The effect of partial stroke testing on the reliability of safety valves

M. A. Lundteigen & M. Rausand
Department of Production and Quality Engineering
Norwegian University of Science and Technology

November 19, 2007

Abstract

Safety instrumented systems (SIS) are used to protect against consequences of hazardous events in the oil and gas industry. It is important to detect failures that may impede the SIS from performing upon demands. Recently, partial stroke testing has been introduced as an automatic means to test the SIS valves. Partial stroke testing is able to detect failures that traditionally have been revealed by function testing without causing process disturbances. Unfortunately, authors have different views on how partial stroke testing contributes to SIS reliability, and how failures detected by partial stroke testing should be classified. In this paper, it is shown that the failure classification may influence the hardware design, whereas the reliability modeling approach is not affected. In addition, a partial stroke test coverage factor has been proposed based on historical data.[1]

1 Introduction

Safety instrumented systems (SIS) are installed on oil and gas installations to detect the onset of hazardous events and/or mitigate their consequences to humans, material assets, and the environment. A SIS generally consists of one or more input elements (e.g., sensors, transmitters), one or more logic solvers (e.g., programmable logic controllers, relay logic systems), and one or more final elements (e.g., safety valves, circuit breakers).

The international standards IEC 61508 and IEC 61511 are widely used in the oil and gas industry for design and follow-up of SIS. The standards comprise requirements for specifying the desired performance of the SIS, estimating the predicted performance and verifying the actual performance in the operational phase. IEC 61508 and IEC 61511 use safety integrity level (SIL) as a measure of SIS reliability.

[1] A version of this paper was presented at the ESREL conference in Stavanger, 2007

In the operational phase, it is important to monitor the actual performance of the SIS. One may split the SIS performance into unknown and known unavailability as suggested by PDS[2] [17], a reliability estimation method that is frequently used in the Norwegian oil and gas industry. The known unavailability can be calculated from the rate of failures and the associated downtime, for example, due to repair. The unknown unavailability may be calculated from the rate of "critical" failures and the time until these failures are discovered. IEC 61508 and IEC 61511 refer to this category of failures as dangerous failures, where dangerous means that the SIS is not able to perform its safety functions as long as the failures are present. Dangerous failures may be hidden until they are discovered by a function test or a real demand. In this case, the failures are referred to as dangerous undetected (DU) failures. In other cases the failures may be detected shortly after they have been introduced, for example, by online diagnostics. Such failures are referred to as dangerous detected (DD) failures.

Traditionally, function testing has been considered as offline means, and diagnostic testing as online means to detect failures. For safety valves, a function test means to perform a full stroke operation of the valves. In recent years, automatic means have been introduced that can partly replace the need for offline function testing. One such example is partial stroke testing (PST) of safety valves [19]. PST means to partially test a safety valve's ability to perform its safety function (e.g., close on demand), by moving the valve without fully closing the valve. A small valve movement may be sufficient to detect several causes of dangerous undetected failure modes without interrupting the production. The fraction of dangerous undetected failures detected by PST among all dangerous undetected failures is referred to as the PST coverage factor. PST is often performed at regular intervals that are shorter than the function test interval. In this case, the PST may reduce the unknown unavailability of the SIS. There are different approaches to how PST is taken into account for SIS hardware design and reliability estimation [1, 2, 9, 11, 12, 19, 20]. Some authors disagree that PST is a function test, which again influences the classification of the failures detected by PST.

The objective of this paper is to clarify the reliability implications of PST, and to propose a PST coverage factor based on analysis of failure modes and historical failure data. The PST system installed to test the safety valves in a subsea High Integrity Pressure Protection System (HIPPS) at the Kristin field [3], is used to illustrate the application of PST. Kristin is an oil and gas field located outside mid Norway that is operated by Statoil. The term HIPPS is used to describe an instrumented based protective system that replaces mechanical protection of pressurized vessels or pipeline. The HIPPS at Kristin comprises pressure transmitters (voted 2oo4), a solid state logic solver (voted 1oo1) and fast closing safety valves (voted 1oo2) operated by a separate directional control valve (solenoid). Upon high pressure, the safety valves are intended to close. The maximum allowable HIPPS valve closure time depends on the pipeline pressure; a higher pipeline pressure causes

