Uses and Misuses
of
Probabilistic Safety Assessment
at
DOE's Defense Nuclear Facilities

Presented at the
PSA-99, International Topical Meeting
on Probabilistic Safety Assessment
Willard Inter-Continental Hotel
Washington, DC
August 23, 1999

Herbert John Cecil Kouts
Board Member
Defense Nuclear Facilities Safety Board
Washington, D.C.

Uses and Misuses of Probabilistic Safety Assessment at DOE's Defense Nuclear Facilities

The Department of Energy (DOE) is not a prime user of the most sophisticated methods of Probabilistic Safety Assessment (PSA). Its facilities are diverse in nature and function, a feature that prevents construction of a well-fed database that would permit widely applicable analysis of event trees and fault trees. Yet DOE has used and uses PSA in some forms.

The Nuclear Regulatory Commission (NRC) on the other hand has recently become committed to a regulatory framework termed "risk informed regulation." Presumably this means that the NRC seeks to achieve the maximum benefit possible from analysis of risk for all its activities. Among these are all of the nuclear power plants that have been subject to full Level 3 risk assessments, with the implications for possible improvement of safety in individual cases.

Yet the Nuclear Regulatory Commission is not alone in its quest to increase and improve the use of risk information in regulatory decision-making. Since 1993 the Department of Energy and indeed all US regulatory bodies have been under a mandate to use some form of risk assessment in the management of safety and health. This requirement stems from Executive Order 12866, *Regulatory Planning and Review*, which requires the following of each regulatory agency: "In setting regulatory priorities, ...consider, to the extent reasonable, the degree and nature of the risks posed by...activities within its jurisdiction." The Order also requires the use of cost/benefit analysis in the regulatory process. Since DOE regulates the health and safety of facilities and organizations subject to its control, the executive order applies to it as well.

The process by which risk is to be taken into account is not spelled out by the executive order. In the first place, risk is not definitively defined by the Order. The concept of risk has been subject to controversy ever since it was first injected into probabilistic safety assessment by the Rasmussen Report, WASH-1400. Many have opposed its use as in WASH-1400. Some are opposed because it implicitly seems to give equal standing to high-probability, low-consequence events and low-probability, high consequence ones. Some believe that the high-consequence events deserve disproportionate weighting in any scheme that compares assessed risks from different scenarios or one that integrates them into a single index of risk. Others prefer to regard the concept of risk as equivalent to hazard. Any degree of risk is then a mark of danger implying a need to avoid.

Probabilistic safety analysis is commonly used when the statistical expectation of an event cannot be derived from the historical record, because the record is either void or so scanty as to be not useful. The first vague application of the concept actually dates back to the report WASH-740 of ill fame. The authors of that report not only estimated a set of consequences that were perhaps relatively useless then because of their remote likelihood, but they also conducted what today would be called an expert solicitation of the probability of an accident with severe consequences. Interestingly, that ancient expert solicitation led to a value of about 10^{-6} per reactor year, a value in the range of probabilities now estimated for occurrence of a large reactor accident. Looked at in this way, WASH-740 led to estimates of probability and consequence for a single accident bin. At the time there really was no design of a modern nuclear plant with its full containment and its engineered safety features, so these results were if anything fortuitous.

WASH-740 and its successor study in 1965 as well as WASH-1400 in 1973 responded to requests from Congress for estimates of probabilities and consequences of accidents. Congress sought actuarial help for structuring the Price-Anderson compensation legislation of that era (how the form and intent of the legislation by that name have changed!). Because of the intended use in connection with commercial nuclear plants, the techniques and applications of Probabilistic Safety Assessment have been closely structured along lines useful to the mission of the Nuclear Regulatory Commission in regulation of the nuclear power industry. During that period of existence of the Atomic Energy Commission when those reports were being developed and used, little or no attention was given to probabilistic methods by that part of the Commission which was later folded into the Department of Energy and which had other responsibilities, such as those dealing with research activities and with the production of nuclear weapons. That is part of the reason for late attention that those engaged in activities in these areas have given to probabilistic methods. The remainder of the reason I have already mentioned; the diversity of activities in DOE does not foster use of such a systematic process.

There have, however, been probabilistic safety analyses of some nuclear reactors operated for the Department of Energy. Such an analysis was conducted for the K-Reactor at the Savannah River site in the early 1990s, when that reactor was awaiting the restart that never took place. PSAs have also been done for some of the larger research reactors operated for DOE. Needless to say, these PSAs profited to some extent from the large data banks that have been a basis for the analysis for commercial nuclear plants. But since these data banks have not been particularly suited to DOE's reactors, the uncertainty margins have been larger when such extrapolation of data from those data banks has taken place. Also, I do not know of any special results of these analyses that have proved useful as sources of improvement of safety of the systems.

In late 1990, DOE promulgated formal requirements for the performance of quantitative risk assessment for credible accidents that could lead to dispersal of plutonium during nuclear explosive operations. In the early 1990s, a study was conducted by groups from the weapons laboratories, of operations conducted for DOE with the B-57 and the B-83 weapon systems. This study, called *The Tri-Lab Study*, was undertaken to determine if quantitative risk assessment would be of value in estimating and possibly improving the safety of operations with nuclear explosives. A second objective was to determine the utility of risk acceptance criteria for these activities.

