KOSHA GUIDE
M-192-2017

기계안전을 위한 제어시스템의 안전관련부품류 설계 기술지침

2017. 11.

한국산업안전보건공단

안전보건기술지침의 개요

◦ 작성자 : 한국산업안전보건공단 이 진 우

◦ 제·개정경과

- 2017년 11월 기계안전분야 제정위원회 심의

◦ 관련규격 및 자료

- KS B ISO 12100, 기계안전 - 설계 일반원칙 - 위험성평가와 위험성감소
- KS B ISO 13849-1, 기계안전 - 제어시스템의 안전관련 부품 - 제1부: 설계 일반원칙
- KS B ISO 13849-2, 기계안전 - 제어시스템의 안전관련 부품 - 제2부: 검증
- KS C IEC 60204-1, 기계류의 안전성 - 기계의 전기장비 - 제1부: 일반 요구사항
- KS C IEC 61508-1, 전기/전자프로그램 가능한 전자장치 안전관련 시스템의 기능안전성 - 제1부: 일반 요구사항
- KS C IEC 61508-3, 전기/전자프로그램 가능한 전자장치 안전관련 시스템의 기능안전성 - 제3부: 소프트웨어 요구사항
- KS C IEC 61508-4, 전기/전자프로그램 가능한 전자장치 안전관련 시스템의 기능안전상 - 제4부: 정의 및 약어
- KS C IEC 62061, 기계안전-전기/전자프로그램 가능한 전자장치 안전관련 시스템의 기능안전성

◦ 관련 법규·규칙·고시 등

- 산업안전보건 기준에 관한 규칙 제2편 안전기준 제1장(기계·기구 및 그 밖의 설비에 의한 위험예방 관련)

◦ 기술지침의 적용 및 문의

이 기술지침에 대한 의견 또는 문의는 한국산업안전보건공단 홈 페이지 안전보건기술지침 소관 분야별 문의처 안내를 참고하시기 바랍니다.

공표일자 : 2017년 11월 27일
제 정 자 : 한국산업안전보건공단 이사장

KOSHA GUIDE
M-191-2017

기계안전을 위한 제어시스템의 안전관련부품류 설계 기술지침

1. 목 적

이 지침은 사업장에서 사용되는 각종 기계·기구 및 설비에 설치되는 제어시스템의 안전관련부품류의 설계를 위한 성능수준(PL) 결정에 필요한 사항을 정함을 목적으로 한다.

2. 적용범위

이 지침은 소프트웨어의 설계를 포함한 제어시스템의 안전관련 부품류의 설계 및 통합원칙에 대한 안전요건과 지침을 제공하고, 제어시스템의 안전관련 부품(SRP/CS)이 안전기능을 수행하는데 필요한 성능수준을 포함한 특성을 명시한다. 또한 이 지침은 전기, 유압, 공압, 기계 등 사용되는 에너지 형태에 관계없이 모든 종류의 기계류를 위한 제어시스템의 안전관련 부품에 적용된다.

3. 용어의 정의

(1) 이 지침에서 사용하는 용어의 뜻은 다음과 같다.

(가) “제어시스템의 안전관련부품(SRP/CS: Safety-Related Part of a Control System)"이라 함은 안전관련 입력신호에 응답하고 안전관련 출력신호를 발생시키는 제어시스템의 부품류를 말한다.

(나) “범주(Category)"이라 함은 결함에 대한 내성 및, 부품의 구조적 배치, 결함의 감지 및 또는 감지 신뢰성에 의해 달성되는 결함 상태에서의 후속조치 관점에서의 제어시스템 안전관련 부품들의 분류를 말한다.

(다) “결함(Fault)"이라 함은 예방정비작업 중이나 기타 계획된 활동 또는 외적 자원의 부족에 기인한 경우를 제외하고, 주어진 기능을 수행할 능력이 상실된 품목의 상태를 말한다.

(라) “고장(Failure)"이라 함은 품목에 있어 요구되는 기능을 수행할 수 있는 능력이 중단된 것을 말한다.

(마) “위험한 고장(Dangerous Failure)"이라 함은 SRP/CS를 위험한 상태나 기능장애 상태로 만들 수 있는 가능성이 있는 고장을 말한다.

(바) “공통원인고장(Common Cause Failure)"이라 함은 단일사건으로부터 유발된 다른 품목들의 고장으로 이 고장은 품목간 상호작용의 결과가 아니다.

(사) “계통적 고장(Systematic Failure)"이라 함은 특정한 원인에 대해 확정적으로 관계된 고장으로, 설계나 제조공정, 작업절차, 문서화 또는 다른 관련 요소의 수정에 의해서만 제거 가능한 고장을 말한다.

(아) “기능정지(Muting)"이라 함은 SRP/CS에 의한 안전기능이 일시적으로 자동정지하는 것을 말한다.

(자) “수동 리셋(Manual Reset)"이라 함은 한 개 또는 그 이상의 안전기능을 기계를 재시작하기 전에 수동으로 회복시키는 SRP/CS에 내재된 기능을 말한다.

(차) “상해(Harm)"이라 함은 신체적 부상이나 건강상의 손실을 말한다.

(카) “위험요인(Hazard)"이라 함은 잠재적인 상해의 근원을 말한다.

(타) “위험한 상황(Hazardous Situation)"이라 함은 사람이 한 가지 이상의 위험요인에 노출되어 즉시 또는 장기간에 걸친 상해를 야기할 수 있는 가능성이 있는 상황을 말한다.

(파) “위험성(Risk)"이라 함은 상해 발생확률과 상해 심각성의 조합을 말한다.

(하) “잔존위험성(Residual Risk)"이라 함은 보호조치 시행 이후에도 남아있는 위험성을 말한다.

(거) “위험성평가(Risk Assessment)"이라 함은 위험성분석과 위험성추정 결정/결과평가로 구성되는 전체 과정을 말한다.

(너) “위험성분석(Risk Analysis)"이라 함은 기계의 한계 명시, 위험요인 파악식별 및 위험성추정의 조합을 말한다.

(더) “위험성 결정/결과평가(Risk Evaluation)"이라 함은 위험성분석을 토대로 위험성감소 목표의 달성 여부를 판단하는 것을 말한다.

(러) “기계의 의도된 사용(Intended Use of a Machine)"이라 함은 사용설명서에 명시된 사용정보에 따라 기계를 사용하는 것을 말한다.

(머) “합리적으로 예측 가능한 오용(Reasonably Foreseeable Misuse)"이라 함은 설계자가 의도하지 않은 방식으로 기계를 사용하지만, 쉽게 예측할 수 있는 인간행동에 기인한 오용을 말한다.

(버) “안전기능(Safety Function)"이라 함은 고장이 나면 위험성이 바로 증가할 수 있는 기계의 기능을 말한다.

(서) “감시(Monitoring)"이라 함은 구성품이나 요소의 기능수행능력이 감소할 경우 또는 위험성감소의 양이 줄어들도록 공정조건이 변화하는 경우 보호조치가 개시되는 것을 보장하는 안전기능을 말한다.

(어) “프로그램 가능한 전자시스템(PES: Programmable Electronic System)"이라 함은 하나 이상의 프로그램 가능한 전자 장치를 구동하기 위하여 적용되는 제어, 보호 또는 감시를 위한 시스템으로서, 전원공급 장치, 센서, 그 외의 입력장치, 전원보호장치 및 그 외의 출력장치가 포함된 것을 말한다.

(저) “성능수준(PL: Performance Level)”이라 함은 예측 가능한 상태에서 안전기능을 수행할 수 있는 제어시스템의 안전관련 부품류의 능력을 규정하는 불연속적인 수준을 말한다.

(처) “성능요구수준(PLr: Required Performance Level)"이라 함은 각 안전기능에 대한 위험성감소를 달성하기 위해 요구되는 성능수준(PL)을 말한다.

(커) “평균위험고장시간($MTTF_d$: Mean Time to Dangerous Failure)"이라 함은 위험한 평균 고장시간의 기대값을 말한다.

(터) “단위시간당 위험한 고장확율(PFHd: Probability of Dangerous Failure Hour)"이라 함은 시간당 발생하는 위험한 고장의 평균 확률을 말한다.

(퍼) “진단범위(DC: Diagnostic Coverage)"이라 함은 감지된 위험한 고장의 고장률과 모든 위험한 고장의 고장률의 비율로 결정되는 진단 유효성의 척도를 말한다.

(허) “보호조치(Protective Measure)"이라 함은 위험성감소 달성을 목적으로 시행하는 조치를 말한다.

(고) “임무시간(T_M: Mission Time)"이라 함은 SRP/CS의 의도된 사용시간 동안의 기간을 말한다.

(노) “시험빈도(r_t: Test Rate)"이라 함은 SRP/CS의 결함을 감지하기 위해 자동으로 수행하는 시험의 주기로 진단시험 간격의 역수값을 말한다.

(도) “요구빈도(r_d: Demand Rate)"이라 함은 SRP/CS의 안전관련 조치에 대한 요구의 빈도를 말한다.

(로) “수리율(r_r: Repair Rate)"이라 함은 온라인 시험이나 시스템의 명백한 오작동에 의한 위험한 고장의 감지와 수리 후 동작의 재개나 시스템/요소 교환 후 동작의 재개 간 시간주기의 역수값을 말한다.

(모) “기계제어시스템(Machine Control System)"이라 함은 기계요소, 작업자, 외부 제어장치 또는 이들의 조합으로부터의 입력신호에 반응하고 의도한 방식으로 기계가 동작하도록 출력신호를 생성하는 시스템을 말한다.

(보) “안전무결성수준(SIL: Safety Integrity Level)"이라 함은 E/E/PE 안전관련 시스템의 안전기능의 안전무결성 요구사항을 규정하기 위한 불연속적 수준(가능한 4개 중 1개)으로 안전무결성수준 4가 가장 높은 안전무결성수준을 가지며, 1이 가장 낮은 것을 말한다.

(소) “제한된 변화언어(LVL: Limited Variability Language)"이라 함은 안전요구사항 시방을 구현하기 위해 수용가능한 사전 정의된 언어와 특정 응용프로그램용 라이브러리 함수를 제공하는 언어의 형태를 말한다.

(오) “전체 변화언어(FVL: Full Variability Language)"이라 함은 광범위한 함수와 어플리케이션을 구현할 수 있는 능력을 제공하는 언어의 형태를 말한다.

(조) “응용 소프트웨어(Application Software)"이라 함은 응용 목적에 특정한 소프트웨어로, 기계 제작자에 의해 구현되고, 일반적으로 로직 시퀀스, 적절한 입출력, SRP/CS의 요구사항을 만족시키기 위해 필요한 계산과 결정을 제한하고 제어하는 표현들을 포함하고 있는 것을 말한다.

(초) “임베 디드 소프트웨어(Embedded Software), 펌웨어(Firmware), 시스템 소프트웨어(System Software)"이라 함은 제어제작사에 의해 공급되는 시스템의 일부분인 소프트웨어로, 기계류의 사용자는 수정을 위한 접근이 불가능한 것을 말한다

(2) 그 밖에 이 지침에서 사용하는 용어의 정의는 이 지침에 특별한 규정이 있는 경우를 제외하고는 산업안전보건법, 같은 법 시행령, 같은 법 시행규칙, 안전보건규칙 및 고용노동부 고시에서 정하는 바에 의한다.

4. 설계 고려사항

4.1 위험성 감소 전략

(1) 일반사항

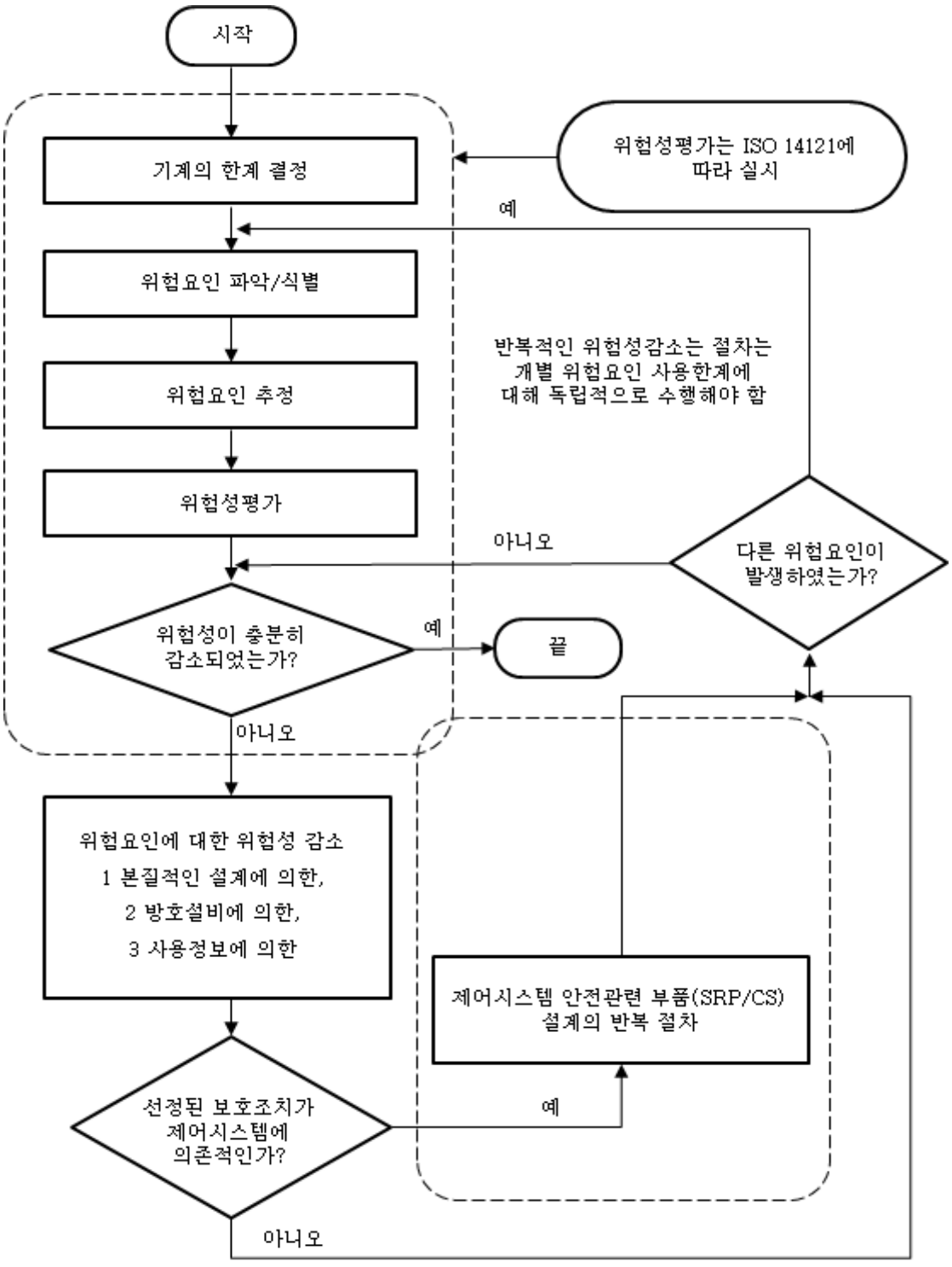
(가) 기계에 대한 위험요인분석과 위험성감소 절차는 아래와 같이 단계적 조치를 통한 위험요인의 제거 또는 감소를 요구한다.

