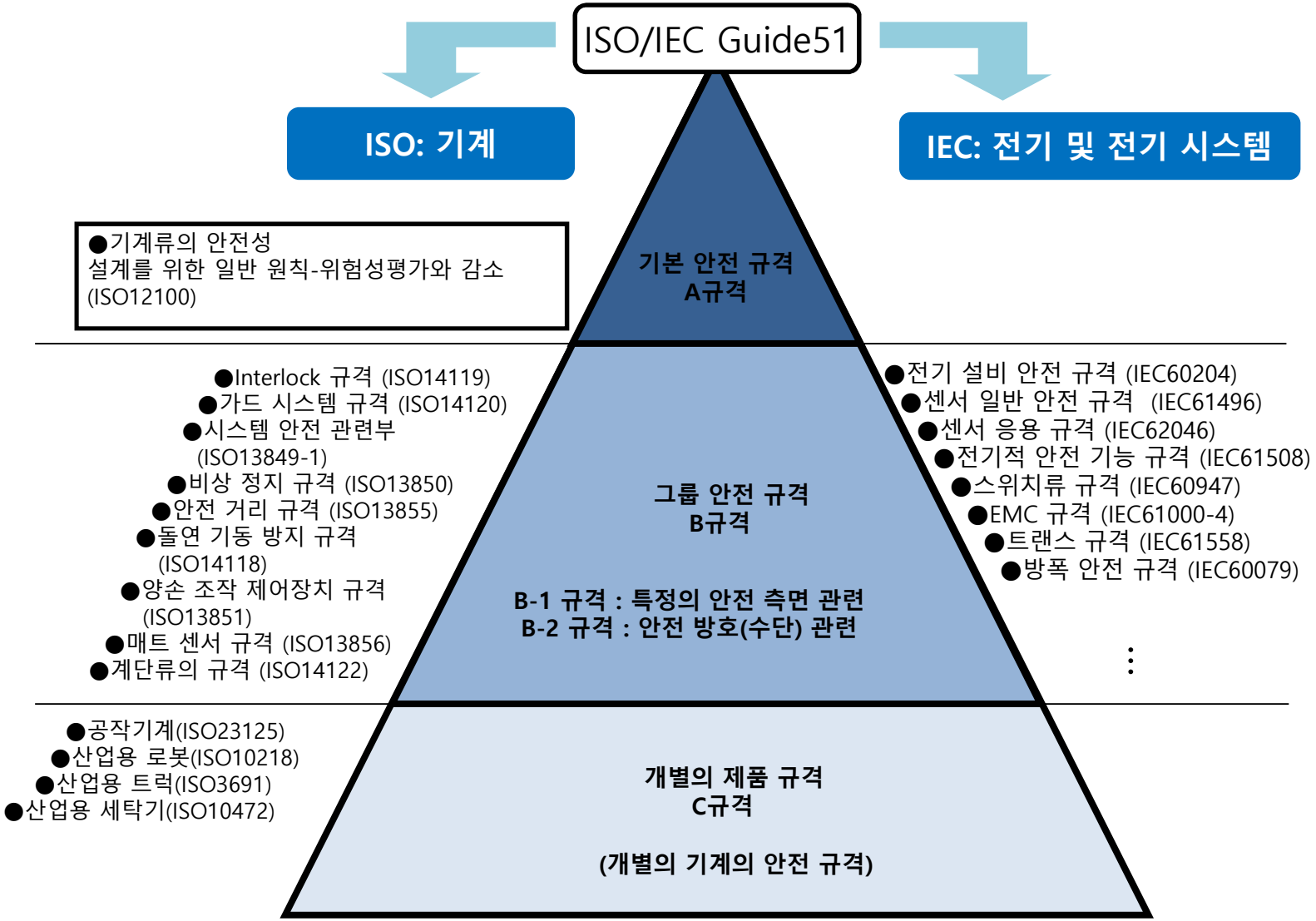
로봇 시스템 안전 대응 위험성평가
(ISO 12100)

KAR 한국로봇산업협회
Korea Association of Robot industry

기계 안전에 관한 국제 규격의 구조



ISO 12100 및 기존 B, C규격의 관계

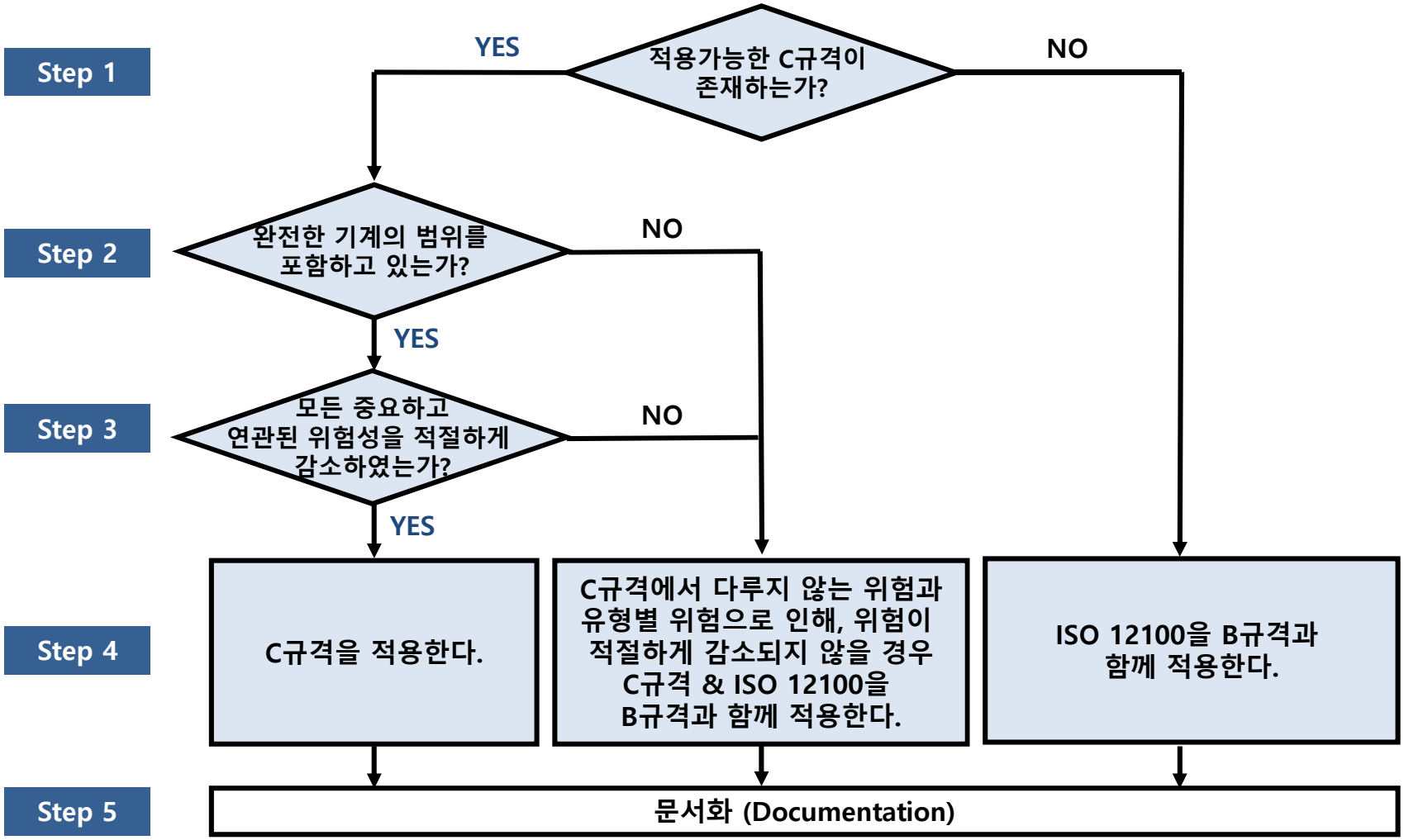


Figure 4 — Recommended steps for the practical use of ISO 12100 and existing type-B and type-C standards within this system

Refers to ISO/TR 22100-1:2015

* 기술 보고서 (TR: Technical Report)는 말그대로 보고서로서 규범 문서 라기보다는 정보를 제공하는 문서

산업용 로봇 안전규격에서의 위험성 평가

ISO 10218-1 : 2011

Robot and robotic devices – Safety Requirements for Industrial Robot – Part 1: **Robot**

Foreword
Introduction
1. Scope
2. Normative References
3. Terms & Definition
★ **4. Hazard identification and risk assessment (위험원 인지와 위험도 평가** KS B ISO 10218-1**)**
5. Design requirements and protective measures(설계 요구사항 및 보호 수단)
6. Verification and validation of safety requirements and protective measures
7. Information for use

근본 핵심

ISO 10218-2 : 2011

Robot and robotic devices – Safety Requirements for Industrial Robot – Part 2: **Robot systems and integration**

Foreword
Introduction
1. Scope
2. Normative References
3. Terms & Definition
4. Hazard identification and risk assessment (위험원 식별과 위험도 평가 KS B ISO 10218-2**)**
5. Safety requirements and protective measures (안전 요구사항 및 보호 대책)
6. Verification and validation of safety requirements and protective measures
7. Information for use

ISO 10218-2 Robot systems

Clause 4. Hazard identification and risk assessment

5절에 포함된 요구사항은 부속서 A에 명시된 위험원들에 대하여, ISO 12100에서 설명하는 안전수단을 반복적으로 적용하여 얻은 것이다. Refers to ISO 10218-1/2 Clause 4.

평가로부터 확인된 위험도를 5절의 요구사항을 적용하여 적절하게 감소시켜야 한다. 만일 위험도가 적절하게 감소되지 않았다면, 감소될 때까지 추가 위험도 경감 수단을 적용하여야 한다. Refers to ISO 10218-2 Clause 4.

로봇 시스템의 안전성능 수준은 PL "d"와 Cat. 3을 요구하지만, 포괄적인 위험성 평가를 통해, 다른 안전 관련 제어 시스템 성능이 결정될 수 있음 Refers to ISO 10218-2 5.2.3

위험성 평가 국제 규격 ISO 12100

ISO 12100 : 2010
Safety of machinery —General principles for design — **Risk assessment and risk reduction**

Foreword
Introduction
1. Scope
2. Normative References
3. Terms & Definition
4. Strategy for risk assessment and risk reduction
★ **5. Risk assessment**
(위험성 평가 KS B ISO 12100)
핵심
6. Risk reduction
(위험성 감소 KS B ISO 12100)
7. Documentation of risk assessment and risk reduction

ISO 12100에서는 산업용 로봇은 물론 모든 기계, 설비를 설계할 때, 예측할 수 있는 위험성을 위험성 평가 및 위험성 감소 원칙을 통해, 방법론을 제시하는 표준이다.

(1) 위험성평가
산업용 로봇 혹은 설비가 얼마나 위험한 것인지를 분석하고 판단하여 최대로 가능한 수준으로 정량화 하는 과정

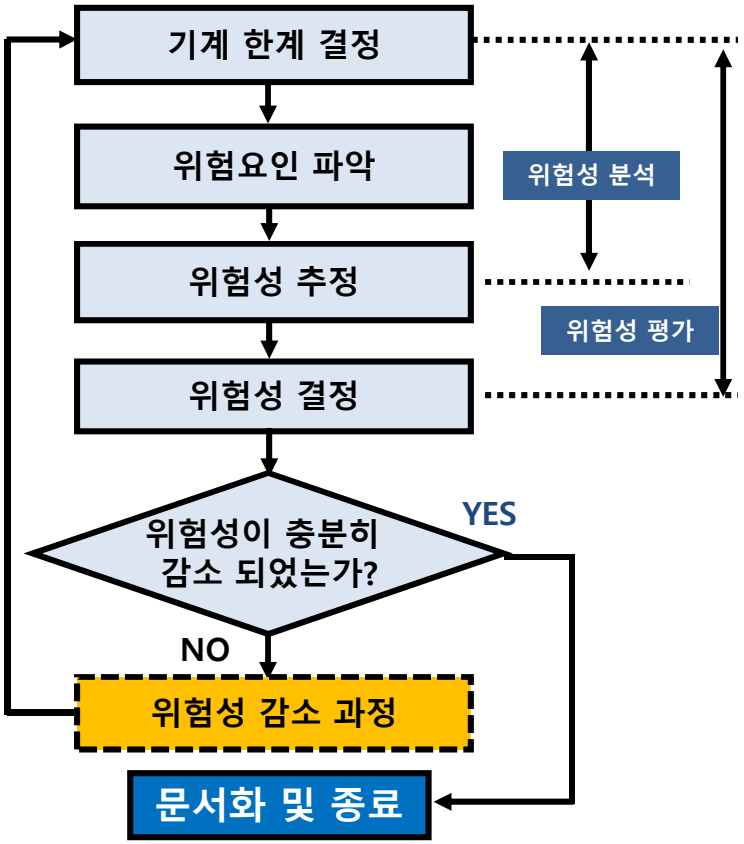
(2) 위험성 감소
위험성 평가를 통해 평가된 위험성을 현재의 기술 수준으로 최대한 합리적이고, 객관적으로 감소 시키는 과정

위험성 평가의 핵심

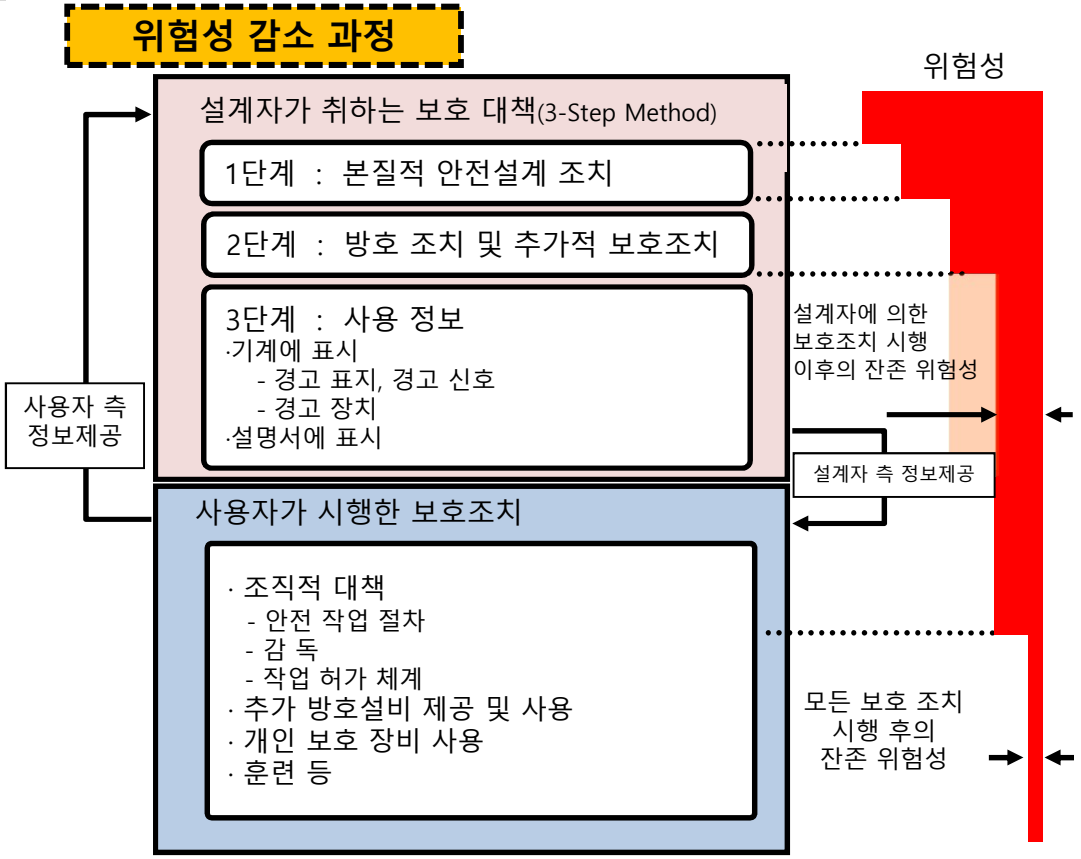
ISO 12100 : 2010

기계안전—설계 일반원칙 — 위험성 평가와 위험성 감소 (Risk assessment and risk reduction)

Clause 4. Hazard identification and risk assessment

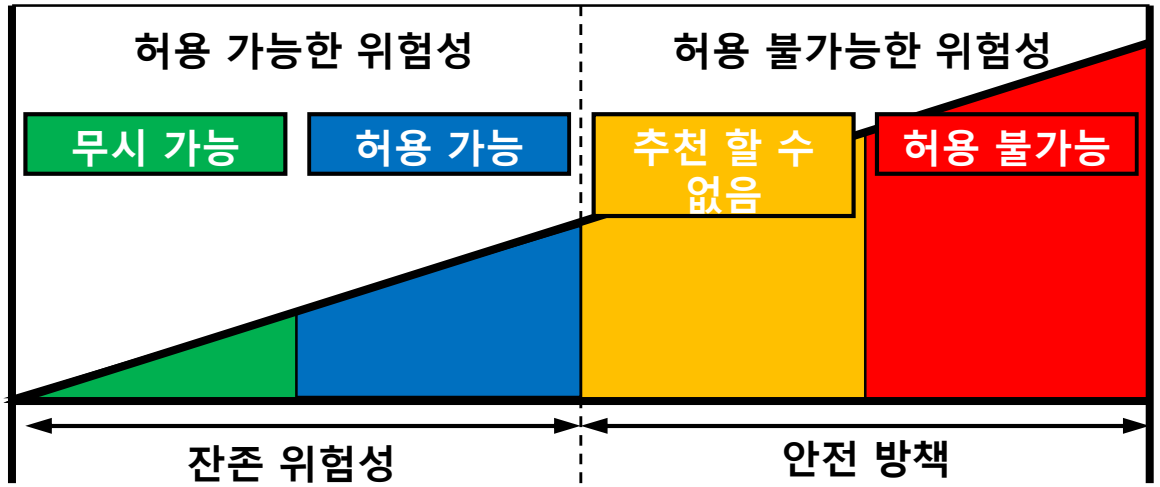


Clause 5. Design & Safety requirements and protective measures



어느 정도가 안전인가?

- 「안전」이란 「허용 불가능한 위험성은 없다」이다.
- 허용 가능한 위험성은 그 시대의 사회적 가치관에 의해서 바뀌는 경우가 있다
- 보통 허용 가능한 위험성은 안전 방책으로 이루어지지만,
  안전 방책 없이도 허용 가능한 수준의 위험성인 경우도 있다.
- 잔존 위험성은 위험성 감소 후에 남은 위험성이다.
  이 위험성은 허용 가능한 위험성보다 작거나 같다.



3.2 tolerable risk(견딜 수 있는 위험)
Level of risk that is accepted in a given context based on the current values of society
(사회의 현재 가치에 기초하여 주어진 맥락에서 수용할 수 있는 위험의 수준)

Refers to ISO/TR 22100-1:2015

* 기술 보고서 (TR: Technical Report)는 말그대로 보고서로서 규범 문서 라기보다는 정보를 제공하는 문서

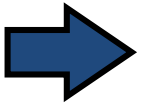
위험성 평가 규격 개정

- 기존의 Risk Assessment 관련 내용들의 규격들을 ISO12100:2010으로 통합 개정

ISO12100-1:2003

ISO12100-2:2003

ISO14121-1:2007



ISO12100:2010

Safety of machinery —General principles for design — **Risk assessment and risk reduction**

문서화에 대한 내용을 프로세스에 추가

ISO/TR 14121-2:2012

Safety of machinery — Risk assessment — **Part 2: Practical guidance and examples of methods**

이 기술 보고서는 ISO 12100에 따른 기계류의 위험성 평가 수행에 대한 실질적인 지침을 제공하고 있으며, 위험을 측정하는 다양한 방법의 예가 포함되어 있음.

* 기술 보고서 (TR: Technical Report)는 말그대로 보고서로서 규범 문서 라기보다는 정보를 제공하는 문서

KS B ISO 12100:2010 용어 선택

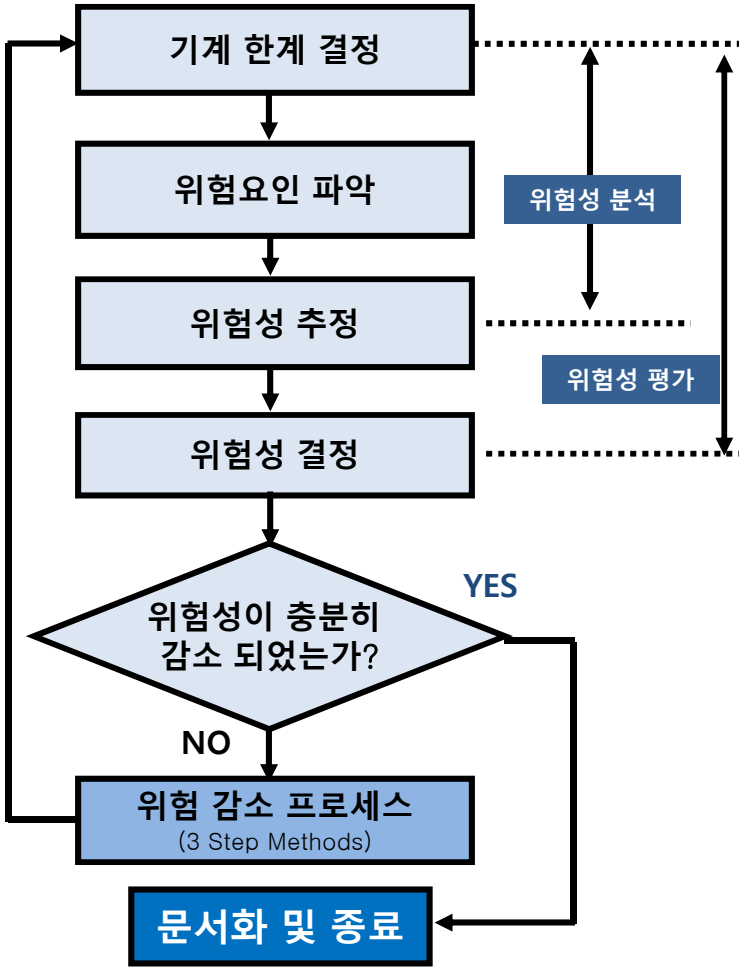
- 다음은 ISO 원문의 용어, 이에 대응되어 사용되는 용어 및 이 표준에서 사용한 용어이다.

* KS B ISO 12100-1:2010 해설 참조

ISO 원문	대응 용어	이 표준에서 사용된 용어	용어 채택의 이유
Risk	위험성, 위험도 리스크, 위험	위험성	risk가 정량적, 정성적 의미로 위험도와 위험성으로 정의될 수 있으나 산업안전보건법령에서는 위험성으로 사용되고 있어 이를 채택하였다.
Hazard	위험요인, 위험원, 유해 위험요인, 위험	위험요인	다른 분야에서는 위험원으로도 사용하였고 기계안전 분야에서는 위험으로도 사용하였으나 산업안전보건법령에서 유해·위험요인으로 사용되고 있어 보건 분야에서 사용하는 유해요인을 제외하여 위험요인으로 채택하였다.
Identification	파악, 확인, 식별	파악/식별	기계안전 분야에서는 주로 위험요인이나 위험성을 파악하는 의미로 사용되나 식별의 의미도로 사용되는 경우도 있으므로 이를 채택하였다.
Residual	잔존, 잔류	잔존	다른 분야에서는 잔류도 사용하나 기계안전 분야에서 잔존을 사용해왔으므로 이를 채택하였다
Reduction	감소, 저감	감소	다른 분야에서는 저감도 사용하나 산업안전보건법령에서 감소를 사용하므로 이를 채택하였다.
Guard	가드. 방어벽	가드	다른 분야에서는 방어벽도 사용하나 벽으로 한정하는 느낌이 있어 보다 포괄적인 의미를 부여하고자 가드를 채택하였다.
Evaluation	결정, 판정	결정/ 결과평가	다른 분야에서는 판정도 사용하나 산업안전보건법령에서 결정을 사용하며, 결과평가의 의미가 크므로 이를 채택하였다.
Estimation	추정, 예측	추정	다른 분야에서는 예측도 사용하나 산업안전보건법령에서 추정을 사용하여 이를 채택하였다.

위험성 평가의 순서와 상세내용

※ 위험성 분석과 평가 (Risk Analysis & Assessment)



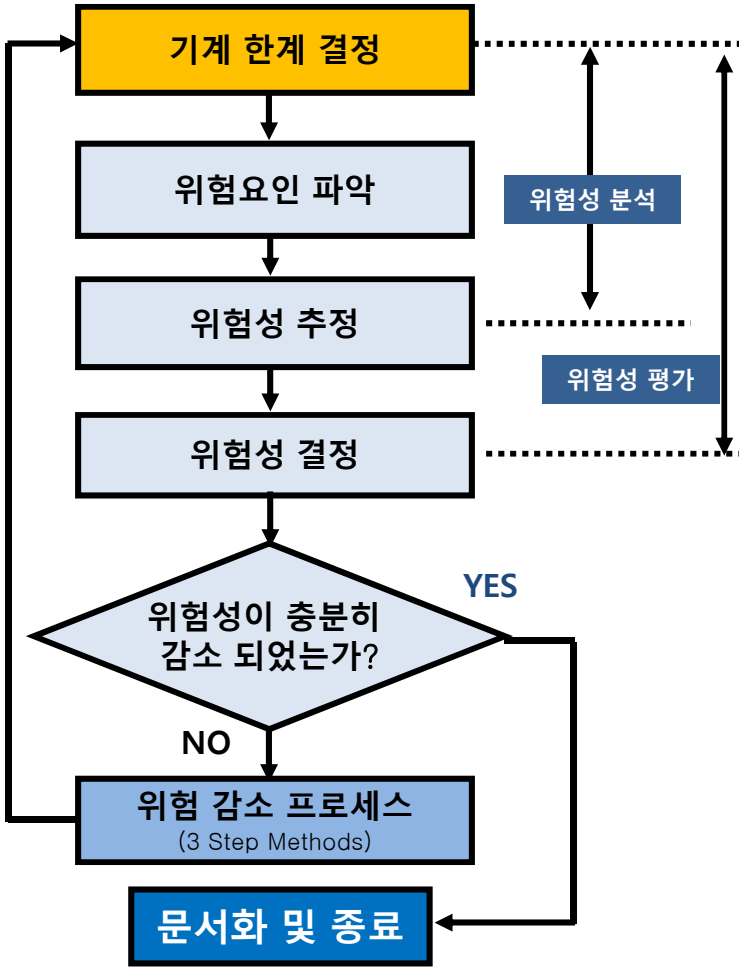
▣ 위험성평가는 설비의 정상 동작하는 상황 뿐 아니라, 전체의 상황 (즉, 설치,조정,생산, 유지보수,수리,해체)전체 상황의 위험성을 체계적으로 분석 및 평가한다

▣ 위험성 감소는 설계자가 시행하는 보호조치와 사용자가 시행하는 보호조치로 나뉜다

▣ 위험성 평가 이후, 허용가능한 위험만 남을 때까지, 현재의 기술 수준으로 최대한 합리적이고, 법률적 근거하에 반복적으로 감소한다.

위험성 평가의 순서와 상세내용

※ 기계 한계 결정(Determination of the limits of the machinery)



▣ 기계의 한계 결정

기계 수명 안에서, 특징과 사용 목적을 명확하게 한다

사용한계

기계의 여러 동작 및 조작 과정에서 충분히 예상 가능한 오용
작업자의 성별, 연령, 능력, 숙련도 등에 따른 오용

공간한계

이동범위, 운전 및 유지보수 시의 공간
작업자의 성별, 연령, 능력, 숙련도 등에 따른 오용

시간한계

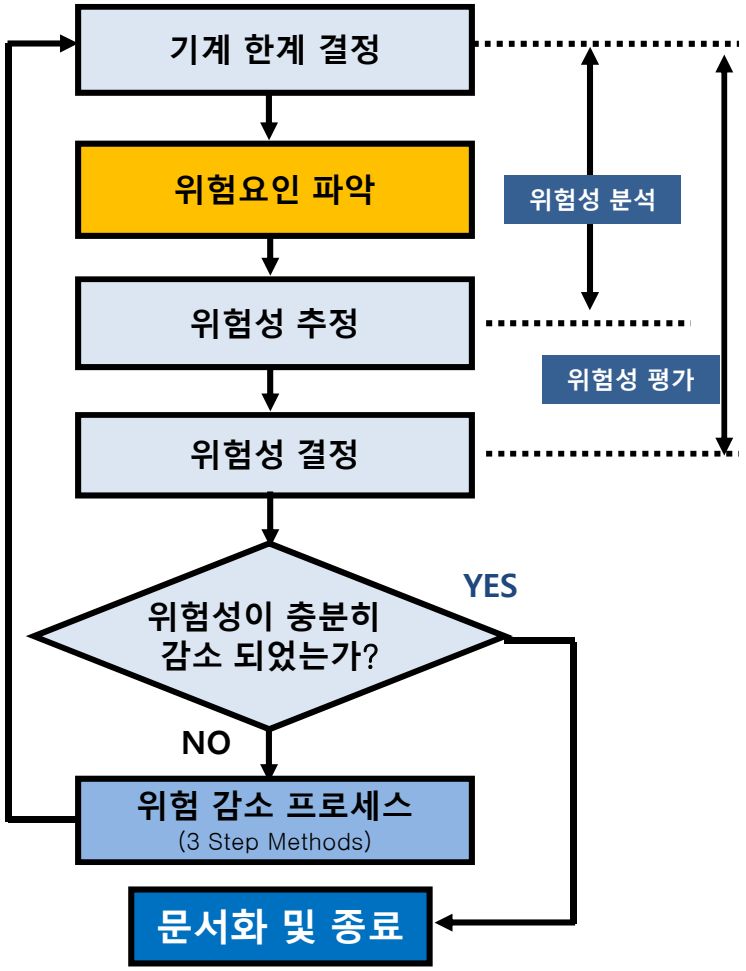
기계의 수명에 관한 모든 부분(제조, 운반, 사용, 분해 등)

기타한계

물질 속성, 청결 수준, 환경, 온도, 먼지, 습기 등

위험성 평가의 순서와 상세내용

※ 위험 요인 파악 (Hazard identification)



▣ 기계의 한계를 결정한 후, 기계 수명주기 전체 단계에서 합리적으로 예측 가능한 위험요인, 위험상황, 위험한 사건을 파악/식별한다.

▣ 설계자의 고려사항

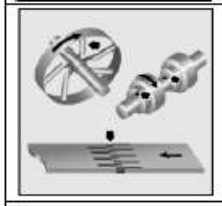
- **기계 전체 수명주기** 동안의 인적 상호작용
- 기계의 가능한 상태**(의도된 기능 및 공정상의 오작동)**
- 운전자의 **의도하지 않은 행동**
- **합리적으로 예측가능한** 기계의 오용

▣ "부속서 B"에는 위험요인, 위험 상황 및 위험한 사건의 예가 명시되어 있다

(참고자료)

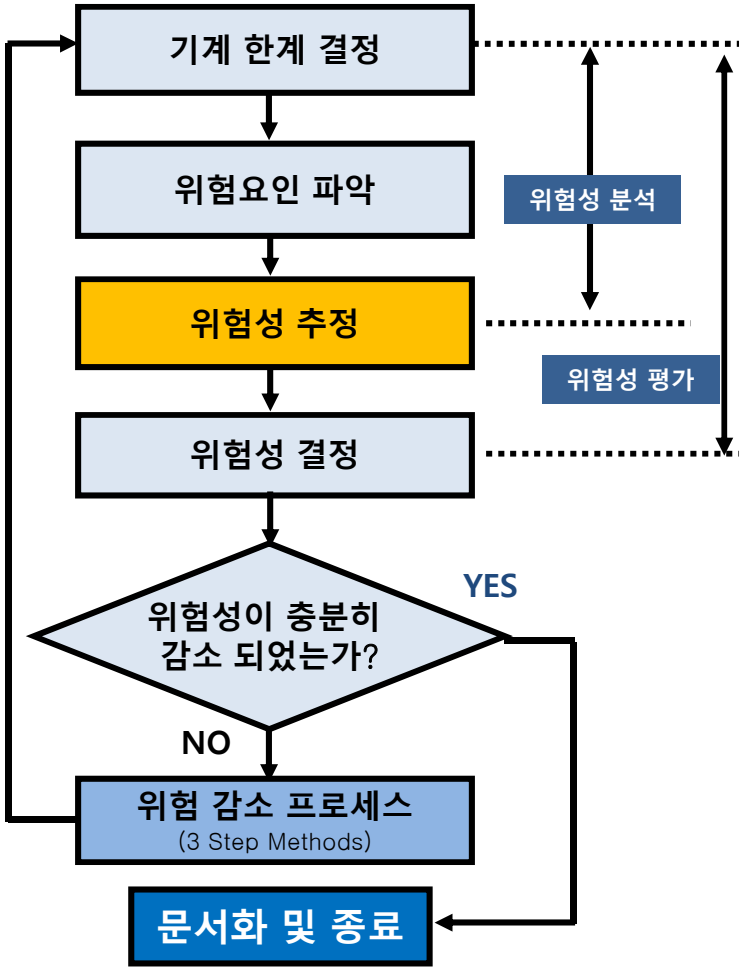
※ 부속서 B의 주요 위험 요인 목록 (일부)

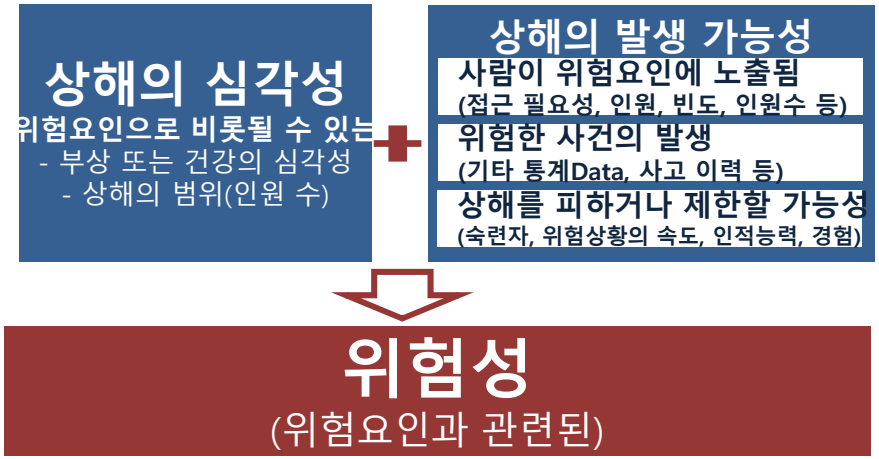
번호	유형 또는 범주	위험요인의 예	
		근원[a]	잠재적 결과[b]
1	기계적 위험요인	— 가속, 감속 — 뾰족한 부품 — 고정부품에 움직이는 요소의 접근 — 부품 절단 — 탄성 요소 — 낙하물 — 중력 — 고소 — 고압 — 불안정성 — 운동 에너지 — 기계 이동성 — 움직이는 요소 — 회전 요소 — 거칠고 미끄러운 표면 — 날카로운 가장자리 — 저장 에너지 — 진공	— 전복 — 비래(내던져짐) — 압착 — 절단 또는 분리 — 끌려 들어감 또는 걸림 — 말림 — 마찰 또는 마모 — 충격 — 분사 — 전단 — 미끄러짐, 걸려 넘어짐, 추락 — 찔림 또는 관통 — 절삭
2	전기적 위험요인	— 아크 — 전자기 현상 — 정전기 현상 — 충전부 — 고전압이 흐르는 작동 부품과 가까운 거리 — 과부하 — 결함 조건에서 작동되는 부품 — 단락 — 열복사	— 화상 — 화학적 영향 — 의료용 보철물에 영향 — 감전사 — 낙하, 비래 — 화재 — 용융 입자의 분출 — 전격(전기충격)
3	열적 위험요인	— 폭발 — 화염 — 고온 또는 저온의 물체나 재료 — 열원으로부터의 복사열	— 화상 — 탈수 — 불쾌감 — 동상 — 열원으로부터의 복사열로 인한 부상 — 데임

위험요인		위험요인	
	근원 부품 절단 잠재적 결과 — 절단 — 분리		근원 추락물 잠재적 결과 — 압착 — 충격
	근원 움직이는 오소 잠재적 결과 — 압착 — 충격 — 전단		근원 움직이는 오소 잠재적 결과 — 끌려 들어감 — 마찰, 마모 — 충격
	근원 중력, 안정성 잠재적 결과 — 압착 — 걸림		근원 움직이는 오소의 고정된 부분에 접근 잠재적 결과 — 압착 — 충격
	근원 회전 부품 또는 움직이는 오소 잠재적 결과 — 절단 — 얽힘		근원 움직이는 오소 잠재적 결과 — 압착 — 마찰, 마모 — 충격 — 절단
	근원 작동 부품 잠재적 결과 — 감전 — 화상 — 관통 — 데임		근원 고온 또는 저온 물체나 재료 잠재적 결과 — 화상

위험성 평가의 순서와 상세내용

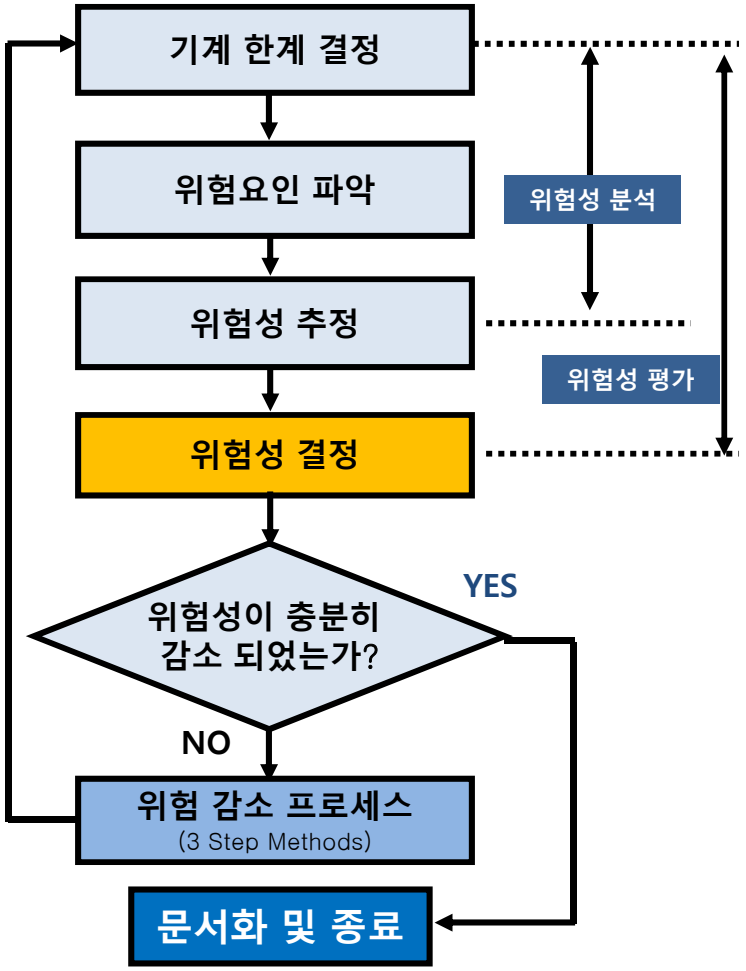
※ 위험성 추정(Risk estimation) 일반사항





위험성 평가의 순서와 상세내용

※ 위험성 추정(Risk estimation) 일반사항



▣ 위험성 추정이 완료되면, 위험성 감소가 필요한지 여부를 파악하기 위해, 위험성 결정을 해야함.

▣ 위험성 추정 및 결정의 방법은 SEMI, ANSI, EN, ISO 등 매우 다양한 방식이 존재함.
본문에서는 두가지의 방식만 다루겠음.

