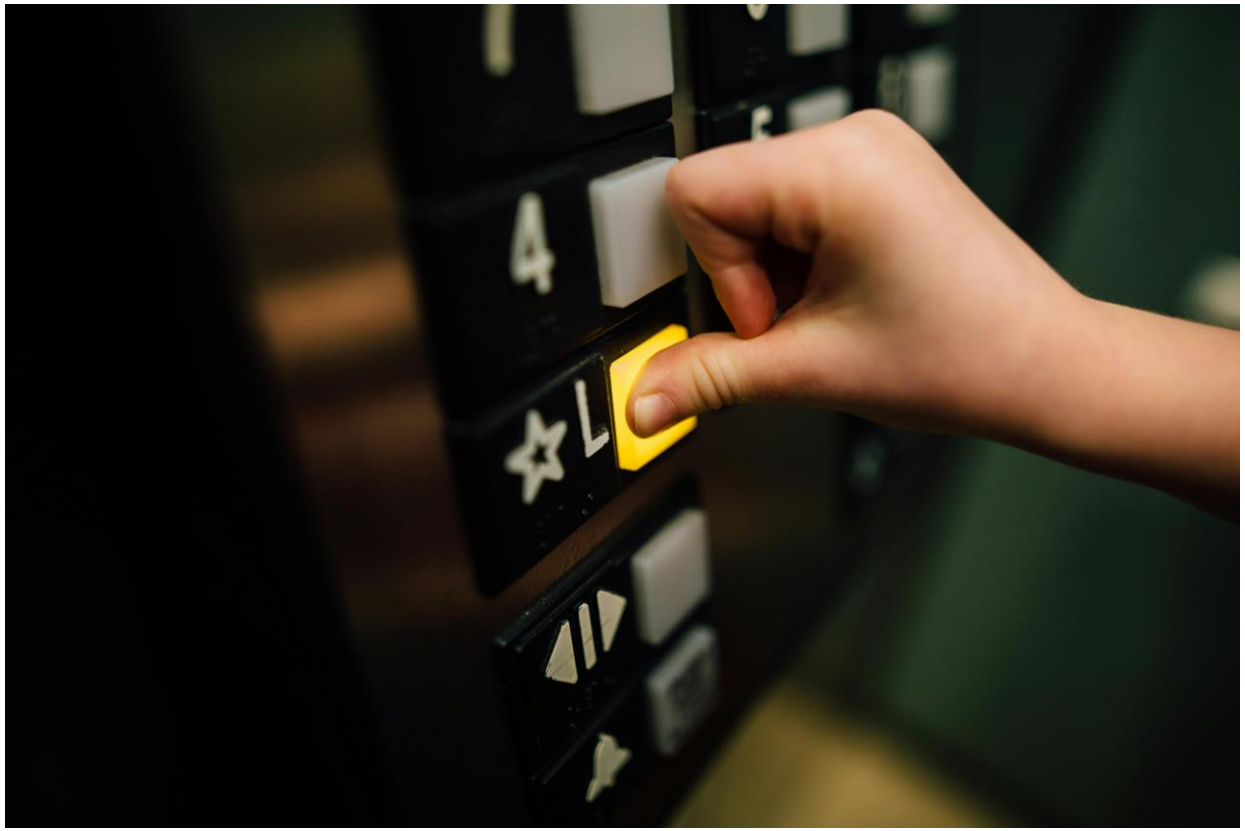


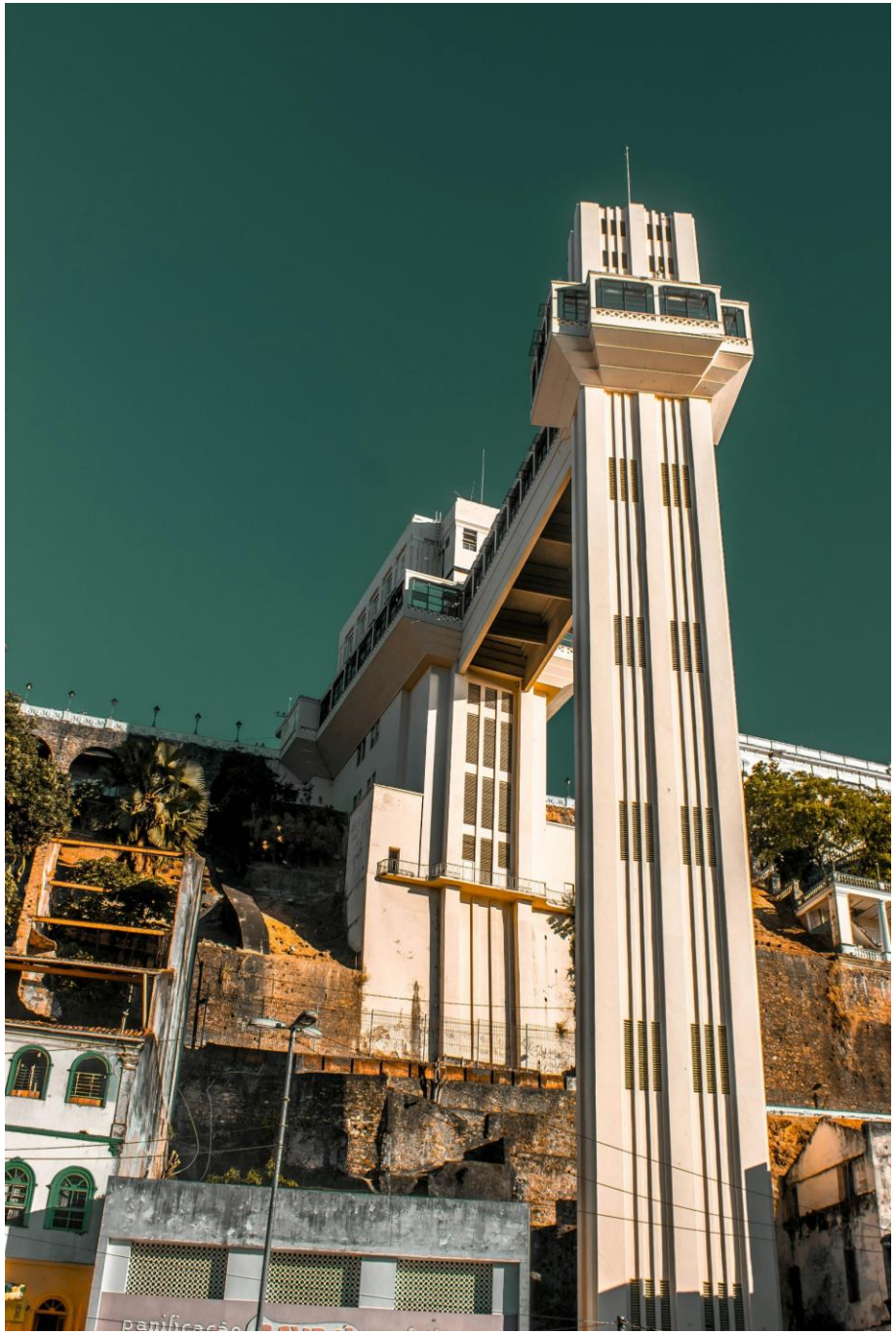
한국승강기안전공단
KOREA ELEVATOR SAFETY AGENCY

Functional Safety for Elevator & Escalator

한국승강기안전공단 안전인증실 하 태 원

목차

KoELSA



Ⅰ. 소개

1.1. 강사 소개

1.1. 강사 소개

하태원
특급인증심사원

승강기안전기술원
안전인증처/안전인증실
T 055-940-9943 M 010-4416-7414
E topgun@koelsa.or.kr

□ 1996.04. ~ 1999.08.
- 한국승강기안전관리원 입사(검사원: 대구경북지역)

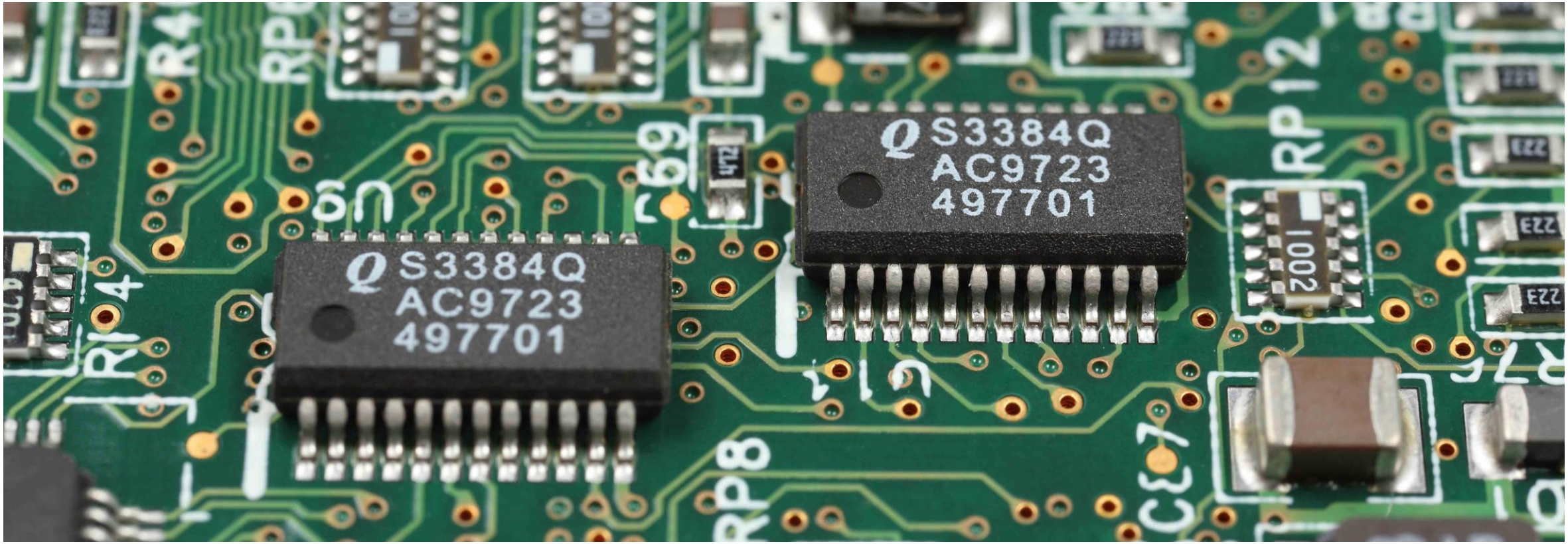
□ 1999.08. ~ 2001.12.
- 벤처기업 창업 / 개발 책임자 역임: 임베디드 시스템 설계

□ 2002.01. ~ 2018.11.
- 한국승강기안전관리원 재입사(대구경북지원 검사원)
- 한국승강기안전공단 변경

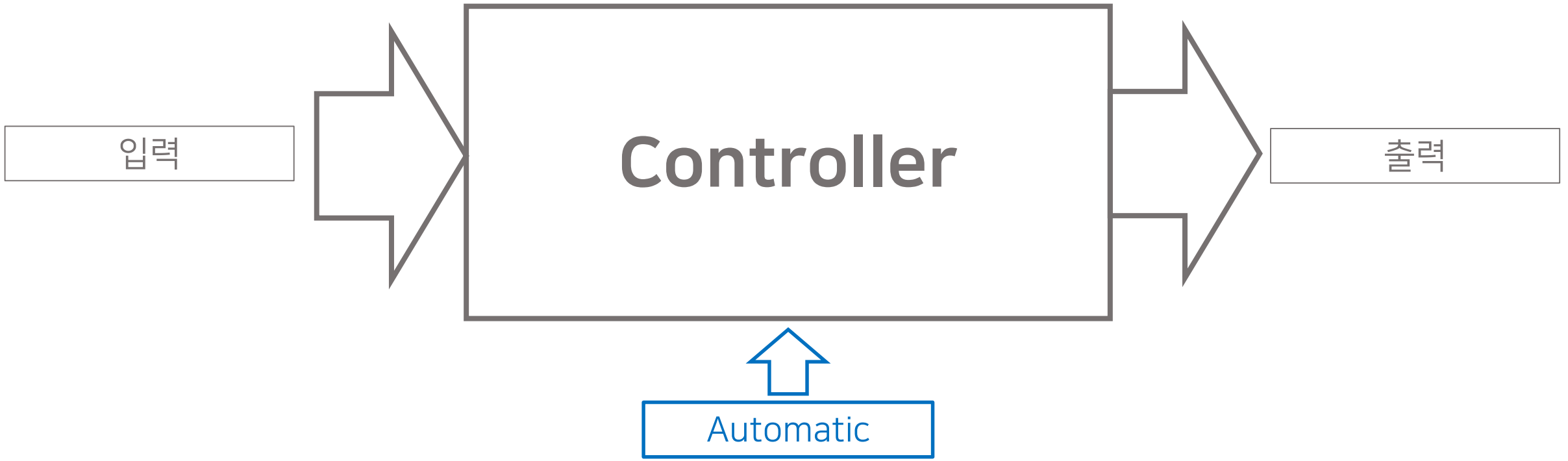
□ 2018.12. ~ 현재
한국승강기안전공단 승강기안전기술원 안전인증처 안전인증실
- 부품안전인증 전기파트 총괄
- 기능안전인증(PESSRAL, PESSRAE) 심사원
- 경북대학교 전기전자공학부 석사

