Procedures for updating test intervals based on experience data

Jørn Vatn
eMail: jorn.vatn@ntnu.no

Updated 2024-09-25

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.

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 or PDS data). 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. Offshore Norge has issued a Recommended guidelines for the Application of IEC 61508 and IEC 61511 in the petroleum activities on the continental shelf. In appendix F of the 070-guidelines 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 070-guidelines. The paper is based on Procedures for updating test intervals based on experience data presented at an ESReDA-seminar in 2006.

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.

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 PFD^T.

The calculation of the PFD for a given subsystem is here assumed to be straightforward. 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 λ_{DU}, where λ_{DU} is an unknown parameter. The interpretation of parameters is often debated and our position in 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, λ_{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 λ_{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 λ_{DU} which will have no uncertainty if we observe the world long enough. Since we have not observed the world for very long time, there is uncertainty in λ_{DU}, and the uncertainty is related to what will be the value in the long run.

2.2 Bayesian methods

In Bayesian methods the reliability parameters used in reliability assessments are considered as stochastic variables. The analyst will newer have complete knowledge regarding the value of the these parameters, and this lack of knowledge is often denoted epistemic uncertainty.

Based on our knowledge, experience and explicit analysis of reliability data, the analyst may state his or her belief about reliability parameters. This is done 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 θ as the (vector) of reliability parameters of interest. The Bayesian approach comprised four basic steps:

1. Specify a *prior* uncertainty distribution of the reliability parameter, $\pi(\theta)$.
2. Structure reliability data information into a likelihood function, $L(\theta;\mathbf{t})$ (The likelihood function was discussed in Chapter 14 in the textbook).
3. Calculate the *posterior* uncertainty distribution of the reliability parameter vector, $\pi(\theta|\mathbf{t})$. The posterior distribution is found by $\pi(\theta|\mathbf{t}) \propto L(\theta;\mathbf{t})\pi(\theta)$, and the proportionality constant is found by requiring the posterior to integrate to one.
4. The Bayes estimate for the reliability parameter is given by the posterior mean, which in principle could be found by integration.

2.3 Problem formulation

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

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

U_2 is denoted the shape parameter whereas U_2 is denoted the intensity parameter. In literature these parameters are usually given by Greek letters. 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 $\mathrm{E}[\Lambda_{\mathrm{DU}}] = U_2/U_1$, and $\mathrm{Var}(\Lambda_{\mathrm{DU}}) = U_2/U_1^2$. Further, if we know the mean (E) and variance (V) of Λ_{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 λ_{DU} is required. The Bayesian approach would be to use the prior or posterior mean of the distribution of Λ_{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 rather easy to verify that

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

for reasonable values of U_2. Thus, an estimate in line with the IEC 61508 recommendations would be to use

$$\hat{\lambda}_{\mathrm{DU}} = U_2/U_1 + 0.3\sqrt{U_2}/U_1 \tag{3}$$

where U_1 and U_2 are either prior or posterior uncertainty parameters.

3 Procedure

The recommended procedure for parameter estimation and final updating of inspection intervals comprises the following steps

1. Establish a prior distribution from generic data
2. Update the prior distribution to a posterior distribution based on vendor data
3. Calculate a conservative estimate (70% percentile) based on the posterior distribution
4. Use the conservative estimate in the procedure for determining the proof-test interval, based on e.g., SIL-requirements, cost/benefit analysis or other approaches
5. As failure data becomes available from the actual site, update again the posterior distribution, and GoTo step 3. This is repeated at regular intervals, e.g., every three years.

3.1 Establish a prior distribution from generic data

Generic data such as OREDA,PDS data) and Exida provides failure rate estimates with uncertainty intervals. The manner these uncertainty intervals are established vary between the various data sources. In the following we assume that lower, λ_{L}, and the upper, λ_{H}, values are given, and that the interval represent an uncertainty interval where the "true" value of the failure rate is contained in this interval with some probability α, for example $\alpha = 90\%$.

