KOSHA GUIDE
X - 77 - 2018

안전관련 시스템의 하드웨어 고장확률 계산에 관한 기술지침

2018. 11.

한국산업안전보건공단

안전보건기술지침의 개요

○ 작성자 : 서울과학기술대학교 류보혁

○ 제·개정 경과

- 2018년 10월 리스크분야 제정위원회 심의(제정)

○ 관련규격 및 자료

- IEC 61508-6 Edition 2.0 2010-04 Functional safety of electrical /electronic/programmable electronic safety related systems - Part 6 Annex B: Guidelines on the application of IEC 61508-2 and IEC 61508-3

○ 관련법규・규칙・고시 등

○ 기술지침의 적용 및 문의

- 이 기술지침에 대한 의견 또는 문의는 한국산업안전보건공단 홈페이지(www.kosha.or.kr)의 안전보건기술지침 소관 분야별 문의처 안내를 참고하시기 바랍니다.
- 동 지침 내에서 인용된 관련규격 및 자료, 법규 등에 관하여 최근 개정본이 있을 경우에는 해당 개정본의 내용을 참고하시기 바랍니다.

공표일자 : 2018년 11월 05일
제 정 자 : 한국산업안전보건공단 이사장

KOSHA GUIDE
X - 77 - 2018

안전관련 시스템의 하드웨어 고장확률 계산에 관한 기술지침

1. 목 적

이 지침은 산업안전보건기준에 관한 규칙 제327조(전자파에 의한 기계설비의 오작동 방지) 등에 따라, 사업장에서 설비, 공정제어 또는 안전장치를 위해 전기/전자/프로그램 가능형 전자장치 기반으로 구성된 안전관련 시스템의 하드웨어 고장확률 계산에 필요한 사항을 정함을 목적으로 한다.

2. 적용범위

(1) 이 지침은 전기/전자/프로그램 가능형 전자장치 기반으로 구성된 안전관련 시스템의 하드웨어의 고장확률을 계산하기 위한 방법 중 저요구 모드의 신뢰도 블록다이어그램(Reliability Block Diagram, 이하 “RBD” 라 한다) 방법론에 한하여 적용한다.

(2) 이 지침은 다음의 가이드를 인용 또는 보완하여 적용할 수 있다.

(가) X-77(안전관련 시스템의 공통원인고장의 영향 정량화에 관한 기술지침)

(나) E-149(제어시스템에서의 안전무결성등급(SIL) 결정에 관한 지침)

(다) M-191(안전제어시스템 설계를 위한 평균위험고장시간 계산지침)

(라) M-192(기계안전을 위한 제어시스템의 안전관련부품류 설계 기술지침)

3. 용어의 정의

(1) 이 지침에서 사용되는 용어의 정의는 다음과 같다.

(가)“전기/전자/프로그램 가능형 전자장치(Electric/Electronic/Programmable electronic devices)”라 함은 전기/전자/프로그램이 가능한 전자기술을 기반으로 한 장치를 말한다.

(나) “프로그램 가능형 전자장치(Programmable electronic devices, PED)”라 함은 하드웨어, 소프트웨어 및 입출력 장치로 구성된 컴퓨터 기술을 기반으로 한 전자장치를 말한다.

(다) “안전관련 시스템(Safety-related system)”이라 함은 운전설비의 안전상태를 유지하도록 안전기능을 수행하는 전기/전자/프로그램 가능형 시스템, 기타 다른 기술로 구성된 시스템 또는 외부의 리스크 감소 설비 등을 말한다. 이 지침에서는 “안전계장기능” 또는 “안전계장설비”를 말한다.

(라) “안전기능(Safety function)”이라 함은 안전계장기능, 또는 다른 기술적 안전(관련)시스템 또는 외부 리스크 저감설비에 의한 수행되는 기능으로 안전한 상태를 유지하거나 성취하기 위한 기능을 말한다.

(마) “안전계장기능(Safety instrumented function, SIF)”이라 함은 높은 안전무결성수준(safety integrity level, SIL)을 지닌 안전기능으로, 여러 가지의 하부시스템의 조합으로 구성되어 있는 것을 말한다.

(바) “하부시스템(Subsystem)”이라 함은 안전계장기능의 작동을 위한 시스템으로써 감지부, 논리기, 조작부 등으로 개별 채널과 이를 연결을 위한 전자인터페이스를 포함한 조합을 말한다.

(사) “채널(Channel)”이라 함은 안전계장기능의 하부시스템을 구성하는 감지부(sensors), 논리기(logic solver) 및 조작부(final elements) 중의 하나를 말한다.

(아) “안전계장설비(Safety instrumented system, SIS)”이라 함은 하나 또는 그 이상의 안전계장기능 및 관련 부속설비를 통합한 계장시스템으로 안전관련 시스템의 일종을 말하며, 운전조건을 벗어난 상태가 발생했을 때, 해당공정을 안전하게 정지시키거나, 리스크를 저감하기 위한 설비를 말한다.

(자) “안전무결성(Safety integrity)”이라 함은 안전(관련)시스템이 주어진 시간동안 모든 운전상태에서 요구되는 안전기능을 만족스럽게 수행할 수 있는 확률을 말한다.

(차) “요구시 고장확률(Probability Failure on Demand, PFD)이라 함은 안전관련 시스템 등의 하부시스템을 구성하는 요소 등과 같이 안전 기능 작동이 요구될 시점에 고장이 발생하여 작동이 되지 않을 수 있는 확률을 말한다.

(카) “위험감소분률(Risk Recuction Fraction, RRF)”이라 함은 요구시 고장확률의 역의 개념으로 정수로 나타내기 위한 수치를 말하며, 식은 1/PFD 이다.

(타) “안전무결성수준(Safety integrity level, SIL)”이라 함은 전기/전자/프로그램 가능형 전자장치로 구성된 안전관련 시스템에서, 안전기능의 안전무결성 요건을 <표 1> 과 같이 명시한 불연속의 수준(1~4)을 말한다.

<표 1> 안전관련 시스템의 안전무결성수준(SIL) 구분

SIL 요구수준	요구시 고장확률(PFD)	RRF=(1/PFD)
SIL 1	$10^{-2} \leq PFD \leq 10^{-1}$	$10 \leq RRF \leq 100$
SIL 2	$10^{-3} \leq PFD \leq 10^{-2}$	$100 \leq RRF \leq 1{,}000$
SIL 3	$10^{-4} \leq PFD \leq 10^{-3}$	$1000 \leq RRF \leq 10{,}000$
SIL 4	$10^{-5} \leq PFD \leq 10^{-4}$	$10{,}000 \leq RRF \leq 100{,}000$

(파) “신뢰도 블록다이어그램(Reliability block diagram, RBD)”이라 함은 설비의 전체 시스템의 신뢰도(또는 고장률)를 결정하기 위해 활용할 수 있도록 각 부품(요소)들과 그 연결 관계를 도식화하여 펼쳐 놓은 그림을 말한다.

(하) “공통원인고장(Common cause failure, CCF)”이라 함은 안전계장설비에 전원공급 중단과 같이 한가지의 고장원인이 설비 전체의 고장으로 이어지는 원인고장이나, 하부시스템의 채널 모두에 공통의 영향을 미치는 원인고장을 말한다. 이 지침에서는 채널에 공통의 영향을 미치는 원인고장에 한한다.

(거) “저요구 모드(Low demand mode)”라 함은 안전관련 시스템과 같이 이상이 발생이 할 때 작동하는 요소로, 작동이 가끔 일어나는 채널의 고장률(λ)로써 시간당 고장 횟수(회/h) 또는 연당 고장 횟수(회/year)로 표현하는 것을 말한다.

(너) “고요구 모드(High demand mode)”라 함은 공정제어관련 시스템과 같이 운전 중에 작동이 지속적으로 일어나는 채널의 고장률(λ)로써 시간당 고장 횟수(회/h)로 표현하는 것을 말한다.

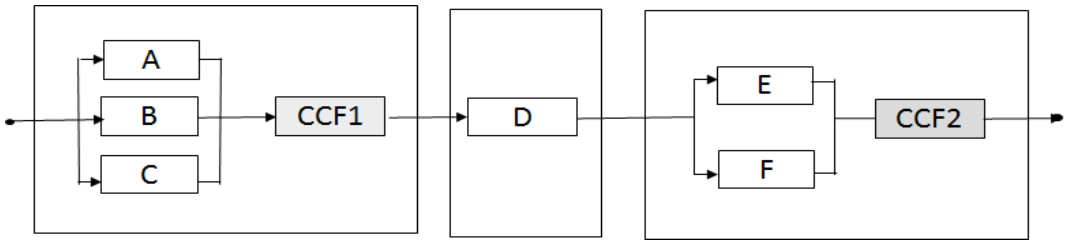
(댜) “안전고장분율(Safety Failure Fraction, SFF)”이라 함은 장치(부품)의 총고장률(λ) 중에 안전한 고장률(λ_S)과 위험한 검출 고장률(λ_{Dd})의 합의 분율을 말한다.

(2) 기타 이 지침에서 사용하는 용어의 정의는 특별한 규정이 있는 경우를 제외하고는 산업안전보건법, 같은 법 시행령, 같은 법 시행규칙, 산업안전보건기준에 관한 규칙에서 정하는 바에 의한다.

4. 고장 확률계산 시 고려사항

4.1 일반 사항

(1) 안전관련 시스템이 3 개의 감지부(A, B, C), 1 개의 논리기(D), 2개의 조작부(E, F), 및 공통요인고장(CCF)으로 안전 루프가 구성되어 있다고 가정하면, 이와 관련된 RBD는 <그림 1>과 같이 표현할 수 있다.



<그림 1> 전체 안전관련 시스템의 RBD의 예

(2) 5 개의 구성요소들의 고장률을 결합하면 해당 안전관련 시스템의 고장률을 구할 수 있다.

(3) 5 개 요소들을 최소 컷셋(minimal cut set)이라 한다.

