등을 수행하였다. 자동시험 및 연계프로세서는 주로 건전성 감시 및 진단, 수동시험, 자동시험, 수동개시 자동시험에 대한 기능을 포함하고 있으며 각 시험이 수행되기 위한 논리 등이 적절한지 평가하기 위해서 시험절차서 및 시험보고서 작성이 필요하다. 이를 수행하기 위해서 비교논리프로세서(BP), 동시논리프로세서(CP)와의 연관관계 등을 잘 숙지하여 시험절차서 및 시험을 통한 시험보고서 작성 업무를 수행한다.

2. 안전등급제어기기(PLC) 프로세서 모듈 S/W 고신뢰도화 개발

- 안전등급제어기기(PLC) 프로세서 모듈 RTOS 고신뢰도화 개발

  · 안전등급 PLC 프로세서 모듈 RTOS 요구사항 명세서 개발

  · 안전등급 PLC 프로세서 모듈 RTOS 설계 명세서 개발

  · 안전등급 PLC 프로세서 모듈 RTOS 시험계획서/절차서/보고서 개발

  · 안전등급제어기기 특정주제기술보고서 작성 지원

- 안전등급제어기기(PLC) 프로세서 모듈 PLD 고신뢰도화 개발

· 안전등급 PLC 프로세서 모듈 PLD 요구사항 명세서 개발

· 안전등급 PLC 프로세서 모듈 PLD 설계 명세서 개발

· 안전등급 PLC 프로세서 모듈 PLD 시험계획서/절차서/보고서 개발

· 안전등급제어기기 특정주제기술보고서 작성 지원

- 안전등급제어기기(PLC) 이중화 모듈(HED) 고신뢰도화 개발

· 안전등급 PLC 이중화 모듈(HED) 소프트웨어 요구사항 명세서 개발

· 안전등급 PLC 이중화 모듈(HED) 소프트웨어 설계 명세서 개발

· 안전등급 PLC 특정주제기술보고서 개정 지원

3. RPS 구조 검증

- RPS 구조 검증

· RPS 계통설계문서 및 소프트웨어 기능요건 작성 및 개정 지원

· RPS 계통설계문서 및 소프트웨어 연계요건서 작성 및 개정 지원

- RPS 개발 지원

· RPS 소프트웨어 정형 명세서 개정 지원

· RPS 계통설계문서 및 소프트웨어 요구사항 정형명세서 개정 지원

· RPS 기능/성능시험 계획서/통합시험 문서 개정 지원

KAERI

4. 목표달성도

단 계	목 표	달성도	비고
2단계 1차년도	· 안전등급제어기기 (PLC) 프로세서 모듈 RTOS 고신뢰도화 개발 (SRS/SDS)	S	
	· RPS 구조 검증 및 계통설계 문서 작성 지원	S	
2단계 2차년도	· 안전등급제어기기 (PLC) 프로세서 모듈 RTOS 고신뢰도화 개발 (시험)	S	
	· RPS 계통설계 관련 문서 개정 지원	S	
2단계 3차년도	· 안전등급제어기기 (PLC) 프로세서 모듈 PLD 고신뢰도화 개발 및 PLC 특정주제기술보고서(TR) 작성 지원	S	
	· RPS 시험 관련 문서 작성 및 개정 지원, 정형명세 개정 지원	S	
2단계 4차년도	· 안전등급제어기기 (PLC) 이중화 모듈(HED) 고신뢰도화 개발 및 PLC 특정주제기술보고서(TR) 개정 지원	S	
	· RPS 계통 및 소프트웨어 설계 문서 개정 지원	S	

KAERI

제 2 장 국내외 기술현황

제 1 절 국내기술 현황

우리나라는 원자력 분야에서 신고리 1&2 및 신월성 1&2의 주요 계약이 최근에 완료되었으며 신고리 3&4의 계약이 진행되고 있는 등, 세계적으로 가장 활발하게 원전 건설이 진행되고 있는 나라 중의 하나이다. 원전 건설 기술의 국산화 성과도 주목할 만하여 현재 95% 이상의 원전 건설 기술이 국산화되어 있다. 그러나 원전 계측제어 분야의 국산화 성과는 상대적으로 미흡한 실정이다.

제 2 절 해외기술 현황

해외의 안전등급제어기기 개발은 독일 Siemens의 Teleperm XS, 미국 Westinghouse 사의 AC160 등이 있는데, 대부분 상용제품인증절차를 통하여 원전에 적용되고 있으며 실시간 운영체제를 비롯하여 전체 시스템 소프트웨어를 원전 규격에 따라 자체 개발하여 인허가를 획득한 사례는 없다.

제 3 절 개발결과가 국내외에 미치는 영향

본 연구를 통하여 원전 계측제어 분야에 적합한 고신뢰도 소프트웨어 개발 기술이 확립될 것으로 전망된다. 안전등급제어기기 (PLC) 프로세서 모듈 PLD 고신뢰도화 개발을 통해 가동원전의 안전계통 제어기기에 전반적으로 확대될 수 있을 뿐 아니라 차후에 건설될 원자력발전소 안전계통 제어기기 까지도 확대될 수 있을 것이다. 따라서 해외에서 수입하던 주요 안전등급제어기기의 국산화에 대한 기술적 뒷받침을 할 수 있을 것으로 기대된다. 더불어 안전등급제어기기의 해외 수출과 이와 관련된 다양한 원전 기술을 해외로 판매할 수 있을 것으로 기대된다.

제 3 장 연구수행 내용 및 결과

제 1 절 연구수행 개요

본 연구는 한국원자력연구원의 안전계통개발팀 및 (주)포스콘과의 긴밀한 연계업무를 통해 안전등급제어기기 프로세서 모듈 RTOS 및 PLD 고신뢰도화 개발업무 및 원자로보호계통 분석 및 업무 지원을 통한 인허가획득 지원 업무를 수행하였다. 또한, 본 과제는 KNICS 안전등급 PLC 소프트웨어 개발계획서 및 KNICS 원자로보호계통 소프트웨어 개발계획서에 준하여 소프트웨어 공학적인 원칙들을 준수하여 수행하였다. 구체적인 적용 기법은 소프트웨어 공학 분야에서 검증된 기법을 위주로 선택하였으나, PLD 시험과 같이 새로운 기법을 적용할 필요가 있을 경우에는 본 연구를 통해 새로 고안된 기법을 적용하기도 하였다.

그림 3.1 1차년도 및 2차년도 연구수행 개요

1차 년도에는 PLC RTOS S/W 개발과 관련하여 S/W 개념문서, S/W 계획 문서, RTOS SRS, RTOS SDS를 작성하였다. 또한 원자로보호계통 구조/기능 분석 및 평가와 관련하여서는 원자로보호계통 기능의 예비구현 및 시험논리의 분석 및 평가를 수행하였다. 이를 기반으로 원자로보호계통의 주기시험 기능이 원활히 수행될 수 있도록 주기시험절차를 개발하였다.

2차 년도에는 PLC RTOS S/W 컴포넌트시험, 통합시험, 시스템시험에 필요한 계획서, 절차서, 보고서 등을 작성하였다. 또한 원자로보호계통 개발 지원과 관련하여서는 SRS 논리를 분석 및 평가하고 시험기능에 대한 보완사항을 반영하여 소프트웨어를 구현하였으며, Technical Manual 중 주기시험과 관련된 업무를 지원하였다.

3차 년도에는 PLC 특정기술주제보고서를 보완하는데 필요한 프로세서 모듈 관련한 모든 설계 문서 개정을 수행함과 동시에 PLC 프로세서 모듈의 PLD 고신뢰도화 개발을 위해 SRS 개발, SDS 개발, 컴포넌트 시험, 통합 시험을 수행하였다. 또한 RPS 통합 시험계획서/시험 보고서 작성 지원을 하여 RPS 계통설계 관련 문서 작성 및 개정을 지원하였다.

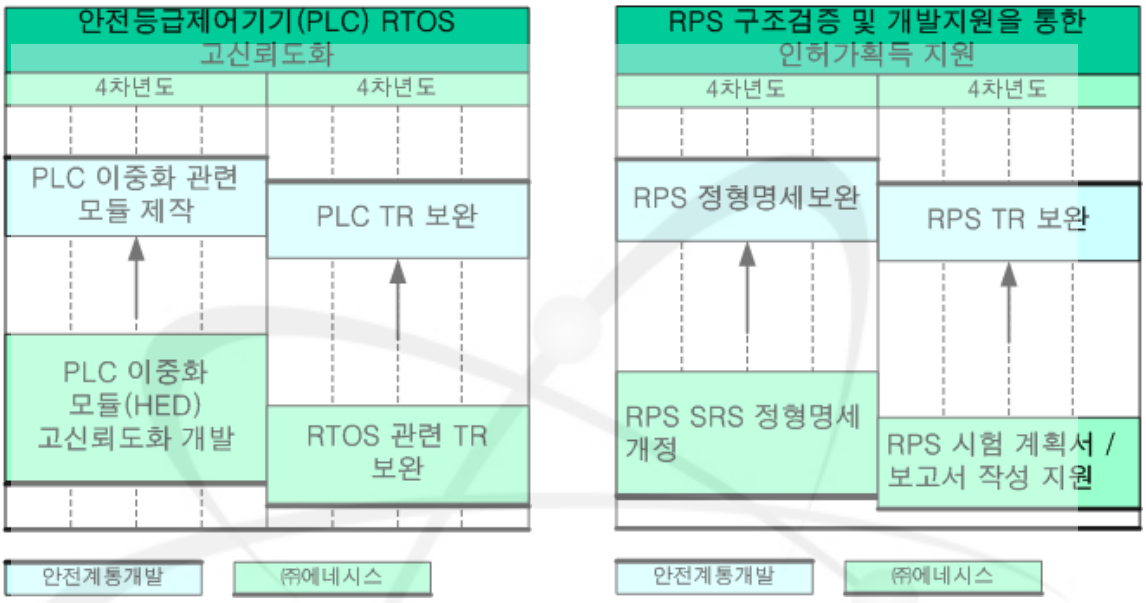


그림 3.2 4차년도 연구수행 개요

4차 년도에는 PLC 특정기술주제보고서를 보완하는데 필요한 프로세서 모듈 관련한 모든 설계 문서 개정을 수행함과 동시에 PLC 이중화 모듈 중 HED 모듈 고신뢰도화 개발을 위해 SRS 개발, SDS 개발을 수행하였다. 또한 RPS SRS 정형명세 개정지원을 하여 RPS 소프트웨어 설계 관련 문서 작성 및 개정을 지원하였다.

제 2 절 안전등급제어기기(PLC) 프로세서 모듈 S/W 고신뢰도화 개발

1. 안전등급제어기기(PLC) 프로세서 모듈 RTOS 고신뢰도화 개발

가. 개념문서 개발

(1) RTOS 개념문서

본 연구에서 개발한 RTOS 개념문서는 POSAFE-Q 설계요건서, POSAFE-Q 연계요건서 등이며, 이러한 개념문서의 내용을 간략히 요약하면 다음과 같다.

기능요건

POSAFE-Q에 탑재된 운영체제는 실시간 운영체제(Real Time Operating System: RTOS)로서 제어행위를 수행하는데 필요한 최소한의 필수 기능만을 포함한다.

POSAFE-Q의 프로세서 모듈의 운영체제는 다음과 같은 기능을 가져야 한다.

- 입력모듈로부터의 데이터 취득 기능
- 작동 모드(Run Mode) 동안 연속 루프내의 응용 프로그램 수행 기능
- 출력모듈로의 데이터 로딩 기능
- 태스크 스케줄링 기능
- 태스크 간 통신 기능
- 인터럽트 처리 기능
- 디바이스 드라이버 처리 기능
- 전원 투입(Power Up) 및 작동 시간(Run Time) 진단 기능 및 기타 온- 라인 진단 기능
- 데드-록(Dead-Lock) 및 라이브-록(Live-Lock) 방지 기능
- 통신모듈과의 연계가 프로세서모듈의 안전기능 수행을 방해하지 않음을 보장하는 결정론적 통신 기능
- 프로그래밍 모드상태에서 응용 프로그램 업-로딩(uploading)을 지원하는 기능
- 전원 투입 시 PLC 작동을 보증할 수 있는 초기화 동작(전원 투입 후 자가진단, PLC 설계에 따른 I/O 구성 및 I/O설정, 사용자 정의 값으로 메모리 설정 등) 수행 기능
- pSET과의 인터페이스 및 통신 기능
- 보안-인증 기능

POSAFE-Q의 RTOS는 8개까지의 응용 프로그램 태스크를 지원하며, 응용 프로그램 태스크의 크기는 512KDW이고, 사용자가 한 태스크 크기를 256KDW이내에서 유연하게 설정할 수 있다. RTOS 커널은 내장된 시스템 태스크와 PLC 엔지니어링 도구로부터 다운로드 된 응용 프로그램 태스크를 함께 스케줄링 할 수 있게 하는 기능을 제공한다. 또한, 메모리 보호, 우선순

위 전도 방지, 진단 기능 등 안전성-필수 소프트웨어 시스템에 적용되는데 필요한 사양을 갖는다.

입력 스캐닝(scanning) 및 응용 프로그램을 멀티태스킹(multi-tasking)으로 처리하는 POSAFE-Q의 경우, 운영체제 또는 엔지니어링 도구들은 각 사이클 동안에 입력 스캐닝과 응용 프로그램 실행이 결정론적으로 처리되며 또한 완전히 처리된다는 것을 보증할 수 있다. 결정론적 응용 프로그램 실행이 투명하게 입증되지 않는 한 비결정적 프로그램의 실행에 의한 인터럽트는 허용되지 않는다.

한편, 응용 프로그램에서 미의도/미사용된 기능들을 격리하거나 줄이기 위해서 다음의 요건들을 참고하여 설계한다.

- 비정상 조건 및 사건(ACEs: Abnormal Conditions and Events)의 해결 및 분석을 위해 "고장모드 및 영향분석(FMEA)"을 수행하여, 시스템이 고장-안전(Fail-Safe) 특성을 가지고 있음을 보여야 한다. IEEE Std 7-4.3.2 Appendix F에는 FMEA 수행이 "비안전 기능이 안전 기능에 대해 비정상 조건 및 사건을 발생시키지 않는다"는 것을 보장하는데 도움이 되는 방법임을 명시하고 있다.
- "소프트웨어 품질보증(SQA)"과 관련된 7장의 요건과 그 관련 요건을 명확히 정의하고 그에 따라 개발되어야 한다.
- "Heartbeat"의 생성 및 감지 요건을 만족해야 한다.

KAERI

성능요건

POSAFE-Q 운영체제는 실시간 성능 요건을 만족해야 하며, 실시간 성능 요건은 우선순위 전도, 인터럽트 지연시간, 인터럽트 응답시간, 인터럽트 복귀시간, 스케줄링 자체 소요 시간 등의 관점에서 평가되어야 한다. POSAFE-Q 응답시간의 분해능은 최소 10ms가 될 수 있어야 하며, 안전계통에서 요구하는 50ms 응답시간(PLC 데이터 입력에서 출력까지 응답시간)을 만족해야 한다.

연계요건

POSAFE-Q 운영체제는 소프트웨어 도구, 각종 디바이스 드라이버, 입출력 장치, 기타 하드웨

어와 연계를 가진다. 이러한 연계는 안전등급 PLC 상호 간 및 타 컴퓨터 장치와의 통신을 위한 연계도 포함한다.

User 인터페이스

원자로 보호계통 및 공학적 안전설비 기기제어계통과 같은 POSAFE-Q 응용 시스템 개발자는 POSAFE-Q가 제공하는 소프트웨어 도구를 통하여 응용 프로그램을 RTOS 상에 동작시킨다. 원자력 발전소 운전 및 유지보수 관련자는 POSAFE-Q 가 제공하는 하드웨어 인터페이스 장치(리셋 스위치, 운전모드선택 스위치 등)를 통하여 OS 재가동 및 응용 프로그램을 정지할 수 있어야 한다. 또한, LED와 같은 지시 기능을 통한 사용자 인터페이스를 제공한다.

하드웨어 인터페이스

OS는 연산장치 내의 메모리와 같은 하드웨어 부품, 아날로그 입/출력모듈, 디지털 입/출력모듈, 통신모듈 및 LED와 같은 기타 하드웨어와 인터페이스를 한다. 이러한 인터페이스는 대부분 메모리 읽기/쓰기 방식으로 이루어진다.

소프트웨어 인터페이스

RTOS는 커널과 시스템 태스크로 구성되어 상호 인터페이스를 한다. 한편, RTOS는 디바이스 드라이버 소프트웨어 및 통신 소프트웨어와 소프트웨어적으로 인터페이스를 한다.

통신 인터페이스

RTOS는 엔지니어링 도구(pSET)와 RS-232C 직렬통신을 통하여 인터페이스를 한다. 또한 원자로 보호계통 및 공학적 안전설비 기기제어 계통의 통신을 위하여 통신장치 소프트웨어와의 인터페이스를 제공한다. RTOS는 통신과의 인터페이스가 안전등급 PLC 고유의 안전 기능 수행을 방해하지 않도록 해야 한다.

(2) RTOS 소프트웨어 계획문서

본 연구에서 개발한 RTOS 소프트웨어 계획문서는 POSAFE-Q 소프트웨어 개발계획서로서, 개발계획서의 내용을 간략히 요약하면 다음과 같다.

소프트웨어 생명 주기 모델

소프트웨어 생명 주기 모델(SLCM: Software Life Cycle Model)은 개념 정립에서부터 구현까지 하향식 접근 방법을 채택한 폭포수(Waterfall) 모델, 폭포수 모델의 단점을 보완하기 위해 점진적으로 시스템을 개발해 나가는 접근 방법을 채택한 원형(Prototyping) 모델과 폭포수 모델과 원형 모델의 장점에 새로운 요소인 위험 분석을 추가하여 시스템을 개발하면서 생기는 위험을 관리하고 최소화하는 접근 방법을 채택한 나선형(Spiral) 모델 등이 주로 사용된다.

POSAFE-Q 소프트웨어 2단계 개발 과제는 4년 동안 수행된 과제이다. 이미 1단계에서는 위에서 언급한 세 종류의 생명 주기 모델의 장점을 종합하여 정의한 혼합형 모델을 적용하여 POSAFE-Q 시제품을 개발하였고 2단계에서도 혼합형 모델에 따라 생명주기 절차를 따라 POSAFE-Q 완제품을 개발한다. 제 2 단계(2004.7 ~ 2008.6)에서는 제 1 단계 업무를 보완하여 POSAFE-Q 개발, 제작 및 인허가 업무를 수행한다.

POSAFE-Q의 소프트웨어 생명 주기 모델은 13개의 주요 업무 단계와 32개의 세부 업무 단계로 이루어지며, 주요 업무 단계 중 I 단계부터 VI 단계까지는 1 단계 기간 동안 수행되었고, VII 단계부터XIII 단계까지는 2 단계 기간 동안 수행된다. 1단계와 2단계 모두 혼합형 모델의 생명주기를 따른다. 폭포수 모델의 개념 단계, 요구사항 단계, 설계 단계, 구현 단계, 통합 단계, 검증 단계, 운영 및 유지보수 단계를 진행하고 나선형 모델을 적용하는 단계를 진행한다. 그리고 본 과제의 최종 목표인 인허가 획득을 위하여, 완제품 인허가 획득 단계가 추가된다.

개발계획서에는 위에서 기술한 소프트웨어 생명 주기 모델 외에도 세부적인 소프트웨어 개발 전략, 프로젝트 수행 상의 위험 분석, 품질 측정, 각 단계별 소프트웨어 개발 절차, 일정, 개발 도구, 관련 표준 및 개발할 문서 목록 등이 기술되어 있다.

(3) RTOS 소프트웨어 요구사항 명세서

본 연구에서 개발한 RTOS 소프트웨어 요구사항 명세서는 POSAFE-Q 프로세서 모듈 RTOS에 요구되는 소프트웨어 기능, 성능, 연계 등의 요건과 기타 안전성 및 품질 관련 요건 등이 기술되어 있으며, 요구사항 명세서의 내용을 간략히 요약하면 다음과 같다.

그림 3.3은 안전등급 PLC RTOS의 범위와 구성 요소를 보여준다. RTOS는 커널인 pCOS와

시작(Startup) 소프트웨어, 그리고 Shell 태스크, Diagnosis 태스크, pSET 태스크(LoaderRxrdy 태스크, Loader_service 태스크로 구성됨), Communication 태스크 등의 시스템 태스크와 응용 프로그램을 실행시켜주는 User_task 태스크로 구성된다. RTOS는 LoaderRxrdy 태스크와 Loader_service 태스크를 통하여 pSET으로부터 입력을 받거나 pSET으로 출력을 제공한다. 또한, RTOS는 커널과 시스템 태스크 및 Application 태스크의 동작 상태에 따라 하드웨어와 입출력을 주고받는다.

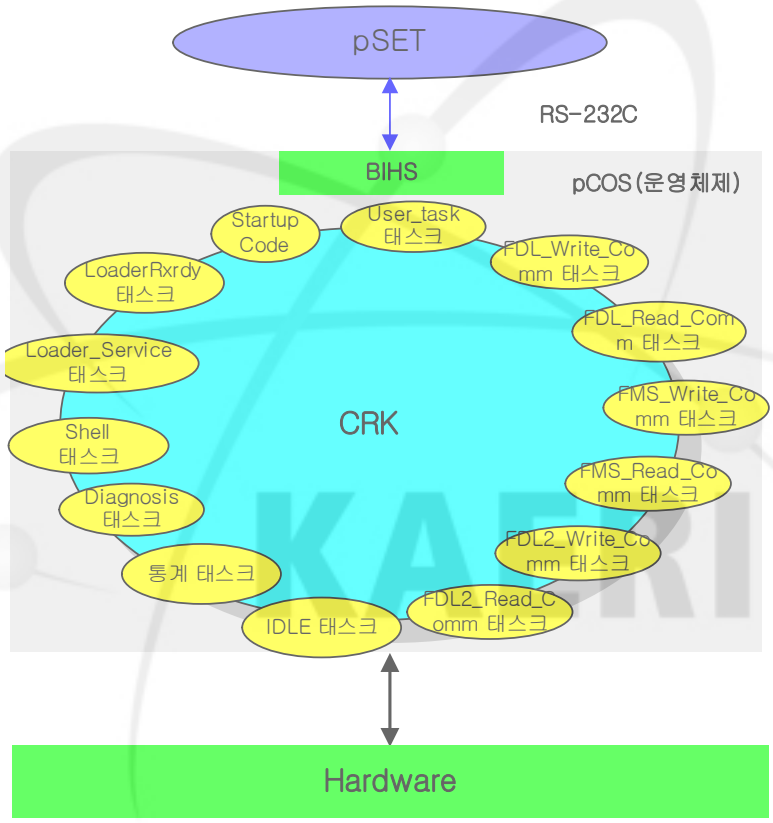


그림 3.3 RTOS 구성요소

프로세서 모듈의 계층적 구조

안전등급 PLC 프로세서 모듈의 계층적 구조는 그림 3.4와 같다. 하드웨어는 SMQ320C32-60를 기반으로 하여 구성되고, BIHS와 RTOS Kernel을 합한 소프트웨어 패키지를 pCOS라고 정의하며, pCOS와 시스템 태스크를 합하여 RTOS(Real Time Operating System)라 정의한

다. 실행프로그램은 pSET에서 생성한 제어프로그램이다.

