

Comparison between testing methodologies to achieve the required SIL level

Ulrich Gensicke
Metso Automation GmbH

The IEC 61508/61511 (Equiv. ISA - S.91 (TR.84)) safety standards are creating more stringent testing requirements for safety equipment.

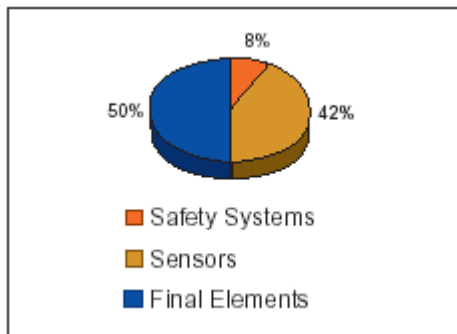
It is clear from existing data (OREDA – Offshore Reliability Data book) that the largest proportion of undetected failures are due to the Final Element. Sensor technology has already integrated ‘smart’ principles for some time. Common failure modes such as plugged lines can be detected by noise signal analysis. The safety system itself has developed to a level where it has both redundancy and a high level of diagnostic coverage. Therefore, that leaves us with the ‘Final Element’. Some typical applications to consider are: Safety shut down systems, Double Block Valves, Bleed Valves, Emergency Blow Down Valves, Gas Exhaust Valves, Burner Management System Valves, Fire Water Service, Steam Venting Valves, Excess Heat Relief Valves, Dump Valves.

Final elements fail due to:

- wrong specifications, selection or sizing
- valves stick due to e.g. crystallisation
- soft materials “cold flow “
- valves/solenoid corrosion
- actuators corrode
- foreign objects inside
- pneumatic leaks



In order to meet your applications defined SIL requirement, you must ensure you achieve the required Probability of Failure on Demand (PFD).



Before we look at any evaluation involving the Probability of Failure on Demand, it is important to clarify, all further discussion will be concerning the final element. However, it is also clear that this is often the weakest link, to quote a senior advisor to BP:

“...The fail to trip probability for a ESD system is dominated by the proof test interval for the ESD valves.”

With these various failure modes affecting the final element you might look at several options: Redundancy, Valve selection and diagnostics (which can either be offline – full stroke or complete strip down, or **online testing**). We will investigate the options open to the safety engineer:

Plant Shutdown

$$PFD_{SYS} = PFD_S + PFD_L + PFD_{FE}$$

There are increasing pressures to run most continuous process plants for longer between shutdowns. This goes against the SIL requirements. It can be seen from the equation opposite that the result is a PFD1001 (Probability of Failure on Demand for a 1 out of 1 system) that is simply a multiple of a Mean Time To Failures (1/MTTF) component and the period between shutdowns (TIm). This means for a MTBF_d of 50 years and a shutdown period of 2 years, will give a PFD of 0.02, which is only SIL 1! Or to look at it another way the Plant would have to shut every 52 weeks, for even the PFD of the final element to be within SIL 2 (with all the loop elements included it would more likely need to be around 20 weeks).

Final element Redundancy

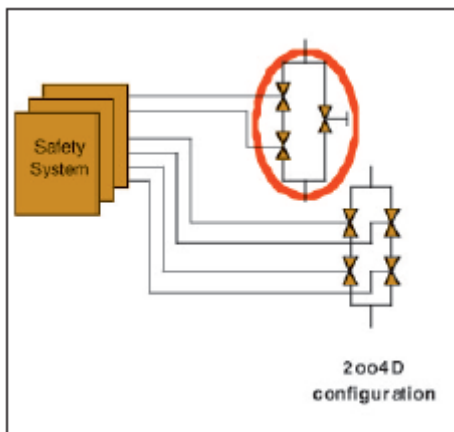
It is possible to meet the requirements utilising greater system redundancy. This has a significant cost impact, therefore leaves most sites looking at the other alternatives. One other issue to consider is common mode failure effects. Two valves in the same line, if one valve fails due to corrosion there is a high probability that given the same body materials and process conditions, the other is likely to fail also.

