Nov. 2012

Risk Management Processes –
A Quantitative Model for Fusing Cost and Time of Risks and Risk Response Actions

Bernard M. Gordon Center (BMGC)
The Technion – Israel Institute of Technology

Dr. Moshe Weiler
The Technion – Israel Institute of Technology

Dr. Avner Engel
Tel-Aviv University

Table of contents

Abstract

A difficult question which concerns anyone involved with risk management is how one should select an optimal Risk Response Action (RRA) strategy. One of the first steps needed to achieve this aim is to quantify the cost and time associated with the risk handling strategy. This paper briefly describes several existing quantitative risk management methods and presents a new quantitative model for determining the cost and time of performing risk management throughout the system's lifecycle. The model combines costs/times associated with performing a given RRA strategy together with expected risk impacts. In addition, the paper describes a use-case based on a historical pilot project aimed at developing and fielding a new avionics system for transport helicopters. We use traditional risk management terminology to quantify costs and times associated with risks, risk probabilities, risk impacts and risk response actions and argue that quantitative modeling of the risk management processes will lead to optimizing the risk response strategy which will usher considerable reduction in overall systems' lifecycle costs while increasing systems' availability time.

1. Introduction

1.1 Motivation and contents

In the past decade, one of the authors was involved in the field of Verification, Validation and Testing (VVT) of systems throughout the systems' lifetime. In this domain, it is virtually impossible to prove that the system is completely free of faults. Typically, the tester may ask: What in the system should be tested? How should one test? When should one test? And, when should one stop testing? Or better said, how should one select a VVT strategy and how should it be optimized? A method for modeling the VVT cost and time and optimizing system VVT strategies is described in Engel, (2010[1]).

Similar questions exist in the risk management domain. In particular, risk management practitioners grapple with the issues of selecting and optimizing their Risk Response Action (RRA) strategy. Therefore, the purpose of this paper is to add to the existing repertoire, a new method for modeling the cost and time associated with the risk management process, based on the above-mentioned VVT research. The key contribution of this paper is the philosophical and mathematical fusion of cost and time elements associated with systems' risks, together with their corresponding Risk Response Actions (RRAs) strategies. The payoff of this approach is in the optimization stage, where optimal RRA strategy can be naturally derived from this fused modeling. By and large, current quantitative risk models deals with the former and ignore the latter so an overarching risk management optimization is not achieved.

In a future paper we will expand this topic dealing with the optimization of the risk response strategy in order to achieve typical optimization objectives like reducing the overall cost/time associated with the risk management process, reducing the variance of the predicted process cost/time, removing risk outliers and other important issues.

This paper is divided into the following main sections. 1) An introduction covering motivation and contents, basic risk management concepts and historical models for cost of quality, 2) literature review on quantitative risk modeling, 3) overview of the proposed risk management process model, 4, 5) quantitative modeling of risk management cost and time, 6) a risk management use-case and 7) a discussion and conclusion. Finally, Appendix-A provides raw data for the use-case.

1.2 Risk management concepts

Risk Management provides us with a lifetime proactive process for resolving uncertainties that may reduce the stakeholders' value of a project or a system. Some of the major tasks in Risk Management Process are performing Risk Identification, initial Risk Assessment, Risk Prioritization, as well as the development and implementation of a risk handling strategy (see for example, Pennock and Haimes, 2002, Weiler et al., 2010). Throughout our paper we use the following terms (see ISO 31000, 2009).

---

[1] See also: Hoppe et al. (2007), Engel and Last (2006), Barad and Engel (2006), Engel and Shachar (2006), and Engel and Barad (2003).

- Risk - An uncertain event or set of circumstances that, should it or they occur, will have an effect[2] on achievement of one or more objectives (APM, 2004). In this paper, risks will be measured in terms of waste in the domains of Risk Cost $(Risk_c)$ or Risk Time $(Risk_t)$.
- Risk Probability $(P,\ 0 < P < 1)$ - The likelihood of a risk event to actually materialize. One should note that when an impact event does happen (i.e. the Probability equals 100%) we no longer call it a risk, but rather a problem (to be resolved).
- Risk Impact (I) – The impact upon the system, if the risk event will, in fact occur (commonly called consequence of occurrence). In this paper, impacts are measured in terms of waste in the domains of Impact Cost (Ci) or Impact Time (Ti) [3].

Risk may be manifested as some combination of Risk Probability and Impact Cost or Impact Time. Traditionally, however, risk is computed by multiplying the probability of an undesired event by the impact or consequence of such an event. In this paper we assume that these components are statistically independent and, the basic relationships among these elements are Risk Cost $Risk_c$, $Risk_c = P * Ci$ and Risk Time $Risk_t$, $Risk_t = P * Ti$.

Risk Response Action (RRA) is the process of eliminating or reducing perceived impacts to a project or system. This is commonly done by reducing either the probability (P) of the identified risk or the Impact Cost (Ci) or Impact Time (Ti) (i.e., time wasted) associated with the risk in question (as well as any combination of these elements). Our risk management model assumes that actual risks impacts emerge as a result of partial (or no) performance of RRA. Obviously, the risk response process itself entails Response Cost (Cr) and Response Time (Tr). Therefore, the art of devising an optimal response strategy is to optimize the system's cost, performance and delivery time or a combination thereof.

1.3 Historical models for cost of quality

Generally, there is a negative correlation between risk response investment and systems' failure cost. Early in the 1950s, two quality luminaries (Joseph Juran and Philip Crosby) proposed two different qualitative models, defining "quality cost" as the sum of risk mitigation costs plus failure costs. Juran suggested that there is an optimal risk mitigation strategy that will yield minimum total cost (Juran and Gryna, 1980).

Crosby coined the slogan "Quality is free", advocating the notion that the more one invests in quality the more savings will be realized (Crosby, 1979). Translated into the risk management domain, "the more one invests in risk response efforts the more savings are realized". Despite the beauty of Crosby's slogan, many practicing engineers agree with Juran. The main reason for that agreement is that the cost of preventing the "last problems" increases exponentially, rather than linearly (see Figure 1).

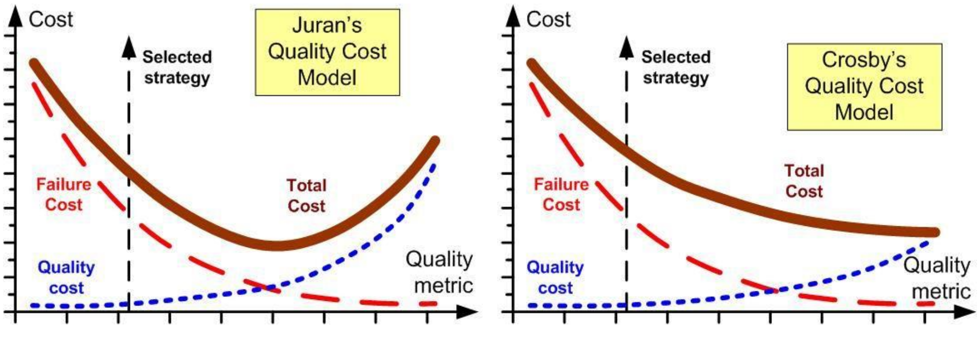


Figure 1 - Qualitative cost of quality models

---

2 Traditionally, risks are considered in negative connotation as threats, potentially impacting systems in an undesired way. More recently, the term risk has been extended, referring both to threats and opportunities. Our preference is to employ the term "Risk" within its widespread, daily interpretation as a threat, accepting the term "Opportunity" as its counterpart. We share Haimes' (2009) view that risk and opportunity associated with a system, can be explained and quantified through a systems-based theoretical approach.

3 Technical risk is the possibility that the "system may fail to achieve performance requirements; to meet operability, producibility, testability, integration requirements; or to meet environmental protection requirements" (INCOSE-2011). Ultimately, such failure results in losses (i.e. cost and time) in attempting to rectify the problem or other losses in the marketplace. Therefore, the input data to the model should take into account these losses. Bottom line: Our model assumes that such consequences are already embodied within the first two components and we do not address this aspect within this paper.

The main weakness of both models is that they are qualitative and therefore do not help in designing practical risk response strategies. Even if an optimal risk response strategy cost could be identified, large numbers of risk response strategies of equal cost would be possible so the question remains: which one is the best?

2. Literature review on quantitative risk modeling

The following is a quantitative risk modeling state-of-the-art review.

2.1 Risk modeling in systems development projects

In system development projects, the consequences of ignoring risks are system failures, project completion delays or costs overruns. Software development projects attract most of the attention of risk management experts; as this domain is historically rife with the above problems, leading in a fair number of cases to project cancelations and heavy fines. These are the commonly applied risk models:

1. ***"Conventional" risk management modeling***. The vast majority of systems development projects use a risk matrix as a means to visualize and rank risks (See for example, INCOSE-2011 Systems Engineering Handbook, NASA's NMP-GL-07-V1, 2005). Typically, risk matrices are composed of 5x5 or 9x9 elements. One axis represents the likelihood of risk occurrence in numerical or textual values (e.g., 1=very unlikely, 2=unlikely, 3=occasional, 4=likely and 5=very likely). The other axis represents the consequences of a realized risk (e.g., 1= negligible, 2= minor, 3= moderate, 4= major and 5= extreme). The ranking of risks is done by multiplying the likelihood of risk occurrence by the consequence of a realized risk. The advantage of this method is that it is simple to implement and there exist many commercial tools supporting it. On the other hand, the numbers assigned to each axis represent arbitrary relationships so risk ranking and, especially, interpretation of risk significance may be skewed.
2. ***Stochastic simulation modeling***. Houston et al. (2001) describe a stochastic simulation system that models risk factors and simulates their effects, as a means of supporting certain software development risk management activities. They stochastically simulated the effects of six widespread software development risk factors, in order to ascertain the consequence of the following traditional risk management activities: 1) assessment, 2) mitigation, 3) contingency planning and 4) intervention. We think that the main advantage of their approach stems from the dynamic view provided by their method, as contrasted with direct probabilistic computation.
3. ***Neural network modeling***. Hu et al. (2007) employed a Neural Network (NN) and a Support Vector Machine (SVM) for supervised classification and learning, in order to model a risk evaluation in project development. In their model, the input is a vector of software risk factors that were solicited from domain experts, and the output is the final outcome of the project. Their described model was validated with data collected from 120 real software projects and enhanced using various genetic algorithms. The main advantage of this approach stems from the learning capability of Neural Network systems. As more data is collected and the higher the quality of the data, machine training can achieve more and more accurate predictions.
4. ***Riskit modeling***. Professor Jyrki Kontio proposed this risk management method in 1996. It provides precise and unambiguous definitions for risks, resulting in explicit definition of objectives, constraints and other drivers that influence a project. It documents risks qualitatively and models the process using the concept of utility loss, to rank the loss associated with risks (Kontio, 1997). One advanced application of the Riskit methodology is described by Kyoomarsi et al. (2008). These authors first changed the Riskit analysis graph using fuzzy logic and then added new diagrams and tables, utilizing a Unified Modeling Language (UML) terminology like risk management cycle, process definition information template etc. Finally, Kyoomarsi et al. describe an optimized Riskit method. The main advantage of this approach stems from the clear definitions and organized approach inherent in their approach.
5. ***Goal-driven modeling***. Islam (2009A, 2009B) describes a goal-driven risk management model for assessing and managing software development risks. Such risks emanate from both technical and non-technical elements. For example, key management risk factors affect offshore outsourcing of software development. In offshore outsourcing, development activities are usually moved to low-cost development environments that are locally managed. However, outsourcing also entails moving control

and responsibility away from the main contractor, substantially increasing system development complexity and risk. The author utilized Delphi surveys to obtain typical goals and the risk factors in a different cultural environment for offshore vendors in Bangladesh. Thereafter, a goal-driven software development risk management modeling (GSRM) was used to supports appropriate management decision.

6. ***Association rule mining technique***. A variant of Goal-Driven modeling is proposed by Shan et al. (2009). Here an estimation of a software project success potential uses an association rule mining technique. Their approach identifies the relationship between individual risk dimensions and project outcome. Such association rules take risk dimensions as the condition and the project outcome as the result, thus providing project managers means to estimate whether a project will succeed or fail.

7. ***Simple fuzzy logic modeling***. Caballero and Yen (2004) propose a simple method of evaluating risks and uncertainty factors affecting a construction project. Relevant data is obtained using questionnaires and in-depth interviews. From which, a risk management fuzzy logic model is constructed for identifying optimal risk mitigation strategy. We think that the main advantage of this approach stems from the relatively easy manner in which raw data is obtained, appropriate to somewhat less sophisticated organizations.

8. ***Multiobjective decision trees and Multiobjective risk impact analysis***. Dicdican and Haimes (2005) compare two decision support methods: Multiobjective decision trees and Multiobjective risk impact analysis. Multiobjective decision trees include multiple, usually independent, objective functions over a given period whereas Multiobjective risk impact analysis evaluate risk and decision impacts in a dynamic framework. Depending on various statistical assumptions, modeling risks using the two methods should provide similar results. The authors illustrate these two methods by considering a highway section that must be paved at certain intervals. Similarly, funding decisions must also be made depending on specific objectives. The decision-maker considers what action is best for each budget interval, what the effects of the action will be and what option should be adopted. Under the above simplifying assumptions, the two methods yield equivalent solutions.

9. ***Efficient risk response Actions set.*** Kujawski, (2002) uses Markowitz's portfolio selection principles in order to optimizing project RRA strategy by way of Monte Carlo simulation. Risks and RRAs are characterized using scenarios, decision trees, and cumulative probability distributions. Consequently, decision-makers can select an optimal RRA set in accordance with their attitude toward project risk. As we will see, the basic aim of this research is similar to the one presented in this and the future companion paper (i.e. regarding both risks and RRAs). However, Kujawski's approach treats the RRAs set as whole, whereas we treat each risk and corresponding RRA individually.

10. ***Dynamic risk response actions modeling***. Recently, Kujawski and Angelis (2010) point out that the sources and consequences of risks evolve and change over systems' life. Therefore, risk mitigation or, in more general terns, Risk Response Actions (RRA)[4] should be considered beyond macroscopic perspectives by evaluating and tracking project-specific risks and RRAs at the microscopic level as well. The key elements of this microscopic approach are: 1) develop risk scenarios, 2) model these scenarios using generalized decision trees, and 3) quantify the risks in these scenarios using stochastic simulation (e.g. Monte Carlo simulation). Dynamic risk curves may be generated to provide the necessary information to analyze, track, and manage the performance of the selected RRAs over time. Project managers can then use the information thus generated in order to dynamically manage the RRAs in accordance with a changing project situation. The beauty of this approach stems from the dynamic visibility of risk reduction actions over time as a function of different risk response strategies. However, in real life situations, the combinations of different strategies increase exponentially, causing a strategy permutation explosion for all but the most trivial cases.

