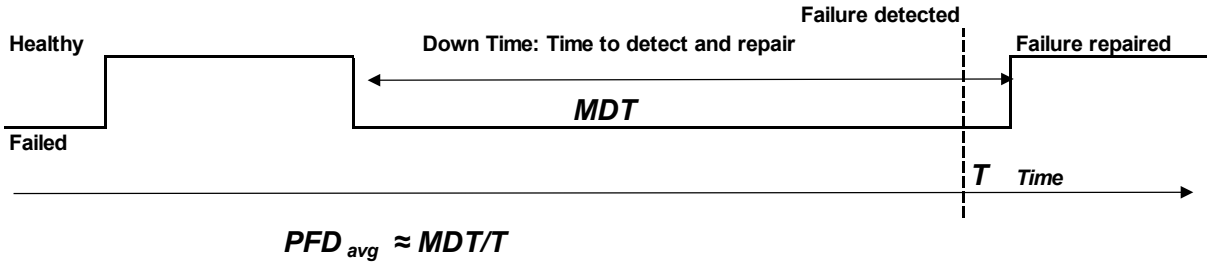
1 PRINCIPLES BEHIND SIF FAILURE RATE EQUATIONS

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.



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

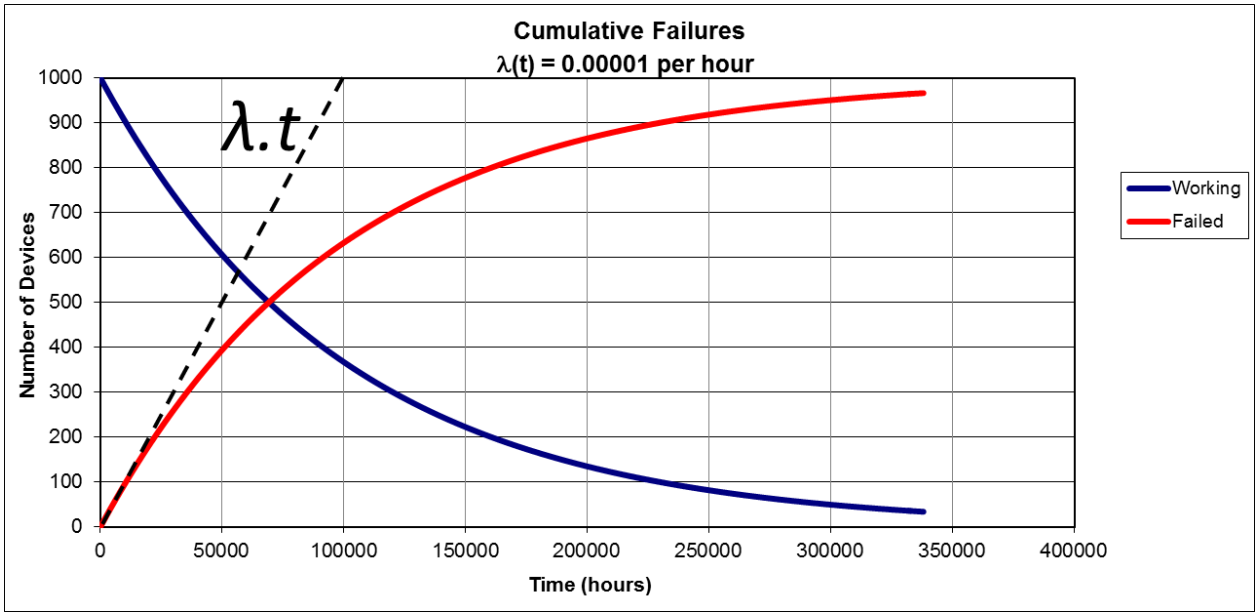
MDT represents the Mean Dead Time. We can think of 2 contributions to the dead time, corresponding to failures detected by continuous diagnostics, and failures that remain undetected until a full test or until there is a demand on the safety function.