By-Pass

Although a full stroke may be performed the Diagnostic Coverage is questionable. A valve can be stroked through its full travel, but this test is not run under process pressure. When it is back in service process pressure can cause the valve not to shut off. If the test is to automated, some form of feedback is needed (visual, electrical). The cost of implementing a bypass solution

relatively high, with additional piping, valve and manpower requirements for periodic testing. Depending configuration, the system is unavailable whilst the being carried out, which can have a safety implication. When using manual by-pass valves the possibility human error is also introduced, before, during and completion of testing. In summary the issues are:A

- OPEX and CAPEX Cost
- Feedback needed (visual, electrical)
- Multiple valves
- Piping and space
- Maintenance is required



Partial Stroke Testing

The critical equation for all Partial stroke testing is shown here, this may appear in different forms but contains the same elements. Partial Stroke testing can be an essential element in meeting your safety requirements, but not all tests are equal, some offer a significantly higher Diagnostic Coverage than others do. The other critical factor is the Mean Time To Failure of the Final element ($\lambda_d = 1/MTTF$)

$$PF_{1001} = DC \cdot \lambda_d \cdot \left(MTTR + \frac{TI_d}{2} \right) + (1 - DC) \cdot \lambda_d \cdot \left(\frac{TI_m}{2} \right)$$

← Online testing
Offline testing →

- λ_d = dangerous failure rate = $1/MTTF_d$
- $MTTF_d$ = mean time to fail
- DC = diagnostic coverage factor dangerous
- TI = test interval (a = on-line, m = off-line)
- MTTR = Mean time to repair (how long to fix)

Mechanical Jammer and Test Cabinets

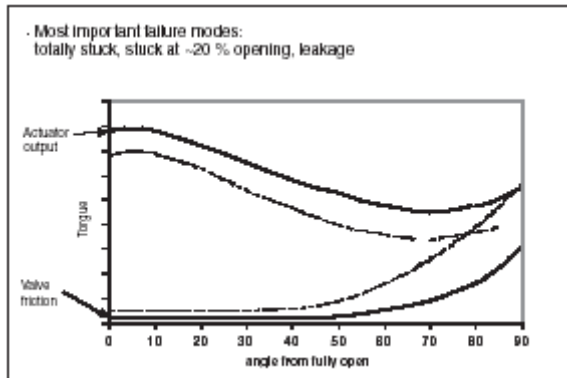
The Mechanical Jammer method has been utilised for a number of years now and is recognised as being a valuable testing method to give an amount of diagnostic coverage.

There is a fundamental problem with these forms of partial stroke test. They do not include any further analysis. You can see why this is so important in the graph of torque against valve angle of opening.

One common failure mode is stuck at 20 % opening (70° angle from fully open). As either valve friction increases, or actuator torque decreases (worn seal rings) there is an increasing

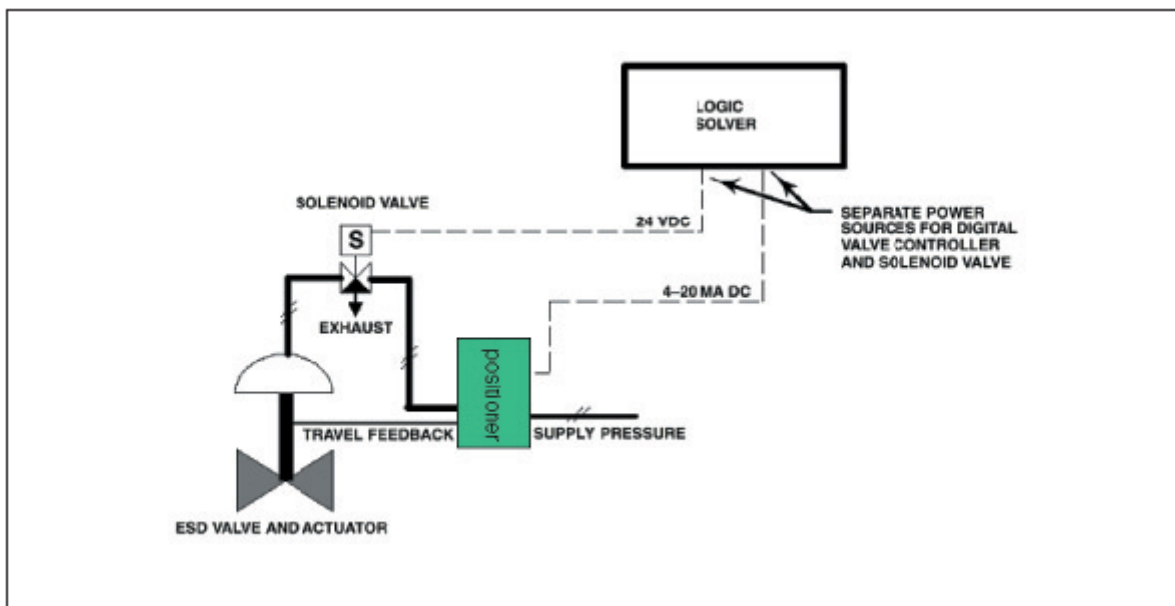
probability that there will not be enough force to shut-off the valve. Even if the valve does travel through 90°, there is not necessarily enough force to shut-off against process conditions. By this basic test method these remain undiagnosed and therefore greatly lessen the diagnostic coverage. This is a major weakness of both the Mechanical Jammer and Test Cabinet.