예1) ISO13849-1 : 2015
예2) ISO TR 14121-2 : 2012

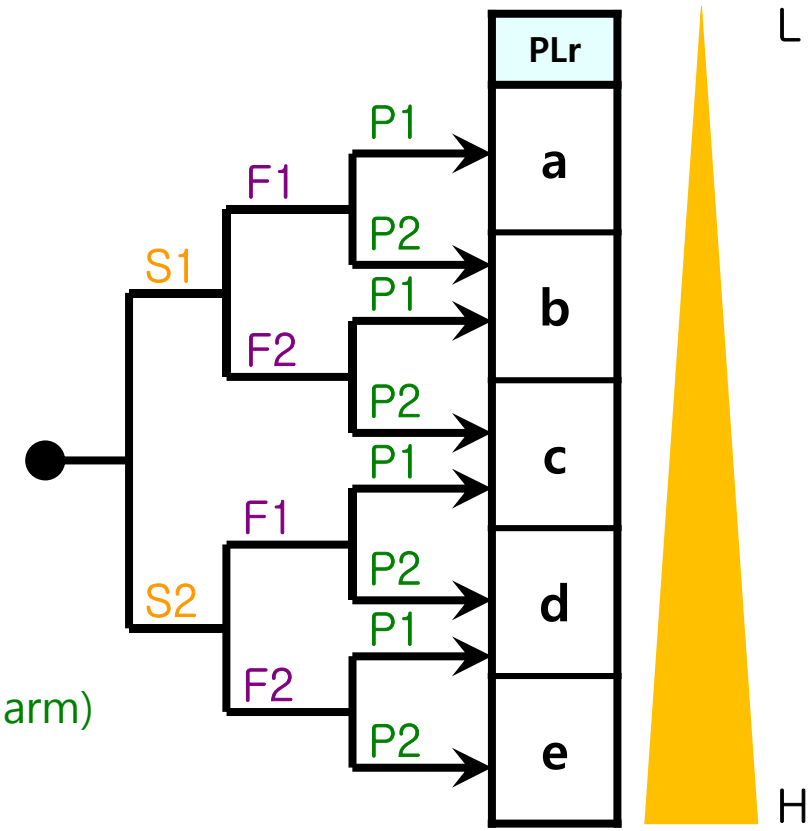
위험성 추정 및 결정의 예 (ISO13849-1)

예1) ISO13849-1:2015

S : 상처의 중대도
(Severity of Injury)
- ·S1 : 경상
- ·S2 : 중증(후유증, 사망 등)

F : 위험에 처해지는 빈도
(Frequency and/or Exposure to Hazard)
- ·F1 : 보기 드물게 발생하거나 단시간
- ·F2 : 빈번히 발생하거나 장시간

P : 위험을 피하거나 손해를 제한할 가능성
(Possibility of Avoiding Hazard or Limiting Harm)
- ·P1 : 특정의 조건하에서 가능
- ·P2 : 불가능



It should be noted that the method given in ISO 13849-1 is primarily intended to be used for safety functions carried out by safety-related control systems.
(ISO 13849-1은 안전관련 제어 시스템에 의해 수행되는 안전기능에만 사용할 수 있음을 유의)

For example, a resulting category or performance level makes no sense for a slipping hazard or falling hazard.
(예를 들면, 미끄러지는 위험이나, 추락위험에 대하여 PL 및 안전 카테고리는 의미 없음)

Refers to ISO/TR 22100-2:2013

위험성 추정 및 결정의 예 (ISO/TR 14121-2:2012)

예2) ISO/TR 14121-2:2012

S : 상해의 심각도

·S1 : 경미한 상해

·S2 : 심각한 상해(후유증, 사망 등)

F : 위험요인 노출 주기 및 지속기간

·F1 : 드문 경우/단기간 노출

·F2 : 지속적 및 장기간 노출 빈번 (15분/2회 이상)

O : 위험 사고 발생 가능성

·O1 : 낮음 (충분한 기술, 증명 안전 어플리케이션)

·O2 : 중간 (6개월 이상 경험자의 부적절한 행동)

·O3 : 높음 (6개월 미만의 비 숙련자의 부적절한 행동)

A : 상해 회피 및 감소 가능성

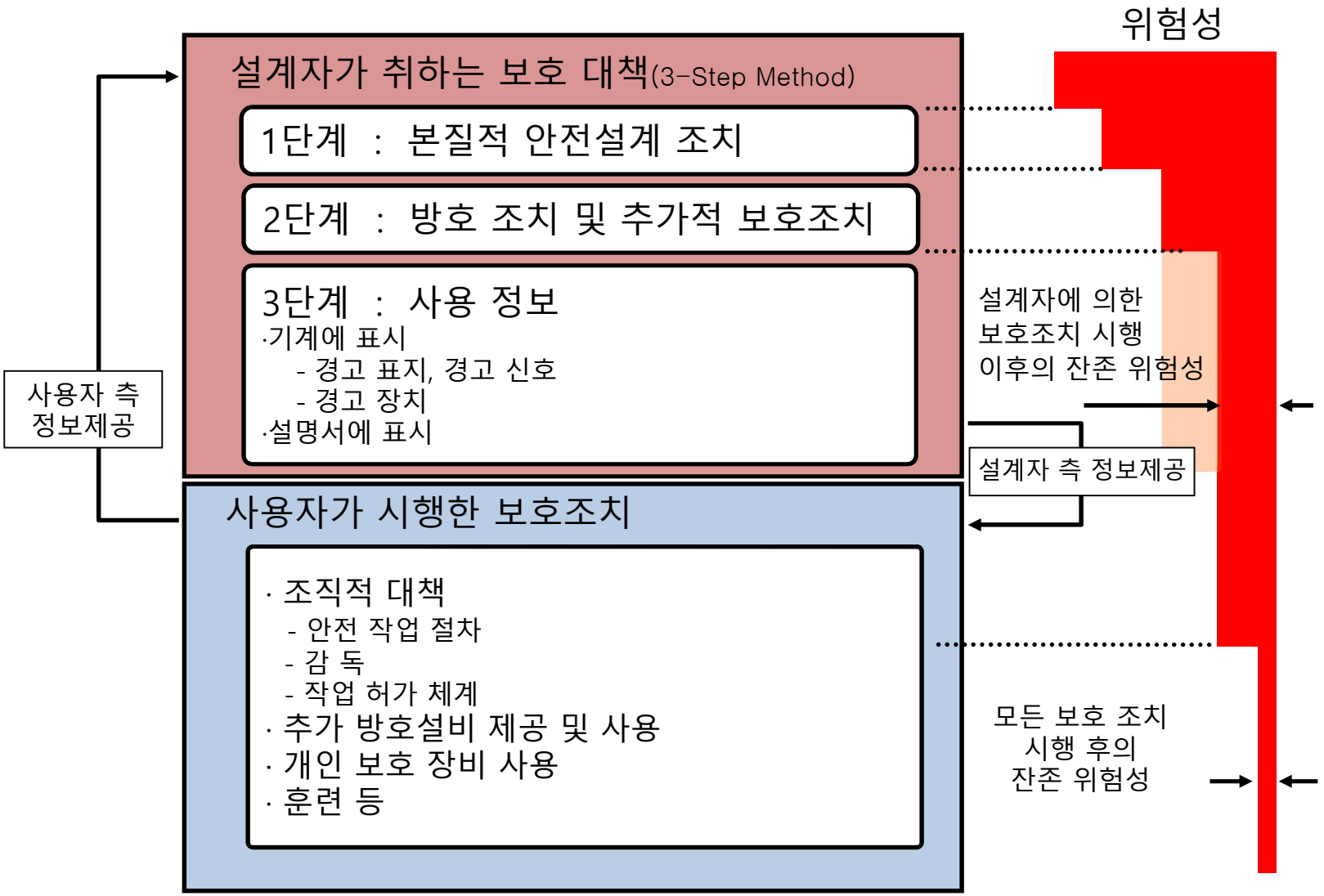
·A1 : 특정의 조건하에서 가능

·A2 : 불가능함

Figure 4 — Risk matrix equivalent to the risk graph in Figure 3

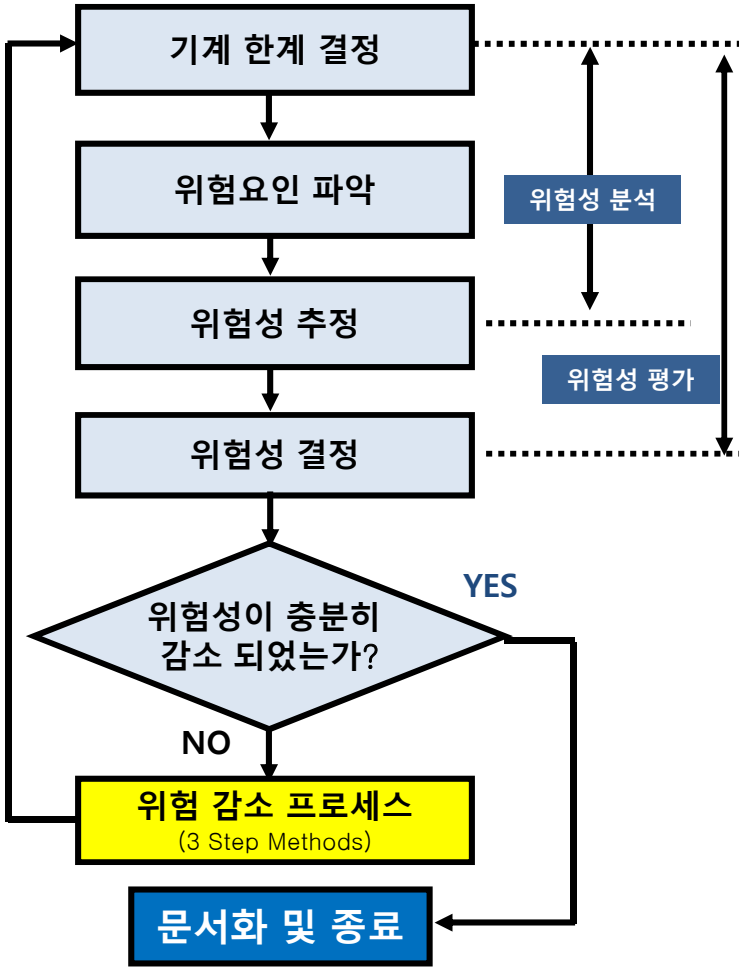
		Risk index calculation					
		O1		O2		O3	
		A1	A2	A1	A2	A1	A2
S1	F1	1				2	
	F2						
S2	F1	2			3		4
	F2	3	4		5		6

위험성 감소 (Risk Reduction)



위험성 감소 (Risk Reduction)

※ 설계자가 취하는 보호대책 (3-Step Methods)



▣ 1단계 : 설계상의 대책 (본질안전설계)

근본적으로 노출된 사람과 기계 사이에 상호작용을 적절하게 선택하여 위험 요인을 제거

▣ 2단계 : 안전 장치 및 추가 보호 대책

적절하게 선택된 방호조치 및 추가적인 보호조치를 사용하여 위험성을 줄임 ex) 공간적, 시간적 분리

▣ 3단계 : 사용상의 정보

위 두 단계를 시행하고도 잔존하는 위험성을 경고표식 등으로 감소

설계자가 취하는 보호대책 (3-Step Methods)

1단계 : 본질안전설계

무게 분산, 진동, 재질, Cable 색상

2단계 : 안전장치 및 추가보호

가드, 도어sw, 안전시스템

3단계 : 사용상의 정보

경고표시, 경광등

1단계 : 설계상의 대책 (본질안전설계)

1단계 : 본질안전설계

무게 분산, 진동, 재질, Cable 색상

2단계 : 안전장치 및 추가보호

가드, 도어sw, 안전시스템

3단계 : 사용상의 정보

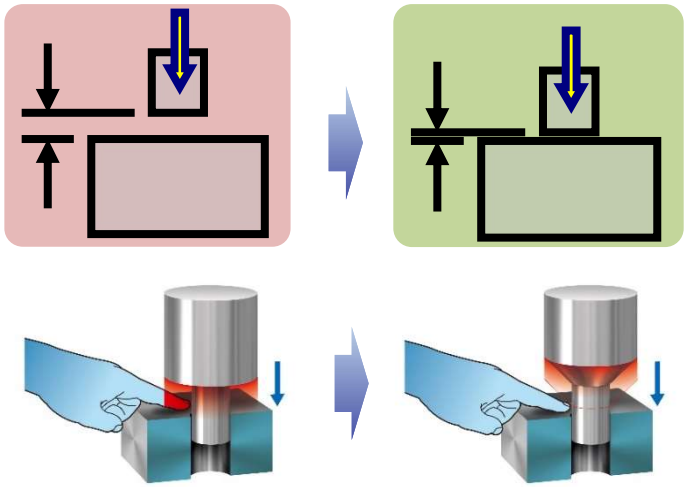
경고표시, 경광등

1단계 : 설계상의 대책 (본질안전설계)

끼임 위험 방지를 위해

·손가락 등이 들어가지 않게 개구부를 좁게

·가동 범위를 좁게



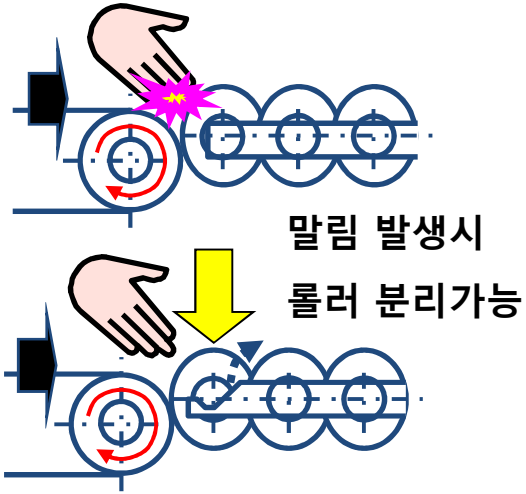
찔림 등의 위험 방지를 위해

·위험을 미칠 우려가 있는 예리한 절단부
모퉁이, 돌기물 등을 제거하는 것

말림 위험 방지를 위해

·구동력을 적게, 회전수를 천천히

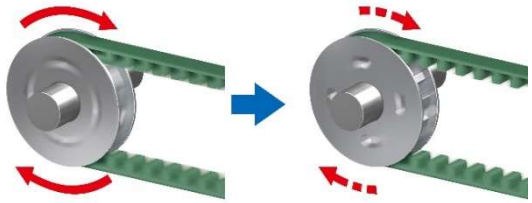
·말려 들어가지 않도록 틈새를 만듬



말림 위험 방지를 위해

·구동력을 적게

·회전수를 천천히



1단계 : 설계상의 대책 (본질안전설계)

- 접속 오류 방지
  - Cable색의 통일 또는 Label에 의한 확인
  - 배관 연결 부분의 커넥터/색

【예】

- Cable색의 통일(IEC 60204 기준한 기기내 배선색)
  - 보호접지(Ground)회로 : 녹/황의 Spiral 
  - 전력중성회로 : 밝은 파랑 
  - 동력(1차측)회로 : 흑색 
  - 제어회로(DC) : 청색 
  - 제어회로(AC) : 적색 
  - Interlock 회로 : 주황색 

1단계 : 설계상의 대책 (본질안전설계)

기계를 설계함에 따라 안전 방호물 등의 부가적인 장치를 설치 하지 않고 Risk를 감소시키는 안전방책을 말함.

*** 본질 안전 설계의 요건은**

① 위험을 유발하는 예리한 절단면, 돌기물 등을 제거하는 것.
② 끼임이 우려되는 부분을 신체가 들어 가지 않을 정도로 좁게 하는 것, 또는 신체에 피해가 생기지 않을 정도로 작동부분의 구동력을 작게 하는 것.
③ 감전 초래되는 전압사용을 지양, 유해성 없는 재료사용 및 방폭기기등을 사용하는 것.
④ 인간공학에 기초를 둔 신체적 부담 감소, 오조작 발생 예방
⑤ 제어 시스템에 대해서는 신뢰성 높은 부품의 사용, Fail Safe화, 전원 노이즈 대책 등을 행하는 것.
⑥ 자동화 등에 의한 유해물질에 노동자가 노출되는 기회를 줄이는 것.

2단계 : 안전 장치 및 추가 보호 대책

1단계 : 본질안전설계
무게 분산, 진동, 재질, Cable 색상

2단계 : 안전장치 및 추가보호
가드, 도어sw, 안전시스템

3단계 : 사용상의 정보
경고표시, 경광등

2단계 : 안전 장치 및 추가 보호 대책

- 안전방호의 원칙은 두 가지

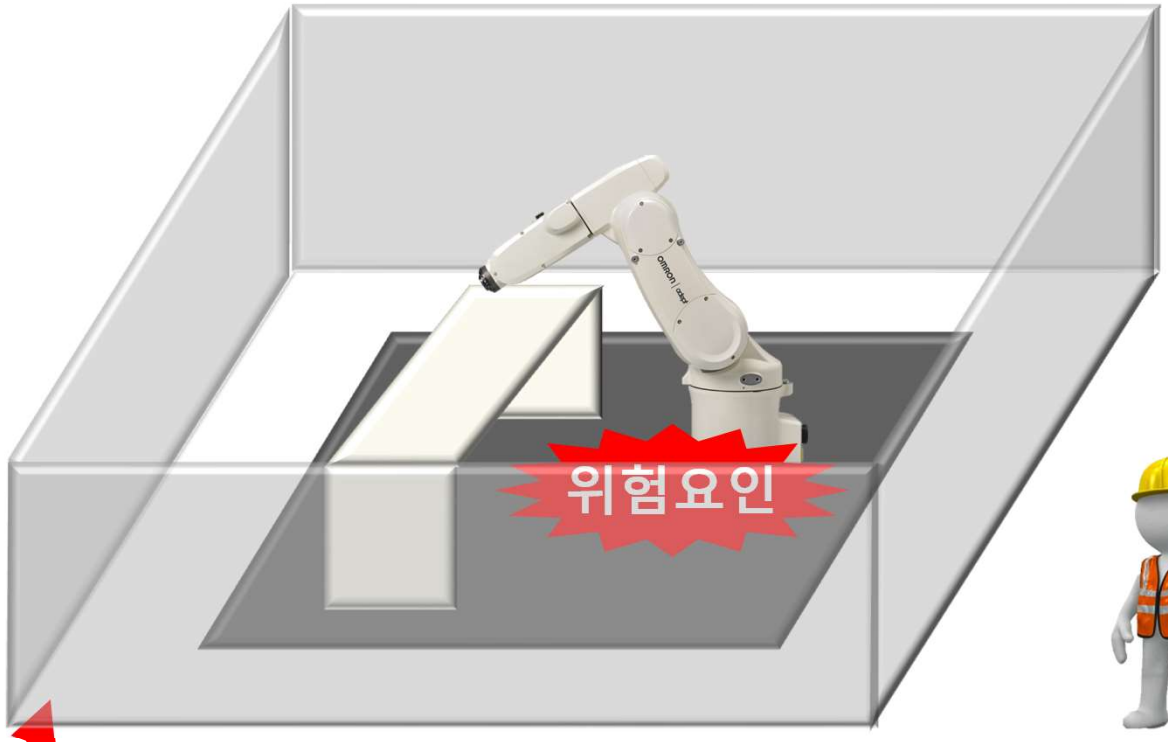
공간적인 분리	시간적인 분리
격리원칙 가드에 의한 안전방호	**정지원칙** 인터록에 의한 안전방호
• 위험은 모두 격리한다 • 필요시 최소한 연다	• 안전이 확인되지 않으면 정지 • 정지를 확인하는 구조를 만든다

사례1 · · · 노출된 위험요인

무심코 방치하면 부상가능성 큼

작업자에 대해서 위험요인이 드러난 상태

사례2 · · · 공간적 분리



부상은 나지 않지만 이 상태로는 작업 불가능

안전 펜스등을 설치하여 작업자와 위험요인을 격리시킨다.

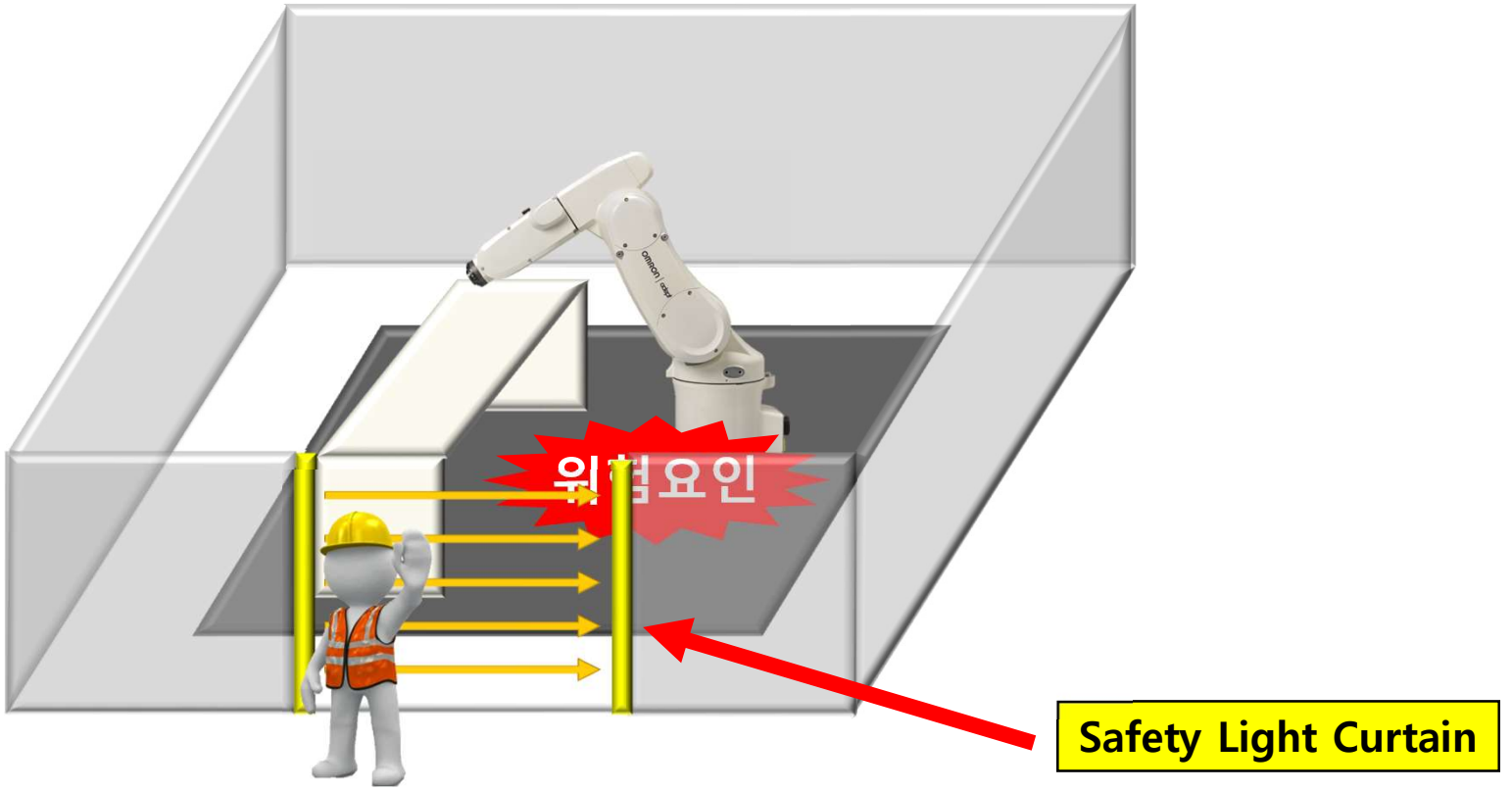
사례3 . . . 시간적 분리

Door Switch와 안전회로에 따른 위험요인의 정지

도어를 열면 자동적으로 정지

도어를 열고 있을 때는 기동 안됨

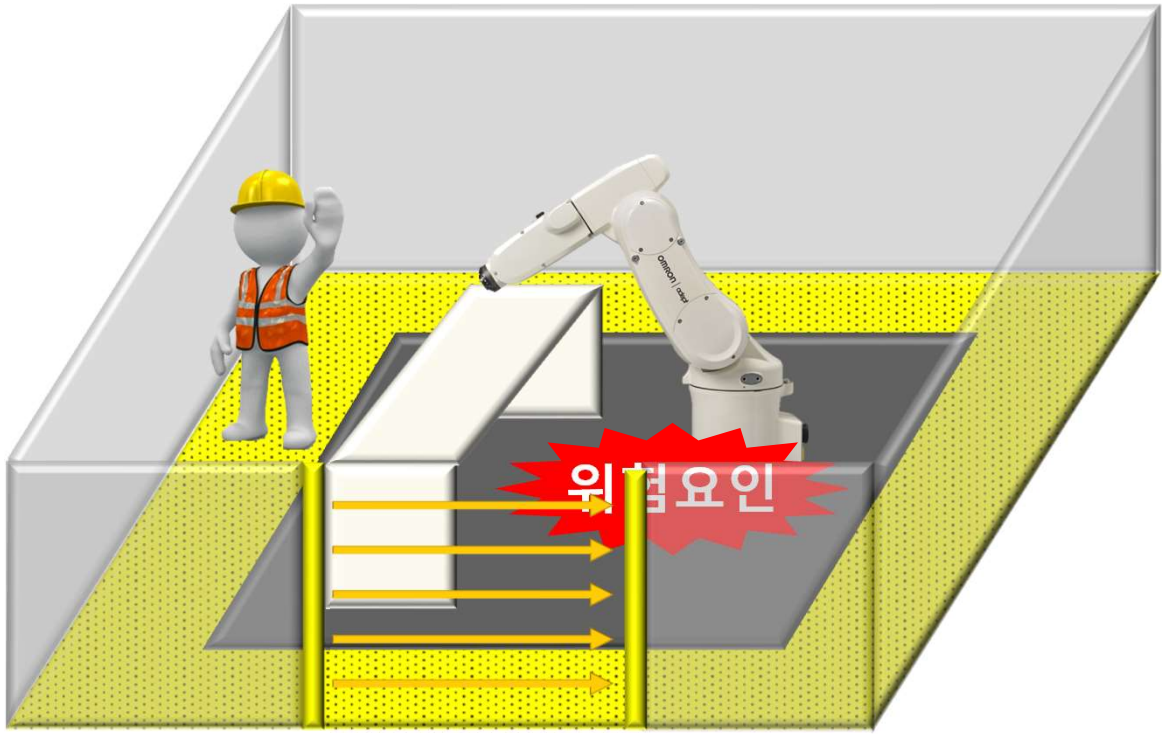
사례4 . . . 안전확보와 작업성



Light Curtain과 안전회로에 의한 위험요인의 정지

작업 프로세스의 관계로 위험요인에 빈번하게 접근 할 때 편리

사례5 · · · 존재검지

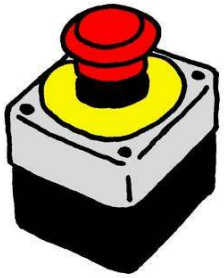


안전 방책의 내부(위험요인측)에 작업자가 진입하고 있는 것을 검지한 경우에 위험요인(장치)을 동작시키지 않음.
위의 그림에서는 매트스위치를 사용한 예 이지만
레이저 스캐너를 사용하는 방법도 있다.

2단계 : 안전 장치 및 추가 보호 대책

- 추가 보호 대책의 예

비상 정지 장치



에너지 차단 장치
락아웃 ·태그 아웃

안전한 접근 대책
적당한 난간, 기둥 및 발판

이네이블 장치

3단계 : 사용상의 정보

1단계 : 본질안전설계

무게 분산, 진동, 재질, Cable 색상

2단계 : 안전장치 및 추가보호

가드, 도어sw, 안전시스템

3단계 : 사용상의 정보

경고표시, 경광등

3단계 : 사용상의 정보

- 사용상의 정보

ISO·IEC

	**IEC 61310**		**IEC 3864 ISO 7000**
	**IEC 61310**		**IEC 61310**
	**IEC 61310 ISO 3864**		**IEC 61310**

ANSI

	**ANSI Z535.3**
	**ANSI Z535.3**
	**ANSI Z535.3**

SEMI S1

	**SEMI S1**
	**SEMI S1**
	**SEMI S1**

- 신호 및 경보

경광등

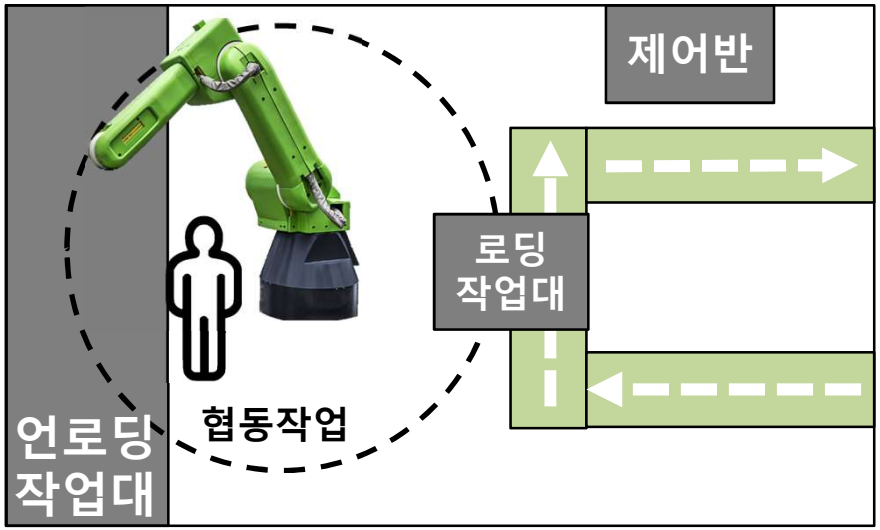
경고음

위험성평가 사례 및 실습

KAR 한국로봇산업협회
Korea Association of Robot industry

위험성평가 사례1

공정 레이아웃

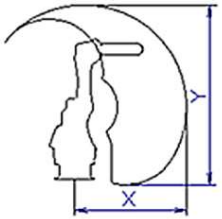


공정 작업순서

순서	작업 내용
1	컨베이어를 타고 제품 로딩 작업대 위치 고정
2	협동 로봇 제품 로딩-> 언로딩 작업대 이동
3	협동 작업영역으로 작업자 진입 및 언로딩 작업 중에 핸드가이딩 작업
※	핸드가이딩 작업 중에 **무게작업은 로봇, 육안 검사진행 및 정밀 언로딩은 작업자가 진행**

위험성평가 사례1

사용로봇 정보



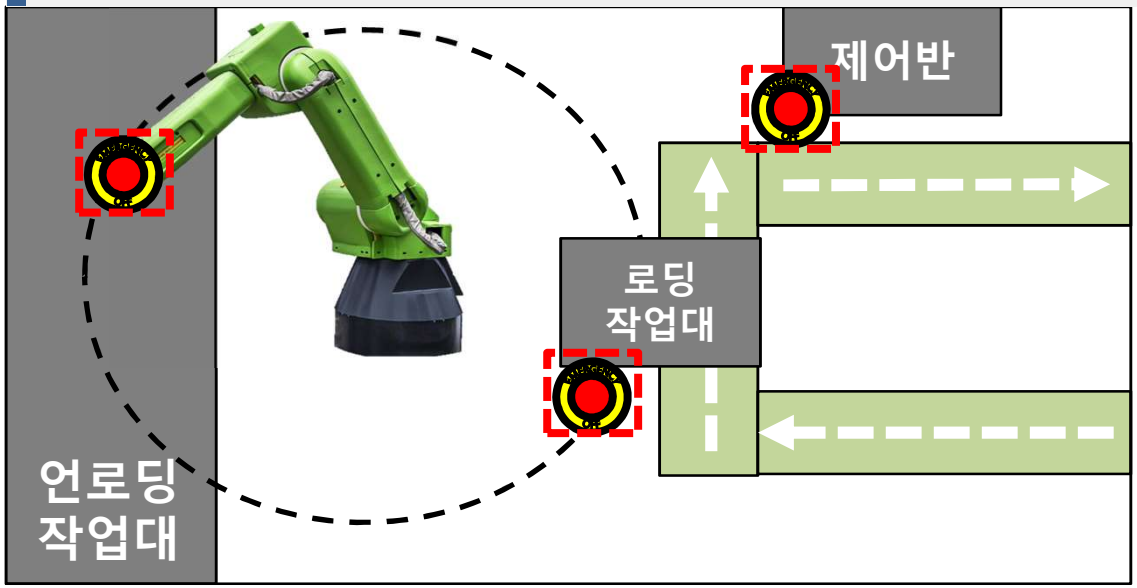
로봇 제작사	FANUC
형식(규격)	CR-35iA
안전인증 이력	ISO 10218-1 ISO 13849-1 IEC 60204-1

공정 구성품 정보

번호	기계 설비	축/규격 (mm)	주요 재질
1	협동로봇	(최대동작 범위X,Y) 1,813 * 2,931	알루미늄, 스테인리스
2	컨베이어(세로)	800 * 300 * 400	금속, 수지
3	컨베이어(가로)	800 * 1,500 * 400	금속, 수지
4	작업대	1,100 * 1,800 * 1,400	금속

위험성평가 사례1

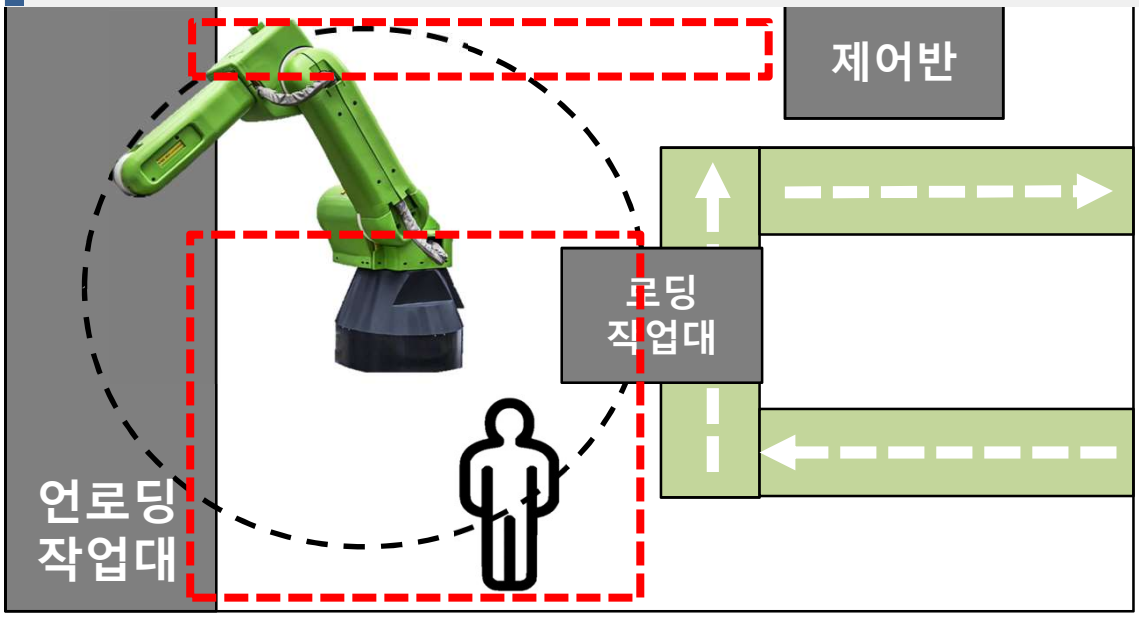
주요 위험요인 (비상정지장치)



순번	위험한 사건	위험 감소 조치 및 관련 규격
1	비상정지 장치가 충분하지 않아, 비상 상황에서, 특정위치에서는 비상정지를 누르지 못해 사고로 이어질 가능성 있음	**(1) 산업용로봇검사기준 29항 비상정지장치** 비상정지장치는 각 제어반 및 그 밖에 비상정지장치가 필요한곳에 설치하되, 접근이 용이하게 배치되어 정상적으로 작동될 것 **(2) ISO 10218-2 Annex G 5.3.8.2** 비상정지 시스템의 작동은 하나의 작업 영역 안에서 같은 제어범위를 가져야 하며, 모든 로봇 동작과 기타 위험한 기능을 멈추게 해야 한다 **(3) 산업용로봇검사기준 29항 비상정지장치** 회로상에 여러 개의 비상정지장치가 설치된 경우, 작동된 모든 비상정지장치가 복귀되기 전에는 기계가 작동되지 않을 것
2	비상정지 장치의 제어범위가 명확하지 않거나, 같은 보호영역 내에서, 정지시키는 제어범위가 다를 경우, 위험상황을 발생시키는 위험요인을 멈출 수 없어, 추가 위험상황이 발생할 수 있음	

위험성평가 사례1

주요 위험요인 (협동영역)

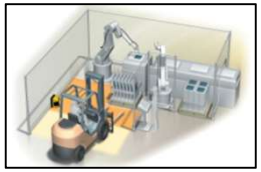


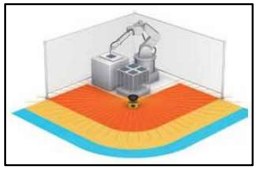
순번	위험한 사건	위험 감소 조치 및 관련 규격
1	협동운전을 위한 작업자의 협동 영역 접근 시에, 작업자의 존재를 검지하는 시스템이 없어, 로봇에 충돌할 수 있는 위험이 존재함	**(1) ISO 10218-2 Annex G 5.11.2** 사람이 협동 공간에 들어왔을 때, 로봇의 동작은 정지하고, 안전 감시 정지가 유지 되어야 한다
2	협동운전을 위한, 접근 통로 외에, 뒤로 돌아 들어오는 사람의 존재를 검지하는 시스템이 없어, 로봇에 충돌할 수 있는 위험이 존재함	**(2) ISO 10218-2 Annex G 5.11.2** 협동작업 영역을 넘어서 보호영역 안으로 침투한 경우, 로봇은 정지되고, 위험 요인들이 중단되도록 설계한다
3	협동 운전을 하는 협동 작업 공간이 명확하기 정의되지 않아, 작업자의 혼란으로 인해, 추가 위험이 발생할 수 있음	**(3) ISO 10218-2 Annex G. 5.11.2** 사람이 직접적으로 로봇과 상호작용을 하는 협동 작업 공간은 명확하게 정의한다(예: 바닥 시, 신호 등)

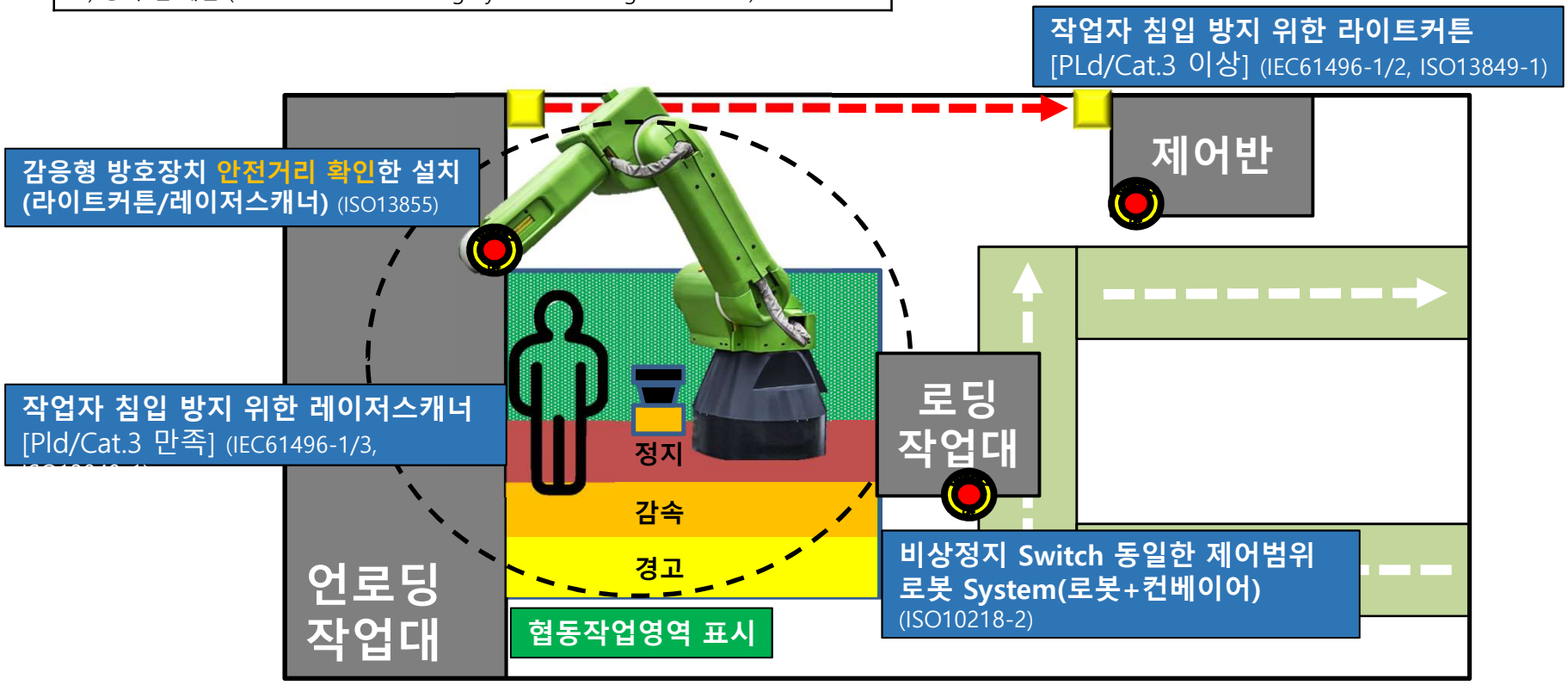
위험성평가 사례1

SOLUTION. KS B ISO TS 15066에 따른 협동로봇 솔루션

※ 협동 운전은 다음의 방법들 중 하나 또는 그 이상을 포함할 수 있다. (ISO TS 15066)
a) 안전 정격 감시 정지 (Safety-rated monitored stop)
b) 핸드 가이딩 (Hand guiding)
c) 속도 및 위치 감시 (Speed and separation monitoring)
d) 동력-힘 제한 (Power and force limiting by inherent design or control)

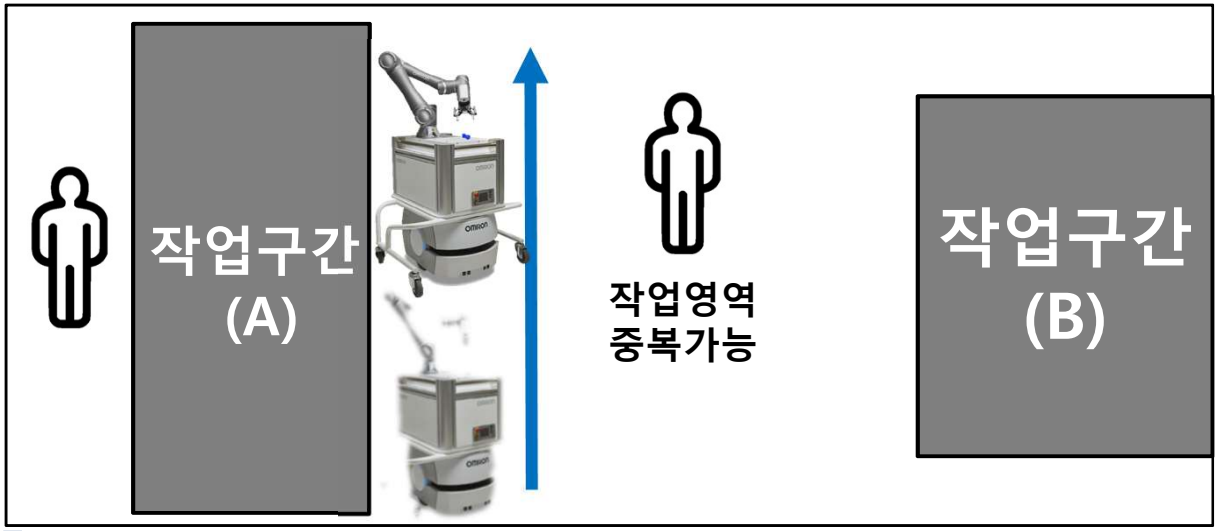






위험성평가 사례2

공정 레이아웃



공정 작업순서

순서	작업 내용
1	작업자 작업구간(A) 준비 후, 모바일 매니퓰레이터 호출
2	모바일매니퓰레이터 작업구간(A)이동 후, 협동로봇 상품 로딩
3	작업구간 (B)로 이동 후, 상품 로딩/언로딩
※	모바일로봇 및 협동로봇의 **결합으로 인한, 위험요인** 고려

위험성평가 사례2

사용로봇 정보

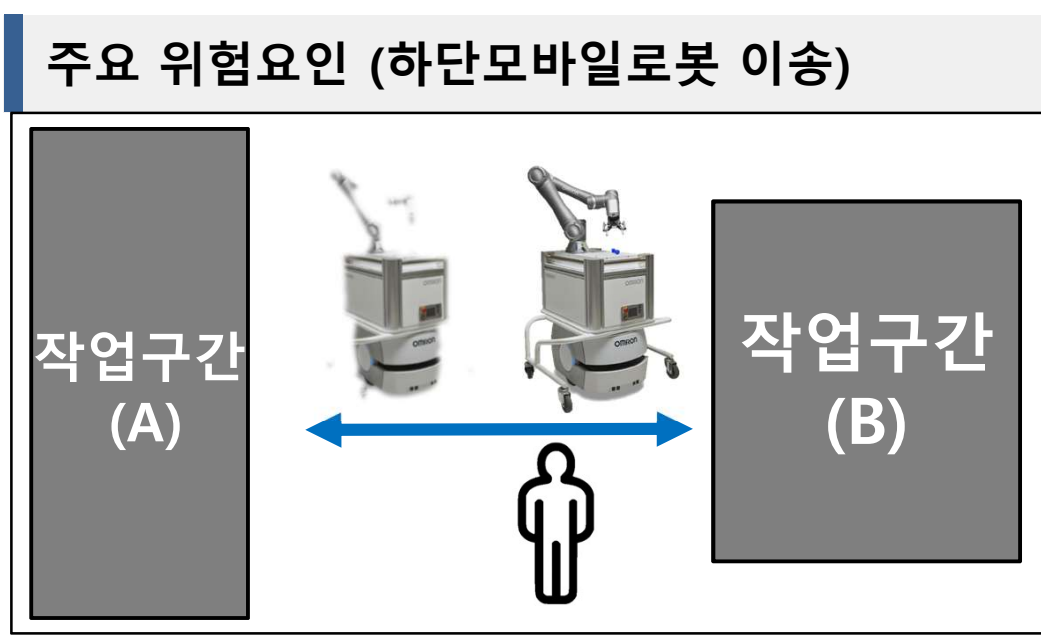
로봇 제작사	OMRON
형식(규격)	협동로봇 TM-12M 모바일로봇 LD-90X
안전인증 이력	협동로봇 : KCs자율안전확인 ISO 10218-1 ISO 13849-1 IEC 60204-1 모바일로봇 : S마크

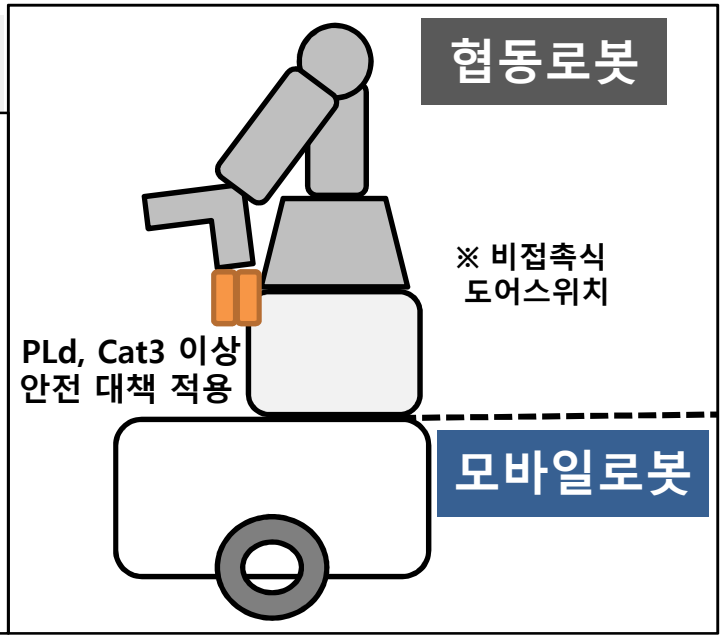
공정 구성품 정보

번호	기계 설비	축/규격 (mm)	주요 재질
1	협동로봇	(최대동작 범위X,Y) 1,204 * 1,194	알루미늄, 스테인리스
2	모바일로봇	500 * 700 * 379	금속, 수지
3	작업대(A)	1,800 * 1,800 * 2,100	금속
4	작업대(B)	1,800 * 1,300 * 1,100	금속

위험성평가 사례2

주요 위험요인 (하단모바일로봇 이송)

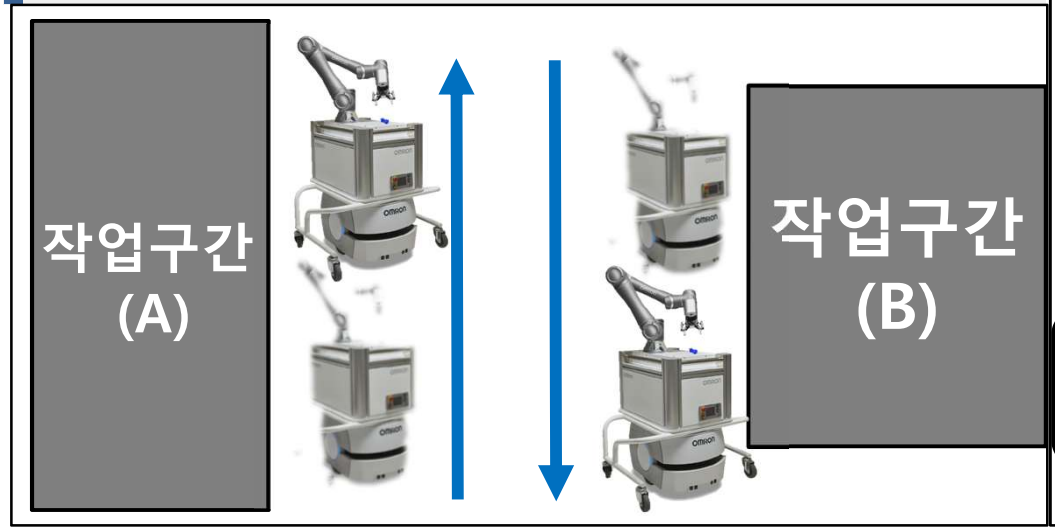


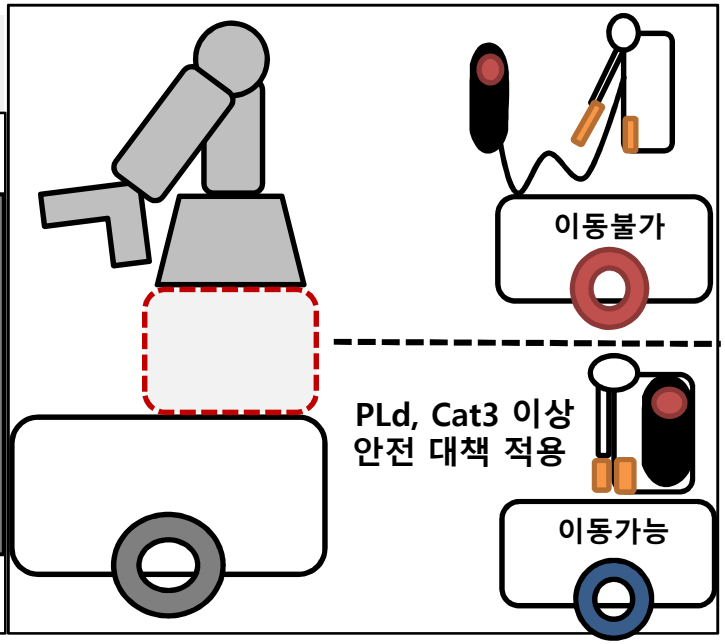


순번	위험한 사건	위험 감소 조치 및 관련 규격
1	펜스로 보호되지 않고, 자율 주행을 하는 모바일로봇 특성으로 인해, 작업자와 작업공간이 겹쳐, 충돌할 수 있는 상황 발생	**(1)** 모바일 로봇 내부에 국제 규격에 준하는 안전 레이저 스캐너가 적용되어, 이동 중에 예상치 못한 작업자를 검지하면, 모바일 로봇이 정지하는 대책 적용(PLd/Cat3) **(2)** 하단부 모바일로봇 이송 시에, 상단부에 결합된 협동로봇의 관성에 의한 전복 위험성을 감소하기 위해 두 가지 감소 대책 실시 1) 모바일 로봇 이동 시엔, 상단부 협동로봇 정지 2) 이동 시 관성을 최소화하기 위한, 협동로봇의 최상의 Home position 적용
2	하단부의 모바일로봇이 움직일 때, 상단부 협동로봇이 움직일 경우, 결합으로 인한, 추가 위험상황 발생 가능	
3	기존 모바일 로봇의 상단 부에 협동로봇 시스템이 결합하였으므로, 이송 중 전복이 되는 위험상황 발생	

