고신뢰성 다중화 제어기기의 버스구조에 대한 결함수목분석(Fault-tree Analysis) 모델링

노진표*, 김준교*, 손광섭**, 김동훈**, 박재현*
*인하대학교 정보통신공학부
**한국원자력연구원 계측제어인간공학센터
e-mail: {jpnoh,jkkim}@emcl.org, {ksson78,dhkim4}@kaeri.re.kr, jhyun@inha.ac.kr

Fault-tree Analysis Modeling for Bus Structure of High Reliable Redundant Controller

Jinpyo Noh*, Joonkyo Kim*, Kwang-Seop Son**, Dong-Hoon Kim**, Jaehyun Park*
*School of Information and Communication Engineering, Inha University
**Korea Atomic Energy Research Institute

요 약

원자력발전소에 사용되는 모든 시스템은 IEEE에서 최고 수준의 안전도인 CLASS 1E로 분류된다. 그중에서 안전계통은 원자력발전소 안전에 관련한 모든 분야를 관리하는 계통이다. 산업이 발전함에 따라 안전계통 또한 그 규모와 복잡성이 높아지고 있고, 이에 적용되는 요구사항 또한 엄격해지고 있다. 따라서 발전소에 적용되는 안전 동작에 대한 기준을 결정하기 위해서 철저한 오류 예측분석이 수행 되어야 한다. 그 중에서도 NUREG-0492로 규정되어 있는 결함수목분석(Fault Tree Analysis)은 연역적 오류 예측 분석방법으로 원자력 발전소, 우주 산업 등에 관련된 분야는 본 방법을 통하여 오류 예측 분석이 이루어 져야한다. 본 논문에서 원전안전계통을 관리하는 구현 모델인 원전안전등급제어기기(Safety Programmable Logic Controller)에 대하여 결함수목분석을 통한 오류 예측 분석을 하였다. 또한, 위의 구조에 대하여 MSC(Message Sequence Chart)를 통한 모델링을 수행하여, 결함수목분석을 적용하는 과정에서 신뢰도 향상을 더하였다.

1. 서론

원자력 발전소에서 시스템의 오류나 고장은 특성 상 방사선 누출 및 오염 등과 같은 심각한 재해로 이어질 수 있기 때문에 원전 안전 계통 시스템은 높은 수준의 안전성 및 고 신뢰도가 요구된다. 지속적으로 높은 안전수준을 만족해야 하는 시스템의 신뢰도를 높이기 위한 다양한 방법들이 연구되고 있으며, 그 중에서 신뢰도 향상을 위한 오류에 대한 안전성 분석은 시스템 설계에서 운용까지 적용되어야 할 필수적인 요소이다[1,2,3].

원자력 발전소는 보통 100개 이상의 개별적인 기능을 가진 계통(System)으로 구성된다. 많은 계통 중 원자로 보호계통은 원자로 보호기능을 수행하고, 원자력발전소에 사고가 발생하더라도 원자력 발전소를 안전한 상태로 유지하고, 방사선 및 방사능 물질이 외부로 누출되지 않도록 하는 기능을 한다. 따라서 원자로 보호계통은 원자력 발전소의 안전성 및 신뢰성에 가장 중요한 계통이다.

위에서 언급된 원자로 보호계통에 사용되는 제어기인 PLC(Programmable Logic Controller)는 2005년부터 아날로그 형에서 디지털 형으로 개발이 적용되어 왔다. 이중 안전계통에 사용되는 제어기를 SPLC(Safety Programmable Logic Controller)라고 하며, SPLC는 전원, 입출력 모듈, 프로세서 모듈, 버스 및 통신 모듈 등의 구성요소들을 조합하여 하나의 Rack 단위로 구성된다. Safety Critical 등급인 원전계통 PLC는 엄격한 원전 요건에 따라 설계, 제작, 시험 등 모든 과정이 일반 산업용 제어기기와 달리 높은 안전수준에 맞추어 개발되고 있다. 나아가 원자력 계통은 안전성과 고 신뢰도의 요구사항을 충족시키기 위해 다양한 다중화 구조들을 사용한다[4,5].

