Nigerian Journal of Technology (NIJOTECH)
Vol. 36, No. 4, October 2017, pp. 1218 – 1225

Print ISSN: 0331-8443, Electronic ISSN: 2467-8821
www.nijotech.com
http://dx.doi.org/10.4314/njt.v36i4.31

AVERAGE PROBABILITY OF FAILURE ON DEMAND ESTIMATION FOR BURNER MANAGEMENT SYSTEMS

A. A. Okubanjo[1,*], O. K. Oyetola[2], A. Groot[3] and A. J. Degraaf[4]
[1,2,] COMP., ELECTRICAL & ELECTRONICS ENG'RG DEPT., OLABISI ONABANJO UNIV., AGO IWOYE, OGUN STATE. NIGERIA
[3,] BELDICK AUTOMATION BV, 6716BA, EDE, THE NETHERLANDS
[4,] HAN UNIVERSITY OF APPLIED SCIENCES, RUITENBERGLAAN 26, 6826CC, ARNHEM, THE NETHERLANDS
E-mail addresses: [1] *okubanjo.ayodeji@oouagoiwoye.edu.ng,* [2] *oyetola.oluwadamilola@oouagoiwoye.edu.ng,* [3] *agroot@beldick.nl,* [4] *aarjan.degraat@han.nl*

ABSTRACT
Proper estimation of Safety Integrity Level (SIL) depends largely on accurate estimation of Safety performance in terms of average Probability of Failure on Demand, (PFD_{avg}). For complex architectures of logic solvers, sensors, and valves, this can be calculated by distinguishing combinations of subsystems with basic (K-out-of-N) KooN approach for identical components. In the case of the typical configurations of valves for a burner management systems with non-identical subsystem configurations the KooN approach does not apply. Hence, it becomes an issues to calculate the correct safety performance since some of the established methods give too optimistic results due to lack of Common cause Failure information and data on non-identical components or sub-systems. This paper formulates a Markov model for determination of average probability of failure on demand for non-identical components and also proposes a more conservative lowest failure rate approach and maximum beta factor contrary to pragmatic minimum or average beta for correct estimation of average probability of failure on demand. It can be deduced that the measure of safety performance for components or subsystems with unequal failure rates depends largely on common cause failure, but a single beta factor is not appropriate to model the commonality of the failure. The result revealed that both geometric mean and lowest failure rate approaches result in different PFD_{avg} values with the lowest failure rate being the most conservative and optimistic result.

Keywords: *burner management systems, probability of failure on demand, common cause failure, KooN configurations, and lowest failure rate, Markov Analysis.*

NOMENCLATURE:
CCF – Common Cause Failure
KooN – K-out-of N redundant arrangement
PFD – Probability of failure on demand
β – *Conditional probability that a component fails due to common cause given that there is a failure*
$\beta_{A,B}$ – *Representative of maximal of* β_A *and* β_B
$\beta_{A,B,C}$ – *Representative of maximal of* β_A , β_B *and* β_C
C_{KooN} - *Configuration factor for KooN channel architecture.*
λ_C - *Common cause failure*
τ - *Proof test interval*
P_{ij} – *Probability from state i to j*

1. INTRODUCTION
In the process industry, the plant is designed to keep the process within specified parameters considered acceptable for normal and safe operation. However, when a process exceeds the pre-defined set point such as overpressure in a vessel due to mass, moles, or energy accumulated in a contained volume or space with restricted outflow or excessively high temperature arise from loss of control of reactors and heater [1] as a result of variation in process parameters, the dangerous condition may occur. If the situation is not addressed, it can often lead to hazardous events with potential consequence to human life or plant assets. Conversely, the risk associated with such a process variation may be reduced with adequate knowledge of safety instrumented systems (SIS) such as Burner Management systems, BMS.
A SIS is a system composed of any combination of sensors, logic solvers, and finial elements and the main significant purpose of a SIS is to bring the systems it supervises to a safe state, i.e. in a situation where it does not create a risk for environment or people

*** Corresponding author, tel: + 234 – 705 – 541 – 8857**

whenever the equipment under control (EUC) goes to a hazardous situation causing a real risk to people or environment [2].

Since a SIS protects against hazardous conditions, it is imperative for the system itself to be dependable and the dependability of a SIS is related to its functionality and integrity. Safety Integrity Level, SIL is a quantitative index that indicates the acceptable probability of dangerous failure that a system can have to consider it appropriate for a given safety integrity requirement [3]. The international standard for handling functional safety of electrical/electronic/programmable electronic safety-related systems, IEC61508 uses four discrete level to classify integrity level with SIL1 as the lowest (least reliable) and SIL4 as the highest (most reliable).

The probability of failure on demand expresses the safety performance of safety instrumented function. Articles [2 – 4], use simplified formula based on approximation to calculate PFDs of SIL and this method is extended to generalized K-out-of–N configurations. The simplified formula consists of two main elements only: failure rate and proof test. IEC61508 uses SIL as a measure of the risk –reduction level of the safety function; hence, the SIL is estimated from the probability of failure on demand. For a low demand mode, the required PFD is related to unavailability, $U(t)$ of the SIF.

2. A BURNER MANAGEMENT SYSTEM

A burner management system is to ascertain a safe start-up, operation, monitor and shut off the fuel supply in the event of dangerous conditions (such as low fuel pressure, high fuel pressure and loss of flame). Figure (1) represents the architecture of shutdown valves on a typical burner management system with different SIFs architecture. The safety function consists of a 1oo2 series configuration voted in 6oo6 architecture in the Main gas SSOVs to ensure that all the six valves close in case of high pressure provided that one out of two (1oo2) configuration valve close on demand. Also a 1oo3 series configuration valve is voted with 6oo6 architecture to ensure that one out of three valves close in order to bring all the 6oo6 ignition gas SSOVs to safe state whenever sit required on demand.

