IEC 61508 Part 2 기반
안전관련 하드웨어 및 시스템 설계 정리

The Safety Critical Systems Handbook, Chapter 3 학습 노트

Chapter 3은 IEC 61508 Part 2의 요구사항을 설명한다. 대상은 안전관련 시스템의 하드웨어와 전체 시스템 설계이다. 핵심은 목표 SIL을 만족하는 설계를 수행하고, 그 결과를 계산서, 시험성적서, 검토기록 및 운전기록으로 입증하는 것이다.

Contents

1 키워드 정의

1.1 적용 범위와 기본 개념

키워드	정의
IEC 61508 Part 2	안전관련 전기 · 전자 · 프로그램 가능 전자 시스템의 하드웨어 및 전체 시스템 설계 요구사항을 다룬다. 소프트웨어 개발 요구사항은 Part 3에서 다룬다.
E/E/PE 시스템	Electrical, Electronic, Programmable Electronic System의 약어이다. 전기, 전자 또는 프로그램 가능 전자기술을 이용하여 안전기능을 수행하는 시스템이다.
EUC	Equipment Under Control의 약어이다. 안전시스템이 감시하거나 보호하는 대상 설비이다.
안전기능	특정 위험과 관련하여 EUC를 안전상태로 유지하거나 안전상태로 전환하는 기능이다.
안전상태	위험이 허용 가능한 수준으로 감소된 설비 상태이다. 공정 정지, 밸브 차단, 에너지 차단 등이 해당할 수 있다.
SIL	Safety Integrity Level의 약어이다. 안전기능에 요구되는 무결성 수준이다. SIL이 높아질수록 설계, 독립성, 검증 및 문서화 수준이 강화된다.

1.2 생명주기와 요구사항

키워드	정의
안전 생명주기	요구사항 정의, 설계, 제작, 설치, 시험, 운전, 유지보수, 변경 및 폐기까지 안전을 관리하는 전체 절차이다.
기능안전관리	Functional Safety Management의 의미이다. 역할, 책임, 역량, 문서, 검토, 감사 및 형상관리를 체계적으로 운영하는 관리체계이다.
Quality and Safety Plan	프로젝트의 기능안전 목표, 조직, 책임, 문서체계, 검증계획 및 확인계획을 정의하는 최상위 계획서이다.
SRS	Safety Requirements Specification의 약어이다. 안전기능, SIL, 응답시간, 안전상태, 운전모드, 인터페이스 및 시험조건을 명확하고 시험 가능한 형태로 정의한 문서이다.
추적성	요구사항이 설계, 구현, 시험 및 결과보고서와 연결되는 성질이다. 요구사항 누락과 미검증 항목을 방지한다.

1.3 설계와 독립성

키워드	정의
구조화 설계	기능을 명확히 분할하고 계층과 인터페이스를 식별할 수 있도록 설계하는 방법이다.
모듈화	시스템을 독립적인 기능 단위로 분리하는 방법이다. 결함의 전파를 제한하고 시험과 변경을 용이하게 한다.
분리	EUC, 일반 제어시스템, 안전시스템 및 중복 채널 사이의 물리적 · 전기적 · 데이터적 독립을 확보하는 활동이다.
중복성	동일한 안전기능을 둘 이상의 채널이 수행하도록 구성하는 방식이다. 하나의 고장이 전체 기능 상실로 이어지는 것을 방지한다.
다양성	서로 다른 원리, 설계 또는 구현을 사용하는 방식이다. 동일 원인으로 중복 채널이 동시에 실패하는 것을 방지한다.
CCF	Common Cause Failure의 약어이다. 공통된 원인으로 둘 이상의 채널이 동시에 고장 나는 현상이다.
진단범위	Diagnostic Coverage의 의미이다. 위험고장 중 자동진단으로 검출되는 고장의 비율이다.
Watchdog	CPU 정지, 프로그램 순서 이상 또는 실행시간 이상을 감시하는 기본 진단기능이다.