* 논문: YOLO를 이용한 에스컬레이터 사고 감지 알고리즘 설계 및 구현
(2024년 한국승강기학회 게재 – 추계학술대회 발표)

Ⅱ. Embedded System

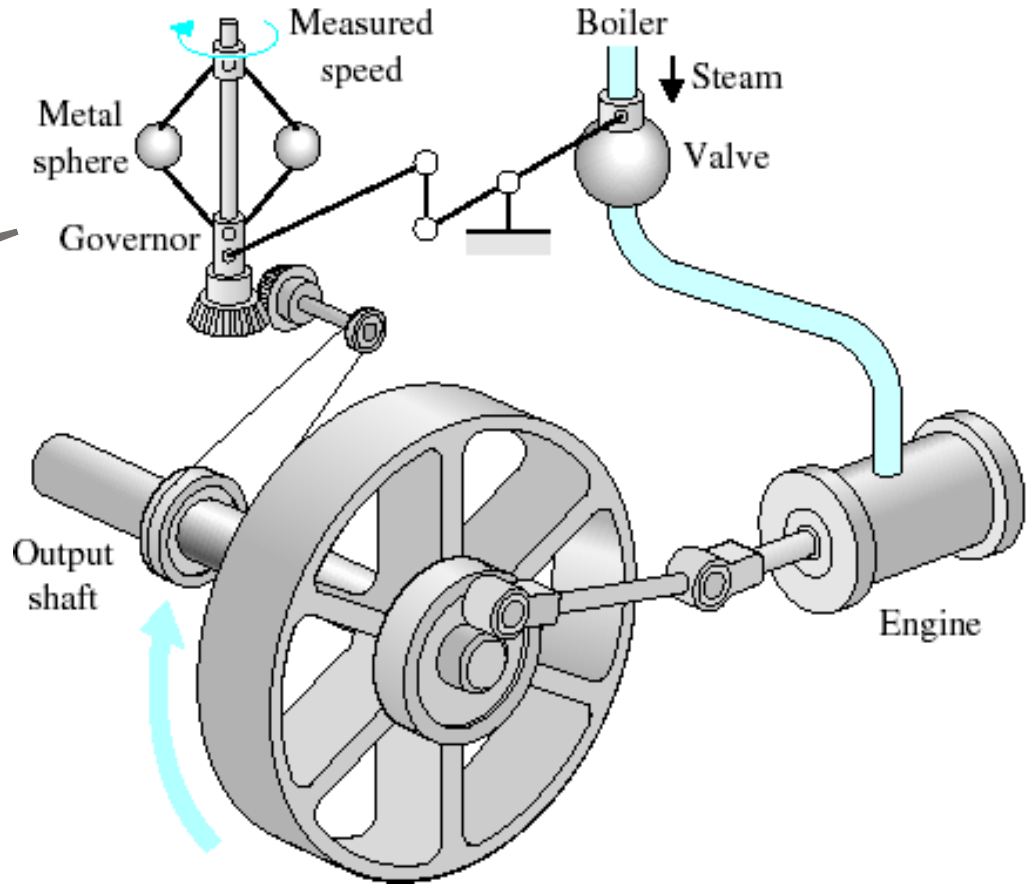


□ Controller의 목적



☐ Automatic Controller of 18th Century : Watt's Flyball Governor

엘리베이터 유사장치 – 플라이볼형 과속조절기



https://www.youtube.com/watch?v=HS_YGZXP2xY

KoELSA

□ 다양한 입력과 출력형태를 갖는 Controller

☐ Airbus 380: 680 ton maximum take-off weight, 75,000 HP engines

This material is taken from The University of NewCastle.

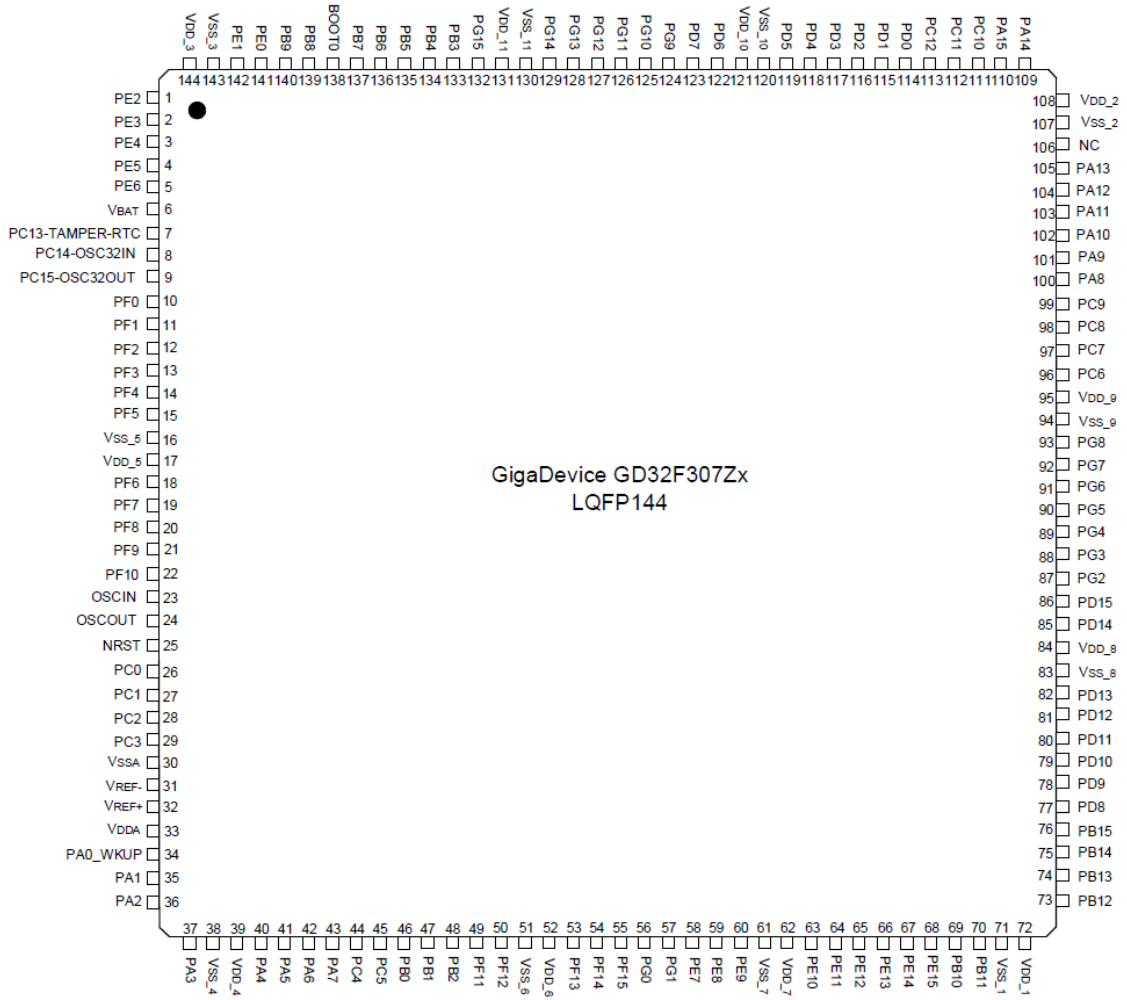
☐ Airbus 380 Controller

비행기 속도
엔진의 회전속도
항공유의 주입량
공기의 주입량
고도
바람 속도
승객의 무게
비행기 수평도
날개 상태
꼬리날개 상태
랜딩기어 상태
네비게이션 센서
…

안전이 보장된
다양한 최적의
출력제어가 필요

KoELSA

☐ GD32F307Zx LQFP144 pinouts(GIgaDevice)



Pin Name	Pins	Pin Type(1)	I/O Level(2)	Functions description
PE2	1	I/O	5VT	Default: PE2 Alternate: TRACECK, EXMC_A23
PE3	2	I/O	5VT	Default: PE3 Alternate: TRACED0, EXMC_A19
PE4	3	I/O	5VT	Default: PE4 Alternate:TRACED1, EXMC_A20
PE5	4	I/O	5VT	Default: PE5 Alternate:TRACED2, EXMC_A21 Remap: TIMER8_CH0(3)
PE6	5	I/O	5VT	Default: PE6 Alternate:TRACED3, EXMC_A22 Remap: TIMER8_CH1(3)
VBAT	6	P		Default: VBAT
PC13-TAMPER-RTC	7	I/O		Default: PC13 Alternate: TAMPER-RTC
PC14-OSC32IN	8	I/O		Default: PC14 Alternate: OSC32IN
PC15-OSC32OUT	9	I/O		Default: PC15 Alternate: OSC32OUT
PF0	10	I/O	5VT	Default: PF0 Alternate: EXMC_A0 Remap: CTC_SYNC
PF1	11	I/O	5VT	Default: PF1 Alternate: EXMC_A1
PF2	12	I/O	5VT	Default: PF2 Alternate: EXMC_A2
PF3	13	I/O	5VT	Default: PF3 Alternate: EXMC_A3
PF4	14	I/O	5VT	Default: PF4 Alternate: EXMC_A4
PF5	15	I/O	5VT	Default: PF5 Alternate: EXMC_A5
VSS_5	16	P		Default: VSS_5
VDD_5	17	P		Default: VDD_5

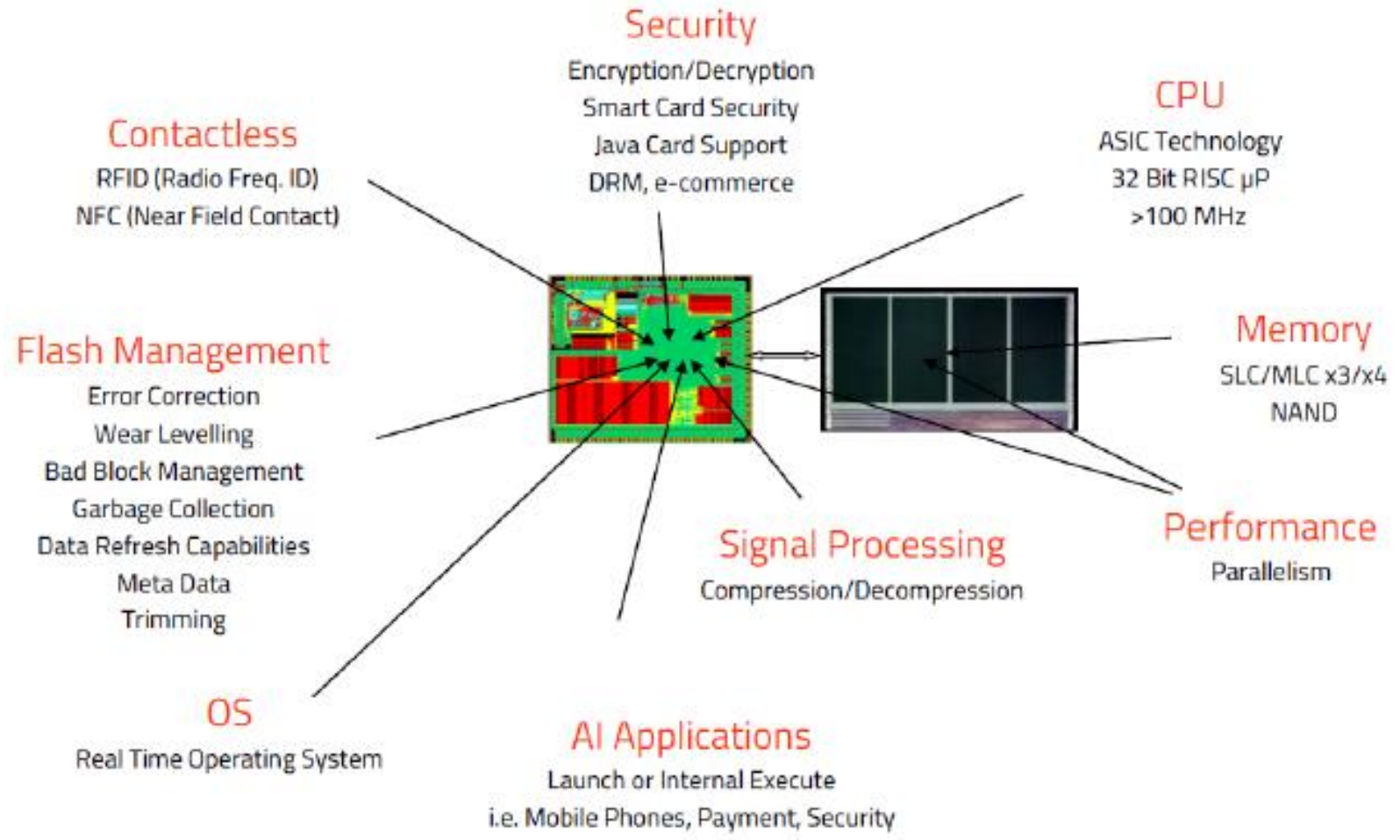
Pin Name	Pins	Pin Type(1)	I/O Level(2)	Functions description
PB8	139	I/O	5VT	Default: PB8 Alternate: TIMER3_CH2, TIMER9_CH0(3), ENET_MII_TXD3 Remap: I2C0_SCL, CAN0_RX
PB9	140	I/O	5VT	Default: PB9 Alternate: TIMER3_CH3, TIMER10_CH0(3) Remap: I2C0_SDA, CAN0_TX
PE0	141	I/O	5VT	Default: PE0 Alternate: TIMER3_ETI, EXMC_NBL0
PE1	142	I/O	5VT	Default: PE1 Alternate: EXMC_NBL1
VSS_3	143	P		Default: VSS_3
VDD_3	144	P		Default: VDD_3

