



석유 화학플랜트 안전시스템의 해석 및 설계

조 성 호 / 삼성엔지니어링
livevil@empal.com

1. 서론

최근 석유 화학플랜트 운영과 관련하여 제품 생산의 효율을 높이기 위해 신기술을 적용하며 포화 상태인 석유 화학제품 시장에서 가격 경쟁력을 높이기 위해 노력을 하고 있다. 동시에 대규모의 자본이 투자된 석유 화학플랜트에서 사고가 발생한다면 막대한 금전적 손실이 발생하므로 안전성 확보도 최우선 사항으로 고려해야 한다. 따라서 공장 운전 효율은 최대한으로 끌어 올리면서도 플랜트 안전 관련 요구사항도 만족시키기 위해 공장 운전 효율과 안전 관련 사항을 서로 적절한 수준에서 맞추어야 하는데 이는 과도한 안전 요구 사항은 잦은 검사와 확인으로 운전 효율을 낮추기 때문이다.

2. 석유 화학플랜트의 안전성

2.1 석유 화학플랜트 내의 위험

석유 화학플랜트 내의 위험은 플랜트를 위태롭게 만드는 사고의 발생 빈도와 발생 시 피해의 규모의 척도이며, 아래에 플랜트 내에 발생할 수 있는 위험들에 대한 분석을 통해 그 정도를 판단할 수 있다.

- 프로세스 상 또는 장치 상의 위험스러운 사고
- 위험스러운 사고를 유발하는 연속적인 사고
- 위험스러운 사고와 관련되어 있는 프로세스상의 위험
- 위험을 필요 수준까지 감소시키기 위한 안전조치 기능
- 안전조치 기능에 계기가 필요한지 여부

이러한 판단을 위해 사전에 위험스러운 사고를 유발하는 요인들에 대한 설명, 사고의 빈도 및 발생 시 피해의 정도, 정상 운전 또는 플랜트 보수 시에 대한 고려사항, 추가적인 위험 감소를 위한 요구사항들에 대해 조사, 위험 분석 시 필요한 데이터들의 가정조건들의 조건들에 대한 조사도 병행되어야 석유 화학플랜트 내의 위험에 대해 정확한 판단이 이루어진다.

2.2 안전 관련 국제 규격

안전 관련 대표적인 국제 규격은 3개가 있다. IEC 61508은 안전시스템의 Manufacturer나 Supplier들을 위한 규격이고, IEC 61511은 안전시스템의 Designer, Integrator, User를 위한 규격이다. ANSI/ISA-S84.00.01는 미국이나 캐나다에서 적용하고 있으나 이 규격도 IEC 61508의 프로세스 부문의 적용을 위한 것으로 IEC 61511과 동일한 내용이다.

2.3 기존 석유 화학플랜트의 안전성 분석 예

(1) 울산 메셀로스 증설 프로젝트

① 위험 분석

과도한 반응의 결과는 반응기 내부의 압력과 온도의 급격한 상승을 수반하는데 메셀로스 합성 중 반응기 내부에서 과도한 반응이 발생할 수 있는 경우는 아래와 같다.

- 경우 1 : 반응 물질의 과다 투입
- 경우 2 : 반응 온도 조절의 실패.



- 승온을 위한 Steam의 과다 투입 또는 관련 Valve의 조절 실패
- COOLING WATER 실패
- 경우 3 : 기타 원인을 알 수 없는 이상 반응.

② 안전성 분석

반응 상태를 확인하기 위해 설치된 대부분의 계측기(온도, 압력계)가 이중으로 구성되어 있으며, 반응물 투입부터 반응, 제품 배출까지 전체 순차 반응 과정이 자동화 시스템으로 구축되어 있어 운전자 실수로 인한 실패가 발생할 가능성을 제거하였으며, Cooling Water 실패를 방지하기 위해 5기의 펌프와 열병합 발전의 예비 시스템이 구성되어 있어 Cooling Water 실패 가능성을 극도로 낮춘 상태이다.

③ 분석내용의 판단

위험 분석 후 안전성 분석을 장치 고장률과 같은 객관적 데이터를 사용하지 않고 많은 장치를 사용하였으므로 안전하다고 주관적으로 분석하고 판단하였고 하드웨어적으로 설치한 안전시스템 설계의 정당성 및 유효성을 증명할 수 없다. 따라서 위험방지를 위해 상당히 노력하였으나 플랜트가 안전하다고 증명할 수 없다.