1.4 하드웨어 안전무결성 평가

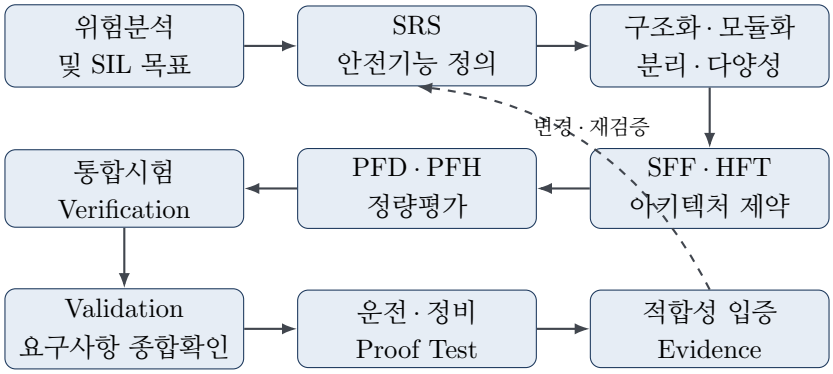
키워드	정의
랜덤 하드웨어 고장	부품 열화나 물리적 손상처럼 고장률로 정량화할 수 있는 고장이다.
체계적 고장	요구사항, 설계, 제작, 변경 또는 운전절차의 결함처럼 특정 조건에서 반복되는 고장이다. 일반적으로 고장률로 직접 예측하지 않는다.
SFF	Safe Failure Fraction의 약어이다. 전체 고장 중 안전측 고장과 자동진단으로 검출되는 위험고장의 비율이다.
HFT	Hardware Fault Tolerance의 약어이다. 시스템이 안전기능을 상실하지 않고 허용할 수 있는 하드웨어 고장 개수이다.
Type A 요소	고장모드, 고장 시 동작 및 고장데이터가 충분히 알려진 비교적 단순한 요소이다.
Type B 요소	복잡한 전자장치처럼 고장모드, 고장 시 동작 또는 고장데이터가 충분히 알려지지 않은 요소이다.
PFD	Probability of Failure on Demand의 약어이다. 저수요 안전기능이 요구될 때 실패할 평균 확률이다.
PFH	Probability of dangerous Failure per Hour의 의미이다. 고수요 또는 연속운전 안전기능의 시간당 위험고장 빈도이다.
FMEA	Failure Mode and Effects Analysis의 약어이다. 부품별 고장모드와 시스템 영향을 분석하는 기법이다.
FTA	Fault Tree Analysis의 약어이다. 상위 위험사건의 원인을 논리적으로 전개하는 기법이다.
Proof Test	자동진단으로 발견되지 않는 잠재 위험고장을 주기적으로 확인하는 시험이다.
Route 1H	SFF와 HFT에 따른 아키텍처 제약을 적용하여 최대 SIL을 판단하는 방법이다.
Route 2H	충분하고 검증된 현장 고장데이터를 이용하여 하드웨어 아키텍처 적합성을 주장하는 대안 경로이다.

1.5 시험, 확인 및 증거

키워드	정의
Verification	각 생명주기 단계의 산출물이 이전 단계의 요구사항을 올바르게 만족하는지 검토하고 시험하는 활동이다. “설계를 올바르게 구현했는가”를 확인한다.
Validation	완성된 안전관련 시스템이 실제 사용환경에서 전체 안전요구사항을 만족하는지 확인하는 활동이다. “필요한 안전시스템을 만들었는가”를 확인한다.
Safety Manual	안전관련 장치의 기능, 구성, 고장모드, 고장률, 진단범위, HFT, 사용제한 및 Proof Test 조건을 제공하는 문서이다.
영향분석	변경이 안전기능, 인터페이스, 시험범위 및 기존 검증결과에 미치는 영향을 평가하는 활동이다.
Proven in Use	유사한 환경과 용도에서 축적된 충분한 현장 운전 및 고장데이터를 이용하여 적합성을 주장하는 방법이다.
적합성 입증	IEC 61508의 각 요구사항과 이를 충족하는 사양서, 계산서, 시험성적서, 검토서 및 운전기록을 연결하는 활동이다.

2 키워드 간 관계 정리

2.1 전체 관계



관계의 핵심

- SIL은 출발점이다. SIL은 안전기능별 요구수준을 결정한다.
- SRS는 SIL을 시험 가능한 요구사항으로 변환한다.
- 설계기법은 체계적 고장을 줄인다.
- SFF와 HFT는 허용 가능한 하드웨어 구조를 제한한다.
- PFD 또는 PFH는 랜덤 하드웨어 고장에 대한 정량 목표 달성 여부를 판단한다.
- Verification과 Validation은 요구사항 충족을 시험과 기록으로 확인한다.
- 운전 · 정비와 변경관리는 달성된 안전무결성을 수명주기 동안 유지한다.

2.2 랜덤 하드웨어 고장과 체계적 고장의 관계

구분	랜덤 하드웨어 고장	체계적 고장
발생 원인	부품 열화, 물리적 손상, 우발적 고장	요구사항 오류, 설계 결함, 제작 오류, 변경 오류, 운전절차 오류
평가 방법	고장률, PFD, PFH, 신뢰도 모델, FMEA, FTA	생명주기 관리, 설계표준, 독립검토, 시험, 형상관리, 역량관리
주요 키워드	SFF, HFT, 진단범위, Proof Test, CCF	SRS, 구조화 설계, 모듈화, 분리, 다양성, Verification
판정 방식	정량적 목표와 비교	SIL에 대응하는 절차와 기법의 엄격성으로 판단

목표 SIL 달성은 하나의 계산으로 결정되지 않는다. 랜덤 하드웨어 고장에 대한 정량평가와 체계적 고장에 대한 정성적 방어가 동시에 필요하다.

