# Procedures for updating test intervals based on experience data

Jørn Vatn
Department of Production and Quality Engineering, NTNU
S.P Andersens v. 5
7491 Trondheim, Trondheim

***Abstract***

*The paper presents procedures for updating intervals for functional tests of safety instrumented systems (SIS). The background situation is that during design and engineering of SISs, reliability assessment is made in order to verify that the required safety integrity level (SIL) has been met. However, in these early phases of the SIS development we have to base the calculation of probability of failure on demand (PFD) on generic reliability data which does not necessarily reflect the reliability performance of the new equipment. A procedure is therefore proposed for how to update the PFD calculations based on new experience data as they become available during real operation of the actual SIS. This also enables a process where maintenance intervals can be updated. The procedure utilises a Bayesian-like updating process, where the generic data for failure rates is used as a prior distribution, and real failure data is used to update to a posterior distribution. The procedure also allows for a pre-processing of the failure data in situations where experienced failures are believed to be eliminated by implementation of new risk reducing measures after a proper root cause analysis. In order to capture negative trends as the equipment deteriorates, a Nelson Aalen plot is used for visualisation of the cumulative number of failures. Such a plot is very easy to construct, and enables recognition of negative trends. The calculations are supported by a simple EXCEL spread sheet.*

*Keywords: SIL, PFD, Bayesian methods, test intervals*

## 1. Introduction

### 1.1 Background

Collection and analysis of reliability data is an important part of the maintenance management on an installation. For a new installation only generic reliability parameters are available (e.g. from OREDA (2002) or PDS data, see Hauge et.al 2006b). By proper collection and analysis of the reliability data for a given site, it is possible to establish site specific reliability parameters, and thus establish a maintenance program that is adapted to the actual reliability performance of that site. Further collection and analysis is an important means to ensure reliability growth during the lifecycle of an installation. By proper collection and analysis of failure causes, it is possible to eliminate systematic failures by implementing measures

against these failure causes. On the other hand, if this systematic approach fails it is likely that reliability performance is impaired to an unacceptable level.

Oljeindustriens Landsforening (OLF) in Norway has issued a guideline for the application of IEC 61508 and IEC 61511 in the petroleum activities on the continental shelf (OLF 070). In appendix F of this guideline a method for updating intervals for functional tests of safety instrumented systems (SIS) is presented. This paper presents a slightly more comprehensive approach than the OLF approach.

### 1.2 Outline of the proposed methodology

The objective of the methodology is to ensure a consistent way to determine maintenance intervals for safety instrumented systems. Different approaches exist for establishing maintenance intervals. Often we try to specify some object function to optimise. Such an object function comprises different cost elements, such as the cost of preventive maintenance, the cost of failures, the cost of accidents etc. A challenge in such an approach is to be explicit about safety costs, which is a controversial issue. Another approach would be to specify some target value for the safety performance of the SIS. The relevant safety performance measure is the probability of failure on demand (PFD), at least when so-called low demand systems are considered (see IEC 61508).

We assume that there exist target values for the PFD for the SIS under consideration. The PFD will be linked to the safety integrity level (SIL) which is established during the specification of the SIS in order to achieve a necessary risk reduction, see IEC 61508. It should also be mentioned that the SIL is specified for the entire system, i.e. the input devices, the control logic unit, and the final element. In principle different maintenance intervals are applied for these three "subsystems". Therefore, the proposed methodology assumes that separate target values are specified for the PFD. The target value to be used in the determination of maintenance intervals is denoted $\text{PFD}^T$.

The calculation of the PFD for a given subsystem is here assumed to be straight-forward. Different principles exist, and we have adopted the PDS approach, see Hauge et al. (2006a). Input to the PFD calculation formulas are the failure rate, the common cause factor, the length of the test interval, and the configuration. The uncertain reliability parameters are the failure rate and the common cause factor. In this paper we primarily discuss the assessment of the failure rate. Initially, when no failure data exists for the SIS under consideration, we have to base the failure rate assessment on data from other systems, or identical implementations in another context. To qualify the reliability parameters for the current SIS it is recommended to analyse the experienced failure causes, and make relative judgements. For example, if one failure cause has been eliminated in the design of the new SIS, we could reduce the failure rate estimate, at least to some extent. A structured procedure to such a qualification is proposed in the following. According to IEC 61508 we should apply so-called 70% uncertainty estimates. This will require that we specify some uncertainty distribution of the failure rate. To do this, a Bayesian approach is suggested. In the specification of the initial maintenance program, we thus apply the upper 30% percentile in the uncertainty distribution of the failure rate. This failure

rate is then used to optimise the maintenance interval, which here means to maximise the interval as long as the target PFD value is not exceeded.