(2) 사우디 PDH/PP 프로젝트

① 안전 시스템 설계

사우디 PDH/PP 플랜트의 Licensor에 의해 위험 분석된 모든 경우에 대해 안전 등급 3에 맞는 안전 시스템을 요구하여 안전 등급에 상관없이 무조건 Sensor는 3개, Logic Solver는 TMR (Triplicated Modular Redundant), Final Element는 2개를 사용하였고 1년마다 부분 테스트를 실시해야 한다.

② 설계내용의 판단

정확한 위험 분석에 따른 안전 등급의 결정으로

안전 시스템의 설계가 이루어 지지 않고 안전 등급에 상관없이 많은 하드웨어를 사용하여 불필요한 금액이 추가로 사용되었으며, 충분히 안전성을 확보하였으나 추가로 1년마다 부분 테스트를 실시해 운전 효율성을 낮추는 결과를 가져올 수 있다.

3. 안전 등급

3.1 안전 등급 기준

안전 등급(SIL, Safety Integrity Level)은 일정 기간 내에 안전시스템이 위험 방지 기능을 정확하게 수행할 수 있는 확률의 등급을 말한다. 안전 등급이 높을수록 요구되어진 기능을 잘 수행할 확률이 더 높아지며, 이용 가능성(Availability, 어떤 시간대에 시스템이 정상적으로 작동하는 확률)과 시스템의 구성의 요구 사항이 증가한다. 안전 등급은 1부터 4까지 있으며 등급 4가 가장 높고 등급 1이 가장 낮다.

(1) 요구 고장 확률 개념과 계산

① 신뢰도

신뢰도(Reliability)란 기기가 작동 기간 중에 그 기능을 충족시키는 능력을 의미한다. 그러나 수치화하기가 아주 까다로워 MTBF(Mean Time Between Failure)라는 정의가 종종 신뢰도를 측정하는 방법으로 채택된다. 이것은 가동 중인 시스템에 의해 통계학적으로 또는 사용된 부품의 고장률로 계산된다. 신뢰도는 시스템의 안전과는 무관하다.

② 이용가능성

이용가능성(Availability)이란 시스템이 정상적으로 작동하는 확률이다. 이것은 MTBF와 MDT(Mean Down Time)를 이용하여 구해진다.

MDT는 고장 감지 시간(Fault detection time)과 모듈 시스템의 경우 장애 모듈 교체에 필요한 시간으로 구성된다. 따라서 시스템의 이용가능성



은 MDT가 짧아짐에 따라 크게 증가된다. 이용가능성은 이중화(Redundancy) 또는 삼중화(Triplicated)로 시스템을 구성하면 증가될 수 있다.

③ 고장률

고장률(Failure rate, λ)은 식 (1)과 같이 False trip의 원인의 되는 λS 와 안전시스템이 위험한 상황에 대응하지 못하게 하는 λD 의 합으로 구해진다.

$$\lambda = \lambda S + \lambda D \quad (1)$$

또한 각 고장률 λS 와 λD 는 detected와 undetected로 나누어져 식 (2)와 식 (3)으로 자세히 구분되어진다.

$$\lambda S = \lambda SD + \lambda SU \quad (2)$$

$$\lambda D = \lambda DD + \lambda DU \quad (3)$$

④ 요구 고장 확률

요구 고장 확률(PFD, Probability of Failure on Demand)를 구하는 방법 중에 비신뢰성

(Unreliability) 접근 방법으로 설명하겠다. 비신뢰성(Unreliability)은 장치의 특정 시간(Proof test interval)의 간격과 고장률(Failure rate) 간의 함수식으로 식 (6)과 같다. 이러한 관계를 일정한 고장률(Failure rate, λ)을 가진 싱글 채널 시스템에 대해 식으로 나타내면 failure rate는 식 (4), reliability는 식 (5), unreliability는 식 (6)으로 표현된다.

