Will a Partial Valve Stroke Testing lead to a higher SIL?

Hassan EL-Sayed

BSc (Hons) MSc PhD CEng FInstMC
CSA Group, Unit 6 Hawarden Industrial Park
Hawarden, CH5 3US, United Kingdom

Email: hassan.el-sayed@csagroup.org

Abstract:

Diagnostics may form part of smart devices and final elements as an enhancement for the safety integrity levels, and to offer improvement in maintenance programs to ensure continual operation and detecting of hiding faults. Diagnostics are widely used to identify critical conditions, parts not performing reliably, hidden faults where demands for safety functions may not be fulfilled.

Partial valve stroke testing (PVST) of the final element is used to ensure safety function availability without interrupting operation and extend the recommended full proof test interval. This improves the probability of failure on demand (PFD) while the safe failure fraction (SFF) remains unchanged. As seen in some of the current certified products to IEC 61508, SFF is improved because the PVST is considered as a diagnostic tool since it is used in the derivation of the failure mode and effect analysis (FMEA). This conflicts with the practice of the IEC 61508 which eventually affects the final calculation of the intended safety loop. This PVST function is designed to be integrated internally or implemented externally to the final element as far as it adheres to the main assessment rules.

Before, and even after the release of issue 2 of the IEC 61508:2010, many final elements were certified and achieved safety integrity level (SIL 3) based either on route 2_H or route 1_H. These claims were based on having PVST as a tool for diagnostic of dangerous undetected components without examining the rest of the overall safety related structure and whether it meets the general requirements of the safety integrity level (SIL) as specified in IEC 61508-2, clause 7.4.4.1.

The paper reviews a few examples of already certified products in the market using PVST capability, and shows the impact of PVST in the FMEA analysis for which a higher SIL capability is being claimed. The paper will discuss a newly certified final element based on the analysis published in the IET conference in 2013 (ref1). It shows that when a PVST tool is used as an internal part of the element, the final element becomes a type B as stated in IEC 61508-2, clause 7.4.4.1.3, and the improvement made is noticeable to the PFD values while SFF remains unchanged. In this example, PVST algorithm has been assessed to IEC 61508 part 3 and received full certification.

This paper looks at the past, the current practice of using PVST and highlights the issues that lead to misunderstanding the main purpose of PVST. It will provide guidance for proper use of the PVST which is based on an independent point of view with no vested interest, tangible or intangible, from the certification bodies.

Introduction

After the release of issue 2 of the IEC 65108:2010, it is assumed that Annex A of ICE 61508 part 2 becomes very clear and expected to provide suitable guidance when using diagnostic features in the E/E/PE safety element. Unfortunately, several final elements are certified to SIL 3 capability based on hardware fault tolerance (HFT:0) by using Annex A of part 2 of IEC 61508 in their FMEA calculation. This is based on considering PVST as a diagnostic tool for dangerous undetected without further consideration to the additional requirement when diagnostic is used and at the same time, ignoring the type of elements when complex diagnostic is used irrespective if it is internal or external to the elements. The calculation found in some of the certified elements showed that when PVST is used, as diagnostic tool, the reliability figures demonstrated that the safe failure fracture is boosted up to a higher figures which is completely wrong.

This approach leads to wrong assessment of the overall safety integrity level and the probability of failures of the whole safety loop. The safety instrument system calculation did not consider the impact of the element type when diagnostic used that is type B or type A. This demonstrated luck of understanding to Annex A part 2 and misuse of its intended purposes. At the same time the standard was not clear in specifying this type of partial testing.

It is supposed that the changes made in IEC 61508:2010 (edition 2) which may affect the assessment of the final element with diagnostic becomes simplified. It turns out that little or perhaps not a great deal of understanding is considered. The current implication of these changes on product certification is examined and demonstrated with a proof analysis for a certified product with and without PVST. At the same time the author extracted some data from the current certified products for clarity to illustrate the problem in the current practice.

Partial Valve Stroke Testing (PVST)

Lots of valves and actuators manufacturers offer PVST as one of the features in their products portfolio. PVST is a useful feature in the final element it has been implemented in some of the safety instrumented system, mainly because these final elements are considered as slave devices. Hence the use of PVST has made a significant contribution to the improvement of the product availability in the safety instrumented system (SIS) and considered as a measure of enhancing the probability of demands i.e improving the product availability, in particular where a demand of a safety function such as an emergency shutdown (ESD) is required.