KAERI

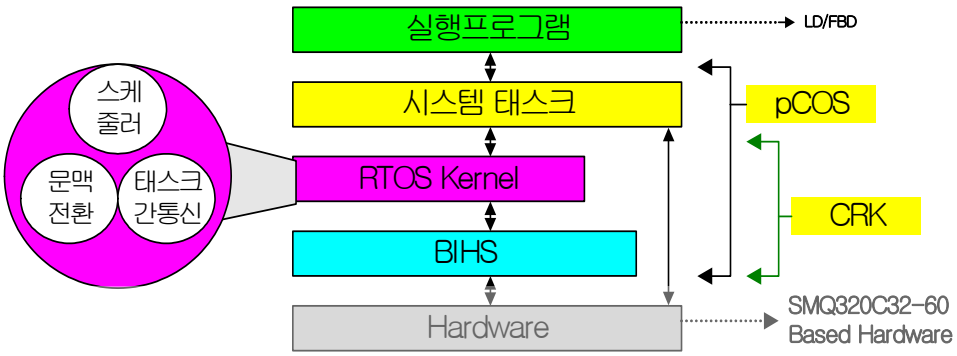


그림 3.4 RTOS 계층적 구조

하드웨어

SMQ320C32-60 기반의 하드웨어로서, Backplane Unit을 통하여 다른 유닛들과 연결된다. 운영체제의 효율적인 동작을 위해 필요한 ROM, RAM 등을 제공할 뿐만 아니라 타 유니트와의 인터페이스를 위한 로직이 있다. 메모리 구성은 표 3.1과 같다.

표 3.1 CPU 메모리 구성

시작 어드레스	Length	항 목	속성	마이크로프로세서영역	기타
200000H	64K per module	Piggy Back	R/W	STRB0	16비트 Max. 4
400000H	1	SCC_CONTROL	W	STRB0	16비트
410000H	1	RTC_CONTROL	W	STRB0	16비트
420000H	1	INT_STATUS0	R	STRB0	16비트
420001H	1	INT_STATUS1	R	STRB0	16비트
420002H	1	AC_FAIL_COUNT0	R	STRB0	16비트
420003H	1	AC_FAIL_COUNT1	R	STRB0	16비트
420004H	1	전원모듈_STATUS0	R	STRB0	16비트
428000H	1	하드웨어 형상	R	STRB0	16비트
430000H	1	INPORT0	R	STRB0	16비트
440000H	1	INPORT1	R	STRB0	16비트
450000H	1	OUTPORT0	W	STRB0	16비트
460000H	1	EN_OUTPORT0	W	STRB0	16비트
480000H	1	Software Reset	W	STRB0	16비트

490000H	1	RTC_ALE	W	STRB0	16비트
498000H	1	RTC_DATA	R/W	STRB0	16비트
498001H	1	Watchdog Timer Data	W	STRB0	16비트
500000H	2K per module	입출력 모듈 영역	R/W	STRB0	16비트 Max. 128
600000H	32K per module	통신 모듈 영역	R/W	STRB0	16비트 Max. 16
900000H	512K	Boot Loader	R	STRB1(BOOT3)	16비트
A00000H	256K	운영체제	R/W	STRB1	32비트
B00000H	32K	특정변수 Back-Up 영역	R/W	STRB1	16비트
C00000H	2M	실행영역	R/W	STRB1	32비트
E00000H	2M	Back-Up 영역	R/W	STRB1	32비트

RTOS

RTOS 는 BIHS, 커널, 시스템 태스크 등으로 구성된다. RTOS의 구조는 아래에 개략적으로 기술되어있다.

실행프로그램

pSET는 그래픽 에디터에서 LD, FBD, ST 등을 이용하여 작성한 프로젝트 파일을 TMS320C32에서 직접 실행할 수 있는 기계어 코드로 변환하여 CPU Unit에 다운로딩한다. 이 기계어 코드를 실행프로그램이라 한다. RTOS는 이 실행프로그램을 동작시켜주는 태스크(User_task 태스크)를 가지고 있다.

Boot Loader

안전등급 PLC는 RTOS와는 별도로 Boot Loader를 가지고 있다. Boot Loader는 안전등급 PLC의 부팅을 담당한다. Boot Loader에 대한 요구사항은 본 요구사항명세서의 범위에서 제외한다.

RTOS 의 계층적 구조

BIHS

BIHS(Basic Interrupt Handling System)는 CPU Unit 하드웨어와 RTOS 커널을 연결하는 기능을 가지고 있다. 그 구성 요소로는 주기적으로 클럭 틱을 생성하는 Timer Interrupt 0, 문맥전환에 사용되는 Trap2, pSET로부터의 데이터 송수신에 필요한 INT0 등이 있다.

RTOS Kernel

시스템의 시작 및 초기화하는 일을 하는 시작(Startup) 소프트웨어에 의하여 멀티태스킹이 시작된다. pCOS는 선점형 멀티태스킹을 구현할 수 있는 커널로서 태스크의 선점형 문맥전환을 지원할 뿐만 아니라 태스크의 동기 및 자원의 공유에 사용되는 세마포어, 태스크간의 정보의 교환을 위한 메일박스와 큐 등이 있다.

시스템 태스크

안전등급 PLC의 pCOS 상에서 동작하는 태스크이다. 시스템 태스크는 표시(Display) 기능을 하는 Shell 태스크, 자가진단을 하는 Diagnosis 태스크, pSET과의 통신관련 기능을 하는 LoaderRxrdy 태스크와 Loader_Service 태스크, 통신장치와의 인터페이스를 담당하는 Communication 태스크가 있다.

User_task 태스크

사용자가 프로그래밍하는 최대 8개까지의 응용(Application) 프로그램을 실행시켜 주는 태스크이다.

시스템 인터페이스

RTOS는 pSET, BSP(AI, SDL, FMS), DI/DO, 기타 하드웨어와 인터페이스를 한다. SDL 및 FMS BSP는 통신 인터페이스를 담당한다.

User 인터페이스

원자로 보호계통 및 공학적 안전설비 기기제어 계통 개발자는 pSET을 통하여 Application 프로그램을 RTOS상에 동작시킨다. 원자력 발전소 운전 및 유지보수 관련자는 안전등급 PLC가 제공하는 하드웨어 인터페이스 장치를 통하여 RTOS를 정지 및 재가동 할 수 있다.

하드웨어 인터페이스

RTOS는 TMS320C32 연산장치, AD/DA 카드, DI/DO 카드, 통신장치 및 LED와 같은 기타 하드웨어와 인터페이스를 한다. 이러한 인터페이스는 메모리 읽기/쓰기 방식으로 이루어진다.

소프트웨어 인터페이스

RTOS의 커널인 pCOS는 시스템 태스크(Diagnosis, Shell, LoaderRxrdy, Loader_service, Communication)와 인터페이스를 하며, 응용 프로그램을 실행시켜주는 User_task 태스크와도 인터페이스를 한다. RTOS는 AD/DA BSP 소프트웨어, SDL 및 FMS BSP 소프트웨어와 인터페이스를 한다.

통신 인터페이스

RTOS는 pSET과 RS232C 직렬통신을 통하여 인터페이스를 한다. 또한 RTOS는 원자로 보호계통 및 공학적 안전설비 기기제어 계통의 통신을 위하여 SDL 및 FMS BSP와의 인터페이스를 제공한다.

메모리 제약사항

1M double word의 크기를 가지는 실행영역(B00000(H) ~ BFFFFF(H))에서 Application 태스크가 차지하는 영역은 512K double word이다. 한 개의 Application 태스크가 가질 수 있는 최대 크기는 256K double word이며, 512K double word를 넘지 않는 한 최대 8개까지의 Application 태스크를 실행시킬 수 있다.

(4) RTOS 소프트웨어 설계 명세서

본 연구에서 개발한 RTOS 소프트웨어 설계 명세서는 POSAFE-Q RTOS에 대한 모듈 분해 설계, 모듈 간의 의존성 설계, 인터페이스 설계, 상세 설계 등이 기술되어 있으며, 설계 명세서의 내용을 간략히 요약하면 다음과 같다.

안전등급 PLC 프로세서모듈 운영체제는 안전등급 PLC 시스템의 중심에서 외부장치들을 제어하고 통제하는 역할을 수행한다. 프로세서모듈 운영체제는 외부장치들과 서로 명령신호와 데이터를 주고받음으로써 안전등급 PLC 시스템이 정상적으로 동작할 수 있도록 한다. 운영체제 관

점의 안전등급 PLC 시스템의 전체적인 구조는 그림 3.5와 같이 표현할 수 있다.

그림 3.5 운영체제 관점의 안전등급 PLC 시스템의 전체적인 구조

안전등급 PLC 프로세서 모듈 운영체제를 기술하기 위하여 소프트웨어의 전체적인 구조를 논리적 또는 기능적으로 구분한다. 소프트웨어 구성에 관련된 정보들은 분해 설계기술(Decomposition Description)을 통해 나타내고, 컴포넌트들 간의 데이터나 신호의 교류는 의존성 설계기술(Dependency Description)로서 표현한다. 의존성 설계기술은 안전등급 PLC 프로세서 모듈 운영체제 내부의 태스크들 간의 연관 관계에 대해 기술한다. 외부장치(DRAM, SRAM, Flash Memory 등)와 안전등급 PLC 프로세서 모듈 운영체제와의 데이터 송수신에 대한 사항은 인터페이스 설계기술(Interface Description)에서 나타내고, 프로세서모듈 운영체제의 상세한 설계는 상세 설계기술(Detailed Description)에서 나타낸다. 상세 설계기술은 커널의 경우에는 Statecharts를 통하여, 시스템 태스크들의 경우에는 Flow Chart를 통하여 함수 단위의 세부 설계를 기술한다. 그림 3.6에서 그림 3.9는 각각 시작 소프트웨어에 대한 분해 설계기술, 의존성 설계기술, 인터페이스 설계기술, 상세 설계기술을 나타내고 있다.

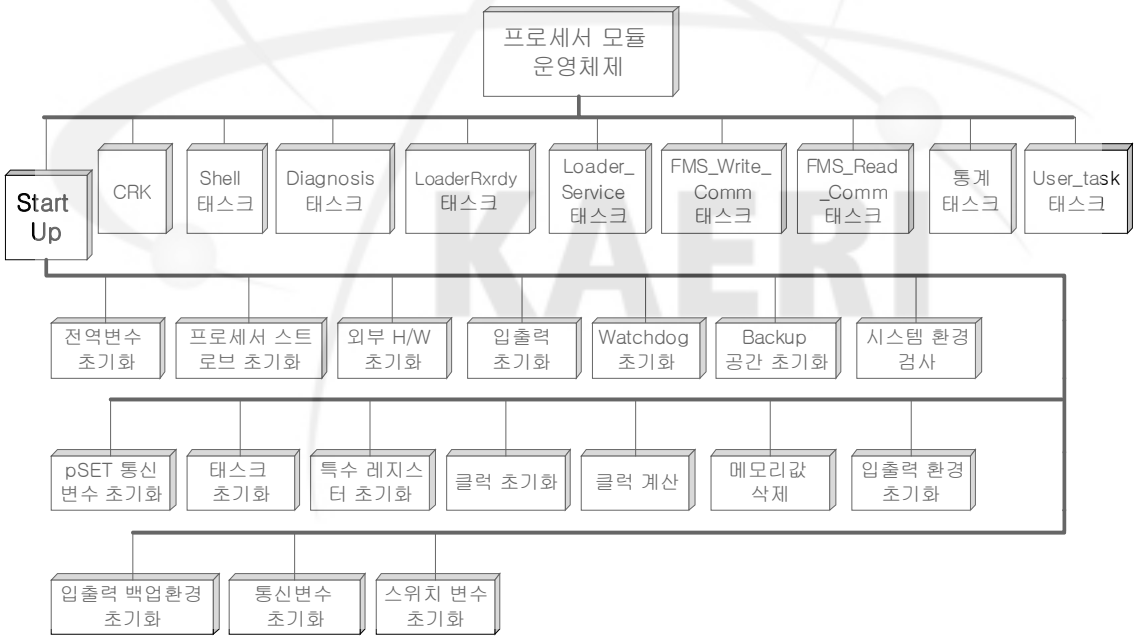


그림 3.6 시작 소프트웨어 분해 설계기술

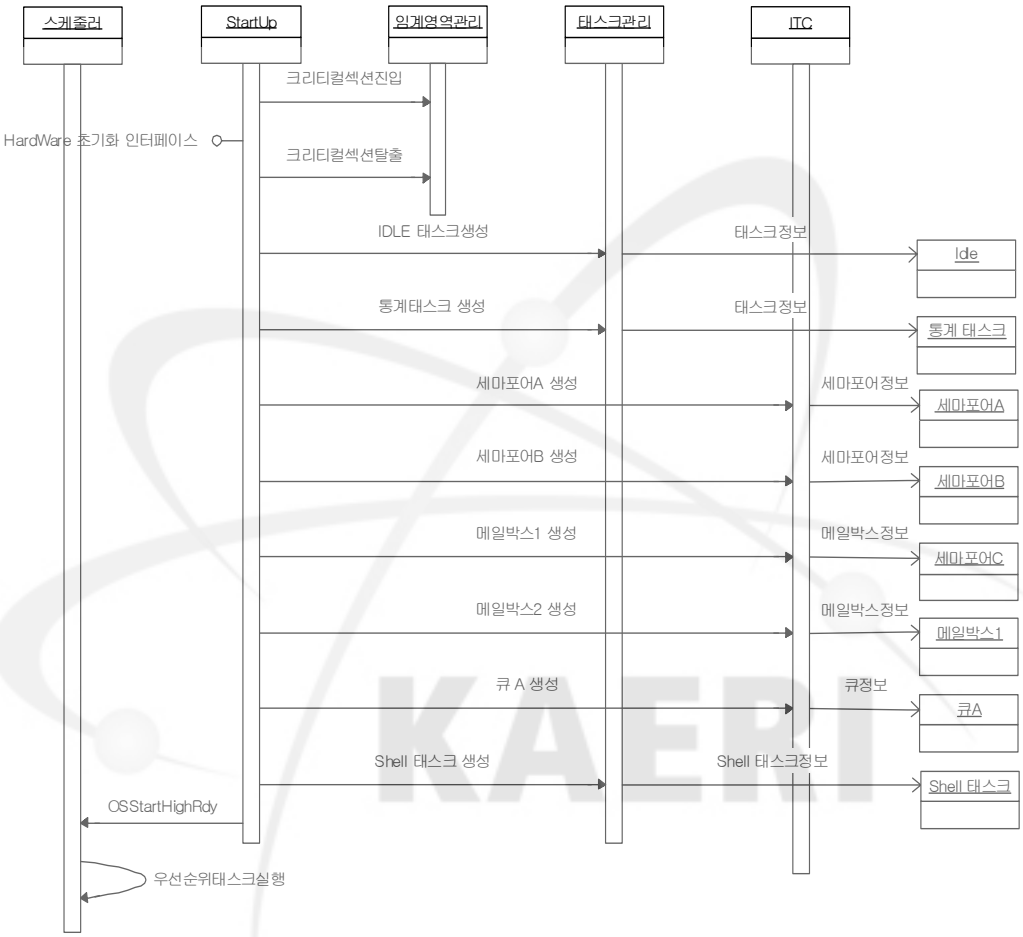
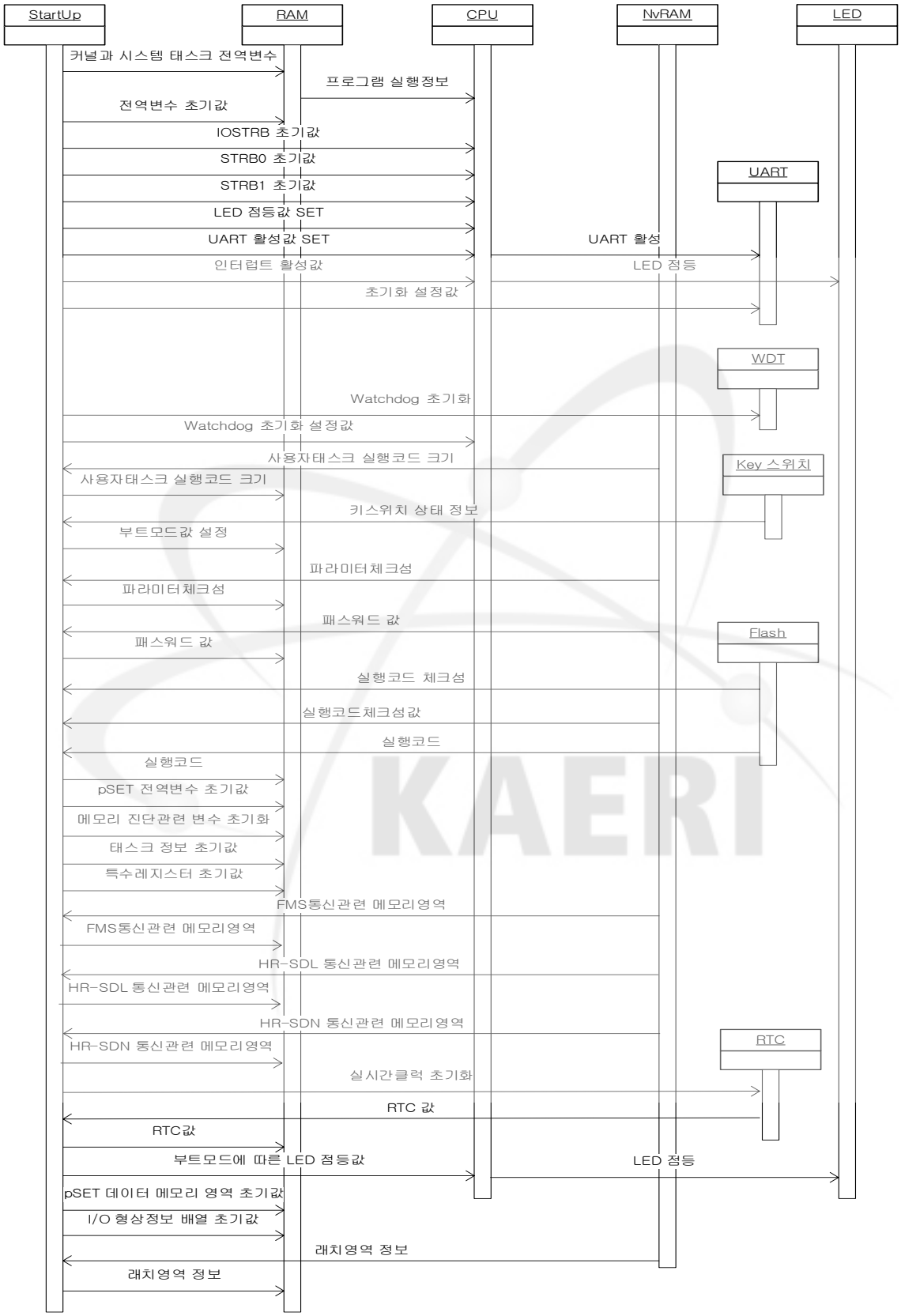


그림 3.7 시작 소프트웨어와 커널 간 의존성 설계기술


StartUp
RAM
CPU
NvRAM
LED
UART
WDT
Key 스위치
Flash
RTC
커널과 시스템 태스크 전역변수
프로그램 실행정보
전역변수 초기값
IOSTRB 초기값
STRB0 초기값
STRB1 초기값
LED 점등값 SET
UART 활성값 SET
UART 활성
인터럽트 활성값
LED 점등
초기화 설정값
Watchdog 초기화
Watchdog 초기화 설정값
사용자태스크 실행코드 크기
사용자태스크 실행코드 크기
키스위치 상태 정보
부트모드값 설정
파라미터체크섬
파라미터체크섬
패스워드 값
패스워드 값
실행코드 체크섬
실행코드체크섬값
실행코드
실행코드
pSET 전역변수 초기값
메모리 진단관련 변수 초기화
태스크 정보 초기값
특수레지스터 초기값
FMS통신관련 메모리영역
FMS통신관련 메모리영역
HR-SDL 통신관련 메모리영역
HR-SDL 통신관련 메모리영역
HR-SDN 통신관련 메모리영역
HR-SDN 통신관련 메모리영역
실시간클럭 초기화
RTC 값
RTC값
부트모드에 따른 LED 점등값
LED 점등
pSET 데이터 메모리 영역 초기값
I/O 형상정보 배열 초기값
래치영역 정보
래치영역 정보

