PFD_{avg} Calculation based on Minimal Cut Set with Safety Condition

Nattawadee Thiemthummawong, Arjin Numsomran, Vittaya Tipsuwanporn *, and Twitch Chumuang

***Abstract*—Average probability of dangerous failure on demand or PFD_{avg} plays a pivotal role in reliability of SIS. However, in the previous studies, PFD_{avg} verification for redundant schemes has a limitation to apply with conditional safety function and the studies result calculates the estimated PFD_{avg} value that is not a practical value due to the error of conditional analysis. Hence, this research presents PFD_{avg} calculation which complies with IEC 61508-6 and covers safety condition by using minimal cut set. Since this set is specified from realistic requirement of safety instrumented function, the proposed new method can be applied with various redundant architectures. In conclusion, this developed method provides the solution for the conditional safety function problems and gives more accuracy PFD_{avg} value than the other methods.**

***Index Terms*— Average probability of dangerous failure on demand, Safety instrumented function, Minimal cut set, Safety condition, Nonrandom failure; IEC 61508**

I. Introduction

SAFETY instrumented system (SIS) plays a key role in reliability and safety of industrial manufacturing because this system consists of many safety instrumented functions (SIF). These functions protect production process from the hazard event which may affect to people, asset and environment. Each SIF reduce unacceptable risk of each process unit to safety or tolerable risk by functioning with safety condition that has the safety integrity level (SIL) be an indicator for functional availability.

The SIL of this function can be improved by specifying architecture in redundant schemes, and then be verified in term of average probability of dangerous failure on demand (PFD_{avg}) base on operation mode following IEC 61508/ 61511 standard [1], [2]. The operation mode includes low demand mode and high demand mode, however, general production is operated in low demand mode because the frequency of demands for operation made on SIS is no greater than one per year and no greater than twice the proof test frequency.

In SIL verification of the redundant element group, IEC 61508-6 standard [1] determines PFD_{avg} formulas for instrument with basic architecture such as 1oo1, 2oo2, 1oo2, 1oo3 and 2oo3 which these architectures is regularly applied in process. Furthermore, for architectures which are not covered in the standard are proposed by other methods e.g. Fault-tree analysis [10], Markov analysis [10], [11]. However, the results do not correspond with the standard formulas. Using system degradation [5] and general KooN (K out of N) formula [4], [7], [9] in PFD_{avg} calculation gives the result that complies with the standard. On the other hand, these methods cannot be applied with function which has nonrandom failure. The approach of Catelani M. [6], who studies the simplified procedure for PFD_{avg} analysis by using reliability block diagram (RBD) reduction, can adapt to this failure problem. Nevertheless, the formula and application of this method are incorrectly presented to practical functioning. Chung S. [3] applies RBD in grouping the common work instruments and then calculates PFD_{avg} by formula following the standard. This technique can analyze the nonrandom failure but does not have the clearly presentation procedure.

This paper proposes the developed method for PFD_{avg} analysis and calculation process using minimal cut set (MCS), which can analyze SIF functioning with nonrandom failure or safety condition properly. Moreover, the obtained result from this technique also complies with the typical standard formulas. The rest of the paper is organized as follows. Terms and assumptions are presented in section II of this paper. The developed method is applied for PFD_{avg} verification of basic architecture and case study in section III and IV respectively. In section V, the results are compared with result from the other method and discussed. Finally, conclusion is given.

II. Terms and Assumptions

TABLE I
TERMS

Abb.	Term
PFD_{avg}	Average probability of dangerous failure on demand
PFD_{IND}	Independent PFD_{avg}
PFD_{CCF}	Common cause PFD_{avg}
τ	Proof test interval
MRT	Mean time to restoration
MTTR	Mean repair time – $MTTR = MRT + Time\ to\ detect\ the\ failure$
λ_D	Dangerous failure rate – $\lambda_D = \lambda_{DU} + \lambda_{DD}$
λ_{DD}	Detected dangerous failure rate
λ_{DU}	Undetected dangerous failure rate
β	The fraction of undetected failure that have a common cause
β_D	The fraction of detected failure that have a common cause
t_i	Mean downtime of i^{th} element in voted group failure
t_{CE}	Mean downtime of 1st element in voted group failure–$t_{CE} = t_1$
t_{GE}	Mean downtime of 2nd element in voted group failure–$t_{GE} = t_2$
t_{G2E}	Mean downtime of 3rd element in voted group failure–$t_{G2E} = t_3$
DC	Diagnostic coverage – $DC = \lambda_{DD} / \lambda_D$
1ooM	1 out of M voted group
KooN	K out of N voted group

Manuscript received May 31, 2017; revised June 30, 2017.

