National Aeronautics and Space Administration

SP-6105
June 1995

NASA Systems Engineering Handbook

by
Robert Shishko, Ph.D.

with contributions by
Robert Aster
Robert G. Chamberlain
Patrick McDuffee
Lee Pieniazek, Ph.D.
Tom Rowell
Beth Bain
Renee I. Cox
Harold Mooz
Lou Polaski
Mark Sluka
Guy Beutelschies
Kevin Forsberg, Ph.D.
Mary Beth Murrill
Neil Rainwater
Ron Wade

edited by
Randy Casseingham

graphics by
Stephen Brewster
John Matlock

4.6 Risk Management

Risk management comprises purposeful thought to the sources, magnitude, and mitigation of risk, and actions directed toward its balanced reduction. As such, risk management is an integral part of project management, and contributes directly to the objectives of systems engineering.

NASA policy objectives with regard to project risks are expressed in NMI 8070.4A, *Risk Management Policy*. These are to:

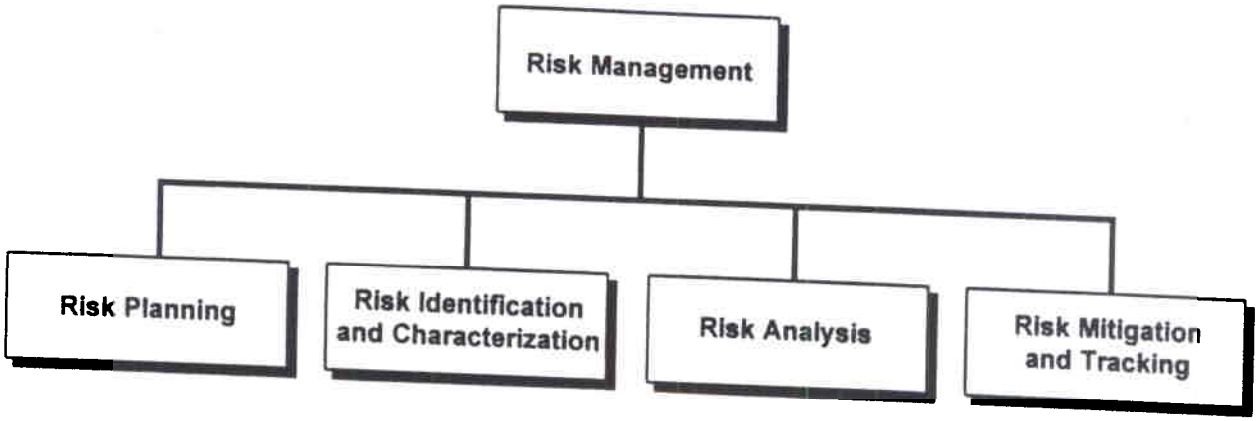


Figure 15 — Risk Management Structure Diagram.

- Provide a disciplined and documented approach to risk management throughout the project life cycle
- Support management decision making by providing integrated risk assessments (i.e., taking into account cost, schedule, performance, and safety concerns)
- Communicate to NASA management the significance of assessed risk levels and the decisions made with respect to them.

There are a number of actions the system engineer can take to effect these objectives. Principal among them is planning and completing a well-conceived *risk management program*. Such a program encompasses several related activities during the systems engineering process. The structure of these activities is shown in Figure 15.

Risk

The term *risk* has different meanings depending on the context. Sometimes it simply indicates the degree of variability in the outcome or result of a particular action. In the context of risk management during the systems engineering process, the term denotes a combination of both the likelihood of various outcomes *and* their distinct consequences. The focus, moreover, is generally on undesired or unfavorable outcomes such as the risk of a technical failure, or the risk of exceeding a cost target.

The first is planning the risk management program, which should be documented in a *risk management program plan*. That plan, which elaborates on the SEMP, contains:

- The project's overall risk policy and objectives
- The programmatic aspects of the risk management activities (i.e., responsibilities, resources, schedules and milestones, etc.)
- A description of the methodologies, processes, and tools to be used for risk identification and characterization, risk analysis, and risk mitigation and tracking
- A description of the role of risk management with respect to reliability analyses, formal reviews, and status reporting and assessment
- Documentation requirements for each risk management product and action.

