T6A042

"Development Paper – Effects of Proof Testing"

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	Title changed and document restructured to fully cover the topics of synchronised and staggered proof testing. 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 basic concepts of reliability and the maths behind it: mostly as a helpful reminder for myself. The modelling of reliability is taught in many higher education establishments and there are many text books on the subject but I haven't found a text that develops what I need to know from the ground upwards.
This model (together with an associated calculation tool) is developed from first principles using consistent terminology and is arranged over a series of papers (an attempt to break it down into manageable chunks). I hope it may also be of help to others.

There are four papers:

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

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 diagnosed and undiagnosed failures;
- The differing effects of diagnosed and undiagnosed 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.

This paper is the second in the series. It looks specifically at the effect of proof testing and the strategy employed. Proof testing scenarios considered are:

- synchronous proof test (where all components in parallel are proof tested in the same task at time interval, T)
- staggered proof test (where the proof testing is on each component is carried out at time intervals, T, but where they are evenly spaced in time.

Each of the above has a distorting effect on PFD^i such that $PFD^i \neq (PFD)^i$

The study of both strategies returns *Test Factors* which are used to compensate for the above inequality.

It should be noted that:

- synchronous proof testing has a detrimental effect such that $PFD^i > (PFD)^i$
- staggered proof testing has a beneficial effect such that $PFD^i < (PFD)^i$

Here we expand on some of the issues already discussed by looking at further at the distorting effects of proof testing strategy on the algebra but not the sub-sets for:

- Synchronous proof testing
- Staggered proof testing

Note: The generation of coefficients for staggered proof testing is complex and thus there is an additional document *Staggered Proof Testing Coefficients* dedicated to their development.

Because of my interests in functional safety, I have tried to relate this theory to safety where relevant. But it should be understood that reliability and availability are broader topics. So, although I try to relate them to functional safety where relevant, it is not a 'safety only' subject and the maths derived is just as applicable to reliability in general.

There are other models available - e.g. ISA 84 Part 2 [3], SINTEF PDS method [4]. Some are more comprehensive than others and all have limitations. IEC 61508 [1] stresses the importance that the analyst understands the techniques and the limitations of any underlying hypothesis. I don't think this is possible without the use of a text that derives the approach from first principles and emphasises the limitations in any step.

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_R	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.

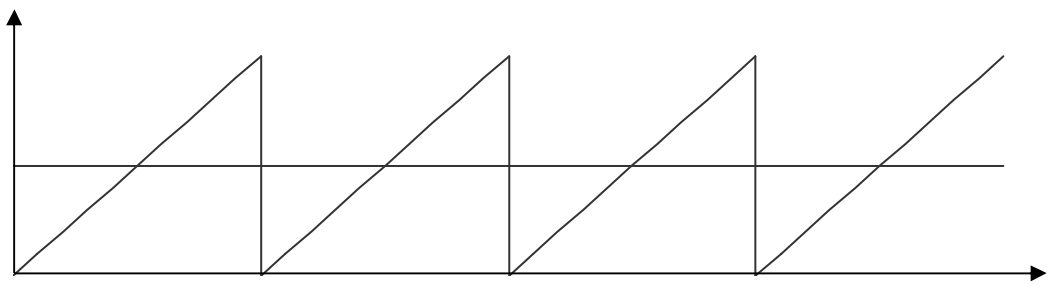
The reader is advised to read as widely as practicable in order to understand the pitfalls of over-reliance on unrealistic assumptions. Books such as *Reliability, Maintainability and Risk* by Dr David J Smith [5] and papers such as *New approach to SIL verification* by Mirek Generowicz [6] make very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

7 Synchronised Proof Testing in Simple Redundancy

Each time a device is tested it will either be found to be working or it will be repaired.

The effect on the probability of failure as a function of time is shown below. At each proof test, the probability of failure is 'reset' to 0. This results in the 'saw tooth' type function.

Note: In safety systems, we refer to the *probability of failure on demand* (PFD) but this is no different from F(t). In particular, we refer to the average probability of failure on demand (PFD_{AV}) because this becomes a very useful measure when considering overall risk.



We can see from the above that the average over time is the same as the average over one proof test interval.

$$PFD_{AV} = \frac{1}{T}\int_0^T \lambda t dt = \frac{\lambda}{T}\frac{T^2}{2} = \frac{\lambda T}{2}$$

$$PFD_{AV} = \frac{\lambda T}{2}$$

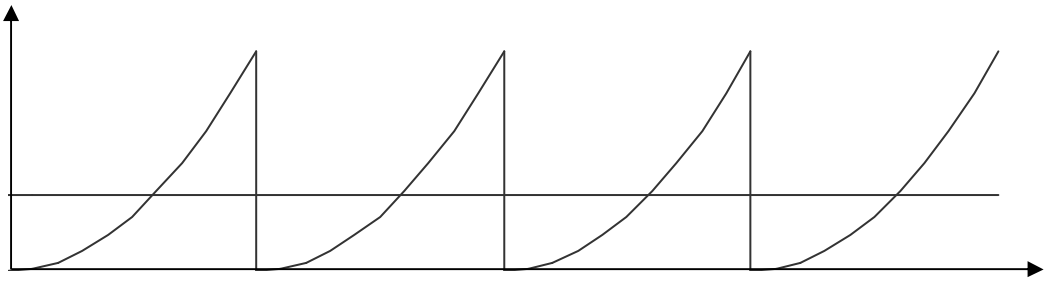
We can write this as:

$$PFD_{1oo1} = \frac{\lambda T}{2}$$

Note: The above ignores the time out of service during which an item discovered in the failed condition is 'under repair'.

