

What is PFDavg?

Dr. Julia V. Bukowski, Villanova University, Villanova, PA, USA

Dr. Jan Rouvroye, Eindhoven University of Technology, Eindhoven, Netherlands

Dr. William M. Goble, exida, Sellersville, PA, USA

Introduction

IEC61508 requires probabilistic evaluation of each set of equipment used to reduce risk in a safety related system. Different order of magnitude risk reduction levels are achieved depending on the average probability of failure on demand (often called average probability of dangerous failure). In practice, a number of different methods have been used to calculate this probability. Among the most popular are fault tree analysis, reliability block diagrams, simplified equations (derived using a number of different ways) and Markov models. For those who use Markov models, different solution techniques are used. A debate has existed in various circles about the appropriateness of various methods. A tutorial of the different methods is available in a text by Goble, reference 1. A good comparison of the different methods is stated by Rouvroye in reference 2.

The fundamental problem is that these different methods give results that vary by 2X+ for same set of input parameters.

What is PFDavg – unavailability or unreliability?

Part of the problem may be different interpretations of the meaning of PFDavg. Two fundamentally different ways to calculate the metric are described. Note that a number of assumptions are made. These are listed at the end of the paper.

The unreliability approach

In one method, an unreliability function is calculated as a function of time interval for a specified mission time usually equal to a “proof test” interval for industrial equipment. Then the function is “averaged” over the entire mission time.

This model is used for safety related systems with the assumption that the system is periodically inspected and tested. It is often assumed that the periodic test will detect all failed components and the system will be renewed to perfect condition. Therefore the unreliability function is perfect for the problem. It is further reasoned that the system may fail right after the inspection, right before the inspection or at any time in between. Therefore, PFDavg is the average value of the unreliability function plotted over the inspection period.

It is a well known equation for a single channel system with a constant failure rate that:

Unreliability for a specified mission time, t : $F(t) = 1 - e^{-\lambda t}$. This is sometimes called Probability of Failure, PF. $PF(t) = 1 - e^{-\lambda t}$.

For one failure mode, fail-danger, $\lambda = \lambda_d$ and the probability of failure in the dangerous mode:

$PFD(t) = 1 - e^{-\lambda_d t}$. This is approximated by:

$PFD(t) = \lambda_d t$. (The approximation works acceptably when the result is small with a result greater than 0.1, having an error of less than 3%. Since all safety integrity levels require a PFDavg value less than 0.1, the approximation is acceptable.)

PFDavg is obtained by arithmetic average over the time interval T.

$$PFD_{avg} = \frac{1}{T} \int_0^T PFD(t) dt$$

Using the approximation:

$$PFD_{avg} = \lambda_d T / 2 \quad \text{(Equation 1)}$$

The unavailability approach

In a different approach, PFDavg is interpreted as steady state unavailability. Unavailability of a system is calculated using some probability combination method using unavailability of various components. An example of this approach for a simplex repairable system starts with the well known equation for unavailability of a single channel system:

$$U_{\text{steady state}} = \lambda / (\lambda + \mu)$$

And if μ is much greater than λ ,

$$U_{\text{steady state}} = \lambda / \mu \quad \text{(Equation 2)}$$

Assuming that failures are not detected during normal operation, it is argued that the average time to restore includes detection time plus actual repair time. The average detection time equals one half the inspection period (proof test period) assuming that failures are equally likely at any time. If the actual repair time is insignificant compared to the inspection period, the average "repair" time (called mean time to restoration in IEC61508) is:

$$MTTR = T/2 \text{ and}$$

$$\mu = 2/T$$

Substituting this into equation 2 gives

$$PFD_{avg} = \lambda_d T / 2, \text{ the same result as Equation 1.} \quad \text{(Equation 3)}$$

The identical approximations of equation 1 and equation 3 lead many to conclude that either method, unreliability averaged or unavailability, may be used to calculate PFDavg. However, the equations are different for systems with redundancy in the safety function. A common example of this is the "1oo2" architecture. Different methods yield different results.

