

소방수 공급설비에 대한 공통원인고장을 고려한 확률론적 신뢰도 분석 Reliability Analysis on Firewater Supply Facilities based on the Probability Theory with Considering Common Cause Failures

고재선[†] · 김 호

Jae-Sun Ko[†] · Hyo Kim

서울시립대학교 화학공학과
(2003. 9. 4. 접수/2003. 12. 10. 채택)

요 약

본 논문에서는 공통원인고장의 이론적 고찰로서 정의와 그 원인, 분석방법을 기술하고 대표적인 소방설비의 하나인 소방펌프에 대해 공통원인고장을 고려한 신뢰도분석에 적용함으로써 공통원인고장의 중요성과 그 한계성을 규명하고자 한다. 공통원인고장을 고려한 소방수 공급설비에 대한 신뢰도분석 결과 알 수 있듯이 펌프의 운전고장이 계통실패의 가장 큰 요인으로 나타났으며 특히 두 펌프의 공통원인고장이 지배적이다. 다시 말하면 공통원인고장을 고려하지 않을 경우에 계통신뢰도를 실제보다 2배 이상 초과하여 평가할 수 있다는 것이다. 이로서 계통 신뢰도분석에서 공통원인고장의 중요성을 인식할 수 있으며 분석결과는 공통원인고장의 변수인자의 값에 크게 의존하는 것을 알 수 있다. 그리고 소방수 공급설비설비에 계통설계 시 다중성을 반영하면 신뢰도가 증가하는 것은 사실이나 공통원인고장 요인 때문에 다중기 설치대수에 비례하는 정도의 신뢰도 향상을 얻지 못할 수도 있다. 또한 공통원인고장의 한계성으로는 분석모델의 차이로 인한 차이는 미미한 수준이었으나 각각 다른 데이터 원을 사용했을 경우 그 결과는 큰 차이를 나타내었다. 따라서 공통원인고장 분석에 사용되는 모델보다는 이용 가능한 경험데이터의 품질이 그 분석결과와의 신뢰성에 큰 영향을 미친다는 것을 알 수 있었다. 결과적으로 다중기기의 공통원인고장을 방지하기 위한 기본적인 공학적인 방안으로는 설계시 요구되는 적정 신뢰도를 유지하는 것이므로 적어도 소방펌프에 요구되는 신뢰도수준으로 설계되어야 한다. 즉 SIS(Safety Instrumented system)에 요구되는 신뢰도수준인 안전건전성수준(SIL: Safety integrity level)에 적합한가의 유무를 PFD를 활용하여 정량적으로 파악하는 것이다. 공통원인고장을 고려한 소방수 공급설비에 대한 신뢰도분석 결과 계통작동요구시 실패확률(PFD: Probability of failure on demand), 즉 계통 이용 불능도는 3.80E-3이므로 규정목표인 SIL5의 범주 안에 들어있지 않아 안전건전성수준으로 설계되어 있지 않다고 판단되며, 만일 공통원인고장을 고려하지 않았을 경우인 계통 이용불능도 또한 1.82E-3으로 계산되는데, 이 또한 SIL5의 범주 안에 들어있지 않으므로 안전건전성수준으로 설계되어 있지 않다고 판단된다.

ABSTRACT

In this study, we write down the definitions, their causes and the techniques of analysis as a theoretical consideration of common cause failures, and investigate the limitation and the importance of the common cause failures by applying to the analysis on the fire protection as a representative safety facility. As you can know in the reliability analysis, most impressive cause is the malfunctions of pumping operations; especially the common cause failure of two pumps is dominant. In other words, it is possible to assess system-reliability as twice as actual without CCF. From these, CCF is extraordinarily important and the results are highly dependent on the CCF factor. And although it would increase with multiple installations, the reliability are not defined as linear with those multiplications. In addition, the differences in results due to the models for analysis are not significant, whereas the various sources of data produce highly different results.

[†]E-mail: 119kjs@hanmail.net

Therefore, we conclude that the reliabilities are dependent on the quality of the usable data much better than the variety of models. As a result, the basic and engineering device for the preventions of CCF of the multiple facilities is to design it as reliably as to design the fire-water pump. That is to say, we must assess those reliabilities using PFD whether they are appropriate to SIL (Safety Integrity Level) which is required for the reliability in SIS (Safety Instrumented System). The result of the analysis on the reliability of the fire-water supply with CCF shows that PFD is $3.80E-3$, so that it cannot be said to be designed as safely as in the level of SIL5. However, without CCF, PFD is $1.82E-3$ which means that they are designed as unsafely as before.

Keywords : Common cause failure, Independent failure probability, Functional dependency, Parametric model, Safety Integrity Level, Probability of failure on demand

1. 서 론

1.1 연구배경 및 목적

가연성물질을 대량으로 취급하는 화학공장, 가스시설, 발전소 등에서는 누출사고와 이로 인한 화재 및 폭발사고를 방지하거나 영향을 최소화 하기 위하여 각종 방재설비를 구비하고 있다. 특히 방재설비 중에서 소방설비는 사고발생시 사고현장 전면에서 성능을 발휘하여야 하는 사고 진압에 가장 필수적인 안전설비이다. 소방설비는 플랜트의 정상운전 중에는 대기상태에 있다가 가연성물질의 누출사고 및 이로 인한 화재가 발생하였을 때 성공적으로 기능을 수행할 수 있어야 한다. 따라서 소방설비 설계에서는 설비작동이 성공적으로 작동될 가능성, 즉 신뢰성이 가장 중요한 요소가 된다. 또한 일반적으로 소방수 공급펌프 등 소방설비의 주요 기기에 대해서 필수 대수 이상의 기기를 병렬로 설치함으로써 소방설비의 신뢰성을 보장하기 위한 방향으로 설계하고 있다. 그러나 동일한 기능을 갖는 동일한 형태의 기기를 다중으로 설치하면 시스템의 신뢰도는 증가하나 그 증가 정도가 반드시 설치대수에 비례하지는 않는다. 그 이유는 다중으로 설치된 두 대 이상의 기기가 동일한 원인으로 인하여 동시에 작동불능상태가 될 가능성이 있기 때문이다. 따라서 본 연구의 목적은 공정안전과 관련하여 각종 방재설비 중 소방수 공급설비에 대해 공통원인고장(Common Cause

