# 3 안전무결성기준(SIL) 검토 기법 소개
## Introduction to Review of Safety Integrity Level(SIL)

글 박경수 ＼ 플랜트엔지니어링부 이사 ＼ 전화 02-3433-7858 ＼ E-mail kspark450@ssyenc.com

## 1. 머리말

화학공장의 주요 설비는 유해 위험물질을 다량으로 취급하고 있으며 복잡한 장치설비로 자동제어가 되도록 시스템화 되어 있다. 복잡한 화학장치설비에 내재되어 있는 잠재적 위험요소를 식별 평가하여 위험을 제거하거나 대책을 세우고 관리할 수 있는 공정 위험성평가를 수행할 필요가 있다.

공정위험성평가로 '위험요인 및 운전성 검토(HAZOP)' 그리고 '안전무결성기준(SIL) 검토'가 프로젝트 수행에 요구되고 있으나 안전무결성기준 검토는 아직까지 활발하게 추진되지 않고 있으므로 본 고에서는 안전무결성 검토의 수행 절차 및 방법에 대해 세부적인 내용을 이해할 수 있도록 소개하고 수행상 유의점을 설명하고자 한다.

## 2. 설계

### 2-1. 일반

안전무결성은 안전기능을 수행하는 안전계장 시스템(SIS)의 성능과 관련된다. 이것은 정해진 시간 주기 내에 모든 정해진 조건하에 필요한 안전계장기능(SIF)을 만족하며 수행하는 안전계장 시스템의 평균확률이다. 안전계장시스템에 필요한 안전무결성기준(SIL), 기술적 안전관련시스템 및 외부 위험감소 설비 즉, 독립적인 보호층(IPL)은 다음과 같은 사항을 만족하게 하도록 한다.

- 안전관련시스템의 결함 빈도를 위험한 사건 주기의 '참을 수 없는 위험'이 되는 것을 방지하도록 충분히 낮도록 한다.
- 안전관련시스템은 '참을 수 있는 위험(ALARP)' 정도로 결함 영향을 개선한다.

안전무결성기준은 각각의 특별한 안전계장시스템 적용에 대해 요구되는 성능(가용성/신뢰성) 수준으로 정의된다.

안전무결성기준 구분은 모든 플랜트의 안전계장 시스템 보호폐회로망에 적용되고, 각각의 안전계장시스템 보호 폐회로망에는 안전무결성기준을 지정한다.

각각의 안전계장시스템 보호폐회로망은 다음 항목으로 구성된다.

- 기동요소(공정 감지기)
- 논리해결기(긴급정지장치(ESD))
- 최종요소(정지 밸브, 기계 등)

즉, 안전계장시스템 보호폐회로망은 유체와 유체 사이에 모든 구성품을 포함한다.

수동스위치는 자동보호시스템을 제공하지 않으므로 고려되지 않는다. 이들 운전은 운전절차에 포함되어야 한다.

식별된 안전무결성기준을 기준으로 안전계장시스템 설계 및 실행에 대해 가장 적절한 전략이 선정될 필요가 있다. 계장시스템의 무결성을 보증하기 위해 다음 규칙을 따른다.

- 안전계장시스템은 단순하게 유지되며, 실제 제어시스템에 있는 기능은 제어시스템에서 유지된다. 계장보호 시스템으로 구성된

이들 조합이 안전계장 시스템으로 결정된다.

- 안전계장시스템은 완전히 제어시스템과 독립적이다. 안전계장 시스템은 제어시스템의 결함에 관하여 다른 것들부터 독립된다.

안전한 설계를 반드시 준수한다. 안전계장 시스템의 구성품의 결함으로 일어나는 대부분은 자체적으로 드러나게 되고, 차단(케이블 절단, 솔레노이드 단락, 열전대 단락, 전송기로부터 신호 없음 등)이 원인이 된다.

안전계장시스템의 변경은 플랜트 변경에 대한 절차와 동일하게 적절한 승인절차에 포함되며 자료화되어야 한다.

- 적절한 폐기(Override) : 공정이(시운전) 일정 시간 폐기되는 기능을 요구한다. 적절한 운전 폐기가 제공되어야 하며 설계단계 이후 운전자에게 적절히 지적되고 규정되어야 한다. 계장보호 판넬에서 폐기는 도약의 의지로부터 제외된다.
- 시험설비 : 안전계장시스템은 감지기, 논리해결기 및 최종요소 등 3가지 주요 구성품으로 구성된다. 시스템은 감추어진 결함 혹은 계장시스템의 착오를 확인하기 위해 예정된 주기에 시험되어야 한다.

기동요소/감지기는 6개월마다 시험한다. 필요한 경우 정비 폐기가 적용될 수 있다.