7.1 1oo2 simple redundancy

If we assume that testing is synchronised (i.e. both devices are tested at the same time), the PFD_{AV} is derived as follows.



The average of a cycle is given by:

$$PFD_{AV} = \frac{1}{T}\int_0^T \lambda^2 t^2 dt = \frac{\lambda^2}{T}\frac{T^3}{3} = \frac{\lambda^2 T^2}{3}$$

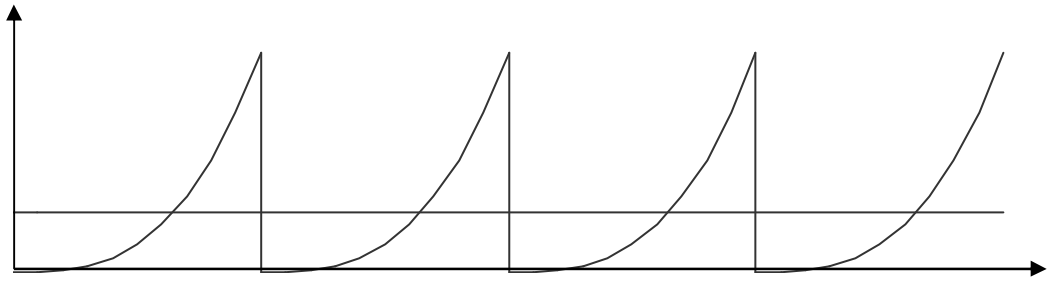
$$PFD_{AV} = \frac{\lambda^2 T^2}{3}$$

So, for synchronised proof testing there is a degradation factor of 4/3, i.e.:

$$PFD_{1oo2} = \frac{4}{3} PFD_{1oo1}^2$$

7.2 1oo3 simple redundancy

If we assume that testing is synchronised, the resulting PFD_{AV} is derived as follows.



The average of a cycle is given by:

$$PFD_{AV} = \frac{1}{T}\int_0^T \lambda^3 t^3 dt = \frac{\lambda^3}{T}\frac{T^4}{4} = \frac{\lambda^3 T^3}{4}$$

So, for synchronised proof testing there is a degradation factor of 8/4, i.e.:

$$PFD_{1oo3} = 2PFD_{1oo1}^{3}$$

In this latter case, the PFD average of the system is twice what we would get by taking the cube of the simplex PFD_{AV}.

7.3 1ooN simple redundancy

The effect on PFD_{AV} of synchronised proof testing on simple redundancy is summarised in the following table. Note: here 1ooN represents 1 out of N for system survival.

To survive	PFD_{AV}
1oo1	PFD_{1oo1}
1oo2	$4/3(PFD_{1oo1})^2$
1oo3	$8/4(PFD_{1oo1})^3$
1oo4	$16/5(PFD_{1oo1})^4$
1oo5	$32/6(PFD_{1oo1})^5$
1ooN	$(2^N/N+1)(PFD_{1oo1})^N$

Trying the formula for 2oo2 to fail, $PFD_{AV} = 4/3(PFD_{1oo1})^2$, i.e.:

$$PFD_{AV} = \frac{4}{3}\frac{\lambda^2 T^2}{4}$$

Note: For 2oo3, there are 3 possible combinations of 2oo2 to fail so the PFD_{AV} is 3 times that.

$$PFD_{2oo3} = \lambda^2 T^2$$

So 2oo3 has a worse safety performance than 2oo2 to fail!

The reasons we commonly use 2oo3 are:

- it reduces spurious system failure rate and
- it allows additional discrepancy checking.

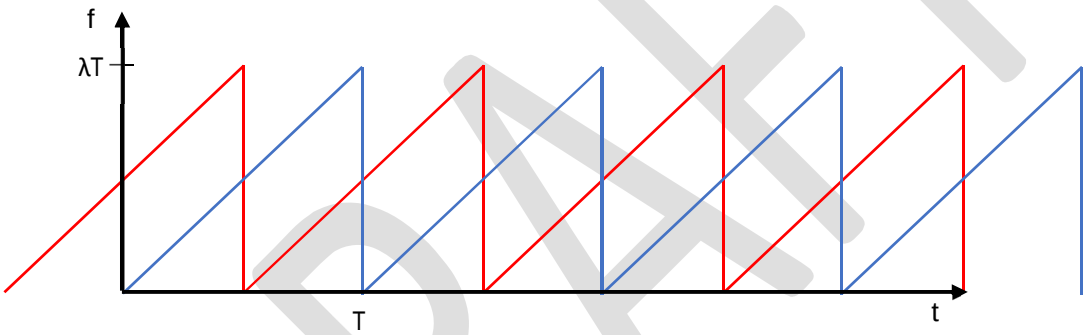
8 Staggered Proof Test in Simple Redundancy

Staggered proof testing has a different effect on PFD_{AV}. Whereas, with synchronous testing, the effect for 1ooN system is a PFD_{AV} which is worse than $(PFD_{1oo1})^N$, staggered proof testing has the opposite effect.