In the operating phase of the installation we expect to get site specific reliability data. This data is used to update the (prior) failure rate distribution. Again, the upper 30% percentile of the (posterior) distribution is used in the optimisation of the maintenance interval. An important aspect of the methodology is that we should not simply repair failures, but rather analyse the situation in order to find the root causes and eliminate them. If we are able to mitigate some of the failure causes, we could also expect the system to perform better in the future. The proposed methodology gives a structure approach to treat the effect of improvement measures.

## 2. Theoretical background

### 2.1 Failure rate considerations

In this presentation focus is on dangerous undetected failures, i.e. so-called DU failures according to IEC 61508. The DU failures are failures of a component that fail to operate upon on demand, and where the transition from a functioning state to a failed state is undetected. The time to failure is assumed to be exponentially distributed with parameter $\lambda_{DU}$, where $\lambda_{DU}$ is an unknown parameter. The interpretation of parameters is often debated (see e.g., Aven, 2003) . Our position in such a debate is that a parameter is a construct we utilise in order to give probability statement about observables in the real world. The observables here are the failure times, say $T_i$. Given the value of the parameter, $\lambda_{DU,}$ we may e.g. assume that the $T_i$'s are exponentially distributed with this parameter. By observing the system, e.g. recording time to failures of relevant components, we estimate the unknown parameter, e.g. by Bayesian methods. Since $\lambda_{DU}$ is a construct it may seem strange to estimate such a construct, and it becomes even more challenging to define what is meant by uncertainty of a construct. The idea is simply that we could imagine a value of $\lambda_{DU}$ which will have no uncertainty if we observe the world long enough. Since we have not observed the world there is uncertainty in $\lambda_{DU}$, and the uncertainty is related to what will be the value in the long run.

### 2.2 Bayesian methods

Although the philosophy behind Bayesian methods is demanding, the application of Bayesian methods is usually straight forward, see e.g., Martz and Waller (1982) for methods and techniques. Based on our knowledge, experience and explicit analysis of reliability data, we may state our belief about reliability parameters. We do that in terms of probability statements. These probabilities are, however, not a property of the "nature", but a measure of our knowledge about the system under consideration. We use the notation of $\boldsymbol{\theta}$ as the (vector) of reliability parameters of interest. The Bayesian approach comprised four basic steps:

1. Specification of a *prior* uncertainty distribution of the reliability parameter, $\pi(\boldsymbol{\theta})$.
2. Structuring reliability data information ($\mathbf{t}$) into a likelihood function, $L(\boldsymbol{\theta};\mathbf{t})$.

3. Calculation of the *posterior* uncertainty distribution of the reliability parameter vector, $\pi(\boldsymbol{\theta}|\mathbf{t})$ where . $\pi(|\boldsymbol{\theta}\mathbf{x}) \propto L(\boldsymbol{\theta};\mathbf{x}) \times \pi(\boldsymbol{\theta})$.
4. Choosing the Bayes estimate for the reliability parameter vector, usually the posterior mean.

Often the parametric distribution for the prior is chosen in such a way that it is possible to find the posterior in a known class of distributions. This will be illustrated in section 2.3. The Bayesian updating process is illustrated in **Figure 1**. The idea is that initially a best estimate and a conservative estimate is agreed upon in the analysis group. These two estimates could be based on data from generic reliability data handbooks, and/or judgements from experts. The updating procedure is in principle very schematic, but as we will see in Section 3 judgements will be necessary if mitigating measures are implemented against root causes.

