THE 61508 ASSOCIATION
Guidance in Compliance

The MooN Safety Function Failure Probability Model

$$PFD_{\mathrm{MooN}\ AVG} \approx \binom{\mathrm{N}}{\mathrm{N-M+1}}.\left(\left(1-\beta_D\right).\lambda_{DD}.MTTR + \left(1-\beta\right).\frac{(\lambda_{DU}-\lambda_{DN}).T_1}{2} + \left(1-\beta\right).\frac{\lambda_{DN}.T_2}{2}\right)^{\mathrm{N-M+1}}$$

$$+\,\beta_D.\lambda_{DD}.MTTR \,+\, \beta.\frac{(\lambda_{DU}-\lambda_{DN}).T_1}{2} + \beta.\frac{\lambda_{DN}.T_2}{2}$$

$$\approx \frac{2}{3}.\,\beta_{\mathrm{MooN}}.\lambda_{DU}.T_1$$

SYSTEMS

I&E Systems Pty Ltd

ACN 069 813 958

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.

Introduction

MoonSIF Spreadsheet Workbook

The purpose of this document is to explain the failure probability model used in the **'MoonSIF'** spreadsheet workbook published by I&E Systems Pty Ltd in conjunction with The 61508 Association (T6A). **The model extends the equations described in IEC 61508-6 into generalised 'MooN' forms**.

The workbook can be used to evaluate whether safety functions comply with the chosen standards (such as IEC 61511, IEC 61508, or IEC 62061) and to estimate the probability of failure that safety functions might achieve.

Each distinct type of safety function is modelled on a separate worksheet within the spreadsheet workbook. The safety function worksheet has a section for each of the subsystems that make up the safety function: the sensor, logic solver and final element subsystems.

The evaluation of each subsystem includes:

- Evidence that selected equipment is suitable for use in a safety function.
- Reference to reliability data sources.
- Reference to failure mode and effect analysis (FMEA) for each sub-system as a whole for each specific application. Each distinct type and application of a subsystem is analysed on a separate FMEA worksheet.
- Architectural constraints (using IEC 61508 route 1_H, or 2_H or the IEC 61511 constraints).
- Selection of test intervals and repair times.
- Failure probability estimate.
- Consideration of uncertainty.

Creative Commons Licence

The MoonSIF workbook and this document are created and licensed by I&E Systems Pty Ltd.

The work was prepared by Mirek Generowicz of I&E Systems Pty Ltd.

It was reviewed and contributed to by Ray Martin, on behalf of T6A.

CONTENTS

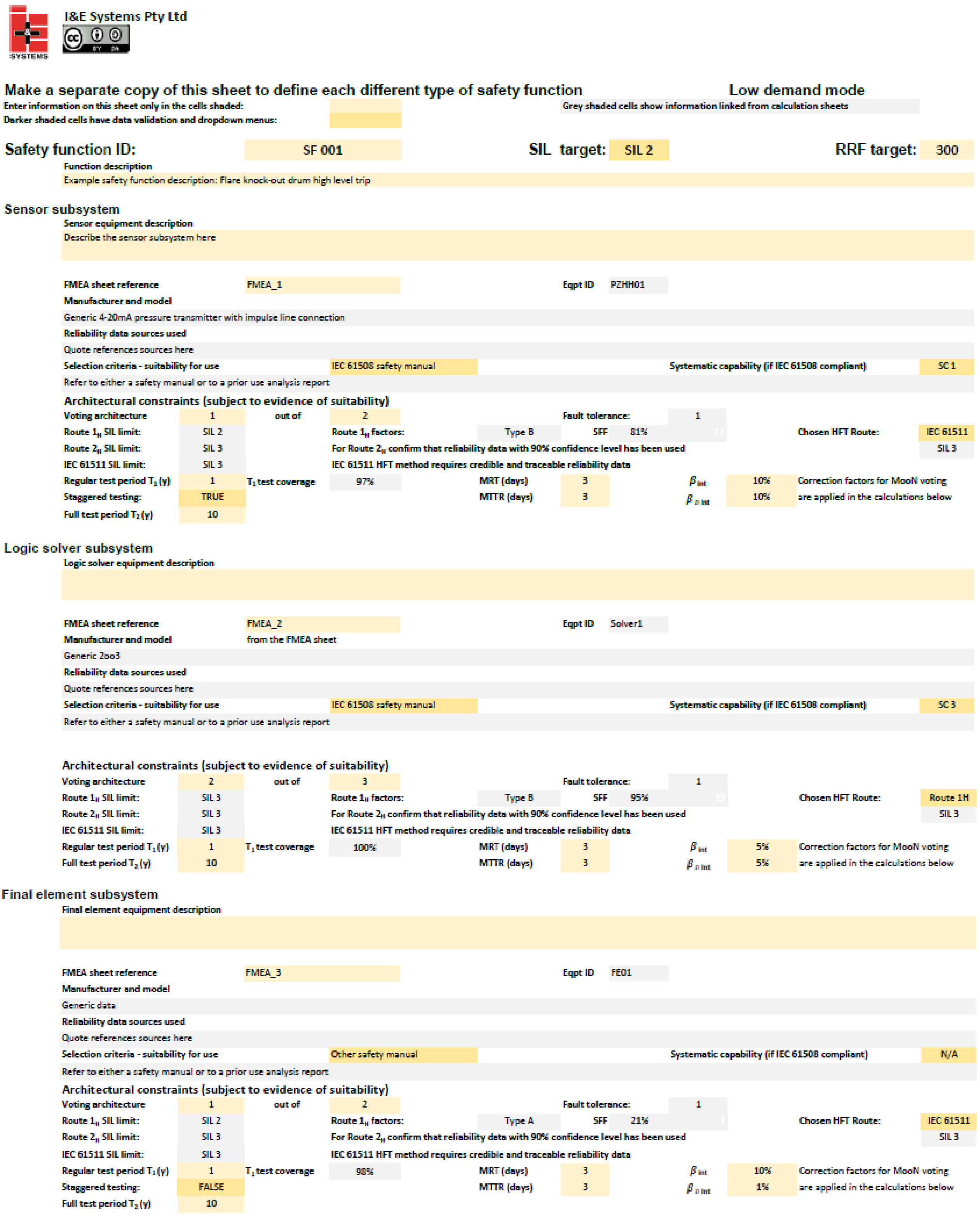
Revision notes

Revision 2 added the simplified ‘corrected average before product’ model for MooN low-demand mode with synchronised testing. The model uses a correction factor derived from the cross-products in the fully expanded model.

Revision 3 added explanation and justification for the assumptions made in the simplified ‘average before product’ models for staggered testing and synchronised testing (based on $(PFD_{1oo1\ AVG})^{\mathrm{N-M+1}}$). Explanation and justification were also added for simple approximations (based on $\frac{2}{3}.\ \beta_{\mathrm{MooN}}.\lambda_{DU}.T_1$). The sections on constant failure rate assumption, and on precision and uncertainty were moved into the introduction. The hyperlink address to the MoonSIF spreadsheet was updated in revision 3.1.

MoonSIF workbook

Example safety function evaluation worksheet input section



I&E Systems Pty Ltd

Make a separate copy of this sheet to define each different type of safety function			**Low demand mode**	
Enter information on this sheet only in the cells shaded:			Grey shaded cells show information linked from calculation sheets	
Darker shaded cells have data validation and dropdown menus:				
Safety function ID:	SF 001	**SIL target:** SIL 2	**RRF target:**	300

Function description
Example safety function description: Flare knock-out drum high level trip

Sensor subsystem

Sensor equipment description
Describe the sensor subsystem here

FMEA sheet reference	FMEA_1		Eqpt ID	PZHH01
Manufacturer and model				
Generic 4-20mA pressure transmitter with impulse line connection				
Reliability data sources used				
Quote references sources here				
Selection criteria - suitability for use	IEC 61508 safety manual		Systematic capability (if IEC 61508 compliant)	SC 1
Refer to either a safety manual or to a prior use analysis report				

Architectural constraints (subject to evidence of suitability)

Voting architecture	1	out of	2			Fault tolerance:	1		
Route 1_H SIL limit:	SIL 2		Route 1_H factors:	Type B	SFF	81%	12	Chosen HFT Route:	IEC 61511
Route 2_H SIL limit:	SIL 3		For Route 2_H confirm that reliability data with 90% confidence level has been used						SIL 3
IEC 61511 SIL limit:	SIL 3		IEC 61511 HFT method requires credible and traceable reliability data						
Regular test period T_1 (y)	1	T_1 test coverage	97%	MRT (days)	3	β_{int}	10%	Correction factors for MooN voting	
Staggered testing:	TRUE			MTTR (days)	3	$\beta_{D\,int}$	10%	are applied in the calculations below	
Full test period T_2 (y)	10								

Logic solver subsystem

Logic solver equipment description

FMEA sheet reference	FMEA_2		Eqpt ID	Solver1
Manufacturer and model	from the FMEA sheet			
Generic 2oo3				
Reliability data sources used				
Quote references sources here				
Selection criteria - suitability for use	IEC 61508 safety manual		Systematic capability (if IEC 61508 compliant)	SC 3
Refer to either a safety manual or to a prior use analysis report				

Architectural constraints (subject to evidence of suitability)

Voting architecture	2	out of	3			Fault tolerance:	1		
Route 1_H SIL limit:	SIL 3		Route 1_H factors:	Type B	SFF	95%	13	Chosen HFT Route:	Route 1H
Route 2_H SIL limit:	SIL 3		For Route 2_H confirm that reliability data with 90% confidence level has been used						SIL 3
IEC 61511 SIL limit:	SIL 3		IEC 61511 HFT method requires credible and traceable reliability data						
Regular test period T_1 (y)	1	T_1 test coverage	100%	MRT (days)	3	β_{int}	5%	Correction factors for MooN voting	
Full test period T_2 (y)	10			MTTR (days)	3	$\beta_{D\,int}$	5%	are applied in the calculations below	

Final element subsystem

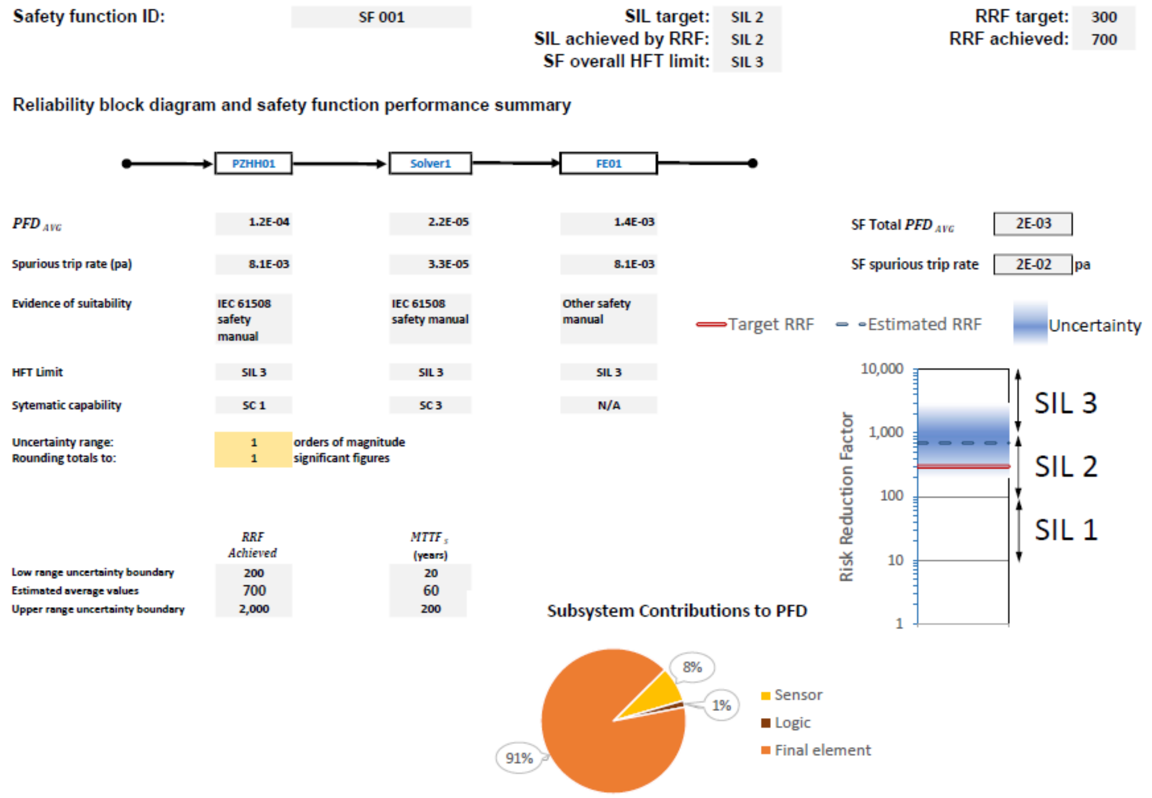
Final element equipment description

FMEA sheet reference	FMEA_3		Eqpt ID	FE01
Manufacturer and model				
Generic data				
Reliability data sources used				
Quote references sources here				
Selection criteria - suitability for use	Other safety manual		Systematic capability (if IEC 61508 compliant)	N/A
Refer to either a safety manual or to a prior use analysis report				

Architectural constraints (subject to evidence of suitability)

Voting architecture	1	out of	2			Fault tolerance:	1		
Route 1_H SIL limit:	SIL 2		Route 1_H factors:	Type A	SFF	21%	1	Chosen HFT Route:	IEC 61511
Route 2_H SIL limit:	SIL 3		For Route 2_H confirm that reliability data with 90% confidence level has been used						SIL 3
IEC 61511 SIL limit:	SIL 3		IEC 61511 HFT method requires credible and traceable reliability data						
Regular test period T_1 (y)	1	T_1 test coverage	98%	MRT (days)	3	β_{int}	10%	Correction factors for MooN voting	
Staggered testing:	FALSE			MTTR (days)	3	$\beta_{D\,int}$	1%	are applied in the calculations below	
Full test period T_2 (y)	10								

Example safety function evaluation worksheet calculation results summary section



Safety function ID:	SF 001	SIL target:	SIL 2
		SIL achieved by RRF:	SIL 2
		SF overall HFT limit:	SIL 3
		RRF target:	300
		RRF achieved:	700

Reliability block diagram and safety function performance summary

	PZHH01	Solver1	FE01
PFD $_{AVG}$	1.2E-04	2.2E-05	1.4E-03
Spurious trip rate (pa)	8.1E-03	3.3E-05	8.1E-03
Evidence of suitability	IEC 61508 safety manual	IEC 61508 safety manual	Other safety manual
HFT Limit	SIL 3	SIL 3	SIL 3
Sytematic capability	SC 1	SC 3	N/A

SF Total *PFD* $_{AVG}$	2E-03	
SF spurious trip rate	2E-02	pa

Uncertainty range:	1	orders of magnitude
Rounding totals to:	1	significant figures

	RRF Achieved	*MTTF* $_S$ (years)
Low range uncertainty boundary	200	20
Estimated average values	700	60
Upper range uncertainty boundary	2,000	200

MoonSIF probability models

The MoonSIF workbook includes separate worksheets for these 3 different modes of safety function:

- Low-demand mode
- High-demand mode
- Continuous mode

The MoonSIF models are based on the reliability block diagram method described in IEC 61508-6.

IEC 61508-6 provides equations to estimate the overall failure rate or the overall probability of failure on demand for the commonly used safety function architectures 1oo1, 1oo2, 1oo3 and 2oo3.

MoonSIF extends the IEC 61508-6 method to include the effect of staggered test intervals as well as the effect of partial coverage in routine periodic testing and inspection.

The MoonSIF spreadsheet uses generalised equations that can be applied for any ‘MooN’ voting architecture with N up to and including 7.

In this context, MooN voting describes an architecture in which M out of N separate channels need to function successfully for a safety function to complete its safety action successfully.

The architecture will tolerate N-M faulty channels. It will fail if N-M+1 channels have failed.

The low-demand mode worksheet implements two different versions of the MooN *PFD* model. The first model is based on unsynchronised testing. It assumes that each of the N channels is tested at different times, at evenly staggered intervals. The second model is based on synchronised testing, assuming that all N channels are tested at the same time.

The high-demand mode and continuous mode worksheet each implement the same model for estimating the rate of dangerous failure. The difference is that credit is taken for automatic response to failure of the function in high-demand mode but not in continuous mode.

The generalised 'MooN' forms, and the addition of staggered tests and partial tests are based on these references:

Smith, D. J. '*Reliability, Maintainability and Risk*' [1]

SINTEF PDS Method Handbook [7]

Brissaud, Barros, and Bérenguer, *Probability of Failure of Safety-Critical Systems Subject to Partial Tests* [11]

Jahanian, *Generalizing PFD formulas of IEC 61508 for KooN configurations'* [12]

The 61508 Association T6A042 *Development Paper – Effects of Proof Testing* [13].

Constant failure rate assumption

The mathematical models for estimating probability of failure assume that failures are purely random (in a mathematical sense) and that failure rates remain fixed and constant over time.

This assumption can never be justified because in the real world, ***failure frequencies always vary over time***. Failures that are classed as random are inevitably subject to many systematic and environmental influences.

The resulting models are still useful because they reveal how probability of failure is related to failure rate. Failure probability will usually vary in direct proportion to variations in the overall average failure rates. The models enable failure probability to be estimated with sufficient precision to confirm whether a safety function will be capable of meeting its target for safety integrity.

All estimates of safety function performance should start with failure modes and effect analysis. The effect of each failure mode depends on the specific context for each safety function.

The failures rates assumed in the estimates should be plausible and achievable. They should be based on failure performance that has been demonstrated in a similar environment.

The actual performance of any safety function will depend on whether the operations and maintenance team can achieve and maintain similar failure rates.

Precision and uncertainty

IEC 61511 §11.9.4 requires that '***the reliability data uncertainties shall be assessed and taken into account when calculating the failure measure***.'

All failure rates vary over a range of at least one order of magnitude (i.e. a factor of >10). Mathematical models can only predict probability of failure of safety functions to within an order of magnitude. Refer to Smith, D. J. [1], to OREDA [2] and [3], and to IEC 61709 for evidence of variation.

The actual performance in practice could be at least 3 times worse or 3 times better.

A performance margin of x 3 in the design of a safety function should be enough to allow for the typical uncertainty (or variation) expected in equipment performance and in maintenance effectiveness.

For example, a safety function that is estimated to achieve $RRF \approx$ 100 would not provide any margin for a target of $RRF \approx$ 100. A safety function that achieves $RRF \approx$ 300 would have a sufficient margin to ensure that the residual risk is likely to be below the tolerable risk target.

Calculation results should be presented with realistic precision. The range of expected variation should be clearly stated.

For example, the result of an estimate might be $PFD_{AVG} \approx \quad 1.5 \text{ x } 10^{-2}$

It is reasonable to work the with 2 significant figures during the calculation, but it is more appropriate to round final results to **1 significant figure.**

The example 1.5 x 10^{-2} could be rounded up and expressed as $PFD_{AVG} \approx$ 2 x 10^{-2}, with variation expected to be at least in a range from about 5 x 10^{-3} to 5 x 10^{-2}. In this example the expected minimum limits of variation were calculated as 0.3 x 1.5 x 10^{-2} and 3 x 1.5 x 10^{-2}.

The same result could also be presented as a risk reduction factor (RRF). It would then be appropriate to express it as $RRF \approx 70$ with an expected range of variation between 20 and 200.

Results presented with 2 or 3 significant figures would be misleading. That level of precision is not consistent with the level of variability an uncertainty in the failure rates.

Settings are provided on the MoonSIF worksheet to allow the selection of the number of figures of precision and the declared uncertainty interval.

The default precision settings are for 2 significant figures within the calculations and 1 significant figure in the overall results.

The default uncertainty interval has a span of 1 order of magnitude.

Simple approximations

The MoonSIF spreadsheet implements detailed models that are explained in this document.

However, manual calculations using simple approximations are usually sufficiently accurate. Detailed models are not necessarily any more accurate. Calculation accuracy is limited by the wide uncertainty intervals in failure rates and in common cause failure fractions.

A series of trials using the detailed models revealed that the following simple approximations can be used for most applications. The trials revealed the limits within which the approximations are valid. Refer to the section 'Validation of the simple approximations' below for a summary of the trials.

