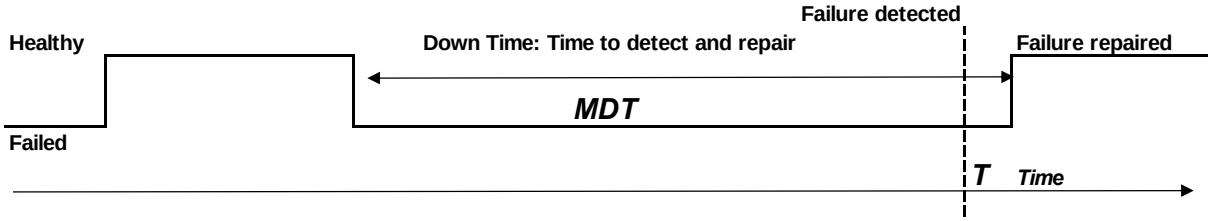
AN EXPLANATION OF THE PRINCIPLES BEHIND SIF FAILURE RATE EQUATIONS

The probability of failure calculations are based on the idea of 'fractional dead time'. This is the proportion of time that a 'channel' will be unable to perform its function.



$$PFD_{avg} \approx MDT/T$$

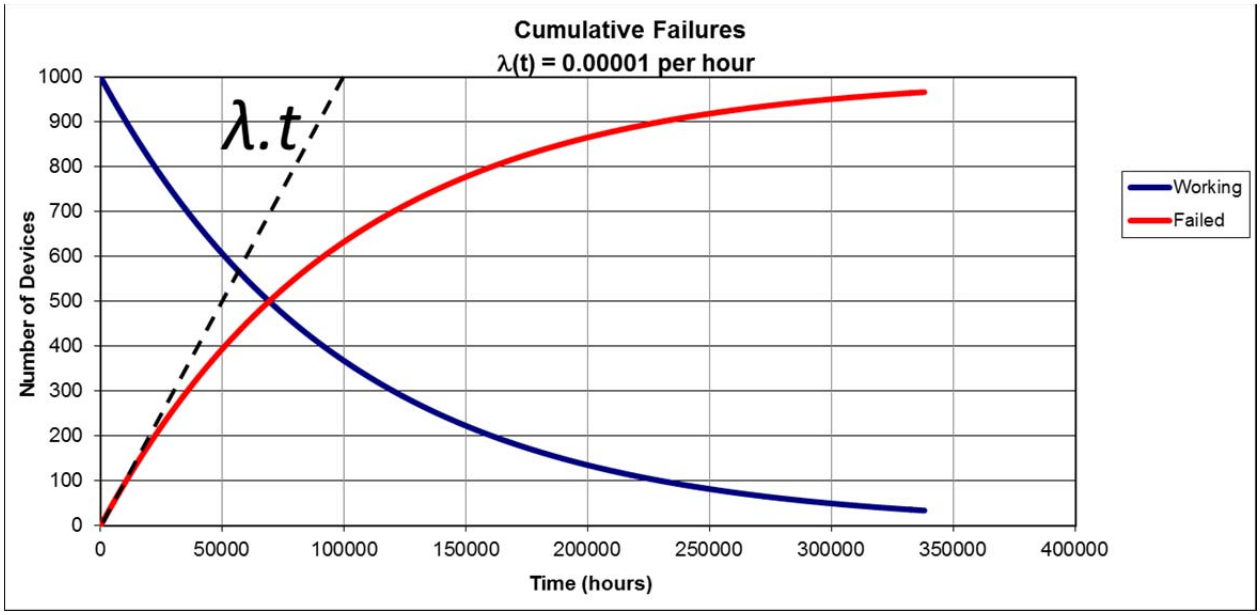
MDT represents the Mean Dead Time. We can think of 2 contributions to the dead time, corresponding to failures detected by continuous diagnostics, and failures that remain undetected until a full test or until there is a demand on the safety function.

The dead time includes the time to detect and then to repair the failure. The dead time for 'detected failures' that are detected by continuous automatic diagnostics is relatively short.

The dead time for the 'undetected failures' is much longer. The failures may remain undetected until the next proof test, so the dead time depends on the interval between proof tests.

