T6A043

"Reliability – Fault Tolerant Systems"

DISCLAIMER: Whilst every effort has been made to ensure the accuracy of the information contained in this document neither "The 61508 Association" nor its members will assume any liability for any use made thereof.

1 Contents

2 Revision History

Version	Date	Author	Comments
0.1	18/01/2022	R. Martin	Draft release for public comment.
0.2	28/02/2022	R. Martin	Added wider context of reliability and references.
0.3	25/01/2023	R. Martin	Minor corrections to text. In 8.3.1, changed the 'du' common cause term for staggered testing to reflect the fact that one fault found would lead to further testing.
0.4	17/03/2023	R. Martin	MTTR updated to cover variants for diagnosed, undiagnosed and residual.
0.5	16/08/2023	R. Martin	Minor corrections to text. Foreword and Executive Summary updated.
0.6	04/01/2024	R. Martin	Corrected named references to other papers
0.7	17/01/2024	R. Martin	Update to add correction factor for the effect of synchronised testing and mission time replacement
1.0	26/01/2024	R. Martin	First issue.

3 Introduction / Foreword

This document covers the topic of fault tolerant systems in relation to functional safety and is part of a series of documents linking together to support a reliability calculation tool.

There are four documents in the series:

1. Reliability and Availability
2. Effects of Proof Testing
3. Fault Tolerant Systems
4. Staggered Proof Testing Coefficients

This document builds on the concepts developed in *Reliability and Availability* and *Effects of Proof Testing*.

Reliability and Availability explores the basic mathematics of reliability and explains:

- What is meant by constant failure rate;
- The effect of parallel and series networks;
- The relationship between λ and MTBF;
- The importance of repairable systems and Availability (as an average over time);
- The time average likelihood of being in a failed state (so called PFD_{AV});
- The other terms in common use for detected and undetected failures;
- The differing effects of detected and undetected failures;
- The effects of common proof testing regimes on multiple failures;
- The effects of common cause failures
- Simple and complex redundancy;
- Conditional Probability;
- Estimating reliability from data.

Effects of Proof Testing explores:

- The basic effects of synchronous proof testing.
- The basic effects of staggered proof testing.

This document pulls the developed ideas from the earlier documents to create an algorithm for calculating the system PFD and failure rate for an MooN fault tolerant system taking into account:

- detected, undetected and residual failures ('residual' covers the effect of an incomplete proof test);
- common cause factors for detected, undetected and residual failures;
- synchronous and staggered proof testing.

The resulting formulae (for MooN system failure rate and PFD) have been constructed as spreadsheet formulae covering 1oo1, 1oo2, 1oo3, 2oo3 and 2oo4 systems. These standard forms are on the workbook sheet labelled 'Calc Sheet'. For other MooN configurations, the workbook has a sheet labelled 'N-f': this uses VBA to calculate results. See this link to download workbook.

Note: There is an additional document *Staggered Proof Testing Coefficients* which details the algorithms and coding used to generate them.

4 Executive Summary

The development of this series of documents came as a result of *The 61508 Association* (T6A) setting up a working group (WG) to produce good practice guidance on 'SIL Assessment' (the assessment of the ability of a system to perform a required safety function with the required integrity).

The history of the development is as follows:

- T6A set up WG15 to produce a good practice guide for 'SIL Assessment'.
- It became apparent that a spreadsheet would be the most suitable tool to use because of its ability with computational calculations and the ease of access and familiarity to most people.
- It also became apparent that the spreadsheet needed a 'built in' reliability calculator so that all important reasoning could be separated from number crunching but also that 'verification' in any instance of use would be confined to the reasoning and the appropriate use of the calculator rather than the calculator itself. So, it was decided to create the 'built in' calculator.
- Before creating the calculator, it became necessary to produce the formulae upon which the calculator would be based.
- Reliability is taught at many higher educational establishments and there is much information on safety related systems calculations in circulation. However, the authors were unable to find a source that pulled it all together into general formulae. A document entitled 'Fault Tolerant Systems' was therefore created covering the development of the necessary formulae for calculating the failure rate and the probability of failure for so called 'MooN' fault tolerant systems.
- The formulae developed catered for diagnosed and undiagnosed failures, distortion due to synchronous proof testing and common cause failures.
- However, when the document was being verified, it became clear that verifiers needed some further explanation of the maths and (importantly) the development of the necessary terminology.
- Over time, it emerged that limited proof test coverage was becoming an issue of interest (especially to regulators). It also emerged that staggered proof testing for higher order systems gave considerable 'on paper' benefits. So, it was decided to add these two features to the calculator.
- As a result, three further documents were considered necessary:
    - One that covered the theory from first principles (now entitled Reliability and Availability).
    - One that covered the distorting effects of synchronous and staggered proof testing on the calculations (now entitled Effects of Proof Testing).

