CS-TR-3705 August 1996
UMIACS-TR-96-75

Experiences from an Exploratory Case Study with a Software Risk Management Method

Jyrki Kontio[*]*, Helena Englund*[†] *and Victor R. Basili*[*]

[*] Institute for Advanced Computer Studies and
Department of Computer Science
University of Maryland
A.V.Williams Building
College Park, MD 20742, U.S.A.
Email: {jkontio, basili}@cs.umd.edu

[†] Software Metrics Laboratory
Department of Computer & Systems Sciences
Kungliga Tekniska Hogskolan
Electrum 230
S-164 40 Kista, Sweden
Email: d91-hen@nada.kth.se

Version 1.00
Status: Final
Release date: November 1, 1996

Abstract:

This paper presents the results of an exploratory case study in which a risk management method was used and compared with a method currently used by the organization. The goal of the case study was to obtain feedback on an early version of a risk management method, called *Riskit*, that has been developed at the University of Maryland. This paper also presents an overview of Riskit method version 0.10 and describes the comparison method currently used by the case study organization, as well as the case study design.

Table of Contents

List of Figures

List of Tables

1. Introduction

This paper presents the results of an exploratory case study in which a recently developed risk management method was used and compared with a method currently used by the case study organization. The primary goal of this work was to obtain feedback on an early version of a risk management method that had been developed at the University of Maryland. The method, called *Riskit*, is based on a graphical modeling technique that supports qualitative analysis of risks. This case study used an early version of the method (version 0.10) and the results of the case study were used to improve the method.

This paper presents the Riskit method version 0.10, the comparison method currently used by the case study organization, as well as the results of the case study that was performed.

2. Acknowledgments

We would like to thank the Software Engineering Laboratory for the opportunity to carry out the case study described in this report. Sharon Waligora (CSC) recommended the study and lead to Jean Liu (CSC) who was instrumental in finding a suitable project to work on. Sharon also gave us valuable comments on earlier versions of this report. We are also grateful to Scott Green (NASA) who supported the experiment from NASA's side and provided feedback on this report. Filippo Lanubile helped us to discuss our experimental design and arrangements more thoroughly. The biggest contribution, however, to the project was given by Thomas Gwynn of the Computer Sciences Corporation. He made much of his time and expertise available for the case study and his comments and insights proved to be essential in the execution and analysis of the study.

3. Motivation for Risk Management

Software development is often plagued with unanticipated problems that cause projects to miss deadlines, exceed budgets, or deliver less than satisfactory products. While these problems cannot be eliminated totally, some of them can be controlled better by taking appropriate preventive action. Risk management is an area of project management that deals with these threats before they occur. Organizations may be able to avoid a large number of problems if they use systematic risk management procedures and techniques early in projects.

Several risk management approaches have been introduced during the past decade (Boehm, 1989; Charette, 1989; Carr et al. 1993; Karolak, 1996) and while some organizations, especially in the U.S. defense sector (Boehm, 1989; Edgar, 1989), have defined their own risk management approaches, most organizations do not manage their risks explicitly and systematically (Ropponen, 1993). Risk management based on intuition and individual initiative alone is seldom effective.

When risk management methods are used, they are often simplistic and users have little confidence in the results of their risk analysis results. We believe that the following factors contribute to the low usage of risk management methods in practice:

- Risk is an abstract and fuzzy concept and users lack the necessary tools to define risk more accurately for deeper analysis.
- Many current risk management methods are based on quantification of risks for analysis and users are rarely able to provide accurate enough estimates for probability and loss for the analysis results to be reliable.
- Risks have different implications to different stakeholders. Few existing methods provide support for dealing with these different stakeholders and their expectations.
- Each risk may affect a project in more than one way. Most existing risk management approaches focus on cost, schedule or quality risks, yet their combinations or even other characteristics (such as future maintenance effort or company reputation) may be important factors that influence the real decision making process.
- Many current risk management methods are perceived as complex or too costly to use. A risk management method should be easy to use and require a limited amount of time to produce results, otherwise it will not be used.

Given the increasing interest in risk management in the industry, we believe that for risk management methods to be applied more widely, the risk management community will need to address the above issues. Furthermore, risk management methods should also provide comprehensive support for risk management in projects, they should provide practical guidelines for application, they should support communications between participants, and they should be credible. The Riskit method was developed to address these issues.

4. The Riskit Method, version 0.10

This section presents an overview of the Riskit method as it was defined when the case study was carried out (Kontio, 1995). It is important to point out that a new version of the method is being released at the time of writing of this report (Kontio, 1996), largely based on the feedback obtained during the case study described in this report.

4.1 Decomposing Risk: The Risk Analysis Graph

In everyday language risk can mean various things, it can refer to a possibility of loss, it can mean events that cause loss, it can refer to objects, characteristics or factors that usually are associated with danger or loss (Anonymous, 1992). Clearly, the range of different meanings associated to the word risk is too broad for accurate discussion and analysis.

The *Riskit analysis graph* is a graphical formalism that is used to define the different aspects of risk more formally. The Riskit analysis graph can be seen both as a conceptual template for defining risks, as well as a well-defined graphical modeling formalism. In both cases, it can be used as a communication tool during risk management.

When we use the term risk on its own, we are using it in its original, somewhat fuzzy meaning: risk is defined as *a possibility of loss or any characteristic, object or action that is associated with that possibility.* The two important characteristics of risk are loss and uncertainty. Despite the obvious disadvantages of such broad definition, we have noticed that in the early stages of risk identification and analysis it is beneficial to have such a "fuzzy" concept to facilitate discussion.

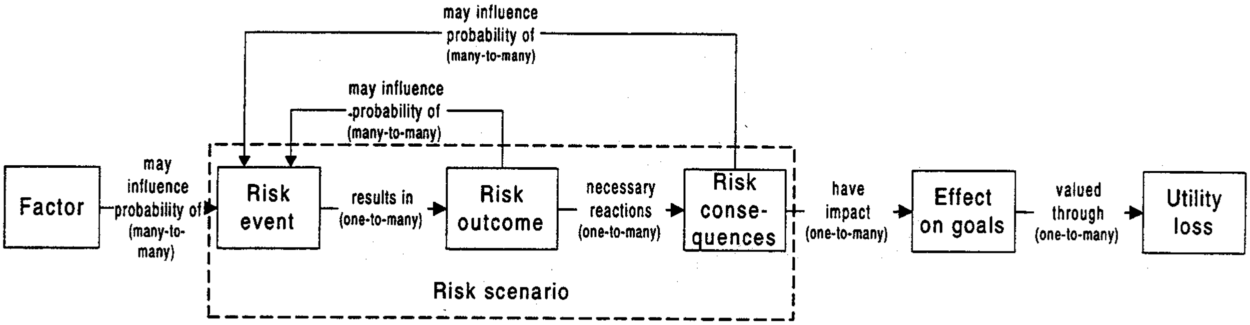

may influence probability of (many-to-many)
may influence probability of (many-to-many)
Factor
may influence probability of (many-to-many)
Risk event
results in (one-to-many)
Risk outcome
necessary reactions (one-to-many)
Risk consequences
have impact (one-to-many)
Effect on goals
valued through (one-to-many)
Utility loss
Risk scenario

Figure 1: Definition of the Riskit analysis graph[1]

The Riskit analysis graph is used during the Riskit process to decompose risks into clearly defined components, *risk elements*, as we call them in this document. The components of the Riskit analysis graph are presented in Figure 1. Each rectangle in the graph represents a risk element and each arrow describes the possible relationship between risk elements. The relationship arrow is read in the direction of the arrow, that is, "*[a] factor may influence the probability of [a] risk event*". We have also defined the allowed cardinalities[2] of these relationships, written in parenthesis on each relationship arrow, read in the direction of the arrow. We will define the components of the graph in the following paragraphs.

Risk element	Software Engineering Examples	General Examples
Risk factor	• inexperience of personnel • use of new methods • use of new tools • unstable requirements[3]	• a high cholesterol diet • living near a fault line of earth's plates (e.g., San Francisco) • wet (slippery) driving conditions
Risk event	• a system crashes • a key person quits • extra time spent on learning a method • A major requirements change	• a doctor's diagnosis of a patients heart problem • an earthquake • a car accident
Risk outcome	• the system out of service for a time, some data lost • knowledge is lost, effort shortage • less time spent on actual development	• awareness of the heart problem • buildings collapse, injuries to humans • car demolished, passenger injuries
Risk consequence	• system operational after delay, back up data restored • recruiting process initiated, staff reassigned	• treatment of heart problem • reconstruction of roads and building • treatment of injuries, purchase new car
Risk Effect	• added cost $50K • two calendar-month delay • some functionality lost • reputation as a reliable vendor damaged	• hospital stay, cost of medical care • cost and inconvenience of reconstruction, loss of human life, medical expenses • medical costs, permanent injury effects, raised insurance premiums

Table 1: Examples of risk elements

[1] Note that in the later versions of the method this has been modeled differently, i.e., "event" and "outcome" are combined and "consequence" is replaced by a "reaction".

[2] In this context cardinality refers to the number of allowed connections between risk elements. E.g., in Figure 1 the one-to-many relationship between "risk outcome" and "risk consequence" indicates that each risk outcome can have more than one risk consequence but each risk consequence can only have one risk outcome associated with it.

[3] Note that this is different from "a change in requirements", which would be a risk event. When defined as a factor, "unstable requirements" refers to the characteristics of the situation.

A risk factor is a characteristic that affects the probability of a negative event (that is, risk event) occurring. A risk factor describes the characteristics of an environment, it is not an event itself. Examples of risk factors are listed in Table 1. Risk factors that are documented typically increase the probability of risk events occurring, but they may also reduce them (e.g., "the development team recently developed a similar application").

The purpose of risk factors is not to document all possible characteristics that may influence a risk event as there may be an infinite number of such factors. Instead, a risk factor is relative to the general assumptions made for the situation (e.g., project), that is, it documents aspects that are somehow different from the "normal" situation. As the arrow in Figure 1 shows, each risk factor can influence one or more risk events.

A *risk event* represents the occurrence of a negative incident – or a discovery of information that reveals negative circumstances. Risk event is a stochastic phenomenon, that is, it is not known for certain whether it will happen or not. This uncertainty can be characterized by a probability estimate associated to the risk event. Examples of risk events are listed in Table 1.

As the arrow in Figure 1 shows, each risk event can be influenced by many risk factors. However, a risk event does not have to have a risk factor associated with it. Each risk event results in one or more risk outcomes. In case there are more than one risk outcome associated with the risk event, the different outcomes represent stochastic relationships.

The *risk outcome* describes the state of the project domain[4] after the risk event has occurred and before any corrective reaction is taken. Risk outcome essentially describes the immediate situation after the risk event. Examples of risk outcomes are listed in Table 1. Risk outcomes can influence the probabilities of other risk events. If the influence is stochastic, they are have a similar relationship as a risk factor has to a risk event. In case of a deterministic relationship (that is, a risk outcome directly results in another risk event) the outcome of the resulting deterministic risk event should be included in the original risk outcome.

If a risk event occurs, the resulting outcome is rarely accepted as such. Instead, organizations take some corrective reaction[5] that reduces the negative impact of the risk event. The *risk consequences* represent the state of project domain after corrective reaction has been taken. Examples of risk consequences are listed in Table 1. These corrective reactions are an important part of understanding what is the overall impact of the risk event to the project domain. Each risk outcome is associated with one or more risk consequences, as shown by the one-to-many relationship arrow the corresponding arrow in Figure 1. Risk consequences may also influence the probabilities of other risk events, as indicated by the arrow in Figure 1.

The *risk effect* represents the impact of risk scenario to project goals after risk has occurred and corrective reactions have been carried out. 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). Examples of different effects on goals are listed in

[4] Project domain refers to all relevant characteristics of the project and organization.

[5] Note that we use the term "corrective reaction" to action that is taken after the risk event occurs, as opposed to controlling actions that are taken before risk events occur.

Table 1. Each risk consequence can have one or more risk effects associated with it (see Figure 1).

