Journal of the Korea Academia-Industrial cooperation Society
Vol. 24, No. 1 pp. 237-246, 2023

https://doi.org/10.5762/KAIS.2023.24.1.237
ISSN 1975-4701 / eISSN 2288-4688

고밀도 폴리에틸렌(HDPE) 플렌트 중합공정의 안전건전성수준(SIL)을 이용한 반정량적 신뢰도 분석에 관한 연구

고재선
호원대학교 소방안전학과

A Study on the Semii-Quantitative Reliability Analysis of High Density Polyethylene (HDPE) by Plant Safety Process Safety Integrity Level (SIL)

Jae-Sun Koh
Department of Fire Safety Engineering, University of Howon

요 약 본 분석의 목적은 HDPE(High Density Polyethylene) 플랜트 중합공정에서 폭주반응 등의 원인으로 반응기와 후단라인에 과압방지를 위해 설치를 계획하고 있는 SIS(Safety Instrumented System)의 신뢰도가 압력방출밸브(PSV: Pressure Safety Valve)가 요구되는 안전건전성 수준(SIL: Safety Integrity Level)으로 설계되어 있는지를 정량적으로 분석하고자 한다. 연구결과로는 신뢰도 자료를 입수하여 압력방출밸브의 요구시 실패확률(PFD: Probability of Failure on Demand)을 조사한 결과 압력방출밸브의 PFD는 최대 2.83E-4부터 최소 1.52E-3에 걸쳐 분포되어 있으며, 이로부터 SIS에 대한 안전건전성 수준(Safety Integrity Level, SIL)의 목표 등급을 SIL 3으로, PFD는 1.00E-3에서 1.00E-4로 결정하였고, SIS에 대한 성공기준을 마련하기 위하여 신뢰도모델을 구축하고 이를 토대로 고장수목 분석(FTA: Fault Tree Analysis) 기법을 이용하여 SIS의 요구시 실패확률에 대한 정량화를 수행한 결과 SIS에 대한 PFD는 7.30E-4로 계산되었다. 따라서 SIS의 신뢰도가 압력방출밸브가 요구되는 안전건전성 수준(SIL)으로 설계되어 있다고 판단된다.

Abstract This study analyzes the reliability of the SIS (Safety Instrumented System) to be installed in the reactor and downstream line. The SIS helps in preventing overpressure due to runaway reactions, etc., during the polymerization process of the HDPE (High Density Polyethylene) plant. This study is a quantitative analysis to determine whether the pressure safety valve is designed to the required safety integrity level (SIL). Reliability data were obtained from the results, and the Probability of Failure on Demand (PFD) was investigated. We determined that the target grade of the Safety Integrity Level (SIL) for SIS was SIL 3, and the PFD ranged between 1.00E-3 to 1.00E-4. Quantification of the failure probability upon request of the SIS using the Fault Tree Analysis (FTA) technique based on the model building revealed the PFD for the SIS to be 7.30E-4. Our results indicate that the reliability of the SIS is designed to the required safety integrity level (SIL) for the pressure relief valve.

Keywords : Safety Instrumented System, Safety Integrity Level, Probability of Failure on Demand, Reliability Block Diagram, Fault Tree Analysis, Pressure Safety Valve, Target Process

*Corresponding Author : Jae-Sun Koh(Howon Univ.)
email: 119kjs@howon.ac.kr
Received October 24, 2022 Revised December 26, 2022
Accepted January 6, 2023 Published January 31, 2023

1. 서론

1960년대 이후 우리나라는 경제 및 산업구조를 근대화시키기 위한 정부의 중화학공업 육성정책에 의해서 발전을 지속하였다. 특히 화학공업의 발달은 산업발전에 획기적인 전기가 되어 신흥공업국으로 발전하는데 중추적인 역할을 하였다. 그러나 각종 공정 설비의 규모가 증가하고 유해한 화학물질의 사용이 크게 증가함에 따라 화재 및 폭발 사고 등으로 작업 중인 근로자는 물론 인근 지역주민까지도 영향을 미칠 잠재적 가능성이 증가하고 있다. 화재 및 폭발로 인한 중대 사고를 야기할 수 있는 대형 위험사업장의 종류로는 정유공장, 석유화학공장, 정밀화학공장 농약 및 도료제조공장, 화학비료공장, 가솔린 등의 연료저장을 위한 탱크터미널, 도시가스 제조공장, LPG 및 LNG 저장기지 등으로 전국에 약 300개소의 사업장이 분포되어 있다. 이들 중에는 설치 후 10년 이상이 경과한 사업장이 약 60%를 점하고 있고 20년 이상도 10%를 넘고 있으며 그 현황은 Table 1[1]과 같다. 또한 2010년부터 2016년까지 화학공업 분야의 중대사고(사망자 발생 사고나 사회 물의를 일으킨 사고)발생 현황은 총 46건으로 Table 2[1]와 같으며, 발생형태는 폭발이 41%, 화재가 26%로 분석되었고, Table3[1]에서 나타난 것처럼 중대사고 발생 원인을 분석한 결과 설비결함이 39%, 오조작이 31%, 제조공정 이상이 4% 등으로 분석되어 설비결함에 의한 사고 발생가능성이 높음을 보여주고 있다.