[2] PDS is the Norwegian acronym for "reliability of computer-based safety systems"

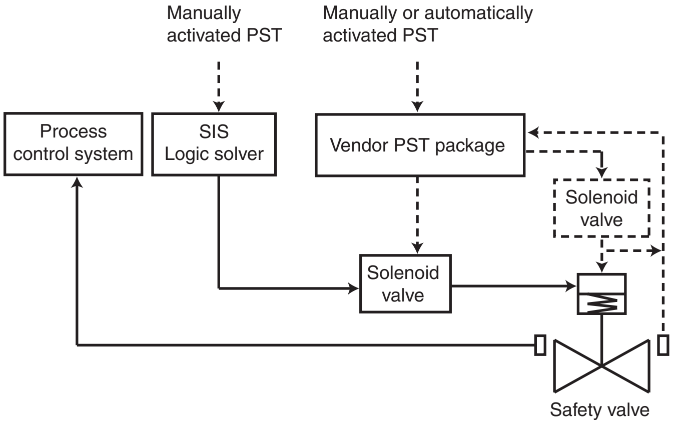

Figure 1: Different PST concepts

the valve to close faster. A maximum leakage rate in closed position is specified to avoid downstream pressure build-up.

The paper is organized as follows: A brief introduction to the main principles and benefits of PST is given in Section 1, together with an outline of the objectives of the paper. The main PST concepts are introduced in Section 2 and the advantages and disadvantages of introducing PST are briefly discussed in Section 3. The PST coverage factor is introduced in Section 4 where the various failure rates are also defined. The effect of introducing PST on the SIS reliability is discussed in Section 5 and the effects on systematic failures and architectural constraints are outlined in Section 6. In Section 7 we estimate the PST coverage of safety valves based on a failure mode analysis and recorded failure data. PST versus function testing is discussed in Section 8 and a case study is presented in Section 9. Some concluding remarks are given in Section 10.

2 PST concepts

A PST may be implemented in several ways [8, 19]. Two different concepts are illustrated in Figure 1: (i) A PST that is integrated with the SIS, and (ii) a separate PST package, usually supplied by the vendor. Other concepts like mechanical limiting and position control, that are not further discussed here, may also be selected [1, 19].

In case (i) the hardware and software necessary to perform a PST is implemented into the SIS logic solver. This solution is selected for PST of the Kristin HIPPS valves. When PST is initiated based on a manual request, the logic solver deactivates its outputs for a certain period of time (typically a few seconds). The deactivated outputs cause the solenoid valve (or in some cases, a directional control valve) to start depressurizing the safety valve, and the safety valve starts to move towards the fail safe closed position. Just as the valve starts to move, the logic solver outputs are re-energized, and the safety valve returns to the normal (open) position. The test results may be monitored manually from the operator stations, by verifying that the valve leaves its end positions and returns to the normal state when the test is completed, or alternatively an automatically generated alarm if the valve fails to move, or to return to its initial position.

The separate PST packages perform the same type of test sequence, but the hardware and software are implemented into separate systems, usually supplied by the valve vendors. Some vendors interface the existing solenoid, while others install a separate solenoid for testing purposes. The vendor supplied PST packages may automatically generate the PST at regular intervals. In many cases, the control room operators want to be in control with the actual timing of the PST, and manual activation may therefore be preferred.

The SIS implemented PST is considered to be able to test a larger fraction of the safety function than the vendor packages, since the test includes all components from the logic solver output cards to the safety valve. On the other hand, the PST vendor packages often suggest the installation of additional sensors, and use the sensor feedback for more advanced analysis of the safety valve response.

3 Advantages and disadvantages

PST may be introduced as a supplement to function testing. Two different approaches may be chosen when introducing PST:

(A) To improve the unknown unavailability by adding PST to the initial test schedule, i.e., keeping the initial function test interval unchanged.

(B) To introduce PST in order to extend the initial test interval while keeping the unknown unavailability unchanged.

Approach A will improve system safety while approach B will contribute to reduced operating costs. Further comments to the advantages and disadvantages of introducing PST are given in Table 1.

