KOSHA GUIDE
X - 76 - 2018

# 안전관련 시스템의 공통원인고장의 영향 정량화에 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 D: 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 - 76 - 2018 |

# 안전관련 시스템의 공통원인고장의 영향 정량화에 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 공통원인고장의 영향 정량화에 필요한 사항을 정함을 목적으로 한다.

## 2. 적용범위

(1) 이 지침은 전기/전자/프로그램 가능형 전자장치 기반으로 구성된 안전관련 시스템의 하부시스템내 각 채널에서 발생할 수 있는 공통원인고장의 영향에 한하여 적용한다.

(2) 이 지침은 다음의 가이드를 보완 또는 인용하여 적용할 수 있다.

(가) X-76(안전관련 시스템의 하드웨어 고장확률 계산에 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 안전계장설비를 말한다.

(라) “안전기능(Safety function)”이란 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(sensor), 논리부(logic solver), 조작부(final element) 등으로 개별 채널과 이를 연결을 위한 전자인터페이스를 포함한 조합을 말한다.

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

(아) “랜덤 하드웨어 고장(Random hardware failures)”이라 함은 안전계장기능의 하부시스템내 채널 등에서 임의적인 시간에 독립적으로 개별 채널에서 고장이 발생하여 안전관련 시스템 기능의 이상을 초래하게 하는 고장을 말한다.

(자) “시스템적 고장(Systemic failures)”이라 함은 하부시스템 또는 채널이나 관련 지원요소들에서 하나의 원인에 의한 고장이 동시에 공통으로 발생하여 안전관련 시스템 기능의 이상을 초래하는 고장을 말한다.

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

(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. 공통원인고장의 일반사항

4.1 전형적인 공통원인고장의 주요 원인

(1) 안전관련 시스템의 하부시스템 요소들의 불충분한 설계 및 시방(예, 신뢰도등이 과소평가된 부품들)

(2) 하부시스템 요소(부품)의 생산 제조과정에서의 불량

(3) 안전관련 시스템 작동에 필요한 지원설비의 부족이나 고장요인(예, 공통 전원, 계장공기 등)

(4) 안전관련시스템이 설치되어 있는 장소의 열약한 운전조건(예, 공정온도, 습도, 진동 등)

(5) 기타 안전관련 시스템이 설치되어 있는 장소의 외부 요인(예, 화재, 지진, 날씨 등)

4.2 잠재적 공통원인고장의 감소 방법

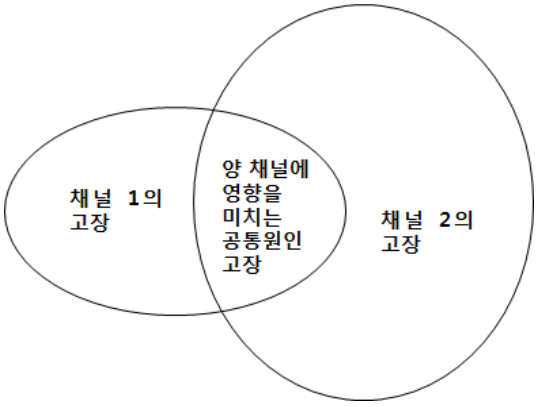
(1) 랜덤 하드웨어 고장과 시스템적 고장의 수를 전체적으로 감소시킨다. <그림 1>과

같이 2개의 타원형 부분을 감소시키면, 궁극적으로 중복되는 부분을 감소를 가져올 수 있다.

(2) 채널의 독립성을 최대화하고, 각 채널의 연결을 분리하거나 다양성을 준다. <그림 1> 의 2개 타원형을 중복부분을 최소화 한다.

(3) 두 번째 채널에서 공통의 원인에 의한 고장에 발생하기 전에 첫 번째 채널고장을 발견할 수 있도록 자가진단 시험기능을 갖춘다.

(4) 제조자 매뉴얼에 따른 주기적인 보증시험을 실시하여 채널 1의 고장을 찾아내어 채널 2까지 영향을 주기전에 보수한다.




<그림 1> 개별 채널에서의 고장과 공통원인고장과의 관계

4.3 공통원인고장의 확률값 추정방법

(1) 공통원인고장의 확률을 추정하는 대부분의 방법론은 랜덤 하드웨어 고장확률을 통하여 예측한다.