논리해결기는 전형적으로 각각의 주요 정비 보수기간 동안(예를 들어, 12 개월) 그리고 각각의 개조 후에 시험된다.

최종요소는 전형적으로 각각의 주요 정비 보수 기간 동안(예를 들어, 12 개월) 시험된다. 높은 빈도가 필요한 경우 특히 운전 중 시험을 위해 특별한 설비가 설치되어야 한다.

지정된 안전계장시스템을 달성하기 위해 짧은 기간이 요구되면 이것은 안전무결성기준 검토 작업서에서 강조되어야 한다.

## 2-2. 논리해결기

SIL-1 이하의 분류되지 않는 무결성기준의 안전 기능성은 공정제어시스템으로 실행된다.

SIL-1, SIL-2 및 SIL-3의 안전기능성은 긴급정지시스템(ESD)에서 실행된다.

긴급정지시스템의 논리해결기의 기능은 플랜트의 결과로 높은 안전무결성기준의 실행에 대해 적절한 IEC 61508과 일치하여 증명된 프로그램화 전자시스템에 의해 실행된다.

동일한 프로그램화 전자시스템은 여러가지 SIL 구분(SIL-1, SIL-2 및 SIL-3)을 실행하는데 이용된다.

모든 SIL 구분에 적용되는 I/O 모듈은 적절히 중복된다. 그러나 운전정지, 지시등 및 반복되는 신호같은 안전과 관련되지 않는 기능에 대한 I/O 모듈은 중복되지 않는다.

## 2-3. 기동기 · 구동기와 부속품

식별된 안전무결성기준 구분을 기준으로 실행에 대한 가장 적절한 전략이 선정된다. 요구되는 안전무결성기준 구분은 다음 전략과 1개 이상 일치해야만 적용할 수 있다.

- 구성품의 중복성
- 낮은 결함률을 갖는 구성품
- 공통 모드 결함을 피할 수 있는 구성품의 다양성
- 시험 기간의 증가 및 감소

안전무결성기준 요구사항에 일치하기 위해 기동기는 1 out of 1, 1 out of 2, 2 out of 2 혹은 2 out of 3 구성으로 배열할 수 있다. 동일하게 최종요소도 1 out of 1 혹은 1 out of 2 구성으로 배열할 수 있다. 이런 목적으로 가능한 안전계장 시스템 구성표가 사용된다.

정기적 시험을 수행하기 위해 적절한 대책이 고려된다. 시험 기간에 닫혀있지 않고 열려 있는 밸브에 대해 운전중 시험 혹은 일부 스트로킹 설비가 고려된다.

안전계장시스템으로 구동되는 전용 솔레노이드에 의해 정지되는 모든 제어밸브가 운전하는 중 항상 움직이므로 일부 스트로킹같은 시험장치로는 제공 되지 않는다.

요구되는 폐회로망 무결성을 일치시키기 위해 이와 상응하는 고려가 솔레노이드 밸브 같은 구성품의 선정 및 적용에서 이루어진다.

## 2-4. 안전계장시스템에 대한 안전무결성기준 Matrix

요구결함의 영향평가 및 추천사항의 확인 후 각 안전계장기능은

표 1 안전계장기능에 대한 안전무결성기준

| 발생주기 | S1 | S2 | S3 | S4 | S5 |
|---|---|---|---|---|---|
| F5 | NR | NR | 2 | 3 | NS(4) |
| F4 | NR | NR | 1 | 2 | 3 |
| F3 | NR | NR | NR | 1 | 2 |
| F2 | NR | NR | NR | NR | 1 |
| F1 | NR | NR | NR | NR | NR |

강도기준

- NR : 안전계장시스템이 필요하지 않는다.
- NS(4) : 불충분함. 그래서 추가적이며 독립적인 보호층이 요구되거나 공정을 재설계하여야 한다.

안전무결성기준으로 구분된다.

안전계장시스템의 안전계장기능은 주어진 공정 일탈 및 바람직하지 않은 사건에 대해 가장 높은 목표의 안전무결성기준과 일치되도록 설계되고 시험되어야 한다.

이를 위한 Matrix는 다음 인자를 기준으로 한다.