The technique used so far is well known, however, a few questions must be put forward, such as:

- What is maximum (practical) undetected dangerous failures λ_{DU} percentage can be claimed?
- Is partial testing a diagnostic tool or part of the full proof interval test (PTI)?
- Can PVST be implemented internally or externally to the final element, and what is the impact on the final element? Will it be type A or B as defined in IEC 61508-2, clause 7.4.4.1, [1]
- What is the impact on the SFF if PVST considered as a diagnostic tool?
- How are the measures used in IE 61508 (ed.2) for diagnostic technique?
- What is the proper mathematical equation recommended for PVST use for the improvement of the probability of failure on demand?
- What is the final element safety integrity level (SIL) with and without PVST? The list goes on and on?

The objective of this paper is not to discuss the techniques of the PVST implementation. It is rather to explain the above stated issues since the author has identified misunderstanding in the implementation of PVST and its intended use in a number of certified products which led to create confusion in the market. Some safety designers only follow product certificates and ignore the details, such as which standard and its edition the products were certified to without questioning, because the end user specification dictates to have the final elements with SIL 3 (HFT:0) without looking deeply into the hardware architecture constraints and the systematic capability assessment. Hence manufactures will search for a certification agency to certify the product to match the client demands and win the bid. End users should seek proper full assessment reports and if they are in doubt about the product certificates, they should contact independent association or institution for clarity and guidance.

Diagnostic as defined in IEC 61508

The market is swamped with products claiming SIL 3 with hardware fault tolerance equals to zero (no hardware redundancy, HFT=0, and without even a proper assessment to the product systematic integrity). Experienced safety process engineers may be able to recognise and judge these types of certifications which do not provide solid proof of certifications and no more the insurance companies are able to accept certified products if proof of systematic and full analysis reports was not provided.

This hypothesis in claiming a SIL 3 capability with (HFT:0) which produces low dangerous failures will of course lead to vulnerable SIFs because of less of redundancy and proof testing is probably not required anymore if PVST is doing the job.

Diagnostic as defined in IEC 61508 part 2 (ed.2), clause 7.4.9.4-J [2] that the failure rate of the diagnostics, due to random hardware failures, must be considered in the realisation of the SFF or diagnostic coverage. Edition 2 considers this part (diagnostics) contributes in the detection of the dangerous components and making considerable improvement in the diagnostic coverage and claiming higher SIL. As this diagnostic part plays an important role in detecting a percentage of the dangerous components, and subsequently yield a better SFF, this diagnostic section which is part of the subsystem is subject to fail. Therefore edition 2 considers the failure rate of the diagnostic is a part of the overall failure rate because it plays a part in implementing the diagnostic coverage and architecture constraints.

According to Edition 2 [2], diagnostics can be internal or external as defined in clause (part 2, 7.4.9.4), that a safety function can fail as a result of random hardware failures which are detected by the internal diagnostics tests or detectable by diagnostics externally to the element.

Also, diagnostic is identified as credit, as defined in “NOTE 2: that the diagnostic coverage and diagnostic test interval are required to allow credit to be claimed for the action of the diagnostic tests performed in the element in the hardware safety integrity model of the E/E/PE safety related system part 2 (clauses 7.4.5.2, 7.4.5.3 and 7.4.5.4) [2].

In particular as a means of using external diagnostics for the detection of failure modes of a specific function, sufficient information shall be provided to facilitate the development of an external diagnostics capability. The information shall include details of failure modes and their failure rates, (part 2, Annex D) [2].

From the above aforesaid, diagnostics as described in Edition 2 can be internal or external to the subsystem. In either case, random hardware failure assessment of the diagnostic section is required and shall be taken into consideration during the calculation of the overall probability of demands of the SIS. Having said that, then the elements shall be re-assessed if this this type of diagnostics makes the product type B.

If PVST is considered as diagnostic on line function, then a credit shall only be taken for the diagnostic if the sum of the diagnostic test interval and the time to perform the repair of a detected failure is less than the mean time to restoration (MTTR) used in the calculation to determine the achieved safety integrity for that safety function. MTTR consists of the time to detect the failure (diagnostic time) plus the mean repair time which consists of the time spent before starting the repair, the effective time to repair and the time before the component is put back into operation, (IEC 61508-4) [7].

