This paper was presented at the SEI Conference on Risk Management, 1997, Atlantic City, NJ.

Empirical Evaluation of a Risk Management Method

Jyrki Kontio[1]
Nokia Telecommunications /
Helsinki University of Technology
P.O.Box 315
NOKIA GROUP, FIN-00045, Finland
Email: jyrki.kontio@ntc.nokia.com
http://www.cs.umd.edu/users/kontio/

and

Victor R. Basili
University of Maryland
Department of Computer Science
A.V.Williams Building
College Park, MD 20742, U.S.A.
Email: basili@cs.umd.edu
http://www.cs.umd.edu/users/basili/

Abstract

This paper argues that three main obstacles for wider use of risk management technology are low awareness of the technology, limitations of existing risk management approaches, and lack of empirical evidence of the usefulness of risk management methods. This paper addresses the last two of these issues. First, we present a risk management method that attempts to avoid the limitations we have recognized in many current risk management approaches. The method, called Riskit, allows a thorough documentation of risk scenarios, uses a sound approach for ranking risks, and supports multiple goals and stakeholders. Second, we will discuss the inherent difficulties in evaluating risk management methods empirically and present an example of an empirical study that was carried out to evaluate the feasibility of the method.

1. Introduction

Several risk management approaches have been proposed and used [9,10,16,21,25,26,30,32] since Boehm [2,3] and Charette [7,8] brought risk management to the attention of the software engineering community. Although there are several individual reports of successful deployment of risk management techniques in practice, the software industry as a whole does not seem to apply risk management methods actively and systematically [27]. The limited survey data from the 1995 International Workshop on Software Engineering Data (IWSED-95) by Basili and Koji Tori [18] supports this observation: a minority of software organizations use specific methods for risk management systematically.

We believe that there are three primary reasons for the low penetration rate of risk management technology. First, despite recent publications and conferences in risk management, knowledge about possible risk management methods and tools has not reached most practitioners: "lack of knowledge about risk management techniques and practices" was cited as the most common reason for not using explicit risk management techniques in the IWSED-95 survey [18].

Second, we believe that many existing risk management approaches have both practical and underlying, theoretical limitations that hinder the usability of these methods, as discussed in the following.

- Many methods are based on seemingly precise quantification of risks, yet users merely guess the input values for these calculations. This may result in low confidence in the results of risk analysis or -- in the other extreme -- in false confidence in seemingly accurate numbers.

[1] Jyrki Kontio is also affiliated with Helsinki University of Technology. There he can be reached at Otakaari 1, 02150 Espoo, Finland, E-Mail: jyrki.kontio@cs.hut.fi.

- Many methods limit their view on one or few quantifiable metrics, such as cost, schedule and quality, yet in reality additional goals may be affected by risks. Use of a predefined set of goals or attributes in risk evaluation is likely to limit the scope of risk analysis and bias the results.
- Many methods fail to account for different stakeholders and balance their interests in risk analysis. At best, methods attempt to manage two or three stakeholder views assuming that they can reach a consensus view of the risks.
- Few methods provide accurate enough definitions of risks to cover the whole range of aspects associated with risks. The general definition of risk, possibility of loss, is too generic to act as a operational definition on a detail level during risk analysis.
- Finally, hardly any recognize the dangers associated with not accounting for the possible non-linearity of the utility functions, as we have discussed in a separate paper [19].

Given all these potential limitations, it is not surprising that practitioners see limited added value in applying defined risk management techniques. They may not be much worse off by relying on intuition.

Third, while there are several anecdotal descriptions of managing risks in practice [5,13,14,23,33], there are few reports on systematic and scientifically sound evaluations to provide empirical feedback on their feasibility and benefits. Practitioners deserve better proof than war stories told by consultants.

This paper attempts to address the last two of the above problems: we are presenting a method that, we propose, succeeds in avoiding the limitations described above and we are presenting an empirical study design that, we hope, is an example of how more detailed information about risk management process can be captured and subsequently analyzed.