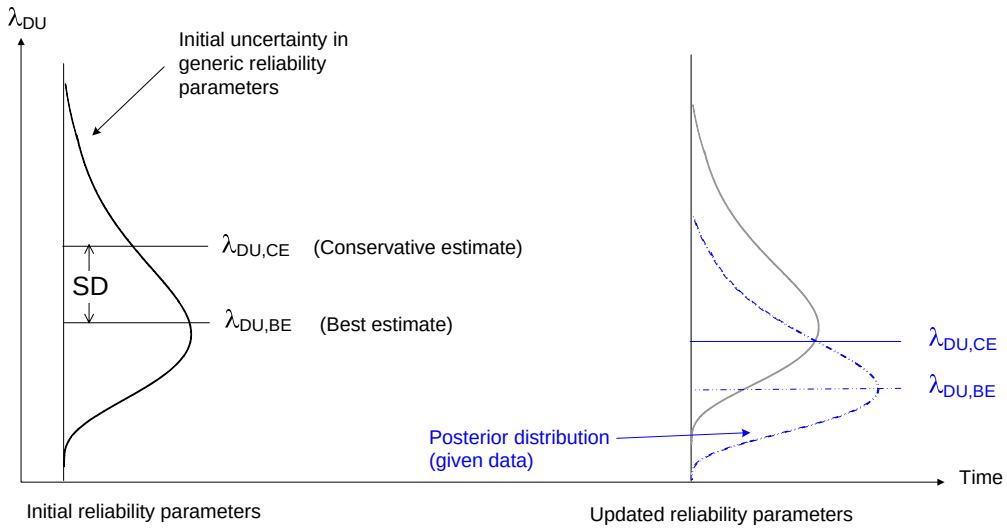


**Figure 1** Bayesian updating

## 2.3 The gamma distribution

In this presentation the Gamma distribution will be used to describe the uncertainty in $\lambda_{DU}$. We treat $\lambda_{DU}$ as a random variable, and use the notation $\Lambda_{DU}$. The parameterisation used is:

$$f_{\Lambda_{DU}}(\lambda_{DU}) = \frac{U_1^{U_2}}{\Gamma(U_2)}(\lambda_{DU})^{U_2-1}e^{-U_1\lambda_{DU}} \qquad (1)$$

where the uncertainty parameter $U_1$ corresponds to a scale parameter, and the uncertainty parameter $U_2$ corresponds to a shape parameter. The reason why we introduce $U_1$ and $U_2$ rather than the more familiar Greek letters is that the expected users of the proposed procedure might find the procedure more unattractive with too many Greek letters.

For the gamma distribution the mean and variance are given by $E(\Lambda_{DU}) = U_2/U_1$, and $\mathrm{Var}(\Lambda_{DU}) = U_2/U_1^2$ respectively. Further, if we know the mean ($E$) and variance ($V$) of

$\Lambda_{DU,}$ we may obtain the corresponding uncertainty parameters by $U_1 = E/V$, and $U_2 = U_1 \times E$.

In the reliability calculations we need to select one value for the failure rate, i.e. a numeric value for $\lambda_{DU}$ is required. The Bayesian approach would be to use the prior or posterior mean of the distribution of $\Lambda_{DU.}$ However, in the IEC 61508 standard Part II, §7.4.7.4a, it is recommended to use a conservative estimate, i.e. a 70% lower percentile in the uncertainty distribution. Now, it is easy to verify that

$$\Pr\left(\Lambda_{DU} < U_2/U_1 + 0.3\sqrt{U_2}/U_1\right) \approx 70\% \tag{2}$$

for reasonable values of $U_{2.}$ Thus, an estimate in line with the IEC 61508 recommendations would be to use $\lambda_{DU} = U_2/U_1 + 0.3\sqrt{U_2}/U_1$, where $U_1$ and $U_2$ are either prior or posterior uncertainty parameters.

The gamma distribution is attractive in a Bayesian setting. Assume that a gamma distribution with parameters $U_1$ and $U_2$ represents the prior knowledge about the rate of DU failures, and $X$ failures in a period of length $t$ have been recorded, then it can be shown (see e.g., Martz and Waller 1982) that the gamma distribution applies for the posterior, and the new parameters are $U_1$(new) = $U_1$(old) + $t$, and $U_2$(new) = $U_2$(old) + $X$. Thus, the Bayesian updating is very simple. At any time we may use the formula $\lambda_{DU} = U_2/U_1 + 0.3\sqrt{U_2}/U_1$ to find a conservative estimate of the failure rate. Note that as more and more data become available the prior distribution will be wiped out, and we remain with $X/t$ as the expression for the rate of DU failures.

