Control Valve Handbook Chapter 12
안전계측시스템과 제어밸브 최종요소

용어 · 약어 · 상호관계 중심 재구성

1 문서의 목적

Chapter 12의 핵심은 높은 등급의 밸브나 제어기를 개별적으로 구매하는 것이 아니다.

공정위험을 분석하고, 특정 위험을 처리하는 안전계측기능을 정의하며, 그 기능에 필요한 안전무결성수준을 부여해야 한다.

그다음 센서, 로직 솔버 및 최종요소로 안전기능을 구현하고, 검증시험과 부분 스트로크 시험을 통해 숨은 위험고장을 관리해야 한다.

위험 식별 → 위험감소 요구 결정 → SIF 정의
→ 목표 SIL 할당 → SIF 설계
→ PFD 검증 → Proof Test와 PST
→ 기능안전 유지

본문의 부분집합, 교집합 및 독립 기호는 표준에 직접 사용된 수학적 정의가 아니다.
Chapter 12의 용어 관계를 쉽게 이해하기 위한 **개념적 표현**이다.

2 관계 기호의 의미

기호	의미	SIS 예시
$A \subset B$	A가 B의 구성요소 또는 하위개념	$\text{SIF}_i \subset \text{SIS}$
$A \cap B$	두 개념이 일부 목적이나 영역을 공유	HIPPS와 Relief System은 과압방지 목적을 공유
$A \cap B \approx \varnothing$	기능적으로 분리·독립되도록 설계	$\text{BPCS} \cap \text{SIS} \approx \varnothing$
$A \rightarrow B$	정보 또는 동작의 전달방향	Sensor → Logic Solver → Final Element
$A = \text{attribute}(B)$	A가 B의 구성품이 아니라 B의 속성	$\text{SIL}_i = \text{target}(\text{SIF}_i)$
$A \neq B$	두 용어가 서로 다른 개념	SIS ≠ SIF, SIF ≠ SIL
$D_A \subset D_B$	A가 검출하는 고장집합이 B보다 작음	$D_{\text{PST}} \subset D_{\text{Proof}}$

3 주요 약어와 용어

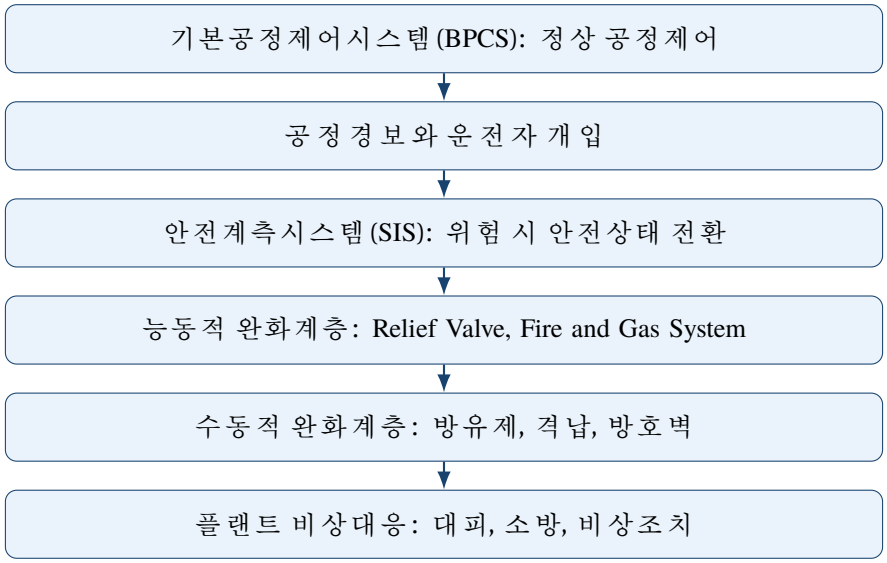
약어	영문	국문	핵심 관계
BPCS	Basic Process Control System	기본공정제어시스템	SIS와 동일 공정을 다루지만 안전기능 경로는 분리
SIS	Safety Instrumented System	안전계측시스템	여러 SIF를 포함하는 상위 시스템
SIF	Safety Instrumented Function	안전계측기능	특정 위험에 대응하는 개별 안전기능
SIL	Safety Integrity Level	안전무결성수준	SIF에 부여되는 성능목표
LS	Logic Solver	로직 솔버	Sensor 신호를 판정하여 Final Element에 출력
FE	Final Element 또는 Final Control Element	최종요소 또는 최종제어요소	안전동작을 실제 공정에 구현
IPL	Independent Protection Layer	독립보호계층	독립적으로 위험을 감소시키는 보호계층
HAZOP	Hazard and Operability Study	위험 및 운전성 검토	공정위험분석에 사용하는 대표적 위험식별 기법
PHA	Process Hazard Analysis	공정위험분석	위험 식별과 위험감소 요구 결정의 상위 활동
PFD	Probability of Failure on Demand	요구 시 고장확률	안전기능이 요구될 때 실패할 확률
PFDavg	Average Probability of Failure on Demand	평균 요구 시 고장확률	시험주기 동안 변화하는 PFD의 평균
RRF	Risk Reduction Factor	위험감소계수	$1/\mathrm{PFD}_{\mathrm{avg}}$
HFT	Hardware Fault Tolerance	하드웨어 고장허용도	몇 개의 하드웨어 고장을 견딜 수 있는지 표현
TI	Test Interval	시험간격	증가할수록 일반적으로 $\mathrm{PFD}_{\mathrm{avg}}$ 증가
PST	Partial Stroke Testing	부분 스트로크 시험	최종요소의 일부 스트로크를 시험
ESD	Emergency Shutdown	비상정지 또는 비상차단	최종요소가 공정을 격리하는 안전동작
BDV	Blowdown Valve	비상감압밸브	안전요구 시 열려 설비를 감압
HIPPS	High-Integrity Pressure Protection System	고신뢰성 압력보호시스템	고압원을 차단하는 SIS 적용사례
OREDA	Offshore and Onshore Reliability Data	해상·육상 설비 신뢰성 데이터	고장률과 PFD 계산에 사용하는 데이터 출처
MooN	M out of N	N개 중 M개 동작논리	Voting Architecture의 일반표현
1oo1	One out of One	1개 중 1개 동작	단일채널 구조
1oo2	One out of Two	2개 중 1개 성공	HIPPS 직렬 차단밸브의 기능성공 구조
2oo3	Two out of Three	3개 중 2개 Voting	HIPPS 압력센서의 대표 구조