GD32F307Zx LQFP144 pin definitions

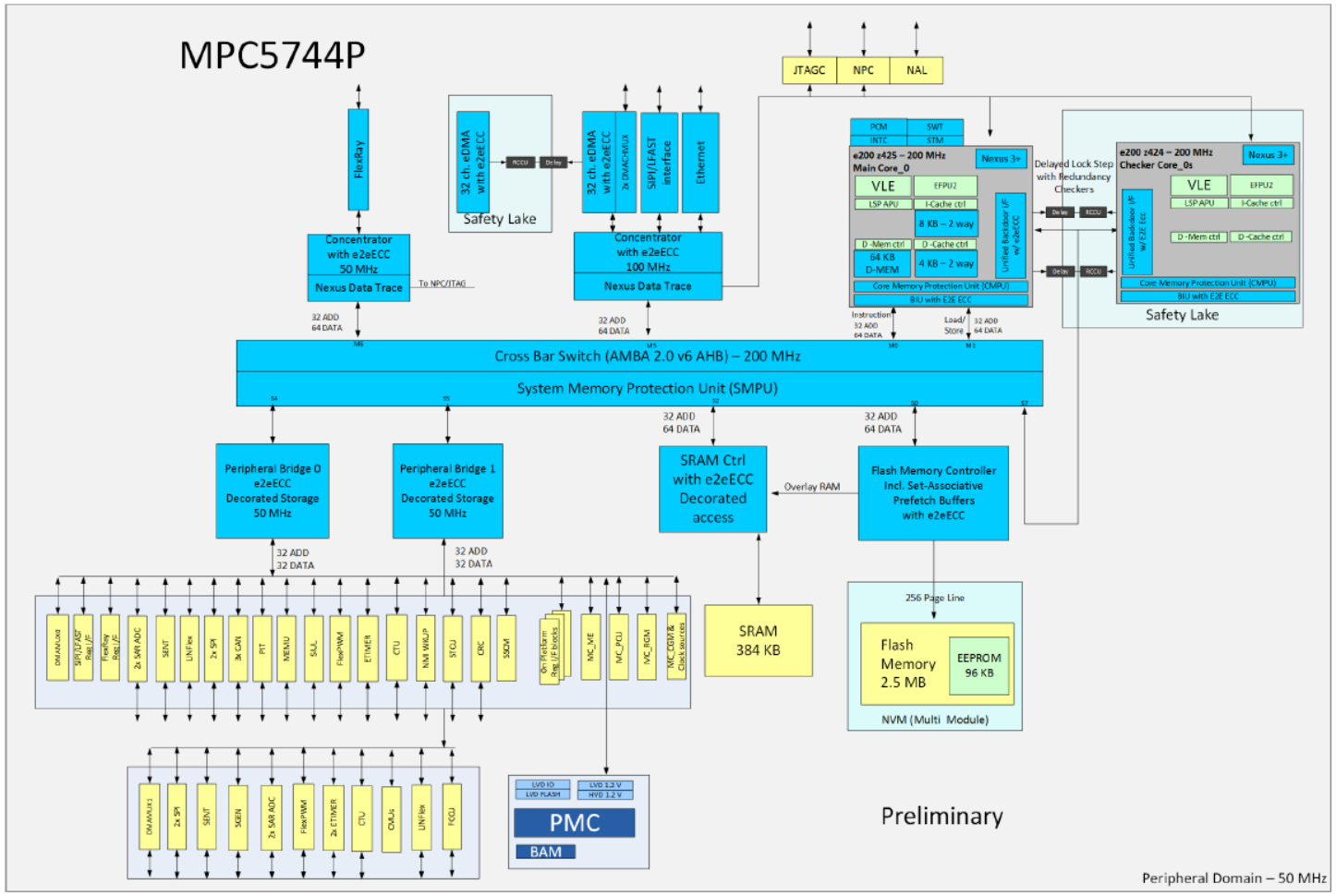
KoELSA

□ 임베디드 시스템이란?

하드웨어에 소프트웨어가 Embedded 된 시스템



□ MCU 내부구조



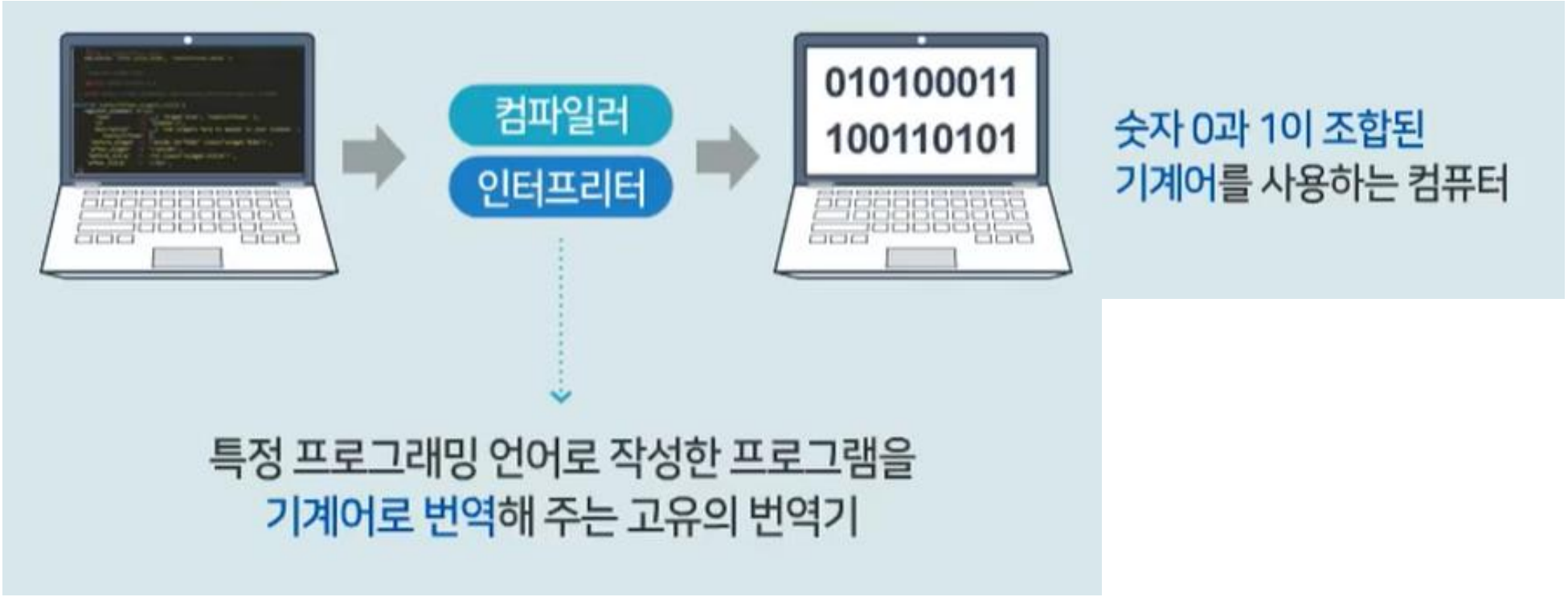
MPC5744P(NXP Semiconductors) System Block Diagram

하드웨어에서 원하는 결과가 나오도록
소프트웨어를 작성하는 일 : 프로그래밍

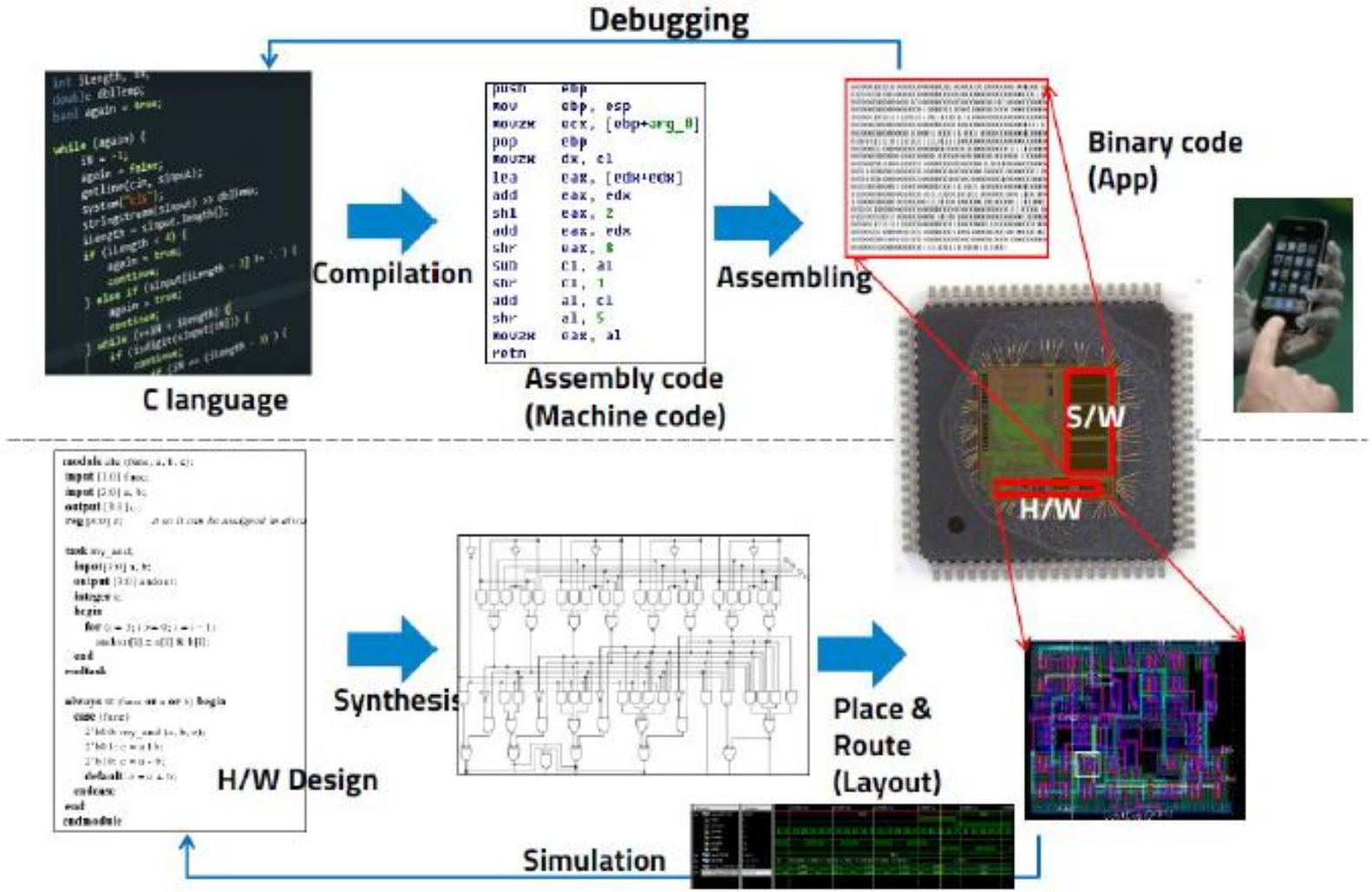
KoELSA

☐ Programming Language

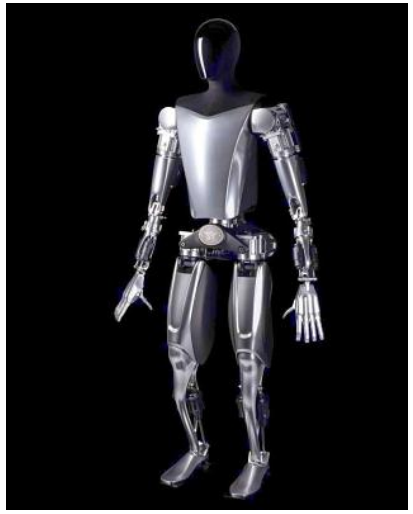
- 사람이 컴퓨터(MCU)에게 원하는 작업을 언어로써 체계적으로 표기하는 것 : 사람이 사용하는 언어에 가깝도록 정의
- MCU는 숫자 0과 1의 조합으로 된 기계어만 이해함
- 시스템 Programming 부분에서 가장 많이 사용되는 Language : C, C++