### 2.4 PFD calculations

In this presentation we assume that there is some target value, say $\text{PFD}^T$, for which we aim at when our main concern is to determine the maintenance intervals. The probability of failure on demand could in principle be described as a function of the rate of dangerous failures ($\lambda_{DU}$), the common cause factor ($\beta$), the test interval ($\tau$), and the voting ( $M$oo$N$), i.e. we will require:

$$\text{PFD} = \text{PFD}(\lambda_{DU}, \beta, \tau, M, N) \le \text{PFD}^T \tag{3}$$

In the IEC 61508 standard it is proposed to use an ordinary $\beta$-factor model for the PFD calculations. The problem with this approach has been that for any $M$oo$N$ voting the rate of dependent failures is the same, and thus the approach does not distinguish between e.g. a 1 oo 2 and a 2 oo 3 voting. Therefore, the so-called PDS method was developed in order to have a more realistic consideration of dependent failures of a general $M$ oo $N$ voting. The PDS method is described by Hauge et al. (2006a). It is outside the scope of this presentation to give the details for the PFD calculations in the PDS approach. The calculation formulas have been implemented in a simple Excel spreadsheet which could be downloaded from http://www.itk.ntnu.no/sil.

## 2.5 Treating empirical data

Empirical data and evidence will be available at two critical decision points. First when establishing the initial maintenance interval, and next when we get data from the installation to be used to update maintenance intervals. Initially, we do not have reliability data for the system under consideration since it is a new system, or at least on old system installed in a new context. However, there may be some relevant reliability data available, either for the same system, or a similar system. The question then is how to treat such data. A failure mode and effect analysis (FMEA) is often recommended for qualification of new technology (see e.g. the recommended practice for *Qualification Procedures for New Technology*, DNV recommended practice, DNV-RP-A203). Such an FMEA could be used when comparing the new system with existing systems. Essential questions to be answered are:

- Has there been any change in environmental load that will affect the importance of this failure cause compared to existing technology and operating conditions?
- Have there been any changes (improvements) in order to eliminate known failure causes in the new technology?
- Could new failure causes have been introduced?

These questions are taken into consideration when we shall assess formally the rate of DU failures. Assume that a failure rate, $\lambda_{DU}$, is estimated based on the most relevant data we have access to, and further assume that the total estimated failure rate could be split into $n$ different failure causes:

$$\lambda_{DU} = \lambda_1+\lambda_2+\ldots+\lambda_n \tag{4}$$

It is now reasonable to conduct a comparison analysis, where the new system to be implemented is compared with the system(s) for which we have data. The comparison is made on a failure cause level. Each failure cause is analysed systematically with respect to which conditions have been changed from the old system(s) to the new system. Typically some modifications and improvements have been implemented in order to mitigate some of the known failure causes. Thus, if we are quite certain about the effect of the improvement measures we could take credit of this in the failure rate estimate to be used for the new system. In section 3 we have proposed a method for how to adjust the failure rate estimates on the basis of this initial failure cause analysis.

Later, in the updating process, we will benefit from a proper failure cause analysis. The main reason for conducting a failure cause, or root cause analysis, is to eliminate failures that we experience with the new system. Further, if failure causes are analysed and improvements are implemented, it is reasonable to benefit of this, and not "count" all failures in the updating procedure. If we for example record $X = 5$ failures in a reporting period, and believe that two of these failures in the future will not occur because an improvement measure has been implemented, it seems reasonable to use $X = 3$ in the Bayesian updating procedure. A challenging question is, however, can we claim 100% effect of the implemented measures, or could it still be that the same failure occurs again (with a smaller rate of occurrence)? In section 3 a method is proposed for adjusting the number of observed failures in the light of implemented measures.

# 3. Proposed methodology for determination of maintenance intervals

In this section the proposed methodology for determination of maintenance intervals is presented. The theoretical background for the methodology was discussed in section 2, and we therefore give very few arguments. Thus the presentation in the following should be considered more as a guide on what to do, rather than the arguments why to do it.

Generally, a (sub)function is specified, for which it is decided to use an identical test interval of length, $\tau$. Thus, a group of components (e.g. transmitters) is identified, which is also considered identical, (e.g. assuming same failure rate and beta-factor), and has the same voting logic, denoted $M$oo$N$.

It must also be decided how often the test interval is considered for updating. The steps 1- 4 are performed *once* (providing some fundamental input to the updating), the remaining steps are carried out each time a possible update of the test interval is considered.

A common time unit must be specified (hours, days, months, years). Below it is assumed that we use "hours" both for the test interval $\tau$ and the failure rate $\lambda_{DU}$.

