PRESSURIZED WATER REACTOR TECHNOLOGY

Metropolitan Edison Company
TMI Unit 2

Volume 4

Babcock & Wilcox

15. SAFETY ANALYSIS

CONTENTS

List of Figures

be reached by the provision of a summary written statement of the technical and operational considerations that justify the selection. The physical format for technical specifications, therefore, assumes importance in that the collection of specifications and their written bases can form a document that delineates facility features that are important to operating safety, the reasons for their importance, and their relations to one another, and provides both the AEC and licensee management personnel with understandable terms of reference with respect to safety.

Furthermore, as experience in operation and technical knowledge accrues, changes in specifications become desirable from time to time, and the written basis for a specification provides for orderly analysis and evaluation of such changes.

15.9.4. Development of Technical Specifications*

The five categories of technical specifications defined in section 50.36 of 10 CFR 50 are derived from considerations of factors that bear on the use and maintenance of physical barriers in the operation of a facility. In the following discussion, each of the categories is examined, and the development of technical specifications is outlined.

15.9.4.1. Safety Limits and Limiting Safety System Settings

Specifications of this category are intended to apply to process variables which are continually observable and measurable, e.g., pressures, temperatures, flow rates, power, and neutron flux. Such variables are directly related to the performance and integrity of fuel and coolant barriers. The safety limit is a value of the chosen variable at which one can say with confidence that no serious consequences will occur. If the value of the variable were to be at this limit, and all other variables were at the upper limit of their operating range, and if all uncertainties in technical knowledge of the process were resolved unfavorably, then no hazard to the public would exist.

---

* Only the specifications become license conditions. The bases are supporting information.

Near the safety limit and separated from it by a finite margin is a danger zone in which unacceptable consequences may occur. Somewhere in this zone is a real limit which divides values that are sure to result in such consequences for any given accident and those that will not. This limit usually cannot be precisely located because of uncertainties in the technical knowledge of the process and because it is related to the values of other variables. Therefore, the safety limit is chosen after consideration of experience, experimental results, interaction between variables, and all other pertinent plant characteristics, and is located comfortably within the bounds of knowledge. The practical result of this approach is that transgressing a safety limit by a small amount will not produce unacceptable consequences. However, this would represent a significant and undesirable departure from proper operation. To transgress a safety limit, significant equipment malfunction or failure, or one or more significant deviations from operating procedures, or both, would have to occur.

A limiting safety system setting is selected at a level on the safe side of the safety limit. The region between this setting and the safety limit should be sufficient to allow for corrective action by the safety (protection) system to return the situation to normal or to shut the reactor down before the safety limit would be reached for the most severe abnormal situation anticipated during the life of the plant. This means that circuit response times and transient characteristics, including overshoot, must be taken fully into account. Also included must be an allowance for calibration uncertainties and instrument inaccuracies. On the safe side of the limiting safety system setting lies the zone of normal operations. Allowance must be made for the possibility that the value of the variable may transgress the normal zone occasionally due to instrument drift, minor operational errors, and normal fluctuations in process or control characteristics. Therefore, a margin for these factors should be left between the normal operating zone and the safety system setting. Usually, alarms or annunciators are provided between the operating zone and the safety system action point to promote corrective action and to help prevent any significant invasion of the safety margin.

One result of proper relations of the safety system setting and the normal operating zone is that the safety system would seldom be activated.

15.9.4.2. Limiting Conditions for Operation

This category of technical specifications covers two general classes of matters (1) equipment and (2) the technical conditions and characteristics of the plant necessary for continued operation.

1. Equipment — Two classes of equipment are important to the integrity of barriers. first, those systems and components directly related to the control of variables and operating conditions (including those on which safety limits have been placed) and, second, those systems and components necessary to cope with abnormal situations. Some examples of the first class are as follows:

a. Instrument systems.
b. Control systems.
c. Hydraulic systems for pumping and control working fluids.
d. Electrical systems.
e. Waste control systems.
f. Refueling systems.

In the second class of equipment specifications are the following:

a. Emergency power systems.
b. Emergency cooling systems.
c. The containment and associated systems.
d. Safety systems.

For both classes of equipment mentioned above, it is intended that technical specifications should establish the lowest acceptable level of performance for a system or component or the minimum number of components or portion of the system that must remain operable in order that plant operation may continue.

4. Technical Conditions and Characteristics

—Technical conditions and characteristics may be stated in terms of allowable quantities, e.g., the concentration of radioactive material in certain systems, the volume of fluid required in a system, the chemical constitution of certain fluids, or the allowable configurations of equipment. To derive a limiting condition for operation, one must consider both the minimum complement of equipment necessary to maintain operation in the "normal" range, and what is necessary to accommodate abnormal situations.

The term "adequate margin" is used in a number of places in paragraph 50.36 of 10 CFR 50, this means that sufficient equipment in all systems must be operable, so that further, but limited and defined, failure of equipment, a power outage, or other transient situation, or an error in operation will not prevent safe shutdown or that the design basis accident can be accommodated while the equipment remains available.

15.4.4.1. Surveillance Requirements

It is intended that major emphasis in surveillance specifications be placed on those systems and components that are essential to safety during all modes of operation or those which are necessary to prevent or mitigate the consequences of accidents. Tests, calibrations, or inspections are necessary to verify the performance and availability of important equipment. This is particularly true of those systems that are not used for normal operation but which are necessary to cope with abnormal situations.