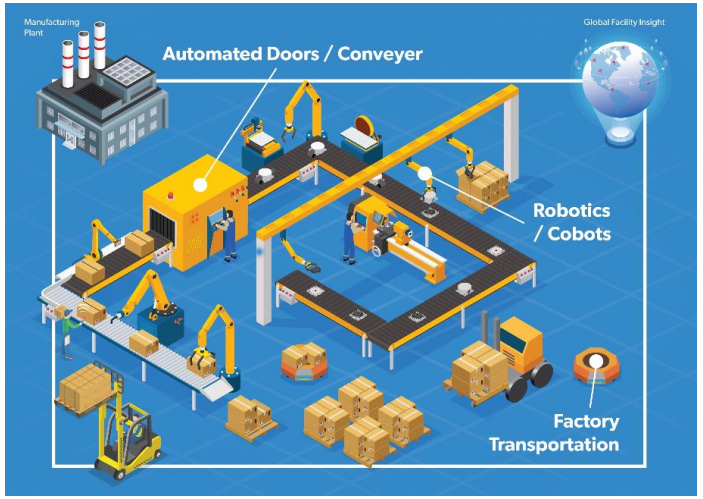


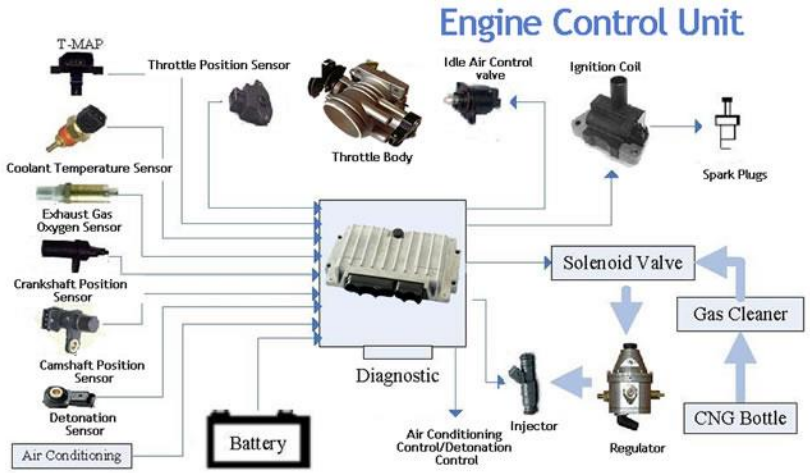
□ 임베디드 시스템에서 Hardware 및 Software의 개발과정



□ 임베디드 시스템의 활용 : 현재, 미래의 모든 분야에 직, 간접적으로 관여







KoELSA

Ⅲ. Functional Safety

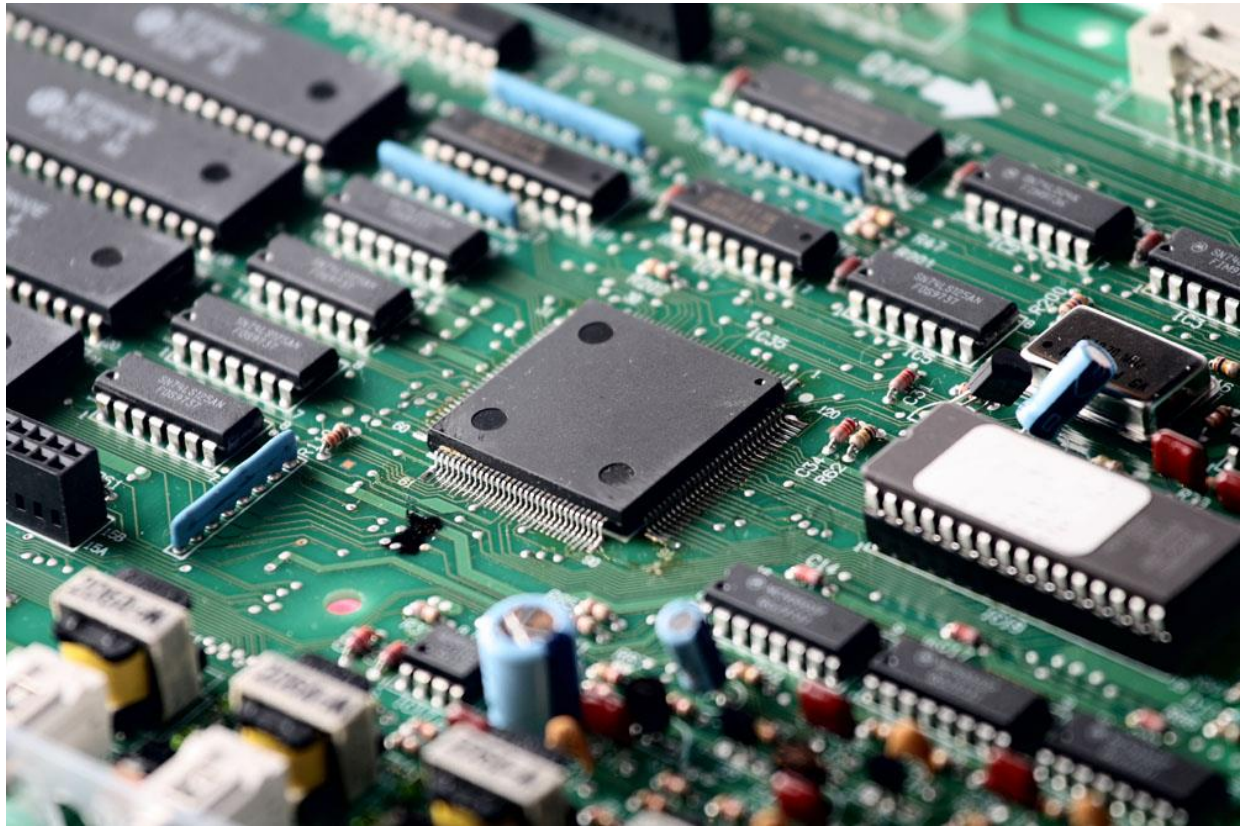
3.1. 기능안전의 개요

3.2. Elevator 및 Escalator 기능안전 개요

3.2.1. Elevator 기능안전 대상 및 적용 SIL

3.2.2. Escalator 기능안전 대상 및 적용 SIL

3.2.3. Elevator 기능안전 세부적인 요구사항



3.1 기능안전의 개요

모든 제어 시스템은 예고 없이 고장이 날 수 있다.

그런데, 안전관련 제어시스템이라면?

KoELSA

3.1. 기능안전의 개요

2012년 9월 18일 페맥스 가스시설 화재

멕시코의 천연가스시설에서 대형 화재가 발생해 인부 26명이 숨지고 46명이 다쳤으며 인근 주민들이 대피하는 사태를 빚었다. 멕시코 국영석유회사 PENEX 는 미국과 국경을 접한 북동부의 레이노사시(市)에서 19km 떨어진 곳에 있는 자사의 가스시설에서 불이 나 90분만에 진화됐다고 밝혔다.

KoELSA

3.1. 기능안전의 개요

'양치기 소년' 화재경보기에 주민들 불안감 증폭

김해령 기자 mer@kyeonggi.com | 송고시간 2020. 01. 04 10 : 09 | 댓글 0

대피하지 않는 등 '안전 불감증'... "제대로 된 화재경보기 설치해야"

수원 영통구 인계동에 있는 B 오피스텔 주민들은 지난여름부터 불이 나지 않았는데도 걸핏하면 울리는 화재 경보에 몸살을 앓고 있다. 이곳에서 6개월간 지낸 P씨(28)는 "이사 온 당일부터 지금까지 일주일에 1번, 많게는 3번 화재경보가 울린다"고 하소연했다. 이곳 관리사무소 관계자는 "보일러실에 설치된 경보기가 너무 민감하다 보니 습기 등으로도 화재 경보가 울린다"며 "화재경보기 교체를 위해 소방서와 수원시청 등에 자문을 구하고 있다"고 말했다.

인도 주정부 "5월 가스사고 LG화학 잘못"

기사입력 2020-07-07 20:14:58
기사수정 2020-07-07 20:14:56

"안전규칙 미준수"... 조사결과 발표 / "예방체계 없고 당시 경보기 고장"

▲인도 소방관들이 지난 5월 7일(현지시간) 가스 누출 사고가 발생한 남부 안드라프라데시 주 비사카파트남의 LG폴리머스인디아 공장 앞에서 산소 실린더를 들고 걸어가고 있다. 비사카파트남=AP연합뉴스

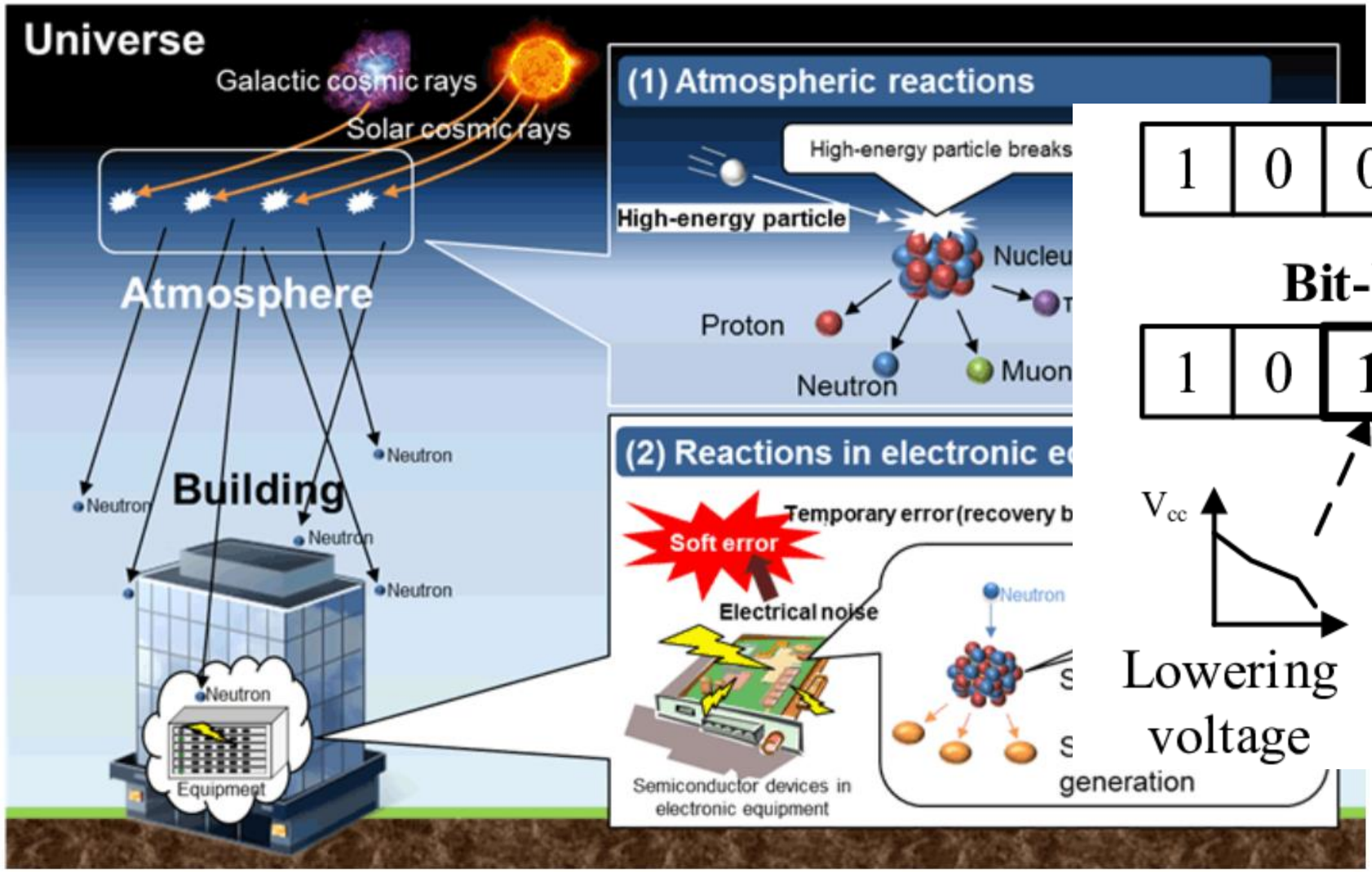
인도 남부 안드라프라데시 주정부가 지난 5월 발생한 LG폴리머스 공장의 화학가스 유출 사고에 대해 "회사의 관리 태만 과실"이라는 결론을 내렸다.

회사의 관리 태만 과실이 근본적인 문제일까요?

