Safety-PLC's striking role for Partial Valve Stroke Testing

Bert Knegtering
Honeywell Safety Management Systems
P.O. Box 116
5201 AC 's-Hertogenbosch
The Netherlands
bert.knegtering@honeywell.com

Key words

Safety-PLC, Safety Integrity, IEC 61508, Partial Valve Stroke Testing

Abstract

Partial Valve Stroke Testing or PVST, is an emerging concept to automatically increase the performance of Safety Instrumented Systems. PVST is a concept where safety-related valves like ESD valves and shut-off valves are automatically tested concerning failure modes that are related to valve sticking and slowing down operation. Current trends in the industry show an upcoming number of dedicated technical PVST solutions by various automation and instrumentation vendors.
The added value of PVST within the process industries is a significant reduction of the frequency of required manual periodic valve proof tests, its related manual test cost and reduced spurious trips due to manual errors. Partial testing is performed by additional automated test instrumentation, which can easily be initiated and controlled by the safety-instrumented systems' logic solver such as the safety-related PLC.
This paper will discuss practical examples of Partial Valve Stroke Testing in which it appears that SIL 1 rated valves can be upgraded to SIL 2, and off-line proof test intervals which can be extended from 2 to 5 years.

1 Introduction

Trends in the market place show an increasing demand for partial valve stroke testing techniques. At the same time, more and more vendors of process instrumentation offer technical solutions that have the ability to realize a certain level of partial valve stroke testing. The underlying cause for this trend is partly due to the growing insight that cost can be saved by automated on-line partial valve stroke testing and partly by new safety standards that push the industry to implement a minimum level of automated on-line fault diagnostic coverage. Safety PLC-based systems appear to play an important central role concerning the initiating, registration an responding to PVST, whereas other solutions may use non-safety related equipment.

2 What is PVST?

A substantial amount of safety valves that are applied in process installation are only used in case of an out-of-control process. The frequency by which these dedicated safety valves are activated during its entire lifetime of many years, is in most situations restricted to only once or a few times. Some safety valves will never need to come to action. Because of the importance of reliable operation of these valves in case of such an out-of-control process, periodic tests will reveal possible failures. Due to the very rare moments that the valve is operated, one of the most likely failure modes that may occur is sticking of the valve. Physical influences may lead to erosion, corrosion or pollution, which obstruct the valve to move and correctly close or open. During periodic off-line proof tests, these failure modes can be revealed, but due to the fact that such off-line tests can most times only be done during a complete unit or plant shut-down, such tests normally only take place once per year or even once per couple of years.

One can imagine the impact of valve sticking in combination with the low-test frequency on the reliable operation of the valve. At the moment the valve does not function anymore, the failure will reside in the valve until the next off-line test. The longer the time span until this next test, the higher the probability will be that due to an out-of-control process, a demand is done on this valve.

As a result of this, the reliability performance (i.e. the likelihood of the availability of its functionality) of the valve globally depends on two aspects. First of all, the mean time to failure due to corrosion and pollution, and secondly the time it takes to detect and resolve this failure.
Partial Valve Stroke Testing (PVST) is a concept that is characterized by partly on-line valve testing. This partly testing concerns the test of the valve whether it is sticking at its defined normal position or whether it is not sticking and still able to move. PVST implies the partially opening or closing of the valve, e.g. 10% of a full stroke, detection with sensors like position switches that the valve has reached this 10% movement and moving the valve back to its normal position. If this test is done within a relatively short predefined time frame, it will in many applications not lead to a disturbance of the process and can therefore be done on-line.

Figure 1 shows a typical example of a basic PVST solution which can be found in ISA-TR84.0.002 [ISA84b]. This PITT (Partial Instrument Trip Test) solution uses a second solenoid to create a controlled leakage of the valve and uses the normal trip solenoid for emergency situations. Obviously, it must be noted that for this solution the valve including the actuator is tested but not the normal trip solenoid. This is a typical situation that illustrates the importance of a thorough and dedicated Failure Mode and Effect Analysis (FMEA) of the initial valve including the additionally needed PVST equipment.

