UNIVERSITÄT DER BUNDESWEHR MÜNCHEN
Fakultät für Elektrotechnik und Informationstechnik

Acceptable Risk Criteria Catalogue for Technical Risk Management

Muhammad Saleem

Vorsitzender des Promotionsausschusses: Prof. Dr.-Ing. B. Lankl
1. Berichterstatter: Prof. Dr.-Ing. S. Schäffler
2. Berichterstatter: Prof. Dr.-Ing. J. Schulze

Tag der Prüfung 11. Mai 2011

Mit der Promotion erlangter akademischer Grad:
Doktor-Ingenieur
(Dr.-Ing.)

Neubiberg, den 18. Mai 2011

Contents

Acknowledgements

All praises to the Almighty Allah who bestows us intelligence, knowledge and wisdom. It is He who gave me ability, perseverance and determination to complete this work successfully.

My foremost thanks are to my supervisor, Prof. Dr. Stefan Schäffler for many useful discussions and providing me an opportunity to complete my PhD thesis at the University of Federal Armed Forces, Munich, Germany. I owe my special thanks to my advisor on spot, Prof. Dr. Jörg Schulze, whose support and guidance enabled me to complete my thesis work. He has been actively interested in my work and has always been available to advise me. I am very grateful for his patience, motivation, enthusiasm, and immense knowledge in Technical Risk management, taken together, make him a great mentor. The things which I have learnt from him are invaluable and which have helped me a lot to improve myself not only scientifically but also professionally.

I gratefully acknowledge the funding source, Siemens PG, which made my PhD work possible. I am thankful to the Department Manager, Mrs. Antje Lembcke, at the Department of Probabilistic Design and Risk Assessment for providing me an opportunity to work in her group.

My special thanks to Dr. Hanno Gottschalk for the useful discussions during the period we worked together at the Department of Probabilistic Design and Risk Assessment. My thanks are also due to my colleagues in Siemens PG for their co-operative, nice and friendly company throughout the period of my work in Siemens.

Many appreciations and special thanks to Mr. Gerd Weber in Siemens PG for providing useful literature and his time for fruitful discussions during the first year of this PhD work.

My special thanks goes to Prof. Dr. Johannes Gottschling at the University of Duisburg - Essen for always standing by me, encouraging and providing me his possible help in every context. I would like to thank Dr. Heiko Gemming for his valuable suggestions during the software development. My thanks are also due to my colleagues, Thilo H. Beuke and Sebastian Brieler, for their help during the final editing, proof reading and printing of this thesis.

I wish to express the heartfelt thanks and deep gratitude to my Parents, Parents - in-law, Sisters, and Brothers for their special prayers and encouragement. Their unconditional love and undoubted belief in me gave me a strength to be able to complete this work.

Last, but not least, I would like to thank my wife Saadia and children, Anas and Aiza, for providing me the encouragement necessary to succeed as well as having the patience to deal with the amount of time that comes with success.

1 Deutsche Zusammenfassung

1.1 Einführung

Für industrielle Unternehmen, die komplexe Serienprodukte herstellen, ist die Produktentwicklung wegen auftretender Langzeiteffekte und der ökonomischen Bedeutung ein essentieller Erfolgsfaktor. Die strategische Planung von Produkten definiert auch den Zeitpunkt, wann Produkte in den Markt eingeführt werden sollten. Im Rahmen dieser Vorgaben werden Entwicklungsprojekte gestartet, die diese Produktstrategie realisieren sollen. Während des Projekts sollten die geplanten Produkte einer Serienproduktion mithilfe von Wissen, Arbeitskräften und finanziellen Ressourcen so entworfen werden, dass die definierten Ziele bzgl. Qualität, Kosten und Zeit erreicht werden.

Steigende Konkurrenz im internationalen Markt, stagnierende Absatzmärkte und kürzere Produktlebenszyklen erhöhen die Anforderungen für industrielle Unternehmen mehr und mehr, um am Markt erfolgreich zu sein. Laut einer Untersuchung von McKinsey [McKinsey (2001)] im Bereich Automobilindustrie, welche repräsentativ für komplexe Serienprodukte ist, wird sich die Produktvielfalt in den nächsten fünf Jahren verdoppeln, Die Produktentwicklungszeit dagegen wird sich bei gleichbleibender Personalkapazität um ein Viertel reduzieren. Des Weiteren stellt McKinsey [McKinsey (2001)] in dieser Studie am Beispiel einer Pkw - Entwicklung (Bild 1-1) dar, welche Auswirkungen die verschiedenen Zielabweichungen auf den Deckungsbeitrag haben.

Bei Herstellern von komplexen Serienprodukten sind die Kosten für Garantie und Kulanz in den letzten Jahren sehr gestiegen. Zum Beispiel erhöhten sich die Ausgaben für Garantie und Kulanz der Marke Mercedes in den Jahren 1998 bis 2000 um das Dreifache [Harnischfeger & Reinking (2001)]. Die Marke Mercedes schätzte die Kosten für Garantie und Kulanz im Jahr 2000 auf 1,7 Milliarden Euro, was ungefähr dem Budget der Entwicklungskosten entspricht. Mit der Erweiterung der Garantie auf zwei Jahre in Europa seit Januar 2000 nimmt McKinsey [McKinsey (2001)] an, dass sich die Garantie- und Kulanzkosten um 30% bis 150%, abhängig von Hersteller und vorher gewährter Kulanz, erhöhen werden. Die Fehler, die zu Garantie- und Kulanzkosten führen, entstehen hauptsächlich in der Produktentwicklungsphase.

Die Produktentwicklung muss deshalb in immer kürzeren Zeiträumen kundenorientiert, kosteneffizient und zuverlässig sein. Unternehmen müssen ihre Bemühungen mehr denn je auf die frühen Stadien der Produktentwicklung konzentrieren, um auf die steigenden Bedürfnisse der Kunden einzugehen. Eine wichtige Rolle spielen dabei Produktqualität, Kosten und die Zeit der Markteinführung. Späte Korrekturen von Produkt eigenschaften oder Modifikationen an einem bereits eingeführten Produkt erhöhen die Ausgaben erheblich und führen zu signifikanten ökonomischen Nachteilen.

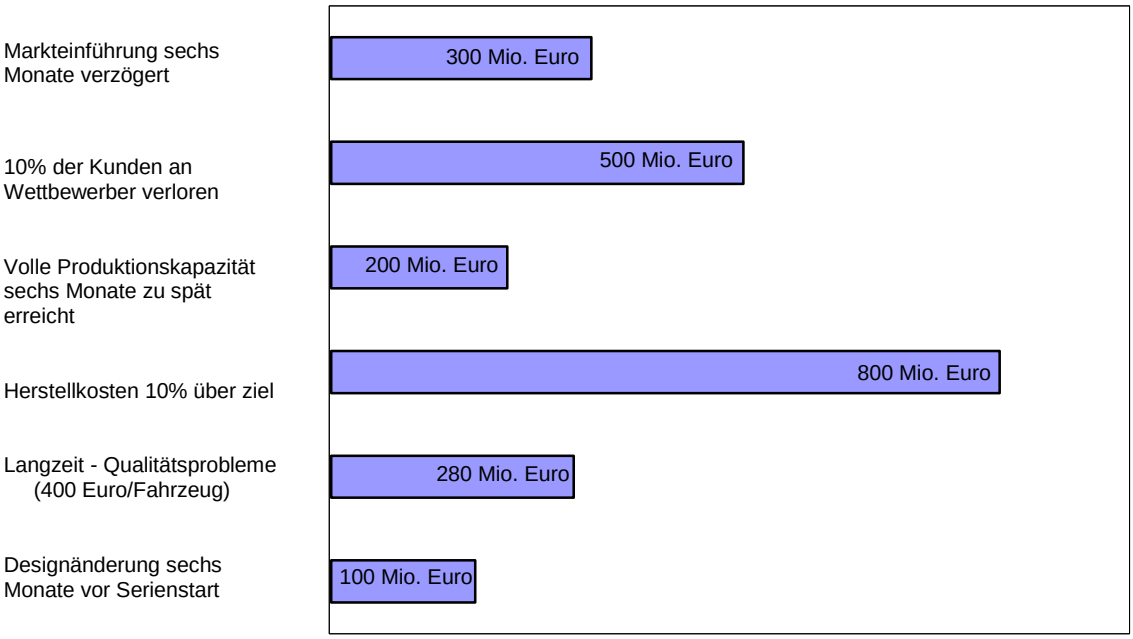


Bild 1-1: Entgangener Deckungsbeitrag bei einem Pkw der oberen Mittelklasse

Die Ungewißeit die Entwicklungsziele zu erreichen, sind die technischen Risiken, welche sich aus Qualitäts-, Kosten- und Zeitrisiken zusammensetzen. Die Entwicklung komplexer Serienprodukte ist charakterisiert durch eine lange Entwicklungszeit, Involvierung vieler Arbeitskräfte, die teilweise an verschiedenen Orten arbeiten, und eine hohe Komplexität von Produkten und Prozessen. Unter solchen Bedingungen sind viele Risiken vorhanden, die gesetzten Entwicklungsziele nicht zu erreichen.

Die Erreichbarkeit und Risiken der fundamentalen Ziele müssen regelmäßig und umfassend abgeschätzt werden, um den Fortschritt der Produktentwicklung im Zeitrahmen zu halten. Da die Risikominderung ein großes Budget erfordert, welches normalerweise für die Industrie nicht realisierbar ist, ist die vollständige

Vermeidung von Risiken nicht umsetzbar. Deshalb müssen Risikolevel existieren, die akzeptabel sind.

Akzeptable Risikolevel zu definieren ist Aufgabe des Managements, da dieses genau die Unternehmensziele und die zugehörigen Auswirkungen kennt, sollten diese nicht erreicht werden. Es ist die endgültige Verantwortung des Managements sicherzustellen, dass das Unternehmen diese Vorgaben und Ziele erreicht.

Technisches Risikomanagement spielt eine unerlässliche Rolle für den notwendigen Prozess, Risiken zu vermindern. In den letzten Jahren wurden enorme Anstrengungen unternommen, ein technisches Risikomanagement während der Komponentenentwicklung verschiedener komplexer Serienprodukte durchzuführen. Aus diesem Grund verfügt jedes große Industrieunternehmen über eine Datenbank, in der die Risiken von Fehlerszenarien -kombiniert mit Schätzungen des Einflusses auf das Budget, den Zeitverlust und die Risikowahrscheinlichkeiten verschiedener Hauptbestandteile komplexer Maschinen- beschrieben werden.

Die Auffassung, dass es gewisse Risikolevel gibt, die für jeden annehmbar sind, ist nur schwer zu akzeptieren. Es ist aber nicht möglich ohne solche grundlegenden Vorgehensweisen die notwendigen Richtlinien und Standards zu entwerfen. Aus diesem Grund gibt es einen großen Bedarf für eine Methodologie, welche die Kriterien für die Risikoakzeptanz beschreibt. Bisher gibt es keine veröffentlichten wissenschaftlichen Arbeiten, die eine Methodologie für akzeptable Risikokriterien beschreiben. Diese Dissertation leistet einen ersten Beitrag zum technischen Risikomanagement mit der Beantwortung der Frage: „Was sind akzeptable Risikokriterien?“. Sie bietet somit einen wichtigen Schritt in Richtung Herleitung einer Methodologie für einen akzeptablen Risikokriterienkatalog.

Ziel dieser Dissertation ist es, eine Methodologie für einen akzeptablen Risikokriterienkatalog zu entwickeln, welcher dem Management helfen kann, ein optimiertes Budget für Vermeidungsmaßnahmen festzulegen. Dieser Katalog trägt außerdem dazu bei, Produkte schneller auf den Markt zu bringen. Um dem Management auf einfache Weise diese Methodologie zur Verfügung zu stellen, wird zusätzlich eine benutzerfreundliche Software entwickelt.

Die weiteren Kapitel dieser Dissertation haben folgende Struktur:

In Kapitel 3 werden die fundamentalen Risiken und technischen Risikomanagementprozesse, die in der relevanten Literatur bekannt sind, erklärt. Die Herleitung der Methodologie für einen akzeptablen Risikokriterienkatalog ist in Kapitel 4 beschrieben.

Um die Methodologie der akzeptablen Risikokriterien zu benutzen, ist ein optimierter Vermeidungsmaßnahmenkatalog notwendig. In Kapitel 5 werden sowohl die mathematische Modellierung, als auch die Lösungsverfahren für die Herleitung eines solchen Vermeidungsmaßnahmenkatalogs beschrieben.

In Kapitel 6 wird das Softwaredesign kurz beschrieben. Eine ausführliche Beschreibung wird im Anhang B gegeben.

Kapitel 7 stellt sowohl die Simulationsdetails der akzeptablen Risikokriterien, als auch die Analyse der erzielten Resultate bereit.

Schlussfolgerungen und weitere mögliche Entwicklungen der Methodologie werden in Kapitel 8 beschrieben.

1.2 Zusammenfassung und Ausblick

Die Entwicklung komplexer Serienprodukte ist charakterisiert durch eine lange Entwicklungszeit, Involvierung vieler Arbeitskräfte, die teilweise an verschiedenen Orten arbeiten, und eine hohe Komplexität von Produkten und Prozessen. Unter solchen Bedingungen sind viele Risiken vorhanden, die dazu führen können, dass die gesetzten Entwicklungsziele nicht erreicht werden.

Es ist Aufgabe des Managements, akzeptable Risikolevel zu definieren. Nur das Management kennt genau die Unternehmensziele und die zugehörigen Auswirkungen, sollten diese nicht erreicht werden.

Die Risikominderung benötigt ein großes Budget, welches für Unternehmen nicht realisierbar ist. Es ist schwer zu entscheiden, welche Risiken, unter den Einschränkungen eines limitierten Budgets gemindert werden sollen, so dass die Entwicklungsziele des Produkts erreicht werden können. Aus diesem Grund hat die Antwort auf die Frage: „Was ist ein akzeptable Risikokriterienkatalog?“ größte Wichtigkeit für das Management von Herstellern komplexer Serienprodukte. Diese Dissertation leistet einen ersten Beitrag zum technischen Risikomanagement mit der Beantwortung dieser Frage. Ein erster Weg Richtung

Herleitung einer Methodologie eines Risikokriterienkataloges wurde präsentiert. Software für die Realisierung dieser Methodologie mit einem webbasierten, benutzerfreundlichen User Interface wurde entwickelt.

Die entwickelte Methodologie ist eine praktische Ergänzung zu den existierenden Herangehensweisen für das Risikomanagement in Projekten der Produktentwicklung. Es stellt ein Hilfsmittel für das Management bereit, um über das Minderungsbudget zu entscheiden, damit das Produkt schneller auf den Markt gebracht werden kann.

Da es keine veröffentlichten wissenschaftlichen Arbeiten zu diesem Thema gibt und diese Methodologie als erster Weg in Richtung eines akzeptablen Risikokriterienkatalogs unter ökonomischen Gesichtspunkten entwickelt wurde, gibt es viele Möglichkeiten der Erweiterung. Bei der Methodologieentwicklung sind die Abhängigkeiten zwischen den Minderungsmaßnahmen nicht im mathematischen Model berücksichtigt. Deshalb bestünde der nächste Schritt in der weiteren Entwicklung, das Model um abhängige Minderungsmaßnahmen zu erweitern.

Das Risiko wurde mit deterministischen Werten definiert. Eine weitere Entwicklung könnte die Nutzung des Risikowertes als ein stochastischer Wert sein, um eine robustere Methodologie zu entwickeln.

Die Methodologie bietet einen Budgetbereich mit Rücksicht auf maximale Risikosenkung an. Das Management kann aus diesem Bereich ein Minderungsbudget auswählen und bekommt die globalen Zielwerte. Die Idee für eine weitere Entwicklung in diese Richtung wäre, globale Zielwerte zu optimieren unter der Nebenbedingung eines optimalen Budgetbereichs. Bei diesem Schritt kann der entwickelte optimierte Minderungsmaßnahmenkatalog als Preprozessor genutzt werden und die globalen Ziele können mit Hilfe der Vektoroptimierung optimiert werden.

2 Introduction

The development of products is an essential factor of success for industrial enterprises that produce series products because of their long term effects and its economic importance. The strategic planning of products defines the time when the product should be in the market. Based on this framework development projects are started to realize the product strategy. During the project, the planned products should be developed ready for series production with the aid of knowledge, manpower, and financial resources obeying to reach the defined goals of quality, cost and time.

Increasing pressure of international competition, stagnant selling markets and shorter life cycle of products make the requirements highly challenging for industrial companies to be successful in the market. According to a research studies by McKinsey [McKinsey (2001)] in the automobile industry, which is considered to be a representative of complex series products, the variety of products will be doubled in five years whereas the product developing time will be reduced by one fourth with the same staff capacity. This research further demonstrates the impact of deviations from different objectives on the gross profit in the development of a car illustrated in figure 1.1.

Among the manufacturers of complex series products, the warranty and goodwill costs in recent years have greatly increased. For example, the Mercedes brand gave, warranty and goodwill costs, three times higher during the period 1998 to 2000 [Harnischfeger & Reinking (2001)]. The Mercedes estimated 1.7 billion Euro as warranty and goodwill costs in 2000 which is approximately equivalent to the development cost. With the extension of the warranty period of two years in Europe since January 2000, McKinsey [McKinsey (2001)] assumes that warranty and goodwill costs will increase by 30% to 150% depending on the manufacturer and the previously granted grace.

The failures that lead to warranty and goodwill costs are mainly in the product development phase. The product development, therefore, must always be in a shorter time period, customer oriented, cost effective and reliable. To meet the increasing demands of customers as well as the product quality, cost and time to market, companies must focus their efforts more than ever on the early stages of product development. Late corrections of the product features or modifications in a product already available in the market will raise a considerable amount of expenditures leading to significant economic disadvantages.

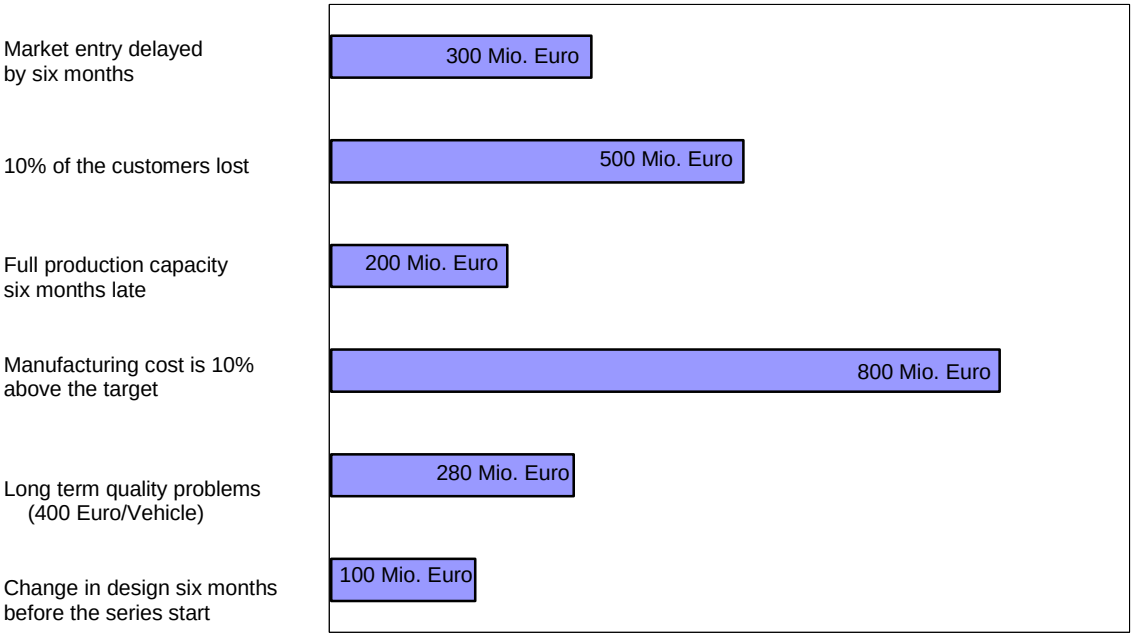


Figure 1.1: Loss of gross profit for a car of the upper middle class

The uncertainty to reach these development goals are the technical risks that are composed of quality, cost and time risks. The development of complex series products is characterized by a long development time, many involved persons partly working at different places, and a high complexity of products and processes. In such conditions there are many risks that prohibit to achieve the given development goals.

The risks and attainment of the fundamental goals must be regularly and widely assessed in order to keep the progress of product development with in time limits. Since mitigations of risks require a huge budget which is usually not possible for the industries so a zero risk is completely unachievable. Therefore, there must be some level of risks which should be agreed to be accepted at priori.

Defining the company's acceptable risk level falls to management because they intimately understand the company's business drivers and the corresponding impact if these business objectives are not met. It is management’s ultimate responsibility to ensure that the company meets these business objectives and goals.

Technical Risk Management plays a vital role for risks mitigation process. During the recent past, huge efforts have been made to perform Technical Risk Management during components development for different complex series products. Therefore a large database is available describing risk of failure scenarios combined with the estimations of technical as well as monetary impacts, time losses and risk probabilities for different major components of the complex machinery.

The notion that there exists some level of risk acceptable to everyone is a difficult idea to reconcile and yet, without such a baseline, how can it ever be possible to set guideline values and standards, given that life can never be risk free? Therefore, there is a great need for a methodology, describing criteria for the risk acceptance. However, we are unaware of any published work available on a methodology for Acceptable Risk Criteria.

This thesis makes an attempt to contribute to the Technical Risk Management by answering the question, “What are acceptable risk criteria?” and provides a methodology for deriving an Acceptable Risk Criteria Catalogue (ARCC). This will help the decision makers to decide for an optimized mitigation budget in order to bring a product faster in the market.

The plan of the thesis is as follows:

Chapter 3 is devoted to explain the fundamentals of risk and Technical Risk Management that already exist in the literature and practice. The derivation of ARCC methodology is discussed in *Chapter 4*. In order to use the ARCC methodology, an optimized mitigation measures catalogue is required. The mathematical modelling and solution strategies for the derivation of such a catalogue are derived in *Chapter 5*. *Chapter 6* briefly describes the software design for the ARCC methodology prototype system whereas the details of the developed software are provided in *Appendix B*. The simulation details of ARCC methodology as well as the analysis of results are given in *Chapter 7*. The conclusion along with further possible developments is discussed in *Chapter 8*.

3 Technical Risk Management

3.1 Introduction

Our environment has always been a risky place. Humans have always made risk based decisions, initially considering direct experience and later using historical data passed on to succeeding generations [Gould (1998)]. A systematic decision making consultancy group can be traced back to 3200 B.C. The group called, Asipu used to live in the Tigris-Euphrates valley and their primary role was to serve as consultants for risky, uncertain or difficult decisions. If a decision needed to be made concerning a forthcoming risky venture, one could consult with a member of the Asipu. The Asipu would identify the important dimensions of the problem, identify alternative actions and collect data on the likely outcomes. From their perspective, the best available data were signs from the gods. The Asipu would then create a ledger with a space for each alternative. If the signs were favorable, they would enter a plus in the space; if not, they would enter a minus. After the analysis was completed, the Asipu would recommend the most favorable alternative. However, unlike modern risk analysis, the Asipu of ancient Babylonia expressed their results with certainty, confidence and authority. Probability played no part in their analyses, since they were empowered to read the signs of the gods [Covello & Mumpower (1985)].

Engineering of today's systems is sophisticated and complex. Increasingly, systems are being engineered by bringing many separate systems together, that as a whole provide an overall capability, which is otherwise not possible. Pressures to meet cost, schedule and technical performance are the practical realities in engineering systems of today. Risks are present in large part of the system because expectations push what is technically or economically feasible. Managing risk is managing the inherent contention that exists within and across all these dimensions.

Risk is a driving consideration in decisions that determine how engineering systems are developed, produced and sustained. Critical to these decisions is an understanding of risk and how it affects the engineering of systems. The process of identifying, measuring and managing risks is known as Risk Management. Successfully engineering today's systems requires deliberate and continuous attention to the management of risk. Managing risk is an activity designed to

improve the chance that these systems will be completed on time, within cost and meet performance and capability objectives.

