# REASSESSING FAILURE RATES

**M. Generowicz, MIET, MIEAust, TÜV Rheinland FS Senior Expert**

**A. Hertel, AMIChemE**

**I&E Systems Pty Ltd**

## SUMMARY

In the context of process industries, automated safety functions are applied to achieve hazard risk reduction at industrial facilities.

The 2016 edition of the functional safety standards IEC 61511-1[1] places a strong emphasis on the need to obtain credible failure rate data for use in failure probability calculations. However, these calculations are flawed because the basic assumptions underlying them are invalid:

- Failures are almost never purely random, and as a result
- Failure rates are **not** fixed and constant.

At best, the calculations provide an order of magnitude estimate for the probability of failure. Nevertheless, even with such imprecise results the calculations are still useful.

Over the past several decades, enough information has been collected to enable failure rates to be estimated for all of the commonly used components in safety functions. The information shows the failure rates that are being achieved in practice. It also shows that the failure rates measured for any particular type of device vary by at least an order of magnitude. The variation depends largely on the service, operating environment and maintenance practices.

The failure rates from industry databases are useful in demonstrating the feasibility of the risk reduction being targeted by safety functions, which is important in setting an operational reliability benchmark.

The failure rates measured from a facility's maintenance data are useful in demonstrating the risk reduction that a safety function can achieve, for a given operating service, environment and set of maintenance practices.

Most failures in safety function components (including software) are predictable, preventable or avoidable to some degree, suggesting that many failures are mostly systematic in nature. Therefore, safety function reliability performance can be improved through four key strategies:

1. Eliminating systematic and common-cause failures throughout the design, development and implementation processes and throughout operation and maintenance practices.
2. Designing the equipment to allow access to enable sufficiently frequent inspection, testing and maintenance, and to enable suitable test coverage.
3. Deployment of risk-based inspection and condition-based maintenance techniques to:
    - Identify and then control conditions that induce early failures,
    - Actively prevent common-cause failures.
4. Disciplined use of root cause analysis for all failures to prevent recurrence.

## FUNCTIONAL SAFETY OBJECTIVES

The basic purpose of functional safety is to provide defined levels of risk reduction for the hazards associated with some sort of equipment. That equipment could be a machine used by a human operator. It could be part of a plant that produces, handles or stores hazardous materials such as chemicals.

Either way, the levels of risk reduction are determined within a company's overall risk management framework to ensure that the overall risk to people is as low as reasonably practicable.

Functional safety relies on systems of electrical, electronic or programmable functions and interlocks. These systems can be complicated and subject to hidden or latent failures. There is always some chance that the systems will not work effectively when a hazardous event occurs.

The fundamental question is this:

> ***How can we be confident that our functional safety system will reliably achieve the risk reduction that we need?***

Functional safety maintains safety integrity of assets in two ways:

**Systematic safety integrity** deals with preventable failures. These are failures resulting from errors and shortcomings in the design, manufacture, installation, operation, maintenance and modification of the safeguarding systems.

**Hardware safety integrity** deals with controlling random hardware failures. These are the failures that occur at a reasonably constant rate and are completely independent of each other. They are not preventable and cannot be avoided or eliminated, but the probability of these failures occurring can be calculated.

## CALCULATION METHODS

Functional safety depends on an objective demonstration that the automated safety systems can reliably achieve the specified risk reduction.

The order of magnitude of the risk reduction factor (RRF) required determines the safety integrity level (SIL) of a safety function:

| | |
|---|---|
| RRF range 10 to 100 | SIL 1 |
| RRF range 100 to 1,000 | SIL 2 |
| RRF range 1,000 to 10,000 | SIL 3 |

The risk reduction is inversely proportional to the probability of failure on demand (PFD). A safety function with a PFD of 0.01 achieves a RRF of 100.

IEC 61508-6:2010 Annex B[2] provides basic guidance on evaluating probabilities of failure. State-of-the-art methods for reliability calculations are described in more detail in the Technical Report ISO 12489 '*Petroleum, petrochemical and natural gas industries — Reliability modelling and calculation of safety systems'.*[5]

Several other useful references are available on this subject, including:

ISA-TR84.00.02-2015 *'Safety Integrity Level (SIL) Verification of Safety Instrumented Functions'*[6]

SINTEF 2013 *'Reliability Prediction Method for Safety Instrumented Systems – PDS Method Handbook'*[7].

These calculation methods enable users to estimate of the PFD for safety functions and the corresponding RRF achieved.

The calculations are all based on the assumptions that:

- Dangerous undetected failures of the devices that are used to make up the safety function can be characterised by fixed constant failure rates $\lambda_{DU}$
- Failures occurring within a population of devices are independent events

The basic assumption is that if dangerous undetected failures occur independently at a fixed rate within a population of similar components then undetected failures will accumulate exponentially. The PFD of each component is directly proportional to the number of failures that have accumulated. It can be estimated as:

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

The PFD of an overall system of devices or components can be estimated by applying probability theory to combine the PFD of the individual components.

## HARDWARE FAULT TOLERANCE

The functional safety standards IEC 61508 and IEC 61511 recognise that there is always some degree of uncertainty in the assumptions made in calculation of failure rate and probability. For this reason the standards specify a minimum level of fault tolerance (i.e. redundancy) in the architectural design of the safety functions. The required level of redundancy increases with the risk reduction required.

Designers aim to minimise the level of fault tolerance because the addition of fault tolerance increases the complexity and cost of safety functions. It also increases the likelihood of inadvertent or spurious action, which in itself may lead to increased risk of hazards.

IEC 61508 provides two strategies for minimising the required hardware fault tolerance:

- Increasing the coverage of automatic and continuous diagnostic functions to reduce the rate of failures that remain undetected (‘Route $1_H$’)
- Increasing the confidence level in the measured failure rates to at least 90% (‘Route $2_H$’).

A confidence level of 90% effectively means that there is only a 10% chance that the true average failure rate is greater than the estimated value.

IEC 61511 adopts a strategy that is consistent with Route $2_H$ though it requires only a confidence level of 70%. However, IEC 61511 also requires documentation showing that the failure rates are credible, based on field feedback from a similar operating environment.

## FAILURE RATE CONFIDENCE LEVEL

If all of the failures for a given type of equipment are recorded the failure rate $\lambda$ can be estimated with any required level of confidence by applying a $\chi^2$ (chi-squared) distribution. The failure rate estimated with confidence level of ‘a’ is designated $\lambda_a$. The confidence level indicates the chance that the actual average failure rate is less than or equal to the estimated rate.

The ratio of $\lambda_{90\%}$ to $\lambda_{70\%}$ depends only on the number of failures recorded. It does not depend directly on the failure rate itself or on the population size. The width of the uncertainty band becomes narrower with each recorded failure. With a higher failure rate or a larger population failures will occur more frequently so the confidence level will improve more quickly. A good estimate for λ can be obtained with as few as 3 failures. If 10 or more failures have been recorded the overall confidence is increased; $\lambda_{90\%}$ will be no more than about 20% higher than $\lambda_{70\%.}$

After about 5 failures have been recorded there is enough information to tell whether the failure rate seems to be reasonably constant or whether it appears to be increasing or decreasing. Guidance is given in IEC 60605-6:2007 *Equipment reliability testing Part 6: Tests for the validity and estimation of the constant failure rate and constant failure intensity*[2].

## FAILURE RATE SOURCES

The Offshore and Onshore Reliability Data (OREDA) project provides a useful source of failure rate information. The website www.oreda.com explains that:

> *'OREDA is a project organization sponsored by eight oil and gas companies with worldwide operations. OREDA's main purpose is to collect and exchange reliability data among the participating companies and act as The Forum for co-ordination and management of reliability data collection within the oil and gas industry. OREDA has established a comprehensive databank with reliability and maintenance data for exploration and production equipment from a wide variety of geographic areas, installations, equipment types and operating conditions.'*

The preface to the OREDA handbooks clarifies that the failures considered are from the normal steady state operating period of equipment. In general the data exclude infant mortality failures and end-of-life failures.

The failure rate tables published by OREDA[11] show that failure rates recorded by different users typically vary over one or two orders of magnitude. OREDA fits the reported failure rates into Gamma distributions to estimate the overall mean failure rate and standard deviation for each type of equipment and type of failure.

The tables also show the upper and lower limits of a 90% *uncertainty* interval for the reported failure rates. This is the band stretching from the 5% certainty level to the 95% certainty level. The certainty level is not the same as the confidence level relating to a single dataset, but the intent is similar.

The average failure rates recorded by 95% of users are less than or equal to the upper limit of the 90% interval. The mean and standard deviation allow users to interpolate rates that might be achieved with a certainty of 70% or 90%.

Two other widely used sources of failure rate data are the SINTEF *PDS Data Handbook*[8] and the *exida* failure rate database in *exSILentia* software. The *exida* database is also published in the *exida Safety Equipment Reliability Handbook*[12].

The failure rates in both of these references are reasonably consistent with the OREDA data.

## VARIABILITY IN FAILURE RATES

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

One reason for the variability in rates is that these datasets include all failures, systematic failures as well as random failures.

The wide variability in failure rates has been understood for many years. W. Goble and J. Siebert published an informative white paper on this topic in 2008: '*Field Failure Data – the Good, the Bad and the Ugly*'[15].

## RANDOM FAILURE AND SYSTEMATIC FAILURE

It is important to understand the distinction between random failure and systematic failure.

The definitions for random failure vary between the different standards and references but they are generally consistent with the dictionary definitions of the word 'random':

> '*Made, done, or happening without method or conscious decision*; *haphazard.*'

ISO/TR 12489:2013[5] Annex B explains that both hardware failures and human failures can occur at random. It makes it clear that not all random failures occur at a constant rate.

Constant failure rates are typical in electronic components before they reach the end of their useful life.

Random failures of mechanical components are caused by deterioration due to age and wear **and the failure rates are not constant**.

The reference book *'Safety instrumented systems verification: practical probabilistic calculations'* by Goble and Cheddie[14] includes a typical failure modes, effects and diagnostics analysis (FMEDA) for an actuated ball valve. The FMEDA reveals that virtually all of the failure modes of actuated valves are associated with damage to components.

The failure rates of mechanical components depend on the age of the equipment, wear and tear, severity of service and on the effectiveness of maintenance programs.

The definitions of random failure in ISA TR84.00.02-2015[6], IEC 61508-4:2010[3] and IEC 61511-1:2016[1] are all similar:

> *'…failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware'*

The mathematical analysis of failure probability is based on the concept of a 'random process' or 'stochastic process'. In this context the usage of the word random is narrower. For the mathematical analysis these standards all assume that:

> '*failure rates arising from random hardware failures, can be predicted with reasonable accuracy*'.

Failures that occur at a fixed constant rate are purely random, but in practice only a small proportion of random failures are purely random.

The following definition of a **purely random process** was taken from '*A Dictionary of Statistical Terms*', by F.H.C Marriott[16]:

> *'The simplest example of a stationary process where, in discrete time, all the random variables z, are mutually independent. In continuous time the process is sometimes referred to as "white noise", relating to the energy characteristics of certain physical phenomena.'*

The key difference is the requirement for mutual independence. Failures due to damage or deterioration from wear and age are not mutually independent.

By contrast, the standards note that systematic failures cannot be characterised by a fixed rate (though to some extent the probability of systematic faults existing in a system may be estimated).

