sciendo

Consideration of quantitative risk reduction and risk achievement measures in safe NPP design

Ivan Vrbanic (ID),
Ivica Basic (ID)

Abstract. In the models developed by probabilistic safety analyses (PSA) and in their applications associated with nuclear power plants (NPPs), the risk importance of a particular feature can be, most generally, divided into two categories: importance with respect to the risk-increase potential and importance with respect to the risk-decrease potential. A representative measure of the first category is risk achievement worth (RAW), while a representative measure of the second category is risk reduction worth (RRW). The present paper discusses the use of RAW and RRW in achieving safe design and points out some implications of their mutual dependency on the selection of a risk-reduction strategy. A simple example is provided to illustrate the differences between the two basic strategies and point out to the main issues and conclusions.

Introduction

Models developed by probabilistic safety analysis (PSA) are essential tools for quantitatively assessing the safety of the design and the operation of nuclear power plants (NPPs). In PSA, safety is quantified in terms of its inversion, risk, which is usually represented by a specified type of event, which is rare, but has highly undesired consequences (e.g., reactor core damage). A quantitative measure of risk is, then, defined as a frequency or probability of such an event or condition, e.g., core damage frequency (CDF) or core damage probability (CDP) given certain disturbances. PSAs for NPPs are nowadays performed in accordance with well-established normative and guiding documents. Examples of internationally recognized and well-known high-level referential documents for NPP PSA include Refs. [1–3]. As a part of PSA results, risk-importance measures are usually generated for PSA model elements such as equipment failure or human failure events. Generally, a risk-important measure shows how much the calculated risk would change in the case of certain change in reliability or status of considered component (equipment) or human action.

A number of risk-importance measures were defined and used in reliability and risk analyses. Some are related to each other, and some produce the same risk ranking. Their theory and use are described in a number of books such as Refs. [4–6] and in stud-

I. Vrbanic⊠, I. Basic
APOSS, Zabok, Croatia
E-mail: ivan.vrbanic@zg.t-com.hr

ies or engineer's handbooks and guidelines such as Refs. [7–9]. Risk-importance measures kept finding their way into different aspects of risk-informed or risk-oriented applications concerning NPP safety, e.g., Refs. [10–12].

In this paper, we focus on those importance measures, which are most widely used in current NPP PSAs. The risk importance of a particular feature (e.g., function, system, component, failure mode, or operator action) can be, most generally, divided into two categories: importance with respect to risk-increase potential and importance with respect to risk-decrease potential. A measure representative of the first category is risk achievement worth (RAW). A representative measure of the second category of risk importance is risk reduction worth (RRW). We will define them according to Ref. [7]:

$$(1) \qquad I_{\mathrm{RAW},X} = \frac{R_X^+}{R}; \; I_{\mathrm{RRW},X} = \frac{R}{R_X^-}$$

In the above expression, the terms $I_{\mathrm{RAW},X}$ and $I_{\mathrm{RRW},X}$ refer to RAW importance and RRW importance of the feature X, respectively, with others being: R – present ("nominal") risk level; R_X^+ – increased risk level with feature X assumed failed; R_X^- – decreased risk level with feature X assumed to be perfectly reliable.

Therefore, RAW associated with feature X shows how much would risk increase, relatively to the nominal risk, in the case that status of X changes from nominal reliability to failed or unavailable state. Analogously, RRW associated with feature X shows how much would risk decrease, relatively to the nominal risk, in the case that status of X changes from nominal reliability to "perfect" state (i.e., successful implementation of the mission is granted).

It is easy to show, in Ref. [13], that the RAW and RRW for a particular failure event X are related to each other, with the probability of the considered failure event, $P(X)$, as a parameter. Particularly:

$$(2) \qquad I_{\mathrm{RRW},X} = \frac{1 - P(X)}{1 - P(X)I_{\mathrm{RAW},X}} \; \text{ or }$$

$$I_{\mathrm{RRW},X} = \frac{1}{P(X)} - \frac{1 - P(X)}{P(X)I_{\mathrm{RRW},X}}$$

It is pointed out that this relation is established on the basis of the probability theory and is not specific for PSA modeling. The relation is shown in Fig. 1.

