고신뢰도 안전등급 제어기기 개발

Development of the High Reliable Safety PLC for the Nuclear Power Plants

손 광 섭^{*} · 김 동 훈^{*} · 손 철 웅^{**}

(Kwang-Seop Son · Dong-Hoon Kim · Choul-Woong Son)

Abstract - This paper presents the design of the Safety Programmable Logic Controller (SPLC) used in the Nuclear Power Plants, an analysis of a reliability for the SPLC using a markov model. The architecture of the SPLC is designed to have the multiple modular redundancy composed of the Dual Modular Redundancy(DMR) and the Triple Modular Redundancy(TMR). The operating system of the SPLC is designed to have the non-preemptive state based scheduler and the supervisory task managing the sequential scheduling, timing of tasks, diagnostic and security. The data communication of the SPLC is designed to have the deterministic state based protocol, and is designed to satisfy the effective transmission capacity of 20Mbps. Using Markov model, the reliability of SPLC is analyzed, and assessed. To have the reasonable reliability such as the mean time to failure (MTTF) more than 10,000 hours, the failure rate of each SPLC module should be less than $2 \times 10^{-5}/\text{hour}$. When the fault coverage factor (FCF) is increased by 0.1, the MTTF is improved by about 4 months, thus to enhance the MTTF effectively, it is needed that the diagnostic ability of each SPLC module should be strengthened. Also as the result of comparison the SPLC and the existing safety grade PLCs, the reliability and MTTF of SPLC is up to 1.6-times and up to 22,000 hours better than the existing PLCs

Key Words : Safety PLC, Non-preemptive state based scheduler, Deterministic state based protocol, Markov model, Reliability, MTTF

1. 서 론

일반적으로 원전안전계통은 원자로보호계통(RPS, Reactor Protection System), 원자로노심보호계통(RCOPS, Reactor Core Protection System), 공학적안전설비-기기제어계통(ESF-CCS, Engineered Safety Features-Component Control System), 주요변수지시 및 감시계통(QAIS-P, Qualified Indication and Alarm System-Post accident monitoring instrumentation)로 구성되고, 각 계통은 다음과 같은 기능을 수행한다[1].

- 원자로보호계통 : 안전관련 변수들을 감시하여 기 설정된 안전운전 범위를 벗어날 때, 원자로정지신호와 공학적 안전설비 개시신호를 발생
- 원자로노심보호계통 : 원자로 노심의 주요 운전변수를 입력 받아 국부출력 밀도(LPD, Local Power Density)와 핵비등 이탈율(DNBR, Departure from nucleate boiling ratio)을 계산하여 기 설정된 운전 제한치를 벗어날 때 원자로정지신호를 PPS로 출력

- 공학적안전설비-기기제어계통 : 원전 설계기준사고 발생 시 사고영향 완화를 위해 공학적안전설비(펌프, 밸브 등)를 포함한 모든 안전관련 기기들의 제어기능을 수행
- 주요변수지시 및 감시계통 : 원자로 수위 감시 및 사고 상황 시 안전계통 주요변수를 지시하고 경보를 발생

기존 원전안전계통의 경우 대부분 아날로그 기기 및 릴레이로 구성되어 운영되어 왔다. 그러나 아날로그 기기의 생산감소 및 중단에 따라 디지털 기기의 사용이 요구되어 국내에서는 2005년 상업 운전을 시작한 울진 5&6호기부터는 안전계통에도 디지털 기기인 PLC(Programmable Logic Controller) 기반의 디지털 안전계통이 설치되고 있다[2].

일반적으로 PLC는 공정제어 시스템에 사용되는 제어기기로서, 해당 PLC 모듈을 용도에 따라 조합하고 프로그램을 통해 원하는 제어 기능을 수행한다. 원전안전계통에 사용되는 PLC는 엄격한 원전 요건에 따라 설계, 제작, 시험 등 모든 과정이 일반 산업용 제어기기와는 다르게 개발되고 있다. 특히 원전안전계통에 사용되는 PLC는 Safety Critical 등급이며, 고신뢰성, 안전성이 중요한 요소로서, 이를 개선시키기 위하여 다양한 다중화 구조들이 사용된다. 원전안전계통에 사용되는 제어기기 구조는 입출력 모듈, 프로세서 모듈, 버스, 통신모듈을 단중화로 구성하고, 전원모듈만 이중화로 구성되는 구조, 프로세서 모듈과 전원 모듈만 이중화로 구성되는 구조[3], 모든 구성 모듈을 독립적 삼중화로 구성되는 구조[4] 등이 많이 사용된다. 원전안전계통에 사용되는 PLC의 운영체제 또한 한정된 자원을 효율적으로 관리하는 기능에 초점이 맞춰진 산업용 또는 산업용 PLC의 운영체제와는 다르게 안전성, 결정론성, 격리성 등이 중요한 요소로

* Principle researcher, I&C human research division, Korea Atomic Research Institute

** Researcher, I&C human research division, Korea Atomic Research Institute

† Corresponding Author : Senior researcher, I&C human research division, Korea Atomic Research Institute

E-mail : ksson78@kaeri.re.kr

Received : August 17, 2012; Accepted : December 27, 2012

[5,6] 우선순위기반의 실시간 운영체제(RTOS, Real Time Operating System)이 사용되었으나, 제어권 선점을 위한 경쟁 과정에서 무한대기와 기아상태가 발생하는 등의 불확실성이 내포되어, 원전에서 요구하는 신뢰성을 보장하기 어려웠다. 원전안전계통에 사용되는 통신 또한 운영체제와 마찬가지로 효율성에 맞춰진 산업용 통신방식과는 다르게 원전에서 요구하는 특성을 만족시키기 위하여, 제어 데이터 통신의 경우는 3.1Mbps 전송속도의 1:1 데이터 링크 방식을 사용하고, 상태 데이터 통신의 경우는 기존 산업용 통신망을 수정 보완하여 1.5Mbps의 전송속도를 갖는 통신망을 사용했으나, 성능 측면에서 만족할만한 수준을 보여주지 못했다.

