Session Ten
Achieving Compliance in Hardware Fault Tolerance

Mirek Generowicz
FS Senior Expert (TÜV Rheinland #183/12)
Engineering Manager, I&E Systems Pty Ltd

Abstract

The functional safety standards ISA S84/IEC 61511 and IEC 61508 both set out requirements for 'hardware fault tolerance' or 'architectural constraints'.

The method specified in ISA S84 and IEC 61511 for assessing hardware fault tolerance has often proven to be impracticable for SIL 3 in the process sector. Many users in the process sector have not been able to comply fully with the requirements.

Further confusion has been created because there are many SIL certificates in circulation that are undeniably incorrect and misleading.

This paper describes common problems and misunderstandings in assessing hardware fault tolerance.

The 2010 edition of IEC 61508 brought in a new and much simpler and more practicable method for assessing hardware fault tolerance. The method is called Route 2_H.

This paper explains how Route 2_H overcomes the problems with the earlier methods.

The proposed new edition of IEC 61511 will be based on Route 2_H.

Why do we need Hardware Fault Tolerance?

The standards impose '**architectural constraints**' to compensate for the uncertainty in the failure rates and the assumptions made in the design.

AS IEC 61508 and AS IEC 61511 both set architectural constraints according the required integrity level.

The architectural constraints are characterised by '**hardware fault tolerance**', (HFT), the ability to perform a required function in the presence of a fault.

> '*Hardware fault tolerance is the ability of a component or subsystem to continue to be able to undertake the required safety instrumented function in the presence of one or more dangerous faults in hardware. A hardware fault tolerance of 1 means that there are, for example, two devices and the architecture is such that the dangerous failure of one of the two components or subsystems does not prevent the safety action from occurring.*'

AS IEC 61511 explains that hardware fault tolerance is necessary:

> '*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.*'

The simple calculation of probability of failure is not enough. If we don't have sufficient confidence in the failure rate data the calculated probability may be unrealistically optimistic.

We need to have a certain minimum level of fault tolerance in addition to showing that the calculated probability of failure is low enough to meet the SIL target. Exactly what level of fault tolerance we need depends on:
- The level of confidence we have in the failure rate data,
- The dominant failure behaviour (safe or dangerous)
- Whether we can detect and respond to failures.

Fault tolerance may be achieved by using redundant elements in a fault tolerant circuit architecture, for instance 2 valves in series:
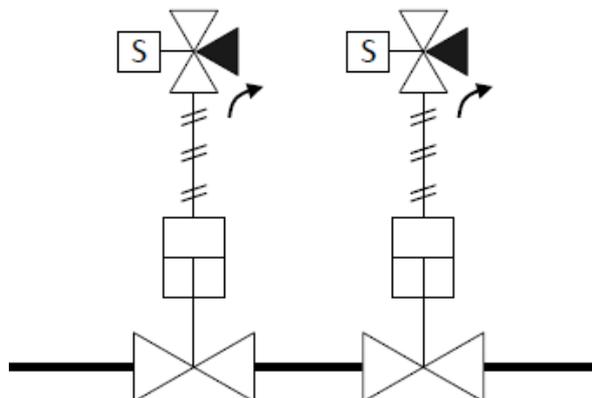
The AS IEC 61511-1 method for HFT can only be used for relatively simple architectures. The AS IEC 61508-2 methods can be applied to assess hardware fault tolerance requirements for complex architectures.

What is the problem?

AS IEC 61511 sets requirements for HFT in Sub-clause 11.4.

Table 6 specifies the level of HFT for sensors and final elements. The level of HFT required increases with SIL.

The basic table shows the requirement provided that the dominant failure mode is to the safe state, or dangerous failures are detected:

SIL	Minimum HFT
SIL 1	0
SIL 2	1
SIL 3	2

If the dominant failure is to dangerous state, and if we don't have effective diagnostics we need to increase the HFT:

SIL	Dominant failure to a dangerous state	Dominant failure to a safe state
SIL 1	1	0
SIL 2	2	1
SIL 3	3	2

Actuated shutdown valves generally have dominant failure to a dangerous state. They tend to jam or stick in an open position. They tend to leak. These failure modes are not only dangerous, they are also undetected.

