53-81
4976

N95-32431

THE BACKGROUND AND THEORY OF INTEGRATED RISK MANAGEMENT

Final Report
NASA/ASEE Summer Faculty Fellowship Program - 1994
Johnson Space Center

Prepared by: John L. Hunsucker, Ph.D., P.E.

Academic Rank: Associate Professor

College and Department: University of Houston
Department of
Industrial Engineering

NASA/JSC

Program: Space Station

Office: Integrated Risk Management

JSC Colleague: James E. Van Laak

Date Submitted: August 5, 1994

Contract Number: NGT-44-005-803

REFERENCES

[1] Bret F. Draayer, Gary W. Carhart, and Michael K. Giles, "Optimum classification of correlation-plane data by Bayesian decision theory," *Applied Optics,* Vol. 33, No. 14, May 10, 1994, pp. 3034–3049.

[2] Kenneth Augustyn, "A new approach to automatic target recognition," *IEEE Transactions on Aerospace and Electronic Systems,* Vol. 28, No. 1, January 1992, pp. 105–114.

[3] Richard O. Duda and Peter E. Hart, *Pattern Classification and Scene Analysis,* Wiley–Interscience, New York, 1973.

[4] Keinosuke Fukunaga, *Introduction to Statistical Pattern Recognition,* Second edition, Academic Press, Boston, 1990.

[5] Richard D. Juday, "Optimal realizable filters and the minimum Euclidean distance principle," *Applied Optics,* Vol. 32, No. 26, September 10, 1993, pp. 5100–5111.

[6] Bahram Javidi and Joseph L. Horner, eds., *Real–Time Optical Information Processing,* Academic Press, Boston, 1994.

[7] Jerome Knopp, "Spatial weighting of synthetic reference objects for joint correlation by random pixel mixing," *Proceedings of SPIE,* Orlando, Florida, April 16–18, 1990, Vol. 1295, Real–Time Image Processing II, pp. 138–145.

ABSTRACT

While all good managers have always considered risk in their decision making, only recently have formal programs to do so been introduced. This report covers the logical structure behind the formulation of an integrated risk management plan (IRM). Included in the report are factors forcing the development of a formal plan to consider risk, the basic objective or purpose of an IRM, and desirable traits of such a plan. The report moves on to a discussion of background issues, seeks to formalize some definitions, and then discusses required information on threats. The report concludes with the steps for an IRM.

INTRODUCTION:

Any program should have a strong foundation that explains why the program is needed, what drives the program, what characteristics the program should possess, how the program will be used and by whom, and what the program hopes to accomplish. Said another way, every program needs a strong theoretical background that relates to not only its design but also to its usage. Action or activity demands reason. The intention of this paper is to present the beginning formulation of the background and theory of an integrated risk management program.

BACKGROUND AND PURPOSE

An integrated risk management plan, IRM, is related to helping a particular office or program incorporate risk into its decision making. The plan is tied to the entity that it supports.

Following a logical formation of ideas requires a statement of the purpose of an IRM. For reasons expressed later, a success statement is also necessary.

BASIC OBJECTIVE OF AN IRM PLAN

TO FACILITATE GOOD DECISIONS WHICH
INCORPORATE THE CONSIDERATION OF RISK
AND
MOVE TO THE FOREFRONT OF MANAGERIAL CONSIDERATION THOSE
ITEMS WHICH ARE REAL AND MEANINGFUL THREATS TO THE STATED
PURPOSE OF THE OFFICE OR PROGRAM

SUCCESS STATEMENT

THIS MODEL WILL BE SUCCESSFUL IF
IT ASSISTS IN THE DECISION PROCESS
THREATS ARE MOVED TO THE FOREFRONT
IT GETS INCORPORATED WIDELY THROUGHOUT THE SYSTEM WHICH IT
SUPPORTS

In essence, the objective statement expresses what the plan purports to do and the success statement helps to identify if the plan has successfully accomplished its objective. Note that while the two statements are similar and related, they are also somewhat different.

DRIVERS FOR IRM

All good managers have always considered risk. A reasonable question to ask then is what is new with IRM? A common question within the space station is what does IRM bring to the table? If it has always been done and good managers have always done it, why is it needed?

While it is true that risk has always been considered, what has been missing is a formal, structured program to consider risk. There are at least three drivers that mandate structure on the consideration of risk - complexity, consequence, and credibility.

