T6A041

"Reliability and Availability"

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	Minor corrections. Foreword expanded. 'Redundancy' section included (removed from Random Hardware Failures). Added wider context of reliability and references.
0.3	16/08/2023	R. Martin	Minor corrections to text. Foreword and Executive Summary updated.
1.0	26/01/2024	R. Martin	First issue.

3 Introduction / Foreword

This document covers the topic of reliability and availability 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 is the first in the series. It 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.

Because of the interests in functional safety, the theory is related to safety wherever possible. It should however be understood that reliability and availability are broader topics. So, although it is related to functional safety, 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 hypotheses. This series of documents is written with that in mind. Note: The standard itself uses a complex approach where 'mean channel downtime' is treated as critical and often causes confusion in what turn out to be 'self-cancelling' formulae. There is no reasoning offered for this approach and, in this respect, the authors feel the standard fails its own criteria. These documents use a more traditional approach.

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 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 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 throughout the useful life of a component. 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 an advantage 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 - 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 Chance Events

7.1 Probability of a Chance Event

Consider the following:
If 300 people in a population of 60,000,000 die per year of cause 'A' and there is equal chance of it happening to anyone and at any time, then we can say that the probability of an individual dying of cause A (F_A) in any one year is 300 in 60,000,000.

$$F_A = \frac{3 \times 10^2}{6 \times 10^7} = 5 \times 10^{-4}$$

This is a useful way of handling cause of death statistics when events are few and far between.

7.2 Failure Rate

Rather than consider the probability of failure over a specific period of time, we often use the failure rate which is an instantaneous value of expected failures. The number of failures accumulated over the period of a year and the instantaneous failure rate are not the same thing unless the population remained constant.

Using the failure rate can be expressed in any units of time. For instance, a failure rate of 5 x 10^{-4} per year has the same meaning as a failure rate (to 2sf) of 5.7 x 10^{-8} per hour.

However, in estimating the failure rate, the use of an appropriate period is important. If we measured the number of deaths hour by hour, we would get wildly differing results. It is important to understand that the units in which a failure rate is expressed do not imply anything about the period over which data is collected.

7.3 Individual versus Population

Although the above is true for a population, for any individual, the chances of dying in any one year of cause A must vary. From an individual's perspective, it has to be 'given that you are alive'. If you happened to have already died (of this cause or any other), your chances of dying in years following have to be zero.

To emphasise this point: looking at the probability of dying from any cause in one year, the probability for an individual would be approximately 0.02. But we know the sum of probabilities has to be 1. So what if the individual lives to 70? How can the probability of an individual dying be 70 x 0.02 = 1.4?.

The 'failure rate' is the key parameter in modelling failures. For an individual, the chances of dying in any one year of life would tend to decay because you have to take in to account the chance that you have survived to that point in time. If the 'failure rate' was constant, the resulting function would be an exponential decay. But the rate of failure corresponding to an exponential time function cannot be constant! This point emphasises an issue of terminology and where care is needed: this is discussed later.

7.4 The Bath Tub Curve

We have statistics for what ages people die at and we can see from this that (although there is an exponential decay which governs most of the time) there are increases in the early years and in the late years. This is the 'so called' bath tub curve where the failure rate is higher in the early years and the later years. Note: early failures are often referred to as 'infant mortalities' and late failures are often said to be 'old age' even when applied to mechanical failure.

If we are dealing with components and not people, they follow a similar pattern, the probability of failure density function is roughly exponential but has distortions at either end. In high reliability applications, to overcome the 'infant mortality' issues, an initial stress test is

commonly used. In electronics it is often a 'heat soak'; in pressure equipment the pressure may be taken to a point significantly above the maximum rated pressure.

At the other end of the spectrum, people 'die of old age' and in the same way so do components: the insulation on an electrical motor winding eventually breaks down; a stressed piece of metal eventually fatigues. In high reliability components it is important therefore to stipulate a 'design life' which is comfortably within the time period where 'old age' would start to distort the constant failure rate.
For components where early stress testing has taken place and a suitable design life has been stipulated the constant failure rate model with added conservatism is a good enough fit.

8 Failure Rate

8.1 Constant underlying failure rate

In general, if we have a population of items with equal probability of failure and we do not replace or repair them when they fail, we would expect the population to decay over time. In order to model the decay mathematically and ignoring any 'bath tub' effect, we would expect the failure rate to be constant (i.e. the rate of failures varies in time but remains proportional to the current population).

In fact, that is the definition of what we mean by constant failure rate: not that the number of failures per unit time remains constant but that the number of failures per unit time is proportional to the current population.

Studies have shown that, in a closed system, where a population of components operate, each until failure point without replacement, through time, the rate of failures remains proportional to the number of survivors.

It gives us a governing differential equation:

$$\frac{dn}{dt} = -\lambda n$$

where n is the population and f is the constant 'failure rate'.

Solving this equation:

$$\int \frac{dn}{n} = \int -\lambda dt$$

$$ln\, n = -\lambda t + c$$

where c is a constant $n = e^{(c-\lambda t)}$

If at time t=0, the population is N then

$$e^c = N$$

and therefore $n = Ne^{-\lambda t}$

For constant failure rates the population decays exponentially.

Note: The rate of decay of the population is also a 'failure rate' but that is not a constant in time. This highlights an unfortunate complication: the words 'failure rate' can have different meanings depending on context. Here we use λ to represent the constant of the underlying failure rate and, if required, f to represent the number of failures in time.

The probability of survival (R) of a single item at time t is given by the ratio n/N, i.e.

$$R = e^{-\lambda t}$$

The probability of survival of a single item decays exponentially for a constant failure rate.

The probability of failure is given by the complement:

$$F = 1 - e^{-\lambda t}$$

Note: by differentiating the probability of failure and substituting t = 0, we can see that the initial failure rate is λ.