2.2 Risk modeling in finance

Numerous papers describe risks models employed within the financial sector. The one introduced by Chen et al. (2008) is worth discussing. These authors proposed a generalized hyperbolic adaptive volatility (GHADA) risk management model based on the generalized hyperbolic (GH) distribution and on a nonparametric adaptive methodology. Compared to a normal distribution, the GH distribution has semi-heavy tails more appropriately representing the financial risk factors. Nonparametric adaptive

[4] Uncertainties may cause undesired impacts to be mitigated but also, may lead to opportunities to be exploited.

methodology has the desirable property of being able to estimate homogeneous volatility over a short time interval and accurately reflect a sudden change in volatility. Chen et al. provide an example, showing that the proposed model provides a more accurate Value at Risk (VaR) parameter than would models that assume either a normal or t-distribution. A t-distribution is a continuous probability distribution that arises when estimating the mean of a normally distributed population, where the sample size is small.

2.3 Risk modeling in manufacturing

Enyinda (2008) describes a risk modeling methodology for managing disruptive risks in pharmaceutical global supply chain logistics and selecting the optimal mitigation strategy. His paper describes a multi-criteria analysis using Analytic Hierarchy Process (AHP). AHP (Saaty, 1980) is a structured technique for dealing with complex decisions used to support decision makers in finding an optimized risk policy options. The results indicate that, in this particular industry (i.e. highly regulated and supply-chain dependent), regulation/legislation risks are the most important risk factor, followed by operational risks and reputation risks. Among the classic alternative policy options, risk reduction is the most important risk mitigation strategy, followed by risk transfer, risk avoidance, and risk acceptance.

2.4 Risk modeling in Systems of Systems (SoS)

1. ***Natural disasters, accidents, and terror risk modeling.*** Yan and Haimes (2010A) suggest a somewhat similar approach to the one described by Enyinda. Here, the problem is how to mitigate risks emanating from natural disasters, accidents, or deliberate military or terror attacks against large-scale hierarchical systems (i.e. systems of systems). Such systems are characterized by geographical dispersion and having multiple decision makers in various roles, each with different risk management objectives. The authors propose a Multiobjective Multi-Decisionmaker Resource Allocation (MOMDRA) model and a Hierarchical Multiobjective (HMO) approach to generate Pareto optimal resource allocation strategies to reduce or eliminate potential risk impacts. In a companion paper (Yan and Haimes, 2010B), the authors demonstrate the applicability of the MOMDRA framework by means of a case study depicting the hurricane protection water pumping system in the greater New Orleans area, which played a critical role during the Katrina disaster. Hurricane Katrina struck southeast Louisiana and the city of New Orleans on August 29, 2005. It breached the levee system and flooded some 80% of the city. Over 1,800 people lost their lives and the property damage was estimated at 80 billion dollars.
2. ***Probabilistic risk assessment modeling.*** Stamatelatos et al., (2002) describe Probabilistic Risk Assessment (PRA) procedures that reflect the best thinking of NASA's post-Challenger accident. These PRA procedures are also used in other large and high-risk industries, such as nuclear, petrochemical, automobile, offshore platforms, defense, etc. In fact, because of its logical, systematic and comprehensive approach, PRA has repeatedly proven capable of uncovering intricate design and operation weaknesses. The crucial insight emanating from this research is that "it was very important to examine not only low-probability and high-consequence individual mishap events, but also high-consequence scenarios which can emerge as a result of occurrence of multiple high-probability and nearly benign events."

2.5 Catastrophic risk modeling

Catastrophe modeling is a risk management technique for assessing the losses caused by unusual natural or man-made catastrophes. There are a number of commercial catastrophe modeling tools used by insurance companies, government agencies, and academia. Such tools combine historical and geographic disaster information with current demographic, infrastructure, scientific and financial data to determine the potential cost of catastrophes for specified geographic areas (see for example: Wallace and Ziemba (2005), Grossi and Kunreuther (2004). Typically, catastrophic modeling entails four steps:

Step-1: Define hazard phenomena. This first step involves the generation of a stochastic event set, which is a collection of scenarios. Each event is defined by a specific strength, location, and probability of occurrence. Many possible event scenarios are stochastically simulated based on realistic parameters and historical data to probabilistically model potential catastrophic events.

Step-2: Assess level of physical hazard. This second step entails the assessment of the hazard component of the catastrophe. That is the level of physical hazard that may occur within the defined geographical area at risk. For example, modeling an earthquake catastrophe will determine the level of ground motion across the region of interest.

Step-3: Quantify population and property vulnerability. This third step entails the calculation of the expected harm to population and property at risk. Parameters defining this susceptibility include size and distribution of population as well as existing infrastructure in the affected area. Different vulnerability curves are used to estimate human vulnerability and property damage as well as time element coverage, such as business interruption, loss or relocation expenses, etc.

Step-4: Measure loss from various financial perspectives. This final step entails the translation of physical damage to humans and property into total monetary loss. Some, more sophisticated catastrophic modeling tools calculate cost parameters for different mitigation policy strategies.

3. Overview - risk management process model

3.1 Risk management horizon and response strategy

We start by defining the following two concepts: *Risk Management Horizon* and *Risk Response Strategy*:

1. Risk Management Horizon is defined as “a specific sequence of system phases for which the modeling results of risk management process is of interest to the stakeholders of a given system”.
2. Risk Response Strategy is defined as “a policy, for a given risk management horizon, under which, a subset of the RRA is fully performed, another subset of RRA is partially performed, and the remaining RRAs are not performed at all”.

Figure 2 shows a specific risk management horizon and risk impacts emanating from a specific RRA strategy[5]:

- In this example, the risk management horizon encompasses the Definition, Design, Implementation, Integration and Qualification phases, thereby ignoring the rest of the system lifecycle phases (Production, Use/Maintenance, and Disposal), which are identified in the figure with large X's.
- The RRA strategy in this example is: “Perform a part or none of each risk response action during the Definition, Design and Implementation phases” and "Fully perform each risk response action during the Integration and Qualification phases”.
- This horizon and strategy selection exposes the system to risks as depicted in the figure. We can see that, based on this risk response strategy, each of the first three phases generate risks that may affect the current phase as well as all the following phases within the risk management horizon. For example, since the RRA strategy during the Definition phase is only partially performed, some risks may affect the system during the Definition, Design, Implementation, Integration and Qualification phases.

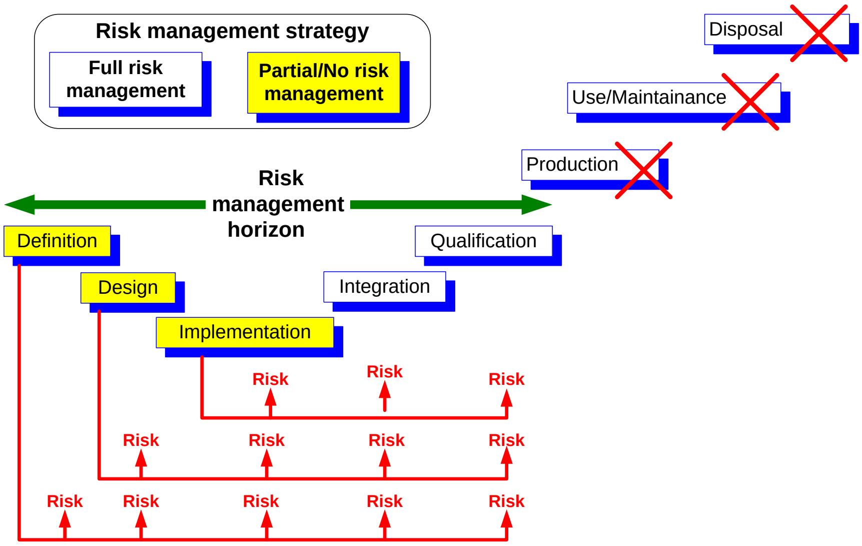


Figure 2 – Example of risk management horizon and strategy

5 The figure shows a linear progression of steps which, on the surface, appears to contradict how risk management is performed in practice. However, engineering activities, by and large, are planned on a more or less linear progression of events. Then, when unexpected event do happened the plan is updated as needed (again, more or less along linear lines).

3.2 Risk management scenario

We describe a Risk Impact Scenario[6] (see Figure 3) in which a given risk exists. The relevant Risk Response Action is either partially performed or not performed at all (we identify it in the figure with a large X). As a result, some RRA cost/time expenditure is saved (we identify it in the figure with a small X). Consequently, a risk impact may occur with a probability P $(0 < P < 1)$, causing a resource expenditure and/or time delay. The impact may occur during the current system lifecycle phase or during any subsequent phase.

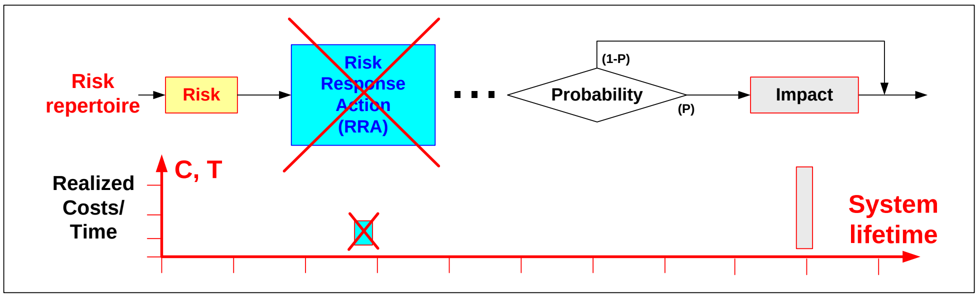


Figure 3 – Risk Impact Scenario

3.3 Risk management modeling overview

For a given risk response strategy, the estimation of actual cost is a straightforward process. Assuming we are interested only in efforts of individuals involved in the process, we simply sum up these cost components. The key problem to be addressed is: "How to estimate costs/times emanating from partially performing risk response?" Accordingly, this paper proposes systems' risk management process model which hinges on three quantitative sub-models associating a given risk response strategy with system behavior and failure consequences.

1. A *Canonical Risk Model* (CRM) - a maximal set of risks together with their individual occurrence probabilities, costs, time durations, and instance (i.e., system lifecycle phase) of potential impact.
2. A *Risk Response Model* (RRM) - a set of risk response actions together with their individual costs, time durations and instance of execution.
3. A *Response Strategy Model* (RSM) - a corresponding set of decision variables identifying the actual planned risk response performance levels.

Within this risk model, these particular three sub-models, with their individual datasets, represent a minimal ensemble required to compute the overall cost/time of the risk management process. The CRM defines all the risks that may affect the system, the RRM defines the space of potential risk response actions and the RSM defines the selected strategy to respond to the identified system's risks (see Figure 4):

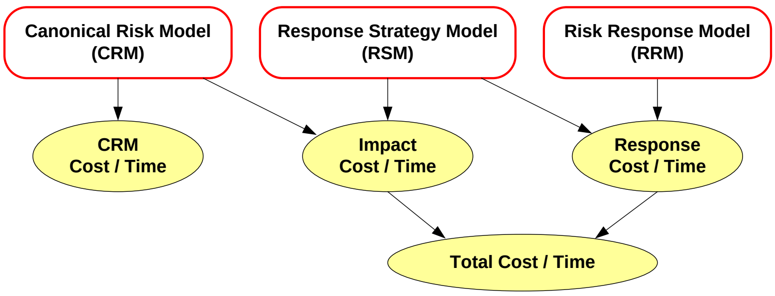


Figure 4 – Overall risk management cost/time model

We embrace recent scientific thinking, which maintains that risk uncertainty emanates from inherent stochastic variability as well as from fundamental lack of knowledge (Oberkampf et al., 2002). Accordingly, we develop a method for computing the cost and time associated with system's risk management processes.

[6] Anticipatory Failure Determination (AFD) provides a systematic way for identifying potential future failures (AFD is a successor to TRIZ, a research effort conducted in the former Soviet Union). AFD methodology offers a strategy to identify failure scenarios by way of finding possible failure initiation events and drawing the resulting failure trees from each. Initiating events are defined as failures of individual subsystems or components of the system as well as unexpected external events. Thus, for a given system, one would work through each system element, asking, "What would happen if this part failed?" or "What kind of external event can cause this part to behave in an unplanned manner?" This process can be carried out at various levels of detail and thoroughness and every failure scenario can be broken down into sub scenarios (Visnepolschi, 2009).

The natural stochastic variability is enhanced by adopting Marczyk (1999) approach were a risk cost model contains a stochastic processor to represent the dynamic characteristics of the problem. Along this line, we created a software package that utilizes both probabilistic and simulation (Monte-Carlo based) paradigms for computing expected risk as well as risk response costs and times. Once a mathematical risk management process model exists, one can easily add a software program to optimize the risk response strategy for various objectives.

3.4 Risk modeling and conventional risk management process

In general, applying the risk management quantitative modeling to a system or a project matches the conventional (ISO 31000, 2009) risk management process. This relation is depicted in Table 1.

Table 1 – Traditional risk management process and risk model activities

Traditional risk management process			Risk model activity
Step	**Name**	**Activity**	
1.	Establish the Context	Define the risk management strategic, organizational and business context	• N/A
2.	Identify Risks	Define risks that could prevent, degrade, delay (or enhance, in case of opportunities) the achievement of the organization's objectives	• Create Canonical Risk Model (CRM)
3.	Analyze Risks	Consider the likelihood and potential consequences of risk occurrence	
4.	Evaluate Risks	Rank risks according to likely adverse outcomes (or potential benefits in case of opportunities)	
5.	Treat Risks	Develop and implement plans for increasing potential benefits and reduce adverse risk impacts	• Create Risk Response Model (RRM) • Create Response Strategy Model (RSM)
6.	Monitor and Review	Monitor the performance of the risk management process over time with a view for continuous improvements	• Execute the risk management model • Periodically evaluate and re-execute the risk management model
7.	Communicate and Consult	Communicate and consult with internal and external stakeholders at each stage of the risk management process	• N/A

4. Modeling risk management cost

In this section, we address the issue of modeling the risk management cost.

4.1 Canonical Risk Model (CRM)

In discussing risk management processes, we refer to the set of all possible risks to a system during its lifetime as "Canonical risks".

4.1.1 Risk impact concept

The risk impact exhibits the following characteristics:

1. System's lifecycle phases are ordered serially, depicting the execution order of the overall risk response process. Similarly, the risk response actions within each phase are performed in the same order.
2. Lifecycle phases $\{\mathbf{L}\}$ is a vector defined such that:

$L_i = i\ ;\{i = 1, 2, \cdots, z\}$ **(Remark: In this model, z = 8)** 1

3. When a particular risk response action, $RRA_{i,j}$ is not fully performed, it fails to eliminate a risk:

$$Risk_{i,j}\left\{ j(i)=1,2,..,n_i\ ,\ i=1,2,..,z\right\} \quad \text{.........}2$$

4. Each risk, $Risk_{i,j}$, can cause an impact cost $Ci_{i,j}$ with probability $P_{i,j}$:

$$Ci_{i,j}\left\{ j(i)=1,2,..,n_i\ ,\ i=1,2,..,z\right\} \quad \text{.........}3$$

$$P_{i,j}\left\{ j(i)=1,2,..,n_i\ ,\ i=1,2,..,z\right\} \quad \text{.........}4$$

4.1.2 Canonical Risk Model - (CRM)

A Canonical Risk Model (CRM) is a conceptual entity, with unique individual components for each industry, product or project. CRM is defined as "a model describing a comprehensive set of risks that may affect the system together with their impact probabilities and their potential impact cost and impact time". Figure 5 depicts a Canonical Risk Model (CRM).