The basic requirement is 4 valves in series to achieve SIL 3!
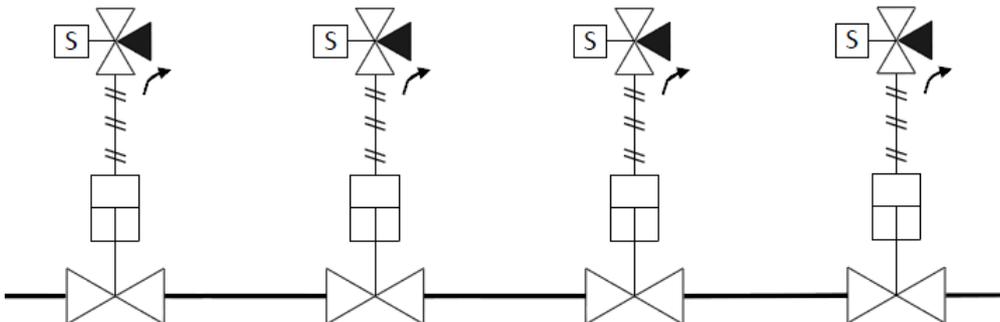
The standard allows us to reduce the HFT requirement if we can demonstrate 'limited adjustment' and 'prior use' (with extensive evidence):

SIL	Prior use, limited adjustment, dominant failure to a dangerous state	Prior use, limited adjustment, dominant failure to a safe state
SIL 1	0	0
SIL 2	1	0
SIL 3	2	1

The bare minimum requirement for SIL 3 is therefore to have 3 valves in series:
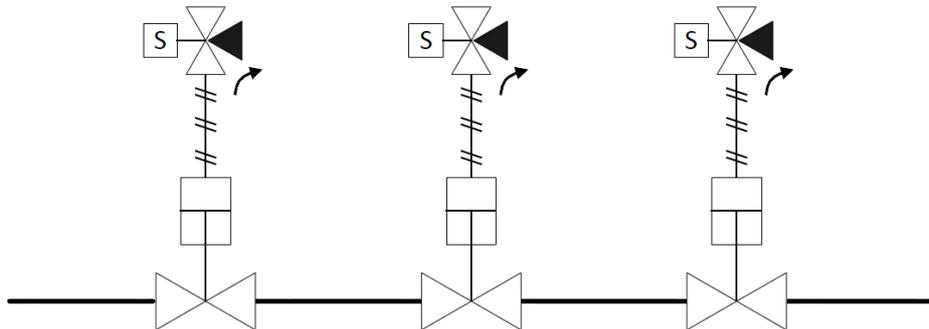
This is simply NOT practicable. Installing 3 valves rather than 2 increases capital cost as well as maintenance costs and it reduces reliability.

An alternative approach: AS IEC 61508 Route 1$_H$

AS IEC 61508 Route 1$_H$ is allowed as an alternative to AS IEC 61511 to determine the HFT required.

Route 1$_H$ distinguishes between simple 'Type A' devices and complex 'Type B' devices.

'Type A' devices have:
- Well defined failure modes
- Deterministic behaviour
- Sufficient dependable failure rate data

Other devices are classified as 'Type B'. These devices with complex behavior and failure modes, typically devices containing software.

Route 1$_H$ requires comprehensive data and documentation for every element and rigorous quality management and configuration management. Safety manuals must be provided for every element to demonstrate compliance to AS IEC 61508.

The requirements for 'Type A' are equivalent to those for 'limited adjustment' and 'prior use' in AS IEC 61511.

Route 1_H applies the concept of Safe Failure Fraction (SFF). This is another way of assessing whether the dominant failure is to the safe state. The maximum SIL that can be claimed depends on the HFT.

The results are very similar to those of the AS IEC 61511 method.

