한국의 엘리베이터/에스컬레이터에 대한 기능안전 평가

ktl 한국산업기술시험원
Korea Testing Laboratory

한국승강기안전공단
KOREA ELEVATOR SAFETY AGENCY

기능안전

기능안전

• E/E/PE 안전관련 시스템 및 기타 위험성 감소 조치들의 올바른 기능에 의존하는 EUC 및 EUC 제어 시스템과 관련된 전반적인 안전의 일부분 [IEC 61508-4]

EUC 제어 시스템
예: 에스컬레이터 제어장치

제어되는 설비 (EUC)
예: 에스컬레이터

E/E/PE 안전관련 시스템
안전 기능
PESSRAE
PESSRAL

위험요인
예: 의도되지 않은 운행 방향의 역전

+

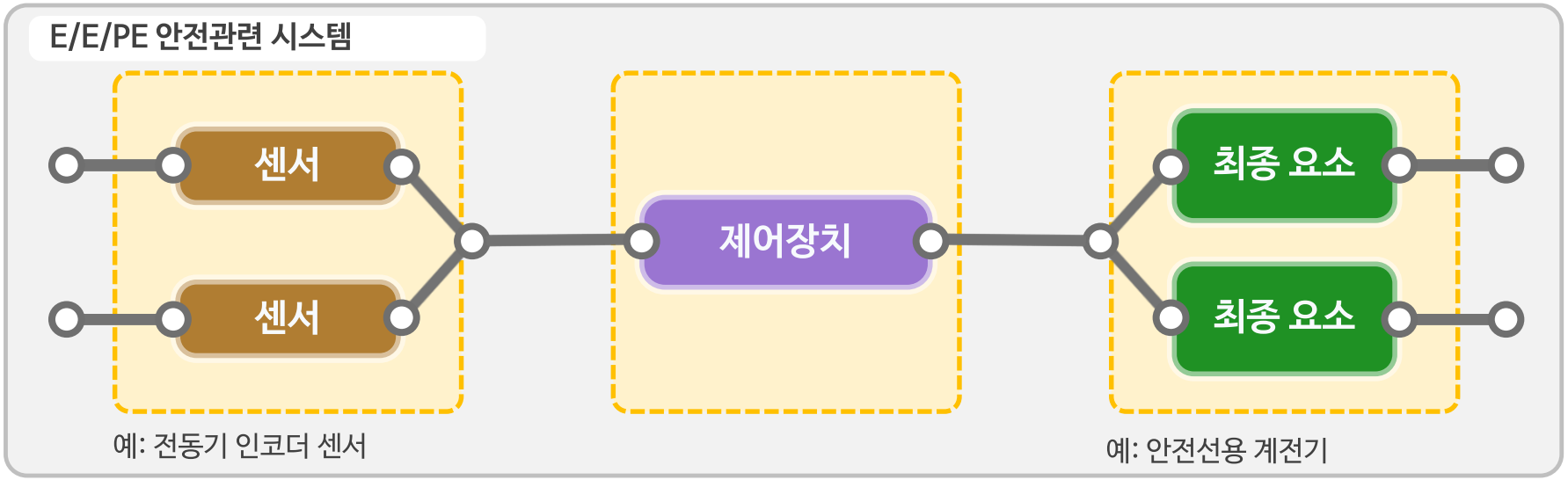
상황/사건
예: 아침 혼잡 시간대

피해
신체적 부상

기능안전(FS)에서 안전 보장 방법

안전 기능

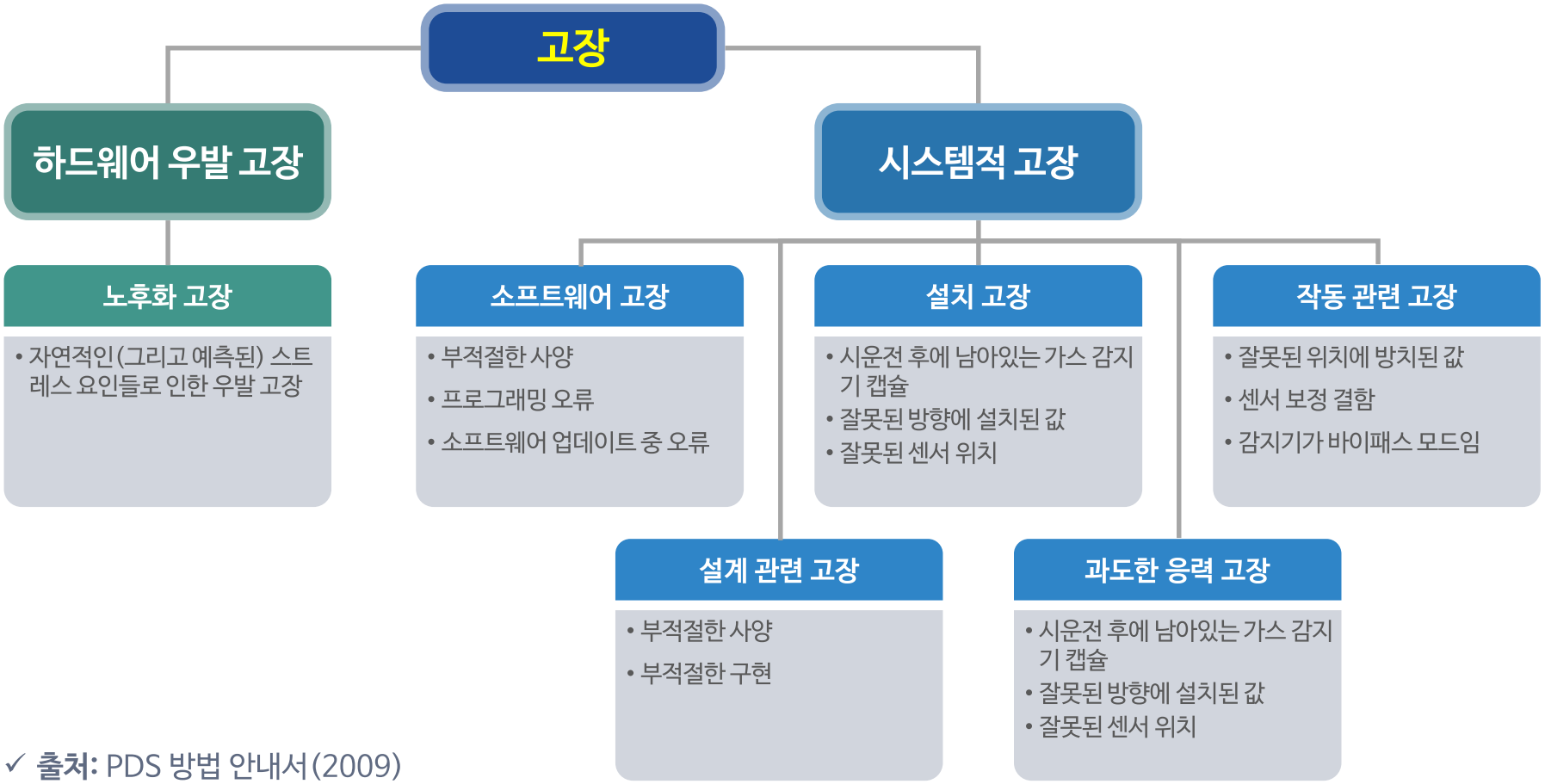
• 특정 위험한 사건과 관련하여 EUC에 대한 안전 상태를 달성하거나 유지하도록 의도된 E/E/PE 안전관련 시스템 또는 기타 위험성 감소 조치에 의해 구현되어야 하는 기능 [IEC 61508-4]