N. T., A. J. and V. T. (*Corresponding) are with the Faculty of Engineering, King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand (e-mail: nattawadee.th@hotmail.com and vittaya.ti@kmitl.ac.th).

T. C. is with the Deputy Engineering Business, PTT Maintenance and Engineering Company Limited, Rayong, Thailand.

A. Terms

In order to understand this paper better, terms are defined as above table.

B. Assumption

For the scope limitation in PFD_{avg} calculation, basis assumption is determined as below. The further assumption can be referred in Annex B of IEC 61508-6 [1]

1) Element failure rates are constant over the life of the system.

2) All elements in voted group have the same failure rate and diagnostic coverage.

3) For each SIF, there is perfect proof testing and repair i.e. all undetected failures are detected by proof test.

4) All elements in voted group have the same single proof test interval and MRT

5) For element that has the diagnostic, undetected failure is detected and repaired within MTTR. Because of less time to detect failure, MTTR is approximately equal to MRT.

6) Failure of any element does not affect the probability in occurring failure of other element, except common cause failure (CCF).

III. PFD_{AVG} ANALYSIS AND CALCULATION

A. PFD_{avg} Analysis for 1ooM Architecture

$$PFD_{avg,1ooM} = (\lambda_{DD}\tau)^M / (M+1) \quad (1)$$

The simplified PFD_{avg} formula for 1ooM architecture is presented in [7] as (1), which assume that the element in voted group does not have diagnostic, $\lambda_D = \lambda_{DU}$, and repair time consideration and common cause failure. This formula is rewritten as (2) that consist of 3 main terms i.e. number of element, failure rate and mean downtime. These terms will be modified when assumptions change as the following.

$$PFD_{avg,1ooM} = PFD_{IND,1ooM} = M! \times (\lambda_{DU})^M \times \prod_{i=1}^{M}\left(\frac{\tau}{i+1}\right) \quad (2)$$

1) Diagnostic and repair consideration affect to failure rate, $\lambda_D = \lambda_{DU} + \lambda_{DD}$, and the added downtime for repairing. Equation (2) will be improved as (3).

$$PFD_{avg,1ooM} = PFD_{IND,1ooM} = M! \times (\lambda_{DU} + \lambda_{DD})^M \times \prod_{i=1}^{M}(t_i) \quad (3)$$

where $t_i = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{i+1} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$

2) Common cause failure consideration is discussed when voted group has 2 or more elements. β and β_D indicate the probability of common cause failure that be formulated as (4). The remain failure rate that does not include common cause failure rate is used in PFD_{avg} calculation of independent failure as (5). And PFD_{avg} formula is generated from the relationship between (4) and (5), which is expressed as (6)

$$PFD_{CCF} = \beta\lambda_{DU}\left(\frac{\tau}{2} + MRT\right) + \beta_D\lambda_{DD}MTTR \quad (4)$$

$$PFD_{IND,1ooM} = M! \times ((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD})^M \times \prod_{i=1}^{M}(t_i) \quad (5)$$

$$PFD_{avg,1ooM} = PFD_{IND,1ooM} + PFD_{CCF} \quad (6)$$

B. PFD_{avg} Calculation for Basic Architecture

TABLE II
MINIMAL CUT SET OF BASIC ARCHITECTURE

Architecture	Hardware Fault Tolerance	Minimal Cut Set
1oo1	0	{1}
2oo2	0	{1}, {2}
1oo2	1	{1, 2}
1oo3	2	{1, 2, 3}
2oo3	1	{1, 2}, {1, 3}, {2, 3}

The probability analysis of the failed element in voted group can be applied in PFD_{avg} evaluation. The element group, which occur undetected dangerous failure then the function cannot operate, is called cut set. The cut set that cannot be reduced without losing its status as cut set is called minimal cut set [8]. The minimal cut set analysis for basic architecture is shown in Table II. Suppose number in the set is tag no. of the element.