The MacLaurin expansion tells us that:

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots.$$

Therefore:

$$e^{-\lambda t} = 1 - \lambda t + \frac{(\lambda t)^2}{2!} - \frac{(\lambda t)^3}{3!} + \ldots$$

and:

$$F = \lambda t - \frac{(\lambda t)^2}{2!} + \frac{(\lambda t)^3}{3!} - \ldots$$

If $\lambda t \ll 1$, the powers of λt can be ignored and the following approximation can be used.

$$F \approx \lambda t$$

In the following that assumption holds and often it is written as:

$$F = \lambda t$$

8.2 Non-constant underlying failure rate

Although we are following a model of constant underlying failure rate (λ) it is worth noting the more general case of the underlying failure rate $w(t)$.

Using the same governing equation but replacing $\lambda \; with \; w(t)$:

$$\frac{dn}{dt} = -w(t)n$$

$$\int \frac{dn}{n} = \int -w(t)dt$$

Assuming $n = N$ at time $t = 0$ and integrating over the interval T

$$\int_{N}^{n(T)} \frac{dn}{n} = \int_{0}^{T} -w(t)dt$$

$$[ln\, n]_{N}^{n(T)} = \int_{0}^{T} -w(t)dt$$

$$ln\left(\frac{n(T)}{N}\right) = \int_{0}^{T} -w(t)dt$$

$$R(T) = e^{-\int_{0}^{T} w(t)dt}$$

9 Components in Parallel

9.1 Probability of Failure

If there are several components in parallel with probabilities of failure $F_1, F_2, F_3\ etc$ respectively, where the system survives if one of more components survive, then the overall probability of failure is the product.
In general:

$$F_s = \prod_{i=1}^{n} F_i$$

9.2 Failure Rate

For a system of n channels, a system failure event occurs when a channel fails given that all the other channels have already failed.

Where f represents the failure rate of a channel, consider the case of 3 channels
The system failure rate is given by:

$$f_s = f_1.F_2.F_3 + f_2.F_1.F_3 + f_3.F_1.F_2.$$

For the general case:

$$f_S = \sum_{i=1}^{n} f_i \prod_{j=1}^{n} F_j \qquad (i \neq j)$$

10 Components in Series

10.1 Probability of Failure

If there are several components in series with probabilities of survival $R_1, R_2, R_3\ etc$ respectively, then the overall probability of survival is the product.
In general:

$$R_s = \prod_{i=1}^{n} R_i$$

Remembering that: $R_i = 1 - F_i$

Substituting to express the general case in terms of failure:

$$1 - F_s = \prod_{i=1}^{n} (1 - F_i)$$

Consider the case where $n = 3$ and expanding:

$$1 - F_s = (1 - F_1)(1 - F_2)(1 - F_3)$$

$$1 - F_s = (1 - F_1 - F_2 - F_3 + F_1 F_2 + F_1 F_3 + F_2 F_3 - F_1 F_2 F_3)$$

Again, where $F \ll 1$, we can discount the higher powers. Thus, for 3 components in series:

$$F_s = F_1 + F_2 + F_3$$

In general:

$$F_S = \sum_{i=1}^{n} F_i$$

Note: we have used the '=' where we should remember that this only holds true for very small values of F.

10.2 Failure Rate

Looking at the same scenario from a failure rate perspective: If there are 3 components in series with failure rates of f_1, f_2, and f_3 respectively; then the overall failure rate we would expect would be the sum of the three:

$$f_s = f_1 + f_2 + f_3$$

In general:

$$f_s = \sum_{i=1}^{n} f_i$$

11 Mean Time Between Failures

The Mean Time Between Failures (MTBF) is a useful concept especially when it comes to parts which are repaired or replaced. There are three sections below which examine the mathematical relationship between $R(t)$, λ and MTBF – starting with the more rigorous.

11.1 MTBF from Probability Density Function

The MTBF is the first moment in time (about time $t = 0$) of the probability of failure density function (f). The probability of failure density function (f) is the first derivative of the probability of failure function (F); and F is the complement of R.
i.e.

$$F(t) = 1 - R(t)$$

$$f(t) = \frac{dF(t)}{dt} = -\frac{dR(t)}{dt}$$

$MTBF$ is given by the first moment of $f(t)$ about $t = 0$, i.e.:

$$MTBF = \frac{\int_0^\infty tf(t)dt}{\int_0^\infty f(t)dt} = -\int_0^\infty t\frac{dR(t)}{dt}dt$$

Note that:

$$\int_0^\infty f(t)dt = 1$$

Integrate by parts (u,v) where $u = t$ and $dv = \frac{dR}{dt}$

$$MTBF = -\int_0^\infty t\frac{dR(t)}{dt}dt = -[tR(t)]_0^\infty + \int_0^\infty R(t)dt$$

The first term is 0 because evaluated at infinity in all practical cases, the inverse of R(t) approaches infinity much faster than t. Hence the average lifespan (MTBF) is given by:

$$MTBF = \int_0^\infty R(t)dt$$

Note: The equation above holds true where $R(t)$ is any function in time that represents the probability of survival.