Table 1. Hazard presents of major facilities in chemistry industrial

Classification	total	Operation Time(yr)				
		0~5	6~10	11~15	16~20	21≥
Total	284	38	80	79	58	29
Oil	5	1	-	1	-	3
Petroleum chemistry	53	8	12	15	16	2
Precise chemistry	82	11	21	25	17	8
Chemistry	18	1	6	9	-	2
Manure	3	-	-	-	1	2
Toxic Substance	20	2	2	4	9	3
Hazardous material terminal	68	11	16	18	15	8
Urban Gas factory	28	4	19	4	-	1
LPG, LNG Terminal	7	-	4	3	-	-

Table 2. Presents of major accidents in chemistry industrial

Accident Type	No. of Occurrence	Percentage(%)
total	46	100
explosion	19	41
fire	12	26
release	11	24
others	4	9

Table 3. Causes of major accident in chemistry industrial

Causes	No. of Occurrence	Percentage(%)
total	46	100
facilities default	18	39
miss operation	14	31
product process default	2	4
corrosion	4	9
others	8	17

따라서 화학공정상에 있어서 설비결함에 의한 사고 발생가능성을 줄이기 위한 기법으로 IEC 60508[2,3]에 대한 전반적인 내용 중 안전무결성레벨(SIL) 평가방법에 대한 연구로써 SIL등급의 분리 및 할당 방법에 대해 설명하고 이를 토대로 운영 및 유지 보수단계에서 효과적인 시스템의 신뢰성, 가용성, 유지보수성 및 안전성 확보방안을 제시하고자 한다.

1.1 연구 배경 및 목적

위에서 언급한 내용과 같이 화학 산업은 시스템이 복잡한 장치산업으로서 설비상 잠재위험요소 및 각종 위험물 보유량이 많기 때문에 화재 및 폭발 사고가 발생할 경우 대형 사고를 유발하기 쉽고 이러한 피해의 광역화와 인명피해를 방지하기 위하여 유사한 사고로부터의 교훈을 토대로 하여 안전설계, 작업안전관리 등에 활발히 적용되고 있고, 아울러 최근 4차산업과 관련하여 각 산업의 융합분야의 연구동향을 살펴보면 화학공정산업은 물론 원자력산업, 조선산업, 철도관련 산업의 각종 디지털 제어기 및 신호시스템, 전자•전기의 프로그램시스템, 경영 및 정보관리 소프트웨어 안전성분석, 자동차관련산업에서의 산업용 로봇 등을 통한 자동화 시스템, 의료용 ESS에서 첨단 배터리 관리 솔루션 등 신뢰성과 관련된 산업 등에서 SIL(Safety Integrity Level)과 연관하여 광범위하게 공학적, 기술적 연구가 진행되고 있다[4-12].

따라서 본 분석에서는 HDPE 플랜트의 중합공정에서 SIS(SIL : Safety Instrument Systeml)로서 반응기 후단설비의 가압방지를 위해 설치된 압력방출밸브(PSV : Pressure Safety Valve)가 요구하는 신뢰도인 안전건전성수준(Safety Instrument Level)으로 설계되었는지를 반정량적으로 분석하고 판단하는 것이다.

1.2 연구 방법

본 분석을 수행하기 위한 개략적인 방법은 먼저, 해당 공정관련 자료를 정성적으로 검토하여 사고 발생 원인 및 현재의 안전 조치들을 파악해봄으로써 이로부터 SIS의 기능 및 구성을 파악하고 다음으로 일반신뢰도 데이터 자료를 (EPRI, IEEE Standard 500, CCPS, OREDA)[13-15]를 조사하여 SIS(Safety Instrumented System)[19]에 대한 안전건전성수준(Safety Integrity Level)의 목표값을 결정함으로서 SIS에 대한 성공기준을 마련하기 위하여 신뢰도 모델(RBD : Reliability Block Diagram)[16,19]을 구축하고자 한다. 이를 토대로 정량적인 고장수목분석(FTA: Fault Tree Analysis)기법을 이용하여[17,18] SIS의 요구시 실패확률에 대한 정량화를 수행하고 마지막으로 정리와 과정을 통해 도출된 SIS에 대한 요구 시 실패확률(PFD: Probability of Failure on Demand)이 목표 안전건전성수준(Target Safety Integrity Level)에 부합되는지를 판단하고자 한다.

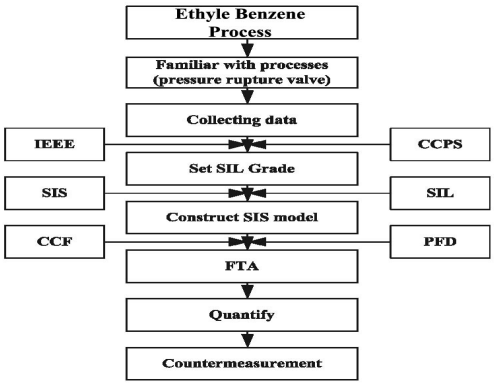

Fig. 1. Flow chart on study.

2. 본론

2.1 안전장치 시스템(SIS :Safety Instrumented System)

1996년에 수많은 산업사고들에 대응하기 위해서 미국의 ISA(The Instrument Society of America)는 미국 내에서 산업공정에 관한 안전장치시스템(SIS)에 대한 기준을 제정하였다. 이 기준은 ISA S84.01로서 안전건전성수준(SIL : Safety Integrity Level).[19]의 개념이 소개되었다. 그 후 IEC(International Electrotechnical Commission)는 안전과 관련된 시스템들을 프로그램화하고 안전을 정량화하는데 도움을 주기 위하여 산업에 대해 중립적인 IEC 61508[3,4]을 제정하였다. 이러한 기준들은 산업공정의 본질적인 안전을 개선하게 될 해결도구를 찾는데 있어서 Hydrocarbon공정 및 Oil 및 Gas산업에서 특별히 발전되어 왔다. 또한 이러한 기준들의 부산물로서 안전건전성수준(SIL)을 수립하기 위한 중심적인 수많은 파라메타들을 발견되었고, 최적화 되었으며 공정과 시간이 관련된 신뢰성이 추가적으로 제공되었다.