고려 요인

고장

• 요구되는 기능을 제공하거나 요구되는 방식 이외의 어떠한 방식으로 기능 단위의 동작을 제공할 수 있는 기능의 중지



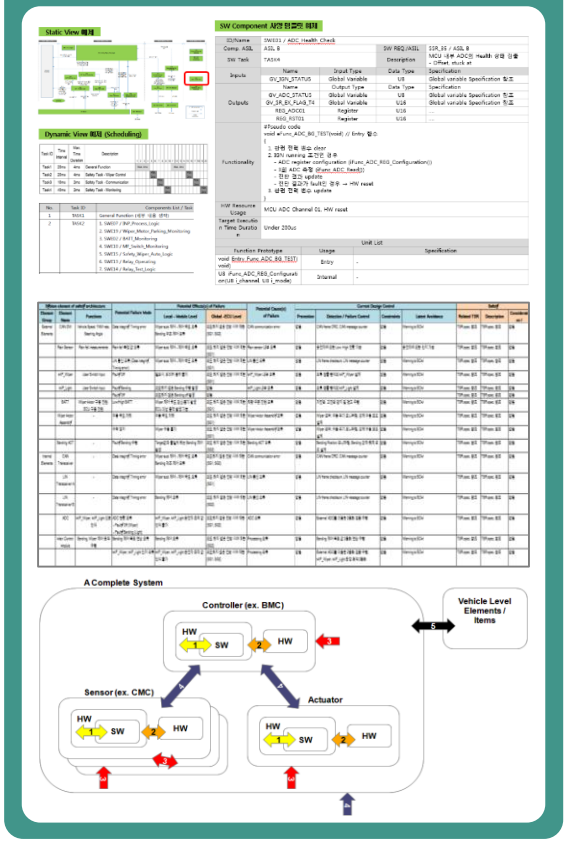
✓ **출처:** PDS 방법 안내서(2009)

고장 대처 방법

예방/통제

- 적절한 기술 및 조치를 통해 표준에서 요구되는 안전 수명주기와 같은 시스템적 조치의 적용
- 센서 자가 진단, 프로그램 흐름 모니터링 및 데이터 유효성 검사와 같은 진단 기능의 구현

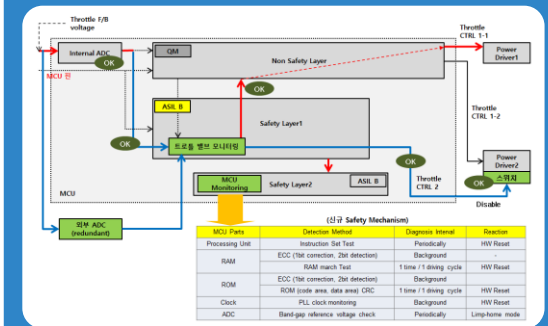
시스템적 조치
설계/검증/유효성 검사



시스템적 고장

하드웨어 우발 고장

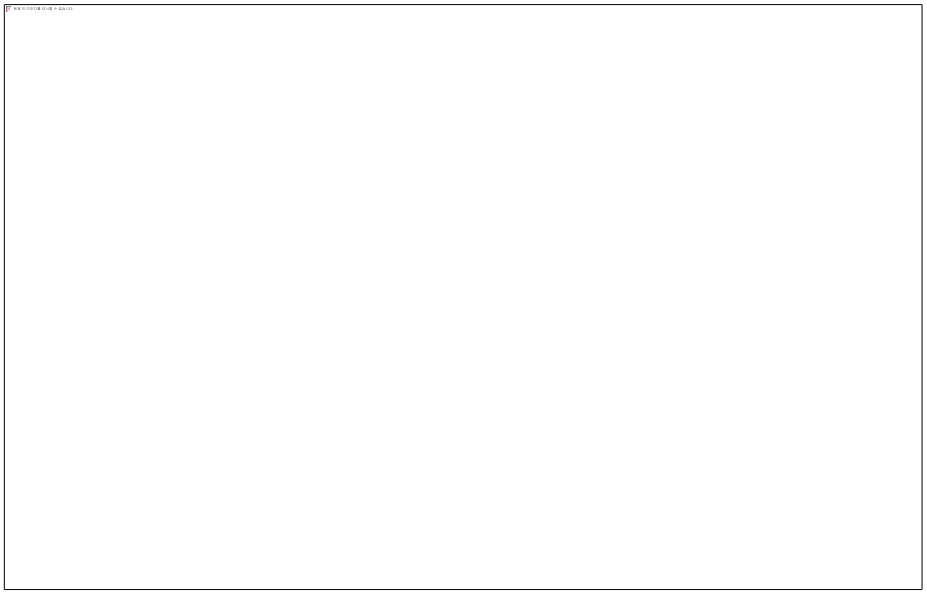
기술 솔류션
예: 진단



국가 표준의 내용(1)

시스템적 조치(간소화된 안전 수명주기)

- 안전 기능의 개발 과정을 감사하는 방법
- ISO 8100-2 부속서 B(PESSRAL)를 고려한 최소 안전 수명주기
- 작업물에 어떤 내용이 필요한가?