Undetected Failures

Random failure occurring continuously and independently at a constant average rate can be described as a Poisson process. The accumulating failures follow an exponential distribution, building up until eventually the entire population has failed:

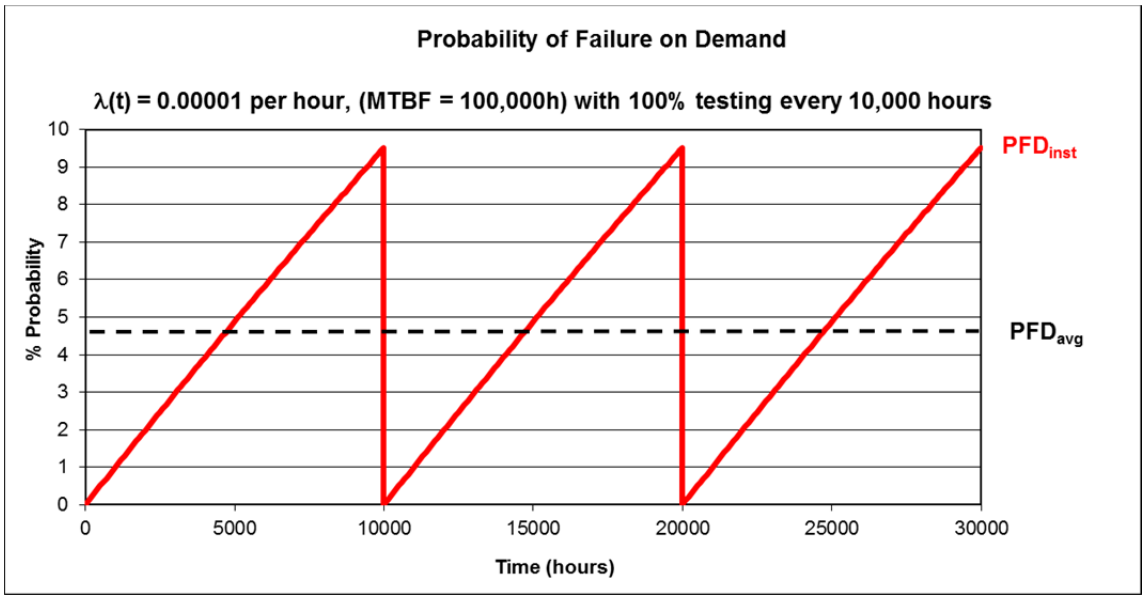


The initial rate of accumulation of failures is proportional to the elapsed time and the rate of failures (λ_{DU}). The failure rate λ_{DU} is the reciprocal of the mean time between failures, $= 1/MTBF_{DU}$.

The number of devices failed at time $t \approx \lambda_{DU}.t$, provided that the elapsed time t is much less than mean time between undetected dangerous failures ($MTBF_{DU}$).

The probability of failure is proportional to number of failures that have accumulated in the population.

Failures that are undetected by diagnostics accumulate in this manner as time progresses. The failed devices remain failed until the proof test at time *T*.



The average number of failed devices and therefore the average probability of failure can be calculated as:

$$PFD_{AVG} = \frac{1}{T}\int_0^T \lambda_{DU}\,(t).\,dt$$

If $T << MTBF_{DU}$ we can use the approximation $\lambda_{DU}(t) \approx \lambda_{DU}.t$

$$PFD_{AVG} = \frac{1}{T}\int_0^T \lambda_{DU}\,.t.\,dt$$

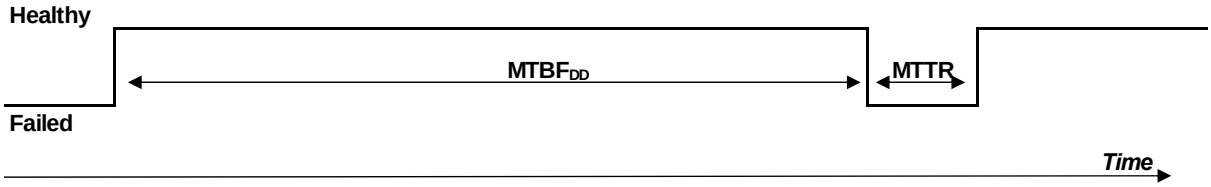
$$= \frac{1}{T}.\frac{\lambda_{DU}T^2}{2}$$

$$= \frac{\lambda_{DU}.T}{2}$$

Strictly speaking we need to add in the mean repair time *MRT* to represent the time that the function is out of action after the failure is found at time *T*. The *MRT* is usually measured in measured in hours or days, much shorter than *T* which is measured in years. In practice the process is taken out of service during the repair or else additional risk mitigation is implemented. The *MRT* is usually neglected.

Detected Failures

Detected failures are detected by continuous, automatic diagnostic functions. Detected failures are detected and repaired within the mean time to restoration, *MTTR*:



If $MTBF_{DD}$ is the mean time between detected dangerous failures, and the *MTTR* is the mean time to restoration (= time to detect + time to repair), then the probability of failure is simply the fraction of time that the channel is out of action, $MTTR/MTBF_{DD}$.

