What to Do About Risk

Lev Virine, Michael Trumper, Eugenia Virine

Intaver Institute Inc.
Calgary, AB, Canada

In this article, we are going to learn how to deal with risk. You may be familiar with the PMBOK® Guide which describes a formalized approach to risk management. We are going to use a slightly different approach and focus on how choice engineering can be used for managing project risk. We will discuss a few simple techniques that you can use that will improve your ability to handle risk during the course of your projects.

Make It Simple

A couple of years ago we participated in a risk management conference for the aerospace industry. One of the presentations was titled "Risk Management for Human Space Exploration" and drew an especially large crowd. There were a couple of hundred engineers, researchers and students who gathered to learn about how to manage space exploration risk from a representative of one the largest aerospace organizations. However, topics did not cover risks associated with hostile aliens, deadly space debris, or black holes, instead attendees were presented with descriptions of the multiple regulations, procedures, directives, rules, and other documents which regulate risk management in these organizations. It was mind boggling to see how many documents are created by one particular organization for what is really quite a narrow subject. It probably took at least a dozen man years to write them. Merely showing an extremely compressed version of these documents caused mass lethargy in the audience. In fact, the presenter himself almost seemed to take on the persona of a hypnotist, droning on and on, seemingly intent on putting the crowd in a trance. It may well have happened for after the presentation ended and the lights snapped on, it was as if the hypnotist has snapped his fingers to bring his subject out of hypnosis. People wandered out of the presentation with a slightly mystified look, unable to recall many details of the past hour. This is really not the effect you are going for when you discuss risk processes.

In reality, risk management processes should be relatively simple, especially when you are trying to establish them. To help simplify the processes, choice engineering should be the main foundation of your risk management processes. Along these lines, you should first look to establish a few unobtrusive procedures which will steer people towards make better judgment regarding risk.

Consider these three issues:

1. What events might occur during your project and what would be the impact of these?

2. What is the probability that they will occur?
3. What can we do either to minimize or take advantage of these events?

Many problems occur in the projects because, for one reason or another, people fail to ask these questions. When something happens during a project and causes a major problem and you asked why it happened, most project managers, if they were honest, would answer "We just did not think about it."

Risk management guidelines, procedures, and regulations often hide the most important thing about risk management: it is a *thinking exercise*. So start with these three questions. Later on, when you are more confident, you can begin asking a few more questions, such as what triggered or caused this risk, what is the cost of the risk if it occurs, and so on. The process constitutes *qualitative risk analysis*. If you wanted to perform a more detailed statistical risk analysis based on your project schedule, we refer to this as *quantitative risk analysis*. If you are interested in finding out more about this, it is covered in detail our book "Project Decisions: The Art and Science) (Virine and Trumper, 2007).

To answer these questions, you should create a list of the risks with their probabilities (answer to question 1) and their impacts (answer to question 2). For example, before sending James Bond out to stop an evil mastermind from sabotaging the world's economy, we suspect that his managers would ask him to complete a quick risk list that they had put together as part of their risk engineering process.

	Risk	Probability	Impact
1	Drive on mountain road without brakes	50%	Minor Project Delay
3	Jump from top of sky scraper without parachute	40%	Minor Project Delay
4	Meet with beautiful, yet dangerous woman	99%	Major Project Delay

Risk list of James's Bond project

Strategies for Dealing With Risks

Let's imagine the following situation. The American public tires of having lawyers, actors, and professional sport team managers as the President, instead because a government is a set of complex projects, they elect a professional project manager to run the country. Moreover, due to your demonstrated prowess in delivery successful projects, you are elected Project Manager in Chief. In your first major international crisis, you are informed by your National Security Advisor that the Democratic Empire of Lawless Lands (DELL) has plans to launch new computer virus that will destroy all text documents on infected networks. What should you do?