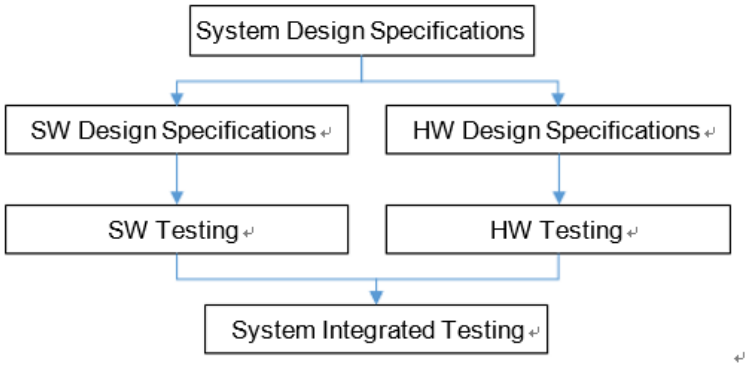


Figure 3 — Assumed Safety Life Cycle

4.3.2.2.1 Document Review

4.3.2.2.1.1 Specifications of the safety function shalled be evaluated. The existence and accuracy of the following items must be evaluated.

a) Input and output interface of safety functions
NOTE It can be checked through the I/O interface of the connector end of the safety device.

b) The standards and defined safety conditions that cause the operation of the safety function

c) The interface between components consisting the safety functions
NOTE It can be expressed in a logical form, taking into account the implementation of hardware and software performing safety functions. These components and interfaces should be represented in the system architecture.

d) Time constraints of safety functions
NOTE The validation of time constraints shall be supported by reasonable grounds, such as test data.

국가 표준의 내용(2)

기술적 조치들을 이해하는 방법(안전분석)

- 시스템적 안전 무결성과 하드웨어 안전 무결성을 평가하는 방법에 대한 설명
- 핵심은 예시를 통해 안전분석을 수행하는 방법이다.

