IE Interfaces
Vol. 25, No. 4, pp. 405-415, December 2012. http://dx.doi.org/10.7232/IEIF.2012.25.4.405
ISSN 1225-0996 | EISSN 2234-6465 | © 2012 KIIE

공통원인고장을 고려한 안전제어시스템의 신뢰성 평가척도에 관한 고찰 : IEC 61508을 중심으로

서 순 근†

동아대학교 산업경영공학과

On Reliability Performance of Safety Instrumented Systems with Common Cause Failures in IEC 61508 Standard

Sun-Keun Seo

Department of Industrial and Management Systems Engineering, Dong-A University

The reliability performance measures for low and high or continuous demand modes of operation of safety instrumented systems(SISs) are examined and compared by analyzing the official definitions in IEC 61508 standard. This paper also presents a status of common cause factor(CCF) models used in IEC 61508 and problems relating CCF modelling are discussed and ideas to solve these ones are suggested. An example with mixed M-out-of-N architecture is carried out to illustrate the proposed methods.

Keyword: common cause failure(CCF), functional safety, IEC 61508, M-out-of-N architecture, probability of failure on demand(PFD), safety instrumented system(SIS)

1. 서 론

위험한 사건을 예방하고 인간과 환경, 재산에 미치는 영향을 경감하기 위한 안전제어시스템(Safety Instrumented System; SIS)의 기능안전성(functional safety)에 대한 요구조건을 정립하는 IEC 61508(2000)이 10여년 전 공표된 이래 매우 높은 안전 방호시스템을 요구되는 산업부문에서 이들의 적용이 일반화되고 있다. 기능안전성은 모 표준에 해당되는 IEC61508 외에 프로세스 산업(IEC 61511, 2002), 원자력 발전소, 철도차량, 기계류 제품에 대한 국제표준과 더불어 2011년에는 자동차에 대한 규격 ISO 20262 (2011)가 제정되어 안전이 요구되는 다양한 분야에 채택되고 있다.

이런 국제표준에 적용된 라이프 사이클 접근법의 핵심은 요구되는 안전무결성(Safety Integrity Level; SIL) 수준을 결정하고, SIS 설계자가 적용한 시스템의 아키텍처가 이와 적합한지 따져 보는 것이 된다.

IEC 61508(2000, 2010)은 SIS의 작동모드를 두 가지, 낮은 요구 작동모드(low demand mode)와 높은 요구 작동모드(high demand mode)로 대별한다. 즉, 요구율이 연간 1회보다 크거나 보증시험(proof or functional test) 빈도의 2배보다 클 경우는 높은 요구 작동모드로 보며, 이 모드에는 연속적 작동도 포함된다. 그리고 요구율이 연간 1회보다 작거나 보증시험 빈도의 2배보다 작을 경우는 낮은 요구 작동모드로 구별한다. 높은 요구 작동모드의 예로는 긴급 정지 시스템(emergency shutdown system), 화재가스 검출시스템, 공정 정지 시스템, 자동차의 에어백, 낮은 요구 작동모드로는 선박이나 해상 플랫폼의 동적 위치유지 시스템(dynamic positioning system), 자동차의 ABS(anti-lock braking system), 철도 신호시스템이 속한다(Jin *et al*., 2011). 일반적으로 SIS는 낮은 고장모드에 속하는 경우가 많다고 알려져 있다.

IEC 61508 1판(2000)에 대한 개정판(2010)이 2010년에 공표되어 그 동안 관련 전문가들의 관심이 되고 있던 문제점이 일부

이 논문은 동아대학교 교내연구비 지원에 의하여 연구되었음.
†연락저자 : 서순근 교수, 604-714 부산광역시 사하구 낙동대로 550번길 37번지 동아대학교 공과대학 산업경영공학과,
Fax : 051-200-7697, E-mail : skseo@dau.ac.kr
투고일(2012년 07월 27일), 심사일(1차 : 2012년 09월 05일, 2차 : 2012년 09월 11일), 게재확정일(2012년 09월 11일).

해소되었지만 표준이 가지고 있는 한계점으로 인해 이의 적용 시 여러 가지 난점을 접하게 된다.

IEC 61508에서 두 요구 작동모드에 따라 분리 적용되는 PFD (Average Probability of Failure on Demand)와 PFH(Probability of Dangerous Failure per Hour)로 표현되는 신뢰성 평가척도가 신뢰성 분야에서 널리 쓰이는 순간 및 평균 고장률, 신뢰도와 불신뢰도, B수명, 가용도와 비가용도 등과 달라 의미가 쉽게 전달되지 못하고 있다. 또한 IEC 61508 2판(2010)에서는 1판(2000)에 비해 이런 두 척도의 정의를 구체적으로 기술하는 부분을 Part 6에 추가하였지만 아직도 명쾌하게 이해하기가 쉽지 않다. 특히 PFD보다 모호한 PFH의 정의에 대한 고찰과 요구율이 낮은 요구와 높은 요구 작동모드를 구분하는 경계에 있을 경우는 어떻게 적용해야 되는지 등 두 신뢰성 척도를 통합하는 연구도 있다(Bukowski, 2008; Innal *et al*., 2010; Jin *et al*., 2011).

따라서 본 논문에서는 N 중 M 구조일 경우에 먼저 낮은 요구 작동모드와 높은 요구 작동모드의 신뢰성 평가 척도에 대한 이해와 고찰, IEC 61508에서 제공되는 공식의 근사 정확도를 조사하고자 한다.

더불어 공통원인고장(Common Cause Failure; CCF)은 시스템의 신뢰도를 제고시키는 용장성 설계의 장점을 감소시키므로 (Hoepfer *et al*., 2009), IEC 61508의 SIL 수준 결정에 중요한 역할을 하고 있다. IEC 61508의 1판(2000)에서는 가장 널리 쓰이면서 간편한 베타인자 모형을 채택하고 있으며, 2판(2010)에서는 베타인자 모형 외에 이를 확장한 다중 베타인자(Multiple Beta Factor; MBF) 모형(Hokstad *et al*., 2004; Hauge *et al*., 2006; Hokstad *et al*., 2006) 과 충격모형인 이항 고장률(binomial failure rate) 모형 (Atwood, 1986; Mosleh *et al*., 1988)을 Part 6에서 추천하고 있다.

베타인자 모형은 시스템 구조에 관련 없이 CCF가 발생시키는 시스템 고장 비율을 β로 설정하여, 각 채널의 CCF에 의한 기여 고장률을 일률적으로 해당 채널 고장률에 대한 비율로 간주함으로써 실제와의 부합도가 떨어진다. 이를 보완한 MBF 모형은 CCF에 의해 모든 채널의 고장이 발생한다는 조건을 완화하면서 보다 간편하게 N 중 M 구조의 특성에 맞게 적용시킬 수 있는 장점을 가지고 있다.

그러나 CCF 모형을 실제 적용 시 각 채널의 고장률이 다를 경우가 보편적인데, 이에 대한 구체적 접근방법이 표준 등에 명시되어 있지 않으며, 여러 가지 N 중 M 구조가 혼합되어 있는 경우 등 실무 적용 시에 여러 가지 난점이 발생된다.

본 논문은 IEC 61508 2판에 제시된 CCF 방법론에 대해 고찰과 더불어 SIL 수준 결정 시 신뢰성 평가척도를 산정하는데 일어나는 문제점의 일부를 해결할 수 있는 방법을 제안하며, 예제로서 이의 유용성을 보여주고자 한다.

2. N 중 M 구조의 신뢰성 평가 척도

IEC 61508(2000, 2010)은 안전무결성(이하 SIL)수준을 <Table 1>과 같이 4등급(1등급이 가장 낮은 수준)으로 구분하며, 낮은 요구 작동모드는 평균 요구 고장확률(이하 PFD)과 높은 요구 작동모드는 시간 당 위험 고장확률(이하 PFH)을 신뢰성 평가 척도로 제안하고 있다.