Where the probability of survival follows the underlying constant failure rate λ,

$$R(t) = e^{-\lambda t}$$

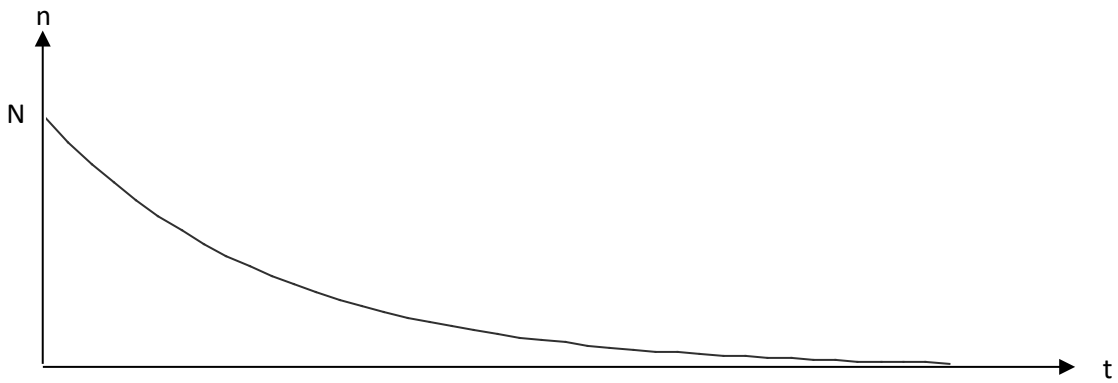
And therefore:

$$MTBF = \int_0^\infty R(t)dt = \int_0^\infty e^{-\lambda t}dt = \left[\frac{e^{-\lambda t}}{-\lambda}\right]_0^\infty = [0 - \frac{1}{-\lambda}] = \frac{1}{\lambda}$$

$$MTBF = \frac{1}{\lambda}$$

11.2 **MTBF from Probability Function**

For the definition of the $MTBF$, we can either look at the first moment about $t = 0$ of the probability of failure density function or we can go back to where the function $R(t)$ originally came from and consider a population.



At $t = 0$, the population is N and it decays at a rate governed by λ.

The resulting population $n(t)$ is given by:

$$n(t) = NR(t)$$

We can picture the area below the curve being made up of a series of N horizontal bars. Assuming that each bar represents the life time of an individual unit we can see the total life expectancy of all units to be the area under the curve. Dividing by N will then give the average life (or the MTBF).

$$MTBF = \frac{\int_0^\infty n(t)dt}{N} = \frac{\int_0^\infty NR(t)dt}{N} = \int_0^\infty R(t)dt$$

For the case of constant underlying failure rate λ, the remainder of the derivation is as in the section above.

11.3 **MTBF Intuitively**

If we had a component which had failure rate of λ and each time it failed, we replaced it with an identical component, we would expect over time that the failure rate was the reciprocal of the MTBF. Note: In this case we would be keeping the population constant at 1.

$$MTBF = \frac{1}{\lambda}$$

12 Redundant Components

Firstly, lets restate what we have for simplex components:

For a simplex component with constant failure rate λ, the general form is:

$$R(t) = e^{-\lambda t}$$

$$F = 1 - e^{-\lambda t}$$

$$MTBF = \frac{1}{\lambda}$$

When components are placed in parallel (meaning that all the components must fail for the system to fail), the probability of failure of the system is the probability that all the components fail. If these events are independent, the joint probability is given by the product of the individual probabilities.

$$F_s = \prod_{i=1}^{n} F_i$$

When the components have a constant underlying failure rate λ

$$F_s = \prod_{i=1}^{n} (1 - e^{-\lambda_i t})$$

Suppose we have a system of two identical redundant components whose probabilities of failure remain independent.

$$F_s = (1 - e^{-\lambda_i t})^2$$

Expanding:

$$F_s = 1 - 2e^{-\lambda_i t} + e^{-2\lambda_i t}$$

The failure rate in time f is the first derivative of the probability of failure.
Note that the **initial failure rate is 0!**

This may lead us to believe that putting two components in parallel is a perfect solution even on a system with no repair or replacement but we would need to be careful about in which circumstance the use is justified. To understand this, we look at the $MTBF$.

$$MTBF = \int_0^\infty R(t)dt = \int_0^\infty 2e^{-\lambda t} - e^{-2\lambda t}dt$$

$$MTBF = \left[\frac{2e^{-\lambda t}}{-\lambda}\right]_0^\infty - \left[\frac{e^{-2\lambda t}}{-2\lambda}\right]_0^\infty = \left[0 - \frac{2}{\lambda}\right] - \left[0 - \frac{1}{2\lambda}\right]$$

$$MTBF = \frac{3}{2\lambda}$$

This represents only a 50% increase in the $MTBF$ over a single component!
The practical benefits of components in parallel do however exist if:

- the components have an $MTBF$ that is several times the life expectancy of the system as a whole, or;
- the components are replaced at intervals $\ll MTBF$, or;
- the components are tested at intervals $\ll MTBF$.

Notes:

- The last of the options above usually turns out to be most cost effective.
- In the case of $MTBF$ being much greater than life expectancy of the system as a whole, $MTBF$ is not a meaningful measure.

13 Availability

If we assume that when our item fails, it can be replaced or repaired then the concept of availability arises. The availability is simply the average probability in time that a repairable system is functioning.

We usually assume an average time taken to restore it to working. This is referred to as Mean Time to Restore ($MTTR$). But, importantly, this time is taken from the time the failure is known to have happened (and that differs with types of failure).

The Availability (A) can be defined simply as follows:

$$A = \frac{Total\ Time - \ Time\ spent\ in\ failed\ state}{Total\ time}$$

Where $Total\ Time$ is suitably long to cover many failures.

13.1 **Revealed Failure**

We have:

$$A = \frac{Total\ Time - \ Time\ spent\ in\ failed\ state}{Total\ time}$$

If an item has been operating for N times the period of its $MTBF$ then we would expect it to have failed and been repaired or replaced N times.

Because this failure is *revealed* it means that we know about the failure as soon as it happens. The time it is unavailable after each failure is therefore taken as $MTTR$.

Over an extended period of time ($N \times MTBF$) we expect N failures to have occurred and N repairs to have occurred.