Remember that you need to ask your National Security Advisor three questions:

1. What might happen during a course of your project and what would be the impact? If the virus is launched successfully onto a national computer network, it will destroy all of the text documents on the infected network.
2. What is the probability that it might happen? Your National Security Advisor estimates that there is a 5% chance that it will be successful. To be more exact, it is better to use an actual percentage for probability rather than a verbal description. Why, if the national security advisor says that chance is minimal, you might think that it is 1%, and he may actually be implying that it is 10%. That represents a large difference in perception of the risk. State estimated probability as accurately as possible to avoid this type of confusion.
3. What can you do about it? This can be quite a difficult question to answer. As project manager in chief, you have decide what would be the best *risk management strategy* given all the possible outcomes of your decisions. Your National Security Advisor may give you few options:

   a). Do nothing. In each set of choices these is always the option to do nothing. Perhaps it would not be such a bad thing if all the text documents were destroyed. It would certainly reduce red tape and bureaucracy. Unfortunately, the problem with bureaucracies is not the documents themselves, but rather the people who manage them. This do nothing option is called a *risk acceptance* strategy in risk management.

   b). Send agents to assassinate DELL's president. This strategy will probably not eliminate the threat, as the president of DELL is not actually the individual who would release the virus, but in theory, it may deter people from releasing virus. This is called a *risk mitigation* strategy.

   c). Develop an antivirus program. This would also be a risk mitigation strategy, as the antivirus is not a 100% certainty and it may take some time to develop it. Essentially the risk has not been eliminated; just its probability and impact are reduced.

   d). Let the Canadian Prime Minister deal with it. This is called a *risk transfer*. Though it is unclear whether the Canadian Prime Minister would take on this risk unless you provided something in return, perhaps eliminating duties on softwood lumber might persuade him, but that would entail political costs. It is the same anytime you transfer risk; their will be a cost as the party it is transferred to will expect some type of payment in return, for example if you purchase insurance against the risk.

   e). Decide to discontinue the use of computers and computer networks in the government, back to paper and abacus. This strategy is called *risk avoidance*. By eliminating the use of electronic documents, we manage to avoid the risk.

The only way that you as the President could select the best risk handling strategy strategy is to perform a more detailed analysis. We will give you an idea about how the President should select an alternative later, but before that, we will discuss how to compare different risks.

How to Build a Rocket or Risk Ranking

What if rocket science was not actually rocket science? If you are not an aerospace engineer or otherwise employed by the industry, here is a simple explanation on how to build a rocket. Basically speaking rocket design is fairly straight forward process. At a high level, it requires only engines, fuel tanks, and a pay load. To ensure reliability, you can add many redundant systems, sensors, and enforce it to ensure it can withstand even the most extreme launch forces. Your rocket would never explode, but it would never fly: it would be too heavy. To decide which systems or components will have the most affect on improving reliability or safety and should be included in the design, engineers must analyze and rank multiple risks. The simple way to do it would be multiply probabilities on impact. Risks with higher ranks should be mitigated or avoided first. In case of James's Bond project, the most important risk would be "Meet with beautiful, yet dangerous woman" and risk "Drive on mountain road without brakes" would be the ranked second.

This type of process is used by engineers at the SpaceX corporation. SpaceX is an American space transport company that builds the Falcon 1 and Falcon 9 rockets and the Dragon series of spacecraft that will be orbited by the Falcon 9 launchers. NASA is planning to use SpaceX rockets for resupplying the International Space Station after the Space Shuttle retires in 2010. During the planning of one of the early launches of the Falcon rocket, SpaceX engineers decided to mitigate their 10 most critical risks. For all remaining risks, they just chose to accept as the most effective strategy. Almost predictably using hindsight, the launch failed because the 11^{th} ranked risk occurred (Insprucker, 2008).

But were the engineers incorrect in their ranking or should they have chosen to include the 11th risk as part of their mitigation plans? We will review a potential solution later.