Failure : CFC)를 고려한 정량화된 신뢰도 분석을 통해 개인, 장치설비 및 주위 인근의 지역사회에 미치는 공정관련 산업재해 및 사고를 예방하려는데 그 목적이 있다.

1.2 연구 방법

본 연구에서는 분석대상설비인 “천연가스 처리공장 시설의 소방수공급설비”의 엔지니어링 문서, 즉 대상설비에 대한 도면, 설명서, 절차서 등을 검토 함으로서 설비의 설계 및 운영상황을 파악하고, 분석 목적인 공통원인고장으로 인한 설비 작동 시 실패할 가능성을 추정하기 위해 계통논리모델인 고장수목(fault tree)과 공통원인고장을 분석하는 매개변수모델(parametric model)인 Beta모델과 연결시켜 계통신뢰도를 정량화한 후 SIS(Safety Instrumented system)에 요구되는 목표 신뢰도수준인 즉 안전전전성수준(SIL:Target Safety integrity level)에 적합성을 판단할 수 있는 공학적인 방안 및 전반적인 대책을 마련하고자 한다.

2. 공통원인고장의 이론적 고찰

2.1 공통원인고장의 정의

두 대 이상의 동일한 형태의 다중기기가 동일한 원인으로 동시에 고장이 발생하는 사건을 공통원인고장(Common Cause Failure: CCF)이라 하며 인적 오류와

Table 1. Requirements of common cause failures^{1,2)}

조건	내용	성립 예	불 성립의 예
동일기능	동일한 기능을 가진 기기이어야 함	소방펌프들의 고장	소방펌프/재순환 펌프 고장
동일형태	동일한 형태의 기기여야 함	전동펌프들의 고장	전동펌프/엔진펌프의 고장
다중기기	두 대 이상의 다중기기이어야 함	두 대 이상의 병렬로 설치된 경우	두 대의 기기가 직렬로 설치된 경우
동일원인	고장의 원인이 동일하여야 함	두 대 이상의 펌프가 과도한 진동으로 고장	하나는 과전동, 다른 하나는 과열인 경우
동시고장	시간적으로 거의 동시에 발생해야 함	두 대의 펌프가 동시에 작동 불량	하나는 지난해에, 다른 하나는 올해에 고장

Table 2. Basic classifications of common cause failures^{1,2)}

Classifications	Causes
Functional dependency	두 대 이상의 기기가 주어진 기능을 완수하기 위해서 동일한 보조설비(supporting system)가 필요한 경우 해당 보조설비의 기능이 상실되면 그 설비의 지원을 받는 모든 기기가 이용 불능 상태가 된다. 이러한 경우 다중기기가 동일한 보조설비에 대해서 서로 기능적 의존성을 갖고 있다고 말함.
Human factors	플랜트 정상운전 중의 작동실수, 기기시험 또는 보수 중의 실수, 그리고 설계, 제작, 시공상의 오류 등 어느 한 가지 인간실수로 인해 여러 기기가 동시에 이용 불능하게 될 가능성이 있음.
External factors	외부로부터의 스트레스 또는 충격의 예로서는 온도, 압력 등 운전조건이 매우 열악하여 과도한 운전환경이 부과되는 경우와 지진, 태풍, 홍수 그리고 인접시설에서의 사고영향 등이 있음.

함께 시스템의 신뢰도에 가장 큰 영향을 미치는 요인으로 알려져 있다.

2.2 공통원인고장의 성립조건

공통원인고장이란 다음의 Table 1의 다섯 가지 요소를 모두 만족할 경우에만 공통원인고장이 성립되며 하나의 조건이라도 이에 해당되지 않으면 공통원인고장을 고려할 필요가 없다.

2.3 공통원인고장의 원인

Table 2은 공통원인고장의 원인으로 비교적 용이하게 파악할 수 있도록 정리한 것으로 크게 3가지 경우인 기능적 의존성, 인적 오류, 외부적 요인으로 분류할 수 있다.

2.4 공통원인고장 분석절차¹⁾

공통원인고장을 분석하는 절차는 Fig. 1과 같다. 계

통논리 수립단계에서는 먼저 대상설비에 대한 도면, 설명서, 절차서 등 엔지니어링 문서를 검토함으로써 설비의 설계 및 운영 상황을 파악하고, 분석하고자 하는 목적에 따라 논리모델을 구축한다. 공통원인고장의 그룹 선별단계에서는 설비를 구성하는 모든 기기를 검토하여 Table 1의 공통원인고장의 성립조건에 해당하는 다중기기를 파악하고, 이들 공통원인고장 그룹 중에서 발생 가능성이 높은 그룹만 선별한다. 이렇게 선별된 그룹에 대해서는 분석모델링 단계로 진행한다.