For example, a 1oo2 architecture has two components (Reference1, page 348). Using a probabilistic approach with steady state unavailability as PFDavg, each

component has a $PFD_{avg} = \lambda_d T / 2$ as stated in equation 3. In a fault tree with an AND gate, the probability of failure for two such components is multiplied giving a average (steady state based) system unavailability of:

$$PFD_{avg} = \lambda_d^2 T^2 / 4 \quad (\text{Equation 4})$$

If the same problem is modeled calculating steady state unavailability with a Markov model using a “one repairman” model, (Appendix 1) the

$$PFD_{avg} = \lambda_d^2 T^2 / 2 \quad (\text{Equation 5})$$

The same Markov model using a “two repairman” model (Appendix 2) shows a

$$PFD_{avg} = \lambda_d^2 T^2 / 4 \quad (\text{Equation 6})$$

The probability combination model shows the same result as a two repairman Markov model solved for steady state unavailability. It should be noted however that only the Markov model shows the assumption, it is hidden in the probability analysis.

There is a question. Which repairman model is more correct for the situation in which restoration time is dominated by the periodic inspection/test time interval?

In reality a repair team once summoned can restore one or two component failures in roughly the same time. So the Markov model should show a repair rate back to a fully operational system (as shown in Appendix 3).

The steady state solution for unavailability for this model provides a result of:

$$PFD_{avg} = \lambda_d^2 T^2 / 2 \quad (\text{Equation 7})$$

Most detail Markov models show this repair rate back to the fully restored state. Even if one uses a one repairman model and does not go back to the restored state, the results are the same or very close depending on the model.

Taking the same example further, consider the case of a 1oo2 system with PFD_{avg} calculated by averaging the unreliability function (shown in Appendix 4).

The unreliability (PFD) of a component is approximated by:

$$PFD(t) = \lambda_d t.$$

System failure occurs only if both components fail. Therefore, using a probabilistic approach expressed with a fault tree AND gate:

$$PFD(t) = (\lambda_d t)^2 \quad (\text{Equation 8})$$

When the average is calculated using

$$PFD_{avg} = \frac{1}{T} \int_0^T PFD(t) dt$$

the result is:

$$\text{PFD}_{\text{avg}} = (\lambda_{\text{dt}})^2/3 \quad (\text{Equation 9})$$

Another approach is to solve the Markov model for unreliability by obtaining the time dependent equations. This equation can be analytically averaged. This is shown in appendix 5. The result is:

$$\text{PFD}_{\text{avg}} = (\lambda_{\text{dt}})^2/3$$

The results show that the same results are obtained from either probabilistic methods or Markov methods. The differences are not caused by one method or another. The differences are caused by the approach – “steady state unavailability” versus “average unreliability.” The question remains as to which method is correct for this problem.

Insight can be gained by thinking about the real situation. After a period of time, an inspection and test of system is done. Any failures detected during the test and inspection are repaired. This is done periodically. The system never reaches steady-state. The steady-state unavailability approach is simply not valid. It is not valid using Markov models, probabilistic fault trees or any other method.

For this problem, the average unreliability approach provides the correct solution. This is explained in detail in the journal paper by Bukowski, reference 3. The average unreliability method was used to derive the simplified equations in ISA TR84.00.02, reference 4. Many SIL verification tools use Markov calculation techniques based on average unreliability, reference 5. More detailed equations for a full set of architectures based on average unreliability are provided in Appendix B of reference 6.

Conclusion

The solution technique where time dependent results are calculated and averaged will provide the most accurate model for “PFD_{avg}” in the situation where periodic inspection and test is done. Those who use the steady state unavailability approach with a one repairman model will get conservative, pessimistic results. This will result in a design that may provide too much safety.

A potential results when a steady state unavailability approach is used with a two repairman model. This is sometimes deliberately done with Markov analysis or accidentally done with a fault tree or other probabilistic analysis approach. That situation will lead to a result where insufficient safety may be designed into the system.