2. The Riskit Method

The Riskit method has been developed to support systematic risk analysis. An attempt was made to design the method so that the common pitfalls listed in the previous section could be avoided. The Riskit method uses a graphical formalism to support qualitative analysis of risk scenarios before quantification is attempted, its risk ranking approach can be selected based on the availability of history data or accuracy of estimates, it supports multiple goals and stakeholders, and its risk ranking approach is based on the utility theory [19].

A central part of the Riskit method the graphical formalism used to document risks, the *Riskit analysis graph.* The Riskit analysis graph is used to define the different aspects of risk explicitly and more formally than is done in casual conversation. The Riskit analysis graph is primarily a communication tool during risk management.

The Riskit analysis graph is used during the Riskit process to decompose risks into clearly defined components, *risk elements*. Its components are presented in Figure 1. Each rectangle in the graph represents a risk element and each arrow describes the possible relationship between risk elements. We will define the components of the graph in the following paragraphs.

A risk factor is a characteristic that affects the probability of a negative event (i.e., risk event) occurring. A risk factor describes the characteristics of an environment, it is not an event itself. Risk factors that are documented typically increase the probability of risks events occurring, but they may also reduce them (e.g., "the team recently developed a similar application").

Each risk factor in the graph can influence one or more risk events. A *risk event* represents the occurrence of a negative outcome. As the arrow and the cardinality indication in Figure 1 show, each risk event can be influenced by many risk factors. However, a risk event does not necessarily have to have a risk factor associated with it. A risk event can also influence the probabilities of other events.

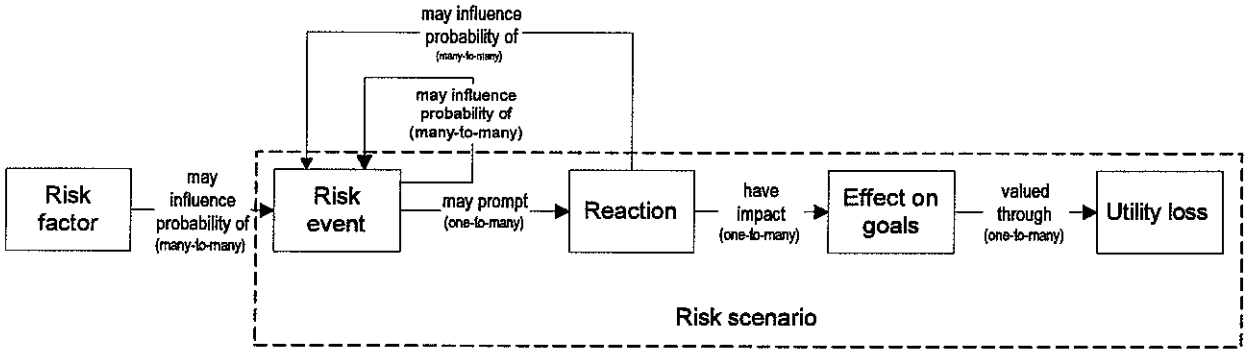

Figure 1: A conceptual view of the elements in the Riskit analysis graph

If a risk event occurs, the resulting situation is rarely accepted as such. Instead, organizations react to the situation to reduce the negative impact of the event. Thus, each risk event is associated with one or more reactions: a *risk reaction* describes a possible action that can be taken as a response to risk event.

The *risk effect* represents the impact of risk event-reaction combination to project goals. Each risk reaction is associated with at least one effect description. The effects are stated for all goals that are affected. For instance, it could be that a risk event was a loss of a key person in a project. Corrective reaction includes search for a new person and training of that person. The final effect on project goals could be a delay (search and training took time) and added cost (search and training costs and reduced productivity).