- Because finding the distorting effects of staggered testing proved to be quite complex (a mixture of analytical and numerical techniques were used) it was decided to make the deduction of the staggered testing coefficients into a separate documents (now entitled Staggered Proof Testing Coefficients).

The formulae have now been developed from first principles and the spreadsheet calculator produced. The documents and the calculator have been independently verified.

5 Terminology

f General term for 'fault tolerance' – i.e. for simple redundancy, the number of failed devices a system can tolerate and still perform its function.

Note: r is the general term for the number of survivors required for a system to perform its function.

F Probability of failure (normally a function of time).

Note: this has the same meaning at PFD (probability of failure on demand).

MT Mission Time (for use with residual failures)

MTBF Mean time before failure. $\mathrm{MTBF} = 1/\lambda$ (for constant λ)

MTTR Mean time to restore.

PFD Probability of failure on demand.

Notes:

- this has the same meaning as F (probability of failure).
- This is sometimes used in the text as shorthand for $\mathrm{PFD}_{\mathrm{AV}}$.

PFD_{AV} Time average of PFD.

PFD_D PFD for diagnosed failures for single channel / device.

$$PFD_D = PFD_D^1 = \left((1-\beta_D)\lambda dd.MTTR\right)$$

PFD_R PFD for residual failures for single channel / device.

$$PFD_R = PFD_R^1 = \left(\frac{(1-\beta_R)\lambda drMT}{2}\right)$$

PFD_U PFD for undiagnosed failures for single channel / device.

$$PFD_U = PFD_U^1 = \left(\frac{(1-\beta_U)\lambda duT}{2}\right)$$

PFD_D^k PFD for diagnosed failures for k channels / devices

$$PFD_D^k = (PFD_D)^k$$

PFD_R^k PFD for residual failures for k channels / devices

$PFD_R^k \neq (PFD_R)^k$ due to test regime

PFD_U^k PFD for undiagnosed failures for k channels / devices

$PFD_U^k \neq (PFD_U)^k$ due to replacement regime

PFD^N PFD rolled up for all failures for N channels / devices (including common causes)

R Probability of survival (normally a function of time).

$_S$ Used as a suffix to represent attributes of a system.

E.g. F_S is used to represent probability of system failure.

T Proof test interval.

β Beta factor – general term for fraction of failures which affect all channels / devices.

β_D Beta factor specific to diagnosed failures

β_D Beta factor specific to residual failures

β_U Beta factor specific to undiagnosed failures

λ General term for underlying failure rate – a function of time that represents the failure rate 'given that there is no current failure'. This document assumes it is a constant in time.

Note: this is not the same as $\dot{F}(t)$ (which is the failure rate not assuming current survival).

λ_d General term for diagnosed failure rate – i.e. failure that is automatically revealed.

λ_u General term for undiagnosed failure rate.

λ_{dd} Dangerous diagnosed failure rate.

λ_{dr} Dangerous residual failure rate – i.e. dangerous failure rate that is not automatically revealed or revealed by periodic proof test.

λ_{du} Dangerous undiagnosed failure rate.

6 Reliability Model

The accepted model (including that adopted by IEC 61508) is that of random hardware failures and constant failure rates in the throughout the useful life. Whilst this is a useful approximation in estimating reliability, it should be understood that reliability is not an exact science and approaches to modelling are still evolving.

Industrial databases of reliability statistics (such as OREDA) are often used in modelling the expected failure rates of complex systems. In practice, such databases tend to be conservative because they often account for failures wider than those of random hardware failures. This tends to lead to conservative claims (which is probably where we would like them to be in matters of safety).

However, caution is advised. Reliability of components of similar type can vary depending on the source. Stress factors in the installed environment can lead to considerable variation (i.e. it is not unusual to see variances of up to a factor of 3 either side of the norm.