In Figure 2, the channels can be distinguished as:

Channel A comprises SSOV01X1 and SSOV01X3 in a 1oo2-arrangement with identical $PFD_{avg}{}^{(Valve)}$ for both valves, where X denotes 1, 2, 3, 4, 5 and 6.

Channel B comprises six Channels A's in 6oo6-arrangement, with identical PFD's,

Channel C comprises SSOV012 and Channel B in 1oo2-arrangement, where the $PFD's_{avg}$ for these two valves is not identical.

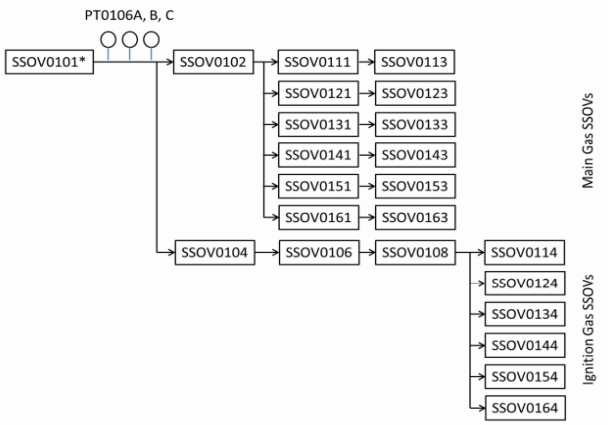

Figure 1: Valves Configuration in Burner Management Systems

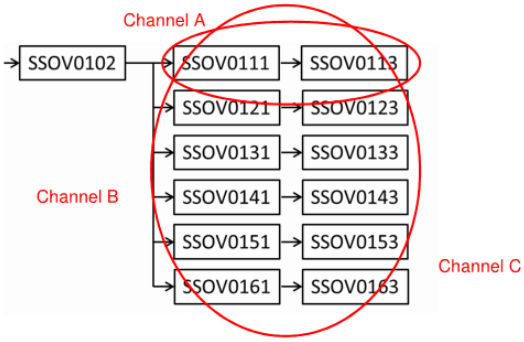

Figure 2: Voting of the main gas

The main issue in evaluating the probability of failure on demand for the gas valves is that PFD of 1oo2-arrangement of channel B and C is not identical, therefore, the PFD generic formula for K-out-of-N identical component cannot be used in such configuration. While failure events from independent faults (i.e. the probability of both failure occur) can be modelled by simply multiplying their probabilities of occurrence.$P(A).P(B)$, but dependent failure shows a different probability thus:

$$P(A \cap B) = P(A).P(B|A) = P(B).P(A|B) \neq P(A).P(B) \quad (1)$$

For simplicity, figure 3 is further presented as

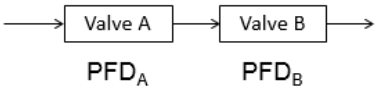

Figure 3: Reduced 1oo2 configuration for non-identical component

Based on the assumption that the poorer valve (in this case valve B) improved safety performance, the PFD_{avg} for 1oo2 configuration show in figure 3is expressed by [5] as:

$$PFD_{avg}{}^{(1oo2)} \approx \frac{4}{3} PFD_A.PFD_B + \beta PFD_A \quad (2)$$

In order to assign the safety integrity level in a system that provides multiple layer of defense against

complete functional failure, the estimation of the PFD must be sufficiently accurate to depict the SIF unavailability. Hence, common cause failure influences the numerical value of the PFD as result of components, sub-system dependency. However, if the contribution is ignored in probabilistic risk assessment it may lead to underestimation of unavailability of the SIF.

3. COMMON CAUSE FAILURE

To enhance reliability or availability of a SIS against random failures, redundancy is often implemented in the system configuration. However, redundancy introduced a subclass of dependent failures called common-cause failure (CCF)[6]which dominant effect drastically reduced intended benefit of redundancy. Thus, common-cause failures can result in the SIS failing to perform its intended function when a demand occurs.

The definition of CCF is not consistent, even, there are discrepancies in the definition of CCF among SIS related standards. It was pointed out in [6] that there is no generally accepted definition of CCF. This connotes that people in different sectors have different opinions about common cause failure. IEC61508 (2010) defines a CCF as:

A failure that is the result of one or more events, causing concurrent failures of two or more separate channels in a multiple channel system, leading to a system failure[7].

PDS[7], *the fraction of CCFs (β) is defined as "The fraction of failure of a single component that causes both components of a redundant part to fail simultaneously"*

There are inconsistency and ambiguity regarding the definition and use of the terms random failures and systematic failures, and the way these are related to common cause failure (CCF)[8]. The reliability related to random hardware failure is quantified based on failure rate, but systematic failure cannot be accurately estimated because of its deterministic nature, however, IEC61508 standard suggests, as a general rule, not to quantify systematic failure. If systematic failure is neglected the predicted unavailability will be of lower value and less conservative compared with actual unavailability, but its contribution is not completely ignored in reliability quantification[9, 10].

However, PDS method uses the same classification as IEC61508, but gives a more detailed breakdown of the systematic failure as shown in figure 4.

