2001년 춘계학술발표 논문집
한국원자력학회

디지털 안전 계통에 대한 확률론적 안전성 평가의 주요인자 및 정량분석

Quantitative Analysis on Important Factors of the PSA of Digital Safety-Critical Systems

강현국, 성태용, 이기영

한국원자력연구소
대전광역시 유성구 덕진동 150

요 약

디지털 기기가 원전의 안전 계통에 도입되면서 그 안전성의 정량적 평가에 대한 필요성이 높아지고 있다. 본 논문에서는 이러한 정량평가의 기초 단계로서, 분석의 결과에 큰 영향을 미치는 인자들을 정리하고 그 인자들의 변화에 따른 전체 계통의 안전성 변화를 정량적으로 분석하였다. 소프트웨어의 오류 가능성, 오류 검출 기법의 검출범위, 공통원인 고장의 적용 등이 정량적 안전성 분석 결과에 중요한 영향을 미치는 인자로 추출되어 분석의 대상이 되었으며, 소프트웨어/하드웨어 상호작용, 시분할 시스템 모델링 방법, 환경인자 등은 분석 결과에 영향을 미칠 것으로 판단되나 현실적인 분석에는 난점이 있으므로 본 논문의 범위에서 제외하였다. 정량 분석의 결과, 추출된 세가지 인자의 변화는 디지털 시스템의 안전성에 수배에서 수십배까지의 영향을 미치는 것으로 나타났으므로 정량평가 결과의 왜곡을 최소화하기 위해서는 이러한 주요 인자를 적절하게 취급하는 것이 중요한 것으로 나타났다. 또한 계통 설계자의 입장에서는 이들 주요 인자를 고려하여 설계를 수행하면 보다 효과적으로 계통의 안전성을 높일 수 있을 것으로 판단된다.

Abstract

The introduction of digital equipment to the safety-critical system requires the quantitative assessment of digital systems. The aim of this paper is to summarize the factors which should be represented by the model for probabilistic safety assessment and to analyze the effect of those factors. We also demonstrate the effect of these critical factors. The failure rate of software, the coverage of fault-tolerant mechanism, and the treatment of common mode failures are considered in this study. Because the result of quantitative analysis shows the severe effect of these factors, inappropriate considerations on these factors will induce unreasonable assumptions and severely distort the analysis results. We expect that the analysis result will provide valuable feedback to the system designers of digital safety systems.

제 1 장 서론

1-1. 디지털 시스템의 원자력 발전소 안전계통에의 적용

아날로그 기기에 비해 데이터의 전송과 처리 능력이 뛰어나며, 보다 정확하고 신뢰성있게 신호를 처리할 수 있다는 장점 때문에 디지털 기기들의 사용이 급속히 확산되어 기존의 아날로그 기기를 거의 완전히 대체하고 있다. 원자력 분야에서도 디지털 계측제어계통의 전면 채택이 전세계적으로 연구·설계중인 차세대 원자력 발전소의 중요한 특징 중의 하나가 되고 있다. 그러나 여러가지 장점에도 불구하고 디지털 계측제어계통이 가지는 불확실성 때문에 세계 각국의 안전규제기관의 견해가 신중하고 유보적인 입장을 견지하고 있어 이러한 설계의 실제 채택에 어려움으로 작용하고 있다. 안전성을 중요시하는 원자력산업계에서 고장기전이 불명확하고 급속한 기술진보가 발생하는 디지털 기술이 엄격한 원자력 산업계의 안전성 요건을 만족하기 어렵기 때문이다. 그러나 기존의 아날로그 기기를 사용하는 플랜트들은 부품 조달이 원활하지 못해 더 이상의 유지·보수에서 어려움을 겪고 있다. 또한 설계와 제작의 측면에서도 디지털 기기를 이용할 경우 단순화·표준화로 인한 설계 편의성 및 유지보수 편의성 향상 등 많은 장점이 있다.

국내에서도 신규 건설중인 한국형 표준원전 및 차세대원전의 원자로 보호계통과 공학적안전설비 작동계통과 같은 안전기능을 수행하는 계통에 디지털계측기술을 적용하고 있으며, 가동중인 원전에 대해서도 노후 기기에 대한 디지털 기기로의 대체가 추진되고 있다. 디지털 기술 특유의 불확실성·불명확성을 극복하고 원자력발전소의 안전관련 분야에 적용하기 위해서는, 확률론적 안전성평가(probabilistic safety assessment; PSA)와 같은 정량평가 방법의 적극적인 활용이 중요한 역할을 할 것으로 판단된다.

1-2. 정량적 안전 평가와 디지털 기기

PSA는 인허가 측면에서뿐만 아니라 원전의 설계 및 운전을 포함하여 원전의 안전성을 종합적으로 평가하는 도구로써 1980년대부터 사용이 확대되어왔다. 원자력 발전소에서 일어날 수 있는 가상사고에 대해 발전소 설비 및 운전원의 대응을 논리적인 모델로 구축하여 노심손상을 유발하는 사고시나리오를 도출하고 그 발생 가능성 및 결과를 평가하여 대상 원전의 안전성을 평가한다. 발전소 모델 구축 시에는 초기사건을 완화시킬 수 있는 비상노심냉각계통과 같은 안전 기능들과 이들의 운전에 필요한 계측제어나 전력 계통과 같은 지원 계통도 모델되어 각 계통의 신뢰도를 구할 수 있다.