① 설계에 의한 위험요인제거 또는 위험성감소

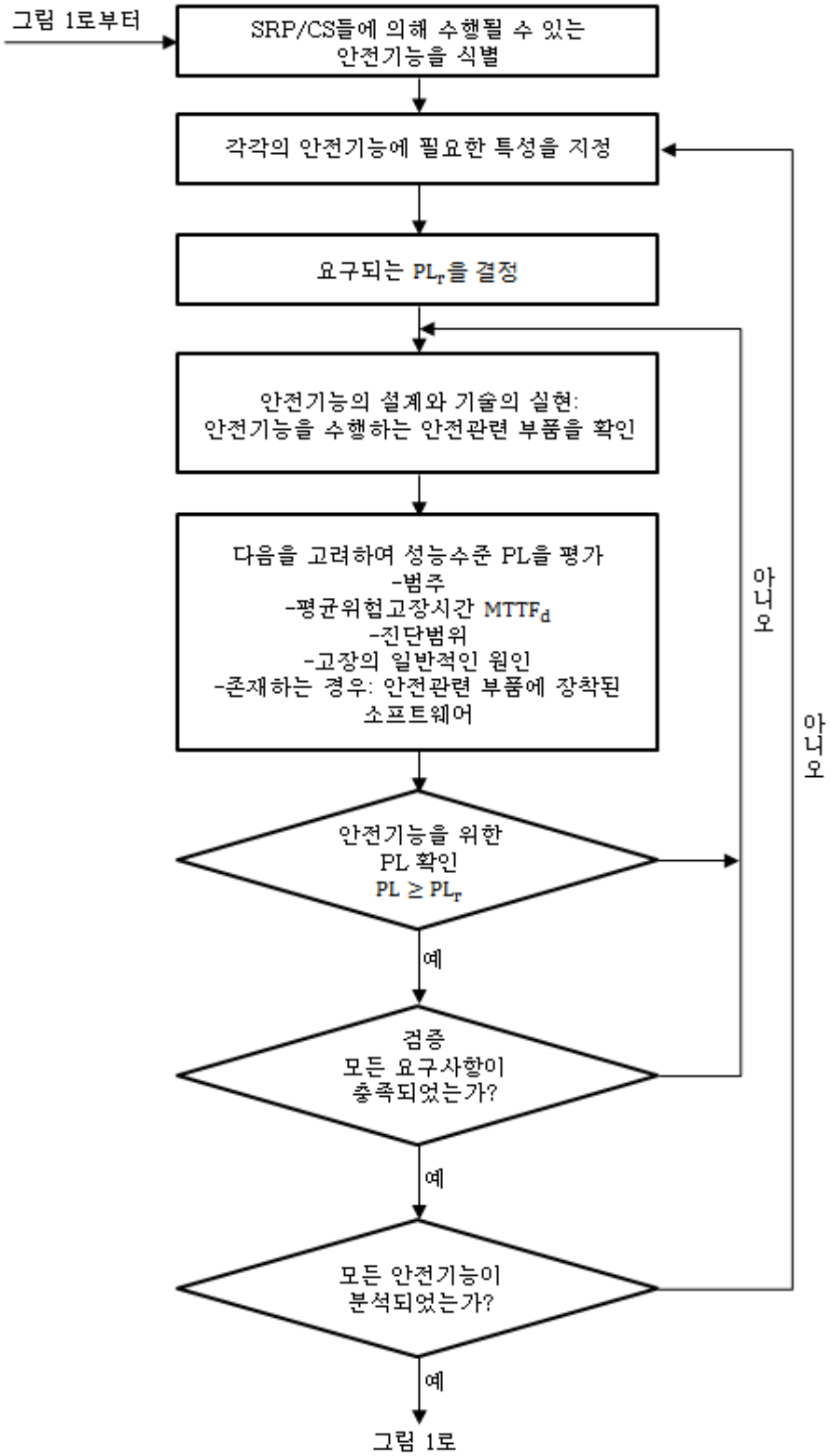
② 방호조치 및 보조보호조치에 의한 위험성감소

③ 잔존위험성에 대한 사용정보의 제공에 의한 위험성감소

(2) 제어시스템을 이용한 위험성 감소 전략



〈그림 1-1〉 위험성평가/위험성감소의 개요



〈그림 1-2〉 제어시스템의 안전관련 부품(SRP/CS)의 반복적인 설계절차

(가) 기계설비 제어시스템의 안전관련 구성품들에 의하여 수행될 수 있는 안전기능-을 목록화하고 각각의 안전기능에 필요한 특성을 지정한 후 <그림 1-2>과 같은 반복적인 설계절차를 수행한다.

(나) 각각의 안전기능에 대한 특성과 성능요구수준이 명시되어야 하고 안전요건 시방이 작성되어야 한다.

(다) 다섯 단계의 성능수준은 시간당 위험한 고장이 발생하는 확률의 범위로 규정되어 있다.

<표 1> 성능수준(PL)

PL	시간 당 위험한 고장의 평균확률 1/h
a	$\geq 10^{-5} \backsim < 10^{-4}$
b	$\geq 3 \times 10^{-6} \backsim < 10^{-5}$
c	$\geq 10^{-6} \backsim < 3\times10^{-6}$
d	$\geq 10^{-7} \backsim < 10^{-6}$
e	$\geq 10^{-8} \sim < 10^{-7}$

(3) 위험성 감소 조치

(가) 성능수준(PL) 결정평가 결과 성능요구수준(PLr)을 충족시키지 못할 경우 위험성을 감소하기 위한 보호조치는 주로 다음과 같이 적용한다.

① 안전기능에 영향을 미치는 고장이나 결함의 가능성을 줄이는 것이므로 구성요소의 신뢰성을 높인다.

② SRP/CS의 구조를 개선하여 결함의 위험한 영향을 회피하는 것이므로 어떤 결함은 감지될 수 있도록 중복 또는 감시되는 구조를 적용한다.

③ 두 방법은 개별적으로 또는 조합하여 적용할 수 있다.

4.2 성능요구수준(PLr) 결정

4.2.1 일반사항

(1) 제어시스템의 안전관련 구성품(SRP/CS)에 의해 수행되는 안전기능에 대해 성능

요구수준(PLr)을 결정하는 것이며, 이러한 성능요구수준의 결정은 위험성평가의 결과이다.

(2) 성능요구수준(PLr)은 제어시스템의 안전관련 구성품에 의해 수행되어야 할 위험성감소의 크기를 나타내는 것이며, 제어시스템의 안전관련 구성품에 의해 제공되는 위험성감소의 크기가 클수록 PLr 값이 높게 된다.

4.2.2 성능요구수준(PLr) 결정방법

(1) 성능요구수준은 제어시스템(예를 들면, 기계적 보호장치) 또는 추가적인 안전기능들과 무관한 다른 기술적 방법에 의하여 위험성감소가 기대되는 안전기능에 의하여 결정한다.

(2) 상해의 심각도 S1, S2

(가) 안전기능의 고장으로부터 발생하는 위험성의 추정에서는 오직 경미한 부상들(보통 원상회복이 가능한)과 심각한 부상들(보통 원상회복이 불가능한) 그리고 사망만을 고려한다

(나) 합병증이 없는 타박상 또는 열상은 S1 으로 분류하고 절단 또는 사망은 S2로 설정한다.

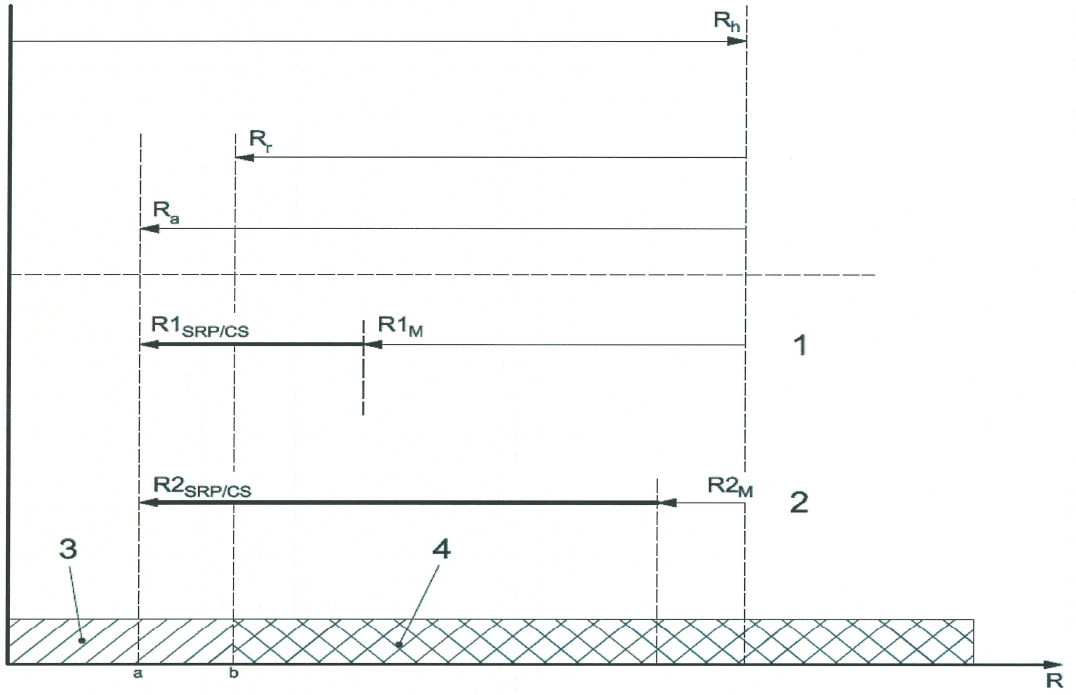
(3) 위험요인에 대한 빈도, 노출시간 F1, F2

(가) 파라미터 F1 또는 F2에 대해 선택되는 일반적인 유효시간주기는 명시하기 어려우나 사람이 자주 또는 지속적으로 위험요인에 노출된다면 F2로 선택한다.

(나) 빈도 파라미터는 위험요인에 대한 접근 빈도와 기간에 따라서 선택한다.

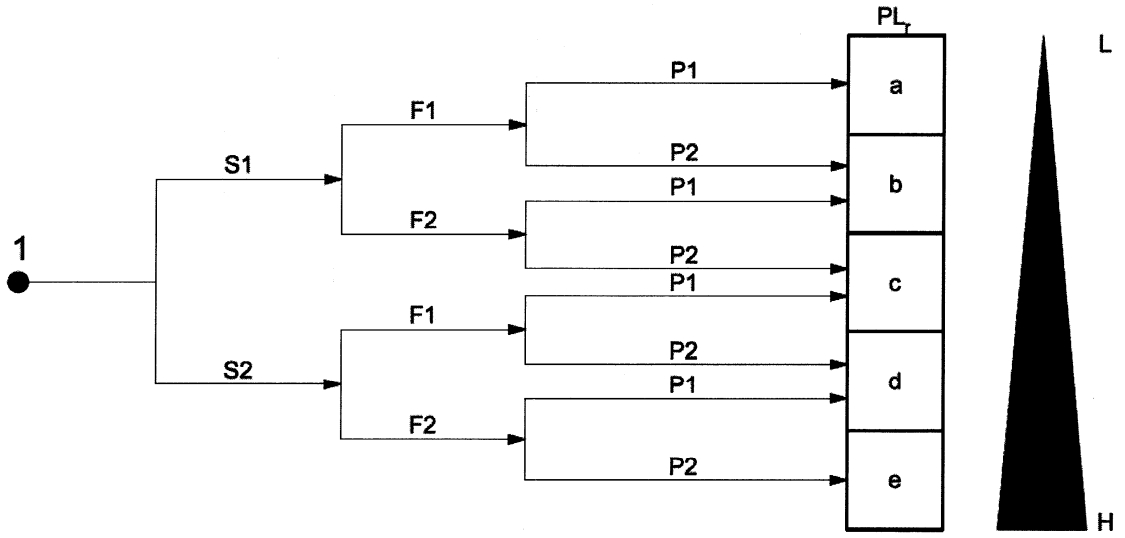
(다) 위험요인에 대한 노출기간은 장비가 사용되는 총 기간에 대하여 측정한 평균을 기준으로 결정하고 결과를 평가하는 것이 바람직하다. 예를 들면 작업물을 공급하고 이동시키기 위한 주기적 작업의 사이사이에 기계와 기구들 사이에

정기적으로 접근하는 것이 필요하다면 F2가 선택되는 것이 좋고, 간헐적인 접근만이 요구된다면 F1 이 바람직하다.



R_h	특정한 위험한 상황에 대한, 보호조치가 적용되기 전의 위험성
R_r	보호조치로부터 요구되는 위험성감소
R_a	보호조치에 의해 달성된 실제 위험성감소
1	해결책 1 - SRP/CS 외의 보호조치(예를 들면, 기계적 수단)에 소의 중요한 부분, SRP/CS에 의해 위험성 이 감소된 작은 부분
2	해결책 2 - SRP/CS에 의해 위험성이 감소된 주요한 부분(예를 기), SRP/CS 외의 보호조치(예를 들면, 기계적 수단)에 의해 작은 부분
3	충분히 감소된 위험성
4	불충분한 위험성감소
R	위험성
a	해결책 1,2에 대한 잔존위험성
b	충분히 감소된 위험성
$R1_{SRP/CS}$ $R2_{SRP/CS}$	SRP/CS에 의해 수행된 안전기능으로 인한 위험성감소
$R1_M$, $R2_M$	SRP/CS 이외의 보호조치로부터의 위험성감소 (예. 기계적 수단
비고	위험성감소에 대한 추가정보는 KSB ISO 12100 참조

〈그림 2〉 위험한 상황에 대한 위험성감소 절차의 개요



위험성 파라미터:

식별부호			
1	안전기능 결정/결과평가의 시작 점	S	부상의 심각도
L	위험성감소에 대한 기여도 낮은	S1	경미(보통 원상회복이 가능한 부상)
H	위험성감소에 대한 기여도 높은	S2	심각(보통 원상회복이 불가능한 부상는 사망)
PLr	성능요구수준	F	빈도 및또는 위험요인에 대한 노출
		F1	가끔-빈번하지는 않은 및/또는 짧은 출시간
		F2	자주지속적 및또는 긴 노출시간
		P	위험요인 회피 또는 상해 제한의 가능
		P1	특정 조건에서 가능
		P2	거의 불가능

<그림 3> 안전기능에 요구되는 PLr 결정을 위한 위험성 그래프

(2) 위험요인 P1과 P2를 회피할 수 있는 가능성

(가) 위험한 상황이 사고로 이어지기 전에 인지하고 회피할 수 있는지를 아는 것은 중요하므로 위험요인이 물체의 물리적 특성에 의해 직접 파악이나 식별되는지 또는 지시기와 같은 기술적 수단에 의해서만 인지되는지의 여부를 고려한다.