2.5 공통원인고장 분석모델²⁾

본 연구에서 적용된 공통원인고장을 분석하는 모델은 Table 3과 같이 일반적으로 매개변수모델(parametric model)인 베타모델을 이용하는데, 공통원인고장 그룹에 대한 매개변수 모델분석의 결과를 계통 논리모델과 연결시켜 신뢰성에 영향을 미치는 다른 원인들과 함께 계통신뢰도를 정량화하고 모델 및 데이터에 대한 민감



Fig. 1. Procedures of analysis on common cause failures.

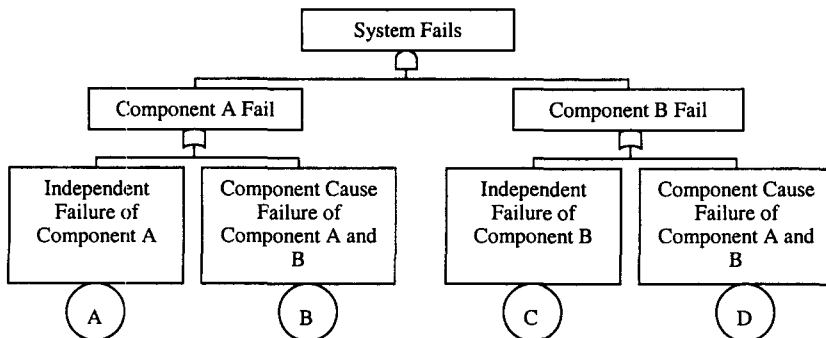


Fig. 2. Simple example of fault-tree analysis with common cause failures.

도 분석 및 중요도 분석을 수행함으로써 정량화 결과를 해석한다. 이에 따라 공통원인고장을 비롯한 계통 신뢰도 저해요인을 파악하고 신뢰도 수준을 향상시키기 위한 공학적 방안을 제시할 수 있다. 공통원인고장을 고려한 계통 고장수목의 간단한 예는 Fig. 2와 같다.

Fig. 2와 같이 계통신뢰도 모델에 다중기기의 공통원인고장에 관한 기본사건(basic event)을 각 기기의 고장원인의 하나로 독립적 고장(independent failure)의 기본사건과 함께 고려한다. 일단 계통모델에서 독립적 고장과 공통원인고장에 관한 기본사건이 정의되면 정량적으로 평가하여야 하는 매개변수의 수를 줄이기 위하여 대칭성(symmetry)을 가정하는 데 이는 동일한 대수의 고장을 의미하는 기본 사건들의 발생확률은 서로 같다고 가정하는 것이다. 예를 들면 A, B, C, 3대의 기기가 있다고 할 때

$$P(A_i) = P(B_i) = P(C_i) = Q_i, \\ P(C_{AB}) = P(C_{AC}) = P(C_{BC}) = Q_2, \quad P(C_{ABC}) = Q_3$$

라고 가정한다. 여기서 $P(A_i)$, $P(B_i)$, $P(C_i)$ 는 A, B, C 각각의 독립적 고장으로, 그 발생확률은 Q_1 으로 정의하였고, $P(C_{AB})$, $P(C_{AC})$, $P(C_{BC})$ 는 3대 중에 2대 즉, 각각 A와 B, A와 C, B와 C가 공통원인고장으로 실패하는 것으로 그 발생확률을 Q_2 로 정의한 것이다.

일반적으로 k대의 기기가 동시에 실패하는 공통원인 고장 기본사건의 발생확률 Q_k 를 추정하기 위한 매개변수모델로는 Basic parameter, Multiple Greek letters, Alpha factor, Binomial failure rate 등 여러 가지 매개변수모델이 개발되어 있는데 그 중 본 연구에서 사용한 계통 신뢰도분석모델인 베타모델(Beta factor model)의 주요특성과 일반식을 간단히 요약한 것이 Table 3이다. 또한 Beta factor model은 그 적용이 다른 모델에 비해 단순하기 때문에 신뢰성 및 안전성분석에 주로 사용 하는 모델로서, 이 모델에서 필요

한 데이터는 기기의 총 고장확률데이터(Q_i)와 공통원인고장분율(β)이 전부이며 공통원인고장을 고려하기 위해 필요한 매개변수가 하나 이므로 단일변수(single parameter)이라고도 한다.

3. 사례를 통한 공통원인고장의 신뢰도 분석

앞서 기술한 바와 같이 대표적인 안전설비인 “소방수 공급설비에 대해 다중기기의 공통원인고장을 고려한 신뢰도분석”을 수행한 예를 제시함으로써 이에 따른 공통원인고장의 중요성과 한계성 등을 규명하고자 한다.

3.1 소방수 공급설비의 구성

선정된 소방수 공급설비는 천연가스 처리공장의 시설로서 설비 단순도는 Fig. 3과 같다. 본 소방수 공급계통은 1개의 소방수 저장탱크와 3대의 소방수 공급펌프로 구성되어 있으며 1대(P-73)는 30 m³/hr의 용량을 갖는 진동 충압 펌프(jockey pump)로서 가스처리공장의 정상운전 시 소방수 환상 망의 배관 내 압력을 10 kg/cm²로 유지 시켜주는 역할을 한다. 실제로 공장 내 가스누출 및 화재발생시 진압을 위하여 사용되는 소방수 공급펌프는 340 m³/hr의 용량을 갖는 P-71A와 P-71B로서 엔진펌프 2대가 설치되어 있고, 정상운전 시 대기상태(standby)에 있다가 작동 요구 시 기동하여 소방수를 공급하도록 되어 있다. 공장 내 최악의 화재 발생시 8시간의 진압시간을 기준으로 설계되어 있고, 필요 소방수 유량은 330 m³/hr으로 계산되어 있다. 따라서 2대 중 한대의 펌프만 성공하면 되는 동일기능의 동일펌프 2대의 다중성을 갖고 있으며 소방수 저장탱크는 펌프 1대의 8시간 작동 분의 소방수(340 m³/hr* 8 hr = 2,720 m³)를 저장하고 있다.