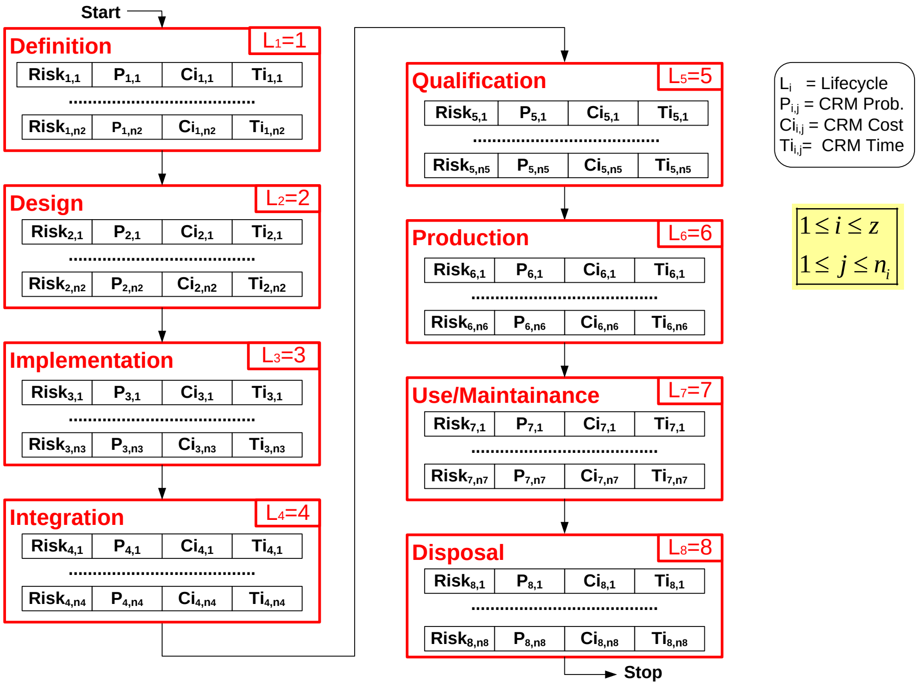


Figure 5 - Canonical Risk Model - (CRM)

4.1.3 Canonical risk cost

Assuming risk impact costs to be independent and additive, we can calculate the canonical risk impact cost (i.e. the maximum potential risk expenditures when no risk response is implemented and all potential risks do, in fact, happen):

$$Ci_{Canonical}=\sum_{i=1}^{z}\sum_{j=1}^{n_i} Ci_{i,j} \quad \text{.........}5$$

4.2 Risk Response Model (RRM)

The Risk Response Model (RRM) paradigm is introduced in order to capture the qualitative and quantitative implications of undertaking systems' risk management process. Generation of an RRM entails defining a collection of risk response actions together with their costs and performance times, where each action is carried out within a specific system lifecycle phase.

In order to simplify the problem of modeling the system risk management process, we assume total independence amongst individual risk response actions. We further assume a one to one relation between systems' risks and response actions (i.e. for each risk there is a corresponding single response action). An

RRM is defined as a "complete set of actions and associated costs and time parameters designed to prevent all system's risks throughout its lifecycle".

It is worth noting that the RRM is an idealized concept. It is not likely to be carried out in practical applications in its all-inclusive form, since it could require excessive financial and time resources. Many industrial and governmental organizations perform about 15% - 25% of RRM and, in special circumstances (e.g., manned missions into space); perhaps 25% - 50% of RRM is performed. The intent here is to create a yardstick for evaluating selected partial sets of actions with respect to the complete set.

4.2.1 Risk response concept

Risk Response exhibits the following characteristics:

1. Within the {$\mathbf{L_i}$} risk response lifecycle phases, there are {n_1, n_2, … n_i, … n_z} sets of risk response actions. Each one is designated as:

$$RRA_{i,j}\left\{\ j(i)=1,2,...,n_i\ ,\ \ i=1,2,...,z\right\} \text{ ....} \mathbf{6}$$

2. The cost of performing a risk response action {$\mathbf{RRA_{i,j}}$} is:

$$Cr_{i,j}\left\{j(i)=1,2,...,n_i\ ,\ \ i=1,2,...,z\right\} \text{ ....} \mathbf{7}$$

3. The time require to perform response action {$\mathbf{RRA_{i,j}}$} is:

$$Tr_{i,j}\left\{j(i)=1,2,...,n_i\ ,\ \ i=1,2,...,z\right\} \text{ ....} \mathbf{8}$$

4.2.2 Risk Response Model (RRM)

Figure 6 describes the Risk Response Model (RRM) paradigm. It depicts the lifecycle phases $\left\{L_i\right\}$, the Risk Response Actions $\left\{RRA_{i,j}\right\}$, Response Costs $\left\{Cr_{i,j}\right\}$ and Response Times $\left\{Tr_{i,j}\right\}$ elements of the model.

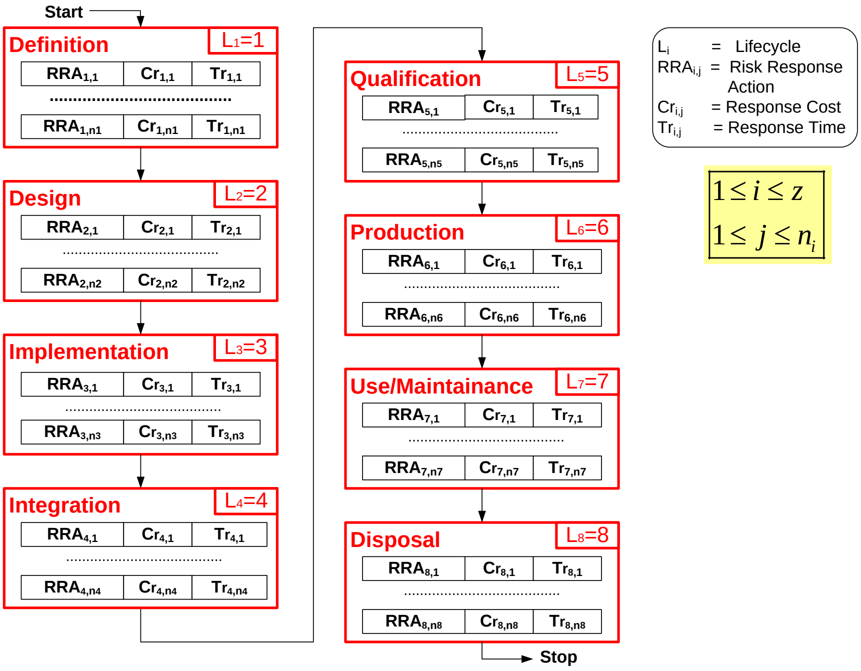


Figure 6 - Risk Response Model (RRM)

4.2.3 Executing the RRM

1. The terms "Executing the Risk Response Model" or "Performing the risk response process In Accordance With (IAW) the RRM", entail performing serially all the risk response actions in the defined order described in the RRM. The ensemble of all RRM actions is designated RRM.

$$RRM = \bigcup_{i=1}^{z} \bigcup_{j=1}^{n_i} RRM_{i,j} \quad \text{.......... 9}$$

2. Assuming risk response costs to be independent and additive, the total risk response cost (C_{RRM}) (i.e. the cost to perform all the risk response actions defined in the RRM) is:

$$\boxed{C_{RMM} = \sum_{i=1}^{z} \sum_{j=1}^{n_i} Cr_{i,j}} \quad \text{.......... 10}$$

4.3 Risk management cost

Selecting a risk response strategy entails designating the performance level of each risk response action. This includes identifying a set of risk responses performance variables that should be fully or partially performed, as well as those that may not be performed at all. A basic assumption of this methodology is that any partially performed risk response action or any risk response action not performed at all give rise to a system risk. These risks have uncertain effects on the system or project and, of course, they may lead to undesirable expenditure that can be regarded as an outcome of implementing a selected risk response strategy. They are discernible only subsequent to the risk insertion (during the same lifecycle phase or at a later lifecycle phase).

As mentioned earlier, executing the all-inclusive Risk Response Model (RRM) is not practical, due to risk response funding limitations or time to market considerations. Therefore, industrial organizations elect to perform only a subset of the RRM, and within this subset some risk response actions are only partially performed. We have called such policy a risk response strategy and have encapsulated this concept in a Response Strategy Model (RSM). We define the cost of actually carrying out this risk response subset as the *actual risk response cost*.

The specific design of an optimal risk response strategy requires a prudent consideration of this issue. Risk response strategy for developing and fielding rockets or space crafts, which are produced in very small quantities and cannot be repaired after launch, is very different from risk response strategy implemented in an automobile production line, which are built for tens of thousands of units per year. At the core, a risk response strategy should support organization business objectives like[7]:

- reduce product cost
- reduce time to market
- reduce internal and external failure costs
- increase market share
- increase quality of products
- improve delivery time
- increase stakeholders satisfaction

Other considerations, less directly linked to business objectives, are meeting standards and statutory directives as well as following ethical and other societal values. In order to deal with a realistic qualitative and quantitative modeling of the costs and risks associated with an incomplete set of risk response actions, some basic concepts are introduced in the next subsections.

4.3.1 Response Strategy Model (RSM)

A risk Response Strategy Model (RSM) is depicted in Figure 7. The reader should note the following:

1. For each response action $RRA_{i,j}\left\{ j(i)=1,2,...,n_i\,,\ i=1,2,...,z \right\}$, there exists a Decision Variable, $X_{i,j}^{(k,l)}$, $0 \le X_{i,j}^{(k,l)} \le 1$, which defines the risk Response Performance Level (RPL) of risk $Risk_{k,l}\left\{ k=j,\ j+1,...,z, \quad l(k)=1,2,...,n_k \right\}$
2. Here, $X_{i,j}^{(k,l)}=1$ means that risk response action $RRA_{i,j}$ is to be fully performed, whereas $X_{i,j}^{(k,l)}=0$ means that risk response action $RRA_{i,j}$ is not to be performed.

[7] However, in reality most organizations strive only to optimize the system's cost, performance, delivery time or a combination thereof.

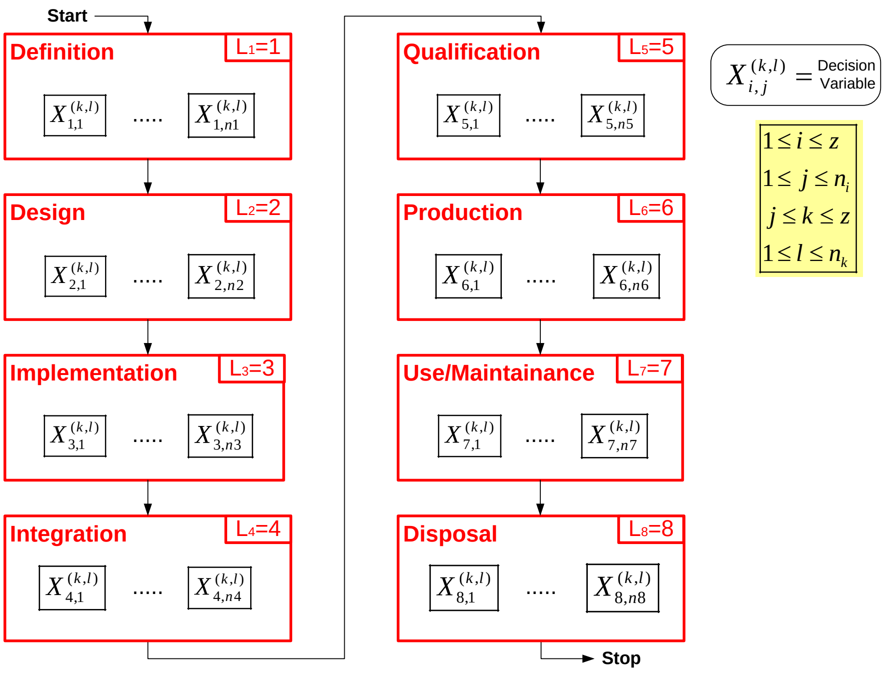


Figure 7 – Risk Response Strategy Model (RSM)

4.3.2 Practical risk response cost

Defining a specific risk response strategy, provides means to capture a realistic qualitative set of risk response actions as well as to compute practical quantitative risk response costs.

1. A symbolic representation of the ensemble of risk response actions performed at their respective RPLs $RRA_{Strategy}$ will be:

$$RRA_{Strategy} = \bigcup_{i=1}^{z}\bigcup_{j=1}^{n_i}\left\{RRA_{i,j}X_{i,j}^{(k,l)}\right\} \quad \text{.........11}$$

2. We have assumed that the cost invested in a risk response action $RRA_{i,j}$ performed at level $X_{i,j}^{(k,l)}, 0 \le X_{i,j}^{(k,l)} \le 1$, represents an $X_{i,j}^{(k,l)}$ fraction of the cost $Cr_{i,j}$ for fully performing the action. Accordingly, the total risk response strategy cost $Cr_{Strategy}$ incurred would be:

$$Cr_{Strategy} = \sum_{i=1}^{z}\sum_{j=1}^{n_i}\left\{Cr_{i,j}X_{i,j}^{(k,l)}\right\} \quad \text{.........12}$$

4.3.3 Practical risk impact cost

We have assumed a negative nonlinear[8] model in order to describe the functional relationships between the *Risk Impact Cost* and the risk Response Performance Levels (RPL). A simplified[9] system's lifecycle *Risk Impact Cost* associated with a given risk response strategy $(X_{i,j}^{k,l}; 0 \le X_{i,j}^{k,l} \le 1)$, is:

$$Ci_{Strategy} = \sum_{i=1}^{z}\sum_{j=1}^{n_i}\left\{P_{i,j}Ci_{i,j}(1 - X_{i,j}^{(k,l)})\right\} \quad \text{.........13}$$

[8] The affect of a risk response action on a given impact risk is near but not quite linear. The reason for this is that, in reality, performing risk mitigation at low levels will eliminate or reduce the impacts of glaring and simple risks with minimal effort. Conversely, risk mitigation at high levels requires substantial efforts for eliminating or reducing impacts of obscure and intractable risks. This nonlinear situation may be characterized by a function having an inflection point about midway, which can be modeled by a piecewise linear function. The practical insight from this phenomenon is that virtually all Response Performance Levels should lie in the range: 0<x<1 (x=0 and x=1 are hardly ever optimal RPLs)

[9] For simplicity sake, we show a linear equation. However, actual model computations implements non-linear relationships utilizing a piecewise linear function.

4.4 Total risk management cost

Within the overall context of risk management cost modeling, the total cost is the sum of the risk response cost and the risk impact cost:

$$C_{Total} = Cr_{Strategy} + Ci_{Strategy} \quad \text{.......14}$$

$$C_{Total} = \sum_{i=1}^{z}\sum_{j=1}^{n_i}\left\{Cr_{i,j}X_{i,j}^{(k,l)} + P_{i,j}Ci_{i,j}(1 - X_{i,j}^{(k,l)})\right\} \quad \text{.......15}$$

5. Modeling risk management time

In this section, we address the issue of modeling the risk management time.