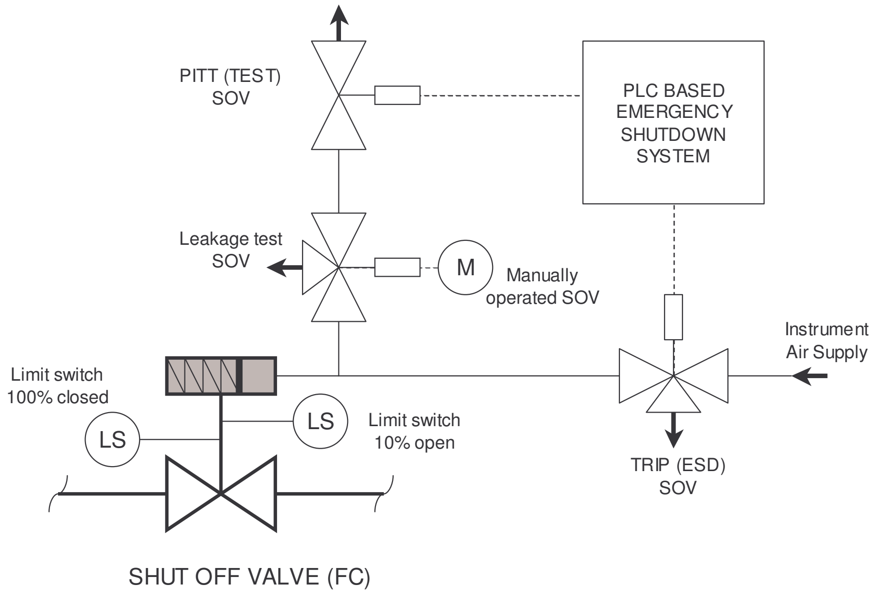

Figure 1 Example of a PVST solution

3 Market expectations and needs

In July 2003 a survey was conducted among 16 operating companies in the process industries, which were stationed in the Netherlands and Belgium. Based on this customer survey, the following general conclusions were drawn:

- More or less all operating companies in the process industries are familiar with the PVST-concepts.
- The general opinion is that PVST adds value to their business.
- To date, not many companies have already applied the PVST concept.
- Different companies have different ideas on the added value and potential negative aspects of PVST.

Al together, it was concluded that there is a serious market for PVST solutions, which can only be swept if the added value can be proven.

4 Detectable failures

Failures related to 100% operation i.e. fully closing or fully opening are not covered by PVST, because testing against such failure modes normally results in an undesired process upset or shutdown. As in most cases the most dominant failure mode appears to be sticking of a valve at its normal position, PVST is considered to contribute significantly to the detection of this type of failures and resolve them in a relatively short time period. The reliability of the valve will therefore significantly increase. This will be explained in the next section. Typically, PVST might help to deduce the failure modes that are related to:

- Valve sticking
- Packing problems

- Leakage (pneumatic)
- Actuator spring rate deviation
- Delayed operation

The ability to automatically and on-line detect instrument failure by additional test instrumentation, is normally expressed in terms of Diagnostic Coverage or DC. The higher the fraction of failures that is automatically detected, the higher the DC. This DC is a parameter that is often expressed in a percentage or the coverage factor. Obviously, this DC level depends on the PVST technique that is used and it depends on the application for which the valve is used. Figure 2 shows an example of the failure mode categories of a safety valve that is normally open and normally energized. In case of an out of control process, the valve needs to close. The design specifications such as normally open or normally closed, normally energized or normally de-energized, determine the consequence per failure mode i.e. resulting in a safe state or in a potentially dangerous failure to function. These design specifications combined with the likelihood of the occurrence of these failure modes will subsequently determine the DC level.

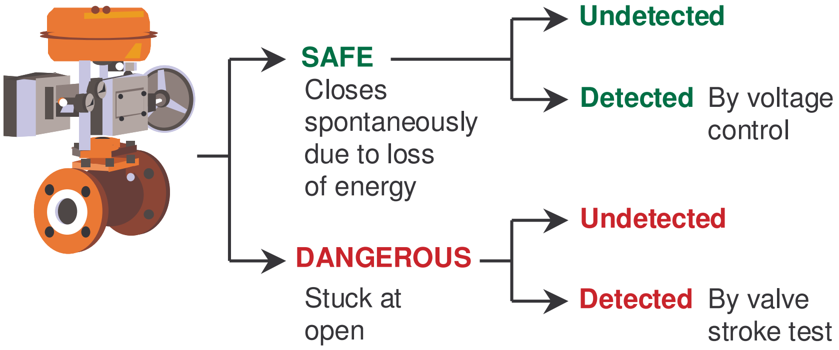

Figure 2 Failure modes of a safety valve

Therefore, concerning the establishment of the actual achieved level of DC a FMEA should be conducted. Aspects like the design of the valve, the design of the PVST equipment, the application of the valve, the environmental circumstances, etc. should all be taken into account.