Technical Risk Management (TRM) is a process by which the engineering risks to a project are identified, ranked, and addressed so as to reduce the chances of project failure. Applied early, TRM can expose potentially crippling areas of risk in the engineering of systems. This provides management time to define and implement corrective strategies. Moreover, TRM can bring realism to technical and managerial decisions that define a system's overall engineering strategy.

More and more of today's high-tech industries are adopting TRM approaches as a means of improving the likelihood of success of their programs and also to prioritize their tasks and achieve optimum balancing of their technical resources. In recent years, many high-tech industries have begun to actively institute TRM as a part of major design programs. A recent Aerospace Risk Analysis Survey stated, "Increasingly, Government customers and Industry contractors seek better methods to identify and manage technical, schedule and cost risks [Black (2001)]." The survey goes on to document that 39% of industry representatives surveyed expect engineers to play the major role in TRM, whereas 33% place that responsibility on the cost estimators, 14% on management and 14% elsewhere. Aerospace is one industry where engineers are being expected to participate more and more in the management of technical risks. The medical device industry is another such industry. Ron Kaye and Jay Crowley [Kaye & Crowley (2000)] describe the use of TRM in that field, saying "Risk Management is a systematic application of policies, procedures and practices to the analysis, evaluation, and control of risks. It is a key component of quality management systems, and is a central requirement of the implementation of design controls in the Quality Systems Regulation.

Many U.S. Department of Defense programs have begun requiring that TRM procedures be defined in the proposal stage and that plans for managing technical risks be a part of every major review. Guidelines for estimating probability of occurrence and magnitude are published as part of military standard MIL-STD-882, System Safety Program Requirements, which states "A formal safety program that stresses early hazard identification and elimination or reduction of associated risk to a level acceptable to managing activity is the principal contribution to effective system safety [MIL-STD-H82H (1984)]".

Lewis Branscomb [Branscomb (2000)] expressed the situation well in the forward to a government-sponsored paper entitled Managing Technical Risks, when he

said "The risks associated with science-based commercial innovations are real and often hard to quantify and circumscribe. These risks contribute to business failures, but more importantly to underinvestment in the early stages of research and to opportunities foregone."

The benefits of TRM are so strong that any major engineering project would gain from having an active TRM program, regardless of the level of technology involved. The early identification, assessment, and mitigation of technical risks greatly diminish the chance of project failure and associated loss of revenue, reputation and jobs. Anything that helps avoid failure is a program benefit, regardless of whether it involves the design of jet engines or concrete blocks.

3.2 Risk and uncertainty

Philosophically view of the term "risk" is the fundamental experience that the man has been given his fate. General notion of the term risk is understood as a loss or a possibility of loss or the uncertainty of the occurrence or the absence of a certain success. From this understanding, different starting points for the definition of the risk emerge and the opinions of members of various disciplines diverge.

Basically, there is an agreement about the fact that a technical and a business point of view of the risk exists: The technical point of view of risk is also referred to as "pure risk" because only the negative impacts or disturbances caused by the loss risk will be seen. The business view of the risk is a possible difference between the initial target and the actual condition to be seen. Thus, both the positive and the negative deviations involved, hence the term "speculative risk" is used.

The different fields of science show different approaches and different definitions of notions easy to misunderstand. For many engineers, risk is simply another word for the probability of the occurrence of a defined event, while, for example, the insurance industry terms risk as money ‘at risk’.

Several authors in the literature of risk point out to the “problem” of terminology since the meanings of numerous concepts vary depending on what professional area the risk analyses are conducted [e.g., Covello & Merkhofer (1993)] . At the 1996 Annual Meeting of the Society for Risk Analysis, Kaplan [Kaplan (1997)] held a speech about the problems with the language in the risk analysis

community and concluded that “maybe it is better not to define risk. Let each author define it in his own way, only please each should explain clearly what way it is.”

Kaplan & Garrick [Kaplan & Garrick (1981)] argued that when one asks, “What is the risk?” One is really asking three questions:

1. What can happen?
2. How likely is it to happen?
3. If it does happen, what are the consequences?

The first question is promoting hazard (source of potential harm) scenario thinking. The second aims to state the likelihood of a certain scenario to occur. The third question relates to the undesired consequences linked with a specific scenario. This means risk is an event that, if it occurs, adversely affects the ability of a project to achieve its outcome objectives.

From this, a risk event has two aspects. The first is its occurrence probability. The second is its impact (or consequence) to an engineering system project. Therefore the risk event is a function of probability and impact and its general expression can be written as given by equation 3.1.

$$Risk = F(Probability, Impact). \tag{3.1}$$

The probability formalism is used in risk management because a risk is a potential event; probability is used to express the chance that event will occur. Often, the nature of these events is such that subjective measures of probability are used in the analysis instead of objectively derived measures.

A risk event’s consequence is typically expressed in terms of its impact on an engineering system’s cost, schedule and technical performance. However, there are often other important dimensions to consider. These include programmatic, social, political, and economic impacts. The consequence can be measures in many ways. Common methods include techniques from utility and value function theory. These formalisms enable risk events that impact a project in different types of units (e.g., Euro, months, processing speed) to be compared along normalized, dimensionless scales. This is especially necessary when risk events are rank-ordered or prioritized on the basis of their occurrence probabilities and impacts.

An event is uncertain if there is indefiniteness about its outcome. There is an important distinction between the terms risk and uncertainty. Risk is the chance of loss or injury. In situations that include favorable and unfavorable events, risk is the probability that an unfavorable event occurs. Uncertainty is the indefiniteness about the outcomes of these situations. The uncertainty is analyzed for the purpose of measuring risk. In an engineering system, the analysis might focus on measuring the risk of failing to achieve performance objectives, overrunning the budget cost, or delivering the system too late to meet user needs [Garvey(2000)].

3.3 Subjective and Objective Probabilities

Probability theory is the formal study of events whose outcomes are uncertain. Technical Risk Management aims to identify and manage those events whose outcomes are not certain. Its focus, in particular, is on events that, if they occur, have unwanted consequences to a project or program. The phrase "*if they occur*" means these events are probabilistic in nature. Thus understanding them in the context of probability concept is essential.

3.3.1 Equally Likely Interpretation

The set of all possible outcomes of an experiment is called the *sample space* denoted by Ω and an *event* is any subset of the sample space.

Now if a sample space Ω consists of a finite number of outcomes n, which are all equally likely to occur, then the probability of each simple event is 1/n. If an event A consists of m of these n outcomes, then the probability of event A is given by

$$P(A) = \frac{m}{n}.$$

Here it is assumed that the sample space consists of a finite number of outcomes and all outcomes are equally likely to occur. This is the view of the probability known as equally likely interpretation. However, what if the sample space is finite but the outcomes are not equally likely?

In such cases, probability might be measured in terms of how frequently a particular outcome occurs when the experiment is repeatedly performed under

identical conditions. This leads to a view of probability known as the frequency interpretation.

3.3.2 Frequency Interpretation

In this view, the probability of an event A is the limiting proportion of time the event occurs in a set of n repetitions of the experiment. In particular, this can be written as

$$P(A) = \lim_{n\to\infty} \frac{n(A)}{n},$$

Where, n(A) is the number of times event A occurs in an experiment repeated n times. In this sense, P(A) is the limiting frequency of event A. Probabilities measured by the frequency interpretation are referred to as *objective probabilities*.

In many circumstances it is appropriate to work with objective probabilities. However, there are limitations with this interpretation of probability. It restricts events to those that can be subject to repeated trials conducted under *identical conditions*. Furthermore, it is not clear how many trials of an experiment are needed to obtain an event's limiting frequency.

3.3.3 Axiomatic Definition

In 1933, the Russian mathematician A. N. Kolmogorov presented a definition of probability in terms of three axioms [Feller (1968)]. These axioms define probability in a way that encompasses the *equally likely and frequency interpretations* of probability. It is known as the axiomatic definition of probability. Under this definition, it is assumed for each event A, in the sample space Ω, there is a real number P(A) that denotes the probability of A. In accordance with Kolmogorov's axioms, a probability is simply a numerical measure that satisfies the following:

Axiom 1 $0 \le P(A) \le 1$ for any event A in Ω.

Axiom 2 $P(\Omega) = 1$.

Axiom 3 For any sequence of mutually exclusive events A_1, A_2, ….. defined on Ω, it follows that

$$P(\bigcup_{i=1}^{\infty} A_i) = \sum_{i=1}^{\infty} P(A_i).$$

3.3.4 Measure of Belief Interpretation

From the axiomatic view, probability needs only be a numerical measure satisfying the three axioms stated by Kolmogorov. Given this, it is possible for probability to reflect a "measure of belief" in an event's occurrence. For instance, an engineer might assign a probability of 0.60 to the event "the radar software for the Advanced Air Traffic Control System (AATCS) will not exceed 100 thousands delivered source instructions". We consider this event to be non-repeated. It is not practical or possible to build the AATCS n-times (and under identical conditions) to determine whether this probability is indeed 0.60. When an event such as this arises, its probability may be assigned. Probabilities assigned on the basis of personal judgment or measure of belief is known as *subjective probabilities*.

Subjective probabilities are the most common in engineering system projects. Such probabilities are typically assigned by expert technical judgment. The engineer's probability assessment of 0.60 is subjective probability. Ideally, subjective probabilities should be based on available evidence and previous experience with similar events. Subjective probabilities become suspect if they are premised on limited insights or no prior experience.

In many circumstances, the probability of an event is conditioned on knowing another event has taken place. Such a probability is known as a *conditional probability*. *Conditional probabilities* incorporate information about the occurrence of another event. The conditional probability of event *A* given event *B* has occurred is denoted by *P*(A|B). Furthermore, all probabilities are conditional in the broadest sense that one can always write:

$$P(A|\Omega) = P(A),$$

where *A* is an event (a subset) contained in the sample space Ω.
In a similar way, one can consider subjective or judgmental probabilities as conditional probabilities. The conditioning event (or events) may be experience

with the occurrence of events known to have a bearing on the occurrence probability of future event.

3.4 The Structure of Technical Risk Management

The Technical Risk Management (TRM) process consists of three phases: Risk Identification. Risk Assessment, and Risk Control. The figure 3.1 illustrates this structure.

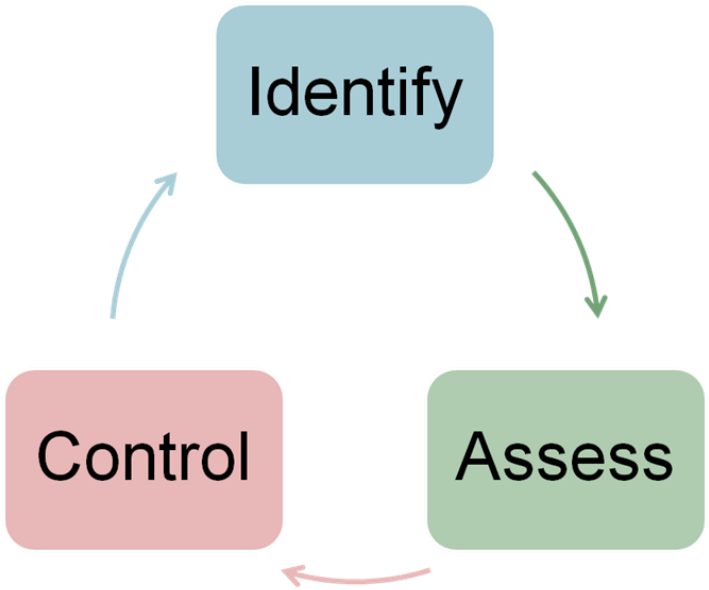


Figure 3.1: The structure of Technical Risk Management

Risk Identification is the critical first step of the TRM process. Its objective is the early and continuous identification of risks to the engineering system project. The Risk Identification phase forces the design team to take a serious look at the design with an eye toward possible failure modes that could hinder success of the project.

The Risk Assessment phase helps to determine which potential failure modes pose the greatest threat to the project, thus helping to prioritize the necessary analyses required to ensure success. In this step, an assessment is made of the impact each risk could have on the engineering system project. Typically, this includes how the event could impact cost, schedule or technical performance objectives. Impacts are not limited to only these criteria. Additional criteria such as political or economic consequences may also require consideration. An assessment is also made of the probability each risk event will occur. This often

involves the use of subjective probability assessment techniques, particularly if circumstances preclude a direct evaluation of the probability by objective methods (i.e., engineering analysis, modeling and simulation).

The overall set of identified risk events, their impact assessments and their occurrence probabilities are processed to derive a most-to-least-critical rank-order of identified risks. Decision analytic techniques such as utility theory, value function theory or ordinal ranking techniques are formalisms often used to derive a most-to-least-critical rank-order of identified risks.

A major purpose for prioritizing risks is to form a basis for allocating critical resources. These resources include the assignment of additional personnel and funding (if necessary) to focus on resolving risks deemed most critical to the engineering system project.

The Risk Control phase defines actions to avoid, or at least minimize, the project risk associated with the failure modes identified and ranked in the previous steps. This phase forces the design team into critical problem solving mode early in the program avoiding last-minute panics. Once the mitigation plans designed to manage, reduce risk to an acceptable level is implemented, it is continually monitored to assess its efficacy with the intent of revising the courses-of-action if needed.

3.4.1 Risk Identification

It is never too early in a design project to identify a potential risk. Risk Identification is the first and most important step in the risk management process, illustrated in figure 3.1. Risk Identification defines the set of future events that, if any occur, could have unwanted impacts on an engineering system project's cost, schedule, technical performance or any other evaluation criteria defined by the engineering team. The design team expected to perform its first Risk Identification soon after the initial concept is formulated.

The objective of the Risk Identification is to enumerate known risks and, in doing so, identify risks not immediately evident to the engineering team. As a process, Risk Identification is a continuous activity that operates regularly throughout the engineering phases of an evolving system.

Inputs to the Risk Identification process come from many sources. Some sources are particularly relevant to the pre/post-contract award phases of an engineering system project. The content in these sources and materials often provide the basis for a risk and justify why it is a potential concern to an engineering system project.

Risks can be identified and validated through systematic engineering analyses, such as modeling and simulation, as well as by the application of observation, judgment and experience. Risk Identification efforts include reviews of written materials and interviews with experts in specific areas of the project.

Risk Identification is best performed as a team. A team brainstorming session is a good way to start. Every member should try to step back and look at possible failure modes. At this time, all of these should be considered a valid risk to the project and no effort should be made to determine relative importance or to define design solutions to eliminate potential risks. When risks are being identified, it is essential that subject matter experts from all the engineering disciplines participate. This includes staff from the project's cost schedule team, logistic/supportability team, and the production/manufacturing team.

Table A.1 presents a summary of common, but significant, risk areas that can negatively affect an engineering system project. Table A.2 present a set of guidelines for identifying risks associated with an engineering system project. These guidelines are excerpted from the United States Department of Defense *Risk Management Guide*, June 2003 [Bahnmaier (2003)]. Both tables are presented in the Appendix A.

3.4.1.1 Writing a Risk Statement

Each identified risk should be expressed formally. A "best practice" for expressing an identified risk is to write it in a form known as the *risk statement*. A risk statement aims to provide clarity and descriptive information about the identified risk so that a reasoned and defensible assessment can be made on the risk's occurrence probability and its areas of impact.

A protocol for writing a risk statement is the *Condition-If-Then* construct [Garvey(2005)]. The *Condition* reflects what is known today. It is the root cause of the identified risk event. Thus, the *Condition* is an event that has occurred, is presently occurring, or will occur with certainty. Risk events are future events that may occur *because* of the *Condition* present. This protocol applies in all risk

management processes designed for any systems engineering environment. It is a recognition that a risk event, by its nature, a probabilistic event and one that, if it occurs, has unwanted consequences.

Consider the following two events. Define the *Condition* as event *B* and the *If* as event *A* (the risk event):

B = {Current test plans are focused on the components of the subsystem and not on the subsystem as a whole}

A = {Subsystem will not be fully tested when integrated into the system for full-up system-level testing}

The risk event is the *Condition-If* part of the construct; specifically,

Risk Event : {*Subsystem will not be fully tested when integrated into the system for full-up system-level testing, because current test plans are focused on the components of the subsystem and not on the subsystem as a whole.*}

From this, one can see the *Condition-If* part of the risk statement construct is equivalent to a probability event; formally, one can write

$$0 < P(A|B) = \alpha < 1,$$

where α is the probability of occurrence of risk event *A* given the conditioning event *B* (the root cause event) has occurred.

The *Then* part of the construct contains the additional information; that is, information on the risk's consequences. An example of a risk statement is shown in figure 3.2.

3.4.2 Risk Assessment

Forcing the design team to take a hard look at possible failure modes is a positive step in and of itself. But how is the team to decide which ones need to be addressed first? Industrial Technical Risk Management programs recognize the need for optimum prioritization and allocation of resources. They do this by creation of a Risk Assessment or scoring system. For each risk identified in the first step, the team should consider its likelihood and its consequence. Likelihood

is the probability that the identified failure might actually occur. These probabilities may ultimately come from probabilistic calculations but in the beginning will probably come from educated estimates based on the amount of preliminary design work done at any point in time.

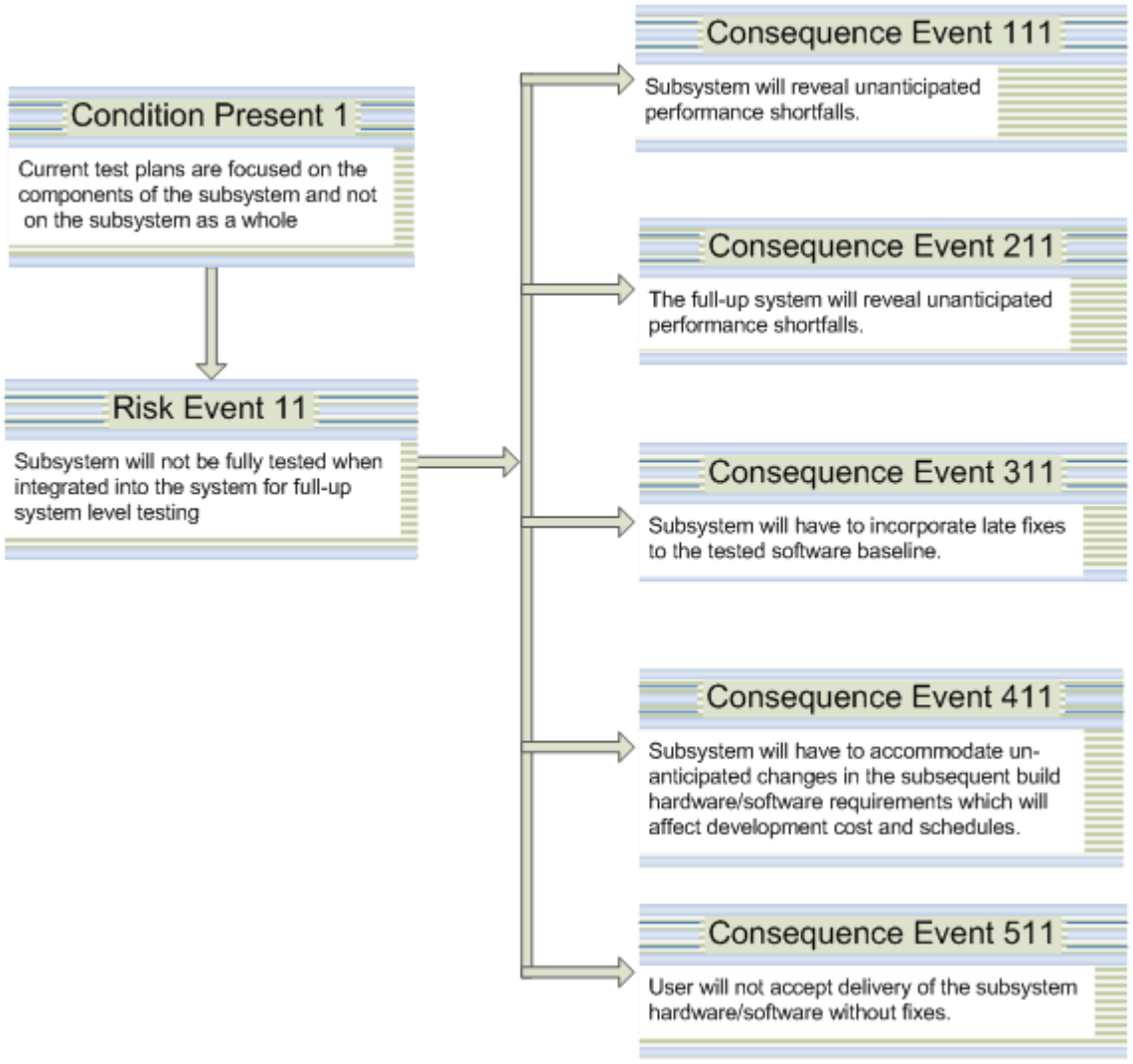


Figure 3.2: An illustration of the Condition-If-Then construct

In their mathematical treatment of probabilistic risk, Kumamoto, Hiromitsu and Ernest Henley [Kumamoto & Henley (1996)] prefer that each risk should be expressed as an objective probability, percentage, or density per action or unit time, or during a specified time interval. But they added, unfortunately, the likelihood is not always exact; probability, percentage, frequency, and ratios may be based on subjective evaluation. Verbal probabilities such as rare, possible,

plausible, and frequent are also used. In fact, at the beginning stage of the design process, exact calculations are simply not possible, so subjective assessments must be made by the design team.

Next the impact or consequence should be assessed. Consequences are even harder to relate to hard numbers and verbal and ambiguous terms such as catastrophic, severe and minor may be used instead of quantitative measures. They also point out that consequences definitely need to be tailored to the particular project because significance depends on intangibles such as cultural attributes, ethics, emotion, reconciliation, media coverage, context, or litigability, as well as the fact that people estimate the outcome significance differently when population risk is involved in addition to individual risk. Obviously, the consequences of a failure in a rocket launch are different than in a sewer design. Nonetheless, there are consequences to all programs which mean that the risk assessment needs to be tailored to each individual program. Program consequences tend to fall into the following three types:

1. Budget Impact - How big is the monetary impact if the failure occurs? Obviously, a failure that results in the loss of a rocket and pay load has huge financial implications. But the failure of a sewer system that causes significant private property damage plus repair and replacement costs can just as easily bankrupt a small design and construction firm, which makes it catastrophic in its own right. Thus, exactly what constitutes a budget impact of low versus moderate versus high consequence must be tailored to each individual product.
2. Schedule Impact - Again, schedule impact varies from project to project. On some programs, a delay of three months may be considered "high impact." On others, a three-week delay may have a huge detrimental impact on the company, especially if late penalties are written into the contract with the customer.
3. Technical Impact - Technical impact involves the amount of redesign effort required. This would include the necessary redirection of effort and resources to perform a redesign if the failure occurs.

These probabilities and consequences can now be reduced to a Risk Score via a scoring matrix. Once again, this matrix can be tailored to specific projects, but in general, risks with both high probability and high consequence receive the highest risk score. The scoring matrix does two things. First it quantifies the risks in a way that allows them to be prioritized. Second, it allows them to be categorized into three simple and easily comprehensible levels. These levels

(High, Medium, and Low) are usually color coded (Red, Yellow, and Green) in industry as a means of quickly and clearly highlighting which risks are the biggest concern. To the engineers, this might seem an over simplification of a complex issue, but as Jarrett [Jarrett (2000)] explains, the corporate executive is the member of the organization who deals ultimately with risk decisions, and even if it was possible to develop complex representations of risk accurately, it is difficult for the executive to deal with them. Instead, the executive is able to deal with a few scenarios and possible cases, and only with three general levels of conceptual risk associated with them: High Risk, Medium Risk, and Low Risk.

3.4.3 Risk Control

Risk control is a widely exercise handling strategy by the project's management. Risk control actively engages strategies to reduce or mitigate risk. It monitors and manages risk in a manner that reduces its occurrence probability and/or consequences on the project. The risk mitigation plan, in many ways, the most useful and challenging part of TRM. The design team must now use their knowledge, skills and resources to plan and schedule a series of risk mitigation steps that will reduce the high risk items to low risk scores. In industry, this is the step that forces the team to plan a course of action that reduces the risk to some acceptable level.