A.1.2.3 Hardware circuit diagram

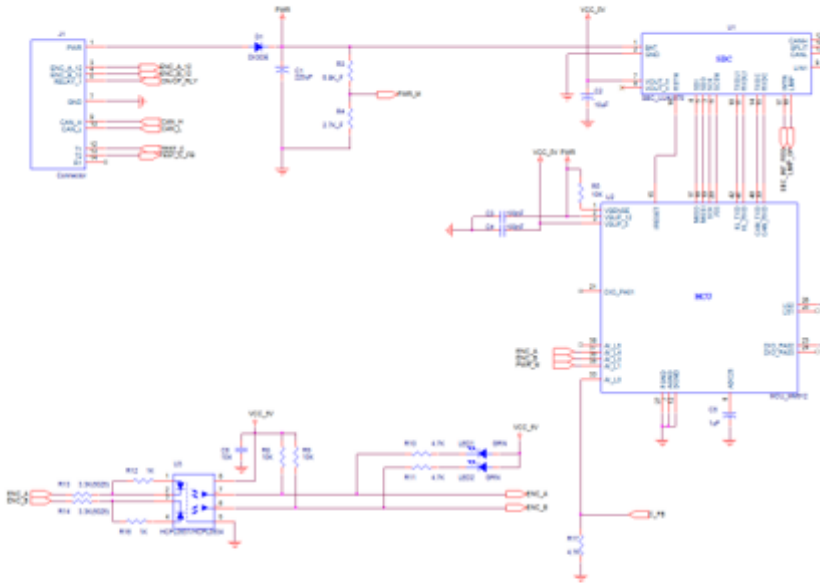


Figure A.2 — Circuit diagram

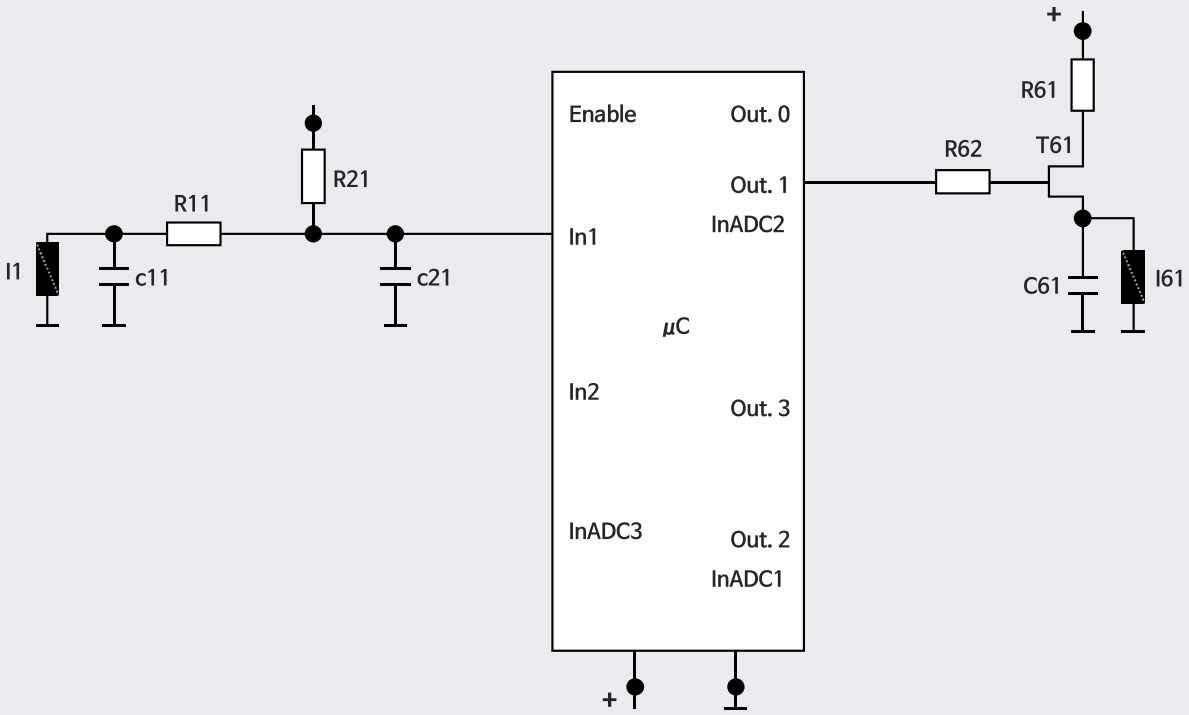
NOTE The circuit diagram in Figure A.2 is drawn for the analysis example of hardware architecture metrics, and it is abstracted and simplified to a certain level. Thus, technical operation and deployability shall not be considered in this diagram.

Table A.5 — Analysis of failure effect and single-point failure

Failure rate and mode					Failure effect		Analysis on single-point failure	
Hardware block	Identifier	Element form	Element function	Failure mode	Failure effect (excluding diagnostic function)	Possibility of malfunction of safety function	Possibility of single-point failure	Response · diagnostic function
Power interface	D1	Diode	Respond to reverse polarity.	Short	Lost the reverse polarity response function.	X		
				Open	ECU lost power supply. → MCU lost power. → Open relay.	X		
	C1	220uF/ electrolysis	Remove power noise.	Short	ECU lost power supply.	X		
				Open	BATT power noise → Unstable operation of SBC and MCU	O	O	DG01 / Monitor power.
System basis	C2	10uF/ electrolysis	Stabilize 5V power.	Short	Impossible to operate MCU. Impossible to supply power to multi-function switch. Emergency control function is unavailable.	X		
				Open	Unstable 5V power → Unstable operation of MCU	O	O	Response measure is unavailable. (Need to monitor 5V power.)
	R1	60 ohm/chip metal film	Stabilize CAN bus voltage.	Open	CAN bus voltage stabilization is lost. → Possible to cause CAN communication error.→ Impossible to receive speed information.	X		
				Drift	There is no failure effect.	X		