- 발생주기 : F1 – 희박한(〈$10^{-3}$ 사건/년)
  F2 – 드문($10^{-3}$ 사건/년)
  F3 – 아마도($10^{-2}$ 사건/년)
  F4 – 가끔($10^{-1}$ 사건/년)
  F5 – 자주(〉$10^{-1}$ 사건/년)

표 2 강도기준

| | S1 | S2 | S3 | S4 | S5 |
|---|---|---|---|---|---|
| 1 안전 | 응급치료 및 혹은 경미한 회복될 수 있는 건강 영향 | 제한되는 근무 상해 및 혹은 중간의 회복될 수 있는 건강 영향 | 불구 아닌 노동불능 상해 및 혹은 뚜렷이 회복될 수 있는 건강 영향 | 영구적 불구의 상해 및 혹은 회복될 수 없는 만성적 건강 영향 | 사망 및 혹은 다수의 입원을 갖는 상해 및 혹은 회복될 수 없는 건강 영향 |
| 2 환경 | 민감하지 않는 서식지, 종 혹은 생활환경에서 국지적 단기 영향 | 국지적 단기 영향 혹은 민감한 서식지, 종 혹은 생활 환경 | 민감한 자원, 종 혹은 분배되지 않는 습성의 큰 장소 혹은 시간의 규모의 영향 | 민감한 개체, 서식지 혹은 임시적 큰 큐모의 자원 손실 | 종 혹은 서식지 사멸 혹은 위험에 빠질 값 있는 자원의 큰 규모의 손실 |
| 3 재산 손해 | 〈 50만$ | 50만$ ~ 5백만$ | 5백만$ ~ 5천만$ | 5천만$ ~ 2억5천만$ | 〉2억5천만$ |

## 3. 안전계장시스템의 검토

### 3-1. 개요

안전계장시스템 확인은 안전계장시스템 구성표와 일치하도록 하는 플랜트의 정지조작에 대해 수행된다.

안전무결성기준은 〈표 3〉에서 규정된 요구 결함의 확률로 정의된다.

표 3 안전무결성기준

| 안전무결성기준(SIL) | 요구결함의 확률(PFD) |
|---|---|
| 1 | $10^{-1}$ ~ $10^{-2}$ |
| 2 | $10^{-2}$ ~ $10^{-3}$ |
| 3 | $10^{-3}$ ~ $10^{-4}$ |

안전계장시스템 검토는 어떤 안전계장시스템 보호 폐회로망과 관련된 요구결함의 확률이 안전무결성기준 구분에 의해 이미 지정된 기준에 일치하는지를 검토하는 것이다.

- SIL–1 구분에 대해 특정한 검토가 수행되지 않으나 최악의 경우 결함율을 기준으로 전형적인 요구결함의 확률계산이 수행된다.
- SIL–2 구분에 대해 안전계장시스템 구성표 및 명시된 것과 같이 이루어진다.
- SIL–3 구분에 대해 검토를 항상 수행하고 검토작업서를 작성한다.

안전계장시스템 검토는 실제 구성요소의 결함자료를 기준으로 수행한다. 실제 구성요소의 자료가 불가능한 경우에는 통계적 자료로부터 취한 전형적인 결함율을 기준으로 검토가 수행된다.

### 3-2. 기능적 단계

안전계장시스템 검토를 수행하기 위해 다음 자료를 수집한다. 상세설명 및 각각의 인터록 혹은 안전관련 기능에 요구되는 안전무결성기준, 각각의 차단 및 정지에 대해 실행되는 2가지 조작은 아래와 같다.

- 일차적인 정지 조작 : 안전 상태로 도달하기 위해 필요하고 충분한 조작
- 이차적인 정지 조작 : 직접적으로 안전과 관련되지 않은 조작 그러나 차단 후 실행하도록 예상되는 조작

각 인터록 혹은 안전관련 기능에 대해 이것은 일차 및 이차 정지조작을 구별하고 일차 정지조작에서만 분석을 제한하는 것이 필요하다.

가열로(Fire Heater) 과압 안전시스템을 예로 들면, 압력전송기가 연소실의 고압을 감지할 때 다음 조작이 이루어 진다.

❶ 주가스 밸브의 닫힘은 주가스 공급을 막고 폭발을 방지하기 위해 충분하기 때문에 일차 정지조치함
❷ 배출 밸브가 열림
❸ 슬러지 공급펌프 정지(조작은 직접적으로 안전과 관련되지 않는다)
❹ 연소공기 팬 정지(조작은 직접적으로 안전과 관련되지 않는다)
❺ 파이롯트 가스 밸브 닫힘(조작은 직접적으로 안전과 관련되지

않는다)

폭발위험은 주로 조작 ❶을 실행하는 폐회로망의 요구결함 확률과 관련된다.

제작자는 안전계장시스템 폐회로망의 각각 구성품에 대한 신뢰성 자료를 제출하여야 한다.

요구결함의 확률 계산에서 중요한 규칙을 나타내는 입증시험 사이에 예상되는 기간 $T_1$ 동안에(플랜트 운전 및 정비에 제공되기 위해) 다음 단계가 실행된다.