As per clause (7.4.5.4), the diagnostic test interval of any subsystem (operating in low demand mode, shall be such that the sum of 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 maximum approximate active time quoted to complete one PVST test is no more than 2 minutes [8], and since PVST is typically used at a relatively low rate for example between (weeks to months) for the next interval test time. Based on the above definition, if PVST is claimed as diagnostic interval test, and if it can be achieved within the time window to repair, which is between 8 to 72 hours, not as claimed that PVST can be performed within a few weeks to months then the implication would be that MTTR would be immensely high value [9].

However, as stated in [9], If (PVST) is considered as partial proof test, it does not enhance the SFF; it is a tool which can be considered to improve the Probability of Failure on Demand (PFD).

The next section will consider the implication of using PVST as a means of a partial proof test not as a diagnostic test for a safety element.

Classification of partial valve stroke testing

PVST is one of the features that most of the valve manufactures claim in their products specification. It is a method for satisfying the need to return the subsystem close to “as good as new” while a full test interval (full proof stroke test) is performed to evaluate the full subsystem parameters and performance.

PVST is widely described in many articles and vendors data sheets [4, 5 and 6] to the extent that a valve with PST can be deployed in SIL3, as PVST is interpreted as a kind of diagnostic test, therefore, eliminating the need for redundancy, reducing the probability of failure on demand (PFD) due to random hardware failure, and some claims are providing unsubstantial arguments for increase on the safe failure fraction to derive higher SIL i.e valves with PVST sold as a very cost effective alternative of using one valve instead of installing two valves on SIL 3 safety instrumented systems.

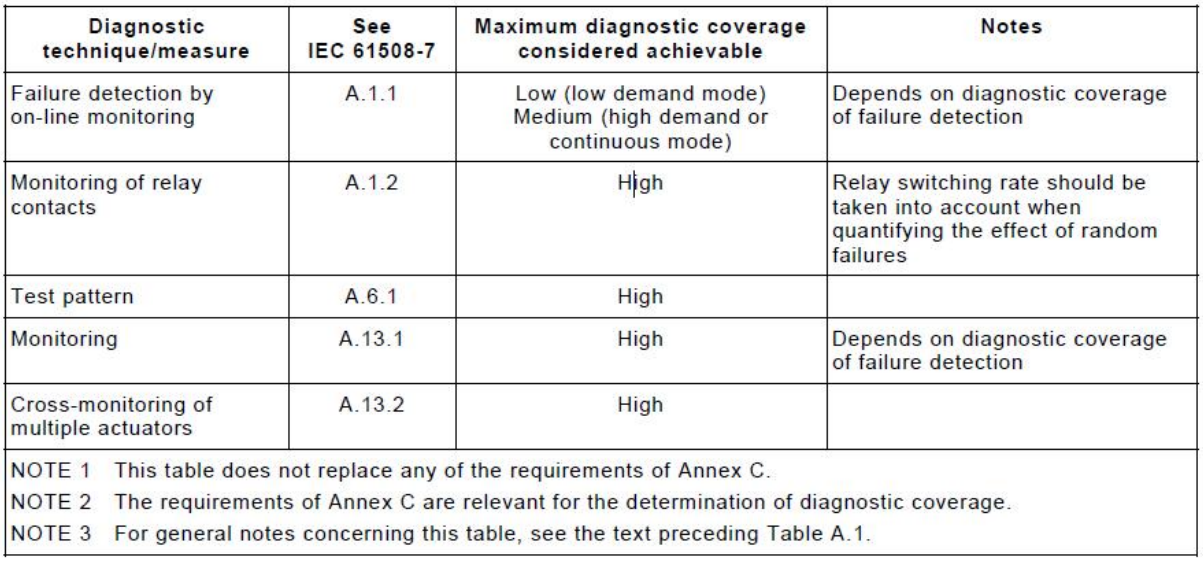
The claims are accepted by the market, since the arguments are as far as the valves are certified by recognised third party agencies (not sure if they are accredited!), hence no substantial questions need to be raised about the products assessment and the validity of these results.

Under edition 2, the definition of diagnostics and its applications become clear. One of the main reason behind this paper that the market is still under the influence and understanding that PVST is considered as diagnostics tool, i.e referred as (“DC: diagnostic coverage) and credit is granted for this type of tests, and not counted in wide scope as a complementary tool as a “proof test coverage” to a full stroke testing coverage.

The author will first look at some final elements certified products to edition 2, and then as part of the compliance, a separate example will be considered to illustrate the effects of diagnostic on the PFD calculation and its impact on the safe failure fraction and followed with an actual final element assessment being conducted recently using PVST in the final element where SFF is assessed under type B and improvement to PDF has been shown when PVST is implemented.