4 12.1 플랜트 안전과 보호계층

플랜트 안전은 하나의 장치로 확보하지 않는다.

사고 발생을 방지하는 예방계층과 사고 발생 후 피해를 줄이는 완화계층을 함께 사용한다.

$$\boxed{\text{Plant Safety} = \text{Prevention Layers} \cup \text{Mitigation Layers}}$$



용어 관계

$$\text{BPCS},\ \text{Operator Intervention},\ \text{SIS} \subset \text{Prevention Layers}$$

$$\text{Relief},\ \text{Containment},\ \text{Emergency Response} \subset \text{Mitigation Layers}$$

따라서 SIS는 플랜트 안전 전체가 아니라 여러 보호계층 중 하나이다.

5 12.2 BPCS와 SIS

5.1 BPCS의 역할

BPCS는 정상운전에서 압력, 온도, 유량 및 레벨을 목표값에 유지한다.

$$\boxed{\text{BPCS 목적} = \text{생산 안정성} + \text{품질} + \text{생산량}}$$

정상 압력제어는 다음과 같이 구성된다.

$$\text{Pressure Transmitter} \rightarrow \text{Controller} \rightarrow \text{Control Valve}$$

5.2 SIS의 역할

SIS는 위급상황이 발생하면 공정을 사전에 정의한 안전상태로 전환하는 전용 시스템이다.

$$\boxed{\text{SIS 목적} = \text{위험상태 검출} + \text{안전동작 실행}}$$

5.3 BPCS와 SIS의 독립

용어 관계

$$\boxed{\text{BPCS} \cap \text{SIS} \approx \varnothing}$$

이는 두 시스템이 현실적으로 아무 접점도 없다는 뜻이 아니다.
동일 공정을 대상으로 하지만 다음 항목을 가능한 한 독립적으로 구성한다는 의미이다.

- 공정 센서와 Process Tap
- 로직과 프로그램
- 입출력 채널
- 최종요소
- 전원과 통신
- 시험 및 정비절차

$$\text{Process Domain}_{\text{BPCS}} \cap \text{Process Domain}_{\text{SIS}} \neq \varnothing$$

즉, 같은 공정을 다루지만 안전기능 수행경로는 분리한다.

6 SIS, SIF 및 SIL의 관계

6.1 SIS는 여러 SIF를 포함한다

하나의 SIS에는 여러 위험에 대응하는 복수의 안전계측기능이 포함될 수 있다.

$$\boxed{\text{SIS} = \{\text{SIF}_1, \text{SIF}_2, \ldots, \text{SIF}_n\}}$$

따라서:

$$\boxed{\text{SIF}_i \subset \text{SIS}}$$

반응기 SIS 예

- SIF-1: 반응기 고압 시 원료공급밸브 폐쇄
- SIF-2: 반응기 고온 시 열원 차단
- SIF-3: 냉각유량 저하 시 비상냉각밸브 개방
- SIF-4: 비상상황에서 Blowdown Valve 개방