$$\lambda(t) = \lambda \quad (4)$$

$$R(t) = e^{-\lambda t} \quad (5)$$

$$F(t) = 1 - e^{-\lambda t} \quad (6)$$

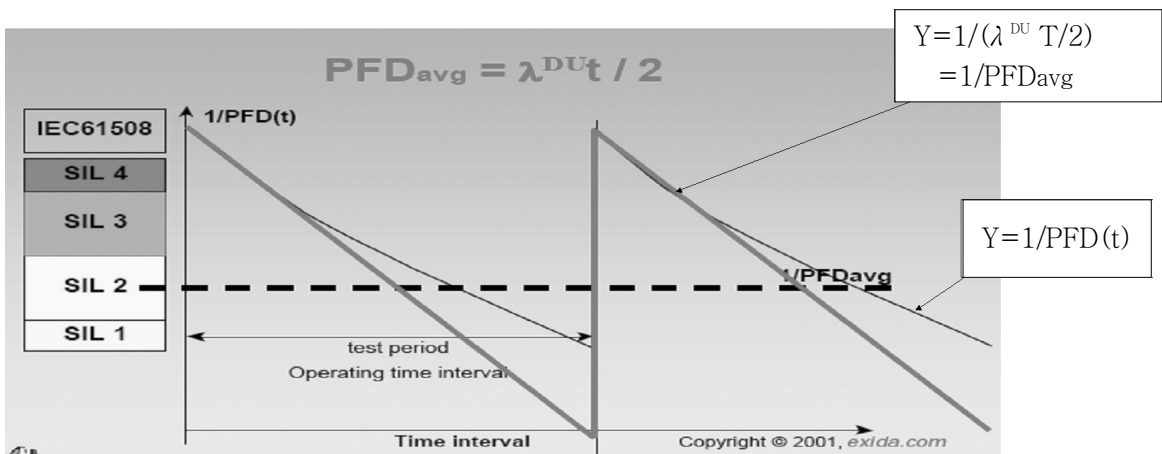
위의 식 (6)은 아래와 같은 방법으로 간략하게 될 수 있다.

$$e^X = 1 + X + \frac{X^2}{2} + \frac{X^3}{3} + \frac{X^4}{4} + \dots \approx 1 + X \quad (7)$$

$$e^{-\lambda t} = 1 - \lambda t \quad (8)$$

$$F(t) = 1 - e^{-\lambda t} = 1 - (1 - \lambda t) \approx \lambda t \quad (9)$$

따라서 요구 고장 확률 평균값(PFDavg)은 그림 1과 같이 검사 주기 동안의 비신뢰성



[그림 1] 요구 고장 확률 평균값의 기본 개념



(Unreliability) 값의 평균으로 식 (10)으로 구해진다. 여기서 장치는 주기적인 시험 및 검사를 통해 위험 요소를 감지하고 완벽한 상태로 새롭게 된다고 가정한다.

$$PFD_{avg} = \lambda_{DU} \frac{t}{2} \quad (10)$$

3.2 안전 등급 수준

사우디 에틸렌 플랜트는 안전 등급의 수준 결정을 위해 이중 위험 매트릭스를 사용하므로 여기서는 위험 매트릭스에 대해서만 설명하겠다. 위험 매트릭스는 세 가지 위험 변수, 빈도(Frequency), 결과(Consequence), 점유기간(Occupancy)과 위험 감소를 위한 독립적 위험 방지 설비 (IPL,

Independent Protection Layers)로 구성되어 있다. 이 요소들이 위험 매트릭스의 변수로 되어 있어 분석된 위험 변수를 대입하면 쉽게 안전 등급의 수준을 얻을 수 있다.

(1) 위험 매트릭스

표 1에서 보면 위험 매트릭스는 (2)항으로부터 얻은 위험의 결과(Consequence)가 X-축, 위험의 빈도(Frequency)가 Y-축의 조합으로 안전등급의 수준을 구한다.

(2) 위험의 빈도

위험 빈도(Frequency)는 안전시스템이 없을 경우 위험한 사고가 일 년간 발생한 횟수이다. 빈도는 표 2와 같이 다섯 가지의 등급으로 나눌 수 있다.

<표 1> 위험 매트릭스

		Consequence				
		1	2	3	4	5
Frequency	4	no action	change design b) (SIL 1)	change design b) (SIL 3)	change design c) (SIL 4)	change design c) (SIL 4)
	3	no action	a) (SIL 0)	Medium SIL 2	High SIL 3	change design c) (SIL 4)
	2	no action	a) (SIL 0)	Low SIL 1	Medium SIL 2	High SIL 3
	1	no action	no action	a) (SIL 0)	Medium SIL 2 d) (10E-2)	Medium SIL 2
	0	no action	no action	no action	Low SIL 1	Low SIL 1

<표 2> 위험에 대한 위험 빈도

		Return period (x times per year)		Demand Rate (every x year)
Frequency	likely	4	> 2	< 0.5
	frequent	3	2 to 0.25	0.5 to 4
	probable	2	0.25 to 0.05	4 to 20
	remote	1	0.05 to 0.01	20 to 100
	improbable	0	0.01 <	100 >



(3) 위험의 점유기간

위험 점유 기간(Occupancy)은 위험한 사고 발생 시 외부에서 위험에 노출될 확률이며 이는 근무 시간동안 사고 발생 가능 지역에 머무르는 시간의 비율로 계산되어질 수 있다. 이 확률은 0.2 또는 1로 나타낸다. 이때 만약 0.2 이하이면 위험 매트릭스에서 Y-축인 위험 빈도의 등급을 한 등급을 낮춘다.