(2) 하부시스템의 랜덤 하드웨어 고장이 높을수록 다음과 같은 사항을 알 수 있다.

(가) 하부시스템에 요구되는 유지관리가 더욱 요구되어 유지보수하는 동안 시스템적 고장확률은 높아진다. 따라서 공통원인고장을 가져올 다음과 같은 휴먼에러의 확률을 높아진다.

① 랜덤 하드웨어 고장이 발생할 때마다 수리, 시험 및 교정 등이 요구됨
② 안전무결성수준이 높을수록 더 많은 보증시험 등이 요구되어 더 많은 간섭 초래

(나) 더 복잡한 채널로 구성된 하부시스템이다. 채널 수가 많으면 많을수록, 또는 복잡성에 따라 랜덤 하드웨어 고장확률은 높아진다.

(3) 하부시스템의 공통원인고장의 확률값은 β-factor 모델을 활용한 접근법이 가장 많이 활동되고 있다.

## 5. β-factor를 이용한 공통원인고장의 확률 계산

5.1 일반사항

(1) β-factor 모델은 랜덤 하드웨어 고장이 공통원인고장과 연계된다고 가정한다.

(2) 안전관련 시스템 전체와 관련된 공통원인고장의 확률은 시스템 복잡성에 영향을 받는다. 특히 하드웨어뿐만 아니라 소프트웨어와 연관되어 있다.

(3) 소프트웨어 고장을 모델화하는 것은 매우 어렵기 때문에 본 지침에서는 하드웨어 고장에 국한한다.

(4) 감지부, 논리기 및 조작부 등 하부시스템내 개별 채널로 분리하여 β-factor 모델화 한다. 이는 논리기 설치의 환경조건과 감지부와 조작부의 설치 위치의 환경조건이 다르고, 또한 자가진단 시험주기 등도 다르기 때문이다.

(5) 프로그램 가능형 전자장치(논리기)는 정교한 자가진단 시험기능을 수행하여야 하므로 다음과 같은 조건을 충족한다.

(가) 채널 내에서 높은 자가진단 범위를 가질 수 있다.

(나) 추가적으로 중복성 채널들로 감시할 수 있다.

(다) 높은 반복율을 가질 수 있다.

(라) 고장이 증가함에 따라, 감지부 및 조작부들도 감시할 수 있다.

(6) 공통원인고장이 모든 채널들에 동시에 고장을 일으키는 비율은 높지 않다. 그러므로 자가진단 시험의 반복횟수가 충분히 많다면, 다른 채널에 영향을 받기 전에 대부분의 공통원인고장은 밝혀질 것이다.

(7) 각 채널이 영향을 받는 독립적으로 2개의 채널에 비해 3개 채널이 공통원인고장이 적게 발생할 수 있으나, 본 지침에서는 2개 채널에 한하여 X와 Y로 각각 구분한다.

5.2 가정 및 계산방법

(1) β-factor 모델을 이용한 위험한 공통원인고장확률은 $\lambda_D\beta$이다. 여기서 $\lambda_D$는 각 채널의 위험한 랜덤 하드웨어 고장확률이며, β는 자가진단 시험을 하지 않을 경우 β-factor이다. 이는 모든 채널에 영향을 미치는 단일 채널 고장 비율이다.

(2) 공통원인고장은 모든 채널에 영향을 미치는 시간적 간격은 없는 것으로 가정한다.

(3) 모든 채널에 자가진단 시험을 실시한다면, 위험한 공통원인고장확률로 인한 총 고장률은 $\lambda_{Du}\beta + \lambda_{Dd}\beta_D$ 이다.

(가) $\lambda_{Du}$는 단일 채널의 검출되지 않는 고장확률로서 자가진단 시험에서도 검출되지 않는 고장확률이다. 이는 반복적인 자가진단 시험을 실시해도 β-factor의 감소는 없다.

(나) $\lambda_{Dd}$는 단일 채널의 검출되는 고장확률로서 자가진단 시험에서 검출되는 고장확률이다. 이는 반복적인 자가진단 시험을 실시하면 $\beta_D$는 감소된다.

(다) 자가진단 시험이 반복율이 증가하면 할수록 $\beta_D$값는 β 이하로 점점 낮아진다.

5.3 표를 활용한 추정 방법

(1) β-factor 계산은 감지부, 논리기, 조작부에 대하여 분리하여 계산한다.