Note: It would be very unusual for inputs of a SIF function to be tested 'on rotation'. Given that it leads to some quite complex algebra, it would be possible to accept that proof testing on rotation (staggered proof testing) is a possibility but not to study the development of the relevant coefficients.

8.1 1oo2 simple redundancy (2oo2 to fail)

If we assume that testing is staggered evenly, the PFD_{AV} is derived as follows:



The red and blue lines represent the failure probability of the two channels. The failure probability of the system is the product of the two. We can see that the system failure probability repeats each period of T/2.

The average can therefore be found by integrating over any period T/2 and dividing by the period. Starting at T=0:

$$F(t) = \lambda t.(\lambda t + \frac{\lambda T}{2})$$

$$F(t) = \lambda^2(t^2 + \frac{T}{2}t)$$

$$PFD_{AV} = F_{AV} = \frac{1}{T/2}\int_0^{T/2} F(t)\,dt$$

$$PFD_{AV} = \frac{1}{T/2}\int_0^{T/2} \lambda^2\left(t^2 + \frac{T}{2}t\right)dt$$

$$PFD_{AV} = \frac{\lambda^2}{T/2}\left[\frac{t^3}{3} + \frac{T}{2}.\frac{t^2}{2}\right]_0^{T/2}$$

$$PFD_{AV} = \frac{\lambda^2}{T/2}\left(\frac{T^3}{3.2^3} + \frac{T^3}{2.2^3}\right)$$

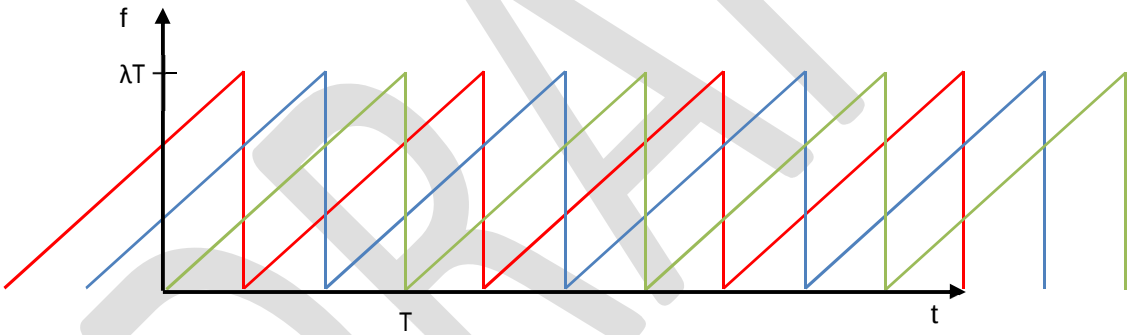
$$PFD_{AV} = \lambda^2 T^2\left(\frac{1}{3.2^2} + \frac{1}{2.2^2}\right)$$

$$PFD_{AV} = \frac{\lambda^2 T^2}{2^2}\left(\frac{1}{3} + \frac{1}{2}\right) = \frac{5}{6}.\frac{\lambda^2 T^2}{2^2}$$

$$PFD_{AV} = \frac{5}{6} PFD_{1oo1}{}^2$$

8.2 **1oo3 simple redundancy**

If we assume that testing is staggered evenly, the resulting PFD_{AV} is derived as follows.



The red, blue and green lines represent the different channels and the combined system failure is the product of the three. We can see that the system failure repeats each period of T/3.

The average is found by integrating over the period and dividing by the period. In each period of T/3:

$$F(t) = \lambda t.\left(\lambda t + \frac{\lambda T}{3}\right).\left(\lambda t + \frac{2\lambda T}{3}\right)$$

$$F(t) = \lambda^3\left(t^3 + 3\left(\frac{T}{3}\right)t^2 + 2\left(\frac{T}{3}\right)^2 t\right)$$

$$PFD_{AV} = F_{AV} = \frac{1}{T/3}\int_0^{T/3} F(t)\,dt$$

$$PFD_{AV} = \frac{1}{T/3}\int_0^{T/3} \lambda^3 \left(t^3 + 3\left(\frac{T}{3}\right)t^2 + 2\left(\frac{T}{3}\right)^2 t \right) dt$$

$$PFD_{AV} = \frac{\lambda^3}{T/3}\left[1.\frac{1}{4}t^4 + 3.\frac{1}{3}\left(\frac{T}{3}\right)t^3 + 2.\frac{1}{2}\left(\frac{T}{3}\right)^2 t^2\right]_0^{T/3}$$

$$PFD_{AV} = \frac{\lambda^3}{T/3}\left(1.\frac{1}{4}\left(\frac{T}{3}\right)^4 + 3.\frac{1}{3}\left(\frac{T}{3}\right)^4 + 2.\frac{1}{2}\left(\frac{T}{3}\right)^4\right)$$

$$PFD_{AV} = \frac{\lambda^3 T^3}{2^3}.\frac{2^3}{3^3}\left(1 \times \frac{1}{4} + 3 \times \frac{1}{3} + 2 \times \frac{1}{2}\right)$$

$$PFD_{AV} = \frac{\lambda^3 T^3}{2^3}\left(\frac{2^3}{3^3}.\frac{9}{4}\right)$$

$$PFD_{AV} = \left(\frac{2}{3}\right)\frac{\lambda^3 T^3}{2^3}$$

$$PFD_{AV} = \frac{2}{3}PFD_{1oo1}{}^3$$

8.3 1ooN simple redundancy

The general case is slightly complicated because the number pattern is difficult to generate.