The following table shows that maximum SIL that can be claimed for Type A elements under Route 1_H, depending on the HFT and SFF:

Safe Failure Fraction of the element	Hardware Fault Tolerance		
	0	1	2
SFF < 60%	SIL 1	SIL 2	SIL 3
60% ≤ SFF < 90%	SIL 2	SIL 3	SIL 4
90% ≤ SFF < 99%	SIL 3	SIL 4	SIL 4
SFF ≥ 99%	SIL 3	SIL 3	SIL 4

If the SFF < 60% then the dominant failure mode is not to the safe state and to claim SIL 3 we still need HFT 2, requiring 3 valves in series:
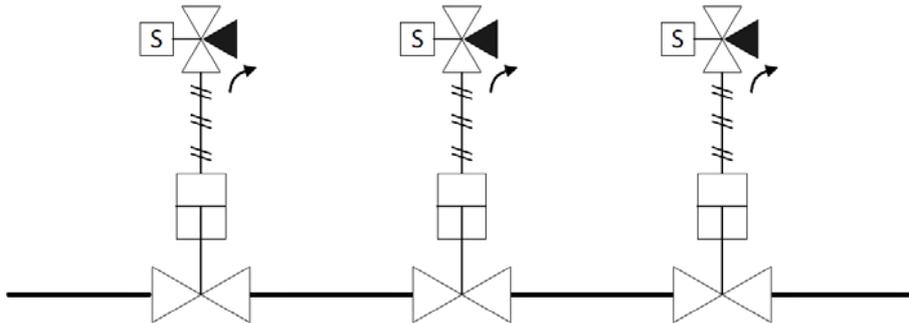
To claim SIL 3 with only 2 valves we need to prove that **SFF ≥ 60%:**
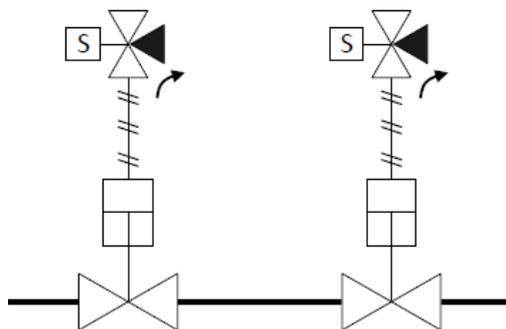
Common errors in trying to show compliance

The total failure rate is the sum of failure rates for 'safe' failures, those causing a trip (λ_S), plus the rate of 'dangerous' failures detected by on-line diagnostics (λ_{DD}) and rate of 'dangerous' failures that remain undetected (λ_{DU}):

$$\Sigma\lambda = \Sigma\lambda_S + \Sigma\lambda_{DD} + \Sigma\lambda_{DU}$$

The SFF is the proportion of failures that are either 'safe' (λ_S) or are 'dangerous' but detected by on-line diagnostics (λ_{DD}):

$$SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD})/ \Sigma\lambda$$

Understandably, equipment suppliers and designers have been creative in trying to prove that SFF ≥ 60%.

Error No. 1: No-effect Failures

The first trick is to add in irrelevant 'no-effect' failures as if they were 'safe'. For example, a typical valve and actuator assembly will have:

> $\lambda_S \approx 0.5 \times 10^{-6}$ failures per hour
>
> $\lambda_D \approx 1 \times 10^{-6}$ failures per hour,
>
> and no diagnostic functions, so
>
> $\lambda_{DD} = 0$
>
> SFF ≈ 0.5 / 1.5 ≈ 33%

'No-effect' failures have absolutely no effect on the safety function. A typical 'no-effect' failure might be a faulty position switch on the actuator.

Adding in the no-effect failures increases the SFF:

> $\lambda_S \approx 0.5 \times 10^{-6}$ failures per hour
>
> $\lambda_{NE} \approx 1 \times 10^{-6}$ failures per hour,
>
> $\lambda_D \approx 1 \times 10^{-6}$ failures per hour,
>
> $\lambda_{DD} = 0$
>
> SFF ≈ 1.5 / 2.5 ≈ 60%

The formula for SFF given in AS IEC 61508 has never allowed the inclusion of 'no-effect' failures. The 2010 revision AS IEC 61508 Ed. 2 (2010) added specific clarification that 'no-effect' failures must be excluded from SFF.