(4) 독립적 위험 방지설비

독립적 위험 방지 설비(IPL, Independent Protection Layer)는 다른 설비에 의존하지 않고 하나의 자체 설비로만으로 위험을 방지하는 안전 조치를 취할 수 있는 설비를 말한다. 따라서 IPL 1은 안전 등급 1과 동일하게 취급되어 위험 매트릭스에서 한 단계 안전등급의 수준을 낮출 수 있다.

하지만, 운전자의 조치는 IPL 1으로만 간주할 수 있고 그 이상은 자세한 운전 절차의 명기나 연구가 이루어져야 한다. 표 3은 여러 독립적 위험 방지 설비를 나타내었다. 일반적으로 표 3의 여러 위험 방지 설비가 같이 사용되어 안전 등급을 낮추게 된다.

4. 안전시스템의 구성

4.1 안전시스템의 구성요소

안전시스템은 플랜트 내에서 아무런 조치를 취하지 않으면 증가하는 위험 발생 확률을 낮추거

나, 사고 발생 시 치명적인 결과를 완화시키기 위한 조치를 하는 시스템이다.

안전시스템은 Sensor(s), Logic Solver(s), Final Element(s), 세 가지 요소의 조합으로 구성된다.

- Sensor(s) : 프로세스 조건을 측정하기 위한 장치 (예, transmitters, transducers, process switches, position switches)
- Logic Solver(s) : 하나 이상의 Logic 기능을 수행하는 장치 (예, electrical systems, electronic systems, programmable electronic systems, pneumatic systems, hydraulic systems)
- Final Element(s) : 안전한 상태로 만들기 위해 필요한 물리적 작동을 하는 장치 (예, valves, switch gear, motors including their auxiliary elements)

Sensor나 Final Element는 transmitter나 valve처럼 하나의 장치이므로 안전 등급에 따른 사양 선정에 별다른 어려움이 없이 쉽게 결정할 수 있으나 Logic Solver는 안전 등급에 따라 결정하는데 구조에 대한 이해가 필요하다. 따라서 안전 시스템 사양 결정에 앞서 Logic Solver 구조에 대해 알아보겠다.

(1) Logic Solver의 구조

Logic 기능을 수행하는 장치인 Logic Solver의

<표 3> 독립적 위험 방지 설비

Prevention / Mitigation Measures	IPL
Independent SIS having SIL 1	1
Independent SIS having SIL 2	2
Independent SIS having SIL 3	3
Safety valves or rupture disk	3
Swing check valve or nozzle check valve	1
Lift check valve (ball or piston) or dual plate check valve	0.5



구조는 대략 아래 7가지로 구분할 수 있다.

- 1oo1 (1 out of 1)
- 2oo2 (2 out of 2)
- 1oo2 (1 out of 2)
- 1oo2D (1 out of 2D, D는 TUV에서 인정하는 높은 자가진단 기능)
- 2oo3 (2 out of 3)
- 1oo3 (1 out of 3)
- 2oo4 (2 out of 4)

이러한 Logic Solver의 구조에 대해서 TUV에서 제시하는 시스템 반응은 표 4와 같다. 표 4에서 보면 일반적으로 단일 채널로는 AK 6의 기준을 맞추지 못한다. 그러나 아주 드문 경우에 프로세스 Shutdown 그 자체가 매우 위험하거나 잘 정의된 Shutdown Sequence를 따라야 하는 경우가 있다. 이러한 경우엔 Shutdown Sequence 상태에서 단시간 단일 채널 운전으로 안전등급의 감소는 추가적인 조치사항으로 보충될 수 있다. 단일 채널로 운전 가능한 최대 시간은 프로세스에 따라 다르며, 적용에 따라 일일이 시간이 명기되어야 한다. 명기된 시간은 인증서에 의해 보장되는 최대 시간을 의미한다. AK 5의 경우는 72 시간이고, AK 6인 경우 즉시 Shutdown된다. 하지

만, 특별한 경우에는 1시간까지 연장되기도 한다. 그러나 TUV 요구사항 AK 6 / SIL 3 인 경우에는 운전 시간제한이 없다.