The calculations described in this guideline may be applied to estimate the probability of failure for electrical, mechanical, pneumatic or hydraulic devices, but the precision is limited by the extent to which users can achieve reasonably consistent failure performance. The performance of equipment should be continually kept under review and maintenance practices and associated calculations modified to take account of findings.

The reader is advised to read as widely as practicable in order to understand the pitfalls of over-reliance on unrealistic assumptions. Books such as *Reliability, Maintainability and Risk* by Dr David J Smith [5] and papers such as *New approach to SIL verification* by Mirek Generowicz [6] make very useful reading in setting the overall context.

There are many other sources of information and guidance for reliability and availability, for example simplified formulas via ISA-TR84.00.02 and VDI/VDE 2180 Part 3 or IEC 61508-6:2010 Annex B (informative) for examples of more complete formulas.

7 Revision

The following is all revision from *Reliability and Availability* and from *Effects of Proof Testing* but is repeated here for ease of reading.

7.1 Diagnosed and Undiagnosed Failures

See *Reliability and Availability*.

For undiagnosed failures of a device:

$$PFDav = \lambda\left(MTTR + \frac{T}{2}\right)$$

Or where $MTTR \ll T$

$$PFDav = \frac{\lambda T}{2}$$

For diagnosed failures of a device:

$$PFDav = \lambda MTTR$$

Note: For a system that has diagnosed and undiagnosed failures, we distinguish the failure rates where: λ_u represents the undiagnosed failure and λ_d represents the diagnosed failures.

7.2 Simple Redundancy

For or fault tolerant systems with diagnosed failures, the $PFDav$ of the system is the product of the $PFDav$ of the devices.

For instance, for a 2oo2 to fail system: $PFDav = \lambda^2 MTTR^2$

And for a 3oo3 to fail system: $PFDav = \lambda^3 MTTR^3$

Note: this assumes the ideal case where failure and repair of one device is independent of another.

For undiagnosed failures, it may first be assumed that for the testing regime has a distorting effect. For example, for a 2oo2 to fail system, we may initially assume the PFD is the square of that for 1oo1 to fail – i.e. for 2oo2 to fail system:

$$PFDav = \frac{\lambda^2 T^2}{4}$$

However, for undiagnosed faults (see *Effects of Proof Testing)* for a 2oo2 to fail system, synchronised testing has a distorting effect which gives:

$$PFDav = \frac{\lambda^2 T^2}{3}$$

Later, we apply a Test Correction Factor to compensate for this effect.

7.3 General Equations for N-f

Where:

- N is the total number of units
- r is the number of survivors required to for the system to survive
- f is the Fault Tolerance (where f = N – r)

Then, from the above, the general form for the Probability of Failure on Demand and the Failure Rate of the system are given by the following (see *Reliability and Availability)*:

$$PFD_f^N = C_{f+1}^N . PFD^{f+1}$$

$$\lambda_f^N = C_f^N PFD^f . (N - f)\lambda$$

8 General N-f repairable system.

8.1 Systems with Diagnosed and Undiagnosed Faults

We split the failure rates into two components representing undiagnosed and diagnosed faults:

$$\lambda = \lambda_u + \lambda_d$$

Thus, for a 2oo2 to fail system which has a mixture of diagnosed and undiagnosed faults and synchronised testing, the PFDav is given by:

$$PFDav = \lambda^2 MTTR^2 + \frac{{\lambda_u}^2 T^2}{3} + 2\lambda MTTR \frac{\lambda_u T}{2}$$

Important note: In the above expression for PFDav, the term for diagnosed fault uses λ, rather than λ_d. This is because where a fault is found during testing, it results in a further outage during the repair time – in effect, it becomes a diagnosed failure at the point of testing and all faults are subject to repair.

In the following, we look at various system configuration in order to deduce the common rule for evaluating system failure likelihood.

Because the development of these equations is aimed at 'dangerous' failures, we have introduced an extra 'd' in the suffix to adopt more familiar terminology, where:

$$\lambda_d = \lambda_{du} + \lambda_{dd}$$

Note: In the following $PFDav$ is replaced by PFD for ease of reading.

8.2 Common Cause Failures.

Where there are common cause failures, this is usually represented as fraction (referred to as the 'β factor'). Note that the β factor can be different for diagnosed and undiagnosed failure. So here, we use βU and βD to distinguish them.

