Functional Safety Assessment for Lift/Escalator in Korea

ktl 한국산업기술시험원
Korea Testing Laboratory

한국승강기안전공단
KOREA ELEVATOR SAFETY AGENCY

Functional Safety

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 [IEC 61508-4]

EUC control system

Ex. Escalator controller

Equipment Under Control (EUC)

Ex. Escalator

E/E/PE safety related system

Safety function

PESSRAE
PESSRAL

Hazard
ex. Unintended reversal

Situation / Event
ex. Morning rush hour

Harm
physical injury

The way to ensure safety in FS

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 [IEC 61508-4]

Functionality

"What has to be done"

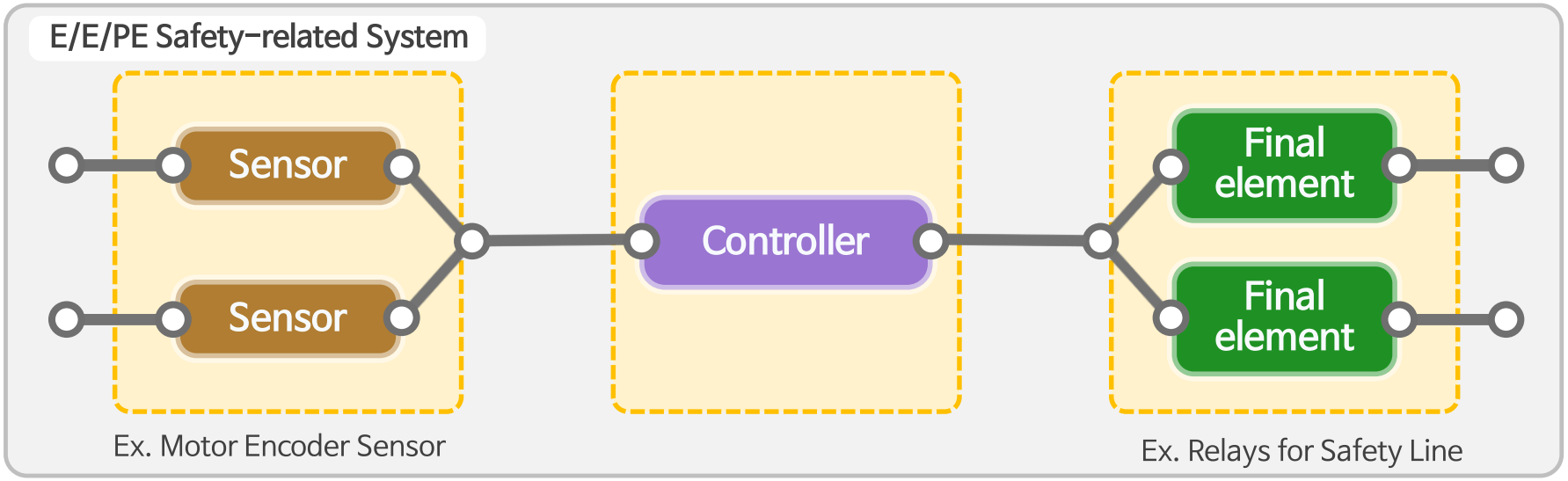
Determined from the hazard analysis

Safety function

Safety integrity

"Safety performance"