(2) 이중화 시스템

이중화 시스템(Redundant or Fault-Tolerant System)은 안전성 배열(Safe Configuration, 2->0) 또는 이용가능성 배열(Available Configuration, 2->1->0)로 적용할 수 있다. 안전성 배열은 고장 허용은 가능하지 않고 어느 한 쌍이 고장 났을 경우 시스템의 문제만으로 전체 혹은 부분 공정의 종료를 유발한다. 그렇기 때문에 이러한 배열은 대단히 안전하지만 이용가능성 면에서 상당히 떨어진다. 실제로 안전성 배열로 된 이중화 시스템은 안전성에서는 삼중화 시스템보다 3배 이상 높지만 이용가능성 면에서는 상당히 비효율적이다. 이런 이용가능성과 안전성 문제를 해결하기 위하여 이중화 시스템에 자기진단기능을 부합시켜 자기진단기능을 포함한 이용가능성 배열(1 out of 2D)이 개발되었다.

(3) 삼중화 시스템

삼중화 시스템(TMR, Triplicated Modular Redundant System)은 안전제어 시스템으로 가장

<표 4> TUV에서 제시하는 시스템 반응

Configuration	TUV approved operating Mode w/Restrictions	TUV Class Approval for Safety	Nuisance Trip Rate		TUV Time Requirements for Repair of Logic Solver
			High	Low	
1oo2	2-0	AK 5,6	0		NA
2oo2	Not approved	Not approved		0	NA
1oo2D	2-1-0	AK 5	0		72 Hours
1oo2D	2-0	AK 6	0		Note
1oo3	3-0	AK 5,6	0		NA
2oo3	3-2-1-0	AK 5,6		0	1500 Hours
2oo4	4-2-0	AK 5,6		0	NA



보편적으로 알려져 있고, 일반적으로 선호되고 있는 시스템이다. 삼중화 시스템은 안전성과 이용가능성을 모두 제공하지만 시스템 특성상 3→2→0 배열로 작동한다. 삼중화 시스템은 투표(Voting)와 정상적인 상태에서의 비교로 작동된다.

삼중화 시스템은 자기진단기능이 충분하지 않기 때문에 단일채널이 고장 났을 경우 작동 시간에 제한이 있다. 이 시간제한은 공정상 차이가 있으며, 대체적으로 1시간에서 1500시간이다. 또한 이중화 시스템과 비교해서 초기비용이 비싸고 작동기간 비용이 상대적으로 많이 드는 편이다.

(4) 사중화 시스템

사중화 시스템(QMR, Quadruple Modular Redundant System)은 Pair-and-Spare 구조로 각 중앙 모듈은 두개의 프로세서를 보유함으로써 네 개의 프로세서가 로직을 수행한다. 한 개의 중앙 모듈이 입력 읽기를 수행하고 이 결과를 다른 중앙 모듈로 전달한다. 두개의 프로세서를 갖는 각 중앙 모듈은 로직을 수행하며 그 결과를 비교한다. 그리고 나서 각 중앙 모듈의 결과가 다시 비교된다. 모든 비교가 완료 되면 입력 읽기를 수행했던 중앙 모듈이 그 결과를 출력에 기록한다. 다음 사이클에서는 다른 중앙 모듈이 입력 읽기와 출력 쓰기를 수행한다. 이 방식은 이중화 시스템에서 진단 기능이 문제점을 찾지 못 할 때 두 개 프로세서가 동시에 정지되는 고유의 신뢰도 문제를 해결 한다.

4.2 안전시스템의 사양

안전등급에 따른 안전 시스템의 하드웨어 수량은 실패 허용 수량에 따라 결정된다. 여기서 실패 허용 수량이란 하드웨어의 오류가 발생한 상황에서 하에서도 위험 예방 조치를 계속 수행할 수 있는 최소한의 수량을 말한다. 즉, 실패 허용 수량 “1”이란 하드웨어 1개가 고장이 나도 위험 예방 조치를 계속하기 위한 최소의 수량인 2개의 하드웨어로 구성해야 한다는 의미이다. 예를 들어 실패 허용 수량 “1” 이면 Sensor 는 2개, Logic Solver 는 1oo2, Final Element는 2개를 최소한 사용해야 한다. 실패 허용 수량 “2” 이면 Sensor는 3개, Logic Solver는 삼중화 또는 사중화 시스템 구조, Final Element는 3개를 최소한 사용해야 한다.

