'99 추계학술발표회 논문집
한국원자력학회

Success Path Alarm 설계를 위한 시스템 기능 분석 방법에 대한 연구

The Study of System Function Analysis Method for Success Path Alarm Design

강성곤*, 신영철

전력연구원
대전광역시 유성구 문지동 103-16

요 약

MMIS 설계는 발전소 주제어실 운전원에게 발전소의 정상/비정상시 운전을 수행하는데 있어서 필요한 정보와 제어 수단을 효율적으로 제공하는 설계를 목표로 한다. 특히 원자력 발전소 주제어실은 안전성과 신뢰성을 바탕으로 하여 발전소를 운영할 수 있도록 설계해야 하는데, 성공 경로(Success Path) 계통은 발전소에서 반드시 유지되어야 하는 필수 기능(Critical Function)들을 만족시키기 위해서 제공되어야 하는 시스템들로 정의 할 수가 있다. 성공 경로 감시 기능은 성공 경로 경보와 상태 정보로 나눌 수가 있다. 경보는 성공 경로 시스템이나 기기의 동작 상태와 이상 상태 정보를 통해 이상 유무를 감시한다. 상태 정보는 시스템이나 기기의 현재 상태를 표시하여 발전소의 운전 상황 판단에 도움을 주는 역할을 하고 있다. 성공 경로 계통의 경보와 상태 정보를 설계하고, 감시 범위를 결정하기 위해서는 시스템 기능 분석이 필수적이다. 이러한 시스템 기능 분석을 통해 도출된 정보들은 기기의 경보 상태와 운전 상태, 시스템의 성능 측정 지표인 대표 공정 변수들을 정의하는데 사용된다. 시스템 기능 분석 결과는 경보와 상태 처리 설계를 위한 자료로 사용되며, 시스템이 기동하는데 필요한 조건과 시스템이 정지해야 될 상태에 대한 정보를 가지고서 성공 경로 계통에 대한 시스템 경보를 설계 할 수가 있다. 본 논문에서는 성공 경로 시스템의 경보와 상태 정보들을 설계하기 위해 수행해야 하는 시스템 기능 분석 방법을 소개하고자 한다.

Abstract

The key benefit to the common use of the critical function approach for safety and mission functions is that monitoring methods expected to be used by operaotrs during emergency condition are used continuously during normal operation. For each critical

safety function there exists two or more success paths. Information Processing System monitors the availability, operation state and performance of the critical function success paths. In this paper, We have studied System Function Analysis(SFA) for the design of Success Path Alarm(SPA) for applying in KNGR. In here, we thought that SFA will help the design of SPA. The SFA can be applicable to the design of SPA according to NUREG-0711, also can induce the algorithm for alarm of system, train and flow path. We present a method of system function analysis for designing Success Path Alarm

1. 서 론

첨단 발전소 설계에서 주요한 흐름 중 하나는 기존에 운전원에 의해 수행되던 직무에 대해서 자동화가 이루어진다는 점이다. 자동화 기능이 증가한다는 것은 운전원이 손수 제어하던 제어기로부터 자동 제어기나 시스템 감시와 같이 운전원의 기능이 이양되는 결과를 의미한다. 이러한 역할 변화의 형태는 신뢰성 관점에서 본다면 긍정적으로 볼 수도 있다. 이러한 근거는 운전원이라는 요소는 시스템적인 관점에서 가장 예측 할 수 없는 요소 중 하나로 고려되고 있기 때문이다[1]. 자동화는 사람의 작업 행위의 필요성을 줄이거나 없애므로서 전체적인 시스템의 신뢰성을 높일 것으로도 판단된다[1]. 그러나 문제는 운전원 행위(Operator's performance)를 전체 시스템에서 필요한 구성 요소로 고려하지 않고, 가능한 기술력에만 근거로 하여 자동화된다는 점에 있다[1]. 이와 같은 점에 착안하여 시스템 기능 분석을 적절히 잘 수행해 본다면, 분석된 정보들로부터, 다양한 정보와 설계 방향을 제시 할 수 있을 것으로 생각된다. 또한 이러한 방법은 시스템의 상위 수준에서 하위 수준의 기기에 이르기까지 운전원의 감시 범위를 결정 할 수가 있다는 점이다.

