Chapter 2 목표 SIL 결정의 정확한 절차

The Safety Critical Systems Handbook 기반

이 문서의 목적

Chapter 2의 핵심은 SIL 표에서 등급을 바로 고르는 것이 아니다. 먼저 허용 가능한 위험을 정하고, 사고가 사망 또는 손실로 전파되는 확률과 기존 보호계층을 반영하여 **최대 허용 위험사건 빈도**를 구한다. 그다음 안전기능이 담당해야 할 목표 PFD 또는 PFH를 계산한 뒤 마지막에 SIL 구간을 판정한다.

Contents

1 Chapter 2가 실제로 결정하는 것

Chapter 2는 설계가 달성한 SIL을 인증하는 장이 아니다. 위험분석을 바탕으로 각 안전기능이 달성해야 할 **목표 SIL(Target SIL)**을 정하는 장이다.

> 목표 SIL = 해당 안전기능에 요구되는 위험저감 수준

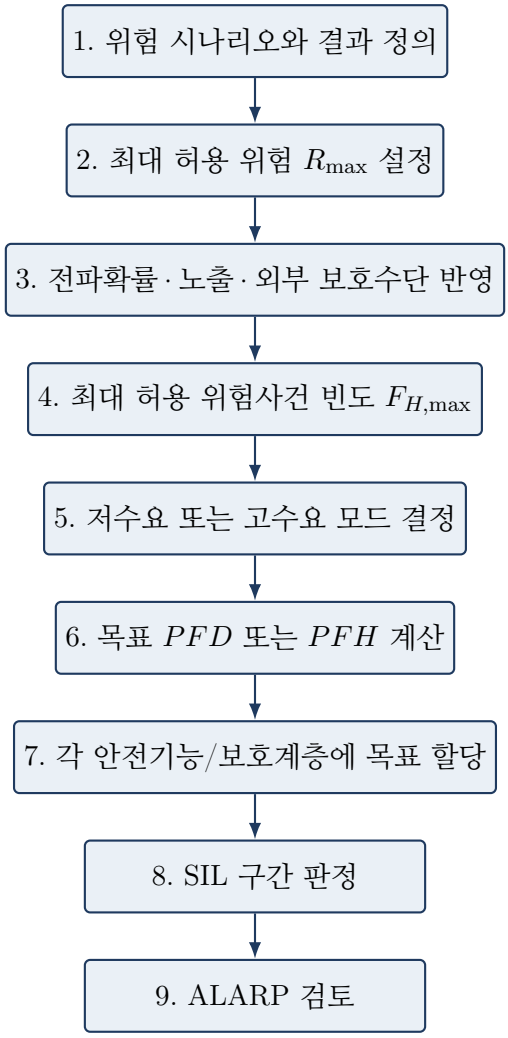
Chapter 2의 결과는 두 가지 형태로 남는다.

1. 랜덤 하드웨어 고장 평가에 사용할 **정확한 수치목표** (PFD_{avg} 또는 PFH)
2. 체계적 고장을 통제하기 위한 **SIL 등급별 생명주기 엄격도**

가장 흔한 오류

위험 시나리오와 허용 위험을 계산하지 않고 "이 기능은 중요하므로 SIL 2"라고 먼저 정하는 것은 Chapter 2의 순서와 반대이다. SIL은 위험분석의 출발점이 아니라 계산의 결과이다.

2 목표 SIL 결정의 전체 흐름



핵심 구분

최대 허용 위험은 사람에게 발생하는 사망·상해 등의 최종 위험 목표이다. **최대 허용 위험사건 빈도**는 설비의 위험사건이 발생해도 되는 최대 빈도이다. **목표** PFD/PFH는 그 위험사건을 방지하는 안전기능에 요구되는 신뢰도이다. **SIL**은 계산된 PFD/PFH가 속하는 등급이다.

3 1단계: 위험 시나리오와 최대 허용 위험

3.1 위험 시나리오를 구체적으로 정의한다

예를 들어 다음과 같이 정의한다.

$$\text{탱크 과충전} \rightarrow \text{가스 방출} \rightarrow \text{점화} \rightarrow \text{폭발} \rightarrow \text{사망}$$

위험 시나리오에는 최소한 다음이 포함되어야 한다.