KAERI

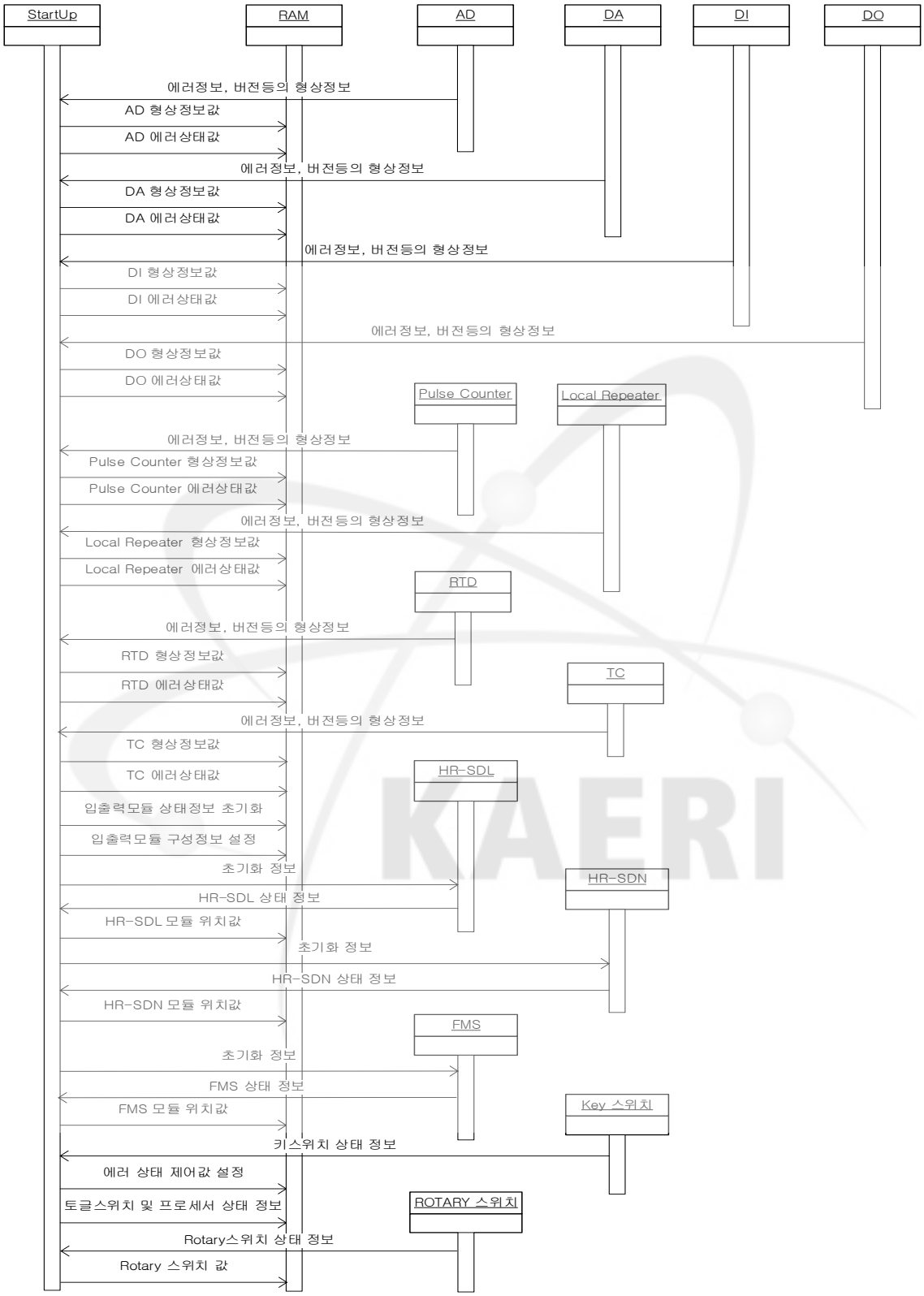


그림 3.8 시작 소프트웨어 인터페이스 설계기술

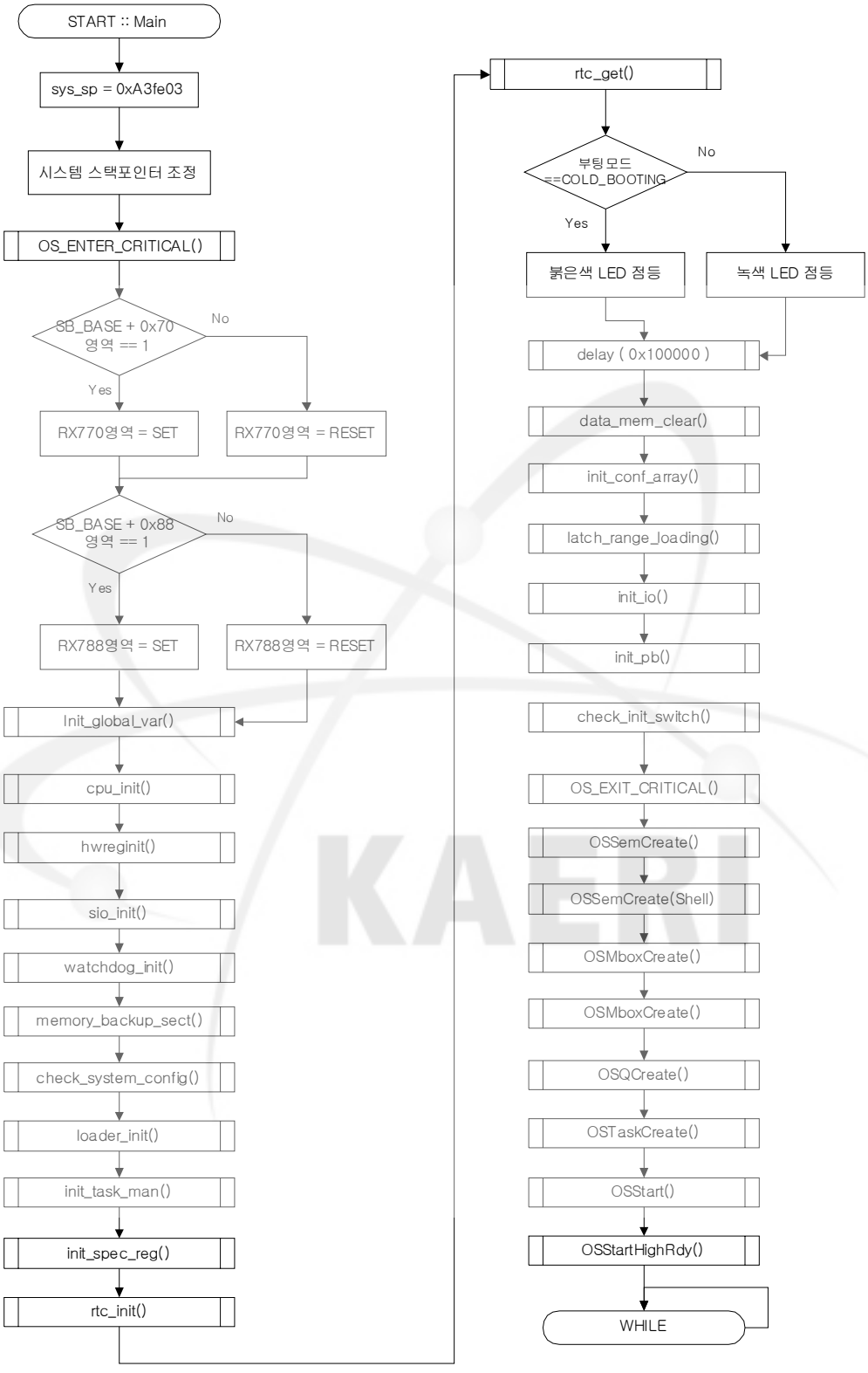


그림 3.9 시작 소프트웨어 상세 설계기술

2. 안전등급 PLC 프로세서 모듈 PLD 고신뢰도화 개발 및 PLC 특정주제기술보고서(TR) 작성 지원

가. 안전등급 PLC 프로세서 모듈 PLD 요구사항 명세서 개발

본 연구에서는 안전등급 PLC 프로세서 모듈 PLD(NLCPU-1Q)는 NCPU-1Q 프로세서 모듈을 위한 Chip Selector 신호 생성기능, 접근주기 대기신호 (Access Cycle Wait) 생성기능, Piggyback Connector 연계기능, Watchdog 연계기능, RTC 연계기능, UART 연계기능, LED 연계기능, 스위치 연계기능, Reset 신호 생성기능, 인터럽트 생성기능 및 전원모듈 연계기능을 수행하였다.

Chip Selector 신호 생성기능

NLCPU-1Q PLD는 CPU로부터 버스 제어신호를 입력으로 받아 메모리 영역을 구분하여 해당 메모리 칩을 선택하는 기능을 가져야 한다. 또한 NLCPU-1Q PLD는 CPU로부터 버스 제어신호를 입력으로 받아 입출력 모듈 및 통신 모듈과의 연계를 위한 백플레인 버스 영역을 선택하는 기능을 가져야 한다.

접근주기 대기신호 생성기능

NLCPU-1Q PLD는 각종 메모리 칩의 버스 접근 주기에 따라 CPU가 버스 사이클을 기다리도록 하는 기능을 가져야 한다.

Piggyback Connector 연계기능

NLCPU-1Q PLD는 CPU로부터 버스 제어신호를 입력으로 받아 Piggyback 영역을 선택하는 신호를 출력하는 기능을 가져야 한다.

Watchdog Timer 관련 기능

NLCPU-1Q PLD는 Watchdog 관련 설정 및 Watchdog 타임아웃 발생 여부에 따라 Watchdog 타이머를 업데이트하는 신호를 제공하는 기능을 가져야 한다.

RTC (Real Time Clock) 연계기능

NLCPU-1Q PLD는 CPU로부터 버스 제어신호를 입력으로 받아 RTC와 CPU를 연계하는 기

능을 제공해야 한다.

UART 연계기능

NLCPU-1Q PLD는 CPU로부터 버스 제어신호를 입력으로 받아 UART 칩과 CPU를 연계하는 기능을 제공해야 한다.

LED 연계기능

NLCPU-1Q PLD는 CPU로부터 버스 제어신호를 입력으로 받아 LED와 CPU를 연계하는 기능을 제공해야 한다.

스위치 연계기능

NLCPU-1Q PLD는 CPU로부터 버스 제어신호를 입력으로 받아 스위치와 CPU를 연계하는 기능을 제공해야 한다.

리셋신호 생성기능

NLCPU-1Q PLD는 프로세서 모듈의 다양한 리셋 신호를 받아 CPU를 리셋 시키는 신호를 출력하는 기능을 가져야 한다.

인터럽트 생성기능

NLCPU-1Q PLD는 각종 인터럽트를 CPU가 처리할 수 있도록 하는 신호를 출력하는 기능을 가져야 한다.

전원모듈 연계기능

NLCPU-1Q PLD는 AC 전원 고장 시에 인터럽트를 발생하여 프로세서 모듈이 해당 동작을 수행할 수 있도록 하는 기능을 제공해야 한다.

나. 안전등급 PLC 프로세서 모듈 PLD 설계 명세서 개발

안전등급 PLC 프로세서 모듈 PLD 설계 명세서는 NLCPU-1Q 요구사항명세서의 기능 요구사항과 기타 요구사항을 만족하기 위한 설계 내용을 기술하고 있다. 설계는 소프트웨어 설계와는

달리 PLD의 특성을 반영하여 연계 설계와 구조설계, 상세 설계로 나누어 수행하였으며, 이러한 내용을 설계 명세서에 반영하였다.

기능 블록간 연계 신호

NCPU-1Q의 PLD 로직은 그림 3.10에 나타나는 바와 같은 기능 블록과 그들의 연계 신호들로 설계된다.

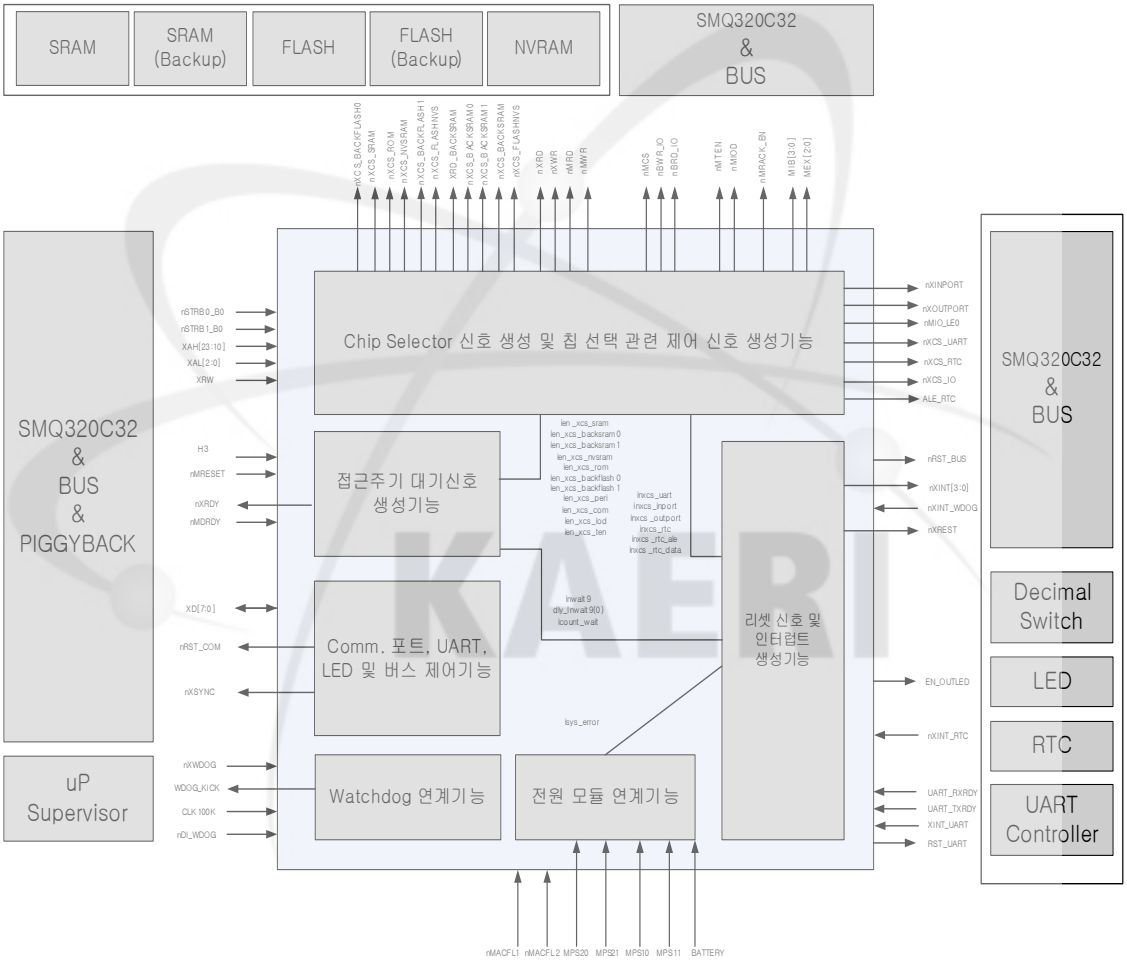


그림 3.10 기능 블록간 연계 신호도

PLD 로직 외부 입/출력 신호

NCPU-1Q의 PLD 로직은 표 3.2와 같이 입력 및 출력신호를 갖는다. 표 3.2는 PLD의 각 입출력 핀과 PLD 로직의 입출력 신호와의 관계를 기술한다.

표 3.2 PLD 입출력 핀 및 PLD 로직 입출력 신호

Pin Number	Signal Name	Direction
P1	nXREST	Output
P2	nXWR	Output
P4~P6	XAL[2:0]	Input
P7~P12, P14~P16, P18~P21, P23	XAH[23:0]	Input
P25~P32	XD[7:0]	Input/Output
P34	nIOSTRB	Input(Not Used)
P35	nSTRB0_B0	Input
P36	nSTRB1_B0	Input
P37	nMACFL1	Input
P39	MPS10	Input
P40	MPS11	Input
P41	nMACFL2	Input
P43	MPS20	Input
P44	MPS21	Input
P45	nMIRQ0	Input (Not Used)
P46	nMIRQ1	Input (Not Used)
P47	nMIRQ2	Input (Not Used)
P48	nMAS	Output (Not Used)
P49, P53~P55	MIB[3:0]	Output
P56, P60~P61	MEX[2:0]	Output
P62	nRST_COM	Output
P63	nMRACK_EN	Output
P65	nMTEN	Output
P66	nMIOD	Output
P67	nMIO_LE0	Output
P68	nMIO_LE1	Output (Not Used)
P69	nMRD	Output
P70	nMWR	Output
P75	nXCS_BACKSRAM	Output
P77	nXCS_BACKFLASH0	Output
P78	nXCS_SRAM	Output
P79	nXCS_ROM	Output
P80	nXCS_RTC	Output
P81	nXCS_UART	Output
P82	nXCS_COM_ALL	Output (Not Used)
P83, P84	nXCS_COM[1:0]	Output (Not Used)
P87	nBRD_IO	Output
P88	nBWR_IO	Output
P89	XSEL_COM_CH	Output (Not Used)
P90	nXINPORT	Output
P91	nXOUTPORT	Output
P92	nEN_OUTLED	Output
P93	nRST_BUS	Output
P94	XINT_UART	Input
P96	nXINT_WDOG	Input
P97~P100	nXINT_COM[3:0]	Input(Not Used)
P101	nXINT_RTC	Input

P102	**nXCS_NVSRAM**	**Output**
P103	**nDI_WDOG**	**Input**
P104	**nXCS_BACKFLASH1**	**Output**
P106	**RST_UART**	**Output**
P107	**ALE_RTC**	**Output**
P110	**nXCS_IO**	**Output**
P111	**nXCS_FLASHNVS**	**Output**
P112	**XRD_BACKSRAM**	**Output**
P113	**BATTERY**	**Input**
P114	**TP1**	**Output (Not Used)**
P116	**nUART_RXRDY**	**Input**
P117	**nUART_TXRDY**	**Input**
P118	**nXCS_BACKSRAM0**	**Output**
P119	**nXCS_BACKSRAM1**	**Output**
P120	**nXBUSY_COM**	**Input(Not Used)**
P122	**nMDRDY**	**Input**
P125	**CLK100K**	**Input**
P126	**nMRESET**	**Input**
P127	**H3**	**Input**
P128	**XRW**	**Input**
P132	**nXRD**	**Output**
P133	**nXRDY**	**Output**
P134	**nXHOLD**	**Output (Not Used)**
P136~P139	**nXINT[3:0]**	**Output**
P140	**WDOG_KICK**	**Output**
P141	**nXSYNC**	**Output**
P142	**nMCS**	**Output**
P143	**nXWDOG**	**Input**

PLD 구조설계

NCPU-1Q의 PLD 구조설계는 PLD의 기능을 구현하기 위한 기능 모듈의 정의와 구성에 대해 기술한다. PLD는 7개의 기능부를 가지고, 각 기능부는 PLD 요구사항 명세서에 기술된 기능 요구 사항을 만족하도록 여러 개의 기능 모듈을 포함한다. 그림 3.11은 Chip Selector 신호 생성 기능 모듈에 대한 구조설계를 나타낸다.

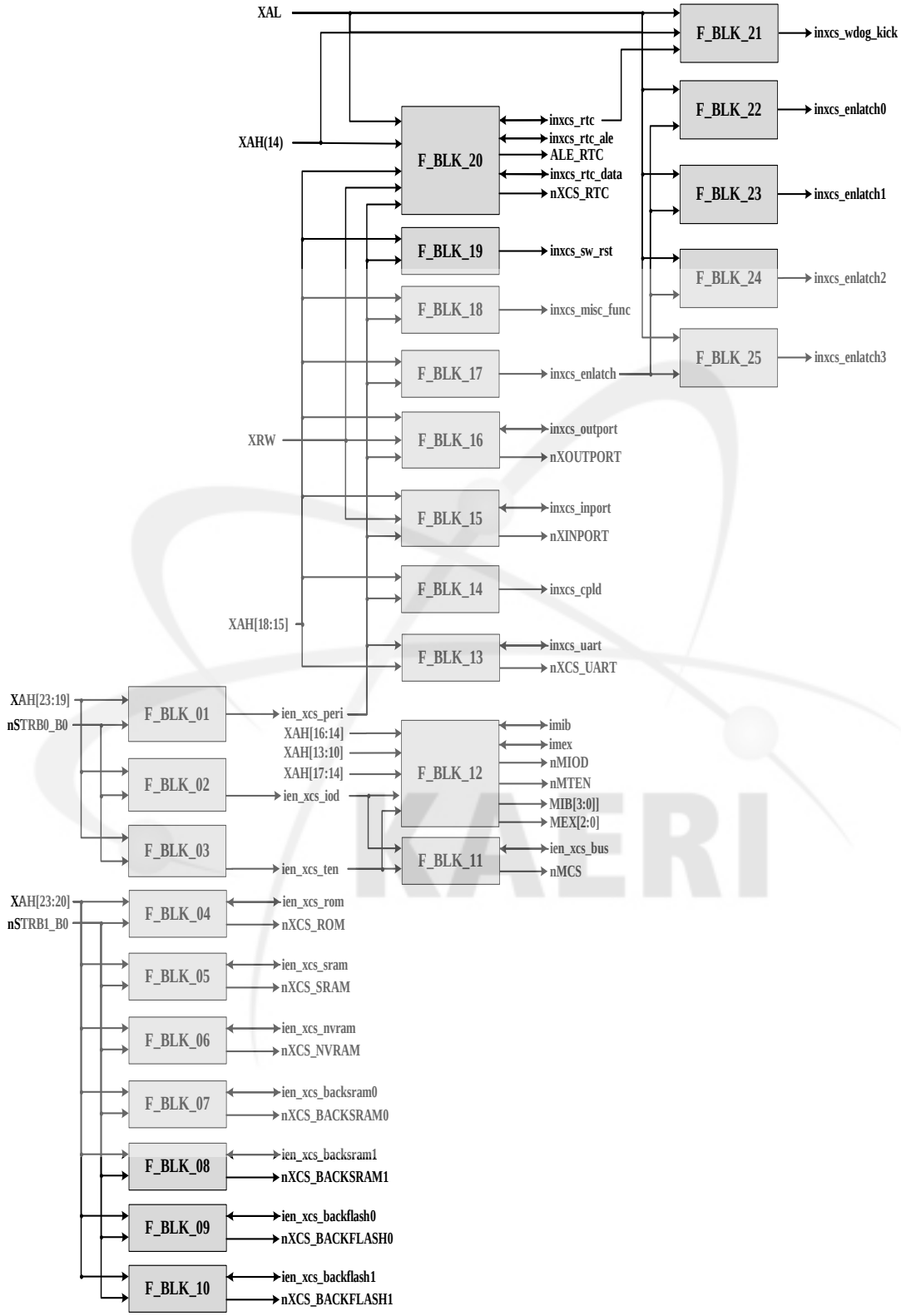


그림 3.11 Chip Selector 신호 생성 기능 모듈

PLD 상세설계

NCPU-1Q의 PLD 구조설계는 PLD의 기능을 구현하기 위한 기능 모듈의 정의와 구성에 대해 기술한다. Peripheral을 위한 chip select signal(ien_xcs_peri) 생성 기능 모듈(F_BLK_01)에 대한 상세설계는 다음과 같다.

0x40_0000~0x4F_FFFF에 할당된 peripheral(uart, rtc, led, switch, pld register, etc)을 위한 chip select signal 설계는 다음의 Pseudo Code와 같다.

```
If (nSTRB0_B0='0' and XAH(23 downto 19)="00100") then
   ien_xcs_peri shall be '1'
Else
   ien_xcs_peri shall be '0'
Endif
```

다. 안전등급 PLC 프로세서 모듈 PLD 시험계획서/절차서/보고서 개발

NLCPU-1Q PLD는 CPU 및 프로세서 모듈의 주변 장치들과의 연계 신호들을 처리하는 기능을 위주로 구성되어 있어서 컴포넌트 시험과 통합 시험을 수행할 때 프로세서 모듈 내에 기능별 연계가 발생하도록 하는 별도의 프로그램을 탑재하여 수행하는 방식으로 시험을 진행하였다. PLD 특성 상 컴포넌트로 분리되지 않는 기능들에 대해서는 컴포넌트 시험 없이 통합 시험만을 수행하였다.

표 3.3은 기능 별 출력을 나타내며, 이것을 중심으로 컴포넌트시험을 수행한다.

