KAERI/TR-2908/2005

한국형표준원전 디지털 보호계통 공통원인고장 모델링에 관한 연구

The Common Cause Failure Probability Analysis on the Hardware of the Digital Protection System in Korean Standard Nuclear Power Plant

2005. 2

한 국 원 자 력 연 구 소

제 출 문

한국원자력연구소장 귀하

본 보고서를 2004년도 “정지/저출력 및 디지털 계통의 위험도 평가기술 개발” 과제의 기술보고서로 제출합니다.

2005. 2.

주 저 자 : 강현국 (종합안전평가부)

공 저 자 : 엄흥섭 (종합안전평가부)

장승철 (종합안전평가부)

하재주 (종합안전평가부)

요 약 문

디지털 계통 중 안전기능을 수행하는 계통은 그 기능수행을 보장하기 위하여 다중의 기기를 설치하는 것이 일반적이다. 펌프나 밸브류는 4중 정도의 다중성에 그치는데 비해 현재 한국형표준원전(KSNPP)에 설치된 안전계통에서는 4중 채널이 그 내부에서 다시 4중화되어 총 16중의 설비를 갖추는 등 매우 높은 수준의 다중성을 가지도록 설계되어 있다. 이렇게 높은 수준의 다중성 설계를 채택함으로 인하여 개별 기기의 고장으로 인한 기능상실 확률은 아주 저하되는데 비해 공통원인고장(CCF)에 대한 분석의 중요성은 매우 증대된다.

CCF 분석에서 중요한 요인은 확률모수의 추정과 추정된 확률모수를 이용한 모델링의 두가지 이다. 본 보고서는 후자인 확률모수를 이용한 모델링에 초점을 맞추었다. 즉, 기존의 확률론적안전성평가(PSA) 방법에서 이용하던 CCF 분석방법론을 활용하여 고장수목을 작성하기 위하여 각 계통에 대한 기능 요구사항 및 물리적 배치 등을 체계적으로 분석하고 이를 이용하여 현실적으로 구현가능한 모델을 개발하는 것이다.

높은 수준의 다중성을 갖춘 기기일수록 CCF를 분석하여 모델을 구축하기가 어려워진다. 기존의 방법으로 모든 CCF를 기본사건화하여 모델을 구축할 경우 비현실적으로 거대한 모델을 만들어야 하기 때문이다. 그러므로 최대한 이론적인 값에 가까운 결과를 얻으면서도 현실적으로 모델링이 가능하도록 단순화 알파펙터 방법을 도입하였다. 이런 단순화 방법을 이용함으로써 예를 들어 16중 다중화 트레인의 CCF를 65519개의 기본사건으로 모델하는 대신 1개의 축약된 사건으로 표현할 수 있다.

디지털 계통의 특성상 기존 아날로그 회로를 이용하는 계통에 비교할 때 매우 복잡한 논리 흐름을 가지며, 다중의 변수를 동일한 기기가 처리하도록 되어 있어 CCF의 분석에 신중한 접근이 필요하다. 디지털 기기의 멀티태스킹 기능으로 인해, 어떤 경우에는 동일 기기가 다른 기능을 수행하거나 기능 수행에 참여하지 않다가 다른 경우에는 동일 기능을 수행하게 되어 CCF분석의 대상이 되기도 한다. 본 보고서에서는 한국형표준원전 보호계통의 복잡한 기능을 분석하여 단순화 알파펙터 모델에 적용할 수 있도록 하였다.

또한 기존의 아날로그 회로와는 달리 디지털 기기의 경우 안전기능 수행에 필수적인 부품은 기기내에서도 한정되어 있음을 고려하여, 이러한 부품의 용도에 맞는 고장율을 계산하여 CCF확률 산정에 이용할 수 있도록 방법론을 제시하였다. 즉, 소프트웨어 중의 안전기능 부분이 정상적으로 작동하는 상태에서 호출하는 부품만이 안전기능 수행에 필수적인 부품이므로 이러한 분석을 바탕으로 보다 현실적인 위험도를 계산할 수 있도록 하였다.

또한 이기종의 기기를 이용하여 동일 기능을 수행하도록 설계할 수도 있다. 동일 기능을 수행한다는 것은 동일한 소프트웨어 로직을 공유한다는 뜻이므로 만일 공통으로 부품을 사용한 부분이 있다면 이를 고려하여 CCF 모델을 수행하여야 한다. 본 보고서에서는 이러한 상황에 맞도록 방법론을 제시하였다.

본 보고서의 연구는 KSNPP의 디지털 보호계통 안전성분석에서 CCF의 중요성이 부각됨에따라 수행된 것이다. 디지털계통 특유의 복잡한 논리를 분석하고 안전기능에 필수적인 부품의 고장율만을 고려하여 보다 실제 값에 근접하면서도 보다 현실적인 CCF모델링이 가능한 방법을 제시하였다.

Summary

Safety-critical systems adopt the multiple-redundancy design in order to reduce the risk from the single component failure. The digitalized safety-signal generation system is also designed based on the multiple-redundancy strategy which consists of more redundant components when we compare their number with those of conventional mechanical components. This higher redundancy would clearly reduce the risk from the single failure of components, but raise the importance of the common cause failure (CCF) analysis.

This research aims to develop the practical and realistic method for modeling the CCF in digital safety-critical systems. Higher level of redundancy causes the difficulty of CCF analysis because the fault tree model with conventional CCF modeling methods will be impractically large. We apply the simplified alpha-factor method to the digital system CCF analysis. For example, in the case of 16-redundant-train system, this method could reduce the number of CCF basic events from 65519 to 1.

The digital system is usually operated based on more complex logics when we compare it with the analog system because multiple functions could be performed in single processor. Therefore the CCF probability calculation of the digital system should be carefully treated. This report presents the case study of the application of simplified alpha-factor method to the digital protection system of the Korean Standard Nuclear Power Plant (KSNPP).

The number of components in a digital module for performing the safety functions is smaller than the total number of components in a module. In consideration of safety function actuation, we must consider the safety-critical components only. In order to consider this situation in a more realistic manner, we have to analyze the module design and hardware-software interactions.

The different modules from different vendors could be used to perform the same safety function in order to reduce the CCF probability. The digital components, however, could be produced by the same vendor or the same process. This report also presents the method to cope with this situation.

목　　차

표 목 차

그 림 목 차

제 1 장　서 론

제 1 절　연구 배경

안전계통이 아닌 경우에는 기존의 국내 원자력 발전소에도 이미 많은 디지털 기기들이 도입되어 활용되고 있다. 비안전 계통의 디지털화의 경우 원자력 발전소 전체의 안전성에 미치는 영향이 미미할 것으로 추측되어서 그 동안 안전성 평가의 대상으로 거론되지 않았었다. 그러나 최근 한국형 표준 원전(Korean standard nuclear power plant; KSNPP)의 안전계통에도 디지털 기기가 적극 도입됨으로써 원자력 발전소 전체의 안전성에 최근 도입된 디지털 기기가 미치는 영향에 대한 평가의 중요성이 증대되고 있다.

전세계적으로 연구·설계중인 차세대 원자력 발전소의 중요한 특징 중의 하나는 디지털 계측제어계통의 전면 채택이라고 할 수 있다. 디지털 계통 설계의 채택이 단순화와 표준화를 용이하게 하며 드리프트(drift)나 이력(hysteresis) 문제가 제거되는 등 운전중 유지보수 측면에서도 많은 장점을 지닌 것으로 판단되기 때문이다. 또한 최근에는 기존 아날로그 보호계통 기기들의 성능저하, 노후화, 부품 품귀 등의 이유로 인해 더 이상 아날로그 계통을 유지보수하기가 어려워졌으므로, 극히 보수적으로 취급되어 온 안전관련 계통에서도 디지털 기기의 도입이 시도되고 있다. 국내의 경우, 중수로인 월성 원전에서는 안전정지 계통에 이미 디지털 기기들을 도입하여 활용하고 있으며, 경수로에서도 영광 3,4 호기에 마이크로프로세서를 활용한 interposing logic system (ILS)을 도입함으로써 안전 관련 계통에의 디지털 기기의 적용이 시작되었다.

우리나라의 표준 원전인 울진 5,6 호기에서도 이러한 추세와 같이 디지털기기를 적극 활용하고 있고, 안전계통인 원자로 정지계통과 공학적 안전설비 작동계통에도 디지털 기기를 적용하고 있으며 가동중인 원전에 대해서도 노후 기기에 대한 디지털 기기로의 대체가 추진되고 있다. 또한 차세대 원전의 설계는 네트워크 기능까지 활용하는 본격적인 디지털 계측제어로의 전환을 기본 개념으로 하고 있다.

디지털 설계는 다중의 기능을 하나의 하드웨어내에 소프트웨어로 구현하며 복잡한 내부 설계로 인해 고장 기전이 잘 알려져 있지 않아 기존의 아날로그 설계에 비해 분석의 불명확성이 높다. 이러한 불명확성을 극복하고 원자력발전소의 안전관련 분야에 적용하기 위해서는, 확률론적 안전성평가(Probabilistic Safety Assessment; PSA)와 같은 정량평가 방법의 적극적인 활용이 중요한 역할을 할 것으로 판단된다. 원전의 안전성을 종합적이며 정량적으로 평가하기 위한 중요한 안전성평가 수단으로 PSA가 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 파악할 수 있으며, 각 계통의 주어진 기능을 수행실패에 대해서도 원인과 각 확률 값을 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 규제의 수단으로 사용하고 있으며, 국내에서도 이의 채택이 적극적으로 추진되고 있다 [1], [2]. 또한 PSA는 초기 설계 단계에 적용되어 설계 검증에 이용되며 설계 개선에도 활용[3]될 수 있다.

국내뿐만 아니라 전 세계의 원자력 산업계는 안전성과 경제성을 동시에 추구하기 위한 방법으로 위험도 정보 이용 규제 및 활용(risk-informed regulation and application; RIR&A)분야에 많은 노력을 기울이고 있는 실정으로, 이는 PSA 활용의 확장을 의미한다. RIR&A를 위한 공통의 접근 방법은 실제의 현장 경험자료를 바탕으로 수행된 PSA로부터 얻게 되는 위험도 추정치들의 비교 분석을 통하여 발전소 위험도 측면에서 중요한 계통/부품들의 신뢰도는 지속적인 감시 대상이 되는 반면 중요하지 않은 계통/부품에 대해서는 규제요건의 완화로부터 경제적 이득을 추구하는 것이다. 이를 위하여 일차적으로 위험도에 중요한 계통들이 PSA 경험에 비추어 적절히 선정되어야 하며, 선정된 계통에 대한 PSA는 일정 수준 이상의 품질과 발전소의 안전성에 대한 예측 가능성을 보장할 수 있는 범위에서 수행되어야 한다.

한편, 디지털 계통 중 안전기능을 수행하는 계통에서는 그 기능 수행을 보장하기 위하여 다중의 기기를 설치하는 것이 일반적이다. 일반적으로 펌프나 밸브류는 4중 정도의 다중성에 그치는데 비해 현재 한국형표준원전에 설치된 안전

계통에서는 4중 채널이 그 내부에서 다시 4중화되어 총 16중의 설비를 갖추는 등 매우 높은 수준의 다중성을 가지도록 설계되어 있다.

이렇게 높은 수준의 다중성 설계를 채택할 경우 다수의 기기가 동시에 고장을 일으키지 않는 한은 주어진 기능을 수행하여 안전하게 원자로를 정지시키거나 공학적안전설비(engineered safety feature; ESF)를 기동시킬 수 있다. 따라서 이런 경우에는 개별 기기의 고장으로 인한 기능상실 확률은 아주 저하되고 공통원인고장(common cause failure; CCF)으로 인한 복수의 기기가 고장상태가 되어 기능을 상실할 가능성에 대한 분석이 매우 중요해 진다.

디지털 기기 자체의 안전성 평가에 대해서는 모델링 방법에 대해서 보고서[4][5]를 발간한 바 있고, 디지털 기기가 원전 플랜트 전체에 미치는 영향에 대해서도 분석 보고서[6]를 발간하였다. 그러나 이러한 분석 과정에서 디지털 기기 하드웨어의 공통원인 고장은 개략적으로만 다루어졌으며, 상세한 분석지침의 결여와 복잡한 기능/배열로 인해 정확한 CCF 분석이 수행되지 못하였다. 본 보고서는 보다 정확하고도 현실성있는 디지털기기 공통원인 고장 분석 방법을 제시하고 한국형표준원전의 디지털 안전계통에 시범적용하는 것을 목적으로 한다.

제 2 절 디지털 기기의 공통원인고장 분석

디지털 계통으로의 대체 필요성이 강하게 제기되고 있고, 실제로 그 대체가 진행 중인데 비해, 디지털 계통에 대한 정량적인 신뢰도 평가 방법이 확보되어 있지 않아 그 안전성 확보에 어려움을 겪고 있다. 그 대표적인 사례중의 하나가 디지털 기기의 CCF 분석 방법의 미비이다. 디지털 기기의 경우 범용 하드웨어 시스템에 소프트웨어를 통해 기능을 부여하는 방식부터 아날로그 시스템과는 크게 다르다. 이러한 적용의 유연성(flexibility)은 하나의 디지털 기기에서 두개 이상의 기능을 수행하도록 하는 것이 가능하도록 한다. 또한 공통의 범용 하드웨어를 사용하고 환경에 민감한 기기의 특성상 CCF에 대한 우려가 높아지고 있는데, 이러한 고장의 파급은 원자력 발전소의 안전을 위해 필수적인 다중성을 상실시킬 가능성을 높이므로 주의해서 다루어야 한다.

CCF이란 어떤 공통된 원인에 의해 하나 이상의 기기가 동시 또는 비슷한

시기에 고장나는 사건을 의미한다. 원자력발전소 안전성 확보를 위한 기본 설계 원칙은 다중성(Redundancy)과 다양성(Diversity)이다. 기존 연구에서, PSA 결과에 의하면 일반적으로 CCF는 원전의 다중성에 손상을 주어 원전의 안전성을 저해시키는 것으로 나타난다. 그러므로 CCF 분석의 결과는 PSA 결과 분석에 매우 중요한 인자이다.

CCF 분석에서 중요한 요인은 확률모수의 추정과 추정된 확률모수를 이용한 모델링의 두가지 이다. 본 보고서는 후자인 확률모수를 이용한 모델링에 초점을 맞추었다. 즉, 기존의 확률론적안전성평가(PSA) 방법에서 이용하던 CCF 분석방법론을 활용하여 고장수목을 작성하기 위하여 각 계통에 대한 기능 요구사항 및 물리적 배치 등을 체계적으로 분석하고 이를 이용하여 현실적으로 구현가능한 모델을 개발하는 것이다.

높은 수준의 다중성을 갖춘 기기일수록 CCF를 분석하여 모델을 구축하기가 어려워진다. 고전적인 방법으로 모든 CCF를 기본사건화하여 모델을 구축할 경우 비현실적으로 거대한 모델을 만들어야 하기 때문이다. 예를 들어 16중의 다중성을 가진 계통의 경우 CCF를 정확히 모델링하기 위해서는 65519개의 CCF기본사건을 모델링하여야 한다. 그러므로 최대한 이론적인 값에 가까운 결과를 얻으면서도 현실적으로 모델링이 가능하도록 단순화 알파펙터 방법을 도입하였다. 이런 단순화 방법을 이용함으로써 예를 들어 16중 계통의 경우 CCF를 65519개의 기본사건으로 모델하는 대신 1개의 축약된 사건으로 표현할 수 있다.

디지털 계통의 특성상 기존 아날로그 회로를 이용하는 계통에 비교할 때 매우 복잡한 논리 흐름을 가지며, 다중의 변수를 동일한 기기가 처리하도록 되어 있어 CCF의 분석에 신중한 접근이 필요하다. 디지털 기기의 멀티태스킹 기능으로 인해, 어떤 경우에는 동일 기기가 다른 기능을 수행하거나 기능 수행에 참여하지 않다가 다른 경우에는 동일 기능을 수행하게 되어 CCF분석의 대상이 되기도 한다. 본 보고서에서는 한국형표준원전 보호계통의 복잡한 기능을 분석하여 단순화 알파펙터 모델에 적용할 수 있도록 하는 것을 목적으로 한다.

또한 기존의 아날로그 회로와는 달리 디지털 기기의 경우 안전기능 수행에 필수적인 부품은 기기내에서도 한정되어 있음을 고려하여, 이러한 부품의 용도에 맞는 고장율을 계산하여 CCF확률 산정에 이용할 수 있도록 방법론을 제시하였다. 즉, 소프트웨어 중의 안전기능 부분이 정상적으로 작동하는 상태에서 호출하

는 부품만이 안전기능 수행에 필수적인 부품이므로 이러한 분석을 바탕으로 보다 현실적인 위험도를 계산할 수 있도록 하였다.

제 3 절 연구 개요

본 보고서의 연구는 KSNPP의 디지털 보호계통 안전성분석에서 CCF의 중요성이 부각됨에따라 수행된 것이다. 기존에 원전의 안전성 평가에 많이 적용되어온 고장수목(fault tree; FT) 방법을 이용하여 디지털화된 한국형 표준원전의 위험도를 평가하기 위해서는 이에 맞는 CCF 모델링 방법을 개발하여야 한다. 디지털계통 특유의 복잡한 논리를 분석하고 안전기능에 필수적인 부품의 고장율만을 고려하여 보다 실제 값에 근접하면서도 보다 현실적인 CCF모델링이 가능한 방법을 제시하였다.

제 4 절 보고서의 구성

본 보고서는 5개의 장으로 구성되어 있다. 제1장에서는 연구의 배경과 개요를 다루었으며, 제2장에서는 PRIME(한국형 표준 PSA 모델)에서 사용되는 알파펙터에 의한 CCF분석 방법을 설명하고, 단순화 알파펙터 방법의 개요와 장단점을 기술하였다. 제3장에서는 한국형표준원전의 디지털안전계통 CCF 분석을 위한 기능 분석과 단순화 알파펙터 방법을 이용한 CCF모델링을 설명하였다. 제4장에서 기능 수행을 고려한 고장율 및 CCF 확율 산정 방법을 다루었다. 요약 및 결론은 제5장에 기술한다.

제 2 장 알파펙터 모델과 단순화 알파펙터 모델

제 1 절 공통원인 고장

CCF이란 어떤 공통된 원인에 의해 다중 계통에서 하나 이상의 기기가 동시 또는 비슷한 시기에 고장나는 사건을 말한다. 이러한 CCF는 다중 계통에 설치된 기기들의 고장을 동시에 일으키므로 계통의 신뢰도에 큰 영향을 미친다. 원전 안전성의 확보를 위한 기본 설계 원칙은 다중성(redundancy)과 다양성(diversity)이라 할 수 있는데, 국·내외 확률론적 안전성 평가 결과에 의하면 CCF는 원전의 다중성에 치명적인 손상을 주어 계통 이용불능도와 노심손상빈도에 큰 영향을 주는 것으로 밝혀졌다. 따라서, 주요 계열(train) 별로 CCF의 잠재성 및 그 확률을 정확히 평가하여 계통의 취약성 및 개선방안을 마련하는 일은 매우 중요하다. 즉, CCF이 위험도에 미치는 영향을 파악하는 것은 위험도 관리 측면에서 중요하다는 것을 의미한다. 이에 따라, 국/내외적으로 CCF 분석 기법에 대한 연구는 항상 관심의 대상이 되어 오고 있다. 특히, 근래 들어 위험도 정보를 활용한 기법들이 발전소 운영에 도입됨에 따라 CCF의 불확실성에 대한 문제가 대두되어 이를 해결하고자 하는 연구가 활발하다.

CCF를 분석하는 방법은 여러 가지가 있는데, 일관성이 없이 분석을 수행하면 결과에 차이가 있어 위험도 관리 측면에서 올바른 결정을 내릴 수가 없다. 그러므로 PSA수행을 위해서는 CCF를 분석할 수 있는 일관적인 수행 지침의 개발이 필요하다. 뿐만 아니라, 사고경위를 분석하는 사건수목에서 동일계통이 여러 곳에 나타나는 경우가 많은데, 각각의 상황에서 계통의 가용 계열 수와 성공기준 등은 달라질 수 있다. 계통의 정비로 인한 상태 변화, 또는 동일 계통이 사고의 방지를 위한 여러 가지의 역할을 담당할 경우 성공기준의 변화에 따라 CCF 기본사건이 자주 바뀌게 된다. 이러한 변화에 따라 매번 이를 다시 모형화 하는 일은 상당한 노력을 필요로 할 뿐 아니라, CDF의 계산에 있어서 심각한 비효율성을 초래한다. 따라서, 계통의 가용 계열 수, 성공기준 등의 변화에 따른 CCF 사건 발생확률을 효율적으로 모형화하고 계산을 수행할 수 있는 방법의 개발이 필요하다.