Table 3. Properties to Beta factor model²⁾

매개변수 모델	Beta factor model
주요특성	기기고장데이터의 일정부분이 그룹 내 다른 기기와의 공통원인 고장에 해당되며, 일단 공통원인이 발생하면 그룹내의 모든 기기가 실패한다는 가정
일반식	$Q_1 = (1 - \beta)Q_i, \quad Q_m = \beta Q_i$ 위의 두 가지 관계에서 $\beta = Q_m / (Q_1 + Q_m)$ 으로 정의. 예) 한 기기의 총 고장확률은 $Q_i = Q_1 + Q_m$

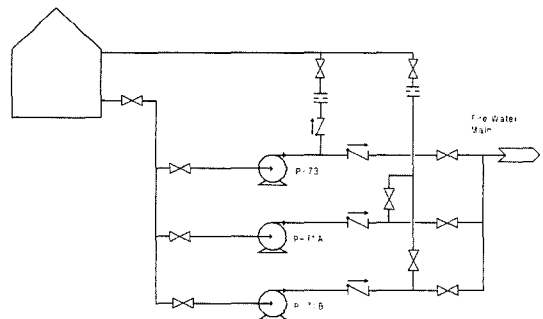


Fig. 3. Simple draft of fire protection water supply facility.

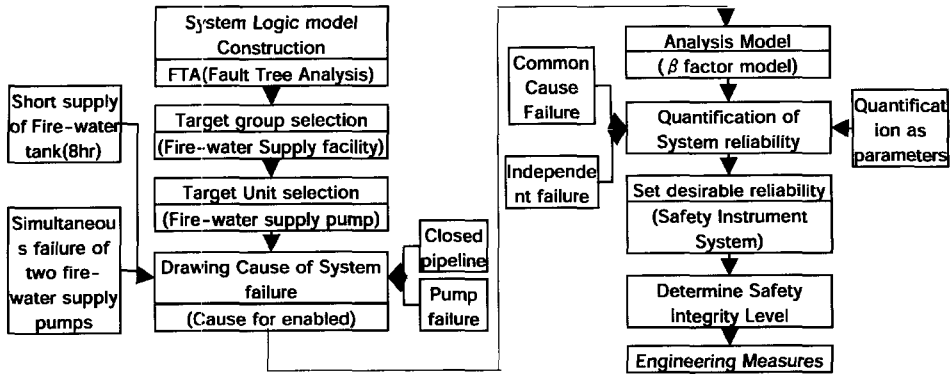


Fig. 4. The Flowchart of study in example for fire water supply facility.

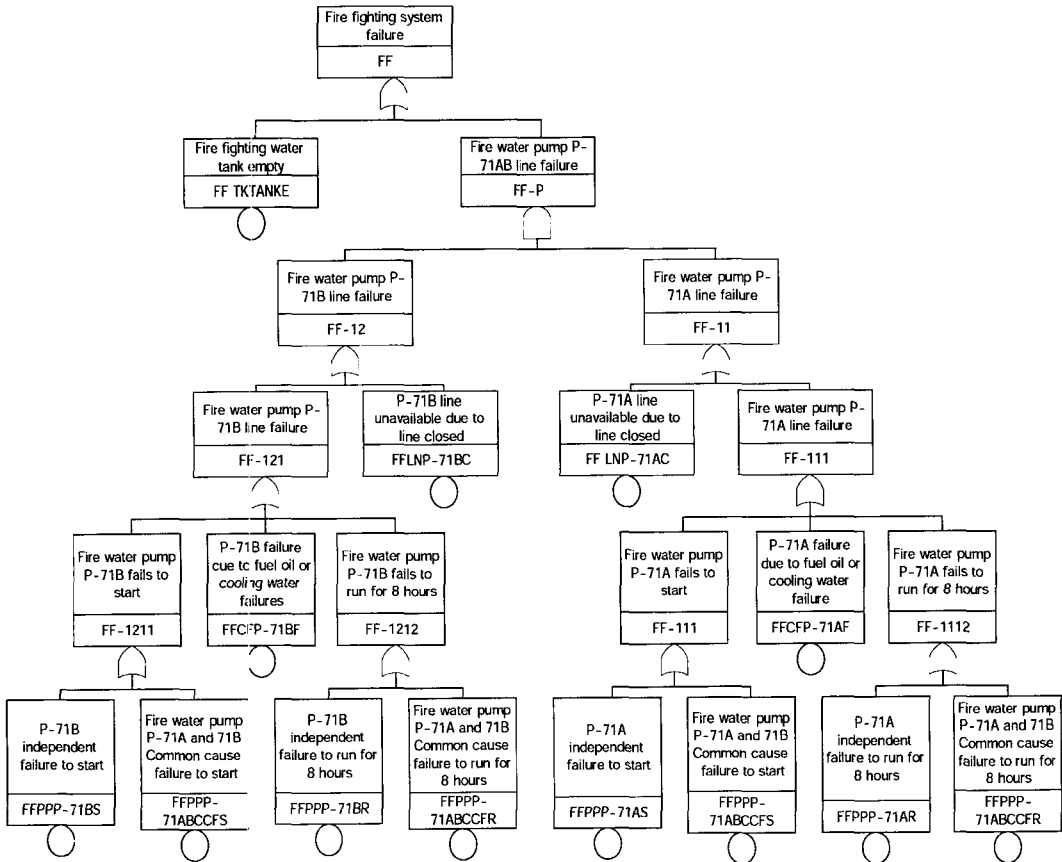


Fig. 5. Reliability fault tree analysis of fire protection water supply facility.

