UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

March 11, 1977

MEMORANDUM FOR: L. J. Evans, Jr., Chief
Requirements Analysis Branch

FROM: Dean M. Kunihiro, Program Analyst
Requirements Analysis Branch

SUBJECT: LANGUAGE FOR OTHER THAN PERFORMANCE AND SYSTEM SPECIFICATION REQUIREMENTS

The purpose of this memo is to expand upon the issues relating to the language of other than performance and systems specification portions of the upgrade rule that were identified and outlined in my memo to you dated March 8, 1977.

a. Threat

No change in wording of the threat statement contained in 73.55 is advisable. The same basis and rationale given in the Rusche-Chapman memo to the Commission (2 Feb 77) is applicable to justify its use in the upgrade rule.

b. Redundancy and Diversity

To require the licensee to provide redundancy and diversity in the design of his safeguard systems is conceptually appealing. However, many practical considerations make such a requirement questionable.

First of all, without any established degree of sufficiency, what constitutes adequate redundancy and diversity? To require that systems are designed against common and single mode failures may have significant justification in reactor safety system design where system breakdown may lead directly to an unacceptable event, but for safeguards systems the requirement may be too stringent and ill defined. It is difficult to appreciate how the breakdown of a single safeguard component can directly lead to the successful completion of an undesirable release or illicit acquisition of protected nuclear material. The vagueness of the requirement can be illustrated by extracting the following example

from the SD draft, "Subsystem failure or component redundancy provides protection against single failure. For example, and adversary cannot defeat an alarm system by cutting off power if there is an emergency or back-up power source for safeguard equipment." What if the wire to the alarm were cut? Is an alternate circuit required? Should two alarms be installed? etc. (This nebulous nature of the requirement can result in a seemingly endless amount of redundance, which could in turn lead to racheting.)

Secondly, with the in-depth design of safeguards system inherently built into the rules by the establishment of MAs, VAAs, and PAs, and with the diversity and flexibility provided by the use of guard forces, the utility of the redundancy and diversity requirement is even more suspect.

It is not clear how the scope of application can be limited so as to resolve these fundamental difficulties and, unless they can be resolved, it is recommended that this requirement be deleted, and substituted with the requirement contained in 73.55(g), (1). It adequately states the intent of the redundancy and diversity requirements while allowing the licensee a great deal of latitude in fulfilling that requirement. Paragraph 73.55(g), (1) is shown below:

> (1) All alarms, communication equipment, physical barriers, and other security related devices or equipment shall be maintained in operable condition. The licensee shall develop and employ compensatory measures including equipment, additional security personnel and specific procedures to assure that the effectiveness of the security system is not reduced by failure or other contingencies affecting the operation of the security related equipment or structures.

c. Quality Assurance

Regulatory Guide 5.52, Chapter 3, states that a licensee should establish a quality assurance program "to provide assurance that the design, construction, and operation of the physical protection systems for a plant are in conformance with applicable regulatory requirements and with the design bases and criteria specified in the license applications." It goes on to elaborate the minute detail that the system should consist of.A copy of Chapter 3 is attached, (Enclosure A).

It is not clear that such an elaborate and detailed QA System is absolutely necessary to insure that an effective safeguards systems is employed, particularly in the design phase. Given the regulatory requirements, it would seem that an effective plant Safeguards System could be developed without a formal QA program. Either the safeguards plan is or is not acceptable to the NRC. This obviously being determined during the license review. Extending that reasoning thru the construction phase, the final system is either adequate or it is not. This again will be determined by the NRC in its compliance and site assessment inspections. To insure that the final product or system emplaced will meet NRC requirements should be the responsibility of the licensee. One would expect that the prudent licensee will take measures necessary to produce an acceptable end product. Whether he does that with a formal, detailed QA program, an informal QA program, or no QA program at all should be left up to the licensee. To expect the detailed QA program outlined in Reg Guide 5.52 Chapter 3 is a classic example of over regulation.

Once the system is operational it is clearly intended that the licensee maintain it so as to insure its continued and effective operation at all times. Since the NRC obviously does not have the resources to continuously inspect or test its operation effectiveness it is reasonable to expect the licensee to perform test and maintenance functions. If any component or subsystem fails, it is also prudent to expect that he take actions necessary so as to maintain the effectiveness of the system. These requirements to test, to maintain, and to employ compensatory measures to offset failures of the safeguards are clearly delineated in 73.55(g), (1), Test and Maintenance.