Symbol	Definition
Factor <name>	**Risk factor.** Represents risk factors. Risk factors name is entered in the symbol. May be connected from the right-hand side to one or more risk events.
Event <name> Prob:	**Risk event.** Represents risk events. Event name in entered in the symbol and the probability of the event entered in the "Prob:" field. Need to be connected to one or more outcomes.
Outcome <name> Desc:	**Outcome.** Represents the outcome of the risk event. Descriptive name of the outcome entered in the symbol. Description of the outcome can be included if required. Need to be connected to one or more consequences.
Consequence <name> Desc:	**Consequence.** Represents the consequences and actions that may be taken after the risk event has resulted in an outcome. Descriptive name of the consequence entered in the symbol. Additional description of the consequence or actions included in it. Need to be connected to one or more effects.
Effect <goal1>: <goal2>: <goal3>: <etc.> Impact: <impact>/ <stakeholder>	**Effect.** Effect of a scenario to project goals. Each goal is listed and the scenarios effect on it is described. The effect on goals is expressed using the same metric or description as were used when the goal was defined. The effect is entered as a positive or negative value on each goal and the unit of measure must be included. A zero ("0") is used to indicate that there is no impact for a given goal. Thus, the format is: <sign> <effect> <unit> Below are some examples: Sched: + 2 mo two month increase in project duration Cost: -$100 K a $100,000 decrease in project cost Func: -undo feature the "undo" function will not be available in the system The field "Impact" indicates the total effect on stakeholders' utility. If more than one stakeholder are included in the analysis, the stakeholders are each listed separately.
Action: <description>	**Action.** Risk reducing actions that are planned. The targeted impact on Riskit analysis graph entities is marked by arrows. Actions can be expressed in three ways. Potential actions that have been considered but whose decision whether to implement them or not has not been taken are marked with dashed ovals. Actions that should be taken are marked with solid border. Actions that have already been implemented are marked with a checkmark attached to the action symbol.
————→	**Deterministic connector.** Represents a certain relationship between risk elements in the Riskit analysis graph.
--------→	**Stochastic connector.** The causality between risk elements is either probabilistic or can be decided.
---+/- ---→	**Factor-event connector.** A stochastic connector between risk elements. A positive sign represents an increase in the probability of an event, a negative sign a decrease in the probability.

Table 2: Riskit analysis graph symbols

While the effect on goals represents the impact the risk had on each goal, the concept of *utility loss* captures how severe the loss has been to different stakeholders. The concept of utility loss is based on the utility theory[6], a concept used in economics and decision theory (Von Neumann and Morgenstern, 1944; French, 1989). Increased costs that are within the limits of project contract may not have any meaningful utility loss associated with the project manager. However, the customer paying the bill will consider this loss higher. Also, analyzing utility loss separately allows more appropriate consideration for non-linear and discontinuous utility functions[7].

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

We use the term *risk scenario* for any unique event-outcome-consequence combination. Risk scenario is marked in Figure 1 with a named rectangle. Each such scenario can be associated with risk effect and, correspondingly, a set of utility losses. Examples of risk elements can be seen in Figure 3.

The risk elements can be visually represented in the *Riskit analysis graph.* The Riskit analysis graph is based on a graphical modeling formalism developed to support the modeling of risk elements and risk scenarios. The definition of Riskit analysis graph symbols is given in Table 2.

4.2 The Riskit Risk Management Process

This section presents an overview of the Riskit method as it was used during the case study (i.e., version 0.10 of the method). More details are available in a separate report (Kontio, 1995). The updated method has been documented separately (Kontio, 1996).

The risk management cycle in a project can be viewed as consisting of some basic activities: review and definition of goals; risk identification and monitoring; risk analysis; risk control planning; and controlling of risks. The flow of information between these activities is represented in Figure 2. The activities in Figure 2 are represented by circles (process symbols in the dataflow diagram notation used) and the arrows represent information flows between entities. Each of the activities can be instantiated several times during the project duration and they may be enacted concurrently. However, the most critical instances of the risk management cycle are the ones enacted in the beginning of the project.

The risk management approach used in the Riskit method aims at proactive risk management, it attempts to identify actions that can be taken before risks occur, including making contingency plans (that is, the action of planning for reactions should the risks occur). Strictly speaking, once a risk occurs, it is no longer a risk but a problem that needs attention.

[6] The utility theory states that people make relative comparisons between alternatives based on the utility (or utility loss) that they cause. The utility is the level of satisfaction, pleasure or joy that a person feels or expects.

[7] There are strong reasons to assume that utility functions are both non-linear (Friedman and Savage, 1948; Boehm, 1981) and there are points of discontinuity in it.

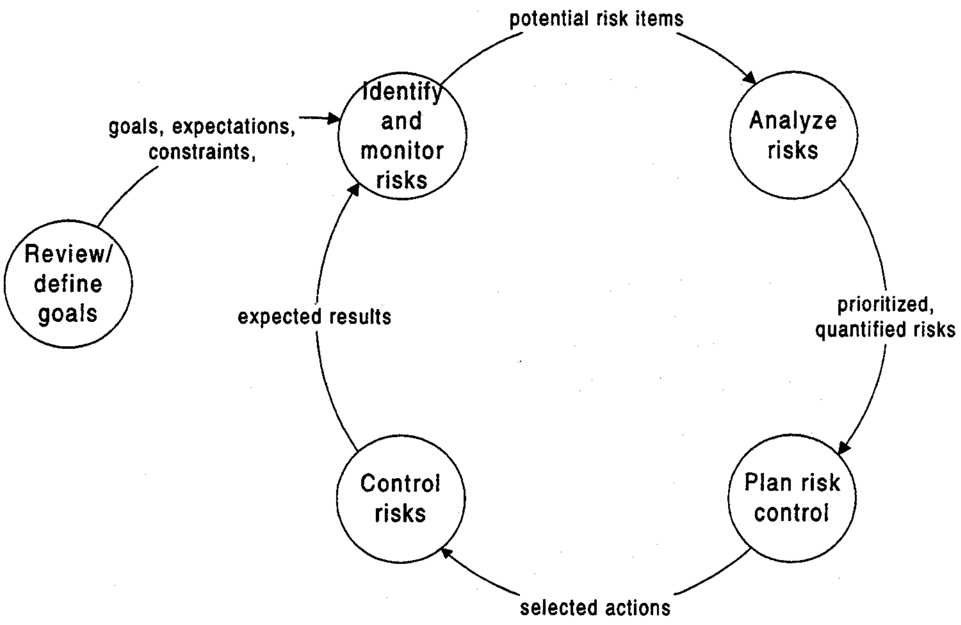


Figure 2: The Riskit risk management cycle

Riskit step	Description	Output
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 and constraints.	Explicit goal and constraint definition
Risk identification and monitoring	Identify all potential threats to the project using multiple approaches. Monitor the risk situation.	An unanalyzed list of potential 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.	Completed risk analysis graphs for all identified risks.
Risk control planning	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 3: Overview of outputs and exit criteria of the Riskit process

4.2.1 Review and Define Goals

Risks do not exist without a reference to goals, expectations or constraints that are associated with a project. If goals are not recognized, the risks that may affect them may be ignored totally or, in the best case, they cannot be analyzed in any detail as the reference level is not defined. Some of a project's goals typically have been explicitly defined but many relevant aspects that influence management decisions may be implicit. Therefore, it is necessary to begin the risk management process of a project by a careful review, definition and refinement of goals and expectations that are associated with a project.

A goal is a general statement of purpose, direction or objective. We have used the term goal in a broad meaning in this text. When defined more accurately, there are three types of possible goals:

Objective: A goal that has an achievable, well-defined target level of achievement, e.g., "drive from A to B in one hour".

Driver: A goal that indicates a "direction" of intentions without clearly defined criteria for determining when the "goal" has been reached, e.g., "drive from A to B as fast as you can"..

Constraint: A limitation or rule that must be respected, e.g., "... while obeying all traffic laws".

The Riskit process is initiated by a review of project's goals, which often leads to definition of some additional, previously implicit objectives, drivers and constraints. The purpose of this step is to produce formal definitions of these issues for the stakeholders that the project manager must satisfy. The goals and constraints are expressed using the template presented in Table 4.

Goal attribute	Description
Name	Name of the goal.
Type of goal	Objective / driver / constraint
Description	Description of the goal.
Stakeholder(s)	Names of the stakeholders for the goal.
Measurement unit	Measurement unit used for the goal (e.g., $, date, or person-month).
Target value	Target value for the goal. Relevant for objectives and possibly for constraints.
Direction of increasing utility	Definition of whether an increase or decrease in goal value increases the utility near the target. I.e., whether an increase in goal value is good or bad. Stated as "growing" or "decreasing".
Required value range	Minimum or maximum value required for the goal.

Table 4: Goal and constraint definition template

As Table 4 indicates, goals are linked to different stakeholders that are affiliated with a project. This information will later be used in risk analysis to compare and rank risks. The stakeholders also determine the scope of a project's risk management mandate: which stakeholders are to be defended by the project's risk management activities and which are beyond the risk management mandate of the project. This needs to be explicitly defined for the project, possibly including a prioritization of stakeholder interests.

The goals and constraints are often defined in the project plan or the project contract. However, all the goals and, especially, constraints may not be in these documents. For instance, efficient resource utilization may be an important consideration for the contractor but this typically is not considered a project goal. However, if these goals are real for some of the stakeholders in the project, they must be included in the risk management process. Goals and constraints can typically be found in the following areas:

- schedule
- resources used, most often personnel time
- cost of development
- product requirements, which can include both functional and other quality characteristics.
- resource utilization
- technical constraints, such as hardware platforms, operating systems and use of particular software tools

The goal review can be considered completed when project manager and stakeholders have agreed on the goals and they are formally defined. However, the goal definition process may often need to be re-initiated as new goals are identified during the risk analysis process.

4.2.2 Identify and Monitor Risks

The identify and monitor activity is enacted more thoroughly in the beginning of the project and repeated frequently later in the project as the risk situation is monitored.

The goal of the initial identify and monitor activity is to identify all possible risks that the project may face. It produces a gross list of potential risk factors and risk events for the project, possibly some risk outcomes as well. There are various techniques that can be used to facilitate effective risk element identification, such as brainstorming, checklists (Boehm, 1989; Carr et al. 1993; Karolak, 1996), critical path analysis, and review of goals.

The later instances of the identify and monitor process rely on the results of the initial identification process. The goal of these later process instances is to identify any changes in the risk situation. Changes can include identification of new risks, changes in the risk factor or event information or the consequences of the risk events. The Riskit analysis graph is used as a supporting tool to discuss possible changes.

The risk identification and monitoring activity can be considered completed when the participants have agreed that the produced risk list is comprehensive enough for the project's purposes. The output of the activity is a "raw" list of risks, i.e., each risk has been briefly described.

4.2.3 Risk Analysis

Risk analysis is a process where the information from the identify and monitor process is used and risks are analyzed in detail. The purpose of this activity is to provide detailed descriptions of project's risks so that highest risk elements and appropriate risk controlling action can be planned and implemented in the next step of the Riskit cycle.

The Riskit analysis process consists of the following steps:

- 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.

The first step, classifying risks into risk factors and risk events, is based on the risk list produced during the identification and monitoring step. The categorization is based on the definitions given in section 4.1 and results are documented in the Riskit analysis graph (Table 2). An example of a Riskit analysis graph is given in Figure 3.