2.3 SFF, HFT, PFD/PFH의 관계

1. **SFF**는 전체 고장 중 안전측 고장과 자동진단으로 검출되는 위험고장의 비율을 나타낸다.
2. **HFT**는 하드웨어 고장을 몇 개까지 허용할 수 있는지를 나타낸다.
3. **SFF와 HFT**는 해당 구조에서 주장할 수 있는 최대 SIL을 제한한다.
4. **PFD 또는 PFH**는 선택한 구조의 실제 위험고장 확률 또는 빈도를 계산한다.
5. 따라서 아키텍처 제약을 만족하더라도 PFD/PFH 목표를 만족하지 못하면 설계는 부적합하다.
6. 반대로 PFD/PFH 계산값이 충분히 낮더라도 SFF/HFT 제약을 충족하지 못하면 해당 SIL을 주장할 수 없다.

$$\text{SIL 적합성} = \text{아키텍처 적합성(SFF/HFT)} + \text{정량 적합성(PFD/PFH)} + \text{체계적 고장 방어}$$

2.4 중복성, 다양성, 분리 및 CCF의 관계

관계	설명
중복성 → HFT 증가	하나의 채널이 고장 나도 다른 채널이 안전기능을 유지한다.
중복성 ⇏ CCF 제거	동일 전원, 동일 환경, 동일 설계 오류가 있으면 모든 채널이 동시에 실패할 수 있다.
다양성 → CCF 감소	서로 다른 원리, 부품 또는 논리를 적용하여 동일 원인에 의한 동시고장을 줄인다.
분리 → 독립성 증가	물리적 · 전기적 · 데이터적 간섭과 고장전파를 제한한다.
진단 → SFF 증가	위험고장을 자동으로 검출하여 안전상태로 전환할 수 있다.
Proof Test → 잠재고장 감소	자동진단이 검출하지 못한 위험고장을 주기적으로 발견한다.

2.5 Verification과 Validation의 관계

구분	Verification	Validation
핵심 질문	설계를 요구사항대로 올바르게 구현했는가?	완성된 시스템이 실제 안전요구를 충족하는가?
대상	단계별 사양서, 설계서, 모듈, 인터페이스, 통합 결과	전체 안전관련 시스템과 실제 운전조건
주요 방법	검토, 입력분할, 경계값시험, 비정상 입력시험, 논리조합시험	기능시험, 환경시험, 간섭시험, 고장삽입, 종합 인수시험
결과	단계별 검증기록과 결함조치 기록	전체 요구사항 추적표와 종합 확인보고서

3 흐름에 맞춘 설명

3.1 1단계: 기능안전관리체계를 수립한다

프로젝트를 시작할 때 역할, 책임, 역량 및 독립성을 정한다. Quality and Safety Plan을 작성한다. 이 계획에는 문서체계, 검토방법, 시험전략, 형상관리, Validation 계획 및 기능안전감사 계획이 포함되어야 한다. 모든 활동은 기록되어야 한다. 기록이 없으면 표준 준수 여부를 평가할 수 없다.

3.2 2단계: 안전요구사항을 SRS로 정의한다

위험분석 결과를 바탕으로 안전기능별 SIL을 정한다. 각 안전기능의 저수요 또는 고수요 모드를 구분한다. 응답시간, 안전상태, Trip 설정값, Reset 조건, 전원상실 시 동작, 운전모드, 인터페이스 및 Proof Test 요구사항을 정의한다. 요구사항은 명확하고 모호하지 않으며 시험 가능해야 한다.

3.3 3단계: EUC와 안전시스템의 경계를 정한다

일반 제어기능과 안전기능의 경계를 정의한다. 두 시스템 사이의 전기 및 데이터 인터페이스를 명확히 한다. 필요한 경우 물리적으로 분리한다. 독립성을 입증할 수 없다면 일반 제어시스템을 포함한 전체 시스템을 안전관련 시스템으로 취급해야 한다.

3.4 4단계: 구조화 · 모듈화된 설계를 수행한다

검증된 부품과 설계방식을 사용한다. 기능을 모듈로 분리한다. 안전관련 요소와 비안전관련 요소의 인터페이스를 제한한다. 고장을 검출하면 안전상태로 전환하도록 설계한다. 온도, 진동, EMC 및 전원 이상을 고려한다. 온라인 변경을 제한하고 운전자 오조작을 방지한다.