예: 초기 설계

전(前)



- **안전 기능: 과속 감지**
- **안전무결성등급(SIL):** SIL 2
- **안전 상태: 안전밸브I61** 개방

예: 초기 설계에 대한 안전분석

안전 기능(SIL2)

부품명	고장률/FIT	계산 시 안전관련 부품을 고려해야 하는가?	고장 모드	고장 모드 분포	진단의 부재 시 안전 기능을 위반할 가능성이 있는 고장 모드인가?	λ_S	λ_D	진단은 고장 모드가 안전 목표를 위반하는 것을 방지할 수 있는가?	안전 목표 위반에 관한 고장 모드 커버리지	λ_{Dd} (FIT)	λ_{Du} (FIT)
R11 비고 1, 비고 6, 비고 7	2	예	open	90%	X		1.8				1.8
			closed	10 %	X		0.2				0.2
WD	20	예	Out. Stuck at 1	50 %		20					
			Out. Stuck at 0	50 %							
μC	100	예	모두 (위험)	50 %	X		50				50
			모두(안전)	50 %		50					
									∑		52

고장률 합계 122 FIT

안전관련 합계 122 FIT

비-안전관련 합계 0 FIT

안전측 고장비율 = 1−(52/122) = 57.4 %

불만족

잔존 고장률 = 52 FIT

건축상의 제한

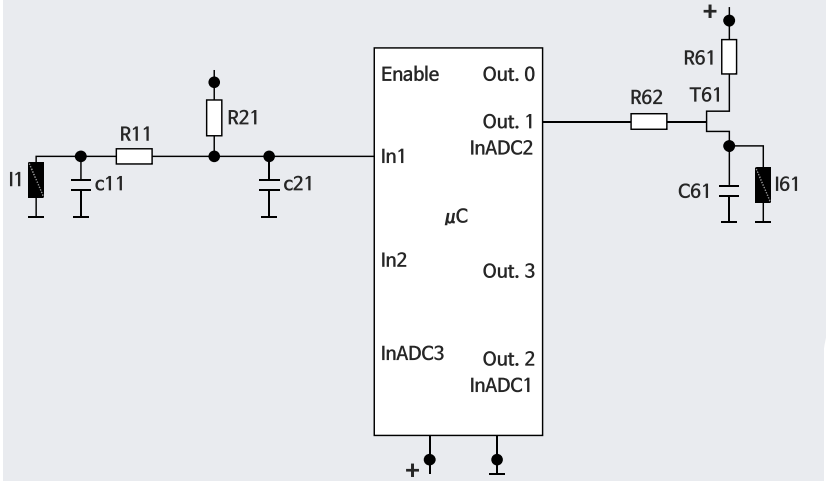
안전측 고장 비율	하드웨어 고장 허용범위		
	0	1	2
<60%	N/A	SIL1	SIL2
60% ≤ 90%	SIL1	SIL2	SIL3
90% ≤ 99%	SIL2	SIL3	SIL4
≥ 99%	SIL3	SIL4	SIL4

하드웨어 우발 고장의 정량화

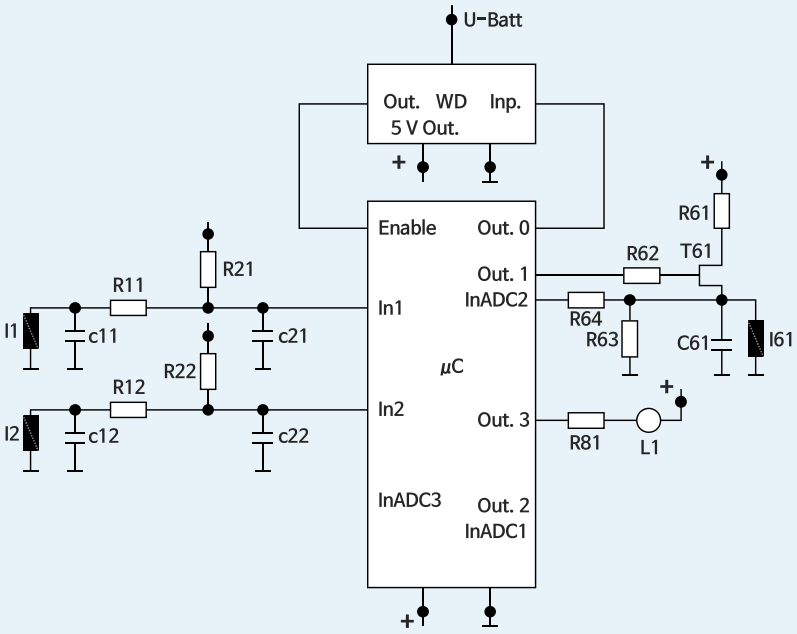
안전무결성등급(SIL)	안전 기능의 위험한 고장의 평균 빈도 [h^{-1}] (PFH)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