- 초기사건 또는 원인
- 보호되지 않은 설비의 위험사건
- 사고가 최종 결과로 진행되는 조건
- 노출 인원과 노출시간
- 기존의 독립 보호수단
- 사망·상해·환경손실 등의 최종 결과

3.2 개인위험과 사회적 위험을 구분한다

개인위험(Individual Risk)은 특정 위험으로 인해 가상의 한 사람이 사망할 연간 빈도이다. **사회적 위험(Societal Risk)**은 한 사고에서 다수의 사망자가 발생할 가능성을 고려한다.

다수 사망 시나리오는 동일한 사망자 수가 여러 단일 사고로 나뉘는 경우보다 더 엄격하게 평가될 수 있다. 따라서 사고의 예상 사망자 수에 따라 최대 허용 위험을 조정해야 한다.

3.3 여러 위험원이 같은 사람에게 동시에 작용할 때

하나의 장소에서 동일한 사람이 여러 위험원에 노출되면, 전체 허용 위험을 각 위험원에 나누어 배분해야 한다.

예를 들어 전체 허용 위험이 10^{-4}/yr이고 동일한 사람에게 동시에 작용하는 위험원이 10개라면, 각 위험기능의 평균 목표는 다음과 같이 더 엄격해질 수 있다.

$$R_{\text{max,per hazard}} = \frac{10^{-4}}{10} = 10^{-5}/\text{yr}$$

4 2단계: 최대 허용 위험사건 빈도

4.1 왜 위험과 위험사건 빈도를 구분하는가

위험사건이 발생한다고 항상 사망으로 이어지는 것은 아니다. 사고가 최종 결과로 진행되는 조건을 확률로 반영해야 한다.

대표적인 인자는 다음과 같다.

- 설비가 위험을 제공하는 시간 비율
- 별도의 외부 완화수단이 실패할 확률
- 누출 · 과압 · 과열 등이 실제 사고로 전개될 확률
- 사람이 위험범위에 있을 확률
- 점화 또는 폭발 확률
- 사고가 사망으로 이어질 조건부 확률

4.2 기본식

사고 전파인자와 외부 보호수단 실패확률을 $p_1, p_2, \ldots, p_n$이라 하면,

$$R = F_H \times \prod_{i=1}^{n} p_i$$

이므로 최대 허용 위험사건 빈도는

$$\boxed{F_{H,\max} = \frac{R_{\max}}{\prod_{i=1}^{n} p_i}}$$

이다.

여기서:

- $R_{\max}$: 최대 허용 사망 · 상해 위험 (/yr)
- $F_{H,\max}$: 최대 허용 위험사건 빈도 (/yr)
- p_i: 노출, 점화, 치명성, 외부 보호계층 실패 등의 조건부 확률

> **계산 방향**
> 전파확률이 작을수록 하나의 위험사건이 최종 사망으로 이어질 가능성이 작다. 따라서 $R_{\max}$를 전파확률의 곱으로 나누어 위험사건의 최대 허용 빈도를 구한다.

5 3단계: 운전모드 결정

목표 $F_{H,\max}$를 구한 뒤, 보호기능이 저수요인지 고수요 · 연속 운전인지 구분한다.

구분	저수요 모드	고수요 · 연속 모드
기능의 성격	정상 제어와 분리된 추가 보호시스템이 드문 Demand에 대응	제어기능의 고장이 곧바로 위험에 노출시키거나 지속적으로 기능이 필요함
주요 지표	PFD_{avg}: 요구 시 실패할 평균확률	PFH: 시간당 위험고장빈도
단위	무차원 확률	1/h
책의 판단 기준	Demand가 연 1회 이하인 추가 보호기능이 대표적	Demand가 연 1회를 초과하거나 계속 위험에 노출되는 경우

6 4단계: 저수요 기능의 목표 PFD

6.1 계산식

보호되지 않은 EUC의 위험사건 빈도를 F_{EUC}라 하면,

$$F_{\text{residual}} = F_{\text{EUC}} \times PFD_{\text{target}}$$

잔여 위험사건 빈도가 최대 허용값 이하가 되어야 하므로,

$$\boxed{PFD_{\text{target}} = \frac{F_{H,\max}}{F_{\text{EUC}}}}$$

이다.