When there is a proportion of common cause failures it has the following modifying effect on the above formulae (where a fraction (β) of the failures act as though there is only one unit and the remaining fraction $(1 - \beta)$ act as though the failures are independent).

For example, for a 1oo2 to survive system (2oo2 to fail) with synchronous testing and undiagnosed failures:

$$PFD_S = \frac{((1-\beta_U)\lambda_{du}T)^2}{3} + \frac{\beta_U\lambda_{du}T}{2}$$

Note: only the first component of this formula has fault tolerance.

Likewise, for 1oo2 to survive system with diagnosed failures:

$$PFD_S = ((1-\beta_D)\lambda_{dd}MTTR)^2 + \beta_D\lambda_d MTTR$$

where only the first component has fault tolerance.

8.3 Expansion of the PFD term for du and dd faults

Allowing for common cause failures, if the effect of proof testing strategy on multiple channels is ignored, the general expansion of the PFD term has several terms depending on the diagnostic coverage, and common cause factors.

For a simplex system (1oo1), there is no common cause issue, and the expansion is:

$$PFD_{1oo1} = \frac{\lambda_{du}T}{2} + \lambda_d MTTR$$

This is in its simplest form, but we can also write:

$$PFD_{1oo1} = \frac{\lambda_{du}T}{2} + \lambda_{du}MTTR + \lambda_{dd}MTTR$$

We can expand this further to assist in the general form:

$$PFD_{1oo1} = \left[\left(\frac{(1-\beta_U)\lambda_{du}T}{2}\right) + \big((1-\beta_D)\lambda_{dd} + (1-\beta_U)\lambda_{du}\big)MTTR\right] + \frac{\beta_U\lambda_{du}T}{2} + (\beta_D\lambda_{dd})MTTR$$

Note: for a fault tolerant system, only the part in the square brackets has fault tolerance.

For a duplex system (2oo2 to fail), PFD_{2oo2} is written $(PFD)^2$ where:

$$(PFD)^2 \Rightarrow \left[\left(\frac{(1-\beta_U)\lambda_{du}T}{2}\right) + \big((1-\beta_D)\lambda_{dd} + (1-\beta_U)\lambda_{du}\big)MTTR\right]^2 + \frac{\beta_U\lambda_{du}T}{2} + (\beta_D\lambda_{dd})MTTR$$

For a triplex system (3oo3 to fail), PFD_{3oo3} is written $(PFD)^3$ where:

$$(PFD)^3 \Rightarrow \left[\left(\frac{(1-\beta_U)\lambda_{du}T}{2}\right) + \big((1-\beta_D)\lambda_{dd} + (1-\beta_U)\lambda_{du}\big)MTTR\right]^3 + \frac{\beta_U\lambda_{du}T}{2} + (\beta_D\lambda_{dd})MTTR$$

In general, we write:

$$(PFD)^N \Rightarrow [PFD_U + PFD_D]^N + \frac{\beta_U\lambda_{du}T}{2} + (\beta_D\lambda_{dd})MTTR$$

Where:

$$PFD_U = \frac{(1-\beta_U)\lambda_{du}T}{2}$$

and:

$$PFD_D = \big((1-\beta_D)\lambda_{dd} + (1-\beta_U)\lambda_{du}\big)MTTR$$

However, it is emphasised that there is a distortion effect on the above depending on proof testing strategy – see below.

8.3.1 Effect of Proof Testing Strategy in simple redundancy

8.3.1.1 Synchronised Proof Testing

We know from *Effects of Proof Testing* that synchronised proof testing on a fault tolerant system has a distorting effect such that:

$$PFD_{NooN} = \frac{2^N}{N+1}PFD_{1oo1}$$

Here, we write the same thing but using our new notation – the reason for the new notation will become apparent.

In general, where K is any positive integer, the formula for undetected failures (where synchronised testing is used) becomes:

$$PFD^K_{U_{Sy}} = \frac{2^K}{(K+1)}(PFD^1_U)^K$$

Where:
U denotes 'undetected'
S_y denotes 'synchronous testing'
PFD^K denotes PFD for $KooK$

In effect the 'test correction factor' for synchronised testing is:

$$\frac{2^K}{K+1}$$

8.3.1.2 Staggered Proof Testing

We know from *Staggered Proof Testing* that staggered (on rotation) proof testing has an associated 'test correction factors' that is available from a look-up table, such that:

$$PFD^K_{U_{St}} = St_{N,K}(PFD^1_U)^K$$

Where St$_{N,K}$ is given in the following table below (where *N* is the row and *K* is the column).

