신뢰성응용연구
제16권, 제3호. pp.231-237, 2016

IEC 61508에 기반한 원자력 발전소용 안전 등급 제어기의 SIL 분석에 대한 사례연구*

김 건 명†

(주)우 진

A Case Study of SIL Analysis for Single Station Controller in Nuclear Power Plant Based on IEC 61508*

Gun Myung Kim†

Woojin, Inc.

Purpose: It is not easy to suggest a quantitative data related to safety analysis. The objective of this paper is to propose a method of Safety Integrity Level (SIL) analysis and to suggest a SIL analysis result for single station controller in nuclear power plant based on IEC 61508.
Methods: The Failure Modes and Effects Diagnostic Analysis (FMEDA) and average probability of failure on demand (PFD) are used for SIL assessment.
Results: A SIL of single station controller is evaluated 4 by a reliability analysis results and PFD.
Conclusion: A SIL analysis method and result for single station controller based on IEC 61508 are proposed in this paper. It can applicable for a manufacturer data in safety-related system.

Keywords: Single Station Controller, FMEDA, PFD, SIL

1. 서 론

원자력 발전소의 방사능 누출 사고는 대중에게 심각한 피해를 입힐 수 있으므로 발전소의 안전성을 유지하기 위해 확률론적 안전성 평가(Probabilistic Safety Assessment; PSA) 등을 적용하여 주기적으로 위험 요인들을 관리하고 있다[1-3]. 이에 따라 원자력 발전소에 안전과 관련된 장치를 납품하는 제조사들은 발전소의 확률론적 안전성 평가를 위해 필요한 신뢰성 분석 자료를 납품 시 제공할 필요가 있다.

일반적으로 제조사들은 안전과 관련된 분석으로 안전사고가 발생할 확률을 산출한 고장수목분석(Fault Tree Analysis; FTA), 어떤 고장으로 인해 시스템 및 안전 분야에 어떤 영향을 미치고 이를 방지하기 위한 대책을 수립할 수 있는 고장모드 및 영향 분석(Failure Modes and Effects Analysis; FMEA) 등과 같은 방법들을 적용하였다. 이와 같은 분석 방법 외에도 안전제어 시스템의 기능 안전성을 정량적으로 분석하는 방법으로 IEC 61508에 기반한 안전무결성(Safety Integrity Level; SIL) 분석 방법이 널리 적용되고 있으며 고장 모드, 영

* 본 논문은 산업통상자원부 원자력융합원천기술개발사업(안전등급 공정제어계측용 지시 및 제어기 개발)의 지원(관리번호: 20131520202390)을 받아 연구되었음.
† 교신저자 gmkim@woojininc.com
2016년 8월 24일 접수; 2016년 9월 13일 수정본 접수; 2016년 9월 16일 게재 확정.

향 및 진단 분석(Failure Modes and Effects Diagnostic Analysis; FMEDA) 기법을 적용하여 쉽게 SIL 분석을 수행하고 있다[4].

기존에 SIL에 관한 연구들은 광범위하게 수행되고 있으나 그 중에서 FMEDA를 이용한 SIL에 관한 연구로는 김성규 외(2012)가 화염검출기를 대상으로 FMEDA 기법을 활용하여 SIS에 대한 정량적인 측정치를 도출하여 SIL 등급을 결정하는 사례 연구를 수행하였고, Kim *et al.*(2012)은 전극 수준(Electrode Type Level)을 측정하는 시스템을 대상으로 FMEDA를 적용하여 SIL을 평가하는 방법에 대해 제시하였다[5, 6].

따라서, 본 논문에서는 원자력 발전소 내에 설치되는 안전 등급 제어기에 대한 정량적인 안전성 분석을 위해 FMEDA를 이용하여 SIL 분석하는 방법에 대해 기술하고, 실질적인 분석 결과를 통해 산출된 SIL 수준을 제조사 안전성 분석 결과로 제시하고자 한다

2. FMEDA를 이용한 SIL 분석 방법

IEC 61508에 기반한 SIL 분석을 위해 먼저 분석 대상품의 기능 및 계층구조를 기초로 각 기능 및 구성품의 고장률을 예측하고, RBD(Reliability Block Diagram; RBD)과 FMEDA를 이용하여 낮은 요구 작동모드에 대한 평균 요구 고장확률(Average Probability of Failure on Demand; PFD)을 산출한 후 SIL 등급 기준에 따라 판정한다. SIL 분석시 적용되는 FMEDA, 공통원인고장, PFD 산출 방법 그리고 SIL 판정 기준을 정리하면 다음과 같다.