Beware that there are many certificates in circulation that are invalid because they take credit for 'no-effect' failures.

This example certificate is no longer valid and has been withdrawn:

Certificate of Conformity No.: 28711185   TÜVRheinland

Manufacturer: Cameron Italy S.r.l.
CAM Engineered Valves Voghera
Via Italo Betto, 11
I-27058 Voghera (PV)

Specifications: IEC 61508-1÷7:2010

Product: Side-Entry Trunnion Mounted Ball Valves

RESULT:
As per the TÜV Rheinland Italia Report No. FS 28711185 Rev. 0 we declare that the product meets the below requirements:

IEC 61508:   2010, part 1 to 7

Functional Safety of electrical/electronic/programmable electronic safety related systems;

Type A, Low Demand Mode, HFT=0, Systematic Capability=3

Safety Action	λ_D [1/h]	λ_{NE} [1/h]	SFF
Close / Open	2,86E-08	1,13E-06	> 90 %
Close with Tight Shut Off	8,41E-08	8,92E-07	> 90 %

For detailed results: see TÜV Rheinland Italia Report No. FS 28711185 Rev. 0.

As per these values, the aforementioned product can be used up to SIL 3 as a "single device".

Any certificate taking credit for 'no-effect' failures is invalid.

Beware that some of the commercial software packages commonly used for SIL calculations take credit for 'no-effect' failures (also called 'residual' failures) if the 'IEC 61508-2000' method is selected.

The 3rd edition of the SERH 'Safety Equipment Reliability Handbook' published by *exida* in 2007 takes credit for called 'residual' failures in the calculation of SFF. Users should recalculate the SFF excluding the 'residual' failures.

Error No. 2: Partial Stroke Testing

The following example certificate takes credit for partial stroke testing in the calculation of SFF:

Certificate of Conformity No.: 28711191 Rev. 1

TÜVRheinland®

Manufacturer: Cameron Italy S.r.l. – Ledeen Facility
Via Gandini, 4
I-27058 Voghera (PV)

Specifications: IEC 61508-1÷7:2010

Product: Pneumatic Actuator

RESULT:

As per the TÜV Rheinland Italia Report No. FS 28711191 Rev. 1 we declare that the product meets the below requirements:

IEC 61508: 2010, part 1 to 7

Functional Safety of electrical/electronic/programmable electronic safety related systems;

Type A, Low Demand Mode, HFT=0, Systematic Capability=3

Series	λ_D [1/h]	SFF
LIN…DA	3,19E-08	> 90 %
LIN…SR (FTC)	2,22E-08	> 90 %
LIN…SR (FTO)	1,97E-08	> 90 %
VA/GS/SY/HT/MT…DA GS/SY…P-A GS/SY…P-S	3,80E-08	> 90 %
GS/SY/HT/MT…SR GS/SY…P-A-SR… GS/SY…P-S-SR…	2,78E-08	> 90 %
VA…SR	2,46E-08	> 90 %

For detailed results: see TÜV Rheinland Italia Report No. FS 28711191 Rev. 1.

As per these values, the aforementioned product can be used up to SIL 3 as a "single device".

Partial stroke testing *can* be claimed as a diagnostic if it is sufficiently frequent.

AS IEC 61508-2 §7.4.4.1 defines the requirements for the frequency of diagnostic functions.

In low demand mode

> '*credit shall only be taken for the diagnostics if the sum of the diagnostic test interval and the time to perform the repair of a detected failure is less than the MTTR used in the calculation to determine the achieved safety integrity for that safety function.*'

The diagnostic interval must be included in the MTTR that is used in calculating probability of failure:

Mean Time to Restoration (MTTR)							
Fault detection time	Mean Repair Time (MRT)						
	Administrative delays (work orders, permits)	Technical delays, materials identification	Logistical delays, materials procurement	Active repair time			Reinstatement delay
				Fault localisation	Fault correction	Testing	

If the MTTR is extended to periods measured in months it will lead to a significant increase in the probability of failure of the safety function.