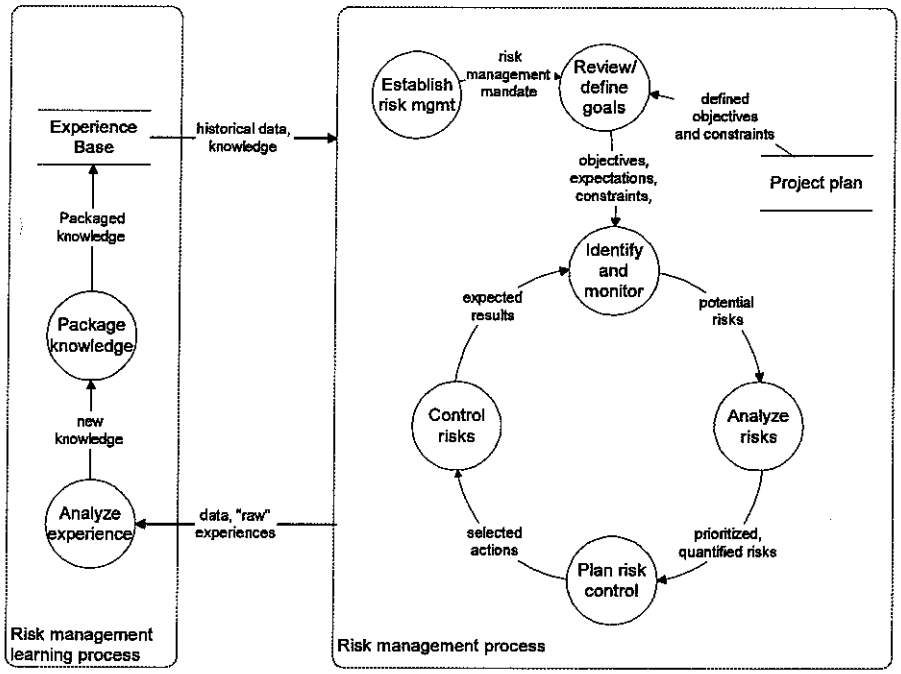

Figure 2: The Riskit risk management cycle

While the effect on goals represents the impact the risk had on each goal, the concept of *utility loss* captures how severe the overall impact of effects has been to different stakeholders. The use of utility function allows the simultaneous consideration of multiple criteria and consideration of several stakeholders. Furthermore, it is likely to result in more realistic evaluation of the losses as the utility functions of stakeholders are likely to be non-linear [1,12] and there may be points of discontinuity in

them. The utility loss is estimated for each relevant stakeholder. Thus, each risk effect has at least one utility loss estimate associated with it.

We have presented an overview of the activities in the Riskit process in Figure 2. We have presented summary descriptions of the steps in the Riskit process in Table 1. As we want to keep the method presentation concise, we will only discuss some selected highlights of the method in the text that follows. Further details are available in a separate publication [19].

Risk is a relative concept and it is always dependent on the goals, expectations and constraints involved. The more realistically we are able to define them, the better we are able to identify and analyze risks. A goal is a general statement of purpose, direction or objective. We identify three types of goals:

- *Objective*: A goal that has an achievable, well-defined target level of achievement, e.g., "develop
- *Driver*: A goal that indicates a "direction" of intentions without clearly defined criteria for determining when the "goal" has been reached, e.g., "minimize the number of defects found".
- *Constraint*: A limitation or rule that must be respected, e.g., "use C++".

The goals are documented using a predefined template [19] and their relevance for each stakeholder is recognized.

Riskit step	Description	Output
Establish risk management	Define risk management infrastructure, i.e., methods, techniques, responsibilities. Define the scope and frequency of risk management.	Risk management infrastructure Risk management mandate
Review and definition of goals	Review the stated goals for the project, refine them and define implicit goals and constraints explicitly. Recognize all relevant stakeholders and their associations with the goals.	Explicit goal definition
Risk identification and monitoring	Identify all potential threats to the project using multiple approaches. Monitor the risk situation.	An list of "raw" risks
Risk analysis	Classify identified risks into risk factors and risk events. Complete risk scenarios for all risk events. Estimate risk effects for all risk scenarios Estimate probabilities and utility losses of risk scenarios using appropriate level of metrics.	Completed risk analysis graphs for all analyzed risks.
Risk control planning	Rank risks scenarios based on their probability and utility loss for each stakeholder, using appropriate ranking method. Select the most important risks for risk control planning. Propose risk controlling actions for most important risks. Select the risk controlling actions to be implemented.	Selected risk controlling actions
Controlling of risks	Implement the risk controlling actions.	Reduced risks.