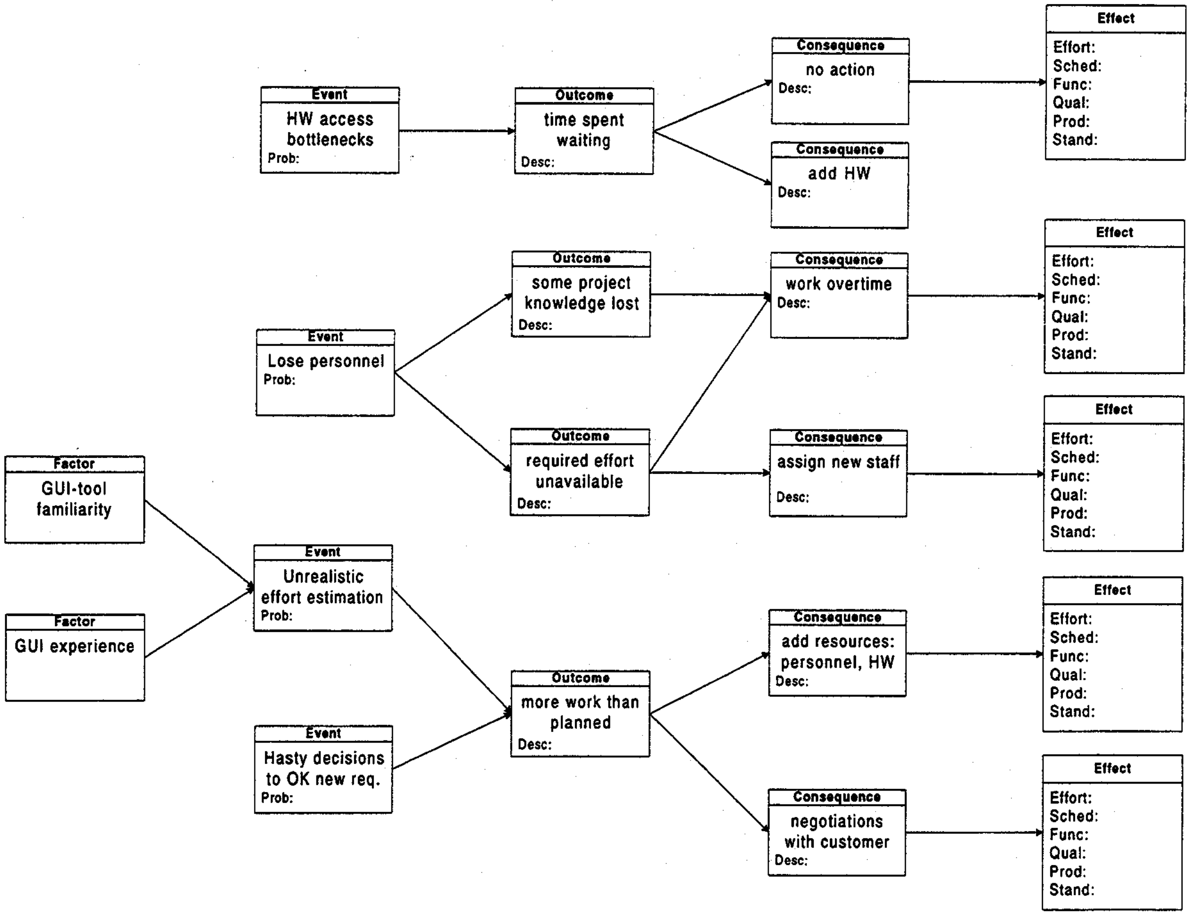


Figure 3: The Riskit analysis graph example

The classification of risks into factors and events is supported by two templates that augment and formalize the graphical presentation of the Riskit analysis graph. Table 5 and Table 6 present these two templates.

Risk factor attributes	Description
Name	Name of the risk factor to be used as an identifier.
Description	Description of the risk factor.
Normal/assumed reference level	Description of the "normal" level for the risk factor.
Project's risk factor state	Description of the risk factors state for the project

Table 5: Risk factor attribute table

Risk event attributes	Description
Name	Name of the risk event to be used as an identifier.
Description	Description of the risk event.
Probability of occurrence	Assessment of the probability of the event occurring.
Uncertainty of the estimate	Assessment of the uncertainty in the probability assessment.
Information source	Description of sources of information about the risk event for monitoring the changes in the probability or event occurrence.

Table 6: Risk event attribute table

As factors and events are being reviewed and positioned on the Riskit analysis graph, the relationships between the two are documented by "influence" arrows Table 2.

The classification process also reviews the listed risks and, when necessary, combines, decomposes or even deletes risks as they are discussed. It is also likely that new risk factors or events may be recognized during the classification process.

The next step in the analysis is to define risk scenarios for all risk events, i.e., define risk outcomes and risk consequences in a scenario. Each risk event has at least one risk outcome, in which case there is a deterministic "result in" relationship between the event and the outcome. Sometimes the outcome may be probabilistic and more than one possible outcome needs to be defined. In such a case, a stochastic connector is used to indicate "may result in" relationship (see Table 2). Similarly, there is at least one risk consequence for each risk outcome (marked by a deterministic relationship) but sometimes alternative lines of action need to be considered and they are marked with a stochastic relationship connector. Templates for risk outcome and risk consequences are presented in Table 7 and Table 8, respectively.

Risk outcome attributes	Description
Name	Name of the risk outcome to be used as an identifier.
Description	Description of the outcome after the risk occurrence. Describes the project state after the event before any other action is taken and this does not need to be directly linked to project goals.
Certainty of the outcome	Assessment of the probability of the outcome if the risk event occurs (when not deterministic).

Table 7: Risk outcome attributes

Risk consequence attributes	Description
Name	Name of the risk consequence to be used as an identifier.
Description	Description of the risk consequence, i.e., the results of possible set of actions that may be required to correct the situation. Note that some of the consequences should be mutually exclusive.

Table 8: Risk consequence attributes

After the risk scenarios have been completed, the risk effects on goals are estimated. Depending on the estimation methods and tools available, the effects can be stated qualitatively (e.g., as textual descriptions or classifications high/medium/low) or quantitatively. Ranges can be expressed as well, if participants consider this necessary.

Not all goals are affected by all risk scenarios and sometimes the effects may be positive for some goals (e.g., loss of personnel may reduce costs while delaying schedule and limiting functionality). Effects on goals are documented in the Riskit analysis graph with the dedicated symbol (see Table 2).

The final step in risk analysis is to rank or estimate the probabilities and utility losses for each risk scenario. The Riskit method itself does not dictate how accurate these estimates are. They may be estimates based on historical data and expressed in ratio scale metrics (e.g., probabilities of events) or they may be ordinal scale rankings of items (Fenton, 1991). As a general rule we suggest that estimates are done using the type metrics that can be supported by the available data or experience. If relevant, reliable historical data exist on probabilities of the events, probabilities may be stated in percentage points. If reliable methods are used to elicit utility loss estimates (e.g., (Saaty, 1990)), they may be expressed in ratio scale preference values. However, it may often be more practical to use ordinal scale rankings or classification categories for this purpose. The goal of risk management is primarily to *identify* the most important risks to be controlled. This identification does not require precise *quantification* of risks.

The utility losses should be estimated separately for all different stakeholders that are to be defended against risk under the risk management mandate of the project.

The probabilities and utility losses are marked in the appropriate risk element symbols in the Riskit analysis graph (see Table 2).

4.2.4 Plan Risk Control

Once the risks have been analyzed and ranked, possible controlling action is planned. The goal of this activity is to determine which risk control activities are necessary to take. This involves three main steps:

- Select the high risk scenarios to be considered for risk control.
- Define possible preventive risk management action for each high risk scenario.
- Select cost-effective actions for all high risk scenarios.

The Riskit method does not advocate any strict rule in determining what are the highest risk scenarios to be controlled. Traditionally, *risk exposure* (i.e., probability * loss) has been used as a metric for risk. If scenario probabilities and utility losses were quantitatively estimated, risk exposures of different scenarios can be used to select highest risk scenarios.

If either probability or loss has been estimated using an ordinal scale, high risk scenarios must be selected using a more qualitative approach, i.e., ranking scenarios into pareto optimal[8] sets, considering scenarios that are in the highest sets, and continuing selection into lower sets until risk scenarios become so insignificant that they do not require any further consideration.

[8] A choice *a* is considered pareto optimal over *b* when $\forall\ i\ a_i >= b_i$ and $\exists\ i\ a_i > b_i$ (French, 1986; Keeney and Raiffa, 1976).

Once the high risk scenarios have been selected, possible controlling actions are proposed for each of them. Identifying possible controlling actions is a creative process and can be carried out in a free format manner. We have also used a simple taxonomy of risk controlling actions as a checklist to verify that no obvious categories of actions are ignored. This taxonomy is presented in Figure 4.

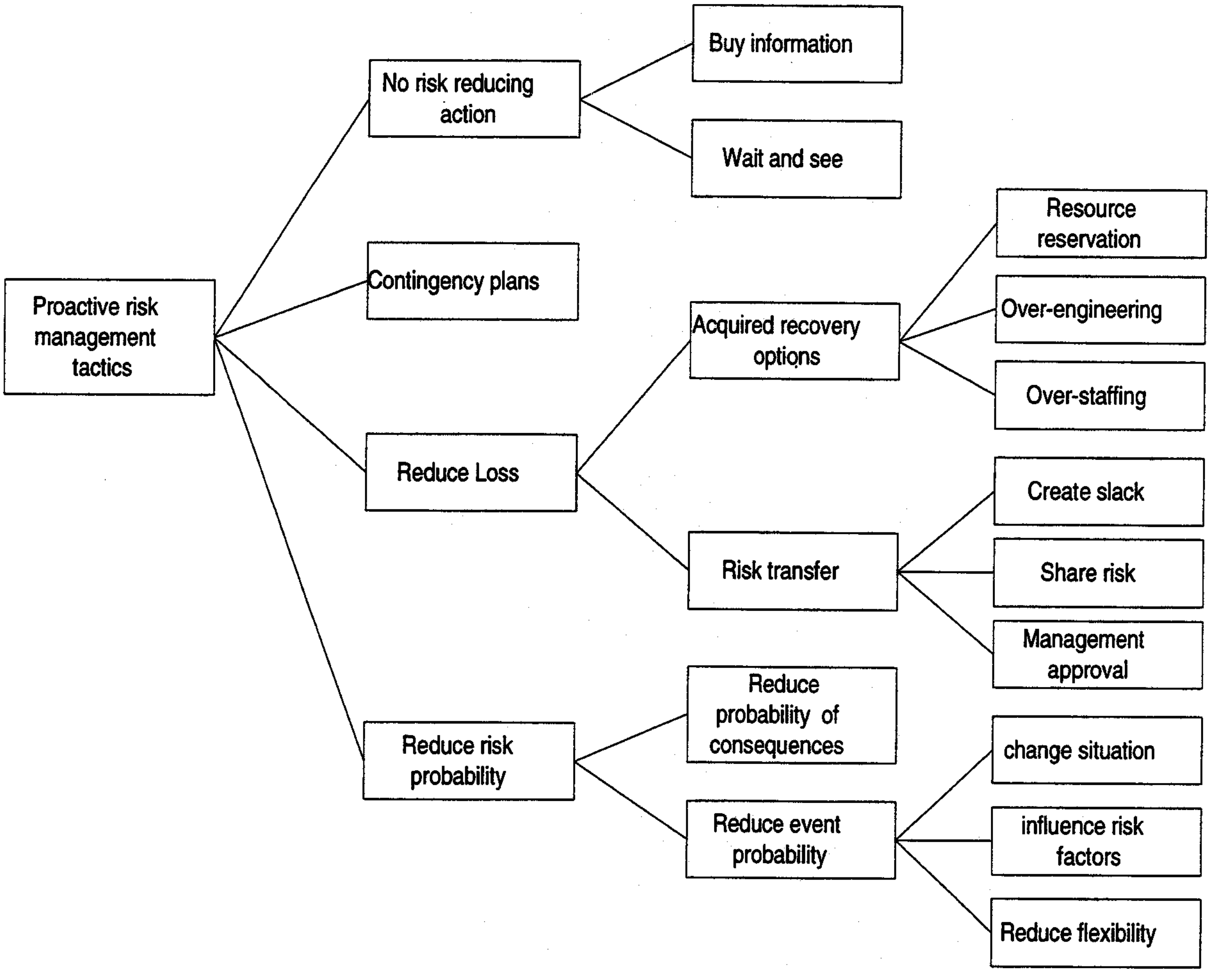


Figure 4: Options for risk management decision making

The first set of options in Figure 4, *no risk reducing action* means that an organization does not take any immediate action to prepare for risk or to reduce risk. *Buying information* is an option that is used when the management does not have enough information to decide what to do about a risk and there is a possibility to obtain more information. In principle, it is only a temporary option that results in a new decision as the information becomes available. After additional information becomes available, some of the other options are selected. Buying information can take many forms. Sometimes information can be literally bought from outside sources, such as market research organizations or by hiring a consultant that knows about the area that risk is relevant to. However, more typical way of buying information is to develop prototypes, run simulations, initiate feasibility studies or conduct, e.g., performance tests.