The rate of detected dangerous failures, λ_{DD} = 1/MTBF$_{DD}$., so we can express the probability as:

$$PFD_{AVG} = \lambda_{DD}.MTTR$$

Overall probability of failure

The overall probability of failure is the sum of the probabilities of failure for undetected and detected failures.

It is valid approximation to simply add the probabilities because the probabilities are << 1.

$$PFD_{AVG} = \frac{\lambda_{DU}.T}{2} + \lambda_{DD}.MTTR$$

In a low demand function the last term for detected failures is usually very small compared to the undetected failures, so it may usually be neglected.

Probability of failure for 1oo2 voting

In a 1oo2 architecture, the function will fail only if ***both*** channels fail, so the probability is proportional to the product of the probability of each channel failing, $(\lambda_{DU}.t).(\lambda_{DU}.t)$

To derive the basic equation calculating PFD$_{AVG}$ for a 1oo2 architectures we integrate the probability function over time to *T*, (the test interval) and divide by the time period *T* to get the average probability:

$$\frac{1}{T}\int_0^T {\lambda_{DU}}^2 t^2.dt =$$

$$\frac{1}{T}.\frac{{\lambda_{DU}}^2 T^3}{3} =$$

$$\frac{{\lambda_{DU}}^2 T^2}{3}$$

The probability of common cause failures should always be added to the PFD for any architecture with voting, as it usually dominates.

The factor β represents the proportion of failures that have a common cause. These common failures behave in the same way as a single channel, so the average probability of failure due to common causes is:

$$\beta.\frac{\lambda_{DU}.T}{2}$$

If the *MTTR* is short we can neglect the contribution from detected failures again, so the end result is:

$$PFD_{AVG} = \frac{{\lambda_{DU}}^2.\ T^2}{3} + \frac{\beta.\lambda_{DU}.T}{2}$$

'M out of N' equations

The method of calculating probability of failure on demand for 'M out of N' architecture is based on:

> Florent Brissaud, Anne Barros, Christophe Bérenguer. (2010). '*Probability of Failure of Safety-Critical Systems Subject to Partial Tests*. Reliability and Maintainability Symposium, RAMS 2010, San Jose (referenced in Cornell University Library, < **arXiv:1007.5448** >).

The simplified equation is:

$$PFD_{AVG} = \binom{N}{N-M+1}.\frac{(\lambda_{DU}.\ T)^{N-M+1}}{N-M+2} + \frac{\beta.\lambda_{DU}.T}{2}$$

$$= \frac{N!}{(N-M+1)!.(M-1)!}.\frac{(\lambda_{DU}.\ T)^{N-M+1}}{N-M+2} + \frac{\beta.\lambda_{DU}.T}{2}$$

This simplified equation neglects *MRT* and *MTTR* on the basis that they are << *T*. This is a valid simplification that is commonly used with the IEC 61508 and ISA S84 calculations.

The second term $(\lambda_{DU}.T)^{N-M+1}/(N-M+2)$ is the average number of accumulated failures, calculated by the integration of the accumulated failures over time T, as demonstrated above for 1oo2.

The term **N-M+1** in the exponent is the hardware fault tolerance + 1. It is **the number of channels that have to fail for the function to fail**, which is why it appears as the exponent for the term.

For instance in 2oo3, N-M+1 = 3-2+1 = 2. As the probability of one device failing is proportional to $(\lambda_{DU}.t)$ the probability of 2 devices failing together is $(\lambda_{DU}.t)^2$.

The factor N-M+2 in the denominator comes from integrating $t^{N-M+1}.dt$ to calculate the average over the period *T*.

The first term $\binom{N}{N-M+1}$ 'N choose N-M+1' takes into account the different combinations of the N-M+1 faulty channels. The PFD increases in direct proportion to the number of ways we can choose a combination of enough faulty channels for the SIF to fail. 1oo2 voting and 2oo3 both need 2 coincident failures for the function to fail, but failure is 3 x more likely with 2oo3 because there are 3 times as many ways of having 2 coincident failures.

In 1oo2 voting between channel A and channel B, both A and B must fail for the function to fail.