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:

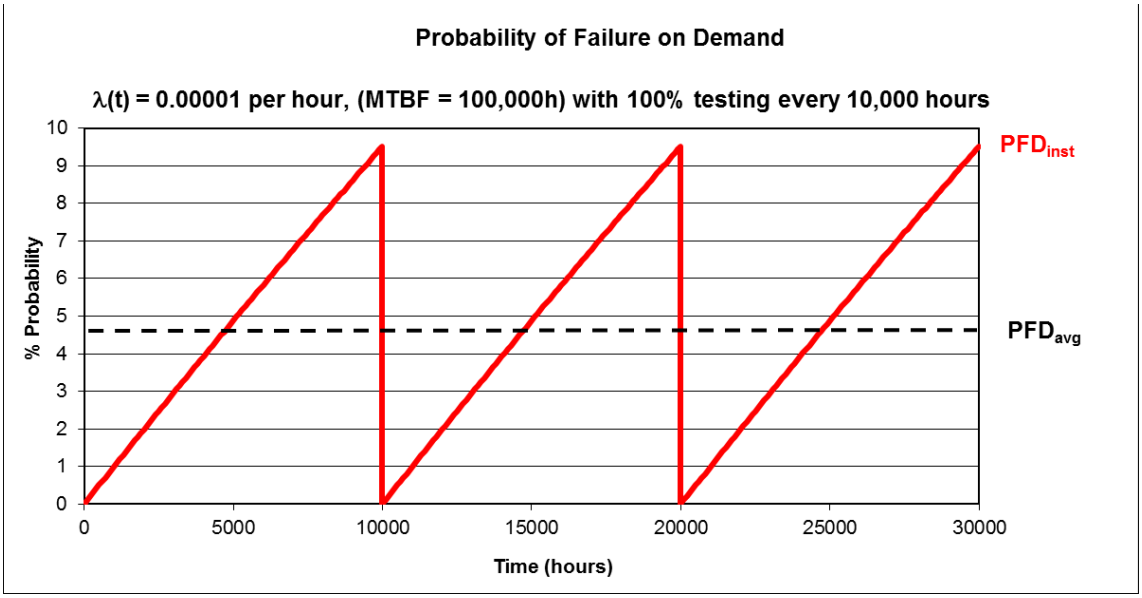


The initial rate of accumulation of failures is proportional to the elapsed time and the rate of failures (λ_{DU}). The failure rate λ_{DU} is the reciprocal of the mean time between failures, $= 1/MTBF_{DU}$.

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 $\lambda_{DU}(t) \approx \lambda_{DU}.t$

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

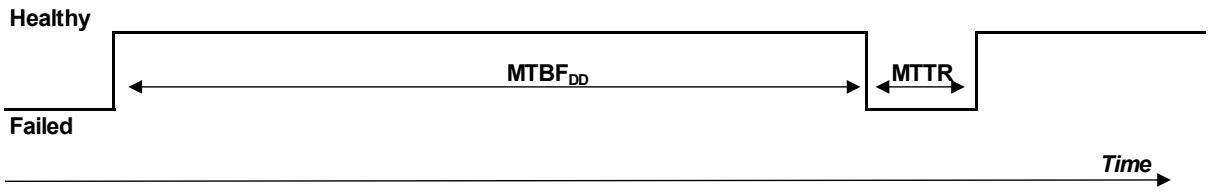
$$= \frac{1}{T}.\frac{\lambda_{DU}T^2}{2}$$

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

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. β is typically in the range 0.02 to 0.15. The common failures behave in the same way as a single channel, so the average probability of failure due to common causes is:

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

The proportion of λ_{DU} for which the channels behave as if they are independent is $(1 - \beta).\lambda_{DU}$

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

$$PFD_{AVG} \approx \frac{(1-\beta).{\lambda_{DU}}^2.\ T^2}{3} + \frac{\beta.\lambda_{DU}.T}{2}$$

The equation can be simplified further by assuming that $(1 - \beta) \approx 1$. This is a conservative simplification because the PFD will be slightly higher but the increase will be negligible:

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

'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* and it assumes that (1 - β) ≈ 1 because β << 1.

Note that the estimate of β depends on the voting. For instance, 9 out of 10 voting is much less susceptible to common cause failure than 1 out of 10. Refer to section 4 of the SINTEF PDS Method Handbook, Reliability Prediction Method for Safety Instrumented Systems' (2013).

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, so 2 devices failing cause the function to fail. As the probability of one device failing is proportional to $(\lambda_{DU}.t)$ the probability of 2 devices failing concurrently 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.

