YOKOGAWA

Co-innovating tomorrow™

Effects on PFDavg

Due to changes during the operational lifetime of a Safety Instrumented Function

White paper - January 2021

Bulletin 43D07T31-03EN

CONTENTS

White paper: Effects on PFDavg
Due to changes during the operational lifetime of a Safety Instrumented Function

General introduction

Processes in the Process Industry are more and more safeguarded using instrumented safeguarding systems according the IEC61511 (Functional safety - Safety instrumented systems for the process industry sector). The life of an instrumented safeguard starts at the engineering table of a project team. Often the requirements from an operational point of view are not (clearly) specified, resulting in engineered solutions which are sometimes impractical during the operational phase of a plant.

Most processes are running within a certain process operating window. With all the controls, alarming and operator actions the number of demands on the safety system is (relatively) low, in the order of years. As in that time the safety system is not acting, there is an increasing uncertainty that the safety system will perform the safety action when required. To ensure an instrumented safeguard will perform the safety function periodic proof testing is done as part of regular maintenance.

This white paper will specifically address the issue of proof testing, extension of lifetime and changed components with respect to the following facts:

- System Lifetimes are extended
- Changed Proof Test Intervals caused by
  - Proof tests are missed out to conduct
  - Proof Test Interval extension (or reduction)
- Changed Proof test procedures (including practices not conform procedures)
- Different components are used in instrumented safeguards over the system lifetime

All above situations will lead to a need to recalculate the PFDavg value of a Safety Instrumented Function (SIF) to maintain the Safety Integrity Level (SIL).

Short introduction on SIL

The IEC61511 recognizes Safety Instrumented Functions (SIFs) as safeguarding loops. This means that a complete function should be considered from the sensor, via a logic solver to the final element, including all interfaces in between. This is sometimes also called the pipe-to-pipe approach. Refer to below Figure 1:

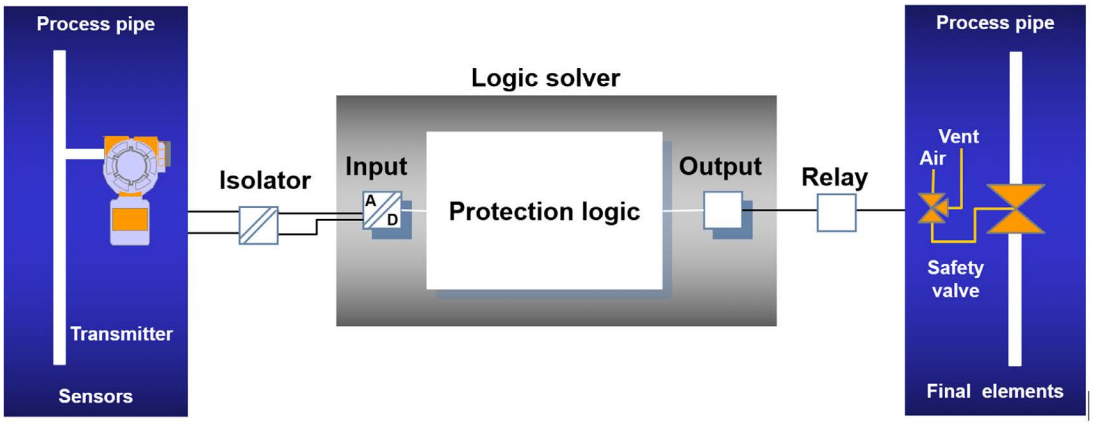

Figure 1 Safety Instrumented Function

Reliability of a Safety Instrumented Function is expressed in a Safety Integrity Level (SIL). There are four Safety Integrity Levels expressed as SIL1 to SIL4, whereas SIL1 has the lowest reliability requirements and SIL4 the highest.
Applying the IEC61511 correctly means that the following items must be considered to reach and maintain a required SIL:

- Probability of a failure on demand (PFDavg) of the complete pipe-to-pipe SIF
- Hardware Fault Tolerance (HFT) of all the pipe-to-pipe devices in the SIF
- Systematic Capability (SC) of both the pipe-to-pipe device manufacturers, as well as the end-user, (EPC) (sub) contractors, SIS integrators, etc.

This white paper will focus on PFDavg only.
Table 1 shows the relation between the SIL, PFDavg and RRF.

DEMAND MODE OF OPERATION		
Safety Integrity level (SIL)	**PFDavg**	**Required risk reduction**
4	$\geq 10^{-5}$ to 10^{-4}	> 10 000 to ≤ 100 000
3	$\geq 10^{-4}$ to 10^{-3}	> 1 000 to ≤ 10 000
2	$\geq 10^{-3}$ to 10^{-2}	> 100 to ≤ 1 000
1	$\geq 10^{-2}$ to 10^{-1}	> 10 to ≤ 100

Table 1 Safety integrity requirements: PFDavg (IEC61511-1 – table 4)

Note that the PFDavg is a statistical approach based on constant failure rates during the lifetime of the components.
Depending on the risk assessment method a specific Risk Reduction Factor (RRF) may be required to be met. The RRF can be calculated by taking the reciprocal value of PFDavg (RRF = 1/PFDavg).

