Some Issues Related to Goal Allocation and Performance Criteria

G. Apostolakis
University of California, School of Engineering and Applied Science, Los Angeles, California 90024, U.S.A.

1. Introduction

The significance of the issues of safety goal allocation and performance criteria can be better appreciated in the context of a reliability assurance program, a definition of which is as follows [1]: "A reliability program for LWRs is defined as a set of reliability engineering and management techniques (i.e., elements) to help licensees achieve and maintain an acceptable level of plant safety over the lifetime of the plant". This definition implies the adoption of numerical guidelines, although at which level and by whom remains unanswered.

The level at which the guidelines are set determines their degree of prescriptiveness. For example, the proposed goals by the NRC [2] deal with individual and societal mortality risks and the frequency of large-scale core melt (10^{-4} per reactor year). They also include a benefit-cost guideline for use in decisions on safety improvements ($1,000 per man-rem averted). These goals are, of course, set at a very high level; the Commission leaves it as an open question, however, whether further guidance should be given.

It is interesting to note that the definition of a reliability assurance plan requires that the acceptable level of safety be maintained "over the lifetime of the plant". The proposed safety goals, however, do not make specific references to time. Although it may be argued that the stated goals should be met at all times, the question of what to do when the goals are exceeded has been raised.

The level at which the numerical guidelines are set by the regulators depends on the prevailing regulatory philosophy. The two extremes are the highly prescriptive approach, which attempts to regulate even minute details and the general approach, which sets overall goals without entering into details. While the current deterministic regulatory policy is criticized by many as being overly prescriptive, the NRC safety goals are very much less so. However, the large uncertainties are found to be a cause for concern and are likely to lead to a more prescriptive policy, in which case methods for allocating the high-level goals to functions, systems, etc. will be needed.

Even if the regulators decide to set the numerical goals at a high-level, the issue of goal allocation will become important to the plant owners, since they will probably wish to have a more prescriptive set of guidelines to be used by their design and operations groups. These guidelines must, of course, be consistent with those of the regulators.

2. Goal Allocation

Since the "acceptable level of safety" is likely to be given at some high level, e.g.,

core melt frequency, safety function unavailability, etc., the owners (and regulators) must make decisions regarding the design and operation of the plant. This means that they must make decisions concerning component and other "elementary event" reliabilities, in such a way that their combination will lead to the desired high-level goal.

Several of the difficulties in allocating goals can be discussed in terms of the Master Logic Diagram (MLD). Figure 1 shows a MLD as it applies to LWRs. The purpose of such a diagram (in PRAs) is to use fault-tree type logic to identify initiating events, which, in turn, determine the event trees that must be developed for PRA.

The top levels of the MLD are general enough to include the safety goals that may be proposed. Core damage appears in level 3, while, if the goals are in terms of early and delayed deaths, the MLD would have to be extended to levels higher than "Excessive Offsite Release".

The MLD, with appropriate extensions, could serve as a plant model which would depict the logical relationships among events, thus aiding in the allocation of reliability. This top-down approach is, of course, a natural way to allocate numerical goals that are given at a high level (see, for example, References 4 and 5). The MLD, like all logic diagrams, serves as a visual display of this process making communication easier. However, several problems may be encountered in attempting to implement this approach, as discussed in References 6 and 7.

One problem arises from the fact that the MLD, like all fault trees, is a static depiction of logical relationships. In some instances, however, this may not be sufficient and time may be a necessary variable. Such a case occurs at levels 1 and 2 of the MLD, where the timing of the accident sequences leading to a release of radioactive material would have to be included in the analysis.

Level 4 of the MLD involves safety functions either to prevent extensive core damage or to prevent containment failure. Of course, the designers would need further development of the MLD to levels 5, 6, etc., dealing with systems, subsystems and components. As Reference 6 observes, there would be practical problems at these levels having to do with how these functions are performed. For example, reactivity control is accomplished in a relatively few ways and would be relatively easy to analyze. However, residual heat removal has to be done under a wide variety of circumstances and utilizes support systems that are not dedicated to this function. The wide variety of frontline and support systems that can exist is reflected on the highly plant specific dominant accident sequences that the PRAs have identified.

Practical problems are also expected at the bottom level of the MLD, which will serve as the set of guidelines under which the plant and its components and structures will be designed and constructed. As an example, consider a system which consists of two components or trains in parallel. An expression for the average unavailability of the system which includes several possible failure causes is as follows [8]:

$$q_{av} = q_R + q_C + q_D + q_M \qquad \text{eq. (1)}$$

where we define:

a. "random" independent failure contribution

$$q_R = \frac{1}{3}\lambda_R^2\tau^2 + \lambda_R\tau_r, \qquad \text{eq. (2)}$$

b. dependent (due to shocks) failure contribution

$$q_C = \frac{1}{2}\lambda_C\tau + \lambda_C\tau_r \qquad \text{eq. (3)}$$

c. demand failure contribution

$$q_D = Q_0(Q_1 + \gamma_0 + \lambda_R\tau + 2\frac{\tau_r}{\tau}) \qquad \text{eq. (4)}$$

d. test contribution

$$q_M = \gamma_0\left[\gamma_1 + (1 - \gamma_1)\,Q_0 + (2 - \gamma_1)(\lambda_R + \lambda_C)\,\frac{\tau}{2} + 2\frac{\tau_r}{\tau}\right] \qquad \text{eq. (5)}$$

The terms of Equation (2) are the standard unavailability expression for the one-out-of-two system under exponential failure assumptions.