본 논문에서는 기존 안전등급제어기기보다 안전성 및 성능이 개선된 SPLC(Safety Programmable Logic Controller)의 구조, 운영체제 및 통신 등의 핵심 설계사항에 대하여 기술하고, 설계된 구조에 대하여 Markov modeling을 통해 신뢰도를 분석 및 평가하고, 기존 안전등급제어기기와 신뢰도를 비교 분석하였다.

2. SPLC 설계

2.1 구조 및 다중화 보팅

2.1.1 구조

SPLC의 구성요소인 입출력 모듈, 프로세서 모듈, 통신 모듈, 전원, 버스 등에 대한 모듈 다중화는 사용자의 요구에 따라 다중화 정도를 선택할 수 있는 구조적 유연성을 갖도록 개발하였다. 즉, 능동적인 판단이나 결정이 요구되는 입출력 모듈과 프로세서 모듈은 최대 삼중화까지 구성 가능하고, 장치 고장에 대한 tolerant 기능이 요구되는 통신모듈, 버스, 전원은 이중화로 구성하였다.

그림 1 원전안전계통에 사용되는 SPLC 기본구조

Fig. 1 SPLC basic structure used in nuclear safety systems

원전안전계통은 기본적으로 독립적인 채널 4중화로 구성되므로, 각 채널 내부의 다중화는 물리적 요소보다는 다중화 구성 요소에 대한 고장과 그에 따른 출력 논리의 결정론성이 가장 중요한 요구사항이다. 따라서 SPLC는 물리적으로

간결하고, 신뢰성과 가용성을 만족하며, 미 감지 고장에 대처할 수 있도록 그림 1과 같이 단일 랙안에 삼중화를 기본 구조로 설계하였다. 즉, 입출력 모듈과 프로세서 모듈은 삼중화로 구성하고, 통신모듈, 버스는 이중화로 구성하였다. SPLC의 통신모듈은 제어 데이터 전송용과 상태 데이터 전송용으로 분리하여 설계하였고 버스는 이중화, 고속, 확장성에 강점을 갖는 결정론적 통신방식의 직렬 버스를 사용하였다.

2.1.2 다중화 보팅

다중화 모듈의 출력에 대한 최종 판단은 다음 단계인 수신 모듈에서 결정한다. 그림 1의 경우, 삼중화로 구성된 입력모듈의 출력값이 이중화된 버스를 통하여 삼중화로 구성된 프로세서 모듈로 전달되면, 각 프로세서 모듈은 다중화 보팅 논리를 통하여 삼중화된 입력 모듈들의 값을 결정한다. 또한, 프로세서 모듈의 출력값은 수신모듈인 출력모듈에 의해서 결정된다. 삼중화와 이중화 조합에 의해서 구성된 SPLC의 구체적인 보팅 방법은 다음과 같다.

2.1.2.1 이중화 모듈

Hot-standby 개념의 이중화 구조를 갖는 버스, 통신 모듈의 고장에 따른 절환은 수신모듈에서 수행된다. 즉, 버스, 통신 모듈의 수신 모듈은 박동신호, CRC(Cyclic Redundancy Check) 등의 진단기능을 수행하여 송신모듈 및 경로의 고장 여부를 판단하고, 양쪽 모두 고장 발생이 없을 시에는 Primary로 부터의 데이터를 이용하고, Primary의 고장을 감지하면, Secondary 모듈의 값을 이용한다. 이중화 모듈 모두 고장이 감지될 경우에는 미리 설정된 일정한 값을 출력한다. 원전 안전계통의 경우, 다중화 모듈이 모두 고장 시에는 일반적으로, 안전 조치(Safe Action)을 위한 출력을 생성한다.

2.1.2.2 삼중화 모듈

입출력 모듈과 프로세서 모듈과 같은 삼중화 모듈의 보팅 방법은 그림 2와 같다. 진단 모듈의 고장이 감지되지 않았을 경우, 수신된 3개의 값에 대하여 디지털 값인 경우 2/3 보팅 논리를 수행하고, 아날로그 값인 경우는 중간값을 설정한다. 만약 진단 모듈 고장이 한 개 이상 감지되면 고장난 모듈의 값을 제외하고 보팅 논리를 수행하되, 감지된 고장 모듈의 개수와 미 고장 모듈의 값 또는 상태에 따라 출력값이 결정된다.

2.2 운영체제 및 데이터 통신

SPLC의 운영체제는 비선점형 상태기반 운영체제로, 그림 3과 같이 커널(Kernel), IHS(Interrupt Handling System), Supervisory 및 시스템 태스크로 구성된다. 운영체제는 프로세서 모듈, 입출력 모듈, 통신 모듈 등의 SPLC 구성 모듈과 응용 프로그램 개발을 위한 프로그램 도구인 SET(Software Engineering Tool)과 주기적으로 통신한다.

상용 실시간 운영체제(RTOS)의 우선순위 기반 스케줄링은 제어권 선점을 위한 경쟁 과정에서 무한대기와 기아상태가 발생하는 등의 불확실성이 내포되어, 원전 안전등급 제어

그림 2 삼중화 모듈의 보팅방법

Fig. 2 Voting method of Triple Modular Redundancy(TMR)

기기에 적용 시 신뢰성을 보장하기 어렵다. 따라서 원전 특성이 고려되고 결정론적인 기능을 수행하는 실시간 운영체제를 개발하였다.

그림 3 운영체제 구조

Fig. 3 Architecture of operating system

SPLC 운영체제는 결정론성을 위하여, 그림 3의 Supervisory 기능을 개발하였다. Supervisory는 결정론적인 스케줄링 기능과 태스크의 순차적 실행이 가능하도록 태스크와 시간을 제어한다. Supervisory의 스케줄링 기능은 실행 중인 태스크가 다른 태스크에 선점되지 않는 비선점형의 상태기반 방식으로 실행된다. 각 태스크는 최소 분해능인 Tick의 배수로 수행시간이 할당되며, 매 주기마다 순차적으로 실행된다. 또한, Supervisory는 프로세서모듈의 내부 진단 기능과 보안기능 등 운영체제의 전반적인 주요 기능들을 제어 및 관리한다.