5.1 Time modeling approach

The basic issue of planning and modeling duration of projects is well established and in common use. For example, the Critical Path Method (CPM) and the Program Evaluation and Review Technique (PERT) were developed in the late 1950s, by DuPont and Remington Rand in order to manage plant maintenance and by Lockheed for the Polaris Missile Program (Grant, 1983).

Modeling risk management time entails computing the duration of each system's lifecycle phase within the risk management horizon and then aggregating these time intervals. Firstly, we must take into account the level of risk response performance level $X_{i,j}^{k,l}$, $0 \le X_{i,j}^{k,l} \le 1$ associated with each risk response action $RRA_{i,j}$ as well as the stochastic phenomena of the risk time impact, $Ti_{i,j}$. Secondly, although our primary interest is with risk management processes, modeling risk times is necessarily intertwined with system actions $S_{i,j}$ and their durations $Ts_{i,j}$. Thirdly, we must consider the overlaying nature of practical systems' phased development process. That is, frequently, a lifecycle phase starts before the end of the previous lifecycle.

Figure 8 shows an example of project actions network diagram. Within each phase, systems and response actions duration as well as times associated with risk impacts are related in a complex network. Sometimes, response actions are carried out in order to support other response actions (e.g. risk response planning, risk response infrastructure building, etc.). On other occasions, risk response actions are performed before or after the completion of corresponding system actions.

The System lifecycle network example represents a typical set of System and risk response actions commonly adhered to, by many industries during the Definition phase. System actions $\{S_{1.1}, S_{1.2}, \ldots, S_{1.5}\}$ are intertwined with response actions $\{V_{1.1}, V_{1.2}, \ldots, V_{1.12}\}$. Each response action is performed at a selected level $X_{i,j}^{k,l}$, $0 \le X_{i,j}^{k,l} \le 1$ and therefore, gives rise to a corresponding risk impact.

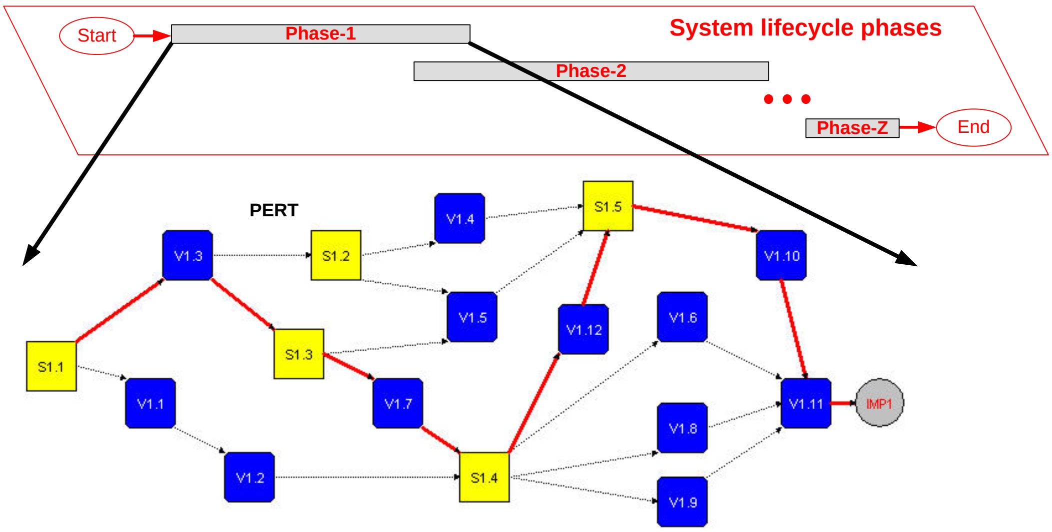


Figure 8 - System lifecycle network example

5.2 Modeling phase management time

5.2.1 Time Modelling Variables

Time modeling must take the following into account:

1. System action time $Ts_{i,j},\ j(i)=1,2,...,n_i,\ i=1,2,...,z$ required for performing system actions $S_{i,j}$ where *i* represents the system lifecycle phase and *j* represents the system action index within that phase.
2. Risk response action time $Tr_{i,j},\ j(i)=1,2,...,n_i,\ i=1,2,...,z$ required to perform response action $RRA_{i,j}$.
3. Risk response performance level $X_{i,j}^{(k,l)},\ 0 \le X_{i,j}^{(k,l)} \le 1$, which defines how much risk response action $RRA_{i,j}\left\{ j(i)=1,2,...,n_i\ ,\ i=1,2,...,z\right\}$ should be performed in order to reduce or eliminate a given risk, $Risk_{k,l}\left\{k=j,\ j+1,\ ...,\ z,\quad l(k)=1,2,...,n_k\right\}$.
4. Risk impact time $Ti_{k,l}$ is defined as the required time needed to carry out a corrective action due to risk impact $Risk_{k,l}\left\{k=j,\ j+1,\ ...,\ z,\quad l(k)=1,2,...,n_k\right\}$.
5. Probability $P_{i,j},\ 0<P_{i,j}<1$ of risk impact $Risk_{k,l}$.

5.2.2 Time modelling assumptions

The following assumptions have been made:

1. System actions $(S_{i,j})$ are linked via specified network arrangement and their time durations $(Ts_{i,j})$ are assumed to be known and deterministic[10].
2. Risk response actions $(RRA_{i,j})$ are interspersed with system actions in a network arrangement. Their time durations $(Tr_{i,j})$ are deterministic[11] and linearly dependent upon the level of response performance levels $X_{i,j}^{(k,l)},\ 0 \le X_{i,j}^{(k,l)} \le 1$.
3. Risk impacts may emanate from incomplete risk response performance, conducted during either one of the previous lifecycle phase or during the current lifecycle phase. They could cause unplanned delays and unexpected remedial process extending the system schedule. For modeling simplicity, we aggregate the materialized risk impact times and place the aggregated risk impact at the end of the relevant lifecycle phase. Therefore, impact time extends the duration of lifecycle phases in which they occur.

5.2.3 System's time computation per phase

The following steps are used to compute the system time $(Ts\_phase_{i^\circ})$ associated with a specific system lifecycle phase i°:

1. Identify each system action time $Ts_{i^\circ,j}$ associated with each system action $S_{i^\circ,j}$ in phase i°.
2. Sum up the set of system action time $Ts_{i^\circ,j}$ associated with the critical path using the Critical Path Method (CPM):

$$Ts\_phase_{i^\circ} = \sum_{j=Critical\_path} \left\{Ts_{i^\circ,j}\right\} \quad \textbf{16}$$

---

10 A sophisticated user can certainly make other, nondeterministic assumptions, regarding System actions.

11 Ditto for Risk Response Actions.

5.2.4 Risk response time computation per phase

The following steps are used to compute the risk response time $(Tr\_phase_{i^\circ})$ associated with a specific system lifecycle phase i° :

1. Identify all pairs of risk response action times $Tr_{i^\circ,j}$ and risk response performance levels $X^{k,l}_{i^o,j}$ associated with each risk response actions $M_{i^\circ,j}$ in phase i° .
2. Use the Critical Path Method (CPM) in order to identify the longest path. The risk response time for this phase $(Tr\_phase_{i^\circ,j})$ associated with the critical path is summed as follows:

$$Tr\_phase_{i^\circ} = \sum_{j=Critical\_path} \left\{ Tr_{i^\circ,j} X^{k,l}_{i^\circ,j} \right\} \quad \textbf{17}$$

5.2.5 Risk impact time computation per phase

The following steps are used to compute risk impact time $(Ti\_phase_{i^\circ})$ associated with a specific system lifecycle phase i° :

1. Identify risk impact times $Ti_{i^\circ,j}$ associated with each risk response actions $RRA_{i^\circ,j}$ in phase i° .
2. Identify all risk response performance levels $X^{k,l}_{i^o,j}$ associated with each risk response actions $RRA_{i^\circ,j}$ in phase i° .
3. Compute each risk impact time item emanating from the individual risk response actions $RRA_{i^\circ,j}$, affecting lifecycle phase i° :

$$Ti\_item_{i^\circ,1} = P_{i^\circ,1} Ti_{i^\circ,1} (1 - X^{k,l}_{i^\circ,1}) \quad \textbf{18}$$

$$Ti\_item_{i^\circ,2} = P_{i^\circ,2} Ti_{i^\circ,2} (1 - X^{k,l}_{i^\circ,2}) \quad \textbf{19}$$

…….

$$Ti\_item_{i^\circ,j} = P_{i^\circ,j} Ti_{i^\circ,j} (1 - X^{k,l}_{i^\circ,j}) \quad \textbf{20}$$

Aggregating impact times

As stated earlier, impact cost aggregation is achieved by adding up all the impact costs that occur during a given project phase. This technique is not valid for time aggregation. The reason is that individual impacts occur randomly (sometimes serially, sometimes in parallel with other systems or risk response actions) during a given lifecycle phase. The duration of each impact time (the time required to fix a problem) is stochastic. In addition, the availability of staff to deal with the problem is also stochastic. Therefore, the question we are dealing with is: What will be the overall effect of a group of impact times on the total duration of a given lifecycle phase? One can envision several models to represent this problem. However, expert systems engineers suggest modeling the above problem analogously to modeling measurement errors propagation. Impact times are similar to measurement errors in the following properties: 1) they occur stochastically and 2) they are independent of one another. We can envision measuring N components, say resistors, where each measurement is subject to a known potential error ε_i . We ask the question: What will be the overall error if we measure all the resistors connected serially? Based on Taylor (1996), we can compute the total propagated error ε :

$$\varepsilon = \sqrt{\varepsilon_1^2 + \varepsilon_2^2 + \varepsilon_3^2 + \ldots \varepsilon_N^2} = \sqrt{\sum_{i=1}^{N} \varepsilon_i^2} \quad \textbf{21}$$

We model the aggregated impact time by applying the above approach and assuming it occurs at the end of each lifecycle phase.

$$Ti_{i^\circ} = \sqrt{\sum_{j=Critical\_path} \left\{ \left(Ti\_item_{i^\circ,j} \right)^2 \right\}} \quad \text{.......} 22$$

This equation provides the most realistic result, which is in between the maximal and minimal aggregated impacts.

Earlier phases impact times

1. We must now consider impact times emanate from risks undertaken at earlier phases which affect the system during the current phase i° :

$$Ti_{i\_i^0}, \quad \{ i = 1, 2, ..., i^o - 1 \} \quad \text{.......} 23$$

2. Therefore, the total impact time during phase i° is:

$$Ti\_phase_{i^\circ} = Ti_{i^\circ} + \sum_{i=1}^{i^0-1} Ti_{i\_i^0} \quad \text{.......} 24$$

5.2.6 Total phase time

The above three time components are summed up to arrive at the total phase i° time duration:

$$T_{Phase\_i^\circ} = \sum \left\{ Ts\_phase_{i^\circ} + Tr\_phase_{i^\circ} + Ti\_phase_{i^\circ} \right\} \quad \text{.......} 25$$

5.3 Total risk management time

The ideal system lifecycle describes each lifecycle phase as strictly following the previous phase. In practice, this is rarely the case. Often, a new phase starts before the previous phase has finished. We have introduced a Premature Next Phase Start (PNPS) factor $(0 \le PNPS_i \le 1)$ that identifies the incomplete portion of phase $\{i\}$ in which phase $\{i+1\}$ starts. A set of PNPS factors is depicted in Figure 9. Here, for example, the Definition phase starts at the beginning of the system lifecycle, The Design phase starts when the Definition phase is 30% incomplete, etc.

Lifecycle Phase Number		Premature Next Phase Start (PNPS) factor
Number	Name	
1	Definition	0.0
2	Design	0.3
3	Implementation	0.4
4	Integration	0.1
5	Qualification	0.2

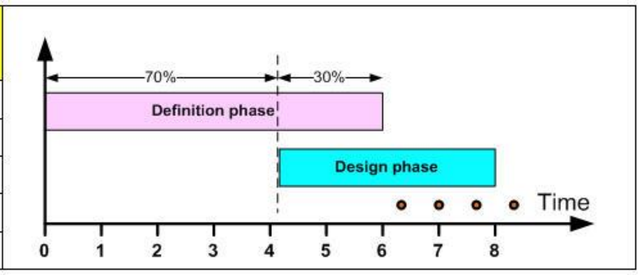


Figure 9 - Example- a set of PNPS used in the pilot project

Based on the above, the overall time required for carrying out a system and risk response actions for the entire lifecycle is:

$$T_{Total} = T_1 + \sum_{i=2}^{z} T_i - (T_{i-1} * PNPS_i) \quad \text{.......} 26$$

Please note that the team developing, manufacturing or maintaining the system provides PNPS data. Such data may be provided at the beginning of a project development and then, periodically, when a new RRA strategy is contemplated (at which times, the risk management model may be re-executed using actual failure events which replace previous uncertainties). The risk management model is designed to compute the duration of each lifecycle phase by itself and then to calculate the overall duration of the risk management horizon (for example, the expected overall project development duration), taking into account the phase overlap data.

6. Risk management use-case

The use-case presented in this section is based on a historical pilot project, aimed at developing and fielding new avionics system for transport helicopters. A specialized software tool was constructed to compute the expected cost/time using probabilistic approach as well as capture and visualize the nondeterministic nature of the problem, using Monte-Carlo simulations. Monte-Carlo simulation is a class of numerical analysis techniques, simulating physical systems, in this case, drawing stochastic values representing the actual occurrence or non-occurrence of risk impacts.

Appendix-A depicts the following use-case raw data: 1) the identified system development risks, 2) the set of Risk Response Actions identified by the project team and 3) the selected Risk Response Action strategy.

6.1 Risk - cost distribution by category

The cost results derived from modeling the risk management process is depicted in Figure 10. These results were obtained using a direct probabilistic calculations as well as a Monte-Carlo simulation which yielded the same cost results. In this particular use-case, the risk response strategy cost was 346K$. The selected strategy induced a notably high impact cost of 432K$, leading to a total risk management process cost of 778K$. However, this cost is appreciably less than the Canonical Risk Model (CRM) cost of 1,431K$.

Cost categories	Cost [K$]	Cost [%]
Risk Response Action cost	346	44%
Risk Impact cost	432	56%
Total cost	778	100%
CRM cost	1,431	184%
STD-DEV	97	13%
VaR95%	1,003	129%
Rang	581	75%
	1,399	180%

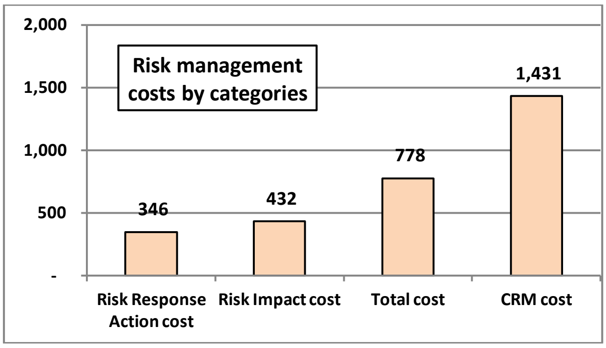


Figure 10 – Risk management costs by categories

Figure 11 depicts the total risk management process cost density distribution (histogram) derived from modeling the cost associated with the selected risk management strategy, i.e., cost stemming from risk response actions during system development plus cost stemming from risk impacts (realized risks). These results were obtained by means of Monte-Carlo simulations, performing 3,000 iterations within the software tool. The X-axis represents the cost and the Y-axis represents the percentage of iterations associated with each of 50 histogram bins. The vertical line on the left hand side of the figure represents the selected risk response strategy cost of 345K$. Similarly, the vertical line on the right hand side represents the Canonical Risk Model (CRM) cost of 1,431K$. The mean risk management process cost was 7,74K$[12] with a standard deviation of 97K$. The range of simulation results were between 5,81K$ and 1,399K$, the skewness and kurtosis of the simulated costs were 1.60 and 1.24 respectively and the Value-at-Risk (VaR) at 95% was 1,003K$. Clearly, the selected risk response strategy led to a large variance of the overall expected risk management cost process and, most ominously, the right hand side "catastrophic risk tail" indicate costly real-life outliers near the CRM cost.