3.1 Existing Methods for CCF Modelling

Common cause failures modelling can be addressed as either explicit or implicit model, but due to lack of sufficient information and data on CCFs the implicit (or parametric) model is developed to model CCFs by quantitatively taking into cognizance the effect of dependent failures in a system failure. The paper lays more emphasis on the beta (β)-factor model and the PDS method.

β-factor is a single parameter model proposed by Fleming in 1975 and it has gained wide acceptance in quantifying CCF in process industry because of its simplicity. A crucial assumption in the model is that whenever a common cause event occurs, all the components in that specific CCF group are assumed to fail [8, 11].

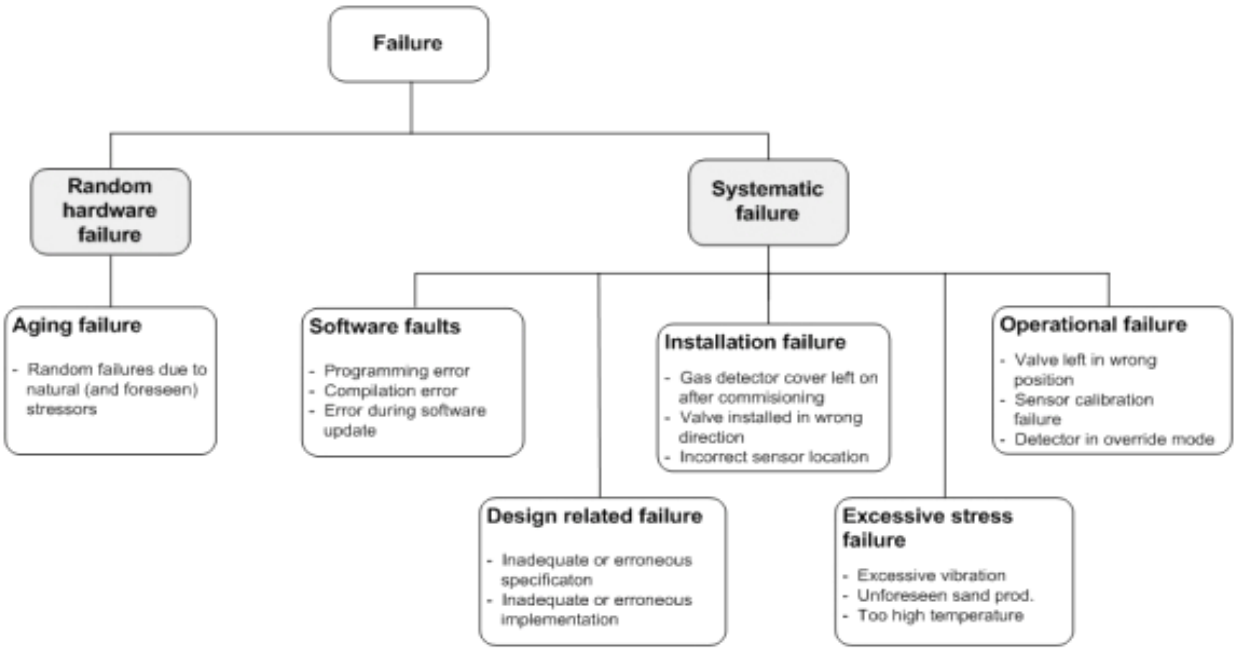

Figure 4: PDS failure classification adopted from [10]

In IEC61508 standard, regardless of the voting configuration beta-factor (β) is the same for any KooN and the contribution of common cause failure based on this approach is equal to $\boldsymbol{\beta}\frac{\lambda_{DU}}{2}$. The main drawback of the β-factor model is its inability to provide a distinction between the different numbers of multiple failures for systems with more than two units. For instance, a pressure transmitter voting in 2oo3 may fail due to CCF of two units. Figure 5illustrates β-model for a triplicate system.

The PDS method is introduced to overcome the weakness of β-factor model especially in redundancy system and employ the same techniques for quantifying common cause failures (CCFs) as MBF (Multiple Beta Factor) discussed in [12].

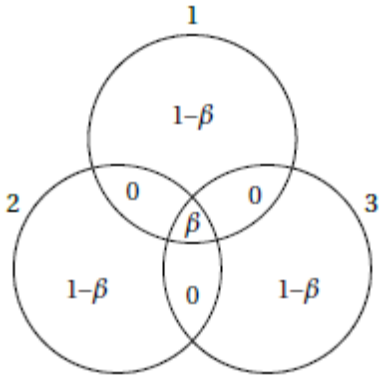

Figure 5: β-factor model for a triplicate system

Furthermore, the method considered different multiplicity of failures for KooN configuration and has therefore, introduced a configuration factor, C_{KooN} formula that modifies the contribution of CCFs for some typical voting configuration.

$$PFD_{KooN} = C_{KooN}.\beta.\left(\frac{\lambda_{DU}.\tau}{2}\right) + \frac{\mathrm{N!}(\lambda_{DU}.\tau)^{N-K+1}}{(N-k+2)!\,(K-1)!} \quad (3)$$

For $K < N; N = 2,3, \ldots$

Where, $C_{KooN\ is}$ a configuration factor given in table 1which depends on the voting configuration.