Over the same period, we expect the time spent in a failed state to be $N \times MTTR$.
The Total Time would be given by:

$$Total\ Time = N \times MTBF + \ N \times MTTR$$

The Availability of the system is the proportion of time it is in operation.

$$A = \frac{N \times MTBF + \ N \times MTTR - \ N \times MTTR}{N \times MTBF + \ N \times MTTR}$$

$$A = \frac{MTBF}{MTBF + MTTR}$$

13.2 **Unrevealed Failure**

We have:

$$A = \frac{Total\ Time - \ Time\ spent\ in\ failed\ state}{Total\ time}$$

or

$$A = \frac{Time\ spent\ in\ working\ state}{Time\ spent\ in\ working\ state + Time\ spent\ in\ failed\ state}$$

If an item has been operating for N times the period of its $MTBF$ then we would expect it to have failed and been repaired or replaced N times.

Over an extended period of operations approximately $N \times MTBF$ we expect N failures to have occurred and N repairs to have occurred.

Because this failure is *unrevealed* it means that we don't know about the failure when it happens. We can only find it to be in a failed state when we test it. Over this extended period where N failures have occurred, we can assume that on average, it has been failed for half the test interval T .

The average time it is unavailable after each failure is therefore taken as $MTTR + T/2$.

The Total Time would be given by:

$$Time\ spent\ in\ working\ state = N \times MTBF$$

and:

$$Time\ spent\ in\ failed\ state = \ N \times MTTR + N \times T/2$$

$$A = \frac{N \times MTBF}{N \times MTBF + \ N \times MTTR + N \times T/2}$$

$$A = \frac{MTBF}{MTBF + \ MTTR + T/2}$$

13.3 **Components in Series**

If we have a number of components or subsystems in series, then the probability that the system is available is the joint probability that all the subsystems are available.

Assuming the failure of the subsystems to be independent then the joint probability is the product of all the individual availabilities.

i.e.

$$A_s = \prod_{i=1}^{n} A_i$$

13.4 **Components in Parallel**

If we have a number of components or subsystems in parallel, then the probability that the system is available is the probability that any of the subsystems is available.

The easiest way to think of this is in terms of unavailability – i.e. the probability of the system being unavailable is the joint probability of all the subsystems being unavailable.

Assuming failure of the subsystems to be independent this can be written as:

$$1 - A_s = \prod_{i=1}^{n} (1 - A_i)$$

Rearranging:

$$A_s = 1 - \prod_{i=1}^{n} (1 - A_i)$$

14 Types of Failure

In the section above, we distinguished between *revealed* and *unrevealed* failures. These are sometimes also referred to in texts as *diagnosed* and *undiagnosed* failures or *detected* and *undetected* failures.

In particular, when it comes to *safety related systems* as dealt with by the international standard *IEC 61511*, the terms used are *diagnosed* and *undiagnosed*.

In *safety related systems*, safety functions are either *protective functions* or *control functions*. Where they are *protective functions* the concept of *probability of failure on demand* arises where that term refers to the probability that a protective function is in a failed state and cannot perform its safety function.

Note: We have seen in preceding sections that the probability of failure F, is variable in time. This is true whether even if parts are repaired or replaced when found to be faulty. Importantly, in *safety related* systems, the measure used is *average probability of failure on demand* where that represents a time average.

The terminology in *safety related systems* also distinguishes between *safe* failures and *dangerous* failures. With a safety function, we are primarily interested in *dangerous failures* (where a safety function becomes incapable of performing its safety duty). But safe failures are

also referred to because these would often result in an item of plant tripping and potential commercial loss.

By convention, *safety related systems* terminology also distinguishes between a *fault* and a *failure*: a *fault* is something that may only degrade the reliability of a function but not necessarily cause its *failure* whereas a failure is defined as the inability to perform its safety duty.

Where a *safety function* contains redundancy, it is said to be *fault tolerant*.

In order to avoid as much confusion as possible, these documents adopt the above *safety related systems* terminology.

15 Probability of Failure on Demand

The key currency in *IEC 61511* is the average probability of failure on demand when referring to a protective function of low demand rate (e.g. a shutdown system).

The average probability of failure on demand is written as PFD_{AV}. We should realise that there is no difference between *Probability of Failure on Demand* and *Probability of Failure*. The words '*on demand*' are superfluous. In the early sections in this document, we use $F(t)$ to represent the probability of failure as a function of time. If we wished to represent the average, we could equally use the term F_{AV}.

When we use the term PFD_{AV} , we usually drop the $_{AV}$ and just refer to PFD.

The PFD_{AV} of a safety function is therefore the complement of its availability.

$$PFD = 1 - A$$

15.1 Diagnosed Failures

We have:

$$A = \frac{MTBF}{MTBF + MTTR}$$

Therefore:

$$PFD = 1 - \frac{MTBF}{MTBF + MTTR}$$

$$PFD = \frac{MTBF + MTTR - MTBF}{MTBF + MTTR}$$

$$PFD = \frac{MTTR}{MTBF + MTTR}$$

And if:

$$MTBF \gg MTTR$$

$$PFD \approx \frac{MTTR}{MTBF}$$

$$PFD \approx \lambda.MTTR$$

This is a universal approximation and is often written as:

$$PFD = \lambda.MTTR$$

15.2 **Undiagnosed Failures**

We have:

$$A = \frac{MTBF}{MTBF + MTTR + T/2}$$

Therefore:

$$PFD = 1 - \frac{MTBF}{MTBF + MTTR + T/2}$$

$$PFD = \frac{MTBF + MTTR + T/2 - MTBF}{MTBF + MTTR + T/2}$$

$$PFD = \frac{MTTR + T/2}{MTBF + MTTR + T/2}$$

In all practical cases $MTBF \gg MTTR$ and $MTBF \gg T$
So

$$PFD \approx \frac{MTTR + T/2}{MTBF}$$

$MTBF = 1/\lambda$

$$PFD \approx \lambda(MTTR + T/2)$$

This is a universal approximation and is often seen written as:

$$PFD = \lambda(MTTR + T/2)$$

In most practical cases $T \gg MTTR$ so this is often (although not universally) shortened to:

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

The argument against this approximation is that items in general have both undiagnosed and diagnosed failure. If account is to be taken of the $\lambda.MTTR$ (unavailability) component for diagnosed failures then it feels wrong not to take it into account for undiagnosed failures.

