Journal of Institute of Control, Robotics and Systems (2013) 19(4):328-333
http://dx.doi.org/10.5302/J.ICROS.2013.12.1857 ISSN:1976-5622 eISSN:2233-4335

다중화 구조 제어시스템에 대한 신뢰도 분석

Reliability Analysis of Redundant Architecture of Dependable Control System

노 진 표, 박 재 현*, 손 광 섭, 김 동 훈
(Jinpyo Noh[1], Jaehyun Park[1], Kwang-Seop Son[2], and Dong-Hoon Kim[2])
[1]Inha University
[2]Korea Atomic Energy Research Institute

Abstract: Since a slight malfunction of control systems in a nuclear power plant may cause huge catastrophes, such control systems usually have multiple redundancy and reliable features, and their reliability and availability should be analyzed and verified thoroughly. This paper performed the reliability analysis of the SPLC (Safety Programmable Logic Controller) that is under developed as the control systems for the next generation nuclear power plant. One of the key features of SPLC is that it has multiple redundancy modes as faults happen, which means the reliability analysis for one fixed redundant model is not enough to analyze the reliability of SPLC. With considering this reconfigurable concept, FTA (Fault Tree Analysis) was used to capture fault-relationship among sub-modules. The analysis results show that MTTF (Mean Time to Fault) of SPLC is 45,080 hours, which is a about 4.5 times longer than the regulation, 10,000 hours.

Keywords: reliability, nuclear power plant, fault tree analysis, safety programmable logic controller, redundant structure

I. 서론

원자력발전소, 고속전철, 항공기와 같이 고장 혹은 사고 발생 시 치명적인 인명 손실 및 환경 파괴를 초래할 수 있는 고 신뢰성이 요구되는 시스템의 경우 구성 부품 및 전체 시스템의 신뢰성에 대한 사전 평가는 필수적인 절차로 인식되고 있다. 시스템 수준의 신뢰성 분석과 예측을 위해서는 방대한 량의 데이터를 취합하는 것은 필수적이지만 시간 또는 공간상의 제약으로 인해 대부분 구성 요소 단위로 시험을 실시하며, 이들 데이터로부터 시스템 단위의 신뢰성을 해석적 방법과 시뮬레이션을 통하여 분석하는 접근 방법이 사용된다[1,2]. 국내에서도 원자력발전소의 제어계통 및 항공기와 같이 고신뢰성이 요구되는 시스템에 대한 신뢰도 분석과 구조 연구 등이 진행된 바 있다[3-5]

고신뢰성 제어시스템 중, 원자력 발전소의 원자로를 직접 제어하는 안전시스템에 사용되는 제어시스템은 IEEE에서 정한 최고안전도 기준을 적용해야 하는 CLASS 1E로 분류되어 있으며 특히 간헐적으로 발생할 수 있는 여러 형태의 고장 및 오류 상황에 대처할 수 있도록 다중화 기능(redundancy)을 가지도록 설계하는 등, 일반 산업용 제어기기와는 차별화 된 구조로 설계된다[6,7]. 현재 국내에서는 차세대 원전제어시스템을 개발 중에 있으며, 제어시스템의 핵심 제어기로서 프로세서 모듈 및 입출력 모듈의 삼중화(triple redundancy) 기능, 이중화된 버스 등의 다중화 구조를 지원하는 원전안전시스템의 제어기(SPLC: Safety Programmable Logic Controller)를 개발 중에 있다[8,9]. 현재 개발 중인 SPLC의 경우, 삼중화된 구조에서 고장 모드에 따라 구성을 유연하게 변화하는 구조로서, 이러한 구조의 PLC에 대한 신뢰성 분석은 많이 이루어지고 있지 않다. 따라서 SPLC와 같이 고장 발생에 따라 유연하게 구조가 변경되는 시스템에 대한 신뢰성 분석에 관한 연구가 필요하다.

본 논문에서는 현재 개발중인 SPLC의 신뢰도를 해석적 방법으로 분석하였다. 이를 위하여 입력모듈-프로세서모듈-출력모듈 등 각 구성 모듈간의 시스템 의존 관계를 분류하고 다중화 모듈의 구조가 반영된 SPLC 전체 시스템 신뢰도 분석을 수행하였다. 논문의 구성은 다음과 같다. II 장에서는 본 논문에서 다루는 다중화 제어기의 구조를 간략히 설명하고, III 장에서는 결함수목분석을 실시하였으며. IV 장에서는 시스템의 신뢰도를 해석적 방법으로 분석하였으며, V 장에서 결론을 맺는다.