SPLC의 다중화의 목적은 단일 채널에서의 고장에 대비한 Fault-Tolerant 능력을 제공함을 목적으로 한다. 따라서 원전 통합안전계통의 요건에 의하여 신호 검증과 능동적 결정이 요구되는 입출력 모듈과 프로세서 모듈은 삼중화가 요구된다. 따라서 프로세서 모듈과 입출력 모듈은 삼중화로 구성하고, 이들을 연결하는 버스를 이중화로 구성한 구조로 되어 있다. 하지만, SPLC에 적용된 구조에 대하여, 신뢰도와 안전성 측면에서 이를 증명하기 위한 검증된 증명도구가 필요하다.

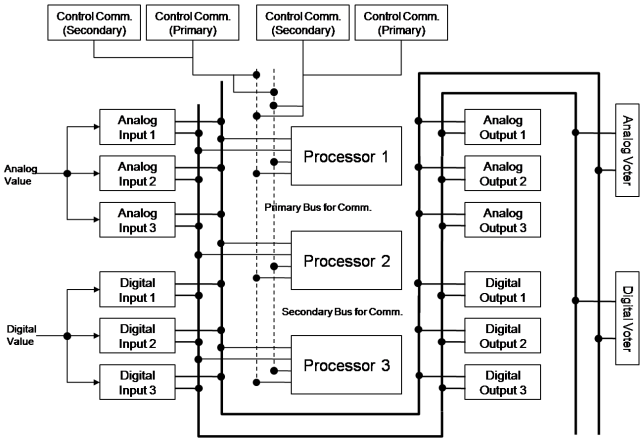
본 논문에서 적용된 검증된 증명도구로는 MSC (Message Sequence Chart)와 FTA(Fault Tree Analysis) 기법이다. MSC기법의 장점은 데이터의 흐름을 기준으로 동작에 대한 일련의 순서에 대하여, 정확히 모델링을 할 수 있다는 점이며, 실제 실시간 시스템의 상태 모델링이 적용되고 있다. FTA는 원전 오류예측 분석 도구의 요건 중의 하나이고, 표준(NUREG-0492)로 정의된 분석 방식이다. 이 방식은 오류에 대한 관련성을 나열하고 우선순위를 구분하여, 오류에 대한 하위수준의 요구조건을 만듬으로써

무엇보다 상위오류로 인하여 파생되는 모든 오류에 대하여 식별하고 수정할 수 있는 진단도구로 활용할 수 있다.

본 논문에서는 원전 안전계통에 사용되는 SPLC의 구조에 대해, MSC(Message Sequence Chart)를 이용하여 모델링을 수행하고, 그 모델에 대하여 FTA방식을 수행하여 제안되고 있는 버스 이중화에 적용하였다[3,6,7].

2. 원전안전계통 SPLC 구조

그림 1에 나타낸 SPLC는 입출력 모듈, 프로세서 모듈, 통신 모듈, 전원, 버스들의 선택적 다중화로 구성될 수 있다. 원전안전계통은 기본적으로 독립적인 채널 4중화로 구성되므로, 각 채널 내부에서 다중화 구조를 취할 경우, 각 요소들의 고장으로 인한 출력 값들의 논리 결정론성이 가장 중요한 요구사항이다. 그러므로 능동적인 판단이나 결정이 요구되는 입출력 모듈과 프로세서 모듈은 고 신뢰도를 위하여 삼중화 구조를 취한다. 장치 고장에 대한 tolerant 기능이 요구되는 통신 모듈, 버스, 전원은 이중화로 구성되어 있다. 특히 통신 모듈은 제어 데이터 전송용과 상태 데이터 전송용으로 분리하여 설계하였고, 버스는 결정론적 통신 방식인 Serial 버스를 적용하였다.