The same requirement applies to high demand mode and continuous mode functions that have HFT > 0.

In high demand mode and continuous mode functions with HFT = 0 then either:

- The diagnostic interval + time for safety action response must be less than the process safety time OR

- The diagnostic test rate must be at least 100 times more frequent than the demand rate.

Automatic weekly or daily testing *might* be sufficiently frequent for low demand applications in the process sector but it is usually impractical.

6-monthly testing cannot be classed as a diagnostic and does not contribute to improving SFF.

TÜV Rheinland has published a statement clarifying how these certificates should be interpreted:

△ TÜVRheinland®
Precisely Right.

TÜV Rheinland Industrie Service GmbH
Postfach, 51101 Köln

Dr. Thorsten Gantevoort
Kst. 969 / gan-nie

Tel.   +49/221/806-4061
Fax   +49/221/806-1539
Mail   Thorsten.Gantevoort
       @de.tuv.com
Web   www.tuv.com

2014-08-13

Failure Modes and SFF of final elements esp. valves, Revision 2

To whom it may concern

For the certification of final elements, especially valves, according to the requirements of Functional Safety standard IEC 61508:2010 for a certain SIL the safety parameter Safe Failure Fraction (SFF) is a crucial factor.

As the SFF is the ratio of safe plus dangerous detected failures to all failures it is necessary to have sufficient of the safe and dangerous detected failure, depending on the required SIL.

Regarding to the more precise definition of IEC 61508:2010 for safe failures, it is obvious that a final element - especially a valve - does not have sufficient safe failures (or even has no safe failures) in order to achieve a SIL higher than 1. Therefore a diagnostic measure has to be applied to the final element to increase the dangerous detected failures and the SFF.

The following requirements apply to diagnostic measures:

-   A diagnostic measure has to be an <u>automatic online</u> testing
-   The test frequency shall be at least 10 times higher than the demand rate
-   A partial stroke test normally can reach max. up to DC = 70 %
-   The Proof Test is <u>no</u> diagnostic measure and can therefore not be used to increase the SFF

An alternative approach for the determination of the required Hardware Fault Tolerance using an alternative definition of the SFF is defined in EN 161:2011/A3:2013. This approach is based on an FMEA and takes into account fault exclusions, which are treated as equal with detected faults. During the cause of the FMEA these fault exclusions have to be justified and proven. The method defined in EN 161:2011/A3:2013 requires a Hardware Fault Tolerance of at least HFT = 1 for SIL 3 systems. It has to be declared in the certificate, if this alternative approach was used for the estimation of SFF.

Best regards from Cologne

Automation, Functional Safety
Business Unit Applications & Systems

Test Centre for
Energy Appliances

ppa.

i. V.

i. V.

Dipl.-Ing. Heinz Gall

Dr.-Ing. Thorsten Gantevoort

Dipl.-Ing. Wolf Rückwart

TÜV Rheinland
Industrie Service GmbH
Am Grauen Stein
51105 Köln

Tel   +49 221 806-0
Fax   +49 221 806-1753
Mail industrie-service@
      de.tuv.com

Management board:
Stephan Frense (Spokesman)
Eckhard Lippold
Marcus Staude

Köln HRB 26876

Chairman of the supervisory board
Stephan Schmitt

Web www.tuv.com

Error No. 3: Assuming prior use without evidence

AS IEC 61511-1 §11.5.3 stipulates rigorous documentary requirements to support claims for 'prior use'.

The requirements are onerous and difficult to achieve in practice. Most users find it easier to demonstrate compliance to AS IEC 61508-2 and/or AS IEC 61508-3 but sourcing independently certified components.