2 RULES OF THUMB

It is easy to estimate the overall probability of failure for a demand safety function by using some simple rules of thumb. Though these estimates are coarse they are useful for quickly identifying whether a safety function is likely to meet its failure performance target.

The rules of thumb are not presented here as an alternative to detailed calculations. They are presented only to give a quick feel for what performance is achievable.

Final elements (usually) dominate

In process sector applications with clean service the overall failure rate λ and the PFD_{AVG} is usually strongly dominated by the contribution from actuated on-off valves or electrical contactors as the final elements. This is because it is usually not practicable to implement automatic and continuous fault diagnostic functions on mechanical and electromechanical final elements. Without diagnostics dangerous faults remain undetected until the function is inspected and tested or until it fails to respond to a demand.

Sensors and logic solvers tend to have much lower dangerous failure rates than final elements because they are based on electronic devices. Electronic components can usually be equipped with automatic and continuous fault diagnostic functions. Most failures can be detected and remedial action can be taken to ensure that safe operation is achieved or maintained.

As a result, the rates of undetected dangerous failures for electronic components are generally at least an order of magnitude lower than for mechanical and electromechanical components.

Where the final elements are tested on an annual basis the final elements can be expected to contribute between 70% and 90% of the failure measure. The sensors typically contribute up to 25% of the failures and the logic solver less than 5% of the failures.

From this we can derive simple rules of thumb. An explanation of these rules of thumb is included in Section 5 below.

The overall failure rate may be dominated by the sensor failure rates in severe services where reliable sensing is difficult. For example, in minerals processing the sensors can have high failure rates and failures can difficult to detect. Similar rules of thumb could then be applied based on the sensor failure rate instead of the final element failure rate.

Single FE (1oo1)

For a first approximation with a single final element we can use:

$$RRF^{SIF} \approx 1.5 \times \frac{MTBF_{DU}^{FE}}{T}$$

$MTBF_{DU}$, the mean time between **d**angerous **u**ndetected failures of the final element and T is the test interval. Both need to be in the same units of measure and are usually measured in years.

For instance, for an actuated on/off shutdown valve a typical feasible value of $MTBF_{DU}^{FE}$ is in the range 40 y to 100 y. (Refer to the section below on '*Finding failure rates*'.)

With a single shutdown valve as a final element and with annual testing (T = 1 y) it is feasible for a safety function to achieve RRF in the range 60 to 150.

The bare minimum $MTBF_{DU}^{FE}$ of a single final element required to achieve a given RRF can be estimated as:

$$MTBF_{DU}^{FE} > 0.6 \times \quad RRF^{SIF} \times T$$

To achieve SIL 2 (i.e. RRF> 100) with T = 1 y requires $MTBF_{DU}^{FE}$ of at least 60 y.

This means that the failure performance of the valve will need to be optimised; a $MTBF_{DU}^{FE}$ of 40 y would not be sufficient to achieve SIL 2 with annual testing.

Electrical contactors can typically achieve $MTBF_{DU}^{FE}$ in the region of 200 y, so SIL 2 is easily achieved.

Dual FE (1oo2)

For a first approximation with two similar (1oo2) final elements we can assume $\beta \approx$ 10% and use:

$$RRF^{SIF} \approx 15 \times \frac{MTBF_{DU}^{FE}}{T}$$

With 1oo2 shutdown valve as final elements and annual testing (T = 1 y) and $MTBF_{DU}^{FE}$ in the range 40 y to 100 y it is feasible for a safety function to achieve RRF in the range 600 to 1,500.