The standards are reasonably consistent in their definition of systematic failure:

> *'…failure related in a deterministic way to a certain cause or pre-existing fault. Systematic failures can be eliminated after being detected while random hardware failures cannot.'*

In the ISA TR84.00.02-2015[6] definition systematic failures are only deterministic to an extent:

> *'Unfortunately, since systematic failures are often related to human error, it is difficult to predict when and how frequently they can occur. Thus, the failures are deterministic only to an extent, as humans by their very nature are not fully predictable'*

The distinction between random and systematic failures may be difficult to make when the random failures are not purely random. Very few failures are purely random.

The seemingly random failures of mechanical components are related in a partially deterministic way to causes that are well known and understood. To some extent the failures can be prevented if the degradation is monitored.

Degradation of mechanical components is not usually a purely random process. Degradation can be monitored. It might be theoretically possible to prevent failure from degradation but it is simply not practicable to prevent all failures. Inspection and maintenance can never be perfect.

It is common practice to treat these failures as quasi-random to the extent that they are not eliminated through maintenance, overhaul and renewal.

They are characterised by a constant failure rate even though that rate is not fixed.

The reasons for the wide variability in reported failure rates seem to be clear:

- Only a small proportion of failures occur at a fixed rate that cannot be changed
- The failure rates of mechanical components vary widely depending on service and on effectiveness of maintenance
- The failure rates of mechanical components can only be predicted with any reasonable accuracy within a given environment and maintenance regime
- The rates of systematic failures vary widely from user to user, depending on the effectiveness of the quality management practices
- No clear distinction is made between systematic failure and random failure in the reported failures.

## COMMON CAUSE FAILURE

Where hardware fault tolerance is provided the common cause failures of redundant devices are modelled assuming a common cause factor, β. This is a fixed constant factor representing the fraction of failures with a common cause that will affect all of the devices at about the same time.

Common cause failures are never purely random because they are not independent events. These failures are largely systematic and preventable.

The SINTEF Report A26922 '*Common Cause Failures in Safety Instrumented Systems*'[10] shows that in practice β for final elements (such as shutdown valves) is more than 10%.

## WRONG BUT USEFUL

The SINTEF Report A26922 includes the pertinent quote from George E.P. Box:

> *'Essentially, all models are wrong, but some are useful'*

The quote is in the context of a discussion regarding different models that may be used to estimate the common cause factor, β. Similarly we can conclude that although the models used for calculating PFD are wrong they are still useful.

The OREDA failure statistics show that failure rates of mechanical components are not fixed and constant, and the band of uncertainty spans more than one order of magnitude. The statistics suggest that the failure rates of sensors are also not constant.

The published failure rates are useful as an indicator of failure rates that can easily be achieved in practice.

The PFD cannot be calculated with precision because the failure rates are not constant. It is misleading to report calculated PFD with more than one significant figure of precision.

Application of Markov models, Petri nets and Monte Carlo simulations leads to an unfounded expectation of precision. The results are much more precise, but no more accurate. The detailed guidance given by ISO/TR 12489[5] is misleading because it implies that the precision is meaningful.

The PFD calculated for any safety function should be considered to be only an order-of-magnitude estimate. This is sufficiently precise to estimate the risk reduction factor with at best one significant figure of precision. That precision is enough to categorise the function by the safety integrity level (SIL) achieved.

The failure rate that is assumed in the calculation can then be used to set a useful benchmark for the failure rate to be achieved in operation.

Proof test coverage is considered when calculating PFD. Though the effect of the proof test coverage cannot be calculated with any meaningful precision the calculation is still very useful. It illustrates the relative impact of proof test coverage and is useful in guiding the design of proof testing facilities and procedures.

## WRONG AND MISLEADING

The simplified PFD equations given in Table C.1 of ISA TR84.00.02-2015[6] are misleading because the common cause failure terms are excluded. The exclusion can rarely be justified.

With voted architectures the common cause failure term will usually only become insignificant if the β-factor can be reduced to much less than 1%.

The SINTEF Report A26922[10] suggests that in practice the common cause failure fraction can be expected to be greater than 10%. Typical values achieved are in the range 12% to 15%.

With typical failure rates the simplified PFD equation terms for voted architectures given in the ISA table C.1 will usually be around an order of magnitude smaller than the common cause failure term.

For example, consider a safety function using actuated valves in a 1oo2 (i.e. 1 out of 2) architecture as the final elements. A typical value for the rate of undetected dangerous failures $\lambda_{DU}$ in an actuated valve assembly is around 0.03 failures per annum (approximately 1 failure in 30 years, or around 3 failures per $10^6$ hours). The average PFD of the valve subsystem may be approximated by:

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

The last term in this equation represents the contribution of common cause failures and usually strongly dominates the result. It will be negligible only if the following is true:

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

If the test interval T is 1 year and $\lambda_{DU}$ = 0.03 pa, then the common cause failure term will be greater than the first term unless $\beta < 2\%$.

For the common cause failure term to be negligible the test interval T would usually have to be significantly longer than 1 year and/or the β-factor would have to be much less than 2%.

It is clear that the PFD depends most heavily on these three factors: β, $\lambda_{DU}$ and T.

## SETTING FEASIBLE TARGETS

During the architectural design of safety functions the PFD is calculated to show that it will be feasible to achieve and maintain the required risk reduction.

In the process sector the final elements are usually actuated valves, though some safety functions may be able to use electrical contactors or circuit breakers as final elements.

The example value of 0.03 pa quoted above for $\lambda_{DU}$ is a typical failure rate that is feasible to achieve for infrequently operated actuated valves. For contactors or circuit breakers it is feasible to achieve failure rates in the order of 0.01 pa.

The SIL 1 range of risk reduction can be achieved without hardware fault tolerance (i.e. 1oo1 architecture) using either a valve or contactor.

It is feasible to achieve the SIL 2 range of risk reduction with 1oo1 architecture, but the PFD may be marginal particularly if a valve is used as the final element. If actuated valves are used attention will need to be given to minimising $\lambda_{DU.}$ Alternatively the PFD may be reduced by reducing the interval between proof tests, T. If these parameters cannot be minimised it may be necessary to use a 1oo2 architecture for the final elements in order to achieve SIL 2.

For SIL 3 risk reduction it will always be necessary to use at least a 1oo2 architecture because of the IEC 61511 requirement for hardware fault tolerance. If the final elements are actuated valves then the β-factor and $\lambda_{DU}$ will need to be minimised to achieve even the minimum risk reduction of 1,000.

This will result in design requirements that improve independence (reducing β) and facilitate inspection, testing and maintenance (reducing $\lambda_{DU}$ and improving test coverage). If reducing β and $\lambda_{DU}$ is not sufficient it may also be necessary to shorten the test interval T.

The end result of the PFD calculations is a set of performance targets for β, $\lambda_{DU}$ and T.

## MEASURING PERFORMANCE AGAINST BENCHMARKS

IEC 61511-1 §5.2.5.3 requires operators to monitor and assess whether reliability parameters of the safety instrumented systems (SIS) are in accordance with those assumed during the design. §16.2.9 requires operators to monitor the failures and failure modes of equipment forming part of the SIS and to analyse discrepancies between expected behaviour and actual behaviour.

The SINTEF Report A8788 *Guidelines for follow-up of Safety Instrumented Systems (SIS) in the operating phase*[9] provides useful guidance on the analysis of failures recorded during operation of a plant.

The guidelines suggest setting target values for the expected number of failures based on the failure rates assumed in the design.

If the actual measured failure rates are higher than the target it is necessary to analyse the cause of the failures. Compensating measures to reduce the number of future failures must be considered.

The need for increased frequency of inspection and testing should also be considered, but it is not sufficient to rely on increased frequency of testing alone.

## ANTICIPATING RATHER THAN MEASURING FAILURES

It may be difficult to measure meaningful failure rates on some types of critical equipment. If the random hardware failure rates are relatively low and the population of devices is small there may be too few failures to allow a rate to be measured.

In a hypothetical example the operator of a plant has had only 7 high voltage circuit breakers in service since 1998. Only one failure was recorded in 2010 when a circuit breaker failed to trip.

One of these circuit breakers acts a final element in a safety function so its failure rate must be evaluated and monitored.

With 7 breakers in continuous service for 20 years the average failure rate is about $9 \times 10^{-7}$ failures per hour. This failure rate is similar to the failure rates reported in the SINTEF *PDS Data Handbook* but no conclusions can be drawn from this about the current failure rate. After 20 years we cannot assume that the condition of the equipment is acceptable and that the target failure rate is being met.

With only a single failure having been recorded the 90% confidence interval spans more than an order of magnitude:

$$\lambda_{5\%} \approx 3 \times 10^{-7} \text{ per hour} \qquad \lambda_{95\%} \approx 4 \times 10^{-6} \text{ per hour}$$

Without a detailed analysis of the failure there is not enough information to determine whether the failure can be classed as purely random.

There is no evidence to suggest that the failure rate is constant. There is not enough information to predict what the failure rate will be over the next few years. The circuit breaker that failed to trip was already 12 years old when the failure was recorded. The circuit breakers are now 20 years old.

As a minimum detailed inspection and testing is required to assess the condition of the equipment. Overhaul, renewal or replacement may be required.

Most of the modes of failure should be predictable and it should be feasible to prevent failures through condition based maintenance.

A FMEDA study can identify the key parameters that need to be monitored to detect deterioration and incipient failure. The uncertainty in failure rate can be mitigated through a better understanding of the likely failure modes of components and of the measurable conditions that are symptomatic of component deterioration. The likelihood of failure depends on the condition of the components.

The equipment manufacturer can also recommend techniques and measures to assess the condition of the equipment and the requirements for renewal.

## DESIGNING FOR TESTABILITY AND MAINTAINABILITY

A common problem for plant operators is that the plants are designed to minimise initial construction cost. The equipment is not designed to facilitate accessibility for testing or for maintenance.

For example on LNG compression trains access to the equipment is often constrained. Some critical final elements can only be taken out of service at intervals of 5 years or more.

Even if the designers have provided facilities to enable on-line condition monitoring and testing, the opportunities for corrective maintenance are severely constrained by the need to maintain production. Deteriorating equipment has to remain in service until the next planned shutdown.

It is common practice to install duty/standby pairs of pumps and motors where it is critical to maintain production. The 2oo3 voting architecture used for safety function sensors fulfils a similar purpose. It facilitates on-line testing of sensors. It is not common practice to provide duty/standby pairing for safety function final elements, but it is possible. Duty/standby service can be achieved at by using 2 x 1oo1 or 2oo4 architectures. The justification for the additional cost depends on the value of process downtime that can be avoided.

If duty/standby pairing is not provided for critical final elements then accessibility for on-line inspection, testing and maintenance must be considered in the design.

A safety function cannot provide any risk reduction if it is bypassed or taken out of service during normal plant operation. The probability of failure on demand is directly proportional to the proportion of time that the safety function is out of service (characterised as mean time to restoration, MTTR).

This can be seen as an extension of safety-by-design principles, designing the systems to enable failures to be found and eliminated. Designing the system to facilitate inspection, testing and maintenance enables both the $\lambda_{DU}$ and the MTTR to be minimised in operation.

Consider the example of a set of double block shutdown valves in a 1oo2 arrangement on an LNG train. After 3 years of operation deterioration is detected in the stem seals of both valves. Partial stroke testing reveals that the valve stroking times have increased to beyond the specified limit. The next available opportunity for maintenance is in 2 years' time. The safety functions that depend on those valves are now effectively out of service.