위험성평가 사례2

주요 위험요인 (상단협동로봇)



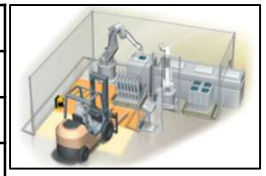


순번	위험한 사건	위험 감소 조치 및 관련 규격
1	상단 부 협동로봇을 티칭하는 상황에서, 하단 부 모바일 로봇의 이동으로 인한, 추가 위험상황 발생 가능	**(1)** 티칭 펜던트 보관 상자에 인터락 장치를 설치하여, 펜던트 사용 여부를 검지하고, 모바일 로봇으로 별도의 신호를 주어, 위험성 감소
2	협동운전을 위한 작업자의 협동 영역 접근 시에, 작업자의 존재를 검지하는 시스템이 없어, 로봇에 충돌할 수 있는 위험이 존재함	**(2) ISO 10218-2 Annex G 5.11.2** 사람이 협동 공간에 들어왔을 때, 로봇의 동작은 정지하고, 안전 감시 정지가 유지 되어야 한다
3	협동 운전을 하는 협동 작업 공간이 명확하기 정의되지 않아, 작업자의 혼란으로 인해, 추가 위험이 발생할 수 있음	**(3) ISO 10218-2 Annex G. 5.11.2** 사람이 직접적으로 로봇과 상호작용을 하는 협동 작업 공간은 명확하게 정의한다(예: 바닥 시, 신호 등)

위험성평가 사례2

SOLUTION. KS B ISO TS 15066에 따른 협동로봇 솔루션

※ 협동 운전은 다음의 방법들 중 하나 또는 그 이상을 포함할 수 있다. (ISO TS 15066)
a) 안전 정격 감시 정지 (Safety-rated monitored stop)
b) 핸드 가이딩 (Hand guiding)
c) 속도 및 위치 감시 (Speed and separation monitoring)
d) 동력-힘 제한 (Power and force limiting by inherent design or control)



레이아웃

협동 운전 방호대책 레이저스캐너
[PId/Cat.3 만족] (IEC61496-1/3, ISO13849-1)

감응형 방호장치 안전거리 확인한 설치 (레이저스캐너)
(ISO13855)

작업구간A

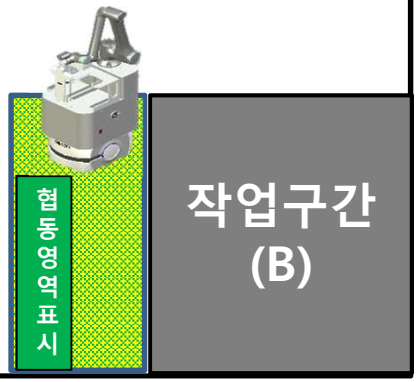
작업구간A에서 협동운전 작업

1. 모바일 로봇 정지
2. 작업자 진입 시 정격감시 정지
(ISO 10218-2, ISO/TS 15066)

작업구간B

작업구간B에서 협동운전 작업

1. 모바일 로봇 정지
2. 작업자 진입 시 정격감시 정지
(ISO 10218-2, ISO/TS 15066)



Risk Assessment 실습

위험성 평가 기준 (ISO13849-1)

[참조규격] KS B ISO13849-1:2015

S : 상처의 중대도

(Severity of Injury)

- S1 : 경상
- S2 : 중증(후유증, 사망 등)

2일 이내 복귀가능

2일 이내 복귀불가

F : 위험에 처해지는 빈도

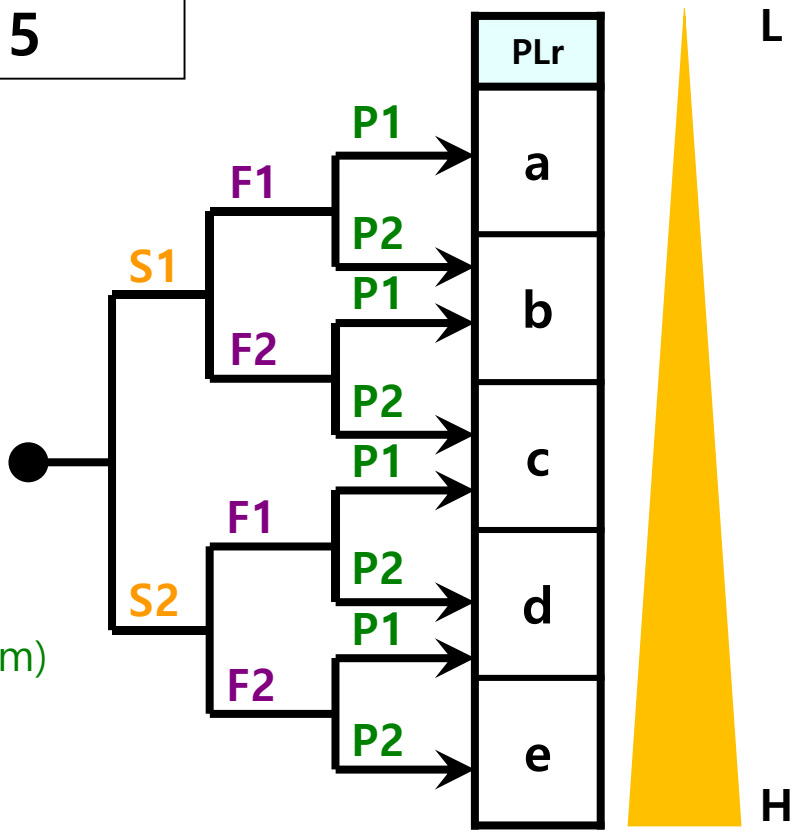
(Frequency and/or Exposure to Hazard)

- F1 : 보기 드물게 발생하거나 단시간 — 1일 15분, 2회 미만
- F2 : 빈번히 발생하거나 장시간 — 1일 15분, 2회 이상

P : 위험을 피하거나 손해를 제한할 가능성

(Possibility of Avoiding Hazard or Limiting Harm)

- P1 : 특정의 조건하에서 가능 — 250mm/sec 미만
- P2 : 불가능 — 250mm/sec 이상



※ S/F/P의 기준은 ISO13849-1에 구체적으로 명시 되어있지 않으며, 위 기준은 예제를 위해, 임의로 설정한 값 입니다.

위험성 평가 기준 (ISO TR 14121)

[참조규격] ISO/TR 14121:2012

S : 상해의 심각도

- S1 : 경미한 상해 — 2일 이내 복귀가능
- S2 : 심각한 상해(후유증, 사망 등) — 2일 이내 복귀불가

F : 위험요인 노출 주기 및 지속기간

- F1 : 드문 경우/단기간 노출 — 1일 15분, 2회 미만
- F2 : 지속적 및 장기간 노출 빈번 — 1일 15분, 2회 이상

O : 위험 사고 발생 가능성

- O1 : 낮음 (충분한 기술, 증명 안전 어플리케이션)
- O2 : 중간 (6개월 이상 경험자의 부적절한 행동)
- O3 : 높음 (6개월 미만의 비 숙련자의 부적절한 행동)

A : 상해 회피 및 감소 가능성

- A1 : 특정의 조건하에서 가능 — 250mm/sec 미만
- A2 : 불가능함 — 250mm/sec 이상

		Risk index calculation					
		O1		O2		O3	
		A1	A2	A1	A2	A1	A2
S1	F1	1				2	
	F2						
S2	F1	2			3		4
	F2	3	4		5		6

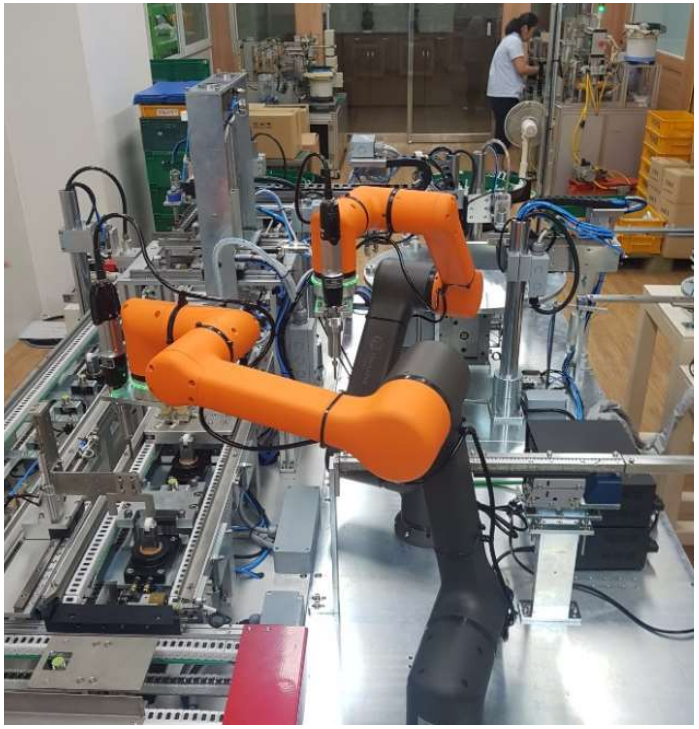
Figure 4 — Risk matrix equivalent to the risk graph in Figure 3

위험성 결정	위험수준	위험 관리 기준
1	저위험	해당 설비에 대하여 추가적인 위험감소 조치가 필요하지 않은 상태
2		해당 설비에 대하여 근로자에게 유해 위험정보 제공 및 정기 교육 실시
3	중위험	해당 설비에 대하여 근로자에게 유해 위험 대비 개인 보호구 제공
4		해당 설비에 대하여 경고, 위험 관리 대책이 필요하고, 추가안전보호 대책을 수립하여 개선이 필요한 상태
5	고위험	해당 설비에 대하여 접근 제한, 대체, 에너지 감소 및 개선이 필요한 상태
6		해당 설비를 즉시 정지 또는 위험요인을 제거시키며 작업을 지속하려면 설계 변경 등 즉시 개선이 필요한 상태

※ S/F/O/A의 기준은 ISO TR 14121에 구체적으로 명시 되어있지 않으며, 위 기준은 예제를 위해, 임의로 설정한 값 입니다.

위험성 평가 실습

◆ 위험성 평가 실습 예제1



설비 명: 볼트 체결 로봇

<설비조건>

<전기>
설비 공급전원: A.C 3Φ 220V, 60Hz, 850KVA
설비 정격전압: A.C 3Φ 220V, 60Hz
설비 구동모터의 용량: A.C 3Φ 550W

<기계/기구>
기구의 재질: 스테인리스, 철제
아무런 방호대책을 하지 않은 초기 설치 단계
자동모드 동작 속도는 800mm/sec

(1) 제품 별 설비 개조	1회 (10분)/week
(2) 워크 확인	1회 (5분)/1hour
(3) 정기 유지 보수	1회 (60분)/month

※전기, 기계/기구 부 외 위험 요인에 대해서는 고려하지 않으며,
본 사진 외 다른 별도의 안전대책은 적용되어 있지 않음.

위험성 평가 실습

위험성 평가

No	작업내용	위험한 사건	잠재적 결과	위험성 추정				RI	PLr
				S	F	O	A		
1									
2									
3									

위험성 평가 실습

위험성 감소

No	위험한 사건	위험성 감소 대책	위험성 재추정				RI
			S	F	O	A	
1							
2							
3							

위험성 평가 실습

위험성 평가

No	작업내용	위험한 사건	잠재적 결과	위험성 추정				RI	PLr
				S	F	O	A		
1	초기 설치 중	뾰족하고, 날카로운 부분에 신체의 일부가 부딪혀 관통되는 경우 초기 설치 중 절단기에 손가락이 끼는 경우	절단, 찔림	2	2	3	1	5	d
2	제품 생산 중	회전하는 구동부에, 신체의 일부가 말려들어가는 경우	말림, 압착	2	1	3	2	4	d
3	제품별 개조상황	개조 상황에 예기치 못한 기동으로, 신체의 일부가 말려들어가거나, 기동 된 전단기에 손가락이 끼는 경우	절단, 압착	2	1	3	2	4	d

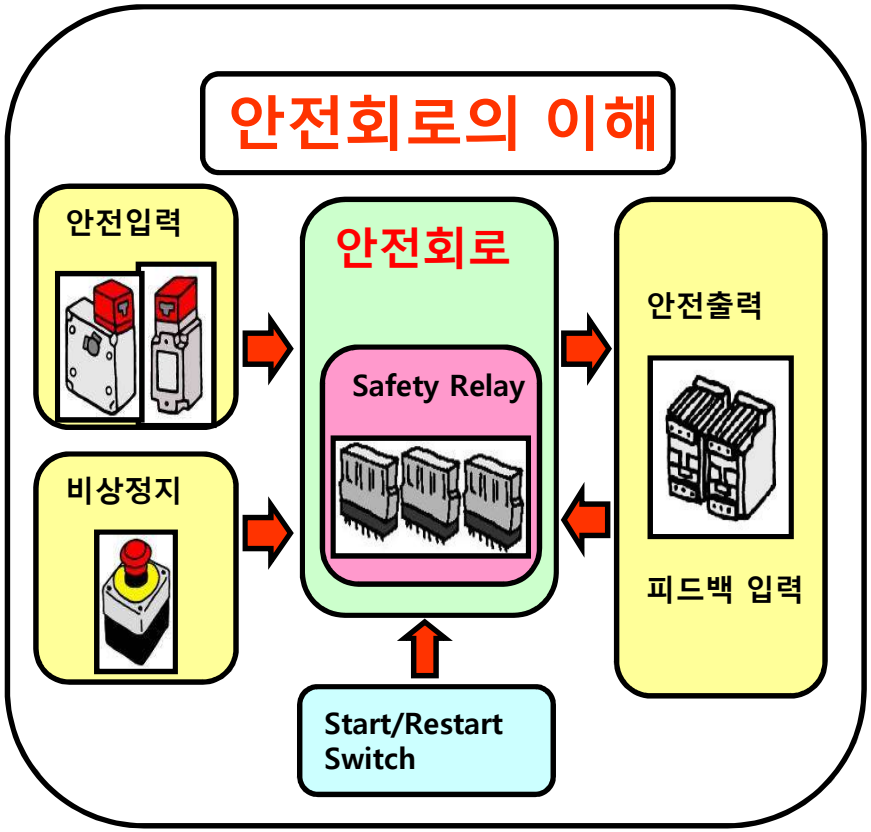
위험성 감소

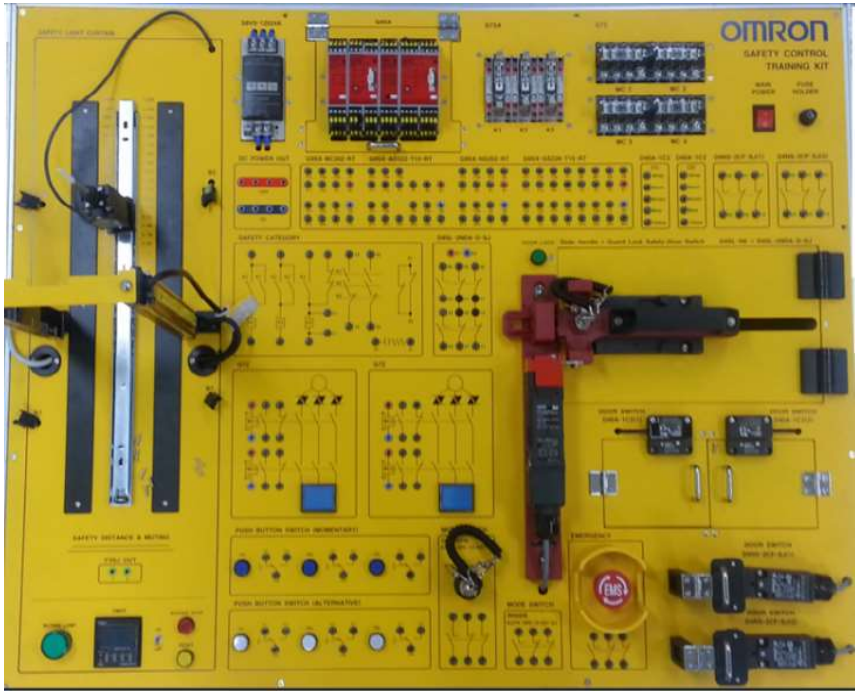
No	위험한 사건	위험성 감소 대책	위험성 재추정				RI
			S	F	O	A	
1	뾰족한 부분에, 신체의 일부가 부딪혀 관통되는 경우 초기 설치 중 절단기에 손가락이 끼는 경우	Step 1. 뾰족한 부분을 공정을 해치지 않는 선에서, 가공하여 위험성을 감소한다. 가공하는 선에서 충분히 위험성이 해소되지 않을 경우, 추가 방호 대책을 실시한다. Step 2-1. 절단, 찔림, 압착, 말림의 위험성을 감소하기 위해, 위험요인과 작업자를 분리할 수 있는, 펜스를 설치하고 펜스 문이 열릴 경우, 구동부가 멈출 수 있도록 연동식 가드를 설치한다. Step 2-2. 연동식 가드 조치 후에 남은 잔존위험성에 관해서는 비상정지 스위치를 두어, 추가적 보호조치를 실시한다. Step 2-3. 설비내부로 들어가서, 티칭작업이 필요할 경우, 3 포지션(Enable) SW를 적용하여, 250mm/sec의 속도로 티칭하도록 한다. Step 3. 안전 방호대책 및 연동식 가드의 사용법에 관한, 매뉴얼을 비치하고, 관련 교육을 실시한다.	2	1	1	1	2
2	회전하는 구동부에, 신체의 일부가 말려들어가는 경우		2	1	1	1	2
3	개조 상황에 예기치 못한 기동으로, 신체의 일부가 말려들어가거나, 기동 된 전단기에 손가락이 끼는 경우		2	1	1	1	2

로봇 시스템 안전방호 구성 및 어플리케이션 실습

한국로봇산업협회
Korea Association of Robot industry

세이프티 DEMO KIT 구성



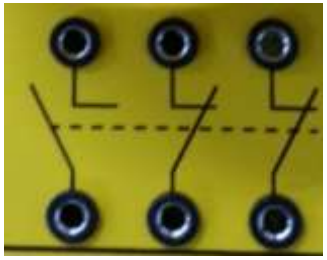
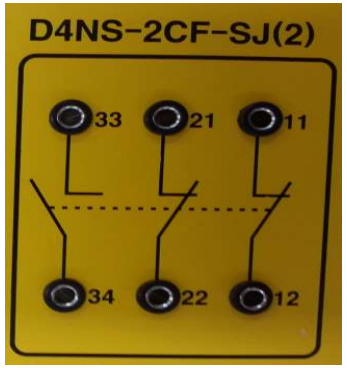


목표

- 세이프티 실습 DEMO KIT 구성을 확인한다.

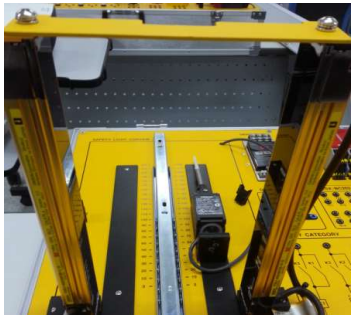
세이프티 DEMO KIT 구성

1.입력 기기 종류

이 름	모 양	접점 구성도	기기 역할
비상 정지 스위치			위험 발생 시 스위치를 조작하면 위험 원의 전원을 차단하여 설비를 정지 시킨다.
일반타입 세이프티 도어 스위치			일반 도어 스위치이며 설비 내 도어 개폐 검지를 한다.

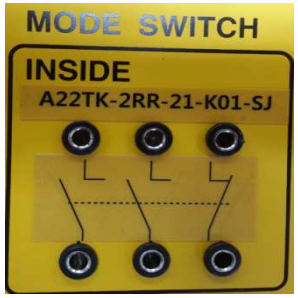
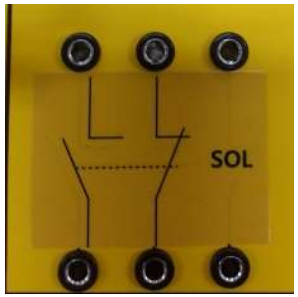
세이프티 DEMO KIT 구성

1.입력 기기 종류

이 름	모 양	접점 구성도	기기 역할
락 타입 세이프티 도어 스위치			세이프티 락 도어 스위치이며 설비가 기동 시 도어 락이 ON 되어 도어를 열 수 없다.
세이프티 라이트 커튼			인체 감지용 세이프티 라이트 커튼이며 차광 시 안전 출력이 OFF 된다.

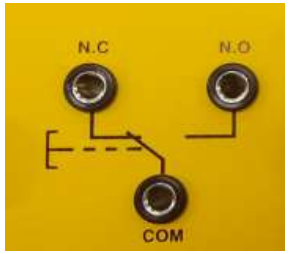
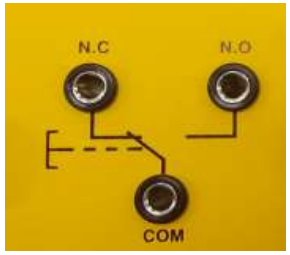
세이프티 DEMO KIT 구성

1.입력 기기 종류

이 름	모 양	접점 구성도	기기 역할
세이프티 모드 변환 키 스위치 (내부)			설비 내부에서 정상 동작 모드(AUTO 모드) 또는 유지 보수 동작 모드를 (TEACH 모드) 선택하기 위한 세이프티 모드 변환 키 스위치이다.
세이프티 락 모드 변환 키 스위치 (외부)			설비 외부에서 정상 동작 모드(AUTO 모드) 또는 유지 보수 동작 모드를 (TEACH 모드)선택하며 유지 보수 모드 시 락을 할 수 있는 모드 변환 키 스위치이다.

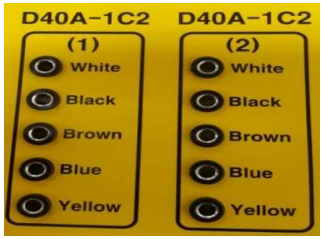
세이프티 DEMO KIT 구성

1.입력 기기 종류

이 름	모 양	접점 구성도	기기 역할
PUSH 스위치 (MOMENTARY)			PUSH 스위치이며 MOMENTARY 타입으로 스위치 조작 시 접점이 변경되었다가 스위치 조작을 멈추면 접점이 복귀하는 스위치이다.
PUSH 스위치 (ALTERNATIVE)			PUSH 스위치이며 ALTERNATIVE 타입으로 스위치 조작 시 변경된 접점이 유지되었다가 다시 조작 했을 때 복귀하는 스위치이다.

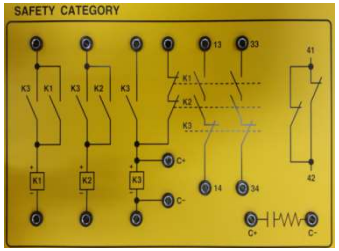
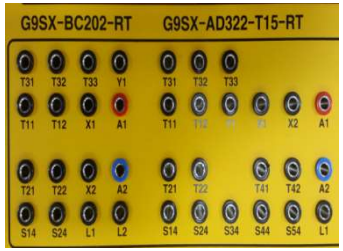
세이프티 DEMO KIT 구성

1.입력 기기 종류

이 름	모 양	접점 구성도	기기 역할
비 접촉 도어 스위치			비 접촉 도어 스위치이며 설비 내 도어 개폐 검지를 한다.

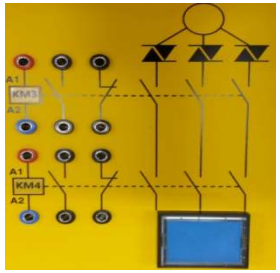
세이프티 DEMO KIT 구성

2.제어 기기 종류

이 름	모 양	접점 구성도	기기 역할
세이프티 릴레이			세이프티 릴레이를 활용하여 안전 카테고리 구성 실습을 한다.
세이프티 컨트롤러			G9SX 안전 컨트롤러를 활용하여 실제 설비에 적용되는 안전 회로 구성 실습을 한다.

세이프티 DEMO KIT 구성

3.출력 기기 종류

이 름	모 양	접점 구성도	기기 역할
MC			제어 기기의 안전 출력을 입력으로 받아 파란색 LED를 ON/OFF 하여 동작 유무 확인이 가능하다.

세이프티 DEMO KIT 구성

4.기타

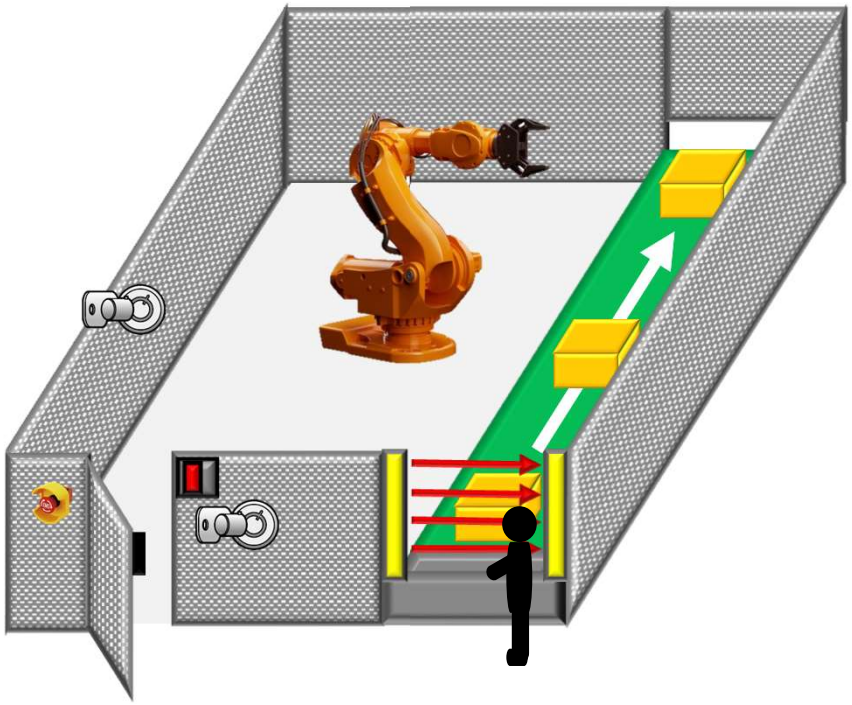
이 름	모 양	기기 역할
배선 케이블		안전 입력 기기 또는 안전 컨트롤러의 출력을 릴레이나 제어기기에 결 선 시 사용하는 배선 케이블 이다.

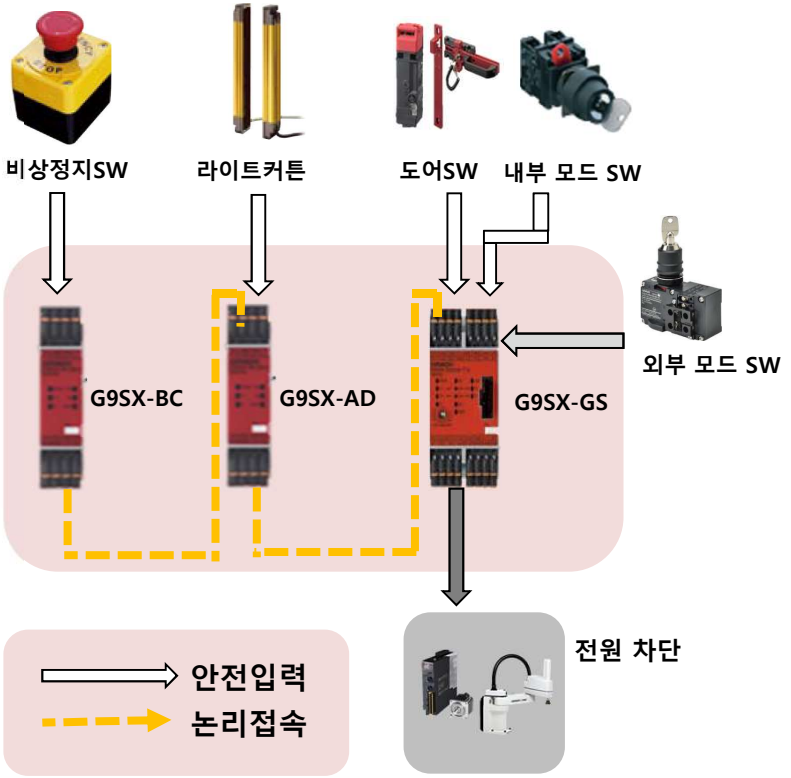
데모기를 이용한 어플리케이션 배선 실습

☑ 안전 방책 모드 변환 어플리케이션

데모키트를 활용하여, 안전 방호 대책을 적용한 전체 시스템

*** 유지보수 모드 변경(외부Key) + (내부Key) 변경 시 ☞ 도어SW 무효화 (비상정지SW, 라이트커튼은 정상 동작)**

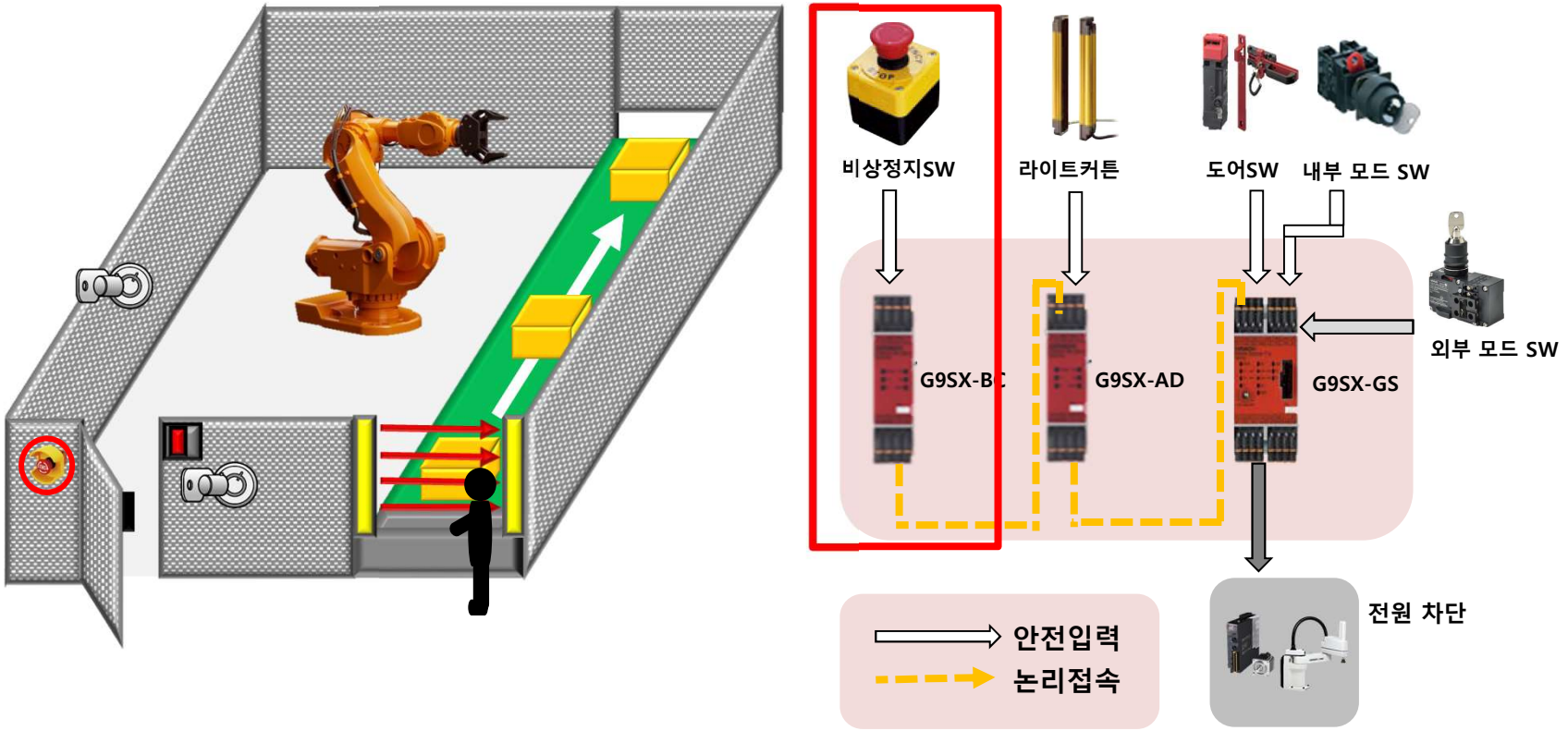




데모기를 이용한 어플리케이션 배선 실습

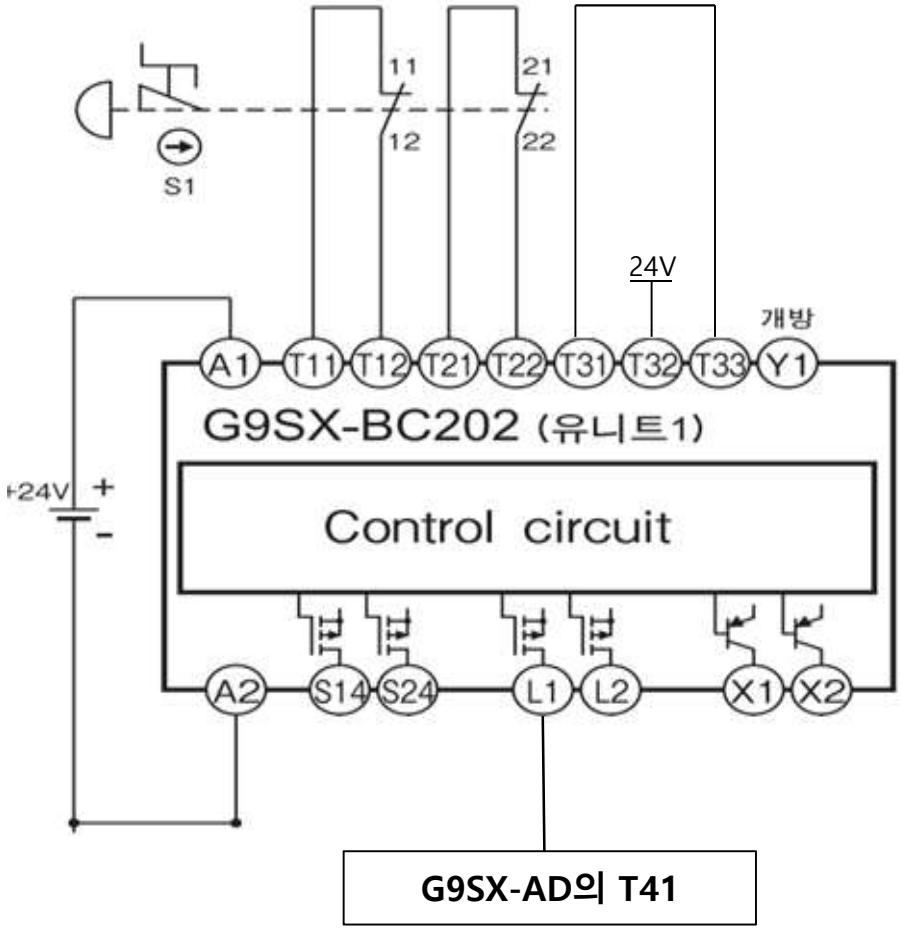
1-1. 비상정지 스위치 적용

로봇의 작동 및 유지보수 중 위험 상황이 발생하였을 때, 비상정치 스위치를 눌러야 한다.
비상정지 스위치 동작 시 로봇의 출력은 최우선적으로 즉시 OFF 된다.

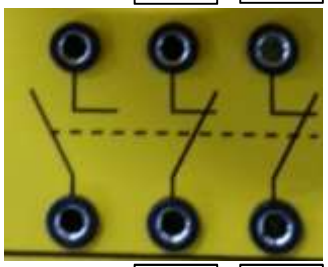


데모기를 이용한 어플리케이션 배선 실습

1-2. 비상정지 스위치 배선도

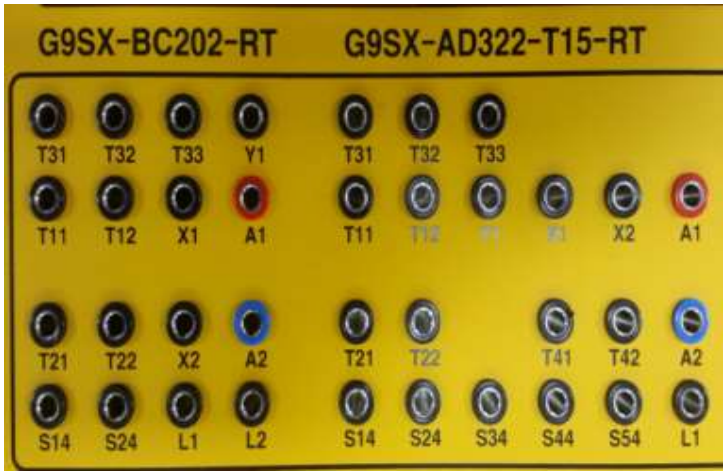


비상정지SW



G9SX-BC

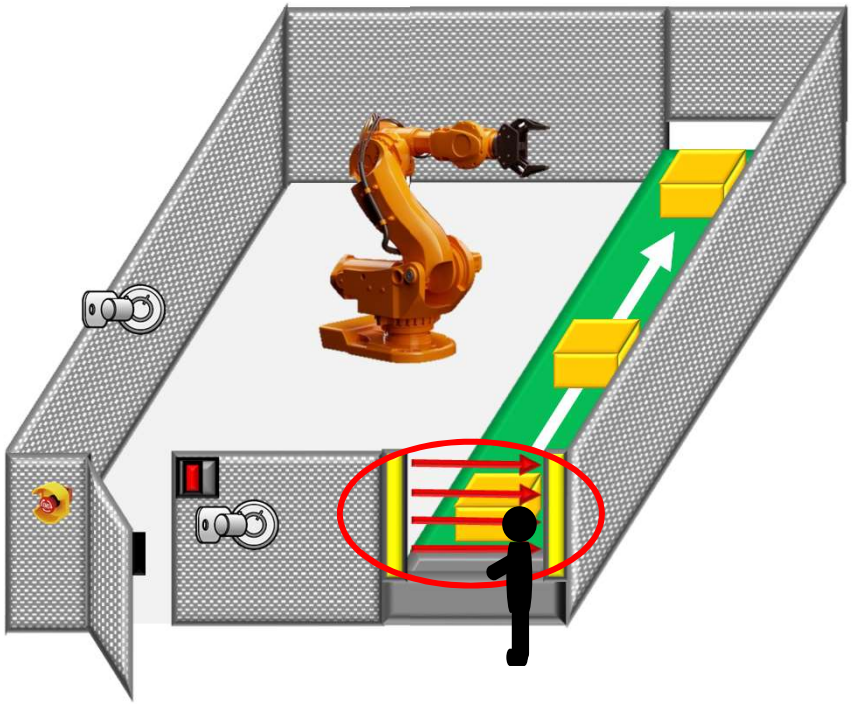
G9SX-AD

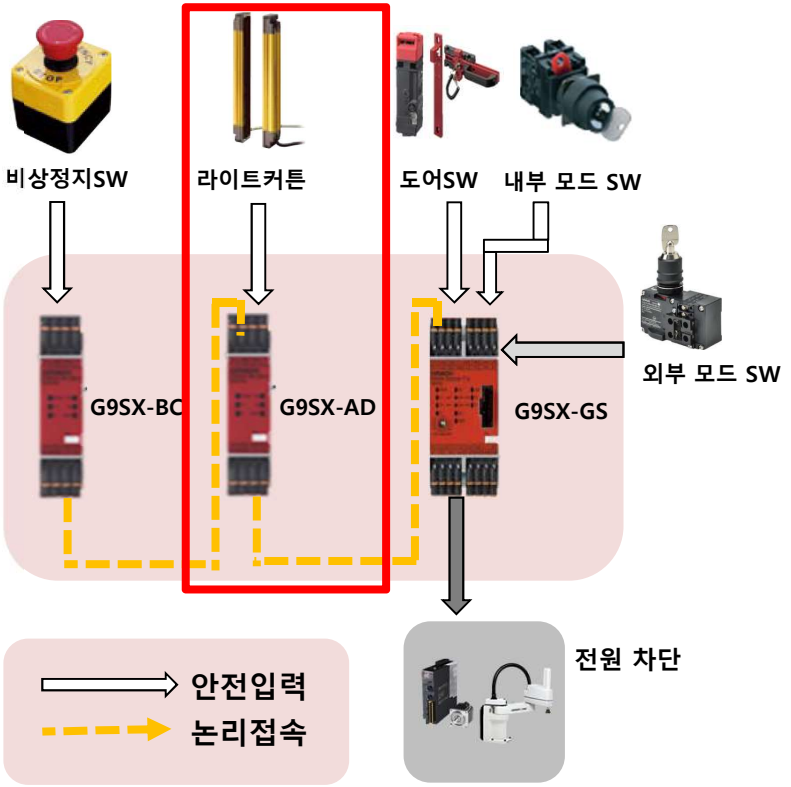


데모기를 이용한 어플리케이션 배선 실습

2-1 Safety 라이트 커튼 적용

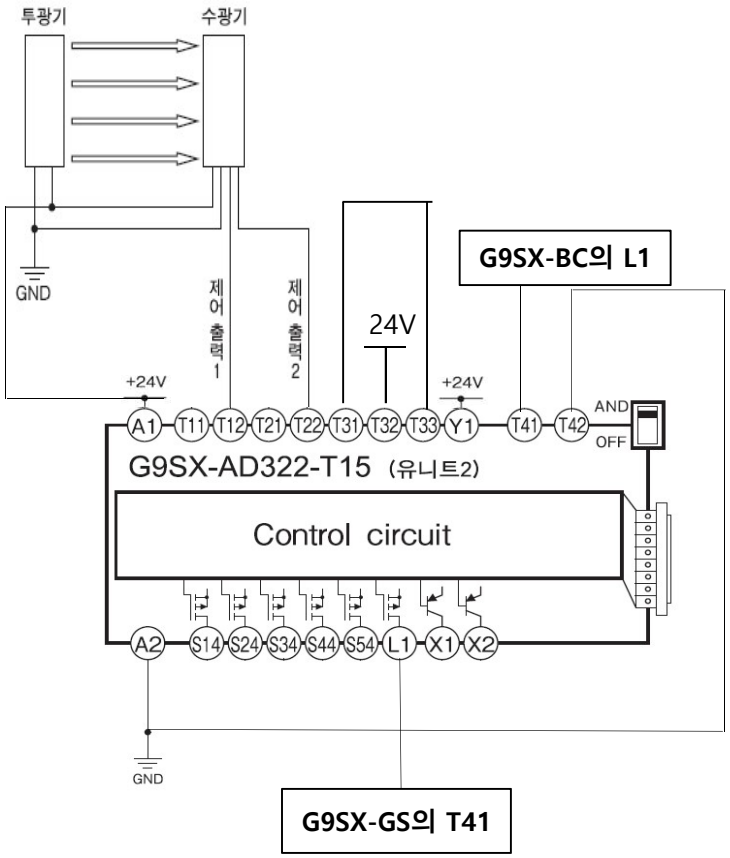
로봇 운전 중, 제품 투입부 부분에 뮤팅 조건없이 라이트 커튼이 차광될 경우,
로봇의 출력은 즉시 OFF 된다.



