Preventing preventable failures

Mirek Generowicz
I&E Systems Pty Ltd - Australia

The need for credible failure rates

IEC 61511 Edition 2 (2016) reduced requirements for hardware fault tolerance

Instead the new edition emphasises that the ‘*reliability data used in quantifying effect of random failures should be* ***credible****, traceable, documented and justified based of field feedback from similar devices used in a similar operating environment*’
(IEC 61511-1 §11.9.3)

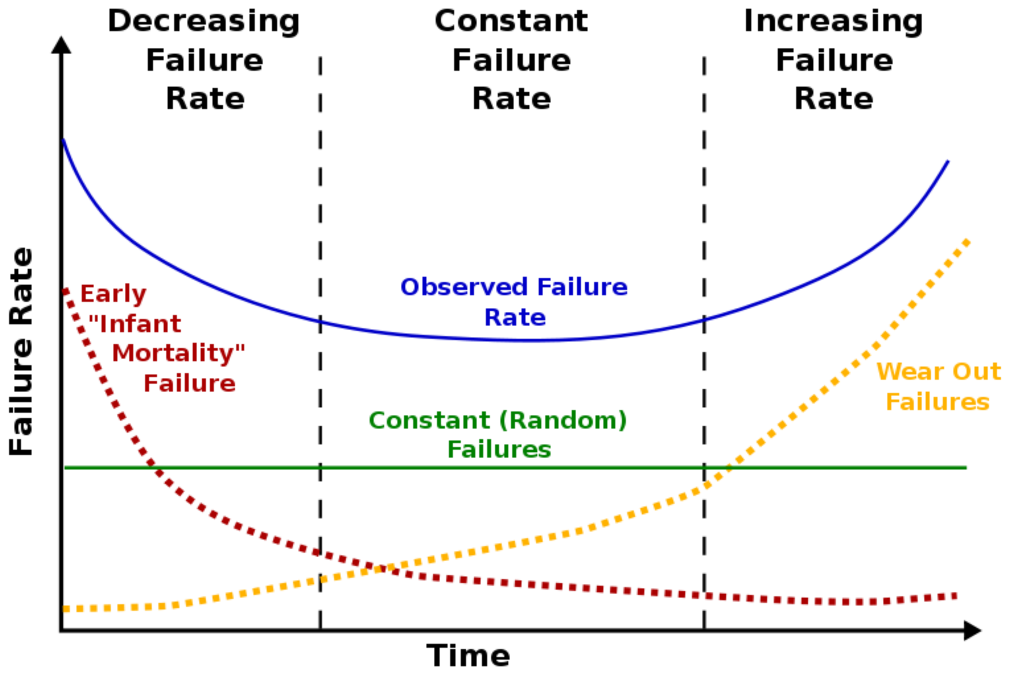
In practice how do we find ‘credible reliability data’?

Answering this question revealed that most failure probability calculations are based on a misunderstanding of probability theory

‘Wrong but useful’

Failure probability calculations depend on estimates of equipment failure rates

The basic assumption has been that during mid-life the failure rate is constant and **fixed**:



This assumption is **WRONG**

- The rate is not fixed
- …but the calculations are still useful

We need a different emphasis

We cannot predict probability of failure with precision

- Failure rates are not fixed and constant
- We can estimate PFD within an order of magnitude only
- We can set feasible ***targets*** for failure rates
- We must design the system so that the rates can be achieved

In operation we need to monitor the actual PFD achieved

- We must measure actual failure rates and analyse all failures
- Manage performance to meet target failure rates
  by preventing preventable failures

Hardware fault tolerance

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

So 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’*

HFT in IEC 61511 Edition 2

New, simpler requirement for HFT

SIL 3 is allowed with only two block valves (HFT =1)

- Previously SIL 3 with only two valves needed SFF > 60% or ‘dominant failure to the safe state’ (difficult to achieve)

SIL 2 low demand needs only one block valve (HFT = 0)

- Previously two valves were required for SIL 2

HFT in IEC 61511 Edition 2

Based on the IEC 61508 ‘Route 2_H’ method

- Introduced in 2010
- Requires a confidence level of ≥ 90% in target failure measures (only 70% needed for Route 1_H)

e.g. λ_{AVG} = No. of failures recorded / total time in service

IEC 61511 Ed 2 only requires 70% confidence level instead of 90%, but similar to Route 2_H, it requires: ***credible, traceable failure rate data*** *based on field feedback from similar devices in a similar operating environment*

Why not 90%?

So what is confidence level?