4 Failure rates and coverage

It is important to distinguish between the PST coverage and what IEC 61508 and IEC 61511 refer to as diagnostic coverage. One starting point is to consider the relationship between detection method and the allocation of failure rates, see Figure 2. Here, λ_{D} denotes the rate of dangerous failures, λ_{DD} is the rate of dangerous detected failures and λ_{DU} the rate of dangerous undetected failures. λ_{D} is further split into $\lambda_{\mathrm{DU,PST}}$ and $\lambda_{\mathrm{DU,FT}}$ to illustrate that dangerous undetected failures may be revealed by a partial stroke test or a function test.

Table 1: Advantages and disadvantages of PST

Advantages	Disadvantages
Reduced wear of the valve seat area since the valve is less frequently brought to a closed position, see [19] (in case approach B is selected).	More complex system due to added software and hardware.
Reduced probability of sticking seals due to more frequent operation of the valve.	Increased wear due to more frequent operation.
Reduced operational disturbance due to testing (in case approach B is selected).	Potentially increased spurious trip rate since the valve may continue to fail safe position instead of returning to the initial position.

The diagnostic coverage (DC) is by IEC 61508 and IEC 61511 defined as the fraction of dangerous failures that are detected by diagnostics among all dangerous failures. Mathematically, the diagnostic coverage, θ_{DC}, may be expressed as:

$$\theta_{\text{DC}} = \frac{\lambda_{\text{DD}}}{\lambda_{\text{D}}} \tag{1}$$

The DC has two different interpretations:

1. The mean fraction of dangerous failures that are detected by diagnostics among all dangerous undetected failures.

2. The probability that a dangerous failure is detected by the diagnostics once a dangerous failure is present (conditional probability).

The PST coverage may be defined as the fraction of dangerous undetected failures detected by PST relative to the total number of dangerous undetected failures, or

$$\theta_{\text{PST}} = \frac{\lambda_{\text{DU,PST}}}{\lambda_{\text{DU}}} \tag{2}$$

Analogous to the DC, there are two interpretations of the PST coverage:

1. The mean fraction of dangerous undetected failures that are detected by PST among all dangerous undetected failures.

2. The probability that a dangerous undetected failure is detected by the PST once a dangerous undetected failure is present (conditional probability).

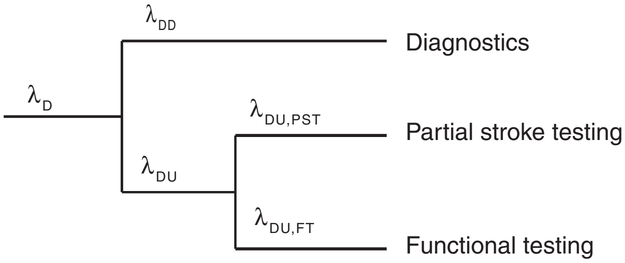

Figure 2: Overview of the relevant failure rates

The three failure rates λ_{DD}, $\lambda_{\text{DU,PST}}$ and $\lambda_{\text{DU,FT}}$ may all be expressed in terms of λ_{D} as follows:

$$\begin{aligned}
\lambda_{\text{DD}} &= \theta_{\text{DC}} \cdot \lambda_{\text{D}} && (3)\\
\lambda_{\text{DU,PST}} &= (1-\theta_{\text{DC}}) \cdot \theta_{\text{PST}} \cdot \lambda_{\text{D}} && (4)\\
\lambda_{\text{DU,FT}} &= (1-\theta_{\text{DC}})(1-\theta_{\text{PST}}) \cdot \lambda_{\text{D}} && (5)
\end{aligned}$$

5 Reliability models

The SIS may operate in the high demand or continuous mode or in the low demand mode, depending on the expected demand frequency. For SIS operating in low demand mode (which is the typical situation at oil and gas installations), the reliability, or more precisely the unreliability, is often measured as the average probability of failure on demand (PFD), e.g., see [15]. A SIS operating in low demand may experience on average one demand or less per year. The estimated PFD must comply with the PFD range of the SIL requirement described in IEC 61508 and IEC 61511. For example, to meet a SIL 3 requirement the predicted PFD must be less than $1 \cdot 10^{-3}$.

