2001 춘계학술발표회 논문집
한국원자력학회

디지털 원자로보호계통 고 신뢰도 소프트웨어 개발방법 연구
(A Study on the High Reliable Software Development Method for the DRPS)

신 현국, 남 상구, 손 세도, 장 훈선
한국전력기술주식회사
대전광역시 유성구 덕진동 150

유 준, 신 정훈, 윤 석영
충남대학교
대전광역시 유성구 궁동 220

손 한성
한국과학기술원
대전광역시 유성구 구성동 373-1

요 약

원자로보호계통(Reactor Protection System)은 원자력발전소 설계기준사고시 중요 운전변수가 안전제한치(Safety Limits)를 초과할 경우 원자로 정지 및 공학적안전설비를 작동시켜 핵연료 피복재의 과열을 방지하고 원자로 냉각재계통의 건전성을 유지해 주는 설비로써, 원자력발전소의 안전운전에 필수적이다. 과학기술부가 지원하는 국가지정연구실에서는 소프트웨어 공통유형고장(Common Mode Failure)을 배제하기 위해 한 채널 내부에서 하드웨어 및 소프트웨어의 다양성을 갖는 디지털 원자로보호계통을 개발하고 있다. 이에 따라, VME bus 방식의 단일보드컴퓨터(Single Board Computer)를 사용하여 프로토타입을 제작하고, C 언어를 이용하여 응용소프트웨어를 개발중에 있다. 디지털 원자로보호계통 (Digital Reactor Protection System) 개발에 있어 고 신뢰도의 소프트웨어를 확보하기 위해서는 설계 초기단계에서 상세한 기능 분석 및 시뮬레이션이 매우 중요하며, 또한, 서술적인 소프트웨어요건명세서(Software Requirements Specification)와 병행하여 정형기법을 사용하여 소프트웨어에 대한 명세를 정확하고 완전하게 정의하여야 한다. 본 논문에서는 Dynamic Simulation Tool을 이용한 원자로보호계통의 기능 분석 및 시뮬레이션 결과와 State Chart를 사용한 정형기법의 소프트웨어 명세방법에 대해 기술하였다.

Abstract

The functions of Reactor Protection System (RPS) are to protect the nuclear fuel design limits and reactor coolant system boundary by tripping the reactor when the plant parameter exceeds these limits. The RPS also provides assistance in mitigating the consequences of accidents through actuation of separate Engineered Safety Features (ESF) system. The National Research Laboratory, funded by Ministry of Science and Technology, is developing Advanced Digital Reactor Protection System with diverse dual processors in one channel to prevent Common Mode Failure (CMF). In this research, the prototype is being developed with VME based Single Board Computer and its application program is being implemented using C language. The detail functional analysis and simulation in the initial stage of software development are very important to ensure high reliable software for Digital Reactor Protection System (DRPS). Also, the Software Requirement Specification (SRS) should be defined as well clearly and completely using formal methodologies. In this paper, the functional analysis and simulation result on DRPS using Dynamic Simulation Tool, and the formal type Software Requirement Specification using State Chart are described.

1. 서론

원자력발전소의 디지털 계측제어계통에서 소프트웨어 역할이 증가함에 따라 공통유형고장의 가능성이 중요한 관심사항이 되고 있다. 종래의 아날로그 보호계통에서는 공통유형고장 발생 가능성이 매우 희박하다고 간주되어 왔고, 비록 공통유형고장이 발생하더라도 아날로그 기기의 기계적, 전기적 부식과 마모의 과정은 서서히 진행되므로 큰 문제가 되지 않았다. 그러나, 디지털 기술은 기존의 기능들이 소프트웨어에 의해 작동된다는 것이다. 즉, 아날로그 기술은 그 구성요소인 부품 (캐패시터, 저항기, 반도체 소자, 집적회로 등) 의 품질을 규격화하여 생산할 수 있으나, 디지털 기술의 핵심인 소프트웨어는 프로그래머(사람)가 작성하기 때문에 개인의 특성과 능력에 따라 생산되는 소프트웨어의 품질은 규격화하기가 어렵다. 그리고 프로그래머의 오류나 실수가 생산된 소프트웨어 내에 존재할 가능성이 있게 된다. 이렇게 발생된 오류나 잘못된 소프트웨어가 운전중 계통의 같은 구성품에서 어느 순간 동시에 발생된다면, 계통 전체가 오동작으로 인한 기능 상실 상태가 되는 것이다. 따라서, 이러한 소프트웨어의 공통유형고장은 하드웨어의 다중성을 파기하는 결과를 초래할 수 있다.

일반적으로 소프트웨어의 개발은 개념설계단계(Concept Phase), 요구사항단계(Requirement Phase), 설계단계(Design Phase), 구현단계(Implementation Phase) 및 시험단계(Test Phase)의 5개 단계로 구분된다. 최근의 소프트웨어 통계자료와 논문을 종합해 보면 요구사항단계(Requirements Phase)에서 가장 많은 소프트웨어 오류가 발생하며, 이를 시험단계에서 검색 발견하는 것 보다 설계 초기 단계인 요건명세단계에서 확인 및 검증하는 것이 소프트웨어의 오류가 적고 경제적임을 알 수 있다.

한편, 새로운 계통에 대한 하드웨어 구성 및 소프트웨어 개발은 계통 모델링과 시뮬레이션을 통한 집중적인 검토와 분석이 필요하다. 본 연구의 하드웨어 구성 및 기능분석에 사용된 Dynamic Simulation Tool인 Matlab 소프트웨어는 프로토타입의 제작 및 소프트웨어 구현에 앞서 보호계통을 모델링하고 시뮬레이션을 통해 설계상 문제점을 도출하는데 활용할 수 있으며, 그 결과를 분석하여 계통설계명세서/기능요건명세서의 오류를 수정하는데 효과적이다.

또한, 고 신뢰도의 소프트웨어를 생산하기 위해서는 요건명세단계에서 정형기법의 하나인 State Chart를 사용하여 요건을 분석하고, States 사이의 Transition과 Simulation을 통해서 정확하고 완전한 명세를 정의하여야 한다. 즉, State Chart를 지원하는 도구를 사용하여 State Chart를 작성하고, 이를 기존의 서술적인 요건과 결합하여, 정형기법을 도입한 소프트웨어 요건명세서를 작성하는 것이 바람직하다. 본 연구의 State Chart 작성에 사용된 Statemate 소프트웨어는 Graphic 모델링 및 Simulation, C 코드 자동생성 기능 등을 갖고 있어 정형적 소프트웨어 요건명세서 작성 및 검증에 활용할 수 있다.

본 논문에서는 과학기술부가 지원하는 국가지정연구실사업의 일환으로 개발중인 디지털 원자로보호계통에 대한 소프트웨어 V&V 수행방안, Dynamic Simulation Tool을 이용한 기능 분석 및 시뮬레이션 결과와 State Chart Graphic으로 표현되는 정형명세서를 사용한 고신뢰도 소프트웨어 개발방법에 대하여 설명하고자 한다.

2. 개선된 소프트웨어 개발방법

일반적으로 소프트웨어 개발은 계통설계(System Design)가 완료된 후 소프트웨어 요건명세서(Software Requirement Specification)를 작성하고, 그 다음 상세 기능 및 코딩요건을 기술하고 있는 소프트웨어 설계설명서(Software Design Description)를 바탕으로 소프트웨어를 구현하게 된다. 소프트웨어 작성이 완료되면 컴퓨터 하드웨어에 내장되어 모듈별 시험을 거쳐서 기능 및 성능을 확인하는 종합시험(공장인수시험)을 하게 된다. 이후 장비를 설치 현장으로 이동하여 시운전시험기간동안 정상적으로 운전되는 것이

확인되면 운영자(발주자)에게 인도된다. 이러한 일련의 과정을 기기설계(Component Design)와 기기공급(Equipment Supply)이라 한다.

한편, 원전에 적용되는 안전등급의 소프트웨어 개발은 계통설계의 내용과 기기설계를 함께 고려하여 소프트웨어를 생산해야 고신뢰도의 품질을 달성할 수 있다. 그림 1에는 안전등급 소프트웨어 개발에 적용되는 설계 및 독립된 형태의 확인검증(Verification & Validation) 업무흐름을 보여주고 있다.