	1	2	3	4	5	6	7	8	9	10
1	1.0000									
2	1.0000	0.8333								
3	1.0000	0.8889	0.6667							
4	1.0000	0.9167	0.7500	0.5229						
5	1.0000	0.9333	0.8000	0.6144	0.4053					
6	1.0000	0.9444	0.8333	0.6765	0.4938	0.3117				
7	1.0000	0.9524	0.8571	0.7215	0.5598	0.3917	0.2383			
8	1.0000	0.9583	0.8750	0.7555	0.6107	0.4558	0.3076	0.1814		
9	1.0000	0.9630	0.8889	0.7821	0.6511	0.5080	0.3666	0.2398	0.1376	
10	1.0000	0.9667	0.9000	0.8035	0.6840	0.5514	0.4170	0.2920	0.1858	0.1041

Note: For proof testing against common cause failures in a staggered testing regime, if a fault is found in one channel, then all channels would need to be tested to cover potential common cause failure. This has an effect on the common cause $PFDu$.

Therefore, the formula for PFD taking into account common cause, diagnostic coverage and testing strategy becomes:

$$PFD^N = [PFD_U + PFD_D]^N + \frac{\beta_U \lambda_{du} T}{2(N)^{St}} + \beta_D \lambda_{dd} MTTR$$

Where:

for synchronised testing

$$PFD^K_U = \left(\frac{2^K}{(K+1)}\right)(PFD^1_U)^K$$

$$St = 0$$

for staggered testing

$$PFD_U^K = St_{N,K}(PFD_U^1)^K$$

$$St = 1$$

$$PFD_U^1 = \left(\frac{(1-\beta_U)\lambda_{du}T}{2}\right)$$

$$PFD_D^1 = ((1-\beta_D)\lambda_{dd} + (1-\beta_U)\lambda_{du})MTTR$$

8.3.2 Effect of Residual Hardware Failures

In general, were refer to a 'diagnostics' coverage factor (often denoted as 'C') as the fraction of dangerous failures of a component which are 'detected' and thus may be acted upon. The remainder is taken to be the 'undetected' portion which is the subject of proof testing.

In some cases, however, there are potential failures which are not detected by diagnostics or by proof test: the result of an incomplete proof test.

It has the effect of a residual hardware failure term which can only be reset to zero as a consequence of renewal. The term used here is 'residual' failures and it is associated with the mission time (MT) of an item but could equally be related to a longer test period where complete testing is carried out.

$$PFD_R^1 = \left(\frac{(1-\beta_R)\lambda_{dr}MT}{2}\right)$$

Where λ_{dr} is the residual dangerous failure rate and MT is the mission time.

$$\lambda_d = \lambda_{du} + \lambda_{dd} + \lambda_{dr}$$

Note that there will be an element of channel unavailability based on the need for replacement at the end of the mission time.

Assuming that the down time is the same as for others (i.e. $MTTR$), the expression of unavailability is given by:

$$\frac{MTTR}{MT}$$

The unavailability due to being replaced is generally covered by the PFD_D term. We therefore update this term:

$$PFD_D^1 = ((1-\beta_D)\lambda_{dd} + (1-\beta_U)\lambda_{du} + \frac{1}{MT})MTTR$$

It can be seen that this formula has the same general form as that for the PFD of other undetected failures with the proof test interval replaced by mission time.

Note: it is possible to replace items at the same time or on a staggered basis.

In some cases, the $MTTR$ can vary depending on the event that leads to the requirement to restore. It is therefore replaced by three separate terms.

$$PFD_D^1 = (1-\beta_D)\lambda_{dd}MTTR_d + (1-\beta_U)\lambda_{du}MTTR_u + \frac{MTTR_r}{MT}$$

Therefore, the formula for PFD taking into account common cause, diagnostic coverage and testing strategy becomes:

$$PFD^N = [PFD_U + PFD_R + PFD_D]^N + \frac{\beta_R\lambda_{dr}MT}{2} + \frac{\beta_U\lambda_{du}T}{2(N)^{St}} + \beta_D\lambda_{dd}MTTR_d$$