Table 1. SIL Requirements

SIL	PFD	PFH
4	$10^{-5} \le PFD < 10^{-4}$	$10^{-9} \le PFH < 10^{-8}$
3	$10^{-4} \le PFD < 10^{-3}$	$10^{-8} \le PFH < 10^{-7}$
2	$10^{-3} \le PFD < 10^{-2}$	$10^{-7} \le PFH < 10^{-6}$
1	$10^{-2} \le PFD < 10^{-1}$	$10^{-6} \le PFH < 10^{-5}$

IEC 61508의 Part 6은 여러 시스템의 신뢰성 평가척도에 관한 근사식을 제공하고 있다. 1판(2000)에서는 한 채널의 PFD와 PFH에 대한 근사식과 더불어 2중 1, 2중 2, 3중 2, 그리고 2중 1 구조의 변형에 대한 PFD와 PFH에 대한 근사식을 제공하고 있으며, 2판(2010)에서는 3중 1구조에 대한 식을 추가하고 있지만, 이론적 근거나 설명이 상당히 부족하다.

또한 PFD와 PFH를 도출하는 방법으로 해석적 공식(ISA-TR84.00.02, 2002; Oliveira and Abramovitch, 2010), Fault tree, Markov 모형(Zhang *et al*., 2003; Bukowski, 2008), Petri net 등을 2판(2010)의 Part 6에 기술하고 있으며, 표준에서 제공된 식은 해석적 공식에 의한 방법을 기초로 하고 있다.

따라서 본 절에서는 IEC 61508 2판(2010)에서 정의된 PFD와 PFH에 대한 근거를 고찰하며, 대표적인 N 중 M($M \le N$, MooN로 표기) 구조 중에서 표준에 언급된 구조(2중 1구조의 변형인 1oo2D 구조는 제외)에 대해 이들 식의 근사 정확도를 조사해 보고자 한다.

일반적으로 기능안전성 국제표준인 IEC 61508(2000, 2010)과 61511(2003)에서 고장은 안전고장과 위험고장으로, 각각은 보증시험보다 간격이 상당히 짧은 진단시험에 의해 검출되는 고장과 검출되지 않는 고장으로 구별되는데, 주 관심 고장모드는 요구가 발생되거나 보증시험에 의해서만 나타나는 비 검출 위험고장(Dangerous Undetected; DU)이다.

또한 T_1 간격으로 정기적인 검사(즉, 보증시험 간격)가 실시되는 SIS에서 교체나 수리가 수행되면 신품상태(as good as new)로 회복된다고 가정하며, 보증시험에 의해 모든 잠재적인 위험고장은 모두 발견된다고 가정한다.

1판(2000)과 달리 2판(2010)에서는 보다 명확하게 신뢰성 척도를 Part 6 Annex B에서 다음과 같이 정의하고 있다. 즉, PFD를 T_1마다 검사될 때 SIS의 평균 비가용도로서 식 (1)과 같이 정의하고 있다.

$$PFD = \frac{MDT(T_1)}{T_1} \tag{1}$$

여기서 $MDT(T_1)$는 구간 $[0, T_1]$ 에서 기대 비 작동시간임.

또한 PFD보다 더 모호하여 논란이 되고 있었던 PFH는 $w(t)$가 비조건부 고장강도(unconditional failure intensity)나 고장빈도일 때 위험고장의 평균 빈도인 식 (2)로 정의하면서,

$$PFH(T_1) = \frac{\int_0^{T_1} w(t)dt}{T_1} \tag{2}$$

하나의 안전 방벽(safety barrier)이 작동하는 연속 작동모드일 때는 단위시간 당 불신뢰도인 식 (3)으로,

$$PFH(T_1) = \frac{1-\exp(-\int_0^{T_1} \Lambda(t)dt)}{T_1} = \frac{F(T_1)}{T_1} \tag{3}$$

여기서 $\Lambda(\cdot)$는 순간 고장률, $F(\cdot)$는 불신뢰도임.

$\Lambda(t)$가 시간에 대해 일정하지 않고 의존할 때는 평균 고장률(AF)을 이용하여 근사적으로 다음과 같은 보충적인 정의를 하고 있다.

$$PFH(T_1) = \frac{1-\exp(-AF \cdot T_1)}{T_1} \approx AF$$

그리고 다수의 안전 방벽이 작동하는 높은 작동모드 일 때는 극한 가용도를 이용하여 다음과 같이 정의하고 있다.

$$PFH = \frac{1}{MUT+MDT} \approx \frac{1}{MUT}$$

여기서 MUT와 MDT는 평균 작동시간과 평균 비 작동시간임.

PFH보다 널리 쓰이는 PFD에 대해 IEC 61508(2000, 2010)는 한 채널(구성품)의 비 검출 위험고장률과 검출 위험고장률이 각각 λ_{DU}, λ_{DD} 일 때, 식 (4)와 같이 정의하고 있다.

$$PFD = (\lambda_{DU}+\lambda_{DD})t_{CE} \tag{4}$$

여기서 $t_{CE} = \frac{\lambda_{DU}}{\lambda_{DU}+\lambda_{DD}}\left(\frac{T_1}{2}+MRT\right)+\frac{\lambda_{DD}}{\lambda_{DU}+\lambda_{DD}}MTTR$, MRT과 MTTR은 평균 수리시간(Mean Repair Time)과 평균 회복시간(Mean Time to Restoration)임.

일반적으로 MRT, $MTTR$은 T_1보다 상당히 작으므로 비검출 위험고장률 λ_{DU}만 고려하고, λ_{DD}, MRT, $MTTR$을 무시해도 이론의 전개에는 무리가 없다. 또한 공통원인고장을 고려하는 경우는 제 3장에서 다룬다.

IEC 61508 2판(2010) Part 6 Annex B에서 다루고 있는 N중 M 구조($N \le 3$, $M \le 3$)에 대해 제공하고 있는 PFD(이하 IEC 표준 근사식)에 대한 근거를 다음과 같이 유추할 수 있다.

$$\begin{aligned} PFD_{MooN} &= \text{고장상태로 들어가는 빈도} \\ &\quad \times \text{고장상태에 머무는 기대시간} \\ &= \nu_{MooN} \times MDT_{MooN} \end{aligned} \tag{5}$$

N중 M 구조에서 고장상태로 들어가는 빈도는 $(N-M)$개가 이미 고장이 난 상태이고 남아있는 $N-(N-M)$개 중에서 $(N-M+1)$번째 고장이 발생하는 상황이므로

$$\begin{aligned} \nu_{MooN} &= N(N-1)\cdots[N-(N-M)+1](\prod_{j=1}^{N-M}\lambda_{DU}D_j) \times M\lambda_{DU} \\ &= \frac{N!}{(M-1)!}\lambda_{DU}^{N-M+1}\prod_{j=1}^{N-M}D_j \end{aligned}$$

가 되며, 보증시험의 간격이 T_1이고 j개가 고장이 나면 그 상태에 머무는 평균 시간(D_j)은 $T_1/(j+1)$(또한, $MDT_{MooN} = D_{N-M+1}$임)로 볼 수 있으므로 N 중 M 구조에 대한 IEC 표준 PFD 근사식은 식 (6)과 같이 구한 것으로 간주할 수 있다.

$$\begin{aligned} PFD_{MooN} &= \frac{N!}{(M-1)!}\lambda_{DU}^{N-M+1}(\prod_{j=1}^{N-M}\frac{T_1}{j+1}) \times \frac{T_1}{N-M+2} \\ &= \frac{N!}{(N-M+2)!(M-1)!}\lambda_{DU}^{N-M+1}T_1^{N-M+1} \\ &= \binom{N}{N-M+1}\frac{(\lambda_{DU}T_1)^{N-M+1}}{N-M+2} \end{aligned} \tag{6}$$

식 (6)의 IEC 표준 근사식은 이 장에서 가정된 상황을 반영한 ISA-TR84.00.02(2002)와 Oliveira and Abramovitch(2010)에 의한 PFD 공식과 Rausand and Høyland(2004)가 최소절단집합의 수를 이용한 근사식과 일치한다.