Table 1: Overview of outputs and exit criteria of the Riskit process

The risk identification process in the Riskit method uses both brainstorming, checklists [6,22], and goal review [19] to produce a list of un-analyzed, "raw" risks. These risks are classified into risk elements and placed on the Riskit analysis graph. Scenarios for all events are completed, i.e., reactions and effects on goals are defined or estimated.

Selecting the highest risk scenarios for risk control planning is straight-forward if ratio scale data is The estimation of probabilities can be based on ratio scale estimates if reliable historical data is available. More often, however, it is more appropriate to either rank risks with each other or assign

ordinal scale values for them (e.g., low, medium, high). Similarly, the utility losses are estimated for each scenario and stakeholder. In a simple situation where there are few goals, scenarios and stakeholders involved, scenario ranking or ordinal scale value assignment can be used. In more complex situations we recommend that multiple criteria decision making support tools are used to elicit utility loss estimates. We have used the Analytic Hierarchy Process (AHP) [28] and Expert Choice software [29] for this purpose as it is has been widely reported as a successful tool for eliciting such preferences [11,15,24,31].

available for both probabilities and utility loss, i.e., the expected utility loss can be used as a metric to prioritize scenarios:

expected utility loss(RS) = probability(RS) * utility loss(RS)

If ordinal scale metrics were used in estimating either one, ranking can be based on ranking scenarios into Pareto-efficient sets, using a simple Pareto-efficient risk sorting method [19]. Simply stated, scenarios that are Pareto efficient over other scenarios but whose are grouped into same category of seriousness.

Finally, risk controlling actions are identified and defined for highest risks and the most effective actions are selected for implementation. The Riskit method provides some guidelines and checklists for this purpose but this process is largely dependent on the individual judgment of participants.

A more complete description of the Riskit method is available in [19].

3. Empirical Study

Evaluating a risk management method is fundamentally difficult. In this section we describe the main constraints that limit our ability to design and perform empirical studies in this field. We have identified some key constraints that make experimentation with risk management methods particularly challenging:

- C-1 The real values for probability and loss are not known, or even knowable.
- C-2 Each set of events occurring in a system is unique and not repeatable.
- C-3 Risk management method cannot be separated from the object of study: if a method results in some action, the state of the system irrevocably changes.
- C-4 Risks are probabilistic phenomena. A single occurrence of a risk, whether predicted or not, cannot be used to draw any conclusions about the accuracy of our risk analysis methods.
- C-5 Introduction of a risk management method changes the behavior of participants in a system.
- C-6 Software projects have relatively long cycle times and are costly.

The above constraints limit the empirical study design options available in risk management. While these constraints are severe, they do not prevent us from applying systematic, scientific principles in our empirical studies. Recognition of these constraints allows us to design such empirical studies that provide more reliable results than anecdotal case descriptions.

In the following we present some highlights of a study performed to evaluate the Riskit method in practice[2]. We recognized the previously listed constraints in the design of the study but attempted to apply some well-known case study principles whenever applicable [4,17,34]. The case study organization was a mature risk management organization with an experienced project manager and project team.

We arranged our case study so that we were able to apply the two risk management methods during the project. As Figure 3 shows, the case study started by a joint session where project goals were reviewed and risks identified. Using the list of risks produced the project manager used the comparison

[2] Note that a full description of the case study is available in a separate report [20].

method to carry out risk analysis the way he normally does it. After this the Riskit method was applied in the analysis of the same set of initial risks. After both analyses the project manager decided on which risk controlling actions he should actually take.