표 3.3 NLCPU1의 컴포넌트시험 대상

기능	시험번호	이름	시험대상	설명
Chip Selector 신호 생성 기능	NLCPU1 -CT01	nXCS_ROM	F_BLK_04	ROM 선택
	NLCPU1 -CT02	nXCS_SRAM	F_BLK_05	SRAM 선택
	NLCPU1 -CT03	nXCS_NVSRAM	F_BLK_06	NvSRAM 선택
	NLCPU1 -CT04	nXCS_BACKSRAM0	F_BLK_07	BackSRAM0 선택
	NLCPU1 -CT05	nXCS_BACKSRAM1	F_BLK_08	BackSRAM1 선택
	NLCPU1 -CT06	nXCS_BACKFLASH0	F_BLK_09	FLASH0 선택
	NLCPU1 -CT07	nXCS_BACKFLASH1	F_BLK_10	FLASH1 선택
	NLCPU1 -CT08	nMCS	F_BLK_02, F_BLK_03, F_BLK_11	버스용 칩 선택 신호
	NLCPU1 -CT09	nMIOD	F_BLK_02, F_BLK_03,	I/O 장치 연계

			F_BLK_12	
	NLCPU1 -CT10	nMTEN	F_BLK_02, F_BLK_03, F_BLK_12	통신 장치 연계
	NLCPU1 -CT11	MEX	F_BLK_02, F_BLK_03, F_BLK_12	Backplane Bus Decorder와 연결 (통신)
	NLCPU1 -CT12	MIB	F_BLK_02, F_BLK_03, F_BLK_12	Backplane Bus Decorder와 연결 (I/O)
	NLCPU1 -CT13	nXCS_UART	F_BLK_01, F_BLK_13	UART 칩 선택 신호
	NLCPU1 -CT14	nXINPORT	F_BLK_01, F_BLK_15	스위치 상태 래치용 출력
	NLCPU1 -CT15	nXOUTPORT	F_BLK_01, F_BLK_16	LED 출력
	NLCPU1 -CT16	ALE_RTC	F_BLK_01, F_BLK_20	RTC Address Latch
	NLCPU1 -CT17	nXCS_RTC	F_BLK_01, F_BLK_20	RTC 칩 선택 신호
칩 선택 관련 제어 신호 생성 기능	NLCPU1 -CT18	nMRACK_EN	F_BLK_02, F_BLK_03, F_BLK_12, F_BLK_26	Backplane Bus Enable
	NLCPU1 -CT19	nBRD_IO	F_BLK_02, F_BLK_03, F_BLK_27	I/O Read
	NLCPU1 -CT20	nBWR_IO	F_BLK_02, F_BLK_03, F_BLK_28	I/O Write
	NLCPU1 -CT21	nMWR	F_BLK_29	Backplane Bus Write
	NLCPU1 -CT22	nMIO_LE0	F_BLK_02, F_BLK_03, F_BLK_11, F_BLK_30, F_BLK_40, F_BLK_41	Extra Backplane Bus Write
	NLCPU1 -CT23	nXCS_IO	F_BLK_01, F_BLK_13, F_BLK_15, F_BLK_16, F_BLK_20, F_BLK_31	Peripheral 연계 출력 Enable 신호
	NLCPU1 -CT24	nXCS_FLASHNVS	F_BLK_06, F_BLK_09,	FLASH 및 NVSRAM Output Enable

			F_BLK_10, F_BLK_32	
	NLCPU1 -CT25	nXCS_BACKSRAM	F_BLK_07, F_BLK_08, F_BLK_33	BackSRAM 선택
	NLCPU1 -CT26	XRD_BACKSRAM	F_BLK_34	BackSRAM Output Enable
	NLCPU1 -CT27	nXRD	F_BLK_35	Memory Read
	NLCPU1 -CT28	nMRD	F_BLK_35	Backplane Bus Read
	NLCPU1 -CT29	nXWR	F_BLK_35	Memory Write
접 근 주 기 대기신호 생성 기능	NLCPU1 –CT30	nXRDY	F_BLK_01, F_BLK_02, F_BLK_03, F_BLK_04, F_BLK_06, F_BLK_07, F_BLK_08, F_BLK_09, F_BLK_10, F_BLK_11, F_BLK_36, F_BLK_37, F_BLK_38, F_BLK_39, F_BLK_40	Ready
Watchdog 연계 기능	NLCPU1 –CT31	WDOG_KICK	F_BLK_01, F_BLK_17, F_BLK_20, F_BLK_21, F_BLK_22, F_BLK_25, F_BLK_42, F_BLK_43, F_BLK_44, F_BLK_49, F_BLK_55, F_BLK_57	Watchdog 발생(Kick)
리셋 신호 및 인터럽트 생성 기능	NLCPU1 –CT32	nXINT	F_BLK_01, F_BLK_17, F_BLK_22, F_BLK_23, F_BLK_24, F_BLK_25,	인터럽트

			F_BLK_47, F_BLK_48, F_BLK_55, F_BLK_57	
	NLCPU1 –CT33	nXREST	F_BLK_01, F_BLK_17, F_BLK_25, F_BLK_43, F_BLK_44, F_BLK_49	CPU Reset
Comm, 포트, UART, LED 및 버스 제어 기능	NLCPU1 –CT34	nXSYNC	F_BLK_01, F_BLK_18, F_BLK_19, F_BLK_50, F_BLK_55	동기화 신호
	NLCPU1 –CT35	nRST_COM	F_BLK_51, F_BLK_55, F_BLK_57	Piggy Back 영역 리셋
	NLCPU1 –CT36	RST_UART	F_BLK_52, F_BLK_55, F_BLK_57	UART 리셋
	NLCPU1 –CT37	nRST_BUS	F_BLK_01, F_BLK_17, F_BLK_25, F_BLK_43, F_BLK_44, F_BLK_49, F_BLK_53, F_BLK_55, F_BLK_57	리셋 스위치에 의한 버스 리셋
	NLCPU1 –CT38	nEN_OUTLED	F_BLK_01, F_BLK_17, F_BLK_22, F_BLK_54, F_BLK_57	LED 출력 Enable

그림 3.12와 3.13은 표 3.3에서 정의한 시험항목 중 NLCPU1-CT01 에 대한 시험입력을 넣었을 때의 예상결과와 실제결과이다.

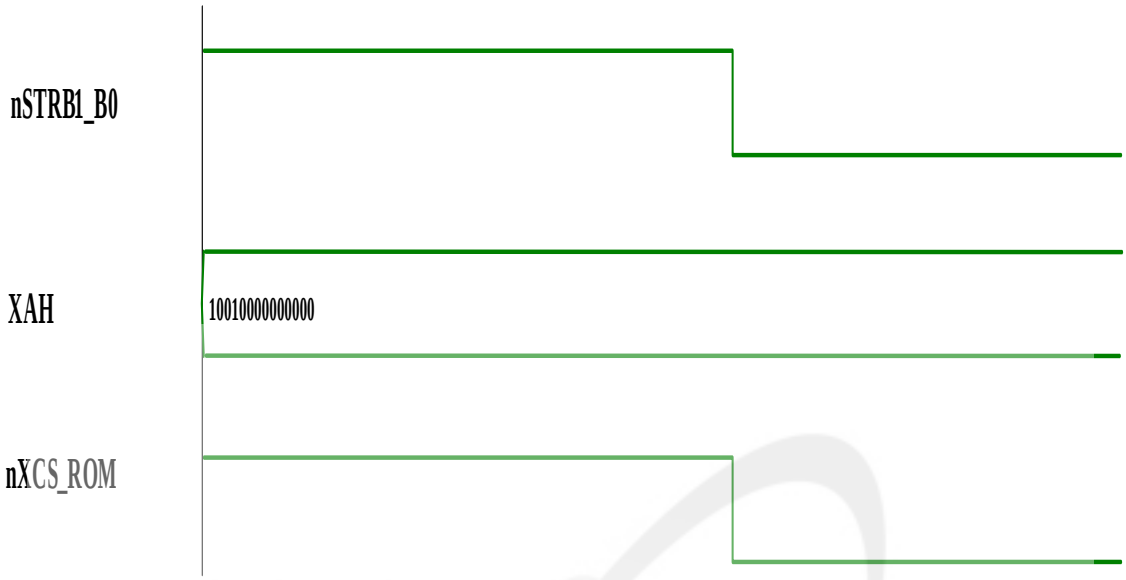


그림 3.12 NLCPU1-CT01 예상결과

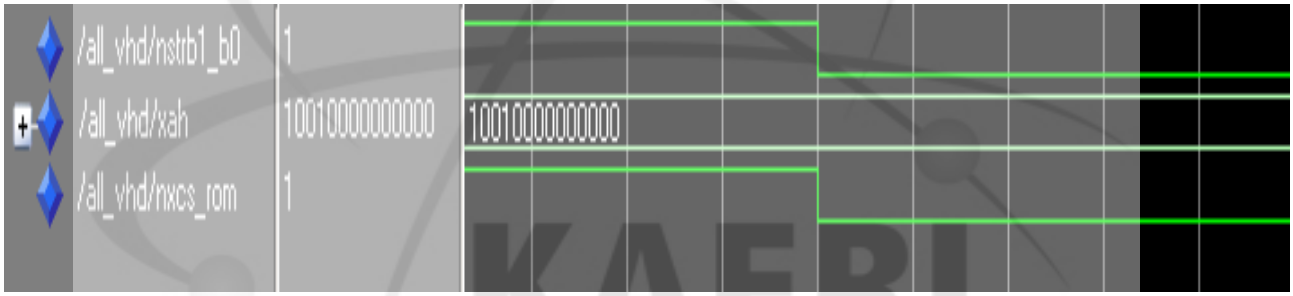


그림 3.13 NLCPU1-CT01 실제결과

라. 안전등급제어기기 특정주제기술보고서 작성 지원

안전등급제어기기 POSAFE-Q에 대한 특정주제기술보고서는 주로 개념단계의 설계문서들과 소프트웨어 요구사항 명세서를 토대로 작성되었다. 본 과제에서는 개념단계의 설계문서를 개정하여 특정주제기술보고서에 품질 높은 내용을 반영하도록 함과 동시에 특정주제기술보고서 중 PLC 프로세서 모듈에 해당하는 부분을 직접 작성하였다.

3. 소프트웨어 시험 및 이중화 PLC 개발 지원

가. RTOS 소프트웨어 컴포넌트 시험 및 통합 시험

본 연구에서는 RTOS 소프트웨어에 대한 컴포넌트 시험 및 통합 시험을 모과제와 협력하여 수행하였다. pCOS에 대한 소프트웨어 컴포넌트 시험 및 통합 시험은 다음 그림 3.14와 같은 환경에서 수행되었다.

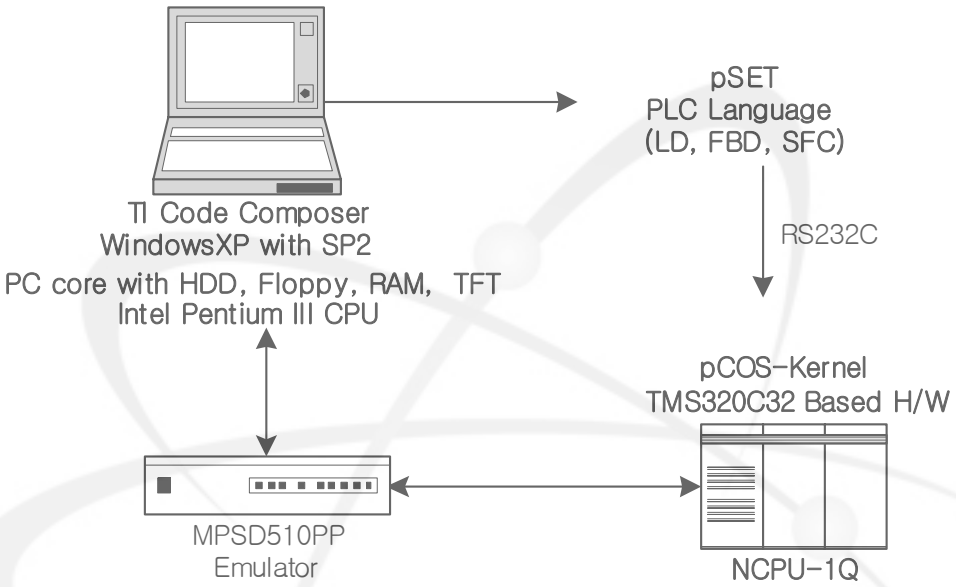


그림 3.14 소프트웨어 시험 환경

시험 항목은 소프트웨어 요구사항 명세서, 소프트웨어 설계 명세서 및 소스 코드를 근거로 도출하였고, 각 항목 별로 ID를 부여하여 체계적인 시험 설계 및 수행이 되도록 하였다. 표 3.4는 컴포넌트 시험 항목에 대한 예로서, 커널의 컴포넌트 시험 항목들을 보여준다.

표 3.4 커널에 대한 컴포넌트 시험 항목

시험 항목 ID	시험 대상 컴포넌트	설명
K-TI-1-01	OSSched	스케줄링
K-TI-2-01	OSTimeDly	시간 지연
K-TI-3-01	OSSemCreate	세마포어 생성
K-TI-3-02	OSSemPend	세마포어 대기
K-TI-3-03	OSsemPost	세마포어 전송
K-TI-3-04	OSMboxCreate	메일박스 생성
K-TI-3-05	OSMboxPend	메일박스 대기
K-TI-3-06	OSMboxPost	메일박스 전송
K-TI-3-07	OSQCreate	큐 생성
K-TI-3-08	OSQPend	큐 대기
K-TI-3-09	OSQPost	큐 전송
K-TI-4-01	OSTaskCreate	태스크 생성
K-TI-4-02	OSTaskDel	태스크 삭제

소프트웨어 컴포넌트 시험 및 통합 시험 결과 주로 소프트웨어 요구사항 명세 및 소프트웨어 설계 명세 상의 오류들이 많이 발견되었으며, 일부 프로그램 소스 코드 상의 오류나 추가 및 삭제해야 하는 부분들이 발견되어 수정하였다.

나. 이중화 PLC 개념 설계

CPU 이중화는 다음 그림 3.15와 같은 구성을 가진다. 이중화 구성은 CPU, HBU, Network부분으로 나눠진다. 각각은 모두 piggy back 형태로 독립해서 장착되며, HBU는 HBU끼리 연결되어서 동기화등의 HBU에 관련된 일을 수행하고, Network부분은 Master/Slave구조로 I/O의 데이터의 입출력 작업을 한다.

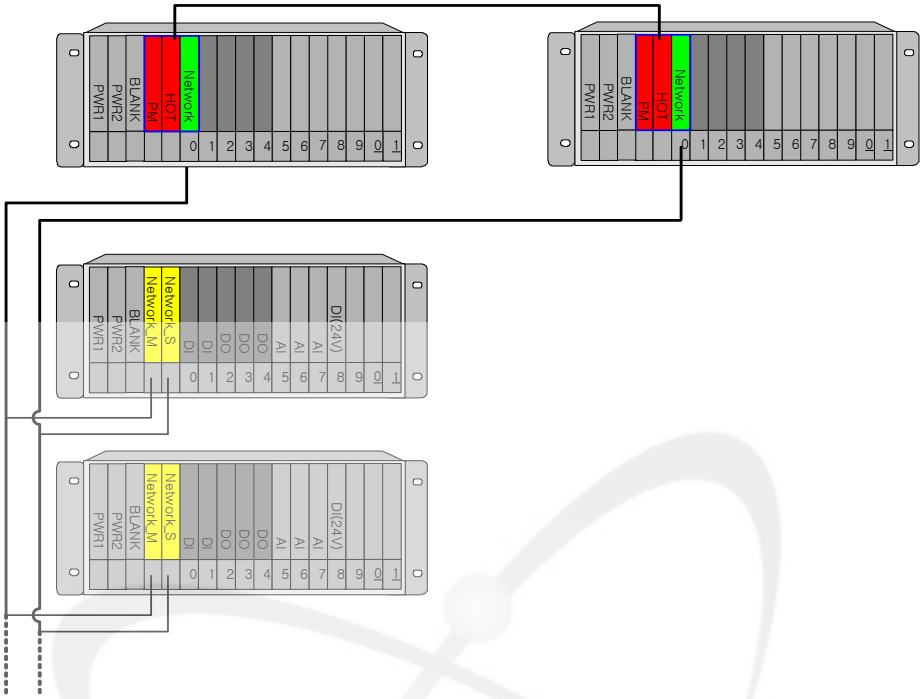


그림 3.15 이중화 PLC 구성 안

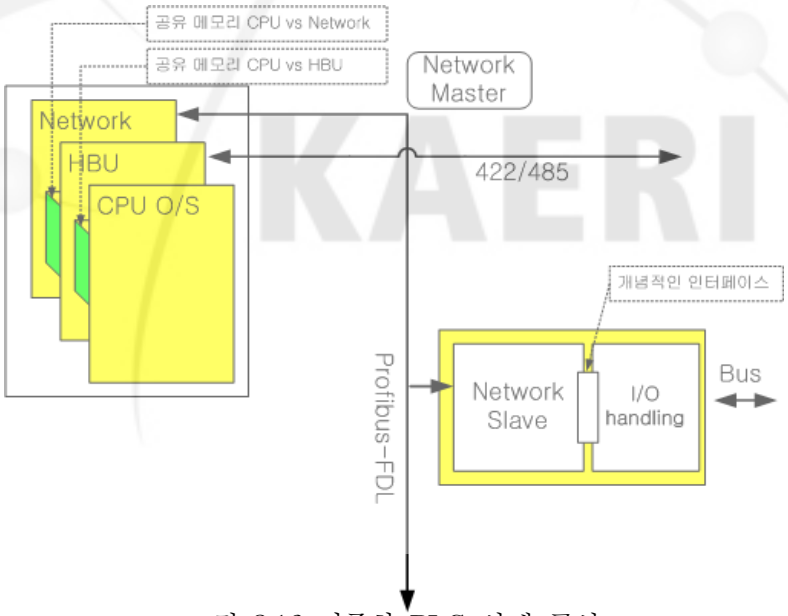


그림 3.16 이중화 PLC 상세 구성

그림 3.16의 경우는 좀 더 구체적으로 구성을 보이고 있다. CPU, HBU, Network부분은 모두 공유메모리로 정보를 교환하고, 경우에 따라 HBU가 없이 Network Piggy back만 올릴 수도 있는 구조이어야 한다. Network Master/Slave는 Profibus-DPM/S와 유사한 구조가 되도록 설계한다.

소프트웨어간 Interface

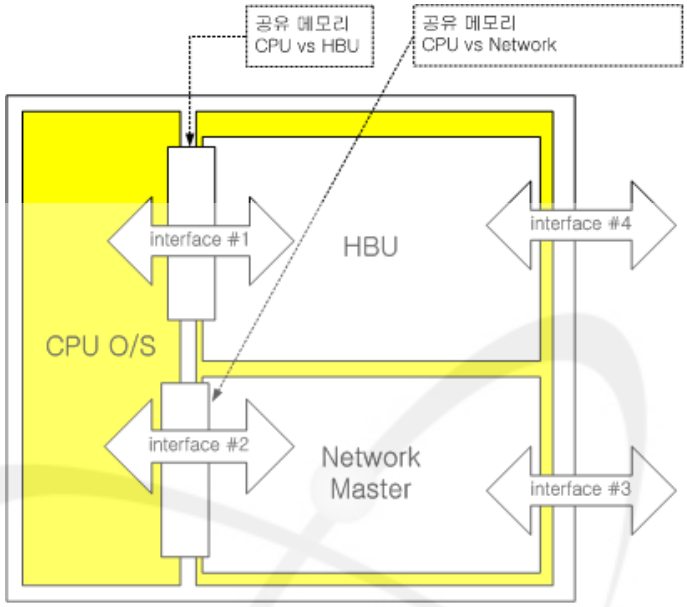


그림 3.17 소프트웨어 간 인터페이스

Interface #1

CPU O/S와 HBU는 다음과 같은 인터페이스를 한다.

1. HBU간의 동기화를 위한 정보를 CPU에게 전달한다.
2. HBU는 CPU의 상태를 감시하기 위해 CPU의 상태 정보를 읽어온다.
3. 상대편 CPU로 데이터를 보내거나 읽기위한 인터페이스를 제공한다.

Interface #2

1. Network Master와 CPU와의 인터페이스이다.
2. Network Master의 상태 정보를 CPU에 전달한다.
3. Network Master의 파라메터를 CPU로 부터 받는다.
4. Network Slave를 통해 Network Master로 들어온 I/O 데이터 CPU에 전달한다.
5. CPU로 부터 데이터를 읽어온다.

Interface #3

1. Network Master 와 Network Slave간의 인터페이스를 한다.
2. Network Master의 I/O 출력 데이터를 Network Slave로 전달한다.
3. Network Slave의 I/O 입력 데이터를 Network Master로 전달한다.
4. Netwrok Save의 상태 정보를 Network Master로 전달한다.
5. Network Master에서 상태 정보를 Network Slave로 설정한다.

Interface #4

1. HBU간의 인터페이스를 한다.
2. 일정 주기의 동기신호를 서로 주고받는다.
3. 동기 신호는 각 응용프로그램 타스크 간에 동기를 맞추어줘야 한다.
4. 실행 코드 및 구성 파일의 동일함을 확인하거나 다운로드 업로드를 할 수 있도록 한다.
5. CPU간의 모든 정보 Path를 제공한다.

KAERI

이중화 CPU O/S

이중화 CPU O/S 소프트웨어는 HBU에 의해 동기를 맞춰야한다. 동기가 일치하지 않으면 일치하도록 조정해야 하고 계속해서 동기가 맞지 않으면 실행에 문제가 있으므로 적절한 에러 처리를 해야 한다. 이 이중화는 마스터/슬레이브의 개념보다는 시스템 이중화의 개념이다. 즉, 양 PLC 시스템은 똑같이 입력을 한다. 다만 슬레이브 단에서 선택적으로 출력을 내보낸다. 여기서도 동기가 맞지 않는 경우 어떻게 처리해야 할지는 좀 더 연구해야 한다.

이중화 CPU에서는 Master Station에 실행코드 (응용프로그램)을 다운로드하면 이중화 모드에서는 Slave Station에 같은 코드가 다운로드 될 수 있도록 한다.

좀 더 확대된 개념으로 pSET은 Master Station인지 Slave Station인지에 대한 구분이 없이 두 대의 PLC가 하나인 것처럼 동작을 해야 한다. 예를 들면, Task Run시 두 대의 PLC가 동시에 Run의 상태에 들어가야 한다. 명령을 똑같이 받아서 처리한다.

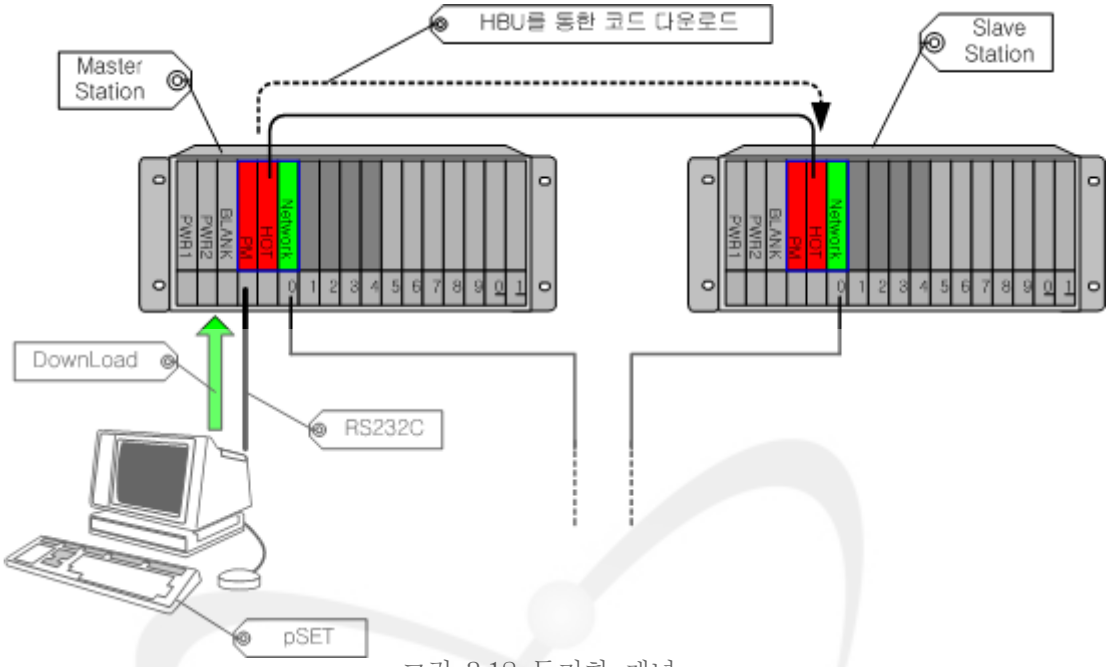


그림 3.18 동기화 개념

Master/Slave 지정 방법

1. Slave CPU보다 Master CPU가 먼저 시작(Power On)되는 경우 Master가 된다. (즉, Power가 먼저 들어온 CPU가 Master이다.)

2. Master/Slave CPU지정은 따로 하드웨어적으로는 없다.

이중화 모드

Master/Slave CPU는 둘 중 어느 쪽도 Master나 Slave CPU Mode를 담당할 수 있다. 즉 두 CPU는 같은 조건이고 다만 전원이 먼저 들어온 쪽이 Master가 된다. 그 작동 모드는 다음과 같게 볼 수 있다.