Simple approximations for low-demand mode

The basic MooN approximation is derived from the observation that usually at least about 75% of the total PFD_{AVG} of a subsystem with MooN architecture results from undetected dangerous failures. If that is valid, then:

$$PFD_{AVG} \approx \frac{4}{3} . \frac{\beta_{\text{MooN}} . \lambda_{DU} . T_1}{2} \approx \boldsymbol{\frac{2}{3} . \beta_{\text{MooN}} . \lambda_{DU} . T_1}$$

β_{MooN} is the common cause failure factor scaled for the chosen MooN voting architecture. For a first approximation assume $\beta_{\text{MooN}} = 0.1$ for 1oo2 architecture and $\beta_{\text{MooN}} = 0.15$ for 2oo3 architecture. Common cause failures and β factors are explained in detail below.

Undetected dangerous failures usually contribute > 90% of the total PFD_{AVG} in NooN architectures. That leads to a basic approximation that can be applied for any NooN architectures:

$$PFD_{AVG} \approx \boldsymbol{\frac{N}{2} . \lambda_{DU} . T_1}$$

There are four limiting cases in which these two basic approximations need to be modified:

1. **Dangerous failure rate λ_D > 0.05 pa and zero diagnostic coverage in MooN architectures**

   The basic approximation is still useful but will err on the low side. For example, the PFD_{AVG} in MooN architectures will be about 15% higher than the simple approximation if $\beta = 0.1$ and $\lambda_{DU} \approx 0.1$ pa (i.e. $\lambda_{DU} \approx$ 10,000 FITS or 1×10^{-5} h^{-1}, which corresponds with $MTTF_{DU} \approx 10$ years).

   The error may be as much as 30% on the low side with λ_{DU} > 0.05 pa in 2oo3 or 3oo4 architectures. The MooN approximation could be modified to $\approx \beta_{\text{MooN}} . \lambda_{DU} . T_1$ for a more conservative estimate, but it may be feasible to achieve λ_{DU} < 0.05 pa by adding diagnostics.

2. **Diagnostic coverage > 95%**

The contribution to PFD_{AVG} from detected dangerous failures becomes significant with diagnostic coverage >95%. The approximations should then be modified to:

For MooN: $PFD_{AVG} \approx \beta_D . \lambda_{DD} . MTTR \ + \ \beta . \frac{\lambda_{DU} . T_1}{2}$

For NooN: $PFD_{AVG} \approx \mathrm{N} . \lambda_{DD} . MTTR \ + \ \mathrm{N} . \frac{\lambda_{DU} . T_1}{2}$

3. **Proof test coverage < 95%**

Proof test coverage (PTC) is the fraction of faults detected by routine inspection and proof test at an average interval T_1. The remaining fraction of faults (1 - PTC) remains undetected until revealed by failure of the function on demand, or by full inspection and test. The average interval T_2 can be either the demand interval or the interval between tests with full coverage.

The approximations should then use $(PTC . T_1 + (1 - PTC) . T_2)$ instead of T_1:

$$PFD_{AVG} \approx \frac{2}{3} . \ \beta_{\mathrm{MooN}} . \lambda_{DU} . \left(PTC . T_1 + (1 - PTC) . T_2\right)$$

$$PFD_{AVG} \approx \frac{\mathrm{N}}{2} . \lambda_{DU} . \left(PTC . T_1 + (1 - PTC) . T_2\right)$$

4. **Common cause failure fraction β < 0.05**

The simple approximations for MooN are not valid if β < 0.05. Achieving β lower than 0.05 is likely to require complete diversity in devices between the N channels. Detailed FMEA would be necessary to justify such a low value of β, and detailed failure probability calculations would be appropriate.

Simple approximation for high-demand or continuous mode

The overall average dangerous failure rate $\lambda_D^{\mathrm{MooN}}$ in MooN architectures for high-demand mode and continuous mode safety functions can be approximated as:

$$\lambda_D^{\mathrm{MooN}} \approx \beta_D . \lambda_{DD} + \beta . \lambda_{DU} \approx \beta . \lambda_D$$

The rate of *detected* dangerous failures λ_{DD} may be excluded from this equation in a high-demand mode function ***if*** the function will put equipment into a safe state as an automatic reaction in response to detected faults. A continuous mode safety function cannot be assumed to include a fault reaction that works on demand in response to detected faults. An automatic fault response would usually need to be distinguished as a separate demand-mode safety function.

Note that IEC 61508 uses the term ‘probability of failure per hour’ (PFH) in place of failure rate λ_D. The term ‘probability of failure per hour’ may be mathematically correct, but it is avoided here to prevent confusion. Probability is dimensionless and ≤ 1. Failure rates are expressed as failures per unit time (not necessarily per hour) and are not constrained to ≤ 1. For example, a failure rate of 10^{-6} per hour can also be expressed as 1000 FITS, or 1000 failures per 10^9 hours.

Failure modes and failure rates

Failure modes

If we were to investigate every failure of every device, we would distinguish many different modes of failure and many different causes of failure. Different failure modes occur with different frequencies. Device failures can be caused by many different failure modes of many different components within a device. Refer to IEC 60812 for guidance on how to distinguish failure modes.

Failure performance will vary between different versions, models, or types of devices. Failure performance will vary depending on environmental factors and systematic factors.

ISO 14224 gives guidance on how to identify device types in failure rate analysis and how to investigate and identify the failures modes and failure causes. Every failure of every device in safety-related service must be investigated.

The primary concerns are:

- What is the effect of the failure?
- What causes led to the failure?
- Is the observed failure rate acceptable?
- Can similar failures be prevented if necessary?

If the failure rate is higher than acceptable for the target integrity level, then the failure rate might be improved through reliability-centered maintenance, or by selecting devices with a more suitable design.

There are many different types of failure. Failures are classed as safe if they result in a safer state. They are classed as dangerous if they increase the risk of a hazard. Some failures might have no effect on safety performance at all.

Failures might be complete and sudden, or they may be progressive and may result in degraded performance.

Degraded failure might involve an increased response time or a reduction in accuracy. A degraded failure would be classified as dangerous if it increases the risk of a hazard occurring.

Obviously, different types of failure will occur with different frequencies. With safety function devices we are concerned with the overall effect on the safety function and the overall average rates of failures that have the same effect. We categorise failure modes and failure rates by the effect on the function and by whether the failure can be detected by continuous diagnostic functions or by periodic inspection and testing.

Failure measures are distinguished using subscripts to indicate whether the failures are dangerous or safe and whether the failures are detected by diagnostic functions or remain undetected until periodic inspection and testing. The Greek letter λ is used here to represent failure rate.

λ_D The rate of dangerous failures, i.e. failures that increase the probability of a hazardous event.

λ_S The rate of safe failures, i.e. failures that increase the probability of spurious operation of a safety function, resulting in a safer state.

λ_{DD} The rate of detected dangerous failures, detectable by diagnostic functions.

λ_{DU} The rate of undetected dangerous failures, remaining undetected until they are revealed by inspection and testing or revealed when function failure causes a hazard to develop.

λ_{DN} The rate of dangerous failures that are not detected by *routine* periodic inspection and testing (at time intervals T_1). They are only revealed when function failure causes a hazard to develop, or when the device is taken out of service for full overhaul or renewal, or when the device can be subject to occasional testing and inspection with perfect coverage.

λ_{SD} The rate of detected safe failures which can be remedied without causing a spurious trip.

λ_{SU} The rate of undetected safe failures, failures that increase the likelihood of a spurious trip.

λ_{NE} The rate of failures that have no effect on a safety function at all. These failures are irrelevant and are not considered in any functional safety calculations.

The effect of a failure depends on the success criteria for a safety function

The specific application must always be considered when determining whether failures are safe or dangerous, and how failures might be detected.

Different applications may have different versions of the failure mode analysis. The same failures of the same type of device may have different effects in different applications.

For example:

- An unexpected reduction in liquid density might cause a level transmitter to indicate a level that is lower than the actual level in a tank. That would be a safe failure if the safety function is intended to respond to a low level. It would be a dangerous failure if the function is to act on a high level. This type of failure might be detected through a separate density measurement.
- An inductive proximity sensor might be used to measure speed of rotation on a turbine by counting pulses from flywheel teeth. Loss of signal from the sensor would be a safe failure in the case of a low-speed trip but might be a dangerous failure for a high-speed trip. This type of failure could be detected through a plausibility check (the machine is running, but the train of pulses suddenly stops rather than decelerating gradually).

Failure rate data

Ideally the failure rates that are used in the calculations should be measured in the target application and in the target environment. ISO 14224 provides guidance on how to classify and measure failure rates.

It is important to understand that all failure rates vary over at least an order of magnitude depending on environmental and systematic factors.

Systematic influences apply not only in the design and manufacture of devices, but also in the design, installation, operation and maintenance of complete systems.

IEC 61709 describes a model to account for the effect of stress factors on the reliability of electronic components. Even the rates of purely random failures should be expected to vary over at least one order of magnitude unless environmental factors can be tightly controlled.

For example: a failure rate might be estimated to be around 0.003 pa, corresponding to $MTBF$ of approximately 300 y (the $MTBF$ is rounded from 333 y, because only one significant figure of precision is appropriate). The failure rate could be expected to vary in the range from 0.001 pa to 0.01 pa. The corresponding $MTBF$ would vary from around 100 y to 1,000 y.

Performance in achieving failure rates depends on:

- Eliminating systematic failures throughout the design, development and implementation process and throughout operation and maintenance
- Maintaining a reasonably stable environment and operating devices within their specified environmental limits
- Designing the equipment to allow timely access for inspection, testing and maintenance
- Risk based inspection and condition-based maintenance
- Root cause analysis of all failures and active prevention of common cause failures.

There are several useful references that report failure rates that can be typically achieved in industrial applications. The reported ranges of failure rates are consistent across these references, given that variation should be expected to span at least an order of magnitude.

- SINTEF Reliability Prediction Method for Safety Instrumented Systems PDS Data Handbook. 2021
- *exida* Safety Equipment Reliability Handbook ('SERH'), 3rd Ed. 2007
- *exida* Safety Equipment Reliability Handbook ('SERH'), 4th Ed. 2015
- OREDA 'Offshore Reliability Data Handbook' Volume 1, 5th Ed. SINTEF. 2009
- OREDA 'Offshore and Onshore Reliability Data Handbook' Volume 1, 6th Ed. SINTEF. 2015
- ISO 13849 Safety of machinery — Safety-related parts of control systems
- Smith, D. J. 'Reliability, Maintainability and Risk', 10th Ed. Butterworth Heinemann. 2021
- silsafedata.com

Failure rates of composite sub-systems and devices can be estimated to within an order of magnitude using FMEA. Refer to IEC 60812 for guidance on FMEA procedures.

Fault tolerance

Fault tolerant safety function architectures are used in functional safety to reduce the probability of failure for those failures that cannot reasonably be prevented.

If the events A and B are **completely independent** and have the probability of occurrence $P(A)$ and $P(B)$, then we can estimate the probability of both events occurring concurrently as the product of the two individual probabilities:

$$P(A \cap B) = P(A)\,.\,P(B)$$

Common cause failures

In the real world it can be difficult to make safety function channels completely independent. The equipment in different channels of a fault tolerant architecture might be of the same type, the same age, the same material, the same condition. It might be maintained, inspected, and tested by the same person. The equipment might be operated in the same environmental conditions and at about the same time.

We cannot simply multiply the probabilities of failure together as $P(A) \,.\, P(B)$ because **a significant proportion of failures will have a common cause.**

Common cause failures can only be eliminated if we use devices that are completely diverse:

- Different designs,
- Different types,
- Different principles of operation,
- Different operators,
- Different maintainers,
- Different inspectors.

The proportion of common cause failure can be estimated from FMEA or from heuristic models.

IEC 61508 part 6 and IEC 62061 include heuristic methods for estimating the fraction of failures that can be expected to have a common cause. The symbol β (Greek letter beta) is used to represent the common cause failure fraction.

If devices are not completely diverse, we can expect the proportion of common cause failures to be in the range 0.03 to 0.3. A common cause fraction of 0.1 is typical in functional safety applications. The IEC 61508 method suggests that it will usually be difficult to achieve β better than 0.1.

SINTEF reviewed the proportion of common cause failures reported in operational experience with safety functions and concluded that β is typically in the range 0.12 to 0.15. Refer to the SINTEF paper A26922 '*Common Cause Failures in Safety Instrumented Systems; Beta-factors and equipment specific checklists based on operational experience.* ' (2015)

The SINTEF PDS Method Handbook has useful guidance about common cause failures. The PDS method assumes that common cause failures occur at a predictable fixed rate that can be characterised as a fraction of an overall failure rate.

β factor models are all based on subjective analysis of many factors, all of which are systematic rather than random.

IEC 61508-4 defines systematic failure as '*failure, related in a deterministic way to a **certain cause**, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors*'. Common cause failures are all at least partially systematic by this definition. They cannot be characterised by any fixed failure rate.

Common cause failures result from environmental influences (such as temperature, vibration, corrosion, radiation, interference etc), or from human action or inaction (such as ineffective installation or maintenance practices).

All common cause failures have causes that can be remedied to some extent, though they cannot usually be eliminated. We choose to model them with fixed rates as if they were random, but that is a coarse assumption. The actual failure rates achieved in operation will vary over at least a range 10:1.

Common cause failure susceptibility in M out of N architectures

The IEC 61508-6 and SINTEF PDS methods for estimating common cause failure factor β is based on 1oo2 architecture. The β factor must be modified for other MooN voting.

IEC 61508-6 and the SINTEF PDS Method Handbook suggest scaling factors to estimate β for MooN architectures. For example, a 4 out 5 voting architecture might be selected to reduce the rate of spurious trips. At least 4 devices must work correctly to trip the function. The 4oo5 architecture can tolerate 1 faulted channel, the same as 1oo2, but 4oo5 is more likely to have 1 faulted channel because it has 2.5 times as many channels. It is more susceptible to common cause failures if the 5 channels are identical.

A 1oo5 voting architecture is less susceptible to common cause failure because only 1 out of the 5 channels needs to work correctly for successful action.

The MooN scaling factors for β vary significantly between IEC 61508-6 and the SINTEF PDS Method. IEC 61508-6 suggests a factor of 2 for 4oo5; SINTEF PDS Method suggests a factor of 3.7. Both references suggest a factor of 0.2 for 1oo5. Neither reference explains how the factors have been estimated. Refer to *Reliability, Maintainability and Risk'* [1] for a discussion on this topic.

The MoonSIF workbook includes a table of β scaling factors on the hidden 'MooN table' worksheet. The factors are based on IEC 61508-6 using the extensions proposed by Dr David J Smith [1] for higher values of M and N. The worksheet may be modified to use SINTEF PDS Method (or any other) scaling factors.

Diagnostic coverage

Diagnostic coverage describes the proportion of failures that can be detected by continuous automatic diagnostic functions. It can be applied to either dangerous or safe failures:

$$\mathrm{DC}_D = {}^{\lambda_{DD}}\!\Big/_{(\lambda_{DD} + \lambda_{DU})} \qquad \text{and} \qquad \mathrm{DC}_S = {}^{\lambda_{SD}}\!\Big/_{(\lambda_{SD} + \lambda_{SU})}$$

Diagnostic coverage is considered separately for each sub-system of a safety function.

Some devices may be supplied with internal diagnostic functions, but diagnostic coverage is determined for the sub-system as a whole. A significant proportion of failures can occur in the interfaces between devices and the equipment under control, or in the interfaces between devices such as cabling and signal processing.

Diagnostic techniques might include:

- Sensor comparison
- Signal plausibility checks
- Monitoring loop voltage/current characteristic to detect degradation in wiring impedance
- Monitoring process signal noise spectrum or time constants to detect sensor clogging
- Actuator position feedback

FMEA may be used to identify the failure modes that could be detected through diagnostics, and to estimate the coverage of proposed diagnostic functions.

The overall diagnostic coverage within a sub-system can only be estimated if all the failure modes are understood. Some sort of failure mode analysis is necessary - such as FMEA, reliability centred maintenance, or fault tree analysis.

The purpose of diagnostic coverage is to detect faults as soon as they occur so that action can be taken to prevent a hazard or to prevent a spurious trip.

Mean Time to Restoration

The mean time to restoration ($MTTR$) is the average time taken to detect and repair a failure that is detected through continuous diagnostics. On average, 50% of repairs are repaired within the $MTTR$.

A dangerous detected failure may be made safe if the $MTTR$ is shorter than the process safety time.

Process safety time

The **process safety time** is the period between when a hazardous failure occurs in the process or in the control system, and the occurrence of the hazardous consequences if escalation is not detected and prevented. Process safety time is a property of the process itself; it does not depend on how the failure is detected, nor on protective responses.

Proof test coverage

IEC 61508-6 section B.3.2.5 and ISO/TR 12489 section 14.2.4 explain how to deal with imperfect test coverage.

Periodic proof test and inspections might not be perfect. They might fail to reveal some proportion of the undetected dangerous failures in the safety function.

Some failures might not be detectable in routine testing. For instance, a high-level trip system might be designed in such a way that it cannot be fully tested. It might not be safe to operate the system right up to the trip point. The trip condition might have to be simulated. If a system cannot be fully tested, then some failures might only be revealed when the safety function eventually fails to perform in response to an actual demand.

The term ‘not-detected dangerous failures’ is used here to describe failures that are not revealed by the planned routine tests and inspections at time intervals T_1. Some references use the equivalent term ‘not detectable by the planned testing’, or the term ‘never-detected failure’. Note that the term ‘residual failure’ may also be applied, but that term is also used to describe failures that have no effect on a safety function.

The calculation method presented in IEC 61508-6 section B.3.2.5 assumes that the failures that remain undetected by normal proof testing will eventually be revealed when the safety function fails on demand. IEC 61508-6 defines T_2 as **the expected period between demands** on the safety function. The probability of failure includes a term that is proportional to the rate of faults that remain undetected and in proportion to the period T_2.

IEC 61508-6 defines **proof test coverage (*PTC*)** as the fraction of faults detected when a proof test is performed at the normal proof test interval T_1. The rate of faults that remain undetected, λ_{DN}, is then estimated as $\lambda_{DU}.(1-PTC)$.

By implication, proof test coverage may be estimated from the proportion of the dangerous undetected failures that cannot be revealed by the normal routine inspection and testing:

$$PTC \quad = \quad \frac{\lambda_{DU} - \lambda_{DN}}{\lambda_{DU}} \quad = \quad 1 - \frac{\lambda_{DN}}{\lambda_{DU}}$$

The SINTEF PDS Method Handbook section 5.3.2 and ISA-TR84.00.02 section 6.2 provide similar guidance on the effect of incomplete test coverage. These references both consider T_2 to be the **time between full tests** instead of being the expected period between demands. The assumption is that tests with complete coverage can be executed at time intervals T_2, and the complete tests will reveal all faults not detected by the partial tests at time intervals T_1.

ISO/TR 12489 uses the **mission time T_M** instead of T_2. The mission time is defined as the time in service before scheduled overhaul or replacement. The use of mission time in this context assumes that refurbishment or replacement process includes complete inspection and testing before the refurbished or replacement device is put back into service. Revalidation is assumed to be equivalent to the original validation process. This usage is effectively the same as taking T_2 to be the time between full tests, if full tests are only carried out at validation and revalidation.

The methods in IEC 61508, SINTEF PDS, ISA-TR84 and ISO/TR 12489 all assume that all failure rates are constant, and that the probability of failure increases linearly over time if they are not detected. This includes dangerous failures that are not detected by regular periodic testing. The probability of a safety function device failing on demand is assumed to increase with time until the demand occurs or until a full test reveals the failure.

The concepts of PTC and λ_{DN} may be misleading because they imply that dangerous failure rates are fixed and constant. There is no real justification for assuming that most failures would occur at some constant failure rate.

Not-detected failures are more likely to be systematic rather than purely random because they usually result from a pre-existing condition. They result from shortcomings in the design, installation, inspection, testing, operation or maintenance of equipment. They do not result from stochastic processes. The resulting failures may occur due to an unexpected combination of extremes in environmental and/or service or process conditions. Faults that lead to failure may exist before the equipment is commissioned and might not be detected during the validation process.

ISO/TR 12489 section 14.2.1.3 clarifies the variability in failure rates and warns that *'even in the simplest cases, the reliability analyst should verify that the hypothesis of constant failure rates is realistic when he/she decides to implement formulae, Boolean or Markov calculations.'* ISO/TR 12489 sections 7.2 and B.3 also provide useful clarification.

Long-term average failure frequencies are useful for estimating the average probability of failure over the whole life of the safety function. Failure rates *during operation* are not constant.