확률 이론에 의하면, 기본사건 사이의 잠재적 종속성을 고려하지 않으면, 한 사건의 확률을 더 기초적인 사건으로 분류하여 평가하는 방법으로 의미있는 결과를 생성하지 못한다. 계통신뢰도 분석에 있어서 어떤 종속성은 직접적이고 외형적으로 설명할 수 있는데, 이런 종속성은 기기나 하부 계통 간의 기능적 혹은 물리적 상호관계로부터 발생하는 것으로서 계통 기본 설계의 내재적 속성이다. 고장수목이나 신뢰도 블럭도면 같은 논리적 모형 기법들은 이러한 종속성을 외형적으로 나타낼 수 있는 방법을 제공한다. 한 기기의 고장에 기인한 다른 기기의 고장 같은 연쇄적 혹은 확산적 종속성은 계통의 논리모형 내에 외형적으로 반영하여 설명할 수 있다.

과거의 신뢰도 분석은 많은 경우 기능적, 논리적 종속성을 고려한 반면, 계통 논리모형 내의 기본사건들이 독립적이라는 가정 하에 수행되었다. 예를 들면, 계통신뢰도 분석에 사용되는 거의 모든 컴퓨터 코드들이 정량화과정에서 모델내의 기본 사건들이 확률적으로 독립이라는 가정을 사용하고 있다. 그러나 고도의 신뢰도를 갖는 원전 계통의 운전이력을 살펴보면, 기능적, 논리적 종속성 이외에도 외형적으로 잘 설명되어지지 않는 여러 종속성의 원인들이 존재함을 알 수 있다. 실제적으로 관심의 대상이 되는 것은 CCF인데, 이는 계통신뢰도를 향상시키기 위해 도입된 중복성이나 다양성을 무력화시키는 종속적 고장을 말한다. 즉, 종속고장이 노심손상에 기여하는 비율이 지배적으로 나타난다. 이러한 결과는 주요 기기나 계통의 독립적 고장들이 동시에 발생하여 사고를 발생시키는 경우를 방지하기 위하여 높은 신뢰도의 기기를 사용한데 기인한다고 볼 수 있다.

논리모델에서 외형적으로 설명되지 않는 종속성을 다루는데 사용된 방법은 주로 모수적 방법으로서, 이러한 다중고장의 발생빈도를 매개확률모수를 통하여 나타내는 것이다.

CCF 분석을 위해서는, 첫째, 계통 논리모델 개발을 위한 준비를 해야 한다. 둘째, CCF의 가능성이 있는 기기군(component group)을 선별한다. 그리고 세째, 고장수목에 모델할 공통원인 기본사건에 대한 정의를 하고 확률모델을 선택한 후, 이들 기기에 대한 대상 발전소의 CCF 자료를 수집한다.

다시 말하자면, CCF를 포함하는 계통 논리모델 개발을 위해, 계통을 숙지하고 문제점을 파악하여 계통 논리모델을 개발한다. 이후, 정성적 및 정량적 선별

과정을 거쳐 CCF으로 고려할 공통원인 기기그룹을 선별한다. CCF 사건 선별 과정은 기기에 대한 특정 그룹을 확인하여 잠재적 CCF 그룹을 만드는 것이다. 즉, CCF를 일으킬 것으로 인지되는 모든 중요 기기 그룹을 보수적인 방법으로 간단히 확인하여 CCF 취약성 분석을 수행하는 것이다. CCF 사건 선별 결과, CCF를 일으킬 것으로 예상되는 기기 목록을 얻을 수 있다. 이와 같은 선별과정을 통해 수집해야 할 자료의 범위를 줄일 수 있고, 어떤 기기들 사이에 CCF이 발생하는지를 판단할 수 있다. 일반적인 CCF 그룹 선별절차와 확인절차는 그림 1과 2에 도시하였다. 표 1에 공통원인고장 분석을 위한 자료원을 기술하였다. 기능 분석에 의한 KSNPP(울진5,6호기)의 디지털 보호계통에 대한 CCF 모델 개발은 제3장에서 상세히 설명한다.

그리고 CCF를 고장수목에 모델하기 위해, CCF 기본사건을 정의하고 기본사건에 대한 확률모델을 선택하여 정해진 CCF 방법 및 절차에 따라 CCF 사건을 모델한다. CCF 기본사건에 대한 확률값 계산을 위해, 데이터를 분류하고 선별하여 CCF 모수를 도출한다. CCF 사건은 희귀한 사건이므로 대상 발전소 자료만으로 CCF 사건 확률값을 계산하기 어렵다. 그러므로 사용 가능한 모든 발전소로부터 자료를 취합하여 각 자료에 포함된 고장원인 연계인자를 파악하고, 그 고장원인 연계인자가 해당 발전소에서 발생 가능한가 결정한다. 즉, 적용인자를 할당한다. 그리고 가능한 영향을 고장 기기수로서 표현하며, 유사 발전소 고유 데이터베이스를 생성하여 다중도가 N일 경우, 1부터 N 개의 기기가 고장날 사건의 수를 제시한다. 즉, N개의 기기 중 k개의 기기가 고장을 일으킬 모수를 계산한다. 최종적으로 각 CCF 사건에 대해서는 방법론에 따라 CCF 모수를 사용하여 확률값을 계산한다. 그리고 계산된 확률값을 모델된 각 CCF 기본사건에 입력하고 정량화를 수행한 후, 민감도 분석을 수행하면 CCF를 포함한 계통 정량화가 마무리된다[7].

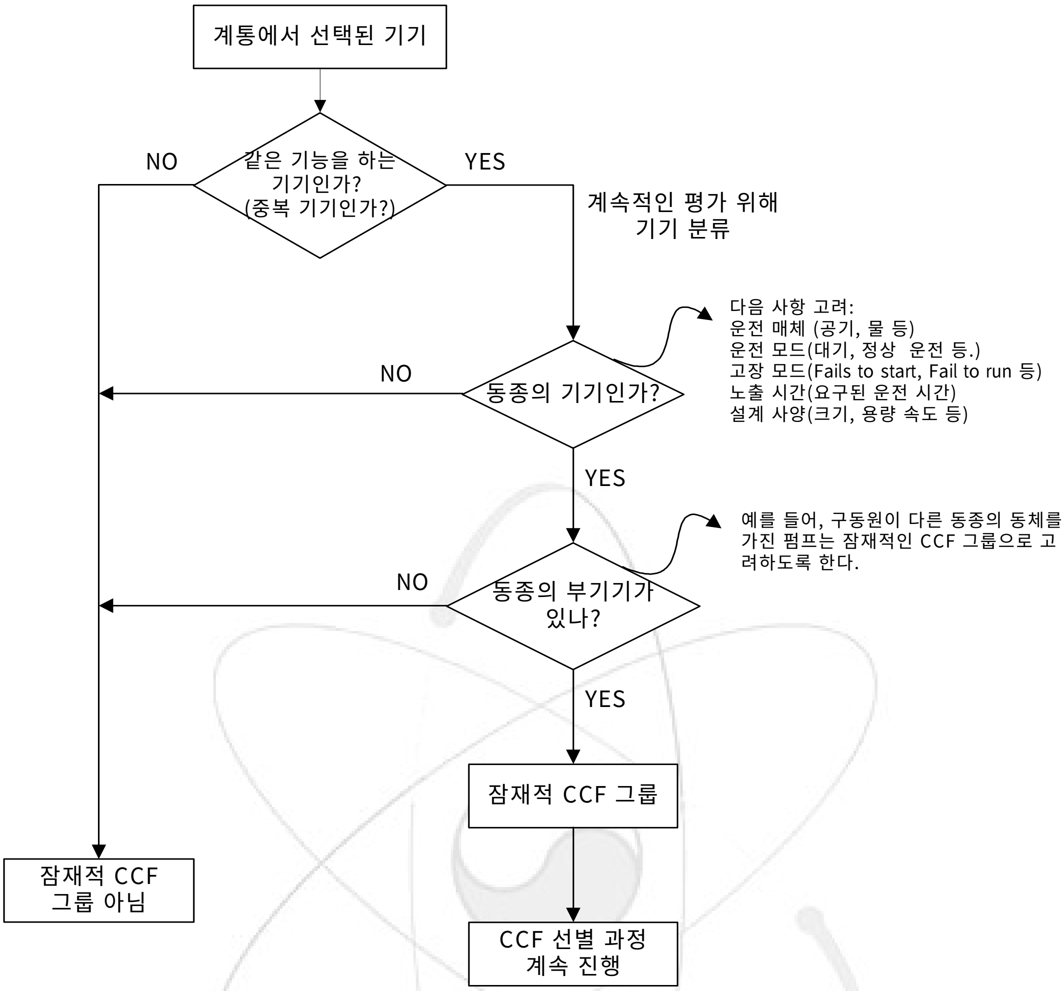

그림 1. 계통내 CCF 그룹 확인 절차[7]

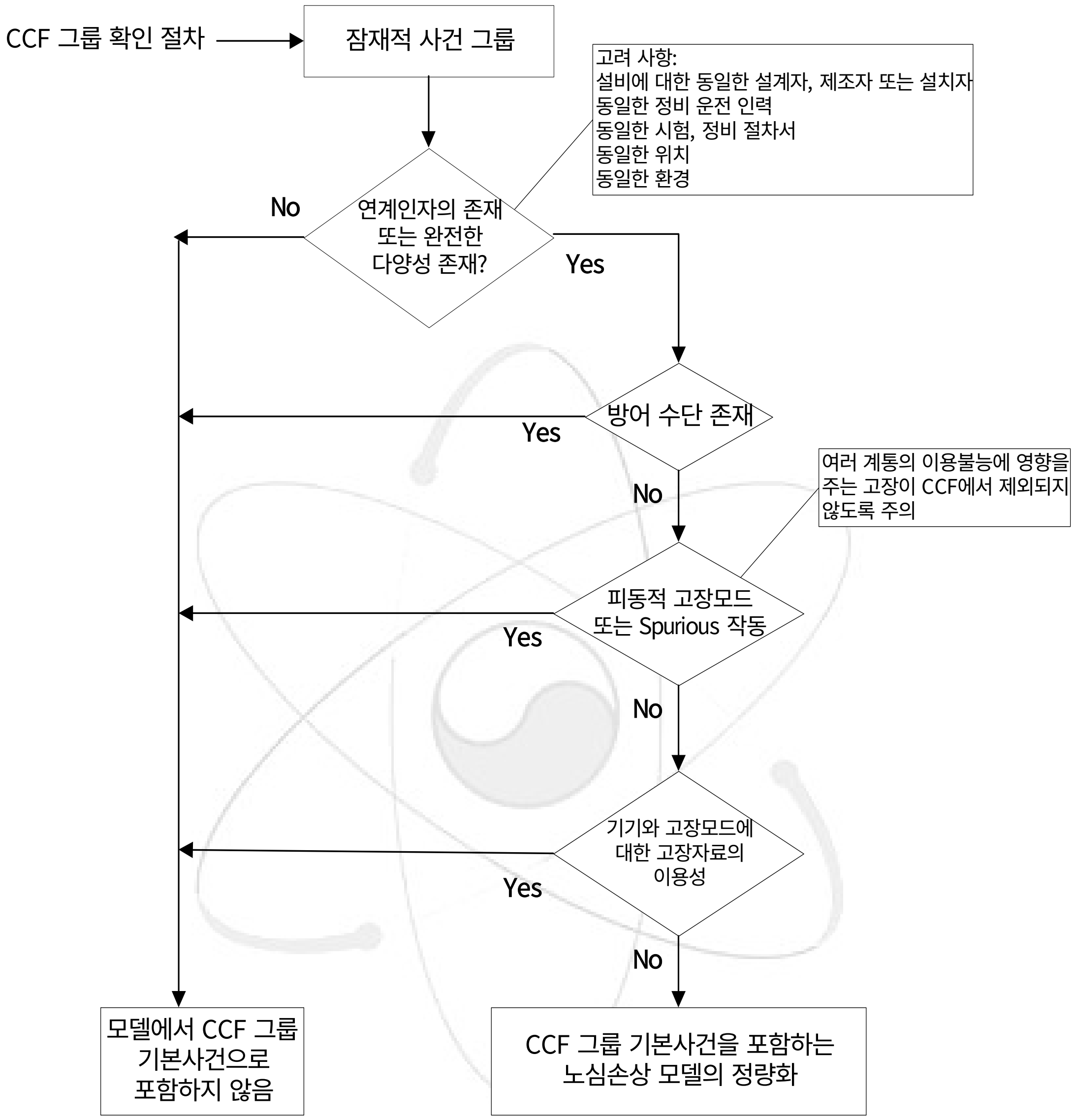

그림 2. CCF 그룹 선별 절차[7]

표 1. 공통원인고장 분석을 위한 자료원 [7]

자료 종류	자료원
일반 이력자료 (raw data) 간행물	License Event Reports Nuclear Plant Reliability Data System
대상 발전소 고유 이력자료	기기 시험 및 보수 기록 작업 지시서 운전 일지 등.
일반적으로 분류된 사건자료 및 모수 추정치	NUREG/CR-2770 NUREG/CR-2098 CCF (Computerized database and data analysis tool)

제 2 절 공통원인고장 모델

CCF를 확률론적안전성 분석에서 모델하기 위한 방법론은 다양한 형태로 개발되어 있다. 각 방법론 별로 적용의 복잡성이나 실제 자료의 반영정도는 상이하나, CCF의 확률을 계산하여 고장수목에 반영하는 것을 목적으로 하는 것은 동일하다. 아래에 각 방법론의 특징을 간단히 요약[7]하고, 표준PSA방법에서 사용하기로 결정된 알파 펙터 모델에 대해 상세히 설명하기로 한다.

Basic parameter 모델은 m개의 CCF 관련 기기 집단에서 특정 k개의 기기가 동시에 고장나는 사건들을 각기 하나의 사건으로 정의한다. 이 모델은 각 CCF 사건에 대한 확률들은 수집한 고장자료로부터 직접 추정하며, 이를 이용하여 계통의 고장 확률을 구하는 방법이다. 이 모델은 기기 수가 늘어남에 따라 필요한 모수의 수도 증가하며, 각 CCF 사건마다 고장난 CCF 수 및 시험 수에 대한 정확한 자료를 요구한다. CCF 사건 확률들의 대칭성을 가정하면, Basic Parameter 모델에서 기본적인 모수는 $Q_k^{(m)}$ 이며, 이는 m개의 공통원인 기기 집단에서 k개의 기기가 동시에 고장 날 사건의 확률로 정의된다.

베타 펙터 모델은 CCF 가 발생하면 계통내의 모든 기기들이 동시에 고장나는 것으로 가정한다. 즉, CCF 충격은 치명적(lethal)이어서 다중도와 관계 없이 전체 계통의 고장을 일으킨다. 또한 한 기기의 총 고장확률 내에서 CCF에 의한 고장확률이 차지하는 비율은 일정하다고 가정한다. 따라서 CCF 모델이 간단하며 CCF 모수의 수도 적어 적용하기가 쉽다. 그러나 중복에 따른 계통의 신뢰도를 적절히 평가할 수 없다는 단점이 있다.

C 펙터 모델은 CCF 데이터베이스에 표본추출 체계가 기록되지 않음으로 인해 발생하는 베타 펙터 모수 추정의 불완전성을 보완하기 위하여 개발되었다. C 펙터 모델은 독립고장 강도에 대한 CCF 강도의 비율로 정의된다.

MGL (Multiple Greek Letter) 모델은 기본적으로 단일 모수 모델인 베터 펙터 모델을 다항 모수 모델로 확장한 것이다. 기기 수가 늘어남에 따라 모수의 수도

많아지므로 모수 추정 및 적용이 복잡해지지만, 그 만큼 현상을 자세히 반영할 수 있다. MGL parameter들은 특정한 k-1개 기기의 고장 하에서 그 고장 원인이 다른 기기와 공유될 조건부 확률로 정의된다.

Binomial Failure Rate (BFR) 모델은 충격이라는 개념을 도입하여 CCF 현상을 모델한다. 고장은 independent failure, non-lethal shock failure, lethal shock failure 의 3 가지로 구분한다. Independent failure는 CCF를 유발하지 않는 사건이며, lethal shock failure는 충격이 왔을 때 모든 기기가 고장나는 사건이다. Non-lethal shock failure는 충격이 왔을 때 일정한 확률로 독립적으로 기기들이 고장나는 사건이다. BFR 모델은 CCF 현상을 간단히 잘 설명하고 있는 모델로서 모수의 수도 적고 계열 수에 영향을 받지 않는 장점이 있다. 단점으로는 충격 발생시 조건부 고장확률이 독립적이라는 가정이 검증된 바가 없다는 것이며 모수 추정이 타 모델이 비해 복잡할 수 있다는 것이다.

알파 펙터 방법은 계통 내에서 발생하는 고장 사건의 수를 기초로 한다. MGL 방법과 마찬가지로 기기 수가 늘어남에 따라 모수의 수도 많아지므로 모수 추정 및 적용이 복잡해지지만, 그 만큼 현상을 자세히 반영할 수 있다. 알파 펙터 방법은 계통 내에서의 CCF 고장 수에 근거하기 때문에 모수 추정에 MGL 방법과는 달리 시험절차의 영향을 받지 않는다. 알파 펙터의 모수는 계통 내에서 발생하는 고장 사건의 총 빈도에 대하여 k중 기기 고장 사건의 비로 정의된다.

이러한 모델들 이외에도 Common Load 모델, Multiple Dependent Failure Fraction (MDFF) 모델, Multiple Failure Rate (MFR) 모델, Random Probability Shock (RPS) 모델, Environmental 모델 등이 개발된 바 있다.

알파 펙터의 모수는 다음 식과 같이 정의될 수 있다:

$$\alpha_k^{(m)} = \frac{n_k}{\sum_{i=1}^{m} n_i} = \frac{{}_mC_k * Q_k}{\sum_{i=1}^{m} ({}_mC_i * Q_i)}$$

즉, 전체 고장 횟수 중에서 특정갯수의 공통원인고장이 발생한 횟수가 모수가 된다. 여기서, ${}_mC_k * Q_k$ 는 m개 기기의 CCF 그룹에서 k개 기기의 고장을 포함

하는 사건의 빈도이다. 그러므로 $\alpha_k^{(m)}$ 는 계통 내에서 발생하는 고장사건의 총 빈도에 대하여 k개의 기기가 고장난 사건이 차지하는 비율이다.

그러므로 예를 들어 3개의 계열을 가진 계통의 경우, α-factor 모수는 다음과 같이 표현할 수 있다 (비순차 시험의 경우).

$\alpha_1 = 3Q_1 / [3Q_1 + 3Q_2 + Q_3]$

$\alpha_2 = 3Q_2 / [3Q_1 + 3Q_2 + Q_3]$

$\alpha_3 = Q_3 / [3Q_1 + 3Q_2 + Q_3]$

그리고 α-factor들의 합은 1이 된다.

$\alpha_1 + \alpha_2 + \alpha_3 = 1$

m개의 기기를 포함하는 CCF그룹에 대해 k개의 기기가 고장나는 CCF 확률값 $Q_k^{(m)}$ 는 다음과 같이 정의될 수 있다.

$$Q_k^{(m)} = \frac{k}{{}_{m-1}C_{k-1}} \cdot \frac{\alpha_k^{(m)}}{\alpha_t} \cdot Q_t \text{, (비순차 시험일 경우)}$$

$$Q_k^{(m)} = \frac{1}{{}_{m-1}C_{k-1}} \cdot \alpha_k^{(m)} \cdot Q_t \text{, (순차 시험일 경우)}$$

여기서,

$$\alpha_t = \sum_{i=1}^{m} i \cdot \alpha_i^{(m)} ,$$

$$Q_t = \sum_{i=1}^{m} ({}_{m-1}C_{i-1} * Q_i) .$$

참고로, 비순차 시험과 순차시험은 한번의 시험을 수행할 때 계통내의 다중기기를 모두 시험하는지 그렇지 않은지로 구분한다. 즉, 한번에 모든 기기를 시험하는 경우를 비순차 시험이라 하고, 시험주기를 기기수로 나누어 기기별로 시험을 수행하는 경우를 순차시험이라 한다. 상세한 내용은 참고문헌[7]의 부록에 기술되어 있다. 일반적으로 순차시험을 수행할 경우 공통원인 고장에 노출될 확률이 낮아진다.