5 Theoretical analysis of the impact of PVST on the PFD performance

Based on a number of valve related reliability influencing parameters the Probability of Failure on Demand (PFD) value can be calculated. Equations for the PFD calculation are for instance given by safety standards like IEC 61508 (part 6 annex B).
In case no tests are done and no repairs are made, one can imagine that the PFD of the valve will increase over time. Therefore, a distinction needs to be made between the momentary PFD or PFD(t) and the average PFD with regard to a predefined time period, such as the off-line proof test interval. The following set of equations illustrates the relationship between the PFD of the valve and the most relevant reliability influencing parameters. These parameters are:

— $\lambda_{Dangerous}$: The rate or frequency of dangerous failures of the valve
— DC : Diagnostic Coverage
— TI : The off-line proof Test Interval

— MTTR : Mean Time To Repair

$$PFD(t) = (1 - DC) * \lambda_{Dangerous} * t^{0 \to TI} + DC * \lambda_{Dangerous} * t^{0 \to MTTR} \qquad \text{(Equation 1)}$$

$$PFD_{Average[0 \to TI]} = \int_{t=0}^{t=TI} \frac{PFD(t)}{TI} dt \qquad \text{(Equation 2)}$$

With the assumption that MTTR << TI, this results in:

$$PFD_{Average[0 \to TI]} = \frac{(1 - DC) * \lambda_{Dangerous} * TI}{2} + DC * \lambda_{Dangerous} * MTTR \qquad \text{(Equation 3)}$$

As end-users of valves are primarily interested in the reliability performance of a valve for a particular period of time, the $PFD_{Average}$ value is considered to be the most important performance indicator. The DC is one of the parameters that strongly influence the $PFD_{Average}$ value.

6 PFD calculations based on different DC factors

Based on a MTTR of 8 hours and a dangerous failure rate of 10^{-2} [failures/hour], a number of $PFD_{Average}$ calculations are made for a range of Test Intervals from 1 year up to 10 years, and for a range of DC factors, for 0%, 30%, 60%, 90% and 99%. Figure 3 shows a graphical plot of the calculation results.

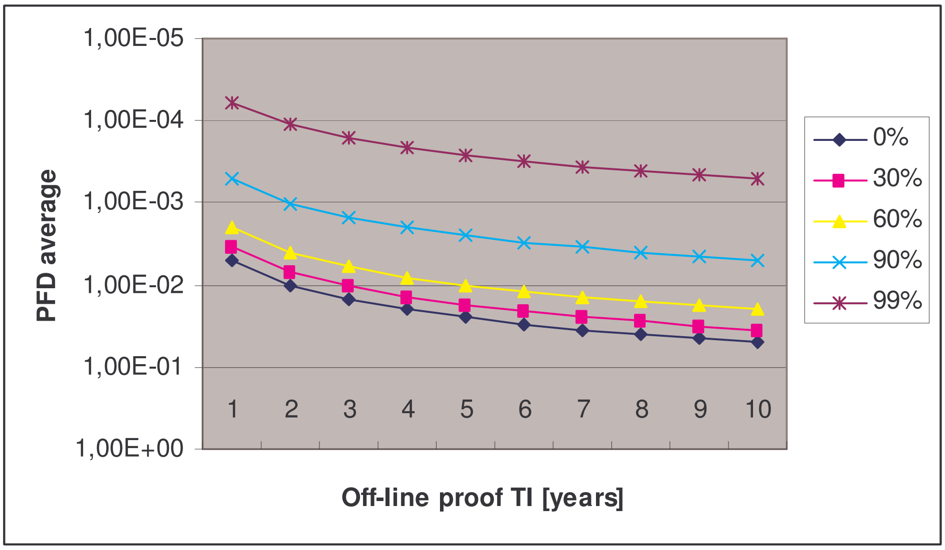

Figure 3 $PFD_{Average}$ related to TI for different DC factors

Figure 3 illustrates that with regard to the various DC factors, it is observed that significantly different $PFD_{Average}$-values are achieved. Figure 3 also illustrates that the higher the DC-factor, the smaller the $PFD_{Average}$ will be. Based on this observation it is concluded that with a high DC, the $PFD_{Average}$ changes