The assumption of a fixed rate λ_{DN} is a simple approximation that enables the order of magnitude of failure probability to be estimated. It cannot produce precise and dependable predictions.

The long-term average rate is estimated from the number of failures ***n*** that were eventually revealed:

- By failures on demand or
- When faults are found after a test and inspection with complete coverage, or

- When faults found after equipment is taken out of service for overhaul or replacement and/or off-site testing
- When faults found after destructive testing of samples (such as testing of rupture disks or fuses).

The average rate is ***n*** divided by the total aggregated time in service **τ** (the total time in service T_i summed for each *i* of *N* devices).

$$\lambda_{DN} \quad = \quad \frac{n}{\tau}$$

Where

$$\tau \quad = \quad \sum_{i=1}^{i=N} T_i$$

The only information about probability of not-detected failure that can be known with any certainty is that the probability ***was n***/***N*** after an overall average time in service of **τ**/***N***.

Failures do not necessarily occur at consistent and predictable rates, let alone at a constant rate.

There could have been ***n*** failures on day 1 if the failures resulted from design or installation faults. The probability of failure may have remained constant at *n*/*N* since day 1. Random hardware failure calculations are not intended to include pre-existing failures.

The SINTEF PDS Method Handbook discusses P_{TIF}, the probability of 'Test Independent Failure', failure of the function due to faults not found by testing.

Probability of not-detected failure could be modelled by setting P_{TIF} = *n*/*N.*

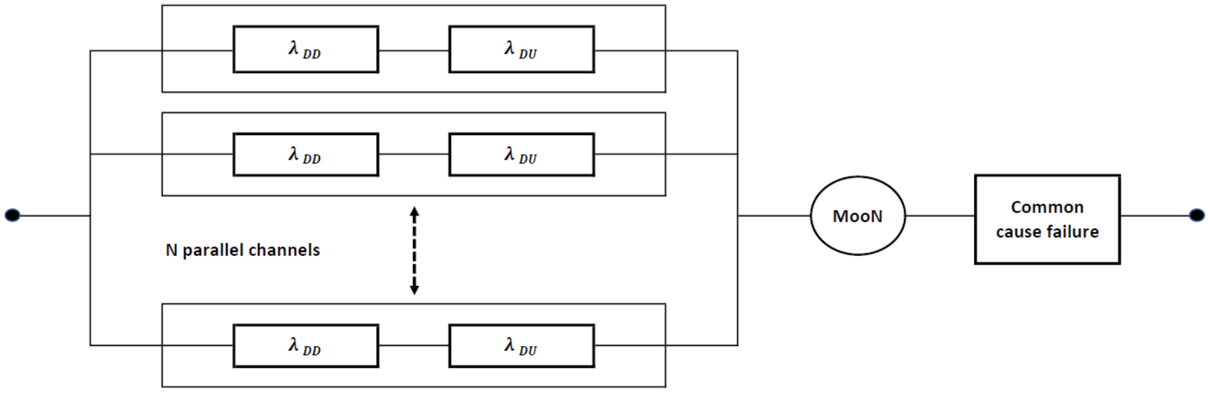
The appropriate way to deal with not-detected failures is:

- Conduct FMEA to identify all failure modes that can be expected
- Design the systems so that all failure modes can be revealed by either diagnostic tests or by periodic proof test and inspection
- Design the periodic proof test and inspection on the basis of FMEA to ensure that all undetected failures can be revealed.

MooN reliability block diagrams

The reliability block diagrams included here are based on the reliability block diagrams and methods presented in IEC 61508-6 Annex B.

Block diagram for overall failure rate of continuous mode functions and high-demand mode functions

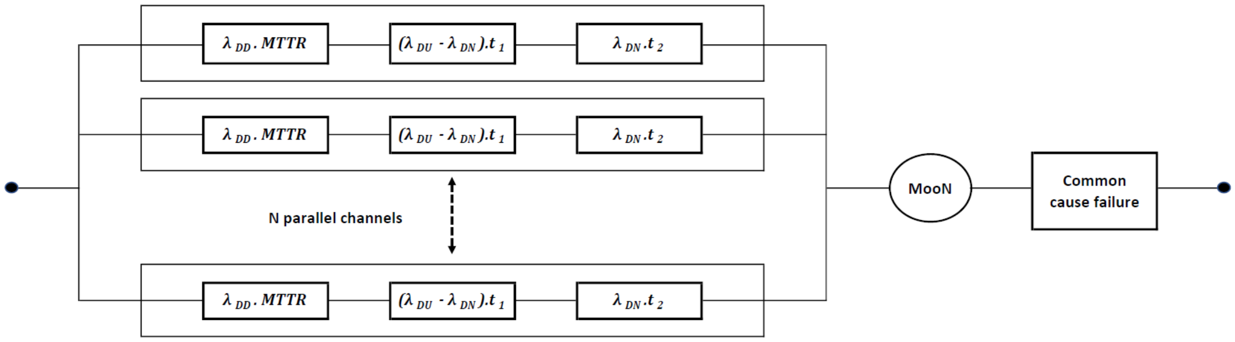


This analysis does not distinguish between λ_{DU} and λ_{DN} for continuous mode functions or high-demand mode functions. The expected period T_2 between demands on the safety function is shorter than the planned periodic inspection and testing. Both undetected and not-detected failures in a single channel architecture are revealed on demand rather than through testing if the function operates in a high-demand mode. Dangerous failures in continuous mode cause immediate loss of function, which would usually be immediately revealed.

The model can be extended to include not-detected failures in fault tolerant architectures where it is not feasible to achieve complete test coverage.

The rationale for neglecting not-detected failures in the MoonSIF spreadsheet is explained further in the analysis below.

Block diagram for probability of failure on demand



Calculation method

Fractional dead time

The MoonSIF spreadsheet failure probability models are based on the idea of **fractional dead time**: This is the proportion of the time that we can expect a safety function channel to be 'dead' due to some dangerous failure.

Failure rate for continuous mode and high-demand mode

Continuous mode safety functions are those where a dangerous failure directly causes a hazardous event, if not protected against those failures by some other independent means. They are characterised by failure rate instead of by a probability of failure on demand.

Dangerous failures in high-demand mode functions do not immediately cause a hazard, but a hazardous event can be expected to occur soon after the failure if no other action is taken. The failures are more likely to be revealed on demand rather than by inspection and testing because the demands are more frequent than the periodic inspections and tests.

The targets for high-demand functions are therefore set in terms of failure rate, in a similar way to continuous mode functions.

Detection of dangerous failures in continuous mode and high-demand mode functions

Safety function failure modes and effects need to be analysed and understood before the probability of dangerous failure can be estimated. Diagnostic functions and fault reactions need to be defined.

IEC 61508-2 §7.4.8.3 states the response required to any detected failure in a single-channel high-demand mode or continuous mode safety function as follows:

> *The detection of a dangerous fault (by diagnostic tests, proof tests or by any other means) in any subsystem having a hardware fault tolerance of 0 shall, in the case of a subsystem that is implementing any safety function(s) operating in the high-demand or the continuous mode,* ***result in a specified action to achieve or maintain a safe state****.*

The mathematical model for failure rate may need to be modified or adapted, depending on how fault detection and fault reactions are implemented.

The MoonSIF spreadsheet model allows credit to be taken for detection of dangerous failures in fault-tolerant architectures with continuous mode and high-demand mode safety functions. Fault tolerant architecture in this context refers to MooN architectures with redundant channels. If a channel fails, the function can be executed by the remaining N-1 healthy channel or channels.

The FMEA worksheets in the MoonSIF workbook record the assumptions made regarding fault detection and fault reactions.

Diagnostic functions are never perfect. Some failures will remain undetected until periodic testing and inspection, or until revealed by a failure in safety function operation.

Continuous mode and high-demand mode safety functions generally execute a continuous or frequent action that can be readily monitored. Faults can be detected as soon as they occur in redundant channel architectures by comparing the states of the channels.

Sensor faults can be detected by sensor signal comparison. Final element faults can be detected by comparing the element position or by comparing the values of the manipulated process variable in each channel.

Sensor comparison and final element comparison may be implemented as automatic continuous diagnostic functions or may be part of the periodic inspection and testing.

Any discrepancy between sensors or final elements should be treated as a dangerous fault and corrective active should be taken. The failed channel could be taken out of service and repaired if it is clear which channel has failed. Otherwise, some other action would be needed to achieve a safe state.

In some applications there may be dangerous faults that cannot be detected due to the design of the system. Some dangerous faults might not be detected during periodic inspection and testing because the comparison is neglected or ineffective due to human error.

Continuous mode – single channel

A single channel safety function architecture can be described as having ‘1 out of 1’ (1oo1) voting.

The overall rate of dangerous failures in a single-channel continuous mode safety function is simply the sum of the rates of dangerous failures in each of the subsystems that are essential for the function to work correctly:

$$\lambda_D^{SF} = \lambda_D^{sensor} + \lambda_D^{logic\ solver} + \lambda_D^{final\ element}$$

All dangerous failures in a single-channel continuous mode safety function cause the safety function to fail. The detection of a dangerous failure does not prevent failure of the safety function, though it enables corrective action to be taken (fault reaction).

Continuous mode safety functions are designed to maintain a safe state. They are not necessarily capable of putting equipment into a safe state in response to some failure.

Dangerous failures in a continuous mode safety function may result in demands on other independent safety functions and/or other protection layers to achieve a safe state.

Diagnostic functions may be implemented to put the equipment into a safe state automatically when a dangerous failure is detected in a single-channel continuous mode safety function.

Diagnostic functions may need to be classed as separate SIL-rated safety functions if:

- They act on demand in response to the hazard caused by failure of any part of a continuous mode safety function
- They execute an action through an independent final element to put the equipment into a safe state
- They are claimed to detect > 90% of the dangerous failures, so in effect they are allocated a target probability of failure on demand < 0.1

Sensors in SIL-rated diagnostic functions would need to be independent from the function being monitored.

Operator response to alarms from independent sensors could be considered as an independent protection layer. There would need to be some assurance that the operator will take appropriate remedial action ***within the process safety time***.

For example, a single-channel safety-rated speed controller may be applied on a steam turbine. Failure of the function might be caused by a fault in the speed sensor, or by a stuck control valve. The operator is not likely to have enough time to respond. An independent overspeed trip could be used to detect failure of the continuous mode function and to put the turbine into a safe state through a separate valve.

High-demand mode – single channel

Safety functions that operate in the high-demand mode have an executive action that puts the equipment into a safe state on demand.

High-demand mode safety function may be designed so that the safety action is executed when dangerous faults are detected within the sensor or logic sub-systems. The fraction of failures that can be detected can then be excluded from the overall rate of dangerous failures.

The overall rate of undetected dangerous failures in a single-channel high-demand mode safety function is then:

$$\lambda_{DU}^{SF} = \lambda_{DU}^{sensor} + \lambda_{DU}^{logic\ solver} + \lambda_{DU}^{final\ element}$$

Dangerous faults within the final element sub-system prevent the function from achieving a safe state, regardless of whether they are detected. The fault reaction for those failures would need to be implemented in a separate safety function or other protection layer.

Continuous mode – 1oo2 dual channel architecture

The overall rate of dangerous failure can be reduced by applying a fault tolerance architecture to a continuous mode safety function.

Dual channel redundant architecture can be described as having ‘1 out of 2’ voting (1oo2).

The safety function will continue to work correctly if at least 1 of the 2 channels is working as specified.

The function is described as having a hardware fault tolerance level (HFT) of 1, because one faulted channel can be tolerated without loss of function (HFT = N-M).

If we can detect which of two channels has failed, we can maintain the safe state with the remaining healthy channel.

For example, a separate trip might be necessary to achieve fault reaction in the case of a discrepancy between the sensors. A discrepancy indicates a fault in one of the sensors, but not which of the two has failed. Continued safe operation is not possible.

The mathematical model that is used for fault tolerant continuous mode safety functions depends on the fault reactions that have been chosen.

The effectiveness of the fault reaction may depend on systematic factors. A generic model cannot be used for all possible variations in fault reaction. The basis of the MoonSIF spreadsheet model is explained here. Users may need to adapt the model depending on their chosen fault detection and fault reaction strategies.

As for a single channel, the overall rate of dangerous failures in a fault-tolerant continuous mode safety function is the sum of the rates of dangerous failures in each of the subsystems that are essential for the function to work correctly:

$$\lambda_D^{SF} = \lambda_D^{sensor} + \lambda_D^{logic\ solver} + \lambda_D^{final\ element}$$

A safety function with a 1oo2 voted architecture will fail in a dangerous way if dangerous failures occur in both channels at the same time *and* if there is no immediate action to achieve a safe state within the process safety time.

Overall function failure can occur in two ways:

1. Both channels fail at a similar time for the same reason (a common cause failure)
2. One channel fails first, and the second channel fails before the first failure is detected and repaired.

Credit may be taken for detection of failures in a channel if the failed channel can be restored to service before the remaining channel fails.

The contribution to failure rate of each subsystem corresponding to **common cause failures** is:

$$\beta_D.\lambda_{DD} + \beta.\lambda_{DU}$$

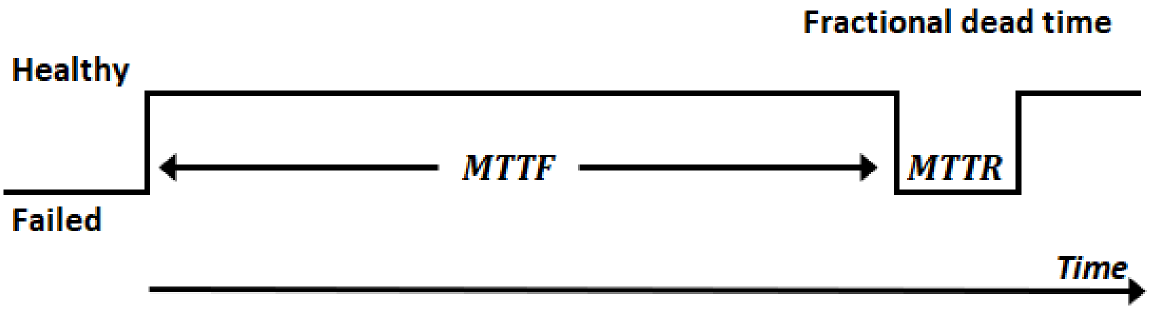
Both detected and undetected dangerous failures cause the safety function to fail in the same way as a single-channel safety function.

Common cause dangerous failures in a fault-tolerant continuous mode safety function may result in demands on other independent safety functions and/or other protection layers.

If a single sub-system channel has failed, then the remaining sub-system channel operates in a single-channel mode until the failed channel is restored to full service. Any dangerous failure of the remaining channel will result in a hazard if it occurs before the failed channel is restored. During that period the overall dangerous failure rate of the subsystem is λ_D.

The fraction of time that a channel has failed is called the ***fractional dead time***. It is equivalent to the probability that the channel is out of service.

The average fractional dead time for detected failures is the mean time to restoration, $MTTR$:



The rate at which the first detected dangerous failure occurs in either 1 of 2 channels is $2.(1-\beta_D).\lambda_{DD}$, twice the failure rate of a single device.

Common cause failures are excluded because they cause both channels to fail at the same time and are accounted for separately as explained above.

The mean time to failure $MTTF = \dfrac{1}{2.(1-\beta_D).\lambda_{DD}}$

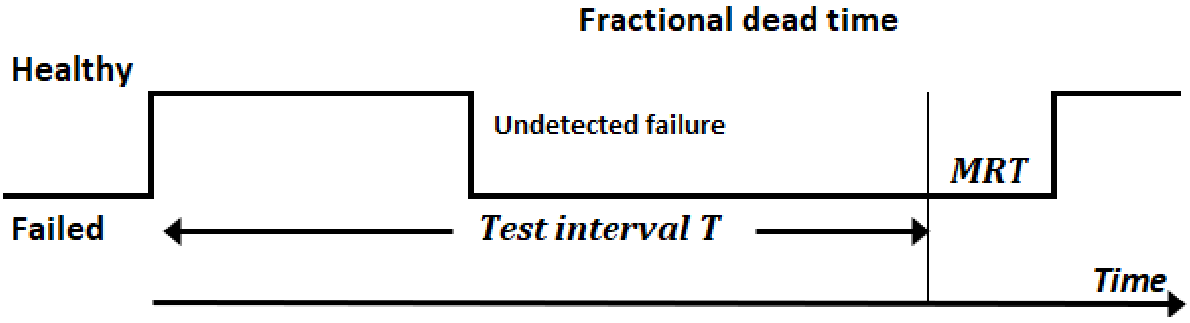
The fractional dead time is $\dfrac{MTTR}{MTTF} = 2.(1-\beta_D).\lambda_{DD}.MTTR.$

The overall failure rate of each subsystem corresponding to any dangerous failure in one channel during the dead time for a **detected dangerous failure** in in the other channel is therefore λ_D multiplied by the fractional dead time:

$$\lambda_D.\frac{MTTR}{MTTF} = \lambda_D.\ 2.(1-\beta_D).\lambda_{DD}.MTTR$$

The first failure may remain undetected until the next periodic inspection and test. In that case the average time at risk is half of the test interval Tplus the mean time to repair the channel after a failure is found, MRT.

Any dangerous failure of the remaining channel will result in a hazard if it occurs before the failed channel is restored.



The rate at which the first undetected dangerous failure occurs in either 1 of 2 channels is $2.(1-\beta).\lambda_{DU}$.

The fractional dead time is the average time to discover and repair the failure:

$$2.(1-\beta).\lambda_{DU}.(T/2+MRT)$$

The overall failure rate of each subsystem corresponding to any dangerous failure in one channel during the dead time for an **undetected dangerous failure** in in the other channel is therefore λ_D multiplied by the fractional dead time:

$$\lambda_D.\ 2.(1-\beta).\lambda_{DU}.(T/2+MRT)$$

The overall dangerous failure rate for the 1oo2 combination of each subsystem is therefore:

$$\begin{aligned}\lambda_D^{1oo2} = \ &\beta_D.\lambda_{DD} + \beta.\lambda_{DU} \\ &+ 2.\lambda_D.\big((1-\beta_D).\lambda_{DD}.MTTR\ + (1-\beta).\lambda_{DU}.(T/2+MRT)\big)\end{aligned}$$

In most applications the common cause failure terms are at least 2 orders of magnitude larger than the other terms. Typically:

$$\lambda_D^{1oo2} \approx \ \beta_D.\lambda_{DD} + \beta.\lambda_{DU}$$

High-demand mode – 1oo2 architecture

It may be possible to design high-demand mode safety functions so that the safety action is executed in reaction to detection of coincident dangerous failures in both channels. The rate of the detected failures can then be excluded from the overall for λ_D for the function. The rate of coincident dangerous failures in both channels is:

$$\lambda_D^{1oo2} = \beta.\lambda_{DU} + 2.\lambda_{DU}.\left((1-\beta_D).\lambda_{DD}.MTTR + (1-\beta).\lambda_{DU}.(T/2+MRT)\right)$$

This model is equivalent to Equation B.3.3.2.2 in IEC 61508-6.

Accounting for failures not-detected in continuous mode functions and high-demand mode functions

The MoonSIF spreadsheet model does not include **not-detected** failures in continuous mode and high-demand mode functions. These are the failures that are not detected either by diagnostics or by periodic inspection and testing. The calculation model could be extended to include not-detected failures where appropriate.

One option for modelling the effect of not-detected failures assumes the failures can be expected to occur at a fixed and predictable rate λ_{DN}, and that not-detected failures are revealed at time T_2. The term T_2 could either represent the interval between inspection and tests with full coverage, or the planned mission time.

For a 1oo2 architecture the fractional dead time could be modelled as:

$$2.((1-\beta_D).\lambda_{DD}.MTTR + (1-\beta).(\lambda_{DU}-\lambda_{DN}).(T_1/2+MRT) + (1-\beta).\lambda_{DN}.(T_2/2+MRT))$$

Another option is to model the probability of failure due to not-detected faults by adding a fixed constant P_{TIF} (for test independent failure) to the fractional dead time:

$$\lambda_D.\ P_{TIF}$$

For example, it may be known that 3 devices out of a total of 300 were found to have failed on test after having been taken out of service at the end of life. The probability of not-detected failure could be assumed to be constant over time and in the order of 0.01, rather than assuming a constant failure rate.

Common cause dangerous failures in high-demand mode functions are expected to result in a hazardous event within the time T_2, the period between demands on the safety function.

