T6A043

"Development Paper – Fault Tolerant Systems"

1 Contents

2 Revision History

Version	Date	Author	Comments
0.1	18/01/2022	RM	Draft release for public comment.
0.2	28/02/2022	RM	Added wider context of reliability and references.

3 Introduction / Foreword

This development paper is not yet complete or fully reviewed by members of The 61508 Association. This paper has been published to elicit further comment and input on the comments within the paper from both members of the Association and any other interested party from outside the Association. Please send all comments on this paper to the Association coordinator via the email: info@61508.org.

Message from the initial author:
I've put this together to help explain some of the more detailed concepts of reliability and the maths behind it when it comes to random hardware failures: again, mostly as a helpful reminder for myself.

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 rest to create an algorithm for calculating the system PFD and failure rate for a N-f 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 idea is then to embed formulae for standard configurations into an Excel spreadsheet with additional VBA programming for higher order systems.

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

Ray Martin

4 Executive Summary

This paper is not yet complete; therefore, an executive summary is not yet required. This paper has been published in this form to elicit comments on the content.

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. 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 PFD_{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 paper 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.

7 Revision

The following is all revision from *Reliability and Maintainability* and from *Random Hardware Failures* 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 *Random Hardware Failures)* 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 β_U and β_D 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-β) 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:

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

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:

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

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

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

In general, we write:

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

Where:

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

and:

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

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 *Random Hardware Failures* 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

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

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

Where:

for synchronised testing

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

for staggered testing

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

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

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

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. These may be the result of failed diagnostics and/or the result of an incomplete proof test.

In either case, 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 of an item.

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

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.

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

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

Where

for synchronised testing

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

for staggered testing

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

for synchronised replacement

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

for staggered replacement

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

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

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

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

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:

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

We now write:

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

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

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

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

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

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

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

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

8.4 PFD and λ for N-f Fault Tolerant Systems

From section 6.3, 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:

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

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

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

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

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

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

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

$$PFDcc_D = (\beta_U \lambda_{du} + \beta_D \lambda_{dd})MTTR$$

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

$$PFDcc_U = \frac{\beta_U \lambda_{du} T}{2}$$

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

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

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

8.5 Common Configurations

8.5.1 1oo1

$$PFD_0^1 = (\lambda_{dd} + \lambda_{dd} + \frac{1}{MT})MTTR + \left(\frac{\lambda_{dr} MT}{2}\right) + \left(\frac{\lambda_{du} T}{2}\right)$$

$$\lambda_0^1 = \lambda_d$$

8.5.2 1oo2 (N=2, f=1)

$$PFD_1^2 = (PFD_D^1)^2 + (PFD_U^1)^2 . TF_U^2 + (PFD_R^1)^2 . TF_R^2 + 2(PFD_D^1 + PFD_U^1 + PFD_R^1) + PFDcc_U + PFDcc_R + PFDcc_D$$

$$\lambda_1^2 = 2\lambda_d (PFD_D^1 + PFD_U^1 + PFD_R^1) + \lambda cc_U + \lambda cc_R + \lambda cc_D$$

Where TF represents the relevant Test Correction Factor

8.5.3 2oo3 (N=3, f=1)

$$PFD_2^3 = 3((PFD_D^1)^2 + (PFD_U^1)^2 . TF_U^2 + (PFD_R^1)^2 . TF_R^2) + 6(PFD_D^1 + PFD_U^1 . + PFD_R^1 .) + PFDcc_U + PFDcc_R + PFDcc_D$$

$$\lambda_2^3 = 6\lambda_d (PFD_D^1 + PFD_U^1 . + PFD_R^1 .) + \lambda cc_U + \lambda cc_R + \lambda cc_D$$

Where TF represents the relevant Test Correction Factor

9 References

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

10 Conclusion

This paper is not yet complete; therefore, a conclusion is not yet required. This paper has been published in this form to elicit comments on the content.

11 Existing and Emerging Standards

IEC 61508 Edition 2.
IEC 61511 Edition 2.

12 61508 Association Recommended Practices

This document sets out to describe current best practices in *Reliability and Availability* 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.

This paper is not yet completed, it has been published solely to elicit comment and encourage input to further develop the technical content.

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 ***