The level of risk management activities should be consistent with the project's overall risk policy established in conjunction with its NASA Headquarters program office. At present, formal guidelines for the classification of projects with respect to overall risk policy do not exist; such guidelines exist only for NASA payloads. These are promulgated in NMI 8010.1A, *Classification of NASA Payloads, Attachment A*, which is reproduced as Appendix B.3.

With the addition of data tables containing the *results* of the risk management activities, the risk management program plan grows into the project's Risk Management Plan (RMP). These data tables should contain the project's identified significant risks. For each such risk, these data tables should also contain the relevant characterization and analysis results, and descriptions of the related mitigation and tracking plans (including any descope options and/or required technology developments). A sample RMP outline is shown as Appendix B.4.

The technical portion of risk management begins with the process of identifying and characterizing the project's risks. The objective of this step is to understand

what uncertainties the project faces, and which among them should be given greater attention. This is accomplished by categorizing (in a consistent manner) uncertainties by their likelihood of occurrence (e.g., high, medium, or low), and separately, according to the severity of their consequences. This categorization forms the basis for ranking uncertainties by their relative riskiness. Uncertainties with both high likelihood and severely adverse consequences are ranked higher than those without these characteristics, as Figure 16 suggests. The primary methods used in this process are qualitative; hence in systems engineering literature, this step is sometimes called *qualitative risk assessment.* The output of this step is a list of significant risks (by phase) to be given specific management attention.

In some projects, qualitative methods are adequate for making risk management decisions; in others, these methods are not precise enough to understand the magnitude of the problem, or to allocate scarce risk reduction resources. Risk analysis is the process of *quantifying* both the likelihood of occurrence and consequences of potential future events (or "states of nature" in some texts). The system engineer needs to decide whether risk identification and characterization are adequate, or whether the increased precision of risk analysis is needed for some uncertainties. In making that determination, the system engineer needs to balance the (usually) higher cost of risk analysis against the value of the additional information.

Risk mitigation is the formulation, selection, and execution of strategies designed to economically reduce risk. When a specific risk is believed to be intolerable, risk analysis and mitigation are often performed iteratively, so that the effects of alternative mitigation strategies can be actively explored before one is chosen. Tracking the effectivity of these strategies is closely allied with risk mitigation. Risk mitigation is often a challenge because

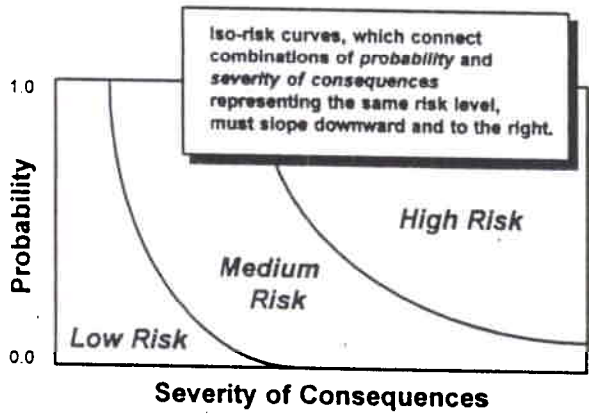


Figure 16 — Characterizing Risks by Likelihood and Severity.

Table 1 — Techniques of Risk Management.

Risk Identification and Characterization	Risk Analysis	Risk Mitigation and Tracking
Expert interviews	Decision analysis	Watchlists/milestones
Independent assessment (cost, schedule and technical)	Probabalistic Risk Assessment (PRA)	Contingency planning/ descope planning/par-allel development
Risk templates (e.g., DoD 4245.7-M)	Probabilistic network schedules (e.g., PERT)	Critical items/issues lists
Lessons learned files from previous projects	Probabilistic cost and effectiveness models (e.g., Monte Carlo models)	Cost/schedule control systems and Technical Performance Measure (TPM) tracking
FMECAs/FMEAs/Digraphs/ Fault Trees		

efforts and expenditures to reduce one type of risk may increase another type. (Some have called this the systems engineering equivalent of the Heisenberg Uncertainty Principle in quantum mechanics.) The ability (or necessity) to trade one type of risk for another means that the project manager and the system engineer need to understand the system-wide effects of various strategies in order to make a rational allocation of resources.

