

Chapter 1 · 2 · 5 통합 정리

허용위험에서 부품 위험고장률까지

The Safety Critical Systems Handbook 기반 학습 노트

문서 범위

이 문서는 Chapter 3의 하드웨어 설계 요구사항을 정리하는 문서가 아니다. Chapter 1, Chapter 2, Chapter 5를 연결하여 다음 흐름을 설명한다.

허용위험 → 위험사건 허용빈도 → 목표 PFD/PFH → 목표 SIL
→ 고장모드 → λ, μ, MDT, T → 실제 PFD/PFH

Contents

1	먼저 용어 · 단위 · 대상을 구분한다	3
1.1	위험목표와 안전기능 목표	3
1.2	부품 신뢰도와 시간 관련 용어	3
2	λ , 고장확률, 비가용도의 관계	4
2.1	λ 는 확률이 아니다	4
2.2	복구 가능한 부품의 2상태 모델	4
2.3	MDT를 이용한 표현	5
2.4	Q 와 PFD 의 관계	5
3	고장모드와 λ 의 분류	6
3.1	고장원인 · 고장모드 · 고장영향	6
3.2	Safe 또는 Dangerous는 안전기능을 기준으로 결정한다	6
3.3	전체 고장률의 분해	7
4	검출 위험고장과 미검출 위험고장	7
4.1	위험 검출 고장: λ_{DD}	7
4.2	위험 미검출 고장: λ_{DU}	8
4.3	왜 $\lambda/(\lambda + \mu)$ 를 DU 에 그대로 적용하지 않는가	9
4.4	단순 1oo1 부품의 PFD 근사식	9

5	허용위험에서 목표 SIL까지	9
5.1	최대 허용위험에서 위험사건 허용빈도로	9
5.2	저수요 기능의 목표 PFD	10
5.3	고수요·연속 기능의 목표 PFH	10
5.4	SIL 구간	11
6	목표 SIL에서 부품 고장률 요구치까지	11
6.1	안전기능의 구성	11
6.2	고장모드별 λ 를 얻는다	11
6.3	부품의 허용 λ_{DU} 역산	12
7	중복구조와 공통원인고장	13
8	전체 스토리	13
8.1	1단계: 위험 시나리오와 최종 피해를 정의한다	14
8.2	2단계: Maximum Tolerable Risk를 정한다	15
8.3	3단계: 위험사건의 최대 허용빈도를 계산한다	15
8.4	4단계: 저수요와 고수요·연속 운전모드를 구분한다	15
8.5	5단계: 정량목표를 SIL 구간에 대응시킨다	16
8.6	6단계: 안전기능을 구성요소로 모델링한다	17
8.7	7단계: 각 부품의 고장모드를 식별한다	17
8.8	8단계: 전체 λ 를 고장범주별로 나눈다	18
8.9	9단계: λ 를 비가용도와 PFD로 변환한다	18
8.10	10단계: 구성요소와 시스템의 실제 PFD를 계산한다	19
8.11	11단계: 처음 설정한 정량목표와 비교한다	21
8.12	전체 수치 예제의 연결	21
9	최종 판정과 주의사항	22
	참고문헌	23

1 먼저 용어 · 단위 · 대상을 구분한다

기능안전 계산에는 사람의 위험, 위험사건의 빈도, 안전기능의 실패확률, 부품의 고장률이 함께 나타난다. 이 값들은 의미와 단위가 서로 다르다.

1.1 위험목표와 안전기능 목표

용어	기호	의미	단위
Maximum Tolerable Risk	$R_{\max}$	사망 · 상해 등 정해진 최종 피해에 대해 허용하는 최대 위험	yr^{-1}
Maximum Tolerable Failure Rate	$F_{H,\max}$	해당 최종 피해로 이어질 수 있는 위험사건의 최대 허용 발생빈도	yr^{-1}
사고 전파확률	p_i	위험사건이 노출 · 점화 · 사망 등 최종 피해로 진행될 조건부 확률	무차원
Demand Frequency	F_D	안전기능이 작동해야 하는 원인사건 또는 요구의 발생빈도	yr^{-1}
Probability of Failure on Demand	PFD	Demand가 발생했을 때 안전기능이 실패할 확률	무차원
Average PFD	PFD_{avg}	Proof Test 주기 전체에서 평균한 PFD	무차원
Probability of dangerous Failure per Hour	PFH	고수요 · 연속 안전기능의 시간당 위험고장빈도	h^{-1}
Safety Integrity Level	SIL	안전기능에 요구되는 무결성의 이산 등급	없음

