What PRA Needs From A Digital I&C Systems Analysis: An Opinion

(Last Technical Revision - 12/8/97; Last Revised 4/22/99)

Introduction

In broad terms, probabilistic risk assessment (PRA) is the process of: 1) qualitatively identifying accident scenarios ("what can go wrong"), 2) quantifying the likelihood of these scenarios, and 3) assessing the qualitative and quantitative consequences of these scenarios (Kaplan and Garrick, 1981). Although it is intended to support decision making, it is not solely aimed at producing a "bottom line number." The qualitative results of a PRA (e.g., descriptions of dominant scenarios which enable the identification of potentially effective risk management alternatives) are as important as the quantitative results (e.g., the scenario risk contributions which provide the basis for prioritizing risk management alternatives).

A digital I&C systems analysis intended to support PRA must perform these three functions. In particular:

1. It must qualitatively model the I&C portions of accident scenarios to such a level of detail and completeness that:

    a. subsequent (non-I&C) portions of the scenario can be properly analyzed (see #3 below), and

    b. useful decisions (e.g., concerning the I&C system design, implementation, and operation, inspection, testing, and maintenance) can be formulated and analyzed.

2. It must quantify the likelihood of system failure in a credible manner.

3. It must assess the likelihood of all system failure modes which can significantly affect the performance of other plant systems and the plant operators.

It can be seen that such a systems analysis can be viewed as a PRA; the consequences of interest are the I&C failure scenario endstates which affect the performance of the plant systems and operators.

In the following section, the general treatment of I&C in a current nuclear power plant (NPP) PRA is discussed. The remainder of the paper then addresses the needs of current NPP PRA relative to the I&C analysis and identifies potential technical barriers to meeting these needs.

The PRA Framework and Current Treatment of I&C

The general definition of PRA, as indicated above, does not prescribe a particular modeling approach. When applied to nuclear power plants, however, PRA tends to take a specific form. On the qualitative side, event trees are used to model accident progression at a safety function or system level, and fault trees are used to determine how a particular function or system can

be failed.[1] The event tree/fault tree model leads to definitions of accident scenarios in terms of "initiating events" (initial upsets in plant operation requiring the response of safety equipment[2]) and one or more "basic events" (elementary faults, i.e., the lowest level faults included in the model). Some typical initiating events modeled in at-power NPP PRAs are loss of coolant accidents (LOCAs), loss of offsite power events, loss of feedwater events, and general transients (which cover other reactor trip events). Component-related basic events are often defined at an unavailability cause level; typical events include: component failure on demand, component failure while running, component unavailable due to maintenance, component unavailable due to human error, and component unavailable due to common cause failure. Component "failures" (failures to perform necessary functions) due to support system (e.g., electric power, instrument air, I&C) faults are usually handled by explicit modeling of faults within the support system. Thus, for example, the PRA model may have a submodel devoted towards the analysis of an event like the failure to generate a High Pressure Core Spray (HPCS) actuation signal; this submodel feeds into the analysis of failure of HPCS, as shown in Figure 1.

On the quantitative side, NPP PRA employs available data and the laws of probability to determine the likelihood of the accident scenarios identified using the event tree/fault tree approach. Collection of data relevant to the analysis is a key challenge as many of the events in the model represent relatively rare occurrences; some may not have even been observed. A key analytical challenge in this process is the identification and quantification of dependencies between failure events in an accident sequence. Failure to treat important dependencies, and subsequent treatment of the failures as being independent, can result in gross underestimates of risk. Three key types of dependencies involving plant hardware are as follows.

C Functional Dependencies: The performance of one component depends on the performance of another. Example: a safety injection pump fails to automatically start because the I&C system does not generate an autostart signal.

C Spatial Dependencies: The performance of multiple components located in the same general area is affected by threats affecting their common environment. Example: I&C boards in an electrical cabinet fail when a nearby fire causes excessively high temperatures in the cabinet.

C Human Dependencies: The performance of components affects and is affected by actions taken by the plant crew. Example: miscalibration of multiple sensors during routine maintenance prevents the proper operation of these sensors. A more complicated example: an I&C fault causes incorrect instrumentation readings which

---

[1]This paper focuses on at-power Level 1 PRAs (where core damage due to operational events is the consequence of interest). Most of the issues raised should also be applicable to low power and shutdown core damage analyses.