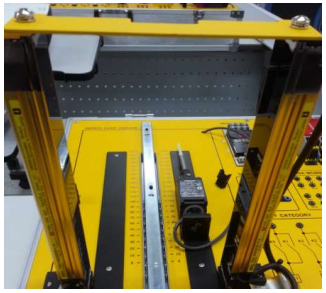


데모기를 이용한 어플리케이션 배선 실습

2-2 Safety 라이트 커튼 배선도

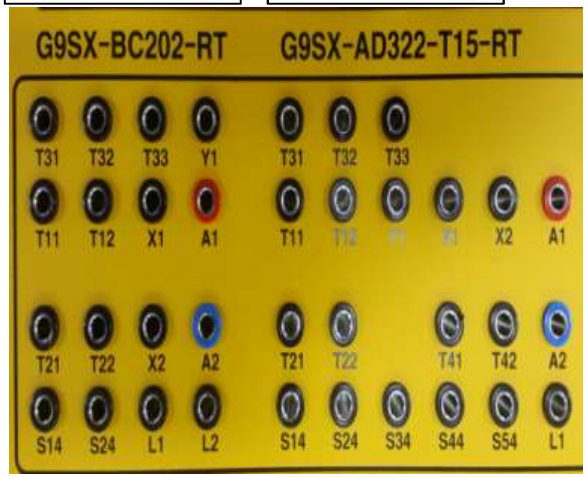


라이트커튼



제어출력1 제어출력2

G9SX-BC G9SX-AD

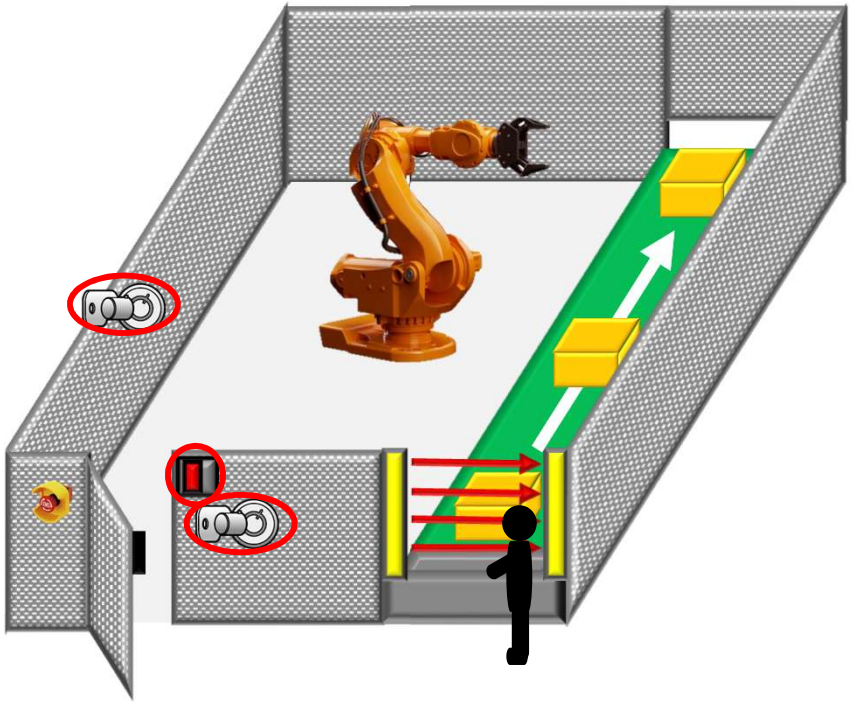


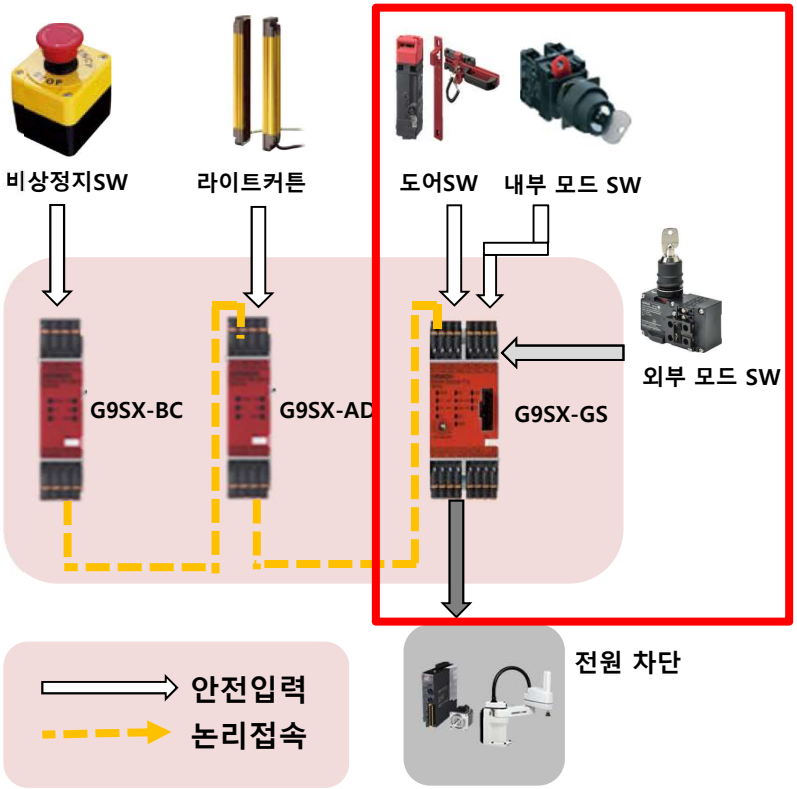
G9SX-GS

데모기를 이용한 어플리케이션 배선 실습

3-1. 도어 스위치 및 내부/외부 Key 적용

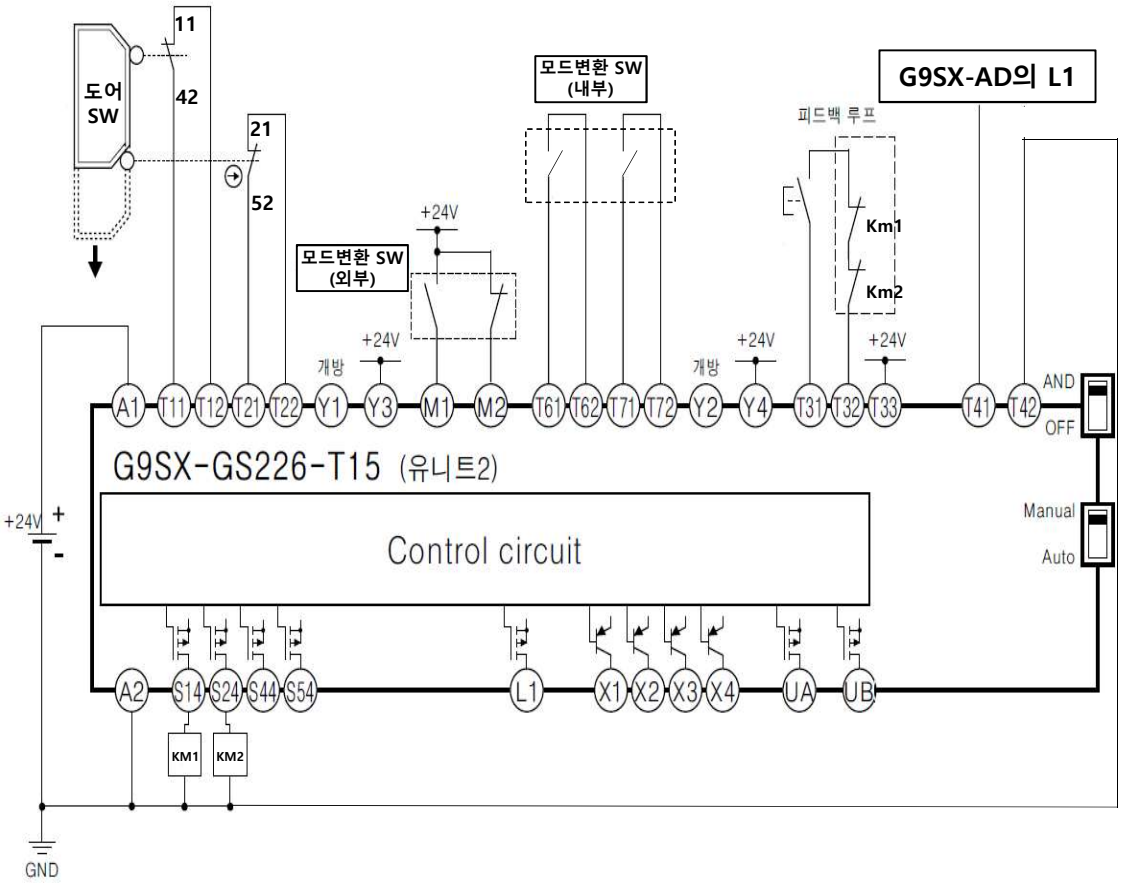
로봇 작동 중에 안전 펜스의 출입구인 도어가 OPEN될 경우, 로봇의 출력은 즉시 OFF 된다.
단, 유지보수 모드로 변경 후 내부키 삽입시에는 로봇을 동작 시킬 수 있다.
유지보수 모드 변경(외부Key) + (내부Key) 변경 시 ☞ 도어SW 무효화 (비상정지SW, 라이트커튼은 정상 동작)



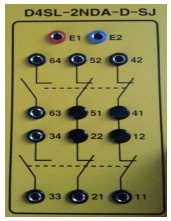


데모기를 이용한 어플리케이션 배선 실습

3-2. 도어 스위치 및 내부/외부 Key 배선도

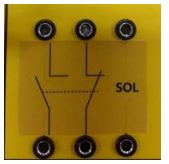


도어 SW



모드(내부)

모드(외부)



G9SX-GS

세이프티 라이트 커튼 안전거리 실습

목표

- 라이트 커튼 설치 시 안전 거리를 고려해서 설치해야 하는 이유를 실습을 통해 알아본다.

라이트 커튼 안전 거리 실습 준비

1. 라이트 커튼을 세운다.
2. 리미트 스위치를 설치한다.
3. 하단부 타이머의 토클 스위치를 ON한다.

1.

2.

3.

라이트 커튼 안전 거리 실습 방법

1. 설비의 정지 시간을 측정하여 임의의 시간을 타이머에 설정한다.

2. 리미트 스위치와 라이트 커튼의 거리를 설정한다.

3. 타이머 옆의 리셋 스위치를 누른다.

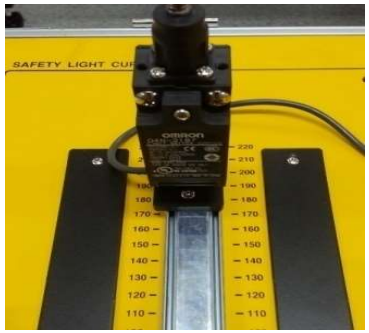
4. 안전한 거리를 알맞게 설정하였는지 확인하기 위하여 라이트 커튼에 손을 넣어 리미트 스위치를 터치한다.

► 벨이 울리지 않는다 = 리미트 스위치에 손이 닿기 전에 라이트 커튼의 안전 출력이 OFF 되었기 때문에 안전거리는 충분하게 이격된 상태이다.

► 벨이 울렸다 = 리미트 스위치에 손이 닿을 때까지 라이트 커튼의 안전 출력이 OFF 되지 않았기 때문에 안전거리는 충분하게 이격된 상태가 아니다.

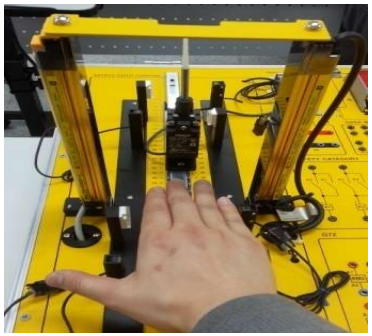
1.

2.



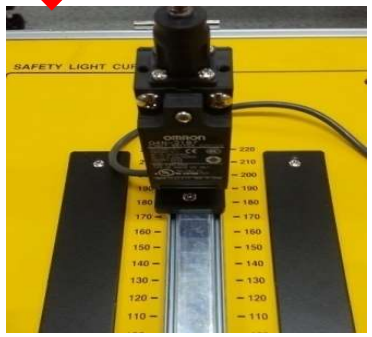
3.

4.

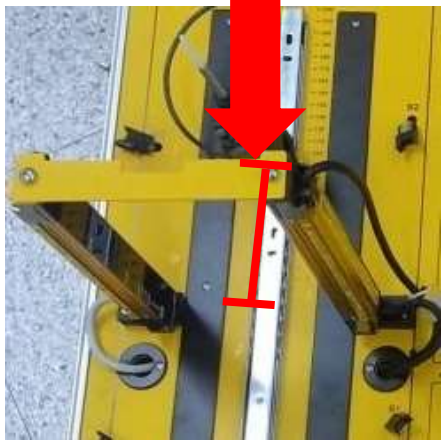


라이트 커튼 안전 거리 실습 준비

안전 거리 측정 실습 도구가 가지는 의미



위험원의 최대동작영역과 라이트 커튼사이의 최단거리 = 리미트 스위치의 위치



안전거리 = 라이트 커튼에서 리미트 스위치 까지의 거리

로봇 제어 시스템 기능안전(PL) 적용

KAR 한국로봇산업협회
Korea Association of Robot industry

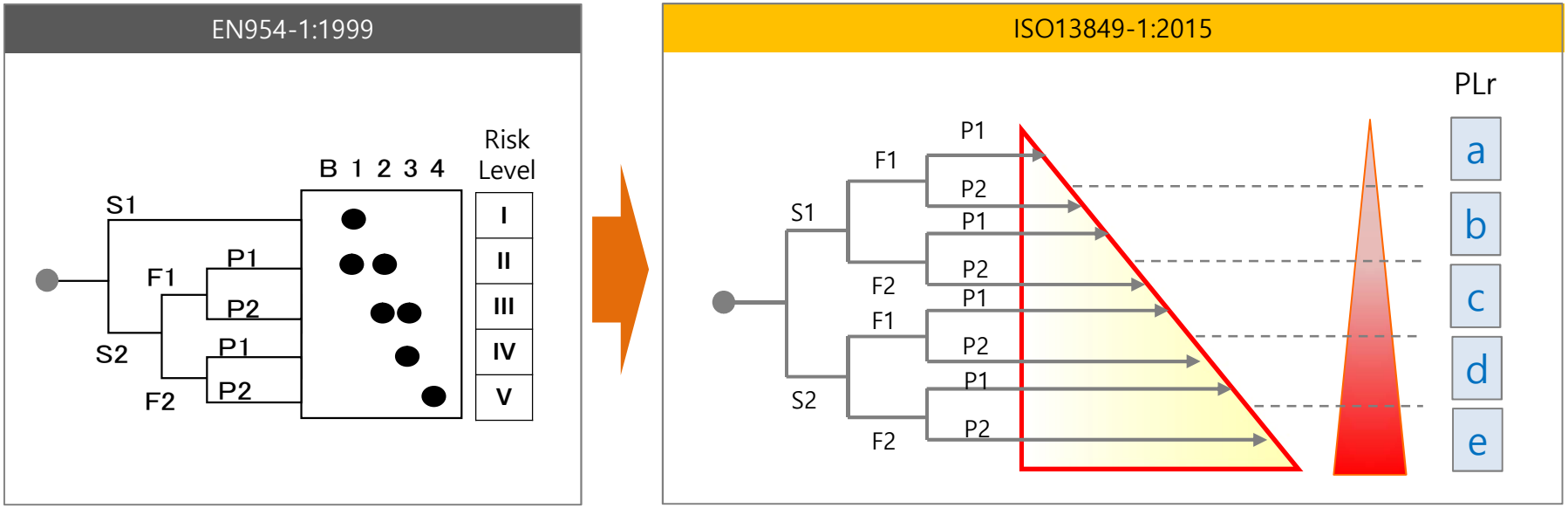
ISO13849-1의 개요

ISO 13849-1:2015

ISO13849-1 개정 포인트

과거에는 안전 성능을 평가할 때 위험수준에 따라 Safety Category 개념으로 안전 수준을 결정하였습니다. 이 원칙은 EN954-1:1999에 도입되었으며, ISO13849-1의 전신이기도 합니다.

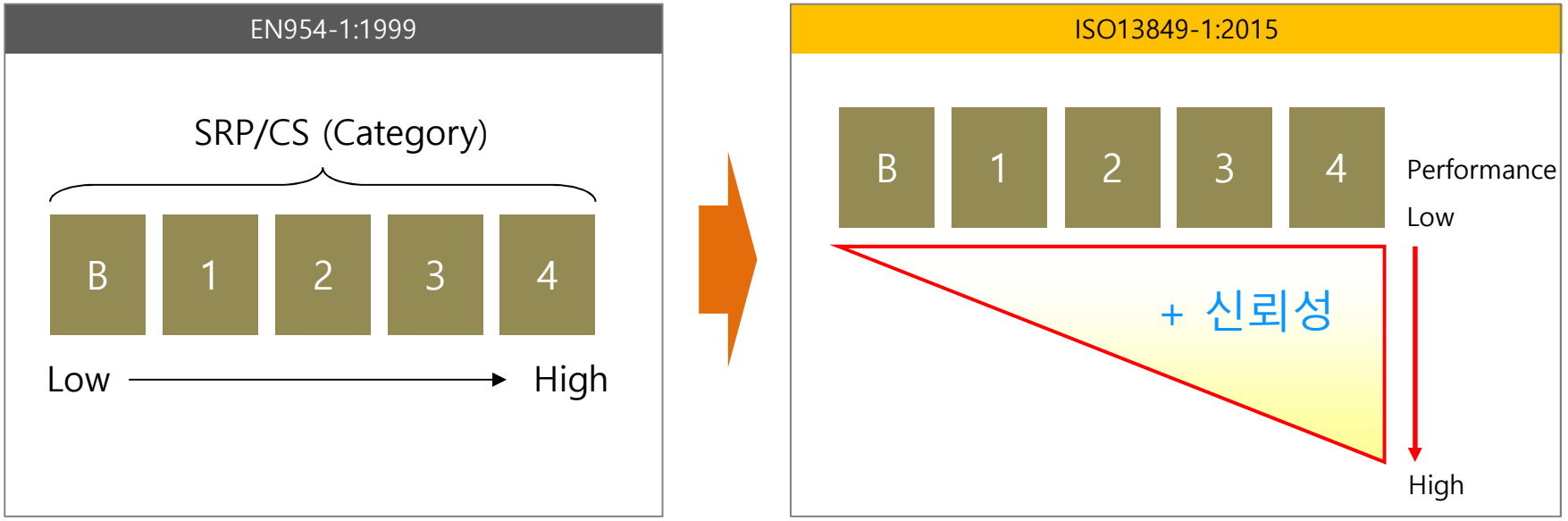
평가 방법은 Safety Category뿐 아니라 표준에 따른 매개 변수를 포함하여 새로 채택 된 성능 수준으로 변경되었습니다. ISO13849-1은 EN954-1보다 명확하고 안전 수준을 적절히 평가하기 위한 방법을 제시합니다.



ISO13849-1 개정 포인트

EN954-1에 제시된 평가 방법은 확정론적인 기법에 바탕을 둡니다. 그러나 ISO13849-1에는 추가적인 확률론적 접근법이 포함되어 있습니다.

예를 들어 EN954-1은 안전 시스템의 구조적 평가만을 기반으로 하는 반면 ISO13849-1은 구조적 특징 뿐만 아니라 시스템 요소의 고장 위험까지의 수명을 고려합니다. 이것은 시스템 평가에서 보다 신뢰할 수 있는 부분입니다.

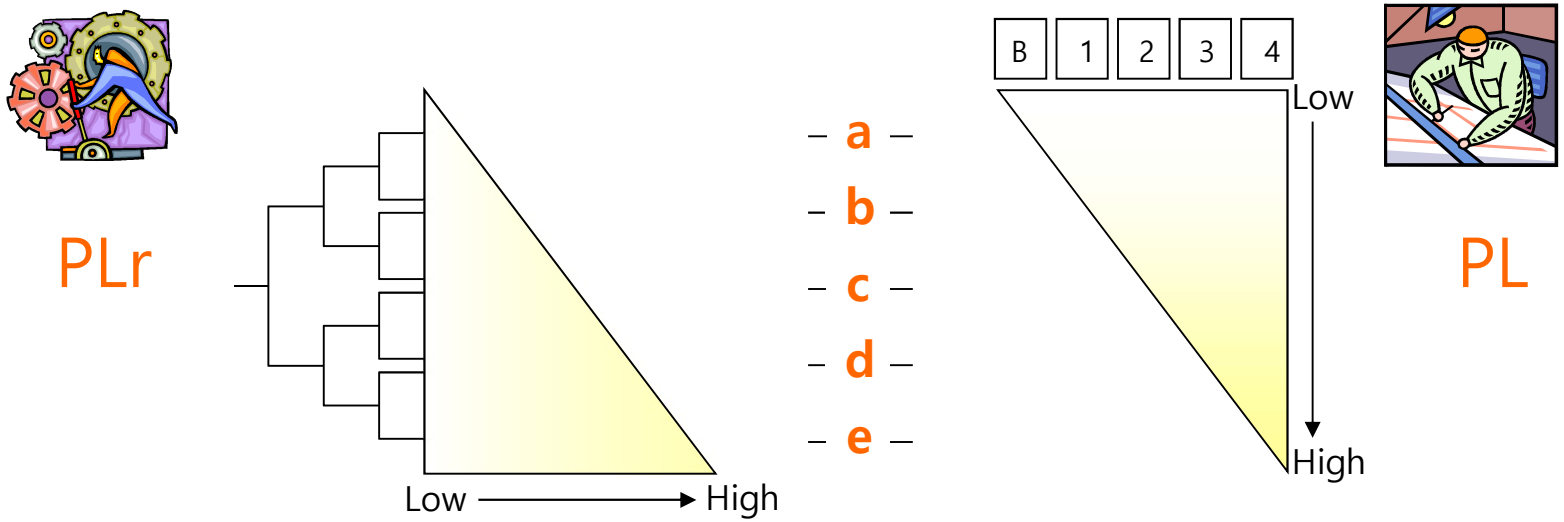


PL과 PLr의 관계

평가 시 리스크 수준에 따른 안전 제어 시스템의 성능 평가는 "a"에서 "e"까지 총 5단계로 나누어 지게 됩니다.

PLr (Required Performance Level)- 최소한의 요구되어지는 안전 성능

PL (Performance Level)- 안전 성능의 평가 수준

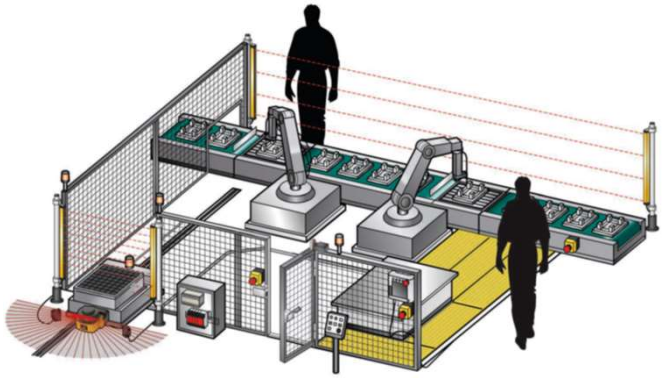


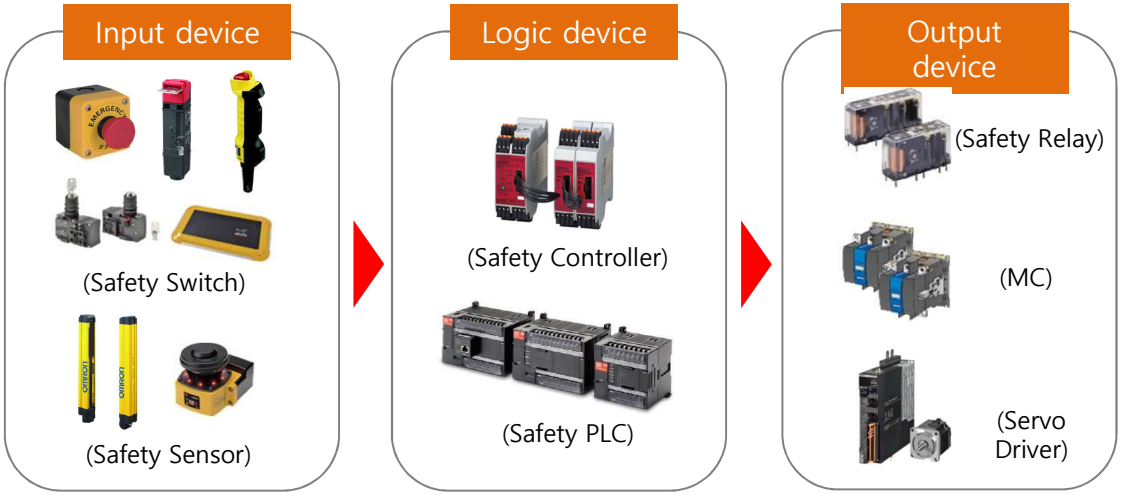
PLr≦PL

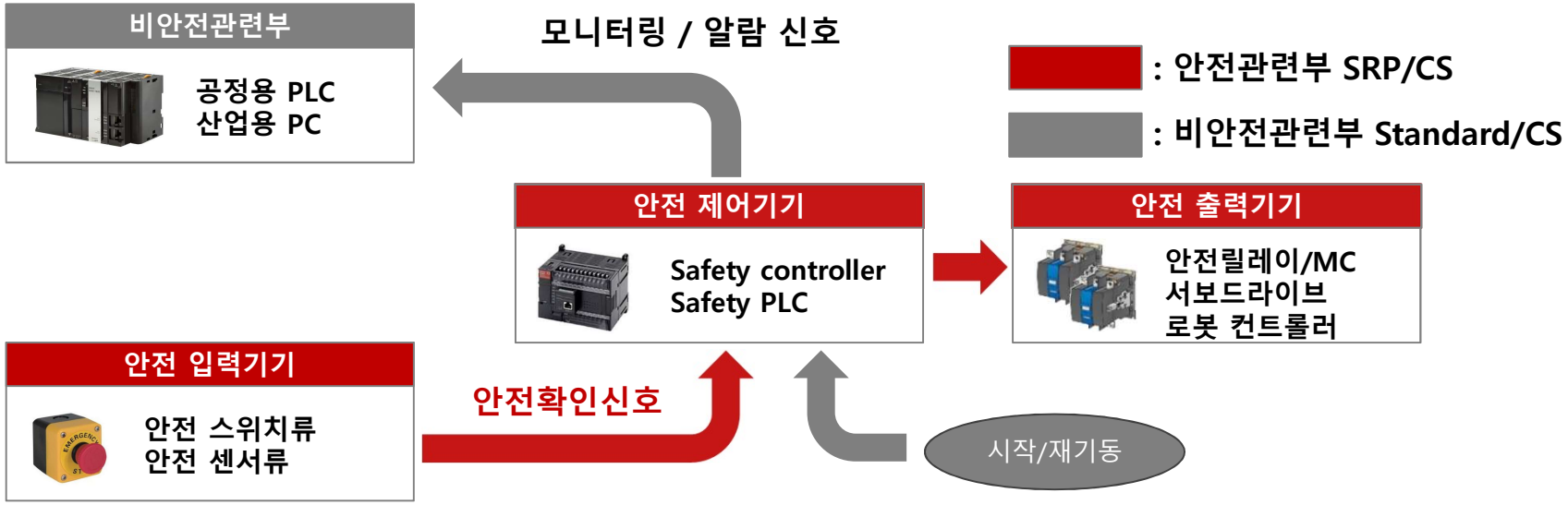
안전 제어 시스템의 성능 수준은(PL) 항상 최소로 요구되는 성능 수준(PLr)보다 크거나 같아야 합니다.

ISO13849-1의 컨셉

I, L, O를 하나의 채널 또는 시스템으로서 구성하였을 때 얼만큼의 안전 성능이 보장될 수 있는지를 평가해야 합니다.

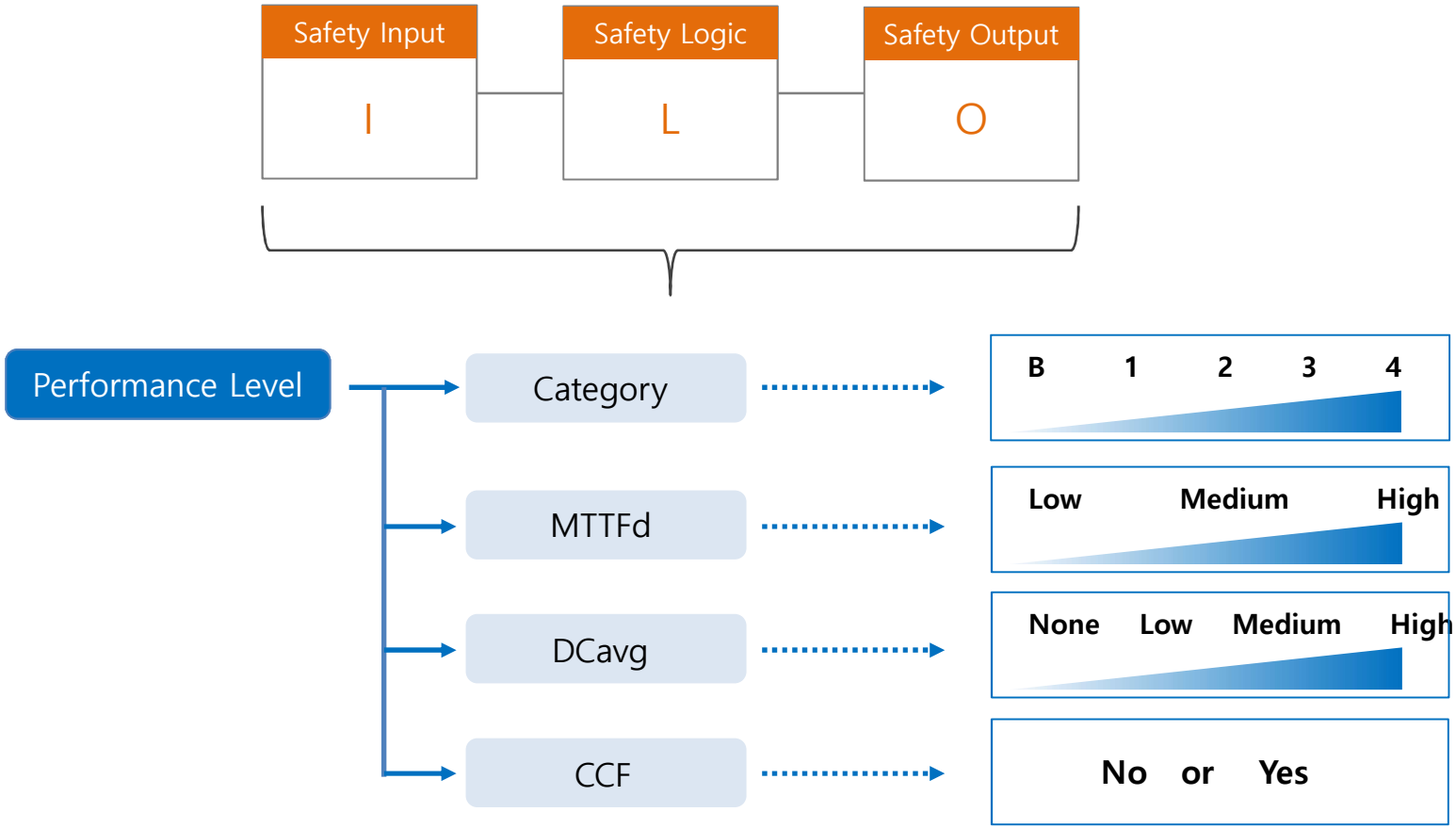






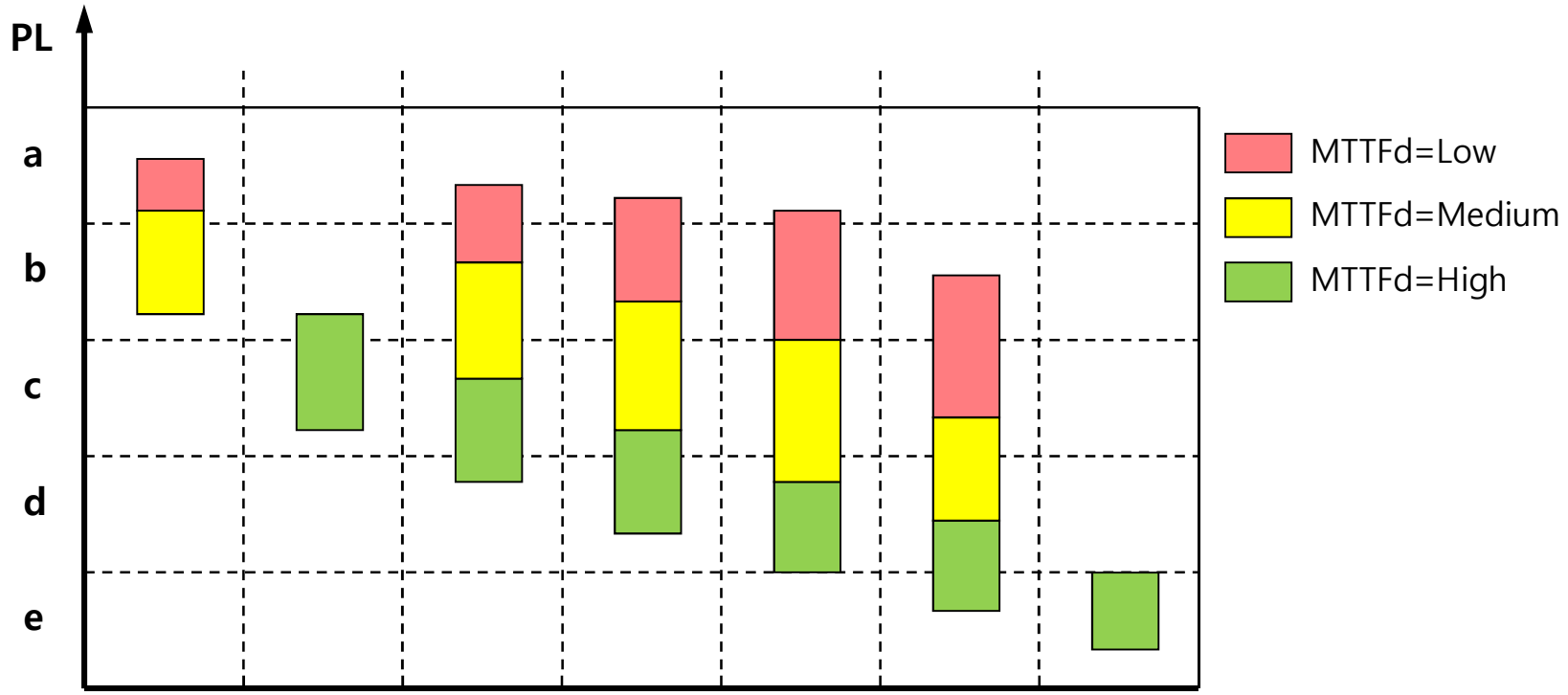
PL의 이해

- I, L, O의 연결을 하나의 채널로 인식하고 단을 채널을 기준으로 PL을 평가합니다.
- PL을 평가하기 위한 4개의 변수가 있으며, 최종 PL은 각 평가 결과의 조합에 의해 결정됩니다.



PL의 평가

Figure 5 — Relationship between categories, DC_{avg}, $MTTF_D$ of each channel and PL



Safety Cat.	Cat.B	Cat.1	Cat.2	Cat.2	Cat.3	Cat.3	Cat.4
DC average	None	None	Low	Medium	Low	Medium	High

PL의 평가

PL 매개 변수

하드웨어적 구조

Category → 카테고리는 특정 PL을 달성하는데 사용되는 기본 변수입니다. 안전 제어 시스템의 구조를 정의 합니다.

위험측 고장이 나기까지의 시간

$MTTF_D$

① 부품 단위
1) MTTFd from maker
2) Annex C & B10d

$$MTTFd = \frac{B10d}{0.1 \times Nop}$$

- B10d
- Nop

기계 설계자가 Nop의 변수 파악 필요!

② 시스템

$$MTTFd = \frac{1}{\sum_{i=1}^{n} \frac{1}{MTTFdi}}$$

시스템의 신뢰성

DCavg

① 부품 단위
1) Select DC in Annex E

- DC
- MTTFd

컨트롤러가 카테고리 구조를 만족하면 더 쉽게 달성 할 수 있습니다.

② 시스템

$$DCavg = \frac{\sum_{i=1}^{n} \frac{DCi}{MTTFdi}}{\sum_{i=1}^{n} \frac{1}{MTTFdi}}$$

디자인의 확실성

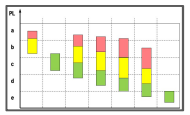
CCF → 부속서 F 체크리스트에서 65점 이상 확보

1)EMC
2)Procedure of design
3)Analysis of fault

관련 내용에 확인 필요!

평가

- B, 1, 2, 3, 4 (5가지 항목)
- High, Medium, Low (3가지 항목)
- High, Medium, Low, None (4가지 항목)
- No or Yes (2가지 항목)



안전 카테고리 (Category)

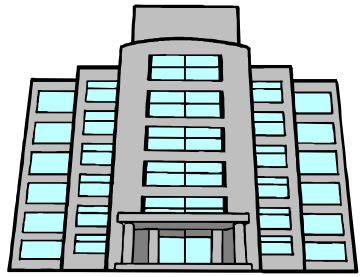
- 안전 카테고리:
  - 제어 시스템의 안전 관련부의 구조

예 :「비바람을 막을 수 있는 공간」

텐트

목조주택

오피스 빌딩



안전 카테고리 (Category)

안전 카테고리는 안전 시스템의 구조를 결정하는 첫번째 매개변수 입니다.
기본적으로 카테고리의 결과 값이 높으면 고 성능의 안전 제어 시스템 수준에 도달이 유리해집니다.
따라서 안전 제어 시스템을 설계 하는 데에 있어서 매우 중요한 단계입니다.

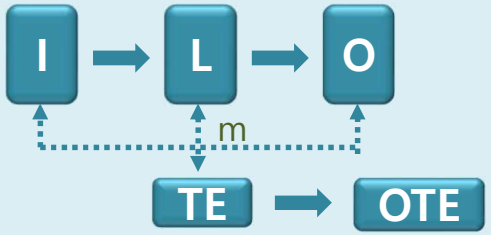
Category B, 1

카테고리 B는 기본 카테고리입니다. 고장이 발생하면 안전 기능이 손실될 수 있습니다. 카테고리 1에서 고장에 대한 개선된 저항은 주로 구성요소의 선택 및 적용에 의해 달성 됩니다.

Category 2

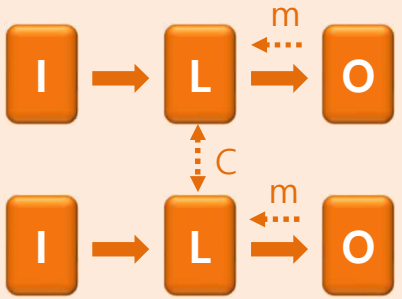
카테고리 2에서는 지정된 안전 기능이 수행되고 있는지 주기적으로 점검하여 제공됩니다.

TE: 점검 기기
OTE: 점검 결과의 출력



Category 3, 4

카테고리 3과 4에서 단일 고장으로 인해 안전기능이 손실되지 않도록 보장합니다.
카테고리 4에서는 카테고리 3에서 합리적으로 실행 가능할 때마다 이러한 결함이 감지 됩니다.
카테고리 4에서는 결함 축적에 대한 저항이 지정됩니다.



카테고리 B

➢ 카테고리 구조

I → L → O

- I : 입력 기기
- L : 제어 기기
- O : 출력 기기

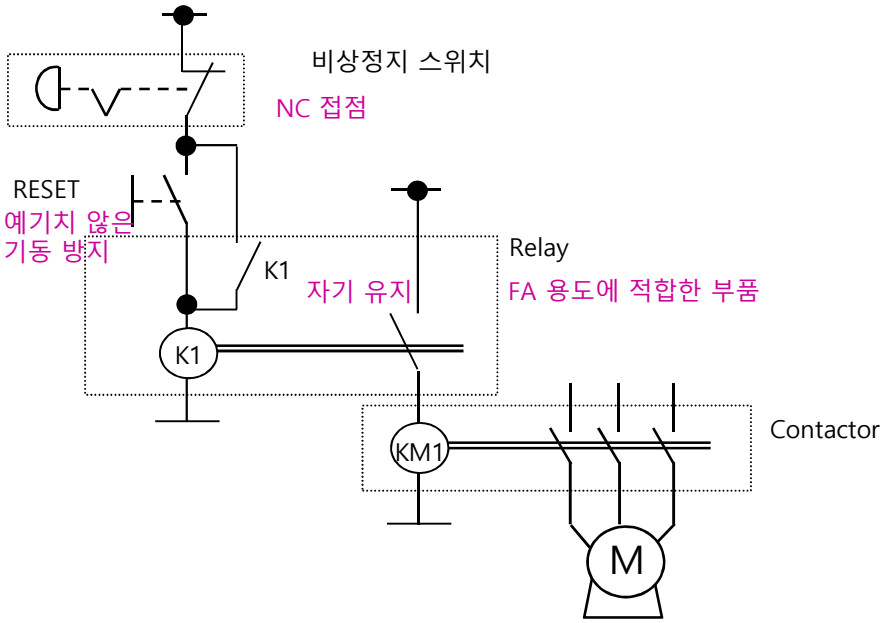
SRP/CS는 최소한 관련 표준에 따라 설계, 구성, 선택, 조립 및 결합되어야 하며, 예상되는 작동 응력, 가공된 재료의 영향, 기타 관련성을 견딜 수 있도록 특정 적용에 대한 기본 안전 원칙을 사용해야 합니다. 외부 영향 예) 진동, 차단용량, 전원 공급 장치

※ 카테고리 B의 특징

✓DC 값 없음(DCavg=None)
✓각 채널의 $MTTF_D$ = Low – Medium
✓CCF 고려사항 없음
✓최대 달성가능 PL → PLb
✓고장 발생으로 안전 기능 손상

예시)

안전 기능의 목적에 적합



안전 시스템이 반드시 갖추어야할 기능 조건에 충실하지만 각 구성 요소는 해당 기능에 대해 신뢰할 수 없습니다. 따라서 구성 요소 장애로 인해 시스템 손상이 발생할 수 있으므로 장애를 보상하거나 모니터할 수 있는 시스템이 필요합니다.

카테고리 1

➢ 카테고리 구조

I → L → O

- I : 입력 기기
- L : 제어 기기
- O : 출력 기기

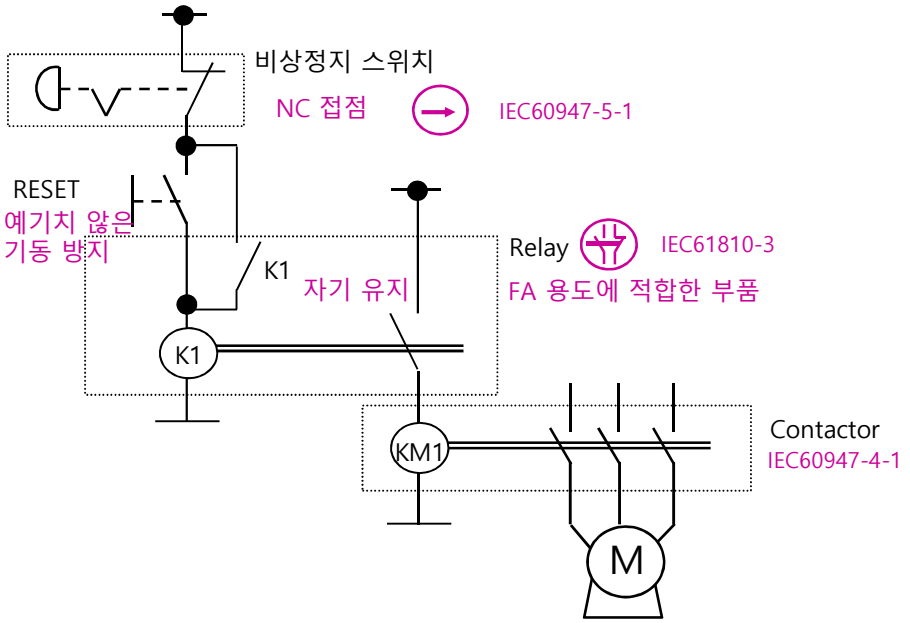
카테고리 1의 경우 카테고리 B의 6.2.3에 따른 요구 사항과 동일한 요구사항이 적용됩니다. 카테고리 1의 SRP/CS는 충분히 검토된 부품과 안전 원칙을 사용하여 설계 및 구성되어야 합니다.

※ 카테고리 1의 특징

✓DC 값 없음(DCavg=None)
✓각 채널의 $MTTF_D$ = High
✓CCF 고려사항 없음
✓최대 달성가능 PL → PLc
✓고장 발생으로 안전 기능 손상

예시)

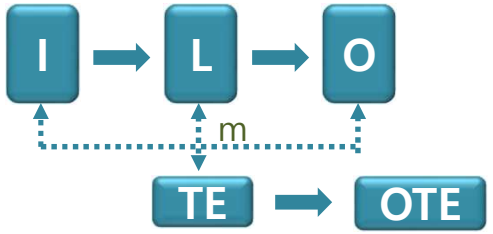
충분히 검증된 안전 원칙



각 구성 요소에는 안전 시스템에 적용할 수 있는 고유한 기능 신뢰성이 있습니다.
그러나 단일 채널로 구성되므로 카테고리 1 내에서 단일 고장에 대한 복구를 할 수는 없습니다.

카테고리 2

➢ 카테고리 구조



- TE: 점검 기기
- OTE: 점검 결과의 출력

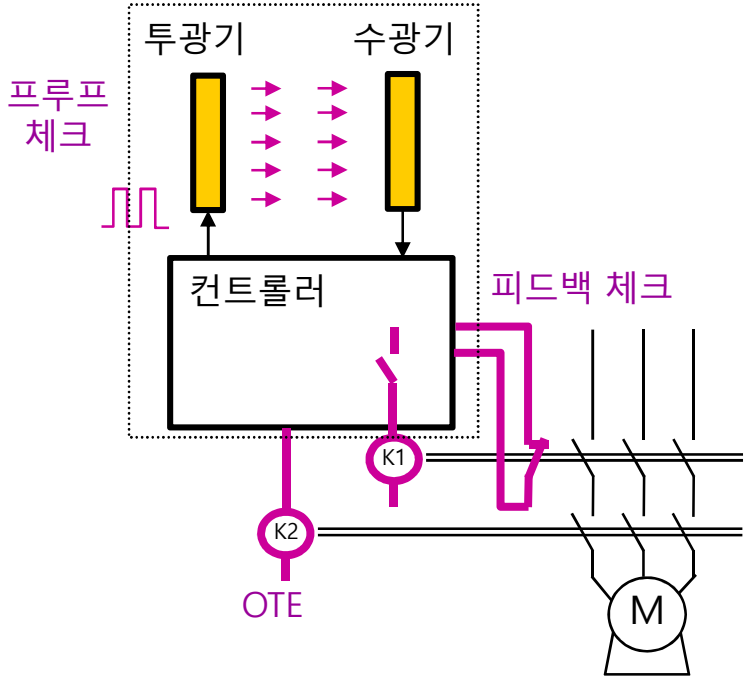
카테고리 2의 SRP/CS는 기계 제어 시스템에 의해 기능이 적절한 간격으로 점검되도록 설계되어야 합니다.
안전 기능 점검은 기계 시동 시 및 위험한 상황이 시작되기 전에 수행해야합니다.

