안전인증 제도 설명회

승강기 기능안전 심사방법

한국승강기안전공단 안전인증실 방승환 과장

목차

1. 기능안전인증 개요

■ 기능안전인증 정의

1. 제어 시스템과 관련된 모든 **시스템을 안전한 상태로 유지하거나 안전성을 달성**하기 위하여 필요한 활동을 수행하는 **E/E/PE[1] 안전시스템, 기타 안전시스템, 외부 리스크 감소 설비의** 상호 작용을 말한다.

2. 기능안전이 승강기 분야에 접목된 것을 **PESSRAL[2]/PESSRAE[3]**라 한다.

1) E/E/PE(Electronical/Electronic/Programmable Electronic)_전기/전자/프로그램 가능한 전자부품

2) PESSRAL(Programmable Electronic System Safety Related Application for Lifts)_엘리베이터 안전관련 프로그램 적용 가능한 전자시스템

3) PESSRAE(Programmable Electronic System Safety Related Application for Escalators and moving walks)_에스컬레이터의 안전관련 프로그램 적용 가능한 전자시스템

1. 기능안전인증 개요

■ 기능안전인증의 시행

승강기안전부품 안전기준 및 승강기 안전기준 부칙 제2조

❍ 제2조(제어반에 관한 적용례)

- 별표 2의 4.4・5.3, 별표16의 4.4・5.4, 별표 22의 15.2.6, 별표 23의 15.1.3.3 및 별표 24의 5.12.2.6.3의 개정규정은 **2020년 3월 28일**부터 출고 또는 통관되는 엘리베이터 제어반 및 에스컬레이터 제어반에 적용

❍ 적용대상

- 2020년 03월 28일 이후 신규/정기/변경/ 인증 신청하는 제어반

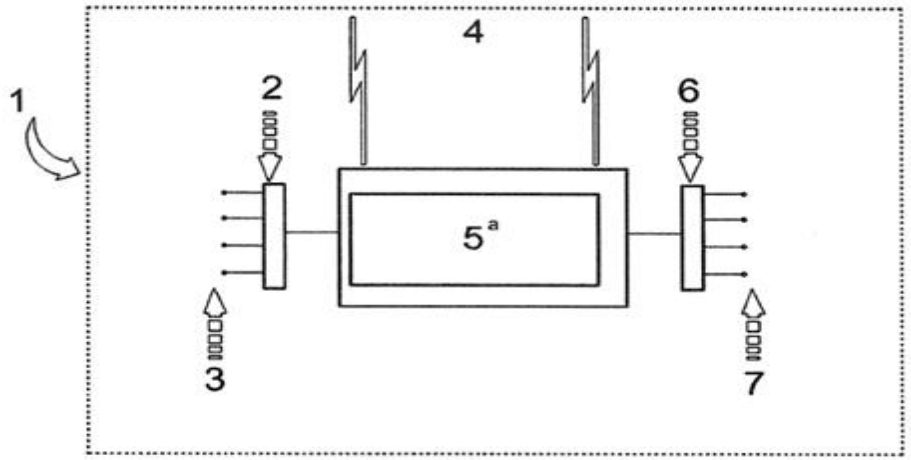
※ 변경인증 시 변경대상이 기능안전과 무관한 경우 미적용

1. 기능안전인증 개요

■ 용어 정의

❍ **프로그램 가능한 전자 시스템(PES: Prgrammable Electronic System)**

- 하나 이상의 프로그램 가능한 전자 장치를 기반으로 하는 제어, 보호 또는 감시 시스템으로 전원공급장치, 센서, 및 기타 입력장치, 데이터 전송장치와 기타 통신 경로 등의 시스템 요소를 포함한다.



1. PES의 범위
2. 입력 인터페이스
3. 입력장치(센서)
4. 통신 장치
5. 프로그램 가능한 장치(PE)
6. 출력 인터페이스
7. 출력 장치

[그림1- 프로그램 가능한 전자 시스템(PES)의 기본 구조]

1. 기능안전인증 개요

■ 용어 정의

❍ **안전장치(Safety Device)**

- E/E/PE 안전시스템, 기타 안전시스템, 외부 리스크 감소 설비에 의해 수행되는 기능으로 **시스템을 안전한 상태를 유지하거나 달성하기 위한 장치**

  시스템의 목표 안전기능을 달성하기 위해 할당되고, PES 요소와 non-PES 요소로 구성될 수 있으며 기능안전 검증을 위해 **PES 요소와 non-PES 요소의 분리**를 권고

1. PES 요소
2. non-PES 요소

[그림2- 안전장치]

1. 기능안전인증 개요

■ 용어 정의

❍ **공통원인고장(CCF: Commom Cause Failure)**

- 안전 관련 시스템에 **전원공급 중단과 같이 한가지의 고장원인이 설비 전체의 고장**으로 이어지는 원인고장이나, 하부시스템의 채널 모두에 공통영향을 미치는 원인고장을 말한다.

❍ **단일점 고장(Single point fault)**

- 안전 관련 시스템으로 보호되지 않으며, **단일 고장에 의해 실제 시스템에 고장이 발생하는** 경우를 단일점 고장이라 한다.
  단일점 고장의 경우 안전기능에 의해 진단이 되지 않아 하드웨어 파트에서 안전무결성 수준을 결정하는 중요한 인자 중 하나이며, **기능안전의 목표는 단일점 고장을 최소한**으로 하는 것이다.