Where for synchronised testing:

$$PFD_U^K = \left(\frac{2^K}{(K+1)}\right)(PFD_U^1)^K$$

$$St = 0$$

and for staggered testing:

$$PFD_U^K = St_{M,N}(PFD_U^1)^K$$

$$St = 1$$

Where for synchronised replacement:

$$PFD_R^K = \left(\frac{2^K}{(K+1)}\right)(PFD_R^1)^K$$

and for staggered replacement:

$$PFD_R^K = St_{N,K}(PFD_R^1)^K$$

$$PFD_D^1 = (1-\beta_D)\lambda_{dd}MTTR_d + (1-\beta_U)\lambda_{du}MTTR_u + \frac{MTTR_r}{MT}$$

$$PFD_R^1 = \left(\frac{(1-\beta_R)\lambda_{dr}MT}{2}\right)$$

$$PFD_U^1 = \left(\frac{(1-\beta_U)\lambda_{du}T}{2}\right)$$

8.3.3 Expansion of non-common cause term

Here, we're going to remind ourselves of binomial expansion and extend it.

In the section above, to expand the term in square brackets, the binomial expansion is applied.

$$(a+b)^n = a^n + na^{n-1}b + \frac{n(n-1)a^{n-2}b^2}{2!} + \frac{n(n-1)(n-2)a^{n-3}b^3}{3!} + \ldots$$

for a total of $n+1$ terms

This can be written as:

$$(a+b)^n = \sum_{j=0}^{n} C_j^n \, a^{n-j} b^j$$

If it is required to expand with a third term, replace b in the above by $b+c$

$$(a+(b+c))^n = \sum_{j=0}^{n} C_j^n \, a^{n-j}(b+c)^j$$

But from the above it can be seen that:

$$(b+c)^j = \sum_{i=0}^{j} C_i^j \, b^{j-i} c^i$$

So

$$(a+b+c)^n = \sum_{j=0}^{n} (C_j^n \, a^{n-j} \sum_{i=0}^{j} (C_i^j \, b^{j-i} c^i))$$

Using this form to replace the previously developed expression:

$$PFD^N = [PFD_U + PFD_R + PFD_D]^N + \frac{\beta_R \lambda_{dr} MT}{2} + \frac{\beta_U \lambda_{du} T}{2(N)^{St}} + (\beta_D \lambda_{dd}) MTTR_d$$

We now write:

$$PFD^N = \sum_{j=0}^{N} \left(C_j^N . PFD_D^{N-j} \sum_{i=0}^{j} (C_i^j . PFD_U^{j-i} . {PFD_R}^i) \right) + \frac{\beta_U \lambda_{du} T}{2} + \frac{\beta_R \lambda_{dr} MT}{2} + (\beta_D \lambda_{dd}) MTTR_d$$

Where for synchronised testing $PFD_U^K = \left(\frac{2^K}{(K+1)}\right) (PFD_U^1)^K$

$$St = 0$$

for staggered testing $PFD_U^K = St_{N,K}(PFD_R^1)^K$

$$St = 1$$

for synchronised replacement $PFD_R^K = \left(\frac{2^K}{(K+1)}\right)(PFD_R^1)^K$

for staggered replacement $PFD_R^K = St_{N,K}(PFD_R^1)^K$

$$PFD_D^1 = (1-\beta_D)\lambda_{dd}MTTR_d + (1-\beta_U)\lambda_{du}MTTR_u + \frac{MTTR_r}{MT}$$

$$PFD_R^1 = \left(\frac{(1-\beta_R)\lambda_{dr}MT}{2}\right)$$

$$PFD_U^1 = \left(\frac{(1-\beta_U)\lambda_{du}T}{2}\right)$$

8.3.4 Synchronised Testing and Replacement

The formulae have so far assumed that PFD_R is independent of PFD_U . However, in the case where testing and replacement are both synchronised and they are synchronised with one another, there is a further distorting effect that requires correction.

The most common form of testing regime is for synchronised testing on an annual basis. If parts of a function remained untested due to partial proof testing then the thorough testing, refurbishment or replacement is also likely to be synchronised and the two regimes (testing and replacement) synchronised with one another. Where MT>>T, the effect is limited but otherwise, it can be significant.

