Proceedings of IMECE 2011
International Mechanical Engineering Conference and Exposition
November 11-17, 2011 Denver, Colorado

IMECE2011-63490

RISK ASSESSMENT OVERVIEW

Peter G. Prassinos and John W. Lyver, IV
National Aeronautics and Space Administration, Washington, DC
and
Chinh T. Bui
Hamilton Sundstrand Company, Windsor Locks, CT

Abstract

Risk assessment is used in many industries to identify and manage risks. Initially developed for use on aeronautical and nuclear systems, risk assessment has been applied to transportation, chemical, computer, financial, and security systems among others. It is used to gain an understanding of the weaknesses or vulnerabilities in a system so modification can be made to increase operability, efficiency, and safety and to reduce failure and down-time. Risk assessment results are primary inputs to risk-informed decision making; where risk information including uncertainty is used along with other pertinent information to assist management in the decision-making process. Therefore, to be useful, a risk assessment must be directed at specific objectives.

As the world embraces the globalization of trade and manufacturing, understanding the associated risk become important to decision making. Applying risk assessment techniques to a global system of development, manufacturing, and transportation can provide insight into how the system can fail, the likelihood of system failure and the consequences of system failure. The risk assessment can identify those elements that contribute most to risk and identify measures to prevent and mitigate failures, disruptions, and damaging outcomes. In addition, risk associated with public and environment impact can be identified. The risk insights gained can be applied to making decisions concerning suitable development and manufacturing locations, supply chains, and transportation strategies. While risk assessment has been mostly applied to mechanical and electrical systems, the concepts and techniques can be applied across other systems and activities. This paper provides a basic overview of the development of a risk assessment.

INTRODUCTION

The conduct of a risk assessment requires integrated and comprehensive analysis and modeling. The analysis is conducted in the context of a system's operation and environment, and accounts for the presence of hazards. The model includes all systems, subsystems, events, failures, and conditions that can have a significant impact on the results. The risk analyst studies the system's configuration; its operation, its past performance and history, and its interaction with other systems and collects data to develop an analytical model reflecting the state of the system being analyzed. For some assessments, the model and analysis must account for changes in the system's state (phased mission analysis) as a mission progresses or for processes that change from start-up to steady state operation. This paper will discuss the steps in the risk assessment process, risk definition, modeling, events, uncertainty, and application to risk-informed decision making.

RISK ASSESSMENT

Risk assessment is defined as a systematic methodology for analyzing a system, a process, or an activity to answer three basic questions:

- What can go wrong that would lead to loss or degraded performance (i.e., scenarios involving undesired consequences of interest)?
- How likely is it (probability of scenarios)?
- What is the severity of the degradation (consequences)?

The conduct of a risk assessment is the process of generating the risk triplet set, as shown in Table 1 [1]:

$$R \equiv RISK \equiv \{\langle S_i, p_i, C_i \rangle\}$$

where:

S_i is the i^{th} scenario;
p_i is the probability (or likelihood) of the i^{th} scenario; and
C_i is the consequences associated with the i^{th} scenario.

Probabilistic Risk Assessment (PRA) is the formal methodology used to derive and quantify the risk triplet for the

derived scenarios of the system, process, or activity being analyzed in an integrated manner. PRA provides a framework to prioritize risks, identify risk contributors, and quantify cumulative (aggregate) risk and associated uncertainties.

Scenario	Likelihood (Probability)	Consequence
S_1	p_1	C_1
S_2	p_2	C_2
S_3	p_3	C_3
.	.	.
.	.	.
.	.	.
S_N	p_N	C_N

Table 1: Scenarios, Probabilities, and Consequences

A SYSTEMS VIEW

A system is a combination of elements that function to produce the capability required for a desired outcome. The elements include hardware, software, equipment, personnel, facilities, processes, procedures, and resources which can collectively be called assets. All assets are subject to various threats dependent on the system configuration, contained hazards, and operating environment. Threats are the initiating events in a risk assessment and include internal hardware and software failures, external environmental or physical events (such are earthquakes, wildfire), unintentional human error, or intentional events (such as terrorist acts). Systems are designed with controls to prevent threats from impacting assets. However, not all threats will be prevented from reaching the asset. When that occurs, the asset will respond to the impact. This response is dependent on the system configuration, the nature of the threat, and the failure mechanism of the preventative controls. Realizing that affected assets can cause harm, systems are designed with controls to mitigate undesired outcomes. These controls eliminate or reduce consequences that can occur from the response of the asset to a particular threat and preventative control failure. Consequences can be injury, fatality, loss of property, monetary loss, etc. and are dependent on the makeup of the system. A systems look at risk assessment is shown in Figure 1.

