A New Risk Identification Model Based on Improbability of Potential Software Project Risks: Validated by Real Empirical Studies

Ahdieh Sadat Khatavakhotan and Dr. Siew Hock Ow and Dr. Navid Hashemitaba

1, 2, 3 Department of Software Engineering, Faculty of Computer Science and Information Technology, University of Malaya, 50603, Kuala Lumpur, MALAYSIA

ahdiehkhotan@yahoo.com

Abstract: This study provides a model that investigates as a first step potential probable as well as improbable risks in the first step. Concentration on improbable risks and ensuring about their improbability would minimize the possibility of missing an important risk. This is an empirical study on 66 post-graduate students to investigate the risks involved in a software project, with a dedicated focus on the probability and improbability of these risks. The obtained results indicated that the ratio of time spent on the determination of probability of a risk (as the most important cost factor) to the overall time spent on the determination of probable and improbable risks was less than 20%. This amount is negligible given the costs incurred by the fallout reported in recent studies - resulting from missing a risk as well as the escalated consequences introduced in the next assessment and management phases.

Keywords: Risk identification, Risk assessment, Materialized risks, Non materialized risks, Statistical test, Software Risk Management.

1. Introduction

Project risk assessment and management models start with identifying the risks in a given project. A precise definition of risk and its effective classes and factors is vital in the success of subsequent phases (Xue, 2009). The next step – “risk assessment” – involves assessing risk likelihoods and their devastating effects using different models. Risk ranks and impacts are determined using the relevant classical, fuzzy, or co-integrated methods (Bannerman, 2008).

The risk identification, assessment, and management methods applied to software projects are naturally different from other projects (Boehm, 1991; Schmidt, et al., 2001). This is because software projects do not produce physical work products; thus, measurement of work products and, subsequently, measurement of the associated risks and consequences is very different and sensitive. Definition of characteristics, features, and specification of work products as a substitute for physical dimensions is the most logical and applicable approach. Because of this, risk management should focus on the consequences that affect these characteristics, features, and specifications.

2. Definitions and Background

2.1 Risk Improbability

Although risk management models usually have similar mechanisms – including identification and assessment of risks and provision of risk management solutions – risk assessment methods and risk consequence mitigation procedures are different. Note that moving towards the next risk management phases, i.e. concentration on the assessment and
mitigation of risk, does not afford any opportunity for focusing on the possibly neglected risks. Therefore, risk identification activities are very important, and any incorrectly identified risk would be a potentially permanent risk to software projects (Zwikael, & Ahn, 2011). The undiagnosed risks will no longer be considered as risks once they have been materialized; rather, they are regarded as a fault, defect, or at least a constraint. The main problem is that proactive methods are not applicable to these and risk management budgets rarely include undiagnosed risks.

2.2 Probable and Improbable Risk Models
The provided model was designed based on probable and improbable risks. As shown in Figure 1, the first phase of this model is providing a comprehensive classification of probable risks in the investigated software project. This risk classification is independent of the implementation and management procedures of software projects - a competitive advantage over the existing risk management models (Bodea, and Purnus, 2012). This is included as a central feature of the proposed model to provide the possibility of modifying the development procedures throughout the project if necessary. Thus, a comprehensive classification allows fast and renewed focus on re-including those risks that might become probable.

3. Weaknesses of Existing Risk Management Models
One of the most important weaknesses in the majority of software project risk assessment and management models/processes is the lack of a coherent project risk classification (Elzamly & Hussin, 2015). Although the approach used for the development of software has its associated risks, it does not eliminate the need for an integrated classification. Provision of an integrated classification for different probable software project risks would not be considered as inefficiency if it included the improbable risks involved in a software project.

On the other hand, provision of a comprehensive classification allowed analysts to freely identify the risks. Risk identification, assessment, management, and other related activities are especially focused on in Human Wier's software projects. Therefore, two essential factors determine the success of every risk management model: (1) knowledge, capability, and experience of the analysts involved in the field, and the way such knowledge is exploited, and (2) availability of environmental facilities, required tools, and relevant information. The greater the number of tools, facilities, instructions, and information available to the analysts, the more efficient her outcome would be (Lindholm, 2015).