Should We Protect Commercial Airplanes Against Surface-to-Air Missile Attacks by Terrorists*?*

Do you protect yourself against dog bites? You could wear special Kevlar pants that would be difficult to bite through; you might instead opt to carry a T-bone steak with you that you could use to distract menacing dogs while you climb up the nearest tree. Or do you really put much credence to this at all, sure you might get bitten, but unless you are a mail man, we doubt that you are taking all necessary precautions. Why? Because if you have done a risk assessment, you would probably come to the same conclusion as pretty well everyone else around you, the chance that you will be bitten by a dog is very slight. In fact this is an illusion. The official survey determined there were 4.7 million dog bite victims annually in the USA. A more recent study showed that 1,000 Americans per day are treated in emergency rooms as a result of dog bites. In 2007 there were 33 fatal dog attacks in the USA and losses due to dog attacks exceeds $1 billion per year, with over $300 million paid by homeowners insurance (Dog Bite Low, 2010). When you decide how to deal with potential dog attack you intuitively determined the probability and, to a less extent, the impact of the risk. Since the probability and impact did not seem very significant, you decided not to take any precautions other than avoiding the attention of mean looking dogs.

Here is another example. A few years ago, the government asked experts in decision analysis to conduct a research on whether we should install special defensive equipment on commercial aircraft to protect against surface-to-air missile attacks by terrorists. One of the

motivations behind this research was a failed attempt by terrorists in Kenya to shoot down an Israeli commercial airplane in December 2002 using shoulder mounted missiles similar to the relatively compact Stinger missiles used in the James Bond movie "License to Kill"

Here is a brief description of the problem the experts were asked to address. There is a chance that terrorists will try to use such missiles to shoot down planes. The anti-missile technology that they were considering is available for military planes, but it is very expensive. Can they, the government, justify the cost of installing this equipment on each commercial plane operated in US given the potential risk? The researchers first analyzed the chance that terrorists would be able to mount such an attack, and then the chance that one of these attacks would actually bring down a plane (von Winterfeldt, 2008). Once they had determined this, they calculated the cost in monetary terms if the plane was lost. Finally, they calculated the cost of installing and operating the missile defense equipment on every plane. As it happens, it would be very expensive – millions of dollars per plane. The researchers concluded that unless the cost of the equipment was drastically reduced, it would not make any economic sense to install the devices. The results of the study were presented to policy makers and they agreed not to require the installation of these devices. The current risk management strategy is to accept this risk, at least for now.

You may question whether a straightforward economic cost/benefit analysis is the right way to go about making this decision, what about the cost in human life and suffering, the grief of the loved ones, how can you measure that. Well, you can't, but you have to be able to use some measure to assess and make decisions regarding risk in a meaningful way. Analysis of the *potential loss* is a valid approach that will help you to decide on a course of action. The concept is very simple:

1. Calculate the potential loss, which is the cost you will have to pay if the risk occurs. For example, as President you are told the potential loss due to the DELL virus is approximately $100B.
2. Calculate of cost of mitigation efforts. If you decided to develop an anti-virus program it is estimated to cost $10,000,000.
3. Calculate total cost associated with risk: potential loss multiplied on probability of risk plus cost of mitigation efforts. In our example it would be $100 B (potential loss of the virus attack) * 10% (probability) + $100,000 (antivirus development) = $10,001,00,000.

4. Perform similar calculation for different risk management strategies. If you decide to transfer the risk to the Canadian PM, the potential costs in terms of political capital as well as lost forestry jobs in the US may make it one of your less advisable courses of action.

Zero-risk bias

A friend of ours was very concerned about the risk of medical mistakes. Reading and hearing examples and statistics about medical mistakes had caused him to become quite anxious, so he decided to eliminate this risk by refusing to see a doctor regardless of his symptoms. No doctors – no potential mistakes – very straight forward solution. The problem was that he significantly increased his chances of another risk: the risk that if he got ill and it would go untreated.

A lot of people believe that the best strategy is to completely eliminate risk. However, completing eliminating risk can be extremely expensive and can cause other risks. In most cases, a better course of action is to reduce the probability and impact of risks in the most cost effective manner. In our example with the threat of a computer virus, one option for the President is to completely eliminate the risk by ordering the government to discontinue the the use of computers and computer networks (option e). While this would eliminate the risk, it would be very expensive and could trigger many other risks.