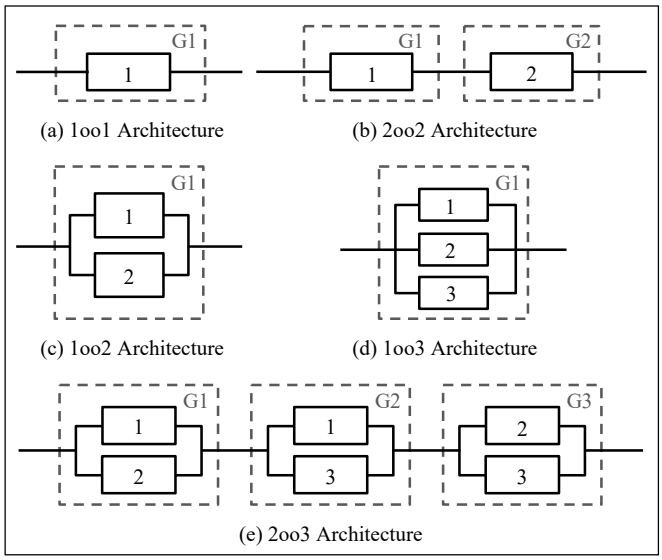

Fig. 1. Reliability block diagram from minimal cut set analysis.

The RBD can be created by the minimal cut set of architecture according to Figure 1. Block of element in the same set is in parallel and block of set in the same architecture is in series. The PFD_{avg} formulas of basic architecture can be generated by applying the RBD, (5) and (6) as Table III.

IV. CASE STUDY WITH SAFETY CONDITION

This case studies PFD_{avg} verification of the final element group i.e. safety valve. According to the process in Figure 2, two reboilers are operated for increasing temperature and product reflux to distillation column with the safety valves protection. These valves will be commanded to close at the same time by I-1 interlocking for cutting heat source when process condition is in the abnormal scenario. For this

ISBN: 978-988-14047-5-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

TABLE III
PFD_{AVG} EQUATION OF BASIC ARCHITECTURE

Architecture	Average Probability of Dangerous Failure on Demand
1oo1	$= PFD_{IND,G1} + PFD_{CCF}$ $= PFD_{IND,1oo1} + PFD_{CCF}$ $= (\lambda_{DD} + \lambda_{DU}) t_{CE}$
2oo2	$= PFD_{IND,G1} + PFD_{IND,G2} + PFD_{CCF}$ $= 2PFD_{IND,1oo1} + PFD_{CCF}$ $= 2(\lambda_{DD} + \lambda_{DU}) t_{CE}$
1oo2	$= PFD_{IND,G1} + PFD_{CCF}$ $= PFD_{IND,1oo2} + PFD_{CCF}$ $= 2((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD})^2 t_{CE} t_{GE} + \beta\lambda_{DU}\left(\frac{\tau}{2} + MRT\right) + \beta_D \lambda_{DD} MTTR$
1oo3	$= PFD_{IND,G1} + PFD_{CCF}$ $= PFD_{IND,1oo3} + PFD_{CCF}$ $= 6((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD})^3 t_{CE} t_{GE} t_{G2E} + \beta\lambda_{DU}\left(\frac{\tau}{2} + MRT\right) + \beta_D \lambda_{DD} MTTR$
2oo3	$= PFD_{IND,G1} + PFD_{IND,G2} + PFD_{IND,G3} + PFD_{CCF}$ $= 3PFD_{IND,1oo2} + PFD_{CCF}$ $= 6((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD})^2 t_{CE} t_{GE} + \beta\lambda_{DU}\left(\frac{\tau}{2} + MRT\right) + \beta_D \lambda_{DD} MTTR$

system is available, this operation needs at least 2 of 4 safety valves be available in functioning. HFT of the valves can be considered as 2, which interpret the element group has 2oo4 architecture. Minimal cut set for 2oo4 is analyzed and expressed as the first row in Table IV. However, this case has more safety condition because the two available valves will not service in the same heat source line, this is nonrandom failure. Minimal cut set of this case is reconsidered as the last row in Table IV.

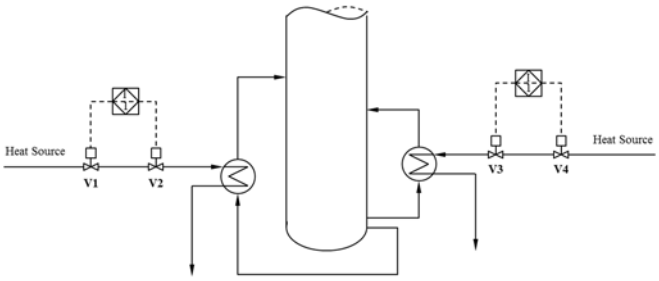

Fig. 2. Heat source cutting system of two reboilers for distillation column.