(나) 파라미터 P의 선택에 영향을 미치는 다른 중요한 측면은 감독 없는 경우나 감독이 있는 경우의 작동 여부, 전문가 또는 비전문가에 의한 작동여부, 위험요인이 발생하는 속도(예를 들면 빠르거나 느리게), 위험요인 회피의 가능성(예를 들면 탈출에 의해)여부, 공정에 관계된 실질적인 안전 경험의 보유여부 등에 따라 설정한다.

(다) 위험한 상황이 발생했을 때 사고를 회피하거나 그 영향을 현저히 저하시킬 수 있는 가능성이 있는 경우에는 P1, 위험요인을 회피할 가능성이 거의 없는 경우 P2를 선택한다.

4.3 제어시스템의 안전관련 부품(SRP/CS)의 설계

(1) 위험성감소 절차의 일부분은 기계의 안전기능을 결정하는 것이며, 이는 제어시스템의 안전기능을 포함한다.

(2) 안전기능은 하나 또는 그 이상의 SRP/CS에 의해 구현될 수 있다. 여러 안전기능은 하나 이상의 SRP/CS을 공유할 수 있다.

(3) 하나의 SRP/CS은 안전기능 및 표준제어기능을 구현하는 것도 가능하므로 설계 시 기술을 단독이나 조합으로 사용할 수 있다.

(4) 전형적인 안전기능의 도식적 표현이 제어시스템의 안전관련 부품(SRP/CS)의 조합을 나타내는 <그림 4>에 나타나 있다.

① 입력 (SRP/CS_a)

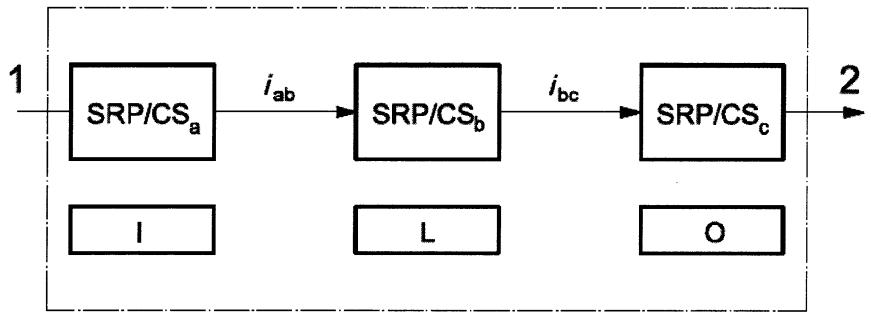
② 로직공정 (SRP/CS_b)

③ 출력전원제어부품 (SRP/CS_c)

④ 상호연결수단(i_{ab}, i_{bc})

(5) 제어시스템의 안전기능 파악식별 후, 설계자는 SRP/CS을 파악/식별해야 하고

<그림 1-2>, 필요에 따라 그것들을 입력, 로직, 출력 및 중복의 경우 개별 채널로 할당한 후 성능수준 PL을 결정하고 결과를 평가해야 한다. 단, 모든 상호연결수단은 안전관련 부품에 포함되어 있다.



I(입력), L(로직), O(출력), 1(개시 사건(예를 들면 누름 단추의 수동 누름, 가드 열기, 광전자식 방호장치의 빔), 2(기계 액추에이터(예를 들면, 모터제동기)

<그림 4> 전형적인 안전기능 수행을 위한 제어시스템의 안전관련 부품 조합의 도식적 표현

4.4 달성된 성능수준 PL의 결정 및 결과평가

4.4.1 성능수준 PL

(1) 안전기능을 수행하는 안전관련 부품의 능력은 성능수준의 결정을 통해 표현된다.

(2) 안전기능을 수행하는 선택된 개별 SRP/CS 또는 조합된 SRP/CS에 PL의 예측이 수행되어야 한다.

(3) 제어시스템의 안전관련부품(SRP/CS)의 PL은 다음과 같은 측면의 추정에 의해 결정되어야 한다.

① 단일 구성요소의 $MTTF_d$

② DC

③ CCF

④ 제어시스템 구조

⑤ 결함상태에서의 안전기능의 동작

⑥ 안전관련 소프트웨어

⑦ 계통적 고장

⑧ 예상되는 환경조건에서 안전기능을 수행하는 능력

4.4.2 각 채널의 평균위험고장시간($MTTF_d$)

(1) 각 채널의 $MTTF_d$ 값은 3개의 수준(<표 2> 참조)으로 주어지고, 단일채널, 다중 시스템의 각 채널마다 개별적으로 고려되어야 한다.

(2) $MTTF_d$ 는 100년을 최대값으로 고려한다.

<표 2> 각채널의 평균위험고장시간($MTTF_d$)

MTTFd	
각 채널의 표기	각 채널의 범위
하	3년 ≤ $MTTF_d$ < 10년
중	10년 ≤ $MTTF_d$ < 30년
상	30년 ≤ $MTTF_d$ ≤ 100년

(3) 각 채널의 3년 미만의 $MTTF_d$ 값은 시장에 나온 1년 후에 모든 시스템의 약 30%가 고장나거나 교체할 필요가 있다는 것을 의미하기 때문에 실제 SRP/CS에서 발견되지 않을 것으로 예상한 것이다.

(4) 고위험성에 대한 SRP/CS는 단일요소만의 신뢰성에 의존하지 않는 것이 좋으므로 각 채널의 100년 이상의 $MTTF_d$ 값은 허용되지 않는다.

(5) 체계상의 고장과 우발적인 고장에 대하여 SRP/CS를 강화하기 위해 중복성과 시험과 같은 추가 수단이 요구되는 것이 좋으나 실용적인 목적을 위해 범위는 3개로 제한되어 있다.

(6) 구성품의 $MTTF_d$의 예측을 위해 데이터를 찾기 위한 계층적 절차는 다음 순서와 같아야 한다.

① 제조사의 데이터 사용

② 단일구성요소의 $MTTF_d$ 값 계산 또는 결정/결과 평가[안전제어시스템 설계를 위한 평균 위험고장시간($MTTF_d$)계산 지침 참조]

③ 각각의 채널에 대한 $MTTF_d$ 추정의 간단한 방법[안전제어시스템 설계를 위한 평균 위험고장시간($MTTF_d$)계산 지침 참조]

④ 10년을 선택

4.4.3 진단범위(DC)

(1) DC는 감지된 위험한 고장율과 전체 위험한 고장의 고장율의 비율로 결정된다.

(2) 진단범위(DC)의 값은 <표 3>과 같이 4개의 수준으로 나누어진다.

<표 3> 진단범위(DC)

DC 명칭	DC 범위
해당없음	DC<60%
하	60%≤DC<90%
중	60%≤DC<99%
상	99%≤DC

(3) 진단범위(DC)의 추정을 위해, 대부분의 경우 고장모드 영향분석(FMEA) 또는 이와 유사한 방법을 사용할 수 있다. 다만 이 경우 모든 관련 결함모드나 고장모드를 고려해야하며, 안전기능을 수행하는 SRP/CS 조합의 PL이 성능요구수준(PLr)에 비추어 확인되는 것이 바람직하다.

(4) 기능과 모듈에 대한 진단범위의 간단한 추정방법은 <표 4>를 참조하여 구할 수 있다

(5) 평균 진단범위(DCavg)의 예측은 다음과 같이 할 수 있다.

① 많은 시스템에서, 결함감지에 대해 다양한 방법들이 사용될 수 있다. 즉 이러

한 방법들은 SRP/CS의 다른 부품들을 검사할 수 있고 그리고 다른 DC를 가질 수 있다는 의미이다.

② <표 2>에서 따른 PL 추정 시, 안전기능을 수행하는 전체 SRP/CS에 대해 유일하게 평균 DC만 적용할 수 있는 것이다.

③ 평균 진단범위 DC_{avg}는 다음 공식에 의하여 추정된다.

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \cdots + \frac{DC_N}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \cdots + \frac{1}{MTTF_{dN}}}$$

④ 여기서 결함 제외가 없는 SRP/CS의 모든 부품이 고려되고, 더해지는 것이 좋고 각각의 블록에 대해 $MTTF_d$ 와 DC가 고려되는 것이 바람직하다.

⑤ 이 공식에서 DC는, 부품의 모든 위험한 고장의 고장률과 부품의 감지된 위험한 고장률에 대한 비율을 의미한다.

⑥ 고장감지가 없는 부품(예를 들면 시험되지 않은)은 DC 값이 0 이고, DC_{avg}의 분모에만 기여한다.

4.4.4 PL을 예측하기 위한 단순한 절차

(1) PL은 관련된 모든 매개변수와 계산을 위한 적절한 방법을 이용하여 예측할 수 있는데 여기서는 지정아키텍처를 기반으로 SRP/CS의 PL을 예측하기 위한 단순화된 절차를 보여준다.

(2) 유사한 구조를 갖는 몇 가지 다른 아키텍처는 PL의 예측을 얻기 위해 지정아키텍처로 변환할 수 있다.

(3) 지정아키텍처는 블록다이어그램으로 표현되며 6절의 각 범주의 내용에 나열되어 있다.

<표 4> 진단범위(DC)의 추정 (2의 1)

방법	DC
입력장치	
입력신호의 동적변화에 의한 반복실험자극	90%
타당성 확인, 예를 들면 통상 NO, NC는 기계적으로 연결된 접점(contacts)의 사용	99%
동적시험 없이 입력을 교차 감시	0%∽99%, 적용에 따라 얼마나 자주 신호변화가 일어나는지에 따라 다름
합선을 감지할 수 없을 때 동적시험을 통한 입력신호의 교차감시(여러 I/O에대하여)	90%
논리(L)내에서의 입력신호와 중간결과의 교차감시, 그리고 프로그램흐름의 순간적 그리고 논리적 소프트웨어 감시 및 정적인 결함과합선의 감지여러 I/O에대하여)	99%
간접적인 감시(예를 들면 압력스위치, 액추에이터의 전기적 위치감시)	적용에 따라 90%-99%
직접적인 감시(예를 들면 제어밸브의 전기적 위치감시, 기계적으로연결된 접촉요소를 이용한 기전장치의 감시)	99%
공정에 의한 결함감지;	적용에 따라 0%∽99%까지, 이 방법하나만으로는 성능요구수준 e에 충분하지 않다!
센서의 몇몇 특성 감시(응답시간, 아날로그 신호의 범위, 예를 들면전기저항, 전기용량)	60%
논 리	
간접적인 감시(예를 들면 압력스위치를 이용한 감시, 액추에이터의전기적인 위치감시)	적용에 따라, 90%∽99%
직접적인 감시(예를 들면 제어밸브의 전기적 위치감시, 기계적으로연결된 접촉요소를 이용한 기전장치의 감시)	90%
간단한 논리의 순간적 시간 감시(예를 들면 트리거 지점이 논리 프로그램내에 있는 경우 워치독으로서의 타이머)	60%
시험장치가 논리의 동작에 대한 타당성 검증을 하는 경우, 워치독을 이용하는 논리의 시간적 그리고 논리적 감시	90%
논리의 일부분에 잠재하는 결함을 감지하기 위한 자가시험 개시 (예를 들면 프로그램과 데이터 메모리, 입력/출력포트. 인터페이스)	90%(시험 기술에 따라)
시작점 또는 안전기능이 요구될 때마다 또는 외부신호가 입력 장치를 통해 요구할 때마다 주 채널을 이용한 감시 장비의 반응 능력의검증(예를 들면 워치독)	90%
동적원리(안전기능이 요구될 때 논리의 모든 부품은 상태를 ON- OFF-ON으로 바꿔야 함, 예를 들면 릴레이에 의해 구현되는 연동회로	99%

<표 4> 진단범위(DC)의 추정 (2의 2)

방법	진단범위
불변 메모리: 한 워드 (8 bit)의 특징	90%
불변 메모리: 두 개의 워드(16 bit)의 특징	99%
가변 메모리: 중복 데이터를 이용한 RAM-시험. 예를들어, 플래그, 마커, 상수, 타이머와 이 데이터에 대한 교차비교.	60%
가변메모리 : 사용된 데이터 메모리 셀의 읽고 쓸수 있는 능력에 대한 검증	60%
가변메모리 : 수정된 Hamming 코드를 이용한 RAM 감시 또는RAM 자가 테스트 (예를 들어. “galpat"또는 “Abraham")	99%
프로세스 유닛 : 소프트웨어에 의한 자가테스트	60% ~ 90%
프로세스 유닛 : 코드화된 처리	90%~99%
프로세스에 의한 결함감지	적용에 따라 0%~99%, 이 방법 하나만으로는 성능요구수준 e에 충분하지 않다!
출력장치	
동적시험 없는 단일채널에 의한 출력감시	0%~99%, 응용에 의해 얼마나 자주 신호 변화가 일어나는지에 따라
동적시험 없는 교차감시	0%~99%, 응용에 의해 얼마나 자주 신호 변화가 일어나는지에 따라
합선을 감지 없이 동적시험에 의한 출력신호의 교차감시	90 %
논리(L)내에서의 출력신호와 중간결과의 교차감시, 그리고 프로그램흐름의 순간적 그리고 논리적 소프트웨어 감시 및 정적인 결함과합선의 감지(여러 I/O에 대하여)	99%
액추에이터 감시 없는 중복 차단경로	0%
논리 또는 시험장치에 의해 액추에이터 중 한 개를 감시하는 기능을 갖는 중복 차단경로	90%
논리 또는 시험장치에 의해 액추에이터 감시기능을 갖는 중복 차단경로	99%
간접적인 감시예를 들면 압력스위치, 액추에이터의 전기적인 위치감시)	90%~99% 적용에 따라
프로세스에 의한 결함감지	0 적용에 따라 0%~99%, 이 방법 하나만으로는 성능요구수준 e에 충분하지 않다!
직접적인 감시예를 들면 제어밸브의 전기적위치감시, 기계적으로연결된 접촉요소를 이용한 기전장치의 감시)	99%
논리에 대해 중간 혹은 높은 DC값이 요구될 때, 각 DC가 적어도 60%인 가변메모리, 비가변 메모리, 그리고 처리장치에 대해 적어도 한 개의 방법이 적용되는 것이 좋다.	

(4) 지정아키텍처는 각 범주의 시스템 구조의 논리적인 표현을 알려주는 것이다.

① 지정아키텍처는 결합된 SRP/CS에 대해 그려져 있는데, 안전관련 신호가 시작

되는 지점에서 시작하여 전원제어요소의 출력에서 마무리한다.

② 지정아키텍처는 입력신호에 대응하고 관련 출력신호를 생성하는 제어시스템의 일부나 부속요소를 설명하는데 사용할 수 있다.

③ "입력" 요소는 제어논리소자 입력회로나 입력스위치뿐만 아니라 라이터커튼(AOPD)으로도 나타낼 수 있다.

(5) 지정아키텍처에 대해서는 다음과 같은 가정을 한다.