The uncertainty in the rate of **independent** events depends on how many events are measured

Confidence level relates to the width of the uncertainty band, which depends on the number of failures recorded

We can evaluate the uncertainty with the chi-squared function χ^2

α = 1- confidence level

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

n = the number of failures in the given time period

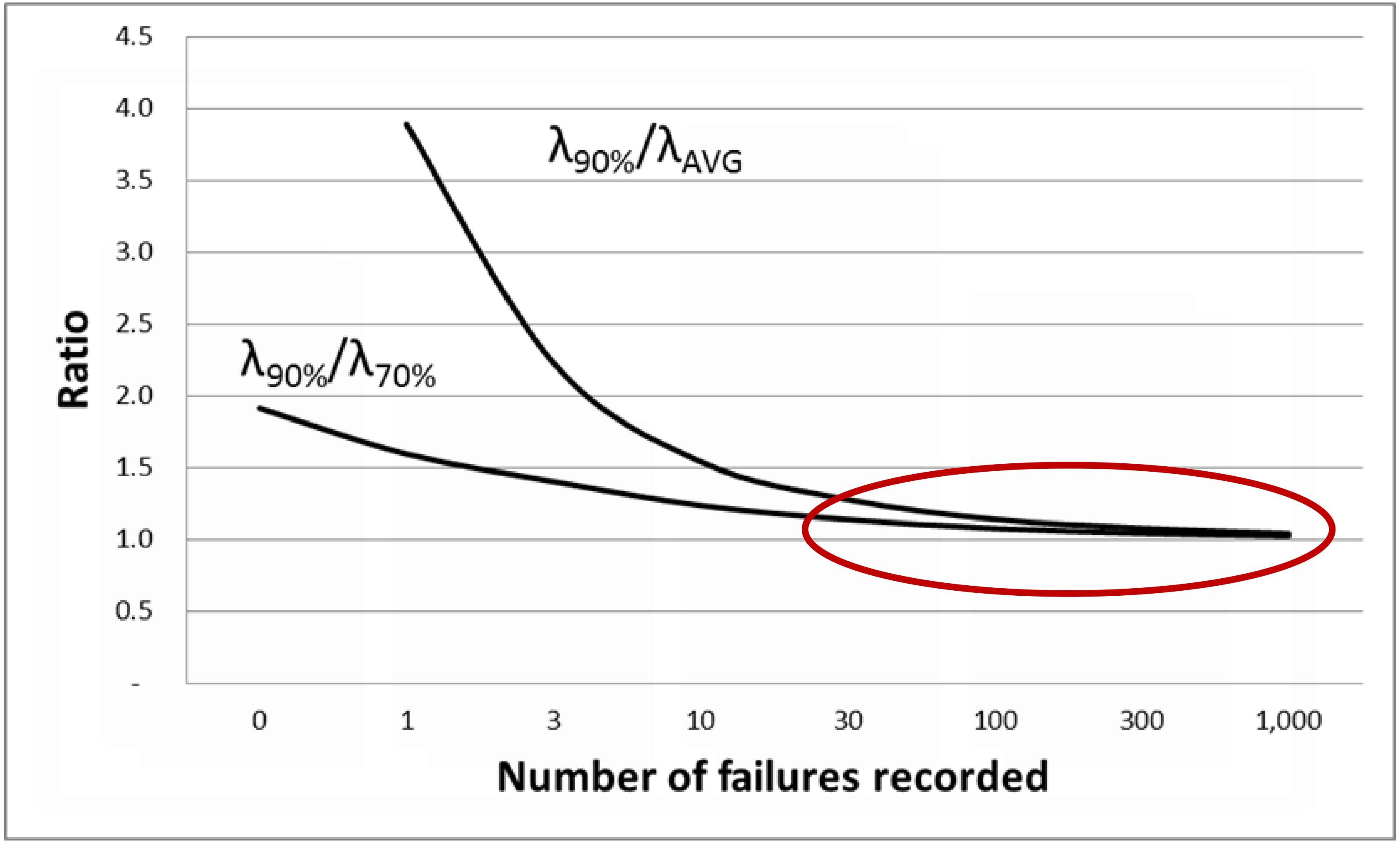
T = the number of device-years or device-hours, i.e. the number of devices x the given time period

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

Confidence level does ***not*** depend directly on 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

With an MTBF of 100 years, to measure 10 failures we only need 100 similar devices in service for 10 years

Surely by now we must have recorded enough many failures for most commonly applied devices?

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

Where can we find credible data?