Complexity

The complexity of technological decision making has increased significantly with time. Technological systems have more component parts and there are a larger number of choices for each of these parts. This increase in numbers, of course, increases the interaction between component systems. Said another way, society desires to do more than it has ever done and has more to do it with. As a specific example, the Space Station is arguably the most complex project ever undertaken by mankind.

Consequence

The consequences of technical decisions can have a much greater negative impact that ever before. One only needs to consider Chernobyl, Bhopal, and other well publicized incidents to realize that the wrong decision can wipe out a program, a product, a company, a culture, or even a civilization.

The dollar value of decisions is only one of many parameters which can be negatively impacted. The environment, culture, government, and even heredity are all candidates for damage from a bad technical decision. Never before in history has man had the capability to do so much damage and to do it so quickly.

Credibility

Given that complexity and consequence have increased, a conscientious manager is going to demand that subordinates present convincing arguments that risk has been considered. Otherwise, when this manager presents the case to upper management, credibility will be lost. As an aside, most managers would favor the consideration of a risk and perhaps the taking of a risk over the posture of never having considered the risk, particularly if the risk materializes into a negative incident.

Perhaps in the age of the slide rule, risk need not be considered formally. In the age of the computer, with rapid communications and advanced technologies, a formal program to consider risk is mandatory.

DESIRABLE TRAITS OF AN IRM PLAN

There are certain traits that are desirable in an IRM plan. These characteristics will help to identify component parts of a proposed plan.

Reproducible

Work effort that is produced by an IRM should be reproducible in the sense that given the same input and assumptions at a later date, then it should be possible to arrive at basically the same conclusions concerning risk. The logic should not decay with time.

As the program matures it is foreseeable that some early decision will be reconsidered at a much later date. At this point, the conclusions concerning risk and the logic and structure that led to these conclusions should be reproducible.

Transportable

Two different analysts, sitting in different locations and given the same data and assumptions, should arrive at somewhat the same conclusions regarding risk. As an example with the space station, analysts at JSC, KSC, MSFC, and Headquarters should have somewhat the same results given the same basic information.

Simple

Given that one of the criterion's for success is that the system be widely accepted, it must be as simple as possible. As an aside, many engineering managers have little or no training in statistics. As of this writing for example, two of five engineering undergraduate programs at the University of Houston do not require statistics To this end, a complicated statistics package will have difficulty gaining wide spread acceptance. Simpler is better and the leaner the plan, the more likely is the acceptance. The longevity of the plan is also more than likely tied to its simplicity.

Based on the normal method of doing business

The supposition here is that good managers have always considered risk management. The IRM should just fit in naturally with what the managers are used to doing. For the most part this means that the IRM should follow the same breakdown that is used to structure the work. If a work break down structure is used, for example, then the IRM should follow the same WBS structure.

Managers will have enough to learn and do without having a system imposed on them that is totally different than what they normally do. The closer this system fits with the normal work of the managers then the more likely that it will be adopted and used.

Helps to remove or identify bias

Managers use intuition. Intuition is gained by experience. Experience introduces bias. Some people are risk takers and some are risk avoiders. All are influenced by past experience. Change the experience base and the underlying factors which influence decisions may become obscured. A

desirable trait of an IRM would be to eliminate bias in the decision process. This would seem to be virtually impossible. Thus the goal becomes one of identifying and understanding the bias.

Should be capable of evolution

With time, the concept of the work will change. The IRM must change with the work. As a prime example, early on, design and development are prime considerations. Hopefully, the plan will evolve with the work into the manufacturing or operations stage.

Verifiable

One of the real worries with risk management is whether all of the important issues have been considered. Has something been overlooked that shouldn't have been? A verification step helps to provide credibility and to increase confidence that nothing major has been missed.

BACKGROUND ISSUES

The following is a brief discussion of some of the background issues related to risk management . The intent here is to provide additional insight to the plan that is developed later.

Two different uses of RM

Risk management can be used either in alternative selection, a static use, or operations/development control, a dynamic use. In the static use, RM can be used to choose between alternatives. Risk, then, becomes another variable to consider in the selection among choices. In the dynamic version of RM, risk is used to predict how well a particular plan is going to work.

Much of the literature on risk is related to the dynamic use of RM. One of the characteristics of the dynamic state is the existence of data. Having data allows for the usage of such tools as control limits. The scarcity of data and data streams makes the consideration of risk in the static usage more complex.