4 Acceptable Risk Criteria Methodology

4.1 Introduction

Complex systems possess characteristics that will cause them to fail. Many studies cite how engineers architect systems to counter single point of failure in complex systems but have difficulty with component interactions. For example, the Mars Polar Lander (MPL) was destroyed due to the unpredictable nature of component interactions [Perrow (1984)].

Failure is inevitable and inherent. Management techniques can only manage how failure is likely or unlikely to occur. Engineering is a human endeavor and because of this one cannot achieve a risk free technology as we become more dependent on ever more complex technologies.

To regulate a technology in a logically defensible way, one must consider all its consequences, i.e., both risks and benefits. To be able to set an enterprise wide acceptable risk level, a few points need to be investigated and understood. A company must understand: its federal and state legal requirements; its regulatory requirements; its business drivers and objectives; and it must carry out a risk and threat analysis. The result of these findings is then used to define the company's acceptable risk level.

Perhaps the most widely sought quantity in the management of technologies is the acceptable level of risk. For designers and operators, having a well-defined acceptable level of risk would provide a clear target for managing their technology. For regulators, identifying an acceptable level of risk would mean resolving value issues at the time when standards are set, allowing an agency's technical staff to monitor compliance mechanically.

Risk needs to be understood across a continuum from those events that

- present the potential for damage to the business strategy,
- compose the uncertainties implicit in the execution of that strategy,
- must be embraced in order to achieve the goals of the organization.

Expanding the definition of risk management in this manner has the potential to engage the entire organization as it requires collaboration between business and operational managers to gather and assess the risks that are not only to be

avoided but also be embraced in the service of achieving the goals of the organization.

Technical Risk Management (TRM) involves thinking about the happenings that need to go right as well as what can go wrong [Bernstein (1996)]. In the recent past, huge efforts were made to perform Technical Risk Management during components development for different complex series products. Therefore a large database is available describing risk of failure scenarios combined with the estimations of technical as well as monetary impacts, time losses and risk probabilities for different major components of the complex machinery.

TRM procedures have been developed through classical Failure Mode and Effects Analysis (FMEA). The FMEA technique dates back to the United States military procedures MIL-P-1629 [MIL-P-1629 (1949)]. The theoretical basis of FMEA was firmly established at the times of the birth of NASA and the onset for the Apollo program. The primary push came during the 1960s, while developing the means to land a man on the moon and of his safely return to earth [Bilstein (1980)].

FMEA is used during the design stage with an aim to avoid future failures. Later it is used for process control, before and during ongoing operation of the process. FMEA can provide an analytical approach, when dealing with potential failure modes and their associated causes. When considering possible failures in a design – like safety, cost, performance, quality and reliability – an engineer can get a lot of information about how to alter the development/manufacturing process in order to avoid these failures [Fries (1992)]. FMEA provides an easy tool to determine which risk has the greatest concern and therefore an action is needed to prevent a problem before it arises. The development of these specifications ensures that the product will meet the defined requirements.

Structure of FMEA

Bongiorno [Bongiorno (2001)] provides an overview as well as the basic mechanics of the FMEA technique. The typical structure of FMEA is shown in figure 4.1.

The first step of FMEA procedure is to detect a failure mode. In the second step, each effect is given a Severity Number (S) from 1 (no danger) to 10 (critical). These numbers help an engineer to prioritize the failure modes and their effects. In the third step, a failure mode is given an Occurrence ranking (O), again 1–10. Each combination from the second and the third step receives a detection

number (D) from 1–10 as a fourth step. The assigned detection number measures the risk that the failure will escape detection. A high detection number indicates that the chances of escaping detection of failure are high or, in other words, that the chances of detection of failure are low.

After ranking the severity, occurrence and detectability, the Risk Priority Numbers (RPN) can be easily calculated by multiplying these three numbers, i.e. RPN = S * O * D. These RPN do not play an important role in the choice of a mitigation action against failure modes. They are more threshold values in the evaluation of these actions.

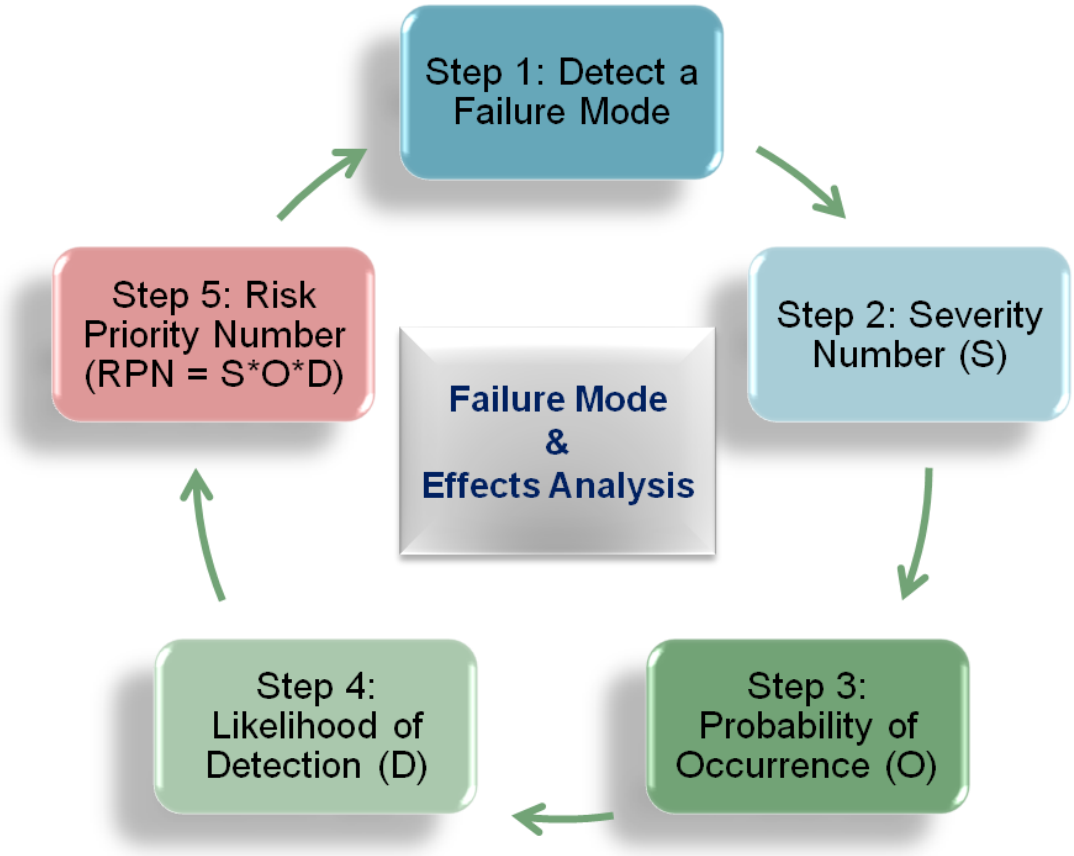


Figure 4.1: Structure of FMEA

The purpose of the FMEA is to take actions to eliminate or reduce failures, starting with the highest-priority ones. It may be used to evaluate risk management priorities for mitigating known threat vulnerabilities. FMEA helps to select remedial actions that reduce cumulative impacts of life-cycle consequences (risks) from a system failure (fault). Currently, FMEA technique is

an integral part of ISO-9000 and QS-9000 quality certification levels [Steven (2004)].
TRM based on FMEA approach certainly proved to be successful in Apollo mission [Levine (1982)]. In this mission, the role of RPN was only to prioritize the risks but each risk had to be mitigated whatever budget was required. For this mission, the target was “failure is not an option” and nearly unlimited budget was available to achieve this mission.

TRM based on FMEA approach is now extensively used in a variety of industries producing complex series products. The RPN provide the prioritization of risks reduction but, of course, it is not possible to reduce all the risks like Apollo mission due to a limited budget available to TRM in these industries. This is a major gap between the TRM during “Apollo Era” and in “current industrial structure”.

In order to fill this gap, there must be some criteria for the optimum utilization of the limited mitigation budget that helps TRM to set a threshold for the acceptance of some risks. However, the open available literature does not provide any methodology for such an acceptance criteria.

The notion that there is some level of risk that everyone will find acceptable is a difficult idea to reconcile. Defining the company’s acceptable risk level falls to management because they intimately understand the company’s business drivers and the corresponding impact if these business objectives are not met. Senior managers are charged with growing the enterprise and generating profits for their shareholders. Activities that do not contribute to that goal are generally viewed as a cost of business, certainly necessary, but not central to the myriad of tasks essential for growth. Growth is driven by the execution of strategy and that execution requires an understanding of the risks that must be undertaken to be successful.

In order to answer the question, “What are acceptable risk criteria?” this chapter provides a methodology for the derivation of an acceptable risk criteria catalogue.

4.2 Risk Criteria Catalogue (RCC) Numbers

Engineering concept of acceptable risk is to find a catalogue of those failure probabilities of components which are always less than or equal to some specified values. Engineers can calculate the failure probability of a component

but to find an acceptable value of such failure probabilities is almost impossible. For example, if failure probability of a component is 80% which can be reduced to 60%, 50%, 30% and so on with some engineering efforts but there is no idea where to stop this reduction. It is a great need to have some specified value where this reduction is quite enough because a huge amount of budget is required for reduction of such failure probabilities. Here comes the concept of an Acceptable Risk Criteria Catalogue (ARCC). In order to derive an ARCC, in an economics point of view, one needs first to understand the Risk Criteria Catalogue (RCC) numbers.

In order to have better understanding, consider an example shown in the table 4.1.

MAJOR COMPONENT	
SUB – COMPONENT 1	
CC 123456 – SUB - COMPONENT 11	POF 1.79×10^{-8}
CC 123457 – SUB - COMPONENT 12	POF 1.45×10^{-5}
CC 123458 – SUB - COMPONENT 13	POF 2.78×10^{-3}
CC 123459 – SUB - COMPONENT 14	POF 1.62×10^{-6}
…….	….

Table 4.1: Major Components Structure – POF

Here “CC” stands for Component Code and “POF” means “Probability of Failure”.

The Probability of Failures can then be transformed into the probability categories to get RCC numbers on the basis of repeated or one time event risks. The tables 4.2 & 4.3 give an overview for the definition of these probability categories respectively.

Definition of Probability Categories (repeated event risks)				
Category		**Frequency**		**Value**
		Events per operating	**Illustration (5000 operating hours per year)**	
5	frequent	>1E-03	one part has more than seven failures per year	1.0E-03
4	probable	1E-03 to 1E-4	one part has one failure per year	1.0E-04
3.5	occ- probable			1.0E-04
3	occasional	1E-4 to 1E-5	one part has one failure within four years	1.0E-05
2.5	rem- occ			1.0E-06
2	remote	1E-5 to 1E-7	one part has one failure within one hundred and fifty years. 100 parts have one failure within 1.5 years	1.0E-06
1.5	improbable- rem			1.0E-07
1	improbable	1E-7 to 1E-9	one part has one failure within fifteen thousand years. 10000 parts have one failure within 1.5 years	1.0E-08
0	incredible	<1E-9	one part has less than one failure within two hundred thousand years. 100000 parts have one failure within 2 years	1.0E-09

Table 4.2: Definition of Probability Categories (repeated event risks)

Definition of Probability Categories (one time risks)			
Category			**Value**
		Illustration	
5	frequent	frequently occurs	95%
4	probable	repeatedly occurs	90%
3.5	occ- probable		78%
3	occasional	could repeatedly occur	65%
2.5	rem- occ		50%
2	remote	could occasionally occur during the durability	35%
1.5	improbable- rem		23%
1	improbable	occurrence is improbable but possible	10%
0	incredible	extremely improbable occurrence	5%

Table 4.3: Definition of Probability Categories (one time risks)

4.2.1 Classical Approach - Measurements (using experiments)

In the classical and well established Availability & Reliability Analysis, the RCC numbers are used to determine the availability and reliability of machines or systems. Using a block diagram of the machine or system, all relevant risk scenarios/failure paths are analyzed and the failure probability of the machine or system is calculated for each path by using the RCC numbers. Based on these

calculations, the overall availability and reliability of the machine or system is then derived [Misra (1992)]. An example of system block diagram is illustrated in the figure 4.2.

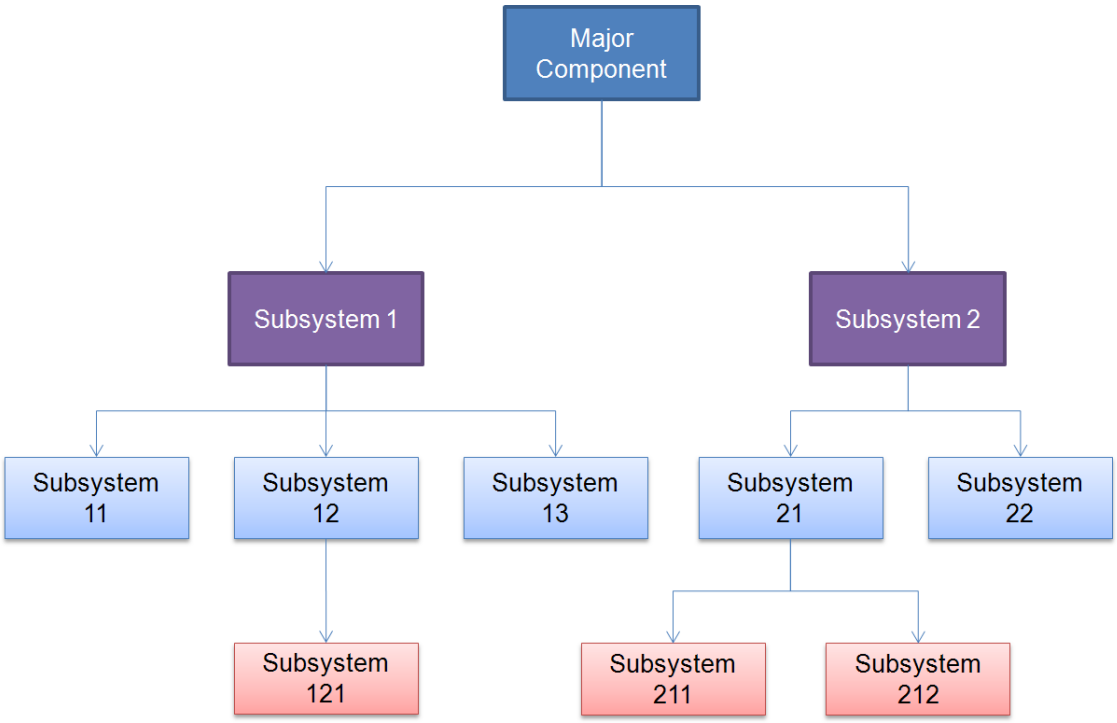


Figure 4.2: Example of a System Block diagram

Often it is tried to derive RCC numbers by using the classical Availability & Reliability Analysis. The overall availability & reliability of the machine/system is fixed and by using the relevant risk scenarios/failure paths, a backward calculation is tried to find the required RCC numbers to fulfill the overall availability & reliability. From a mathematical point of view, this leads to an optimization task. Often this optimization task cannot be achieved due to lot of uncertainties and complexity of the machine/system.

4.2.2 Ideal Approach - Predictions (using modeling and simulation)

As an ideal approach to derive a RCC, imagine that a company would have a simulator for the probabilistic modelling and simulation of a whole machine in operation where one can run each component with different failure probabilities to observe the impact. This means that a fully 3-D mechanical, chemical, thermo and aero dynamical modelling and simulation of the system is required. With the

help of such a simulator, these RCC numbers can then be used to predict life time, availability and reliability of the machine.

The problem is that at present companies do not have such a powerful simulator yet and it is almost impossible to have it in the near future. It requires a lot of computing efforts and may take several years to have complete knowledge of all such failure probabilities catalogue.

4.3 Challenging Market Requirements

The companies permanently have to face the challenging market requirements in order to launch their products in the global market. Consider the example of an automobile which is a representative of complex series products. If a company is going to bring a car of a given class for the year 20yy in the global market, it will first analyse the market in order to get the market requirements. Suppose the analysis shows that market requires the following features for this car:

- Engine power greater than120 kW,
- Fuel consumption less than 8 L / 100 km,
- Pollution caused by the car less than 0.5 PPM ,
- Fuel tank should be large enough so that car can travel more than 1000 km with one filling,
- No recall for some corrective measures once it is in the market, etc.

On the basis of such an analysis, the company can now transform the market requirements into the development goals/Global Features (GFs) of the product. These GFs, with respect to the above example of a car, could be Efficiency, Emissivity, Power, Reliability, Availability, Capacity, etc.

In general, the GFs for a product can be defined as:

- Global Feature 1 (GF1),
- Global Feature 2 (GF2),
- Global Feature 3 (GF3),
- Global Feature 4 (GF4),
- …,
- … .

These GFs do not have exact values but a range of values which give more choices to a company for setting its target. In the above example of a car, the Emissivity value less than 0.5 PPM provides an Emissivity range of, e.g., 0.01 PPM to 0.5 PPM.
It is necessary for a company to meet such GFs values for a product to be successful in the global market. In order to meet these GFs, a company must, therefore, define its ideal target values for the GFs of the product, i.e.

- ideal target value of Global Feature 1 ($GF1_{iT}$),
- ideal target value of Global Feature 2 ($GF2_{iT}$),
- ideal target value of Global Feature 3 ($GF3_{iT}$),
- ideal target value of Global Feature 4 ($GF4_{iT}$),
- …,
- ….

Here the subscript ”iT” stands for the ideal target value of the GF.

The ideal target values are important to bring the product successfully in the market. However, in order to achieve these ideal target values, the company must define its internal target values which must be better than the ideal targets values. There can be some GFs values whose internal target values must be higher than the ideal target values while the others can have internal target values less than ideal target values. For example, the internal target values of Reliability must be higher than the ideal target values while the internal target values of the Emissivity must be set lower than the ideal target values. Therefore, as in the example of a car given above, the Emissivity values 0.3 PPM to 0.5 PPM can be set as an ideal target values for the development of a car while the values less than 0.3 PPM can be set as an internal target for the development team to be sure to achieve ideal target values.

However, this should be kept in mind that the company is not the only supplier of such a complex series products in the global market. Now what if a competitor develops same product in less development time with values $GF1 < GF1_{iT}$, $GF2 < GF2_{iT}$, $GF3 < GF3_{iT}$, $GF4 > GF4_{iT}$, $GF5 > GF5_{iT}$, etc. but with an unbeatable price and develops the market first? This fact raises the question, “What would be the acceptable values of these GFs to bring the product faster into the market”?

The answer to this question is not easy and one needs a criterion for minimum acceptable target values of the GFs.

4.3.1 Acceptable Risk Criteria Catalogue (ARCC) Numbers

To understand the definition of ARCC, the example presented in table 4.1 can now be presented in table 4.4.

MAJOR COMPONENT	
SUB – COMPONENT 1	
CC 123456 – SUB - COMPONENT 11	**a**POF≤1.25×10^{-9}
CC 123457 – SUB - COMPONENT 12	**a**POF≤1.01×10^{-7}
CC 123458 – SUB - COMPONENT 13	**a**POF≤1.46×10^{-5}
CC 123459 – SUB - COMPONENT 14	**a**POF≤1.03×10^{-7}
…….	….

Table 4.4: Major Components Structure – aPOF

Here "CC" stands for Component Code and "**a**POF" means "**a**cceptable Probability of Failure".

The ARCC numbers for each machine component design define criteria which at least have to be fulfilled by the components to obtain the acceptable value of Global Features.

4.4 Derivation of an Acceptable Risk Criteria Catalogue

In the last years, huge efforts were made to perform Technical Risk Management during components development for different complex machines of different classes. Therefore a large database is available describing risk of failure scenarios combined with the estimations of technical as well as monetary impacts, time losses and risk probabilities for different major components of the complex machinery.

Typical structure of TRM Risk Items:
The typical structure of the Technical Risk Management risk items list is defined by a Risk Breakdown Structure (RBS) consisting of all relevant machine components, time schedule, suppliers' lists, etc. Every item of the RBS is a headline for all related risk items. In principle, the content of each risk item is as given in the table 4.5.

			Before Mitigation			After Mitigation			Mitigation Measures	
Risk Breakdown Structure	**Risk ID**	**Risk Description**	**Prob.** (%)	**Imp.** (€)	**Risk** (€)	**Prob.** (%)	**Imp.** (€)	**Risk** (€)	**Cost** (€)	**Description**
1. MAJOR COMPONENT										
SUB – COMPONENT 1										
CC 123456 – SUB - COMPONENT 11										
	…	… …	…	…	…	…	…	…	…	…
CC 123457 – SUB - COMPONENT 12										
	…	… …	…	…	…	…	…	…	…	…
CC 123458 – SUB - COMPONENT 13										
	10- 1.1	Sub-Component 13 breaks leading to a loss in GF1 by 0.X%	X1	A1	X1 * A1	Y1	B1	Y1 * B1	C1	Measure M1
	11- 1.1	Not optimal design of Sub-component 13 leads to loss in GF4 by 0.0Y%	X2	A2	X2 * A2	Y2	B2	Y2 * B2	C2	Measure M2
	12- 1.1 …	… … … …	… …	… …	… …	… …	… …	… …	… …	… …
CC 123459 - SUB - COMPONENT 14										
	… …	… … … …	… …	… …	… …	… …	… …	… …	… …	… …

Table 4.5: Risk Breakdown Structure

In the hypothetical example given in table 4.5, an Acceptable Risk Criteria (ARC) is equal to an Acceptable Probability of Failure (aPOF) for the *sub-component 13* can be derived as follows:

1. If risk 10-1.1 (X1 % *A1 €) is acceptable, then aPOF of the *sub-component 13* is less than or equal to X1 %.

2. If risk 10-1.1 is not acceptable, the mitigation measure M1 must be realized and aPOF of the *sub-component 13* is then less than or equal to Y1 %.

CC 123458 – SUB - COMPONENT 13										
	10- 1.1	Sub-Component 13 breaks leading to a loss in GF1 by 0.X%	X1	A1	X1 * A1	Y1	B1	Y1 * B1	C1	Measure M1
	11- 1.1	Not optimal design of Sub-Scomponent 13 leads to loss in GF4 by 0.0Y%	X2	A2	X2 * A2	Y2	B2	Y2 * B2	C2	Measure M2

3. If risk 11-1.1 (X2 % * A2 €) is not acceptable, then mitigation measure M2 (e.g. a re-design) must be realized. This could affect the risk evaluation of risk 10-1.1. In this case, steps 1 and 2 must be repeated to derive aPOF of the *sub-component 13* after new evaluation of risk 10-1.1.

This means that question of an ARCC is then question of an acceptable Technical Risk Management catalogue defining the minimum required mitigation measures catalogue. To answer that, the focus must be laid on the Global Features of the product to be manufactured. In general, these Global Features are:

- Global Feature 1,
- Global Feature 2,
- Global Feature 3,
- Global Feature 4,
- … .,
- … ..