Because of the paucity of defendable failure data, the *Tri-Lab Study* relied heavily on the use of expert panels for estimates of both probability and consequences in fault trees and event trees. The study concluded that the real benefit of use of the PSA methodology was to be found in reduction of risk through improvements in design of processes and safety features. As has been the case in applications to commercial nuclear reactors, these benefits were identified through event trees that stood out as principal contributors to risk. The studies showed that specific characteristics of certain weapon systems and certain aspects of processes to be conducted with them were sources of most of the risk. These conclusions had great value in considerations of structure of the enduring stockpile of nuclear weapons, to be retained for the nation's defense. That value was real even though uncertainties in input data made precise values of risk evaluated in the studies not dependable. Estimates of relative risk are generally more reliable than those of absolute risk, because in comparisons much of the input data tends to cancel out.

More often, DOE relies on a combination of deterministic analysis and simplified probabilistic methods. The probabilistic analysis is begun as usual by construction of event trees to specify the initiating events and the sequential developments that could lead to release of radioactive material. At this point the generalists who are conducting the analysis postulate the branching probabilities in the event trees as single sets of paired numbers adding to unity for each branching into alternative possibilities, such as failure and success. This is done through use of the best available information. Expert elicitation methods are not commonly used. Estimation of consequences may use methods ranging up to the most sophisticated available. We might term this a semi-quantitative estimation of risk, since the value of probability is determined in relatively coarse treatment of event trees, using judgements of probabilities by the analysts while the estimate of consequences is made through a more dependable deterministic and quantitative calculation.

In 1994, analysts from the Los Alamos National Laboratory , the Sandia National Laboratory, and the Pantex Plant conducted safety assessments of the process of disassembly of the B-61 nuclear weapon to quantify the risk of the operations posing the greatest hazards, for the purpose of deciding on best processes before the final disassembly procedures were set. Two methods of analysis were used in parallel, one the semi-quantitative method and the other attempting a more complete Probabilistic Safety Analysis. Estimates were made of the relative advantages and disadvantages of the two methods. The semi-quantitative method was determined to provide an appropriate balance between a simple best estimate of hazard and a full PSA with the accompanying expense and time.

DOE’s Orders require use of deterministic methods to define the precautionary measures that must be singled out in protection of workers and the public. Considerations similar to those used to specify the initiating events in PSAs define accident sequences that might call for special protective measures. Special protective features of systems that serve to ensure an offsite dose less that 25 Rem to any member of the public are defined as safety class, and special requirements are laid out to ensure their function ability and effectiveness. This requirement is approximately equivalent to assurance that DOE’s operations are in accord with NRC’s reactor site criteria. Other features that would serve to prevent serious injury or fatality to workers are defined as safety-significant class, but the serviceability of these measures is less well-specified. Note that the 25 Rem limit attached to safety class systems is generally CEDE (committed effective dose equivalent), because few of DOE’s operations these days carry any threat of short-term dose such as that which might follow an accident to a nuclear power plant. The use of effective committed dose rather than short-term dose means that in this respect DOE's requirements exceed those of NRC's reactor site criteria.

The semi-quantitative methods have some applications which many of us on the Defense Nuclear Facilities Safety Board regard as questionable in some respects. In hazard analysis for operations involving nuclear weapons, DOE has chosen to use a table known as the Target Levels of Control, which sets *a priori* goals for the type and number of controls that must be adopted for a given scenario in light of estimated consequences absent the controls. This Table is shown in my only slide. Note that the categorization of accidents as anticipated, unlikely, etc is made qualitatively, although a natural tendency would lead a user to associate each bin with a rough quantitative likelihood. The questionable aspect of the application is attached to the definition of preventive or mitigative measures associated with each bin. The accompanying text notes that preventive measures are to be preferred over mitigative ones. These notes also state that each engineered preventive safety control designed according to safety class philosophy can reduce the likelihood of an accident by approximately 10^{-3} to 10^{-4} on a per year basis. It is stated that an acceptable administrative control might reduce the likelihood by 10^{-1} or 10^{-2} on a per year basis. The approximate objective relative to nuclear detonation is to reduce the likelihood to a value below 10^{-8} per year.

If use of the Target Levels of Control were to always be made as originally intended, with engineered controls and administrative controls as effective as is assumed, the methodology would have considerable attraction. But one problem is the variability of effectiveness of different possible controls. Some can be so effective as to be worth several of others, and some could be ineffective or almost so. The documentation attached to the Table is careful to point out that this is only guidance, and that intelligent application of protective measures must be used in every case. Sometimes more protection could be needed; at other times less would suffice. I agree that intelligent use would always be required. But if the intelligent capability is there, the guidelines as to number of controls should not be necessary. I am concerned that the tendency over time will be to focus on the number of controls stated for each box in the table, with less and less attention on the real objective of preventing the accident. Then the game would be reduced to seeking the least inconvenient sets of controls that would be compatible with the numerology of the table.

There is one other concern as to actual methods that have been used by DOE's sites at different times. This affects operations at all facilities including those subject to the Target Levels of Control. There appears to be a weakness in specification of requirements for a protective system that is based on defense-in-depth. One sees on looking into operations that the defense is there, generally in the form of documents internal to the operations of the contractor conducting the operation, but the requirement for the defense in depth was not well stated, and there is no clear requirement that DOE as the owner of the facility should ensure its presence. The game is not won at the point where measures are in place ensuring that no accidents expose people off-site to radiation doses exceeding the guideline value of 25 Rem. In fact, though it is not explicitly stated, it should be, that protective measures aimed at accident prevention and accident mitigation must be in place and reliable, directed to ensuring that members of the public are not exposed to radiation doses of any appreciable amount, and that workers are protected from injury. It is a failing of PSA generally, at DOE and elsewhere, that this requirement is not addressed by the methodology.