The Price of Risk Reduction: Optimization of Test and Maintenance Integrating Risk and Cost

Duško Kančev, Marko Čepin
Jožef Stefan Institute
Jamova cesta 39, SI-1000 Ljubljana, Slovenia
dusko.kancev@ijs.si, marko.cepin@ijs.si

ABSTRACT

The primary purpose of surveillance testing and maintenance (T&M) is to assure the reliability of standby safety systems and components in nuclear power plants. The optimal schedule of safety equipment outages due to testing and maintenance is one of the parameters of the plant safety. Early optimizations of single component test intervals were based on minimizing the risk without cost considerations. However, the appropriate development of T&M strategy depends not only on the T&M intervals but also on the resources (human and material) available to implement such strategies. Since these testing and maintenance activities are associated with substantial cost, they present an important domain, where risk reduction and costs can be balanced.

The objective of this paper focuses on assessing how the costs may affect the T&M optimization. The costs are expressed as a function of the selected risk measure. The time-averaged function of the selected risk measure is obtained from probabilistic safety assessment, i.e., the fault tree analysis at the system level, extended with inclusion of time parameters. The testing strategy sequential versus staggered is compared. Results of case study analysis have shown that relatively high system unavailability reduction is gained on the account of relatively low total T&M costs increase. The contribution of component aging to risk is, in general, negligible.

1 INTRODUCTION

Engineered safety systems are usually standby systems that are tested periodically to reveal and repair failures that may have occurred since the previous activation or inspection. The issue of risk effectiveness versus resource utilization is an optimization problem where the resources are to be minimized while the performance or unavailability is constrained to be at a given level. Optimal test intervals usually exist for minimizing costs while satisfying the safety goal [1].

Probabilistic Safety Assessment (PSA) is a standard method for assessing, maintaining, assuring and improving the nuclear power plant (NPP) safety. PSA studies not only evaluate safety of systems but also their results are used in safe, economical and effective design and operation of NPPs. The latter application is known as “Risk-Informed Decision Making”.

As a technique, PSA can be also used to assess the Surveillance Requirements (SRs), which are part of the TS in NPP. The SRs prescribe periodic tests for detecting faults and verifying the operability of safety equipment. This interval between two consecutive tests and/or maintenances is called the Surveillance Test Interval (STI) [2], [3], [4].

Technical Specifications (TS) define the limits and conditions for operating nuclear plants safety. These rules were originally formulated with margins on the safe side, based
more on results of a deterministic analysis. It is therefore possible that risk based TS will differ from existing ones.

The purpose of this study is to propose a methodology to reduce the risk contribution of T&M activities of safety equipment in NPPs by optimization of the STIs, while encompassing component aging and total T&M costs for different test strategies. Thus, the general objective is to stress out one of many potential benefits of the risk-informed regulation, which is the improvement of SRs and therefore TS.

Importance of PSA and its tools, such as fault trees (FTs) and event trees (ETs), increases rapidly with the number of applications to nuclear and non-nuclear fields. The risk-informed applications emphasize both effective risk control and effective resource expenditures at NPPs. These risk-informed approaches make the requirements and activities more risk effective and at the same time utilizing fewer resources by making use of PSA results to focus better on what is critical to safety. A general approach for optimizing the STI, integrating the risk and costs at the system level, was applied to the case study.

The fault tree is a static model that uses the average unavailability. It is known that such a static FT model under- and/or overestimates the unavailability of a system due to dormant failure. The error becomes especially large when a system consists of many trains. Also, the effects of maintenance strategy cannot be incorporated into the fault tree model. This is the reason why various analytical and computational models are used instead of fault trees in optimizing the STI of a system [5]. The analytical unavailability model is developed to overcome the limitations of fault tree analysis (FTA). The analytical unavailability model enables us to know the unavailability of the systems and the effect of a T&M strategy. Simultaneously, different aging scenarios are included in the model and their influence on the system unavailability and STI optimization analyzed and discussed.

2 MATHEMATICAL MODEL

In this Section, the definition of the analytic unavailability model is addressed. A general unavailability model is defined in Section 2.1, as a function of STI. The parameters such as failure rate, demand failure probability and repair time are considered to be constants in earlier work [2], [3], [5]. This paper presents and defines two unavailability functions where two characteristic component aging types are separately included, i.e. the linear- and power-law (Weibull) aging functions in addition to the no-aging unavailability function.

