

디지털 I&C 시스템의 신뢰성·안전성 확보 기술

산업계측제어기술사 핵심 서브노트

1. 핵심 개념

디지털 I&C(Instrumentation and Control)는 센서 입력을 PLC, DCS, 안전 PLC 또는 컴퓨터 기반 보호계가 처리하여 감시·제어·보호 기능을 수행하는 시스템이다.

$$\text{Digital I\&C Risk} = \text{Random HW Failure} + \text{Systematic SW Failure} + \text{CCF} + \text{Cyber Threat}$$

따라서 신뢰성과 안전성은 다음 네 축을 통합하여 확보한다.

V모델 기반 V&V → 형상관리 → 다양성·독립성 → 심층방어형 OT 보안

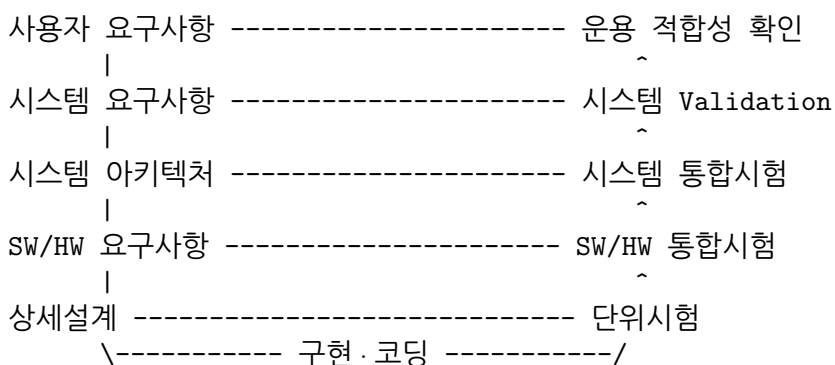
2. 주요 국제표준

분야	주요 표준	핵심 내용
일반 기능안전	IEC 61508	E/E/PE 안전관련 시스템의 기능안전 생명주기
프로세스 플랜트	IEC 61511	SIS/SIF의 명세, 설계, 운전, 유지보수
원자력 I&C	IEC 61513	안전 중요 I&C의 전체 아키텍처와 생명주기
원자력 SW	IEC 60880	Category A 기능 수행 소프트웨어 개발 및 V&V
원자력 CCF	IEC 62340	Category A I&C의 공통원인고장 대응
철도 SW	IEC 62279	철도 제어·보호 소프트웨어 개발
철도 RAMS	IEC 62278	신뢰성·가용성·유지보수성·안전성 생명주기
산업제어 보안	IEC 62443	IACS 보안관리, 위험평가, 시스템·제품 보안

3. V모델 기반 개발과 V&V

3.1. V모델

V모델은 개발단계와 시험단계를 대응시켜 요구사항부터 구현 및 운용 적합성까지 추적하는 생명주기 모델이다.



- **Verification:** 제품을 명세에 맞게 올바르게 만들었는가?
- **Validation:** 사용 목적에 적합한 올바른 제품을 만들었는가?

3.2. RTM

요구사항 추적성 매트릭스(Requirements Traceability Matrix, RTM)는 위험원, 안전요구사항, 설계, 구현, 시험결과를 양방향으로 연결한다.

- **Forward Traceability**: 모든 요구사항이 설계 · 코드 · 시험으로 구현되었는지 확인
- **Backward Traceability**: 모든 설계와 코드가 승인된 요구사항에서 유래했는지 확인

답안 핵심문장: RTM은 요구사항 누락, 과잉 구현, 변경 영향 및 시험 누락을 통제하는 V&V의 핵심 관리 수단이다.

3.3. MC/DC

MC/DC(Modified Condition/Decision Coverage)는 복합 결정문을 구성하는 각 조건이 다른 조건의 영향을 고정한 상태에서 결정 결과에 독립적으로 영향을 주는지를 확인하는 구조적 커버리지 기준이다.

$$Y = (A \wedge B) \vee C$$

A, B, C 각각이 단독으로 Y의 참 · 거짓을 변경하는 시험쌍을 확보해야 한다.

- 단순 문장 · 분기 커버리지보다 논리 검증력이 높다.
- AND/OR 오류, 반전조건 오류, Masking된 조건을 찾는 데 유리하다.
- 요구사항 오류, 타이밍 오류, 인터페이스 오류까지 보장하지는 않는다.

주의: MC/DC의 의무 수준은 산업별 표준과 안전등급에 따라 구분해야 하며, 항공 Level A의 요구를 원자력 Category A나 철도 SIL 4에 그대로 등치해서는 안 된다.

4. 형상관리와 기준선

형상관리(Configuration Management)는 형상항목을 식별하고 변경을 통제하며, 상태를 기록하고 실제 제품과 기준선의 일치 여부를 감사하는 활동이다.

기준선	핵심 개념
Functional Baseline	시스템이 수행해야 할 기능, 성능 및 인터페이스 정의
Allocated Baseline	상위 기능을 HW, SW, 센서, 네트워크 등 하위 구성품에 할당
Product Baseline	실제 제작 · 배포될 코드, 도면, 설정, 시험절차 및 매뉴얼 확정

4.1. CCB 승인 절차

변경요청 → 영향분석 → CCB 심의 → 구현 → 회귀시험 → 형상감사 → 기준선 갱신

CCB(Configuration Control Board)는 기능, 안전, 보안, 비용, 일정, 시험범위 및 복구 가능성을 종합 평가한다.