2. 기능안전인증 적용범위

■ 기능안전인증 대상

❍ 엘리베이터

- 프로그램이 적용된 안전회로(제어반 내 PCB, 별도 모듈화 제품)
-「승강기안전부품 안전기준」[별표2] 엘리베이터 휠체어리프트 제어반 안전기준
-「승강기안전부품 안전기준」[별표22] 엘리베이터 안전기준
-「승강기안전부품 안전기준」[별표23] 경사형 엘리베이터 안전기준

❍ 에스컬레이터

- 프로그램이 적용된 안전회로(제어반 내 PCB, 별도 모듈화 제품)
-「승강기안전부품 안전기준」[별표16] 에스컬레이터 제어반 안전기준
-「승강기안전부품 안전기준」[별표24] 에스컬레이터 안전기준

2. 기능안전인증 적용범위

■ 적용범위 및 대상

기능안전인증 적용 범위 및 대상

❍ **기능안전인증의 범위**

- Input : 입력(Sensor 등)에 대한 검증 및 정의
- Control Board : Program 적용 제어부 - 부품
- Final element : 출력(Relay, contact 등)에 대한 검증 및 정의

[그림3- 기능안전인증 범위]

2. 기능안전인증 적용범위

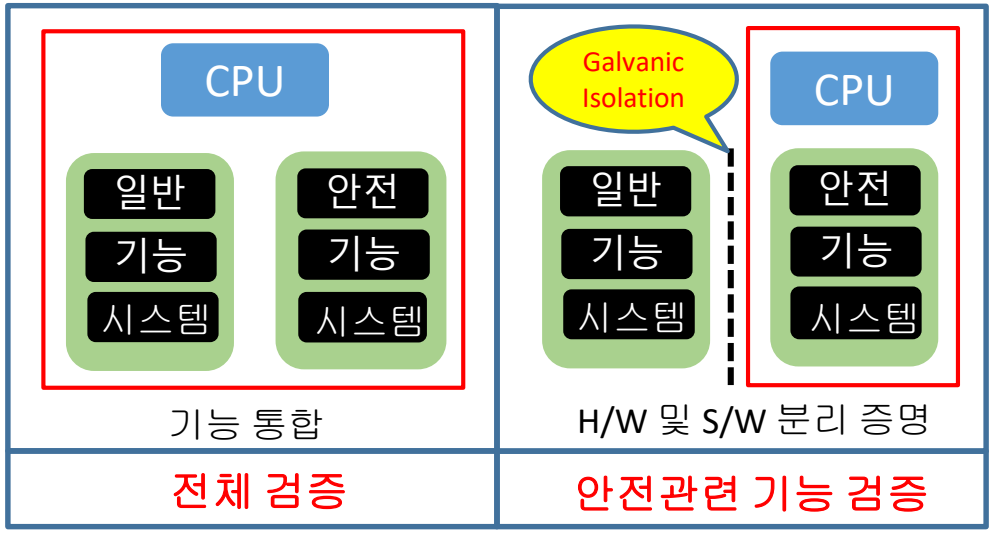
■ 적용범위 및 대상

기능안전인증 적용 범위 및 대상

○ 기능안전인증 적용 대상

- 별도의 기판에 안전을 위한 Program이 적용된 경우
- 하나의 기판에 안전 및 일반 기능을 위한 Program이 적용된 경우
- 별도의 기판/모듈에 안전 및 일반 기능을 위한 Program이 적용 된 경우

※ 기능안전인증 적용 대상이 아닌 경우 입력, 출력, 제어에 대해 승강기안전인증에서 검증



[그림4- 기능안전인증 검증 범위]

3. 기능안전인증 절차

기능안전 시스템 분석

❍ 시스템 요구사항의 완전성

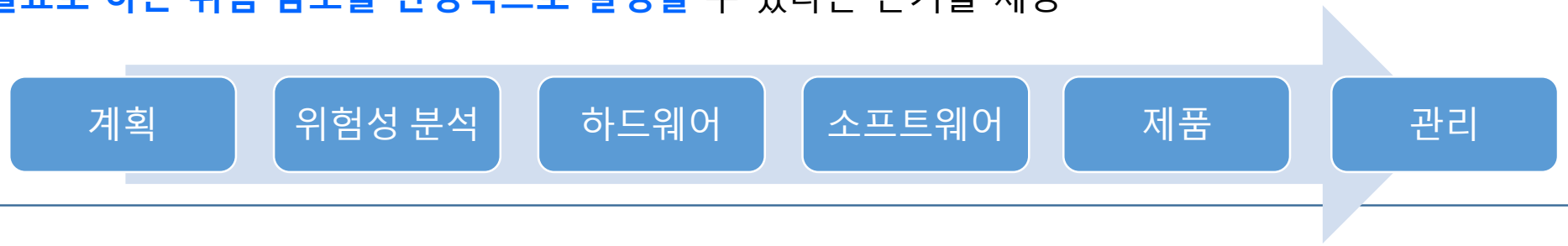
- 안전기능의 기능안전성 달성을 위해 **위험원 분석 및 리스크 평가**를 통한 안전관련 시스템의 요구사항에 대해 명확히 제시

❍ 시스템 요구사항, 적용방법, 규칙 및 명세의 이행

- 전기/전자/프로그램 가능한 전자장치로 안전관련 시스템을 적용함으로 **지정된 수준의 위험 저감을 달성**을 위한 요구사항, 적용 방법, 적용 규칙에 대한 이행 결과.