[12] One should expect some small variations in results obtained using direct probabilistic calculations versus several runs of Monte-Carlo simulations, as each simulation run is dependent on certain randomness.

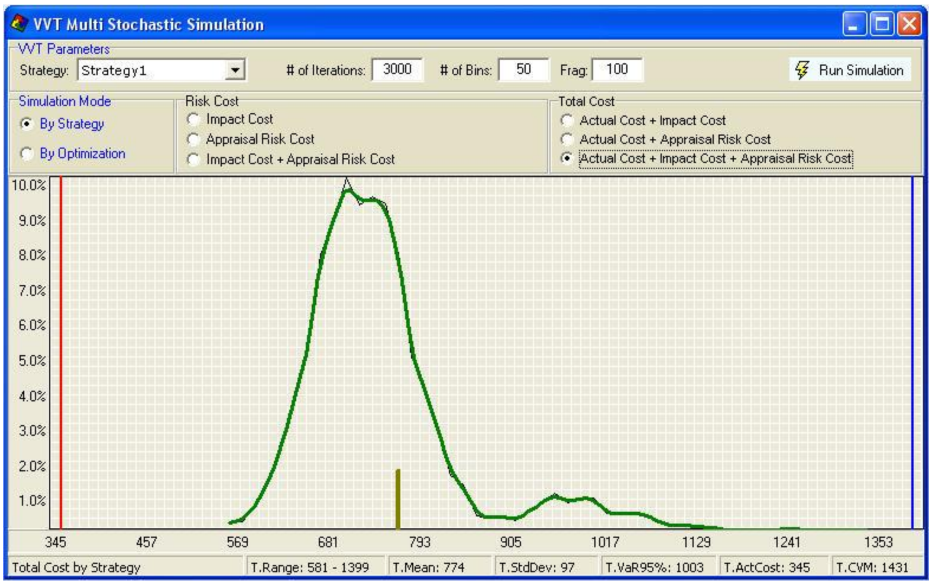


Figure 11 – Cost distribution after 3000 iterations of Monte-Carlo simulations

6.2 Risk - cost distribution by project phase

Table 2 and Figure 12 show the risk management cost distribution over the development lifecycle phases. One can clearly observe that the funds allocated to the risk response actions increases in a near linear fashion over time. Nevertheless, very high impact costs materialize during the Integration and Qualification phases, a time when the system is put together and many problems become visible. One can speculate that these high impact costs stem, in a large measure, from an inadequate or ineffective risk response strategy employed during the Definition, Design and Implementation phases. (Preferably, the slope of the dotted line in Figure 12, should be downward instead of upward.)

Table 2 – Risk management costs distribution during system's development phases

Cost categories	Definition [K$]	Design [K$]	Implementation [K$]	Integration [K$]	Qualification [K$]	Total [K$]
Risk Response Activity cost	35	68	49	88	106	346
Risk Impact cost	11	32	40	168	180	432
Total cost	46	100	89	256	286	778
CRM Cost	266	455	224	169	317	1,431
STD-DEV						101
VaR95%						1,003
Range					Minimum	581
					Maximum	1,399

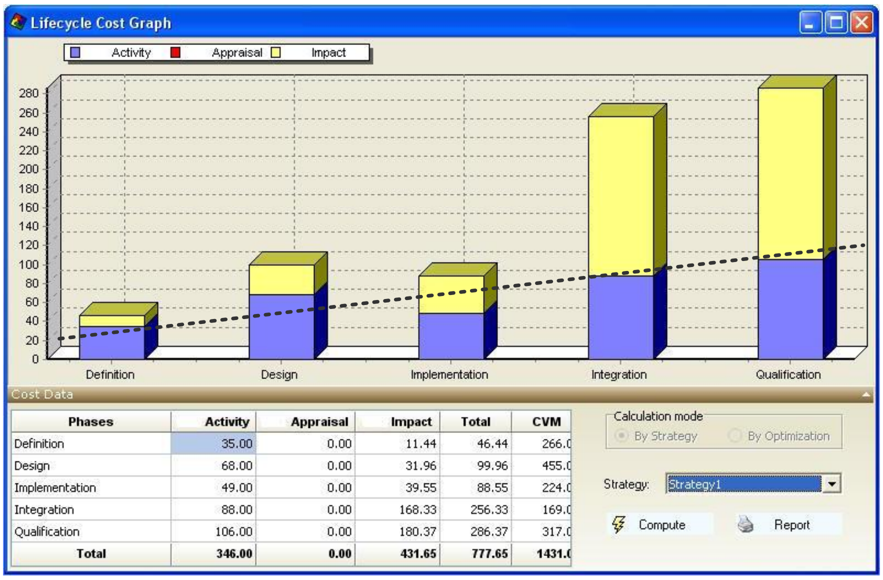


Figure 12 - Risk management costs distribution during system's development phases

6.3 Risk - time computation

This section describes the pilot project time results that were derived from modeling the system development time interlaced with risk response actions as well as impact times. Figure 13 depicts a PERT chart of the pilot project Definition phase. This includes the System actions $\{S_{1,1}, S_{1,2}, ..., S_{1,5}\}$, the risk response actions $\{V_{1,1}, V_{1,2}, ..., V_{1,12}\}$, and the risk impact generated during this lifecycle phase, $Impact_1$. The total duration of the Definition phase, given the specific risk response strategy selected by the project was 73.1 days.

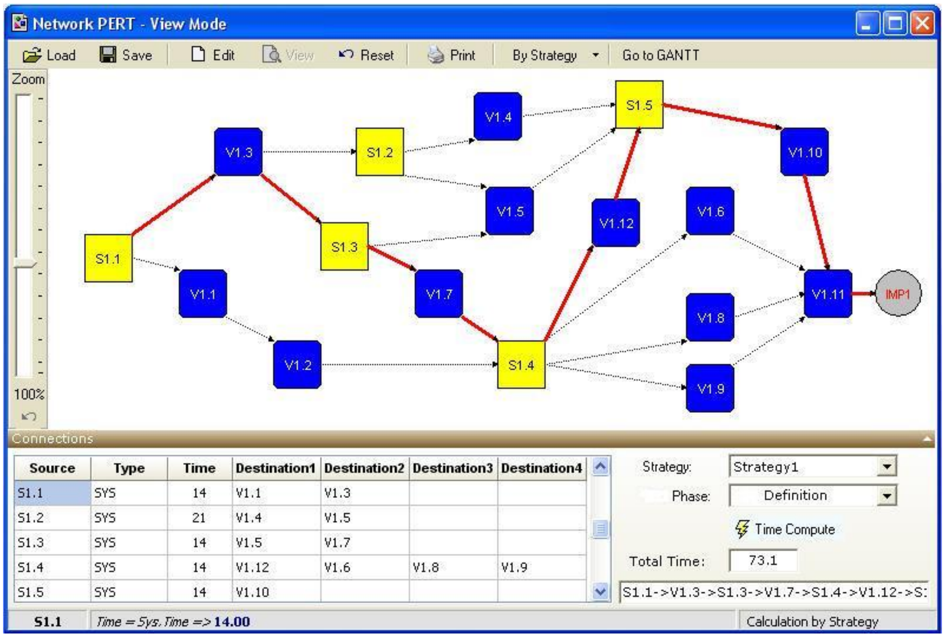


Figure 13 - PERT chart of the pilot project Definition phase

Table 3 depicts the duration of each pilot project phase (T_{Phase_i}) calculated when considering the risk response actions chained along the critical path. In addition, the table identifies the Premature Next Phase Start $(PNPS_i)$ factors and the Start time and End time of each lifecycle phase.

Table 3 - System and risk management time duration and phase overlap

Phase	Duration	PNPS factor	Start time	End time
Definition	73.1	0.0	0.0	73.1
Design	117.2	0.3	51.2	168.4
Implementation	183.2	0.4	121.5	304.7
Integration	147.8	0.1	286.4	434.2
Qualification	104.1	0.2	404.6	508.7

Similarly, Figure 14 depicts the Gantt chart of the entire pilot project presented in this use-case. The length of each bar within the Gantt chart is based on the time duration of each lifecycle phase. Again, the reader should note that the duration of each bar reflects times for 1) carrying out system actions, 2) performing risk response actions and 3) risk impacts times, all chained along the critical path of the given lifecycle phase. The specific placing of each bar is derived from the relevant Premature Next Phase Start (PNPS) factor and the overall duration of the project is 509 days.

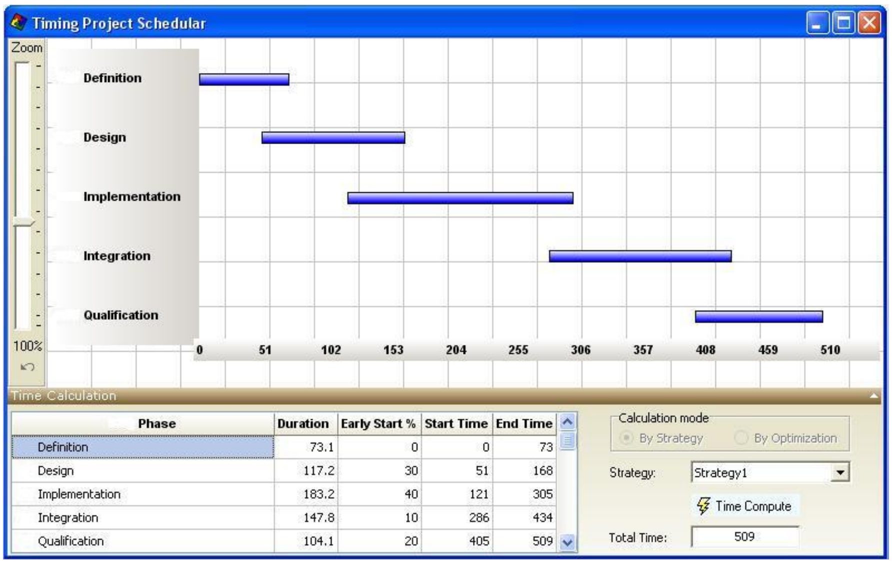


Figure 14 – Model calculations of pilot project development time

Figure 15 depicts a hypothetical Gantt chart of the pilot project under CRM strategy (i.e. fully performing all risk response actions). In this case the project CRM time is calculated to be 632 days (124% of actual project execution time).

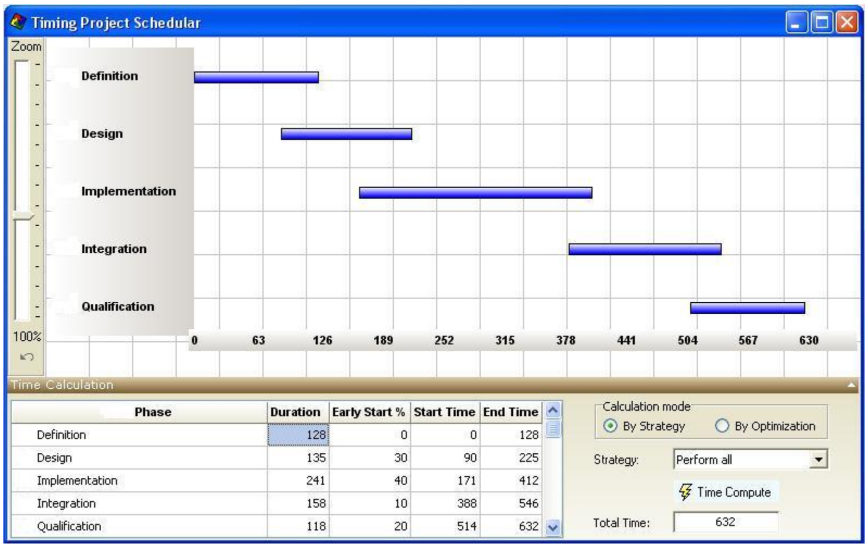


Figure 15 - Pilot project development time under CRM strategy

7. Discussion and conclusion

The rationale for this paper lies in the fusion of cost and time elements associated with systems' risks, together with their corresponding Risk Response Actions (RRAs). This approach can yield overarching risk management optimization not attainable by considering each component separately.

However, quantitative modeling of the risk management process is no panacea. "Nancy Leveson of MIT and her collaborators have argued (in Marais, 2004) that the chain-of-event conception of accidents typically used for such risk assessments cannot account for the indirect, non-linear, and feedback relationships that characterize many accidents in complex systems. These risk assessments do a poor job of modeling human actions and their impact on known, let alone unknown, failure modes" (Ramana, 2011).

Our model makes many simplifying assumptions. This admittedly could lead to a reduction in the overall accuracy of the results. Other critics may say that the model we present is too complex to be useful.

Another, often heard criticism of our approach, is that our model requires data on risk and risk response cost and time which are not readily available. Thus, many engineers and professionals used to exact science explanations look with disdain on such models. This may be attributed to a lack of training, or possibly to personal preferences. We argue that there is a large body of knowledge about the methods we used to obtain and process risk and risk response cost and time data. For example, much valuable information is routinely gathered in diverse domains like sociology, economics, marketing, and political science using these techniques. For example, the Delphi method uses systematic techniques for eliciting data from domain experts and then aggregating it (see Cooke, 1991, Loveridge, 2002).

All in all, our experience is that, given a software package embodying the model and reasonable training, the presented model can successfully be utilized in many medium-to-large projects. Notwithstanding the model simplifications, our intuition suggests that uncertainties in the values of the input parameters play a more significant role in skewing the results[13].

We suggest that quantitative modeling of risk management processes will facilitate the process of optimizing the risk response strategy. The designers of such strategy will be able to choose among several optimization alternatives. Firstly, they can concentrate on either a single optimization objective or on multi-objective optimization. Secondly, they can optimize the risk response strategy for a verity of objectives and their combinations, for example:

1. RRA Cost/Time. The RRA strategy cost/time is deterministic and dependent solely upon the selected RRA strategy. The objective here is either (1) to minimize the overall cost/time of performing the risk response activity or (2) to optimize it for a specific cost/time target.
2. Expected risk impact Cost/Time. The risk impact cost/time is a stochastic variable dependent upon the individual impact cost/time and the impact probability as well as the selected RRA strategy. The objective here is to either (1) minimize the expected risk impact cost/time or (2) to optimize it for a specific cost/time target.
3. Variance of risk impact Cost/Time. The variance of the risk impact cost/time represents the dispersion or the uncertainty of the risk impact measure. The objective here is to minimize this uncertainty in order to increase the confidence in predicting the impact cost/time.
4. Specific Risks. The objective here is to optimize the RRA strategy in order to eliminate or diminish the cost/time impacts emanating from specific risks and, in particular, avoiding the phenomena of catastrophic risk tail (low probability / high impact risks).