일반적인 원전에 대한 모델 구축은 초기사건 발생 이후 이를 완화시키는 계통들의 대응을 모델한 사건수목 (event tree)과 각 계통의 요구되는 기능 수행을 나타내는 고장수목 (fault tree)으로 구성된다. 이들 모델을 정량화하여 사고경위나 계통의 기능 실패에 대해 발생원인을 나타내는 최소 단절집합 (minimal cutset)과 이들의 발생 빈도나 확률을 구한다. 계통 설계 시에는 이들 결과로부터 기능 고장을 유발하는 고장 원인과 그들의 순위를 파악함으로써 설계의 타당성을 입증할 수 있으며, 설계의 취약점을 파악하여 개선안을 도출할 수 있다. PSA에서 의미 있는 결과를 도출하기 위해서는 발전소의 사고에 대한 대응이나 계통의 기능과 물리적 구성 상태를 정확히 모델하여야 하며, 사용되는 신뢰도 자료가 정확하여야한다.

PSA는 원전의 안전성을 종합적이며 정량적으로 평가하기 위한 중요한 안전성평가 수단으로 사용되고 있으며, 신규 원자력 발전소 건설시 인허가 사항으로 제출이 요구된다. PSA는 논리적으로 이상사건에 대한 발전소 대응을 모델하며, 이를 통해 각 사고경위의 원인 및 발생빈도를 기기의 단위까지 파악 할 수 있으며, 각 계통의 주어진 기능을 수행실패에 대해서도 원인과 각 확률값을 구할 수 있다. 이러한 결과는 원하지 않는 사건의 발생 확률과 원인을 밝힐 수 있기 때문에 이를 이용하여 설계 검증, 정비 최적화 등에 다양하게 이용된다. 최근에는 미국을 중심으로 PSA 결과를 결정론적인 규제의 보완 수단으로 사용하고 있으며, 국내에서도 이의 채택이 적극적으로

추진되고 있다 [1. 2]. 또한 PSA는 초기 설계 단계에 적용되어 설계 검증에 이용되며 설계 개선에도 활용될 수 있다[3].

그러나 기존 원전에 적용되어 왔던 PSA 방법론을 그대로 최근의 디지털 기기에 적용하여 안전성을 정량화하는 데에는 몇가지 문제점이 있다 [4]. 디지털 기술의 특성상 PSA에서 모델이 힘든 부분이 있으며, 대표적인 것으로는 소프트웨어에 대한 신뢰도 평가, 동적인 디지털 기술 특성 모델 방법, 고장내구성 기법의 평가 등이 있다. 이외에도 정량평가 방법론과 관련된 고장 유형의 평가, 신뢰도 자료의 타당성, 초기사건 모델, 공통원인 고장 (Common Cause Failure : CCF) 모델 방법 등과 같은 다양한 문제가 있다.

본 논문에서는 이러한 디지털 시스템의 정량평가에서의 주요 인자들을 정리하여 제시하고, 실제 한국형 표준원전을 예제로 하여 PSA를 적용해 보았다. 한국형 표준원전은 아직 설계가 확정되지 않았으므로 많은 가정을 포함하여 모델링을 수행하였으나, 이러한 분석을 통해 각 인자들이 원자로 보호 계통의 불가용도에 미치는 영향을 정량적으로 파악할 수 있다. PSA의 특징인 정량적인 결과 생성이라는 측면을 적극적으로 활용하므로써, 설계 개선을 한층 효율화할 수 있을 것으로 판단된다. 이러한 연구는 디지털 기기의 특성을 적절히 반영한 신뢰도 모델을 구축하고 결과를 도출할 수 있도록 함으로서 원전에의 디지털 기기 적용을 위한 인허가에 필수적인 역할을 수행할 뿐만 아니라, 신뢰도 배분 및 향상 등 계통 설계에 유용한 정보를 제공하여 궁극적으로는 원전의 안전성 향상에 기여할 것으로 기대한다.

2. 디지털 보호 계통의 정량적 안전 평가 현안

서론에 언급한 바와 같이, 디지털 시스템의 정량적 평가를 수행하는데는 여러가지 문제점이 있다. 디지털 기술의 특성상 정적인 특성을 가지는 PSA에서 모델이 힘든 부분이 있으며, 대표적인 것으로는 소프트웨어에 대한 신뢰도 평가, 동적인 디지털 기술 특성 모델 방법, 고장내구성 기법의 평가 등이 있다. 이외에도 정량평가 방법론과 관련된 고장 유형의 평가, 신뢰도 자료의 타당성, 초기사건 모델, 공통원인 고장 (Common Cause Failure : CCF) 모델 방법 등과 같은 다양한 문제가 있다. 이를 나열해 보면 다음과 같다 [5].

Modeling the multi-tasking of digital systems

Estimating software failure probability

Estimating the effect of software diversity and V&V efforts

Estimating the coverage of fault-tolerant features

Estimating the CCF probability in hardware

Modeling the interactions between hardware and software.