The bare minimum $MTBF_{DU}^{FE}$ of dual final elements required to achieve a RRF in a 1oo2 arrangement can be estimated as:

$$MTBF_{DU}^{FE} > 0.6 \times \beta \times RRF^{SIF} \times T$$

and with β around 10%:

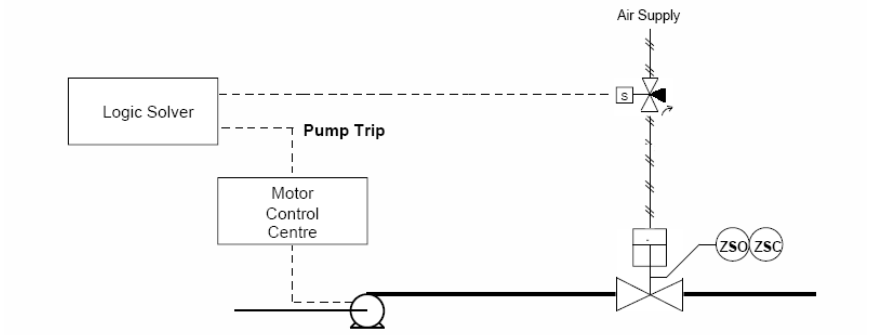
$$MTBF_{DU}^{FE} > {}^{6}/_{100} \times RRF^{SIF} \times T$$

To achieve SIL 3 (i.e. RRF> 1,000) with two valves and T = 1 y requires a $MTBF_{DU}^{FE}$ of at least 60 y.

With lower $MTBF_{DU}^{FE}$ either the failure performance of the valves will need to be improved, or β will need to be reduced below 10%, or else the inspection and test interval will need to be shortened to less than a year.

Diverse FE (1oo2)

Common cause failures can be minimised by using independent and diverse final elements. For instance, it may be possible to either stop a pump or close a valve to achieve a safe state.



The failure modes and the failure rates for electrical contactors are completely different to failure modes and the failure rates of valves.

The question is sometimes asked: 'which value of failure rate λ_{DU} should be used in the common cause failure term $\beta.\frac{\lambda_{DU}.T}{2}$, the failure rate of the valve, or of the contactor?'.

A much better question to ask is: 'what types of failure could possibly affect the valve and the contactor to cause them both to fail dangerously at about the same time?' and 'how can we eliminate those common cause failures?'

With diverse elements it is better to identify exactly what the causes of common cause failures might be and what is the expected rate at which those failures will occur. For instance, with the example shown above the common cause failures are limited to factors simultaneously affecting multiple output circuits of the logic solver.

It may be possible to eliminate almost all of the common causes of failure by design, so the probability of failure of the final elements would be approximately:

$$PFD_{AVG}^{FE} \approx \frac{\left(\lambda_{DU}^{valve}.T\right).\left(\lambda_{DU}^{contactor}.T\right)}{3}$$

Safety functions with completely independent and diverse final elements easily achieve SIL 3 levels of risk reduction.

3 FINDING FAILURE RATES

There are several useful references for failure rate information:

- OREDA 'Offshore and Onshore Reliability Handbook'
- *exida* database incorporated into exSILentia software,
  and tabulated in the *exida* SERH 'Safety Equipment Reliability Handbook'
- SINTEF PDS Data Handbook
  'Reliability Data for Safety Instrumented Systems'
- Users' own failure rate data
- Equipment certificates

The OREDA project provides a useful source of failure rate information gathered over many years by a consortium of oil and gas companies. The OREDA handbooks summarise all failures recorded over the normal useful operating life of equipment (i.e. excluding end-of-life failure). Different editions of the handbook cover different periods of time. The tables can be difficult to interpret but they are useful because they indicate the ranges of failure rates that are achieved in operation.

The failure rate tables published by OREDA show that failure rates recorded by different users typically vary over one or two orders of magnitude. OREDA fits the different reported failure rates into probability distributions to estimate the overall mean failure rate and standard deviation for each type of equipment and type of failure.

It is evident from the OREDA tables that the failure rates are not constant across different users and different applications. Some users consistently achieve failure rates at least 10 times lower than other users. The implication here is that it may be feasible for other users to minimise their failure rates through best practice in design, operation and maintenance.

The SINTEF PDS Data Handbook provides a concise summary of failure rates that are typically achievable. It includes OREDA data as an input source.

The *exida* failure rate database is based on failure mode analysis. It provides estimated failure rates and failure modes for specific makes and models of many commonly used devices. The failure rates are calculated from typical failure rates of the individual components that make up each device. The *exida* failure rates are calibrated with field failure data. The database is regularly updated with current failure measurements from users.

The *exida* failure rates are reasonably consistent with the OREDA data and can be taken as a good indication of failure rates that are achievable in practice. It presents failure rates that typically at least 70% of users are achieving in practice.