[2]The term "safety equipment" will be loosely used in this paper to refer to all equipment that may be used in achieving safe shutdown.

cause the operators to misunderstand current plant conditions and incorrectly stop a makeup pump.

Most of these dependencies are treated in a PRA through explicit modeling. (So-called errors of commission, such as that in the last example, provide an important exception; the current state-of-the-art in human reliability analysis does not allow a general, quantitative treatment of these errors.) Other dependencies, e.g., those due to a common manufacturer or common service conditions, are typically treated implicitly under the general purpose title of "common cause failures."

It is potentially important to observe that the event tree/fault tree approach is generally considered to model "aleatory uncertainty" (also called stochastic or random variability -- see Apostolakis, 1995). "Epistemic uncertainties" (also called state of knowledge uncertainties) are addressed by propagating uncertainties in the event tree/fault tree model parameters through the model. A key distinction between these two types of uncertainty is that, within the modeling framework being employed, epistemic uncertainties can be reduced to negligible levels with the collection of additional information, whereas aleatory uncertainties cannot.

The preceding discussion outlines the overall approach taken by current NPP PRAs. When it comes to implementation, the accuracy of the analysis varies with the particular characteristics of the risk contributor being analyzed. In the particular case of I&C, current studies only model a portion of the I&C contribution to risk. For example, the AP600 PRA explicitly addresses I&C contributions to initiating event frequencies through: a) explicit analyses of LOCAs caused by spurious operation of automatic depressurization system valves, and b) implicit inclusion of I&C-induced transients as contributors to the likelihood of general transients. The same study has an extensive, circuit board-level analysis of the likelihood of safety system failures due to I&C faults and treats the effects of fire on I&C system components. On the other hand, the study does not treat spurious equipment operation in a general manner, nor does it treat the generation of signals that confuse the operators or prompt them to take incorrect actions. This latter issue (neglect of inappropriate signal generation) appears to be common to all NPP PRAs to date and may be the most risk significant problem with the current state-of-the-art. The event tree/fault tree framework does not preclude its treatment (although alternative frameworks, e.g., digraphs or Petri nets, might be better suited); rather, the problem lies with the current inability to define, identify, and quantify key signal patterns.[3]

Qualitative Modeling Requirements

In order to support NPP PRA in the near term, a digital I&C system model must satisfy two general qualitative modeling requirements. First, the model must be compatible with the structure of current NPP PRAs. Second, the model must have a structure which supports proper analysis of the accident sequences addressed in the PRA, as stated in bullet #1a earlier.

---

[3]Note that the current inability to model errors of commission should not prevent the analysis of faulty signals. The difficulty in treating errors of commission lies with a somewhat separate issue: the quantification of the likelihood that the operator will make a mistake, e.g., develop an incorrect diagnosis, given a particular scenario (including faulty signals).

Compatibility

The event tree/fault tree methodology currently employed in NPP PRAs is not the only means to assess NPP accident scenario risk. A variety of alternative modeling approaches which couple process plant dynamics with the stochastic behavior of operators and equipment have been proposed for this purpose (Siu, 1994). Promising examples include dynamic event trees and event simulation. However, these "dynamic PRA" approaches have not yet been employed in practical NPP analyses. Therefore, a current requirement is that the I&C model must be useable in a static, logic-based model structure.

This is not to say that the I&C model must itself be of an event tree or fault tree form. It does mean that the model input and output will be constrained. On the input side, the model cannot require time-dependent or continuous plant state information. At best, a PRA model can provide the binary status of equipment for a given phase of the accident. (For example, the model can show if, for a given scenario, a particular 125VDC bus is available during the injection phase following a LOCA.) Qualitative indications of the plant process variables (e.g., pressure high and rising) are not provided by the PRA model, but can be inferred. On the output side, the model must provide discrete system states which can be directly related to the performance of components or operator actions dependent on the I&C system. Note that the relationship need not be deterministic (e.g., I&C system state 1 implies unavailability of component X); probabilistic relationships (e.g., I&C system state 1 increases the failure probability of component X by an amount Y) can also be used in the analysis. (Deterministic relationships are generally appropriate when modeling automatic actuations; both deterministic and probabilistic relationships are likely to be useful when modeling the effect of I&C failures on operator actions.) Note also that, as a practical matter, the number of system states generated by the I&C system model should be kept as small as possible, in order to minimize analysis costs.