From *Effects of Proof Testing*, the correction factor (limited to 2nd order) takes the form:

$$1 + P_1Z^{-1} + P_2Z^{-2}$$

Where:

$$P_1 = \frac{x(y+1)}{2x+4}$$

$x = 1$: $P_2 = 0$

$y = 1$: $P_2 = 0$

x≠1, y≠1:

$$P_2 = (-4.847e^{-4}x^2 + 1.047e^{-2}x - 1.054e^{-2})(y^2 + y)$$

x is the index applied to PFD_U and y is the index applied to PFD_R

$$Z = \frac{MT}{T}$$

The formula for therefore becomes:

$$PFD^N = \sum_{j=0}^{N}\left(C_j^N.PFD_D^{N-j}\sum_{i=0}^{j}(C_i^j.PFD_U^{j-i}.PFD_R{}^i.TF_{UR})\right) + \frac{\beta_U\lambda_{du}T}{2} + \frac{\beta_R\lambda_{dr}MT}{2} + (\beta_D\lambda_{dd})MTTR$$

Where, for synchronised testing and replacement:

$$TF_{UR} = 1 + P_1Z^{-1} + P_2Z^{-2}$$

Else:

$$TF_{UR} = 1$$

Where:

$$Z = \frac{MT}{T}$$

and:

$P_1 = 0$ $(i < 1)$

$P_1 = 0$ $(j - i < 1)$

$P_1 = (j - i)(i + 1)/(2(j - i) + 4)$ (else)

$P_2 = 0$ $(i = 1)$

$P_2 = 0$ $(j - i = 1)$

$P_2 = (-4.847e^{-4}(j - i)^2 + 1.047e^{-2}(j - i) - 1.054e^{-2})(i^2 + i)$ (else)

8.4 PFD and λ for N-f Fault Tolerant Systems

From section 7.3, we have the following generalised formulae which come from *Reliability and Availability*:

$$PFD_f^N = C_{f+1}^N . PFD^{f+1}$$

$$\lambda_f^N = (N-f)\lambda_d . C_f^N . PFD^f$$

We are going to use formulae developed above to insert into these generalised formulae for system PFD and failure rate. Note: the terminology on the left hand side of the equation is slightly different from the right where PFD_f^N means the PFD for a system of N channels with fault tolerance of f.

These terms are now expanded to include the derived terms due to synchronised or staggered testing and for common cause failures.

We get:

$$PFD_f^N = C_{f+1}^N . \sum_{j=0}^{f+1}\left(C_j^{f+1} . PFD_D^{f+1-j}\sum_{i=0}^{j}\left(C_i^j . PFD_U^{j-i} . PFD_R^i . TF_{UR}\right)\right) + PFDcc_U + PFDcc_R + PFDcc_D$$

$$\lambda_f^N = (N-f)\lambda_d . C_f^N\sum_{j=0}^{f}\left(C_j^f . PFD_D^{f-j}\sum_{i=0}^{j}\left(C_i^j . PFD_U^{j-i} . PFD_R^i . TF_{UR}\right)\right) + \lambda cc_U + \lambda cc_R + \lambda cc_D$$

Where for undiagnosed failures $PFD_U^K = TF^K(PFD_U^1)^K$

and for residual failures $PFD_R^K = TF^K(PFD_R^1)^K$

Where for synchronised testing or replacement:

$$TF^K = \left(\frac{2^K}{(K+1)}\right)$$

and, for staggered testing or replacement

$$TF^K = St_{N,K}$$

Where:

$TF_{UR} = 1 + P_1 Z^{-1} + P_2 Z^{-2}$ (for synchronised testing and replacement)

$TF_{UR} = 1$ (else)

Where: $Z = MT/T$

and: $P_1 = 0$ $(i < 1)$

$$P_1 = 0 \qquad (j - i < 1)$$

$$P_1 = (j - i)(i + 1)/(2(j - i) + 4) \qquad \text{(else)}$$

$$P_2 = 0 \qquad (i < 2)$$

$$P_2 = 0 \qquad (j - i < 2)$$

$$P_2 = (-4.847e^{-4}(j - i)^2 + 1.047e^{-2}(j - i) - 1.054e^{-2})(i^2 + i) \qquad \text{(else)}$$

$$PFD_D^1 = (1 - \beta_D)\lambda_{dd}MTTR_d + (1 - \beta_U)\lambda_{du}MTTR_u + \frac{MTTR_r}{MT}$$

