Approach to improving the reliability prediction for Software Systems

Jamal Krini\textsuperscript{a1}, Ossmane Krini\textsuperscript{a2}, Abderrahim Krini\textsuperscript{a3}, Josef Börsökö\textsuperscript{a4}

Accepted 10\textsuperscript{th} August 2015

Abstract: For example, software is used in the automobile industry, in aerospace engineering and in medical technology. These scopes are considered to be safety-critical. In the case of failure human life as well as its environment might be in danger. Therefore, software reliability plays a huge role in safety critical applications. They provide information on how long and with the help of which resources a software needs to be tested in order to reach a desired reliability. Currently, there are more than 100 reliability growth models existing. The distinction between the models is based on different assumptions. Most of the models are simply improvements of other models. The littlewood model asserts, errors leading earlier to a breakdown possess a higher hazard rate than errors leading much later to a breakdown. This model should be assumed by means of quality-factor improves the prognosis.

Keywords: reliability, littlewood model, software, safety, reliability, growth models, probability of failure, hazard rate, gamma distribution, density function.

1. Introduction

The reliability of a product or a technical system is characterised by its ability to make reliable claims regarding the functions of a product or system at a particular time interval. The term „reliability” is a familiar term in the field of functional safety. Hereby, the term is linked with the proper functioning/ functionality of a product. A reliable system is a product, whose functioning is assured at all times and under all conditions. As safety can also be reached when reducing the intended function and assuring a safe condition if necessary, one can also talk about the safety integrity of a system. For example, software is used in the automobile industry, in aerospace engineering and in medical technology. These scopes are considered to be safety critical. In the case of failure human life as well as its environment might be in danger. Therefore, software reliability plays a huge role in safety critical applications. It becomes critical when, for example, a software error costs lives. For example, in treating patients suffering from cancer, a machine for radiotherapy had miscalculated the dosage and this had resulted in the loss of eight lives with another 20 people heavily injured. This provides us with another example, demonstrating the danger of software errors. In order to prevent this from happening, software is extensively tested. In this process, various methods exist to make software even more reliable and for this reason, reliability growth models are used.

2. Forecast models

Based on a forecast it is possible to make certain statements about future events. “Prognosis” originates from the Old Greek and means „to predict”. Weighing all relevant and known mistakes, a prognosis tries to predict a future development of a certain phenomenon or a certain situation. Last but not least means providing an estimation. A very important prediction is the reliability prediction. They provide information on how long and with the help of which resources a software needs to be tested in order to reach a desired reliability. Currently, there are more than 100 reliability growth models existing. The distinction between the models is based on different assumptions. Most of the models are simply improvements of other models. The littlewood model asserts, errors leading earlier to a breakdown possess a higher hazard rate than errors leading much later to a breakdown. This model should be assumed by means of quality-factor improves the prognosis.

Examples for complexity are:
- Inherent faults
- Operating errors
- Inherent faults

Another important factor for functional safety is the probability of failure. It indicates the probability for failure or destruction of a system. The term ‘failure’ stands for cutting out the performance of a task. It results in shifting from workable to corrupt condition. The term ‘fault’ represents the non-performance of at least one of the given requirements. Reasons for the failure of software can be classified into two causes of failure:
- Operating errors
- Inherent faults

\textsuperscript{1}Department of Computer Architecture and System Programming
University of Kassel, Wilhelmshöher Allee 71 – 73, 34121 Kassel, Germany
\textsuperscript{* Corresponding Author: Email: j.krini@uni-kassel.de
Note: This paper has been presented at the International Conference on Advanced Technology & Sciences (ICAT'15) held in Antalya (Turkey), August 04-07, 2015.
Whereas reasons for the failure of hardware can be classified into three causes of failure:
- Operating errors
- Inherent faults
- Physical faults

Examples for operating errors can be human failures as well as application errors. An inherent fault can be an implementation fault. A physical fault can be caused by attrition, consumption as well as by the aging process. Physical faults can only occur with hardware.
Software does not have any attrition or aging process.

Next figure illustrates the failure causes graphically.

### 3. Mathematical basics

Nowadays, more and more complex systems do exist. Mostly they consist of software components. As a logical consequence, the probability of failure of a software component increases. This can lead into catastrophic results.

In order to get a reliable prediction, it is important to resort to the default data. These default data do represent the valid default data in reality, which have been collected during a software test. The following table serves to show the default data that have been detected after a test.

<table>
<thead>
<tr>
<th>Failure number</th>
<th>TBF</th>
<th>Cumulative number of failures</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>45</td>
<td>45</td>
</tr>
<tr>
<td>2</td>
<td>53</td>
<td>98</td>
</tr>
<tr>
<td>3</td>
<td>19</td>
<td>117</td>
</tr>
<tr>
<td>4</td>
<td>62</td>
<td>179</td>
</tr>
<tr>
<td>5</td>
<td>34</td>
<td>213</td>
</tr>
<tr>
<td>6</td>
<td>112</td>
<td>325</td>
</tr>
<tr>
<td>7</td>
<td>268</td>
<td>593</td>
</tr>
<tr>
<td>8</td>
<td>102</td>
<td>695</td>
</tr>
<tr>
<td>9</td>
<td>251</td>
<td>946</td>
</tr>
</tbody>
</table>

MTTF stands for the mean time to failure. MTBF stands for the mean time between failures. MTTR stands for the mean time to repair. This is equivalent to the time needed for detecting and repairing a failure. The lower figure illustrates the relation between MTTF, MTTR and MTBF.