Risk is temporal

The objective of a program, and the related definition of success, change with time. As the definition of success changes, so must the concept of risk. As a specific example, consider the space shuttle. For its first launch, success was more than likely defined as getting it up, getting it down, and not injuring anyone or anything. After fifty launches, one would suppose that the objective would be significantly more robust.

The concept of risk being tied to time is, of course, related to the trait concerning evolution discussed above. The RM program must have the capability of changing as the program changes.

Risk is hierarchical

It would be naive to suppose that the person at the top of a very complex program would define success in the same manner as the person in charge of some small sub-element many levels down in the structure. While these concepts of success are related, they are different. Thus the risk is considered differently and, to some extent, must be managed differently.

The risk manager is like a lifeguard

The question comes up, unfortunately too frequently, as to what does the risk manager bring to the table. After all, the functional manager has some capability or they would not be the manager. What do they need the risk manger for?

As a philosophical orientation to the subject, consider a lifeguard at the local swimming pool. They are not there to stop you from swimming in deep water. They are there to warn you when the water is getting deep and to assist you if you get in over your head and cannot cope. Too some degree, the job of the risk manager is similar. They are not there to make the decision for the functional manager. They are there to warn of trouble and to assist in the event that trouble does indeed occur.

Exposure

This program, like any other innovative program, requires real, substantial involvement of upper management. If the upper management exposure is not real and tangible, then middle management will kill it off. When middle management sees that upper management has committed to the program in a real and tangible way, then they too will commit and the program has a chance.

DEFINITIONS

One of the difficulties in discussing risk is that the words, to a large degree, are known and understood by everyone. Unfortunately they are usually understood differently by different people. One of the first things to do with any risk management plan is to well define the terms and then to discipline everyone to use the terms as defined and only as defined. This, more than anything else, will help to abate the hours of discussion that the consideration of an IRM will promulgate.

The following list defines many of the terms used in the rest of this paper. While the list is not complete, it does contain the most common terms.

Threat - Any real or perceived state or condition which would or could have a negative impact on the stated purpose or success of an entity.

Note that a perceived condition is important. If people feel that something is true, then their actions are influenced, whether the thing is true or not. Also note that threat is tied to purpose, objective, and success.

Risk - Throughout this paper, risk is used in the non-technical sense. To be more precise, to some authorities, risk is the analytical product of likelihood and consequence, the mathematical expectation. In this paper, it will be used only in the vague sense.

Prodromal event - An event which is a precursor of a condition, a warning.

Unfortunately, prodromes are those things most often seen in retrospect, looking backwards, after a calamity. Storm clouds are a prodrome for rain and wind. An open barn door is a prodrome for a stolen horse.

Parameter - Something which is measured with the intention of reflecting or showing a condition or state.

In the sense that it is used here, part of the task is to determine what parameters to measure so that they, to some degree, reflect the risk that is involved.

THREATS

Must be tied to a purpose or objective

When one discusses threats, the first question is and must be - a threat to what? If one does not know what is threatened, the concept becomes fuzzy and the possibility of successful abatement becomes less likely. Too often the discussion of threat or risk is reduced to a sort of "boogie man in the closet" issue. For a threat to be real, what is threatened must be known.

Threats can be self, up, down, or across threats

Consider the tree diagram of a typical WBS chart. An office in that diagram has offices above it and below it. It also has offices which are not in the same string of offices and which can only be reached by going up, across, and then down another string.

Self threats are those against the stated purpose or objective of the given office. These are threats which that office should know and understand best. To some degree, the office will also be familiar with up and down threats. It is the across threats which may be the most obscure. It is reasonable to suppose that the given office will have less knowledge about environments far from them. It is with threats of this sort that the IRM office may be most useful.

Required information on any threat

Other than the basic assumptions and determining what the threat is to, there is some desired information on any threat. Almost any manager, when presented with a statement of threat, will want to know at least four things: confidence, warning, likelihood, and consequence.

Confidence - What confidence does the analyst have in the figures or statements presented? Is the threat information based on solid firm information or is it based on a vague feeling? The confidence that the analyst has in the figures will, to some degree, be reflected in how seriously management considers the threat.

Prodromal events - Will the threat materialize with little or no warning or will there be time to react as events unfold? Threats which materialize with little warning represent, to some degree, a less palatable threat than one which gives you plenty of time to get ready.