## PREVENTING PREVENTABLE FAILURES

### Preventing systematic failures

All of the major accident reports and the many 'what went wrong' studies[13][17] have shown that all major accident events are caused by multiple systematic failures. Not even one single major hazard event has been caused by purely random failure.

Bob Weiss discussed the prominence of systematic failures in the paper *'Are any failures "random"? – A major question in Functional Safety'* presented at the IChemE Hazards Australasia conference in 2016[18]. The paper included these conclusions:

> *'Rather than focussing on the PFDavg of a device it is of more critical importance to manage and address human factors in order to achieve and maintain the required SIL.* […]
>
> *'Perhaps it would be more appropriate to redefine SIL in terms of the basic measures required to control systematic failures at each integrity level. This may at least re-focus organisations on the more important aspects of managing functional safety that reduce systematic failures.'*

Systematic failures cannot be characterised by failure rate. The probability of systematic faults existing within a system cannot be quantified with precision. But by definition, systematic failures can be eliminated after being detected. The implication of this is that systematic failures can be prevented.

Due diligence must be demonstrated in preventing systematic failures as far as is practicable **in proportion to the target level of risk reduction**. Plant owners need to satisfy themselves that appropriate processes, techniques, methods and measures have been applied with sufficient effectiveness to eliminate systematic failures. The attention given to SIL 3 safety functions needs to be proportionately higher than for SIL 1 functions. Owners and operators need to be able to demonstrate that reasonable steps have been taken to prevent failures, and must measure and monitor the effectiveness of those steps.

The main purpose of IEC 61508 and IEC 61511 is to provide management frameworks that facilitate prevention of preventable failures. The standards describe processes, techniques, methods and measures to prevent, avoid and detect systematic faults and resulting failures.

Some failures can be prevented by designing the equipment to suit the service conditions and operating environment. These failures would clearly be categorised as systematic failures.

The principles underlying FMEA can be applied to the management of systematic faults and failures. A methodical approach should be taken to identify common classes and types of systematic fault and failure.

Activities, techniques, measures and procedures can be selected to detect or to prevent faults and failures. IEC 61511-1 §6.2.3 requires planning of activities, criteria, techniques, measures and procedures throughout the safety system lifecycle. The rationale needs to be recorded.

## Preventing ‘random’ failures

This same approach of active prevention should be extended to include the management of the random failures that are not purely random. Most failures that are usually classed as random are actually preventable to some extent. This includes all common cause failures.

## Techniques and measures to avoid or control failure

For guidance on how to plan and apply techniques and measures refer to:

IEC 61508-2:2010 Annexes A and B

IEC 61508-3:2010 Annexes A, B and C

IEC 61508-6:2010 Annex E

IEC 61508-7:2010

# CONCLUSIONS

## Estimating risk reduction

Safety functions are designed to achieve dependable risk reduction. Designers of safety functions estimate the risk reduction by assuming fixed constant failure rates.

## Wide variation in failure data

The precision in the estimates of risk reduction depends on the uncertainty in the failure rates.

OREDA statistics clearly show that the failure rates vary over at least an order of magnitude. The rates are not fixed and constant.

The reported failure rates are an indication of the failure rates that can be feasibly achieved with established practices for operation, inspection, maintenance and renewal.

## Confusion between random and systematic

There is no clear and consistent definition to distinguish random failures from systematic failures.

Very few failures are purely random. Most failures have a certain cause, though the development from fault to failure is not deterministic. Some degree of randomness is involved.

It is not practicable to find and eliminate all systematic failures. Though systematic failures tend to be deterministic they may also involve a degree of randomness.

Most failures fall somewhere in the middle between the two extremes of purely random and purely deterministic. Most failures are preventable if the failure mode can be anticipated and inspections and tests can be designed to detect incipient failure. In practice failures are not completely preventable because access and resources are limited.

Failures are treated as quasi-random to the extent that it is not practicable to eliminate the causes and prevent the failures.

## PFD Calculations set feasible performance benchmarks

The PFD calculations are based on the incorrect assumption that failure rates and the proportion of common cause failures are fixed and constant. Although the assumption is not correct it is a very useful simplification.

The PFD calculations demonstrate the order of magnitude of RRF that is feasible from a safety function, given reasonably effective quality control in design, manufacture, operation and maintenance.

The pertinent question becomes:

> ***How can we be confident that the failure rates of the equipment in operation are no more than the failure rates that were assumed in the PFD calculation?***

## Strategies for improving risk reduction

1. The first priority in functional safety is to eliminate, prevent, avoid or control systematic failures throughout the entire system lifecycle.

   Prevent the preventable failures by applying conventional quality management and project management practices.

   This includes designing and specifying the equipment to be suitable for the intended service conditions and the intended function.

   The level of attention to detail and the effectiveness of the processes, techniques and measures must be in proportion to the target level of risk reduction. SIL 3 functions need much stricter quality control than SIL 1 functions.

   This involves subjective judgement because the effectiveness cannot readily be quantified. The planning of processes, techniques and measures should be methodical and based on an understanding of the systematic faults that are likely to occur.

2. The second priority in functional safety is to enable early detection and effective treatment of the deterioration that cannot be prevented.

   The failure causes and failure modes of conventional safety equipment are well understood.

   The design of the safety functions needs to take into account the failure modes and to include requirements for accessibility for diagnostics, inspection, testing, maintenance and renewal.

   The requirements for accessibility depend on the target failure rates that need to be achieved in order to deliver the target risk reduction. The requirements also depend on the cost of downtime. SIL 3 safety functions must be designed to enable ready access for inspection, testing and maintenance.

   The planning for inspection and testing should be in proportion to the target level of risk reduction.

   The planning for maintenance and renewal should be in proportion to the target level of risk reduction and should be based on the measured condition of the equipment.

3. Avoidance and prevention of common cause failures is of primary importance in the design and operation of safety functions.

   The control of common cause failures is more important than the measurement of failure rate. Common cause failures dominate the PFD in all voted architectures of sensors and of final elements.

4. The measurement of failure rates in operation provides essential feedback on the effectiveness of the design, inspection, testing, maintenance and renewal.

   The measured failure rates should be compared with the rates assumed in the PFD calculations.

   Root cause analysis is necessary for all failures in order to identify common cause failures and to identify strategies for preventing similar failures in the future.

   If the measured failure rates are higher than the target benchmark then the reasons need to be understood and remedial action taken.

The failure rates for some items of equipment will be too low to measure accurately in a small population of devices. Leading indicators of failure can be developed based on the measurement of deterioration and the anticipation of incipient failure.

## REFERENCES

[1] '*Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements',* IEC 61511-1:2016

[2] '*Equipment reliability testing Part 6: Tests for the validity and estimation of the constant failure rate and constant failure intensity',* IEC 60605-6:2007

[3] *'Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations',* IEC 61508-4:2010

[4] *'Functional safety of electrical/electronic/programmable electronic safety-related systems - Guidelines on the application of IEC 61508-2 and IEC 61508-3',* IEC 61508-6:2010

[5] *'Petroleum, petrochemical and natural gas industries — Reliability modelling and calculation of safety systems',* ISO/TR 12489

[6] *'Safety Integrity Level (SIL) Verification of Safety Instrumented Functions',* ISA-TR84.00.02-2015

[7] 'Reliability Prediction Method for Safety Instrumented Systems – PDS Method Handbook', SINTEF, Trondheim, Norway, Report A24442, 2013.

[8] 'Reliability Prediction Method for Safety Instrumented Systems – PDS Data Handbook', SINTEF, Trondheim, Norway, Report A24443, 2013.

[9] S. Hauge and M. A. Lundteigen, 'Guidelines for follow-up of Safety Instrumented Systems (SIS) in the operating phase' SINTEF, Trondheim, Norway, Report A8788, 2008

[10] S. Hauge *et al*., 'Common Cause Failures in Safety Instrumented Systems', SINTEF, Trondheim, Norway, Report A26922, 2015

[11] *OREDA Offshore and Onshore Reliability Data Handbook Vol 1,* 6th ed. SINTEF Technology and Society: Department of Safety Research, Trondheim, Norway, 2015.

[12] *Safety Equipment Reliability Handbook,* 4th ed. exida.com LLC, Sellersville, PA, 2015

[13] T. Kletz, *What Went Wrong? Case Histories of Process Plant Disasters and How They Could Have Been Avoided,* 5th Edition, Burlington, MA, Butterworth-Heinemann, 2009

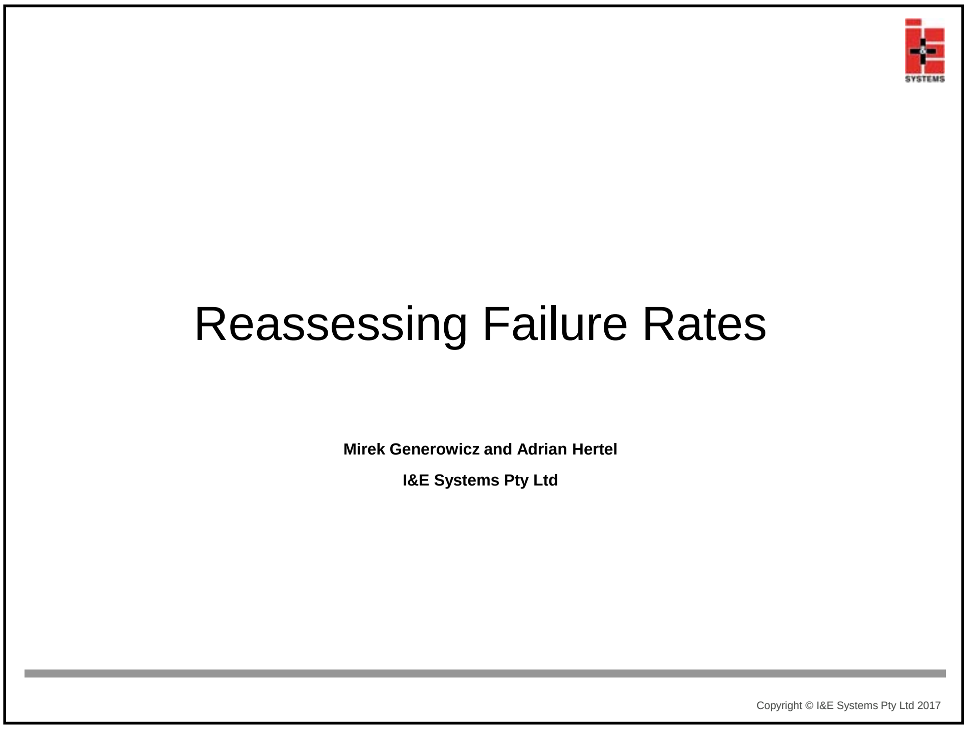
[14] W. M. Goble and H. Cheddie, *Safety instrumented systems verification : practical probabilistic calculations*, Research Triangle Park, NC, ISA, 2005

[15] W. M. Goble and J. F. Siebert, (2008). '*Field Failure Data – the Good, the Bad and the Ugly*' [Online]. Available: http://www.exida.com/Resources/Whitepapers/Field-Failure-Rates-The-Good-The-Bad-The-Ugly

[16] F.H.C. Marriott, '*A Dictionary of Statistical Terms*', 5th Edition, , International Statistical Institute, Longman Scientific and Technical, 1990

