Presentation: Product Risk Analysis Clarifies Requirements
By: Jim Kandler

OUTLINE

This presentation re-emphases that requirements are important. The difference between functional and nonfunctional requirements will be covered. Then, Product Risk Analysis will be described, along with the elements of the analysis and steps toward performing the analysis.

REQUIREMENTS ARE IMPORTANT

The Requirements Phase is the most important phase of the development process. If the customer and the developer don't have a good understanding of what is desired, then it is difficult for the developer to be successful.

In the past, most code was written without strong written requirements. In the best cases the developer would sit with the customer and demonstrate what was being developed. The requirements were not documented, but at least there was an exchange of information that occurred, and the project was completed. As projects grew and teams became larger and dispersed, documented requirements became more important. Today there are numerous standards by the military and others for requirement documents. Most people now expect that some requirements document will exist. So we are improving by some people's standards.

DEFECTS ORIGINATE IN REQUIREMENTS PHASE

But still today the Requirements Phase of a project generates most of the defects. Over 50% of the defects are injected during the requirements phase. This is important since this phase forms the foundation for the product that more of the later work will build on. So, if the requirements are not correct there may be fundamental issues that are not surfaced until the later phases, which may require complete redesign of major portions of the product. The amount of rework to fix assumptions or undiscovered issues can have a major impact on a project. That is, undoing and redoing work already completed.

Considering that about half the resources for a project are spent fixing defects, the importance of good requirements becomes very evident. It would appear that if one spends more time on requirements to make them better, then the delivery date could be pulled in. Still today we hear of project managers who are concerned about delays in the project; since the engineers still haven't written a line of code. When you understand that requirements are the foundation for the rest of the project, any extra time spent in this phase can easily provide payback later.

FUNCTIONAL REQUIREMENTS

The Requirements Phase is only as good as the requirement documents that come out of it. A poorly developed requirements document can still leave many missed or vague requirements that can later delay the project. There are many methods in use to help us develop more complete requirements. Some of these are object oriented analysis, object oriented modeling, specification languages, use cases, etc. These methods are all function oriented. So the requirement documents developed while using them will be function oriented. This would not be a problem, except the customers, developers, and project leaders are also very function oriented. So the nonfunctional requirements of a product are missed, forgotten, or barely addressed. How many of you can give me a nonfunctional requirement for your car? There are many; serviceability, maintenance cost, reliability, resale value, safety, etc. We are not accustomed to thinking this way, so we need help.

NONFUNCTIONAL REQUIRMENTS

The nonfunctional requirements are very important to a product. You all have seen the software product that is great when it works, but look out when it stops working! This is evidence of a nonfunctional requirement for robustness or stability that was not properly addressed. There is a user expectation and need for the software to function long enough for someone to use it. When there are problems with the product it must fail softly. Software that corrupts your saved files and the operating system will not be used for very long. So reliability is another of those nonfunctional requirements. There are many other nonfunctional requirements, some of them are listed here.

TERMINOLOGY

Since the Product Risk Analysis is looking at risks there is a different set of terms to learn. Harm is a physical injury and/or damage to health or property. Hazard is a potential source of harm. So a cut is harm, while a sharp edge is a hazard. Risk is the rate of occurrence of a hazard. So if you work in a butcher shop you have a higher risk from sharp edges. Safety is the freedom from unacceptable risk. In the butcher shop the users of the knives are trained so the risk is tolerable. Risk Index is the numerical rating of the risk relative to the other items analyzed. Safety is the freedom from unacceptable risk. Safety and reliability should not be confused. A gun is reliable and unsafe, while Win 95 is safe and unreliable.

PRODUCT RISK ANALYSIS

So how do we overcome this tendency of our's to focus on functionality? Realization of this tendency is a step in the right direction. The requirement standards that are out also indicate items to be covered that are nonfunctional. The method that I am going to show you today is another means to compensate for this tendency.

Product Risk Analysis gets to the nonfunctional requirements by taking you through a process that establishes the areas of concern, then asks that you list efforts to reduce or mitigate these areas. The method attempts to capture all concerns no matter how insignificant they may be. Once the concerns are captured, the most important concerns are identified. This identification of the important concerns is a very powerful activity. It is often very enlightening for people to see the concerns that are ranked as most important. The results are often not as was expected. The assumptions are broken down and replaced will quantitative analysis.

The Product Risk Analysis method has been in use for many years. It was first used by the military to evaluate the risk of using a product or device and evaluating the consequences of failure of the product. Product Risk Analysis is a method that uses brainstorming techniques to identify all potential hazards, and their causes. The elements that would be implemented to mitigate the risks would be the nonfunctional product requirements. I have called this method Product Risk Analysis to differentiate it from Project Risk Analysis, which many of you have heard about before. This analysis has a process that considers the potential impact of product designs vs. project plans. There are several other acronyms that are used for other product type analysis.