The cost function associated with testing and maintenance is defined in Section 2.2.2. The testing strategy is considered in Section 2.2.1. At the component and system level, the risk measures are component and system unavailability, respectively.

2.1 Component level

The component is the smallest part of the system. It is an entity that is not further subdivided and is both necessary and sufficient to be considered for analysis. Probabilistic models of components represent the standpoint for probabilistic modelling of systems. Input data to probabilistic models differ from model to model regarding the function and operation of the component under consideration. Input data may include a number of parameters, such as failure rate for the component, probability of failure per demand, repair time, test interval, test duration and test placement time.

Analysis at the component level starts with the identification of a component, its critical failure modes, and collecting component data, which has to correspond to selected probabilistic models for calculation of component unavailability.
Calculation of optimal STI which results in minimal component mean unavailability is done, in general, by setting to zero the partial derivative of component mean unavailability over the surveillance test interval. The universal equation [2], [6] for calculation of the time-averaged standby component unavailability, including contributions of test and repair, is:

\[ Q_{\text{mean}} = \rho + \frac{1}{2} \lambda_0 T_i + \frac{T_r}{T_i} + (\rho + \lambda_0 T_i) \frac{T_r}{T_i} \]  

(1)

where:
- \( Q_{\text{mean}} \) mean unavailability;
- \( T_i \) test duration;
- \( T_r \) mean time to repair;
- \( \rho \) failure probability per demand;
- \( \lambda_0 \) standby failure rate;
- \( T_i \) surveillance test interval (STI).

Eqn. (1) addresses the case where the failure rate \( \lambda \) is constant, i.e. the no-aging scenario. Optimal STI, \( T_{\text{opt}} \), in this case of constant failure rate is obtained by differentiating Eqn. (1):

\[ T_{\text{opt}} = \sqrt{\frac{2(T_r + \rho T_r)}{\lambda_0}} \]  

(2)

Equation (2) shows that STIs for more reliable components with lower failure rates should be longer. Longer \( T_i \) and \( T_r \) also result in an extended STI, but they also increase the mean unavailability of the component.

The term containing the failure rate contribution, i.e. the second term on the right-hand side of Eqn. (1), is derived as a result of some assumptions [7], [8]. Namely, if we assume negligible \( T_i \) and \( T_r \) in comparison with the T&M interval \( T_i \), also assume that any repair is carried out immediately after a test, as well as negligible test inefficiencies in a way that the component unavailability at the end of the test is zero (repair same-as new), the time-dependent probability for a random failure, \( q(t) \), and its average value over the test interval (the above mentioned second term), \( q \), rise according to the following set of formulas:

\[ q(t) = 1 - e^{-\lambda t} \approx \lambda_0 t \Rightarrow q = \frac{1}{T_i} \int_0^{T_i} q(t) dt = 1 - \frac{1}{\lambda_0 T_i} (1 - e^{-\lambda_0 T_i}) \approx \frac{1}{2} \lambda_0 T_i \ ; \ (\lambda_0 t < 0.1) \]  

(3)

Regarding the two other aging scenarios, \( \lambda \) is not anymore a constant value, but it becomes a function of time. This fact plus the above mentioned assumption (\( T_r << T_i \)), implies that only the second term of Eqn. (1) changes, i.e. might have substantial impact on results.

In the case of linear aging, the following equations are valid:

\[ \lambda_{\text{lin}} = \lambda(t) = \lambda_0 + \theta_1 t \]  

(4)

\[ Q_{\text{mean,lin}} = \rho + \frac{1}{6} T_i (3 \lambda_0 + \theta_1 T_i) + \frac{T_r}{T_i} + (\rho + \lambda_0 T_i) \frac{T_r}{T_i} \]  

(5)

In the case of power-law (Weibull) aging, the following equations are valid:

\[ \lambda_{\text{Weib}} = \lambda(t) = \theta_2 t^{\theta_3} \]  

(6)

\[ Q_{\text{mean,Weib}} = \rho + \frac{\theta_2 T_i^{1+\theta_3}}{(1 + \theta_3)(2 + \theta_3)} + \frac{T_r}{T_i} + (\rho + \lambda_0 T_i) \frac{T_r}{T_i} \]  

(7)

where:
\( \theta_1, \theta_2, \theta_3 \) aging rate coefficients.