KoELSA

3.1. 기능안전의 개요

3.1. 기능안전의 개요



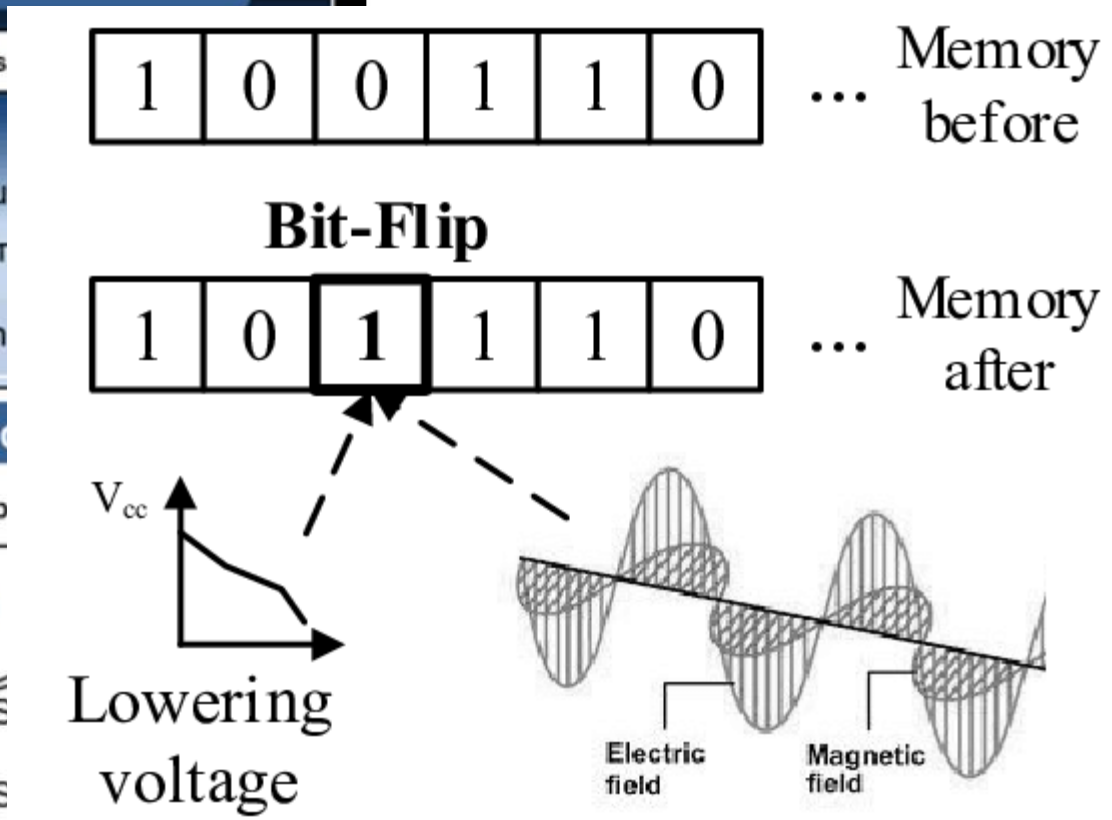


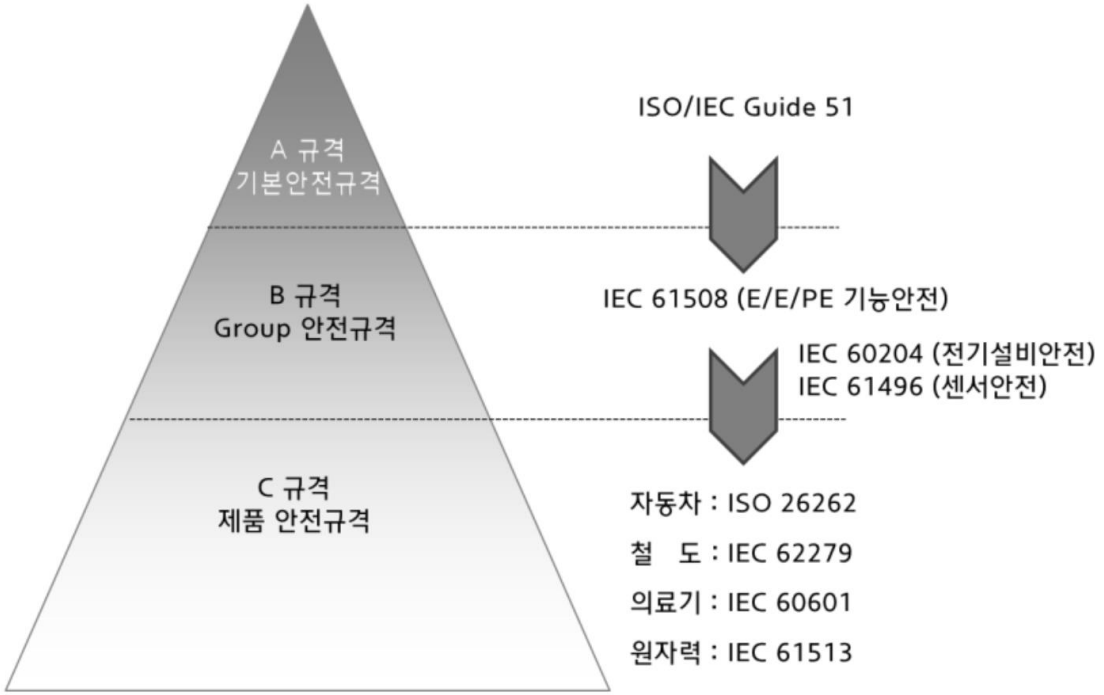
Figure 1 Soft error generation mechanism

KoELSA

기능안전 (Functional Safety)이란?

기능안전(Functional Safety)

- 안전에 대한 진화된 개념으로 IEC 61508 국제표준에서 등장한 용어
- 시스템이나 장비의 총체적인 안전의 일환으로 하드웨어 고장, 소프트웨어 오류, 운영자 오류, 그리고 환경적인 영향 등 전반에 대한 안전관리(management of safety)를 포함
- HW와 SW가 융합된 안전시스템에 대한 안전을 보장하기 위한 평가



안전(Safety)관련 국제표준

A 규격: 광범위한 제품. 프로세서 및 서비스에 적용하는 일반적인 안전측면에 대한 요구사항

B 규격: 유사한 제품에 적용할 수 있는 기능안전 측면을 포함하는 규격

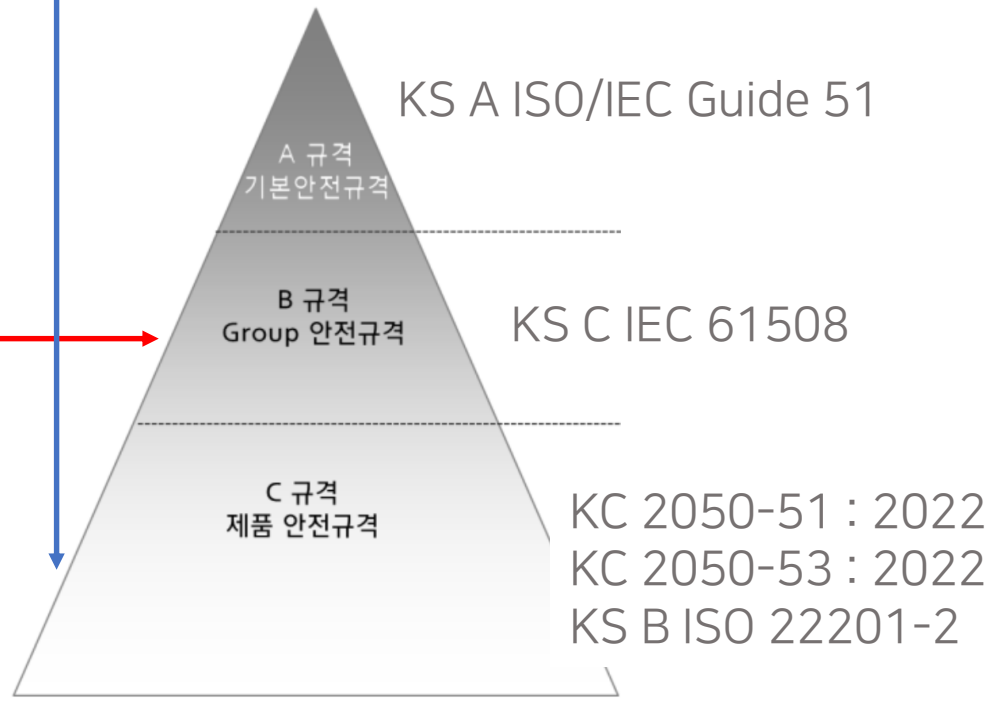
C 규격: 산업분야별로 파생되어 특정제품(자동차, 철도, 의료 기기, 원자력 등)에 대한 기능안전 규격

KoELSA

국내 승강기 Domain에서의 Functional Safety 규격의 구조

[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



KoELSA

3.1. 기능안전의 개요

SIL 이란?

1. 용어의 정리

- 안전 무결성 등급(Safety Integrity Level) : 안전 시스템의 무결성을 나타내는 통계적 기준

2. 배경

- 영국 Buncefield 연료저장소 폭발 사고(2005년 12월 11일, 월요일)

  * Buncefield Terminal : 영국에서 5번째로 큰 연료 저장소로써 총 저장능력이 7700만 리터,
    영국 자동차 연료의 5% 공급 및 Heathrow, Gatwick 공항과 항공유 파이프라인 연결

  * 피해정도 : 총 26개 탱크 중 21개 파손, 인근 주민의 강제 대피 및 화염, 연기 등으로 외출금지 명령

- 사고조사위원회(영국 HSE : Health and Safety Executive) 연료저장소의 설계 및 운영에 대한 최종제안

  * 안전성 검증요구 및 체계적인 안전 무결성 수준의 확보

  * 높은 안전 무결성을 지닌 시스템에 기반한 저장소의 오작동, 결함 등의 사전 탐지

  * 주요 저장소 및 외부 저장소의 오작동, 결함 등의 단계적 확재(Escalation) 시나리오에 대응하는 설계 및 개발

  * 높은 신뢰도를 지난 조직의 운영(Operating with high reliability organizations)

3.1. 기능안전의 개요

Buncefield, Aerial picture of fire and smoke plume
(Photographed by Chiltern Air Support Unit)

Buncefield 화재는 2005년 12월 11일 영국 하트퍼드셔주 헤멜 헴스테드 (Hemel Hempstead) M1 고속도로 근처에 위치한 허트포드셔 (Hertfordshire) 석유 저장 터미널에서 석유 저장 시설에서 발생한 주요 화재입니다.

3.1. 기능안전의 개요

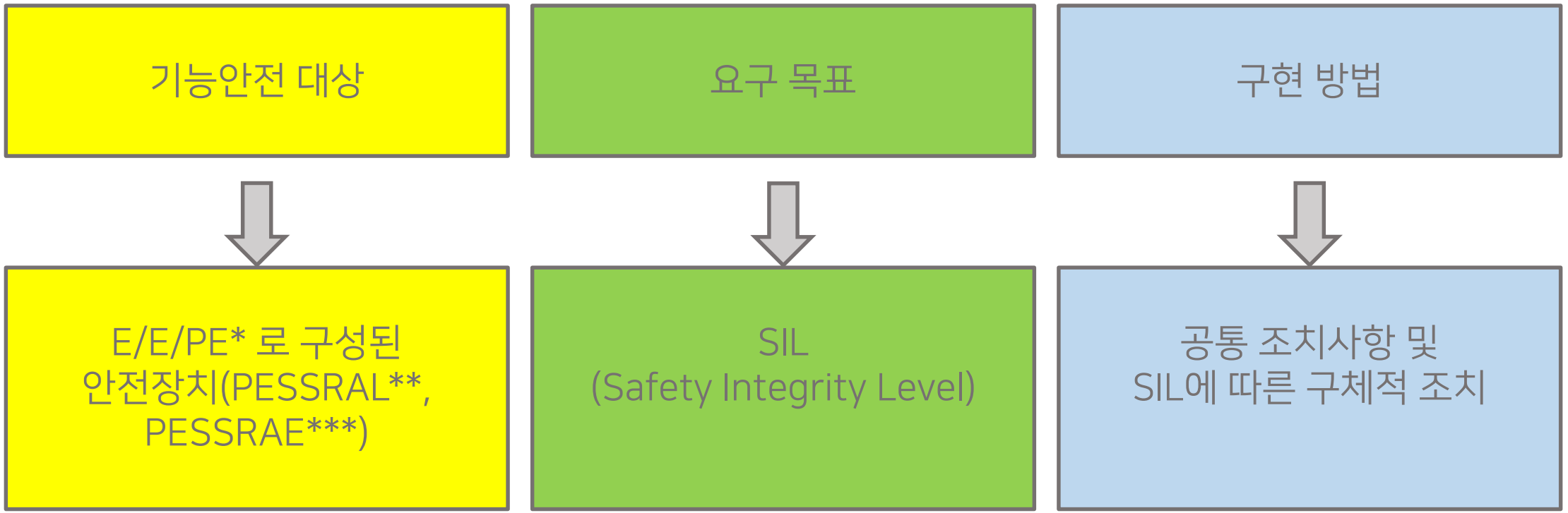
SIL 이란?