The *exida* dataset has some advantages over OREDA: It allows comparison of different designs and different makes and models of devices. It is easier to interpret than OREDA because it presents failure rate data in a more consistent form.

One concern with *exida* failure rates is that they are presented with 3 or 4 significant figures of precision, implying that the rates are fixed and constant. In practice the uncertainty in these rates is as wide as in the OREDA data. The variation in the rates that can be achieved in operation spans at least an order of magnitude.

Failure rates on SIL certificates need to be treated with caution if the quoted failure rates are significantly lower than failure rates in the industry-wide databases. Certifying bodies may specifically exclude systematic failures when evaluating failure rate. Such low failure rates cannot be easily achieved in practice.

4 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 = $2.\lambda_S$

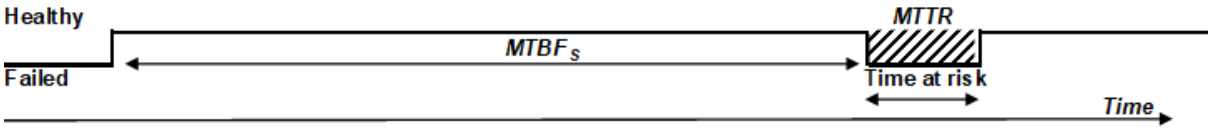
1oo3 STR = $3.\lambda_S$

1ooN STR = $N.\lambda_S$

'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:

$$FDT = MTTR.2.\lambda_S$$

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

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

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 ($MTTR$. 3 . λ_S).

The rate of another 1 of the 2 remaining devices failing is $2.\lambda_S$.

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

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

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 $MTTR$. N . 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) . λ_S, and so the spurious trip rate is:

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

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

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

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

'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**:

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

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

'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:

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

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

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

'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:

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

$$= MTTR^2 . \lambda_S^2 .N .(N-1).(N-2)$$

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

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

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

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

'MooN' Spurious Trip Rate

With **MooN voting** the M^th^ failure cause a trip. The fractional dead time in which M-1 devices have failed into a trip state is:

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

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

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

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

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

'MooN' Spurious Trip Rate – complete equation

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

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

5 FAILURE RATE EQUATIONS FOR CONTINUOUS MODE

Continuous mode safety functions are those where a dangerous undetected failure directly causes a hazard to occur. They are characterised by failure rate instead of by a probability of failure on demand.

In these estimates it is assumed that some appropriate response can be made to dangerous failures that are detected.

Estimating the overall dangerous failure rate of different SIF architectures follows a process that is similar to estimating spurious trip rate.

With 'NooN' voting all of the devices are required to be in service for continued safe operation. Any one device failing will cause a hazard. The overall rate of dangerous undetected failures is simply proportional to the number of devices. The failure rate with 2 devices is 2 x the failure rate for a single device.

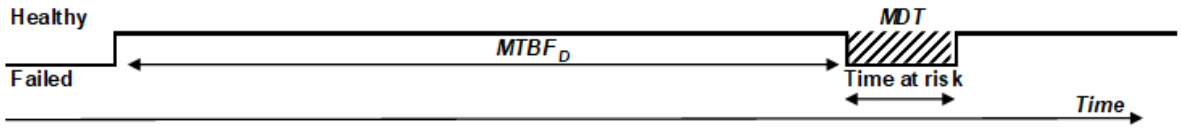
2oo2 $\lambda_{DU} = 2.\lambda_{DU}$

3oo3 $\lambda_{DU} = 3.\lambda_{DU}$

NooN $\lambda_{DU} = N.\lambda_{DU}$

'1oo2' Failure Rate

With '1oo2' voting 2 coincident dangerous failures are needed before a dangerous loss of function occurs. The hazard 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 the first dangerous failure (1oo2) is 2 x λ_D. The rate at which the one remaining device fails dangerously without being detected (1oo1) is λ_{DU}. We assume that if the failure can be detected by diagnostics the system can be shut down safely.

