Q

Probabilistic Risk Assessment (PRA)

OSMA Information Paper 00-002 July 2000

Probabilistic risk assessment (PRA) has become a rigorous technical discipline that has been used in countless complex technological applications to reveal design, operation and maintenance vulnerabilities, to enhance safety and to reduce costs. A typical PRA process is as follows.

First, the **objective** of the risk assessment must be well defined and, associated with it, the undesirable consequences of interest (**end states**) must be identified and selected. These may include items like degrees of harm to humans (e.g., injuries or deaths) or degrees of loss of a mission.

Familiarization with the system under analysis is the next step. This covers all relevant design and operation information including 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 must be on the **as-is** rather than on the **as-designed** system. Visual inspection of the system at this point is recommended if possible.

Next, the complete set of important **initiating events**, the trigger event for each series of mishaps (**accident scenario**) leading to the end states, must be identified and the unimportant ones screened out. This can be accomplished with special types of top-level fault trees, called **master logic diagrams** (**MLD**).

The modeling of each accident scenario can be accomplished with **inductive logic** and probabilistic tools called **event trees**. An event tree starts with the initiating event and progresses through a series of successes or failures of intermediate events, called **pivotal events**, until an end state is reached. Sometimes, a graphic tool called **event sequence diagram (ESD)** is first used to describe an accident scenario because it lends itself better to engineering thinking than does an event tree. The ESD must then be converted to an event tree for quantification. The failure (or of its complement, success) of each pivotal event (also called **top event**) is usually modeled with **deductive logic** and probabilistic tools called **fault trees**.

A fault tree consists of a **top event** (the failure of the pivotal event), a middle structure of **intermediate events** (failures) causing the failure of the top event which are linked with **logic gates** (e.g., **AND gates** and **OR gates**), and **basic events**. These are simple events whose failure ultimately causes the top event to occur. The fault trees are then simplified (**Boolean reduction**) and quantified to yield the failure probability of each pivotal event in each scenario. Then the probability of occurrence of each end state is calculated and the probabilities of all like end states are summed up.

Following quantification of risk, **uncertainty** and **sensitivity analyses** are performed. The former evaluate the degree of knowledge or confidence in the calculated numerical risk results and the latter indicate what input changes are the analysis results most sensitive to. **Monte Carlo simulation** methods are generally used to perform uncertainty analysis.

When the PRA is complete, special techniques are often used to identify what lead contributors to risk in accident sequences. The ranking of these contributors in decreasing order of importance is called **importance ranking**. Last, but not least, it must be mentioned that various types of data must be collected and processed for use throughout the PRA process. This activity is called **data collection, analysis and development**.

For further information: **Dr. Michael Stamatelatos, HQ, (202) 358-1668, mstamate@hq.nasa.gov**