Error No. 4: Assuming compliance to AS IEC 61508

AS IEC 61508-2 §7.4.9.6 requires that suppliers must provide a safety manual for each item that is claimed to be in compliance with the IEC 61508 series. Annex D describes very detailed requirements for what should be included in a safety manual.

Compliance cannot be claimed unless the safety manuals are provided. The information required in the manuals is similar to what is required to support claims of 'prior use'.

The solution: AS IEC 61508 Route 2$_H$

AS IEC 61508 Route 1H and AS IEC 61511 are based on having failure rates with a confidence level of at least 70%.

This means that 70% of the recorded time intervals between failures are longer than the MTBF to be used in the calculations.

In other words, the calculations are based on the failure rate $\lambda_{70\%}$, which is at least as high as 70% of the failure rates recorded.

The purpose of HFT is to compensate for uncertainty in the failure rate data and assumptions. If we can reduce the uncertainty we can reduce the HFT.

Route 2$_H$ is based on confidence level increased to 90%.
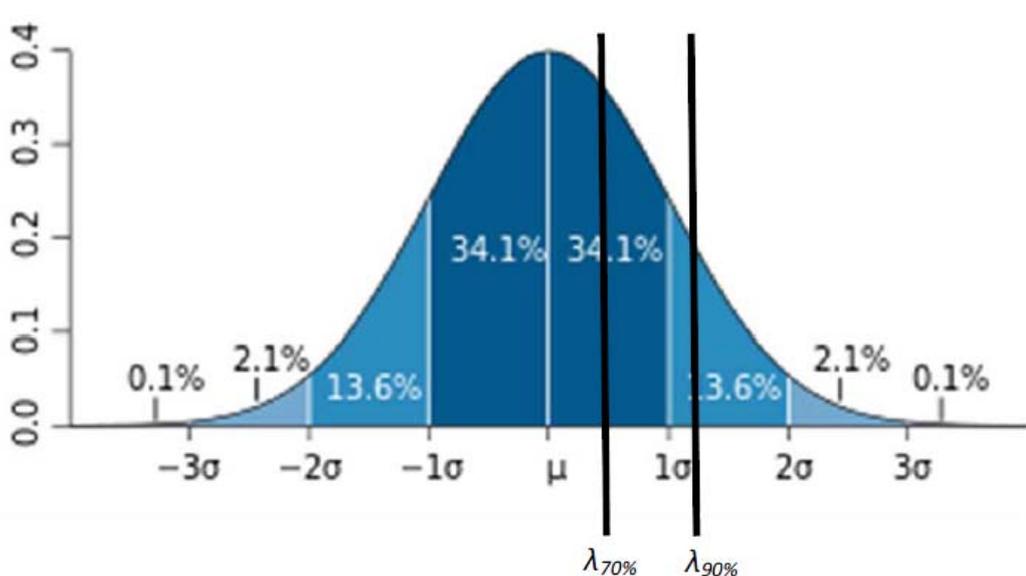
The requirement for Route 2_H is very simple. If the confidence level can be demonstrated then HFT of 1 is sufficient for SIL 3, and HFT of 0 is acceptable for SIL 2.

There is no need to consider SFF for Type A elements.

The requirement for Type B elements is simply that

> *'All type B elements used in Route 2_H shall have, as a minimum, a diagnostic coverage of not less than 60 %.'*

Failure rates with a confidence level of 90% can be expected to be approximately 0.8 standard deviation (0.8σ) higher than failure rates with a confidence level of 70%.

Finding data

Two dependable sources: OREDA and *exida* SERH

The OREDA 'Offshore Reliability Handbook' published by SINTEF gives the standard deviation and the mean for failure rates of components commonly applied in the hydrocarbons industry.

OREDA is based on extensive field experience, though in limited applications.

The SERH 'Safety Equipment Reliability Handbook' is published by exida.

The failure rates in exida SERH are calculated using FMEDA, but are based on extensive datasets for individual component parts.

The results are broadly consistent, though OREDA includes some 'site specific' failures and OREDA failure rates may be twice as high as corresponding exida rates.