An enormous effort has been made to determine λ

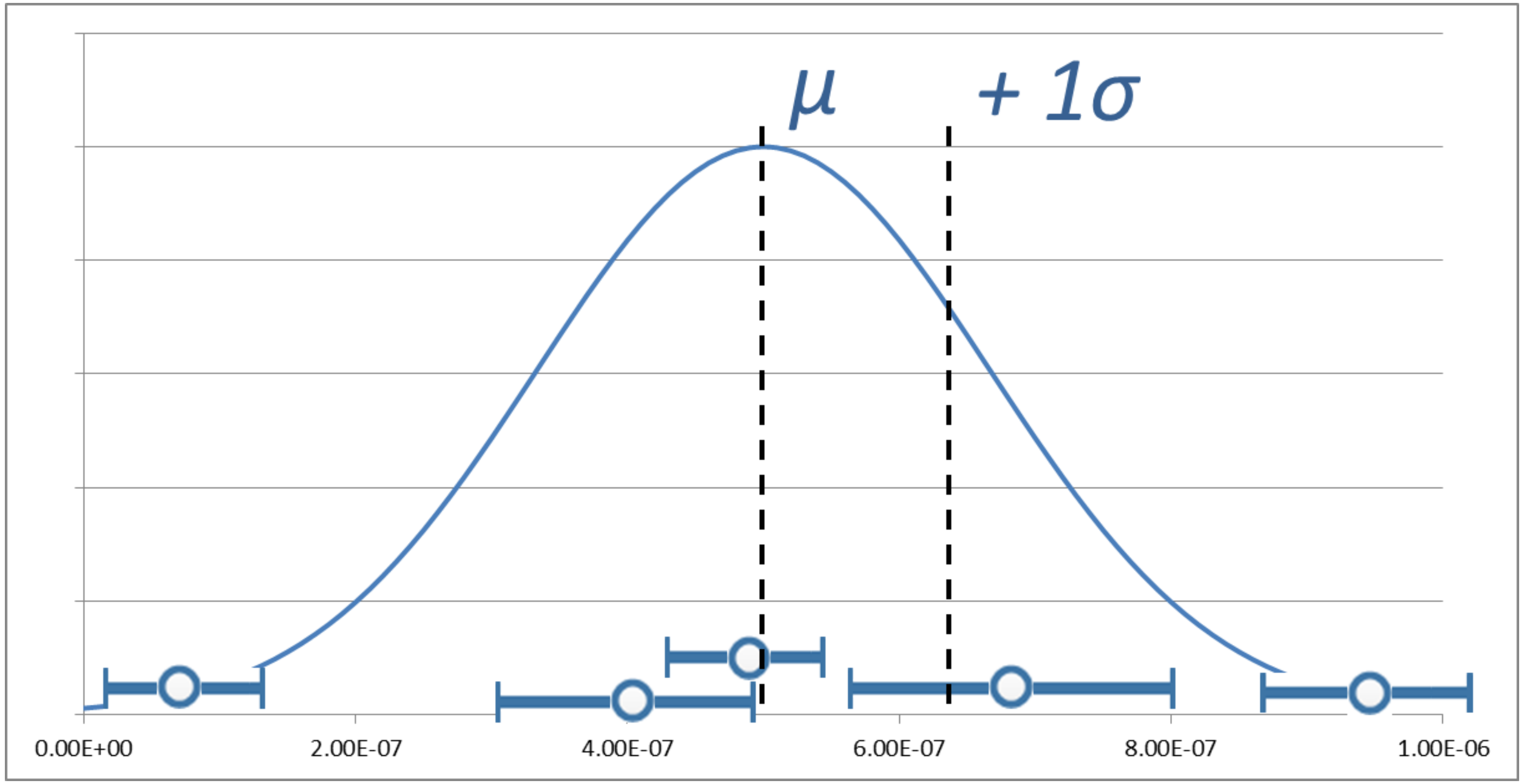
Some widely used sources:

- 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’
- FARADIP database
- 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

- only some are random
- some are systematic (depending on the application)
- site-specific factors influence failure rate

λ is NOT constant; χ^2 function confidence levels do not apply, OREDA provides lower and upper deciles to show uncertainty

A long-standing debate

Should the calculated probability of failure take into account systematic failures?

The intent of IEC 61508, IEC 61511 and ISO/TR 12489
is to calculate failure probability only for **random** failure

ISA TR84.00.02, *exida,* SINTEF PDS Method and OREDA specifically include some systematic failures

The intent of the standards:

Manage risk of ***systematic*** (i.e. preventable) failures

- **Prevent** errors and failures in design and implementation
- By applying quality management methods

Reduce risk of ***random*** hardware failures

- For the failures that cannot be effectively prevented
- **Calculate** failure probability based on failure rates
- Reduce the probability of failure to achieve the required risk reduction target:
  - Apply diagnostics for fault detection and regular periodic testing
  - Apply redundant equipment for fault tolerance

What is random?

Which of these are random:

- Tossing a coin?
- Horse race?
- Football match?

If I record 47 heads in 100 tosses, P(head) ≈ ?

If a football team wins 47 matches out of 100 what is the probability they will win their next match?

What is random?

Dictionary:

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

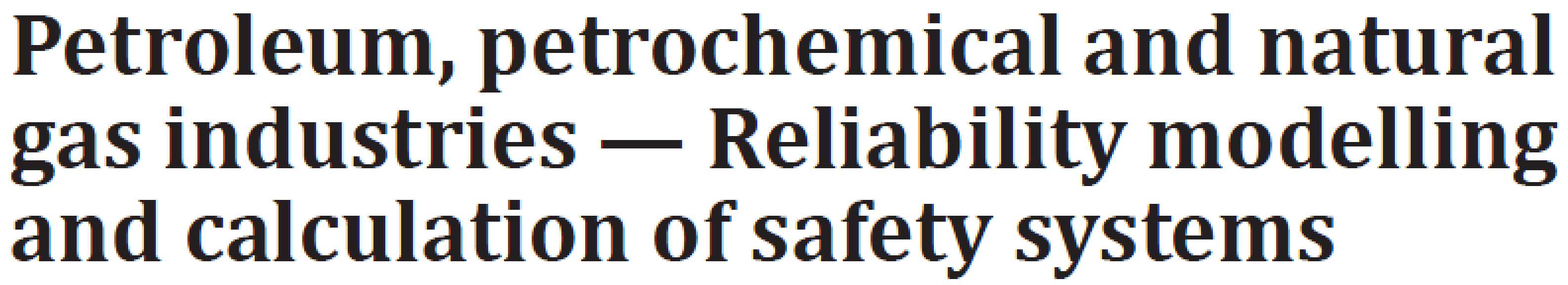
Mathematics:

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

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

These definitions are significantly different

Guidance from ISO/TR 12489



Petroleum, petrochemical and natural gas industries — Reliability modelling and calculation of safety systems

ISO/TR 12489 provides detailed explanation and guidance for the failure probability calculations given in IEC 61508-6

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

Purely random failure

Only ‘catalectic’ failures have constant failure rates:

ISO/TR 12489 §3.2.9

catalectic failure

sudden and complete failure

Note 1 to entry: […] a catalectic failure occurs without warning and is more or less **impossible to forecast by examining the item**. It is the contrary of failures occurring progressively and incompletely.

Note 2 to entry: Catalectic failures characterize **simple components with constant failure rates** (exponential law): they remain permanently “as good as new” until they fail suddenly, completely and without warning. Most of the probabilistic models used in reliability engineering are based on catalectic failures of the individual component of the system under study (e.g. Markovian approach)

Definition in IEC 61511 and IEC 61508

IEC 61511 §3.2.59 and IEC 61508-4 §3.6.5

random hardware failure

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

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of a total equipment comprising many components occur at predictable rates but at unpredictable (i.e., random) times.

Not limited to ‘catalectic’ failure

Cannot be characterised by fixed constant failure rate – though the rates are measurable and may be predictable

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)

Most failures are partially systematic and partially random

Quasi-random hardware failures

Most hardware failures are **not purely random**

The failure causes are well known and understood

But many failures cannot be prevented in practice

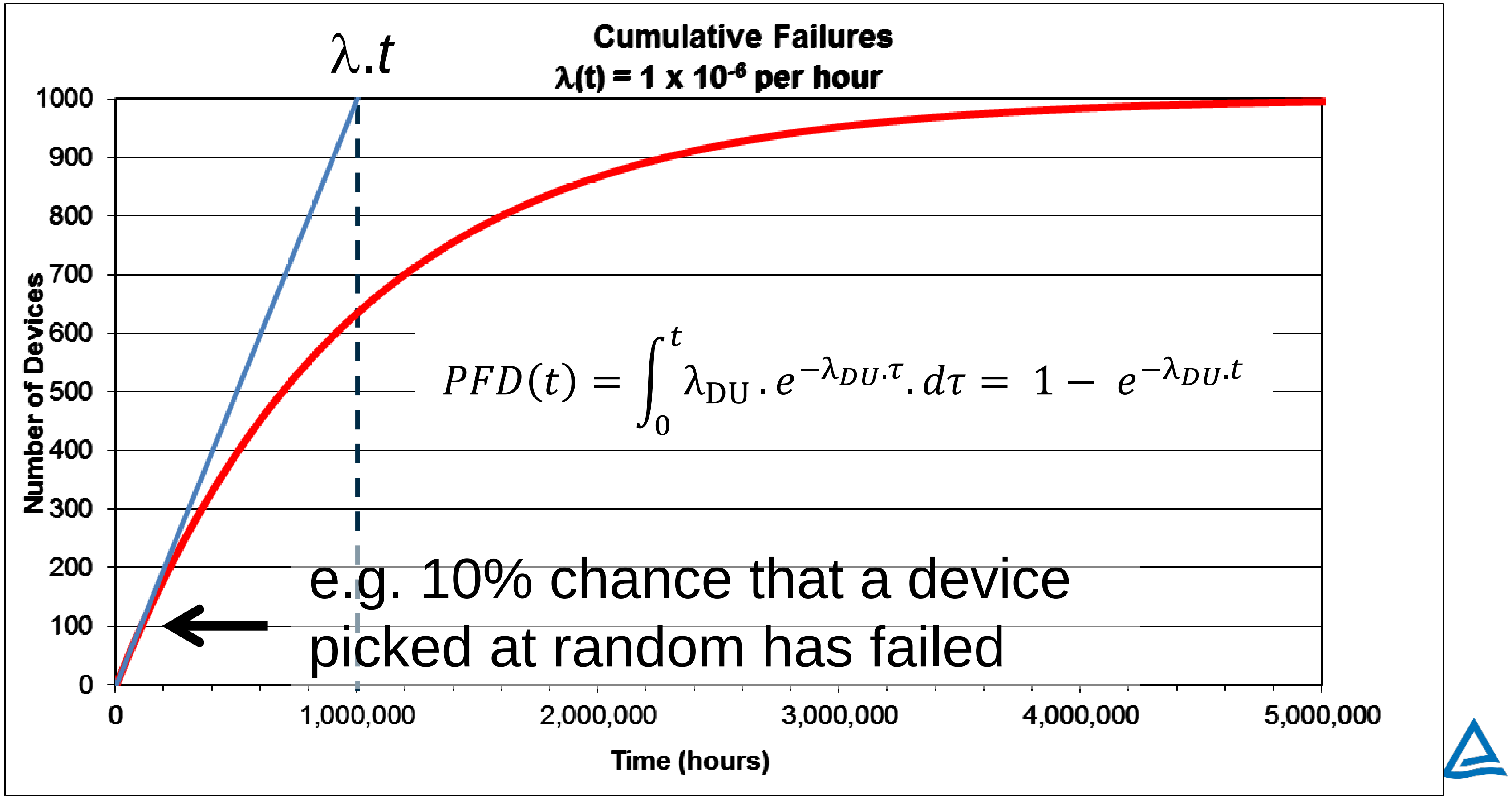
- due to lack of maintenance resources and access
- treated as **quasi-random**