From the expression (2) above, RAW values would not go above $1/P(X)$. (Note: $0 < P(X) < 1$). This is an important point, because it shows that only the components with small failure probabilities can achieve very high RAW values. This can also be recognized in Fig. 1. For example, the curve $P(X) = 0.1$ sharply rises beyond the RAW value of, approximately, 8 and would be asymptotically approaching the value of $1/0.1 = 10$, with increasing RRW. The figure also indicates that, when $P(X)$ gets small (e.g., 0.05 or smaller), only a small increase in $P(X)$ can lead to a considerable increase in RAW at approximately the same RRW value. (See curves $P(X) = 0.05$ and $P(X) = 0.01$). It is worth mentioning that
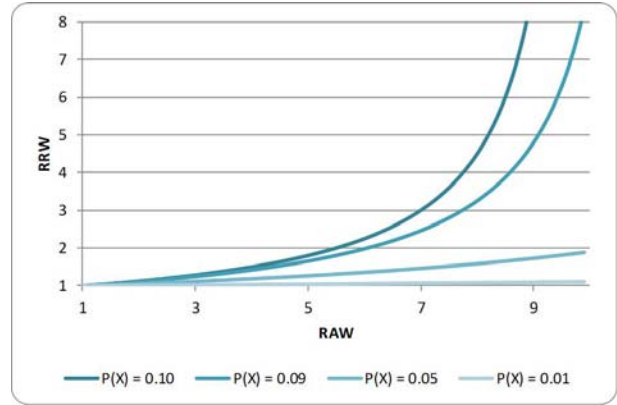

Fig. 1. Illustration of RRW as a function of RAW with $P(X)$ as a parameter.

in a real PSA model, most of the failure probabilities would normally have values <0.05 (at least, in a model for internal initiating events).

One of the implications of this discussion is that a large RAW value (possibly implying not well-balanced design from the risk perspective) is really a concern with small failure probability events (because RAW is bounded by $1/P(X)$. Nonreliable components cannot have huge RAW. They cannot achieve huge risk because they already are nonreliable (within the nominal risk estimate). On the other hand, a component with very low failure probability or very high reliability can achieve huge risk (if there are no redundant or diverse means to compensate for its failure). For a highly reliable component, there is always a hazard that its reliability (availability) may degrade.

In this paper, we discuss the use of risk-importance measures in achieving a safe design of facility, with due attention paid to the above outlined implications and the main concerns that may come out of them.

Reducing facility's risk through consideration of risk-importance measures

Reducing the facility's risk either at the design stage or at the operating stage is a complex process, which involves a detailed evaluation of the complete risk profile and its contributors. For our purposes, we focus on risk-reduction possibilities through consideration of the discussed importance measures. Typically, risk-reduction options are identified by obtaining a list of plant features (e.g., systems or components) with significant RRW. This is usually done by calculating the RRW values for the representative basic events in the PSA model and sorting them in the decreasing order. The next general step is to find the possibilities for decreasing any significant RRW value. Any significant decrease in such RRW value would, by definition, reflect in significant reduction of the facility's risk.

Let us consider a situation where a significant RRW was identified for a feature X and the target was set to reduce it from the value $\mathrm{RRW}_{\mathrm{old}}$ to a lower value $\mathrm{RRW}_{\mathrm{new}}$. Generally, there would be two basic strategies for reaching the target, Ref. [14]:

Strategy 1: Decreasing the $I_{RRW}(X)$ by decreasing the failure probability $P(X)$. Examples of this strategy may include: reducing the test/inspection period; improving testing strategies (test efficiency); extending the scope of inspection; improving the operating procedures or maintenance procedures; extending/improving preventive or predictive maintenance; etc. In principle, these are, usually, relatively affordable (not–so-expensive) measures.

Strategy 2: Decreasing the $I_{RRW}(X)$ with the failure probability $P(X)$ kept at the same level. In this strategy, the feature X and the operational practices associated with it are maintained the same. However, some additional feature is introduced into the facility, which provides a diverse means for the function normally performed by the feature X. In many cases, this strategy may be expensive, as it may require modifications to the design of the existing systems, including the costs of design basis safety re-evaluation as well as developing technical specifications, manufacturing, and installation of the new feature, together with costs associated with design basis re-licensing. On the other hand, in a number of cases, it may be implemented in a relatively affordable way by means of flexible equipment or equipment with relaxed safety requirements.