The second terms on the right-hand side of the Eqn. (5) and Eqn. (7), are obtained after applying Eqn. (3) to the corresponding failure rate types, i.e. Eqn. (4) and Eqn. (6), respectively.

2.2 System level

At the system level, minimal system unavailability \( Q_{sys}(T_{opt}) \) cannot be determined analytically as it is at the component level mainly due to complexity of systems in NPPs and interactions among them.

System unavailability model in the PSA is adopted to represent the risk function. It is obvious that by optimizing STIs based on minimizing the corresponding safety system unavailability one can improve the safety level of NPP. A PSA model of the selected engineered safety system is done. Unavailability function of the system is generally derived from FTA, which is in fact a logical and graphical description of various combinations of failure events, i.e. the basic events (BEs). In that sense the minimal cut sets (MCSs) are obtained. After that, the BEs’ simple unavailability functions are extended with addition of new time parameters, concerning the contribution of test and repair (Eqn. 1). The analytical model created in this way is used in continuation for calculating the time-averaged unavailability and comparison of different scenarios regarding the balance between the risk and cost. Thus, system unavailability is expressed as a function of unavailability of components.

System unavailability is assessed (a simplified, 1st order approximation) as a sum of \( j \) number of MCSs and the product \( k \) extents to the number of BEs in the \( j \) th cut set as:

\[
Q_{sys}(T) \approx \sum_j \prod_k Q_{jk}(T) \quad (8)
\]

where \( Q_{jk} \) represents the unavailability associated with the basic event \( k \) belonging to the MCS number \( j \).

2.2.1 Testing strategy considerations

Analysis at the system level takes into account the testing strategy. Sequential versus staggered testing comparison is stressed out. The criterion for consideration regarding the testing strategy is the minimal system mean unavailability.

In sequential testing, \( n \) redundant components are tested consecutively, one immediately after another at the beginning of the test interval \( T_i \) or at the end. The test duration is \( T \). On the other hand, when staggered testing strategy is selected, \( n \) redundant components are tested in a way that every time \( nT_i \) one component is tested.

In the no-aging scenario, commonly used in numerous works and already trivial case, the two- and three- component unavailability contribution due to a sequential testing, is given in [7]. The new approach suggested in this paper, which includes aging in the calculation of the mean system unavailability, comprises the equations (9), (11) and (10), (12) for the linear- and Weibull-aging cases, respectively. Due to the space limitation, only the equations concerning the testing of three \( (n = 3) \) components are presented below as an example. Equations corresponding to other \( n \) s are analogous. They were derived from two general equations, each regarding the corresponding testing strategy according to Vaurio [8], in a way...
that instead of the constant $\lambda$, the corresponding $\lambda(t)$ was inserted, and the yield after averaging over a $T_i$ is:

$$Q_{seq,lin,3} = \frac{1}{140} T_i^3 \left( 20 T_i^3 \theta_1^3 + 70 T_i^2 \theta_1^2 \lambda_0 + 84 T_i \theta_1 \lambda_0^2 + 35 \lambda_0^3 \right) + \left[ \rho + \frac{T_i}{T_i} + (\rho + \lambda_0 T_i) \frac{T_i}{T_i} \right]$$  \hspace{1cm} (9)

$$Q_{seq,Weib,3} = \frac{\theta_2^3 T_i^4 + 3 \theta_2}{4 + 3 \theta_3} + \left[ \rho + \frac{T_i}{T_i} + (\rho + \lambda_0 T_i) \frac{T_i}{T_i} \right]^3$$  \hspace{1cm} (10)

$$Q_{agg,lin,3} = \frac{T_i^3 (146T_i^3 \theta_1^3 + 1596T_i^2 \theta_1^2 \lambda_0 + 6111T_i \theta_1 \lambda_0^2 + 8505 \lambda_0^3)}{102060} + \left[ \rho + \frac{T_i}{T_i} + (\rho + \lambda_0 T_i) \frac{T_i}{T_i} \right]^3$$  \hspace{1cm} (11)

$$Q_{agg,Weib,3} = \frac{3^{-3-3 \theta_0} T_i^4 + 3 \theta_2^2 (18 + 37 \theta_3 + 18 \theta_3^2)}{8 + 26 \theta_3 + 27 \theta_3^2 + 9 \theta_3^3} + \left[ \rho + \frac{T_i}{T_i} + (\rho + \lambda_0 T_i) \frac{T_i}{T_i} \right]^3$$  \hspace{1cm} (12)

