
Chapter 6.

Risk Analysis and Management

6.1 Introduction

- A risk is the possibility that an undesirable event (called the risk event) could happen.
- Risks involve both uncertainty (events that are guaranteed to happen are not risks) and loss (events that don't negatively affect the project are not risks).
- Proactive risk management is the process of trying to minimize the possible bad effects of risk events happening.
- There is disagreement about what risks should be managed. Some experts suggest that only risks that are unique to the current project should be considered in risk analysis and management. Their view is that the management of risks common to most projects should be incorporated into the software process.

Stage of Risk Analysis

- Risk identification
 - Identify potential risks that may arise.
- Risk analysis and classification
 - Assess the seriousness of each risk.
- Risk decomposition
 - Decompose risks to discover their potential root causes.
- Risk reduction assessment
 - Define how each risk must be taken into account or reduced when the system is designed.

6.2 Risk Identification

- This is the process of identifying possible risks.
- Risks can be classified as affecting the project plan (project risks), affecting the quality (technical risks), or affecting the viability of the product (business risks).
- Some experts exclude events that are common to all projects from consideration for risk management. These experts consider those common events as part of standard project planning.

6.2 Risk Identification

EXAMPLE 6.1

Consider a project that involves trying to develop safety critical software on cutting-edge hardware. List risks and classify each as project, technical, or business and as common to all projects or special to this project.

Risk	Project	Technical	Business	Common	Special
Hardware not available		X			X
Requirements incomplete	X			X	
Use of specialized methodologies		X			X
Problems achieving required reliability		X			X
Retention of key people	X			X	
Underestimating required effort	X			X	
The single potential customer goes bankrupt			X		X

6.3 Risk Estimation

- Risk estimation involves two tasks in rating a risk. The first task is estimating the probability of the occurrence of a risk, called the risk probability, and the second task is estimating the cost of the risk event happening, often called the risk impact.
- Estimating the risk probability will be hard. Known risks are much easier to manage, and they become part of the software process. The new risks that are unique to the current project are those most important to manage.
- The cost of the risk may be easier to determine from previous experience with project failures.

6.4 Risk Exposure

- Risk exposure is the expected value of the risk event. This is calculated by multiplying the risk probability by the cost of the risk event.

EXAMPLE 6.2

Consider two dice. Consider a rolling a 7 as an undesirable event that would make you lose a pot of \$60. Calculate the risk probability and the risk impact of rolling a 7. Calculate the risk exposure.

The risk probability is 6 cases out of 36 combinations, or $1/6$. The risk impact is \$60. The risk exposure is $1/6$ times \$60, or \$10.

6.4 Risk Exposure

6.4.1 RISK DECISION TREE

- A technique that can be used to visualize the risks of alternatives is to build a risk decision tree.
- The top-level branch splits based on the alternatives available. The next split is based on the probabilities of events happening. Each leaf node has the risk exposure for that event. The sum of the risk exposures for all leafs under the top-level split gives the total risk exposure for that choice.

6.4 Risk Exposure

EXAMPLE 6.3

A friend offers to play one of two betting games with you. Game A is that you toss a coin twice. He pays you \$10 if you get two heads. You pay him \$2 for each tail you toss. Game B is that you also toss a coin twice, but it costs you \$2 to play and he pays you \$10 if you get two heads. Which game should you play?

The risk decision tree is shown in Fig. 6-1. Both games total to \$0.50. Thus, each time you play, your average gain is 50 cents. No matter which game you choose.