16 Redundancy

In section 9, we looked at what is often called *Simple Redundancy* – i.e. where there are n components in parallel and all the components have to fail for the system to fail. In many practical cases that is over simplistic.

The following binomial expansion is an important concept – it is aimed at *identical redundant components* where a certain number are needed for system survival.

Theoretically, if we have a system with M redundant identical elements, and we need N out of M to have a working system, we should be able to model the likelihood of NooM surviving using the binomial expansion.

We know that probability of failure (F) and probability of survival (R) sum to 1. i.e.:

$$(F + R) = 1$$

If this is true then (where M is any positive integer), the following is also true:

$$(F + R)^M = 1$$

But the use comes when we expand this binomially. We get:

$$1 = F^M + \frac{MF^{M-1}R}{1!} + \frac{M(M-1)F^{M-2}R^2}{2!} + \ldots$$

For example, where M = 4:

$$1 = F^4 + \frac{4F^3R}{1!} + \frac{12F^2R^2}{2!} + \ldots$$

i.e. $$1 = F^4 + 4F^3R + 6F^2R^2 + 4FR^3 + R^4$$

In doing this expansion, we have worked out all the combinations of failure and survival.

For instance, the second term is for 3 failures and 1 survival: with a population of 4, we can see there are 4 different combinations that can give you 1 survivor and hence the coefficient is 4.

If the system needs 2 out of 4 to survive (2oo4) then the probability that the system fails is given by the first two terms.

$$F_s = F^4 + 4F^3R$$

Expanding in this way always groups the system failures to the left and survivors to the right. But because the probability of failure and survival is always 1, we only need to calculate one side. In *safety related systems*, we focus primarily on probability of failure.

The above is always true where F and R are functions in time. With unrepairable systems the probability of survival always reduces over time.

If the system is unrepairable, the above can be expressed as a function of time by remembering that:

$$R = e^{-\lambda t}$$

And

$$F = 1 - R$$

In practical cases, we find ourselves interested in repairable systems and the *average in time*.

16.1 **Simple Redundancy**

If we assume that we are operating with equipment that is in the mid range of its life (i.e. beyond infant mortality and prior to old age) which also has a constant underlying failure rate, the reliability of a single unit is given by $R(t)$ where:

$$R(t) = e^{-\lambda t}$$

If λt is small then a first approximation of this is given by:

$$R(t) \cong 1 - \lambda t$$

and the probability of failure $F(t)$ is given by:

$$F(t) = 1 - R(t) \cong \lambda t$$

Because we are only interested in values of λt that are small, in the following we drop the approximation.

In order to derive the average probability of failure of a system, where the failures of its components are not truly independent in time, we must study them as a joint function in time before averaging.

We now look at several simple redundancy cases (where all items have to fail for the system to fail). We represent device survival as $R(t)$ and device failure as $F(t)$, with system survival as $R_S(t)$, and failure as $F_S(t)$.

16.1.1 **1oo1 (simplex)**

The definition of a 1oo1 system is that there is one unit and one unit is required to survive for the system to survive.

$$F_S(t) = F(t) = \lambda t$$

16.1.2 **1oo2 (duplex)**

The definition of a 1oo2 system is that there are two units but only 1 unit has to survive for the system to survive. In other words, for the system to fail, both units must fail.

If we now consider two identical units in parallel. We can see the elements that constitute failure by the expanding as follows:

$$(R + F)^2 = R^2 + 2RF + F^2$$

The system failure is given by the last term only.

$$F_S(t) = (F(t))^2 = (\lambda t)^2 = \lambda^2 t^2$$

16.1.3 **1oo3 (simple redundancy)**

The definition of a 1oo3 system is that there are three units but only 1 unit has to survive for the system to survive. In other words, for the system to fail, three units must fail.

If we now consider three identical units in parallel, we can see the elements that constitute failure by the expanding as follows:

$$(R + F)^3 = R^3 + 3R^2F + 3RF^2 + F^3$$

The system failure is given by the last term only.

$$F_S(t) = (F(t))^3 = (\lambda t)^3 = \lambda^3 t^3$$

16.2 **Complex Redundancy**

For example, where $N = 4$, we get:

$$1 = F^4 + \frac{4F^3R}{1!} + \frac{12F^2R^2}{2!} + \ldots$$

i.e. $$1 = F^4 + 4F^3R + 6F^2R^2 + 4FR^3 + R^4$$

In this expansion, we have revealed all the combinations of failure and survival.

For instance, the second term is for 3 failures and 1 survival: with a population of 4, we can see there are 4 different combinations that can give you 1 survivor and hence the coefficient is 4.

If the system needs 2 out of 4 to survive (2oo4) then the probability that the system fails is given by the first two terms.

$$F_s = F^4 + 4F^3R$$

An example of complex redundancy would be the case of a power supply system where there may be a total of 5 parallel power supplies of which at least 3 are required to meet the demands of the system.

The following expansion aids our thinking.

$$(R+F)^5 = R^5 + 5R^4F + 10R^3F^2 + 10R^2F^3 + 5RF^4 + F^5$$

The system fails for any of the terms with less than 3 survivors (which we can see is the last 3 terms).
Where F <<< 1 the probability of survival is very close to 1 and is therefore often ignored. We can also see that three right hand terms would in that case be dominated by the F^3 term. Hence, for this case, the probability of failure is given by:

$$F_s \cong C_3^5 . F^3$$

Note: Whether $F^i = (F)^i$ or whether the relationship is more complex, the above expansion gives the 'cases' for survival and failure which still holds true where $F^i \neq (F)^i$. The strength of this system is it finds all the outcomes.

16.3 **Conditional Probability**

Conditional Probability is really a way of looking at a probability within a probability – i.e. a device has failed but there are different failure modes which have different effects.