The terms appearing in Equations (2) through (5) can be readily interpreted. For example,

$\frac{1}{3}\lambda_R^2\tau^2$ = contribution of "random" independent failures

$\gamma_0\gamma_1$ = contribution of (dependent) maintenance errors on both components

Q_0Q_1 = both components fail on demand

γ_0Q_0 = one component down due to human error and the other fails on demand, etc.

The symbols in these equations are defined as follows:

λ_R = failure rate due to "random" causes

λ_C = rate of occurrence of common cause failures

τ = interval between periodic tests

τ_r = duration of a test

Q_0 = probability of failure on demand

Q_1 = Pr[one component fails on demand given that the other component have failed on the same demand]

γ_0 = probability that a testing error occurs for the first time in one period.

γ_1 = probability that a testing error occurs for the second time in one period.

This simple case of a one-out-of-two system illustrates the freedom as well as the difficulties that the designers will have in allocating reliability goals at the component level. Of course, there are also interactions of this system, e.g., through the support systems, the testing schedules, etc., with other systems complicating the allocation process even more. At this level it is doubtful that the process will be strictly one of allocation, since technical feasibility, costs, and regulatory requirements will also have to be included in the analysis. For example, the human error rate γ_0 is usually assessed in a generic way using the methods and numerical ranges of [9]. Thus, the designer cannot do much about it except to use it as an input. On the positive side, it would be relatively easy to assess the impact of employing a staggered testing, rather than a simultaneous testing, policy. Since human actions separated in time tend to be independent, the conditional probability of error, γ_1, will be smaller for staggered tests. Equations (1-5) could, then, be used to quantitatively assess the change in the average unavailability of the system.

An additional consideration that would further complicate the calculations is the

state-of-knowledge dependence of the failure rates of nominally identical components [10]. This would couple Equations (1-5) with similar expressions for other systems in which nominally identical events appear (this coupling, however, does not appear to have a significant numerical impact, unless highly redundant systems and very broad distributions are involved).

A methodology that may be useful at this point is the "bottom up" approach of [11], which utilizes techniques of multiobjective optimization to eliminate designs that are "inferior" in some sense.

3. Performance Criteria

Performance criteria are at the center of a reliability assurance program. A working (yet somewhat unsatisfactory in its vagueness, at this time) definition is as follows: They are a set of conditions, each accepting a yes-no answer, which, if true, will create a consensus among reasonable experts that a given reliability level is met.

A desirable (but not easily achievable) property that a condition ought to possess to qualify as a performance criterion is immediate verifiability [12] (for example, by inspection and measurements or by undisputed analysis). The current regulatory philosophy rests on four groups of verifiable criteria [1]: limiting conditions for operation, testing and surveillance procedures, operating and maintenance procedures, and a quality assurance program.

In the context of meeting a safety goal there are some complications. The Master Logic Diagram of the preceding section is a convenient framework in which the difficulties can be appreciated. While the safety goals are set at the high levels of the MLD, criteria at these levels are not immediately verifiable. Criteria must be set at lower levels, thus the credibility of the probabilistic analysis, which produces high-level frequencies by synthesizing those of low-level events, becomes an important consideration. Doubts about the completeness of the analysis, as well as the large uncertainties, usually undermine this credibility. For example, elaborate codes and standards exist for the design of piping systems. To actually derive a distribution for λ_R of the pipe involves many calculations and judgments. The uncertainties are very large and differences of opinion may be significant. Similarly, λ_C, the rate of common cause failures for a redundant system, is highly system specific and its evaluation relies heavily on judgment.

An additional difficulty occurs at the bottom level of the MLD. Some of the criteria would have to be probabilistic. This is easily seen in Equations (1-5) of the preceding section. While τ and τ_r can be verified in a (reasonably) deterministic way, the elemental probabilities Q_0, Q_1, λ_R, etc., can not. One would have to have some means of verifying that the numerical values of these quantities are consistent with experience. Decision theory and the theory of statistical hypothesis testing would probably be useful at this point; however, considerable research would be required to eventually develop workable performance criteria.

Given a set of performance criteria, as discussed in this section, the question arises as to what the proper course of action would be, if one or more of these criteria were found to be violated. Even though the safety goals, expressed in terms of frequencies per year, may be exceeded, the level of safety over the lifetime of the plant, as demanded by the definition given in Section 1, may still be acceptable, if corrective action is taken within a reasonable time. Furthermore, the large uncertainties are likely to create the

attitude (at least among some of the interested parties) of "do nothing-study further". The conditions for the acceptability of this option need further study. Several proposals for action criteria for LWRs are reviewed in [13]. They are formulated in terms of "high-level" quantities, e.g., individual risk of death per site year, core melt frequency, etc., thus suffering from lack of immediate verifiability, as discussed earlier.