The cumulative number of default data is represented by the sum of the individual TBFs “Time Between Failure”. An important aspect of the reliability prediction is the hazard rate. The hazard rate serves to represent the current intensity level of the failure rate. Furthermore, it is often referred to as default rate or failure rate.

The hazard rate is defined as follows:

\[ z(t) = \lim_{\Delta t \to 0} \frac{R(t) - R(t + \Delta t)}{\Delta t} = \frac{1}{R(t)} \frac{dR(t)}{dt} \]

\[ R(t) \] is the reliability of a system. For reliability one has:

\[ R(t) = e^{-\lambda t} \]

Failure density is the temporal derivation of probability of failure

\[ f(t) = \frac{df(t)}{dt} = - \frac{dR(t)}{dt} \]

Thus it follows for the hazard rate:

\[ z(t) = \frac{f(t)}{R(t)} = \frac{f(t)}{1 - F(t)} \]

Through the derivation of the probability of failure, the failure density function can be determined. For the failure density function is obtained:

\[ f(t) = z(t) \cdot e^{-\int_0^t z(s)ds} \]

For non-repairable systems applies:

\[ \lambda(t) = z(t) \]

For a constant hazard rate applies:

\[ \lambda(t) \neq z(t) \]

For all other cases applies:

\[ \lambda(t) \neq z(t) \]

The program hazard rate depends is time-dependent and it also depends on the history of the process. The history of the process concentrates merely on the number of errors that have been detected and removed before the point in time \( M(t) \).

The following may be applied for the program hazard rate:

\[ z(t, V_i) = (u_0 - M(t)) \cdot z_0(t) \]

With the help of the mean value function the expected number of detected and removed errors before a point in time \( M(t) \) may be indicated.

\[ \mu(t) = E[M(t)] \]

The following applies with regards to that:

\[ E[M(t)] = u_0 \cdot F_a(t) \]

Therefore, the following applies for the mean value function:

\[ \mu(t) = u_0 \cdot F_a(t) = u_0 \cdot \left[ 1 - e^{-\int_0^t z_0(s)ds} \right] \]

The intensity of failure corresponds to the expected value of the program hazard rate. At the same time it corresponds to the mean value function after the point in time.

\[ \lambda(t) = E[z(t, V_i)] = \frac{d\mu(t)}{dt} \]

### 4. Reliability models

The Jelinski- Moranda- Model is one of the first models and was published in 1972. For this model, Jelinski and Moranda made the following assumptions:
- the amount \( A_0 \) of unknown mistakes in a software is firm
- every fault is just as dangerous given the probability of immediately making a mistake
- the hazard rate of a mistake does not change over time and stays constant
- the times in between mistakes stays
- default is corrected immediately

As can be seen, in this model a constant hazard rate \( z_0(t) = \phi \) is
assumed for any errors, which is unrealistic.

A better model is at this point the Littlewood model. The model asserts, errors leading earlier to a breakdown possess a higher hazard rate than errors leading much later to a breakdown. Thus, the hazard rate must decrease with time, regardless of whether an error was detected or not. Consequently, the program hazard rate does not drop steadily during breakdowns like with the Jelinski–Moranda–Model, but it rather tends to gradually decrease. This effect may be presented with the help of a Binomial model. The littlewood model considered exactly this phenomenon. In reliability engineering, the gamma distribution helps describe the time until the “i-th” failure, assuming that times are exponentially distributed. For the gamma distribution, the probability density function (PDF) may be defined as the following:

\[ f(x) = \begin{cases} \frac{\alpha}{\Gamma(i)} x^{i-1} e^{-\lambda x}, & x \geq 0 \\ 0, & x < 0 \end{cases} \]

Thereby, \( \lambda \) corresponds to the failure rate and \( \Gamma(i) \) corresponds to the gamma function. The gamma function is defined as the following:

\[ \Gamma(i) = \int_{0}^{\infty} x^{i-1} e^{-x} dx \]

For \( i = 1 \), the gamma distribution leads to the exponential function. The gamma distribution \( (\alpha, \beta) \) is used in order to assign a higher hazard rate to errors occurring earlier and in order to assign a lower hazard rate to errors occurring later, thus preventing that error rates do not remain constant but that they rather depend on the use of the program. In this process, random draws from the gamma distribution \( (\alpha, \beta) \) are used for the hazard rates. If the program is run for a total time period \( t \), the following time-dependent hazard rate will be applied by means of the Bayes’ theorem:

\[ \alpha \frac{1}{\beta + t} \]