We collected both qualitative and quantitative data on the case study. The qualitative feedback from the method user indicated that Riskit seemed to have had a simpler "interface" – it had clearly defined items that need to be included in the analysis. It also seemed to have provided good summaries of each individual risks. The Riskit method seemed to provide a good overview of the risk situation in the project and it seemed to highlight most important risks well.

The method user expressed more confidence in the results produced by the Riskit method. He considered it a thorough and complete method. In particular, he valued its risk analysis and ranking approach. He also indicated an interest in applying or experimenting with the method, or its components, in future projects.

The case study design (e.g. the joint risk identification session) made it difficult to measure the effort used by the methods. However, if the risk identification is excluded, the Riskit method required 12 hours of effort to use and the comparison method's three hours.

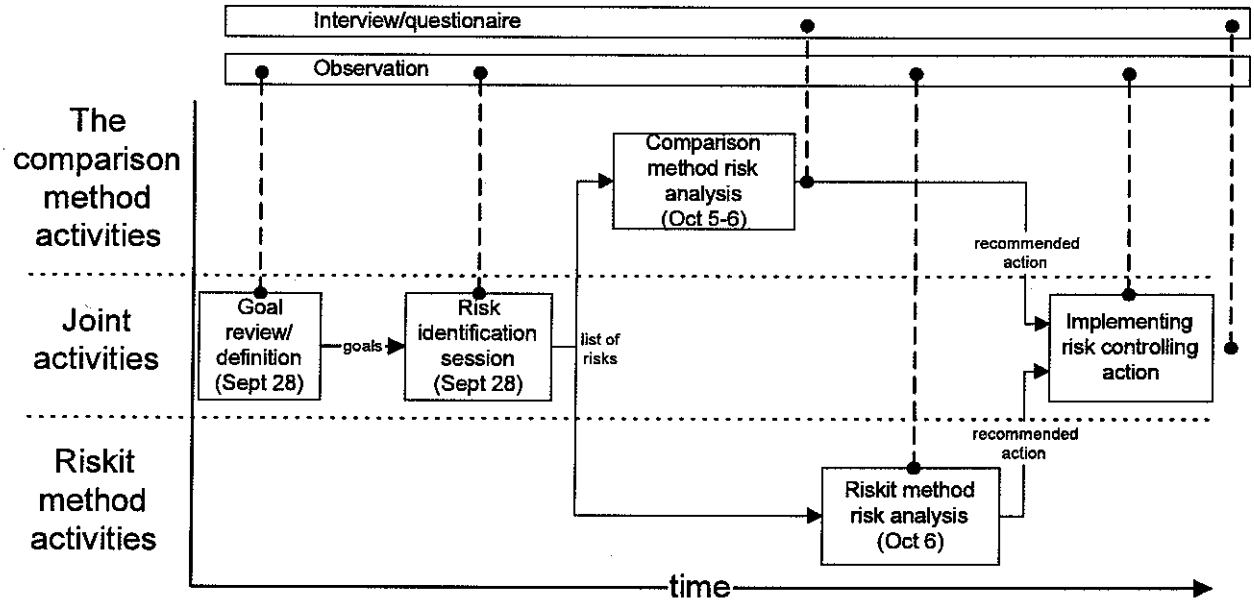

Figure 3: The timeline of case study activities

We analyzed the granularity and coverage of the methods by defining a set of specific metrics for risks and controlling actions that were produced. Risks were made comparable by counting them in different classes: same risks, unique risks, subsumed risks, containing risks and overlapping risks were each counted separately and results summarized [20]. Based on this analysis, the Riskit method analyzed seven comparable risks and the comparison method three. We also calculated *risk coverage ratios* for the methods. We assumed that the union of analyzed risks represents the best available set of all relevant risks in the situation and counted same, subsumed, containing and overlapping risks as one instance each, the resulting risk coverage ratios were 38% for the comparison method and 88% for the Riskit method.

