Reactor Safety Management Systems for the Savannah River Reactors

Ben C. Rusche

Abstract

Reactor safety management systems for the Savannah River heavy-water-moderated production reactors were established to ensure that public and employee health and safety were protected while meeting very demanding production objectives. Operational approaches and philosophies to achieve both safety and production objectives were developed by Du Pont based on experience at the Hanford Works and earlier experience in hazardous chemical and explosive manufacturing operations elsewhere in Du Pont Company. These systems were formally approved by the Atomic Energy Commission (AEC) as meeting the stated objectives and serving the national interest. This paper describes the evolution and function of these processes and practices and briefly chronicles the excellent performance at the Savannah River Plant (SRP).

Reactor Safety Management Systems

Origin

In the 1940s, after Enrico Fermi and his colleagues had achieved the first controlled nuclear chain reaction at the University of Chicago's Stagg Field, the promise for producing enormous amounts of energy and converting plentiful U-238 to Pu-239 was confirmed. Concurrently, the chemistry of uranium and the transuranic elements (e.g., neptunium, plutonium) were investigated by Glenn Seaborg (and others in later years) and his colleagues at the University of California. With understanding the chemical properties of these exotic elements, it became evident that the path to substantial quantities of fissionable material for power production or weapons was more practical and efficient by converting U-238 to Pu-239 in a reactor using the naturally occurring mix of uranium isotopes followed by chemical separation. The earlier processes of separating U-235 from natural uranium electro-magnetically in Calutrons (located at Oak Ridge) and later by the gaseous diffusion process (also located at Oak Ridge) continued to be used in the transition using natural uranium. Realizing the preferred course to plutonium production was through converting uranium in a nuclear reactor led to the request that the Du Pont Company undertake the task to design, engineer, and operate a major manufacturing complex at Hanford, Washington, to produce plutonium. To this task Du Pont assigned many of its best and most highly regarded engineers, physicists, chemists, and technical staff.

Those activities were important precedents to developing and implementing the system that became the pre-cursor for safety management systems for the Savannah River heavy-water-moderated reactors, which began operation in 1953. These reactors became a major source of U.S. plutonium production and the leading source of tritium for the free world. In later years, the U.K. and the Soviet Union developed substantial capabilities as well. First the Hanford and later the Savannah River reactors were designed and built by Du Pont with input and participation of some of America's most outstanding scientists and engineers.

Management Systems

Reactor safety management systems at SRP were prescribed by nuclear safety control

procedures. These documents were authorized and approved by the senior management of the Atomic Energy Division (AED) of the Du Pont Company, and constituted the exercise of Du Pont's commitment to protect public health and safety while maximizing production rates and product quality. The activity was carried out by two divisions of the AED, the Manufacturing Division and the Technical Division. Upon completion of construction by the Construction Division, the Manufacturing Division operated and maintained the facilities. The Technical Division ensured that the best available technical designs were developed and tested, and that parameters for managing and controlling the operations were consistent with the procedures.

The material requirements of the AEC changed as weapons technology and national security needs evolved. The designs of the individual reactor charges were virtually tailor-made or adapted to meet specific product requirements even though the physical features of the SRP reactor systems changed only occasionally over the years.

It is the purpose of this paper to briefly describe the reactor safety management systems that allowed the AEC's objectives to be carried out safely and efficiently.

Organizational Relationships and Detailed Descriptions

The Atomic Energy Commission (AEC), established in the 1940s as a successor to the Manhattan Project, carried out its functions through several divisions. Of particular relevance is the Production Division responsible for manufacturing nuclear weapons materials. The AEC also established an Advisory Committee on Reactor Safeguards (ACRS) to provide independent review and advice on the adequacy of AEC reactors and their operating contractors (e.g., Du Pont at Savannah River) to protect the public and employees. In August 1964, the ACRS reviewed the SRP reactor operations and raised questions on terminology and on the safety bases for operations. In response to these questions, an active dialog followed for several months.