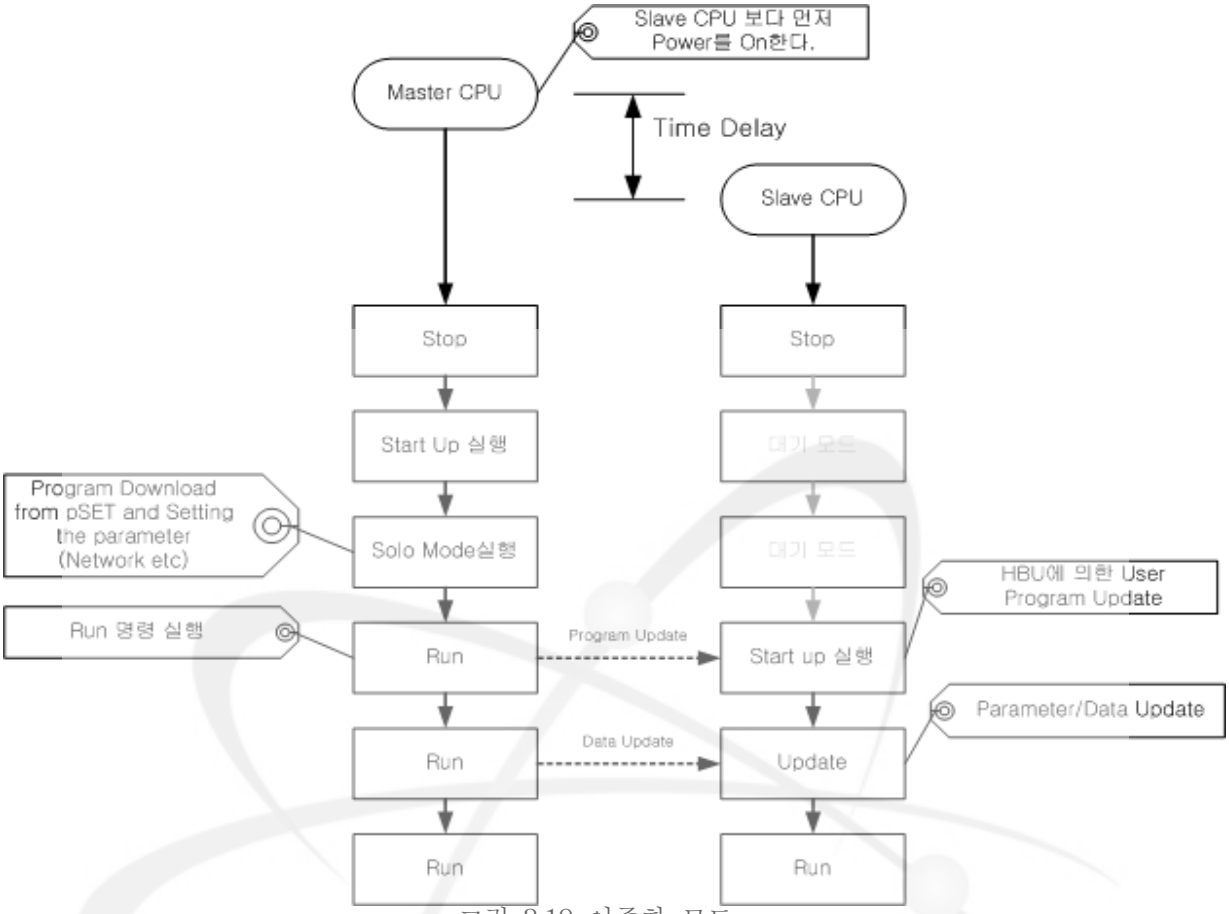


그림 3.19 이중화 모드

그림 3.19에서 Program Update는 한 스캔주기에 일어나는 것이 아니고 여러 스캔주기에 걸쳐 일어나야 한다(프로그램 사이즈가 크기 때문에 한 스캔주기에는 Update가 어려울 것으로 보임). 다만 Data Update는 한 스캔주기에 일어나야 한다. 그래야 Slave CPU의 실행을 할수 있다. Data Update는 입력, 출력, 타이머, 카운터, 메모리(특수 레지스터)등이다.

이와 같이 하는 이유는 하나의 CPU를 교체하고 다시 Slave CPU의 전원을 올렸을 때도 위와 같이 자동으로 Program/Data가 Update되어야 동기를 맞출 수 있기 때문이다. HBU가 Slave CPU의Start up 상태를 확인해서Program/Data를 Update한다.

CPU는 Solo 모드, 이중화 모드, 동기 모드로 구분될 수 있는데 이중 동기모드는 Master와 Slave간의 동기(Program/Data)맞추는 것을 뜻한다.

이중화 HOT Backup S/W

HBU는 동기 신호를 위해 HBU간의 통신을 한다. HBU는 일정한(정확한) 주기로 동기신호를

주어야 하며 동기 신호가 불확실하거나 일정치 않으면 에러를 발생해서 이를 상태 LED로 보여줘야 하며, pSET은 Master Station을 통해서 Slave Station의 구성을 Upload하거나 DownLoad할 수 있어야 한다.

HBU는 자신이 Master인지 Slave인지를 설정할 수 있는 기능을 제공해야 한다.

이중화 동기 방안

이중화 동작 중에는 CPU모듈 간에 데이터와 운전시점의 동기를 맞춰져야한다.

1. 출력 Data Update
2. Data 변경 시 Update (강제 설정시)
3. 태스크 시작 시
4. CPU 내부 시간 데이터의 변경 시

동기 방법

1. 입력은 각각의 CPU가 입력으로 받기 때문에 동기를 맞추지는 않아도 되나 입력된 데이터가 동일하다를 것에 대한 동기 방법이 있어야 한다.
2. 출력은 각각의 CPU가 입력된 데이터를 가지고 연산을 하고 그 연산 값이 같아야 하는데 이에 대한 동기 방법이 있어야 한다.
3. 스캔타임이 같게 설정되어있어도 CPU내의 연산 시간은 차이가 날수 있으므로 이에 대한 스캔타임의 동기를 맞춰주는 동기 방법이 있어야 한다.
4. pSET을 통한 데이터 변경 시 동기 방법이 있어야 한다.
5. 태스크 시작 시 (Run) 시작 시점을 일치시키는 동기 방법이 있어야 한다.
6. CPU내부의 시간 데이터를 일치하는 동기 방법이 있어야 한다.

Master/Slave Change 조건

이중화 운전 중 Master Station측의 결함으로 운전 불능 상태가 되면, Master는 운전정지 상태가 Slave(StandBy)가 Master로 운전을 한다. 운전 중 Master가 Change되는 조건은 다음과 같다.

1. Master의 Power가 Off 되었을 때

2. Master의 응용 프로그램 수행이 정지되었을 때

3. Master의 프로그램 실행이 Stop에 의해 정지되었을 때

4. Master의 자가진단의 결과가 에러를 발생하였을 때(자체 테스트)

5. Master의 네트워크가 이상이 발생하였을 경우

Network Master 소프트웨어

Network Master는 네트워크의 상태를 확인하고 데이터를 전송하거나 수신한다. Network Master는 기본적으로 Profibus-FDL H/W 로 구성되며 기능은 Profibus-DPM와 유사한 기능을 수행하되 최소한의 데이터의 처리와 네트워크 기능하도록 구성한다. Network Master는 수신된 데이터를 CPU로 전송하거나, CPU로 수신된 데이터를 Network Slave로 전송한다. Network Master의 기본적인 파라메터는 CPU를 통해 받는다. Network Master는 모두 16스테이션의 Network Slave를 가지도록 한다.

Network Slave 소프트웨어

Profibus-DPS의 프로토콜을 활용한다. DPS의 특성상 취급가능한 접점은 512Word이므로 DI/DO의 경우는 16슬롯까지 수용가능하나, AD, DA는 최대 10슬롯만 가능하다.

Network Slave I/O Handling 소프트웨어

I/O Handling은 I/O Update를 한다. 최종 I/O의 데이터 출력은 H/W적으로 구현한다. 내부적으로 Network부분과 I/O handling부분이 구분되어서 개발되어야 한다.

KAERI

제 3 절 RPS 구조 검증

1. 개발 개요

본 연구에서는 KNICS 과제에서 개발한 원자로보호계통 중 자동시험 및 연계프로세서(ATIP : Auto Test and Integrate Test Processor), BP(Bistable Processor), CP(Coincidence Processor)의 구조 및 성능이 제대로 수행되는지 시험하기 위해 각종 시험을 수행하고 추가적으로 보완될 사항에 대해서는 예비구현 및 선행 시험을 통해 원자로보호계통이 원활하게 수행될 수 있도록 하였다. 또한 특정주제기술보고서(TR) 작성에 필요한 사항 및 기술적 지원을 수행하였다. RPS 구조 검증과 관련된 전체 업무 내용을 그림 3.20에 나타내었다.

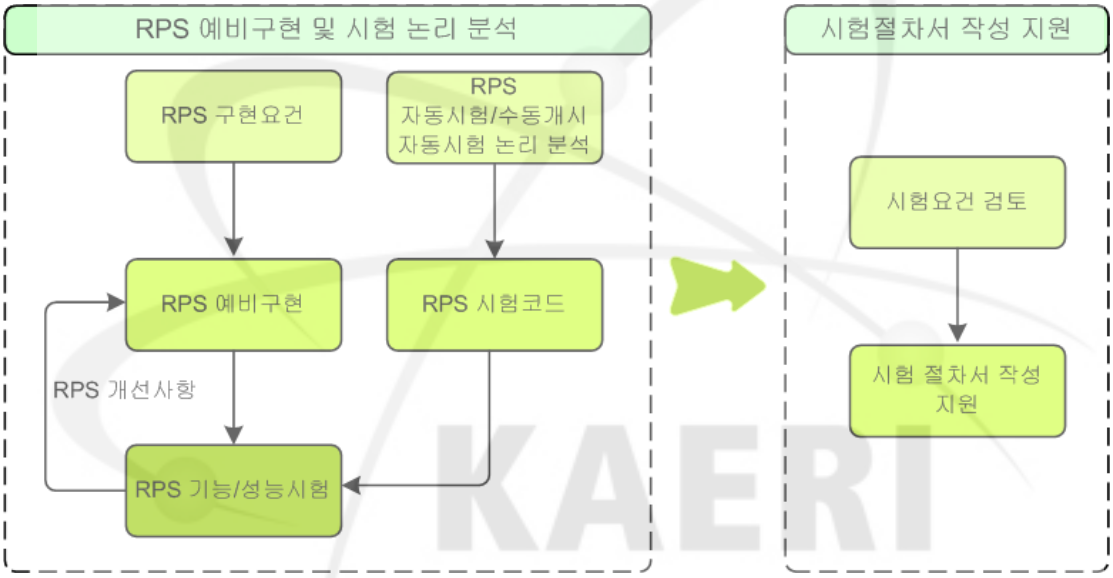


그림 3.20 원자로보호계통 구조검증 업무개요

본 연구에서 수행한 RPS 구조검증은 아래와 같은 3가지 업무로 구분된다.

- 원자로보호계통 예비구현 및 기능/성능시험
- 원자로보호계통 자동시험 및 수동개시 자동시험 논리분석
- 원자로보호계통 시험절차서 작성 지원

원자로보호계통 예비구현 및 기능/성능시험에서는 전 단계에서 구현된 원자로보호계통의 알고

리즘 및 구조가 성능을 원활히 수행 가능한지에 대한 기능/성능 시험을 수행하는 업무를 수행하였다. 원자로보호계통 중 자동시험 및 연계프로세서는 BP, CP의 건전성을 위해 시험 수행 및 그 결과를 판단하여 COM, QIAS로 전송하는 역할을 수행한다. 이러한 일련의 동작이 적절히 수행되기 위해서는 구현된 시험 기능 및 구조가 적절한지 재평가가 필요하다.

원자로보호계통 자동시험 및 수동개시 자동시험 논리분석 연구에서는 자동시험이 가지고 있는 시험 기능이 적절하게 수행되며 자동시험 수행 시 원자로 트립 유발, 원자로보호계통 문제가 발생하는 경우, 적절한 시점에 자동시험이 중지되는지 여부를 확인하는 업무가 필수적이다. 또한 수동개시 자동시험 시 중요하게 대두되는 채널우회, 전채널 우회 수행으로 유발될 수 있는 문제점에 대해서 파악하고 그 논리가 적절한지 시험하고 문제 발생 시 보완 사항을 제시하는 업무를 수행하는 것이다.

마지막으로 원자로보호계통 시험절차서 작성 업무는 주로 자동시험 및 연계프로세서 시험에 대한 시험절차서 및 시험보고서 등을 수행하였다. 자동시험 및 연계프로세서는 주로 건전성 감시 및 진단, 수동시험, 자동시험, 수동개시 자동시험에 대한 기능을 포함하고 있으며 각 시험이 수행되기 위한 논리 등이 적절한지 평가하기 위해서 시험절차서 및 시험보고서 작성이 필요하다. 이를 수행하기 위해서 비교논리프로세서(BP), 동시논리프로세서(CP)와의 연관관계 등을 잘 숙지하여 시험절차서 및 시험을 통한 시험보고서 작성 업무를 수행하였다.

가. 원자로보호계통 예비구현 및 기능/성능시험

원자로보호계통 연구를 통해 기본적인 시험 기능은 대부분 구현된 상태이다. 본 연구에서 추가적으로 구현된 기능은 시험을 위해 BP, CP에서 추가적으로 필요로 하는 기능을 구현하는 업무를 수행하였다. 시험 기능의 다양화에 따라 각 프로세서별 추가적인 기능이 필요하게 되었다. 시험 기능은 주로 인허가요건과 맞물려 시험 가능, 시험 요건, 시험 방법 등에 대해 인허가 요건을 충족하고 고장 및 진단을 최대한 빨리 찾아내도록 하기 위해서 다양한 시험 및 중복을 채택하였다. 이를 위해서 원자로보호계통 예비구현 시 발견하지 못한 오류들을 찾아내고 이를 기반으로 기능의 적절성, 안전성을 시험하고 응답요건 만족 범위 내에서 성능이 제대로 발휘하는지를 시험하였다.

나. 원자로보호계통 자동시험 및 수동개시 자동시험 논리분석

원자로보호계통의 고장 및 오류 진단을 위해서 다양하고 중복적인 방법을 통해 실시간, 운전원

판단에 의해 시험을 수행하게 된다. 본 연구에서는 자동주기 시험 및 수동시험 기능을 바탕으로 시험 요건 및 범위 안에서 시험을 적절히 수행하고 오류를 발생시킬 수 있는 조건을 최대한 활용하여 각종 시험에 대한 논리가 적절하게 구현되어 있으며 오류가 없는지를 판단하도록 구현하였다. 그러나 자동주기 시험으로 발생하는 채널우회, 전채널 우회 등에 대한 소프트웨어 안전등급으로 인해 다양한 문제가 제기되었다. 예를 들어 안전등급이 낮은 자동시험 및 연계프로세서에서 시험 시작 신호 발생에 따른 하위 안전등급 소프트웨어가 상위 안전등급 소프트웨어에 시험신호, 시험값 생성을 통한 시험 시작에 대한 논란의 여지가 있었다. 그 동안 자동주기 시험에 대한 각종 대안이 제시되었다. 그러나 자동주기 시험 방법을 기반으로 한 예비구현 등은 수행되었으나 이를 실제 적용한 사례가 없었다. 이를 위해 본 연구를 통해 수동개시 자동시험은 BP, CP에서 수행하고 그 결과는 운전원 판단에 의해 수행하도록 하였다. 또한 자동주기 시험은 BP, CP에서 정해진 시험 시간에 따라 시험을 수행하고 그 결과를 COM, QIAS 로 전송하는 방식을 채택하여 원자로보호계통의 기능과 시험에 대한 내용을 구현하였다.

다. 원자로보호계통 시험절차서 작성 지원

원자로보호계통과 관련된 구현이 완료되면 각종 시험 기능 및 트립 및 동시 논리가 적절히 수행되는 지를 시험보고서를 통해 증명할 필요가 있다. 이는 그 동안 수행하였던 연구내용 들이 정확하고 중복성과 다중성을 고려하여 설계하였다는 점을 인증기관으로부터 확인할 수 있는 과정이다. 이를 위해서는 각 프로세서에 대한 시험절차를 작성하여 시험보고서를 제출해야 하는 것이다.

KAERI

2. 개발 내용

가. 원자로보호계통 예비구현 및 기능/성능시험

본 연구에서 수행한 RPS 기능 예비구현 및 기능/성능시험에 대한 내용을 간략히 요약하면 다음과 같다. RPS 요건을 기반으로 비교논리 및 동시논리 기능에 대해 예비구현을 수행하였다. 비교논리 프로세서는 표 3.5에 나타낸바와 같이 18개의 공정변수를 포함하고 있다. 공정변수는 6가지 트립 결정 논리를 가지고 있다. 모든 비교논리 프로세서의 설정치 유형별로 논리를 구현하였다.

표 3.5 원자로보호계통 공정변수 및 설정치 종류

순서	변수명	설명	운전우회	설정치 종류
1	VA_OVR_PWR_Hi	가변 과출력		자동비율 상승
2	LOG_PWR_Hi	고 대수출력 준위	유	고정치 상승
3	LPD_Hi	고 국부출력 밀도		고정치 상승
4	DNBR_Lo	저 핵비등이탈률		디지털
5	PZR_PRS_Hi	가압기 고압력(NR)		고정치 상승
6	PZR_PRS_Lo	가압기 저압력(WR)	유	수동리셋 하강
7	SG1_LVL_Lo_RPS	증기발생기-1 저수위(WR)		고정치 하강
8	SG2_LVL_Lo_RPS	증기발생기-2 저수위(WR)		고정치 하강
9	SG1_LVL_Lo_ESF	증기발생기-1 저수위(WR)		고정치 하강
10	SG2_LVL_Lo_ESF	증기발생기-2 저수위(WR)		고정치 하강
11	SG1_LVL_Hi	증기발생기-1 고수위(NR)		고정치 상승
12	SG2_LVL_Hi	증기발생기-2 고수위(NR)		고정치 상승
13	SG1_PRS_Lo	증기발생기-1 저압력		수동리셋 하강
14	SG2_PRS_Lo	증기발생기-2 저압력		수동리셋 하강
15	CMT_PRS_Hi	격납건물 고압력(WR)		고정치 상승
16	CMT_PRS_HH	격납건물 고-고압력(NR)		고정치 상승
17	SG1_FLW_Lo	원자로냉각재-1 저유량		자동비율 하강
18	SG2_FLW_Lo	원자로냉각재-2 저유량		자동비율 하강

대표 공정변수에 대핸 트립 결정 논리를 포스콘에서 개발한 PLC Loader인 pSET을 이용하여 예비구현 하였다. 가변 상승형 구현한 논리를 그림 3.21에 나타내었다.

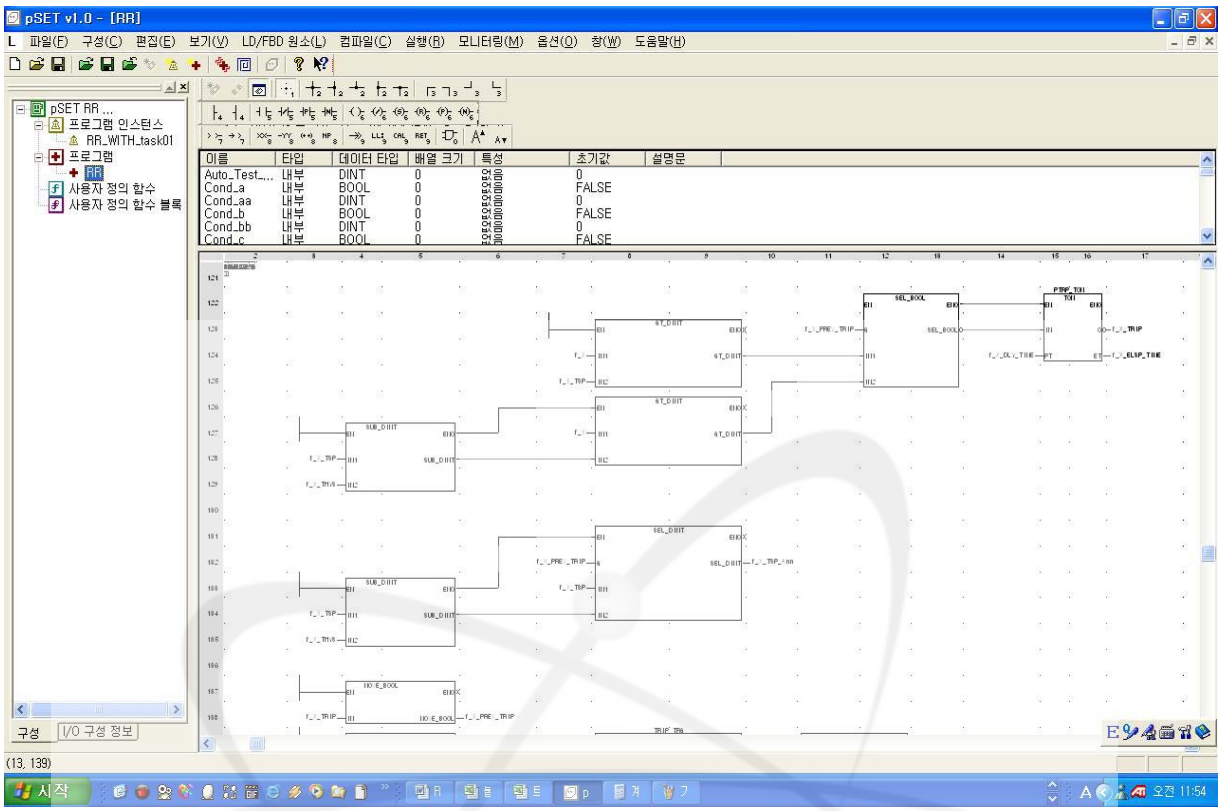


그림 3.21 비교논리 구현 예 (트립 결정 논리)

구현된 트립 논리 기능이 정상적으로 동작하는지 평가하기 위해 기능/성능시험을 수행하였다. 기능시험은 비교논리프로세서의 트립 논리가 트립 및 예비 트립 논리에 의해 트립을 제대로 수행하는지를 판단하는 것이다. 비교논리에서 기능/성능 시험은 2가지로 구분되어 수행되었다. 먼저 트립 결정 논리의 정확성 및 명확성에 대해서 시험하였다. 그림 3.21은 가변 상승형 설정치 논리에서 공정 입력값에 따라 예비트립, 트립이 정확히 수행되는지를 pSET을 이용하여 시험한 결과를 나타낸 것이다. 정상적으로 동작함을 확인하였으며 시간지연 및 SRS에서 요구하는 사항에 대해 만족함을 확인하였다. 성능시험은 가변형 설정치 비교논리에서 공정값 변화에 따른 트립 설정치 변경이 제대로 수행되는지 확인하였으며 제한된 조건내에 그 기능을 제대로 수행하는지 성능을 확인하였다. 즉 트립설정치 논리에서 요구하는 조건에 따라 트립 설정치 변경과 이를 통해 트립, 예비 트립이 원활히 수행되는지를 확인하는 시험을 수행하였다.