From the λ_L and λ_H we calculate an expected value by the geometric mean, say $E = \sqrt{\lambda_L \lambda_H}$. A standard deviation could be assessed by say $S = (\lambda_H - \lambda_H)/4$. From these values we obtain $U_1 = E/\sqrt{S}$, and $U_2 = U_1 \times E$. The values for U_1 and U_2 are only rough estimates. The next step is to fine-tune these values such that the lower and upper values matches the gamma distribution with parameters U_1 and U_2. That is, we shall have

$$\Pr(\Lambda_{DU} < \lambda_H) = 1 - (1 - \alpha)/2 \tag{4}$$

and

$$\Pr(\Lambda_{DU} < \lambda_L) = \alpha/2 \tag{5}$$

To ensure that Equations (4) and (5) are fulfilled we need a numerical routine to calculate the cumulative distribution function, and then a numerical routine to obtain the values for U_1 and U_2. Excel provides such functions if the Solver is installed. A spreadsheet has been derived to accomplish the calculations. The values obtained are now denoted $U_{1,\text{Prior}}$ and $U_{2,\text{Prior}}$ to reflect that these are the prior parameters.

3.2 Update the prior distribution to a posterior distribution based on vendor data

If vendor data is provided they can be used to update the prior distribution to a "posterior" distribution. If both number of DU-failures, n, and total time on test T is available, we can update the prior distribution to a posterior distribution with:

$$U_{1,\text{Posterior}} = U_{1,\text{Prior}} + T \tag{6}$$
$$U_{2,\text{Posterior}} = U_{2,\text{Prior}} + n \tag{7}$$

Often only a single estimate if provided from the vendor. Let this estimate be denoted λ_V. By a subjective judgement we may specify a proxy value for n, say n_P. The n_P-value express how confident we are in the value λ_V and shall be interpreted as: The confidence in the vendor estimate is as if statistical data were evident, and n_P failures were reported. Since the failure rate is low, it is not likely that the vendor have experience many failures, such that n_P in the order 2 to 4 seems reasonable.

A corresponding proxy T-value can be established by $T_P = n_P/\lambda_V$, which gives the following updating regime:

$$U_{1,\text{Posterior}} = U_{1,\text{Prior}} + n_P/\lambda_V \tag{8}$$
$$U_{2,\text{Posterior}} = U_{2,\text{Prior}} + n_P \tag{9}$$

3.3 Calculate a conservative estimate (70% percentile) based on the posterior distribution

A conservative estimate for the failure rate is now given by

$$\hat{\lambda}_{\mathrm{DU}} = \frac{U_{2,\mathrm{Posterior}} + 0.3\sqrt{U_{2,\mathrm{Posterior}}}}{U_{1,\mathrm{Posterior}}} \tag{10}$$

3.4 Use the conservative estimate in the procedure for determining the proof-test interval

The conservative estimate $\hat{\lambda}_{\mathrm{DU}}$ in Equation (10) is now used to make sure that prof-test intervals are appropriate. Typically the various failure rate estimates are input to overall calculation of PFD for a safety instrumented function, and the PFD number should match the SIL-requirements. Also cost/benefit analysis could be carried out based on the conservative estimates in the so-called ALARP region.

3.5 Update intervals based on on-site data

When failure data becomes available from the actual site it is recommended to use these data to update the failure rate estimated on a regular basis. Let $U_{1,\text{Previous posterior}}$ and $U_{2,\text{Previous posterior}}$ be the latest update of the posterior parameters, and let X be the total number of DU-failures observed since the last update of posterior parameters. Let T be the total time on test since the last update for the components we have data for.

$$U_{1,\text{New posterior}} = 0.9U_{1,\text{Previous posterior}} + T \tag{11}$$

$$U_{2,\text{New posterior}} = 0.0U_{2,\text{Previous posterior}} + X \tag{12}$$

Equation (10) is still used to obtain the new conservative estimate $\hat{\lambda}_{\mathrm{DU}}$. Note that we have introduced a damping factor DF = 0.9 to give lower weight to "old" data. In particular if the components deteriorate over time, the data in the early life is not that relevant any more. Also if reliability improvement programs have been established to cope with known root causes, there are arguments to use such a damping factor.

An Excel file is available to support some of the calculations.