1.2 부품 신뢰도와 시간 관련 용어

용어	기호	의미	단위
Failure Rate	λ	정상상태에서 고장상태로 전이하는 단위 시간당 비율	h^{-1}
Repair or Restoration Rate	μ	고장상태에서 정상상태로 복구되는 단위 시간당 비율	h^{-1}
Mean Down Time	MDT	고장 발생부터 기능 복구까지 고장상태로 존재하는 평균시간	h
Mean Repair Time	MRT	실제 수리작업에 필요한 평균시간	h
Proof Test Interval	T	자동진단으로 찾지 못한 잠복고장을 확인하는 시험 간격	h, yr
Unavailability	Q	임의 시점에 장치가 고장상태일 확률	무차원
Beta Factor	β	전체 고장 중 공통원인고장으로 취급하는 비율	무차원

가장 먼저 바로잡아야 할 표현

$F_{H,\max}$ 와 λ 는 모두 문장상 “failure rate”로 보일 수 있지만 대상이 다르다.

$$F_{H,\max} \neq \lambda$$

$F_{H,\max}$ 는 위험사건의 허용빈도이고, λ 는 센서·로직솔버·밸브 등의 부품 고장률이다.

2 λ , 고장확률, 비가용도의 관계

2.1 λ 는 확률이 아니다

λ 는 단위시간당 고장률이다.

$$[\lambda] = h^{-1}$$

일정한 고장률을 가정하면 시간 t 이내에 고장이 발생할 정확한 확률은,

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

이다.

$\lambda t \ll 1$ 이면,

$$P_f(t) \approx \lambda t$$

로 근사한다.

표현	의미	단위
λ	단위시간당 고장률	h^{-1}
λt	시간 t 동안의 누적 고장위험도 또는 기대 고장횟수	무차원
$1 - e^{-\lambda t}$	시간 t 이내 최소 한 번 고장날 확률	무차원

2.2 복구 가능한 부품의 2상태 모델

복구 가능한 부품은 다음 두 상태를 반복한다고 본다.

$$\text{정상} \xrightarrow{\lambda} \text{고장} \xrightarrow{\mu} \text{정상}$$

λ 는 고장상태로 들어가는 속도이고, μ 는 고장상태에서 빠져나오는 속도이다.

정상상태 확률을 P_U , 고장상태 확률을 P_D 라고 하면 정상상태에서,

$$P_U \lambda = P_D \mu$$

이고,

$$P_U + P_D = 1$$

이다. 따라서,

$$Q = P_D = \frac{\lambda}{\lambda + \mu}$$

이다.

2.3 MDT를 이용한 표현

단순 2상태 모델에서 유효 복구율을,

$$\mu = \frac{1}{MDT}$$

로 정의하면,

$$Q = \frac{\lambda}{\lambda + \frac{1}{MDT}} = \frac{\lambda MDT}{1 + \lambda MDT}$$

이다.

$\lambda MDT \ll 1$ 이면,

$$Q \approx \lambda MDT$$

이다.

식의 물리적 의미

$$\text{비가용도} \approx \text{고장 발생속도} \times \text{고장상태 지속시간}$$

고장이 자주 발생할수록 Q 가 커지고, 고장상태가 오래 지속될수록 Q 가 커진다.

2.4 Q 와 PFD의 관계

저수요 안전기능의 Demand가 운전기간 중 임의의 시점에 발생한다고 가정한다. Demand 순간에 장치가 고장상태이면 기능이 실패하므로 단순한 경우,

$$PFD \approx Q$$

로 연결할 수 있다.

그러나 이는 저수요 기능과 임의 Demand 가정에서 사용하는 관계이다. 모든 Q 가 항상 PFD와 동일한 것은 아니다.

3 고장모드와 λ 의 분류

3.1 고장원인 · 고장모드 · 고장영향

구분	질문	예
Failure Cause	왜 고장났는가?	부식, 결빙, 전원 상실, 설계 오류
Failure Mode	어떻게 고장났는가?	밸브 열림 고착, 센서 Low 고착
Failure Effect	그 결과 무엇이 발생하는가?	과압 미검출, 비상차단 실패

고장원인 → 고장모드 → 고장영향

예를 들면,

수분 결빙 → 밸브 열림 고착 → 과압 시 차단 실패

이다.

3.2 Safe 또는 Dangerous는 안전기능을 기준으로 결정한다

고장모드 자체가 항상 안전고장 또는 위험고장으로 고정되는 것은 아니다. 다음 사항을 먼저 정의해야 한다.

1. 안전기능
2. 안전상태
3. Demand
4. 허용 응답시간
5. 시스템 경계

예를 들어 안전기능을 다음과 같이 정의한다.

압력이 10 bar를 초과하면 2s 이내에 차단밸브를 완전히 닫는다.