Table 1 :Numerical values of C_{KooN} and C_N proposed by PDS method. Adopted from[3] also cited in [7]

	C_{KOON}					C_N
	K=1	K=2	K=3	K = 4	K = 5	
$N = 2$	1.0	-	-	-	-	1.0
$N = 3$	0.30	2.4	-	-	-	2.7
$N = 4$	0.15	0.75	4.0	-	-	4.9
$N = 5$	0.08	0.45	1.2	6.0	-	7.7
$N = 6$	0.04	0.26	0.8	1.6	8.1	10.8

4. ESTIMATION OF PFD_{avg} BASED ON MARKOV ANALYSIS

As a result of dependency in the channel, the average probability of failure on demand for the main gas is not just a product of probability of failure on demand. The PFD_{avg} is implicitly modelled with Markov analysis considering the sub-system in Figure 3 as channels with different failure rates and the contribution of channel CCF is also taken into account. In the Markov analysis, the system is considered to be in one of the four states at any time as detailed in Table 2.

Tabel 2:System State

State Probability	State	State description
$\boldsymbol{P_0}$	0	Components A & B are operational
$\boldsymbol{P_1}$	1	Component A is operational and Component B failed
$\boldsymbol{P_2}$	2	Component B is operational and Component A failed
$\boldsymbol{P_3}$	3	Component A and B failed

The transition from state 0 to 3 is due to common cause influence and it is known as absorbing state; the Markov state transition diagram is shown in figure 6.

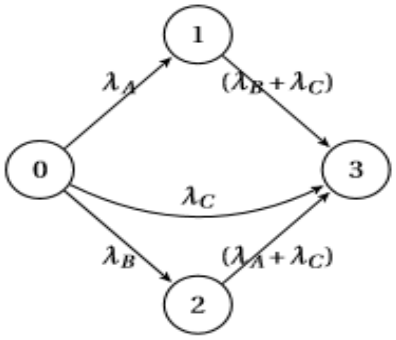

Figure 6: Markov state transition diagram adapted from[12]

The following set of differential equations are obtained by applying Kolmogorov forward equation:

$$\frac{dP_0(t)}{dt} = (\lambda_{DU_A} + \lambda_{DU_B} + \lambda_C)P_0(t) \quad (4)$$

$$\frac{dP_1(t)}{dt} = \lambda_{DU_A}P_0(t) - (\lambda_{DU_B} + \lambda_C)P_1(t) \quad (5)$$

$$\frac{dP_2(t)}{dt} = \lambda_{DU_B}P_0(t) - (\lambda_{DU_A} + \lambda_C)P_2(t) \quad (6)$$

$$\frac{dP_3(t)}{dt} = \lambda_{DU_A}P_0(t) + (\lambda_{DU_B} + \lambda_C)P_1(t) + (\lambda_{DU,A} + \lambda_C)P_2(t) \quad (7)$$

These set of the differential equations are solved by both separating the variables and integrating factor methods and the initial conditions of $P_0 = 1, P_1 = 0, P_2 = 0$ &$P_3 = 0$ are substituted into general solution obtained to obtain the constant of integration, hence a particular solution for each equation yield,

$$P_0(t) = e^{(\lambda_{DU_A,} + \lambda_{DU_B} + \lambda_C)t} \quad (8)$$

$$P_1(t) = e^{(\lambda_{DU_B} + \lambda_C)t} - e^{(\lambda_{DU_A,} + \lambda_{DU_B} + \lambda_C)t} \quad (9)$$

$$P_2(t) = e^{(\lambda_{DU_A} + \lambda_C)t} - e^{(\lambda_{DU_A} + \lambda_{DU_B} + \lambda_C)t} \quad (10)$$

$$P_3(t) = 1 + e^{(\lambda_{DU_A} + \lambda_{DU_B} + \lambda_C)t} - e^{(\lambda_{DU_A,} + \lambda_C)t} - e^{(\lambda_{DU_B} + \lambda_C)t} \quad (11)$$

For $2oo2_{A,B}$ configuration, the system is unavailable if at least one of the components A or B failed upon demand and the corresponding states are 1, 2 and 3. Hence, the sum of the state probabilities is

$$PFD_{2oo2A,B} = P_1(t) + P_2(t) + P_3(t) = 1 - P_0(t) = 1 - e^{(\lambda_{DU_A} + \lambda_{DU_B} + \lambda_C)t} \quad (12)$$

The average probability of failure on demand for $2oo2_{A,B}$ is calculated by taking the average sum of the probabilities in state 1, 2, and 3 over the time interval$(0, \tau)$.

$$PFD_{avg} = \frac{1}{\tau}\int_0^\tau 1 - e^{(\lambda_{DU_A} + \lambda_{DU_B} + \lambda_C)t}\, dt \quad (13)$$

Integrating equation(13), then:

$$PFD_{avg} = \left(\frac{(\lambda_{DU_A} + \lambda_{DU_B} + \lambda_C)\tau + e^{(\lambda_{DU_A} + \lambda_{DU_B} + \lambda_C)\tau} - 1}{(\lambda_{DU_A} + \lambda_{DU_B} + \lambda_C)\tau}\right) \quad (14)$$

Recall that:

$$e^{(\lambda_{DU_A} + \lambda_{DU_B} + \lambda_C)\tau} = 1 - (\lambda_{DU_A} + \lambda_{DU_B} + \lambda_C)\tau + \frac{(\lambda_{DU_A} + \lambda_{DU_B} + \lambda_C)^2\tau^2}{2!} + \cdots \quad (15)$$

The first three terms of Taylor's series for exponential function in equation (15)are substituted in equation[11]. After cancellation of equal terms, the $PFD_{2oo2A,B}$ is

$$PFD_{avg,A,B}{}^{(2oo2)} = \frac{(\lambda_{DU_A} + \lambda_{DU_B})\tau}{2} \quad (16)$$

For 2oo2 configuration, it is reasonable to assume that if one component fails the system will fail, even though, the failure of the two components might not occur due to common cause failure. Invariably, NooN ($N = 1,2, \ldots$) configurations do not exist, hence, the contribution due to common cause failure is neglected.

