Partial stroke tests as a procedure for the extension of the proof test interval

J. BÖRCSÖK[1, 2], D. MACHMUR[2]

HIMA Paul Hildebrandt GmbH + Co KG [1]
Albert-Bassermann-Str. 28
Bruehl, Germany
http://www.hima.com

University of Kassel [2]
Department of Computer Architecture and System Programming
Wilhelmshoeher Allee 73
Kassel, Germany
http://www.rs.eecs.uni-kassel.de

Abstract: This paper describes a procedure to reduce the probability of failure on demand (*PFD*) for systems and to extend the proof test interval by using partial stroke test (PST). The goal of partial stroke tests is to discover a part of the dangerous undetected failures at an earlier time. The difference between a partial stroke test and a proof test (PT) is that a component is only partially tested by a PST. However, after carrying out a PST, the system has a residual of dangerous undetected failures. This residual can be eliminated by a proof test. The probability of failure can be improved with the diagnostic coverage factor for partial stroke tests. It is important to know the difference between probability of failure *PFD* and the average probability of failure *PFD*$_{avg}$. The values of both *PFDs* with partial stroke test are lower than the probability of failure without partial stroke test. The factor *B* shows the improvement between a system with and without partial stroke tests at the time of the proof test. The larger the factor *B* is the larger is the system's improvement.

Key-words: IEC/EN 61508, SIS, failure rates, *PFD*, proof test, partial stroke test, system improvement, extension of PTI

1 Safety Instrumented Systems

A safety instrumented system (SIS) consists of a sensor, a logic unit and an actuator. With these three components a lot of different architectures can be created.

The *PFD* (probability of failure on demand) is the probability that a system fails in a time in which it is needed. The smaller the *PFD* value is the better the system becomes. In order to calculate the *PFD* value of a system, only the dangerous failures are important. The system goes into the fault state, if a dangerous failure is not discovered. Safe failures and dangerous detected failures do not harm the system and so the system goes into the safe state.

A periodical manual test can reduce the maximum of allowed dangerous failures of a SIS. This test-mode is called proof test (PT). According to the international standard IEC 61508, part 4, a proof test is defined as a fully executed proof-test. The definition according to IEC 61508 is [5]:

"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".

2 Failure rates of proof tests

To calculate the failure rate, the safe failures λ_S and dangerous failures λ_D have to be analyzed. The basis failure rate λ_B is the sum of both failure rates. The safe failure rate λ_S is divided into the safe detected failure rate λ_{SD} and the safe undetected failure rate λ_{SU}. Both safe failures do not harm the system. The dangerous failure value λ_D can lead to a safety critical loss. Such dangerous failures are divided into the dangerous detected failure rate λ_{DD} and the dangerous undetected failure rate λ_{DU}. The equations of the different failure rates are shown in Equations 1, 2 and 3

$$\lambda_B = \lambda_S + \lambda_D \tag{1}$$

$$\lambda_S = \lambda_{SD} + \lambda_{SU} \tag{2}$$

$$\lambda_D = \lambda_{DD} + \lambda_{DU} \tag{3}$$

The following conditions describe important details for further calculations. If there exists a system with a complete proof test and there is an online diagnosis, then we get the following failure rates:

- safe failure rate λ_S
- dangerous detected failure rate $\lambda_{DD,\,online}$
- dangerous undetected failure rate $\lambda_{DU,\,PT}$

The dangerous detected failure rate $\lambda_{DD,online}$ is diagnosed over an online diagnostic coverage *DC*$_{online}$ in time interval ranges of milliseconds to seconds [7]. The graphic in Fig. 1 explains the allocation of the failure rates with a full proof test. Dangerous undetected failures $\lambda_{DU,\,PT}$ will be eliminated with a proof test. Afterwards, the system is considered as failure free. It is assumed that all errors are eliminated and the system is considered as "new".

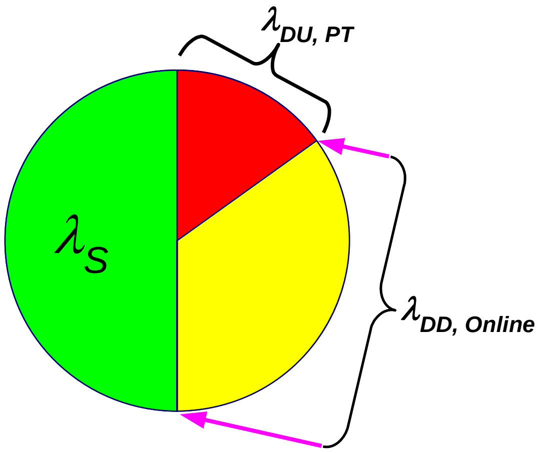

Fig. 1 Allocation of failure rates without PST

As shown in Fig. 1 the dangerous failures are:

$$\lambda_D = \lambda_{DU} + \lambda_{DD} = \lambda_{DU,\,PT} + \lambda_{DD,online} \quad (4)$$

$$\lambda_{DD,online} = DC_{online} \cdot \lambda_D \quad (5)$$

$$\lambda_{DU,PT} = (1 - DC_{online}) \cdot \lambda_D \quad (6)$$

It is widely accepted that the DC_{online} factor has a value larger than 99 % [4].