This is a particularly important concept when it comes to failure of safety related systems when we are considering modes of failure (and in particular, dangerous modes of failure).

Consider a de-energise to trip 2oo3 voting system that has 3 input 'channels' and voting module. In this case, the voting module has a reliability that is infinitely higher than the inputs and so failures of the voting module can be ignored.

If we set out the survive / fail expansion for 3 units, we get:

$$(R+F)^3 = R^3 + 3R^2F + 3RF^2 + F^3$$

We see that the first two terms represent the survive case and the second two represent the fail case. Failures are:

$$3RF^2 + F^3$$

In our voting trip system, however, the failure of the system as a whole depends on the state of the failed unit. A failed unit can either fail to 0 (i.e. it votes for a trip – toward safe) or it could fail to 1 (it votes against a trip – towards danger).

In the case of a single failure, the state of the failure doesn't matter because the other two inputs have the vote. In the case of two failures where both inputs fail to the 1 state then the 3rd functioning input is prevented from controlling the output: this also happens if both inputs fail to a 0 state. If two inputs fail in opposite state, the surviving input has the casting vote and therefore the system survives.

So, if we wish to model **all the outcomes** we need to expand the failure terms by making the following replacement:

$$F^2 = (F_0 + F_1)^2 = {F_0}^2 + 2F_0F_1 + {F_1}^2$$

$$F^3 = (F_0 + F_1)^3 = {F_0}^3 + 3{F_0}^2F_1 + 3F_0{F_1}^2 + {F_1}^3$$

We get:

$$(R + F)^3 = R^3 + 3R^2F + 3R\left({F_0}^2 + 2F_0F_1 + {F_1}^2\right) + {F_0}^3 + 3{F_0}^2F_1 + 3F_0{F_1}^2 + {F_1}^3$$

Dangerous failure is represented by the terms with more than 1 channel failed dangerously – i.e. any powers of F_1. Dangerous failures are:

$$3R{F_1}^2 + 3F_0{F_1}^2 + {F_1}^3$$

We can see that dangerous failures are a subset of the above failures.

Note: this expansion also demonstrates that with two channels failed in different modes (the subset $6RF_0F_1$) the system continues to perform its desired function – and by definition that is not a system failure.

We could also use the above expansion technique to look for spurious sets of failures – i.e. where failures in the system cause a trip. In safety related systems these are referred to as *safe failures* and these occur for any powers of F_0. Safe failures are:

$$3R{F_0}^2 + {F_0}^3 + 3{F_0}^2F_1$$

Note: Although the middle term exists, it is very unlikely to be the cause of a trip because a trip would have occurred before hand.

16.4 **Repairable Systems**

For a repairable system, we need to think in terms of the availability or probability of failure on demand.

Note: What follows is theory. In practice, we cannot claim that the failure of one unit is independent of another because of common causes and we cannot claim that reinstatement of one unit is independent of another unless we have unlimited repair resources. However, this serves as a useful approximation.

If undetected faults are being considered then testing must be taken into account.

Assume that we have a proof test (a test that proves an item performs its function) and that test occurs at the *proof test interval* of T.

For undetected failures, we have Probability of Failure on Demand (PFD) given by:

$$PFD = \frac{\lambda T}{2} + \lambda . MTTR$$

For detected failures, we have PFD given by:

$$PFD = \lambda . MTTR$$

In the following, we use the suffices *D* and *U* for detected and undetected.

Note: for fault tolerant systems with **detected** faults, the PFD of the system is the product of the PFD of the components. For instance, for a 2oo2 to fail system:

$$PFD_D = \lambda^2 . MTTR^2$$

Note: for fault tolerant systems with **undetected** faults with independent testing, the PFD is given by the product of the components. Assuming $MTTR \ll T$, for a 2oo2 to fail system:

$$PFD_U = \frac{\lambda^2 . T^2}{4}$$

For a component which has both detected and undetected failures:

$$PFD = PFD_D + PFD_U$$

Thus, for a 2oo2 to fail system which has a mixture of detected and undetected faults and synchronous testing, we would expect:

$$PFD = (PFD_D + PFD_U)^2$$

$$PFD = {PFD_D}^2 + {PFD_U}^2 + 2PFD_D . PFD_U$$

i.e. $$PFD = {\lambda_d}^2 . MTTR^2 + \frac{{\lambda_u}^2 . T^2}{4} + \lambda_d . MTTR . \lambda_u . T$$

Note: In this formula, no account is yet taken of the distorting effects of proof test regime or of common cause failure. In the following, there is a development of the relationship between single component reliability and the reliability of components in complex redundancy. Although the 'distorting' effects need to be grafted on (see *Effects of Proof Testing*), these relationships underly.

16.4.1 **1oo2 (2oo2 to fail) repairable system**

For a system of units A and B, the probability of failure on demand (PFD) of the system is given by the product of the PFDs of the individual units (i.e. all possible combinations of 2 from 2).

The failure rate of the system is found by looking at all the possibilities and then looking at the associated probabilities of failure on demand of the path other than the final element to fail. Note: The final element's failure rate acts as a multiple to give the contribution to the overall system failure rate.

There are two possible paths to failure before the final element, either A fails or B fails (i.e. possible combinations of 1 from 2).

This gives rise to:

$$PFD_S = PFD_A . PFD_B$$

$$\lambda_S = PFD_A . \lambda_B + PFD_B . \lambda_A$$

If A and B are identical units, this reduces to:

$$PFD_S = (PFD)^2$$

$$\lambda_S = 2PFD . \lambda$$

16.4.2 **1oo3 (3oo3 to fail) repairable system**

For a system of units A, B and C, the probability of failure on demand (PFD) of the system is given by the product of the PFDs of the individual units (i.e. all the possible combinations of 3 from 3).

For the failure rate, we must look at all the possible combinations of 2 from 3 – which is the level of fault tolerance.