제 3 절 단순화 알파펙터 모델

앞절에서 설명한 바와 같이 알파 펙터 방법은 현상을 자세히 반영할 수 있다는 장점이 있는 반면에 다음의 두가지 단점도 가지게 된다. 첫째는 기기 수가 늘어남에 따라 모수의 수도 많아지므로 모수 추정 및 적용이 복잡해 진다는 것인데, 이것은 본 연구의 범위를 넘어서는 문제이므로 본 보고서에서는 다루지 않는다. 두번째 문제는 이렇게 상세한 모델을 수행할 경우 다중기기 수가 많은 디지털 계통의 경우 너무 많은 CCF 사건을 고장수목에 모델하여야 하는 문제가 발생한다.

예를 들어 16중으로 다중화된 디지털 계통의 경우에는 CCF를 65519개의 기본사건을 고장수목에 일일이 모델하여야 하는 어려운 점이 있다. 이렇게 많은 수의 CCF 사건을 사용하게 되면 고장수목 개발 자체도 어려워지지만, 생성되는 단절집합의 숫자가 너무 많아지므로 정량화 과정에서도 큰 어려움을 겪게 된다. 4개로 이루어진 CCF 그룹 경우는 11개, 8개로 이루어진 경우는 247개의 CCF 사건이 모델되어야 한다. 따라서 현실적으로는 상세 알파펙터 모델을 디지털계통 이용불능도 산출을 위한 고장수목에 포함시키는 것이 어렵다.

한국형표준원전의 디지털 보호 계통은 4개의 채널로 다중화되어 있으며 채널 내부에서도 2중 또는 4중으로 다중화된 기기가 많이 있기 때문에, 계통 전체적으로 대부분의 모듈이 8중 또는 16중의 다중성을 가지게 되므로 이것을 모두 고려하여 상세 고장수목을 작성하는 것은 지나치게 많은 노력을 소모하기 때문이다.

따라서 알파펙터 모델의 장점을 살리면서도 디지털 계통에의 적용성을 높이기 위해 단순화된 알파펙터 모델을 이용하는 방법을 택하였다. 베타펙터 모델의 경우처럼 하나의 사건으로 CCF를 모델하되, 그 CCF 확률값은 알파펙터 방법론에 기반하여 계산하는 방법이다.

단순화하지 않은 알파 펙터 방법과의 비교 설명을 위해 참고문헌[8]의 SMART-P 원전의 PRHRS (Passive Residual Heat Removal System)에 대한 신뢰도 평가 예제를 그대로 옮기면 다음과 같다.

Ms Isolation Electro-Hydro Valves는 4개의 Train으로 구성되며, 각 train에 2개씩이 redundancy로 설치되어 있다. 총 8개가 하나의 CCF 그룹으로 처리된다. 만일 8개가 동시에 고장나는 CCF 하나만을 고려한다면, 각 Train에 대해서는 다음의 그림3과 같은 방식의 fault tree가 구성된다. (B, C, D Train에 대해서도 마찬가지 모양이다.)

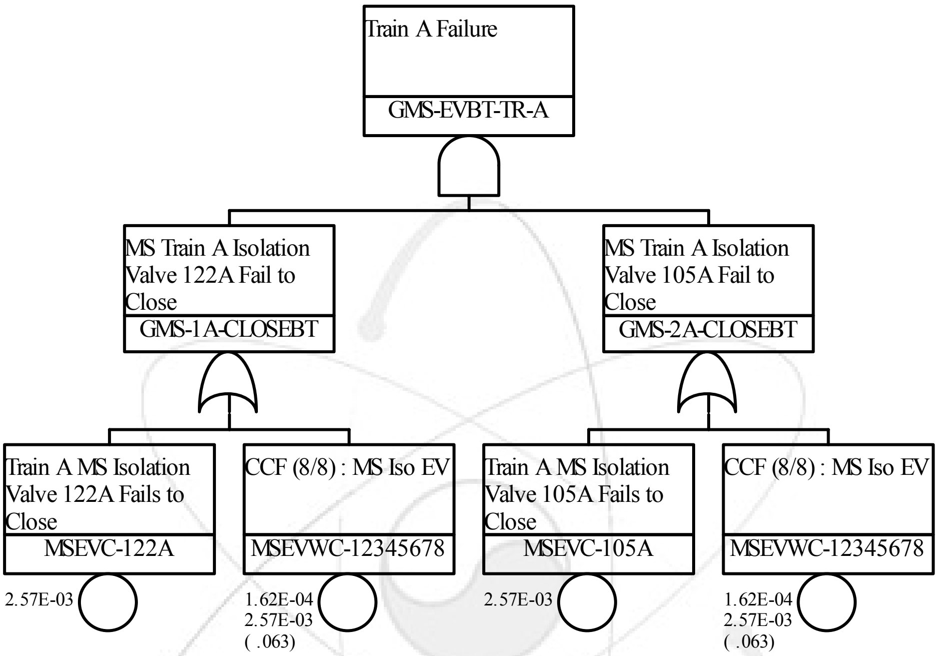

그림 3. 하나의 CCF만을 고려한 경우의 Ms Isolation Electro-Hydro Valves Train A의 고장수목

4 Train 중 2 Train만 성공하면 되는 성공기준을 가지는 경우에는 Top Logic이 다음의 그림 4와 같이 구성된다.

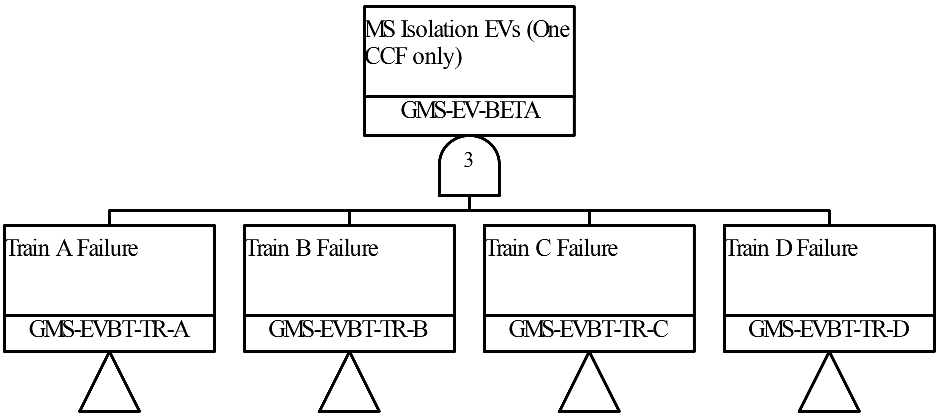

그림 4. 2/4성공기준을 가지는 Ms Isolation Electro-Hydro Valves의 Top Logic

이 경우 정량화하면 Top Logic에 대해서는 CCF하나만이 대부분을 차지한다. 만일 8 train에 대해 Full 알파펙터 모델을 도입한다면, 각 Train 별 고장수목이 그림 5와 같이 변경된다.

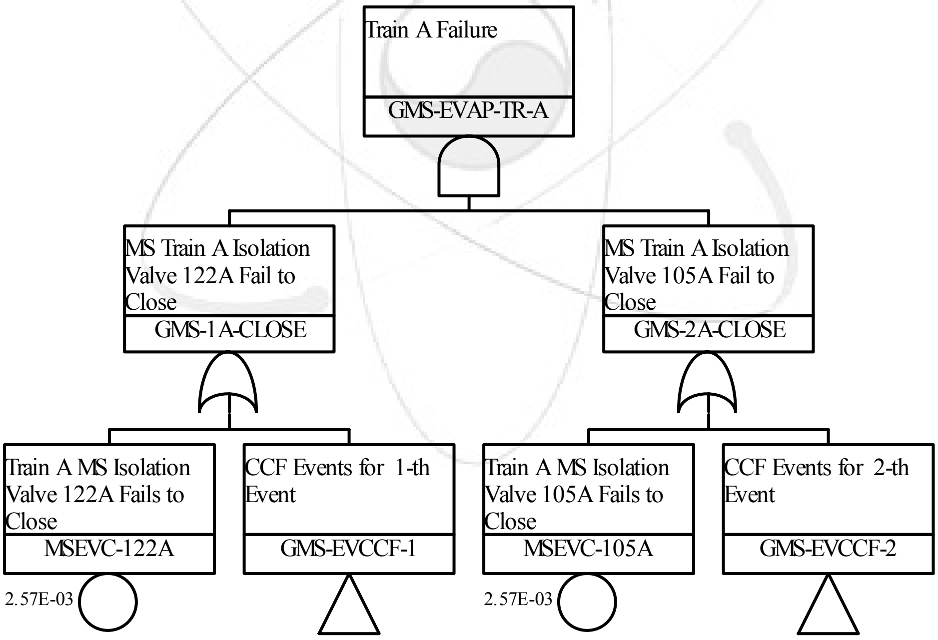

그림 5. 알파 펙터 방법을 이용하여 CCF를 모델한 경우 Ms Isolation Electro-Hydro Valves Train A의 고장수목

각 Train에 있는 기기 별로 CCF가 alpha factor 방법에 따라 모델된다. 따라

서 각 기기마다 2에서 8개의 모든 기기들의 조합에 대한 CCF가 모델된다. 그림6 은 2에서 8개의 조합이 모델된다는 것과, 그리고 2개 조합에 대해 1번 기기를 포함하는 모든 조합의 Event들을 보여준다.

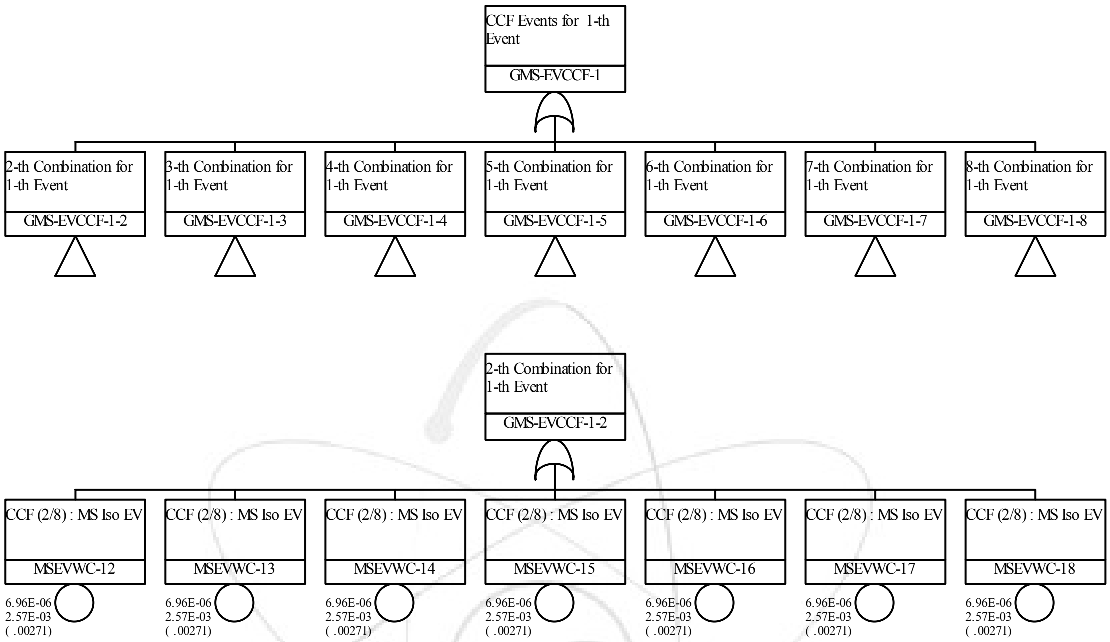

그림 6. 알파 펙터 방법을 이용한 CCF 모델 일부

8개 기기가 하나의 CCF 그룹이므로, 총 247개의 CCF event가 나타난다. 다시 말해 하나의 CCF 그룹을 모델하기 위하여 247개의 Event를 모델하여야 한다. 각 조합 (2개가 고장나는 CCF 사건, 3개가 고장나는 CCF 사건 등을 표현함)에 속하는 CCF 사건 수 및 각 조합에서 특정 기기와 관련된 CCF Event 수는 표 1과 같다. 하나의 특정기기 고장을 모델하기 위해서 127개의 CCF사건을 모델하여야 하는 것이다.

표2. 8개의 다중성을 가지는 경우에 대한 CCF 사건

조합의 수	각 조합에 속한 CCF Event 수	각 조합에서 특정 기기와 관련된 CCF Event 수
2	28	7
3	56	21
4	70	35
5	56	35
6	28	21
7	8	7
8	1	1
계	247	127

이러한 어려움을 해결하기 위해서, 단순화된 알파펙터 방법을 적용하는데, 각 기기종류별로 다양한 성공조건에 대해 CCF 특성을 검토하여 CCF 모델을 단순화시키는 것이다. 선행연구의 결과 단일 CCF event가 cut set으로 나타나는 것만을 고려한다면 정량화 결과에 차이가 없는 것으로 나타나고 있다[8]. 즉, 단순화된 단일CCF사건 모델을 사용하더라도 알파 펙터 모델에서 나타나는 Single CCF cut set의 값을 더하여 사용한다면 모델은 단순하면서 정량화에 거의 오차가 없게 된다.

알파 펙터 모델을 사용한 경우, Top logic에 대한 값은 2.033e-4로 평가되어 전체가 고장나는 것만을 고려한 경우에 비해 25%가 증가한다. 알파 펙터를 이용하여 상세 모델을 했으므로 3 개 train 이상이 고장나는 CCF 사건들이 단일 사건으로 이루어진 cut set으로 나타나게 되어 보다 실제에 가까운 모델이 되었기 때문이다. 그리고 이들 cut set으로 인한 계통 이용불능도가 전체의 대부분(99.9%)을 차지하는 것을 표3에서 확인할 수 있다.

단일 Event가 cut set이 되는 CCF 사건들의 합은 2.03e-4이므로 위에 언급한 계통 이용불능도 2.033e-4와 거의 차이가 없다. 따라서 계통 이용불능도에 직접 큰 영향을 주는 CCF사건들의 확률을 모두 합하여 한 개의 CCF사건으로 모델한다고 해도 전체 모델에서 오차가 거의 없는 것이다. 이것이 단순화 알파펙터 방법이다.

표3. 8개의 다중성을 가지는 경우에 대한 CCF 사건

No	Cut set 값	F-V	누적치	Cut set
1	1.62E-04	0.7967	0.7967	MSEVWC-12345678
2	4.32E-06	0.0212	0.818	MSEVWC-1345678
3	4.32E-06	0.0212	0.8392	MSEVWC-2345678
4	4.32E-06	0.0212	0.8604	MSEVWC-1234568
5	4.32E-06	0.0212	0.8817	MSEVWC-1235678
6	4.32E-06	0.0212	0.9029	MSEVWC-1234567
7	4.32E-06	0.0212	0.9242	MSEVWC-1245678
8	4.32E-06	0.0212	0.9454	MSEVWC-1234678
9	4.32E-06	0.0212	0.9667	MSEVWC-1234578
10	1.62E-06	0.008	0.9746	MSEVWC-345678
11	1.62E-06	0.008	0.9826	MSEVWC-123478
12	1.62E-06	0.008	0.9906	MSEVWC-125678
13	1.62E-06	0.008	0.9985	MSEVWC-123456

다만, 이 방법은 계통의 성공 조건에 따라 크게 차이가 날 수 있으므로 성공조건에 따른 효과 등을 상세히 검토하여 사용하여야만 한다. 계통분석과 성공조건 분석에 따라 단일 사건으로 이루어진 cut set에 해당하는 범위가 달라지기 때문이다.

정리하자면, 단순화 알파펙터 방법을 이용하는 경우의 장점은 전체 플래트 모델이나 상위 계통 모델에서 지나친 복잡성을 피하면서도 상세 모델에 가까운 정량화 결과를 얻을 수 있다는 것이다. 반면에 이 방법의 단점은 상세 계통 분석과 성공조건 분석을 미리 수행하여 단일 사건으로 이루어진 cut set에 해당하는 범위를 미리 산정하여야 한다는 것이다. 한국형 표준원전 디지털 보호계통에 단순화 알파펙터 방법을 적용하기 위한 분석을 다음장에서 다루었다.

제 3 장 한국형표준원전의 디지털안전계통 공통원인고장 분석

제 1 절 울진5,6호기 디지털 원자로보호계통

한국형표준원전인 울진5,6호기의 디지털 원자로 보호계통(Digital Plant Protection System; DPPS)에 대한 설명은 기존의 신뢰도 상세분석 보고서[4]에 기술된 계통설명을 다음에 요약 정리하였다.

DPPS는 발전소가 원자로 정지 조건을 만족하게 되면 신속하고 정확하게 정지신호를 발생시키기 위하여 그림 7의 개념도에서 보는 바와 같이 다수의 다중성을 갖추고 있으며 각 프로세서의 기능은 독립적으로 작동하도록 되어 있다. 그림 7은 아날로그 변수 13개의 경우에 해당하는 것이고, 실제 DPPS는 노심 보호 연산기(core protection calculator; CPC)로부터 입력되는 디지털 변수 2개를 위한 디지털입력 모듈도 추가로 존재한다.

KSNPP의 DPPS는 측정 채널 또는 CPC로부터 발생한 신호에 대하여 입력 모듈을 거쳐 정지논리(Bistable; BS) 프로세서모듈에서 각 정지 변수별로 설정치에 도달하였는지의 비교를 수행한 후, 다중 채널의 비교 결과를 동시논리(Local Coincidence Logic; LCL) 프로세서에서 최종적인 정지 신호를 생성한다. 이 신호가 개시 회로로 전송되어 정지 회로 차단기(trip circuit breaker; TCB) 개방을 통하여 제어봉 구동장치(control element drive mechanism; CEDM)의 코일을 비여자시킴으로써 모든 제어봉들을 노심하부로 떨어지게 하여 원자로 정지 기능을 수행한다.

DPPS는 각각의 정지 변수에 대하여 전기적으로 독립되어 있으면서 물리적으로 격리된 4개의 측정채널이 제공되며, 원자로 정지 신호를 발생하기 위해서는 어떤 한 개의 정지 변수에 대하여 2개 이상의 채널의 계측값이 동시에 설정치에 도달하여야 한다.

원자로의 정지 기능은 운전원의 수동 정지 이외에 0-10V의 전압 신호치를 이용하는 13개의 아날로그 신호와 CPC로부터 제공되는 2개의 디지털 신호(DNBR 및 LPD)로 총 15종의 원자로 정지 신호에 의해 수행된다. 각 정지변수는 증기 발생기 #1과 #2에 중복되는 것을 제외하면 다음과 같이 정리될 수 있다.