2.2 안전건전성 수준(SIL : Safety Integrity Level)

SIL(Safety Integrity Level)은 주어진 공정에 대한 안전수준을 측정하는 것이다. 특별히 안전한 방법에 의한 공정 수행시 일어날 수 있는 실수 및 고장의 경우에 있어서 나타나는 의문점들에 대해 마지막 사용자가 공정을 예측할 수 있는 것은 어떤 범위까지인가 하는 것이다. 이런 측정치들에 대한 사양은 정성적인 방법을 기술한 IEC 61508, 반(Semi)정량적인 방법을 기술한 IEC 61511, JIS C 0508 그리고 ISA SP84.01기준들에 요약이 기술되어있다[3,4,19]. Figure 2는 공정과 관련하여 SIL등급들이 연계되고 추론되기 위한 필요도구인 RAT (Risk Assessment Tree)[14,19]이다. RAT는 해당 공정에 대해 안전과 위험을 평가하는 도구로서 특히 위험에 대해 수용 가능하거나 수용 가능하지 못함을 분류하는 것이다. 아울러 SIL등급의 분리 및 할당 방법에 대해 좀더 설명하면 IEC 61508에서는 SIL을 4등급, ISA에서는 3등급으로 분류하고 있으며, 독일에서는 SIL을 7등급으로 분류하여 사용하고 있다. 이러한 등급의 차이가 발생하는 이유는 적용되는 산업 분야에 따른 안전성 요구사항 수준이 다르기 때문이며 SIL4등급은 공정산업에서 적용되지 않으며 항공, 원자력 등 특수산업에만 적용된다. 또한 시스템의 가용도 요건에 따라 다양한 산업에 필요한 SIL을 표시하는데 사고가 발생하였을 경우 경제환경에 미치는 파급효과가 큰 산업일수록 높은 SIL이 필요하다는 것을 알 수 있으며 그 중 공정산업은 보통 SIL을 3등급으로 하고 있다. SIL 1등급이 갖는 의미는 잠재위험이나 경제적위험등급이 낮으면서 90%의 이용가능상태를 유지하는 시스템을 의미한다.

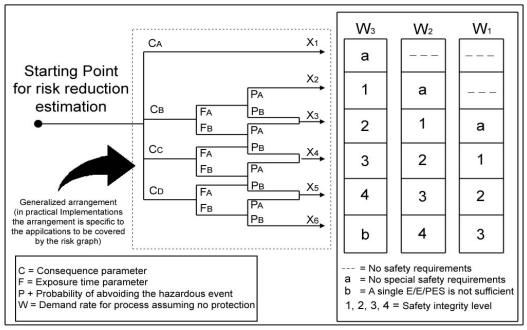

Fig. 2. Draw on Risk Assessment.

2.3 안전건전성 수준과 신뢰성 (SIL Versus Reliability)

SIL등급의 중요한 요점은 공정의 본질적인 안전에 대해 해석하는 것이고, SIL등급 계산에 사용된 중요한 통계적인 부산물로는 안전에 관한 해석상의 신뢰성에 대한 기술일 것이다. 만약 신뢰성을 결정하기 위해서 어떤 안전에 관한 해석이 주어진 SIL환경에서 사용되었다면 그 안전에 관한 해석은 어떤 예정된 등급에서 나타내는 임무를 수행함에 있어서 “수용 가능함”이라고 나타내어진다. “수용 가능함”을 결정할 때 MTBF(Mean Time Between Failure), MTTR(Mean Time to Repair), PFD(Probability to Fail on Demand)가 포함된 고려사항들을 참작해야 한다[14,16,19]. 이러한 고려사항들은 설계시스템에 기반을 둔 변수들에 따라서 안전에 관한 해석의 신뢰성이 결정된다. 이어서 이 신뢰성 데이터, 즉 안전한 방법으로 공정을 수행할 때 실수를 야기하는 가능성을 통계적으로 측정하고 조합하는데 사용되는 것으로 알려진 것은 SFF(Safe Failure Fraction)[14,19]이고, 그 측정치로 최대로 등급화 된 SIL환경을 결정한다. SIL 등급은 공정에 대한 의문점들에 대한 “요구시 실패확률”을 방정식으로 나타낼 수 있다. 아래의 Table 4와 5[14,19]는 공정이" Demand mode"인지에 대한 관계를 나타낸 것이다.

Table 4. Safety integrity level : probability of failure on demand

Demand Mode of Operation		
Safety Integrity Level	Average Probability of Failure on Demand	Risk Reduction
4	≥ 10-5 to 〈 10-4	〉10,000 to ≤100,000
3	≥ 10-4 to 〈 10-3	〉1000 to ≤10,000
2	≥ 10-3 to 〈 10-2	〉100 to ≤1000
1	≥ 10-2 to 〈 10-1	〉10 to ≤100

2.4 안전건전성 수준의 결정 (Determining SIL values)

앞서 언급한 것과 마찬가지로 주어진 공정에서 SIL의 등급을 결정하기 위해 사용되는 방법으로는 2 가지가 있는데 이것들은 Fault Tree Analysis와 Markov Analysis[17,18]로서 각각의 이러한 방법들에 대해 첫 번째 단계는 공정 구성품 각각에 대해서 PFD를 결정하는 것이다. 예를 들면 대상공정(Target Process)에서 PFD는 다음에 나타낸 관계식을 사용한다.