Obviously, any combination of the two strategies can also be considered and used in the practice. However, we will focus on them separately in order to identify and point out to certain aspects or concerns associated with each one.

Strategy 1 is illustrated by Fig. 2. To achieve a decrease in the RRW value of the considered feature X from RRW$_{old}$ to RRW$_{new}$, a certain reduction in the failure probability or unavailability $P(X)$ would be needed. How large, exactly, a reduction in $P(X)$ would be required (for the predefined decrease in RRW) would depend on the configuration of the facility, i.e., on its elements other than X. The issue with this strategy is that it may, in a new constellation, lead to an increase in the RAW of the considered feature X. Thus, for example, Fig. 2 shows that a reduction in $P(X)$ from the initial 0.03–0.02 already causes an increase in RAW. If reductions in $P(X)$ larger than this are needed, an increase in RAW may be considerable.

High RAW values are generally not desirable in design solutions because they mean over-reliance on particular safety features. Thus, there are established and recognized PSA application guidelines, which
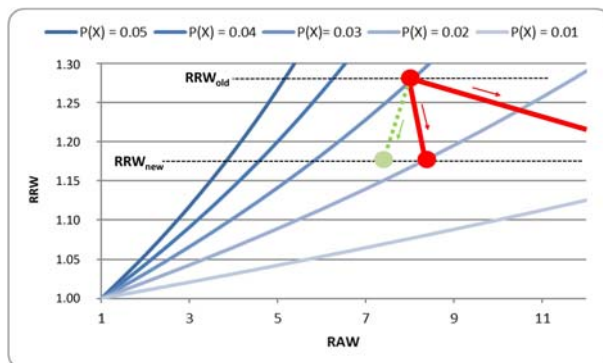
have set the safety significance threshold already at RAW >2 (e.g., NEI 00-04, Ref. [15]). Over-reliance on certain features means that the overall risk becomes very sensitive upon any degradation of this feature. As a measure of the importance of degradation (e.g., due to aging or environmental conditions), a reliability importance can be considered, which is defined as (e.g., Ref. [13] and its references):

$$(3) \qquad I_{rel,X} = \frac{\partial R}{\partial P(X)}$$

It can easily be shown, Ref. [13], that:

$$(4) \qquad I_{rel,X} = R\left(I_{RAW,X} - \frac{1}{I_{RRW,X}} \right)$$

By using the relation (2), this can be rearranged into the form:

$$(5) \qquad I_{rel,X} = R\, I_{RAW,X} \left(\frac{1 - \dfrac{1}{I_{RAW,X}}}{1 - P(X)} \right)$$

Normally, $P(X)$ is $\ll 1$ (i.e., $1 - P(X) \approx 1$). Therefore, if RAW is high enough (e.g., >10), $I_{rel,X}$ becomes directly proportional to RAW, and the overall risk becomes very sensitive to the degradation in the reliability of the feature X.

Strategy 2 is illustrated by Fig. 3. In comparison, it has an important property that the RAW value of feature X would, in the new constellation, always decrease or, if already close to the asymptote (i.e., $1/P(X)$), remain the same (but would never increase). This can be clearly seen in Fig. 3 where the RRW of the considered feature X is reduced from RRW$_{old}$ to RRW$_{new}$, by moving downward through a curve defined by $P(X) = const$. As RRW decreases, RAW would also decrease.

In principle, this means that the risk profile of the facility's new status (with lower risk) would remain, as far as the feature X is of concern, as balanced as it was (or better).

Illustration by a simple example

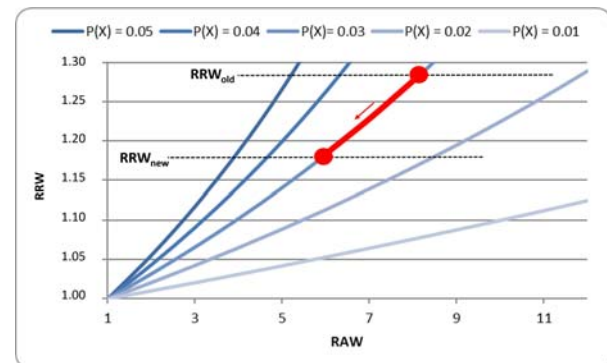The above points of discussion of the two basic strategies will be illustrated by a very simple example

Fig. 2. Reducing the risk reduction worth of feature X via strategy 1.

