The purpose of this article is to help on your decision making process when presented with the option of implementing ESD/PSD Valve Partial Stroke Testing. There are several methods of partial stroke testing divided in three general areas: mechanical limiters, solenoid valve arrangements, and position control using logic solvers and/or smart positioners.

The most useful type of partial stroke test to use would be the smart positioners and/or logic solver controller doing the automatic partial stroke test of the valve. It should also be mentioned that the logic solver and/or positioner also form part of the safety instrumented loop and therefore must comply with the performance requirements, or Safety Integrity Level, SIL, requirements.

If the requirements for the Safety Instrumented Function, SIF, call for a SIL 1 level, then Partial stroke test will be useful in extending the proof test interval. If the requirements call for a SIL 2, then partial stroke test will be useful for finding an alternative for the minimum hardware fault tolerance of final element requirements, (according to IEC 61511-1), and/or extending the proof test interval.

Before getting into details about partial stroke testing, is good to review some basic concepts from TÜV, the IEC 61511 and IEC 61508 international standards.

Diagnostic coverage (DC) is defined as the ratio of the detected failure rate to the total failure rate of the component or subsystem as detected by diagnostic tests. Diagnostic coverage does not include any faults detected by proof tests. [IEC61511-1]

\[ DC = \sum \frac{\lambda_{dd}}{\lambda_d} \]

\[ DC = \frac{\lambda_{dd}}{\lambda_{dd} + \lambda_{du}} \]

\[ DC = 1 - \frac{\lambda_{du}}{\lambda_{dd} + \lambda_{du}} \]

\[ C_d = \text{Diagnostic Coverage factor of dangerous failures} \]

\[ \lambda_{dd} = \lambda_d \times C_d \]

\[ \lambda_{du} = \lambda_d \times (1 - C_d) \]

\[ \lambda_d = \text{Total dangerous failure rate} \]

\[ \lambda_{dd} = \text{Dangerous Detected Failure Rate} \]

\[ \lambda_{du} = \text{Dangerous Undetected Failure Rate} \]

The safe failure fraction (SFF) is the fraction of the overall random hardware failure rate of a device that results in either a safe failure or a detected dangerous failure.
The sum is taken over all relevant items, and:

- \( \lambda_s \) is the rate of safe failures
- \( \lambda_d \) is the rate of dangerous failures
- \( \lambda_{dd} \) is the rate of dangerous failures that are detected by the internal diagnostic testing

The SFF may alternatively be defined as the conditional probability that a failure is either a safe failure or a detected dangerous failure (when we know that a failure has occurred).

\[
SFF = 1 - \frac{\lambda_{du}}{\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}}
\]

Only failures detected by diagnostic tests can be accounted for in the safe failure fraction calculation. Failures detected by periodic proof tests cannot be accounted for in the safe failure fraction calculations. The greater the level of diagnostics the less redundancy is required.

The proof test is defined in IEC 61508 as:

“Periodic test performed to detect failures in a safety-related system so that, if necessary, the system can be restored to an “as new” condition or as close as practical to this condition”

IEC 61511 has a similar definition:

“Test performed to reveal undetected faults in a safety instrumented system so that, if necessary, the system can be restored to its designed functionality”.

Note 3 of paragraph 7.4.3.2.2 of IEC 61508-2 explains that a test is a diagnostic test if the test interval is at least a magnitude less than the expected demand rate.

According to TÜV, a test is a diagnostic test if:

1. It is carried out automatically (without human interaction) and frequently (related to the process safety time considering the hardware fault tolerance) by the system software and/or hardware;
2. The test is used to find failures that can prevent the safety function from being available, and
3. The system automatically acts upon the results of the test.

Once a failure is found a decision needs to be made on what to do with that failure. (i.e. shutdown or switch to partial failure mode if the safety system has sufficient redundancy).
Conclusion is that a test to detect failures is called a “diagnostic test” if the test is carried out automatically and more often than a magnitude less than the expected demand rate. In all other cases we can refer to a test as a proof test.