The average PFD for a single component can generally be determined from the dangerous failure rates and the test intervals. If more than one component is installed to protect against the same hazardous event (redundant configurations), it is also necessary to consider potential common cause failures (CCF). In the following, the analysis is restricted to a single safety valve.

When PST is not implemented, the average PFD of the safety valve is approximately to the sum of the average PFD relative to function testing (PFD_{FT}) and the average PFD for diagnostic testing (PFD_{DT}):

$$\begin{aligned}
\text{PFD} &\approx \text{PFD}_{\text{FT}} + \text{PFD}_{\text{DT}}\\
&\approx \frac{\lambda_{\text{DU}} \cdot \tau_{\text{FT}}}{2} + \frac{\lambda_{\text{DD}} \cdot \tau_{\text{DT}}}{2} && (6)
\end{aligned}$$

where τ_{FT} is the function test interval and τ_{DT} is the diagnostic test interval. In most cases, the diagnostic test interval is very short, and PFD_{DT} is therefore negligible.

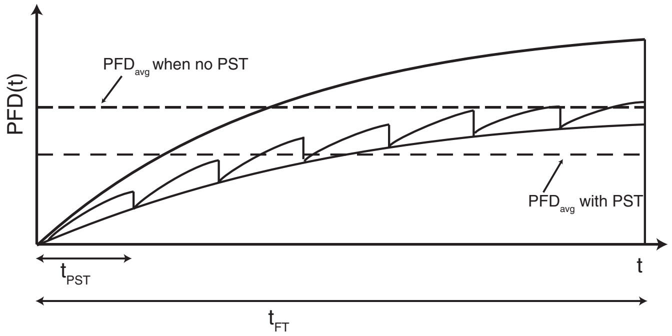

Figure 3: PST contribution to PFD

The PST may detect a fraction of the dangerous undetected failures, corresponding to the PST coverage θ_{PST}. The PFD may then be expressed as:

$$\begin{aligned}\mathrm{PFD} &\approx \mathrm{PFD}_{\mathrm{FT}} + \mathrm{PFD}_{\mathrm{PST}} + \mathrm{PFD}_{\mathrm{DT}} \\ &\approx (1-\theta_{\mathrm{PST}}) \cdot \frac{\lambda_{\mathrm{DU}}\tau_{\mathrm{FT}}}{2} \\ &\quad + \theta_{\mathrm{PST}} \cdot \frac{\lambda_{\mathrm{DU}}\tau_{\mathrm{PST}}}{2} + \frac{\lambda_{\mathrm{DD}}\tau_{\mathrm{DT}}}{2} \qquad (7)\end{aligned}$$

where τ_{PST} is the PST interval. The PFD *with* and *without* taking PST into account may be illustrated as shown in Figure 3.

The estimated PFD is improved when PST is introduced, since a portion of the dangerous undetected failures are detected and corrected within a shorter time interval after their appearance, than by function testing.

The PFD is the unknown unavailability of the safety valve. The safety valve may also be unavailable after a failure has been detected (by diagnostics, PST, function test or a real demand). In this case, the unavailability is known. The PDS method [16, 17], refers to the known unavailability as the downtime unavailability (DTU). The average or mean time to restore the component, including repair time and delay, is often referred to as the mean time to restoration (MTTR). In this case, the DTU may be expressed as:

$$\begin{aligned}\mathrm{DTU} &\approx \mathrm{DTU}_{\mathrm{FT}} + \mathrm{DTU}_{\mathrm{PST}} + \mathrm{DTU}_{\mathrm{DT}} \\ &\approx (1-\theta_{\mathrm{PST}}) \cdot \lambda_{\mathrm{DU}} \cdot \mathrm{MTTR}_{\mathrm{FT}} \\ &\quad + \theta_{\mathrm{PST}} \cdot \lambda_{\mathrm{DU}} \cdot \mathrm{MTTR}_{\mathrm{PST}} \\ &\quad + \lambda_{\mathrm{DD}} \cdot \mathrm{MTTR}_{\mathrm{DT}} \qquad (8)\end{aligned}$$

where $\mathrm{MTTR}_{\mathrm{FT}}$, $\mathrm{MTTR}_{\mathrm{PST}}$ and $\mathrm{MTTR}_{\mathrm{DT}}$ are the MTTR for failures detected by function testing, partial stroke testing, and diagnostic testing, respectively. The MTTR is usually some hours (e.g., 8 hours) for topside equipment if crew and spare parts are available. For subsea equipment requiring mobilization of an intervention rig/vessel, or when equipment spare parts have a long lead time, the MTTR may be weeks or months. Possible unavailability during PST and function testing is not included in Eq. 8.