나. 자동시험 및 수동개시자동시험 논리 분석

비교논리프로세서와 동시논리프로세서는 주기적으로 자동시험을 수행하여야 한다. 비교논리프로세서는 고정형 설정치 비교논리에 대해서만 자동시험을 수행하도록 논리가 구성되어 있다. 반

면에 동시논리프로세서는 모든 변수에 대해 동시논리 시험을 수행하도록 구현되어 있다. 자동시험 결과는 COM을 통해 운전원 화면에 지시된다. 자동시험 논리는 비교적 시험 요건이 간단하여 시험 수행 및 논리가 명확하여 원활히 논리 분석 업무를 진행하였다.

반면에 수동개시자동시험은 운전원의 요구에 따라 시험의 시작이 되며 일정 시간이 지나면 시험은 자동적으로 해지되는 것이 자동시험과 다른 점이다. 수동개시자동시험은 케비닛운전원 모듈을 이용하여 운전원이 수동으로 시험을 요청하면 비교논리프로세서 및 동시논리프로세서에 구현되어있는 시험 논리를 시작시켜 그 결과를 자동시험 및 연계프로세서에 전송한다. 자동시험 및 연계프로세서에서는 그 결과를 케비닛운전원 모듈로 전송한다. 시험 결과를 화면에 지시하여 시험의 건전성을 운전원이 판단한다. 본 연구에서는 이러한 자동시험 및 수동개시자동시험을 수행할 수 있도록 비교논리 프로세서에 시험논리를 추가 구현하여 시험을 수행하였다. 또한 시험 기능이 원활히 수행됨을 확인하였다.

그림 3.22에는 수동개시자동시험의 시작논리를 나타내었다. 이 논리는 운전원의 수동개시자동시험 시작 요구 신호에 의해 시험이 수행되는 논리를 구현하였으며, 특히 자동비율 제한형에 대한 비교논리의 건전성을 확인하기 위해 트립설정치 계산 및 트립논리의 건전성을 동시에 시험할 수 있는 논리를 비교논리에 구현하였다. 표 3.6은 수동개시 자동시험을 수행하기 위한 Scan time별 공정값 변화에 따른 각 공정값 변화를 보여주는 시나리오이다. 이를 그래프로 나타낸 것이 그림 3.23이다. 시나리오 기반으로 수행한 시험결과를 그림 3.24에 나타내었다.

KAERI

표 3.6 수동개시 자동시험을 위한 변수정의 및 결과값

변수명	Scan1	Scan2	Scan3	Scan4	Scan5	Scan6	……	Scan180
시험주기	1	2	3	4	5	6	……	180
공정값 증가율	0	0	0	0	0	5	……	5
공정값	105	105	105	105	105	110	……	795
트립설정치	115	115	115	115	115	115	……	800
이전주기 트립설정치	110	110	110	110	110	115	……	795
최대변화율	5	5	5	5	5	5	……	5
트립/Non 트립	Non-Trip	Non-Trip	Non-Trip	Non-Trip	Non-Trip	Non-Trip	……	Non-Trip
이전주기 트립여부	Non-Trip	Non-Trip	Non-Trip	Non-Trip	Non-Trip	Non-Trip	……	Non-Trip
시험결과값 전송시점			O					

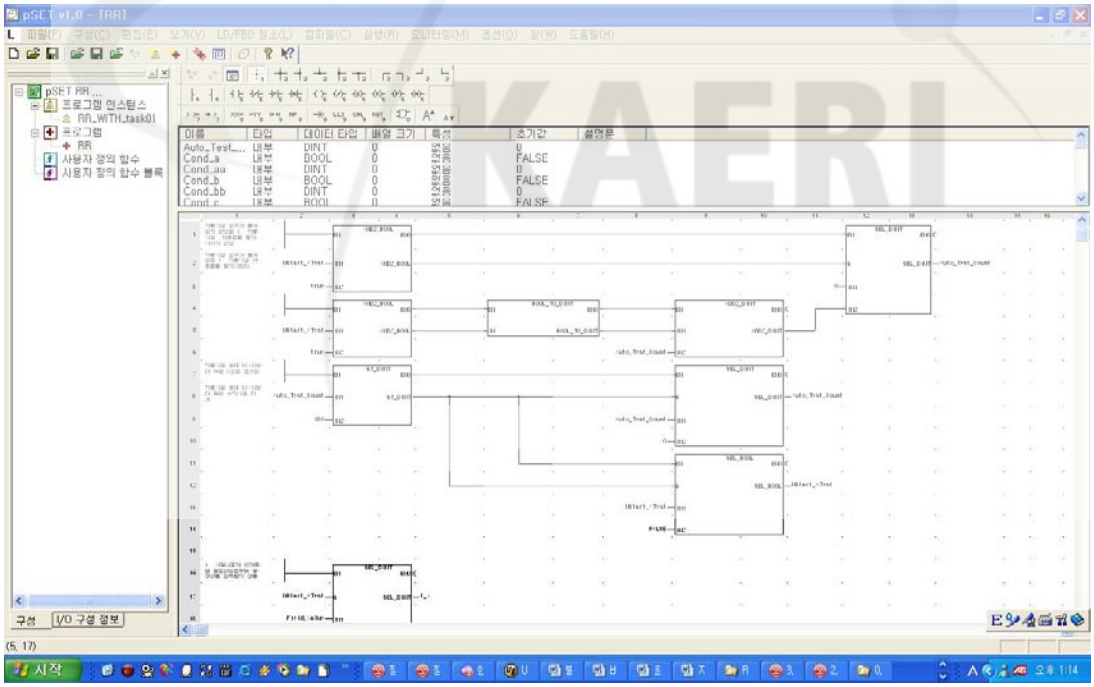


그림 3.22 수동개시 자동시험 시작논리

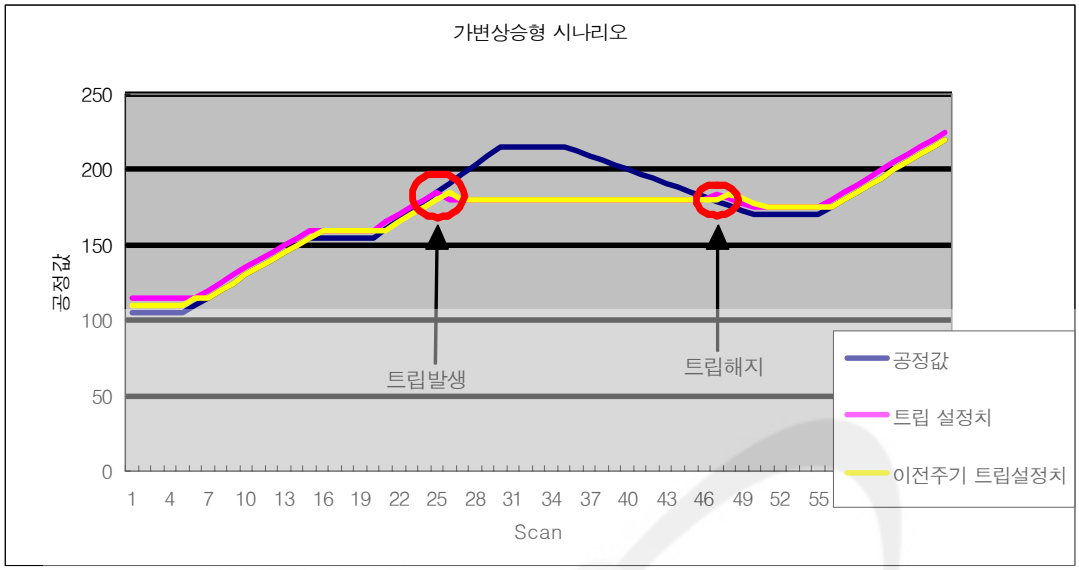


그림 3.23 수동개시 자동시험 비율제한형 시나리오

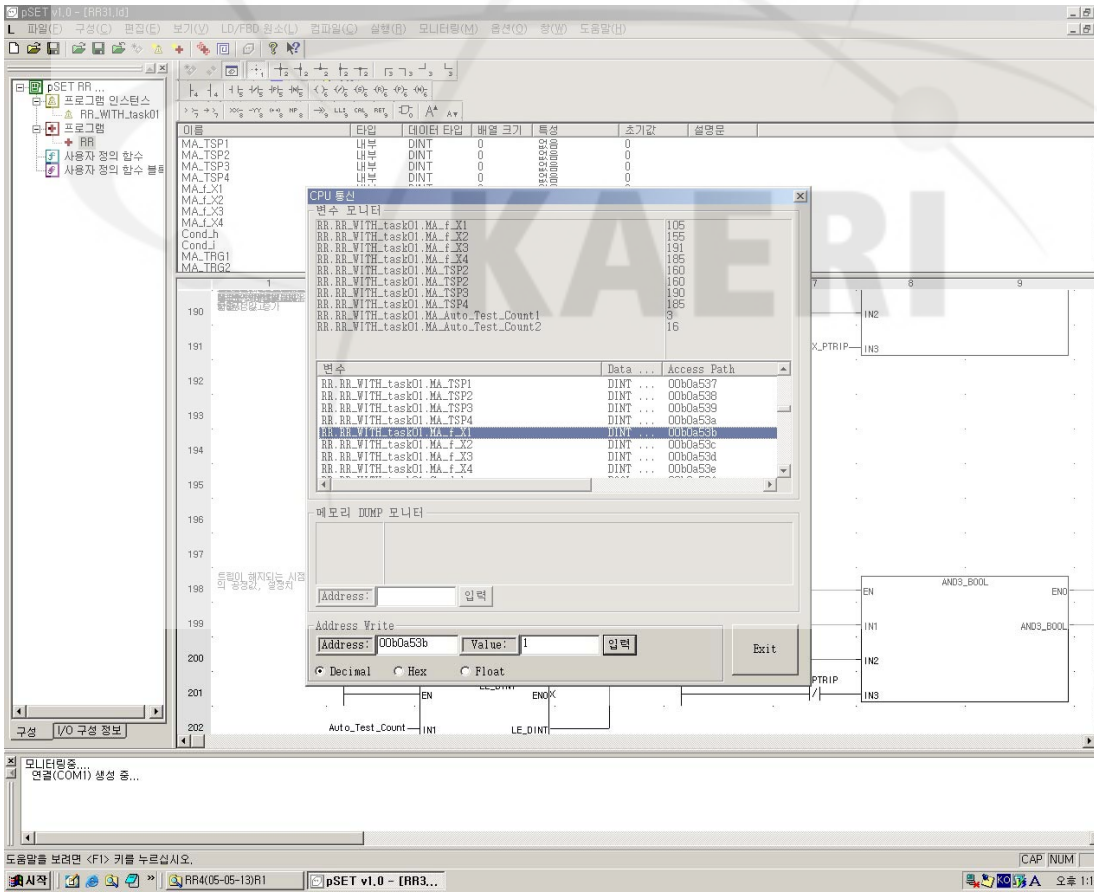


그림 3.24 가변제한형 설정치 비교논리 시뮬레이션 화면

다. 주기시험 절차서 작성 지원

본 연구를 통해 한국원자력연구소에서 작성한 원자로보호계통 주기시험 절차서 작성을 지원하였다. 원자로보호계통에서 적용되고 있는 시험 종류 및 방법은 다음과 같다. 원자로보호계통 하드웨어 기기들의 상태를 감시하는 하드웨어 진단, 원자로보호계통의 입출력 신호를 감시하는 건전성 감시 및 진단, 비교논리프로세서 및 동시논리프로세서 자체로 시행되는 자동주기시험, 자동시험 및 연계프로세서에서 시험신호를 발생하고 시험을 수행하는 수동개시자동시험, 운전원이 수동으로 수행하는 수동시험 및 응답시간시험으로 구분되어 수행된다.

본 연구를 통해 구현된 주기시험 절차는 다음과 같다.

- 건전성 감시 및 진단
- 자동주기시험
- 수동개시자동시험
- 수동시험

원자로보호계통 주기시험절차를 개발하기 위해 기존에 운영하고 있는 발전소보호계통의 주기시험에 대한 내용을 검토하였다. 이를 기반으로 현재 개발 중에 있는 원자로보호계통 주기시험 절차 방안에 대해 절차를 제시하였고 주기시험에 순서 및 방법의 적절성을 검토하였다. 주기시험 절차를 작성하기 위해 다음과 같은 업무 흐름을 통해 절차서 작성을 지원하였다.

첫째, 주기시험 절차의 정확성을 검토하였다. 제시된 주기시험이 적절하고 정확하게 수행할 수 있는지를 검토 및 수행하여 주기시험 절차의 정확성을 검토 및 보완하는 업무를 수행하였다.

둘째, 주기시험 절차를 통한 비교 논리 및 동시 논리의 보완을 수행하였다. 제시된 주기 시험을 원활히 수행하기 위해서는 시험 기능에 대한 논리가 필수적이다. 이를 위해 pSET을 이용하여 비교논리 및 동시논리 기능을 보완하였다.

셋째, 주기시험에 기반한 기능/성능 시험을 일부 수행하였다. 주기시험에 대한 종합적인 검토 후 주기시험이 요건을 만족할 수 있는지 기능/성능 시험을 수행하였다. 이를 통해 보완 사항을 도출하여 주기시험 작성 지원을 수행하였다.

주기시험은 다음과 같이 구분되어지며 본 연구를 통해 자동시험 및 연계프로세서(ATIP)에 대한 Component Test를 위한 시험절차서 및 시험보고서를 작성하였다. Component Test 는 각

ATIP 기능에 대한 상세 논리를 시험하는 것으로써 각 논리의 적절성을 평가하기 위해 가상 입력값에 대한 결과가 정확한지 일일이 모두 판단하는 과정을 수행하였다. 또한 Component Test가 완료되면 통합시험을 통해 각 프로세서(ATIP, BP, CP)가 모두 원활히 수행되는지 확인하는 시험을 수행한다. 본 보고서에서는 위탁연구로 담당한 ATIP Component Test에 대한 시험절차서 및 시험보고서 작성에 대한 간략한 내용만을 기술하였다.

ATIP Component Test 시험을 위해서는 우선 완료된 ATIP Code, PLC 1 Set, pSET이 필요하다. 시험우선 ATIP 논리에 대한 내용을 기반으로 시험절차서를 작성한다.

시험절차서는 다음에 기술한 8개 모듈을 모두 시험한다.

Module 1 : Data Update

Module 2 : Equipment Status Check

Module 3 : Operating Parameter Check

Module 4 : Testing Priority Check

Module 5 : Manual Test Check

Module 6 : Manual Initiated Automatic Test Check

Module 7 : Automatic Periodic Test Check

Module 8 : Integrity Surveillance and Diagnosis Check

시험을 위해서는 원자로보호계통 비교논리프로세서의 단위모듈시험은POSAFE-Q PLC로 구성된 자동시험 및 연계프로세서 랙 단위로 수행된다. 자동시험 및 연계프로세서에는 운용소프트웨어가 탑재되어서 작동되어야 한다.

자동시험 및 연계프로세서의 단위모듈시험에는 그림 3.25와 같이 pSET을 구동하기 위한 PC, 비교논리프로세서 응용소프트웨어 실행코드가 탑재된 POSAFE-Q PLC, 신호입력을 위한 신호입력기 등이 필요하다.

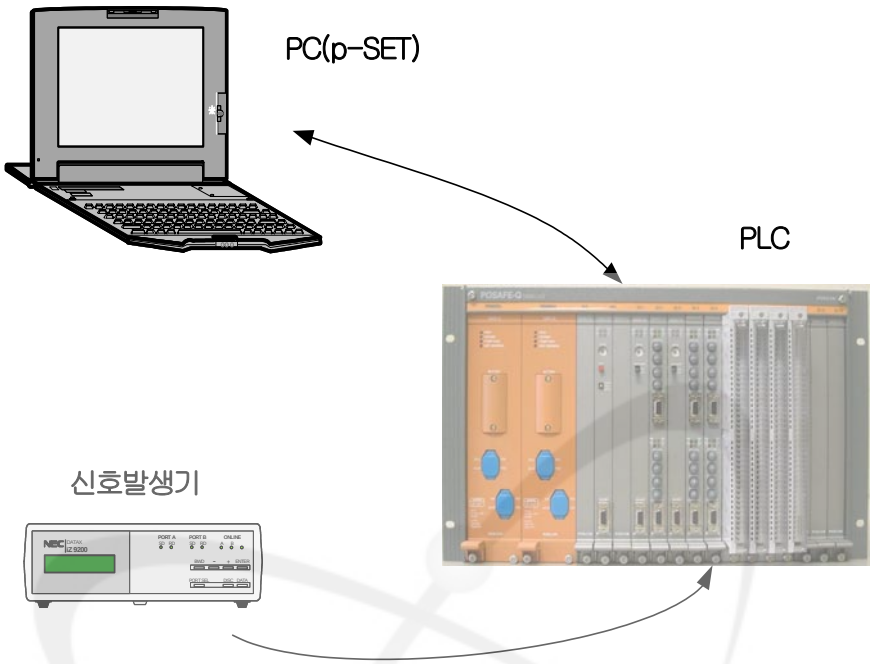


그림 3.25 자동시험 및 연계프로세서 단위모듈시험 장치구성도

자동시험 및 연계프로세서의 단위모듈시험을 하기 위한 장치사양 및 연결사항은 다음과 같다.

- PC
- PLC
- 신호발생기
- PC와 PLC를 연결하기 위한 RS-232C 케이블이 있어야 한다.
- 신호발생기와 PLC를 연결하기 위한 하드와이어 선이 있어야 한다.

다음은 자동시험 및 연계프로세서를 시험하기 위한 소프트웨어 준비사항을 기술한 것이다. 즉, 자동시험 및 연계프로세서 응용소프트웨어 단위모듈시험을 수행하기 위해서 먼저 다음과 같은 하드웨어 및 소프트웨어 준비사항을 점검해야 한다.

- PLC는 정상적으로 작동하며 각종 입출력 카드는 정상적으로 작동하여야 한다.
- 시험을 위해 PLC와 연계된 PC는 운영체제가 오류, 바이러스에 감염되어 있지 않아야 한다.
- 시험을 위해 설치된 PC는 엔지니어링 도구가 설치되어 있어야 한다.
- PLC와 PC는 RS232통신을 이용한 통신 포트가 정상적으로 작동하여야 하며 정상적으로 연결되어야 한다.
- PC에 설치되어 있는 엔지니어링 도구는 컴파일 및 PLC의 상태를 정상적으로 모니터링 할 수 있어야 한다.

위와 같은 조건을 만족할 때 다음과 같은 사항을 점검하고 그 결과를 괄호안에 “O”, “X”를 기입한다. 만족한 경우에는 “O”를 그렇지 않은 경우에는 “X”를 기입한다.

OS : Windows XP Professional 인지 확인한다.

( )

엔지니어링 툴 : pSET 인지 확인한다.

( )

시험을 위해 준비된 PC에서 pSET을 기동한다.

( )

시험 프로그램 포함된 프로젝트 파일을 열고 컴파일 하여 목적 코드를 생성한다.

( )

PLC 프로그램에서 RS232 통신 포트를 확인하여 PC와 PLC가 서로 통신하고 있는지 확인한다.

( )

통신에 이상이 없는 경우에는, 생성한 목적 코드를 PLC에 다운로드 한다.

( )

PLC에 다운로드 한 다음 코드를 실행시킨다.

( )

PLC의 각종 LED와 입출력 카드가 정상적으로 작동하고 있음을 확인한다.

( )

소프트웨어 및 하드웨어 준비 사항이 완료되면 하드웨어 동작 사항을 미리 점검하고 이를 이용하여 가상 입력값을 pSET, 신호 발생기를 이용하여 신호입력단자에 입력시켜 시험을 수행한다.

표 3.7은 단위모듈 시험은 하드와이어로 입력되는 디지털 입력모듈에 대한 메모리 점검시험을 수행한다. 다만, SDL을 통해 입력되는 통신신호는 원자로보호계통 통합시험에서 수행한다.

디지털 입력 모듈은 코드에 의해서 입력되는 부분이 아니며, PM모듈과 COMM-PM (ICN/ICDN/SDL) 및 입출력모듈(DI, DO, AO) 사이에 전달되는 데이터의 주기와 우선도를 정의하는 프로그램에 의해 설정된다. 표 3.7에 나타낸 바와 같이 DI 입력 모듈의 입력 주소의 값을 기입하여 정확한지 점검한다.

KAERI

표 3.7 D/I 하드웨어주소 점검표

프로세서	입력모듈	채널	변수명	메모리
ATIP	DI1	1	ATIP_DI_DI1CH1	
		2	ATIP_DI_DI1CH2	
		3	ATIP_DI_DI1CH3	
		4	ATIP_DI_DI1CH4	
		5	ATIP_DI_DI1CH5	
		6	ATIP_DI_DI1CH6	
		7	ATIP_DI_DI1CH7	
		8	ATIP_DI_DI1CH8	
		9	ATIP_DI_DI1CH9	
		10	ATIP_DI_DI1CH10	
		11	ATIP_DI_DI1CH11	
		12	ATIP_DI_DI1CH12	
		13	ATIP_DI_DI1CH13	
		14	ATIP_DI_DI1CH14	
		15	ATIP_DI_DI1CH15	
		16	ATIP_DI_DI1CH16	
		17	ATIP_DI_DI1CH17	
		18	ATIP_DI_DI1CH18	
		19	ATIP_DI_DI1CH19	
		20	ATIP_DI_DI1CH20	
		21	ATIP_DI_DI1CH21	
		22	ATIP_DI_DI1CH22	
		23	ATIP_DI_DI1CH23	
		24	ATIP_DI_DI1CH24	
		25	ATIP_DI_DI1CH25	
		26	ATIP_DI_DI1CH26	
		27	ATIP_DI_DI1CH27	
		28	ATIP_DI_DI1CH28	
		29	ATIP_DI_DI1CH29	
		30	ATIP_DI_DI1CH30	
		31	ATIP_DI_DI1CH31	
		32	ATIP_DI_DI1CH32	

기기 상태 점검은 건전성 감시 및 진단 프로세서가 제대로 동작하기 위해 반드시 확인해야 하는 각종 하드웨어 및 박동신호 생성 논리를 포함하고 있다. 이 모듈의 단위모듈시험은 다음과 같은 사항을 점검한다.

- ATIP PLC Status
- BP1 PLC Status
- BP2 PLC Status
- CP1 PLC Status
- CP2 PLC Status
- Cabinet Status
- COM Status
- Channel Status
- Intra-Channel ATIP Heartbeat Status
- ETIP Heartbeat Status

이중에서 기기 상태 점검에서 가장 많이 사용되고 있는 박동신호와 관련된 점검절차 (ATIP PLC Status)에 대해서 설명하도록 하겠다.

우선 PLC는 1주기(Scan Time)이 50msec이므로 사람의 눈으로 동작을 제대로 확인할 수 있는 방법이 불가능하다. 따라서 이런 경우, 시험을 위해서 주기를 1초 정도로 늘려서 시험을 수행하게 된다. 이런 경우 정확한 시험 수행이 이루어졌는지를 파악할 수 있다. 또한 시험주기 연장으로 문제가 되는 부분에 있어서는 시험을 위한 프로그램을 구성하여 시험이 제대로 동작하는지를 파악해야 한다. 또한 본 시험을 위해 각 단계를 정하여 시험을 순차적으로 수행하고 다시 원래 상태로 복귀시키거나, 시험을 위한 프로그램을 삭제하는 방식으로 시험을 수행하였다.

자동시험 및 연계프로세서의 PLC의 상태를 점검하기 위해서 p_SET에서 박동신호 생성값과 결과값이 박동신호 최소값과 최소값 사이에 존재하는지 점검한다. 박동신호는 각 프로세서별로 그 범위값이 다르기 때문에 각 프로세서별로 박동신호 범위 내에 존재하는지 확인은 매우 간단

하다.

