



● codd Brian Shevon
57 FR 59363
MAR 19 1993 12/15/93
⑮ ✓

March 11, 1993
JPN-93-014
IPN-93-010

Regulatory Publications Branch
Division of Freedom of Information
and Publications Services,
Office of Administration
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

Subject: James A. FitzPatrick Nuclear Power Plant
Docket 50-333
Indian Point 3 Nuclear Power Plant
Docket 50-286
Comments on Regulatory Guide 1.28 - Quality
Assurance Program Requirements

Dear Sir:

This letter is in response to the Commission's November 24, 1992 invitation to provide comments on proposed Revision 4 of Regulatory Guide 1.28 "Quality Assurance Program Requirements" (DG-1010). Emphasis is given on how to apply risk-based techniques to quality assurance programs. A methodology for ranking of systems, structures, and components (SSCs) according to their safety significances is proposed and for addressing the regulatory processes that should be applied to important SSCs. Comments are also provided on how performance-based regulation might be utilized when implementing quality assurance programs.

Attachment I to this letter provides detailed recommendations where risk-based techniques can be applied to the QA process. The Authority requests that these recommendations be incorporated into part B of this regulatory guide. The Discussion portion of the guide related to performance-based regulation (on page 5) could be expanded to include risk-based regulation concepts, as well. Indeed, both risk-based and performance-based regulatory processes provide opportunities for improving QA programs.

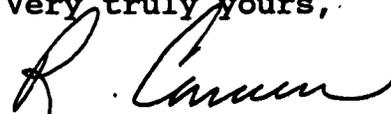
In the near term, the Authority recommends that review of quality assurance should concentrate on active and passive components. In operating plants, there appears to be little

incentive for quality assurance program changes for structures, although the consideration of risk significance might allow greater use of conventional construction codes for plant modifications.

Attachment II contains a broader discussion of the issue.

If you have any questions, please contact Herschel Specter at 914-681-6994.

Very truly yours,



Radford J. Converse
Vice President -
Nuclear Support

RJC:HS:gs

cc: Mr. M. Nicola F. Conicella, Project Mgr.
Project Directorate I-1
Division of Reactor Projects - I-11
U. S. Nuclear Regulatory Commission
Mail Stop 14B2
Washington, D. C. 20555

Mr. Brian C. McCabe, Project Mgr.
Project Directorate I-1
U. S. Nuclear Regulatory Commission
Mail Stop 14B2
Washington, D. C. 20555

ATTACHMENT I TO
JPN-93-014 AND IPN-93-010

I. RECOMMENDATIONS

In the recommendations given below, the term "risk significant" is frequently used. It is suggested that a value of one percent of the mean core melt frequency be used as the definition of risk significance. With such a definition an SSC whose risk ranking shows that it does not impact the core melt frequency by more than one percent, would be considered as not-risk-significant. Additionally, if enhanced QA practices on an important SSC do not lead to a one percent impact on core melt frequency, relative to normal, commercial QA practices, then such enhancements could be considered as not risk significant.

1. If, after applying risk-based techniques, it is determined that certain SSCs are not risk significant, then normal, commercial QA practices should be applied to such SSCs,
2. If an SSC is found to be risk significant, then searches should be made for data bases that record the performance of such a risk significant SSC. One of these data bases should reflect SSC performance where nuclear QA practices have been applied to the SSC, while the other data base should reflect SSC performance under normal commercial QA practices. If an examination of these data bases reveal that there are no statistically meaningful differences in the performance in safety grade and not-safety grade versions of the same type of SSC, then normal QA commercial practices should be used for this risk significant SSC. Should these data bases searches reveal statistically meaningful performance differences, probabilistic safety analyses should then be made to evaluate if such performance differences are themselves risk significant. If such performance differences are not risk significant, then normal, commercial QA practices should be used.
3. If the search for safety-related and not safety-related SSC performance data bases does not yield two distinct

data bases, then PRA sensitivity analyses should be made with a single data base. [One can assume a normal distribution of an SSC's availabilities and reliabilities around median values, determined from the single data base.] If PRA analyses using availability and reliability values at one or two standard deviations away from their median values do not result in risk significant differences, then normal, commercial QA practices should be used.