6 SIL is more than PFD

To comply with a specified SIL, it is not sufficient to verify that the predicted PFD is within a specified range [5, 10, 18]. There are two additional requirements that must be met:

1. Avoidance and control of systematic failures
2. Selection of hardware configuration within the architectural constraints

Systematic failures are according to IEC 61508 and IEC 61511 failures that are due to a certain cause (e.g., design error, installation deficiency, maintenance procedure error), and may only be removed by modification to design, manufacturing, installation, operation and maintenance procedures, and so on. Some requirements for avoidance and control of systematic failures are common for all SIL levels, while others, particularly for software development, may depend on the specified SIL.

Architectural constraints have been introduced to restrict the obtainable SIL for a function implemented into the SIS. The architectural constraints limit the freedom of hardware design, to compensate for uncertainty in reliability estimates and input data. The architectural constraints specify a minimum level of hardware fault tolerance for a combination of SIL and the safe failure fraction (SFF). The hardware fault tolerance is the same as the number of failures the system tolerates before the safety function is affected. The SFF is an extension of the DC, also considering the safe failures, and is defined as:

$$\mathrm{SFF} = \frac{\lambda_{\mathrm{DD}} + \lambda_{\mathrm{S}}}{\lambda_{\mathrm{DU}} + \lambda_{\mathrm{DD}} + \lambda_{\mathrm{S}}} \tag{9}$$

where λ_{S} is the rate of safe failures, and the other failure rates are defined as above. The hardware fault tolerance is in IEC 61508 and IEC 61511 presented in two separate tables, one for high complexity components and one for low complexity components. A safety valve is normally defined as low complexity. The higher the SFF, the lower the hardware fault tolerance requirements. For the Kristin subsea HIPPS, where a SIL 3 is specified, a hardware fault tolerance of one is required. Installing two safety valves in series fulfills this requirement.

7 Assessing the PST coverage

The PST coverage may be derived from a failure modes and effect analysis (FMEA), alternatively estimated based on analysis of historical failure data. The latter approach has been selected here. The OREDA handbooks [13, 14], containing failure data collected in the period 1988 to 1992 and 1993 to 1996, respectively, have been used to determine the distribution of dangerous failure modes. OREDA distinguishes between critical, degraded, and incipient failures. A critical failure is defined as “a failure that causes immediate and complete loss of a systems capability of providing its outputs.” A degraded failure is a failure that impedes the system from providing its outputs within specifications, while an incipient failure is a failure that is not yet critical but may become so if not attended to. The three failure categories comprise spurious trip failures as well as dangerous failures. When estimating the PST coverage, it is important to extract the failure modes that are relevant, i.e., the dangerous failure modes.

It may be relevant to take dangerous critical failures as well as dangerous degraded failures into account, since the practical distinction between the two may be vague, particularly when taking uncertainty in the recording of failures into account. The critical and degraded failure modes that may be considered as dangerous are:

- Delayed operation (DOP)
- External leakage of process medium (ELP)
- Failure to close on demand (FTC)
- Leakage in closed position (LCP)

The PST coverage *per* dangerous failure mode may be derived from detailed analysis of how the actual PST installation is able to capture the various failure modes. A preliminary evaluation of the PST coverage is indicated in Table 2.

By analyzing the distribution of dangerous failure modes for different types of safety valves (and aggregated data for safety valves) and combining these with an assessment of the PST coverage for each failure mode, the PST coverage factors in Table 3 are obtained. Even though the HIPPS valves at the Kristin field are gate valves, data are also presented for ball valves to show the differences. The overall perception is that failure rates collected in the period 1993-1996 are better than for the period from 1988-1992. As seen, the PST coverage varies between 27% and 97%. A weighted average of the PST coverage factors for the most relevant valves in Table 3 gives a PST coverage for the Kristin HIPPs valves of approximately 62%.