### 2.2.2 Cost function

The mean system unavailability, $Q_{sys}$, of the selected safety system in this paper is expressed as a function arising from unavailability of components, including the contributions of test and repair. Similarly, the cost model is given as follows:

$$c_T = C_I + (1 - Q_{sys})C_R + Q_{sys}C_F$$  \hspace{1cm} (13)

where:

- $C_I$ total cost of T&M of system;
- $C_R$ restorative maintenance cost of system;
- $C_F$ surveillance testing cost of system;
- $C_F$ full repair or replacement cost of system.

### 3 CASE STUDY

The standby safety system under consideration is a simplified high-pressure injection system (HPIS) of a pressurized water reactor (PWR) [9],[10]. This system is normally in stand-by and consists of three pumps and seven valves organized as shown in Figure 1.

![Figure 1: The sample system](image)

The T&M activities, integrating aging and different test strategies, are concerning only the three pumps. The STI for each pump, specified by the TS, is 2190 hrs T&M costs $C_I$, $C_R$, $C_F$, defined in the previous chapter, adapted from ref. [5], are 70$, 350$ and 52.500$, respectively.

Mean unavailability evaluation was done for a whole spectrum of different $T_i$, regarding the two mentioned aging scenarios, two different testing strategies and two different
maintenance (repair) duration times $T_r$, i.e. 21.5 hrs that is the mean repair duration time [11] and 68 hrs, which is the allowed outage time (AOT) specified in TS. The average time to test a pump is 4 hrs [10].

3.1 Selected results of the case study

Figure 2 represents system unavailability calculation results for the $T_r = 21.5$ hrs scenario. The $T_r = 68$ hrs scenario is qualitatively the same, with slight differences (1%-3%) from quantitative aspect.

![Figure 2: System unavailability](image)

It can be seen that $Q_{sys}$ is the lowest for about half-month $T_i$ (352 hrs & 440 hrs for the sequential and staggered testing strategy, respectively). By shortening the $T_i$, substantial unavailability decrease is observable. As $T_i$ increases, the difference among the three aging scenarios increases too, especially between the linear- and Weibull aging. The cost function is represented with two curves, each corresponding to one of the aging scenarios ($Q_{sys,lin}$ & $Q_{sys,Weib}$ - Eqn. 13). It can be seen that minimizing the cost generally leads to longer characteristic intervals than minimizing the risk (unavailability) alone. Figure 3 shows results of relative comparison $X$ ($X = (Q(T_i) - Q(T_{i,opt}))/Q(T_i)$) to optimal value at minimal $Q_{sys}$ for the no-aging scenario.

Table 1 shows the calculated system mean unavailabilities based on the optimal test interval, $T_{i,opt}$, implied from minimal risk. The relative unavailability reduction (if sequential is replaced by staggered testing) for the three different aging scenarios is emphasized.

![Figure 3: Relative comparisons](image)

Table 1: Comparison of system unavailabilities for both testing strategies

<table>
<thead>
<tr>
<th>$Q_{top}(T_{i,opt}) = Q_{min}$</th>
<th>NO AGING</th>
<th>LINEAR</th>
<th>WEIBULL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$T_r = 21.5$ hrs</td>
<td>$T_r = 68$ hrs</td>
<td>$T_r = 21.5$ hrs</td>
</tr>
<tr>
<td>sequential</td>
<td>3.65E-05</td>
<td>3.97E-05</td>
<td>3.65E-05</td>
</tr>
<tr>
<td>staggered</td>
<td>3.37E-05</td>
<td>3.62E-05</td>
<td>3.37E-05</td>
</tr>
<tr>
<td>seq. vs. stgg. [%]</td>
<td>8.13 %</td>
<td>9.70 %</td>
<td>8.13 %</td>
</tr>
</tbody>
</table>