※ 카테고리 2의 특징

✓ DCavg= Low, Medium
✓ 각 채널의 $MTTF_D$ = Low - High
✓ 최대 달성가능 PL → PLd
✓ 안전 시스템의 고장을 검출하기 위한 주기적인 테스트
✓ 피드백 체크

예시)

프루프 체크



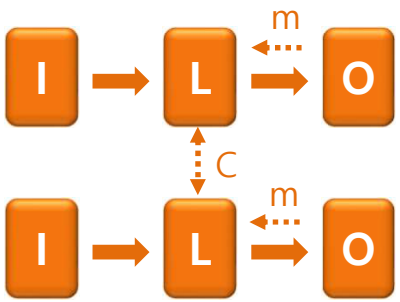
카테고리 2에서는 점검율과 수요율에 대한 요구사항이 있습니다.

수요율 ≤ 1/100 점검율

계산 식에따라 기능을 시작하기 전 기능이 안정적인지를 100번 확인해야 하는 조건입니다.

카테고리 3

➢ 카테고리 구조



카테고리 3의 SRP/CS는 구성하는 부품 중 하나의 단일 고장으로 인해 안전 기능이 손실되지 않도록 설계해야 합니다. 합리적으로 실행 가능한 경우에는 단일 고장은 안전기능에 대한 다음의 요구 또는 그 이전에 감지되어야 합니다.

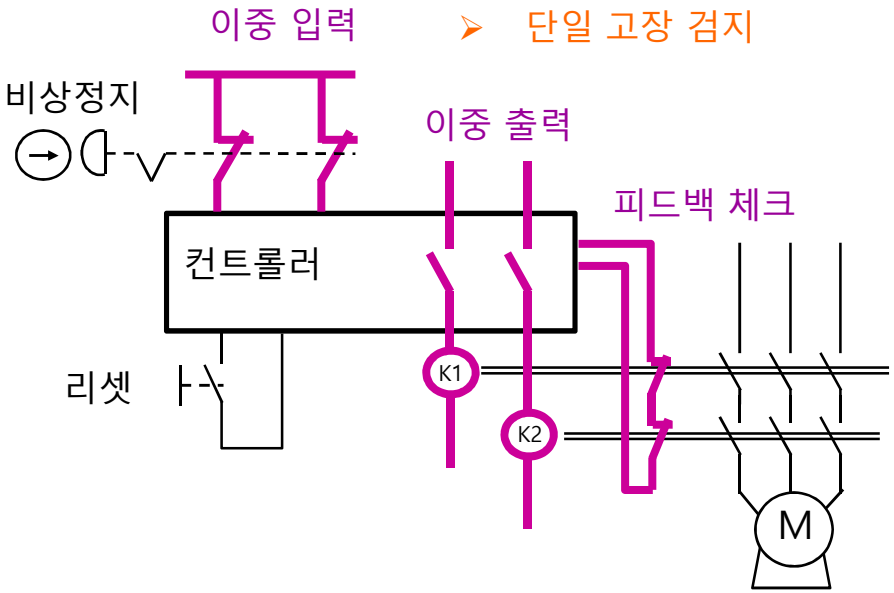
※ 카테고리 3의 특징

✓ DCavg= Low, Medium
✓ 각 채널의 $MTTF_D$ = Low - High
✓ 최대 달성가능 PL → PLe
✓ 이중 채널 & 피드백 체크

예시)

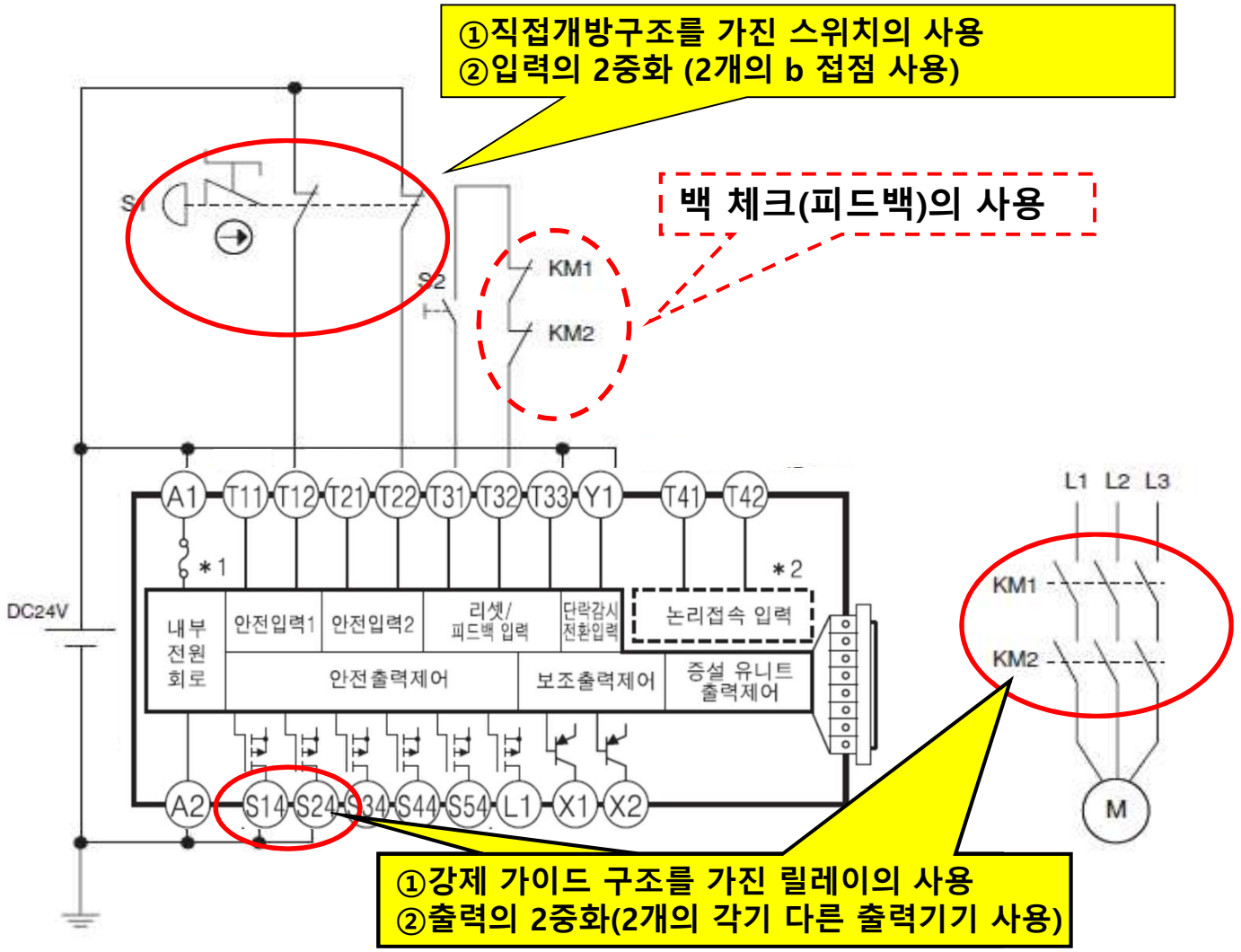
이중화 채널의 구조

➢ 단일 고장 검지



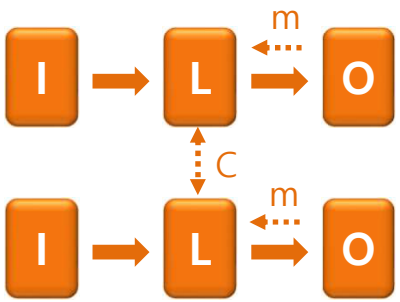
카테고리 B, 1, 2에서는 단일 채널 구조를 이루고 있어 단일 고장을 방지할 수 없습니다. 카테고리 3은 동일한 고장 상황을 보상하고 이중 채널 구조로 인해 기계를 안전하게 정지 시킵니다.
피드백 확인을 통해 출력 작동 상태를 모니터링 할 수 있습니다. 출력에 결함이 있으면 시스템을 시작할 수 없습니다.

안전 카테고리 3 회로 예


①직접개방구조를 가진 스위치의 사용
②입력의 2중화 (2개의 b 접점 사용)
백 체크(피드백)의 사용
S1
S2
KM1
KM2
A1
T11
T12
T21
T22
T31
T32
T33
Y1
T41
T42
*1
*2
DC24V
내부 전원 회로
안전입력1
안전입력2
리셋/ 피드백 입력
단락감시 전환입력
논리접속 입력
안전출력제어
보조출력제어
증설 유니트 출력제어
A2
S14
S24
S34
S44
S54
L1
X1
X2
L1 L2 L3
KM1
KM2
M
①강제 가이드 구조를 가진 릴레이의 사용
②출력의 2중화(2개의 각기 다른 출력기기 사용)

카테고리 4

➢ 카테고리 구조



카테고리 4의 SRP/CS는 구성하는 부품 중 하나의 단일 결함으로 인해 안전기능이 손실되지 않고 감지되지 않은 결함이 누적되어 안전 기능이 손실되지 않도록 설계합니다.

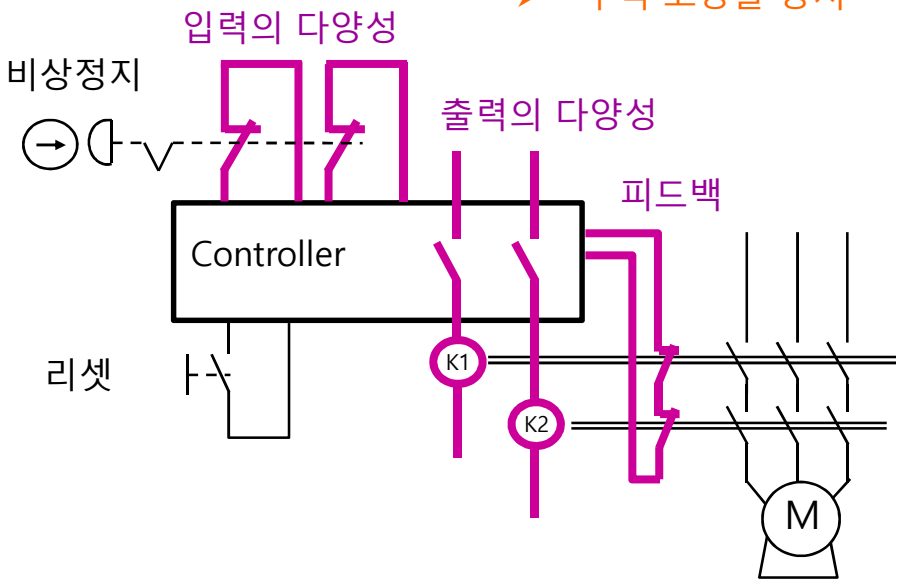
※ 카테고리 4의 특징

✓ DCavg= High
✓ 각 채널의 $MTTF_D$ = High
✓ 최대 달성가능 PL → PLe
✓ 이중 채널 & 피드백 체크
✓ 누적 고장 방지

예시)

채널의 다양성

➢ 누적 고장을 방지



카테고리 3과 4의 차이점은 입력과 출력의 다양성입니다. 각 채널은 이중 채널로 결합되어 단일 고장을 방지하고 다른 기술적 방법을 사용하여 고장의 축적을 방지합니다. 카테고리 4로 설계하는 것으로 간주되면 PLe를 쉽게 달성 할 수 있습니다.

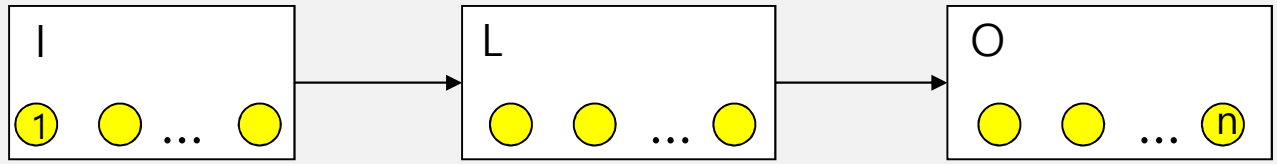
MTTFD (mean time to dangerous failure)

$MTTF_D$는 위험한 고장까지의 평균시간에 대한 기대치를 정의합니다.
각 채널의 $MTTF_D$ 값은 세가지 수준으로 제공되며 각 채널마다 개별적으로 고려되어야 합니다.

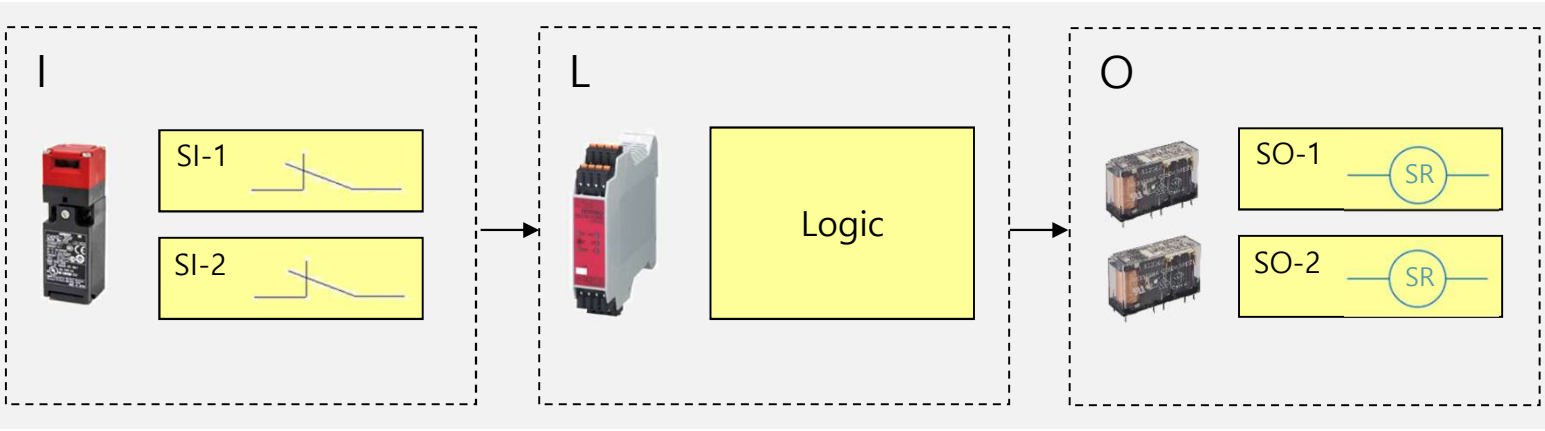
체크 항목	Tent (aluminum pipes, pins)	Timber house(wood)	Office building (H beam)
내구도 (y)			
사용빈도	1년에 2회	24시간, 365일	일 8시간 / 1년 200일
고장이 예측되는 시기			

MTTFD (mean time to dangerous failure)

$MTTF_D$의 계산 방식



ⓘ :시스템(1채널을 구성하는 각 부품)



MTTFD (mean time to dangerous failure)

$MTTF_D$의 계산식

- 제조사가 $MTTF_D$ 값을 제공하는 경우 (예, 시스템 부품 등)
- 제조사가 B10d 값만 제공하는 경우 (예, 스위치, 코일류 등)

$$MTTFd = \frac{B10d}{0.1 \times N_{OP}} \quad \text{... (1)}$$

B10d: 10%의 부품이 위험측 고장을 내기까지 운전 횟수 (소모품에 적용)

Nop: 1년 당의 총 운전 횟수 (단위: cycle/year)

$$N_{OP} = \frac{dop \times hop \times 3{,}600}{tcycle} \quad \text{... (2)}$$

- tcycle: 1조작 사이클의 평균 시간간격(sec/cycle)
- hop: 1일 당의 가동 시간 (hour/day)
- dop: 연간 가동 일수 (day/year)

MTTFD (mean time to dangerous failure)

각 부품의 $MTTF_D$ 값이 결정되면, 전체 시스템에 대한 $MTTF_D$ 값을 계산해야 합니다.

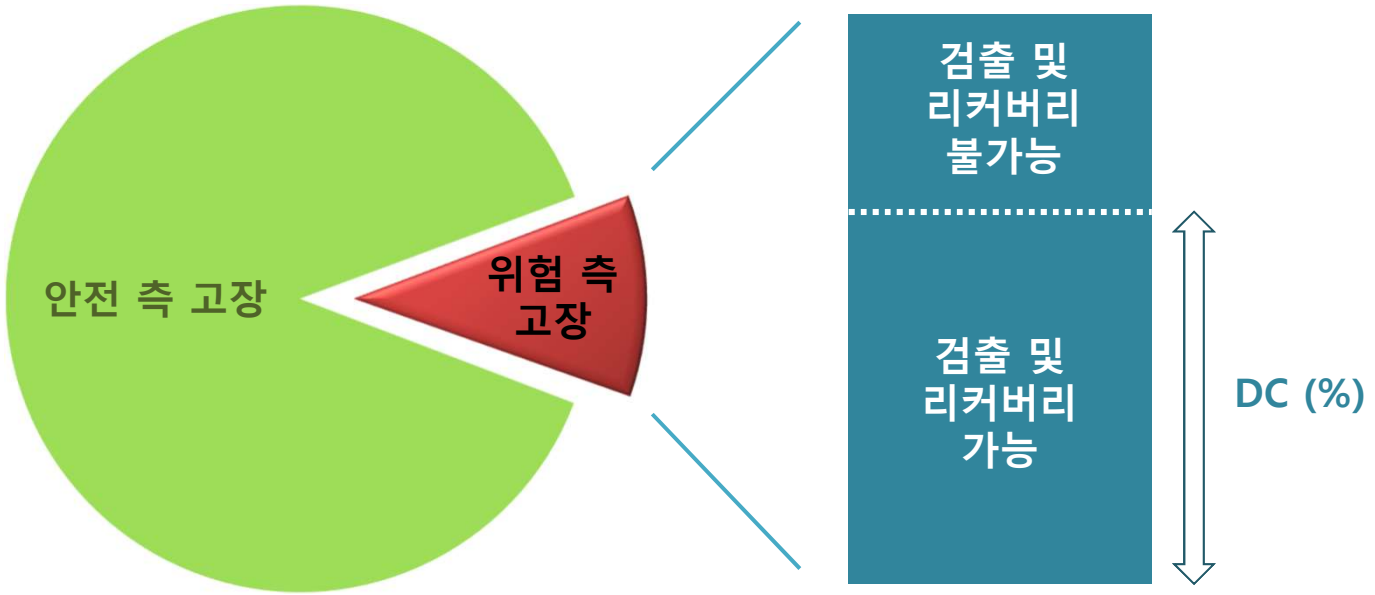
$$MTTFd = \frac{1}{\sum_{i=1}^{n} \frac{1}{MTTFd_i}} \quad \text{... (3)}$$

한 채널에 대한 전체 $MTTF_D$ 값이 결정되어지면 아래의 평가표를 이용하여, $MTTF_D$ 값의 Value를 판정합니다.

평가 결과	범위
Low	3 years ≤ MTTFd < 10 years
Medium	10 years ≤ MTTFd < 30 years
High	30 years ≤ MTTFd ≤ 100 years

DC (diagnostic coverage)

DC는 진단 범주의 측정을 의미하며, 이는 감지된 오류의 고장율과 총 위험한 고장율 사이의 비율로 결정될 수 있습니다.



DC (diagnostic coverage)

Average Diagnostic Coverage:진단 범주
- 소프트웨어를 포함한 시스템의 신뢰성

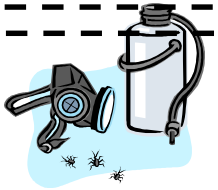
전체가 제대로 작동하는지를 점검하여 조치를 취하고 있는가

(사용 목적 또는 주기에 따라 고장을 진단하는 주기와 범위는 달라야 한다.)

텐트

쓰기 전에 손질

목조 주택



필요에 따라 대책
흰개미 퇴치, 누수 등

오피스 빌딩

정기적인 빌딩 유지보수로
미리 문제를 발견

DC (diagnostic coverage)

<입력>

Measure	DC
Input device	
Cyclic test stimulus by dynamic change of the input signals	90 %
Plausibility check, e.g. use of normally open and normally closed mechanically linked contacts	99 %
Cross monitoring of inputs without dynamic test	0 % to 99 %, depending on how often a signal change is done by the application
Cross monitoring of input signals with dynamic test if short circuits are not detectable (for multiple I/O)	90 %
Cross monitoring of input signals and intermediate results within the logic (L), and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O)	99 %
Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90 % to 99 %, depending on the application
Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99 %
Fault detection by the process	0 % to 99 %, depending on the application; this measure alone is not sufficient for the required performance level e!
Monitoring some characteristics of the sensor (response time, range of analogue signals, e.g. electrical resistance, capacitance)	60 %

<제어>

Measure	DC
Input device	
Cyclic test stimulus by dynamic change of the input signals	90 %
Plausibility check, e.g. use of normally open and normally closed mechanically linked contacts	99 %
Cross monitoring of inputs without dynamic test	0 % to 99 %, depending on how often a signal change is done by the application
Cross monitoring of input signals with dynamic test if short circuits are not detectable (for multiple I/O)	90 %
Cross monitoring of input signals and intermediate results within the logic (L), and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O)	99 %
Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90 % to 99 %, depending on the application
Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99 %
Fault detection by the process	0 % to 99 %, depending on the application; this measure alone is not sufficient for the required performance level e!
Monitoring some characteristics of the sensor (response time, range of analogue signals, e.g. electrical resistance, capacitance)	60 %

<출력>

Measure	DC
Input device	
Cyclic test stimulus by dynamic change of the input signals	90 %
Plausibility check, e.g. use of normally open and normally closed mechanically linked contacts	99 %
Cross monitoring of inputs without dynamic test	0 % to 99 %, depending on how often a signal change is done by the application
Cross monitoring of input signals with dynamic test if short circuits are not detectable (for multiple I/O)	90 %
Cross monitoring of input signals and intermediate results within the logic (L), and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O)	99 %
Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90 % to 99 %, depending on the application
Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99 %
Fault detection by the process	0 % to 99 %, depending on the application; this measure alone is not sufficient for the required performance level e!
Monitoring some characteristics of the sensor (response time, range of analogue signals, e.g. electrical resistance, capacitance)	60 %

입력, 제어, 출력 관련 DC 체크사항을 판단하고 각각의 결과값에 대해 평균값 계산을 실시합니다.

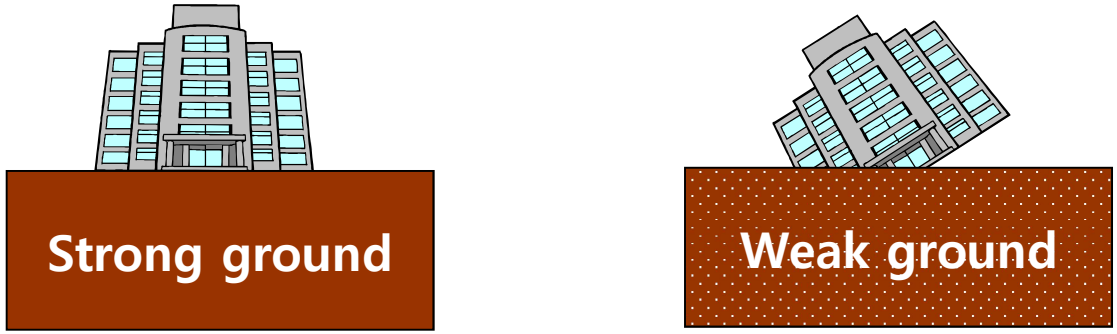
$$DCavg = \frac{\sum_{i=1}^{n} \frac{DC_i}{MTTFd_i}}{\sum_{i=1}^{n} \frac{1}{MTTFd_i}}$$

(DC 평균 / Annex E)

평과 결과	DCavg
None	DC<60%
Low	60%≦DC<90%
Medium	90%≦DC<99%
High	99%≦DC

CCF (common cause failure)

CCF는 공통 원인 고장을 의미하며 이러한 원인에 대한 대책이 어떻게 적용되어 있는지 평가하는 매개변수 입니다. 제어 관점에서 볼 때 이는 하나의 원인으로 여러 구성 요소의 고장을 피하는 것을 의미합니다. 그러나 이중화 개념은 안전 회로구조에 도입되었지만 그러한 단순 이중화 개념은 없습니다. 평가 점수는 65를 초과해야 하며 오류 진단 사양을 향상 시켜줍니다.



오피스 빌딩이 지어진 부지가 약하면 건물 전체가 무너질 위험이 있습니다. 이와 관련한 위험에 대해 적절한 방지 대책이 필요합니다.

CCF (common cause failure)

CCF 점수배점 절차와 정량화 (ISO13849-1, Annex F)

No.	Measure against CCF	Score
1	Separation/ Segregation	
	Physical separation between signal paths, for example: — separation in wiring/piping; — detection of short circuits and open circuits in cables by dynamic test; — separate shielding for the signal path of each channel; — sufficient clearances and creepage distances on printed-circuit boards.	15
2	Diversity	
	Different technologies/design or physical principles are used, for example: — first channel electronic or programmable electronic and second channel electromechanical hardwired, — different initiation of safety function for each channel (e.g. position, pressure, temperature), and/or digital and analog measurement of variables (e.g. distance, pressure or temperature) and/or Components of different manufactures.	20
3	Design/application/experience	
3.1	Protection against over-voltage, over-pressure, over-current, over-temperature, etc.	15
3.2	Components used are well-tried.	5
4	Assessment/analysis	
	For each part of safety related parts of control system a failure mode and effect analysis has been carried out and its results taken into account to avoid common-cause-failures in the design.	5

CCF (common cause failure)

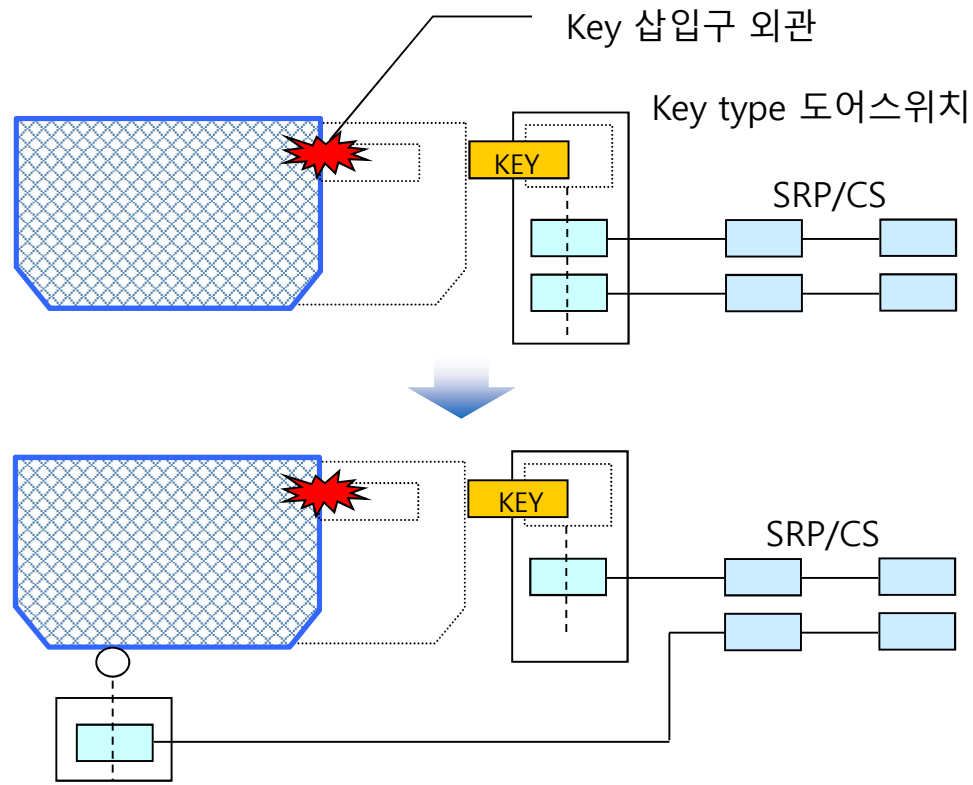
CCF 점수배점 절차와 정량화 (ISO13849-1, Annex F)

No.	Measure against CCF	Score
5	Competence/training	
	Training of designers to understand the causes and consequences of common cause failures.	5
6	Environmental	
6.1	For electrical/electronic systems, prevention of contamination and electromagnetic disturbances (EMC) to protect against common cause failures in accordance with appropriate standards (e.g. IEC 61326–3-1). Fluidic systems: filtration of the pressure medium, prevention of dirt intake, drainage of compressed air, e.g. in compliance with the component manufacturers' requirements concerning purity of the pressure medium. NOTE For combined fluidic and electric systems, both aspects should be considered.	25
6.2	Other influences Consideration of the requirements for immunity to all relevant environmental influences such as, temperature, shock, vibration, humidity (e.g. as specified in relevant standards).	10
	Total	Max. 100

65점 이상의 정량적 결과가 나오면 CCF에 대해서는 통과입니다.

CCF (common cause failure)- 예시

도어 인터락 스위치의 CCF 개념을 고려할 때 전체 시스템의 고장은 Key 삽입구의 형상 파괴로 인해 발생할 수 있습니다.



* ISO14119:2013 개정 포인트

CCF (common cause failure)- 예시

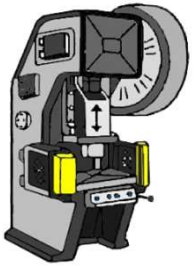
열에 대한 고려의 예

스위치 등 입력 부품을 가공부 주변에 달아 열(고온, 저온)이나, 화학물질의 영향 (부품의 정격을 넘는 사용 또는 그러한 환경에 설치)에 의해 부품의 파손이나 기능 불량으로 위험 측 고장을 초래하지 않도록 고려되고 있다.

예를 들면, 히터(고온부)의 커버에 부착하는 스위치

진동에 대한 고려의 예

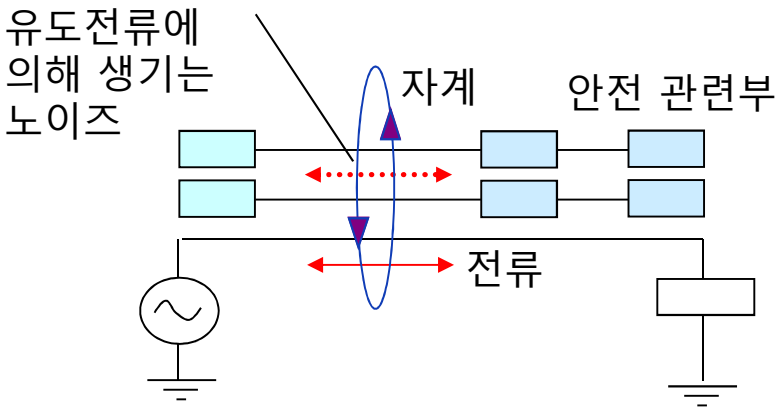
릴레이 등의 기계 접점 부품을 진동이 큰 장소에 설치하지 않는다.



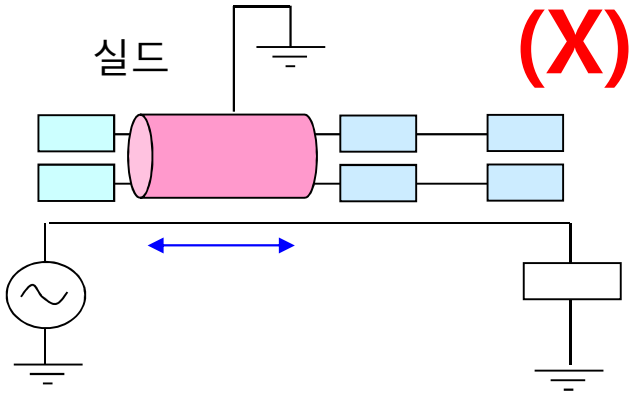
예를 들면, 프레스기의 제어반은 따로 설치

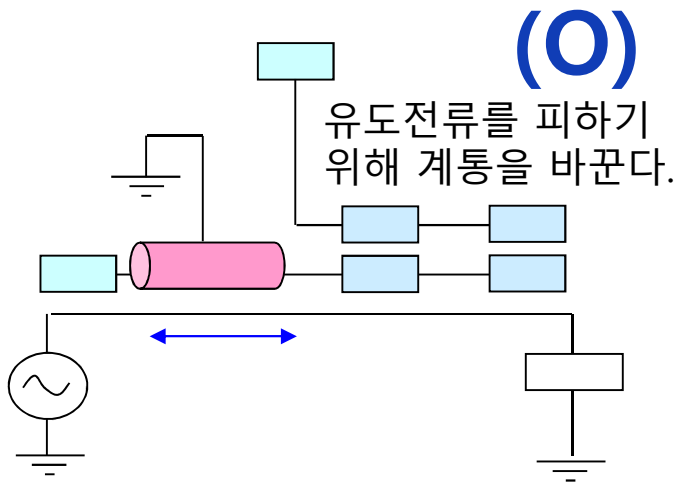
CCF (common cause failure)- 예시

전자파 적합성의 예



유도 노이즈가 발생하기 쉬운 회로





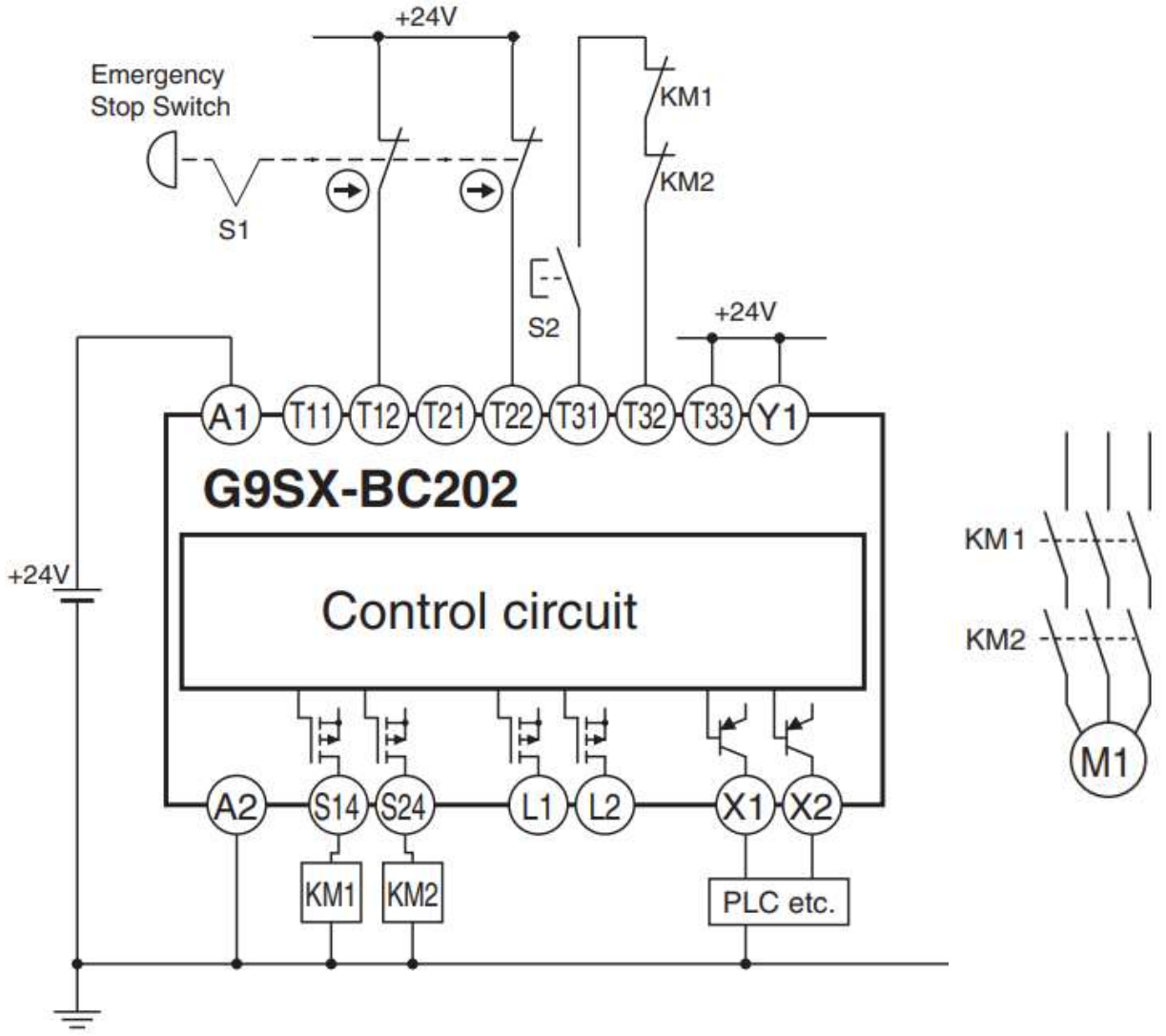
EMC는 2가지 있음

1. 전자파 내성 (EMI)
   - 기계에 외부에서 노이즈를 가하는 테스트
2. 전자파 장해 (EMS)
   - 기계가 외부로 내는 노이즈 측정

안전카테고리 회로 예제

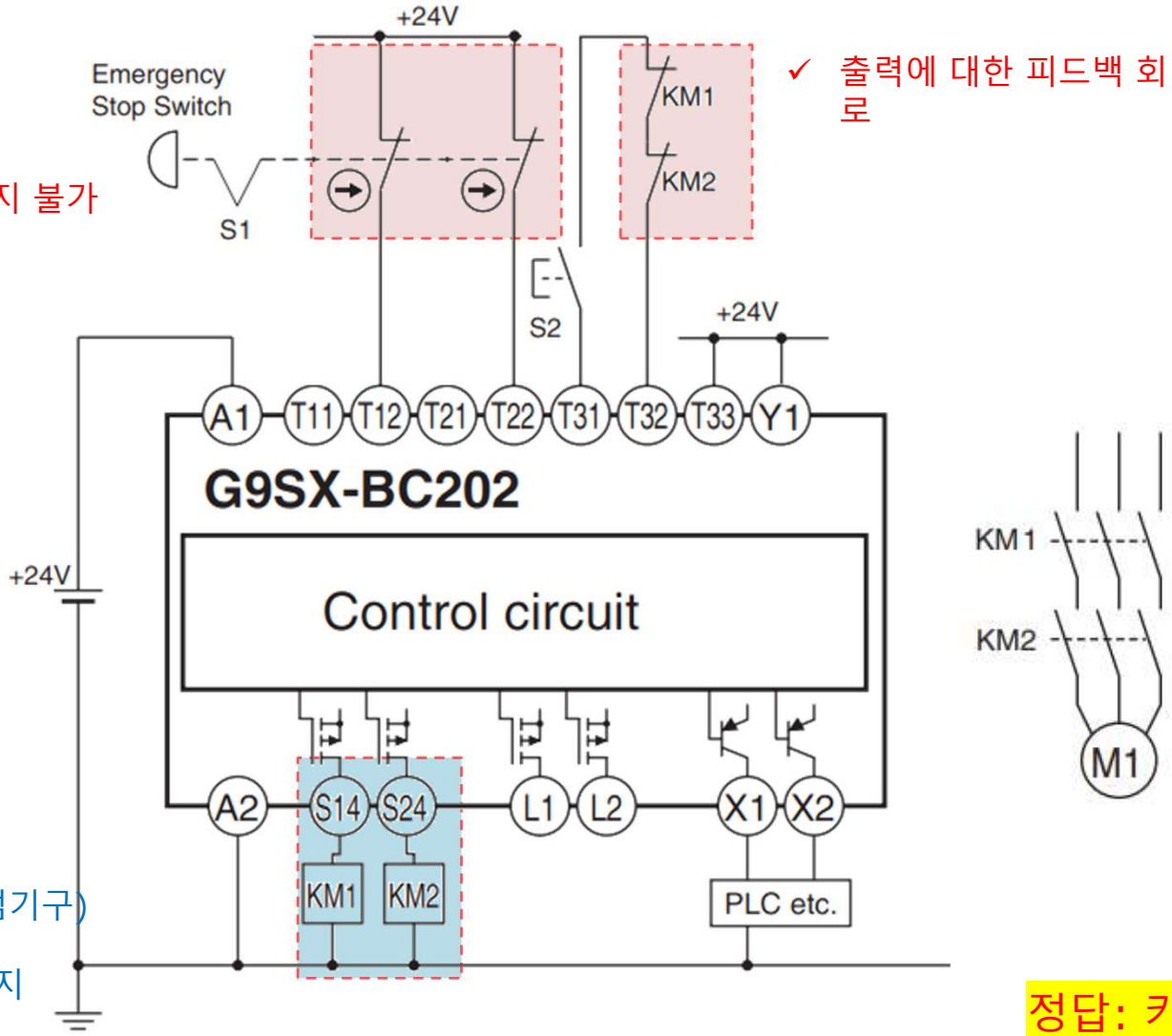
KAR 한국로봇산업협회
Korea Association of Robot industry

Q1. 다음의 전기 도면을 보고 카테고리를 결정하시오.



A1. 다음의 전기 도면을 보고 카테고리를 결정하시오.

✓ 안전인증품
(직접개방구조)
✓ 이중화 입력
✓ 신호간 단락 검지 불가

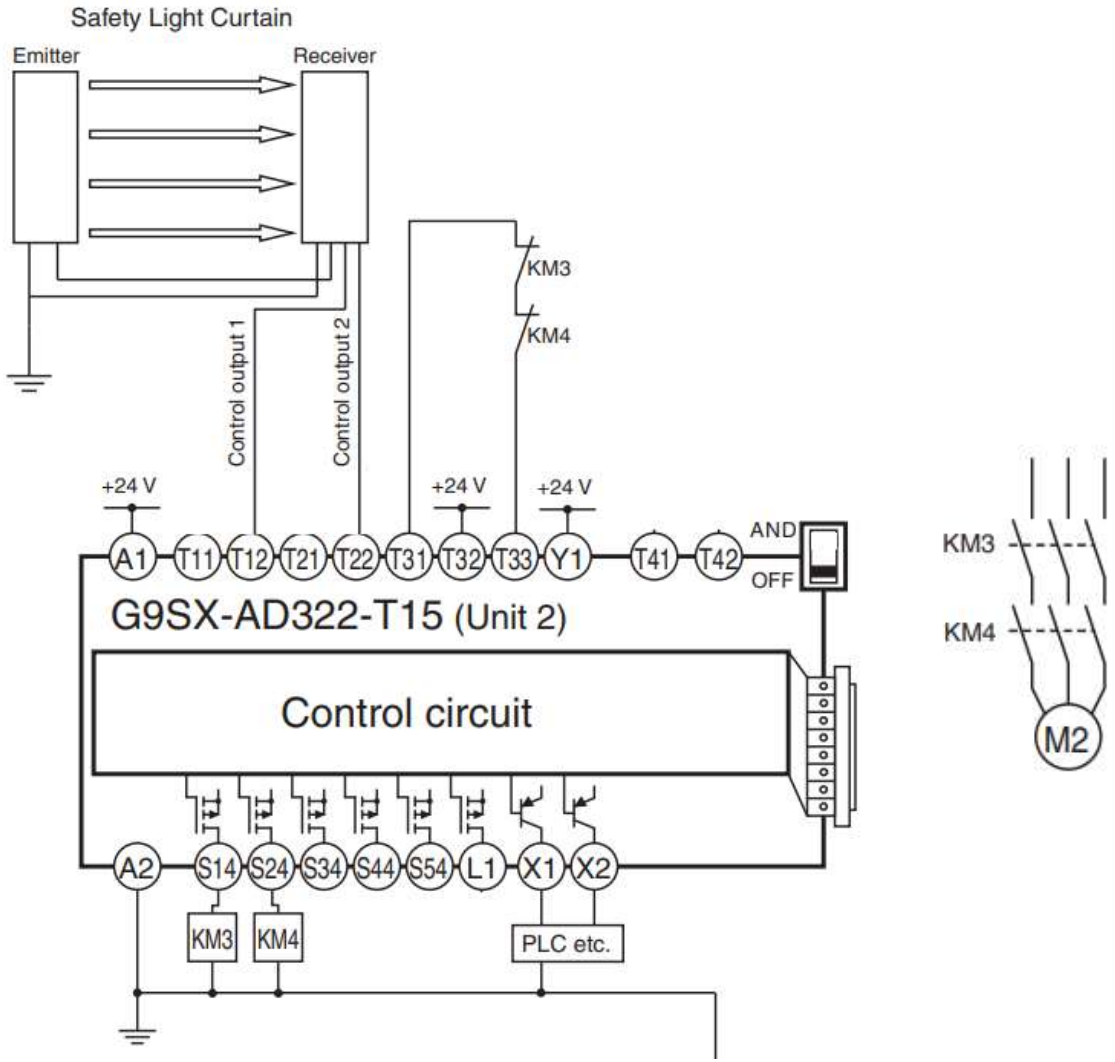


✓ 출력에 대한 피드백 회로

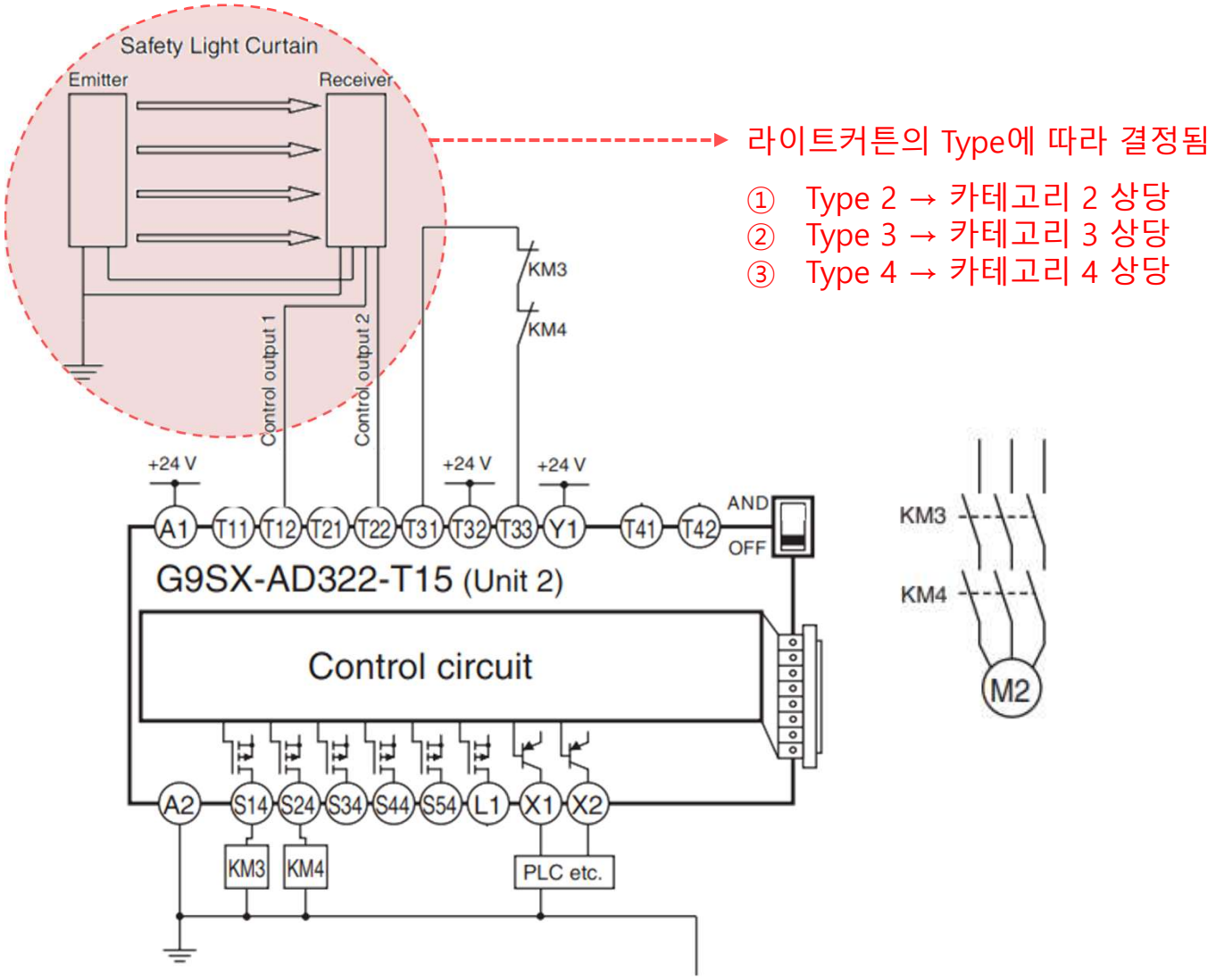
✓ 안전인증품
(강제가이드 접점기구)
✓ 이중화 출력
✓ 신호간 단락 검지

정답: 카테고리 3

Q2. 다음의 전기 도면을 보고 카테고리를 결정하시오.