(가) (A, B, C)는 3중 고장

(나) (E, F)는 2중 고장

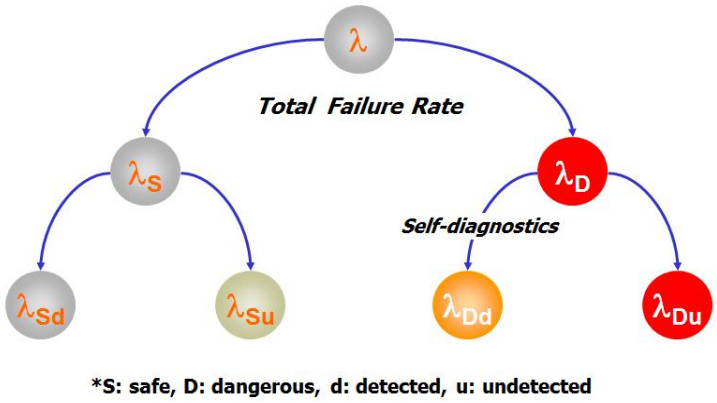
(다) (D), (CCF1), (CCF2)는 단일 고장

4.2 안전계장기능의 고장형태 분류

(1) 안전계장기능의 고장률(λ)은 고장의 형태에 따라 "안전한 고장률(safe failure rate, λ_S)"과 "위험한 고장률(dangerous failure rate, λ_D)"로 나눈다. 이를 <그림 2> 및 <표 2>와 같이 4가지로 분류하여 정의 할 수 있다.

(2) "안전한 고장률(λ_S)"은 고장이 나면 안전기능의 작동 시 이상을 줄 수 있으나, 안전관련 시스템의 안전무결성에 영향을 주지 않는 고장률이다.

(3) "위험한 고장률(λ_D)"은 고장이 날 경우 안전기능의 작동 수행에 이상을 줄 수 있는 고장률이다.



<그림 2> 안전계장기능의 고장형태 분류

(4) 고장 중에서는 "안전한 고장률(λ_S)"과 "위험한 고장률(λ_D)" 중에 "위험한 검출 고장률(λ_{Dd})"은 안전기능에 영향을 주지는 않는다. "위험한 미검출 고장률(λ_{Du})"만이 안전기능의 이상에 영향을 준다.

(5) 따라서 안전관련 시스템 및 안전계장기능의 요구시 고장 평균확률(PFD_{avg}) 계산 시에는 유일하게 "위험한 미검출 고장률(λ_{Du})"이 사용된다.

<표 2> 4 가지 고장형태의 분류

고장형태		정의 및 설명
안전한	검 출 (λ_{Sd})	요소(부품)가 고장이 나면, 궁극적으로 하부시스템에 안전한 상태(safe state)를 가져온다. 예, 에너지 방전 모듈 출력에서 출력이 발생할 경우 연결된 밸브가 잠김.
	미검출 (λ_{Sd})	요소(부품)가 고장이 났는데도 불구하고 기능이 지속된다. 예, 한 입력 모듈의 고장이 없으나 전방의 LED의 표시기가 고장상태임.
위험한	검출 (λ_{Dd})	요소(부품)가 안전기능을 수행할 수 없으나, 그 고장 상태를 이미 알고 있는 경우임.
	미검출 (λ_{Du})	요소(부품)가 안전기능을 수행할 수 없으며, 이 사실을 모르는 경우로서, 요구시 작동이 되지 않을 것임.

4.3 하부시스템 구조의 결정

(1) 안전관련 시스템의 하부시스템(subsystem)의 구조(architecture)는 KS C IEC 61508 part 2(2010)에서는 엄격하게 제한을 하고 있으며, "최소 하드웨어 고장허용치(Minimum Hardware Fault Tolerance, HFT)"를 요구한다.

(2) KS C IEC 61508 에서는 사용된 장치(부품)와 구조에 따라 최고로 높은 단계의 안전 무결성수준이 결정되므로 다음과 같이 3가지 조건을 요구한다.

(가) 하부시스템에 대한 구조적 제한(architectural constraints) ; 최소 하드웨어 고장 허용치(HFT) 평가

(나) 안전고장분율(Safe Failure Fraction, SFF) 계산 및 적용

(다) 요구시 고장 평균확률(PFD_{avg})

(3) 안전고장분율과 최소 하드웨어 고장허용치의 적용은 다음과 같이 수행한다.

(가) Type A는 구성된 모든 하위시스템 요소(부품)의 고장유형이 쉽고, 명확한 고장 데이터가 확보된 간단한 조작부 요소(부품)들(예, mechanical devices, simple electronic devices, isolator, solid-state relay 등)에 <표 3,a)> 와 같이 적용한다.

<표 3.a)> A형 요소(부품)의 최소 HFT

요소의 안전고장분율(SFF)*	HFT**		
	0	1	2
SFF<60 %	SIL 1	SIL 2	SIL 3
60 % ≤SFF<90 %	SIL 2	SIL 3	SIL 4
90 % ≤SFF<99 %	SIL 3	SIL 4	SIL 4
SFF ≧90 %	SIL 3	SIL 4	SIL 4

(나) Type B는 Type A의 이외의 것들로 sensor transmitter, logic solver 등 복잡하고, 전자 부품의 모든 것들에 <표 3, b)>와 같이 적용한다.

(다) 예를 들면 하나의 smart sensor(type B)는 안전한 고장분율(SFF)=91 %로 안전계장기능의 SIL 3 수준을 사용된다고 할 경우,

① 단계 1 : Type B 이므로, <표 3, b)>를 선택한다.

② 단계 2 : SFF의 구간 90 %≤SFF≤99 %를 선택한다.

③ 단계 3 : 목표 SIL 3를 찾으면 HFT = 1임을 알 수 있다.
④ 단계 4 : N+1(1+1)인 smart sensor는 2 개를 설치하여야 한다.

<표 3.b)> B형 요소(부품)의 최소 HFT

요소의 안전고장분율(SFF)*	HFT**		
	0	1	2
SFF<60 %	허용 불가	SIL 1	SIL 2
60 % ≤SFF<90 %	SIL 1	SIL 2	SIL 3
90 % ≤SFF<99 %	SIL 2	SIL 3	SIL 4
SFF ≧90 %	SIL 3	SIL 4	SIL 4

* SFF = (safe detected failure rate+ safe undetected failure rate +dangerous detected failure rate)/total failure rate
** HFT에서 N이란 N+1 개의 결합이 안전기능의 확보를 의미함.
*** source IEC 61508 part 2, table 2 and 3

(4) 안전계장기능의 안전무결성수준(SIL)을 결정할 경우 구조적 제약 평가결과에 따라 하위시스템의 각 요소(부품)의 가지고 있는 값 중 가장 낮은 수준으로 결정한다. 예를 들면, 하위시스템의 각 요소(부품)의 안전무결성수준이 SIL 4와 SIL 3 로 분포되어 있을 경우 최종 안전계장기능은 SIL 3로 결정한다.

4.4 안전관련 시스템의 평균 고장시간 산출

(1) 안전관련시스템은 저요구모드를 적용하여 요구시 고장평균확률($PFD_{avg.}$)을 계산한다.

(2) 요구시 고장 평균확률은 기간 [0, T]에서의 평균정지시간(Mean Down Time, 이하 “MDT” 라 한다)의 비율로 단순히 MDT(T)/T로 표현한다.

(3) 안전(관련) 시스템의 대부분은 고장확률이 매우 낮으므로, 동시에 2개의 최소 컷셋이 일어나는 고장확률은 무시한다.

(4) 따라서 각 컷셋의 MDT의 합이 보수적으로 전체 시스템의 MDT로 추산할 수 있다. <그림 1>의 불럭다이어그램에 대한 MDT는 식 (1)과 같이 추산할 수 있다.

$$MDT \approx MDT^{ABC} + MDT^{D} + MDT^{EF} \quad (1)$$

(5) 식 (1)를 시간 T로 나누면 식 (2)와 같이 요구시 고장 평균확률을 구할 수 있다.

$$PFD_{avg} \approx PFD_{avg}^{ABC} + PFD_{avg}^{D} + PFD_{avg}^{EF} \quad (2)$$

(6) 직렬의 경우 PFD_{avg} 계산은 값 1보다 아주 작은 수일 경우에는 보통 확률을 계산하는 것과 매우 유사하다.

(7) 그러나 (E, F) 요소와 같이 기능 실패(고장) 전에 요구되는 여러 건의 고장이 병렬인 경우에는 MDT^{EF}를 MDT^{E}, MDT^{F}에서 직접적으로 단순하게 계산할 없으며, (E, F) 요소의 MDT는 식 (3)과 같이 계산할 수 있다.

$$MDT^{EF} = \int_0^T PFD^{E}(t) PFD^{F}(t) dt \quad (3)$$

(8) 이에 따라 보통의 확률적 계산(더하기 및 곱하기)으로는 병렬의 경우 PFD_{avg} 계산을 단순하게 할 수 없으며, 정확한 확률값을 얻을 수 없다.

(9) 그러므로, 안전관련 시스템의 PFD_{avg} 는 전통적인 방법으로 여러개 요소의 $PFD_{avg.i}$ 로부터 계산할 수 없다.

(10) 안전관련 시스템의 PFD_{avg} 는 분석적인 방법 또는 Monte Carlo 방법론을 수행하여야 한다. 여기서는 전통적인 Boolean 기반의 RBD를 수행한다.

5. 하드웨어 고장률의 계산 방법

5.1 계산 시에 필요한 가정

다음의 가정을 근거로 한 후 계산을 수행한다.

(1) 시스템의 요구시 평균 고장확률은 10^{-1}이하 이거나 평균 고장빈도는 10^{-1}/년 이하이다.

(2) 각 요소(부품)들의 고장률은 시스템 수명 기간에는 일정하다.