Consequence/impact - If the threat materializes, what will be the end result or range of results? How bad can it get?

Likelihood - Here the consideration is one of probability. How probable is the threat to materialize?

As a special consideration, the determination of likelihood and of consequence is very difficult. It is at this point that the discussion of proposed risk management plans seems to become impaled on hours and hours of circular

reasoning. For this reason, and others, in what follows, we will use a five point scale to represent each of confidence, likelihood or consequence: very low, low, moderate, high, and very high. Obviously, these words will have different interpretations in different situations. The intent is to use the term and then to let discussion add meaning to the term.

USAGE

The question now becomes one of usage. Who will use the IRM and for what will it be used? Knowing the intended usage of a system is of paramount importance in designing the system.

The plan which is described in this paper will, of course, be used by everyone. However, the end user will be upper management. They are the ones charged with the most responsibility, thus they are the ones who have the end authority on whether risk has been considered and managed. To some degree, an IRM can be considered as a security blanket for upper management.

At this point, a word about numerical representations of risk is appropriate. The danger with any parameterized system is that too much will be read into a number that is generated. The only thing that can add definition and understanding to a generated number is usage and time.

As an example, suppose the risk of a particular entity was reported to be 0.7 on a 0 to 1 scale with 0 being low and 1 being high. What does 0.7 mean? How does it compare to someone else's 0.6 or 0.8? Only use and time can add the required definition. The most important use of the number is two-fold. One is to track the number over time. In our example, if the risk went to 0.8 in the next reporting period, most managers would understand that the risk posture was getting worse. Conversely, if the risk went to 0.6, most would understand that the risk was getting better. Tracking over time and looking at the trending of the number provides insight into the risk posture. The other use of a number is to give management the opportunity to explain the number. If the risk is reported as 0.7, the obvious question is why is it 0.7 and not 0.6 or 0.8. What is the explanation for the number? Again, time and use will add definition and reason to any parameter that is produced.

THE ENVIRONMENT

In order to understand the proposed plan, a brief discussion of the author's understanding of the environment is essential. No plan can be lifted directly from one environment and placed into another without modification. The literature is replete with examples of industries and companies who have tried this and failed.

The way the work at the space station seems to be structured is that the tasks are distributed among integrated product teams (IPT's). There are somewhere around 100 such teams, depending on how they are counted. If one thinks of a typical tree structure as in a WBS the IPT's are somewhat

similar. Every so often in the structure, they have introduced an Analysis and Integration team charged with the responsibility of integrating the levels below them. The intention of this structure is to empower the teams by forcing the decision making to as low a level as possible.

THE PLAN

The basic plan is to have the IPT's report their risk posture to upper level management on a routine and regular basis. If this is done often enough, then trending will develop and information will be gained. Due to the large number of teams, some subset will have to report each time. A typical plan would have a regular time slot each week for reporting, say two hours. Then the teams would be grouped in some natural ordering following the AIT structure and each would expect to report during their time slot when their particular grouping was presenting. Their turn would come up again every four or six weeks or whatever time was appropriate. Note that this method immediately franchises the risk management program. Teams will naturally turn to the office of IRM to get help.

The upper level manager reviewing the findings will add definition to any of the parameters generated simply by asking why the team assigned a certain number to a parameter. This system might well be chaotic at the start but time will add definition, stability and insight.

STEPS FOR THE REPORT

There are five basic steps that each team will have to take in order to generate the required information: background, threats, metric, reconciliation and transition. Each of these steps will provide a integral piece of their report.

Step 1: Background

In the background step there are three separate pieces of required information:

- Determine the purpose/objective of the IPT
- Write out the success statement of the IPT
- List the ground rules and assumptions of the IPT

The purpose of the background information is to insure that everyone has the same basic understanding of the basic function of the IPT, i.e., what they are supposed to do, how they will know if they have done it, and the ground rules covering the doing. Note that all three of these pieces of information will change with time.

Step 2: Threats - Top Ten Plus One

Each IPT needs to develop a top ten plus one threat list. The first part of this report contains a list of about ten threats. The term about ten is used to allow some flexibility in the number of threats listed. The intent is to not discourage a fairly significant eleventh or twelfth threat or to encourage the manufacture of a tenth threat.