① 임무시간, 20년

② 임무시간 내의 일정한 고장률

③ 범주 2 경우 요구빈도 ≤ 1/100 테스트 빈도

④ 범주 2 경우 시험채널의 $MTTF_d$ 가 기능채널 $MTTF_d$의 절반보다 큼

(6) 각 SRP/CS의 성능수준은 아키텍처, 각 채널의 평균위험고장시간($MTTF_d$)과 DC_{avg}에 따라 달라지며, 공통원인고장(CCF)도 고려하는 것이 좋다.

(7) 소프트웨어를 갖는 SRP/CS의 요구사항은 다음 절을 참고하고 정량적 데이터를 구할 수 없거나 사용하지 않는 경우(예를 들면, 복잡하지 않은 시스템), 모든 관련 파라미터는 최악의 경우를 선택하는 것이 좋다.

(8) <그림 5>에서 안전기능의 요구되는 PL을 달성하기 위해 범주를 각 채널의 $MTTF_d$와 Dc_{avg}를 조합하여 선택하는 절차가 나타나 있다.

① PL의 예측을 위해 <그림 5>는 DC_{avg}(가로축)와 각 채널의 $MTTF_d$(막대)를 갖는 다른 가능한 범주의 조합을 제공하고 있음

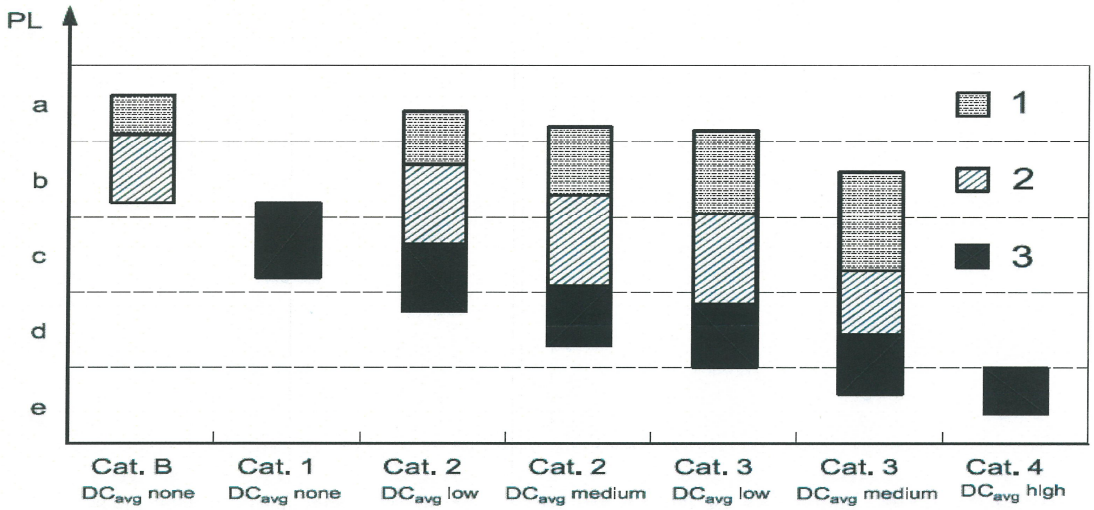
② 그림의 막대는 요구되는 PL을 달성하기 위해 선택할 수 있는 각 채널의 3개의 $MTTF_d$의 범위(낮음, 중간, 높음)를 나타낸 것임

③ <그림 5>의 단순화된 접근법을 사용하기 전에, 평균진단 범위와 각 채널의 $MTTF_d$뿐만 아니라 SRP/CS의 범주가 결정되어야 함

(9) 이 영역의 수직위치는 수직축으로부터 읽을 수 있는 달성된 PL을 결정한다.

① 구역이 2개 또는 3개의 가능한 성능수준을 포함하는 경우, 달성된 PL은 <표 5>에 기재되어 있음

② 정확한 PL 수치의 선택은 각 채널의 $MTTF_d$의 정확한 값에 따라 다름



PL 성능수준
1 각 채널의 $MTTF_d$ = 하(low)
2 각 채널의 $MTTF_d$ = 중(medium)
3 각 채널의 $MTTF_d$ = 상(high)

<그림 5> 범주, DC_{avg}, 각 채널별 $MTTF_d$과 PL사이의 관계

<표 5> SRP/CS에 의해 달성되는 PL을 평가하기 위한 단순화된 절차

범주	B	1	2	2	3	3	4
DC_{avg}	해당없음 (none)	해당없음 (none)	하	중	하	중	상
각 채널의 $MTTF_d$							
하	a	포함하지 않음	a	b	b	c	포함하지 않음
중	b	포함하지 않음	b	c	c	d	포함하지 않음
상	포함하지 않음	C	c	d	d	d	e

4.4.5 공통원인고장(CCF)에 대한 추정

(1) 공통원인고장(CCF)의 효과를 추정하기 위한 정량적인 절차는 전체시스템에 대하여 진행하는 것이 바람직하다.

(2) 제어시스템의 안전관련부품의 모든 부분이 고려되는 것이 좋다.

(3) <표 6>은 공학적인 판단에 기초하여 방법을 나열하고 관련된 값을 포함하고 있는데, 이 값들은 공통원인고장을 줄이는데 기여한 정도를 나타낸다.

(4) 각각 나열된 방법에 대하여 오직만점이나 0점만을 줄 수 있다. 만일 항목이 일부만 달성되었다면 동 항목에 대한 점수는 0점으로 처리한다.

(5) 각 항목의 값을 모두 합산한 값이 65점 이상일 경우 4.4.4절에서 예측된 성능지수 PL의 요건이 충족된 것으로 인정하지만 65점 이하일 경우 추가적인 방법을 선택하여야 한다.

<표 6> CCF에 대응하는 방법의 점수배점(CCF)

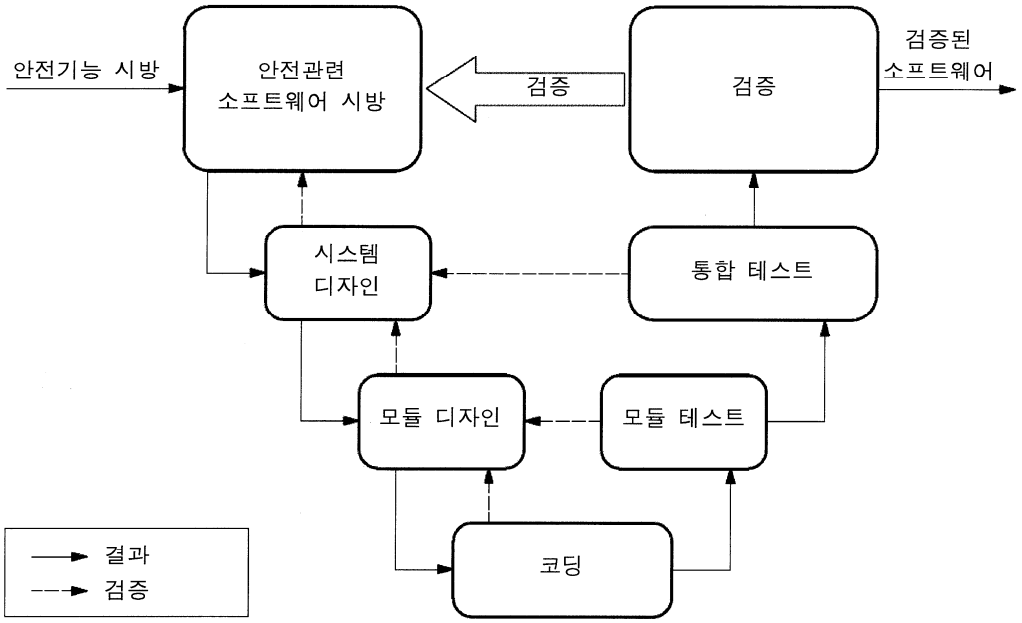
번호	CCF에 대응하는 방법	점수
1	구분격리	
	신호경로 사이의 물리적인 분리 배선/배관에서의 분리 인쇄기판상의 유격과 creep age 거리	15
2	다양성	
	다른 기술설계 또는 물리적 원리가 사용된다, - 예를 들어 프로그램 가능한 전자의 첫번째 채널 그리고 확실히 연결된 두번째 채널, 시작의 종류, 압력과 온도거리와 압력 측정, 디지털과 아날로그, 다른 제조자의 부품들	20
3	설계/응용/경험	
3.1	과전압, 과압력, 과전류에 대한 보호 등	15
3.2	사용된 부품들은 충분한 시험을 거친 것이다.	5
4	평가/분석	
	설계에서 공통원인고장을 회피하기 위해 고장모드와 효과분석의 결과를 고려하였는가 ?	5
5	`숙련도/훈련	
	설계자가 공통원인고장의 원인과 결과를 이해할 수 있도록 훈련을 받았는가?	5
6	환경	
6.1	- 적절한 표준에 따른 오염방지와 CCF에 대한 전자기 적합성(EMC) - 유체시스템: 압축 매개체의 여과, 먼지흡입 방지, 압축공기의 배출, 예를 들면 압축 매개체의 순도에 대한 부품제조사의 요구사항 준수 - 전기시스템 : 시스템이 전기자기적합성에 대하여 검사되었는가? 예를 들면, CCF 대응 표준에 명시된 대로 - 유체 및 전기 혼합 시스템의 경우 두 개의 관점을 모두 고려되는 것이 좋다.	25
6.2	다른 영향들 - 온도, 충격, 진동, 습도와 같은 모든 관련된 환경적 요인들에 대한 적합성에 대한 요구사항들을 고려하였는가	10
	총합	100

4.5소프트웨어 안전 요구사항

4.5.1 일반사항

(1) 안전관련 임베디드 또는 응용 소프트웨어의 전체수명주기 활동은 소프트웨어 수명주기 동안 유발되는 결함을 피하는 것을 일차적으로 고려해야 한다.

(2) 소프트웨어는 읽기 쉽고, 이해하기 쉽고, 테스트 가능하고, 보수 가능한 것이어야 한다.



<그림 6> 소프트웨어 안전수명주기의 단순화된 V-모델

4.5.2 안전관련 임베디드 소프트웨어(SRESW)

(1) PLr이 a∽d를 갖는 요소의 SRESW는 다음과 같은 기본적인 조치가 적용되어야 한다.

① 소프트웨어 안전수명주기의 검증 활동과 타당성 확인 활동

② 시방과 설계문서

③ 모듈, 구조설계 및 코딩

④ 계통적 고장의 제어

⑤ 무작위한 하드웨어 고장 및 올바른 구현의 검증을 위하여 소프트웨어 기반의 제어대책 사용

⑥ 기능 테스트

⑦ 수정 후 적절한 소프트웨어 안전수명주기 활동

(2) PLr이 c나 d인 SRESW는 다음의 추가조치가 적용되어야 한다.

① 소프트웨어 안전수명주기 동안 관련된 모든 활동의 문서화

② SRESW 출시 관련 모든 구성 항목 및 문서의 파악식별을 위한 구성관리

③ 안전요구사항과 설계를 포함한 구조화된 시방

④ 적절한 프로그래밍 언어 사용과 능숙한 컴퓨터 기반도구 사용

⑤ 모듈과 구조적 프로그래밍, 비 안전관련 소프트웨어의 분리, 완전하게 정의된 인터페이스와 한정된 모듈크기, 설계 및 코딩규격의 사용

⑥ 제어흐름 분석을 포함한 단계별 수행검토에 의한 코딩검증

⑦ 확장된 기능테스트(예를 들면 성능테스트 및 시물레이션)

⑧ 수정 후 충격분석과 적절한 소프트웨어 안전수명주기 활동

(3) PLr = e인 경우의 SRESW는 SIL 3에 적합한 기준을 준수해야 한다.

다만 시방 범주 3 또는 4를 갖는 SRP/CS의 두 채널에 대해 설계, 코딩의 다양성을 이용하는 경우, PLr=e는 위에서 언급한 c나 d의 PLr에 대한 조치로 달성 가능하다.

4.5.3 안전관련 응용 소프트웨어(SRASW)

(1) 소프트웨어 안전수명주기는 SRASW에도 적용된다.(<그림 6> 참조)

(2) PLr이 a~e를 가지는 SRASW의 구성요소는 다음의 기본적인 조치가 적용되어야 한다.

① 검증 활동과 확인 활동을 포함한 수명주기의 개발은 <그림 6>을 참조

② 시방과 설계의 문서화

③ 모듈과 구조적 프로그래밍

④ 기능 테스트

⑤ 수정 후 적절한 개발 활동

(3) PLr이 c~e를 가지는 구성요소의 SRASW는 다음의 효율 증대를 수반한 추가적인 조치가 필요하거나 권장된다.

(가) 안전관련 소프트웨어의 시방은 반드시 검토되어야 하고, 수명주기에 관련된 모든 사람이 이용 가능해야 하며 아래 설명을 포함해야 한다.

① 요구되는 PL을 갖춘 안전기능 및 관련된 동작모드

② 성능기준, 예를 들면 반응시간

③ 외부 신호 인터페이스를 갖춘 하드웨어 아키텍처

④ 외부 고장의 감지와 제어.

(나) 도구, 라이브러리 및 언어의 선택

① 사용자가 능숙한 도구: 하나의 구성 요소와 도구를 사용하여 달성된 PL = e에 대한 도구는 적절한 안전표준을 준수해야 한다. 만약 다양한 도구를 포함한 두 다양한 구성요소가 사용되는 경우, 사용자의 숙련도만으로도 충분하다.

② 시스템 오류를 유발할 수 있는 조건을 검출하는 기술적 특징(예를 들면 데이터 형식 불일치, 애매한 동적 메모리 할당, 불완전한 인터페이스, 포인터 연산 등)이 사용되어야 한다.

③ 검사는 실행 중일 때 뿐만 아니라 주로 컴파일하는 동안 실시하는 것이 보다 효과적이다.

④ 도구는 언어의 부분집합 및 코딩 지침을 적용하도록 감독하고 개발자들이 사용하도록 유도한다.

⑤ 합리적이고 실행 가능한 경우, 검증된 기능블록(FB) 라이브러리를 사용하는 것이 좋다: 도구 제조자(PL=e가 권장 됨)에 의해 제공되는 안전관련 검증된 FB 라이브러리 혹은 특화되고 이 표준에 부합하는 검증된 FB 라이브러리 중 하나를 사용한다.

⑥ 모듈 방식에 적합한 정당화된 LVL의 부분집합(일부분)을 사용하는 것이 좋다.

(다) 소프트웨어 설계는 다음 특징을 가져야 한다.

① 데이터와 제어의 흐름을 설명하기 위한 준 정형화된 방법, 예를 들면 상태 다이어그램이나 프로그램 흐름 차트

② 주로 안전관련 검증된 기능블록 라이브러리에서 파생된 기능블록에 의해 구현된 모듈화 및 구조화된 프로그래밍

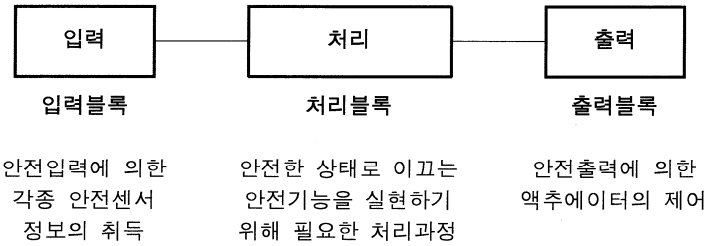
③ 제한된 크기의 코딩 기능블록

④ 하나의 입구와 하나의 출구 지점을 가져야만 하는 내부 기능블록의 코드 실행

⑤ 3단계의 아키텍처 모델: 입력 => 처리과정 => 출력

⑥ 한 프로그램 지점에서만의 안전출력의 할당

⑦ 외부고장 검출 및 안전한 상태를 도출하는 입력블록, 처리블록 및 출력블록에서의 방어프로그래밍 기술의 사용.



