Volume-7, Issue-3, May-June 2017
International Journal of Engineering and Management Research
Page Number: 543-546

Quality Risk Analysis: An Approach for the Refinement of Traditional Risk Analysis

Shipra Kalra[1], Rachika Sharma[2]
[1]Department of Computer Science, Gitarattan International Business School, INDIA
[2]Department of Computer Science, Delhi Public School, Raj Nagar, INDIA

ABSTRACT

Risk analysis is the systematic study of uncertainties and risks we encounter in business, engineering, public policy, and many other areas. Risk analysts seek to identify the risks faced by an institution or business unit, understand how and when they arise, and estimate the impact (financial or otherwise) of adverse outcomes. Since it is not possible to test everything, it is necessary to pick a subset of the overall set of tests to be run. Quality risks analysis can help one focus the test effort.

This paper first describes the traditional risk analysis and then the quality risk analysis. After that techniques of quality risk analysis are discussed followed by quality risk analysis process.

***Keywords*--** Quality, Risk, Testing

I. INTRODUCTION

Since it is not possible to test everything, it is necessary to pick a subset of the overall set of tests to be run. Quality risks analysis can help one focus the test effort

While the phrase “quality risk analysis may sound forbidding, mystifying, and complex”, the underlying ideas—and the techniques—need not be. Simply put, quality risk analysis is a process for identifying, analyzing, and prioritizing categories of potential quality problems (that is, bugs) in one’s systems Because quality risks are potential problems— with probabilities between zero and 100 percent—one factor that influences the relative importance of a risk is the likelihood of the undesirable outcome. In other words, is it likely that these kinds of bugs exist in the system and is it likely that users will encounter these kinds of bugs if they exist?

Another factor that influences the relative importance of a risk is the impact of that undesirable outcome on the users, customers, or other stakeholders. In other words, if these kinds of bugs exist in the system and users encounter them, how will the symptoms of the bugs affect the users? The impact of bugs can range from trivial to catastrophic on some systems, even deadly.

For example, suppose one is developing an online shopping application. This application allows users to log into their accounts over the Internet. They can then shop, pay bills, and download shopping statements

For such an application, security is clearly a major quality characteristic. In the area of security, risks to system quality include the possibility that criminal hackers gain unauthorized access to other customers’ accounts or that hackers intercept account information in transit between the data center and customers’ PCs.

II. TRADITIONAL RISK ANALYSIS

Risk analysis is often viewed as a “black art”—part fortune telling, part mathematics. Successful risk analysis, however, is nothing more than a business-level decision-support tool: it’s a way of gathering the requisite data to make a good judgment call based on knowledge about vulnerabilities, Fidelity threats, impacts, and probability.[2]

number of tests that one can conceivably run. How does one choose the best possible subset? A smart approach would be to pick those tests that address the most important risks. Testing reduces risks to system quality. It helps identify areas of the system that work properly (that is, the tests pass). It also helps identify opportunities to make the system better (that is, the tests fail, detecting bugs). So smart test managers should ask, “How do we test the most critical areas and find the most critical bugs?”

In **quantitative risk analysis**, an attempt is made to numerically determine the probabilities of various adverse events and the likely extent of the losses if a particular event takes place.

Qualitative risk analysis, which is used more often, does not involve numerical probabilities or predictions of loss. Instead, the qualitative method involves defining the various threats, determining the extent of vulnerabilities and devising countermeasures should an attack occur.

Basic Terminologies

Asset

The asset, or object of the protection efforts, can be a system component, data, or even a complete system.

Risk

Risk are future uncertain events with a probability of occurrence and a potential for loss.

Threat

The threat, or danger source, is invariably the danger a malicious agent poses and that agent's motivations (financial gain, prestige, and so on). Threats manifest themselves as direct attacks on system security

Countermeasures and Safeguards

Countermeasures or safeguards are the management, operational, and technical controls prescribed for an information system that, taken together, adequately protect the system's confidentiality, integrity, and availability as well as its information. For every risk, a designer can put controls in place that either prevent or (at a minimum) detect the risk when it triggers.

Impact

The impact on the organization, were the risk to be realized, can be monetary or tied to reputation, or it might result in the breach of a law, regulation, or contract.

Vulnerability

A weakness in a computing system that can result in harm to the system or its operations, especially when this weakness is exploited by a hostile person or organization or when it is present in conjunction with particular events or circumstances.