2.3 데이터 통신

SPLC용 데이터 통신은 상태기반의 결정론적 통신방식으로 전송지연시간은 50msec, 실패 전송용량은 20Mbps를 만족시키도록 개발 하였다. 프로토콜 구조는 IEEE 802.3 100Mbps의 물리계층과 주기적이면서 전송보장이 요구되는 보장형 시분할 방식(GTS:Guaranteed Time Slot)의 MAC(Medium Access Control) 계층과 데이터 분할, 망 가입과 탈퇴 기능을 수행하는 Network 계층으로 구성된다[7]. 통신망 구조는 그림 4와 같이 메시지 교환 및 망 관리 기능

그림 4 통신망 구조

Fig. 4 Structure of communication networks

을 수행하는 통신 교환 장치와 메시지 송수신 기능을 수행하는 통신노드장치로 구성되고, 데이터 송수신 및 스위칭을 수행하는 각 장치의 핵심기능은 FPGA(Field Programmable Gate Array)로, 진단 및 감시 기능은 CPU(Central Process Unit)로 각각 구현하였다.

그림 4와 같이 구현된 통신노드장치와 통신교환장치(CSW, Central Switch, GSW, Group Switch)를 이용하여 그림 5와 같이 시험환경을 구축하였다. 구축된 시험환경을 토대로 기본적인 통신 기능 시험과 최대전송용량 분석을 위하여 전송지연시간 및 통신교환장치의 스위칭시간을 측정하였다. 각 통신노드장치(그림 5의 PLC, PC 해당)는 50 msec의 주기로 114 Byte의 데이터를 해당 통신노드장치로 전송한다. 오실프로스코프를 이용하여 114 Byte에 전송지연시간을 측정한 결과, 28 usec로 전송된 데이터의 Dummy 비트를 고려하면, 대략 1 Byte의 전송 지연 시간은 240 nsec이다.(그림 6 참조) 또한 통신교환장치의 114 Byte에 대한 스

그림 5 통신망 시험환경

Fig. 5 Test bed of communication networks

그림 6 114 Byte 대한 전송지연시간

Fig. 6 Transmission delay for 114 Byte

그림 7 114 Byte 대한 스위칭 시간

Fig. 7 Switching time for 114 Byte

위칭 시간을 측정한 결과 27.4 usec로 대략 1 Byte 스위칭 시간은 240 nsec이다.(그림 7 참조)

원전안전계통의 통신노드장치는 최소 64개 이상을 필요로 하므로[8], 그림 8과 같이 9개의 통신교환장치와 64개의 통신노드장치로 통신망을 구성하고, 각 통신노드장치들이 50 msec의 주기로 2048 Byte로 데이터를 전송한다면 총 지연 시간은 다음과 같이 계산된다.

그림 8 64개 통신노드장치를 이용한 통신망 구성

Fig. 8 Configuration of communication networks using 64 nodes

- $t1 = 2048\text{Byte} \times 240\text{ns} + 2048\text{Byte} \times 8(\text{GSW 1개에 연결된 통신노드장치 개수}) \times 240\text{ns} = 4.423\text{msec}$
- $t2 = 2048\text{Byte} \times 240\text{ns} + 2048\text{Byte} \times 8(\text{GSW 1개에 연결된 통신노드장치 개수}) \times 8(\text{CSW에 연결된 GSW장치 개수}) = 31.948\text{msec}$
- $t3 = t1$
- $t4 = 2048\text{Byte} \times 240\text{ns} = 0.5\text{msec}$

제안한 통신방식은 시분할 통신방식이므로, 전체 시간동기를 위한 비콘 전송시간은 2msec, GTS #1=5msec, GTS #2=33msec, GTS #3=5msec, GTS #4=1msec로 설정가능하다. 따라서 총 지연시간은 46msec이므로 최대 전송용량은 다음과 같이 계산된다.

- $\text{최대전송용량} = (2048\text{Byte}) \times 8 \times 8 \times 1000 / 46 = 22.8\text{Mbps}$

3. SPLC 신뢰도 분석

3.1 마코프 모델

본 절에서는 신뢰도 분석을 위하여 SPLC를 비롯한 기존 안전등급 제어기기들(단중화 제어기기, 프로세서 이중화 제어기기, 독립 삼중화 제어기기)에 대한 마코프 모델링 방법에 대하여 기술하고자 한다.

3.1.1 이중화와 삼중화 모듈

이중화와 삼중화 모듈은 위에서 언급한 안전등급 제어기기에 모두 사용되는 다중화 구성 방식으로, 이들 모듈에 대한 마코프 모델링 후 SPLC를 비롯한 안전등급 제어기기들에 대한 마코프 모델링을 하고자 한다.

3.1.1.1 이중화 모듈

그림 9는 FCF(Fault Coverage Factor)를 고려한 이중화 모듈 구성에 대한 마코프 모델을 보여준다. 2.1.2.1에서 설명한 바와 같이, 이중화 모듈은 Primary 모듈의 고장이 미 감지되거나 Primary 모듈 및 Secondary 모듈이 모두 고장상태이면 이중화 모듈은 고장 상태가 된다. 그리고 Primary 모듈의 고장이 발견되고 Secondary 모듈이 정상상태(Normal state)이거나, Primary 모듈이 정상상태이고 Secondary 모듈이 정상 혹은 고장상태이면 이중화 모듈은 정상상태가 된다.