**Step 1 Establish the target value, PFD$^T$**

Specify the highest acceptable PFD for the given (sub)function, i.e.

$$\text{PFD} \le \text{PFD}^T \quad = \_\_\_\_\_$$

The target values should be set in such a way that the SIL for the entire SIS is not compromised.

**Step 2 Specify parameters of (sub)function**

Initial failure rate estimates could be found by search in generic reliability databases, e.g. the OREDA (2002) and/or the PDS data (Hauge et al. 2006b). The conservative estimate is here defined as the mean value plus one standard deviation. The standard deviation could be found in OREDA, but is not given in the PDS data. Insert the following parameters for the (sub)function in question:

| | | |
|---|---|---|
| *Best estimate, rate of DU failures,* | $\lambda_{\text{DU,BE}}$ | = _____ |
| *Conservative estimate, rate of DU failures,* | $\lambda_{\text{DU,CE}}$ | = _____ |
| *Beta factor,* | $\beta$ | = _____ |
| *Min. no. of components that have to function to ensure system function,* | $M$ | = _____ |
| *No. of redundant "channels" of subfunction,* | $N$ | = _____ |

**Step 3 Failure cause analysis, initial failure rate estimate**

The initial value for the DU failure rate, $\lambda_{\text{DU,BE}}$, should be investigated with respect to relevant failure causes, and what has been done to mitigate these. First decompose the generic failure rate into the contributions from the various failure causes:

$$\lambda_{\text{DU,BE}} = \lambda_1+\lambda_2+\ldots+\lambda_n$$

where the index $i = 1,2,\ldots,n$ runs through the $n$ different failure causes. Such a decomposition could be based on generic data such as OREDA data, or other relevant data where failure causes are available. Next, each failure cause is analysed with respect to what has explicitly been done to eliminate the failure cause for the installation being the subject for the study. **Table I** shows a list of situations related to how the (generic) failure cause relates to installation specific conditions. A correction factor $\gamma_i$ to use could also be obtain from **Table I**. The result is to be documented in **Table II**.

**Table I** Correction factors, γ i based on failure cause analysis

| $\gamma_i$ | Explanation/situation |
|---|---|
| 0.1 | The failure cause is eliminated, or not relevant |
| 0.5 | Measures to prevent the failure cause are implemented |
| 1.0 | No specific conditions indicate that anything is changed for the failure cause |
| 1.5 | Failure cause not considered |
| 2 | The situation indicates that the conditions are extra bad for this failure cause |
| 5 | The situation is significantly worse with respect to this failure cause |

**Table II** Failure cause analysis of generic failure causes

| $\lambda_i$ | $\gamma_i$ | $\lambda_i \times \gamma_i$ | Failure cause | Measure implemented, and anticipated effect |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| $\sum_i \lambda_i \times \gamma_i =$ | | | (adjusted best estimate) | |

Based on the failure cause analysis calculate:

Best estimate: $\lambda_{DU,BE} = \gamma_1\lambda_1+\gamma_2\lambda_2+\ldots+\gamma_n\lambda_n$ = _____

Conservative estimate: $\lambda_{DU,CE} = \lambda_{DU,CE(2)}\,(\gamma_1\lambda_1+\gamma_2\lambda_2+\ldots+\gamma_n\lambda_n)/(\lambda_1+\lambda_2+\ldots+\lambda_n)$ = _____

Where $\lambda_{DU,CE(2)}$ is the conservative estimate found in Step 2.

### Step 4 Specify initial value for "uncertainty parameters" (for the rate of DU failures)

Generally, the estimate of $\lambda_{DU}$ will be written as $\lambda_{DU} = U_2/U_1$. These $U_1$ *and* $U_2$ are denoted the *uncertainty parameters*, and initial values for these have to be specified, e.g.

*Uncertainty parameter 1* $U_1 = \lambda_{DU,BE}/[\lambda_{DU,CE} - \lambda_{DU,BE}]^2$ = _____

*Uncertainty parameter 2* $U_2 = U_1 \times \lambda_{DU,BE}$ = _____

*Failure rate estimate to use in PFD calculations* $\lambda_{DU} = \dfrac{U_2 + 0.3\sqrt{U_2}}{U_1}$ = _____

*The following steps are performed each time an update of the test interval is considered (based on new operational data). Initially we jump to step 6 since no installation specific data exists.*

**Step 5 Collect new field specific failure data, and update the failure rate estimate**
Let $X$ denote the accumulated number of component failures observed since the last update, and let $t$ denote the total operational time for all components during this period, (this is typically the calendar time since last update multiplied with the number of components). If no failure cause analysis is conducted, Step 5a is performed, and in case of a failure cause analysis exist Step 5b is performed.