Figures 2a and 2b illustrate how the I&C system model can be integrated into a PRA event sequence model. Figure 2a shows how the system can be treated as an event tree top event. (Note that in some PRA software packages, the single top event with multi-state output must be replaced by multiple top events with binary outputs.) Figure 2b shows how the system model can be treated as a fault tree event. This figure illustrates the common case where different plant components receive different signals from the I&C system. Care must be taken in the quantification process that dependencies between multiple I&C failure events in the same accident scenario are properly analyzed.

Figures 2a and 2b imply a "failure on demand" approach to modeling the I&C system.[4] This approach is appropriate for modeling protection system actuations *following* an initiating event. It is important to note that NPP PRA also requires input on the occurrence of I&C system failures over time that *cause* initiating events. For system failures which have no further impact other than the initiating event, a separate analysis may not be required; the I&C contribution can be included with the non-I&C contribution in a simple statistical model. For

[4]Failures during the mission are also incorporated, but, from a qualitative modeling standpoint, they are effectively addressed in the same manner as demand failures.

failures which affect the performance of safety systems, a separate analysis may be required, depending on the likelihood and consequences of such failures. A discussion on the notion of random software failures is provided at the end of this paper.

Internal Model Structure

The preceding discussion considers the requirements on the I&C system model input and output as defined by NPP PRA. It is reasonable to ask if NPP PRA imposes any requirements on the internal structure (i.e., the basic elements and their interactions) of the system model as well. For example, can the entire I&C system be treated as a single black box? Should software faults be distinguished from hardware faults? If so, should higher level programming faults be distinguished from lower level (e.g., compiler) faults? How should software/hardware interactions be treated? Should embedded software be treated differently?

Regarding level of detail, an NPP PRA models the responses of multiple trains of safety equipment and plant operators to initiating events. These responses are often dependent on the behavior of the I&C system. Clearly, therefore, the I&C analysis needs to be detailed enough to identify and treat those I&C system faults which can cause significantly different levels and modes of degradation in safety equipment and operator performance. For example, system faults which fail one safety system function should be distinguished from those that fail multiple functions. (As a particular case, system faults which cause an initiating event and fail one or more safety functions should be identified.) Similarly, faults that cause loss of function should be distinguished from those that cause spurious operation. One simple approach is to use models which interface with the NPP PRA model as exemplified in Figure 2b: different (but not necessarily independent) modules are provided for different signals. Alternatively, a technically correct single black box model can be constructed (see Figure 2a), although, depending on the particulars of plant and system design, a modular approach may be easier to review and understand. Either approach, if properly executed, can yield acceptable results for the PRA.

The same reasoning applies to the other questions on model structure. The NPP PRA needs an I&C analysis which distinguishes between system events (e.g., failures) on the basis of the level and mode of consequential degradation in the performance of safety equipment and plant operators. The PRA does not place a requirement on how the I&C analysis arrives at these results (other than the analysis must be scrutable and credible).

I&C is not unique in this regard. PRA employs a similar approach with analyses of other potential sources of dependent failure, including human reliability analysis (HRA), external events analysis, and common cause failure (CCF) analysis. For example, PRA requires (in principle) that operator diagnoses and actions which can affect the status of multiple systems be addressed in an HRA. Whether the analyst employs a task-oriented behavioral analysis or a cognitive simulation model to do this is not specified. It is worth noting that, in practice, very simple models which may not even address potentially important failure causes (e.g., errors of commission in the case of HRA, smoke damage in the case of fire risk assessment) are currently being used.

Quantitative Modeling Requirements

The NPP PRA requirements placed on the I&C system model from a quantification standpoint are not unique to I&C. The model results must be sufficiently accurate to support the needs of the decision makers, they must be credible, and they must include an indication of the level of uncertainty. Each of these issues is discussed below.

Accuracy

Two major characteristics of PRA models which affect their accuracy are their treatment of dependencies between (failure) events and their degree of completeness. In cases where dependencies are modeled explicitly, the analyst only needs to ensure that the associated modeling terms are quantified appropriately. When dependencies have not been identified explicitly, the analyst needs to raise the possibility of common cause failure (CCF) and treat this either through direct quantification of the likelihood of the basic events in a minimal cut set or, more commonly, through the addition of additional basic events representing different CCF events. Note that in the case of treating intra-system dependencies, special care must be taken to address CCF when employing a detailed (e.g., processor card level) I&C system model.