(3) 감지부는 센서(들), voting, 및 입력모듈 등 다른 요소들로 구성되며, 이는 연결선으로 이어진다. 다만, <그림 3>과 같이 센서와 센서간에 신호는 연결되지 않는다.

(4) 논리기는 감지부로부터 신호를 받는 입력모듈과 연결되며, 조작부에 신호를 주는 출력모듈을 포함한 여러 요소(들)로 구성되어 있다.

(5) 조작부는 논리기에서 받은 신호를 최종 수행(actuator 등)하는 요소(들)로 구성되어 있으며, 이는 연결선으로 이어진다.

(6) 하드웨어 고장률은 계산식이 사용되며, 기존 표의 값은 하부시스템이 단순 채널인 경우 사용한다.(예, 2oo3 voting 감지부가 사용된다면, 하나의 센서를 위해 고장률은 표의 값을 사용되고, 2oo3의 voting효과는 별도로 분리하여 계산한다.)

(7) voting 그룹이 있는 채널들은 동일한 고장률을 가지며, 자가진단 기능을 갖는다.

(8) 하부시스템 채널의 전체 하드웨어 고장률(λ)은 위험한 고장률(λ_D)과 안전한 고장률(λ_S)의 합이다. 이들 고장률은 동일하다고 가정한다.

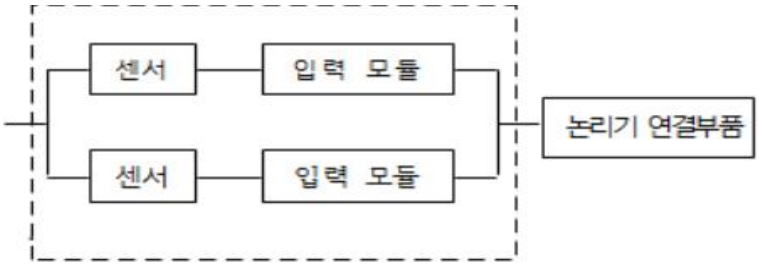
(9) 각각의 안전기능을 위해 완전한 보증시험(proof test) 및 보수가 이루어진다. (즉, 검출되지 않고 남아 있는 모든 고장들은 보증시험 시에 검출됨)

(10) 보증시험의 주기는 평균보수시간(Mean Repair Time, 보통 8 시간으로 가정, 이하 “MRT”라 한다)에 비해 상당히 긴 기간으로 6 개월 이상이다.

(11) 하부시스템별로 보증시험과 MRT를 가진다.

(12) 자기진단 기능을 갖는 하부시스템인 경우 평균복구시간(Mean Time To Restoration, MTTR)에는 고장 검출과 보수시간이 포함된다.

(13) 채널이라는 용어는 <그림 3>과 같이 안전계장기능의 요소로서 대체로 감지부, 논리기 및 조작부 등 하부시스템 중의 하나이다.



<그림 3> 2 개의 센서로 구성된 안전계장기능의 감지부 구성의 예

5.2 요구시 고장 평균확률 계산

5.2.1 계산 과정

(1) 안전계장기능의 구성 요소 중 1개만 고장이 나면, 안전기능이 완전히 고장이 난다.

(2) 안전계장기능의 하부시스템 요소(부품)의 미검출 고장을 계산할 수 있기 때문에 전체 안전계장기능의 수행하지 못할 가능성(확률)은 계산할 수 있다.

(3) 따라서 전체 안전계장기능이 감지부, 논리기 및 조작부로 <그림 4>와 같이 하부시스템으로 구성되어 있다면, 하부시스템 구성 개별 요소의 요구시 고장 평균확률(PFDavg)로부터 전체 $PFD_{SYS,avg}$ 는 식 (4)과 같이 각 요소의 요구시 고장확률을 더해서 계산한다.

$$PFD_{SYS,avg} = PFD_S + PFD_L + PFD_{FE} \quad (4)$$

여기서

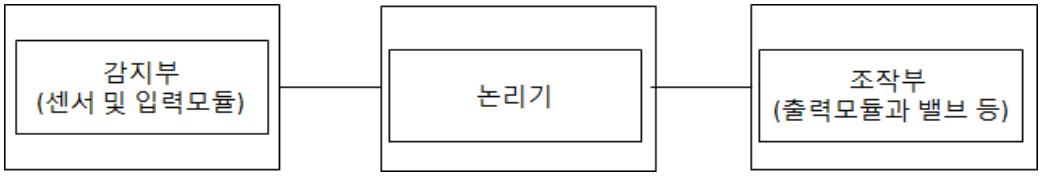
$PFD_{SYS,avg}$: 안전관련 시스템을 위한 안전기능의 요구시 고장 평균확률

PFD_S : 감지부를 위한 요구시 고장 평균확률

PFD_L : 논리기를 위한 요구시 고장 평균확률

PFD_{FE} : 조작부를 위한 요구시 고장 평균확률

(4) 안전계장기능의 요구시 고장확률(PFD) 계산에 필요한 약어 및 정의는 <별표 1> 과 같다



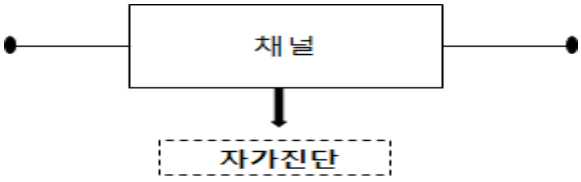
<그림 4> 안전계장기능의 하부시스템 구성

5.2.2 각 구조 및 연결구성에 따른 계산

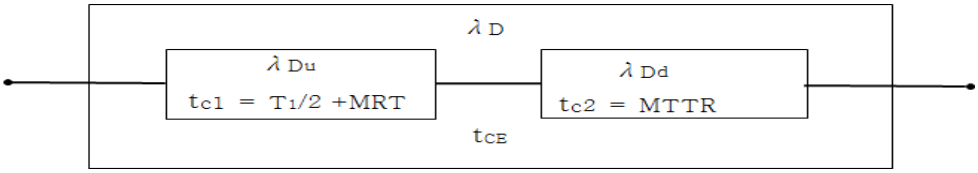
5.2.2.1 1 out of 1 voting 기능

(1) 안전계장기능의 하부시스템은 <그림 5> 및 <그림 6>의 불럭다이어그램과 같이 1개의 채널로 구성되어 있으며, 채널의 "위험한 고장률(λ_D)"이면 안전기능의 상실하는 경우이다.

(2) 1 개 채널을 위한 위험한 고장률은 식 (5) 와 같다.



<그림 5> 1oo1 물리적 불럭다이어그램



<그림 6> 1oo1 신뢰도 불럭다이어그램

$$\lambda_D = \lambda_{Dd} + \lambda_{Du} \quad (5)$$

(3) <그림 6>은 2 개의 요소들의 결합을 고려한 것이다. 1 개는 미검출된 고장의 결과로 위험한 미검출 고장률(λ_{Du})이며, 다른 1 개는 검출된 고장의 결과로 위험한 검출 고장률(λ_{Dd})이다.

(4) 양 요소의 개별 정지시간 t_{c1}과 t_{c2}을 더한 평균정지시간 t_{CE}에 상당하는 기간으로 계산할 수 있다. 이는 식 (6)과 같이 각 요소별 채널 고장확률의 비율로 나타낸다.

$$t_{CE} = \frac{\lambda_{Du}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{Dd}}{\lambda_D} MTTR \quad (6)$$

(4) 안전계장기능의 모든 하부시스템에서 위험한 검출 고장률(λ_{Dd}) 과 위험한 미검출 고장률(λ_{Du})은 식 (7) 과 같다.

$$\lambda_{Du} = \lambda_D(1-DC);\ \lambda_{Dd} = \lambda_D DC \quad (7)$$

(5) 위험한 고장의 결과로부터 정지시간 t_{CE}기간의 요구시 고장확률은 식 (8)과 같다.

$$PFD = 1-e^{-t_{CE}\lambda_D} \approx \lambda_D t_{CE} \quad \text{여기서} \quad \lambda_D t_{CE} \ll 1 \quad (8)$$

(6) 따라서, 1oo1 하부시스템 구성의 요구시 고장 평균확률(PFD_G)은 식 (9) 와 같이 계산한다.

$$PFD_G = (\lambda_{Dd} + \lambda_{Du})t_{CE} \quad (9)$$

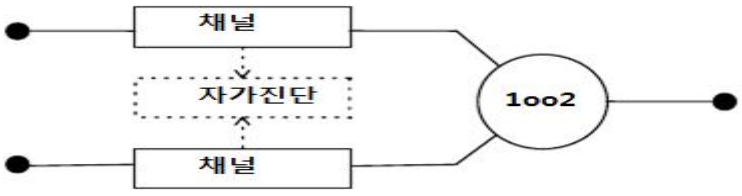
5.2.2.2 1 out of 2 voting 기능

(1) 안전계장기능의 하부시스템이 <그림 7> 및 <그림 8>의 불럭다이어그램과 같이 2개의 채널이 병렬로 구성되어 있으며, 각각 안전기능을 수행할 수 있다.

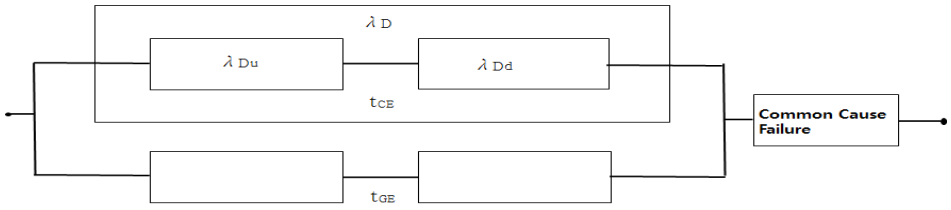
(2) 요구 시 안전기능이 작동하지 않으려면, 안전기능이 요구 이전에 양 채널에서 위험한 고장이 있어야 한다.

(3) 자가진단시험은 발견된 결함만 보고할 뿐이며, 어떤 출력상태의 변화나 출력 voting의 변화가 없다고 가정한다.