최근 소프트웨어 관련 논문과 시험 통계자료를 분석해 보면, 소프트웨어 요건명세단계(Software Requirement Phase)에서 가장 많은 소프트웨어 오류가 발생됨을 알 수 있다. 따라서 오류를 최종 시험단계나 소프트웨어 코딩단계에서 찾아내려는 노력보다는 프로그래머가 소프트웨어 요건명세를 명확히 이해할 수 있도록 초기 단계에서 확인 검증이 충분히 실시된다면 소프트웨어 오류를 제거하는데 보다 용이하고 경제적이다. 이에 따라 선진 각국에서는 이미 이러한 소프트웨어 요건명세서 개발에 많은 노력을 기울여 왔다. 특히, 카나다 AECL사는 정형기법인 Graphic과 수식이 복합된 Rule을 사용하여 안전등급 소프트웨어를 개발하고 원자로정지계통인 Shutdown System No.1과 No.2에 적용하여 성공적으로 운영하고 있다.

본 연구에서는 계통설계에서 발생할지도 모르는 설계 결함을 배제하기 위해서 Dynamic Simulation Tool을 사용하여 계통설계상의 모든 기능을 시뮬레이션 하였으며, 그 결과 및 특성 등을 분석하여 계통설계요건서를 검증하는 한편, 이를 바탕으로 State Chart를 작성하는 소프트웨어 툴을 사용함으로써 독립된 확인 검증외에도 설계 업무과정에서도 자체적인 설계 검증이 가능하도록 계통 및 소프트웨어 설계 체제를 갖추었다. 그림 2는 본 연구에서 채택하고 있는 고신뢰도 소프트웨어 개발 및 독립된 소프트웨어 V&V 업무흐름도를 보여주고 있다. 여기서, 각 단계별 문서의 확인 검토는 Requisite Pro라는 소프트웨어 툴을 이용하여 요건추적매트릭스(Requirements Traceability Matrix)를 작성하여, 문서의 수정 및 작성을 보다 쉽게 추적 관리할 수 있는 체제를 도입하였다.

새로 고안된 고신뢰도 소프트웨어 개발방법의 특징은 설계과정에서 수행되는 3중의 자체 검증이다. 첫 번째 검증은 계통설계 단계에서 Dynamic Simulation Tool 인 Matlab 소프트웨어로 계통 입출력 동작, 비교논리 및 동시논리 알고리즘과 원자로의 안전변수에 따른 디지털 보호계통의 동작 특성까지 세부적으로 모두 재현해 본다는 것이다. 따라서, 소프트웨어 엔지니어에게 계통설계단계 이후에 구현할 설계내용에 대해서 충분한 정보를 제공해 줄 수 있다.

설계과정의 두 번째 검증은 소프트웨어 코딩단계에서 수행된다. 즉 국가지정연구실에서 추진하는 디지털 원자로보호계통에서는 이기종 이중화 설계를 채택하고 있으며, 컴퓨터 운영체제(Operating System)로 VxWorks와 QNX를 사용하고 있다. 따라서 State Chart를 사용한 정형적인 소프트웨어 요건명세서(SRS)에 의해서 VxWorks 운영체제를 사용하는 소프트웨어 설명서와 코딩과 QNX 운영체제를 사용하는 소프트웨어 설명서와 코딩이 별도로 작성된다. 코딩된 소프트웨어 모듈들이 시험된 후 시험결과를 비교하여 오류가 있을 경우 소프트웨어 설계설명서(SDD) 단계로 되돌려지고, 이상이 없으면 종합시험 단계로 진행된다.

설계과정의 세 번째 검증은 종합시험단계에서 수행된다. 종합시험결과와 Simulation Tool로 시뮬레이션한 각종 예측결과와 일치하는지를 확인하고 이상이 없을 경우 소프트웨어 개발을 완료한다. 종합시험단계에서 불일치 사항이 발생하면 소프트웨어 개발요건서(SRS) 단계로 되돌려져 설계결함이 수정된다. 그림 3은 상기의 소프트웨어 설계 및 확인검증업무를 흐름도(Flow Chart) 형식으로 나타내고 있다. 이상과 같은 방법은 국가지정연구실에서 수행하고 있는 방법으로 소프트웨어의 오류를 막고 고신뢰도의 소프트웨어를 생산하는데 매우 효과적이라고 판단된다.