PFD ave = (Failure Rate)2 * Test Interval (1)

Note : Failure rate = 1 / MTBF

다음 단계는 공정의 모든 구성품들에 대해 PFD 값들을 합산하는 것이다. 합산된 PFD는 그 때 위의 Table 4[14]에서의 공정에 관한 SIL 등급과 비교된다. 본 논문에 사용된 Fault Tree Analysis 방법의 경우에 있어서의 다음 단계는 Fault tree를 다이어그램으로 작성하는 것이다. 이 다이어그램은 잠재적인 위험 사건을 포함하여 여러 가지 공정의 구성품들을 목록화 한 것이다. 그 구성품들은 Boolean Logic을 거쳐 tree 안에서 연계되어 진다. 일단 이것이 완료되면 각각의 계통에 대한 PFD는 논리적인 관계에 근거하여 결정되어진다. 마지막으로 PFDs는 공정에 관한 PFDave를 산출하기 위해서 합산되어지고, 다시 한번 PFDave는 적절한 SIL등급을 위하여 Table 5[19]를 참조하게 된다.

Table 5. Safety integrity level : frequency of dangerous failure per hour

Continuos Mode of Operation	
Safety Integrity Level	Frequency of Dangerous Failure per Hour
4	≥ 10-9 to 〈 10-8
3	≥ 10-8 to 〈 10-7
2	≥ 10-7 to 〈 10-6
1	≥ 10-6 to 〈 10-5

2.5 데이터 자료

Safety Instrumented System(SIS)의 목표 Safety Integrity Level(SIL) 및 고장수목의 정량화시 검토해야 할 일반신뢰도 데이터자료로서는 Table 6[13-15]과 같다. (EPRI, IEEE Standard 500, CCPS , OREDA)

Table 6. Classification of national data reliability

Classification	Description
EPRI	- Reliability data used by Basically when perform a probabilistic safety assessment of new light water reactor at american EPRI (Electric Power Research Institute) - This data is also used to extract reliable data that are deemed suitable by reviewing data collected from several different dates, and general reliability in nuclear power plants, each plant type - That contains information about the common-cause failures - In addition, appendix A contains a description that is sure to extract liability data by any assumption - And given only point estimates(Point Estimate Value), or whether the value is the average value or 50% value, including assumption about the distribution not given. - These data are given a total of 104 data reliability, this type of equipment is separated 24, detailed specifications are 44.
IEEE Standard 500	- This data is analyzed by collecting data on the nuclear power plant facilities and equipment as dates published by the IEEE (Institute of Electrical and electronics Engineers). - Compared to other literature data that the reliability for the electric and electronic equipment is given in detail
CCPS	- Reliability data for use reference when analyzing the reliability of chemical plants at CCPS (Center for Chemical Process Safety of the American Institute of Chemical Engineers) - This data is extracted using reliability data on the number of facilities required from the general liability data - That the advantages of this dates is given figure determining the boundaries equipment and the average upper limit/lower limit is given - The separated dates has given a total of 113 data reliability, equipment types 34, 73 for detailed specifications.
OREDA	- Given that oil plant reliability data for the facility as a kind of one hundred kinds of data collected for the equipment associated with(mostly petroleum related facilities) - Given that has been detail classified as a failure mode and failure severity, upper and lower limits, the failure rate and maintenance time the basis of the calculation, - The number is not given the failure rate per operation - Each facility-specific data collection period is an advantage that the reliability of the data that have been collected from hundreds of thousands to millions of times higher

3. 사례를 통한 High-Density Polyethylene중합공정에서 안전장치시스템의 안전건전성성 수준의 분석

3.1 HDPE 중합반응 공정

HDPE 공정은 중합반응을 통해 고밀도 폴리에틸렌을 생산하는 공정으로 공정흐름을 간략히 나타내면 Figure 3과 같다.

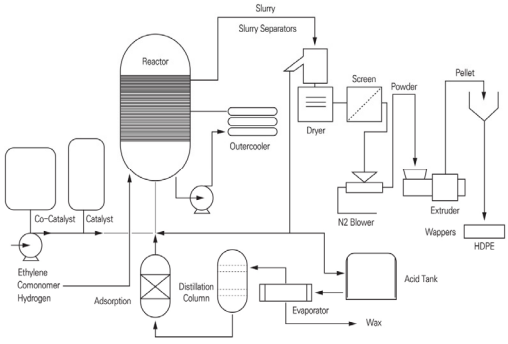

Fig. 3. P&ID on product unit of high density polyethylene.

고밀도 폴리에틸렌 생산에 필요한 원료는 에틸렌과 지글러 타입의 촉매, 촉매의 활성을 높여주는 조촉매, 용제로 사용되는 헥산, 반응종결물질인 수소 등이 있다. 이러한 원료들은 반응기에서 중합반응을 거쳐 반응한 후 분리, 건조, 압축공정을 거쳐 최종 제품을 생산하게 된다. 중합반응이 이루어지는 반응기(R-2103)에서 폭주반응(Run Away Reaction) 발생 시 반응기의 압력이 상승하게 되는데 그 압력이 반응기 후단의 압력방출밸브의 설정치 이상으로 상승하게 되면 반응기가 폭발할 수도 있고 2차적인 사고현상으로 화재의 위험성을 내재하고 있다. 이러한 사고를 대비하여 반응기내 압력상승을 감지하여 고압시 주촉매 펌프와 원료공급라인의 밸브를 차단하는 SIS(Safety Instrument System)가 설치되어 있다.

3.2 Target SIL (Safety Integrity Level)

Table 7과 같이 PSV의 PDF(요구시 열림실패 : Fails to Open on Demand)데이터는 최대 7.03E-03, 최소 2.1E-04로 분포되어있다. Table 7 및 8[13-15]을 비교하여 볼 때 PSV의 PFD는 SIL의 3등급(0.001~0.0001)에 해당한다. 따라서 HDPE 플랜트의 SIS는 3등급의 SIL을 만족해야 한다.