4. Methodology
Experimental and empirical study in a real environment could be assumed as a reliable method to validate the effectiveness and efficacy of proposed model (Remenyi, et al., 2002). To use this methodology, a completed software project whose risk management documents are available was selected. Then the project definition documents, as well as certain work products on its analysis and design, along with the project’s work products, were given to post-graduate students of a certain university. Inclusion criteria in this case study was completion of two courses, namely, Software Project Management and Advanced Software Engineering Topics in System Development. The proposed comprehensive and integrated classification of risk factors was given to the students in addition to the artifacts. These risk factors included the probable project risks, given the project risk management records, as well as the improbable risks. In addition to studying the artifacts, the students determined the probable and improbable risks in this project. The forms designed for evaluating the participants’ attempts reflected the time each student spent to identify the probability and improbability of each risk. Then, quantitative and qualitative investigations into the participants’ opinions were initiated.
A New Risk Identification Model Based on Improbability of Potential Software Project Risks: Validated by Real Empirical Studies

Figure 1. Determining the Improbable Project Risks.

4.1 Metrics of Efficiency and Effectiveness

The ratio of the time allocated to identifying improbable risks to the overall time allocated to identifying the probability or improbability of that risk is the most important metric for specifying the effectiveness of the proposed classification. Certainly, the time spent on risk identification, its probability and improbability, or its consequences has nothing to do with the evaluation of the model. This is because these items should be evaluated in every model and their effectiveness or ineffectiveness is independent of risk classification: rather, they relate to risk management model and capability of risk analysts. The important factors collected in this study (Ferguson, 2004; Chua, 2009;):

i) The number of those who confirmed the existence of a risk (in percentage).

ii) The number of those who rejected the existence of a risk (in percentage).

iii) The mean time allocated to the confirmation of probability of a risk.

iv) The mean time allocated to the confirmation of improbability of a risk.

v) The time allocated to determination of improbable risks to the time allocated to determination of probable risks.

vi) The time allocated to determination of probable risks to the overall time allocated to determination of probability.

A weighted metric for evaluating the effectiveness of the proposed classification is the time allocated to probable risks multiplied by the percentage of the students who confirmed these risks as probable. In this way, the time needed for confirming each risk is determined. The mean amount of time spent on determination of improbability of a risk is obtained by measuring the overall allocated time divided by the number of those who voted to the improbability of that indicator.

The normality of data is tested by Skewness with SPSS ver. 22. Because the distribution of data was not normal, the Friedman’s two-way analysis test (non-parametric related samples) is used. Figure two shows the sample histogram of data for only two risk factors (RF1 and RF19) (see Figure 2).
Eventually, division of the mean amount of time spent on each probable risk by the overall risks gives the efficient time required for determination of probable risks. Similarly, division of the mean time spent on detection of improbable risks to the overall time spent on detection of all risks is considered to be false positive or inefficient time spent on improbable risks.

5. Data Collection

As can be observed in diagram of Figure 3, there was a consensus on improbability of Risks 8, 9, and 12. Among them, only Risk 9 had been identified in the risk management process; however, it did not materialize and basically the context for its occurrence was not provided. The Risk 3, with 90% consensus on its improbability, also never occurred.

The only exception was Risk 11 which — although marked as improbable by the majority of participants — was actually probable and did actually occur. Although this is a marginal risk, it was placed between critical and negligible categories. In other words, on average, the probability of 46% of the candidate risks was confirmed at least by one analyst. Among them, 25% of the candidate risks were confirmed by all analysts. This means that there was a consensus on the probability of more than 65% of the risks, which is an acceptable percentage in support of the proposed model. In addition, more than 90% of the probable risks were confirmed by 80% of the analysts.

With respect to improbable risks, 80% of the analysts had a consensus on 85% of the improbable risks. In addition, 65% of the improbable risks were confirmed by all the analysts, indicating the effectiveness of the proposed classification as well as normality of the analysts’ behaviors. Finally, the mean time spent on the rejection the probability of a risk is an important criterion in determining the effectiveness of the model. This amount of time accounts for the one third of the overall time allocated to the detection of probability.

6. Conclusion

This case study showed that a model focused on detection of probability or improbability of a risk before initiating precise measurement of the risks would be a sufficiently acceptable model. Qualitatively, only one out of 16 risks, recognized as improbable, turned out to be actually probable; however, as it was a marginal risk, it did not affect the
validity of the original model. With respect to efficiency, the ratio of time allocated to the detection of improbability of a risk to the overall time allocated to the detection of probability of a risk was less than 30%. This not only saves a huge cost in project risk management by preventing detection of improbable risks, but also minimizes concerns regarding improbable risks' materializing in the future or allocating budget and policy for mitigation and management of improbable risks.

Considering the flaw escalation models, we can conclude that it would be much more justifiable to employ extra workforce (less than 33%) to ensure risk probability than to be obliged to allocate costs (tens of times more) to compensate for missing probable risks.

References