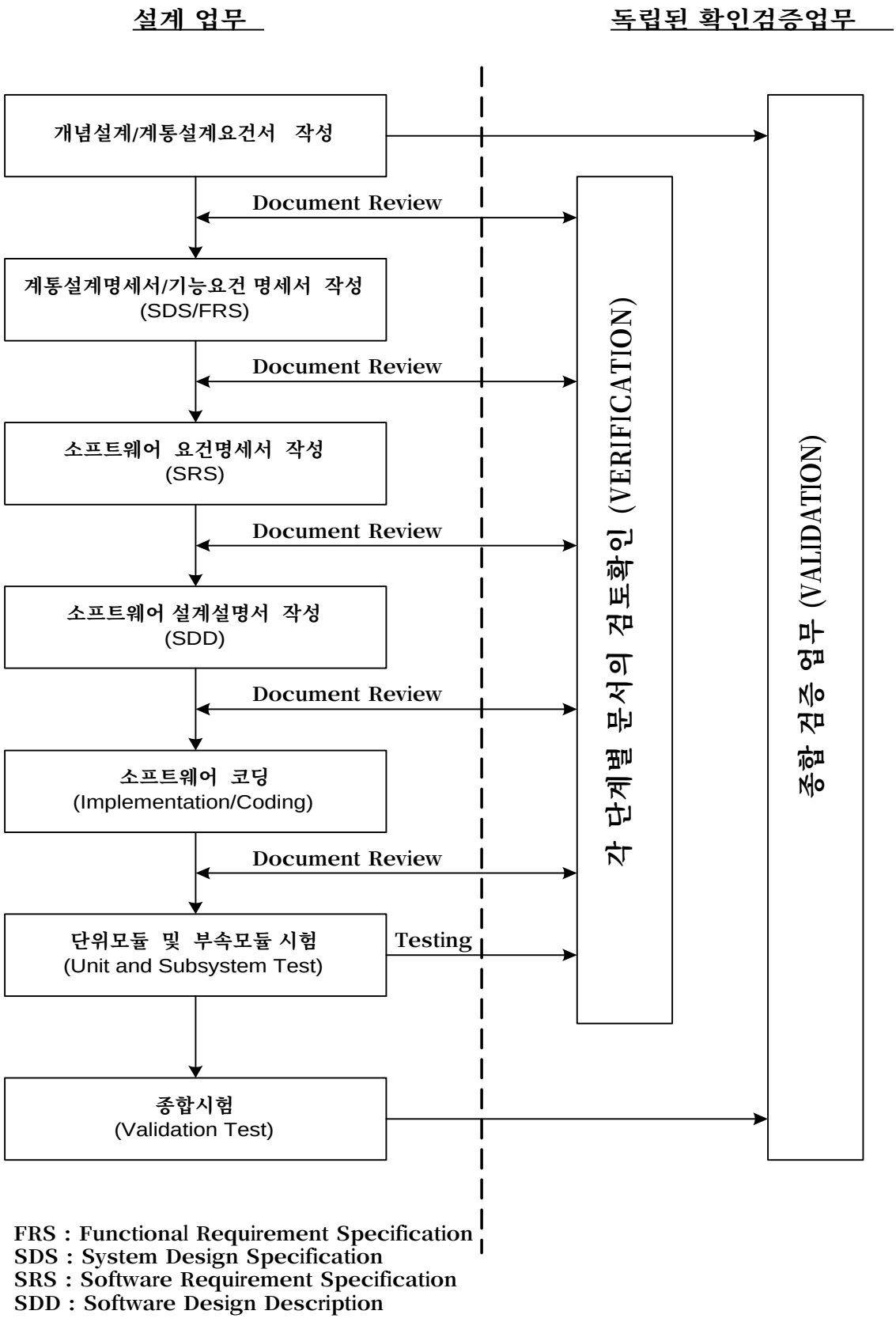
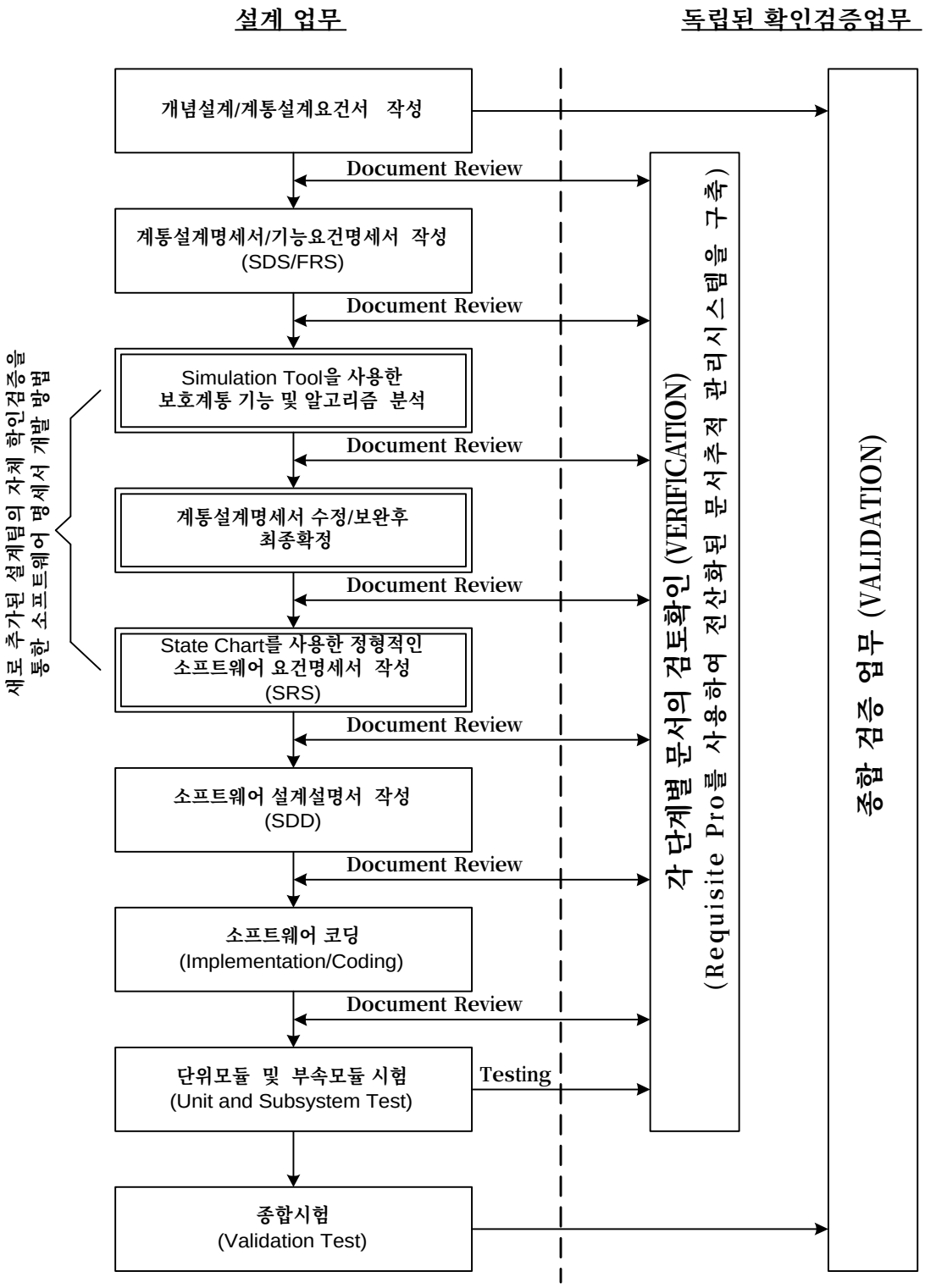


그림 1 소프트웨어 설계 및 확인검증 업무 흐름도



FRS : Functional Requirement Specification
SDS : System Design Specification
SRS : Software Requirement Specification
SDD : Software Design Description

그림 2개선된 소프트웨어 설계 및 확인검증 업무흐름도

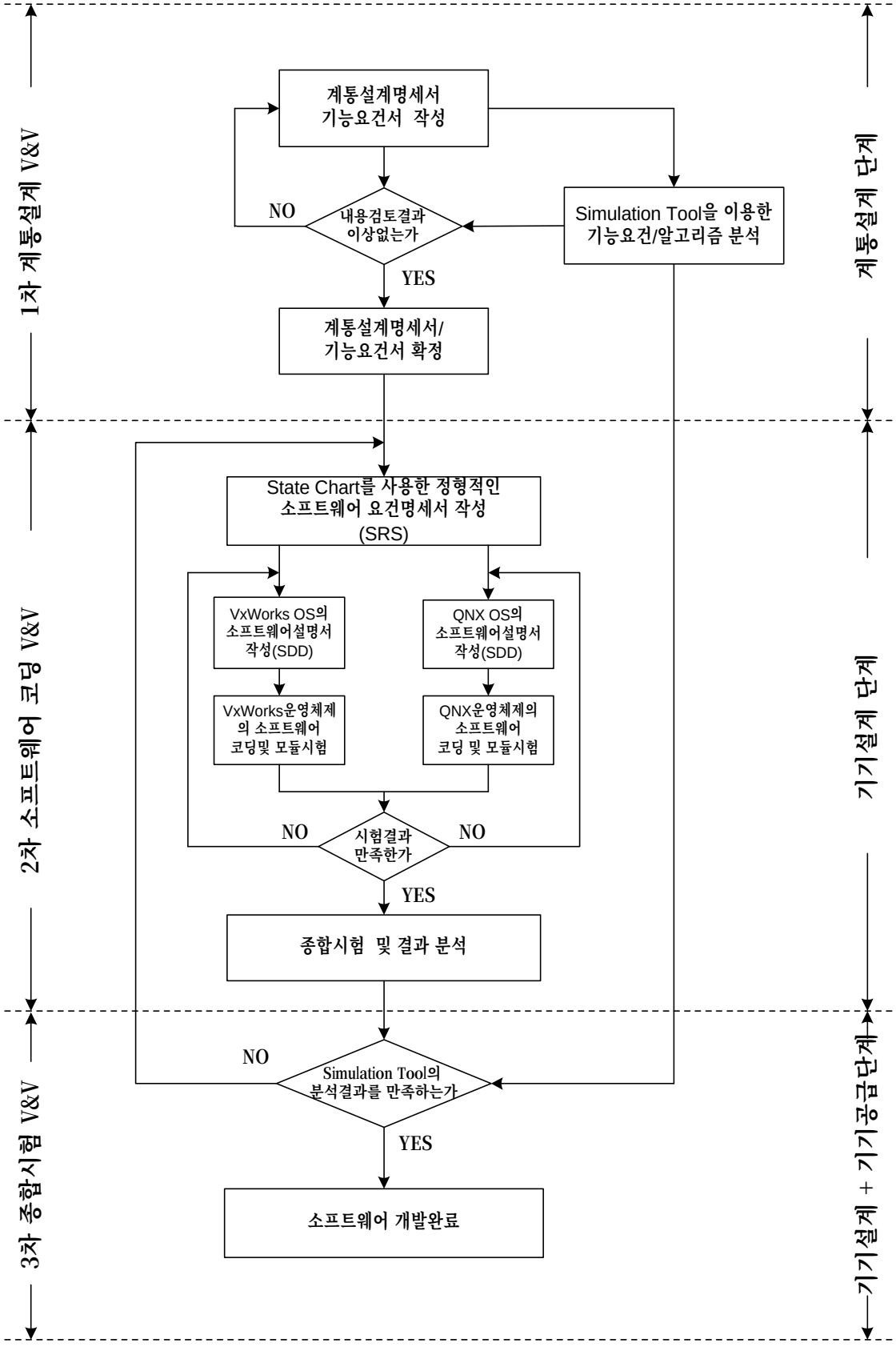


그림 3 DRPS 소프트웨어 설계 및 확인검증 세부업무 흐름도

3. 디지털 보호계통 설계특성

3.1 계통 구성 및 기능

디지털 원자로보호계통(Digital Reactor Protection System)은 그림 4와 같이 4 개의 다중 채널(A, B, C, D)로 구성되며, 각 채널은 비교논리 프로세서(Bistable Processor), 동시논리 프로세서(Local Coincidence Logic Processor), 계통연계 프로세서(System Interface Processor), 원자로정지 및 공학적안전설비작동계통 개시회로(RT and ESFAS Initiation Logic), 보수시험반 (Maintenance and Test Panel) 및 운전원 모듈(Operator Module)을 갖고 있다.