ELEMENTS

There are several elements that are used for the analysis. I will cover these is their order of usage. The hazards of using the product are identified. The causes and subcauses of these hazards are also identified. Using these hazards and causes the risk is evaluated in the form of a Risk Index of matrix space. The mitigation for each of the hazards and their causes are developed and discovered. The risk is reevaluated with the mitigation in place and working.

OVERVIEW OF THE PROCESS

This is a team activity. The members of the team will each contribute their own perspective to the aanlysis. So it is important that the team members have overall knowledge of the product. There should be a designated leader to walk the team through the analysis. The hazards are identified and logged. The risk is evaluated and established for each of the hazards and causes. If the risk is at an acceptable level there is only monitoring to do. If the risk is too great, then additional mitigation are needed to reduce the risk. The mitigated risk is evaluated and if not acceptable, further mitigation are needed.

STEP1 IDENTIFY THE PRODUCT

Identification of the product is important since the risk analysis can be applied so many different ways. You will not remember in 2 months just where you focused the analysis or why things were left out if this is not documented now. Also team members may become confused and this can easily get them refocused. It sounds too simple, but you need to document the use of the product. You need to define the interfaces that are not being considered in the analysis. The elements of the system need to be documented. Do it now, and save on the grief that will surely come later.

STEP 2 IDENTICATION OF THE POSSIBLE HAZARDS
The objective here is to identify ALL possible hazards, no mater how small. This is a brainstorming activity. Just collect all of the ideas without judgement or criticism. There should be items for each of the sources listed here. Some of the hazards may have multiple causes or sources.

If all of the currently know sources of hazards have been gathered, then it is time to organize the causes of the hazard. Take all of the suggestions previously generated and organize them. For each idea place the potential causes for it underneath. So the hazard will have potential causes for it branching out form the hazard. If an item you have designated as a hazard can be used as a cause for another hazards then it is a cause and not a hazard. So you must rearrange the items to get the correct structure of hazards, causes, and subcauses. A cause can apply to several hazards, but a hazard cannot be a cause for another hazard.

This step is important, so reorganize the hazards, causes, and subcauses until the structure is right. Complete the outline or table for the data you have just refined.

STEP 3 ESTIMATION OF THE RISK INDEX
For each hazard and cause, estimate a risk index. This can be done using the matrix or numeric method. Both methods use similar categories, with the matrix being simpler.

The numeric method can also use Detectability, Severity, & Occurrence and a numeric Risk Index value. The numeric value is calculated as the product of the individual ratings. If the ratings range 1 – 5, least significant to most significant, the range of the RI is 1 –125. It is desirable to have the wider range of the RI as the product becomes more significant, so that there is less tendency to split hairs over small differences in the RI.

The matrix uses Severity and Occurrence only. So it is simpler and provides less detail, if this is desired. The matrix uses a rating of the two elements from 1-3. This results in a RI that is one of nine boxes of the matrix. The least acceptable values occurring in the upper right hand boxes.

STEP 4 ACCEPTABILITY OF THE RISK
Review the collected data and calculated Risk Index. Is the risk of each item within the acceptable level if the numeric method is used? With the matrix method, the unacceptable boxes are marked as such, and if an of the evaluations fall in these boxes, more mitigation is required.

STEP 5 MITIGATION OF THE RISK
For each item, list the controls that are put in place to reduce or mitigate the risks. The best controls are those that reduce the severity of the hazard. If the hazard is less severe when it occurs, this is optimal. If the severity is reduced then the effect on all is reduced. Unfortunately this is also difficult to do. The second best approach is to reduce the frequency of occurrence of the hazard. If the hazard occurs with the same severity but less frequent this a good mitigation. The least desirable is to improve the delectability of the hazard. This is the least desirable, and is not even considered by the matrix approach.

STEP 6 EVALUATION OF THE NEW RISK INDEX
After the mitigation is applied, reevaluate the risk. The risks will be reduced in the appropriate area for the mitigation applied. For instance if there is an automatic detection that is applied that will detect every occurrence of the hazard before harm can be done, then the delectability rating might go to 1, so the RI is then reevaluated with the new delectability. If the frequency can be

reduced the occurrence rating will be reduced accordingly, so the RI is then reevaluated with the new occurrence.

STEP 7 TRANSFER THE MITIGATION TO REQUIREMENTS

The mitigations are the requirements that are needed to make the product safer. These need to be added to the requirement documents.