그림 9 이중화 모듈의 마코프 모델

Fig. 9 Markov model for DMR

구성 모듈의 고장률을 λ , FCF를 C 라고 할 때, 이중화 모듈의 상태방정식은 다음과 같이 표현된다.

$$\frac{d}{dt} \begin{bmatrix} P_2(t) \\ P_{1p}(t) \\ P_{1s}(t) \\ P_F(t) \end{bmatrix} = \begin{bmatrix} -2\lambda & 0 & 0 & 0 \\ \lambda & -\lambda & 0 & 0 \\ \lambda & 0 & -\lambda & 0 \\ 0 & \lambda & \lambda & 0 \end{bmatrix} \begin{bmatrix} P_2(t) \\ P_{1p}(t) \\ P_{1s}(t) \\ P_F(t) \end{bmatrix} \quad (1)$$

여기서 $P_x(t)$ 는 시간이 t 일 때, x 상태가 될 확률로, 이중화 모듈이 정상일 확률은 고장상태를 제외한 P_2, P_{1p}, P_{1s} 를 모두 합한 확률로 표현된다. (1)의 상태 방정식의 초기조건은 $t=0$ 일 때, 이중화 모듈은 Primary 모듈과 Secondary 모듈 모두 고장이 발생하지 않은 상태로 다음과 같이 주어진다.

$$[P_2(0) P_{1p}(0) P_{1s}(0) P_F(0)] = [1000] \quad (2)$$

(1), (2)를 이용하여 이중화 모듈이 정상일 확률, 즉 신뢰도는 다음과 같다.

$$R_{DMR} = P_2(t) + P_{1p}(t) + P_{1s}(t) = \frac{e^{\lambda t} - C + Ce^{\lambda t}}{e^{2\lambda t}} \quad (3)$$

여기서, DMR : Dual Modular Redundancy(이중화 모듈)를 의미한다.

이중화 모듈의 고장률 함수는 정의[9]에 따라 다음과 같이 구해진다.

$$\Lambda_{DMR} = -\frac{dR_{DMR}/dt}{R_{DMR}} = \lambda - \frac{C\lambda}{e^{\lambda t} - C + Ce^{\lambda t}} \quad (4)$$

3.1.1.2 삼중화 모듈

그림 10은 FCF를 고려한 삼중화 모듈 구성의 마코프 모델을 보여준다. 2.1.2.2에서 설명한 바와 같이, 삼중화 모듈은 고장 미감지의 경우, 1개 고장은 정상 상태가 되지만, 2개 고장부터는 고장상태가 된다. 고장 감지의 경우는 2개 고장을 모두 감지하면 정상상태가 되지만, 1개 고장은 감지하고 1개 고장이 미 감지되면 고장상태가 된다.

그림 10 삼중화 모듈의 마코프 모델

Fig. 10 Markov model for TMR

그림 10의 마코프 모델을 이용한 삼중화 모듈의 상태 방정식은 다음과 같다.

$$\frac{d}{dt} \begin{bmatrix} P_3(t) \\ P_{UD}(t) \\ P_2(t) \\ P_1(t) \\ P_F(t) \end{bmatrix} = \begin{bmatrix} -3\lambda & 0 & 0 & 0 & 0 \\ 3\lambda(1-C) & -2\lambda & 0 & 0 & 0 \\ 3\lambda C & 0 & -2\lambda & 0 & 0 \\ 0 & 0 & 2\lambda C & -\lambda & 0 \\ 0 & 2\lambda & 2\lambda(1-C) & \lambda & 0 \end{bmatrix} \begin{bmatrix} P_3(t) \\ P_{UD}(t) \\ P_2(t) \\ P_1(t) \\ P_F(t) \end{bmatrix} \quad (5)$$

삼중화 모듈의 초기화 조건은 이중화 모듈과 마찬가지로 다음과 같이 주어진다.

$$[P_3(0) P_{UD}(0) P_2(0) P_1(0) P_F(0)] = [10000] \quad (6)$$

(5)와 (6)을 이용하여 삼중화 모듈의 시간에 따른 신뢰도 함수를 구하면 다음과 같다.

$$R_{TMR}(t) = P_3(t) + P_{UD}(t) + P_2(t) + P_1(t) = \frac{3e^{\lambda t} + 3C^2 - 6C^2e^{\lambda t} + 3C^2e^{2\lambda t} - 2}{e^{3\lambda t}} \quad (7)$$

여기서 TMR : Triple Redundancy Module(삼중화 모듈)를 의미한다. 삼중화 모듈의 고장률 함수는 다음과 같이 구할 수 있다.

$$\Lambda_{TMR}(t) = -\frac{dR_{TMR}/dt}{R_{TMR}} = \frac{3\lambda(e^{\lambda t} - 1)(C^2 e^{\lambda t} - 3C^2 + 2)}{3e^{\lambda t} + 3C^2 - 6C^2 e^{\lambda t} + 3C^2 e^{2\lambda t} - 2} \quad (8)$$

3.1.2 단중화 제어기기

단중화 제어기기는 입출력 모듈, 프로세서 모듈, 통신 모듈, 버스가 단중화로 구성되고, 전원 모듈만 이중화로 구성된 제어기기로 신뢰도 블록 다이어그램(RBD, Reliability Block Diagram)은 그림 11과 같다.

그림 11 단중화 제어기기의 신뢰도 블록 다이어그램

Fig. 11 RBD of simplex PLC

그림 12 단중화 제어기기의 마코프 모델

Fig. 12 Markov model of simplex PLC

단중화 제어기기는 단중화로 구성된 모듈의 고장이 발생하거나, 이중화 모듈인 전원 모듈의 고장이 발생하면 고장상태가 되므로 마코프 모델링하면 그림 12와 같다. 그림 12에서 보는 바와 같이 전원 모듈은 이중화 모듈로 구성되므로 그림 9의 마코프 모델을 이용하고, 단중화로 구성되는 모듈들 중 고장이 하나라도 발생하면 고장상태가 되기 때문에 단중화 제어기기의 신뢰도 함수는 다음과 같이 표현된다.