- 이전에 설명된 자료를 이용하여 IEC 61508/61511 표준에서 명시된 대로 계산을 수행한 후에 각각 안전계장시스템 폐회로망에 대한 신뢰성이(요구결함의 확률) 결정된다.
- 계산된 요구결함의 확률과 안전무결성기준 요구사항을 비교한다. 요구사항과 일치하지 않는 각각의 폐회로망에 대해 다음과 같이 적절한 조치가 수행된다.

❶ 요구결함의 확률을 감소시키기 위해 폐회로망 위상을 재배치 (예를 들면, 1 out of 1 구조를 1 out of 2로 변경)

❷ 높은 결함 사이의 평균시간(MTBF) 장치 사용

❸ 입증시험 사이의 기간을 감소시키고 계산을 반복함

## 3-3. 기동기/프로그램논리제어기(PLC)/구동기

다음 아래의 표는 안전계장시스템 폐회로망 구조의 검토에 사용된다.

표 4 안전무결성기준 구성표

| 감지기수 | 1 out of 1 | 1 out of 2 | | 3 out of 3 |
|---|---|---|---|---|
| 감지기 시험기간 | 6개월 | 6개월 | | 6개월 |
| 논리해결기의 종류[2] | SIL-3 | SIL-3 | | SIL-3 |
| 긴급정지밸브 수 | 1 out of 1 | 1 out of 1 | 1 out of 2[3] | 1 out of 2[3] |
| 밸브 시험기간 | 12개월[6][4] | 12개월[5] | [5] | [5] |
| 회전기기 정지계통 | 1 out of 1 | 1 out of 1 | | 1 out of 2 |
| 회전기기 시험기간 | [7] | [7] | | [7] |
| 필요한 검토 | No | Yes | No | Yes |

❶ SIL-4는 대안으로 추천되지 않음

❷ 모든 SIL 구분에 대해 논리해결기로 예비 선정된 SIL-3의 승인된 PLC임

❸ 다음 조건이 일치되면 약간의 경우 제어밸브(분리된 긴급정지 솔레노이드 밸브를 갖고 동작)가 긴급정지 밸브(1 out of 1 경우) 혹은 하나의 긴급정지 밸브(1 out of 2 경우)로 사용된다.

밸브의 결함 상태는 안전기능 결함 상태로 대응한다. 제어밸브 결함의 닫힌 상태인 경우 관련 수동 바이패스 밸브는 닫힌 상태에서 차단됨

폐쇄회로망의 안전기능은 TSO 누출 구분을 필요로 하지 않음

❹ 시험기간을 24개월 이내로 줄이는 것이 필요한 경우 기동하에 시험 능력은 결함 폐쇄 제어밸브에 대해 수동바이패스가 설치되며 온-오프 밸브에 대해 위치 제어 기동기가 설치됨

❺ 시험기간을 24개월 이내로 줄이는 것이 필요한 시점에서 1 out of 2 밸브의 경우 가동시 시험을 위해 결함폐쇄 제어밸브에 대해 수동 바이패스 그리고 온-오프 밸브에 대한 위치 제어 기동기가 설치됨

❻ 전형적인 요구결함의 확률 계산이 최악의 경우의 결함률을 기준으로 주어지는 경우 SIL 검토가 이루어지지 않음

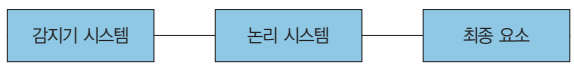
❼ 시험기간은 SIL 요구사항에 따라 정의된다. 시험적용시에는 대기 펌프가(대기 펌프는 보통 SIL 적용에 대해 사용되는 펌프를 말한다) 항상 가능하여야 함

전형적으로 성능 요구사항을 맞출 수 있는 구조는 다음과 같다.

- SIL-1 : 한 개의 감지기, 한 개의 논리해결기 및 한 개의 제어요소를 갖는 1 out of 1 구조
- SIL-2 : 더 많은 진단이 요구되고 전형적으로 필요하면 이중의 최종요소를 갖는 이중의 논리해결기 및 감지기를 포함
- SIL-3 : 전형적으로 각각의 감지기, 논리해결기 및 최종요소를 갖는 2개의 1 out of 1 을 배열

## 3-4. 폐쇄회로망 요구결함의 확률 계산

일반적으로 폐쇄회로망은 다음과 같이 그려진다.




감지기(S), 논리(L) 및 최종요소(F)의 서브시스템은 약간의 다른 구성품을 포함한다. 예를들면 L은 입력카드 및 CPU 출력카드를 포함한다. 서브시스템은 연속으로 연결된 검은 상자로 그려진다.

