2001 추계학술발표회 논문집
한국원자력학회

RBD 및 고장률을 이용한 원자로 보호계통 수명평가

Evaluation of Mean Time Between Forced Outage for Reactor Protection System Using RBD and Failure Rate

이동영, 박주현, 황인구, 차경호, 최종균, 이기영, 박종균

한국원자력연구소
대전광역시 유성구 덕진동 150

요 약

최근 건설되고 있는 원전의 설계수명은 50~60년인 반면, 현장에 설치된 제어시스템 모듈이 정상적인 기능으로 동작할 수 있는 기간은 기껏해야 5~10년 정도이다. 원전 설계수명에 비해 짧은 수명을 갖는 제어시스템을 원자로 보호계통에 적용하기 위해서는, 다중화 설계 및 적절한 유지보수 전략을 복합적으로 수립하여야 한다. 계측제어계통의 정량적 신뢰도 평가를 위해, 확률론적 안전성분석에 적용하고 있는 FTA(Fault Tree Analysis) 기법이 사용되고 있다. 그러나 이 기법은 유지보수에 따른 보전(maintenance)의 결과를 반영하기가 어렵다. 본 논문에서는 보전의 효과를 반영하기 위해서, 신뢰성 블록도(Reliability Block Diagram)와 고장률을 이용한 신뢰도 정량적 평가기법을 분석하고, 이를 차세대 원자로 보호계통의 수명평가에 적용하였다.

Abstract

The design life of nuclear power plants (NPPs) under recent construction is about fifty to sixty years. However, the duration that equipments of control systems operate without failures is at most five to ten years. Design for diversity and adequate maintenance strategy are required for NPP protection system in order to use the control equipment which has shorter life time than the design life of NPP. Fault Tree Analysis (FTA) technique, which has been applied to Probabilistic Safety Analysis (PSA), has been introduced to quantitatively evaluate the reliability of NPP I&C systems. The FTA, however, cannot properly consider the effect of maintenance. In this work, we have reviewed quantitative reliability evaluation techniques using the reliability block diagram and failure rates and applied it to the evaluation of mean time between forced outage for reactor protection system.

1. 서 론

EPRI-URD는 다음과 같은 계측제어계통의 신뢰도 요건을 요구하고 있다.

'Mean time between forced outage caused by failures of MMIS equipment shall be greater than fifty reactor operating years over the entire design life of the MMIS equipment. The meaning of forced outage includes shutdowns that result directly from the failure, and shutdown the operators must perform to avoid violation of plant Technical Specifications due to these failures.'

기존에 운영중인 원전 계측제어계통은 아날로그 기술을 사용하고 있으며, 아날로그 계측제어계통의 고장으로 발전소가 불시정지(forced outage)될 확률이 한 발전소 당 1년에 한번 이상인 것으로 보고되었다. 그러나 디지털 계측제어계통의 적용에 따른 다중화설계 및 자동고장검출·우회(bypassing) 기능의 구현 결과로써, 고장 파악 및 수리에 필요한 시간을 감소시켜 계측제어계통의 고장으로 인한 원전 불시정지 확률을 많이 줄일 수 있다. 이러한 기술적인 발전에 따라 차세대원전은 계측제어계통의 신뢰도목표를 60년의 Mean Time Between Forced Outage로 설정하였다.

원전 계측제어계통은 다중화로 설계되어 있으며, 다중화된 각 채널은 독립적으로 구성되어 있다. 예를 들면, 총 4채널로 구성되어 2/4로직을 수행하는 보호계통은, 4개의 채널중 2개가 고장날 경우 트립신호가 발생하여 원자로가 트립되지만 3개 이상의 채널이 정상적으로 작동하면 보호계통의 기능을 수행할 수 있다. 채널고장을 발견하고 수리하고 있는 동안 다른 채널에서 추가적으로 고장이 발생하면 Trip Breaker가 작동하여 발전소가 정지된다. 그러므로 채널고장을 신속히 파악하여 운전원에게 알려주고 고장난 채널의 우회 또는 고장수리를 적절히 수행하면, 보호계통의 고장으로 인한 발전소의 불시정지(forced outage) 확률을 감소시킬 수 있다. 이와 같이 유지보수를 수행하는 시스템은, 한번 설치된 후 고장까지 연속적으로 사용하고 폐기하는 부품과는 다른 방법으로 신뢰도를 평가하여야 한다.