[17] Health and Safety Executive UK, (2003). *'Out of control: Why control systems go wrong and how to prevent failure'* [Online]. Available: http://www.hse.gov.uk/pubns/books/hsg238.htm

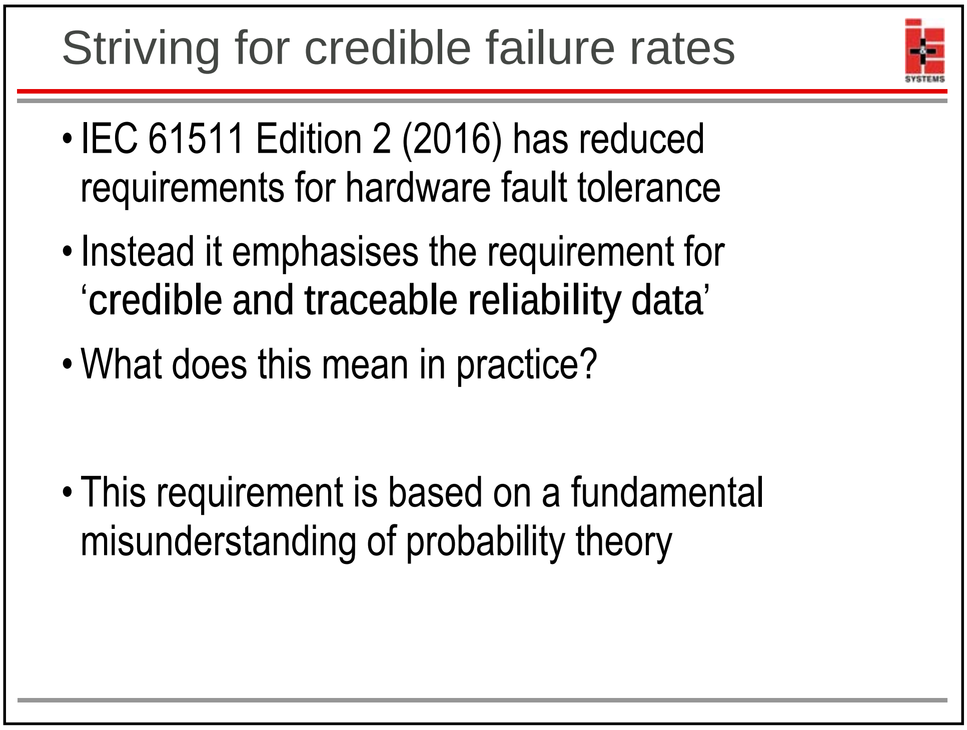
[18] R. Weiss, *'*Are any failures "random"? – A major question in Functional Safety*'* presented at IChemE Hazards Australasia Conference Hazards Australia, Brisbane, Queensland, 2016.



# Reassessing Failure Rates

**Mirek Generowicz and Adrian Hertel**

**I&E Systems Pty Ltd**



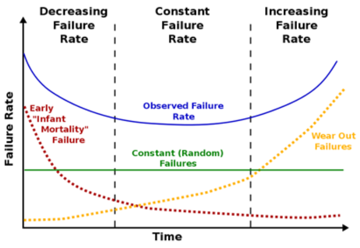
## Striving for credible failure rates

- IEC 61511 Edition 2 (2016) has reduced requirements for hardware fault tolerance
- Instead it emphasises the requirement for ‘credible and traceable reliability data’
- What does this mean in practice?

- This requirement is based on a fundamental misunderstanding of probability theory

## ‘Wrong but useful’

- Failure probability calculations depend on estimates of equipment failure rates
- The basic assumption is that during mid-life the failure rate is constant:



- This assumption is WRONG

…but it is still useful

- We can use failure rates to manage performance even though the rates are not fixed and constant

## What is ‘Functional Safety’?

An introduction for those not familiar with IEC 61511:

In IEC 61511 Functional Safety refers to:

“Safety instrumented systems” (SIS) that implement “Safety instrumented functions” (SIF) as part of a company’s overall risk management strategy

Safety instrumented functions deliver risk reduction

# Risk reduction and SIL

Risk reduction required from safety functions is characterised by risk reduction factor (RRF) and Safety Integrity Level (SIL)

SIL ≈ order of magnitude of RRF

| Safety Integrity Level | Risk Reduction Factor |
|---|---|
| SIL 1 | 10 < RRF ≤ 100 |
| SIL 2 | 100 < RRF ≤ 1,000 |
| SIL 3 | 1,000 < RRF ≤ 10,000 |
| SIL 4 | RRF > 10,000 |

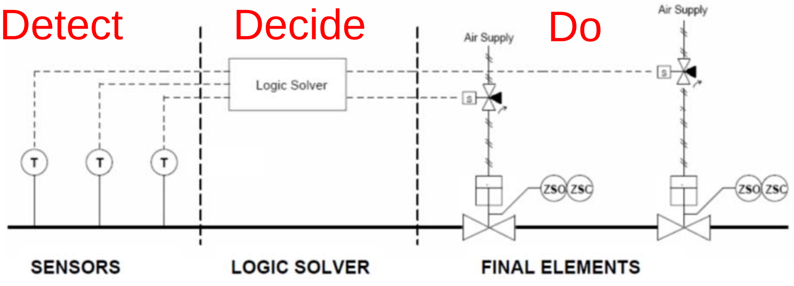
RRF = 1/ PFD, probability of failure on demand

# What is a SIF?

Safety instrumented functions

- Respond to a specific, defined hazard
- Implement a specific action
- Put the equipment into (or maintain) a safe state
- Provide specified risk reduction

Detect Decide Do

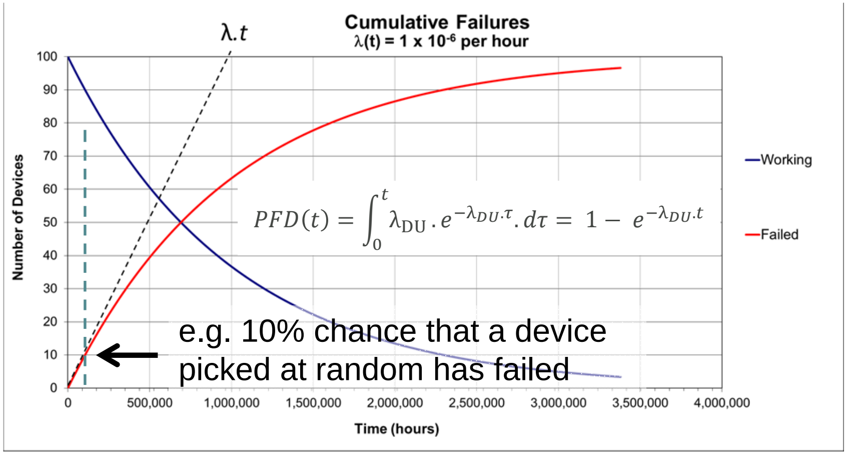


# Safety integrity has two aspects:

- Manage risk of *systematic* failures
  - Prevent errors and failures in design and implementation
  - By applying quality management methods
- Reduce risk of *random* hardware failures
  - For the failures that can’t be effectively prevented
  - Calculate failure probability based on failure rates
  - Reduce the probability of failure to achieve the required risk reduction target
  - Apply fault detection and regular testing
  - Apply redundant equipment for fault tolerance

# Estimating PFD

*If* SIF device failures occur continuously and independently at a constant average rate then accumulation of failures follows an exponential distribution:



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

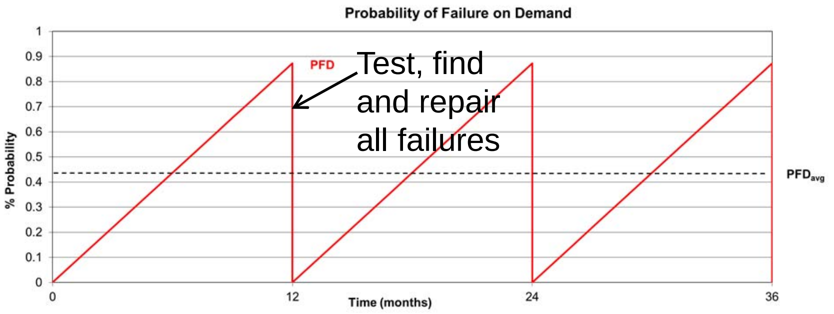
e.g. 10% chance that a device picked at random has failed

# Approximately linear increase in PFD

With a constant rate of undetected dangerous failures $\lambda_{DU}$ and a proof test interval T << 1 / $\lambda_{DU}$

$$PFD_{max} \approx \lambda_{DU}.T$$

$$PFD_{avg} \approx \lambda_{DU}.T / 2$$



Test, find and repair all failures

# Hardware fault tolerance (HFT)

Calculations of failure probability are not enough, because they depend on very coarse assumptions

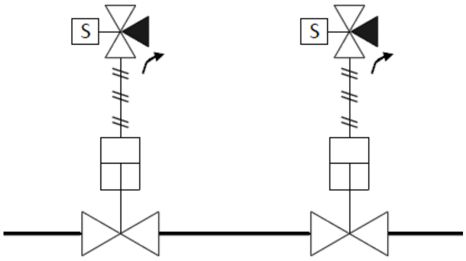
IEC 61511 also specifies minimum requirements for redundancy, i.e. '**Hardware fault tolerance**':

> *'to alleviate potential shortcomings in SIF design that may result due to the number of* ***assumptions made*** *in the design of the SIF, along with* ***uncertainty in the failure rate*** *of components or subsystems used in various process applications'*

## Hardware fault tolerance (HFT)

Fault tolerance requires **redundant** elements:

HFT = 1



Now that we know the basics of functional safety…

## HFT in IEC 61511 Edition 2

New, simpler requirement for HFT

Now allows SIL 3 with only two block valves (HFT =1) and only one block valve for SIL 2

- previously two valves were required for SIL 2

Based on the IEC 61508 ‘Route $2_H$’ method

- new in 2010
- requiring a confidence level of at least 90% in the failure rate $\lambda$, rather than the standard 70%

$\lambda_{AVG}$ = Number of failures recorded / total time in service

But what is the **confidence level**?