*Step 5a Simple approach without a failure cause analysis*

*No. of DU failures (component level),* $X$ = _____
*Total operational time (all components),* $t$ = _____

Next update $U_1$ *and* $U_2$ (we have introduced a damping factor DF = 0.9 to give lower weight to "old" data):

$U_1(\text{new}) = 0.9U_1(\text{old}) + t$ = _____
$U_2(\text{new}) = 0.9U_2(\text{old}) + X$ = _____

*Failure rate estimate to use in PFD calculations* $\lambda_{DU} = \dfrac{U_2 + 0.3\sqrt{U_2}}{U_1}$ = _____

*Step 5b Approach with failure cause analysis*

In situations where failure causes are analysed, and appropriate measures are implemented, we can benefit from this. First assume that the failures are classified according to the failure cause, and assume that we could group in $i = 1,\ldots,n$ different failure causes. Prior to any measures we then have:

$$X = X_1 + X_2 + \ldots + X_n$$

If compensating measures are implemented we estimate a future "equivalent" to this number by:

$$X' = \gamma_1 X_1 + \gamma_2 X_2 + \ldots + \gamma_n X_n$$

Where $\gamma_i$, $i = 1,\ldots,n$ are correction factors due to the anticipated effect of implemented measure. The values of the parameters $\gamma_i$ could be obtained from Table III.

**Table III** Adjusting failure statistics when measures are implemented

| $\gamma_I$ | Explanation/situation |
|---|---|
| 0.75 | The measure is expected to have a certain effect on the given failure cause |
| 0.5 | The measure is expected to have a significant effect on the given failure cause |
| 0.25 | The measure is expected to have a significant effect on the given failure cause, and we are able to explicitly describe the content of the measure, and the anticipated effect |
| 0.1 | The measure is expected to eliminate the failure cause. For such a judgment the measure should be documented completely, and it should be explained how the measure will eliminate the actual failure cause |

To calculate $X$' the results are documented in Table IV.

**Table IV** Documentation of measures against failure causes

| $X_i$ | $\gamma_i$ | $X_i \times \gamma_i$ | Failure cause | Measure implemented/argumentation for failure prevention |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| $\sum_i X_i \times \gamma_i =$ | | | | |

*No. of equivalent DU failures (component level),* $X' = \gamma_1 X_1 + \gamma_2 X_2 + \ldots + \gamma_n X_n$ = _____

*Total operational time (all components),* $t$ = _____

Next update $U_1$ and $U_2$ :

$U_1(\text{new}) = 0.9U_1(\text{old}) + t$ = _____

$U_2(\text{new}) = 0.9U_2(\text{old}) + X$ = _____

*Failure rate estimate to use in PFD calculations* $\lambda_{DU} = \dfrac{U_2 + 0.3\sqrt{U_2}}{U_1}$ = _____

**Step 6 Determination of maintenance intervals**

The PFD can be calculated based on the length of the test interval, $\tau$, the rate of DU failures, $\lambda_{DU}$, the beta factor $\beta$, and the voting $M$oo$N$. All parameters except $\tau$ are given/updated in the previous steps, and thus PFD can be calculated for various values of $\tau$. A simple spreadsheet in MS Excel (PDS-PFD.xls) can be downloaded from http://www.itk.ntnu.no/sil to do these calculations for various relevant values of $\tau$. The PDS-PFD.xls program has a "goal seek" function that finds the largest $\tau$ satisfying PFD $\leq$ PFD$^T$

The maximum $\tau$ satisfying in accordance with the target PFD is now recorded:

$\tau_0$ = _____

PFD = _____

This $\tau_0$ is a candidate to be the new updated length of the test interval.

**Step 7 Verify new test interval**

If Step 6 results in an increase of the length of the test interval, $\tau_0$, some verification is required before this increase is implemented, i.e. to obtain the final test interval, $\tau$.

- The increase of the length of the test interval (in one updating) should never exceed 50%
- The increase of the length of the test interval (in one updating) should never be more than 0.5 year.
- In order to optimise the grouping of several maintenance intervals, one can accept up to 10% increase in the PFD, i.e. we could accept PFD $\leq 1.1 \times$PFD$^T$ in Step 6.