(1) IEC-61511 에 의한 사양

① 로직솔버

IEC-61511에 의한 Logic Solver의 수량 기준은 표 5와 같다. 표 5는 SFF 값이 90% 이상인 Logic Solver를 사용한다면 안전등급 3 에서도 최소 실패 수량이 1 이므로 하드웨어가 2개로 구성되어야 하므로 이중화 시스템을 사용하면 된다는 뜻이다. 즉 앞에서 설명한 표 5의 1oo2D, 이중화 시스템 구조 이상을 사용하면 된다. 반면 SFF 값이 60%에서 90% 이상인 Logic Solver는 안전등급 3에서는 최소 실패 수량이 2 이므로 하드웨어가 3개가 구성되어야 하므로 삼중화 또는 사중화 구조 시스템을 사용해야 한다. 여기서 SFF

<표 5> IEC-61511 에 의한 로직 솔버의 수량 기준

SIL	Minimum hardware fault tolerance		
	SFF < 60%	SFF 60% to 90%	SFF > 90%
1	1	0	0
2	2	1	0
3	3	2	1
4	Special requirements apply (IEC-61508)		



(Safe Failure Fraction)는 고장 중에서 안전한 고장의 비율을 의미하며 식 (11)로 구해진다.

$$SFF = \frac{(\lambda_{SD} + \lambda_{SU} + \lambda_{DD})}{(\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU})} \quad (11)$$

② 센서와 최종 구성요소

IEC-61511에 의한 Sensor와 Final Element의 수량 기준은 표 6과 같다. 표 6은 안전 등급 3에서는 최소 실패 수량이 2 이므로 하드웨어가 3개로 구성되어야 한다. 즉 Sensor나 Final Element가 모두 3개씩 설치되어야 한다. 그러나 이런 조건은 한 배관 라인에 밸브가 연속으로 세 개가 설치되는 것이므로 상당히 과도한 안전 요구 사항이라 할 수 있다. 따라서 IEC-61511에서는 아래 4가지 조건을 모두 만족하면 표 6의 실패 허용 수량에서 하나를 줄일 수 있도록 허용하고 있다.

- Prior Use 로 정의된 하드웨어 선택
- 오직 프로세스에 관련된 요소만 조정 가능한 하드웨어 선택
- 프로세스에 관련된 요소 조정 시 보안 가능한 하드웨어 선택
- 안전등급 4 보다 낮은 곳에서 사용

4.3 안전등급의 확인

결정된 안전등급의 수준에 따라 선정된 안전시스템의 사양이 정말로 안전 등급의 요구 확률을 만족하는지 확인해야 한다. 안전시스템의 세 가지 요소인 Sensor(s), Logic Solver(s), Final Element(s)

모두 자체 요구 고장 확률을 가지고 있는데 식 (12)와 같이 세 요소의 요구 고장 확률 총 합이 안전등급이 요구하는 확률 이하이어야 한다.

$$PFD_{AVG} = PFD_{SE} + PFD_{LS} + PFD_{FE} \quad (12)$$

만약 안전등급 요구 확률보다 세 가지 요소의 실패 확률 총 합이 이를 초과할 경우 안전시스템 하드웨어의 수량 또는 액서 세리를 추가하여 확률을 낮추거나, 테스트 간격을 보통 적용하는 1년보다 더 짧게 줄여서 실패 확률을 낮추는 방법 등으로 요구되어지는 안전등급 확률 이하로 반드시 낮추어야 한다.

5. 안전시스템의 적용

5.1 적용 대상

(1) 대상 프로젝트

삼성엔지니어링이 수행한 기존 PDH/PP 공장부지내 연간 1,000,000톤 에틸렌 및 연간 200,000톤 프로필렌을 생산하는 사우디 에틸렌 플랜트의 건설 사업에 적용한다.

(2) 에틸렌 플랜트의 공정 개요

에틸렌 공정은 원료의 분해공정, 급냉공정, 압축공정 그리고 정제공정으로 나누어진다. 원료인 에탄, 프로판 가스를 외부 버너로 가열된 분해로의 반응관을 희석증기와의 혼합 기체 상태로 통과시키면 열분해 가스를 얻게 된다. 반응관 출구에서

<표 6> IEC-61511에 의한 Sensor와 Final Element의 수량 기준

SIL	Minimum hardware fault tolerance
1	0
2	1
3	2
4	Special requirements apply (IEC-61508)



의 열분해 가스의 온도는 보통 섭씨 750 ~ 850 °C, 압력은 0.5 기압 정도이다.

급냉공정에서는 열 회수와 동시에 75기압에 해당하는 고압증기를 발생시켜 공장 내의 분해가스 압축기나 냉동기의 동력원으로 유효하게 이용한다. 열분해 가스는 급냉탑에서 중질유 및 물이 분리된 후 압축공정에서 36기압까지 승압한다.