6.2 SIL은 SIF에 부여되는 성능목표이다

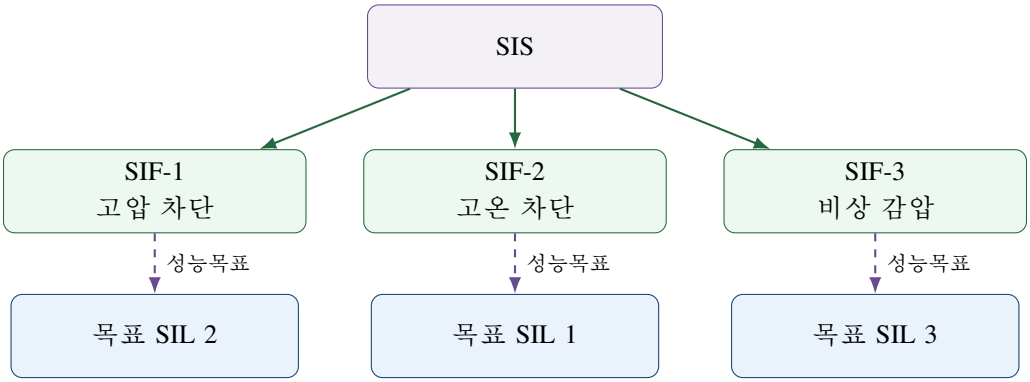
SIL은 SIF 내부의 장치가 아니다.

$$\boxed{\text{SIL}_i = \text{target}(\text{SIF}_i)}$$

따라서:

$$\text{SIL} \not\subset \text{SIF}$$

$$\text{SIL} \neq \text{SIF}$$



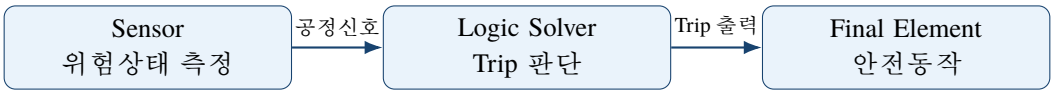
"이 밸브 자체가 SIL 3이다" 라는 표현은 불완전하다.
정확한 표현은 다음과 같다.

> 특정 SIF에 SIL 3 성능목표가 할당되었고, 이 밸브 어셈블리는 해당 SIF의 최종요소로 사용된다.

7 SIF의 세 구성요소

하나의 SIF는 센서, 로직 솔버 및 최종요소가 직렬로 연결된 기능구조이다.

$$\boxed{\text{SIF} = \text{Sensor Subsystem} \rightarrow \text{LS} \rightarrow \text{Final Element Subsystem}}$$



7.1 Sensor Subsystem

센서는 공정이 위험상태에 도달했는지를 측정한다.

- Pressure Transmitter
- Temperature Transmitter
- Level Switch
- Flow Transmitter
- Gas Detector

용어 관계

$$\text{Sensor} \subset \text{SIF}$$

하지만:

$$\text{Sensor} \neq \text{SIF}$$

센서는 위험을 측정하지만 Trip을 판단하거나 공정을 직접 차단하지 않는다.

7.2 LS: Logic Solver

로직 솔버는 센서 신호를 판정하고 최종요소에 안전동작 명령을 보낸다.

$$\text{Sensor Signal} \rightarrow \text{Trip Logic} \rightarrow \text{Final Element Output}$$

주요 기능은 다음과 같다.

- Trip Setpoint 판정
- Voting Logic
- Interlock
- Time Delay
- 최종요소 출력
- 경보와 상태기록

7.3 FE: Final Element

최종요소는 로직 솔버의 판단을 실제 공정동작으로 변환한다.

$$\boxed{\text{Final Element} = \text{Valve} + \text{Actuator} + \text{Valve Instrumentation}}$$

밸브 계장품에는 다음이 포함될 수 있다.

- Solenoid Valve
- Digital Valve Controller
- Limit Switch
- Position Transmitter
- Volume Booster
- 공기배관과 공기공급 부속품

용어 관계

$$\text{Valve} \subset \text{Final Element} \subset \text{SIF}$$

따라서:

$$\text{Valve} \neq \text{Final Element}$$

센서와 로직 솔버가 정상이어도 밸브·액추에이터·솔레노이드 중 하나가 실패하면 안전기능을 수행하지 못할 수 있다.

8 Safe State, Fail-Safe 및 Fault Tolerance

8.1 Safe State

안전상태는 공정위험을 허용 가능한 수준으로 낮추는 상태이다.
안전상태가 항상 밸브 폐쇄를 의미하지는 않는다.

위험상황	필요한 안전동작의 예
가연성 원료 과다공급	원료공급밸브 폐쇄
냉각수 공급 상실	비상냉각수밸브 개방
공정용기 과압	Blowdown Valve 개방
고압원에서 저압계통으로 유입	HIPPS 차단밸브 폐쇄

8.2 Fail-Safe

Fail-Safe는 공기, 전원 또는 신호가 상실될 때 안전방향으로 이동하는 특성이다.

$$\boxed{\text{Failure} \rightarrow \text{Safe State}}$$

$$\text{Fail-Close},\ \text{Fail-Open} \subset \text{Fail-Safe Actions}$$

8.3 Fault-Tolerant

Fault-Tolerant는 일부 고장이 발생해도 요구기능을 계속 수행하는 능력이다.

$$\boxed{\text{Fail-Safe} \neq \text{Fault-Tolerant}}$$

- Fail-Safe: 고장이 발생하면 안전상태로 전환
- Fault-Tolerant: 일부 고장이 있어도 기능을 계속 수행

두 특성은 동시에 적용될 수 있다.

$$\text{Fail-Safe} \cap \text{Fault-Tolerant} \neq \varnothing$$

9 12.3 기능안전 표준

9.1 IEC 61508

IEC 61508은 전기·전자·프로그래머블 전자 안전관련 시스템의 기능안전을 다루는 일반표준이다.