고장모드	안전기능에 미치는 영향	분류
열림 상태로 고착	과압 시 차단 실패	위험고장
요구 없이 닫힘	생산중단, 안전상태 이동	안전고장
닫힘시간 초과	허용시간 내 차단 실패	위험고장
내부 누설	완전한 격리 실패	위험고장
위치 피드백 오류	실제 상태 오판	영향 분석 필요

3.3 전체 고장률의 분해

부품의 전체 고장률은 안전기능에 미치는 영향과 검출 여부에 따라 나눈다.

$$\lambda_{\text{total}} = \lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}$$

안전기능에 영향이 없는 고장을 별도 분류하면,

$$\lambda_{\text{total}} = \lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU} + \lambda_{NE}$$

로 표현할 수 있다.

기호	명칭	의미
λ_{SD}	Safe Detected	안전고장이 자동으로 검출됨
λ_{SU}	Safe Undetected	안전고장이 자동으로 검출되지 않음
λ_{DD}	Dangerous Detected	위험고장이 자동진단으로 검출됨
λ_{DU}	Dangerous Undetected	위험고장이 Proof Test 또는 Demand 전까지 검출되지 않음
λ_{NE}	No Effect	해당 안전기능에 영향을 주지 않음

안전고장률은,

$$\lambda_S = \lambda_{SD} + \lambda_{SU}$$

위험고장률은,

$$\lambda_D = \lambda_{DD} + \lambda_{DU}$$

이다.

4 검출 위험고장과 미검출 위험고장

4.1 위험 검출 고장: λ_{DD}

자동진단으로 위험고장이 발견되면 수리와 복구가 시작된다.

정상 $\xrightarrow{\lambda_{DD}}$ 위험고장 검출 $\xrightarrow{\mu}$ 정상

이 경우 단순 2상태 모델의 비가용도는,

$$Q_{DD} = \frac{\lambda_{DD}}{\lambda_{DD} + \mu}$$

이다.

$$\mu = \frac{1}{MDT_{DD}}$$

이면,

$$Q_{DD} = \frac{\lambda_{DD}MDT_{DD}}{1 + \lambda_{DD}MDT_{DD}}$$

이고, 작은 값에서는,

$$Q_{DD} \approx \lambda_{DD}MDT_{DD}$$

이다.

검출 후 Down Time은 다음처럼 볼 수 있다.

$$MDT_{DD} \approx MRT + L$$

여기서 L 은 작업허가, 정비인력 도착, 예비품 확보, 복구시험 등의 지연시간이다.

4.2 위험 미검출 고장: λ_{DU}

위험 미검출 고장은 고장이 발생해도 자동진단으로 발견되지 않는다.

고장 발생 → 잠복 → Proof Test에서 검출 → 수리

Proof Test 주기를 T 라고 하면 평균 검출지연은,

$$\frac{T}{2}$$

이다.

따라서,

$$MDT_{DU} \approx \frac{T}{2} + MRT + L$$

이고,

$$Q_{DU,avg} \approx \lambda_{DU} \left(\frac{T}{2} + MRT + L \right)$$

이다.

보통 $T/2$ 가 수리시간과 지연시간보다 훨씬 크면,

$$PFD_{avg} \approx \frac{\lambda_{DU}T}{2}$$

로 근사한다.

4.3 왜 $\lambda/(\lambda + \mu)$ 를 DU에 그대로 적용하지 않는가

$$Q = \frac{\lambda}{\lambda + \mu}$$

는 고장이 발생한 뒤 일정한 복구율로 복구가 시작되는 단순 2상태 모델이다.

그러나 DU 고장은 Proof Test 전까지 검출되지 않으므로 복구가 즉시 시작되지 않는다. 따라서 DU에서는 Proof Test 대기시간을 포함한 평균 Down Time을 사용해야 한다.

같은 기본원리

$$Q \approx \lambda \times \text{고장상태 지속시간}$$

- DD 고장: 지속시간 $\approx MDT_{DD}$
- DU 고장: 지속시간 $\approx T/2 + MRT + L$

4.4 단순 1oo1 부품의 PFD 근사식

$$PFD_i \approx \lambda_{DU,i} \left(\frac{T_i}{2} + MRT_i + L_i \right) + \lambda_{DD,i} MDT_{DD,i}$$

수리시간이 Proof Test 주기보다 매우 짧으면,

$$PFD_i \approx \frac{\lambda_{DU,i} T_i}{2} + \lambda_{DD,i} MDT_{DD,i}$$

이다.

근사식의 적용 조건

이 식은 단순한 저수요 1oo1 모델과 작은 고장확률을 전제로 한 근사식이다. 중복구조, 공통원인고장, 불완전 Proof Test, 시험 중 Bypass가 있으면 별도의 신뢰도 모델이 필요하다.