3 Failure rates with partial stroke test

The difference between a partial stroke test (PST) and a PT is that PST examines a component only partially. A PST detects a smaller part of dangerous undetected failures but earlier in comparison to a PT. However, after carrying out a PST, the system has a residual of dangerous undetected failures. This residual can be eliminated by a PT.

For dangerous failure rates the following notations are selected:

- safe failure rate λ_S (is the same safe failure rates like a proof test)
- online test detected failure rate $\lambda_{DD,\,Online}$
- partial stroke test detected “dangerous undetected” failure rates $\lambda_{DD,PST}$ and
- only by a proof test eliminated dangerous undetected failure rates $\lambda_{DU,PT-PST}$

Fig. 2 shows the allocation of failure rates for a partial stroke test in comparison to a proof test. After a PST, the system is not considered “as new”. So, the system is not error free, because no complete proof test is accomplished.

The following equations describe the failure rates of partial stroke tests according to Fig. 2.

$$\lambda_D = \lambda_{DU,\,PT-PST} + \lambda_{DD,\,PST} + \lambda_{DD,\,online} \quad (7)$$

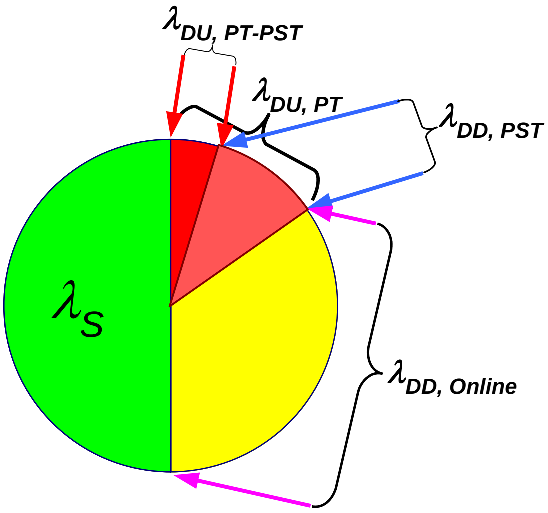

Fig. 2 Allocation of failure rates with PST

$\lambda_{DD,online}$ is equal to a system with PT without PST

$$\lambda_{DD,online} = DC_{online} \cdot \lambda_D \quad (8)$$

and for a system with PST

$$\lambda_{DU} = \lambda_{DD,\,PST} + \lambda_{DU,\,PT-PST} \quad (9)$$

with

$$\lambda_{DD,PST} = DC_{PST} \cdot \lambda_{DU} \quad and \quad \lambda_{DD,PT-PST} = (1 - DC_{PST}) \cdot \lambda_{DU} \quad (10)$$

The diagnostic coverage factor of a PST, called DC_{PST}, is the ratio of $\lambda_{DD,PST}$ and λ_{DU}. The relationship between the dangerous undetected failure rates in a system with and without PST is given in Equation 11 below.

$$\lambda_{DU,\,PT} = \lambda_{DU,\,PT-PST} + \lambda_{DD,\,PST} \quad (11)$$

And with Equation 6, it results in

$$(1 - DC_{online}) \cdot \lambda_D = \lambda_{DU,\,PT-PST} + \lambda_{DD,\,PST} \quad (12)$$

Without online diagnostic the Equation 12 can be simplified to:

$$\lambda_D = \lambda_{DU,\,PT-PST} + \lambda_{DD,\,PST} \quad (13)$$

4 PFD calculation for a 1oo1 system with and without PST

4.1 1oo1 system without partial stroke test

If an exponential distribution of failures is assumed, then the failure rate λ is constant related to the time *t*. The Reliability *R(t)* is the probability that a component identifies its demand for a predefined time.

$$R(t) = e^{-\lambda \cdot t} \quad (14)$$

The probability of failure *P(t)* is given by Equation 15.

$$P(t) = 1 - R(t) = 1 - e^{-\lambda \cdot t} \qquad (15)$$

With this approximation of:

$$\lambda \cdot t << 1 \qquad (16)$$

The probability of failure *P(t)* is:

$$P(t) = \lambda \cdot t \qquad (17)$$

In a safety related system, the probability of failure on demand (*PFD*) is an important safety parameter. It is defined in the international standard IEC 61508. With Equation 15, the *PFD* value can be determined as:

$$PFD(t) = 1 - e^{-\lambda \cdot t} \qquad (18)$$

This equation calculates the exact probability of failure under the condition that the failure rate is constant [6]. System aging and wear out is not considered.