$$F(t) = \lambda t\left(\lambda t + \frac{\lambda T}{N}\right)\left(\lambda t + \frac{2\lambda T}{N}\right)\left(\lambda t + \frac{3\lambda T}{N}\right)\ldots\ldots$$

$$F = \prod_{i=0}^{n}\left(\lambda t + \frac{i\lambda T}{N}\right)$$

To make the algebraic development a little easier to follow, make the following substitution.

$$F_1(t) = a$$

$$F_2(t) = a(a+b) = a^2 + ab$$

$$F_3(t) = a(a+b)(a+2b)$$
$$F_3(t) = (a^2 + ab)(a+2b)$$
$$F_3(t) = a^3 + a^2b$$
$$+2a^2b + 2ab^2$$
$$F_3(t) = a^3 + 3a^2b + 2ab^2$$

The coefficients for F_3 are 1, 3, 2.

$$F_4(t) = (a^3 + 3a^2b + 2ab^2)(a+3b)$$
$$F_4(t) = (a^4 + 3a^3b + 2a^2b^2)$$
$$+3a^3b + 9a^2b^2 + 6ab^3)$$
$$F_4(t) = (a^4 + 6a^3b + 11a^2b^2 + 6ab^3)$$

The coefficients for F_4 are 1, 6, 11, 6.

By using the expansion method above, the coefficients can be developed (although the number pattern is quite complex).

	1	2	3	4	5	6	7	8	9	10
1	1	0	0	0	0	0	0	0	0	0
2	1	1	0	0	0	0	0	0	0	0
3	1	3	2	0	0	0	0	0	0	0
4	1	6	11	6	0	0	0	0	0	0
5	1	10	35	50	24	0	0	0	0	0
6	1	15	85	225	274	120	0	0	0	0
7	1	21	175	735	1624	1764	720	0	0	0
8	1	28	322	1960	6769	13132	13068	5040	0	0
9	1	36	546	4536	22449	67284	118124	109584	40320	0
10	1	45	870	9450	63273	269325	723680	1172700	1026576	362880

For the general case of $1ooN$:

$$PFD_{AV} = \left(\frac{\lambda T}{2}\right)^N . \left(\frac{2}{N}\right)^N . \left(\frac{St_{N,1}}{N+1} + \frac{St_{N,2}}{N} + \frac{St_{N,3}}{N-1} + \frac{St_{N,4}}{N-2} + \cdots\right)$$

Therefore:

$$PFD_{AV} = {PFD_{1oo1}}^N . \left(\frac{2}{N}\right)^N . \left(\frac{St_{N,1}}{N+1} + \frac{St_{N,2}}{N} + \frac{St_{N,3}}{N-1} + \frac{St_{N,4}}{N-2} + \cdots\right)$$

$$PFD_{AV} = {PFD_{1oo1}}^N . \left(\frac{2}{N}\right)^N \sum_{i=1}^{N} \left(\frac{St_{N,i}}{N+2-i}\right)$$

Where $St_{N,i}$ is the coefficient given in row N and column i in the table above.

For example, for $N = 5$, the PFD_{AV} is found to be:

$$PFD_{AV} = \frac{\lambda^5 T^5}{2^5} \cdot \frac{2^5}{5^5}\left(1 \times \frac{1}{6} + 10 \times \frac{1}{5} + 35 \times \frac{1}{4} + 50 \times \frac{1}{3} + 24 \times \frac{1}{2}\right)$$

$$PFD_{AV} = \frac{\lambda^5 T^5}{2^5} \cdot \frac{2^5}{5^5}\left(39\frac{7}{12}\right)$$

$$PFD_{AV} = \frac{152}{375}\frac{\lambda^5 T^5}{2^5}$$

$$PFD_{AV} = \frac{152}{375} {PFD_{1oo1}}^5$$

9 Standard Configurations

Our common configurations are 1oo1 to fail (simplex), 2oo2 to fail (duplex) and 2oo3.

Both 1oo1 to fail and 2oo2 to fail are deal with above. That leaves the case for 2oo3 to solve explicitly.

9.1 1oo1 to fail

For 1oo1 to fail, the we would expect for both synchronised and staggered testing for the result to be identical – i.e. there is no difference.

$$PFD_{AV} = PFD_{1oo1} = \frac{\lambda T}{2}$$

Using the formula for staggered testing, we get:

$$PFD_{AV} = {PFD_{1oo1}}^N \cdot \left(\frac{2}{N}\right)^N \sum_{i=1}^{N} \left(\frac{St_{N,i}}{N + 2 - i}\right)$$

Where

$$N = 1$$

$$PFD_{AV} = PFD_{1oo1} \cdot 2 \sum_{i=1}^{1} \left(\frac{St_{1,i}}{1 + 2 - i}\right)$$

$$PFD_{AV} = PFD_{1oo1} \cdot 2 \cdot \frac{1}{2}$$

$$PFD_{AV} = PFD_{1oo1}$$

As we would expect.

9.2 2oo2 to fail

For 2oo2 to fail, we would expect a difference.