Completeness is clearly difficult to achieve and impossible to prove (at a practical level) when analyzing rare events involving incompletely understood systems. Nevertheless, it remains a goal for the analysis; the analyst must at least demonstrate that a reasonable process for identifying and addressing failure causes has been employed. Such a demonstration might, for example, show how lessons from past relevant experiences has been incorporated in the analysis. It is recognized that the demonstration is likely to be more difficult for software failures than for hardware failures.

In striving towards increased accuracy in the analysis, it is important to recall that the purpose of an NPP PRA is to support some form of decision making. Consequently, the answers obtained need not be perfect; they only need to be "good enough," i.e., sufficiently accurate that refinements in the analysis would not change the decision being made. One approach for drawing this conclusion is to show that the risk contribution of a system, structure or component (SSC) is small. Some commonly-used criteria are as follows.

C The total CDF from the scenarios involving the SSC is a small percentage (e.g., 1%) of the CDF from all other scenarios. (More generally, the "risk importance" of the SSC, as quantified by a number of formal metrics, e.g., the Fussell-Vesely importance measure, is small.)

C All of the cutsets involving the SSC have frequencies below the cutset truncation frequency (typically ranging from 10^{-9}/yr to 10^{-12}/yr) employed when quantifying the PRA model.

C The likelihood of scenarios involving the SSC is much smaller than the likelihood of scenarios not involving the SSC but having a similar impact on the plant.

Because, in general, no single SSC failure leads directly to core damage[5], each of these criteria includes the likelihood of failure of other SSCs, operator actions, or both. It can be seen that careful attention to the quantification of these other contributors to a scenario can reduce the need to perform a detailed analysis for the SSC in question.

Consider a hypothetical BWR where a failure of the digital I&C system can lead to a small LOCA and failure of automatic actuation signals to HPSI. If it can be shown that the means to detect and diagnose the problem and to actuate necessary equipment (e.g., manual actuation of HPSI or the combination of ADS and RHR) are independent of the I&C failure, the frequency of core damage due to this event can be considerably less than the frequency of the initiating I&C failure. Schematically,

$$\lambda_{CD} = \lambda_{I\&C} * P_{HE} * P_{HDWR}$$

where λ_{CD} is the frequency of core damage due to the postulated scenario, $\lambda_{I\&C}$ is the frequency of failure of the I&C system in the mode postulated, P_{HE} is the probability that the operators fail to properly detect, diagnose, and respond; and P_{HDWR} is the unavailability of the other hardware systems. Depending on the available time and indications, the quality of procedures and training, etc., a simple, conservative analysis might put P_{HE} on the order of 10^{-1} to 10^{-2}. Depending on the specific systems involved, P_{HDWR} might be on the order of 10^{-2} to 10^{-4}. Assuming a typical total BWR CDF of around 10^{-5}/yr, it follows that $\lambda_{I\&C}$ need not be especially small to ensure that the contribution of the postulated scenario is a small fraction of the total CDF. If the total number of scenarios involving the I&C system is small, it can be seen that a relatively conservative analysis of the I&C system may suffice.

The same situation can be examined without considering P_{HE} and P_{HDWR}; if it can be shown that a conservative estimate of $\lambda_{I\&C}$ is much smaller than the product of the small LOCA frequency and the HPSI unavailability, a detailed analysis of the I&C system may not be required. The catch with this approach and the preceding one has to do with the assumed independence of the I&C system failure and subsequent operator and safety system responses. If the I&C failure significantly degrades these responses, a conservative I&C analysis may not lead to conservative CDF predictions.

Credibility

Because the PRA is intended to support decision making, it must be credible to the decision maker. Among other things, this requirement implies that the data used in the quantification process must be at least arguably credible to a significant portion of the technical community. The problem is, for NPP digital I&C systems (and with new systems in general), the experiential data are sparse or non-existent. The analyst must consequently use alternative, less satisfactory sources of information. The two most commonly used sources are: a) data from other industries and applications, and b) expert judgment.

[5]The reactor pressure vessel provides one possible exception.