3.2 소방수 공급설비에 대한 공통원인고장을 고려한 신뢰도 분석

3.2.1 소방수 공급설비의 고장수목 구성²⁾

소방수 공급설비 작동요구시 작동실패확률을 구하기 위한 고장수목을 구성하면 Fig. 5와 같다. 본 고장수목

을 작성하기 위한 계통 성공기준은 2대 중 1대의 펌프가 기동되어 8시간 동안 소방수를 공급해야 한다는 것이다. 계통 실패의 원인으로서는 소방수 저장탱크의 저장량이 8시간의 화재진압에 충분치 못한 경우와 2개의 소방수 공급펌프 라인이 동시에 실패하는 경우가

Table 4. Basic data of fault tree^{4,5-8)}

Name	Mean	Description
FFTKANKE	1.00E-04	Fire fighting water tank empty
FFPPP-7!AR	1.71E-02	P-71A independent failure to run for 8 hours
FFPPP-7!BR	1.71E-02	P-71B independent failure to run for 8 hours
FFPPP-7!AS	2.25E-03	P-71A independent failure to start
FFPPP-71BS	2.25E-03	P-71B independent failure to start
FFPPP-71ABCCFS	2.50E-04	Fire water pump P-71A and 71B common cause failure to start
FFPPP-71ABCCFR	1.90E-03	Fire water pump P-71A and 71B common cause failure to run for 8 hours
FFLNP-71AC	1.00E-02	P-71A line unavailable due to line closed
FFLNP-71BC	1.00E-02	P-71B line unavailable due to line closed
FFCFP-71AF	1.00E-02	P-71A line unavailable due to fuel oil or cooling water failure
FFCFP-71BF	1.00E-02	P-71B line unavailable due to fuel oil or cooling water failure

있다. 계통 실패의 원인으로서 소방수 저장탱크의 저장량이 8시간의 화재진압에 충분치 못한 경우와 2개의 소방수 공급펌프 라인이 동시에 실패하는 경우가 있다. 각 공급라인의 실패는 배관상에 위치하는 기기의 막힘 상태로 인한 이용불능과 펌프 자체의 고장이 있을 수 있다. 펌프 자체의 고장은 연료유 또는 냉각수 공급기능 실패의 경우와 펌프의 기동실패(fails to start) 및 지속운전실패(fails to run)의 고장모드가 있다. Fig. 5의 고장수목에서 소방펌프의 기동실패와 지속운전 실패의 두 가지 고장모드에 대해서 공통원인고장 기본사건(FFPPP-71ABCCFS, FFPPP-71ABCCFR)을 고려하였다.

3.2.2 데이터 분석

소방설비 신뢰도 고장수목에 고려된 기본사건의 데이터를 구하기 위하여 OREDA(Offshore Reliability Data Handbook, 3rd Edition, 1997)를 참고 하였다. 이는 가스처리 시설에 대한 신뢰성 있는 기기 고장률 데이터로서 널리 사용되는 데이터베이스이다.⁴⁾ 이 데이터베이스에서 구할 수 없는 데이터는 유사 관련 데이터 복인 "IEEE Guide Handbook("Sensing Component, and Mechanical Equipment Reliability Data for Nuclear Power Generating Stations," 1993), CCPS ("Guidelines for Process Equipment Reliability Data", 1989) 등을 참고하여 공학적 판단을 적용하여 추정하였다. 고장수목 기본사건의 목록과 그 데이터를 정리 하면 Table 4과 같다.

또한 펌프고장에 관한 공통원인고장 기본사건의 데이터를 추정하기 위하여 beta인자 모델을 사용하였다. 소방펌프의 공통 원인 고장에 대한 인자로서 일반 데

Table 5. The probabilities of common cause failures & independent failures with the OREDA data

매개변수모델	OREDA Data	
β Parameter model (β factor=0.1)	펌프시동실패확률	8 hr지속운전실패
	2.50E-3	1.90E-2
	공통원인고장확률(CCF)	
	2.50E-4	1.90E-3
	독립고장확률	
	2.25E-3	1.71E-2

이터인 0.1을 사용하였다. 즉 OREDA의 데이터에 따른 펌프 시동 실패확률인 2.50E-3과 8시간 지속운전 실패확률인 1.90E-2에 각각 0.1의 인자를 적용하여 2.50E-4와 1.90E-3의 공통원인고장 확률을 각각 사용한다. 그리고 독립고장 확률은 이므로 각각 2.25E-3, 1.71E-2가 된다.

3.2.3 Beta Factor 모델을 통한 신뢰도 정량화

소방설비 신뢰도 고장수목에 기본사건의 데이터를 입력하여 설비 작동실패에 관한 최소단절집합(minimal cut set)을 도출하고 계통신뢰도를 구하면 Table 6와 같다. 정량화 작업은 한국원자력연구소에서 개발한 정량분석코드인 KIRAP-KWT REE(Fault Tree Editor for Windows, 1996)을 사용하여 수행하였다.