Differing treatment of systematic failures

One of the reasons for the differences between sources is in how the decision is made whether to include or exclude failures from the datasets.

Failures of non-electronic components such as valves are always 'systematic' but can be treated as 'quasi-random'.

The standards require that systematic failures should be avoided or controlled through the application of appropriate techniques and measures. However many systematic failures cannot be eliminated easily. The intention of the standards is that these 'quasi random' failures should be included in the probability of failure calculations.

Judgement is needed in deciding which failures to exclude.

Confidence levels

The confidence level in *exida* SERH is stated as 70%.

OREDA shows full details of the spread of failure rates recorded, including the mean and the standard deviation.

The standard deviation allows us to estimate failure rates with 90% confidence level ($\lambda_{90\%}$) from failure rates with 70% confidence level ($\lambda_{70\%}$).

In a normal distribution approximately 90% of population lies within $\pm\ 1.6\sigma$ of μ. Typically failure rates are distributed over one or two orders of magnitude.

According to OREDA, the following failure rates are typical for actuated ball valves:

$\lambda_{50\%} \approx 2.3$ per 10^6 hours
$\sigma \approx 2.7$ per 10^6 hours
$\lambda_{70\%} \approx 3.6$ per 10^6 hours
$\lambda_{90\%} \approx 5.8$ per 10^6 hours

$\lambda_{90\%} / \lambda_{70\%} \approx\ 1.6$

This value of ratio of $\lambda_{90\%} / \lambda_{70\%}$ is typical.

We might infer that the calculated probability of failure for designs relying on Route 2_H will typically be around 60% higher than calculations based on Route 1_H.

Less dependable: Studies based on vendor returns

Many SIL certificates have been published that show failure rates up to *50 x lower* than those in SERH or OREDA **and** claiming 90% confidence level.

The example certificates shown above have:

$\lambda \approx 3 \times 10^{-8}$ per hour for a ball valve
$\lambda \approx 3 \times 10^{-8}$ per hour for a pneumatic actuator
$\Sigma\lambda \approx 6 \times 10^{-8}$ per hour for the assembly

For similar equipment, SERH has
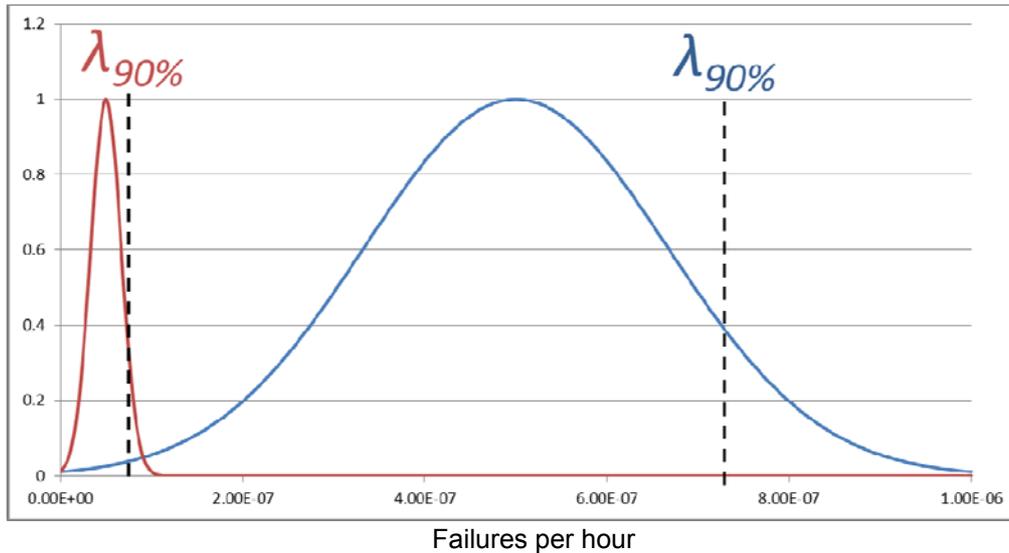$\lambda \approx 1.4 \times 10^{-6}$ per hour

OREDA has
$\lambda \approx 3.6 \times 10^{-6}$ per hour.