A further consideration of the test cabinet is both initial cost and for both methods the operational cost and element of human error.



Smart Positioner and separate Solenoid valve

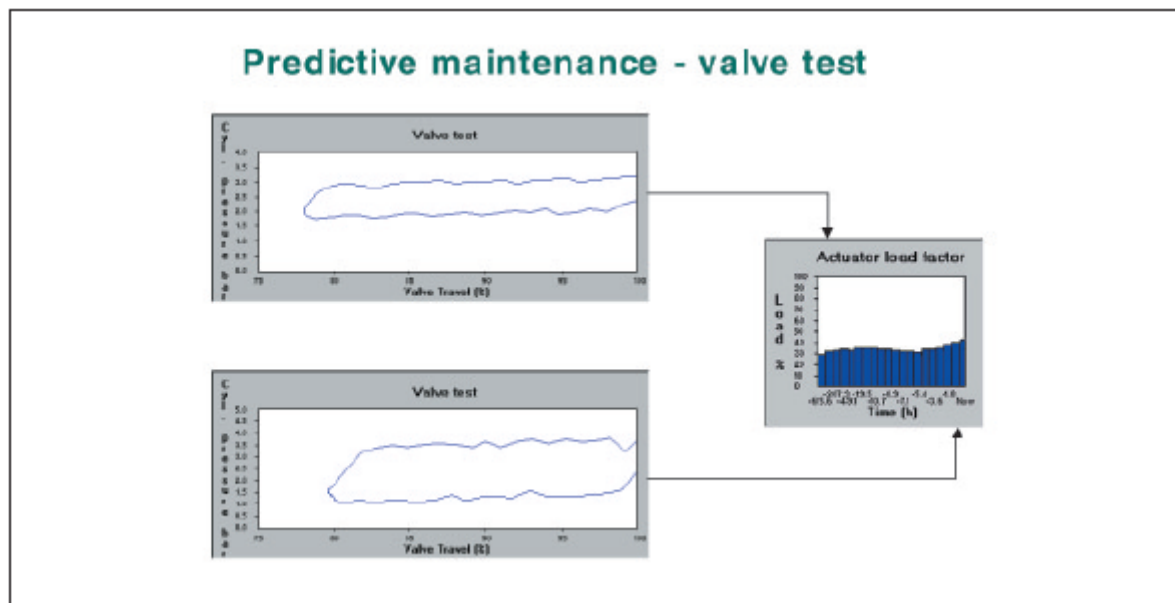
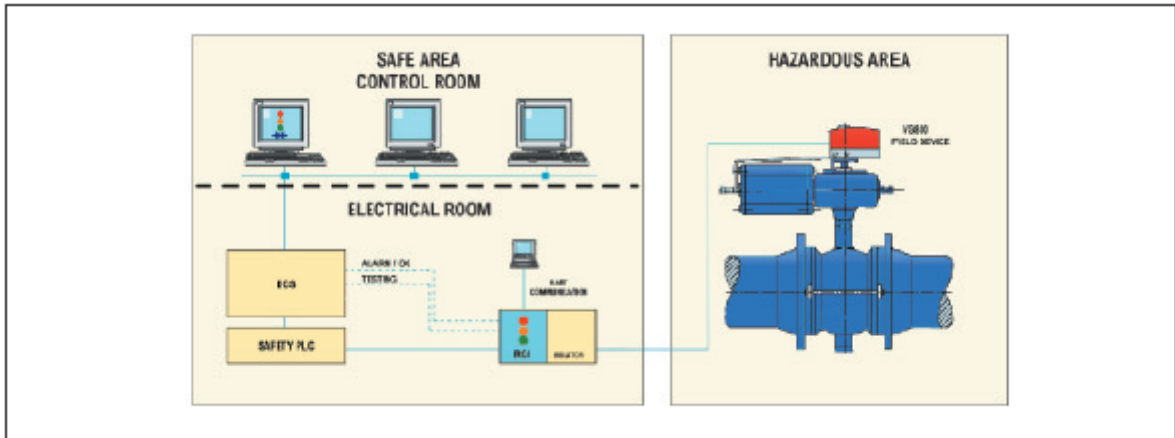
There are now a wide number of smart positioners, some of these have the possibility to perform and analyse a partial stroke test, through which some frictional analysis can be made. This is a good step forward, however there are problems with this method. The primary issue is the lack of direct regular testing of the solenoid, a jammed solenoid is a recognised failure mode and this greatly reduces the possible diagnostic coverage (DC) factor. The other issue is currently these tests are not automated and require some further analysis, judgements can be erroneous or just an overlooked part of the procedure.