예: 설계 개선

전



후

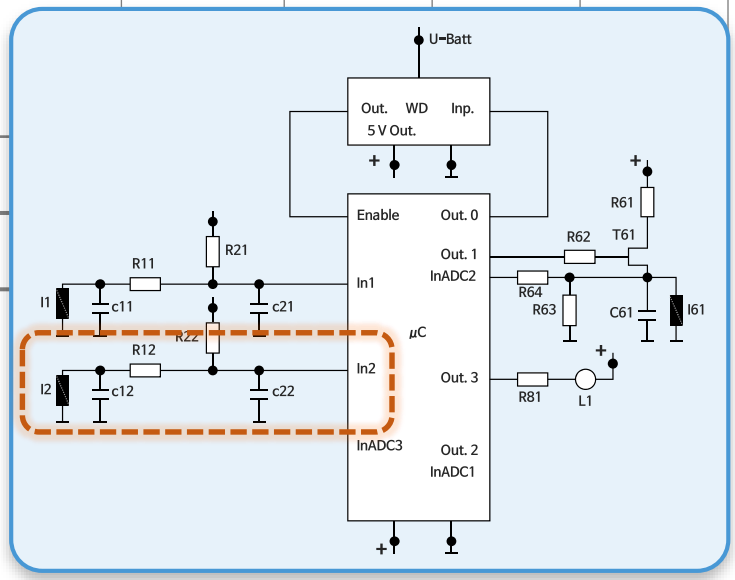


- **안전 기능: 과속 감지**
- **안전무결성등급(SIL):** SIL 2
- **안전 상태: 안전밸브I61** 개방
- **진단 2 :** 센서 I1, I2의 펄스 값은 마이크로컨트롤러에 의해 판독된다. 휠 속도는 센서들에 의해 제공되는 평균값을 사용하여 계산된다. 안전 메커니즘 2는 두 입력을 비교한다.
- 진단 4 : 안전밸브 피드백 모니터링

예: 개선된 설계에 대한 안전분석

안전 목표 2

부품명	고장률/FIT	계산 시 안전관련 부품을 고려해야 하는가?	고장 모드	고장 모드 분포	진단의 부재 시 안전 기능을 위반할 가능성이 있는 고장 모드인가?	λ_S	λ_D	진단은 고장 모드가 안전 목표를 위반하는 것을 방지할 수 있는가?	안전 목표 위반에 관한 고장 모드 커버리지	λ_{Dd} (FIT)	λ_{Du} (FIT)
R11 비고 1, 비고 6, 비고 7	2	예	open	90%	X		1.8	진단 2	99 %	1.782	0,018
			closed	10 %	X		0.2		99 %	0.198	0,002
WD	20	예	Out. Stuck at 1	50 %		20					
			Out. Stuck at 0	50 %							
µC	100	예	모두 (위험)	50 %	X						
			모두 (안전)	50 %		50					



고장률 합계 122 FIT

안전관련 합계 122 FIT

비-안전관련 합계 0 FIT

안전측 고장 비율

= 1-(5,02/122) = 95.8 %

ktl 한국산업기술시험원
Korea Testing Laboratory

경청해 주셔서 감사합니다!

Q&A

ktl 한국산업기술시험원
Korea Testing Laboratory

한국승강기안전공단
KOREA ELEVATOR SAFETY AGENCY