Next, the approximation of $\lambda \cdot t << 1$ is used to obtain the PFD value, as presented below.

$$P(t) = \lambda \cdot t \qquad (19)$$

The average probability of failure on demand PFD_{avg} is given with approximation of $\lambda \cdot t << 1$ [1, 4, 5]:

$$PFD_{avg}(t = T_{PT}) = \frac{1}{2} \cdot \lambda \cdot T_{PT} \qquad (20)$$

The proof test is executed at the time $t = t_{PT}$. Only the dangerous failures λ_D are relevant for the *PFD* calculation. $\lambda_{DD,online}$ and $\lambda_{DU,PT}$ are defined according to the international standard IEC 61508 as follow [5]:

- the dangerous detected failures $\lambda_{DD,online}$ are detected with the online diagnostic
- the dangerous undetected failures $\lambda_{DU,PT}$ are detected after a PT

Taking these conditions into account, Equations 19 and 20 are changing to Equation 21 and 22.

$$PFD(t) = (\lambda_{DD,online} + \lambda_{DU,PT}) \cdot t \qquad (21)$$

and

$$PFD_{avg}(T_{PT}) = \frac{1}{2} \cdot (\lambda_{DD,online} + \lambda_{DU,PT}) \cdot T_{PT} \qquad (22)$$

As shown, the advantage of a system with PST compared to a system without PST is that the online diagnostic is negligible. To simplify the equations above the online diagnostic is not considered anymore and Equations 19 and 20 become:

$$PFD(t) = \lambda_{DU,PT} \cdot t \qquad (23)$$

and

$$PFD_{avg}(T_{PT}) = \frac{1}{2} \cdot \lambda_{DU,PT} \cdot T_{PT} \qquad (24)$$

Table 1 *PFD* without partial stroke test

t in h	0	4380	8760	13,140
***PFD*(t) without PST**	0.00E+00	1.31E-04	2.63E-04	3.94E-04

t in h	17,520	21,900	26,280
***PFD*(t) without PST**	5.26E-04	6.57E-04	7.88E-04

Table 2 PFD_{avg} without partial stroke test

t in h	0 to 26,280
***PFD*(t) without PST**	3.94E-04

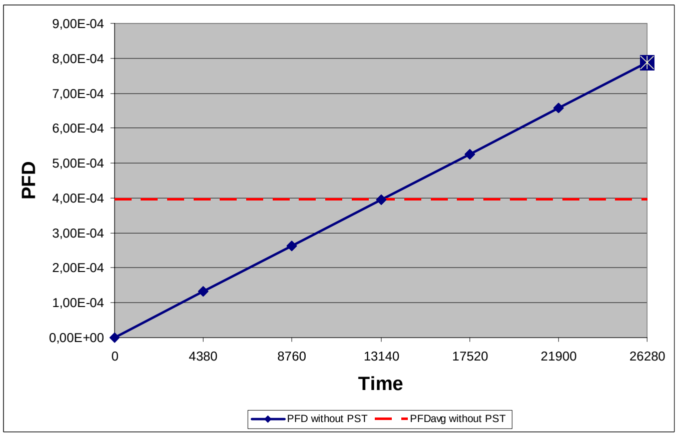

Fig. 3 *PFD* (full-line) and *PFDavg* (dashed line) without partial stroke test.

4.1.1 Application set-up for the calculation of PFD and PFDavg

A 1oo1 system is assumed which has a dangerous failure rate of:

$$\lambda_D = \lambda_{DU,PT} = 3 \cdot 10^{-8} \, \frac{1}{h} \qquad (25)$$

This assumption is the same for all calculations:

- there is no online diagnostic
- the dangerous failure rate is equal to the dangerous undetected failure rate

For the proof test interval it is assumed that $T_{PT} = 3 \; years$.

With Equations 23 and 24 the probability of failure *PFD* and the average probability of failure PFD_{avg} over the time $t = 0$ to $t = T_{PT} = 3$ years is shown in Table 1 and Table 2. The table shows that over time *t* the PFD_{avg} value is constant. The results are shown in Fig. 3. Table 2 shows the results of PFD_{avg}.

