

안전인증 제도 설명회
승강기 기능 안전 표준

PESSRAL/E 안전무결성 평가 KS개발

2020.10.

한국산업기술시험원 허제호 선임연구원





배경

국내 승강기 고시 개정

- 「승강기 안전관리법」제11조제3항 및 제17조제3항에 따른 「승강기안전부품 안전기준 및 승강기 안전기준」이 고시(2019년 3월 28일 시행)가 시행됨.
- 제어반을 인증품으로 지정하면서 안전회로기판에 대한 기능안전을 확인(PESSRAL, PESSRAE)하도록 하였으나 관련 시험방법 및 기준이 없어 2020년 3월 28일까지 유예하였으므로 이에 따라 시험방법 및 적용방법에 대한 기준 필요

승강기 안전관리법 (약칭: 승강기법)
[시행 2019. 3. 28.] [법률 제16526호, 2018. 3. 27., 전부개정]

행정안전부(승강기안전과), 044-205-4294

제1장 총칙

■ 제1조(목적) 이 법은 승강기의 제조·수입 및 설치에 관한 사항과 승강기의 안전인증 및 안전관리에 관한 사항 등을 규정함으로써 승강기의 안전성을 확보하고, 승강기 이용자 등의 생명·신체 및 재산을 보호함을 목적으로 한다.

■ 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. "승강기"란 건축물이나 고정된 시설물에 설치되어 일정한 경로에 따라 사람이나 화물을 승강장으로 옮기는 데에 사용되는 설비(「주차장법」에 따른 기계식주차장치 등 대통령령으로 정하는 것은 제외한다)로서 구조나 용도 등의 구분에 따라 대통령령으로 정하는 설비를 말한다.
2. "승강기부품"이란 승강기를 구성하는 제품이나 그 부분품 또는 부속품을 말한다.
3. "제조"란 승강기나 승강기부품을 판매·대여하거나 설치할 목적으로 생산·조립하거나 가공하는 것을 말한다.
4. "설치"란 승강기의 설계도면 등 기술도서(技術圖書)에 따라 승강기를 건축물이나 고정된 시설물에 정착(행정안전부령으로 정하는 범위에서의 승강기 교체 포함한다)하는 것을 말한다.
5. "유지관리"란 제28조제1항에 따른 설치검사를 받은 승강기가 그 설계에 따른 기능 및 안전성을 유지할 수 있도록 하는 다음 각 목의 안전관리 활동을 말한다.
 - 가. 주기적인 점검
 - 나. 승강기 또는 승강기부품의 수리
 - 다. 승강기부품의 교체
 - 라. 그 밖에 행정안전부장관이 승강기의 기능 및 안전성의 유지를 위하여 필요하다고 인정하여 고시하는 안전관리 활동
6. "승강기사업자"란 다음 각 목의 어느 하나에 해당하는 자를 말한다.
 - 가. 제6조제1항 전단에 따라 승강기나 승강기부품의 제조업 또는 수입업을 하기 위하여 등록을 한 자
 - 나. 제9조제1항 전단에 따라 승강기의 유지관리를 업(業)으로 하기 위하여 등록을 한 자
 - 다. 「건설산업기본법」 제9조제1항에 따라 건설업의 등록을 한 자로서 대통령령으로 정하는 승강기설치공사사업에 종사하는 자(이하 "설치공사사업자"라 한다)
7. "관리주체"란 다음 각 목의 어느 하나에 해당하는 자를 말한다.
 - 가. 승강기 소유자
 - 나. 다른 법령에 따라 승강기 관리자로 규정된 자
 - 다. 가폭 또는 나목에 해당하는 자와의 계약에 따라 승강기를 안전하게 관리할 책임과 권한을 부여받은 자

배경

별표 2, 22, 16, 24의 간결함

- 기능 안전 세부 요구사항 정의의 필요성
- IEC 61508, IEC 62061 등 국제표준의 방대함

부속서 XIII
(규정)

엘리베이터의 안전 관련 프로그램 적용 가능한 전자시스템(PESSRAL)

XIII.1 공통 조치

[표 XIII.1 - 결함용]

목적이 불분명 - 목적을 알아야 올바른 설계 적용 여부를 확인 할 수 있음

NO	대상	조치	KS C IEC 61508-7 참조표준
1	처리장치	감시장치의 사용	A.9
2	부품선정	시장 내의 부품만 사용	
3	입출력장치 및 통신연결을 포함한 인터페이스	진원부입 실패 또는 리셋의 경우 정의된 안전한 상태	
4	진원공급장치	과전압 또는 부족전압의 경우 정의된 안전한 차단 상태	A.8.2
5	가변메모리범위	고정 상태 메모리만 사용	
6	가변메모리범위	부팅 절차 동안 가변 데이터 메모리의 읽기/쓰기 시험	
7	가변메모리범위	유용한 데이터(예, 통계)에만 원격 접속	
8	불변메모리범위	시스템이나 원격조정에 의해 자동으로 프로그램코드 변경 가능성 없음	
9	불변메모리범위	검사용 합계와 동등이상의 방법을 갖는 부팅절차 동안 프로그램 코드 메모리와 고정 데이터 메모리의 시험	A.4.2

[표 XIII.2 - 결함을 방지하고 감지하기 위한 공통 조치 - 소프트웨어 설계]