답안 핵심문장: CCB는 변경 자체보다 변경으로 인한 안전성 · 보안성 · 검증범위 · 복구가능성을 통제하여 기준선의 무결성을 보호한다.

5. CCF와 다양성 설계

공통원인고장(Common Cause Failure, CCF)은 하나의 원인으로 둘 이상의 채널이나 계통이 동시에 기능을 상실하는 고장이다.

2oo3 구조의 독립 채널 실패확률을 q 라 하면,

$$Q_{2oo3} = 3q^2(1 - q) + q^3 = 3q^2 - 2q^3$$

그러나 동일 소프트웨어, 공통 전원, 공통 네트워크 또는 공통 환경을 공유하면 독립성 가정이 깨진다.

Redundancy → 우발고장 내성 향상

Diversity + Independence → CCF 위험 감소

다양성 유형	적용 예
기능적 다양성	서로 다른 물리량으로 동일 안전목표 달성
신호 다양성	서로 다른 센서와 측정원리 사용
설계 다양성	서로 다른 알고리즘과 아키텍처 적용
SW 다양성	다른 언어, OS, 개발도구 및 개발팀 적용
HW 다양성	다른 CPU, I/O, 제조사 및 기술 적용
관리적 다양성	독립 개발·검증·형상관리 조직 운영

다양성은 단순히 제조사를 다르게 선택하는 것이 아니라 공통 실패경로를 분석하고 의도적으로 차단하는 설계활동이다.

6. IEC 62443 기반 OT 보안

심층방어(Defense in Depth)는 하나의 보안통제가 실패하더라도 다음 방어계층이 공격의 확산을 제한하도록 조직, 물리, 네트워크, 호스트 및 복구수단을 다층화하는 개념이다.

```

Enterprise IT
|
Industrial DMZ
|
OT Operations Zone
|
Basic Control Zone
|
Field Zone
    
```

Safety Zone ---- 제한된 Conduit ---- Monitoring/DMZ

6.1. Zone과 Conduit

- **Zone**: 위험도, 중요도 및 보안 요구사항이 유사한 자산의 집합
- **Conduit**: Zone 사이에서 허용된 통신경로

IEC 62443-3-2는 시스템을 Zone과 Conduit로 분할하고 위험평가를 통해 목표 보안수준(SL-T)을 결정하도록 한다. IEC 62443-3-3은 시스템 보안요구사항을 정의한다.

- IT/OT 네트워크 분리 및 DMZ 구성
- SIS와 BPCS의 독립성 확보
- 허용 프로토콜·포트 최소화
- 원격접속 승인, 시간제한 및 기록
- Engineering Workstation과 이동식 매체 통제
- 백업, 복구 및 사고대응 절차 확보

7. 기술사적 Trade-off

기술	기대효과	한계
V모델 · RTM	누락 방지, 검증근거 확보	문서량과 관리비용 증가
MC/DC	복합논리 검증 강화	요구사항 · 타이밍 오류는 별도 검증 필요
형상관리 · CCB	무단변경 방지, 재현성 확보	긴급변경 속도 저하
2oo3	단일 우발고장 허용	CCF에는 취약
다양성	공통 실패경로 감소	비용 · 복잡도 · 유지보수 부담 증가
Zone · Conduit	침해확산 제한	운전 · 진단 편의성 감소

8. 권장 도서

1. **The Safety Critical Systems Handbook, 5th Ed.**
David J. Smith, Kenneth G. L. Simpson
IEC 61508 · 61511, SIL, 기능안전 생명주기 및 신뢰도 계산의 핵심 교재
2. **Plant Hazard Analysis and Safety Instrumentation Systems, 2nd Ed.**
Swapan Basu
SIS · SIF · SIL, 위험분석 및 안전계장 설계의 현장 적용에 적합
3. **Industrial Network Security, 3rd Ed.**
Eric D. Knapp et al.
SCADA · DCS · PLC 보안, 네트워크 분리 및 침증방어 학습에 적합
4. **Software Engineering, 10th Ed.**
Ian Sommerville
V모델, 요구사항공학, 시험 및 형상관리의 기초 보완
5. **Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems**
원자력 디지털 I&C, 소프트웨어 신뢰성 및 사이버보안 사례 참고

9. 권장 학습 순서



시간이 부족하면 1번 도서로 기능안전 체계를 정립한 후, 2번 도서로 SIS 현장 적용을 학습한다. 이후 IEC 62443과 소프트웨어공학 도서를 보완한다.

10. 최종 정리

결함을 줄이는 V&V + 변경을 통제하는 형상관리 + 공통고장을 차단하는 다양성 + 공격을 제한하는
심층방어

디지털 I&C의 신뢰성과 안전성은 개별 기술의 단순 적용이 아니라, 요구사항 정의부터 설계, 구현, 시험, 변경 및 운전까지 전 생명주기에서 통합적으로 확보해야 한다.