또한 IEC 61508에서 N 중 M 구조의 IEC 표준 PFH 근사식은 비조건부 고장강도의 평균에 해당되는 식 (5)의 ν_{MooN}로 식 (6)으로부터 다음과 같이 설정하고 있다고 볼 수 있다.

$$PFH_{MooN} = \binom{N}{N-M+1}\lambda_{DU}^{N-M+1}T_1^{N-M} \tag{7}$$

상기와 같이 IEC 61508은 두 신뢰성 척도를 연관시키고 있으므로 본 절에서는 PFD를 주로, PFH를 부가하는 형식으로 이 식들의 근사 정확도를 조사하였다.

2.1 한 채널의 PFD

고장 발생시간을 나타내는 확률변수가 T이고 신뢰도가 $R(t)$일 때 식 (1)의 기대 비 작동시간 $MDT(T_1)$는 다음과 같이 구할 수 있으므로,

$$MDT(T_1) = 0 \times R(T_1) + (T_1 - E[T \mid T \le T_1]) \times F(T_1)$$

여기서 $E[T \mid T \le T_1] = \dfrac{-T_1 R(T_1) + \int_0^{T_1} R(t)dt}{F(T_1)}$ 임.

IEC 61508의 공식적인(official) 정의에 따른 PFD는 식 (8)에 의해 구할 수 있다.

$$PFD^{(O)} = \frac{MDT(T_1)}{T_1} = 1 - \frac{\int_0^{T_1} R(t)dt}{T_1} \tag{8}$$

IEC 61508과 같이 한 채널의 고장률을 상수로 간주할 경우 고장률이 λ_{DU}인 지수분포를 따르므로 보증시험 간격이 T_1일 때 기대 비 작동시간은 다음과 같이 구해진다.

$$\begin{aligned} MDT_{1oo1}(T_1) &= T_1 - \frac{1-\exp(-\lambda_{DU}T_1)}{\lambda_{DU}} \\ &\approx \lambda_{DU}T_1^2/2 \end{aligned}$$

상기 식의 두 번째 항은 지수함수를 테일러 급수로 2차 항까지 전개하여 근사한 값으로 IEC 표준 근사식에 사용된다. 따라서 식 (8)에 의한 정확한 PFD와 IEC 표준 근사식은 식 (9)와 같은 관계를 가진다.

$$\begin{aligned} PFD_{1oo1}^{(O)} &= \frac{MDT_{1oo1}}{T_1} = 1 - \frac{1-\exp(-\lambda_{DU}T_1)}{\lambda_{DU}T_1} \\ &\approx \lambda_{DU}T_1/2 \end{aligned} \tag{9}$$

<Figure 1>은 $\lambda_{DU} = 10^{-6}/hr$일 때 $T_1 = 2{,}000 \sim 100{,}000\,hr$범위에서 PFD에 대한 IEC 표준 근사식의 표준의 공식적 정의에 의한 정확한 값에 대한 상대오차((근사값-정확한 값)/정확한 값)를 도시한 것으로 T_1이 커질수록 상대오차가 증가하고 있다.

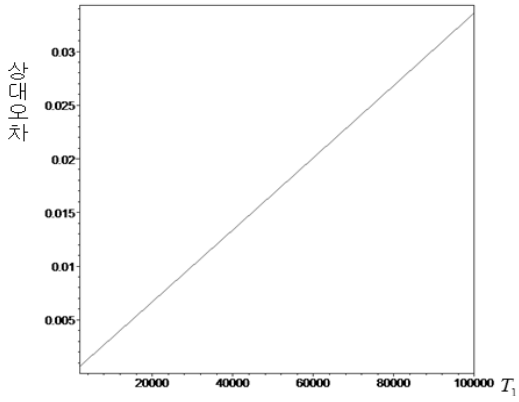

Figure 1. Accuracy of Approximate PFD Formula for a Single Channel

2.2 N 중 M 구조의 PFD

각 부품의 고장률 λ_{DU}가 동일하고 독립일 때 N 중 M 구조의 신뢰도는 식 (10)이 된다.

$$R_{MooN}(t) = \sum_{j=M}^{N} \binom{N}{j} e^{-j\lambda_{DU}T_1}(1-e^{-\lambda_{DU}T_1})^{N-j} \tag{10}$$

이를 식 (8)에 대입하면, N 중 M 구조에 대해 표준의 공식적 정의에 의한 PFD는 다음과 같이 구할 수 있다.

$$PFD_{MooN}^{(O)} = \frac{MDT_{MooN}(T_1)}{T_1} = 1 - \frac{\int_0^{T_1} R_{MooN}(t)dt}{T_1}$$

<Figure 2>와 <Figure 3>에는 $\lambda_{DU} = 10^{-6}/hr$이고 각각 $N=2$와 $N=3$일 때 $T_1 = 2{,}000 \sim 100{,}000hr$ 범위에서 IEC 61508에서 다루고 있는 구조의 상대오차를 도시하고 있는데 $N=3$일 때가 오차가 더 크며, 상대오차가 10%를 초과하는 경우도 있어 사용 시 주의가 필요하다. 다만 IEC 표준 근사식은 조사된 모든 경우에 PFD를 과대평가하고 있으므로 SIS의 성격을 고려하면 안전적인 근사법으로 볼 수 있다.

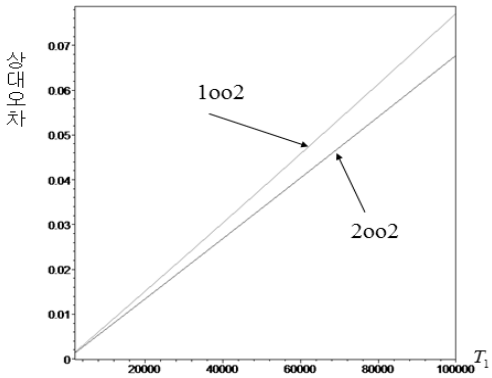

Figure 2. Accuracy of Approximate PFD Formula for Moo2 Architecture

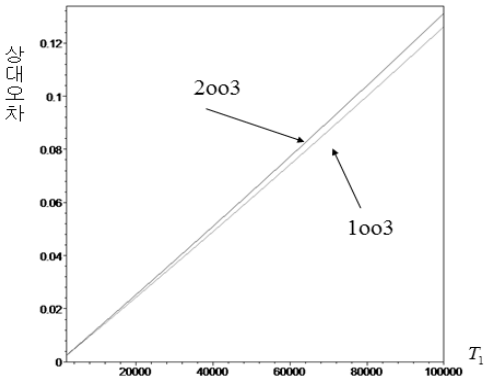

Figure 3. Accuracy of Approximate PFD Formula for Moo3 Architecture

2.3 한 채널의 PFH

PFH는 식 (3)의 신뢰도만 고려한 경우로 한정하면 다음과 같이 정의되므로 보증시험의 간격이 T_1일 때 높은 또는 연속 요구 작동모드에서 IEC 61508의 공식적인 정의에 의한 PFH는 식 (11)이 된다.

$$PFH^{(O)} = \frac{F(t)}{T_1} = \frac{1-e^{-\lambda_{DU}T_1}}{T_1} \tag{11}$$

상기 식에서 지수항을 1차 항까지 테일러 급수로 전개하면 IEC 표준 근사식인 λ_{DU}가 된다.

$\lambda_{DU} = 10^{-6}/hr$일 때 $T_1 = 0 \sim 10{,}000hr$범위에서 대응되는 표준의 공식적 정의인 식 (10)에 따라 계산된 값에 대한 IEC 표준 근사식에 의한 PFH의 상대오차가 <Figure 4>에 도시되어 있다. 즉, 낮은 요구 작동모드로 접근해 감에 따라 상대오차가 커지고 있다.