9.2 IEC 61511

IEC 61511은 공정산업용 SIS에 적용되는 기능안전 표준이다.

9.3 ISA S84

ISA S84 계열은 공정산업의 안전계측시스템 수명주기를 다룬다.

용어 관계

$$\text{IEC 61508} = \text{일반 기능안전 기반표준}$$

$$\text{IEC 61511} = \text{공정산업 SIS 적용표준}$$

$$\text{IEC 61511} \cap \text{ISA S84} \neq \varnothing$$

두 표준체계는 공정산업 SIS라는 공통영역을 다룬다.

9.4 기능안전 수명주기

$$\boxed{\text{Functional Safety} = \text{설계} + \text{검증} + \text{시험} + \text{정비} + \text{문서화}}$$

10 12.4 위험분석과 목표 SIL 결정

10.1 Hazard와 Risk

Hazard는 인명, 환경 또는 설비에 피해를 줄 수 있는 잠재적 원인이다.
Risk는 위험사건의 발생 가능성과 결과 심각도의 조합이다.

$$\boxed{\text{Risk} = f(\text{Likelihood}, \text{Consequence})}$$

10.2 PHA와 HAZOP

PHA는 공정위험을 식별하고 필요한 위험감소 수준을 결정하는 전체 활동이다.
HAZOP은 설계의도에서 벗어나는 상태를 다분야 팀이 체계적으로 검토하는 대표적인 기법이다.

용어 관계

$$\text{HAZOP} \subset \text{PHA Techniques}$$

예를 들어 PHA에는 다음 방법이 포함될 수 있다.

- HAZOP
- What-if
- Checklist
- 기타 공정위험분석 기법

10.3 IPL

IPL은 다른 보호수단의 실패와 독립적으로 위험을 감소시킬 수 있는 보호계층이다.

$$\text{IPL} \subset \text{Protection Layers}$$

하나의 SIF는 위험분석에서 하나의 IPL 역할을 할 수 있다.
그러나 두 용어는 동일하지 않다.

$$\text{SIF} \neq \text{IPL}$$

- SIF: 센서·로직·최종요소로 구현된 계측 안전기능
- IPL: 독립적으로 위험을 줄이는 보호계층의 분류

10.4 SIL 결정 흐름

위험 식별 → 위험도 평가
→ 기존 IPL 평가 → 추가 위험감소 요구
→ SIF 정의 → 목표 SIL 할당

11 SIL, PFDavg 및 RRF

11.1 PFD

PFD는 안전기능이 실제로 요구됐을 때 SIF가 작동하지 않을 확률이다.

$$\boxed{\text{Safety Demand} + \text{SIF Failure} = \text{Failure on Demand}}$$

11.2 PFDavg

PFDavg는 시험과 시험 사이에서 변화하는 PFD를 시간평균한 값이다.

11.3 RRF

RRF는 위험감소계수이다.

$$\boxed{\text{RRF} = \frac{1}{\text{PFD}_{\text{avg}}}}$$

예를 들어:

$$\text{PFD}_{\text{avg}} = 10^{-3}$$

이면:

$$\text{RRF} = 1000$$

이다.

11.4 저요구 모드의 SIL 범위

SIL	PFD_{avg} 범위	RRF 범위
SIL 1	$10^{-2} \leq \text{PFD}_{\text{avg}} < 10^{-1}$	10–100
SIL 2	$10^{-3} \leq \text{PFD}_{\text{avg}} < 10^{-2}$	100–1,000
SIL 3	$10^{-4} \leq \text{PFD}_{\text{avg}} < 10^{-3}$	1,000–10,000
SIL 4	$10^{-5} \leq \text{PFD}_{\text{avg}} < 10^{-4}$	10,000–100,000

용어 관계

$$\text{PFD}_{\text{avg}} \downarrow \Longleftrightarrow \text{RRF} \uparrow \Longleftrightarrow \text{SIL} \uparrow$$

세 용어는 동일하지 않다.

- PFDavg: 요구 시 평균 고장확률
- RRF: 위험을 감소시키는 배수
- SIL: PFDavg 범위를 등급화한 성능목표

12 SIL 달성에 필요한 세 조건

목표 SIL은 PFD 계산만으로 달성되지 않는다.

$$\begin{aligned}\text{SIL 달성} = {} & \text{Systematic Integrity} \\ & \cap \text{Architectural Constraints} \\ & \cap \text{Random Integrity}\end{aligned}$$

12.1 Systematic Integrity

사양, 설계, 소프트웨어, 설치, 시험 및 변경관리에서 발생하는 체계적 오류를 관리한다.
예:

- 잘못된 Trip Setpoint
- 잘못된 Fail Action
- 프로그램 오류
- 배선 오류
- 시험절차 누락
- 무단 변경

$$\text{Systematic Integrity} \neq \text{PFD}_{\text{avg}}$$

체계적 오류는 장치 고장률 계산만으로 충분히 관리할 수 없다.