A2. 다음의 전기 도면을 보고 카테고리를 결정하시오.

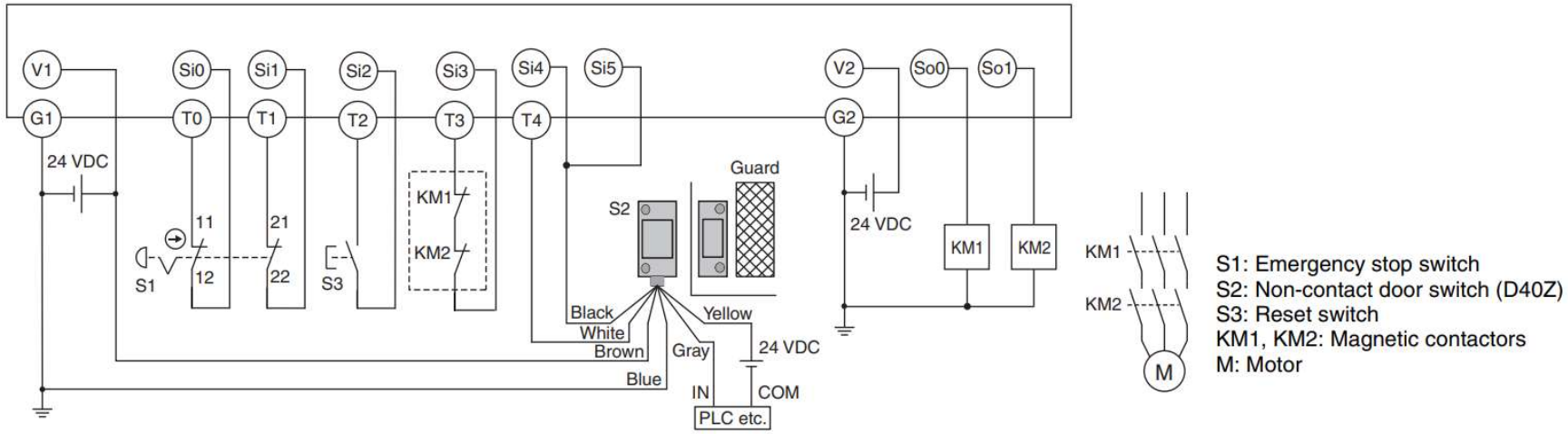


라이트커튼의 Type에 따라 결정됨

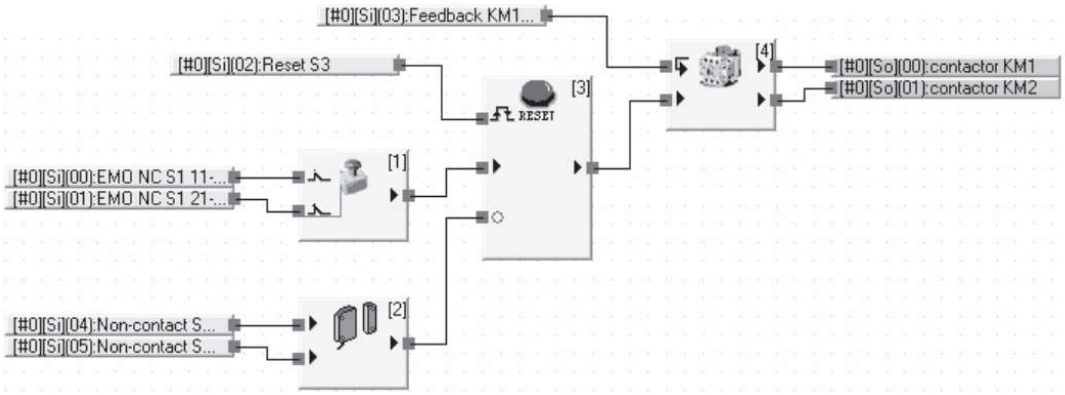
① Type 2 → 카테고리 2 상당
② Type 3 → 카테고리 3 상당
③ Type 4 → 카테고리 4 상당

Q3. 다음의 전기 도면을 보고 카테고리를 결정하시오.

Safety PLC 배선

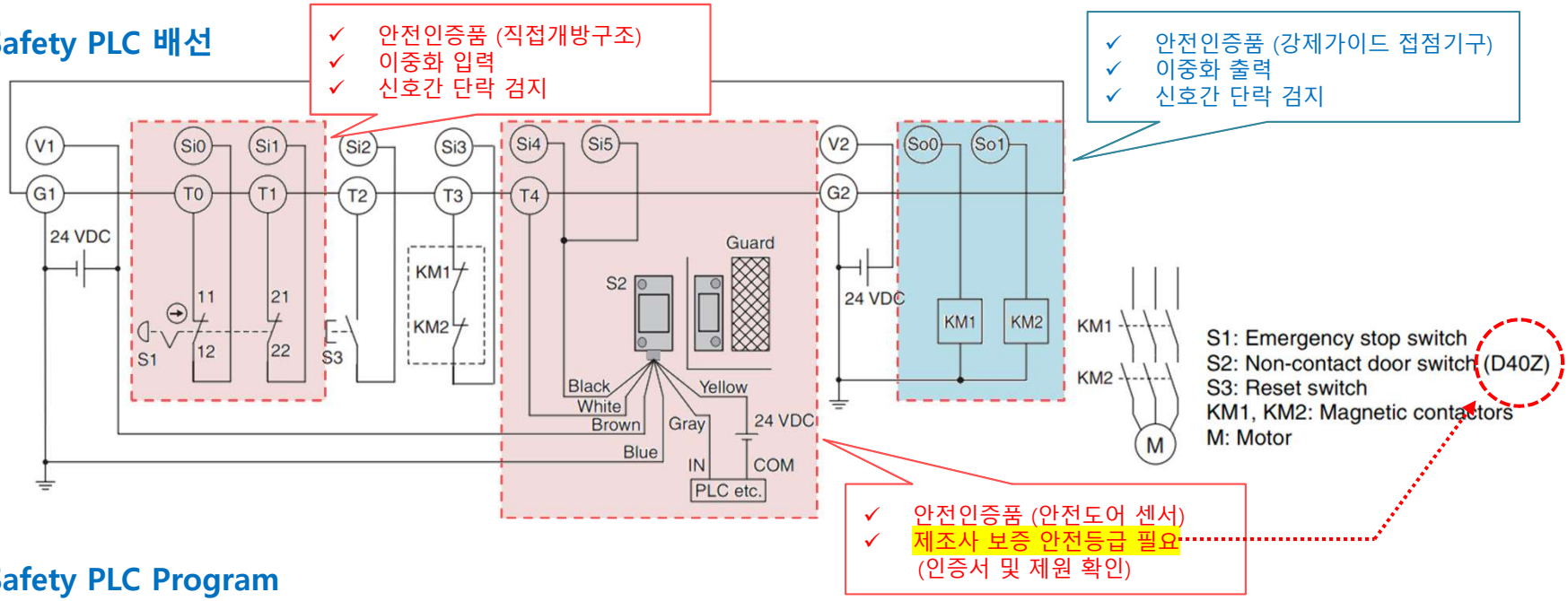


Safety PLC Program

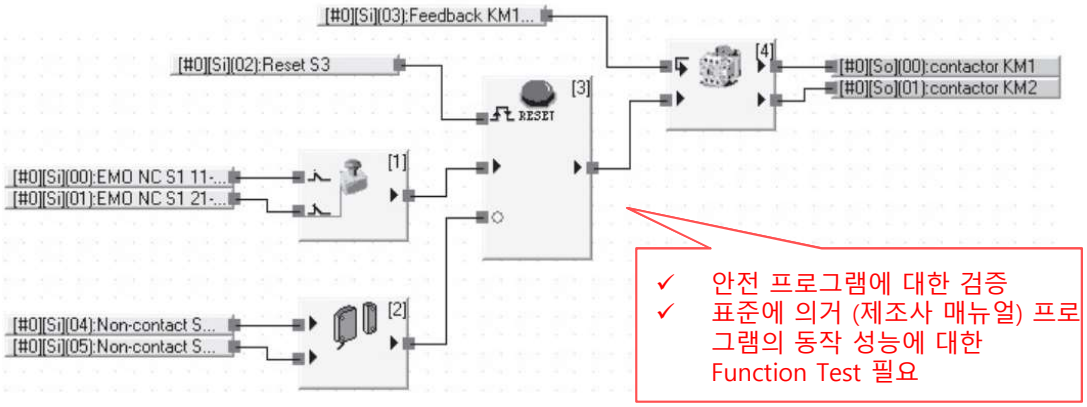


A3. 다음의 전기 도면을 보고 카테고리를 결정하시오.

Safety PLC 배선

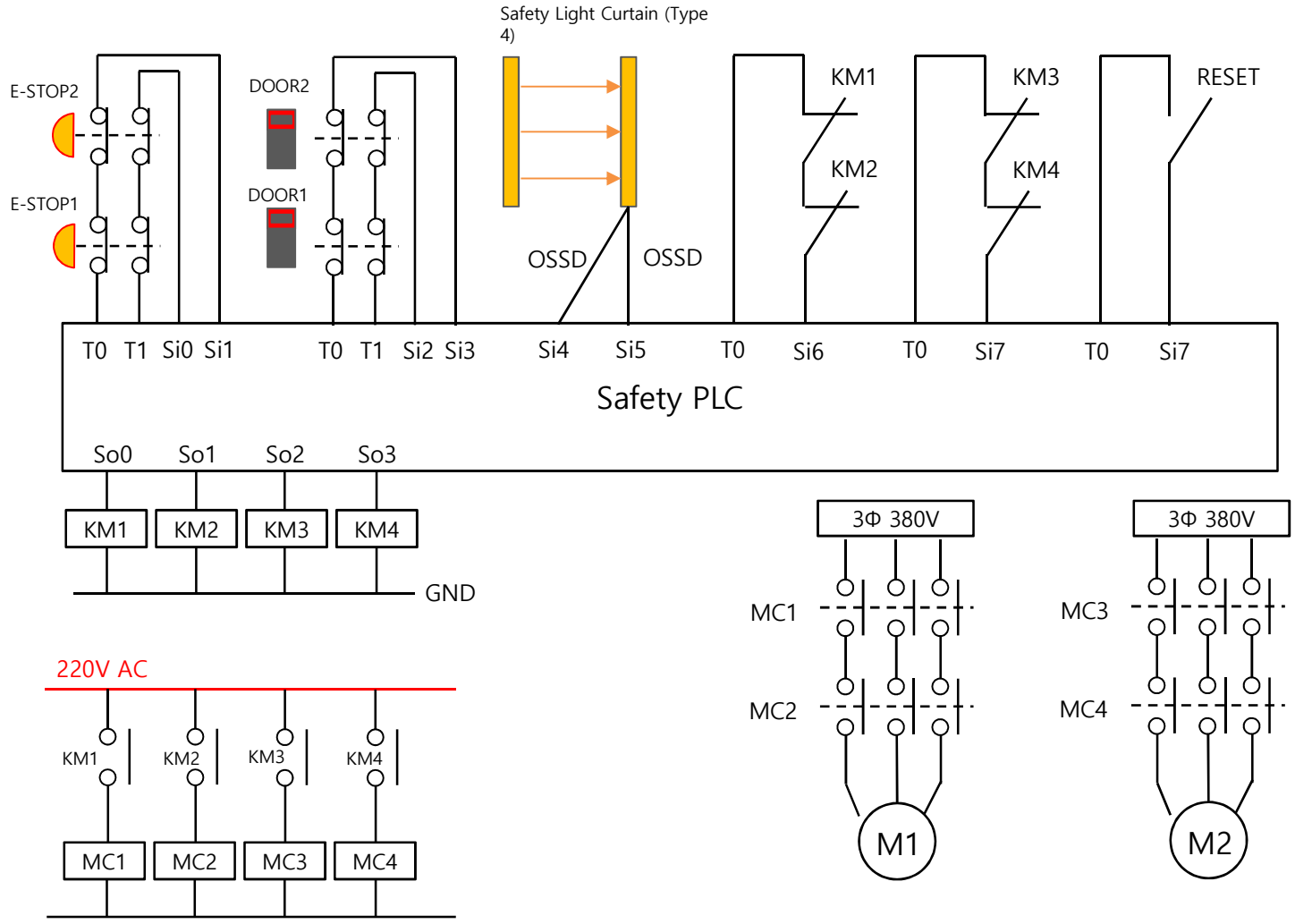


Safety PLC Program



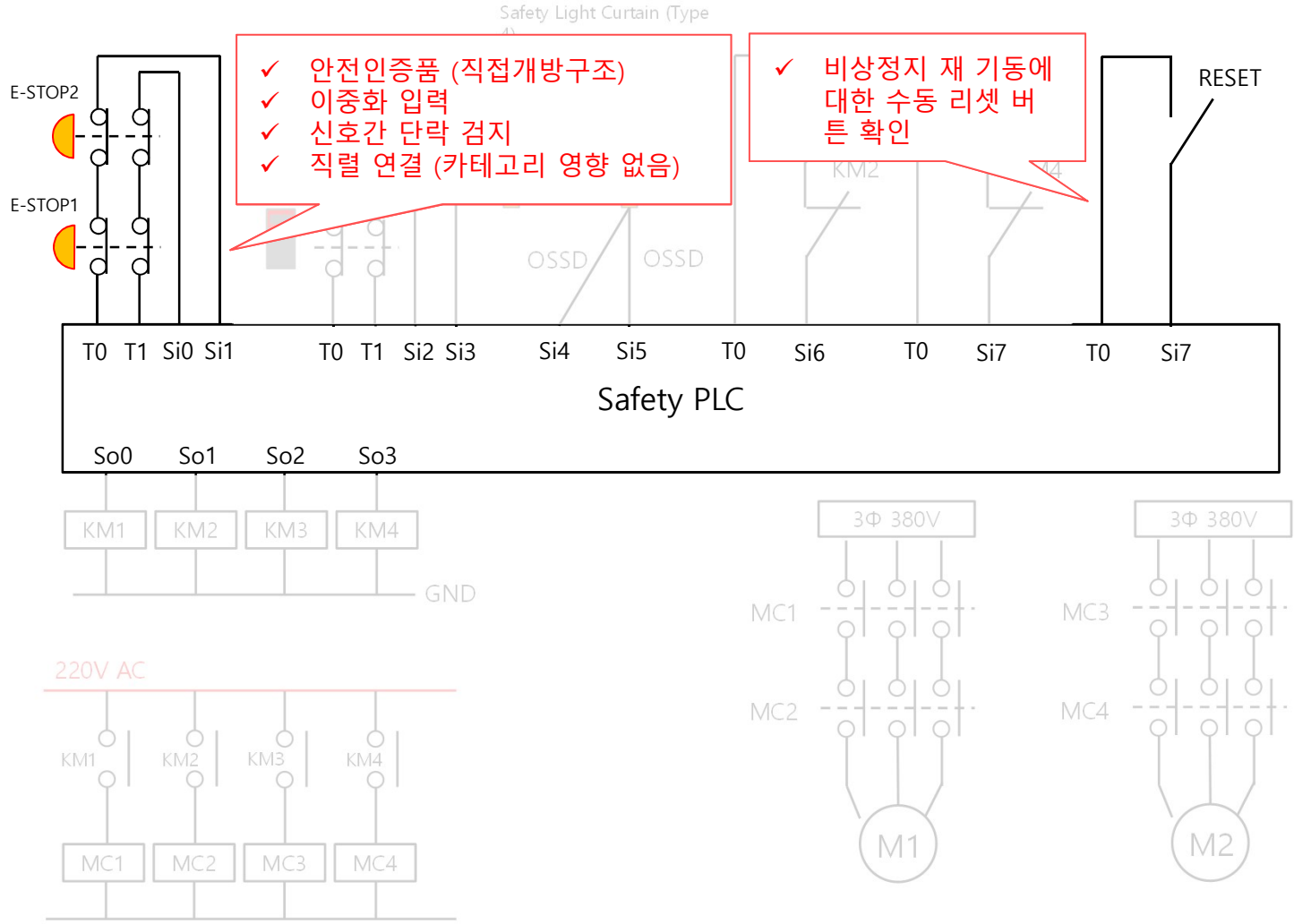
Q4. 안전 사양 요구조건에 충족한지 판단하시오.

<요구조건> 카테고리 4 / PLe 이상의 장비



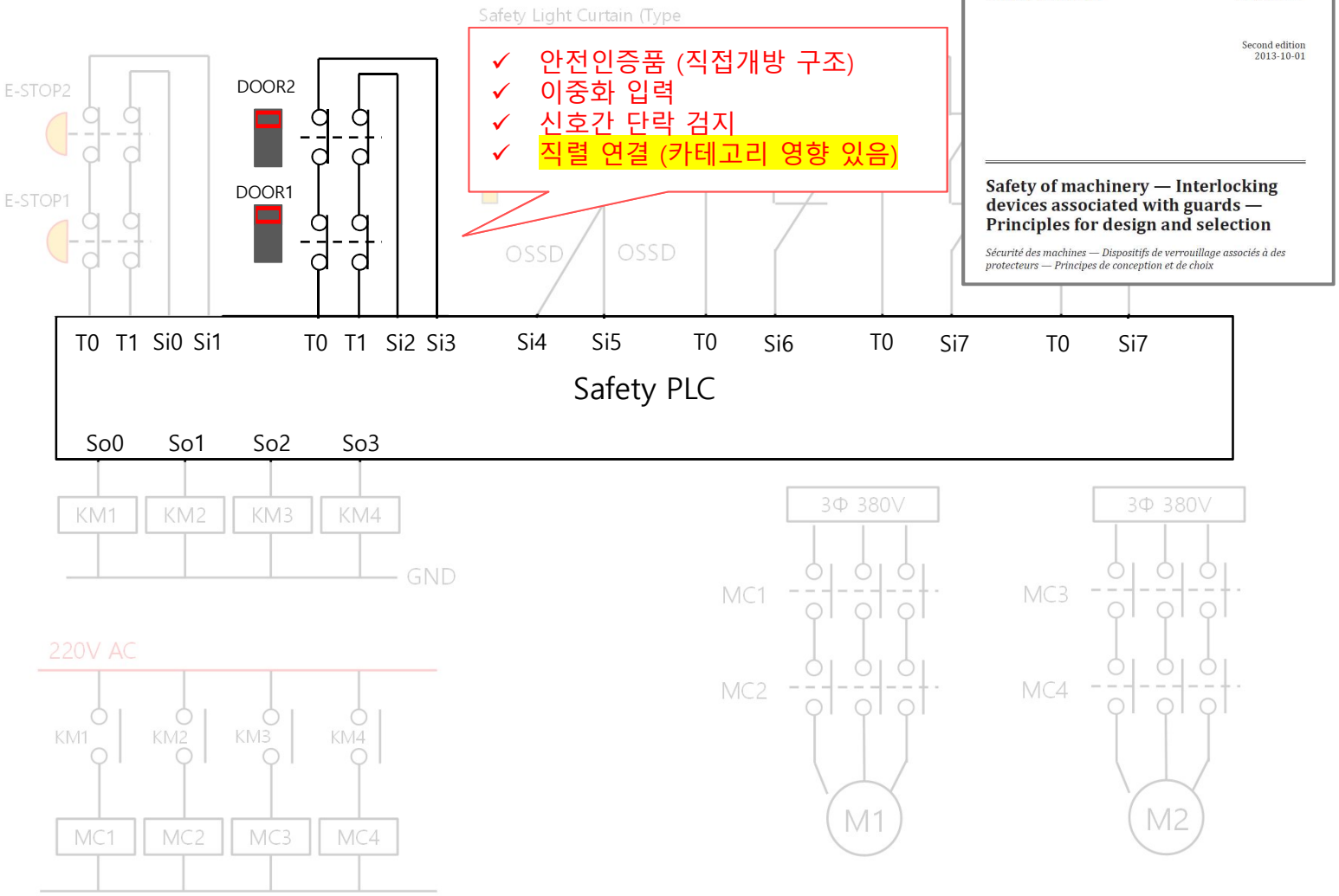
A4. 안전 사양 요구조건에 충족한지 판단하시오.

<요구조건> 카테고리 4 / PLe 이상의 장비



A4. 안전 사양 요구조건에 충족한지 판단하시오.

<요구조건> 카테고리 4 / PLe 이상의 장비



INTERNATIONAL STANDARD **ISO 14119**

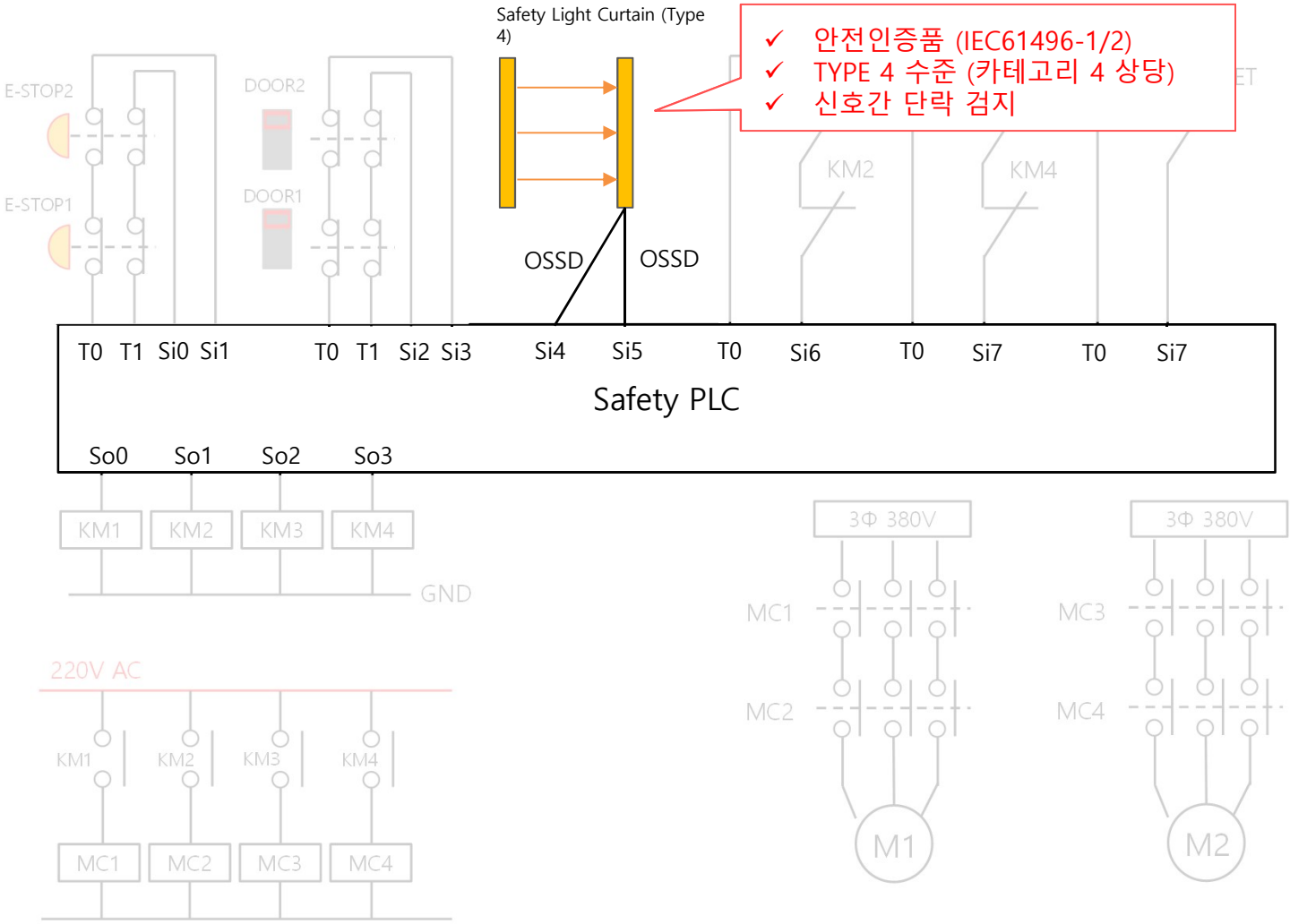
Second edition
2013-10-01

Safety of machinery — Interlocking devices associated with guards — Principles for design and selection

Sécurité des machines — Dispositifs de verrouillage associés à des protecteurs — Principes de conception et de choix

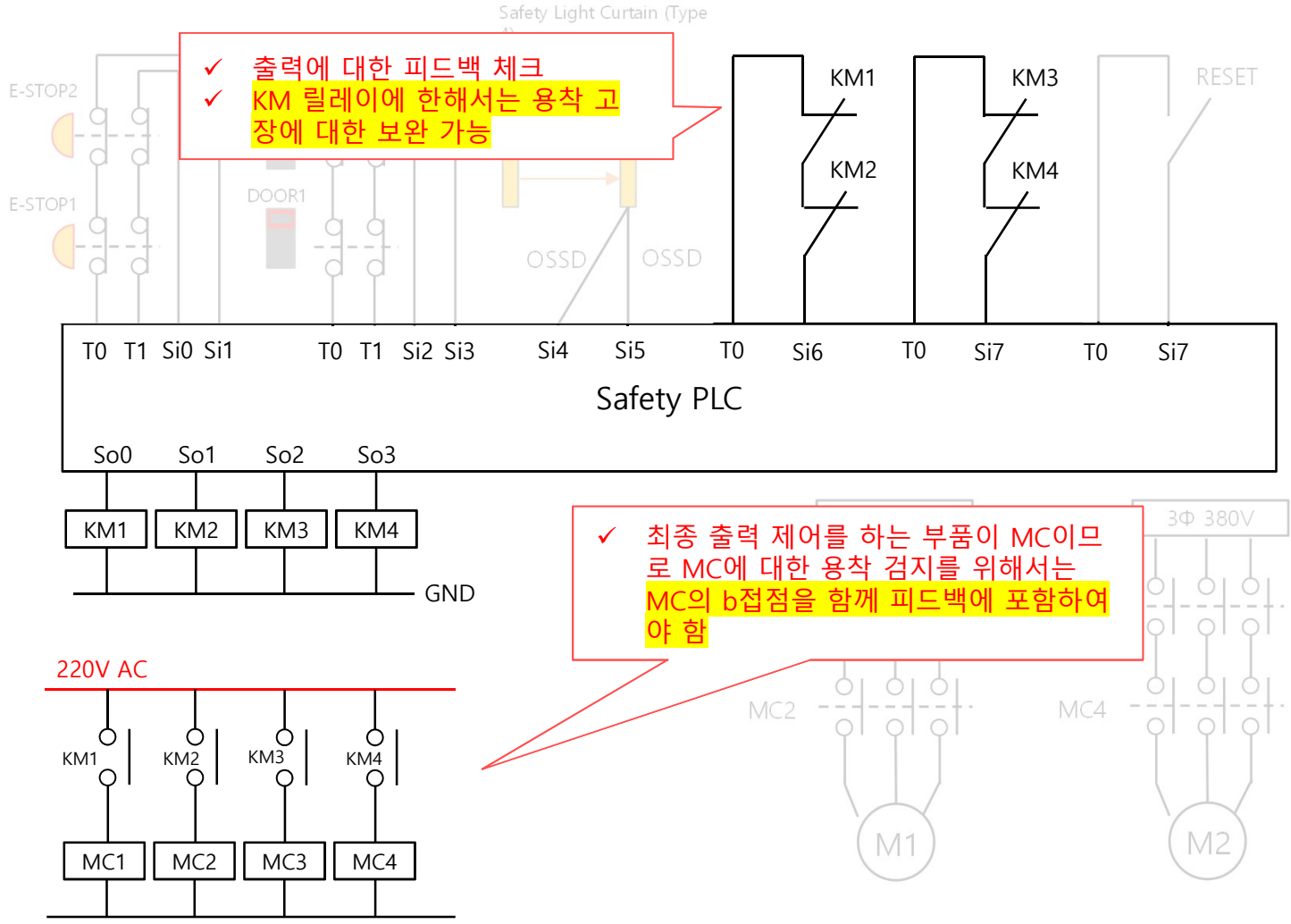
A4. 안전 사양 요구조건에 충족한지 판단하시오.

<요구조건> 카테고리 4 / PLe 이상의 장비



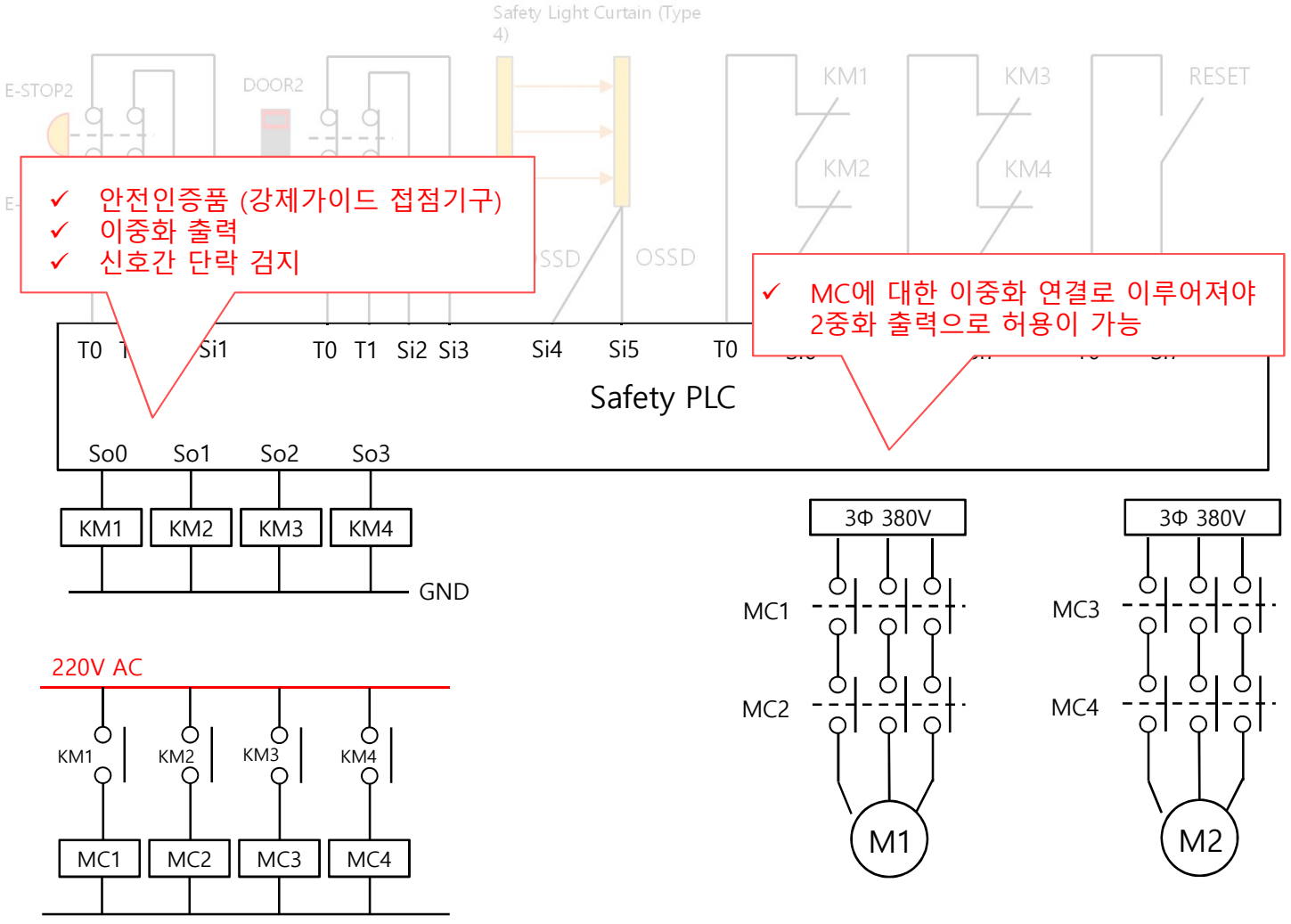
A4. 안전 사양 요구조건에 충족한지 판단하시오.

<요구조건> 카테고리 4 / PLe 이상의 장비



A4. 안전 사양 요구조건에 충족한지 판단하시오.

<요구조건> 카테고리 4 / PLe 이상의 장비



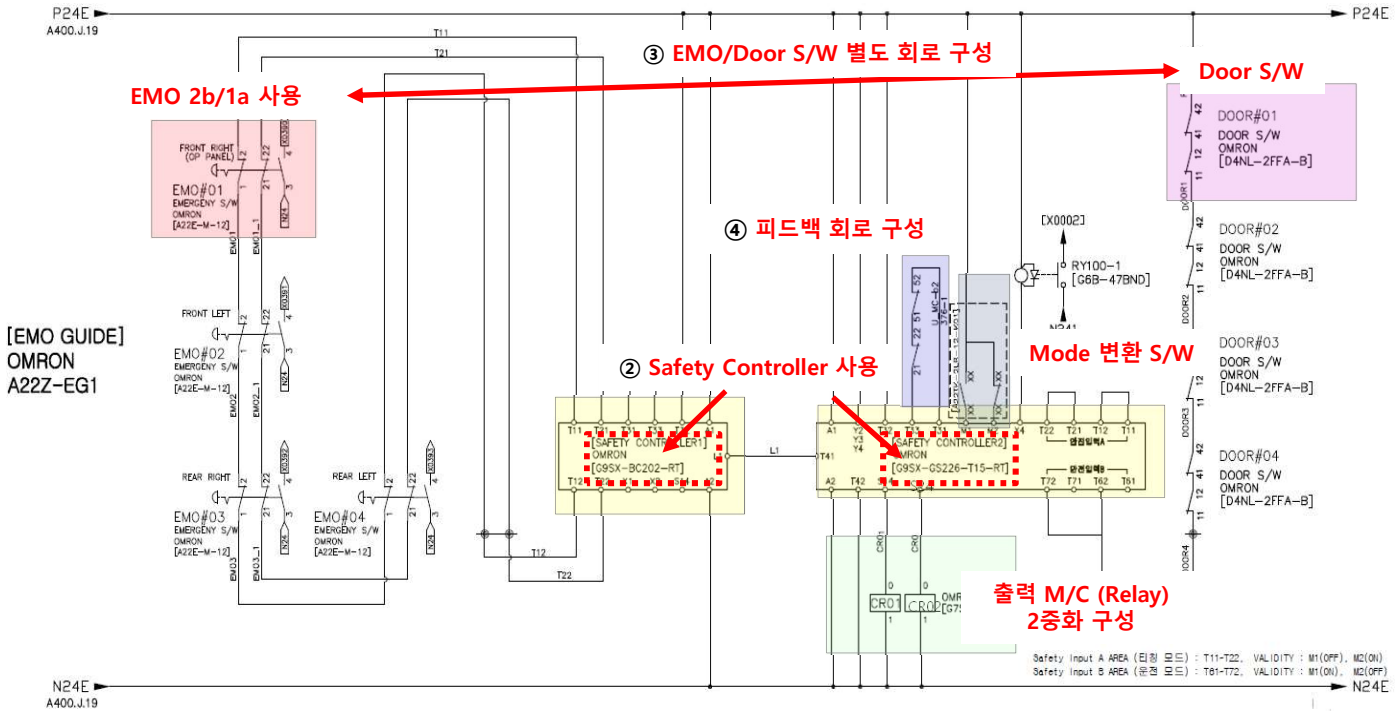
안전카테고리 실제 회로 분석

KAR 한국로봇산업협회
Korea Association of Robot industry

안전 회로 구성 및 분석-비상정지

비상 정지회로 등급 및 구성요소(ISO13849-1:2015)

① 비상정지, 차단장치의 안전회로는 위험성평가 실시 후 안전 카테고리 3 이상의 안전회로로 구성함
② 안전용 비상정지 스위치의 접점은 Safety Controller 또는 Safety PLC를 통해 입력하여 제어 함
③ 비상정지, 차단장치와 기타(Door Interlock등) 안전관련 회로는 용도별로 각각 분리 함(직렬연결, 혼합배선 불가)
④ Safety Relay 및 전자 접촉기 b접점의 작동 여부는 모니터링 되어 회로의 고장 여부를 판단할 수 있어야 함
(Feedback 회로 구성)
단, 회로의 고장이 발생하면 설비의 재기동이 되지 않도록 구성해야 함



안전 회로 구성 및 분석-안전 도어 스위치

Door Safety System 회로구성(Monitoring 포함)

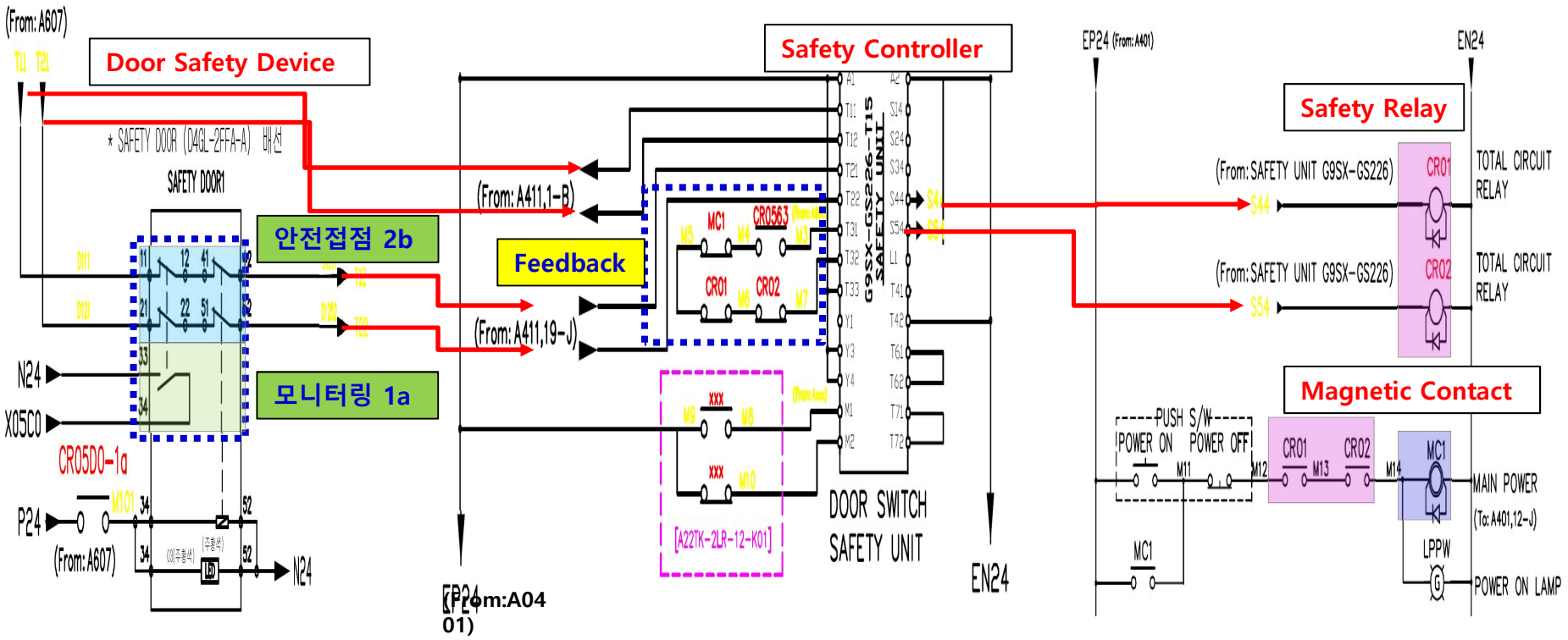
Door Safety 회로조건

① 비상 정지, 비상 차단 장치 그리고 Door Interlock의 회로는 각각 분리하여 Safety Controller 또는 Safety PLC로 구성 및 제어(범용 PLC 적용불가)

② Door Safety Device의 출력 접점은 2b(안전접점)/1a(Monitoring 접점)를 사용하여 이상 발생 시 즉시 위치 확인이 가능해야 함(Monitoring이 되어야 함)

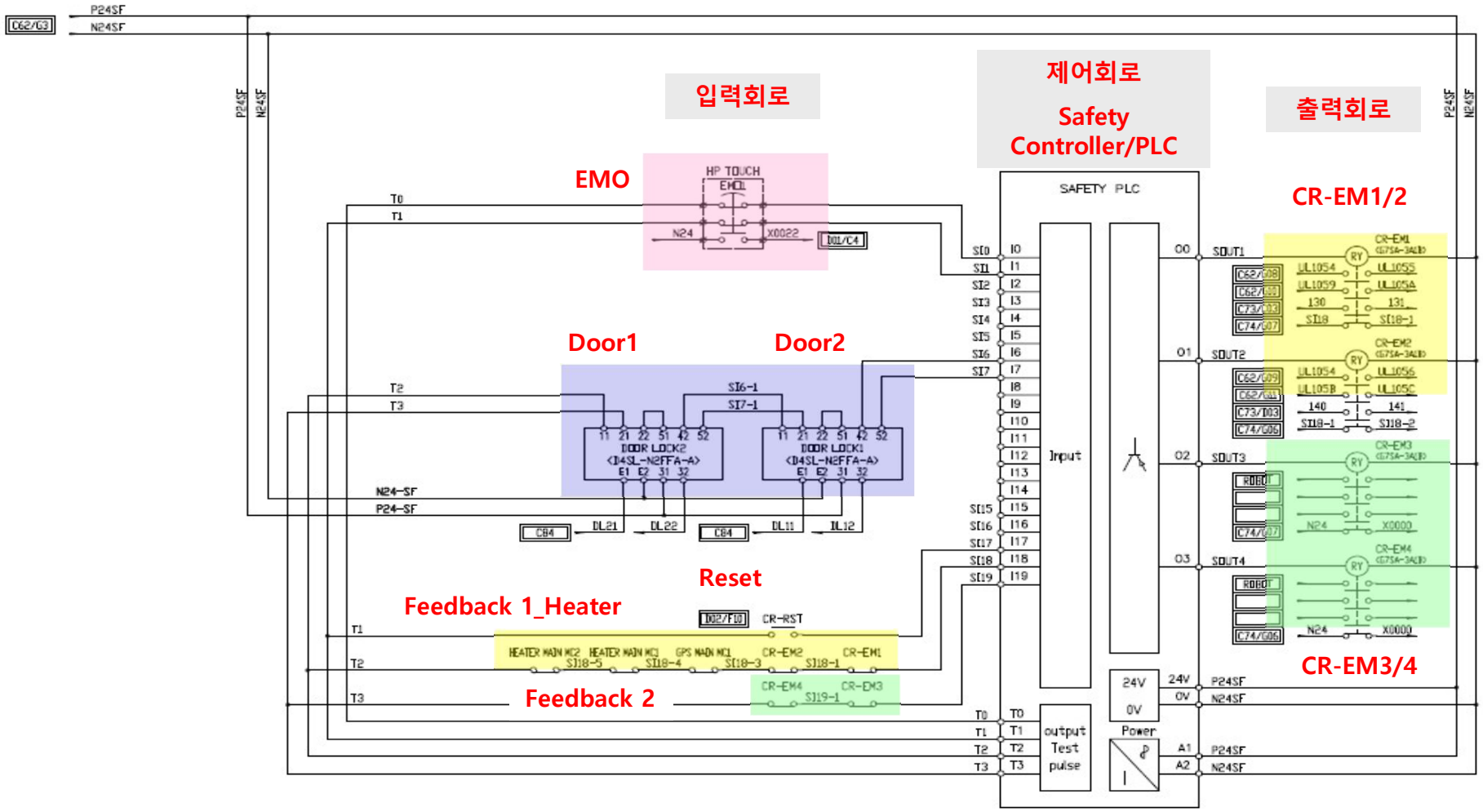
③ Door Safety Device를 통해 차단되는 전원의 Safety Relay(EN50205를 만족) 와 MC(EC60947-4-1(Mirror Contact Type)) 인증 품 사용해야 함