II. 원전 다중화 제어기기 구조

그림 1은 본 논문에서 분석하는 차세대 원전 안전등급제어기기인 SPLC의 구성도이다[10]. 일반적으로 다중화 구조에서의 동작형태는, k/n/G 구조, 병렬구조(parallel), 대기이중계(혹은 축차병렬구조; stand-by)로 분류할 수 있는데, SPLC의 다중화 구조의 기본 원칙은 신호 검증과 능동적 의사결정이 요구되는 입출력모듈과 프로세서모듈은 삼중화로 구성하여 2/3/G 구성을 가지며, 버스와 통신모듈은 이중화 구조로서 병렬구조와 대기이중계 구조로 구성된다. 표 1은 SPLC의 고장 모드에 따른 상태별 구성을 보이고 있다. 예를 들어, 프로세서 모듈의 경우 정상상태인 삼중화 프로세서 모듈이 모두 정상 동작하는 경우(n=3)는 3개 중 2개의 값을 선택하는 2/3/G

* 책임저자(Corresponding Author)
논문접수: 2012. 12. 26., 수정: 2013. 2. 28., 채택확정: 2013. 3. 6.
노진표: 인하대학교 대학원 정보통신공학과(jpnoh@emcl.org)
박재현: 인하대학교 정보통신공학부(jhyun@inha.ac.kr)
손광섭, 김동훈: 한국원자력연구원
(ksson78@kaeri.re.kr/dhkim4@kaeri.re.kr)
※ 본 연구는 2012년도 지식경제부 재원으로 한국에너지 기술평가원(KETEP)의 지원을 받아 수행한 원전기술혁신사업 연구과제임(과제번호: 20101610100001G).

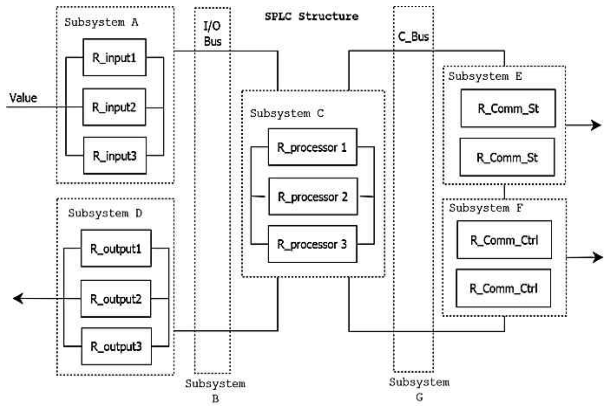

그림 1. 원전 안전시스템 제어기의 다중화 구조.
Fig. 1. Redundant structure of nuclear SPLC.

보팅 구조를 가지며, 만일 하나의 프로세서가 고장이 나서 2개만 정상 동작하는 경우(n=2)는 Hot-Standby로 동작함을 의미한다. 이와 같은 동작모드의 변경은 SPLC의 고유한 특성으로 신뢰도를 향상시키기 위하여 도입된 설계 개념이다.

시스템의 신뢰도 란 어떤 부품 또는 시스템이 일정한 환경하에서 일정시간 고장없이 그 능력을 발휘하는 확률로 정의할 수 있다. 이를 정량적으로 표현하기 위하여 신뢰도 함수를 사용하는데 신뢰도 함수 $R(t)$는 시간 t 까지 고장없이 시스템이 동작할 확률, 즉 t 시간 동안 잔존 비율을 의미한다. 시스템의 고장 확률 함수인 고장률을 $\lambda(t)$로 정의하면 신뢰도 함수 $R(t)$와 $\lambda(t)$ 사이에는 식 (1)과 같은 관계가 성립한다[9].

$$R(t) = e^{-\int_0^t \lambda(t)dt} \tag{1}$$

본 논문에서는 식 (1)의 신뢰도 함수를 활용하여 SPLC의 신뢰도를 산출하고 이를 기반으로 무고장시간, 즉 MTTF (Mean Time To Failure)를 예측하도록 한다.

k/n/G 구조는 n개의 구성요소 중 k개 이상이 동시에 가동되어야 시스템이 가동 되는 구조로서 삼중화 이상의 고도 다중화 구조에서 채택하는 방식으로 신뢰도는 식 (2)과 같이 계산된다[8]. 수식에서 λ는 각 모듈의 고장률이며, 서브시스템을 구성하는 각 모듈은 동일한 것을 사용한다고 가정한다.

$$R(t) = \sum_{r=k}^{n} \binom{n}{r} \left(e^{-\lambda r t}\right)^r \left[1 - \left(e^{-\lambda t}\right)\right]^{n-r} \tag{2}$$

병렬구조(parallel)는 n개의 구성요소들이 동시에 가동되고 있고, 어느 하나만이라도 작동하면 그 시스템이 가동되는 구조로서 신뢰도는 식 (3)와 같이 계산된다.

$$R(t) = 1 - (1 - e^{-\lambda t})^n \tag{3}$$

대기이중구조(stand-by sparing)는 이중화된 대기시스템의 상태에 따라 Hot/Warm/Cold Stand-by 시스템으로 나뉘는데, n개의 구성요소 중 하나만 가동되며, 나머지 구성요소들은 가동되지 않다가 가동중인 요소가 고장이 발생할 경우 예비 요소가 즉시 이어서 동작하는 경우인 Warm/Cold Stand-by 구조의 경우로서 신뢰도는 식 (4)과 같이 계산되며, 즉시 전환이 가능한 Hot Stand-by 시스템의 경우 신뢰도는 병렬구조와 같이 식 (3)로 계산된다.