No distinction is made between undetected and not-detected common cause dangerous failures in continuous mode functions because common cause dangerous failures cause an immediate failure of the function. Common cause failures will not remain unrevealed until testing and inspection.

Continuous mode – 2oo3 architecture

A continuous mode safety function with 2oo3 architecture will continue to work correctly if at least 2 of the 3 channels is working as specified. This architecture has HFT = 1 because one faulted channel can be tolerated without loss of function.

The rate at which the first detected dangerous failure occurs in either 1 of 3 channels is $3.(1-\beta_D).\lambda_{DD}$. The fractional dead time is $3.(1-\beta_D).\lambda_{DD}.MTTR$.

The rate at which the first undetected dangerous failure occurs in either 1 of 3 channels is $3.(1-\beta).\lambda_{DU}$. The fractional dead time is $3.(1-\beta).\lambda_{DU}.(T/2+MRT)$

The function fails if either 1 of the 2 remaining channels fails dangerously during the fractional dead time. The overall dangerous failure rate for a 2oo3 subsystem therefore corresponds to the rate $2.\lambda_D$ multiplied by the fractional dead time, plus the rate of dangerous failures that have a common cause:

$$\begin{aligned}\lambda_D^{2oo3} \;=\;& \beta_D.\lambda_{DD} + \beta.\lambda_{DU}\\ &+ 6.\lambda_D.\big((1-\beta_D).\lambda_{DD}.MTTR + (1-\beta).\lambda_{DU}.(T/2+MRT)\big)\end{aligned}$$

High-demand mode – 2oo3 architecture

The rate of the detected failures could be excluded for functions that operate in a high-demand mode if the safety action is executed in response to detection of dangerous failures:

$$\begin{aligned}\lambda_D^{2oo3} \;=\;& \beta.\lambda_{DU}\\ &+ 6.\lambda_{DU}.\big((1-\beta_D).\lambda_{DD}.MTTR + (1-\beta).\lambda_{DU}.(T/2+MRT)\big)\end{aligned}$$

Continuous mode – 1oo3 voting architecture

1oo3 architecture has HFT = 2, because only 1 channel is necessary for successful performance. The architecture tolerates 2 faulted channels without loss of function.

Common cause failures are modelled as causing immediate failure of continuous mode safety functions with 1oo3 architecture, as for 1oo2.

Common cause dangerous failures cause the safety function to fail in the same way as a single-channel safety function, regardless of whether the failures are detected or undetected. Other independent safety functions and/or other protection layers may be used to put the equipment into a safe state if dangerous failure is detected.

Comparison between the 3 channels should always be possible except for common cause failures.

The MoonSIF spreadsheet model assumes that a single-channel failure in a 1oo3 system will be detected either through diagnostics or through periodic inspection and testing. The remaining two channels work in a 1oo2 arrangement after the first single-channel failure.

The fraction of time for which the system operates in a 1oo2 architecture can be modelled as:

$$3.(1-\beta_D).\lambda_{DD}.MTTR + 3.(1-\beta).\lambda_{DU}.(T/2+MRT)$$

The dangerous failure rate resulting from coincident failures affecting multiple channels is therefore:

$$= 3.\big((1-\beta_D).\lambda_{DD}.MTTR + (1-\beta).\lambda_{DU}.(T/2+MRT)\big).\lambda_D^{1oo2}$$

$$= 6.\lambda_{DU}.\big((1-\beta_D).\lambda_{DD}.MTTR + (1-\beta).\lambda_{DU}.(T/2+MRT)\big)^2$$

The common cause contribution is added to estimate the overall dangerous failure rate:

$$\lambda_D^{1oo3} = \beta_D.\lambda_{DD} + \beta.\lambda_{DU} + 6.\lambda_{DU}.\big((1-\beta_D).\lambda_{DD}.MTTR + (1-\beta).\lambda_{DU}.(T/2+MRT)\big)^2$$

High-demand mode – 1oo3 voting architecture

If the safety action is executed in response to detection of dangerous failures, then:

$$\lambda_D^{1oo3} = \beta.\,\lambda_{DU} + 6.\lambda_{DU}.\big((1-\beta_D).\lambda_{DD}.MTTR + (1-\beta).\lambda_{DU}.(T/2+MRT)\big)^2$$

This model is equivalent to Equation B.3.3.2.6 in IEC 61508-6. The IEC 61508-6 modelling includes some inconsistencies in the usage of β and β_D. IEC 61508-6 uses $T^2/3$ in the quadratic terms rather than $T^2/4$ because it assumes that tests are synchronised rather than staggered. These differences will not have any significant effect on the results.

MooN modelling for continuous mode

Other MooN voting architectures might be used in continuous mode and high-demand mode safety functions.

For example, 2oo4 might be used. The form of the equation is similar to the equation for 1oo3 architecture. This architecture also has HFT = 2, but there are 4 choices for the first failure, and then the remaining 3 channels operate in a 2oo3 mode. There are 3 choices for the second failure. Finally, there are 2 choices for 1 failure in the 2 last remaining channels.

$$\lambda_D^{2oo4} = \beta_D.\lambda_{DD} + \beta.\lambda_{DU} + 24.\lambda_{DU}.\big((1-\beta_D).\lambda_{DD}.MTTR + (1-\beta).\lambda_{DU}.(T/2+MRT)\big)^2$$

A safety function with MooN voting will fail if N-M+1 channels have failed at the same time.

There are N choices for the first failure, N-1 choices for the second failure and so on up to M choices for the final failure, which is the (N-M+1)th. The series of multipliers has (N-M+1) terms:

$$\mathrm{N}.(\mathrm{N}-1).(\mathrm{N}-2).\ [\ldots].(\mathrm{N}-(\mathrm{N}-\mathrm{M}))$$

This series product can be represented in factorial form as:

$$\frac{\mathrm{N}!}{(\mathrm{M}-1)!}$$

The general MooN model used for continuous mode in the MoonSIF spreadsheet is:

$$\lambda_D^{\mathrm{MooN}} = \beta_D.\lambda_{DD} + \beta.\lambda_{DU} + \frac{\mathrm{N}!}{(\mathrm{M}-1)!}.\lambda_{DU}.\big((1-\beta_D).\lambda_{DD}.MTTR + (1-\beta).\lambda_{DU}.(T/2+MRT)\big)^{\mathrm{N-M}}$$

MooN modelling for high-demand mode

The rate of the detected failures can be excluded from the overall for λ_D for high-demand mode functions, if it can be established that the safety action is executed in response to detection of dangerous failures.

$$\lambda_D^{\mathrm{MooN}} = \beta.\lambda_{DU} + \frac{\mathrm{N}!}{(\mathrm{M}-1)!}.\lambda_{DU}.\big((1-\beta_D).\lambda_{DD}.MTTR + (1-\beta).\lambda_{DU}.(T/2+MRT)\big)^{\mathrm{N-M}}$$

Common cause failures will usually dominate

The overall failure rate will usually be dominated by common cause failures.

For example, a braking system on a mineshaft winder drum acts as the final element in a high-demand mode safety function. In this hypothetical example the safety function depends on the application of at least 4 out of 7 brake disc callipers. The function will fail if more than 3 callipers have failed, but that is likely only if the failures have a common cause. The common cause failure term will be the most significant factor. Pressure sensors are fitted to each calliper. Calliper failure can be detected through the pressure signal and/or through daily inspection.

The term raised to the power N-M is usually purely academic. It has no significance because it is always some orders of magnitude smaller than the uncertainty in the component failure rates (and therefore smaller than the uncertainty in the common cause failure terms).

For example, the failure rates λ_D and λ_{DU} are typically in the order of 0.01 pa. $MTTR$ is typically in the order of 0.01 year, and T is typically in the order of 1 year at most. The fault tolerance in a system relying on 4 out of 7 callipers is 7-4 = 3.

$$\frac{\mathrm{N}!}{(\mathrm{M}-1)!}.\lambda_{DU}.\big((1-\beta_D).\lambda_{DD}.MTTR + (1-\beta).\lambda_{DU}.(T/2+MRT)\big)^{\mathrm{N-M}}$$

$$\approx 840.\lambda_{DU}.\big(\lambda_{DD}.MTTR + \lambda_{DU}.(T/2)\big)^3$$

$$\approx 840.10^{-2}.\big(10^{-2}.10^{-2} + 10^{-2}.(1/2)\big)^3$$

$$\approx 10^{-6} \text{ pa}$$

In contrast, the common cause failure terms $\beta_D.\lambda_{DD} + \beta.\lambda_{DU}$ can be expected to be in the order of 10^{-3} pa.

In this 4oo7 example β_{MooN} would be expected to be ≈0.2, so:

$$\beta_D.\lambda_{DD} + \beta.\lambda_{DU} \approx 2.10^{-1}.10^{-2} + 2.10^{-1}.10^{-2} \text{ pa}$$

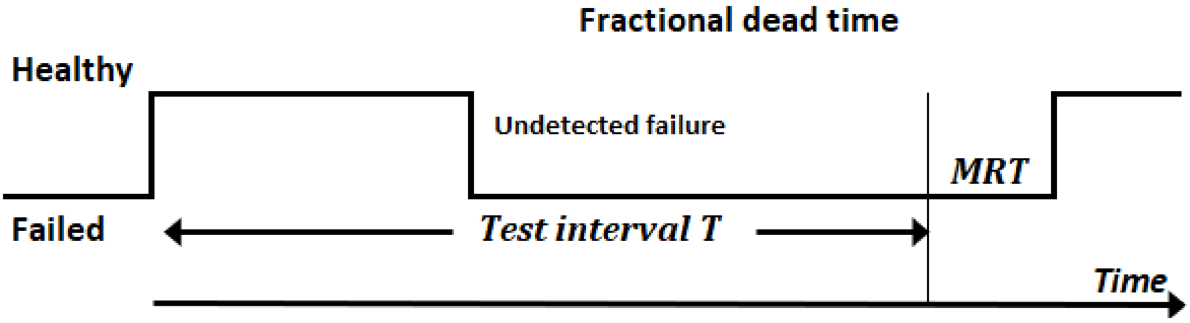
$$\approx 4.10^{-3} \text{ pa}$$

Typically: $\lambda_D^{\mathrm{MooN}} \approx \beta_D.\lambda_{DD} + \beta.\lambda_{DU}$

PFD for low-demand mode single channel architecture

For low-demand mode safety functions (demand rates less frequent than once per year) the target is set in terms of the average probability of failure on demand, PFD_{AVG}.

Again, the probability of failure is estimated using the **fractional dead time**:

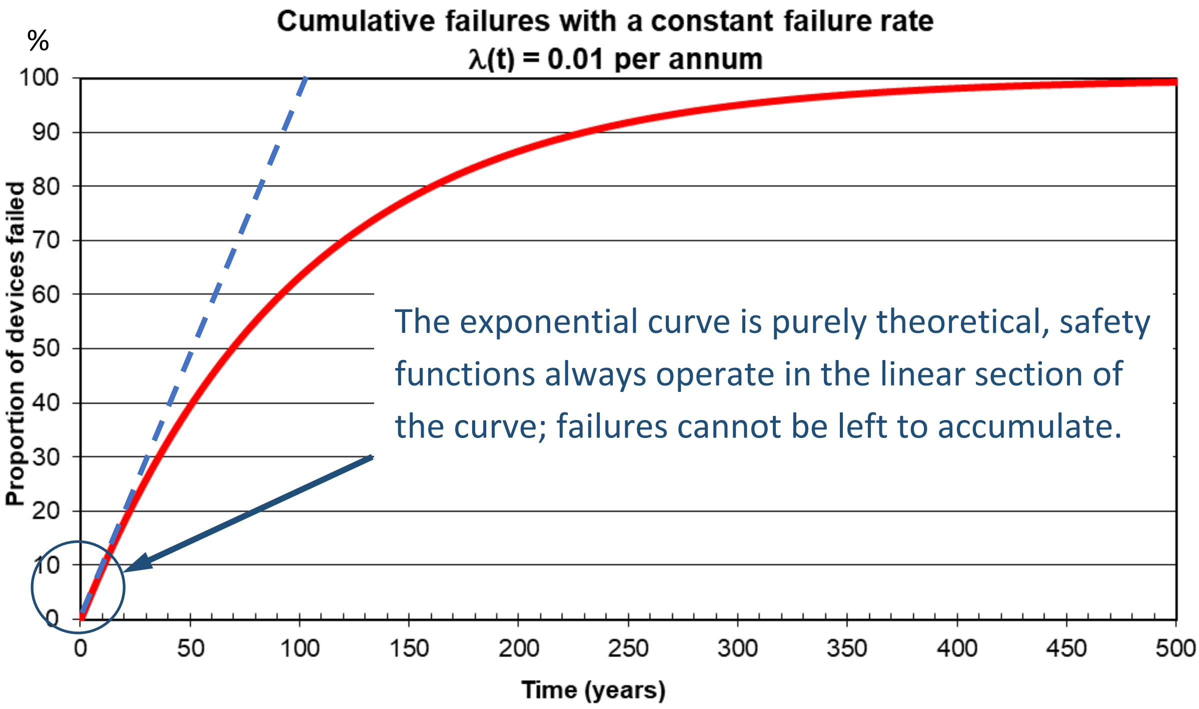


The time T represents the time interval between routine periodic inspection and testing.

The channel down time might be anywhere between 0 and T plus the MRT. The average down time is $T/2 + MRT$.

Single channel *PFD* due to undetected failures

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



The exponential curve is purely theoretical, safety functions always operate in the linear section of the curve; failures cannot be left to accumulate.

By definition, safety functions are designed to achieve $PFD_{AVG} < 0.1$, so failures cannot be left to accumulate beyond 0.1 in any SIL-rated safety functions.

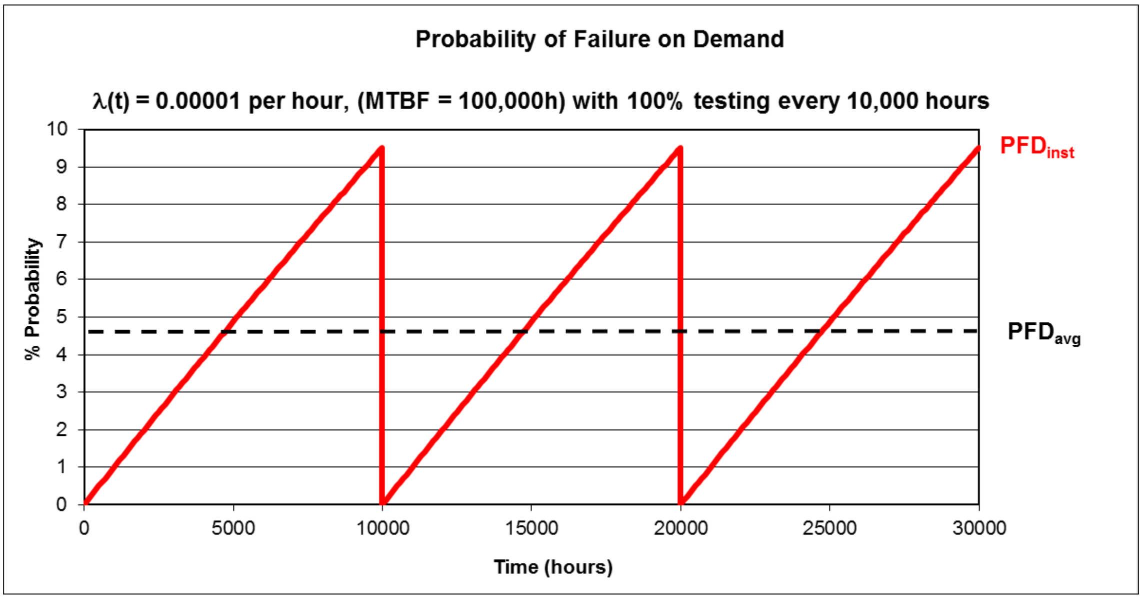
Safety functions always operate in the linear region of the exponential curve where $t << MTBF_{DU}$, where t is the time elapsed since the last full test and $MTBF_{DU}$ is the mean time between undetected dangerous failures in the safety function.

A straight-line approximation can be used instead of an exponential characteristic. The proportion of failed devices at time t in any population can be estimated as $\approx \lambda_{DU}.t$.

If the undetected failure rate (λ_{DU}) is reasonably constant, the number of accumulated failures is proportional to the elapsed time and the rate of undetected failures.

The probability that any one device has failed is proportional to the total number of failed devices 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_1.



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

$$PFD_{AVG} = \frac{1}{T_1}\int_0^{T_1} \lambda_{DU}\,(t).\,dt$$

Safety functions typically have $MTBF_{DU} >$ 30 years and test interval T_1 = 1 year.

If the rate remains constant and $T_1 << MTBF_{DU}$ we can use the approximation $\lambda_{DU}(t) \approx \lambda_{\mathrm{DU}}.t$

$$PFD_{AVG} \approx \frac{1}{T_1}\int_0^{T_1} \lambda_{DU}\,.\,t.\,dt$$

$$\approx \frac{1}{T_1}.\frac{\lambda_{DU}{T_1}^2}{2}$$

$$\approx \frac{\lambda_{DU}.T_1}{2}$$

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_1. The MRT is usually measured in hours or days, much shorter than T_1, which is measured in years in low-demand mode applications. For example, typically T_1 = 1 year and MRT = 3 days (about 0.01 year). Test intervals are not usually precisely controlled. Annual test intervals might vary by a month or more, so the addition of MRT is not meaningful.

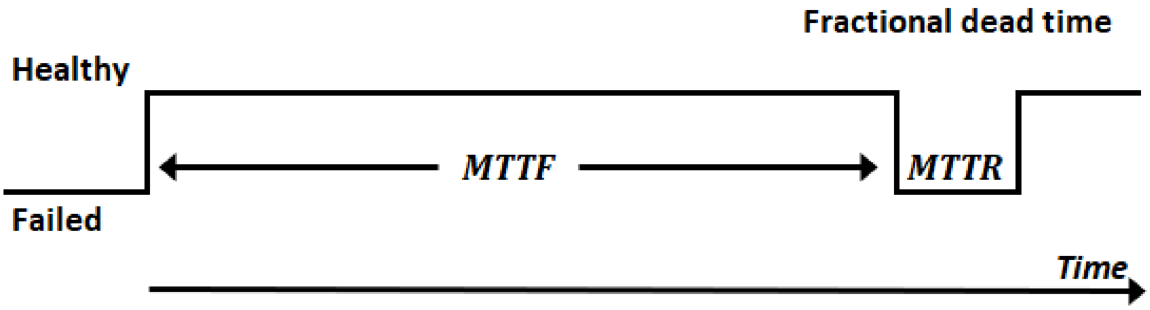
The MRT is neglected in the MoonSIF spreadsheet model.

Single channel PFD due to detected failures

It can be expected that restoration of 50% of failures will take longer than the $MTTR,$ and could take as long as the maximum permitted repair time. The model assumes that on average, detected failures are detected and repaired within the mean time to restoration, $MTTR$ (= time to detect + time to repair).

The mean time to failure for dangerous failures detected by diagnostics is represented as $MTTF_{DD}$.

The probability of failure can be estimated from the fractional dead time, the fraction of time that the channel is out of action, $MTTR/MTTF_{DD}$



The rate of detected dangerous failures, $\lambda_{DD} = 1/MTTF_{DD}$., so we can express the probability as:

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

Overall single channel PFD due to undetected and detected failure

The overall probability of failure is approximately equal to the sum of the probabilities of failure for undetected and detected failures. It is a valid approximation to sum the probabilities because the probabilities are << 1.

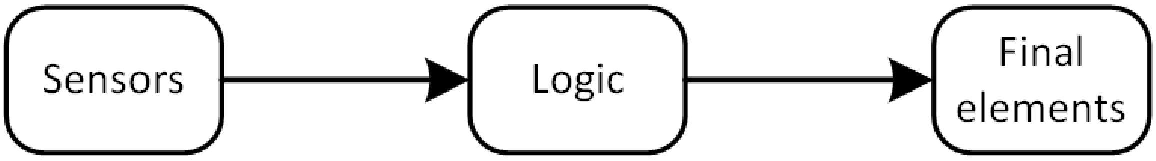
$$PFD_{AVG} \approx \frac{\lambda_{DU}.T_1}{2} + \lambda_{DD}.MTTR$$

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.

All three of the subsystems in a safety function must work successfully for the overall safety function to carry out its function.