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
- can be reduced by deliberate effort

Failure probability depends on failure rate

If undetected device failures occur at a **constant average rate** then failures accumulate exponentially:



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

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

SYSTEMS

TÜVRheinland®
Precisely Right.

The basic assumption in failure probability

If undetected device failures occur at a **constant average rate** then failures accumulate exponentially:

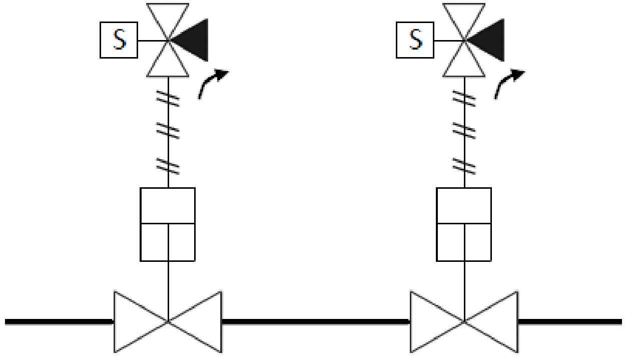
SIFs always require $PFD_{avg} < 0.1$,
in this region the accumulation is linear:

$$PFD \approx \lambda_{DU}.t$$

With a proof test interval T the average is simply

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

PFD for 1oo2 final elements



In the process sector SIF PFD is dominated by the PFD of final elements

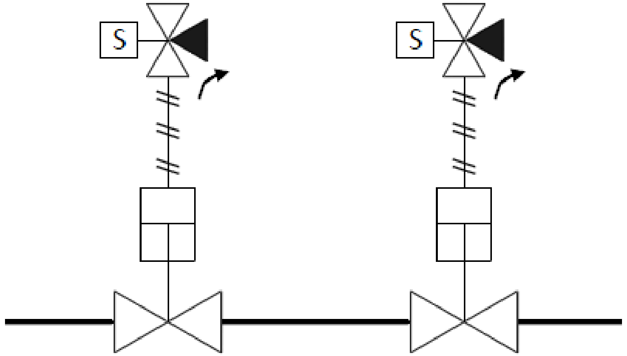
With 1oo2 valves the PFD is approximately:

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

β is the fraction of failures that share common cause

PFD for 1oo2 final elements

In the process sector SIF PFD is dominated by the PFD of final elements



With 1oo2 valves the PFD is approximately:

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

β is the fraction of failures that share common cause

Common cause failure always strongly dominates PFD

The PFD depends equally on λ_{DU}, β and T

Dependence on failure rate

Our estimate of PFD is only as good as our estimate of the undetected failure rate λ_{DU} of the final elements

The failure rate:

- can be measured
- may be predictable
- is not a fixed constant rate

Typical failure rates are easy to obtain

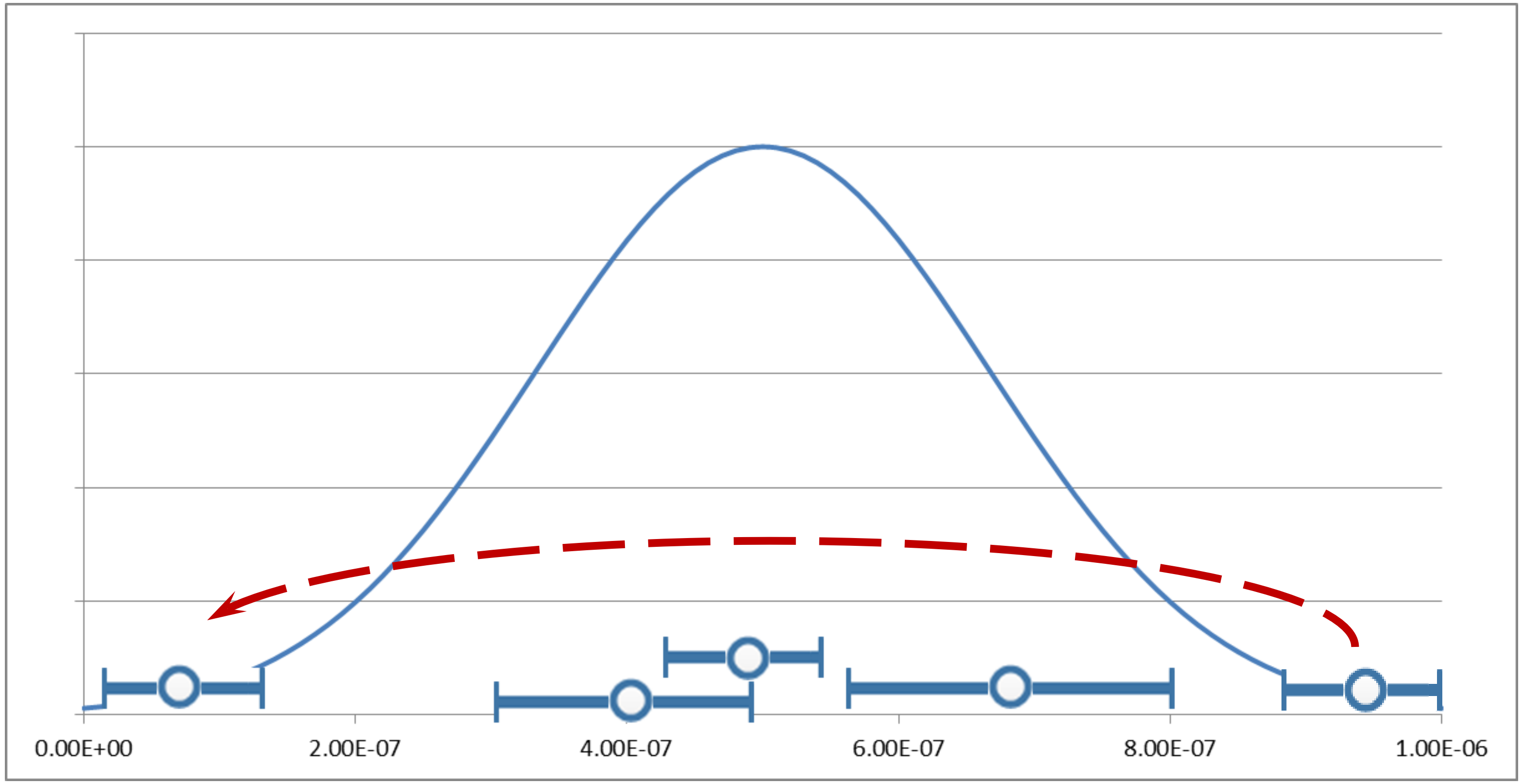
Failure rates can be controlled and reduced

Managing and reducing failures

OREDA reports failure rates that are **feasible** in practice

Typically failure rates vary over at least an order of magnitude:

Reduction in rate by a factor of 10 may be feasible



Typical **feasible** values for λ_{DU}

Sensors typically have MTBF ≈ 300 years,
λ_{DU} ≈ 0.003 per annum

Actuated valve assemblies typically have MTBF ≈ 50 years,
λ_{DU} ≈ 0.02 per annum

Contactors or relays typically have MTBF ≈ 200 years,
λ_{DU} ≈ 0.005 per annum

These are order of magnitude estimates –
but are sufficient to show feasibility of PFD and RRF targets

(risk targets can only be in orders of magnitude)

Typical feasible values for β

IEC 61508-6 Annex D suggests a range of 1% to 10%

Typically $\beta \approx$ 12% - 15% in practice (Ref: SINTEF Report A26922)

- difficult to reduce below 5% with **similar** devices
- strongly dominates PFD of voted architectures

Minimise β through

- independence and **diversity** in design and maintenance
- preventing systematic failures

Typical values for T depend on application

Batch process: $T < 0.1$ years

- Results in low PFD, final elements might not dominate

Continuous process: $T \approx 1$ year

LNG production: $T > 4$ years

- Low PFD is more difficult to achieve

Production constraints may make it difficult to reduce T

What architecture is typically needed?

For typical values $\beta \approx 10\%$, $\lambda_{DU} \approx 0.02$ pa, $T \approx 1$ y

SIL 1 is always easy to achieve without HFT

SIL 2 needs 1oo2 final elements unless
overall λ_{DU} can be reduced to < 0.02 pa (MTBF$_{DU}$ > 50 y)

SIL 3 would need 1oo2 final elements ***and***
overall $\lambda_{DU} <$ 0.02 pa

- either λ_{DU}, β and/or T must be minimised
- needs close attention in design

Design assumptions set performance benchmarks

Probability of SIF failure on demand is proportional to
β, λ_{DU}, T and *MTTR*

The values assumed in design set **performance standards** for availability and reliability in operation and maintenance

Achieving these performance standards depends on the design, and on operation and maintenance practices

Monitoring performance is essential

Operators must monitor the failure rates and modes

- Calculate actual λ_{DU}, compare with design assumption
- Analyse discrepancies between expected and actual behaviour
- Root cause analysis, prevent the preventable failures

Operators must also monitor MTTR against targets

- Safety functions deliver zero RRF while bypassed

Design for maintainability to enable performance

Failure rates can be reduced if maintainers have ready access to the equipment for:

- inspection
- testing
- maintenance and repair

Accessibility and testability **must be considered** and specified as design requirements

- additional cost
- requirement depends on target RRF, PFD and λ_{DU}
- may only be necessary for SIL 2 and SIL 3

SYSTEMS

TÜVRheinland®
Precisely Right.