$$R_{simplex} = e^{-\int (\Lambda_{simplex} + \Lambda_{par}) dt} = e^{-\Lambda_{simplex} t} \left(\frac{2\mathcal{C}e^{\lambda_{par}t} - 2\mathcal{C} + 1}{2\mathcal{C}e^{\lambda_{par}t}} \right) \quad (9)$$

$$\text{여기서 } A_{pwr} = \lambda_{pwr} - \frac{C\lambda_{pwr}}{e^{\lambda_{pwr}t} - C + Ce^{\lambda_{pwr}t}},$$

$$\begin{aligned} \lambda_{simplex} &= \lambda_{ai} + \lambda_{di} + \lambda_{ao} + \lambda_{do} + \lambda_{bus} + \lambda_{sc} + \lambda_{ssc} + \lambda_{pro}, \\ \lambda_{ai} &= \text{아날로그 입력 모듈의 고장률}, \lambda_{di} = \text{디지털 입력 모듈의 고장률}, \\ \lambda_{do} &= \text{디지털 출력 모듈의 고장률}, \lambda_{bus} = \text{버스의 고장률}, \end{aligned}$$

 λ_{scc} = 안전제어 통신 모듈의 고장률,

λ_{ssc} = 안전상태 통신모듈의 고장률, λ_{pro} = 프로세서 모듈의 고장률이다.

3.1.3 프로세서 이중화 제어기기

프로세서 이중화 제어기기는 프로세서 모듈, 전원 모듈만 이중화로 구성되고 나머지 모듈은 단중화로 구성된 제어기기로 신뢰도 블록 다이어그램은 그림 13과 같다.

그림 13 프로세서 이중화 제어기기의 신뢰도블록다이어그램

Fig. 13 RBD of processor DMR PLC

그림 14 프로세서 이중화 제어기기의 마코프 모델

Fig. 14 Markov model of processor DMR PLC

프로세서 이중화 제어기기는 이중화 구성된 프로세서 모듈이나 전원 모듈의 고장이 발생하거나, 단중화로 구성된 모듈의 고장이 발생하면 고장상태가 되기 때문에 마코프 모델은 그림 14와 같이 표현된다. 그림 14를 이용하여 프로세서 이중화 제어기기의 신뢰도 함수를 구하면 다음과 같다.

$$R_{P,DMR} = e^{-\int (A_{P,DMR} + A_{PMR} + A_{PRO})dt} = e^{-A_{P,DMR}t} \left(\frac{2C\epsilon^{\lambda_{PMR}} - 2C + 1}{e^{2\lambda_{PMR}t}} \right) \left(\frac{2C\epsilon^{\lambda_{PRO}} - 2C + 1}{e^{2\lambda_{PRO}t}} \right) \quad (10)$$

여기서 $\Lambda_{PDMR} = \lambda_{ai} + \lambda_{di} + \lambda_{ao} + \lambda_{do} + \lambda_{bus} + \lambda_{scr} + \lambda_{ssc}$,

$$A_{PWR} = \lambda_{pwr} - \frac{C\lambda_{pwr}}{e^{\lambda_{pwr}t} - C + C e^{\lambda_{pwr}t}}, \quad A_{PRO} = \lambda_{pro} - \frac{C\lambda_{pro}}{e^{\lambda_{pro}t} - C + C e^{\lambda_{pro}t}}$$

이다.

3.1.4 독립 삼중화 제어기기

독립 삼중화 제어기기는 모든 구성모듈들이 독립적 삼중화로 구성된 모듈로 출력단의 Voter에 의해서 최종 출력값이 결정되는 제어기이다. 독립 삼중화 제어기기의 신뢰도 블록 다이어그램은 그림 15와 같다. 세 개의 독립된 그룹

제어기기로 구성된 독립 삼중화 제어기기는 각 구성모듈의 고장은 해당 그룹 제어기기를 고장 상태로 만들지만, 독립 삼중화 제어기기는 고장상태로 만들지 않는다. 즉 독립 삼중화 제어기기의 고장은 세 개의 독립된 그룹 제어기기의 고장상태에 따라 결정되며, 그 결정논리는 앞에서 기술한 삼중화 제어기기의 마코프 모델과 동일하다. 단지 삼중화 제어기기의 모듈 고장률이 그룹 제어기기 고장률로 바뀌었을 뿐이다.

그림 15 독립 삼중화 제어기기의 신뢰도블록다이아그램
Fig. 15 RBD of processor independent TMR PLC

그림 16 독립 삼중화 제어기기의 마코프 모델
Fig. 16 Markov model of independent TMR PLC

독립 삼중화 제어기기의 마코프 모델은 그림 16과 같고, 이를 이용하여 신뢰도 함수를 구하면 다음과 같다.

$$R_{ITMR} = e^{-\int (\lambda_{ITMR} + \lambda_{voter}) dt} = \left(\frac{3e^{\lambda_{ITMR} t} + 3C^2 - 6C^2 e^{\lambda_{ITMR} t} + 3C^2 e^{2\lambda_{ITMR} t} - 2}{e^{3\lambda_{ITMR} t}} \right) e^{-\lambda_{voter} t} \quad (11)$$

$$\text{여기서 } \lambda_{ITMR} = \frac{3\lambda_{ITMR,G}(e^{\lambda_{ITMR} t} - 1)(C^2 e^{\lambda_{ITMR} t} - 3C^2 + 2)}{3e^{\lambda_{ITMR} t} + 3C^2 - 6C^2 e^{\lambda_{ITMR} t} + 3C^2 e^{2\lambda_{ITMR} t} - 2},$$

$$\lambda_{ITMR,G} = \lambda_{ai} + \lambda_{di} + \lambda_{ao} + \lambda_{do} + \lambda_{bus} + \lambda_{scc} + \lambda_{ssc} + \lambda_{pro} + \lambda_{pwr}$$

이다.

3.1.5 SPLC

SPLC는 입출력 모듈, 프로세서 모듈은 삼중화로 구성하고, 버스, 통신, 전원 모듈은 이중화로 구성된 제어기기로 신뢰도 블록 다이어그램은 그림 17과 같다.