각 채널의 비교논리 프로세서는 공정으로부터 독립적인 측정값을 받으며, 공정변수마다 미리 지정된 트립설정치와 비교함으로서 트립상태를 결정한다. 비교논리 프로세서의 트립상태는 데이터링크를 경유하여 동일 채널 및 타 채널의 동시논리 프로세서에 주기적으로 전송된다. 다중 채널간 고속데이터링크의 전송경로는 독립성과 격리성을 고려하여 광섬유케이블이 사용된다.

동시논리 프로세서는 트립변수마다 독립적인 2/4 동시논리를 갖고 있어, 4개 채널중 2개 채널에서 트립상태가 발생하면 원자로 정지 및 공학적안전설비작동계통의 동작을 위해 개시회로로 트립신호를 보낸다. 한편, 2/4 동시논리는 채널시험 및 보수시 운전원 요구에 의해 2/3 동시논리로 변환된다.

보수시험반은 계통의 운전상태를 표시하고, 트립채널우회 및 시험을 수행하는데 사용되며, 계통연계 프로세서는 계통의 운전상태를 감시하고, 자동시험을 수행하며, 채널 내부의 프로세서 및 타 계통과의 데이터통신을 수행한다. 한편, 주제어반에 설치되는 운전원 모듈은 운전원이 가변설정치 리셋 및 운전우회기능 등을 수행할 수 있도록 해준다.

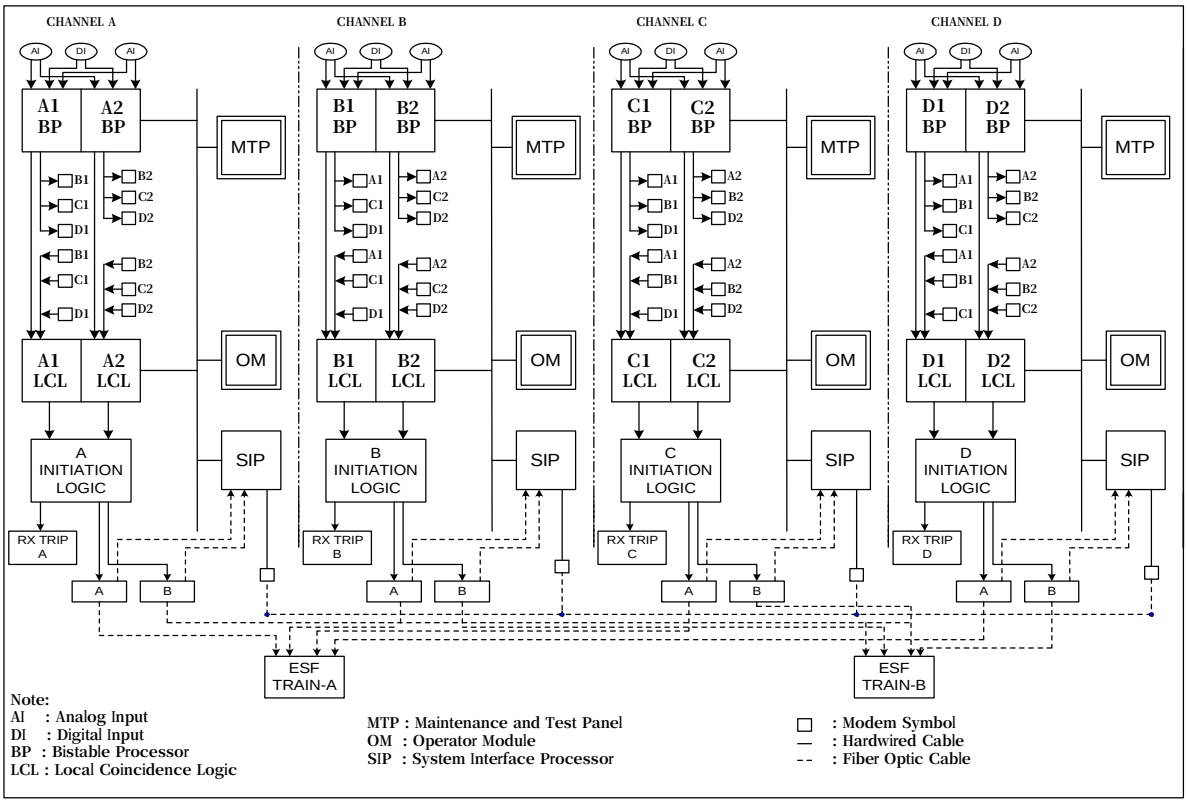


그림 4 디지털 원자로보호계통 기능 블록도

3.2 하드웨어 및 소프트웨어 다양성 설계

공통유형고장 문제는 디지털 시스템이 소프트웨어를 기반으로 하기 때문에 발생한다. 공통유형고장은 동일한 디지털 기기 및 소프트웨어를 사용함으로써 필수안전기능이 동시에 상실되는 것을 의미한다. 본 연구에서는 이러한 공통유형고장을 계통내에서 해결할 수 있도록 이기종의 Dual Processor를 사용한 계통 구조의 개념설계를 개발하였다. 이기종의 Dual Processor 구조는 서로 다른 이기종의 논리 Processor를 사용하고 있으며, 또한 운영체제인 Operating System(OS)이 서로 달라 공통유형고장이 동시에 서로 다른 구조에서 발생할 수가 없다.

디지털 원자로보호계통의 각 채널에는 그림 5와 같이 2개의 비교논리 프로세서 모듈(BP1, BP2) 및 2개의 동시논리 프로세서 모듈(LCL1, LCL2)이 있다. 여기서, 한 쌍의 비교논리 프로세서와 동시논리 프로세서 (BP1, LCL1)에는 Intel CPU 프로세서 모듈을 다른 쌍(BP2, LCL2)에는 Motorola CPU가 장착된 프로세서 모듈로 구성하여, 프로세서 기기 내부의 중요 부분의 하드웨어 설계 구조가 다르게 하였다.

특히 프로세서의 운영을 담당하는 소프트웨어인 운영체제(Operating System)에도 다양성을 도입하여 Intel CPU 모듈에는 QNX OS를 탑재하고, Motorola CPU 모듈에는 VxWorks OS를 탑재하였다. QNX와 VxWorks 운영체제의 선정은 성능 및 사용실적을 검토하였으며, 특히 안전성과 관련된 분야(원전, 군사, 우주산업 등)의 적용사례를 고려하였다.