❍ 허용 가능한 수준으로 위험도 감소 또는 제거

- 하드웨어 우발 결함과 시스템적 결함 모두를 제어하거나 방지하기 위한 수단 및 방법을 적용하여 **필요로 하는 위험 감소를 안정적으로 달성할** 수 있다는 근거를 제공



3. 기능안전인증 절차

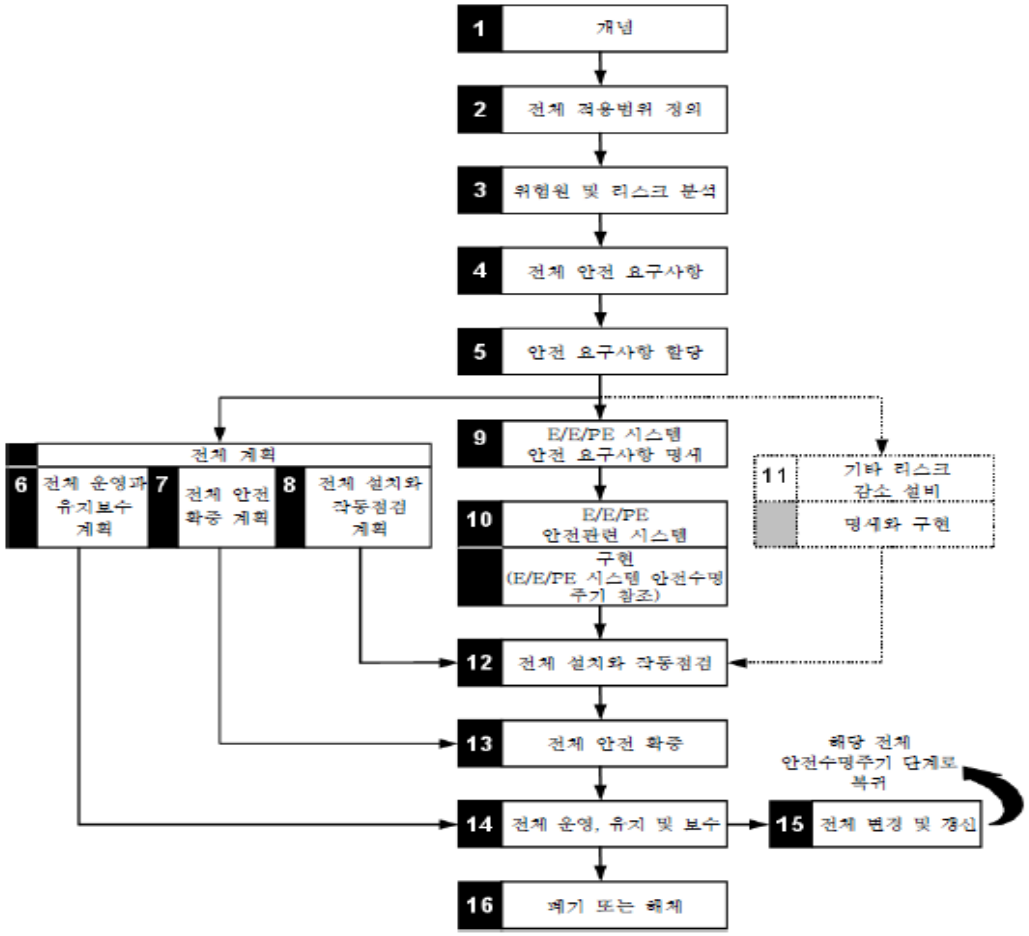
기능안전 단계별 요구 문서

❍ 단계별 요구 문서

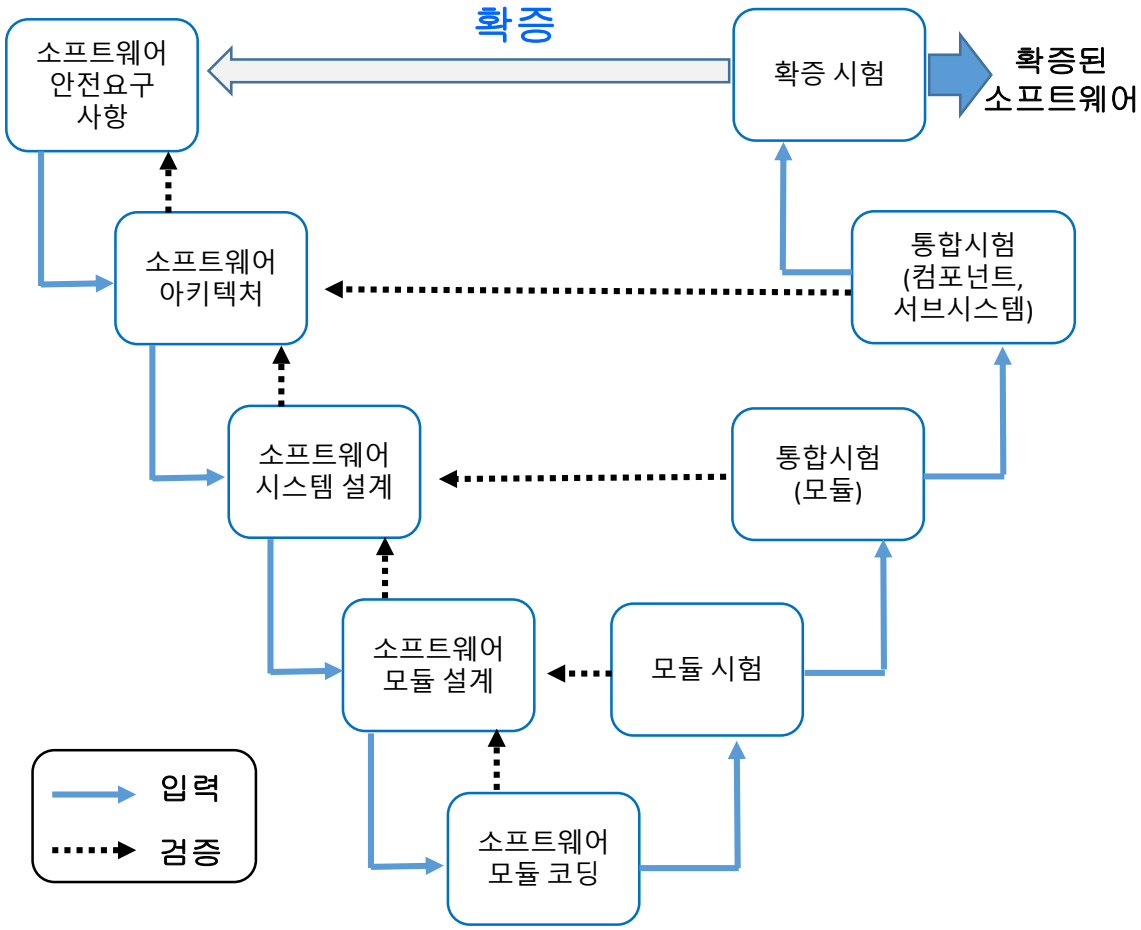
계획	계획,개발 관련 문서(설계, 개발, 검증)등
위험성 분석	안전무결성 달성을 위한 위험성 분석 및 안전요구사양서 명세
하드웨어	안전무결성 등급에 따른 시스템 및 하드웨어 관련 문서(구조, 설계 등)
소프트웨어	안전수명주기에 따른 개발, 시험, 검증 결과 등(사례, 결과)
제품	통합된 시스템에의 시험 방법 및 시험 결과 관련 문서 등(사례, 결과)
관리	사용자 설명서, 안전매뉴얼, 형상관리 프로세스 및 증빙 관련 서류

3. 기능안전인증 절차

안전수명주기에 따른 기능안전 단계별 요구 사항



[그림5- 안전수명주기에 따른 시스템 요구사항]



[그림6-안전수명주기에 따른 소프트웨어 요구사항]

3. 기능안전인증 절차

시스템 설계, 개발 계획, 검증에 관련 문서

❍ **안전수명 주기에 따른 시스템 개발 계획, 활동, 조정, 실행, 검증 등 개발단계의 안전요구사항을 정의**

- 전체 시스템 개발 계획
- 기능안전성 평가 계획 및 실행
- 시스템 개발 수행에 대한 적절한 방법을 정의

❍ **시스템 개발 조직에 대한 역할과 책임 정의**