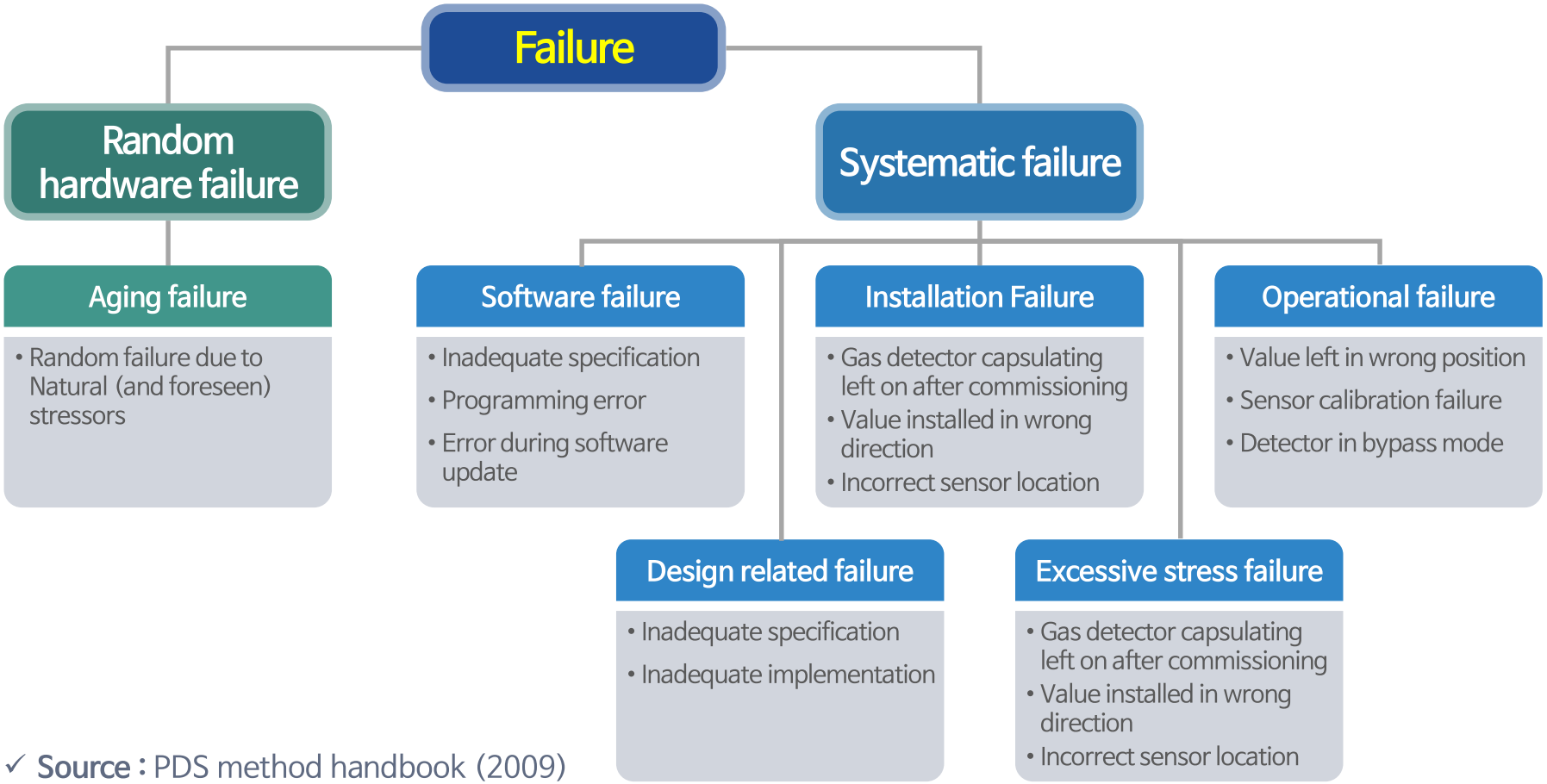
Determined from the risk assessment



Consideration Factors

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



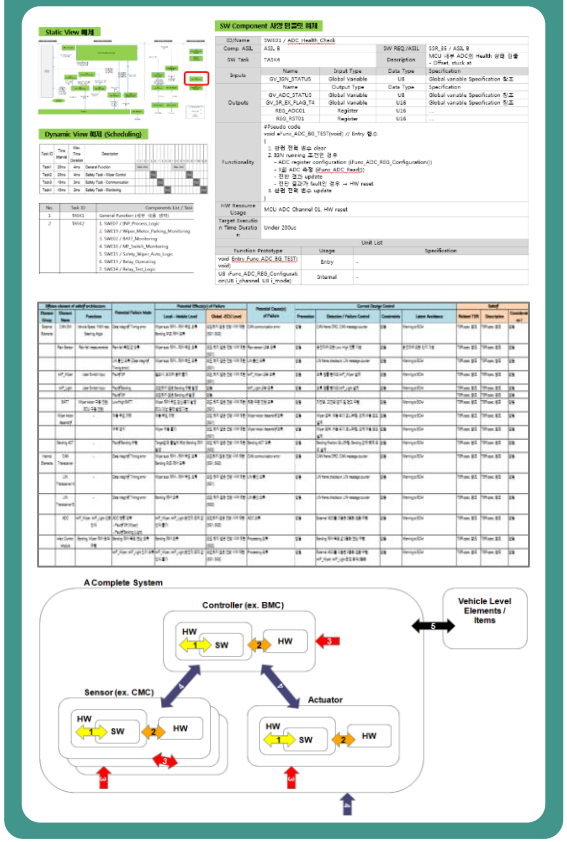
✓ **Source :** PDS method handbook (2009)