In the same vein, the average probability of failure on demand,PFD_{avg} for series configuration of non-identical components A and B is computed by taking the PFD_{avg} of state 3. $P_3(t)$ over the time interval $(0, \tau)$

$$PFD_{avgA,B}{}^{(1oo2)} = \frac{1}{\tau}\int_0^\tau P_3(t)\, dt \quad (17)$$

$$PFD_{avgA,B}{}^{(1oo2)} = \frac{(\lambda_{DU_A}.\lambda_{DU_B})\tau^2}{3} + \frac{\lambda_C\tau}{2} \quad (18)$$

Equation (18) is further split based on the contribution of independent failure,$PFD_{avg}{}^{(ind)}$ and common cause (dependent) failure,$PFD_{avg}{}^{(CCF)}$.

$$PFD_{avg}{}^{(ind)} = \frac{4}{3}\left(PFD_{avg,A}{}^{(1oo1)}.\ PFD_{avg,B}{}^{(1oo1)}\right) \quad (19)$$

$$PFD^{(CCF)} = \frac{\lambda_C\tau}{2} \quad (20)$$

λ_C represents the representative failure rates for channel A and B and it is expressed as

$$\lambda_C = \lambda_{DU,A,B}\beta_{A,B} \quad (21)$$

In [13], [14] geometric mean approach for a representative failure rate ($\lambda_{DU,A,B}$) was suggested. However, the problem with geometric mean is that for components, sub-systems or channels with different failure rate or PFD, the "weighting" of the largest failure rate or PFD will become dominating and this might cause the CCF contribution to exceed the likelihood of independent failure of the most reliable component or channel. A conservative approach, lowest failure rate, is proposed which improves the probability of failure on demand of the lowest in the case of worst event because most reliable component or channel will not fail more often. The beta-factor,$\lambda_{DU,A,B}$ expressed the contribution of each fraction of individual failure rate to common cause failure in the channel and it is selected based on the maximum β (refer to equation(21)) of the channel from conditional probability point of view contrary to the pragmatic minimum or average β suggested in[13][15].

4.1 $PFD_{avg}$for 1oo2 and 2oo3 Non-Identical Components

The computation of PFD for these configurations is based on the following assumptions:

For 1oo2 and 1oo3 configurations the dangerous undetected failure rates of the valve ($\lambda_{DU}{}^{(Valve)}$) and valve E ($(\lambda_{DU}{}^{(E)}$) are considered as the lowest dangerous failure rates respectively.

The beta-factor for the valve is the maximum value for 1oo2 and the beta-factor for valve E is the maximum for 1oo3 configurations.

Geometric mean of the CCF failure rates of two valves is $\lambda_{DU,A,B} = \sqrt{(\lambda_A\,.\,\lambda_B)}$ and $\lambda_{DU,A,B\ldots,N} = \sqrt{(\lambda_A\,.\,\lambda_{B\ldots.}\lambda_N)}$ for N valves.

4.2. PFD_{avg} Calculations, Results and Findings

The overall average probability of failure on demand for the burner management systems shown in figure 1is computed as:

$$PFD_{avg}{}^{(Loop)} = PFD_{avg}{}^{(Sensors)} + PFD_{avg}{}^{(Logic)} + PFD_{avg}{}^{(Actuator)} \quad (22)$$

The unreliability data for the components is given in Table (4) and the proof test interval, τ is 8750 (1 year).

Table 3: Simplified formulae for PFD based on Markov derivation for non-identical component:

Configuration	Geometric mean Approach	Lowest Failure rate Approach
1oo2	$PFD_{avgA,B}{}^{(1oo2)} \approx \beta_A PFD_{avg,A}{}^{(1oo1)}$	$PFD_{avgA,B}{}^{(1oo2)} \approx \beta_A\sqrt{\left(PFD_{avg,A}{}^{(1oo1)}.PFD_{avg,B}{}^{(1oo1)}\right)}$
1oo3	$PFD_{avgA,B,C}{}^{(1oo3)} \approx \frac{1}{2}\beta_A PFD_{avg,A}{}^{(1oo1)}$	$PFD_{avgA,B,C}{}^{(1oo3)} \approx \frac{1}{2}\beta_A.\sqrt[3]{\left(PFD_{avg,A}{}^{(1oo1)}.PFD_{avg,B}{}^{(1oo1)}.PFD_{avg,C}{}^{(1oo1)}\right)}$

Table 4: Unreliability data for the BMS adopted from[5].

component	Unreliability data for BMS			
	Extracted values			
	λ_{DU} (per hour)	β	SFF	TYPE
Pressure Transmitter (PT)	3.9×10^{-8}	-	90%	B
SIS Analogue Input (AI)	7.4×10^{-10}	2%	>90%	B
SIS common Circuitry (CC)	8.0×10^{-10}	2%	>99%	B
SIS Digital Output (DO)	2.2×10^{-10}	2%	>99%	B
Solenoid	3.9×10^{-7}	-	62%	A
Actuator	3.4×10^{-7}	-	82.6%	A
Valve	3.0×10^{-7}	-	48%	A