Valve Guarding Concept

There is another alternative that seems to address many of the aforementioned concerns. A valve guarding system is made up of an intelligent field device and interface connected to the plant control system. The field device is essentially a solenoid valve with smart diagnostic capabilities. Two wires from the control room provide both 24-volt power and a communication path. An electronic module provides simple relay feedback of the condition of the Final Element:

Green: Good
 Yellow: Deterioration
 Red: Alert



The essential elements are:

1. The possibility to **automate all tests**.
2. **On-line Diagnostic analysis**, with simple traffic light feedback system.
3. **Remote valve test**. Partially exercises the valve as much as the process will allow (e.g., 20), with Load Factor analysis under process conditions this clearly indicates reduction in force to shut off the valve and therefore a high degree of diagnostic coverage.

4. Pneumatic test. Since the solenoid is an integral part of the assembly it can be fully tested at regular intervals. The pneumatic test assesses the availability of the emergency system (including the pneumatics of the smart field device, piping, electrical circuits and connections) without actually moving the valve.

Malfunctions and alerts are transmitted in real time to the operators, thereby eliminating “unreported failure” risks. To be able to upgrade existing systems with minimum cost, the Neles ValvGuard system can be easily retrofitted to existing valves or incorporated in new installations.

The Impact

Independent assessment has shown the system to have a diagnostic coverage of between 75-95 % depending on the valve assembly. This level of diagnostic coverage, linked with automated regular testing, gives the opportunity to significantly reduce the PFD of the final element. This can be seen in the worked example.

Field experience has shown the value of the Neles ValvGuard system:

- Partial, on-line stroke testing of safety valves took place at frequent intervals ranging from hourly to once a day. This was far more testing than would have been practical with previous testing methods.
- The simple traffic light system was easy to use and required no interpretation (Trends are automatically analyzed after each partial stroke test).
- Users at one plant noted that the system was 100 % effective in quickly identifying valves that froze during harsh winter conditions.