Zero risk bias is common when people make decisions about health, safety, and environment. This bias often manifests itself in managing hazardous waste, using nuclear energy, and rules and regulation regarding public safety. If you want to completely eliminate an accident on an assembly line, you have two choices:

1. Replace all workers with robots including those workers who maintain and repair the robots.
2. Shut down the assembly line.

A more realistic solution for the assembly line would be to use some robots in addition to additional safety measures to reduce the chance of accidents.

Risk Engineering

Bridges across river are designed to withstand large floods. But what if there is a massive once in a 100 year flood? Floods like this will probably destroy most bridges, but it is not a design flaw. In fact, it is a part of the construction code. Can a bridge be built to withstand these types of events? Of course it can, but it would be cost prohibitive. Instead of having many conveniently located river crossings with fast flowing traffic, you would have only a few and traffic would slow to a crawl. Since the chance that an extreme event is relatively small, it is cheaper to rebuild a bridge if it is destroyed rather than over-engineer it in the first place. Bridge

engineers must select the right balance between different risk mitigation strategies to make this bridge cost effective.

Risk engineering involves accepting, mitigating, avoiding and transferring certain risks in such way that the final project is cost-effective and less risky at the same time. This requires that you analyze different combinations of risk management strategies on a full set of project risks.

> Risk engineering is a continuous process of balancing risk response strategies for different risks in the project or program.

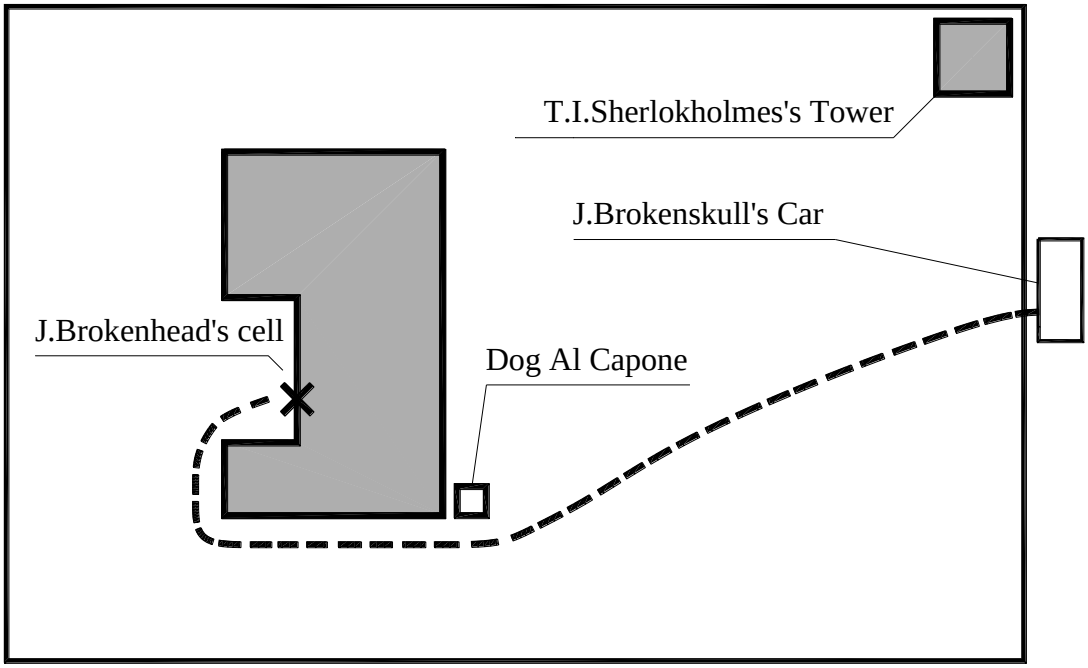
When considering risk engineering, it is most important is that it is performed continuously over the course of a project. During the project lifecycle, the risk management strategy may change based on new information. This balance between between various risk handling strategies will change as well. If as a result of the unsuccessful SpaceX rocket launch, the 11th ranked risk is now considered critical for future launches, it must be avoided. However, since all risks associated with this rocket cannot be avoided, the strategy for another risk may have to be shifted from avoidance to mitigation. In the example we provided regarding the surface-to-air missile protection for the commercial airplanes, the cost of such systems may go down. In this case, it becomes a viable response to switch the risk management strategy from acceptance to mitigation.