Table 7. Probability of Failure on demand of pressure safety valve.

No.	PFD	Data Source	Others
1	4.15E-3*	CCPS 4.3.3.1	Pilot operated type
2	2.12E-4*	CCPS 4.3.3.2	Spring loaded type
3	3.20E-3*	IEEE-500 11.2.b.1	Pressure relief valve
4	1.00E-3**	EPRI ALWR URD Annex A Table A2-1	Pressurizer safety valve for PWR
6	7.00E-3**	EPRI ALWR URD Annex A Table A2-1	Safety/relief valve for BWR, actuation mode
7	5.00E-3**	EPRI ALWR URD Annex A Table A2-1	Pilot operated type

* : mean 값을 기준, ** : 점추정치 기준, E-3는 10-3을 의미함.

Table 8. Probability of failure on demand from Safety Integrity Level.

Ranking	PFD	(1-PFD)
SIL 1	0.1 to 0.01	0.9 to 0.99
SIL 2	0.01 to 0.001	0.99 to 0.999
SIL 3	0.001 to 0.0001	0.999 to 0.9999

3.3 Safety Instrumented System (SIS)의 구성 및 성공기준

Safety Instrumented System(SIS)는 압력상승감지 시스템, Logic Solver 시스템 그리고 공급라인 밸브차단 시스템 등의 3부분으로 이루어진다. SIS의 성공기준은 Sensor System 중 하나와 Logic System 중 하나가 작동하고 원료공급라인이 성공적으로 차단되는 것을 기준으로 하였다. 이와 같은 성공기준을 바탕으로 Safety Instrumented System(SIS)의 Reliability Block Diagram (RBD)[14,16,19]을 작성하면 Figure 4와 같다.

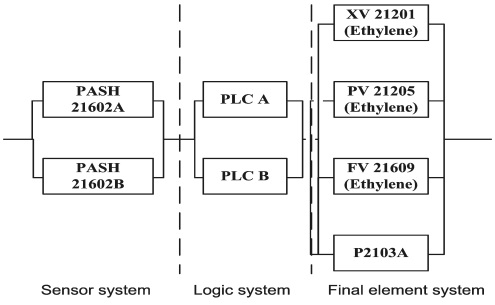

Fig. 4. Reliability block diagram by success criteria of SIS.

3.4 고장수목분석구성

Safety Instrumented System(SIS)의 요구시 이용불능확률(Probability of Failure on Demand, PFD)을 계산하기 위한 기준이 Table 9[14,16,19]이며 이를 기반으로 구성한 고장수목이 Figure 5이다.

Table 9. Fault tree by failure on demand of SIS for HDPE Plant.

Classification	Description
Unavailability when sensor system requirements	- 2103 reactor pressure switch installed on the top, PASH21602A & 21602B the inability to have failed all available upon request2B - If the pressure switch is out of use when the signal is not sent to the PLC in response to a pressure rise
Unavailability when Logic System requirements	- If the inability to use both the PL cconnected in parallel - If the signal from the pressure switch does not transfer to the final element
Blocked failure when catalyst line needs or ethylene supply line requirements	- The flow control valve (FV21609), a pressure control valve(PV21205), the emergency shut-off valve(XV21201) in the ethylene feed line are both closed on failure requires - In the case of failure when the ethylene supply line blocked, and the co-catalyst pump has failed to stop when required

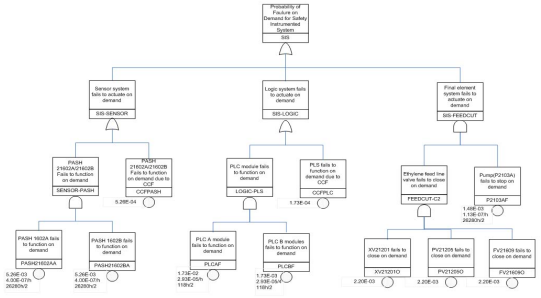

Fig. 5. Fault tree for SIS failure on demand.

4. 기본사건의 요구시 이용불능확률의 (Probability of Failure on Demand, PFD) 계산

고장수목에서 나타나는 기본사건의 요구시 이용불능확률(Probability of Failure on Demand, PFD)[14,19]를 계산하기 위해서는 기기 고장모델을 구성해야 하며 본 분석에 사용된 기기 고장모델식은 다음과 같고, 계산의

정확성과 수월성을 확보하기 위해 "KIRAP-KWTREE Beta 1.0"과[17] "Fault Rree with Aerospace", Version 1.1[18]의 Tool 그리고 고장률 분석 확률론적 통계프로그램인 미니탭을 활용하여 계산하였다.

4.1 요구시 고장율을 가진 대기상태(Standby) 기기의 고장 모델식

에틸렌 공급라인의 유량조절밸브, 압력조절밸브, 긴급차단밸브와 같이 작동요구에 대한 고장율(λ_d)에 대한 데이터가 있는 경우에는 요구 시 고장율이 그대로 PFD 값으로 이용된다.

$$PFD = \lambda_d \tag{2}$$

4.2 시간당 고장율을 가진 기기의 고장 모델식

주촉매펌프(P2103A)와 같이 시간에 따른 고장율 (λ_t)분포만 알려진 기기의 요구시 이용불능확률인 PDF(Probability of Failure on Demand)는 테스트 주기(t)사이의 모든 시점에서 작동요구가 일어날 가능성이 동일하다고 가정하여 다음과 같이 계산한다.

$$PFD = (1/T)\int_0^T 1 - e^{-\lambda_t t}\, dt \cong \lambda_t \times T/2 \tag{3}$$