(그림 1) 원전안전계통에 사용되는 SPLC 기본구조

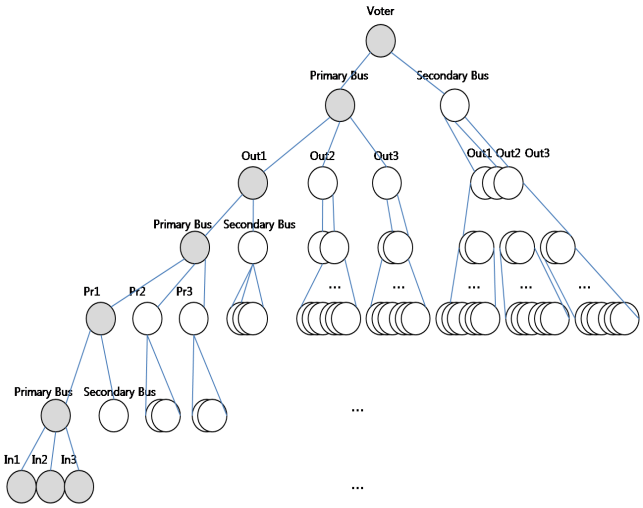
앞서 언급한, 버스 이중화 구조에서 두 개의 버스에 우선순위를 두어 그 용도를 달리 하여, 유연성을 확대시켰다. 삼중화로 구성된 입력 모듈에서 각 모듈은 데이터를 Primary 버스와 Secondary 버스를 통하여, 프로세서 모듈로 전송한다. 이 때, 우선적으로 Primary 버스의 값을 우선적으로 취하지만, Primary 버스 고장 감지 시에는 Secondary 버스에서 값을 취하게 된다. 각 프로세서 모듈은 취득된 3개의 데이터에 2/3 투표방식을 적용하고, 그 결과데이터를 마찬가지로 이중화 버스를 통하여 출력 모듈로 전송한다. 출력 모듈은 입력된 값을 비교하여, 동일 방식인 2/3 투표방식을 적용한다.

3. MSC를 이용한 SPLC 모델링

MSC(Message Sequence Chart)기법은 모델링의 한 기법으로 UML의 Sequence 다이어그램과 유사한 상호작용 다이어그램이다. 실시간 시스템의 상태 모델링에 주로 사용된다. 본 MSC를 사용하여 원전안전계통 SPLC의 동작의 한 시나리오를 구상하여, 이중화 버스 구조에 적용하여 오류분석에 적합한 모델링을 수행하였다[9].

SPLC의 구조는 같은 동작의 다중화 형태로 각 노드에서 수행하는 절차는 각 노드마다 데이터 요청, 수락, 무응답, 오류응답 4가지 형태를 반복하는 상태천이를 가진다.

각 상태에는 2가지 내부노드가 존재한다. 본 논문에서는 보내는 쪽(Sender), 받는 쪽(Receiver)로 구분하였다. 각 단계에서 보내는 쪽, 받는 쪽만 다를 뿐 동작행태는 동일하다. 이를 계층적으로 구분하고, 관계를 트리로 구성하여, SPLC 구조의 데이터 흐름을 모델링 하였다. 최상위 노드부터 깊이 우선 탐색(Depth-First Search) 방법으로 각 노드를 거치게 되고, 각 노드마다 앞서 제시한 상태 천이에 따라 동작이 수행된다. 깊이 우선 탐색에서 판단기준은 각 노드마다 지정된 Receiver로부터 수락상태면 전진탐색, 무응답 상태이면 후진을 한다. 예를 들어, 최종 값을 출력하려면, 2/3 투표법을 수행하여 결과를 뽑아낸다. 2/3 투표법을 수행하려면 각 출력 모듈로부터 값을 받아오는 과정이 필요하고, 버스가 이중화 되어있으므로, 버스선택의