Implication of PVST on the reliability calculation

Looking first into Annex (A) of part 2 which provides guidance for claiming diagnostics coverage which is divided into 3 parts, low up to 60%, medium up 90% and high up to 99%. This Annex (A) is prepared when quantifying the effect of Random hardware failures and to be considered in the derivation of the safe failure fraction (SFF). Annex (A) consists of 17 tables of which table no. 14 is dedicated to the final elements (actuators), as seen below in Table 1.



Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Failure detection by on-line monitoring	A.1.1	Low (low demand mode) Medium (high demand or continuous mode)	Depends on diagnostic coverage of failure detection
Monitoring of relay contacts	A.1.2	High	Relay switching rate should be taken into account when quantifying the effect of random failures
Test pattern	A.6.1	High	
Monitoring	A.13.1	High	Depends on diagnostic coverage of failure detection
Cross-monitoring of multiple actuators	A.13.2	High	

NOTE 1 This table does not replace any of the requirements of Annex C.
NOTE 2 The requirements of Annex C are relevant for the determination of diagnostic coverage.
NOTE 3 For general notes concerning this table, see the text preceding Table A.1.

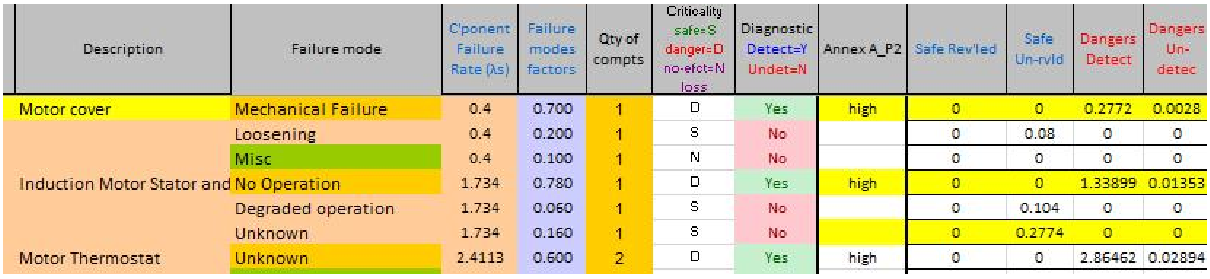
Table 1: Final element (actuators), quoted from IEC 61508 part 2, Annex A. Requirements for diagnostic coverage claimed: Low:60%, medium: 90% and high: 99%.

The table shows that maximum diagnostic coverage considered achievable for low demand safety function is low (up to 60%), medium (90%) for high demand for failure detection by on line monitoring. This type of monitoring is used for the detection of abnormal behaviour of the equipment under control (EUC). This type of online monitoring provides automated control monitoring for up-to-the-minute information to help optimizing the operation of the EUC. It is not intended for the functionality of the partial testing as the later requires specific software algorithms to implement the functions and measure the output signals. This type of testing only takes place when product is in halt or during maintenance. Therefore, PVST cannot be used in Annex A as a means of diagnostic. Even if the online monitoring used forms part of Profibus or Foundation fieldbus or alike, this will automatically dictates to have a type B product in the downstream (final element) to implement the communication process and perform the PVST function.

As can be seen in the example below (Table 2), that selection for dangerous detections are selected in the FMEA table without even considering the diagnostic coverage factor (DCF), claiming high (99%) coverage. The analysis carried on to the end of the FMEA table and eventually the summary produces higher SFF and lower PFD. This emphasis the misunderstanding of Annex A and its use.