4. In the event that adequate data do not exist to perform PRA sensitivity analyses, an expert elicitation process should be used to establish which QA codes and practices should be applied.
5. If warranted, experiments or tests should be made on specific SSCs to see if different levels of QA practices reduce their failure modes in a risk significant manner.
6. Where it has been established that enhanced QA efforts are warranted, the use of performance-based approaches should be encouraged, where practical.

II. OTHER OBSERVATIONS

1. Even for SSCs that are risk significant, it should be established that nuclear QA practices lead to higher reliabilities and availabilities for the important SSCs when performing their safety functions. If the dominant causes of an SSC's non-performance of its safety function are station blackout, human error, or other non-QA related reasons, then normal commercial QA practices should be utilized. Stated differently, it should be demonstrated that QA practices, beyond those in normal commercial practice, effectively reduce an SSC's dominant failure modes enough to cause a risk significant change.
2. The relationships between active components and QA should be examined closely. Because of the redundancy of safety-related active components brought about by the application of the single failure criterion, random failures may not be risk significant. If random failures of active components are not risk significant,

QA efforts directed at limiting random failure rates may not be risk significant. The importance of QA in active components might be limited to preventing simultaneous common cause failures in like components or in the support systems that serve these components.

3. With regard to passive components, progress is being made through the ASME on risk-based approaches to important pressure boundaries. This results of this ASME effort should be utilized, if acceptable.

ATTACHMENT II TO
JPN-93-014 AND IPN-93-010

DISCUSSION

The need to reexamine how quality assurance is conducted in the nuclear industry has been identified before^{1,2}. One conclusion, shared by many, is that the original and fundamental purpose of quality assurance is sound: "The quality assurance program shall provide control over activities to an extent consistent with their importance to safety." What differs today is our increased ability to identify, in a quantitative way, the risk significance of SSCs and then to evaluate if specific quality assurance programs applied to these important SSCs result in risk significant improvements.

As discussed in reference 2, the two most fundamental questions to be answered in any regulatory process, including quality assurance, are: (1) What is important?, and (2) What do we do about it?

A. What is important?

With regard to this question, probabilistic safety assessment (PSA) studies can be utilized to rank the safety significances of various SSCs. Using core melt frequency (CMF) as a measure of safety significance, a number of PSA studies have shown that the number of active components that affect the CMF is comparatively small. For example, an NRC sponsored study of the Surry nuclear plant revealed that 99% of the CMF was dominated by just 75 active components³. At 99.9% of the CMF, the important active component list only grew to be 115 for this plant. Not only are lists short, such as Surry's, the length of such lists and its members are relatively independent of the ranking process selected. While some variations exist among ranking processes, one can always take the most conservative ranking process and this still results in a short list. These recent PSA ranking studies also reveal that some concerns about the uncertainties in PSA analyses are of little matter. For example, if the goal were to apply quality assurance efforts to those active components that control 99% of the CMF, the top 99.9% could be selected. This approach minimizes some uncertainty issues with only a modest impact on the scope of the quality assurance program. Furthermore, many PSA ranking methods are based on comparisons of relative risk

measures, thereby eliminating some uncertainty issues associated with absolute risk calculations. The observation that the number of plant components that are risk significant is low, means that the overall role of QA itself is limited in reducing public risks.

The Surry results were based upon a ranking process called the cumulative risk reduction. Another useful ranking process is to perturb a base case PSA analysis of a nuclear plant by setting the unavailabilities of various components equal to 1.0, one at a time, while observing the resultant increases in the CMF. The physical interpretation of an unavailability equal to 1.0 is that the PSA treats the component as if it didn't even exist. When such a ranking process was applied to the FitzPatrick nuclear power plant's PSA, the total "disappearance" of the 220th most important active component only increased the calculated CMF by $1.7 \times 10^{-7}/\text{RY}$. Thus, both the cumulative risk ranking method, and setting the unavailabilities equal to 1.0, yield similar overall results, i.e., that only a limited number of active components are risk relevant.

One must, however, go beyond utilizing CMF as the only measure of safety significance. For example, certain components are not important to CMF, but are important to maintaining containment integrity. A recent PSA ranking analysis of motor-operated valves at a nuclear plant revealed that of all the MOVs in the plant, only about 25% were important to CMF. However, by examining level 2 PSA results, some additional important MOVs were identified.