2. Success Path Alarm 개념과 기본 구조

제어 가능성(Controllibility), 가용성(Availability), 성능(Performance)과 같은 정보를 이용하여 해당기기들과 시스템에 대한 이용 능력을 진단할 수가 있다. 특히 발전소의 필수 안전기능을 유지시키거나 회복시키기 위해서는 항상 성공 경로(Success Path) 시스템들에 대한 모든 상태 정보들이 감시되어야 한다[2]. 성공 경로 상태는 경로의 운전 상태와 운전원이나 제어/보호 시스템에 의해서 운전 상태가 변화될 수 있는 능력으로 판정 할 수가 있다. 이러한 정보는 운전원에게 성공 경로의 현재 사용 여부와 성공 경로 상태의 가용성이나 성능에 미치는 영향 여부를 인지하는데 있어서도 중요하다. 성공 경로 상태를 설정하기 위해서는 기기 수준의 정보가 조합되어 Sub-section, Flow path, Train System 수준의 정보로 만들어야 한다.

가) Composed Activity 알고리즘

최소한 하나의 Train이라도 Active하면, 그 시스템이 Active하다고 한다. 여러 Flow path 중 최소한 하나의 Flow path가 유량을 형성시켜 준다면, 그 Train은 Active하다고라고 정의한다. Flow path를 형성시키는 기기들이 Active 하다면 Flow path가 Active하다. Activity 알고리즘에서는 중요한 Manual valve의 상태도 Activity의 상태를 결정하기 위한 요소로 포함된다.

나) Composed Controllability 알고리즘

최소한 하나의 Train이 Active 하거나 Controllable 하다면, 그 시스템은 Controllable 하다라고 정의한다. 여러 Flow path 중 최소한 하나의 Flow path가 Controllable하거나 Active 하다면, 그 Train은 Controllable 하며, Flow path를 형성하는 기기들이 Controllable하거나, Active 하다면 Flow path가 Controllable 할 수 있다라고 정의한다.

다) Success Path Availability 알고리즘

이 알고리즘은 시스템에 속해 있는 각 CCS 기기의 Control과 Activity 상태와 중요한 Isolation 밸브와 같은 상태, Parameter Alarm 신호를 필요로 한다. 성공 경로 가용성은 EPG(Emergency Procedure Guidelines)에서 성공 경로로 정의된 시스템들에 대해서만 평가한다. 기기의 이상유무를 나타내는 Uncontrollability 경보, display symbol 속성에 포함된 시스템 Controllability 상태와 성공 경로 경보의 가용성 사이에는 구분이 되어야 한다. Controllability는 운전원이 시스템을 운전할 수 있는지, 배열 변화가 가능한지를 결정할 수가 있다. 가용성은 발전소의 비상절차 지침에서 제시된 최소 요건들을 만족시키기 위해 충분한 매개체들을 보유한 시스템이 적절하게 배열될 수 있는 여부를 결정하게 한다.

라) Success Path Performance 알고리즘

Success Path Performance 알고리즘에서는 주요한 기기의 Activity 상태와 성공 경로 성능을 결정할 parameter 경보 신호를 필요로 한다. 성공 경로를 구동하는 목적은 필수 기능을 회복하거나 유지하기 위한 것이기 때문에, 주제어실 운전원은 성공 경로의 성능의 만족 여부를 인지 할 필요가 있다. 운전의 Quality를 결정하기 위해서도 각 성공 경로의 성능을 평가하여 불만족스러운 상태로 검출될 경우 운전원에게 이를 경보로써 알려준다.