(4) 1oo2는 주로 조작부의 솔레노이드 밸브 연결에 활용한다.



<그림 7> 1oo2 물리적 불럭다이어그램



<그림 8> 1oo2 신뢰도 불럭다이어그램

(5) 하부시스템의 정지시간에 상당하는 t_{GE} 기간은 식 (10)과 같이 계산할 수 있다.

$$t_{GE} = \frac{\lambda_{Du}}{\lambda_D}\left(\frac{T_1}{3} + MRT\right) + \frac{\lambda_{Dd}}{\lambda_D} MTTR \quad (10)$$

(6) 1oo2 하부시스템 구성의 요구시 고장 평균확률(PFD_G)은 식 (11)과 같이 계산한다.

$$PFD_G = 2[(1-\beta_D)\lambda_{Dd} + (1-\beta)\lambda_{Du})]^2 t_{CE} t_{GE} + \beta_D \lambda_{Dd} MTTR + \beta\lambda_{Du}\left(\frac{T_1}{2} + MRT\right) \quad (11)$$

5.2.2.3 2 out of 2 voting 기능

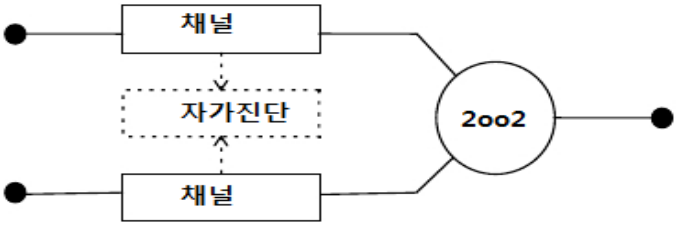
(1) 안전계장기능의 하부시스템이 하부시스템이 <그림 9>및 <그림 10>의 불럭다이어그램과 같이 2개의 채널이 병렬로 구성되어 있다.

(2) 이 경우 2 개의 안전기능의 작동이 요구되며, 동시에 안전기능이 작동된다.

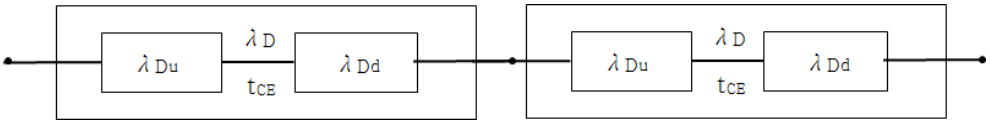
(3) 자가진단시험은 발견된 결함만 보고할 뿐이며, 어떤 출력상태의 변화나 출력 voting의 변화가 없다고 가정한다.

(4) 2oo2 하부시스템 구성의 요구시 고장 평균확률(PFD_G)은 식 (2-22)와 같이 계산되며, 1oo1의 2배에 해당한다.

(5) 대부분 안전무결성수준(SIL) 3 이상을 요구할 경우, 조작부의 솔레노이드 밸브 연결에 활용하며, 감지부를 2oo2로 구성할 경우에는 오작동 등 잘못된 고장 확률을 줄일 수 있다.



<그림 9> 2oo2 물리적 불럭다이어그램



<그림 10> 2oo2 신뢰도 불럭다이어그램

(6) 2oo2 하부시스템 구성의 요구시 고장 평균확률(PFD_G)은 식 (12)와 같이 계산되며, 1oo1의 2배에 해당한다.

$$PFD_G = 2\lambda_D t_{CE} \quad (12)$$

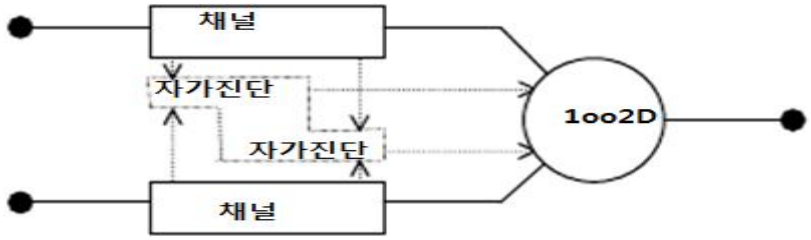
5.2.2.4 1 out of 2D voting 기능

(1) 안전계장기능의 하부시스템이 <그림 11> 및 <그림 12>의 불럭다이어그램과 같이 2개의 채널이 병렬로 구성되어 있다.

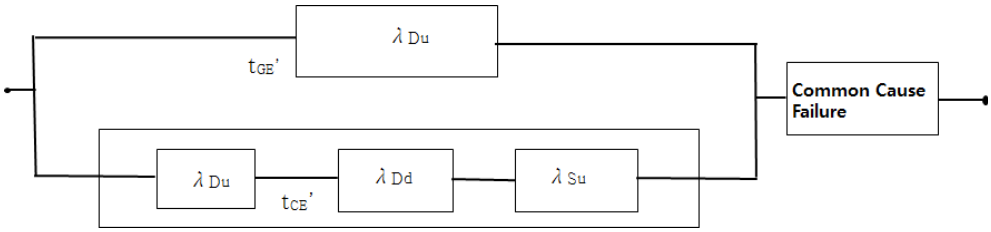
(2) 정상 작동 중에는 양 채널이 동시에 발생하도록 안전기능을 요구한다. 추가로, 만약 어느 한쪽채널의 자가진단시험에서 결함이 발견되면, 출력 voting은 다른 채널에 주어진 모든 상태로 전체가 출력된다.

(3) 자가진단시험에서 양 채널 모두에서 결함이 발견되거나 한쪽 채널에서 할당의 불일치가 발견된다면, 출력은 안전한 상태이다.

(4) 채널간 불일치를 검출하기 위해, 각각 채널은 독립적인 방법을 통해 다른 채널의 상태를 결정할 수 있다.



<그림 11> 1oo2D 물리적 불럭다이어그램



<그림 12> 1oo2D 신뢰도 불럭다이어그램

(5) 각각의 안전한 검출 고장률(λ_{Sd})는 식 (13) 과 같이 구한다.

$$\lambda_{Sd} = \lambda_S DC \tag{13}$$

(6) 하부시스템의 정지시간에 상당하는 t'_{CE} 및 t'_{GE} 기간은 각각 식 (14) 및 식 (15) 과 같이 계산할 수 있다.

$$t'_{CE} = \frac{(\lambda_{Sd} + \lambda_{Dd})MTTR + \left(\frac{T_1}{2} + MRT\right)\lambda_{Du}}{(\lambda_{Sd} + \lambda_{Dd}) + \lambda_{Du}} \tag{14}$$

$$t'_{GE} = \frac{T1}{3} + MRT \tag{15}$$

(7) 1oo2D 하부시스템 구성의 요구시 고장 평균확률(PFD_G)은 식 (16)과 같이 계산한다.

$$PFD_G = 2[(1-\beta)\lambda_{Dd} + [(1-\beta)\lambda_{Du} + (1-\beta_D)\lambda_{Dd} + \lambda_{Sd}]t'_{CE}t'_{GE} + 2(1-k)\lambda_{Dd}t'_{CE} + \beta\lambda_{Du}\left(\frac{T_1}{2} + MRT\right) \tag{16}$$

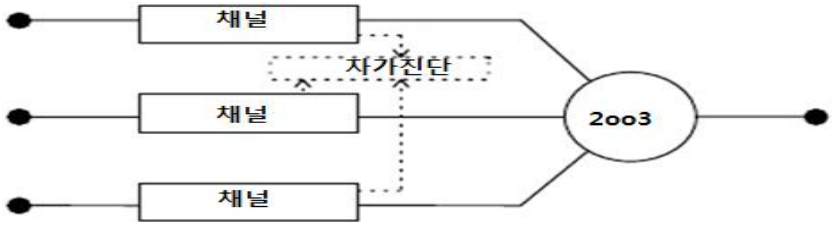
5.2.2.5 2 out of 3 voting 기능

(1) 안전계장기능의 하부시스템이 <그림 13>및 <그림 14>의 불럭다이어그램과 같이 3개의 채널이 병렬로 구성되어 있으며, 통합 출력신호로 구성되어 있다.

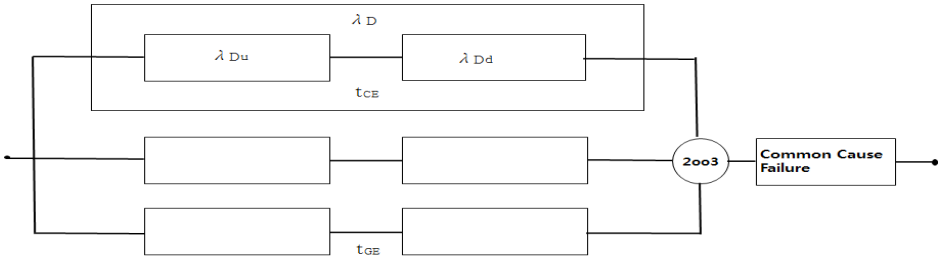
(2) 만약 1개 채널에 다른 결과(검출, 신호)를 가져와도 다른 2개의 채널의 동의하지 않으면 출력상태의 변화는 없다.

(3) 자가진단시험은 발견된 결함만 보고할 뿐이며, 어떤 출력상태의 변화나 출력 voting의 변화가 없다고 가정한다.

(4) 2oo3 연결은 대부분 안전무결성수준(SIL) 3 이상을 요구할 경우, 감지부 또는 논리기에 활용한다.



<그림 13> 2oo3 물리적 불럭다이어그램



<그림 14> 2oo3 신뢰도 불럭다이어그램

(5) 식 (17)과 같이 요구시 고장 평균확률(PFD_G)를 계산한다.

$$PFD_G = 6[(1-\beta_D)\lambda_{Dd} + (1-\beta)\lambda_{Du})]^2 t_{CE} t_{GE} + \beta_D \lambda_{Dd} MTTR + \beta \lambda_{Du}\left(\frac{T_1}{2} + MRT\right) \quad (17)$$

5.2.2.6 1 out of 3 voting 기능

(1) 안전계장기능의 하부시스템이 3 개 채널이 병렬로 구성되어 있으며, 1개의 voting으로 출력 신호가 있다. 1oo3의 불럭다이어그램은 2oo3과 동일하나 출력 voting만 1 개이다.