- 시스템 개발에 참여한 인원의 역량 확인(경력,교육 이력 등의 문서화)
- 필요한 경우 참여 인원의 역량 향상을 위한 교육,훈련 계획 포함

❍ **형상관리**

- 변경관리는 모든 작업 결과물의 일관성을 유지하면서 변경에 대한 체계적인 계획, 관리, 감독, 수행, 문서화.
- 변경 실시 전 기능안전에 미치는 잠재적 영향이 평가되어야 하고, 변경에 대한 의사 결정 절차가 수립

3. 기능안전인증 절차

안전무결성 달성을 위한 위험성 분석 및 안전요구사양서 명세

❍ 시스템 안전요구사항 사양서

- 요구사항은 위험원 분석 및 리스크 평가를 기반으로 작성
- 시스템 안전요구사항에서 요구되는 안전기능을 명확히 제시
- 서브 시스템에 대한 요구사항(하드웨어, 소프트웨어)

❍ 안전기능의 동작 사양

- 안전기능의 입/출력 인터페이스 조건 명시
- 안전기능 동작을 유발하는 조건 및 안전기능 정의
- 안전기능의 감지 및 동작에 대한 시간 명시
- 위험원 분석 및 리스크 평가를 통한 안전무결성 등급에 따른 안전기능 구조 명시

3. 기능안전인증 절차

안전무결성 등급에 따른 시스템 및 하드웨어 관련 문서(구조, 설계 등)

❍ 하드웨어 설계 자료

- 시스템 요구사항이 하드웨어 설계에 구현되어야 한다.
- 안전기능 및 진단기능과 관련된 하드웨어 구성요소를 명확히 하여야 한다.
- 하드웨어 구성요소의 입/출력 인터페이스를 명확히 하여야 한다.
- 안전기능과 비안전기능의 독립성 제시
- 안전무결성 등급에 따른 하드웨어의 구조적 제약 확인 [부속서 13참조]