9.2.1 Synchronised Testing

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

Where $N = 2$

$$PFD_{2oo2} = \frac{2^2}{2+1} {PFD_{1oo1}}^2$$

$$PFD_{2oo2} = \frac{4}{3} {PFD_{1oo1}}^2$$

9.2.2 Staggered Testing

$$PFD_{AV} = {PFD_{1oo1}}^N . \left(\frac{2}{N}\right)^N \sum_{i=1}^{N} \left(\frac{St_{N,i}}{N+2-i}\right)$$

Where $N = 2$

$$PFD_{2oo2} = {PFD_{1oo1}}^2 . \left(\frac{2}{2}\right)^2 \sum_{i=1}^{2} \left(\frac{St_{2,i}}{4-i}\right)$$

$$PFD_{2oo2} = {PFD_{1oo1}}^2 . \left(\frac{1}{3} + \frac{1}{2}\right)$$

$$PFD_{2oo2} = \frac{5}{6} {PFD_{1oo1}}^2$$

As above.

9.3 2oo3 to fail

2oo3 is an example of a voted system which is not covered by the above general $1ooN$ formula.

9.3.1 Synchronised Testing

In a 2oo3 configuration, if 2 of the 3 fail then the system fails. There are 3 possible combinations that will give a pair of failures, where each pair has the same probability of failure. The probability of failure of a pair is the same as for the 2oo2 to fail configuration.

Therefore:

$$PFD_{2oo3} = 3\frac{2^N}{N+1}PFD_{1oo1}{}^N$$

Where

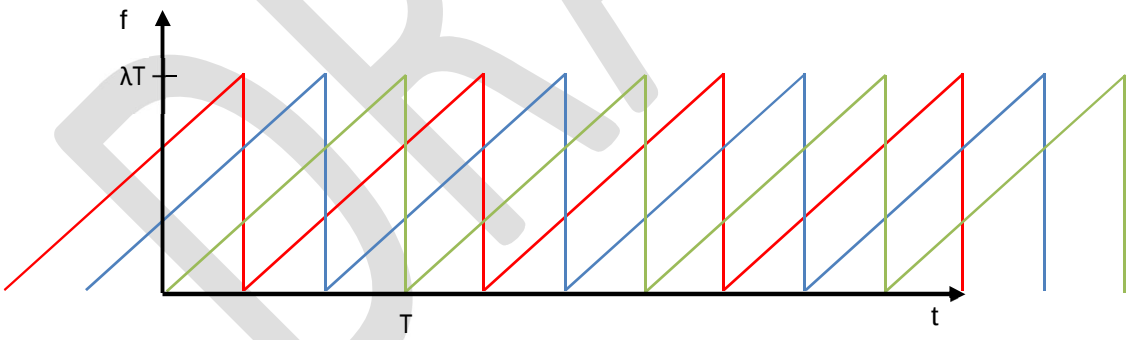
$$N = 2$$

$$PFD_{2oo3} = 3\frac{2^2}{2+1}PFD_{1oo1}{}^2$$

$$PFD_{2oo3} = 4PFD_{1oo1}{}^2$$

9.3.2 **Staggered Testing**

If we assume that we have 3 components (A, B and C), the system fails if A and B fail, B and C fail or A and C fail. We therefore need to look at the probability of each pair failing.



If we look at any pair in the above, we see they are not evenly distributed in time. But the period between them is always T/3. So, whichever pair we are considering will always have the same PFD_{AV}.

Let's take the green and red as a pairing in look at the average over the period T.

$$F(t) = \lambda t.\left(\lambda t + \frac{2\lambda T}{3}\right) for\ [t{:}\,0, \frac{T}{3}]$$

$$F(t) = \lambda t.\left(\lambda t - \frac{\lambda T}{3}\right) for\ [t{:}\,\frac{T}{3}, T]$$

This leads to:

$$PFD_{2oo3} = \frac{2}{3}\lambda^2 T^2$$

$$PFD_{2oo3} = \frac{8}{3} PFD_{1oo1}{}^2$$

Refer to the *Staggered Proof Testing* document for derivation.

9.4 Summary

For general NooM configurations, the effect of staggered proof testing is more challenging.

The reason for this is that it is dependent on where the selection comes in the testing cycle.

For higher values of M and N, the complexity increases considerably and. for that reason, this topic is dealt with separately in *Staggered Proof Testing*.

In instrumented functional safety systems, staggered proof testing would be very unusual because it would be inefficient. However, for larger systems or machines (e.g. standby generators) it would be the more common approach.

Clearly staggering proof testing makes a considerable improvement to the system reliability over synchronised.