Reactor Safety Management Systems Principles and Terminology

The following material, largely extracted and condensed from a letter from J. W. Croach of Du Pont to R. C. Blair of AEC, Savannah River, dated September 24, 1965, presents the features of the Du Pont reactor safety management systems (Croach 1965).

Introduction

We believe it is important for the ACRS and for all personnel who have an interest in reactor safety at SRP to understand our principles of management controls and to appreciate the significance of the terms we use. It is especially important for the members of the ACRS because approval for new operating modes at Savannah River is sought on the basis that we will establish limits of operation in accordance with our standard practice; approval is not sought for specific power levels or other numerical parameters of operation.

Savannah River reactors are operated under a system of management controls that are designed, above all, to ensure safety, but also to permit the achievement of high performance levels. We believe reactor safety is best ensured by the multiple defenses of a sound process, reliable facilities, and responsible operation by qualified personnel. Perfection cannot be attained in any one of these; we believe the risk of a serious accident is minimized by incorporating multiple, independent protective features in the process, in the equipment and instrumentation, and in the management of operation. Most of the system of "defense in depth" is beyond the scope of this discussion (but underlies the entire philosophy). The basic features of the management controls that govern safe operation are discussed briefly in the following section.

Objective

It is our objective to operate the reactors under conditions where: (1) the limiting hazards of operation have been identified and evaluated, (2) regions of operation with acceptable risks have been established and duly authorized, and (3) methods of operation have been agreed upon and approved in advance of operation.

Principles

There are no generally accepted methods for quantitatively weighing and specifying risks. In general, a "risk" combines the concepts of potential damage to the reactor or its components and the likelihood of such damage. Associated with damage is the risk of releasing radioactivity that could be hazardous to the public. What constitutes an acceptable risk depends on technical analysis, management experience, and judgment. It is recognized that zero risk is a desirable limiting state but can only be achieved in practice by not operating the reactors.

For a given operating mode, the condition of the reactor at any time is described by values of measured or calculated variables that characterize the performance of fuel assemblies and of the entire reactor. These variables include such quantities as temperatures, coolant flows, heat fluxes, radiation fields, and thermal and mechanical stresses on the reactor structure. Prior analysis of operating characteristics and experimental data establish the values of critical operating variables at which actual damage or other undesirable consequences would occur in the reactor. Safe operation demands that these critical variables be rigorously controlled. There are usually several potentially limiting conditions that must be guarded against in operation, and any one of these might limit operation at a given time. For instance, depending upon the cooling water temperature and the radial flux distribution, a particular fuel loading might be limited by one or the other of the following: (a) boiling instability in some subchannels of the coolant passages in fuel assemblies, (b) film boiling burnout on the most vulnerable surfaces of the fuel, or (c) boiling the moderator outside the fuel assemblies.

For a particular critical variable, the principles of safe control employed at SRP involve the following:

1. Analysis to determine what value of the variable will yield actual damage—or what range of values has a high probability of damage. (Real Limit)

2. Agreement upon the value at which the probability of damage or harmful consequence is acceptably low. (Technical Standard Limit)

3. Designation of a safety margin to be maintained between the Technical Standard Limit and the range authorized for normal operation. The margin is selected to provide an acceptably low risk that equipment failure, operating error, or process fluctuations will result in damage. (Minimum Margin; Operating Limit)

4. Methods of operating the reactor and of measuring or calculating the critical variables are agreed to in writing in advance of operation. (Standard Operating Procedures)

5. Operation is continually surveyed and audited to ensure that the operation is in accordance with the intended control methods and that risks associated with the particular critical variable do not exceed those anticipated when the methods were specified.

6. Control methods and values are modified to reflect pertinent operating experience, improved equipment and instrumentation, new technical data, or changes in operating modes.

Terminology

Important terms used in the system of management controls are discussed briefly.