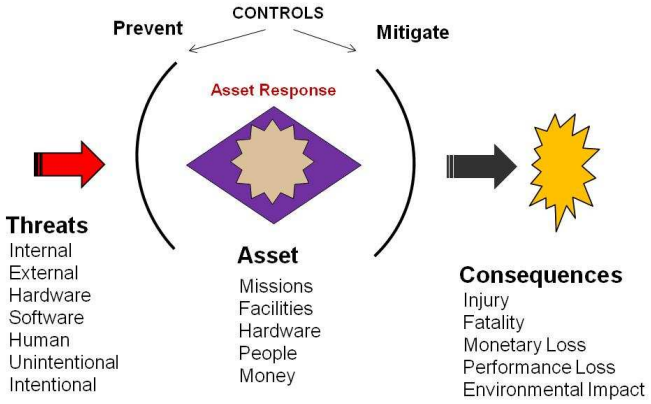


Figure 1: A systems look at risk assessment

In a risk assessment, each of these elements is evaluated in a comprehensive and integrated manner. In a PRA, the probabilities of each element are determined along with their uncertainties to assess the overall probabilities of identified consequence.

STEPS IN THE PRA METHODOLOGY

A scenario-based risk assessment involves the following steps:

- Definition of objective
- System familiarization
- Identification of initiating events
- Scenario modeling
- Failure modeling
- Quantification
- Uncertainty analysis
- Sensitivity analysis
- Importance ranking
- Data analysis

Definition of Objectives

The objective of the risk assessment must be well defined and directed toward its intended use, particularly to be used for risk-informed decision making. The objective should include the identification and selection of the undesired consequences of interest (end states): harm to humans (e.g., injury, illness, or death), degradation of functional capabilities, loss of operability, property losses, or other consequences. Depending on the scope of the PRA, applicable system configuration, and time frame; rules for considering initiators (i.e., whether to include external events) should be defined. Rules for both scope and detail should be developed and reviewed by the intended users of the PRA results.

System Familiarization

Familiarization with the system under analysis includes all relevant design and operational information, engineering and process drawings, as well as operating and emergency procedures. If the PRA is performed on an existing system that has been operated for some time, the engineering information should be on an as-built or as-operated basis rather than on an as-designed system. Visual inspection of the system being analyzed is recommended. The purpose of this effort is to become thoroughly familiar with the system and its operation, and to gain an understanding of the success states needed for proper function and operation.

Identification of Threats or Initiating Events

A complete set of threats or initiating events (events that trigger subsequent scenarios) should be identified and analyzed. These events initiate scenarios leading to defined end states. Events in a set of scenarios leading to the same end state but having very low probabilities can be screened out. The identification of the initiating events can be accomplished with special types of top-level logic trees called master logic diagrams (MLD). Additional techniques, like Failure Modes and Effects Analysis (FMEA), can also be used to identify initiators. Independent initiating events can be grouped according to the similarity of challenges that they pose to the system (system responses that result from their occurrence). When initiating events are treated as a group, their frequencies should be summed to derive the group initiator frequency.

Scenario Modeling

A scenario is a sequence of events starting with the threat (or initiating event) progressing through pivotal event(s) leading to the undesired end states as shown in Figure 2.

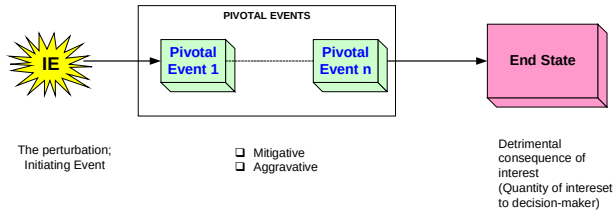
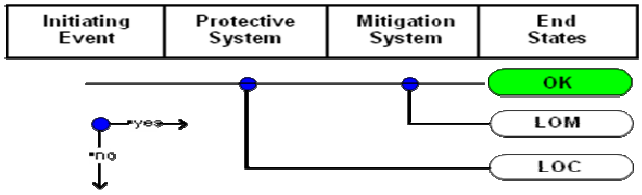


Figure 2: An accident scenario

The modeling of scenarios is an inductive process that usually involves tools called event trees. An example of a simple event tree is shown in Figure 3. An event tree starts with the initiating event and progresses through the scenario, a series of successes or failures of intermediate events (also called pivotal events or top events), until end-states are reached. Sometimes, a graphical tool called an event sequence diagram (ESD) is used to describe an accident scenario, because this type of diagram better suits engineering thinking than does an event tree. An ESD is shown in Figure 4. An ESD is logically equivalent to an event tree. Other types of inductive modeling tools can also be employed.