3.3 결과 및 고찰

3.3.1 신뢰도 분석 결과

Table 7에서 공통원인고장을 고려한 소방수 공급설비에 대한 신뢰도분석 결과 계통자동요구시 실패확률,

Table 6. Results of Reliability analysis

NO	Value	F-V	Cumulative	Cutset	
1	1.90E-03	0.5002	0.5002	FFPPP-71ABCCFR	-
2	2.92E-04	0.0700	0.5772	FFPPP-71AR	FFPPP-71BR
3	2.50E-04	0.0658	0.6430	FFPPP-71ABCCFS	-
4	1.71E-04	0.0450	0.6880	FFLNP-71BC	FFPPP-71AR
5	1.71E-04	0.0450	0.7330	FFLNP-71AC	FFPPP-71BR
6	1.71E-04	0.0450	0.7781	FFCFP-71BF	FFPPP-71AR
7	1.71E-04	0.0450	0.8231	FFCFP-71AF	FFPPP-71BR
8	1.00E-04	0.0263	0.8494	FFTKTANKE	-
9	1.00E-04	0.0263	0.8757	FFLNP-71AC	FFCFP-71BF
10	1.00E-04	0.0263	0.9021	FFCFP-71AF	FFLNP-71BC
11	1.00E-04	0.0263	0.9284	FFCFP-71AF	FFCFP-71BF
12	1.00E-04	0.0263	0.9547	FFLNP-71AC	FFLNP-71BC
13	3.85E-05	0.0101	0.9648	FFPPP-71AS	FFPPP-71BR
14	3.85E-05	0.0101	0.9750	FFPPP-71AR	FFPPP-71BS
15	2.25E-05	0.0059	0.9809	FFCFP-71AF	FFPPP-71BS
16	2.25E-05	0.0059	0.9868	FFLNP-71BC	FFPPP-71AS
17	2.25E-05	0.0059	0.9927	FFLNP-71AC	FFPPP-71BS
18	2.25E-05	0.0059	0.9987	FFCFP-71BF	FFPPP-71AS
19	5.06E-06	0.0013	1.0000	FFPPP-71AS	FFPPP-71BS
Sum	3.80E-03	-	-	-	-

F-V : Fussell-Vesely 중요도(해당 기본사건이 포함되는 모든 최소단절군 빈도의 합과 전체 빈도의 비로 정의)

Table 7. The failure probabilities on system operation demand

구 분	이용불능도(PFD)	
	CCF고려 함	CCF고려치 않음
계통작동요구시 실패확률		
2EA(Engine pump)	3.80E-3	1.82E-2
1EA(Engine pump)	4.16E-2	

즉 계통 이용 불능도는 3.80E-3으로 나타났는데 이는 260번의 요구에 한 번 정도 실패할 수 있다는 의미이다. 또한 Table 6에서 알 수 있듯이 펌프의 운전고장이 계통실패의 가장 큰 요인으로 나타났으며 특히 두 펌프의 공통원인고장이 지배적이다. 만일 Table 7에서 공통원인고장을 고려하지 않을 경우에는 계통 이용불능도가 1.82E-3으로 계산되는데 이는 공통원인고장을 고려한 경우에 비해 1/2에도 미치지 못한다. 다시 말하면 공통원인고장을 고려하지 않을 경우에 계통신뢰도를 실제보다 2배 이상 초과하여 평가할 수 있다는

것이다. 이로서 계통 신뢰도분석에서 공통원인고장의 중요성을 인식할 수 있으며, 분석결과로서 Table 8은 초기 기기 고장을 값을 이용하여 분석모델링인 베타모델의 인자값을 달리하여 최종 고장모드인 “펌프시동실패” 및 8 hr “지속운전실패”에 대하여 공통원인고장 및 독립고장을 일으킬 전체 확률치를 계산한 결과이며 변수인자의 값에 크게 의존하는 것을 알 수 있다.

그리고 소방수 공급설비설비에 다중성을 반영하지 않고 1대의 소방펌프만 설치했을 경우에는 계통 이용불능도가 4.16E-2으로 계산된다. 따라서 Table 9와 Fig. 6과 같이 계통설계 시 다중성을 반영하면 신뢰도가 증가하는 것(이용율이 증가)은 사실이나 공통원인고장 요인 때문에 다중기기 설치대수에 비례하는 정도의 신뢰도 향상을 얻지 못할 수도 있다.

3.3.2 공통원인고장에 있어서 신뢰도 분석시 한계성
공통원인고장은 매우 희소한 사건으로서 일반적으로 플랜트 고유의 특성에 의해 발생한다. 플랜트의 수명 기간 동안 관측되는 공통원인고장의 수는 극히 적거나

Table 8. The whole-range probabilities of common cause failures & independent failures with β factors

β factor model	초기 Data		초기 Data	
	펌프시동실패	8 hr 지속 운전실패	펌프시동실패	8 hr 지속 운전실패
	2.50E-03	1.90E-02	2.50E-03	1.90E-02
β values	공통원인 고장 확률		독립 고장 확률	
0.05	1.25E-04	9.50E-04	2.38E-03	1.81E-02
0.065	1.63E-04	1.24E-03	2.34E-03	1.78E-02
0.08	2.00E-04	1.52E-03	2.30E-03	1.75E-02
0.095	2.38E-04	1.81E-03	2.26E-03	1.72E-02
0.1	2.50E-04	1.90E-03	2.25E-03	1.71E-02
0.11	2.75E-04	2.09E-03	2.23E-03	1.69E-02
0.125	3.13E-04	2.38E-03	2.19E-03	1.66E-02
0.14	3.50E-04	2.66E-03	2.15E-03	1.63E-02
0.155	3.88E-04	2.95E-03	2.11E-03	1.61E-02
0.17	4.25E-04	3.23E-03	2.08E-03	1.58E-02
0.185	4.63E-04	3.52E-03	2.04E-03	1.55E-02
0.2	5.00E-04	3.80E-03	2.00E-03	1.52E-02