# Estimating confidence in $\lambda_{AVG}$

$$\lambda_\alpha = \frac{\chi^2(\alpha,\nu)}{2T}$$

$\chi^2$ = chi-squared function

$\alpha$ = 1- confidence level

$\nu$ = degrees of freedom, in this case = 2.(*n* + 1)

*n* = the number of failures in the given time period

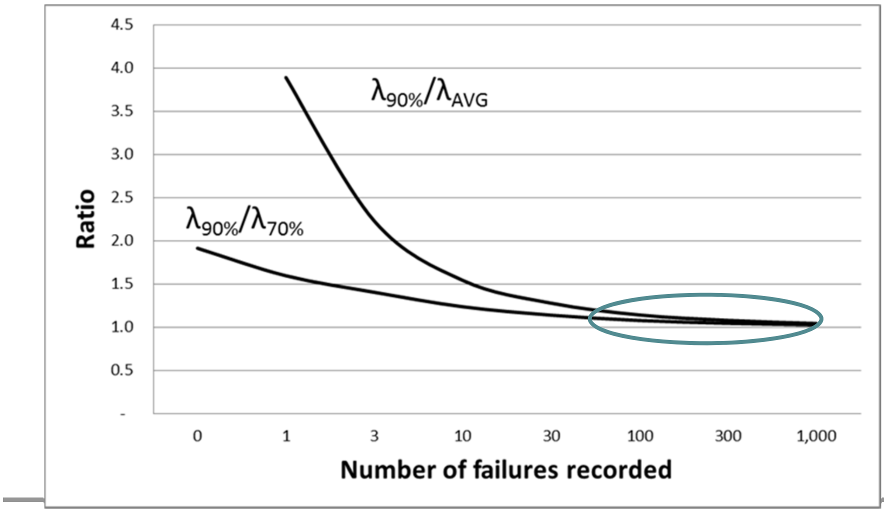
*T* = the number of device-years or device-hours, i.e. the number of devices x the given time period

The confidence level depends heavily on the actual number of failures recorded

It does *not* depend directly on the population size

# $\lambda_{90\%}$ compared with $\lambda_{70\%}$

$$\lambda_{90\%} = \frac{\chi^2(0.1,2n+2)}{2T}$$



## Can we be confident?

- Users have collected so much data over many years in a variety of environments
- Surely by now we can have full confidence in the data

$$\lambda_{90\%} \approx \lambda_{70\%}$$

- Instead of requiring a confidence level of 90% for the reduced HFT, IEC 61511 (2016) requires '**credible failure rate data**' based on field feedback from a similar operating environment

## Where can we find credible data?

An enormous effort has been made to determine λ

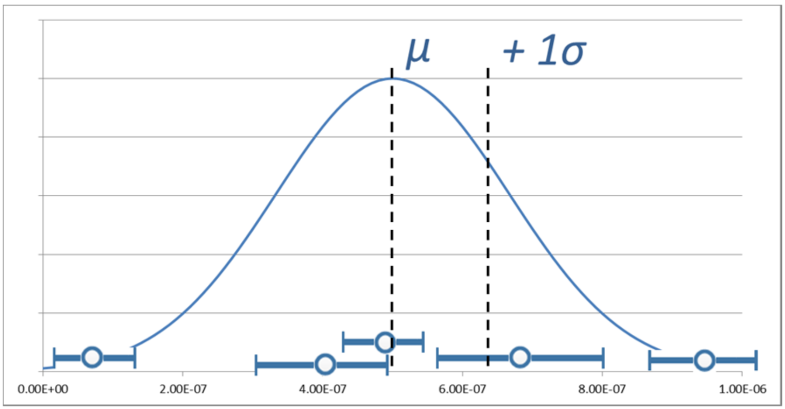
Some widely used sources of λ:

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

## Combining data from multiple sources

OREDA combines data from multiple sources in a probability distribution, but the spread is very wide

Uncertainty intervals span 1 or 2 orders of magnitude

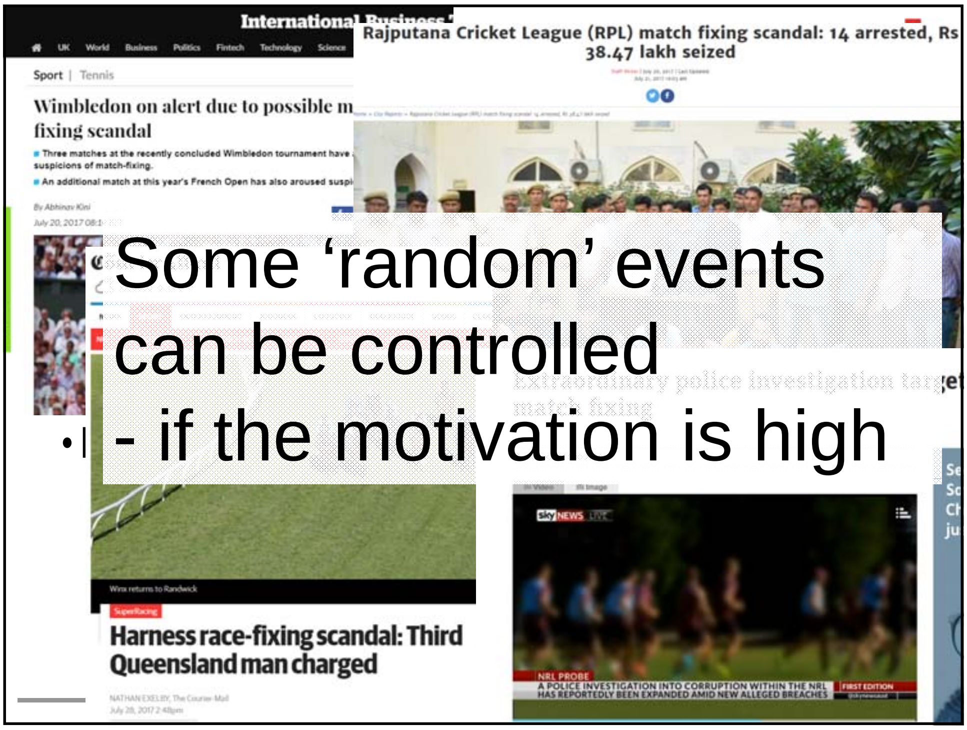


## Wide variation in reported λ

- Why is the variation so wide if λ is constant?

- OREDA includes all mid-life failures,
some are random,
some are systematic (depending on the application)

- How do we define random?
  - Coin toss?
  - Horse race?
  - Football match?



International Business Times

Sport | Tennis

Wimbledon on alert due to possible m

fixing scandal

- Three matches at the recently concluded Wimbledon tournament have suspicions of match-fixing.
- An additional match at this year's French Open has also aroused suspi

By Abhinav Kini

July 20, 2017 08:1

Rajputana Cricket League (RPL) match fixing scandal: 14 arrested, Rs 38.47 lakh seized

Extraordinary police investigation target match fixing

Harness race-fixing scandal: Third Queensland man charged

NATHAN EXELBY, The Courier-Mail

July 28, 2017 2:48pm

NRL PROBE

A POLICE INVESTIGATION INTO CORRUPTION WITHIN THE NRL HAS REPORTEDLY BEEN EXPANDED AMID NEW ALLEGED BREACHES

Some ‘random’ events can be controlled
- if the motivation is high

## What is random?

Dictionary:

Made, done, or happening without method or conscious decision; haphazard

Mathematics:

A **purely random process** involves mutually independent events

The probability of any one event is not dependent on other events

## Guidance from ISO/TR 12489

Random

Hardware – electronic components: constant λ

Hardware – mechanical components: non constant λ (age and wear related failures in mid-life period)

Human – operating under stress, non-routine: variable λ

Systematic - cannot be quantified by a fixed rate

Hardware - specification, design, installation, operation

Software - specification, coding, testing, modification

Human – depending on training, understanding, attitude

## Random or systematic failures?

Pressure transmitters:

- Blocked tubing
- Corroded diaphragm
- Sudden electronic component failure
- Calibration drift due to vibration
- Overheated transducer
- Tubing leak
- Isolation valve closed
- High impedance joint
- Water ingress, partial short circuit
- Supply voltage outside limits
- Age or wear related deterioration? (rate not constant)

# More failure mode examples

- Actuated ball valves
  - Valve stem stuck or seized
  - Stem sheared
  - Actuator jammed
  - Port clogged
  - Tubing leak
  - Air pressure too low
  - Insufficient torque
  - Spring failed
  - Valve seats worn
  - Position switches misaligned

Are any purely random?

# Confusing definitions

Systematic failure:

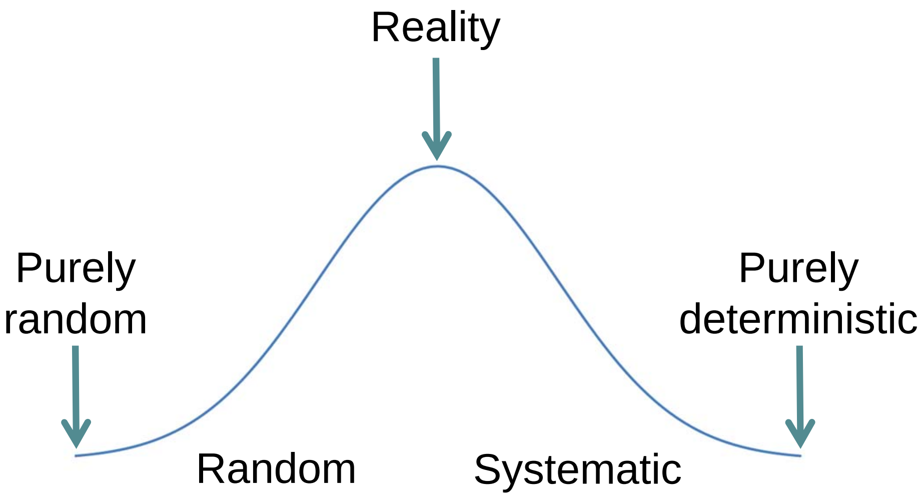
*'…failure related in a* ***deterministic*** *way to a certain cause or pre-existing fault.*

*Systematic failures can be eliminated after being detected while random hardware failures cannot.'*

*'Unfortunately, since systematic failures are often related to human error, it is difficult to predict when and how frequently they can occur. Thus, the failures are* ***deterministic only to an extent, as humans by their very nature are not fully predictable****'*

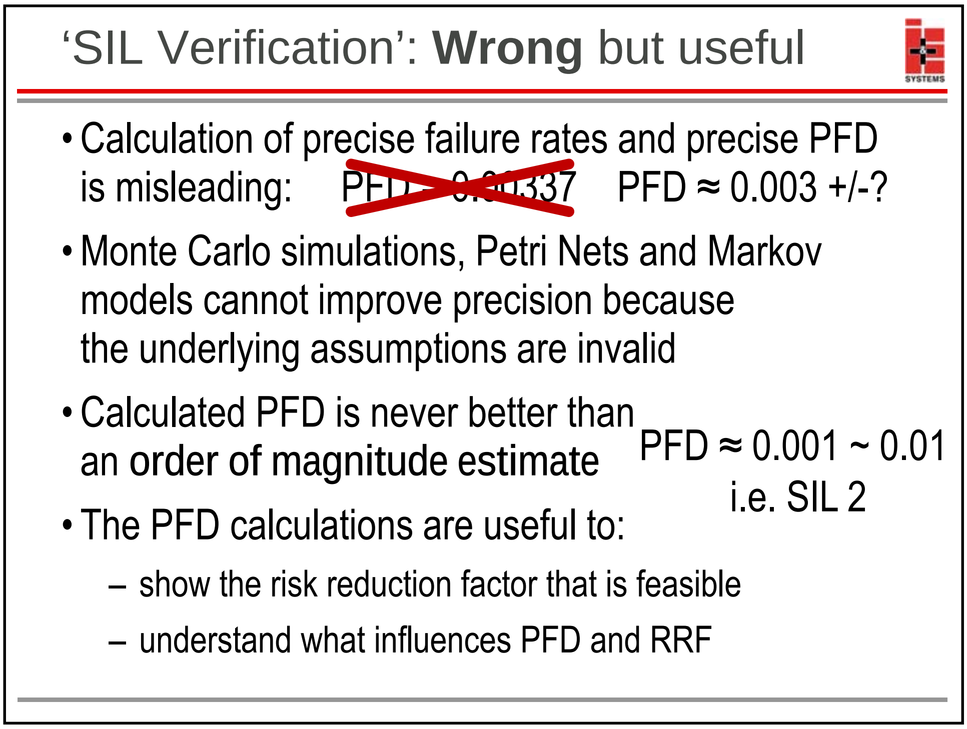
## Somewhere in the middle

Most failures are partially deterministic, partially random



## Quasi-random hardware failures

- Most hardware failures are not purely random
- The failure causes are well known and understood
- Failure development is partially deterministic
- But many failures cannot be prevented in practice
  - due to lack of maintenance resources and access
  - treated as **quasi-random**
- The failure rates can be measured
  - may be reasonably constant for a given operator
  - but a wide variation between different operators
  - not a **fixed** constant rate

