Chapter 1: The Meaning and Context of Safety Integrity Targets

안전 무결성 목표의 정량적 · 정성적 통합 검증 및 수명주기 엔지니어링

산업계측제어 기술사 노트

August 23, 2026

1. 핵심 용어 및 정의 (Core Terminology)

- **HAZID (Hazard Identification):** 프로젝트 초기 개념 설계 단계에서 공정, 설비, 입지 환경 전체의 대형 위험 요소를 포괄적으로 식별하는 고수준(High-level) 정성적 위험 식별 기법입니다.
- **HAZOP (Hazard and Operability Study):** 상세 설계 단계에서 가이드워드(Guide Word)와 공정 변수(Parameter)의 조합을 통해 설계 의도에서 벗어나는 이탈(Deviation)을 체계적으로 도출하는 공정 위험성 분석 기법입니다.
- **Risk (위험성):** 사고 발생 빈도(Likelihood)와 사고 발생 시 피해 결과의 심각도(Consequence)의 조합으로 산출되는 정량적/정성적 척도입니다.
- **Safety Target / Tolerable Risk (허용 위험 목표):** 위험도를 0으로 만드는 절대적 안전(Absolute Safety)은 불가능하므로, 사회적 · 기술적으로 수용 가능한 수준으로 설정한 목표 위험 수치입니다.
- **ALARP (As Low As Reasonably Practicable):** 위험 감축에 투입되는 비용과 이득 간의 비대칭성을 고려하여, 합리적으로 실행 가능한 수준까지 위험을 낮추는 평가 원칙입니다.
- **SIF (Safety Instrumented Function, 안전 계장 기능):** 특정 비상 위험 이벤트를 막기 위해 독립적으로 동작하는 단일 안전 제어 루프입니다.
- **SIS (Safety Instrumented System, 안전 계장 시스템):** 하나 이상의 SIF를 실행하기 위해 센서, 로직 솔버, 최종 제어 요소(밸브 등)로 구성된 전체 통합 하드웨어/소프트웨어 시스템입니다.
- **SIL (Safety Integrity Level, 안전 무결성 등급):** SIF가 요구되는 시점에 제 기능을 정상 수행할 수 있는 신뢰도 및 위험 감축 능력을 나타내는 1~4단계 등급입니다.
- **Demand Mode (Low vs High / Continuous):** 비상 작동 요구 빈도가 연 1회 이하인 저빈도 모드(Low Demand)와 연 1회 초과 또는 연속 운전인 고빈도/연속 모드(High/Continuous Demand)로 구분됩니다.

- **$\mathbf{PFD_{avg}}$ / PFH:** 저빈도 모드에서의 평균 요구시 고장 확률(PFD_{avg}) 및 고빈도/연속 모드에서의 시간당 위험 고장 확률(PFH)입니다.
- **Proof Test Interval (T_1, 정기 점검 주기):** 자가 진단으로 검출되지 않는 숨은 위험 고장(Undetected Failure)을 도출하기 위해 수행하는 정기 수동 점검 간격입니다.
- **SRS (Safety Requirements Specification, 안전 요구사항 사양서):** 위험 평가 결과와 실제 상세 하드웨어/소프트웨어 설계를 연결하는 핵심 규격 문서입니다.
- **SFF (Safe Failure Fraction) / HFT (Hardware Fault Tolerance):** 전체 고장 중 안전한 고장 및 검출된 고장의 비율(SFF)과 하드웨어가 여분의 중복성(Redundancy)을 가지는 결함 허용도(HFT)입니다.
- **Systematic Capability (SC) / FSM (Functional Safety Management):** 개발자의 설계 오류나 절차적 결함 등 체계적 고장(Systematic Failure)을 방지하기 위한 정성적 장비 역량 등급(SC 1~4) 및 조직적 관리 체계(FSM)입니다.

2. 용어 간 상호 관계 (Relationships)