Note: LOM = loss of mission, loss of function: LOC = loss of crew, loss of personnel

Figure 3: A simple event tree

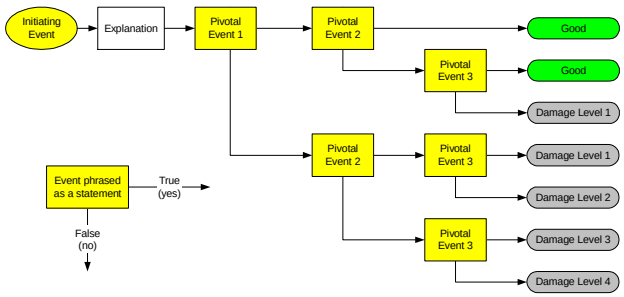


Figure 4: An event sequence diagram

Failure Modeling

The modeling of the failure (or its complement, success) of each pivotal event or event tree top event is a deductive process that usually involves tools called fault trees. A fault tree consists of three parts. The top part is the top event, which corresponds to the failure of a pivotal event in the accident scenario. The middle part consists of intermediate events (faults) that can cause failure of the top event. These events are linked through logic gates (e.g., AND gates and OR gates) to the bottom part of the fault tree. The events at the bottom of the fault tree are called basic events, whose failure ultimately led to the occurrence of the top event. A fault tree is shown in Figure 5. The fault trees are then linked to the accident scenarios and simplified (using Boolean reduction rules) to support quantification. Other deductive modeling tools can also be employed to evaluate the failure of top events.

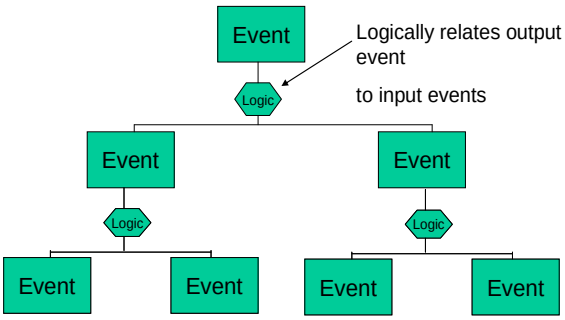


Figure 5: A fault tree

Quantification

Quantification refers to the process of estimating the frequency and the consequences of the undesired end states. The frequency of occurrence of each end state is calculated using a fault tree linking approach resulting in the logical product of the initiating event frequency and the (conditional) probabilities of each pivotal event along the scenario path from the initiating event to the end-state. The fault trees for each pivotal event are linked to the event tree to quantify the pivotal events in terms of the basic events. A diagram for event tree and fault linking is shown in Figure 6. All like end states are then grouped; i.e., their probabilities are logically summed into the probability of the representative end-state

Uncertainty Analysis

Uncertainty is a term used to describe an imperfect state of knowledge or a variability resulting from a variety of factors including, but not limited to, lack of knowledge, applicability

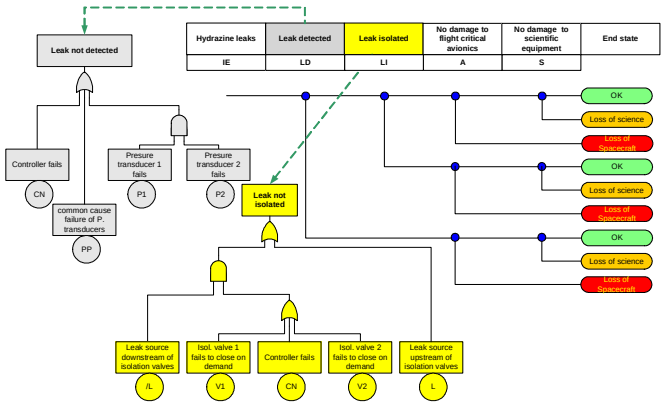


Figure 6: Event tree and fault linking

of information, physical variation, randomness or stochastic behavior, indeterminacy, judgment, and approximation.

There are two types of uncertainty:

- Aleatory uncertainty associated with variation or stochastic behavior in physical properties or physical characteristics of the systems addressed.

  This term pertains to stochastic events, the outcome of which is described by a probability. It is derived from the Latin “alea” (game of chance, die).