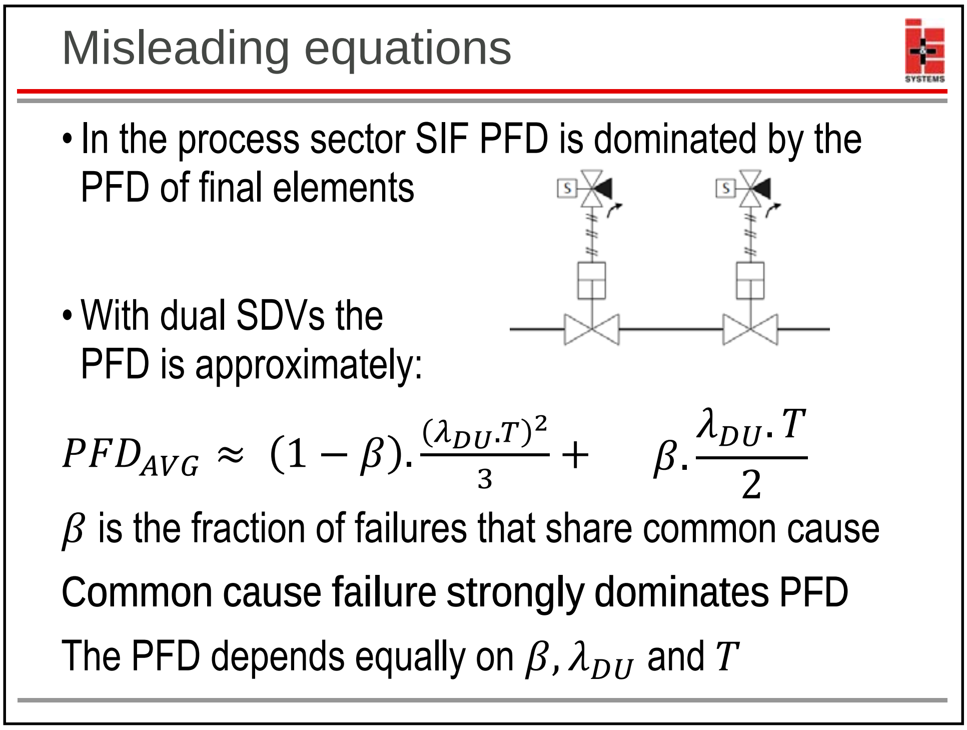


## ‘SIL Verification’: **Wrong** but useful

- Calculation of precise failure rates and precise PFD is misleading: ~~PFD = 0.00337~~ PFD ≈ 0.003 +/-?
- Monte Carlo simulations, Petri Nets and Markov models cannot improve precision because the underlying assumptions are invalid
- Calculated PFD is never better than an order of magnitude estimate

PFD ≈ 0.001 ~ 0.01
i.e. SIL 2

- The PFD calculations are useful to:
  - show the risk reduction factor that is feasible
  - understand what influences PFD and RRF



## Misleading equations

- In the process sector SIF PFD is dominated by the PFD of final elements
- With dual SDVs the PFD is approximately:

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

$\beta$ is the fraction of failures that share common cause

Common cause failure strongly dominates PFD

The PFD depends equally on $\beta, \lambda_{DU}$ and $T$

## Common cause failures $\beta$

- Identical devices are subject to common cause failures
  - failing in the same way at around the same time
  - limits the benefit of redundancy
- Minimise $\beta$ through
  - independence and diversity in design and maintenance
  - preventing systematic failures
- Typically $\beta \approx 12\% - 15\%$,
  - difficult to reduce below 5%
  - strongly dominates the calculated PFD

## Typical values for $T$

Short: $T < 0.1$ years

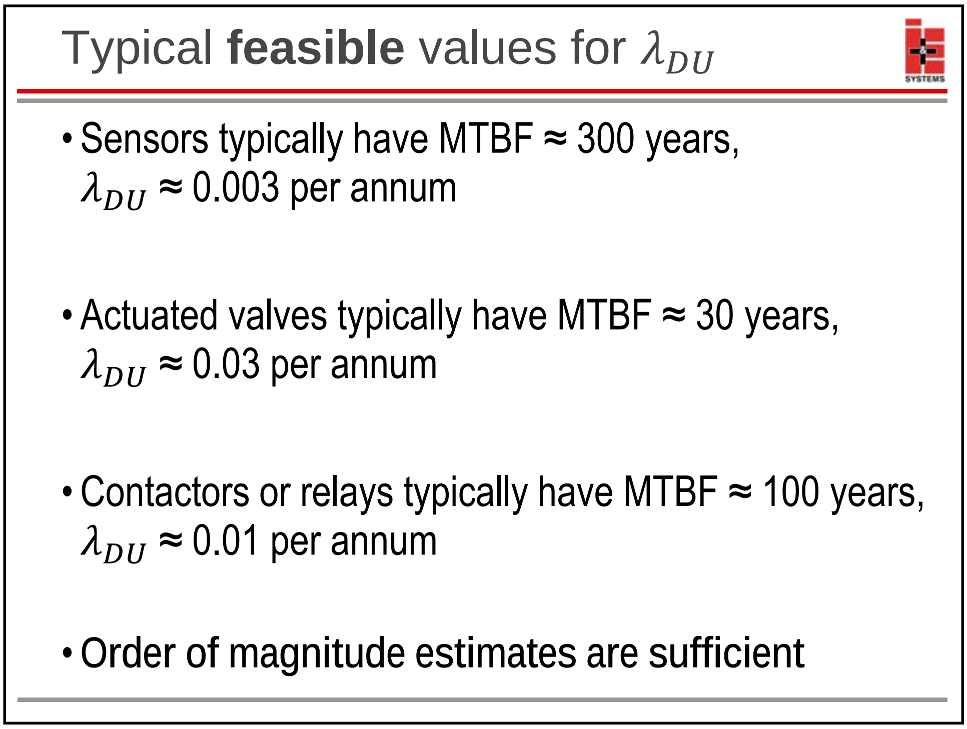
- Typical in batch processes, results in very low PFD (final elements might not be the dominant factor)

Normal: $T \approx 1$ year

Extended: $T > 3$ years

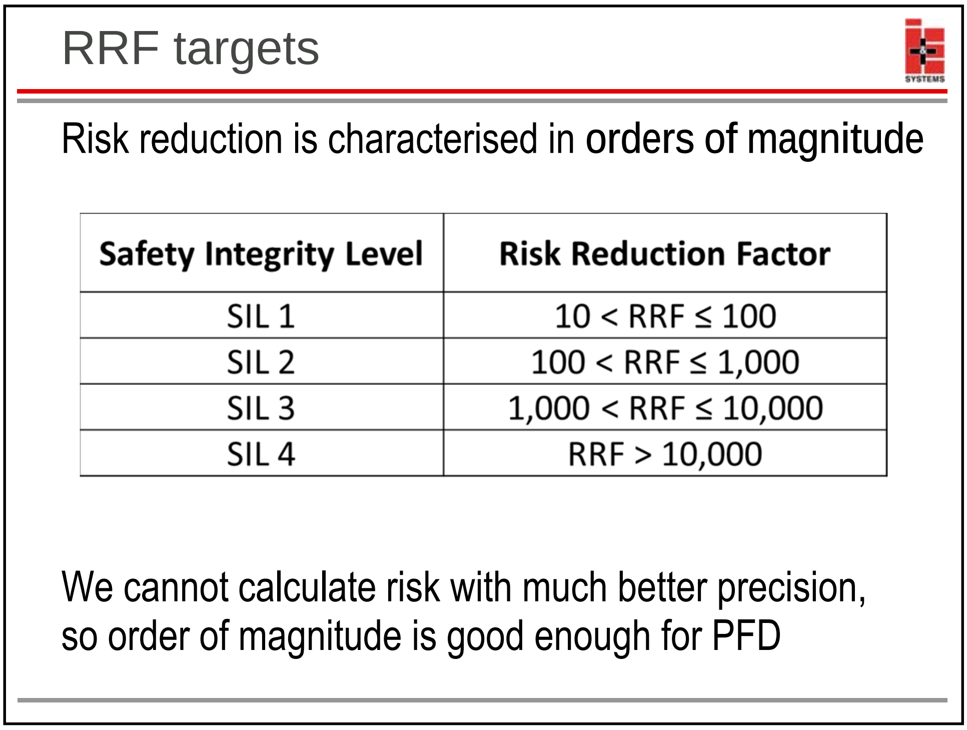
- Typical in LNG trains, e.g. 6 year test interval

Usually restricted, short $T$ may be impractical



## Typical **feasible** values for $\lambda_{DU}$

- Sensors typically have MTBF ≈ 300 years, $\lambda_{DU}$ ≈ 0.003 per annum
- Actuated valves typically have MTBF ≈ 30 years, $\lambda_{DU}$ ≈ 0.03 per annum
- Contactors or relays typically have MTBF ≈ 100 years, $\lambda_{DU}$ ≈ 0.01 per annum
- Order of magnitude estimates are sufficient

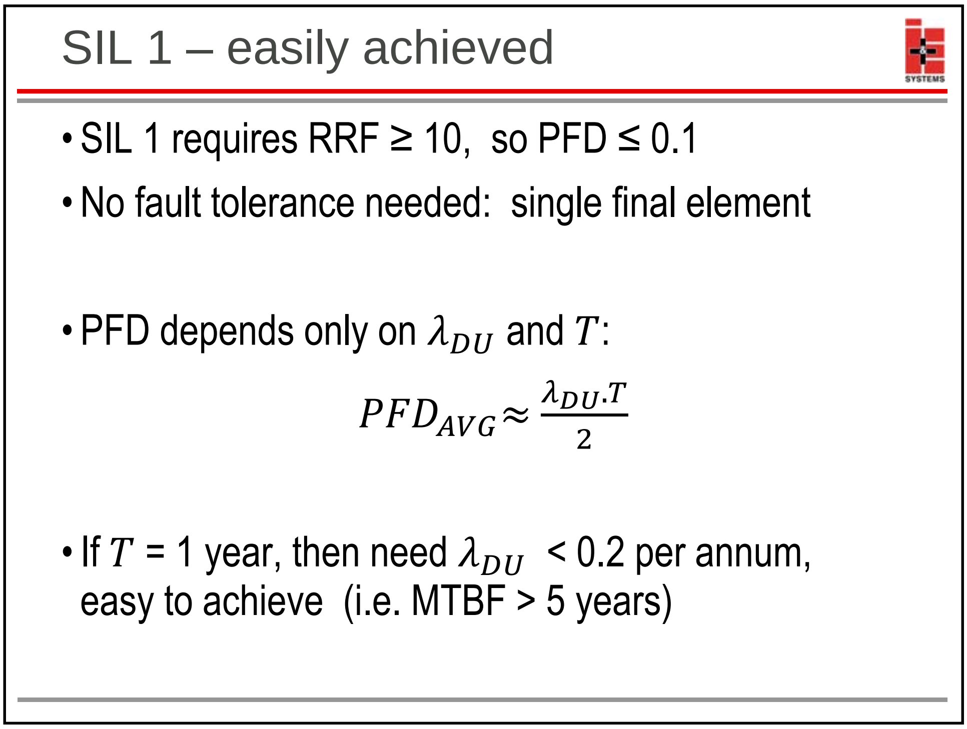


## RRF targets

Risk reduction is characterised in orders of magnitude

| **Safety Integrity Level** | **Risk Reduction Factor** |
|---|---|
| SIL 1 | 10 < RRF ≤ 100 |
| SIL 2 | 100 < RRF ≤ 1,000 |
| SIL 3 | 1,000 < RRF ≤ 10,000 |
| SIL 4 | RRF > 10,000 |