압축공정에서는 분해가스에 포함된 황화수소, 이산화탄소 등과 같은 부식성 물질을 수산화나트륨 수용액을 이용하여 제거한다. 저온 정제 공정의 배관계통의 막힘을 방지하기 위해 분자체와 같은 흡착제를 통과시킴으로써 분해가스 내의 수분을 제거한다.

정제공정에서는 탈수된 분해가스를 -40 ~ -100 °C의 범위까지 냉각시켜 에틸렌, 프로필렌을 비롯한 혼합 C4류, 가솔린 등을 분리하게 되며 이 중 혼합 C4류는 재순환되어 프로판과 함께 분해로에 주입된다.

5.2 안전시스템 설계

현재 사우디 에틸렌 프로젝트는 초기 설계 단계를 진행 중이어서 P&ID, 각종 설계 기본 개념 등을 정립하기 위해 사업주와 Licensor와 계약서 기준으로 계속 검토 및 협의를 하는 중이다. 따라서 아직 위험 분석 및 평가는 이루어 지지 않은 상태이나 안전시스템의 설계와 관련하여서는 사업

주, Licensor와 안전시스템의 기본 사양만 협의 완료하여 결정되어 있는 상태이다. 이는 앞서 설명한 위험 분석 및 평가 후 안전등급을 정하고 그에 맞는 안전시스템 사양을 정하는 정석과는 다른 진행인데 사우디 에틸렌 프로젝트가 대형 프로젝트 임에도 불구하고 36개월로 공기가 짧아서 초기 P&ID 확정이 가장 큰 관건인 프로젝트이기 때문이다. 여기서는 사전에 정해진 안전시스템의 사양에 대한 설명과 내부적으로 사양에 따른 등급 확인 절차를 통해 상세 설계된 최종 안전시스템의 사양을 설명하겠다.

(1) 안전시스템의 사양

사우디 에틸렌 프로젝트의 안전시스템의 기본 사양은 IEC-61511에 의한 방법과 계약서를 기준으로 표 7과 같이 결정하였다.

(2) 안전등급 확인

먼저, 사우디 에틸렌 프로젝트가 과거 수행하였던 프로젝트와 가장 특이한 조건은 5년 동안 연속 운전을 해야 한다는 것이다. 이 의미는 테스트 간격이 5년에 한번 해야 한다는 뜻인데 이에 대해 Sensor나 Logic Solver 계약서에 의거하여 등급에 상관없이 다수의 계기와 고 사양을 사용하여 문제가 없으나 Final Element의 경우 안전등급에

<표 7> 사우디 에틸렌 프로젝트의 안전시스템의 기본 사양 결정

SIL	Sensor	Logic Solver	Final Element	
1	2oo3 (Contractual requirement even though IEC-61511 requirement)	SIL 3 Certificate QMR	1oo1	Shut Down Valve
2	2oo3 (Contractual requirement even though IEC-61511 requirement)	SIL 3 Certificate QMR	1oo1	Shut Down Valve
3	2oo3 (Contractual requirement even though IEC-61511 requirement)	SIL 3 Certificate QMR	1oo2 (1oo1)	1st Shut Down Valve 2nd Control Valve



따른 수량보다 더 많이 설치해야만 하거나, 배관 라인에 By-Pass 라인을 추가로 설치해야 하는 경우가 발생할 수 있다. 이는 전체 프로젝트의 금액적인 면에서나 일정적인 면에서 상당히 큰 리스크를 가지고 있는 내용이다.

Sensor 나 Logic Solver는 아래 (13)과 (14)과 같이 요구 고장 확률이 상당히 낮으므로 고려할 필요가 없으므로 여기서는 Final Element의 확률만 확인하도록 하겠다. P&ID가 아직 확정되지 않은 상태이므로 임의로 Tag No.를 지정하였고, 필요 데이터는 OREDA5 (Offshore reliability data base)를 참고하였다. 추후 하드웨어가 선정되어 메이커의 자세한 데이터를 사용하면 변경될 소지는 있다.

$$\text{Sensor} \quad : \text{PFD} = 4.297 \times 10^{-5} \quad (13)$$

$$\text{Logic Solver} : \text{PFD} = 1.0 \times 10^{-5} \quad (14)$$

(3) 최종 안전시스템 설계

조건들을 검토한 결과 Final Element의 전체 테스트는 5년을 유지하면서 부분 테스트를 6개월에 한번 실시하는 것으로 기본 설계 방향을 잡고 추진하기로 하였다.