The way to deal with Failures

Prevention / Control

- Applying systematic measures such as safety life cycle required in standards with proper techniques and mea
- Implementing diagnostic functions such as a sensor self-test, program flow monitoring and data validation

Systematic Measures Design/Verification/Validation

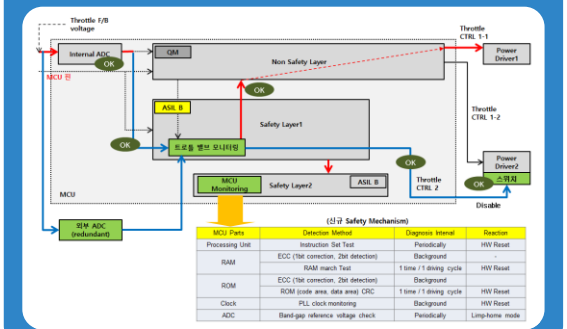


Systematic Failure

Failure Category

Random HW Failure

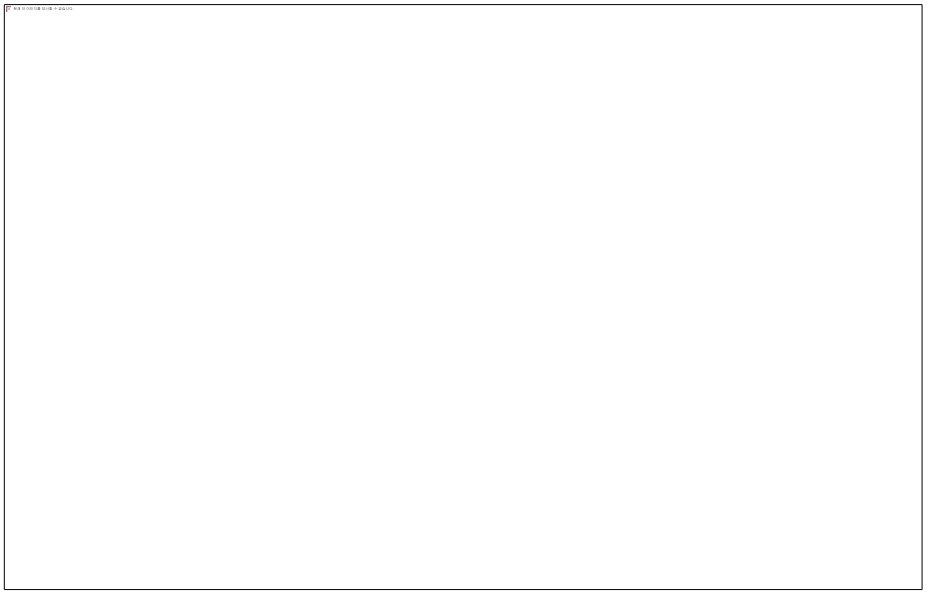
Technical solution Ex. diagnostics



Contents of National Standard (1)

Systematic Measures (Simplified Safety Life Cycle)

- The way to audit development process of safety function.
- A minimum safety life cycle considering ISO 8100-2 annex B (PESSRAL)
- What contents are needed in work product



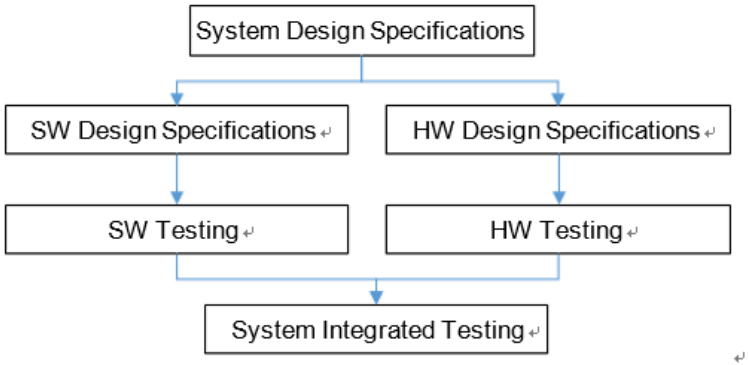


Figure 3 — Assumed Safety Life Cycle

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.