We cannot calculate risk with much better precision, so order of magnitude is good enough for PFD

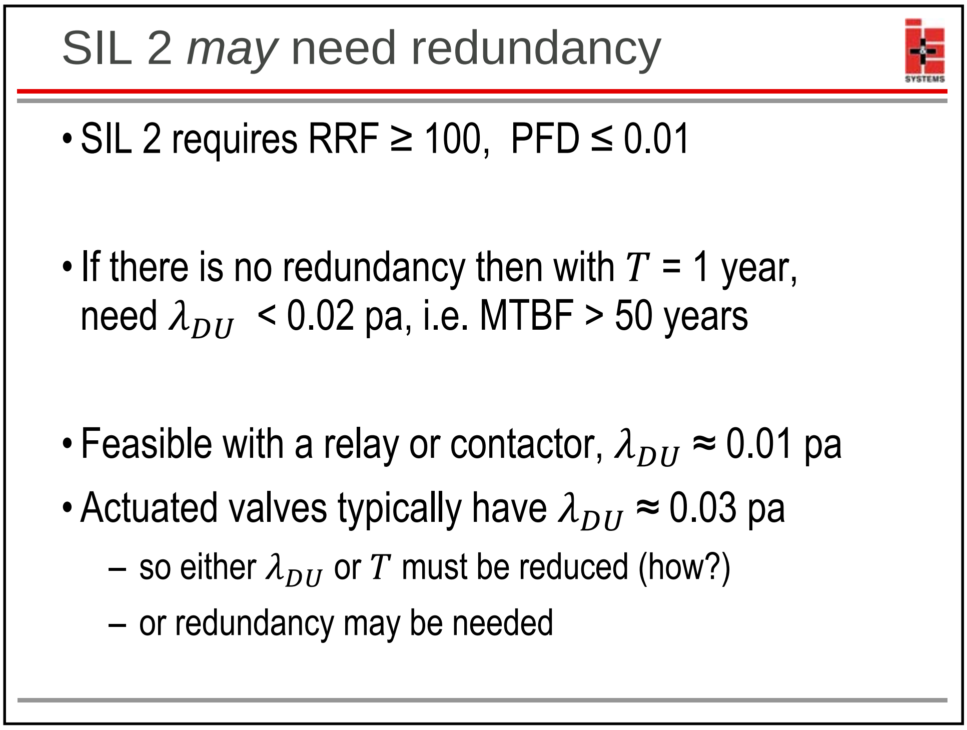


## SIL 1 – easily achieved

- SIL 1 requires RRF ≥ 10, so PFD ≤ 0.1
- No fault tolerance needed: single final element
- PFD depends only on $\lambda_{DU}$ and $T$:

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

- If $T$ = 1 year, then need $\lambda_{DU}$ < 0.2 per annum, easy to achieve (i.e. MTBF > 5 years)



## SIL 2 *may* need redundancy

- SIL 2 requires RRF ≥ 100, PFD ≤ 0.01
- If there is no redundancy then with $T$ = 1 year, need $\lambda_{DU}$ < 0.02 pa, i.e. MTBF > 50 years
- Feasible with a relay or contactor, $\lambda_{DU} \approx$ 0.01 pa
- Actuated valves typically have $\lambda_{DU} \approx$ 0.03 pa
  - so either $\lambda_{DU}$ or $T$ must be reduced (how?)
  - or redundancy may be needed

## SIL 3 always needs redundancy

- SIL 3 always needs hardware fault tolerance

RRF ≥ 1000, PFD ≤ 0.001

- Cannot be achieved with a single final element

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

- If $\beta$ ≈ 10% and $T$ = 1 year,
  then need $\lambda_{DU}$ < 0.02 pa, i.e. MTBF > 50 years
  - either $\beta$, $\lambda_{DU}$ or $T$ must be minimised

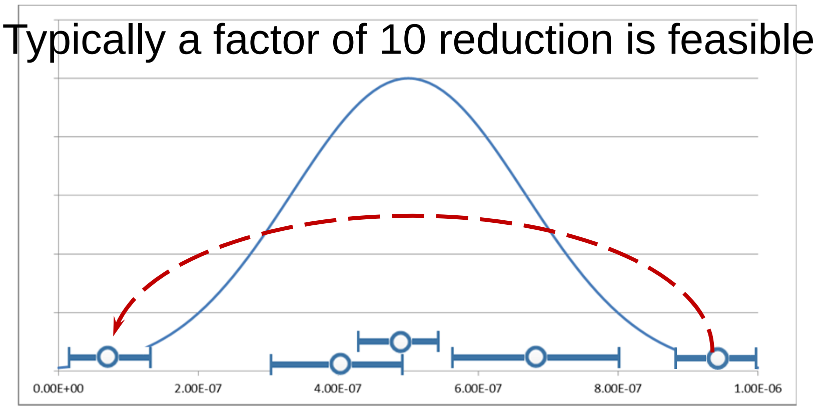
## Reducing PFD for SIL 2 and SIL 3

- Common cause failures are systematic failures, $\beta$ can be reduced (not much) by design and management in operation and maintenance
- Proof test interval $T$ is usually constrained by production requirements, cannot be reduced easily
- Failure rates $\lambda_{DU}$ are not fixed and constant, can be reduced by design and management in operation and maintenance
- SIL 3 always needs work to reduce $\beta, \lambda_{DU}$ and/or $T$
- SIL 2 with single SDV may need to reduce $\lambda_{DU}$ or $T$

# Managing and reducing failures

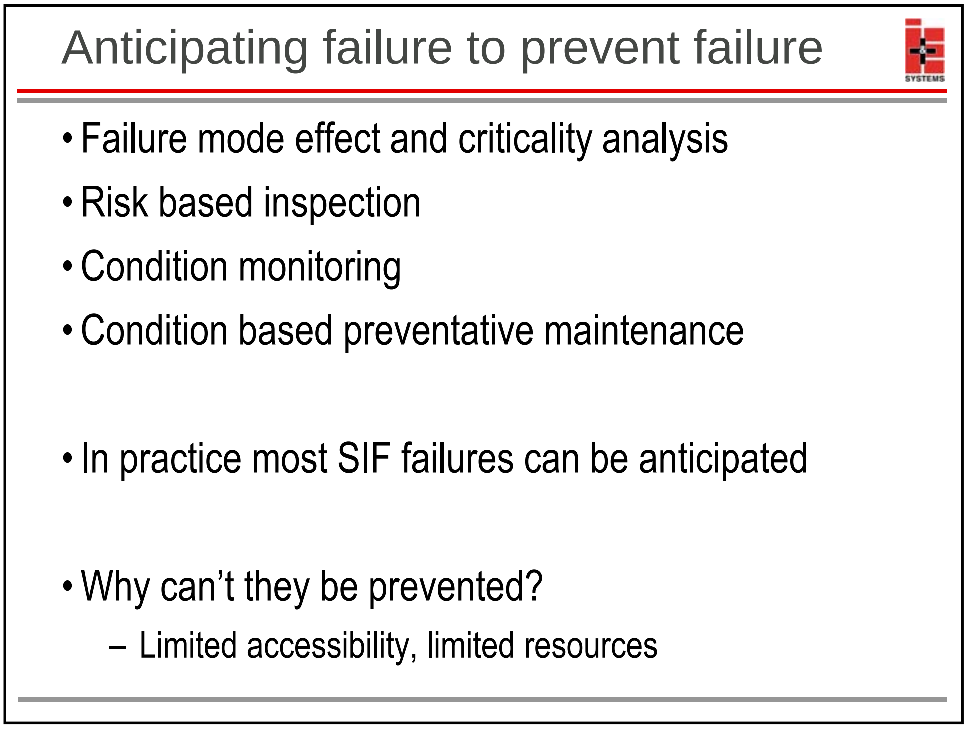
- OREDA reports failure rates that are **feasible** and easily achievable in practice
- The scope for **reduction** in failure is also clear:

Typically a factor of 10 reduction is feasible



# Benchmarks

- The failure rate $\lambda_{DU}$ assumed in design is not a fixed physical constant, it is a performance benchmark
- Failure rate targets must be acceptable to operators
- Operators must monitor the failure rates and modes
  – Calculate actual $\lambda_{DU}$, compare with design assumption
  – Analyse discrepancies between expected and actual behaviour
  – Root cause analysis, determine preventable failures
- Operators must monitor MTTR against targets
  – Safety functions deliver zero RRF while bypassed!

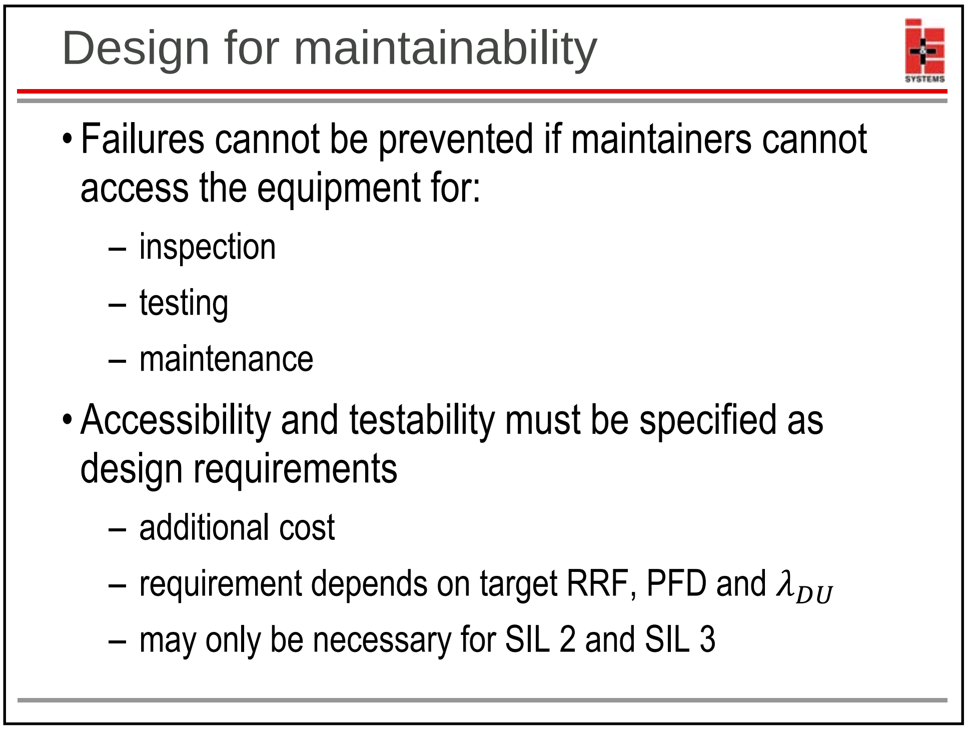


## Anticipating failure to prevent failure

- Failure mode effect and criticality analysis
- Risk based inspection
- Condition monitoring
- Condition based preventative maintenance