4.2.1. Sensors

Pressure transmitters PT0106A, PT0106B and PT0106C are located on the main gas header on the fuel gas skid and each transmitter is connected independently to analogue input of the SIS (on a separate not redundant input cards). In the SIS, a 2oo3 configuration is applied, hence, the channel comprising transmitter and analogue input has a failure rate

$$\lambda_{DU_{(PT,AI)}} = \lambda_{DU_{PT}} + \lambda_{DU_{AI}} = 3.9 \times 10^{-8} + 7.4 \times 10^{-10} \approx 4.\times 10^{-8}$$

$$PFD_{avg}{}^{(1oo1)} = \frac{1}{2}\left(\lambda_{DU_{(PT,AI)}}\right).\tau \quad (22)$$

$$= \frac{1}{2} \times 4.\times 10^{-8} \times 8750 = 1.75 \times 10^{-10}$$

The combined $PFD_{avg}{}^{(2oo3)}$ is equal to $PFD_{avg}{}^{(Sensors)}$ with beta value of ($\beta = 0.05$), hence, the $PFD_{avg}{}^{(Sensors)}$ is computed as:

$$PFD_{avg}{}^{(2oo3)} = PFD_{avg}{}^{(1oo1:ind)} + PFD_{avg}{}^{(CCF)}$$

$$= 4\left(PFD_{avg}{}^{(1oo1)}\right)^2 + 2\beta.PFD_{avg}{}^{(1oo1)}$$

$$= 4(1.75 \times 10^{-4})^2 + 2(0.05 \times 1{,}75 \times 10^{-4})$$

$$PFD_{avg}{}^{(2oo3)} \approx 1.7 \times 10^{-5} \quad (23)$$

4.2.2. Logic Solver

The logic solver has 2oo2 architecture to improve availability.

$$PFD_{avg}{}^{(Logic)} = PFD_{avg}{}^{(1oo1:ind)}$$

$$= 2\left(\frac{1}{2} \times 8.0 \times 10^{-4} \times 8750\right)$$

$$PFD_{avg}{}^{(Logic)} \approx 7.0 \times 10^{-6}$$

4.2.3. Actuator

The PDF_{ValVe} is first calculated for single valve and the combined PFD_SSOVs for the network of valve is then computed based on single valve. It is important to point out that all the valves in BMS systems are identical including solenoids and the actuator.

4.2.4. PFD_{avg} for single valve

The digital output is arranged in 2oo2 configuration while the solenoid, actuator and valve are single. The combined PFD for the digital output, solenoid, actuator and valve in the SIF is referred to as $PFD_{avg}{}^{(Valve)}$.

$$PFD_{avg}{}^{(Valve)} = PFD_{avg}{}^{(DO:ind)} + PFD_{avg}{}^{(SAV:ind)}$$

$$= 2\left(\frac{1}{2}\lambda_{DU_{DO}}\tau\right) + \frac{1}{2}\left(\lambda_{DU_{ACTUATOR}} + \lambda_{DU_{SOLENOID}} + \lambda_{DU_{VALVE}}\right)\tau$$

$$= 2\left(\frac{1}{2}\ 2.2 \times 10^{-10} \times 8750\right) + \frac{1}{2}(3.9 \times 10^{-7} + 3.4 \times 10^{-7} + 3.0 \times 10^{-7}) \times 8750$$

$$PFD_{avg}{}^{(Valve)} \approx 4.5 \times 10^{-3}$$

4.2.5. PFD_{avg} for Main Gas Valves

The PFD_{avg} for channel A, $PFD_{avg}{}^{(A)}$ is calculated from two $PFD_{avg}{}^{(Valve)}$ in a 1oo2 voting (with $\beta = 5\%$). Subsequently, $PFD_{avg}{}^{(B)}$is calculated from $PFD_{avg}{}^{(A)}$ using 6oo6 voting, hence,

$$PFD_{avg}{}^{(\boldsymbol{B})} = PFD_{avg}{}^{(Valve:ind)} + PFD_{avg}{}^{(PFD_{avg}{}^{(A)}alve:CCF)}$$

$$PFD_{avg}{}^{(B)} = 6\left[\left(PFD_{avg}{}^{(Valve)}\right)^2 + \beta.PFD_{avg}{}^{(Valve)}\right]$$

$$= \left[\frac{4}{3} \times (4.5 \times 10^{-3})^2 + 0.05 \times 4.5 \times 10^{-3}\right]$$

$$PFD_{avg}{}^{(B)} \approx 1.35 \times 10^{-3}$$

Channel C finally combines all the main gas valves. It comprises channel B and SSOV0102 ($PFD_{avg}{}^{(Valve)}$) in 1oo2 architecture but they are not identical valve. The solution is obtained by both geometric approach and lowest failure rate for comparison.