<그림 7> 소프트웨어의 일반 아키텍처 모델

(라) SRASW 및 non-SRASW가 하나의 구성요소에 결합되는 경우

① SRASW 및 non-SRASW는 잘 정의된 데이터 링크를 갖는 다른 기능블록으로 코딩해야 함

② 안전관련 신호의 무결성의 하향 조정으로 이어지는 비 안전관련 데이터와 안전관련 데이터의 논리적 조합이 없어야 함

(마) 소프트웨어 구현/ 코딩

① 코드는 읽기 쉽고, 이해하기 쉽고, 시험하기 쉬워야 하며 이로 인해 기호변수(명시적인 하드웨어 주소 대신)를 사용

② 정당화되거나 허용된 코딩 지침을 사용

③ 데이터 무결성 및 응용프로그램 계층(방어 프로그래밍)에 사용할 수 있는 타당성 검사(예를 들면 범위 검사)를 사용

④ 코드는 시뮬레이션에 의하여 테스트

⑤ 검증은 PL=d 또는 e에 대한 데이터 흐름 분석과 제어에 의해서 수행

(바) 테스트

① 적절한 검증방법은 기능적인 동작 및 성능기준(예를 들면 타이밍 성능)을 입증하는 블랙박스 테스트

② PL=d 또는 e의 경우 경계값 분석에서의 시험 케이스 실행 권장

③ 시험 계획이 권장되며 완료 기준과 요구되는 도구들을 갖춘 시험 사례들을 포함

④ 입출력 시험은 안전관련 신호가 SRASW 내에서 올바르게 사용되고 있는지 확인

(사) 문서화

① 모든 수명주기 및 수정 활동은 문서화

② 문서는 완전해야 하고 사용 가능하여야 하며 읽기 쉽고 이해 가능

③ 원본 텍스트 내의 코드 문서는 법인명, 기능, 입출력 설명, 버전, 사용되는 라이브러리 기능블록의 버전, 네트워크명령 그리고 선언 행에 대한 충분한 설명을 수반한 모듈 헤더를 포함

(아) 검증[1]: 검토, 조사, 단계별 수행 또는 다른 적절한 활동

(자) 수정

① SRASW의 수정 후 영향 분석은 시방을 보장하기 위해 수행해야 함.

② 적절한 수명주기 활동을 수정 후에 수행해야 함.

③ 변경에 대한 접근 권한은 관리되어야 하고 변경 내역은 문서화해야 함

4.5.4 소프트웨어 기반 파라미터화

(1) 안전관련 파라미터들의 소프트웨어 기반 파라미터화는 소프트웨어 안전요구 시방서에 설명될 SRP/CS 설계의 안전관련 측면으로 고려되어야 한다.

(2) 파타미터화는 SRP/CS 공급자에 의해 제공된 전용 소프트웨어 도구를 이용하여 수행되어야 한다.

1) 검증은 특정 응용 코드에 대해서만 필요할 뿐 인증된 라이브러리함수에 대해서는 필요하지 않다

(3) 이 도구는 고유식별(이름, 버전, 등등)을 가지고, 승인되지 않은 수정을 방지할 수 있어야 한다.(예를들면 비밀번호의 사용)

(4) 파라미터화에 이용된 모든 데이터의 무결성은 유지되어야 하고, 이는 다음의 적용된 조치들에 의해서 이루어져야 한다.

① 유효한 입력 범위의 제어

② 전송 이전의 데이터 변조 제어

③ 파라미터 전송과정으로부터의 오류효과의 제어

④ 불완전한 파라미터 전송의 효과를 제어

⑤ 파라미터화를 위해 사용된 하드웨어와 소프트웨어의 결함과 고장 효과의 제어

(5) 파라미터화 도구는 SRP/CS에 대한 다양한 모든 요구사항을 만족하여야 하나, 어려울 경우에는 별도의 안전관련 파라미터 설정을 위해서 특별한 절차가 사용되어야 한다. 이 절차는 다음 두 절차 중 하나에 의해서 SRP/CS 입력 파라미터를 확인하는 것을 포함한다.

① 파라미터화 도구로 수정된 파라미터의 재전송

② 차후 확인뿐만 아니라, 파라미터의 무결성을 확인하는 다른 적절한 방법(예를 들면, 적절하게 숙련된 사람과 파라미터화 도구에 의한 자동점검을 사용하는 것)

(6) 전송/재전송 과정에서의 엔코딩/디코딩을 위해 사용된 소프트웨어 모듈들과, 사용자에 대한 안전관련 파라미터들의 시각화를 위해 사용된 소프트웨어 모듈들은 계통적 고장을 피하기 위해서 기능의 다양성을 최소화 하여 사용해야 한다.

(7) 다음 내용은 소프트웨어 기반 파라메터화에 적용되어야 한다.

① 안전관련 파라미터(최소, 최대 그리고 대표적인 값들) 각각의 정확한 설정의 확인

② 안전관련 파라미터의 타당성 점검의 확인, 예를 들어, 무효한 수치의 사용 등

③ 안전관련 파라미터들의 승인되지 않은 수정의 방지를 확인

④ 파라미터화를 위한 데이터신호들이 결함이 안전기능의 상실로 이어질 수 없는 방식으로 생성되고 처리되는지를 확인

5 안전기능

5.1 안전기능 시방

(1) 설계자는 SRP/CS에 의해서 제공될 수 있는 안전기능의 목록과 세부사항들을 제시하고, 제어시스템에 요구되는 안전조치를 달성하기 위해 필요한 것들을 포함해야 한다. 예를들면 안전관련 정지기능, 예상치 못한 시동의 방지, 수동 리셋 기능, 기능정지 기능, 실행유지 기능 등이 있다.

(2) <표 7>은 각각 몇몇 전형적인 안전기능, 특징들의 일부와 안전관련 파라미터들을 열거하고 있으며 동시에 안전기능, 특징 또는 파라미터에 관련된 요구사항을 가지는 다른 국제표준을 인용한 것이다. 설계자는 모든 해당되는 요구사항들이 표에 열거된 관련된 안전기능들을 만족하는 것을 확인해야 한다.

(3) <표 7>의 인용표준들 대부분이 전기표준과 관계되므로 해당되는 요구사항들은 다른 기술(예, 유압, 공압)의 경우에는 변형을 하여 사용한다.

(4) 안전기능을 확인하거나 명시할 때, 최소한 다음의 것들이 고려되어야 한다.

① 각각의 특정한 위험요인 또는 위험한 상황에 대한 위험성평가 결과

② 다음의 것들을 포함한 기계작동 특징들,

- 기계의 의도된 용도(합리적으로 예측가능한 오용을 포함)
- 작동모드(예를 들면 지역모드, 자동모드, 기계의 구역 또는 부품에 관련된 모드들)
- 사이클 시간
- 반응시간

③ 비상조치

④ 다른 작업절차와 수동 활동(수리, 설정, 청소, 고장수리, 등등.) 사이의 상호작용에 대한 설명

⑤ 안전기능이 달성하거나 방지하도록 의도된 기계의 거동
⑥ 기계의 활성화 또는 비활성를 결정짓는 기계의 상태(예를 들면, 작동모드)
⑦ 작동 빈도
⑧ 동시에 활성화될 수 있고 모순되는 행동을 유발할 수 있는 기능들의 우선순위

5.2 안전기능의 주요 세부사항

5.2.1 안전관련 정지기능(연동장치와 제한장치 포함)

(1) 위험한 상황을 초래할 수 있는 기계의 움직임은 감시되어야 하나 수동제어기계에서는 운전자가 감시기능을 할 수 있어야 한다. 다만 운전자가 감시할 수 없는 불가피한 경우에는 과속감지장치, 기계식 과부하 방지장치, 충돌방지장치 등을 포함한 별도의 방법이 강구되어야 한다.

(2) 보호장치에 의해서 시작되는 안전관련 정지 기능(연동장치와 제한장치 즉 과속, 과열, 과압 등을 포함)을 적용해야 하며 필요시 보호장치 및 연동장치에 연결되어야 한다.

(3) 안전관련 정지기능은 필요하다면 작동 즉시 기계가 안전한 상태가 되게 해야 한다. 이러한 정지는 작업상 이유에 의한 정지에 대해 우선권을 가져야한다.

(4) 정지기능의 복귀 시에는 어떠한 위험상태도 유발되지 않아야 한다.

(5) 하나 이상의 조작반이 설치된 경우 모든 조작반에 정지명령이 유효하여야 한다.

(6) 비상정지는 기계에서 1차적인 위험의 축소수단이 아닌 보완적인 보호조치 이다.

<표 7> 전형적인 기계안전기능들과 그 특징들의 일부분에 적용 가능한 몇몇 표준들

안전기능/ 특징	KS B ISO 12100:2010	추가적인 정보
보호장치에 의해서 시작되는 안전관련 정지 기능 a	3.28.8, 6.2.11.3	IEC 60204-1:2005, 9.2.2, 9.2.5.3, 9.2.5.5
수동 리셋 기능	-	IEC 60204-1:2005, 9.2.5.3, 9.2.5.4
시작/재시작 기능	6.2.11.3, 6.2.11.4	IEC 60204-1:2005, 9.2.1, 9.2.5.1, 9.2.5.2, 9.2.6
부분 제어 기능	6.2.11.8, 6.2.11.10	IEC 60204-1:2005, 10.1.5
기능정지기능	-	-
실행유지 기능	6.2.11.8 b)	IEC 60204-1:2005, 9.2.6.1
가동장치 기능	-	IEC 60204-1:2005, 9.2.6.3, 10.9
예상치 못한 시작방지	6.2.11.4	KS B ISO 14118 IEC 60204-1:2005, 5.4
끼인 사람의 탈출과 구조	6.3.5.3	'
격리와 에너지 방출 기능	6.3.5.4	KS B ISO 14118 IEC 60204-1:2005, 5.3, 6.3.1
제어 모드들과 모드 선택	6.2.11.8, 6.2.11.10	IEC 60204-1:2005, 9.2.3, 9.2.4
제어시스템들의 다른 안전관련 부품들과의 상호작용	6.2.11.1 (마지막 문장)	IEC 60204-1:2005, 9.3.4
안전관련 입력 값의 감시 파라미터화	-	-
긴급 정지 기능 b	6.3.5.2	KS B ISO 13850 IEC 60204-1:2005, 9.2.5.4
반응시간	-	ISO 13855:2000, 3.2, A.3, A.4
속력, 온도 또는 압력과 같은 안전관련 파라미터	6.2.11.8 e)	IEC 60204-1:2005, 7.1, 9.3.2, 9.3.4
동력원의 변동, 손실과 회복	6.2.11.8 e)	IEC 60204-1:2005, 4.3, 7.1,7.5
알림와 경고신호	6.2.8	ISO 7731, KS A ISO 11428 KS A ISO 11429, KS C IEC 61310-1 IEC 60204-1:2005, 10.3, 10.4 IEC 61131, IEC 62061

5.2.2 수동 리셋 기능

(1) 리셋의 명령은 기계를 재시동해서는 아니 되고 단지 재시동을 허용하기만 해야 한다.

(2) 방호설비에 의해서 정지명령이 개시된 이후에, 정지상태는 재시작을 위해 안전상태가 존재할 때까지 유지되어야 한다.

(3) 방호설비의 리셋에 의한 안전기능의 복구는 정지명령을 취소시켜야 한다.

(4) 수동 리셋 기능은 다음조건을 유지해야 한다.

① SRP/CS 내에서 분리되고 수동으로 작동되는 기구를 통해서 제공되어야 함

② 모든 안전기능들과 방호설비가 작동할 때에만 가능해야 함

③ 스스로 동작 또는 위험한 상황을 시작하지 않아야 함

④ 의도적인 작동에 의해야 함

⑤ 제어시스템이 별도의 시작명령을 받아들일 수 있게 해야 함

⑥ 액추에이터를 동력이 전달된 상태로부터 분리될 때에만 허용되어야 함

(5) 수동 리셋 기능을 제공하는 안전관련 부품들의 성능수준은 수동 리셋 기능이 포함되어 있는 안전기능의 요구 안전성을 저하시키지 않도록 유지되어야 한다.

(6) 리셋 액추에이터는 위험영역의 외부와 위험영역에 사람이 있는지를 검사하기에 좋은 가시성이 있는 안전한 장소에 설치되어 있어야 한다.

(7) 위험영역에 대한 가시성이 완전하지 않은 곳에서, 특별한 리셋 절차를 구성하여 운영해야 한다.

① 한가지 해결책은 두 번째 리셋 액추에이터를 사용하는 것임

② 리셋 기능은 위험영역 내에서 위험영역의 밖(방호설비 근처)에 위치한 두 번째 리셋 액추에이터와 조합된 첫 번째 액추에이터에 의해서 개시됨

5.2.3 시동 재시동 기능

(1) 기계가 비정상적으로 정지된 이후(예를들면 정전, 무선제어신호의 상실 등)에는 원치 않는 작동을 방지하는 조치가 되어 있어야 한다.

(2) 하나이상의 조작반이 설치된 경우 다른 조작반의 명령개시가 위험한 상황을 초래하지 않도록 하여야 한다.

(3) 재시동은 위험한 상황이 존재할 수 없을 때에만 자동적으로 작동할 수 있어야 한다.

(4) 시동과 재시동에 대한 이 요구사항들은 원격으로 제어될 수 있는 기계들에도 적용해야 한다.

(5) 안전장치를 적용하기 곤란한 기계(이동기계)의 경우에는 적용 가능한 합법적인 장치와 함께 잡고 있을 때에만 가동되는 수동제어 작동이 되도록 하여야 한다.

(6) 기계의 기동제어반이 하나 이상일 경우에는 다음조건이 만족되어야 한다.

① 각 제어반은 별도의 수동식 기동제어장치를 구비해야 함

② 기계작동에 필요한 모든 조건이 만족되어야 함

③ 모든 기동제어장치는 기동되기 전에 안전위치에 있어야 함

④ 모든 기동제어장치는 동시에 작동되도록설계되어야 함

5.2.4 부분개별 제어기능(local control function)

(1) 기계가 부분적으로 제어될 때, 예를 들면, 휴대용 제어장치나 펜던트의 경우 다음의 요구사항들이 적용되어야 한다.