표 1. SPLC 다중화 상태별 동작 구분.
Table 1. Sort for status of redundancy structure of SPLC.

구분	n=3	n=2	n=1	n=0
아날로그입력	2/3/G*	Parallel	Fail Safe	-
디지털입력	2/3/G*	Parallel	Fail Safe	-
프로세서	2/3/G*	Hot-standby	Mono	Fail Safe
아날로그출력	2/3/G*	Parallel	Fail Safe	-
디지털출력	2/3/G*	Parallel	Fail Safe	-
통신모듈(제어)	-	Hot-standby*	Mono	Fail Safe
통신모듈(상태)	-	Hot-standby*	Mono	Fail Safe
입출력 버스	-	Parallel*	Mono	Fail Safe
통신용 버스	-	Parallel*	Mono	Fail Safe

* : 초기 다중화 상태, Mono : 단일구조

$$R(t) = \left[1 + \lambda t + \cdots + \frac{(\lambda t)^{n-1}}{(n-1)!}\right] e^{-\lambda t} \tag{4}$$

일반적인 다중화 제어기의 경우 초기 구성이 변화하지 않으나, SPLC의 경우 정상 동작 중인 하부모듈의 개수에 따라 다중화 모드가 변경되는 구조를 취한다.

입력모듈은 외부의 입력신호를 프로세서모듈로 전달하는 기능을 하며, 용도에 따라 아날로그용과 디지털용으로 구분되며, 각 삼중화로 구성되어 있다. 세 모듈이 모두 살아있는 경우는 2-out-of-3 보팅 구조를 취하며, 두 모듈만 살아 있는 경우는 두 모듈의 결과값을 비교하고, 하나의 모듈만 살아있을 경우는 정상동작을 할 수 없는 것으로 판단하여 원자로의 안정성을 유지하는 안전모드(fail-Safe)로 전환된다. 프로세서 모듈은 입력장치, 통신장치, 출력장치와 제어 및 데이터 송수신을 담당하고, 기본적으로 삼중화 구조로서 2-out-of-3 보팅 구조로 동작하나 고장이 발생하여 n = 2인 경우는 대기이중구조(hot-standby)로 동작한다. 대기이중구조에서는 주(master) 제어기만 동작하며, 주제어기에 문제가 있을 경우 보조(slave) 제어기 중 하나가 곧 바로 주 제어기가 되어 동작한다. 만일 두 개의 프로세서 모듈에 고장이 발생하는 경우 다중화가 되지 않은 단일구조(mono)로 동작한다. 통신모듈은 프로세서모듈과 외부기기들과의 통신을 위한 데이터를 수신, 송신, 저장의 기능을 하며, 용도에 따라 제어용과 상태 송수신용으로 나뉘며, 병렬구조의 이중화로 구성되어 있다. 하나의 통신모듈에 고장이 발생하면, 나머지 모듈이 대체하여 동작한다. 즉, 다중화가 되지 않은 단일구조로 동작한다. 버스는 통신용과 입출력버스 용 두 가지로 구분되며, 이는 병렬구조로 구성된다. 마지막으로 출력모듈은 프로세서모듈에서 나온 결과 데이터를 외부로 내보내는 역할을 하며, 이 또한 디지털용과 아날로그용으로 구분되며, 동작 형태는 입력모듈의 형태와 동일하다. 따라서 SPLC를 구성하는 각 서브시스템의 신뢰도를 계산하면 3중화 구조의 입출력 및 프로세서 서브시스템의 경우 신뢰도는 식 (2)로부터

$$R(t) = 3e^{-2\lambda t} - 2e^{-3\lambda t} \tag{5}$$

와 같고, 병렬구조 및 대기이중구조(Hot Stand-by)인 버스, 통신 서브시스템의 경우 신뢰도는 식 (3)로부터

$$R(t) = 2e^{-\lambda t} - e^{-2\lambda t} \tag{6}$$

와 같이 계산될 수 있다.

III. SPLC 결함수목분석 (Fault Tree Analysis)

결함수목분석(FTA: Fault Tree Analysis)은 미국 산업 표준문서(NUREG-0492)를 비롯하여, IEC61025, MIL-HDBK-338에 규정되어 있는 연역적 방법의 오류분석 도구이다. 결함수목분석을 적용하면 오류에 대한 관련성을 나열하여, 우선순위를 구분하고, 하위 레벨에 대한 요구조건을 만들고, 고장률을 산출할 수 있다. 또한, 최상위 오류가 야기한 요소들을 식별하고 수정할 수 있는 진단도구로 활용할 수 있다[12-14].