Contents of National Standard (2)

How to figure out technical measures (Safety Analysis)

- Description of he way to evaluate systematic safety integrity and hardware safety integrity
- The key point is how to do safety analysis with examples.

A.1.2.3 Hardware circuit diagram

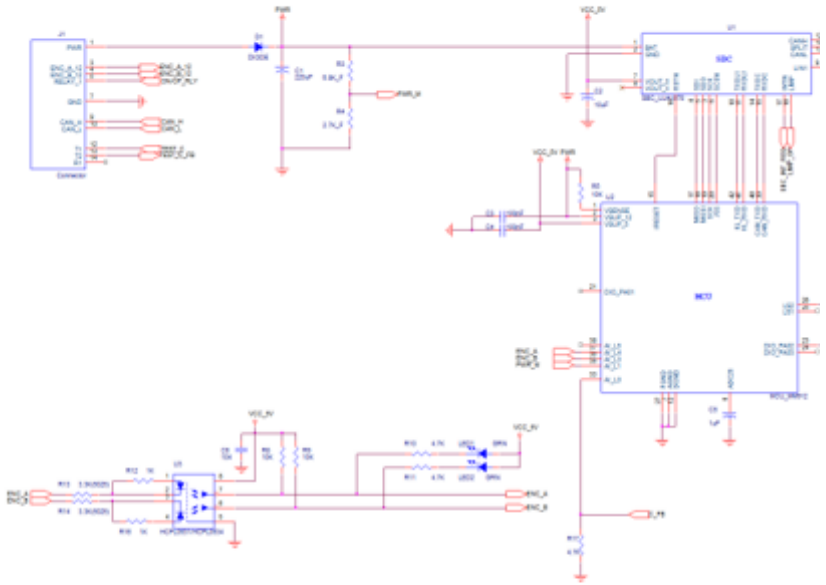


Figure A.2 — Circuit diagram

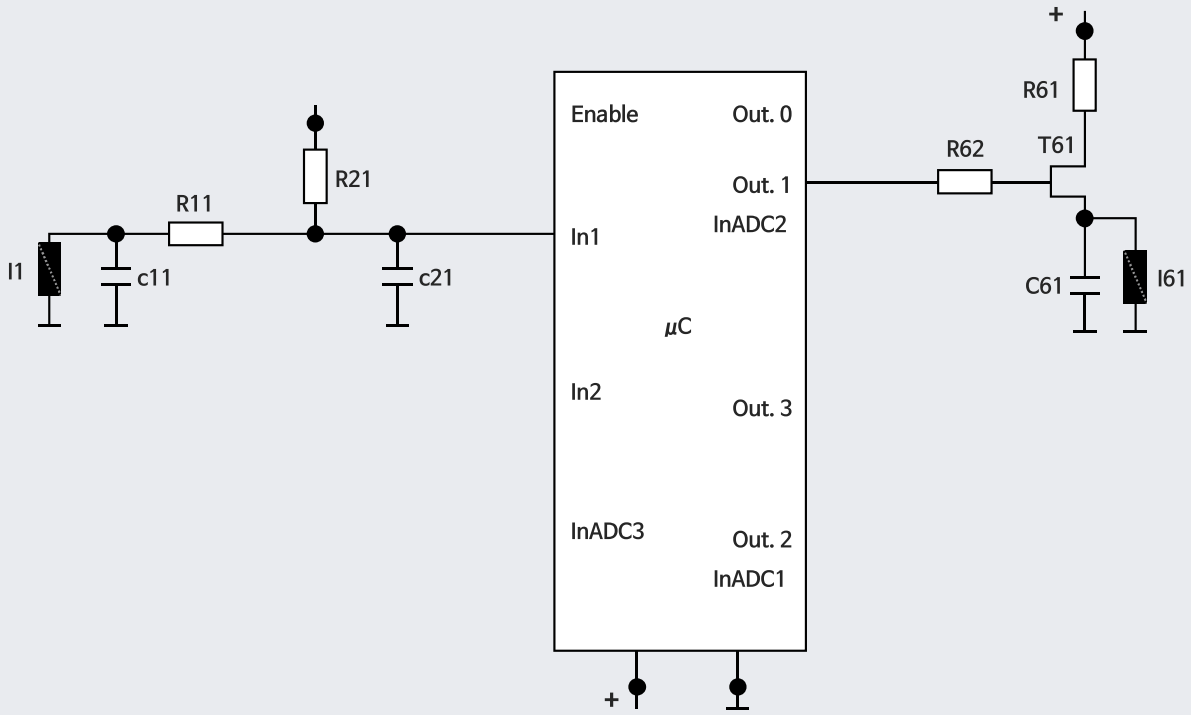
NOTE The circuit diagram in Figure A.2 is drawn for the analysis example of hardware architecture metrics, and it is abstracted and simplified to a certain level. Thus, technical operation and deployability shall not be considered in this diagram.