Failure mode of digital system

Environmental effects

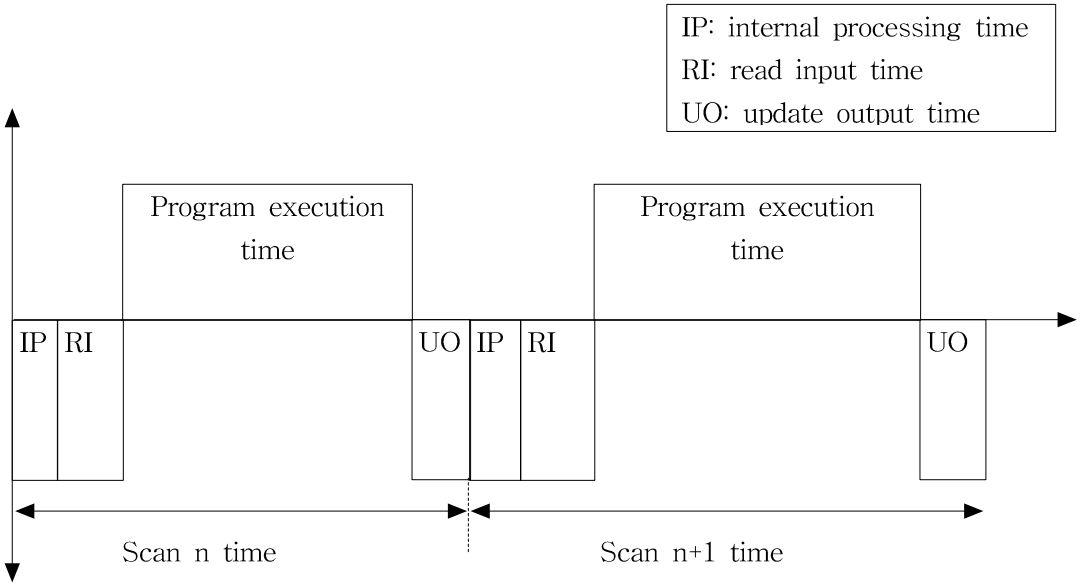
Digital system induced initiating events including human errors

본 논문에서 이들 분야를 모두 다루는 것은 현실적으로 어려우므로, 그중 가장 PSA 결과에 미치는 영향이 크다고 생각되는 인자들 3가지(소프트웨어 신뢰도, 고장내구성 기법의 검출 범위, 하드웨어의 CCF 적용)만을 다루었다.

2-1. 고장내구성 기법의 검출 범위

일반적으로 산업 현장에서 많이 이용되는 대표적인 컴퓨터 기반 시스템(computer-based system)인 PLC의 경우에는 감시 타이머를 내장하고 있다. 원전에서는 이렇게 내장된 감시 타이머를 이용하기 보다는 외부에 별도의 감시 타이머를 장착하여 계통을 감시하는 방법을 많이 이용한다. 감시 타이머는 디지털 시스템에 이상이 생겼을 경우, 이를 감지해 내기 위한 가장 기초적인 장치인데, PLC와 같이 주기적인 반복실행(cyclic operation)을 위주로 하는 시스템에 특히 효과적으로 적용될 수 있다.

감시 타이머는 하드웨어 interrupt를 발생시키는 일종의 interval timer로서, <그림 1>에 도시된 바와 같은 작업 수행 시간을 이용하여 일정시간 이상 신호가 발생하지 않을 경우 시스템에 문제가 생긴 것으로 판단하여 원전의 정지 신호를 발생시킨다. 이것은 “정해진 시간을 초과하는 코드 실행은 시스템의 오류를 의미한다”는 가정하에 이루어진다. 그러나 모든 시스템의 오류가 시간 지연을 유발하는 것은 아니므로, 감시 타이머의 유효범위는 제한되어 있다는 점에 유의하여야 한다. 문제는 이와 같은 유효 검출 범위를 추정하는 것이 쉽지 않다는 것이며, 이와 관련한 추후 연구가 필수적일 것으로 판단된다.



<그림 1> PLC의 작업 수행 시간 개념도

2-2. 소프트웨어의 신뢰도

소프트웨어의 신뢰도를 확률적인 방법으로 추정할 수 있는가 하는 것은 소프트웨어공학 분야에서도 오랜 논란을 불러 일으켰던 문제이다 [6]. 최근에는 일반적으로 소프트웨어의 오류는 설계 오류로 정의하고 있다. 즉, 소프트웨어는 결정론적인 것이며 '고장률(failure rate)'의 개념으로 표현될 수는 없다는 것이다. 그러나 실제 적용에 있어서는 소프트웨어 오류 발생의 무작위성을 인정하는 '고장률'을 이용하는 경우가 많은데, 이것은 소프트웨어에 대한 고장률 개념은 '빈도'가 아니라 '기대치(확신도)'의 개념이기 때문이다. 테스트 결과 한번도 오류를 일으킨 적이 없는 소프트웨어가 잠재되어 있던 문제점으로 인해 '앞으로의 실제 사용시 고장을 일으킬 것으로 기대하는 정도'를 추정하는 문제가 되기 때문이다. 이러한 무작위성 가정에 대해서 'error crystal'의 개념을 이용하여 정당성을 설명하는 것이 일반적이다. 즉, 소프트웨어의 잠재된 오류가 특정부분(error crystal)에 숨어 있다가 입력값이 그 부분을 활성화시킬 경우에 비로소 외부로 오류가 드러난다는 것인데, 이 입력값의 무작위성으로 인해 소프트웨어가 오류를 발생시키는 양상이 무작위성을 띄게 된다는 것이다 [7].