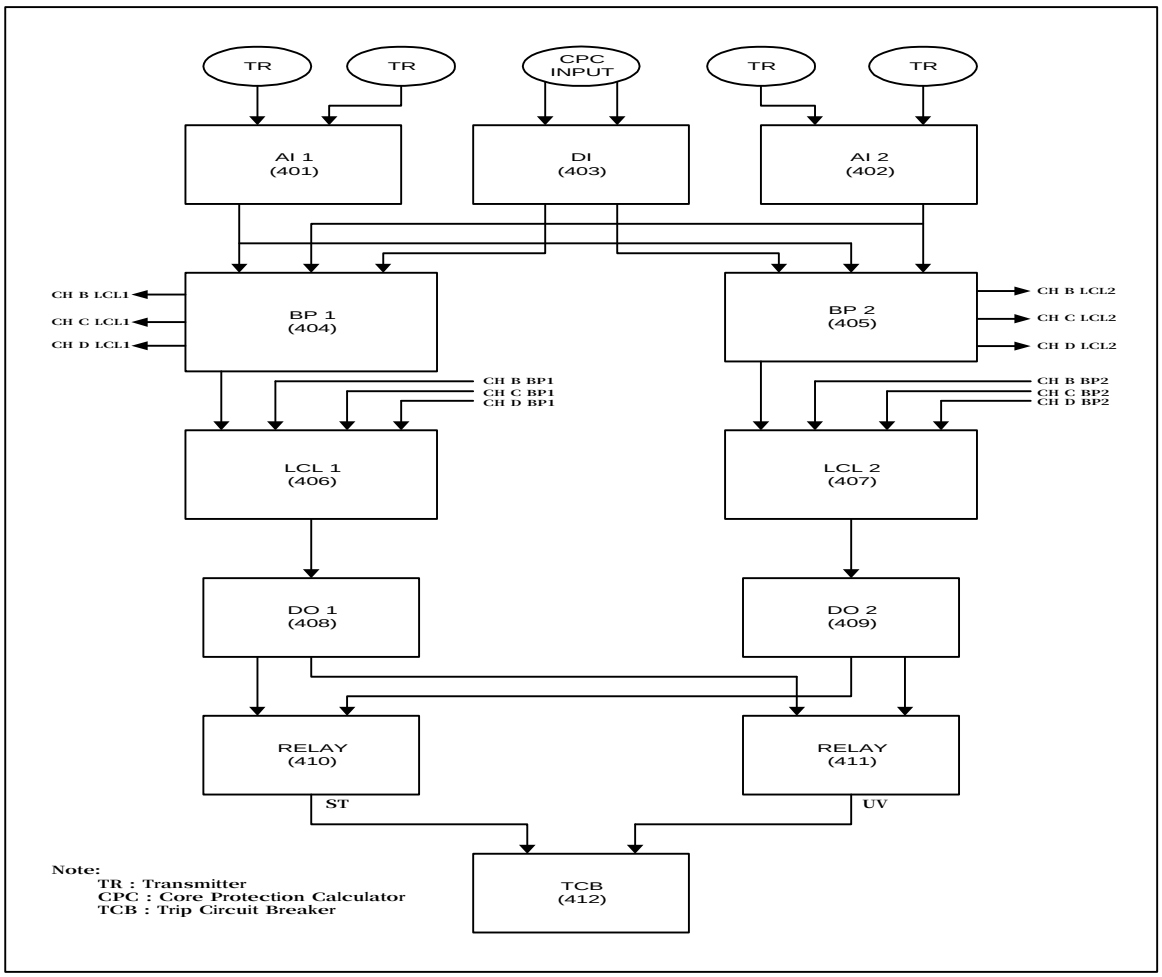


그림 5 디지털 원자로보호계통 단일 채널 블록도

4. Dynamic Simulation Tool을 이용한 원자로보호계통 기능분석 및 시뮬레이션

4.1 모델링 범위 및 트립변수

Dynamic Simulation Tool인 Matlab 소프트웨어를 이용한 디지털 원자로보호계통의 모델링 범위는 공정입력 채널에서부터 인터포징릴레이 출력까지 모두 포함하였으며, 트립알고리즘에 대한 입출력신호, 비교논리, 동시논리 및 채널간 신호전송에 대한 시뮬레이션을 수행하였다. 모델링에 사용된 모의 트립변수는 표 1과 같이 가압기 저압력 트립, 가변 과출력 트립, 증기발생기 저수위 트립, 격납건물 고압력 트립 및 고 국부출력밀도 트립의 5가지를 선정하였으며, 트립변수별 모델링 회로는 아날로그 입력신호, 디지털 입력신호, 변수에 따른 설정치 계산 방식, 비교논리 방식 및 운전우회 기능 등에 따라 다양하다. 이런 점을 고려하여 선정된 트립변수의 설정치 방식 및 트립유형(트립방식, 운전우회 여부)은 모든 트립변수(총 17개)의 유형을 모두 포함하게 된다.

표 1 모의 트립변수별 설정치 방식 및 트립유형

트립변수	설정치방식	트립방식	운전우회	트립설정치(예)
가압기 저압력	수동리셋형 가변설정치	하강트립	있음	1,700 psia, 400 psia decrease/reset
가변 과출력	자동비율제한형 가변설정치	상승트립	없음	Ceiling : 109.2% Band : 15% Rate : 11%/min
증기발생기 저수위	고정설정치	하강트립	없음	44%
격납건물 고압력	고정설정치	상승트립	없음	1.9 psig
고 국부출력밀도	이진신호	이진비교	없음	Trip = 1

4.2 가변 과출력 비교논리 회로 모델링 및 시뮬레이션 결과 (예)

가변과출력 트립(Variable Overpower Trip)은 원자로 출력이 프로그램 설정값 이상으로 증가하거나, 기설정된 최고값에 도달하게 되면 원자로를 정지시키는 기능으로, 트립설정치가 그림 6과 같이 원자로 출력에 따라 변화되는 특성을 갖고 있다.

가변과출력 설정치 회로는 공정변수값(원자로 출력)과 설정치 사이에 항상 일정한 차이(Band)가 유지되도록 설계하되, 설정치가 상승하는 변화율(Rate) 및 최고값(Ceiling)은 제한하도록 설계하여야 한다. 따라서, 정상 운전시에는 비교논리에 입력되는 공정변수값에 따라 설정치가 자동으로 증가하거나 감소하지만, 원자로 출력이 너무 빠른 비율로 증가할 경우에는 공정변수값과 설정치의 차이가 영(0)으로 접근하게 되어 비교논리는 트립상태가 된다. 그림 7은 25 msec의 Sampling Time(Ts)을 갖는 공정 입력에 대해 정격출력의 11 %의 상승 비율과 15 %의 밴드폭을 갖도록 하는 설정치를 생성하는 모델이며, 그림 7-1 에서 7-10은 시뮬레이션 신호 및 결과를 보여주고 있다.

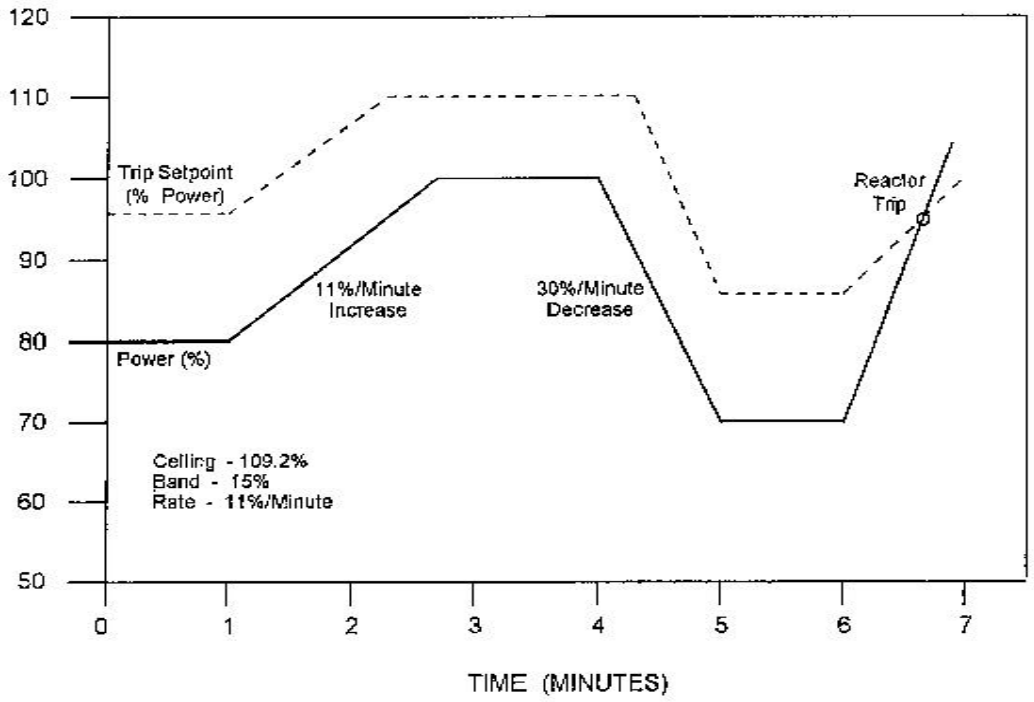


그림 6 자동 비율제한형 가변설정치 (가변 과출력 트립)