The use-case presented above shows that the specific risk response strategy employed by the pilot project team was poor. Firstly, the impact cost seems to be large. One wonders whether a different risk response strategy could have reduced the overall risk management expenditures. Secondly, the variance of the cost distribution is large, indicating that the specific RRA strategy leaves substantial exposure to critical risks. Similarly, the simulation exposes a "right hand side catastrophic risk tail". This tail represents costly outliers i.e., risks that rarely materialize but cause extremely expensive impacts. In classic risk management, "unimportant risk events" (i.e., where $R = P * C$ is relatively small), catastrophic events that may happen very seldom do not receive due scrutiny. However observing such a catastrophic risk tail is important, since it identifies risks that should be mitigated[14].

Analyzing the overall risk distribution over the pilot project phases suggests that 349K$ (over 80%) of the realized risk cost is materialized during the Integration and Qualification phases on impacts, probably stemming from ineffective risk response strategy. A possible explanation of this phenomenon is the relatively limited efforts devoted to risk mitigation efforts during the Definition, Design and Implementation phases of the system, some 152K$ (44%) of the total risk response action budget.

An important key to avoiding risk waste is to measure and model the risk management process. Minimizing the overall risk cost management can be achieved by applying the following simple rule: "Perform a risk response action only if its cost/time is smaller than its corresponding risk cost/time".

In a future paper, the authors will show that an optimized risk response strategy can significantly reduce project cost and/or time. Furthermore, optimized strategy can provide meaningful reduction in the variance of the expected risk cost density distribution. And, most importantly, the potential outliers (i.e., the catastrophic risks that may rarely occur) can be greatly reduced and perhaps eliminated.

---

13 See David Hale paper on ways to make risk assessments more comparable and repeatable (Hall, 2011).

14 For example, on June 4, 1996, the maiden flight of the Ariane-5 launcher ended in failure, 40 seconds into the flight sequence. The failure was traced to a software error in the Inertial Navigation System (INS), a critical subsystem that was used extensively in previous Ariane-4 launchers. This type of INS was installed in the new Ariane-5 on an "as is" basis (with minimal testing). The probability that a "tried and tested" system will not work is near zero, but the impact (about 500M$ and 2 years setback) is huge (Nuseibeh , 1997).

References

APM 2004, Project Risk Analysis and Management (PRAM) Guide, Association for Project Management (APM), ISBN-10: 1903494125, ISBN-13: 978-1903494127, 2004

Barad M. and Engel A., "Optimizing VVT strategies - A decomposition approach", Journal of the operation research society (JORS), 57(8), pp. 965–974, Aug. 2006.

Caballero A.A. and Yen K.K., Fuzzy Model for Risk Evaluation in Construction Projects. WSEAS Transactions on Business and Economics, Issue 4, Vol. 1, pp. 275-280, October 2004

Chen Y., Härdle W. and Jeong SO, Nonparametric Risk Management With Generalized Hyperbolic Distributions, Journal of the American Statistical Association. 103(483), pp. 910-923, September 1, 2008

Cooke M.R., Experts in uncertainty: Opinion and subjective probability in science, Oxford University Press, Oxford, 1991

Crosby P. B., Quality is Free: The Art of Making Quality Certain, McGraw-Hill, 1979.

Dicdican Y.R. and Haimes Y.Y., Relating Multiobjective Decision Trees to the Multiobjective Risk Impact Analysis Method, Systems Engineering, Volume 8 Issue 2, June 2005

Engel A., Verification, Validation and Testing of Engineered Systems (Wiley Series in Systems Engineering and Management), Wiley, ISBN-10: 047052751X, ISBN-13: 978-047527511, Hardcover: 687 pages, June 2010.

Engel A. and Last M., "Modeling Software Testing Costs and Risks Using Fuzzy Logic Paradigm", Journal of Systems and Software, Volume 80, Issue 6, Pages 817-835, June 2007.

Engel A. and Shachar S., "Measuring and Optimizing Systems’ Quality Costs and Project Duration", Systems Engineering Journal, Volume 9, issue 3, pages 259-280, June 2006.

Engel A. and Barad M., "A Methodology for Modeling VVT Risks and Costs", Systems Engineering Journal, Volume 6, issue 3, Pages 135-151, May 2003.

Enyinda C.I., Modeling Risk Management in Pharmaceutical Industry Global Supply Chain Logistics Using Analytic Hierarchy Process Model, Ph.D. Dissertation, North Dakota State University, Fargo, 2008

Grant P.D., Pert and CPM: Network methods for project planning, scheduling and control, Small-Scale Master Builder, ASIN: 0911215018, 1983.

Grossi P. and Kunreuther H. (Editors), Catastrophe Modeling: A New Approach to Managing Risk, Springer, ISBN-10: 0387230823, ISBN-13: 978-0387230825, 2004

Haimes Y.Y, On the Complex Definition of Risk: A Systems-Based Approach, Risk Analysis, Volume 29, Issue 12, pages 1647–1654, December 2009

Hall, D.C., Making risk assessments more comparable and repeatable. Systems Engineering, Volume 14, Issue 2, pages 173–179, 2011

Hoppe M., Engel A. and Shachar S., "SysTest: Improving the Verification, Validation & Testing Process - Assessing Six Industrial Pilot Projects", Systems Engineering Journal, Volume 10, Issue 4, Pages 323-347, Sep. 2007.

Houston X.D., Mackulak T.G. Collofello S.J., Stochastic simulation of risk factor potential effects for software development risk management, Journal of Systems and Software, Volume 59, Issue 3, Pages 247-257, 15 December 2001

Hu Y., Huang J., Chen J., Liu M. and Xie K., Software Project Risk Management Modeling with Neural Network and Support Vector Machine Approaches, International Conference on Natural Computation, vol. 3, pp. 358-362, Third International Conference on Natural Computation (ICNC 2007), 2007

INCOSE-2011, Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities, Version 3.2.1, International Council on Systems Engineering, ISBN 0972056297, 9780972056298, 2011

Islam S., Goal and Risk Factors in Offshore Outsourced Software Development from Vendor's Viewpoint, Fourth IEEE International Conference on Global Software Engineering, Limerick, Ireland, July 13-July 16, 2009A

Islam S., Software development risk management model: a goal driven approach, The 7th joint meeting of the European Software Engineering Conference (ESEC) and the ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE), Amsterdam, The Netherlands, August 24-28, 2009B

ISO 31000:2009, Risk management - Principles and guidelines, ISO (International Organization for Standardization) Standard 31000, 2009

Jackel P., Monte Carlo Methods in Finance, ISBN: 047149741X, John Wiley & Sons, 2002.

Juran J.M. and Gryna F.M., Quality Planning and Analysis: From Product Development Through Use, 2nd ed., McGraw- Hill, New York, 1980.

Kontio J., The Riskit Method for Software Risk Management, version 1.00. CS-TR-3782 / UMIACS-TR-97- 38, College Park, MD, University of Maryland. Computer Science Technical Reports, 1997.

Kujawski, E., Selection of technical risk responses for efficient contingencies, Systems Engineering, Volume 5, Issue 3, pages 194–212, 2002

Kujawski E. and Angelis D., Monitoring Risk Response Actions for Effective Project Risk Management, Systems Engineering, Vol. 13, No. 4, 2010

Kyoomarsi F., Dehkordy K.P., Peiravy H.M. and Heidary E., Using UML and Fuzzy Logic in Optimizing Risk Management Modeling, International Association for Development of the Information Society (IADIS) Conference, Freiburg, Germany 13 - 15 October 2008

Loveridge D., Experts and foresight: review and experience, Paper 02-09, PRES, The University of Manchester, Manchester, UK, 2002

Marais N., Dulac N. and Leveson N., Beyond Normal Accidents and High Reliability Organizations: The Need for an Alternative Approach to Safety in Complex Systems, Working paper presented to Engineering Systems Division Symposium, Massachusetts Institute of Technology (MIT), Cambridge, Mass, March 24, 2004

Marczyk J., Principles of simulation-based computer-aided engineering, FIM Publications, Dep. Legal B-38994-99, Barcelona, Spain, 1999.

NMP-GL-07-V1, New Millennium Program - Guidelines for Preparing Project Risk Management Plans, National Aeronautics and Space Administration, New Millennium Program, June 7, 2005

Nuseibeh B., Ariane 5: Who Dunnit?, IEEE Software, pp. 15-16, May/June 1997

Oberkampf L.W., Trucano G.T. and Hirsch C., "Verification, Validation and Predictive Capability in Computational Engineering and Physics", Foundation for V&V in the 21st century workshop, John Hopkins University, Laural, Md. Oct. 2002.

Pennock J.M. and Haimes Y.Y., Principles and guidelines for project risk management, Systems Engineering, Volume 5, Issue 2, pages 89–108, 2002

Ramana V.M., Beyond our imagination: Fukushima and the problem of assessing risk, Bulletin of the atomic scientists, 19 April 2011

Saaty T.L., The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation, McGraw-Hill, 1980.

Shan X., Jiang GR. and Huang T., A Framework of Estimating Software Project Success Potential Based on Association Rule Mining, International Conference on Management and Service Science, 2009, MASS '09, 20-22 Sept. 2009

Stamatelatos, M., Apostolakis, G., Dezfuli, H., Everline, C., Guarro, S., Moieni, P., Mosleh, A., Paulos, T. and Youngblood, R. Probabilistic risk assessment - Procedures guide for NASA Managers and Practitioners, NASA, Office of Safety and Mission Assurance, August, 2002

Visnepolschi S. and Ramsey J.D. (Editors), How to Deal with Failure - Failure Prediction and Analysis Using Anticipatory Failure Determination, Aptimise - edu, 2009

Wallace W.S. and Ziemba T.W. (Editors), Applications of Stochastic Programming, Society for Industrial and Applied Mathematics, ISBN-10: 0898715555, ISBN-13: 978-0898715552, 2005

Weiler M., Homsky O. and Raveh A., "Patterns for Risk Management – towards a pattern Language", EuroPLoP 2010, the 15th European Conference on Pattern Languages of Programs, Bavaria, Germany, July, 2010.

Yan Z. and Haimes Y.Y., Risk-Based Multiobjective Resource Allocation in Hierarchical Systems with Multiple Decisionmakers. Part I: Theory and methodology, Systems Engineering, published online: 2 FEB. 2010A

Yan Z. and Haimes Y.Y., Risk-Based Multiobjective Resource Allocation in Hierarchical Systems with Multiple Decisionmakers. Part II: A Case Study, Systems Engineering, published online: 2 FEB. 2010B

8. Appendix A - use case raw data

Appendix-A depicts the raw data utilized in creating the use case example provided in the article. It includes 1) Risk scenarios data, 2) Risk Response Action (RRA) data and 3) RRA strategy data. All values in this appendix have been estimated from: (1) Organization historical data and (2) Formal Delphi process conducted with between four and ten domain experts.

8.1 Risk scenarios data

The risk scenarios table defines: 1) the system lifecycle phase $L_{i,j}$ in which the risk may occur, 2) the risk identifier, 3) the nature of the risk $R_{i,j}$, 4) the risk probability $P,\ 0<P<1$, 5) the impact cost $Ci_{i,j}$ of the risk, should it occur and 6) the impact time $Ti_{i,j}$, should it occur.

Impact phase	Risk ID	Risk impact scenario	Risk prob.	Risk cost [K$]	Risk time [Day]
Definition	R1.12.1	Because the quality of the system requirements was poor, the System Requirements Review (SRR), conducted during the definition phase, may have failed. This may require rewriting most of the requirements and repeating the SRR process, which may add cost and may delay the development schedule.	0.80	22.0	16.0
Design	R1.3.1	Because the system requirements have not been presented and discussed with all stakeholders of the system, a major redesign of the system may be required during the system design phase.	0.33	53.0	62.6
	R1.10.1	The software design does not meet existing hardware and operating system stipulation and limitations imposed by the customer. As a result the design may have to be scrapped and a new design may be required. This may cause a programmatic delay and added costs.	0.95	10.0	10.1
	R2.1.1	The designers of the system may be unable to meet system weight and size requirements. This may require renegotiations vis-à-vis contract technical parameters or undertaking radical modifications to existing COTS (Commercial Off The Shelf) components of the system.	0.83	10.0	13.3
Implementation	R1.11.1	Because implementing the system necessitates stakeholders support while the developing organization culture does not support information exchange with other parties, implementation of several capabilities may not proceed as expected resulting in loss of money and time.	0.83	10.0	6.6
	R2.2.1	Because some subcontractors deliver their subsystems without proper testing documentations, some defective subsystem may be delivered, necessitating either lengthy in-house retesting or requiring subsystems to be returned to original manufacturers.	0.67	21.0	2.4
	R2.4.1	The system design may be inconsistent with the system requirements. This could be discovered during the implementation phase, necessitating either redesign of the relevant system's elements or correcting the original system requirements.	0.95	10.0	4.7
	R3.1.1	Because the engineering team ignored key action-items generated during earlier project phases, serious problems associated with incorrect requirements or design may surface during the implementation phase. This may impede the implementation process as the identified problems may be corrected.	0.50	21.0	20.2
	R3.3.1	Because the software department is understaffed and the most programmers are inexperienced in real-time applications the delivered software may be available late and may contain many errors.	0.17	21.0	30.3
Integration	R1.1.1	Because system integration simulators, tools and equipment were not purchased or developed, the integration process may be hampered.	0.33	75.0	28.3
	R1.2.1	Because subsystems testing infrastructure was not identified and developed, the subsystems acceptance process may require both additional funding and more checkout time slowing the system integration.	0.83	64.0	79.3
	R1.8.1	Because quality attributes requirements are habitually not addressed by the engineering department, certain problems, which may be discovered during the integration phase may require expansive system modifications and may delay the project substantially.	0.50	32.0	15.9
	R2.3.1	Because design reviews of subsystems are not regularly performed, the interface design of some subsystems may not meet requirements. This may slow the system integration process.	0.95	21.0	10.1
	R2.7.1	Because the development team is isolated from post-development activities (production, use/maintenance and disposal), the design may not meet or be optimized for these, later phases, needs. The problem may be detected during the integration phase and substantial system re-design may be required.	0.83	21.0	4.5
	R2.8.1	Because a large physical part of the system is not designed for transportability and is built far from the integration facility, the system integration may be postponed until this part may be redesigned or a special means of transportation may be arranged.	0.33	21.0	11.5