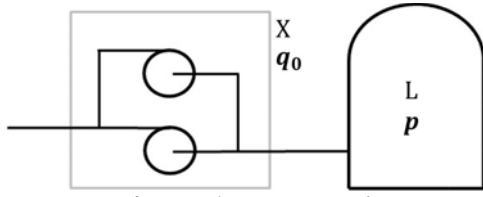**Fig. 3.** Reducing risk reduction worth of feature X via strategy 2.

Fig. 4. Diagram of a simple system used as an example.

based on a system for emergency water injection for which a diagram is shown in Fig. 4. The system, which is a part of an operating plant, consists of the pumping station X and the water tank L. Its intended function is to inject the water from the tank in the case of occurrence of a design basis initiator or hazard. Probability of failure of the pumping station X to perform the mission on demand, $P(X)$, is designated as q_0. Probability that tank L is unavailable or otherwise in a faulted condition at the time of demand, $P(L)$, is designated as p. Their values have been assessed at $q_0 = 1E–03$, and $p = 1E–04$. For simplicity, in all the calculations that follow the "rare event approximation" will be used, i.e., assuming that A and B are the events of concern, the probability of their logical sum ("OR" operation) is approximated as: $P(A + B) \approx P(A) + P(B)$. For the purposes of this example, this approximation will be good enough.

As a measure of risk, R, a probability of the intended function's failure on demand will be taken. Considering the above, the current or initial value of risk, R_{init}, is estimated at:

$$(6) \qquad R_{init} \approx P(X) + P(L) = q_0 + p = 1.1E–03$$

We will assume that the possibilities are explored for reducing the risk. It can be seen that there is a large risk-reduction potential with regard to the pumping station X. Considering that $R^-_{init,X} = P(L)$:

$$(7) \qquad I_{RRW,X} = \frac{R_{init}}{R^-_{init,X}} \approx \frac{q_0 + p}{p} = 11$$

On the other hand, the potential for reduction of risk on account of the tank L is much smaller: $I_{RRW,L} \approx \{[P(X)+P(L)]/P(X)\} = 1.1$. Thus, the efforts to reduce the risk will be focused on improving the reliability of the pumping station. Let us further assume that the target has been set to reduce the risk to the values not higher than 2E–04 (from the current 1.1E–03).

Two hypothetical options will be considered here, each representing one of the two strategies discussed above. Refer to Fig. 5. Strategy 1 represents increase in the reliability of the existing pumping station X, which would reflect in decreasing its failure probability from the current q_0 to q_1 ($q_1 < q_0$). Strategy 2 is represented by providing a mobile pump R which can, if needed, be transported from its parking place to the location close to the pumping station and connected by means of the hoses in order to inject water from the tank. Probability of failure of the mobile pump R to be established or otherwise to fail the mission will be designated as $P(R) = r$.

New risk values upon implementation of strategy 1 ($R_{new,1}$) or strategy 2 ($R_{new,2}$) would then be (assuming independency between X and R):

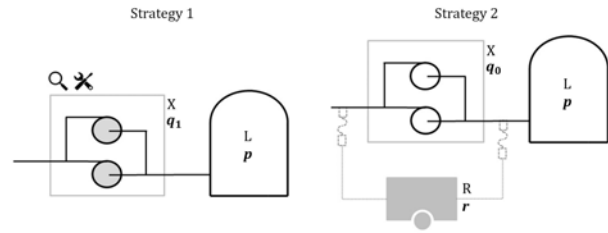**Fig. 5.** Illustration of two strategies for risk reduction.

$$(8) \qquad \begin{aligned} R_{new,1} &\approx P(X) + P(L) = q_1 + p \\ R_{new,2} &\approx P(X)P(R) + P(L) = q_0 r + p \end{aligned}$$

With regard to strategy 1, it can be seen that in order to reach the target $R_{new} \le 2E–04$, the failure probability $P(X)$ would need to be reduced to at least 1E–04 (i.e., $q_1 \le 1E–04$). We do not open the question here whether it is feasible to reduce a failure probability of an existing pumping system by an order of magnitude merely by means of improving the maintenance and testing practices. In principle, it is possible to considerably reduce failure probabilities by decreasing test/maintenance intervals, by increasing test/in-service inspection efficiency and scope, by introducing preventive maintenance, and using similar techniques. Those aspects are beyond the scope of this discussion. The example is very simple and its purpose is to introduce and illustrate the basic concepts and concerns.