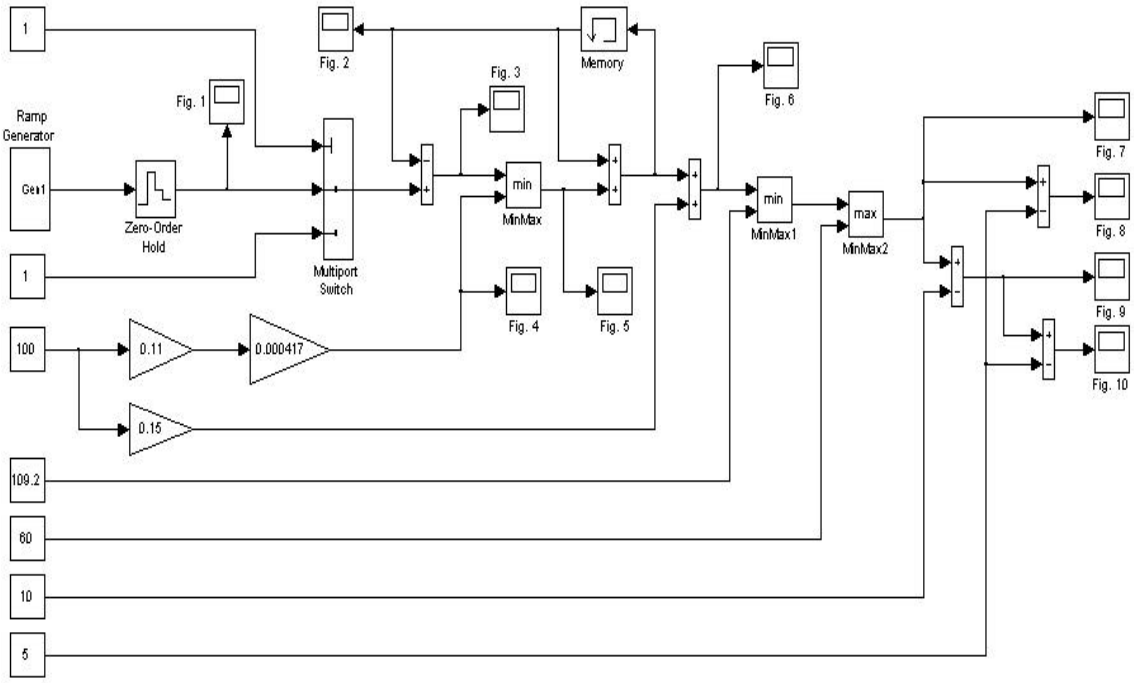
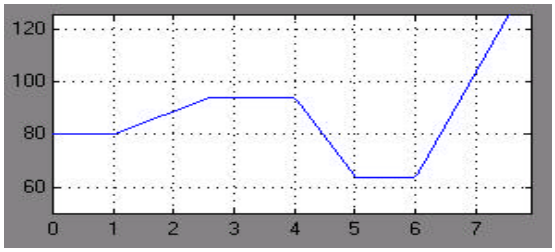
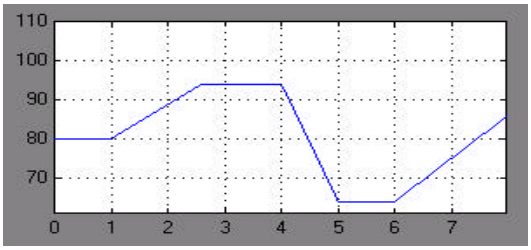


그림 7 제한된 상승비율 설정치 설정에 대한 모델 (가변 과출력 비교논리 회로)



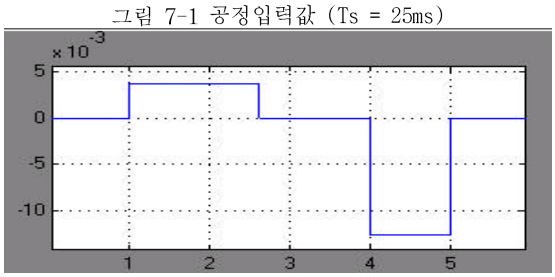
Time(Min)

그림 7-1 공정입력값 (Ts = 25ms)



Time (Min)

그림 7-2 Ts만큼 지연된 공정 입력값

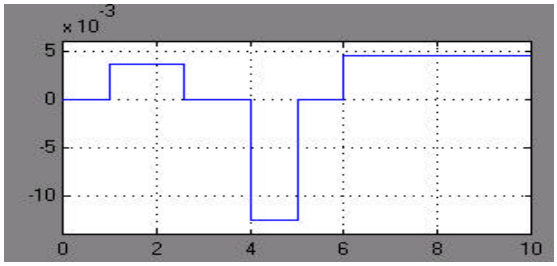


Time (Min)

그림 7-3 공정입력 차

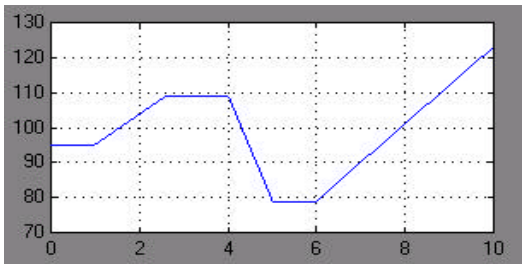
Time (Min)

그림 7-4 공정입력차의 한계치 (11 %/Min)



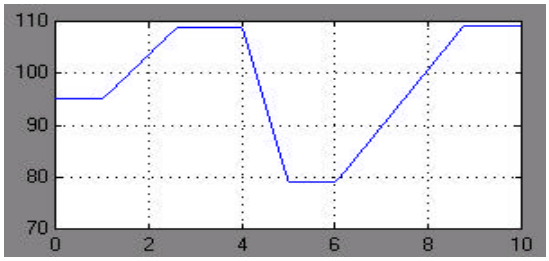
Time (Min)

그림 7-5 공정입력차에 대한 한계치 영향



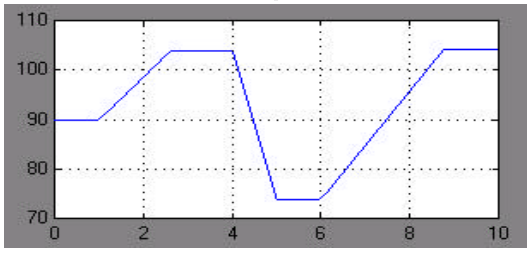
Time (Min)

그림 7-6 공정입력에 여유폭(15%/Min)을
더하여 Trip을 위한 설정치 생성



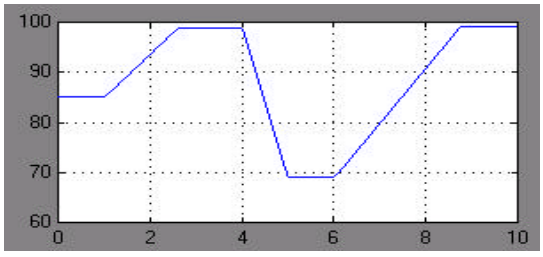
Time (Min)

그림 7-7 상한(109.2%)과 하한(60.0%)의 영향



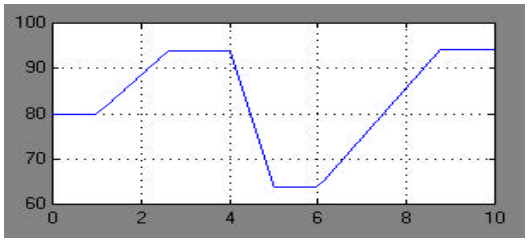
Time (Min)

그림 7-8 트립을 위한 설정치에 히스테리
시스값(5.0%)이 더해진 결과값



Time (Min)

그림 7-9 예비트립을 위한 설정치 생성 (-10.0% 더함)



Time (Min)

그림 7-10 예비트립을 위한 설정치에
히스테리시스값(5.0%)을 더한 결과값

5. State Chart를 이용한 소프트웨어 요건서

5.1 정형적 명세기법

원자력발전소의 디지털계측제어 시스템의 소프트웨어 개발시에는 반드시 시스템의 안전성, 신뢰성, 무결성 등을 고려해야 한다. 일반적으로 소프트웨어의 개발은 개념설계단계(Concept Phase), 요구사항단계(Requirement Phase), 설계단계(Design Phase), 구현단계(Implementation Phase) 및 시험단계(Test Phase)의 5단계로 구분되며, 소프트웨어의 안전성, 신뢰성, 무결성 등을 확보하기 위해서는 소프트웨어 개발초기단계인 소프트웨어 요구사항 단계에서 체계적이고 명확한 개발방법을 이용하여 시스템을 기술하고, 분석 및 검증을 수행할 수 있어야 한다.