These Global Features are also addressed in the RBS by the Technical Risk Management:

CC 123458 – SUB - COMPONENT 13										
	10- 1.1	Sub-Component 13 breaks leading to a loss in GF1 by 0.X%	X1	A1	X1 * A1	Y1	B1	Y1 * B1	C1	Measure M1
	11- 1.1	Not optimal design of Sub- component 13 leads to loss in GF3 by 0.0Y%	X2	A2	X2 * A2	Y2	B2	Y2 * B2	C2	Measure M2

The ideal target values of these GFs are already explained in section 4.3. Now if one starts with these ideal target values of the GFs, an ideal target vector for a machine of a given class for the year 20yy with required GFs can be defined.

$$\vec{V}_{iT} = \begin{pmatrix} \text{Global Feature 1} \\ \text{Global Feature 2} \\ \text{Global Feature 3} \\ \text{Global Feature 4} \\ \ldots \end{pmatrix} = \begin{pmatrix} GF1_{iT} \\ GF2_{iT} \\ GF3_{iT} \\ GF4_{iT} \\ \ldots \end{pmatrix}.$$

In order to derive minimum acceptable target values of these GFs, the right question, in an economics point of view, is: “What would be an acceptable target vector to reduce the development time and cost for shorten time-to-market (i.e. to be first in the market)”? This acceptable target vector can be defined as:

$$\vec{V}_{aT} = \begin{pmatrix} \text{accept. Global Feature1} \\ \text{accept. Global Feature2} \\ \text{accept. Global Feature3} \\ \text{accept. Global Feature4} \\ \ldots \end{pmatrix} = \begin{pmatrix} GF1_{aT} \le GF1_{iT} \\ GF2_{aT} \le GF2_{iT} \\ GF3_{aT} \le GF3_{iT} \\ GF4_{aT} \ge GF4_{iT} \\ \ldots \end{pmatrix}.$$

Now the market may accept product if the values of these GFs values are less than the ideal target values with some additional incentives offered by the product manufacturer but there are still some limiting values for these GFs. If a company brings a product even faster in the market but the values of GFs are below that limit, no customer will purchase that product. Considering these unacceptable values of the GFs, a non-acceptable target vector can be defined as:

$$\vec{V}_{naT} = \begin{pmatrix} \text{not accept. Global Feature1} \\ \text{not accept. Global Feature2} \\ \text{not accept. Global Feature3} \\ \text{not accept. Global Feature4} \\ \ldots \end{pmatrix} = \begin{pmatrix} GF1_{naT} < GF1_{aT} \le GF1_{iT} \\ GF2_{naT} < GF2_{aT} \le GF2_{iT} \\ GF3_{naT} < GF3_{aT} \le GF3_{iT} \\ GF4_{naT} > GF4_{aT} \ge GF4_{iT} \\ \ldots \end{pmatrix}.$$

For better understanding of the acceptable and not acceptable target vector values, consider the following two examples:

Suppose a GF, say Reliability, of a product which has an ideal target value of greater than 97%. Then there is likelihood of acceptance of the value of this GF even if it is less than or equal to 97% but greater than 92%, under some additional incentives corresponding to these values of the GF. However, a value less than 92% of this GF may not be acceptable and the product could be out of the market.

Similarly, consider another example of a GF, say Emissivity, of a product having an ideal target value of less than 0.5 PPM. Now a value greater than or equal to 0.5 PPM but less than 0.9 PPM could be acceptable for a customer under some incentives offered by the manufacturer corresponding to these values of the GF. However, a value greater than 0.9 PPM of this GF may not be acceptable and the product could be out of the market.

These two examples also give an understanding about the GFs inequalities $GF1_{aT} \leq GF1_{iT}$ and $GF4_{aT} \geq GF4_{iT}$ defined in acceptable target vector.

Since the major goal of Technical Risk Management is to ensure that the finally obtained target vector is as close as possible to the ideal target vector by keeping development time and costs as low as possible. An Acceptable Risk Criteria Catalogue (ARCC) can be derived by combining the *classical approaches* to derive Risk Criteria Catalogues to develop complex machinery with ideal target vectors and the *classical Technical Risk Management* (TRM) to control and manage the complex machinery development projects.

4.5 Methodology for the Derivation of ARCC

This section describes the details of the methodology developed as a first possible way towards the derivation of an ARCC.

4.5.1 Global Features Matrix

It is important for a company to first identify its Global Features (GFs) and then define a range of the values for these Global Features in order to bring the product successfully in the market. The internal target values of these GFs must

always be set higher or equal to the values promised to the customer. The threshold of these values has great importance which brings the product out of the market. This means no customer will go for this product if one or some of the values of the GFs are outside this threshold.
The range of the values of the GFs is divided into four zones and a GFs matrix is developed which is starting point of the ARCC methodology. The four zones are marked with colors Blue, Green, Yellow, and Red in this matrix. This GFs matrix is the key for the methodology.

The values of the GFs in Blue zone are the internal ideal target values which a company has to set for the development of its new product.

The starting point of the Green zone values is the ideal target value for the corresponding GF which has to be achieved in order to sell the product successfully in the global market. Usually industries try to do everything in order to reach this target.

The starting point of the Red zone is the value which is not acceptable at any cost. It is almost impossible to sell the product if a GF value enters in this zone and, as a result, product will be out of market.

The Yellow zone lies between the Green and Red zones. If the value of a GF is in Yellow zone then a penalty cost must be paid to the customer as per contract. The penalty costs can be seen as additional manpower cost, costs due to time delays and some other relevant costs in case a GF value lies in the Yellow zone. However, the yellow zone plays an important role for the decision makers. Although a penalty cost has to be paid if a value of a GF falls in this zone but this gives the idea of bringing the product faster in the market saving development and production costs. The possible structure of such a GFs matrix is presented in figure 4.3.

GF1	$GF1_{iiT}$	…	…	$GF1_{iT}$	…	$GF1_{naT}$	…	…
GF2	$GF2_{iiT}$	…	$GF2_{iT}$	…	…	…	$GF2_{naT}$	…
GF3	$GF3_{iiT}$	$GF3_{iT}$	…	…	…	$GF3_{naT}$	…	…
GF4	$GF4_{iiT}$	$GF4_{iT}$	…	…	…	…	…	$GF4_{naT}$
…	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…

Figure 4.3: Structure of a Global Features Matrix

For example, suppose a company defines the value 65% for a GF, say GF2, of the machine as an internal ideal target for the design team. The marketing department of the company promises a value of 63% to the customer for this GF. The market analysis shows that a value, say, between 59% and 63% would also be acceptable for the customer if company is paying a penalty cost (say X€ per 0.5% difference) in case the values of GF2 fall in this range. However, the analysis also shows that no customer will purchase this machine and therefore the product is out of market if the value of the GF2 is less than 59%.

In this example, the GF2 value greater than or equal to 65% lies in the Blue zone of the GFs matrix. The value range 63% - 64.9% lies in the Green zone and 63% is the starting value of the ideal target value. The values of the GF2 less than or equal to 59% fall in the Red zone and the values range 59.1% - 62.9% is in the Yellow zone. A decision maker can play in this range of the GF2 values in order to bring the product faster in the market as well as save development and production costs.

The research and development tries to bring all GFs values into Blue/Green zones and this, of course, requires a huge budget. However, the limited mitigation budget tends to move the GFs values into Yellow/Red zone. This is an optimization task which needs to be solved in order to get an acceptable target vector. The constraint in this optimization is that no GF value should fall in the Red zone.

These four zones of the GFs matrix defines the values of the internal ideal target vector (starting values of the GFs in Blue zone), ideal target vector (starting values of the GFs in Green zone), acceptable target vector (GFs values in Yellow zone) and not acceptable target vector (starting values of the GFs in Red tone) given as:

$$\vec{V}_{iiT} = \begin{pmatrix} GF1_{iiT} \\ GF2_{iiT} \\ GF3_{iiT} \\ GF4_{iiT} \\ \dots \end{pmatrix}, \quad \vec{V}_{iT} = \begin{pmatrix} GF_{iT} \\ GF2_{iT} \\ GF3_{iT} \\ GF4_{iT} \\ \dots \end{pmatrix}, \quad \vec{V}_{aT} = \begin{pmatrix} GF1_{aT} \le GF1_{iT} \\ GF2_{aT} \le GF2_{iT} \\ GF3_{aT} \le GF3_{iT} \\ GF4_{aT} \ge GF4_{iT} \\ \dots \end{pmatrix},$$

$$\vec{V}_{naT} = \begin{pmatrix} GF1_{naT} < GF1_{aT} \leq GF1_{iT} \\ GF2_{naT} < GF2_{aT} \leq GF2_{iT} \\ GF3_{naT} < GF3_{aT} \leq GF3_{iT} \\ GF4_{naT} > GF4_{aT} \geq GF4_{iT} \\ ... \end{pmatrix}.$$

4.5.2 Risks Clustering

The typical structure of Technical Risk Management presented in table 4.5 explains the effect on GFs values due to different risks. A risk may affect all or some of the GFs values. This fact brings the idea of breaking down a risk into different sub risks with respect to the GFs values. Therefore, each risk in the Risk Breakdown Structure items list can be written as:

$$R_i = \{R_{i,1}, R_{i,2}, R_{i,3}, ...\},$$

where, $R_{i,1}$ is the i^{th} risk affecting GF1, $R_{i,2}$ is the i^{th} risk effecting GF2 and so on.

For example, if Risk 1 affects GF1 and GF3 only then it can be written as:

$$R_1 = \{R_{1,1}, R_{1,3}\}.$$

This means that all those components of different risks which affect one particular GF can be grouped together and form a cluster with respect to this particular GF. In this way, the complete Technical Risk Management risk items list can be clustered on the basis of defined GFs. This cluster of the risks, under consideration that risks are independent of each other, can be written as:

$$R_{c,j} = \sum_{i=1}^{n} R_{i,j},$$

where, $R_{c,j}$ is the cluster of all those risks which are affecting the j^{th} GF.

For example, if risk 1, risk 5 and risk 6 are affecting GF2 then risk cluster with respect to GF2 can be written as:

$$R_{c,2} = R_{1,2} + R_{5,2} + R_{6,2}.$$

In this way, a risk cluster vector containing all such clusters can be defined as

$$\vec{R}_c = \begin{pmatrix} R_{c,1} \\ R_{c,2} \\ R_{c,3} \\ R_{c,4} \\ \ldots \end{pmatrix}.$$

This risks cluster vector is important for some further calculations in the ARCC methodology.

4.5.3 Possible Target Vector

The next step of the methodology is to calculate the effect of all risks on GFs values under the consideration that no mitigation measure has been applied and a possible target vector can be defined. The risks cluster vector helps to calculate the initial values of such a possible target vector

$$\vec{V}_{pT} = \begin{pmatrix} \text{possible GF1 value} \\ \text{possible GF2 value} \\ \text{possible GF3 value} \\ \text{possible GF4 value} \\ \ldots \end{pmatrix} = \begin{pmatrix} GF1_{pT} \\ GF2_{pT} \\ GF3_{pT} \\ GF4_{pT} \\ \ldots \end{pmatrix}.$$

This vector can be obtained by summing up the risks cluster vector and the internal ideal target vector, i.e.

$$\vec{V}_{pT} = \vec{V}_{iiT} + \vec{R}_c.$$

Since no mitigation measure has been applied so far, it is expected that at least one vector value will fall into the Red/yellow zone of the GFs matrix. The possible target vector gives the worst case scenario of the values of GFs because it is considered that no mitigation measures are applied.

Consider the example of GF2 given in sub-section 4.5.1. Suppose that there are three risks which affect the GF2 as follows:

Risks	**Effect on GF 2 value**
R_1	-0.7%
R_2	-1.9%
R_3	-0.2%
Total effect	**-2.8%**

The negative sign shows the decrease in the value of GF2 due to risks.

By adding this total effect to the internal ideal target value 65% results a reduced value 62.2% of the GF2. This value lies in the Yellow zone of the GFs matrix.

4.5.4 Best Possible Target Vector

After observing the worst case scenario of the values of GFs in the form of possible target vector, now calculate the best case scenario and define a best possible target vector under the assumption that all risk mitigation measures are applied, i.e.

$$\vec{V}_{bpT} = \begin{pmatrix} \text{Bets possible GF1 value} \\ \text{Best possible GF2 value} \\ \text{Best possible GF3 value} \\ \text{Best possible GF4 value} \\ \dots \end{pmatrix} = \begin{pmatrix} GF1_{bpT} \\ GF2_{bpT} \\ GF3_{bpT} \\ GF4_{bpT} \\ \dots \end{pmatrix}.$$

This vector can be calculated by summing up the internal ideal target vector into mitigated risks cluster vector

$$\vec{V}_{bpT} = \vec{V}_{iiT} + \vec{R}_{mc},$$

where, $\vec{R}_{mc}$ represents the mitigated risks cluster vector.

If the Technical Risk Management is sufficient and the technology to be used is mature, the best possible target vector values will fall into the Blue/Green zone of the GFs matrix.

Since the best possible target vector is calculated under the assumption that all mitigation measures have been applied, the maximum mitigation budget $B_{max\ mit}$ needed to perform all identified risk mitigation measures can now be determined by adding costs of all the mitigation measures.

4.5.5 Optimized Possible Target Vector

In general, it is not possible to implement all the mitigation measures in the catalogue because of the limited budget available to the Technical Risk Management. Therefore, one needs to determine a minimum required mitigation measures catalogue which brings the maximum risk reduction under the constraint of the budget. Such an optimal mitigation measures catalogue can be obtained in the following way:

1. Find the mitigation budget B_{mit} from the maximum budget $B_{max\ mit}$ obtained in section 4.5.4 such that

   $$0 < B_{mit} \leq B_{max\ mit},\ (B_{mit} = n * \Delta B,\ n = 1, 2, 3 \ldots),$$

   where ΔB is the minimum starting value of the budget.
   For example, if $B_{max\ mit}$ =10,000€ then ΔB can be taken as 1000€.

2. For n = 1 to k : Determine an optimal mitigation measures catalogue (detailed explanation and algorithm for finding an optimal mitigation measures catalogue will be discussed in *Chapter 5*) for the resulting budget. In contrast to the worst and the best case scenarios explained in previous two sub-sections 4.5.3 and 4.5.4 respectively, there will now be two risks cluster vectors. One of the cluster vectors contains all those risks which are mitigated and the second contains the remaining unmitigated risks. Now summing up the values of these two cluster vectors into the internal ideal target vector, the values of an optimized possible target vector can be calculated. In this case, all vector values will fall into the Blue/Green/Yellow zone of the GFs matrix.

   The case n = k is defined as:

$$\vec{V}_{opT}(k) = \begin{pmatrix} GF1_{naT} < GF1_{opT}(k) \\ GF2_{naT} < GF2_{opT}(k) \\ GF3_{naT} < GF3_{opT}(k) \\ GF4_{naT} > GF4_{opT}(k) \\ \ldots \end{pmatrix}.$$

If the values of the GFs lie in the yellow zone then a penalty cost (PC) should be paid to customer as per contract. This penalty cost can be calculated for each GF from the optimized possible target vector. The following example explains the calculation of this penalty cost:

Suppose an ideal target value of a GF is greater than 63% and a penalty cost, say 1000€ per 0.5% difference in the GF value, must be paid to the customer if the GF value lies from 59% to 63%. Now suppose that the optimized target vector gives a value 61% of this GF. This means the difference to the ideal target value is 2% and hence a penalty cost to be paid against this GF is 4000€.

4.5.6 Acceptable Risk Criteria Catalogue

On the basis of the penalty cost (PC) value calculated for the optimized possible target vector, an acceptable risk criteria catalogue can be derived as follows:

1. If PC ≤ ($B_{max\ mit} - B_{mit}$), an acceptable state is reached and the ARCC for that machine can be derived from the final respective risk probabilities from the Risk Breakdown Structure items list.

2. If PC > ($B_{max\ mit} - B_{mit}$) then the steps 2 in *sub-section 4.5.5* must be repeated by further increasing n until the condition C ≤ ($B_{max\ mit} - B_{mit}$) is satisfied.

This first possible way to derive an ARCC only works if all risks are independent, the Technical Risk Management is sufficient and the technology to be used is mature. This means that values of the best possible target vector will fall into the Blue/Green zone of the GFs matrix if all mitigation measures are performed.

In case of the development of a next generation machine, one has to face the possibility that the Technical Risk Management is sufficient but the technology to be used is not mature. This means that the values of the best possible target vector will not fall (completely) into the Blue/Green zone of the GFs matrix if all mitigation measures are performed. In such a case, the probabilities of relevant risks after mitigation measures must be adjusted (lowered) as long as the values of the best possible target vector fall into the Blue/Green zone. This gives a first estimation of the new ARCC relevant for this next generation machine.

4.6 Summary

The overview of the methodology developed as a first possible way towards the derivation of ARCC is presented in figure 4.4.

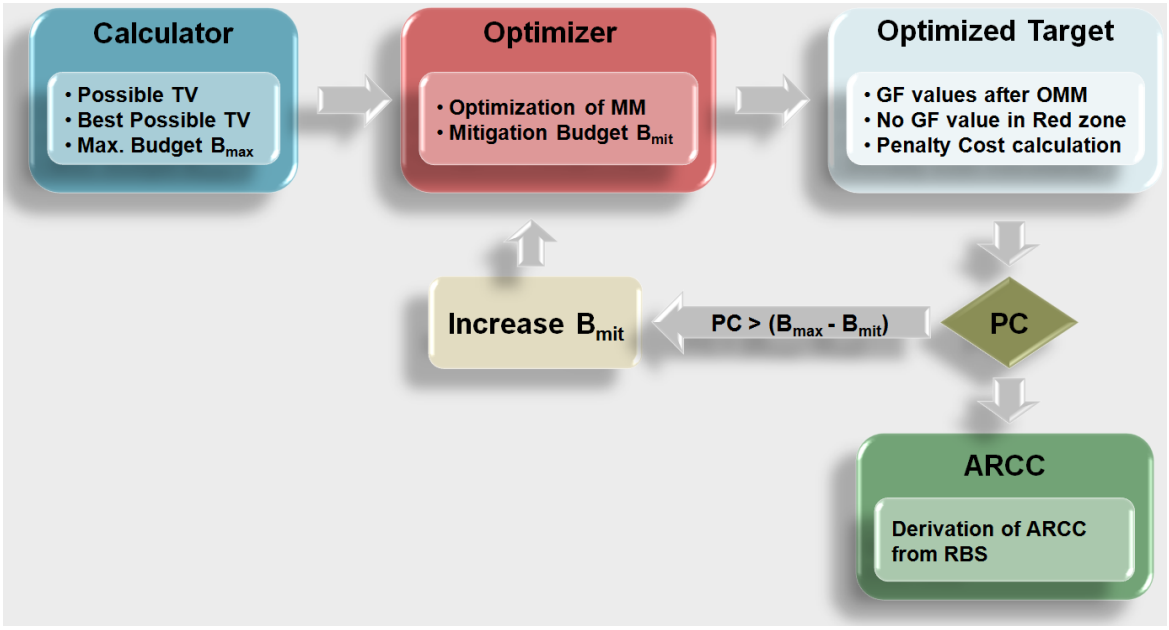


Figure 4.4: ARCC Methodology

After defining a Global Features matrix, the methodology works in four steps namely:

1. Calculator
2. Optimizer (Mitigation Measures Catalogue)
3. Optimized Target
4. ARCC

The first step “Calculator” has the internal ideal target vector as an input and calculates the possible and best possible target vectors as well as the maximum budget required to realize all the mitigation measures.

The second step “Optimizer” stores the optimized mitigation measures budget as well as the optimized mitigation measures catalogue.

The third step “Optimized Target” calculates the target vector after the realization of the optimized mitigation measures and Penalty Cost (PC).

In the step four “ARCC”, Acceptable Risk Criteria Catalogue can be derived from Risk Breakdown Structure if the penalty cost is less than the difference between maximum budget and optimized budget. However, if Penalty cost is greater than the difference of the budgets then the process goes back to the second step “Optimizer”.

5 Optimized Mitigation Measures Catalogue

5.1 Problem Statement

The tasks of Technical Risk Management (TRM) cover the recognition of the risks as well as their prevention. In order to prevent the risks, several mitigation measures are required. These mitigation measures can either reduce the probability of occurrence or the impact or both.

In order to decide which mitigation measures should be implemented, the costs for these mitigation measures are important considerations. Because of the limited budget available to the TRM, it is not possible to implement all the mitigation measures in the catalogue. The choice for the mitigation measures must be in relation to lowest possible cost while maintaining the best possible risk reduction. Therefore, determination of an optimum mitigation measures catalogue has great importance for TRM. This optimized catalogue is then used to implement the methodology for the derivation of an acceptable risk criteria catalogue presented in *Chapter 4.*

It is already mentioned in *Chapter 3* that risk can be considered as a function of its occurrence probability and its impact to an engineering system project. This relationship is represented by equation 3.1. What functional form is appropriate for this relationship? There could be many answers to this question.

Stewart and Melchers [Stewart & Melchers (1997)] state that risk more and more defines the probability of an undesirable event occurrence and the possibility of damage, and can be evaluated as the product of probability and value of consequences, where consequences might be evaluated in terms of money.

This “product rule” is a popular formulation in the risk management community and can be written by the equation

$$R = P \cdot I, \tag{5.1.1}$$

where R is the risk, P is the probability of occurrence, and I is the monetary impact (consequence) due to occurrence of this risk.

In order to reduce risk R to a residual risk R_M, various mitigation measures are required to be implemented. The set M contains all mitigation measures. The indices of the mitigation measure m with respect to the risk R_i is represented as m_{j_i}. All those mitigation measures which are needed to reduce risk R_i correspond to the set M_i. Therefore, each risk R_i can be reduced to a residual risk $R_{M;i}$ and the risk reduction ΔR_i can then be calculated as:

$$\Delta R_i = R_i - R_{M;i}. \tag{5.1.2}$$

The cost for the implementation of mitigation measure m_j is considered as c_j. Due to cost consideration, $m_j \in \mu$ are mitigation measures which can be implemented and $m_j \in \lambda$ are those which can not be implemented This implies two different subsets of the mitigation measures $\mu \subseteq M$ and $\lambda \subseteq M$ such that $\mu \cup \lambda = M$, $\mu \cap \lambda = \varphi$.

5.2 Mitigation Measures Types

A risk R_i can be reduced to ΔR_i by implementing different types of the mitigation measures m_{j_i}. These different mitigation measures types are discussed below in detail:

1. The first possibility is that a risk needs only one mitigation measure for its reduction. This means that there are as many risks as mitigation measures. For each mitigation measure m_j, a weighting $\hat{m}_j$ can be determined as:

   $$\hat{m}_j = \frac{c_j - \Delta R_i}{c_j}. \tag{5.2.1}$$

   The risks will be strongly reduced by implementing a mitigation measure with a smaller weighting.

2. The second possibility could be that a mitigation measure m_{j_i} can reduce many risks R_l , $l = 1,2,...,k$ at the same time. To get the best effect of such a mitigation measure, all the corresponding risk reductions ΔR_l, $\forall l$ can be summed up together. This reduces multi-mitigations type to a single mitigation type 1, i.e., for each risk there will be only one mitigation measure required. The weighting of the mitigation in this case can be determined as:

$$\hat{m}_j = \frac{c_j - \sum_l \Delta R_l}{c_j}. \qquad (5.2.2)$$

3. The third possibility could be that several mitigation measures are required in order to reduce one single risk. This further leads to different cases:

   a. If mitigation measures are independent of each other and risk R_i can be divided into sub risks R_{ij} so that for each sub risk one mitigation measure m_{j_i} can be implemented then this type of the mitigation measure can be reduced again to type 1. The risk reduction ΔR_i can then be obtained by adding all reduced sub risks $\Delta R_i = \sum_j \Delta R_{ij}$. The weighting of the mitigation measures, in this case, can be calculated by

   $$\hat{m}_{j_i} = \frac{c_{j_i} - \Delta R_{ij}}{c_{j_i}}. \qquad (5.2.3)$$

   b. If mitigation measures are dependent or a risk can not be divided into sub risks with respect to each mitigation measure then the third type of the mitigation measures can not be reduced to the type 1.

This thesis considers only mitigation measures of type 1 or those which can be reduced to type 1.

5.3 Optimization Model

The problem of finding an optimized mitigation measures catalogue is a decision problem and therefore an optimization model is required. The problems with the decision of yes/no are considered as the integer programming problem.

The following model [Jensen & Bard (2003)] states the general integer programming problem:

Constraint: $f_i(\underline{x}) \le 0,\ i = 1,\dots,m$
$x_i \in Z^+,\quad i = 1,\dots,n \qquad (5.3.1)$

Objective function: $F(\underline{x}) \to \min$

The model (5.3.1) consists of m constraints and an objective function. The objective function can be converted from minimization to maximization by multiplying it with -1. The variables x_i are positive integers. In case, some of the variables are restricted to be integers and some not then the problem leads to mixed integer programming problem. The case where the integer variables are restricted to be 0 or 1 comes up surprising often. Such problems are called binary integer programming problems.

The optimization model to be determined is used for the selection of those mitigation measures which can reduce the risks of a product in a best possible way. In this decision problem, there are only two possibilities: either a mitigation measure is fully implemented or not. The mitigation measures can, therefore, take only the values 0 or 1 which leads to binary integer programming problem.

There exist several models for the binary integer programming problems. Some well known models are *the* Knapsack Problem, the Partition and Set Packing Problem, and the Travelling Salesman Problem [Wolsey (1999)].