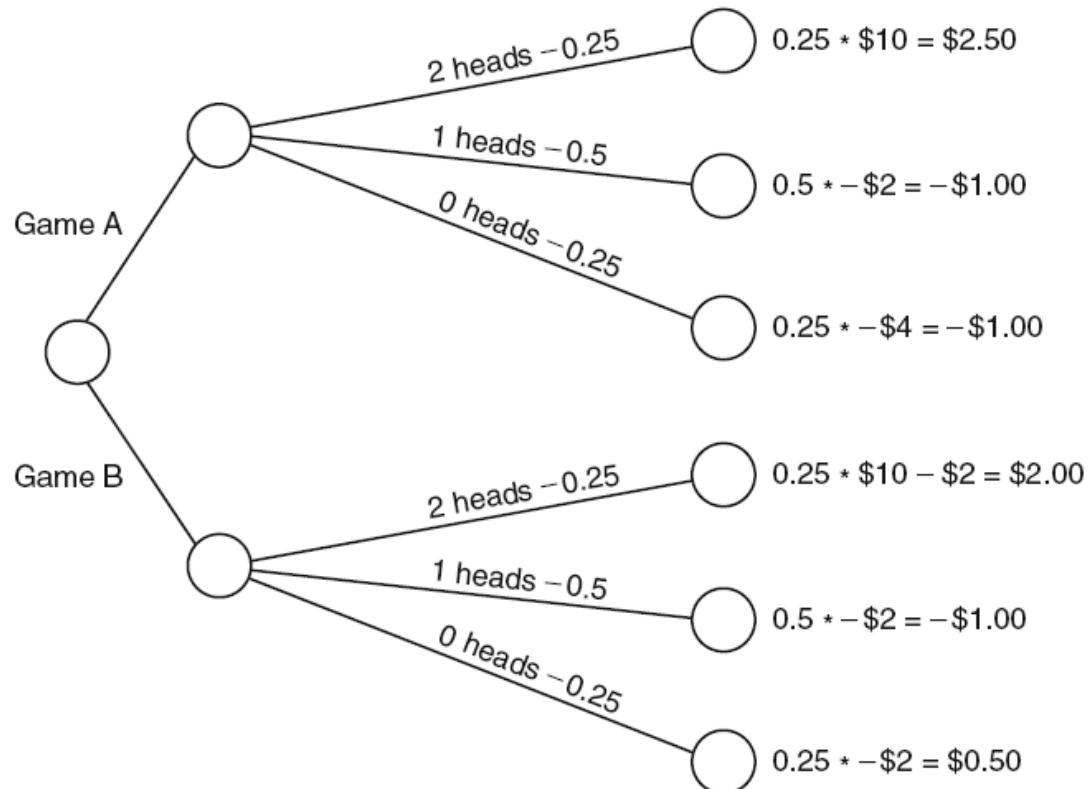


Fig. 6-1
Software Engineering

6.5 Risk Mitigation

- ***Risk mitigation*** is the proactive strategy of trying to find ways to either decrease the probability of the risk event happening or the impact of it happening. While there are no magic ways to reduce risk, a common approach is to try to resolve risks related to uncertainty early. For example, if there is concern about particular systems that need to be used, investigating those systems early is better. Often, a prototype can be built that would identify problems early.

6.5 Risk Mitigation

EXAMPLE 6.4

Consider the risks identified in the risk identification problem. Suggest an approach for either decreasing the probability or decreasing the impact or both.

Risk	Decrease Probability	Decrease Impact
Hardware not available	Accelerate dev. of hardware	Build simulator
Requirements incomplete	Increase review of requirements	
Use of specialized methodologies	Increase staff training, hire experts	
Problems achieving required reliability	Design for reliability	
Retention of key people	Pay more	Hire additional personnel
Underestimating required effort	Hire external estimator	Build in slack time, reestimate often
The single potential customer goes bankrupt	Have external evaluation of area	Identify other potential clients

6.6 Risk Management Plans

- A risk management plan must include an identifier, a description of the risk, an estimate of risk probability, an estimate of risk impact, a list of mitigation strategies, contingency plans, risk triggers (to determine when contingency plans should be activated), and responsible individuals. Additional fields might include current and/or past status of related metrics.

6.6 Risk Management Plans

EXAMPLE 6.5

Develop a form for risk management and insert sample data.

Risk ID: 1-010-77	Prob: 10 percent	Impact: very high
Description: Specialized hardware may not be available.		
Mitigation strategy: Build simulator, accelerate hardware development.		
Risk trigger: Hardware falling 1 week or more behind schedule.		
Contingency plan: Outsource hardware development as backup, deliver system on simulator.		
<p>Status/date/responsible person: Created – Jan 1,01 – Fred Jones Sim. completed – Feb 10, 01 – Bill Olson</p>		