- **HAZID → HAZOP → LOPA → SIL Determination:** HAZID로 개념 단계의 대형 위험을 식별하고, HAZOP으로 상세 공정 이탈을 도출하며, LOPA(Layer of Protection Analysis) 등 정량/semi-정량 평가를 거쳐 목표 SIL 등급을 결정합니다.
- **Risk → Tolerable Risk → ALARP:** 식별된 Risk가 허용 기준(Tolerable Risk)보다 높으면 ALARP 원칙에 따라 정량적 · 경제적 평가를 거쳐 위험을 목표치 이하로 낮춥니다.
- **ALARP → SIF / SIS → SRS:** 위험 감축을 위해 필요한 안전 동작인 SIF와 이를 실행할 전체 시스템인 SIS를 정의하고, 요구사항을 SRS 문서에 기술합니다.
- **SRS → Demand Mode → SIL ($\mathbf{PFD_{avg}}$/PFH):** 운전 조건(Demand Mode)에 따라 SIL의 정량적 평가 지표인 PFD_{avg} 또는 PFH 목표 수치가 수립됩니다.
- **SIL → Quantitative (SFF/HFT/T_1) + Qualitative (SC/FSM/V&V):** SIL 등급은 수식 계산(PFD, T_1) 및 구조적 조건(SFF, HFT)이라는 정량적 검증과, 체계적 고장을 막기 위한 프로세스 준수(SC, FSM, V-Model)라는 정성적 검증을 동시 만족해야 완성됩니다.

3. Chapter 1 엔지니어링 스토리 및 세부 내용

3.1 [1단계] 위험 식별 및 목표 수립 (Hazard to Risk Target)

안전 수명주기(Safety Life-Cycle)의 초기 단계에서는 공정과 설비가 가진 잠재적 위험을 체계적으로 식별하고 정량화합니다.

3.1.1 1. HAZID와 HAZOP을 통한 위험 식별 (Hazard Identification)

- **HAZID (Hazard Identification Study):**
  - **수행 시기:** 프로젝트 초기 개념 설계(FEED) 또는 부지 선정 단계.
  - **목적:** 플랜트 전체 관점에서 화재, 폭발, 독성 물질 누출, 자연재해, 외부 요인 등 대형 위험(Major Hazards)을 신속하게 식별.
  - **특징:** 체크리스트 기반으로 진행되며, 공정 상세 도면(P&ID)이 작성되기 전에 전체적인 위험 관리 방향을 설정함.
- **HAZOP (Hazard and Operability Study):**
  - **수행 시기:** 상세 설계 단계 (P&ID 완비 시점).
  - **목적:** 공정의 설계 의도(Design Intent)에서 벗어나는 이탈(Deviation)이 유발하는 위험 및 운전성 문제를 브레인스토밍 방식으로 도출.
  - **원리: Guide Word** (No, More, Less, As Well As, Part Of, Reverse, Other Than) + **Process Parameter** (Flow, Pressure, Temperature, Level 등) → **Deviation** 도출.
  - **예시:** `MORE` + `PRESSURE` → "반응기 과압 발생" (원인: 냉각수 정지, 결과: 반응기 파열 및 가스 누출).

3.1.2 2. 위험성의 정량화 모델링 (Quantitative Risk Modeling)

HAZID와 HAZOP을 통해 도출된 위험 요인의 단순 발생 빈도만으로는 실제 피해 위험을 정확히 산정할 수 없습니다. 따라서 원인이 실제 사고로 이어지기까지의 세부 확률 요소를 정밀하게 분해하여 계산합니다.

$$\text{Risk} = f \times P_e \times P_a \times C \tag{1}$$

- f **(Initiating Event Frequency):** HAZOP 등에서 도출된 초기 위험 유발 원인(밸브 고장, 배관 누출 등)의 연간 발생 빈도 (yr^{-1}).
- P_e **(Exposure Probability):** 위험 이벤트 발생 시, 위험 구역 내 상주 인원 또는 시스템이 노출될 확률. (예: 무인 구역인 경우 $P_e \approx 0$)
- P_a **(Possibility of Avoidance):** 비상 경보/상황 발생 시, 작업자가 위험을 인지하고 비상 탈출/회피하지 못할 확률(회피 실패 확률).
- C **(Consequence):** 회피 실패 후 사고가 최종 발생했을 때의 손실/인명 피해 규모.

즉, 수식의 $\underbrace{(f \times P_e \times P_a)}_{\text{실제 사고로 이어질 최종 빈도}}$ 부분은 위험 원인 발생 빈도(f)에 현장 노출 확률(P_e)과 회피 실패

확률(P_a)을 곱하여 **실제 인명/설비에 피해가 도달할 정밀한 최종 확률**을 도출한 뒤, 이에 피해 규모(C)를 곱해주는 구조입니다.

3.1.3 3. Tolerable Risk 산정 및 ALARP 적용

절대적 Zero Risk는 존재하지 않으므로 사회적 · 기술적으로 수용할 수 있는 Tolerable Risk를 설정합니다. 남아있는 위험이 수용 한계를 넘어서는 경우, 감축 비용 대비 효율성을 따지는 ALARP 원칙에 의거하여 방호계통 수립을 결정합니다.