4.2 1oo1 system with partial stroke test

PST is an incomplete proof test. With a PST compared to PT one only discovers a small part of dangerous undetected failures. Equation 26 shows the PFD value without PST ($PFD_{wo.PST}$).

$$PFD_{wo.\,PST}(t) = \lambda_D \cdot t = \lambda_{DU,PT} \cdot t \qquad (26)$$

A *PFD* value for a system with partial stroke tests ($PFD_{w.PST}$) possesses a part of dangerous detected failures

$\lambda_{DD,PST}$ and a part of dangerous undetected failures $\lambda_{DU,PT-PST}$.

$$PFD_{w.\,PST}(t) = \lambda_{DD,\,PST}\cdot t_A + \lambda_{DU,\,PT-PST}\cdot t_B \qquad (27)$$

The time t_A is the time between 0 and the first PST (t_{1stPST}). The time t_B is the time between 0 and the first proof test t_{PT}. If one has a periodical partial stroke test after given time, then Equation 27 is a function of t_{1stPST} and t.

$$\begin{aligned} PFD_{w.\,PST}(t) &= f(t_{1st\,PST}, t) \\ &= \lambda_{DD,\,PST}\cdot t_{1st\,PST} + \lambda_{DU,\,PT-PST}\cdot t \end{aligned} \qquad (28)$$

Equation 28 consists of two linear functions. The first function defined on the time interval [*0. . . t_{1stPST}*] and the second function on the time interval [*0. . . t*].

The following assumptions are considered: The first partial stroke test is accomplished at the time $t_{1stPST} = T_{1stPST}$. The proof test is executed much later than the first PST. Therefore, the first part of Equation 28 becomes constant and the second is a linear function of the time *t*. The *PFD* value of a PST at time T_{1stPST} is shown in Equation 29.

$$\begin{aligned} PFD_{w.\,PST}(t_{1.PST}) = {} & PFD_{DD,\,PST}(T_{1stPST}, \lambda_{DD,\,PST}) \\ & + PFD_{DU,\,PT-PST}(t, \lambda_{DU,\,PT-PST}) \end{aligned} \qquad (29)$$

The *PFD* value for the first PST consists of $PFD_{DD,PST}$ and $PFD_{DU,PT-PST}$. $PFD_{DD,PST}$ is the probability of failure of the failure rate $\lambda_{DD,PST}$ and the time t_{1stPST}. Such failures are detected by a partial stroke test and estimate the value for the $PFD_{DD,PST}$. The second term $PFD_{DU,PT-PST}$ gives the probability of failure for the failure rate $\lambda_{DU,PT-PST}$ at the time *t*. The failures $\lambda_{DU,PT-PST}$ are only detected after a PT. To get the value $PFD_{DU,PT-PST}$ for the first PST one has to accomplish an imaginary proof test at the time $t = t_{1stPST}$. With the diagnostic coverage factor DC_{PST} and Equations 28, it results in

$$PFD_{w.\,PST}(t) = \lambda_{DU}\cdot[DC_{PST}\cdot t_{1st\,PST} + (1-DC_{PST})\cdot t] \quad (30)$$

Table 3 PFD with and without partial stroke test

t in h	0	8760	after PST 8760	17,520
***PFD*(t) without PST**	0.00E+00	6.13E-04	--------------	1.23E-03
***PFD*(t) with PST**	0.00E+00	6.13E-04	2.45E-04	8.58E-04

t in h	after PST 17,520	26,280
***PFD*(t) without PST**	------------	1.84E-03
***PFD*(t) with PST**	4.91E-04	1.10E-03

With a PST only dangerous detected failures can be identified. Dangerous undetected failures are only detectable with a PT [1, 4]. After a PST a residual failure rate remains, which can only be detected by a PT and therefore the probability of failure after a PST ($PFD_{a.PST}$) is equal to $PFD_{DU,PT-PST}$.

$$\begin{aligned} PFD_{a.\,PST}(t) &= PFD_{DU,\,PT-PST} \\ &= (1-DC_{PST})\cdot\lambda_{DU}\cdot t \end{aligned} \qquad (31)$$

4.2.1 Application set-up for the calculation

A 1oo1 system is assumed with the same dangerous detected failure rate as in the previous case. The proof test interval is T_{PT} = 3 years and the partial stroke test interval is T_{1stPST} = 1 year. The diagnostic coverage factor for the PST is DC_{PST} = 60%. The *PFD* with PST is calculated by Equation 30 and the *PFD* after PST is calculated by Equation 31. The *PFD* values are shown in Table 3.