For the above reasons, quality assurance, as envisioned for reactor safety should not be extended to safeguards. A toning down can be accomplished by merely relying on a restatement of 73.5(g), (1), as quoted earlier, and deleting reference to (Chapter 3 of Reg Guide 5.52). (Part 50, Appendix B) should be deleted and not referenced, for the same reasons given above, and in addition, its frequent reference to safety functions as opposed to safeguards.

d. LLEA and Self-test

The following statement of purpose should be the basis for the LLEA and Self-test requirement:

> "To demonstrate the effectiveness and to allow assessment of subsystems as well as the entire safeguards system by both the NRC and License Management"

Recommended wording of the proposed rule:

> Each licensee shall conduct tests to demonstrate as well as assess his capability to provide physical protection against industrial sabotage and against theft of special nuclear materials. These tests shall be conducted semi-annually. In the conduct of the tests, the licensee shall take all reasonable and prudent actions required to endure the safety of all personnel involved, the protection of all property involved, and the maintenance of physical protection capabilities during and subsequent to all tests. To the extent possible the tests should be based on a variety of contingency responses, and include LLEA participation. The licensee shall notify the appropriate NRC Regional Office of these tests at least two weeks prior to the conduct of the test.

The self test would logically fit into the "Test and Maintenance" section of the existing rules if kept essentially intact as recommended above.

e. Material Amount

The SD draft uses the wording presently contained in 73.50. Without any concrete justification there exists no basis for recommending any changes in the scope of material covered.

f. Examples

Examples can in many cases be used to illustrate a particular point. However, at the same time, the examples themselves may lead to confusion and countered examples. A case in point was illustrated in the discussion in paragraph (b), above. Therefore, the use of examples in the rules is not recommended. The Regulatory Guide has been designated as the vehicle for clarification or amplification of the regulations.

Dean M. Kunihiro
Requirements Analysis Branch

Encl:
1. Chap 3 - Quality Assurance

CHAPTER 3 QUALITY ASSURANCE

To provide assurance that the design, construction, and operation of the physical protection systems for a plant are in conformance with applicable regulatory requirements and with the design bases and criteria specified in the license applications, the applicant should establish a Quality Assurance (QA) Program. In this chapter, the Preliminary Physical Security Plan should include a description of the QA Program to be established and executed for the physical protection system during the design and construction stages.

Prior to operation, the applicant should describe in his final plan the QA Program to be established and executed for the operation of the system. The QA Program should be established at the earliest possible time consistent with the schedule for accomplishing the activity covered. If some portions of the QA Program have not yet been established at the time of the preconstruction submission because the activity will be performed in the future, the description should provide a schedule for implementation. The QA Program should meet the requirements of Appendix B of 10 CFR Part 50 that are applicable and appropriate to a physical protection system.

If a portion of the QA Program to be implemented will conform to a rticular quality assurance standard, such as one adopted by the American tional Standards Institute, the description may consist of a statement that the particular standard will be followed. Where Regulatory Guides have been issued on acceptable methods of implementing portions of the QA Program, the description should specifically indicate whether the regulatory positions of the Regulatory Guides will be followed.

The applicant should provide a description of the proposed QA Program activities that will govern the quality of the physical protection systems during design and construction as well as during operation. These activities include operating, maintaining, repairing, and modifying the systems.

3.1 Organization

Organization charts for the project should be provided to denote the lines and areas of responsibility, authority, and communication within each of the major organizations involved, including those of the applicant, the architect-engineer, the system supplier, the constructor, and the construction manager (if different from the constructor). In addition, a single overall organization chart should denote how these companies interrelate for the specific project.

These charts and related explanatory material should clearly indicate the organizational location, organizational freedom, and authority of the individual or groups assigned the responsibility for checking, auditing,

inspecting, or otherwise verifying that an activity has been correctly performed. The charts and discussions should indicate the degree of the applicant's involvement in verifying the adequacy of the QA programs implemented by the applicant's contractors and suppliers, even in those cases where the applicant has delegated to other organizations the work of establishing and implementing the QA Program, or any part thereof.

3.2 Quality Assurance Program

The structures, systems, components, and equipment to be covered by the QA Program should be identified, along with the major organizations participating in the program and the designated functions of these organizations. The written policies, procedures, or instructions that implement the QA Program should be described. If these written policies, procedures, or instructions are not yet effective, a schedule for their implementation should be provided.

3.3 Design Control

A description of the design control measures should be provided. Included should be measures to ensure that appropriate quality standards are specified in design documents and that deviations from such standards are controlled; measures for the selection and review of suitability of application of materials, parts, equipment, and processes; measures for the identification and control of design interfaces and for coordination among participating organizations; and measures for verifying or checking adequacy of design, such as by design reviews, alternate or simplified calculational methods, or suitable testing programs. The descriptions should also cover measures to ensure that design changes, including field changes, will be subject to design control measures commensurate with those applied to the original design and will be reflected in accurate "as built" drawings and specifications.