The *wait and see* option can be used in two situations. First, it is a good option for all risks that are considered to be small enough not to require any other action. Second, it can also be considered when there are no inexpensive ways of obtaining additional information and a major part of the risk is in the uncertainty of the magnitude of the risk itself. In other words, the ranges of estimates of risk are wide and management has no special reason to believe that higher risk estimates are probable. This option, in fact, would be the same as the reactive strategy we discussed earlier. Clearly, using this option to cover high uncertainty risks is, to say it simply, risky. A conservative approach would be to use some of the other options for high uncertainty risks.

Contingency planning means that recovery plans are made for a risk. These plans should describe the actions that will be taken if the risk occurs. Note that this option does not imply that any other preparations are made. Plans are written and approved and they are put on the side and used only if risks occur. Contingency plans do not reduce risk, or loss, to be exact. They help organization to make sure that there is a way to recover from the risk. Contingency plans, in effect, are a way to detail the size of loss.

The options under the term *Reduce loss* build upon recovery plans and include some additional actions that reduce the loss that would result if the risk were to occur. The *Acquired recovery options* refers to a set of actions that buy options that can be used to limit the loss. They typically have a cost associated with them. The *Resource reservation* option refers to a situation where some resources are reserved for limiting the impact of risk if the risk occurs. Resources can be human, computer or financial. *Over-engineering* mean implementing some features in the product or design so that there will be alternative ways of action if the risk occurs. For instance, Over-engineering could mean that extra effort is spent during design or coding to make sure that alternative system architecture or compilers can be used. *Over-staffing* may be introduced to make sure that more than one person knows enough about each area in the project. All these actions buy different options that can be started if risks occur.

Risk transfer can include three different options. The most straight-forward way is to *create slack* in the aspects of project are threatened, i.e., relax objectives of constraints. In other words, lengthen the schedules, make more memory available, or increase budget. Due to competitive situations this may be often difficult. However, if risks are analyzed and communicated well to the management and customers of the project, this option is likely to work better than without risk management.

It is also possible to *share risks*. Sharing can happen, e.g., with customers or subcontractors of the project. Again, a critical issue is to analyze the risks well and communicate their significance to all stakeholders. This typically requires, sometimes lengthy, contractual negotiations.

It is also possible to obtain a *management approval* for some risks. In such a case the management accepts the risk and takes the responsibility for it. Project is still responsible for monitoring the risk but additional actions are not taken. This option may be used when a project is very important for the organizations and there are no available resources for reducing risk.

Reducing the probability of risk can take many forms and is dependent on the type of risk that is to be managed. We have divided this into two categories, *reduce event probability* and *reduce probability of negative consequences* if the risk occurs. For instance, personnel unavailability probabilities can be reduced, to some degree, by financial incentives (project reward on completion) or by addressing the causes that may result in personnel unavailability. Good engineering or design practices can diminish the probability of performance or memory problems.

Once the potential risk controlling actions have been identified, their costs and estimated impacts need to be estimated. The selection of appropriate actions is based on the available resources for risk control and risk reduction effectiveness of the proposed actions. In principle, actions with highest risk reduction leverage[9] (Boehm, 1989) while monitoring that the risk control budget is not exceeded (e.g., some risk controlling action may have a very high risk reduction leverage but the overall cost may be too high for the available budget).

The controlling actions can be presented in the Riskit analysis graph to document their intended and estimated impact. This is done by a specific symbol, an oval, that has arrows pointing to the entities that are targeted (see Table 2). This will highlight how each risk reducing action is intended to influence the risks.

4.2.5 Risk Control

The control process implements the risk controlling actions. From the perspective of the Riskit method this is a project management activity that is not explicitly supported by the Riskit method. However, as risk controlling actions are implemented, they are marked with a checkmark in the Riskit analysis graph. As new information about risks becomes available, the identify and monitor activity may be initiated.

5. Case Study Design

5.1 Case Study Organization

This case study was carried out at the Software Engineering Laboratory (NASA, 1995). The SEL is a partnership organization that was established in 1976 at NASA Goddard Space Flight Center (GSFC) by its Flight Dynamics Division (FDD), Computer Sciences Corporation (CSC) and the department of Computer Science at University of Maryland. The SEL was established for understanding and improving the software products and development process in the FDD. The SEL has a consistent and long track record of systematic process improvement and in 1994 it was awarded the first IEEE Computer Society Software Process Achievement Award to "recognize its outstanding achievements in software process improvement" (McGarry et al. 1994).

The SEL has also been a working example of the Experience Factory and Quality Improvement Paradigm in practice (Basili et al. 1992). The software product and process improvement in the SEL have been improved over the years based on systematic data collection, analysis and organizational learning (Basili and Green, 1994).

The SEL supports the software development within the FDD. Software developed by the FDD is mainly scientific applications that process data received from earth orbiting satellites in the areas of orbit, attitude and mission analysis. The total FDD software development staff,

[9] Risk reduction leverage is defines as $\frac{\text{Risk Exposure}_{before} - \text{Risk Exposure}_{after}}{\text{Risk Reduction Cost}}$

including contractor support, is approximately 250-275, and about half of this is allocated to software maintenance. Typical project involves between 5 to 25 staff members and results in system size of 100-300 KSLOC. The SEL itself has a staff of 10-15 analysts (McGarry et al. 1994).

The project selected for study was a small utility that was part of the Flight Dynamics Support System (FDSS) developed by the FDD in support of the Tropical Rainfall Measuring Mission (TRMM). The utility, known as the Maneuver Command Utility (MCU), produces spacecraft maneuver command sheet for use by mission operators. The project had been estimated to be approximately 5 person months in effort and was scheduled to take place between October 1995 and January 1996, including independent system testing. Two people had been assigned to the project along with the project manager.

The project manager that participated in our case study had been using the comparison risk management method for about three years and had used it in close to ten projects.

5.2 The Comparison Method

The project organization in our case study used a systematic risk management approach that was supported by a tool. Based on our assessment, the case study organization's risk management was more mature than what the industry average seems to be (Ropponen, 1993).

The case study organization has provided most managers with training on risk management, primarily focusing on the risk management tool that is used. Risk management is a required activity in all projects and risks are discussed with the management and customer frequently. Risk estimates are normally updated monthly.

The risk management approach is supported by a spreadsheet-based tool that guides risk analysis and helps in quantifying and ranking the risks. This internally developed tool has been in use since 1992 and it has been updated and improved during its usage. This risk management tool seems to be the driver of the risk management process in projects.

The comparison risk management tool collects the following information about each risk:

- Risk title, i.e., the name of the risk
- Risk description, i.e., a textual description of the risk
- Risk source, i.e., list of causes or factors that contribute to the risk
- Risk impact, i.e., a description of the impact the risk would have on the project
- Importance to the customer, i.e., ranking of risk's impact on the customer (expressed as Hi / Med / Lo)
- Current status, i.e., what has been done to the risk item (open / closed / in mitigation)
- Probability of occurrence, i.e., estimated probability of risk occurring, expressed as a probability percentage

The tool also collects information about the impact of risk if no mitigation action is taken, estimating the impact on quality (using a scale of Hi / Med / Lo / None), schedule impact (in weeks) and cost impact (in $K). The weight of these impacts can be set for each risk.

Once each risk has been identified, information about risk mitigation plans is entered into the tool:

- a description of the risk mitigation approach
- the trigger that is used to initiate the risk mitigation
- quality impact of the risk mitigation
- schedule impact of risk mitigation, i.e., the time delay caused by risk mitigation, regardless of whether mitigation is successful or not
- cost impact of risk mitigation, i.e., the additional cost caused of risk mitigation action is taken, regardless of whether mitigation is successful or not
- probability of risk mitigation success

The above information is used to calculate the risk analysis results using three scenarios (i) risk does not occur and no mitigation is done, (ii) risk occurs and mitigation is done but fails, and (iii) risk occurs, mitigation is done and it succeeds. These scenarios and the attributes used are presented in Table 9.

	Risk does not occur	risk occurs	
	no mitigation is done	mitigation is done but fails	mitigation is succesful
Probability	80%*	2%	18%
Quality factor	None	Med	None
Schedule	10 weeks	17 weeks	12 weeks
Cost	$16 K	$26 K	$18 K

* the values do not necessarily represent actual data

Table 9: Results of the comparison method's risk management tool

The decision of the appropriate risk mitigation action is left to decision makers evaluating the risk analysis data.

We interviewed the participating project manager after he had completed the risk analysis using the comparison method. According to him, the main benefit of the method is that it forces projects to think about risks frequently, every month. The approach also gives a quantitative indication of whether risk mitigation should be done. The results are often used in the decision making with management.

When inquired about the usage experiences and possible problems with the comparison risk management approach, the project manager pointed out that probability values are difficult to obtain and there is little support for estimating them, yet they play a critical role in the risk analysis process. "The risks associated with the estimation errors and assumptions used when making these estimates may contain some risks", he pointed out.

5.3 Case Study Goals and Metrics

The objectives of the case study were to assess the feasibility of the Riskit method in an industrial project, investigate the cost and time effectiveness of the method, evaluate the credibility of the method, and compare the Riskit method with the method currently used by the project. Furthermore, the case study was used to provide practical feedback on the use of the method.

Before our case study we initially formulated our evaluation goals and case study metrics in detail using the GQM method (Basili et al. 1994; Basili, 1992). These GQM-based metrics are presented in appendix A. Even though we used most of these metrics in our questionnaire and interviews, they did not result in useful data for our analysis. As we anticipated this problem, we documented the case study in detail so that different types of analyses could be done after the case study, i.e., exploring data or issues that were not necessarily identified in advance. This was done by taking detailed notes during the interviews and observation sessions, storing all the artifacts produced during the case study and writing synthesis reports shortly after the sessions.

Our first evaluation goal, expressed using the format GQM method (Basili et al. 1994; Basili, 1992) was as follows:

Analyze the Riskit method
in order to characterize it
with respect to its feasibility
from perspective of project manager
in the context of an industrial project.

We considered the Riskit method feasible, which was our hypothesis, if it meets the following criteria:

- The method produces intended results, i.e., is able to list and rank potential risks and is able to produce a list of controlling action.
- The method can be applied within reasonable time and effort. We are using the recommendations from Ropponen's survey as a guideline: effort allocation between two and eight percent of the project total is considered reasonable (Ropponen, 1993).
- The users of the method give a positive opinion of its feasibility.

In order to evaluate this goal and hypothesis we collected all the output the method produced, including intermediate ones, collected effort data, and interviewed the method user after the use of the method.

Our second goal was to investigate the cost and time effectiveness of the method. This was also described as a GQM goal:

Analyze the Riskit method
in order to characterize it
with respect to its cost-effectiveness
from perspective of project manager
in the context of an industrial project.

This goal attempted to measure the effort required to use the method, relative to various aspects of the method, such as number of risks identified and number of risk controlling actions proposed.

Our third goal was to evaluate the credibility of the method. This was also described as a GQM goal:

Analyze the Riskit method
in order to characterize it
with respect to its credibility
from perspective of project manager
in the context of an industrial project.

We define a risk management method's credibility as the level of confidence its users have in the results, i.e., the degree to which the output of the method is believable (Garrabrants et al. 1990; Kontio, 1994). This was assessed through asking about the level of confidence directly from the method user as well as monitoring whether the proposed risk controlling actions were actually implemented.

Our fourth goal was to compare the Riskit method with the method currently used by the project. This was defined as the following GQM goal:

Analyze the Riskit method and the comparison method
in order to compare them
with respect to effort, granularity, coverage, accuracy and effectiveness
from perspective of project manager
in the context of an industrial project.

As we intended to discover qualitative differences between the methods we did not specify specific metrics for this goal in advance. Instead, we planned to use the data collected to identify possible differences and compare the methods qualitatively.