2개 혹은 3개의 폐쇄회로망 동시 결함의 확률은 무시되므로 조합된 요구결함의 확률은 고려되지 않는다. 시스템 요구결함의 확률은 다음과 같이 계산된다.

$$PFD_{SYS} = PFD_S + PFD_L + PFD_{FE}$$

## 4. 안전무결성기준 검토 절차

### 4-1. 팀 구성

안전무결성기준 검토를 수행함에 있어서 팀 참가 인원의 적절한 선정이 매우 중요하다. 검토팀은 공정기술에 대한 지식이 있고 공장운전에 경험이 있는 인원으로 구성된다.

팀은 검토를 수행하는 동안 제기되는 대부분의 질문에 답할 수 있는 필요한 기술적인 전문기술을 갖고 있어야 한다.

안전무결성기준 검토의 수행을 위해 필요한 다수 분야의 팀은 다음과 같다.

- 공정엔지니어
- 계장 · 계측엔지니어
- 운전엔지니어
- 팀리더
- 서기

팀내의 고정 인원에 의해 추천된 다른 분야의 전문가가 추가로 참석한다.

### 4-2. 역할과 책임

**1) 팀리더**

팀리더는 높은 수준의 기술적 및 관리적인 숙련이 요구되며, 토의시 독립성을 유지한다. 팀리더의 역할은 회의의 성공에 매우 중요하며, 팀에서의 역할은 다음과 같다.

- 검토하기 전에 검토팀에 의해 사용되는 모든 규칙 및 예상 내용을 작성한다.
- 안전무결성기준 검토 기법을 통해 팀을 선도한다.
- 브레인스토밍 노력을 증진시키고 토의를 조정한다.
- 팀에 의해 제기된 주요 쟁점을 선별한다.
- 요구율 및 영향의 평가를 촉진하고 등급의 일치성을 확인한다.
- 서기가 작성한 결과물의 기록을 확인한다.
- 식별된 사항에 관하여 완전히 반영된 회의록을 확인한다.
- 검토보고서를 작성한다.

**2) 서기**

서기의 역할은 토의를 정확하게 기록하기 위해 팀리더가 완전히 집중할 수 있도록 검토에 포함되지 않는 인원으로 선정된다. 많은 경험이 필요하지는 않지만 엔지니어링 전문용어에 익숙할 필요가 있고 역할은 다음과 같다.

- 검토 시작 전에 결과물을 기록하기 위해 사용되는 컴퓨터 소프트웨어에 익숙하여야 한다.
- 팀의 결과물을 기록하는데 있어 팀리더의 지시를 따른다.
- 검토 후에 팀 보고서 작성시 팀리더를 돕는다.

**3) 계장 · 계측엔지니어**

검토 전에 계장/계측엔지니어는 P&ID 및 HAZOP을 검토를 완료한 각 안전계장 기능에 대하여 안전무결성기준 검토작업서의 다음 요소를 완성할 임무가 있다.

- 기동기를 기입한다.
- 최종요소를 기입한다.
- 기동기 및 최종요소에 대한 성공적인 기준을 정의한다(Voting).
- 관련된 조작을 지적한다.

이것을 어떻게 자료화하는가의 예를 검토 작업서에 제시한다. 검토를 수행하는 동안 계장 · 계측 엔지니어는 팀의 고정 인원이 된다.

**4) 공정엔지니어**

검토 전에 공정엔지니어는 안전계장기능의 설계 의도를 설명하고 안전무결성기준 검토작업서 수행을 위한 정보를 계장 · 계측엔지니어에게 제공할 책임을 진다. 이것을 어떻게 자료화하는가의 예를 검토작업서에 제시한다. 검토수행 중 공정엔지니어는 팀의 고정 인원이 된다.

**5) 팀인원**

검토의 품질은 모든 팀원의 기여도와 전체적인 경험으로부터 크게 좌우된다. 정성적인 결과를 달성하기 위해 팀원은 다음과 같이 요구된다.

- 다른 팀원의 기여에 대해 긍정적인 태도를 취한다.
- 프로젝트 특성과 다른 유사한 경험으로부터 전문기술을 제공한다.
- 모든 인원이 이해할 수 있도록 크고 뚜렷하게 발표한다.

### 4-3. 요구되는 자료

다음 자료가 토의에 대한 입력자료로 제공되어야 한다.