(2) 안전관련 시스템에서 공통원인고장 발생 방지를 하기위한 공학적, 관리적 및 운전적 조치가 효과적으로 수행된다면 β-factor 값은 감소할 것이다.

(3) <표 1>은 공학적 조치 등을 각 항목으로 구분하였으며, 이들의 방법 및 조치에 따라 공통원인고장의 감소에 미치는 영향을 나타낸다. <표 1>의 활용 방법은 다음과 같다.

(가) 감지부와 조작부는 설치 위치 등 환경조건이 동일함으로, 동일한 점수항목으로 하고, 논리기의 점수항목은 분리하였다.

(나) X값과 Y 값의 비율은 자가진단 시험에 의한 공통원인고장의 검출 등 개선에 대한 각 항목이 기여하는 정도를 나타낸다.

(다) 각 항목의 점수는 최고 점수를 나타내며, 각 하부시스템의 채널 평가 시 조건에 따라 이 점수 이하를 줄 수 있다.

(라) $X_{LS}$와 $Y_{LS}$는 논리기에 관한 각 열을 나타내고, $X_{SF}$ 와 $Y_{SF}$는 감지부 및 조작부에 관한 각 열을 나타낸다. 이 합계는 X와 Y로 언급된다.

(마) X열은 직접적인 영향을 고려한 것이며, Y열은 간접적인 영향을 고려한 것이다. 예를들면 온라인에 의한 공통원인고장을 검출하는 시험 등은 X열이며, 현장에서 이루어지는 점검 등은 Y열이다.

(4) <표 2>와 <표 3>은 자가진단 시험의 빈도와 범위에 따른 Z factor를 결정하는데 사용한다. 자가진단 시험 주기가 길어지면(1 주 이상) Z값이 0에 가깝다.

(가) Z 값이 0이 아닌 값으로 사용되려면, 비동시적 공통원인고장이 모든 채널에 영향을 미치기 전에 안전관련 시스템이 안전한 상태로 놓여 있도록 보장되어야 한다.

<표 1> 논리기, 감지부 및 조작부의 β-factor 값 결정을 위한 점수표

| 항 목 | 논리기 | | 감지부/조작부 | |
|---|---|---|---|---|
| | $X_{LS}$ | $Y_{LS}$ | $X_{SF}$ | $Y_{SF}$ |
| **분리/분할** | | | | |
| 채널들에 대해 모든 위치에서 각각의 경로별로 모든 신호 케이블이 분리되어 있는가? | 1.5 | 1.5 | 1.0 | 2.0 |
| 분리된 회로기판 위에 논리기 채널들이 설치되어 있는가? | 3.0 | 1.0 | | |
| 효과적으로 작동하기 위해 논리기는 물리적으로 분리되어 있는가? 예, 별도의 케비넷에 설치됨. | 2.5 | 0.5 | | |
| 감지부/조작부가 전용의 제어 전자장치를 가지고 있다면, 각 채널에 분리된 회로기판 위에 전자장치가 설치되어 있는가? | | | 2.5 | 1.5 |
| 감지부/조작부가 전용의 제어 전자장치를 가지고 있다면, 각 채널이 내부에 있고, 별도의 케비넷에 전자장치가 설치되어 있는가? | | | 2.5 | 0.5 |
| **다양성/중복성** | | | | |
| 채널들은 상이한 전기 기술을 채택했는가? 에, 하나의 전자장치 또는 프로그램 가능형 전자장치와 다른 릴레이(relay)로 되어 있음. | 8.0 | | | |
| 채널들은 상이한 전기 기술을 채택했는가? 에, 하나의 전자 또는 다른 프로그램 가능형 전자장치로 되어 있음. | 6.0 | | | |
| 탐촉기 요소가 상이한 물리적 원리를 채택한 부품인가? 예, 압력 및 온도 풍량계 및 변환계 등 | | | 9.0 | |
| 상이한 전기적 원리/설계를 채택한 부품인가? 예, 아날로그 및 디지털, 다양한 제조자 또는 기술 등 | | | 6.5 | |
| 낮은 정도의 다양성을 사용했는가? 예, 같은 기술을 사용하여 하드웨어 자가진단시험을 실시 | 2.0 | 1.0 | | |
| 중간정도의 다양성을 사용했는가? 예, 상이한 기술을 사용하여 하드웨어 자가진단시험을 실시 | 3.0 | 2.0 | | |
| 설계하는 동안 설계자간에 정보공유 없이 채널들은 상이한 설계자들에 의해 설계되었는가? | 1.5 | 1.5 | | |
| 시운전하는 동안 각각 채널을 위해 분리된 시험방법과 운전원들이 활용되었는가? | 1.0 | 0.5 | 1.0 | 2.0 |
| 상이한 시간에 여러 검사원들이 각각 채널들을 유지보수되었는가? | 3.0 | | 3.0 | |
| **복잡성/설계/적용/완성/경험** | | | | |
| 채널간 교차연결 시 자가진단시험이나 voting 목적으로 이용되는 것 이외의 다른 정보가 교환되는 것을 방지하였는가? | 0.5 | 0.5 | 0.5 | 0.5 |
| 설계는 5 년 이상 현장에서 성공적으로 사용되었던 설비에 적용된 기술을 기반하여 설계되었는가? | 0.5 | 1.0 | 1.0 | 1.0 |
| 유사 환경에서 사용된 동일한 하드웨어에 대한 경험이 5년 이상인가? | 1.0 | 1.5 | 1.5 | 1.5 |
| 시스템이 단순한가? 예, 채널 당 입력 및 출력이 10 미만으로 적은가? | | 1.0 | | |
| 입력 및 출력이 잠재적 수준의 과전류 및 과전압으로부터 보호되어 있는가? | 1.5 | 0.5 | 1.5 | 0.5 |
| 모든 부품/요소들이 보수적으로 평가되고 있는가? 예, 2개이상의 요인으로 | 2.0 | | 2.0 | |