Table 9. PFD & PSD[†] as the increasing number of pumps

펌프 개수	이용불능도 (PFD)		이용율 (1-PFD)	
	CCF고려	CCF비고려	CCF고려	CCF비고려
1	3.80E-3	4.16E-2	9.58E-1	9.96E-1
2	7.59E-3	8.15E-2	9.19E-1	9.92E-1
3	1.14E-2	1.20E-1	8.80E-1	9.89E-1
4	1.51E-2	1.56E-1	8.44E-1	9.85E-1
5	1.89E-2	1.91E-1	8.09E-1	9.81E-1
6	2.26E-2	2.25E-1	7.75E-1	9.77E-1
7	2.63E-2	2.57E-1	7.43E-1	9.74E-1
8	3.00E-2	2.88E-1	7.12E-1	9.70E-1
9	3.37E-2	3.18E-1	6.82E-1	9.66E-1
10	3.74E-2	3.46E-1	6.54E-1	9.63E-1

[†]PSD: Probability of Success on Demand(=1-PFD)

전혀 관측되지 않는 경우가 많으며 실제 발생한 공통원인고장의 원인을 분석해 보면 대부분 플랜트 고유의 설계 및 운영특성에 기인하는 것으로 나타나고 있다. 따라서 공통원인고장의 경험 데이터의 수가 극히 적고, 통계적 처리에 부적합할 경우, 이러한 문제점을 해결하기 위해 의사고유분석(pseudo-specific analysis) 방법론을 사용하는데, 이 방법은 타 플랜트의 특성 및 유

사 데이터 복에 비추어 재해석하고 이에 근거하여 공통원인고장 데이터를 도출하는 방법으로 이러한 분석을 위해서는 공통원인고장 경험 데이터에 대한 상세한 검토를 필요로 한다. 이러한 공통원인고장분석방법론에 대한 Benchmark시험이 수행된 바 있다. 이 시험에서는 몇의 팀이 동일한 계통에 대해 각각 다른 모델을 사용했을 때와 각각 다른 데이터 원(sources)을 사용하였을 때의 분석 결과를 비교 검토한 결과 분석모델의 차이로 인한 차이는 미미한 수준이었으나 각각 다른 데이터원(source)을 사용했을 경우 그 결과는 큰 차이를 나타내었다. 따라서 공통원인고장 분석에 사용되는 모델보다는 이용 가능한 경험데이터의 품질이 그 분석 결과의 신뢰성에 큰 영향을 미친다는 것을 알 수 있다.

3.3.3 신뢰도 분석결과에 따른 공통원인고장에 대한 공학적인 방안

다중기기의 공통원인고장을 방지하기 위한 공학적인 방안으로는 설계시 요구되는 적정 신뢰도를 유지하는 것이므로 적어도 소방펌프에 요구되는 신뢰도수준으로 설계되어야 한다. SIS(Safety Instrumented system)에 요구되는 신뢰도수준은 일반적으로 안전건전성수준(SIL : Target Safety integrity level)으로 표현되는데, 이는 작동 요구 시 실패확률(PFD : Probability of failure on demand)에 대한 구간을 의미한다. PFD와 SIL의 관계는 “ISA-84.01: Application of Safety Instrumented Systems for the Process Industries(1996)”와 “ICE-

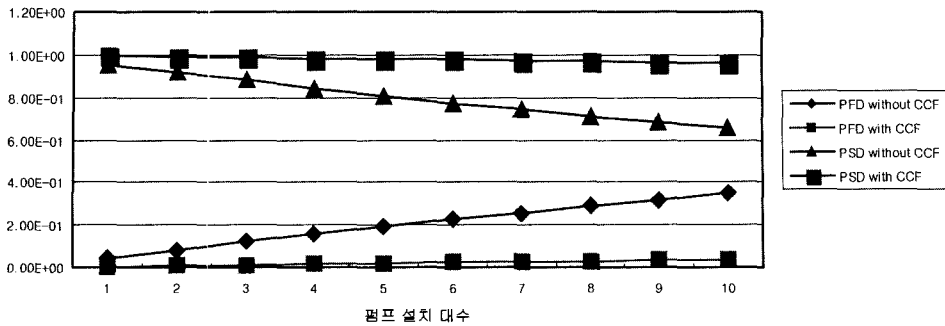


Fig. 6. Plot of PFD & PSD as the increasing number of pumps.

Table 10. Probability of failure on demand to safety integrity levels

등급	PFD	이용율(1-PFD)
SIL(1)	0.1 to 0.01	0.9 to 0.99
SIL(2)	0.01 to 0.001	0.99 to 0.000
SIL(3)	0.001 to 0.0001	0.999 to 0.9999
SIL(4)	0.0001 to 0.00001	0.9999 to 0.99999
SIL(5)	0.00001 to 0.000001	0.99999 to 0.999999
SIL(6)	0.000001 to 0.0000001	0.999999 to 0.9999999

61508-1: Functional Safety of Electrical / Electronic / Programmable Electronic Safety-related System Part 1 : General Requirements(2000)” 지침을 따랐으며 이를 정리하면 Table 10과 같다. Table 11에서 제시된 소방펌프에 대한 PFD는 최대 4.25E-2부터 최소 1.41E-6에 걸쳐 분포되어 있으며 이를 바탕으로 Table 10을 참고하여 소방펌프의 PFD에 대한 엄격한 SIL등급은 5이라고 판단된다. 따라서 SIS의 목표 SIL등급은 SIL5를 만족 유지 되어야만 한다