We repeated a similar process for risk controlling actions that were produced. The Riskit method proposed 12 controlling actions and the comparison method seven. The unique controlling actions were nine for Riskit and four for the comparison method. Using the same principle as above, the coverage ratios for risk controlling actions were 75% for the Riskit method and 44% for the comparison method.

We assessed the accuracy of the methods indirectly through the risk controlling actions that were actually taken in the project, vs. the actions that were planned. For Riskit this ratio was 83% and for the comparison method 44% [20].

The goal of this empirical study was to investigate the feasibility of the Riskit method in industrial context. The criteria we defined for determining feasibility were met [20]: the method produced intended results (identified risks, ranked them and proposed controlling action), the overall effort spent on the use of the method was within acceptable limits (20% of the management time of the project, and 2% of the total effort in the project, and the method user gave a positive assessment of the method with respect to its thoroughness, indicated a higher level of confidence in its results and considered its risk ranking approach more sound. Based on these findings we conclude that the Riskit method was a feasible approach in the case study project.

4. Conclusions

This paper presented an overview of a risk management method that has synthesized advances in risk management and management science into an operational method. The method was designed to address some key limitations that we had identified as factors preventing wider use of risk management technology in industry.

We also discussed some empirical study design issues related to risk management and presented an example of a systematic study to evaluate a risk management method. The results of this study suggest that the Riskit method is a feasible method in industrial context. However, it is important to emphasize that the comparative aspect of the study was primarily aimed to aid the qualitative analysis of the two risk management approaches. We are not suggesting that any conclusions can be made about the differences of the methods. Such conclusions and generalizations would require more data points and evidence.

The case study did, however, provide us practical feedback on how risk management is done in practice and what seem to be the strengths and weaknesses of the methods. This feedback was used to improve the method further.

We are currently performing several additional industrial case studies to study the characteristics of the Riskit method further.

5. References

[1] B. W. Boehm. *Software Engineering Economics*, Englewood Cliffs, N.J. Prentice Hall, 1981.

[2] B. W. Boehm, A Spiral Model of Software Development and Enhancement, *IEEE Computer*, vol. 21, pp. 61-72, 1988.

[3] B. W. Boehm. *Tutorial: Software Risk Management*, IEEE Computer Society Press, 1989. pp. 1-469.

[4] D. T. Campbell and J. C. Stanley. *Experimental and Quasi-Experimental Designs for Research*, Boston: Houghton Mifflin Co. 1963.

[5] M. A. Caplan, Risk Management in Practice, 1994. Proceedings of the Third SEI Conference on Software Risk Management. SEI. Pittsburgh, PA.

[6] M. J. Carr, S. L. Konda, I. A. Monarch, F. C. Ulrich, and C. F. Walker. *Taxonomy-Based Risk Identification, SEI Technical Report SEI-93-TR-006*, Pittsburgh, PA: Software Engineering Institute, 1993.

[7] R. N. Charette. *Software Engineering Risk Analysis and Management*, New York: McGraw-Hill, 1989.

[8] R. N. Charette. *Applications Strategies for Risk Analysis*, New York: McGraw-Hill, 1990.

[9] C. Chittister, R. J. Kirkpatrick, and R. L. Van Scoy, Risk Management in Practice, *American Programmer*, vol. pp. 30-35, 1992.

[10] R. E. Fairley. Risk Management: The Key to Successful Software Projects. In: *Proceedings of the 3rd IFAC/IFIP Workshop*, eds. F. J. Mowle and P. F. Elzer. Oxford: Pergamon, 1989.pp. 45-50.

[11] G. R. Finnie, G. E. Wittig, and D. I. Petkov, Prioritizing Software Development Productivity Factors Using the Analytic Hierarchy Process, *Journal of Systems and Software*, vol. 22, pp. 129-139, 1995.