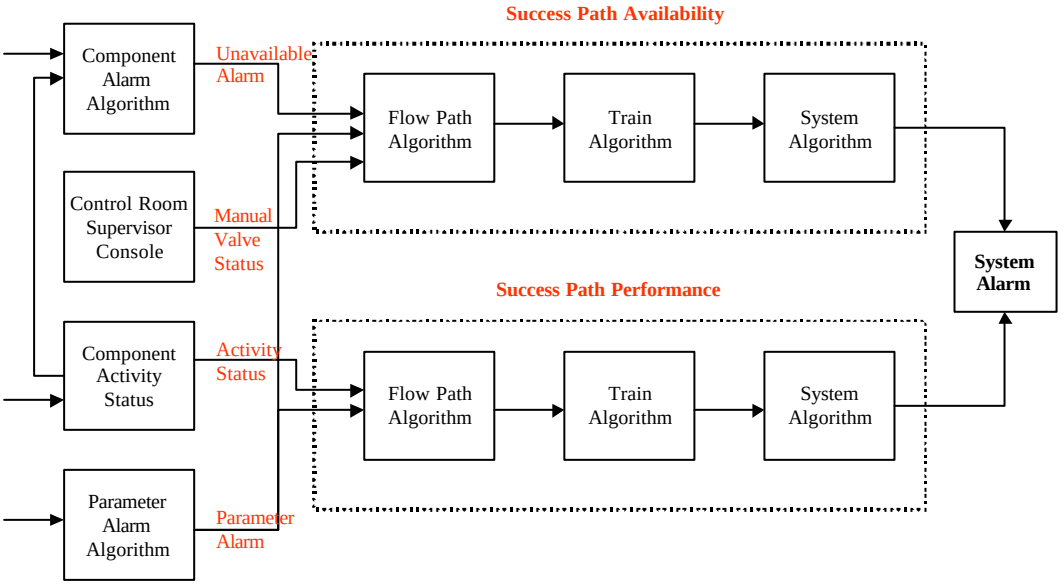

그림 1 성공 경로 시스템 경보 처리 알고리즘 흐름도

3. 시스템 기능 분석 방법

시스템을 분석하는 방법은 여러 가지 방법이 있을 수 있지만, 본 논문에서는 성공 경로 계통의 성격에 따라 시스템의 기능에 따라 분석하는 것을 원칙으로 한다. 각 기능마다 필요로 하는 기기들과 이 기기들을 포함하는 Flow path들과 Train들로 분석할 수가 있다. 각 Flow path는 몇 개의 Sub-section으로 구성되며, 이러한 Sub-section들은 기능과 관계없이 Flow path를 구성하기 위해 일정한 규칙에 따라 나눈 것이다. Flow path는 시스템의 한 기능이 수행되기 위해 필요한 기기들의 조합으로 정의한다. 이러한 Flow path는 Train내에서 한 기능을 담당하거나, 그 자체로 Train 기능을 할 수도 있다. Train이나 Flow path들이 기능에 따라 구성되어 System의 기능을 수행 할 수 있게 된다. 시스템의 기능을 수행 할 때도 시스템의 성능을 표시해 주는 대표적인 공정변수들이 필요하며, 성능 유지를 위해서는 기기의 상태들에 대한 감시도 항상 요구되고 있다. 시스템이 동작되지는 않지만, 언제든지 발전소의 안전 기능이 손상되었을 경우, 이를 회복해야 할 필요가 있는 경우를 대비해서 항상 시스템의 가용성 여부를 감시해야 한다. 이와 같은 필요성에 따라 성공 경로의 모든 시스템에 대해서 두 종류의 감시 기능을 주제어실에서 제공 할 수 있다. 시스템 기능 분석 방법에 따라 시스템의 감시 범위가 결정 될 수 있으며, SPA 설계를 위해 수행해야 할 시스템 기능 분석은 다음과 같다.