- SIL은 안전을 위해 설치되는 제어 설비의 등급을 나타내는 것으로 안전제어시스템의 무결성의 통계적 기준
- Safety Function에 의해 제공되는 위험 저감 수준을 나타내며, Safety Instrument Function(SIF)에 요구되는 성능에 대한 measurement 임
- SIL의 숫자가 높아질 수록 요구되는 안전 무결성의 수준이 높음(설계/유지/폐기에 관련된 관리의 수준 포함)
- ANSI/ISA-S84.01(ANSI: 미국표준협회)과 IEC 61508(IEC: 국제전기표준협회)에서 사용되는 기준으로, 현재 4등급으로 구분되어 있음
- SIL에 따른 고장 확률

SIL	고장확률	고요구 작동모드 안전기능의 위험측 평균고장(IEC 61508)
SIL1	10~100년 사이에 예상치 못한 고장 발생 가능	$10^{-6} \leq PFH^* < 10^{-5}$
SIL2	101~1,000년 사이에 예상치 못한 고장 발생 가능	$10^{-7} \leq PFH < 10^{-6}$
SIL3	1,001~10,000년 사이에 예상치 못한 고장 발생 가능	$10^{-8} \leq PFH < 10^{-7}$
SIL4	10,001~100,000년 사이에 예상치 못한 고장 발생 가능	$10^{-9} \leq PFH < 10^{-8}$

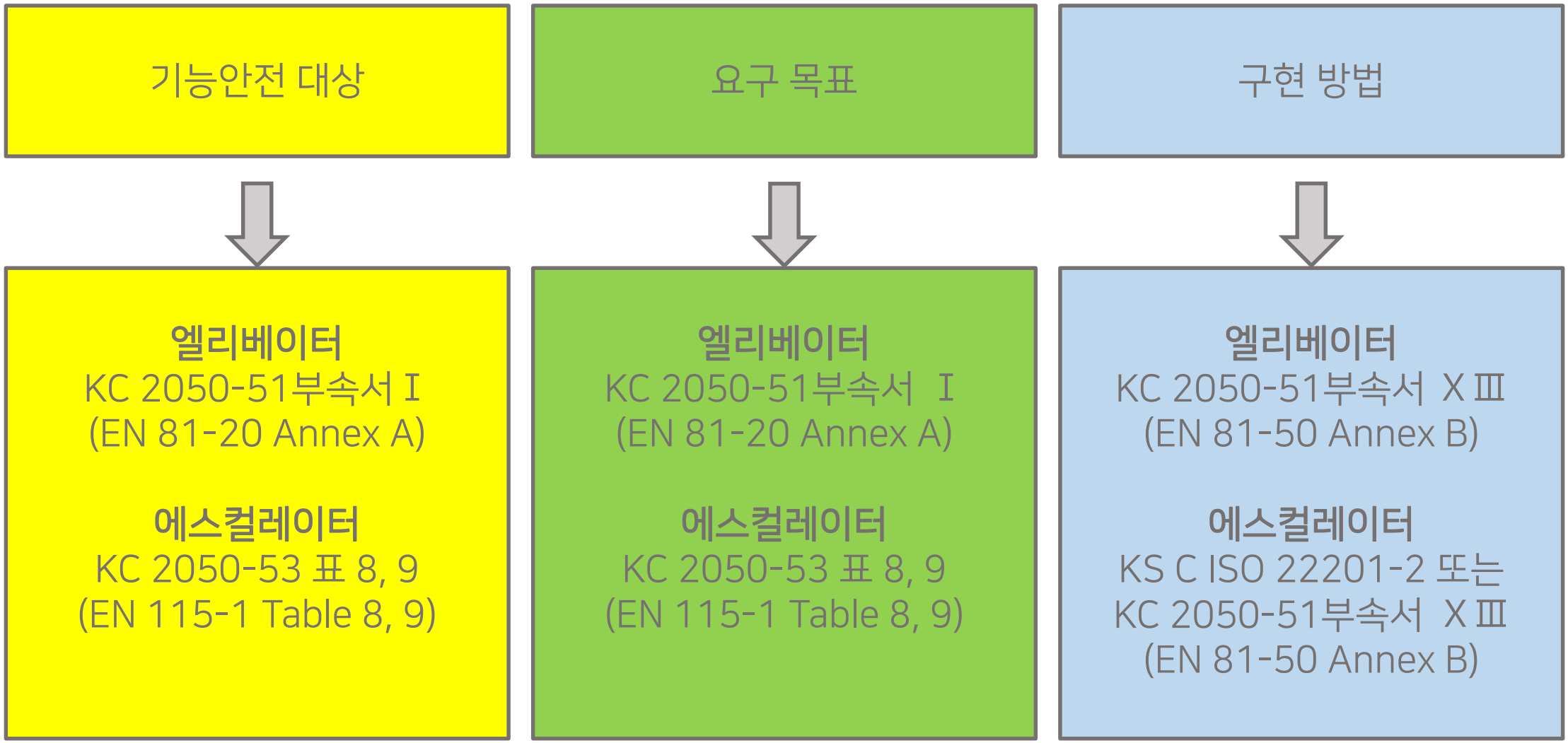
* PFH: Probability of Failure per Hour(안전기능의 위험측 고장 평균빈도)

3.2. EL 및 ES 기능안전의 개요



* E/E/PE: Electrical/Electronic/Programmable Electronic
** PESSRAL: Programmable Electronic System in Safety Related Applications for Lifts
*** PESSRAE: Programmable Electronic System in Safety Related Applications for Escalators & M/Ws

3.2. EL 및 ES 기능안전의 개요



KoELSA

3.2.1 EL 기능안전 대상 및 적용 SIL

KC 2050-51 부속서 I : 전기안전장치 목록 (EN 81-20 Annex A : List of the electric safety devices)

항목	확인 장치	최소 SIL
6.1.5.1 가)	피트 내 정지 장치	3
6.1.5.2 다)	풀리실 내 정지 장치	3
6.2.4	피트 사다리의 저장 위치 확인	1
6.3.3	비상문과 점검문의 접근 및 닫힘 상태 확인	2
6.5.3.1 다)	카문 잠금 확인	2
6.6.4.3.1 나)	기계 장치의 비활성화 상태 확인	3
6.6.4.3.3 마)	카 벽 점검문의 잠금 상태 확인	2
6.6.4.4.1 라)	피트에 접근을 허용하는 문의 열림 확인	2
6.6.4.4.1 마)	기계적인 장치의 작동에 따른 카의 비활성화 확인	3

3.2.1 EL 기능안전 대상 및 적용 SIL

KC 2050-51 부속서 I : 전기안전장치 목록 (EN 81-20 Annex A : List of the electric safety devices)

항목	확인 장치	최소 SIL
6.6.4.4.1 바)	기계적인 장치의 작동상태에서 카의 활성화 확인	3
6.6.4.5.4 가)	작업 플랫폼의 완전히 집어넣어진 위치 확인	3
6.6.4.5.5 나)	멈춤 쐐기가 완전히 집어넣어진 위치 확인	3
6.6.4.5.5 다)	멈춤 쐐기의 완전히 연장된 위치 확인	3
7.9.1	승강장문 잠금장치의 잠금 위치 확인	3
7.9.4.1	승강장문의 닫힘 위치 확인	3
7.11.2	잠금 장치가 없는 문짝의 닫힘 위치 확인	3
7.13.2	카문의 닫힘 위치 확인	3
8.6.4	카의 비상구출문 잠금 확인	2

3.2.1 EL 기능안전 대상 및 적용 SIL

KC 2050-51 부속서 I : 전기안전장치 목록 (EN 81-20 Annex A : List of the electric safety devices)

항목	확인 장치	최소 SIL
8.8 나)	카 지붕의 정지 장치	3
9.3.1 다) 2)	카 또는 균형추의 상승 확인	1
9.5.3 가)	2가닥의 로프나 체인이 있는 매다는 장치에서 로프나 체인의 1가닥이 비정상적으로 늘어남 확인	1
9.5.3 나)	포지티브 구동 및 유압식 엘리베이터의 로프 또는 체인 이완 확인	2
9.6.2 바)	보상 로프의 인장 확인	3
9.6.1 다)	튀어오름 방지장치 확인	3
10.2.1.5	카 추락방지안전장치 작동에 따른 카의 비활성화 확인	1
10.2.2.1.6 가)	과속 감지	2
10.2.2.1.6 나)	과속조절기 해제 확인	3

3.2.1 EL 기능안전 대상 및 적용 SIL

KC 2050-51 부속서 I : 전기안전장치 목록 (EN 81-20 Annex A : List of the electric safety devices)

항목	확인 장치	최소 SIL
10.2.2.1.6 다)	과속조절기 로프의 인장 확인	3
10.2.2.3 마)	안전 로프의 파단 또는 이완 확인	3
10.2.2.4.2 아)	추락방지안전장치 레버의 완전히 집어넣어진 위치 확인	2
10.5.9	멈춤 쇠 장치의 복귀 위치 확인	1
10.5.10	멈춤 쇠 장치에 에너지 분산형 완충기가 사용된 경우, 완충기가 정상 위치로의 복귀 확인	3
10.6.5	카의 상승과속방지장치 작동 확인	2
10.7.7	개문출발 감지	2
10.7.8	개문출발방지장치 작동 확인	1
12.2.2.4	완충기의 정상 위치로의 복귀 확인	3

3.2.1 EL 기능안전 대상 및 적용 SIL

KC 2050-51 부속서 I : 전기안전장치 목록 (EN 81-20 Annex A : List of the electric safety devices)

항목	확인 장치	최소 SIL
13.2.3.1가) 3)	수동핸들의 탈착 여부 확인	1
14.5.2	주 개폐기 제어	2
16.1.3	감소된 완충기 행정의 경우 구동기의 정상 감속 확인	3
16.1.4 가)	착상, 재-착상, 예비운전 확인	2
16.1.5.1.2 가)	점검운전스위치	3
16.1.5.2.3 나)	점검운전에 대한 누름 버튼 확인	1
16.1.6.1	전기적 비상운전 스위치	3
16.1.8.2	승강장문 및 카문의 접점을 위한 바이패스장치	3
16.1.11.1 라)	점검운전 조작반의 정지장치	3

3.2.1 EL 기능안전 대상 및 적용 SIL

KC 2050-51 부속서 I : 전기안전장치 목록 (EN 81-20 Annex A : List of the electric safety devices)

항목	확인 장치	최소 SIL
16.1.11.1 마)	엘리베이터 구동기의 정지장치	3
16.1.11.1 바)	비상운전 및 작동시험을 위한 패널의 정지장치	3
16.2.2.3	카에 간접적으로 연결된 장치의 인장 확인(파이널 리미트 스위치)	1
16.2.2.4	카에 간접적으로 연결된 장치의 인장 확인(파이널 리미트 스위치)	1
16.2.2.5	램에 간접적으로 연결된 장치의 인장 확인(파이널 리미트 스위치)	1
16.2.3.1 나)	파이널 리미트 스위치	1

비고 SIL 수준은 15.2.6에 설명된 PESSRAL에만 해당된다.

KoELSA

3.2.2 ES 기능안전 대상 및 적용 SIL

KC 2050-53 [표 8] - 안전장치가 감지해야 할 사항 (EN 115-1, Table 8 - Events to be detected by safety devices)

항번	설명	참조	안전장치의 수단	고장 잠금	점검모드 가능여부
가)	과속 감지	5.12.2.7.2	5.12.2.6.1 또는 5.12.2.6.2 또는 5.12.2.6.3(SIL 2)	Y	Y
나)	의도되지 않은 운행방향의 역전 감지	5.12.2.7.3	5.12.2.6.1 또는 5.12.2.6.2 또는 5.12.2.6.3(SIL 2)	Y	Y
다)	보조 브레이크의 미-작동 감지	5.12.2.7.4	5.12.2.6.1 또는 5.12.2.6.2 또는 5.12.2.6.3(SIL 1)	Y	N
라)	디딤판을 직접 구동하는 부품의 파손 또는 과도한 늘어짐 감지	5.12.2.7.5	5.12.2.6.1 또는 5.12.2.6.2 또는 5.12.2.6.3(SIL 1)	Y	Y
마)	인장장치의 움직임 감지	5.12.2.7.6	5.12.2.6.1 또는 5.12.2.6.2 또는 5.12.2.6.3(SIL 1)	Y	Y
바)	콤 끼임 감지	5.12.2.7.7	5.12.2.6.1 또는 5.12.2.6.2 또는 5.12.2.6.3(SIL 1)	N	Y
사)	연속되는 에스컬레이터 및 무빙워크의 정지 감지	5.12.2.7.8	5.12.2.6.1 또는 5.12.2.6.2 또는 5.12.2.6.3(SIL 2)	N	N
아)	손잡이 입구에서의 끼임 감지	5.12.2.7.9	5.12.2.6.1 또는 5.12.2.6.2 또는 5.12.2.6.3(SIL 1)	N	Y

3.2.2 ES 기능안전 대상 및 적용 SIL

KC 2050-53 [표 8] - 안전장치가 감지해야 할 사항 (EN 115-1, Table 8 - Events to be detected by safety devices)

항번	설명	참조	안전장치의 수단	고장 잠금	점검모드 가능여부
자)	스텝 또는 팔레트 처짐 감지	5.12.2.7.10	5.12.2.6.1 또는 5.12.2.6.2 또는 5.12.2.6.3(SIL 2)	Y	N
차)	스텝 또는 팔레트 누락 감지	5.12.2.7.11	5.12.2.6.1 또는 5.12.2.6.2 또는 5.12.2.6.3(SIL 2)	Y	N
카)	브레이크의 미-작동 감지	5.12.2.7.12	5.12.2.6.1 또는 5.12.2.6.2 또는 5.12.2.6.3(SIL 1)	Y	N
타)	손잡이의 속도 편차 감지	5.12.2.7.13	5.12.2.6.1 또는 5.12.2.6.2 또는 5.12.2.6.3(SIL 1)	N	N
파)	점검용 덮개 열림 감지	5.12.2.7.14	5.12.2.6.1 또는 5.12.2.6.2 또는 5.12.2.6.3(SIL 1)	N	N
하)	비상정지장치의 작동 감지	5.12.2.7.15	5.12.2.6.1 또는 5.12.2.6.2 또는 5.12.2.6.3(SIL 1)	N	Y
거)	수동핸들의 설치 감지	5.12.2.7.16	5.12.2.6.1 또는 5.12.2.6.2 또는 5.12.2.6.3(SIL 1)	Y	Y
너)	점검 등 유지관리 업무를 위한 정지장치 감지	5.12.2.7.17	5.12.2.6.1 또는 5.12.2.6.2 또는 5.12.2.6.3(SIL 2)	N	Y