그림 17 SPLC의 신뢰도 블록 다이어그램
Fig. 17 RBD of SPLC

그림 18 SPLC의 마코프 모델
Fig. 18 Markov model of SPLC

이중화로 구성되는 모듈의 마코프 모델은 그림 9를 이용하고, 삼중화로 구성되는 모듈의 마코프 모델은 그림 10을 이용하면 SPLC의 마코프 모델은 그림 18과 같다. 그림 18에서 보는 바와 같이 SPLC는 이중화 및 삼중화 모듈의 고장이 하나라도 발생하거나 최종 출력단인 Voter의 고장이 발생하면 고장상태가 된다.

그림 18의 마코프 모델을 이용하여 SPLC의 시간에 따른 신뢰도 함수를 구하면 다음과 같다.

$$R_{SPLC} = e^{-\int \Lambda_{SPLC} dt} = e^{-\int \sum_{i=1}^{10} \Lambda_i + \lambda_{voter} dt} \quad (12)$$

$$= \prod_{i=1}^5 \left(\frac{3e^{\lambda_i t} + 3C^2 - 6C^2 e^{\lambda_i t} + 3C^2 e^{2\lambda_i t} - 2}{e^{3\lambda_i t}} \right) \times \prod_{i=6}^{10} \left(\frac{e^{\lambda_i t} - C + C e^{\lambda_i t}}{e^{2\lambda_i t}} \right) e^{-\lambda_{voter} t}$$

여기서 $\Lambda_{SPLC} = \Lambda_{AI} + \Lambda_{DI} + \Lambda_{PRO} + \Lambda_{AO} + \Lambda_{DO} + \Lambda_{IOBUS} + \Lambda_{CBUS} + \Lambda_{SCC} + \Lambda_{SSC} + \Lambda_{PWR} + \lambda_{voter}$ 이고, Λ_i , λ_i 는 다음과 같다.

$$\begin{bmatrix} \Lambda_1 \\ \Lambda_2 \\ \Lambda_3 \\ \Lambda_4 \\ \Lambda_5 \\ \Lambda_6 \\ \Lambda_7 \\ \Lambda_8 \\ \Lambda_9 \\ \Lambda_{10} \end{bmatrix} = \begin{bmatrix} \Lambda_{AI} \\ \Lambda_{DI} \\ \Lambda_{PRO} \\ \Lambda_{AO} \\ \Lambda_{DO} \\ \Lambda_{IOBUS} \\ \Lambda_{CBUS} \\ \Lambda_{SCC} \\ \Lambda_{SSC} \\ \Lambda_{PWR} \end{bmatrix}, \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \\ \lambda_4 \\ \lambda_5 \\ \lambda_6 \\ \lambda_7 \\ \lambda_8 \\ \lambda_9 \\ \lambda_{10} \end{bmatrix} = \begin{bmatrix} \lambda_{ai} \\ \lambda_{di} \\ \lambda_{pro} \\ \lambda_{ao} \\ \lambda_{do} \\ \lambda_{iobus} \\ \lambda_{cbus} \\ \lambda_{scc} \\ \lambda_{ssc} \\ \lambda_{pwr} \end{bmatrix} \quad (13)$$

3.2 SPLC 신뢰도 및 평균고장시간 분석

3.2.1 신뢰도 분석

그림 19 구성모듈들의 고장률(λ)에 따른 신뢰도
Fig. 19 Reliability depending on failure rate of modules

식(12)을 이용하여 구성 모듈들의 고장률(λ)에 따른 신뢰도 그래프는 그림 19와 같다. 원전안전계통에 사용되는 안전등급 제어기기의 FCF는 일반적으로 0.9 이상을 요구하므로, FCF=0.9로 가정 하였다. 그림 19에서 보는 바와 같이, 구성 모듈들의 고장률이 $10^{-4}/hour$ 이상이 되면 시간에 따라 급격하게 감소한다. 따라서 SPLC 구성 모듈들의 고장률은 최대 $10^{-5}/hour$ 이하이어야 한다.

3.2.2 평균고장시간 분석

평균고장시간(MTTF, Mean Time To Failure) 식(14)와 같이 정의된다[10]. 식(14)를 이용하여 FCF=0.9일 때, 구성 모듈들의 고장률에 따른 평균고장시간은 그림 20과 같다.

$$MTTF = \int_0^{\infty} R(t) dt \quad (14)$$

여기서 $R(t)$ 는 신뢰도 함수이다.

개량형 원전안전등급 제어기기의 평균고장시간은 10,000 시간 이상을 요구하므로[9], 이 요건을 만족시키기 위해서는 구성 모듈들의 고장률이 $2 \times 10^{-5}/hour$ 이하가 되어야 한다.

그림 20 구성모듈들의 고장률(λ)에 따른 평균고장시간
Fig. 20 MTTF depending on failure rate of modules

$$\begin{bmatrix} \lambda_{ai} \\ \lambda_{di} \\ \lambda_{pro} \\ \lambda_{ao} \\ \lambda_{do} \\ \lambda_{iobus} \\ \lambda_{cbus} \\ \lambda_{scc} \\ \lambda_{ssc} \\ \lambda_{pwr} \\ \lambda_{voter} \end{bmatrix} = \begin{bmatrix} 4.49/10^6 hour \\ 7.72/10^6 hour \\ 7.78/10^6 hour \\ 5.83/10^6 hour \\ 6.11/10^6 hour \\ 8.4/10^6 hour \\ 8.4/10^6 hour \\ 6.88/10^6 hour \\ 3.44/10^6 hour \\ 5.44/10^6 hour \\ 6.23/10^6 hour \end{bmatrix} \quad (15)$$

그림 21은 구성모듈들의 고장률이 식(15)과 같이 기존 안전등급 제어기기에 사용되었던 고장률[11]이고, 원전안전계통의 정비(Overhaul)가 18개월마다 수행되므로, $t=18$ 개월 일 때, FCF에 따른 평균고장시간을 나타내는 그래프이다. FCF가 각각 0, 1일 때, 평균고장시간은 19,000시간, 50,000시간으로 FCF가 0.1씩 증가함에 따라 평균고장시간은 약 4개월 정도 증가한다. 따라서 평균고장시간을 효과적으로 증가시키기 위해서는, FCF를 좌우하는 각 구성모듈들의 진단능력 강화가 필요하다.