Fig. 4 shows the *PFD* value with PST (line 2) and without a PST (line 0). The PFD values of the characteristic line without PST are represented in Table 1. Up to the first PST, the *PFD* values are equal. After the first PST, the lines differ, because a system with partial stroke tests possesses a residual probability of failure $PFD_{a.PST}$. After three years a complete proof test is carried out and the system is regarded as “new”.

The advantage of a system with PST compared with a system without PST is the reduction of the probability of failure on demand. The reduction is marked in Fig. 4 with the parameter *B*.

The Factor *B* is the difference between the *PFD* values with and without PST at the time $t = t_{PT}$. Factor *B* can be calculated with Equation 26, 30 and $t = t_{PT}$:

$$\begin{aligned} B(t = T_{PT}) &= PFD_{wo.\,PST}(t = t_{PT}) - PFD_{w.\,PST}(t = t_{PT}) \\ &= \lambda_D\cdot DC_{PST}\cdot(t_{PT} - t_{1st\,PST}) \end{aligned} \qquad (32)$$

Assuming factor B, first PST $t = t_{1stPST}$ and the proof test interval $t = t_{PT}$ are given, then the DC_{PST} value can be calculated by reorganizing Equation 32:

$$DC_{PST} = \frac{B(t)}{\lambda_D\cdot(t_{PT} - t_{1st\,PST})} \qquad (33)$$

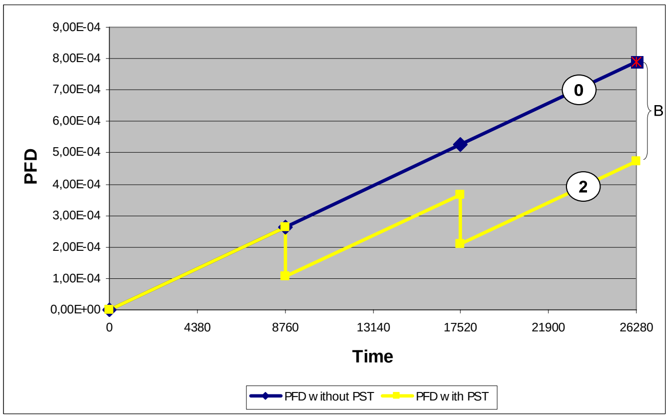

Fig. 4 *PFD* without and with partial stroke test

5 Partial stroke test and proof test

As mentioned a system with partial stroke test (PST) the dangerous undetected failure rate consists of two terms: a failure rate $\lambda_{DD,PST}$ which is detected by a PST and a failure rate $\lambda_{DU,PT-PST}$ which is detected only through a proof test (PT) [Börcsök & Machmur 2007]:

$$\lambda_{DU} = \lambda_{DD,PST} + \lambda_{DU,PT-PST} \qquad (34)$$

with

$$\begin{aligned} &\lambda_{DD,PST} = DC_{PST} \cdot \lambda_{DU} \quad and \\ &\lambda_{DD,PT-PST} = (1 - DC_{PST}) \cdot \lambda_{DU} \end{aligned} \qquad (35)$$

The diagnostic coverage factor of a PST, called DC_{PST} , is the ratio of $\lambda_{DD,PST}$ and λ_{DU}. The objective of a system with PST compared with a system without a PST is to reduce the probability of failure.

In an application set-up the PST is executed every 6 months and the proof test interval is set to three years. In order to observe how the *PFD* values are changing, the PST interval is set to 12 and 18 months to compare the three PSTs. The following graphs show the PST intervals t_{1stPST} of 4380 and/or 13140 hours.

For the calculations below, a 1oo1 system is assumed which has a dangerous failure rate:

$$\lambda_D = \lambda_{DU,PT} = 3 \cdot 10^{-8} \frac{1}{h}$$

No online diagnostic is implemented and the dangerous failure rate is equal to the dangerous undetected failure rate. The proof test interval ist set to $t_{PT} = 3$ years and the diagnostic coverage factor DC_{PST} to 60 %.

5.1 1oo1 system with partial stroke test, PFD$_{w.PST}$

In the following, the probability of failure $PFD_{w.PST}$ is tested by different PST intervals.