The PFDavg values of all safety components in a specified SIF must be added up to reach the total PFDavg of the SIF and this value can be compared to a specific SIL.

Proof test

As described earlier during the lifetime of a SIF proof testing is conducted to see if a SIF is working.
When the proof test is 100 % effective this means that after each proof test the SIF is considered without failures. This is represented by Figure 2:

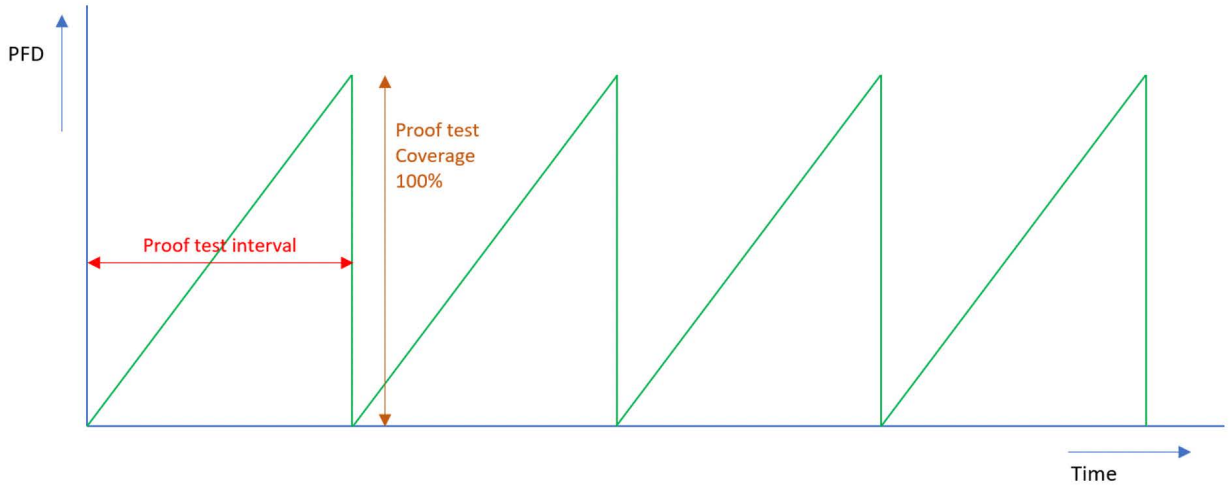

Figure 2 Proof test with 100% coverage

In practice 100% effective proof testing is unrealistic.
Having a less than 100% effective proof test means that after a proof test some undetected failures can/will exist, and the Probability of Failure on Demand (PFD) therefore will increase. The effectiveness of a proof test is expressed in a fraction called Proof test Coverage (PC). When the total PFD increases, this also means that the total average PFD (PFDavg) will increase, Figure 3.