계측제어계통의 신뢰도 분석에 확률론적 안전성분석에서 사용하는 FTA(Fault Tree Analysis) 기법을 일반적으로 적용하고 있다. FTA는 불필요한 사건을 유발하는 고장을 연역적인(deductively) 논리과정으로 조직화하여 논리도형(logic diagram)으로 표현하며, 이 논리도형을 이용하여 고장의 원인을 정성 또는 정량적으로 분석한다. 이러한 FTA 기법은 고장수리와 같은 시스템의 상태(state)와 이들 상태들 사이에서의 전이(transition)를 반영할 수 없는 단점이 있다. 본 연구에서는 정량적 신뢰도 평가방법의 일환으로 신뢰성 블록도 및 고장률을 이용한 확률론적 방법의 타당성을 검토하였다. 또한 검토된 방법을 유지보수를 수행하는 원자로 보호계통에 적용하여, 60년의 원전 설계수명보다 짧은 수명을 갖는 계측제어시스템이 원전의 안전에 영향을 미치는 Mean Time Between Forced Outage를 정량적 입증하는 수명평가를 수행하였다.

2. 신뢰성 척도 정의

신뢰성을 나타내기 위한 척도에는 신뢰도함수, 고장확률밀도함수, 고장누적확률함수, 고장률, 평균수명 등 여러 가지가 있다. 초기에 주어진 샘플의 수를 N, 시점 t에서 고장나지 않고 남아있는 수를 $n(t)$라 하면, 시점 t에서 고장나지 않고 남아있을 확률 즉 **신뢰도함수**

R(t)는

$$R(t)=\frac{n(t)}{N} \qquad (1.1)$$

가 된다. 시점 *t*까지의 **고장누적확률 *F(t)***는 다음 식으로 표시된다.

$$F(t)=1-\frac{n(t)}{N} \qquad (1.2)$$

또한 단위시간당 고장발생 비율을 나타내는 **고장확률밀도함수**(failure probability density function) ***f(t)***는 다음과 같다.

$$f(t)=\frac{dF(t)}{dt} \qquad (1.3)$$

누적 고장확률 *F(t)*와 신뢰도 *R(t)*를 고장확률밀도함수 *f(t)*로 표시하면

$$F(t)=\int_0^t f(t)dt \qquad (1.4)$$

$$R(t)=\int_t^\infty f(t)dt=1-F(t) \qquad (1.5)$$

이 되고, 식(1.5)를 식(1.3)에 대입하면 다음 식과 같다.

$$f(t)=-\frac{dR(t)}{dt} \qquad (1.6)$$

단위시간 Δt 동안 현재 사용 중인 장비가 그 구간 내에서 고장을 일으킬 확률을 고장률이라 하며, $\lambda(t)$로 표시한다. 시간 *t=0*에서 장비가 가동을 시작했을 때 운영시간이 경과함에 따라 일부의 장비에 고장이 발생한다. 시각 *t*에 고장나지 않고 남아있는 장비의 수를 *n(t)*라 하면 **고장률 $\lambda(t)$**는 다음과 같이 표시된다.

$$\lambda(t)=\frac{[n(t)-n(t+\Delta t)]/n(t)}{\Delta t} \qquad (1.7)$$

식 (1,1)의 신뢰도를 고장률 함수로 표시하면 다음과 같다.

$$R(t)=\exp[-\int_0^t \lambda(t)\,dt] \qquad (1.8)$$

신뢰도 *R(t)*는 주어진 시간 *t*에서 전체의 몇 퍼센트가 만족하게 동작하는가를 나타내는 확률이므로 이를 평균하면 **평균수명(mean life)**을 구할 수 있다.