가) System Function Analysis(SFA)

- 계통 기능 구조 및 정보 분석(성공 경로 계통 기능 분석 포함)
- 시스템 상위 분석 : 기능에 근거한 Flow Path 분석에서 System까지의 분석
- 시스템 하위 분석 : 기능과 관계없이 Node/Branch 분석에 기초를 두어 Subection을 결정하는 과정

나) Subsection 결정 방법

- Subsection은 계통의 물리적 형상에 의해 결정되는 것으로 기능과 관계가 없다
- 전기계통인 경우는 Node Branch Analysis를 적용하며 각 Branch가 하나의 Subsection이 된다.
- 유체계통인 경우는 아래와 같이 Node와 Branch를 정의하고 각 Branch가 하나의 Subsection이 된다.
- 하나의 Branch 두개의 Node 사이에서, 아무리 길이가 길고 여러 개의 Component를 가진다 해도, 동일한 양의 Flow가 형성되는 단일 유로를 말한다.
- Node는 두개이상의 Branch가 만나는 동일한 압력을 가진 Cross-Section, Inlet Header, Outlet Header, Intake, Discharge또는 Tank 이다. 또한 Node는 단일 흐름이 복수개의 흐름으로 분리되는 점으로서 예는 Three-Way Valve이다.

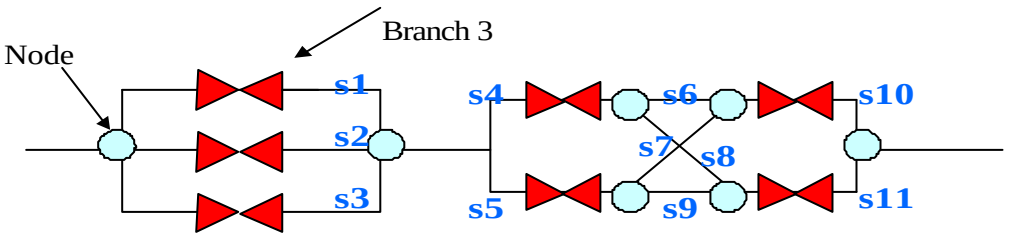

그림 2 Subsection 정의 개념도

다) Flow Path 결정 방법

- Flow Path는 기능과 관련 지을 때 결정되는 것임
- 어느 특정할 기능의 수행을 위하여 필요한 에너지나 유체Source로부터 Sink까지의 Subsection들의 직렬연결조합을 의미한다.
- Source는 어느 특정기능을 수행을 위해 필요한 에너지나 유체의 통상적인 재고를 가지는 Node를 의미한다.
- Sink는 어느 특정기능이 발휘되기 위해서 에너지나 유체의 주입/분출이 발생하는 Node를 말함.

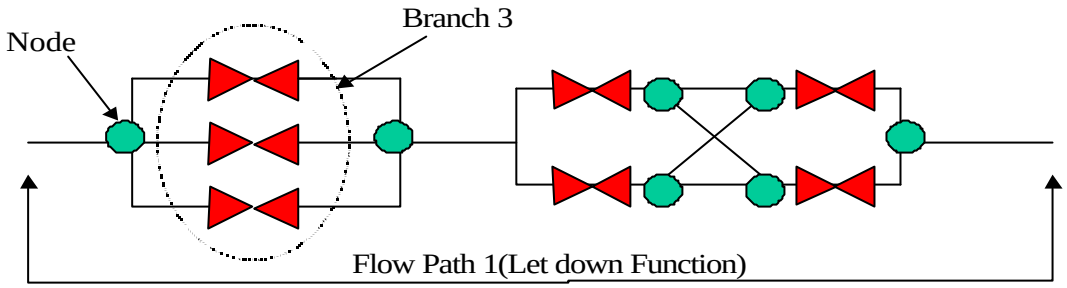

그림 3 Flow Path 정의 개념도

라) Success Path System 결정

- FRA(Functional Requirement Analysis)과 FA(Function Allocation) 설계에 의하여 결정되는 계통으로 필수 안전 기능을 회복 또는 유지시키는데 필요한 계통이다. 예를 들면 RCS Inventory Control을 위한 계통으로는 Safety Injection System, CVCS와 같은 계통이 해당될 수 있다.