① 부분제어를 선택하기 위한 수단은 위험영역의 밖에 위치되어야 함

② 위험한 상태를 개시하는 것은 위험성평가에 의해 정의된 영역인 부분제어에 의해서만 가능해야 함

③ 부분제어와 주제어 사이의 전환은 위험한 상황을 유발하지 않아야 함

(2) 휴대형 및 펜던트(매달기형) 제어반과 그 제어장치는 운전원이 제어반을 떨어뜨리거나 부딪칠 경우에 충격이나 진동으로 인한 오동작의 우려가 최소화되도록 선정 및 배치 되어야 한다.

5.2.5 기능정지 기능

(1) 기능정지 기능은 기능정지 동안에 다른 수단을 통하여 안전조건들이 제공되어 어떤 사람도 위험한 상황에 노출되지 않도록 하여야 한다.

(2) 기능정지가 끝날때, SRP/CS의 모든 안전기능들은 회복되어야 한다. 이때 기능정지 기능을 제공하는 안전관련 부품들의 성능수준은 기능정지 기능이 포함된 안전기능의 요구되는 안전성을 저하시키지 않도록 선정되어야 한다.

5.2.6 실행유지 기능

(1) 작동신호가 있을 때에만 제어하는 가동유지제어(Hold-To Run Controls)는 조작 완료 시까지 제어장치가 연속적으로 실행되어야 한다.

5.2.7 허용제어 장치

(1) 가동을 위한 제어장치는 다음과 같은 수동조작제어기능 연동장치 이다.

① 작동시 별도 기동제어에 의하여 기계작동이 개시될 수 있음

② 비활성시 정지기능을 활성화하여 기계작동 개시를 방지해야 함

(2) 시스템의 일부로서 허용제어장치가 제공될 때에는 하나의 위치로만 조작을 허용

하기 위해 허용신호를 보내어야 한다. 즉 다른 위치로의 조작은 중지 또는 방지되어야 한다.

5.2.8 예상치 못한 시작 방지

(1) 유지 보수 도중에 기계의 기동으로 위험을 초래할 우려가 있는 경우에는 불시기동방지 장치를 설치하여야 한다.

(2) 불시기동방지장치는 사용에 적합하고 편리하여야 하며, 용이하게 식별이 가능한 곳에 있어야 한다.

5.2.9 격리와 에너지 방출 기능

(1) 기계위에서 필요한 작업을 할 경우 기계동작에 의한 위험을 발생시키지 않도록 전기장비의 전원을 차단하여야 하나, 다음의 회로는 전원차단장치에 의하여 차단할 필요가 없고 자체 차단장치로 차단할 것을 권고한다.

① 유지 보수 수리 중에 필요한 조명용 전기회로

② 수리 또는 유지 보수용 도구 및 장비의 접속용 플러그 및 소켓 수구(핸드드릴, 시험장비 등)

③ 전원공급 실패시 자동 차단용으로만 사용하는 부족 전압 보호회로

④ 정상작동을 위하여 항상 전원이 공급되어야 하는 선로(온도제어측정장치, 공정상(연속작업 시)의 가열기, 프로그램 저장장치)

⑤ 연동장치용 제어회로

(2) 위의 회로들이 전원차단장치로 차단되지 않는다면 다음의 조치를 취하여야 한다.

① 전원차단장치 가까운 위치에 반영구적인 경고 표지를 부착

② 적용제외 회로를 다른 회로와 구별함

(3) 전원차단장치의 조작도구(손잡이)는 쉽게 접근이 가능한 위치에 설치하되 지면위로부터 0.6m ∽ 1.9m 사이에 위치(가능한 1.7m 이하 권고)하도록 한다.

(4) 에너지가 방출되는 기능으로부터 근로자를 보호하기 위하여 간접접촉방지 조치를 취하여야 한다. 즉 전기장비의 각 회로 또는 각 부분은 “위험한 접촉 전압의 발생방지를 위한 조치” 또는 “접촉 전압이 위험한 준위까지 올라가기 전에 전원의 자동 차단” 조치 중 하나이상의 방법을 적용하여야 한다.

(5) 위험한 접촉 전압의 발생억제 조치 방안은 다음과 같다.

① 기초절연 파괴시 접촉이 우려되는 부위에 위험한 접촉전압의 발생을 억제하기 위하여 절연에 의한 보호

② 선로 충전부의 기초절연파괴에 의해 충전될 수 있는 노출 도전부와의 접촉을 통한 위험한 접촉전압을 억제하기 위하여 각 선로의 전기적 분리에 의한 보호

5.2.10 제어모드들과 모드선택

(1) 각 기계는 그 형태 및 사용 용도에 따라 하나이상의 작동방식을 가지게 되는데, 그 작동방식이 위험한 상황을 일으킬 수 있는 경우 적합한 수단에 의해 이를 방지하여야 한다.

(2) 모드 선택스위치 자체로 기계가 작동되어서는 아니되며 운전자에 의하여 별도의 작동이 요구되어야 한다.

(3) 각 특정한 작동방식, 관련 안전기능 및 보호장치가 이행되어야 한다.

(4) 방식 선정기 위치, 표시광 구비, 시각표시 등과 같이 선정된 작동방식이 표시되어야 한다.

5.2.11 제어시스템들의 다른 안전관련 부품들과의 상호작용

(1) 동시 작동 시 위험한 상태를 초래할 수 있는(예: 역운동을 야기시키는 것) 접점, 릴레이 등 제어 기구는 상호 연동되어야 한다.

(2) 역회전용 접점(예: 전동기 회전 방향을 제어하는 것)은 스위치 조작 시 회로 단락 사고가 일어나지 않도록 상호 연동되어야 한다.

(3) 기계 작동의 연속성과 안전상 기계의 여러 기능이 상호 연계되어 작동되는 경우(계단식 속도 제어 등), 상호 원만한 협조가 되도록 적절한 연동 기능을 구비하여야 한다.

(4) 여러 기계가 상호 연계되어 작업이 이루어지는 경우에는 제어기 사이에 적절한 상호 연동이 이루어져야 한다.

(5) 기계 제동 액추에이터의 고장이 당해 기계의 액추에이터를 작동시켜 위험 상태를 초래할 우려가 있는 경우의 연동 장치는 당해 액추에이터의 전원이 차단되도록 되어야 한다.

5.2.12 안전관련 입력값의 감시 파라미터화

(1) 파라미터화에 이용된 모든 데이터의 무결성은 유지되어야 하고, 이는 다음의 적용된 조치들에 의해서 이루어져야 한다.

① 유효한 입력 범위의 제어

② 전송 이전의 데이터 변조 제어

③ 파라미터 전송과정으로부터의 오류효과의 제어

④ 불완전한 파라미터 전송의 효과를 제어

⑤ 파라미터화를 위해 사용된 하드웨어와 소프트웨어의 결함과 고장 효과의 제어

(2) 파라미터화 도구는 SRP/CS에 대한 다양한 모든 요구사항을 만족하여야 하나, 어려울 경우에는 별도의 안전관련 파라미터 설정을 위해서 특별한 절차가 사용되어야 한다.

① 파라미터화 도구로 수정된 파라미터의 재전송

② 차후 확인뿐만 아니라, 파라미터의 무결성을 확인하는 다른 적절한 방법(예를 들면 적절하게 숙련된 사람과 파라미터화 도구에 의한 자동점검을 사용하는 것)

(3) 전송/재전송 과정에서의 엔코딩/디코딩을 위해 사용된 소프트웨어 모듈들과, 사용자에 대한 안전관련 파라미터들의 시각화를 위해 사용된 소프트웨어 모듈들은 계통적 고장을 피하기 위해서 함수에서의 다양성을 최소한으로 사용을 자제한다.

5.2.13 긴급정지 기능(보조 보호조치)

(1) 긴급정지 기능 등 비상조작은 다음사항의 개별적 또는 조합을 포함한다.

① 비상정지: 위험한 공정 또는 이동을 멈추게 하기 위한 비상조작

② 비상기동: 위험한 상태의 제거 또는 회피하기 위한 공정 또는 이동을 시작하기 위한 비상조작

③ 비상전원 차단: 감전 또는 기타 전기적 위험과 관련된 경우, 설비의 일부 또는 전체에서 전기 에너지의 공급을 차단하기 위한 비상 조작

④ 비상전원 투입: 비상 상태 시 사용하기 위한 설비의 일부에 전기 에너지의 공급을 하기 위한 비상 조작

(2) 비상 정지의 조작 또는 비상 전원 차단 조작기가 작동되면 리셋 시까지 정지되어야 한다.

① 리셋은 명령이 개시된 해당 위치에서만 가능해야 하는데, 명령의 리셋은 기계를 재시동해서는 안 되고 단지 재시동을 허용하기만 해야 함

② 모든 비상 정지 및 비상전원 차단 명령이 리셋된 후에 기계 재시동이 가능해야 함

(3) 비상정지의 범주선정은 기계의 위험성평가에 의해 결정되어야 하며, 다음사항을 만족해야 한다.

① 모든 방식에서 기타 다른 모든 기능 및 작동을 무효화하여야 함

② 위험한 상태를 유발시킬 수 있는 기계 액추에이터의 동력은 즉시 제거 되거나, 기타 위험한 상태가 야기되지 않도록 가능한 한 신속히 차단하여야 함

③ 복귀가 기계를 재 기동시켜서는 아니됨

(4) 다음의 경우에는 비상전원 차단장치가 설치 되어야 한다.

① 직접 접촉(예: 컬렉터 선, 컬렉터 봉, 슬립 링 조립체, 전기 취급 지역의 제어 장치) 방지를 위해 장애물이나 이격 설치한 경우

② 전기로 인하여 다른 위험 요인의 발생 또는 손상 우려가 있는 경우

5.2.14 반응시간

(1) SRP/CS의 반응시간은 SRP/CS의 위험성평가에 의해 필요한 것으로 밝혀진 경우 결정되어야 한다.

① 제어시스템의 반응시간은 기계의 전체 반응시간의 일부분임

② 기계에 요구되는 전체 반응시간은 안전관련 부품의 설계에 영향을 미칠 수 있음(예를 들면 제동시스템의 제공 필요성).

5.2.15 안전관련 파라미터(속도, 온도, 압력 등)

(1) 안전관련 파라미터들(예를 들면 위치, 속력, 온도 또는 압력)이 주어진 한계로부터 벗어날 때, 제어시스템은 적절한 조치를 시작해야 한다.

(2) 프로그램 가능한 전자시스템에 안전관련 데이터의 수동입력의 오류가 위험한 상황을 유발할 수 있다면, 그때 안전관련 제어시스템 내에 데이터 점검시스템이 제공되어야 한다.

5.2.16 동력원의 변동, 손실과 회복 등

(1) 지정 작동범위 밖에서 에너지 공급의 손실을 포함하는 에너지 수준변동이 일어난다면, SRP/CS는 다른 기계시스템의 부품들이 안전한 상태를 유지할 수 있도록 하는 출력신호를 제공하거나 개시하는 것을 계속하여야 한다.

5.2.17 알람과 경고신호

(1) 표시등은 작업자의 주의를 끌거나 지정된 절차를 준수하여야 하는 것을 나타내고자 할 경우, 적색, 황색, 녹색 및 청색으로 표시한다.

(2) 확인은 명령 상태를 확인하거나 변경 또는 전환 시간 종료의 확인이 필요할 경우, 황색과 흰색을 사용한다.(필요 시 녹색도 사용 가능함)

① 표시등 및 디스플레이는 작업자의 정상 위치로부터 시각적으로 확인 가능한 방식으로 선정 및 설치되어야 함

② 경고등에 사용된 표시등 회로에는 이런 등의 조작을 점검하기 위한 장치가 장착되어야 함

(3) 공급자와 사용자 사이에 별도의 약정이 없는 경우, 표시(안내)등의 렌즈는 기계의 조건(상태)에 관하여 색상 부호화하여야 하며, 기계의 표시 타워 색은 위에서 아래로 적색, 황색, 청색, 녹색, 흰색 순으로 한다.

(4) 다음과 같은 목적에 따라 그 이상의 식별이나 정보, 특히 추가적인 강조가 필요한 경우에는 점멸등을 설치할 수 있다.

① 주의를 환기시킬 필요가 있을 경우

② 즉각적인 조치가 필요할 경우

③ 명령과 실제 상태의 불일치를 나타낼 경우

④ 처리 과정 중 변경을 나타낼 경우(전이 과정 중 점멸)

(5) 우선 순위가 높은 내용의 전달 시에는 점멸 속도가 빠른 점멸등을 사용한다.

① 점멸등 또는 디스플레이가 더 높은 우선순위의 정보를 전달하기 위해 사용될 경우, 청각 경고 장치도 제공되어야 함

② 조광 누름 버튼 액추에이터는 색상 부호화하여야 함

③ 적절한 색상을 정하기 어려운 경우에는 흰색을 사용하되, 비상정지 액추에이터용 적색은 자체의 발광에 의존하여서는 아니됨

6 범주와 각 채널의 $MTTF_d$, DC_{avg} 그리고 CCF의 관계

6.1 일반사항

(1) SRP/CS는 6.2절에 명시된 다섯 범주의 하나 혹은 여러 개의 요구사항에 부합하여야 한다.

(2) 범주는 특정 PL을 성취하기 위해 사용되는 기본 파라미터들인데, 제4장에서 설명된 설계고려사항에 근거하여 결함들에 대한 저항 관점에서 SRP/CS에 요구되는 동작을 서술한다.

(3) 범주 B는 기본 범주다. 결함의 발생은 안전기능의 손실을 유발할 수 있다.

(4) 범주 1에서 결함에 대한 개선된 저항은 대개 부품의 선택과 활용에 의해서 달성된다.

(5) 범주 2에서는 특정 안전기능이 작동상태임을 주기적으로 점검함으로써 달성된다.

(6) 범주 3과 범주 4에서는 단일결함이 안전기능의 손실을 유발하지 않음을 보장함으로써 달성된다. 범주 4와 범주 3에서는 합리적으로 수행 가능할 때마다, 그러한 결함이 감지될 것이다.

(7) <표 8>은 SRP/CS 범주들의 개요, 요구사항 그리고 결함상황에서의 시스템 거동을 제시한 것이고, 특정 SRP/CS에 대한 범주의 선택은 주로 다음 사항에 의해 결정된다.