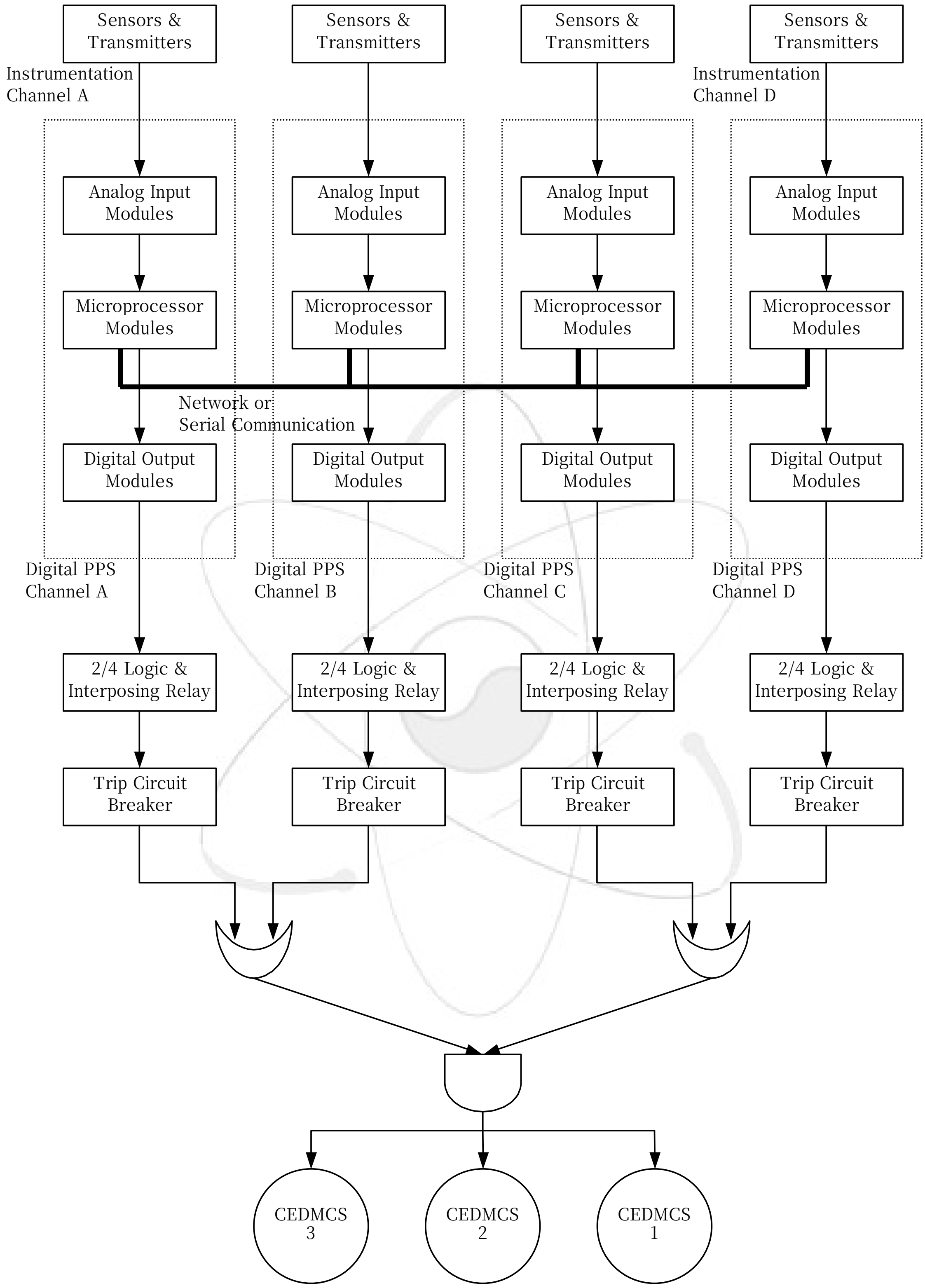

그림 7. DPPS의 구조 개념도

가변 과출력 (variable overpower)

고 대수 출력 (high logarithmic power)

고 국부 출력 밀도 (high local power density)

저 핵비등 이탈율 (low departure from nucleate boiling ratio)

가압기 저 압력 (low pressurizer pressure)

가압기 고 압력 (high pressurizer pressure)

증기 발생기 저 압력 (low steam generator pressure)

증기 발생기 저 수위 (low steam generator level)

증기 발생기 고 수위 (high steam generator level)

격납 건물 고 압력 (high containment pressure)

원자로 냉각재 저 유량 (low reactor coolant flow)

또한, 상기의 자동 정지 신호 이외에 운전원에 의한 원자로 수동 정지 기능이 DPPS에 포함된다. 운전원에 의한 수동 정지는 주제어실 뿐만 아니라 원자로 정지 스위치기어 케비넷, 또는 원격제어반(remote shutdown panel; RSP)에서도 가능하다.

DPPS에 이용되는 디지털 기기는 Programmable logic controller (PLC)로 분류되는 장비이다. PLC는 소규모 처리 시스템에 적합하도록 개발된 디지털 제어기기 집합의 통칭인데, 입력 모듈과 프로세서 모듈, 출력 모듈로 구성되는 것이 일반적이다. 프로세서 모듈은 마이크로프로세서와 메모리를 내장하고 있으므로 소프트웨어를 변경함으로써 해당 PLC의 기능을 쉽게 변경할 수 있도록 되어 있으며, 소프트웨어는 제작사에서 판매하는 툴을 이용하여 쉽게 작성하고 탑재(upload)할 수 있다.

정지변수별로 4개 채널의 측정 루프로부터 전달된 신호는 아날로그 입력모듈을 거쳐 BS 프로세서 모듈로 전달된다. 아날로그 입력(Analog Input; AI) 모듈에는 Analog-to-digital Converter (ADC)가 내장되어 있어 BS 프로세서 모듈은 버스를 통해 전송된 데이터를 디지털 연산을 이용하여 처리하게 된다. CPC에서 계산하는 DNBR과 LPD의 경우는 측정 신호들이 CPC로 전송된 후 원자로 정지 설정치에 도달했는지는 계산하여 디지털 입력(Digital Input; DI)모듈을 통해 BS 모듈에

전달된다.

일단 BS 프로세서에 제공된 신호들은 미리 정해진 원자로 정지 설정치와의 비교를 거친다. 모두 15개의 정지 변수가 있으며, 각각에 대해서 BS 프로세서가 설정치와 비교하는 작업을 수행한다. 이 작업은 4개의 독립된 채널 내부에 각각 2대씩 총 16대가 설치된 BS 프로세서 내에서 독립적으로 수행된다. 각 디지털 모듈의 배치와 신호 흐름은 그림 8에 도시한 바와 같다. BS 프로세서에서 수행되는 모든 작업은 각 변수별로 순차적으로 이루어진다. 즉 각각의 BS 프로세서가 모든 변수에 대한 계산을 독립적으로 수행하여, 그 결과를 각각 출력하는 것이다.

설정치와의 비교가 끝나면 그 신호들은 그림 7에 도시한 바와 같이 다른 채널의 LCL 프로세서들을 포함한 모든 LCL 프로세서에 전달된다. 이 과정은 RS-232 포트를 이용한 디지털 통신을 통해 이루어진다. 이 디지털 통신의 내용중에는 BS 프로세서의 자체 건전성을 점검한 내용이 담겨 있으므로 수신측인 LCL 프로세서에서는 신호를 보내온 BS 프로세서가 정상이 아니라고 판단되면, 안전성 증진을 위해 정지 신호가 생성된 것으로 간주하여 처리를 수행한다. 이 프로세서 간의 신호전달의 상세한 배열은 그림 8에 정리한 바와 같다. 각 LCL 프로세서들은 4개 채널의 BS 프로세서들의 신호를 모두 받아서 판단을 내리는데, 4개의 채널 중에서 2개 이상의 채널에서 정지 신호를 발생시켰을 경우 최종적으로 원자로 정지 신호를 발생시킨다. 이 과정은 총 16개의 LCL 프로세서 각각에서 독립적으로 수행되며, LCL 프로세서에서 수행되는 모든 작업은 각 정지 변수별로 순차적으로 이루어진다.

각 LCL 프로세서에서 생성된 원자로 정지신호는 역시 각 LCL 프로세서별로 독립 할당된 디지털 출력 모듈을 통해 중첩계전기(Interposing Relay)로 전송된다. 이때 각 LCL 프로세서를 감시하는 감시타이머(Watchdog Timer)에서 생성된 신호와 그림 10과 같은 형태로 합성된다. LCL 프로세서 모듈은 자신이 정상적으로 작동하고 있는지를 확인하여 주기적으로 신호를 Heart beat의 형태로 감시 타이머에 전달하는데, 이 Heart beat이 일정한 시간이상 감시타이머에 입력되지 않을 경우 감시타이머는 해당 프로세서 모듈이 비정상상태에 있는 것으로 판단하여 고장시 안전(Fail Safe)개념에서 원자로 정지 신호를 발생시키게 된다. 중첩계전기 이전의 단계에서는 각 정지 변수별로 신호처리가 독립적으로 이루어지지만, 중첩계전기 이후의 단계에서는 정지 변수 구별은 없어지고 정지 상태인지 아닌

지의 신호만으로 처리가 수행된다.

원자로 정지는 개시계전기의 정지에 의해 원자로 정지 스위치기어(RTSS)에 속해 있는 TCB를 개방시킴으로써 이루어진다. 원자로 정지 스위치기어에는 4개의 TCB가 있으며 TCB마다 한 개씩의 개시 회로가 연결되어 있다. 개시 회로의 개방은 RTSS회로를 구성하는 분로 정지 코일(Shunt Trip Coil)의 여자 또는 저전압 코일(Under-voltage Coil)의 비여자를 통해 이루어 지는데 이것은 그림 8과 그림 10에 개념을 도시하였다. 정지신호는 일반적인 2/4논리가 아닌 선택적 2/4논리에 의해 발생되는데, 1번과 3번 중의 하나의 채널에서 신호가 발생하고 또한 동시에 2번과 4번 중의 하나의 채널에서 신호가 발생해야만 정지가 이루어지는 선택적 2/4 논리이다. TCB를 필요에 따라 개방하기 위하여 주제어실에 2개의 수동 정지 누름 스위치 세트가 제공되고, 운전원에 의한 수동 정지는 정지 논리회로를 완전히 우회하게 된다. PPS 케비넷과는 완전히 분리되어 있는 RTSS 케비넷에서도 각각의 TCB마다 누름 스위치가 설치되어 있어 운전원에 의한 수동 정지가 가능하다.

정리하자면, DPPS는 15개의 핵 증기 공급계통(NSSS)의 정지변수들을 감시하며, 현장에서 계측된 각각의 정지변수 측정값들은 직류 전압신호로 바꾸어 공급되는데, 만일 감시중인 어떤 정지변수가 설정치에 도달하게 되면 RTSS의 TCB를 개방시켜 궁극적으로는 원자로를 정지시키는 역할을 하게 된다.

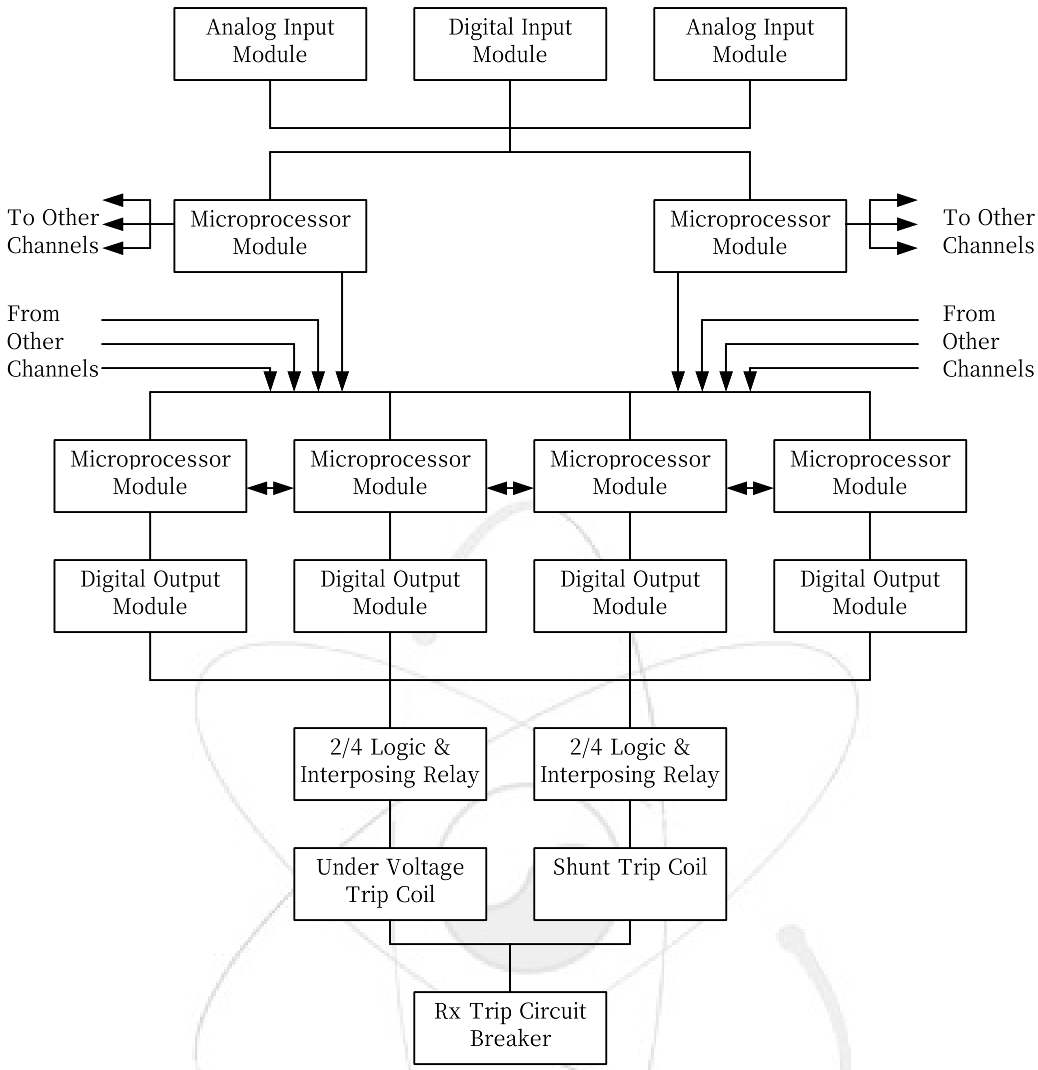

그림 8. DPPS 단일 채널 내부의 기능 블록도

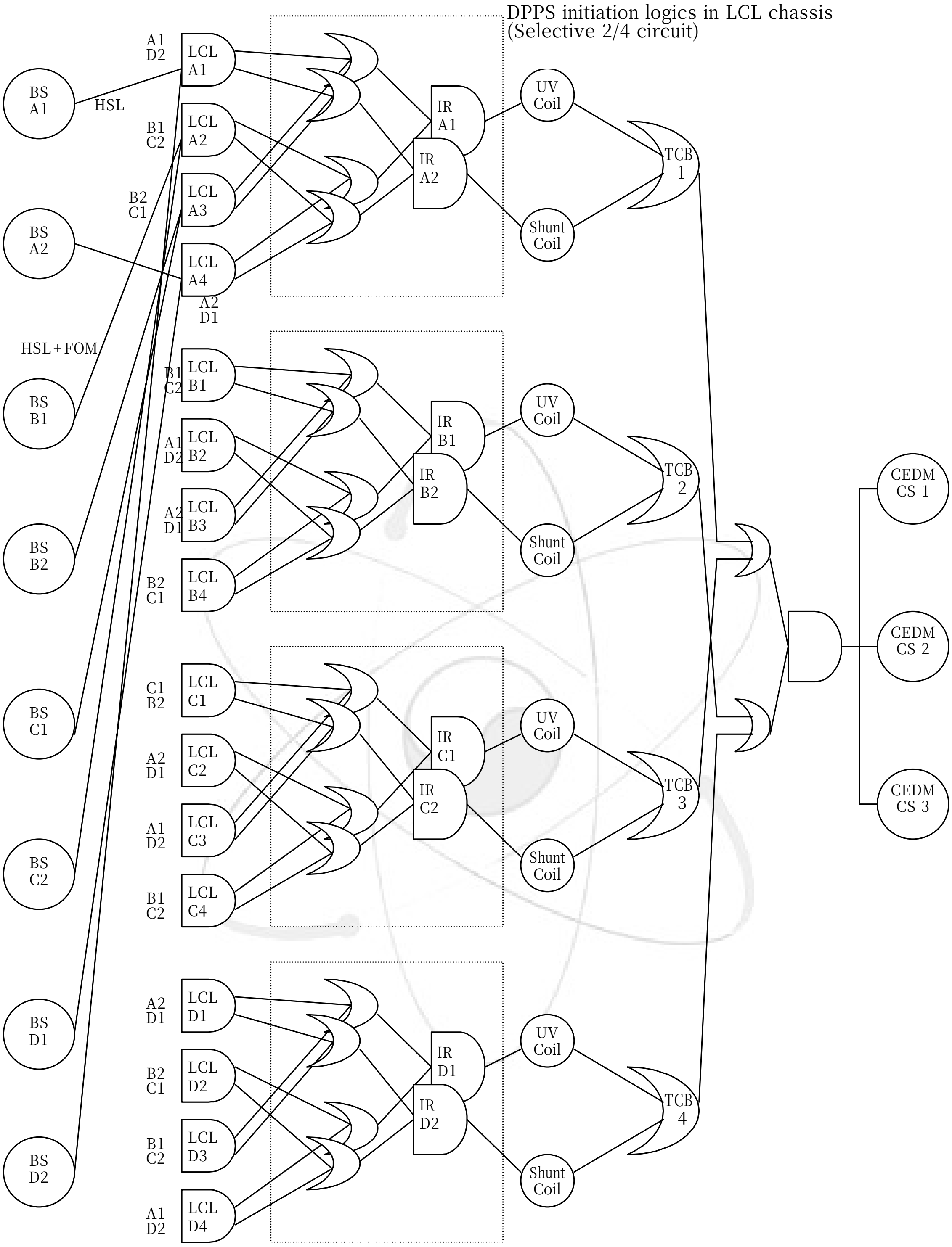

그림 9. DPPS 결선 개념도

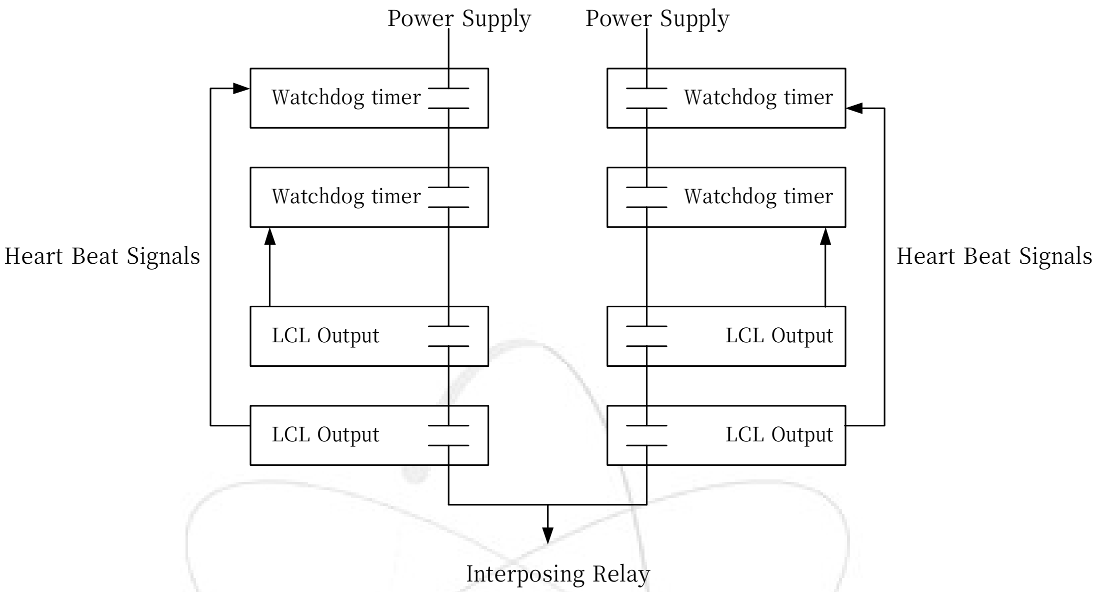

그림 10. 감시타이머의 배치 (LCL: local-coincidence-logic)

제 2 절 출력모듈의 공통원인고장 분석

제 1 절에서 설명한 바와 같이 DPPS의 출력모듈은 각 LCL 프로세서에 하나씩 할당되므로, 4채널에 각 채널당 4개씩 총 16개의 다중성이 존재한다. 이 기기들의 공통원인 고장이 전체 계통의 기능상실을 유발하는 경우를 분석하는 것이 필요하므로, 그림 9에 나타난 출력 결선을 고려하여 기기들의 배열을 개념적으로 정리해 보면 그림 11에 보이는 것과 같다.

이 개념도는 전기의 접점으로 각 모듈의 기능상실이 계통에 미치는 영향을 표현한 것이므로 전기가 위쪽에서 아래쪽으로 흐르는 것을 막지 못하게 되는 경우가 전체 계통이 기능을 상실하는 경우에 대응한다. 즉, 접점이 고장나서 계속 연결상태에 있게 되면 결국은 전기의 흐름을 막지 못하는 경우가 발생하게 되고, 그것이 곧 계통의 기능상실로 연결된다는 개념이다.