At first glance, it might be supposed that industry failure data should be useful. Indeed, in the case of certain types of hardware (e.g., commercial off-the-shelf processor boards), the data may be directly relevant. In the case of software, however, it is not clear that failure data for one package is applicable for another package. Even if the two packages are nominally identical, this concern can arise if they are deployed in different operational environments. A discussion on the issue of applicability is provided later in this paper. For the purposes of this discussion, it is sufficient to note that when using experiential data to quantify the likelihood of occurrence of a software fault, it is especially important to provide the basis for assuming that the data are applicable.

Expert judgment is used in PRA in situations where data needed to estimate PRA model parameters are sparse and the resources and/or time available to generate such data (e.g., through experiments) are too limited. The use of appropriately structured elicitation techniques can require significant resources but is generally required to develop credible parameter estimates. One issue of relevance to a digital I&C system analysis concerns the experts' understanding of the specific parameters they are trying to estimate. If they are trying to estimate parameters for which they may have little direct experience, the elicitation process must be designed to ensure that they are properly educated and baselined. As a simple example, it is important to recognize that failure rates are computed quantities and may be unfamiliar to some experts, while failure events are observable and widely understood; confusing the two can lead to incorrect assessments of uncertainty. The elicitation process must also ensure that the experts share the same understanding of each question. This is particularly important when asking about software failure rates, as variations in the boundary conditions assumed by each expert (e.g., whether the input stream is completely specified) is likely to lead to significant variations in the provided answers, or even in the belief that the question is meaningless.

Uncertainty

Epistemic uncertainties in the results of the I&C analysis (which are typically in the form of conditional or total failure frequencies, i.e., measures of aleatory uncertainties) arise from two sources: uncertainties in the values of the parameters of the I&C system model, and uncertainties in the form of the model. Parameter uncertainties arise because the data needed to quantify the model parameters are sparse. The treatment of these uncertainties, once specified, is routine and easily accomplished using current tools. Model uncertainties arise because there is insufficient understanding of the process being modeled, the model's approximation of reality introduces a bias of unknown magnitude, or both. PRAs sometimes treat these uncertainties when dealing with external events (e.g., earthquakes, fires) because: a) the underlying phenomenology is not well understood, and b) the different explanations of the phenomenology can lead to significantly different estimates of risk.

A digital I&C system analysis appears to require a treatment of model uncertainties for similar reasons: there is no agreed upon approach to address the software contribution to system failure (see the discussion in the following section), and system failures may have far reaching consequences on other plant systems. It should be recognized that there is no widely accepted generic approach for dealing with model uncertainties. For example, the pragmatic approach of assigning probabilities to each model and summing the weighted results has

philosophical difficulties.[6] For the present, until a standard approach is defined, it appears that the most a PRA can require is the identification of key modeling assumptions that can lead to significantly different results and a discussion of the reasonableness of these assumptions, given currently available evidence on digital I&C systems behavior.

Issues in Analyzing Digital I&C System Performance

In principle, it appears that the treatment of digital I&C hardware failures can be treated straightforwardly within a PRA framework. This section provides some brief comments on two areas of controversy in the treatment of software failures.

On the Concept of Software Failure Rates

One argument raised concerning the difference between software and hardware is that the former doesn't age. Consequently, software failure is a design error phenomenon. Either the fault exists at the beginning of life, or it doesn't; it does not come into existence at some point in time. This argues against the use of aleatory models for random failure which quantify the fraction of times the software fails. Instead, it implies an epistemic model in which the software is always failed (with some probability) or always good (with the complementary probability). The aleatory and epistemic models can lead to different decisions, as shown in Figure 3. In this figure, it is assumed that the software is demanded to function with rate λ. The aleatory model (Figure 3a) says that with frequency λp, the software is demanded and fails. The epistemic model (Figure 3b) says that the frequency of software demand and failure is λ with probability p and 0 with probability 1 - p.

While this argument has some merit when considering software in isolation, the problem is all practical systems employing software also employ hardware and can be affected by operator input. Consider, for example, the triggering of software faults (e.g., coding errors). While the behavior of the software portion, once coded, is deterministic, the precise input stream which may trigger a software fault may be the result of hardware or human faults and is random (at least from the point of view of typical PRA models). As another example, the hardware on which the software runs is subject to aging; assumptions built into the software (e.g., regarding event timing) may no longer be valid when key hardware degrades or fails. Even considering software by itself, software revisions to fix existing faults, provide functional improvements, or allow compatibility with upgraded hardware can also introduce errors.