The estimated PST coverage factors are uncertain due to a number of reasons:

- No data has been collected especially for HIPPS valves. HIPPS valves are normally gate valves designed for quick closure, and the failure mode distribution may be different from ESD/PSD gate valves.
- OREDA does not specify the type or design of the subsea isolation valves. The data may therefore not be representative for HIPPS subsea valves.

The estimated PST coverage for the topside safety valves is similar to the result obtained by [19]. They found that the maximum percentage of dangerous

Table 2: PST coverage for various failure modes

Failure mode	PST coverage	Comment
DOP	100%	Any obstruction that may impede the valve from moving may be detected by the PST if existing solenoid is used. If a separate solenoid is used, the PST coverage may be somewhat reduced.
ELP	20%	The leakage may occur when the valve has been fully closed, and the upstream pressure is increased. A small fraction of external leakage is therefore expected to be detected by PST.
FTC	95%	It is likely that the valve will continue to move to a closed position once it starts to move.
LCP	0%	Leakage testing requires that the valve is fully closed.

Table 3: PST coverage for different valves

Type of valve	PST coverage
Topside-all [14]	67%
Topside-all gate [14]	55%
Topside-all ball [14]	87%
Topside ESD ball [14]	97%
Topside ESD ball2 [14]	92%
Topside ESD gate [14]	92%
Topside ESD/PSD ball [14])	85%
Topside ESD/PSD gate [14])	96%
Topside-all ESD/PSD [13]	27%
Topside ESD/PSD gate [13]	27%
Topside ESD/PSD ball [13]	27%
Subsea-all isolation [14]	51%
Subsea manifold isolation [14]	29%

undetected failures that may be revealed by a PST is 70%. However, [19] recommend that plant specific considerations are taken into account when giving credit to the PST. If a valve is specified for tight shut-off, the contribution of PST is less than if the valve is specified for just closure.

8 Diagnostic vs. function testing

It is not straightforward from IEC 61508 and IEC 61511 to decide whether or not a PST should be defined as a function test or a diagnostic test. The standards are confusing in terms of any restriction to the diagnostic test interval when estimating the unknown unavailability from the diagnostics. An upper constraint is set for SIS operating in high demand mode, while no similar restriction is set for low demand mode, see IEC 61508 (part 2, 7.4.3.2.2e, note 3). Several authors have tried to clarify the distinction on a more general level [4, 21]. The standards recommend that the diagnostic test interval is taken into account through the MTTR.

As long as the PFD is estimated by taking into account all dangerous failures and their associated test frequency as shown in Eq. 7, it makes no difference to the estimated PFD improvement. However, if the fraction of failures $\theta_{\text{PST}} \cdot \lambda_{\text{DU}}$ is considered as a contribution to the rate of dangerous detected failures, the SFF may improve. Improving the SFF may allow a lower hardware fault tolerance, and thereby a less costly hardware design. With respect to the architectural constraints, it is important to decide whether or not a PST should be considered as a means to improve the SFF.

The distinction between function testing and diagnostic testing has been discussed with SIS vendors, system integrators and oil companies, who also indicate different interpretations. Some consider a diagnostic test as a test that is run once every CPU cycle (which means close to continuously), some claim that a diagnostic test should be run at least once every 24 hours, while others believe that the rule of an order less than the expected demand frequency should apply to a SIS operating in low demand and high (or continuous) mode. There are also different views on whether or not PST should contribute to SFF.