Several techniques have been developed for each of these risk management activities. The principal ones, which are shown in Table 1, are discussed in Sections 4.6.2 through 4.6.4. The system engineer needs to choose the techniques that best fit the unique requirements of each project.

A risk management program is needed throughout the project life cycle. In keeping with the doctrine of successive refinement, its focus, however, moves from the "big picture" in the early phases of the project life cycle (Phases A and B) to more specific issues during design and development (Phases C and D). During operations (Phase E), the focus changes again. A good risk management program is always forward-looking. In other words, a risk management program should address the project's on-going risk issues and future uncertainties. As such, it is a natural part of concurrent engineering. The RMP should be updated throughout the project life cycle.

4.6.1 Types of Risks

There are several ways to describe the various types of risk a project manager/system engineer faces. Traditionally, project managers and system engineers have attempted to divide risks into three or four broad categories — namely, cost, schedule, technical, and, sometimes, safety (and/or hazard) risks. More recently, others have entered the lexicon, including the categories of organizational, management, acquisition, supportability, political, and programmatic risks. These newer categories reflect

the expanded set of concerns of project managers and system engineers who must operate in the current NASA environment. Some of these newer categories also represent supersets of other categories. For example, the Defense Systems Management College (DSMC) Systems Engineering Management Guide wraps "funding, schedule, contract relations, and political risks" into the broader category of programmatic risks. While these terms are useful in informal discussions, there appears to be no formal taxonomy free of ambiguities. One reason, mentioned above, is that often one type of risk can be exchanged for another. A second reason is that some of these categories move together, as for example, cost risk and political risk (e.g., the risk of project cancellation).

Another way some have categorized risk is by the degree of mathematical predictability in its underlying uncertainty. The distinction has been made between an uncertainty that has a known probability distribution, with known or estimated parameters, and one in which the underlying probability distribution is either not known, or its parameters cannot be objectively quantified.

An example of the first kind of uncertainty occurs in the unpredictability of the spares upmass requirement for alternative Space Station *Alpha* designs. While the requirement is stochastic in any particular logistics cycle, the probability distribution can be estimated for each design from reliability theory and empirical data. Examples of the second kind of uncertainty occur in trying to predict whether a Shuttle accident will make resupply of *Alpha* impossible for a period of time greater than x months, or whether life on Mars exists.

Modern subjectivist (also known as *Bayesian*) probability theory holds that the probability of an event is the degree of belief that a person has that it will occur, given his/her state of information. As that information improves (e.g., through the acquisition of data or experience), the subjectivist's estimate of a probability should converge to that estimated as if the probability distribution were known. In the examples of the previous paragraph, the only difference is the probability estimator's perceived state of information. Consequently, subjectivists find the distinction between the two kinds of uncertainty of little or no practical significance. The implication of the subjectivist's view for risk management is that, even with little or no data, the system engineer's subjective probability estimates form a valid basis for risk decision making.

4.6.2 Risk Identification and Characterization Techniques

A variety of techniques are available for risk identification and characterization. The thoroughness with which this step is accomplished is an important determinant of the risk management program's success.

Expert Interviews. When properly conducted, expert interviews can be a major source of insight and information on the project's risks in the expert's area of knowledge. One key to a successful interview is in identifying an expert who is close enough to a risk issue to understand it thoroughly, and at the same time, able (and willing) to step back and take an objective view of the probabilities and consequences. A second key to success is advanced preparation on the part of the interviewer. This means having a list of risk issues to be covered in the interview, developing a working knowledge of these issues as they apply to the project, and developing methods for capturing the information acquired during the interview.

Initial interviews may yield only qualitative information, which should be verified in follow-up rounds. Expert interviews are also used to solicit quantitative data and information for those risk issues that qualitatively rank high. These interviews are often the major source of inputs to risk analysis models built using the techniques described in Section 4.6.3.

Independent Assessment. This technique can take several forms. In one form, it can be a review of project documentation, such as Statements of Work, acquisition plans, verification plans, manufacturing plans, and the SEMP. In another form, it can be an evaluation of the WBS for completeness and consistency with the project's schedules. In a third form, an independent assessment can be an independent cost (and/or schedule) estimate from an outside organization.