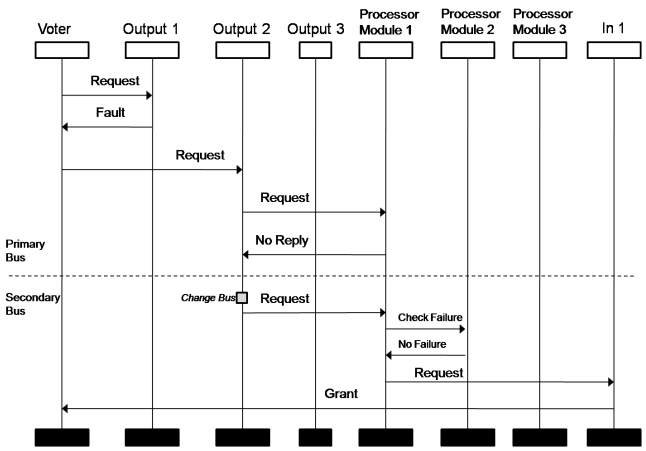
(그림 2) MSC를 적용한 SPLC 구조의 트리화

노드가 필요하다. 출력 모듈 역시 버스이중화를 거쳐, 3개의 프로세서 모듈로부터 값을 가져오고, 다시 버스이중화를 거쳐, 3개의 입력 모듈로부터 값을 가져온다. 이를 트리로 표현하면 그림 2와 같다.

트리로 표현한 이유는, 데이터가 입력부터 출력까지 각각의 입출력 모듈, 버스, 프로세서 모듈을 거쳐 순회하게 되는데, 중간과정에서 모듈이 하나 고장이 발생하면 남아있는 정상적인 모듈에 대해서 값을 가지고 온다. 따라서 고장에 대한 모든 경우의 수를 표현하기 위해서 트리를 이용하여 구성하였다.

그림 2의 회색노드를 예를 들면, 2/3투표를 적용하기 위해서 총 3가지 경우의 값을 가져와야하는데, 그 회색노드

가 첫 번째 값을 입력부터 출력까지 가지고 오는 하나의 경로가 된다. 최상위 노드(Voter)를 기준으로 우선순위가 적용된 버스에서 우선적으로 Primary 버스로부터 값을 요청하고 버스에 이상이 없다면, Primary 버스는 출력 모듈 1로부터 값을 요청하고, 이상이 없으면, 다시 Primary 버스를 통하여 프로세서 모듈 1로 값을 요청한다. 마찬가지로 요청에 대한 응답이 정상이면, Primary 버스를 통하여 최종 입력 모듈로 값을 가져오는 일련의 과정을 수행하게 된다.



(그림 3) 특정 상태의 SPLC 구조의 MSC 모델링

나아가, 오류가 발생 했을 상황에 대한 상태를 그림 3과 같이 모델링하였다, 투표를 하는 모델 즉, 그림 2의 트리의 최상단에서 출력모듈 1로부터 값을 요청하고, 잘못된 값을 받을 시, 출력모듈 고장으로 판단 후, 출력모듈 2에 값을 요청한다. 출력모듈 2가 정상이면, 프로세서 모듈 1로 값을 요청하는데 정해진 시간보다 늦게 아무런 반응이 없으면 버스고장으로 판단하고, 나아가 인접한 프로세서 모듈로부터 고장유무 또한 판단하는 과정을 거친다. 이상이 없으면 정상적으로 입력모듈 1로 값을 요청하고, 정상적으로 값을 불러오게 된다. 그림 3은 그 흐름에 대한 MSC를 나타낸 것이다.

4. Fault Tree Analysis 적용

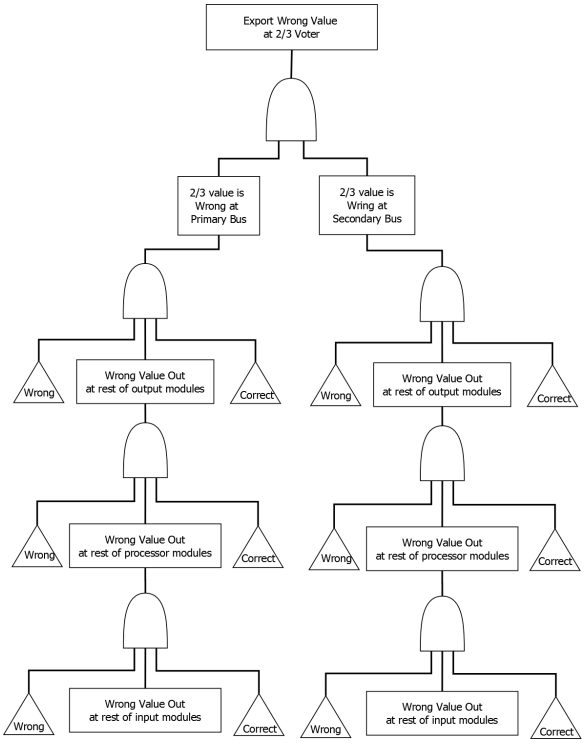
FTA(Fault Tree Analysis)는 미국 산업 표준문서(NUREG-0492)를 비롯하여, IEC61025, MIL-HDBK-338에 규정되어 있는 연역적 방법의 오류분석 도구이다. FTA를 구현함에 있어서 기대효과는 오류에 대한 관련성을 나열하여, 우선순위를 구분하고, 하위 레벨에 대한 요구조건을 만드는 도구로 사용가능하다는 것이다. 또한, 최상위 오류가 야기한 요소들에 대해 식별하고 수정할 수 있는 진단도구로 활용가능하다[6,7].

