U.S. NUCLEAR REGULATORY COMMISSION

Revision 1
January 1996

REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

REGULATORY GUIDE 1.152

(Draft was issued as DG-1039)

CRITERIA FOR DIGITAL COMPUTERS IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS

A. INTRODUCTION

Criterion 21, "Protection System Reliability and Testability," of Appendix A, "General Design Criteria for Nuclear Power Plants," in 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," requires, among other things, that protection systems be designed for high functional reliability commensurate with the safety functions to be performed. Criterion III, "Design Control," of Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," of 10 CFR Part 50 requires, among other things, that quality standards be specified and that design control measures be provided for verifying or checking the adequacy of design.

This regulatory guide describes a method acceptable to the NRC staff for complying with the Commission's regulations for promoting high functional reliability and design quality for the use of digital computers in safety systems of nuclear power plants. The term "computer" is a system that includes computer hardware, software, firmware, and interfaces.

The Advisory Committee on Reactor Safeguards has been consulted concerning this guide and has concurred in the regulatory position.

Any information collection activities mentioned in this regulatory guide are contained as requirements in 10 CFR Part 50, which provides the regulatory basis for this guide. The information collection requirements in 10 CFR Part 50 have been approved by the Office of Management and Budget, Approval No. 3150-0011.

B. DISCUSSION

Instrumentation and Control (I&C) systems that use digital computers in safety systems make extensive use of advanced technology, i.e., equipment and design practices that are expected to be significantly and functionally different from current designs. These designs include, but are not limited to, the use of microprocessors, digital systems and displays, fiber optics, multiplexing, and different isolation techniques to achieve the needed independence and redundancy.

IEEE Std 7-4.3.2-1993, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,"[1] was jointly prepared by the Nuclear Power Engineering Committee of the Institute of Electrical and Electronics Engineers (IEEE) and the Nuclear Power Plant Standards Committee of the American Nuclear Society (ANS). The NRC staff has worked with IEEE and ANS in developing IEEE Std 7-4.3.2-1993 to ensure that the guidance provided by the consensus standard is consistent with the Commission's regulations. IEEE Std 7-4.3.2-1993

[1]IEEE publications may be purchased from the IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854.

has evolved from ANSI/IEEE-ANS-7-4.3.2-1982, "Applications Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations." IEEE Std 7-4.3.2-1993 is a significant improvement over its 1982 version. The 1993 version was approved by the IEEE Standards Board on September 15, 1993. This standard identifies guidelines for digital computers (including hardware, software, firmware, and interfaces) to supplement IEEE Std 603-1991, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations."[1] The NRC staff recognizes that development processes for computer systems continue to evolve.

Digital I&C systems share data transmissions, functions, and process equipment to a greater degree than analog systems. Although this sharing forms the bases for many of the advantages of digital systems, it also raises a key concern with respect to its vulnerability to a different type of failure. The concern is that a design using shared data bases and process equipment has the potential to propagate a common cause failure of redundant equipment. Another concern is that software programming errors can defeat the redundancy achieved by the hardware architectural structure. Because of these concerns, the NRC staff has placed significant emphasis on defense-in-depth against propagation of common cause failures within and between functions.

The principle of defense-in-depth is to provide several levels or echelons of defense to challenges to plant safety, such that failures in equipment and human errors will not result in an undue threat to public safety. A detailed defense-in-depth study and failure mode and effect analysis or an analysis of abnormal conditions or events should be made to address common cause failures. The Commission's position for providing defense against common cause failures in digital I&C systems for future light-water reactors is given in the Staff Requirements Memorandum of July 21, 1993, on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs"[2] (specifically in point 18: II Q, "Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems").

Section 5.15, "Reliability," of IEEE Std 7-4.3.2-1993 states, "When qualitative or quantitative reliability goals are required, the proof of meeting the goals shall include software used with the hardware." The staff does not endorse the concept of quantitative reliability goals as a sole means of meeting the Commission's regulations for reliability of the digital computers used in safety systems. The NRC staff's acceptance of the reliability of the computer system is based on deterministic criteria for both the hardware and software rather than on quantitative reliability goals.

