# Probabilistic Risk Assessment: What Is It And Why Is It Worth Performing It?

**Dr. Michael Stamatelatos**
**NASA Office of Safety and Mission Assurance**

## What is Probabilistic Risk Assessment?

*Probabilistic Risk Assessment (PRA)* has emerged as an increasingly popular analysis tool especially during the last decade. PRA is a systematic and comprehensive methodology to evaluate risks associated with every life-cycle aspect of a complex engineered technological entity (e.g., facility, spacecraft, or power plant) from concept definition, through design, construction and operation, and up to removal from service.

*Risk* is defined as a feasible detrimental outcome of an activity or action (e.g., launch or operation of a spacecraft) subject to hazard(s). In a PRA, risk is characterized by two quantities: (1) the *magnitude* (or *severity*) of the adverse *consequence*(s) that can potentially result from the given activity or action, and (2) by the *likelihood* of occurrence of the given adverse consequence(s). If the measure of consequence severity is the number of people that can be potentially injured or killed, risk assessment becomes a powerful analytic tool to assess safety performance.

If the severity of the consequence(s) and their likelihood of occurrence are both expressed qualitatively (e.g., through words like high, medium, or low), the risk assessment is called a *qualitative risk assessment*. In a *quantitative risk assessment* or a *probabilistic risk assessment*, consequences are expressed numerically (e.g., the number of people potentially hurt or killed) and their likelihoods of occurrence are expressed as *probabilities* or *frequencies* (i.e., the number of occurrences or the probability of occurrence per unit time).

Probabilistic Risk Assessment usually answers three basic questions:

1. What can go wrong with the studied technological entity, or what are the *initiators* or *initiating events* (undesirable starting events) that lead to adverse consequence(s)?

2. What and how severe are the potential detriments, or the adverse *consequences* that the technological entity may be eventually subjected to as a result of the occurrence of the initiator?

3. How likely to occur are these undesirable consequences, or what are their *probabilities* or *frequencies*?

The answer to the first question requires technical knowledge of the possible causes leading to detrimental outcomes of a given activity or action. In order to focus on the most Important initiators while screening out the unimportant ones, logic tools like Master Logic Diagrams (MLD) or Failure Modes and Effects Analyses (FMEA) have been successfully used. The answers to the second and third questions are obtained by developing and quantifying *accident* (or mishap) *scenarios*, which are chains of events that link the initiator to the end-point detrimental consequences.

The answer to the second question is obtained from *deterministic* analyses (e.g., thermal, fluid, structural or other engineering analyses) that describe the phenomena that could occur along the path of the accident scenario when the initiator and the other subsequent events (through the detrimental consequences) take place. The methods used for these deterministic evaluations depend on the specifics of the technology involved.

The answer to the third question is obtained by using Boolean Logic methods for model development and by probabilistic or statistical methods for the quantification portion of the model analysis. Boolean logic tools include *inductive* logic methods like *event tree analysis* (ETA) or *event sequence diagrams* (ESD) analysis and *deductive* methods like *fault tree analysis* (FTA). In cases when the probability of an event is well known from past experience statistical *actuarial* data can be used if the uncertainty in these data are acceptably low. For rare events (e.g., system failures), for which there is no past failure experience at all or the data are very sparse, probabilistic failure models are developed with deductive logic tools like fault trees, or inductive logic tools like *reliability block diagrams* (RBD) and FMEAs.

The final result of a PRA is given in the form of a *risk curve* and the associated uncertainties. The risk curve is generally the plot of the frequency of exceeding a consequence value (the ordinate) as a function of the consequence values (the abscissa). If the risk assessment is qualitative, the result can be represented as a two-dimensional matrix showing probability categories versus consequence categories.

In addition to the above model development and quantification, PRA studies require special but often very important analysis tools like *human reliability analysis* (HRA) and dependent-failure or *common-cause analysis* (CCF). HRA deals with methods for modeling human error while CCF deals with methods for evaluating the effect of inter-system and inter-component dependencies which tend to cause significant increases in overall system or facility risk.

PRA studies can be performed for *internal initiating events* as well as for *external initiating events*. Internal initiating events are here defined to be hardware or system failures or operator errors in situations arising from the normal mode of operation of the facility. External initiating events are those encountered outside

the domain of the normal operation of a facility. Initiating events associated with the occurrence of natural phenomena (e.g., earthquakes, lightning, tornadoes, fires and floods) are typical examples of external initiators.

What are the benefits of PRA?

Early forms of PRA had their origin in the aerospace industry before and during the Apollo space program. Later on, other industries (e.g., nuclear power industry, chemical industry), US Government laboratories and US Government agencies expanded PRA methods to higher levels of sophistication in order to assess safety compliance and performance. In recent years, Government regulatory agencies, like the Nuclear Regulatory Commission and the Environmental Protection Agency have begun to use *risk-based* or *risk-informed regulation* as a basis for enhancing safety without applying undue conservatism. The use of PRA is expected to grow both in the Government and in the private sectors.

Early on, industry began using PRA reluctantly, at the request of some regulatory agencies, to assess safety concerns. For example, the NRC required that each nuclear power plant in the US perform an *independent plant evaluation* (IPE) to identify and quantify plant vulnerabilities to hardware failures and human faults in design and operation. Although no method was specified for performing such an evaluation, the NRC requirements for the analysis could be met only by applying PRA methods.

After completing the compulsory PRA efforts, however, performing organizations usually discovered benefits beyond mere compliance with regulation. These have included new insights into and an in-depth understanding of:

- Design flaws and cost-effective ways to eliminate them in design prior to construction and operation;

- Normal and abnormal operation of complex systems and facilities even for the most experienced design and operating personnel;

- Design flaws and hardware-related, operator-related and institutional reasons impacting safety and optimal performance at operating facilities and cost-effective ways to implement upgrades;

- Approaches to reduce operation and maintenance costs while meeting or exceeding safety requirements;

- Technical bases to request and receive exemptions from unnecessarily conservative regulatory requirements.

PRA studies have been successfully performed for complex technological systems at all phases of the life cycle from concept definition and pre-design through safe removal from operation. The amount of probabilistic failure information that is available as input to the quantification process of PRA models dictates the accuracy of the results and their uncertainties. Thus, at the concept definition and pre-design levels of a first-of-a-kind system, the necessary specific failure information is sparse or simply does not exist. For these cases, data can be adapted or *specialized* (by mathematical techniques) from generic or similar sources and the results of the PRA are more useful to perform *relative* risk comparisons and risk ranking rather than to perform *absolute* (or *bottom line*) risk evaluations. Nevertheless, even for these types of applications, performing a PRA has proven to be an extremely valuable tool to improve concepts and designs cost-effectively.