일단 소프트웨어의 신뢰도를 무작위성을 가지는 고장률의 개념으로 취급할 수 있다고 가정하면, 고장률의 추정이 필요하게 된다. 하드웨어의 경우에는 각 부품들의 고장률에 관한 많은 표준을 참고할 수 있으나 소프트웨어는 이 같은 것이 없으므로 직접적인 테스트가 필요하게 된다. 원자력발전소의 안전계통에 오류가 발견된 소프트웨어를 그대로 적용하는 것을 상정하는 것은 비현

실적이다. 따라서 테스트를 몇회 수행하던지 간에, 소프트웨어 관련하여 발생한 오류가 없는 결과를 얻게 될 것이다. 위에 언급한 바와 같이 '앞으로의 실제 사용시 고장을 일으킬 것으로 기대하는 정도'를 추정하기 위한 기본 자료로 테스트 횟수를 사용하는 것이다. 테스트 방법 개발의 핵심 요소는 테스트 횟수의 결정, 하드웨어 고장과 소프트웨어 고장의 구분, 테스트 입력자료 생성, 테스트의 coverage 산출로 정리될 수 있다. 이 중 테스트 횟수의 결정은 결과 자료의 처리 방법과 깊은 관련이 있으며, 테스트의 현실성을 가늠하는 중요한 척도가 될 것이다. 또한 시간관련 알고리듬을 포함한 소프트웨어(예를 들어 PPS의 variable setpoint)의 경우 현재의 입력값만으로 결과를 산출하는 것이 아니라 과거의 자료까지 이용하므로, 이러한 소프트웨어의 테스트를 위한 방법론 개발도 실행적인 면에서 중요한 역할을 할 것으로 판단된다.

2-3. 공통원인 고장의 적용

공통원인 고장(CCF)의 적용은 계통의 설계에 의해 결정된다. 디지털 시스템의 경우 위험도가 일부 기기에 집중되게 되므로 특히 CCF의 처리가 중요하다. CCF의 처리 방법에 따라 PSA결과가 크게 달라지기 때문이다. 서로 상이한 제작자의 제품이라 할 지라도 동일 부품을 이용하거나 동일 소프트웨어를 이용함으로써 CCF의 확률을 가질 수 있으므로 세심한 처리가 필요하다. 따라서 디지털 기기의 특성을 정확히 고려한 CCF 처리 방법론에 대한 연구가 시급하다.

디지털 안전 계통에서는 많은 수의 다중화를 기본으로 한다. 즉, 하나 또는 두개의 시스템에 의지할 경우 원전이 이상상태가 되었을 때 시스템이 제대로 구동되지 않을 가능성이 있으므로, 여러 채널에 여러개의 시스템을 병렬로 두어 그 신뢰도를 높이는 것이다. 실제로 한국형 표준 원전의 디지털 원자로 보호 계통에서는 꼭 같은 역할을 하는 동시논리 프로세서 모듈과 디지털 출력 모듈이 각각 16개나 사용되고 있다. 그런데, 이렇게 많은 다중성을 두었다고 할 지라도 그 많은 기기가 동시에 같은 원인으로 고장을 일으키는 확률이 높다면 그 다중성은 효력을 상실하게 된다. 따라서 이 공통원인 고장을 회피하기 위한 설계가 매우 중요하다.