It therefore appears that, from a philosophical standpoint, modeling "software failures" as the result of aleatory (random) processes is reasonable (as long as detailed models for the input stream, time-dependent hardware degradation and failures, software revisions, etc. are not employed). From a current PRA standpoint, such an approach will eliminate the need to significantly modify existing plant models to accommodate digital I&C systems.

---

[6]Such an approach implies that one and only one model is "correct", whereas, by definition, all models are imperfect representations of reality. Furthermore, the alternative models are mixtures of sub-models and are often not mutually exclusive. Papers presented in (Mosleh, et al, 1996) provide differing viewpoints on the proper treatment of model uncertainty.

As an aside, it should be noted that concerns over the meaningfulness of conventional reliability modeling approaches for treating software due to the deterministic behavior of software can easily be raised in current PRA treatment of operators and hardware. It can be argued that if a particular operator or component was modeled in great detail, and if the boundary conditions of the analysis were drawn very tightly, the failure process could be (and perhaps should be) treated as being far more deterministic. For example, in the case of human error, some important types of operator errors can be triggered nearly deterministically by faulty input, yet such failure events are modeled as being random. While it is probably safe to say that, when considering a specific software package and a specific operator, software failures are inherently more deterministic than human errors, the degree of this difference is arguable.

As a second example, a PRA model for a given pump does not ask if the pump has a crack in the shaft which will, under planned service conditions, cause failure with certainty upon demand. Instead, crude Poisson or Bernoulli process models are used to represent the analyst's uncertainties in pump performance (e.g., due to variability in components and their service conditions). It is not completely clear that a software analysis must be performed at a greater level of detail than used for human or hardware faults, even if such a detailed analysis is possible.

Note that this discussion is focused on the needs of current PRA. If and when more detailed (e.g., dynamic) models for plant response are employed, the needs of PRA may be changed.

On the Applicability of Software Failure Data

A key issue in determining the probability that a software package performs as intended is the applicability of failure data collected for other software packages. The concern arises because of the "non-linearity of software", i.e., the fact that very small physical changes in the software can lead to radically different behaviors of the package. It therefore can be argued that each software package, especially when considered in the context of its own operational environment, is unique. Therefore, data for other packages, even if they are nominally similar or even identical, may be irrelevant.

While this argument has some merit from a deterministically predictive viewpoint, it does not reflect the modeling philosophy of PRA. First recall that the probability that a software package fails in a particular manner (denote this by Q_S) reflects both aleatory uncertainties and epistemic uncertainties. While the former may be negligible if the analysis boundaries around the software package are drawn tightly enough (see the preceding discussion on the notion of software failure rates), the latter invariably exist. The analyst simply does not know for certain if the software package has errors that will cause the specified fault.

As a probability, Q_S, by definition, is supposed to reflect the analyst's complete, current state of knowledge about the possibility of failure. Thus, as long as a particular failure event informs the analyst to some degree about this possibility, it is relevant to the estimation of Q_S. The real question is, from a Bayesian estimation perspective, what is the appropriate likelihood function for the data. If the random failure model is judged to be acceptable for software, the likelihood function can be developed in a manner analogous (if not identical) to that used to estimate

hardware failure rates. If the random failure model is not acceptable, some additional thought may be required.

It is useful to note that a similar situation is commonly addressed in current PRAs. In the analysis of common cause failure (CCF) events, arguments have been raised concerning the applicability of multiple failure data. (CCF events tend to involve very plant-specific features -- it is not clear that events occurring at one plant are directly applicable in the analysis of another plant.) To address these arguments, a somewhat *ad hoc* approach is being employed in which "impact vectors" are used to measure of the degree of applicability of a CCF event for a particular analysis. Of course, there are situations where the data are clearly inapplicable (e.g., the failure mode involves a particular piping configuration not present at the plant being analyzed). Expert judgment, based on the engineering characteristics of the plant suffering the event and the plant being analyzed, provides the basis for determining this applicability as well as for quantifying the impact vectors.

A similar approach may be useful for a software analysis. The key, of course, is the identification of the software package characteristics (perhaps function, operating environment, method of production, method of verification and validation, etc.) that will allow the determination of gross applicability and the systematic quantification of impact vectors.

References

Apostolakis, G., "A commentary on model uncertainty," in *Model Uncertainty: Its Characterization and Quantification*, A. Mosleh, N. Siu, C. Smidts, and C. Lui, eds., Center for Reliability Engineering, University of Maryland, College Park, MD, 1995, pp. 13-22.