Real Limit. This term is frequently used in the discussion of a potentially limiting phenom-

enon that is capable of causing damage to the reactor, such as melting fuel. When a critical variable that governs the phenomenon has a value at which actual damage is expected or is highly probable, the value may be referred to as a "real limit". Sometimes the term is used to designate a particular value of a variable where there is an abrupt transition in the nature of the associated phenomenon (such as the onset of boiling) and where large uncertainties enter into the attempt to extrapolate the subsequent course of events. In any case, the probability of associated damage is high.

Frequently, the "real limit" is more appropriately regarded as a band of unacceptably high risk of damage. The probability of damage approaches unity and the magnitude of possible damage increases as the value of the variable approaches one edge of the band, while at the other edge of the band the risk borders on the acceptable—and in fact coincides with the Technical Standard Limit which will be discussed next. It is apparent that risks—both from the point of view of consequences and probability—can rarely be assigned definite quantitative values and that the selection of a boundary between regions of acceptable and unacceptable risks must be made through analysis on the basis of judgment and experience.

Technical Standard Limit. This is a formally approved and authorized limit that is not to be exceeded. It states the value of a critical variable that separates safe operation from operation where undesirable consequences may occur. The limit is selected on the basis that, at this value and for less extreme values, the risk is acceptably low. The analysis on which the limit is based includes a conservative allowance for uncertainties in the calculations, the accuracy and applicability of the data, and, if significant, an allowance for the accuracy with which the critical variable can be measured (or calculated from measurements).

If a Technical Standard Limit is exceeded, the condition must be corrected immediately. A special investigation and the preparation of a report to management in Wilmington are required. The objective of our system of management and controls is to maintain operation within the limits set by Technical Standards.

Minimum Margin. When a Technical Standard defines a limit that is critical and potentially limits reactor power, it specifies a Minimum Margin. This is defined as the minimum separation between the Technical Standard Limit and the Operating Limit. The Operating Limit may provide for a greater margin than the Minimum Margin. The Minimum Margin is established on the basis of technical information and a conservative evaluation of the consequences of abnormal operation and/or credible accidents; the bases for selection are specified in the Technical Standard. The purpose of the Minimum Margin is to provide factors of safety that will maintain a low risk of damage if any of the abnormal operating conditions and/or credible accidents described by the Technical Standard occur.

Operating Limit. In general, the operating departments specify Operating Limits on the basis of process knowledge, operating experience, available control instrumentation, and expected modes of operation. The choice of an Operating Limit may take into account factors other than safety, such as economy and operating convenience. One important objective in the selection of an Operating Limit for a reactor variable that has safety implications is to provide an adequate margin so that process fluctuations have a vanishingly low probability of exceeding the Technical Standard Limit. When a Minimum Margin is specified by the Technical Standard, it may be judged to be an adequate safety factor, or an additional margin may be specified. The Operating Limit indicates the highest level of authorized operation.

Standard Operating Procedure. The Standard Operating Procedures are the embodiment of the principle that operation of the reactors is to be carried out by methods that have been agreed to and approved in advance. These procedures specify in detail how the reactors are to be operated, what data shall be recorded,

and what action must be taken to cope with unusual or emergency conditions. The Operating Procedures contain detailed limits and rules designed to keep the critical variables within the limits and intent of the Technical Standards and Operating Limits.

Technical Specifications. The Technical Specifications represent the instrument of administrative control of reactor operation by the AEC and, for SRP, are administered by the Savannah River Operations Office (SROO). Conformance with Technical Specifications is achieved by the requirement that Technical Standards must be equally restrictive or more restrictive than corresponding Technical Specifications. Violation of a Technical Specification requires a special investigation and the preparation of a report to management in Wilmington and a report to SROO.

For those who might desire more detail, a later version of Nuclear Safety and Control Procedures (1976) may be found in the last reference. Also, see Millison (1991), which contains a compilation of precedents to the final version of Technical Specifications utilized by Westinghouse Savannah River Company (WSRC). It is apparent that the level of detail increased and the scope broadened somewhat. Even so, the concepts and approaches for assuring the safety of the SRP reactors remained consistent with the earlier version.