시스템의 오류여부를 결정하기 위해서 오류에 대한 영역을 구분하여야 하는데, 본 논문에서 결함수목분석을 적용할 경계는 각 모듈의 동작상태이며, "정상", "고장" 2가지로 구분하였다. 이를 근거로 다중화 시스템의 고장 상태는 그림 2 같이 4가지로 구분하였다. TS (Total Success) 상태는 다중화의 초기 구조로 어떤 모듈도 고장이 발생하지 않은 다중화 상태이다. MAF (Minimum Anticipated Failure)는 받아들일 수 있는 최소한의 오류상태로 다중화 된 모듈 중 고장이 났지만 더 고장이 발생하여도 동작에 지장이 없도록 예비모듈이 남아 있는 상태이다. MTF (Maximum Tolerable Failure)는 받아들일 수 있는 최대한의 오류상태로 현재 동작은 가능하지만 더 이상 오류에 대한 대비를 할 수 없는 상태이다. 마지막으로 CF (Complete Failure)상태는 다중화된 구성요소가 모두 고장이 발생하여 해당 모듈은 더 이상 기능을 하지 못함을 의미한다.

그림 3은 전체시스템의 FTA 분석을 위한 Fault Tree이다. 고장에 따른 다중화 구조의 상태가 변경되는 것을 "Top Event"로 하였다. 어떤 모듈도 고장이 발생하지 않은 상태를 TS 상태를 TS상태로 둘 수 있으며, 구체적으로 입출력모듈, 프로세서모듈, 통신모듈, 버스가 초기 다중화 상태를 유지하는 상태이다. 이때 프로세서모듈만 하나 고장이 발생하고, 다른 모듈은 고장이 발생하지 않은 상태를 MAF상태로 두고 프로세서모듈은 2-out-of-3에서 n=2인 hot-standby상태로 다중화 상태가 변한다. MTF상태는 TS상태에서 프로세서모듈을 제외한 나머지 모듈 중 하나 이상의 종류가 고장이 발생하는 경우

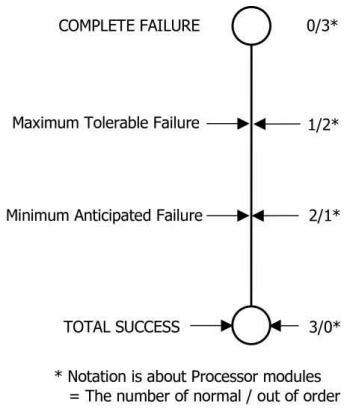

그림 2. 프로세서모듈 다중화 고장상태 분류.

Fig. 2. Fault space for redundant structure of processor module.

표 2. 안전등급제어기의 모듈별 고장상태.

Table 2. Fault status by module of SPLC.

구분	TS	MAF	MTF
Processor	3/0	2/1	1/2
	2-out-of-3	Hot-standby	No Redundancy
Analog Input	3/0	3/0	2/1
	2-out-of-3	2-out-of-3	Parallel
Digital Input	3/0	3/0	2/1
	2-out-of-3	2-out-of-3	Parallel
Comm. Ctrl	2/0	2/0	1/1
	Hot-standby	Hot-standby	No Redundancy
Comm. Status	2/0	2/0	1/1
	Hot-standby	Hot-standby	No Redundancy
Analog Output	3/0	3/0	1/2
	2-out-of-3	2-out-of-3	Parallel
Digital Output	3/0	3/0	1/2
	2-out-of-3	2-out-of-3	Parallel
I/O Bus	2/0	2/0	1/1
	Hot-standby	Hot-standby	No Redundancy
Comm. Bu	2/0	2/0	1/1
	Hot-standby	Hot-standby	No Redundancy