The probability that the second failure happens during the time at risk from the first failure is proportional to the 'fractional dead time', $FDT = 2 \times MDT/MTBF_D$ (multiplying by 2 for 2 devices) and this can be written as:

$$FDT = 2.MDT.\lambda_D$$

The **rate** λ_G ('G' for group) at which we can expect a coincident failure of both devices in a group voted 1oo2 is therefore:

$$\lambda_G = 2.MDT.\lambda_D.\lambda_{DU} + \beta.\lambda_{DU}$$

The mean down time *MDT* depends on whether the first failure is detected or undetected.

If the failure is detected through continuous diagnostics we assume it will be repaired within the mean repair time, *MRT*.

If the failure is not detected through continuous diagnostics we assume that the average time to restore it to service will be approximately half the periodic test interval *T*.

The *MDT* can be estimated from the proportion of dangerous failures that remain undetected by continuous diagnostics:

$$MDT = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D}(MTTR)$$

$$MDT \approx \frac{\lambda_{DU}}{\lambda_D}.\frac{T}{2} + \frac{\lambda_{DD}}{\lambda_D}.MTTR$$

In this case the *MTTR* term can be significant because usually $\lambda_{DD} >> \lambda_{DU}$.

We can often achieve a high diagnostic coverage in continuous mode functions because the functions take continuous action that can be easily monitored.

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 3 x *MDT* x λ_D.

The rate of another 1 of the 2 remaining devices failing without being detected is 2 x λ_{DU}.

The failure rate of the group as a whole is therefore the rate of the coincident failure:

λ_G = 3.*MDT*.λ_D.(2.λ_{DU}) + $\beta.\lambda_{DU}$

λ_G = 6.*MDT*.λ_D.λ_{DU} + $\beta.\lambda_{DU}$

'MooN' Failure Rate – complete equation

Deriving the MooN forms is more complicated than for spurious trip because the $T/2$ and $MTTR$ terms need to be treated separately when multiple coincident failures are considered.

For a detailed explanation refer to Smith, D. J. '*Reliability, Maintainability and Risk*', 9th Ed. Butterworth Heinemann. 2017.

For revealed failures the general form is:

λ_G = N! / [(N-M)!.(M-1)!] . ($\lambda^{(N-M+1)}$.*MDT*$^{(N-M)}$), where MDT is estimated from $MTTR$.

For unrevealed failures the general form is:

λ_G = N! / [(N-M+1)!.(M-1)!] . ($\lambda^{(N-M+1)}$.*MDT*$^{(N-M)}$), where MDT is estimated from T.

As always, the common cause failure term must be added:

+ $\beta.\lambda_{DU}$

The overall failure rate of any voted group will usually be strongly dominated by the common cause failure term. In practice the two $\lambda^{(N-M+1)}$.*MDT*$^{(N-M)}$ terms are negligible.

6 MORE DETAIL: DERIVING THE RULES OF THUMB

Single FE (1oo1)

Calculations of failure probability for demand functions are based on the coarse assumption that **d**angerous **u**ndetected failures occur at a constant rate, λ_{DU}.

In any set of similar devices undetected failures would then accumulate exponentially. Once any individual device fails it remains failed until its failure is revealed by either inspection, a test or a demand on the function.

The probability of failure of any individual device in a given set of devices is proportional to the number of failures that have been allowed to accumulate in the time t since the last full test and inspection:

$$PFD(t) = \int_0^t \lambda_{\mathrm{DU}} \,.\, e^{-\lambda_{DU}.\tau}.\, d\tau = \; 1 - \; e^{-\lambda_{DU}.t}$$

The exponential curve is almost linear for $PFD < 0.2$. Safety functions always have $PFD_{AVG} < 0.1$, so it is always valid to use a linear approximation for the curve. There is no benefit at all in making a more precise calculation because the initial assumption of constant failure rate is coarse. Any additional precision would be meaningless because in practice the failure rate is a variable rather than a constant.

The average probability of failure PFD_{AVG} of a single final element can then be approximated by:

$$PFD_{AVG}^{FE} \;\approx\; \frac{\lambda_{DU}.T}{2}$$

where T is the test interval.

Failures that are detected make a smaller contribution to the probability of failure because they can be repaired promptly or the system can be taken out of service. The contribution from the rate of detected dangerous failures λ_{DD} is negligible.