	On-line diagnostics* (= testing)	Off-line diagnostics* (= periodic maintenance)
$PFD_{1001} =$	$\lambda_{dd} \cdot \left(MTTR + \frac{TI_a}{2} \right)$	$+ \lambda_{du} \cdot \left(\frac{TI_m}{2} \right)$
$PFD_{1001} =$	$0.8 \cdot \left(\frac{1}{115 \cdot 365 \cdot 24} \right) \cdot \left(8 + \frac{2 \cdot 24}{2} \right)$	$+ 0.2 \cdot \left(\frac{1}{115 \cdot 365 \cdot 24} \right) \cdot \left(\frac{365 \cdot 2}{2} \right)$

$PFD_{1001} = 9.5 \times 10^{-4}$ SIL4

Where λ_{dd} = dangerous detected failure rate = DC · λ_d
 λ_{du} = dangerous undetected failure rate = (1 · DC) · λ_d
 λ_d = failure rate = 1/MTTF_d
 MTTF_d = mean time to fail
 DC = diagnostic coverage factor
 TI = test interval (a = on-line, m = off-line)
 MTTR = Mean time to repair (how long to fix)

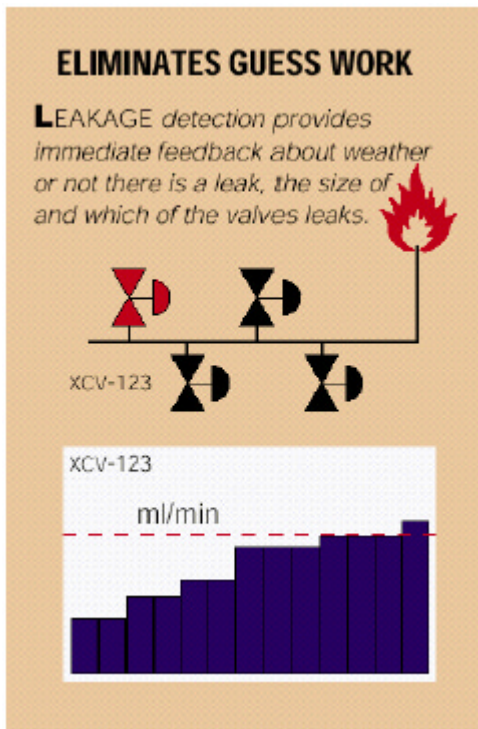
Neles ValvGuard™ Identifies ESD Valve Leakages

For many years, acoustic leakage detection technology (pioneered by Physical Acoustics Group, Cambridge, UK) has been widely used in refineries, chemical processing plants and offshore oil rigs for estimating through-valve gas leakage. These portable systems have proven themselves to be extremely accurate and reliable.

Leakage creates an acoustic emission that travels through nearby solid materials as a sound wave. Remote sensors situated on a containing structure readily detect this acoustic wave

energy. This data can be accurately analyzed by software to reveal levels of leakages much better than ANSI Class V.

The Neles ValvGuard™ System with leak detection capabilities can continuously monitor the permanent remote sensors for acoustic energy. The results are improved safety, more accurate maintenance planning and minimized production losses.



Conclusions

The potential of a non-operating field device is still a big problem in most safety systems. Many specialized dual and triplicate logic solvers are independently certified for use in SIL 3 applications. Unfortunately, this is not enough because the final elements, often valves, account for 50 % of the target reliability of the safety loop.

The only way to ensure the valve's availability is to activate the system. But, closing the valves completely and stopping production, in most cases, is not a feasible solution. That is why on-line, partial stroke testing, with additional diagnostics, is increasingly more important. All the methods of partial stroke testing offer measured improvements over full stroke testing in isolation. Automating the partial stroke testing routine using intelligent emergency valve technology will help increase safety with more frequent testing and optimize maintenance of the final elements with the additional data received. At the same time, automated testing will decrease the costs and risks associated with manual on-line testing.

A valve guarding system, which fulfils SIL 3 safety level requirements, allows users to continuously monitor valve condition improving the likelihood that the emergency valves will be available on demand. This allows plants to avoid using dual systems in SIL2 applications or triplicate systems SIL 3 applications. Remote, automatic, online testing also eliminates the

manpower costs previously required for manual emergency valve testing. The most important feature is that for the first time good quality feedback from the final control element is available to operators and maintenance personnel, to truly minimise the probability of failure on demand.

The information provided in this bulletin is advisory in nature, and is intended as a guideline only.