9 Reliability assessment

In the following, the SIS reliability without using PST is compared to the case where PST is used. In this example, the contribution from known unavailability (due to repair) is not taken into account, and the reliability estimates are restricted to a single HIPPS valve. Further improvements may be to extend the reliability model to also consider the PST coverage for the other SIS components of the safety function. The selected input data are presented in Table 4. The failure rates used for estimating the reliability in this article are derived from the PDS handbook [16], and are not the same data that were used for the Kristin design. The PST interval and the function test interval have been selected in accordance with what Kristin

Table 4: Input parameters

Parameter	Value	Comment
λ_{S}	$2.7 \cdot 10^{-6}$	Failures per hour
λ_{D}	$2.7 \cdot 10^{-6}$	Failures per hour (OREDA)
θ_{PST}	60%	See main text
θ_{DC}	25%	See [17]
τ_{FT}	8760	Hours in a year
τ_{PST}	1460	Hours in two months
τ_{DT}	1	Hours
MTTR	730	Hours in a month
SFF	63%	Estimated using Eq. 9

Table 5: Reliability estimates

	PFD	
Contribution	No PST	With PST
Diagnostics	$3.4 \cdot 10^{-7}$	$3.4 \cdot 10^{-7}$
PST	–	$8.9 \cdot 10^{-4}$
Function test	$8.9 \cdot 10^{-3}$	$3.6 \cdot 10^{-3}$
Total	$8.9 \cdot 10^{-3}$	$4.4 \cdot 10^{-3}$

has selected, that are 2 months and every year respectively (in the initial phase of Kristin operation the function test interval may be shorter).

Following the recommendations by [19], the plant specific installation should be considered when selecting a PST coverage. On Kristin, the HIPPS valves are located on the seabed. This may not affect the PST coverage as such but the predicted failure rates may differ from valves installed topside. The PST could potentially have been increased if a vendor specific package had been used to analyze the valve response, rather than just verifying that the safety valves leaves and returns to its end positions. An argument for selecting PST coverage close to the factor estimated in Section 7, is that the most critical failure mode, FTC, is well covered by the current implementation of PST. By using the input data in Table 4 and Eqs. 3, 4, 5 and 7, the resulting PFD is obtained as shown in Table 5.

As shown in Table 5, the estimated PFD is improved (reduced) when PST is introduced. The PFD improvement depend on how frequent the PST is performed compared to the function test interval.

If PST is also considered as a contribution to the SFF (redefining the dangerous failures detected by PST as dangerous detected), the SFF will increase. If the improvement is sufficiently large, it may imply a reduction in the hardware fault tolerance. The initial SFF is estimated to 63%, see Table 3. To meet the SIL 3 requirement (which is the case for Kristin HIPPS) it is required to have a hardware fault tolerance of one (e.g., to install two valves in series, where one is sufficient to protect against overpressure). If PST is given credit through the SFF, the SFF may increase to about 83%. An optimistically set PST coverage (e.g. 75%) may increase the SFF above 90% and thereby allow the hardware fault tolerance to be reduced by one (meaning that one HIPPS valve would be sufficient for overpressure protection).

10 Concluding remarks

PST is a valuable supplement to function testing of safety valves. The magnitude of reliability improvement is determined by the PST coverage and the PST interval. The discussion on whether failures detected by PST should be considered as dangerous detected or dangerous undetected failures is irrelevant when estimating the average PFD, as long as each failure rate is related to the corresponding test interval. The estimated PST coverage is very sensitive to the quality of historical failure data, the selected valve design and the plant specific conditions. An application specific PST coverage should therefore be used rather than a generic value.

Classification of failures detected by PST becomes important when assessing the architectural constraints. If PST is classified as dangerous detected failures rather than dangerous undetected failures, the SFF may be improved. On the other hand; if the failures are still classified as dangerous undetected, the SFF is not influenced by PST.

So which approach is the most correct one? One may look at the intended interpretation of the SFF. The SFF may be understood as a conditional probability; that is the probability that the failure is safe or known (dangerous detected) once a failure has occurred. If time between PST is long, it is likely that a dangerous failure is undetected at the time a dangerous failure occurs. It is therefore recommended to allow improvements in the SFF due to PST in cases where the PST interval is short. A short PST interval should be selected such that the corresponding unavailability of the SIS is negligible. In real applications, the PST interval is often in months rather than hours, for example on the Kristin field where the subsea HIPPS valves are tested by PST every second month. In this situation, we believe that the the PST is not run frequently enough to justify any improvements to the SFF.