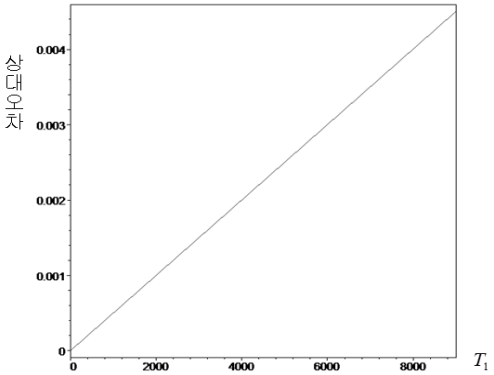

Figure 4. Accuracy of Approximate PFH Formula for a Single Channel

2.4 N 중 M 구조의 PFH

각 부품의 고장률 λ_{DU}가 동일하고 독립일 때 N 중 M 구조의 신뢰도가 식 (10)과 같이 주어지므로 N 중 M 구조의 정확한 PFH는 식 (11)으로부터, IEC 표준 근사식은 식 (7)로부터 구할 수 있다.

$\lambda_{DU} = 10^{-6}/hr$일 때 $T_1 = 0 \sim 10{,}000hr$범위에서 IEC 61508에서 다루고 있는 대표적인 N 중 M 구조에 대해 IEC 표준 근사식의 정확도를 나타내는 상대오차 값이 <Figure 5>와 <Figure 6>에 도시되어 있는데, PFD보다 오차가 작은 편이며, PFD와 마찬가지로 과대평가를 하고 있어 보수적인 근사법이 된다.

3. 공통고장방식을 수용한 신뢰성 평가 척도

공통원인고장에 대한 신뢰성 모형은 30여년 전 원자력 발전 산업에서 발전되었는데, 최근 들어 공표된 IEC 61508의 SIL 수준 결정에도 중대한 영향을 미치고 있다.

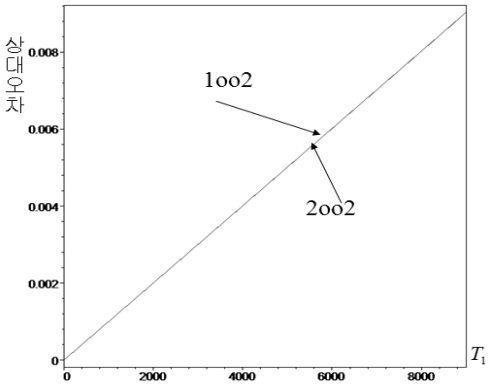

Figure 5. Accuracy of Approximate PFH Formula for Moo2 Architecture

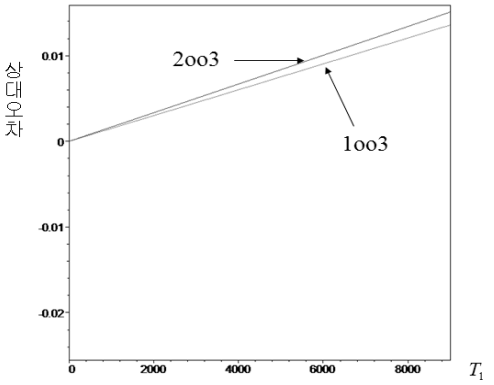

Figure 6. Accuracy of Approximate PFH Formula for Moo3 Architecture

CCF에 대한 정의는 여러 가지 있지만 이 중에서 Rausand and Høyland(2004)는 동시 또는 짧은 시간 구간 내에 공유하는 원인에 의해 둘 이상의 채널 고장을 초래하는 종속적 고장으로, IEC 61508(2000, 2010)]에서는 하나 이상의 사건으로 인해 다중 채널시스템에서 둘 이상의 채널 고장을 유발하여 시스템의 고장을 초래하는 고장으로 정의하고 있다.

CCF의 모형으로는 정확도는 높지만 실용성이 떨어지는 기본모수(basic parameter) 모형과 반대로 가장 간편하지만 정확성의 손실을 초래하는 베타인자 모형까지 다양하다(Mosleh *et al.*, 1998; Hoepfer *et al.*, 2009).

IEC 61508의 1판(2000)에서는 베타인자 모형을 채택하고 있으며, 2판(2010)에서는 베타인자 모형 외에 이를 확장한 Hokstad *et al.*(2004, 2006)의 다중 베타인자(MBF) 모형과 Altwood(1986)와 Mosleh *et al.*(1988) 등에 소개된 충격모형인 이항 고장률모형을 Part 6 Annex D에 기술하고 있다. 여기서 충격의 수가 4를 초과할 때는 이항고장률 모형을 추천하고 있는데, 본 논문에서는 N 중 M 구조에 유용한 다중 베타인자 모형을 대상으로 삼고자 한다.

가장 단순하고 널리 쓰이는 베타인자 모형은 CCF가 기여하는 고장률을 공통 고장률(λ_0)에 대한 비율을 β로 설정하고 CCF가 발생되면 모든 시스템 내 채널이 모두 고장이 난다고 가정하고 있어 N 중 M 구조의 특성을 반영하지 못하는 등 실제와 맞지 않는 경우가 자주 발생된다. 이를 개선한 MBF 모형은 CCF에 의해 모든 채널 고장이 발생한다는 조건을 완화하여 2 채널, 3 채널 고장 등 CCF에 의한 고장 채널 수에 따른 조건부 확률을 도입한 다중 그리스 문자(Multiple Greek Letter; MGL)모형과 유사하지만 보다 간편하게 N 중 M 구조에 적용할 수 있는 장점을 가지고 있다. MBF 모형을 도입하여 SIS에 적용할 수 있도록 Hauge *et al*.(2006, 2010a, 2010b)의 PDS법이 개발되어 있다.

3.1 다중 베타인자 모형

Hokstad *et al*.(2004, 2006)이 제안한 다중 베타인자 모형은 N 중 M 구조일 때 식 (11)의 형상계수(configuration factor) C_{MooN}을 도입하여 CCF가 기여하는 고장률을 다음과 같이 정의하고 있다.

$$\lambda_{MooN} = C_{MooN} \cdot \beta\lambda_0 \tag{12}$$

여기서 β는 두 채널 이상의 공통고장을 유발하는 베타인자, λ_0는 각 채널의 CCF에 의한 기여 고장률 산정하는데 필요한 공통 고장률임.

MBF 모형에서 C_{1oo2}는 1이 되므로 두 채널일 경우는 베타인자 모형과 같아진다. 이 모형에서 C_{MooN}을 구하기 위해 β_j를 채널 $1, 2, \cdots, j$가 CCF에 의해 고장이 발생했을 때 채널 $j+1$에 고장이 발생할 확률 $\Pr(A_{j+1}|A_1 \bigcap \cdots \bigcap A_j)$로 정의하는데, 여기서 $\beta_1 = \beta$가 된다.

<Figure 7>은 $N=3$인 경우로 각 채널의 고장률이 λ_0로 동일하다면 각 채널의 독립 고장률은 $[1-(2-\beta_2)\beta]\lambda_0$, 특정 두 채널만 CCF에 의한 발생 고장률은 $(1-\beta_2)\beta\lambda_0$, 세 채널 모두 CCF에 의해 발생하는 고장률은 $\beta_2\beta\lambda_0$가 된다. 여기서 $\beta_2 = 1$이면 베타인자 모형이 되며, 전술한 MGL 모형은 β_2에 해당되는 γ를 최소한 하나의 다른 채널에 의해 고장이 발생한 채널이 최소한 두 추가 채널과 CCF를 공유할 조건부 확률로 정의하므로, 특정 두 채널만 CCF에 의한 발생 고장률은 $(1-\gamma)\beta\lambda_0/2$가 되어 MBF 모형과 다르게 정의되지만, 세 채널 모두 CCF에 의해 발생하는 고장률은 $\gamma\beta\lambda_0$로 동일한 형태가 되는 차이점이 있다.

C_{MooN}을 도출하기 위해 N개 중에서 j개의 채널이 CCF에 의해 고장이 발생할 확률은 다음과 같이 정의한다.

$$g_{j,N} = \Pr(A_1 \bigcap A_2 \bigcap \cdots \bigcap A_j \bigcap \overline{A_{j+1}} \bigcap \cdots \bigcap \overline{A_N})$$

여기서 $\overline{A_j}$ 는 채널 j가 CCF에 의해 고장이 발생되지 않을 확률임.