NO	대상	조치	KS C IEC 61508-7 참조표준
1	구조	첨단기술에 따른 프로그램구조(즉, 모듈화, 데이터 처리, 인터페이스 정의) (EN 61508-3 참조).	B.3.4 / C.2.1 C.2.9 / C.2.7
2	부팅과정	부팅 과정 중 승강기의 안전한 상태 유지	
3	인터럽트	인터럽트의 제한적 사용: 인터럽트의 모든 가능한 한시퀀스가 예측되는 경우 만중첩인터럽트의 사용	C.2.6.5
4	인터럽트	다른 프로그램 서블루틴과 결합된 경우를 제외하고 인터럽트 절차에 의해 감시장치가 작동되지 않음.	A.9.4

[표 XIII.3 - 설계 및 구현 프로세스의 공통 조치]

No	조치	KS C IEC 61508-7 참조표준
1	응용 프로그램의 기능, 환경 및 인터페이스 측면에 대한 평가	A.14/B.1
2	안전 요구사항을 포함한 요구사항의 사양	B.2.1
3	모든 자원이 5.6.1에서 요구하는 설계 문서화 및 - 시스템 구조와 하드웨어/소프트웨어 상호작용을 포함한 기능 설명 - 기능과 프로그램 흐름 설명을 포함한 소프트웨어 문서화	C.5.9
5	설계 검토 보고서	B.3.7 / B.3.8, C.5.16
6	고장모드 및 영향분석(FMEA) 같은 방법을 사용한 신뢰성 확인	B.6.6
7	제조사 테스트 사양, 제조사의 시험 보고서 및 현장시험 보고서	B.6.1
8	의도된 사용을 위한 제한을 포함한 사용 지침서	B.4.1
9	제품이 변경된 경우 상기 기술된 방법의 반복 및 업데이트	C.5.23
10	하드웨어와 소프트웨어 버전 관리 및 호환성의 구현	C.5.24

또 다른 국제표준의 참조 - IEC 62061, KS B ISO 22201-2 (IEC 61508)

4.7 프로그램 작동 전자시스템(PESSRAE)의 설계 규칙

프로그램 작동 전자시스템(PESSRAE)는 IEC 62061 또는 KS B ISO 22201-2에 따라 설계되어야 한다.

프로그램 작동 전자시스템(PESSRAE)의 안전과 관련 없는 시스템이 동일한 하드웨어를 공유하는 경우, 프로그램 작동 전자시스템(PES)에 대한 기준을 만족해야 한다.



포함 되어야 하는 내용의 수준을 가늠하기 어려움

현황

단계적 적용

- 안정적 도입과 정착을 위해 단계적 적용 예정

승강기안전을 선도하는 국내 최고의 생활안전 전문기관
경험으로 출발! 안전으로 도착!

한국승강기안전공단

수신자 수신자 참조
(경유)
제목 기능안전인증 단계별 적용 안내

1. 귀 사의 무궁한 발전을 기원합니다.

2. 「승강기안전부품 안전기준 및 승강기 안전기준」(행정안전부고시 제2019-32호) 부칙 제2조에 따라 시행('20.03.28.)되는 기능안전인증 관련입니다.

3. 승강기업계의 기능안전인증 준비 미흡 등이 확인됨에 따라 안정적인 도입과 정착을 위하여, '기능안전인증의 단계별 적용'을 아래와 같이 안내드리오니 적극적인 준비를 바랍니다.

단계	적용시점	단계별 적용방법
1 단계	'20.03.28. 이후	신뢰성 확보를 위한 최소요건 검증
2 단계	'23.03.28. 이후	신뢰성 검증방법 심화(정량적 검증방법)
3 단계	'26.03.28. 이후	기능안전규격에 따른 범위 검증(제조사 시스템)

* 각 단계별 적용 주기는 시행일 이후 3년을 기준으로 함

4. 기능안전인증 단계별 적용(1단계 적용방법) 안내와 기능안전인증 설명회 및 세미나 일정은 조속한 시일 내에 안내드릴 예정입니다.
* 기능안전인증 단계별 적용 가이드라인 작성-배포(1단계 적용 6월 이내 안내) 예정
* 설명회 및 세미나는 코로나19로 인한 국가간염병 위기 경보 해제시 일정 안내 예정

붙임 (업체 안내) 기능안전인증 단계별 적용(안) 1부. 끝.

승강기안전기술원장

현대엘리베이터 대표이사, 티센크루프엘리베이터코리아 대표이사, 오티스엘리베이터 대표이사,
한국미쓰비시엘리베이터 대표이사, 칸들러엘리베이터 대표이사, 승강기부품 제조수입업자, 승
강기 제조수입업자 등

1. 단계별 세부 적용 방법

가. 기능안전의 안정적 도입과 정착을 위해 3단계 순차 적용

1) 1단계('20.03.28. 시행)

- 기능안전 신뢰성 확보를 위한 필수 요건 검증
- 인증기준 고시 [별표22] 부속서 X III에 기술된 문서와 **안전 분석 보고서의 정성적 검증**

< 안전기능 요구사항 >

- ▶ 시스템 안전요구사항 사양서
- 안전기능 요구사항 정의
- 시스템 설계 및 검토 보고서 검증

< 시스템 안전분석 >

- ▶ 시스템 안전 분석 보고서
- 시스템 구성 요소의 **고장모드 영향분석(FMEA4) 자료 검증**
- 시스템 구성 요소의 **결함을 회피하기 위한 조치 방법 검증**
- 소프트웨어 결함 방지 방법 검증

< 시스템 시험 >

- ▶ 시스템 시험 결과 보고서
- 안전기능 정상동작 확인을 위한 테스트 케이스 확인
- 테스트 케이스 시험 결과 검증
- 시스템 결과물 검증 시험