Impact phase	Risk ID	Risk impact scenario	Risk prob.	Risk cost [K$]	Risk time [Day]
	R2.9.1	Because subcontractors are not required to prove their subsystems functionality and interfaces prior to delivery to the System Integration Laboratory (SIL), several {delivery-tests-failure-return} iterations may be required before subsystems may be properly integrated into the system.	0.95	21.0	5.5
	R2.10.1	Due to interdepartmental rivalry, the software may be designed to meet quite different objectives and its interfaces may not be compatible with the rest of the system. This may be discovered during the integration phase and may necessitate redesigning and rewriting of the software.	0.95	32.0	10.1
	R3.2.1	Because several implemented subsystem interfaces were not verified against the existing design, major integration problems may disturb the system integration process, possibly causing delays and customers dissatisfaction.	0.33	32.0	18.2
	R3.4.1	Because key enabling products are implemented without proper requirements definition and design, the simulators embedded in the System Integration Laboratory (SIL) may not reflect the behavior of the real subsystems. This may significantly impede the integration process.	0.95	10.0	11.0
	R3.5.1	Because a system integration plan has not been generated, the entire integration process may be chaotic and different components / subsystems may be delivered for integration in a disorderly manner. This may result in uncontrolled integration process causing delays and extra work.	0.83	21.0	8.8
	R4.2.1	Because several subsystems interfaces have not been built In Accordance With (IAW) specifications, the specifications themselves may need corrections or the relevant subsystems may fail during the integration phase and may necessitate corrective action and rework. This may delay the completion of the integration process.	0.83	10.0	2.9
Qualification	R1.4.1	Because safety issues were ignored and plans were not created, a major accident with, possibly involving, loss of life or damage to property may result.	0.05	289.0	283.3
	R1.5.1	Because customer requirements were not thoroughly assessed by the engineering team, certain requirements may not be met at system qualification time and may result in fines and customer dissatisfaction.	0.67	21.0	8.8
	R1.6.1	Because no engineering function is tasked with comparison and evaluation of customer versus engineering requirements, a mismatch between the two sets of system requirements may be found which may cause a delay in project delivery date.	0.50	21.0	13.3
	R1.7.1	Because the system communication frequency/power definition was not evaluated against state regulations, a communication violation may be identified which may necessitate a recall of the system for a retrofit.	0.17	32.0	19.8
	R1.9.1	Because the developed system did not undergo rigorous and formal system reviews, the customer may identify inconsistencies during the qualification phase which may require system corrections related to errors in 1) requirements, 2) design, 3) implementation, 4) integration or 5) qualification.	0.83	21.0	6.6
	R2.5.1	Because design for system safety is marginal, a major accident may occur during the qualification phase which may result in loss of life, property damage or political embarrassment.	0.05	525.0	126.4
	R2.6.1	Because some components of the system were not designed for environmental requirements, the customer may detect this problem at the qualification phase and may insist that these parts be re-designed, re-fabricated and re-qualified.	0.67	10.0	10.1
	R2.11.1	Management mandated a new design tool. The tool is cumbersome and immature, containing many defects. Most design engineers are depressed, discouraged and do not like to use it. The system design may be inferior and may exhibit multiple failures during its qualification.	0.33	52.0	33.1
	R3.6.1	Because training enabling products (e.g. user guide, training simulator, etc.) are not available during the qualification phase, customer training may be delayed. As a result, the customer may not approve system's acceptance.	0.17	10.0	15.2
	R3.7.1	Because the engine selected for powering the air vehicle has never been used in similar helicopter applications, there is a risk that it may not provide the thrust and endurance required for the intended flight environment. This may result in a lengthy qualification process, not originally planned.	0.67	21.0	26.4
	R3.8.1	Because many details of the system are not defined in the requirements and are left to the system implementers, stakeholders of the system may consider these features unacceptable, resulting in major rework detected during systems qualification.	0.83	32.0	15.2
	R4.1.1	Because several subcontractors did not implement some subsystems capabilities, problems may be detected during the qualification phase, requiring returning subsystems to the original manufacturers for correction. This may cause project delays and customer dissatisfaction.	0.33	21.0	20.2
	R4.3.1	Due to schedule limitations up to system shipment date, minimal verification, validation and testing are conducted during the integration process. Consequently, many subsystems may exhibit numerous system errors during the qualification phase which may cause delays and cost overruns.	0.67	10.0	12.1
	R4.4.1	A disgruntled employee maliciously sabotages the software database. This may cause serious project delay as the original software may have to be obtained from old software available at programmers' local computers or the software may have to be recreated.	0.67	10.0	3.4

Impact phase	Risk ID	Risk impact scenario	Risk prob.	Risk cost [K$]	Risk time [Day]
	R4.5.1	Because formal flight Test Readiness Review (TRR) was not conducted, the customer may not approve continuance of the qualification phase. This may result in customer declaring the system qualification as a failure, causing delays and embarrassment.	0.67	10.0	2.6
	R4.6.1	Because some influential stakeholders did not approve or validate the integrated system, several key new requirements or requirements "hidden" within the Request For Proposal (RFP) may surface during the qualification phase. This may delay the transition of the system into production phase.	0.33	21.0	13.3
	R5.1.1	Because some open action-items from previous phases were ignored or forgotten, several problems may be identified during the qualification phase. The cost of correcting these problems at this time may exceed substantially the allocated budget and may negatively impact the schedule.	0.67	10.0	6.7
	R5.2.1	Because the helicopters' external paint did not match the standard required by the customer, the entire painting may have to be manually removed and a new multi layer painting may be required. This may affect cost and schedule of system delivery as well as reputation of contractor.	0.67	10.0	4.1
	R5.3.1	Because fire broke in the system qualification facility, some prototype subsystems may have been damaged, possibly causing qualification delays and substantial unanticipated costs during the qualification phase.	0.67	21.0	6.7
	R5.4.1	Because the customer identifies many content and quantity defects in the Integrated Logistic Support (ILS) as well as inconsistencies with requirements, the qualification phase may be halted until all ILS problems are rectified.	0.50	32.0	79.3
	R5.5.1	Because large numbers of system defects have been discovered, the qualification phase may require substantially more time to complete and the cost of this phase may exceed original budget.	0.67	21.0	11.0
	R5.6.1	Because a Physical Configuration Audit (PCA), discovered numerous inconsistencies between components or subsystems and their documentations the system qualification process may be halted by the customer until all problems are rectified.	0.83	10.0	0.7
	R5.7.1	Because of a labor strike action at a key subcontractor facility, critical activity may halt the progress of the qualification process. This may delay the customer planned acceptance test.	0.83	10.0	6.6

8.2 Risk response action data

The Risk Response Action (RRA) table defines: 1) the system lifecycle phase $L_{i,j}$ in which the RRA may be carried out, 2) the RRA identifier 3) the nature of the RRA $RRA_{i,j}$, 4) the cost $Cr_{i,j}$ of performing the RRA and 5) the time $Tr_{i,j}$ required to perform the RRA and 6) the risk identifier (the risk whose impact the current RRA is expected to eliminate or reduce).

RRA phase	RRA ID	RRA activity	RRA cost [K$]	RRA Time [Day]	Risk ID
Definition	V1.1	Ensure proper planning and preparations of the integration process. This may include, among other, all simulators, tools and equipment needed for the integration, all must be identified and then either purchased or developed.	32.0	15.9	R1.1.1
	V1.2	Ensure appropriate design and implementation of all components and subsystems testing infrastructure. This may include, among other, availability of hardware, software and simulation infrastructure as well as procedures for subsystems acceptance testing.	26.0	24.3	R1.2.1
	V1.3	Ensure full stakeholders management processes. This may include, among other, identification of all stakeholders, assessment of stakeholders' objectives, motives and techno-political power and the ongoing inclusion of stakeholders in the system development process.	20.0	23.8	R1.3.1
	V1.4	Ensure that all relevant project management plans are assessed. This may include, among other, the project risk management plan, project safety management plan, project environmental impact management plan and the like.	19.0	12.1	R1.4.1
	V1.5	Ensure that all customer requirements are thoroughly assessed. In particular such requirements should be checked for functional and interface consistency, feasibility and testability.	38.0	15.9	R1.5.1
	V1.6	Ensure that the engineering department establishes appropriate technical bodies as well as procedures to evaluate customer versus engineering requirements for consistency, feasibility and traceability.	26.0	12.1	R1.6.1
	V1.7	Ensure that all requirements meet (and if possible, exceed) customer standards, laws and environment requirements as well as ethical considerations.	13.0	7.9	R1.7.1
	V1.8	Ensure that all relevant system's quality attributes requirements receive management attention and are regularly reviewed. This may include: Accessibility, Adaptability, Availability, Configurability, Degradability, Dependability, Deployability, Durability, Flexibility, Interchangeability, Maintainability, Modularity, Operability, Recoverability, Reliability, Repeatability, Reproducibility, Safety, Scalability, Supportability, Stability, Survivability, Sustainability, Tailorability, Testability, Usability, etc.	28.0	12.1	R1.8.1

RRA phase	RRA ID	RRA activity	RRA cost [K$]	RRA Time [Day]	Risk ID
	V1.9	Ensure that all relevant system's reviews are conducted in a rigorous and formal manner. This may include: System/Software Requirements Review (SRR), System/Software Design Review (SDR), System/Software Acceptance Test Review (ATR), System Test Readiness Review (TRR), etc.	26.0	7.9	R1.9.1
	V1.10	Ensure that all relevant hardware, software and requirements engineers evaluate system and software design by ways of peer reviews as well as informal and, sometimes, formal reviews.	13.0	12.1	R1.10.1
	V1.11	Ensure that the engineering management will be aware of critical stakeholders and open a relevant dialogue as part a normal business practice. In particular, instill a spirit of cooperation between the engineering team and key stakeholders.	13.0	7.9	R1.11.1
	V1.12	Ensure the quality of all system requirements by reviewing that each requirement is clear, complete, consistent, correct, feasible, non-compounded, precise, succinct, traceable, unambiguous and understandable.	12.0	20.0	V1.12.1
Design	V2.1	Ensure, as a matter of policy, that all project development plans contain sufficient time and funding slack budgets, allowing handling of such unexpected events without affecting the overall allotted schedule and budget.	6.0	6.1	R2.1.1
	V2.2	Ensure, as a matter of policy, that all subsystems are delivered with approved test documentations. This rule should be applied at both the subsystems and system as well as to all enabling products.	106.0	15.9	R2.2.1
	V2.3	Ensure that all subsystems interface design is properly reviewed under both informal - e.g. peer review, as well as formal - e.g. subsystems Preliminary Design Review (PDR) and Critical Design Review (CDR).	38.0	18.2	R2.3.1
	V2.4	Ensure that the system functional and interface design is clearly traced to the system requirements, in other words, system design is consistent with the system requirements. In addition, ensure the internal consistency of the system design.	42.0	23.8	R2.4.1
	V2.5	Ensure that safety consideration permeate all system development projects. This should be enforced during all phases of the systems lifecycle. In addition, management attention must be given to system design for controlled degradation (Failure modes).	26.0	6.1	R2.5.1
	V2.6	Ensure that the design, fabrication and qualification of all parts of the system meet environmental requirements.	13.0	15.9	R2.6.1
	V2.7	Ensure that product development is conducted under an Integrated Product Team (IPT) framework where engineers and other professionals from different disciplines, having multitude of expertise, are involved in all aspects of product development.	58.0	12.1	R2.7.1
	V2.8	Ensure that product all development processes shall include design evaluation for warehousing, transportation and construction needs.	22.0	15.9	R2.8.1
	V2.9	Ensure that contracts with suppliers will mandate subcontractors to conduct approved subsystems tests for all supplied materials, components, subsystems and enabling products prior to delivery to the SIL.	93.0	18.2	R2.9.1
	V2.10	Ensure that management shall be fully aware of human element dimension of engineers within the organization. In addition, regular reviews must be conducted at the team level (peer review) as well as internal/formal reviews (software/system PDRs and CDRs).	38.0	15.9	R2.10.1
	V2.11	Ensure that all support tools introduced during a project's development stage have been thoroughly evaluated. Relevant engineering teams have been properly trained and are, in general, supporting the new development process.	13.0	6.1	R2.11.1
Implementation	V3.1	Ensure that all action-items are closely monitored and raised during regular status meetings by the assigned personnel.	6.0	7.9	R3.1.1
	V3.2	Ensure that all subsystem interfaces are verified for consistency with design (i.e. subsystems prototypes versus subsystems functional design and subsystems prototypes versus system interface design).	32.0	18.2	R3.2.1
	V3.3	Ensure that management is fully aware of the personnel problems in all engineering departments and especially in the critical ones (e.g. software).	13.0	23.8	R3.3.1
	V3.4	Ensure that enabling products are developed within acceptable procedures and undergo proper requirement definition, design, fabrication, integration and qualification. This should include enabling products for: System development, testing, production, deployment, training, operations and disposal.	77.0	60.7	R3.4.1
	V3.5	Ensure that all phases of the development cycle will be planned to a level that will enhance orderly and methodical development progression.	19.0	7.9	R3.5.1
	V3.6	Ensure that management pays attention to all aspects of the engineering business. This should include: 1) Enabling products (in support of System development, testing, production, deployment, training, operations and disposal), 2) Integrated Logistic Support (ILS) issues as well as 3) Target products.	13.0	18.2	R3.6.1
	V3.7	Ensure that projects planning involving new technology insertion into new products will take into account realistic cost and time factors in order to handle unexpected problems.	51.0	63.5	R3.7.1
	V3.8	Ensure that system requirements are defined in the highest reasonable detail. In addition, ensure that interactions between system developers and stakeholders are maintained throughout the development period so undefined details may be discussed as early as possible.	13.0	6.1	R3.8.1
Integr ation	V4.1	Ensure that all components and subsystems be fully qualified before they are accepted into the integration process.	6.0	7.9	R4.1.1
	V4.2	Ensure that all interface definitions are carefully managed, as much as possible by means of database tools, throughout the system development period.	22.0	6.1	R4.2.1

RRA phase	RRA ID	RRA activity	RRA cost [K$]	RRA Time [Day]	Risk ID
	V4.3	Ensure that management follows the progress of the projects, possibly by using the Earned Value Management (EVM) method. In addition, ensure that management does not permit a state where accumulated project delays lead to insufficient system verification, validation and testing.	64.0	95.2	R4.3.1
	V4.4	Ensure that management is aware of internal and external security considerations, prepares operational procedures to handle unexpected eventualities and frequently back up all project data against internal or external hazards emanating from natural disasters or due to malicious intents.	38.0	12.1	R4.4.1
	V4.5	Ensure constructive cooperation between the customer and the main contractor. Ensure the contract as well as ongoing negotiations clearly defines the expectations and responsibilities of each party and milestones to be adhered to by the project.	26.0	7.9	R4.5.1
	V4.6	Insure the ongoing involvement of as many as reasonable stakeholders during the system development period.	13.0	6.1	R4.6.1
Qualification	V5.1	Ensure that all action-items are closely monitored and raised during regular status meetings by the assigned personnel.	10.0	7.9	R5.1.1
	V5.2	Ensure the identification and traceability of all system requirements, preferably using computerized database system. In addition, ensure that incoming raw material, components, etc. (i.e. in this case paint ID), are thoroughly inspected.	83.0	24.3	R5.2.1
	V5.3	Ensure that management is aware of all potential hazards in all development facilities and take proactive actions to mitigate these risks (e.g. meeting safety regulations, insuring facilities, equipment, people, etc.).	38.0	15.9	R5.3.1
	V5.4	Ensure constructive cooperation between the customer and the main contractor. Ensure the contract as well as ongoing negotiations clearly defines the expectations and responsibilities of each party and milestones to be adhered to by the project.	13.0	24.3	R5.4.1
	V5.5	Ensure that verification, validation and testing is performed effectively and as early as reasonably possible within the development lifecycle. This will reduce the overall cost and budgets associated with defect removal.	70.0	47.6	R5.5.1
	V5.6	Ensure that within each engineering project internal, but systematic, PCA is conducted prior to formal system qualification is undertaken.	90.0	6.1	R5.6.1
	V5.7	Ensure that management adopts some aspects of the Just-In-Time (JIT) philosophy, which is based on establishing close working relationships with suppliers. Financial situation, management problems and employee grievances of subcontractors should be followed by management.	13.0	7.9	R5.7.1

8.3 Risk response action strategy data

The Risk Response Action (RRA) strategy table defines: 1) the system lifecycle phase $L_{i,j}$ in which the RRA activity will be carried out, 2) the RRA identifier and 3) the RRA performance level[15] $X,\ 0 \le X \le 1$.