When Quantitative Risk Analysis is Necessary

John Brokennose is two things, both a professional criminal and a poor project manager. He is currently serving time in a state penitentiary for a failed bank heist. He lent some of his tools to his son for his son's school science project and, as a result, did not have them with him when he tried to open the bank vault. Now he sits in his cell planning his next project, escaping from the prison. He has already created a preliminary plan. Here are his planned activities:

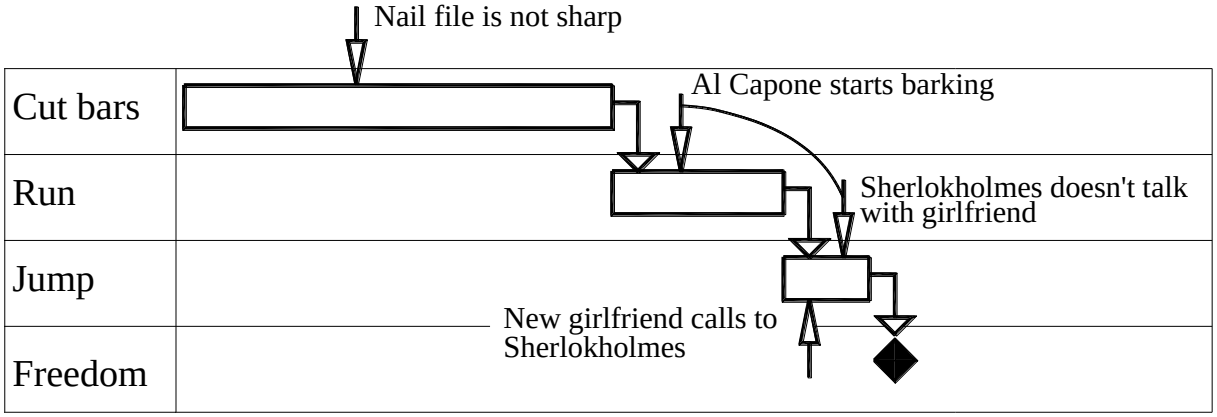
1. Cut through bars on windows: estimate 30 minutes, but these is 50% chance that his nail file will not be very efficient, which could add an additional 10 minutes.
2. Jump from the window and carefully walk towards outside fence, avoiding discovery by guards. He estimates that it will take around 15 minutes. However, there is 30% chance that the guard dogs might be alerted and start barking. Additional evasive maneuvers will cause a delay of 10 minutes.
3. Climb the fence. John has noticed that the guard T.I. Sherlokholmes, who will be on watch duty in the tower, spends 75% of the time of time talking on his cell phone to one of his three girlfriends and doesn't pay any attention to the fence during this time. John has to wait on average 5 minutes until one of the girl friends calls.. However there is also a 10% chance the guard will unexpectedly get a call from a new girlfriend, which will reduce his wait time by 5 minutes.

4. Jump into his associate Jack Wideneck's car. Jack will be waiting for John outside of the fence.



The plan is simple. But there is one additional complication. Jack Wideneck cannot stop his car by the fence for long and John cannot wait for the car. The car must be underneath where John is waiting within a 10 minute window. The question is when John should start to cut the bars to make sure that he lands in the car with 95% probability?

This is an example of a situation when the question cannot be answered without quantitative analysis. John Brokennose must perform this analysis before starting his escape plan. To start with, he has to create a schedule in the form of a Gantt chart. Then he draws risks associated with each task as arrows on the Gantt chart. The project has three threats and one opportunity (if a new girlfriend decides to call Sherlokholmes). Gantt charts with arrows representing risks are called *Event Chain Diagrams*. Threat arrows point down, opportunity arrows are point up, quite simple and intuitive. If threats or opportunities are related to each other, they are connected by line. For example if a guard dog starts barking, Sherlokholmes may stop his conversation with a girlfriend. The size of an arrow represents the probability of the risk. Event chain diagrams can significantly simplify risk analysis.