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		

Ex. Initial Design

Before



- **Safety Function : Overspeed detection**
- **SIL:** SIL 2
- **Safe state: safe valve I61** open

Ex. Safety Analysis for Initial Design

Safety Function (SIL2)

Component Name	Failure rate/FIT	Safety-related component to be considered in the calculation?	Failure Mode	Failure mode distribution	Failure mode that has the potential to violate the safety function in absence of Diagnostic?	λ_S	λ_D	Diagnostic allowing to prevent the failure mode from violating the safety goal?	Failure Mode coverage wrt. violation of safety goal	λ_{Dd} (FIT)	λ_{Du} (FIT)
R11 NOTE 1, NOTE 6 and NOTE 7	2	YES	open	90%	X		1.8				1.8
			closed	10 %	X		0.2				0.2
WD	20	YES	Out. Stuck at 1	50 %		20					
			Out. Stuck at 0	50 %							
µC	100	YES	All (Dangerous)	50 %	X		50				50
			All (Safe)	50 %		50					
										∑	52

Total failure rate 122 FIT

Total Safety-Related 122 FIT

Total Non Safety-Related 0 FIT

Safe Failure Fraction = 1−(52/122) = 57.4 %

Not satisfied

Residual Failure Rate = 52 FIT

Architectural Constraints

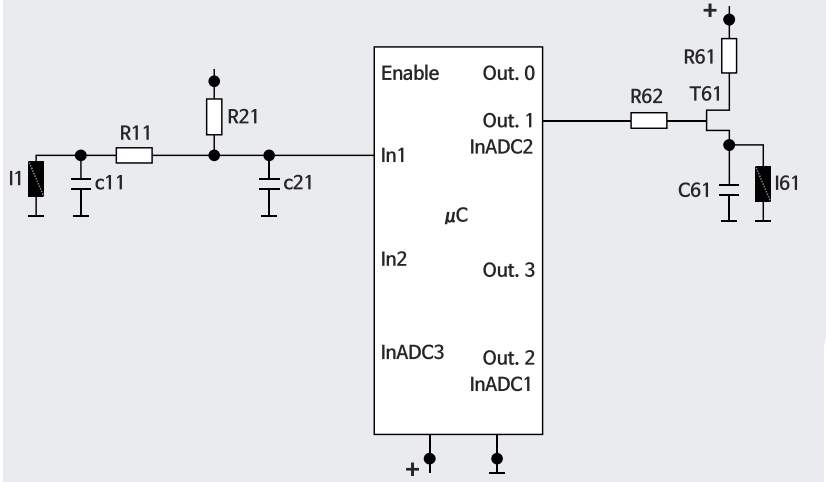
Safe Failure Fraction	Hardware Fault Tolerance		
	0	1	2
<60%	N/A	SIL1	SIL2
60% ≤ 90%	SIL1	SIL2	SIL3
90% ≤ 99%	SIL2	SIL3	SIL4
≥ 99%	SIL3	SIL4	SIL4