Risk Templates. This technique consists of examining and then applying a series of previously developed risk templates to a current project. Each template generally covers a particular risk issue, and then describes methods for avoiding or reducing that risk. The most-widely recognized series of templates appears in DoD 4245.7-M, *Transition from Development to Production ...Solving the Risk Equation*. Many of the risks and risk responses described are based on lessons learned from DoD programs, but are general enough to be useful to NASA projects. As a general caution, risk templates cannot provide an exhaustive list of risk issues for every project, but they are a useful input to risk identification.

Lessons Learned. A review of the lessons learned files, data, and reports from previous similar projects can produce insights and information for risk identification on a new project. For technical risk identification, as an example, it makes sense to examine previous projects of similar function, architecture, or technological approach. The lessons learned from the *Infrared Astronomical Satellite* (IRAS) project might be useful to the *Space Infrared Telescope Facility* (SIRTF) project, even though the latter's degree of complexity is significantly greater. The key to applying this technique is in recognizing what aspects are analogous in two projects, and what data are relevant to the new project. Even if the documented lessons learned from previous projects are not applicable at the system level, there may be valuable data applicable at the subsystem or component level.

FMECAs, FMEAs, Digraphs, and Fault Trees. Failure Modes, Effects, and Criticality Analysis (FMECA), Failure Modes and Effects Analysis (FMEA), digraphs, and fault trees are specialized techniques for safety (and/or hazard) risk identification and characterization. These techniques focus on the hardware components that make up the system. According to MIL-STD-1629A, FMECA is "an ongoing procedure by which each potential failure in a system is analyzed to determine the results or effects thereof on the system, and to classify each potential failure mode according to its severity." Failures are generally classified into four severity categories:

- Category I — Catastrophic failure (possible death or system loss)
- Category II — Critical failure (possible major injury or system damage)
- Category III — Major failure (possible minor injury or mission effectiveness degradation)
- Category IV — Minor failure (requires system maintenance, but does not pose a hazard to personnel or mission effectiveness).

A complete FMECA also includes an estimate of the probability of each potential failure. These probabilities are usually based, at first, on subjective judgment or experience factors from similar kinds of hardware components, but may be refined from reliability data as the system development progresses. An FMEA is similar to an FMECA, but typically there is less emphasis on the severity classification portion of the analysis.

Digraph analysis is an aid in determining fault tolerance, propagation, and reliability in large, interconnected systems. Digraphs exhibit a network structure and resemble a schematic diagram. The digraph technique permits the integration of data from a number of individual FMECAs/FMEAs, and can be translated into fault trees, described in Section 6.2, if quantitative probability estimates are needed.

4.6.3 Risk Analysis Techniques

The tools and techniques of risk analysis rely heavily on the concept and "laws" (actually, axioms and theorems) of probability. The system engineer needs to be familiar with these in order to appreciate the full power and limitations of these techniques. The products of risk analyses are generally quantitative probability and consequence estimates for various outcomes, more detailed understanding of the dominant risks, and improved capability for allocating risk reduction resources.

Decision Analysis. Decision analysis is one technique to help the individual decision maker deal with a complex set of uncertainties. Using the divide-and-conquer approach common to much of systems engineering, a complex uncertainty is decomposed into simpler ones, which are then treated separately. The decomposition continues until it reaches a level at which either hard information can be brought to bear, or intuition can function effectively. The decomposition can be graphically represented as a *decision tree*. The branch points, called nodes, in a decision tree represent either decision points or chance events. Endpoints of the tree are the potential outcomes. (See the sidebar on a decision tree example for Mars exploration.)

In most applications of decision analysis, these outcomes are generally assigned dollar values. From the probabilities assigned at each chance node and the dollar value of each outcome, the distribution of dollar values (i.e., consequences) can be derived for each set of decisions. Even large complex decision trees can be represented in currently available decision analysis software. This software can also calculate a variety of risk measures.

In brief, decision analysis is a technique that allows:

- A systematic enumeration of uncertainties and encoding of their probabilities and outcomes
- An explicit characterization of the decision maker's attitude toward risk, expressed in terms of his/her *risk aversion*
- A calculation of the value of "perfect information," thus setting a normative upper bound on information-gathering expenditures
- Sensitivity testing on probability estimates and outcome dollar values.