① 부품이 기여하는 안전기능에 의해서 성취되는 위험성의 감소,

② 성능요구수준 (PLr),

③ 사용된 기술들,

④ 그 부품에 결함 발생 시 발생하는 위험성

⑤ 그 부품에서 결함을 피할 수 있는 가능성(체계상 결함)

⑥ 그 부품에 결함이 발생할 가능성 및 관련 파라미터

⑦ 평균위험고장시간($MTTF_d$)

⑧ 진단범위(DC)

⑨ 범주 2, 범주 3 및 범주 4의 상황에서의 공통원인고장(CCF)

<표 8> 범주에 대한 요구사항 요약

범주	요구사항의 요약	시스템동작상태	안전을 달성하는 원칙	각채널의 $MTTF_d$	평균진단범위 DC_{avg}
B	SRP/CS와 그들의 구성요소들뿐만 아니 라 그들의 방호장치는, 예상되는 영향을 견딜 수 있도록 관련표준에 맞추어 설계, 제작, 선택, 조립되어야 한다. 기본적 안전 원칙이 적용되어야 한다.	결함의 발생이 안전기능의 상실을 초래할 수 있다	주로 구성요소의한 특성화	낮음 중간	없음
1	B의 요구사항이 적용되어야 한다. 충분한 시험을 거친 구성요소와 안전원칙들이 사용되어야 한다.	결함의 발생이 안전기능의 상실을 일으킬 수 있지만, 발생확률은 범주B 의 경우 보다 낮다	주로 구성요소에 의한 특성화	높음	없음
2	B의 요구사항과 충분한 시험을 거친 안전원칙이 적용되어야 한다. 안전기능은 기계제어시스템에 의해 적절한 간격으로 점검되어야 한다.	결함의 발생은 점검간에 안전기능의 상실을 초래할 수 있다. 안전기능의 상실은점검에 의하여 검출된다.	주로 구조에 의한 특성화	낮음 높음	낮 음 중간
3	B의 요구사항과 충분한시험을 거친 안전원칙이 적용되어야 한다. 안전관련 부품은 다음과 같이 설계되어야 한다 - 이 부품들 중의 어떠한 단일결함도 안전기능의 상실을 초래하지 않는다. - 합리적으로 실현가능한 모든 경우 단일결함이 검출된다.	단일결함이 발생하면 안전기능은 항상 수행된다. 모든 결함은 아니지만 일부 결함이검출된다. 미검출 결함의 축적이 안전기능의상실을 초래할 수도 있다.	주로 구조에 의한 특성화	낮음 높음	낮 음 중간
4	B의 요구사항과 충분한시험을 거친 안전원칙이 적용되어야 한다. 안전관련 부품은 다음과 같이 설계되어야 한다. - 이 부품들 중의 어떠한 단일결함도 안전기능의 손실을 초래하지 않는다. 또한, - 단일결함은 안전기능에 대한 다음 사용요구 시 또는 그 이전에검출된다. 만약 이것이불가능한 경우, 결함의축적이 안전기능의 상실을 초래하지 않아야한다.	단일결함이 일어나면 안전기능은 항상 수행된다. 축적된 결합의 감지는 안전기능의상실 확률을 낮춘다 (높은 DC) 안전기능의 상실방지를 위하여 결함이 적시에 검출된다.	주로 구조에 의한 특성화	높음	실패를 포함하여 높음

6.2 범주의 시방

6.2.1 일반사항

(1) 각 SRP/CS는 관련된 범주의 요구사항들을 준수해야 한다.

(2) 이절의 그림은 일반적인 아키텍처들을 보여준다. 이 아키텍처들로부터 벗어난 아키텍처는 언제나 가능하다. 그러나 어떠한 벗어난 아키텍처도 적절한 해석도구(예를 들면, 결함트리 해석)를 사용하여 정당화되어야 하며, 이로 인해 시스템이 성능요구수준(PLr) 을 충족하도록 해야 한다.

(3) 범주 3과 범주 4의 경우, 이는 모든 부품들이 반드시 물리적으로 중복인 것이 아니라 결함이 안전기능의 손실을 유발할 수 없는 것을 확인하는 다양한 방법이 있다는 것을 의미한다.

6.2.2 지정아키텍처

(1) SRP/CS의 구조는 PL에 큰 영향을 미치는 핵심 특성이다.

① 가능한 구조들의 다양성이 높더라도, 기본개념은 종종 유사함

② 기계 분야에서 존재하는 대부분의 구조들은 범주들 중 하나로 대응될 수 있음

③ 각각의 범주에 대해 전형적인 표현법이 안전관련 블록선도를 이용하여 만들어질 수 있음

(2) <그림 5>에 보여지는 PL은 범주, 각채널의 $MTTF_d$ 그리고 DC_{avg}에 의해 결정되고, 지정아키텍처에 기반한다.

① 만약 <그림 5>가 PL을 예측하는데에 사용된다면 SRP/CS의 아키텍처는 요구되는 범주의 지정아키텍처와 동등하다는 것이 증명되는 것이 바람직 함

② 일반적으로 각각의 범주들의 특성들을 만족하는 설계는 각각의 범주의 지정아키텍처와 동등하게 됨

6.2.3 범주 B

(1) SRP/CS는 다음 사항에 견디기 위해 적어도 관련된 표준들에 부합하고, 특정 응용에 대한 기본안전 원칙의 사용을 통해 설계, 구성, 선택, 조립 그리고 결합되어야 한다.

① 예상되는 작업 스트레스

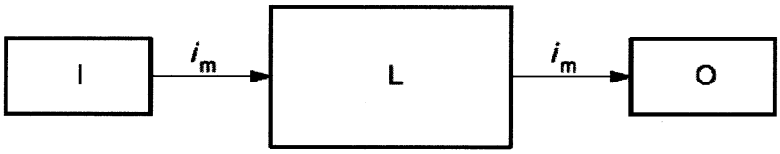
② 가공된 물질의 영향, 예를 들면 세탁기에서의 세제

③ 관련된 다른 외부의 영향들, 예를 들면 기계적 진동, 전자기적 영향, 동력 공급중단, 혹은 장애들

(2) 범주 B 내에는 진단범위(DC_{avg} = none)는 없고 각 채널의 $MTTF_d$는 중간보다 낮을 수 있다. 이러한 구조에서(보통 단일-채널 시스템), CCF의 고려는 적절하지 않다.

(3) 범주 B에서 달성할 수 있는 최대 PL은 PL=b 이다.

(4) 결함이 발생할 때 안전기능의 상실을 유발할 수 있다.



i_m 상호연결수단들, I 입력장치, L 논리, O 출력장치

<그림 8> 범주 B를 위한 지정아키텍처

6.2.4 범주 1

(1) 범주 1의 경우, 6.2.3에 따라 범주 B의 요구사항이 적용되어야 하고 다음 사항이 추가로 적용된다.

(2) 범주 1 에 할당된 제어시스템의 안전관련 부품들은 충분한 시험을 거친 구성요소들과 안전원칙들을 이용하여 설계되고 구성되어야 한다.

(3) 안전관련 응용에 대해 충분한 시험을 거친 구성요소란 다음 중 하나와 같다.

① 유사한 상황에서 성공적 결과를 얻어 과거 널리 사용되었던 구성요소.

② 안전관련 응용에 대해 적합성과 신뢰성을 증명한 원칙을 사용하여 만들어지고 검증된 것

(4) 새롭게 개발된 구성요소와 안전원칙들이 이의 조건을 충족한다면 “충분한 시험을 거친”것과 동등하게 간주될 수 있다.

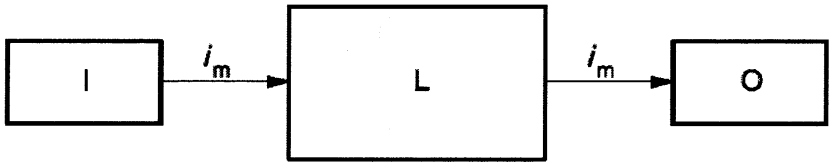
(5) 어떤 특정 구성요소를 충분한 시험을 거친 구성요소로 인정하는 것은 응용에 따라 다를 수 있다.

(6) 각 채널의 $MTTF_d$는 높아야 한다.

(7) 범주 1에서 달성 가능한 최대 PL은 PL = c이다

(8) 범주 1 시스템에는 진단범위(DCavg=none)가 없고, 이러한 구조(단일채널 시스템)에서는 CCF에 대한 고려는 적절하지 않다.

(9) 결함이 발생하면, 안전기능의 손실이 초래될 수 있다. 그러나 각 채널의 범주 1에서의 $MTTF_d$는 범주 B에서보다 높다. 결과적으로 안전기능의 손실이 발생할 가능성은 적다.



i_m 상호연결수단들, I 입력장치, L 논리, O 출력장치

<그림 9> 범주 1에 대한 지정아키텍처

6.2.5 범주 2

(1) 범주 2에 대해서는 6.2.3에 따라 범주 B에 대한 동일한 요구사항이 적용되어야 하며, 6.2.4에 따라 “충분한 시험을 거친 안전원칙”또한 적용되어야 한다. 추가로 다음 사항을 적용한다.

(2) 범주 2의 SRP/CS는 그들의 기능이 기계제어시스템에 의하여 적절한 간격마다

점검되도록 설계되어야 한다. 안전기능의 점검은 다음의 경우에 주기적으로 수행되어야 한다.

① 기계시동 시

② 위험한 상황의 개시 전, 예를 들면 새로운 주기의 시작, 다른 동작의 시작, 그리고 위험성평가 및 동작의 종류에 의해 필요하다고 판명될 경우 등

(3) 안전기능의 점검은 자동으로 시작될 수 있는데 결함이 검출되지 않았다면 작동을 허가하거나, 만약에 결함이 검출되면 적절한 제어행동을 촉발하는 출력을 발생시켜야 한다.

(4) 출력은 안전상태를 개시하여야 한다. 안전상태는 결함이 해결될 때까지 유지되어야 한다. 안전상태를 개시할 수 없을 때(예를 들면, 최종 스위치 장치에서 접촉부가 용접되는 경우), 출력은 위험요인에 대한 경고를 제공해야 한다.

(5) 범주 2의 지정아키텍처의 경우, <그림 10>에 나타난 대로, $MTTF_d$와 DC_{avg}의 계산은 시험채널의 블록이 아닌 기능채널의 블록만을 고려하는 것이 좋다.

(6) 결함감지를 포함한 전체 SRP/CS 진단범위(DC_{avg})는 낮아야 한다. 각 채널의 $MTTF_d$는 성능요구수준(PLr)에 따라 낮음∽높음 사이일 수 있다. CCF에 대한 조치가 적용되어야 한다.

(7) 점검 그 자체가 위험한 상황을 초래하지 않아야 한다. 점검장비는 안전기능을 제공하는 안전관련 부품들과 통합된 것일 수도 있고 또는 분리된 것일 수도 있다.

(8) 범주 2의 경우 성취할 수 있는 최대 PL은 PL = d 이다.

(9) 범주 2의 시스템 동작상태는 다음을 허용한다.

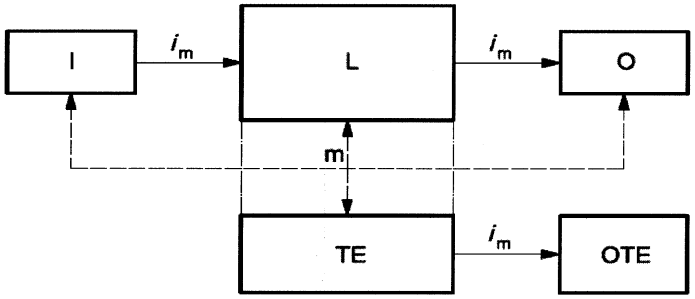
① 결함발생은 점검과 점검 간에 안전기능의 손실을 초래할 수 있음

② 안전기능의 손실은 점검으로 감지됨

6.2.6 범주 3

(1) 범주 3의 경우, 6.2.3에 따라 범주 B에 대한 요구사항이 동일하게 적용되어야

하며, 6.2.4에 따라 “충분한 시험을 거친 안전원칙”또한 적용되어야 한다. 추가로 다음 사항도 적용된다.



i_m 상호연결수단들, I 입력장치, L 논리, m 감시, O 출력장치, TE 시험장치, OTE TE의 출력
(파선은 합리적으로 실현 가능한 결함감지를 나타냄)

<그림 10> 범주 2에 대한 지정아키텍처

(2) 범주 3의 SRP/CS는 이 부품들 중 어느 한 개에 발생한 단일결함도 안전기능의 상실을 유발하지 않도록 설계되어야 한다. 즉 합리적으로 실현 가능한 모든 경우, 단일결함은 안전기능에 대한 다음사용요구 시 또는 그 이전에 감지되어야 한다.

(3) 결함감지를 포함한 전체 SRP/CS의 진단범위 값(DC_{avg})은 낮아야 한다. PLr에 따라 각 중복 채널의 $MTTF_d$는 낮음~높음이어야 한다. CCF에 대한 조치가 적용되어야 한다.

(4) 모든 결함이 감지된다는 것을 의미하지는 않는다. 결론적으로 감지되지 못한 결함의 축적이 기계에 있어서 의도하지 않은 출력과 위험한 상황을 초래할 수 있다.

(5) 범주 3 시스템 동작상태는 다음을 허용한다.

① 단일결함이 발생하여도 안전기능이 항상 수행된다.

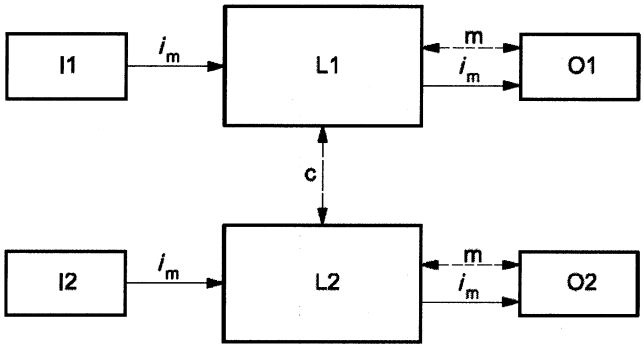
② 모든 결함은 아니지만 일부 결함들이 감지된다.

③ 감지되지 않은 결함의 축적은 안전기능의 상실을 초래할 수 있다.

6.2.7 범주 4

(1) 범주 4의 경우, 6.2.3에 따라 범주 B의 요구사항이 동일하게 적용되어야 하며,

6.2.4에 따라 “충분한 시험을 거친 안전원칙”또한 적용되어야 한다. 추가로 다음 사항이 적용된다.



i_m 상호연결수단들, c 교차감시, I1, I2 입력장치, L1, L2 논리, m 감시, O1, O2 출력장치

<그림 11> 범주 3에 대한 지정아키텍처

(2) 범주 4에 대한 SRP/CS는 다음과 같이 설계되어야 한다.

① 안전관련 부품들 중 어느 것에서의 단일결함도 안전기능의 상실을 초래하지 않아야 한다.

② 단일결함은 안전기능에 대한 다음 번 사용요구 시 또는 그 이전에 감지된다. 그러나 이 감지가 불가능하다면, 결함의 축적이 안전기능의 상실을 초래하지 않아야 한다.

(3) 결함의 축적을 포함한 전체 SRP/CS의 진단범위 값(DC_{avg})은 높아야 한다. 각 중복 채널의 $MTTF_d$는 높아야 한다. CCF에 대한 조치가 적용되어야 한다.

(4) 범주 4의 시스템 동작상태는 다음을 허용한다.

① 단일결함이 발생하여도, 안전기능은 항상 수행된다.