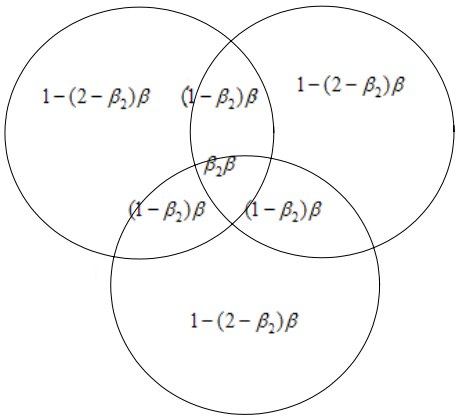

Figure 7. Multiple Beta Factor Model : $N=3$

따라서 CCF에 의해 N채널 중에서 j개 채널만 고장이 날 확률은 다음과 같이 계산된다.

$$f_{j,N} = \binom{N}{j} g_{j,N}$$

N 중 M 구조가 CCF에 의해 고장이 날 확률 Q_{MooN}은 각 채널 확률이 Q로 동일할 때 최소한$(N-M+1)$ 채널이 고장이 발생해야 되므로 형상계수와 베타인자를 도입하여 식 (13)과 같이 적을 수 있다.

$$Q_{MooN} = \sum_{j=N-M+1}^{N} f_{j,N} = C_{MooN}\beta Q \tag{13}$$

Hokstat *et al*.(2006)은 포함-제외 원리를 이용하여 C_{MooN}을 식 (14)와 같이 구하고 있다.

$$C_{MooN} = \sum_{j=N-M+1}^{N} \binom{N}{j} \frac{g_{j,N}}{Q\beta} = \sum_{j=N-M+1}^{N} \binom{N}{j} \sum_{i=0}^{N-j} (-1)^i \times \binom{N-j}{i} \prod_{l=2}^{j-1+i} \beta_l, \ M = 1, 2, \cdots, N \tag{14}$$

단, $\prod_{l=2}^{1} \beta_l = 1$로 정의 됨.

3.2 PDS 방법

PDS(Reliability of Computer Based Safety System에 해당되는 노르웨이어의 약명) handbook은 스칸디나비아 지역에서 가장 큰 독립 연구소인 노르웨이의 STNTEF에서 주도한 SIS의 안전 비가용도에 관한 방법론과 데이터를 수록한 것으로 정유회사, 엔지니어링 기업, 컨설턴트, 벤더, 연구자들이 PDS 포럼에 참여하고 있다. PDS 방법은 1998년 처음으로 발간되었으며, IEC 61508, 61551같은 SIS의 기능안전성에 관한 주요 국제표준에 맞추어 최근 개정판이 2010년에 출간되었다.

Hokstat *et al*.(2006)의 연구결과를 중심하게 반영하고 있는 PDS-2006(Hauge *et al*., 2006)은 C_{MooN}을 식 (14)보다 단순화하여 ($\beta_l = \theta,\ l \geq 3$) 식 (15)와 같이 구하고 있으며 $\beta_2 = 0.3,\ \theta = 0.5$으로 설정한 형상계수 값을 채택하고 있다(<Table 2> 참고).

$$C_{MooN} = \beta_2 \sum_{j=N-M+1}^{N} \binom{N}{j} \theta^{j-3} (1-\theta)^{N-j}, \quad (15)$$
$$M = 1, 2, \cdots, N-2$$
$$C_{(N-1)ooN} = \binom{N}{2}\left(1 - \frac{\beta_2}{\theta}\right) + \sum_{j=2}^{N} \binom{N}{j} \theta^{j-3} (1-\theta)^{N-j}$$

최근의 PDS-2010(Hauge *et al*., 2010b)은 식 (15)보다는 식 (14)을 채택하여 <Table 2>와 같은 형상계수를 추천하고 있다. 이 표 값들로부터 β값들을 유추해보면 $\beta_2 = 0.5,\ \beta_3 = 0.6,\ \beta_4 = 0.7,\ \beta_5 = 0.8,\ \beta_6 = 0.9,\ \beta_l = 1,\ l \geq 7$로 설정하고 있는 것으로 보인다. PDS-2010의 형상계수 값이 보다 합리적으로 오름 순의 β값을 채택하고 있어 보다 현실 부합도가 높아 보이며, $N = 6, 7, 8$인 경우를 추가하고 있다.

그러나 <Table 2>에 수록된 IEC61508 2판(2010)의 형상계수 값은 PDS-2010보다 작은 값을 채택하고 있는데, 표준에서 이의 근거로 Hokstat *et al*.(2006)을 인용하고 있지만 <Figure 7>에 대입하면 특정 채널에서 이를 포함하는 두 채널과 세 채널의 CCF에 의한 고장확률(각각 $\beta/3,\ \beta/2$)의 합이 β가 되지 않으므로 어떤 근거로 작성되었는지 파악이 힘들다.

또한 개별 채널의 독립 고장률을 PDS-2006에서는 <Figure 7>의 독립고장률과 일치하도록 식 (16)와 같이 CCF 기여분을 차감하여 구하고 있으며(Hauge *et al*., 2006; Lilleheier, 2008), PDS-2010(Hauge *et al*., 2010a)에서는 CCF에 의한 기여분을 차감하지 않고 독립고장률을 개별 채널의 고장률로 그대로 쓰고 있다. 한편 IEC 61508 2판(2010)에는 베타인자 모형에 의한 고장률을 차감하고 있지만 MBF 모형을 적용할 경우에는 언급이 없다.

$$\lambda_{ind} = (1 - H_N \beta)\lambda_0 \quad (16)$$

단, $H_N = \dfrac{\sum_{j=1}^{N-1} C_{jooN} + C_{N-1ooN}}{N}$.

여기서 H_N은 다음과 같은 과정으로 구한 것으로 해석된다. N채널 중 중 정확히 $N-j$채널이 고장이 날 때 형상계수는 $C^*_{(N-j)ooN} = C_{(N+1-j)ooN} - C_{(N-j)ooN}$이 되므로, <Figure 7>에서 두 채널 이상이 공유하는 영역과 경우의 수를 고려하여 식 (16)의 H_N을 다음과 같은 근거로 설정했다고 볼 수 있다.

Table 2. Numerical Values of Configuration Factors for MooN Architecture

M	출처	N = 2	N = 3	N = 4	N = 5	N = 6	N = 7	N = 8
1	IEC 61508	1.0	0.5	0.3	0.2			
	PDS-2006	1.0	0.3	0.15	0.08	0.04		
	PDS-2010	1.0	0.5	0.3	0.21	0.17	0.15	0.15
2	IEC 61508		1.5	0.6	0.4			
	PDS-2006		2.4	0.75	0.45	0.26		
	PDS-2010		2.0	1.1	0.7	0.4	0.27	0.15
3	IEC 61508			1.75	0.8			
	PDS-2006			4.0	1.2	0.83		
	PDS-2010			2.9	1.8	1.1	0.8	0.6
4	IEC 61508				2.0			
	PDS-2006				6.0	1.6		
	PDS-2010				3.7	2.4	1.6	1.1
5	IEC 61508							
	PDS-2006					8.1		
	PDS-2010					4.3	3.0	2.1
6	IEC 61508							
	PDS-2006							
	PDS-2010						4.8	3.5
7	IEC 61508							
	PDS-2006							
	PDS-2010							5.3

$$H_N = \sum_{j=2}^{N-1} \frac{\binom{N-1}{j-1} C^*_{(N-j)ooN}}{\binom{N}{j}} + C_{1ooN}$$
$$= \frac{\sum_{j=2}^{N-1} j(C_{(N+1-j)ooN} - C_{(N-j)ooN}) + NC_{1ooN}}{N}$$
$$= \frac{\sum_{j=1}^{N-1} C_{jooN} + C_{N-1ooN}}{N}$$

3.3 적용상의 문제점

N 중 M 구조일 경우 형상계수를 도입한 다중 베타인자 모형을 적용하더라도 실제 적용 시에 다음과 같은 난점이 발생된다.