현황

예고고시 중

- 표준제목 : 엘리베이터, 에스컬레이터 및 무빙워크 - 안전관련 기능이 구현된 프로그램 가능한 전자 시스템 - 안전무결성 평가방법
- 예고고시 기간 : 2020.8.20 ~ 10.19

KS 예고고시

표준 표준화 활동 > KS 예고고시

고시번호(고시일)	제2020-0179호(2020.08.20)
고시제목	KS_B_NEW_2020_2261 등 1종 제정 예고고시
예고고시 기간	2020-08-20 ~ 2020-10-19
담당자	양승배
담당자연락처	043-870-5373
담당부처	국가기술표준원
담당과	기계융합산업표준과
제개정 사유	Ⓞ 사회적 요청에 의한 표준화
제개정 내용	Ⓞ 사회적 요청에 의한 표준화

구분	표준번호	표준명	의견
제정(안)	KS_B_NEW_2020_2261	엘리베이터, 에스컬레이터 및 무빙워크 - 안전 관련 기능이 구현된 프로그램 가능한 전자 시스템 - 안전무결성 평가에 대한 요구사항	<input type="button" value="의견"/>

<https://standard.go.kr/KSCI/standardIntro/standardPrvntcView.do?menuId=920&topMenuId=502&upperMenuId=516>

KSKSKSKS
 KSKSKSK
 KSKSKS
 KSKSK
 KSKS
 KSK
 KS

KS

엘리베이터, 에스컬레이터 및 무빙워크 - 안전
 관련 기능이 구현된 프로그램 가능한 전자 시스템
 - 안전무결성 평가방법
 KS B XXXX : 2020

KS B XXXX

산업표준심의회

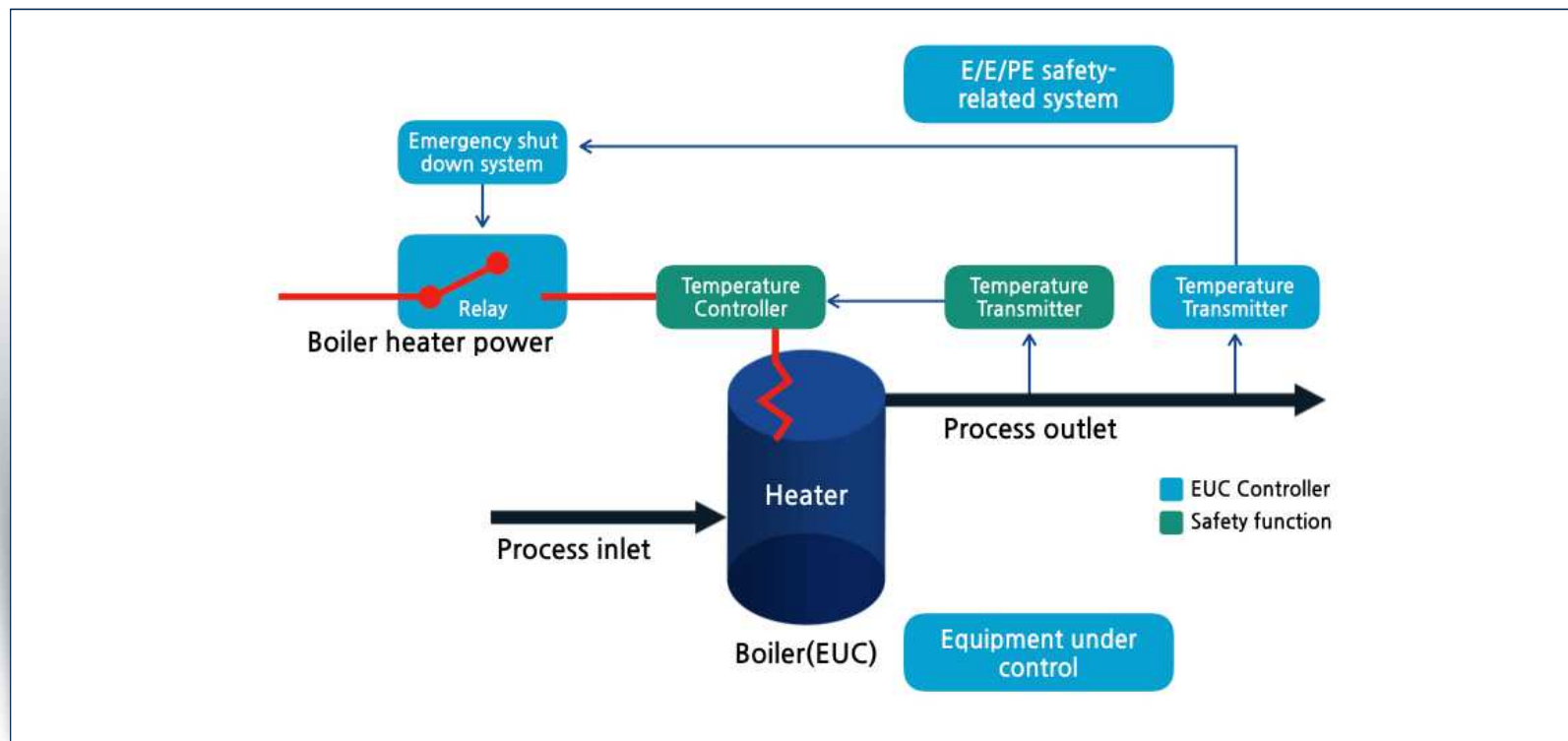
2020년 0월 0일 제정

본 문서는 저작권 규정에 따라 보호 받으며 상업적 이용 및 무단배포를 금지합니다.

기능안전이란?