4.3 자가진단기능(Diagnostics)이 있는 기기의 고장 모델식

PLC(Programmable Logical Controller) 시스템과 같이 고장이 발생하면 경보가 울려 즉시 탐지할 수 있는 기기들이 있다. 이러한 기기의 요구시 이용불능확률인 PFD(Probability of Failure on Demand)는 고장의 빈도와 기기를 보수하는데 걸리는 평균시간(MTTR: Mean Time To Repair), 그리고 자가진단에 의하여 고장이 발견되는 확률(DC: Diagnostic Coverage)에 관련되며 다음과 같이 계산된다.

$$PFD = (\lambda_t/2) \times T_{ce} \tag{4}$$

여기서

$$T_\alpha = (1 - DC) \times (T/2 + MTTR) + DC \times MTTR$$

이며, 고장발견확률(DC)은 0.95 (95%), 평균보수시간은($MTTR$) 8시간을 적용하였다.

4.4 공통원인에 의한 고장 모델식

동일한 기능을 가진 동일한 형태의 기기인 경우 다중으로 설치하면 시스템의 신뢰도는 증가하나 그 증가정도가 반드시 설치 대수에 비례하지는 않는다. 그 이유는 다중으로 설치된 두 대 이상의 기기가 동일한 원인으로 인하여 작동불능 상태가 될 가능성이 있기 때문이다. 본 분석에서 사용된 공통원인에 의한 고장 모델은 β_{Factor} Factor모델로서 공통원인고장으로 인한 요구시 이용불능확률인 PFD(Probability of Failure on Demand)는 다음과 같이 계산된다.

$$PFD = \beta \times \lambda_t \times T \tag{5}$$

여기서, 공통원인고장 인자 β는 요구 시 작동실패의 경우 0.1을 적용하였다.
여기서 계산에 사용한 축약어는 다음Table 10[14,16,19]과 같다.

Table 10. Abbreviation description used PFD calculation for basic event

Abbreviation	Description
t_1	Proof-test interval(hour)
$MTTR$	Mean time to restoration(hour)
DC	Diagnostic coverage(expressed as a fraction in the equations and as a percentage elsewhere)
β	The fraction of undetected failure that have a common cause (expressed as a fraction in the equations and as a percentage elsewhere)(assume $\beta \times \beta_D$)
β_0	Of those failure that are detected by the diagnostic tests. The fraction that have a common cause(expressed as a fraction in the equations and as a percentage elsewhere)
PFD_G	Average probability of failure on demand for the group of voted channels(If the sensor, logic or final element subsystem comprises of only one voted group, then PFD_G is equivalent to PFD_S, PFD_L, and PFD_{FE})
λ	Failure rate(per hour)of a anneal in a subsystem

λ_D	Dangerous failure rate(per hour)of a channel in a subsystem, equal to 0.5 λ(assumes 50% dangerous failure and 50% safe failure)
λ_{DD}	Detected dangerous failure rate(per hour) of a channel in a subsystem(this is the sum of all the detected dangerous failures rates within the channel of the subsystem)
λ_{DU}	Undected dangerous failure rate(per hour) of a channel in a subsystem(this is the sum of all the untected dangerous failures rates within the channel of the subsystem)
λ_{SD}	Detected safe failure rate(per hour) of a channel in a subsystem(this is the sum of all the detected safe failures rates within the channel of the subsystem)
t_{CE}	Channel equivalent mean down time(hour) for 1002, 1002 and 1003 architectures(this is the combined down time for all the components in the channel of the subsystem)
$t_{\geq}$	Voted group equivalent mean down time(hour) for 1002 and 2003 architectures (this is the combined down time for all the channel in the voted group)

5. 정량화수행 분석 결과

Safety Instrumented System(SIS)의 요구시 이용불능확률(Probability of Failure on Demand, PFD)을 계산하기 위하여 구성된 고장수목 정량화 결과를 Table 11에 사고추이별로 나타내었다. Table 12는 기본목록에 의한 각 기기별 평균 고장율을 정리한 것이다.

Table 11에서 Safety Instrumented System(SIS)의 요구시 이용불능확률(Probability of Failure on Demand, PFD) 은 점 추정치 7.31E-04로 계산되었으며, 압력스위치가 공통원인고장에 의해 요구시 이용불능되는 사건과 PLC(Programmable Logical Controller)가 공통원인 고장으로 요구시 이용불능사건의 Cut Set를 구해본 결과 각각의 기여도는 Table 11에 나타난바와 같이 72%와 24%로 가장 크게 영향을 미치는 사건으로 나타났다. 아울러 Safety Instrumented System(SIS)요구시 이용불능확률(Probability of Failure on Demand, PFD) 계산시 기본사건 자료의 불확실성분석에서 계산된 발생빈도에는 불확실성이 존재하게 되므로 정량화 분석결과에 대해서도 불확실성의 정도를 표현할 필요가 있다. 또한 Table 12는 기본 이벤트 목록과 관련된 페일세이프 시스템에 대한 정량화 결과이다.

Table 11. Quantification results of the final cutset.

No	Value (PFD)	f-v	acc	Cut set			Contribution
1	5.260E-004	0.7209	0.7209	CCFPASH			72.1%
2	1.730E-004	0.2371	0.9580	CCFPLC			23.7%
3	2.767E-005	0.0379	0.9959	PASH21602AA	PASH21602BA		3.8%
4	2.993E-006	0.0041	1.0000	PLCAF	PLCBF		0.4%
5	1.576E-011	0.0000	1.0000	P2103AF	XV21201O	PV21205O	FV21609O
Report for SIS value				7.297E-004			

Table 12. Quantification results for the failsafe system related to the basic event list.