그림 21 FCF에 따른 평균고장시간
Fig. 21 MTTF depending on FCF

4. 다른 제어기기와의 신뢰도 및 평균고장시간 비교 분석

본 장에서는 3.1절에서 구한 신뢰도 함수를 바탕으로 원전안전계통에 사용되는 단중화 제어기기, 프로세서 이중화 제어기기, 독립 삼중화 제어기기, SPLC에 대한 신뢰도 및 평균고장시간을 비교 분석하고자 한다.

4.1 신뢰도 비교 분석

4.1.1 시간에 따른 신뢰도 비교 분석

그림 22 시간에 따른 신뢰도 비교
Fig. 22 Reliability comparison depending on time

그림 22는 기존 안전등급 제어기기와 SPLC에 대하여 시간에 따른 신뢰도를 비교한 그래프이다. 각 구성모듈의 고장률은 식(15)를 이용하고 FCF는 0.9라고 가정하였다. $t=18$ 개월 일 때, 각 제어기기의 신뢰도는 표 1과 같다.

표 1 $t=18$ 개월 일 때, 신뢰도 비교

Table 1 Reliability comparison when $t=18$ months

제어기기 종류	단중화	프로세서 이중화	독립 삼중화	SPLC
신뢰도	0.51	0.56	0.73	0.84

표 1에서 보는 바와 같이 SPLC의 신뢰도는 단중화 제어기기보다 약 1.65배, 프로세서 이중화 제어기기보다 1.5배, 독립 삼중화 제어기기보다 1.15배 정도 우수함을 알 수 있다.

4.1.2 고장률에 따른 신뢰도 비교 분석

그림 23 고장률 따른 신뢰도 비교

Fig. 23 Reliability comparison depending on failure rate

표 2 신뢰도=0.8일 때, 요구되는 고장률 비교

Table 2 Reliability comparison when $t=18$ months

제어기기 종류	단중화	프로세서 이중화	독립 삼중화	SPLC
고장률	2.1×10^{-5} /hour	2.3×10^{-5} /hour	5×10^{-5} /hour	8×10^{-5} /hour

그림 23은 고장률에 따른 신뢰도를 비교한 그래프로써, $t=18$ 개월, $FCF=0.9$ 라 가정하였다. 그림 23에서 보는 바와 같이 각 제어기기들은 고장률이 10^{-5} 보다 크면 신뢰도가 급격하게 감소하게 되고, 고장률이 10^{-4} 이후부터는 신뢰도가 거의 0으로 근접하게 됨을 알 수 있다. 그림 22에서 $t=18$ 개월 일 때, SPLC의 신뢰도가 대략 0.8이므로, 신뢰도가 0.8일 때 요구되는 각 구성모듈의 고장률은 표 2와 같다.

SPLC의 각 구성모듈들은 단중화보다 4배, 프로세서 이중

화보다 3.5배, 독립 삼중화보다 1.6배 더 많은 고장이 발생해도 신뢰도 0.8을 유지할 수 있다.

4.1.3 FCF에 따른 신뢰도 비교 분석

그림 24는 FCF에 따른 신뢰도를 비교한 그래프로써, 각 제어기기의 구성모듈의 고장률은 식 (15)를 이용했고, $t=18$ 개월이라 가정하였다. 그림 24에서 보는 바와 같이 SPLC는 FCF 전 구간에서 다른 제어기기보다 우수한 신뢰도 특성을 보인 반면, 독립 삼중화 제어기기는 FCF가 0.4보다 작으면 단중화 제어기기 및 프로세서 이중화 제어기기보다 오히려 낮은 신뢰도를 보여준다. 또한 프로세서 이중화 제어기기도 FCF가 0.2보다 작으면 단중화 제어기기보다 신뢰도가 낮다. 따라서 SPLC를 제외한 제어기기들은 설계 시, FCF를 좌우하는 고장 감지, 진단에 세심한 주의가 필요하다.

그림 24 FCF 따른 신뢰도 비교

Fig. 24 Reliability comparison depending on FCF

4.2 평균고장시간 비교 분석

4.2.1 고장률에 따른 평균고장시간 비교 분석

그림 25 고장률 따른 평균고장시간 비교

Fig. 25 MTTF comparison depending on failure rate

그림 25는 고장률에 따른 평균고장시간을 보여주는 그래프로써, FCF=0.9라 가정하였다. 그래프에서 보는 바와 같이 고장률 전 구간에서 다른 제어기기보다 우수한 평균고장시간 특성을 보인다. 독립 삼중화 제어기기는 그림 22에서와 같이 신뢰도 관점에서는 $t=18$ 개월 일 때, 프로세서 이중화, 단중화 제어기기보다 우수한 신뢰도 특성을 보이지만, 그림 25와 같이 평균고장시간 관점에서는 프로세서 이중화, 단중화 제어기기와 비슷한 특성을 갖는다.

4.2.2 FCF에 따른 평균고장시간 비교 분석

그림 26은 FCF에 따른 평균고장시간을 보여주는 그래프로써, 각 제어기기의 구성모듈의 고장률은 식(15)를 이용하였다. 그래프에서 보는 바와 같이 SPLC의 평균고장시간은 FCF 전 구간에 걸쳐 다른 제어기기보다 우수한 특성을 보인다. 독립 삼중화 제어기기는 FCF가 0.55보다 작으면 오히려 프로세서 이중화, 단중화 제어기기의 평균고장시간보다 낮음을 알 수 있고, 프로세서 이중화 제어기기는 FCF가 0.3보다 작으면 단중화 제어기기보다 낮은 평균고장시간을 갖는다. FCF=0.9일 때 각 제어기기의 평균고장시간은 표 3과 같다.