첫째, 각 채널의 고장률이 다를 경우가 일반적인데, 다중 베타인자모형은 채널이 동일한 고장률을 가정하고 있다. IEC 61508 2판(2010)에는 이에 대한 명확한 언급이 없으며, PDS법은 각 고장률의 기하평균을 추천하고 있다. 이럴 경우 시스템의 신뢰도는 고장률이 가장 큰 채널에 영향을 많이 받으므로 기하평균보다는 산술평균이 보다 더 의미가 있을 수 있다. 또한 식 (17)과 같이 서브시스템이나 시스템의 평균 고장률 $AF(T_1)$을 구하여 이용하는 것이 합리적일 수 있으므로 이의 타당성을 제 4장의 적용예제에서 검토하고자 한다.

$$AF(T_1) = \frac{\int_0^{T_1} \Lambda(t)dt}{T_1} = \frac{-\ln(R(T_1))}{T_1} \tag{17}$$

둘째 IEC 61508에는 각 채널의 보증시험 간격이 다를 경우의 접근법에 대한 기술도 없다. PDS 방법은 각 채널에 대한 보증시험 간격의 산술 평균을 추천하고 있다.

셋째 서브시스템에 N 중 M 구조가 들어 있는 경우나 둘 이상의 혼합구조로 볼 수 있는 시스템에 대한 접근방법도 명시되어 있지 않다.

마지막으로 PFD나 PFH를 계산 시 IEC 61508 2판(2010)의 Part 6 Annex B에는 다중 베타인자 모형이 아닌 베타인자 모형에 의해서 도출된 식을 제공하고 있다. 즉, 다중 베타인자 모형을 채택 시 이를 어떻게 고려해야 하는지 구체적인 기술이나 참고 예제가 없다.

본 논문은 둘째를 제외한 세 가지 상황을 검토할 수 있는 다음 절의 예제를 대상으로 어떻게 이런 난점을 해소해야 되는지를 예시하였다.

4. 적용 예제

<Figure 8>의 대상 예제는 Lilleheier(2008)가 다룬 것으로 윤활유 압력이 낮은지를 검출하는 시스템으로 감지(sensor) 서브시스템은 4개의 구성품으로 구성되어 있으며, 논리(logic) 서브시스템과 구동 서브시스템(actuator)은 분석에서 제외한다. 구성품 1은 압력 검출기이고 구성품 2는 압력 스위치인데 병렬로 연결되어 있으며 내부(inner) 서브시스템으로 명명한다. 이 시스템은 내부 서브시스템과 압력 스위치에 해당되는 동일한 고장률을 가지는 구성품 3과 4중에서 윤활유 압력이 낮다는 경고를 2개 이상 받으면 시스템을 정지시킨다.

대상 시스템은 1년에 1회(즉, $T_1 = 8{,}760hr$) 보증시험을 실시하며, 각 구성품의 고장률은 다음과 같고, CCF 고장비율인 β는 0.05로 알려져 있다. 또한 이 예제는 구성품 고장률이 다를 뿐만 아니라 병렬구조를 가진 서브시스템이 내부에 존재하는 3중 2구조이다.

$$\lambda_1 = 1.7 \times 10^{-6} hr^{-1}$$
$$\lambda_2 = 6.0 \times 10^{-6} hr^{-1}$$
$$\lambda_3 = \lambda_4 = 3.4 \times 10^{-5} hr^{-1}$$

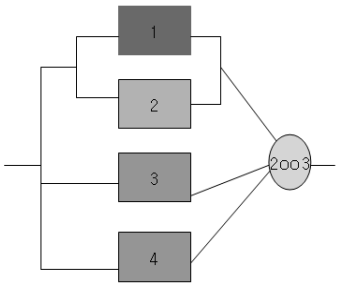

Figure 8. Block Diagram of a System to Detect Low Oil Pressure

4.1 CCF를 고려하지 않는 경우

먼저 CCF가 없다고 가정할 경우의 이 시스템의 신뢰도 함수는 식 (18)과 같이 구할 수 있다.

$$R(t) = 2R_{inner}(t)e^{-\lambda_3 t} + e^{-2\lambda_3 t} - 2R_{inner}(t)e^{-2\lambda_3 t} \tag{18}$$

여기서 $R_{inner}(t) = e^{-\lambda_1 t} + e^{-\lambda_2 t} - e^{-(\lambda_1+\lambda_2)t}$임.

베타와 다중 베타 모형을 CCF에 도입 시 식 (12)의 공통 고장률 λ_0을 먼저 구해야 한다.

본 예제와 같이 각 구성품의 고장률이 다를 경우에 CCF에 의한 기여 고장률 산정방법에 대해 IEC 61508에는 명시된 절차가 없으나 PDS 방법에는 각 고장률의 기하평균을 채택하여 적용하고 있다.

공통의 동일한 고장률로 기하평균도 의미가 있지만 PDS 방법에서 특별히 근거를 제시하지 못하고 있다. 따라서 본 논문에서는 제 3.3절에서 언급한 바와 같이 기하평균 외에 산술평균과 평균 고장률 등을 서브시스템을 감안하여 적용하고 비교하였다.

먼저 가장 단순한 방법으로 내부 서브시스템을 무시하고 기하평균을 구한 것을 $\lambda_0^{(1)}$(<Table 3> 참고)로, 두 번째로 내부 서브시스템의 기하평균을 먼저 구한 다음에 3중 2구조의 기하평균을 구한 값이 $\lambda_0^{(2)}$이다.

$$\lambda_0^{(2)} = (\sqrt{\lambda_1\lambda_2}\,\lambda_3^2)^{1/3} = 1.55\times10^{-5}$$

또한 $T_1 = 8{,}760hr$일 때 내부 서브시스템의 평균 고장률을 구한 후 이를 하나의 구성품으로 간주하여 3중 2구조에 대해 기하평균을 적용하여 구할 수 있다.

$$AF_{inner}(t) = \frac{-\ln(R_{inner}(8{,}760))}{8{,}760} = 0.864\times10^{-7}$$
$$\lambda_0^{(3)} = (AF_{inner}(8{,}760)\lambda_3^2)^{1/3} = 0.464\times10^{-5}$$

그리고 $\lambda_0^{(i)},\ i=1,2,3$에 기하 평균 대신 산술 평균을 적용한 공통 고장률을 $\lambda_0^{(i)},\ i=4,5,6$으로 표기한다. 마지막으로 4 구성품 고장률의 최대값을 공통 고장률로 산정한 것을 $\lambda_0^{(7)}$로, 3중 2구조의 신뢰도인 식 (18)을 이용하여 다음과 같이 시스템의 평균 고장률을 구한 결과가 $\lambda_0^{(8)}$이 된다.

$$\lambda_0^{(8)} = \frac{-\ln(R(8{,}760))}{8{,}760} = 0.787\times10^{-5}$$

$\lambda_0^{(j)}$ 중 5종을 T_1에 대해 도시한 것이 <Figure 9>이다. 이를 보면 T_1에 의존하는 세 가지 λ_0 중에서 $\lambda_0^{(6)}$은 $\lambda_0^{(3)}$이나 $\lambda_0^{(8)}$과 달리 빠르게 안정된 값으로 수렴됨을 파악할 수 있다.

