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

action Boylan/Hartz
#1   #2

FEB 1 1984

MEMORANDUM FOR: Wilbur M. Morrison, Acting Chief
                    Instrumentation and Control Branch
                    Division of Facility Operations
                    Office of Nuclear Regulatory Research

FROM: Edward L. Jordan, Director
                    Division of Emergency Preparedness
                     and Engineering Response
                    Office of Inspection and Enforcement

SUBJECT: REGULATORY GUIDE IC 127-5, COMPUTER SYSTEMS IN SAFETY
                    SYSTEMS

Your memorandum of December 20, 1983, requested that staff review, prior to
issuance of the subject regulatory guide, a package which included:

   American National Standard ANSI/IEEE-ANS-7-4.3.2-1982, "Application Criteria
   for Programmable Digital Computer Systems in Safety Systems of Nuclear
   Power Generating Stations," a standard which establishes criteria for
   development of computer software, integration of software and hardware,
   and validation of the resulting computer system;

   Draft Regulatory Guide Div. 1 IC 127-5, "Criteria for Programmable Digital
   Computing Systems in Safety-Related Systems of Nuclear Power Plants,"
   a regulatory guide which would establish the standard above as an
   acceptable method for meeting NRC requirements for such systems;

   Proposed Regulatory Analysis;

   A collection of comments from the public on the draft regulatory guide;
   and

   Discussion of Public Comments on the regulatory guide.

On July 31, 1980, we recommended affirmative ballot action on the standard.
The standard was approved by the American National Standards Institute on
July 6, 1982.

According to the standard's definitions, verification is the process of
determining that the computer system meets requirements at the end of each
phase of development, and validation is the process of determining that the

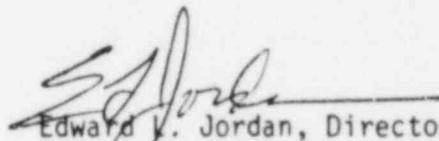CONTACT: R. W. Woodruff, IE
          49-24507

8402210057 RPP
XA

final product meets design requirements. We note, in again reviewing the standard, that it expressly permits verification (Section 4, first paragraph) of software development and validation (Section 6, last paragraph) of the computer system with software tools that have not been verified. We urge that Section C, Regulatory Position, be revised to add a requirement that validation of the computer system be performed with verified software tools.

Section 4.1 of the standard requires that the software development plan provide a method for assuring that software is auditable and testable during the design, implementation, and integration phases of computer system development. Section 6, (first paragraph) requires that the completed computer system be validated by exercising it through simulated static and dynamic input signals. We urge that Section C, Regulatory Position, be revised to add a requirement that the computer system be designed so that software is auditable and testable throughtout plant life and that the computer system be periodically revalidated during the life of the plant.

We would appreciate having your response to these recommendations.

Edward L. Jordan, Director
Division of Emergency Preparedness
and Engineering Response, IE

cc: R. C. DeYoung, IE
     J. M. Taylor, IE
     S. A. Schwartz, IE
     R. L. Baer, IE
     A. W. Dromerick, IE
     W. L. Fisher, IE
     D. C. Kirkpatrick, IE
     M. S. Wegner, IE