5.3 적용 효과

(1) 하드웨어 측면

하드웨어 측면에서 과거 플랜트의 안전시스템과 본 연구 내용을 적용한 안전시스템을 비교해 보면 표 8에서 볼 수 있듯이 테스트 기간의 차이에 따른 액세서리 추가는 논외하고, Logic Solver 구

조와 Final Element 수량이 줄었음을 알 수 있다. 하지만 두 프로젝트 모두 계약서에 Sensor와 Logic Solver 구조가 명기되어 필요 이상으로 하드웨어가 많이 사용되는 프로젝트이다. 계약서의 요구 사항이 없다면 표 8의 안전시스템 구조가 하드웨어를 가장 적게 사용하면서 안전등급의 요구 사항을 만족하는 구조이다.

따라서 프로젝트를 수주하기 이전 단계에서 안전시스템의 사양을 결정할 때에는 계약서를 자세히 검토하여 계약서에 안전시스템 요소들의 사양에 대해 명확히 명시되어 있다면 계약서대로 진행을 해야 하고, 아무런 조건이 없다면 표 8의 안전시스템 사양 기준으로 준비하여 프로젝트 수주 후 업무를 진행할 것을 제안한다.

(2) 금액 측면

금액 측면에서는 플랜트 내에 안전등급이 안전등급 3은 드물고 대부분이 안전등급 1 또는 2라고 보면 표 9와 같이 Final Element 수량이 2개에서 1개로 줄고 금액이 비싼 TMR 구조에서 저렴한 QMR 구조로 변경되면 상당액의 금액을 줄일 수 있다. 더 나아가 설치비, 작업비, 각종 공사용 자재비도 줄일 수 있으므로 플랜트 규모에 따라 그 절감되는 금액은 엄청나다고 할 수 있다. 게다가 계약서에 요구 사항이 없을 경우 표 9의 안전시스템 사양을 적용하면 하드웨어를 가장 적게 사용하면서도 안전 등급의 확률을 만족할 수 있으므로 그 절감 금액이 더 커질 수 있다.

<표 8> 사우디 PDH/PP와 ethylene 프로젝트의 안전시스템 비교

SIL	Saudi PDH/PP			Saudi Ethylene		
	Sensor	Logic Solver	Final Element	Sensor	Logic Solver	Final Element
1	3	TMR	2	3	QMR	1
2	3	TMR	2	3	QMR	1
3	3	TMR	2	3	QMR	2



〈표 9〉 안전 시스템의 효율적 구성

SIL	Sensor	Logic Solver	Final Element
1	1	1oo2D	1
2	1	1oo2D	1
3	2	1oo2D	2

6. 결론

최근 석유 화학플랜트의 안전시스템은 관련 국제 규격이 발표되고 신규 해외 프로젝트에서는 이를 적용하라는 요구 사항이 최근 빈번하게 일어나고 있다. 이에 따라 변화하는 환경에 효과적으로 대처하기 위하여 효율적인 안전시스템 사양의 선정 및 활용이 필요하므로 엔지니어링회사들은 프로젝트 추진 단계에서 부터 계약서와 국제 규격의 요구 사항을 고려해서 최적의 사양을 선정하고자 노력해야 한다. 하지만 새로운 국제 규격을 적용한 과거 실적이 전무한 상태라 참고 자료가 없고, 사업주와 설계 회사 간 국제 규격의 해석의 차이로 인해 어려움이 예상되지만, 신규 해외 프로젝트에서는 계속 국제 규격을 준수하도록 요구하는 것이 국제적인 추세이므로 본 연구 결과가 석유 화학플랜트 수주 경쟁력 강화와 나아가 안전시스템 설계 능력 향상을 위한 기준 자료

로 활용하고자 한다.

본 연구를 통해 다음과 같은 두 가지 결과를 얻었다. 첫번째로 국제 규격의 요구 사항과 사우디 에틸렌 플랜트의 계약서를 만족하며 최소한의 하드웨어 사용과 금액 절감을 이끌어 낼 수 있는 안전시스템의 설계를 할 수 있는 것이고 두 번째로는 국제 규격의 요구 사항을 만족시키는 최소한의 안전시스템의 사양을 제안하여 프로젝트 견적 단계에서 특별한 계약서의 요구 사항이 없을 경우, 안전시스템의 견적 기준으로 활용하는 것이다.

본 연구결과로 설계된 안전시스템의 사양과 견적 기준으로 활용하도록 제안한 사양에 대한 평가는 프로젝트가 진행되면서 이루어 질 수 있을 것이며, 이러한 평가에 의해 향후 안전시스템 설계의 방향이 결정되어질 수 있을 것이다. 향후에도 보다 효율적인 안전시스템의 사양 설계에 대해 지속적인 관심을 가지고 체계적으로 연구를 지속해 나가야 하겠다. (KIPEC)