Name	Mean	Description	Lamda	Remark
CCFPASH	5.26E-04	PASH 21602A/21602B fails to function on demand	5.26E-04	CCPS 2.1.4.1.3 and CCF 0.1
CCFPLC	1.73E-04	PLC fails to function on demand due to CCF	1.73E-04	OREDA 4.1.2 and CCF 0.1
FV21609O	2.20E-03	FV21609 fails to close on demand	2.20E-03	CCPS 3.5.3.3
P2103AF	1.48E-03	Pump(P2103A)fails to stop on demand	1.13E-07	KOSHARI PAGE E-19CCPS 1.4.1.3
PASH21602	5.26E-03	PASH 1602A fails to function on demand	4.00E-07	CCPS 2.1.4.1.3
PASH21602	5.26E-03	PASH 1602B fails to function on demand	2.93E-07	OREDA 4.1.2
PLCAF	1.73E-03	PLC A module fails to function on demand	2.93E-05	OREDA 4.1.2
PLCBF	1.73E-03	PLC B module fails to function on demand	2.93E-05	OREDA 4.1.2
PV21205O	2.20E-03	PV21205 fails to close on demand	2.20E-03	CCPS 3.5.3.3
XV21201O	2.20E-03	XV21201 fails to close on demand	2.20E-03	CCPS 3.5.3.3

Safety Instrumented System(SIS)의 요구시 이용불능확률인 PFD(Probability of Failure on Demand)의 정량화 결과에 대하여 몬테카를로(Monte Carlo)방법을 사용하여[19-21] 불확실성의 분석을 수행하였다. 불확실성분석을 위해 각 기본사건의 분포를 대수정규분포로 간주하여 입력하였고 오차인자는 불확실성이 너무 크지도 혹은 작지도 않다고 가정하여 3을 할당하여 계산한 중요도 결과는 Table 13과 같다. 또한 확률밀도함수로 Figure 6에 나타내었다. Table 14에서 일 수 있듯이 SIS(Safety Instrumented System)의 이용불능확률은 매우 비관적일 경우 1.52E-03이며 매우 낙관적일 경우 2.83E-4의 빈도를 갖는다고 추정할 수 있다.

Table 13. Event importance information.

No	event	mean	f-v	rrw	raw	pd
1	CCFPASH	5.260e-004	0.7209	3.5871	1370.78	1.0000
2	CCFPLC	1.730e-004	0.2371	1.3108	1371.26	1.0000
3	PASH21602BA	5.260e-003	0.0379	1.0394	8.17	0.0053
4	PASH21602AA	5.260e-003	0.0379	1.0304	8.17	0.0053
5	PLCAF	1.730e-003	0.0041	1.0041	3.37	0.0017
6	PLCBF	1.730e-003	0.0041	1.0041	3.37	0.0017
7	P2103AF	1.480e-003	0.0000	1.0000	1.00	0.0000
8	XV21201O	2.200e-003	0.0000	1.0000	1.00	0.0000
9	PV21205O	2.200e-003	0.0000	1.0000	1.00	0.0000
10	FV21609O	2.200e-003	0.0000	1.0000	1.00	0.0000

F-V : Fussel-Vesely 중요도(해당 기본사건이 포함되는 모든 최소 단절군 빈도의 합과 전체 빈도의 비로 정의

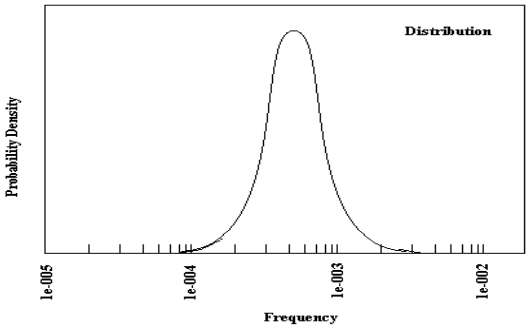

Fig. 6. Probability density function of SIS for PFD

Table 14. Result of inaccurate analysis.

Classification	Frequency
5%	2.83E-4
50%	6.50E-4
Mean	7.31E-4
95%	1.52E-3
point estimation value	7.30E-4

6. 결론

HDPE(High Density Polyethylene) 플랜트의 중합공정에서 폭주반응 등의 원인으로 반응기 R-2103 과 후단라인에 과압 사고가 발생할 경우를 대비하여 설치된 SIS(Safety Instrumented System)의 신뢰도를 고장수목분석을 사용하여 분석한 결과 SIS에 대한 점 추정치 PFD는 7.30E-4로 계산되었고, SIS(Safety Instrumented System)의 요구시 이용불능확률인 PFD(Probability of Failure on Demand)는 2.83E-4와 1.52E-3의 범위 안에 존재하는 것으로 계산되어 SIS(Safety Instrumented System)의 신뢰도는 SIL(Safety Integrity Level)3등급을 만족하고 있다고 보여지며 위와 같은 결과를 종합하여 볼 때 SIS(Safety Instrumented System)의 신뢰도가 압력방출밸브가 요구되는 안전건전성수준(Safety Integrity Level, SIL)으로 설계되어있다고 판단된다. 아울러 안전장치 및 제어 시스템에서 발생하는 고장을 감소시키기 위해 IEC(International Electrotechnical Commission)와 ISA(Instrument Society of America)에서 "SIS(Safety Instrumented System) 표준"을 개발하여 활용하고 있는바 이를 실행하려면 우선적으로 시스템에 대한 SIL(Safety Intergrity Level) 설정이 필요하다. 그러나 SIL을 정성적인 분석방법으로만 결정할 경우 이에 따른 막대한 사회·경제적 피해가 발생할 수 있다. 따라서, 이에 따른 문제점을 해결할 방안으로 정량적인 FTA를 활용한 고장율 분석을 통한 반정량적 방법(정성적+정량적)을 제시하고 적용함으로서 향후 선제적이고 안정적인 유지, 보수를 위한 관리 기준방향을 설정함으로서 각종 산업공정에서 발생할 수 있는 위험을 최소화 하는데 중요한 역할을 하리라 기대한다 .