❍ 하드웨어 블록 다이어그램

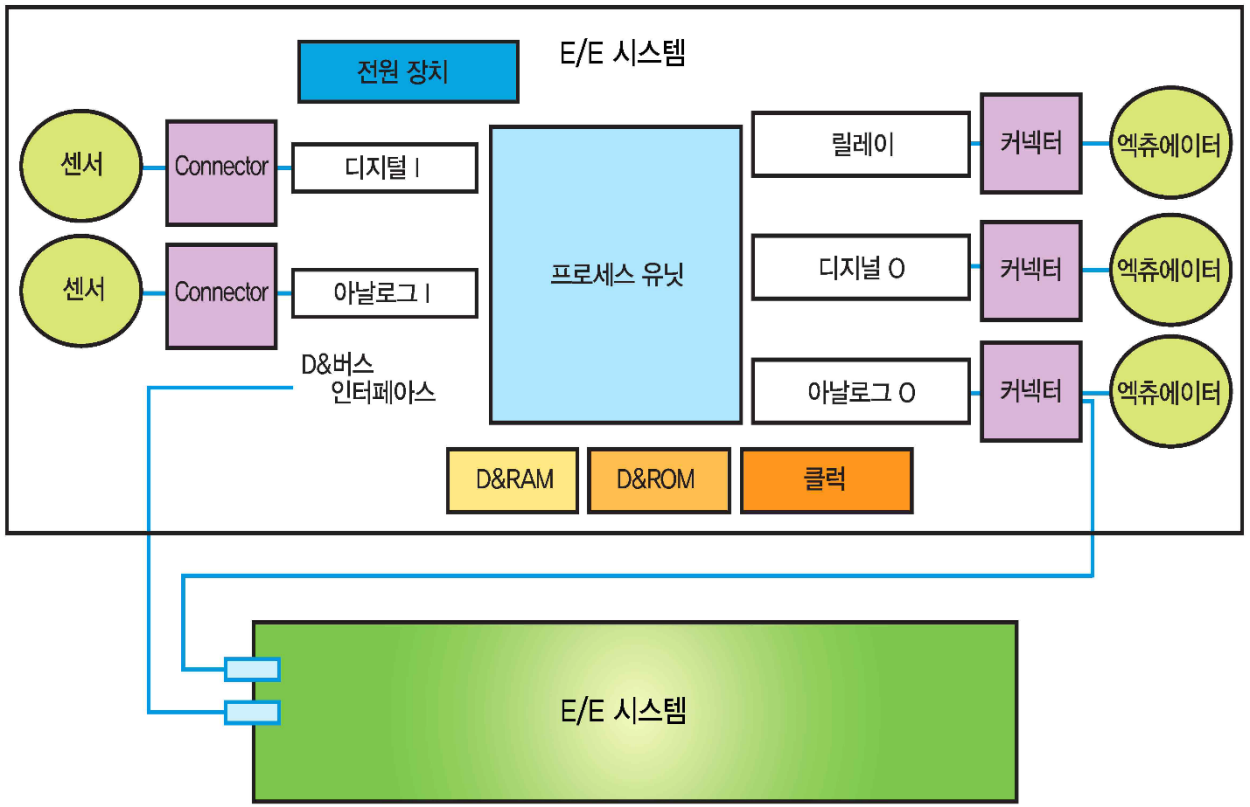
- 구성 요소간의 구조 및 안전장치의 식별

❍ 하드웨어 상세 설계

- 하드웨어의 작동 환경 및 부품선정의 적절성 확인

3. 기능안전인증 절차

안전무결성 등급에 따른 시스템 및 하드웨어 관련 문서(구조, 설계 등)



[그림7- 하드웨어 블록 다이어그램]

3. 기능안전인증 절차

안전수명주기에 따른 소프트웨어 개발, 시험, 검증 결과 등(사례, 결과)

❍ 소프트웨어 안전요구 사양서

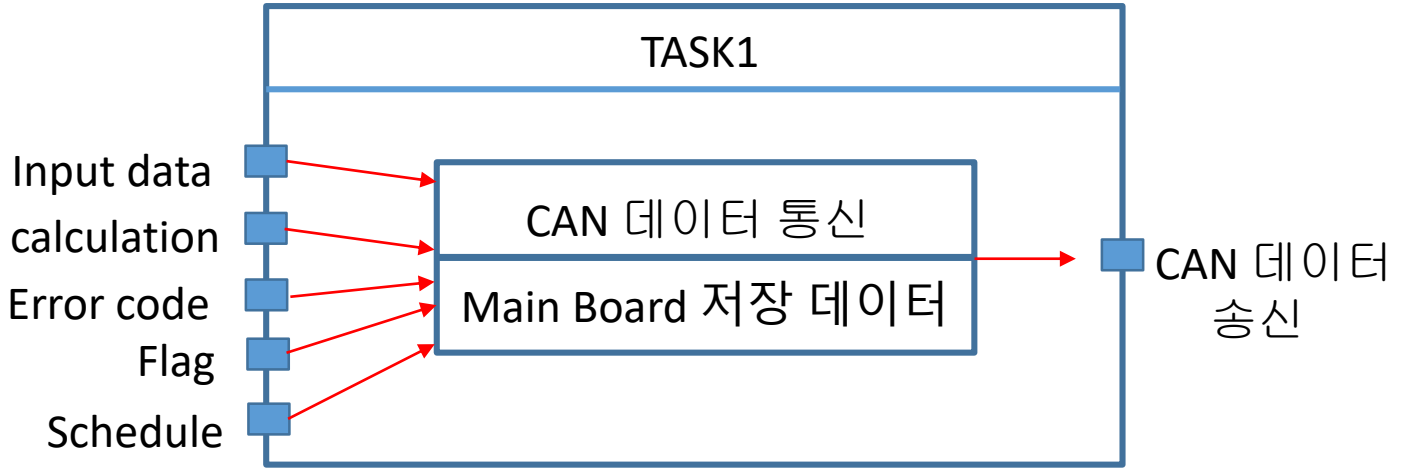
- 안전수명 주기에 따른 소프트웨어 개발 및 시험 계획
- 소프트웨어 개발 활동, 개발 기술 및 검증 방법 명시
- 사용 된 소프트웨어에 대한 일반적인 설명(프로그래밍 규칙, 개발언어, 컴파일러 등)
- 블록, 모듈, 데이터 변수 및 인터페이스에 대한 설명
- 소프트웨어 목록
- 검증 도구의 적절성 검증
- 안전수명 주기에 따른 결과물들에 대한 검증 수행 결과 문서화