아래 표는 채널A ATIP의 박동신호가 5000 ~ 5999 범위 내에 존재하는지 우선 점검하는 항목이다. 시험결과가 5000 ~ 5999 사이에 존재하는 경우, 그 중 하나의 값을 시험결과에 입력하고 통과여부에 “O”를 입력하면 된다.

마지막으로 박동신호의 최대값 “5999”가 되면 다시 최소값 “5000”으로 값이 초기화(Reset)되는지를 점검해야 한다. 해당 프로세서는 고유한 박동신호 범위를 갖게 되므로 이 범위를 초과하거나 증가가 발생하지 않을 경우에는 프로세서 오류이기 때문이다. 이에 대한 점검표를 표 3.8 표 3.9에 나타내었다.

단계 1: ATIP 실행주기를 1초로 변경한다. (O)

단계2 :

표 3.8 박동신호 생성값 점검

변수	설명	기대값	시험결과	통과여부
CHA_ATIP_IAV_HB	A채널 ATIP 박동신호 생성값	5000 ~ 5999	5555	O
CHA_ATIP_AO_HB	A채널 ATIP 박동신호 결과값	5000 ~ 5999	5560	O

단계3 :

박동신호 생성값이 최대값보다 커지면 다시 최소값으로 초기화되는지 확인한다.

표 3.9 박동신호 생성 리셋 점검

변수	설명	기대값	시험결과	통과여부
CHA_ATIP_IAV_HB	A채널 ATIP 박동신호 생성값	5000	5000	O
CHA_ATIP_AO_HB	A채널 ATIP 박동신호 결과값	5000	5000	O

다음은 건전성 감시 및 진단 설정치 운전우회 리셋 설정치의 채널간 비교 논리를 시험하는 항목이다. 각 채널별 운전우회 리셋 설정치 중 1개라도 다른 경우 오류를 발생시키는 논리가 정확한지 검사하는 부분이다. 검사자는 시험하고자 하는 채널 중 1개의 값을 다른 채널과 다른값을 입력하여 오류 검출 논리가 정확한지 시험한다. 오류 검출 논리는 모든 채널의 설정치가 동일하지 않은 경우에 대해서는 이를 오류신호를 발생시키도록 한다.

아래 표는 각 채널의 설정치에 대해 다른 값을 입력한 경우, 건전성 감시 및 진단에서 확인하는 논리를 나타내었다. 건전성 감시 및 진단에 대한 점검표를 표 3.10에 나타내었다.

표 3.10 건전성감시 및 진단 점검

변수	설명	입력값	결과값	통과여부
IV_DL_CHAITST	채널 A 건전성 감시 및 진단 시작	1 1	N/A	N/A
BP1_AI_P06SOBR	BP1 P06 설정치 운전우회 리셋	16.67 15.67	N/A	N/A
CHB_AI_BP1P06SOBR	채널 B BP1 P06 설정치 운전우회 리셋	16.67 16.67	N/A	N/A
CHC_AI_BP1P06SOBR	채널 C BP1 P06 설정치 운전우회 리셋	16.67 16.67	N/A	N/A
CHD_AI_BP1P06SOBR	채널 D BP1 P06 설정치 운전우회 리셋	16.67 16.67	N/A	N/A
COM_DO_BP1P06SOBRR_E	BP1 P06 설정치 운전우회 리셋 비교 오류	N/A	0 1	O

다음은 자동주기 시험에 대한 “자동주기시험 수행주기 오류” 판단에 대한 논리를 점검하는 절차이다. 자동주기 시험 정지 요구신호가 입력되었을 경우, 수동시험 상태인 경우(“3”)이면 수동시험 정지요구 오류 카운트가 증가하여 “290000”에 도달하면 수동시험 정지오류 신호가 발생하게 된다. 즉, 수동시험 정지요구에 대한 응답이 수행되지 않음을 의미하게 된다. 이러한 일련의 판단 논리가 적절한지 점검한다. 수동시험 오류 판단 점검에 관련된 점검표를 표 3.11에 나타내었다.

표 3.11 수동시험 오류 판단 점검

변수	설명	입력값	결과값	통과여부
IV_DG_CHAPTP	COM 수동시험 정지 요구신호	1 1	N/A	N/A

		0		
IV_AG_CHATS	채널 A 수동시험 상태 값	3 2 0	N/A	N/A
IV_AL_PTSTEC	채널 A 수동시험 정지요구 오류 카운트	N/A	290000 0 0	O
COM_DO_CHAPTST_E	수동시험 정지오류 신호	N/A	1 0 0	O

다음은 각 프로세서별 시험 형태에 따른 입력값에 따라 자동주기시험이 시작되는지를 판단하는 논리이다. 자동주기시험은 다른 시험이 모두 정지되었을 경우, 시작되는 시험으로 다른 시험 타입의 값이 모두 “0” 인 경우 시험을 시작하게 된다. 또한 그 이전에 시험주기를 판단하는 논리도 포함되어 있다. 자동시험주기에 대한 점검논리를 표 3.12에 나타내었다.

KAERI

표 3.12 자동시험주기 점검

변수	설명	입력값	결과값	통과여부
BP2_AI_TT	BP1 시험 타입	0 1 2 3 0	N/A	N/A
BP2_AI_TT	BP1 시험 타입	1 2 3 0 0	N/A	N/A
CP1_AI_TT	CP1 시험 타입	2 3 0 1 0	N/A	N/A
CP2_AI_TT	CP2 시험 타입	3 0 1 2 0	N/A	N/A
IV_DG_PTST	채널 A 자동주기시험 시작	N/A	1 1 1 1 0	O

3. 정형 명세서 작성

가. RPS 개발 지원

(1) RPS 계통설계문서 및 소프트웨어 기능요건 개정 지원

당해연도에는 원자로보호계통 자동주기시험 및 다양한 시험에 필요한 요건을 충족시키기 위해 시험요건 충족 여부를 점검한 결과 보완 사항을 도출하여 그림 3.26과 같은 보완사항을 도출하여 소프트웨어 기능요건 개정을 지원하였다.

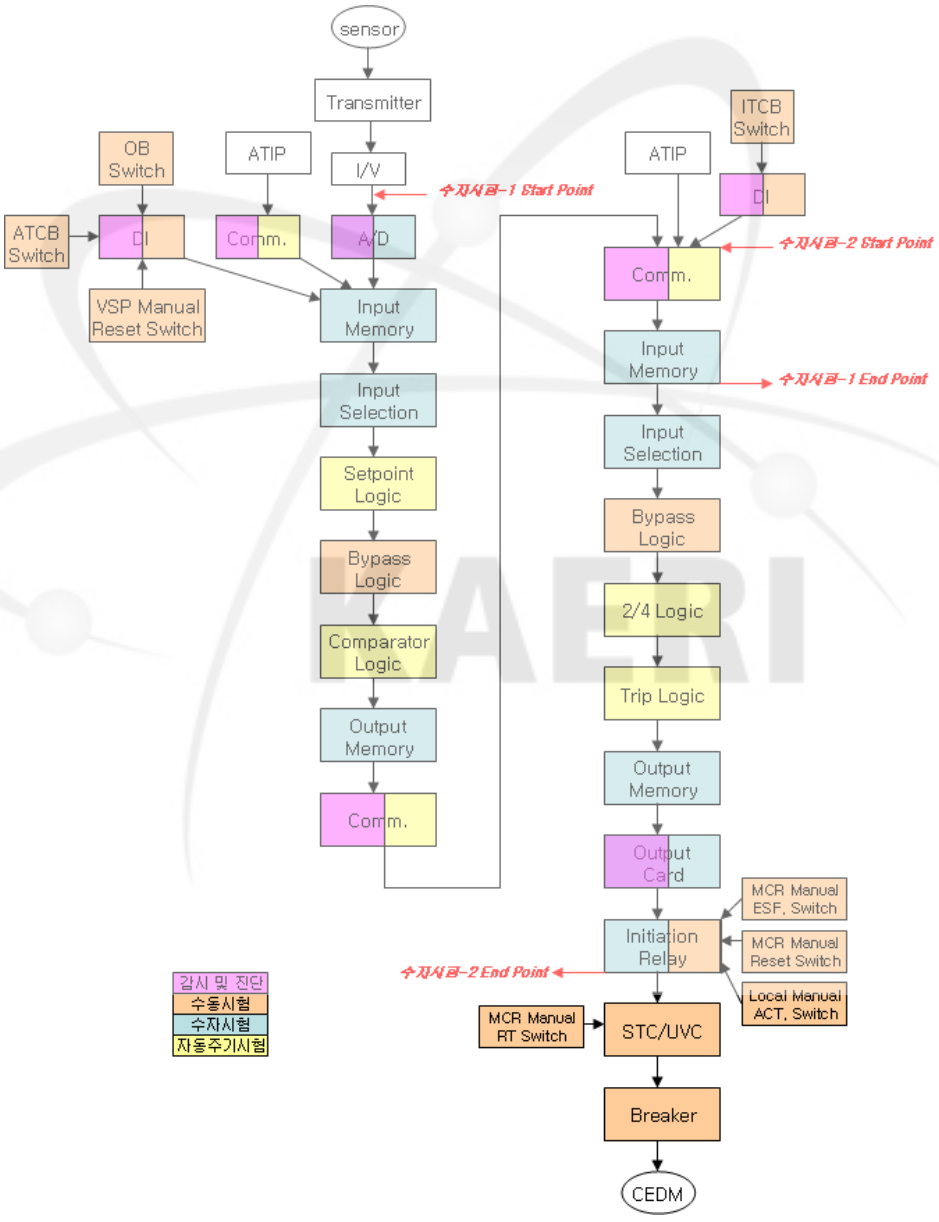


그림 3.26 RPS 시험기능요건 검토 및 개정안

(2) RPS 계통설계문서 및 소프트웨어 연계요건서 개정 지원

소프트웨어 기능요건서 개정 및 구현 사항이 구체화됨에 따라 연계요건서 개정업무를 수행하였다. 아래 그림 3.27과 같이 원자로보호계통을 구성하기 위해 다양한 프로세서 모듈의 필요 여부가 확정되었다. 이러한 모듈 간 연계의 확정 및 필요에 따라 소프트웨어 연계요건서의 보완 및 수정업무가 필요하게 되었으며 이와 관련한 업무를 수행하였다.

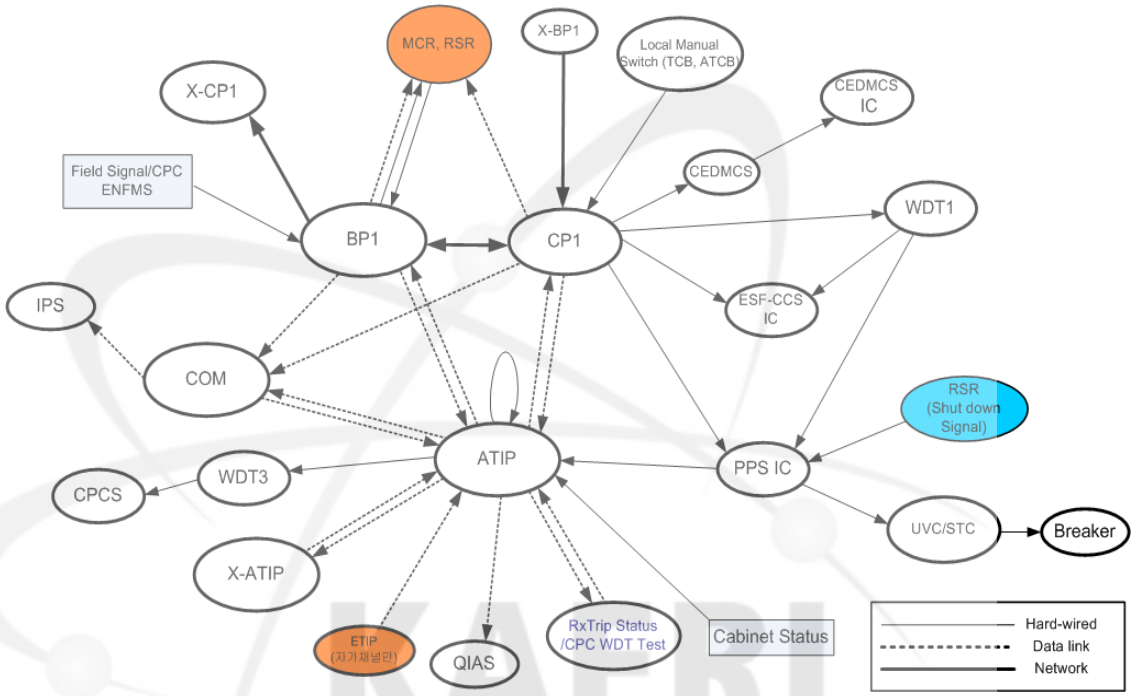


그림 3.27 모듈 간 연계도

(3) RPS 소프트웨어 정형 명세서 개정 지원

소프트웨어 기능요건서의 개정에 따라 자동시험 및 연계프로세서, 비교논리프로세서, 동시논리프로세서의 소프트웨어 자연어 명세서의 개정이 필요하게 되어 두산중공업에서 개정업무를 수행하게 되었다. 자연어 명세서의 개정에 따라 정형 명세서 개정도 수행하였다. 정형 명세서 개정은 역으로 자연어 명세서의 보완 사항을 도출하였고 이에 따른 정형명세서와 자연어 명세서의 상호 보완 사항을 도출하였다.

(가) 비교논리프로세서 정형명세

그림 3.28은 비교논리프로세서 정형명세를 기술한 상위 노드를 표현 한 것이다. 이는 비교논리프로세서를 구성하기 위한 각종 모듈을 비교논리프로세서 요구사항명세서를 기준으로 작성한 것이다. 이에 대한 모듈의 기능의 개략적 설명은 표 3.13과 같다. 비교논리프로세서 정형명세는 입력변수 34개, 출력변수 45개로 기술되었다.

표 3.13 비교논리프로세서 구성모듈

순번	모듈명	모듈 설명	비고
1	g_EquipSelfDiagMdl	자가진단 모듈	
2	g_BypassChkMdl	우회 진단 모듈	
3	g_Test_Module	시험모듈	
4	G_HB_Module	박동신호 모듈	

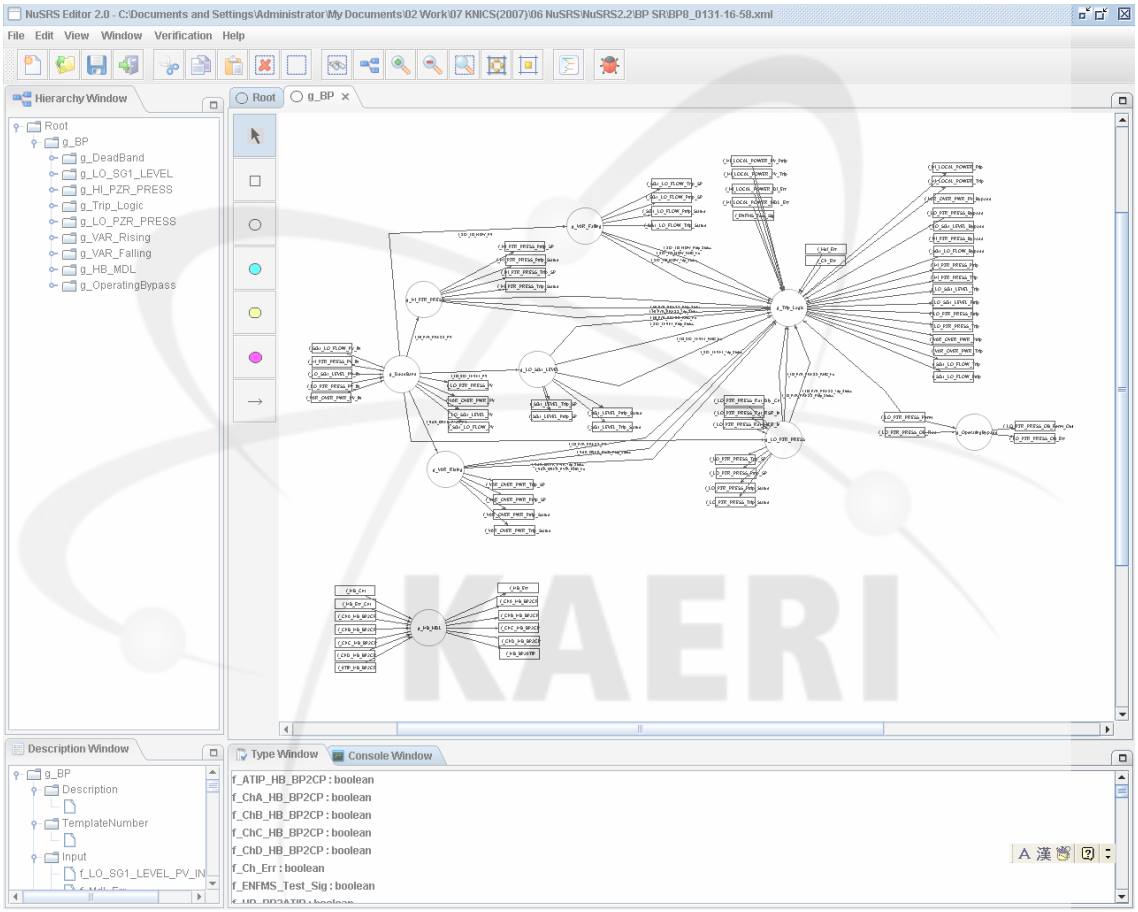


그림 3.28 비교논리프로세서 정형명세서 전체 구성 모듈

(나) 동시논리프로세서 정형명세

그림 3.29는 동시논리프로세서 정형명세를 기술한 상위 노드를 표현 한 것이다. 이는 동시논리프로세서를 구성하기 위한 각종 모듈을 동시논리프로세서 요구사항명세서를 기준으로 작성한 것이다. 이에 대한 모듈의 기능의 개략적 설명은 표 3.14와 같다.

동시논리프로세서는 입력변수 75개, 출력변수 35개로 기술되었다.

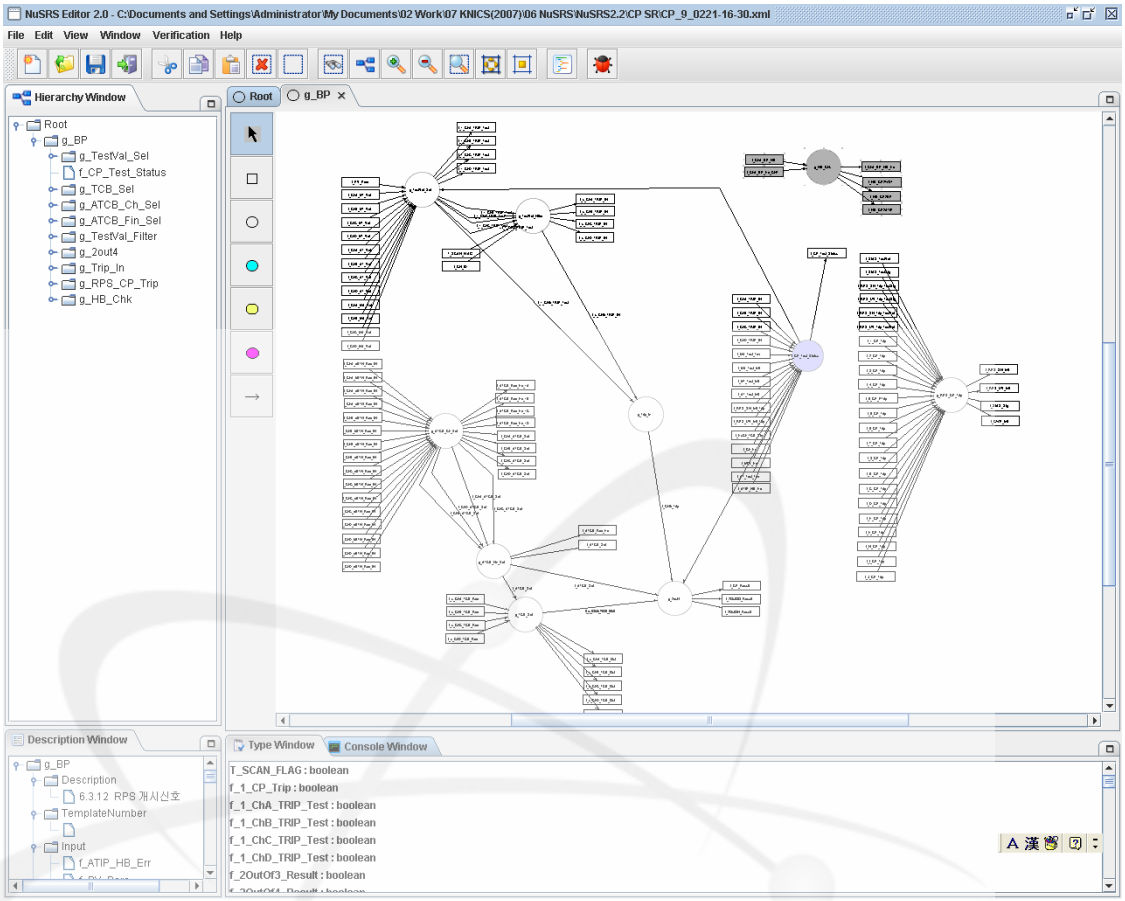


그림 3.29 동시논리프로세서 정형명세서 전체 구성 모듈

표 3.14 동시논리프로세서 구성모듈

순번	모듈명	모듈 설명	비고
1	g_Test_Val_Sel	시험값 선택모듈	
2	g_ TCB_Sel	트립채널 우회 선택 모듈	
3	g_ATCB_Sel	전채널 우회 선택 모듈	
4	g_ATCB_Fin_Sel	전채널 우회 최종 선택 모듈	
5	g_TestVal_Filter	시험값 최종 필터링 모듈	
6	g_2OutOf4	동시논리 모듈	
7	g_Trip_In	트립값 입력 모듈	
8	g_RPS_CP_Trip	동시논리 최종 트립 논리 모듈	
9	g_HB_Chk	박동신호 모듈	

(다) 자동시험 및 연계프로세서 정형명세

그림 3.30은 자동시험 및 연계프로세서 정형명세를 기술한 상위 노드를 표현 한 것이다. 이는 자동시험 및 연계프로세서를 구성하기 위한 각종 모듈을 자동시험 및 연계프로세서 요구사항명세서를 기준으로 작성한 것이다. 이에 대한 모듈의 기능의 개략적 설명은 표 3.15와 같다. 자동시험 및 연계프로세서는 입력변수 186개, 출력변수 132개로 기술되었다.