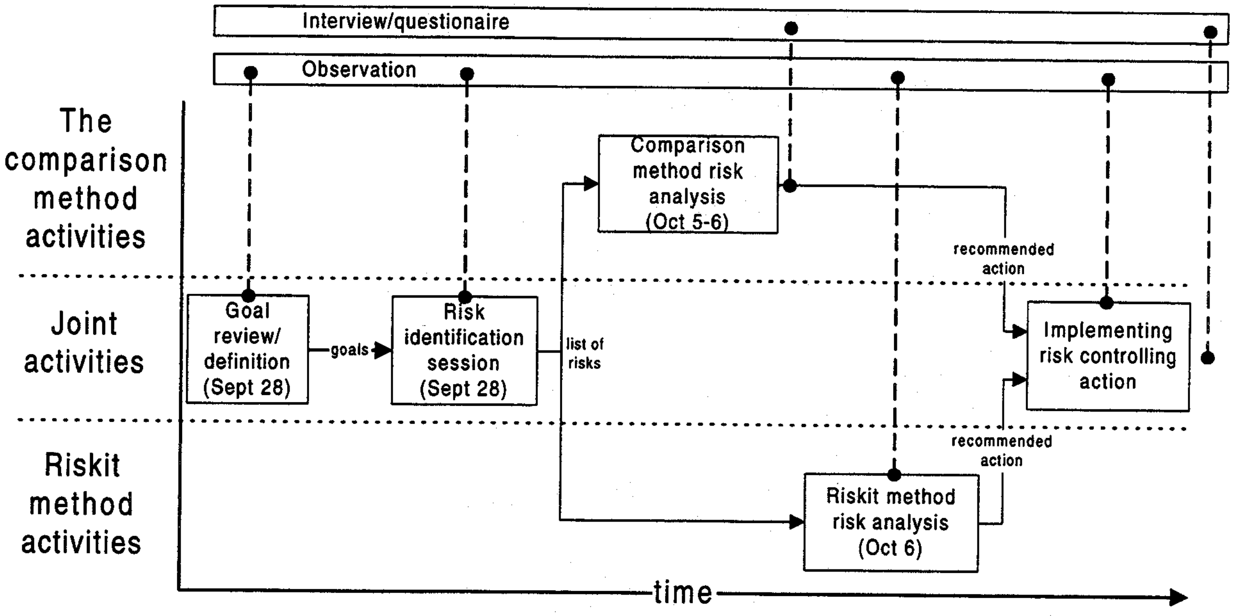
5.4 Case Study Arrangements

We arranged our case study so that we were able to compare the two risk management methods used in the project, the Riskit method and the comparison method. As Figure 5 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 method to carry out risk analysis the way he normally does it. After this the risk analysis using the Riskit method was carried out. After both analyses the project manager decided on which risk controlling actions he should actually take.

The project manager performed the first risk analysis on his own and documented the results of his analysis, including the risk controlling action he was planning to take.

The Riskit method was applied in a session where the method expert (i.e., the method author, J. Kontio) facilitated the session. This was done for two reasons. First, the project manager's time was not available for training him well enough in the method so that he could have reliably applied it on his own. Second, by facilitating the Riskit risk analysis we hoped that we would be able to avoid the effect caused by having applied the comparison method first.

Figure 5 also shows where and how we collected the case study data. A dashed line to the vertical line from a case study activity indicates whether we used observation or interviews and questionnaire to obtain relevant data. A connector appearing after an activity box indicates that the information was obtained after the activity was completed.



Interview/questionaire
Observation
The comparison method activities
Joint activities
Riskit method activities
Comparison method risk analysis (Oct 5-6)
Goal review/ definition (Sept 28)
goals
Risk identification session (Sept 28)
list of risks
recommended action
Implementing risk controlling action
recommended action
Riskit method risk analysis (Oct 6)
time

Figure 5: The timeline of case study activities

5.5 Validity Threats

In this section we discuss the limitations that our case study design had with respect to validity of the results.

As we had only a single project in the study we were forced to apply the methods in sequence and this may have lead to some maturation effects (Campbell and Stanley, 1963; Judd et al. 1991), i.e., the accumulated time spent on risk management may have increased participant's awareness and knowledge about risks. We tried to minimize this effect by taking two specific actions. First, even though the dedicated risk identification session is a characteristic of the Riskit method and not of the comparison method, we decided to conduct a joint risk identification session for both methods. We reasoned that risk identification would be especially vulnerable to maturation effect and could seriously bias the results. As risk identification is not a main aspect of the Riskit method we did not consider this a serious compromise in the method comparison. Second, we avoided analyzing risks in the identification session. We simply listed candidate risks and tried not to analyze or discuss them in any detail.

The sequential application of methods may also have caused a multiple treatment effect: the latter, Riskit method application may have been influenced by earlier analysis done using the comparison method. We tried to control this threat by carrying out the latter risk analysis as independently from the comparison method analysis as possible: we asked the project manager not to think about the results of the comparison method, we used the original list of risks as a starting point, and we facilitated the Riskit risk analysis session according to the Riskit method. Two observations lead us to believe that multiple treatment effect did not occur or was minimal: the risks selected for analysis were different and the method user clearly indicated that the analysis processes were so different that he himself did not observe any effect, the Riskit method seemed to have immersed the user so that he "forgot" his previous analysis.

The interviews and associated questions may have posed some construct validity and instrumentation threats in the study. As the Riskit method sessions were observed and the session notes reviewed shortly after each session, the Riskit observations were not affected by this threat. The interview sessions potentially may have been affected by this threat. As we discussed in section 5.3, the main research constructs were explicitly defined we have reported the resulting data in detail later in this report. It should be noted that many of the original metrics and questions turned out not to be applicable in the study or produced no responses from the method user. In retrospect, these questions and metrics seemed to have been the result of our attempts to "over-measure" the study.

The fact that we facilitated the Riskit risk analysis session may have caused a different kind of bias in the results, i.e., a construct validity threat similar to the Hawthorne effect (Cook and Campbell, 1979). It is plausible that the facilitator may have contributed to the analysis or that the mere presence of a facilitator and a scribe may have improved the performance of the project manager. We tried to minimize these effects by maintaining a strictly facilitating role in the analysis (we refrained from actually making any judgments or conclusions) and by strictly following the Riskit method. However, we cannot rule out the possibility that either our participation or unconscious contributions might have affected the analysis.

As the method developer was involved in the execution of the study and in the analysis of the results the experimenter expectancies may have influenced the results. We tried to control this threat by involving an experimenter whose sole research interest was in the experimental design and by documenting the case study results and outputs in detail in this report. This way outside, objective readers can evaluate possible bias independently.

Overall, we believe that our study design and arrangements prevented any significant validity threats to our results. The two most important validity threats relate to constructs used: the Riskit method changed two important parameters in risk analysis: the amount of effort spent and number of people participating. With the Riskit method more time was spent on risk analysis and risk control planning than with the comparison method. With the Riskit method there also was a member of the technical staff present in the analysis session present. While these factors quite likely had an effect on the results, they are also characteristics of the Riskit method. In other words, they were part of the control variable that we wanted to study.

6. Case Study Results

The following sections describe the progress of the risk analysis in the case study.

6.1 Goal Review

The goal review session was organized jointly for the two methods in the September 28 meeting (Figure 5), even though it is a step specified for the Riskit method (ver 0.10). The goals were listed in the session and the necessary information, as defined by the Riskit (ver 0.10) templates (Kontio, 1995) was documented. The resulting goal definitions are presented in Table 10. The goals were not formally articulated in the session in the format given in Table 10, however. This was done intentionally in order to minimize the possible influence to the comparison method that did not call for an explicit review of goals.

Goal/constraint	Stakeholders	Measurement unit	Target value	Direction of increasing utility
Schedule	CSC NASA	calendar date	Dec. 15, 1995	earlier is better
Effort	CSC NASA	staff months before testing	2.5	less is better
Functionality	CSC NASA	number of functions	satisfy the specification	more functionality is better
Quality	CSC NASA	number of errors in testing	7 (3.3/KLOC)	fewer errors is better
Productivity	CSC	LOC/hr	2.8	higher is better
Standards compliance	CSC	N/A	compliance to standards	N/A

Table 10: MCU project goals

The goal review was done in the beginning of a meeting that continued as a risk identification session.

6.2 Risk Identification

The project manager and two members of the technical staff participated in the risk identification session, as well as the experiment organizers, J. Kontio acting as a facilitator and

1. Unstable requirements
2. Mismatch between specification and actual requirements
3. Mismatch between user interface (UI) tool and required functionality. May have to change design to use the user interface tool.
4. Not familiar with tool (UI or other)
5. Not experienced in GUI development
6. Compatibility with AMPT, reuse. AMPT-- Automated Maneuver Planning Tool. Long-term support utility, in planning phase. AMPT will have, among other things, same functionality as the MCU. They may want to reuse MCU, and MCU will likely be replaced by AMPT in the future.
7. Platform familiarity. No longtime experience with the platform: UNIX and C
8. External interface problems. The tools and programs providing the input to MCU are changing. This may cause change of file format.
9. Staff reassigned. Customer may give directions to shift priorities, e.g., to the mainframe rehosting project. In this case all the goals will be changed.
10. Lose personnel.
11. Bottlenecks resources. Workstations and network may be occupied since more and more of the work move from mainframes.
12. Customer contact availability. If customer contact person changes or he is not available, important decisions may be postponed or have to be made by project manager.
13. Personnel turnover. Personnel may be relocated to other tasks (rehosting project) and be replaced by people with less experience.
14. Overhead of experiment Lots of time spent in meetings and doing extra tasks due to the experiment.
15. Unrealistic effort estimation. Effort estimation is not so accurate in preliminary design phase.
16. Not following standards. Not meeting company project standards
17. Different acceptance criteria between customer and vendor.
18. Unanalyzed acceptance of requirements changes
19. TBDs in the specification. Things "to be defined", requirements that are left unspecified.

Table 11: Risks identified

H. Englund as the observer and scribe.

We used three approaches in the risk identification session. First, we carried out a free-format brainstorming session where participants were allowed to name any risk and it was recorded on the white board. There was little discussion on the items. This session identified the first 14 risks listed in Table 11. These risks were identified in about 25 minutes.

After the free brainstorming step the facilitator asked participants to look at the project goals and consider possible threats to them. This goal-driven analysis produced the risks 15 and 16 (Table 11) and lasted less than ten minutes.

Finally, we used the Taxonomy-Based Questionnaire (TBQ) of the SEI (Carr et al. 1993) and went through the relevant questions to check whether they would prompt participants to recognize any additional risks. This yielded risks 17-19 and one additional goal that was not identified in the initial goal review session.
The TBQ session lasted one hour.

The session concluded with a list of identified risks. They were not classified into the risk analysis graph as this would have had an unintended effect on the comparison method.

6.3 The Comparison Method

The project manager participating in the project carried out the comparison method risk analysis on his own. He was given the list of identified risks and he selected three risks to work on:

- UI tool integration (composite of risks 3 and 4 in Table 11)
- AMPT compatibility (risk 6 in Table 11)
- inadequate staffing (composite of risks 9 and 10 in Table 11)

Note that he consolidated some risks together for his analysis. These risks, in his judgment, were the most important ones to consider, based on their impact, probability and possibilities for control. The risks and their selected risk controlling actions produced by the comparison method are listed in Table 12.