Also, only failures detected by diagnostic tests can be accounted for in the safe failure fraction calculation. Failures detected by periodic proof tests cannot be accounted for in the safe failure fraction calculations.

In this article, I will interpret partial Stroke testing as a diagnostic test, in low demand mode, and not as part of a manual proof test. After clarifying the previous concepts, I can continue with more details.

Due to the lack of internal diagnostics available in valves they represent the weakest link in the instrumented loop. If somehow using an external device, like a smart valve positioner, we could detect some failures, then the probabilities that the valve fails on demand are reduced.

However, from all the valve dangerous failures; what percentage would be taken as dangerous failures detected by the partial stroke test? (While the valve is in service, that is: on-line partial stroke testing).

You can get some answers from valve manufacturers that can give you a percentage value according to their tests. Nevertheless, the best way to gain confidence on how much percentage you can take credit for the diagnostic tests performed on the ESD/PSD valve, may be by understanding how the percentage is obtained.

The following table, based on published data, gives you a reference point on how to identify the failure type and if the failure can be detected using external means to the valve. (i.e. a smart positioner or logic solver). Table taken from reference [1]
Some manufacturers of ESD/PSD valves assemble together the smart positioner and valve, and include the software with the automatic partial stroke testing. Some manufacturers also take credit for the material deterioration of the valves as long as you follow their safety manual and maintenance procedures. In this reference example I took as much credit as 78.82%. \(\left(\frac{70.72}{89.72}\right) \times 100\)

From the total dangerous failure rate of the ESD/PSD valve obtained from your best reliable sources, (most probably from your own facility), you can now subtracts 78.82% from the previous total dangerous valve failure rate.

This means that by recalculating the PFD\(_{avg}\) with the newer and lower dangerous valve failure rate, you will obtain a better performance, or a lower probability of failure on demand of the valve, (Some times as much as achieving SIL 2 level). Also, by analyzing the Safety Failure Fraction, you can see that by having more than 60% dangerous failures detected, the need for valve redundancy, (hardware fault tolerant), is not required for a Safety Integrity level SIL 2. (In accordance to the requirements of IEC 61508-2, Tables 2 and 3).

Nevertheless, if the requirement was SIL 1, you can increase the Proof Test interval and still have Safety Integrity Level SIL 1.
Another factor influencing the PFD\textsubscript{avg} is the Mean Time to Restore, which brings into consideration the reaction time to the failure being detected by the positioner and/or logic solver.

How the positioner is connected to the logic solver is now safety related and must be taken into consideration, whether is a digital bus, (i.e. HART), or other. Remember, the system must automatically act, upon the results of the test, once a failure is found and a decision needs to be made by the system on what to do with that detected dangerous failure. (i.e. shutdown or switch to partial failure mode if the safety system has sufficient redundancy).

Also, other very important factor influencing partial stroke test performance is how often the partial stroke test has to be done. This can be realized from the concept of Diagnostic Coverage as stated above. The more often you perform the test the better. However, every time the test is done the process is disturbed with oscillations, and there may be buildup at the percentage partial movement. Another important fact to consider would be the demand rate of the safety instrumented function with respect to the partial test rate. If the partial test exceeds the demand rate by 100 times, then it may be advisable to consider the safety function to be in continuous mode and not in low demand mode.

The best option, when requiring implementation of partial stroke test of an ESD/PSD valve in a critical process, is to use valve positioners and/or logic solvers with certified software for automatically carrying out on-line diagnostic tests on the emergency shutdown valves.

There are many other additional benefits of using the new smart positioners or safety logic solvers such as giving you the actual real time status of the valve and its response to movement. This is achieved by capturing the valve signature when it was commissioned and later compared with the signature taken at the moment the partial tests are performed. By comparing both signatures it can be predicted if and how fast the valve is degrading or if the valve has a specific problem. Also, the response to a demand of the ESD/PSD valve will not be compromised by the test itself. If the valve needs to be closed the test, which is at a lower execution priority than the response to a demand, will stop and the valve will be activated to the safe position.
References


[4] IEC 61508-2 and IEC 61511-1 Standards

Guillermo Pacanins, P.Eng., TÜV FS Eng.