Functional safety

- Part of the overall safety relating to the EUC and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures



기능안전이란?

Safety (안전)

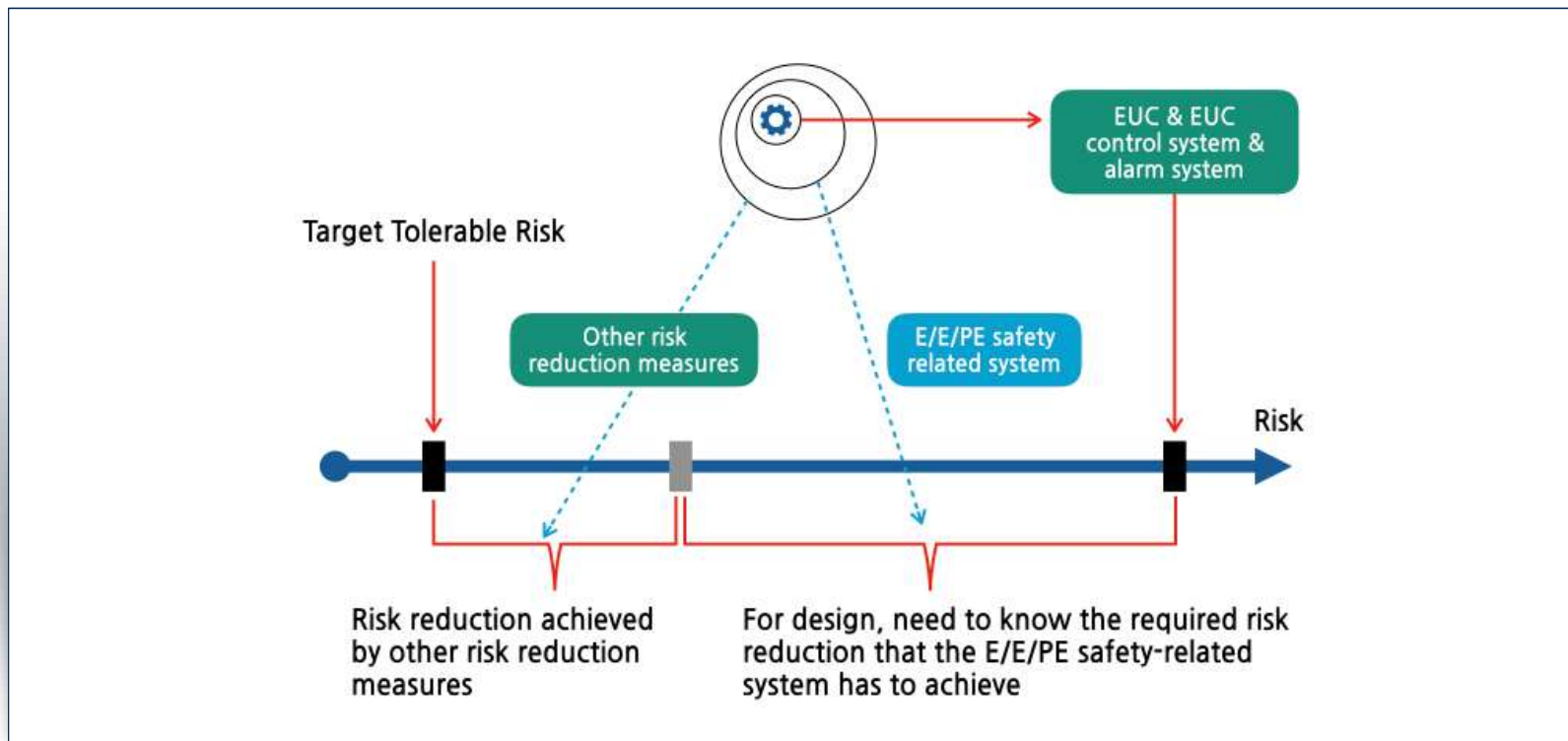
- Freedom from unacceptable risk

Risk (리스크)

- Combination of the **probability** of occurrence of harm and the **severity** of that harm

Harm (위해)

- Physical injury or damage to the health of people or damage to property or the environment



Harm은 왜 일어나는 것일까?

Harmful event

- Occurrence in which a hazardous situation or hazardous event results in harm

Hazardous situation

- Circumstance in which people, property or the environment are exposed to one or more hazards

Hazardous event

- Event that may result in harm

Hazard (위험원)

- Potential source of harm

Hazard

(ex. Unintended reversal)



+

Situation / Event

(ex. Morning rush hour)