| 항 목 | 논리기 | | 감지부/조작부 | |
|---|---|---|---|---|
| | $X_{LS}$ | $Y_{LS}$ | $X_{SF}$ | $Y_{SF}$ |
| **평가/분석 및 자료의 피드백** | | | | |
| FMEA 또는 FTA를 통해 공통원인고장을 파악하기 위한 시험을 실시하고, 미리 찾아낸 공통원인고장 원천을 제거하도록 설계에 반영되었는가? | | 3.0 | | 3.0 |
| 설계 검토 시 고려된 공통원인고장은 설계에 피드백 되었는가? (설계 검토 활동에 문서상 증거로 요구됨) | | 3.0 | | 3.0 |
| 모든 현장의 고장에 대하여 분석되고, 설계에 피드백 되어 있는가? (절차서가 문서 증거로 요구됨) | 0.5 | 3.5 | 0.5 | 3.5 |
| **절차서/조작자 인테페이스** | | | | |
| 모든 요소 고장(또는 성능 저하)를 확실히 검출할 수 있도록 문서화된 시스템이 있으며, 근본 원인과 잠재적 원인과 고장을 파악할 수 있도록 또한 시스템적으로 확보되어 있는가? | | 1.5 | 0.5 | 1.5 |
| 다음 사항을 보증하기 위한 절차서가 제정되어 있는가; 모든 독립된 채널의 각 요소의 유지보수(조정과 교정 포함), 유지보수 수행하기 위한 매뉴얼, 채널에 대한 유지보수 완료와 다음의 채널의 유지보수 시작 사이에 자가진단 시험 | 1.5 | 0.5 | 2.0 | 1.0 |
| 중복 시스템(예, 케이블 등)의 모든 부품이 서로 독립적이어야 하고, 재배치되지 않도록 특별히 문서화된 유지보수 절차서가 있는가? | 0.5 | 0.5 | 0.5 | 0.5 |
| 회로기판 등의 유지보수는 전문 보수회사에서 수행되고, 보수(교체)를 위한 부품은 설치 전에 충분한 시험을 걸치는가? | 0.5 | 1.0 | 0.5 | 1.0 |
| 시스템이 낮은 정도의 자가진단시험 범위(60 % ~ 90 %)인가? 고장을 현장 교체 모듈 수준에 보고되는가? | 0.5 | | | |
| 시스템이 중간 정도의 자가진단시험 범위(90 % ~ 99 %)인가? 고장을 현장 교체 모듈 수준에 보고되는가? | 1.5 | 1.0 | | |
| 시스템이 낮은 정도의 자가진단시험 범위( 99 % 초과)인가? 고장을 현장 교체 모듈 수준에 보고되는가? | 2.5 | 1.5 | | |
| 고장에 대한 자가진단 시험이 현장 교체 모듈 수준에 보고되는가? | | | 1.0 | 1.0 |
| **자격/교육훈련/안전문화** | | | | |
| 공통원인고장의 원인과 영향(결과)을 이해하도록 교육(문서교육포함)을 설계자들은 받았는가? | 2.0 | 3.0 | 2.0 | 3.0 |
| 공통원인고장의 원인과 영향(결과)을 이해하도록 교육(문서교육포함)을 유지보수 담당자들은 받았는가? | 0.5 | 4.5 | 0.5 | 4.5 |
| **환경적 제어** | | | | |
| 개인적 접근을 제한하는가?(예, 캐비닛 잠금, 접근제한 등) | 0.5 | 2.5 | 0.5 | 2.5 |
| 온도, 습도, 부식, 분진, 진동 등으로부터 안전한 범위내에서 운전되고, 외부 환경적 제한없이 범위를 벗어나는지 시험 등을 통해 관리되고 있는가? | 3.0 | 1.0 | 3.0 | 1.0 |
| 모든 신호와 전원 케이블은 모든 위치에서 분리되어 있는가? | 2.0 | 1.0 | 2.0 | 1.0 |
| **환경시험** | | | | |
| 관련된 모든 환경적 영향(예, EMC, 온도, 진동, 쇼크, 습도 등)(으로부터 면역성 시험이 인가된 표준에 의해 적절하게 시험되고 있는가? | 10.0 | 10.0 | 10.0 | 10.0 |