Assumptions

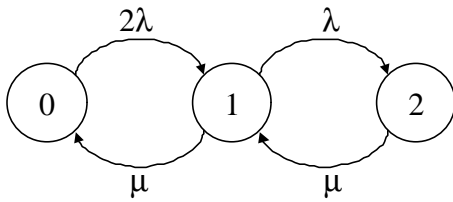
- All examples are done assuming a single failure mode, fail-danger with a constant failure rate.
- No common cause is modeled in the 1oo2 redundant system.
- Proof testing is assumed to be perfect and as such all failures will be detected during such a procedure.
- No diagnostic capability is modeled.

These assumptions are completely unrealistic but help show the point faster by excluding complexity. The conclusions reached apply equally to more complex models without these assumptions.

References

1. Goble, W. M., *Control System Safety Evaluation and Reliability*, ISA, NC: Raliegh, 1998. Available on the www.exida.com webstore.
2. Rouvroye, Jan, Enhanced Markov Analysis as a method to assess safety in the process industry, PhD Thesis, Technical University of Eindhoven, Netherlands, Eindhoven, 2001.
3. Bukowski, J. V., *Modeling and Analyzing the Effects of Periodic Inspection in the Performance of Safety-Critical Systems*, IEEE Transactions on Reliability, Volume 50, Number 3, IEEE, NY: New York, September 2001. Available on the www.exida.com free article web page.
4. ISA - TR84.00.02-2002, Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques, ISA, NC: Research Triangle Park, 2002 .
5. exida, *SILver – Safety Integrity Level Verification Tool*, Brochure, Version 3.0, February 2002.
6. Goble, W. M., The Use and Development of Quantitative Reliability and Safety Analysis in New Product Design, PhD Thesis, Technical University of Eindhoven, Netherlands, Eindhoven, 1998. Available on the www.exida.com webstore.

Appendix 1 – Steady state Markov model of 1oo2 redundancy with one repairman



Steady state equations

$$P_0 \cdot 2\mathbf{l} = P_1 \cdot \mathbf{m}$$

$$P_1 \cdot \mathbf{l} = P_2 \cdot \mathbf{m}$$

$$P_0 + P_1 + P_2 = 1$$

$$P_0 = \frac{\mathbf{m}}{2\mathbf{l}} \cdot P_1 = \frac{\mathbf{m}}{2\mathbf{l}} \cdot \frac{\mathbf{m}}{\mathbf{l}} \cdot P_2 = \frac{\mathbf{m}^2}{2\mathbf{l}^2} \cdot P_2$$

$$\frac{\mathbf{m}^2}{2\mathbf{l}^2} \cdot P_2 + \frac{\mathbf{m}}{\mathbf{l}} \cdot P_2 + P_2 = 1$$

$$P_2 \cdot \left(\frac{\mathbf{m}^2 + 2\mathbf{l}\mathbf{m} + 2\mathbf{l}^2}{2\mathbf{l}^2} \right) = 1$$

$$P_2 = \frac{2\mathbf{l}^2}{\mathbf{m}^2 + 2\mathbf{l}\mathbf{m} + 2\mathbf{l}^2}$$

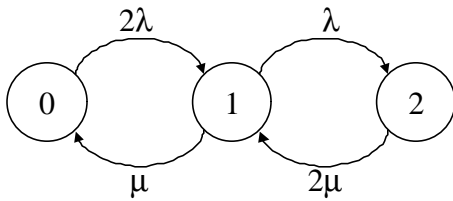
If $\mathbf{l} \ll \mathbf{m}$

$$P_2 = \frac{2\mathbf{l}^2}{\mathbf{m}^2}$$

If $\mathbf{m} = \frac{2}{t}$

$$P_2 = \frac{2\mathbf{l}^2}{\left(\frac{2}{t}\right)^2} = \frac{\mathbf{l}^2 \cdot t^2}{2}$$