$$E(t)=\int_0^\infty R(t)dt \qquad (1.9)$$

위와 같이 정의되는 평균수명 *E(t)*는 시스템을 수리하면서 사용하는 경우에는 MTBF(Mean Time Between Failure)라 부르고, 수리하여 사용할 수 없는 경우에는 MTTF(Mean Time To Failure)라 부른다. 만일 고장확률밀도함수 *f(t)*가 지수분포 즉 제품의 고장률이 사용시간에 관계없이 일정하다면 식(1.8)에 의해 신뢰도 *R(t)*는 $e^{-\lambda t}$가 되고, 평균수명 *E(t)*는

$$E(t)=\int_0^\infty R(t)dt=\int_0^\infty e^{-\lambda t}dt=\frac{1}{\lambda} \qquad (1.10)$$

와 같이 표시되며, 지수분포를 갖는 고장확률밀도함수의 평균수명은 고장률 λ의 역수가 된다.

가동성(availability)은 시스템이 어떤 기간 중에 주어진 기능을 발휘하고 있을 시간의 비율을 말하며 다음과 같이 정의된다.

$$Availability = \frac{MTTF}{MTTF + MTTR} \qquad (1.11)$$

이때 *MTTR*(Mean Time To repair)은 고장발생시 고장을 감지하고 수리하는데 소요된 평균수리시간을 의미한다. 시스템의 불가동성(unavailability)은 다음과 같이 정의 된다.

$$Unabilability = 1 - Availability$$

3. 보호계통 제어기기 구성

보호계통(DPPS)은 단일고장기준(Single failure criteria)을 만족하기 위하여 4개의 다중화된 채널(A, B, C, D)로 구성되어 있으며, bistable, coincidence, initiation logic 및 maintenance/test 기능을 수행한다.

Bistable Processor(BP)는 센서로부터 아날로그 입력, CPC로부터 디지털 입력, 및 노외핵계측계통에서 아날로그 입력신호를 받아서 설정치와 비교하여 Bistable trip 신호를 발생한다. 한 채널의 BP 기능을 수행하기 위한 PLC 구성모듈은 다음과 같다.

- 2개의 통신모듈
- 2개의 프로세서
- 1개의 아날로그 출력 + 2개의 아날로그 입력 모듈
- 8개의 디지털 출력 + 1개의 디지털 입력 모듈