(2) 자가진단시험은 발견된 결함만 보고할 뿐이며, 어떤 출력상태의 변화나 출력 voting의 변화가 없다고 가정한다.

(3) 하부시스템의 정지시간에 상당하는 t_{CE} 는 식(6)과 같고, t_{GE} 는 식 (10)과 같으며, t_{G2E}는 식 (18)과 같이 계산한다.

$$t_{GE} = \frac{\lambda_{Du}}{\lambda_D}\left(\frac{T_1}{4} + MRT\right) + \frac{\lambda_{Dd}}{\lambda_D} MTTR \qquad (18)$$

(4) 1oo3 하부시스템 구성의 요구시 고장 평균확률(PFD_G)은 식 (19)과 같이 계산한다.

$$PFD_G = 6[(1-\beta_D)\lambda_{Dd} + (1-\beta)\lambda_{Du})]^3 t_{CE} t_{GE} t_{G2E} + \beta_D \lambda_{Dd} MTTR + \beta\lambda_{Du}\left(\frac{T_1}{2} + MRT\right) \qquad (19)$$

5.2.3 간단한 계산식을 활용한 요구시 고장확률 계산

(1) 산업현장에서는 안전계장기능 제조자나 공급자의 요구사항에 따라, 정기적으로 작동시험(Manual test)을 실시한다면, 고장률(λ) 중에 위험한 검출 고장률(λ_{Dd})은 문제가 되지 않는다.

<표 4> 간단한 요구시 고장 평균확률 계산식

voting	PFD_{avg} 계산식
1oo1	$\lambda_{Du} \times (\frac{T_I}{2})$
1oo2	$\frac{1}{3}[(\lambda_{Du})^2 \times (T_I)^2]$
2oo2	$\lambda_{Du} \times T_I$
2oo3	$(\lambda_{Du})^2 \times (T_I)^2$

* T_I = Manual test interval
λ_{Du} = Dangerous undetected failures

(2) 따라서 요구시 고장 평균확률(PFD_{avg})을 계산 시에는 위험한 미검출 고장률(λ_{Du})에 근거로 하여 <표 4>과 같이 생략된 간단한 식에 의해 계산할 수 있다.

5.2.4 표를 활용한 요구시 고장 평균확률값 계산

(1) <별표 2>, <별표 3> 및 <별표 4> 과 같이 하부시스템 채널의 1oo1, 1oo2, 2oo2, 1oo2D, 2oo3 및 1oo3 voting 구조별로 보증시험 주기 6 개월, 1년 및 2 년에 따라 계산한 값을 표로 나타내었다.

(2) 각 별표에서 계산값은 개별 고장 후 평균복구시간(MTTR)을 8 시간으로 가정하였다. 고장률은 위험한 고장률(λ_D)를 기준으로 하여, 0.5E-07에서 2.5E-05까지 6단계로 구분하여 값을 나타냈다.

(3) 각 별표에는 구조 및 voting(예, 2oo3), 각 채널별 자가진단범위(예, 60 %), 각 채널별 위험한 고장률(λ_D)(예, 2.5E-06) 및 공통원인고장(β, β_D)(각각 2%, 1 %)를 각각 구분하여 계산값으로 나타내었다.

5.3. 안전계장기능에 대한 안전무결성수준(SIL) 충족 검증

5.3.1 안전계장기능 구성의 가정

(1) 안전계장기능(시스템)은 안전무결성수준(SIL) 2 수준으로 고려한다.

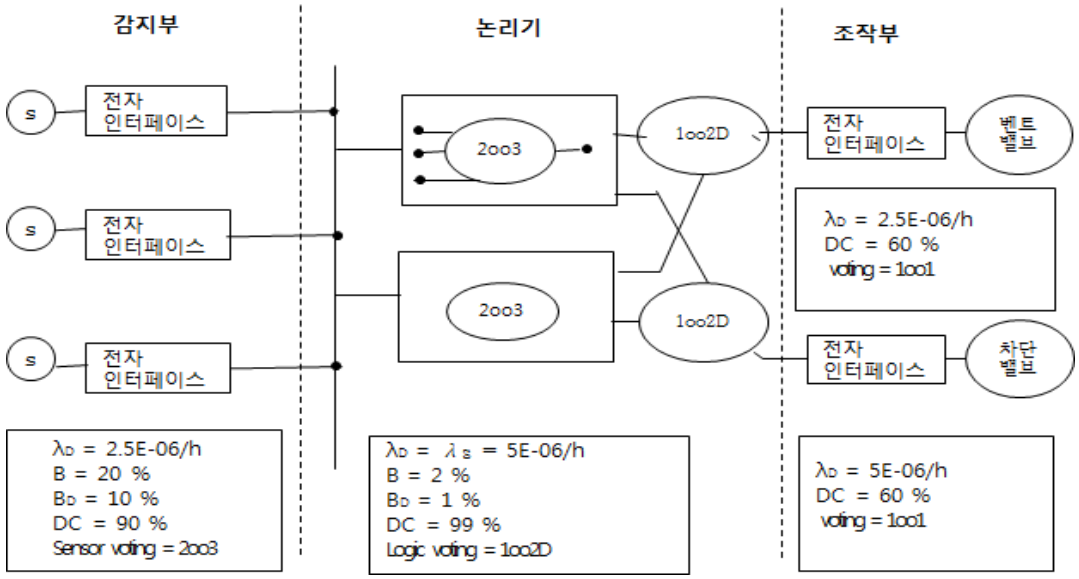
(2) 안전계장기능은 감지부, 논리기 및 조작부로 구성되어 있고, voting은 다음과 같다.

(가) 감지부는 3개의 아날로그 압력센서를 1그룹으로 구성되고, 1oo3 voting으로 연결된다.

(나) 논리기는 PE 시스템으로 자가진단 및 중복성 1oo2D으로 구성되어 있다.

(다) 조작부는 1 개의 차단밸브와 1 개의 벤트밸브가 설치되어 있으며, 안전기능을 성취하려면 차단밸브와 벤트밸브가 동시에 작동되어야 한다.

(3) 하부시스템의 구성, voting 및 설명은 <그림 15> 와 같다.



<그림 15> 안전계장기능의 하부시스템 구성의 예

(4) 요구시 고장 평균확률 계산을 위해서는 보증시험 주기는 1년으로 가정한다.

5.3.2 하부시스템의 안전무결성수준 검증 방법

5.3.2.1 하부시스템의 요구시 고장 평균확률 계산

(1) 감지부에 대한 요구시 고장 평균확률(PFD_S)은 <별표 3> 로부터 2.3E-04 임을 찾을 수 있다.

(2) 논리기에 대한 요구시 고장 평균확률(PFD_L)은 <별표 3> 로부터 4.8E-06 임을 찾을 수 있다.

(3) 조작부에 대한 요구시 고장 평균확률(PFD_{FE})은 <별표 3> 로부터 벤트밸브는4.4E-03, 차단밸브는 8.8E-03 임을 찾을 수 있다. 따라서 이를 더하면, 1.3E-02 이다.

(4) 하부시스템의 안전계장기능의 요구시 고장 평균확률(PFD_{SYS})는 각각의 안전기능의 요구시 고장 평균확률을 더하면 되므로, 이를 더하면 1.3E-02 이다.

(5) 1.3E-02는 안전무결성수준(SIL) 1에 해당하므로, 안전무결성수준 2를 충족하지 못함을 알 수 있다.

5.3.2.2 하부시스템의 안전기능 보강

(1) 보증시험 주기를 6개월로 단축하면, 다음과 같이 각각의 요구시 고장 평균확 률은 개선이 된다.

(가) 감지부에 대한 요구시 고장 평균확률(PFD_S)은 <별표 2> 로부터 1.1E-04 임을 찾을 수 있다.

(나) 논리기에 대한 요구시 고장 평균확률(PFD_L)은 <별표 2> 로부터 2.6E-06 임을 찾을 수 있다.

(다) 조작부에 대한 요구시 고장 평균확률(PFD_{FE})은 <별표 2> 로부터 벤트밸브는 2.2E-03, 차단밸브는 4.4E-03 임을 확인할 수 있다. 따라서 이를 더하면, 6.6E-03 이다.

(라) 하부시스템의 안전계장기능의 요구시 고장 평균확률(PFD_{SYS})은 각각의 안전기능의 요구시 고장 평균확률을 더하면 되므로, 이를 더하면 6.7E-03 이다.

(마) 6.7E-03은 안전무결성수준(SIL) 2에 해당하므로, 안전무결성수준 2를 충족한다.

(2) 조작부의 차단밸브의 1oo1 voting을 중복성을 추가하여 1oo2로 보강하고, β = 10 %, β_D는 5 % 로 가정한다. 이와 같이 보강할 경우 다음과 같이 각각의 요구시 고장 평균확률은 개선이 된다.

(가) 조작부의 차단밸브의 요구시 고장 평균확률(PFD_{FE})은 <별표 3> 로부터 9.7E-04 임을 찾을 수 있다. 따라서 이를 더하면, 5.4E-03 이다.

(나) 하부시스템의 안전계장기능의 요구시 고장 평균확률(PFD_{SYS})은 각각의 안전기능의 요구시 고장 평균확률을 더하면 되므로, 이를 더하면 5.6E-03 이다.

(다) 5.6E-03은 안전무결성수준(SIL) 2에 해당하므로, 안전무결성수준 2를 충족한다.