Probability

Probability measures the likelihood that something specific will occur. If something is absolutely going to happen, its probability of occurring is 1, or 100 percent. If something absolutely will not happen, its probability of occurring is 0, or 0 percent.

III. QUALITY RISK ANALYSIS

Testing any real-world system is potentially an infinite task. Of this infinite set of possible tests, test managers need to focus on the most significant risks to system quality. These are the potential failures that are likely to occur in real-world use or would cost a lot if they did occur.

Basic Terminologies

Risk

Risk is the probability that a hazard will turn into a disaster. Vulnerability and hazards are not dangerous, taken separately. But if they come together, they become a risk or, in other words, the probability that a disaster will happen.

Quality

Quality in business, engineering and manufacturing has a pragmatic interpretation as the *non-inferiority* or *superiority* of something; it is also defined as *fitness for purpose*. Quality is a perceptual, conditional, and somewhat subjective attribute and may be understood differently by different people. If someone talks about 'working on quality', they may simply mean activities designed to improve the organization and its services

Testing

Testing is the process of running a system with the intention of finding errors. Testing enhances the integrity of a system by detecting deviations in design and errors in the system. Testing aims at detecting error-prone areas. This helps in the prevention of errors in a system. Testing also adds value to the product by conforming to the user requirements.

Analysis

Analysis starts with stating the business goals for the deployment project. You then analyze the business problems you must solve and identify the business requirements that must be met to achieve the business goals. Consider also any business constraints that limit your ability to achieve the goals. The business requirements and constraints that you identify are a basis for a business requirements document that you later use to derive system requirements during the technical requirements phase

IV. RELATIONSHIP BETWEEN RISK AND TESTING

Any significant project involves risk. Risk increases with complexity, the number of participants, effort, budget, and duration. Capers Jones (1995) cites probabilities of software project failure ranging from 2 percent to 85 percent. He identifies inadequate testing as one of the four leading causes of failure, along with poor estimation, planning, and project tracking.[1]

Many managers are familiar with project risk management. For example, they manage risks such as loss of key personnel and late deliverables from vendors. Classical risk management says to mitigate these risks using both proactive means (such as cross-training of staff) and reactive means (such as redundant component sourcing). One can mitigate risks to system quality through proactive means like reviews and through reactive means like testing.

Quality is the presence of that which satisfies users, customers, and other stakeholders, and the absence of that which dissatisfies them. A quality system is fit for the users' purposes, provides the needed features, and contains few, if any, important bugs.

One starts testing a system with the intent of finding the errors, he or she evaluates the quality of the system in terms of particular functions, characteristics, and behaviors. While the presence of some bugs is expected, knowing exactly which activities will find those bugs is the challenge.

As testing continues, some of the bugs are discovered. These known bugs are no longer risks; they are now actual undesirable outcomes. It is possible to fix these bugs and improve the quality of the system. The overall risk is reduced.

When running the tests, one also discovers where the bugs are not. The tests that pass show that the system works as expected under the tested conditions. Again, the overall risk is reduced

The more thoroughly one tests the system, the more of the remaining bugs he or she finds. The more bugs one finds, the more bugs one can fix. The more thoroughly one tests the system, the more known-good, tested conditions one identifies. So, the more one tests, the lower the risk to the quality of the system. But the risk will never be reduced to zero, because there’s always one more test one could run. As the steady stream of Internet hacking exploits point out, the likelihood of such problems are all too high. When they do occur, such problems have serious impacts on customers, businesses, and other stakeholders. Clearly, to have confidence in such a system, one would want to develop and test in such a way as to reduce these risks.

V. QUALITY RISK ANALYSIS TECHNIQUES

There are a variety of risk analysis techniques available these days. Each has its strengths and weakness, depending on the needs and practices of the project team. So, selecting the right technique is essential.

All of these techniques involve identifying and prioritizing the risks to the quality of the system under test. Typically, the risks are grouped or organized by major risk categories, such as functionality, performance, security, and so forth. A cross-functional team of project stakeholders usually identifies the risks. Rather than rely only on the stakeholders’ opinions and recollections, the analysis should also draw upon historical bug and field failure data from past projects, requirements and design specifications, sales figures, market research, and anecdotal information from customers, competitors, or clients.