12.2 Architectural Constraints

구성품의 수, 중복성, Voting 구조 및 고장허용도를 제한하는 구조적 요구이다.

$$\text{HFT},\ \text{Redundancy},\ \text{Voting} \subset \text{Architectural Design}$$

12.3 HFT

HFT는 하드웨어 고장이 발생해도 안전기능을 유지할 수 있는 정도이다.

- HFT 0: 한 개 고장으로 기능 상실 가능
- HFT 1: 한 개 고장이 발생해도 기능 유지
- HFT 2: 두 개 고장이 발생해도 기능 유지

$$\text{Redundancy} \neq \text{HFT}$$

중복성은 설계수단이고, HFT는 실제 고장허용능력이다.

12.4 Random Integrity

개별 장치의 무작위 위험고장률을 사용하여 SIF의 PFDavg를 검증한다.

$$\boxed{\mathrm{PFD}_{\mathrm{avg,SIF}} \leq \mathrm{PFD}_{\mathrm{target}}}$$

$$\mathrm{PFD}_{\mathrm{avg}} \text{ 만족} \not\Rightarrow \text{SIL 전체 만족}$$

체계적 무결성과 구조적 제약도 동시에 만족해야 하기 때문이다.

13 12.5 SIF 전체 PFD와 고장형태

핸드북은 SIF의 전체 PFD를 다음과 같이 단순화하여 설명한다.

$$\boxed{\mathrm{PFD}_{\mathrm{total}} = \mathrm{PFD}_{\mathrm{sensor}} + \mathrm{PFD}_{\mathrm{logic}} + \mathrm{PFD}_{\mathrm{final}}}$$

이 식은 각 하위시스템이 직렬로 안전기능에 기여한다는 점을 설명하기 위한 단순 합산식이다.
실제 계산에서는 중복구조, 공통원인고장, 진단, 시험효율 및 수리시간 등을 고려해야 한다.

13.1 Spurious Trip

실제 위험이 없는데 안전시스템이 불필요하게 공정을 정지시키는 고장이다.

$$\text{No Hazard} + \text{Trip} = \text{Spurious Trip}$$

주요 영향은 생산손실과 가동률 저하이다.

13.2 Dangerous Undetected Failure

장치가 고장났지만 정상운전 중에는 검출되지 않고, 안전요구가 발생했을 때 기능을 수행하지 못하는 고장이다.

$$\text{Hidden Failure} + \text{Safety Demand} = \text{Dangerous Failure}$$

용어 관계

$$\text{Spurious Trip} \cap \text{Dangerous Undetected} \approx \varnothing$$

구분	Spurious Trip	Dangerous Undetected
공정동작	불필요하게 정지	필요할 때 정지하지 않음
주요 영향	생산손실	사고 가능성
안전방향	대체로 안전 측	위험 측
PFD와 관계	주로 가용성 문제	PFD 증가의 핵심 원인

14 TI와 숨은 고장

TI는 Proof Test와 다음 Proof Test 사이의 시험간격이다.

시험 직후에는 검출되지 않은 고장이 상대적으로 적지만, 시간이 지날수록 숨은 고장이 존재할 가능성이 증가한다.

$$\boxed{\text{TI} \uparrow \Rightarrow \text{PFD}_{\text{avg}} \uparrow}$$

핸드북의 단순 설명에서는 시험간격을 두 배로 늘리면 PFD도 대략 두 배 증가할 수 있다.

$$\text{TI} \times 2 \Rightarrow \text{PFD}_{\text{avg}} \text{ 약 } 2\text{배}$$

따라서 시험간격은 목표 SIL 검증에서 사용한 조건과 일치하도록 관리해야 한다.

15 12.6 최종요소와 제어밸브

최종요소는 공정을 실제 안전상태로 전환한다.

$$\boxed{\text{Final Element} = \text{Valve} + \text{Actuator} + \text{Valve Instrumentation}}$$

핸드북의 OREDA 도표는 SIF 고장 중 최종요소가 약 50%를 차지할 수 있음을 보여준다.

따라서 고신뢰 센서와 로직 솔버만으로는 SIF의 안전성능을 확보할 수 없다.

15.1 최종요소 선정조건

- 최대 차압에서 안전방향으로 이동 가능한가
- 액추에이터 추력 또는 토크가 충분한가
- 공기·전원 상실 시 안전방향이 적절한가
- 요구 안전시간 이내에 이동하는가
- 요구 Seat Leakage를 만족하는가
- 솔레노이드와 공기배관이 포함되어 검증됐는가
- 주기적인 Proof Test가 가능한가

$$\boxed{t_{\text{final element}} \leq t_{\text{process safety}}}$$

다만 지나치게 빠른 폐쇄는 Surge, Water Hammer 또는 배관충격을 발생시킬 수 있다.