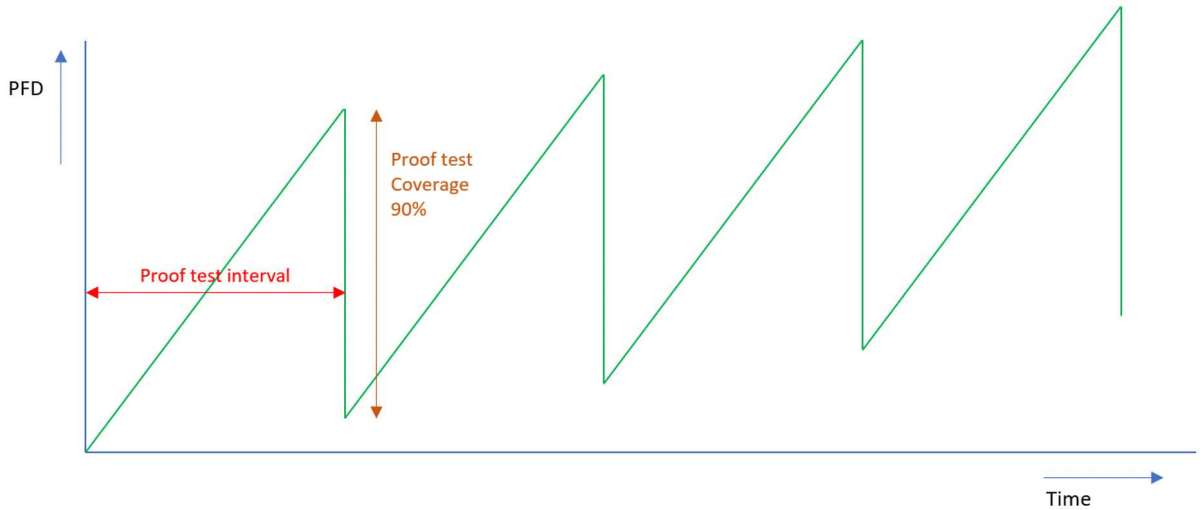

Figure 3 Proof test with 90% coverage

Impact of changes during the lifetime

Calculations of the PFDavg can be performed using different calculation methods ranging from extensive modelling to simplified formulas. This paper will address a practical approach based on the simplified formulas.

For a (component with) 1oo1 voting the PFDavg consists of a portion of failures detected during a proof test (blue part) and a portion of undetected failures during a proof test (green part).

PFDavg = [1/2*PC*λDU*T] + [1/2*(1-PC)*λDU*TL] **[Equation 1]**

Whereas:
PFDavg : average probability on demand
PC : Proof test Coverage
λDU : dangerous undetected failure rate
T : Proof test interval
TL : Lifetime of the SIF

Similar for a 1oo2 voting:
PFDavg = [1/3*(1-β)2*PC2*λDU2*T2]+[1/2*β*PC*λDU*T] + [1/3*(1-β)2*(1-PC)2*λDU2*TL2]+ [1/2*β*(1-PC)*λDU*TL]

[Equation 2]

Whereas:
β : Common Cause factor (the risk of a (near) simultaneous failure of redundant parts)

In the following sections the effect on PFDavg of several changes during the lifetime of a SIF are discussed.

Lifetime extension

When designing a SIF also a lifetime (TL) will need to be specified. Over the whole lifetime the applicable SIL needs to be met. Therefore, the PFDavg value should be in this SIL range. Extending the lifetime will increase the PFDavg with the factor not detected by a proof test, hence the lifetime is directly proportional with the PFDavg. Depending on the proof test coverage the increase of PFDavg can be significant.
In practice this means that the calculation with equation 1 (for 1oo1 voting) or equation 2 (for 1oo2 voting) must be done with a longer lifetime TL as only change.

Please note that when extending the lifetime additional focus on the useful lifetime of the components needs to be considered. For example, for most solenoid valves the failure rates are only guaranteed for 5 years (useful lifetime = 5 years).

Changed Proof Test Interval

A change in proof test interval can be caused by:
- Missing to conduct a proof test within the specified Proof Test Interval (PTI)
- Proof Test Interval extension (or reduction)

In operational environments proof tests are sometimes delayed (due to ad hoc operational considerations or operational scheduling) or totally missed. A proof test is considered as missed when a proof test is not performed at all or delayed with more than 10% of the specified proof test interval.
The IEC61511 considers Proof Testing to be part of regular maintenance so in case of an incident it is found Proof Testing has not been conducted (in time) this can be considered as negligent maintenance and authorities and/or insurance companies can prosecute the responsible persons.

Proof testing is usually labour extensive and therefore costly. Sometimes also the proof test interval selected during the project phase is not practical with respect to the operation of the plant. To reduce the operational costs, optimize the process or fulfil changed SIL requirements, the proof test interval might be extended or reduced.

A missed or extended/reduced proof test interval is affecting the PFDavg value. The calculation of the PFDavg must be performed again.
Since multiple proof test intervals are now introduced for a 1oo1 voting the equation 1 needs to be adjusted to suit these proof test intervals. Only the part of the portion of failures detected during a proof test (blue part) is affected. That means that the equation will now become:

PFDavg = X*[1/2*PC*λDU*T1] + (1-X)*[1/2*PC*λDU*T2] + [1/2*(1-PC)*λDU*TL] **[Equation 3]**

Whereas:

T1	: Initial Proof Test interval
T2	: Changed Proof Test interval
X	: fraction of the TL with Proof Test Interval T1

For a 1oo2 voting:

PFDavg = X*([1/3*(1-β)2*PC2*λDU2*T12]+[1/2*β*PC*λDU*T1]) +
(1-X)*([1/3*(1-β)2*PC2*λDU2*T22]+[1/2*β*PC*λDU*T2]) +
[1/3*(1-β)2*(1-PC)2*λDU2*TL2]+ [1/2*β*(1-PC)*λDU*TL] **[Equation 4]**