Kaplan, S. and B.J. Garrick, "On the quantitative definition of risk," *Risk Analysis*, 1, 11-37(1981).

Mosleh, A., N. Siu, C. Smidts, and C. Lui, eds., *Model Uncertainty: Its Characterization and Quantification*, Center for Reliability Engineering, University of Maryland, College Park, MD, 1995, pp. 13-22.

Siu, N., "Risk assessment for dynamic systems: an overview," *Reliability Engineering and System Safety, 43*, No. 1, 43-73(1994).

Drouin, M.T., et al, *Analysis of Core Damage Frequency: Grand Gulf, Unit 1 Internal Events Appendices*, NUREG/CR-4550, Vol. 6, Rev. 1, Part 2, September 1989.

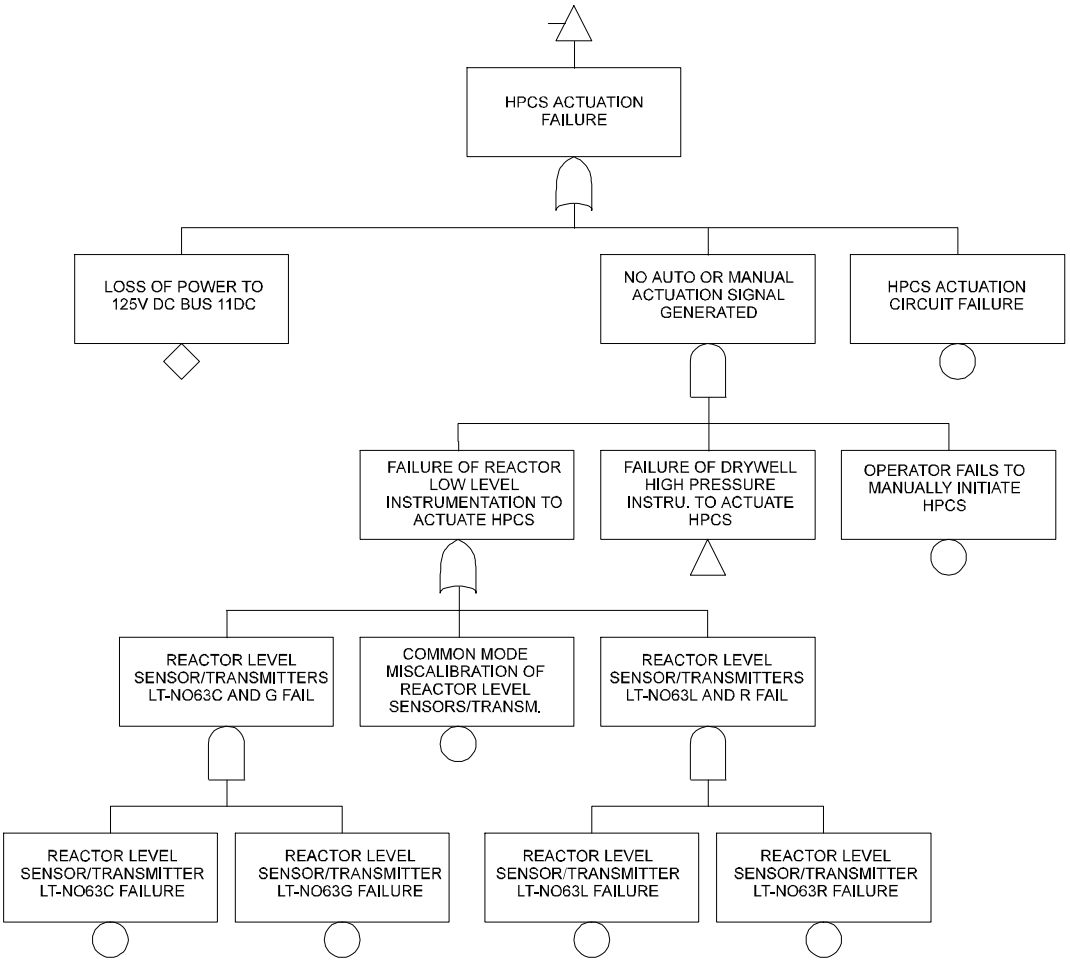

Figure 1. Example PRA Treatment of Actuation Failure
(Adapted from Figure B-1, NUREG/CR-4550, Vol. 6)