The knapsack problem often arises in resource allocation with financial constraints and is analogous to the problem of selecting optimized mitigations for risk reduction.

5.3.1 Knapsack Problem

The Knapsack problem is an example of a combinatorial problem which seeks for a best solution from among many other solutions. It has been studied for a long time in operations research, management science and computer science. It offers many practical applications in many areas.

The family of all knapsack Problems require a subset of some given items to be chosen such that the corresponding profit sum is maximized without exceeding the capacity of the Knapsack(s). Different types of Knapsack Problems occur depending on the distribution of the items and knapsacks: In the 0-1 Knapsack Problem each item may be chosen at most once, while in the Bounded Knapsack Problem one has a bounded amount of each item type. The Multiple-choice knapsack Problem occurs when the items should be chosen from the disjoint classes and, if several Knapsacks are to be filled simultaneously, one gets the Multiple Knapsack Problem. The most general form is the Multi-constrained

Knapsack Problem, which basically is a general Integer Programming Problem with positive coefficients.

All Knapsack Problems belong to the family of *NP – hard* problems, meaning that it is very unlikely that one ever can devise polynomial algorithms for these problems. But despite the exponential worst-case solution times of all Knapsack algorithms, several large scaled instances may be solved to optimality in fractions of a second. This surprising result is the outcome of several decades of research which have exposed the special structural properties of Knapsack Problems that makes the problems relatively easy to solve [Kellerer (2005)].

The 0-1 Knapsack Problem is the problem of choosing a subset of n items such that the corresponding profit sum is maximized without having the weight sum to exceed the capacity c. This can be formulated as the following maximization problem:

$$\text{Objective function:} \quad \sum_{i=1}^{n} p_i \cdot x_i \rightarrow \max$$

$$\text{Constraint:} \quad \sum_{i=1}^{n} w_i \cdot x_i \leq c \qquad (5.3.2)$$

$$x_i \in \{0,1\},\ i = 1,2,\ldots,n$$

5.3.2 Mathematical Modeling of the Problem

To model the problem of an optimized mitigation measures catalogue into 0-1 Knapsack problem, following should be considered:

1. All mitigation measures must be binary. This means that a mitigation measure m_i can either be fully implemented ($m_i = 1$) or not implemented at all ($m_i = 0$).

2. The implementation of each mitigation measures m_i requires a mitigation cost c_i. The sum of all implemented mitigation costs must not exceed the maximum mitigation budget. This makes the constraint analogy to Knapsack problem, i.e.,

$$\sum_{i=1}^{n} c_i \cdot m_i \leq B.$$

3. The implementation of a mitigation measures m_i reduces the risk R_i to ΔR_i. The objective of the mitigation measures catalogue is to select those mitigations for which the risk reduction ΔR_i is maximum. This makes the analogy to the objective function of the Knapsack problem, i.e.,

$$\sum_{i=1}^{n} \Delta R_i \cdot m_i \rightarrow max$$

Therefore, the mathematical model for the optimized mitigation measures catalogue is as follows:

$$\text{Objective function:} \quad \sum_{i=1}^{n} \Delta R_i \cdot m_i \rightarrow max$$

$$\text{Constraint:} \quad \sum_{i=1}^{n} c_i \cdot m_i \leq B \qquad (5.3.3)$$

$$m_i \in \{0,1\},\ i = 1,2,...,n$$

The dependencies between the mitigation measures are not considered in this model and only mitigation measures of type 1 or those which reduces to type 1 are in the scope of this thesis.

5.4 Solution Strategy

In order to find an optimized mitigation measure catalogue, the model (5.3.3) needs to be solved. This can be done by using the methodologies for solving 0-1 Knapsack Problem .

The Knapsack Problem is NP-complete and as such an exact solution for a large input is practically impossible to obtain [Martello (1990)]. Various approaches to solve 0-1 Knapsack problem include Brute Force, Dynamic Programming, Memory functions, Branch and Bound, Greedy Algorithm, and Genetic Algorithm. Three of them; Brute Force, Dynamic Programming and the Genetic Algorithm has been implemented for this work. The Brute Force and Dynamic Programming details are excerpted from.

5.4.1 Brute Force Algorithm

Brute Force is a straight forward approach to solve a problem, usually directly based on the problem's statement and definitions of the concept involved. If there are n items to choose from, then there will be 2^n possible combinations of items for the Knapsack. An item is either chosen or not chosen. A bit string of 0's and 1's is generated which is of length n. If the i^{th} symbol of a bit string is 0, then the i^{th} item is not chosen and if it is 1 then i^{th} item is chosen.

Detail algorithm is presented as follows:

ALGORITHM BruteForce (Weights [1 … N], Values [1 … N], A [1 … N])

//Finds the best possible combination of items for the Knapsack

//Input: Array Weights contains the weights of all items
Array Values contains the values of all items
Array A initialized with 0s; it is used to generate the bit strings

//Output: Best possible combination of items in the Knapsack bestChoice [1 … N]

```
for  i=1 to 2^n  do

        j=n

        tempWeight = 0

        tempValue = 0

        while (A[j] != 0 and j > 0)

                A[j] = 0
                 j = j-1

        A[j] = 1

        for k = 1 to n do

                if (A[k] = 1) then
```

```
            tempWeight = tempWeight + Weights[k]

            tempValue = tempValue + Values[k]

        if ((tempValue > bestValue) AND (tempWeight ≤ Capacity)) then

            bestValue = tempValue

            bestWeight = tempWeight

    bestChoice = A
return bestChoice
```

The complexity of the Brute Force algorithm is $O(n2^n)$. Since the complexity of this algorithm grows exponentially, it can only be used for small instances of the Knapsack Problem [Hristakeva (2005)]..

5.4.2 Dynamic Programming

Dynamic Programming is a technique for solving problems whose solutions satisfy recurrence relations with overlapping sub problems. Dynamic Programming solves each of the smaller sub problems only once and records the results in a table rather than solving overlapping sub problems over and over again. The table is then used to obtain a solution to the original problem. The classical Dynamic Programming approach works bottom-up.

To design a Dynamic Programming algorithm for the 0-1 Knapsack Problem, it first needs to derive a recurrence relation that expresses a solution to an instance of the Knapsack Problem in terms of solutions to its smaller instances.

Consider an instance of the problem defined by the first *i* items, $1 \leq i \leq N$, with:

weights $w_1, \ldots, w_i$,
values $v_1, \ldots, v_i$,
and
Knapsack capacity j, $1 \leq j \leq$ Capacity.

Let Table[i, j] be the optimal solution of this instance i.e., the value of the most valuable subsets of the first i items that fit into the Knapsack capacity of j. All the

subsets of the first i items that fit into the Knapsack of capacity j can be divided into two groups: the subsets that include the i^{th} item and those which do not include the i^{th} item. This leads to following recurrence:

If $j < w_i$ then

Table[i, j] = table[i-1,j]

Else

Table[i, j] = maximum {Table[i-1, j] AND v_i + Table[i-1, j-w_i]}

The goal is to find the Table[N, Capacity], i.e., the maximum value of a subset of the Knapsack.

The two boundary conditions for the Knapsack are:

- The Knapsack has no value when no item is included in it (i.e., i = 0).

  Table[0, j] = 0 for j ≥ 0

- The Knapsack has no value when its capacity is zero (i.e., j = 0), because no items can be included in it.

  Table[i, 0] = 0 for i ≥ 0

ALGORITHM Dynamic Programming
(Weights [1 … N], Values [1 … N], Table [0 … N, 0 … Capacity])

//Input: Array Weights contains the weights of all items
Array Values contains the values of all items
Array Table is initialized with 0s; it is used to store the results from the dynamic programming algorithm.

//Output: The last value of array Table (Table [N, Capacity]) contains the optimal solution of the problem for the given Capacity.

For i = 0 to N do

For j = 0 to Capacity

```
        If j < Weight [i]        then
              Table [i, j] = Table [i-1, j]

        Else
              Table[i, j] = maximum {Table[i-1, j]
                                          AND
                                    Values[i] + Table[i-1, j-Weight[i]}
```

Return Table[N, Capacity]

The following algorithm finds which items are included in the optimal solution:

Start at position Table[N, Capacity]

While the remaining capacity is greater than 0 do

If Table[N, Capacity] = Table[N-1, Capacity] then

Item N has not been included in the optimal solution

Else

Item N has been included in the optimal solution

Process item N

Move one row up to N-1

Move to column Capacity – weight (N)

The complexity of Dynamic Programming is $O(N \cdot \text{Capacity})$. In terms of memory, Dynamic Programming requires a two dimensional array with rows equal to the number of items and columns equal to the capacity of Knapsack [Hristakeva (2005)]..

5.4.3 Genetic Algorithm

Genetic Algorithm (GA) is a search algorithm based on the mechanics of natural selection and natural genetics. Thomas Back said in [Back (1997)] that the most

significant advantage of using evolutionary search such as GA lies in the gain of flexibility and adaptability to the task at hand, in combination with robust performance and global search characteristics. In GA each individual is evaluated by fitness function. Some individuals produce more children than others do according to their fitness. By this mechanism, individuals that have chromosomes with better fitness have more chance of leaving their genes. This leads to better average performance of whole population as generations proceed. GA obtains a near optimized or optimized solution by repeating this process. To implement this process, many factors should be considered such as the representation scheme of chromosomes, the mating strategy, the size of population, and the design of the operators as mutation and/or recombination.

Genetic Algorithms take advantage of natural selection to cull weaker solutions from a population. By allowing successful solutions to produce the next generation they are rewarded, while weaker solutions are less likely to pass their unsuccessful “genes” to the next generation.

All Genetic Algorithms begin with a set of solutions (represented by chromosomes) called population. By taking a population of possible solutions and evaluating them against the best possible solution, the fittest individuals of the population are determined. After evaluation, combining and mutating, the members of the current generation generate a new population. This new generation is then evaluated and the process is repeated until an optimal solution is found [Mitchell (1998)].

In the following, major steps of Genetic Algorithm are explained in detail:

1. The first step in creating a Genetic Algorithm is to determine how a solution can be represented; this will be the template for which the genotypes (solutions) are randomly generated. In the case of a 0-1 Knapsack problem, there are n items that may or may not be placed in the knapsack. A solution is represented by a vector of n bits. If the bit has value of 1 then that item is placed in the knapsack, a value of 0 means the item is not placed in the knapsack.

2. The next step is to prepare a fitness evaluation for a possible solution. The fitness function of the knapsack problem adds up the weights and values of the population of solutions. If the sum weight of the items is greater than the capacity then fitness lower than the fitness of the lowest successful knapsack is given, since it is not an acceptable solution to the problem. If

the weight constraint is met then the fitness for the solution is equal to the sum of values of the items in the knapsack.

3. The next step of a Genetic Algorithm is to create a new generation from the fittest individuals of the previous population. The simplest technique is cloning, where an individual is simply copied to the next generation. Usually only the fit genotypes are copied to the next generation.

Cloning of a bit vector :

11010110 → 11010110

4. The remaining members of the population are generated from crossover and mutation of the most fit individuals of the current population. Mutation simply changes the value of one part of a solution to another random value. In the case of a bit vector representation of a solution, the bit is simply flipped.

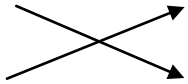
Mutation of a bit vector :

11**0**10110 → 11**1**10110

Crossover is the heart of a Genetic Algorithm, and the driving mechanism behind evolution itself. Crossover takes two genotypes and combines them by copying part of one genotype, then crossing over to the other genotype at some point and copying that genotype. There may be more than one crossover point during the creation of a new genotype.

Crossover of bit vectors :

110|10110 → 110|01101



110|10110 → 110|01101

5. Crossover and mutation are performed on the current generation until the descendant generation has been filled. The descendant generation is then evaluated using the fitness function and the same procedure is used to create yet another generation of possible solutions.

The complexity of the Genetic Algorithm is $O(N \cdot Size)$, where N is the number of items and Size is the number of chromosomes in each generation.

5.5 Comparison of the Algorithms

The algorithms discussed in section 5.4 for solving 0-1 Knapsack Problem can be applied for the model (5.3.3) depending upon the number of risk items in the risk management data and the budget used for the mitigation.

The optimized mitigation measures catalogue is required for the ARCC methodology presented in chapter 4. During the early stage of ARCC methodology development, the brute force algorithm has been applied in order to solve the model (5.3.3) because of its exact solution and easy to program. However, this can only be used for very small set of data since its complexity grows exponentially.

In the next step, Dynamic Programming has been implemented. It worked well with comparatively large number of items as well as not difficult with regards to programming efforts and seems a good candidate to solve the model (5.3.3). However, by increasing the capacity (mitigation budget), the number of basic operations and memory increases drastically.

The Genetic Algorithm is then tried to implement for solving the model (5.3.3). It has been observed that number of basic operations increase with almost same rate by increasing the number of items as it was in the case of Dynamic Programming. However, the increase in capacity (mitigation budget) does not increase the number of operations and memory.

Therefore, as long as the capacity of the knapsack is less than the size of population, the Dynamic Programming will outperform the Genetic Algorithm. However, once the capacity becomes greater than the size of population, the Dynamic Programming number of operations and memory required will be a lot greater than the Genetic Algorithm.

6 Software design for ARCC Methodology

This chapter briefly discribes the implementation details of ARCC methodology prototype system. The proposed ARCC methodology is developed as web-based application. The software consists of two parts: database in MySQL and business logic in java classes. The tools used for the development are Netbeans 6.1, JDK 1.6, Apache Tomcat and MySQL 5.0.32.

For the storage of data, Relational Data Base Management System (RDBMS) MySQL 5.0.32 is chosen for its free availability and portability. The database consists of seven tables. Table *component* keeps the information of a product's components along with their hierarchal levels. All the possible levels in system are stored in table level. The possible levels are of type 0, 1 and 2 for Major system level, Major system components and sub components of components respectively.

The table *global_felature_zones* keeps the detail of Global Features and their various zones such as Blue, Green, Yellow, and Red. Information regarding the individual risks is stored in the table *risk*. Table *risk_clusters* stores the risk hierarchy and their relation with any of the features. Table *mitigation_measure* keeps the data of mitigation cost and its description. Table *risk_mm* stores the relationship between risks and mitigation measure such as mitigation measures corresponding to risks, what is its occurrence probability, what is its impact etc. An overview of the database design is presented in figure 6.1.

The developed application has 3-tier architecture. The presentation layer is in java server pages and business logic is developed in java. The java source code consists of a number of packages. Package *arcc.data* classes are used to generate the random data. The database connectivity is kept in package *arcc.db*. The package *arcc.models* consists of data structures. The package *arcc.bf* consists of classes that are required to find the optimized mitigation plan using Brute Force algorithm. Classes that are required to find optimized plan using the Dynamic Programming approach reside in the package *arcc.dp*. The package *arcc.ga* keeps logic to find optimized plan using Genetic Algorithm. Web beans are stored in package *arcc.beans*.

The details are given in *Appendix B*.

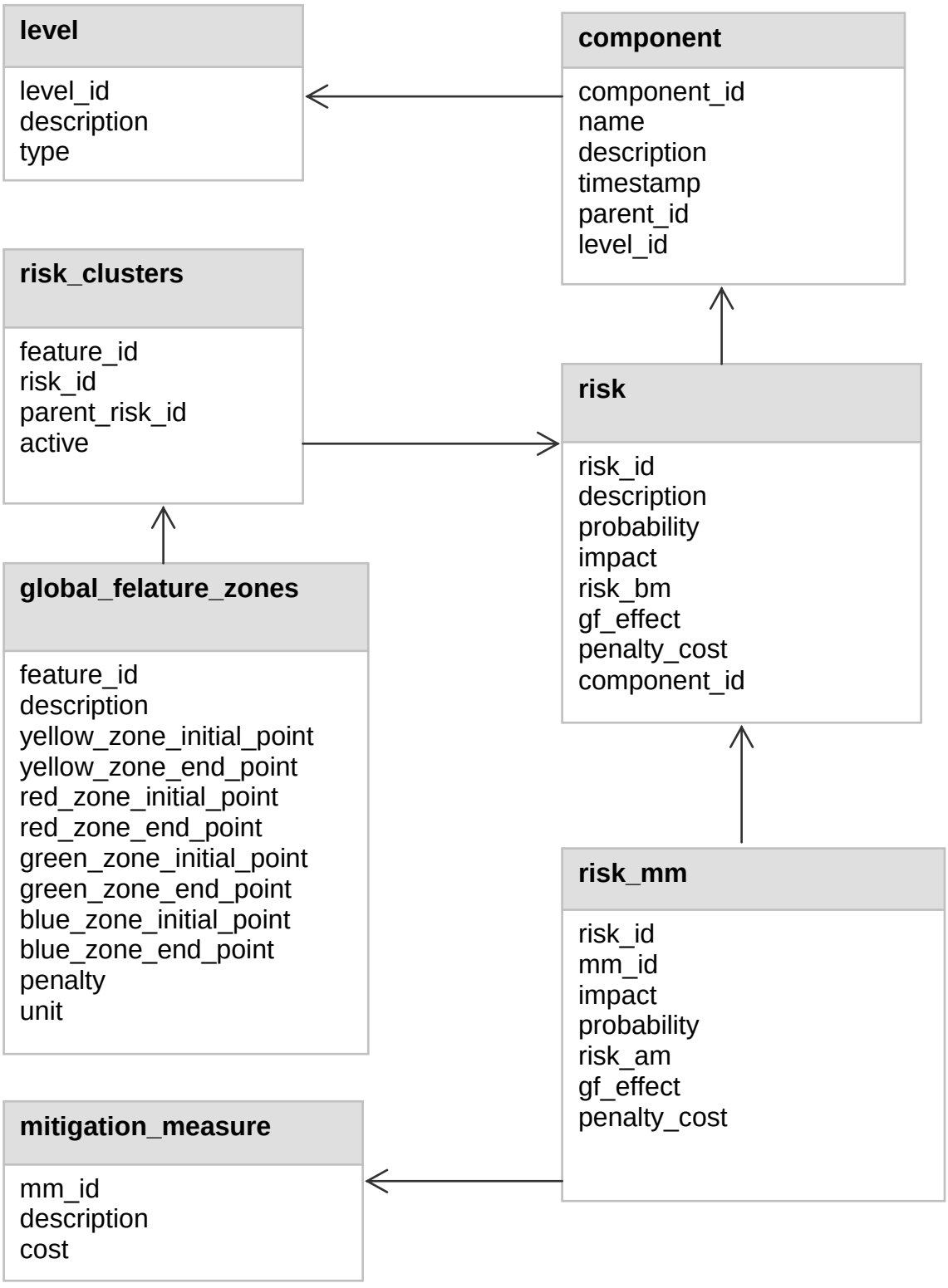


Figure 6.1: The database design of ARCC system

7 Simulations and Analysis of Results

7.1 Simulations

For the simulations of the developed ARCC methodology, four Global Features are considered. Ten risks are randomly generated and stored in the database system according to Risk Breakdown Structure of the Technical Risk Management. It is also considered that each risk is affecting all four Global Features.

7.1.1 Global Features Matrix

According to ARCC methodology, a Global Features matrix must be defined first. Four Global Features GF1, GF2, GF3, and GF4 along with their values in different zones are defined. All values of the Global Features are given in percentages. The internal ideal target and market oriented target zones are represented by Blue and Green colors respectively. The Red color presents the out of the market zone. The range of the Global Features values for which a penalty cost must be paid is presented in Yellow zone. This penalty cost is defined for each unit of respective Global Feature. A web based user interface showing this defined Global Features matrix is given in figure 7.1.

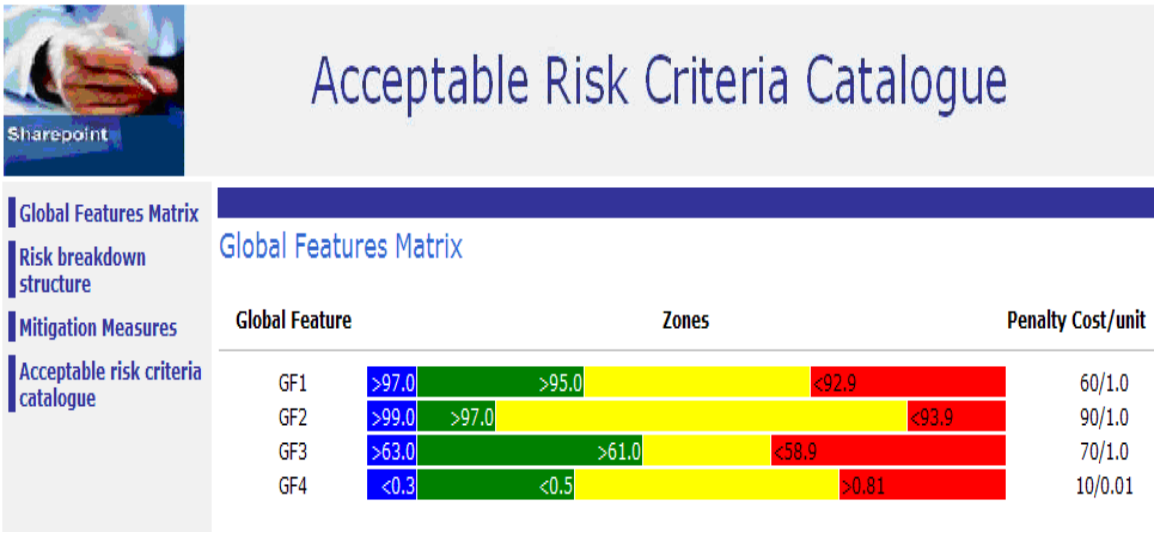


Figure 7.1: Global Features Matrix

Consider the example of GF1 for the better understanding of the Global Features matrix in figure. 7.1. A value greater than 97% of the GF1 lies in the Blue zone, the range of the values from 95% to 97% is in Green zone and the values less than 92.9% is in Red zone. A range of values from 93% to 95% brings the GF1 in Yellow zone and a penalty cost of 60 thousands Euro is defined for each 1% loss in this range.

The values of the GF2 & GF3 have similar behavior as in case of values of the GF1. It is important to notice here that these Global Features values are decreasing when moving from Blue zone to Red zone.

However, the value of GF4 has an opposite behavior. The value of GF4 less than 0.3% lies in Blue zone. A range of values from 0.3% to 0.5% defines the Green zone while the values greater than 0.81% bring the GF4 in Red zone. The Yellow zone is described by the range of the values from 0.5% to 0.8%. In this case, penalty case is defined as 10 thousands Euro for each 0.01% increase in the value of GF4.

Such a behavior in the Global Feature values is not surprising. Consider the scenario that GF1 represents the availability of a machine. Then, of course, higher values of the availability are the market requirements. In contrast, if a GF4 represents time to market for a machine then a shorter time will always be in high demand.

7.1.2 Risk Breakdown Structure

Ten risks are randomly generated according to Risk Breakdown Structure of the Technical Risk Management. This Risk Breakdown structure consists of details of risks, sub-risks and their effect on Global Features. Figure 7.2 shows the Risk Breakdown Structure before the implementation of mitigation measures.

For example, the risk with Id 1 has an impact of 1108€ (in hundreds Euro) and probability of its occurrence 0.537. The risk being the product of probability and impact yields a value of 596€ (in hundreds Euro). The risk 1 consists of four sub-risks with IDs 41, 42, 43 and 44. Each sub-risk is having an impact on one of the Global Features. Sub risk ID 41, for example, affects GF1 and reduces its value to 0.05%. The negative sign indicates the decrease while positive sign represents the increase in the Global Features values respectively. Due to effect of risks on Global Features, penalty cost for each sub risk is calculated by multiplying the

values of GF's effect with unit penalty cost and sum of the penalty costs of all sub risks give the penalty cost of the corresponding risk. For example, penalty cost due to risk 1 is 5.88 which mean 5.88 thousands Euro.