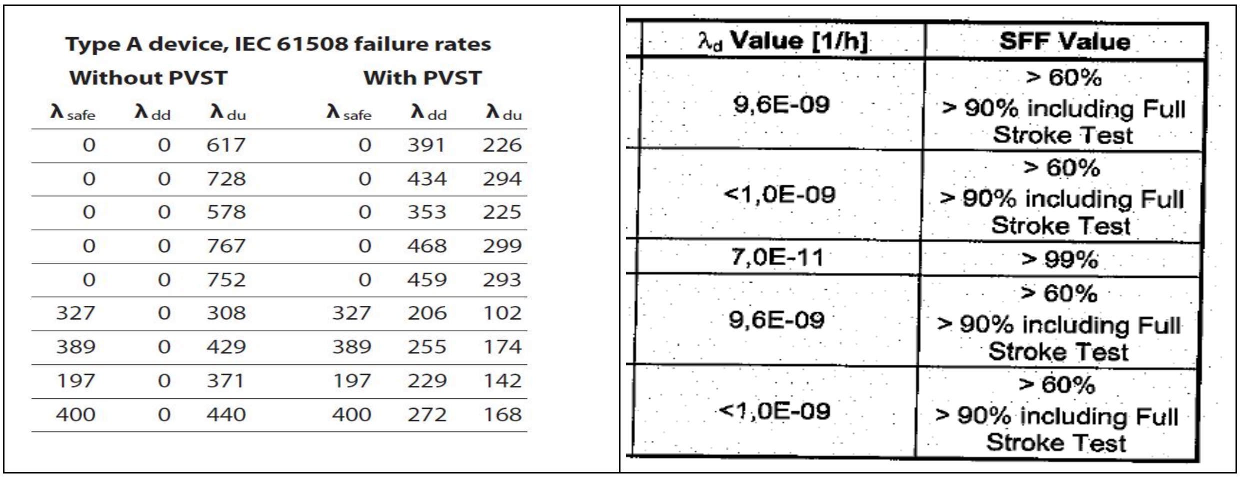
Having said that, there are already some product certificates with these type of analysis, as shown in the table below.

Table 2; A sample of FMEA analysis with PVST used as diagnostic tool.



Description	Failure mode	C'ponent Failure Rate (λs)	Failure modes factors	Qty of compts	Criticality safe=S danger=D no-efct=N loss	Diagnostic Detect=Y Undet=N	Annex A_P2	Safe Rev'led	Safe Un-rvld	Dangers Detect	Dangers Un-detec
Motor cover	Mechanical Failure	0.4	0.700	1	D	Yes	high	0	0	0.2772	0.0028
	Loosening	0.4	0.200	1	S	No		0	0.08	0	0
	Misc	0.4	0.100	1	N	No		0	0	0	0
Induction Motor Stator and	No Operation	1.734	0.780	1	D	Yes	high	0	0	1.33899	0.01353
	Degraded operation	1.734	0.060	1	S	No		0	0.104	0	0
	Unknown	1.734	0.160	1	S	No		0	0.2774	0	0
Motor Thermostat	Unknown	2.4113	0.600	2	D	Yes	high	0	0	2.86462	0.02894

The author looked at various final elements already certified where PVST option as diagnostic was used in the assessment, see Table 3. It has to be made clear to the reader, these data are already available in the public domain and are not meant to point against a specific certification agency. The main intention here is to clarify the main points as addressed by the IEC 61508 and how these should be implemented. Table 3 shows that when PVST is considered, then SFF is boosted up (approaching SIL 3 range and very low value for λ_d. This obviously contributes in constructing wrong safety instrumented systems in terms of SFF and PFD requirements.



Type A device, IEC 61508 failure rates

Without PVST			With PVST		
λ_{safe}	λ_{dd}	λ_{du}	λ_{safe}	λ_{dd}	λ_{du}
0	0	617	0	391	226
0	0	728	0	434	294
0	0	578	0	353	225
0	0	767	0	468	299
0	0	752	0	459	293
327	0	308	327	206	102
389	0	429	389	255	174
197	0	371	197	229	142
400	0	440	400	272	168

λ_d Value [1/h]	SFF Value
9,6E-09	> 60% > 90% including Full Stroke Test
<1,0E-09	> 60% > 90% including Full Stroke Test
7,0E-11	> 99%
9,6E-09	> 60% > 90% including Full Stroke Test
<1,0E-09	> 60% > 90% including Full Stroke Test

Table 3: Reliability data of final elements with and without PVST.

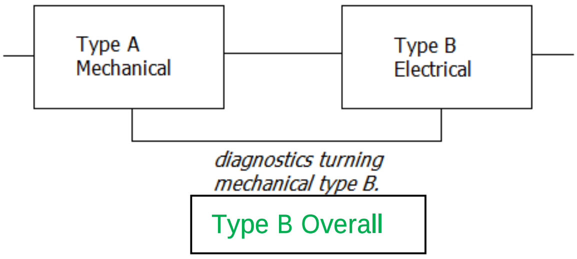
Practical PVST example

As part of this paper and as discussed above that diagnostic can be implemented internally; a study has been carried out to demonstrate that the use of Annex A of IEC 61508 part2, and when and where diagnostic function can be claimed. The author looked at a valve actuator assembly of a final element which consists of an automated actuator with specific hardware and firmware fully integrated with the actuated valve. This can be manually activated or remotely enabled using DCS or Logic Solver.