The following information should be contained with each threat:

- What it is a threat to
- Whether the threat is up, down, self, or across
- The confidence in the analysis
- The consequences
- The likelihood
- Prodromal events

Each of the above items should be expressed in a paragraph form. The confidence, likelihood, and consequence should include in their paragraph a rating on the five point scale mentioned above. A brief justification for the rating should also be included.

The second part of this report should contain a dark horse. The dark horse is presented without any justification. It is the single thing in the managers mind that is worrying them but is still vague. The intent here is to encourage them to present unsubstantiated feeling of risk to management.

This report should be formulated by the IPT and go to the AIT and to the Office of IRM. One of the functions of the IRM would be to insure that the information is circulated to the concerned offices. The report should be presented, as previously discussed, to upper management on a regular basis.

Step 3: The Metric

The intent here is to present a metric which reflects the risk to the objectives and success statements. The metric is developed by each IPT and consists of three parts. The IPT evaluates the risk to themselves. Note that this is not a trade study but an evaluation of whether the IPT feels that they can do what they are supposed to do.

Three parameters are purposed, cost, schedule, and performance. The method is to fix two of the three and then to evaluate a confidence level in being able to accomplish the third, given the first two. The confidence is to be evaluated between 0 and 1 in 0.1 increments.

- Performance

Given your current schedule and budget the confidence that you will meet your technical performance goals is_____.

- Cost

Given your current schedule and technical performance goal, the confidence that you will meet your cost goals is_____.

- Schedule

Given your current budget and technical performance goal, the confidence that you will meet your schedule is _____.

There are any number of parameters that could have been proposed. However, in the interest of developing a simple program with a chance of acceptance, these three were considered the most important.

Again, use will provide definition to these parameters. Their most significant use will come with the tracking of the parameters over time. Trending will provide upper management with a large amount of information on risk and on abatement.

The tendency to combine the three metrics into one will only obscure information and should be avoided. The recommendation that each of the three be tracked separately is yet another reason to restricting ourselves to three metrics.

It is fully expected that each IPT will avail themselves of sophisticated methods to establish the value of the parameters. It may well even be true that each IPT uses a different method. However, over time and with experience, it is reasonable to suppose that some methods will prevail and become common. Here, the intent is to let use determine the method as opposed to method determining the use.

Step 4: Reconciliation

The top ten plus one list should be compared to the three metrics generated to see if the information plays well together. Logic and consistency are important. In essence, the IPT has verified their feelings on risk by working the problem two different ways, one in paragraph form and the other with the metrics. This part of the report should be in paragraph form and discuss how the two different parts support each other.

Step 5: Transition

Risk management is dynamic. The RM plan requires a periodic review to insure it is meeting its required objectives and to insure that the objectives themselves have not changed. As the program becomes more operational in nature, significant changes in the definition of success will occur forcing changes in the IRM plan. Step 5 in the report is a paragraph discussing how the office plans to deal with the change from a risk perspective.

CONCLUSIONS

As was stated earlier in the paper, this is a tentative beginning of the development of the foundations of risk management. Surely significant changes and modifications will occur with time. The question now becomes one of whether the implementation of such a program is worth the overhead that it brings. Can a program afford to implement an IRM plan?

One of the problems with technical decision making is that non-technical people understand neither the principles involved nor the process. Given this, they have to trust the technocrat to do what is right and correct. One thing is resoundingly clear, if the community as a whole loses their faith in the technocrats to make the "good" decision, they can shut the whole process down. If Congress loses its faith in NASA, they can stop the space station. If the public loses its faith in a company, they can force financial ruin. If the auditors and accountants lose their faith in the design team they can stop a project.

Given this and given the high risk of many technical decisions, the question more properly becomes one of can a company or program afford not to institute a formal risk management plan?

54-16
47444

N95-32432

IMPLEMENTATION OF A SINGLE-STAGE-TO-ORBIT (SSTO) MODEL FOR STABILITY AND CONTROL ANALYSIS

Final Report
NASA/ASEE Summer Faculty Fellowship Program--1994
Johnson Space Center

Prepared By:	Stephen A. Ingalls, MSAE
Academic Rank:	Assistant Professor
College and Department:	United States Military Academy Department of Civil and Mechanical Engineering West Point, New York 10996
NASA/JSC	
Directorate:	Engineering
Division:	Navigation, Control, and Aeronautics
Branch:	Control and Guidance
JSC Colleague:	G. Gene McSwain
Date Submitted:	August 5, 1994
Contract Number:	NGT-44-005-803