- Epistemic uncertainty associated with lack of completeness in the analysts’ state of knowledge – reducible in principle given additional information.

  This term pertains to the degree of knowledge of events. It is derived from the Greek “episteme” (knowledge).

A PRA attempts to model uncertain events, and the risk model is effectively an uncertainty analysis model. Recognition of uncertainty analysis as the fabric of the PRA model is paramount to proper application of PRA results in the RM decision-making process. It is incumbent on the PRA analyst to find ways to quantify and present the uncertainty associated with risk results in a manner that is understandable to decision makers. Any PRA insights reported to decision makers should include an appreciation of the overall degree of uncertainty about the results and an understanding of which sources of uncertainty are critical to the results. Monte Carlo simulation methods are generally used to perform uncertainty analysis.

Sensitivity Analysis

One type of uncertainty analysis is sensitivity analysis that focuses on modeling uncertainties in assumptions, modeling and basic events. These analyses are frequently performed in a PRA to indicate those analysis inputs or elements whose value changes cause the greatest changes in partial or final risk results.

Ranking

In some PRA applications, special techniques are used to identify the lead, or dominant, contributors to risk in accident sequences or scenarios. The ranking of these lead or dominant contributors in decreasing order of importance is called importance ranking. This process is usually performed using the fault trees and the event trees.

Data Analysis

Data analysis refers to the process of collecting and analyzing information in order to estimate various parameters of the PRA models. These parameters are used to obtain

probabilities of the various events including component failure rates, initiator frequencies, and human failure probabilities. An example of an event probability distribution is shown in Figure 7. Developing a PRA database of parameter estimates involves: (1) identification of the data needed; (2) data collection; and (3) parameter estimation using statistical methods to develop uncertainty distribution for the model parameters. In cases where there are no statistically significant data to support PRA parameter estimation, the PRA analyst may need to rely on expert judgment. The data analysis task proceeds in parallel or in conjunction with the steps described above.

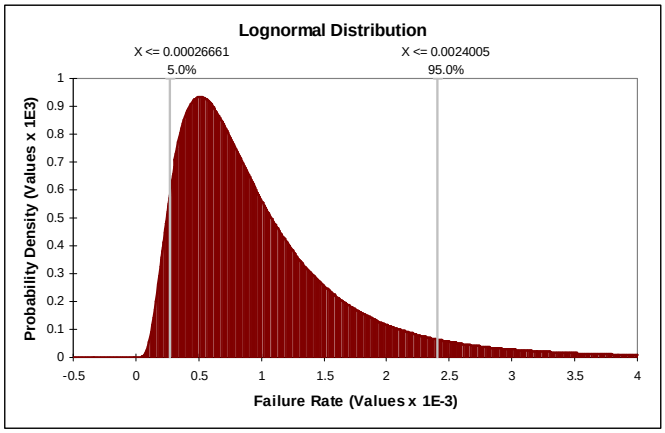


Figure 7: Example of event probability distribution

RISK ASSESSMENT IN RISK-INFORMED DECISION MAKING

Traditional decision making uses mostly "deterministic" safety modeling techniques. Probabilities are not quantified and uncertainties are managed using margins.

In a risk informed approach, decision alternatives are evaluated using both traditional safety methods and probabilistic risk assessment (PRA) approaches. The quantitative and qualitative results of the risk assessment (including scenario probabilities, consequences, and uncertainties) are used to inform the decisions. The risk-informed decision-making process is depicted in Figure 8.

Figure 8: Risk-informed decision making

SUMMARY

Risk assessment is powerful methodology when used to gain insight on the weaknesses or vulnerabilities in system processes and operations.

A risk assessment:

- is a comprehensive and systematic decision analysis tool;
- is integrated and multidisciplinary;
- provides insight into how a system fails;
- provides insights into how various systems interact with one another;
- quantifies uncertainties and identifies what the system safety analysts knows or does not know;
- provides a structure for trade studies;
- identifies the dominant accident scenarios, so that risk management decisions are targeted toward risk significant hazards; and
- quantifies the risk significance of contributing elements.

Risk assessment is a powerful tool when used to assist decision making. When applied to the globalization of trade and manufacturing, risk assessment can lead to system adjustments and changes to increase operability, efficiency, and safety and to reduce failures and down-time.

References

[1] S. Kaplan and B.J. Garrick, On the Quantitative Definition of Risk, Risk Analysis, 1, 11-27, 1981.
[2] Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, August 2002.
[3] Fault Tree Handbook with Aerospace Applications, August 2002.

[NASA/CP-2011-217247]