5 허용위험에서 목표 SIL까지

5.1 최대 허용위험에서 위험사건 허용빈도로

위험사건이 최종 피해로 진행되는 조건부 확률을 p_i 라고 하면,

$$R_{\max} = F_{H,\max} \prod_i p_i$$

이다.

따라서,

$$F_{H,\max} = \frac{R_{\max}}{\prod_i p_i}$$

이다.

$R_{\max}$ 는 사람의 사망·상해 등 최종 피해에 대한 허용위험이고, $F_{H,\max}$ 는 그 피해로 이어질 수 있는 위험 사건의 허용빈도이다.

5.2 저수요 기능의 목표 PFD

보호기능이 없을 때 안전기능에 Demand를 발생시키는 빈도를 F_D 라고 하면,

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

이다.

잔여 위험사건 빈도는 허용빈도 이하이어야 하므로,

$$F_D \times PFD_{\text{target}} \leq F_{H,\max}$$

이다.

따라서,

$$PFD_{\text{target}} \leq \frac{F_{H,\max}}{F_D}$$

이다.

5.3 고수요·연속 기능의 목표 PFH

고수요·연속 기능에서 안전기능의 위험고장빈도가 위험사건 허용빈도와 직접 대응하고, $F_{H,\max}$ 가 연간 단위로 주어졌다면,

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

으로 환산할 수 있다.

다른 조건부 확률이나 보호계층이 있으면 이를 먼저 반영해야 한다.

5.4 SIL 구간

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

SIL은 계산의 출발점이 아니다

먼저 허용위험과 위험사건 허용빈도를 계산한다. 그다음 목표 PFD 또는 PFH 를 구하고 마지막에 SIL 구간을 판정한다. 또한 정확한 수치목표를 SIL 등급으로 대체하면 안 된다.

6 목표 SIL에서 부품 고장률 요구치까지

6.1 안전기능의 구성

안전계장기능은 보통 다음 세 부분으로 구성된다.

센서 → 로직솔버 → 최종요소

단순한 1oo1 직렬구조에서 각 PFD 가 충분히 작으면,

$$PFD_{SIF} \approx PFD_S + PFD_L + PFD_F$$

이다.

전체 목표를 구성요소에 배분하는 것은 설계상 필요한 신뢰도 예산 배분이다. 표준이 센서 · 로직 · 최종요소의 비율을 일률적으로 정하는 것은 아니다.

6.2 고장모드별 λ 를 얻는다

과압 차단용 압력센서를 예로 들면 다음과 같다.

고장모드	결과	분류 예
출력 Low 고착	실제 과압 미검출	λ_{DU}
출력 High 고착	정상상태에서 거짓 Trip	λ_S
단선, 자동진단됨	경보 또는 안전정지	기능에 따라 SD 또는 DD
일정값 고착, 미검출	과압 미검출	λ_{DU}
응답 지연	허용시간 내 Trip 실패	λ_D
출력 노이즈	거짓 Trip 또는 미검출	영향에 따라 분류

따라서,

$$\lambda_{DU,S} = \lambda_{\text{Low 고착}} + \lambda_{\text{미검출 고정값}} + \lambda_{\text{위험 응답지연}} + \dots$$

이다.

6.3 부품의 허용 λ_{DU} 역산

부품 i 에 할당한 PFD 예산을 $PFD_{i,\text{target}}$ 이라고 하자.

$$PFD_i \approx \frac{\lambda_{DU,i}T_i}{2} + \lambda_{DD,i}MDT_{DD,i}$$

이므로,

$$\frac{\lambda_{DU,i}T_i}{2} + \lambda_{DD,i}MDT_{DD,i} \leq PFD_{i,\text{target}}$$

이어야 한다.

이를 $\lambda_{DU,i}$ 에 대해 정리하면,

$$\lambda_{DU,i} \leq \frac{2(PFD_{i,\text{target}} - \lambda_{DD,i}MDT_{DD,i})}{T_i}$$

이다.

DD 항이 충분히 작으면,

$$\lambda_{DU,i} \leq \frac{2PFD_{i,\text{target}}}{T_i}$$

로 단순화할 수 있다.

센서 위험 미검출 고장률 요구치

센서 PFD 예산을,

$$PFD_{S,\text{target}} = 1.5 \times 10^{-3}$$

Proof Test 주기를,

$$T = 8760 \text{ h}$$

라고 하자. DD 항이 충분히 작다면,

$$\lambda_{DU,S} \leq \frac{2 \times 1.5 \times 10^{-3}}{8760}$$

이므로,

$$\lambda_{DU,S} \leq 3.42 \times 10^{-7} / \text{h}$$

이다.