4. References

1. U.S. Nuclear Regulatory Commission, Research Plan to Develop and Evaluate Reliability Program Elements Applicable to LWR's, Division of Risk Analysis, December 28, 1983.

2. U.S. Nuclear Regulatory Commission, Safety Goals for Nuclear Plants: A Discussion Paper, NUREG-0880, February, 1982.

3. PRA Procedures Guide, NUREG/CR-2300, September, 1981.

4. L. CAVE and W.E. KASTENBERG, "The Development of Quantitative Criteria for the Decay Heat Removal Function of LWRs", CSNI Specialist Meeting on Decay Heat Removal Systems, Wurenlingen, Switzerland, April, 1983.

5. L. CAVE, W.E. KASTENBERG and J.N. TWEEDY, "The Development and Application of Quantitative Methods in Licensing Nuclear Power Plants", 5th International Conference on Thermal Reactor Safety, Karlsruhe, September, 1984.

6. R. WHITLEY and D. OKRENT, "On the Development of Performance Criteria", in: On PRA Quality and Use, UCLA-ENG-8269, October, 1982.

7. R.H. WHITLEY, Application of Importance Measures to Nuclear Reactor Systems and the Development of Systems Performance Standards Based on PRAs, Ph.D. Thesis, University of California, Los Angeles, 1984.

8. G. APOSTOLAKIS and T.L. CHU, "The Unavailability of Systems under Periodic Test and Maintenance", Nuclear Technology, 50:5-15, August, 1980.

9. A.D. SWAIN and H.E. GUTTMANN, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Applications, NUREG/CR-1278, U.S. Nuclear Regulatory Commission, Washington, D.C., 1983.

10. G. APOSTOLAKIS and S. KAPLAN, "Pitfalls in Risk Calculations", Reliability Engineering, 2:135-145, 1981.

11. N.Z. CHO, I.A. PAPAZOGLOU and R.A. BARI, A Methodology for Allocating Reliability and Risk, Draft Report NUREG/CR-4048 (BNL-NUREG-51834), November, 1984.

12. G. APOSTOLAKIS, B.J. GARRICK and D. OKRENT, "On Quality, Peer Review, and the Achievement of Consensus in Probabilistic Risk Analysis", Nuclear Safety, 24:792-800, November-December, 1983.

13. D. OKRENT and W.L. BALDEWICZ, "On the Development of Threshold Criteria for Action for Light Water Reactors", Risk Analysis, 2:149-162, September, 1982.

5. Acknowledgement

I have benefited from discussions on these issues with D. Okrent of UCLA and J. Hartung and R.T. Lancet of Rockwell International.

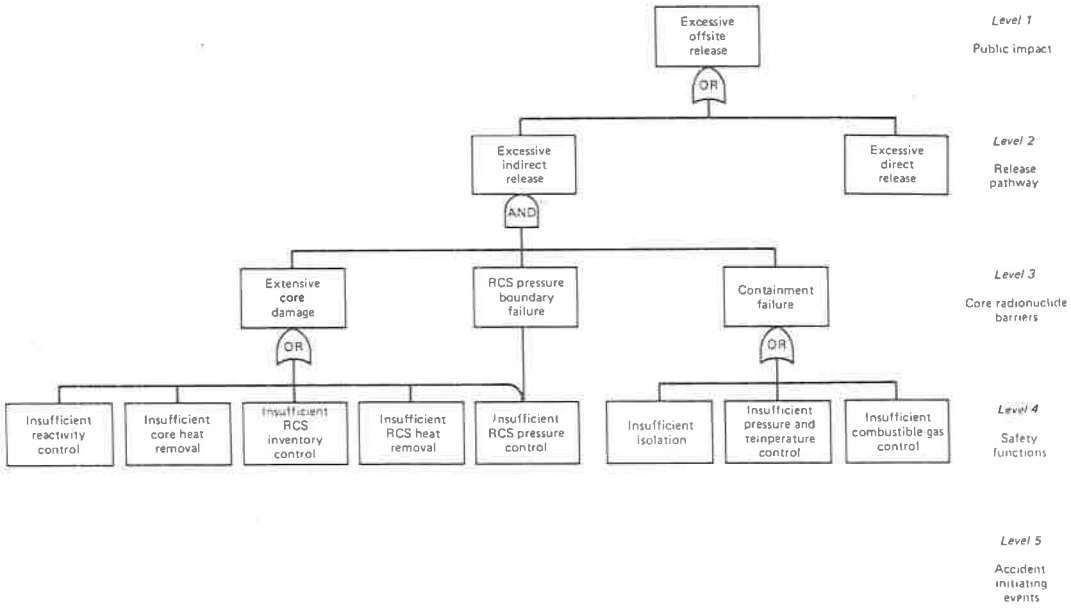

Figure 1. Master Logic Diagram (Reference 3).