2.1 FMEDA

FMEA는 시스템 및 부품의 잠재적인 고장모드를 찾아내고 이와 같은 고장이 발생할 경우 임무 수행에 미치는 영향을 평가하고 대책을 수립하기 위한 분석 방법이다. FMEA에서 분석된 고장모드, 영향, 고장을 탐지하는 부분을 고려하고 안전 고장률과 위험 고장률을 구분하여 SIL 분석에 필요한 지표들을 산출할 수 있도록 활용되는 방법이 FMEDA이며, <Table 1>과 같은 양식에 기초하여 분석을 수행한다.

2.2 공통원인고장 산출

공통원인고장(Common Cause Failure)은 두 개 이상의 부품이 고장원인을 공유함으로써 동시에 혹은 아주 짧은 시간 내에 부품들에 발생하는 고장을 말한다. 다중 채널 시스템에서 하나 이상의 채널에 영향을 미칠 가능성이 있기 때문에, 공통원인고장 확률은 다중 채널 시스템의 전체 고장확률을 결정하는데 있어 주요한 요인이 될 수 있다.

IEC 61508에서 각각의 채널 내부에서 진단 테스트를 수행하는 다중 채널 시스템에서 공통원인고장 확률은 $\lambda_D\beta(\beta-Factor$ 모델)로 산출되며, 이를 다시 진단 가능 및 진단 불가능 부분으로 분리하면 식 (1)과 같이 정리된다.

$$\lambda_{DU}\beta+\lambda_{DD}\beta_D \tag{1}$$

여기서, λ_D는 위험고장확률, λ_{DU}는 단일 채널의 감지되지 않는 위험고장확률, λ_{DD}는 단일 채널의 감지 가능한 위험고장확률, β는 감지되지 않는 위험고장에 대한 공통원인고장 요인이며 β_D는 감지되는 위험고장에 대한 공통원인고장 요인이다

공통원인고장 요인 β와 β_D를 산출하기 위해 <Table 2>와 같은 지수를 이용하며 공통원인고장 지수 중 일부만 제시한 것이다. <Table 2>에서 X_{LS}와 Y_{LS}는 공학적 판단에 의하여 정량화되는 요소로, 로직 서브시스템에서 진단 테스트를 통해 효과가 증가된다고 생각되는 부분과 진단 테스트를 통해 증가되는 효과가 아닌 것으로 분리하여 각 열에 나타나있는 값들의 합계를 각각 X와 Y로 산출한다.

Table 1 FMEDA worksheet

ID	Item	Failure Rate per Total Item (failure/hour)	Failure Mode	Failure Detection Method	Likelihood of Failure Mode	Failure Rate of Failure Mode	Fraction Calculation			Failure Rate of Assembly			
							Safe	Dangerous	Detected	λSD	λSU	λDD	λDU
100,000													
110,000													

Table 2 Example of scoring programmable electrons(IEC 61508)

Item	Logic subsystem	
	X_{LS}	Y_{LS}
Separation/Segregation		
Are all signal cables for the channels routed separately at all positions?	1.5	1.5
Diversity/Redundancy		
Do the channels employ different electrical technologies for example, one electronic or programmable electronic and the other relay?	7.0	-
Complexity/Design/Application/Maturity/Experience		
Does cross-connection between channels preclude th0.5e exchange of any information other than that used for diagnostic testing or voting purposes?	0.5	0.5
Assessment/Analysis and Feedback of data		
Have the results of the failure modes and effects analysis or fault-tree analysis been examined to establish sources of common cause failure and have predetermined sources of common cause failure been eliminated by design?	-	3.0
Procedures/Human interface		
Is there a written system of work to ensure that all component failures (or degradations) are detected, the root causes established and other similar items inspected for similar potential causes of failure?	-	1.5
Competence/Training/Safety culture		
Have designers been trained (with training documentation) to understand the causes and consequences of common cause failures?	2.0	3.0
Environmental control		
Is personnel access limited (for example locked cabinets, inaccessible position)?	0.5	2.5
Environmental testing		
Has the system been tested for immunity to all relevant environmental influences (for example EMC, temperature, vibration, shock, humidity) to an appropriate level as specified in recognized standards?	10.0	10.0