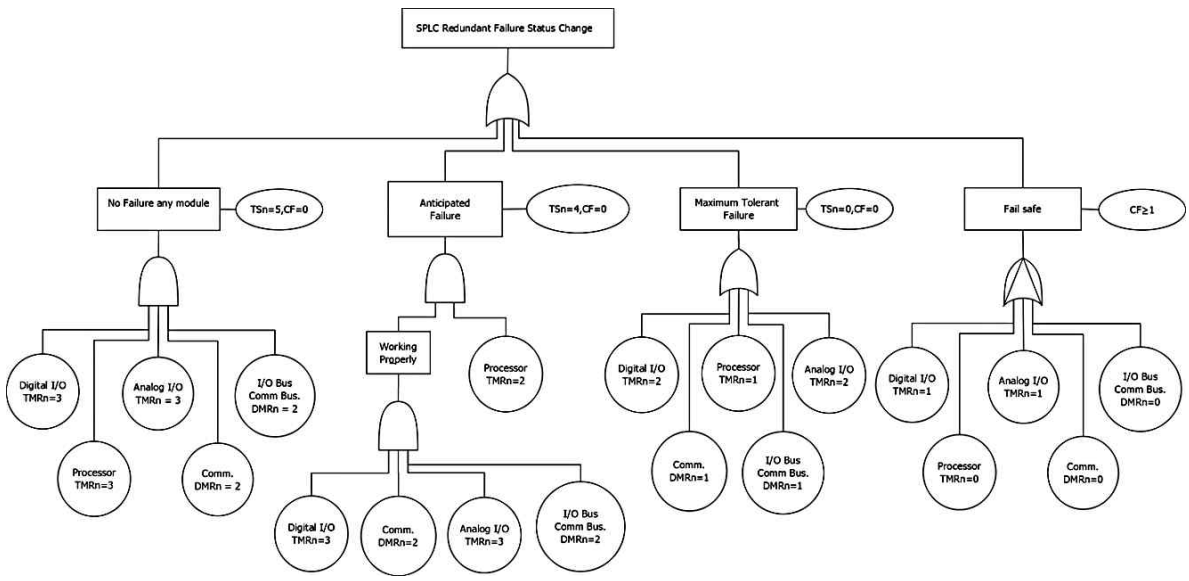

그림 3. 시간에 따른 각 모듈별 신뢰도 함수.

Fig. 3. Reliability functions by each module followed by time.

(MTF_1)와 MAF상태에서 모든 모듈 중 하나이상의 종류가 고장이 발생하는 경우(MTF_2)가 포함된 것이다. 마지막으로 CF 상태는 어떤 모듈이라도 최종고장이 하나라도 발생할 경우 전체 SPLC는 고장이 발생함을 나타내었다. 이와 같은 방법으로 전체 SPLC의 상태에 따른 각 모듈의 다중화 상태를 정리하면 표 2과 같다.

IV. SPLC 시스템 신뢰도

원전안전등급제어기의 전체 동작을 위한 신뢰도는 다중화된 서브시스템들의 조합으로 표현되는데, 데이터의 흐름을 중심으로 보면, 입력 혹은 통신 서브시스템을 통하여 입력된 데이터는 프로세서 서브시스템에서 연산을 거쳐 출력 혹은 통신 서브시스템으로 출력된다. 따라서 데이터를 중심으로 보면 모든 서브시스템은 직렬로 연결된 것으로 간주될 수 있으며 이 경우 전체 시스템의 신뢰도는 그림 1으로부터 식 (7)과 같이 각 서브시스템의 신뢰도의 곱으로 나타낼 수 있다. 식 (7)에서 R_i, R_o, R_b, R_p, R_h, R_c, R_s 는 각각 입력, 출력, 입출력버스, 프로세서, 통신버스, 제어통신, 상태통신 서브시스템의 신뢰도 함수를 의미한다.

$$R_{SPLC}(t) = R_i(t)R_b(t)R_p(t)R_o(t)R_h(t)R_c(t)R_s(t) \quad (7)$$

하지만 본 SPLC의 특수성으로 인하여 다중화 상태에 따른 신뢰도 함수가 맞게 적용되어야 하며, 다중화 상태의 변화에 대한 확률로 이들을 조합하여야 한다. 따라서 고장 발생에 따른 SPLC의 신뢰도를 계산하기 위해서는 동작상태를 초기상태부터 Fail Safe 상태까지 발생할 수 있는 모든 고장을 체계적으로 추적하고 이를 반영한 신뢰도를 산출하여야 한다.

1. 정상상태의 초기 신뢰도

시스템의 초기 신뢰도는 다중화된 각 서브시스템이 정상적인 다중화 기능을 수행할 때의 신뢰도로서, 식 (7)과 같이 계산된다. 삼중화 구조인 입출력 및 프로세서 서브시스템의 신뢰도 $R_i(t)$, $R_o(t)$와 $R_p(t)$의 경우 식 (5)를, 나머지 $R_b(t)$, $R_c(t)$, $R_s(t)$, $R_h(t)$의 경우 식 (6)를 이용하여 계산할 수 있다. 각 서브시스템의 신뢰도를 계산할 때 사용되는 각 모듈의 고장률은 실제 구현된 하드웨어의 고장률 추정 계산치에 따르며 표 3과 같다[15]. 단 입출력 모듈의 경우 발전소마다 구성이 다르므로, 아날로그 및 디지털 입출력 모듈이 1:1로 사용되는 것을 가정하여 두 모듈의 고장률의 평균으로 사용하였다. 이를 근거로 초기시스템 즉 정상상태의 신뢰도를 구하면 그림 5와 같다. 초기상태의 신뢰도는 동시에 두 개 이상의 고장이 발생하지 않는다는 Single-fault 가정과 고장난 부품을 즉시 교체할 수 있다는 가정, 즉 MTBR (Mean Time Between Repair)이 0이라는 가정하에 시스템의 신뢰도를 나타내는 것으로 제어시스템의 신뢰도를 평가하는 척도로 활용될 수 있다. 시스템의 고장간 시간, 즉 평균고장수명(MTTF: Mean Time To Failure)는 신뢰도 함수 $R(t)$를 적분하여 구할 수 있는데[10], SPLC의 초기 구성에서의 신뢰도 함수인 식 (7)로부터 MTTF를 구하면 45,082시간으로 계산된다.

표 3. 안전등급제어기의 모듈별 고장률.
Table 3. Failure rate by module of SPLC.