따라서 본 연구에 공통원인고장을 고려한 소방수 공

Table 11. Probability of failure on demand to fire water pump^{4,5,7,8)}

No	PFD	Source	Failure mode	Type
1	1.08E-2	CCPS3.3.7.2.1.1	Fail to start on demand/Fails while running	Pumps- motor driven pressure centrifugal
2	1.04E-4	CCPS3.3.7.2.1.1	Fail to start on demand/Fails while running	Pumps- motor driven pressure centrifugal
3	1.86E-2	CCPS3.3.7.2.1.1	Fail to start on demand/Fails while running	Pumps- motor driven pressure centrifugal
4	2.62E-2	CCPS3.3.7.3	Fail to start on demand/Fails while running	Pumps- turbine driven
5	9.66E-6	CCPS4.2.3.2	Fails to operate/Spurious operation	Fire suppression systems-water
6	1.41E-6	CCPS4.2.3.3	Fails to operate/Spurious operation	Fire suppression systems-dry powder
7	1.87E-2	CCPS4.2.4.1	Fails to start/Fails while running	Fire water pump-diesel
8	4.25E-2	CCPS4.2.4.2	Fails to start/Fails while running	Fire water pump-electric
9	1.70E-2	IEEE 11.1.2.4.1.1	Fails to start/Fails while running	Fire water pump-diesel(Centrifugal)
10	3.30E-2	IEEE 11.1.2.4.1.1	Fails to start/Fails while running	Fire water pump-electric(Centrifugal)
11	3.80E-3	IEEE 11.1.2.4.1.1	Fails to start/Fails while running	Fire water Jockey pump-electric (Centrifugal)
12	4.73E-3	IEEE 11.1.2.4.1.1	Fails to start/Fails while running	Fire water pump-General (Centrifugal)
13	9.60E-4	OREDA 1.3.1	Fails to start/Fails while running	Fire water pump-electric(Centrifugal)

급설비에 대한 신뢰도분석 결과 계통작동요구시 실패 확률(PFD: Probability of failure on demand), 즉 계통 이용 불능도는 $3.80E-3$ 이므로 엄격한 기준을 적용할 때 앞서 규정한 SIL5의 범주 안에 들어있지 않아, 안전건전성수준으로 설계되어 있다고 판단되지 않으며, 만일 공통원인고장을 고려하지 않았을 경우인 계통 이용불능도 또한 $1.82E-3$ 으로 계산되는데, 이 또한 SIL5의 범주 안에 들어있지 않으므로 안전건전성수준으로 설계되어 있지 않다고 판단된다.

4. 결 론

이상의 연구결과에서 살펴본 바와 같이 계통을 설계할 때 동일한 기능의 기기를 2개, 3개 또는 그 이상을 설치하여 계통의 신뢰성을 높이고자 하는 경우 공통원인고장 요인 때문에 신뢰성의 증가 폭이 기대만큼 크지 못할 수가 있다(Table 9, Fig. 6). 따라서 공통원인고장을 고려한 계통 신뢰도분석을 반드시 수행하여 투자대비 이득을 확인할 필요가 있다. 이는 소방설비 등 안전설비 뿐만 아니라 정상운전 시 생산기능에 참여하는 전 공정설비에 대해서도 마찬가지로 적용 가능하다. 결과적으로 다중기기의 공통원인고장을 방지하기 위한 기본적인 공학적인 방안으로는 설계 시 요구되는 적정 신뢰도를 유지하는 것이므로 적어도 소방펌프에 요구되는 신뢰도수준으로 설계되어야 한다. 즉 SIS(Safety Instrumented system)에 요구되는 신뢰도수준인 안전건전성수준(SIL: Safety integrity level)에 적합한가의 여부를 앞서 기술한 PFD를 활용하여 정량적으로 파악하는 것이다(Table 9, 10). 따라서 본 연구결과를 바탕으로 일반적으로 다중기기의 공통원인 고장을 방지하기 위한 최상의 제안으로서 첫 번째는 서로 다른 유형의 기기를 설치하는 것이 가장 바람직하며, 예를 들면 소방펌프를 2대 설치할 경우 하나는 엔진 펌프로, 그리

고 다른 하나는 전동펌프로 구매하여 설치하는 것이다. 즉 다중성(multiple)을 고려하되 펌프 구동의 다양성 (diversity)을 반영하는 것이다. 공통원인 고장 방지를 위한 두 번째는 두 기기를 운전 환경적 측면에서 물리적으로 격리하는 것이다. 그리고 신뢰도분석에서는 공통원인고장 인자를 포함한 기기고장 데이터에 따라 결과가 달라지므로 데이터의 신뢰성이 상당히 중요하며, 실제의 정량적 분석에서는 데이터의 불확실성(uncertainty)에 대한 논의가 반드시 필요하다.

참고문헌

1. Procedures for Treating Common Cause Failure in Safety and Reliability Studies, EPRI NP-5613, NUREG/CR-4780, Electric Power Research Institute (1988).
2. Singh, C. and Billinton, R., "System Reliability Modeling and Evaluation", Hutchinson(1977).
3. Development of an Improved LNG Plant Failure Rate Data Base, Gas Research Institute, Sep (1981).
4. Offshore Reliability Data, 3rd Edition, OREDA-97, SINTEF industrial Management, Norway(1997).
5. Guidelines for Process Equipment Reliability Data, American Institute of Chemical Engineering (1989).
6. Development of a Risk and Reliability Data Base for Chemical Facility, PLG, Aug(1986).
7. "IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear Power Generating Stations", IEEE std-500-1984, The Institute of Electrical and Electronics Engineers, Nov. (1993).
8. "Guidelines for Process Equipment Reliability Data", CCPS for American Institute of Chemical Engineers(1989).