그림 26 FCF 따른 평균고장시간 비교

Fig. 26 MTTF comparison depending on FCF

표 3에서 보는 바와 같이 SPLC의 평균고장시간은 단중화 제어기기보다 약 22,000시간, 프로세서 이중화 제어기기보다 20,000시간, 독립 삼중화 제어기기보다 16,000시간 우수함을 알 수 있다.

표 3 FCF=0.9일 때, 평균고장시간 비교

Table 3 MTTF comparison when FCF=0.9

제어기기 종류	단중화	프로세서 이중화	독립 삼중화	SPLC
평균고장 시간 (hours)	19,250	21,080	25,750	41,630

5. 결 론

본 논문에서는 원전 안전계통 적용을 목적으로 개발되고 있는 고 신뢰도 제어기기인 SPLC의 구조, 운영체제, 통신등의 핵심모듈에 대한 설계사항과 설계된 구조의 신뢰도 및 평균고장시간을 분석, 평가하고 기존 안전등급 제어기기들과 비교 분석하였다.

SPLC는 구성 모듈의 다중화 정도를 사용자 요구에 따라 최대 삼중화까지 구성 가능한, 구조적 유연성을 갖도록 설계되었다. 특히, SPLC는 안전계통 적용을 목적으로, 고 신뢰도와 안전성은 물론, 구조적 단순화와 연계의 간결성을 위하여 단일 랙상의 삼중화를 기본 구조로 설계되었다. 능동적인 판단을 요구하는 입출력, 프로세서 모듈은 삼중화로 구성하고, 장치 고장에 대한 tolerant 기능이 요구되는 버스, 통신, 전원 모듈은 이중화로 구성하였다. 이중화 모듈의 경우에는 수신측 고장감지에 의한 절환을, 삼중화 모듈은 고장감지에 따른 제거와 논리조합을 다중화 보팅 방법으로 제시하였다. SPLC의 운영체제는 비선점형 상태기반 운영체제로, Supervisory 태스크에 의해 모든 태스크에 대한 순차적인 스케줄링, 시간관리, 시스템 진단 및 보안 기능이 수행됨으로서 운영체제에 대한 결정론성을 확보하였다. SPLC 통신은 상태기반의 결정론적 통신방식으로, 실효 전송용량이 20Mbps 이상인 원전용 고속 통신망 모듈로 설계하였다.

개발된 모듈과 구조에 대한 신뢰도 분석을 수행하였으며, 마코프 모델을 이용한 SPLC의 신뢰도 및 평균고장시간을 분석한 결과, SPLC 각 구성모듈의 고장률은 최대 $2 \times 10^{-5}/\text{hour}$ 이하이어야 하며, FCF의 증가에 따라 신뢰도는 4개월만큼 증가하므로 이를 위한 진단능력의 강화가 신뢰도의 핵심임을 제시하였다. 또한 SPLC의 신뢰도는 기존 안전등급 제어기기보다 최대 1.65배, 평균고장시간은 22,000시간 우수함을 마코프 모델을 이용하여 정량적으로 입증하였다.

감사의 글

본 연구는 지식경제부의 재원으로 한국에너지평가기술원의 원자력 기술 사업의 지원을 받아 수행한 연구과제(No. 2010161010001G)입니다.

참 고 문 헌

- [1] (2010). [On-line]. http://www.nstc.go.kr/_custom/nstc/_common/board/download.jsp?
- [2] K. C. Kwon, D. Y. Lee, C. H. Kim, C. H. Choi, "Development of Nuclear Safety Grade PLC.", in Nuclear industry, p.43-47, Feb. 2007.
- [3] S. J. Hwang, S. H. Song, Y. H. No, D. H. Yun, G. M. Park, M. G. Kim, K. C. Choi, U. T. Lee, "The Interface Between Redundant Processor Modules of Safety Grade PLC Using Mass Storage DPRAM", Transaction of the Korea Nuclear Society Autumn Meeting, p.1209-1210, Oct. 2010.
- [4] (2012). [On-line]. iom.invensys.com/EN/pdfLibrary/ProductSpec_Triconex_Tricon_03-10.pdf
- [5] K. Y. Cha, J. Y. Kim, J. S. Lee, S. W. Cheon, K. C. Kwon, "Software Qualification of a Programmable Logic Controller for Nuclear Instrumentation and Control Applications", Proceedings of the 6th WSEAS International Conference on Applied Information and Communication, Elounda, Greece, 2006, pp.353-358
- [6] D. H. Kim, "Structure of deterministic data communication for nuclear safety data networks", Transaction of KIEE, 2006
- [7] K. S. Son, D. H. Kim, "Development of Broadband-Nuclear Safety Data Network(B-NSDN)", 2011 Symposium for nuclear power plant instrumentation and control, pp 366-373
- [8] D. H. Yun, "Design basis for SPLC", Technical Report in Ponu-tech, Rev00, 2011.
- [9] Ajit K. Verma, A. Srividya, Durga R. Karanki, Reliability and Safety Engineering, Springer Inc. 2010.
- [10] Barry W. Johnson, Design and Analysis of Fault-Tolerant Digital System, Addison-Wesley Publishing Company, 1989
- [11] J. G. Choi "Reliability analysis report for safety grade PLC(POSAFE-Q)", Technical report in KAERI, Rev02, 2008

저 자 소 개

손 광 섭 (孫 光 燮)

1979년 1월 8일생, 2004년 충남대학교 전기전자공학과 졸업, 2006년 한국과학기술원 전기전자공학과 석사 졸업, 2006년 ~ 2007년 LG전자기술원 주임연구원 2007년~현재 한국원자력연구원 선임연구원

김 동 훈 (金 東 勳)

1961년 4월 5일생, 1984년 한국항공대학교 항공전자 졸업, 2001년 한남대학교 정보통신공학 석사 졸업, 2006년 동 대학원 박사 졸업, 1987년~현재 한국원자력연구원 책임연구원

손 철 응 (孫 澈 雄)

1983년 9월 21일생, 2009년 한남대학교 컴퓨터공학과 졸업, 2011년 동 대학원 컴퓨터 공학과 석사 졸업, 2011~현재 한국원자력연구원 연구원