Quantify Random HW failure

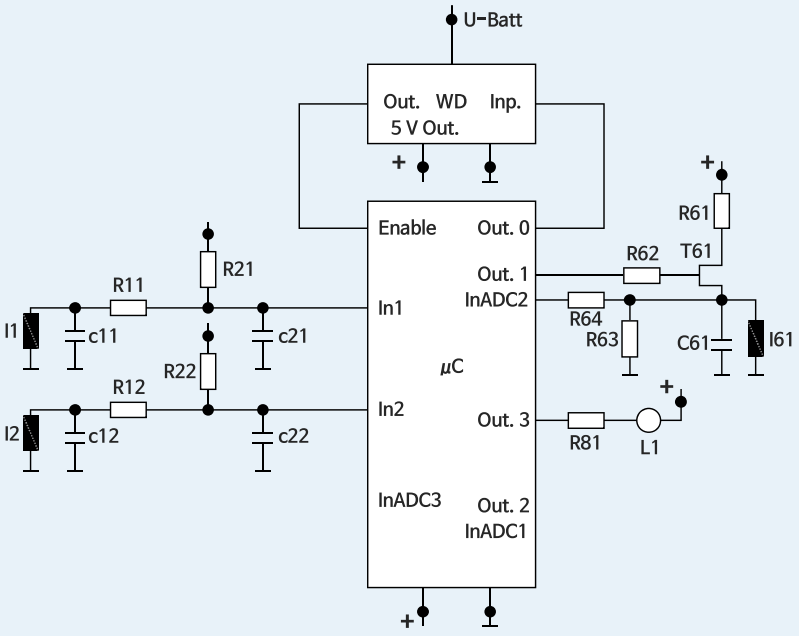
Safety integrity Level (SIL)	Average frequency of a dangerous failure of the safety function [h^{-1}] (PFH)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Ex. - Design Improvement

Before



After

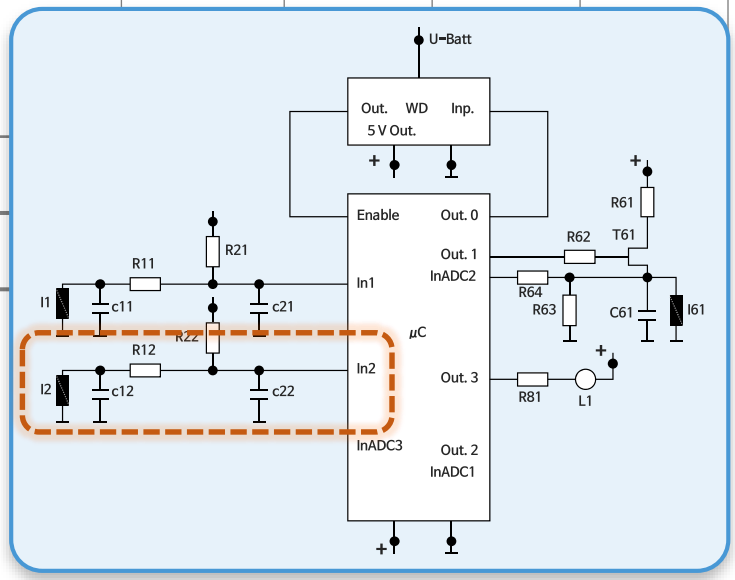


- **Safety Function : Overspeed detection**
- **SIL:** SIL 2
- **Safe state: safe valve I61** open
- **Diagnostic 2 :** The values of sensors I1, I2 pulses are read by the microcontroller. The wheel speed is computed using the mean value given by the sensors. The safety mechanism 2 compares both inputs.
- Diagnostic 4 : Safe Valve Feedback Monitoring

Ex. Safety Analysis for Refined Design

Safety goal 2

Component Name	Failure rate/FIT	Safety-related component to be considered in the calculation?	Failure Mode	Failure mode distribution	Failure mode that has the potential to violate the safety function in absence of Diagnostic?	λ_S	λ_D	Diagnostic allowing to prevent the failure mode from violating the safety goal?	Failure Mode coverage wrt. violation of safety goal	λ_{Dd} (FIT)	λ_{Du} (FIT)
R11 NOTE 1, NOTE 6 and NOTE 7	2	YES	open	90%	X		1.8	Diagnostic 2	99 %	1.782	0,018
			closed	10 %	X		0.2		99 %	0.198	0,002
WD	20	YES	Out. Stuck at 1	50 %		20					
			Out. Stuck at 0	50 %							
µC	100	YES	All (Dangerous)	50 %	X						
			All (Safe)	50 %		50					



Total failure rate 122 FIT

Total Safety-Related 122 FIT

Total Non Safety-Related 0 FIT

Safe Failure Fraction

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

ktl 한국산업기술시험원
Korea Testing Laboratory

Thank you for your attention!

Q&A

ktl 한국산업기술시험원
Korea Testing Laboratory

한국승강기안전공단
KOREA ELEVATOR SAFETY AGENCY