Probabilistic Risk Assessment (PRA). A PRA seeks to measure the risk inherent in a system's design and operation by quantifying both the likelihood of various possible accident sequences and their consequences. A typical PRA application is to determine the risk associated with a specific nuclear power plant. Within NASA, PRAs are used to demonstrate, for example, the relative safety of launching spacecraft containing RTGs (Radioisotope Thermoelectric Generators).

The search for accident sequences is facilitated by *event trees*, which depict initiating events and combinations of system successes and failures, and *fault trees*, which depict ways in which the system failures represented in an event tree can occur. When integrated, an event tree and its associated fault tree(s) can be used to calculate the probability of each accident sequence. The structure and mathematics of these trees is similar to that for decision trees. The consequences of each accident sequence are generally measured both in terms of direct economic losses and in public health effects. (See sidebar on PRA pitfalls.)

Doing a PRA is itself a major effort, requiring a number of specialized skills other than those provided by reliability engineers and human factors engineers. PRAs also require large amounts of system design data at the component level, and operational procedures data. For additional information on PRAs, the system engineer can reference the *PRA Procedures Guide* (1983) by the American Nuclear Society and Institute of Electrical and Electronic Engineers (IEEE).

Probabilistic Network Schedules. Probabilistic network schedules, such as PERT (Program Evaluation and Review Technique), permit the duration of each activity to be treated as a random variable. By supplying PERT with the minimum, maximum, and most likely duration for each activity, a probability distribution can be computed for project completion time. This can then be used to determine, for example, the chances that a project (or any set of tasks in the network) will be completed by a given date. In this probabilistic setting, however, a unique critical path may not exist. Some practitioners have also cited difficulties in obtaining meaningful input data for probabilistic network schedules. A simpler alternative to a full probabilistic network schedule is to perform a Monte Carlo simulation of activity durations along the project's critical path. (See Section 5.4.2.)

Probabilistic Cost and Effectiveness Models. These models offer a probabilistic view of a project's cost and effectiveness outcomes. (Recall Figure 2.) This approach explicitly recognizes that single point values for these variables do not adequately represent the risk conditions inherent in a project. These kinds of models are discussed more completely in Section 5.4.

Probabilistic Risk Assessment Pitfalls

Risk is generally defined in a probabilistic risk assessment (PRA) as the expected value of a consequence function — that is:

$$R = \sum_s P_s C_s$$

where P_s is the probability of outcome s, and C_s is the consequence of outcome s. To attach probabilities to outcomes, event trees and fault trees are developed. These techniques have been used since 1953, but by the late 1970s, they were under attack by PRA practitioners. The reasons include the following:

- Fault trees are limiting because a complete set of failures is not definable.
- Common cause failures could not be captured properly. An example of a common cause failure is one where all the valves in a system have a defect so that their failures are not truly independent.
- PRA results are sometimes sensitive to simple changes in event tree assumptions
- Stated criteria for accepting different kinds of risks are often inconsistent, and therefore not appropriate for allocating risk reduction resources.
- Many risk-related decisions are driven by perceptions, not necessarily objective risk as defined by the above equation. Perceptions of consequences tend to grow faster than the consequences themselves — that is, several small accidents are not perceived as strongly as one large one, even if fatalities are identical.
- There are difficulties in dealing with incommensurables, as for example, lives vs. dollars.

4.6.4 Risk Mitigation and Tracking Techniques

Risk identification and characterization and risk analysis provide a list of significant project risks that require further management attention and/or action. Because risk mitigation actions are generally not costless, the system engineer, in making recommendations to the project manager, must balance the cost (in resources and time) of such actions against their value to the project. Four responses to a specific risk are usually available: (1) deliberately do nothing, and accept the risk, (2) share the risk

with a co-participant, (3) take preventive action to avoid or reduce the risk, and (4) plan for contingent action.