Table 3 Value of Z : programmable electronics

Diagnostic coverage	Diagnostic test interval		
	Less than 1 min	Between 1 min and 5 min	Greater than 5 min
≧ 99%	2.0	1.0	0
≧ 90%	1.5	0.5	0
≧ 60%	1.0	0	0

Table 4 Calculation of β or β_D

Score (S or S_D)	Value β or β_D
	Logic subsystem
120 or above	0.5%
70 to 120	1%
45 to 70	2%
Less than 45	5%

<Table 2>에서 산출된 X와 Y값을 이용하여 β는 $S=X+Y$ 값을 <Table 4>에 적용하고, β_D는 <Table 3>에서 Z값을 구한 후 $S_D=X(Z+1)+Y$ 값을 <Table 4>에 적용하여 산출한다.

2.3 PFD 산출

IEC 61508에서는 안전제어시스템(SIS)의 작동모드를 요구율이 연간1회보다 작거나 보증시험 빈도의2배보다 작은 경우의 낮은 요구 작동모드(Low Demand Mode)와 요구율이 연간1회보다 크거나 보증시험 빈도의 2배보다 클 경우는 높은 요구 작동모드(High Demand Mode)로 구분한다. 낮은 요구 작동모드는 PFD를, 높은 요구 작동모드는 시간당 위험 고장확률(Average Frequency of Dangerous Failure; 이하 PFH라 지칭함)을 신뢰성 평가 척도로 적용한다[7].

본 논문에서는 식 (2)~식 (5)와 같이 안전 등급 제어기의 낮은 요구 작동모드의 직렬(1oo1) 구조와 2중

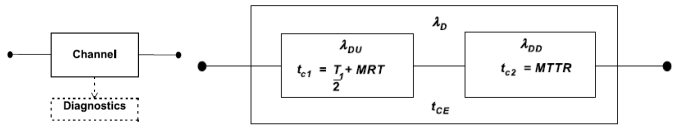

Fig. 1 1oo1 physical and reliability block diagram

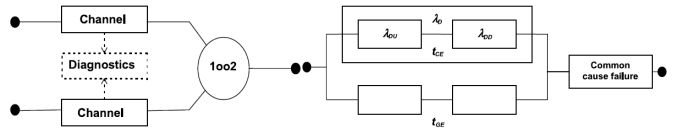

Fig. 2 1oo2 physical and reliability block diagram

Table 5 Safety Integrity Level

Safety Integrity Level(SIL)	Demand Mode of Operation	
	Average Probability of a Dangerous Failure on Demand of the Safety Function(PFD)	Average Frequency of a Dangerous Failure of the Safety Function(PFH)
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

1구조(1oo2)에서 PFD를 적용하여 SIL을 산출한다.

2.3.1 1oo1 구조

직렬 구조의 물리적 블록도와 신뢰성 블록도는 <Fig. 1>과 같으며, 낮은 요구 작동모드에서 PFD 산출식은 식 (2)~식 (3)과 같다.

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \quad (2)$$

$$PFD = (\lambda_{DU} + \lambda_{DD}) t_{CE} \quad (3)$$

여기서, t_{CE}는 channel equivalent mean down time(시간)으로 하위 시스템의 채널 내 모든 부품에 대한 비가동시간, T_1은 보증시험간격(시간), MRT(Mean Repair Time)와 MTTR(Mean Time to Restoration)은 평균 수리시간과 평균 복구시간으로 자동으로 감지되는 경우에는 MRT = MTTR이다.

2.3.2 1oo2 구조

2중 1구조의 물리적 블록도와 신뢰성 블록도는 <Fig. 2>와 같고 해당 구조의 PFD 산출식을 정리한 것이 식 (4)~식 (5)이다.

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \quad (4)$$

$$PFD = 2((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU}\left(\frac{T_1}{2} + MRT\right) \quad (5)$$

여기서, t_{GE}는 voted group equivalent mean down time (시간)으로 이중화 구조에서 모든 채널에 대한 비가동시간이다.

2.4 SIL 판정 기준

제2.3절에서와 같은 방법을 적용하여 산출된 PFD (또는 PFH)를 IEC 61508에 제시된 <Table 5>의 SIL 수준에 따라 등급을 판단한다.