Suitability of components

Certification and prior use are also important:

- Evidence of **quality**, i.e. **systematic capability**
- Evidence of **suitability for service and environment**
  - preventing systematic failures
- Volume of operating experience provides evidence that
  - systematic capability is adequate
  - inspection and maintenance is effective
  - failures are monitored, analysed and understood
  - failure rate performance benchmarks are achievable

(Refer to IEC 61511-1 §11.5.3 and IEC 61508-2 §7.4.4.3.3)

Emphasis on prevention instead of calculation

Prevent systematic failures through quality

- systematic capability, proven in use
- deliberate quality planning, how much quality is enough?
- must always use stricter quality for SIL 3 functions

Design SIL 2 and SIL 3 functions to **reduce** $\boldsymbol{\lambda_{DU}}$:

- avoid systematic failures and common cause failures by design
- enable deterioration to be detected (diagnostics, inspection, test)
- enable equipment to be repaired or renewed ***before*** it fails
- **ensure testability and accessibility**

Monitor and control failure performance in operation

- reduce failure rates that exceed benchmarks

Credible reliability data ≡ feasible performance targets

Performance targets must be feasible, **by design**

PREVENT PREVENTABLE FAILURES

M. Generowicz, FS Senior Expert (TÜV Rheinland #183/12), Engineering Manager
A. Hertel, Principal Engineer

I&E Systems Pty Ltd
Perth, Western Australia

Abstract

IEC 61511-1 Edition 2 (2016) has reduced the requirements for hardware fault tolerance in automated safety functions. The new requirements are based on the IEC 61508-2 'Route 2_H' method, which relies on increased confidence levels in failure rates

Instead of requiring increased confidence level IEC 61511-1 requires 'credible and traceable reliability data' in the quantification of failure probability. It is not immediately obvious what this means in practice.

Failure probability calculations are based on the assumption that failure rates are fixed and constant. That assumption is invalid, but the calculations are still useful.

This paper discusses the reasons for the wide variability and uncertainty in measured failure rates. It draws conclusions on how failure rates and failure probability can be controlled in practice.

Summary

Automated safety functions are applied to achieve hazard risk reduction at industrial process facilities. The calculations of risk reduction achieved have been based on failures being predominantly random in nature and failure rates being fixed and constant.

Over the past several decades, enough information has been collected to estimate failure rates for all commonly used components in safety functions. The information shows that failure rates measured for any particular type of device vary by at least an order of magnitude between different users and different applications. The variation depends largely on the service, operating environment and maintenance practices. It is clear that:

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

At best, the risk reduction achieved by these safety functions can be estimated only within an order of magnitude. Nevertheless, even with such imprecise results the calculations are still useful.

Failure rates from industry databases are useful in demonstrating the feasibility of the risk reduction targeted by safety functions. This is important in setting operational reliability benchmarks.

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 rather than

purely random. 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. Using risk-based inspection and condition-based maintenance techniques to:
    - Identify and then control conditions that induce early failures,
    - Actively prevent common-cause failures.
4. Detailed analysis of all failures to:
    - Monitor failure rates
    - Determine how failure recurrence may be prevented if failure rates need to be reduced.

Functional safety depends on safety integrity

The fundamental objective of the functional safety standards is to ensure that automated safety systems reliably achieve specified levels of risk reduction. 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 (and the resulting risk reduction) can be calculated.

Calculation methods

IEC 61508-6:2010 Annex B[4] 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[5].

Several other useful references are available on this subject, including ISA-TR84.00.02-2015[6] and the SINTEF PDS Method Handbook[7]. These calculation methods enable users to estimate the PFD for safety functions and the corresponding RRF achieved. The calculations are all based on these assumptions:

- Dangerous undetected failures of the devices in a safety function are characterised by **fixed and constant failure rates**
- Failures occurring within a population of devices are assumed to be **independent events**.

ISO/TR 12489 uses the term ‘catalectic failure’ to clarify the types of failures that can be expected to occur at fixed rates.

> *3.2.9*
> ***catalectic failure***
> *sudden and complete failure*

Note 1 to entry: This term has been introduced by analogy with the catalectic verses (i.e. a verse with seven foots instead of eight) which stop abruptly. Then, a catalectic failure occurs without warning and is more or less impossible to forecast by examining the item. It is the contrary of failures occurring progressively and incompletely.

Note 2 to entry: Catalectic failures characterize simple components with constant failure rates (exponential law): they remain permanently "as good as new" until they fail suddenly, completely and without warning. Most of the probabilistic models used in reliability engineering are based on catalectic failures of the individual component of the system under study (e.g. Markovian approach).

If dangerous undetected failures occur independently at a fixed rate λ_{DU} within a population of similar components then undetected failures will accumulate exponentially. The PFD of a component chosen at random is directly proportional to the number of failures that have accumulated in the population.

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. Redundancy 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 Edition 2 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 λ can be estimated with any required level of confidence by applying a χ^2 (chi-squared) distribution. The failure rate estimated with confidence level of 'a' is designated λ_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. 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 $\lambda_{70\%.}$

Failure rate sources

The Offshore and Onshore Reliability Data (OREDA) project provides a useful source of failure rate information gathered over many years by a consortium of oil and gas companies. 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 probability 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.