구 분	기 호	고장률
아날로그 입력모듈	λ_{ai}	4.49×10^{-6}
디지털 입력모듈	λ_{di}	7.72×10^{-6}
프로세서모듈	λ_{p}	7.78×10^{-6}
제어용 통신모듈	λ_{c}	6.88×10^{-6}
상태송수신용 통신모듈	λ_{s}	3.44×10^{-6}
아날로그 출력모듈	λ_{ao}	5.83×10^{-6}
디지털 출력모듈	λ_{do}	6.11×10^{-6}
I/O 버스	λ_{b}	8.40×10^{-6}
통신 버스	λ_{h}	8.40×10^{-6}

2. 고장모드 천이에 따른 시스템 신뢰도

앞 절에서는 초기상태, 즉 모든 다중화 모듈이 정상동작을 하는 경우 시스템의 신뢰도를 계산하였다. 그러나 고장난 모듈의 수리시간이 0이 아닌 경우, 수리에 걸리는 시간 동안은 전체 시스템의 다중화 구조가 실질적으로 변경되며, 따라서 시스템의 신뢰도가 다르게 계산된다. 본 절에서는 3장의 FTA의 결과를 토대로 다수 모듈의 고장으로 인하여 시스템의 정상상태로부터 Fail-Safe 상태까지 천이하는 과정을 고려하여 시스템의 신뢰도를 구한다. 각 고장상태간의 천이도를 보이면 그림 4와 같다. 그림 4에서 각 스테이트간의 천이는 특정 모듈에 고장이 발생함으로써 일어나는데, 각 모듈의 고장이 독립적이라는 가정하에 마코프 프로세스(Markov Process)로 가정할 수 있다. TS상태에서 MAF상태로 가는 확률 P_{MAF}는 그림 4의 FTA에 따라 프로세서 모듈 중 하나가 고장나는 경우이므로 식 (8)와 같이 표기 가능하다. 여기서 F_p, F_i, F_o, F_c, F_b 는 각각 프로세서모듈, 입출력모듈, 통신모듈, I/O버스가 고장나는 경우이며, 입출력모듈의 고장은 아날로그, 디지털 입출력 카드 중 하나라도 고장이 발생하는 경우를 의미한다. 또한 식 (8)에서 ¬ 기호는 해당 모듈이 고장나지 않는 경우를 의미하며, 이는 식 (9)에서도 동일한 의미를 가진다. 예를 들어 $\neg F_p$는 프로세서 모듈이 고장나지 않는 경우이다.

$$P_{MAF} = P(F_p \cap \neg F_i \cap \neg F_o \cap \neg F_c \cap \neg F_s \cap \neg F_b \cap \neg F_h) \quad (8)$$

또한 MTF 상태로의 천이될 확률은 TS상태에서 MTF로 천이하는 경우와 MAF상태에서 MTF로 상태를 천이하는 경우

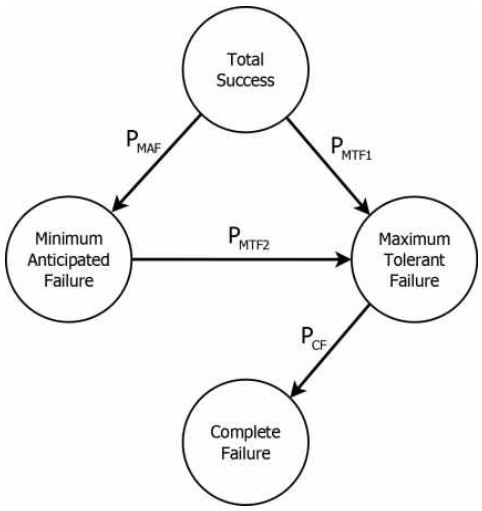

그림 4. SPLC 다중화 상태 천이도.
Fig. 4. State diagram for redundant status of SPLC.

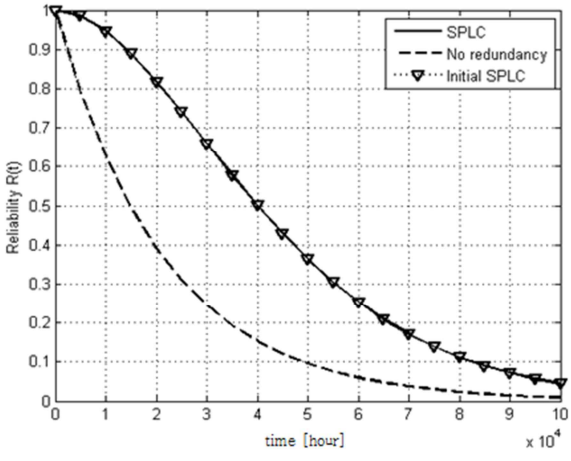

그림 5. SPLC 상태에 따른 신뢰도 곡선.
Fig. 5. Reliability curve by SPLC status.