Acceptable Risk Criteria Catalogue

- Global Features Matrix
- Risk breakdown structure
- Mitigation Measures
- Acceptable risk criteria catalogue

Risk Breakdown Structure

- Before mitigation measure
- After mitigation measure

Risk breakdown structure before mitigation measure

Risk Id	Impact	Probability	Risk	Sub Risk ID	Global feature	Effect	Penalty Cost
1	1108.0	0.5377	596				5.88
				41	1	-0.05	3.0
				42	2	-0.0020	0.18
				43	3	-0.01	0.7
				44	4	0.0020	2.0
2	3997.0	0.934	3733				136.7
				36	1	-0.69	41.4
				37	2	-0.43	38.7
				38	3	-0.5	35.0
				39	4	0.02	20.0
3	9742.0	0.5533	5390				197.7
				31	1	-0.78	46.8
				32	2	-0.55	49.5
				33	3	-0.7	49.0
				34	4	0.05	50.0
4	1612.0	0.3033	489				99.7
				51	1	-0.2	12.0
				52	2	-0.22	19.8
				53	3	-0.25	17.5
				54	4	0.05	50.0
5	9910.0	0.3463	3432				237.1
				56	1	-0.79	47.4
				57	2	-0.56	50.4
				58	3	-0.65	45.5
				59	4	0.09	90.0
6	5984.0	0.9314	5573				134.0
				16	1	-0.45	27.0
				17	2	-0.55	49.5
				18	3	-0.35	24.5
				19	4	0.03	30.0
7	3629.0	0.4186	1519				97.2
				46	1	-0.24	14.4
				47	2	-0.31	27.9
				48	3	-0.33	23.1
				49	4	0.03	30.0
8	2022.0	0.6717	1358				64.2
				21	1	-0.19	11.4
				22	2	-0.27	24.3
				23	3	-0.11	7.7
				24	4	0.02	20.0
9	3803.0	0.998	3795				161.7
				11	1	-0.57	34.2
				12	2	-0.5	45.0
				13	3	-0.55	38.5
				14	4	0.04	40.0
10	7936.0	0.0766	608				82.9
				26	1	-0.3	18.0
				27	2	-0.35	31.5
				28	3	-0.28	19.6
				29	4	0.01	10.0

Figure 7.2: Risk Breakdown Structure before Mitigation Measures

The Risk Breakdown Structure after mitigation measures is similar to the structure presented for before mitigation measures page. However, there are now two additional columns of mitigation measures identity (MM Id) and costs of these mitigation measures (Cost) for each risk. For example, Risk id 1 has MM-Id1 and cost 80€ (in hundreds Euro). This structure is shown in figure 7.3.

Risk breakdown structure after mitigation measure

Risk Id	Impact	Probability	Risk	MM Id	Cost	Sub Risk ID	Global feature	Effect	Penalty Cost
1	827.0	0.5307	439	1	80.0				0.19
						41	1	-0.0020	0.12
						42	2	0.0	0.0
						43	3	-0.0010	0.07
						44	4	0.0	0.0
2	1041.0	0.3211	334	2	1700.0				0.13
						36	1	-0.0010	0.06
						37	2	0.0	0.0
						38	3	-0.0010	0.07
						39	4	0.0	0.0
3	5563.0	0.4823	2683	3	980.0				48.1
						31	1	-0.17	10.2
						32	2	-0.13	11.7
						33	3	-0.16	11.2
						34	4	0.015	15.0
4	377.0	0.1932	73	4	190.0				10.9
						51	1	-0.04	2.4
						52	2	-0.06	5.4
						53	3	-0.03	2.1
						54	4	0.0010	1.0
5	367.0	0.2867	105	5	1620.0				1.3
						56	1	-0.01	0.6
						57	2	0.0	0.0
						58	3	-0.01	0.7
						59	4	0.0	0.0
6	4552.0	0.7095	3230	6	1130.0				31.7
						16	1	-0.12	7.2
						17	2	-0.15	13.5
						18	3	-0.1	7.0
						19	4	0.0040	4.0
7	132.0	0.3928	52	7	590.0				0.85
						46	1	-0.0010	0.06
						47	2	-0.0010	0.09
						48	3	-0.01	0.7
						49	4	0.0	0.0
8	1138.0	0.6713	764	8	200.0				15.25
						21	1	-0.01	0.6
						22	2	-0.07	6.3
						23	3	-0.0050	0.35
						24	4	0.0080	8.0
9	1410.0	0.9322	1314	9	990.0				1.3
						11	1	-0.01	0.6
						12	2	0.0	0.0
						13	3	-0.01	0.7
						14	4	0.0	0.0
10	6936.0	0.0539	374	10	100.0				31.3
						26	1	-0.1	6.0
						27	2	-0.12	10.8
						28	3	-0.15	10.5
						29	4	0.0040	4.0

Figure 7.3: Risk Breakdown Structure after Mitigation Measures

7.1.3 Mitigation Measures

The next step is to calculate the impact of mitigation measures on Global Features values. The ARCC methodology calculates *possible target vector*, *best possible target vector* and *optimized possible target vector* by implementing no mitigation measures, all mitigation measures and optimized mitigation measures respectively. The user interface page *Mitigation Measures* presents the outcome of these calculations.

7.1.3.1 No Mitigation Measures

Now if no mitigation measures are applied and all risks happened, the effect of these risks on Global Features is calculated in this sub-section. The user interface page shows these values in corresponding zones according to Global Features matrix in figure 7.4. For example, value of the GF1 is 92.74% which is in Red zone and remaining three Global Features fall in Yellow zone. The corresponding penalty cost of each Global Feature is shown as well.

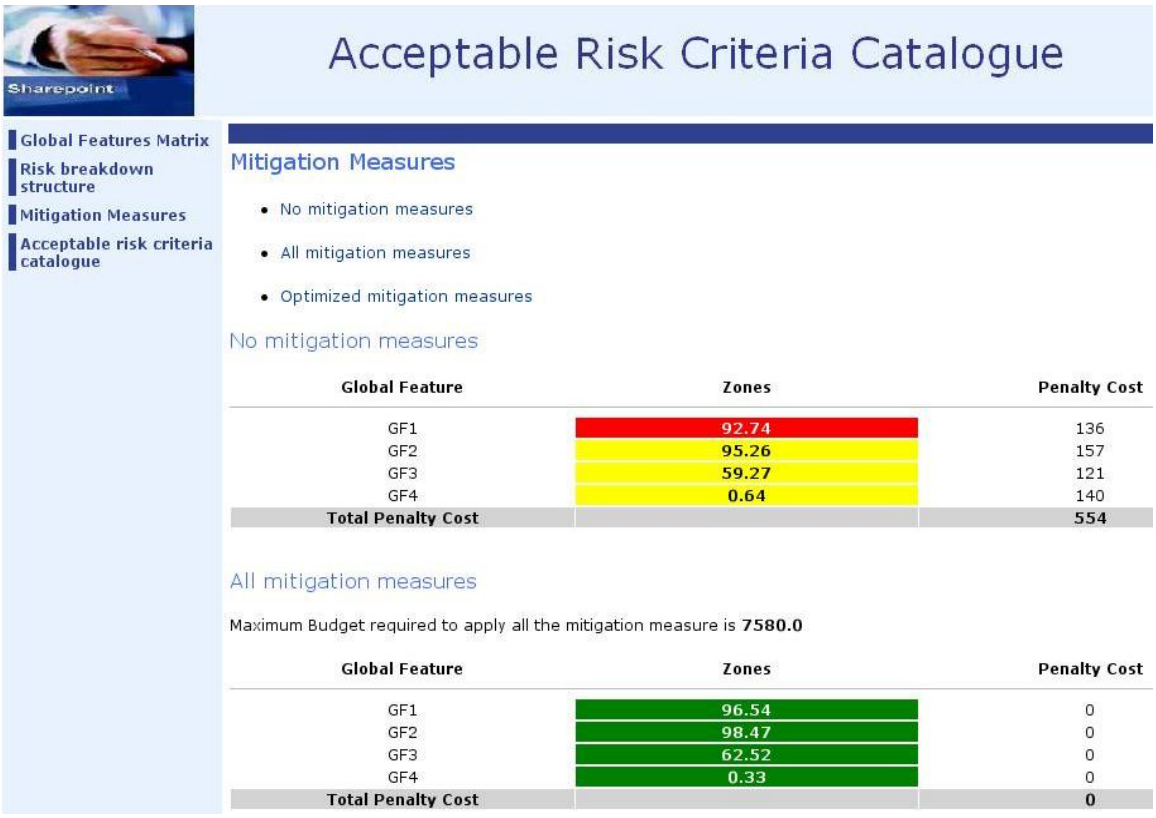


Figure 7.4: Mitigation Measures

7.1.3.2 All Mitigation Measures

In order to calculate the maximum required budget, all mitigations are implemented in this step. The corresponding effect on Global Features values with the implementation of all mitigations is presented as well in the user interface page shown in figure 7.4. In this case, all Global Features are in Green zone and no penalty cost is to be paid. The total required mitigation budget is 758 thousands Euro.

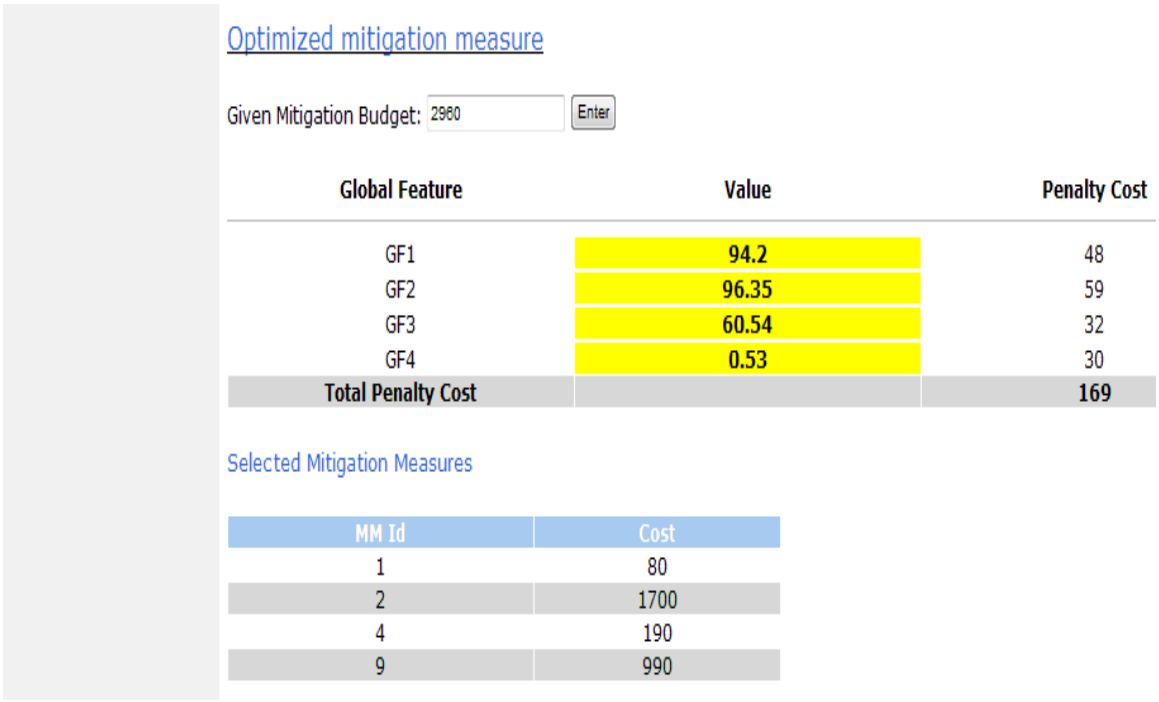
7.1.3.3 Optimized Mitigation Measures

In the previous step (sub-section 7.1.3.2), maximum budget required for all mitigation measures has been calculated. In order to find an optimized budget for ARCC methodology, one can now select different values of the budget less than the maximum budget and can calculate the corresponding values of Global Features as well as the penalty costs. The optimization model developed in chapter 5 has been used, i.e., selection of those mitigation measures which brings maximum risk reduction under the constraint of given budget. The user interface page presented in figure 7.5 shows the utilized budget, values of Global Features in the corresponding zones, corresponding penalty costs, and selected mitigation measures along with their costs.

For example, a budget of 300 thousands Euro results into an optimum set of mitigation measures {1, 2, 4, 9}. In this case, all Global Features values fall in Yellow zone and this results to a penalty cost of 169 thousands Euro.

7.1.4 Acceptable Risk Criteria Catalogue

Once the decision maker decides for the optimum budget in previous step (sub-section 7.1.3.3), the user interface page provides all risks Ids along with their probability of failure and acceptable probability of failure shown in figure 7.6. For example, in case of using 300 thousand Euros, risks 1, 2, 4, and 9 are mitigated. Therefore, probabilities of failure for these risks are taken from Risk Breakdown Structure after mitigation measures. For the remaining risks, the probabilities of failure are taken from Risk Breakdown Structure before Mitigation measures.



Optimized mitigation measure

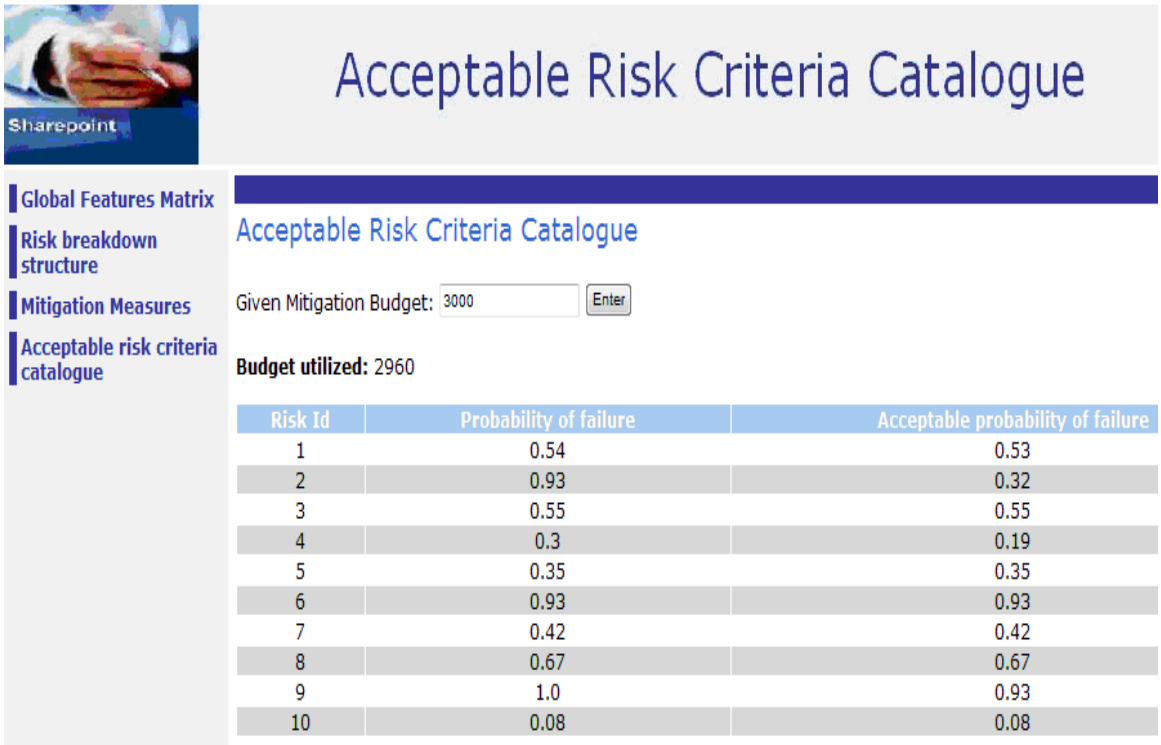
Given Mitigation Budget: 2960 Enter

Global Feature	Value	Penalty Cost
GF1	94.2	48
GF2	96.35	59
GF3	60.54	32
GF4	0.53	30
Total Penalty Cost		169

Selected Mitigation Measures

MM Id	Cost
1	80
2	1700
4	190
9	990

Figure 7.5: Optimized Mitigation Measures



Risk Id	Probability of failure	Acceptable probability of failure
1	0.54	0.53
2	0.93	0.32
3	0.55	0.55
4	0.3	0.19
5	0.35	0.35
6	0.93	0.93
7	0.42	0.42
8	0.67	0.67
9	1.0	0.93
10	0.08	0.08

Figure 7.6: Acceptable Risk Criteria Catalogue

7.2 Analysis of Results

The ARCC methodology has been applied to the Risk Breakdown Structure given in figure 7.2. The mitigation budget is plotted against the risk reduction and the values of Global Features. This section provides the detail explanation of these results.

7.2.1 Budget versus Objective Functions

In order to derive an optimized mitigation budget for the ARCC methodology, the dynamic programming algorithm has been applied to solve the optimization problem. The objective of the optimization model is to select those mitigation measures which maximize the risk reduction under the constraint of mitigation budget. This model has been explained in equation (5.3.3):

$$\text{Objective Function 1 (OF 1):} \quad \sum_{i=1}^{n} \Delta R_i \cdot m_i \rightarrow \max$$

$$\text{Constraint:} \quad \sum_{i=1}^{n} c_i \cdot m_i \leq B \qquad (7.2.1)$$

$$m_i \in \{0,1\}, \quad i = 1,2,\ldots,n$$

The maximum budget required for the implementation of all mitigation measures can be computed by calculating the sum of all mitigation costs. In order to decide which mitigation budget should be used for the constraint in the model 7.2.1, the mitigation budget is plotted against the optimal risk reduction with respect to the Objective Function 1 (OF 1) in figure 7.7.

The budget is given along x-axis and risk reduction along y-axis in thousand Euro [k€]. This plot shows that risk reduction increases continuously with increasing budget. For example, a mitigation budget of 320k€ reduces the risk to 800k€ and a risk reduction of 1.2 million Euro can be obtained by allocating a budget of 520k€. The decision maker can select a mitigation budget and get the corresponding risk reduction. This selected mitigation budget can then be used for the derivation of ARCC.

However, the selection of the budget is still a difficult task for a decision maker from this plot and is not much helpful in the decision process. Therefore, there must be more effective ways which can assist for such decisions.

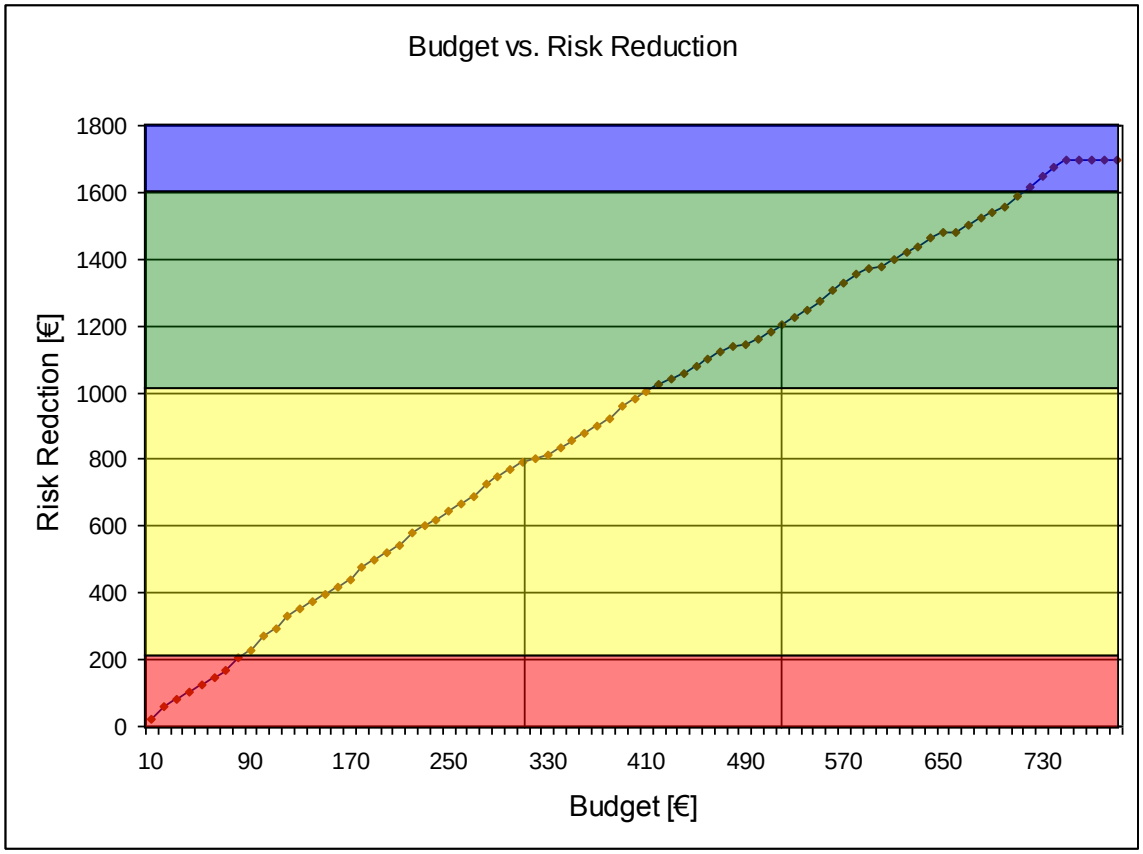


Figure 7.7: Budget VS. Risk Reduction (OF 1)

Since penalty costs paid to the customer has been taken into account while deriving the methodology for ARCC. One of the possibilities to improve the optimization model could be the introduction of the penalty costs in the Objective Function.

The target of the Technical Risk Management is to maximize risk reduction by the application of mitigation measures as well as minimizing the penalty costs. In order to achieve these two objectives, those mitigation measures should be selected which maximizes the ratio of the risk reduction to the penalty cost after mitigation. Therefore, the optimization model (7.2.1) can take the form:

Objective Function 2 (OF 2):
$$\sum_{i=1}^{n}\left(\frac{\Delta R_i}{PC_{i;M}}\right)\cdot m_i \rightarrow max$$

Constraint:
$$\sum_{i=1}^{n} c_i \cdot m_i \leq B \qquad (7.2.2)$$
$$m_i \in \{0,1\},\quad i = 1,2,...,n$$

The mitigation budget is now plotted against the optimal risk reduction with respect to the Objective Function 2 (OF2) in figure 7.8. The budget is given along x-axis and risk reduction along y-axis in thousands Euro [k€]. In this case, the risk reduction is increasing with budget increment but now there are jumps in the risk reduction curve. This is an interesting behavior for the decision maker. For example, a mitigation budget of 160k€ gives a risk reduction of 480k€ while a budget of 180k€ gives risk reduction to 2.6 million Euro. This behavior would better help a decision maker with respect to selection of the mitigation budget.

In order to get better decision idea for the mitigation budget selection, the plot has been divided in to seven zones. If a decision maker decides for a budget in zone-1 and zone-2, this could not be a good choice because there is very less benefit in terms of risk reduction. In addition, only a small increment in mitigation budget to enter in zone-3 can bring huge risk reduction. Therefore, it's better for a decision maker not to select the budget in first two zones. In contrast, the risk reduction is maximum in zone-7 but almost remains constant for a budget of more than 500k€ and therefore zone-7 would not be a good choice as well for decision maker.