3.2.2 ES 기능안전 대상 및 적용 SIL

KC 2050-53 [표 8] - 안전장치가 감지해야 할 사항 (EN 115-1, Table 8 - Events to be detected by safety devices)

항번	설명	참조	안전장치의 수단	고장 잠금	점검모드 가능여부
더)	점검운전 제어장치에서 정지장치의 작동 감지	5.12.2.7.18	5.12.2.6.1 또는 5.12.2.6.2 또는 5.12.2.6.3(SIL 2)	N	Y
러)	쇼핑 카트 및 수하물 카트 접근 방지를 위한 이동식 진입방지대 존재 여부 감지	5.12.2.7.19	5.12.2.6.1 또는 5.12.2.6.2 또는 5.12.2.6.3(SIL 2)	N	N

KC 2050-53 [표 9] – 전기적 차단 시퀀스 감지에 대한 요구조건
(EN 115-1, Table 9 - Requirements for detecting deviations of the electrical braking sequence)

순번	설명	참조	정지 장치의 수단	고장 잠금	점검 모드 가능여부
가)	전기적 차단 시퀀스의 시간 감지	5.12.2.9.2	5.12.2.6.2 또는 5.12.2.6.3(SIL 2)	Y	N

3.2.3 EL 기능안전 세부적인 요구 사항

KC 2050-51 부속서 XIII : 엘리베이터의 안전관련 프로그램 적용 가능한 전자시스템(PESSRAL)

[EN 81-50 Annex B Programmable electronic systems in safety related applications for lifts (PESSRAL)]

XIII.1 공통 조치

표 XIII.1 - 결함을 방지하고 감지하기 위한 공통 조치 – 하드웨어 설계

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

표 XIII.3 - 설계 및 구현 프로세스의 공통 조치

XIII.2 구체적인 조치

표 XIII.4 - SIL 1에 따른 구체적인 조치

표 XIII.5 - SIL 2에 따른 구체적인 조치

표 XIII.6 - SIL 3에 따른 구체적인 조치

❖ 각 SIL 등급에 따른 ①구조, ②처리장치, ③불변 메모리 범위, ④가변메모리 범위, ⑤입출력장치 및 통신연결을 포함한 인터페이스, ⑥클럭, ⑦프로그램 시퀀스의 요구사항과 조치방법이 기술

XIII.3 가능한 조치의 설명

표 XIII.7 - 고장 제어에 대한 가능한 조치의 설명

KoELSA

Ⅳ. Elevator/Escalator 전기안전장치와 Functional Safety

4.1. KC 2050-51(2022) 15.2 전기안전장치

4.2. KC 2050-53(2022) 5.12.2 안전장치 및 기능

4.3 Elevator 안전회로의 일반적 구성

4.4 Escalator 안전회로의 일반적 구성

4.1. 엘리베이터 전기안전장치(15.2)

□ 엘리베이터 전기안전장치 일반사항

15.2.1 일반사항

(전기안전장치 요구사항) 부속서 Ⅰ에 열거된 전기안전장치 중 하나가 작동하는 동안에 구동기 기동 방지 및 즉시 정지

(전기안전장치 구성) 다음과 같이 구성되어야 함

가) 15.2.2를 만족하는 하나 이상의 안전접점. 또는

나) 다음 중 하나 또는 그 조합으로 구성된 15.2.3을 만족하는 안전회로

1) 15.2.2를 만족하는 하나 이상의 안전접점

2) 15.2.2의 요구사항을 만족시키지 못하는 접점들

3) 부속서 XII에 따른 부품

4) 15.2.6에 따른 안전관련 응용 프로그램 작동 전자시스템

16.1.4(개문 재-착상, 예비운전), 16.1.5(점검운전), 16.1.6(전기적 비상운전), 16.1.8(승강장문 및 카 문의 바이패스)를 제외하고 안전라인은 반드시 직렬 연결

4.1. 엘리베이터 전기안전장치(15.2)

□ 안전접점의 요건

15.2.2 안전접점

최소 보호등급이 IP 4X(KS C IE C 60529)인 KS C IEC 60947-5-1, 부속서 K 및 기계적 내구성(최소 100만회 작동 주기) 보장. 또는

1. 용착 되는 경우에도 회로차단장치의 확실한 분리에 의한 작동
2. 외함의 보호등급에 따른 정격절연 전압 및 KS C IEC 60947-5-1 규정의 교류회로 AC-15, 직류회로 DC-13의 범주
   - -IP 4X(KS C IEC 60529) 이상 : 정격 절연전압 250V
   - -IP 4X(KS C IEC 60529) 미만 : 정격 절연전압 500V
3. 외함의 보호등급에 따른 공극 및 연면거리
   - -IP 4X(KS C IEC 60529) 초과 : 공극 3 mm 이상, 연면거리 3 mm 이상
   - -IP 4X(KS C IEC 60529) 이하 : 공극 3 mm 이상, 연면거리 4 mm 이상
4. 다수의 브레이크 접점의 경우 접점 분리 거리는 2 mm 이상
5. 전도체 재질 마모시에도 접점 단락 불가

4.1. 엘리베이터 전기안전장치(15.2)

□ 안전회로의 요건

15.2.3 안전회로

안전 회로의 고장분석은 센서, 신호전송경로, 전원공급장치, 안전논리회로, 안전출력을 포함한 전체 안전회로의 고장을 고려

(가) 2차 결함과 결합된 1개의 결함이 위험한 상황을 초래할 수 있는 경우, 엘리베이터는 늦어도 1차 결함요소가 관여된 다음 작동 순서에서 정지되어야 한다. 엘리베이터의 모든 추가적인 운행은 이 결함이 지속되는 동안에는 불가능해야 한다. 1차 결함 후, 엘리베이터가 상기에 기술된 순서에 의해 정지되기 전까지 2차 결함 발생의 가능성은 고려되지 않는다.

(나) 2개의 결함이 그 자체에 의해 위험한 상황을 초래하지 않으나, 3차 결함과 결합하여 위험한 상황을 초래할 수 있는 경우, 엘리베이터는 늦어도 결함 요소의 하나가 관여된 다음 작동순서에서 정지되어야 한다. 엘리베이터가 상기에 기술된 순서에 의해 정지되기 전에 위험한 상황을 초래하는 3차 결함의 가능성은 고려되지 않는다.

(다) 3개 이상의 결함이 결합될 가능성이 있는 경우, 안전회로는 다중채널과 채널의 동등한 상태를 확인하는 감시회로로 설계되어야 한다. 서로 다른 상태가 감지되면 엘리베이터는 정지되어야 한다. 2개 채널인 경우, 늦어도 엘리베이터가 재-기동하기 전에 감시회로의 기능이 점검되어야 하고 결함일 경우에는 재-기동이 불가능해야 한다.

(라) 전원공급장치가 차단된 후 전원공급장치를 복구한 경우, 다음단계의 정지가15.2.3.3가), 나) 및 다)에 의해 다시 제공되므로 엘리베이터는 정지된 위치에 유지될 필요는 없다.

(마) 이중계 회로에서 하나의 원인으로 2개 이상의 회로에 동시에 발생되는 결함의 위험을 가능한 제한 할 수 있는 조치가 취해져야 한다.

KoELSA

4.1. 엘리베이터 전기안전장치(15.2)

□ 안전회로의 요건

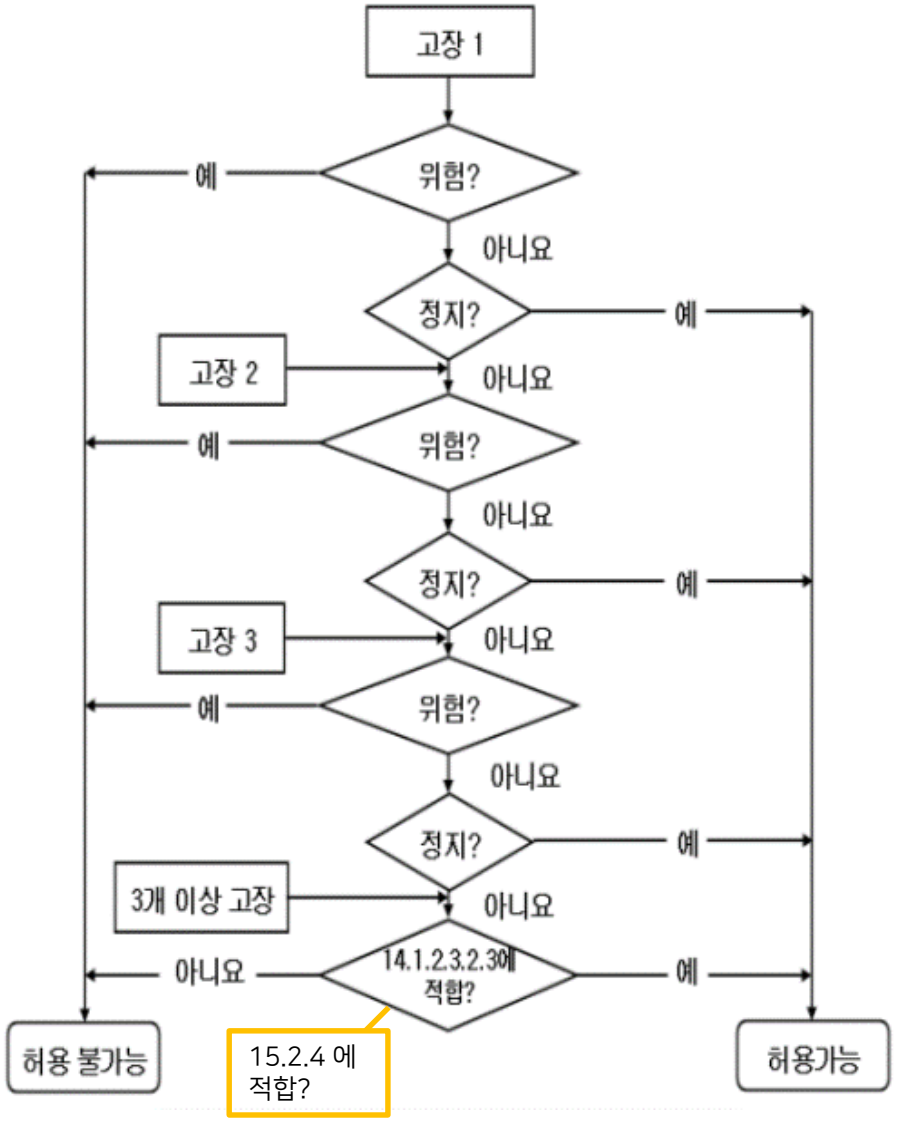
15.2.3 안전회로

안전 회로의 고장분석은 센서, 신호전송경로, 전원공급장치, 안전논리회로, 안전출력을 포함한 전체 안전회로의 고장을 고려

15.2.4 전기안전장치의 운용

1. 전기안전장치가 작동되었을 때, 전기안전장치는 구동기를 즉시 정지시키고 운전 설정을 차단 ▶**주 접촉기 차단**
2. 전기안전장치는 13.2.2.2.3가), 13.2.5 및 13.3.4.의 규정에 따라 구동기에 전원공급을 제어하는 장치에 직접 작동 ▶**주/브레이크 접촉기 차단 및 redundancy 구성**
3. 14.3.1.3에 따라 릴레이 또는 릴레이-접촉기를 사용하여 구동기의 전원공급을 제어하는 장치를 제어하는데 사용되었을 경우, 릴레이 또는 접촉기 릴레이 13.2.2.2.3가), 13.2.5 및 13.3.4.4에 규정된 것처럼 감지 ▶**작동 모니터링**

[그림 21 – 안전 회로 평가를 위한 순서도]



4.1. 엘리베이터 전기안전장치(15.2)

□ 안전관련 프로그램 적용 가능한 전자시스템(PESSRAL)

15.2.6 안전관련 프로그램 적용 가능한 전자시스템(PESSRAL)

1. 부속서 Ⅰ의 표Ⅰ.1 은 각 전기안전장치의 최소 안전 무결성 기준을 제시
2. 15.2.6에 따라 설계된 프로그램 적용 가능한 전자시스템을 포함하는 안전 회로는 15.2.3.3의 요구사항을 포함
3. PESSRAL은 별표 2의 4.8에 기술된 것과 같이 관련 안전 무결성 등급(SIL)에 대한 설계 기준을 준수
4. 안전하지 않은 프로그램 수정 방지를 위해 EPROM사용, 접근 코드 등을 사용하여 안전관련 데이터 및 PESSRAL에 대한 권한이 없는 접근을 방지하는 조치가 제공
5. PESSRAL과 안전과 관련 없는 시스템이 동일한 인쇄회로기판(PCB)를 공유하는 경우, 14.3.2(기판의 연면거리 등)의 요구사항은 두 시스템에 분리하여 적용된다.
6. 하지만, PESSRAL과 안전과 관련 없는 시스템(프로그램)이 동일한 하드웨어를 공유하는 경우, PESSRAL의 규정을 만족
7. 내장 시스템 또는 외부 도구에 의해 PESSRAL의 고장 상태를 식별
8. 외부 도구가 특별한 도구인 경우, 설치 현장에서 이용 가능
9. PESSRAL은 별표 2에 따라 안전성이 입증

4.1. 엘리베이터 전기안전장치(15.2)

□ 안전관련 프로그램 적용 가능한 전자시스템(PESSRAL)

[별표 2] (엘리베이터 휠체어리프트) 제어반 안전기준(KC1030-01 : 2022)

4.8 프로그램 가능 전자시스템(PESSRAL)의 설계 규칙

1. 프로그램 가능 전자시스템(PESSRAL)은 별표 22의 부속서 XⅢ의 표 XⅢ.1, XⅢ.2 및 XⅢ.3에 기술된 모든 SIL에 공통적인 안전 기능의 최소 요건을 준수
2. SIL의 1, 2 및 3에 요구되는 구체적인 조치는 각각 별표 22의 부속서 XⅢ의 표 XⅢ.4, XⅢ.5 및 XⅢ.6 를 참조
   또한, KS B ISO 22201-1을 참조

비고 별표 22의 표 XⅢ.1부터 XⅢ.6까지에 기술된 KS C IEC 61508-7은 KS C IEC 61508-2 및 KS C IEC 61508-3의 관련 요구사항을 나타낸다.