(나) Z 값이 0이 아닌 값은 오직 다음의 경우에만 사용될 수 있다.

① 결함이 발견되자마자 안전관련 시스템이 자동으로 운전이 중단되거나.
② 자가진단 시험을 통해 결함의 위치를 확인하고, 결함을 한부분에 제한하고 안전관련 시스템은 안전한 상태로 유지될 수 있어야 한다.
③ 2oo3 voting의 경우 <표 2>와 <표 3>의 시간 이내에 간단한 고장은 정지(또는 보수)하고, 단일 고장은 확인한다. 이렇게 하지 않으면 두 번째 채널에 고장이 발생하여 정상 채널에도 영향을 미칠 수 있다.

<표 2> 논리기의 Z 값

| 진단 범위 | 자가진단 시험 주기 | | |
|---|---|---|---|
| | 1 분 이하 | 1분과 5분사이 | 5분 이상 |
| ≥99 % | 2.0 | 1.0 | 0 |
| ≥90 % | 1.5 | 0.5 | 0 |
| ≥60 % | 1.0 | 0 | 0 |

<표 3> 감지부와 조작부의 Z 값

| 진단 범위 | 자가진단 시험 주기 | | | |
|---|---|---|---|---|
| | 2시간 이하 | 2시간과 2일 사이 | 2일과 1주 사이 | 1주 이상 |
| ≥99 % | 2.0 | 1.5 | 1.0 | 0 |
| ≥90 % | 1.5 | 1.0 | 0.5 | 0 |
| ≥60 % | 1.0 | 0.5 | 0 | 0 |

<표 4> β값 및 $\beta_D$값의 결정(계산)

| 점수(S 또는 $S_D$) | β값 및 $\beta_D$값 | |
|---|---|---|
| | 논리기 | 감지부나 조작부 |
| 120점 이상 | 0.5 % | 1 % |
| 70점 이상 ~ 120점 미만 | 1 % | 2 % |
| 45점 이상 ~ 70점 미만 | 2 % | 5 % |
| 45점 미만 | 5 % | 10 % |

* 논리기에 대한 0.5 %이하, 감지부에 대한 1 % 이하의 $\beta_D$값은 증명하기 어렵다.

5.4 β-factor 표의 사용방법의 예

(1) 프로그램 가능형 전자장치(논리기)로 단순한 예를 <표 5> 와 같이 β-factor 값을 구한다.

(2) 논리기는 다양성과 중복성을 고려되지 않는 부분에 X와 Y에 대한 대표적인 값들이 이용되었다. 이들의 값은 최고 값의 반 수준이다.

(3) 다양성 유무와 양호한 진단시험, 미흡한 진단시험 등으로 구분하였다.

(4) 다양성/중복성 항목에 다음과 값을 고려하였다.