<별표 1> 안전계장기능의 요구시 고장확률 계산에 필요한 용어의 정의

약어	용어(단위)	사용범위
T_1	보증시험(Proof-test) 주기(hour, month, year)	1개월(730 h)[1] 6개월(2,190 h)[1] 1년(87,60h)[2], 2년(17,520)[2]
MTTR /MRT	평균복구시간(Mean time to restoration)(hour) 평균보수시간(Mean repair time(hour)	8 시간=MRT 위험 고장이 검출되는 시간을 가정한 것으로, 자동 검출은 MRT에 비해 아주 적은 시간임
DC	자가진단범위(공식에서 분률(%)로 표현함).	0 %, 60 %, 90 %, 99 %
β	공통원인 고장의 미검출 고장의 분률 (공식에서 분률(%)로 표현함) (가정 $\beta = 2\times\beta_D$)	2 %, 10 %, 20 %
β_D	공통원인 고장의 분률로써 자가진단 시험에 의해 검출되는 고장(공식에서 분률(%)로 표현함)(가정 $\beta = 2\times\beta_D$)	1 %, 5 %, 10 %
PFD_G	voting된 채널 그룹의 요구시 고장 평균확률 (만약 하부시스템이 감지부, 논리기 및 조작부 단지 1 개로 voting 되어 있다면, PFD_G 는 PFD_S , PFD_L, PFD_{FE} 와 같다.	
PFD_S	감지부 하부시스템의 요구시 고장 평균확률	
PFD_L	논리기 하부시스템의 요구시 고장 평균확률	
PFD_{FE}	조작부 하부시스템의 요구시 고장 평균확률	
PFD_{sys}	E/E/PE 등 안전관련시스템을 위한 안전기능의 요구시 고장 평균확률	
λ	하부시스템내 채널의 총 고장률(시간당)	
λ_D	하부시스템내 채널의 위험한 고장률(시간당) 위험한 고장률(λ_D)은 0.5λ로 가정한다.(위험한 고장 50%, 안전한 고장 50%)	0.05E-06,0.25E-06 0.5E-06, 2.5E-06 5E-06, 25E-06
λ_{Dd}	하부시스템내 채널의 검출된 위험한 고장률(시간당)	
λ_{Du}	하부시스템내 채널의 미검출된 위험한 고장률(시간당)	
λs_u	하부시스템내 채널의 검출된 안전한 고장률(시간당)	
t_{CE}	1oo1, 1oo2, 2oo2 및 2oo3 구조를 위한 동등한 채널의 평균정지시간(시간 단위)	
t_{GE}	1oo2 및 2oo3 구조를 위한 동등한 voting 그룹의 평균정지시간(시간 단위)	
K	1oo2D 시스템에서 자동시험회로의 성공분률	

<별표 2> 6 개월의 보증시험주기와 8 시간 평균복구시간을 위한 요구시 고장평균확률

구성	DC	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β =2% β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β =2% β_D= 1 %	β = 10 % β_D= 5 %	β = 20 % β_D = 10 %	β =2% β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (비고 2 참조)	0%	1,1E-04			5,5E-04			1,1E-03		
	60 %	4,4E-05			2,2E-04			4,4E-04		
	90 %	1,1E-05			5,7E-05			1,1E-04		
	99 %	1,5E-06			7,5E-06			1,5E-05		
1oo2	0%	2,2E-06	1,1E-05	2,2E-05	1,1E-05	5,5E-05	1,1E-04	2,4E-05	1,1E-04	2,2E-04
	60 %	8,8E-07	4,4E-06	8,8E-06	4,5E-06	2,2E-05	4,4E-05	9,1E-06	4,4E-05	8,8E-05
	90 %	2,2E-07	1,1E-06	2,2E-06	1,1E-06	5,6E-06	1,1E-05	2,3E-06	1,1E-05	2,2E-05
	99 %	2,6E-08	1,3E-07	2,6E-07	1,3E-07	6,5E-07	1,3E-06	2,6E-07	1,3E-06	2,6E-06
2oo2 (비고 2 참조)	0%	2,2E-04			1,1E-03			2,2E-03		
	60 %	8,8E-05			4,4E-04			8,8E-04		
	90 %	2,3E-05			1,1E-04			2,3E-04		
	99 %	3,0E-06			1,5E-05			3,0E-05		
1oo2D (비고 3 참조)	0%	2,2E-06	1,1E-05	2,2E-05	1,1E-05	5,5E-05	1,1E-04	2,4E-05	1,1E-04	2,2E-04
	60 %	8,8E-07	4,4E-06	8,8E-06	4,4E-06	2,2E-05	4,7E-05	8,9E-05	4,4E-05	8,8E-05
	90 %	2,2E-07	1,1E-06	2,2E-06	1,1E-06	5,6E-06	1,1E-05	2,2E-06	1,1E-05	2,2E-05
	99 %	2,6E-08	1,3E-07	2,6E-07	1,3E-07	6,5E-07	1,3E-06	2,6E-07	1,3E-06	2,6E-06
2oo3	0%	2,2E-06	1,1E-05	2,2E-05	1,2E-05	5,6E-05	1,1E-04	2,7E-05	1,1E-04	2,2E-04
	60 %	8,9E-07	4,4E-06	8,8E-06	4,6E-06	2,2E-05	4,4E-05	9,6E-06	4,5E-05	8,9E-05
	90 %	2,2E-07	1,1E-06	2,2E-06	1,1E-06	5,6E-06	1,1E-05	2,3E-06	1,1E-05	2,2E-05
	99 %	2,6E-08	1,3E-07	2,6E-07	1,3E-07	6,5E-07	1,3E-06	2,6E-07	1,3E-06	2,6E-06
1oo3	0%	2,2E-06	1,1E-05	2,2E-05	1,1E-05	5,5E-05	1,1E-04	2,2E-05	1,1E-04	2,2E-04
	60 %	8,8E-07	4,4E-06	8,8E-06	4,4E-06	2,2E-05	4,4E-05	8,8E-06	4,4E-05	8,8E-05
	90 %	2,2E-07	1,1E-06	2,2E-06	1,1E-06	5,6E-06	1,1E-05	2,2E-06	1,1E-05	2,2E-05
	99 %	2,6E-08	1,3E-07	2,6E-07	1,3E-07	6,5E-07	1,3E-06	2,6E-07	1,3E-06	2,6E-06

구성	DC	λ_D = 2,5E-06			λ_D = 0,5E-05			λ_D = 2,5E-05		
		β =2% β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β =2% β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β =2% β_D = 1 %	β = 10 % β_D= 5 %	β = 20 % β_D = 10 %
1oo1 (비고 2 참조)	0%	5,5E-03			1,1E-02			5,5E-02		
	60 %	**2,2E-03**			**4,4E-03**			2,2E-02		
	90 %	5,7E-04			1,1E-03			5,7E-03		
	99 %	7,5E-05			1,5E-04			7,5E-04		
1oo2	0%	1,5E-04	5,8E-04	1,1E-03	3,7E-04	1,2E-03	2,3E-03	5,0E-03	8,8E-03	1,4E-02
	60 %	5,0E-05	2,3E-04	4,5E-04	1,1E-04	4,6E-04	9,0E-04	1,1E-03	2,8E-03	4,9E-03
	90 %	1,2E-05	5,6E-05	1,1E-04	2,4E-05	1,1E-04	2,2E-04	1,5E-04	6,0E-04	1,2E-03
	99 %	1,3E-06	6,5E-06	1,3E-05	2,6E-06	1,3E-05	2,6E-05	1,4E-05	6,6E-05	1,3E-04
2oo2 (비고 2 참조)	0%	1,1E-02			2,2E-02			>1E-01		
	60 %	4,4E-03			8,8E-03			4,4E-02		
	90 %	1,1E-03			2,3E-03			1,1E-02		
	99 %	1,5E-04			3,0E-04			1,5E-03		
1oo2D (비고 3 참조)	0%	1,5E-04	5,8E-04	1,1E-03	3,7E-04	1,2E-03	2,3E-03	5,0E-03	8,8E-03	1,4E-02
	60 %	4,6E-05	2,2E-04	4,4E-04	9,5E-05	4,5E-04	8,9E-04	6,0E-04	2,3E-03	4,5E-03
	90 %	1,1E-05	5,6E-05	1,1E-04	2,2E-05	1,1E-04	2,2E-04	1,1E-04	5,6E-04	1,1E-03
	99 %	1,3E-06	6,5E-06	1,3E-05	**2,6E-06**	1,3E-05	2,6E-05	1,3E-05	6,5E-05	1,3E-04
2oo3	0%	2,3E-04	6,5E-04	1,2E-03	6,8E-04	1,5E-03	2,5E-03	1,3E-02	1,5E-02	1,9E-02
	60 %	6,3E-05	2,4E-04	4,6E-04	1,6E-04	5,1E-04	9,4E-04	2,3E-03	3,9E-03	5,9E-03
	90 %	1,2E-05	5,7E-05	**1,1E-04**	2,7E-05	1,2E-04	2,3E-04	2,4E-04	6,8E-04	1,2E-03
	99 %	1,3E-06	6,5E-06	1,3E-05	2,7E-06	1,3E-05	2,6E-05	1,5E-05	6,7E-05	1,3E-04
1oo3	0%	1,1E-04	5,5E-04	1,1E-03	2,2E-04	1,1E-03	2,2E-03	1,4E-03	5,7E-03	1,1E-02
	60 %	4,4E-05	2,2E-04	4,4E-04	8,8E-05	4,4E-04	8,8E-04	4,6E-04	2,2E-03	4,4E-03
	90 %	1,1E-05	5,6E-05	1,1E-04	2,2E-05	1,1E-04	2,2E-04	1,1E-04	5,6E-04	1,1E-03
	99 %	1,3E-06	6,5E-06	1,3E-05	2,6E-06	1,3E-05	2,6E-05	1,3E-05	6,5E-05	1,3E-04

비고 1 이 표는 PFD 값의 예를 나타낸다. 이 값은 각 등식에 따라 계산된다.
비고2 이 표는 $\beta = 2\times \beta D$ 를 가정한다. 1oo1, 1oo2 는 β 와 βD T의 값은 평균 고장확률에 영향을 미치지 않는다.
비고 3 안전한 고장율은 위험한 고장율과 K =0.98과 동등하다고 가정한다.