6.2 Chapter 2의 단순 저수요 예

$$\begin{aligned} R_{\max} &= 10^{-5}/\text{yr} \\ P(\text{fatality} \mid \text{hazardous event}) &= 10^{-2} \\ F_{H,\max} &= \frac{10^{-5}}{10^{-2}} = 10^{-3}/\text{yr} \\ F_{\text{EUC}} &= 2 \times 10^{-1}/\text{yr} \\ PFD_{\text{target}} &= \frac{10^{-3}}{2 \times 10^{-1}} = 5 \times 10^{-3} \end{aligned}$$

5×10^{-3}은 저수요 SIL 2 구간에 속한다.

이 예의 의미

SIL 2를 먼저 정한 것이 아니다. 사망위험 목표에서 위험사건 허용빈도를 구하고, 이를 보호되지 않은 설비의 위험사건 빈도로 나누어 목표 PFD를 구한 뒤 SIL 2를 판정하였다.

7 5단계: 고수요 · 연속 기능의 목표 PFH

고수요 또는 연속 운전에서는 보호기능의 고장이 직접 위험고장빈도가 된다. 따라서 연간 최대 허용 위험사건 빈도를 시간당 빈도로 환산한다.

$$\boxed{PFH_{\text{target}} = \frac{F_{H,\max}}{8760}}$$

7.1 Chapter 2의 단순 고수요 예

$$\begin{aligned} R_{\max} &= 10^{-5}/\text{yr} \\ P(\text{fatality} \mid \text{incident}) &= \frac{1}{400} \\ F_{H,\max} &= 10^{-5} \times 400 = 4 \times 10^{-3}/\text{yr} \\ PFH_{\text{target}} &= \frac{4 \times 10^{-3}}{8760} \approx 4.6 \times 10^{-7}/\text{h} \end{aligned}$$

4.6×10^{-7}/h는 고수요 SIL 2 구간에 속한다.

8 6단계: SIL 구간 판정

SIL	저수요 PFD_{avg}	고수요 · 연속 PFH
4	$10^{-5} \le PFD < 10^{-4}$	$10^{-9} \le PFH < 10^{-8}$/h
3	$10^{-4} \le PFD < 10^{-3}$	$10^{-8} \le PFH < 10^{-7}$/h
2	$10^{-3} \le PFD < 10^{-2}$	$10^{-7} \le PFH < 10^{-6}$/h
1	$10^{-2} \le PFD < 10^{-1}$	$10^{-6} \le PFH < 10^{-5}$/h

수치목표를 버리지 않는다

정확한 목표가 $PFD = 2 \times 10^{-3}$으로 계산되었다면 설계평가에서도 단순히 "SIL 2 범위"만 충족하는 것이 아니라 원래 계산한 2×10^{-3} 목표를 만족하는지 확인하는 것이 원칙이다.

9 여러 보호계층이 있을 때의 SIL 할당

하나의 위험에 두 개 이상의 독립 보호계층이 있으면 전체 요구 PFD를 각각의 계층에 배분할 수 있다. 두 독립 계층의 PFD를 PFD_1, PFD_2라 하면,

$$PFD_{\text{total}} = PFD_1 \times PFD_2$$

이어야 한다.

예를 들어 전체 목표가

$$PFD_{\text{total}} \le 5.3 \times 10^{-3}$$

이라면 가능한 배분은 다양하다.

보호계층 1	등급	보호계층 2	등급
2×10^{-1}	SIL 1 미만	2.65×10^{-2}	SIL 1
7.3×10^{-2}	SIL 1	7.3×10^{-2}	SIL 1
7×10^{-1}	SIL 1 미만	7.57×10^{-3}	SIL 2

핵심

위험 시나리오 전체를 무조건 "SIL 2 시스템"이라고 부르면 안 된다. 먼저 전체 위험저감 목표를 정하고, 각 독립 보호계층에 PFD를 할당한 뒤 각 계층 또는 안전기능의 SIL을 각각 판정한다.