The assembly consists of the following parts:

A) Electronic modules (microcontroller driven), encoder, power supply, control board and interface board for external communication.

B) Gearbox, interfacing, base, drive motor, solenoid and torque sensor. A reliability block diagram is shown in Figure 1.



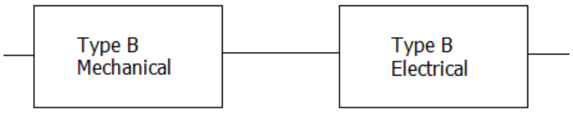


Figure 1: A reliability block diagram of the final element (excluding valve).

Annex (A) of IEC 61508-2 has been used for the electronic modules where diagnostic have been used on board for the measurement of the encoder signals, power supply monitor, control signals electronics conditioning. While diagnostic algorithm for the mechanical parts are not considered as parts of the daily diagnostics routine. This can be seen in Table (4) below that diagnostic claimed for the mechanical parts (type A) is less than 25% used in the FMEA. This is due to a small diagnostic factor can be claimed as part of the interfacing assembly. While the electronics modules (type B), diagnostic coverage is just under 60%. The firmware used is for local diagnostics and to generate PVST function upon a demand from the remote controller. Note that the random hardware failures are considered constant within the useful life of the valve assembly with regular maintenance provided.

When the electronics modules coupled to the valve actuation assembly, this makes the final product as a one kit of hardware. The full assembly becomes type B as quoted by references [4,10] and stated clearly in IEC 61508 part 2, clause 7.4.4.2.4.

In this example, PVST function is internally implemented to perform partial stroke testing function, an external logic signal is fed into the element to enable the processing of the PVST function. On completion of the test, the measured signals are fed back to the DCS system via a separate communication line.

Tables (5 and 6) below show the reliability figures with and without the PVST function. As can be seen table (5), the final element is treated as Type B and the SFF of the final element is SIL 1 based on the PFD value for a proof test interval (PTI) of 1 year, while the SFF is 97% (SIL 2). Hence the product cannot be SIL 2 even if its SFF shows SIL2.

In order to get the product complies with SIL 2 range, a PVST function with a partial diagnostic coverage factor (DCF) equal to 90% is used to enhance the value of the PFDavg. Table (6) shows the effect of 4 months of PVST while SFF is unchanged. This confirms that the use of the PVST improves the PFD as supposed to be while its impact on the SFF does not make the element a higher SIL.

Table 4: FMEA of both type A and Type B products.

Mechanical Type A								
λ	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU_m}	DC	SFF	PFD$_{AVG}$	PTI
7.30E-05	8.16E-06	6.18E-05	6.60E-07	2.42E-06	21.43%	96.69%	2.41E-02	1 yr
Electronic Type B								
λ	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU_e}	DC	SFF	PFD$_{AVG}$	PTI
9.04E-07	2.40E-08	6.69E-07	1.24E-07	8.68E-08	59%	90%	3.82E-04	1 yr

Table 5: Final element without PVST. Note, valve excluded in the calculation.

Parameter name	Symbol	Equation / source	Sira Result
Proof Test Interval	T1	Given, for this example	8760
Mean Time To Repair	MTTR	Given, for this example	24
Type A/B	type A/B	Given, for this example	type B
Total failures:	λ		7.39E-05
Safe diagnosed failures:	λ_{SD}		8.18E-06
Safe undiagnosed failures:	λ_{SU}		6.25E-05
Dangerous diagnosed failures:	λ_{DD}		7.84E-07

Dangerous undiagnosed failures:	λ_{DU}		2.51E-06
Diagnostic coverage:	DC	λ_{DD} / (λ_{DU} + λ_{DD})	0.00%
Safe Failure Fraction:	SFF	(λ_{SD} + λ_{SU} + λ_{DD}) / λ	**96.61%**
PFD$_{AVG}$ (using simplified equation)	PFD$_{AVG}$	λ_{DU} (T / 2+MTTR) + (λ_{DD} MTTR)	**1.11E-02**
SIL capability (Low demand mode)			**SIL 1**

Table 6: Final element with PVST. Note, valve excluded in the calculation.