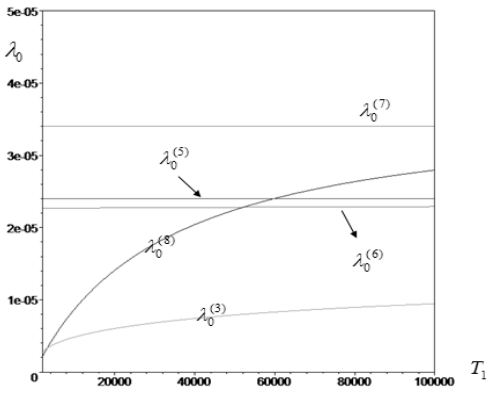

Figure 9. Comparison of Methods to Calculate Common Cause Failure Rate: $\lambda_0^{(i)},\ i=3,5,6,7,8$

여기서 CCF를 고려하지 않을 경우에 보다 수월하게 대상 예제의 시스템 신뢰도를 구할 수 있으므로 먼저 식 (8)에 대입하여 IEC 61508의 공식적 정의에 의해 PFD($PFD^{(O)}$)를 계산하여 $\lambda_0^{(i)}$의 우월성을 비교할 수 있다. 즉, 제시된 8가지 공통 고장률 산정방식에 따라 PFD를 계산하여 $PFD^{(O)}$와 비교함으로써 이들의 우월성을 평가할 수 있다.

또한 현 대상 예제는 4중 2구조와 4중 2구조가 혼합되어 있는데, 예를 들면 4구성품 중 2개만 작동하는 6가지 중 1과 2만 작동하는 경우에 시스템은 고장으로 판정이 나므로 4중 3구조에 해당된다. 따라서 이 구조에서 서브시스템을 하나의 구성품으로 간주하여 3중 2구조로 볼 수도 있으며, 4중 2 구조와 4중 3구조의 혼합 형태로 간주할 수도 있으므로 IEC 61508이 제공하는 PFD 근사식 (6)을 이용하여 먼저 3중 2구조에 의한 PFD를 식 (19)와 같이 구한다. 또한 4중 2구조와 4중 3구조의 PDF를 선형보간하여 현 시스템의 PDF를 식 (19)의 두 번째 식과 같이 구할 수 있다(Lilleheier, 2008; Hauge *et al.*, 2010b). 여기서 CCF가 없는 경우이므로 β는 0이고 T_1은 8,760시간이다.

3중 2구조 :

$$PFD_{2oo3} = 6[(1-\beta)\lambda_0]^2(T_1/2)(T_1/3) + \beta\lambda_0(T_1/2) \qquad (19)$$

4중 2와 4중 3의 혼합구조

$$PFD_{2/3oo4} = \frac{5}{6}PFD_{2oo4} + \frac{1}{6}PFD_{3oo4}$$

단,

$$PFD_{2oo4} = 6[(1-\beta)\lambda_0]^3(T_1/2)(T_1/3)(T_1/4) + \beta\lambda_0(T_1/2)$$
$$PFD_{3oo4} = 12[(1-\beta)\lambda_0]^2(T_1/2)(T_1/3) + \beta\lambda_0(T_1/2).$$

<Table 3>을 보면 기하 평균보다는 산술평균에 의한 산정법이 우수하며, 혼합구조로 간주할 때가 3중 2구조보다 작은 값이 도출되고 있다. 최대 고장률과 평균 고장률을 채택한 경우는 IEC 61508의 공식적 정의에 의한 값과 거리가 있으며 8가지 산정법 중 혼합구조로 구한 $\lambda_0^{(5)}$와 $\lambda_0^{(6)}$이, 3중 2구조로 구한 $\lambda_0^{(4)}$가 공식적 정의에 비교적 가까운 값을 도출하고 있다.

Table 3. Comparison of PFD by Methods to Calculate Common Cause Failure Rate

산정 방법			3중 2구조	4중 2와 4중 3의 혼합구조
공식적 정의			0.0239	
기하 평균	$\lambda_0^{(1)}$	1.04×10^{-5}	0.00833	0.00341
	$\lambda_0^{(2)}$	1.55×10^{-5}	0.0183	0.00818
	$\lambda_0^{(3)}$	0.464×10^{-5}	0.00165	0.000607
산술 평균	$\lambda_0^{(4)}$	1.89×10^{-5}	0.0275	0.0130
	$\lambda_0^{(5)}$	2.40×10^{-5}	0.0440	**0.0224**
	$\lambda_0^{(6)}$	2.27×10^{-5}	0.0395	**0.0197**
최대 고장률	$\lambda_0^{(7)}$	0.34×10^{-5}	0.0887	0.0516
평균 고장률	$\lambda_0^{(8)}$	0.787×10^{-5}	0.00476	0.00126

예제와 같이 내부 서브시스템이 없을 때는 $\lambda_0^{(5)}$와 $\lambda_0^{(6)}$은 동일한 형태가 되고, 또한 $\lambda_0^{(6)}$은 <Figure 9>에서 수렴속도가 빠르다.

따라서 CCF를 고려할 경우에 서브시스템이 포함된 대상 예제에 보다 적합한 산정법에 속하는 혼합구조에 대한 $\lambda_0^{(5)}$와 $\lambda_0^{(6)}$<(Table 3>에서 굵게 표시된 곳)을 추천하여 적용한다.

4.2 베타인자 모형

IEC 61508 1판과 2판에서 제공된 공식(식 (19)의 두 번째 식)에 $\lambda_0^{(5)}$, $\lambda_0^{(6)}$과 $\beta = 0.05$을 대입하여 구한 PFD는 다음과 같이 계산된다.

$$\text{4 중 2와 4 중 3의 혼합구조}: PFD_{2/3oo4}^{(5)} = 0.0251$$
$$\text{4 중 2와 4 중 3의 혼합구조}: PFD_{2/3oo4}^{(6)} = 0.0225$$

CCF를 고려하지 않는 Table 3의 결과와 비교하면 PFD 값이 약간 커짐을 알 수 있다.

4.3 다중 베타인자 모형

각 구성품이 고장률이 다를 경우에 CCF에 의한 기여 고장률 산정방법에 대해서는 전절에서 추천된 두 가지 방법을 적용하고, 형상계수는 근거가 모호한 IEC 61508의 2판(2010)보다는 PDS-2010에서 제공된 값을 적용하고자 한다. 또한 독립 고장률도 CCF가 기여하는 고장률을 차감하는 IEC 61508과의 부합도가 높은 PDS-2006 절차를 따른다.

여기서 형상계수는 2중 1구조로 된 서브시스템이 포함되어 있으므로 표에서 직접 구할 수 없으며 조정이 필요하다. 즉, 현 대상 예제는 4중 2구조와 4중 3구조가 혼합되어 있는데, 4구성품 중 정확히 2개가 고장이 발생할 경우의 형상계수는 다음과 같이 구해진다.

$$C_{2oo4}^{*} = C_{3oo4} - C_{2oo4} = 2.9 - 1.1 = 1.8$$

따라서 대상 예제의 형상계수는 다음과 같이 설정할 수 있다.

$$\begin{aligned} C_{2/3oo4} &= C_{2oo4} + C_{2oo4}^{*}\Pr(\text{시스템 고장} \mid \text{2구성품만 작동}) \\ &= 1.1 + 1.8 \times \frac{1}{\binom{4}{2}} = 1.4 \end{aligned}$$

대상 시스템은 4중 2와 4중 3구조에서 4중 2구조에 가까운 형태인데, Hauge *et al.*(2010a)이 PDS-2010을 예제(Example 2)에 적용한 방법을 따르면 4중 3구조의 형상계수보다 커지므로 타당성이 의심되며, Lilleheier(2008)가 적용한 선형보간법이 상기 결과와 일치한다.