In 2oo3 voting, the function will fail if 2 channels are faulty and 1 remains healthy. There are 3 possible choices for the 2 failed channels (A and B), (B and C) or (C and A), or the other way of thinking about it is that there are 3 choices for having only 1 healthy channel: A, B or C.

$$\binom{3}{2} = \binom{3}{1} = \frac{3!}{1!.\,2!} = 3$$

We saw above that the PFD_{AVG} for 1oo2 voting is given by:

$$PFD_{AVG} = \frac{{\lambda_{DU}}^2.\ T^2}{3} + \frac{\beta.\lambda_{DU}.T}{2}$$

The equation for 2oo3 voting is then simply:

$$PFD_{AVG} = 3.\frac{{\lambda_{DU}}^2.\ T^2}{3} + \frac{\beta.\lambda_{DU}.T}{2}$$

$$= {\lambda_{DU}}^2.\ T^2 + \frac{\beta.\lambda_{DU}.T}{2}$$

This is therefore consistent with the formula given in IEC 61508-6 and ISA S84.

Systematic Failures

The equations in ISA technical report ISA-TR84.00.02-2002 include a factor to quantify 'systematic failures', (λ_F) but strictly speaking systematic failures cannot be quantified using a constant failure rate.

For instance errors in the design of a component or in the coding of software do not occur at a measurable rate. The probability of systematic failures cannot be calculated. Appropriate techniques and measures should be applied to avoid or to control systematic faults. They can never be completely eliminated.

In practice only electronic components are subject to purely random failure. Virtually all failures of mechanical components (such as actuated valves) are systematic failures but they are treated as quasi-random failures. They are caused by age or wear related deterioration. They can't be prevented and within the useful life of the equipment the expected failure rates are close enough to being constant. They can be considered to be quasi random and modelled by a constant failure rate.

The failure rate statistics that are provided by OREDA and *exida* include systematic failures.

There is no need to add the separate term λ_F but it is good practice to include a safety margin over our calculated PFD. There is no rule defining how much margin is needed. A factor of 2 or 3 might be enough.

We need to consider the feasibility of maintaining that rate during the life of the plant, allowing for deterioration and for problems in maintenance (such as lack of accessibility for testing, lack of opportunity for maintenance). So if you calculate a RRF of 1007 will you be confident in claiming SIL 3 is achieved? No, maybe not, because it might not be maintainable. But yes, you might be confident that SIL 2 is achieved.

It is important to remember that the uncertainty in our input data is typically not much better than half an order of magnitude. Use only 1 significant figure of precision in expressing calculation results. The difference between an RRF of 990 and an RRF of 1100 is not meaningful.

SPURIOUS TRIP RATE EQUATIONS

The ISA technical report ISA-TR84.00.02-2002 - Part 2 provides equations for estimating spurious trip rates. The derivation of the equations is explained below.

'1ooN' Spurious Trip Rate

Put simply, the spurious trip rate (STR) for a single device is the same as its safe failure rate, λ_S. Spurious trip rates are usually measured in failures per year.

If detected dangerous failures also cause a trip condition the rate of dangerous detected failures should be added to give STR = $\lambda_S + \lambda_{DD}$.

Strictly speaking we should use the rate of safe failures that are undetected (λ_{SU}) and will cause a trip condition. In logic solver voting arrangements such as 1oo2D some safe failures can be detected by diagnostic functions. If a safe failure is detected the voting is automatically adapted rather than causing a trip. The term 'safe detected' (and the rate λ_{SD}) is only used in architectures with adaptive voting. It does not apply to sensors or final elements. For simplicity in the following explanation the term λ_S is used.

With '1ooN' voting the rate of spurious trips is simply proportional to the number of devices. The trip rate with 2 devices is 2 x the trip rate for a single device.

1oo2 STR = 2 x λ_S

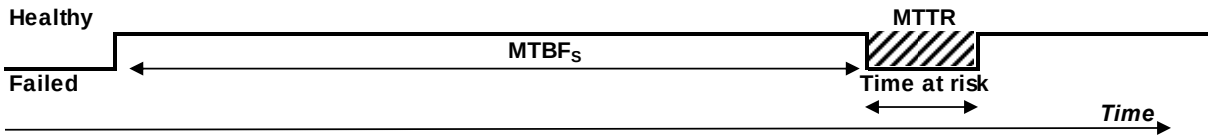
1oo3 STR = 3 x λ_S

1ooN STR = N x λ_S

'2oo2' Spurious Trip Rate - simplified

With '2oo2' voting 2 coincident safe failures are needed before a spurious trip occurs.

The spurious trip occurs only if a second failure occurs during the time at risk, the period in which the first failure is being repaired:



As there are 2 devices the rate of one safe failure (1oo2) is 2 x λ_S. The rate of the one remaining device failing safely (1oo1) is λ_S. The probability that the second failure happens during the time at risk from the first failure is proportional to the 'fractional dead time', FDT = MTTR/MTBF$_S$, and can be written as:

FDT = MTTR x 2 x λ_S.