Conclusion

The exceptional combination of conceptual approach in Reactor Safety Management Systems, physical design of the reactor systems, operational procedures, safety equipment, prior and concurrent technical design input, and large-scale verification (i.e., an extensive quality control and assurance activity) led to achievement of the AEC's and Du Pont's safety goals while increasing production rates (i.e., thermal power) by a factor of more than four over the operating life of the facility. For all operations at SRP through September 1998, the two highest hypothetical annual effective radiation doses to the maximally exposed individual in the public because of atmospheric releases of radionuclides from SRS were 11 mrem in 1955 and 14 mrem in 1956. All other annual radiation doses through 1998 were below 10 mrem. The current DOE (1990) and EPA (1989) annual limit is 10 mrem. This limit did not exist in 1955-56 (Carlton 1988).

For releases from SRP to drinking water sources for the entire operational period, the annual public exposure value has not exceeded 1 mrem—the maximum value was 0.8 mrem at Port Wentworth (Savannah, Georgia) in 1963. The national standard is 4 mrem adopted by DOE in 1990 and EPA in 1977. Thus, both the safety and production objectives were met (Carlton 1988).

The efficacy of the Safety Management Systems to commercial power reactor processes was recognized in the mid 1960s when a task force of experienced people from the AEC complex were formed to recommend regulatory and control processes for commercial power reactors. Marvin Mann of the AEC, a former Du Pont Savannah River Plant technical manager, formed the group which included A. A. Johnson of Du Pont, SRP; Herb Kouts of BNL and the ACRS; Joe DiNunno, AEC Division of Licensing; and a representative from Los Alamos National Laboratory. (The author served as staff to A. A. Johnson.) Out of this effort emerged the prototypical technical specification system as the licensing basis for acceptably safe operation of commercial reactors. As a final footnote, the author was appointed the first Director of Nuclear Reactor Regulation in 1975 when the Nuclear Regulatory Commission was established by Congress. The experience and relevance of the Du Pont commitment to reactor safety and the writer's personal participation in that evolution under the direction of A. A. Johnson were certainly factors in that selection.

On this note the story is closed, and the operation of reactors at Savannah River became history when the last remaining operating reactors were shut down in 1988.

References

Carlton, W. H., WSRC, *Assessment of Radionuclides in the Savannah River Site Environment – Summary Unclassified*, WSRC-TR-98-00162, September 1998.

Croach, J. W., Du Pont, to R. C. Blair, Manager SROO-AEC, *Terminology of Management Controls for Reactor Operation at SRP*, September 14, 1965.

Millson, M. G., to R. L. Salizzoni, *Technical Specification Precedents*, WSRC-TR-91-42-026, June 18, 1991.

Nuclear Safety and Control Procedures for the Savannah River Reactors, DPW-75-123, Savannah River Laboratory, May 10, 1976.

Acknowledgments

The author acknowledges with appreciation and gratitude the opportunity to know and work for and with many individuals in Du Pont. Among those that stand out in my personal experience are: A. A. Johnson, Jesse Croach, Marvin Mann, Peter Morris, C. W. J. Wende, and Gerry Merz. To them and all the others that contributed to SRS and to my personal odyssey, my thanks.

Biography

Ben Rusche joined the Du Pont Company at Savannah River Plant in 1953 with a BS in Physics from Tennessee Polytechnic University with later study in Nuclear Engineering at Georgia Institute of Technology and Stanford University. After 20 years at SRP, the Nuclear Regulatory Commission selected him as the first Director of Nuclear Reactor Regulation in 1975. He returned to Du Pont two years later as Corporate Director of Health and Safety. In 1980, he went to Washington as Special Assistant for Policy and Programs to Energy Secretary Dr. James B. Edwards. In 1984, he was appointed Director of the Office of Civilian Radioactive Waste Management (Assistant Secretary) for the Department of Energy in President Reagan's presidency. In 1988, he became Senior Vice-President in the Law Engineering Company in Atlanta. Since retirement in 1996, he consults in energy and environmental matters through his own company, Management and Technical Resources, Inc., located in Columbia, South Carolina.