such that a higher Safety Integrity Level (SIL) can be claimed. This is a major advantage that can be achieved by PVST and might prevent the need of additional valves that would be required to realize the needed $PFD_{Average}$ by implementing fault-tolerance.
Obviously, it must be noted that also the other SIS-subsystems need to be considered when it come to calculation of the $PFD_{Average}$ of the complete safety instrumented function.

The graphical plot illustrated in Figure 4 zooms into part of Figure 3 for the parameter values TI for 1 to 5 years and for DC factors 0%, 30% and 60%.

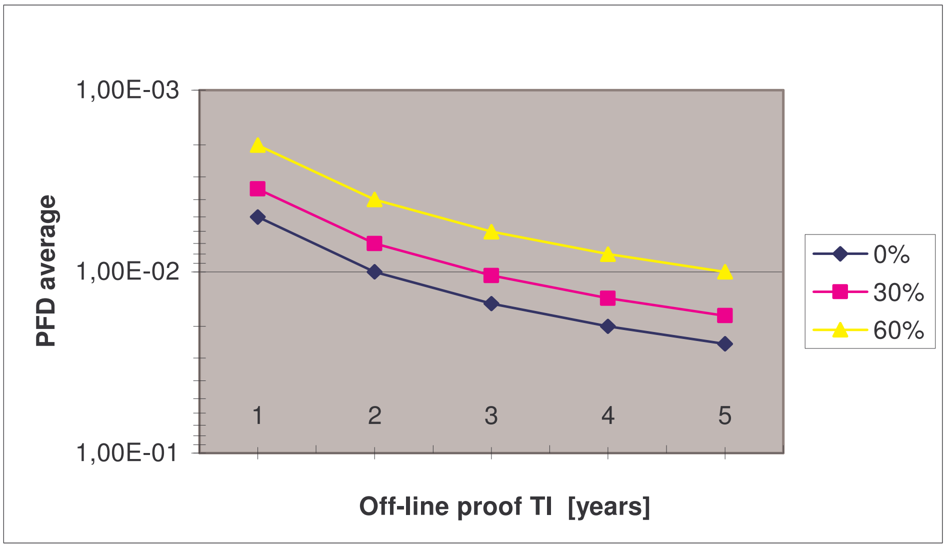

Figure 4 $PFD_{Average}$ related to TI for 1 to 5 years and for DC factors 0%, 30% and 60%

Figure 4 clearly shows the critical boundary between $PFD_{Average}$ values that are higher than 1,00E-2 and values that are smaller than 1,00E-2. According to safety standards like IEC 61508 the 1,00E-2 represents the boundary between SIL 1 and SIL 2. The importance of PVST is clearly illustrated in Figure 5. This figure shows that if;