(가) 하나의 전자장치와 다른 하나는 고전적인 릴레이(relay) 시스템 기술을 사용한다.

(나) 하드웨어 자가진단 시험은 상이한 기술을 사용한다.

(다) 설계하는 과정에서 여러 설계자간에 정보교환이 없었다.

(라) 시운전 중에 상이한 시험 방법과 시험 종사자가 수행하였다.

(마) 유지보수는 여러 시간에 상이한 점검자가 수행하였다.

<표 5> 프로그램 가능형 전자장치(논리기)에 대한 β값 및 $\beta_D$값의 결정의 예

| 주요 항목 | | 양호한 진단시험과 함께 다양성이 높은 시스템 | 미흡한 진단시험과 함께 다양이 높은 시스템 | 양호한 진단시험과 함께 다양성이 없는 시스템 | 미흡한 진단시험과 함께 다양성이 없는 시스템 |
|---|---|---|---|---|---|
| 분리/분할 | X | 3.50 | 3.50 | 3.50 | 3.50 |
| | Y | 1.50 | 1.50 | 1.50 | 1.50 |
| 다양성/중복성 | X | 14.5 | 14.5 | 2.00 | 2.00 |
| | Y | 3.00 | 3.00 | 1.00 | 1.00 |
| 복잡성/설계.... | X | 2.75 | 2.75 | 2.75 | 2.75 |
| | Y | 2.25 | 2.25 | 2.25 | 2.25 |
| 평가/분석.... | X | 0.25 | 0.25 | 0.25 | 0.25 |
| | Y | 4.75 | 4.75 | 4.75 | 4.75 |
| 절차서/인터페이스 | X | 3.00 | 3.00 | 3.00 | 3.00 |
| | Y | 1.50 | 1.50 | 1.50 | 1.50 |
| 자격/교육훈련... | X | 1.25 | 1.25 | 1.25 | 1.25 |
| | Y | 3.75 | 3.75 | 3.75 | 3.75 |
| 환경적 제어 | X | 2.75 | 2.75 | 2.75 | 2.75 |
| | Y | 2.25 | 2.25 | 2.25 | 2.25 |
| 환경시험 | X | 5.00 | 5.00 | 5.00 | 5.00 |
| | Y | 5.00 | 5.00 | 5.00 | 5.00 |
| 자기진단 범위 | Z | 2.00 | 0.00 | 2.00 | 0.00 |
| 합계 X 값 | | 33.5 | 33.5 | 21.0 | 21.0 |
| 합계 Y 값 | | 25.5 | 25.5 | 23.5 | 23.5 |
| 점수 S | | 59 | 59 | 44.5 | 44.5 |
| β값 | | 2 % | 2 % | 5 % | 5 % |
| 점수 $S_D$ | | 126 | 59 | 86.5 | 44.5 |
| $\beta_D$값 | | 0.5 % | 2 % | 1 % | 5 % |

<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]<br>6개월(2,190 h)[1]<br>1년(87,60h)[2],<br>2년(17,520)[2] |
| MTTR<br>/MRT | 평균복구시간(Mean time to restoration)(hour)<br>평균보수시간(Mean repair time(hour) | 8 시간=MRT<br>위험 고장이 검출되는 시간을 가정한 것으로, 자동 검출은 MRT에 비해 아주 적은 시간임. |
| DC | 자가진단범위(공식에서 분률(%)로 표현함). | 0 %, 60 %, 90 %, 99 % |
| $\beta$ | 공통원인 고장의 미검출 고장의 분률 (공식에서 분률(%)로 표현함) (가정 $\beta = 2\times\beta_D$) | 2 %, 10 %, 20 % |
| $\beta_D$ | 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 | |
| $\lambda$ | 하부시스템내 채널의 총 고장률(시간당) | |
| $\lambda_D$ | 하부시스템내 채널의 위험한 고장률(시간당) 위험한 고장률($\lambda_D$)은 0.5$\lambda$로 가정한다.(위험한 고장 50%, 안전한 고장 50%) | 0.05E-06,0.25E-06<br>0.5E-06, 2.5E-06<br>5E-06, 25E-06 |
| $\lambda_{Dd}$ | 하부시스템내 채널의 검출된 위험한 고장률(시간당) | |
| $\lambda_{Du}$ | 하부시스템내 채널의 미검출된 위험한 고장률(시간당) | |
| $\lambda s_u$ | 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 | |