The **rate** at which a coincident failure of both devices can be expected is therefore:

STR = (MTTR x 2 x λ_S) x λ_S.

With **2oo3 voting**, the first failure is any 1 out of the 3. After the first failure there are then 2 functioning devices left in service, essentially in a 1 out of 2 arrangement. Either one of those 2 failing will cause a trip.

The time at risk is the repair period after 1 failure out of 3 devices (MTTR x 3 x λ_S).

The rate of another 1 of the 2 remaining devices failing is 2 x λ_S.

The spurious trip rate is therefore the rate of the coincident failure:

$$STR = (MTTR \times 3 \times \lambda_S) \times (2 \times \lambda_S).$$

With **2ooN voting**, after the first failure there are (N-1) functioning devices left in service, in a 1oo(N-1) arrangement. Any one of those failing during the time at risk will cause a trip.

At any point in time the probability that one failure has already occurred is MTTR x N x λ_S (the time at risk, using the 1ooN equation for failure rate). After that first failure there are N-1 in service. The rate with which we can expect a second failure is (N-1) x λ_S, and so the spurious trip rate is:

$$STR = (MTTR \times N \times \lambda_S) \times ((N-1) \times \lambda_S).$$

For example the equation for **2oo4 voting** is

$$STR = (MTTR \times 4 \times \lambda_S) \times (3 \times \lambda_S).$$

$$= 12 \times MTTR \times \lambda_S^2$$

'2ooN' Spurious Trip Rate - complete

The complete form of the equation adds the λ_{DD} term (assuming that detected failures lead to a trip) and a **common cause failure term**:

$$STR = [MTTR \times N \times (\lambda_S + \lambda_{DD})] \times [(N-1) \times (\lambda_S + \lambda_{DD})] + [\boldsymbol{\beta \times (\lambda_S + \lambda_{DD})}]$$

The **common cause failure term must always be added** because usually ($\beta \times \lambda_S$) >> λ_S^2.

'3oo3' Spurious Trip Rate

With **3oo3 voting** the time at risk is the fraction of time during which the first 2 failed devices are both out of service:

$$FDT = MTTR \times [(MTTR \times 3 \times \lambda_S) \times (2 \times \lambda_S)],$$

The spurious trip rate is the failure rate of the 3rd device (only 1 left) x the FDT:

$$STR = MTTR \times [(MTTR \times 3 \times \lambda_S) \times (2 \times \lambda_S)] \times \lambda_S$$

'3ooN' Spurious Trip Rate

With **3ooN voting** after the first **2** failures there are **(N-2)** devices to choose from for the 3rd trip. Any one of those failing safely will cause the trip. The equation becomes:

$$STR = MTTR \times [(MTTR \times N \times \lambda_S) \times ((N-1) \times \lambda_S)] \times \mathbf{(N-2)} \times \lambda_S$$

$$= MTTR^2 \times \lambda_S^2 \times N \times N-1 \times N-2$$

$$= MTTR^2 \times \lambda_S^3 \times N! / (N-3)!$$

For example the equation for **3oo4 voting** is

$$STR = (MTTR^2 \times \lambda_S^3) \times 4! / 1!$$

$$= 24 \times MTTR^2 \times \lambda_S^3$$

'MooN' Spurious Trip Rate

With **MooN voting** the fractional dead time in which M-1 devices have failed into a trip state is:

$$FDT = MTTR^{(M-1)} \times \lambda_S^{(M-1)} \times N \times (N-1) \times (N-2) \ldots\ldots \times (N-(M-2))$$

After the first **M-1** failures there are then **(N-(M-1))** devices to choose from for the Mth trip. Any one of those failing safely will cause the trip. The equation becomes

$$STR = [MTTR^{(M-1)} \times \lambda_S^{(M-1)} \times N \times (N-1) \times (N-2) \ldots\ldots \times (N-(M-2))] \times \mathbf{(N-(M-1))} \times \lambda_S$$

The series of multipliers can be neatly written using the factorial form:

$$STR = MTTR^{(M-1)} \times \lambda_S^M \times N! / (N-M)!$$

'MooN' Spurious Trip Rate – complete equation

The complete form of the equation adds the λ_{DD} term and the common cause failure term:

$$STR = [MTTR^{(M-1)} \times (\lambda_S + \lambda_{DD})^M \times N! / (N-M)!] + [\beta \times (\lambda_S + \lambda_{DD})]$$