i. Geometric mean approach

$$PFD_{avg}{}^{(C)} = \frac{4}{3}\left(PFD_{avg}{}^{(B)}.PFD_{avg}{}^{(Valve)}\right) + \beta_{min}.\sqrt{\left(PFD_{avg}{}^{(B)}.PFD_{avg}{}^{(B)}\right)}$$

$$= \frac{4}{3}(4.5\times10^{-3}\times1.35\times10^{-3}) + 0.05 \times \sqrt{(4.5\times10^{-3}\times1.35\times10^{-3})}$$

$$PFD_{avg}{}^{(C)} = 1.23\times10^{-4}$$

ii. Lowest failure rate approach

$$PFD_{avg}{}^{(Valve)} > PFD_{avg}{}^{(B)}$$

$$PFD_{avg}{}^{(C)} = \frac{4}{3}\left(PFD_{avg}{}^{(B)}.PFD_{avg}{}^{(Valve)}\right) + \beta_{Valve}.PFD_{avg}{}^{(Valve)}$$

$$= \frac{4}{3}(4.5\times10^{-3}\times1.35\times10^{-3}) + 0.05\times1.35\times10^{-3}$$

$$PFD_{avg}{}^{(C)} = 6.75\times10^{-5}$$

4.2.6. PFD_{avg} for Ignition Gas Valves

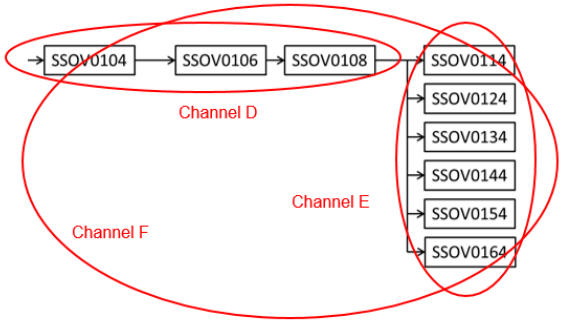

Figure 7: Voting of the ignition gas

In figure (7), the channels can be distinguished as:
Channel D comprises SSOV0104, SSOV0106 and SSOV0108 in a 1oo3-arrangement with identical $PFD_{avg}{}^{(Valve)}$ for the three valves.
Channel E comprises six SSOV01X4 in 6oo6-arrangement, with identical$PFD_{avg}{}^{(Valve)}$.
Channel F comprises D and Channel E in 1oo2-arrangement, where the $PFD's_{avg}$ for these two valves is not identical.
$PFD_{avg}{}^{(D)}$ for the channel D is calculated from the$PFD_{avg}{}^{(Valve)}$. It follows that $PFD_{avg}{}^{(D)}$ is given as:

$$PFD_{avg}{}^{(D)} = \frac{8}{4}\left(PFD_{avg}{}^{(Valve)}\right)^3 + \beta_{min}.PFD_{avg}{}^{(Valve)}$$

$$= 2(4.5\times10^{-3})^3 + \beta_{max}.4.5\times10^{-3}$$

$$PFD_{avg}{}^{(D)} = 2.25\times10^{-4}$$

and that of channel E is computed as:

$$PFD_{avg}{}^{(E)} = 6.PFD_{avg}{}^{(Valve:ind)} = 2.70\times10^{-2}$$

Hence, channel F which is a combination of channel D and F as 1oo2 non-identical valve, so that average probability of failure is calculated from both geometric approach and lowest failure rate approach.

i. Geometric mean approach

$$PFD_{avg}{}^{(F)} = \frac{4}{3}\left(PFD_{avg}{}^{(E)}.PFD_{avg}{}^{(D)}\right) + \beta_{min}.\sqrt{\left(PFD_{avg}{}^{(E)}.PFD_{avg}{}^{(D)}\right)}$$

$$= \frac{4}{3}(2.70\times10^{-2}\times2.25\times10^{-4}) + 0.05 \times \sqrt{(2.70\times10^{-2}\times2.25\times10^{-4})}$$

$$PFD_{avg}{}^{(F)} \approx 1.23\times10^{-4}$$

Lowest failure rate approach

$$PFD_{avg}{}^{(E} > PFD_{avg}{}^{(D)}$$

$$PFD_{avg}{}^{(F)} = \frac{4}{3}\left(PFD_{avg}{}^{(E)}.PFD_{avg}{}^{(D)}\right) + \beta_E.PFD_{avg}{}^{(E)}$$

$$= \frac{4}{3}(4.5\times10^{-3}\times1.35\times10^{-3}) + 0.05\times2.25\times10^{-4}$$

$$PFD_{avg}{}^{(F)} \approx 1.125\times10^{-5}$$

4.2.7. PFD_{avg} for Actuator

Finally, the combination of the main gas valves (channel C) and ignition gas valve (channel F) in 2oo2 configuration is referred to as Actuator.

i. Geometric approach

$$PFD_{avg}{}^{(Actuator)} = 1.23\times10^{-4} + 1.23\times10^{-4}$$

$$PFD_{avg}{}^{(Actuator)} \approx 2.46\times10^{-4}$$

ii. Lowest failure rate

$$PFD_{avg}{}^{(Actuator)} = 1.75\times10^{-5} + 6.75\times10^{-5}$$

$$PFD_{avg}{}^{(\mathbf{Actuator})} \approx 8.5\times10^{-5}$$

The overall average probability of failure on demand for the burner management systems is 2.71×10^{-4} based on geometric mean approach and 1.1×10^{-5} for lowest failure rate.

5. RESULT AND DISCUSSION

It can be deduced that the measures of safety performance for components or sub-system with unequal failure rates depends predominantly on common cause failure, but a single beta-factor is not appropriate to model the commonality of the failure as presented in equation (2)by[5], since the fraction of individual failure rate that lead to common cause failure is enigmatic. This permits a pragmatic choice of beta-factor for modeling non-identical components or sub-systems.
The geometric mean approach is valid if all the undetected dangerous failure rates are in the same order of magnitude. However, the estimation of the probability of failure on demand based on geometric mean approach leads to unrealistic result due to underestimation of PFD which can result in inappropriate assignment of Safety Integrity Level.
Hence, the lowest failure rate approach improves the average probability of failure on demand of the lowest valve because most reliable valve will not fail more often. Both approaches are sensitive to the value of β factor as shown in Figure 8.