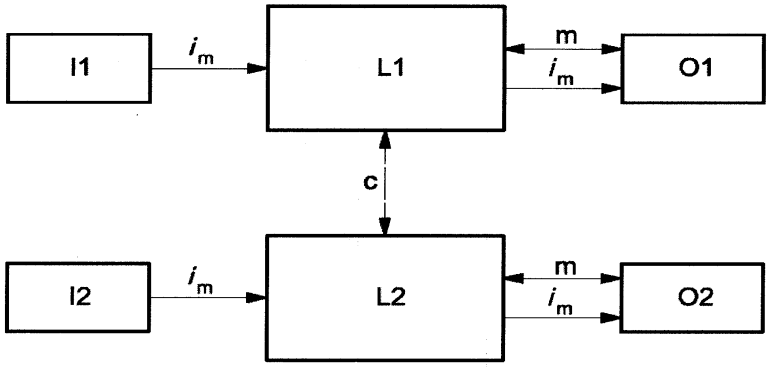
② 결함은 안전기능의 상실을 방지하기 위해 늦지 않게 감지된다.

③ 감지되지 않은 결함의 누적을 고려한다.

6.3 전체 PL을 달성하기 위한 SRP/CS 조합

(1) 안전기능은 몇 개의 SRP/CS의 조합에 의해 구현할 수 있다. 예를들면 입력 시스템, 신호 처리 유닛, 출력시스템.

(2) SRP/CS는 하나 또는 다른 범주로 할당될 수 있다. 사용된 각각의 SRP/CS에 대해 6.2절에 따라 범주가 선택되어야 한다.



i_m 상호연결수단들, c 교차감시, I1, I2 입력장치, L1, L2 논리, m 감시, O1, O2 출력장치(감시에 대한 실선은 범주 3에 대한 지정아키텍처보다 높은 진단범위를 나타냄)

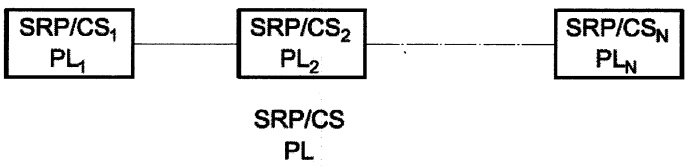
<그림 12> 범주 4에 대한 지정아키텍처

(3) SRP/CS의 전체적인 조합의 경우 전체 PL은 <표 8>을 이용하여 파악/식별될 수 있다. 이 경우, SRP/CS 조합에 대한 검증이 요구된다.

(4) 6.2절에 따라 SRP/CS의 조합은 안전관련 신호가 개시된 지점에서 시작하고 동력 제어요소의 출력에서 끝난다. 그러나 조합된 SRP/CS는 선형적 (직렬 배열) 또는 복수 방식(병렬 배열)으로 연결된 몇 개의 부품으로 구성될 수 있다.

(5) 모든 부품들의 개별 성능수준(PL)들이 이미 계산되어 있는 조합된 SRP/CS에 의해 달성되는 PL의 새롭고 복잡한 예측을 피하기 위해 직렬배열 SRP/CS의 경우 다음의 예측방법이 제시된다.

(가) 전체로서 안전기능을 수행하는 직렬 배열된 A에의 분리된 SRP/CSj을 가정하자. 각각의 SRP/CS_i, 에 대해 이미 PL_i 는 결정/결과평가 되어 있다. 이 상황이 <그림 13>에 나타나 있다.



<그림 13> 전체 PL을 달성하기 위한 SRP/CS의 조합

(나) 다음 방법을 이용하면 안전기능을 수행하는 조합된 SRP/CS의 전체 PL을 계산할 수 있다.

① 가장 낮은 PL_i을 파악/식별한다. 이 값이 PL_{low} 이다.

② SRP/CS_i 의 숫자 $N_{low} \leq N$ 을 파악/식별한다. 이때 $PL_i = PL_{low}$.

③ <표 8>에서 PL을 찾는다.

<표 9> 제어시스템의 안전관련 부품 직렬정렬을 위한 PL계산

PL_{low}.	N_{low}	⇒	PL
a	> 3	⇒	없음, 허용안됨
	≤ 3	⇒	a
b	> 2	⇒	a
	≤ 2	⇒	b
c	> 2	⇒	b
	≤ 2	⇒	c
d	> 3	⇒	c
	≤ 3	⇒	d
e	> 3	⇒	d
	≤3	⇒	e

7 결함 고려사항, 결함 제외

7.1 일반사항

선택된 범주에 따라, 안전관련 부품들은 성능요구수준(PLr)을 달성할 수 있도록 설계되어야 한다. 결함에 저항할 수 있는 능력이 평가되어야 한다.

7.2 결함 고려사항

(1) 한 가지 결함의 결과로 후속요소가 고장나면, 최초의 결함과 그에 따르는 모든 결함들은 하나의 결함으로 간주되어야 한다.

(2) 한 개의 공통원인을 갖는 두 개 또는 그 이상의 분리된 결함은 하나의 결함(CCF로 알려진) 으로 간주되어야 한다.

(3) 독립적인 원인을 갖는 두 개 또는 그 이상의 결함의 동시 발생은 거의 발생하지 않을 것으로 볼 수 있으므로 고려할 필요가 없다.

7.3 결함 제외

(1) 어떤 결함들은 제외될 수 있다는 가정 없이 SRP/CS을 결정하고 결과를 평가하는 것이 항상 가능한 것은 아니다.

(2) 결함 제외는 기술적 안전요구사항과 결함발생의 이론적 가능성 사이의 절충이다.

(3) 결함 제외는 다음사항에 근거할 수 있다.

① 어떤 결함발생이 기술적으로 일어날 것 같지 않음

② 고려하는 응용분야와 무관하게 일반적으로 인정되는 기술적 경험

③ 응용과 특정한 위험요인에 관계되는 기술적 요구사항

(4) 결함이 제외되는 경우 상세한 근거가 기술문서에 제시되어야 한다.

8 검증

SRP/CS의 설계는 검증되어야 한다(<그림 3> 참조). 검증은 각 안전기능을 제공하는 SRP/CS들의 조합이 이 표준의 모든 관련 요구사항을 충족시킨다는 것을 증명하여야 한다.

9 정비

(1) 예방정비 또는 사후정비는 통상 안전관련 부품들의 규정된 성능을 유지하기 위하여 필요할 수 있다.

(2) 시간이 지남에 따라 규정된 성능으로부터 벗어나게 되는 경우 안전성 저하나 심지어 위험한상황이 초래될 수도 있으므로 SRP/CS의 사용자 정보는 SRP/CS의 보전에 대한 지침(주기적 검사 포함)을 포함해야 한다.

(3) 제어시스템의 안전관련 부품들의 정비에 관한 규정은 KS B ISO 12100:2010의 6.2.7의 원칙을 따라야 한다.

10 기술 문서화

(1) SRP/CS의 설계 시, 안전관련 부품에 관련된 다음 정보에 대해 문서화해야 한다.

① SRP/CS에 의해 제공된 안전기능

② 각 안전기능의 특징

③ 안전관련 부품들의 정확한 시작과 끝

④ 환경조건

⑤ 성능수준 (PL)

⑥ 선택된 범주 또는 범주들

⑦ 신뢰성에 관련된 파라미터($MTTF_d$, DC, 및 임무시간)

⑧ 체계상의 고장에 대한 조치

⑨ 사용된 기술 또는 기술들

⑩ 고려한 모든 안전관련 결함

⑪ 결함 제외에 대한 정당성

⑫ 설계의 논거(예를 들면 고려된 결함, 제외된 결함)

⑬ 소프트웨어 문서화

⑭ 합리적으로 예측 가능한 오용에 대한 조치

11 사용자 정보

(1) SRP/CS들의 안전한 사용을 위하여 중요한 정보는 사용자에게 제공되어야 한다.

(2) 사용자 정보에는 다음 사항들이 포함되어야 하지만 이들에 국한되는 것은 아니다.

① 선택된 범주에 대한 안전관련 부품들의 한계와 결함 제외

② SRP/CS의 한계와 결함 제외(7.3 참조)에 대해 선택된 범주와 안전성능의 유

지가 중요할 때 결함 제외에 대한 지속적인 정당성을 확보하기 위해 적절한 정보 (수정, 보전 및 수리)가 반드시 주어져야 한다

③ 규정된 성능으로부터의 이탈이 안전기능에 미치는 영향

④ SRP/CS들과 방호장치에 대한 인터페이스의 명확한 설명

⑤ 반응시간

⑥ 환경조건을 포함하는 작동한계

⑦ 지시와 경보

⑧ 안전기능의 중지와 차단

⑨ 제어모드

⑩ 보전 점검목록 및 보전관련 사항

⑪ 접근과 내부부품 교체의 용이성

⑫ 쉽고 안전한 고장수리를 위한 수단

⑬ 참고한 범주에 관련된 응용분야에 대한 정보

⑭ 검사시험 주기(해당되는 경우)

(3) SRP/CS들의 범주와 성능수준에 대한 구체적 정보가 다음과 같이 주어져야 한다

① 이 표준에 인용된 문헌의 시기 (예를들면 “ ISO 13849-1:2006")

② 범주: B, 1,2, 3 또는 4

③ 성능수준: a, b, c, d, 또는 e.

【붙임】

<그림 5>의 수치표시 (2의 1)

	시간(1/H)당 위험한 고장의 평균확률과 해당 성능수준(PL)													
각 채널에 대한 $MTTF_d$ 년	Cat.B DC_{avg}=없음	PL	Cat.1 DC_{avg}=없음	PL	Cat.2 DC_{avg} =낮음	PL	Cat.2 DC_{avg} =중간	PL	Cat.3 DC_{avg} =낮음	PL	Cat.3 DC_{avg} =중간	PL	Cat.4 DC_{avg} =높음	PL
3	3.80×10-5	a			2.58×10-5	a	1.99×10-5	a	1.26×10-5	a	6.09×10-6	b		
3.3	3.46×10-5	a			2.33×10-5	a	1.79×10-5	a	1.13×10-5	a	5.41×10-6	b		
3.6	3.17×10-5	a			2.13×10-5	a	1.62×10-5	a	1.03×10-5	a	4.86×10-6	b		
3.9	2.93×10-5	a			1.95×10-5	a	1.48×10-5	a	9.37×10-6	b	4.40×10-6	b		
4.3	2.65×10-5	a			1.76×10-5	a	1.33×10-5	a	8.39×10-6	b	3.89×10-6	b		
4.7	2.43×10-5	a			1.60×10-5	a	1.20×10-5	a	7.58×10-6	b	3.48×10-6	b		
5.1	2.24×10-5	a			1.47×10-5	a	1.10×10-5	a	6.91×10-6	b	3.15×10-6	b		
5.6	2.04×10-5	a			1.33×10-5	a	9.87×10-6	b	6.21×10-6	b	2.80×10-6	c		
6.2	1.84×10-5	a			1.19×10-5	a	8.80×10-6	b	5.53×10-6	b	2.47×10-6	c		
6.8	1.68×10-5	a			1.08×10-5	a	7.9.×10-6	b	4.98×10-6	b	2.20×10-6	c		
7.5	1.52×10-5	a			9.75×10-6	b	7.10×10-6	b	4.45×10-6	b	1.95×10-6	c		
8.2	1.39×10-5	a			8.87×10-6	b	6.43×10-6	b	4.02×10-6	b	1.74×10-6	c		
9.1	1.25×10-5	a			7.94×10-6	b	5.71×10-6	b	3.57×10-6	b	1.53×10-6	c		
10	1.14×10-5	a			7.18×10-6	b	5.14×10-6	b	3.21×10-6	b	1.36×10-6	c		
11	1.04×10-5	a			6.44×10-6	b	4.53×10-6	b	2.81×10-6	c	1.18×10-6	c		
12	9.51×10-6	b			5.84×10-6	b	4.04×10-6	b	2.49×10-6	c	1.04×10-6	c		
13	8.78×10-6	b			5.33×10-6	b	3.64×10-6	b	2.23×10-6	c	9.21×10-6	d		
15	7.61×10-6	b			4.53×10-6	b	3.01×10-6	b	1.82×10-6	c	7.44×10-6	d		
16	7.13×10-6	b			4.21×10-6	b	2.77×10-6	c	1.67×10-6	c	6.76×10-6	d		
18	6.34×10-6	b			3.68×10-6	b	2.37×10-6	c	1.41×10-6	c	5.67×10-6	d		
20	5.71×10-6	b			3.26×10-6	b	2.06×10-6	c	1.22×10-6	c	4.85×10-6	d		

<그림 5>의 수치표시 (2의 2)

	시간(1/H)당 위험한 고장의 평균확률과 해당 성능수준(PL)													
각 채널에 대한 $MTTF_d$ 년	Cat.B DC_{avg}=없음	PL	Cat.1 DC_{avg}=없음	PL	Cat.2 DC_{avg} =낮음	PL	Cat.2 DC_{avg} =중간	PL	Cat.3 DC_{avg} =낮음	PL	Cat.3 DC_{avg} =중간	PL	Cat.4 DC_{avg} =높음	PL
22	5.19×10-6	b			2.93×10-6	c	1.82×10-6	c	1.07×10-6	c	4.21×10-7	d		
24	4.76×10-6	b			2.65×10-6	c	1.62×10-6	c	9.47×10-7	d	3.70×10-7	d		
27	4.23×10-6	b			2.32×10-6	c	1.39×10-6	c	8.04×10-7	d	3.10×10-7	d		
30			3.80×10-6	b	2.06×10-6	c	1.21×10-6	c	6.94×10-7	d	2.65×10-7	d	9.54×10-8	e
33			3.46×10-6	b	1.85×10-6	c	1.06×10-6	c	5.94×10-7	d	2.30×10-7	d	8.57×10-8	e
36			3.17×10-6	b	1.67×10-6	c	9.39×10-7	d	5.16×10-7	d	2.01×10-7	d	7.77×10-8	e
39			2.93×10-6	c	1.53×10-6	c	8.40×10-7	d	4.53×10-7	d	1.78×10-7	d	7.11×10-8	e
43			2.65×10-6	c	1.37×10-6	c	7.34×10-7	d	3.87×10-7	d	1.54×10-7	d	6.37×10-8	e
47			2.43×10-6	c	1.24×10-6	c	6.49×10-7	d	3.35×10-7	d	1.34×10-7	d	5.76×10-8	e
51			2.24×10-6	c	1.13×10-6	c	5.80×10-7	d	2.93×10-7	d	1.19×10-7	d	5.26×10-8	e
56			2.04×10-6	c	1.02×10-6	c	5.10×10-7	d	2.52×10-7	d	1.03×10-7	d	4.73×10-8	e
62			1.84×10-6	c	9.06×10-7	d	4.43×10-7	d	2.13×10-7	d	8.84×10-8	e	4.22×10-8	e
68			1.68×10-6	c	8.17×10-7	d	3.90×10-7	d	1.84×10-7	d	7.68×10-8	e	3.80×10-8	e
75			1.52×10-6	c	7.31×10-7	d	3.40×10-7	d	1.57×10-7	d	6.62×10-8	e	3.41×10-8	e
82			1.39×10-6	c	6.61×10-7	d	3.01×10-7	d	1.35×10-7	d	5.79×10-8	e	3.08×10-8	e
91			1.25×10-6	c	5.88×10-7	d	2.61×10-7	d	1.14×10-7	d	4.94×10-8	e	2.74×10-8	e
100			1.14×10-6	c	5.28×10-7	d	2.29×10-7	d	1.01×10-7	d	4.29×10-8	e	2.47×10-8	e