3. 가상의 한국형 표준원전 원자로 보호계통의 PSA 모델

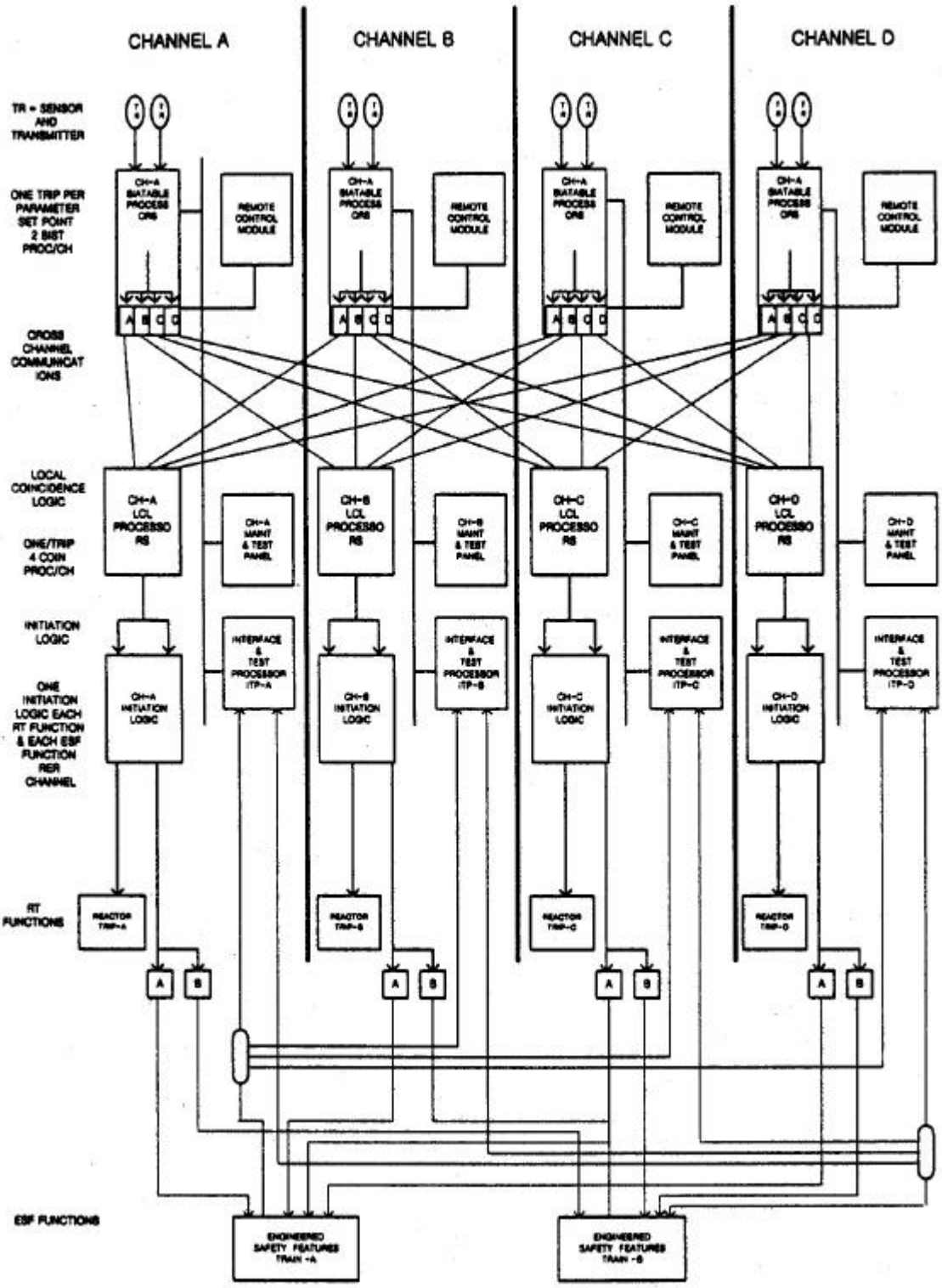
한국형 표준원전은 현재 건설중인 단계이므로 그 세부 시스템 설계가 아직 확정적이지 않거나 외부에 공개되어 있지 않다. 따라서 본 논문에서는 일반적인 가압경수로의 보호계통으로 가정할 수 있는 형태의 가상의 시스템을 대상으로 분석을 수행하였다. 본 논문에서 제시한 결과는 가상의 시스템에 대하여 많은 가정을 포함하고 수행한 정량평가의 결과이므로, 실제 시스템 설계가 확정되었을 때에는 새로운 정량 평가의 수행이 불가피하다. 그러나 이러한 초기 분석을 통해 다양한 설계의 대안을 정량적으로 검토해 볼 수 있으며 어떤 부분에서 설계를 개선해야 할지를 효율적으로 찾아낼 수 있다는 장점이 있다.