- HAZOP 검토후 개정된 공정도(PFD)
- 물질수지 자료
- HAZOP 검토후 개정된 P&ID, 안전무결성기준 검토에 사용되는 P&ID는 공급 범위를 포함 하는 모든 계장, 체크밸브, 안전밸브, 제어기, 압력 및 액면 스위치 등이 표현되어야 함
- 이전의 프로젝트 HAZOP 검토 결과물
- 제어 및 안전보호 개요
- 인터록 설명
- 배치도/Plot Plan(가능한 경우만)

## 4-4. 절차

### 1) 검토의 준비, 안전무결성기준 검토의 도입

검토 전에 팀리더는 계장 · 계측엔지니어로부터 관리 파일에 기입된 안전계장기능 설명내용(안전계장기능의 명칭, 기동기, 최종요소, 성공적인 기준, 관련조작 및 설계의도)을 수집한다.

안전무결성기준 검토 수행 전에 검토에 대한 기대치를 일치시키기 위해 각 팀원의 숙련과 경험을 나타내는 간단한 자기소개시간을 가진다.

팀리더는 팀원의 노력을 집중시키기 위해 안전무결성기준 검토의 목적과 범위를 설명한다. 또한 팀리더는 안전무결성기준 검토에 사용되는 방법에 관한 설명시간을 갖는다. 이것은 효과적인 안전무결성기준 검토의 수행을 위해 필요한 팀에 대한 일반적인 착수기준을 수립하게 해준다.

안전무결성기준에 관한 평가 검토에 사용하기 위해 프로젝트 위험 Matrix의 인자를 팀원에게 설명한다.

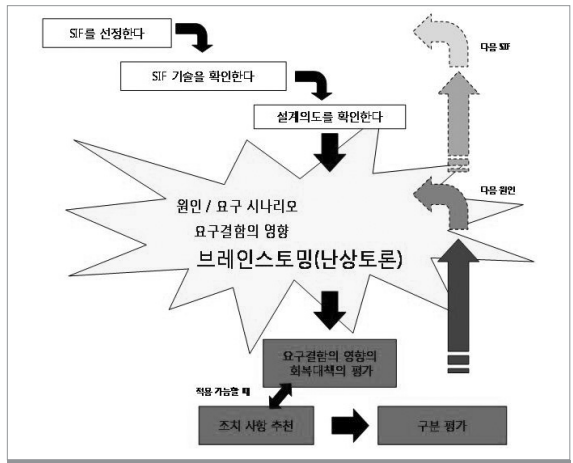
공정엔지니어는 모든 팀원에게 플랜트의 기본 운전이 확실히 이해가 되도록 공정의 전체적인 것을 설명한다. 이것은 팀원으로 하여금 위험한 조건으로부터 유도되는 전형적인 시나리오에 대해 익숙해지게 한다.

### 2) 안전무결성기준 검토 수행

안전무결성기준 검토 순서는 다음 단계로 구분되면 가장 이해하기 쉽다.

- 안전계장기능을 선정한다.
- 안전계장기능의 설명을 확인한다(계장 · 계측 엔지니어에 의해 검토작업서에 이미 자료화 됨).
- 설계의도를 확인한다(공정엔지니어에 의해 검토 작업서에 자료화됨).
- 브레인스토밍에 의해 안전계장기능 조작을 일으키는 모든 잠재적 원인 및 요구 시나리오를 결정한다.
- 각 원인의 신뢰성을 확인한다.
- 안전계장기능 요구결함의 영향을 평가한다.
- 예방, 보호 및 감소 안전 특징을 평가한다.
- 문제의 조작 혹은 추후 고려사항에 적용이 가능하면 추천사항에 동의한다.
- 안전무겨성 기준 평가와 관련하여 위험 기준을 평가한다.
- 선정된 안전계장기능과 관련하여 다음 원인을 적용한다.
- 전체 검토가 수행된 후 다음 시스템의 안전계장기능으로 이동된다.

검토는 다음 [그림 1]과 같이 기술된 대로 수행된다.




[그림 1] SIL 검토공정도

### 3) 안전계장기능(SIF) 설명의 확인

각각의 안전계장기능은 각 팀원이 설계에 의도한 목적과 상세한 것을 동일하게 이해하기 위해 팀원에게 설명한다.

### 4) 원인, 요구 시나리오

팀은 안전계장기능을 일으키는 조건이 발생 가능한 원인을 찾아내기 위해 질문한다. 또한 이것은 다수의 이유에 의해 발생할 수도 있다(예를 들면 제어 계장의 불량, 운전자 실수, 공급 정지 등). 각각은 검토작업서에 명확히 자료화된다.

팀은 안전계장기능이 설계된 것에 대해 위험요인의 모든 가능성 있는 원인에 초점을 두고 이들 모두가 안전계장기능에 대한 요구의 근원인지 확실하게 한다.