Table 2 shows the relative ($((Q(T_{i,TS}) - Q(T_{i,opt}))/Q(T_{i,TS})$) reduction in the mean system unavailability if the test interval specified by the TS, $T_{i,TS}$, is replaced by the optimal one, $T_{i,opt}$. This relative difference, although high in general, is higher for the sequential testing strategy ($\approx 95\%$) than for the staggered one ($\approx 88\%$). The price of this unavailability
309.7

and risk reduction, due to optimization of SR in TS and replacement of $T_{i_{TS}}$ with $T_{i_{opt}}$, is shown in Table 3. It can be seen that this relatively high reduction of risk would mean increase of (“only”) $\approx 10\%$ of the T&M costs in the worse case (if sequential testing strategy is applied during the T&M). In the other case, i.e. in the case of staggered testing, this increase of cost would be $\approx 5\%$. It can be seen that although there are slight differences ($1\%-2\%$) in the results between the two aging scenarios, in general they are negligible in the vicinity of $T_{i_{opt}}$. These differences begin to increase out of this area of $Q_{sys,min}$, especially with the extension of $T_i$ (Figure 4).

Table 2: Comparison of risk reduction between different scenarios

<table>
<thead>
<tr>
<th>$Q_{top}(T_{iTS})$ vs. $Q_{top}(T_{i_{opt}})$</th>
<th>sequential</th>
<th>staggered</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$Tr = 21.5\ hrs$</td>
<td>$Tr = 68\ hrs$</td>
</tr>
<tr>
<td>NO AGING</td>
<td>95.6 %</td>
<td>95.2 %</td>
</tr>
<tr>
<td>LINEAR</td>
<td>95.6 %</td>
<td>95.3 %</td>
</tr>
<tr>
<td>WEIBULL</td>
<td>94.7 %</td>
<td>94.3 %</td>
</tr>
</tbody>
</table>

Table 3: Comparison of total T&M costs

<table>
<thead>
<tr>
<th>Costs($T_{iTS}$ vs. $T_{i_{opt}}$)</th>
<th>sequential</th>
<th>staggered</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>NO AGING</td>
<td>LINEAR</td>
</tr>
<tr>
<td>$Tr = 21.5\ hrs$</td>
<td>9,81 %</td>
<td>9,83 %</td>
</tr>
<tr>
<td>$Tr = 68\ hrs$</td>
<td>9,77 %</td>
<td>9,80 %</td>
</tr>
</tbody>
</table>

Figure 4: Relative comparison between aging scenarios

4 CONCLUSIONS

An optimization approach of SRs in TS, concerning risk and costs, was developed to achieve one of many potential benefits of PSA. The main advantage of this approach is that it integrates the contributions of component aging from one side and T&M strategy from other side in deriving the system mean unavailability, $Q_{sys}$, as a risk measure.

Results indicate that the optimal STI for the motor-driven pumps, implying minimal risk, is about half-month. System mean unavailability at STIs between half-month and 3 months (as specified in the TS) differs notably. The contribution of component aging to risk is negligible, in general. Negligible difference between the two aging scenarios is observed in the vicinity of the proposed $T_i$, although this difference rises with extension of the test interval.
The minima of the risk and cost functions are relatively flat. The minimum of the cost function corresponds to slightly longer test intervals than minimizing the risk alone.

Both testing strategies, sequential and staggered, have been included in analysis. Risk reduction of \(\approx 9\%\) (sequential testing) and \(\approx 3\%\) (staggered testing) in the vicinity of \(T_{i_{-opt}}\) has been found.

Variations in the repair time, \(T_r\), of analyzed components have relatively small impact on the system unavailability.

Research based on a case study has shown that active use of PSA results leads to unavailability reduction. The case study has shown that significant economical benefits can be obtained by optimizing T&M intervals. Namely, replacement of the STI, specified by TS \(T_{i_{-TS}}\), with the proposed one, \(T_{i_{-opt}}\), implies risk reduction of \(\approx 90\%\) and total T&M costs increase of only \(\approx 10\%\).

ACKNOWLEDGMENTS

The Slovenian Research Agency supported this research (contract No.1000-08-310002).

REFERENCES