3-1. 모델링 대상 계통의 개요 및 가정

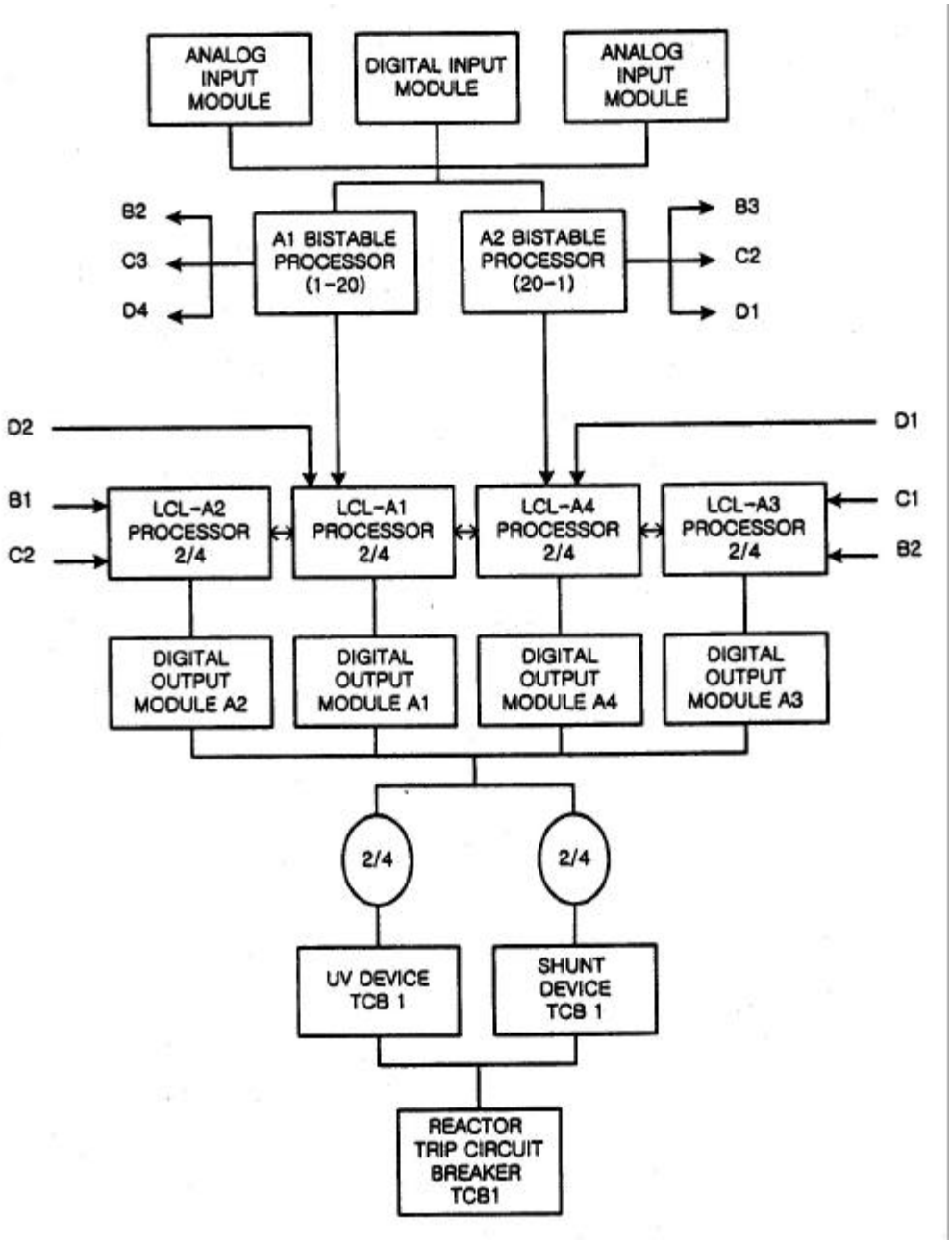
모델링의 대상이 되는 시스템은 전체적으로 4개의 채널로 구성되어 있으며, 각 채널은 2대의 비교논리 프로세서와 4대의 동시논리 프로세서를 포함하고 있다. 각 비교논리 프로세서에 아날로그 입력을 제공하는 모듈은 2개씩에 연결된 것으로 가정하고, 동시 논리 프로세서는 1개씩의 디지털 출력 모듈에 연결된 것으로 가정하였다.

본 논문의 목적은 대상 시스템 설계간의 정량 비교를 통해 최적 설계를 찾고자 하는데 있으며, 고려의 대상이 되는 인자는 제2장에서 설명한 바와 같이, 소프트웨어 신뢰도, 고장내구성 기법의 검출 범위, 하드웨어의 CCF 적용으로 한정되어 있으므로 다른 요인들에 대해서는 과감한 가정을 도입하였다. 따라서 본 논문에서 사용된 가정들이 적절하다는 것은 보장되지 않으며 추후 연구의 필요가 있는 부분이 많이 포함되어 있다. <그림 2> 와 <그림 3>은 [8]에 제시된 설계 개념도들이다.

대상 계통내에서 비교논리 프로세서는 동시논리 프로세서를 이용하여 감시가 가능하므로 그 신뢰도는 1로 가정하였으며, 동시논리 프로세서는 감시 타이머를 이용하여 감시를 수행하는데 그 고장 검출 확률은 본 논문에서 가변적인 것으로 처리하여 분석하였다. 또 각 동시논리 프로세서 내에는 소프트웨어가 탑재되어 있는데, 그 소프트웨어가 동일한 것으로 가정하고 소프트웨어 오류가 시스템의 공통원인 고장으로 작용하는 것으로 가정하였다. 소프트웨어 고장율은 가변적으로 처리하여 분석의 대상으로 하였다.



<그림 2> 원자로 보호계통 기능 개념도



<그림 3> 채널내의 기능 불럭도

감시의 대상이 되지 않는 입출력 모듈의 경우 그 구성을 다르게 하여 CCF를 회피하는 설계를 하므로써 신뢰도 향상을 도모할 수 있다. 본 논문에서는 입출력 모듈의 설계의 3가지로 나누어, 단일 종류의 입력 모듈과 출력 모듈을 사용하는 경우, 2종류의 입력 모듈과 단일종류의 출력 모듈을 사용하는 경우, 입력 모듈과 출력 모듈 모두 각자 2종류의 기기를 사용하는 경우로 나누어 분석을 수행하였다. 이때 2종류의 모듈내에서는 공통원인 고장이 전혀 발생하지 않는 것으로 가정하여 모델링을 수행하였다.

분석의 대상이 되는 것은 디지털 계통에 한정되므로, interposing relay에서 정지차단기(trip circuit breaker; TCB)까지의 계통에서 사용된 기기의 신뢰도는 1로 두었다. 마찬가지 이유로 센서 및 송출기(transducer)의 신뢰도도 1로 하였다.