The overall probability of failure for the whole safety function is approximately equal to the sum of the probabilities of failure on demand for its three subsystems:

$$PFD_{AVG}^{SF} \approx PFD_{AVG}^{sensor} + PFD_{AVG}^{logic\ solver} + PFD_{AVG}^{final\ element}$$



NooN architectures

NooN voting is applied when it is more important to prevent spurious trip rather than to achieve risk reduction in response to safety demands.

All N channels must work correctly for the safety function to trip, so:

$$PFD_{AVG} \approx \mathrm{N}.\frac{\lambda_{DU}.T_1}{2}$$

PFD for low-demand mode 1oo2 architecture

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 the average PFD_{AVG} for a 1oo2 architectures we can integrate the probability function over time to T, (the test interval). The integral is divided by the time period T to estimate the average probability:

$$\frac{1}{T}\int_0^T \lambda_{DU}{}^2\, t^2.dt \;= \frac{1}{T}.\frac{\lambda_{DU}{}^2 T_1{}^3}{3} \;=\; \frac{\lambda_{DU}{}^2 T_1{}^2}{3}$$

This assumes that the tests of the two separate channels are **synchronised**. Both channels are tested at time T.

The probability of common cause failures must be added to the PFD_{AVG} for any architecture with voting, and it usually dominates the result. Common cause failures can never be neglected.

The common failures are the failures expected to affect both channels in a similar way at a similar time. For that fraction of failures, the 1oo2 architecture will behave in the same way as a single channel, so the average probability of failure due to common causes is:

$$\beta.\frac{\lambda_{DU}.T_1}{2}$$

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:

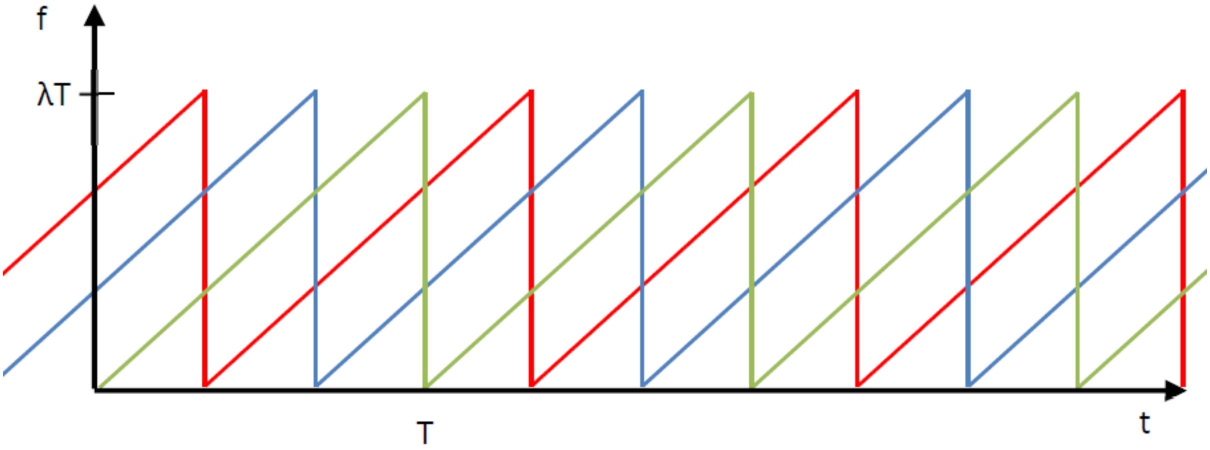
$$PFD_{AVG} \approx \frac{(1-\beta).\lambda_{DU}{}^2.\ T_1{}^2}{3} + \frac{\beta.\lambda_{DU}.T_1}{2}$$

The equation can be simplified slightly 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:

$$PFD_{AVG} \approx \frac{\lambda_{DU}{}^2.\ T_1{}^2}{3} + \frac{\beta.\lambda_{DU}.T_1}{2}$$

Staggered testing

The probability of failure is reduced if the tests of individual channels are staggered at equal time intervals T/N. This illustration is taken from a paper published by The 61508 Association, T6A042 *Development Paper – Effects of Proof Testing* [13]



As a first approximation the average probability can be simply estimated as the product of the average probability of each channel failing:

$$\frac{\lambda_{DU}.T}{2} \times \frac{\lambda_{DU}.T}{2} = \frac{{\lambda_{DU}}^2 T^2}{4}$$

The probability is reduced by a factor of ¾ when compared to synchronised testing. The average probability will be slightly lower if the tests are perfectly staggered. The T6A042 *Development Paper – Effects of Proof Testing* [13] and the SINTEF PDS Method Handbook [7] both include detailed analysis.

With perfectly staggered tests (at intervals of $T/2$ between channel tests) the minimum probability that can be achieved is:

$$\frac{5}{6} \times \frac{{\lambda_{DU}}^2 T^2}{4}$$

T6A042 includes a table of correction factors $\mathrm{St}_{\mathrm{M,N}}$ that are applied to the product $\left(\frac{\lambda_{DU}.T}{2}\right)^{N-M+1}$ for MooN voting with N up to 7:

$\mathrm{St}_{\mathrm{M,N}}$	N					
M	**2**	**3**	**4**	**5**	**6**	**7**
1	0.83	0.67	0.52	0.41	0.31	0.24
2		0.89	0.75	0.61	0.49	0.39
3			0.92	0.8	0.68	0.56
4				0.93	0.83	0.72
5					0.94	0.86
6						0.95

This table is included in the MoonSIF workbook.

The main benefit of staggered testing is that the contribution from common failures can be reduced for two different reasons.

The first reason is that common cause failures should be revealed when any 1 of N channels is inspected or tested. The remaining N-1 channels should be inspected and tested to determine if they have also failed due to the same cause. The average probability of failure due to common causes is reduced to:

$$\beta.\frac{\lambda_{DU}.\boldsymbol{T}/\mathbf{N}}{2}$$

The second reason is that staggered testing may also reduce the value of β itself.

It may be possible to reduce β to 0.05 or lower with staggered tests in combination with other techniques, such as FMEA and root cause analysis of all failures.

PFD for low-demand mode 2oo3 architectures

2oo3 architecture has the same level of fault tolerance as 1oo2. A 2oo3 function will fail only if 2 channels fail concurrently, so the probability is proportional to the square of the probability of one channel failing, $(\lambda_{DU}.t)^2$.

In 1oo2 voting with channels A and B there is only 1 way of having 2 failures: Both A and B fail.

In 2oo3 voting with channels A, B and C there are 3 ways of having 2 failures: (A and B fail), (B and C fail), or (C and A fail).

'3 choose 2' can be expressed mathematically as:

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

The *PFD* for 2oo3 voting is then:

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

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

The probability of failure due to detected failures has been neglected here on the basis that $MTTR$ is short and $\lambda_{DD}.MTTR$ << $\lambda_{DU}.T.$

Note that the β factor for 2oo3 voting can be expected to be 1.5 x higher than for 1oo2 (according to IEC 61508) or 2 x higher (according to SINTEF).

PFD due to not-detected failures

If not-detected failures were to occur at a reasonably constant rate, then the probability of failure would increase over time in proportion to the rate of not-detected failures, λ_{DN}.

The probability models are based on the assumption that not-detected failures will be revealed by occasional 'full test and inspection' with 100% coverage of all failure modes at time intervals T_2.

The model for PFD_{AVG} can be extended to include the not-detected failures revealed at T_2 intervals as well as the undetected failures revealed at the routine test intervals T_1.

For 1oo2 voting architecture the terms are:

$$PFD_{AVG} \approx \frac{(\lambda_{DU} - \lambda_{DN}).T_1}{2} + \frac{\lambda_{DN}.T_2}{2}$$

The estimate $\lambda_{DN}.T_2/2$ for the average probability of failure assumes that the probability of failure was zero at time zero and that not-detected failures occur and accumulate at a fixed and predictable rate. There is usually no real justification for making either of those assumptions. Reducing the time T_2 will not necessarily reduce the probability.

Nevertheless, this model is useful for estimating the effect of strategies such as partial stroke testing.

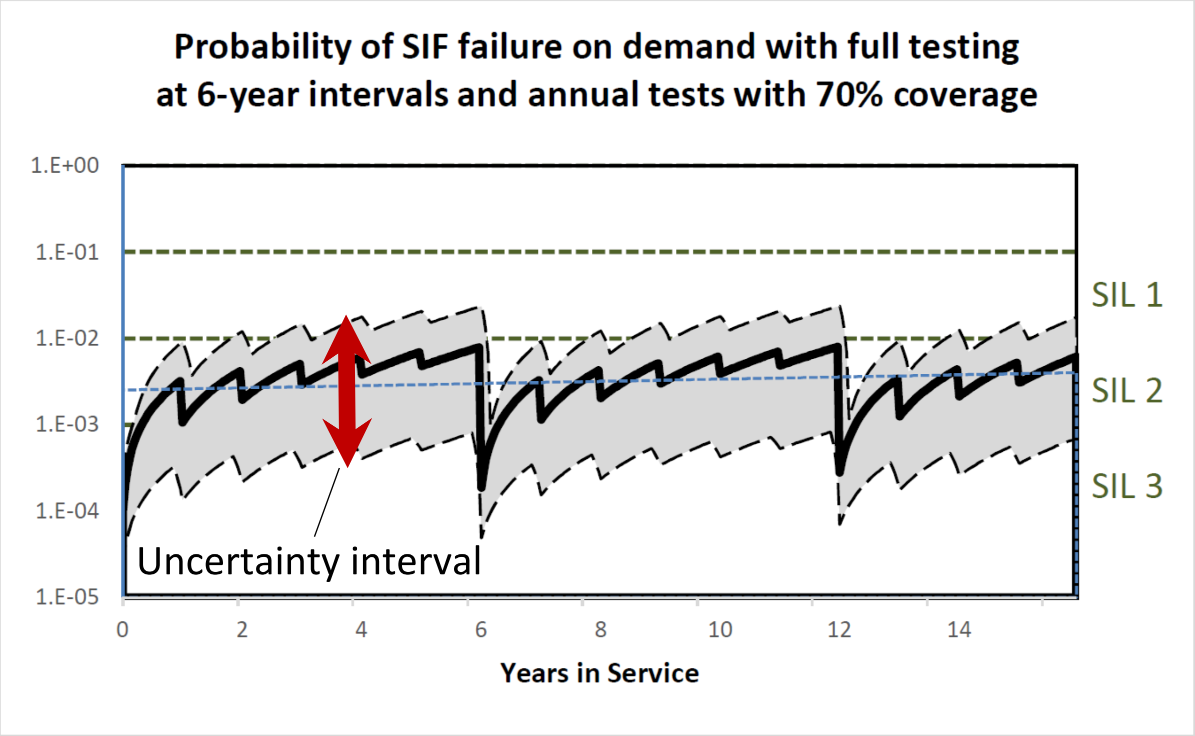
Partial stroke testing

Partial stroke testing may be applied on actuated valves when the opportunity for full test and inspection is limited to planned shutdowns of a plant for maintenance. For example, the planned shutdowns of an LNG plant may be at intervals of 5 or 6 years.

Annual testing of valves might be limited to moving the valve from fully open only as far as the 80% open position.

The parameters λ_{DN} and T_2 can be applied to model the effect of partial stroke testing of actuated valves. A partial stroke test can typically detect about 70% of the dangerous failures. The proportion of dangerous failures that can be detected depends on which failure modes will have a dangerous effect. Classification of safe and dangerous failures depends on the success criteria for the specific application of each valve.

The uncertainty in λ_{DN} and in the estimated probability of failure spans at least an order of magnitude, as always.



Combined MooN model for low-demand mode

The MoonSIF spreadsheet combines detected, undetected and not-detected failures into a single MooN model for low-demand mode. Refer to the reliability bock diagram shown above in the section titled 'Block diagram for probability of failure on demand'.

A safety function with MooN voting will fail if N-M+1 channels have failed at the same time.

The instantaneous probability of failure of a single channel can be estimated as:

$$\lambda_{DD}.MTTR + (\lambda_{DU} - \lambda_{DN}).t_1 + \lambda_{DN}.t_2$$

The term $t_1$represents the time since the last periodic inspection and test. The term $t_2$represents the time since the last test with full coverage.

The first term $\lambda_{DD}.MTTR$ already represents an average. The average of the other two terms can be estimated through integration with respect to time over the intervals T_1 and T_2 and dividing by the time intervals, as explained above.

The average probability of failure on demand for a single channel is then:

$$PFD_{1oo1\ AVG} \approx \lambda_{DD}.MTTR + \frac{(\lambda_{DU} - \lambda_{DN}).T_1}{2} + \frac{\lambda_{DN}.T_2}{2}$$

MooN low-demand mode with unsynchronised testing

The MooN model used for unsynchronised testing splits failures into the fraction with a common cause (β) and the fraction with independent causes (1 – β).

The MooN architecture is assumed to behave as if it were a single channel for the fraction of failure that have a common cause.

The N channels are assumed to behave completely independently for the fraction of failures with independent causes.

The probability of N-M+1 coincident independent failures is based on the average probability of a single channel failing, excluding common cause failures, represented by $PFD_{1oo1\ AVG}$:

$$PFD_{1oo1\ AVG} \approx (1-\beta_D).\lambda_{DD}.MTTR + \frac{(1-\beta).(\lambda_{DU} - \lambda_{DN}).T_1}{2} + \frac{(1-\beta).\lambda_{DN}.T_2}{2}$$

This probability is raised to the (N-M+1)th power for N-M+1 coincident independent failures, and multiplied by the number of different ways of having N-M+1 faulty channels out of a choice of N channels.

The combination 'N choose (N-M+1)' is written as $\binom{\mathrm{N}}{\mathrm{N-M+1}}$ and evaluated as

$$\binom{\mathrm{N}}{\mathrm{N-M+1}} = \frac{\mathrm{N!}}{\mathrm{(N-M+1)!.(M-1)!}}.$$

The overall probability of failure is then estimated by adding the probability of failure due to common cause failures:

$$\boldsymbol{PFD_{\mathrm{MooN}\ AVG}} \approx \binom{\mathbf{N}}{\mathbf{N-M+1}}.\left(\boldsymbol{PFD_{1oo1\ AVG}}\right)^{\mathbf{N-M+1}}$$

$$+\,\boldsymbol{\beta_D.\lambda_{DD}.MTTR} + \boldsymbol{\beta.\frac{(\lambda_{DU}-\lambda_{DN}).T_1}{2}} + \boldsymbol{\beta.\frac{\lambda_{DN}.T_2}{2}}$$

This method is what ISA-TR84.00.02-2002 describes as an 'average before product' method. Scaling factors can be added to the model to account for whether the periodic inspection and testing of individual channels is staggered at equal intervals or synchronised.

MooN low-demand mode with staggered testing

Probability of failure is minimised with perfectly staggered inspection and testing, and if common cause failures are detected at every individual test or inspection. Refer to the section above on Staggered testing. Scaling factors for staggered testing $\mathrm{St}_{\mathrm{M,N}}$ are given in the reference T6A042 [13].

T6A042 applies different scaling factors to the different terms in $PFD_{1oo1\ AVG}$. The detected failure term $(1-\beta_D).\lambda_{DD}.MTTR$ should be treated separately in a fully detailed analysis.

The generalised MooN form of the equation that is used in the MoonSIF spreadsheet depends on the simplification of applying the same scaling factor to the detected failures and undetected failures.

The following assumptions are made to justify the simplification:

- $MTTR \ll T$, (because typically $MTTR \approx 0.01$ year and $T \geq 1$ year)
- Diagnostic coverage < 90% when staggered testing is useful, so $\lambda_{DD} < 0.1\ \lambda_{DU}$
- and so $(1-\beta_D).\lambda_{DD}.MTTR \ll \left(\frac{(1-\beta).(\lambda_{DU}-\lambda_{DN}).T_1}{2} + \frac{(1-\beta).\lambda_{DN}.T_2}{2}\right)$
- The T_1 and T_2 intervals are assumed to be both evenly staggered, so that the scaling factor is equally applicable to the terms containing T_1 and T_2.

The generalised MooN form of the equation can then include the factor $\mathrm{St}_{\mathrm{M,N}}$ in this simplified form:

$$PFD_{\mathrm{MooN}\ AVG} \approx \mathrm{St}_{\mathrm{M,N}}\cdot\binom{\mathrm{N}}{\mathrm{N-M+1}}.\left(PFD_{1oo1\ AVG}\right)^{\mathrm{N-M+1}}$$

$$+\,\beta_D.\lambda_{DD}.MTTR + \beta.\frac{(\lambda_{DU}-\lambda_{DN}).{}^{T_1}/_{\mathrm{N}}}{2} + \beta.\frac{\lambda_{DN}.{}^{T_2}/_{\mathrm{N}}}{2}$$

This simplified model was validated by comparing results with fully detailed long hand calculations for all MooN combinations up to N = 7. The calculations were performed in each case across the typical range of variation for each of the parameter values. The error introduced by the simplification was shown to be < 1%.

Expanded MooN model for low-demand mode with synchronised testing

The probability of failure is slightly higher with synchronised inspection and testing. The peak values of instantaneous probability in each of the N channels coincide. Theoretically, a more accurate estimate is obtained by calculating the average probability by integration over time ***after*** raising the instantaneous probability of failure to the (N-M+1)th power. The calculation is more complicated because each cross-product term needs to be integrated separately, and the number of cross-product terms increases with increasing (N-M+1).

The simpler 'average before product' estimate will be slightly lower than the more accurate 'average after product' model. Scaling factors for synchronised inspection and testing can be determined by comparing the form of the 'average before product' model with the form of the 'average after product' model. The first step in the 'average after product' is to estimate the instantaneous probability of failure:

$$\binom{\mathrm{N}}{\mathrm{N-M+1}}\,[(1-\beta_D).\lambda_{DD}.MTTR + (1-\beta).(\lambda_{DU}-\lambda_{DN}).t_1 + (1-\beta).\lambda_{DN}.t_2]^{N-M+1}$$
$$+ (\beta_D.\lambda_{DD}.MTTR + \beta.(\lambda_{DU}-\lambda_{DN}).t_1 + \beta.\lambda_{DN}.t_2)$$

The expansion of the term raised to the power N-M+1 results in 6 main terms corresponding to:

$$[(1-\beta_D).\lambda_{DD}.MTTR]^{\mathrm{N-M+1}}$$
$$+ [(1-\beta).(\lambda_{DU}-\lambda_{DN}).t_1]^{\mathrm{N-M+1}}$$
$$+ [(1-\beta).\lambda_{DN}.t_2]^{\mathrm{N-M+1}}$$
$$+ \beta_D.\lambda_{DD}.MTTR^{\square}$$
$$+ \beta.(\lambda_{DU}-\lambda_{DN}).t_1$$
$$+\beta.\lambda_{DN}.t_2$$

For the example, an architecture with fault tolerance N-M = 2 has N-M+1 = 3.

The 6 main terms are:

$$[(1-\beta_D).\lambda_{DD}.MTTR]^3$$
$$+ [(1-\beta).(\lambda_{DU}-\lambda_{DN}).t_1]^3$$
$$+ [(1-\beta).\lambda_{DN}.t_2]^3$$
$$+ \beta_D.\lambda_{DD}.MTTR^{\square}$$
$$+ \beta.(\lambda_{DU}-\lambda_{DN}).t_1$$
$$+\beta.\lambda_{DN}.t_2$$

Additional terms are added to account for the probability of coincident **independent** failures of different types in different channels. These additional terms are calculated from the cross-products of probabilities for the three different types of failure (detected failures λ_{DD}, undetected failures λ_{DU}, and not-detected failures λ_{DN}).