5.1.1 First PST after 4380 hours

The *PFD* value for the first PST consists of $PFD_{DD,PST}$ and $PFD_{DU,PT-PST}$. $PFD_{DD,PST}$ is the probability of failure of the failure rate $\lambda_{DD,PST}$ and the time t_{1stPST}. Such failures are detected by a PST and estimate the value for the $PFD_{DD,PST}$. The second term $PFD_{DU,PT-PST}$ gives the probability of failure for the failure rate $\lambda_{DU,PT-PST}$ at the time *t*. The failures $\lambda_{DU,PT-PST}$ are only detected after a PT. To get the value $PFD_{DU,PT-PST}$ for the first PST one has to accomplish an imaginary proof test at time $t = t_{1stPST}$. With the diagnostic coverage factor DC_{PST}, it results in:

$$\begin{aligned} PFD_{w.\,PST}(t) &= f(t_{1st\ PST}, t) \\ &= \lambda_{DD,\,PST} \cdot t_{1st\ PST} + \lambda_{DU,\,PT-PST} \cdot t \end{aligned} \qquad (36)$$

After a PST is carried out Equation 37 becomes valid for the residual dangerous undetected failures.

$$\begin{aligned} PFD_{a.\,PST}(t) &= PFD_{DU,\,PT-PST} \\ &= (1 - DC_{PST}) \cdot \lambda_{DU} \cdot t \end{aligned} \qquad (37)$$

The derivation of these equations can be found in [2, 3]. The probability of failure *PFD* for a system with and without a PST from the time $t = 0$ to $t = t_{PT} = 3$ years is shown in Table 4.

Fig. 5 shows the *PFD* values with (line 1) and without a partial stroke test (line 0). Up to the first PST the *PFD* values are identical. After the first PST, the lines differ, because a system with partial stroke test possesses only a residual probability of failure, $PFD_{a.PST}$. After three years a complete proof test is accomplished and the system is regarded as “new”.

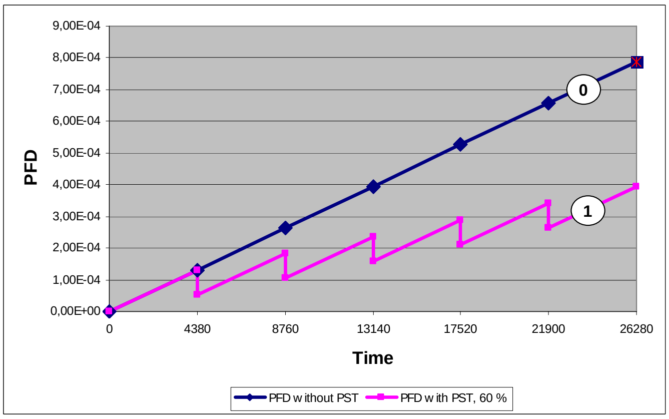

Fig. 5 *PFD* with and without a PST every six months with a proof test interval of three years.

Table 4 PFD with and without partial stroke test

t in h	0	4380	after PST 4380	8760
***PFD* without PST**	0.00E+00	1.31E-04	--------------	2.63E-04
***PFD* with PST**	0.00E+00	1.31E-04	5.36E-04	1.84E-04

t in h	after PST 8760	13,140	after PST 13,140	17,520
***PFD* without PST**	------------	3.94E-04	--------------	5.26E-04
***PFD* with PST**	1.05E-04	2.37E-04	1.58E-04	2.89E-04

t in h	after PST 17,520	21,900	after PST 21,900	26,280
***PFD* without PST**	------------	6.57E-04	--------------	7.88E-04
***PFD* with PST**	2.10E-04	3.42E-04	2.63E-04	3.94E-04

5.1.2 First PST after 13,140 hours

The probability of failure *PFD* for a system with and without a PST after 13,140 hours is shown in Table 5 below. All other conditions are the same.

Fig. 6 shows the *PFD* values with (line 3) and without a partial stroke test (line 0). Again, up to the first PST the *PFD* values are identical. After the first PST the characteristic lines differ, because a system with partial stroke test possesses only residual probability of failure $PFD_{a.PST}$.

5.1.3 PFD comparison between different PST intervals of 4380, 8760 and 13,140 hours

The *PFD* value for a proof test after three years with a PST every six months is smaller than the *PFD* value for the same proof test interval with a PST every twelve or eighteen months. Table 6 and Fig. 7 show this.

Now, the *PFD* values for different PST intervals at the time of the proof test (here: after three years) are going to be compared. Table 7 shows the *PFD* values. Fig. 8 shows the three PFD values for different PST intervals. All *PFD* values are in SIL 3 level.