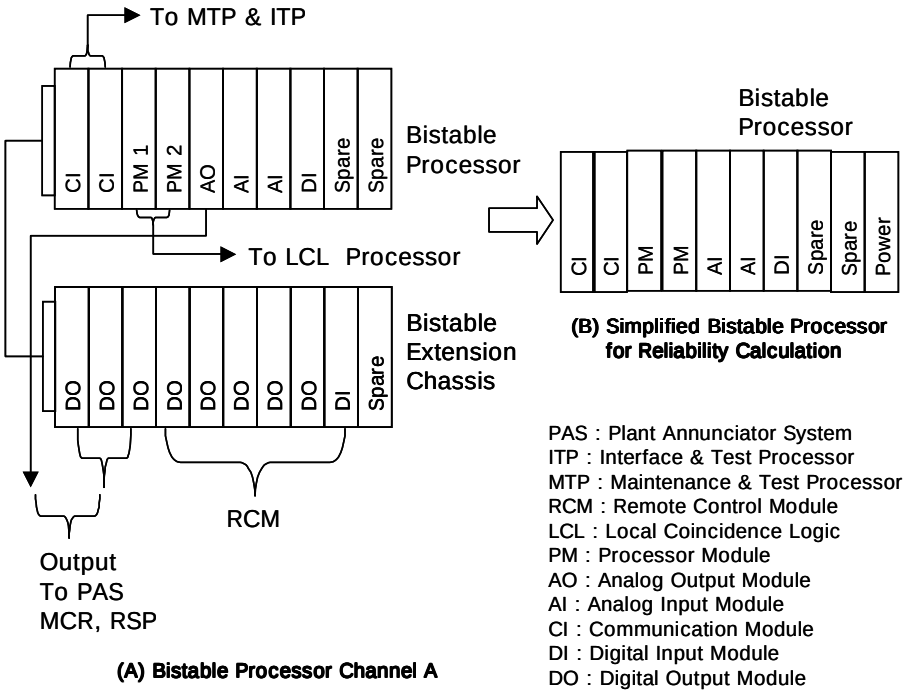

그림 1. BP 제어기기 구성

BP 모듈들 중에서 아날로그 및 디지털 출력 모듈은 제어실과의 인터페이스 기능만을 수

행하므로, 이들 모듈의 고장이 보호계통에 영향을 미칠 확률이 적어 본 연구에서는 단순화된 BP 구조를 사용하여 분석을 수행하였다. 차세대 보호계통의 BP 구성은 그림 1과 같다.

LCL(Local Coincidence Logic)은 각 채널의 BP에서 생성된 Bistable trip 신호를 받아 비교하여 정확한 Local Trip 신호를 발생한다. LCL을 구성하고 있는 한 채널의 PLC 모듈은 다음과 같다.

- 2개의 통신모듈
- 4개의 프로세서
- 5개의 디지털 출력 모듈

한 개의 디지털 출력 모듈은 제어실과의 인터페이스를 담당하고, 이 모듈의 고장이 보호계통에 영향을 미칠 확률이 적으므로 본 연구에서는 단순화된 LCL 구조를 사용하여 분석을 수행하였다. 차세대 보호계통의 LCL 구성은 그림 2와 같다.

본 수명평가에서는 디지털 보호계통 제어기기의 영향을 평가하기 위해 보호계통의 센서, RTSG(Reactor Trip Switchgear) 및 소프트웨어를 제외한 PLC 시스템만을 대상으로 수명평가를 수행하였다.

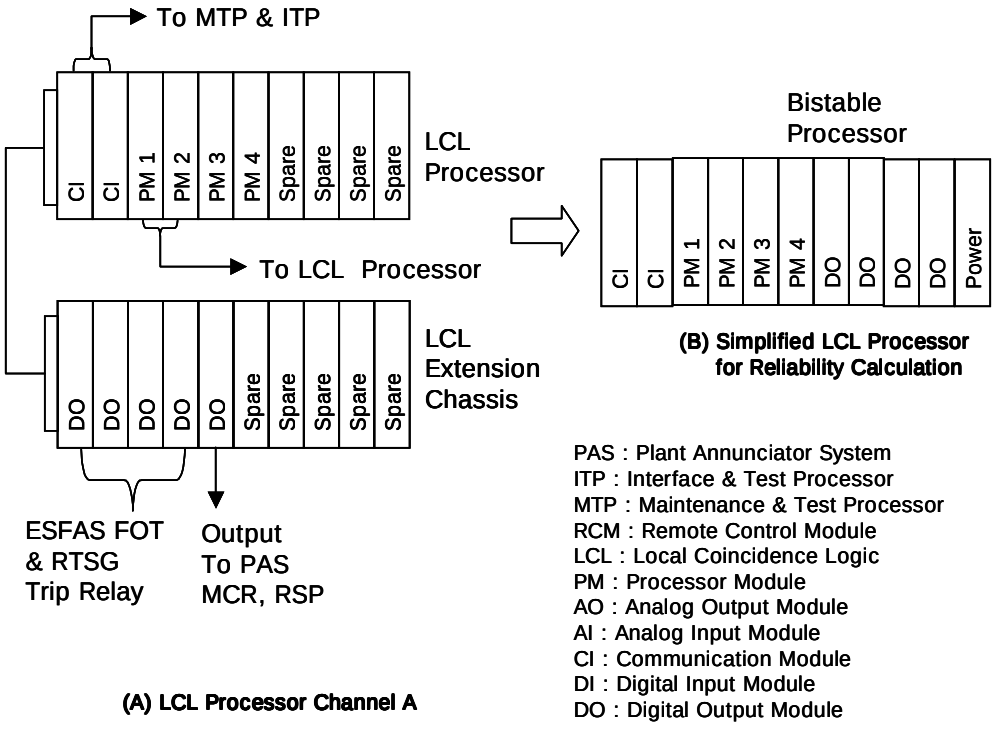

그림 2. LCL 제어기기 구성

4. 신뢰성 블록도(Reliability Block Diagram)