In the example with fault tolerance N-M = 2, the cross-product terms are:

$$+3.(1-\beta_D).\lambda_{DD}.MTTR.[(1-\beta).(\lambda_{DU}-\lambda_{DN}).t_1]^2$$
$$+3.(1-\beta_D).\lambda_{DD}.MTTR.[(1-\beta).\lambda_{DN}.t_2]^2$$
$$+3.(1-\beta).(\lambda_{DU}-\lambda_{DN}).t_1.[(1-\beta_D).\lambda_{DD}.MTTR]^2$$
$$+3.(1-\beta).(\lambda_{DU}-\lambda_{DN}).t_1.[(1-\beta).\lambda_{DN}.t_2]^2$$
$$+3.(1-\beta).\lambda_{DN}.t_2.[(1-\beta_D).\lambda_{DD}.MTTR]^2$$
$$+3.(1-\beta).\lambda_{DN}.t_2.[(1-\beta).(\lambda_{DU}-\lambda_{DN}).t_1]^2$$
$$+ 6.(1-\beta_D).\lambda_{DD}.MTTR.(1-\beta).(\lambda_{DU}-\lambda_{DN}).t_1.(1-\beta).\lambda_{DN}.t_2$$

The average probability of failure over the time intervals T_1 and T_2 can be estimated through integration of the 6 main terms and the cross-product terms with respect to time, and dividing by the relevant time intervals. The factor N-M+2 in the denominator comes from integrating $t^{N-M+1}.dt$ as explained above in the section ***PFD*** for low-demand mode 1oo2 architecture. The resulting 6 main terms in the expanded model are:

Voted term for undetected failures revealed by tests at interval T_1

Common cause term for undetected failures revealed by tests at interval T_1

$$PFD_{AVG} \approx \binom{\mathrm{N}}{\mathrm{N-M+1}} \cdot \frac{((1-\beta).(\lambda_{DU}-\lambda_{DN}).T_1)^{\mathrm{N-M+1}}}{\mathrm{N-M+2}} + \frac{\beta.(\lambda_{DU}-\lambda_{DN}).T_1}{2}$$

Voted term for ‘never’ detected failures revealed by full tests at interval T_2

Common cause term for ‘never’ detected failures revealed by full tests at interval T_2

$$+ \binom{\mathrm{N}}{\mathrm{N-M+1}} \cdot \frac{((1-\beta).\lambda_{DN}.T_2)^{\mathrm{N-M+1}}}{\mathrm{N-M+2}} + \frac{\beta.\ \lambda_{DN}.T_2}{2}$$

Voted term for failures detected by continuous diagnostics and repaired within the $MTTR$

Common cause term for failures detected by continuous diagnostics and repaired within the $MTTR$

$$+ \binom{\mathrm{N}}{\mathrm{N-M+1}} \cdot ((1-\beta_D).\lambda_{DD})^{\mathrm{N-M+1}}.MTTR^{\mathrm{N-M+1}} + \beta_D.\ \lambda_{DD}.MTTR$$

Additional **cross-product** terms account for the probability of coincident **independent** failures in N redundant channels for the three different types of failure (detected failures λ_{DD}, undetected failures λ_{DU}, and not-detected failures λ_{DN}).

The number of cross product terms increases with increasing fault tolerance. The terms shown below apply for fault tolerant architectures (N-M > 0) and cover combinations of up to 3 coincident failures for N-M up to and including 2. These 9 terms remain valid for N-M > 2, but a full expansion would include several more (but progressively smaller) terms to model 4 or more coincident failures of different types.

1. The probability of failure due to a detected failure in one of N channels when N-M undetected failures exist in the remaining N-1 channels.

$$+\ \mathrm{N}.\lambda_{DD}.MTTR\,.\left(\binom{\mathrm{N}-1}{\mathrm{N}-\mathrm{M}}\,.\frac{\left((1-\beta).(\lambda_{DU}-\lambda_{DN}).T_1\right)^{\mathrm{N}-\mathrm{M}}}{\mathrm{N}-\mathrm{M}+1}\right)$$

2. The probability of failure due to an undetected failure in one of N channels when N-M detected failures exist in the remaining N-1 channels. This term is omitted if (N-M) < 2 because it duplicates equation 1 if N-M = 1.

$$+\ \left(\mathrm{N}.\frac{(\lambda_{DU}-\lambda_{DN}).T_1}{2}\right).\left(\binom{\mathrm{N}-1}{\mathrm{N}-\mathrm{M}}\,.\left((1-\beta_D).\lambda_{DD}\right)^{\mathrm{N}-\mathrm{M}}.MTTR^{\mathrm{N}-\mathrm{M}}\right)$$

3. The probability of failure due to a detected failure in one of N channels when N-M not-detected failures exist in the remaining N-1 channels.

$$+\ \mathrm{N}.\lambda_{DD}.MTTR\,.\left(\binom{\mathrm{N}-1}{\mathrm{N}-\mathrm{M}}\,.\frac{\left((1-\beta).\lambda_{DN}.T_2\right)^{\mathrm{N}-\mathrm{M}}}{\mathrm{N}-\mathrm{M}+1}\right)$$

4. The probability of failure due to a not-detected failure in one of N channels when N-M detected failures exist in the remaining N-1 channels. This term is omitted if (N-M) < 2 because it duplicates equation 3 if N-M = 1.

$$+\ \left(\mathrm{N}.\frac{\lambda_{DN}.T_2}{2}\right).\left(\binom{\mathrm{N}-1}{\mathrm{N}-\mathrm{M}}\,.\left((1-\beta_D).\lambda_{DD}\right)^{\mathrm{N}-\mathrm{M}}.MTTR^{\mathrm{N}-\mathrm{M}}\right)$$

5. The probability of failure due to a detected failure in one of N channels when a not-detected failure exists in one other channel and when N-M-1 undetected failures exist in the remaining **N-2 channels**. The equation does not apply for (N-M) < 2 because N-M-1 <= 0.

$$+\,\mathrm{N}.\,(\lambda_{DD}.\,MTTR).\left(\binom{\mathrm{N}-1}{1}.\frac{\lambda_{DN}.\,T_2}{2}\right).\left(\binom{\mathrm{N}-2}{\mathrm{N}-\mathrm{M}-1}.\frac{\left((1-\beta).\,(\lambda_{DU}-\lambda_{DN}).\,T_1\right)^{\mathrm{N}-\mathrm{M}-1}}{\mathrm{N}-\mathrm{M}+2}\right)$$

6. The probability of failure due to an undetected failure in one of N channels when a not-detected failure exists in one other channel and when N-M-1 detected failures exist in the remaining **N-2 channels** (the detected failure is taken as the last failure to occur in this combination because it always has the lowest probability). This duplicates the result of equation 5 if N-M = 2, so this equation only applies for (N-M) > 2.

$$+\left(\mathrm{N}.\frac{(1-\beta).\,(\lambda_{DU}-\lambda_{DN}).\,T_1}{2}\right).\left(\binom{\mathrm{N}-1}{1}.\frac{\lambda_{DN}.\,T_2}{2}\right).\left(\binom{\mathrm{N}-2}{\mathrm{N}-\mathrm{M}-1}\,.\,((1-\beta_D).\,\lambda_{DD})^{\mathrm{N}-\mathrm{M}-1}.\,MTTR^{\mathrm{N}-\mathrm{M}-1}\right)$$

7. The probability of failure due to a not-detected failure in one of N channels when an undetected failure exists in one other channel and when N-M-1 detected failures exist in the remaining **N-2 channels** (the detected failure is taken as the last failure to occur in this combination because it always has the lowest probability). This term is omitted from the model for N-M = 3 because it duplicates the result of equation 6. The equation applies for (N-M) > 3.

$$+\left(\mathrm{N}.\frac{\lambda_{DN}.\,T_2}{2}\right).\left(\binom{\mathrm{N}-1}{1}.\frac{\lambda_{DU}.\,T_1}{2}\right).\left(\binom{\mathrm{N}-2}{\mathrm{N}-\mathrm{M}-1}\,.\,((1-\beta_D).\,\lambda_{DD})^{\mathrm{N}-\mathrm{M}-1}.\,MTTR^{\mathrm{N}-\mathrm{M}-1}\right)$$

8. The probability of failure due to an undetected failure in one of N channels when N-M not-detected failures exist in the remaining N-1 channels.

$$+\,\mathrm{N}.\frac{(\lambda_{DU}-\lambda_{DN}).\,T_1}{2}.\,\left(\binom{\mathrm{N}-1}{\mathrm{N}-\mathrm{M}}\,.\frac{((1-\beta).\,\lambda_{DN}.\,T_2)^{\mathrm{N}-\mathrm{M}}}{\mathrm{N}-\mathrm{M}+1}\right)$$

9. The probability of failure due to a not-detected failure in one of N channels when N-M undetected failures exist in the remaining N-1 channels. This term is omitted if (N-M) < 2 because it duplicates equation 8.

$$+\,\mathrm{N}.\frac{\lambda_{DN}.\,T_2}{2}.\,\left(\binom{\mathrm{N}-1}{\mathrm{N}-\mathrm{M}}\,.\frac{\left((1-\beta).\,(\lambda_{DU}-\lambda_{DN}).\,T_2\right)^{\mathrm{N}-\mathrm{M}}}{\mathrm{N}-\mathrm{M}+1}\right)$$

Simplified MooN low-demand mode with synchronised testing

Inspection of the 'average before' and 'average after' methods reveals that the 'average before' method includes main terms for undetected failures in the form $\frac{(\lambda_D.T)^{\mathrm{N-M+1}}}{2^{\mathrm{N-M+1}}}$.

In comparison, the main terms in the 'average after' method include the factor $\frac{(\lambda_D.T)^{\mathrm{N-M+1}}}{\mathrm{N-M+2}}$.

The 'average after' estimate is larger than the 'average before' by a factor of approximately $\frac{2^{\mathrm{N-M+1}}}{\mathrm{N-M+2}}$.

For instance, the correction factor is 4/3 for N-M = 1 and 8/4 (i.e. 2) for N-M = 2.

Systems with synchronised inspection and testing might therefore be modelled by applying a scaling factor in the 'average before product' model:

$$PFD_{\mathrm{MooN}\ AVG} \approx \frac{\mathbf{2^{N-M+1}}}{\mathbf{N-M+2}}.\binom{\mathrm{N}}{\mathrm{N-M+1}}.(PFD_{1oo1\ AVG})^{\mathrm{N-M+1}}$$
$$+\ \beta_D.\lambda_{DD}.MTTR\ +\ \beta.\frac{(\lambda_{DU}-\lambda_{DN}).T_1}{2}+\ \beta.\frac{\lambda_{DN}.T_2}{2}$$

The reason for using this simplified 'corrected average before product' model is that it avoids the need for expanding all of the cross-products. The number of cross-products in the fully expanded model increases with N-M. Generic fully expanded models that allow for all values of N-M are more complicated. This simplified model was compared with a fully expanded algorithmic model programmed in VBA (Visual Basic for Applications). The simplified model introduces an error of up to about 1% into the estimate because the scaling factor is only correct for the largest terms in the equation.

The scaling factor does not apply to the detected failure term $\lambda_{DD}.MTTR$ within $PFD_{1oo1\ AVG}$ because that term does not include N-M+2 as a denominator. The effect will be negligible if $\lambda_{DD}.MTTR \ll \lambda_{DU}.T$.

The cross-product terms $\lambda_{DD}.MTTR\,.\,\lambda_{DN}.T_2$ and $\lambda_{DD}.MTTR\,.\,(\lambda_{DU}-\lambda_{DN}).T_1$ have N-M+1 in the denominator rather than N-M+2. A different scaling factor would need to be applied for those terms to be accurate. For example, the factor would be 4/2 = 2 for N-M = 1 and 8/3 for N-M = 2.

The cross-product terms $(\lambda_{DU}-\lambda_{DN}).T_1.\lambda_{DN}.T_2$ have [2.(N-M+1)] in the denominator. They may become significant with proof test coverage < 90%, if $(\lambda_{DU}-\lambda_{DN}).T_1 \approx \lambda_{DN}.T_2$. The correct scaling factors would be 4/4 = 1 for N-M = 1 and 8/6 for N-M = 2.

The justification for using this simplified 'corrected average before' model depends on the assumption that these smaller cross-product terms do not make significant contributions to the estimate. The assumption was validated by analysing the relative size of each of the terms in the fully expanded model across a wide range of parameter values in different combinations and MooN architectures. The cross-product terms may become more significant if common cause failures are reduced so that $\beta < 0.05$.

The error introduced by applying the simplified correction to the $(PFD_{1oo1\ AVG})^{\mathrm{N-M+1}}$ term was limited to about 1% in the cases evaluated for this study.

Which terms contribute most to PFD?

The fully expanded model was used in a detailed analysis to reveal the relevant importance of each of the terms in the expanded equation. That analysis was used to examine the validity of simplified 'corrected average before product' model and also to test the simple approximations for manual calculations described in the introduction above.

The analysis was conducted for every MooN permutation with failure rates ranging from 10^{-4} pa to 10^{-1} pa. This range corresponds to about 100 FITS to 10,000 FITS, or 10^{-8} per hour to 10^{-5} per hour. It can be expressed in terms of $MTTF$ as range from 10,000 years to 10 years. Safety function subsystem failure rates are usually expected to be in this range.

Subsystem PFD_{AVG} was estimated with different combinations of values for diagnostic coverage, common cause failure fraction, and proof test coverage.

Analysis demonstrated the validity of the assumptions made in the simplified 'corrected average before product' synchronised testing model based on $\frac{2^{N-M+1}}{N-M+2}.\binom{N}{N-M+1}.(PFD_{1oo1\ AVG})^{N-M+1}$.

The model agrees with the fully expanded model to within about 1%. The error is far smaller than the uncertainty that should always be expected due to range of variation in input parameters.

Representative examples

The following examples are representative of typical failure data and commonly used voting architectures. Pie charts have been included to show that usually only 2 or 3 of the terms in the fully expanded model will be significant.

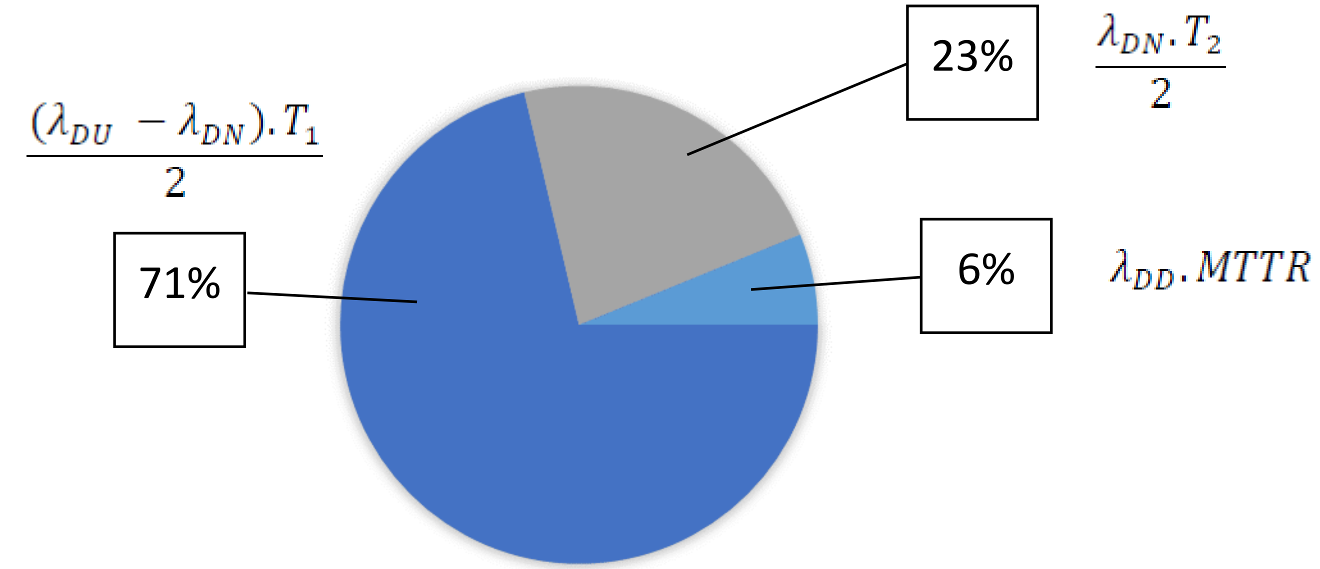
Typical sensor system failure data

These failure rates are typical of sensors such as pressure sensors and include failures in cabling and logic solver input channels.

Dangerous detected failure rate (FITS)	1,000
Dangerous undetected failure rate (FITS)	200
Dangerous not-detected failure rate (FITS)	10
Safe detected failure rate (FITS)	500
Safe undetected failure rate (FITS)	70

$MTTR$ **(days)**	3
Periodic test interval T_1 **(years)**	1
Full coverage test interval T_2 **(years)**	6
Proof test coverage	0.95
Common cause failure fraction	0.1

1oo1 sensor voting architecture

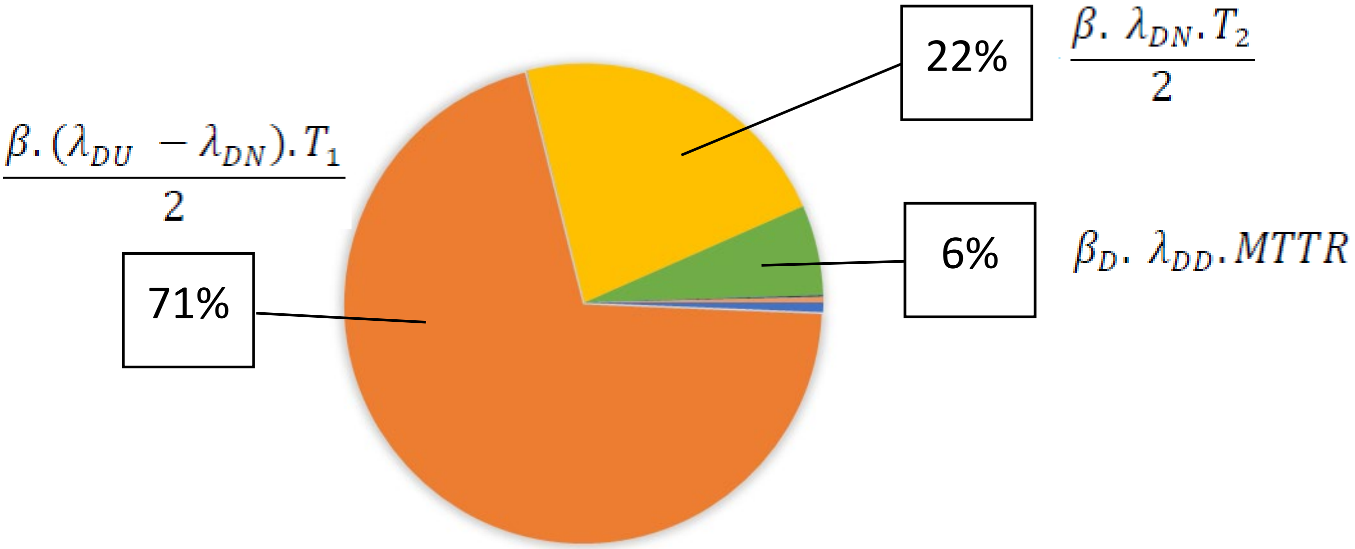


The expanded MooN model gives the result PFD_{AVG}: ≈ 1.2 x 10^{-3}

The simple approximation 2/3.$\lambda_{DU}.T_1$ also gives the result PFD_{AVG}: ≈ 1.2 x 10^{-3}

The approximation 2/3.$\lambda_{DU}.(PTC.\ T_1$. + (1-PTC). T_2) ≈ 1.5 x 10^{-3}

1oo2 sensor voting architecture

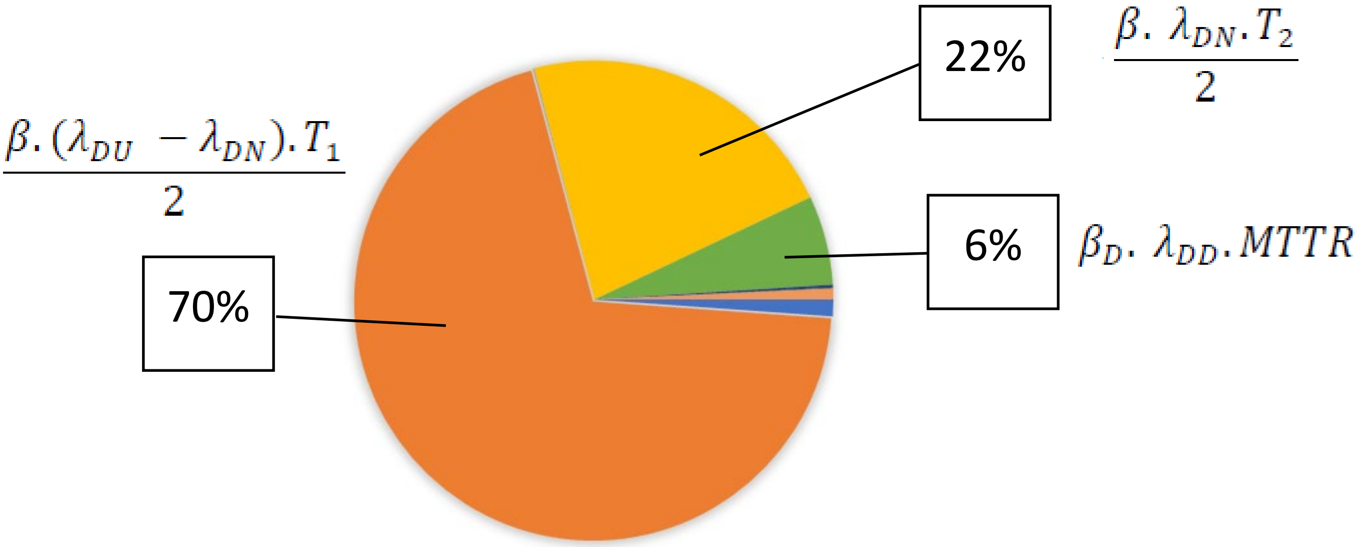


The expanded MooN model gives the result PFD_{AVG}: ≈ 1.2 x 10^{-4}

The simple approximation 2/3.$\beta.\lambda_{DU}.T_1$ also gives the result PFD_{AVG}: ≈ 1.2 x 10^{-4}