Now John Brokennose should use a software program to perform the analysis. He enters project schedule and all risks, assign risks to activities, defines their probabilities and impacts, and performs a calculation. For purposes of brevity, we will skip the mathematical details of how the calculation is performed.

The result of analysis shows that Jack Wideneck must wait in the car for John Brokennose for 22 minutes to ensure that these is 95% chance that John Brokennose will not be discovered, which insignificantly higher than John originally estimated. According to the analysis, the chance of a successful prison escape is only about 70%. John Brokennose is very risk averse and had to abandon the escape plan.

If John Brokennose wants to increase his chances of escaping from prison, he will have to perform some risk engineering. His prison escape plans includes three risks:

1. Nail file doesn't cut quickly enough. Originally, the chance that this risk would occur was 50% and the impact was a 10-minute delay. John believes he can avoid this risk by using a good hacksaw.
2. The guard dog starts barking. John Brokenhead cannot do anything about this and must accept this risk.
3. Sherlockholmes does not speak with one of his girlfriends. Originally, there was a 25% probability that it would cause a delay of 5 minutes. What if John Brokenhead finds an additional girlfriend for Sherlockholmes. This would reduce the probability to 15%.

Now we can perform this analysis again. The results show that Jack must park near the fence for 15 minutes to ensure that there is a 95% chance that John will cross the fence while the car is there and not be discovered. Better, but still not good enough, plus John needs to find a hack saw and a new girlfriend for Sherlokholmes. Perhaps John could try a different scenario to deal with the risks. He could slip some drugs into the dogs' food, which would mitigate the barking risk, and then he might have extra time and not need a hack saw. As part of risk

engineering, we recommend an analysis that uses different risk management plans for each risk be performed multiple times to determine the best course of action.

Unfortunately most criminals do not perform risk analysis before engaging in criminal activities. If they did, they probably would not involve themselves in criminal activities in the first place. Project managers often follow the same path and do not perform risk analysis, in spite of the fact that they have all tools in their disposal to ensure that they don't expose their projects to unnecessary risk.

References

Insprucker, J. 2008. Sometimes Your Top Ten Risk List Should Include Eleven. In Proceedings of 2008 Space Systems Engineering and Risk Management Symposium. February 26–29, 2008, Los Angeles, California

Virine L. and Trumper M. 2007. Project Decisions, The Art and Science., Vienna, VA: Management Concepts.

von Winterfeldt, D. 2008. Should We Protect Commercial Airplanes Against Surface-to-Air Missile Attacks by Terrorists. In Proceedings of INFORMS Annual Meeting, Washington DC, 2008, October 12-15

About the Authors

Lev Virine, PhD

Intaver Institute
Alberta, Canada

Lev D. Virine, Ph.D. has more than 25 years of experience as a structural engineer, software developer, and project manager. He has been involved in major projects performed by Fortune 500 companies and government agencies to establish effective decision analysis and risk management processes as well as to conduct risk analyses of complex projects. Lev's current research interests include the application of decision analysis and risk management to project management. He writes and speaks around the world on the decision analysis process, the psychology of judgment and decision-making and risk management. Lev can be contacted at lvirine@intaver.com

Michael Trumper

Intaver Institute
Alberta, Canada

Michael Trumper has over 20 years' experience in communications, software design, and project risk and management. Michael is a partner at Intaver Institute Inc., a vendor of project risk management and analysis software. Michael has authored papers on quantitative methods in project estimation and risk analysis. He is a co-author of two books on project risk management and decision analysis. He has developed and delivered project risk analysis and management solutions to clients that include NASA, DOE, and Lockheed Martin.

Eugenia Virine, PMP

Alberta, Canada

Eugenia Virine, PMP, is a senior manager for revenue development at Greyhound Canada. Over the past 12 years Eugenia has managed many complex projects in the areas of transportation and information technology. Her current research interests include project risk and decision analysis, project performance management, and project metrics. Eugenia holds B. Comm. degree from University of Calgary.