For strategy 2, if the same target $R_{new} \le 2E–04$ is to be reached, the failure probability of the new mobile pump, $P(R)$, should not exceed 0.1, i.e., $r \le 0.1$. Although feasibility would depend on the actual success criteria (e.g., time windows), meeting such a requirement does not look as if being out of reach.

Let us now assume that the risk target would be reached at exactly $R_{new} = 2E–04$ and then take a look at new values of risk-importance measures for the pumping station X, depending on which of the two strategies is selected. (Consider: if strategy 1 is selected, then $q_1 = 1E–04$; if strategy 2 is selected, then $r = 0.1$). We start with RAW. The initial RAW, considering that $R^+_{init,X} = 1$, was $I_{RAW,X} = \{[R^+_{init,X}/R_{init}] \approx (1 / q_0 + p)\} = 909.09$. This is already a very high value, which partially came due to simplicity of the example. However, if strategy 1 is used, the RAW value becomes alarmingly high:

$$(9) \qquad I_{RAW,X,1} = \frac{R^+_{new,1,X}}{R_{new,1}} \approx \frac{1}{q_1 + p} = 5000$$

On the other hand, if strategy 2 is selected, the RAW would be cut almost in half:

$$(10) \qquad I_{RAW,X,2} = \frac{R^+_{new,2,X}}{R_{new,2}} \approx \frac{r + p}{q_0 r + p} = 500.50$$

RRW initially had a very large value of 11, Eq. (7). The new RRW value will be the same for both strategies, because if success of X is guaranteed, then $R^-_{new,X}$ would only depend on the tank (as initially). Thus, whichever strategy is applied, RRW gets significantly reduced on account of the baseline risk being significantly reduced, i.e.:

$$(11) \qquad I_{RRW,X} = \frac{R_{new}}{R^-_{new,X}} \approx \frac{2E-04}{p} = 2$$

Table 1. Reliability parameters for preselected new risk targets

Case	R_{new}	Strategy 1 q_1	Strategy 2 r
a	2.00E–04	1.00E–04	0.10
b	1.90E–04	9.00E–05	0.09
c	1.80E–04	8.00E–05	0.08
d	1.70E–04	7.00E–05	0.07
e	1.60E–04	6.00E–05	0.06
f	1.50E–04	5.00E–05	0.05

Table 2. RAW and RRW values for the cases from Table 1

Case	Strategy 1 $I_{RAW,X,1}$	Strategy 2 $I_{RAW,X,2}$	Strategy ½ $I_{RRW,X}$
a	5000.00	500.50	2.00
b	5263.16	474.21	1.90
c	5555.56	445.00	1.80
d	5882.35	412.35	1.70
e	6250.00	375.63	1.60
f	6666.67	334.00	1.50

Table 3. Reliability importance measure for the cases from Table 1

Case	Strategy 1 $I_{rel,X,1}$	Strategy 2 $I_{rel,X,2}$
a	1.00E+00	1.00E–01
b	1.00E+00	9.00E–02
c	1.00E+00	8.00E–02
d	1.00E+00	7.00E–02
e	1.00E+00	6.00E–02
f	1.00E+00	5.00E–02

Tables 1 and 2 provide a comparison of new values of the RAW and RRW for the two strategies, for five other cases as the new risk is being further reduced to the values smaller than 2E–04. As it can be seen, as the target risk decreases, RAW in the case of strategy 1 would increase even more, while in the case of strategy 2, it would further decrease. RRW would decrease with decreasing target risk, for the reasons discussed above. (Note that the risk target is the same for both strategies and then the parameters are selected correspondingly).

Additionally, we will take a look at how would a selected strategy reflect on the above-discussed reliability importance, as a measure of degradation of reliability of the pumping station X, with regard to performing its intended mission. Table 3 presents the reliability importance measure for both the strategies and the same cases, as calculated by Eq. (4).

As can be seen, in the case of strategy 1, any degradation in the reliability of the pumping station X would entirely transfer to a risk increase, while in the case of strategy 2, only a small fraction of degradation (10% or less in the cases considered) would reflect as a risk increase.