Note that confidence levels are related to the *spread of data* in a given dataset.

90% confidence levels may be claimed with small datasets, the confidence level is not related to the validity or applicability of the measured failure rates.

Failures per hour

Studies based on vendor returns may inadvertently exclude many failures that were not reported to the vendor. They may also exclude failures considered to be 'systematic' or 'outside the design envelope'.

Low failure rates from restricted datasets may be unrealistically optimistic.

Most dependable: The user's own data

The difficulty is in the large volume of operating experience required. It needs the equivalent of decades of experience with a sizeable population of devices.

Analysis of failure causes is just as important as failure rates. Common systematic causes must be controlled.

IEC 61511 Edition 2 – proposed for release in 2015

The proposed next edition of IEC 61511-1 specifies HFT requirements based on Route 2_H.

HFT of 1 will be sufficient for SIL 3.

SIL	Minimum required HFT
SIL 1	0
SIL 2 (low demand mode)	0
SIL 2 (high demand/continuous mode)	1
SIL 3	1
SIL 4	2

The proposed draft excludes the requirement for 90% confidence level.

Conclusions

The HFT methods in AS IEC 61511 and AS IEC 61508 Route 1_H do not work well in practice for the process sector. These methods require 3 valves in series (1 out of 3) to achieve SIL 3.

IEC Route 2_H is based on confidence level increased to 90%. It is much simpler and easier to apply. It allows SIL 3 to be achieved with only 2 valves as final elements.

The new edition of IEC 61511 will apply Route 2_H though without an explicit requirement for 90% confidence levels.

OREDA and *exida* SERH provide failure rate data that are widely accepted as being dependable. These references provide enough information to allow us to infer failure rates with 90% confidence levels.

There are many certificates in circulation that claim failure rates that are much lower than the rates published by OREDA and *exida*.

Users should collect their own data. Requirements for collection of evidence are onerous. A large volume of evidence is required. User should compare their failure rates with those in OREDA and SERH.

Failure rates from different sources should always be compared and assessed for plausibility. For Route 2_H a conservative approach should be taken, the complete spread of failure rates should be taken into account.

Published failure rates for valves all include systematic failures. All valve failures are essentially systematic in nature and can be avoided or controlled to some extent. In evaluating failure rates the effectiveness of the planned operation and maintenance should be considered. Particular attention should be given to identifying and controlling common cause failures as these will almost always dominate in the calculated probability of failure.

There are some certificates in circulation that take credit for 'no effect' failures or for partial stroke testing in determining SFF. These certificates must be interpreted with caution. It is not valid to claim SFF > 60% for valves by:
- Taking credit for 'no effect' failures
- Taking credit for infrequent partial stroke testing as a diagnostic

Certificates on their own are not sufficient as evidence of compliance to AS IEC 61508-2 and AS IEC 61508-3. Detailed safety manuals must be provided in accordance with AS IEC 61508-2 Annex D.

References

AS IEC 61511.1-2004 'Functional safety—Safety instrumented systems for the process industry sector
Part 1: Framework, definitions, systems, hardware and software requirements'

AS IEC 61508.2-2011 'Functional safety of electrical/electronic/programmable electronic safety-related systems
Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems'

SINTEF 2009, 'OREDA Offshore Reliability Handbook' 5th Edition
Volume 1 – Topside Equipment

exida.com L.L.C. 2007, 'Safety Equipment Reliability Handbook' 3rd Edition
Volume 3 – Final Elements

YouTube video http://youtu.be/SHAiFH4v_K8
'The exida FMEDA Process – Accurate Failure Data for the Process Industries'

Dr. William M. Goble, CFSE, Exida Consulting, February 2012 'Field Failure Data – the Good, the Bad and the Ugly'
http://www.exida.com/images/uploads/Field_Failure_Rates-good_bad_and_ugly_Feb_2012.pdf