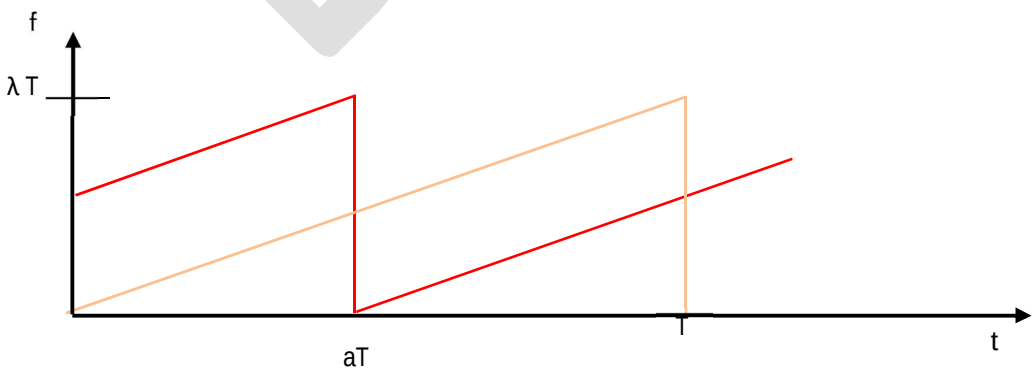
10 Staggered Proof Testing in Complex Redundancy

The latter cases of the standard configurations shown in the previous section are complex redundancy although they are relatively trivial examples.

In this section, we are going to try to generate a way of looking at the general case of MooN failures.

10.1 Failure of 2 Items

Consider the following graph



In the above diagram, there are two items with staggered proof test intervals shown by the 2 colours.

The green function is given by

$F(t)_{green} = \lambda t$ [0,T]

$F(t)_{red} = \lambda t + (1-a)\lambda T$ [0,aT]

$F(t)_{red} = \lambda t + (-a)\lambda T$ [aT,T]

The joint probability of failure is given by

$F(t) = \lambda t(\lambda t + (1-a)\lambda T) = \lambda^2(t^2 + (1-a)Tt)$ [0,aT]

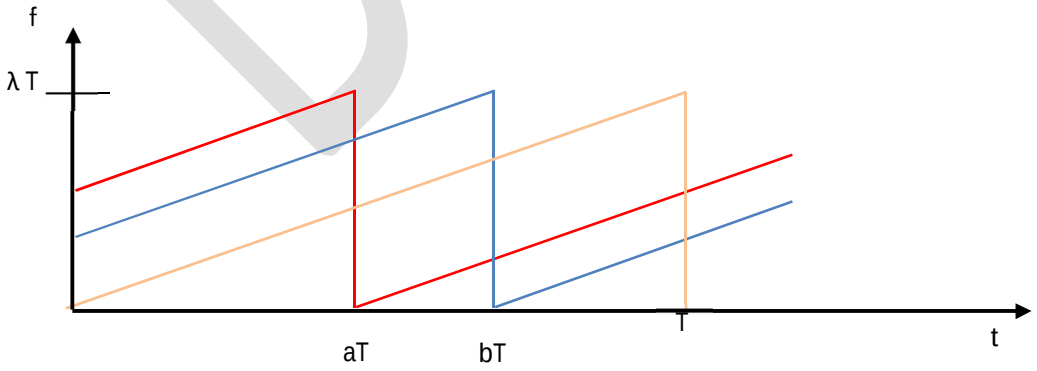
$F(t) = \lambda t(\lambda t + (-a)\lambda T) = \lambda^2(t^2 + (-a)Tt)$ [aT,T]

$$PFD_{AV} = \frac{\lambda^2}{T}\left(\int_0^{aT} t^2 + (1-a)T.t\,dt + \int_{aT}^{T} t^2 + (-a)T.t\,dt\right)$$

$$PFD_{AV} = \frac{\lambda^2}{T}\left(\left[\frac{t^3}{3}\right]_0^{aT} + (1-a)T\left[\frac{t^2}{2}\right]_0^{aT} + \left[\frac{t^3}{3}\right]_{aT}^{T} + (-a)T\left[\frac{t^2}{2}\right]_{aT}^{T}\right)$$

10.2 Failure of 3 Items

Consider the following graph



In the above diagram, there are three items with staggered proof test intervals shown by the 3 colours.

The green function is given by

$F(t)_{green} = \lambda t$ [0,T]

$F(t)_{red} = \lambda t + (1-a)\lambda T$ 0,aT]

$F(t)_{red} = \lambda t + (-a)\lambda T$ [aT,T]

$F(t)_{blue} = \lambda t + (1-b)\lambda T$ [0,bT]

$F(t)_{blue} = \lambda t + (-b)\lambda T$ [bT,T]

Note: $b > a$

The joint probability of failure is given by

$F(t) = \lambda t(\lambda t + (1-a)\lambda T)(\lambda t + (1-b)\lambda T)$ [0,aT]

$F(t) = \lambda t(\lambda t + (-a)\lambda T)(\lambda t + (1-b)\lambda T)$ [aT,bT]

$F(t) = \lambda t(\lambda t + (-a)\lambda T)(\lambda t + (-b)\lambda T)$ [bT,T]

$F(t) = \lambda^3(t^3 + ((1-a) + (1-b))T.t^2 + ((1-a)(1-b))T^2.t)$ [0,aT]

$F(t) = \lambda^3(t^3 + ((-a) + (1-b))T.t^2 + ((-a)(1-b))T^2.t)$ [aT,bT]

$F(t) = \lambda^3(t^3 + ((-a) + (-b))T.t^2 + ((-a)(-b))T^2.t)$ [bT,T]

$$PFD_{AV} = \frac{\lambda^3}{T}\left(\int_0^{aT} t^3 + ((1-a) + (1-b))T.t^2 + \big((1-a)(1-b)\big)T^2.t\,dt\right)$$
$$+\frac{\lambda^3}{T}\left(\int_{aT}^{bT} t^3 + ((-a) + (1-b)).t^2 + \big((-a)(1-b)\big)T^2.t\,dt\right)$$
$$+\frac{\lambda^3}{T}\left(\int_{bT}^{T} t^3 + ((-a) + (-b))T.t^2 + \big((-a)(-b)\big)T^2.t\,dt\right)$$