KoELSA

4.2. 에스컬레이터 안전장치 및 기능(5.12.2)

□ 에스컬레이터 안전장치 및 기능

5.12.2.1 개요

[표 7 - 안전 제어 시스템 구현을 위한 요구조건]

순번	설명	참조
가)	안전장치의 기능	5.12.2.2
나)	안전장치의 감시	5.12.2.3
다)	안전장치에 대한 전원공급	5.12.2.4
라)	안전장치 작동	5.12.2.5
마)	안전장치의 수단	5.12.2.6
바)	안전장치가 감지해야 할 사항	5.12.2.7 (표 8)
사)	고장 잠금 기능	5.12.2.8
아)	전기적 차단 시퀀스 감지 기능	5.12.2.9 (표 9)

4.2. 에스컬레이터 안전장치 및 기능(5.12.2)

□ 에스컬레이터 안전장치 기능

15.2.1 일반사항

(안전장치 요구사항) 표 8에 열거된 안전장치는 정지를 시작하고 5.12.3.9에 따른 재-기동을 방지

(안전장치 구성) 다음과 같이 구성되어야 함

가) 5.12.2.6.1을 만족하는 하나 이상의 안전스위치 및/또는

나) 부속서 II에 따른 전자 부품의 고장 배제를 고려한 5.12.2.6.2 를 만족하는 고장 안전회로 및/또는

다) 5.12.2.6.1에 따른 안전관련 전기, 전자 및 프로그램 가능한 전자장치(E/E/PE)

점검모드 경우의 전기안전장치(5.12.3.13), 고장 배제조건(부속서 II)에 부합한 모니터링을 위한 연결을 제외하고 안전라인은 직렬 연결

4.2. 에스컬레이터 안전장치 및 기능(5.12.2)

□ 안전 스위치의 요건

5.12.2.6.1 안전 스위치

1. 용착 되는 경우에도 회로차단장치의 확실한 분리에 의한 작동
2. 외함의 보호등급에 따른 정격절연 전압 및 KS C IEC 60947-5-1 규정의 교류회로 AC-15, 직류회로 DC-13의 범주
   - -IP 4X(KS C IEC 60529) 이상 : 정격 절연전압 250V
   - -IP 4X(KS C IEC 60529) 미만 : 정격 절연전압 500V
3. 외함의 보호등급에 따른 공극 및 연면거리
   - -IP 4X(KS C IEC 60529) 미만 : 공극 3 mm 이상, 연면거리 4 mm 이상
4. 다수의 브레이크 접점의 경우 접점 분리 거리는 2 mm 이상
5. 전도체 재질 마모시에도(파편이) 접점 단락 불가

4.2. 에스컬레이터 안전장치 및 기능(5.12.2)

□ 안전관련 프로그램 적용 가능한 전자시스템(PESSRAL)

[별표 2] (엘리베이터 휠체어리프트) 제어반 안전기준(KC1030-01 : 2022)

4.8 프로그램 가능 전자시스템(PESSRAL)의 설계 규칙

1. 프로그램 가능 전자시스템(PESSRAL)은 별표 22의 부속서 XⅢ의 표 XⅢ.1, XⅢ.2 및 XⅢ.3에 기술된 모든 SIL에 공통적인 안전 기능의 최소 요건을 준수
2. SIL의 1, 2 및 3에 요구되는 구체적인 조치는 각각 별표 22의 부속서 XⅢ의 표 XⅢ.4, XⅢ.5 및 XⅢ.6 를 참조
   또한, KS B ISO 22201-1을 참조

비고 별표 22의 표 XⅢ.1부터 XⅢ.6까지에 기술된 KS C IEC 61508-7은 KS C IEC 61508-2 및 KS C IEC 61508-3의 관련 요구사항을 나타낸다.

KoELSA

4.2. 에스컬레이터 안전장치 및 기능(5.12.2)

□ 고장안전회로의 요건

5.12.2.6.2 고장안전회로

5.12.2.6.2.1 5.12.1.2에서 나타나는 어떠한 고장도 그 자체에 의해 위험한 상황을 유발 시키지 않아야 된다.

5.12.2.6.2.2 더욱이 아래와 같은 조건은 5.12.1.2.2의 예상되는 고장에 적용된다.

2차 결함과 결합된 1개의 결함이 위험한 상황을 초래할 수 있는 경우, 에스컬레이터 또는 무빙워크는 결함 요소가 관여했던 다음 작동 순서가 발생할 때까지 정지되어야 한다. 에스컬레이터 및 무빙워크가 상기에 기술된 순서에 의해 정지되기 전까지 2차 결함으로 위험한 상황이 초래될 가능성은 고려되지 않는다. 1차 결함을 유발한 부품의 오작동이 상태변화에 의해 감지될 수 없는 경우 적절한 수단이 5.12.3.2에 따라 늦어도 에스컬레이터 또는 무빙워크가 재-기동될 때 고장을 감지하고 운행을 방지하는 것이 보장되어야 한다. 고장안전회로의 MTBF (mean time between failures)는 2.5년 이상이어야 한다. 이 시간은 3개월의 기간 내에 각 에스컬레이터 또는 무빙워크가 5.12.3.2에 따라 적어도 한번 재-기동되어 상태변화가 있었을 것이라는 가정 하에 결정되었다.

5.12.2.6.2.3 3차 결함과 결합된 2개의 결함이 위험한 상황을 초래할 수 있는 경우, 에스컬레이터 또는 무빙워크는 결함 요소 중 하나가 관여했던 다음 작동 순서가 발생할 때까지 정지되어야 한다.

에스컬레이터 및 무빙워크가 상기에 기술된 순서에 의해 정지되기 전까지 3차 결함으로 위험한 상황이 초래될 가능성은 고려되지 않는다.

2개의 결함을 유발한 부품의 오작동이 상태변화에 의해 감지될 수 없는 경우 적절한 수단이 5.12.3.2에 따라 늦어도 에스컬레이터 또는 무빙워크가 재-기동될 때 고장을 감지하고 운행을 방지하는 것이 보장되어야 한다.

고장 안전회로의 MTBF (mean time between failures)는 2.5년 이상이어야 한다.

이 시간은 3개월의 기간 내에 각 에스컬레이터 또는 무빙워크가 5.12.3.2에 따라 적어도 한번 재-기동되어 상태변화가 있었을 것이라는 가정 하에 결정되었다.

5.12.2.6.2.4 3개 이상의 고장 결합은 다음과 같은 경우에 무시해도 된다.

가) 고장 안전회로가 2개 이상의 채널로 구성되어 있고 제어회로에 의해 동등한 상태가 감시되어 진다. 제어회로는 5.12.3.2에 따라 에스컬레이터 또는 무빙워크의 재-기동전에 확인되어 진다.(부속서 III 참조), 또는

나) 고장 안전회로는 3개 이상의 채널로 구성되어 있고 제어회로에 의해 동등한 상태가 감시되어 진다.

가) 또는 나)의 기준을 만족하지 않은 경우, 고장분석을 중단하는 것은 허용되지 않고 5.12.2.6.2.3에 유사하게 지속되어야 한다. 실행을 위하여 5.11.2.2가 적용되어야 한다.

5.12.2.6.2.5 고장안전회로의 설계 및 평가는 그림 III.1과 같아야 한다.

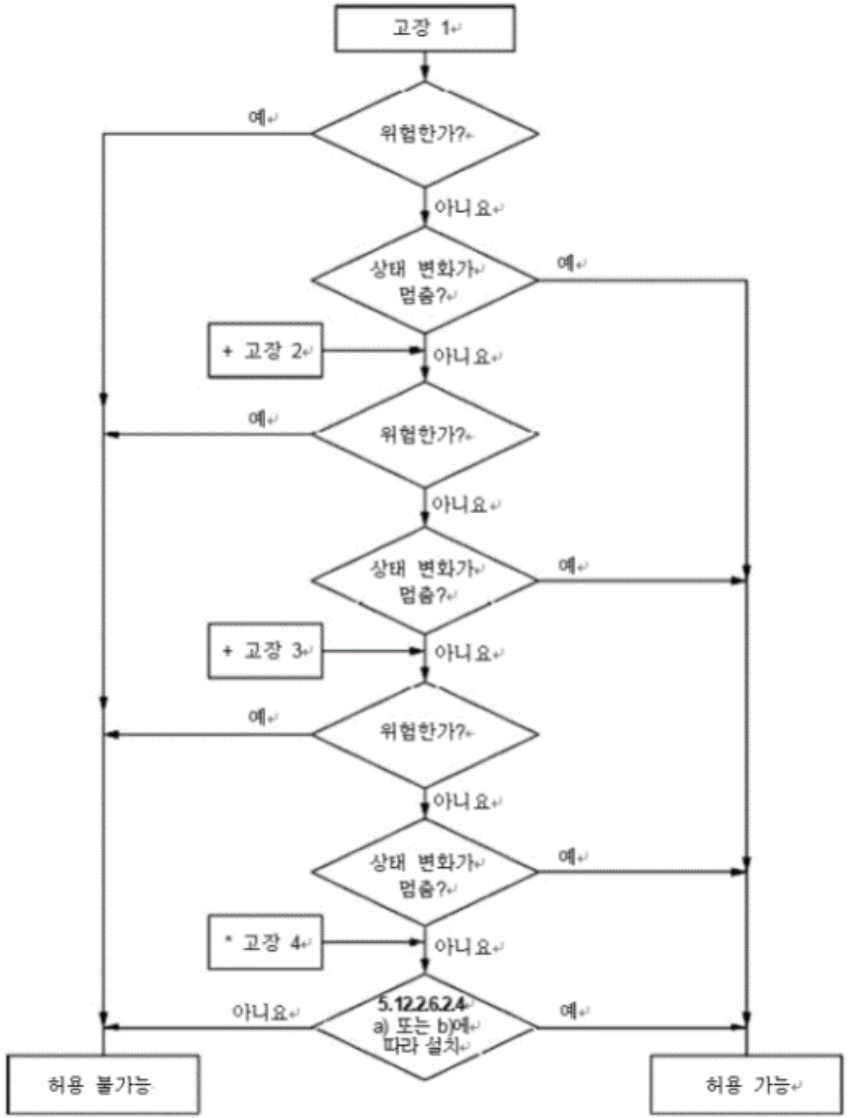
KoELSA

4.2. 에스컬레이터 안전장치 및 기능(5.12.2)

□ 고장안전회로의 요건

부속서 Ⅲ 고장안전회로 초안 작성 및 평가

[그림 Ⅲ.1 – 고장안전회로의 초안 작성과 평가를 위한 흐름도]



4.2. 에스컬레이터 안전장치 및 기능(5.12.2)

□ 안전관련 프로그램 적용 가능한 전자시스템(PESSRAE)

5.12.2.6.3 안전 관련 전기, 전자 및 프로그램 가능한 전자장치(E/E/PE)

안전 관련 전기, 전자 및 프로그램 가능한 전자장치(E/E/PE)를 KS B ISO 22201-2의 기준에 따라 설계해야 한다.

전기, 전자 및 프로그램 가능한 전자장치(E/E/PE) 및 비 안전 관련 시스템이 동일한 하드웨어를 공유하는 경우, 전기, 전자 및 프로그램 가능한 전자장치(E/E/PE)에 대한 기준을 충족시켜야 한다.

5.12.2.10 제어반은 별표 16에 따라 안전성이 입증되어야 한다.

[별표 16] (에스컬레이터) 제어반 안전기준(KC1040-11 : 2022)

5.3 프로그램 작동 전자시스템(PESSRAE)에 대한 기능 및 안전성 시험

프로그램 작동 전자시스템(PESSRAE)에 대한 기능 및 안전성 시험은 별표 2, IEC 62061 또는 KS B ISO 22201-2에 따라 이뤄져야 한다.

KoELSA

(참고) EL 안전제어기 신기술 동향 1 : Kubler

(참고) EL 안전제어기 신기술 동향 2 : ELGO

감사합니다.

KoELSA
Korea Elevator Safety Agency

Electrical Team Leader
TaeWon Ha

80 Seungganggi-gil, Namsang-myeon, Geochang-gun, Gyeongsangnam-do, Korea
T +82 55-940-9943
M +82 10-4416-7414
F +82 55-940-9959
E topgun@koelsa.or.kr