

DS0911
B. MORRIS

THOMAS D. MATTESON
1933 LITTLE RIVER ROAD
FLAT ROCK, NC 28731

870

S-41F E 33987

October 30, 1989

NOV -6 - P 128

8/17/89

(D)

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

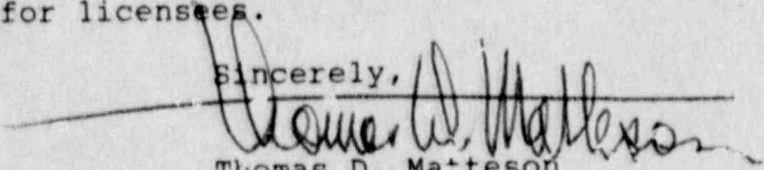
Gentlemen:

Thank you for the opportunity to comment on DG-1001.

It shows considerable progress in the Commission's understanding of maintenance management at nuclear power plants. There are several items that I believe to be of importance which I have discussed in my answers to your specific questions and commented on, in some detail, as I reviewed the text.

I am sure that you have a growing understanding of the awesome task of going from "full stop" to "full speed ahead" in regulating the safety aspects of a technology in which most of knowledge still resides in minds of successful practitioners. Knowing that, I am sure that you see the value in a few powerful, efficient constraints rather than a lot of fuzzy, intuition-based rules which, once established, become a Gordian knot for licensees.

Sincerely,



Thomas D. Matteson

B911010381 B91030
PDR REQD
01. XXX C PDR

COMMENTS ON THE USNRC DRAFT REGULATORY GUIDE DG-1001, AUGUST 1989

Prepared by:

Thomas D. Matteson
1933 Little River Road
Flat Rock, NC 28731

1. What level of detail should be included?

Since the objective of the Guide is to give licensees guidance on methods acceptable to the NRC for planning, conducting and assessing the effectiveness of nuclear power plant maintenance, the Guide must include useful examples, but these must not inhibit creativity by the licensees. (e.g., the "reliability program" designed by United Airlines differs significantly from what the reader of FAA Advisory Circular AC120-17A might expect, unless he had very broad knowledge about the potential alternatives.)

FAA Advisory Circulars have an objective similar to this Regulatory Guide.

2. Is the scope appropriate?

The scope (applicability) should include all hardware whose failure can significantly effect safety. The scope (breadth of function) might better result in 3 separate guides -- one for each operations function (planning, conducting, assessing).

3. What criteria?

This question reinforces my suggestion that separate guides for planning, conducting and assessing be considered. Each of these functions is a separate discipline, and each relies on different families of criteria.

4. Is it appropriate to use quantitative goals?

Quantitative goals are the primary fabric of the managerial process in the air transportation community. Certainly a "seat of the pants" approach works well if an operation is small enough for the senior executive to be in direct contact with the operation, but not for such a large activity as a nuclear power plant.

It is, however, important to recognize that most of the goals used by airline maintenance management are basically economic, not safety, goals. Keep in mind that design plays a major role in ensuring that hardware failures and human error do not affect safety. Therefore, a properly designed plant should require relatively few safety goals.

The "Reliability-Centered Maintenance" process has been used

effectively to identify those elements of a particular operating system whose failures threaten safety. It, of course, focuses primarily on the "planning" function.

Some careful experimentation is necessary to make a rational selection of quantitative goals for the conducting and assessing functions. Failure to conduct such experiments will result in expensive, elegant, misleading information.

For the assessing function, I believe that a few simple time series plots of selected performance measures will be the most efficient means for measuring safety. Keep in mind that if the designer has done his job well, there will be few instances in which reliability and safety are correlated. (Alert managements will, of course, find measures of reliability and maintenance effectiveness that are powerful tools for ensuring or improving the efficiency of operations. These are, I believe, outside of the regulatory charter of the NRC.)

5. What quantitative measures?

After an embarrassing attempt by the FAA to impose some engine overhaul period constraints based on shutdown statistics, the FAA came to several airlines who had experienced analytical resources. A program for understanding the use of quantitative measures was developed jointly that ultimately had a major effect on the design of airline preventive maintenance programs. It would be a major error for the NRC to go through the same trauma.

Quantitative goals should be established at the highest hierarchical level at which they can achieve their objectives. Safety measures should signal the need for action but not, necessarily, provide problem-solving information. Otherwise they require the recording of a great pile of information that will rarely be used.

COMMENTS ON THE TEXT

PARA B-1

1. The first sentence is too broad. Insert "important parts" after "quality"
2. 9th line: add "certain" after "of"
3. 10th line: delete "effectiveness"

PARA B-2

1. first line: delete "at nuclear power plants"
2. 4th line: after "this" add "definition"
3. 5th line: after "this" add "definition"

PARA B-3

1. 2nd line: replace "expected to" with "will"
2. 3rd line: replace "an effective maintenance program" with "safety"
3. Delete the last sentence. Degradation of the function of redundant components need not always promptly be restored. (The more restrictive statement follows immediately in Section C.)

Section C
TOPIC PARA

Delete "or security" in the last line -- and where it is repeated throughout the document.

The phrase "plant safety and security" is confusing. Plant security is obviously an entirely separate problem and should be so treated.

Insert the following:

An operator's maintenance program has four objectives:

- o To ensure realization of the inherent safety and reliability levels of the systems affected
- o To restore safety and reliability to their inherent levels when deterioration has occurred
- o To obtain the information necessary for design improvement of those items whose inherent reliability proves inadequate
- o To accomplish these goals at minimum cost, including maintenance costs and the costs of residual failures (including the opportunity costs of lost revenue)

PARA C-1

1. 2nd line: delete "and their supporting systems" (There is always a temptation to reach out with a fuzzy phrase and destroy the precision of the preceding statement. How do you limit the bounds implied by the words "supporting system"?)
2. 3rd line: delete "or security"
3. 11th line: delete all after "mitigation" (The remainder of the paragraph is "reaching" again.)

PARA C-1.1

1. 2nd line: delete "and security"

PARA C-3.1

1. Note that the quotation in paragraph one is inconsistent with the statement in the topic paragraph (C. REGULATORY POSITION) which correctly limits the scope to items that can significantly affect safety; ("security" should be deleted as previously noted).

PARA C-3.2

1. A plant specific PRA will be useful, but its level is likely to be insufficiently specific for this purpose.
2. Although NPRDS data may be useful, its failure to capture the source's definition of failure is a problem for the careful analyst.
3. The recognition of the importance of redundancy is of major importance in the process of selecting appropriate goals. The paucity of directly applicable data makes the application of confidence bounds as part of the goal-setting process of questionable value. Some major airline "reliability programs" do not use them.

PARA C-4, C-5, and C-6

1. Recommend deletion of these paragraphs, unless the majority of the operators find them to be of great value.

Section D

By what process will the NRC determine what is "an acceptable alternative"? Obviously, there are risks of accepting a bad program and of rejecting a good one. The NRC must therefore, in good faith, be prepared to have a high degree of confidence in its decision-makers. It has limited experience, and the affected power plants are widely distributed, of widely varying design and operated by organizations of widely varying culture and experience. The decisions to be made require knowledge and experience which is a serious challenge that must be recognized and appropriately met. Otherwise, there is considerable risk of the imposition of unnecessary constraints that will increase operators costs as well as actions that may inadvertently increase safety risks.