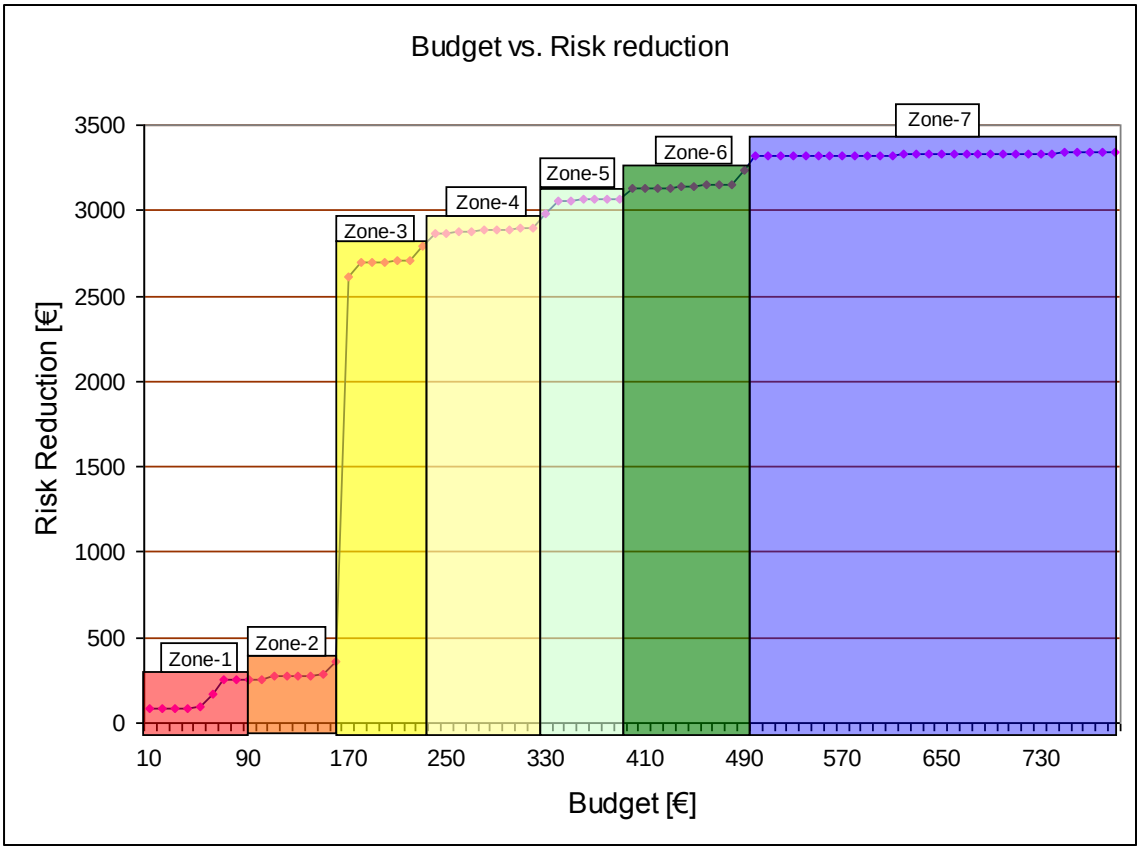


Figure 7.8: Budget VS. Risk Reduction (OF 2)

However, the remaining four zones, zone-3 to zone-6, could be better options in order to decide for an optimum mitigation budget. For a conservative decision maker about risks, zone-5 and zone-6 could be best choices to decide the mitigation budget. If decision maker is more risk taker, zone-3 and zone-4 provides good choice for the selection of the mitigation budget.

7.2.2 Budget versus Global Features

In last section 7.2.1, it has been showed that Objective Function 2 assists better in making the decision about the optimum mitigation budget. After a budget selection from figure 7.8, a decision maker must be interested in corresponding values of Global Features. This can further help for the selection of budget as well in case there is an interest in some particular value of one or some Global Features.

7.2.2.1 Budget versus Global Feature 1

The values of GF1 corresponding to mitigation budget are shown in figure 7.9. The Blue, Green, Yellow, and Red zones in the plot are according to the different zones defined in Global Feature matrix. The value of GF1 in percentages [%] are taken along y-axis while mitigation budget in thousands Euro [k€] is taken along x-axis.

In case, a decision maker must want the value of GF1 in Green zone then budget should be greater than 460k€. This is same as the decision of budget in zone-6 of the plot in figure 7.8. A good choice to decide would always be in the values of GF1 from 93.5% to 94.5% with a budget range of 170k€ to 320k€.

The values of the GF1 show a zick-zack behavior with increasing mitigation budget. These values can be filtered to Pareto-optimal points in order to get only higher values of GF1 with increasing mitigation budget. This is plotted in figure 7.10.

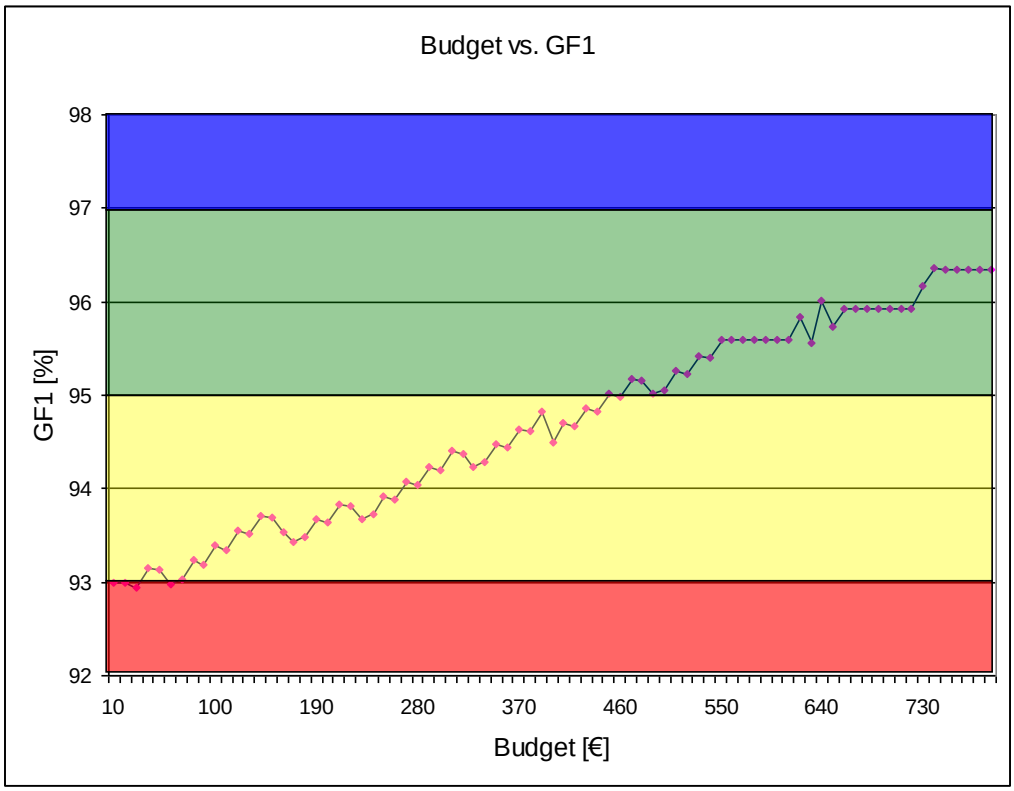


Figure 7.9: Budget VS. Global Feature 1

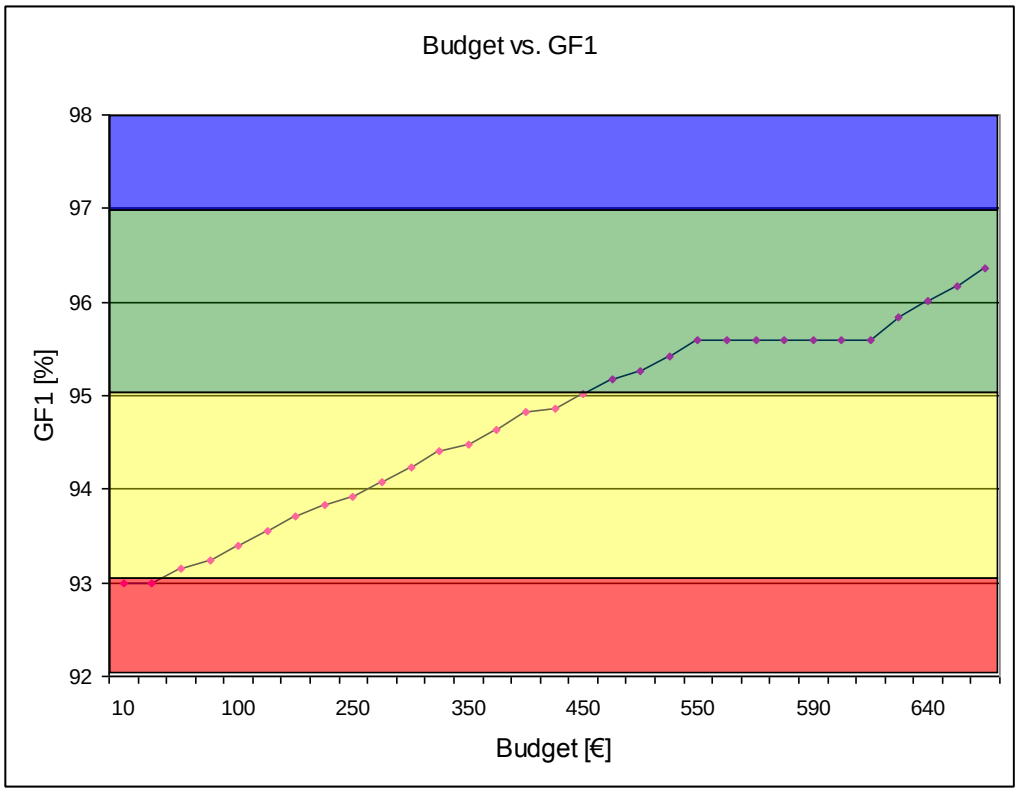


Figure 7.10: Budget VS. Global Feature 1 (Pareto-optimal)

7.2.2.2 Budget Versus Global Feature 2

The values of GF2 corresponding to mitigation budget are shown in figure 7.11. The behavior is similar to the values of GF1 and therefore can be filtered to Pareto-optimal points in order to get only higher values with increasing mitigation budget shown in figure 7.12. In order to get the values of GF2 in Green zone, the budget must be selected greater than 460k€. A budget range from 170k€ to 320k€ also provides a better choice for a decision maker because the values of GF2 still remains in the upper half of Yellow zone giving a range from 96% to 96.5%.

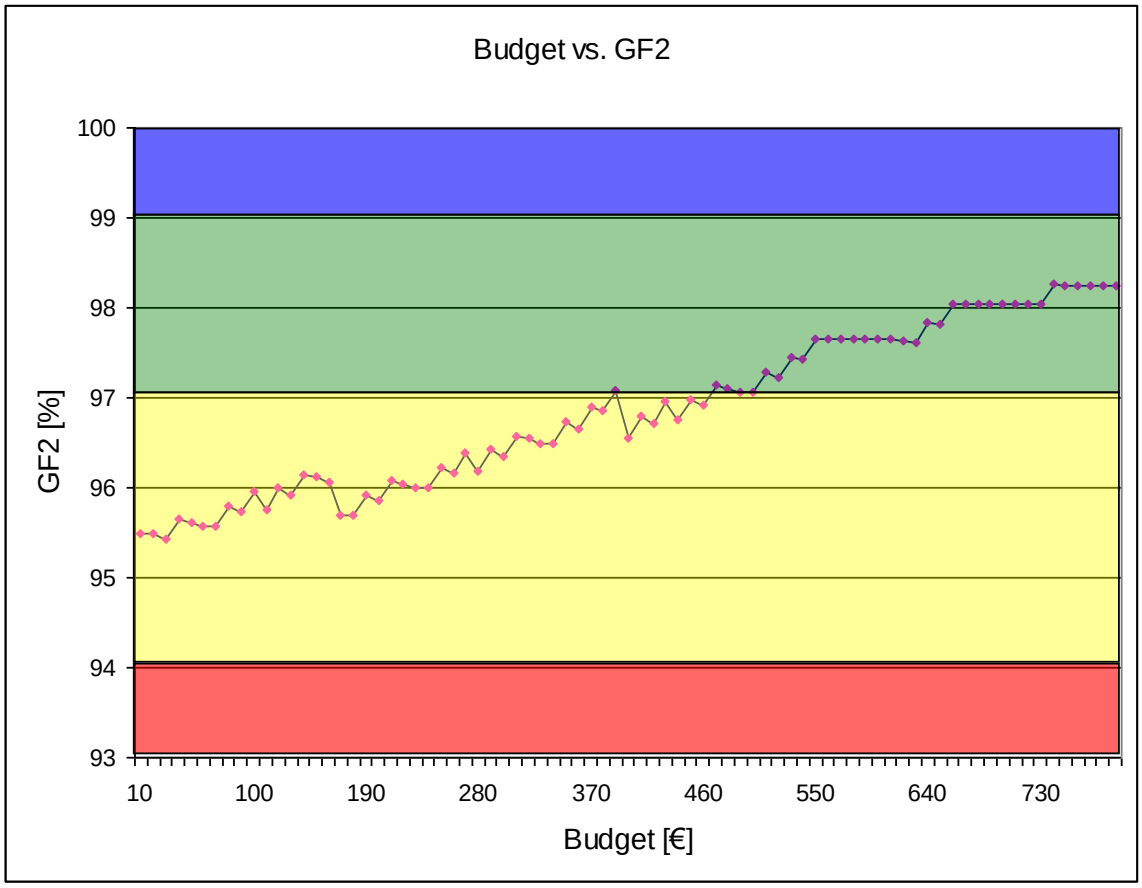


Figure 7.11: Budget VS. Global Feature 2

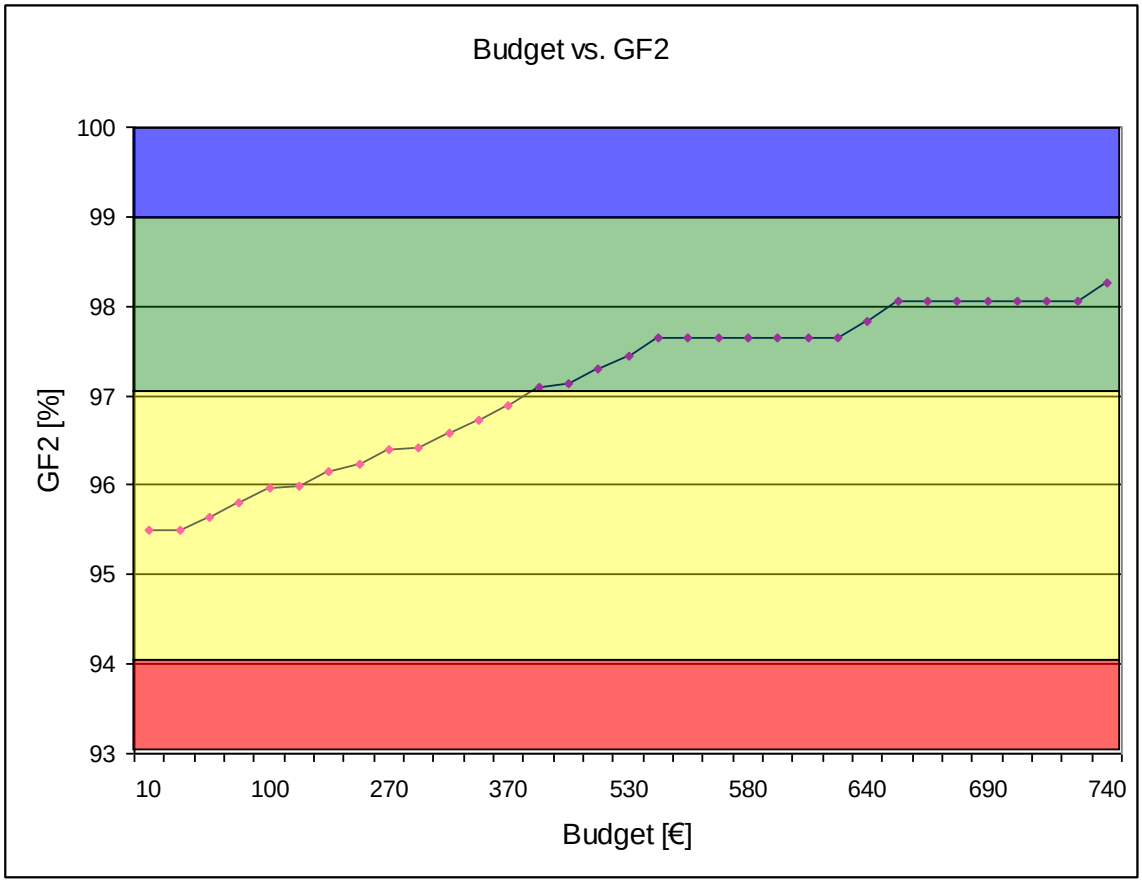


Figure 7.12: Budget VS. Global Feature 2 (Pareto-optimal)

7.2.2.3 Budget Versus Global Feature 3

The values of GF3 corresponding to mitigation budget are shown in figure 7.13. The behavior is also similar to the values of GF1 and GF2 and can be filtered to Pareto-optimal points as well in order to get only higher values with increasing mitigation budget shown in figure 7.14. The selection of budget greater than 440k€ brings the values of GF3 into the Green zone of Global Features matrix. The budget range from 170k€ to 320k€ provides a better choice for a decision maker because the GF3 values still remains in the upper half of Yellow zone giving a range from 60% to 60.6%.

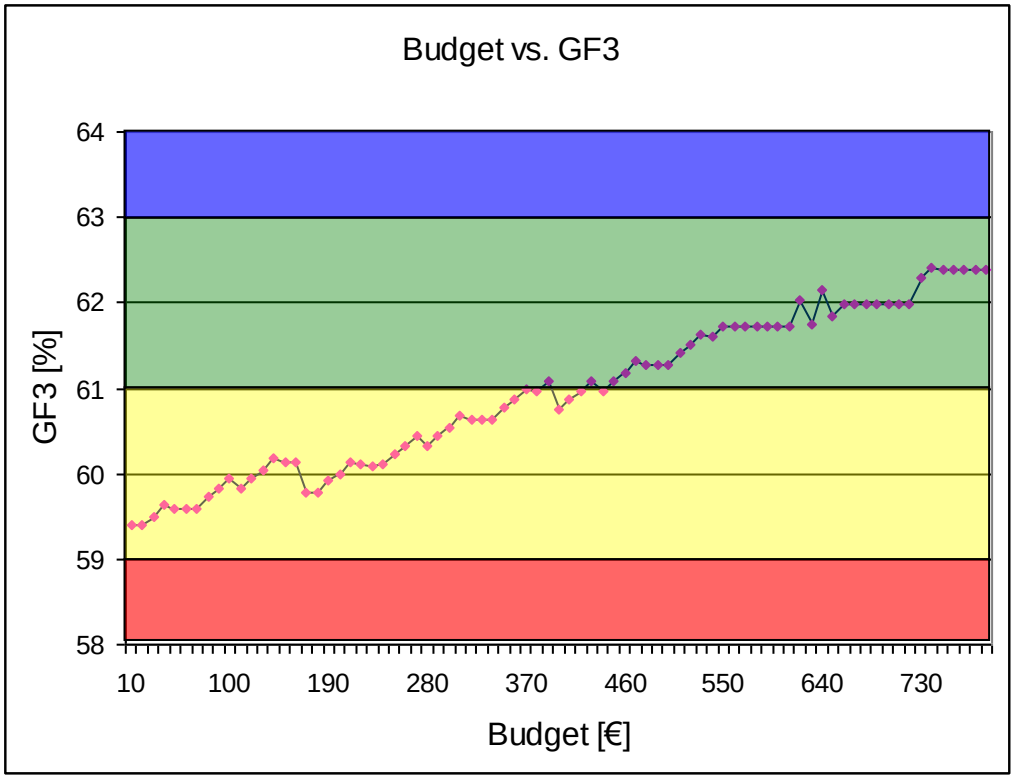


Figure 7.13: Budget VS. Global Feature 3

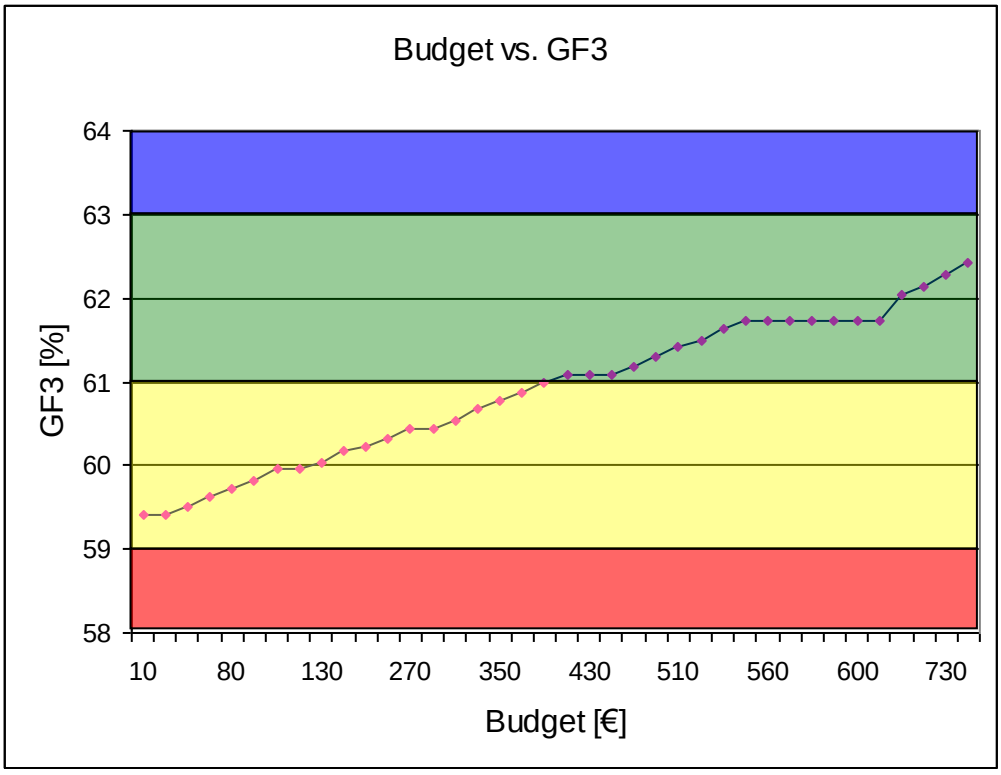


Figure 7.14: Budget VS. Global Feature 3 (Pareto-optimal)

7.2.2.4 Budget Versus Global Feature 4

The values of GF4 corresponding to mitigation budget are shown in figure 7.15. The filtered Pareto-optimal points in order to get only lower values of the GF4 with increasing mitigation budget shown in figure 7.16. The lower values of the GF4 leads to Green zone of the Global Feature matrix. For the budget selection of greater than 370k€, the values of GF4 fall into the Green zone of the Global Features matrix. The budget range from 100k€ to 300k€ provides a good choice because the values of GF4 remains closer to Green zone.