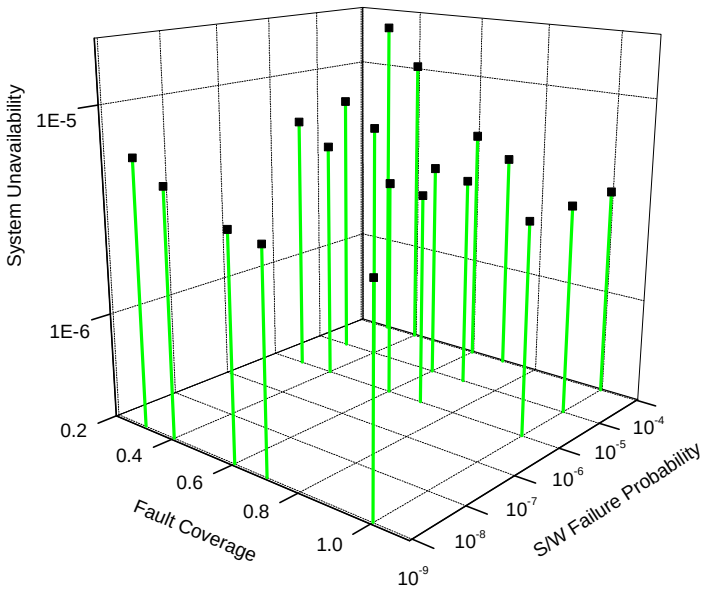
또한 정지변수는 2개만을 고려하였다. 단일 계통이 다수의 변수를 처리하는 디지털 계통의 특성상 많은 정지 변수를 고려할 수록 그 신뢰도가 아날로그 시스템에 비해 상대적으로 낮아질 것으로 판단되므로 실제 설계가 완성되었을 때에는 보다 체계적인 분석이 필요할 것으로 판단된다.

3-2. 모델링 결과

본 논문에서는 한국원자력연구소의 TwTree 안전성 분석 패키지를 이용하여 분석을 수행하였으며, 확률값을 직접 입력해야 하는 기본사건의 확률은 표준원전에서 사용될 것으로 예측되는 PLC 모듈의 신뢰도값을 이용하여 처리하였다. 소프트웨어의 고장률이 상승하거나 감시 타이머의 오류검출률이 감소할 수록 시스템의 불가용도가 높아지는 것을 관찰할 수 있으며, 감시 타이머의 오류검출률이 1일 경우, 즉 모든 오류를 감시 타이머가 검출할 수 있을 경우에는 소프트웨어의 고장은 시스템에 영향을 미치지 못한다.

(1) 단일종류의 디지털 출력과 단일종류의 아날로그 입력 모듈을 사용한 설계

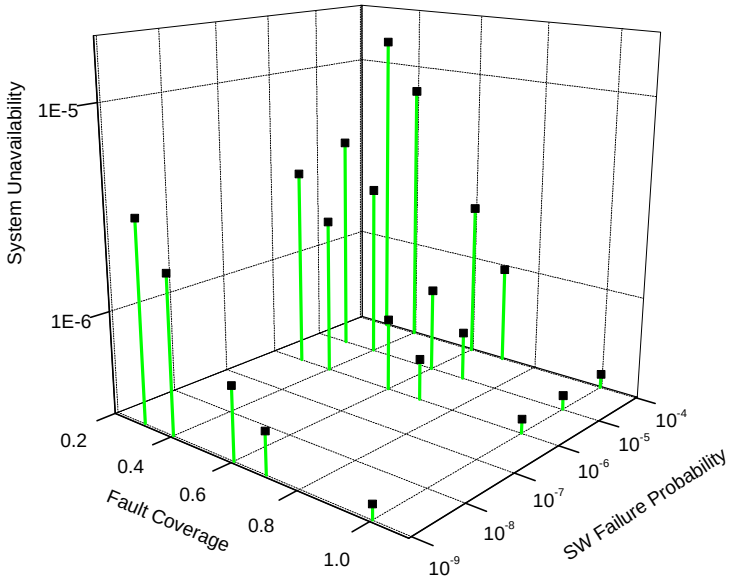
시스템 불가용도		SW Failure Probability			
		0	1E-06	1E-05	1E-04
Fault Coverage	0.3	6.064E-06	6.164E-06	7.061E-06	1.603E-05
	0.4	4.829E-06	4.884E-06	5.378E-06	1.032E-05
	0.6	3.651E-06	3.664E-06	3.774E-06	4.878E-06
	0.7	3.444E-06	3.449E-06	3.491E-06	3.919E-06
	1.0	3.313E-06	3.313E-06	3.313E-06	3.313E-06



<그림 4> 단일종류의 디지털 출력과 단일종류의 아날로그 입력 모듈을 사용한 설계의 경우 감시타이머의 오류 검출률과 소프트웨어 고장률에 따른 계통 불가용도