Table 5 PFD with and without partial stroke test

t in h	0	13,140	after PST 13,140	26,280
***PFD* without PST**	0.00E+00	3.94E-04	--------------	7.88E-04
***PFD* with PST**	0.00E+00	3.94E-04	1.58E-04	5.52E-04

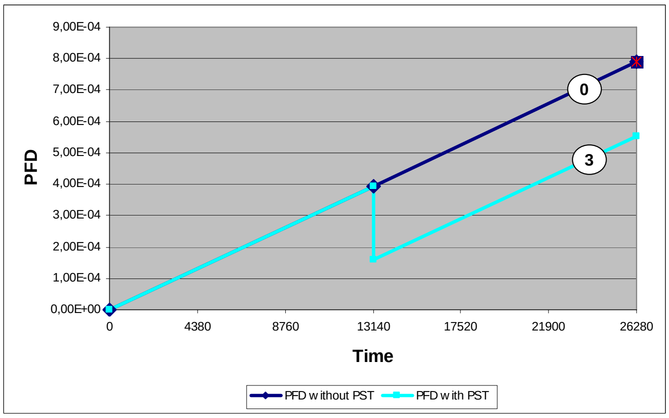

Fig. 6 *PFD* with and without a PST every 18 months with a proof test interval of three years

5.2 Extension of the PT interval

PFD values for systems with partial stroke tests are smaller than systems without PST. So it is possible to extend the proof test interval by using the PST from three to five years, with the same application set-up. Fig 9 shows the *PFD* values for a proof test at three (full line) and five years (dashed line). The *PFD* value for the proof test after five years has to be reduced, so that the *PFD* value of the PT interval of five years is within the SIL 3 level. In order to achieve this, a partial stroke test is accomplished (vertical line) for example every 12 months as shown in Fig. 9.

Fig. 10 shows the results for a selected PST interval of 1 year and a PT interval of 5 years. The *PFD* value for 5 years is clearly within the SIL 3 level. The *PFD* value is reduced and SIL 3 level is achieved. Finally, the proof test interval is extended from 3 to 5 years.

Table 6 *PFD* with and without partial stroke test for several PSTs

t in h	0	4380	after PST 4380	8760	after PST 8760	13,140	after PST 13,140	17,520	after PST 17,520	21,900	after PST 21,900	26,280
***PFD* without PST**	0.00E+00	1.31E-04	--------------	2.63E-04	------------	3.94E-04	--------------	5.26E-04	------------	6.57E-04	--------------	7.88E-04
***PFD* with PST=4380 h**	0.00E+00	1.31E-04	5.26E-05	1.84E-04	1.05E-04	2.37E-04	1.58E-04	2.89E-04	2.10E-04	3.42E-04	2.63E-04	3.94E-04
***PFD* with PST=8760 h**	0.00E+00	------------	------------	2.63E-04	1.05E-04	------------	------------	3.68E-04	2.10E-04	------------	------------	4.73E-04
***PFD* w. PST=13140 h**	0.00E+00	------------	------------	------------	------------	3.94E-04	1.58E-04	-----------	------------	------------	------------	5.52E-04

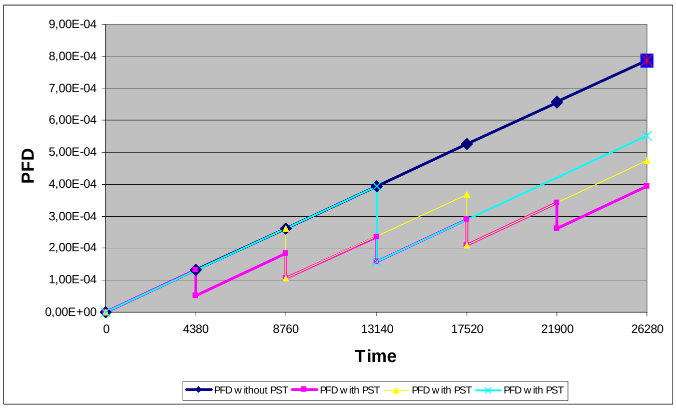

Fig. 7 Comparison of PST for every 6, 12, 18 months with a proof test interval of three years

6 Conclusions

Risk reduction of a Safety Integrity Function is determined by using the average probability of failure (PFD_{avg}). The most common method to classify a SIF is done by estimating the Safety Integrity Level (SIL), based on the standard IEC 61508.

A proof test is a repeated inspection of safety related systems to detect failures in the system. After suitable procedures are carried out, the system is considered as “new”.

In some cases, proof testing can reduce the total operation costs caused by a required SIF. But it has to be mentioned that the costs of carried out proof tests might balance the cost advantage. To execute proof tests it is not always easy and in practice it is not always possible to do complete repair after a failure occurred.

Table 7 PFD with and without partial stroke test at the time of the proof test

t in h	**26,280**
***PFD* without PST**	7.88E-04
***PFD* with PST=4380 h**	3.94E-04
***PFD* with PST=8760 h**	4.73E-04
***PFD* w. PST=13,140 h**	5.52E-04

The theoretical research is nearly completed for a 1oo1-system and will be examined on practical and industrial systems but currently field data are not available.