* source IEC 61508 part 6 Annex B Table B.2

<별표 3> 1년의 보증시험주기와 8 시간 평균복구시간을 위한 요구시 고장평균확률

구성	DC	λ D = 0,5E-07			λ D = 2,5E-07			λ D = 0,5E-06		
		β =2% βD = 1 %	β = 10 % βD = 5 %	β = 20 % βD = 10 %	β =2% βD = 1 %	β = 10 % βD = 5 %	β = 20 % βD = 10 %	β =2% βD = 1 %	β = 10 % βD = 5 %	β = 20 % βD = 10 %
1oo1 (비고 2 참조)	0%	2,2E-04			1,1E-03			2,2E-03		
	60 %	8,8E-05			4,4E-04			8,8E-04		
	90 %	2,2E-05			1,1E-04			2,2E-04		
	99 %	2,6E-06			1,3E-05			2,6E-05		
1oo2	0%	4,4E-06	2,2E-05	4,4E-05	2,3E-05	1,1E-04	2,2E-04	5,0E-05	2,2E-04	4,4E-04
	60 %	1,8E-06	8,8E-06	1,8E-05	9,0E-06	4,4E-05	8,8E-05	1,9E-05	8,9E-05	1,8E-04
	90 %	4,4E-07	2,2E-06	4,4E-06	2,2E-06	1,1E-05	2,2E-05	4,5E-06	2,2E-05	4,4E-05
	99 %	4,8E-08	2,4E-07	4,8E-07	2,4E-07	1,2E-06	2,4E-06	4,8E-07	2,4E-06	4,8E-06
2oo2 (비고 2 참조)	0%	4,4E-04			2,2E-03			4,4E-03		
	60 %	1,8E-04			8,8E-04			1,8E-03		
	90 %	4,5E-05			2,2E-04			4,5E-04		
	99 %	5,2E-06			2,6E-05			5,2E-05		
1oo2D (비고 3 참조)	0%	4,4E-06	2,2E-05	4,4E-05	2,3E-05	1,1E-04	2,2E-04	5,0E-05	2,2E-04	4,4E-04
	60 %	1,8E-06	8,8E-06	1,8E-05	8,9E-06	4,4E-05	8,83E-05	1,8E-05	8,8E-05	1,8E-04
	90 %	4,4E-07	2,2E-06	4,4E-06	2,2E-06	1,1E-05	2,2E-05	4,4E-06	2,2E-05	4,4E-05
	99 %	4,8E-08	2,4E-07	4,8E-07	2,4E-07	1,2E-06	2,4E-06	4,8E-06	2,4E-06	4,8E-06
2oo3	0%	4,6E-06	2,2E-05	4,4E-05	2,7E-05	1,1E-04	2,2E-04	6,2E-05	2,4E-04	4,5E-04
	60 %	1,8E-06	8,8E-06	1,8E-05	9,5E-06	4,5E-05	8,8E-05	2,1E-05	9,1E-05	1,8E-04
	90 %	4,4E-07	2,2E-06	4,4E-06	2,3E-06	1,1E-05	2,2E-05	4,6E-06	2,2E-05	4,4E-05
	99 %	4,8E-08	2,4E-07	4,8E-07	2,4E-07	1,2E-06	2,4E-06	4,8E-07	2,4E-06	4,8E-06
1oo3	0%	4,4E-06	2,2E-05	4,4E-05	2,2E-05	1,1E-04	2,2E-04	4,4E-05	2,2E-04	4,4E-04
	60 %	1,8E-06	8,8E-06	1,8E-05	8,8E-06	4,4E-05	8,8E-05	1,8E-05	8,8E-05	1,8E-04
	90 %	4,4E-07	2,2E-06	4,4E-06	2,2E-06	1,1E-05	2,2E-05	4,4E-06	2,2E-05	4,4E-05
	99 %	4,8E-08	2,4E-07	4,8E-07	2,4E-07	1,2E-06	2,4E-06	4,8E-07	2,4E-06	4,8E-06

구성	DC	λ D = 2,5E-06			λ D = 0,5E-05			λ D = 2,5E-05		
		β =2% βD = 1 %	β = 10 % βD = 5 %	β = 20 % βD = 10 %	β =2% βD = 1 %	β = 10 % βD = 5 %	β = 20 % βD = 10 %	β =2% βD = 1 %	β = 10 % βD = 5 %	β = 20 % βD = 10 %
1oo1 (비고 2 참조)	0%	1,1E-02			2,2E-02			>1E-01		
	60 %	**4,4E-03**			**8,8E-03**			4,4E-02		
	90 %	1,1E-03			2,2E-03			1,1E-02		
	99 %	1,3E-04			2,6E-04			1,3E-03		
1oo2	0%	3,7E-04	1,2E-03	2,3E-03	1,1E-03	2,7E-03	4,8E-03	1,8E-02	2,4E-02	3,2E-02
	60 %	1,1E-04	4,6E-04	9,0E-04	2,8E-04	**9,7E-04**	1,8E-03	3,4E-03	6,6E-03	1,1E-02
	90 %	2,4E-05	1,1E-04	2,2E-04	5,1E-05	2,3E-04	4,5E-04	3,8E-04	1,3E-03	2,3E-03
	99 %	2,4E-06	1,2E-05	2,4E-05	4,9E-06	2,4E-05	4,8E-05	2,6E-05	1,2E-04	2,4E-04
2oo2 (비고 2 참조)	0%	2,2E-02			4,4E-02			>1E-01		
	60 %	8,8E-03			1,8E-02			8,8E-02		
	90 %	2,2E-03			4,5E-03			2,2E-02		
	99 %	2,6E-04			5,2E-04			2,6E-03		
1oo2D (비고 3 참조)	0%	3,7E-04	1,2E-03	2,3E-03	1,1E-03	2,7E-03	4,8E-03	1,8E-02	2,4E-02	3,2E-02
	60 %	9,4E-05	4,5-04	8,8E-04	2,0E-04	9,0E-04	1,8E-03	1,5E-03	5,0E-03	9,3E-03
	90 %	2,2E-05	1,1E-04	2,2E-04	4,5E-05	4,5E-05	4,4E-04	2,3E-04	1,1E-03	2,2E-03
	99 %	2,6E-06	1,2E-05	2,4E-05	**4,8E-06**	2.4E-05	4,8E-05	2,4E-05	1,2E-04	2,4E-04
2oo3	0%	6,8E-04	1,5E-03	2,5E-03	2,3E-03	3,8E-03	5,6E-03	4,8E-02	5,0E-02	5,3E-02
	60 %	1,6E-04	5,1E-04	9,4E-04	4,8E-04	1,1E-03	2,0E-03	8,4E-03	1,1E-02	1,5E-02
	90 %	2,7E-05	1,2E-04	**2,3E-04**	6,4E-05	2,4E-04	4,6E-04	7,1E-04	1,6E-03	2,6E-03
	99 %	2,5E-06	1,2E-05	2,4E-05	5,1E-06	2,4E-05	4,8E-05	3,1E-05	1,3E-04	2,5E-04
1oo3	0%	2,2E-04	1,1E-03	2,2E-03	4,6E-04	2,2E-03	4,4E-03	4,7E-03	1,3E-02	2,3E-02
	60 %	8,8E-05	4,4E-04	8,8E-04	1,8E-04	8,8E-04	1,8E-03	1,0E-03	4,5E-03	8,9E-03
	90 %	2,2E-05	1,1E-04	2,2E-04	4,4E-05	2,2E-04	4,4E-04	2,2E-04	1,1E-03	2,2E-03
	99 %	2,4E-06	1,2E-05	2,4E-05	4,8E-06	2,4E-05	4,8E-05	2,4E-05	1,2E-04	2,4E-04

비고 1 이 표는 PFD 값의 예를 나타낸다. 이 값은 각 등식에 따라 계산된다.
비고2 이 표는 β = 2× βD 를 가정한다. 1oo1, 1oo2 는 β 와 βD T의 값은 평균 고장확률에 영향을 미치지 않는다.
비고 3 안전한 고장율은 위험한 고장율과 K =0.98과 동등하다고 가정한다.