— DC = 0% the maximum acceptable TI = 2 years

— DC = 30% the maximum acceptable TI = 3 years

— DC = 60% the maximum acceptable TI = 5 years

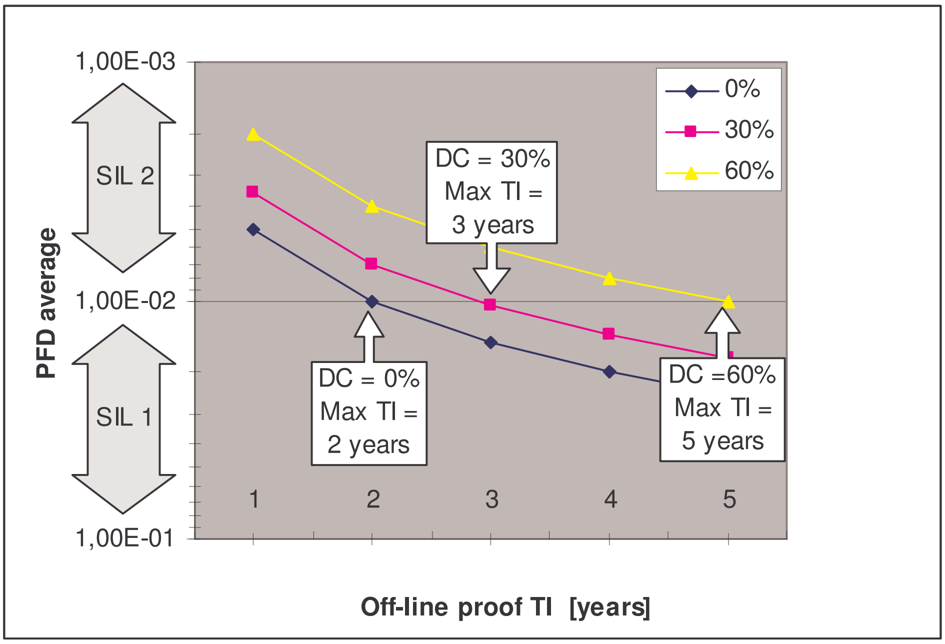

Figure 5 Illustration of the impact of DC on the maximum TI for SIL 2

Based on the calculation, whereas due to PVST the DC is increased from 0% up to 60%, it is concluded that a significant gain is achieved by an extended maximum acceptable off-line proof test interval from 2 years up to 5 years.

7 Architectural constraints

SIS standards like IEC 61508 and IEC 61511 have defined restrictions on the use of a SIS subsystem or device for particular SIL's. These constraints are based on the fault-tolerance, the novelty of the device and the so-called Safe Failure Fraction or SFF. This SFF represents a combination of the fraction of failures that result in a safe state and the fraction of failures that are automatically detected. Typically, using PVST, a DC level of 60-90% is achieved. This DC, combined with the fraction of failures which result in a safe state, result in a SFF of above 60% or sometimes even above 90%. The practical example as given in the ARC white paper [ARC01], where the hazard rate is reduced from 1500 years into 13,000 years, implies a DC level of 88,5%. This would most likely result in an achieved SFF of above 90%. Concerning the architectural constraints, the subject valve would therefore not be restricted to be used up to and including SIL 3.

8 Current technical solutions

Investigation of the current market place of PVST solutions and products has resulted in the observation of about a dozen different types of technical solutions or products as offered by the various instrumentation vendors. These solutions are typically characterized by features such as the application of limit switches, valve positioners, jammers, etc. Most of these techniques offer their test results in graphical formats, often named valve signature, valve footprint, valve fingerprint, etc.

Depending on the typical application and the most dominant failure modes that should be covered by PVST, an available technical solution can be selected. Criteria, such as the inclusion of the solenoid, the actuator, valve leakage internally and externally, travel time requirements and so on, will result in the selection of one of those techniques. Measurement based on air pressure, valve stem position, temperature, will determine whether this technique is adequate.
It must subsequently be noted that no single currently available PVST product is to be considered as being the best choice for any process related practical situation. For each practical problem where PVST is considered to add value the best technique will need to be investigated.

9 The central role of the PLC

Despite the fact that many of the currently available techniques are offered as being fully stand-alone products, practical implementation examples of these products, show that an important role is attributed to the safety PLC. This safety PLC often fulfils the so-called logic solver function as being part of the complete SIF where also the valve is part of as being the actuator.
Obviously, PVST solutions that are characterized by the application of limit switches and the operation of dedicated PVST test-solenoids, the safety PLC forms the intelligent 'hart'. In addition to this, other available 'stand alone' PVST products often make use of the safety PLC for actions such as alarm Management, Periodic PVST initiation, MTTR timer control, safe process shut-down or trip actions, and SOE registration.

Strikingly, it is observed that the safety PLC, which is mostly already in place for process safeguarding purposes, can often be used in an expanded way and combine its primary functions with the tasks to perform or support PVST. A key advantage of using the safety PLC for PVST is that it is already designed according SIS-related standard like IEC 61508. Some Safety PLC systems suppliers have already included PVST as a standardized solution into their product portfolio.