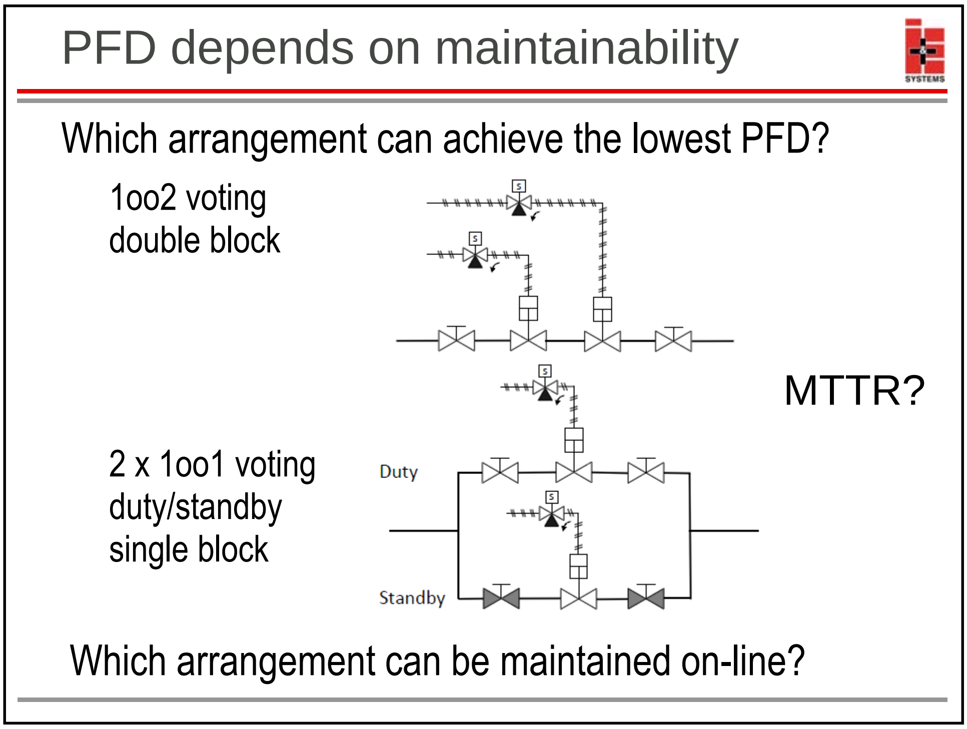
- In practice most SIF failures can be anticipated

- Why can’t they be prevented?
  - Limited accessibility, limited resources



## Design for maintainability

- Failures cannot be prevented if maintainers cannot access the equipment for:
  - inspection
  - testing
  - maintenance
- Accessibility and testability must be specified as design requirements
  - additional cost
  - requirement depends on target RRF, PFD and $\lambda_{DU}$
  - may only be necessary for SIL 2 and SIL 3



## PFD depends on maintainability

Which arrangement can achieve the lowest PFD?

1oo2 voting
double block

MTTR?

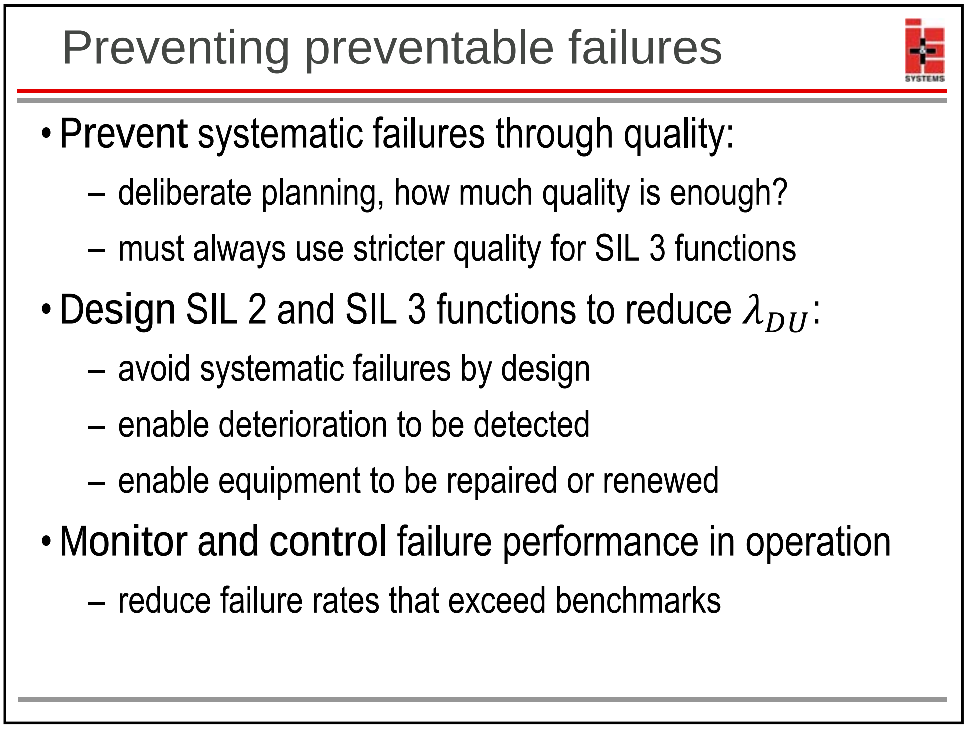
2 x 1oo1 voting
duty/standby
single block

Which arrangement can be maintained on-line?

## Summary

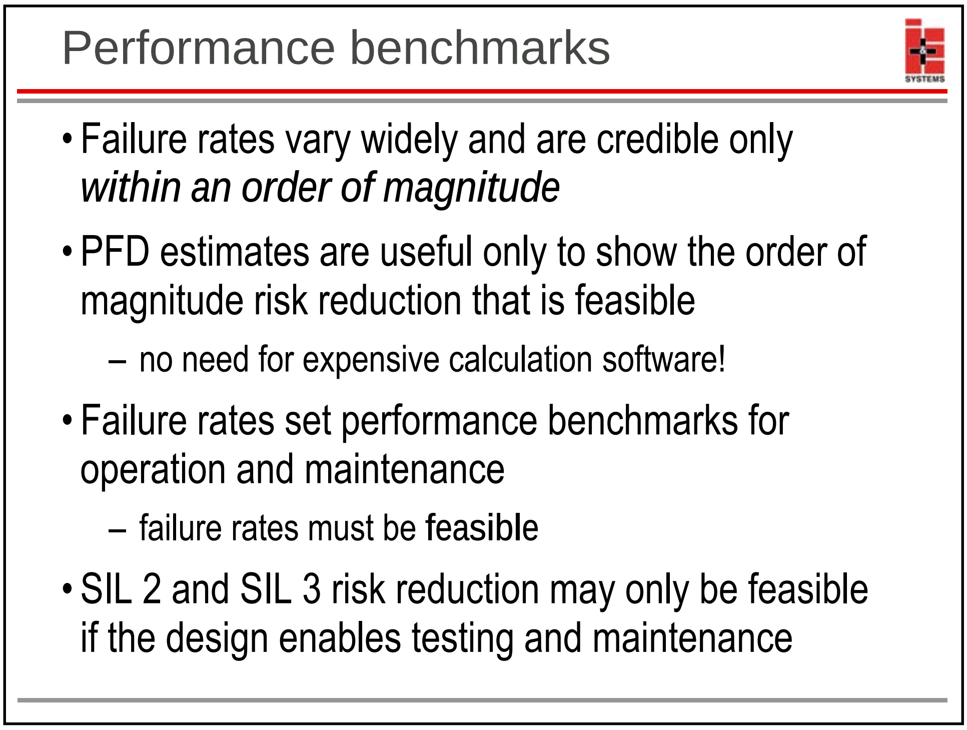
- PFD calculations are based on an invalid assumption of purely random failure
- In practice purely random failures are rare
- Most failures are systematic in nature
- Most failures are preventable to some extent

- In design the emphasis should be on how to prevent failure and how to enable testing and maintenance



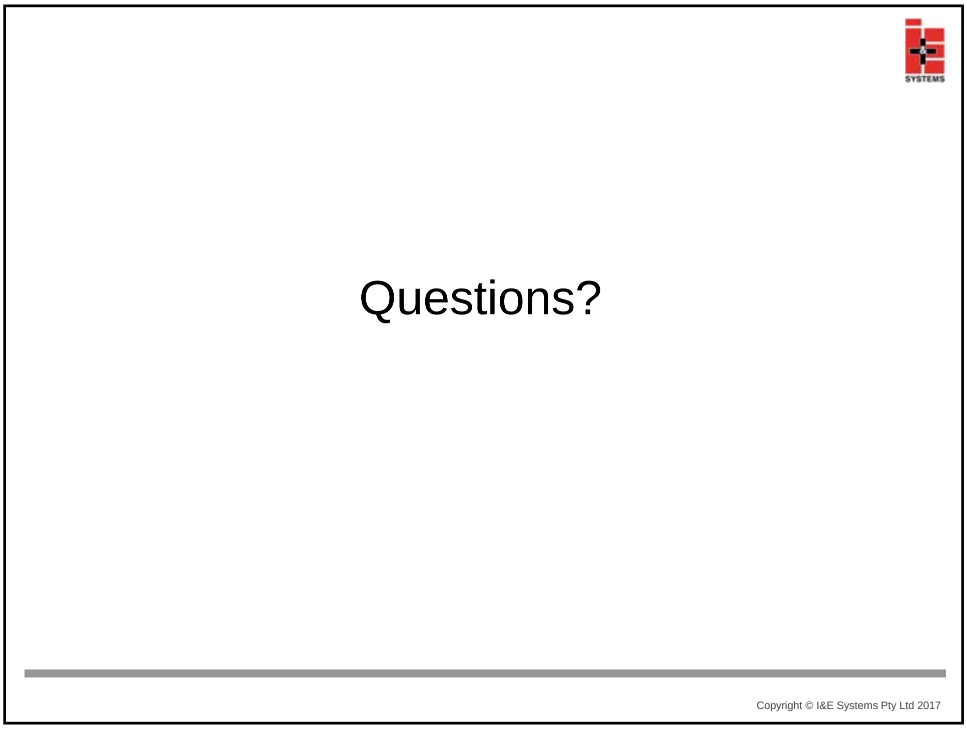
## Preventing preventable failures

- Prevent systematic failures through quality:
  - deliberate planning, how much quality is enough?
  - must always use stricter quality for SIL 3 functions
- Design SIL 2 and SIL 3 functions to reduce $\lambda_{DU}$:
  - avoid systematic failures by design
  - enable deterioration to be detected
  - enable equipment to be repaired or renewed
- Monitor and control failure performance in operation
  - reduce failure rates that exceed benchmarks



## Performance benchmarks

- Failure rates vary widely and are credible only *within an order of magnitude*
- PFD estimates are useful only to show the order of magnitude risk reduction that is feasible
  - no need for expensive calculation software!
- Failure rates set performance benchmarks for operation and maintenance
  - failure rates must be feasible
- SIL 2 and SIL 3 risk reduction may only be feasible if the design enables testing and maintenance



Questions?