NUREG-0492에서는, 오류 예측분석에 선행되어야 하는 두 가지 조건을 다음과 같이 명시하고 있다[7].

- Choice of the appropriate system boundary
- Define to establish a limit of resolution

위의 두 조건을 중심으로 오류를 적용할 범위와 깊이를 정하였다. 오류를 정하는 범위는 그림 1에 나타난 이중화버스를 중심으로 데이터의 흐름에 대하여 분석하였고, 분석 깊이는 각 수준에서의 출력형태만 3단계로 구분하였다.

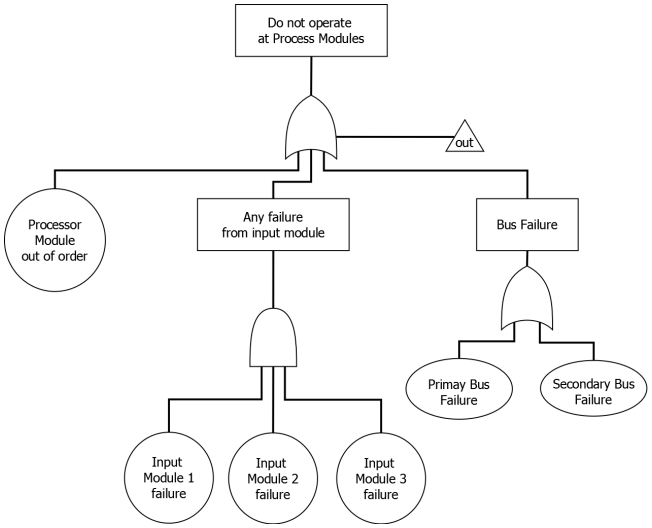
먼저 전체시스템 오류에 대하여 적용하였다. 최상단 오류를 2/3 투표를 수행해서 나온 값이 오작동인 경우를 “Complete Failure”로 규정하였고, 이를 중심으로 예상 오류가능성에 대하여, FTA(Fault Tree Analysis)를 수행하였다. SPLC의 다중화 특성상 동일 입력이 이중화된 버스를 통하여 삼중화 된 프로세서 모듈과 입출력 모듈을 거쳐 나오게 된다.



(그림 4) SPLC 전체 구조에 FTA 적용

결과적으로, 최종 출력 단에서 잘못된 값이 나오려면, 3개의 출력 모듈 중 비정상적인 값이 2개가 나와야 한다. 그림 4를 참조하면, SPLC구조에서 값의 연산오류가 일어날 수 있는 곳은 출력 모듈, 프로세서 모듈, 입력 모듈이다. 각 삼중화 된 모듈에서 오류가 나려면 두 모듈에서는 오류가, 다른 모듈에서는 정상적인 값이 나와야 한다. 이 모든 조건이 모든 모듈에 걸쳐 충족되어 질 때, 오류가 발생하게 된다. AND게이트는 하위 두 조건이 모두 일어나면 일어나는 것이고, 직사각형은 즉각적인 오류사건에 대하여 나타낸 것이다. 마지막으로 세모는 이미 일어난 사건에 대한 입력을 나타낸 것이다.