시스템이나 기기를 분석할 경우 하드웨어나 기기를 기준으로 분석하는 것보다 기능별 블록으로 분석하는 것이 시스템의 전체 기능을 파악하는데 매우 유리하다. 시스템의 로직과

컴포넌트를 수학적으로 표시하는 일반적인 방법으로 신뢰성 블록도가 널리 사용되고 있다. 신뢰성 블록도는 success-oriented diagram 방법으로 시스템의 functional block diagram 및 회로도에서 나타난 기능의 상관관계를 이용하여, 시스템의 전체 기능을 세분화된 기능으로 분리하고, 분리된 각각의 기능을 연결하여 표시한다. 차세대 원전 보호계통의 신뢰성 블록도는 그림 3과 같다. 그림에서 표시된 바와 같이 보호계통이 정상적으로 동작하기 위해서는 최소한 1개 이상의 경로가 유지되어야 한다.

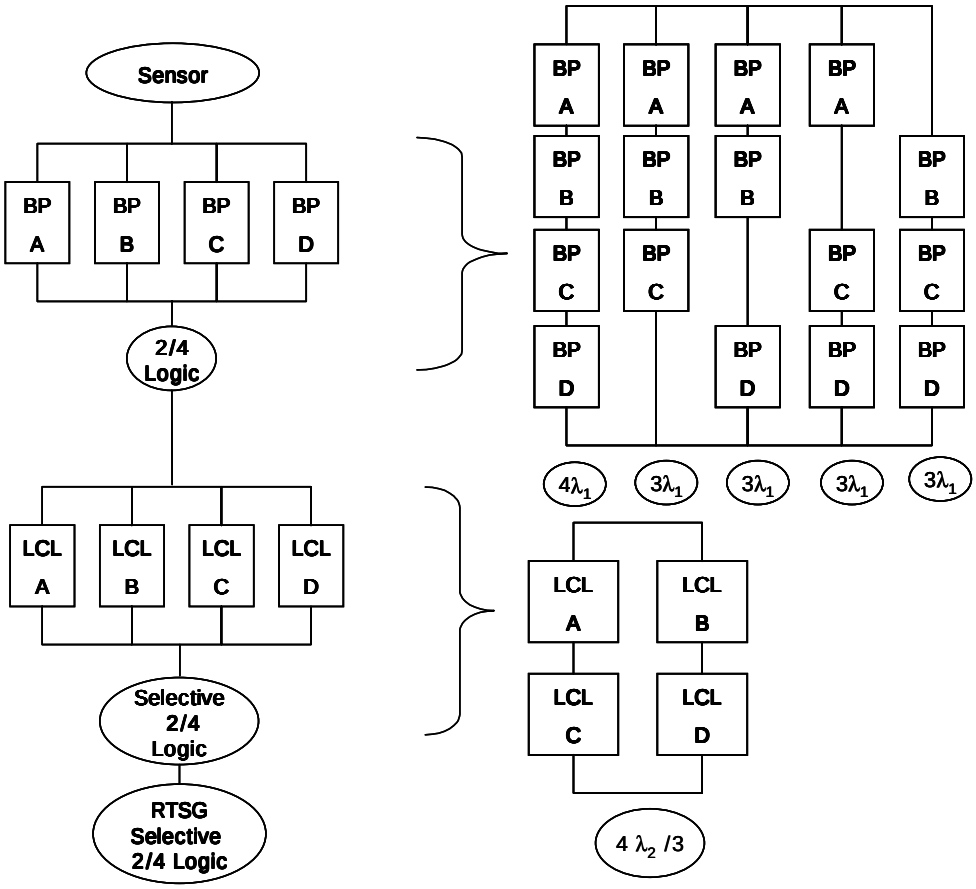

그림 3. 보호계통 신뢰성 블록도

보호계통의 BP(Bistable Processor)는 2-out-of-4 로직으로, fail-safe로 구성된 2개 이상의 채널에서 동시에 고장이 발생하면 플랜트가 트립되므로, 4개의 채널 중 3개 이상의 채널이 정상적으로 작동하여야만 보호계통의 기능을 수행할 수 있다. 또한 LCL(Local Coincidence Logic)은 Selective 2-out-of-4 로직으로 구성되어 있으므로 경로에 포함된 연속된 2개의 LCL이 정상적으로 작동하여야만 보호계통이 고유의 기능을 수행할 수 있다.