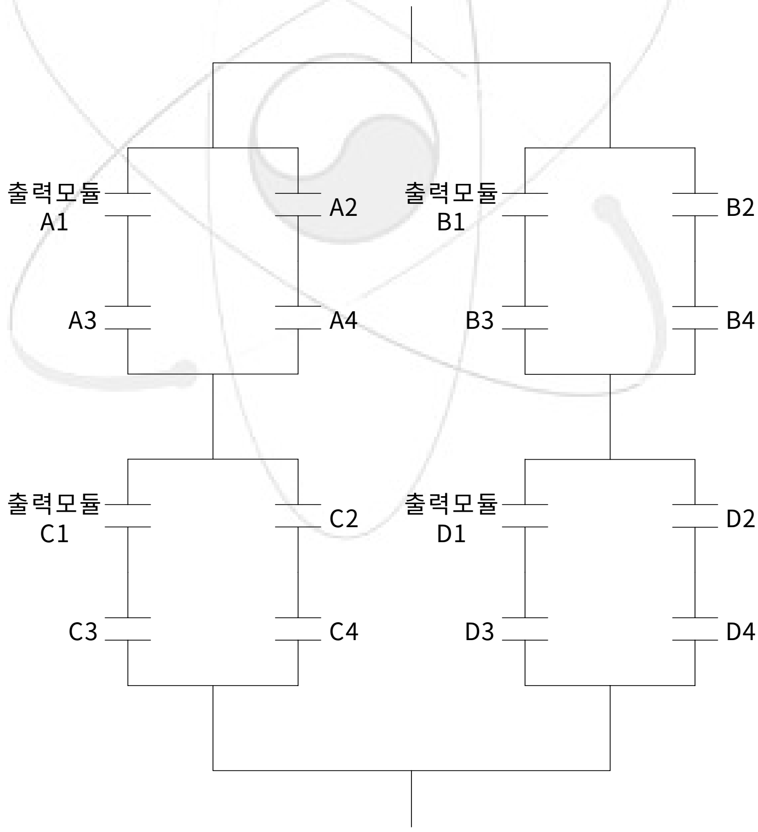

그림 11. 출력모듈 고장이 계통 기능상실에 미치는 영향 개념도

먼저 전체 계통은 보면 16개 기기가 4개씩 짝을지어 한 채널을 구성하고 있다. 채널 4개의 출력이 다시 전체 계통을 구성하는 방식이다. ABCD의 4개의 채널은 선택적 2/4회로를 구성하고 있으므로, 전체 계통이 기능을 상실하기 위해서는 적어도 A와 C채널이 동시에 고장나거나 B와 D채널이 동시에 고장나는 경우가 발생해야 한다. 또한 각 채널이 기능을 상실하기 위해서는 1번기기와 3번기기가 동시에 고장나거나 2번기가와 4번기기가 동시에 고장나는 경우가 발생해야 한다. 이 결과를 정리해 보면 표 4와 같다.

다시 한번 강조하자면 한가지의 기기 공통원인 고장이 단독으로 계통 기능상실을 유발하지 않더라도, 다른 종류의 모듈 고장과 함께 결합해서 나타날 경우 계통 기능상실을 유발할 수 있으나, 그 확률이 낮은 것으로 판단하여 본 분석에서는 고려하지 않았다.

그림 11에 따르면 계통의 기능을 상실시키기 위한 최소 단절집합은 {A1, A3, C1, C3}, {A1, A3, C2, C4} 등 총 8개가 존재하는데, AC경로와 BD경로에 각각 4개씩이다. 이 집합들을 기준으로 각 고장 기기수에 대해 계통 기능상실을 초래하는 경우의 수를 계산하면 다음과 같다.

k= 2: 0

k= 3: 0

k= 4: 8

k= 5: $8*{}_{12}C_1$

k= 6: $8*{}_{12}C_2 - 2*{}_4C_3$

k= 7: $8*{}_{12}C_3 - 2*{}_4C_3*{}_{10}C_1$

k= 8: $8*{}_{12}C_4 - \{2*{}_4C_3*({}_{10}C_2 - 1) + 4*4\} - 3*2$

k= 9: $8*{}_{12}C_5 - \{2*{}_4C_3*({}_{10}C_3 - {}_8C_1) + 4*4*{}_4C_1*2\} - 3*2*{}_8C_1$

k=10: $8*{}_{12}C_6 - \{2*{}_4C_3*({}_{10}C_4 - {}_8C_2 - 4) + 4*4*{}_4C_2*2^2\} - 2*2*4*{}_4C_3 - 3*2*{}_8C_2$

k=11: $8*{}_{12}C_7 - \{2*{}_4C_3*({}_{10}C_5 - {}_8C_3 - 4*{}_6C_1) + 4*4*{}_4C_3*2^3\} - 2*2*4*{}_4C_3*{}_3C_1*2 - 3*2*{}_8C_3$

k=12: $8*{}_{12}C_8 - \{2*{}_4C_3*({}_{10}C_6 - {}_8C_4 - 4*{}_6C_2 - 1) + 4*4*{}_4C_4*2^4\} - 2*2*4*{}_4C_3*{}_3C_2*2^2$
$- 3*\{2*({}_8C_4 - 4) + {}_4C_3*{}_4C_3\} - 4*2*4$

k=13: ${}_{16}C_{13}$

k=14: ${}_{16}C_{14}$

k=15: ${}_{16}C_{15}$

k=16: ${}_{16}C_{16}$

이 식들은 최소단절집합 구성에 필요한 4개의 고장과 그외의 고장들이 구성 가능한 경우의 수로 계산한 것이며, 중복 계산되는 것을 고려하여 2회중복, 3회중복, 4회중복, 5회중복 등을 계산하여 감하는 방식으로 구성되어 있다.

표4. 출력모듈 CCF중 계통 기능상실을 초래하는 고장조합

공통원인고장 기기 수 (k)	가능한 고장조합의 수 ($_{16}C_k$)	계통 기능상실을 초래하는 고장조합의 수 (F_k)	비율 ($p_k=F_k/_{16}C_k$)
1	16	0	0.000
2	120	0	0.000
3	560	0	0.000
4	1820	8	0.004
5	4368	96	0.022
6	8008	520	0.065
7	11440	1680	0.147
8	12870	3584	0.278
9	11440	5264	0.460
10	8008	5352	0.668
11	4368	3728	0.853
12	1820	1756	0.965
13	560	560	1.000
14	120	120	1.000
15	16	16	1.000
16	1	1	1.000

표 4에 보인 비율을 적용하여 알파펙터 방법을 이용하여 각 k에 대하여 계산한 기본모수 $Q_k^{(m)}$에 곱한 후, 2이상의 k에 대한 값을 합산하여 단일 공통원인 사건의 확률로 하는 것이다. $Q_k^{(m)}$는 m개의 공통원인 기기 집단에서 k개의 기기가 동시에 고장 날 사건의 확률로 정의된다. 출력모듈의 경우 m=16이다.

따라서 단일 공통원인고장 사건의 확률은 표 4의 p_k를 이용하여 아래의 식

과 같이 표현할 수 있다.

$$Q_{CCF} = \sum_{k=2}^{m} ({}_{m}C_{k} \times p_k Q_k^m) = \sum_{k=2}^{16} ({}_{16}C_{k} \times p_k Q_k^{16})$$

이때 Q_{CCF}를 계산하는 식이 Q_t를 계산하는 식에서 단순히 p_k항만 추가된 것이 아님을 유의해야 한다. Q_{CCF}는 한 개의 기기의 총 공통원인 고장확률이 아니라, 한 CCF 그룹 기기 전체의 공통원인고장 중 계통 기능상실을 유발하는 확률의 합이기 때문이다.

$$Q_t = \sum_{k=1}^{m} ({}_{m-1}C_{k-1} * Q_k^m)$$

만약 p_k가 모두 1이라면 (즉, 어떤 공통원인고장 조합도 계통의 기능상실을 유발한다면), $Q+Q_1^m$ 은 Q_t보다 큰 값을 갖게 된다. 여기서 Q_t는 모듈의 제조사에서 주어지는 단일 기기의 고장확률이다.

비순차 시험을 통해 기기를 점검하는 경우 각 Q_k^{16} 은 아래의 식으로 구할 수 있다.

$$Q_k^{16} = \frac{k}{{}_{15}C_{k-1}} \cdot \frac{\alpha_k^{16}}{\alpha_t} \cdot Q_t$$

특정기기에 대해 고장 데이터를 충분히 갖추었을 때는 그 데이터를 분석하여 공통원인고장 모수(parameter)를 추정하는 것이 일반적이나, 디지털 기기의 경우 원자력발전소에서 안전계통에 사용한 경험이 없으므로 충분한 데이터를 확보하고 있지 않다. 이런 경우에는 주어진 generic parameter를 이용한다. 표 5는 16개의 기기에 대한 알파펙터 방법의 generic parameter이다. 일반적으로 주어진 16개의 기기그룹에 대한 알파펙터는 구할 수 없으므로, 8개 이상의 기기의 CCF는 모두 치명적 쇼크(lethal shock)으로 인한 것으로 가정하고, 8개 기기그룹의 알파펙터를 16개 기기그룹에 대해 확장한 것이다. 이러한 모수 추정 부정확성은 추후 연구를 통해 보완되어야 할 것으로 판단된다.

표 5의 모수들로부터 아래의 표 6과 같이 단일 공통원인고장 사건의 확률을 계산할 수 있다. 편의를 위해 각 기기의 CCF확률과 독립고장확률의 비를

CCF계수라는 개념으로 정의하였다. 이 계수를 먼저 구하면 단독고장확률에 곱하여 간단히 각 CCF사건의 확률을 계산할 수 있다.

한편, 순차시험을 통해 기기를 점검하는 경우에는 제 2 장의 제 2 절에 기술한 순차시험에서의 $Q_k^{(m)}$ 산출식을 이용하여 상기의 과정을 적용하면 단일 공통원인고장 사건의 확률을 계산할 수 있다.

표5. 16개의 기기에 대한 알파펙터 방법의 Generic Parameter 추정치
(8개 기기에 대한 parameter의 확장)

공통원인고장 기기 수 (k)	알파 모수 (α_k)
1	0.961717
2	0.010950
3	0.007795
4	0.006158
5	0.004350
6	0.002542
7	0.001939
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0
16	0.004551
t	1.155012

표6. 출력모듈에 대한 단일공통원인고장 확률 계산

공통원인고장 기기 수 (k)	가능한 고장조합의 수 ($_8C_k$)	비율 (p_k)	Q_k / Q_t
2	120	0.000	0.0012640
3	560	0.000	0.0001928
4	1820	0.004	0.0000469
5	4368	0.022	0.0000138
6	8008	0.065	0.0000044
7	11440	0.152	0.0000023
8	12870	0.279	0.0000000
9	11440	0.460	0.0000000
10	8008	0.668	0.0000000
11	4368	0.853	0.0000000
12	1820	0.965	0.0000000
13	560	1.000	0.0000000
14	120	1.000	0.0000000
15	16	1.000	0.0000000
16	1	1.000	0.0630381
CCF 계수 (Q / Q_t)			0.07097

다시 한번 강조하지만, 표 6에 계산된 결과는 8개 기기그룹에 대한 generic 알파펙터를 확장하여 적용한 표 5의 결과에 바탕을 둔 것이다. 따라서 표 5의 결과가 개정된다면 CCF계수 또한 다시 계산되어야 한다. 그리고 만약 디지털 기기 고유의 알파펙터값이 추정이 가능하다면, 주어진 generic 앞라펙터를 이용하는 것 보다 더 정확하게 CCF계수를 구할 수 있다. 알파펙터를 직접 구하는 작업은 이 보고서의 범위를 넘어서는 일이므로 여기서는 다루지 않는다.

위에서는 각 공통원인고장 개수 k에 대하여 전체 계통이 기능을 상실하는 경우를 최소단절집합을 기준으로 계산한 결과이다. APR1400의 경우 설계가 개선

되어 각 채널이 격벽으로 분리된 독립된 방에 설치되도록 되었다. 이런 경우에는 채널을 기준으로 기기 공통원인 고장으로 인한 계통 기능상실의 경우를 판단해야 한다. 본 보고서는 한국형표준원전을 대상으로 하므로, 여기서 격벽으로 인해 CCF의 원인이 차단될 가능성을 상세히 고려하는 연구는 언급하지 않는다.

그러나 채널별 계산식을 제공하는 것은 추후 확장 연구를 위해 필요할 것으로 판단되므로 아래에서는 채널 기능고장을 기준으로 계통기능상실의 경우의 수를 계산하는 과정을 보였다.

가. 공통원인고장 개수 = 2

계통 기능상실 불가능. 3개 이하의 기기 고장은 2개이상의 채널 고장을 유발할 수 없으므로 계통 기능상실이 불가능하다.

나. 공통원인고장 개수 = 3

계통 기능상실 불가능. 3개 이하의 기기 고장은 2개이상의 채널 고장을 유발할 수 없으므로 계통 기능상실이 불가능하다.

다. 공통원인고장 개수 = 4

A채널 고장에 2개의 고장이, C채널 고장에서 2개의 고장이 배분되되, 각각 1,3번 기기 또는 2,4번 기기의 고장에 해당하여 채널 고장을 유발하도록 배치되는 경우 계통 기능상실 가능. 마찬가지로 B채널과 D채널에 2개씩 배분되는 경우도 성립.

즉, A1*A3*C1*C3,   A2*A4*C1*C3,   B2*B4*D1*D 등의 경우에는 계통의 기능상실을 유발한다. 이를 고려하여 경우의 수를 계산하면

A/C채널 고장의 경우: ${}_2C_1 * {}_2C_1$

B/D채널 고장의 경우: ${}_2C_1 * {}_2C_1$

총 ${}_2C_1 * {}_2C_1 * {}_2C_1 = 8$개의 경우의 수가 존재한다.

라. 공통원인고장 개수 = 5

역시 2개의 채널 고장을 유발시켜 전체 계통 기능을 상실시키는 방법밖에

없고, 4개의 고장으로 기능상실을 시키는 경우의 수는 8가지 이므로, 나머지 한 개의 고장이 나머지 12개 기기중에서 발생한 것이다.

총 $({}_{2}C_{1} * {}_{2}C_{1} * {}_{2}C_{1}) * {}_{12}C_{1} = 96$개의 경우의 수가 존재한다.

마. 공통원인고장 개수 = 6

6개의 고장은 최대 3개 채널의 고장을 유발할 수 있다. 1개 채널 고장은 기능상실을 유발하지 못하므로 2개 채널과 3개 채널의 고장만 고려한다. 아래와 같이 총 520개의 경우에 대해 계통이 기능을 상실한다.

< 3개 채널 고장 >

4채널중 3채널의 고장이 발생하고, 각 채널내에서는 2개의 고장만으로 채널 고장이 유발되어야 하므로 1,3 조합과 2,4 조합이 존재한다.

${}_{4}C_{3} * {}_{2}C_{1} * {}_{2}C_{1} * {}_{2}C_{1} = 32$

< 2개 채널 고장 >

4개의 고장이 고장 채널에서 발생하고 나머지는 정상 채널에서 발생하는 경우, 5개의 고장이 고장 채널에서 발생하는 경우, 6개 모두 고장 채널내에서 발생하는 경우를 나눠 계산할 수 있다.

고장 채널 내 4개 고장: $({}_{2}C_{1} * {}_{2}C_{1} * {}_{2}C_{1}) * ({}_{8}C_{2} - {}_{4}C_{1}) = 192$

고장 채널 내 5개 고장: $({}_{2}C_{1} * {}_{2}C_{1} * {}_{2}C_{1}) * {}_{4}C_{1} * {}_{8}C_{1} = 256$

고장 채널 내 6개 고장: ${}_{2}C_{1} * ({}_{2}C_{1} * {}_{2}C_{1} * {}_{4}C_{2} - {}_{4}C_{3}) = 40$

바. 공통원인고장 개수 = 7

아래와 같이 총 1680개의 경우에 계통 기능상실이 발생한다.

< 3개 채널 고장 >

${}_{4}C_{3} * {}_{2}C_{1} * {}_{2}C_{1} * {}_{2}C_{1} * {}_{10}C_{1} = 320$

< 2개 채널 고장 >

고장 채널 내 4개 고장: $({}_{2}C_{1} * {}_{2}C_{1} * {}_{2}C_{1}) * ({}_{8}C_{3} - {}_{4}C_{1} * {}_{6}C_{1}) = 256$

고장 채널 내 5개 고장: $({}_{2}C_{1} * {}_{2}C_{1} * {}_{2}C_{1}) * {}_{4}C_{1} * ({}_{8}C_{2} - {}_{4}C_{1}) = 768$

고장 채널 내 6개 고장: ${}_{2}C_{1} * ({}_{2}C_{1} * {}_{2}C_{1} * {}_{4}C_{2} - {}_{4}C_{3}) * {}_{8}C_{1} = 320$

고장 채널 내 7개 고장: ${}_{2}C_{1} * {}_{8}C_{7} = 16$

사. 공통원인고장 개수 = 8

아래와 같이 총 3586개의 경우에 계통 기능상실이 발생한다.

< 4개 채널 고장 >

${}_{2}C_{1} * {}_{2}C_{1} * {}_{2}C_{1} * {}_{2}C_{1} = 16$

< 3개 채널 고장 >

고장 채널 내 6개 고장: $({}_{4}C_{3} * {}_{2}C_{1} * {}_{2}C_{1} * {}_{2}C_{1}) * ({}_{4}C_{2} - {}_{2}C_{1}) = 128$

고장 채널 내 7개 고장: $({}_{4}C_{3} * {}_{2}C_{1} * {}_{2}C_{1} * {}_{2}C_{1}) * {}_{6}C_{1} * {}_{4}C_{1} = 768$

고장 채널 내 8개 고장: ${}_{4}C_{3} * ({}_{2}C_{1} * {}_{2}C_{1} * {}_{2}C_{1} * {}_{6}C_{2} - {}_{3}C_{1} * {}_{2}C_{1} * {}_{2}C_{1}) = 432$

< 2개 채널 고장 >

고장 채널 내 4개 고장: $({}_{2}C_{1} * {}_{2}C_{1} * {}_{2}C_{1}) * ({}_{8}C_{4} - {}_{4}C_{1} * {}_{6}C_{2} + {}_{4}C_{2}) = 128$

고장 채널 내 5개 고장: $({}_{2}C_{1} * {}_{2}C_{1} * {}_{2}C_{1}) * {}_{4}C_{1} * ({}_{8}C_{3} - {}_{4}C_{1} * {}_{6}C_{1}) = 1024$

고장 채널 내 6개 고장: ${}_{2}C_{1} * ({}_{2}C_{1} * {}_{2}C_{1} * {}_{4}C_{2} - {}_{2}C_{1} * {}_{2}C_{1}) * ({}_{8}C_{2} - {}_{4}C_{1}) = 960$

고장 채널 내 7개 고장: ${}_{2}C_{1} * {}_{8}C_{7} * {}_{8}C_{1} = 128$

고장 채널 내 8개 고장: ${}_{2}C_{1} = 2$

아. 공통원인고장 개수 = 9

아래와 같이 총 5264개의 경우에 계통 기능상실이 발생한다.

< 4개 채널 고장 >

${}_{2}C_{1} * {}_{2}C_{1} * {}_{2}C_{1} * {}_{2}C_{1} * {}_{8}C_{1} = 128$

< 3개 채널 고장 >

고장 채널 내 7개 고장: $({}_{4}C_{3} * {}_{2}C_{1} * {}_{2}C_{1} * {}_{2}C_{1}) * {}_{6}C_{1} * ({}_{4}C_{2} - {}_{2}C_{1}) = 768$

고장 채널 내 8개 고장: ${}_{4}C_{3} * ({}_{2}C_{1} * {}_{2}C_{1} * {}_{2}C_{1} * {}_{6}C_{2} - {}_{3}C_{1} * {}_{2}C_{1} * {}_{2}C_{1}) * {}_{4}C_{1} = 1728$

고장 채널 내 9개 고장: ${}_{4}C_{3} * ({}_{2}C_{1} * {}_{2}C_{1} * {}_{2}C_{1} * {}_{6}C_{3} - {}_{3}C_{1} * {}_{2}C_{1} * {}_{2}C_{1} * {}_{4}C_{1}) = 448$

< 2개 채널 고장 >

고장 채널 내 5개 고장: $({}_{2}C_{1} * {}_{2}C_{1} * {}_{2}C_{1}) * {}_{4}C_{1} * ({}_{8}C_{4} - {}_{4}C_{1} * {}_{6}C_{2} + {}_{4}C_{2}) = 512$

고장 채널 내 6개 고장: ${}_{2}C_{1} * ({}_{2}C_{1} * {}_{2}C_{1} * {}_{4}C_{2} - {}_{2}C_{1} * {}_{2}C_{1}) * ({}_{8}C_{3} - {}_{4}C_{1} * {}_{6}C_{1}) = 1280$

고장 채널 내 7개 고장: ${}_{2}C_{1} * {}_{8}C_{7} * ({}_{8}C_{2} - {}_{2}C_{1} * {}_{2}C_{1}) = 384$

고장 채널 내 8개 고장: ${}_{2}C_{1} * {}_{8}C_{1} = 16$

자. 공통원인고장 개수 = 10

아래와 같이 총 5352개의 경우에 계통 기능상실이 발생한다.