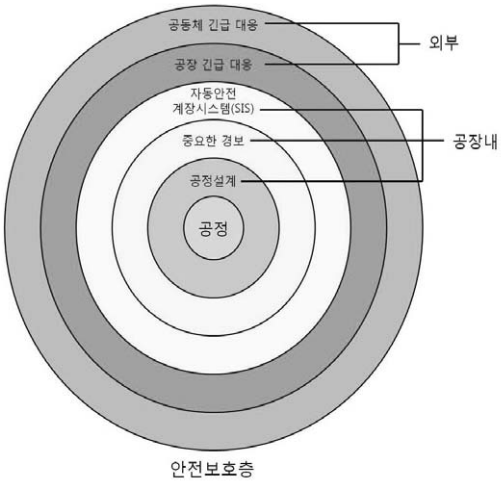
### 5) 요구결함의 영향(CoFD)

팀은 식별된 요구 시나리오의 모든 영향을 식별 하여야 한다. 플

랜트의 위치 및 설치의 상대적인 위치가 중대한 영향을 미치게 한다. 이들 영향의 정확한 평가는 안전계장기능의 적절한 구분이 중요하다.

**6) 독립적인 보호층(IPL)**

적용 가능한 곳에 팀은 사건의 확률을 감소시킬 수 있는 안전계장기능으로부터 독립적인 보호층의 목록을 작성한다.




[그림 2] 안전보호층

**7) 추천사항**

적용 가능한 곳에 팀은 안전한 상태의 달성 또는 기존 자료를 완성하기 위하여 필요한 경우 추천사항을 공식화한다. 추천사항(조치 또는 질문사항)이 기록되고 프로젝트에 의해 추후 이행을 위해 추적조치서가 작성된다. 추적 조치서의 담당 혹은 추후 읽는 사람이 문제가 무엇인지 확실하게 이해할 수 있도록 한다.

**8) 검토의 준비**

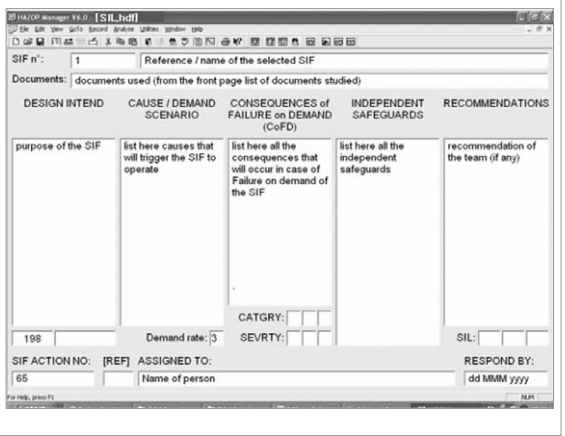
검토 일자 및 기간이 정해지면 적절한 회의실을 확보해 둔다. 회의실은 충분히 밝고 검토팀에게 편리하도록 여유가 있어야 한다(컴퓨터 및 프로젝터). 실제는 팀원이 검토 기간에 높은 수준의 주의력을 유지할 수 있고 커피 등 휴식을 위한 서비스가 공급될 수 있도록 한다.

**9) 검토 시간**

안전무결성기준 검토는 관련된 HAZOP 검토가 완료된 후에 실시한다.

**10) 기록과 보고**

위에서 설명된 방법의 적용 결과물은 컴퓨터 소프트웨어로 서기에 의해 기간 동안 기록된다. 서기는 컴퓨터와 프로젝터를 사용하여 모든 팀원이 볼 수 있도록 식별된 활동의 결과를 기록한다. 다음 [그림 3]은 검토 중에 나타낸 스크린의 예이다.




[그림 3] 검토결과의 예

팀원에게 기록을 보여줄 수 있도록 프로젝터의 사용을 허용한다. 결과물의 기록을 위해 사용되는 검토 작업서는 [그림 4]에 나타냈다.

검토가 완료되면 팀리더는 검토의 결과물을 상세하게 기술한 보고서를 작성한다. 보고서 내용은 다음과 같은 전형적인 목차에 의해 작성된다.

- 요약
- 서론
- 범위
- 팀 구성
- 참고자료
- 일반적인 설명
- 검토 결과물
- 결론
- 첨부
  - 안전무결성기준 검토 절차서
  - 검토중 요구된 참고자료의 복사본
  - 안전계장기능 구분 위험 Matrix
  - 안전무결성기준 검토작업서
  - 안전무결성기준 추적조치서