3.2 [2단계] 안전 기능 정의와 SRS 작성 (SIF/SIS & SRS)

위험을 차단하기 위한 단일 동작인 SIF를 정의하고, 이를 수행할 센서, 로직 솔버, 최종 제어 요소의 집합체인 SIS를 구성합니다. 위험 평가 결과와 상세 설계 단계를 연결하기 위해 Safe State, 응답 시간, Proof Test 주기 등을 명시한 SRS(안전 요구사항 사양서)를 작성합니다.

3.3 [3단계] SIL 개념의 상세 분석 및 이중 검증 (SIL Deep Dive)

SIL은 단순히 단품 장비 스펙이 아닌, 센서-로직솔버-구동부로 연결된 SIF(안전 계장 기능) 루프 전체에 부여되는 정량적 · 정성적 신뢰도 통합 척도입니다.

3.3.1 1. 정량적 검증 (Quantitative Verification)

- **Demand Mode별 지표:** 비상 작동 요구가 연 1회 이하인 Low Demand일 때는 PFD_{avg} 지표를, 연 1회 초과이거나 연속 운전인 High/Continuous Demand일 때는 PFH 지표를 기준으로 SIL 1~4 등급을 판정합니다.

Table 1: IEC 61508 Demand Mode별 SIL 정량적 요구 기준

SIL 등급	Low Demand (PFD_{avg})	High/Continuous (PFH, $/hr$)	위험 감축 계수 (RRF)
SIL 4	$10^{-5} \le \text{PFD} < 10^{-4}$	$10^{-9} \le \text{PFH} < 10^{-8}$	$10,000 \sim 100,000$
SIL 3	$10^{-4} \le \text{PFD} < 10^{-3}$	$10^{-8} \le \text{PFH} < 10^{-7}$	$1,000 \sim 10,000$
SIL 2	$10^{-3} \le \text{PFD} < 10^{-2}$	$10^{-7} \le \text{PFH} < 10^{-6}$	$100 \sim 1,000$
SIL 1	$10^{-2} \le \text{PFD} < 10^{-1}$	$10^{-6} \le \text{PFH} < 10^{-5}$	$10 \sim 100$

- **Proof Test Interval (T_1) 및 Coverage (C):** 1oo1 구조에서 $\text{PFD}_{\text{avg}} \approx \frac{\lambda_{DU} T_1}{2}$ 수식과 같이, 자가진단으로 찾지 못하는 위험 고장률(λ_{DU}) 외에도 수동 정기 점검 주기(T_1)와 복구율인 Proof Test Coverage (C)가 PFD 수치와 SIL 달성 여부를 직접 결정합니다.
- **PST (Partial Stroke Test, 부분 스트로크 시험):** 차단 밸브(ESDV) 등을 5~15%만 오프라인 상태로 동작시켜 구동부 고장을 진단하는 기법으로, 점검 주기(T_1) 사이 동안 PFD가 급증하는 것을 억제합니다.

- **하드웨어 구조적 제약 (Architectural Constraints):** 단순 PFD 계산 수치만 높아서는 안 되며, 장비의 안전 고장 비율(SFF)과 다중화 여유도를 뜻하는 하드웨어 결함 허용도(HFT) 기준을 동시에 충족해야 합니다.

$$\text{SFF} = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_{\text{total}}} = \frac{\lambda_{SD} + \lambda_{SU} + \lambda_{DD}}{\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}} \tag{2}$$

- **Common Cause Failure (β-factor, 공통 원인 고장):** 1oo2 ($\text{PFD}_{\text{avg}} \approx \frac{(\lambda_{DU} T_1)^2}{3} + \frac{\beta \cdot \lambda_{DU} T_1}{2}$), 2oo3 등 장비를 다중화 구성하더라도 동일 전원 문제, 낙뢰 등으로 한 번에 고장 나는 비율(β)이 높으면 단일 구조(1oo1) 수준으로 PFD가 악화되므로 물리적 · 전기적 분리 설계를 반영해야 합니다.

3.3.2 2. 정성적 검증 (Qualitative Verification)

- **Systematic Failure (체계적 고장) 통제:** 무작위 하드웨어 고장이 아닌 개발 단계의 설계 오류, 소프트웨어 버그, 인적 실수를 막기 위한 검증입니다.
- **FSM 및 SC (Systematic Capability):** 조직 차원의 기능안전 관리 체계(FSM) 및 장비/소프트웨어 개발 절차의 정밀도를 나타내는 Systematic Capability (SC 1∼4) 역량 등급을 갖춰야 합니다.
- **V-Model 기반 V&V:** 안전 요구사항 사양서(SRS) 작성부터 상세 설계, 단위/통합 테스트, 시운전까지 일대일 검증(Verification) 및 확인(Validation) 절차를 거칩니다.