$$PFD_R^1 = \left(\frac{(1 - \beta_R)\lambda_{dr}MT}{2}\right)$$

$$PFD_U^1 = \left(\frac{(1 - \beta_U)\lambda_{du}T}{2}\right)$$

$$PFDcc_D = \beta_D\lambda_{dd}MTTR_d$$

$$PFDcc_R = \frac{\beta_R\lambda_{dr}MT}{2}$$

$PFDcc_U = \beta_U\lambda_{du}T/2$ for synchronised testing and $PFDcc_U = \beta_U\lambda_{du}T/2N$ for staggered testing

$$\lambda cc_D = \beta_D\lambda_{dd}$$

$$\lambda cc_R = \beta_R\lambda_{dr}$$

$$\lambda cc_U = \beta_U\lambda_{du}$$

9 References

1. IEC 61508, *Functional safety of electrical / electronic / programmable electronic (E/E/PE) safety related systems*, Parts 1-7, 2010 (includes EN and BS EN variants).
2. IEC 61511, *Functional safety – Safety instrumented systems for the process industry sector*, Parts 1-3, 2017 (includes A1:2017 and the EN and BS EN variants).
3. ISA-TR84.00.02-2002 Part 1, *Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques – Part 1: Introduction*, 2002.
4. ISA-TR84.00.02-2002 Part 2, *Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques – Part 2: Determining the SIL of a SIF via Simplified Equations*, 2002.
5. VDI/VDE 2180 Part 3, *Functional safety in the process industry – Verification of probability of failure on demand (PFD)*, 2019.
6. SINTEF A11612, *Unrestricted Report – Use of the PDS Method for Railway Applications*, June 2009.
7. Reliability Maintainability and Risk (10th Edition) – Dr David J Smith.
8. New approach to SIL verification – Mirek Generowicz of I&E Systems Pty – Australia (available free to download from The 61508 Association website).

10 Conclusion

An Excel workbook ‘PFD Calculator’ has been produced and verified in conjunction with Mirek Generowicz (I&E Systems Pty Ltd.). The PFD Calculator performs system PFD and system failure rate calculations for MooN channel systems. The spreadsheet has been arranged such that calculations can be kept separate from analysis and reasoning, the intention being that a calculation is used for each subsystem. There are standard spreadsheet formulae covering common arrangements (1oo1, 1oo2, 1oo3, 2oo3, 2oo4) but there is also a VBA calculator that can handle up to N=10 for any feasible M.

The calculator could readily be extended for greater values of N (the restriction is quite arbitrary) but, for use with staggered testing or replacement would also require the extension of the staggered test factors for the highest value of M to be used.

The values for staggered test factors have currently been extended empirically to 20. The VBA code that produces them (up to 10) is also included in the workbook where it uses 10 nested loops to produce them (the author was not able to find a way to produce the values without using nested loops and decided to stop at 10).

The contribution of some elements of the calculations can be very small so as to become insignificant in many typical systems, so it could be asked why they are there. The answer is because there are outliers that are not necessarily foremost in our minds but that crop up from time to time which do require the refinements. Because there is no additional effort in performing 'exact' calculations, it is better to have a tool that copes with all possible outliers rather than one that is based on assumptions that may not be universal.

For instance, it may be that what is referred to as 'residual failures' (meaning untested failures) in a particular instance has no significant effect on the overall calculation because the expected channel down time for those failures is insignificant compared to that of other types of failure.

Using a tool that sometimes calculates insignificant components is not a problem when it is done deterministically and in an instant. We should never feel forced to enter every parameter just because it's there. If there are no residual failures to be accounted for, the inputs can all be configured so that there is a null effect.

It is also good to have an 'open' tool (i.e. where it is possible to see how the calculation is being performed) so that any user is able to verify that the calculations are following the stated formulae in this document. The overall gain of this approach is that verification of a particular instance only needs to cover the reasoning and the appropriate use of the tool: the tool itself has been separately verified.

11 Existing and Emerging Standards

IEC 61508:2010 (series of standards, Edition 2).
IEC 61511-1:2017+A1:2017 (Edition 2).

12 61508 Association Recommended Practices

This document sets out to describe current best practices in reliability for functional safety systems, but does not seek to prescribe specific measures, since these will depend on the application and any existing constraints of the installation.

DISCLAIMER: Whilst every effort has been made to ensure the accuracy of the information contained in this document neither "The 61508 Association" nor its members will assume any liability for any use made thereof.

*** END OF DOCUMENT ***