< 4개 채널 고장 >

${}_2C_1 * {}_2C_1 * {}_2C_1 * {}_2C_1 * {}_8C_2 - {}_4C_1 * {}_2C_1 * {}_2C_1 * {}_2C_1 = 416$

< 3개 채널 고장 >

고장 채널 내 8개 고장: ${}_4C_3*({}_2C_1*{}_2C_1*{}_2C_1*{}_6C_2 - {}_3C_1*{}_2C_1*{}_2C_1)*({}_4C_2 - {}_2C_1) = 1728$

고장 채널 내 9개 고장: ${}_4C_3*({}_2C_1*{}_2C_1*{}_2C_1*{}_6C_3 - {}_3C_1*{}_2C_1*{}_2C_1*{}_4C_1)*{}_4C_1 = 1792$

고장 채널 내 10개 고장: ${}_4C_3*({}_2C_1*{}_2C_1*{}_2C_1*{}_6C_4 - {}_3C_1*{}_2C_1*{}_2C_1*{}_4C_2 + {}_3C_2*{}_2C_1)= 216$

< 2개 채널 고장 >

고장 채널 내 6개 고장: ${}_2C_1*({}_2C_1*{}_2C_1*{}_4C_2 - {}_2C_1*{}_2C_1)*({}_8C_4 - {}_4C_1*{}_6C_2 + {}_4C_2) = 640$

고장 채널 내 7개 고장: ${}_2C_1 * {}_8C_7 * ({}_8C_3 - {}_4C_1 * {}_6C_1) = 512$

고장 채널 내 8개 고장: ${}_2C_1 * ({}_8C_2 - {}_2C_1 * {}_2C_1) = 48$

차. 공통원인고장 개수 = 11

아래와 같이 총 3728개의 경우에 계통 기능상실이 발생한다.

< 4개 채널 고장 >

${}_2C_1 * {}_2C_1 * {}_2C_1 * {}_2C_1 * {}_8C_3 - {}_4C_1 * {}_2C_1 * {}_2C_1 * {}_2C_1 * {}_6C_1 = 704$

< 3개 채널 고장 >

고장 채널 내 9개 고장: ${}_4C_3*({}_2C_1*{}_2C_1*{}_2C_1*{}_6C_3 - {}_3C_1*{}_2C_1*{}_2C_1*{}_4C_1)* = 1792$

고장 채널 내 10개 고장: ${}_4C_3*({}_2C_1*{}_2C_1*{}_2C_1*{}_6C_4 - {}_3C_1*{}_2C_1*{}_2C_1*{}_4C_2 + {}_3C_2*{}_2C_1)*{}_4C_1$
$=864$

고장 채널 내 11개 고장: ${}_4C_3*{}_{12}C_{11} = 48$

< 2개 채널 고장 >

고장 채널 내 7개 고장: ${}_2C_1 * {}_8C_7 * ({}_8C_4 - {}_4C_1*{}_6C_2 + {}_4C_2) = 256$

고장 채널 내 8개 고장: ${}_2C_1 * ({}_8C_3 - {}_4C_1 * {}_6C_1) = 64$

카. 공통원인고장 개수 = 12

아래와 같이 총 1756개의 경우에 계통 기능상실이 발생한다.

< 4개 채널 고장 >

${}_2C_1 * {}_2C_1 * {}_2C_1 * {}_2C_1 * {}_8C_4 - {}_4C_1 * {}_2C_1 * {}_2C_1 * {}_2C_1 * {}_6C_2 + {}_4C_2 * {}_2C_1 * {}_2C_1 = 664$

< 3개 채널 고장 >

고장 채널 내 10개 고장: ${}_4C_3*({}_2C_1*{}_2C_1*{}_2C_1*{}_6C_4 - {}_3C_1*{}_2C_1*{}_2C_1*{}_4C_2 + {}_3C_2*{}_2C_1)$

$*({}_4C_2 - {}_2C_1) = 864$

고장 채널 내 11개 고장: ${}_4C_3 * {}_{12}C_{11} * {}_4C_1 = 192$

고장 채널 내 12개 고장: ${}_4C_3 = 4$

< 2개 채널 고장 >

고장 채널 내 8개 고장: ${}_2C_1 * ({}_8C_4 - {}_4C_1 * {}_6C_2 + {}_4C_2) = 32$

파. 공통원인고장 개수 = 13 이상

13개 이상의 기기 공통원인고장은 3개 이상의 채널고장을 유발하므로 모든 경우에 계통 기능상실을 초래한다. 즉, ${}_{16}C_k$ (k는 13이상)의 경우에 계통 기능상실이 발생한다.

제 3 절 동시논리 프로세서 및 감시타이머의 공통원인고장 분석

동시논리 프로세서의 경우 16개의 기기를 CCF그룹으로 분류할 수 있으며 그 기능적 배치가 그림 11에서 보인 출력모듈의 배치와 완전히 동일하다. 동시논리 프로세서로부터 생성된 신호가 각각에 할당된 출력모듈을 통해 전기신호로 바뀌기 때문에, 계통 기능상실의 관점에서 볼 때는 동시논리 프로세서의 고장으로 인한 경우와 출력모듈의 고장으로 인한 경우가 완전히 일대일 대응이 된다.

따라서 제 2 절에서 서술한 값들을 그대로 사용할 수 있으며, 단지 알파펙터의 모수(α_k)와 단일기기의 고장확률(Q_t)의 값만 바뀔 뿐이다. 만일 동시논리프로세서의 경우에도 generic parameter를 사용한다면, Q_t의 값만 해당값으로 바꾸어 주면 된다.

감시타이머도 출력모듈과 동시논리프로세서와 동일한 기능적 배열을 가진다. 그림 10에 보인 바와 같이 하나의 감시타이머가 하나의 동시논리프로세서를 감시하는 구조를 가지기 때문이다. 역시 알파펙터의 모수(α_k)와 단일기기의 고장확률(Q_t)의 값만 바꾸면 제 2 절에 서술한 값을 그대로 사용할 수 있다.

제 4 절 비교논리 프로세서의 공통원인고장 분석

비교논리 프로세서로 인한 계통의 기능상실을 파악하기 위해서는 우선 비교논리 프로세서의 배열과 역할을 정확히 파악하는 것이 중요하다. 앞서 설명한 동시논리 프로세서나 출력모듈 등은 직접 계통의 출력을 생성하므로 그 출력을 생성하지 못하게 하는 고장 조합을 그림 11의 개념도로부터 선정하는 방법으로 계통 기능상실의 경우를 파악하였다. 이에 비해 비교논리 프로세서는 그 출력을 동시논리 프로세서에 제공한다는 점에서 차이가 있다. 따라서 동시논리 프로세서가 정상적인 작동을 하기 위해 필요한 입력을 제공하지 못하는 경우가 바로 비교논리 프로세서의 고장으로 인해 계통의 기능상실이 유발되는 경우라고 판단하는 것이다.

그림 9에 보인 바와 같이 각각의 동시논리 프로세서는 2개의 비교논리 프로세서로부터 입력을 제공받는다. 동시논리 프로세서는 2/4논리를 수행해야 하므로, 이것만으로는 정보가 부족하다. 따라서 내부의 정보 버스를 이용하여 2개씩의 동시논리 프로세서를 하나의 그룹으로 묶어서 서로 비교논리 프로세서로부터 입력된 값들을 공유하도록 한다. 즉, 그림 9의 LCL A1과 LCL A2는 하나의 그룹으로 묶여서 정보를 공유하고 있는 것이다. 그림 12에 도시한 바와 같이 A3-A4, B1-B2, B3-B4, … 하는 식으로 그룹이 형성되어 있다.

만약 그룹내에서 한 비교논리 프로세서가 고장나게 되면 같은 그룹에 속한 또 다른 비교논리프로세서는 입력의 절반을 상실하게 되어 제 구실을 할 수 없게 된다. 본 연구에서는 이런 경우에 fail safe하도록 설계된 것으로 가정한다. 즉, 만약 그런 경우가 발생한다면 정상작동중인 또 하나의 프로세서는 입력받지 못한 값을 보수적으로 설정치 초과로 간주하도록 설계한다고 가정한다.

그림 12의 각 그룹들의 입력을 보면 모두 비교논리 프로세서 A1, B1, C2, D2의 출력이거나 A2, B2, C1, D1의 출력이다. 즉 결선은 복잡해 보이지만 내부적으로 비교논리 프로세서의 출력은 두가지의 세트만을 구성하고 있는 것이다. 이것을 편의를 위해 세트X와 세트Y라 칭하기로 한다.

비교논리 프로세서 세트 X: A1, B1, C2, D2

비교논리 프로세서 세트 Y: A2, B2, C1, D1

각각의 비교논리 프로세서는 2/4 논리를 수행한다. 따라서 하나의 그룹에 입력을 제공하는 동시논리 프로세서 4대중 3개 이상의 기기가 고장을 일으킬 경우 동시논리 프로세서는 기능을 상실하게 된다. 따라서 위의 세트X의 비교논리 프로세서중 3대이상이 공통원인고장을 일으킨 경우에야 비로서 계통의 출력에 영향을 미치게 되며, 세트Y의 경우도 마찬가지이다.

한편, 동시논리 프로세서의 출력은 제 2 절과 제 3 절에서 기술한 바와 같이 선택적 2/4 논리를 거쳐 최종 계통의 출력을 생성하게 된다. 계통의 기능상실을 유발하는 경우만을 고려하면 되므로, 동시논리 프로세서의 고장이 계통의 기능상실을 유발하는지를 검토하기 위해서는 동시논리 프로세서의 기능까지 함께 고려해야 한다.

그림 9의 개념도를 살펴보면 같은 그룹으로 묶이지 않은 두개의 동시논리 프로세서가 먼저 OR논리를 거친 후 나머지의 두개의 OR결과와 AND논리를 통해 결합되는 것을 알 수 있다. 예를 들어 LCL A1과 A3의 출력이 OR논리를 거쳐서 LCL A2와 A4의 OR논리 결과와 AND로 묶인다.

LCL채널A출력 = { (LCL A1) OR (LCL A3) } AND { (LCL A2) OR (LCL A4) }

따라서 LCL A1과 A2가 입력 부족으로 정상적인 작동을 하지 못한다고 해도, LCL A3와 A4만 정상적인 작동을 한다면 전체 계통은 정상적인 작동을 할 수 있게 된다. 다른 채널 B, C, D에서도 동일한 관계가 성립한다.

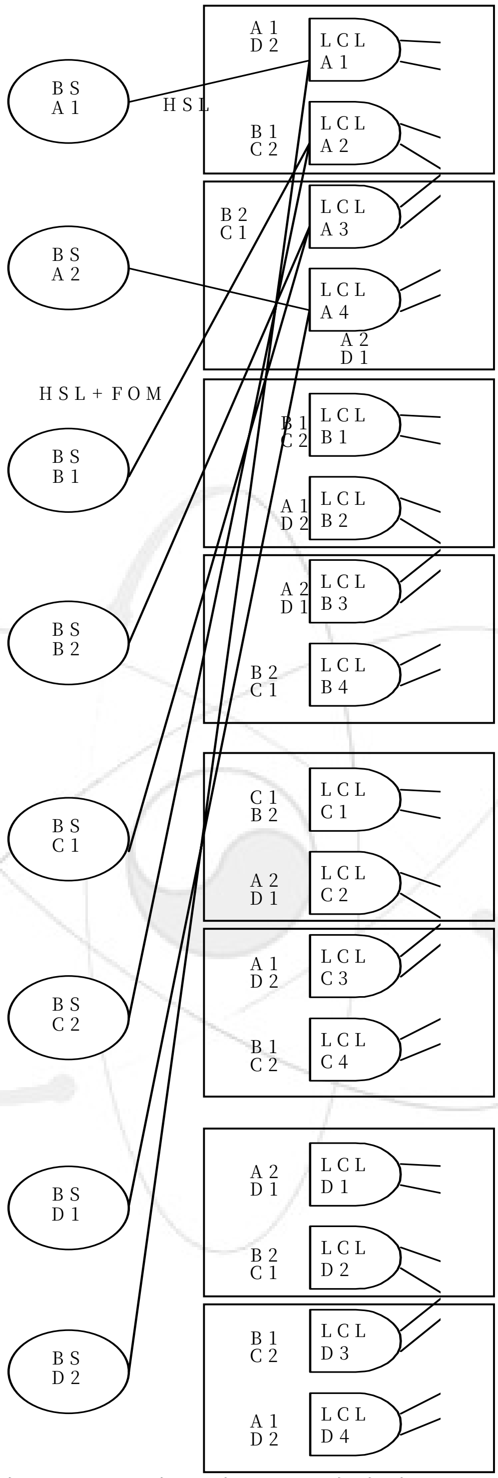

그림 12. 동시논리 프로세서의 그룹

결론적으로 비교논리 프로세서의 고장으로 인한 동시논리 프로세서 입력 상실의 관점에서 볼 때, 위에 설명한 세트X와 세트Y가 모두 각각 3개 이상의 고장기기를 포함하고 있는 경우에만 전체 계통이 기능을 상실한다는 뜻이다. 따라서 총 8개의 비교논리 프로세서중 6개 이상의 프로세서가 공통원인고장으로 기능을 상실한 경우만 분석을 수행하면 된다.

표7. 비교논리 프로세서 CCF중 계통기능상실을 초래하는 고장조합

공통원인고장 기기 수 (k)	가능한 고장조합의 수 ($_8C_k$)	계통 기능상실을 초래하는 고장조합의 수 (F_k)	비율 ($p_k=F_k/_8C_k$)
1	8	0	0.000
2	28	0	0.000
3	56	0	0.000
4	70	0	0.000
5	56	0	0.000
6	28	16	0.571
7	8	8	1.000
8	1	1	1.000

표 7에 보인 비율 p_k를 적용하여 m=8에 대해 제 2 절에 기술한 것과 동일한 과정을 거치면 단일 사건으로 모델된 공통원인고장의 확률을 구할 수 있다.

$$Q = \sum_{k=2}^{m}[{}_mC_k \times p_k Q_k^m] = \sum_{k=2}^{8}[{}_8C_k \times p_k Q_k^8]$$

$$Q_k^8 = \frac{k}{{}_7C_{k-1}} \cdot \frac{\alpha_k^8}{\alpha_t} \cdot Q_t$$

표 8은 8개의 기기에 대한 알파펙터 방법의 generic parameter이다. 실제 자료를 확보할 수 있는 경우에는 그에 해당하는 parameter를 추출하여 사용하여야 하지만, 아직은 디지털 모듈의 공통원인고장 자료가 충분히 확보되지 못하였으므로 generic parameter를 사용하기로 한다. 이 모수들로부터 Q_k를 추정하면 아래의 표 9와 같이 단일 공통원인고장 사건의 확률을 계산할 수 있다.

표8. 8개의 기기그룹에 대한 generic alpha parameter

공통원인고장 기기 수 (k)	알파 모수 (α_k)
1	0.95736
2	0.01090
3	0.00776
4	0.00613
5	0.00433
6	0.00253
7	0.00193
8	0.00906
t	1.14978

표11. 비교논리 프로세서모듈에 대한 단일공통원인고장 확률 계산

공통원인고장 기기 수 (k)	가능한 고장조합의 수 ($_8C_k$)	비율 (p_k)	Q_k / Q_t
2	28	0.000	0.00271
3	56	0.000	0.00096
4	70	0.000	0.00061
5	56	0.000	0.00054
6	28	0.571	0.00063
7	8	1.000	0.00168
8	1	1.000	0.06304
CCF계수 (Q / Q_t)			0.08653

아래는 각각의 공통원인 고장 개수에 대해 계통의 기능상실을 유발하는 조합을 계산하는 과정을 기술하였다.

k= 2: 0

k= 3: 0

k= 4: 0

k= 5: 0

k= 6: ${}_{4}C_{3}$ * ${}_{4}C_{3}$
k= 7: ${}_{8}C_{7}$
k= 8: ${}_{8}C_{8}$

제 5 절 아날로그 입력모듈의 공통원인고장 분석

아날로그 입력모듈의 출력은 비교논리 프로세서에 제공되어 동시논리 프로세서와 출력모듈을 거쳐서 최종적으로는 2/4 논리를 거쳐 전체 계통의 기능을 수행하게 된다. 한 개의 채널에서 하나의 계측변수를 받아들이는 경로는 한 개의 아날로그 입력모듈밖에 없으므로 계통의 기능수행에 미치는 아날로그 입력모듈의 영향은 그림 13의 개념도와 같이 표현될 수 있다. 그림 11에서 설명한 것과 마찬가지로 각 모듈을 접점으로 개념화하고, 위쪽과 아래쪽에 흐르는 전류를 차단할 수 없게 되는 경우가 전체 계통이 기능을 상실하는 경우인 것으로 개념화하였다.

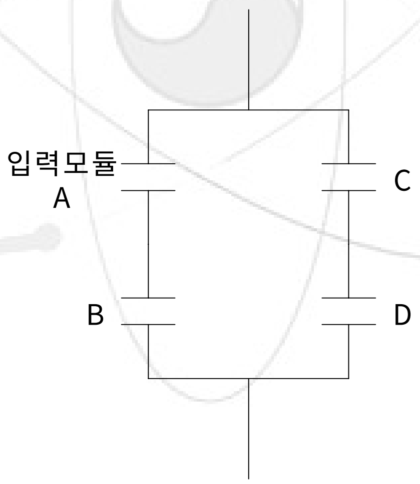

그림 13. 채널별 입력모듈이 전체 계통 기능수행에 미치는 영향 개념도

그런데, 그림 8에 도시한 바와 같이 각 채널에는 2개의 아날로그 입력모듈이 있어 4개 채널에 총 8개의 입력모듈이 있다. 각 채널에는 동일한 종류의 계측변수들이 동일한 배열로 연결된다. 즉, 채널 A, B, C, D에서 아날로그 입력모듈1에 입력되는 변수들은 모두 동일하며 아날로그 입력모듈2에 입력되는 변수들도 마

찬가지이다.

한가지의 계측변수만으로 작동하는 안전 기능(Single Parameter Safety Function; SPSF)에 대한 경우에는 2개중에서 해당 계측변수에 연결된 1개의 입력모듈만 정상적으로 입력을 제공하면 전체 계통은 기능을 정상적으로 수행할 수 있다. 그러나 다중의 계측변수를 바탕으로 작동하는 안전기능(Multiple Parameter Safety Function; MPSF)에 대한 경우에는 여러가지 상황을 고려해야 한다. 우선 MPSF와 SPSF를 분류해 보면 다음과 같다.

Multiple Parameter Safety Function (MPSF):

- Reactor trip signal
- Safety injection actuation signal (SIAS)
- Containment isolation actuation signal (CIAS)
- Main steam isolation signal (MSIS)

Single Parameter Safety Function (SPSF):

- Containment spray actuation signal (CSAS)
- Recirculation actuation signal (RAS)
- Auxiliary feedwater actuation Signal–1 & 2 (AFAS-1 and AFAS-2)

MPSF중에서도 Reactor trip signal은 특수한 경우이다. 기존의 연구[9] 결과에 따르면 어떠한 초기사건의 경우에도 다중의 변수가 원자로 보호를 위해 설정해 놓은 설정치를 초과하는 것으로 나타난다. 즉, 두 세트의 아날로그 입력모듈이 서로의 백업으로 작용할 수 있는 것이다.

반면, 같은 MPSF라 하여도 공학적안전설비 작동변수인 SIAS, CIAS, MSIS의 경우 다중의 변수가 기능수행에 관여할 수도 있고 그렇지 않을 수도 있다. 어떤 초기사건에서 어떤 변수가 설정치를 초과하여 안전기능을 작동시키는 지는 상황에 따라 다르다. 이런 경우 두 세트의 아날로그 입력모듈이 서로의 백업으로 작용할 수 없다고 보수적으로 평가하게 되며, 특히 어떤 계측 변수에 의해 안전기능이 수행될 지 정확히 분석되지 않은 상태에서는, 두 세트의 아날로그 입력모듈이 모두 건전해야만 기능을 수행하는 것으로 보수적인 가정을 도입하는 것이 일반적이다.