3. 기능안전인증 절차

안전수명주기에 따른 소프트웨어 개발, 시험, 검증 결과 등(사례, 결과)

❍ 소프트웨어 설계

- 시스템 요구사항이 소프트웨어 설계 요구사항에 구현되어야 한다.
- 소프트웨어 아키텍처, 소프트웨어 시스템, 소프트웨어 모듈 설계 및 검증
- 소프트웨어 아키텍처 및 하드웨어/소프트웨어 상호 작용을 포함한 기능 설명
- 시스템과 소프트웨어 사이의 구성요소 식별 및 안전기능 및 진단기능의 작동 방법 명시
- 소프트웨어의 안전기능 및 진단기능과 하드웨어와의 인터페이스 정보 제공



[그림8- 소프트웨어 다이어그램]

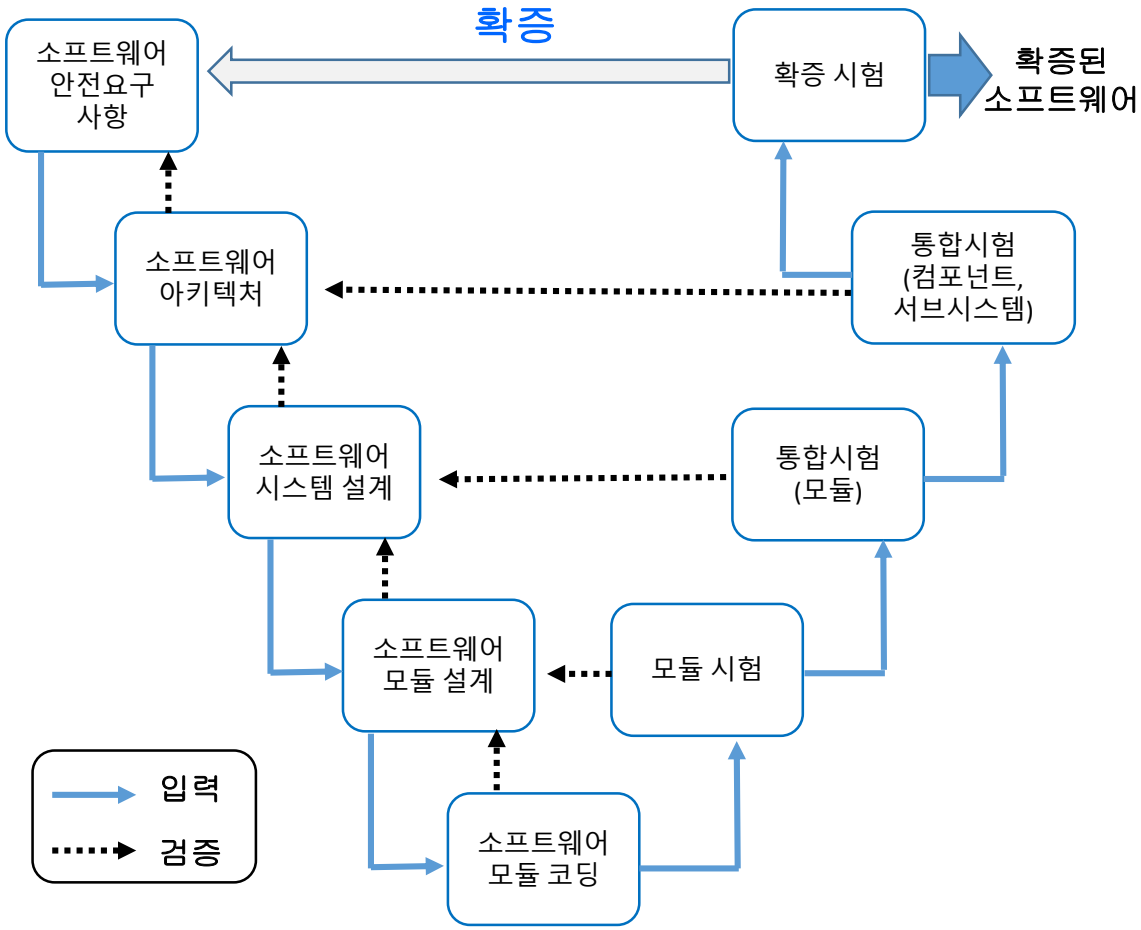
3. 기능안전인증 절차

안전수명주기에 따른 소프트웨어 개발, 시험, 검증 결과 등(사례, 결과)

❍ 시스템 안전의 소프트웨어 측면의 검증

- 코드 검토 결과서를 통한 코딩 표준 준수 여부 확인
- 검증을 위한 절차 및 방법(분석방법, 테스트 케이스)
- 합격/불합격의 기준 정의
- 검증 결과에 대한 처리 절차와 방침 및 재발 방지 절차
- 소프트웨어가 안전요구사항을 충족함을 입증