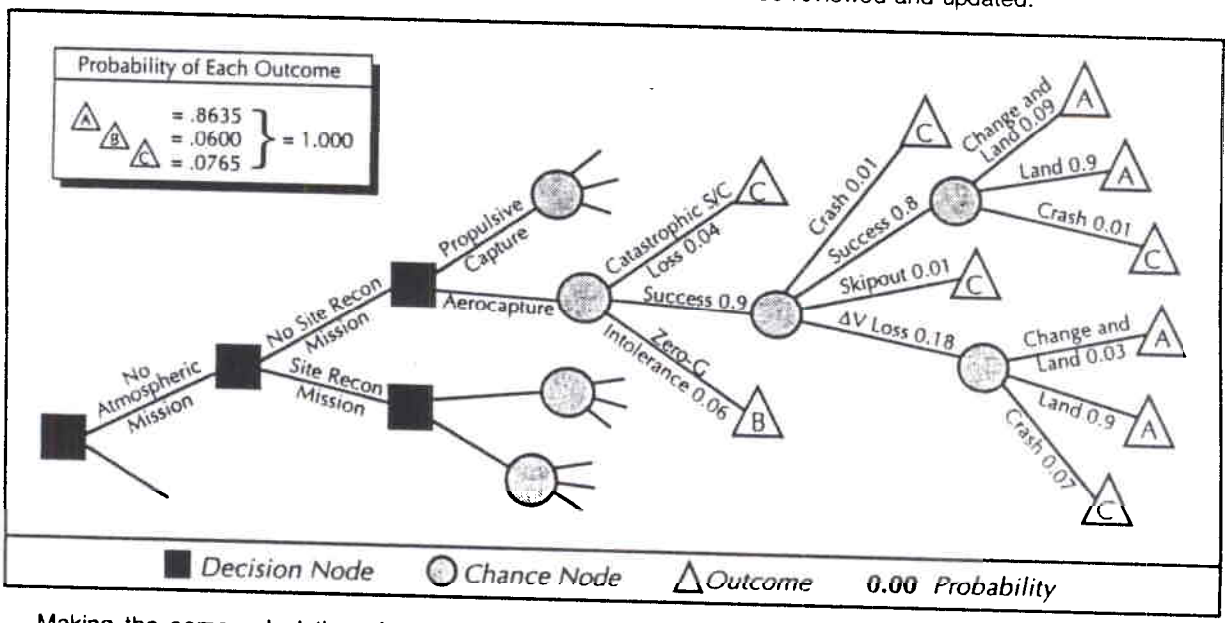
The first response is to accept a specific risk consciously. (This response can be accompanied by further risk information gathering and assessments.) Second, a risk can sometimes be shared with a co-participant — that is, with a international partner or a contractor. In this situation, the goal is to reduce NASA's risk independent of what happens to total risk, which may go up or down. There are many ways to share risks, particularly cost risks, with contractors. These include various incentive contracts and warranties. The third and fourth responses require that additional specific planning and actions be undertaken.

Typical technical risk mitigation actions include additional (and usually costly) testing of subsystems and systems, designing in redundancy, and building a full engineering model. Typical cost risk mitigation actions include using off-the-shelf hardware and, according to Figure 6, providing sufficient funding during Phases A and B. Major supportability risk mitigation actions include providing sufficient initial spares to meet the system's availability goal and a robust resupply capability (when transportation is a significant factor). For those risks that cannot be mitigated by a design or management approach, the system engineer should recommend the establishment of reasonable financial and schedule contingencies, and technical margins.

Whatever strategy is selected for a specific risk, it and its underlying rationale should be documented in a risk mitigation plan, and its effectivity should be tracked

An Example of a Decision Tree for Robotic Precursor Missions to Mars

In 1990, the Lunar/Mars Exploration Program Office (LMEPO) at JSC wanted to know how robotic precursor missions might reduce the risk of a manned Mars mission. Structuring the problem as a decision tree allows the effects of different missions and chance events to be systematically and quantitatively evaluated. The portion of the decision tree shown here illustrates the calculation of the probabilities for three distinct outcomes: (A) a successful Mars landing, (B) a safe return without a landing, or (C) a disaster resulting in mission and crew loss, when no atmospheric or site reconnaissance robotic precursor missions were made and aerocapture at Mars was subsequently selected for the manned mission. As new information becomes available, the decision tree's data can be reviewed and updated.