디지털 계통의 특성상 소프트웨어에 의해 각 모듈의 기능이 결정되며 멀티테스킹에 의해 여러가지 기능이 동일 하드웨어를 기반으로 수행되기도 한다. 위

의 MPSF와 SPSF는 모두 동일 하드웨어를 이용하여 수행된다는데 분석의 어려움이 있다. 위에 언급한 여러가지 상황이 모두 같은 기기의 고장수목에서 모델되어야 하는 것이다. 즉, 어떤 경우에는 각 채널당 1개씩의 아날로그 입력모듈만을 고려하여 하나의 세트만 고려해야 하고, 어떤 경우에는 각 세트의 입력모듈이 서로 백업으로 작용할 수 있는 것으로 고려해야 하고, 또 어떤 경우에는 두개의 세트중 하나라도 기능을 상실하면 계통이 기능을 상실하는 것으로 모델하여야 한다.

각 초기사건과 사고 경위에 대해 모두 독립적인 고장수목을 작성하는 것은 비현실적인 일이다. 이럴 경우 디지털 보호계통의 고장수목이 전체 플랜트 고장수목보다 훨씬 커지게 된다. 본 연구의 목적은 공통원인고장을 최대한 상세히 모델링하되 현실적으로 가능한 방법을 제시하는 것이므로, 보수적인 가정을 도입하여 여러가지 경우중 가장 보수적인 값을 나타내는 경우를 분석하고 그 공통원인 고장 확률을 사용하기로 한다.

따라서 8개의 기기로 이루어진 CCF그룹을 고려하되, 고장난 기기가 목적기능 수행에 사용되는 기기로 보수적으로 가정을 한다. 이것은 상당히 보수적인 가정이므로 향후 각 고장사건의 전개와 각 안전 계측기의 해당여부에 대한 추가 분석을 수행하여 보다 합리적으로 수정할 필요가 있다. 본 연구에서는 이러한 분석이 수행되지 않은 상태에서 가장 보수적인 가정을 도입하여 CCF확률을 산정였음을 다시 한번 밝힌다.

이런 가정을 도입할 경우 그림 13에 보인 개념도는 아래의 그림14와 같이 변경된다. 즉, 각 모듈을 접점으로 개념화하고 위쪽과 아래쪽에 흐르는 전류를 차단할 수 없게 되는 경우가 전체 계통이 기능을 상실하는 경우인 것으로 개념화할 경우, A1이나 A2중 하나의 기기만 고장상태에 있어도 입력모듈 A채널은 기능을 상실하는 것으로 가정하는 것이다.

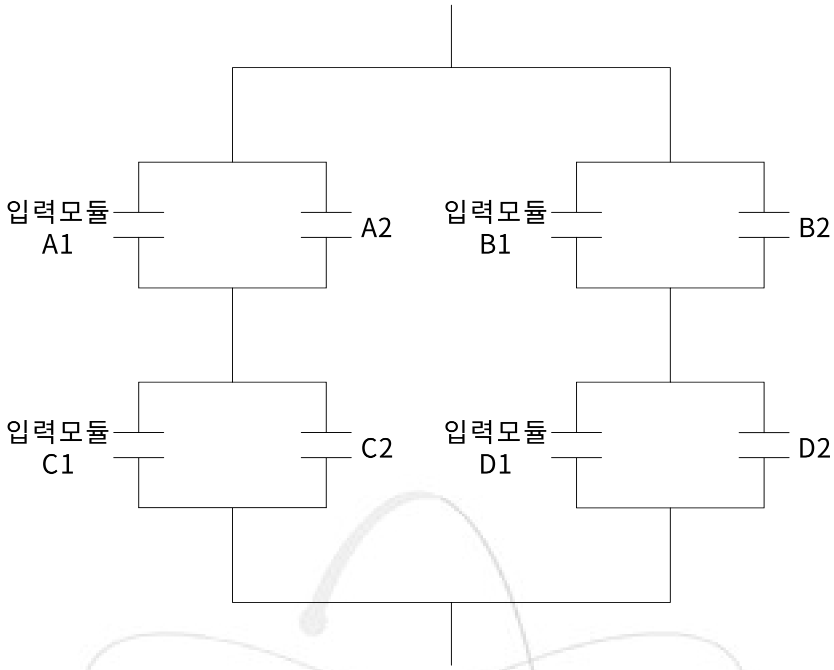

그림 14. 보수적인 가정을 도입할 경우 아날로그 입력모듈이 전체 계통 기능수행에 미치는 영향 개념도

그림 14에 따르면 계통의 기능을 상실시키기 위한 최소 단절집합은 {A1, C1 }, {A1, C2} 등 총 8개가 존재하는데, AC경로와 BD경로에 각각 4개씩이다. 아래에 각각의 공통원인 고장 개수에 대해 계통의 기능상실을 유발하는 조합을 계산하는 과정을 기술하였다. 5개 이상의 기기에서 고장이 발생한 경우 모든 경우에서 계통의 기능상실이 유발된다.

k= 2: 8
k= 3: ${}_8C_3 - 4*4$
k= 4: ${}_8C_4 - 4$
k= 5: ${}_8C_5$
k= 6: ${}_8C_6$
k= 7: ${}_8C_7$
k= 8: ${}_8C_8$

표10. 아날로그 입력모듈 CCF중 계통기능상실을 초래하는 고장조합

공통원인고장 기기 수 (k)	가능한 고장조합의 수 ($_8C_k$)	계통 기능상실을 초래하는 고장조합의 수 (F_k)	비율 ($p_k=F_k/_8C_k$)
1	8	0	0.000
2	28	8	0.286
3	56	40	0.714
4	70	66	0.943
5	56	56	1.000
6	28	28	1.000
7	8	8	1.000
8	1	1	1.000

표 10에 보인 비율 p_k를 적용하여 m=8에 대해 제 2 절에 기술한 것과 동일한 과정을 거치면 단일 사건으로 모델된 공통원인고장의 확률을 구할 수 있다.

$$Q = \sum_{k=2}^{m} [{}_m C_k \times p_k Q_k^m] = \sum_{k=2}^{8} [{}_8 C_k \times p_k Q_k^8]$$

$$Q_k^8 = \frac{k}{{}_7 C_{k-1}} \cdot \frac{\alpha_k^8}{\alpha_t} \cdot Q_t$$

표 8에 보인 8개의 기기에 대한 알파펙터 방법의 generic parameter를 이용하여 아래의 표11과 같이 단일 공통원인고장 사건의 확률을 계산할 수 있다.

표11. 아날로그 입력모듈에 대한 단일공통원인고장 확률 계산

공통원인고장 기기 수 (k)	가능한 고장조합의 수 ($_8C_k$)	비율 (p_k)	Q_k / Q_t
2	28	0.286	0.00271
3	56	0.714	0.00096
4	70	0.943	0.00061
5	56	1.000	0.00054
6	28	1.000	0.00063
7	8	1.000	0.00168
8	1	1.000	0.06304
CCF계수 (Q / Q_t)			0.22465

제 6 절 디지털 입력모듈의 공통원인고장 분석

디지털 입력모듈의 경우 안전신호를 처리하는 기기는 각 채널별로 1개뿐이므로, 계통의 기능수행에 미치는 영향은 그림 13의 개념도와 동일하다. 아래에 각각의 공통원인 고장 개수에 대해 계통의 기능상실을 유발하는 조합을 계산하는 과정을 기술하였다.

k= 2: 2

k= 3: ${}_4C_3$

k= 4: ${}_4C_4$

표12. 디지털 입력모듈 공통원인고장중 계통기능상실을 초래하는 고장조합

공통원인고장 기기 수 (k)	가능한 고장조합의 수 (${}_4C_k$)	계통 기능상실을 초래하는 고장조합의 수 (F_k)	비율 ($p_k=F_k/{}_8C_k$)
1	4	0	0.000
2	6	2	0.333
3	4	4	1.000
4	1	1	1.000

표 12에 보인 비율 p_k를 적용하여 m=4에 대해 제 2 절에 기술한 것과 동일한 과정을 거치면 단일 사건으로 모델된 공통원인고장의 확률을 구할 수 있다.

$$Q = \sum_{k=2}^{m} [{}_m C_k \times p_k Q_k^m] = \sum_{k=2}^{4} [{}_4 C_k \times p_k Q_k^4]$$

$$Q_k^4 = \frac{k}{{}_3C_{k-1}} \cdot \frac{\alpha_k^4}{\alpha_t} \cdot Q_t$$

표 13은 4개의 기기에 대한 알파펙터 방법의 generic parameter이므로, 이 값을 이용하여 아래의 표 14와 같이 Q_k를 추정할 수 있다. 전술한 바와 같이 실제자료를 확보할 수 있는 경우에는 그에 해당하는 parameter를 추출하여 사용하여야 하지만, 아직은 디지털 모듈의 공통원인고장 자료가 충분히 확보되지 못하였으므로 generic parameter를 사용하기로 한다.

표13. 4개의 기기그룹에 대한 generic alpha parameter

공통원인고장 기기 수 (k)	알파 모수 (α_k)
1	0.9500
2	0.0213
3	0.0101
4	0.0186
t	1.0973

표14. 디지털 입력모듈에 대한 단일공통원인고장 확률 계산

k	${}_4C_k$	p_k	Q_k / Q_t
2	6	0.333	0.0129
3	4	1.000	0.0092
4	1	1.000	0.0678
CCF계수 (Q / Q_t)			0.1305

제 4 장 기능 수행을 고려한 고장율 및 공통원인고장율 산정

제 1 절 소프트웨어를 포함하는 디지털 시스템의 특성

기존의 아날로그 방식에서는 불필요한 부품은 계통구성에 포함될 필요가 없었다. 그러나 디지털 시스템의 경우 범용으로 제작되므로 실제 계통의 기능을 수행하는데 필수적인 부품이 아닌 것도 상당수에 이른다. 또한 안전분석을 수행하기 위해서는 계통의 기능 중 안전기능의 수행에 실패하는 경우만을 고려하면 되므로 이를 반영하여야 한다. 그림 15에 하드웨어와 소프트웨어가 결합되어 주어진 기능을 수행하는 관계를 개념적으로 도시하였다. 결국 소프트웨어에 의해 하드웨어 부품들의 사용이 정의되고 필요시 하드웨어가 작동하지 않는다면 계통의 기능수행 실패로 귀결된다.

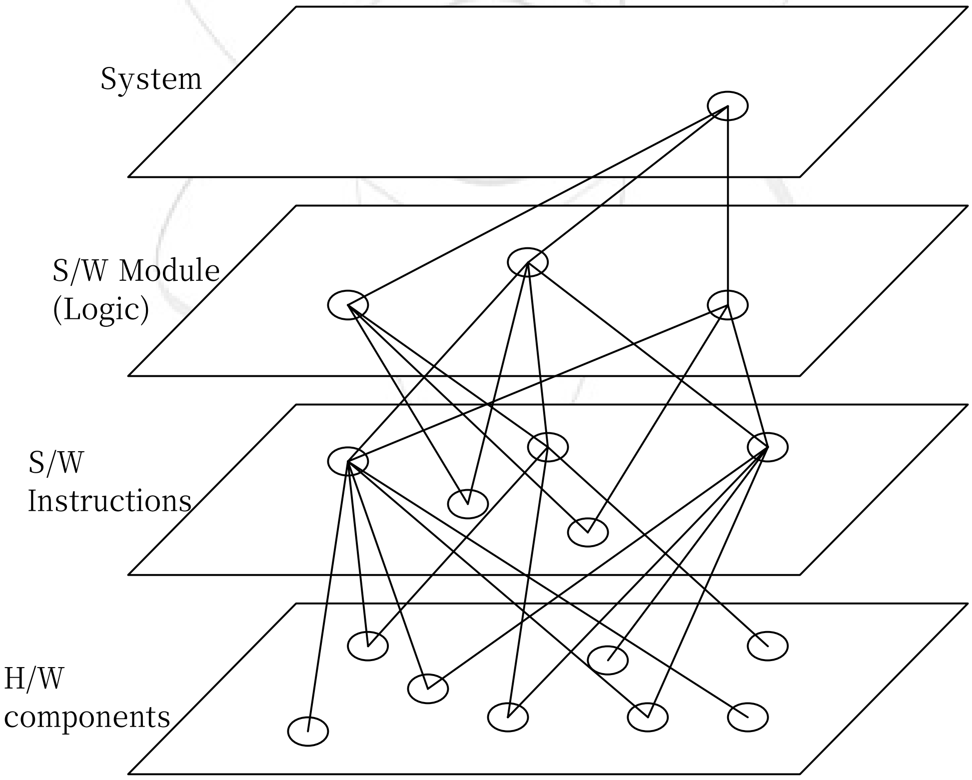

그림 15. 하드웨어와 소프트웨어가 결합되어 기능을 수행하는 것을 고려한 개념적 상관관계

그림 15에 보인 바와 같이 디지털 계통에서 고장은 소프트웨어 로직에서의 오류, 실행 소프트웨어의 오류, 하드웨어의 오류에 기인하는 것으로 분류할 수 있다. 소프트웨어 로직에서의 오류란 처음부터 소프트웨어 설계가 잘못되었거나 기능 사양이 잘 못 주어진 경우에 해당하며, 실행 소프트웨어의 오류는 작성된 코드에 오류가 있는 경우로서 코딩 에러나 컴파일러의 버그로 인한 오류가 이에 해당한다.

상기의 3가지 고장은 모두 CCF의 원인이 될 수 있으며, 이 중 최근 가장 심각하게 논의되는 주제는 소프트웨어 로직에서 발생하는 오류이다. 이것은 동일 기능을 수행하는 기기에는 모두 적용되므로 중요한 CCF의 원인이 되며 전체 플랜트 건전성에 미치는 영향도 매우 크다.

소프트웨어를 탑재하는 디지털 시스템의 특성상 어떤 경우에는 안전기능 수행에 필요했던 부품이 또 다른 경우에는 안전기능 수행에 불필요하기도 하다. 달리 말하자면, 동일한 기기가 완전히 다른 기능을 수행할 수도 있고 이기종의 기기를 이용하여도 상부의 소프트웨어 로직만 동일하면 동일한 기능을 수행하도록 할 수 있는 것이다. 이런 경우에 CCF의 범위를 어떻게 한정하는 것이 합리적인가하는 문제가 남아있다. 이 문제를 확장해 보면 동일한 기능을 수행하는 이기종의 기기가 소프트웨어 로직과 일부 부품을 동일하게 이용한다면 CCF에 얼마나 노출될 것인지까지 생각할 수 있다.

실제로 울진 5,6호기의 DPPS에서도 동일한 프로세서 모듈을 이용하여 비교논리 프로세서와 동시논리 프로세서를 구현하였다. 이 경우에는 비교논리 프로세서가 동시논리 프로세서에 입력을 제공하는 것이고, 이 두가지 프로세서들에 걸치는 CCF가 각각의 CCF에 비해 새로운 기능상실을 유발하지 않으므로 CCF그룹을 한가지로 합치지 않았다. 그러나 만약 서로 다른 기능을 하도록 동일한 기기를 이용하여 구현한 계통의 동시 기능상실이 전체 계통의 기능상실을 유발하는 새로운 원인이 된다면, 전체 기기들을 포함하는 CCF 그룹을 설정하고 분석을 수행하여야 한다.

이런 경우 하드웨어의 고장은 CCF일 수 있지만, 소프트웨어 로직 오류는 CCF의 원인이 되지 않으므로 이것을 고려하여 모델을 작성해야 한다. 다만, 만

약 같은 종류의 컴파일러를 사용하거나 동일한 코딩방법을 사용했다면 실행소프트웨어에 발생하는 CCF는 존재할 수도 있다.

반대의 경우, 즉 이기종의 기기를 이용하여 계통을 구성하였으나 그 이기종의 기기들이 동일한 기능을 수행하는 경우에는 그 이기종 기기들이 동일 CCF그룹에 포함되는지 그렇지 않은지가 중요한 판단사항이다. 일반적으로 디지털 부품의 경우 대량 규격 생산 체제에 의해 제조되어 조립되므로, 이기종의 기기라 하여도 몇가지 부품은 동일한 것을 사용할 수 있다. 동일한 기능을 수행하는 경우에는 동일한 소프트웨어 로직을 이용한다는 뜻이므로, 몇가지 부품이라도 동일한 것이 사용되었을 경우 CCF에 노출될 가능성이 있다고 보고 같은 CCF 그룹으로 분류하는 것이 합당하다.

실제로 초고신뢰도의 안전계통에서 공통원인고장을 회피하기 위하여 다른 기종의 기기가 병렬로 배치되도록 설계하기도 하며, 우리나라에서도 KOPEC의 ADRPS가 이런 방식으로 설계되었다. 이기종의 기기를 이용하였다고 하여도 실제로 동일한 소프트웨어 로직을 이용하여 작성되었으므로 이 부분에서도 CCF의 가능성이 있으며, 하드웨어에서도 동일 부품을 일부라도 사용하였을 경우 CCF의 가능성이 있다.

하드웨어의 CCF를 다루는 방법은 이미 잘 알려져 있고 본 보고서에서도 설명을 하였으므로 동일 기기를 다른 기능수행에 이용한 경우의 모델 작성방법에 대해서는 더 이상 기술하지 않는다. 동일 기능수행을 위해 일부 동일 부품을 사용하는 이기종 기기의 CCF모델에 대해서 제 3절에서 기술하고 실용적인 방법론을 제시한다.

제 2 절 디지털 기기의 범용성에 따른 특성

기존의 아날로그 방식에서는 불필요한 부품은 계통구성에 포함될 필요가 없었다. 그러나 디지털 시스템의 경우 범용으로 제작되므로 실제 계통의 기능을 수행하는데 필수적인 부품이 아닌 것도 포함된 채로 그대로 사용한다. 또한 안전분석을 수행하기 위해서는 계통의 기능 중 안전기능의 수행에 실패하는 경우만을 고려하면 되므로 안전 기능 수행에 관계없는 부품들의 고장은 안전분석에서 고려될 필요가 없다.

이런 상황을 반영하여 분석을 수행하여야 보다 현실적인 안전성 분석이 가능할 것으로 판단된다. 그림 15에 도시된 하드웨어와 소프트웨어가 결합되어 주어진 기능을 수행하는 관계를 고려하면, 결국 소프트웨어에 의해 하드웨어 부품들의 사용이 정의되고 필요시 하드웨어가 작동하지 않는 다면 계통의 기능수행 실패로 귀결된다. 따라서 안전기능 수행에 필수적인 부품을 선별하는 것은 그 기기의 기능분석 및 소프트웨어 로직과 실행 소프트웨어 분석이 선행되어야 가능한 일이다.

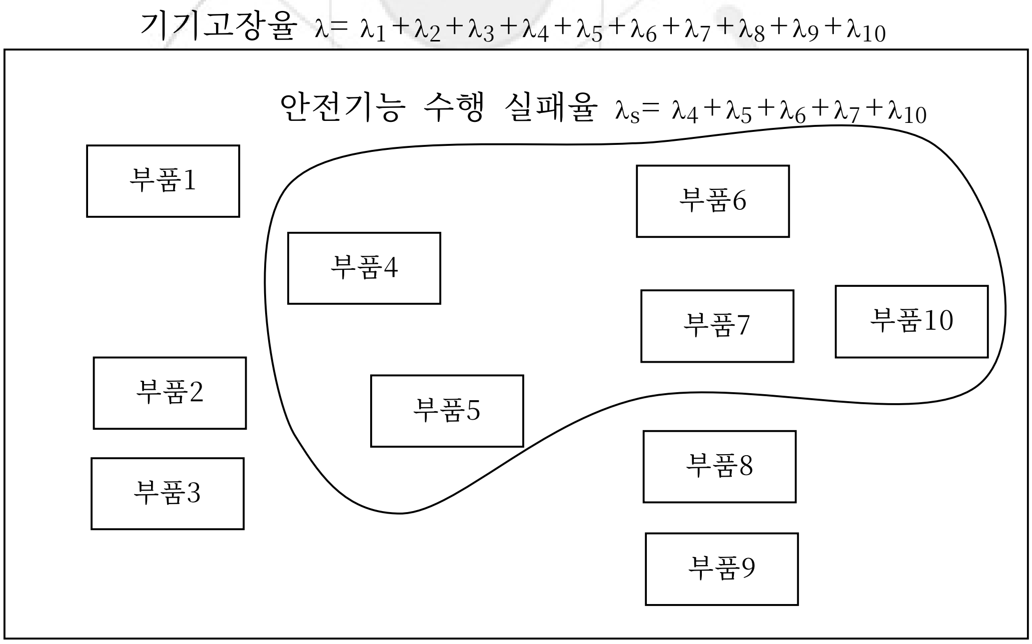

그림 16. 안전 기능 실패율과 기기고장율의 개념도

그림 16은 이러한 관계를 고려하여 기기의 고장 확율과 하드웨어로 인한 안전기능 실패확률 계산의 관계를 개념적으로 도시한 것이다. 이것은 부품 4, 5, 6, 7, 10만이 안전 기능 수행에 관여하고 나머지는 안전기능 수행과 무관한 경우에 대한 예시이다. 즉, λ_s는 안전 기능의 수행 실패율이고, λ는 기기의 고장율이므로 λ를 기기 하드웨어 고장으로 인한 안전 기능 실패율로 가정하는 것은 과도한 보수성을 유발하게 되는 것이다. 특정 목적을 가지고 전용 기기로 처음부터 개발되는 경우에는 이러한 상세 분석의 수행이 가능하나, 범용기기로 사용할 목적으로 개발된 경우에는 다양한 목적에 부응할 수 있도록 설계되므로 상세 분석을 수행하기 어렵다. 이런 경우에는 생산자가 제공하는 기기전체의 고장율값인 λ를 그대로 하드웨어로 인한 안전기능 실패의 확률로 이용한다.