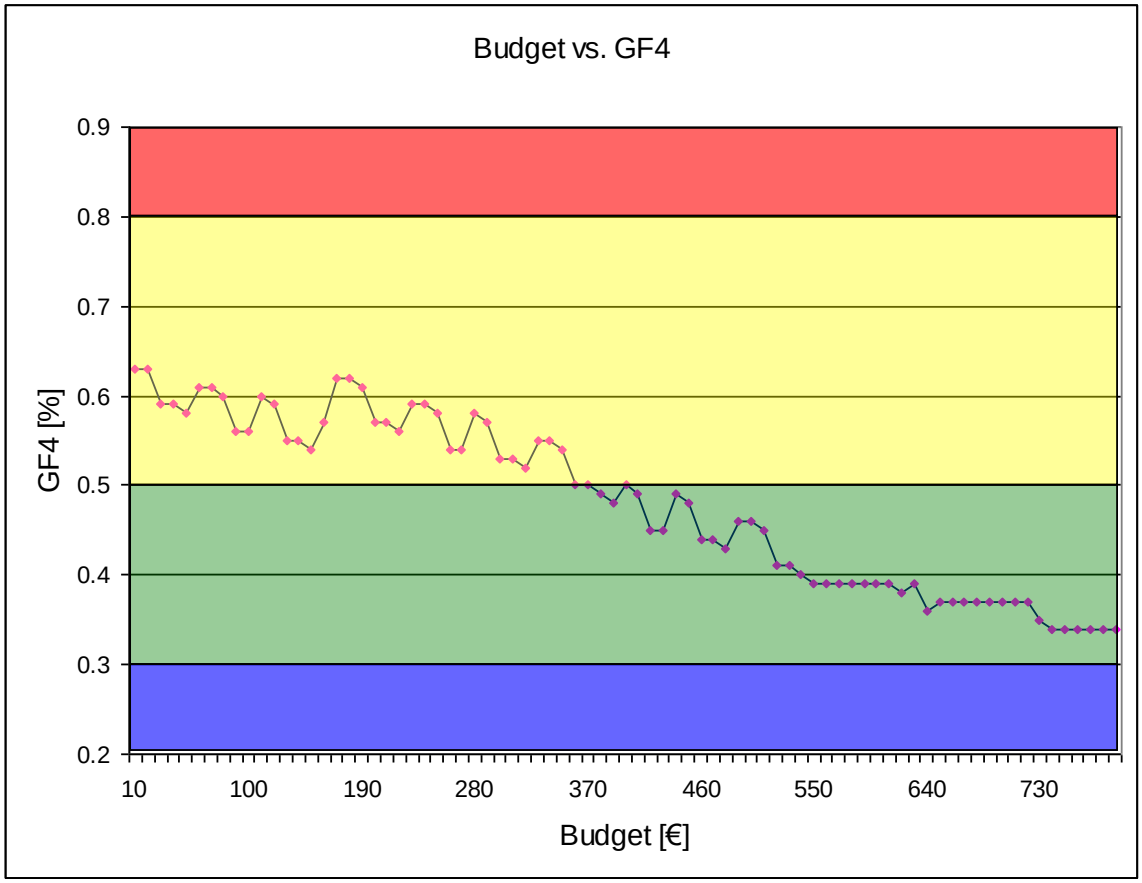


Figure 7.15: Budget VS. Global Feature 4

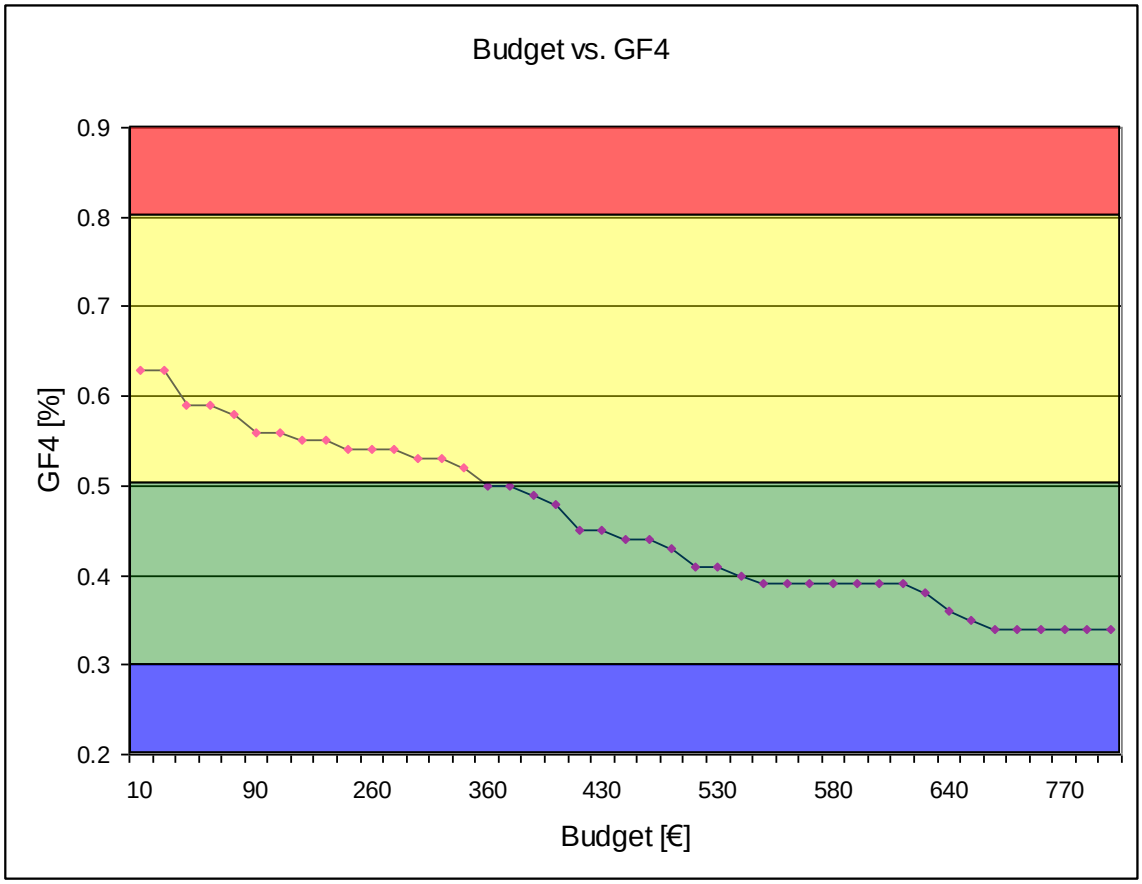


Figure 7.16: Budget VS. Global Feature 4 (Pareto-optimal)

7.3 Summary

In order to realize the developed methodology for ARCC and its software tool, the simulations and the analysis of results as well as the web based user interface has been presented in this chapter. For the simulations, four Global Features have been defined and ten risks are randomly generated according to Risk Breakdown Structure of the Technical Risk Management.

To analyze the optimized mitigation budget, mitigation budget has been investigated against the risk reduction. It has been observed that risk reduction increases with budget increment. However, this gives no clear idea for the selection of an optimized budget to a decision maker.

It has been shown that including penalty costs into the objective function, that is, maximizing the risk reduction as well as minimizing the penalty costs after mitigation, gives better options for the selection of an optimized budget. This

investigation shows that risk reduction is now increasing in different zones with the increment in mitigation budget. A decision maker can play better in these zones in order to decide for an optimum mitigation budget.

The mitigation budget has been further plotted against each Global Feature to get the effect of the selected budget on the values of Global Features. This will provide more choices to a decision maker in order to adjust the mitigation budget against a specific value of a Global Feature.

8 Conclusions and Outlook

The development of complex series products is characterized by a long development time, many involved persons partly working at different places, and a high complexity of products and processes. In such conditions there could be many risks that the given development goals will not be reached.

Defining the company's acceptable risk level falls to management because they intimately understand the company's business drivers and the corresponding impact if these business objectives are not met.

The mitigations of risks require a huge budget which is usually not feasible for the industries. It is difficult to decide which risk should be mitigated under the constraint of limited budget so that the development goals of the product can be achieved. Therefore, answer to the question “What is an Acceptable Risk Criteria Catalogue?” has great importance to decision makers in manufacturing of complex series products.

This thesis makes an important contribution to the management of technical risks to answer this question. A first way towards the methodology for the derivation of an Acceptable Risk Criteria Catalogue has been presented. Software has been developed for the realization of this methodology and a web based user interface has been provided for the easy use of this software.

The developed methodology is a practical supplement of the existing approaches for Technical Risk Management in projects of product development. It provides a helping tool for the decision makers to decide about the mitigation budget in order to bring the product faster into the market.

Since there is no published work in this area and the methodology has been developed as a first way in the direction of Acceptable Risk Criteria Catalogue in an economics point of view, there are many ways for its extension. Followings can give an overview of such extensions:

- In the methodology development, the dependencies between mitigation measures are not considered in the mathematical model. Therefore, the next step in the further development would be to extend the model with dependent mitigation measures.

- The risk has been defined with deterministic values and so another scope for the further development could be to use the risk value as a stochastic value in order to develop more robust methodology.

- The methodology provides a range of budget with respect to maximum risk reduction. A decision maker can decide a mitigation budget from this range and get the corresponding values of Global Features. The idea for the further development in this direction is to optimize the values of Global Features under the constraint of optimum budget range. At this step, the developed optimized mitigation measures catalogue can be used as pre-processor and Global Features can be optimized using the techniques of vector optimization.

Bibliography

Back (1997)	T. Back, U. H. Hammel, and Hans-Paul Schwefel: “Evolutionary Computation: Comments on the History and Current State”. IEEE Trans. on Evolutionary Computation, Vol. 1, No. 1, 1997.
Black (2001)	Black, Mollis: "U. S. Aerospace Risk Analysis Survey." Journal of Cost Analysis & Management, Winter issue, (2001): 1.
Branscomb (2000)	Branscomb, Lewis, et al: “Managing Technical Risk”, U.S. Department of Commerce, NIST GCR 00-787, 2000.
Bahnmaier (2003)	Bahnmaier, W. W., Ed.: “Risk Management Guide for DOD Acquisition”, Defense Acquisition University Press, Fort Belvoir, VA. 5th ed., version 2.0, June 2003.
Bernstein (1996)	Peter L. Bernstein: “Against the Gods, The Remarkable Story of Risk”, Published by John Wiley & Sons, 1996.
Bilstein (1980)	Roger E. Bilstein: “Stages to Saturn, A Technological History of the Apollo/Saturn Launch Vehicles”. Washington, DC: NASA SP-4206, 1980.
Covello & Mumpower (1985)	Covello, V.T., Mumpower, J.: “Risk Analysis and Risk Management, An historical perspective”. Risk Analysis, 5 (2), 103-120, 1985.
Covello & Merkhofer (1993)	Covello, V.T., Merkhofer, M.W.: “Risk assessment methods, approaches for assessing health and environmental risks”. New York: Plenum Press, 1993.
Feller (1968)	Feller, W.: ”An introduction to Probability Theory and Its Applications”, Vol.1. 3rd ed (revised). New York: John Wiley & Sons, Inc., 1968.
Fries (1992)	Sylvia D. Fries: “NASA Engineers and the Age of Apollo”. Washington, DC: NASA SP-4104, 1992.

Garvey (2000) — Garvey, P. R.: “Probability Methods for Cost Uncertainty Analysis, A systems Engineering Perspective”, Marcel Dekker, New York, 2000.

Garvey (2005) — Garvey, P. R.: “System-of-Systems Risk Management, Perspectives on Emerging Process and Practice”, The MITRE Corporation, MP 04B0000054, January 2005.

Gould (1998) — Gould, J H.: “Evaluation of the likelihood of major accidents in industrial processes”.
Handbook of environmental risk assessment and management, Blackwell Science. 1998.

Harnischfeger & Reinking (2001) — Harnischfeger, Uta; Reinking, Guido: “Mercedes Garantiekosten belasten Profite“.
Financial Times Deutschland, 08.05.2001.
URL:http://www.ftd.de/ub/in/1070864.html

Hristakeva (2005) — Hristakeva, Maya and Dipti Shrestha: “Different Approaches to Solve the 0/1 Knapsack Problem”, MICS 2005 Proceedings.

Jarrett (2000) — Jarrett, E.L.: "Effect of Technical Elements of Business Risk on Decision Making", Managing Technical Risk, U.S. Department of Commerce, NIST GCR 00-787, (2000): 75.

Jensen & Bard (2003) — Paul A. Jensen and Jonathan F. Bard: “Operations Research Models and Methods”, published by John Wiley and Sons, 2003.

Kaplan (1997) — Kaplan, S.: “The word of risk analysis”. Risk Analysis, 1997, 17 (4), 407-417.

Kaplan & Garrick (1997) — Kaplan, S., Garrick, B.J.: “On the quantitative definition of risk”. Risk Analysis, 1981, 1 (1), 11-27.

Kaye & Crowley (2000) — Kaye, Ron & Crowley,Jay: “Incorporating Human Factors Engineering into Risk Management”.
Guidance for Industry and Design Control Reviewers, U.S. Dept. of Health and Human Services, Washington D.C., (2000): 8.

Kellerer (2005) — Kellerer, Hans; U. Pferschy, D. Pisinger: “Knapsack Problems“. Springer Verlag, 2005.

Kumamoto & Henley (1996) — Kumamoto, Hiromitsu & Ernest Henley: “Probabilistic Risk Assessment and Management for Engineers and Scientists”. IEEE Press, 1996.

Levine (1982) — Arnold S. Levine: “Managing NASA in the Apollo Era”. Washington, DC: NASA SP-4102, 1982.

Martello (1990) — Martello, Silvano; Paolo Toth: “Knapsack Problems, Algorithms and Computer Implementations”. John Wiley & Sons, 1990.

MIL-P-1629 — MIL-P-1629: “Procedure for performing a failure mode effect and criticality analysis”, United States Military Procedure, November 1949.

MIL-STD-H82H (1984) — MIL-STD-H82H: “System Safety Program Requirements”, U.S. Department of Defense, Washington D.C., AMSC F3329, (1984):2.

Misra (1992) — K.B. Misra: “Reliability Analysis and Prediction: A Methodology Oriented Treatment”.
Elsevier Publishing Company ,1992, ISBN 0-444-89606-6.

Mitchell (1998) — Mitchell, Melanie: “An Introduction to Genetic Algorithms”. Massachusettss: The MIT Press, 1998.

McKinsey (2001) — McKinsey & Company: “Quality Gates verhindern den Garantiefall“, VDI-Nachrichten Nr. 44 , 2001.

Perrow (1984) — Perrow, Charles.: “Normal Accidents: Living with High-Risk Technologies”. Basic Books, Inc., New York, 1984.

Steven (2004) — Kmenta, Steven: "Scenario-Based Failure Modes and Effects Analysis Using Expected Cost".
Journal of Mechanical Design 126 (6): 1027, 2004.

Stewart & Melchers (1997) Stewart, M.G., Melchers, R.E.: “Probabilistic Risk Assessment of Engineering Systems”. Chapman & Hall, London, 1997.

Wolsey (1999) L. A. Wolsey: “Integer Programming”, Wiley, Chichester, UK, 1999.

Appendix A

Table A.1:	Potential Risk Areas to an Engineering System Project
Area	**Significant Risks**
Threat	Uncertainty in threat accuracy; sensitivity of design and technology to threat; vulnerability of the system to threat and threat countermeasures; vulnerability to intelligence penetration.
Requirements	Performance requirements not properly established; requirements not stable; required operating environment not described; requirements do not address logistics and sustainability; lack of user or stakeholder participation in requirement definition.
Design	Design implications not sufficiently considered in concept exploration; system will not satisfy user requirements; mismatch of system design solutions to user needs; human-machine interface problems; increased skills or training requirements identified late in the acquisition process; design not cost effective; design relies on immature technologies or “exotic ” materials to achieve performance objectives; software design, coding, and testing not adequately planned or resourced.
Test and Evaluation	Test planning not initiated early in the project; testing does not address the ultimate operating environment; test procedures do not address all major performance and suitability specifications; test facilities not available to accomplish specific tests, especially system-level tests; insufficient time to test thoroughly.
Modeling and Simulation (M&S)	M&S tools or technologies are not verified, validated or accredited for the intended purpose; project lacks proper analysis tools and modeling and simulation capability or technologies to assess the current design or identified alternatives.
Technology	Project depends on unproven technology for success – there are no defined technology alternatives; project success depends on achieving advances in state-of-the-art technology; potential advances in technology will result in less than optimal costs or make system components obsolete; technology has not been demonstrated in required operating environment; technology relies on complex hardware, software, or integration design.

Table A.1:	Potential Risk Areas to an Engineering System Project *(Continued)*
Area	**Significant Risks**
Logistics	Inadequate supportability late in development or after fielding resulting in need for engineering changes, increased costs, and/or schedule delays; life cycle costs not accurate because of poor logistics supportability analyses; logistics analyses results not included in cost-performance tradeoffs; design trade studies do not include supportability considerations.
Production/Facilities	Production implications not considered during concept exploration; production not sufficiently considered during design; inadequate planning for long lead items and vendor support; production processes not proven; prime contractors do not have adequate plans for managing subcontractors; facilities not readily available for cost-effective production; contract offers no incentive to modernize facilities or reduce cost.
Concurrency	Immature or unproven technologies will not be adequately developed before production; production funding will be available too early – before development effort has sufficiently matured; concurrency established without clear understanding of risks.
Technical Capability of Developer	Developer has limited experience in specific type of development; contractor has poor track record relative to costs and schedule; contractor experiences loss of key personnel; prime contractor relies excessively on subcontractors for major development efforts.
Cost, Funding, Schedule	Cost – Schedule objectives not realistic; cost – schedule estimates do not reflect true program uncertainties; cost – schedule – performance tradeoffs not done; unstable requirements prevent establishing a cost – schedule baseline; funding profiles do not match acquisition strategy across annual budget cycles.
Acquisition and Program Management	Acquisition strategy understates true program challenges (e.g., performance, technology maturity, cost – schedule uncertainties, viability of industrial base, economic stability); alternatives acquisition strategies or program management options not considered or planned; inability to staff program management team with essential skill sets; risk management not performed or not effective or results ignored; none or inadequate socialization with users/stakeholders in key technical or program milestones.

Table A.2:	Some Guidelines for Identifying Risks
Step	**Guidlines**
1	Understand the requirements and the project's performance goals, which are typically defined as thresholds and objectives. Understand the operational (functional and environmental) conditions under which these values must be achieved.
2	Determine technical and performance risks related to engineering and manufacturing processes. Identify those processes that are planned or needed to design, develop, produce, support, and retire the system. Compare these processes with industry best practices and identify variances or new, untried processes. These variances or untried processes are sources of risk. The contractor should review the processes to be used by its subcontractors to ensure they are consistent with best industry practices.
3	Determine technical and performance risks associated with the engineering system project and all its subsystems (e.g., a communications subsystem) to include the following critical risk areas: design and engineering, technology, logistics, supportability, concurrency, and manufacturing.
4	Ensure cost – schedule objectives are realistic and cost – schedule estimates reflect true program uncertainties; identify whether cost – schedule – performance options exist that offer less risk but still meet user needs; work to baseline requirements and that users/stakeholders have been engaged; ensure funding profiles match acquisition strategy across annual budget cycles.
5	All identified risks are documented in a risk management database, with a statement of the risk and a description of the conditions or root cause(s) generating the concern and the context of the risk.

Appedix B

B.1 Database design

For the storage of data, Relational Data Base Management System (RDBMS) MySQL 5.0.32 is chosen for its free availability and portability. The database consists of seven tables namely component, level, global_feature_zones, risk, risk_clusters, mitigation_measures and risk_mm. The database design has been shown in figure 6.1 and a brief description of the tables is given below.

B.1.1 Table component

Table *component* keeps the information of product's components along with their hierarchal levels. Each component can be parent and child. If some component is not having any parent, zero is stored in field parent_id otherwise its parent component_id is saved.

B.1.2 Table level

All the possible levels in system hierarchy are stored in this table. The possible levels are of type 0, 1 and 2 for Major system level, Major system components and sub components of components respectively.

B.1.3 Table global_feature_zones

This table keeps the detail of Global Features and their various zones correspondingly such as Blue, Green, Yellow, and Red zones. It also keeps the information of penalty cost per unit.

B.1.4 Table risk

Information regarding the individual risks is stored in this table. This includes risk, which component is effected by this risk, total impact and its occurrence probability. Each risk can have sub risks and each having an impact on one of the Global Features. This information is also kept in this table.

B.1.5 Table risk_clusters

This table stores the risk hierarchy and their relation with any of the Global Features. For example, table row 1,2,3,1 implies risk 2 is sub risk and its parent risk 3 and it effects Global Feature having id 1. Last field 1 indicates that this Global Feature is active (in use).

B.1.6 Table mitigation_measures

Table *mitigation_measure* keeps the data of mitigation cost and its description.

B.1.7 Table risk_mm

Table *risk_mm* stores the relationship between risks and their corresponding mitigation measures.

B.2 Java Programming

The java source code consists of a number of packages. These include

- arcc.data
- arcc.db
- arcc.constants
- arcc.models
- arcc.bf
- arcc.dp
- arcc.ga
- arcc.beans

B.2.1 Package arcc.data

The classes of this package are used to generate the random data. This includes *class Risks* and *class RiskClusters*.

B.2.1.1 Class Risks

Class *Risks* generates the risks, sub risks and each sub-risk effecting one of the Global Features.

B.2.1.2 Class RiskClusters

This class forms the risk clusters and populates the table *risk_clusters*.

B.2.2 Package arcc.db

This package consists of *class MySQLDatabase*.

B.2.2.1 Class MySQLDatabase
It is responsible for connecting to mysql database.

B.2.3 Package arcc.constants

This package consists of *class Constant.*

B.2.3.1 Class Constant
It consists of number of parameters in order to set different functionalities. For example, change in objective function, budget increment in case of red zone, parameters to connect to the database such as user name and password, etc.

B.2.4 Package arcc.models

This package consists of data structures. This includes classes *GFMatrix, MMCombinations, Risk, RiskMitigation, SubRisk and ZoneLimit*.

B.2.4.1 Class GFMatrix
This class represents Global Features matrix consisting of feature id, feature zones, penalty cost and penalty unit.

B.2.4.2 Class MMCombinations
This class keeps information of mitigation measure combinations, total cost and objective function value e.g. delta risk.

B.2.4.3 Class Risk
This class contains information of risk id, its probability of failure, acceptable prbability of failure and penalty cost.

B.2.4.4 Class RiskMitigation
This class stores global feature values before and after the application of mitigation measures.

B.2.4.5 Class SubRisk
This class contains information of sub risk id, its effect on particular Global Feature and resultng penalty cost.

B.2.4.6 Class ZoneLimit

This class keeps the starting and ending limits of various zones of a certain Global Feature. These include Blue, Green, Yellow, and Red zones.

B.2.5 Package arcc.bf

This package consists of classes that are required to find the optimized mitigation plan using Brute Force algorithm. There are two classes, namely, *CombinationGenerator* and *BruteForceOMPlan*.

B.2.5.1 Class CombinationGenerator

This class generates the combinations systematically of n elements taken r at a time. This class is used to generate all the possible mitigation measures having mitigation cost less than the given budget. There is no constraint on the number of mitigations used such as only three mitigation measure combinations should be made.

B.2.5.2 Class BruteForceOMPlan

This class finds the optimized mitigation plan using Brute Force algorithm. The given below code snippet shows the main flow of finding the optimized plan. It finds all the possible combinations of mitigation measures having costs less than the given budget. It considers only those combinations which have maximum risk reduction. The function *inRedZone* checks this combination effect on the global features. If any of the global feature is in red zone then it increases the budget by 100 and repeats the whole process until it finds such a mitigation plan that costs less than the given budget and all the global features are out of red zone.

```
      boolean redZone=true;

while(redZone)
 {
    orderedMMCombinations=new ArrayList();
    for(int k=1;k<mmIDArray.length;k++){
          compute(mmIDArray, k, budget,riskMMHash);
    }

      Collections.sort(orderedMMCombinations,Collections.reverseOrer());
      mMCombinations=((MMCombinations)orderedMMCombinations.get(0));

      redZone=inRedZone(mMCombinations,riskMMHash);

      budget=budget+100;

}
```

B.2.6 Package arcc.dp

Classes that are required to find optimized plan using the dynamic programming approach included in this package.

B.2.6.1 Class Item

This class represents an item in the Knapsack problem. An item has a mitigation measure id, mitigation cost, and risk reduction information.

B.2.6.2 Class Pair

This class contains two objects of same type such as class Item and compares them.

B.2.6.3 Class DKnapSack

This class implements Dynamic Programming solution of Knapsack problem by recursive checking every combination of items.

B.2.6.4 Class DPOptimizedMitigatzionPlan

This class finds optimized plan using *class DknapSack* for a given budget. It also makes sure that all the Global Features are out of Red zone for the derived mitigation plan and budget doesn't exceed the maximum budget.

B.2.7 Package arcc.ga

This package consists of two parts, a generic Genetic Algorithm and a solution to the Knapsack problem that uses this library. The Genetic Algorithm comprised of three classes, namely, *Genotype*, *GenotypeComparator,* and *GeneticAlgorithm***.** There are four classes for knapsack solution, namely, *KnapsackItem*, *Knapsack*, *GAGraph,* and *KnapsackApplet*.

B.2.7.1 Class Genotype

This class contains a bit-vector with the *genes* and a rating to be determined by the fitness function of the Genetic Algorithm.

B.2.7.2 Class GenotypeComparator

This class is used to compare Genotypes for sorting purpose. It will actually perform reverse-sorting and places the best genotype at the front.

B.2.7.3 Class GeneticAlgorithm

This class controls a population of Genotypes for regeneration using a Genetic Algorithm.

B.2.7.4 Class KnapsackItem

This class keeps information of a specific item that can be kept into a Knapsack.

B.2.7.5 Class Knapsack

This class holds the information of a Knapsack in order to use it with the class *GeneticAlgorithm*.

B.2.7.6 Class GaGraph

This class plots the graph of generation vs. average rating and best rated score from each generation.

B.2.7.7 Class KnapsackApplet

This applet allows the user to manipulate a knapsack object and use a Genetic Algorithm to find the optimal solution.

B.2.8 Package arcc.beans

This package consists of web beans. These include classes *MM, Risk, and GFMatrix*.

B.2.8.1 Class MM

This bean communicates to either of the approaches described above for finding the optimized plan and presents it.

B.2.8.2 Class Risk

This bean collects the information of risk breakdown structure.

B.2.8.3 Class GFMatrix

This bean populates the global features from database and set the colors along with their width for various zones. The color width depends on the starting and ending zone limits.