TABLE IV
MINIMAL CUT SET OF HEAT SOURCE CUTTING SYSTEM

Architecture	Minimal Cut Set
2oo4	{1, 2, 3}, {1, 2, 4}, {1, 3, 4}, {2, 3, 4}
2oo4 with Safety Condition	{1, 2}, {3, 4}

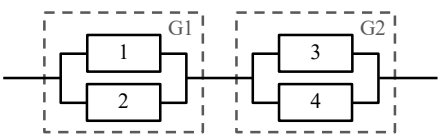

Fig. 3. Reliability block diagram of 2oo4 architecture with safety condition.

Minimal cut set of 2oo4 architecture with safety condition is used in creating the RBD as Figure 3, resulting in the PFD_{avg} formula of this RBD is generated as the following equation by applying (5) and (6).

$$PFD_{avg} = PFD_{IND,G1} + PFD_{IND,G2} + PFD_{CCF}$$

Notice that both G1 and G2 have 1oo2 architecture. And from 2) and 4) in assumption, the equation is written as:

$$\begin{aligned} PFD_{avg} &= 2PFD_{IND,1oo2} + PFD_{CCF} \\ &= 2(2((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD})^2) t_1 t_2 + PFD_{CCF} \\ &= 4((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD})^2) t_{CE} t_{GE} \\ &\quad + \beta\lambda_{DU}\left(\frac{\tau}{2} + MRT\right) + \beta_D \lambda_{DD} MTTR \end{aligned} \quad (7)$$

V. RESULTS AND DISCUSSION

TABLE V
COMPARISON OF PFD_{AVG} EQUATION OF CASE STUDY

Method	Average Probability of Dangerous Failure on Demand
This Paper	$4((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD})^2 t_{CE} t_{GE} + \beta\lambda_{DU}\left(\frac{\tau}{2} + MRT\right) + \beta_D \lambda_{DD} MTTR$
IEC 61508-6	None
Ref. [3]	$4((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD})^2 t_{CE} t_{GE} + 2\beta\lambda_{DU}\left(\frac{\tau}{2} + MRT\right) + 2\beta_D \lambda_{DD} MTTR$
Ref. [4] (2oo4 Archit.)	$24((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD})^3 t_{CE} t_{GE} t_{G2E} + \beta\lambda_{DU}\left(\frac{\tau}{2} + MRT\right) + \beta_D \lambda_{DD} MTTR$

From the results in section III, the comparison between equation in Table II and general formula in IEC 61508-6 found that both results are equal, leading to predicate that the PFD_{avg} calculation based on minimal cut set complies with the standard. Besides, the proposed method is applied to case study in section IV that has the functioning of voted group with nonrandom failure. The obtained result, both in equation and numerical form, is different to of other method. According to Table V, which shows the equation results comparison, there is no standard formula to cover this case. In addition, notice at the equation from method is refers to [3], there is duplicate calculation for the common cause failure. Generally, this common cause failure will be analyzed for once due to this failure will affect to all elements in voted group, resulting to SIF fails. For this reason, the result of method in [3] has over PFD_{avg} value or evaluates availability of voted group less than practical value.

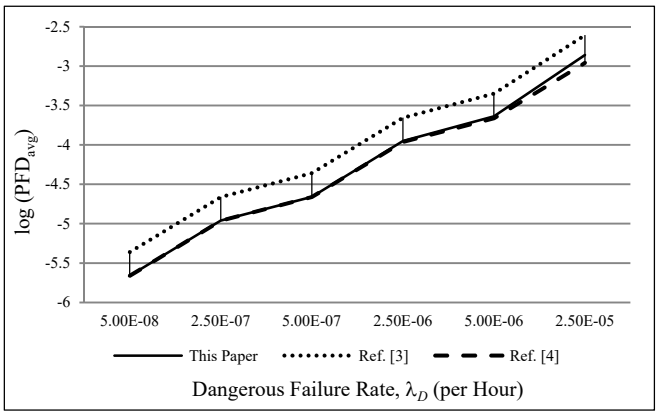

Fig. 4. Comparison of the numerical PFD_{avg} value of case study.