5. 고장률

수리할 수 없는 시스템의 경우 시스템의 고장률이 설정된 고장률을 초과하는 시점까지의 사용시간을 수명으로 볼 수 있다. 그러나 일반적인 디지털 계측제어시스템은 다중화 구조로

설계되어 있으며, 각 모듈이 독립적으로 구성되어 부품을 수리 및 교체하여 사용하고 있다. 그 결과 한 모듈의 고장이 다른 모듈의 고장에 영향을 주지 않으며, 고장이 발생한 모듈을 수리 또는 교체하는 동안에도 계속 시스템 고유의 기능을 수행할 수 있다. 즉, 다중화 구조를 갖는 시스템은 운영 중에도 고장난 모듈을 교체할 수 있으므로 시스템의 수명은 전자부품의 경우와는 다르게 정의된다.

보호계통의 BP 로직은 2-out-of-4 로직으로 구성되어, 4개의 채널 중 3개 이상의 채널이 정상적으로 작동하여야만 보호계통이 고유의 기능을 수행할 수 있다. 즉 하나의 채널에 고장이 발생하여 수리하고 있는 동안 나머지 채널 중 하나 이상의 채널에서 추가적으로 고장이 발생하면 Trip Breaker가 작동하여 발전소가 정지하게 된다. 보호계통의 LCL 로직은 Selective 2-out-of-4 로직으로 구성되어 있으므로, 보호계통이 정상적으로 작동하기 위해서는 LCL processor A와 C 또는 LCL processor B와 D가 동시에 동작 가능하여야 한다.

EPRI-URD는 고장이 발생하여 수리에 필요한 MTTR(Mean Time To Repair)을 4시간, 최대 고장수리 시간을 8시간으로 요구하고 있다. 그러므로 하나의 채널에 고장이 발생하여 고장수리를 하고 있는 최대 8시간 동안, 다른 카드에서 고장이 발생하지 않으면 보호계통의 고장으로 인한 원전의 불시정지를 예방할 수 있다.