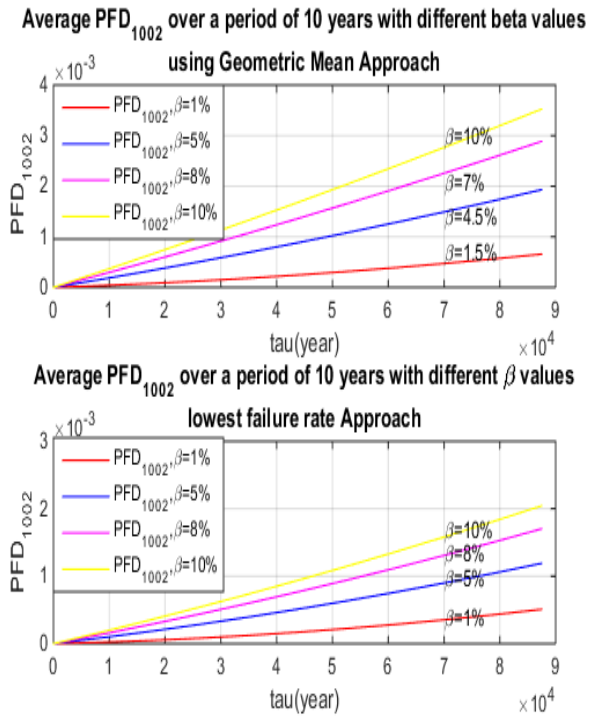

Figure 8: Sensitivity of Geometric mean and lowest failure rate approaches to β- factor

6. CONCLUSION

In this paper, a Markov model was formulated to obtain average probability of failure on demand for a burner management system for non-identical sub-system configurations. To accurately ascertain the safety integrity level, two methods were proposed, the lowest failure rate and the geometric mean. The maximum beta factor was also proposed contrary to pragmatic choice of existing beta-factor to evaluate the commonality of the failure in the BMS.

The result revealed that contribution of common cause failure plays an important factor in determine the average probability of failure on demand because the contribution due to independent failure is quite negligible and disappear into noise. This was evidence from both geometric mean and lowest failure rate approaches. It was obvious that both geometric mean and lowest failure rate approaches result in different PFD_{avg} values with the lowest failure rate being the most conservative and optimistic result.

7. REFERENCES

[1] G. P. Towler and R. K. Sinnott, *Chemical engineering design : principles, practice, and economics of plant and process design*. Butterworth-Heinemann, 2013.

[2] W. Mechri, C. Simon, and K. BenOthman, "Switching Markov chains for a holistic modeling of SIS unavailability," *Reliab. Eng. Syst. Saf.,* vol. 133, no. May, pp. 212–222, Jan. 2015.

[3] A. C. Torres-Echeverría, S. Martorell, and H. A. Thompson, "Modeling safety instrumented systems with MooN voting architectures addressing system reconfiguration for testing," *Reliab. Eng. Syst. Saf.,* vol. 96, no. 5, pp. 545–563, May 2011.

[4] S. Tang, X. Guo, X. Sun, H. Xue, and Z. Zhou, "Unavailability analysis for k -out-of- N:G systems with multiple failure modes based on micro-markov models," *Math. Probl. Eng.,* vol. 2014, 2014.

[5] A. G. Mba and A. Groot, "*Functional Safety Calculation and Principles, course Material* A & B," The Netherlands, 2015.

[6] P. Hokstad and M. Rausand, "Common Cause Failure Modeling: Status and Trends," in Handbook of Performability Engineering, London: Springer London, , pp. 621–640,. 2008.

[7] S. Hauge, T. Kråknes, S. Håbrekke, and H. Jin, Reliability prediction method for safety instrumented systems - PDS Method Handbook 2013 Edition. SINTEF, 2013.

[8] A. K. Verma, S. Ajit, and M. Kumar, Dependability of Networked Computer-based Systems. London: Springer London, 2011.

[9] M. Chebila and F. Innal, "Generalized analytical expressions for safety instrumented systems' performance measures: PFDavg and PFH," J. Loss Prev. Process Ind., vol. 34, pp. 167–176, 2015.

[10] S. Hauge, H. Solfrid, and M. Lundteigen, Reliability prediction method for safety instrumented systems PDS Handbook, no. March. Norway: SINTEF, 2010.

[11] S. Hauge, P. Hokstad, S. Håbrekke, and M. A. Lundteigen, "Common cause failures in safety-instrumented systems: Using field experience from the petroleum industry," Reliab. Eng. Syst. Saf., vol. 151, pp. 34–45, Jul. 2016.

[12] A. Okubanjo, "Modelling Functional Safety Using Markov Analysis, Master's thesis, unpublished, Ruitenberglaan, Arnhem, Netherlands, 2016," 2016.

[13] S. Hauge, P. Hokstad, H. Langseth, S. Hauge, and T. Onshus, Reliability prediction method for safety instrumented systems-PDS Example collection, 2010th ed. Norway: SINTEF, 2010.

[14] J. Jin, Z. Wu, S. Zhao, and B. Hu, "Loss of Safety for Instrumented System including Diverse Redundant Component," in *Computational Intelligence - Foundations and Applications - 9th International FLINS Conference,* 2010, pp. 1090–1097.

[15] J. Börcsök, P. Holub, and M. H. Schwarz, "How safe is my system? Calculation of PFD-values for a safety related system," *in 2nd International Conference on Systems, ICONS*, 2007, pp. 40–40, 2007.