3.4 Procurement Document Control

A description of the procurement document control measures should be provided. Included should be measures to ensure that applicable regulatory requirements, design bases, and other requirements (such as QA Program requirements) which are necessary to obtain adequate quality are included or referenced in procurement documents.

3.5 Instruction, Procedures, and Drawings

Provide a description of the measures to be used to ensure that activities affecting quality will be prescribed by documented instructions, procedures, or drawings and will be accomplished in accordance with these instructions, procedures, or drawings.

3.6 Document Control

A description of document control measures should be provided. It should include measures to ensure that documents, including changes, are reviewed for adequacy, approved for release by authorized personnel, and distributed to and used at the location where the prescribed activity is performed.

3.7 Control of Purchased Material, Equipment, and Services

Provide a description of the measures for the control of purchased material, equipment, and services. Include measures for source evaluation and selection, for assessment of the adequacy by means of objective evidence of quality furnished by the contractor, for inspection at the contractor source, and for examination of products delivery.

3.8 Identification and Control of Materials, Parts, and Components

Describe the measures to be used for the identification and control of materials, parts, and components to ensure that incorrect or defective items will not be used.

3.9 Control of Special Processes

A description of the measures for the control and accomplishment of special processes should be provided. Included should be a listing of the special processes used in the construction and installation of components or systems, such as welding, casting, or nondestructive testing. Include the measures to be used to ensure that such special processes are controlled and accomplished by qualified personnel using qualified procedures.

3.10 Inspection

Describe the program for the inspection of activities affecting quality, indicating specifically the items and activities to be covered. Included should be an organizational description of the individuals or groups performing inspections, indicating the independence of the inspection group from the group performing the activity being inspected. Also indicate how the inspection program for the involved organizations is established.

3.11 Test Control

Describe the test program used to demonstrate that structures, systems and components will perform satisfactorily in service. Included should be an outline of the test program, procedures to be developed, means for

documenting and evaluating test results of the item tested, and designation of the responsibility for performing the various phases of the program. If a test program is used to verify the adequacy of a specific design feature, a description of the qualification testing of a prototype unit should be included.

3.12 Control of Measuring and Test Equipment

Describe the measures used to ensure that tools, gauges, instruments, and other measuring and testing devices are properly controlled, calibrated, and adjusted at specified periods to maintain accuracy within necessary limits. This section does not refer to devices such as metal detectors, motion sensors, alarms, and communications equipment that make up the protection system, but rather to those devices used to test or calibrate the system devices during installations and preoperational testing.

3.13 Handling, Storage, and Shipping

The applicant should describe the measures used to control handling, storage, shipping, cleaning, and preservation of items in accordance with work and inspection instructions to prevent damage or deterioration.

3.14 Inspection, Test, and Operating Status

The applicant should describe the measures used to indicate the inspection and test status of items to prevent inadvertent bypassing of such inspections and tests. A description should also be provided of the measures for indicating the operating status of the structures, systems, components, and equipment.

3.15 Corrective Action

The applicant should describe the measures established to ensure that conditions adverse to quality maintenance are identified and corrected and that the cause of significant conditions adverse to quality is determined and corrective action is taken to preclude repetition.

3.16 Quality Assurance Records

Describe the program for the maintenance of records to document activities affecting quality. Included should be means for identifying the records, the retention requirements for the records (including duration, location, and assigned responsibility), and the means for retrieving the records when needed. Physical protection quality assurance records should be maintained and stored for a minimum of two years.

3.17 Audits

The applicant should describe the system of audits used to verify compliance with all aspects of the QA Program and to determine its effectiveness. Included should be the means for documenting responsibilities and procedures for auditing, required frequency of audits, audit results, and designating management levels to which audit results are reported.

I 8

Page
Evans
See
Comments
III
Seems to me
that some addit'l control
measures are needed.

Upgrade Working Group

DISTRIBUTION:

Upgrade Working Group
O. Chambers (IE)
R. Jones (SD)
T. Michaels (SD)
R. Fonner (ELD)
Mike Smith (SG)
D. Kasun (SG)
C. South (SG)
B. Hatter (SG)
A. Poltorak (SG)
John J. Miller (NRR)
B. Nulsen (SG)

Information List
R. Page (SG) ✓
B. Erickson (SG)
J. Fowers (SG)
T. Thayer (SG)
R. Brightsen (SG)
E. Perchonok (SG)
F. Arsenault (RES)
M. Elliott (NRR)
N. Haller (IE)
T. Sherr (SG)
E. McAlpine (SG)
F. Crane (SG)
D. Sutton (SG)
D. Kunihiro (SG)
M. Levy (SG)
J. Prell (SD)
R. Ramirez (SD)