16 Proof Test, Full Stroke Test 및 PST

16.1 Proof Test

Proof Test는 정상진단으로 발견되지 않은 위험고장을 검출하고 안전기능을 확인하는 시험이다.

최종요소 Proof Test에는 다음이 포함될 수 있다.

- 외관검사
- 전체 스트로크
- 안전방향 동작
- 안전동작시간
- 밸브 Seat Leakage

16.2 Full Stroke Test

Full Stroke Test는 밸브를 정상위치에서 최종 안전위치까지 완전히 이동시킨다.

용어 관계

$$\text{Full Stroke Test} \subset \text{Proof Test}$$

Full Stroke Test는 Proof Test의 중요한 항목이지만, Proof Test에는 외관검사, 누설시험 및 다른 기능검증도 포함될 수 있다.

16.3 PST

PST는 밸브를 전체 스트로크의 일부만 움직였다가 원래 위치로 복귀시키는 시험이다.

핸드북은 일반적인 PST 이동량을 약 10%로 설명하며, 플랜트 안전지침이 허용할 경우 최대 약 30%까지 사용할 수 있다고 설명한다.

$$x_{\text{PST}} \approx 10\% \sim 30\%$$

PST로 검출 가능한 고장의 예는 다음과 같다.

- 스템 또는 샤프트 고착
- 패킹 마찰 증가
- 액추에이터 이상
- 공기배관 막힘 또는 누설
- 안전방향 초기 이동 실패

16.4 PST와 Proof Test의 관계

$$\boxed{D_{\text{PST}} \subset D_{\text{Proof}}}$$

여기서 D는 검출 가능한 고장집합이다.

PST가 완전히 확인하지 못할 수 있는 항목은 다음과 같다.

- 전체 스트로크
- 최종 안전위치 도달
- 최종 Seat 접촉
- 완전 차단 누설
- PST 범위 밖의 국부 고착

- 전체 이동시간

$$\boxed{\text{PST} \neq \text{Full Stroke Proof Test}}$$

PST는 Full Stroke Test를 제거하지 않는다.
PST는 Full Stroke Test 사이에서 일부 숨은 위험고장을 조기에 검출하여 시험주기를 합리적으로 조정하는 보조수단이다.

16.5 PST 중 실제 안전요구 발생

$$\text{PST 진행} \rightarrow \text{Actual Safety Demand} \rightarrow \text{PST 중단} \rightarrow \text{Safe State 이동}$$

디지털 밸브 컨트롤러는 시험 중 실제 Trip이 발생하면 부분시험을 중단하고 밸브를 안전위치로 구동해야 한다.

17 ESD Valve와 BDV

17.1 ESD

ESD는 Emergency Shutdown, 즉 비상정지 또는 비상차단이다.
ESD Valve는 위험물질이나 에너지 공급을 차단하는 최종요소로 사용된다.

17.2 BDV

BDV는 Blowdown Valve, 즉 비상감압밸브이다.
BDV는 안전요구 시 열려 공정압력을 안전한 처리계통으로 방출한다.

용어 관계

$$\text{ESD Valve},\ \text{BDV} \subset \text{Final Elements}$$

하지만:

$$\text{ESD Valve} \neq \text{SIF}$$

$$\text{BDV} \neq \text{SIF}$$

두 밸브는 SIF 전체가 아니라 센서와 로직 솔버의 출력을 실행하는 최종요소이다.

18 12.10 HIPPS

HIPPS는 고신뢰성 압력보호시스템이다.
고압측과 저압측 사이에서 고압원이 저압계통으로 전달되기 전에 차단한다.

$$\boxed{\text{High Pressure Detection} \rightarrow \text{Source Isolation} \rightarrow \text{Downstream Protection}}$$

18.1 HIPPS와 Relief System의 관계

두 시스템 모두 과압방지를 목적으로 한다.

$$\text{Goal}_{\text{HIPPS}} \cap \text{Goal}_{\text{Relief}} = \text{Overpressure Protection}$$

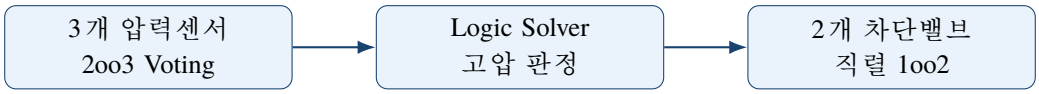
그러나 작동원리는 다르다.

구분	HIPPS	Relief Valve System
기본원리	고압원 차단	초과압력 방출
사고 진행	하류 과압 발생 전 예방	압력 상승 후 완화
보호계층	SIS 기반 예방계층	능동적 완화계층
공정유체	상류측에 격리	Flare 또는 외부계통으로 방출

$$\text{HIPPS} \neq \text{Relief Valve}$$

19 12.11 HIPPS의 기능구조

핸드북의 대표적인 SIL 3 HIPPS 구조는 다음과 같다.