이는 센서의 전체 고장률이 아니라, 과압 미검출을 유발하는 모든 위험 미검출 고장모드의 고장률 합에 대한 요구치이다.

7 중복구조와 공통원인고장

앞의 역산은 단순 1oo1 모델이다.

실제 시스템에서는 다음 항목을 함께 고려해야 한다.

- 1oo1, 1oo2, 2oo3 등의 Voting 구조
- 진단범위
- Proof Test Coverage
- 시험 중 Bypass
- 수리 중 운전방식
- 채널 독립성
- 공통원인고장 CCF와 β

따라서 최종 시스템 PFD는 일반적으로,

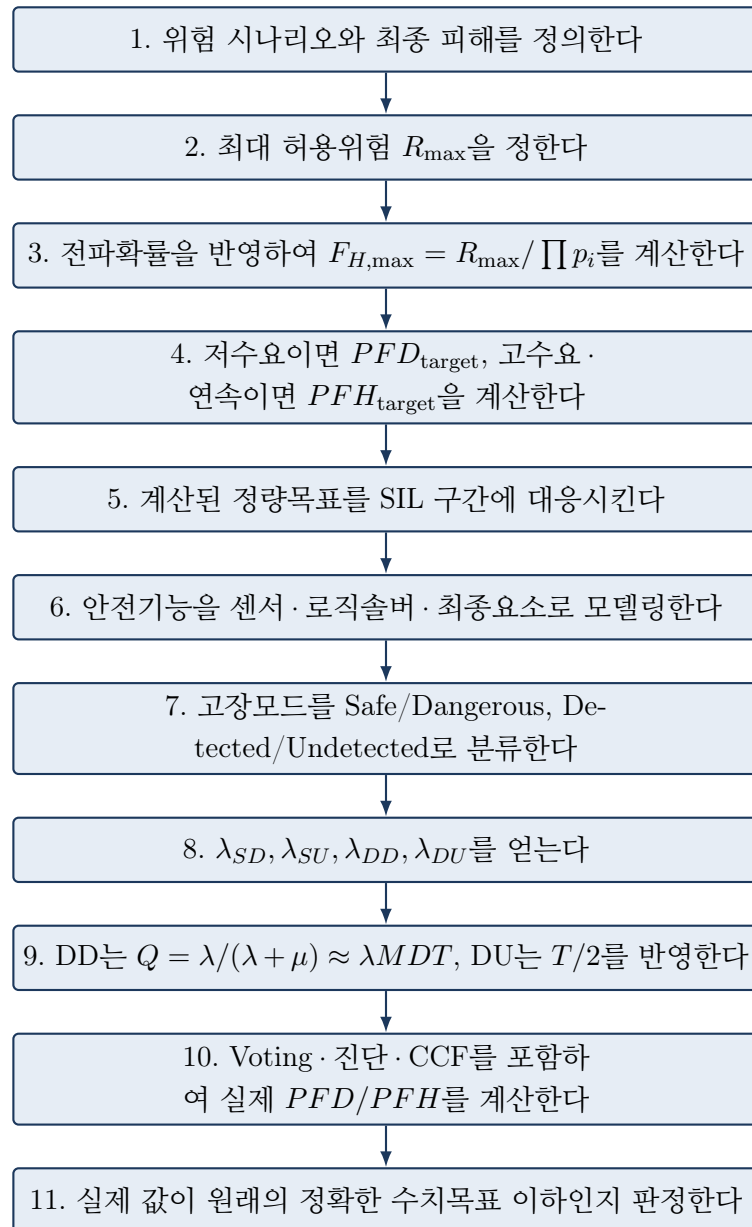
$$PFD_{\text{assessed}} = f(\lambda_{DU}, \lambda_{DD}, T, MDT, \text{Voting}, \beta, \text{Proof Test Coverage})$$

로 표현된다.

1oo2 구조에서는 독립고장에 의한 동시고장 확률이 감소하지만, CCF는 두 채널을 동시에 무력화하므로 작은 β 도 전체 PFD를 지배할 수 있다.

8 전체 스토리

앞의 절에서는 각 식과 용어를 개별적으로 설명하였다. 이 절에서는 그 내용을 하나의 안전기능이 설계되는 순서에 맞추어 연결한다.



8.1 1단계: 위험 시나리오와 최종 피해를 정의한다

계산은 부품의 고장률에서 시작하지 않는다. 먼저 어떤 위험조건이 어떤 사고를 거쳐 어떤 피해로 이어지는지를 정의한다.

예를 들어 과압 보호기능의 위험 시나리오는 다음과 같다.

압력 상승 → 압력용기 파열 → 위험물질 누출 → 점화 → 사망

여기서 안전기능은 다음과 같이 정의할 수 있다.