Appendix 2 – Steady state Markov model of 1oo2 redundancy with two repairmen



Steady state equations

$$P_0 \cdot 2\mathbf{l} = P_1 \cdot \mathbf{m}$$

$$P_1 \cdot \mathbf{l} = P_2 \cdot 2\mathbf{m}$$

$$P_0 + P_1 + P_2 = 1$$

$$P_0 = \frac{\mathbf{m}}{2\mathbf{l}} \cdot P_1 = \frac{\mathbf{m}}{2\mathbf{l}} \cdot \frac{2\mathbf{m}}{\mathbf{l}} \cdot P_2 = \frac{\mathbf{m}^2}{\mathbf{l}^2} \cdot P_2$$

$$\frac{\mathbf{m}^2}{\mathbf{l}^2} \cdot P_2 + \frac{2\mathbf{m}}{\mathbf{l}} \cdot P_2 + P_2 = 1$$

$$P_2 \cdot \left(\frac{\mathbf{m}^2 + 2\mathbf{l}\mathbf{m} + \mathbf{l}^2}{\mathbf{l}^2} \right) = 1$$

$$P_2 = \frac{\mathbf{l}^2}{\mathbf{m}^2 + 2\mathbf{l}\mathbf{m} + \mathbf{l}^2}$$

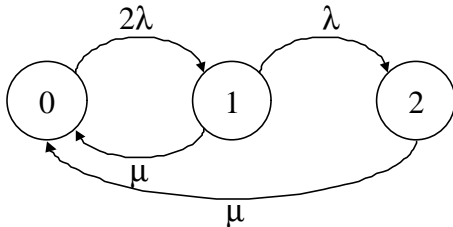
If $\mathbf{l} \ll \mathbf{m}$

$$P_2 = \frac{\mathbf{l}^2}{\mathbf{m}^2}$$

If $\mathbf{m} = \frac{2}{t}$

$$P_2 = \frac{\mathbf{l}^2}{\left(\frac{2}{t}\right)^2} = \frac{\mathbf{l}^2 \cdot t^2}{4}$$

Appendix 3 – Steady state Markov model of 1oo2 redundancy with full restoration after inspection and test period



Steady state equations

$$P_0 \cdot 2I = P_1 \cdot m + P_2 \cdot m$$

$$P_1 \cdot I = P_2 \cdot m$$

$$P_0 + P_1 + P_2 = 1$$

$$P_0 = \frac{m}{2I} \cdot (P_1 + P_2) = \frac{m}{2I} \cdot \left(\frac{m}{I} \cdot P_2 + P_2 \right) = \left(\frac{m^2}{2I^2} + \frac{m}{2I} \right) \cdot P_2$$

$$\left(\frac{m^2}{2I^2} + \frac{m}{2I} \right) \cdot P_2 + \frac{m}{I} \cdot P_2 + P_2 = 1$$

$$P_2 \cdot \left(\frac{m^2 + 3Im + 2I^2}{2I^2} \right) = 1$$

$$P_2 = \frac{2I^2}{m^2 + 3Im + 2I^2}$$

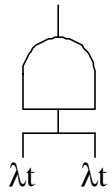
If $I \ll m$

$$P_2 = \frac{2I^2}{m^2}$$

If $m = \frac{2}{t}$

$$P_2 = \frac{2I^2}{\left(\frac{2}{t}\right)^2} = \frac{I^2 \cdot t^2}{2}$$

Appendix 4 – Probabilistic model (shown with fault tree) of 1oo2 redundancy with averaging before and after logic.



Integrate after logic

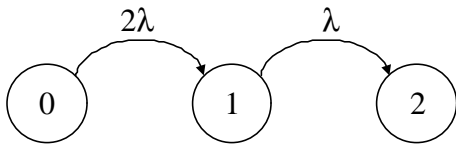
$$P = \frac{1}{t} \int_0^t (\mathbf{I} \cdot t')^2 dt' = \frac{\mathbf{I}^2 \cdot t^2}{3}$$

Integrate before logic

$$P = \left(\frac{1}{t} \int_0^t (\mathbf{I} \cdot t') dt' \right) \cdot \left(\frac{1}{t} \int_0^t (\mathbf{I} \cdot t') dt' \right) = \left(\frac{\mathbf{I} \cdot t}{2} \right) \cdot \left(\frac{\mathbf{I} \cdot t}{2} \right)$$

$$P = \frac{\mathbf{I}^2 \cdot t^2}{4}$$

Appendix 5 - Markov model solved with time dependent equations for average unreliability (reference 2, Appendix C)



The Markov model used in the demonstration of the effect of common cause failures as given in the above figure.