(2) 단일종류의 디지털 출력과 2종류의 아날로그 입력 모듈을 사용한 설계

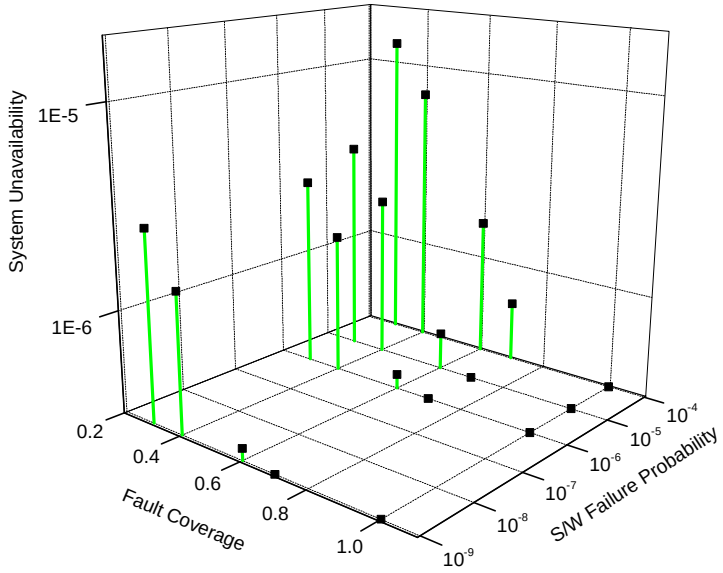
시스템 불가용도		SW Failure Probability			
		0	1E-06	1E-05	1E-04
Fault Coverage	0.3	3.106E-06	3.206E-06	4.103E-06	1.308E-05
	0.4	1.871E-06	1.926E-06	2.420E-06	7.365E-06
	0.6	6.929E-07	7.052E-07	8.156E-07	1.920E-06
	0.7	4.855E-07	4.902E-07	5.330E-07	9.607E-07
	1.0	3.543E-07	3.543E-07	3.543E-07	3.543E-07



<그림 5> 단일종류의 디지털 출력과 2종류의 아날로그 입력 모듈을 사용한 설계의 경우 감시타이머의 오류 검출률과 소프트웨어 고장률에 따른 계통 불가용도

(3) 2종류의 디지털 출력과 2종류의 아날로그 입력 모듈을 사용한 설계

시스템 불가용도		SW Failure Probability			
		0	1E-06	1E-05	1E-04
Fault Coverage	0.3	2.757E-06	2.856E-06	3.754E-06	1.273E-05
	0.4	1.521E-06	1.576E-06	2.071E-06	7.016E-06
	0.6	3.435E-07	3.557E-07	4.662E-07	1.571E-06
	0.7	1.360E-07	1.407E-07	1.835E-07	6.113E-07
	1.0	4.796E-09	4.80E-09	4.801E-09	4.846E-09



<그림 6> 2종류의 디지털 출력과 2종류의 아날로그 입력 모듈을 사용한 설계의 경우 감시타이머의 오류 검출률과 소프트웨어 고장률에 따른 계통 불가용도

4. 결론

본 논문에서는 정량적 안전분석의 결과에 큰 영향을 미치는 인자들을 정리하고 그 인자들의 변화에 따른 전체 계통의 안전성 변화를 분석하였다. 소프트웨어의 오류 가능성, 오류 검출 기법의 검출범위, 공통원인 고장의 적용 등이 정량적 안전성 분석 결과에 중요한 영향을 미치는 인자로 추출되어 분석의 대상이 되었다.

정량 분석의 결과, 추출된 세가지 인자의 변화는 디지털 시스템의 안전성에 수배에서 수십배까지의 영향을 미치는 것으로 나타났다. 감시 타이머의 오류 검출률이나 소프트웨어의 오류 범위가 분석에서 고려한 수치범위 밖에 있을 경우까지 고려하면, 수백배의 안전성 차이가 있을 것으로 판단된다. 그리고 입출력 모듈의 기종을 다양화하여 공통원인 고장을 회피할 수 있다면 시스템의 안전성이 한층 높아지는 것으로 나타났다. 따라서 계통 설계자의 입장에서는 이들 주요 인자를 고려하여 설계를 수행하면 보다 효과적으로 계통의 안전성을 높일 수 있을 것으로 판단된다.

5. 감사의 글

이 논문은 대한민국 과학기술부에서 시행하는 원자력연구개발 중장기사업의 지원으로 수행되었습니다.

참고 문헌

[1] U.S. NRC, Options For Risk-Informed Revisions to 10 CFR Part 50 - "Domestic Licensing of Production And Utilization Facilities" SECY-98-300, 1998.

[2] 이창주, 안전규제에서의 위험도 정보 활용 원칙, KINS/AR-306, Vol 5. Part I, 원자력안전기술 정보회의, 1999.

[3] 성태용 외, 확률론적 안전성 평가기법을 이용한 보조급수계통의 설계 최적화 연구, 한국원자력학회 춘계학술발표회, 1992.

[4] 강현국 외, 확률론적 안전성 평가에서의 디지털 계측제어 계통 고유현안 분석, KAERI/AR-560/2000, 2000.

[5] Taeyong Sung and Hyun Gook Kang, "Intermediate Probabilistic Safety Assessment Approach for Safety Critical Digital Systems," Proceeding of ICONE9, Nice, France, 2001.

[6] 박진균 외, 소프트웨어 신뢰도의 정량적 평가 기법에 대한 고유현안 분석, KAERI/AR-565/2000, 2000.

[7] National Research Council, Digital Instrumentation and Control Systems in Nuclear Power Plant: Safety and Reliability Issues, Chapter 6. Safety and Reliability Assessment Methods, National Academy Press, 1997.

[8] 김인석 외, "디지털 발전소보호계통과 공학적안전설비 작동계통에 대한 고장유형/영향분석 및 신뢰도 분석 적합성 검토," KINS/HR-327, 2000.