압력이 설정값을 초과하면 정해진 시간 이내에 차단밸브를 닫아 압력용기 파열을 방지한다.

이 단계에서 안전상태, Trip 설정값, 허용 응답시간, 보호대상 및 시스템 경계를 함께 정해야 한다. 이 정의가 없으면 밸브 열림 고착이나 센서 Low 고착이 안전고장인지 위험고장인지 판단할 수 없다.

8.2 2단계: Maximum Tolerable Risk를 정한다

다음으로 최종 피해에 대해 허용할 수 있는 최대 위험을 정한다.

$$R_{\max} = \text{정해진 최종 피해에 대한 최대 허용위험}$$

예를 들어,

$$R_{\max} = 10^{-5}/\text{yr}$$

이라면 해당 위험 시나리오로 인한 최종 피해의 연간 위험을 10^{-5} 이하로 제한한다는 의미이다.

이 값은 센서나 밸브의 고장률이 아니다. 사람 또는 환경에 대한 최종적인 위험목표이다.

8.3 3단계: 위험사건의 최대 허용빈도를 계산한다

압력용기가 파열해도 항상 사망으로 이어지는 것은 아니다. 누출, 점화, 사람의 노출, 사망에 이르는 조건부 확률을 고려해야 한다.

$$R_{\max} = F_{H,\max} \prod_i p_i$$

따라서,

$$F_{H,\max} = \frac{R_{\max}}{\prod_i p_i}$$

이다.

예를 들어,

$$R_{\max} = 10^{-5}/\text{yr}, \quad \prod_i p_i = 10^{-2}$$

이면,

$$F_{H,\max} = \frac{10^{-5}}{10^{-2}} = 10^{-3}/\text{yr}$$

이다.

이 값은 압력용기 파열과 같은 위험사건이 허용되는 최대 빈도이다. 부품의 λ 와는 대상이 다르다.

8.4 4단계: 저수요와 고수요 · 연속 운전모드를 구분한다

안전기능이 드물게 요구되면 저수요 모드로 평가한다. 저수요 모드에서는 Demand 순간의 실패확률인 PFD 를 사용한다.

안전기능이 자주 요구되거나 항상 작동해야 하면 고수요 · 연속 모드로 평가한다. 이 경우에는 시간당 위험고장빈도인 PFH 를 사용한다.

운전모드에 따른 정량지표

저수요 기능 $\rightarrow PFD_{avg}$
고수요 · 연속 기능 $\rightarrow PFH$

저수요 기능에서 Demand 빈도를 F_D 라고 하면,

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

이고,

$$F_{\text{residual}} \leq F_{H,\text{max}}$$

이어야 한다.

따라서,

$$PFD_{\text{target}} \leq \frac{F_{H,\text{max}}}{F_D}$$

이다.

예를 들어 Demand 빈도가,

$$F_D = 0.2/\text{yr}$$

이면,

$$PFD_{\text{target}} = \frac{10^{-3}}{0.2} = 5 \times 10^{-3}$$

이다.

이 관계는 F_D 가 분석 대상 안전기능의 실제 Demand 빈도이고, 다른 독립보호계층과 사고 전파확률이 앞 단계에 일관되게 반영되었다는 전제를 가진다.

8.5 5단계: 정량목표를 SIL 구간에 대응시킨다

앞의 예에서,

$$PFD_{\text{target}} = 5 \times 10^{-3}$$

이다.

이 값은,

$$10^{-3} \leq 5 \times 10^{-3} < 10^{-2}$$

이므로 SIL 2 구간에 해당한다.

$$\text{Target SIL} = \text{SIL } 2$$

그러나 실제 설계목표는 단순히 “SIL 2”가 아니다. 원래 계산한 정확한 수치목표를 유지해야 한다.

$$PFD_{\text{assessed}} \leq 5 \times 10^{-3}$$

SIL 2의 경계값인 10^{-2} 만 만족하면 되는 것으로 바꾸면, 위험분석에서 계산한 요구조건보다 느슨해진다.

8.6 6단계: 안전기능을 구성요소로 모델링한다

안전계장기능은 일반적으로 다음 세 부분으로 구성된다.

센서 → 로직솔버 → 최종요소

단순한 1oo1 직렬구조에서 각 구성요소의 PFD가 충분히 작다면,

$$PFD_{\text{SIF}} \approx PFD_S + PFD_L + PFD_F$$

로 근사할 수 있다.

전체 목표를 센서, 로직솔버, 최종요소에 배분한다. 예를 들어,

$$PFD_{\text{SIF,target}} = 5 \times 10^{-3}$$

을 다음처럼 배분할 수 있다.