를 고려하여 MTF에 대한 확률 $P_{M\,TF} = P_{M\,TF1} + P_{M\,TF2}$ 표현 가능하다. $M\,TF_1$의 경로는 TS에서 프로세서 모듈은 고장이 발생하지 않고, 입출력모듈, 통신모듈, 버스에 고장이 발생하는 경우이며, $M\,TF_2$의 경로의 경우는 MAF에서 모듈 중 하나 이상의 모듈에 고장이 발생함을 의미한다.

$$P_{M\,TF1} = P(\neg F_p \cap (F_i \cup F_o \cup F_c \cup F_s \cup F_b \cup F_h)) \quad (9)$$

$$P_{M\,TF2} = P(F_p \cup F_i \cup F_o \cup F_c \cup F_s \cup F_b \cup F_h) \quad (10)$$

마지막으로 CF상태로의 천이는 MTF에 상태에서 어느 모듈이라도 고장이 발생하면 천이되므로 입출력모듈, 통신모듈, 버스, 프로세서모듈의 고장확률 합으로 표현된다.

$$P_{CF} = P(F_p \cup F_i \cup F_o \cup F_c \cup F_s \cup F_b \cup F_h) \quad (11)$$

TS, MAF, MTF, CF 상태에서의 SPLC 시스템의 신뢰도를 각각 $R_{TS}(t)$, $R_{M\,AF}(t)$, $R_{M\,TF}(t)$, $R_{CF}(t)$ 라고 하면, 전체 시스템의 신뢰도 $R_{SPLC}(t)$ 는 식 (12)와 같이 계산된다.

$$R_{SPLC} = (1 - P_{M\,AF} - P_{M\,TF1})R_{TS}(t) + (P_{M\,AF} - P_{M\,TF2})R_{M\,AF}(t) + (P_{M\,TF1} + P_{M\,TF2} - P_{CF})R_{M\,TF}(t) + P_{CF}R_{CF}(t) \quad (12)$$

TS, MAF, MTF, CF 상태에서의 다중상태의 신뢰도 $R_{TS}(t)$, $R_{M\,AF}(t)$, $R_{M\,TF}(t)$, $R_{CF}(t)$는 표 1의 다중화 구분에 따라 각 서브시스템의 신뢰도를 식 (5), (6)에 표 3의 고장률을 대입하여 구한 후 식 (12)에 따라 결합하면 최종적으로 식 (13)과 같이 구할 수 있다.

$$R_{SPLC} = 0.999953 \times R_{TS} - 3.92 \times 10^{-5} \times R_{M\,AF}(t) + 3.92 \times 10^{-5} \times R_{M\,TF}(t) + 4.7 \times 10^{-5} \times R_{CF}(t) \quad (13)$$

3. 고찰

위에서 산출된 최종 신뢰도 함수를 바탕으로 신뢰도 곡선을 산출하였다. 신뢰도를 평가하기 위해서 일반적으로 평균고장수명(mean time to failure) 수치를 이용하여 신뢰도 분석대상의 신뢰도를 표현한다. 평균고장 수명은 해당 신뢰도함수를 시간에 대하여 0부터 ∞ 까지 적분하여 구하는데 원자력발전소용 제어기기는 MTTF가 10,000시간 이상이 되어야 한다. 본 논문에서 분석한 SPLC 신뢰도 곡선은 그림 5와 같다. SPLC의 신뢰도 함수 수식 (10)을 기반으로 한 평균고장수명(MTTF)은 45,080시간으로 원전안전등급기준 10,000시간을 4.5배 넘어서는 평균고장수명을 보였다. 그리고 10,000시간에서 94.63 %의 신뢰도를 보임을 확인할 수 있다.

이를 기준으로 다른 구조와 비교해보면 다중화 구조를 하지 않은 상태의 SPLC의 신뢰도 함수를 구하고, 이를 기반으로 평균수명을 산출한 결과 24,795시간으로 10,000시간은 넘지만 10,000시간 기준 신뢰도가 55%로 현격하게 낮아짐을 확인할 수 있다. 따라서 다중화 구조를 취한 다중화 제어기기가 다중화가 되어있지 않은 제어기기에 비해 신뢰도가 약 1.81배 높음을 보였다. 마지막으로 초기 다중화 상태를 구한 수식 (6)의 신뢰도 곡선을 구한 결과와 고장관계를 고려한 수식 (12)의 신뢰도 곡선은 거의 일치함을 보였다. MTTF는 수식 (12)의 MTTF가 수식 (6)의 그것에 비해 2시간이 적게 나왔다. 이는 다수의 제어기에 고장이 발생하더라도 SPLC의 구조가 능동적으로 변경됨에 따라 SPLC의 신뢰도가 삼중화된 정상상태의 신뢰도와 거의 같은 수준을 유지함을 의미하며 다중 고장에 대한 높은 내고장성을 유지하고 있음을 의미한다.