3. 안전 등급 제어기에 대한 SIL 분석

원자력 발전소용 안전 등급 제어기는 온도, 전압, 전류신호를 입력 받아 PID 또는 On/Off control algorithm에 따라 신호처리를 수행하여 출력신호를 생성

Table 6 FMEDA result for single station controller

ID		Item	Failure Rateper Total Item (failure/hour)	Failure Mode	Failure Detection Method	Likelihood of Failure Mode	Failure Rate of Failure Mode	Fraction Calculation			Failure Rate of Assembly			
								Safe	Dangerous	Detected	λSD	λSU	λDD	λDU
100000	1	Single Station Controller												
110000	1	Control Board Assembly												
111000	1	CPU Board	4.80E-06	Loss of Signal Process Function	Display/ Alarm/ System fail output	33.2%	1.59E-06		√	√	3.68E-06	0.00E+00	3.48E-06	0.00E+00
111000	2		4.80E-06	Loss of Digital Signal Input Function	Display/ Alarm/ System fail output	0.4%	1.87E-08	√		√				
111000	3		4.80E-06	Loss of Digital Signal Output Function	Display/ Alarm/ System fail output	31.6%	1.52E-06	√		√				
111000	4		4.80E-06	Loss of Communication with Display Function	Display/ Alarm/ System fail output	22.1%	1.06E-06	√		√				
111000	5		4.80E-06	Loss of Power Supply Function	Display/ Alarm/ System fail output	12.7%	6.10E-07		√	√				
112000	1	Analog Input(AI) Board	1.08E-06	Loss of Analog Signal Input Function	Display/ Alarm/ System fail output	100.0%	1.08E-06	√		√				
113000	1	Analog Output(AO) Board	1.28E-06	Loss of Analog Signal Output Function	Display/ Alarm/ System fail output	100.0%	1.28E-06		√	√				
120000	1	Terminal Board Assembly												
121000	1	Backplane Board	6.12E-07	Loss of Connection Function	Display/ Alarm/ System fail output	100.0%	6.12E-07		√	√	0.00E+00	0.00E+00	1.99E-06	0.00E+00
122000	1	Main Terminal Board	6.86E-07	Loss of Connection Function	Display/ Alarm/ System fail output	100.0%	6.86E-07		√	√				
123000	1	Backup Terminal Board	6.91E-07	Loss of Connection Function	Display/ Alarm/ System fail output	100.0%	6.91E-07		√	√				

하고 이 신호를 전압 또는 전류 신호로 출력하여 온도, 압력, 유량, 수위 등의 계통을 제어한다. 이와 같은 원자력 발전소용 안전 등급 제어기의 SIL 수준을 분석하기 위해서 먼저 계층구조 및 기능을 정의한 후 <Fig. 3>과 같은 RBD를 기초로 각 부품 및 기능에 대한 고장모드, 영향, 고장 탐지 방법, 안전 및 위험고장으로 구분하여 <Table 6>과 같이 FMEDA 결과를 산출하였다.

<Table 6>에서 안전과 관련된 고장률은 감지되는 경우와 감지되지 않는 경우로 구분하여 각각λ_{SD}와 λ_{SU}로 계산하고, 위험과 관련된 고장률은 감지되는 경우와 감지되지 않는 경우로 구분하여 각각λ_{DD}와 λ_{DU}로 산출된다. 안전 등급 제어기의 경우 고장이 발생할 경우 알람 등을 통해 모두 감지가 되므로 λ_{SU}와λ_{DU}는 0이며, Control Board Assembly와 Terminal Board Assembly의 PFD 산출에 적용되는 λ_{DD}는 각각 3.48×10^{-6}과 1.99×10^{-6}이다.

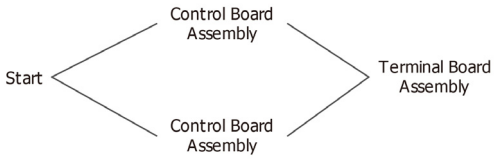

Fig. 3 RBD for single station controller

안전 등급 제어기는<Fig. 3>에서와 같이 2개의 Control Board Assembly는 이중화로 구성되고Terminal Board Assembly와 직렬 구조로 연결되므로, Terminal Board Assembly는 1oo1 구조의 PFD값을, Control Board Assembly는 1oo2 구조의 PFD값을 산출하여 합계를 구하여 <Table 7>과 같이 안전 등급 제어기의 PFD값을 산출한다.