Changed Proof Test Procedure

Proof test Coverage (PC) is the percentage of dangerous undetected failures (λDU) that can be detected during a proof test. During the design phase of the lifecycle a proof test procedure has to be developed of which a proof test coverage can be derived. In some of the safety manuals of safety components specific procedures are described with a certain proof test coverage.
During the operational phase improper proof testing might be observed or the original proof test procedure might be impractical or too labour intensive.
To reduce the operational costs, optimize the process or fulfil changed SIL requirements, the proof test procedure might be changed, resulting in a changed proof test coverage. A changed proof test coverage is affecting the PFDavg value and therefore the PFDavg calculation must be performed again

Since multiple proof test coverages are now introduced for 1oo1 voting the equation 1 needs to be adjusted to suit these proof test coverages. Both parts of the equation will now be affected. That means that the equation will now become:

PFDavg = Y*([1/2*PC1*λDU*T] + [1/2*(1-PC1)*λDU*TL]) + (1-Y)*([1/2*PC2*λDU*T] + [1/2*(1-PC2)*λDU*TL])
[Equation 5]

Whereas:
PC1 : Initial Proof test Coverage
PC2 : Changed Proof test Coverage
Y : fraction of the TL with Proof test Coverage PC1

For a 1oo2 voting:
PFDavg = Y*([1/3*(1-β)2*PC12*λDU2*T2]+[1/2*β*PC1*λDU*T]+
[1/3*(1-β)2*(1-PC1)2*λDU2*TL2]+ [1/2*β*(1-PC1)*λDU*TL]) +
(1-Y)*([1/3*(1-β)2*PC22*λDU2*T2]+[1/2*β*PC2*λDU*T]+
[1/3*(1-β)2*(1-PC2)2*λDU2*TL2]+ [1/2*β*(1-PC2)*λDU*TL]) **[Equation 6]**

Different components are used in instrumented safeguards over the system lifetime

During the design phase of the life cycle decisions are made by the project team about the components to be used. During the operational time some of these components might be the cause of operational problems e.g. spurious trips due to the specified measurement type or location or high maintenance costs caused by e.g. unexpected high amount of errors with a specific device type (sometimes called bad actors). Sometimes observations are made that specific components are causing the SIF to fail to operate because of incorrect type of measurement for the specific process (e.g. process fluids are blocking small diameter of piping to a pressure transmitter and remote seals are required) or valves that are prone to accumulate dirt and will not operate.
In most of these cases the operating company will start a search for different components that will be suitable for their process. These different components come with their own failure rates which are very likely to be different from the failure rates of the components to be replaced and therefore the PFDavg is affected.

The PFDavg for the device can be calculated with the normal simplified formulas. The component is considered as new, therefore as the new component will be integrated in an already existing SIF the lifetime (TL) of the component can be reduced to match the remaining lifetime of the SIF.

In practice this means that the calculation with equation 1 (for 1oo1 voting) or equation 2 (for 1oo2 voting) must be done with the remaining lifetime TLR.

It should be noted that changing components also might impact the Proof test interval (T), Proof test Coverage (PC) and the Common Cause factor (β). So before starting calculating these factors must be re-evaluated as well.

For a 1oo1 voting:
PFDavg = [1/2*PC*λDU*T] + [1/2*(1-PC)*λDU*TLR] **[Equation 7]**
Whereas:
TLR : Remaining Lifetime of the SIF

For a 1oo2 voting:
PFDavg = [1/3*(1-β)2*PC2*λDU2*T2]+[1/2*β*PC*λDU*T] +
[1/3*(1-β)2*(1-PC)2*λDU2*TLR2]+ [1/2*β*(1-PC)*λDU*TLR] **[Equation 8]**

Conclusion

All changes/modifications to a SIF must be re-assessed and re-verified to be able to show the SIF meets the required SIL. When faced with lifetime extension, changes in proof test intervals/procedures, improper proof testing or changed components this means that calculations must be re-done.
In case the conclusion is that the PFDavg value of the complete SIF remains within the applicable SIL range no additional changes are required. However, it might happen that the PFDavg will end up in a lower SIL than specified. This means additional engineering is required.

It should be noted that sometimes argued decisions can be made. This really depends on the requirements and the design of the SIF. E.g. if a SIF is designed in such a way that the PFDavg value is much smaller than the specified SIL (for example SIL 1 is required and PFDavg is in the SIL3 range) changes as described in this paper might not significantly influence the reliability of the SIF.

All changes/modifications must be documented and kept with all other life cycle documents.

More information

Would you like more information? Please ask your local contact person of Yokogawa or contact Marketing in the Netherlands via marketing@nl.yokogawa.com, +31 88 464 1339.

Author

Arjan Kroon, Safety Specialist at Yokogawa Europe Solutions B.V.

YOKOGAWA EUROPE SOLUTIONS BV
Euroweg 2, 3825HD Amersfoort, the Netherlands
http://www.yokogawa.com/eu

YOKOGAWA Co-innovating tomorrow™

Bulletin 43D07T31-03EN