Parameter name	Symbol	Equation / source	Sira Result
Proof Test Interval (hrs)	T1	Given, for this example	8760
PVST Interval (4months)	Tpvst	Given for this example	2920
Mean Repair Time	MRT	Given, for this example	24
Type A/B	type A/B	Given, for this example	type B
Total failures:	λ		7.39E-05
Safe diagnosed failures:	λ_{SD}		8.18E-06
Safe undiagnosed failures:	λ_{SU}		6.25E-05
Dangerous diagnosed failures:	λ_{DD}		7.84E-07
Dangerous undiagnosed failures:	λ_{DU}		2.51E-06
Diagnostic coverage:	DC	λ_{DD} / (λ_{DU} + λ_{DD})	23.82%
PST diagnostic coverage	DCF	Given, for this example	90.00%
Safe Failure Fraction:	SFF	(λ_{SD} + λ_{SU} + λ_{DD}) / λ	**96.61%**
PFD$_{AVG}$ (using simplified equation)	PFD$_{AVG}$	λ_{DU} (T / 2+MTTR) + (λ_{DD} MTTR)	**1.11E-02**
PFDpst	PFDpst	λ_{DU} (T / 2)	**1.10E-02**
PFDavg_pvst	PFDavg_pvst	See equation 2 below	**4.45E-03**
SIL capability (Low demand mode)			**SIL2**

The general equation of the probability of failure on demand given by IEC 61508 is described in equation 1. When PVST function is used as a partial stroke testing for a given diagnostic coverage factor of 90% then equation 1 is expanded as shown in equation 2, as per part 6, clause B 3.2.5.

$$\mathrm{PFDavg_O} = \lambda\mathrm{du} \times \frac{T_{PTI}}{2} + \lambda\mathrm{dd} \times \mathrm{MTTR} \qquad \mathrm{Eq.\,1}$$

Note, equation 1 does not include PVST function, i.e the firmware module is not functioning.

Equation 2 represents an approximation equation of the PFDavg of the final element when PVST is included. Note, valve failure rate is excluded in the calculation.

$$\mathrm{PFDavg} = \mathrm{DCF}\ \lambda_{du}\ (\mathrm{MRT+Tpvst}\ /2\ ) + (1\text{-}\mathrm{DCF})\ \lambda_{du} \times\ \mathrm{PTI}/2\ \ )\times (1\text{-}\ \mathrm{PFDavg\_em}) + \mathrm{PFDavg_0} \times \mathrm{PFDavg\_em} \qquad \mathrm{Eq.2}$$

The first part of equation (2) (DCF λ_{du} (MRT+Tpvst /2) represents the dangerous detected part similar to the second part of equation (1). The time takes to conduct PVST is very small, some literatures specify this value anywhere between 30 to 2 minutes. In this assessment MRT is considered zero as the PVST is conducted while the system is not under repair time.

Based on the above reliability figures, a summary calculation is summarised below in Table 6 and assumption made to the following factors.

DCF = 90%; MRT = 0; Tpvst = 4 months; PTI = 1 yr (8760 hrs).

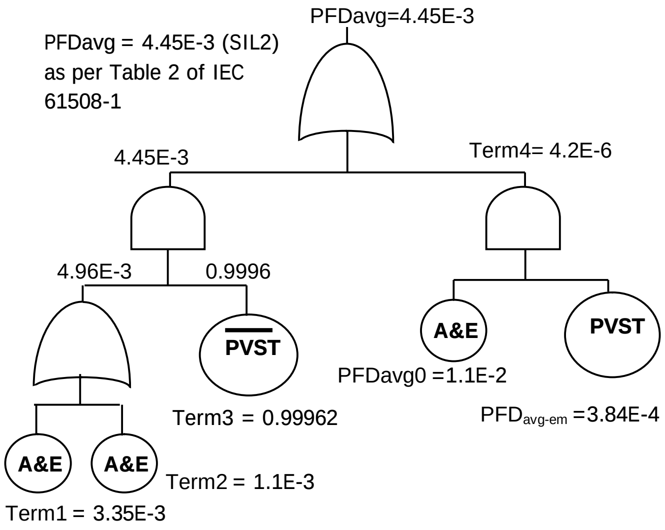
Table 6: Summary of the calculation of the actuating element.