만약 직접 기기를 개발하였거나, 기기 내부의 상세 자료를 이용하는 것이 가능하다면, 전술한 바와 같이 각 특정 목적에 따른 소프트웨어 분석을 병행하여 안전 기능 실패에 기여하는 부품의 고장율만을 계산하는 것이 보다 합리적이다. 그림 16의 경우와 같이 해당 부품만을 가려내어 안전 기능 실패율을 계산하는 것이다.

제 3 절 동일 부품을 포함하는 이기종 기기의 CCF 모델

동일 기능수행을 위해 일부 동일 부품을 사용하는 이기종 기기를 이용하여 계통을 설계하였을 경우, 이 이기종 기기들간의 CCF 존재여부 확인 및 모델 작성을 위한 검토가 필요하다. 동일 기능을 수행하는 경우 동일한 소프트웨어(로직 또는 실행코드)를 사용하는 것이 자명하므로, 동일 부품을 포함하였을 경우 서로 다른 기종의 기기라 하더라도 거기에 포함된 동일 부품은 동일한 상황에서 동일한 논리에 의해 동일한 기능을 수행하는 역할을 맡게 된다. 따라서 동일 CCF그룹으로 고려해야 하는 것이 자명하다.

그러나, 일부 부품을 공유한다고 해서 전체 기기의 CCF를 공유하는 것으로 모델을 작성할 수는 없으므로, 이에 합당한 모델 개발 및 기본사건 확률 추정기법의 개발이 필요하다. 이런 경우 CCF를 두가지로 나누어 모델을 작성하는 것이 합리적이다. 개념적으로 예를 들면 그림 17의 계통을 그림 18의 고장수목으로 모델하는 것이다. A1과 A2는 동종의 기기, B1과 B2는 동종의 기기이며, 이 두가지 기기는 서로 일부의 부품을 공유한다고 가정한다.

그림 16. 안전 기능 실패율과 기기고장율의 개념도

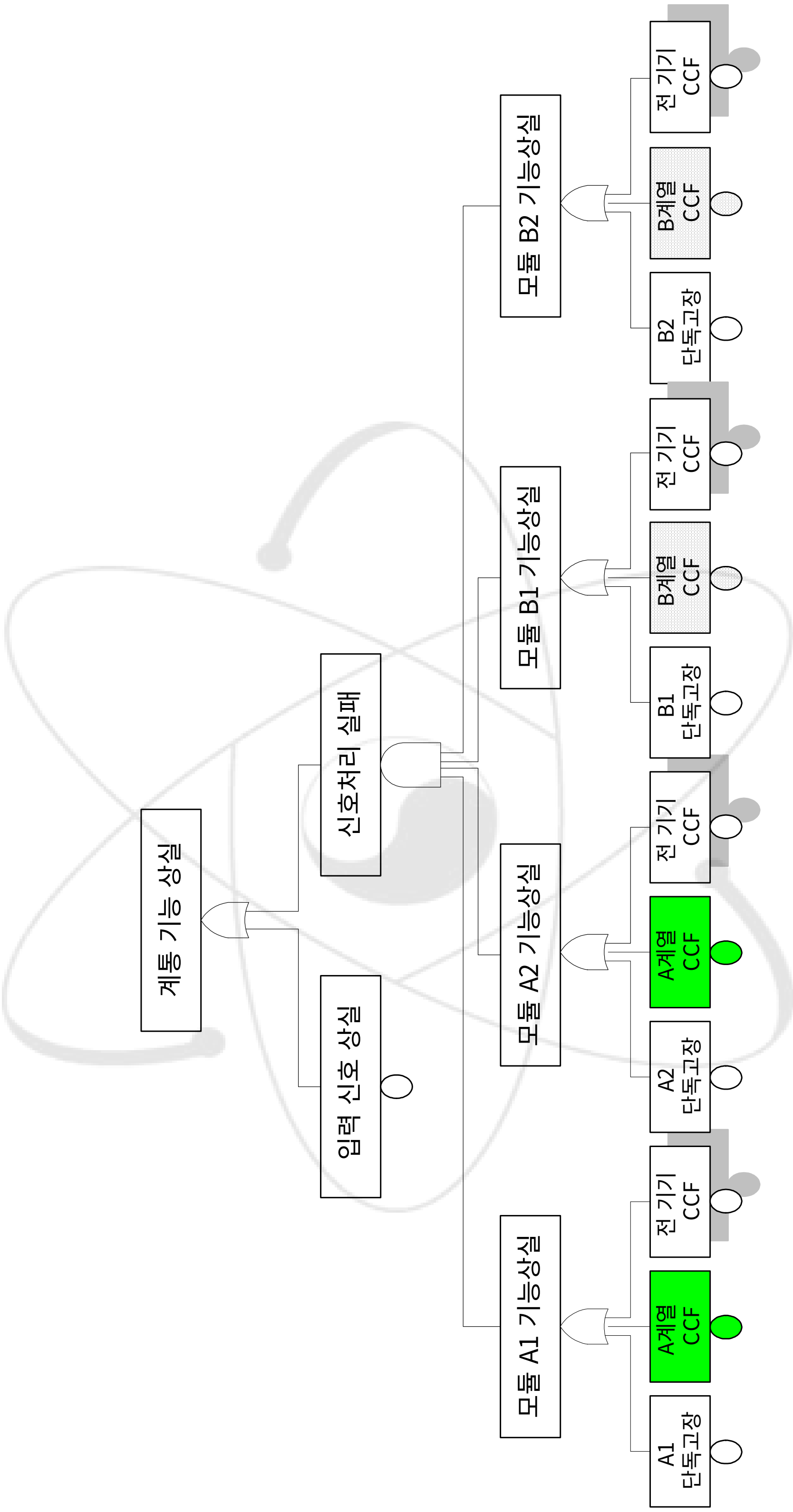

그림 18. 그림 17의 예제 계통에 대한 CCF를 포함하는 고장수목

그림 17의 예제에서는 2가지 기종의 기기들만 사용했으므로 그림 18에 표현된 고장수목에서는 각 기기(모듈)별로 2가지의 CCF 초기 사건을 가지게 된다. 여러 개의 기종을 섞어서 사용하는 경우 CCF초기 사건의 숫자는 증가하게 된다는 것을 유의해야 한다. 이 예제의 경우에서는 2가지 CCF사건의 첫번째는 자신과 동일한 기종의 기기와의 CCF이고, 다른 두번째는 일부부품을 공유하는 이기종 기기까지를 포함하는 CCF이다. 이 두가지의 CCF확률을 제외한 나머지 부분이 각 기기의 단독고장 확률이다.

예를 들어 A기기가 부품 n개로 이루어져 있는데, 그 중에서 m개의 부품은 B기기와 같은 종류를 사용한다고 하자. 그림 17의 예제에서 A기기는 2개만 사용되므로 그에 해당하는 CCF계수(ρ_2)를 구할 수 있는데, B기기와 같은 종류를 사용하는 부품을 제외한 나머지 부품들에만 이 계수가 적용될 수 있다. CCF 계수는 제 3 장에서 설명한 것과 같이 각 부품의 CCF확률과 단독고장확률의 비이다. A기기와 B기기가 공통으로 사용하는 부품에 대해서는 4개의 기기에 대하여 계산한 CCF계수(ρ_4)를 적용하여야 한다.

만약 점검주기가 T이고, 점검에 의해서만 기기의 고장을 발견할 수 있다면, 그림 18의 예제 고장수목에서 사용된 각 초기사건의 확률은 다음의 수식으로 정의된다. *i*는 기기 A와 B가 공통적으로 사용하는 부품을, *j*는 공통으로 사용하지 않는 부품을 나타낸다.

$$p^{CCF(all)} = \frac{T}{2}\sum_{i=1}^{m}\rho_{4(i)}\lambda_i$$

$$p^{CCF(A)} = \frac{T}{2}\sum_{j=m+1}^{n}\rho_{2(j)}\lambda_j$$

$$p^{A1} = \frac{\lambda_{A1}T}{2} - P^{CCF(A)} - P^{CCF(all)} = \frac{T}{2}\sum_{i=1}^{n}\lambda_i - P^{CCF(A)} - P^{CCF(all)}$$

A2의 경우에도 위의 초기사건 확률값을 그대로 이용할 수 있으며 ($p^{A1}=p^{A2}$), B1, B2에 대해서도 똑 같은 방법으로 세가지의 초기사건 확률을 계산할 수 있다. 기기의 숫자가 많아지는 기능적 배열이 복잡해 지는 경우에도 CCF계수를 구하

는 문제만 복잡해질 뿐 똑같은 방법을 역시 적용할 수 있다.

더 다양한 기종의 기기를 섞어서 사용하는 경우에 각 기종간에 공통으로 사용하는 기기가 상이하다. 이러한 경우에는 각 기종간에 공통으로 사용하는 부품을 고려하여 여러 개의 CCF 초기 사건으로 표현해야만 한다. 즉, 각 기기의 고장을 표현하기 위해 필요한 CCF 초기 사건의 숫자가 증가하게 된다. 개념적으로 CCF의 CCF를 모델한다는 것과 같다. 이러한 개념을 사용하면 위 예제를 일반화시킬 수 있다.

만약 3가지 기종의 기기(A, B, C)를 동일 기능 수행을 위해 사용했다면, A와 B 기종의 공통부품으로 인한 CCF인 CCF^{AB}, A와 C를 고려한 CCF^{AC}, B와 C를 고려한 CCF^{BC}, A와 C를 고려한 CCF^{AB}, A와 B와 C를 모두 고려한 CCF^{ABC}를 모델에 반영하여야 하는 것이다. 일반 CCF 모델의 기본 원리와 같이, CCF^{AB}, CCF^{BC}, CCF^{AC}는 CCF^{ABC}에 해당하는 부품은 제외하고 계산하여야 한다.

마찬가지 방법으로 더 많은 수의 기종을 포함하는 계통에서 공통 부품을 고려한 CCF 모델을 작성할 수 있다.

제 5 장 결론

본 보고서에서는 디지털 계통의 특수성을 고려하여 그 CCF를 분석하기 위한 기본적인 방법론을 제시하였다. 본 보고서에서 다룬 디지털 기기의 특수성은 다음과 같이 정리될 수 있다.

– 매우 높은 수준의 다중성 부여
– 소프트웨어의 탑재로 인한 기능의 복잡성
– 특정 목적을 위한 고유 기기가 아닌 범용 기기 활용
– 이기종의 기기를 동일 기능수행에 적용

이러한 특성을 고려하여 기존의 PSA 방법에서 이용하던 CCF 분석방법론을 활용하여 고장수목을 작성하기 위하여 각 계통에 대한 기능 요구사항 및 물리적 배치 등을 체계적으로 분석하고 이를 이용하여 현실적으로 구현가능한 모델을 개발하였다.

높은 수준의 다중성을 갖춘 기기일수록 기존의 방법으로 모든 CCF를 기본사건화하여 모델을 구축할 경우 비현실적으로 거대한 모델이 되므로, 최대한 이론적인 값에 가까운 결과를 얻으면서도 현실적으로 모델링이 가능하도록 단순화 알파펙터 방법을 도입하였다.

기존의 아날로그 회로와는 달리 디지털 기기의 경우 안전기능 수행에 필수적인 부품은 기기내에서도 한정되어 있음을 고려하여, 이러한 부품의 용도에 맞는 고장율을 계산하여 CCF확률 산정에 이용할 수 있도록 방법론을 제시하였다.

이기종의 기기를 이용하여 CCF를 최소화하는 설계라 하여도 전자 부품의 모듈화와 대량생산으로 인해 일부 부품의 경우 공통적으로 사용되는 경우도 있다. 동일 기능을 수행한다는 것은 동일한 소프트웨어 로직을 공유한다는 뜻이므로 동일 부품을 사용할 경우 CCF에 노출되게 된다. 이러한 상황에 맞게 모델링할 수 있는 방법론을 제시하였다.

본 보고서의 연구는 KSNPP의 디지털 보호계통 안전성분석에서 CCF의 중

요성이 부각됨에따라 수행된 것이다. 디지털계통 특유의 복잡한 논리를 분석하고 안전기능에 필수적인 부품의 고장율만을 고려하여 보다 실제 값에 근접하면서도 보다 현실적인 CCF모델링이 가능한 방법을 제시하였다. 또한 KSNPP의 보호계통인 DPPS의 복잡한 기능을 분석하여 단순화 알파펙터 모델에 적용할 수 있도록 하였다.

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, '92 한국원자력학회 춘계학술발표회, 1992.

[4] 강현국 외, 신뢰도 상세분석: 표준원전 디지털원자로보호계통, KAERI/TR-2419/2003, 한국원자력연구소, 2003.

[5] 강현국 외, 신뢰도 상세분석: 표준원전 디지털공학적안전설비작동계통, KAERI/TR-2467/2003, 한국원자력연구소, 2003.

[6] Hyun Gook Kang and Taeyong Sung, "An analysis of safety-critical digital systems for risk-informed design," RESS, Vol. 78, 2002.

[7] 황미정 외, 공통원인고장 분석 지침, KAERI/TR-2444/2003, 한국원자력연구소, 2003.

[8] 한상훈, SMART-P의 PRHRS 설계에 대한 PSA 측면에서의 신뢰도 평가, Technical note, 미출판, 한국원자력연구소, 2004.

[9] Kang, H.G. and Jang, S.C. and Lim, H.G., ATWS Frequency Quantification Focusing on Digital I&C Failures, Journal of Korea Nuclear Society, Vol. 36, 2004.

<table>
<tr><td colspan="6">**서 지 정 보 양 식**</td></tr>
<tr><td colspan="2">**수행기관보고서번호**</td><td colspan="2">위탁기관보고서번호</td><td>표준보고서번호</td><td>INIS 주제코드</td></tr>
<tr><td colspan="2">KAERI/TR- 2908/2005</td><td colspan="2"></td><td></td><td></td></tr>
<tr><td colspan="2">제목 / 부제</td><td colspan="4">한국형표준원전 디지털 보호계통 공통원인고장 모델링에 관한 연구</td></tr>
<tr><td colspan="2">연구책임자 및 부서명
(AR,TR 경우 주저자)</td><td colspan="4">강현국 (종합안전평가부)</td></tr>
<tr><td colspan="2">연 구 자 및 부 서 명</td><td colspan="4">엄흥섭, 장승철, 하재주 (종합안전평가부)</td></tr>
<tr><td>출 판 지</td><td>대전</td><td>발행기관</td><td>한국원자력연구소</td><td>발행년</td><td>2005 년 2 월</td></tr>
<tr><td>페 이 지</td><td>77p.</td><td>도 표</td><td>있음(O), 없음( )</td><td>크 기</td><td>A4</td></tr>
<tr><td>참고사항</td><td colspan="5"></td></tr>
<tr><td>비밀여부</td><td colspan="2">공개(O), 대외비( ), __ 급비밀</td><td>보고서종류</td><td colspan="2">기술보고서</td></tr>
<tr><td>연구위탁기관</td><td colspan="2">과학기술부</td><td>계약 번호</td><td colspan="2"></td></tr>
<tr><td colspan="2">초록(15-20 줄 내외)</td><td colspan="4"></td></tr>
<tr><td colspan="6">본 연구는 디지털계통의 CCF 분석에서 중요한 요인중의 하나인 모델링 방법개발에 초점을 맞추었다. 즉, 기존의 확률론적안전성평가(PSA) 방법에서 이용하던 CCF 분석방법론을 활용하여 고장수목을 작성하기 위하여 각 계통에 대한 기능 요구사항 및 물리적 배치 등을 체계적으로 분석하고 이를 이용하여 현실적으로 구현가능한 모델을 개발하는 것이다.

최대한 이론적인 값에 가까운 결과를 얻으면서도 현실적으로 모델링이 가능하도록 단순화 알파펙터 방법을 도입하였으며, 디지털 계통의 특성인 멀티태스킹 기능 등을 고려하여, 한국형표준원전 보호계통의 복잡한 기능을 분석하여 단순화 알파펙터 모델에 적용할 수 있도록 하였다.

또한 기존의 아날로그 회로와는 달리 디지털 기기의 경우 안전기능 수행에 필수적인 부품은 기기 내에서도 한정되어 있음을 고려하여, 이러한 부품의 용도에 맞는 고장율을 계산하여 CCF 확률 산정에 이용할 수 있도록 방법론을 제시하였다. 즉, 소프트웨어 중의 안전기능 부분이 정상적으로 작동하는 상태에서 호출하는 부품만이 안전기능 수행에 필수적인 부품이므로 이러한 분석을 바탕으로 보다 현실적인 위험도를 계산할 수 있도록 하였다.

또한 이기종의 기기를 이용하여 동일 기능을 수행하도록 설계할 수도 있다. 동일 기능을 수행한다는 것은 동일한 소프트웨어 로직을 공유한다는 뜻이므로 만일 공통으로 부품을 사용한 부분이 있다면 이를 고려하여 CCF 모델을 수행하여야 한다. 본 보고서에서는 이러한 상황에 맞도록 방법론을 제시하였다.</td></tr>
<tr><td colspan="2">주제명 키워드
(10 단어내외)</td><td colspan="4">공통원인고장, 디지털 안전계통, 한국형 표준원전, 확률론적 안전성 평가, 위험도 정보 활용,</td></tr>
</table>

BIBLIOGRAPHIC INFORMATION SHEET			
Performing Org. Report No.	Sponsoring Org. Report No.	Standard Report No.	INIS Subject Code
KAERI/TR-2908/2005			

Title / Subtitle	The Common Cause Failure Probability Analysis on the Hardware of the Digital Protection System in Korean Standard Nuclear Power Plant
Main Author	H.G. Kang (Integrated Safety Assessment)
Researcher and Dept.	H.S. Eom, S.C. Jang, J.J. Ha (Integrated Safety Assessment)

Publication Place	Daejeon	Publisher	KAERI	Publication Date	2005.2
Page	77p.	Fig. & Tab.	Yes(O), No( )	Size	A4
Note					
Classified	Open(O), Restricted( ), ___ Class Document			Report Type	Technical Report
Sponsoring Org.	MOST			Contract No.	

Abstract (15-20 Lines)

The digitalized safety-signal generation system is designed based on the multiple-redundancy strategy which consists of more redundant components when we compare their number with those of conventional mechanical components. This research aims to develop the practical and realistic method for modeling the CCF in digital safety-critical systems. We apply the simplified alpha-factor method to the digital system CCF analysis. We also present the case study of the application of simplified alpha-factor method to the digital protection system of the Korean Standard Nuclear Power Plant.

The number of components in a digital module for performing the safety functions is smaller than the total number of components in a module. In consideration of safety function actuation, we must consider the safety-critical components only. In order to consider this situation in a more realistic manner, we have to analyze the module design and hardware-software interactions.

The different modules from different vendors could be used to perform the same safety function in order to reduce the CCF probability. The digital components, however, could be produced by the same vendor or the same process. This report also presents the method to cope with this situation.

Subject Keywords (About 10 words)	Common Cause Failure (CCF), Digital Safety-Critical System, Korean Standard Nuclear Power Plant (KSNPP), Probabilistic Safety Assessment (PSA), Risk-informed application (RIA)