Surveillance requirements and limiting conditions for operation are frequently complementary. For a specific system, typically, a category 2 specification will establish the minimum performance level, and the surveillance requirement will prescribe the frequency and scope of testing to demonstrate such performance. The frequency and type of surveillance should be based, wherever possible, on quantitative data derived through experience or experiment.

When a change or modification in equipment is contemplated, it should also be examined for its effect on related equipment and procedures, and additionally for its effect on the validity of the basis for related technical specifications. In this way, we can usually determine whether the existing margin of safety is adversely affected. A revised basis should be provided, where necessary, to justify the change. In addition, a revised basis should be submitted whenever it is determined that an existing one is not valid, regardless of whether a specification change is proposed.

15.10. Reference Material

1. General Design Criteria for Nuclear Plants, USAEC, November 1965.
2. Schultz, M. A., Control of Nuclear Reactors and Power Plants, McGraw-Hill.
3. Meteorology and Atomic Energy, USAEC, TID-24190, July 1968.
4. DiNunno, J. J., et al., Calculation of Distance Factors for Power and Test Reactor Sites, USAEC DL&R, TID-14844, March 1962.
5. Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants, USAEC, WASH-740.
6. Blomeke and Todd, Uranium Fission-Product Production as a Function of Thermal Neutron Flux, Irradiation Time, and Decay Time, ORNL-2127 (Part I, Vols 1 and 2; Part II, Vols 1, 2, and 3).
7. Deposition and Washout Computations Based on the Generalized Gaussian Plume Model, ORO-699.
8. Atomic Energy Act of 1954, United States Atomic Energy Commission.
9. United States Atomic Energy Commission Regulations as follows:

   Title 10, Part 2, Rules of Practice: This part governs the conduct of all proceedings under the Atomic Energy Act of 1954.

   Title 10, Part 20, Standards for Protection Against Radiation: The regulations in this part establish standards for protection against radiation hazards arising from the activities under license.

   Title 10, Part 40, Control of Source Material: These regulations deal with the procedure and criteria for issuance of licenses to receive title to, to receive, to possess, and to transfer source material.

   Title 10, Part 50, Licensing of Production and Utilization Facilities: This regulation provides for the licensing of production and utilization facilities pursuant to the Atomic Energy Act of 1954.

5. Review and approval mechanisms for authorizing new procedures as well as changes in procedures, equipment, and process, and for determining whether such changes can be made within the existing technical specifications.

6. Periodic review and audit of operations, including the performance of both equipment and operating personnel.

7. Reports to the AEC.

15.9.5. Changes in Technical Specifications and Plant Equipment

The technical specifications discussed in this guide are incorporated in the license issued for the operation of a facility. This means that the limits and conditions set forth in the specifications become legal bounds within which the licensee is required to operate the facility. The system of specifications described above is intended to provide a reasonable degree of flexibility to licensee management for its control of operations in the interest of safety. Furthermore, in recognition of the fact that, as knowledge and experience increase, changes in specifications or equipment may become desirable or even necessary, the rules of the Commission provide for two kinds of changes

1. Changes in technical specifications or changes that involve an "unreviewed safety question" (see paragraph 50.59 of 10 CFR 50) require prior review and authorization by the Commission.

2. Certain changes in plant equipment and procedures may be made by the licensee, provided that he is able to make a suitable finding to the effect that the change does not involve an unreviewed safety question.

Throughout the operating life of a facility, as equipment and personnel performance data become available, earlier studies and data should be reconsidered regularly and updated to reflect actual experience.

When a change in a technical specification appears in order, its effect on related equipment and procedures should be analyzed and evaluated. The basis for the "old" specification provides a starting point for evaluating the change for both the licensee and the Commission.

15.9.4.4. Design Features

These technical specifications are intended to cover the design characteristics of special importance to each of the physical barriers and to the maintenance of safety margins in the design. The principal objective of this category is to control changes in design of vital equipment. The selection of specifications in this category should be predicated upon an examination of all equipment and materials associated with each barrier, including the barrier itself, with respect to the following questions:

1. Whether a change in design would affect any technical specification.
2. Whether any margin of safety associated with any technical specification would be affected.
3. Whether the equipment or its performance is covered in any other technical specification.

15.9.4.5. Administrative Controls

The safety analysis should contain a full description and discussion of organizational and administrative systems and procedures for the operation of the facility. Specifications of this category should consist of summary statements and descriptions of administrative arrangements for the following subjects:

1. Organization, showing lines of authority from top (licensee) management on through all activities, both technical and operational, with a description of the minimum qualifications established for key management and technical positions, for members of safety committees when such exist, and for positions on the operating staff. If preferred, a chart may be used for this purpose, with footnotes as required.

2. Administrative action to be taken by the licensee in the event that any requirement imposed by technical specifications is violated.

3. Provision of detailed, written procedures governing normal operation, abnormal situations, emergencies, and maintenance operations that may affect reactor safety.

4. Logs and records of operation, maintenance, changes to procedures and equipment, tests, inspections, calibrations, incidents, investigations, and reviews.