➔

Harm

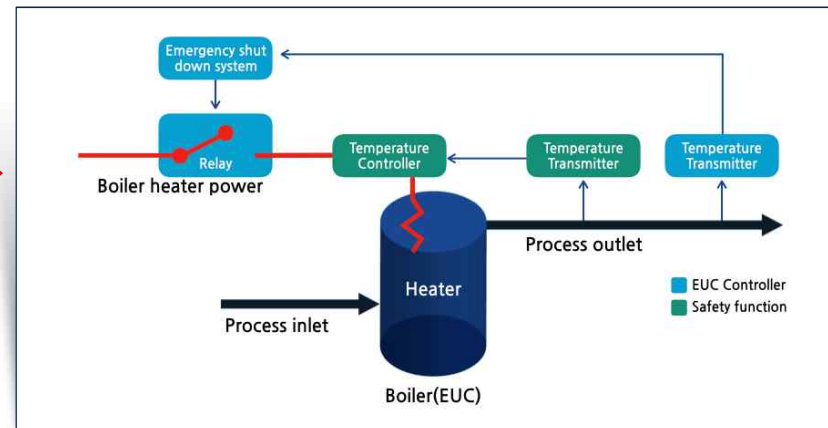
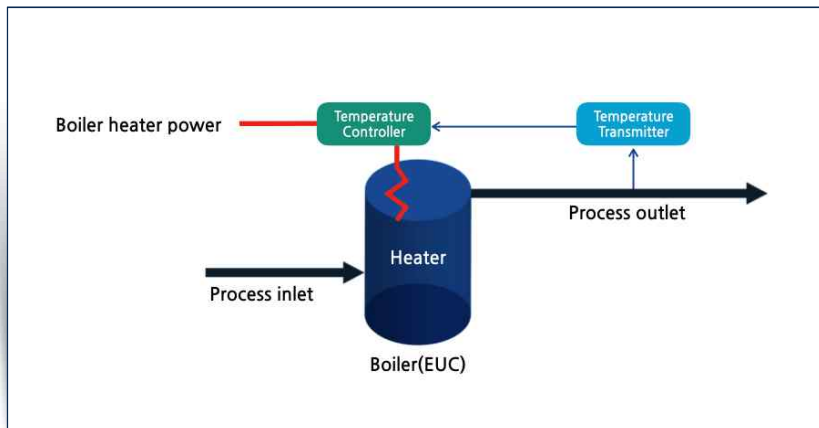
(physical injury)



Hazard는 어떻게 막을 것인가? - 안전기능

Safety function

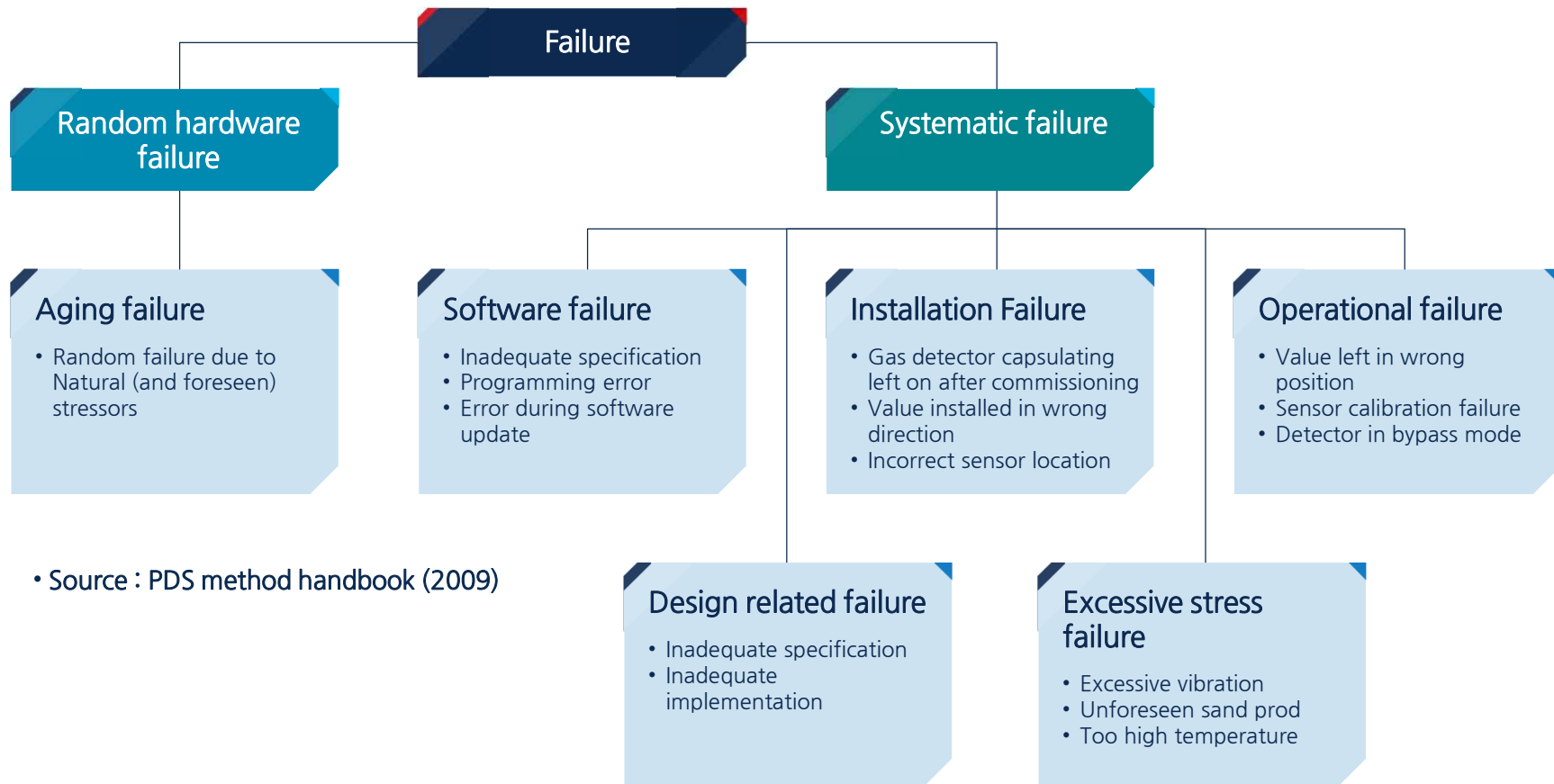
- Function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event



Safety Integrity는 어떻게 확보 할 것인가?