V. 결론

본 논문은 원자력발전소의 주요 안전시스템을 제어하는 내고장성 다중화 제어기의 신뢰도를 분석하였다. 대상 제어기는 차세대 원자력발전소를 위하여 설계된 안전등급의 다중화 제어기(SPLC)로서, 프로세서모듈, 입출력모듈, 통신모듈, 버스 등이 모두 3중화 혹은 2중화로 설계되어 있으며, 고장이 발생함에 따라 능동적으로 구조를 변경하는 제어기이다. 따라서 본 논문에서는 고장 발생에 따른 제어기의 운전 모드에 따라 각각의 다중화 구조와 상태를 고려한 신뢰도 함수를 산출하였다. 이를 위하여 결함수목분석(FTA)를 실행하여, SPLC의 다중화 상태에 따른 고장관계를 분석하였으며 이를 토대로 전체 시스템의 신뢰도를 산출하였다. 분석 결과 다중 고장이 발생하더라도 SPLC의 평균고장수명(MTTF)은 45,080시간으로 추정되어 안전등급 기준인 10,000시간보다 4.5배 높은 안전성을 보였다.

참고문헌

[1] K. P. Parker and E. J. McCluskey, “Sequential circuit output probabilities form regular expressions,” *IEEE Trans. on Computers*, vol. c-27, no. 3, pp. 222-231, Mar. 1978.

[2] J. A. Abraham and D. P. Siewiorek, “An algorithm for the accurate reliability evaluation of triple modular redundancy networks,” *IEEE Trans. on Computers*, vol. c-23, no. 7, pp. 682-692, Jul. 1974.

[3] S. W. Lee and H. S. Yim, “Analysis of a network for control systems in nuclear power plants and a case study,” *Journal of Control, Automation, and Systems Engineering (in Korean)*, vol. 5, no. 6, pp. 734-743, Aug. 1999.

[4] S. S. Kim, S. Park, S. H. Kim, K. Choi, C. B. Park, and C. K. Ha, “Reliability analysis of a system with redundancy management based on Monte-Carlo probability model,” *Journal*

of Institute of Control, Robotics, and Systems (in Korean), vol. 17, no. 11, pp. 1132-1137, Nov. 2011.
[5] S.-H. Cho, J.-K. Lee, and H.-G. Kim, "A study for monitoring & prognostic technology of nuclear power plant critical equipments," *Journal of Institute of Control, Robotics, and Systems (in Korean)*, vol. 17, no. 11, pp. 1090-1094, Nov. 2011.
[6] Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations, IEEE 323, 2003.
[7] V. M. Dwyer, "Reliability of Various 2-Out-of-4:G Redundant Systems with Minimal Repair," *IEEE Trans. on Reliability*, vol. 61, no. 1, pp. 170-179, Mar. 2012.
[8] D. H. Yoon, S. T. Kim, and D. H. Kim, "Safety programmable logic controller structure configuration report," *ANICS-SPLC-DR101*, pp. 1-38.
[9] D. H. Yoon, "Safety PLC Design criteria," ANIC-SPLC-DB101, Rev00, PONUTEC, 2011.
[10] D. H, Kim, "Development of the high reliable safety PLC for the nuclear power plants," Technical report of KEARI, 2012.
[11] T. J. Lim, *System Reliability Engineering*, Soongsil University Publication, 2005.
[12] NUREG-0429, *Fault Tree Handbook*, U.S. Nuclear Regulatory. Commission, Washington D.C. 20555, Jan. 1981.
[13] P. A. Crosetti, "Fault tree analysis with probability evaluation," *IEEE Trans. on Nuclear Science*, vol. 18, no. 1, pp. 465-471, 1971.
[14] R. T. Hessian Jr., B. B. Salter, and E. F. Goodwin, "Fault-tree analysis for system design, development, modification, and verification," *IEEE Trans. on Reliability*, vol. 39, no. 1, pp. 87-91, Apr. 1990.
[15] D. Y. Lee, J. G. Choi, J. Y. Kim, and J. Yoo, "Failure rate prediction and digital control devices RPS stability assessment," KAERI I&C-HF, 2005.

노 진 표

2011년 인하대학교 정보통신공학부 학사. 2013년 인하대학교 대학원 정보통신공학전공 석사. 2013년~현재 LG전자. 관심분야는 임베디드시스템, 고신뢰성 컴퓨터구조.

박 재 현

1986년 서울대학교 제어계측공학과 학사. 1988년 동 대학원 석사. 1994년 동 대학원 박사. 1995년 Univ. of Michigan 연구원. 1995년~현재 인하대학교 정보통신공학부 교수. 관심분야는 임베디드시스템, 고신뢰성 컴퓨터시스템.

손 광 섭

2004년 충남대학교 전기전자공학과 학사. 2006년 한국과학기술원 전기 전자공학과 석사. 2006년~2007년 LG전자기술원 주임연구원. 2007년 현재 한국원자력연구원 선임연구원.

김 동 훈

1984년 항공대학교 전자공학과 학사. 2006년 한남대 대학원 정보통신공학과 박사. 1987년 현재 한국원자력연구소 책임연구원.