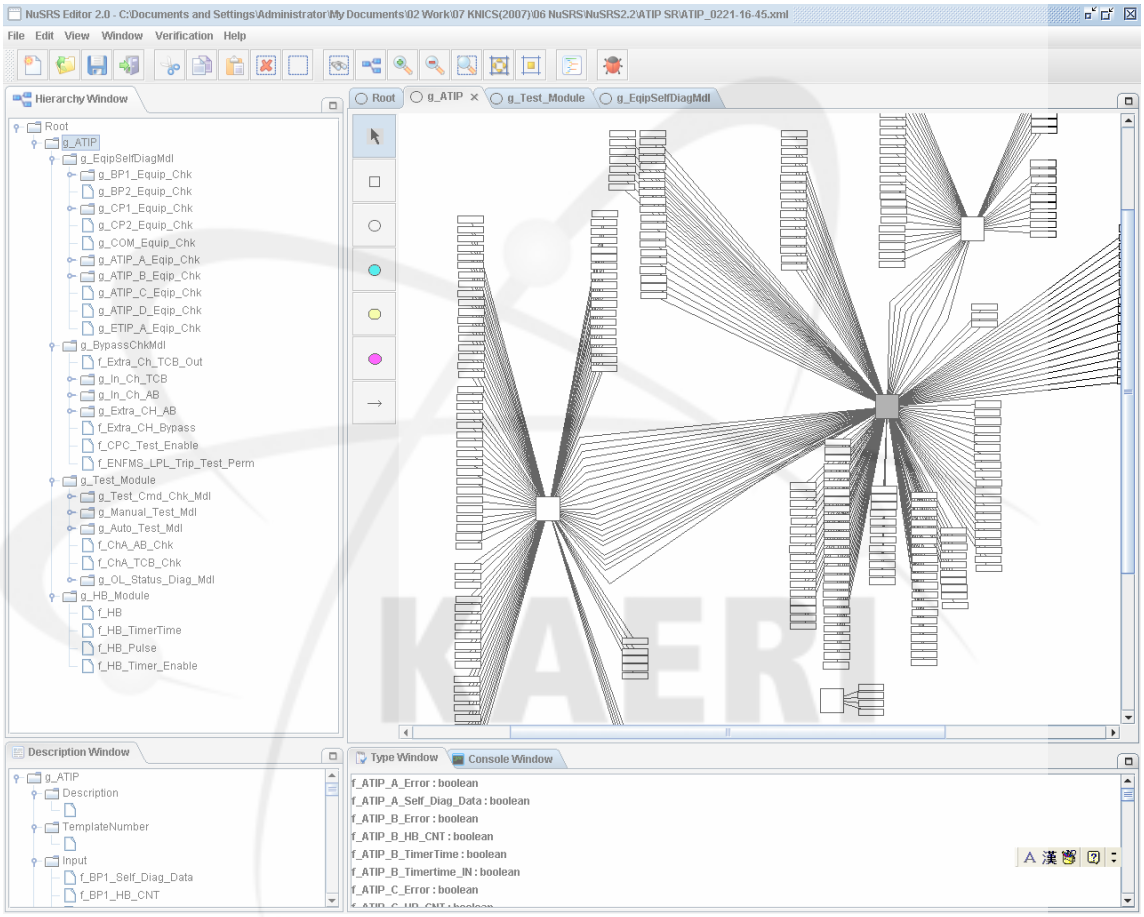


그림 3.30 동시논리프로세서 정형명세서 전체 구성 모듈

표 3.15 자동시험 및 연계프로세서 구성모듈

순번	모듈명	모듈 설명	비고
1	g_EquipSelfDiagMdl	자가진단 모듈	
2	g_BypassChkMdl	우회 진단 모듈	
3	g_Test_Module	시험모듈	
4	g_HB_Module	박동신호 모듈	

제 4 절 개발 결과

본 연구의 결과로서 안전등급제어기기 PLC인 POSAFE-Q의 프로세서 모듈이 고신뢰도화된 소프트웨어를 기반으로 개발되었으며, 관련 설계 문서들이 생산되었다. 표 3.16이 POSAFE-Q 프로세서 모듈 소프트웨어 관련 결과물들을 보여준다. 또한 KNICS RPS가 구조적으로 검증된 설계를 가지게 되었으며, 이를 반영한 설계문서들이 생산되었다. 표 3.17는 RPS 구조검증 관련 결과물들을 보여준다.

KAERI

1. 안전등급 PLC 프로세서 모듈 S/W 고신뢰도화 개발 연차별 목표에 따른 성과 및 만족도

표 3.16 안전등급 PLC 프로세서 모듈 S/W 고신뢰도화 개발
연차별 목표에 따른 성과 및 만족도

년도	년차별 목표	대비 성과물	만족여부
2005	• 안전등급제어기기 (PLC) 프로세서 모듈 RTOS 고신뢰도화 개발 (SRS/SDS)	• 안전등급제어기기 (PLC) 프로세서 모듈 RTOS SRS • 안전등급제어기기 (PLC) 프로세서 모듈 RTOS SDS	만족
2006	• 안전등급제어기기 (PLC) 프로세서 모듈 RTOS 고신뢰도화 개발 (CT/IT)	• 안전등급제어기기 (PLC) 프로세서 모듈 RTOS CT 계획서/절차서/보고서 • 안전등급제어기기 (PLC) 프로세서 모듈 RTOS IT 계획서/절차서/보고서	만족
2007	• 안전등급제어기기 (PLC) 프로세서 모듈 PLD 고신뢰도화 개발 및 PLC 특정주제기술보고서(TR) 작성 지원	• 안전등급제어기기 (PLC) 프로세서 모듈 PLD SRS/SDS • 안전등급제어기기 (PLC) 프로세서 모듈 PLD CT/IT • PLC 특정주제기술보고서(TR)	만족
2008	• 안전등급제어기기 (PLC) 이중화 모듈(HED) 고신뢰도화 개발 및 PLC 특정주제기술보고서(TR) 개정 지원	• 안전등급제어기기 (PLC) 프로세서 모듈 HED SRS/SDS • PLC 특정주제기술보고서(TR) 개정본	만족

2. RPS 구조 검증 연차별 목표에 따른 성과 및 만족도

표 3.17 RPS 구조 검증 연차별 목표에 따른 성과 및 만족도

년도	년차별 목표	대비 성과물	만족여부
2005	• RPS 구조검증 및 계통설계문서 작성 지원	• 기능요건서 및 연계 요건서	만족
2006	• RPS 계통설계문서 및 소프트웨어 기능요건 개정 지원 • RPS 계통설계문서 및 소프트웨어 연계요건서 개정 지원	• 기능요건서 및 연계 요건서 개정본	만족
2007	• RPS 계통설계문서 및 소프트웨어 요구사항 정형명세서 개정 지원 • RPS 기능/성능시험 계획서/통합시험 문서 개정 지원	• 정형명세서 개정본 • 기능/성능 시험문서	만족
2008	• RPS 계통설계문서 및 소프트웨어 기능요건 개정 지원 • RPS 계통설계문서 및 소프트웨어 연계요건서 개정 지원 • RPS 계통설계문서 및 소프트웨어 요구사항 명세서 개정 지원 • RPS 계통설계문서 및 소프트웨어 설계 명세서 개정 지원 • RPS 기능/성능시험 계획서/통합시험 문서 개정 지원	• 정형명세 개정문서 • 설계 명세서 개정 지원 문서 • 기능/성능 시험 문서	만족

제 4 장 연구개발 목표 달성도 및 대외 기여도

제 1 절 연구개발 목표 달성도

안전등급제어기기(PLC) RTOS 고신뢰도화 및 RPS 구조 검증 과제의 최종 목표는 안전계통 중 특히 안전등급 PLC인 POSAFE-Q의 프로세서 모듈 소프트웨어의 고신뢰도화 개발 및 RPS 구조 검증을 통한 계통 및 소프트웨어 설계 지원이다. 이를 위해서 본 연구에서는 POSAFE-Q 및 RPS 개발자에게 안전-필수 소프트웨어 개발 시 필요한 소프트웨어 요구사항 명세서 및 소프트웨어 설계 명세서 작성, 컴포넌트 시험 및 통합 시험 수행을 직접 지원하며, RTOS 고신뢰도화 및 RPS 구조 검증에 필요한 핵심 기술을 지원하였다. 이러한 지원 노력은 고신뢰도화 된 소프트웨어를 탑재한 POSAFE-Q 프로세서 모듈로 결실을 맺었으며, KNICS 만의 독특한 설계를 가지며 안전성 및 신뢰성이 향상된 RPS 설계로 결실을 맺었다. 따라서, 본 연구개발의 목표는 100% 달성된 것으로 평가된다.

제 2 절 대외 기여도

고신뢰도화 된 소프트웨어를 탑재한 POSAFE-Q 프로세서 모듈은 POSAFE-Q의 안전하고 신뢰성 있는 운전을 보장할 것이며, 이는 KNICS 안전계통의 플랫폼에 대한 신뢰로 연결되어 신울진 1,2호기 등 신규 건설 원전은 물론 가동 원전 계측제어계통 교체에도 적용될 가능성을 높여줄 것이다. 여기에 KNICS만의 독특한 설계를 가지며 안전성 및 신뢰성이 향상된 RPS 설계가 수반되어야 함을 물론이다.

한편, 본 연구의 결과물들이 원전 건설 프로젝트에 활용될 경우, 국내 원전 계측제어 기술에 대한 대외 신인도 향상이 예측되며, 따라서 원전 계측제어 기술의 수출도 기대할 수 있을 것이다.

제 5 장 연구개발결과의 활용계획

제 1 절 경제·산업적 측면

무엇보다도 원전 계측제어사업단이 발족되어 원전 계측제어 기술 국산화의 초석을 다지게 되었다는 점이 경제 및 산업적 측면에서의 가장 큰 의의이다. 한편, 본 과제에서 개발한 안전등급제어기기 실시간 운영체제 소프트웨어 기술 및 원자로보호계통 설계 고도화 기술은 원전 계측제어 기술 국산화의 중심 기술에 해당한다. 특히, 원전용 안전등급제어기기의 국산화 개발 자체가 최초로 시도되고 있는 상황에서 제어기기의 핵심 소프트웨어인 실시간 운영체제 개발을 순수 국내 소프트웨어 기술로 수행하면서 원전 규격에 맞는 인허가를 획득한다는 것은 타 시스템 실시간 운영체제 기술 분야에도 큰 파급효과를 가져올 것으로 기대된다.

발전소보호계통 및 플랫폼 국산화 개발은 직접적으로 보호계통 설계, 시험 등에 소요되는 자원을 줄일 수 있어서 발전단가 절감으로 이어질 수 있다. 또한 현재 전 세계적으로 확인 및 검증 도구의 확립이 제대로 이루어져 있지 않은 상태이고, 검증 체계마저 미흡한 상태에 있는 상황에서 국내 기술력을 통한 확인 및 검증 체계의 확립은 그 자체로도 경제적, 산업적으로 큰 파급효과를 거둘 수 있을 것이다. 또한, 원자력발전소 필수안전계통의 소프트웨어를 개발함에 있어서 국내 기술만을 이용할 수 있게 되면, 원전 이용률의 향상을 기대할 수 있고, 또한 외국의 소프트웨어에 전적으로 의존하고 있는 안전 소프트웨어 개발을 순수 국내의 기술력을 이용하여 국산화함으로써 수입대체효과를 거둘 수 있다. 이러한 측면에서 본 연구 결과는 커다란 경제적 가치가 있다고 사료된다. 아울러 본 연구를 통해 안전이 중요한 계통을 위한 소프트웨어 개발 산업의 필요성에 대한 인식이 산업계에 확산될 수도 있으며 벤처기업 창업 등을 통한 경제 및 산업적 측면의 효과도 기대할 수 있을 것이다.

제 2 절 활용방안

본 연구를 통해 개발된 RTOS, PLD, 이중화 모듈 고신뢰도화 기술은 원전 계측제어 계통 및 플랫폼 국산화 연구의 유용한 입력으로 활용될 수 있다. 또한, 확인 및 검증이 인허가 확보에 매우 중요하다는 관점에서, 본 연구를 통해 개발된 기술은 안전이 중요한 원자력발전소 계측제어 계통에 소프트웨어 기반 설비를 적용하고자 할 때, 소프트웨어 개발 공정의 추적 가능성, 완전성 및 일관성 분석과 여러 가지 종류의 시험 등의 확인 및 검증 작업을 효과적으로 수행할 수 있도록 지원함으로써 설비의 안전성 및 신뢰성 향상에 많은 도움을 줄 수 있을 것으로 기대된다. 한편, 이는 가동원전 뿐만 아니라 차후 건설될 원전 계측제어계통에 적용될 소프트웨어 기반 설비에 대한 확인 및 검증 기술을 확립하고 인허가성을 제고하는데 활용할 수 있다.

제 6 장 연구개발과정에서 수집한 해외과학기술정보

- 해당사항 없음.

제 7 장 참고문헌

본 문서에서 언급되는 설계사항은 아래의 문서들을 참고하였다. 참고문서들로부터 필요한 부분만 인용되었으며, 별도의 기술이 없는 경우 최근의 개정본이 적용된다.

제 1 절 적용법규

1. 10CFR 50 Appendix April, 1994, “General Design Criteria”
2. 10CFR 50 Appendix B,4/94, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants”
3. 10CFR 50.55a(h), “Code and Standards - Protection and Safety systems”
4. USNRC Reg. Guide 1.118, Rev. 03, Apr. 1995, “Periodic Testing of Electric Power and Protec-tion Systems”.
5. USNRC Reg. Guide 1.152, Rev. 01, Jan. 1996, “Criteria for Programmable Digital Computers System Software in Safety Related Systems of Nuclear Power Plants”
6. USNRC Reg. Guide 1.152, Rev. 02, Jan. 2006, “Criteria for Programmable Digital Coputers System Software in Safety in Safety Related Systems of Nuclear Power Plants”.
7. USNRC Reg. Guide 1.168, Rev. 00, Jul. 1997, “Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems Of Nuclear Power Plants”.
8. USNRC Reg. Guide 1.169, Rev. 00, Jul. 1997, “Configuration Management Plans for Digital Computer Software Used in Systems of Nuclear Power Plants”.
9. USNRC Reg. Guide 1.170, Rev. 00, Jul. 1997, “Software Test Documentation for Digital Com-puter Software Used in Systems of Nuclear Power Plants”.
10. USNRC Reg. Guide 1.172, Rev. 00, Jul. 1997, “Software Requirements Specifications for Digital Computer Software Used in Systems of Nuclear Power Plants”
11. USNRC Reg. Guide 1.173, Rev. 00, Jul. 1997, “Developing Software Life Cycle Processes for Digital Computer Software Used in Systems of Nuclear Power Plants”.
12. USNRC Reg. Guide 1.22, Rev. 00, February. 1972, “Periodic Testing of Protection System Ac-tuator Functions”.

제 2 절 기술표준

1. IEEE Std. 7-4.3.2-2003, “Standard Criteria for Digital Computers in Safety System of Nuclear Power Generating Stations”

2. IEEE Std. 338-1987 (Reaffirmed 1993), “Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Stations Safety Systems”.

3. IEEE Std. 603-1998, “Standard Criteria for Safety Systems for Nuclear Power Generating Stations”

4. IEEE Std. 730-1989, “Standard for Software Quality Assurance Plans”.

5. IEEE Std. 828-1998, “Standard for Software Configuration Management Plans”.

6. IEEE Std. 829-1998, “IEEE Standard for Software Test Documentation”.

7. IEEE Std. 830-1998, “Recommended Practice for Software Requirements Secification”.

8. ANSI/IEEE Std. 1008-1987 (Reaffirmed 1993), “IEEE Standard for Software Unit Testing”.

9. IEEE Std. 1012-1998, “Standard for Software Verification and Validation Plans”.

10. IEEE Std. 1016-1998, “Recommended Practice for Software Design Description”.

11. IEEE Std. 1016.1-1993, “Guide to Software Design Descriptions”.

12. IEEE Std. 1028-1997, “IEEE Standard for Software and Audits”.

13. ANSI/IEEE Std. 1042-1987 (Reaffirmed 1993), “IEEE Guide to Software Configuration Man-agement”.

14. IEEE Std. 1074-1997, “IEEE Standard for Developing Software Life Cycle Processes”

제 3 절 설계문서

1. 원자력발전소 안전계통에 적용하기 위한 PLC 일반 요건 및 규격, KAERI/TR-2010

2. KNICS-PLC-SR101, “안전등급 PLC(POSAFE-Q) 설계요건서,” 한국원자력연구원

3. KNICS-PLC-DS301, “안전등급 PLC(POSAFE-Q) 설계사양서,” ㈜포스콘

4. KNICS-PLC-IR101, “안전등급 PLC(POSAFE-Q) 연계요건서,” 한국원자력연구원

5. KNICS-PLC-SRS121-01, 안전등급 PLC 프로세서모듈 운영체제 소프트웨어 요구사항명세

서, 한국원자력연구소

6. KNICS-PLC-SRS121-27, “안전등급 PLC(POSAFE-Q) 프로세서 모듈(NCPU-1Q) PLD 로직(NLCPU1) 요구사항 명세서,” 한국원자력연구원

7. KNICS-PLC-SDG131, 안전등급 PLC 소프트웨어 설계명세 작성절차서, 한국원자력연구소

8. KNICS-PLC-SEP101, 안전등급 PLC 소프트웨어 관리 계획서, 한국원자력연구소

9. KNICS-PLC-SEP102, 안전등급 PLC 소프트웨어 개발 계획서, 한국원자력연구소

10. KNICS-PLC-SEP103, 안전등급 PLC 소프트웨어 품질보증 계획서, 한국원자력연구소

11. KNICS-PLC-SEP104, 안전등급 PLC 소프트웨어 통합 계획서, 한국원자력연구소

12. KNICS-PLC-SEP106, 안전등급 PLC 소프트웨어 유지보수 계획서, 한국원자력연구소

13. KNICS-PLC-SEP110, 안전등급 PLC 소프트웨어 확인 및 검증 계획서, 한국원자력연구소

14. KNICS-PLC-SEP111, 안전등급 PLC 소프트웨어 형상관리 계획서, 한국원자력연구소

15. KNICS-RPS-DS101, Rev. 00, 2004, “원자로보호계통 설계사양서”, 한국원자력연구소

16. KNICS-RPS-IR101, Rev. 00, 2005, “원자로보호계통 연계요건서”, 한국원자력연구소

17. KNICS-RPS-DS102, Rev. 00, 2005, “원자로보호계통 기능요건서”, 한국원자력연구소

18. KNICS-RPS-SEP102, Rev. 00, 2005, “원자로보호계통 소프트웨어 개발계획서”, 한국원자력연구소

19. KNICS-RPS-SRS221-01, Rev. 01, 2005, “원자로보호계통 비교논리프로세서 소프트웨어 요구사항 명세서”, 두산중공업㈜

20. KNICS-RPS-SRS221-02, Rev. 00, 2005, “원자로보호계통 동시논리프로세서 소프트웨어 요구사항 명세서”, 두산중공업㈜

21. KNICS-RPS-SRS221-03, Rev. 00, 2005, “원자로보호계통 자동시험 및 연계프로세서 소프트웨어 요구사항 명세서”, 두산중공업㈜

22. KNICS-RPS-SRS221-04, Rev. 00, 2005, “원자로보호계통 캐비닛운전원모듈 소프트웨어 요구사항 명세서”, 두산중공업㈜

23. KNICS-RPS-SDS231-10, Rev. 00, 2005, “원자로보호계통 비교논리프로세서 소프트웨어 설계 명세서”, 두산중공업㈜

24. KNICS-RPS-SDS231-20, Rev. 00, 2005, “원자로보호계통 동시논리프로세서 소프트웨어 설계 명세서”, 두산중공업㈜

25. KNICS-RPS-SDS231-40, Rev. 00, 2005, “원자로보호계통 캐비닛운전원모듈 소프트웨어 설계 명세서”, 두산중공업㈜

제 4 절 기타문서

1. Programming Guidelines for the Digital Reactor Protection System

2. POSAFE-Q User's Guide

3. ASME NQA-1-1997 “Quality Assurance Requirements for Nuclear Facility Applications”

4. pCOS 설명서, 2002, ㈜포스콘

5. uC/OS The Real Time Kernel, 1992, Jean J. Labrosse

6. uC/OS-Ⅱ The Real Time Kernel, 2002, Jean J. Labrosse

7. MicroC/OS-Ⅱ Software Requirements Document Rev 2.3, 1999, Alan D. Ford

8. Embedded System Building Block, 2001, Jean J. Labrosse

9. uC/OS & uC/OS-Ⅱ 홈페이지

10. DIOIZ 홈페이지

KAERI

서 지 정 보 양 식

수행기관보고서번호	위탁기관보고서번호	표준보고서번호	INIS 주제코드
KAERI/CM-1069/2007			

제목 / 부제	안전등급제어기기(PLC) RTOS 고신뢰도화 및 RPS 구조 검증
연구책임자 및 부서명	손한성/(주)에네시스
연 구 자 및 부 서 명	송덕용, 손대성, 김진혁

출 판 지	한국	발행기관	(주)에네시스	발행년	2008
페 이 지	105p.	도 표	있음(o), 없음( )	크 기	Cm.
참고사항					
공개여부	공개(o), 비공개( )		보고서종류	최종연구보고서	
비밀여부	대외비 ( ), __ 급비밀				
연구위탁기관	강원대학교		계약 번호		

초록 (15-20줄내외)

안전등급제어기기(PLC) RTOS 고신뢰도화 및 RPS 구조 검증 과제의 최종 목표는 안전 계통 중 특히 안전등급 PLC인 POSAFE-Q의 프로세서 모듈 소프트웨어의 고신뢰도화 개발 및 RPS 구조 검증을 통한 계통 및 소프트웨어 설계 지원을 수행하기 위함이다. 이를 위해서 본 연구에서는 POSAFE-Q 및 RPS 개발자에게 안전-필수 소프트웨어 개발 시 필요한 소프트웨어 요구사항 명세서 및 소프트웨어 설계 명세서 작성, 컴포넌트 시험 및 통합 시험 수행을 직접 지원하며, RTOS 고신뢰도화 및 RPS 구조 검증에 필요한 핵심 기술을 지원하였다. 이러한 지원 노력은 고신뢰도화된 소프트웨어를 탑재한 POSAFE-Q 프로세서 모듈로 결실을 맺었으며, KNICS만의 독특한 설계를 가지며 안전성 및 신뢰성이 향상된 RPS 설계로 결실을 맺었다.

주제명키워드 (10단어내외): 안전등급제어기기, 원자로보호계통, 리얼타임 운영체제, 설계명세서, 고신뢰도

BIBLIOGRAPHIC INFORMATION SHEET

Performing Org. Report No.	Sponsoring Org. Report No.	Stamdard Report No.	INIS Subject Code
KAERI/CM-1069/2007			

Title / Subtitle	High-Reliable PLC RTOS Development and RPS Structure Analysis
Project Manager and Department	HS Sohn/Enersys Co.
Researcher and Department	DY Song, DS Sohn, JH Kim

Publication Place	Korea	Publisher	Enersys Co.	Publication Date	2008.4.30
Page	105p.	Ill. & Tab.	Yes(o), No ( )	Size	Cm.
Note					
Open	Open(o), Closed( )		Report Type		
Classified	Restricted( ), ___Class Document				
Sponsoring Org.			Contract No.		

Abstract (15-20 Lines)

One of the KNICS objectives is to develop a platform for Nuclear Power Plant(NPP) I&C(Instrumentation and Control) system, especially plant protection system. The developed platform is POSAFE-Q and this work supports the development of POSAFE-Q with the development of high-reliable real-time operating system(RTOS) and programmable logic device(PLD) software. Another KNICS objective is to develop safety I&C systems, such as Reactor Protection System(RPS) and Engineered Safety Feature-Component Control System(ESF-CCS). This work plays an important role in the structure analysis for RPS. Validation and verification(V&V) of the safety critical software is an essential work to make digital plant protection system highly reliable and safe. Generally, the reliability and safety of software based system can be improved by strict quality assurance framework including the software development itself. In other words, through V&V, the reliability and safety of a system can be improved and the development activities like software requirement specification, software design specification, component tests, integration tests, and system tests shall be appropriately documented for V&V. This work was performed on this purpose.

Subject Keywords (About 10 words): Safety Grade PLC, RPS, RTOS, SDS, High Reliability