Making the same calculations for every branch in the decision tree allows a determination of the best mix of robotic precursor missions as an explicit function of: (a) the contribution of each robotic precursor mission to manned mission risk reduction, (b) the cost, schedule and riskiness of each robotic mission, (c) the value of the manned mission, and (d) the science value of each robotic mission in the absence of a subsequent manned mission. Another benefit of this quantitative approach is that robotic precursors can be traded against other risk mitigation strategies in the manned mission architecture.

For more information on decision analysis, see de Neufville and Stafford, *Systems Analysis for Engineers and Managers*, 1971, and Barclay, et al., *Handbook for Decision Analysis*, 1977.

through the project life cycle, as required by NMI 8070.4A. The techniques for choosing a (preferred) risk mitigation strategy are discussed in Chapter 5, which deals with the larger role of trade studies and system modeling in general. Some techniques for planning and tracking are briefly mentioned here.

Watchlists and Milestones. A *watchlist* is a compilation of specific risks, their projected consequences, and early indicators of the start of the problem. The risks on the watchlist are those that were selected for management attention as a result of completed risk management activities. A typical watchlist also shows for each specific risk a triggering event or missed milestone (for example, a delay in the delivery of long lead items), the related area of impact (production schedule), and the risk mitigation strategy, to be used in response. The watchlist is periodically reevaluated and items are added, modified, or deleted as appropriate. Should the triggering event occur, the projected consequences should be updated and the risk mitigation strategy revised as needed.

Contingency Planning, Descope Planning, and Parallel Development. These techniques are generally used in conjunction with a watchlist. The focus is on developing credible hedges and work-arounds, which are activated upon a triggering event. To be credible, hedges often require that additional resources be expended, which provide a return only if the triggering event occurs. In this sense, these techniques and resources act as a form of project insurance. (The term *contingency* here should not be confused with the use within NASA of the same term for project-held reserves.)

Critical Items/Issues Lists. A Critical Items/Issues List (CIL) is similar to a watchlist, and has been extensively used on the Shuttle program to track items with significant system safety consequences. An example is shown as Appendix B.5.

C/SCS and TPM Tracking. Two very important risk tracking techniques — cost and schedule control systems (C/SCS) and Technical Performance Measure (TPM) tracking — are discussed in Sections 4.9.1 and 4.9.2, respectively.

4.6.5 Risk Management: Summary

Uncertainty is a fact of life in systems engineering. To deal with it effectively, the risk manager needs a disciplined approach. In a project setting, a good-practice approach includes efforts to:

- Plan, document, and complete a risk management program
- Identify and characterize risks for each phase of the project; high risks, those for which the combined effects of likelihood and consequences are significant, should be given specific management attention. Reviews conducted throughout in the project life cycle should help to force out risk issues.
- Apply qualitative and quantitative techniques to understand the dominant risks and to improve the allocation of risk reduction resources; this may include the development of project-specific risk analysis models such as decision trees and PRAs.
- Formulate and execute a strategy to handle each risk, including establishment, where appropriate, of reasonable financial and schedule contingencies and technical margins
- Track the effectivity of each risk mitigation strategy.

Good risk management requires a team effort — that is, system engineers and managers at all levels of the project need to be involved. However, risk management responsibilities must be assigned to specific individuals. Successful risk management practices often evolve into institutional policy.

Appendix B.4 — A Sample Risk Management Plan Outline

1.0 Introduction
- 1.1 Purpose and Scope of the RMP
- 1.2 Applicable Documents and Definitions
- 1.3 Program/Project (or System) Description

2.0 Risk Management Approach
- 2.1 Risk Management Philosophy/Overview
- 2.2 Management Organization and Responsibilities
- 2.3 Schedule, Milestones, and Reviews
- 2.4 Related Program Plans
- 2.5 Subcontractor Risk Management
- 2.6 Program/Project Risk Metrics

3.0 Risk Management Methodologies, Processes, and Tools
- 3.1 Risk Identification and Characterization
- 3.2 Risk Analysis
- 3.3 Risk Mitigation and Tracking

4.0 Significant Identified Risks*
- 4.1 Technical Risks
- 4.2 Programmatic Risks
- 4.3 Supportability Risks
- 4.4 Cost Risks
- 4.5 Schedule Risks

* *Each subsection contains risk descriptions, characterizations, analysis results, mitigation actions, and reporting metrics .*