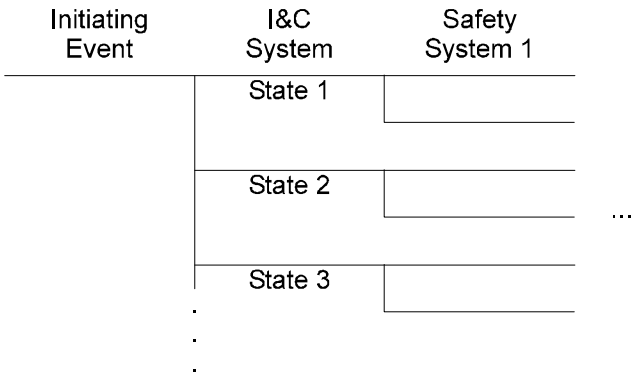

Figure 2a. I&C System as Event Tree Top Event

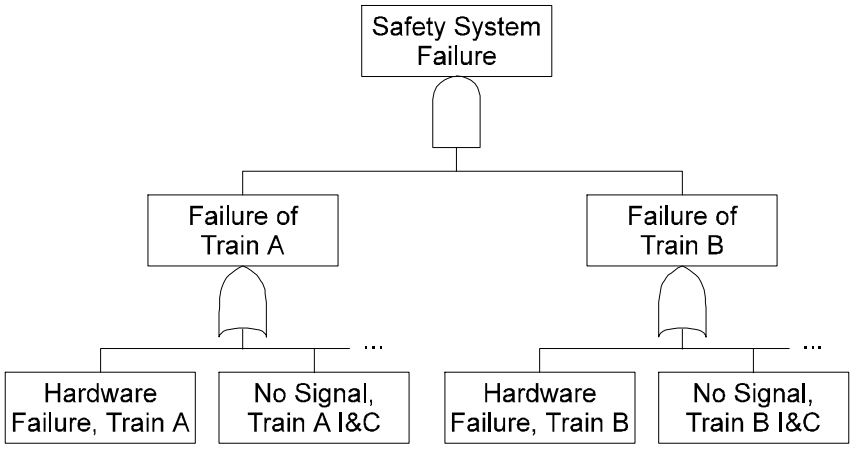

Figure 2b. I&C System as Fault Tree Gates

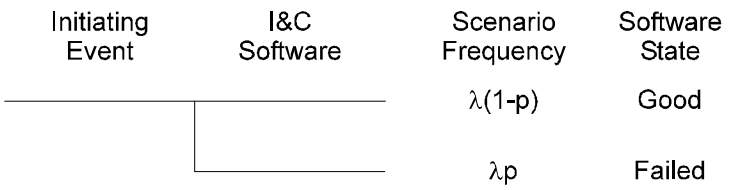

Figure 3a. Aleatory Model of Software Failure

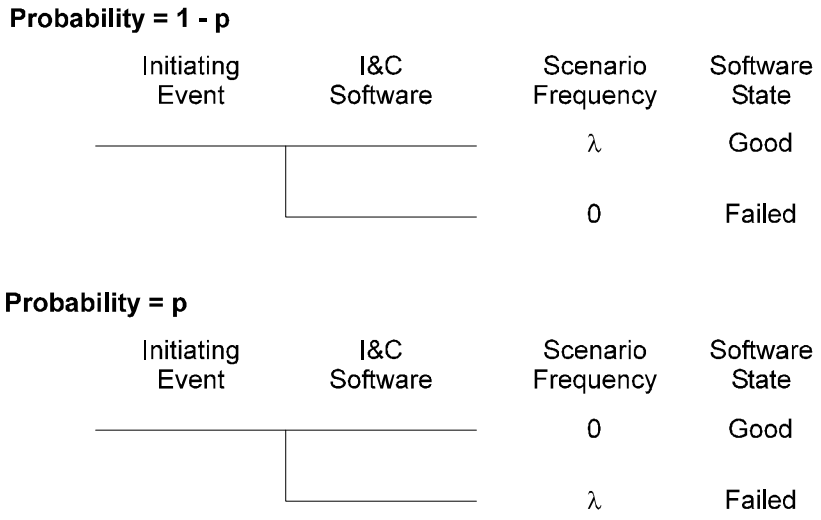

Figure 3b. Epistemic Model of Software Failure