RRA phase	RRA ID	RRA performance level (X)
Definition	V1.1	0.20
	V1.2	0.10
	V1.3	0.00
	V1.4	0.00
	V1.5	0.20
	V1.6	0.05
	V1.7	0.20
	V1.8	0.10
	V1.9	0.20
	V1.10	0.20
	V1.11	0.10
	V1.12	0.20
Design	V2.1	0.00
	V2.2	0.05
	V2.3	0.10
	V2.4	0.20
	V2.5	0.60
	V2.6	0.10
	V2.7	0.00
	V2.8	0.10
	V2.9	0.20
	V2.10	0.30
	V2.11	0.10

RRA phase	RRA ID	RRA performance level (X)
Implementation	V3.1	0.00
	V3.2	0.30
	V3.3	0.00
	V3.4	0.05
	V3.5	0.50
	V3.6	0.40
	V3.7	0.40
	V3.8	0.00
Integration	V4.1	0.00
	V4.2	0.50
	V4.3	0.50
	V4.4	0.60
	V4.5	0.80
	V4.6	0.10
Qualification	V5.1	0.00
	V5.2	0.30
	V5.3	0.80
	V5.4	0.60
	V5.5	0.60
	V5.6	0.00
	V5.7	0.10

15 Each RRA performance level (Xi) is determined by considering the full range of the given RRA (i.e. the components of an all-encompassing risk response) versus the actual subset to be preformed.

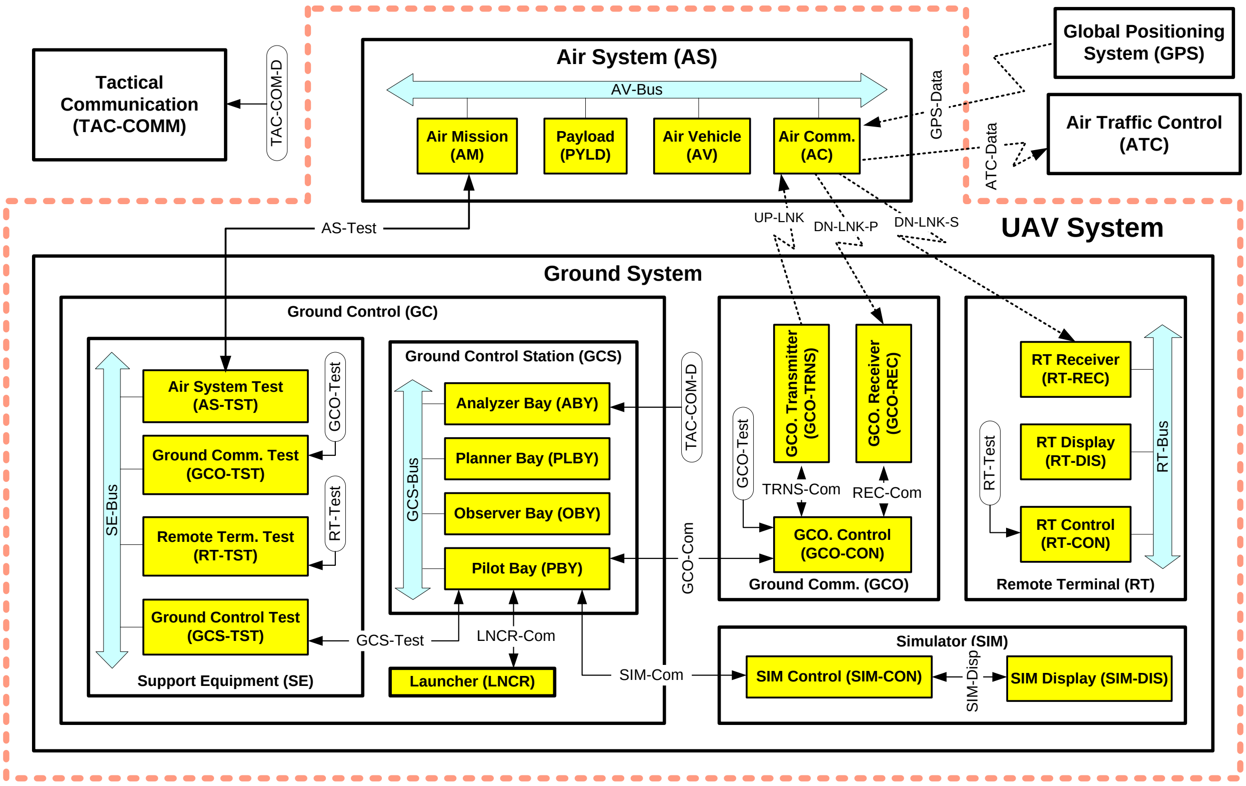
9. Appendix B: Presentation to the RMWG

The Presentation was given to the Risk Management Working Group (RMWG) at INCOSE – ILTAM on 25/12/2011. (Not included).

10. Appendix C: Risk Management Questionnaire

10.1 Use case description

The ADS-95 Ranger System is utilized for information gathering in threat environments that pose risk to a manned or piloted air mission, or where extended mission times are required. Information is gathered by the system for reconnaissance, target acquisition, and battle damage assessment. The information is returned to the ground station via radio signals. The air vehicle is a fixed wing configuration with a rear engine. The vehicle is either flown remotely from the ground station shelter or autonomously using a predetermined flight plan. The following figure depicts the major physical components of the system. The arrows indicate the data flow between system components, and the direction of arrows signals the direction of the data flow. The ADS-95 overall development program (Engineering + Manufacturing) is valued at $235M. The Engineering development work should be completed in 3 years at a cost of approximately $100M.



10.2 Use case raw data

The following table depicts the risk scenarios data for this questionnaire. It defines:

1. The system lifecycle phase in which the risk may occur,
2. The risk identifier,
3. The nature of the risk (risk scenario).

10.3 Practical questions

Given the above risk scenarios, please provide the following information:

1. Order all the risk scenarios from the Most critical (1) to the Least critical (13)
2. Of the funding available for system development ($100 Million), 0.5% or $500,000 (5,000 Hours) was allocated to the risk mitigation activities. Identify how many man-hours you will allocate to mitigate each risk scenario.

Impact phase	Risk ID	Risk impact scenario	Risk order	Risk mitigation investment [$]
Definition	1.	Because the **quality of the system requirements was poor**, the System Requirements Review (**SRR**), conducted during the definition phase, **may fail**. This may require rewriting most of the requirements and repeating the SRR process, which may add cost and may delay the development schedule.		
Design	2.	Because the **system requirements have not been presented and discussed with all stakeholders of the system**, a major redesign of the system may be required during the system design phase.		
	3.	The **software design does not meet existing hardware and operating system stipulation and limitations imposed by the customer**. As a result the design may have to be scrapped and a new design may be required. This may cause a programmatic delay and added costs.		
Implementation	4.	Because some **subcontractors deliver their subsystems without proper testing documentations**, **some defective subsystem may be delivered**, necessitating either lengthy in-house retesting or requiring subsystems to be returned to original manufacturers.		
	5.	Because the **software department is understaffed** and **most programmers are inexperienced** in real-time applications the delivered software may be available late and may contain many errors.		
Integration	6.	Because subsystems **testing infrastructure was not identified and developed**, the subsystems acceptance process may require both additional funding and more checkout time slowing the system integration.		
	7.	Because the development team is isolated from post-development activities (production, use/maintenance and disposal), the **design may not meet or be optimized for** these, later phases, **needs**. The problem may be detected during the integration phase and substantial system re-design may be required.		
	8.	Because key enabling products are implemented without proper requirements definition and design, the simulators embedded in the System Integration Laboratory (**SIL**) **may not reflect the behavior of the real subsystems**. This may significantly impede the integration process.		
Qualification	9.	Because the developed system **did not undergo rigorous system reviews**, the customer **may identify inconsistencies** during the qualification phase which may require system corrections related to errors in 1) requirements, 2) design, 3) implementation, 4) integration or 5) qualification.		
	10.	Because the **engine** selected for powering the air vehicle has **never been used in similar applications**, there is a risk that it m**ay not provide the thrust and endurance required for the intended flight environment**. This may result in a lengthy qualification process, not originally planned.		
	11.	Because many details of the system were not defined in the requirements and were left to the system implementers, stakeholders of the system may consider these features unacceptable, resulting in major rework detected during systems qualification.		
	12.	Due to schedule limitations, **minimal** verification, validation and testing (**VVT**) **are conducted** during the integration process. Consequently, many subsystems **may exhibit numerous system errors** during the qualification phase which may cause delays and cost overruns.		
	13.	Because **large numbers of system defects may have been discovered**, the qualification phase may require substantially more time to complete and the cost of this phase may exceed original budget.		

10.4 Methodological questions

After analyzing the individual responses, it is clear that:

1. Each person generates a "gut feeling" set of responses
2. By and large, different persons have different "gut feeling"
3. Many other issues must be addressed
4. Bottom line: The "gut feeling" approach is not an effective way to create a risk mitigation strategy

10.4.1 Question-1

Is it of value to optimize the risk mitigation strategy?

#	Yes	No
1.		

10.4.2 Question-2

If you had the resources and the ability to gather relevant information to help in optimizing the risk mitigation strategy, what information will you gather?

#	Information
1.	
2.	
3.	
4.	
5.	
6.	

10.4.3 Question-3

Can you suggest an algorithm to optimize the risk mitigation strategy?

11. Appendix-D: Response to Questionnaire

The following results were obtained by the Risk Management expert group.

11.1 Raw results

11.1 Processed results

	13	12	11	10	9	8	7	6	5	4	3	2	1	שאלה:	חשיבות
91	6	5	8	7	4	3	2	1	9	10	11	12	13		
91	13	8	3	10	2	9	12	7	6	11	5	4	1		
91	13	12	11	10	9	8	7	6	5	4	3	2	1		
91	4	3	2	1	5	8	7	6	10	9	11	12	13		
91	8	3	6	11	10	2	5	4	7	9	1	12	13		
91	10	8	2	11	9	5	7	3	4	6	12	1	13		
91	13	12	6	4	11	3	2	10	9	5	8	1	7		
91	13	12	4	3	11	10	7	8	9	6	5	2	1		
91	12	11	1	10	8	7	9	4	5	3	2	6	13		
91	13	12	11	10	9	8	7	6	5	4	3	2	1		
	10.50	8.60	5.40	7.70	7.80	6.30	6.50	5.50	6.90	6.70	6.10	5.40	7.60		
	13	12	1 2	10	11	5	6	3	8	7	4	1 2	9		
	3.37	3.78	3.66	3.71	3.08	2.83	2.99	2.59	2.18	2.83	4.09	4.79	5.97		
	13	12	11	10	9	8	7	6	5	4	3	2	1	אלה:	
100	10	10	10	10	11	12	12	9	4	4	4	3	1		
100	4	15	0	10	0	0	1	20	30	5	5	0	10		
100	6	10	11	11	11	7	6	9	7	6	6	5	5		
100	10	15	5	10	5	15	5	5	5	5	10	5	5		
100	5	10	5	5	5	5	5	10	20	10	10	5	5		
100	3	7	10	7	7	9	7	11	10	8	3	15	3		
100	4	10	4	10	4	9	9	9	20	4	4	9	4		
100	12	13	4	11	4	11	4	7	4	7	7	4	12		
100	4	4	12	10	8	6	8	8	8	4	10	12	6		
100	3	3	3	3	4	3	3	4	9	10	10	18	27		
100	6.10	9.70	6.40	8.70	5.90	7.70	6.00	9.20	11.70	6.30	6.90	7.60	7.80		
	11	2	9	4	13	6	12	3	1	10	8	7	5		
	3.31	4.11	4.03	2.75	3.41	4.45	3.16	4.37	8.71	2.36	2.88	5.74	7.47		
	13	12	11	10	9	8	7	6	5	4	3	2	1	אלה:	
91	6	5	8	7	4	3	2	1	9	10	11	12	13		
91	13	8	3	10	2	9	12	7	6	11	5	4	1		
91	13	12	11	10	9	8	7	6	5	4	3	2	1		
91	4	3	2	1	5	8	7	6	10	9	11	12	13		
91	8	3	6	11	10	2	5	4	7	9	1	12	13		
91	10	8	2	11	9	5	7	3	4	6	12	1	13		
91	13	12	6	4	11	3	2	10	9	5	8	1	7		
91	13	12	4	3	11	10	7	8	9	6	5	2	1		
91	12	11	1	10	8	7	9	4	5	3	2	6	13		
91	13	12	11	10	9	8	7	6	5	4	3	2	1		
	10.50	8.60	5.40	7.70	7.80	6.30	6.50	5.50	6.90	6.70	6.10	5.40	7.60		
	13	12	1 2	10	11	5	6	3	8	7	4	1 2	9		
	3.37	3.78	3.66	3.71	3.08	2.83	2.99	2.59	2.18	2.83	4.09	4.79	5.97		
	13	12	11	10	9	8	7	6	5	4	3	2	1	אלה:	
100	10	10	10	10	11	12	12	9	4	4	4	3	1		
100	4	15	0	10	0	0	1	20	30	5	5	0	10		
100	6	10	11	11	11	7	6	9	7	6	6	5	5		
100	10	15	5	10	5	15	5	5	5	5	10	5	5		
100	5	10	5	5	5	5	5	10	20	10	10	5	5		
100	3	7	10	7	7	9	7	11	10	8	3	15	3		
100	4	10	4	10	4	9	9	9	20	4	4	9	4		
100	12	13	4	11	4	11	4	7	4	7	7	4	12		
100	4	4	12	10	8	6	8	8	8	4	10	12	6		
100	3	3	3	3	4	3	3	4	9	10	10	18	27		
100	6.10	9.70	6.40	8.70	5.90	7.70	6.00	9.20	11.70	6.30	6.90	7.60	7.80		
	11	2	9	4	13	6	12	3	1	10	8	7	5		
	3.31	4.11	4.03	2.75	3.41	4.45	3.16	4.37	8.71	2.36	2.88	5.74	7.47		