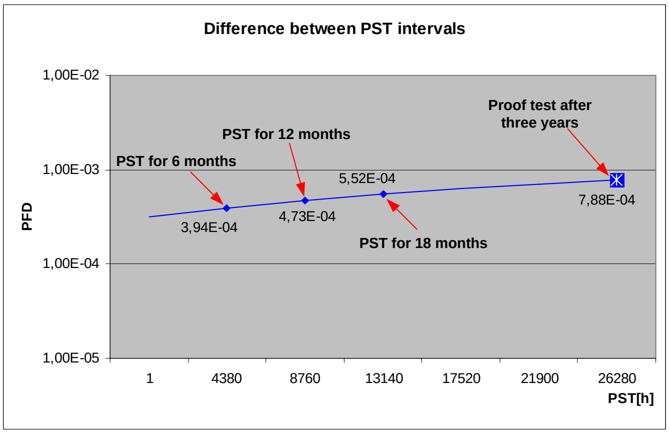

Fig. 8 *PFD* maximum for PST every 6, 12 and 18 months

Therefore, partial stroke tests are a good possibility to reduce the probability of failure. The paper demonstrates that a system with partial stroke tests provides a smaller probability of failures in comparison to a system without PST. Additionally, the proof test interval can be extended if partial stroke tests are carried out. The extended interval depends on the selected DC_{PST} factor and the point in time of the first partial stroke test.

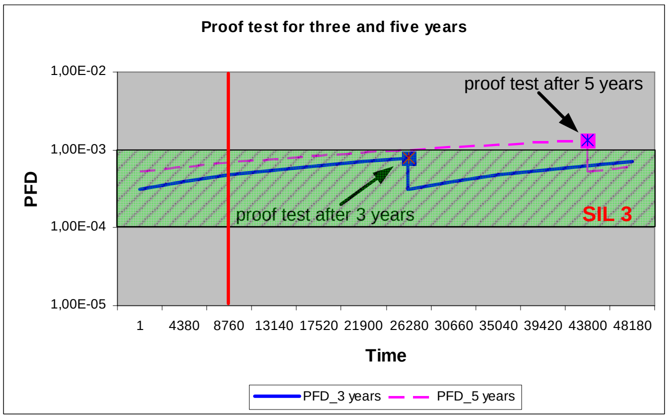

Fig. 9 *PFD* values for a proof test after 3 and 5 years

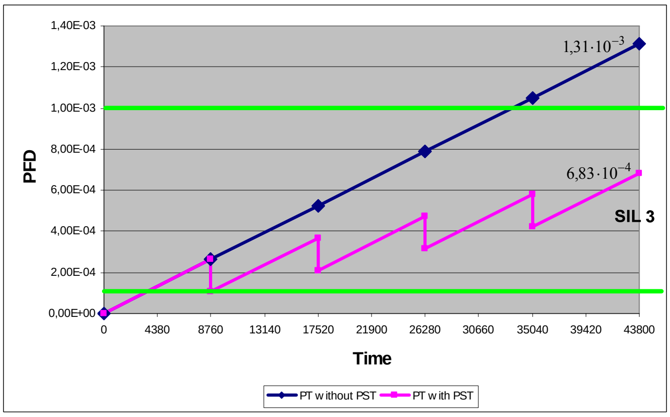

Fig. 10 Proof test for 5 years with PST every 12 months

References:

[1] Börcsök, J. 2007. *Functional safety systems*. Hüthig Verlag.

[2] Börcsök J., Machmur D. 2007. Influence of partial stroke tests and diagnostic measures of the proof test interval. Safety and Reliability for Managing Risk, Safety and Reliability Conference - ESREL2007, ESRA: Stavanger, Norway.

[3] Börcsök J., Machmur D. 2007. Examination of repetitive proof test for safety related systems. Safety and Reliability for Managing Risk, Safety and Reliability Conference - ESREL2007, ESRA: Stavanger, Norway.

[4] Börcsök J. 2004. Electronic safety systems. Heidelberg: Hüthig.

[5] IEC/EN 61508. 2000. Internat. standard 61508 functional safety: Safety-related System, Inter.Elec.Com. Geneva.

[6] Lewis, E. 1996. *Introduction to reliability engineering.* 2nd edition. New York: John Wiley

[7] Goble W.M. 1995. Safety of programmable electronic systems – Critical Issues, Diagnostic and Common Cause Strength In Proceedings of the IchemE Symposium, Rugby.