19.1 MooN

MooN은 N개 채널 중 최소 M개가 동작조건을 만족하면 기능을 수행하는 구조이다.

$$\boxed{\text{MooN} = N\text{개 중 } M\text{개 Voting}}$$

19.2 2oo3 압력센서

$$\boxed{\text{2oo3}: \quad 3\text{개 중 } 2\text{개 고압 검출} \Rightarrow \text{Trip}}$$

장점은 다음과 같다.

- 센서 한 개의 오동작에 의한 불필요한 Trip 감소
- 센서 한 개 고장 시에도 안전판정 가능
- 안전성과 운전 가용성의 균형

19.3 1oo2 차단밸브

두 차단밸브가 직렬로 설치되고 둘 다 폐쇄명령을 받는다.
안전기능 관점에서는 두 밸브 중 하나가 정상적으로 닫혀도 유로를 차단할 수 있다.

$$\boxed{\text{1oo2}: \quad 2\text{개 중 } 1\text{개 성공} \Rightarrow \text{안전기능 성공}}$$

용어 관계

$$2oo3 \subset \text{Voting Architectures}$$

$$1oo2 \subset \text{Redundant Final-Element Architectures}$$

HIPPS는 하나의 밸브가 아니라 센서, 로직 솔버 및 이중 최종요소로 구성된 안전시스템 적용사례이다.

20 12.12 HIPPS 시험 요구사항

20.1 압력센서 시험

정상상태에서는 2oo3 Voting을 사용한다.
센서 한 개를 시험할 때는 나머지 두 센서로 임시 1oo2 구조를 구성할 수 있다.

$$\text{Normal: } 2oo3$$

$$\text{One Sensor Under Test: } 1oo2$$

Voting 변경은 승인된 절차와 Interlock으로 관리해야 한다.

20.2 로직 솔버 시험

로직 솔버에는 다음 기능이 적용될 수 있다.

- Dual Processor
- Continuous Self-Diagnostics
- 고장 검출
- 안전출력
- Redundant Logic Solver 전환

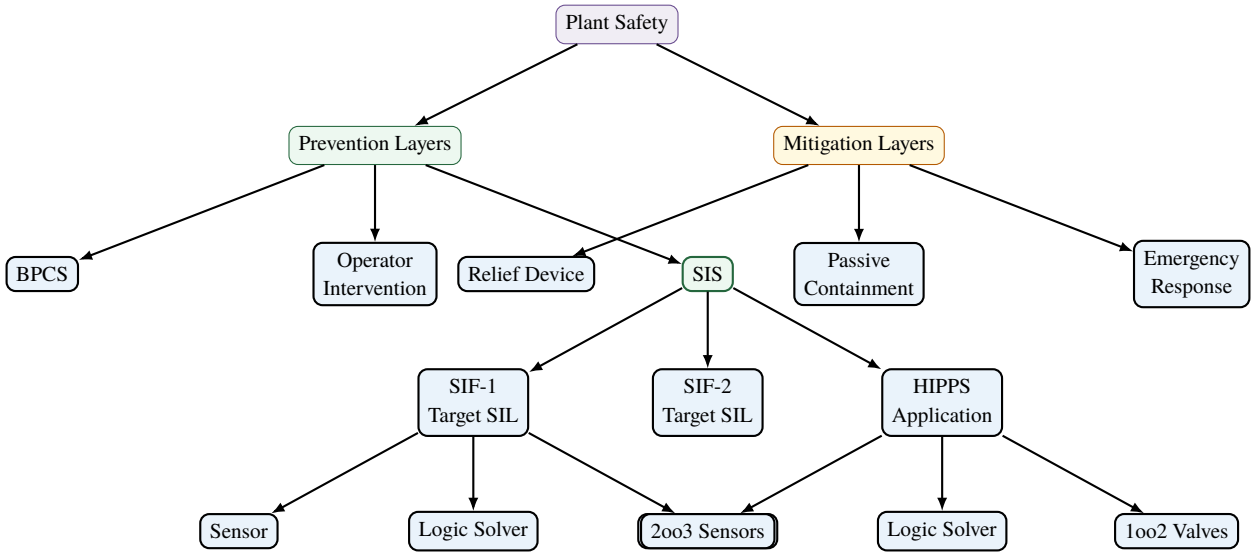
20.3 최종요소 시험

최종요소는 정해진 주기에 다음 시험을 수행한다.