Failure

- Termination of the ability of a functional unit to provide a required function or operation of a functional unit in any way other than as required



• Source : PDS method handbook (2009)

Safety Integrity Assessment

평가 목적

- 제품의 고장의 원인이 되는 요소를 극복하기 위한 절차 및 설계 사양의 적절성을 판단
 - 하드웨어 안전 무결성 (Hardware safety integrity)
 - 체계적인 안전 무결성 (Systematic safety integrity)

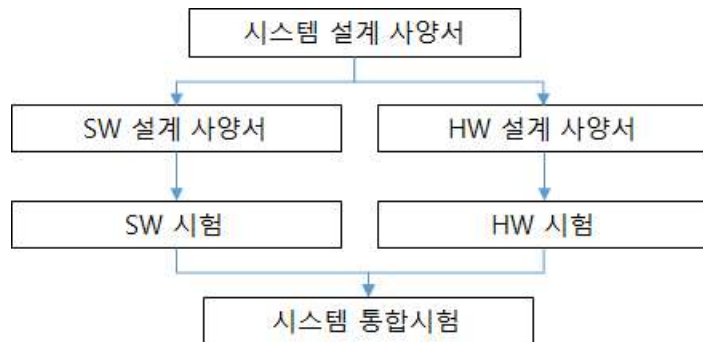
평가 방법

구분	설명	평가대상
문서평가	제품 개발을 위한 계획 및 제품 설계 사양에 대한 정확한 이해를 목적으로 PES SRAL 또는 PESSRAE 개발 업체가 작성한 산출물을 대상으로 제품을 이해하기 위한 정보의 적절성을 판단하는 활동	개발업체 제출 산출물
구현확인	제품 개발을 위한 계획의 이행여부 및 제품 설계 사양의 정확한 구현 여부를 판단하는 활동	개발 계획 이행 하드웨어 및 소프트웨어 구현
안전분석	PESSRAL과 PESSRAE를 구성하고 있는 하드웨어 구성요소를 대상으로 고장 모드 식별, 고장 모드 영향성 분석 및 고장 모드를 제어하기 위한 진단 기능의 구현의 적절성을 평가하는 활동	하드웨어 상세 설계
입회시험	구현된 제품이 설계 사양과 동일하게 동작하는지 시험을 통해 확인하는 활동	동작하는 하드웨어, 소프트웨어

Systematic safety integrity 평가 방안

Systematic safety integrity

- 간단한 안전 개발 프로세스를 가정하고 필요한 산출물과 산출물의 항목을 제공



4.3.2 안전수명 주기 적용에 대한 평가

- ▷ 4.3.2.1 개발 관리 계획 평가
- ▷ 4.3.2.2 시스템 설계 요구사항 및 사양서 평가
- ▷ 4.3.2.3 하드웨어 설계 사양서 평가
- ▷ 4.3.2.4 소프트웨어 설계 사양서 평가
- ▷ 4.3.2.5 안전분석 보고서 평가
- ▷ 4.3.2.6 소프트웨어 시험 계획 및 결과 평가
- ▷ 4.3.2.7 시스템 시험 계획 및 결과 평가
- ▷ 4.3.2.8 안전확인 계획 및 결과 평가
- ▷ 4.3.2.9 사용자 매뉴얼 평가

Systematic safety integrity 평가 방안

Systematic safety integrity

- 별표에 언급된 산출물과 요구사항에 대해 파악해야하는 중점 사항을 식별함

[표 XIII.3 - 설계 및 구현 프로세스의 공통 조치]

No	조치	KS C IEC 61508-7 참고표준
1	응용 프로그램의 기능, 환경 및 인터페이스 측면에 대한 평가	A.14/B.1
2	안전 요구사항을 포함한 요구사항의 사양	B.2.1
3	모든 사양의 검토	B.2.6
4	5.6.1에서 요구하는 설계 문서화 및 - 시스템 구조와 하드웨어/소프트웨어 상호작용을 포함한 기능 설명 - 기능과 프로그램 흐름 설명을 포함한 소프트웨어 문서화	C.5.9
5	설계 검토 보고서	B.3.7 / B.3.8, C.5.16
6	고장모드 및 영향분석(FMEA) 같은 방법을 사용한 신뢰성 확인	B.6.6
7	제조자의 테스트 사양, 제조자의 시험 보고서 및 현장시험 보고서	B.6.1
8	의도된 사용을 위한 제한을 포함한 사용 지침서	B.4.1
9	제품이 변경된 경우 상기 기술된 방법의 반복 및 업데이트	C.5.23
10	하드웨어와 소프트웨어 버전 관리 및 호환성의 구현	C.5.24

4.3.2.2 시스템 설계 요구사항 및 사양서 평가

시스템 설계 요구사항 및 사양서 평가의 목적은 평가자가 PES로 개발된 안전 장치의 안전기능 및 진단기능의 동작의 이해를 바탕으로 구현확인, 입회시험을 수행하기 위함이다.

표 3 - 시스템 설계 요구사항 사양서 평가 요약

구분	시스템 설계 요구사항 및 사양서 평가
관련사항	엘리베이터 안전기준, 별표22, 부속서 XIII, 표 XIII.3/2 엘리베이터 안전기준, 별표22, 부속서 XIII, 표 XIII.3/3 엘리베이터 안전기준, 별표22, 부속서 XIII, 표 XIII.3/4 엘리베이터 안전기준, 별표22, 부속서 XIII, 표 XIII.3/5 엘리베이터 안전기준, 별표22, 부속서 XIII, 표 XIII.4/ 구조 엘리베이터 안전기준, 별표22, 부속서 XIII, 표 XIII.5/ 구조 엘리베이터 안전기준, 별표22, 부속서 XIII, 표 XIII.6/ 구조 KS C IEC 61508-7의 B.2.1, B.2.6, C.5.9, A.3.1, A.3.3, A.2.5, B.3.7 / B.3.8, C.5.16
문서평가 항목	1) 안전기능 사양 확인 2) 진단기능 사양 확인
구현확인 평가 항목	1) 안전기능 및 진단기능을 구현한 하드웨어 및 소프트웨어 구성요소 및 구성요소간 인터페이스 확인

4.3.2.2.1 문서평가

4.3.2.2.1.1 안전기능의 동작 사양이 평가 되어야 한다. 다음의 항목의 존재 유무 및 정확성이 평가 되어야 한다.