The approximation 2/3.$\beta.\lambda_{DU}.(PTC.\ T_1$. + (1-PTC). T_2) ≈ 1.5 x 10^{-4}

2oo3 sensor voting architecture



The expanded MooN model gives the result PFD_{AVG}: ≈ 1.8 x 10^{-4}

The simple approximation 2/3.$\beta.\lambda_{DU}.T_1$ also gives the result PFD_{AVG}: ≈ 1.8 x 10^{-4}

The approximation 2/3.$\beta.\lambda_{DU}.(PTC.\ T_1\ .+(1-PTC).\ T_2)$ ≈ 2.2 x 10^{-4}

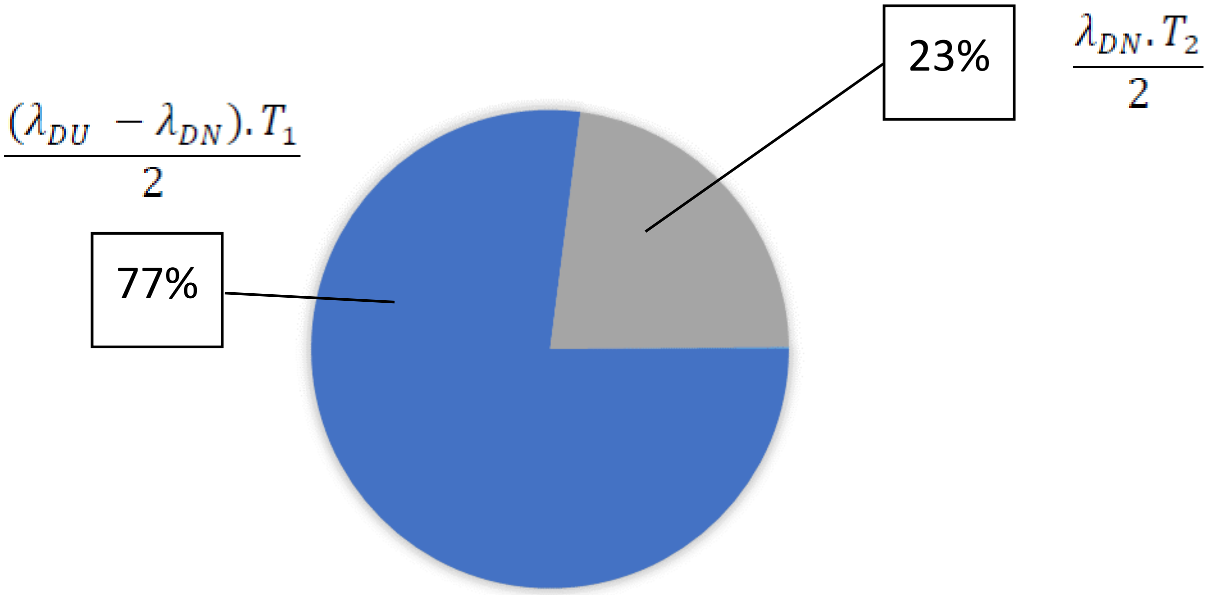
Typical final element system failure data

These failure rates are typical for a pneumatically actuated shutdown valve, including solenoid and actuator, and failures in cabling and logic solver output channels.

Dangerous detected failure rate (FITS)	300
Dangerous undetected failure rate (FITS)	2800
Dangerous not-detected failure rate (FITS)	100
Safe detected failure rate (FITS)	300
Safe undetected failure rate (FITS)	300

$MTTR$ **(days)**	3
Periodic test interval T_1 **(years)**	1
Full coverage test interval T_2 **(years)**	8
Proof test coverage	0.96
Common cause failure fraction	0.1

1oo1 final element voting architecture

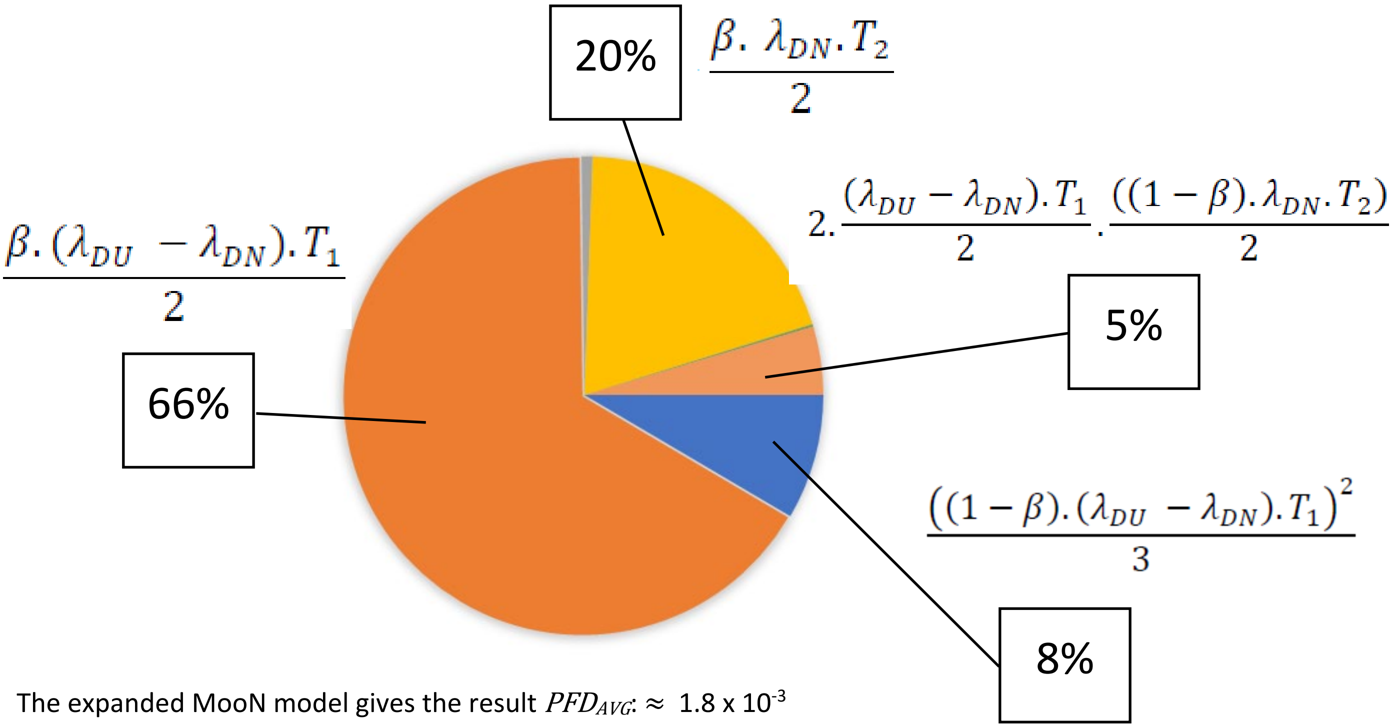


The expanded MooN model gives the result PFD_{AVG}: ≈ 1.5 x 10^{-2}

The simple approximation 2/3.λ_{DU}.T_1 gives the result PFD_{AVG}: ≈ 1.6 x 10^{-2}

The approximation 2/3.λ_{DU}.(*PTC*. T_1 . + (1-*PTC*). T_2) ≈ 2.0 x 10^{-2}

1oo2 final element voting architecture



The expanded MooN model gives the result PFD_{AVG}: ≈ 1.8 x 10^{-3}

The simple approximation 2/3.β.λ_{DU}.T_1 gives the result PFD_{AVG}: ≈ 1.6 x 10^{-3}

The approximation 2/3.β.λ_{DU}.(*PTC*. T_1 . + (1-*PTC*). T_2) ≈ 2.0 x 10^{-3}

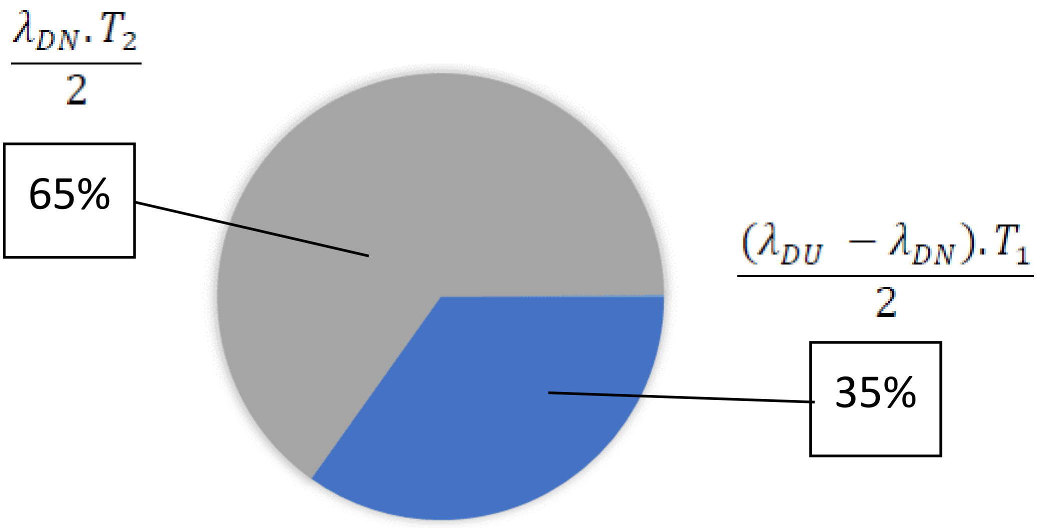
Example with partial stoke testing of actuated valves

These failure rates are typical for a pneumatically actuated shutdown valve with partial stroke testing. It includes the solenoid and actuator, and failures in cabling and logic solver output channels.

Dangerous detected failure rate (FITS)	300
Dangerous undetected failure rate (FITS)	2200
Dangerous not-detected failure rate (FITS)	700
Safe detected failure rate (FITS)	300
Safe undetected failure rate (FITS)	300

$MTTR$ **(days)**	3
Periodic test interval T_1 **(years)**	1
Full coverage test interval T_2 **(years)**	4
Proof test coverage	0.7
Common cause failure fraction	0.1

1oo1 final element voting architecture – with partial stroke testing

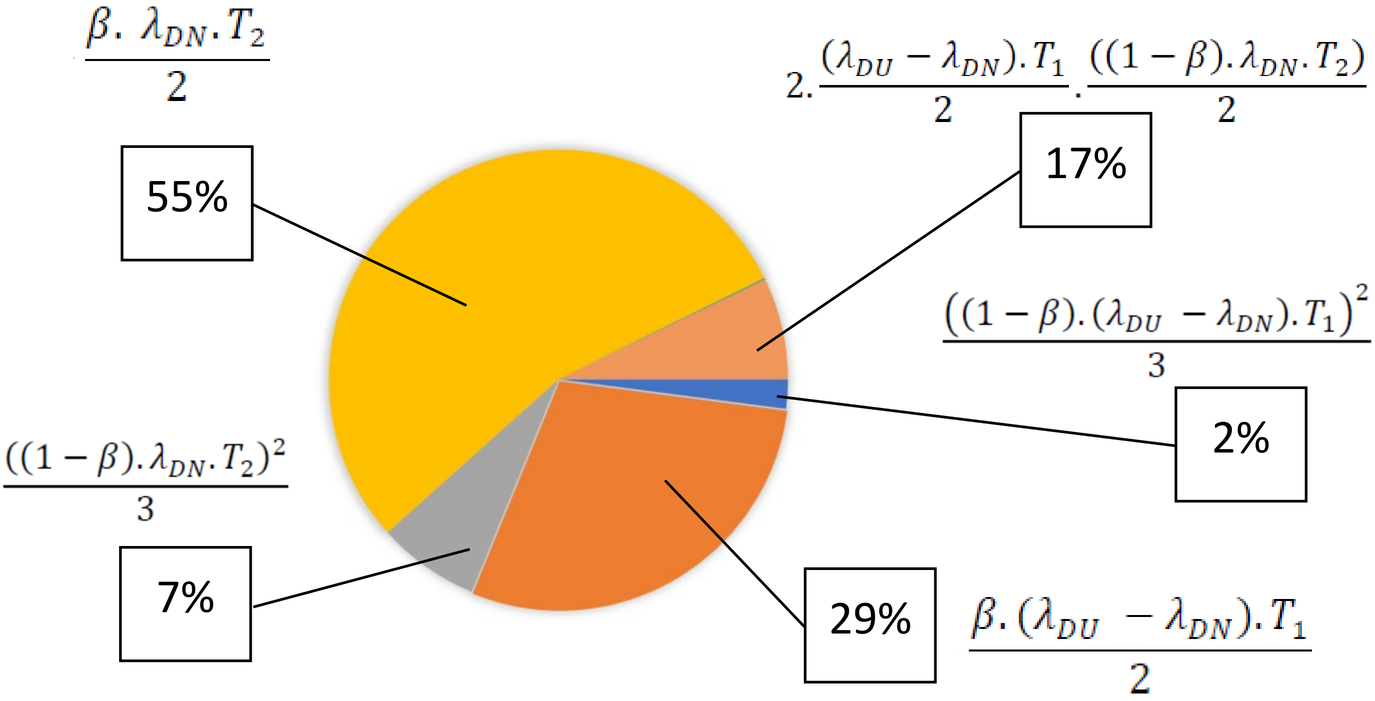


The expanded MooN model gives the result PFD_{AVG}: ≈ 1.9×10^{-2}

The simple approximation $2/3.\lambda_{DU}.T_1$ gives the result PFD_{AVG}: ≈ 1.3×10^{-2}

The approximation $2/3.\lambda_{DU}.(PTC.\ T_1\ . + (1\text{-}PTC).\ T_2) \approx 2.5 \times 10^{-2}$

1oo2 final element voting architecture – with partial stroke testing



The expanded MooN model gives the result PFD_{AVG}: ≈ 2.3 x 10^{-3}

The simple approximation 2/3.$\beta.\lambda_{DU}.T_1$ gives the result PFD_{AVG}: ≈ 1.3 x 10^{-3}

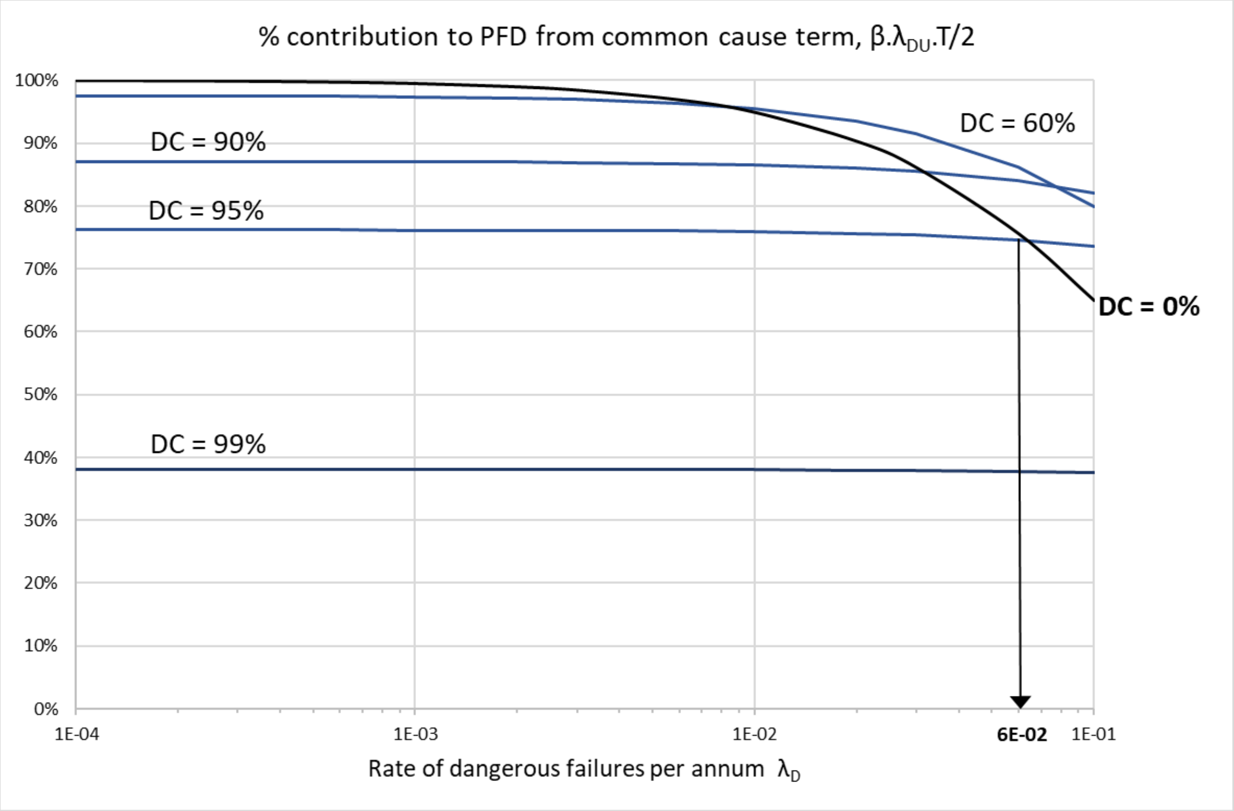
The approximation 2/3.$\beta.\lambda_{DU}$.(PTC. T_1 . + (1-PTC). T_2) ≈ 2.5 x 10^{-3}

Validation of the simple approximations

Detailed analysis also revealed the range of values over which the simpler approximations based on $\frac{2}{3}.\ \beta_{\mathrm{MooN}}.\lambda_{DU}.T$ would be valid. Those approximations are based on the assumption that undetected failures usually contribute at least 75% of the estimated PFD_{AVG} .

The effect of diagnostic coverage

This graph plots the fraction $\frac{\beta.\lambda_{DU}.{}^{T}/_{2}}{PFD_{AVG}}$ against dangerous failure rate with 1oo2 architecture, β= 0.1, and with a range of values of diagnostic coverage (DC).



The results showed that with diagnostic coverage between 10% and 95%, for any value of failure rate:

$$\beta.\lambda_{DU}.{}^{T}/_{2}\ >\ {}^{3}/_{4}.PFD_{AVG}$$

The same results were found to be true for all fault tolerant MooN architectures. Therefore:

$$PFD_{AVG} <\ {}^{2}/_{3}\ \beta_{\mathrm{MooN}}.\lambda_{DU}.T_{1}$$

The contribution from detected failures becomes significant for diagnostic coverage > 95%. The following approximation is valid for all failure rates in MooN systems with diagnostic coverage > 95%:

$$PFD_{AVG}\ \approx\ \beta_{D}.\lambda_{DD}.MTTR + \beta.\lambda_{DU}.{}^{T}/_{2}$$

The effect of MooN with dangerous failure rate λ_{DU} > 0.05 pa

Analysis with different MooN architectures reveals that the basic approximation $^2/_3\ \beta_{\mathrm{MooN}}.\lambda_{DU}.T_1$ is valid for undetected dangerous failure rates up to $\lambda_{DU} \approx$ 0.05 pa ($MTTF_{DU} \approx$ 20 y) in any MooN architectures with N-M > 1, and for N ≤ 2 in MooN architectures with N-M = 1.

The graph below plots the fraction contributed to PFD_{AVG} by common cause failures against the undetected dangerous failure rate with commonly used MooN architectures.