The numerical result is shown in Figure 4, which assumes that all safety valves have diagnostic coverage (*DC*) as 90%

ISBN: 978-988-14047-5-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

and estimated common cause failure β and β_D as 10% and 5% respectively. All elements are tested yearly or every 8640 hours and spend 8 hours for each repairing. Failure rate for this calculation is mentioned from Annex B in IEC 61508-6.

Besides, result from the formula in [4], which is generated by random failure analysis, has under PFD_{avg} value or evaluates availability of voted group more than practical value. However, if element with low failure rate is selected, PFD_{avg} from the developed method and the method that refer to [4] are similar because PFD_{CCF} value is very larger than PFD_{IND}, which can demonstrate from PFD_{IND}, PFD_{CCF} and deviation value in Table VI.

TABLE VI
COMPARISON OF PFD_{IND}, PFD_{CCF} AND PFD_{AVG} VALUE

λ_D	This Paper			Ref. [4]			$\frac{\lvert(1)-(2)\rvert}{(1)}$
	PFD_{IND}	PFD_{CCF}	PFD_{avg} (1)	PFD_{IND}	PFD_{CCF}	PFD_{avg} (2)	
0.50E-07	1.16E-09	2.18E-06	2.18E-06	7.39E-14	2.18E-06	2.18E-06	5.33E-04
2.50E-07	2.91E-08	1.09E-05	1.09E-05	9.23E-12	1.09E-05	1.09E-05	2.66E-03
0.50E-06	1.16E-07	2.18E-05	2.19E-05	7.39E-11	2.18E-05	2.18E-05	5.30E-03
2.50E-06	2.91E-06	1.09E-04	1.12E-04	9.23E-09	1.09E-04	1.09E-04	2.59E-02
0.50E-05	1.16E-05	2.18E-04	2.30E-04	7.39E-08	2.18E-04	2.18E-04	5.03E-02
2.50E-05	2.91E-04	1.09E-03	1.38E-03	9.23E-06	1.09E-03	1.10E-03	2.04E-01

VI. CONCLUSION

Average probability of dangerous failure on demand or PFD_{avg} analysis and calculation based on the minimal cut set can generate the new equation that complies with general equation in IEC 61508-6 standard and also covers architecture with nonrandom failure or safety condition. In addition, the developed method can be applied to various architectures and provides the solution for the conditional safety function problems and gives more accuracy PFD_{avg} value than the other methods because this principle consider practical condition or requirement of safety function.

ACKNOWLEDGMENT

I would like to thank PTT Maintenance and Engineering Co., Ltd. for supporting place and tool in this research.

REFERENCES

[1] IEC 61508. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. Geneva: The International Electrotechnical Commission, 2010.
[2] IEC 61511. Functional Safety – Safety Instrumented Systems for the Process Industry Sector. Geneva: The International Electrotechnical Commission, 2003.
[3] Chung S., Kim S., Yang Y. Use of Hazardous Event Frequency to Evaluate Safety Integrity Level of Subsea Blowout Preventer. International Journal and Naval Architecture and Ocean Engineering 2016; 8: 262-276.
[4] Jahanian H. Generalizing PFD Formulas of IEC 61508 for KooN Configurations. ISA Transactions 2015; 55: 168-174.
[5] Ding L., Wang H., Kang K., Wang K. A Novel Method for SIL Verification based on System Degradation Using Reliability Block Diagram. Reliability Engineering and System Safety 2014; 132: 36-45.
[6] Cetelani M., Ciani L., Luongo V. A Simplified Procedure for the Analysis of Safety Instrumented Systems in the Process Industry Application. Microeletronics Reliability 2011; 51: 1503-1507.
[7] Rausand M. Reliability of Safety-Critical Systems: Theory and Applications. New Jersey: John Wiley & Sons, 2014.
[8] Rausand M., Høyland A. System Reliability Theory: Models, Statistical Methods and Applications. 2nd ed. New Jersey: John Wiley & Sons, 2004.
[9] Innal F. Contribution to Modelling Safety Instrumented Systems and to Assessing Their Performance: Critical Analysis of IEC 61508 Standard. France: University of Bordeaux, 2008.
[10] ISA-TR84.00.02. Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques. United State of America: The Instrumentation, System, and Automation Society, 2002.
[11] Zhang T., Long W., Sato Y. Availability of Systems with Self-diagnostic Components – Applying Markov Model to IEC 61508-6. Reliability Engineering and System Safety 2003; 80: 133-141.