정형명세기법은 소프트웨어의 개발 초기단계에서 소프트웨어 요구사항을 기술하기 위하여 수학적으로 정의된 기호와 논리를 사용하는 기법으로 시스템 개발 초기단계부터 시스템에 대한 분석을 가능하게 하여 불충분한 시스템 요구사항을 사전에 발견하고, 이로 인한 비용 상승을 방지하고 시스템의 신뢰성과 안전성에 기여할 수 있다. 단순기능의 소프트웨어 모듈이라도 그 기능을 문서화할 때는 그 내용이 복잡해지며, 단순한 잘못이라도 결과에 영향을 줄 수 있다. 특히 소프트웨어가 복잡한 계통의 제어를 담당하는 경우에는 그 복잡도는 기하급수적으로 증가하며, 이를 체계적이고 수학적인 기법으로 설계하고 검증하기 위해 고려되는 것이 정형기법(Formal Method)이다.

이런 정형화기법은 정형화 정도에 따라 정형명세 작성만을 지원하는 방법과 정형명세와 이의 검증을 지원하는 방법이 있다. 또한 정형방법도 그래픽한 방법과 로직이나 집합이론에 근거한 정형화 기법이 있다. State Chart 기법은 그래픽한 방법과 이의 Simulation에 근거한 정형적인 방법이다.

5.2 상태도표(State Charts)를 이용한 요건서

상태도표(State Charts)는 시스템 모델링을 기술하는데 사용되는 State Machine을 확장한 것으로 State Machine이 갖는 단점인 State Explosion을 해결하기 위해서 계층성(Hierarchical), 분할성(Compositional), 방송통신(Broadcasting)을 사용하였다. 계층성은 하나의 주상태(State)가 하나이상의 부상태(Sub-State)를 표현할 수 있으며, 이런 주상태를 상위(High -Level)계층이라 하며, 상위계층에 포함된 부상태들은 하위(Low-Level)계층이다. 하위계층의 부상태들은 부상태간에 배타적인 관계를 가지며, 부상태 중 단 하나만이 상위계층의 주상태를 표현한다. 분할성은 부상태들 간에 병렬성을 제공하는 기능으로 주상태를 성격이 서로 다른 여러 가지 부상태들로 표현하고 방송기능(Broadcating) 및 제어기능으로 정보를 주거나 받아 다른 상태로 전이할 수 있게 한다. 즉 하나의 주상태에 있는 여러개의 부상태들이 상태가 동시에 존재하고 각 부상태들의 표현이 주상태를 표현한다.

5.3 DRPS Activity Chart 및 가변 과출력 상태도표

그림 8은 DRPS 전체적 시스템의 Activity Chart를 보여준다. DRPS의 주 구성요소인 비교논리 프로세서(BP), 동시논리 프로세서(LCL), 계통연계 프로세서(SIP), 보수시험반(MTP)이 activity로 표현되어 있고, BP와 LCL은 각각 2개의 다중 구조로 구성되어 있다. DRPS의 외부 디바이스들로는 트립에 관련된 공정변수들을 측정하는 13개(S1-S13)의 센서들과 두개의 디지털 값을 보내주는 CPCS, 중성자속 신호를 보내주는 ENFMS가 있다. 한편, DRPS는 독립된 4개의 채널로 구성되는데 이를 표현하여 각 채널의 트립상태와 우회상태를 입력받는 OTHER CHANNELS 외부 디바이스로 구성된다. BP는 이런 공정변수들을 각각의 설정치 알고리즘에 의해서 계산된 설정치와 비교하고, LCL에서 동시논리를 수행하여 원자로트립(RT)과 공학적안전설비작동계통(ESFAS-AC)으로 전달한다.