This gives rise to:

$$PFD_S = PFD_A . PFD_B . PFD_C$$
$$\lambda_S =$$
$$+PFD_A . PFD_B . \lambda_C$$
$$+PFD_A . PFD_C . \lambda_B$$
$$+PFD_B . PFD_C . \lambda_A$$

If A, B and C are identical units, this reduces to:

$$PFD_S = (PFD)^3$$
$$\lambda_S = 3PFD^2 \lambda$$

16.4.3 **2oo3 (2oo3 to fail) repairable system**

For a system of units A, B and C, the probability of failure on demand (PFD) of the system is all the possible combinations of 2 from 3.

For the failure rate, we must look at all the possible combinations of 1 from 3 – which is the level of fault tolerance.

This gives rise to:

$$PFD_S = \\ +PFD_A.PFD_B \\ +PFD_A.PFD_C \\ +PFD_B.PFD_C \\ \lambda_S = \\ +PFD_A.(\lambda_B + \lambda_C) \\ +PFD_B.(\lambda_A + \lambda_C) \\ +PFD_C.(\lambda_A + \lambda_C)$$

If A, B and C are identical units, this reduces to:

$$PFD_S = 3(PFD)^2$$
$$\lambda_S = 3PFD^2.2\lambda = 6PFD^2\lambda$$

16.4.4 **2oo4 (3oo4 to fail) repairable system**

For a system of units A, B, C and D, the probability of failure on demand (PFD) of the system is all the possible combinations of 3 from 4.

For the failure rate, we must look at all the possible combinations of 2 from 4 – which is the level of fault tolerance.

This gives rise to:

$$PFD_S = \\ +PFD_A.PFD_B.PFD_C \\ +PFD_A.PFD_B.PFD_D \\ +PFD_A.PFD_C.PFD_D \\ +PFD_B.PFD_C.PFD_D$$

$$\lambda_S = \\ +PFD_A.PFD_B(\lambda_C + \lambda_D) \\ +PFD_A.PFD_C(\lambda_B + \lambda_D) \\ +PFD_A.PFD_D(\lambda_B + \lambda_C) \\ +PFD_B.PFD_C(\lambda_A + \lambda_D) \\ +PFD_B.PFD_D(\lambda_A + \lambda_C) \\ +PFD_C.PFD_D(\lambda_A + \lambda_B)$$

If A, B, C, and D are identical units, this reduces to:

$$PFD_S = 4(PFD)^3$$
$$\lambda_S = 6PFD^2.2\lambda = 12PFD^2\lambda$$

16.4.5 **2oo5 (4oo5 to fail) repairable system**

For a system of units A, B, C, D and E, the probability of failure on demand (PFD) of the system is all the possible combinations of 4 from 5.

For the failure rate, we must look at all the possible combinations of 3 from 5 – which is the level of fault tolerance.

This gives rise to:

$$
\begin{aligned}
&PFD_S = \\
&+PFD_A.PFD_B.PFD_C.PFD_D \\
&+PFD_A.PFD_B.PFD_C.PFD_E \\
&+PFD_A.PFD_B.PFD_D.PFD_E \\
&+PFD_A.PFD_C.PFD_D.PFD_E \\
&+PFD_B.PFD_C.PFD_D.PFD_E
\end{aligned}
$$

$$
\begin{aligned}
&\lambda_S = \\
&+PFD_A.PFD_B.PFD_C(\lambda_D + \lambda_E) \\
&+PFD_A.PFD_B.PFD_D(\lambda_C + \lambda_E) \\
&+PFD_A.PFD_B.PFD_E(\lambda_C + \lambda_D) \\
&+PFD_A.PFD_C.PFD_D(\lambda_B + \lambda_E) \\
&+PFD_A.PFD_C.PFD_E(\lambda_B + \lambda_D) \\
&+PFD_A.PFD_D.PFD_E(\lambda_B + \lambda_C) \\
&+PFD_B.PFD_C.PFD_D(\lambda_A + \lambda_E) \\
&+PFD_B.PFD_C.PFD_E(\lambda_A + \lambda_D) \\
&+PFD_B.PFD_D.PFD_E(\lambda_A + \lambda_C) \\
&+PFD_C.PFD_D.PFD_E(\lambda_A + \lambda_B)
\end{aligned}
$$

If A, B, C, D and E are identical units, this reduces to:

$$
\begin{aligned}
&PFD_S = 5(PFD)^3 \\
&\lambda_S = 10PFD^2.2\lambda = 20PFD^2\lambda
\end{aligned}
$$

16.4.6 **f-N repairable system.**

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:

The Probability of Failure on Demand and the Failure Rate of the system are given by the following (as derived above):

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

$$\lambda_S = C_f^N . PFD^f . r\lambda$$

16.5 **Effect of Proof Test Strategy**

There is sometimes a problem when multiplying time averages together and that is when the functions behind the averages are not independent of one another: this is the case with proof testing.

Whether proof testing is synchronous (all units tested at the same time) of whether it is staggered (all units tested on rotation at evenly spaced intervals) the functions are not independent and this has a distorting effect on joint probabilities of failure, such that, where PFD^i represents the PFD of i components in parallel, in general:

$$PFD^i \neq (PFD^1)^i$$

For undetected failure with test interval T, the regime distortion factors are developed in *Effects of Proof* Testing.

For example, for synchronised testing where $MTTR \ll T$:

$$PFD^1 = \frac{\lambda T}{2}$$

$$PFD^2 = \frac{(\lambda T)^2}{3}$$

$$PFD^3 = \frac{(\lambda T)^3}{4}$$

It should therefore be understood that PFD^i is a notation which implies the average probability of failure of i items.

16.6 **Common Cause Failures.**

Common cause failures are a large topic in their own right. Here we introduce the concept. Common cause failures (they should really be referred to as *common cause faults*) occur in redundant systems where a single event can cause a fault in more than one parallel unit.