④ Safety Relay(EN50205를 만족)하는 인증된 Safety Relay를 적용하여 제어하고 고장 상태가 확인될 수 있도록 Feedback 회로를 Safety Controller & Safety PLC에 구성

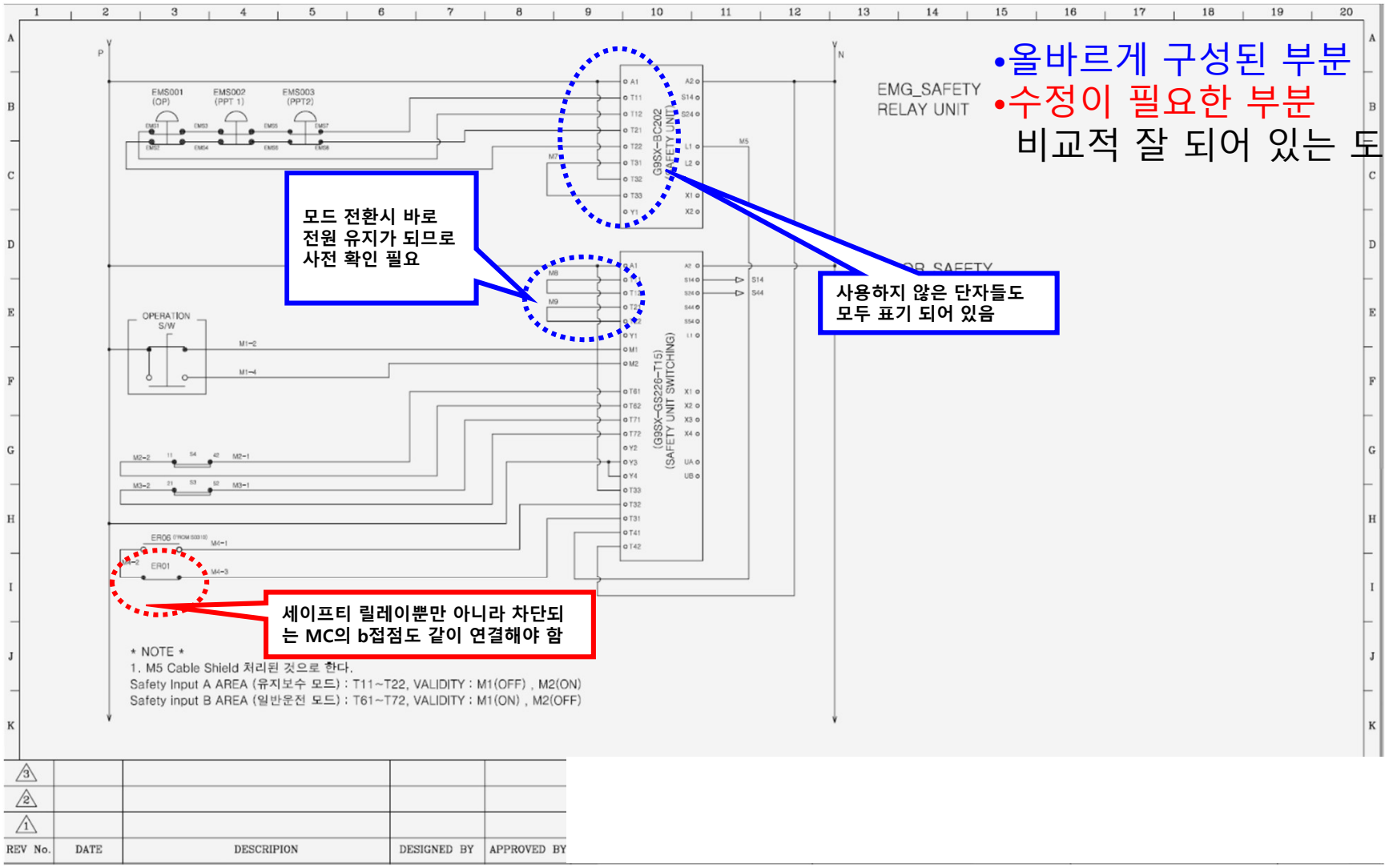


실제 안전 회로 분석

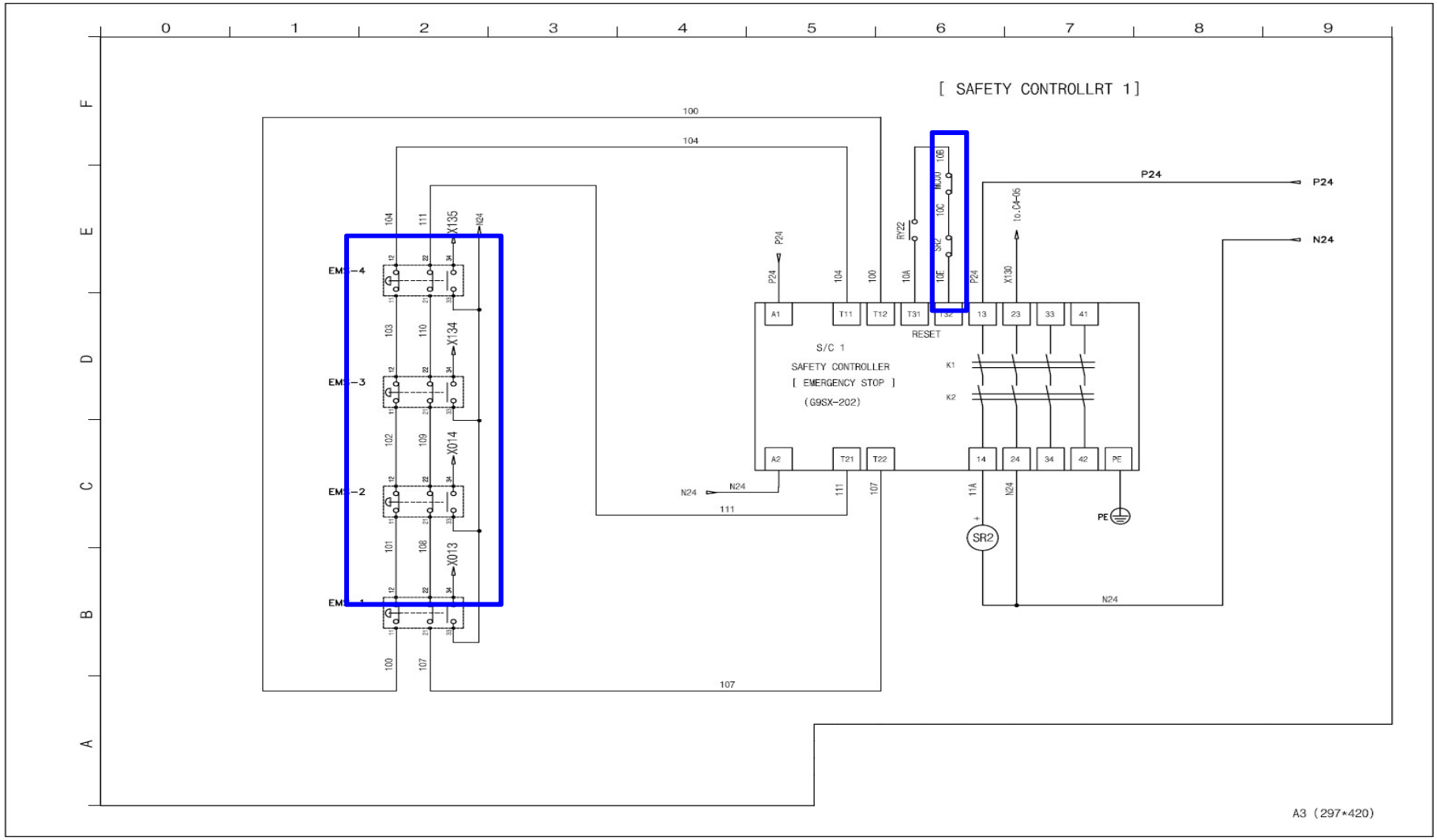
실제 안전 회로 도면 구성 분석



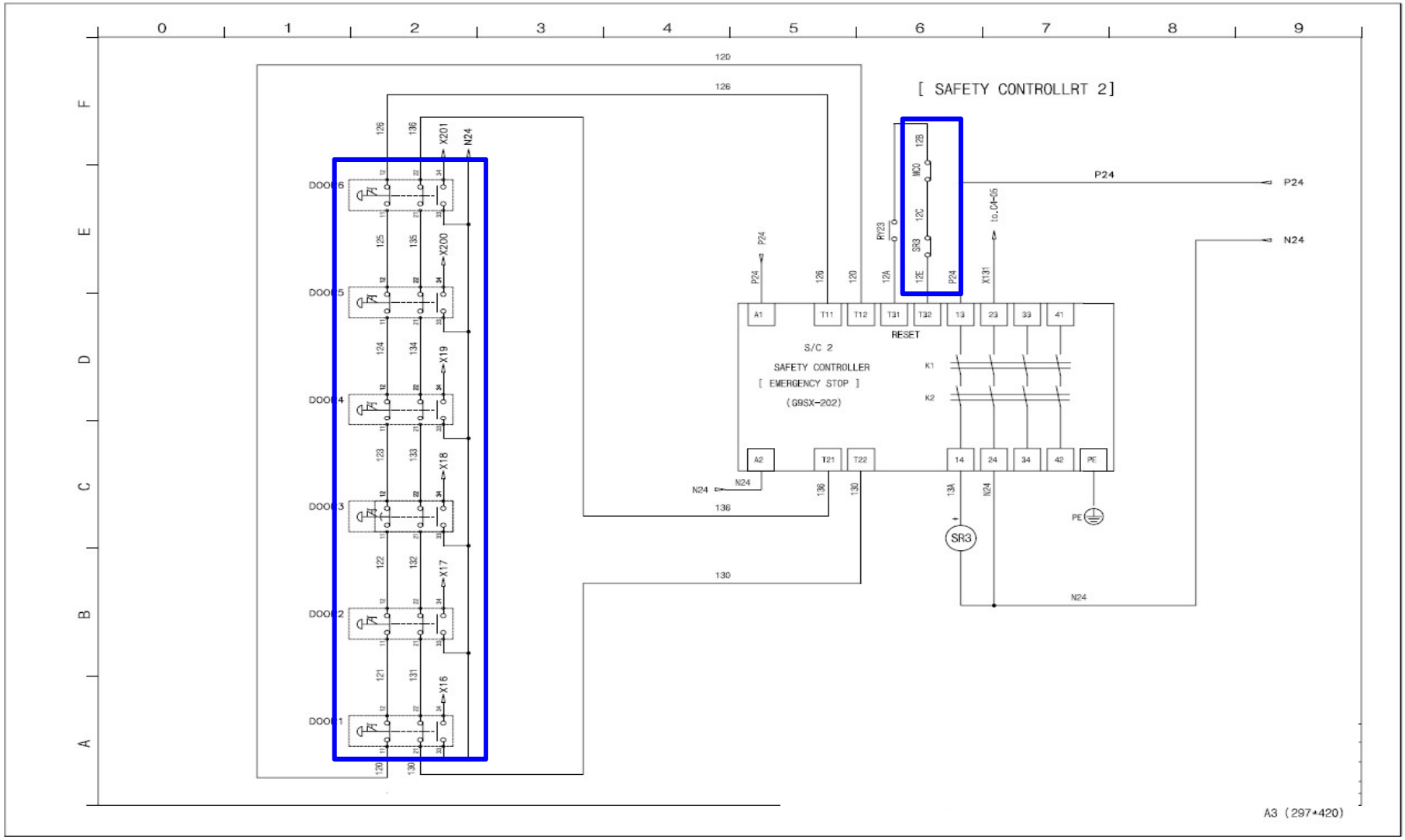
실제 안전 회로 분석


•올바르게 구성된 부분
•수정이 필요한 부분
비교적 잘 되어 있는 도면
EMG_SAFETY
RELAY UNIT
모드 전환시 바로
전원 유지가 되므로
사전 확인 필요
사용하지 않은 단자들도
모두 표기 되어 있음
세이프티 릴레이뿐만 아니라 차단되
는 MC의 b접점도 같이 연결해야 함
EMS001
(OP)
EMS002
(PPT 1)
EMS003
(PPT2)
OPERATION
S/W
G9SX-BC202
(SAFETY UNIT)
(G9SX-GS226-T15)
(SAFETY UNIT SWITCHING)
* NOTE *
1. M5 Cable Shield 처리된 것으로 한다.
Safety Input A AREA (유지보수 모드) : T11~T22, VALIDITY : M1(OFF) , M2(ON)
Safety Input B AREA (일반운전 모드) : T61~T72, VALIDITY : M1(ON) , M2(OFF)
REV No.
DATE
DESCRIPION
DESIGNED BY
APPROVED BY

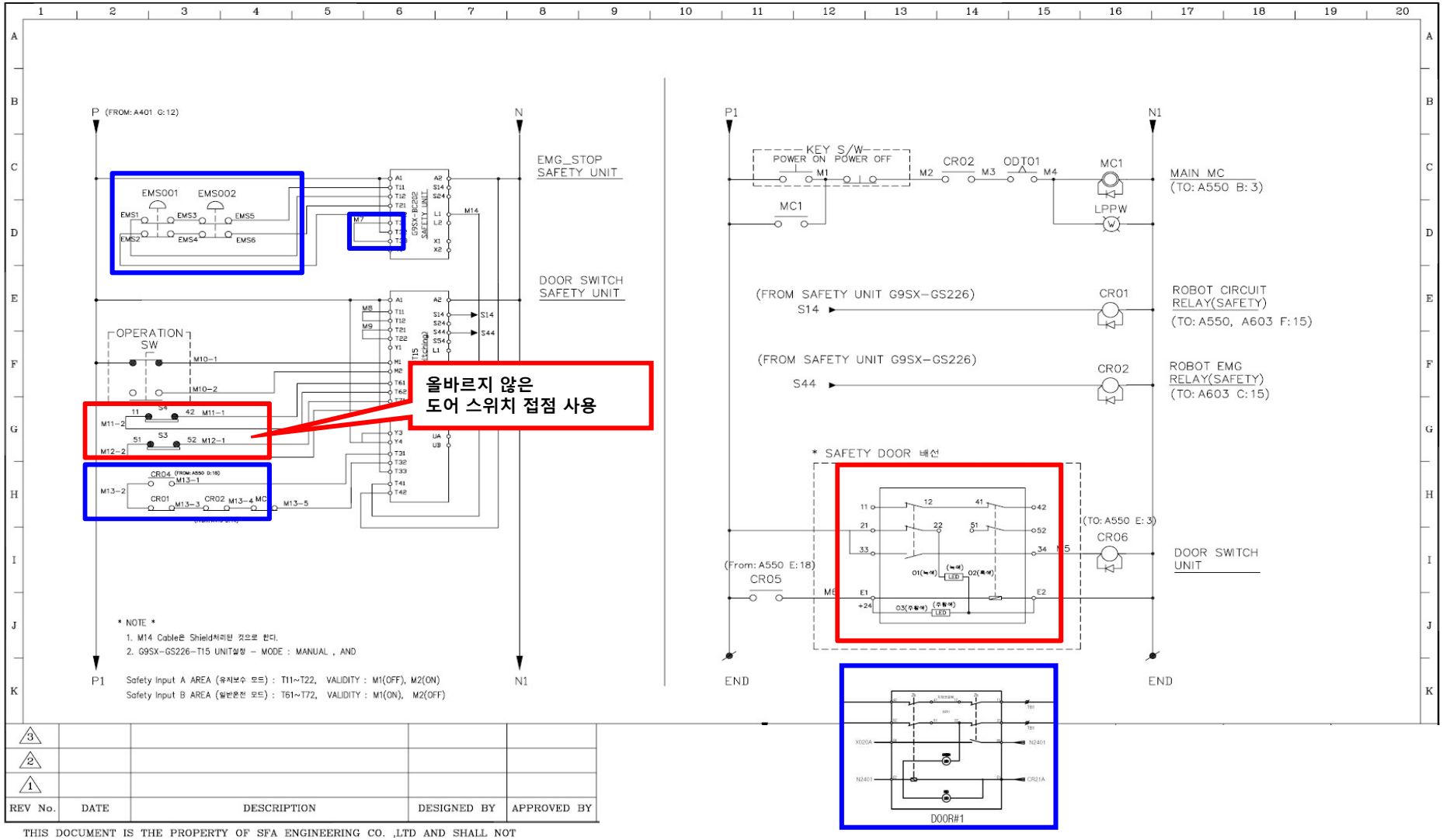
실제 안전 회로 분석


[SAFETY CONTROLLRT 1]
S/C 1
SAFETY CONTROLLER
[EMERGENCY STOP]
(G9SX-202)
RESET
SR2
P24
N24
PE
100
104
107
111
A3 (297*420)

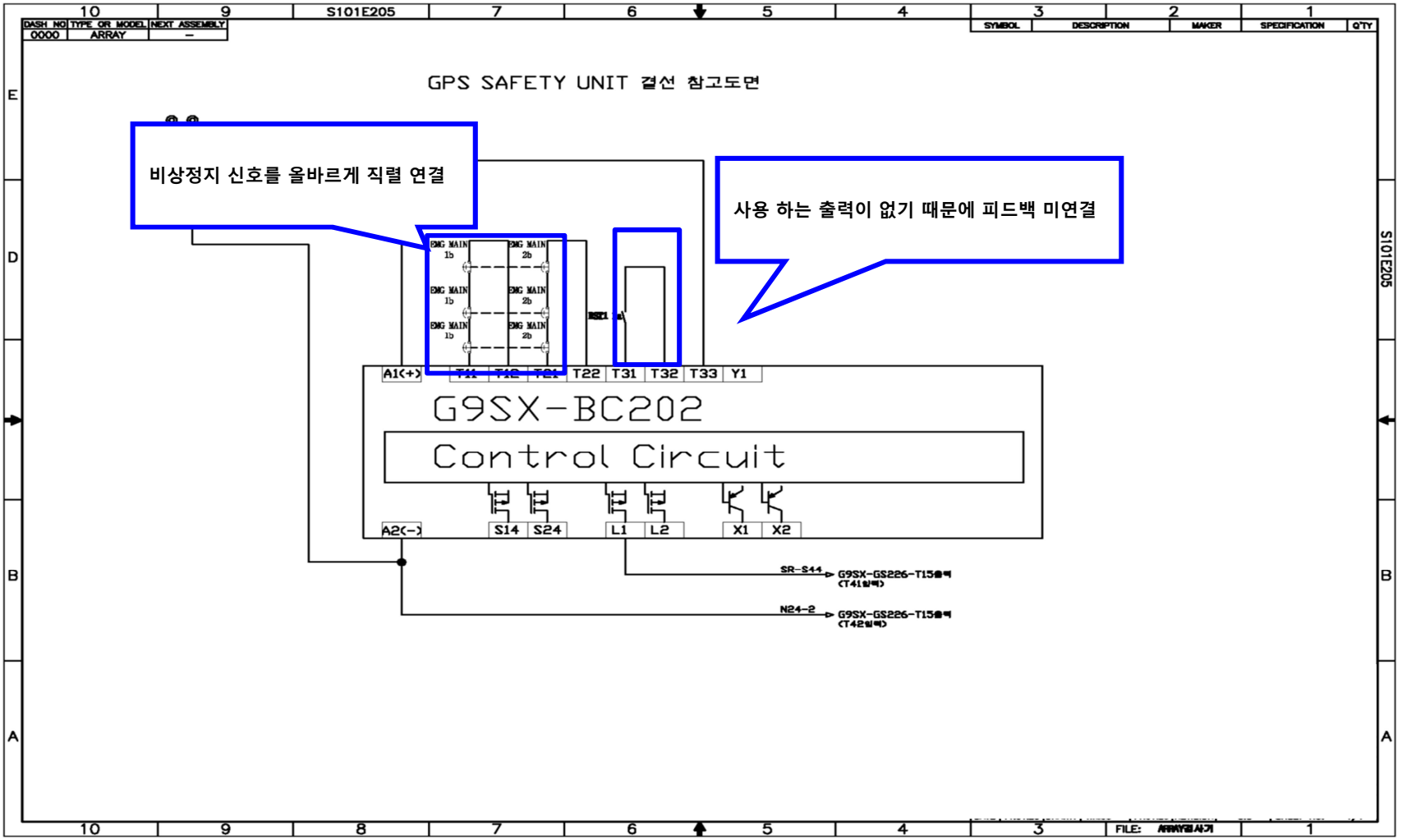
실제 안전 회로 분석


[SAFETY CONTROLLRT 2]
S/C 2
SAFETY CONTROLLER
[EMERGENCY STOP]
(G9SX-202)
RESET
SR3
P24
N24
PE
A3 (297*420)

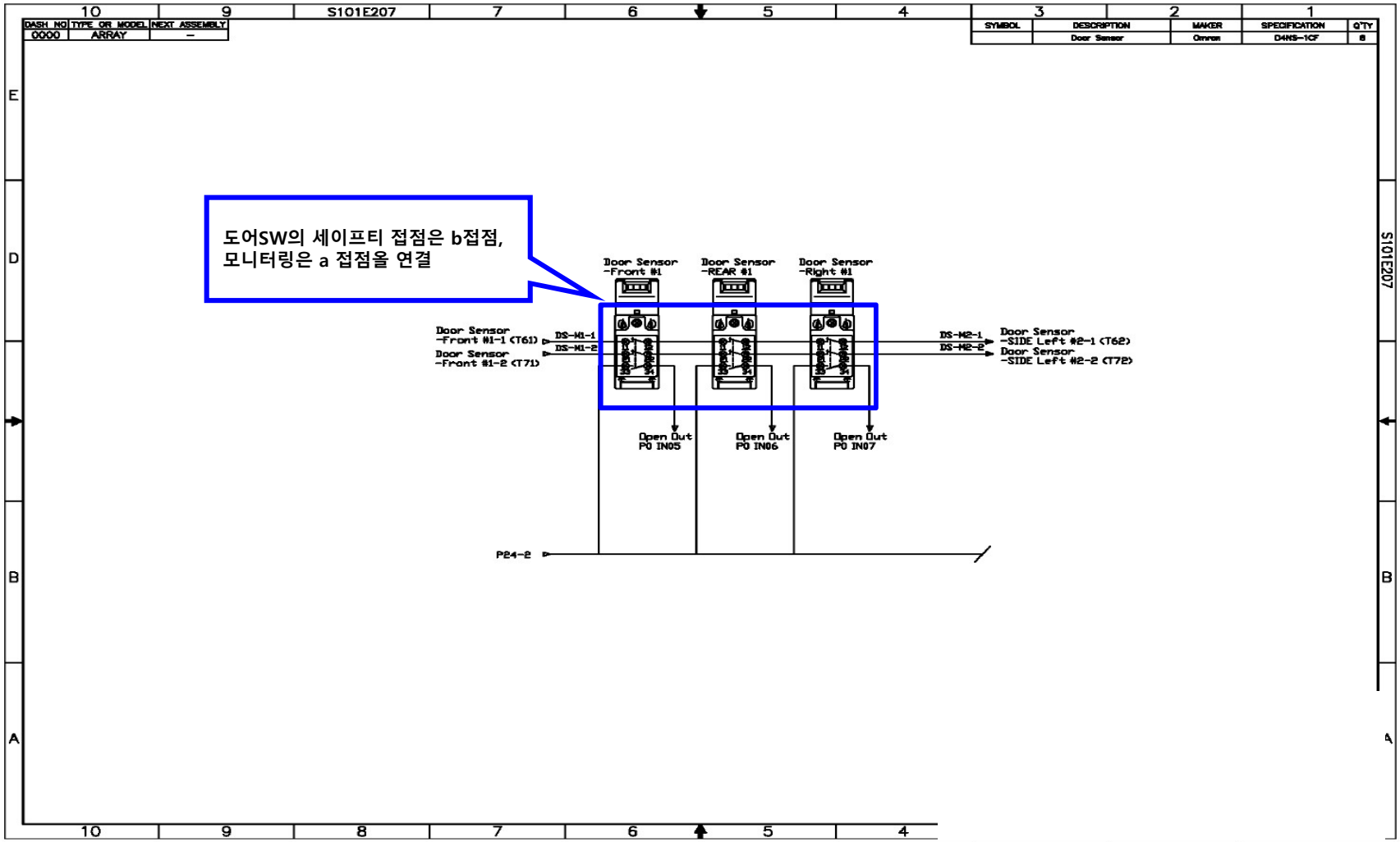
실제 안전 회로 분석



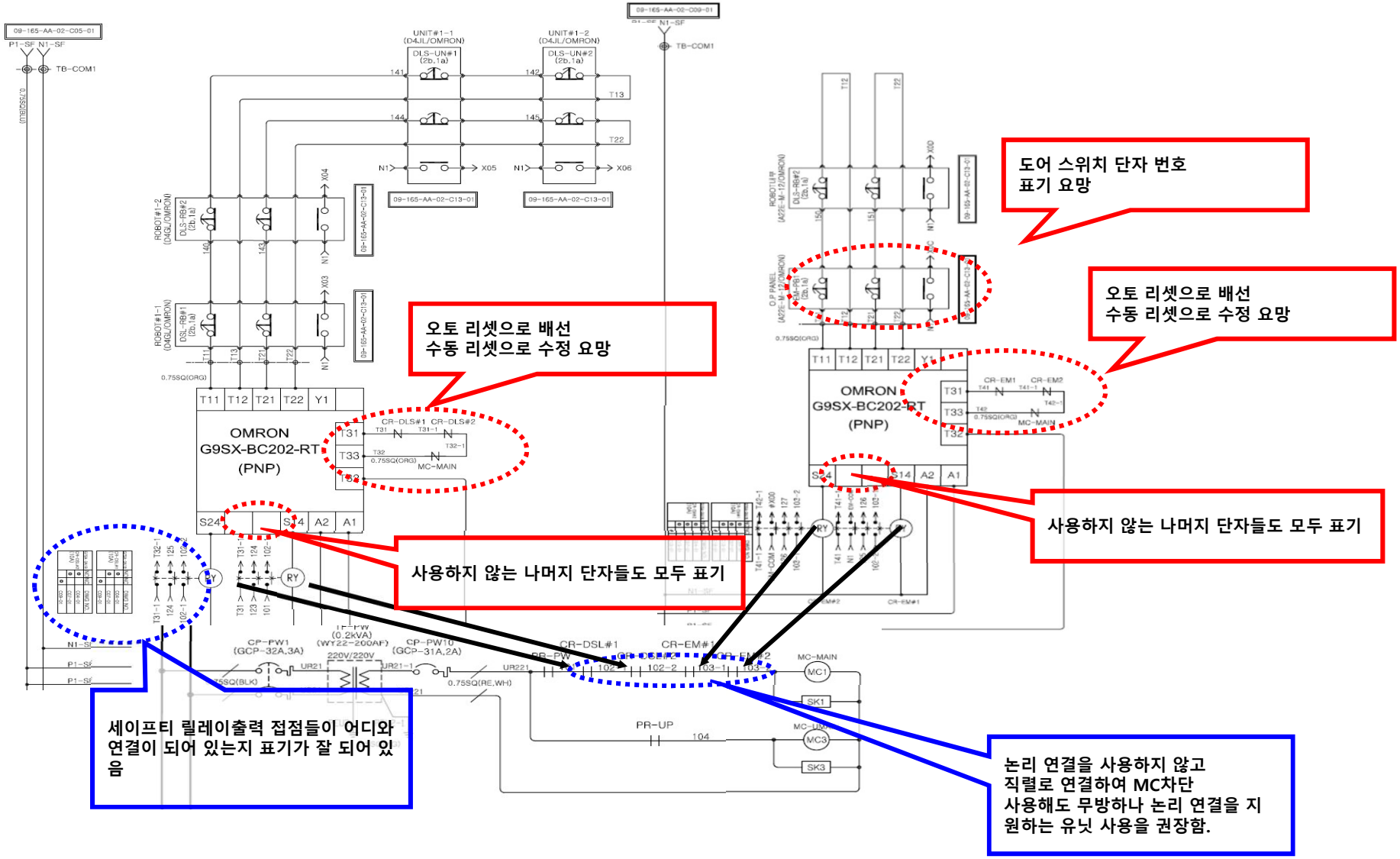
실제 안전 회로 분석


GPS SAFETY UNIT 결선 참고도면
비상정지 신호를 올바르게 직렬 연결
사용 하는 출력이 없기 때문에 피드백 미연결
A1(+)
T22
T31
T32
T33
Y1
G9SX-BC202
Control Circuit
A2(-)
S14
S24
L1
L2
X1
X2
S101E205

실제 안전 회로 분석


S101E207
SYMBOL
DESCRIPTION
MAKER
SPECIFICATION
Q'TY
Door Sensor
Omron
D4NS-1CF
8
도어SW의 세이프티 접점은 b접점,
모니터링은 a 접점을 연결
Door Sensor -Front #1
Door Sensor -REAR #1
Door Sensor -Right #1
Door Sensor -Front #1-1 (T61)
Door Sensor -Front #1-2 (T71)
DS-M1-1
DS-M1-2
DS-M2-1
DS-M2-2
Door Sensor -SIDE Left #2-1 (T62)
Door Sensor -SIDE Left #2-2 (T72)
Open Out P0 IN05
Open Out P0 IN06
Open Out P0 IN07
P24-2

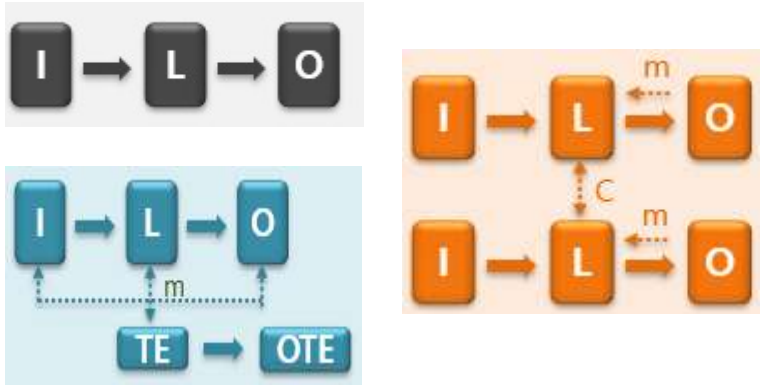
실제 안전 회로 분석


도어 스위치 단자 번호
표기 요망
오토 리셋으로 배선
수동 리셋으로 수정 요망
오토 리셋으로 배선
수동 리셋으로 수정 요망
사용하지 않는 나머지 단자들도 모두 표기
사용하지 않는 나머지 단자들도 모두 표기
세이프티 릴레이출력 접점들이 어디와 연결이 되어 있는지 표기가 잘 되어 있음
논리 연결을 사용하지 않고 직렬로 연결하여 MC차단 사용해도 무방하나 논리 연결을 지원하는 유닛 사용을 권장함.
OMRON
G9SX-BC202-RT
(PNP)
OMRON
G9SX-BC202-RT
(PNP)
T11
T12
T21
T22
Y1
S24
S14
A2
A1
T31
T33
T32
CR-DLS#1
CR-DLS#2
MC-MAIN
CR-EM1
CR-EM2
CP-PW1
(GCP-32A,3A)
CP-PW10
(GCP-31A,2A)
CR-DSL#1
CR-EM#1
MC-MAIN
MC1
SK1
MC3
SK3
PR-UP
104

Performance Level의 구성

PL 평가 요소

CATEGORY

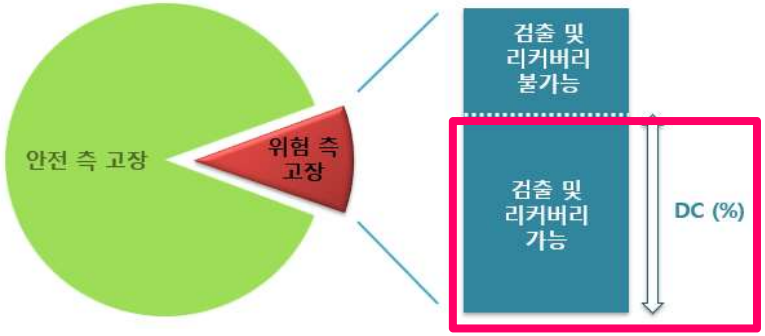


CAT B~4

MTTFd

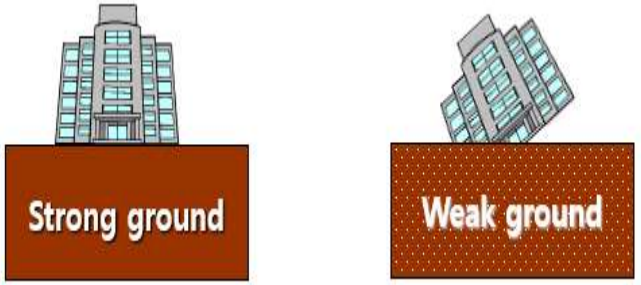
Low or Medium or High

DCavg



None or Low or Medium or High

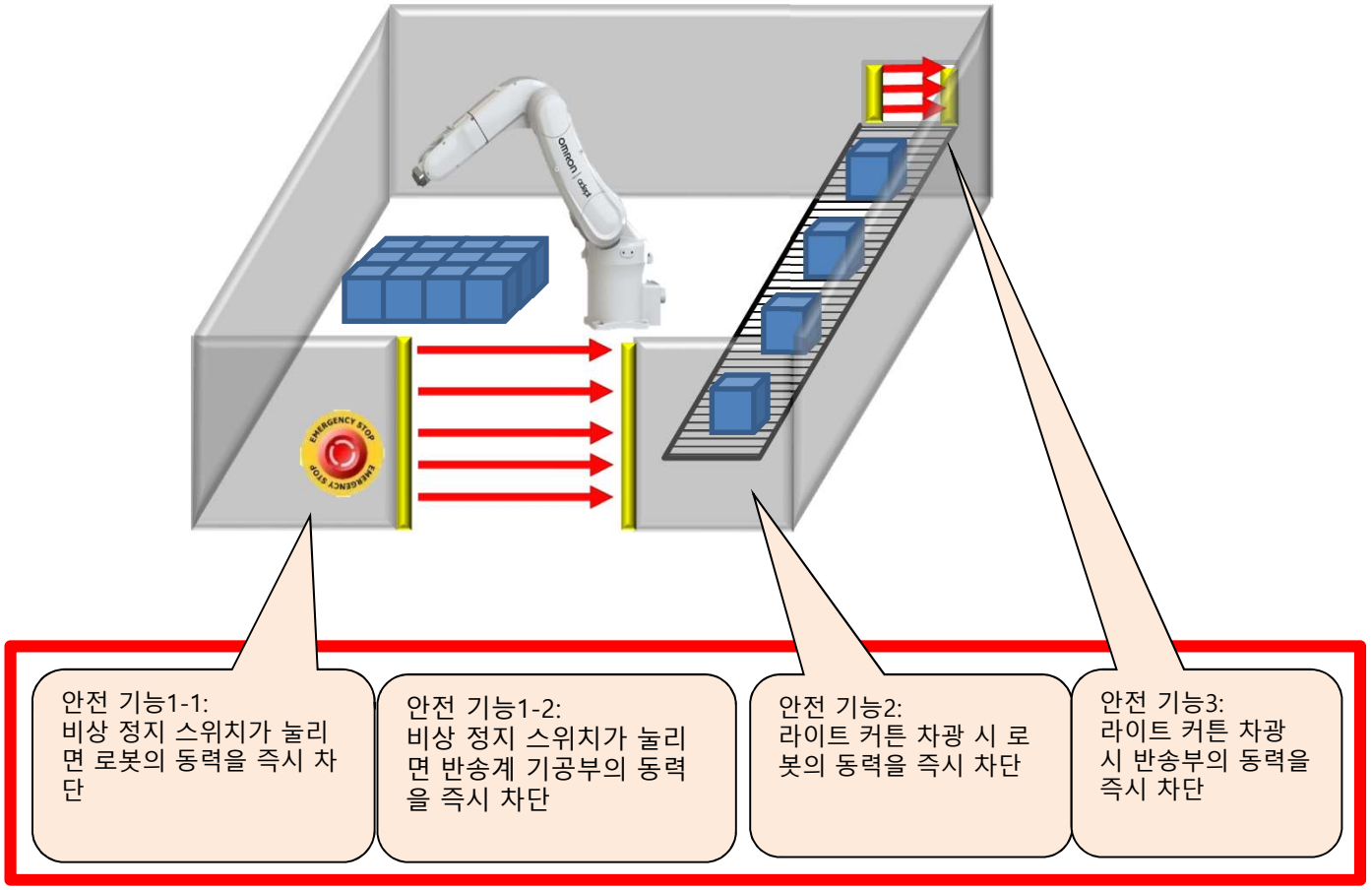
CCF



CCF≥65

PL평가 과정 - 안전 기능 식별

- **SRP/CS들에 의해 수행될 수 있는 안전기능을 식별 및 안전기능에 필요한 특성을 지정**



SRP/CS들에 의해 수행될 수 있는 안전기능을 식별

SRP/CS들에 의해 수행될 수 있는 안전기능을 식별 및 특성 지정

PLr결정

안전기능을 수행하는 안전부품을 확인

성능평가

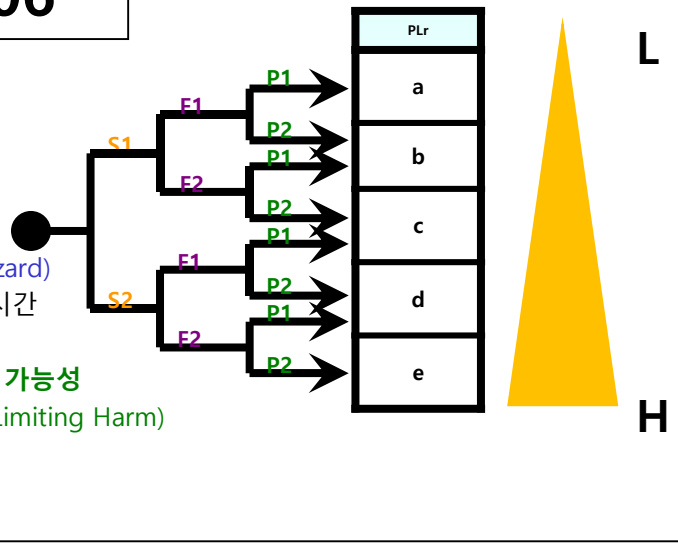
결과 확인 및 검토

PL평가 과정 – PLr 결정

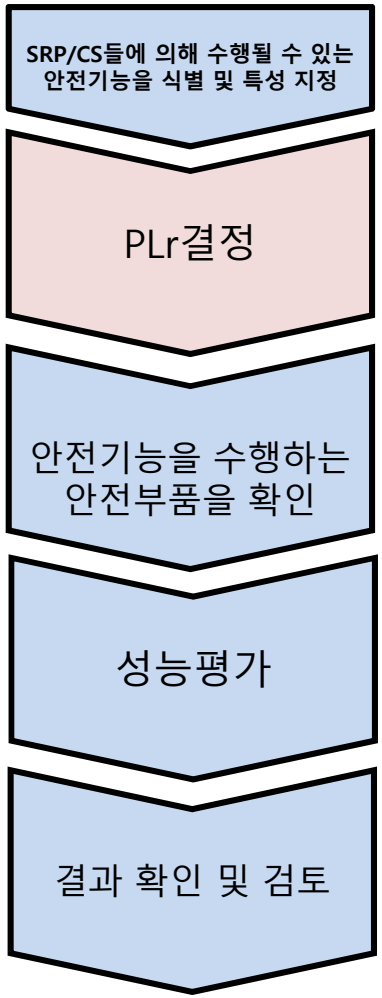
- 요구되는 PLr을 결정

ISO13849-1:2006

S : 상해의 중대도
(Severity of Injury)
·S1 : 경상
·S2 : 중증(후유증, 사망 등)
F : 위험에 처해지는 빈도
(Frequency and/or Exposure to Hazard)
·F1 : 보기 드물게 발생하거나 단시간
·F2 : 빈번히 발생하거나 장시간
P : 위험을 피하거나 손해를 제한할 가능성
(Possibility of Avoiding Hazard or Limiting Harm)
·P1 : 특정의 조건하에서 가능
·P2 : 불가능

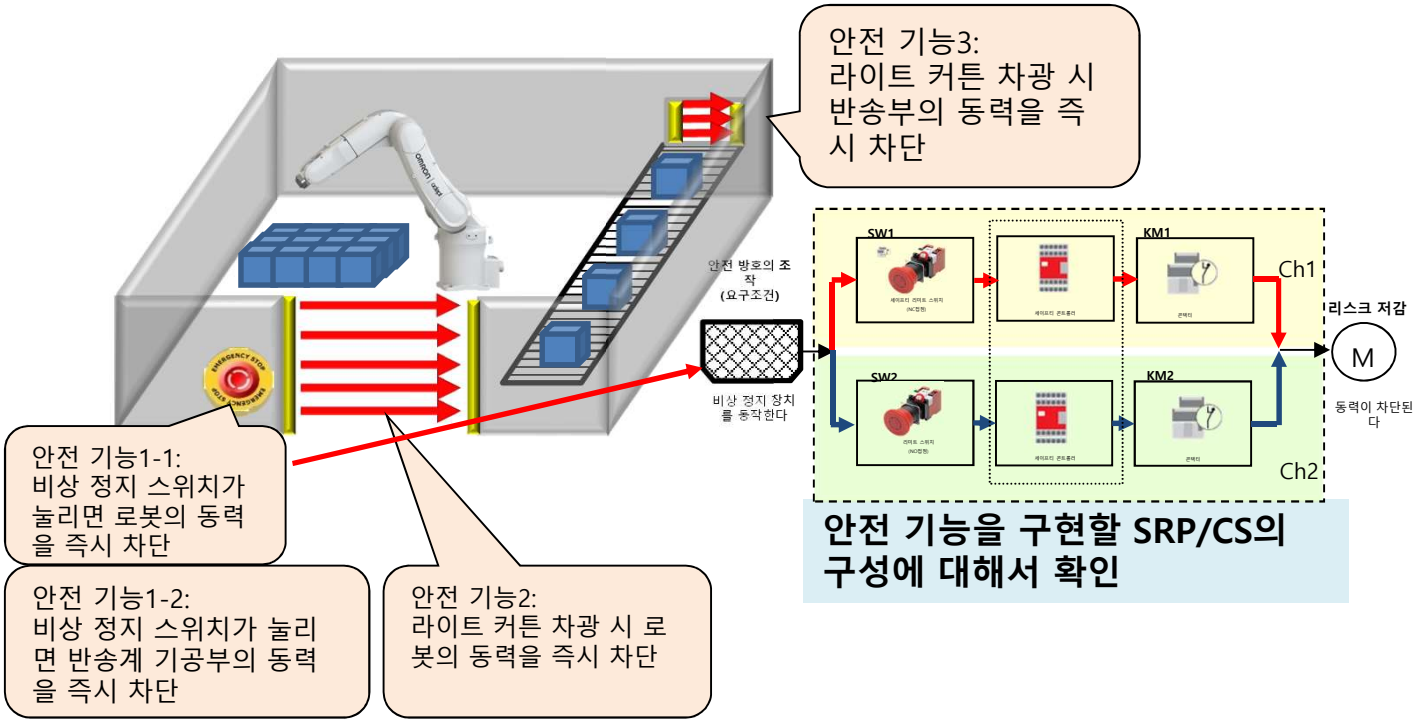


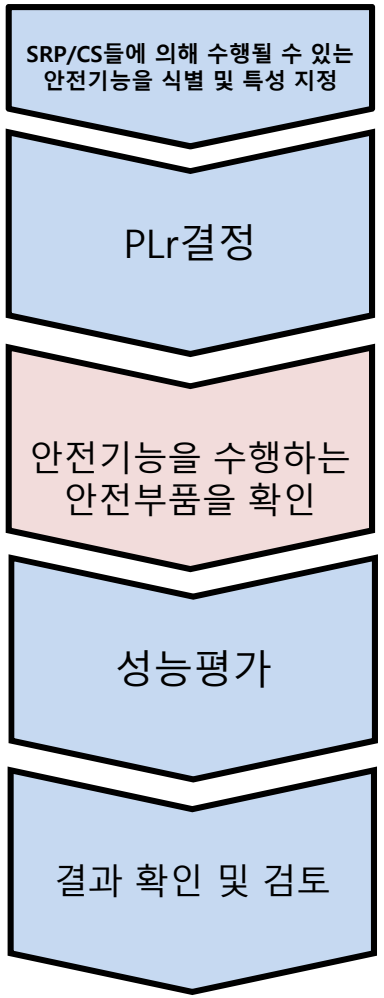
공정을 안전하게 사용하기 위해 SRP/CS로 만족해야 하는 PLr(required Performance Level)측정



PL평가 과정 – 안전 기능 구성 부품 확인

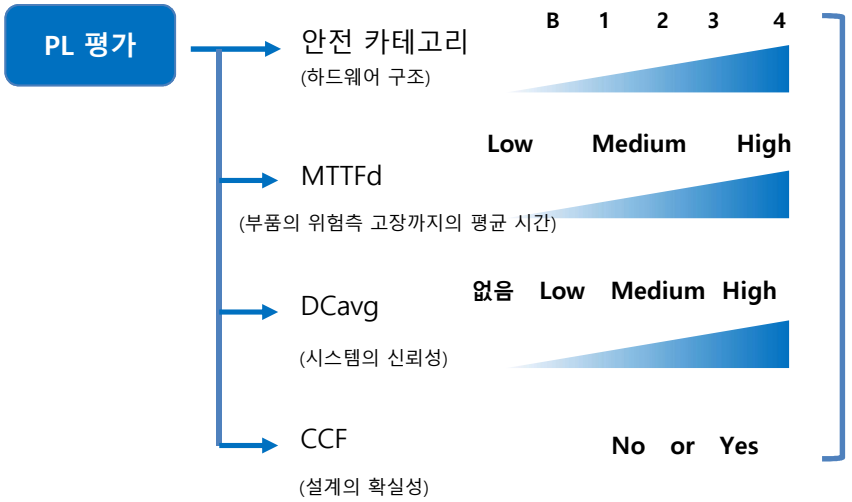
- **안전기능의 설계와 기술의 실현: 안전기능을 수행하는 안전관련 부품을 확인**
  - **안전 기능을 구성하는 안전 부품의 구성에 대해 확인**

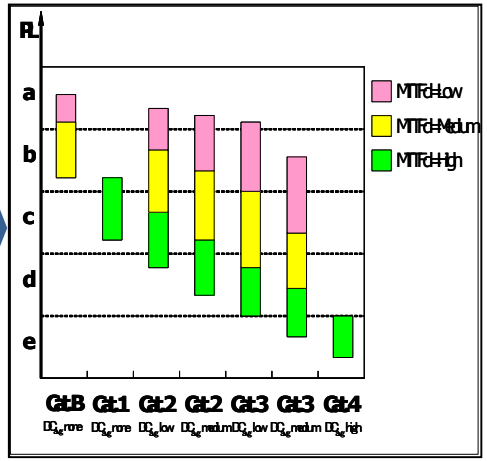




PL평가 과정 – 성능평가

- 성능 수준 평가
  - 구성 된 제품으로 구현 된 안전 기능을 ISO 13849-1에 기준하여 성능 평가 진행





안전 제품으로 구성된 안전 기능에 대한 성능 평가 진행

SRP/CS들에 의해 수행될 수 있는 안전기능을 식별 및 특성 지정

PLr결정

안전기능을 수행하는 안전부품을 확인

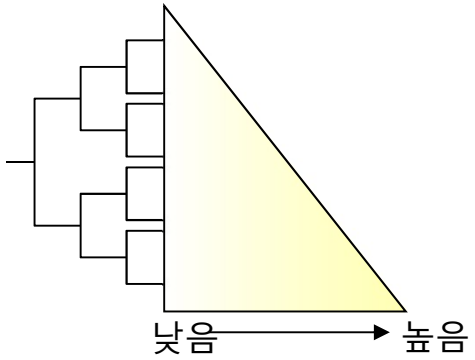
성능평가

결과 확인 및 검토

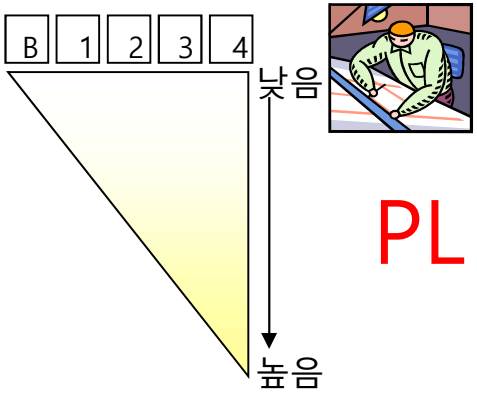
PL평가 과정 – 성능 평과 결과 확인 및 검토

안전기능을 위한 PL 확인 및 검토

PLr



a
b
c
d
e



PL

PLr≦PL

안전 제어 시스템의 성능 레벨(PL)은 항상 요구 성능 레벨(PLr)보다 이상이어야 한다.