A more convenient way of expressing the approximation is in terms of risk reduction factor RRF and $MTBF_{DU}$, the mean time between **d**angerous **u**ndetected failures of the final element.

$$RRF^{FE} \approx \; 2 \; \times \frac{MTBF_{DU}^{FE}}{T}$$

RRF is the reciprocal of PFD_{AVG} and $MTBF_{DU}$ is the reciprocal of λ_{DU}.

The overall RRF of the safety function with a single final element is typically in the range:

$$RRF^{SIF} \approx 0.7 \; \times \; RRF^{FE} \;\; \text{to} \;\; 0.9 \times \; RRF^{FE}$$

$$RRF^{SIF} \approx 1.4 \times \frac{MTBF_{DU}^{FE}}{T} \;\; \text{to} \;\; 1.8 \; \times \frac{MTBF_{DU}^{FE}}{T}$$

For a first approximation use:

$$RRF^{SIF} \approx 1.5 \; \times \frac{MTBF_{DU}^{FE}}{T}$$

For instance, a typical feasible value of $MTBF_{DU}^{FE}$ for an actuated on/off shutdown valve is in the range 40 y to 100 y.

With a single shutdown valve as a final element and with annual testing (T = 1 y) it is feasible for a safety function to achieve RRF in the range 60 to 150.

The bare minimum $MTBF_{DU}^{FE}$ of a single final element required to achieve a given RRF can be estimated as:

$$MTBF_{DU}^{FE} > 0.6 \times \ RRF^{SIF} \times T$$

Dual FE (1oo2)

The PFD_{AVG} of a pair of similar final elements in a 1oo2 arrangement can be approximated by:

$$PFD_{AVG}^{FE} \ \approx \ (1-\beta).\frac{(\lambda_{DU}.T)^2}{3} + \beta.\frac{\lambda_{DU}.T}{2}$$

The last term in this equation applies the β factor to represent the proportion of failures that have a common cause. The common cause term will dominate the PFD_{AVG} unless the following is true:

$$\beta \ll \lambda_{DU}.T$$

If the test interval T = 1 y and λ_{DU} = 0.02 pa ($MTBF_{DU}^{FE}$ = 50 y), then the common cause failure term will be greater than the first term unless β < 2%.

A value as low as 2% is difficult to achieve with similar final elements. A recent SINTEF study (Report A26922) showed that β is typically in the range 12% to 15%. With $\beta \geq$ 5% we can make the further approximation:

$$PFD_{AVG}^{FE} \ \approx 1.1 \times \beta.\frac{\lambda_{DU}.T}{2}$$

and so

$$RRF^{FE} \approx \ 1.8 \times \frac{MTBF_{DU}^{FE}}{\beta.T}$$

For a rule of thumb the common cause factor β can be assumed to be around 10%.

$$RRF^{FE} \approx \ 18 \times \frac{MTBF_{DU}^{FE}}{T}$$

The overall RRF of the safety function with 1oo2 final elements is typically in the range:

$$RRF^{SIF} \approx 0.7 \times RRF^{FE} \ \text{ to } \ 0.9 \times RRF^{FE}$$

so then

$$RRF^{SIF} \approx 12 \times \frac{MTBF_{DU}^{FE}}{T} \ \text{ to } \ 16 \times \frac{MTBF_{DU}^{FE}}{T}$$

or roughly,

$$RRF^{SIF} \approx 15 \times \frac{MTBF_{DU}^{FE}}{T}$$

With 1oo2 shutdown valve as final elements and annual testing (T = 1 y) and $MTBF_{DU}^{FE}$ in the range 40 y to 100 y it is feasible for a safety function to achieve RRF in the range 600 to 1,500.

The bare minimum $MTBF_{DU}^{FE}$ of dual final elements required to achieve a RRF in a 1oo2 arrangement can be estimated as:

$$MTBF_{DU}^{FE} > \ 0.6 \times \beta \times \ RRF^{SIF} \times T$$

and with β around 10%:

$$MTBF_{DU}^{FE} > {}^{6}/_{100} \times RRF^{SIF} \times T$$

To achieve SIL 3 (i.e. RRF > 1,000) with two valves and T = 1 y requires $MTBF_{DU}^{FE}$ of at least 60 y.

Either the failure performance of the valves will need to be optimised, or β will need to be reduced below 10%, or else the inspection and test interval will need to be shortened to less than a year.