At this time the exploration of PSA level 2 or 3 safety significant components has not been as comprehensive as PSA level 1 studies, however there appears to be direct analogy between them. One can set the unavailability of certain active components, such as containment isolation valves, equal to 1.0 and observe the resultant increments in conditional containment failure frequency (CCFF) or expected offsite person-rems. Those PSA level 2 or 3 components that cumulatively capture 99% to 99.9% of the CCFF or expected offsite person-rem might be judged to be safety significant. It is likely that far fewer components in a nuclear power plant have a PSA level 2 or 3 function, compared to those that have a PSA level 1 function.

The identification of risk-significant passive components and risk-significant structures has not been addressed as

comprehensively as active components. For operating plants the need to identify risk significant structures appears to be limited. Relatively few quality assurance actions need be taken once the structures have been erected. For new construction one can estimate the risk significance of particular structural components. A risk significant structure would either house* or would support a risk significant active or passive component, or would itself perform a safety function, or would initiate or worsen an accident sequence upon failure. Using the above definitions, the following are examples of risk significant structures:

- A. The structure that houses the main plant batteries,
- B. The structure (e.g. reactor pedestal) that supports the reactor vessel,
- C. Fire barriers and containments are examples of structures that directly perform safety functions,
- D. If failure of a support structure could cause a water tank at a plant to fail and thereby flood a critical area, then this water tank support structure is safety significant. Only those structures whose failures could cause an increase of one percent in the CMF or CCF should be considered.

It may be possible to estimate the health consequences of failures of particular structures by assuming that such failures also cause the active or passive component(s) served by or affected by the structure, to fail. To convert the above consequences into risk parameters, one has to estimate the frequency of failure of each of the above structures. Such frequency values may be available in the literature for similar structures or through various

*More precisely, a structure is risk significant if it would protect a risk significant SSC against those important plant challenges that both call upon the risk significant SSC to perform its safety function and also might cause the failure of the same risk significant SSC, were it not for the protection given by the structure.

structural analyses, particularly analyses which examine seismic loads on structures. Assuming that reasonable failure frequencies can be gathered, the risk significance of a structure is its failure frequency multiplied by the health consequences of the loss of the active and passive components (and possibly other structures) served by or affected by the failed structure.

The above may be an unnecessarily complicated analysis. A much simpler approach is to first identify the safety significant active and passive components and then using the four definitions, given above, determine the risk significant structures. Structures that are judged to be safety significant might be subjected to enhanced quality assurance programs, provided that it can be determined that the enhanced QA programs affect the failure probabilities of the structures they applied to in a cost-effective way. All other structures should utilize normal commercial practice quality assurance programs.

Ranking passive components according to their safety significances may be derived from previous analyses of active components that serve the same overall function. For example, failure of a heat exchanger in a residual heat removal train may have the same safety consequences as a failed valve in that same train. If the failure of a passive component also causes the initiation of an accident sequence, such as a LOCA, it is likely that this is already accounted for in the PSA. Acquiring acceptable data on passive failure rates may be challenging.

In summary, a considerable amount of progress has been made in the past year in identifying risk significant active components through PSA ranking methods. Identification of risk significant passive components and structures has not received the same emphasis, but it appears that the methodologies applied to active components could be extended to include passive components and structures, provided basic failure rate data exist. In order to generate a comprehensive list of the risk significant SSCs, several measures of significance will need to be used in order to cover PSA levels 2 (or 3) issues, as well as CMF (PSA level 1) issues. Both internal and external initiators have to be considered, at various plant operating configurations (e.g. at power or when shut down).

B. What do we do about it?

Once PSA techniques have been applied to identify the risk significant SSCs, attention can then be turned to the second fundamental regulatory question: "What do we do about it?" One major step forward would be to apply good commercial practices to those SSCs that are not risk significant and remove them from the regulatory review process. Regulatory attention would then turn to the highly ranked SSCs.

What is the benefit of enhanced quality assurance efforts for the risk significant SSCs? If safety-related and non-safety related failure rate data and availability bases exist and comparisons show little difference, then normal commercial practices should be applied. If such data bases are found and the associated failure rates or availabilities do vary appreciably, other PSA evaluations can be made. The starting point is to examine the principal failure modes of these SSCs. For example, if station blackout and human error are major causes of the loss of SSCs (particularly active components), then quality assurance itself for these SSCs, is of limited value. If high failure rates are due to poor maintenance or inappropriate operational testing, then to achieve reduced failure rates, efforts need to concentrate on these areas, not QA. In order for quality assurance to be risk relevant for a SSC, then it must address the principal failure mode(s) of that highly ranked SSC.