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 these references are reasonably consistent with the OREDA data, though they do not give any indication of the wide uncertainty band.

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.

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 **but the failure rates are not constant**.

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** is from '*A Dictionary of Statistical Terms*', by F.H.C Marriott[13]:

> *'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 and are not purely random.

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.'*

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

Failures of mechanical components may seem to be random, but the causes are usually well known and understood and are partially deterministic. The failures can be prevented to some extent if the degradation is monitored and corrective maintenance can be completed when it is needed.

Degradation of mechanical components is not a purely random process. Degradation can be monitored.

While it might be theoretically possible to prevent failure from degradation 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 conditions 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.

Factors that dominate PFD

In the process sector the PFD of a safety function is usually strongly dominated by the PFD of the final elements. This is because the rates of undetected failure of final elements are usually an order of magnitude higher than rates of undetected failure of sensors. With fault tolerance in final elements the PFD is strongly dominated by common cause failures.

As an example, consider a safety function using actuated valves as final elements in a 1oo2 (i.e. 1 out of 2) redundant architecture. A typical rate of undetected dangerous failures λ_{DU} in an actuated valve assembly is around 0.02 failures per annum (approximately 1 failure in 50 years, or around 2.3 failures per 10^6 hours) [8] [11] [12]. 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. It will dominate the PFD unless the following is true:

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

If the test interval T is 1 year and $\lambda_{DU} = 0.02$ pa, then the common cause failure term will be greater than the first term unless $\beta < 2\%$, and such a low value is difficult to achieve.

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%.

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%.

Clearly, the PFD for undetected failures is directly proportional to β, λ_{DU} and T.

For detected failures the PFD is directly proportional to the rate of detected failures λ_{DD} and the mean time to restoration (MTTR).

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 may 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 PFD calculated for any safety function is necessarily limited to 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) that is feasible.

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

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 0.02 pa quoted above for λ_{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 lower than 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/or λ_{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 λ_{DU} and improving test coverage). If reducing β and λ_{DU} is not sufficient it may also be necessary to shorten the test interval T. It is usually impractical to implement automatic continuous diagnostics on final elements.

The end result of the PFD calculations is a set of operational performance targets for β, λ_{DU}, T and MTTR. These factors are **not fixed constants** and are all under the control of the designers and the operations and maintenance team.

Independent certification of systematic capability

The system designers need to demonstrate appropriate systematic capability. Evidence is required to show that appropriate techniques and measure have been applied to prevent systematic failures. This must include showing that the systems are suitable for the intended service and environment. The level of effectiveness in these techniques and measures must be shown to be sufficient for the intended SIL.

Independent certification provides good evidence of systematic capability in the design and construction of the equipment.

Evidence of prior use

Systematic capability is not limited to design. Evidence is also needed to show that operation, inspection, testing and maintenance of the systems will be effective in achieving the target failure performance.

Operators need to plan operation, inspection, testing and maintenance based on a volume of prior operating experience that is sufficient to show that the target failure rates are achievable.

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. It suggests 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 causes 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 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.

Detailed inspection, testing and condition monitoring can then be used to provide leading indicators of incipient failure. Most of the modes of failure should be predictable. It should be feasible to prevent failures through condition based maintenance with overhaul, renewal or replacement when required.

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.

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 must 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 while it is bypassed or taken out of service during normal plant operation. The probability of failure on demand is directly proportional to the time that the safety function is out of service (characterised as mean time to restoration, MTTR).

Designing the system to facilitate inspection, testing and maintenance enables both the λ_{DU} and the MTTR to be minimised in operation.

Preventing 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.

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.

Conclusions

Wide variation in failure data

Designers of safety functions estimate probability of failure by assuming that failures occur randomly and with fixed constant failure rates. The precision in the estimates is limited by 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 serve as 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. 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 to the equipment and resources are limited. Failures are treated as quasi-random to the extent that it is not practicable to prevent the failures.

PFD Calculations set feasible performance benchmarks

PFD calculations are based on the coarse assumptions that failure rates and the proportion of common cause failures are fixed and constant. These assumptions enable the PFD and RRF to be estimated within an order of magnitude, given reasonably effective quality control in design, manufacture, operation and maintenance. The onus is then on the operators to demonstrate that the failure rates of the equipment in operation are no greater 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. Failures are minimised 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. It includes the achievement of an appropriate level of systematic capability.

   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.

2. The second priority in functional safety is to enable early detection and effective treatment of the deterioration that cannot be prevented. The design of the safety functions needs to take into account the expected failure modes and to include requirements for diagnostics, accessibility, inspection, testing, maintenance and renewal.

   The requirements for accessibility depend on the target failure rates that need to be achieved for the target risk reduction. The requirements also depend on the cost of downtime. To achieve SIL 3 safety functions will always need to 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. Planning for maintenance and renewal should also 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. Common cause failures dominate the PFD in all voted architectures of sensors and of final elements.
4. In the operations phase measurements of failure rates and of equipment deterioration provide 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 of all failures is necessary 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. 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] F.H.C. Marriott, '*A Dictionary of Statistical Terms*', 5th Edition, International Statistical Institute, Longman Scientific and Technical, 1990