❍ 안전수명주기에 따른 소프트웨어 요구사항



3. 기능안전인증 절차

안전수명주기에 따른 소프트웨어 개발, 시험, 검증 결과 등(사례, 결과)

❍ 정적시험

- 문장(구문) 커버리지
- 분기(결정) 커버리지
- 조건 커버리지
- 소프트웨어 설계 와 코딩(코딩 규칙, 복잡성 등)
- White-Box Testing

❍ 동적시험

- 동등 분할 기법
- 경계값 분석 기법
- Black-Box Testing

❍ 문장(구문) 커버리지

- 모든 문장이 한번씩 수행되도록 검증

❍ 분기(결정) 커버리지

- 경로내에서 나타나는 모든 분기점 검증

❍ 조건 커버리지

- if, while 문 안에 있는 모든 조건 검증

❍ 동등 분할 기법

- 입력 데이터 값을 일정한 값으로 분할하여 오류 검증

❍ 경계값 분석 기법

- 각 경계값에 해당하는 값을 입력하여 오류 검증

3. 기능안전인증 절차

안전수명주기에 따른 소프트웨어 개발, 시험, 검증 결과 등(사례, 결과)

기술/수단		SIL 1	SIL 2	SIL 3	SIL 4
1	경계값 분석을 통한 테스트 케이스 실행	R	HR	HR	HR
2	오류 추측(Error guessing)에서 테스트 케이스 실행	R	R	R	R
3	오류 시드(Error seeding)에서 테스트 케이스 실행	---	R	R	R
4	모델 기반 테스트 케이스 생성(Model-based test case generation)으로부터 테스트 케이스 실행	R	R	HR	HR
5	성능 모델링	R	R	R	HR
6	동등한 클래스와 입력 파티션 테스트	R	R	R	HR
7a	구조 기반 시험 커버리지 (진입점) 100%	HR	HR	HR	HR
7b	구조 기반 시험 커버리지 (명세서) 100%	R	HR	HR	HR
7c	구조 기반 시험 커버리지 (분기) 100%	R	R	HR	HR
7d	구조 기반 시험 커버리지 (조건, MC/DC) 100%	R	R	R	HR

[표1- 소프트웨어 시험(IEC61508-3 Table B.2) 예]

3. 기능안전인증 절차

통합된 시스템의 시험 방법 및 시험 결과 관련 문서 등(사례, 결과)

❍ 시스템 시험 수행

- 안전수명 주기에 따른 시험 순서에 의거 시험 진행
- 시험 수행결과 기록
- 계획된 모든 시험의 완료되었는지 확인
- 테스트 예상 결과와 실제 결과를 비교
- 결과 불일치 원인을 파악하고 결과의 원인 분석
- 원인 분석 결과를 확인 하기 위한 테스트 활동 반복

❍ 시스템의 시험 결과 문서

- 테스트 케이스 및 시험 결과 데이터
- 시험도구(하드웨어, 소프트웨어), 장비 등의 시험 환경
- 시험 완료시 시험에 대한 합격/불합격 기준

3. 기능안전인증 절차

통합된 시스템의 시험 방법 및 시험 결과 관련 문서 등(사례, 결과)

❍ 시스템 통합시험

- **실패주입시험(Fault Injection Test)**

  정상적으로 작동하는 시스템에 인위적인 결함(Fault)를 강제로 발생 시켜 출력의 결과를 검증

  테스트 케이스는 FMEA등의 자료를 분석하여 위험한 고장 우선으로 선정

- **시뮬레이션 시험**

  하드웨어와 소프트웨어를 통합한 제어반 안전기능의 정상 작동 검증

3. 기능안전인증 절차

사용자 설명서, 안전매뉴얼, 형상관리 프로세스 및 증빙 관련 서류

❍ 사용자 설명서 및 안전매뉴얼

- 안전기능 동작 설명 및 안전관련 특성 설명
- 진단기능 동작 설명
- 하드웨어 및 소프트웨어 버전 정보
- 시스템 설치 절차
- 시스템 설정 방법 등

❍ 형상관리

- 형상관리는 이전 버전과 현재 버전 사이의 차이를 추적할 수 있도록 보장

4. 고장영향 분석[FMEA]