- a) 안전기능의 입력, 출력 인터페이스
 - 비고 안전 장치의 커넥터 단의 입출력 인터페이스를 통해 확인할 수 있다.
 - b) 안전기능의 동작을 유발하는 기준 및 정의된 안전상태
 - c) 안전기능을 구성하고 있는 구성요소 및 구성요소 간 인터페이스
 - 비고 안전기능을 수행하는 하드웨어 및 소프트웨어의 구현을 고려하여 논리적인 형태로 표현되어 질 수 있다. 해당 구성요소 및 인터페이스는 시스템 아키텍처 상에 표현되어 있어야 한다.
 - d) 안전기능의 시간제약 사항
 - 비고 시간제약 사항의 설정에 대한 타당성은 시험자료 등의 합리적인 근거로 뒷받침되어야 한다.
- 4.3.2.2.1.2 안전기능의 구조는 하나의 임의의 고장이 감지되면 시스템이 안전한 상태로 들어가는 구조로 다음의 SIL 등급에 따른 아래 가능한 조치사항의 적용여부가 평가 되어야 한다.

Hardware safety integrity 평가 방안

Hardware safety integrity

- 단일점 결함에 대응하는 수준에 대한 평가 (단일점 결함 - 하나의 결함으로 안전기능을 오동작하게 하는 결함)
- pcb를 구성하는 part, component 전체의 집합을 pessler/e로 보고 개별 part와 component에 대한 고장모드를 식별하고 안전기능에 대한 영향분석을 통해 설계의 적절성 판단
- 분석 단계에 대한 철자 제공

4.4.2 하드웨어 우발결함을 제어하기 위한 진단 기능에 대한 평가 (안전분석)

- ▷ 4.4.2.1 1단계: 소자/컴포넌트 리스트의 산출
- ▷ 4.4.2.2 2단계: 소자/컴포넌트의 고장 모드 도출
- ▷ 4.4.2.3 3단계: 고장 영향 분석
- ▷ 4.4.2.4 4단계: 단일점 결함 분석 및 안전기능의 무결성 확보

비고 2 하드웨어 소자 및 컴포넌트의 고장 모드가 기계적인 관점의 고장 모드를 포함하고 있거나, 복수개의 고장모드가 전기/전자적 관점에서 동일하게 간주 될 수 있는 경우, 고장 모드에 대한 경계를 수행 할 수 있다.

보기 예: 열점, 열점 저항

표 15 - 매달 필름 저항 고장 모드 예

기본 고장 모드	정체 고장 모드	비고
오픈 서킷	오픈 서킷	크랙/균열 및 크랙 포함
적합 값 변화	적합 값 변화	오염 포함
오염	쇼트 서킷	
크랙/균열		
크랙		
쇼트 서킷		

4.4.2.2.2 논리적인 관점에서 보다 세부적인 하드웨어 소자로 분리 될 수 있는 하드웨어 컴포넌트의 경우, 하드웨어 컴포넌트를 구성하는 세부적인 하드웨어 소자 관점의 고장 모드가 정의되어야 한다.

비고 1 필요한 경우, HAZOP 및 FMEA를 통해 하드웨어 소자 및 컴포넌트의 고장 모드를 추정 할 수 있다. 이 경우, 동일 하드웨어 소자 및 컴포넌트라도 그 사용 목적에 따라 서로 다른 고장 모드로 추정 할 수 있다.

비고 2 하드웨어 컴포넌트 내부의 세부적인 하드웨어 소자에 대한 고장 모드에 대한 정보가 불명확한 경우, 하드웨어 소자의 결함이 하드웨어 컴포넌트의 동작에 미치는 영향을 기반으로 고장 모드를 추정 할 수 있다.

보기 1 처리장치의 고장 모드 추정 예

표 16 - 고장 모드 추정 예

컴포넌트	소자	고장 모드
마이크로 컨트롤러	프로세싱 코어	연산 오류 및 데이터 읽기/저장 오류
	메모리 - ROM	1 개 비트 오류
		2 개 이상 비트의 오류
	메모리 - RAM	1 개 비트 오류
		2 개 이상 비트의 오류
내부 전원	MCU 내부 공급 전원 오류	
		부하 드라이버 공급 전원 오류
클럭		클럭 경계
		규정 주파수 이탈
타이머		타이머 기능 정지
		타이머 시간 범위 이탈
CAN 컨트롤러		CAN 메시지 수신 오류
		CAN 메시지 송신 오류
		CAN 통신 기능 상실
		CAN 통신 기능 상실
LIN 컨트롤러		LIN 메시지 수신 오류
		LIN 메시지 송신 오류
		LIN 통신 기능 상실
4 채널 ADC		허용 범위 밖 측정 값 고정

Hardware safety integrity 평가 방안

예제 제공

- 예제 제공으로 안전분석 활동의 이해도 향상

부속서 A
(참고)

하드웨어 수준 안전분석 예

A.1 일반

본 부속서는 하드웨어 수준의 안전 분석 방법에 대한 일반적인 설명을 제공하며 A.2 작성 예는 오직 정보 제공을 목적으로 한다. A.2 작성 예에 기술된 사항은 실제 설계에 대한 기술적 타당성에 근거하지 않으며, 하드웨어 수준의 안전 분석에 대한 설명을 위해 임의적으로 작성된 예제임을 밝힌다.