구성요소	예시 PFD 예산
센서	1.5×10^{-3}
로직솔버	0.5×10^{-3}
최종요소	3.0×10^{-3}
합계	5.0×10^{-3}

이 값은 설명을 위한 예시이다. 표준이 센서 · 로직솔버 · 최종요소의 배분비율을 일률적으로 정하는 것은 아니다. 실제 배분은 고장데이터, 시험성, 구조, 유지보수성과 비용을 반영하여 결정한다.

8.7 7단계: 각 부품의 고장모드를 식별한다

센서의 전체 고장률을 바로 PFD 계산에 넣지 않는다. 먼저 센서가 어떤 방식으로 고장나는지를 식별한다.

과압용 압력센서의 예는 다음과 같다.

고장모드	안전기능에 미치는 영향	분류 예
출력 Low 고착	실제 과압을 검출하지 못함	위험 미검출
출력 High 고착	정상상태에서 거짓 Trip 발생	안전고장
단선, 자동진단됨	경보 또는 안전정지	기능에 따라 SD 또는 DD
일정값 고착, 미검출	과압 미검출	위험 미검출
응답 지연	허용시간 내 Trip 실패	위험고장

고장모드 분류의 기준은 부품 자체가 아니라 정의된 안전기능이다. 냉각수 밸브처럼 열려 있어야 안전한 기능에서는 닫힘 고착이 위험고장이 될 수 있다.

8.8 8단계: 전체 λ 를 고장범주별로 나눈다

고장모드 분석 결과를 이용하여 전체 고장률을 다음과 같이 나눈다.

$$\lambda_{\text{total}} = \lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}$$

여기서,

$$\lambda_S = \lambda_{SD} + \lambda_{SU}$$

는 안전고장률이고,

$$\lambda_D = \lambda_{DD} + \lambda_{DU}$$

는 위험고장률이다.

센서의 위험 미검출 고장률은 여러 위험 미검출 고장모드의 합이다.

$$\lambda_{DU,S} = \lambda_{\text{Low 고착}} + \lambda_{\text{미검출 고정값}} + \lambda_{\text{위험 응답지연}} + \dots$$

따라서 SIL 검토에서 중요한 것은 부품의 전체 고장률이 아니라, 정의된 안전기능을 실패시키는 위험고장모드의 고장률이다.

8.9 9단계: λ 를 비가용도와 PFD로 변환한다

위험고장이 검출되면 고장상태에서 복구가 시작된다.

$$\text{정상} \xrightarrow{\lambda_{DD}} \text{고장} \xrightarrow{\mu} \text{정상}$$

단순한 2상태 모델에서 장기 비가용도는,

$$Q_{DD} = \frac{\lambda_{DD}}{\lambda_{DD} + \mu}$$

이다.

$$\mu = \frac{1}{MDT_{DD}}$$

이면,

$$Q_{DD} = \frac{\lambda_{DD}MDT_{DD}}{1 + \lambda_{DD}MDT_{DD}}$$

이고 작은 값에서는,

$$Q_{DD} \approx \lambda_{DD}MDT_{DD}$$

이다.

즉, 검출고장은 고장률과 고장상태 지속시간을 곱하여 비가용도로 변환한다.

반면 위험 미검출 고장은 Proof Test까지 발견되지 않는다. Proof Test 주기가 T 이면 평균 검출지연은 $T/2$ 이다.

$$MDT_{DU} \approx \frac{T}{2} + MRT + L$$

따라서,

$$Q_{DU,avg} \approx \lambda_{DU} \left(\frac{T}{2} + MRT + L \right)$$

이다.

수리시간이 Proof Test 주기에 비해 작으면,

$$PFD_{DU,avg} \approx \frac{\lambda_{DU}T}{2}$$

이다.

두 계산은 같은 원리를 사용한다.

$$Q \approx \lambda \times \text{고장상태 지속시간}$$

다만 DD는 고장이 즉시 검출되므로 MDT_{DD} 를 사용하고, DU는 Proof Test 전까지 잠복하므로 $T/2$ 를 포함한다.

8.10 10단계: 구성요소와 시스템의 실제 PFD를 계산한다

단순한 저수요 1001 구성요소에서는,

$$PFD_i \approx \frac{\lambda_{DU,i}T_i}{2} + \lambda_{DD,i}MDT_{DD,i}$$

로 근사할 수 있다.

센서에 할당된 PFD 예산이,

$$PFD_{S,target} = 1.5 \times 10^{-3}$$

이고 Proof Test 주기가,

$$T = 8760 \text{ h}$$

라고 하자.

DD 향이 충분히 작다면,

$$\lambda_{DU,S} \leq \frac{2PFD_{S,target}}{T}$$

이므로,

$$\lambda_{DU,S} \leq \frac{2 \times 1.5 \times 10^{-3}}{8760}$$

이다.