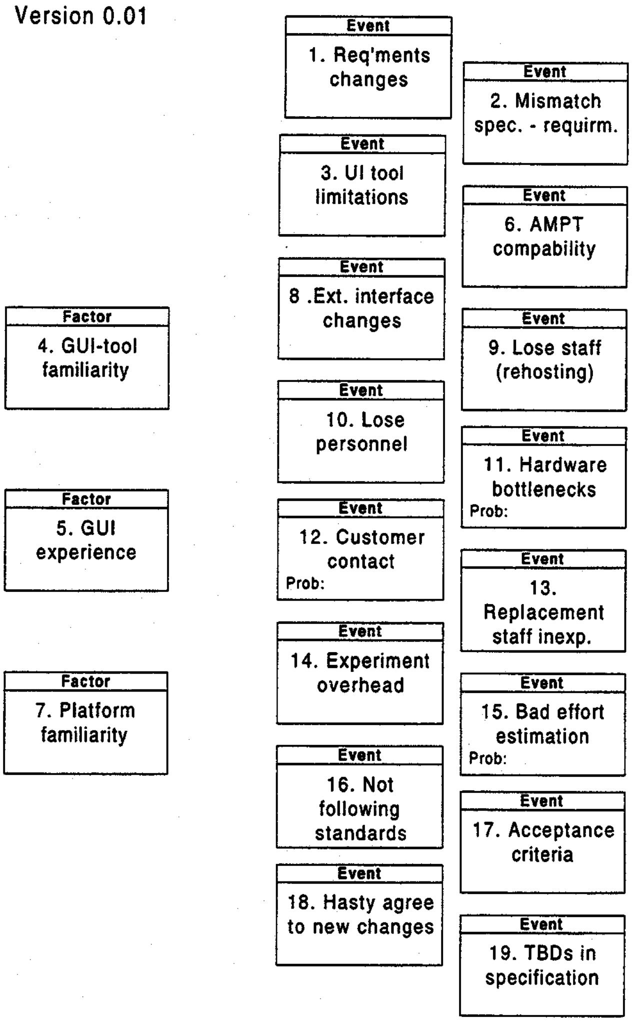


Figure 6: Results of the risk element classification

Risk	Selected controlling actions	Proposed but not implemented controlling actions
UI tool integration (containing risk 3)	A_{C1}: Apply lessons learned from previous UI tool integration (unique) A_{C2}: Have UI personnel review design and implementation products (overlapping A_{R6})	A_{C5}: Add staff or negotiate for more time (same as A_{R8})
AMPT compatibility (unique)	A_{C3}: Present detailed design walkthrough to analysts to ensure a consistent understanding of design approach (same as A_{R2})	A_{C6}: Estimate cost and schedule impact and provide to ATR (unique)
Inadequate staffing (overlapping)	A_{C4}: Finish all unit designs before coding (unique)	A_{C2}: <repeated> A_{C5}: <repeated> A_{C7}: Have available staff work extra hours (unique)

Note that actions A_{C2} and A_{C5} appear twice in the table but are each counted as one action.

Table 12: Risk controlling actions produced by the comparison method

The method user spent two hours on risk analysis using the spread-sheet based tool, which is normal for the type of projects he has been involved with. An example of the comparison method's output is presented in Table 9.

6.4 Riskit Method

6.4.1 Risk Analysis

After the risk identification session we grouped the identified risks (Table 11) into risk factors and risk events and placed them on the Riskit analysis graph, resulting in a graph presented in Figure 6. This was done without project manager's participation and was a relatively straight-forward task, taking approximately an hour to complete. Note that the names and meanings of some risks were slightly modified during this process to avoid ambiguity and overlapping of risks. The numbering used in Figure 6 refers to numbering used in Table 11 to maintain traceability of elements.

After the initial classification of risk elements into the Riskit analysis graph, we extended the graph by adding the other elements that belong to the graph. An initial version of this positioning was done without project manager to save his time. The results of this analysis are presented in Figure 7.

The resulting graph was used as a starting point in the Riskit risk analysis session with the project manager and one member of the technical staff. The graph was first reviewed and changes were made to correspond to project manager's perception of the situation. This resulted in the following changes:

- Risk event "AMPT compatibility" (risk number 6 in Table 11) was dropped because it

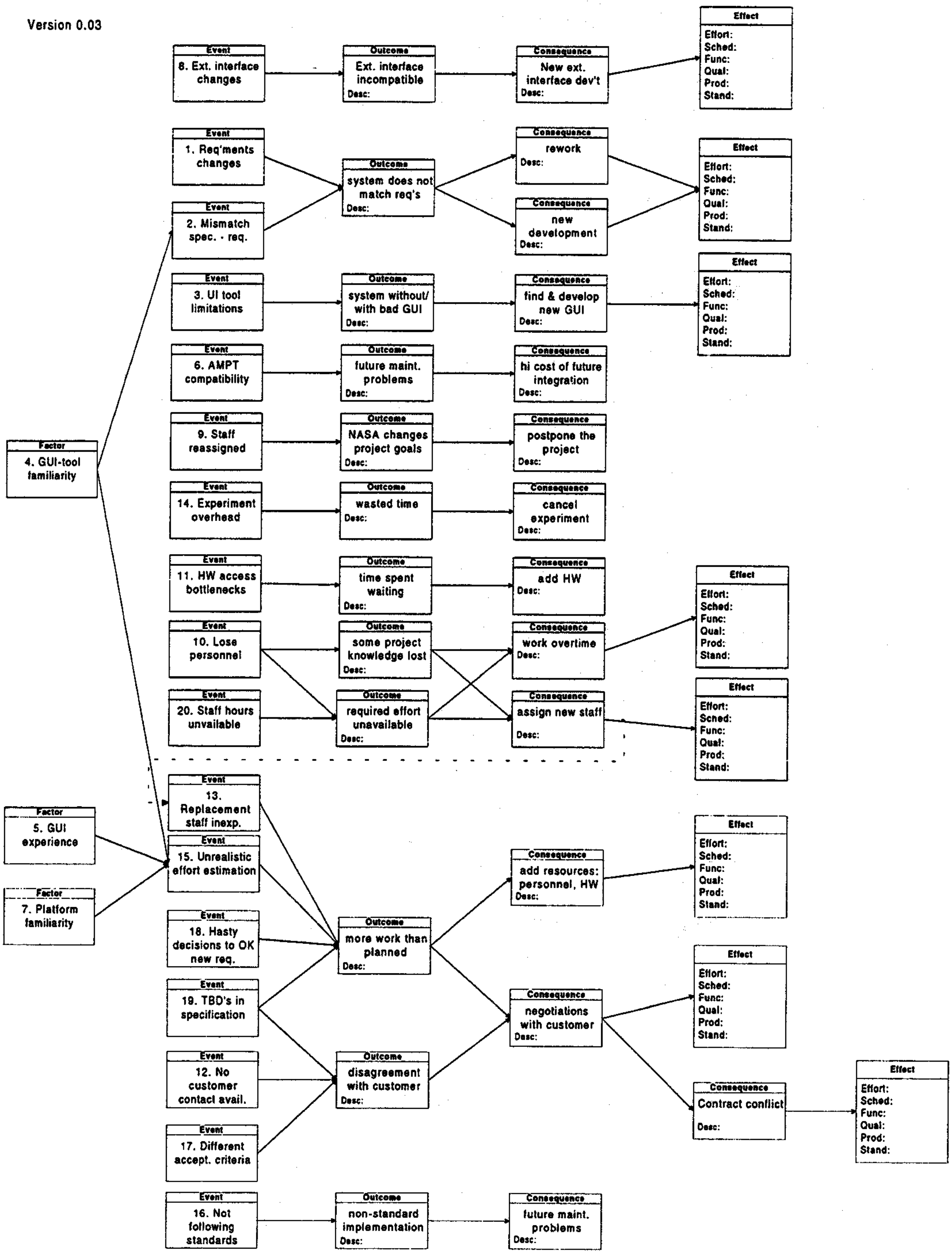


Figure 7: The result of initial risk analysis using the Riskit analysis graph

was not any of the identified goals or stakeholders in the project.

- Risk event "staff reassigned" (risk number 9 in Table 11) was dropped because this would occur as a customer requirement and is therefore not a risk to any stakeholder.
- Risk event "no customer contact available" (risk number 12 in Table 11) was dropped because this would be an unrealistic event (i.e., having infinitely small probability and if occurred, not being a risk to the project contractor).
- Risk event "replacement staff inexperience" (risk number 13 in Table 11) was dropped because of dropping risk 9 ("staff reassigned") due to their causal relationship.
- Risk event "TBDs in the specification" (risk number 19 in Table 11) was dropped as the specification document had been reviewed and there had not been any TBDs.
- A new risk event was added: "staff hours not available". This was done to separate the scenarios where staff members leave the project (risk event 10 in Table 11) and when their time becomes unavailable, e.g., because of the prioritization of other projects. This risk event was numbered as risk 20 in Figure 7.

Risk event	Classification (High/Medium/Low)	Ranking	
		Staff member	Project manager
3. UI tool limitations	High	2	1
1. Requirements changes	High	1	2
2. Mismatch spec. - req.	High	3	3
8. Ext. interface changes	Medium	7	5
15. Unrealistic effort estimation	Medium	6	6
6. AMPT compatibility	Medium	8	7
20. Staff hours unavailable	Medium	9	8
11. HW access bottlenecks	Medium	5	9
17. Different acceptance criteria	Low	12	10
10. Lose personnel	Low	10	11
19. Hasty decisions to OK new req.	Low	14	12
14. Experiment overhead	Low	11	13
16. Not following CSC standards	Low	13	14

Table 13: Risk event probability classification and rankings

Probabilities of risk events were estimated next. This was done using the following approach:

- Each risk event was categorized into as "high", "medium" or "low" using a discussion and consensus opinion of the project manager and the member of the technical staff.
- Both project manager and the member of the technical staff independently ranked risks from most likely to least likely.
- Rankings of the two individuals as well as the results of the classification approach were compared to spot any inconsistencies.

The results of this estimation process are presented in Table 13. As the Table 13 shows, all three estimation approaches yielded results that are reasonably close to each other. Thus, we assumed that we had obtained a reliable ranking of risks and used the results of the high-medium-low classification in the remainder of the analysis.

The next step was to review and refine each risk scenario and estimate the impact of each scenario to project goals. The impacts were quantified or described verbally as they affected the project goals. We then asked project manager to classify the "pain", i.e., utility loss, of each scenario into "High", "Medium" and "Low". The results of this activity are presented in Figure 8, together with other results of the analysis. The pain rankings are marked as the last attribute in the boxes representing the effects of each scenario (the right-most boxes in Figure 8). Scenarios with high pain and events with high probability have been highlighted by darkening the banner of the corresponding boxes.

6.4.2 Plan Risk Control

The final step in the Riskit method was to identify risks that should be controlled and propose some risk controlling actions. For risk control planning activity we selected the event-scenario combinations that met any of the following conditions:

- the event-scenario combination had both high probability and high pain;
- the event-scenario combination had high probability associated with medium pain; or
- the event-scenario combination had high pain associated with medium probability.

Note that we used our judgment in interpreting the above criteria and also reviewed all other scenarios to determine whether they would deserve further consideration even though they did not meet the above criteria.

The risk scenarios that were selected for risk control planning are listed in the left hand column of Table 14. For each risk scenario we tried to identify possible risk controlling action that could be taken. As a tool in this process we used the risk controlling action taxonomy (Kontio, 1995) to act as a checklist for proposing controlling actions.

The possible actions and their impacts on the risks were also documented in the Riskit analysis graph, as shown in Figure 9. The risk controlling actions are marked as ovals in Figure 9.

Risk	Selected controlling actions	Proposed but not implemented controlling actions
8. Ext. interface changes (unique)	A_{R1}: Show designs to the customer for approval (unique)	
1. Requirements changes (unique) 2. Mismatch spec. - req. (unique)	A_{R2}: Verify that walk-through reviews are done well (same as A_{C3})	A_{R11}: Document all requirements changes in detail (unique)
3. UI tool limitations (subsumed to "UI tool integration")	A_{R3}: Use the alternative UI tool (unique) A_{R4}: Train somebody in the alternative UI tool immediately (unique) A_{R5}: Make sure alternative UI tool experts are available (unique) A_{R6}: Consult current UI tool experts to check whether it satisfies the project needs (overlapping A_{C2})	
15. Unrealistic effort estimation (overlapping)	A_{R7}: Review estimates at walk-through review (unique) A_{R8}: Create slack (effort and schedule) with customer (same as A_{C5})	
10. Lose personnel (unique) 20. Staff hours unavailable (unique)	A_{R9}: Agree on project priority with other managers (unique) A_{R10}: Coordinate staff allocation with other managers (unique)	A_{R12}: Document well (unique)

Table 14: Risk scenarios selected for risk control planning and corresponding actions