9.1 독립성 조건

곱셈으로 위험저감 효과를 인정하려면 다음이 성립해야 한다.

- 초기사건과 각 보호계층이 독립적일 것
- 보호계층 상호 간에 독립적일 것
- 공통 전원, 공통 센서, 공통 로직, 공통 정비 등 CCF를 고려할 것
- 독립성이 부족하면 해당 계층을 인정하지 않거나 더 높은 PFD를 사용할 것

10 LOPA에 의한 결정

LOPA는 HAZOP 이후에 수행할 수 있는 구조화된 반정량적 위험분석이다. 주로 저수요 안전기능에 적용한다.

$$F_{\text{mitigated}} = F_{\text{initiating}} \times P_{\text{vulnerability}} \times \prod PFD_{\text{IPL}} \times PFD_{\text{SIF}}$$

따라서 추가 SIF의 목표는

$$\boxed{PFD_{\text{SIF,target}} = \frac{F_{\text{tolerable}}}{F_{\text{initiating}} \times P_{\text{vulnerability}} \times \prod PFD_{\text{IPL}}}}$$

로 구할 수 있다.

LOPA의 주요 입력은 다음과 같다.

- 설비와 공정 설계자료
- 보호가 없을 때의 사고 결과
- 결과의 심각도 등급
- 모든 초기사건과 발생빈도
- 취약성 또는 사고 전파확률
- 안전계장기능의 설명
- 기계적 보호장치와 방유제 등 독립 보호계층

LOPA의 출력은 다음과 같다.

- 추가 계장보호가 없을 때의 중간 사고빈도
- 추가 보호계장 요구 여부
- 완화 후 사고빈도
- 안전계장기능의 목표 PFD

> **LOPA의 주의사항**
> LOPA는 단순 표 채우기가 아니다. 공통원인으로 두 보호계층이 연결되면 독립성을 인정할 수 없고, 보호계층별로 위험목표를 배분하지 않으면 과대평가가 발생한다.

11 Risk Graph에 의한 결정

Risk Graph는 다음 요소를 범주화하여 SIL을 추정한다.

- 결과의 심각도
- 위험에 노출되는 빈도와 시간
- 위험 회피 가능성
- 원하지 않는 사건 또는 Demand의 발생 가능성
- 절차 · 경보 · 기계적 보호수단

그러나 Risk Graph는 연속적인 확률을 큰 범주로 나누고 여러 단계에서 "약 10배" 수준의 판단을 반복하기 때문에 오차가 커질 수 있다.

Chapter 2의 취지는 다음과 같다.

- 정량적 방법 또는 LOPA를 우선한다.
- Risk Graph는 정량화가 어려울 때 사용하는 보조수단이다.
- 저수요 목표에만 적합하다.
- 다수 안전기능의 초기 선별에 사용할 수 있다.
- SIL 2 이상이 나오면 정량적 방법으로 다시 확인한다.

12 SIL은 안전기능에 부여한다

SIL은 명확하게 정의된 안전기능에만 부여한다.

예를 들어 고유량 위험을 방지하는 기능은 다음과 같이 구성될 수 있다.

유량 트랜스미터 → 로직솔버 → 솔레노이드 밸브

이 전체 기능이 특정 위험에 대해 안전상태를 만들기 때문에 목표 SIL을 가진다. 트랜스미터 단품은 적용 시나리오와 무관하게 하나의 SIL을 갖는다고 말할 수 없다.

단품에는 다음과 같은 표현이 더 정확하다.

- 특정 SIL까지 적용할 수 있는 체계적 능력
- 고장률, SFF, 진단범위 및 HFT 자료
- Safety Manual에 명시된 적용조건

13 SIL 1 미만과 SIL 4

13.1 SIL 1 미만

계산된 목표가 SIL 1보다 완화된 경우 IEC 61508 의미에서 “not safety-related” 또는 “no special safety requirement”로 표현할 수 있다.