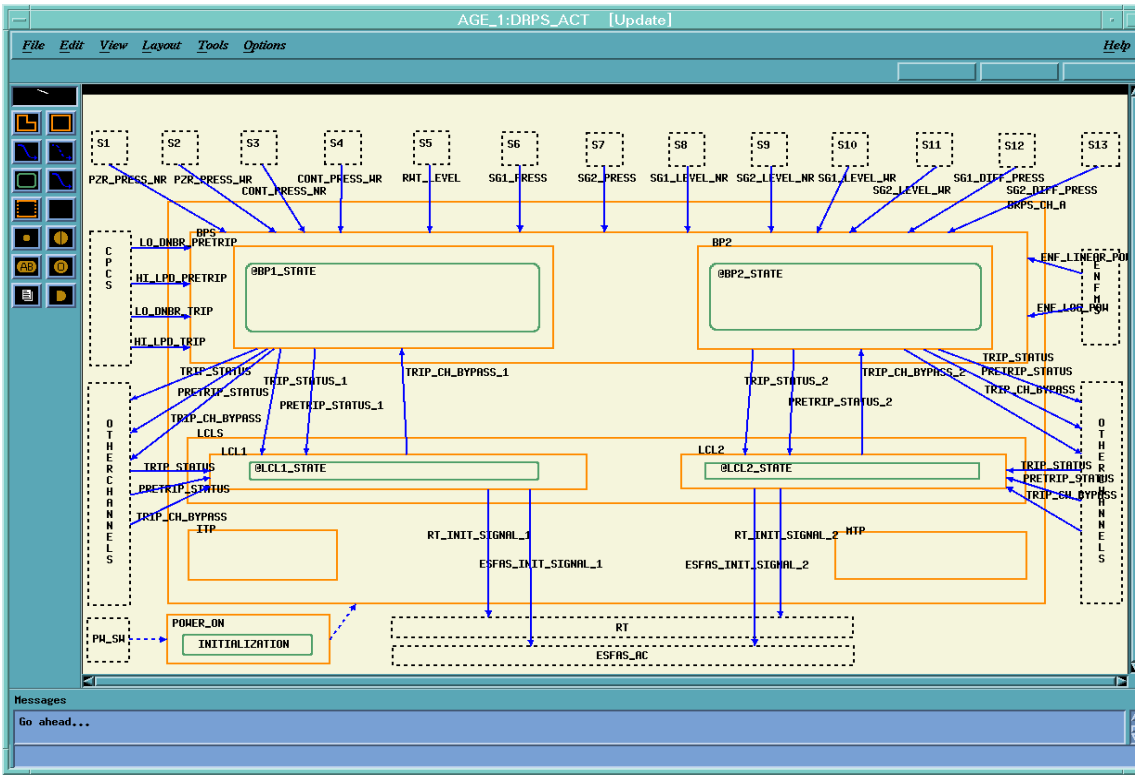


그림 8 DRPS의 Activity Chart

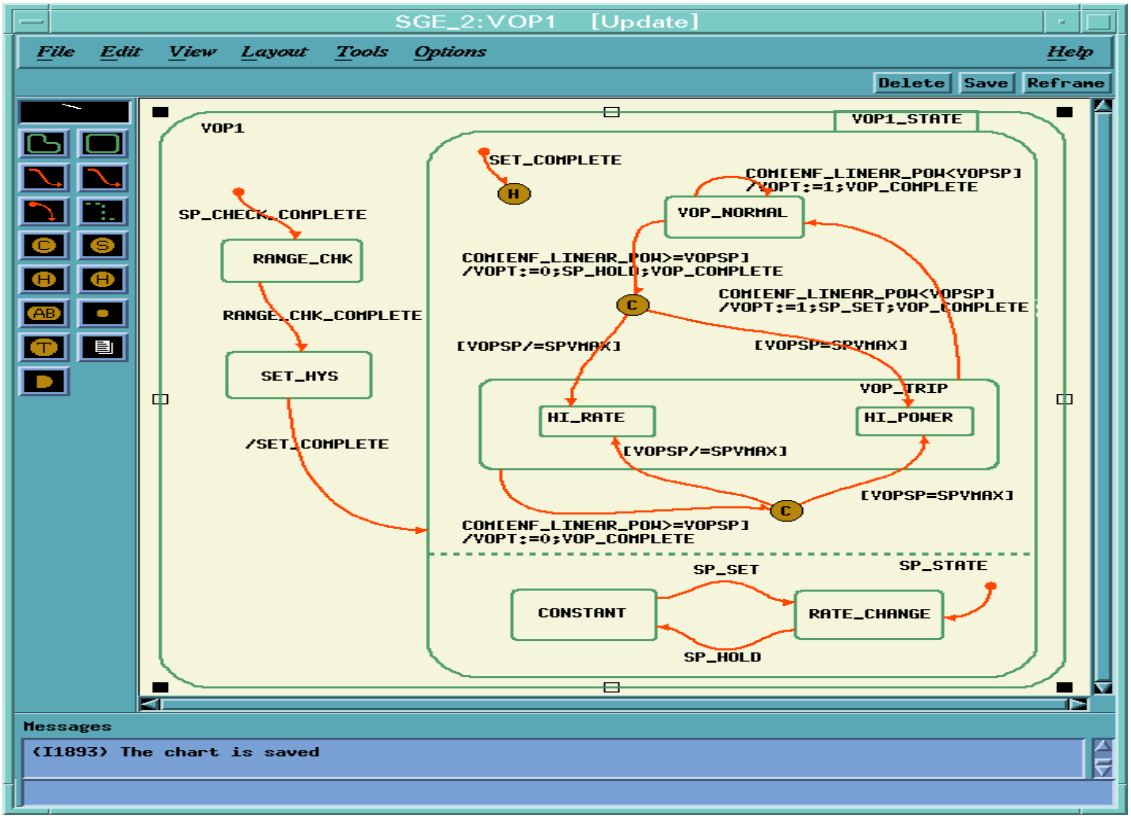


그림 9. 가변과출력 트립에 대한 State Chart

그림 9는 가변 과출력에 대한 BSP 내의 트립 알고리즘의 State Chart를 보여준다. 가변 과출력트립은 자동 비율제한형 가변 설정치 트립의 유형의 특성을 갖는다. 입력된 공정변수(ENF_LINEAR_POWER)와 가변 설정치(VOPSP)와 비교를 통해서 가변 설정치 트립에 관한 정상 및 정지를 결정한다. 가변 설정치 정지 상태에서는 중성자속의 준위 변화율이 프로그램 설정값 이상으로 증가하면 HI_RATE 상태로 전이되고 중성자속이 기 설정된 최대치에 도달하게 되면 HI_POWER 상태로 전이된다. 표 2는 서술적으로 표현한 소프트웨어 요건과 State Chart로 나타낸 형태를 보여주고 있다.

표 2 서술적 소프트웨어 요건과 정형적 요건과의 비교

번호	기능 요건	서술적 명세	State Chart 표시
1	입력신호 처리	입력변수는 히스테레시스를 수행하여 신호의 고주파 부분을 제거한다.	SET_HYS /SET_COMPLETE
2	공정변수 유효범위 검증	공정변수는 기 설정된 범위 이내에 있어야 하며, 그 범위를 초과하는 공정변수는 유효하지 않으며 하한값 또는 상한값을 할당한다.	RANGE_CHK RANGE_CHK_COMPLETE
3	공정변수와 설정치 와의 차이 (Band)	가변설정치 알고리즘은 공정입력이 상승이나 하강할 때 정지 및 예비정지 설정치를 공정입력변수와 일정한 간격을 자동으로 유지한다.	RATE_CHANGE SP_SET
4	공정변수와 설정치 비교논리	공정변수값이 설정치를 초과할 경우 트립신호 발생	C O M [ENF_LINEAR_POWER<VOPTSP] /VOPT : = 1 ; VOP_COMPLETE
5	설정치 변화율 제한 (Rate)	가변설정치 알고리즘은 설정치의 최고변화율을 제한하며, 공정입력 변수의 상승률 및 하강률에 따라서 변화율이 설정된다. 또한 정지나 예비정지에 대한 설정치 변화율은 정지나 예비정지에 관계없이 일정하다.	HI_RATE [VOPSP/=SPVMAX]
6	트립 발생후 설정치 유지	원자로 정지신호가 발생했을 때, 변화율제한형 가변설정치 알고리즘은 정지조건이 확인 및 제거될 때까지 정지 및 예비정지 설정치를 일정하게 유지한다.	CONSTANT SP_HOLD
7	설정치 상한(Ceiling) 요건	가변설정치 알고리즘의 정지 및 예비정지 최대설정치는 출력의 최대값으로 가변설정치가 가질 수 있는 최대값이다.	HI_POWER VOP_TRIP

6. 결론

원자로 안전에 매우 중요한 설비인 디지털 원자로보호계통 개발을 위해서 새로운 안전등급의 소프트웨어 개발방법이 제시되었다. 본 소프트웨어 설계 및 확인검증방법은 국가지정연구실에서 추진하고 있는 공통유형고장을 배제하기 위한 디지털 원자로보호계통 개발과제에 적용하여 고신뢰도를 요구하는 안전등급 계통의 소프트웨어를 생산하고, 그 품질을 검증하기 위해서 개발되었다.

본 논문에서 제시한 새로운 소프트웨어 개발방법의 중요 내용은 다음과 같다.

- Dynamic Simulation Tool을 이용한 보호계통 기능의 모델링 및 시뮬레이션을 통해 기능요건서의 정확성을 검증하였다.

- 서술적인 소프트웨어 요건과 함께 정형기법의 하나인 State Chart를 이용하여 소프트웨어 요건명세서를 작성하여 소프트웨어 개발단계 초기에 결함을 발견할 수 있도록 하였다.

- 계통설계단계, 소프트웨어 코딩단계, 종합시험단계 등 설계업무과정에서 3차례에 걸쳐 자동적으로 확인 및 검증업무가 수행되도록 하였다.

- 한편, 독립된 소프트웨어의 확인검증업무도 인적 오류를 최소화하기 위해 각 단계별 생산문서를 자동적으로 추적 관리할 수 있는 소프트웨어 툴을 사용함으로써, 확인검증 업무를 효과적으로 수행할 수 있게 하였다.

참고문헌

[1] Douglas M. Chapin, et al., "Digital Instrumentation and Control Systems in Nuclear Power Plant," Committee on application of Digital Instrumentation and Control System to Nuclear Power Plant Operations and Safety, National Academy Press, Washington, D.C, 1997, pp. 43 ~ 51

[2] Grady, R., "Successfully Applying Software Metrics," Computer, Vol. 27, No. 9, September 1994, pp. 18-25

[3] H.K.Shin and S.K.Nam et al, "Development of Advanced Digital Reactor Protection System Using Diverse Dual Processors to prevent Common Mode Failure," ANS NPIC and HMIT 2000, Washington D.C, November 2000

[4] NUREG/CR-6463, "Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems," June 1986.

[5] UCRL-ID-114839, "Software Reliability and Safety in Nuclear Reactor Protection Systems," Lawrence Livermore National Laboratory, June 1993, pp. 6-7

[6] KOPEC/00-TN-AQ, "공통유형고장을 배제한 고신뢰도 디지털 원자로보호계통 개발과제 1단계 중간보고서," 한국전력기술(주), September 2000

[7] KOPEC/00000-IC-SM717, "Software Development Manual for Instrumentation & Control System," 한국전력기술(주)

[8] i-Logix Inc. "Statemate MAGNUM Reference Manual," Ver. 7.0, 1996

[9] The Mathworks Inc. "Matlab Reference Manual," Ver. 5.3