One can also perform various PSA sensitivity studies on a highly ranked SSC to judge if a higher failure rate would have a large impact on CMF or CCFF. If both safety and non-safety related failure rate and availability data bases are available, then CMF or CCFF calculations can be made, one at each failure and availability rate. Small differences in CMF or CCFF results means that augmented QA efforts, beyond normal commercial practices, are not warranted. If only one data base is available, one can assume a statistical distribution of failure rates around the mean or median failure rate. Assuming that one or two standard deviations encompass both safety and non-safety related failure rates, then the two PSA results can be compared, as above, when two separate data bases are available.

The possibility exists that the data base is insufficient to make a statistically valid determination on the value of enhanced QA efforts, as applied to some risk significant

SSCs. In such cases one may turn to the expert elicitation process. Experts may be able to judge if one code of practice versus another produces risk significant gains [e.g. ASME Section III (nuclear) versus Section VIII (conventional) for vessels and ACI 349 (nuclear) versus 318 (conventional) and their quality assurance programs]. In such cases of limited data, the QA practices recommended by an expert panel should be followed.

Because of the application of the single active failure criterion, nuclear plants have considerable redundancy and diversity. Occasional random failures in active components is therefore unlikely to result in the loss of an important safety function.

In summary, even though an SSC may be ranked as risk significant, it is not a foregone conclusion that enhanced quality assurance efforts for that SSC are appropriate. There can be a number of failure modes that an SSC may be subjected to and improved quality assurance may not be a risk significant effort relative to other options.

Should an SSC be both highly ranked and its performance potentially affected by a quality assurance program, one still needs to determine which quality assurance program should be utilized. One can set the unavailability of a particular active component equal to zero and rerun the base case PSA. The physical interpretation here is that this is a "perfect" component; it never fails. If the reduction in CMF or CCF is small when the unavailability is zero, then there is little justification for trying to improve the existing quality assurance program. Should QA appear to be valuable, then this could be an important opportunity for performance-based regulation. As described on page 5 of Reference 2, it may be far more effective to test a statistically meaningful sample of material, as delivered to a site, than to rely on our present paper/record intensive QA practices. If the NRC and a utility agree upon some quality assurance goal, then it would be up to the utility to develop a program to implement this goal. In many cases this would be superior to the highly prescriptive QA practices we now have.

Page 4 of Reference 3 cautions that there are safety significant SSCs which, due to their low failure rates, are screened out of typical PSAs. An open question is then:

"If QA were absent in these presently screened out SSCs, would their failure rates increase to the point that they would no longer be below the cut-off level for PSA consideration?" This area needs to be developed further, however, implementation of the Maintenance Rule may be helpful here. For example, the performance of highly ranked SSCs and the frequency of major initiating events, as identified by a plant's PSA, would be monitored under the Maintenance Rule. If such performance degrades unacceptably, then it would have to be determined if this was caused by some SSC originally excluded from the PSA or later excluded because it was below the 99% cut-off-level and subsequently treated as an unregulated item. If so, then corrective action would be taken, with the possibility that the corrective action would be improved QA on this previously excluded SSC.

References:

1. "Nuclear Safety: An Overview of its Effectiveness and Efficiency," H. Specter, ANS Topical Meeting, Portland, Oregon, July, 1991
2. "Shifting the Regulatory Paradigm," H. Specter, ANS Executive Conference, Marco Island, Florida, October, 1992
3. "PSA, Calculus, and Nuclear Regulation," H. Specter, ANS Topical Meeting, "PSA '93," Clearwater, Florida, January, 1993

DISTRIBUTION LIST

JAF

H. Salmon
R. Barrett
D. Lindsey
M. Colomb
A. Zaremba
J. Hoddy
RMS

NYO

G. Goldstein
A. Levine

WPO

R. E. Beedle
R. Converse
S. Zulla
W. Josiger
J. A. Gray, Jr.
T. Dougherty
R. Ram
R. Lauman
A. Klausmann
K. Mavrikis
G. Wilverding
C. Patrick
J. B. Ellmers
J. A. Greene
M. Jacobs
M. Mora
A. Stewart
H. Fish
L. Labruzzo
K. Kingsley
J. Patel
RMS-WPO