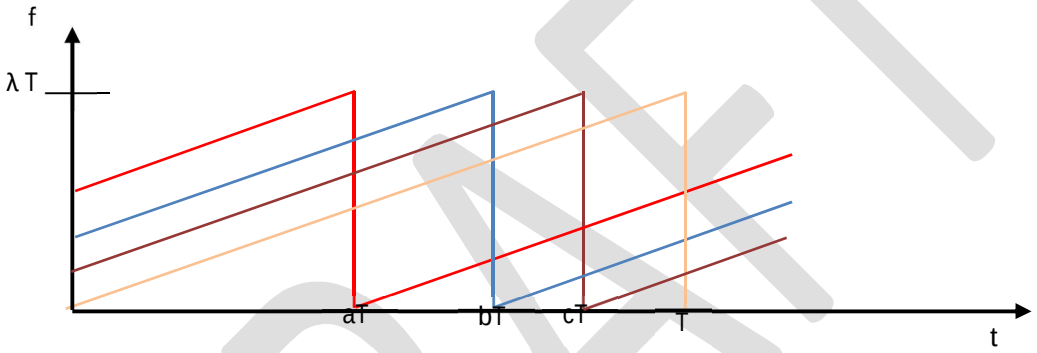
$$PFD_{AV} = \frac{\lambda^3}{T}\left[\frac{t^3}{4} + ((1-a) + (1-b))T.\frac{t^3}{3} + \big((1-a)(1-b)\big)T^2.\frac{t^2}{2}\right]_0^{aT}$$

$$+\frac{\lambda^3}{T}\left[\frac{t^3}{4} + ((-a) + (1-b))T.\frac{t^3}{3} + \big((-a)(1-b)\big)T^2.\frac{t^2}{2}\right]_0^{aT}$$

$$+\frac{\lambda^3}{T}\left[\frac{t^3}{4} + ((-a) + (-b))T.\frac{t^3}{3} + \big((-a)(-b)\big)T^2.\frac{t^2}{2}\right]_{aT}^{bT}$$

10.3 Failure of 4 Items

Consider the following graph



The joint probability of failure is given by

$F(t) = \lambda t(\lambda t + (1-a)\lambda T)(\lambda t + (1-b)\lambda T)(\lambda t + (1-c)\lambda T)$
[0,aT]

$F(t) = \lambda t(\lambda t + (-a)\lambda T)(\lambda t + (1-b)\lambda T)(\lambda t + (1-c)\lambda T)$
[aT,bT]

$F(t) = \lambda t(\lambda t + (-a)\lambda T)(\lambda t + (-b)\lambda T)(\lambda t + (1-c)\lambda T)$
[bT,cT]

$F(t) = \lambda t(\lambda t + (-a)\lambda T)(\lambda t + (-b)\lambda T)(\lambda t + (-c)\lambda T)$
[cT,T]

We can write this as: $F(t) = x(x+A)(x+B)(x+C)$

Where

$x = \lambda t;$

$A = (1-a)\lambda T\ [t < aT]$
$A = (-a)\lambda T\ [t \geq aT]$
B= $(1-b)\lambda T\ [t < bT]$

B= $(-b)\lambda T$ $[t \geq bT]$
$C = (1-c)\lambda T$ $[t < cT]$
$C = (-c)\lambda T$ $[t \geq cT]$

Expanding the expression for F(t)

$$F(t) = (x^2 + Ax)(x + B)(x + C)$$
$$F(t) = (x^3 + (A + B)x^2)(x + C)$$

$$F(t) = x^4 + (A + B + C)x^3 + (AB + AC + BC)x^2 + ABCx$$

Note: The coefficients for powers of x (other than the first) are:

- the sum of all the solos, then
- the sum of all the pairs, then
- the sum of all the triples

This pattern is repeated for greater powers.

So, for 4 failures with staggered proof testing:

$$F(t) = \lambda^4 t^4 + (A + B + C)\lambda^3 t^3 + (AB + AC + BC)\lambda^2 t^2 + ABC\lambda t$$

$$F_{AV} = \frac{1}{T}\left[\lambda^4 \frac{t^5}{5} + (A + B + C)\lambda^3 \frac{t^4}{4} + (AB + AC + BC)\lambda^2 \frac{t^3}{3} + ABC\lambda \frac{t^2}{2}\right]_0^{aT}$$
$$+ \frac{1}{T}\left[\lambda^4 \frac{t^5}{5} + (A + B + C)\lambda^3 \frac{t^4}{4} + (AB + AC + BC)\lambda^2 \frac{t^3}{3} + ABC\lambda \frac{t^2}{2}\right]_{aT}^{bT}$$
$$+ \frac{1}{T}\left[\lambda^4 \frac{t^5}{5} + (A + B + C)\lambda^3 \frac{t^4}{4} + (AB + AC + BC)\lambda^2 \frac{t^3}{3} + ABC\lambda \frac{t^2}{2}\right]_{bT}^{cT}$$
$$+ \frac{1}{T}\left[\lambda^4 \frac{t^5}{5} + (A + B + C)\lambda^3 \frac{t^4}{4} + (AB + AC + BC)\lambda^2 \frac{t^3}{3} + ABC\lambda \frac{t^2}{2}\right]_{cT}^{T}$$