To violate these requirements it would a thorough analysis must be conducted to assure e.g. that an extended interval will not increase the rate of DU failures due to the reduction in preventive maintenance (following the introduction of a longer test interval.)

Similarly, for a new installation with no plant specific data it is not recommended to start with a $\tau > 8760$ hours.

**Step 8 Trend analysis**
A Nelson Aalen plot should be constructed to help identify any systematic change in the failure rate of the components being analysed. The following procedure is recommended for construction of the Nelson Aalen plot.

1. The x-axis represents the calendar time
2. The dates for observed component failures are marked on the x-axis. This will typically be either the data for the functional tests, or the data for any real demand. Let $X_t$ be the number of failures observed at time $t$(date of test or demand). Let $N_t$ denote the number of units included in the analysis at time $t$.
3. Plot ($\Sigma_t X_t / N_t$) against $t$. Here $\Sigma_t X_t / N_t$ is calculated by increasing the y-value with $X_t / N_t$ for each $t$-value.

If the plot shows a convex behaviour, this indicates an increasing failure rate. On the other hand, if the plot shows a concave behaviour, this indicates an improvement of the situation. Note that in the plot we use the actual number of failures (X), and not the adjusted value (X')

## 4. Discussion

In this paper we have proposed a methodology for setting the initial maintenance interval, and for updating this interval as reliability data from the actual installation become available. The approach utilises a standard Bayesian updating regime which should not be controversial. The methodology also introduces a pragmatic approach to failure cause analysis, where the failure rate estimates are modified based on what has been done to mitigate the various failure causes. Default values are supported for how much credit we could claim when improvement measures are implemented. Behind these default values only sound judgement has been applied, and no empirical studies have been carried out to support these judgements. However, we believe that the methodology is rather transparent, and will form a sound basis as decision support when establishing maintenance intervals. A simplified version of the procedure is proposed in the OLF 070 guideline for the Norwegian Petroleum Industry. This approach has been found too complicated for the industry to apply, and it has been suggested to use an even simpler approach based on a control limit regime. In case of a 1 oo 1 configuration this approach records the number of DU failures, $X$, and the number of components subject to test in the last period is recorded, $n$. If $X$ is sufficiently large, the test interval is reduced by a factor 2, and if $X$ is sufficiently low the test interval is doubled. A Bayesian like argument lead to an upper control limit of $4 \cdot n \cdot \text{PFD}^T + 1$, and a lower control limit of $n \cdot \text{PFD}^T - ½$. Even if such an approach is very simple, it has some weaknesses. First of all the approach can only be used for a

1 oo 1 voting, since for higher votings the number of (system) failures should indeed be very low. Further, the statistical performance of such a control limit regime is much weaker than a sound parametric approach. We therefore, recommend to use a parametric approach when updating maintenance interval for safety instrumented systems.

## 5. References


Aven, T.(2003). *Foundatons of risk analysis.*Wiley, West Sussex.

DNV-RP-A203 Qualification Procedures for New Technology. Det Norske Veritas. P.O.Box 300, N-1322 Høvik.

Hauge, S., Hokstad, P., Lanseth, H. and Øien, K. (2006a). Reliability Prediction Method for Safety Instrumented Systems – PDS Method Handbook, 2006 Edition. SINTEF report STF50 A06031. ISBN 82-14-03899-5. SINTEF, N-7465 Trondheim, Norway.

Hauge, S., Lanseth, H. and Onshus, T. (2006b). Reliability Data for Safety Instrumented Systems – PDS Data Handbook, 2006 Edition. SINTEF report STF50 A06030. ISBN 82-14-03898-7. SINTEF, N-7465 Trondheim, Norway.

IEC 61508 Standard. Functional Safety of electrical/electronic/programmable electronic (E/E/EP) safety related systems, part 1-7, Edition 1.0 (various dates).

IEC 61511 Standard. Functional safety – safety instrumented systems for the process industry sector, part 1-3.

Martz, H. F. and Waller, R. A.(1982). *Bayesian Reliability Analysis*. John Wiley & Sons, New York.

OLF guideline no. 070 (2004). Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry, OLF. (http://www.olf.no/?23661.pdf)

OREDA (2002). Offshore Reliability Data Handbook, 4th edition. Distributed by Det Norske Veritas, P.O.Box 300, N-1322 Høvik, Norway. Prepared by SINTEF, N-7465 Trondheim, Norway.