In a mathematical form this model can be described by a set of coupled differential equations and a starting condition given below. The different states are indicated by a subscript 0 for the OK state, a subscript 1 for the state with one component failed and a subscript 2 for the state with 2 components failed.

$$\frac{dP_0}{dt} = -2\mathbf{I}^D P_0$$

$$\frac{dP_1}{dt} = 2\mathbf{I}^D P_0 - \mathbf{I}^D P_1$$

$$\frac{dP_2}{dt} = \mathbf{I}^D P_1$$

$$P_0(t=0) = 1; \quad P_1(t=0) = P_2(t=0) = 0;$$

This model can be solved analytically using Laplace transforms. Using these transforms the set of differential equations is transformed to a set of linear equations. In these equations the Laplace transform of $P_i(t)$ is denoted by $p_i(s)$

$$sp_0 - 1 = -2\mathbf{I}^D p_0$$

$$sp_1 = 2\mathbf{I}^D p_0 - \mathbf{I}^D p_1$$

$$sp_2 = \mathbf{I}^D p_1$$

From the first equation p_0 can be solved:

$$p_0 = \frac{1}{s + 2\mathbf{I}^D}$$

Using this result in the second equation and rearranging gives the solution for p_1 :

$$p_1 = \frac{2\mathbf{I}^D}{(s + 2\mathbf{I}^D)(s + \mathbf{I}^D)}$$

Using partial fraction reduction this can be rewritten as:

$$p_1 = \frac{-2}{(s + 2\mathbf{I}^D)} + \frac{2}{(s + \mathbf{I}^D)}$$

Transforming the Laplace transforms p_1 and p_2 back to the time domain using the starting conditions and using the fact that $P_0(t) + P_1(t) + P_2(t) = 1$ results in:

$$P_0(t) = e^{-2I^D t}$$

$$P_1(t) = -2e^{-2I^D t} + 2e^{-I^D t}$$

$$P_2(t) = 1 + e^{-2I^D t} - 2e^{-I^D t}$$

$$PFD_{avg} = \frac{1}{T} \int_0^T P_2(t) dt = \frac{1}{T} \left[t - \frac{1}{2I^D} e^{-2I^D t} + \frac{2}{I^D} e^{-I^D t} \right]_0^T$$

$$PFD_{avg} = \frac{1}{T} \left[T - \frac{1}{2I^D} e^{-2I^D T} + \frac{2}{I^D} e^{-I^D T} \right] - \frac{1}{T} \left[-\frac{1}{2I^D} + \frac{2}{I^D} \right]$$

$$PFD_{avg} = 1 - \frac{1}{2I^D T} \left[e^{-2I^D T} - 4e^{-I^D T} \right] - \frac{3}{2I^D T}$$

Approximation for $I^D T \ll 1$:

$$PFD_{avg} = 1 - \frac{1}{2I^D T} \left(1 - (2I^D T) + \frac{1}{2}(2I^D T)^2 - \frac{1}{6}(2I^D T)^3 + \dots \right) - \frac{4}{2I^D T} \left(1 - (I^D T) + \frac{1}{2}(I^D T)^2 - \frac{1}{6}(I^D T)^3 + \dots \right) - \frac{3}{2I^D T}$$

$$PFD_{avg} = -\frac{1}{2I^D T} \left[-\frac{1}{6}(2I^D T)^3 + \frac{4}{6}(I^D T)^3 + \dots \right]$$

$$PFD_{avg} = \frac{1}{3}(I^D T)^2$$