하드웨어 고장영향 분석

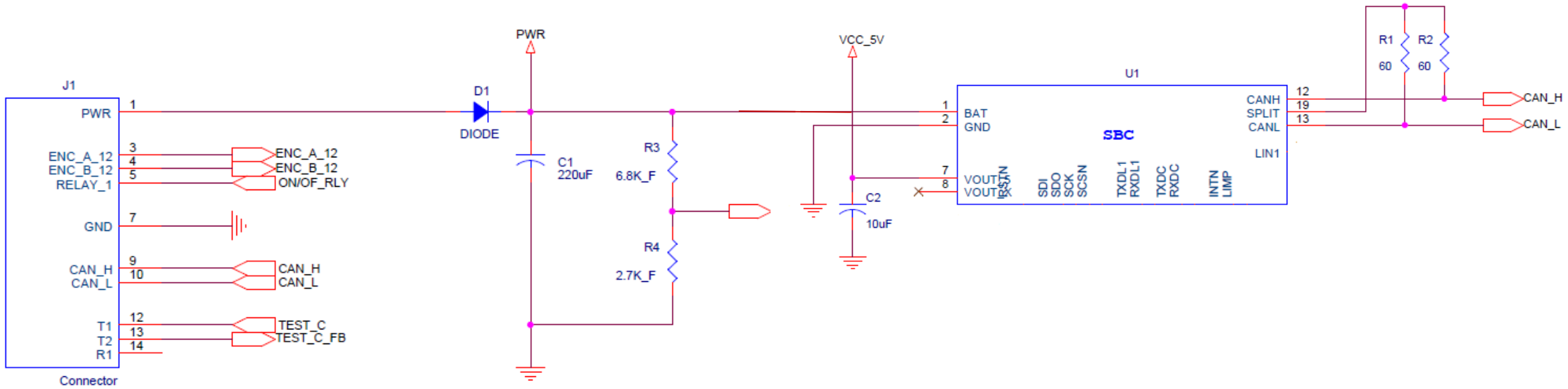
❍ 고장영향 분석

- 하드웨어 소자 및 컴포넌트의 고장모드가 시스템 기능 및 성능에 미치는 영향과 안전기능의 오동작 가능성 확인
- 하드웨어 설계 사양서를 바탕으로 **안전기능의 오동작 분석**
- 하드웨어 설계의 복잡도에 따라 **블록 단위 고장모드와 전체시스템의 고장모드**로 나누어 분석
- 고장모드로 인한 안전기능의 오동작 가능성이 없는 경우도 **시스템의 성능 및 기능에 미치는 영향 분석**

❍ 단일점결함 분석

- 해당 고장모드가 안전기능의 오동작 가능성이 있다고 파단되는 경우, 단일점 결함으로 판단
- 해당 하드웨어의 소자 및 컴포넌트의 결함이 **공통원인고장을 유발 시키는 경우 단일점 결함**으로 분류
- 단일점 결함의 경우, **고장모드를 검출하거나 오동작 가능성 감쇄를 위한 진단기능 필수**

4. 고장영향 분석[FMEA]



[그림7- 하드웨어 회로도 예]

4. 고장영향 분석[FMEA]

소자/컴포넌트 리스트 도출

❍ 하드웨어 회로도상에 존재하는 모든 전기/전자 소자 및 컴포넌트에 대한 리스트 산출

분류	세부분류	소자 리스트
소자	수동소자	저항, 커패시터, 인덕터, 써미스터, 바리스터, 포텐셔미터, 트랜스포터 등
	능동소자	다이오드, 트랜지스터, 사이리스터, 광소자 등
	기타	릴레이,스위치, 퓨즈 등
컴포넌트	직접회로	처리장치, 전원 IC, 시스템 베이시스 IC, 통신 IC, 메모리 등
	기타	인쇄회로기판(PCB: Printed Circuit Board), 컨넥터

※ 전기/전자 소자 및 컴포넌트 리스트는 공인된 산업분야에서 얻은 부품 신뢰성 데이터 참고

※ 직접회로,PCB 및 커넥터는 구조적 특성에 따라 논리적 또는 기술적으로 소자 수준까지 분리

4. 고장영향 분석[FMEA]

소자/컴포넌트 고장모드 도출

❍ 하드웨어 소자 및 컴포넌트의 고장모드에 대한 정보는IEC TR 62380, RiAC FMD97등 신뢰성 데이터 참조

분류	소자	고장모드
소자	커패시터	쇼트
		오픈
		드리프트
	다이오드	쇼트
		오픈
	저항	오픈
		드리프트

※ IEC TR 62380
Reliability data handbook. Universal model for reliability prediction of electronics components, PCBs and equipment.
이 기술 보고서는 탑재된 전자 부품의 고장률을 계산하기 위한 요소를 제공한다.

※ RIAC FMD
Reliability Information Analysis Center에서 발간한 FMD(Failure Modes/Mechanism Distributions)으로 하드웨어 소자에 대한 고장률/고장 분포 산출 시 참고할 수 있는 표준

4. 고장영향 분석[FMEA]

소프트웨어 진단기능

❍ 하드웨어 소자 및 컴포넌트의 단일점 결함 진단기능 예

식별자	진단기능	결함 검출	안전 대응
DG01	전원 모니터링	PWR의 과전압, 저전압 검출	릴레이 개방 CAN 오류 신호 전송
DG02	엔코더 입력 이중화	엔코더 신호 이중화	릴레이 개방 CAN 오류 신호 전송
DG03	릴레이 고장 검출	릴레이 제어신호 피드백	릴레이 개방 CAN 오류 신호 전송

4. 고장영향 분석[FMEA]

고장영향 분석 및 단일점 결함 분석

고장율 및 고장 모드					고장 영향		단일점 결함 분석	
하드웨어 블록	식별자	소자 형태	소자 기능	고장 모드	고장 영향 (진단기능 배제)	안전기능 오동작 가능성	단일점 결함 가능성	대응 진단기능
전원 인터페이스	D1	다이오드	역극성 대응	쇼트	· 역극성 대응 기능 상실	X		
				오픈	· ECU 전원 공급 상실 -> MCU 전원 상실 -> 릴레이 오픈	X		
	C1	220uF/전해	전원 노이즈 제거	쇼트	· ECU 전원 공급 상실	X		
				오픈	· BATT 전원 노이즈 → SBC 및 MCU 동작 불안정	O	O	DG01 / 전원 모니터링
시스템 베이시스	C2	10uF/전해	5V 전원 안정화	쇼트	· MCU 구동 불가 · 멀티펑션 스위치 전원 공급 불가 · 비상 제어 기능 불가	X		
				오픈	· 5V 전원 불안정 → MCU 구동 불안정	O	O	대응방안 없음. (5V전원 모니터링 필요)

감사합니다