Conclusions

Use of risk-importance measures in achieving a safe design, particularly in reducing the risk of an operating facility, was illustrated by a simple example. It was shown that beside RRWs, as a means for identifying risk-reduction potential, it is recommendable to verify RAWs in the modified design, in order to prevent over-reliance on single safety features with claimed high reliability. Among other reasons, over-reliance on a single feature means that the overall risk would become very sensitive on any degradation of this feature, e.g., due to aging or environmental conditions.

The simplistic example that was presented points to the importance of diversification of safety functions or features. Additional diverse (alternative) features may not even necessarily have particularly high reliability. In some cases, it may be easier to introduce an alternative success path with flexible or/and movable equipment with relaxed safety classification requirements than to demonstrate that certain risk target is achieved through improved testing, inspection, maintenance, or quality assurance strategies.

ORCID

I. Basic http://orcid.org/0000-0002-9496-549X
I. Vrbanic http://orcid.org/0000-0001-8769-1729

References

1. International Atomic Energy Agency. (2010). *Development and application of level 1 probabilistic safety assessment for nuclear power plants: Specific safety guide*. Vienna: IAEA. (SSG-3).
2. American Society of Mechanical Engineers. (2009). *Standard for level 1/large early release frequency probabilistic risk assessment for nuclear power plant applications, an American National Standard*. New York: ASME. (ASME/ANS RA-Sa–2009).
3. U.S. Nuclear Regulatory Commission. (2018). *An approach for using probabilistic risk assessment in risk-informed decisions on plant-specific changes to the licensing basis, Revision 3*. Washington D.C.: U.S. NRC. (Regulatory Guide 1.174).
4. Fullwood, R. R., & Hall, R. E. (1988). *Probabilistic risk assessment in the nuclear power industry, fundamentals and applications*. New York: Pergamon Press.
5. Henley, E., & Kumamoto, H. (1981). *Reliability engineering and risk assessment*. Upper Saddle River: Prentice Hall.
6. Barlow, R. E., & Proschan, F. (1975). *Statistical theory of reliability and life testing: probability models*. New York: Holt, Rinehart and Winston, Inc.
7. Vesely, W. E., Davis, T. C., Denning, R. S., & Saltos, N. (1983). *Measures of risk importance and their applications*. Washington D.C.: U.S. NRC. (NUREG/CR-3385).
8. Vesely, W. E., Goldberg, F. F., Roberts, N. H., & Haasl, D. F. (1981). *Fault tree handbook*. Washington D.C.: U.S. NRC. (NUREG-0492).
9. Papazoglou, I. A., Bari, R. A., Buslik, A. J., Hall, R. E., Ilberg, D., Samanta, P. K., Teichmann, T., Youngblood, R. W., El-Bassioni, A., Fragola, J., Lofgren, E., & Vesely, W. (1984). *Probabilistic safety analysis procedures*

guide. Washington D.C.: U.S. NRC. (NUREG/CR-2815).

10. Cheok, M. C., Parry, G. W., & Sherry, R. R. (1998). Use of importance measures in risk-informed regulatory applications. *Reliab. Eng. Syst. Saf.*, *60*(3), 213–226. DOI: S0951-8320(97)00144-0.

11. Kim, K., Kang, D. I., & Yang, J. -E. (2005). On the use of the balancing method for calculating component RAW involving CCFs in SSC categorization. *Reliab. Eng. Syst. Saf.*, *87*(2), 233–242. DOI: 10.1016/j.ress.2004.04.017.

12. Bäckström, O., Krcal, P., & Wang, W. (2016). Two interpretations of the risk increase factor definition. In L. Walls, M. Revie & T. Bedford (Eds.), *Risk, reli-ability and safety: Innovating theory and practice* (pp. 2816–2822). Boca Raton, FL: CRC Press.

13. Vrbanic, I., Samanta, P., & Basic, I. (2017). *Risk importance measures in the design and operation of nuclear power plants*. New York: ASME Press.

14. Vrbanic, I., Samanta, P., & Basic, I. (2018). Some implications of theoretical relation between RAW and RRW measures on risk reduction strategies. *J. Phys. Sci. Appl.*, *8*(3), 38–45. DOI: 10.17265/2159-5348/2018.03.005.

15. Nuclear Energy Institute. (2005). *10 CFR 50.69 SSC Categorization guideline, Revision 0*. U.S.: NEI. (NEI 00-04).