그림 5는 특정 프로세서 모듈의 오류에 대하여 FTA를 적용한 것이다. 이는 프로세서 모듈에 고장이 발생했다고 판단하는 조건을 나열하고 있으며, 버스 고장, 모든 입력 모듈로부터 값을 못 가져온 경우, 프로세서 모듈에 고장이 발생한 경우로 나타낼 수 있다.



(그림 5) 프로세서 모듈에 대한 FTA 적용

그림 5의 FTA 결과를 활용하여 사전에 프로세서 모듈의 고장에 대한 대비 또는 해결책을 강구 할 때, 효과적으로 쓰일 수 있다.

5. 결론

본 논문에서는 원전안전계통 SPLC의 구조에 대해서 MSC를 이용하여 모델링을 수행하였다, 모델링을 기반으로 프로세서 모듈, 입출력 모듈의 삼중화와 버스의 이중화 구조에 대하여 FTA분석을 수행하였다. 분석의 결과로 SPLC 구조에서 최종 오류가 나기위한 조건을 나열하였다. 하지만, 이는 어디까지나 논리적인 분석이다. 이를 수학적으로 모델링하고, 확률의 함수를 적용한 시뮬레이션을 통하여 신뢰도 있는 분석이 필요하다.

감사의 글

본 연구는 2012년도 지식경제부 재원으로 한국에너지 기술평가원(KETEP)의 지원을 받아 수행한 원전기술혁신사업 연구 과제입니다. (No. 20101610100001G)

참고문헌

[1] Jae-Yoon Sul, Ki-Chang Kim, Yoo-Sung Kim, and Jaehyun Park, “Implementation of High-Reliable MVB Network for Safety System of Nuclear Power Plant, The Transactions of the Korean Institute of Electrical Engineers, Vol. 61, No. 6, pp. 859-864, 2012.

[2] IEEE 352 “IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety System”, 1987.

[3] Israel Koren, Stephen Y, H. Su, “Reliability Analysis of N-Modular Redundancy Systems with Intermittent and Permanent Faults”, IEEE Transactions on, Vol. c-28, No. 7, July 1979.

[4] 윤동화, 김성태, 김동훈, “안전등급 제어기기(SPLC) 구조 설정 보고서”, ANICS-SPLC-DR101, pp 1-38.

[5] IEEE 323 “Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations”, 2003.

[6] Crosetti, Paul A, “Fault Tree Analysis with Probability Evaluation,” IEEE Transactions on Nuclear Science, Vol. 18, pp. 465-471, 1971.

[7] NUREG-0492, “Fault Tree Handbook”, U.S. Nuclear Regulatory Commission, 1981.

[8] Robert T. Hessian Jr, Barbara B. Salter, and Edwin F. Goodwin, “Fault-Tree Analysis for System Design, Development, Modification, and Verification”, IEEE Transactions on Reliability, Vol. 39, No. 1, pp. 87-91, 1990.

[9] David Harel, P.S. Thiagarajan, “Message Sequence Charts”, April 8, 2003.

[10] IEEE 7-4.3.2 “Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations”, 2010.

[11] Fan Wang, Duo-Sheng Wu, “Design and Implementation of a Missile Fault Diagnosis System Based on Fault-Tree Analysis”, Machine Learning and Cybernetics, 2007 International Conference on, Vol. 2, pp. 1501-1054, 2007.

[12] Xinqian Bian, Chunhui Mou, Zheping Yan, and Jian Xu, “Simulation model and Fault Tree Analysis for AUV”, Mechatronics and Automation. ICMA 2009. International conference on, pp. 4452-4457, 2009

[13] Lee, W. S., Grosh, D. L., Trillman, F. A., and Lie, C. H., “Fault Tree Analysis, Methods, and Applications, A Review”, IEEE Transactions on Reliability, Vol. R-34, pp. 194-203, 1985.

[14] Batzias, F. A., Siotorou, C. C., “Investigating the causes of biosensor SNR decrease by means of fault tree analysis”, IEEE Transactions on Instrumentation and Measure, Vol. 54, pp. 1395-1406, 2005.

[15] Geymayr. J. A. B, Ebecken, N. F. F., “Fault-tree analysis: a knowledge-engineering approach”, IEEE Transactions on Reliability, Vol. 44, pp.37-45, 1995.