- Full Stroke Proof Test
- 안전동작시간 시험
- 차단성능과 누설시험
- 운전 중 PST
- 솔레노이드와 공기공급 계통 시험

$$\boxed{\text{HIPPS Integrity} = \text{Sensor Test} + \text{Logic Test} + \text{Final Element Test}}$$

21 Chapter 12 전체 관계도



22 주요 오해와 정확한 관계

잘못된 해석	정확한 해석
SIS와 SIF는 같은 개념이다.	SIS는 여러 SIF를 포함하는 상위 시스템이다.
SIL은 밸브 한 대의 등급이다.	SIL은 특정 SIF에 할당되는 안전성능 목표이다.
SIL 인증 밸브를 사용하면 SIL을 달성한다.	센서·로직 솔버·최종요소와 수명주기를 함께 검증한다.
BPCS Trip 로직이면 모두 SIS이다.	SIS는 BPCS와 기능적으로 독립된 안전전용 경로를 요구한다.
Valve와 Final Element는 같은 의미이다.	밸브는 액추에이터와 계장품을 포함하는 최종요소의 일부이다.
PST를 수행하면 Proof Test가 필요 없다.	PST의 검출범위는 전체 Proof Test보다 작다.
시험주기가 길어져도 SIL에는 영향이 없다.	시험주기가 길어지면 숨은 고장 노출시간과 PFD가 증가한다.
HIPPS는 안전밸브처럼 압력을 방출한다.	HIPPS는 고압원을 차단하여 하류 과압을 예방한다.
이중화는 항상 HFT 향상을 보장한다.	공통원인고장과 구조에 따라 실제 HFT가 달라진다.

23 기술사 답안용 전체 스토리

1. HAZOP 등의 공정위험분석으로 위험을 식별한다.
2. BPCS, 경보, Relief Device 등 기존 보호계층과 독립보호계층을 평가한다.
3. 추가 위험감소가 필요하면 특정 위험에 대응하는 SIF를 정의한다.
4. 요구 위험감소량에 따라 SIF의 목표 SIL을 결정한다.
5. SIF를 Sensor, Logic Solver 및 Final Element로 설계한다.
6. 체계적 무결성, 구조적 제약 및 무작위 무결성을 모두 검증한다.

7. Sensor, Logic Solver 및 Final Element의 PFD 기여도를 평가한다.
8. 최종요소의 Full Stroke Proof Test와 PST를 계획한다.
9. 시험간격, 시험결과, 고장수리 및 변경사항을 전체 수명주기 동안 관리한다.
10. HIPPS와 같은 고신뢰성 적용에서는 2oo3 센서와 1oo2 차단밸브 등 적절한 Voting과 이중화 구조를 적용한다.

24 최종 핵심 관계

$$\boxed{\text{SIF}_i \subset \text{SIS}}$$

$$\boxed{\text{SIF} = \text{Sensor} \rightarrow \text{LS} \rightarrow \text{FE}}$$

$$\boxed{\text{SIL}_i = \text{target}(\text{SIF}_i)}$$

$$\boxed{\text{Valve} \subset \text{Final Element} \subset \text{SIF}}$$

$$\boxed{\text{BPCS} \cap \text{SIS} \approx \varnothing \quad \text{(기능적 독립)}}$$

$$\boxed{\text{Full Stroke Test} \subset \text{Proof Test}}$$

$$\boxed{D_{\text{PST}} \subset D_{\text{Proof}}}$$

$$\boxed{\text{PFD}_{\text{avg}} \downarrow \Longleftrightarrow \text{RRF} \uparrow \Longleftrightarrow \text{SIL} \uparrow}$$

$$\boxed{\text{HIPPS} \subset \text{SIS Applications}}$$

25 결론

안전계측시스템은 여러 안전계측기능을 포함하는 상위 시스템이다.
각 안전계측기능은 센서, 로직 솔버 및 최종요소로 구성되며, 특정 위험에 대응하는 독립된 안전기능을 수행한다.
안전무결성수준은 장치 한 대의 명칭이 아니라 각 안전계측기능에 할당되는 성능목표이다.
최종요소는 밸브만을 뜻하지 않으며, 밸브, 액추에이터, 솔레노이드, 디지털 밸브 컨트롤러 및 공기공급 계통을 포함한다.
부분 스트로크 시험은 일부 숨은 고장을 조기에 검출하지만, 전체 스트로크와 최종 차단성능을 확인하는 Proof Test를 완전히 대체하지 못한다.
따라서 기능안전은 설계 시점의 SIL 계산으로 끝나지 않고, 시험·정비·변경관리·문서화를 포함한 전체 안전수명주기 동안 유지해야 한다.

주요 키태그

Safety Instrumented System, Safety Instrumented Function, Safety Integrity Level, Probability of Failure on Demand, Final Element, Proof Test, Partial Stroke Testing, Hardware Fault Tolerance, Protection Layer, HIPPS

참고자료

- Emerson, *Control Valve Handbook*, Sixth Edition, Chapter 12: Safety Instrumented Systems.
- IEC 61508, Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-Related Systems.
- IEC 61511, Functional Safety— Safety Instrumented Systems for the Process Industry Sector.
- ISA 84 Series, Safety Instrumented Systems for the Process Industry Sector.
- OREDA, Offshore and Onshore Reliability Data.