여기서, 공통원인고장의 경우 감지가 되지 않는 위험고장에 대한 공통원인고장 요인(β)은 고려하지 않아도 되므로 감지되는 위험고장에 대한 공통원인고장 요인인 β_D를 산출하기 위해 <Table 2>에 제시된 지수를 이용한다. <Table 2>의 물음에 대해 공학적 판단에 따라 진단 테스트를 통해 효과가 증가된다고 생각되는 부분(X_{LS})과 진단 테스트를 통해 증가되는 효과가 아닌 것으로 생각되는 부분(Y_{LS})에 점수를 체크한 후 X_{LS}에 체크된 점수의 합계와 Y_{LS}에 체크된 점수의 합계는 각각 $X=10, Y=30$으로 산출되었다. <Table 3>에서 Z값은 diagnostic coverage와 진단테스트 구간에 의해 결정되므로 안전 등급 제어기의 경우 고장 발생시 99% 이상 고장을 검지할 수 있고 진단을 수행하는 간격은 1분에서 5분 사이로 가정하였으므로 $Z=1.0$로 산출되어 $S_D=X(Z+1)+Y=50$으로 계산되었다. 따라서, β_D는 <Table 4>에 따라 2%가 적용되고, λ_{DU}가 0이므로 $\lambda_D=\lambda_{DD}$, MTTR = 8시간으로 가정하여 PFD를 산출하였다.

Table 7 PFD results for single station controller

Item Description	t_{CE}	t_{GE}	PFD
Control Board Assembly	8	8	5.59×10^{-7}
Terminal Board Assembly	8	-	1.59×10^{-5}
Single Station Controller			1.65×10^{-5}

원자력 발전소용 안전 등급 제어기의 낮은 요구 작동모드에서 평균 요구 고장확률(PFD)은 <Table 7>에서와 같이 1.65×10^{-5}으로 <Table 5>의 SIL 판정 기준에 따르면 고장확률이 10^{-5}보다는 크고 10^{-4}보다는 작으므로 SIL 4 수준이라도 판단할 수 있다

4. 결 론

본 논문에서는 원자력 발전소용 안전 등급 제어기를 대상으로 IEC 61508에 기반하여 FMEDA와 PFD 산출을 통해 SIL을 분석하는 방법을 제시하였다.

실제 안전 등급 제어기 부품별로 예측된 고장률을 적용하여 감지되는 위험고장에 대한 공통원인고장 요인 β_D는 2%, 평균 수리시간MTTR은 8시간일 경우 안전 등급 제어기의 평균 요구 고장확률(PFD)은 1.65×10^{-5}으로 SIL 4 수준에 해당되는 것으로 판단할 수 있었다.

본 논문에서 제시한 SIL 분석 방법과 결과는 향후 제조사에서 정량적인 안전성을 분석할 경우 가이드라인으로 활용할 수 있으며, 산출된 결과는 고객사에 객관적인 자료로 제시할 수 있을 것으로 기대된다.

References

[1] Song, T. Y. and Yung, B. Y. (2015). “A Study on the Strategy Assessment in Nuclear Power Plants”. The

Korea Society for Energy Engineering, pp. 140.

[2] Yu, G. J. and Chae, S. G. (1987). “Probabilistic Safety Analysis Method”. Nuclear Engineering and Technology, Vol. 19, No. 2, pp. 137-148.

[3] Jeong, I. S., Kim, W. S. and Lee, C. W. (1999). “Nuclear Power Plant Lifetime and Periodic Safety Management”. The Korean Society of Mechanical Engineers, Vol. 2, No. 2, pp. 43-48.

[4] IEC 61508 (2010). “Functional Safety of Electrical/ Electronic/Programmable Electronic Safety-related System - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3”.

[5] Kim, S. K. and Kim, Y. S. (2012). “A Study on FMEDA Process for SIL Certification : A Case Study of a Flame Scanner”. IE interfaces, Vol. 25, No. 4, pp. 422-430.

[6] Kim, B. C. and Kim, Y. J. (2012). “Case Study on the Assessment of SIL Using FMEDA”. IE Interfaces, Vol. 25, No. 4, pp. 376-381.

[7] Seo, S. K. (2012). “On Reliability Performance of Safety Instrumented Systems with Common Cause Failures in IEC 61508 Standard”. IE interfaces, Vol. 25, No. 4, pp. 405-415.