3.3.3 3. SIL Verification(검증) vs SIL Assessment(평가)

- **SIL Verification (기술적 검증):** 설계된 SIF 루프의 PFD/PFH, SFF, HFT 계산값이 목표 SIL 등급을 정량적으로 만족하는지 수식과 고장률 데이터로 산출 · 확인하는 엔지니어링 작업입니다.
- **SIL Assessment (체계적 평가):** 정량적 계산 결과뿐만 아니라 FSM 관리 체계, SC 등급, V&V 문서화 등 정성적 프로세스 요구사항까지 포함하여 해당 시스템이 IEC 61508/61511 표준을 충족하는지 종합 심사 · 인증하는 독립적 평가 절차입니다.

3.4 [4단계] 수명주기 평가 절차 및 경제성 달성 (Assessment & Life-Cycle)

안전 관리는 IEC 61508 Safety Life-Cycle에 의거해 FSM 수립, 위험 목표 산정, SIF 식별, SIL 결정, 정량적 평가, 정성적 평가, ALARP 입증이라는 7단계 Assessment 절차로 운영 및 폐기까지 이어집니다. 규격 준수에 드는 비용(Cost of Compliance)이 발생하지만, 사고 발생 시의 막대한 법적 · 재정적 손실(Cost of Non-Compliance)을 예방하므로 경제적 타당성을 확보하게 됩니다.

3.5 [5단계] 기능안전 규격의 7대 구조 및 비용 경제성 분석 (Standards Structure & Costs)

3.5.1 1. IEC 61508의 7개 파트 구조 (The Seven Parts of IEC 61508)

기능안전 범용 표준인 IEC 61508은 전체 수명주기와 기술적 요건을 다루기 위해 다음과 같이 7개의 파트로 구성되어 있습니다.

- **Part 1 (General Requirements):** 기능안전 관리(FSM), 수명주기 전반의 일반 요구사항 및 위험 평가 정의.
- **Part 2 (E/E/PE Safety-Related Systems):** 전기 · 전자 · 프로그래밍 전자 시스템(E/E/PE) 하드웨어 설계 및 무결성 요구사항.
- **Part 3 (Software Requirements):** 안전 관련 소프트웨어 개발, 구조, 검증을 위한 요구사항.
- **Part 4 (Definitions and Abbreviations):** 표준 전반에 사용되는 전문 용어 및 약어 정의.
- **Part 5 (Methods for Determining SIL):** SIL 정량적 · 정성적 결정 방법에 대한 가이드 및 예시.
- **Part 6 (Guidelines on the Application of Parts 2 and 3):** 하드웨어 및 소프트웨어 안전 무결성 계산 예시 및 적용 지침.
- **Part 7 (Overview of Techniques and Measures):** 체계적 고장 방지 및 설계 기법에 관한 상세 기법 목록.

3.5.2 2. 경제성 분석: 비용과 편익 (Cost of Compliance vs Non-Compliance)

기능안전 체계를 구축하고 유지하는 과정은 비용 발생 수단이 아니라 장기적인 경제적 방어막 역할을 수행합니다.

- **Cost of Compliance (규격 준수 비용):** FSM 조직 운영, 독립적 SIL Verification 및 Assessment 수수료, 중복 설계(Redundancy) 적용, 주기적 Proof Testing 수행에 투입되는 직접 비용입니다.
- **Savings from Implementing (규격 이행에 따른 편익):** 체계적인 위험 관리를 통해 공정 가동 중단(Downtime)을 줄이고 설비 수명을 연장하는 간접적 이익입니다.
- **Cost of Non-Compliance (비준수 및 사고 비용):** 안전 기준을 무시하여 대형 화재, 폭발, 환경 오염 사고가 발생했을 때 부과되는 막대한 인명 피해 배상금, 법적 벌금, 시설 복구비 및 기업 이미지 추락으로 인한 영업 손실입니다.

결론적으로, 기능안전 목표 설정과 수명주기 엔지니어링은 철저한 리스크 기반의 '안전 논증(Safety Argument)'을 구축하여 규제기관 및 사회적 요구를 충족하고, 플랜트의 안전성과 경제성을 동시에 달성하는 핵심 엔지니어링 절차입니다.