Once the risks are identified, each risk is assigned a level—a measure of its degree of importance. Following are five techniques for analyzing risk

1. Informal quality risk analysis:- This technique do not entail much beyond what is described in this section so far. Such technique provides an easy way to get started in quality risk analysis. When one miss some important areas of risk, especially during early risk analysis, then also informal technique make it possible to achieve a better degree of test focus and coverage than one can achieve without any risk analysis at all.

2. ISO 9126 quality risks analysis:- This technique use the quality characteristics and sub characteristics described in the ISO 9126 system quality standard as the categories for the risk analysis. The six main categories of quality are:

- Functionality
- Reliability
- Usability
- Efficiency
- Maintainability
- Portability

In each category there are two or more sub characteristics. ISO 9126 provides a more structured approach and reduces the likelihood of missing some major risk elements. It also tends to add a bit in terms of time and paperwork.

3. Cost of exposure quality risk analysis:- This technique focuses on the following question: What are the expected losses associated with various risks, and how much should one spend to reduce those risks? An expected loss is the product of the probability of the loss multiplied by the cost of the loss. Such techniques allow the project management team to make a hard-nosed, economic decision about testing. For this technique to work well, however, the risk analysis team must be able to accurately estimate the probabilities and costs of various losses.

4. Failure mode and effect analysis:- Using this technique, the risk analysis team tries to identify the different ways the system could fail and all the possible effects those failures would have on customers, clients, the business, society, and so forth. This technique is quite detailed. It can produce finely calibrated testing, but it also can produce a ton of paperwork and lots of invested time.

5. Hazard analysis:- This includes failure mode and effect analysis, but done backward. One starts first with the effects—the hazards—and tries to work backward to causes. Along the way, the likelihood of those causes should become clear. In some cases, though, there are many causes of different kinds of bad behavior, so this technique tends to work best with systems that do only a few things.

VI. QUALITY RISK ANALYSIS PROCESS

Whichever technique one chooses, he or she can follow a similar process for quality risk analysis.

1. Quality risk analysis team is identified.
2. Technique for analysis is selected.
3. Quality risks are identified. Then, risks are prioritized. One may include not only testing at various stages, but also reviews of requirements, design, and code,

programming techniques such as array bounds checking, and so forth.

4. If the problems are identified by risk analysis team in requirements, design, code, or other project documents, models, or deliverables during the analysis, then the problems are reported for the solution.
5. Quality risk analysis document is reviewed, revised and then document is finalized.
6. Quality risk analysis document is checked into the project library under change control.
7. At regular intervals (for example, major project milestones such as the completion of the requirements, design, and implementation phases, and test readiness and exit reviews) and as new information becomes available (for example, completion of a test cycle) then new items are reviewed and risk analysis document is updated, adding new items and reassessing the level of risk for the items.

The quality risk analysis process had two interesting side effects. First, it revealed that the vision of the system was evolving and not entirely consistent, especially at the detail level. Agreeing on what was at risk, quality-wise, helped promote a detailed consensus on what it would mean for the system to have quality. Second, the risks analysis highlighted a number of problems in the requirements and design documents. These problems were resolved, preventing bugs from entering the testing process.

VII. CONCLUSION

This paper explains that risk analysis is, at best, a good general-purpose yardstick by which we can judge our security design's effectiveness. Because roughly 50 percent of security problems are the result of design flaws, performing a risk analysis at the design level is an important part of a solid software security program. It also explains how and why one could use risk analysis as the foundation for testing and other quality assurance tasks. Quality risk analysis provides a foundation for smart test design and development. It also discusses the side effects of quality risk analysis process

REFERENCES

[1] Quality Risk Analysis, By Rex Black, President, RBCS, Inc.

[2] Risk Analysis in Software Design, DENIS VERDON Fidelity National Financial, GARY MCGRAW, Cigital

[3] ISO. 2000. ISO 9126-1:2000 Information technology: Software product quality. Geneva, Switzerland: International Organization for Standardization.

[4] Juran, J. M. 1988. Juran on planning for quality. New York: Free Press.

[5] Qualitative and Quantitative Risk Analysis Intaver Institute Inc. 303, 6707, Elbow Drive S.W. Calgary, AB, T2V0E5, Canada

[6] Classification and Analysis of Risks in Software Engineering ,Hooman Hoodat, and Hassan Rashidi