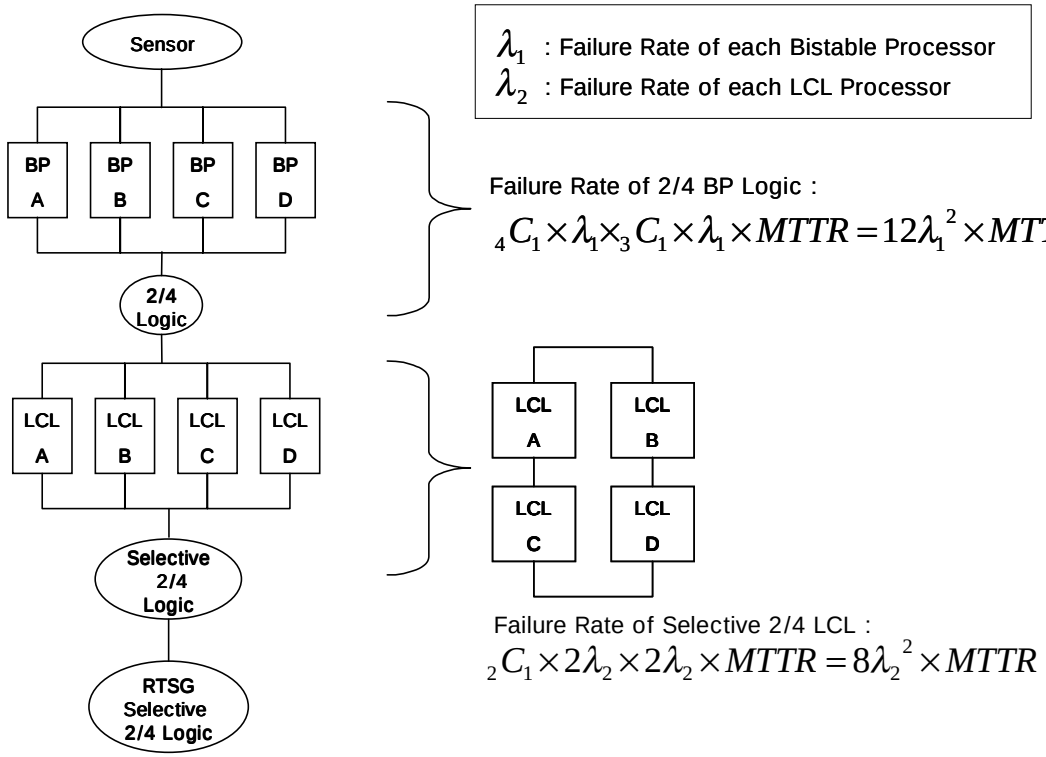

그림 4. 고장률 계산

보호계통의 BP는 2-out-of-4 로직으로 구성되어 있으므로, 한 채널이 고장난 상태에서 고장수리가 완료되기 전에(MTTR 시간 내) 다른 채널에서 중복하여 고장이 발생하면 보호계통의 기능을 상실한다. BP 로직을 구성하고 있는 4개의 PLC 중 어떤 한 PLC의 고장률은

${}_4C_1 \times \lambda_1$ 이고, 식(1.7)에 따라 고장수리 시간 $MTTR$ 동안 나머지 3개 PLC의 고장률은 ${}_3C_1 \times \lambda_1 \times MTTR$ 이다. 그러므로 BP 로직의 전체 고장률 λ_{BP}는 다음과 같다.

$$\lambda_{BP} = {}_4C_1 \times \lambda_1 \times {}_3C_1 \times \lambda_1 \times MTTR = 12\ \lambda_1^2 \times MTTR$$

LCL은 selective 2-out-of-4 로직으로 구성되어 있으므로, 보호계통이 정상적으로 동작하기 위해서는 병렬로 연결된 채널의 한 경로가 정상적으로 동작하여야 한다. 그러므로 LCL 로직의 고장률 λ_{LCL}는 다음과 같다.

$$\lambda_{LCL} = {}_2C_1 \times 2\lambda_2 \times 2\lambda_2 \times MTTR = 8\ \lambda_2^2 \times MTTR$$

보호계통의 BP 및 LCL 프로세서를 구성하고 있는 PLC 전체 고장률 λ_S는 다음과 같다.

$$\begin{aligned}\lambda_S &= \lambda_{BP} + \lambda_{LCL} \\ &= {}_4C_1 \times \lambda_1 \times {}_3C_1 \times \lambda_1 \times MTTR + {}_2C_1 \times 2\lambda_2 \times 2\lambda_2 \times MTTR \\ &= 12\ \lambda_1^2 \times MTTR + 8\ \lambda_2^2 \times MTTR = (12\ \lambda_1^2 + 8\ \lambda_2^2) \times MTTR\end{aligned}$$

6. 결과

본 논문에서는 원자로 보호계통의 고장으로 인해 원자로에 불시정지가 발생하지 않는 확률을 정량적으로 평가하였다. 본 평가는 보호계통의 제어기기에 의한 영향을 평가하기 위해 보호계통의 센서, RTSG(Reactor Trip Switchgear) 및 소프트웨어를 제외한 PLC 시스템만을 대상으로 하였다. 보호계통의 정량분석에 사용한 데이터 값은 CENP사에서 제출한 PLC 각 모듈의 고장률을 사용하였다. MTTR은 앞에서 언급한 바와 같이 EPRI-URD에서 요구한 최대 고장수리시간인 8시간을 사용하였다.