따라서,

$$\lambda_{DU,S} \leq 3.42 \times 10^{-7} / \text{h}$$

이다.

이 값은 센서의 전체 고장률 제한이 아니다. 과압 미검출을 유발하는 모든 위험 미검출 고장모드의 합에 대한 요구치이다.

실제 시스템이 1oo2 또는 2oo3 구조라면 단순 합산식을 사용할 수 없다. 다음을 함께 반영해야 한다.

- Voting 구조
- 진단범위
- Proof Test Coverage
- 시험 중 Bypass
- 수리 중 운전방식
- 채널 독립성
- 공통원인고장 CCF와 β

따라서 실제 시스템 PFD는 일반적으로,

$$PFD_{assessed} = f(\lambda_{DU}, \lambda_{DD}, T, MDT, \text{Voting}, \beta, \text{Proof Test Coverage})$$

로 계산한다.

8.11 11단계: 처음 설정한 정량목표와 비교한다

최종 판정은 계산된 SIL 명칭끼리 비교하는 것이 아니다. 처음 위험분석에서 구한 정확한 수치목표와 실제 계산값을 비교한다.

저수요 기능에서는,

$$PFD_{\text{assessed}} \leq PFD_{\text{target}}$$

고수요 · 연속 기능에서는,

$$PFH_{\text{assessed}} \leq PFH_{\text{target}}$$

이어야 한다.

또한 정량목표를 만족하더라도 아키텍처 제약, 체계적 능력, 검증 · 확인 및 생명주기 요구를 함께 만족해야 목표 SIL을 주장할 수 있다.

8.12 전체 수치 예제의 연결

앞의 과업 차단 예제를 한 번에 연결하면 다음과 같다.

허용위험에서 센서 λ_{DU} 요구치까지

$$R_{\text{max}} = 10^{-5}/\text{yr}$$

$$\prod_i p_i = 10^{-2}$$

$$F_{H,\text{max}} = \frac{10^{-5}}{10^{-2}} = 10^{-3}/\text{yr}$$

$$F_D = 0.2/\text{yr}$$

$$PFD_{\text{target}} = \frac{10^{-3}}{0.2} = 5 \times 10^{-3}$$

따라서 목표는 SIL 2 구간이지만, 정확한 설계목표는 다음과 같다.

$$PFD_{\text{assessed}} \leq 5 \times 10^{-3}$$

센서에 다음 예산을 할당한다.

$$PFD_{S,\text{target}} = 1.5 \times 10^{-3}$$

Proof Test 주기는,

$$T = 8760 \text{ h}$$

이다.

DD 향이 충분히 작다면,

$$\lambda_{DU,S} \leq \frac{2 \times 1.5 \times 10^{-3}}{8760} = 3.42 \times 10^{-7}/h$$

이다.

마지막으로 실제 센서 고장데이터와 시스템 구조를 이용해 PFD_{assessed} 를 계산하고, 원래 목표인 5×10^{-3} 이하인지 확인한다.

전체 스토리의 핵심

사람에 대한 허용위험 → 위험사건의 허용빈도
 → 안전기능의 목표 PFD/PFH
 → 목표 SIL
 → 고장모드별 $\lambda_{DD}, \lambda_{DU}$
 → 시간요소 MDT, T
 → 실제 시스템 PFD/PFH

9 최종 판정과 주의사항

저수요 기능은,

$$PFD_{\text{assessed}} \leq PFD_{\text{target}}$$

을 만족해야 한다.

고수요 · 연속 기능은,

$$PFH_{\text{assessed}} \leq PFH_{\text{target}}$$

을 만족해야 한다.

그러나 정량목표만 만족한다고 SIL이 자동으로 달성되는 것은 아니다. 아키텍처 제약과 체계적 고장 통제도 함께 충족해야 한다.

최종 핵심 문장

Maximum Tolerable Risk는 최종 피해에 대한 허용위험이다. Maximum Tolerable Failure Rate는 위험사건의 허용빈도이다. PFD와 PFH는 안전기능 전체에 대한 정량목표이다. λ 는 부품의 고장률이다.

부품의 전체 λ 는 안전 · 위험 및 검출 · 미검출 고장모드로 분류한다. 검출 위험고장은

$$Q = \frac{\lambda}{\lambda + \mu} = \frac{\lambda MDT}{1 + \lambda MDT} \approx \lambda MDT$$

로 비가용도를 계산한다. 미검출 위험고장은 Proof Test까지의 평균 검출지연 $T/2$ 를 반영한다. 이 결과를 Voting 구조와 CCF에 따라 결합하여 원래 계산한 목표 PFD 또는 PFH 의 충족 여부를

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, Chapters 1, 2, and 5.