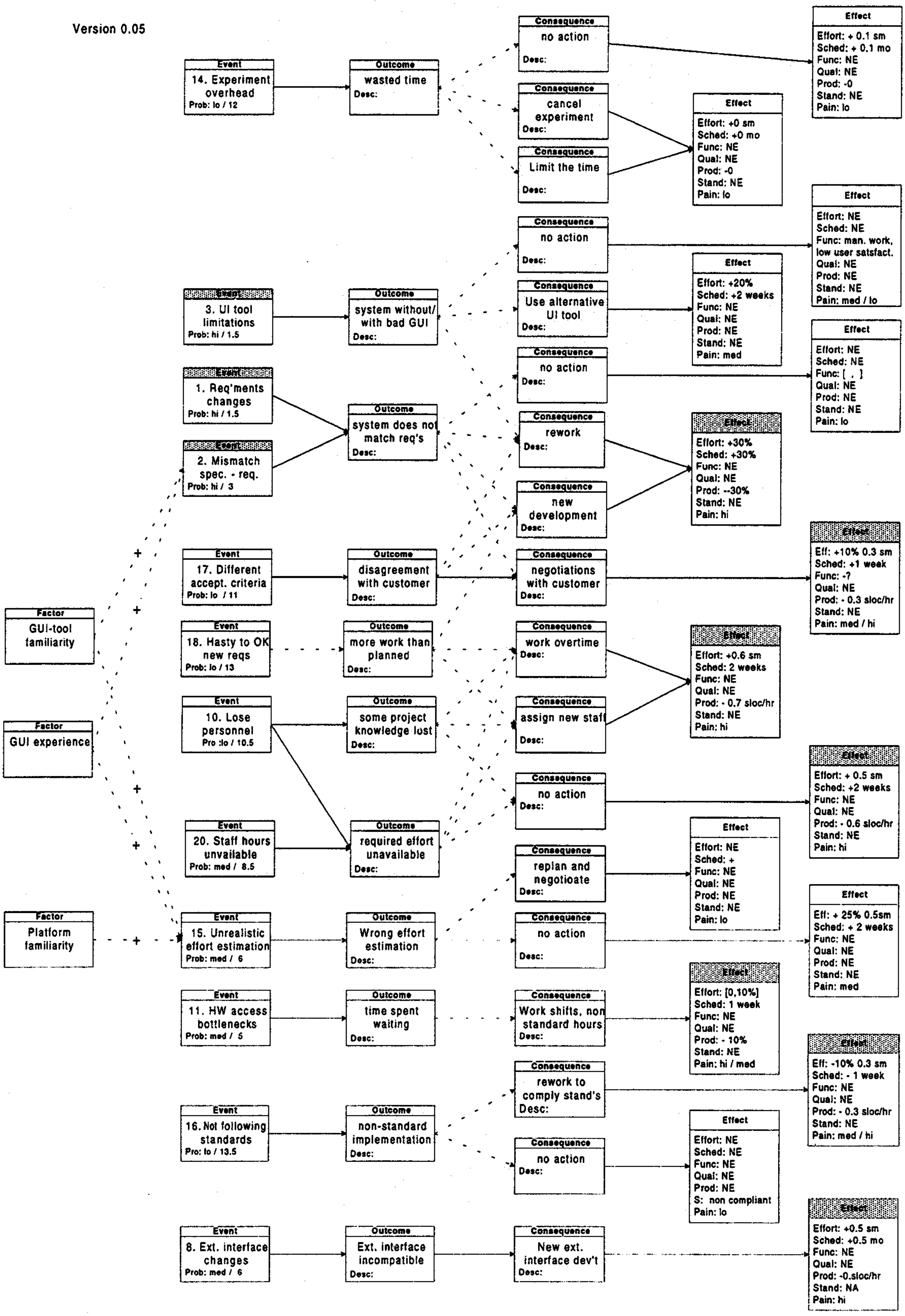


Figure 8: Results of risk analysis step

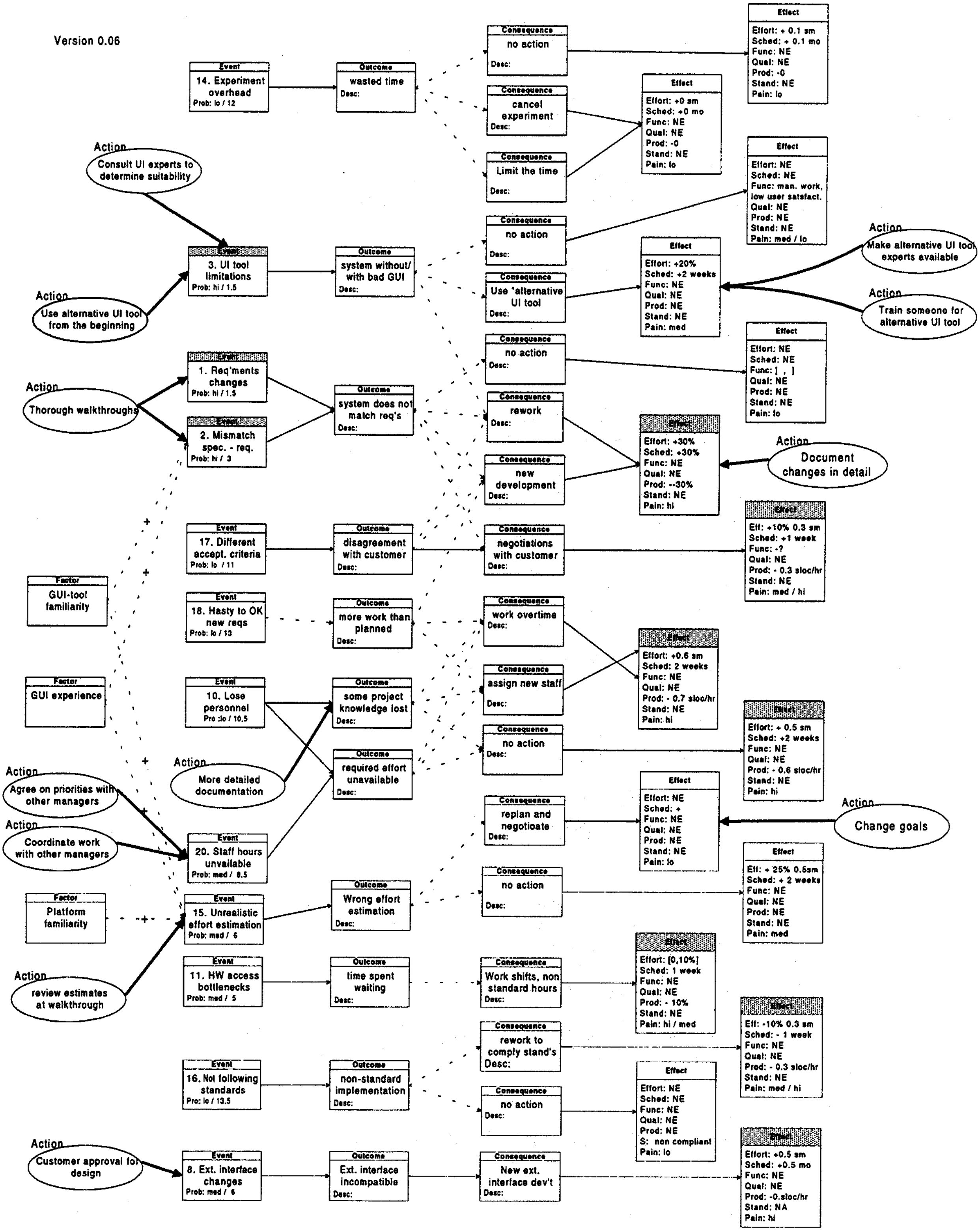


Figure 9: Final results of the Riskit process – risk controlling actions

7. Case Study Analysis

In the following sections we present the case study data and analyze the data with respect to the case study goals we had (presented in section 5.3). As we indicated earlier by Figure 5, the information about the methods was collected through observation, analysis of the artifacts produced, and interviews.

7.1 Qualitative Characterization of the Methods

We used questionnaires and interviews to inquire the method user's experiences and opinions about the two methods. All questions were sent to him in advance by email, he replied to the questions and we held an interview session to discuss his responses in more detail. The following represents the method user's responses to the main questions asked from him[10]:

Are the methods easy to understand and use?

> *"Riskit is easier to get started with – method of identifying risks is better defined. [Comparison method] provides better risk summary. Riskit follows a more scientific way of determining a risk's likelihood of occurrence. [Using the comparison method] we guess at the probability.*
> *Although the Riskit method had a better defined process, it would have been difficult to apply without facilitation.*
>
> *"Comparison method is easier to use, it has a simple, well-defined input format."*

Comment the output format of the methods.

> *"[The comparison method] quantifies risks and provides a good textual summary of them – good for individual risks but does not provide a high-level analysis of all risks, as Riskit does. Riskit has a complex and busy graph, but ranks risks well and presents them in a good summary table."*
>
> *"[The comparison method] cannot highlight the most important risks, Riskit does this clearly and effectively – perhaps its greatest asset."*

What is your opinion of the usability and practical value of the Riskit method?

> *"The method is usable and practical, it is a better risk management method, a more complete one. It may be better utilized in longer, riskier projects.*
>
> *"Riskit is certainly more thorough, [the comparison method] may find too few risks."*
>
> *"Riskit takes more resources. The [Riskit analysis] graph was too big. "*

How much confidence did you have in the risk analysis results produced by the Riskit method and why?

> *"I did have confidence in what it produced because of the process that was used, because of its more complete analysis of risks and because of the risk ranking process it used."*

[10] While most of the answers are verbatim quotes from the email responses, some the answers have been combined from more than one question, as they were addressed in different parts of the follow-up interview.

Which method, or which combination of them, would you recommend for use?

> *"Apply the brainstorming [risk identification] and risk ranking approach, as these do not increase the costs by much. Try out the complete Riskit method on selected projects. Use the [comparison method] for documenting each risk."*

We have evaluated the qualitative responses from three perspectives: ease of use, input and out formats, and practical value of the method.

It is difficult to compare the ease of learning and ease of use of the methods. While the Riskit method has some underlying, more complex principles in it, it is better documented and its application was facilitated in the case study. On the other hand , the comparison method had been used by the method users for several years and they had initially received training on it. However, given that the method user was able to apply and understand the method without any training in a facilitated session leads us to suggest that there are no significant differences in the ease of learning and ease of use between the methods.

Regarding the input and output formats of the methods, the comparison method seems to have an advantage in entering information in it – it has clearly defined items that need to be entered into the tool. It also seems to provide good summaries of each individual risk, although this observation may be largely due to the method user's familiarity of the output. The Riskit method seems to provide a better overview of the risk situation in the project and highlights most important risks well.

The method user expressed clearly more confidence in the results produced by the Riskit method. He saw it as a more 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.

7.2 Cost and Time

The cost and effectiveness of the method was analyzed based on the data presented in Table 15. As we discussed earlier, the risk identification session was shared between the methods. Thus, it is not straight-forward to sum up the effort used by the methods as a separate risk identification session is not normally part of the comparison method. If the risk identification session is included in the totals of both methods, the comparison method consumed 11 person hours and the Riskit method 20 person hours. If the risk identification step is excluded, corresponding figures are 3 and 12 hours, as Table 15 shows. It would be even plausible to compare the comparison method's 3 hours against the total of Riskit method's 20 hours, as they actually represent approximations of what "normally" would have happened without the experimental arrangements.

	Study management	Risk identification	Comparison method	Riskit method	**Total**
MCU project manager	6	2	3	3.5	14.5
MCU technical staff	0	4	0	3.5	7.5
UMD study personnel	NA	2	0	5	7
Total	6	8	3	12	29

Table 15: Study effort distribution in person-hours[11]

7.3 Granularity, Coverage and Accuracy

We have analyzed the granularity and coverage of the two methods by defining a set of specific metrics for risks and controlling actions that were produced. We realized that a mere counting of risk or controlling actions fails to account for the granularity and coverage of respective items. Thus, we use the following additional metrics to characterize the methods:

- Number of *same risks/actions* produced by the method, i.e., risks/actions that are judged to be same or very similar to a risk described by the other method.
- Number of *unique risks/actions* produced by the method, i.e., risks/actions that have not been identified by the other method and which do not overlap or are subsumed by other method's risks/actions.
- Number of *subsumed risks/actions*, i.e., risks/actions that are subsets of risks/actions identified by the other method.
- Number of *containing risks/actions*, i.e., risks/actions that include one or more of the risks/actions identified by the other method.
- Number of *overlapping risks/actions*, i.e., risks/actions that have some similarities but do not belong to any of the previous categories.

We used the above definitions to classify the risks selected for risk control planning and the controlling actions that were produced. Table 16 presents the metrics produced by the analysis of coverage and granularity of risks that were selected for risk control planning for each method.

When analyzing the risks we chose to compare the risks that were selected to risk control planning. The list of identified risks could not be used because the identification session was a joint session for both methods. We have marked the classification of each risk in Table 12 and Table 14 in parenthesis in the right-hand column, e.g., the text "(unique)" indicates that the risk thus marked was a unique risk for the method.