안전무결성기준(SIL) 검토 작업서

| 안전무결성기준(SIL) 번호: 1 | | | | 검토일자: 14/04/12 |
|---|---|---|---|---|
| 안전계장기능 | SIF-023/PSHH-0213 | | | |
| 기동기<br>최종요소<br><br><br><br>기동기 성공 기준<br>최종요소 성공 기준<br>관련 운전 작동 | PSHH-0213<br>FV-0150 닫힘<br>FV-0154 닫힘<br>SIF-030 작동<br>SIF-018 작동<br>SIF-021 작동<br>2 out of 3<br>5 out of 5<br>SIF-019 작동<br>SIF-022 작동 | | | |
| 도면 및 자료 | P&ID-00-21-021<br>원유 증류탑 | | | |
| 설계의도 | 원인/요구 시나리오 | 요구결함의 영향 (CoFD) | 독립적인 보호층 (IPL) | 추천사항 |
| 원유 증류탑에 PSV의 열림 방지 | 환류손실(펌프 P-100A/B, 제어기 FIC-0143)<br>OVHD 응축손실(냉각기 H-019)<br>대기압 가스오일 Pumparound의 손실(펌프 P-007A/B, 제어기 FIC-0142)<br>일반적인 결력 결함<br>냉각수 결함<br>압력제어기 결함(PIC-0216)<br>W2 | 대기 및 환경영향으로부터 방출을 콜레어로 유도되는 PSV 열림(최대 약 800lt/h)<br>안전영향 없음<br>E2<br>SIL 1 | 탑 OVHD 라인의 PAH-0214<br>펌프 P-010A/B 및 펌프 결함 경보<br>환류 펌프의 FAL-0143(펌프 결함단)<br>펌프 OVHD 라인의 TAH-0277<br>환류 드럼(F-005)의 LAH-0128<br>가스오일 Pumparound의 (펌프 결함단) FAL-0142<br>배출 탄의 LAH-0122<br><br>P1 | |

[그림 4] 안전무결성기준 검토 작업서

안전무결성기준(SIL) 추적 조치서

| 안전무결성기준 조치 명칭 | | 담당자 |
|---|---|---|
| 안전무결성기준 조치 번호 1 | | 최의일자: 14/04/12 |
| 도면 및 자료 | P&ID 00-21-013<br>Preflash Drum | |
| 안전계장기능 | SIF-016/LSLL-0117 | |
| 설계 의도 | 펌프 P-004A/B 케비테이션 손상을 방지 | |
| 원인/요구 시나리오 | 1) 상류로부터 공급이 없음(냉각 예열기 및 탈염기)<br>2) FIC-0121 결함<br>W2 | |
| 요구결함의 영향 | 펌프 케비테이션<br>잠재적 펌프 손상 및 전동<br>누설로 유도되는 잠재적 펌프 씰 손상(자연발화온도 이하의 유체온도)<br>순간적인 점화가 아님<br>약 140 ℃의 유체온도<br>인명에 대한 잠재적 위험요인화상)<br>S2, F2, E1, SIL 1 | |
| 독립적인 보호층 | LIC-0116(가열기로 펌프 배출량을 감소)<br>FAL-0127A/H(가열기 B-001A의 각 패스에 1개)<br>FAL—135A/H(가열기 B-001B의 각 패스에 1개)<br>씰 결함 정보를 갖는 이중 기계적 씰<br>P1 | |
| 추천사항 | FIC-0132 (가열기 B-001A로 주유량 제어기) 및 FIC-0140(가열기 B-001B로 주유량 제어기)에 적유량 경보를 추가 | |
| 대응(조치 1) | | 일자 |
| | | |
| 서명 | | |
| 위 관에 대응을 채운 후 서명하고_____에게 반환 | | |
| 주기: 서기만 사용한다) | | |

[그림 5] 안전무결성기준 추적조치서

### 11) 추적 조치서

검토가 완료된 후 프로젝트 엔지니어는 검토 중에 제안된 조치 및 추천사항의 적절한 추적에 대해 책임을 진다.

## 5. 맺는 말

화학공장 설계동안 다루어야 할 특정한 안전계장기능과 이와 관련된 시스템에 필요한 안전무결성기준의 검토 방법을 자세히 소개하였다. 안전무결성기준 검토는 일반적으로 너무 어려운 것으로 생각되어 프로젝트에 적용을 꺼리고 있으나, 본고를 참고하여 향후 공정 위험성평가가 완벽하게 이루어지도록 좋은 자료가 되기를 기대한다.


**참고문헌**

❶ IEC-61508: Functional safety of electrical/electronic/programmable electronic safety related systems-Part 5: Examples of methods for the determination of Safety Integrity Levels-First edition 1998-12

❷ IEC-61511: Functional Safety: Safety Instrumented Systems for Process Industry Sector, Part 3 Guidelines for the determination of the required Safety Integrity Level-First edition 2003-03

❸ ISA-S84.01 Application of Safety Instrumented Systems for the Process Industries