Final assembled product (Ac + Em) λ_{DU} / yr ; 1 yr = 8760 hrs	2.51 E-6 (see table 6) 2.2 E-2 f/yr
PFDavg$_0$ = (2.2 x 1/2) E-2	1.1 E-2 (see table 5)
Dangerous undetected for electronic Module. λ_{DU} / yr ; 1 yr = 8760 hrs	8.68 E-8 f/hr or 8.68 E-4 f/yr
PFDavg_em	3.8E-4
Term1: (DCF λ_{du} (MRT+Tpvst / 2)	3.35 E-3
Term2: (1-DCF) λ_{du} x PTI/2)	1.1 E-3
Term3: (1- PFDavg_em)	0.99962

Term4: (PFDavg$_0$ x PFDavg_em)	4.2 E-6
PFDavg : (term1+term2)xterm3+term4	4.45 E-3

A fault tree analysis is provided to illustrate the assumption made for the calculation of the subsystem PFDavg. Since PVST firmware is part of the final element assembly, claiming dangerous failures is subject to the availability of the PVST function which is generated by the electronic modules. When PVST is required, then partial testing is performed automatically, this means the firmware module produces the PVST function. When PVST firmware is not available, i.e the firmware is not acting, then the PFDavg of the actuator will revert back to equation one, unless a shutdown is taking place. This can be represented as shown in Figure 3 (fault tree graph).

Figure 3: Fault tree analysis of the final assembly.



The example above has demonstrated that PFDavg of the final element is improved from SIL 1 to SIL2 under PFD criteria.

According to edition 2, and as said above the random hardware failure of the diagnostic shall be taken into consideration in the element, see clause (7.4.9.4-J) that makes the final assembly type B, as credit has been claimed for the undetected dangerous failures.

As can be seen in the above example, PVST was used in improving the PFDavg level in terms of the probability of low demand table shown in Table 2 of IEC 61508-1, the possibility of using such a feature to claim appropriate credit in the PFD figures and to improve the SFF is not acceptable, because it violates the above clauses as diagnostics credit cannot be claimed if the tools that implementing such diagnostics are ignored and were not included in the architecture constraints assessment. Of course, implementing a remotely controlled PST is a supportive tool if used as partial tests to extend the full proof test intervals. The PFDavg values of the PLC or DCs who performs the PVST commands and conducts the assessment shall be included in the above calculation in place of the PFDavg_em to rework the overall PFDavg values of the final element whilst the SFF of the final elements shall be unchanged. Therefore, using this feature in the wrong objective may lead to unsatisfactory results and misguiding the end users.

Conclusion

PVST is invaluable on line tool, which is very useful in improving the PFD of the final element as it contributes to reveal parts of the undetected dangerous failures within the scope of the diagnostic coverage factor on the basis as partial tests not as diagnostics test to claim full coverage. It should not be used to affect the calculation of the safety failure fraction SFF as shown in some certifications. If used as a means of diagnostic automated tool, the additional programmable firmware shall be assessed as type B to identify any undetected dangerous failure and should be included in the overall architecture constraints assessment as a fully integrated ESD valves.

The assessment shall be considered to IEC 61508 (ed.2) and PVST credit shall not be considered to overcome any redundancy requirement.

It is known that product SIL classification does not rely only on PFD values, it relies also on the architectural constraints, as said in [9] that “ESD valves should be considered not only on PFD but also on SFF without PVST unless the MTTR claimed includes the PVST interval”.

The final element safety integrity level (SIL) does not rely on the PVST features irrespective if PVST implemented internally or externally. SIL relies on the architecture constraint, type, HFT and the PDF value for a given proof test interval on top of the systematic safety integrity assessment.

References

[1] BS EN 61508:2002; Functional safety of electrical/electronic/programmable electronic safety-related systems
[2] BS EN 61508-2:2010, Ed. 2.0 : Functional safety of electrical/electronic/programmable electronic safety related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety related systems
[3] Chris O’Brien , “too good to be true” , April 2012, Safety automation element list.
[4] Robin McCrea-Steele, “Partial Stroke Testing Implementing for the Right Reasons”, ISA EXPO 2005, 25-27 October [2005]
[5] A.F.M. Prins, “Partial Stroke Testing”, Yokogawa, system centre Europe, [2010].
[6] Bill Mostia, “Partial Stroke Testing, Simple or Not?|”, control magazine, Nov. [2003].
[7] BS EN 61508-4:2010, Ed. 2.0 : Functional safety of electrical/electronic/programmable electronic safety related systems – Part 4: Part 4: Definitions and abbreviations
[8] Translation of special print from atp – Automatisierungstechnische Praxis Volume 47 ·Issue 4 [2005]
[9] Harley Dearden, “Partial Stroke Testing. Diagnostic or Proof test?” Inst. M&C, vol.46, no.5 June [2013].
[10] Web Guidline, M-2790-x-11,”SIS automated block valves (ABV) Assemblies”, draft copy, Sept. [2012]