Concerning a PVST project that was executed already in the mid 90's by the company the author is employee of, the customer had a clear desire concerning the Mean Time To Repair (MTTR) timer control requirements. '*As far as MTTR timing is concerned, the first question is whether it is needed and this depends upon the SIL, the degree of fault tolerance and the improvement in SFF being claimed as a result of the PVST. In some cases it was needed, in others it was not. The next difficult question is what do you do when the MTTR timer elapses? For an input, you trip the input on which the fault has occurred and the MTTR timer has elapsed. There is not a lot of point in doing this for an output which is know to have failed since it won't work anyway. In this case you have to trip other process parts which will remove the hazard by other means such that failure of the valve will not cause a hazard. This can be very difficult to achieve.*' Obviously, such a difficult task needs to be analyzed up front and the required automatic protective action needs to be performed by the safety-related PLC.

Using the safety-related PLC for PVST also significantly increases the amount of information obtained from valve testing. With the increase in equipment status data gathered by safety-related PLC it is possible to compare the performance and condition of each safety valve against the performance of the valve when it was new or newly maintained. This also significantly increases the diagnostic coverage of the safety valve test while, at the same time, the information as handled by the PLC can be used for predicting the maintenance needs of particular valves.

Despite the fact dedicated PVST supporting field equipment is currently available in the market place, it is concluded that the safety-related PLC plays a central and significant role when it comes to the implementation of PVST and gaining its full benefits. This is based on the following aspects:

- Control of the MTTR timer requirements
- Compliance with safety standards like IEC 61508 and IEC 61511
- Periodic initiation of PVST actions
- Data logging, reporting and management
- Universal ability of work with any PVST supporting field device
- Huge installed base which can be expanded for PVST application
- Controlled initiation of required alternative trip actions

10 Conclusion

The benefits PVST is that it might meet governmental-, insurance- and safety standards safety requirements for critical ESD valve loops. Furthermore PVST will reduce the full stroke test interval (process downtime) for given safety level. It enlarges acceptable off-line proof test interval resulting in;

— Less cost of out-of-service of the valve
— Less cost of testing
— Less probability of human errors due to manual testing
— Compliance with a higher SIL, thus no doubled cost due to no longer need for duplicated valves
— Reporting compliant with safety standards IEC 61508 and IEC 61511
— Less probability of people being victim of a hazardous event, if their presence in the hazardous area due to test activities is reduced.

As stated by the ARC Advisory Group back in September 2001 [ARC01]:

> 'Not only is the manual work associated with conventional testing methods expensive, but also unreliable. There are a number of deficiencies in conventional testing methods, which raise the uncertainty over whether safety valves will actually be available in case of an emergency. Concern over the reliability of conventional safety valve testing procedures is due to a number of reasons including the lack of real-time data and the absence of trending data. Another significant drawback to conventional testing methods is that they render the valve unavailable during testing if a real safety issue is encountered. Conventional valve testing procedures also put the burden on BP technicians to manually return safety valves to their proper operating mode after completing the tests. If an emergency were to occur during the testing procedure, or if a safety valve were to be left with its range of motion restricted, the valve would be unavailable to prevent a fire or explosion during a process upset. As a result of these risks, and its highly labor-intensive nature, BP feels it must improve its safety valve testing procedures.'

It is concluded that PVST adds a significant contribution to the valve reliability. Higher SIL's can be achieved, less maintenance costs are made, and less manual tests are required.
The safety PLC appears to fulfill a significant role when is comes to the implementation of many PVST solutions which are currently available in the market place. The massive installed base of safety PLC

offer an excellent platform for PVST expansion. Compliance with safety-related standards is subsequently easily achieved.

11 References

[IEC61508] IEC 61508 – Functional safety of electrical/electronic/programmable electronic safety-related systems 1998/2000

[IEC61511] IEC 61511 – Functional safety: Safety-instrumented Systems for the process industry sector (Draft version 1999)

[ISA96] ANSI/ISA S84.01 – 67 Alexander Drive, P.O. Box 12277, Research Triangle Park, NC 27709 1996

[ISA98] ISA TR84.00.02 Part 4 – 67 Alexander Drive, P.O. Box 12277, Research Triangle Park, NC 27709 1998

[ARC01] ARC Advisory Group– Neles ValvGuard Allows BP to Increase Safety While Reducing Costs

ARC White Paper September 2001