PLr보다 PL이 작은 경우 → **안전 부품 구성 재설계 후 평가**

SRP/CS들에 의해 수행될 수 있는 안전기능을 식별 및 특성 지정

PLr결정

안전기능을 수행하는 안전부품을 확인

성능평가

결과 확인 및 검토

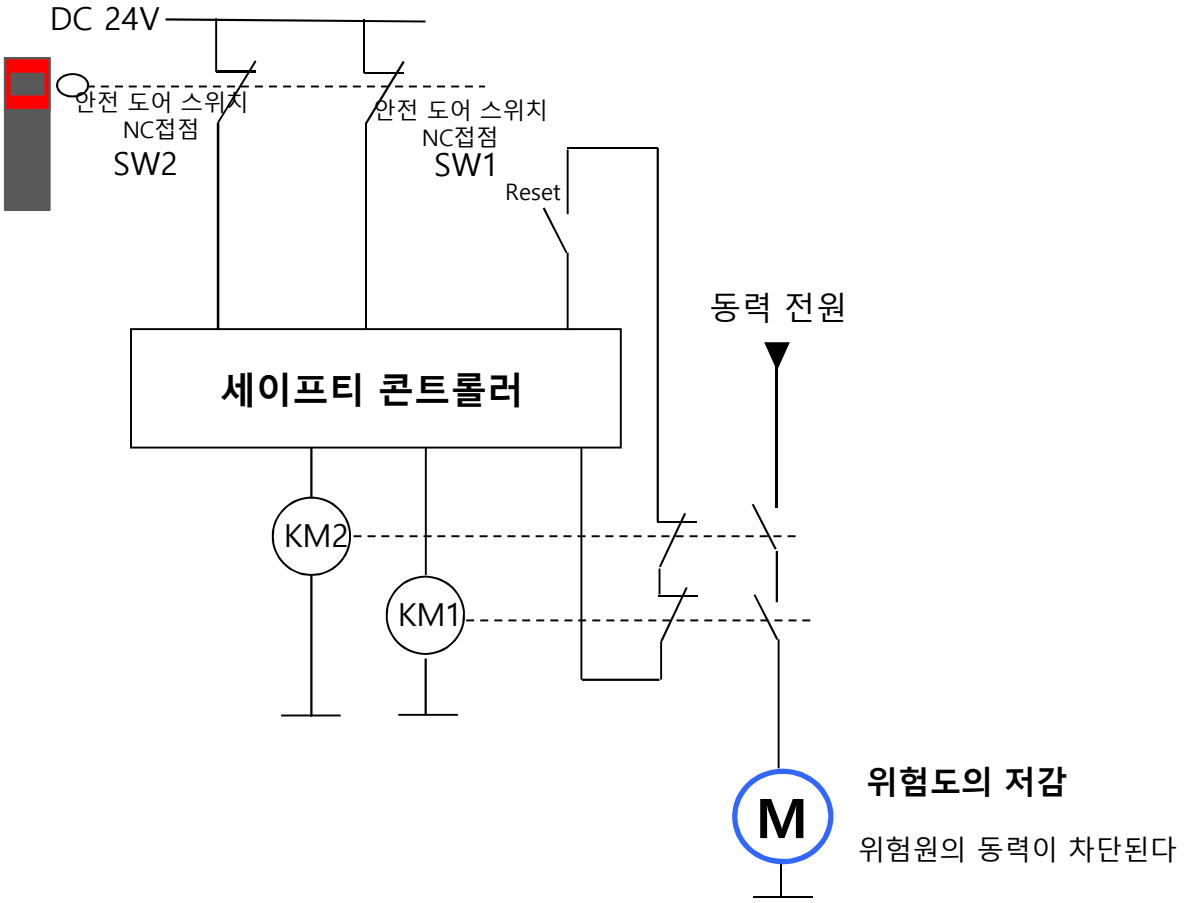
Performance Level의 계산

안전관련부

■ 세이프티 도어 스위치 1개를 이용해 구성한 안전 회로의 PL평가

안전 방호의 조작
(요구조건)

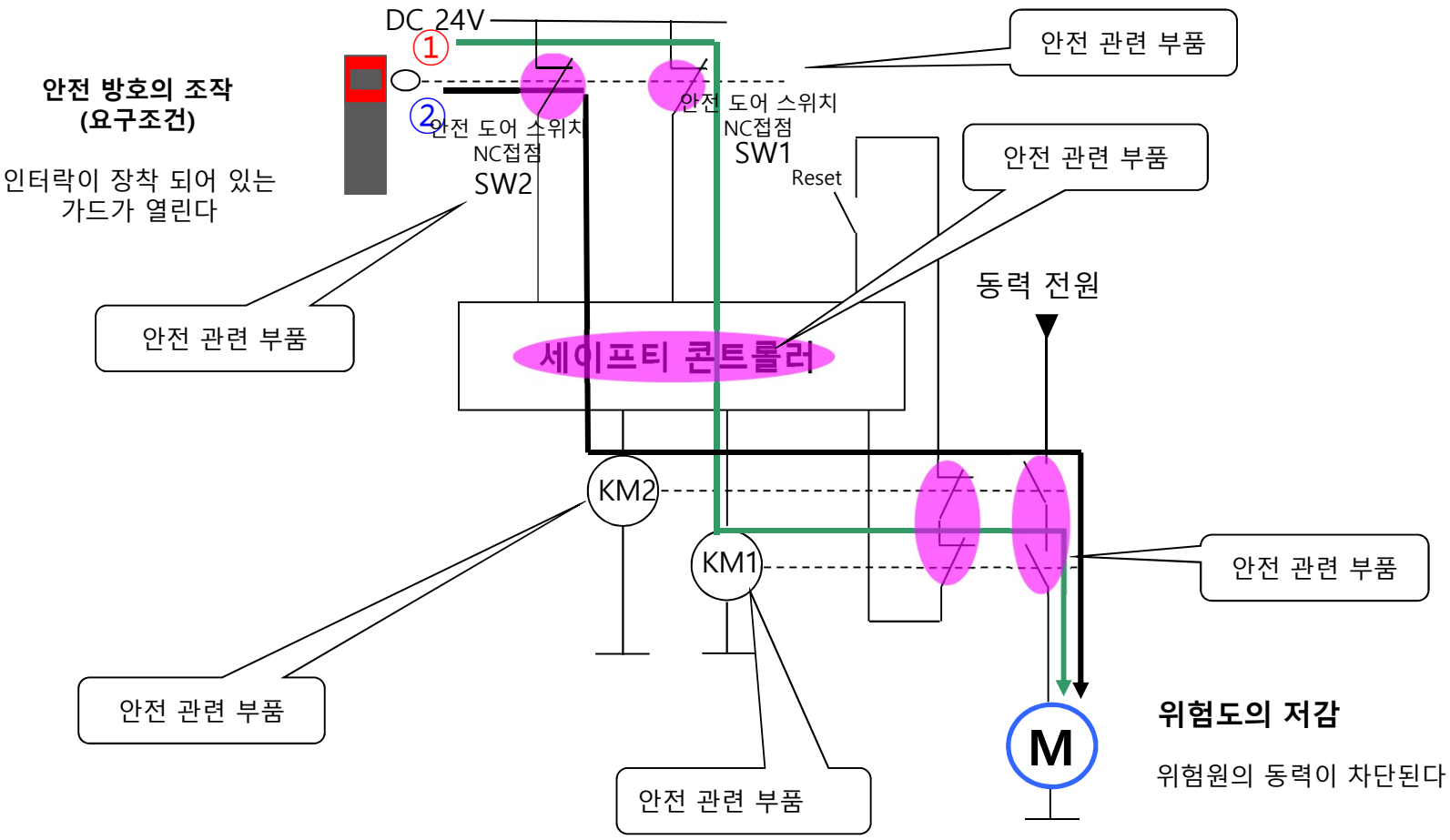
인터락이 장착 되어 있는
가드가 열린다



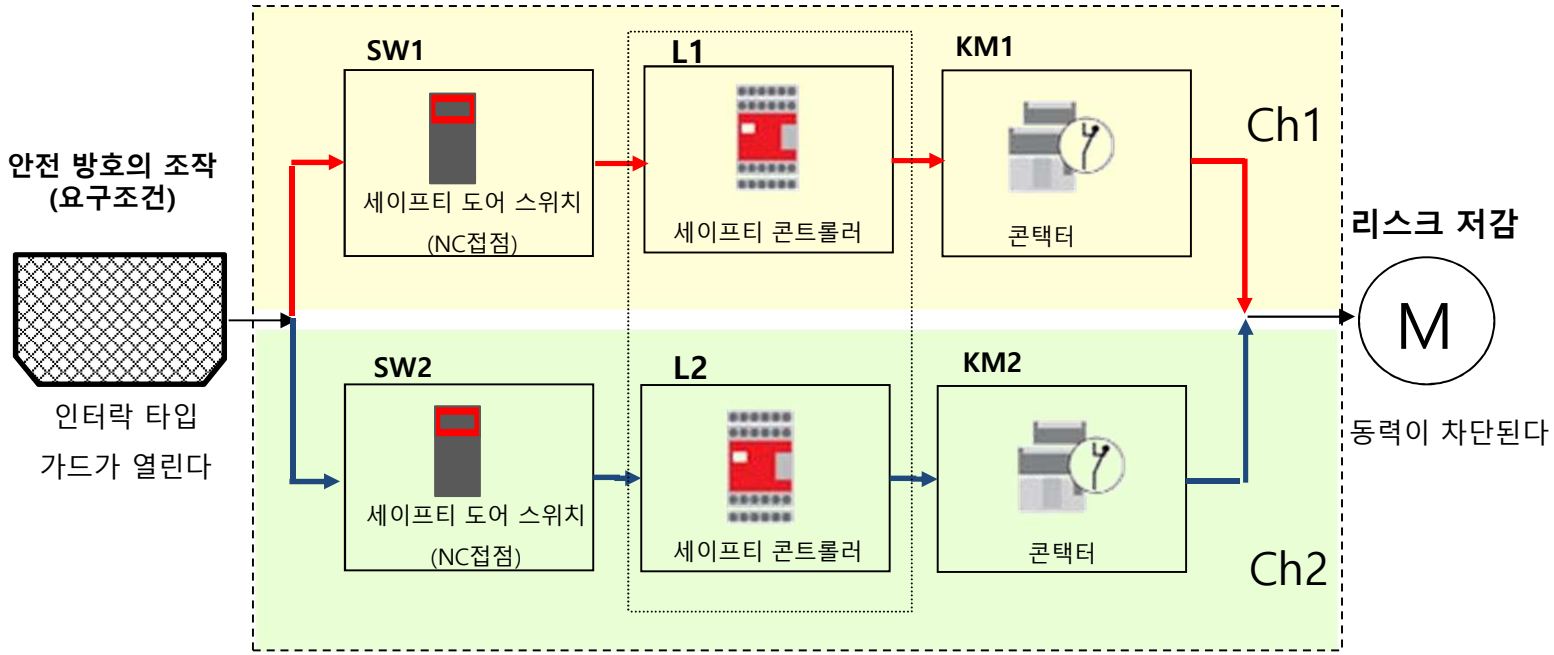
위험도의 저감

위험원의 동력이 차단된다

전달 경로와 안전관련 부품



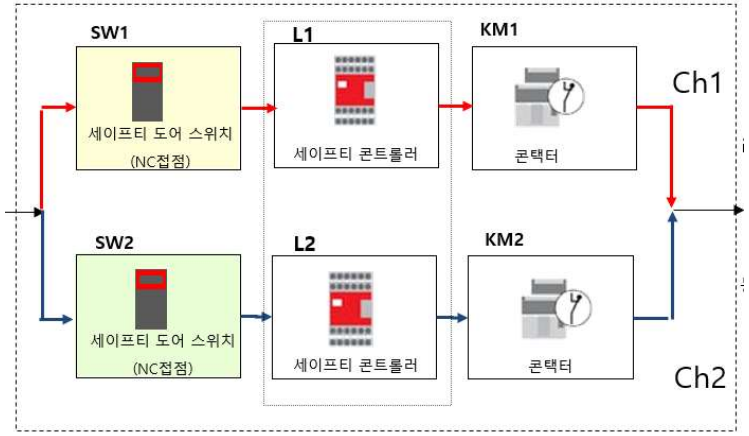
블록 다이어그램화와 카테고리



안전 시스템 관련부 구조 = Category 3

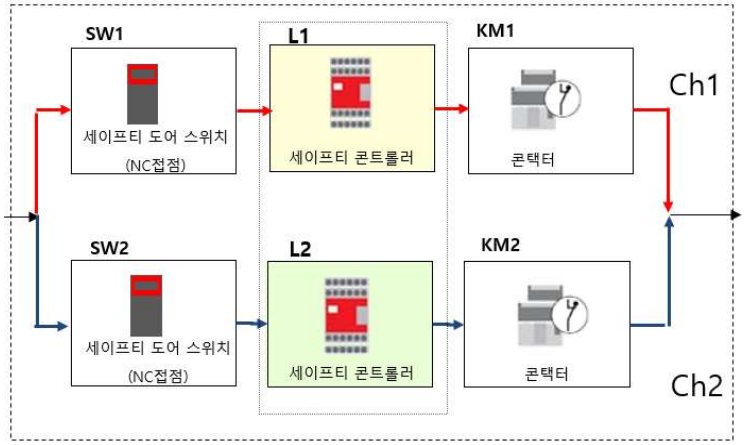
블록 다이어그램화와 MTTFd

➢ Input (입력)



변수	값
Nop (사용자 제공 수치)	20,000회/년
B10d (제조사 제공 수치)	2,000,000
MTTFd(sw1)	1,000년 (식1 참조)
MTTFd(sw2)	1,000년 (식1 참조)

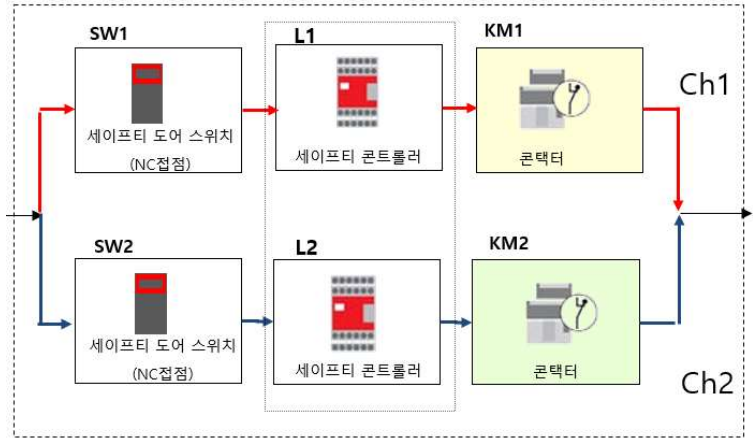
➢ Logic (제어)



변수	값
Nop (사용자 제공 수치)	-
B10d (제조사 제공 수치)	-
MTTFd(sw1)	100년
MTTFd(sw2)	100년

블록 다이어그램화와 MTTFd

➢ Output (출력)



변수	값
Nop (사용자 제공 수치)	20,000회/년
B10d (제조사 제공 수치)	400,000
MTTFd(sw1)	200년 (식1 참조)
MTTFd(sw2)	200년 (식1 참조)

➢ MTTFd 산출 (식3 참조)

채널 1: $MTTFdc1 = \frac{1}{\frac{1}{MTTFdSW1} + \frac{1}{MTTFdL1} + \frac{1}{MTTFdKM1}}$

$= \frac{1}{\frac{1}{1{,}000} + \frac{1}{100} + \frac{1}{200}}$

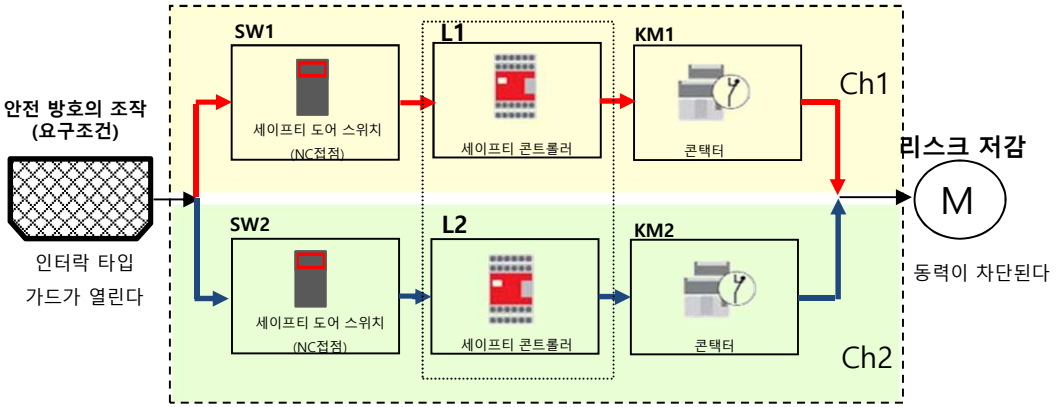
$= \boxed{62.5year}$

채널 2: $MTTFdc2 = \frac{1}{\frac{1}{MTTFdSW2} + \frac{1}{MTTFdL2} + \frac{1}{MTTFdKM2}}$

$= \frac{1}{\frac{1}{1{,}000} + \frac{1}{100} + \frac{1}{200}}$

$= \boxed{62.5year}$

블록 다이어그램화와 DCavg



DC (입력장치)	DC (논리장치)	DC (출력장치)
타당성 확인 (신호 경로 사이 구분 없음)	셀프 체크	논리(L)내에서의 출력신호와 중간 결과의 교차감시와 합선감지
최종 DC 값 =85%	최종 DC 값 = 99%	최종 DC 값 = 99%

➢ DCavg 산출

채널 1: $DCavgc1 = \frac{\frac{DC_{SW1}}{MTTFdSW1}+\frac{DC_{L1}}{MTTFdL1}+\frac{DC_{KM}}{MTTFdKM1}}{\frac{1}{MTTFdSW1}+\frac{1}{MTTFdL1}+\frac{1}{MTTFdKM1}}$

$= \frac{\frac{85}{1{,}000}+\frac{99}{100}+\frac{99}{200}}{\frac{1}{1{,}000}+\frac{1}{100}+\frac{1}{200}}$

$= 98.12\%$

채널 2 : $DCavgc2 = \frac{\frac{DC_{SW2}}{MTTFdSW2}+\frac{DC_{L2}}{MTTFdL2}+\frac{DC_{KM2}}{MTTFdKM2}}{\frac{1}{MTTFdSW2}+\frac{1}{MTTFdL2}+\frac{1}{MTTFdKM2}}$

$= \frac{\frac{85}{1{,}000}+\frac{99}{100}+\frac{99}{200}}{\frac{1}{1{,}000}+\frac{1}{100}+\frac{1}{200}}$

$= 98.12\%$

최종 PL 평가

PL의 판정 (ISO13849-1 Annex K Table K.1 인용)

Category		B	1	2				4
DCavg		None		Low 60≦DCavg	Medium 90≦DCavg	Low 60≦DCavg	Medium 90≦DCavg	High 99≦DCavg
CCF		평가 대상 외		65 ≦ CCF	65 ≦ CCF	65 ≦ CCF	65 ≦ CCF	65 ≦ CCF
Low	**3≦MTTFd**	a		a	a	a	b	
	3.3≦MTTFd	a		a	a	a	b	
	3.6≦MTTFd	a		a	a	a	b	
	3.9≦MTTFd	a		a	a	b	b	
	4.3≦MTTFd	a		a	a	b	b	
	4.7≦MTTFd	a		a	a	b	b	
	5.1≦MTTFd	a		a	a	b	b	
	5.6≦MTTFd	a		a	b	b	c	
	6.2≦MTTFd	a		a	b	b	c	
	6.8≦MTTFd	a		a	b	b	c	
	7.5≦MTTFd	a		b	b	b	c	
	8.2≦MTTFd	a		b	b	b	c	
	9.1≦MTTFd	a		b	b	b	c	
Medium	**10≦MTTFd**	a		b	b	b	c	
	11≦MTTFd	a		b	b	c	c	
	12≦MTTFd	b		b	b	c	c	
	13≦MTTFd	b		b	b	c	d	
	15≦MTTFd	b		b	b	c	d	
	16≦MTTFd	b		b	c	c	d	
	18≦MTTFd	b		b	c	c	d	
	20≦MTTFd	b		b	c	c	d	
	22≦MTTFd	b		c	c	c	d	
	24≦MTTFd	b		c	c	d	d	
	27≦MTTFd	b		c	c	d	d	
High	**30≦MTTFd**		b	c	c	d	d	e
	33≦MTTFd		b	c	c	d	d	e
	36≦MTTFd		b	c	d	d	d	e
	39≦MTTFd		c	c	d	d	d	e
	43≦MTTFd		c	c	d	d	d	e
	47≦MTTFd		c	c	d	d	d	e
	51≦MTTFd		c	c	d	d	d	e
	56≦MTTFd		c	c	d	d	d	e
	62≦MTTFd		c	d	d	d	e	e
	68≦MTTFd		c	d	d	d	e	e
	75≦MTTFd		c	d	d	d	e	e
	82≦MTTFd		c	d	d	d	e	e
	91≦MTTFd		c	d	d	d	e	e
	100≦MTTFd		c	d	d	d	e	e

Category 3

+

62≦ MTTFd < 68

+

DCavg – Mid

+

CCF (65점 이상)

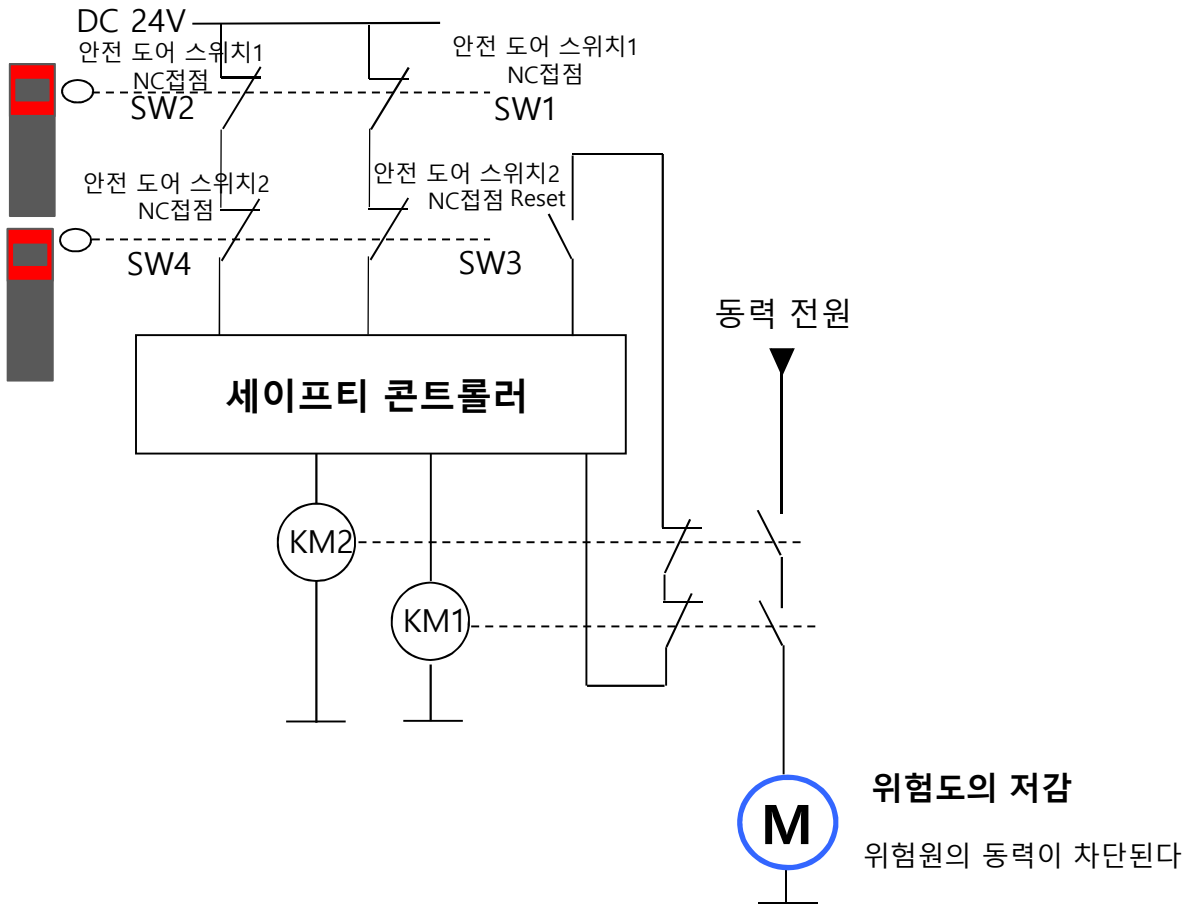
"PLe"

안전관련부

■ 세이프티 도어 스위치 2개를 직렬연결 하여 구성한 안전 회로의 PL평가

안전 방호의 조작
(요구조건)

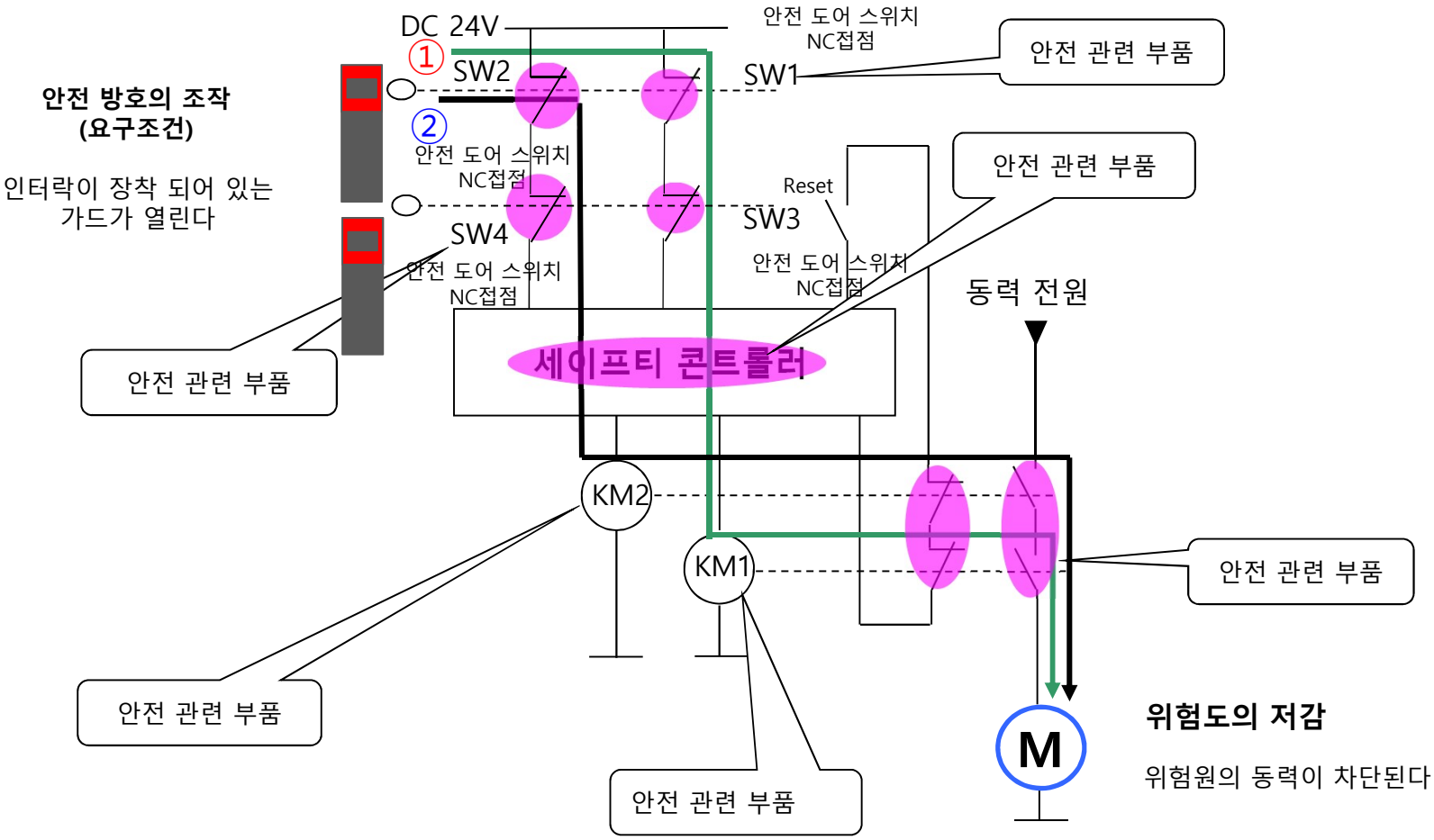
인터락이 장착 되어 있는
가드가 열린다



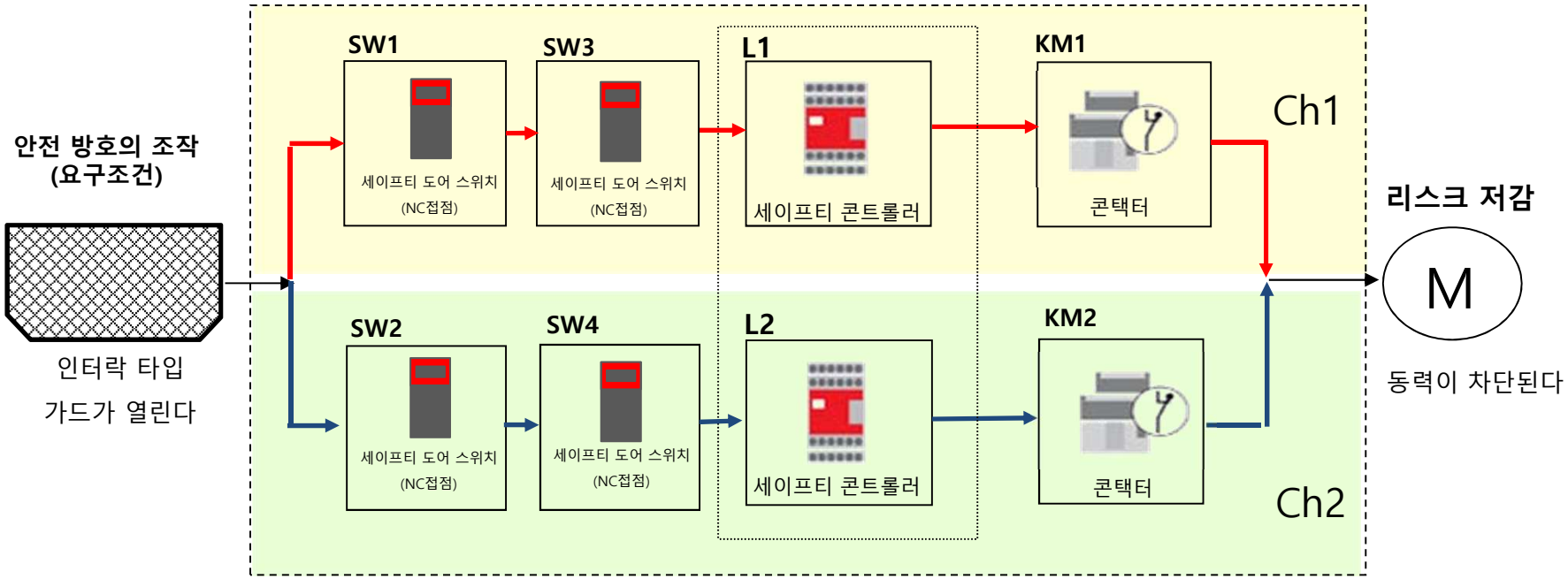
위험도의 저감

위험원의 동력이 차단된다

전달 경로와 안전관련 부품



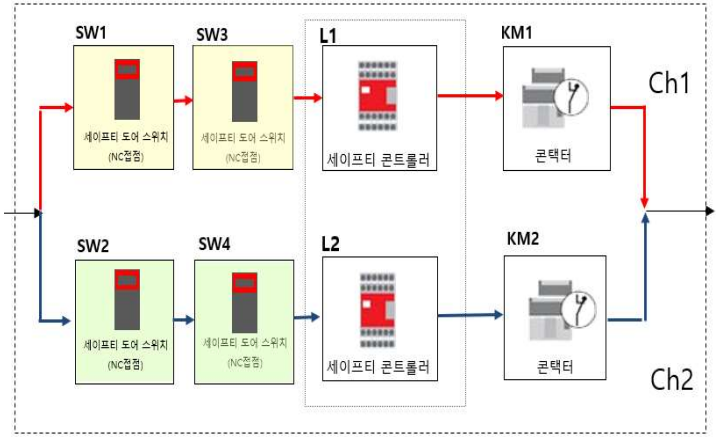
블록 다이어그램화와 카테고리



안전 시스템 관련부 구조 = Category 3

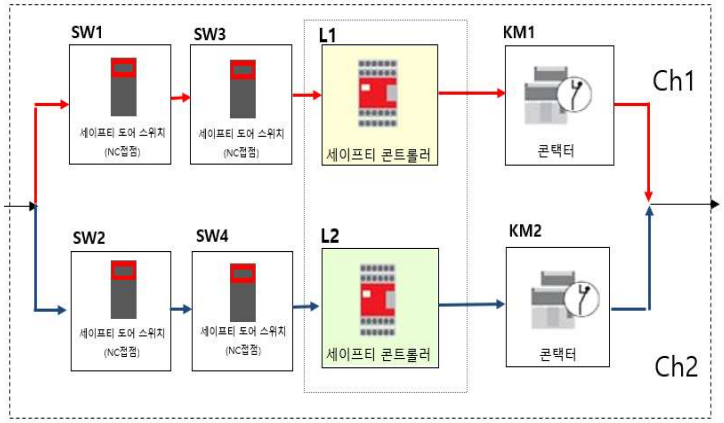
블록 다이어그램화와 MTTFd

➢ Input (입력)



변수	값
Nop (사용자 제공 수치)	20,000회/년
B10d (제조사 제공 수치)	2,000,000
MTTFd(SW1, SW3)	1,000년 (식1 참조)
MTTFd(SW2, SW4)	1,000년 (식1 참조)

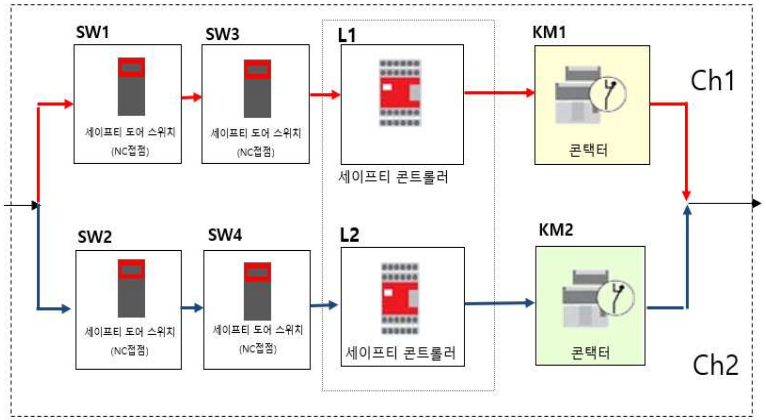
➢ Logic (제어)



변수	값
Nop (사용자 제공 수치)	-
B10d (제조사 제공 수치)	-
MTTFd(sw1)	100년
MTTFd(sw2)	100년

블록 다이어그램화와 MTTFd

➢ Output (출력)



변수	값
Nop (사용자 제공 수치)	20,000회/년
B10d (제조사 제공 수치)	400,000
MTTFd(sw1)	200년 (식1 참조)
MTTFd(sw2)	200년 (식1 참조)

➢ MTTFd 산출 (식3 참조)

채널 1: $MTTFdc1 = \frac{1}{\frac{1}{MTTFdSW1} + \frac{1}{MTTFdSW3} + \frac{1}{MTTFdL1} + \frac{1}{MTTFdKM1}}$

$= \frac{1}{\frac{1}{1{,}000} + \frac{1}{1{,}000} + \frac{1}{100} + \frac{1}{200}}$

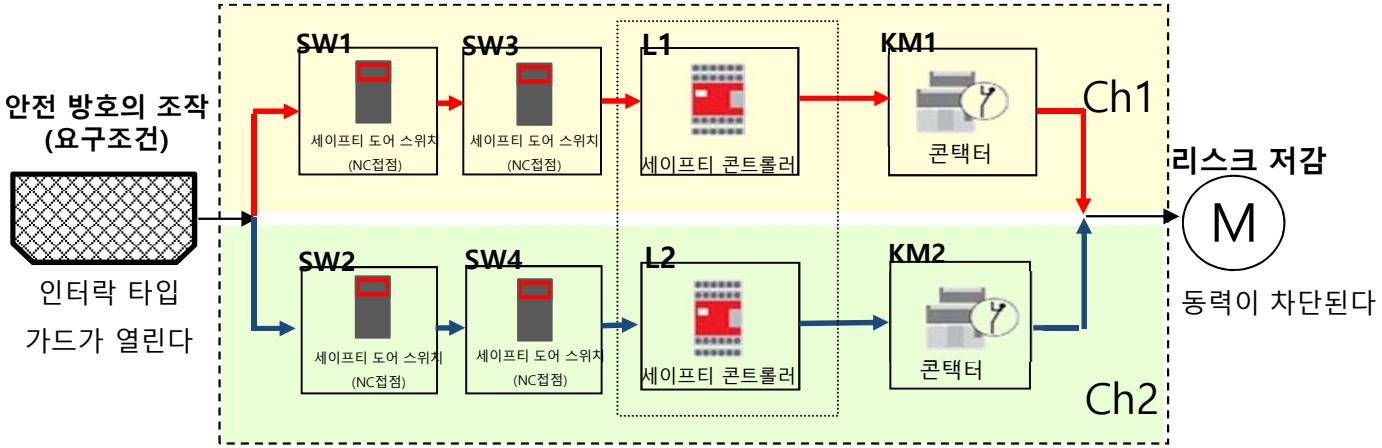
$= 58.82year$

채널 2: $MTTFdc2 = \frac{1}{\frac{1}{MTTFdSW2} + \frac{1}{MTTFdSW4} + \frac{1}{MTTFdL2} + \frac{1}{MTTFdKM2}}$

$= \frac{1}{\frac{1}{1{,}000} + \frac{1}{1{,}000} + \frac{1}{100} + \frac{1}{200}}$

$= 58.82year$

블록 다이어그램화와 DCavg



DC (입력장치)	DC (논리장치)	DC (출력장치)
타당성 확인 (신호 경로 사이 구분 없음)	셀프 체크	논리(L)내에서의 출력신호와 중간 결과의 교차감시와 합선감지
최종 DC 값 = 85%	최종 DC 값 = 99%	최종 DC 값 = 99%

채널 1: $DCavgc1 = \frac{\frac{DC_{SW1}}{MTTFdSW1}+\frac{DC_{SW}}{MTTFdSW3}+\frac{DC_{L1}}{MTTFdL1}+\frac{DC_{KM1}}{MTTFdKM1}}{\frac{1}{MTTFdSW1}+\frac{1}{MTTFdSW3}+\frac{1}{MTTFdL1}+\frac{1}{MTTFdKM1}}$

$= \frac{\frac{85}{1{,}000}+\frac{85}{1{,}000}+\frac{99}{100}+\frac{99}{200}}{\frac{1}{1{,}000}+\frac{1}{1{,}000}+\frac{1}{100}+\frac{1}{200}}$

$= 97.35\%$

채널 2 : $DCavgc1 = \frac{\frac{DC_{SW2}}{MTTFdSW2}+\frac{DC_{SW4}}{MTTFdSW4}+\frac{DC_{L2}}{MTTFdL2}+\frac{DC_{KM2}}{MTTFdKM2}}{\frac{1}{MTTFdSW2}+\frac{1}{MTTFdSW4}+\frac{1}{MTT}+\frac{1}{MTTFdKM2}}$

$= \frac{\frac{85}{1{,}000}+\frac{85}{1{,}000}+\frac{99}{100}+\frac{99}{200}}{\frac{1}{1{,}000}+\frac{1}{1{,}000}+\frac{1}{100}+\frac{1}{200}}$

$= 97.35\%$

최종 PL 평가

PL의 판정 (ISO13849-1 Annex K Table K.1 인용)

Category		B	1	2		3		4
DCavg		None		Low 60≦DCavg	Medium 90≦DCavg	Low 60≦DCavg	Medium 90≦DCavg	High 99≦DCavg
CCF		평가 대상 외		65 ≦ CCF	65 ≦ CCF	65 ≦ CCF	65 ≦ CCF	65 ≦ CCF
Low	**3≦MTTFd**	a		a	a	a	b	
	3.3≦MTTFd	a		a	a	a	b	
	3.6≦MTTFd	a		a	a	a	b	
	3.9≦MTTFd	a		a	a	b	b	
	4.3≦MTTFd	a		a	a	b	b	
	4.7≦MTTFd	a		a	a	b	b	
	5.1≦MTTFd	a		a	a	b	b	
	5.6≦MTTFd	a		a	b	b	c	
	6.2≦MTTFd	a		a	b	b	c	
	6.8≦MTTFd	a		a	b	b	c	
	7.5≦MTTFd	a		b	b	b	c	
	8.2≦MTTFd	a		b	b	b	c	
	9.1≦MTTFd	a		b	b	b	c	
Medium	**10≦MTTFd**	a		b	b	b	c	
	11≦MTTFd	a		b	b	c	c	
	12≦MTTFd	b		b	b	c	c	
	13≦MTTFd	b		b	b	c	d	
	15≦MTTFd	b		b	b	c	d	
	16≦MTTFd	b		b	c	c	d	
	18≦MTTFd	b		b	c	c	d	
	20≦MTTFd	b		b	c	c	d	
	22≦MTTFd	b		c	c	c	d	
	24≦MTTFd	b		c	c	d	d	
	27≦MTTFd	b		c	c	d	d	
High	**30≦MTTFd**		b	c	c	d	d	e
	33≦MTTFd		b	c	c	d	d	e
	36≦MTTFd		b	c	d	d	d	e
	39≦MTTFd		c	c	d	d	d	e
	43≦MTTFd		c	c	d	d	d	e
	47≦MTTFd		c	c	d	d	d	e
	51≦MTTFd		c	c	d	d	d	e
	56≦MTTFd		c	c	d	d	d	e
	62≦MTTFd		c	d	d	d	e	e
	68≦MTTFd		c	d	d	d	e	e
	75≦MTTFd		c	d	d	d	e	e
	82≦MTTFd		c	d	d	d	e	e
	91≦MTTFd		c	d	d	d	e	e
	100≦MTTFd		c	d	d	d	e	e

Category 3

+

56≦ MTTFd < 62

+

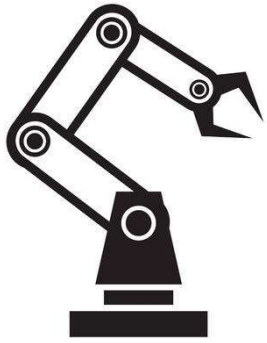
DCavg - Mid

+

CCF (65점 이상)

"PLd"

안전 회로의 구성에 따라 PL값이 바뀔 수 있다.



감사합니다.

Robot System Safety