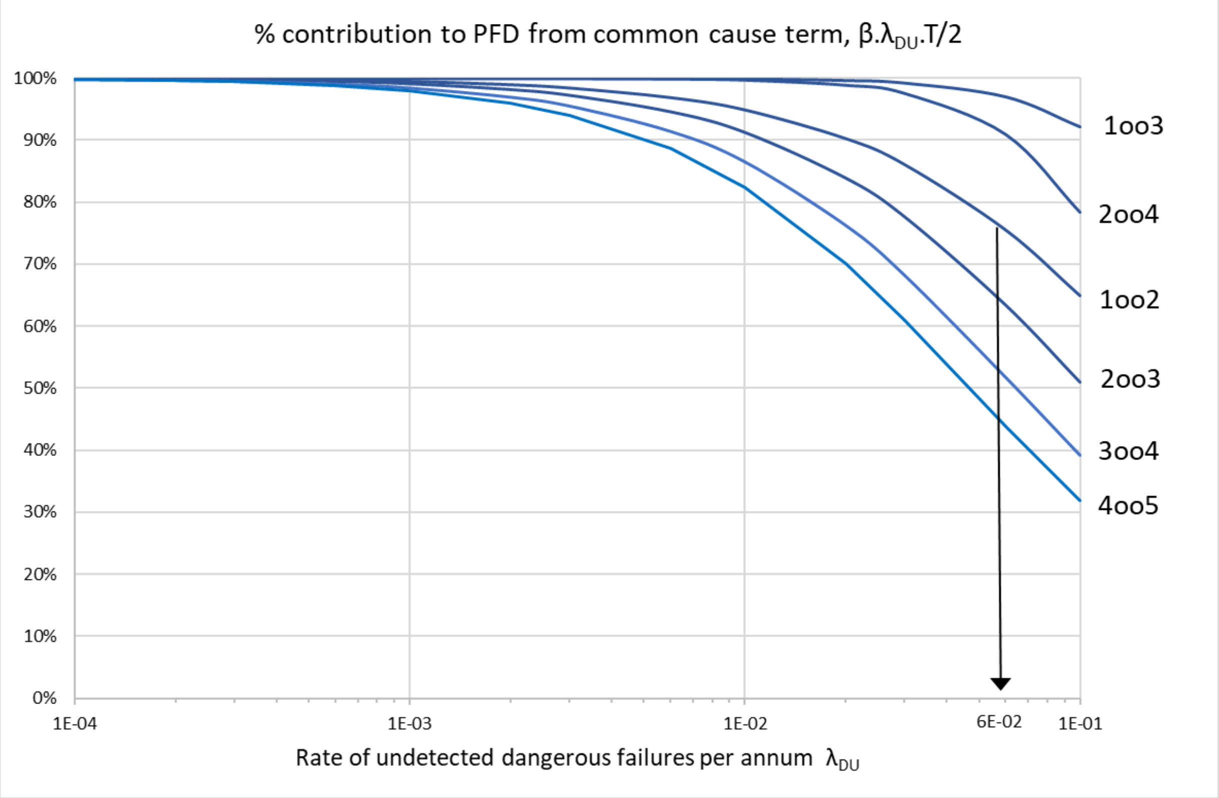
These examples are calculated with β_{MooN} based on β_{1oo2} = 0.1 and using MooN scaling factors for β from IEC 61508-6. The diagnostic coverage in this set of examples is 0%.

The PFD_{AVG} may be about 10% to 30 % higher than the basic approximation if the undetected dangerous failure rate λ_{DU} > 0.05 pa. The error is highest in systems with N-M = 1, and increases with N up to a maximum error at N = 5. Both SINTEF and IEC 61508-6 β models suggest that common cause failure terms become more significant with N > 5.

The curves for 5oo6 and 6oo7 were omitted from this plot for clarity because they overlap with the curves for 2oo3 and 3oo4. The results vary slightly depending on the selection of MooN scaling factors for β. The multipliers given in SINTEF PDS Method 2013 are higher than in IEC 61508-6. The contribution from the common cause term is then correspondingly higher.

A similar conclusion is reached with both the SINTEF and IEC 61508-6 β models: The approximation can be modified to $PFD_{AVG} \approx \ \beta_{\mathrm{MooN}}.\lambda_{DU}.T_1$ for any MooN architecture with N-M = 1 and N > 2 when λ_{DU} > 0.05 pa.

Note that λ_{DU} > 0.05 pa would usually be avoidable for systems with N > 2. The undetected dangerous failure rate can be reduced through diagnostics based on comparison of signals across the N channels.

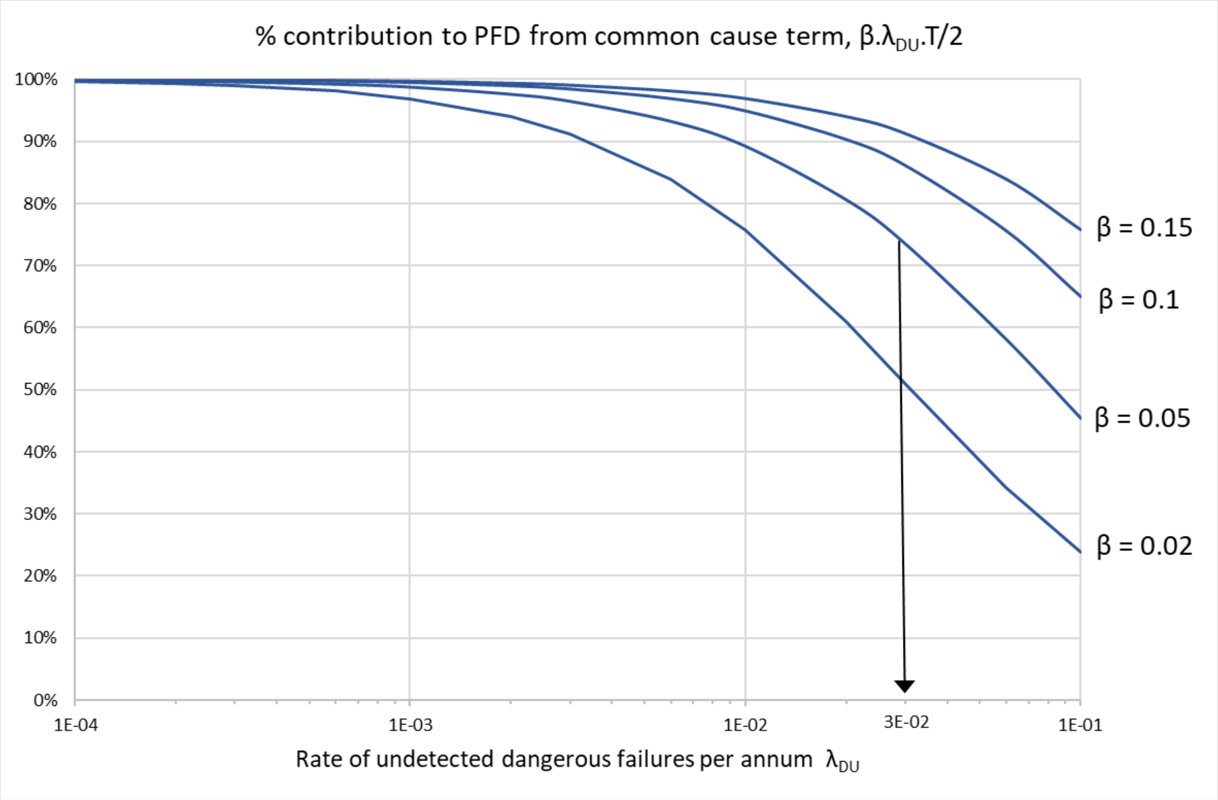


The effect of common cause failure fraction

Varying the value of common cause failure fraction β shows that these simple approximations remain valid for $\beta \geq 0.05$ and $\lambda_{DU} < 0.03$ pa ($MTTF_{DU} > 30$ y).

With zero diagnostic coverage, $\beta = 0.05$ and $\lambda_{DU} \approx 0.1$ pa, $PFD_{AVG} \approx \beta_{\text{MooN}}.\lambda_{DU}.T_1$.

Detailed analysis is recommended if it is necessary to achieve $\beta < 0.05$.



The effect of proof test coverage

The analysis demonstrated that with reduced proof test coverage in any MooN architecture:

$$\left(\beta.(\lambda_{DU}-\lambda_{DN}).{}^{T_1}\!/_2 + \beta.\lambda_{DN}.{}^{T_2}\!/_2\right) > {}^3\!/_4.PFD_{AVG}$$

This may also be expressed as:

$$\left(PTC.{}^{T_1}\!/_2 + (1-PTC).{}^{T_2}\!/_2\right).\beta.\lambda_{DU} > {}^3\!/_4.PFD_{AVG}$$

In general, for any MooN architecture with reduced proof test coverage:

$$PFD_{AVG} \approx {}^2\!/_3\,.\beta_{\text{MooN}}.\lambda_{DU}.(PTC.T_1 + (1-PTC).T_2)$$

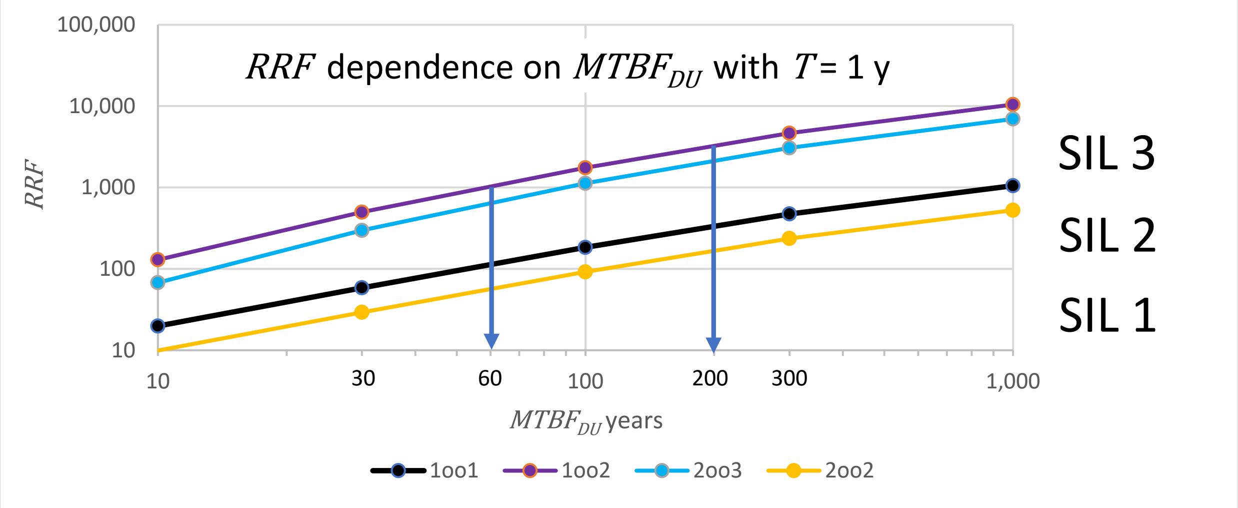
Typical estimated RRF for varying values of $MTBF_{DU}$

It is obvious from the simple approximations that the risk reduction achieved by a safety function is almost directly inversely proportional to the dangerous undetected failure rate of each channel. The relationship between risk reduction and failure rate depends on the level of fault tolerance, the test interval and on the common cause factor β.

Risk reduction is effectively directly proportional to test frequency. The risk reduction can be doubled by inspecting and testing twice as frequently.

Adding one level of fault tolerance improves the risk reduction by one order of magnitude if $\beta \approx 0.1$

The following chart shows how variations in channel $MTBF_{DU}$ will typically affect safety function RRF with annual periodic inspection and testing. The relationship is effectively directly proportional and linear in the commonly used architectures.



$MTBF_{DU} > 30$ years with T = 1 y will generally be enough to achieve RRF > 50 in a 1oo1 architecture. SIL 1 performance can be achieved with a margin of at least x 3.

$MTBF_{DU} \approx 60$ years with T = 1 y is enough to achieve borderline SIL 2 performance in a 1oo1 architecture and borderline SIL 3 performance in a 1oo2 architecture.

Borderline performance leaves no margin for deterioration in equipment condition or in maintenance practices. The safety functions would meet the minimum targets for SIL 2 or SIL 3, but equipment condition and failure performance would need to be monitored closely in operation.

$MTBF_{DU}$ > 200 years with T = 1 y would be enough to achieve a margin of x 3 to allow for some deterioration. Again, 1oo1 would be adequate for SIL 2 and 1oo2 would be needed for SIL3. **SIL 3 performance cannot be expected with a 1oo1 architecture unless the periodic testing is increased to 10 tests per year. Fault tolerance is needed to achieve SIL 3 according to IEC 61511.**

IEC 61508 Route 1_H would allow a single channel architecture subject to constraints on safe failure fraction.

ISO 13849-1 Table 6 and Annex K provide similar guidance for the relationship between $MTTF_D$ and performance levels for varying levels of diagnostic coverage in the designated architectures Category 1 through to Category 4.

PL d (equivalent to SIL 2) can be achieved with $MTTF_D$ ≈ 100 years in a Category 2 (single channel) architecture with 60% diagnostic coverage.

PL e (equivalent to SIL 3) can be achieved with $MTTF_D$ ≈ 100 years in a Category 3 (dual channel) architecture with 90% diagnostic coverage. **A fault tolerant dual channel architecture is always necessary to achieve PL e performance.**

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.

Strictly speaking we should use the rate of **undetected safe failures** that cause a trip condition ($\boldsymbol{\lambda_{SU}}$). 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 usually apply to sensors or final elements. If detected safe failures or detected dangerous failures also cause a trip condition, then those rates should be added to give $STR = \lambda_{SU} + \lambda_{SD} + \lambda_{DD}$.

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 $STR = 3.\lambda_S$

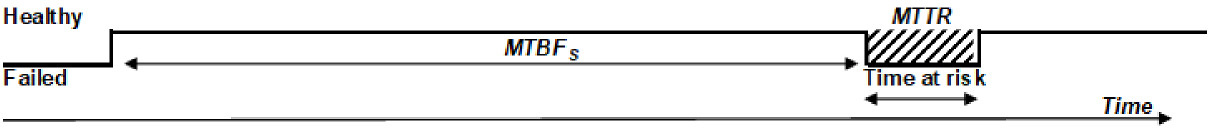
1ooN $STR = N.\lambda_S$

NooN Spurious trip rate

NooN architectures are applied to reduce the likelihood of spurious trip.

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 **3oo3 voting** 3 coincident safe failures are needed before a spurious trip occurs.

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 (the only 1 left) x the FDT:

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

2ooN Spurious trip rate

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.λ_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

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

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

To complete the 2ooN equation a **common cause failure term** must be added. It cannot usually be ignored because (β . λ_S) >> λ_S^2.

The rate of dangerous detected failures $\boldsymbol{\lambda_{DD}}$ could also be added, ***if*** detected failures lead to a trip:

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

MooN Spurious trip rate

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

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

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

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

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

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

The MoonSIF spreadsheet assumes that spurious trip occurs only for undetected safe failures.

A common cause failure term is added to complete the equation that is used in the spreadsheet:

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

The table of MooN scaling factors for β is applied differently for spurious trips.

The rows in the table correspond to the number of channels that are required to operate correctly for the function to act as specified. The columns correspond to N, the total number of channels.

A MooN architecture needs a minimum of M channels in the trip state to trip successfully on demand. The β scaling factor used for PFD calculations is taken from the Mth row and the Nth column.

A MooN architecture will trip spuriously if at least M channels have undetected safe failures putting them into the trip state. The remaining N-M channels might be in a normal healthy state or they might have dangerous faults that prevent trip. N-M**+1** channels are required to be in a non-trip state to avoid spurious trip. The β scaling factor used in estimating the overall spurious trip rate is therefore taken from the (N-M+1)th row and the Nth column.

References

TABLE 1. STANDARDS AND CODES

Number and date	Title
IEC 60812: 2018	Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)
IEC 61508: 2010	Functional safety of electrical/electronic/programmable electronic safety-related systems
IEC 61511: 2016	Functional safety — Safety instrumented systems for the process industry sector
IEC 61709:2017	Electronic components – Reliability – Reference conditions for failure rates and stress models for conversion
IEC 62061: 2021	Safety of machinery – Functional safety of safety-related control systems
ISA-TR84.00.04-2020 Part 1	Guidelines for the Implementation of ANSI-ISA-61511-1:2018
ISO/TR 12489: 2013	Petroleum, petrochemical and natural gas industries — Reliability modelling and calculation of safety systems
ISO 13849-1: 2015	Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design
ISO 13849-2: 2012	Safety of machinery — Safety-related parts of control systems — Part 2: Validation
ISO 14224: 2016	Petroleum, petrochemical and natural gas industries — Collection and exchange of reliability and maintenance data for equipment

TABLE 2. BIBLIOGRAPHY

Ref	Title
1	Smith, D. J. *‘Reliability, Maintainability and Risk’*, 10th Ed. Butterworth Heinemann. 2021
2	OREDA ‘*Offshore Reliability Data Handbook’* Volume 1, 5th Ed. SINTEF. 2009
3	OREDA ‘*Offshore and Onshore Reliability Data Handbook*’ Volume 1, 6th Ed. SINTEF. 2015
4	*exida* Safety Equipment Reliability Handbook (‘SERH’), 3rd Ed. 2007
5	*exida* Safety Equipment Reliability Handbook (‘SERH’), 4th Ed. 2015
6	Bukowski, J.V. and Stewart, L. *‘Quantifying the Impacts of Human Factors on Functional Safety’ exida.*

Ref	Title
	Presented at the American Institute of Chemical Engineers' 12th Global Congress on Process Safety, Houston, Texas. 2016
7	SINTEF Reliability Prediction Method for Safety Instrumented Systems PDS Method Handbook. 2013
8	SINTEF Reliability Prediction Method for Safety Instrumented Systems PDS Data Handbook. 2021
9	SINTEF report A26922, *'Common Cause Failures in Safety Instrumented Systems; Beta-factors and equipment specific checklists based on operational experience. '*, 2015
10	Moubray, J., *'Reliability-Centered Maintenance RCM 2.1'*, 2nd Ed. Butterworth-Heinemann, 1999
11	Florent Brissaud, Anne Barros, Christophe Bérenguer. '*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** >).
12	Jahanian, Hamid. '*Generalizing PFD formulas of IEC 61508 for KooN configurations*'. ISA Transactions 56 pp 168-174. 2015
13	The 61508 Association, T6A042 *Development Paper – Effects of Proof Testing* Version 0.2, February 2022

Abbreviations

TABLE 3. ABBREVIATIONS

Abbrev.	Description
β	The fraction of undetected failures that have a common cause
β_D	Of those failures that are detected by the diagnostic tests, the fraction that have a common cause
β_{MooN}	The fraction of undetected failures that have a common cause in a MooN architecture
CCF	Common Cause Failure
DC	Diagnostic Coverage
FMEA	Failure Modes and Effects Analysis
FMEDA	Failure Modes, Effects and Diagnostics Analysis
λ	Failure Rate Subscripts: S – Safe, SD – Safe Detected, SU– Safe Undetected D – Dangerous, DD – Dangerous Detected, DU– Dangerous Undetected, DN – Dangerous Never Detected NE- No Effect Note that ISA S84 uses superscripts instead of subscripts
LNG	Liquefied natural gas
MooN	'M' out of 'N' voting: at least M channels are required for successful operation
MRT	Mean Repair Time (= time to organise the repair after a failure has been found and then repair and restore the device to service)
MTBF	Mean Time Between Failures
MTTF	Mean Time To Failure (= MTBF + MTTR)
MTTR	Mean Time To Restoration (= time to diagnose a failure plus the MRT)
OREDA	Offshore and Onshore Reliability Data
PF_{inst}	Probability of Failure (Instantaneous)
PFD_{AVG}	Average Probability of Failure on Demand
PFD_G	Average Probability of Failure on Demand for a group of channels or devices
PFH_{AVG}	Average Probability of Failure per Hour (equivalent to failure rate per hour)
PTC	Proof Test Coverage

Abbrev.	Description
RCM	Reliability Centred Maintenance
RRF	Risk Reduction Factor
SERH	Safety Equipment Reliability Handbook (*exida*)
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SINTEF	Norwegian: *Stiftelsen for industriell og teknisk forskning*, The Foundation for Scientific and Industrial Research
SIS	Safety Instrumented System
SFF	Safe Failure Fraction
t	Time
t_{CE}	Channel Equivalent Downtime
T_1	Proof Test Interval
T_2	Full Proof Test Interval (if inspection and testing at T_1 has limited coverage)
T_M	Mission Time (intended lifetime before replacement or renewal)
TIF	Test Independent Failure (failures not found by testing)