위와 같이 계산된 형상계수로부터 PDS-2006에서 제시된 각 구성품의 독립 고장률에 곱해지는 계수는 식 (16)으로부터 다음과 같이 계산된다.

$$H_N = \frac{0.3 + 1.1 + 2.9 + 2.9}{4} = 1.8$$
$$\lambda_{k,ind} = (1 - 0.05H_N)\lambda_0, \quad k = 1, 2, 3, 4$$

따라서 전 소절의 베타인자 모형에서 가장 근접한 값을 제공하여 추천된 $\lambda_0^{(5)}$와 $\lambda_0^{(6)}$을 이용하여 이 혼합구조에 대한 MBF를 고려한 PFD는 다음 식을 식 (19)에 대입하여 구하면 된다.

$$\begin{aligned} PFD_{2oo4} &= 6[(1 - H_N\beta)\lambda_0]^3(T_1/2)(T_1/3)(T_1/4) \\ &\quad + C_{2/3oo4}\beta\lambda_0(T_1/2) \\ PFD_{3oo4} &= 12[(1 - H_N\beta)\lambda_0]^2(T_1/2)(T_1/3) \\ &\quad + C_{2/3oo4}\beta\lambda_0(T_1/2) \end{aligned}$$

MBF 모형과 PDS-2006의 독립 고장률 산정 방법을 적용하여 구한 PFD는 다음과 같다.

$$\text{4중 2와 4중 3의 혼합구조}: PFD_{2/3oo4}^{(5)} = 0.0289$$
$$\text{4중 2와 4중 3의 혼합구조}: PFD_{2/3oo4}^{(6)} = 0.0225$$

CCF 모형으로 MBF를 고려할 때 베타인자를 채택할 경우와 비교하면 PFD값에 약간의 차이가 발생된다. 두 모형의 우월성 비교에는 엄밀한 이론적 및 실제 현장 자료에 의한 검증이 필요하지만 MBF 모형이 보다 실제 현상을 잘 반영한 확장된 모형이므로 이에 의한 PFD 계산이 더 유용할 것으로 예견된다.

5. 결 론

2011년 11월에 자동차에 대한 기능안전성 국제표준인 ISO 26262 (2011)이 공표된 이후 국내 산업계에서 이에 대한 관심이 매우 증대되고 있다. 이런 안전제어시스템의 기능안전성에 대한 모규격으로 볼 수 있는 IEC 61508이 2010년에 개정되었는데 SIL 수준 결정 등 실제 적용 시에 야기되는 난점에 대한 해결책이 명확하지 않다.

이에 따라 본 논문에서는 먼저 IEC 61508에서 요구 작동모드의 수준에 따라 PFD와 PFH으로 구별하여 표현되는 신뢰성 평가척도에 대해 해석과 대표적인 N 중 M 구조에 대해 이의 근사 정확도를 고찰하였다. 비록 표준에서 제공되는 근사공식의 정확도가 상당히 떨어지는 경우도 있지만 대체적으로 과대평가를 하고 있어 안전한 근사법으로 볼 수 있다.

더불어 SIS의 SIL 수준 결정에 중대한 영향을 미치는 공통원인고장(CCF)에 대해 IEC 61508 2판(2010)에 제시된 CCF 방법론

에 대해 고찰을 하고 실제 적용 시 일어나는 몇 가지 문제점, 예를 들면, 각 채널의 고장률이 동일하다고 가정하여 PFD와 PFH에 대한 근사적 공식을 제공하고 있는데 이보다 보편적인 각 채널이 고장률이 다를 경우에 어떻게 공식을 변형해야 되는 등을 해결할 수 있는 방안을 제시하고 이의 활용 가능성을 검토하였다. 이에 따라 CCF에 의한 기여 고장률 산정 시에 기초가 되는 공통 고장률을 산정하는 방법을 추천하였다. 또한 각 구성품이 고장률이 다르고 혼합된 N 중 M 구조를 가진 예제를 선정하여 제시된 방안을 적용하여 이의 유용성을 예시하였다.

앞으로 국내외에 제품 안전의 역할과 관심이 더욱 더 증대될 것이므로 본 논문의 결과가 기능안전성의 평가와 보급에 기여할 수 있을 것이며, 앞으로 다양한 SIS 아키텍처에 대한 공통 고장률 산정방식에 대해 광범위한 수치실험을 통해 우수한 방식을 추천하는 등의 후속연구도 요망된다.

참고문헌

Atwood C. L. (1986), The Binomial Failure Rate Common Cause Model, *Technometrics*, **28**, 139-48.

Bukowski, J. V. (2008), A Unified Model for Evaluating the Safety Integrity Level of Safety Instrumented Systems, 2008 *Proceedings of the Annual Reliability and Maintainability Symposium*, 137-142.

Hauge, S., Häbrekke, S., and Lundteigen, M. A. (2010a), *Reliability Prediction Method for Safety Instrumented Systems-PDS Example Collection*, SINTEF, A-17956, Trondheim(Norway).

Hauge, S., Hokstad, P., Langseth, H., and Øien, K. (2006), *Reliability Prediction Method for Safety Instrumented Systems-PDS Method Handbook*, SINTEF, A-06031, Trondheim(Norway).

Hauge, S., Lundteigen, M. A., Hokstad, P., and Häbrekke, S. (2010b), *Reliability Prediction Method for Safety Instrumented Systems-PDS Method Handbook*, SINTEF, A-13503, Trondheim(Norway).

Hoepfer, V. M., Saleh, J. H., and Marais, K. B. (2009), On the Value of Redundancy Subject to Common-Cause Failures: Toward the Resolution of an On-Going Debate, *Reliability Engineering and System Safety*, **94**, 1904-1916.

Hokstad, P. and Corneliussen, K. (2004), Loss of Safety Assessment and the IEC 61508 Standard, *Reliability Engineering and System Safety*, **83**, 111-120.

Hokstad, P., Maria, A., and Tomis, P. (2006), Estimation of Common Cause Factors from Systems with Different Numbers of Channels, *IEEE Transactions on Reliability*, **55**, 18-25.

IEC 61508 (2000), *Functional Safety of Electrical/Electronic/Programmable Electronic (E/E/PE) Safety Related Systems*, 1.0 ed., Part 1～7, IEC, Switzerland.

IEC 61508(2010), *Functional Safety of Electrical/Electronic/Programmable Electronic (E/E/PE) Safety Related Systems*, 2.0 ed., Part 1～7, IEC, Switzerland.

IEC 61511(2003), *IEC 61511 Standard. Functional safety-Safety Instrumented Systems for the Process Industry Sector*, Part 1～3, IEC, Switzerland.

Innal, F., Dutuit, Y., Rauzy, A., and Signoret, J. P. (2010), New Insight into the Average Probability of Failure on Demand and the Probability of Dangerous Failure per Hour of Safety Instrumented Systems, *Proc. IMechE Part O : J. Risk and Reliability*, **224**, 75-86.

ISA-TR84.00.02 (2002), *Safety Instrumented Functions (SIF)-Safety Integrity Levels (SIL) Evaluation Techniques*, Part 1～5, The Instrumentation, Systems, and Automation Society, USA.

ISO 26262 (2011), *Road Vehicles-Functional Safety*, Part 1～9, ISO, Switzerland.

Jin, H., Lundteigen, M. A., and Rausand, M. (2011), Reliability Performance of Safety Instrumented Systems: A Common Approach for Both Low-and High-Demand Mode of Operation, *Reliability Engineering and System Safety*, **96**, 365-373.

Lilleheier, T. (2008), *Analysis of Common Cause Failures in Complex Safety Instrumented Systems*, Master thesis, NTNU, Norway.

Mosleh, A., Fleming, K. N. Parry, G. W., Paula, H. M., Worledge, D. H., and Rasmuson, D. M. (1988), *Procedures for Treating Common Cause Failures in Safety and Reliability Studies*, NUREG/CR-4780, US NRC and EPI, USA, **1/2**.

Mosleh, A., Rasmuson, D. M. and Marshall, F. M. (1998), *Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment*, NUREG/CR-5485, US NRC, USA.

Oliveira, L. F. and Abramovitch, R. N. (2010), Extension of ISA TR84.00.02 PFD Equations to KooN Architectures, *Reliability Engineering and System Safety*, **95**, 707-715.

Rausand, M. and Høyland, A. (2004), *System Reliability: Models, Statistical Methods and Applications*, 2nd ed., Wiley, New Jersey(USA).

Zhang, T., Long, W., and Sato, Y. (2003), Availability of Systems with Self-Diagnostic Components-Applying Markov Model to IEC 61508-6, *Reliability Engineering and System Safety*, **80**, 133-141.

서 순 근

서울대학교 산업공학과(학사)

KAIST 산업공학과(석・박사)

현재 : 동아대학교 산업경영공학과 교수

관심분야 : 신뢰성공학 및 수명시험, 품질공학, 경제성 분석