If we consider a large human population, two people taken at random are much less likely to die of the same cause than two people taken from the same family: this is because two people from the same family are likely to share the same environment and (importantly) have *shared DNA* which make them susceptible to similar things. Industrial components are similar – if they were made in the same factory, at the same time, they are much more likely to suffer from the same weaknesses than components selected at random. But practicalities of commerce and

construction mean that the components we find in redundant form are likely to have a lot of 'shared DNA' unless we take very specific steps to avoid it.

In truth, hardware faults may appear to be random but if, once failed, we carry out an autopsy, we usually find that there is a systematic issue that lies beneath. We use the concept of random hardware failures because (in large enough numbers) the random model fits well. What follows is an introduction to methods we can use to cope with this phenomenon.

There are various models that have been adopted to include appropriately modified formulae to compensate for common cause failures. The most popular is that adopted by *IEC 61508 [1]* which is referred to as the β model.

Reliability modelling is only an approximation of the real world and no one method can always claim to be superior. This document and those that follow adopt the simple β model where a certain fraction of failures is deemed to cause a fault in all related units and the remaining fraction is treated as independent. All common cause models depend heavily on the estimation of the applicable 'factor' (in our case, the β-factor) and it is noted here that estimation techniques generally include systematic operation and maintenance errors. It is difficult to understand how something which applies to random hardware failures and 'shared DNA' can be affected by systematic operation and maintenance errors. A systematic error in operation and maintenance will result in failure whatever the underlying reliability of the hardware. This document and those that follow adopt the view that systematic operation and maintenance failures are a separate additional class of failures entirely and should be accounted for by procedure: most importantly, they should certainly not be taken as a multiple of the underlying failure.

The following shows the effect the simple $\beta\ model$ has on the above formulae.

This has a modifying effect on the above formulae. For example, for a 1oo2 to survive system **with diagnosed failures only**:

$$PFD_D^2 = \left((1-\beta)\lambda_d MTTR\right)^2 + \beta\lambda_d MTTR$$

Thus, a small fraction (β) of the failures act as though there is only one item.
In general, for **diagnosed failures**:

$$PFD_D^N = \left((1-\beta)\lambda_d MTTR\right)^N + \beta\lambda_d MTTR$$

Likewise, where $MTTR \ll T$, for 1oo2 to survive system for **undiagnosed failures only** and synchronous testing:

$$PFD_U^2 = \left(\frac{(1-\beta)\lambda_d T}{2}\right)^2 + \frac{\beta\lambda_d T}{2}$$

In general, where $MTTR \ll T$, for **undiagnosed failures** and synchronous testing:

$$PFD_U^N = \left(\frac{(1-\beta)\lambda_d T}{2}\right)^N + \frac{\beta\lambda_d T}{2}$$

Notes:

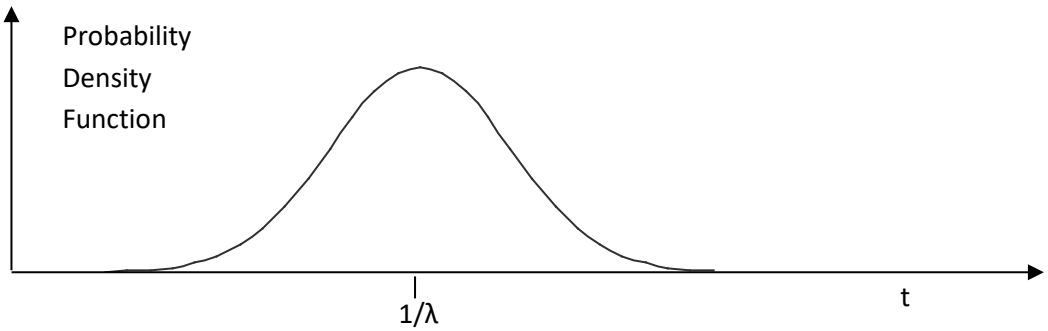
- In general systems have both diagnosed and undiagnosed failures.
- The distorting effects of proof testing are not included here.

17 Estimating Failure Rate from Observation

If we are trying to find the failure rate form observed failures, we need a simple formula:

$$\lambda = \frac{No\_of\_failures}{Component\_Population \times time}$$

For an infinitely large population, the probability of failure density function looks like a normal distribution:



If we estimate our mean time before failure from a small number of observations (n), how do we know we are estimating it accurately enough? The truth is, we don't.

However, we can use the Chi Squared distribution to help compensate on the side of safety using f = (2n+1) for the degrees of freedom.

For example, if we have had 2 failures in a population of 4 motors in a period of 5 years, then the mean failure rate is given by:

$$\lambda = \frac{No\_of\_failures}{Component\_Population \times time} = \frac{2}{4 \times 5} = 0.1y^{-1}$$

Let's say we are looking for a 70% confidence that the value of the actual failure rate is better than the one returned.

Using the Chi squared method of 70% confidence:

Number of failures, $n = 2$

Degrees of freedom, $f = 2(2 + 1) = 6$

Number of component years, $x = 20$

From the Chi squared tables, we get:

$$\chi^2_{70\%} = 7.231$$

We then apply the following formula:

$$\lambda_{70\%} = \frac{\chi^2_{70\%}}{2x} = \frac{7.231}{2 \times 4 \times 5} = 0.181y^{-1}$$

We therefore have a 70% confidence level that a failure rate of 0.181 pa is higher than the true value.

Note: IEC 61508:2010 [1] requires that a minimum 90% confidence interval is used for data used in supporting a *Proven in Use* claim for relevant reliability data. In effect that means that the chances that the MTBF for a device is worse than the figure being used must 5% or less.

18 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, I&E Systems Pty – Australia (available free to download from *The 61508 Association* website).

19 Conclusion

This paper is part of a series of documents (see introduction) and therefore a conclusion is not required at this point.

20 Existing and Emerging Standards

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

21 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 ***