마) 각 계통의 기능을 만족시키는데 필요한 조건

- 프로세스가 필요하다는 것을 알리는 조건
- 프로세스가 가용하다는 것을 알리는 변수
- 프로세스가 운전되고 있음을 알리는 변수(예, Flow indication)
- 프로세스가 목적을 이루고 있다는 것을 알리는 변수
- 프로세스의 운전이 멈출 수 있거나 멈추어야 한다는 것을 알리는 변수

4. 시스템 기능 분석을 통한 SPA 적용 방안

시스템 분석을 통해서 각 기능마다 적용될 성공 경로 계통의 기기들을 도출해 낼 수가 있다. 기기들을 제어하는 제어 계통에서 각 기기의 Activity와 Controllability의 신호를 계산하여 출력된다. 이렇게 출력된 신호들은 그림1에 기술된 것처럼 Component Alarm 알고리즘에서 비가용성 경보를 만들어내게 된다. 제안된 분석 방법에 따라 나누어진 Subsection과

Flow path, Train에 따라 각 기기들을 배치하여 연결하면, 해당 각 부분들의 경보들이 만들어진다. 계통의 기능이 만족되기 위한 조건들도 고려하여, 해당 계통의 가용성 감시와 성능 감시를 결정 지을 수 있게 한다. 다음은 Success Path 관련 기기들의 경보 종류와 경보 발생 조건을 나타낸 것이다.

Success Path 관련 기기 경보	기기 상태(CCS)	조건	Flow path 경보
Component Unavailable Alarm	Component Inoperable State	and	해당 기기가 속한 Flow path Unavailable Alarm
Component Uncontrollable Alarm	Component Inoperable State	and	해당 기기가 속한 Flow path Unavailable Not Alarm

표 1 Success Path 관련 기기 경보 정의

표1에서 나타낸 기기와 Flow path 경보는 시스템 경보에 영향을 미치며, 시스템 가용성 경보를 만들어 내는데 사용된다.

5. 결론

본 논문에서는 원자력 발전소의 운전원에 도움을 줄 수 있는 성공 경로 시스템의 설계를 위해 필수적으로 수행되어야 할 시스템 기능 분석 방안을 제시하였다. 이 분석은 기기의 분석과 기기와 연결된 각 Sub-section 그리고 기능의 의미가 포함된 Flow path, 시스템의 기능을 보유하면서 여러 Flow path의 연결을 통해 구성된 Train, 여러 Train으로 구성된 시스템으로 분석 할 수가 있었다. 물론 분석의 양이 많아질수록 시스템의 감시 범위는 더욱더 넓어질 수 있지만, 감시 범위가 넓어진다고 해서 운전원에게 효율적인 인지 범위가 될 수는 없다. 따라서 여기서 제시한 방법은 시스템을 분석하여, 성공 경로 시스템을 효율적으로 설계를 하기 위한 방법이다. 이러한 방법은 실제로 설계를 해나가면서 보완해야 될 부분을 찾아야 할 것이며, 필요하면 규칙의 수정도 필요하다고 생각된다. 성공 경로 감시 시스템의 기준이 가용성과 성능 진단 문제인 만큼 이를 얼마나 효과적으로 처리하여 표시하느냐 하는 것도 해결해야될 문제로 보고 있다. 따라서 차세대원전 주제어실 설계에서도 이와 같은 시스템 기능 분석 방법을 도입하여 성공 경로 시스템을 분석과 설계를 하면 성공 경로 경보의 처리 방법에 많은 도움이 될 것으로 판단된다.

참고문헌

1. "Computerized Diagnostic Aid-Success Path Monitor," EPRI NP-5088, March 1987
2. "Human Factors Engineering Program Review Model," NUREG-0711, 1994.
3. "The Experimental Evaluation of the Success Path Monitoring System - Results and Conclusions," OECD HWR-224, May, 1988
4. "The Experimental Evaluation of the Success Path Monitoring System - Design and

Methodology," OECD HWR-223, May, 1988

5. "The NORS Success Path Monitoring System - System Description and Implementation Experience," OECD HWR-222, May, 1988
6. "System Description for Critical Function and Success Path Monitoring in NUPLEX 80+," ABB-CE Rev 01, July, 1992.