Software failures that are not the consequence of hardware failures are caused by design errors and, therefore, do not follow the random failure behavior used for hardware reliability. The NRC staff believes that quantitative reliability determination, using a combination of analysis, testing, and operating experience, provides information regarding the safety importance of the computer system and also provides an added level of confidence in its reliable performance. If quantitative software reliability goals are used, the staff believes that the amount of testing of the safety system instrumentation and control equipment will increase. The staff recognizes that the commercial dedication of "commercially" available digital systems in nuclear applications relies a great deal on quantitative methods because of the operating experience data (such as number of hours of successful operation) accumulated over the years. The staff does not intend to preclude operating experience data from the justification of a successful commercial dedication.

Section 6, "Sense and Command Features—Functional and Design Requirements," of IEEE Std 7-4.3.2-1993 indicates that no requirements beyond IEEE Std 603-1991 are necessary. IEEE Std 603-1991 specifies the need to ensure acceptable response time for the instrumentation and control system in order to accomplish necessary safety functions. Consideration of the sampling rate of plant variables is an important aspect of the design of a digital system when satisfying this criterion.

IEEE Std 7-4.3.2-1993 includes 8 annexes. This standard states that these informative annexes are not part of IEEE Std 7-4.3.2-1993. The NRC staff believes these annexes contain information that may be useful. However, the information in these annexes should not be viewed as the only possible solution or method. Since a consensus has not been reached in the nuclear industry, these annexes are not endorsed by the NRC staff.

C. REGULATORY POSITION

Conformance with the requirements of IEEE Std 7-4.3.2-1993, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," with the exception of relying solely on quantitative reliability goals (Section 5.15), is a method acceptable to the NRC staff for satisfying the Commission's regulations with respect to high functional reliability and design quality requirements for computers used as components of a safety system.

[2]Copies are available for inspection or copying for a fee from the NRC Public Document Room at 2120 L Street NW., Washington, DC; the PDR's mailing address is Mail Stop LL-6, Washington, DC 20555; telephone (202) 634-3273; fax (202) 634-3343.

Section 2 of IEEE Std 7–4.3.2–1993 references several industry codes and standards. If a referenced standard has been separately incorporated into the Commission's regulations, licensees and applicants must comply with the standard as set forth in the regulation. If the referenced standard has been endorsed by the NRC staff in a regulatory guide, the standard constitutes an acceptable method of meeting a regulatory requirement as described in the regulatory guide. If a referenced standard has been neither incorporated into the Commission's regulations nor endorsed in a regulatory guide, licensees and applicants may consider and use the information in the referenced standard if appropriately justified, consistent with current regulatory practice.

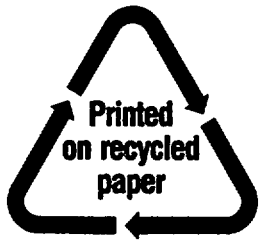
D. IMPLEMENTATION

The purpose of this section is to provide information to applicants and licensees regarding the NRC staff's plans for using this guide.

Except in those cases in which an applicant or licensee proposes an acceptable alternative method for complying with specified portions of the Commission's regulations, the methods described in this guide will be used in the evaluation of submittals in connection with applications for construction permits and operating licenses. It will also be used to evaluate submittals from operating reactor licensees that propose system modifications voluntarily initiated by the licensee if there is a clear nexus between the proposed modifications and this guidance.

VALUE/IMPACT STATEMENT

A draft Value/Impact Statement was published with the draft of this guide, Task DG–1039, when it was published for public comment in May 1995. No substantive changes were necessary, but a few editorial changes were made for clarity and consistency. A copy of the revised Value/Impact Statement for Revision 1 of Regulatory Guide 1.152 is available for inspection or copying for a fee from the NRC Public Document Room at 2120 L Street NW., Washington, DC; the PDR's mailing address is Mail Stop LL–6, Washington, DC 20555; telephone (202)634–3273; fax (202)634–3343.



Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

FIRST CLASS MAIL
POSTAGE AND FEES PAID
USNRC
PERMIT NO. G-67