Where

$A = (1-a)\lambda T$ $[t < aT]$
$A = (-a)\lambda T$ $[t \geq aT]$
B= $(1-b)\lambda T$ $[t < bT]$
B= $(-b)\lambda T$ $[t \geq bT]$

$C = (1 - c)\lambda T \quad [t < cT]$
$C = (-c)\lambda T \quad [t \geq cT]$

We simplify this whole expression by replacing as follows:

$A' = A/\lambda T$

$B' = B/\lambda T$

$C' = C/\lambda T$

Then, for 4 failures with staggered proof testing:

$$F(t) = \lambda^4 t^4 + (A + B + C)\lambda^3 t^3 + (AB + AC + BC)\lambda^2 t^2 + ABC\lambda t$$

$$F_{AV} = \lambda^4 T^4 \left[\frac{x^5}{5} + (A' + B' + C')\frac{x^4}{4} + (A'B' + A'C + B'C')\frac{x^3}{3} + A'B'C'\frac{x^2}{2}\right]_0^a$$
$$+\lambda^4 T^4 \left[\frac{x^5}{5} + (A' + B' + C')\frac{x^4}{4} + (A'B' + A'C + B'C')\frac{x^3}{3} + A'B'C'\frac{x^2}{2}\right]_a^b$$
$$+\lambda^4 T^4 \left[\frac{x^5}{5} + (A' + B' + C')\frac{x^4}{4} + (A'B' + A'C + B'C')\frac{x^3}{3} + A'B'C'\frac{x^2}{2}\right]_b^c$$
$$+\lambda^4 T^4 \left[\frac{x^5}{5} + (A' + B' + C')\frac{x^4}{4} + (A'B' + A'C + B'C')\frac{x^3}{3} + A'B'C'\frac{x^2}{2}\right]_c^1$$

Where

$A' = (1 - a)\ [x < a]$
$A' = (-a)\ [x \geq a]$
$B' = (1 - b)\ [x < b]$
$B' = (-b)\ [x \geq b]$
$C' = (1 - c)\ [x < c]$
$C' = (-c)\ [x \geq c]$

Using this algorithm, we can calculate the F_{AV} for 4oo4 failures for any similar items with staggered proof tests.

10.4 Failure of N Items

It is possible to expand and find the general case from the above.

$$F_{AV} = \left(\frac{\lambda T}{2}\right)^N 2^N \left[\frac{x^{N+1}}{N+1} + (Sum\ of\ solos)\frac{x^N}{N} + (Sum\ of\ pairs)\frac{x^{N-1}}{N-1} + (Sum\ of\ triples)\ \frac{x^{N-2}}{N-2} + \ldots.\right]_0^a$$

$$+ \left(\frac{\lambda T}{2}\right)^N 2^N \left[\frac{x^{N+1}}{N+1} + (Sum\ of\ solos)\frac{x^N}{N} + (Sum\ of\ pairs)\frac{x^{N-1}}{N-1} + (Sum\ of\ triples)\ \frac{x^{N-2}}{N-2} + \ldots.\right]_a^b$$

$$+ \cdots$$

$$+ \left(\frac{\lambda T}{2}\right)^N 2^N \left[\frac{x^{N+1}}{N+1} + (Sum\ of\ solos)\frac{x^N}{N} + (Sum\ of\ pairs)\frac{x^{N-1}}{N-1} + (Sum\ of\ triples)\ \frac{x^{N-2}}{N-2} + \ldots.\right]_{..}^1$$

Where

$A' = (1 - a)\ [x < a]$
$A' = (-a)\ [x \geq a]$
$B' = (1 - b)\ [x < b]$
$B' = (-b)\ [x \geq b]$
$C' = (1 - c)\ [x < c]$
$C' = (-c)\ [x \geq c]$
etc. $a < b < c < d$ … ….

10.5 Calculating Coefficients

In order to make use of this theory, we are looking for a matrix of coefficients $St_{N,K}$, to cover all the cases of N undetected failures out of M, where the coefficient can be used in calculations as a modifier in order that we can calculate the required PFD for N channels combined from the Nth power of the PFD for a single channel.

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

Note: The sections above only cover the evaluation of F_{AV} (i.e. the average of the function) for a specific 'selection' of channels that are tested somewhere in the rotor.

We assume that A', B', C' etc represent a subset of N items out of M where the proof testing of the M items is evenly spaced in time.

It can be seen then that $a, b, c\ etc.$ are rational numbers < 1.

Another process is required where all the possible subsets of N out of M are used to generate the F_{AV}.

The summation of the F_{AV} values for each subset is found and then divided by the number of subsets giving an F_{AV} which is now the average for N out of M.

A separate document called *Staggered Proof Testing Coefficients* shows how the programs carry out the calculations.

$St_{M,N}$ values are given below (for $M \leq 10$) where M is the row and N 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

11 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).

12 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.

13 Existing and Emerging Standards

IEC 61508 Edition 2.
IEC 61511 Edition 2.

14 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.

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 ***