There are several issues related to PST that may require further research. One important area is to develop more accurate estimates for the PST coverage, for example taking into account the valve design and the plant features. It may also be useful to extend the discussion on PST coverage to other SIS components that are covered by the PST, like the solenoid. Other research areas are to develop optimization models for PST and to further investigate the PST-SFF relationship.

References

[1] Ali, R. (2004). Problems, concerns and possible solutions for testing (and diagnostic coverage) of final control elements of SIF loops. In *4th Annual Emerging Technologies Conference, ISA EXPO 2004, October*, Research Triangle Park, NC 27709, U.S.A. ISA - Instrumentation, Systems, and Automation Society.

[2] Ali, R. & Goble, W. (2004). Smart positioners to predict health of ESD valves. Research Triangle Park, NC 27709, U.S.A. ISA - Instrumentation, Systems, and Automation Society.

[3] Bak, L., Sirevaag, R., & Stokke, H. (2006). Experience with the HPHT subsea HIPPS on Kristin. In *Deep Offshore Technology - Conference and Exibition*, 28.-30.November 2006, Houston, Texas.

[4] Brown, S. (2000). Overview of IEC 61508. design of electrical/electronic/programmable electronic safety-related systems. *Computing and Control Engineering Journal*, *11*, 6–12.

[5] Hoekstra, S. (2005). Safety integrity - more than hardware. *Hydrocarbon Engineering*, *10*(3), 79–82.

[6] IEC 61508 (1997). *Functional safety of electrical/electronic/programmable electronic safety-related systems*. Geneva: International Electrotechnical Commission.

[7] IEC 61511 (2003). *Functional safety - safety instrumented systems for the process industry*. Geneva: International Electrotechnical Commission.

[8] ISA (2002). *Guidance for testing of process sector safety instrumented functions (SIF) implemented as or within safety instrumented systems (SIS)*. Number SA-TR84.00.03-2002. NC 27709, U.S.A.: ISA - Instrumentation, Systems, and Automation Society.

[9] Knegtering, B. (2004). Safety-PLC's striking role for partial valve stroke testing. Research Triangle Park, NC 277089, U.S.A. ISA - Instrumentation, Systems, and Automation Society.

[10] Lundteigen, M. A. & Rausand, M. (2006). Assessment of hardware safety integrity. In *ESReDa Conference*, Trondheim, Norway.

[11] McCrea-Steele, R. (2005). Partial stroke testing implementation for the right reasons. Research Triangle Park, NC 27709, U.S.A. ISA - Instrumentation, Systems, and Automation Society.

[12] McCrea-Steele, R. (2006). Partial stroke testing – the good, the bad and the ugly. In *7th International Symposium on Programmable Electronic Systems in Safety Related Applications*, Cologne, Germany.

[13] OREDA (1997). *OREDA Reliability Data* (3rd ed.). Available from: Det Norske Veritas, NO 1322 Høvik, Norway: OREDA Participants.

[14] OREDA (2002). *OREDA Reliability Data* (4rd ed.). Available from: Det Norske Veritas, NO 1322 Høvik, Norway: OREDA Participants.

[15] Rausand, M. & Høyland, A. (2004). *System Reliability Theory; Models, Statistical Methods and Applications* (2nd. ed.). New York: Wiley.

[16] Sintef (2006a). *Reliability data for safety instrumented systems – PDS Data Handbook*. Trondheim, Norway: SINTEF.

[17] Sintef (2006b). *Reliability prediction methods for safety instrumented systems – PDS Method Handbook*. Trondheim, Norway: SINTEF.

[18] Smith, D. J. & Simpson, K. G. L. (2005). *Functional safety – A straightforward guide to applying the IEC 61508 and related standards*. Burlington, U.K.: Elsevier.

[19] Summers, A. & Zachary, B. (2000). Partial-stroke testing of safety block valves. *Control Engineering*, *47*(12), 87–89.

[20] Van Beurden, I. & Amkreutz, R. (2001). The effect of partial valve stroke testing on SIL level. Technical report, http://www.exida.com/company/articles.asp.

[21] Velten-Philipp, W. & Houtermans, M. J. (2006). The effect of diagnostic and periodic proof testing on the availability of programmable safety systems. *WSEAS Transactions on Systems*, *5*(8), 1861–1867.