References

[1] Korea Occupational Safety and Health, "Serious accidents cause statistical analysis", *Korea Occupational Safety and Health Risk Management Center*.2012. https://www.kosha.or.kr/kosha/data/industrialAccidentCause.do

[2] IEC-61508-1, "Functional Safety of Electrical/ Electronic/Programmable Electronic Safety-related Systems Part 1, General Requirements," *International Electro-technical Commission, Apr. 92000*, 2000. https://webstore.iec.ch/preview/info_iec61508-1%7Bed2.0%7Db.pdf

[3] IEC-61508-6, "Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-related Systems Part 6, Guidelines on the application of IEC 61508-2 and IEC 61508-3", *International Electro-technical Commission, Apr*, 2000. https://webstore.iec.ch/p-preview/info_iec61508-6%7Bed1.0%7Db.pdf

[4] E. D. Jung, B. C. Ma, "Research Trends on Safety Integrity Level", The Korean Institute of Chemical Engineering, *2022 Spring Conference Proceeding*, pp396-396, 2022. https://www.kiche.or.kr/files/2022SAbstract.pdf

[5] Y.E.Choi,H.S.Oh,"A study on safety integrity level evaluation and management methods based on IEC 61508", The Korean Society for Railway, *2022 Autumn conference proceedings*, pp 45-45, 2022.
https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE11155397

[6] J. Y. Park, S. G. Jeon, S. G. Park, "IEC61508 SIl Controller", The Korean Society for Railway, *2022 Spring conference proceedings*, pp 40-41, 2022.
https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE11113970

[7] J. H. Park, "The Research on Improvement on Hydrogen Fueling Protocol by HAZOP & LOPA", Soongsil University, *Master's thesis at General Graduate*, 2021.
DOI:https://doi.org/10.31333/kihm.2022.10.1.82

[8] H. Kang, "Automated Synthesis and Design of Safety Instrumented Systems for Toxic Gas Processes", Myongji University, *Master's thesis at General Graduate*, 2016.

[9] G. M. Kim, "Case Study on SIL Analysis of IEC 61508 Safety Level Controller" Korea Reliability Application Research Society, *Journal of the Reliability Application Research*, Vol.16, No.3, pp 231-237, 2016.
https://www.dbpia.co.kr/Journal/articleDetail?nodeId=NODE07020876

[10] H. G, Yang, J. W Lee, "A Study on Signal Function SIL Allocation Using Fuzzy Risk Graph", The Korean Society for Railway, *Journal of the Korean Railway Society*, Vol.19, No.2 pp.145-158, 2016.
https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE06671670

[11] S. K. Kim, Y. S. Kim, "A study on the safety life cycle of IEC 61508 for functional safety", The Korea Reliability Application Research Society, *Journal of the Korean Reliability Application Research*, Vol.14, No.1, pp 81-91, 2014.
https://www.uci.or.kr/?menuno=8
UCI : G704-SER000010073.2014.14.1.008

[12] H. M. Kwon, H. C. Park, Y. W. Chun, "Application direction of Safety Integrity Level to improve public safety", The Korean Society of Safety, *Journal of the Korean Society of Safety*, Vol.27, No.5, pp 64-69, 2012.

[13] IEEE, "Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear Power Generating Stations", IEEE std-500-1983, *The Institute of Electrical and Electronics Engineers*.1993.
DOI:https://doi.org/10.1109/IEEESTD.1983.81548

[14] CCPS, "Guidelines for Process Equipment Reliability Data", *CCPS for American Institute of Chemical Engineers* .1989.
DOI:https://doi.org/10.1007/978-3-642-83721-0_9

[15] "Offshore Reliability Data, 3rd Edition, OREDA-97", *SINTEF Industrial Management, Norway,* 1997.
https://www.cheric.org/files/research/ip/p200309/p200309-301.pdf

[16] "Reliability Data for Safety Instrumented Systems., PDS Data Handbook, Edition", *SINTEF Industrial Management, Norway,* 2004.
https://www.sintef.no/en/publications/publication/1267544/

[17] KIRAP-KWTREE Beta 1.0, "Fault Tree Editor for Windows User manual", *Korea Atomic Energy Research Institute*, 1996.

[18] "Fault Rree with Aerospace", Version 1.1, *Nasa Publication, August 2002.*

[19] ISA-84.01, "Application of Safety Instrumented Systems for the Process Industries", *Instrument Society of America,* 1996.

[20] KEPCO, "Advanced Light Water Reactor Utility Requirements Document (Volume III) Chapter 1, Appendix A, PRA Key Assumptions and Groundrules", *Electric Power Research Institute, Inc*, 1995.

[21] Crarnwood, "Functional Safety and safety integrity", *The Institution of Gas Engineering and Manager, Revision A,* 2002.

고 재 선(Jae-Sun Koh) [정회원]

- 2005년 2월 : 서울시립대학교 대학원 화학공학과 (공학박사)
- 2009년 3월 ~ 2011년 2월 : 대전대학교 소방방재학과 조교수
- 2011년 3월 ~ 2012년 2월 : 소방방재청 국립방재교육연구원 교수
- 2012년 3월 ~ 현재 : 호원대학교 소방안전학과 교수

〈관심분야〉
화재폭발 및 위험성평가