BP 로직의 전체 고장률은

$$\lambda_{BP} = {}_4C_1 \times \lambda_1 \times {}_3C_1 \times \lambda_1 \times MTTR = 1.66E-07/Hour$$

이며, LCL의 전체 고장률은

$\lambda_{LCL} = {}_2C_1 \times 2\lambda_2 \times 2\lambda_2 \times MTTR = 2.01E-07/Hour$ 이다.

BP 및 LCL 프로세서를 포함한 보호계통 고장률 λ_S는 다음과 같다.

$$\lambda_S = \lambda_{BP} + \lambda_{LCL} = 3.67E-07/Hour$$

일반적으로 시스템의 경우 지수분포의 고장확률밀도 함수를 가지며 고장률은 일정하다고 가정된다 이와 같은 경우 평균수명은 고장률을 이용하여 다음과 같이 계산된다.

$$MTBF = \frac{1}{\lambda} = \frac{1}{3.67E-07} \cong 2.73E06[Hour] = 311.4[Year]$$

이상의 정량평가 결과에 나타난 바와 같이 운전 중 유지보수가 가능한 시스템은, 다중화된 시스템의 일부가 고장난 경우에도 제한된 시간 내에 수리가 완료되면 전체 시스템이 고유의 기능을 만족하게 수행하므로, 보전을 수반하는 시스템의 신뢰도는 보전을 수반하지 않는 시스템보다 높은 신뢰도를 유지할 수 있다. <표 1>은 본 연구에서 수행한 원자로 보호계통 대한 정량평가 결과를 요약한 표이다.

원자로 보호계통은 총 4개의 채널로 구성되어 2/4로직을 수행하지만 하나의 채널에 고장이 발생될 경우 이를 우회시키고 나머지 3개의 채널을 이용하여 2/3로직을 수행하여 정상적

인 원자로 보호기능을 수행한다. 본 연구에서는 채널우회를 고려하지 않았지만 더 정확한 보호계통의 수명을 평가하기 위해서는 채널우회를 고려한 수명평가가 수행될 필요가 있다. 또한 원자로 보호계통은 본 연구에서 수행한 PLC뿐아니라 센서, RTSG, 및 기타 여러 기기들로 구성되어 있으며 디지털 계통의 경우 소프트웨어도 포함되어 있다. 앞으로 건설될 원전에는 디지털 보호계통이 적용되므로 소프트웨어를 포함한 전체 보호계통의 수명 평가가 필요하다.

표 1. 정량평가 결과

Description	Part No.	Module Number	Failure Rate /Module	Failure Rate	Unit
(Bistable Logic)					
Processor	PM645C	2	9.07E-06	1.81E-05	
Analog Input	AI620	2	5.60E-06	1.12E-05	
Digital Input	DI620	1	2.51E-06	2.51E-06	
Communication Interface	CI532	2	2.90E-06	5.80E-06	
Power Supply	SA610	1	3.90E-06	3.90E-06	
Failure Rate of Single PLC Rack				4.16E-05	
Failure Rate of 2-out-of-4 Bistable Logic				1.66E-07	
(Local Coincidence Logic)					
Processor	PM645C	4	9.07E-06	3.63E-05	
Digital Output	DO620	4	2.51E-06	1.00E-05	
Communication Interface	CI532	2	2.90E-06	5.80E-06	
Power Supply	SA610	1	3.90E-06	3.90E-06	
Failure Rate of Single PLC Rack				5.60E-05	
Failure Rate of Selective 2-out-of-4 LCL				2.01E-07	
(PPS)					
Total Failure Rate of PPS				3.67E-07	
MTBF				2.73E+06 311.4	Hour Year

* *본 연구는 과학기술부의 원자력연구개발 사업의 일환으로 수행되었습니다.* *

참고문헌

1. KAERI/AR-562/2000, "계측제어기기 수명평가 현안기술", 2000.
2. 박경수, “신뢰도 및 보전공학”, 영지문화사.
3. 김선진 외, “신뢰성공학”, 원창출판사.
4. IEEE Std. 352, "Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems", IEEE, 1987.
5. 강인수 외, “디지털 기반 계측제어 계통의 신뢰도 분석”, 원자력학회 99 추계 학술발표회, 1999.