* source IEC 61508 part 6 Annex B Table B.3

<별표 4> 2년의 보증시험주기와 8 시간 평균복구시간을 위한 요구시 고장평균확률

구성	DC	λ D = 0,5E-07			λ D = 2,5E-07			λ D = 0,5E-06		
		β =2% βD = 1 %	β = 10 % βD = 5 %	β = 20 % βD = 10 %	β =2% βD = 1 %	β = 10 % βD = 5 %	β = 20 % βD = 10 %	β =2% βD = 1 %	β = 10 % βD = 5 %	β = 20 % βD = 10 %
1oo1 (비고 2 참조)	0%	4,4E-04			2,2E-03			4,4E-03		
	60 %	1,8E-04			8,8E-04			1,8E-03		
	90 %	4,4E-05			2,2E-04			4,4E-04		
	99 %	4,8E-06			2,4E-05			4,8E-05		
1oo2	0%	9,0E-06	4,4E-05	8,8E-05	5,0E-05	2,2E-04	4,4E-04	1,1E-04	4,6E-04	8,9E-04
	60 %	3,5E-06	1,8E-05	3,5E-05	1,9E-05	8,9E-05	1,8E-04	3,9E-05	1,8E-04	3,5E-04
	90 %	8,8E-07	4,4E-06	8,8E-06	4,5E-06	2,2E-05	4,4E-05	9,1E-06	4,4E-05	8,8E-05
	99 %	9,2E-08	4,6E-07	9,2E-07	4,6E-07	2,3E-06	4,6E-06	9,2E-07	4,6E-06	9,2E-06
2oo2 (비고 2참조)	0%	8,8E-04			4,4E-03			8,8E-03		
	60 %	3,5E-04			1,8E-03			3,5E-03		
	90 %	8,8E-05			4,4E-04			8,8E-04		
	99 %	9,6E-06			4,8E-05			9,6E-05		
1oo2D (비고 3 참조)	0%	9,0E-06	4,4E-05	8,8E-05	5,0E-05	2,2E-04	4,4E-04	1,1E-04	4,6E-04	8,9E-04
	60 %	3,5E-06	1,8E-05	3,5E-05	1,8E-05	8,8E-05	1,8E-04	3,6E-05	1,8E-04	3,5E-04
	90 %	8,8E-06	4,4E-06	8,8E-06	4,4E-06	2,2E-05	4,4E-05	8,8E-06	4,4E-05	8,8E-05
	99 %	9,2E-07	4,6E-07	9,2E-07	4,6E-07	2,3E-06	4,6E-06	9,2E-07	4,46-06	9,2E-06
2oo3	0%	9,5E-06	4,4E-05	8,8E-05	6,2E-05	2,3E-04	4,5E-04	1,6E-04	5,0E-04	9,3E-04
	60 %	3,6E-06	1,8E-05	3,5E-05	2,1E-05	9,0E-05	1,8E-04	4,7E-05	1,9E-04	3,6E-04
	90 %	8,9E-07	4,4E-06	8,8E-06	4,6E-06	2,2E-05	4,4E-05	9,6E-06	4,5E-05	8,9E-05
	99 %	9,2E-08	4,6E-07	9,2E-07	4,6E-07	2,3E-06	4,6E-06	9,3E-07	4,6E-06	9,2E-06
1oo3	0%	8,8E-06	4,4E-05	8,8E-05	4,4E-05	2,2E-04	4,4E-04	8,8E-05	4,4E-04	8,8E-04
	60 %	3,5E-06	1,8E-05	3,5E-05	1,8E-05	8,8E-05	1,8E-04	3,5E-05	1,8E-04	3,5E-04
	90 %	8,8E-07	4,4E-06	8,8E-06	4,4E-06	2,2E-05	4,4E-05	8,8E-06	4,4E-05	8,8E-05
	99 %	9,2E-08	4,6E-07	9,2E-07	4,6E-07	2,3E-06	4,6E-06	9,2E-07	4,6E-06	9,2E-06

구성	DC	λ D =2,5E-06			λ D = 0,5E-05			λ D = 2,5E-05		
		β =2% βD = 1 %	β = 10 % βD = 5 %	β = 20 % βD = 10 %	β =2% βD = 1 %	β = 10 % βD = 5 %	β = 20 % βD = 10 %	β =2% βD = 1 %	β = 10 % βD = 5 %	β = 20 % βD= 10 %
1oo1 (비고 2 참조)	0%	2,2E-02			4,4E-02			>1E-01		
	60 %	8,8E-03			1,8E-02			8,8E-02		
	90 %	2,2E-03			4,4E-03			2,2E-02		
	99 %	2,4E-04			4,8E-04			2,4E-03		
1oo2	0%	1,1E-03	2,7E-03	4,8E-03	3,3E-03	6,5E-03	1,0E-02	6,6E-02	7,4E-02	8,5E-02
	60 %	2,8E-04	9,7E-04	1,8E-03	7,5E-04	2,1E-03	3,8E-03	1,2E-02	1,8E-02	2,5E-02
	90 %	5,0E-05	2,3E-04	4,5E-04	1,1E-04	4,6E-04	9,0E-04	1,1E-03	2,8E-03	4,9E-03
	99 %	4,7E-06	2,3E-05	4,6E-05	9,5E-06	4,6E-05	9,2E-05	5,4E-05	2,4E-04	4,6E-04
2oo2 (비고 2 참조)	0%	4,4E-02			8,8E-02			>1E-01		
	60 %	1,8E-02			3,5E-02			>1E-01		
	90 %	4,4E-03			8,8E-03			4,4E-02		
	99 %	4,8E-04			9,6E-04			4,8E-03		
1oo2D (비고 3참조)	0%	1,1E-03	2,7E-03	4,8E-03	3,3E-03	6,5E-03	1,0E-02	6,6E-02	7,4E-02	8,5E-02
	60 %	2,0E-04	9,0E-04	1,8E-03	4,5E-04	1,8E-03	3,6E-03	4,3E-03	1,1E-02	1,9E-02
	90 %	4,4E-05	2,2E-04	4,4E-04	8,9E-05	4,4E-04	8,8E-04	4,7E-04	2,2E-03	4,4E-03
	99 %	4,6E-06	2,3E-05	4,6E-05	9,2E-06	4,6E-05	9,2E-05	4,6E-05	2,3E-04	4,6E-04
2oo3	0%	2,3E-03	3,7E-03	5,6E-03	8,3E-03	1,1E-02	1,4E-02	1,9E-01	1,8E-01	1,7E-01
	60 %	4,8E-04	1,1E-03	2,0E-03	1,6E-03	2,8E-03	4,4E-03	3,2E-02	3,5E-02	4,0E-02
	90 %	6,3E-05	2,4E-04	4,6E-04	1,6E-04	5,1E-04	9,4E-04	2,4E-03	4,0E-03	6,0E-03
	99 %	4,8E-06	2,3E-05	4,6E-05	1,0E-05	4,7E-05	9,2E-05	6,9E-05	2,5E-04	4,8E-04
1oo3	0%	4,6E-04	2,2E-03	4,4E-03	1,0E-03	4,5E-03	8,9E-03	2,4E-02	3,7E-02	5,5E-02
	60 %	1,8E-04	8,8E-04	1,8E-03	3,6E-04	1,8E-03	3,5E-03	3,1E-03	9,9E-03	1,8E-02
	90 %	4,4E-05	2,2E-04	4,4E-04	8,8E-05	4,4E-04	8,8E-04	4,6E-04	2,2E-03	4,4E-03
	99 %	4,6E-06	2,3E-05	4,6E-05	9,2E-06	4,6E-05	9,2E-05	4,6E-05	2,3E-04	4,6E-04

비고 1 이 표는 PFD 값의 예를 나타낸다. 이 값은 각 등식에 따라 계산된다.
비고2 이 표는 β = 2× βD 를 가정한다. 1oo1, 1oo2 는 β 와 βD T의 값은 평균 고장확률에 영향을 미치지 않는다.
비고 3 안전한 고장율은 위험한 고장율과 K =0.98과 동등하다고 가정한다.

* source IEC 61508 part 6 Annex B Table B.4

<부록>

안전계장기능의 안전무결성 수준 검증의 예

안전관련 시스템이 <그림 15> 와 같은 안전계장기능의 각 하부시스템으로 구성되어 있다고 가정하고,

- 1년 주기의 보증시험주기(proof test interval)와 8시간의 평균복구시간(MTTR)을 적용
- 감지부에 대한 요구시 고장평균확률을 <별표 3>으로부터 <부록 표 1>과 같이 2.3E-04임을 찾을 수 있다.

<부록 표 1> 감지부에 대한 요구시 고장평균확률(PFD_S)

구성	DC	λ_D = 2,5E-06		
		β =2% β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
2oo3	0 %	6.8E-04	1.5E-03	2.5E-03
	60%	1.6E-04	5.1E-04	9.4E-04
	90%	2.7E-05	1.2E-04	**2.3E-04**
	99%	2.5E-06	1.2E-05	2.4E-05

- 논리기에 대한 요구시 고장평균확률을 <별표 3>으로부터 <부록 표 2>과 같이 4.8E-06임을 찾을 수 있다.

<부록 표 2> 논리기에 대한 요구시 고장평균확률(PFD_L)

구성	DC	λ_D = 0.5E-06		
		β =2% β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo2D	0 %	1.1E-03	2.7E-03	4.8E-03
	60%	2.0E-04	9.0E-04	1.8E-03
	90%	4.5E-05	2.2E-04	4.4E-04
	99%	**4.8E-06**	2.4E-05	4.8E-05

- 조작부에 대한 요구시 고장평균확률을 <별표 3>으로부터 <부록 표 3>과 같이 4.4E-03과 8.8E-03임을 찾아 이를 더하면 1.3E-02를 구할 수 있다.

<부록 표 3> 논리기에 대한 요구시 고장평균확률(PFD_{FE})

구성	DC	λ_D = 2.5E-06	λ_D = 0.5E-05
1oo1	0 %	1.1E-02	2.2E-02
	60%	**4.4E-03**	**8.8E-03**
	90%	1.1E-03	2.2E-03
	99%	1.3E-04	2.6E-04

◦ 따라서 안전계장기능에 대한 총 요구시 고장평균확률(PFD_{SYS})를 구하면, 2.3E-04 + 4.8E-06 + 1.3E-02 = 1.3E-02이다. **이는 안전무결성수준(SIL) 1에 해당한다.**

⇒ **안전계장기능이 안전무결성수준(SIL) 2를 만족하기 위해서는 다음과 같이 보증시험 주기를 6개월로 단축하거나, 조작부 등의 구성(voting)을 1oo1에서 1oo2로 개선하면 된다.**

1. 보증시험 주기를 6 개월로 단축할 경우

- PFD_S = 1.1E-04
- PFD_L = 2.6E-06
- PFD_{FE} = 2.2E-03 + 4.4E-03 = 6.6E-03
- PFD_{SYS} = 6.7E-03을 얻을 수 있다. **이는 안전무결성수준 2를 만족한다.**

2. 조작부의 차단밸브를 1oo2로 개선할 경우(β = 10 % β_D = 5 %로 가정)

- PFD_S = 2.3E-04
- PFD_L = 4.8E-06
- PFD_{FE} = 4.4E-03 + 9.7E-04 = 5.4E-03
- PFD_{SYS} = 5.6E-03을 얻을 수 있다. **이는 안전무결성수준 2를 만족한다.**