As Table 16 shows, the Riskit method analyzed more risks than the comparison method. However, direct count of analyzed risks is not a meaningful indicator of the differences between

[11] Some clarifications are necessary in order to interpret the data in Table 15 correctly. First, the item "study management" includes preparation and planning for the study, data collection and creating additional documentation for the purposes of the study. Consequently, we have estimated the editing work on the Riskit Analysis Graphs to have taken 1.5 hours. Second, the UMD personnel's time for the study management task was not accurately measured (thus the "NA" item in the corresponding cell).

methods. The difference between the number of unique risks produced by the methods is more interesting: Riskit analyzed five unique risks compared to one of the comparison method's.

Metric	Comparison Method	Riskit Method
same risks	0	0
unique risks	1	5
subsumed risks	0	1
containing risks	1	0
overlapping risks	1	1
Total	3	7

Table 16: Coverage and granularity metrics for risks analyzed

The comparison method's "UI tool integration" was a containing risk to Riskit method's subsumed risk "UI tool limitations". As there was only one pair of containing/subsumed risks we cannot make any conclusions from this particular data. In general, however, a high number of subsumed risks indicates finer granularity and, if the subsumed risks cover all or most of the containing risk, this can be considered more precise description of the risks in a situation.

Risks "Inadequate staffing" (comparison method) and "Unrealistic effort estimation" (Riskit) were considered overlapping.

Given the data about the analyzed risks in the case study, the risk management methods seem to differ in their coverage. If we assume that the union of analyzed risks represents the "real" risks in the situation and count same, subsumed, containing and overlapping risks as one instance each, the *risk coverage ratios* for each method can be calculated as follows:

- comparison method: 3/8 = 38%
- Riskit method: 7/8 = 88%

We would like to emphasize that due to the assumptions and interpretations made during the above analysis, the above figures should be interpreted conservatively.

We repeated a similar process for risk controlling actions that were produced. Table 17 presents this data. The classification of actions into our categories have been marked in Table 12 and Table 14 in parenthesis in the middle and left-hand columns.

As Table 17 shows, the Riskit method proposed more controlling actions than the comparison method. It also produced a higher number of unique controlling actions. Using the same principle as above, the coverage ratios for risk controlling actions are as follows:

- comparison method: 7/16 = 44%
- Riskit method: 12/16 = 75%

The above figures suggest that the coverage of actions proposed by the Riskit method is higher, i.e., it proposed a wider range of actions to be considered for implementation.

Metric	Comparison Method	Riskit Method
same controlling actions	2	2
unique controlling actions	4	9
subsumed controlling actions	0	0
containing controlling actions	0	0
overlapping controlling actions	1	1
Total	7	12

Table 17: Coverage and granularity metrics for controlling actions analyzed

We assess the accuracy of the methods indirectly through the risk controlling actions that were actually taken in the project, vs. the actions that were planned. The rationale for this metric is that we assume that the project manager, as a rational decision maker, will take the necessary cost efficient action in the project as further information about the project becomes available. Any action that was planned but not implemented indicates that (i) risk situation changed after the action was planned, (ii) the action did not address a big enough risk to justify it, or (iii) the action was not considered effective enough to justify its costs.

According to the project manager, there were no recognizable changes in the risk situation after the risk control planning and taking the action. Thus, we are using the ratio

Risk controlling action accuracy ratio = number implemented actions / number of planned actions

as an indicator of the accuracy of the results produced. Below are the corresponding ratios for the two methods:

- comparison method: 4/9 = 44%
- Riskit method: 10/12 = 83%

These figures lead us to suggest that the Riskit method was more effective in proposing accurate risk controlling actions, i.e., it proposed actions that were considered worth implementing in the project.

It is also noteworthy to highlight that the Riskit method addressed a risk that actually realized: the UI tool was considered unsuitable for the project and an alternative tool was used. The risk controlling action that was taken mitigated the potential negative impact of this risk in advance. The comparison method addressed a containing risk ("UI tool integration") for the same risk but did not recognize the controlling actions that directly mitigated the risk.

7.4 Feasibility

Our first goal was to investigate the feasibility of the Riskit method in industrial context (page 21). The criteria we defined for determining feasibility were met. First, the method produced intended results (identified risks, ranked them and proposed controlling action). Second, the overall effort spent on the use of the method was 12 hours. This is 20% of the management time of the project, and 2% of the total effort in the project, i.e., well within the effort limit proposed by Ropponen's survey (Ropponen, 1993). Third, as we reported in section 7.1, 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. We would like to point out that the validity threats described in section 5.5 prevent us from generalizing this conclusion outside this project with confidence. However, none of the validity threats directly contradicts such generalization, either.

7.5 Efficiency

The evaluation of the efficiency of the method was based on the data obtained in the characterization process described in sections 7.1 to 7.3. We Defined two derived metrics to characterize the efficiency. The first one, *risk coverage efficiency index*, utilizes *the risk coverage ratio*, defined in section 7.3, and the effort used for risk management using the method. The rationale for this metric is that the risk coverage ratio represents the best available information of the coverage of all relevant risks in a situation. Dividing this by the effort expended to reach that coverage gives an indication of a method's efficiency in risk analysis.

The second metric, *risk controlling action efficiency index*, utilizes the concept *risk controlling action accuracy ratio*, defined in section 7.3, and effort for the method. The rationale for this method is that the total of implemented actions represent the best available information about the correct action to take in a situation. As the *risk controlling action accuracy ratio* numerically describes how well the method was able to produce the ideal set of actions, normalizing the *risk controlling action accuracy ratio* by effort expended gives an indication of risk controlling action efficiency.

The effort used in these calculations was the method's total effort without the shared risk identification session (see Table 15). The two metrics and corresponding data are presented in Table 18.

Metric	Comparison Method	Riskit Method
risk coverage efficiency index = risk coverage ratio / risk management effort	38% / 3 = 13%	88% /12 = 7%
risk controlling action efficiency index = risk controlling action accuracy ratio / risk management effort	44% / 3 = 15%	83% / 12 = 7%

Table 18: Efficiency metrics used in the case study analysis for the two methods

As the results of Table 18 show, the comparison method is more efficient in analyzing risks and proposing actions. This is not surprising, since the comparison method analyzed fewer risks and proposed fewer actions. It is quite likely that the most obvious risks and actions are the least costly to produce. The relative efficiency decreases as more risks and actions are analyzed and proposed. Consequently, we do not think that efficiency is an effective metric to evaluate a risk management method.

7.6 Effectiveness

The evaluation of effectiveness of the methods is to consider whether the unique risks produced by the methods resulted in actions that were actually implemented and whether these actions were unique. From this perspective, the comparison method produced one unique risk ("AMPT compatibility") whose controlling action (A_{C3}) was the same as one of Riskit method's implemented actions (A_{R2}). Riskit, on the other hand, produced five unique risks and seven unique risk controlling actions (see Table 14). This seems us to suggest that while the marginal efficiency if the Riskit method was lower, its overall effectiveness was higher.

8. Conclusions

The purpose of exploratory case studies is to provide real-world data, experience and feedback to in order to identify problems, interesting relationships or concepts, or simply to provide a basis for ideas and innovation. From this perspective the case study was an exploratory one – it gave us insights to the issues in risk management and how the Riskit method addresses these issues. A secondary goal was to investigate the feasibility of the method.

The case study had a major impact on the further development of the method. The Riskit Analysis Graph was simplified and revised, the Riskit process description subsequently detailed, and several application guidelines were identified.

The case study also served to characterize and evaluate the method. Based on the analysis of our experiences we have concluded that Riskit is a feasible method in an industrial context. The Riskit method seems to cover risks comprehensively and propose risk controlling actions accurately. Furthermore, it seems to provide a good overall view of risks and its results seems to be credible. However, it seems to consume more resources than the default method. It seems that Riskit may be a method to be applied when projects are large or when risks are high. Small, low risk projects may be better off with simpler and less costly risk management approaches.

Given the limited size of the case study and limited number of data points available, it is too early to generalize these findings with any confidence. However, they indicate that the method has several potentially significant benefits.

9. References

Anonymous (1992) *The American Heritage Dictionary of the English Language*, 3rd edn. U.S.A. Microsoft Bookshelf/Houghton Mifflin Company.

Basili, V.R. (1992) Software Modeling and Measurement: The Goal/Question/Metric Paradigm. CS-TR-2956, College Park, MD: University of Maryland.

Basili VR, Caldiera G, McGarry F, Pajerski R, Page G, and Waligora S. The Software Engineering Laboratory - an Operational Software Experience Factory. 370 p. -381.(1992)

Basili, V.R., Caldiera, G. and Rombach, H.D. (1994) Goal Question Metric Paradigm. In: Marciniak, J.J. (Ed.) *Encyclopedia of Software Engineering*, pp. 528-532. New York: John Wiley & Sons

Basili, V.R. and Green, S. (1994) Software Process Evolution at the SEL. *IEEE Software* **11**, 58-66.

Boehm, B.W. (1981) *Software Engineering Economics*, Englewood Cliffs, N.J. Prentice Hall.

Boehm, B.W. (1989) *Tutorial: Software Risk Management*, IEEE Computer Society Press.

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

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

Charette, R.N. (1989) *Software Engineering Risk Analysis and Management*, New York: McGraw-Hill.

Cook, T.D. and Campbell, D.T. (1979) *Quasi-Experimentation: Design & Analysis Issues for Field Settings*, Chicago: Rand McNally College Pub. Co.

Edgar, J.D. (1989) Controlling Murphy: How to Budget for Program Risk (originally presented in Concepts, summer 1982, pages 60-73). In: Boehm, B.W. (Ed.) *Tutorial: Software Risk Management*, pp. 282-291. Washington, D.C. IEEE Computer Society Press

Fenton, N.E. (1991) *Software Metrics A Rigorous Approach*, London: Chapman & Hall.

French, S. (1986) *Decision Theory: An Introduction to the Mathematics of Rationality*, Chichester: Ellis Horwood.

French, S. (1989) *Readings in Decision Analysis*, London: Chapman and Hall.

Friedman, M. and Savage, L.J. (1948) The Utility Analysis of Choices Involving Risk. *Journal of Political Economy* **56**, 279-304.

Garrabrants, W.M., Ellis III, A.W., Hoffman, L.J. and Kamel, M. (1990) **CERTS**: A Comparative Evaluation Method for Risk Management Methods and Tools. In: Anonymous *Proceedings of the Sixth Annual Computer Security Applications Conference*, pp. 251-257. Los Alamitos: IEEE Computer Society Press

Judd, C.M., Smith, E.R. and Kidder, L.H. (1991) *Research Methods in Social Relations*, 6th edn. Fort Worth: Harcourt Brace Jovanovich College Publishers.

Karolak, D.W. (1996) *Software Engineering Risk Management*, Washington, DC: IEEE.

Keeney, R.L. and Raiffa, H. (1976) *Decision with Multiple Objectives: Preferences and Value Tradeoffs*, New York: John Wiley & Sons.

Kontio, J. (1994) Software Engineering Risk Management: A Technology Review Report. PI_4.1, Helsinki, Finland: Nokia Research Center.

Kontio, J. (1995) Riskit: An Analytical Model for Risk Management. working paper.

Kontio, J. (1996) The Riskit Method for Software Risk Management, version 1.00. College park, MD: University of Maryland.

McGarry, F., Pajerski, R., Page, G., Waligora, S., Basili, V.R. and Zelkowitz, M.V. (1994) Software Process Improvement in the NASA Software Engineering Laboratory. CMU/SEI-94-TR-22, Pittsburgh, PA: Software Engineering Institute.

NASA (1995) Software Engineering Laboratory World Wide Web home page: http://fdd.gsfc.nasa.gov/seltext.html.

Ropponen, J. (1993) Risk Management in Information System Development. TR-3, Jyväskylä: University of Jyväskylä, Department of Computer Science and Information Systems.

Saaty, T.L. (1990) *The Analytic Hierarchy Process*, New York: McGraw-Hill.

Von Neumann, J. and Morgenstern, O. (1944) *Theory of Games and Economic Behavior*, Princeton: Princeton University Press.