3.5 5단계: 진단과 고장허용 구조를 결정한다

목표 SIL에 따라 Watchdog, 메모리 검사, I/O 진단, 센서 및 액추에이터 진단을 설계한다. 중복구조를 적용할 경우 HFT가 증가한다. 그러나 동일 원인에 의한 동시고장을 방지하기 위해 채널 분리, 전원 분리, 배선 분리 및 다양성 설계를 함께 적용해야 한다.

3.6 6단계: SFF와 HFT로 아키텍처를 검토한다

각 요소를 Type A 또는 Type B로 분류한다. FMEA 또는 고장시험을 통해 안전측 고장, 검출된 위험고장 및 미검출 위험고장을 구분한다. 이를 이용하여 SFF를 산정한다. SFF와 HFT 표를 이용하여 해당 구조가 목표 SIL을 주장할 수 있는지 확인한다. 이것이 Route 1H의 기본 흐름이다.

충분하고 검증된 현장 고장데이터가 있다면 Route 2H를 검토할 수 있다. 이때 제조사 보증반품 자료가 아니라 실제 운전환경에서 수집한 현장데이터가 필요하다. 데이터의 적용환경, 고장분류 및 통계적 신뢰수준을 입증해야 한다.

3.7 7단계: PFD 또는 PFH를 계산한다

신뢰도 모델을 작성한다. 센서, 로직솔버 및 최종요소의 위험고장률을 반영한다. 진단주기, Proof Test 주기, 수리시간, 진단범위 및 CCF를 포함한다. 저수요 기능은 PFD를 계산하고 고수요 또는 연속운전 기능은 PFH를 계산한다. 계산결과는 SIL 범위뿐 아니라 프로젝트에서 설정한 개별 정량목표와 비교해야 한다.

3.8 8단계: 통합시험과 Verification을 수행한다

입력 조합에 따른 출력응답을 시험한다. 입력 영역을 분할하고 경계값을 시험한다. 비정상 입력과 명세되지 않은 입력에 대한 동작도 확인한다. 높은 SIL에서는 운전 경계에서 여러 중요 논리가 동시에 작동하는 조건을 시험한다. 시험버전, 시험도구, 합격기준, 결과 및 불일치 사항을 기록한다.

3.9 9단계: Validation으로 전체 요구사항을 확인한다

SRS의 각 요구사항을 계산서, 검토서 및 시험성적서와 연결한다. 기능시험, 환경시험, 간섭시험 및 고장삽입시험을 수행한다. 발견된 문제는 현상, 원인, 조치 및 재시험 결과까지 닫아야 한다. Validation은 개별 시험의 집합이 아니라 전체 안전요구사항 충족에 대한 종합 확인이다.

3.10 10단계: 운전과 유지보수로 안전무결성을 유지한다

운전절차와 정비절차를 명확히 한다. Proof Test를 정해진 주기로 수행한다. 실제 Demand 횟수, 고장, 오동작, 수리 및 교체이력을 기록한다. 기록을 주기적으로 검토하여 최초 SIL 가정과 고장률 가정이 적절했는지 확인한다. 접근권한과 운전자 교육도 관리한다.

3.11 11단계: 변경을 통제하고 재검증한다

모든 변경은 형상관리 대상이다. 변경사유와 영향분석을 기록한다. 변경된 모듈뿐 아니라 영향을 받는 인터페이스와 관련 모듈도 재검증한다. 변경으로 SRS, 신뢰도 계산, 시험범위 또는 Safety Manual이 달라지면 관련 문서를 모두 갱신한다.

3.12 12단계: 적합성 입증자료를 완성한다

IEC 61508 요구사항별로 증거문서를 연결한다. 증거에는 SRS, 설계서, FMEA, CCF 분석서, PFD/PFH 계산서, 시험계획서, 시험성적서, Validation 보고서, Safety Manual, 변경이력 및 운전기록이 포함된다. 최종 목적은 "표준을 적용했다"고 선언하는 것이 아니라, 각 요구사항이 충족되었음을 추적 가능한 자료로 입증하는 것이다.

최종 흐름 요약

위험분석과 SIL 설정에서 시작한다. SRS로 안전기능을 명확히 한다. 구조화, 모듈화, 분리, 중복 및 다양성으로 체계적 고장을 방어한다. SFF와 HFT로 하드웨어 구조를 검토한다. PFD 또는 PFH로 랜덤 하드웨어 고장 목표를 확인한다. Verification과 Validation으로 요구사항 충족을 입증한다. 운전, 유지보수 및 변경관리로 달성된 안전무결성을 유지한다.

참고문헌

References

[1] 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 3, pp. 57–78.