[12] M. Friedman and L. J. Savage, The Utility Analysis of Choices Involving Risk, *Journal of Political Economy*, vol. 56, pp. 279-304, 1948.
[13] A. Gemmer and P. Koch, Rockwell Case Studies in Risk Management, 1994. Proceedings of the Third SEI Conference on Software Risk Management. SEI. Pittsburgh, PA.
[14] R. Hefner, Experience with Applying SEI's Risk Taxonomy, 1994. Proceedings of the Third SEI Conference on Software Risk Management. SEI. Pittsburgh, PA.
[15] S. Hong and R. Nigam. Analytic Hierarchy Process Applied to Evaluation of Financial Modeling Software. In: *Proceedings of the 1st International Conference on Decision Support Systems, Atlanta, GA*, 1981.
[16] D. W. Karolak. *Software Engineering Risk Management*, Washington, DC: IEEE, 1996.
[17] B. Kitchenham, L. Pickard, and S. L. Pfleeger, Case Studies for Method and Tool Evaluation, *IEEE Software*, vol. 12, pp. 52-62, 1995.
[18] J. Kontio, IWSED-95 Web pages. <*None Specified*>, vol. 1995. University of Maryland. World Wide Web. http://www.cs.umd.edu/projects/SoftEng/ESEG/iwsed/iwsed95/.
[19] J. Kontio, The Riskit Method for Software Risk Management, version 1.00, 1996. Computer Science Technical Reports. University of Maryland. College park, MD.
[20] J. Kontio, H. Englund, and V. R. Basili, Experiences from an Exploratory Case Study with a Software Risk Management Method, CS-TR-3705, 1996. Computer Science Technical Reports. University of Maryland. College Park, Maryland.
[21] K. Känsälä. *An Introduction to RiskMethod*, 1993. (UnPub)
[22] L. Laitinen, S. Kalliomäki, and K. Känsälä. *Ohjelmistoprojektien Riskitekijät, Tutkimusselostus N:o L-4*, Helsinki: VTT, Tietojenkäsittelytekniikan Laboratorio, 1993.
[23] D. J. Meyers and D. R. Trbovich, One Project's Approach to Software Risk Management, 1993. Proceedings of the Second SEI Conference on Software Risk Management. SEI. Pittsburgh, PA.
[24] H. Min, Selection of Software: The Analytic Hierarchy Process, *International Journal of Physical Distribution & Logistics Management*, vol. 22, pp. 42-52, 1992.
[25] M. Myerson. *Risk Management Processes for Software Engineering Models*, Norwood, MA: Artech House Publishers, 1996.
[26] P. Rook and A. Cowderoy, Software Risk Management Practice in Industry and Support for Risk Engineering in the GOAL Toolset, 1993. Proceedings of the Second SEI Conference on Software Risk Management. SEI. Pittsburgh.
[27] J. Ropponen, Risk Management in Information System Development , TR-3, 1993. Computer Science Reports. University of Jyväskylä, Department of Computer Science and Information Systems.
[28] T. L. Saaty. *The Analytic Hierarchy Process*, New York: McGraw-Hill, 1990. pp. 1-287.
[29] T. L. Saaty, Expert Choice software 1995, ver. 9, rel. 1995. Expert Choice Inc. IBM. Windows 95.
[30] A. Safafi. Computer-based Risk Management in Software Planning/Scheduling. In: *Proceedings of the 3rd IFAC/IFIP Workshop*, IFAC, 1989.pp. 69-74.
[31] P. J. Schoemaker and C. C. Waid, An Experimental Comparison of Different Approaches to Determining Weights in Additive Utility Models, *Management Science*, vol. 28, pp. 182-196, 1982.
[32] F. J. Sisti and S. Joseph, Software Risk Evaluation Method Version 1.0 CMU/SEI-94-TR-19, 1994. SEI Technical Report. Software Engineering Institute. Pittsburgh.
[33] J. A. Williamson, Experiences with an Independent Risk Assessment Team, 1994. Proceedings of the Third SEI Conference on Software Risk Management. SEI. Pittsburgh, PA.
[34] R. K. Yin. *Case Study Research: Design and Methods*, Thousand Oaks, CA: SAGE Publications, 1994.