A.1.1 안전 기능, 안전무결성등급 및 안전 상태 정의

표 A.1 - 안전기능, 안전무결성등급 및 안전 상태 예시

안전 기능	안전무결성등급	안전 상태
속도가 정격 속도의 20%를 초과하기 전에 에스컬레이터의 과속이나 이동 보행을 감지하고 기계 모터와 브레이크의 전원을 제거	SIL 2	모터 및 작동 브레이크 동력 제거

A.1.2 기술적 특성

A.1.2.1 하드웨어 블록 다이어그램

분석에 사용된 예제 시스템의 하드웨어는 아래 그림과 같이 총 5개의 하드웨어 블록으로 구성되어 있으며, 각 블록에 대한 설명은 표 A.2를 따른다.

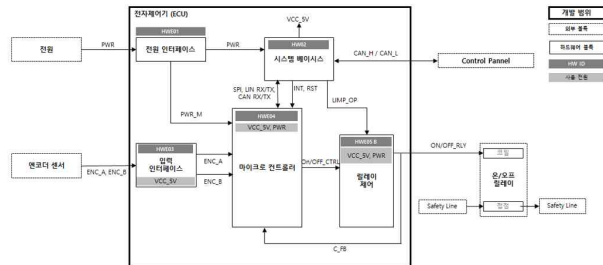
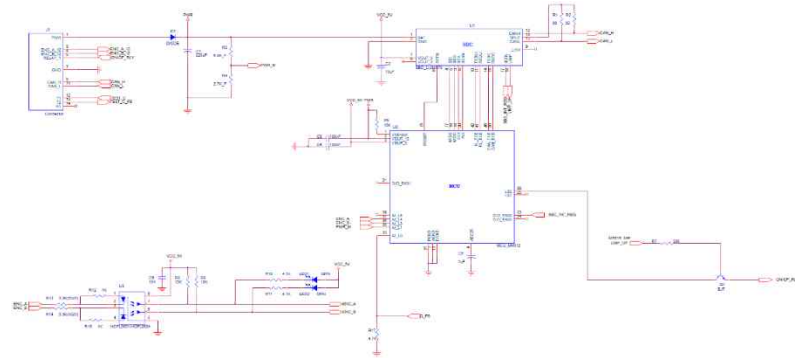


그림 A.1 - 예제 시스템의 하드웨어 블록 다이어그램



하드웨어 블록	식별자	고장을 및 고장 모드		고장 영향 (진단기능 배제)	안전기능 오동작 가능성	단일점 결합 분석	
		소자 형태	소자 기능			고장 영향	고장 영향
R14	3.3K옴/칩 메탈 필름	노이즈 필터 (RC필터)	오픈 서킷	Encoder 신호 경로 유실 → 속도 판정 불가 → 의도하지 않은 안전기능 동작 불가	O	O	DG02 / 엔코더 입력 이중화
				드립트	고장 영향 없음	X	
R12	1K옴/칩 메탈 필름	노이즈 필터 (RC필터)	오픈 서킷	Encoder 신호 경로 유실 → 속도 판정 불가 → 의도하지 않은 안전기능 동작 불가	O	O	DG02 / 엔코더 입력 이중화
				드립트	고장 영향 없음	X	
R16	1K옴/칩 메탈 필름	노이즈 필터 (RC필터)	오픈 서킷	Encoder 신호 경로 유실 → 속도 판정 불가 → 의도하지 않은 안전기능 동작 불가	O	O	DG02 / 엔코더 입력 이중화
				드립트	고장 영향 없음	X	
C6	104nF/칩 세라믹	노이즈 필터 (RC필터), 전 기적 보호	쇼트 서킷	Encoder 신호 경로 유실 → 속도 판정 불가 → 의도하지 않은 안전기능 동작 불가	O	O	DG02 / 엔코더 입력 이중화
				오픈 서킷	노이즈 필터 및 전기적 보호 기능 상실	O	O
R8	10K/칩 메탈 필름	Pull-up	오픈 서킷	Encoder 신호 경로 유실 → 속도 판정 불가 → 의도하지 않은 안전기능 동작 불가	O	O	DG02 / 엔코더 입력 이중화
				드립트	노이즈 필터 및 전기적 보호 기능 상실	O	X

결론 및 향후 계획

표준의 의의

- 기능안전 평가의 체계적이 수행의 기초 마련
- 업체 대응 방향 제시

향후 계획

- 예고 고시 후, 기술심의 위원회를 통해 최종 KS 표준 제정 여부 결정 (10월30일 예정)
- 공단 적용 단계에 따른 지속적인 표준 갱신

단계	적용시점	단계별 적용방법
1 단계	'20.03.28. 이후	신뢰성 확보를 위한 최소요건 검증
2 단계	'23.03.28. 이후	신뢰성 검증방법 심화(정량적 검증방법)
3 단계	'26.03.28. 이후	기능안전규격에 따른 범위 검증(제조사 시스템)

- 해당 표준의 국제 표준화 - ISO TC178 WG8
 - 개발 표준에 대한 해외 전문가 검토 및 최신 기술 수준 유지

감사합니다