By means of this hazard rate, requirements from the start are met. While time increases, the hazard rate sinks. As a result, it can be said that the higher the hazard rate, the earlier an error occurs. In case at least one failure has occurred until the point of time \( t \), the distribution function can be calculated as the following:

\[ F_a(t) = 1 - e^{-\frac{\alpha}{\beta + t} t} \]

After the integral equation has been solved, it becomes evident that a Pareto distribution is followed by a distribution function:

\[ F_a(t) = 1 - \left( \frac{\beta}{\beta + t} \right)^\alpha \]

The following applies for the program hazard rate:

\[ h(t,m(t)) = (u_0 - m(t)) \cdot z_a(t) = (u_0 - m(t)) \cdot \frac{\alpha}{\beta + t} \]

The mean value function is calculated as follows:

\[ \mu(t) = u_0 \cdot F_a(t) = u_0 \cdot \left(1 - e^{-\frac{\alpha}{\beta + t} t}\right) \]

By considering the Limes of the mean value function for \( t \to \infty \), proof for this model being an infinite model is provided.

Furthermore, the following applies for the failure intensity:

\[ \lambda(t) = \frac{d\mu(t)}{dt} = \frac{d}{dt} \left( u_0 \cdot \left(1 - \left( \frac{\beta}{\beta + t} \right)^\alpha \right) \right) \]

Calculating the Limes and the failure intensity, the following applies:

\[ \lim_{t \to \infty} \lambda(t) = 0 \]

Next Figure shows the program hazard rate \( h(t,m(t)) \).

An important part of reliability prediction is the estimation procedure. It is used to determine the model parameters. The Maximum Likelihood Estimation (MLE) is the most effective and most common method in use. It is defined as follows:

\[ L = L(\phi) = \prod_{i=1}^{n} p(X_i = x_i | \phi) \]

For the failure density function follows:

\[ f(t_i) = z(t) e^{-\frac{\alpha}{\beta + t} t_i} \]

\[ = (U_0 - i + 1) \frac{\alpha}{\beta + t} e^{-\frac{\alpha}{\beta + t} (U_0 - i + 1) \cdot \frac{\alpha}{\beta + t} t_i} \]

\[ = (U_0 - i + 1) \frac{\alpha}{\beta + t} e^{-\frac{\alpha}{\beta + t} (U_0 - i + 1) \cdot \log(\beta + t)} \cdot e^{\alpha(U_0 - i + 1) \cdot \log(\beta)} \]

For the parameter estimation of the proposed Littlewood model follows:

\[ L = L(U_0, \alpha, \beta) = \prod_{i=1}^{n} f(t_i) \]

\[ = \prod_{i=1}^{n} \left\{ (U_0 - i + 1) \frac{\alpha}{\beta + t} e^{-\frac{\alpha}{\beta + t} (U_0 - i + 1) \cdot \log(\beta + t)} \cdot e^{\alpha(U_0 - i + 1) \cdot \log(\beta)} \right\} \]

By taking the logarithm follows:

\[ Log(L(U_0, \alpha, \beta)) = \sum_{i=1}^{n} \log(U_0 - i + 1) \]

\[ + n \cdot \log(\alpha) \]

\[ - n \cdot \log(\beta + t) \]

\[ + \sum_{i=1}^{n} \alpha \cdot \log(U_0 - i + 1) \cdot \log(\beta + t) \]

Now the parameters can be estimated.

5. Improve predictive Model with Quality- Factor

In order to improve the prediction accuracy the “Hold-On” method has to be applied. Firstly, the software needs to be tested. A table including the default data will be created after the test. These default data will be taken and they are going to be attached to the Littlewood model.
The data procession block serves for the data measurement value. It is preferable that not all data that is available is evaluated at the same time. Moreover, the goal is to piecewise analyze the data. After the first data amount has been analyzed, and a prediction of reliability is has been made, it can be compared to a real second data amount. By comparing it, the quality – factor (Q- factor) may be determined.

Using this quality - factor an improved prognosis should be created. One potential method is to multiply the hazard rate with the quality factor γ:

For the hazard rate follows:

$$z_a(t) = \alpha \beta t + \gamma$$

For the distribution function follows:

$$F_a(t) = 1 - \left(\frac{\beta}{\beta + t}\right)^{\alpha \gamma}$$

For the program hazard rate follows:

$$z(t, m(t)) = (u_0 - m(t)) \cdot z_a(t) = (u_0 - m(t)) \cdot \frac{\alpha \gamma}{\beta + t}$$

The mean value function is therefore calculated as follows:

$$\mu(t) = u_0 \cdot F_a(t) = u_0 \cdot \left(1 - e^{-\int_0^t \frac{\alpha \gamma}{\beta + t} \, dx}\right)$$

Subsequently, it can be demonstrated by means of comparison whether the required quality factor would lead to an improvement of the prediction.

6. Summary

Currently, there are more than 100 reliability growth models existing. The distinction between the models is based on different assumptions. Most of the models are simply improvements of other models. The littlewood model asserts, errors leading earlier to a breakdown possess a higher hazard rate than errors leading much later to a breakdown. This model should be assumed by means of quality- factor improves the prognosis.

References