다만 SIL 1의 정성적 요구는 대부분 기본적인 우수 엔지니어링 실무이므로, SIL 1 수준의 관리원칙을 좋은 실무기준으로 적용할 수 있다.

13.2 SIL 4

SIL 4는 매우 높은 설계 · 분석 · 검증 노력을 요구한다. Chapter 2는 하나의 기능에 SIL 4를 집중시키기보다 추가적인 독립 위험저감 계층을 도입하여 각 계층의 목표를 낮추는 방향을 권고한다.

14 ALARP는 SIL 결정 후에 다시 확인한다

최대 허용 위험과 목표 SIL을 만족했다고 평가가 끝나는 것은 아니다.

ALARP(As Low As Reasonably Practicable)는 추가 위험저감 비용이 얻을 수 있는 위험저감 편익에 비해 심하게 불균형하지 않다면 추가 조치를 시행해야 한다는 원칙이다.

$$\text{목표 SIL 만족} \not\Rightarrow \text{추가 위험저감 검토 종료}$$

따라서 목표 SIL 결정과 설계평가 후에도 다음을 검토한다.

- 추가 독립 보호계층
- 더 짧은 Proof Test 주기
- 진단기능 강화
- 공정 자체의 본질안전 설계
- 설비배치와 물리적 완화수단

15 정확한 목표 SIL 결정 체크리스트

1. 위험 시나리오와 최종 결과를 한 문장으로 정의했는가?
2. 개인위험과 사회적 위험 중 적절한 기준을 선택했는가?
3. 동일한 사람이 여러 위험원에 노출되는 경우 위험목표를 배분했는가?
4. 노출 · 점화 · 사망 · 외부 완화수단의 조건부 확률을 근거와 함께 기록했는가?

5. 최대 허용 위험사건 빈도 $F_{H,\max}$를 먼저 계산했는가?
6. 저수요와 고수요 · 연속 운전모드를 올바르게 구분했는가?
7. 저수요는 $F_{H,\max}/F_{\mathrm{EUC}}$로 목표 PFD를 구했는가?
8. 고수요는 $F_{H,\max}$를 시간당 PFH로 환산했는가?
9. 여러 보호계층의 독립성과 CCF를 확인했는가?
10. 전체 PFD를 각 보호계층에 명시적으로 할당했는가?
11. SIL은 장비 단품이 아니라 안전기능별로 판정했는가?
12. 정확한 수치목표와 SIL 등급을 모두 기록했는가?
13. 마지막으로 ALARP를 검토했는가?

16 기술사 답안용 요약

단계	답안 핵심
위험기준 설정	개인 · 사회적 위험과 사고결과를 고려하여 최대 허용 위험을 설정한다.
위험사건 목표	노출, 점화, 치명성 및 외부 보호계층을 반영하여 최대 허용 위험사건 빈도를 산정한다.
운전모드 구분	드문 Demand에 대응하는 추가 보호기능은 저수요, 지속적으로 위험을 제어하는 기능은 고수요 · 연속으로 구분한다.
정량목표 계산	저수요는 목표 PFD, 고수요 · 연속은 목표 PFH를 계산한다.
보호계층 할당	독립 보호계층의 PFD 곱이 전체 목표를 만족하도록 각 기능에 목표를 할당한다.
SIL 판정	계산된 PFD/PFH를 SIL 구간에 대응시킨다.
사후 검토	SIL 2 이상은 정량적 방법으로 확인하고, 최종적으로 ALARP를 검토한다.

한 문장 정리

Chapter 2의 목표 SIL 결정은 **허용 위험 설정** → **위험사건 허용빈도 산정** → **운전모드 구분** → **목표 PFD/PFH 계산** → **보호계층별 할당** → **SIL 판정** → **ALARP 검토** 순서로 수행한다.

참고문헌

David J. Smith and Kenneth G. L. Simpson, *The Safety Critical Systems Handbook: A Straightforward Guide to Functional Safety, IEC 61508, IEC 61511 and Related Guidance*, 4th ed., Butterworth-Heinemann, 2016, Chapter 2, pp. 25–55.

학습 대상 블로그: https://now0930.pe.kr/wordpress/the-safety-critical-system-chapter2/