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

SCHWINK

MAR 0 7 1985

Attachment 2 to Enclosure 4 of the minutes of CRGR Meeting #73

MEMORANDUM FOR: Alan S. Hintze
Senior Electronics Engineer
Division of Engineering Technology, RES

FROM: Duane G. Kidd, Chief
Systems Security Branch
Division of Security, ADM

SUBJECT: DRAFT REGULATORY GUIDE "CRITERIA FOR PROGRAMMABLE DIGITAL COMPUTER SYSTEMS SOFTWARE IN SAFETY-RELATED SYSTEMS OF NUCLEAR POWER PLANTS"

Reference is made to your Routing and Transmittal Slip to the Division of Security of February 28, 1985 concerning the above Draft Regulatory Guide.

While it would be preferable if the ANSI standard itself contained more specific references to computer security it is obviously not practical to amend or recommend amendments to it. I believe, however, that the following minor modifications to the guide will highlight the need for security considerations:

Page 4, Section 1, "Background", First sentence, change to read as follows:

> "...processing variables, digital computers, while more vulnerable to unauthorized manipulation, are considered to offer...

Page 5, Section 2.1.1, "Value", First sentence, change to read as follows:

> "...methods to insure the accuracy and reliability, but not necessarily the security, of Programmable...Safety related Systems. The security aspects of such systems will be an NRC concern during the review process."

These recommendations are based on the fact that general purpose programmable computer systems are more vulnerable to manipulation and misuse, both intentional and inadvertent, than single purpose analog processors. This is especially true when the computer is configured with dial up capabilities which allow remote processor interfaces.

In any NRC review of the systems described in this draft Regulatory Guide we should ensure that the computer/communications systems are adequately protected from improper use, alteration, manipulation or other actions which could affect the operation of the plant. Where the systems have dial up communications capabilities we should take considerable precautions to ensure that they are more than just minimally protected (e.g., only a simple password system). We should be as concerned with the possibility of failure due to unauthorized system use as with "glitches" in an operating or application system.

If we can assist you on any computer/communications security matter, please contact me on x24134.

Duane G. Kidd

Duane G. Kidd, Chief
Systems Security Branch
Division of Security, ADM

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

PDR

MAR 26 1985

MEMORANDUM FOR: William J. Dircks
Executive Director for Operations

FROM: Victor Stello, Jr., Chairman
Committee to Review Generic Requirements

SUBJECT: MINUTES OF CRGR MEETING NUMBER 73

The Committee to Review Generic Requirements (CRGR) met on Tuesday, March 12, 1985 from 1-5 p.m. A list of attendees for this meeting is enclosed (Enclosure 1).

1. The CRGR was asked to consider a proposed Revision 1 to SRP 13.5.2, "Operating and Maintenance Procedures." NRR has proposed this revision to implement staff positions contained in NUREG 0737, Supplement 1, and issued in Generic Letter 82-33, "Requirements for Emergency Response Capability," (Category 2 Item). The CRGR members were given the proposed revision (Enclosure 2) at the meeting and asked to consider whether or not it would be necessary for the Committee to review this package. NRR has stated that there are no new requirements beyond the basic requirements of Generic Letter 82-33. The CRGR members were asked to respond to the CRGR Chairman regarding their views. Following receipt of the members views, the CRGR Chairman will either proceed to exempt the proposed revision from review or will schedule the proposed revision for review at a future CRGR meeting.

2. In a March 7, 1985 memorandum to CRGR members, the CRGR Chairman proposed to exempt from Committee review, an enclosed NRR proposal for modifying (relaxing) staff recommendations contained in NUREG-0803, Generic Safety Evaluation Report Regarding Integrity of BWR Scram System Piping, (Category 2 Item). The CRGR agreed to exempt the NRR proposal provided that the staff assure that the proposal concerning generic resolution of the BWR scram system piping issue is consistent with conclusions and recommendations of the NRC Piping Review Committee.

3. M. Jamgochian (RES) presented for CRGR review, a proposed modification of 10 CFR Part 50, Appendix E, "Emergency Planning and Preparedness for Production and Utilization Facilities," to eliminate emergency class entitled "Notification of Unusual Event," (Category 2 Item). Enclosure 3 summarizes the matter.

4. G. Arlotto and A. Hintze (RES) presented for CRGR review the proposed Regulatory Guide (IC-127-5), dated June 6, 1984, "Criteria for Programmable Digital Computer Systems in Safety-Related Systems of Nuclear Power Plants," (Category 2 Item). Enclosure 4 summarizes this matter.

8504100701 XA 2pp

MAR 26 1985

5. D. Ross (RES) discussed with the CRGR, his January 30, 1985 memorandum to Committee members concerning proposed Revision 2 to Regulatory Guide (RG) 1.105, "Instrument Setpoints for Safety-Related Systems," (Category 2 Item). Enclosure 5 summarizes this matter.

Enclosures 2 through 5 of this document contain predecisional information and therefore will not be released to the Public Document Room until the NRC has considered (in a public forum) or decided the matters addressed by the information.

Questions concerning these meeting minutes should be referred to Walt Schwink (492-8639).

Victor Stello, Jr., Chairman
Committee to Review Generic
Requirements

Enclosures:
As Stated

cc: Commission (5)
SECY
Office Directors
Regional Administrators
CRGR Members
G. Cunningham
G. Arlotto
A. Hintze
M. Jamgochian

PDR

Enclosure 4 to the Minutes of CRGR Meeting No. 73
CRGR Review of a Proposed Regulatory Guide Entitled "Criteria for Programmable Digital Computer Systems of Nuclear Power Plants"

G. Arlotto and A. Hintze (RES) presented for CRGR review the proposed Reg. Guide. The initial package submitted for review by the Committee was transmitted by a memorandum dated November 29, 1984, from R. B. Minogue to V. Stello, Jr.; it included the following documents:

1. Proposed Reg. Guide (IC-127-5), dated June 6, 1984, "Criteria for Programmable Digital Computer Systems in Safety-Related Systems of Nuclear Power Plants."

2. Value/Impact Statement

3. ANSI/IEEE-ANS Std. 7-4.3.2-1982, "Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations."

4. Public comments on draft Reg. Guide IC 127-5, dated March 1983.

5. NRC staff discussion of public comment on the draft Reg. Guide.

6. NRC staff comments on draft Reg. Guide IC 127-5, dated June 1984.

Subsequently, the following additional documents were provided to the Committee in connection with the review of this matter:

1. Revised Page 2 to the proposed Reg. Guide, transmitted by note dated February 22, 1985, A. Hintze to W. Schwink (Attachment 1 to this Enclosure).

2. Comments by the Division of Security, ADM, on the proposed Reg. Guide, transmitted by memorandum dated March 7, 1985, D. Kidd to A. Hintze (Attachment 2 to this Enclosure).

CRGR review of this proposed Reg. Guide was initially scheduled for January 23, 1985 but was postponed at the request of RES and subsequently rescheduled for consideration by the Committee on March 12, 1985.

The proposed Reg. Guide was proposed at the request of NRR to provide guidance regarding the use of programmable digital computer systems in safety-related systems of nuclear power plants. It endorses an industry standard, ANSI/IEEE-ANS 7-4.3.2-1982, "Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations." This guidance will improve safety by better assuring, through a verification and validation process specified in the proposed guidance, that programming errors potentially adverse to safety will be detected and eliminated during the design phase. It is expected that identification of such errors in the design phase will result in significant cost savings as well as safety benefit (although no specific cost analysis or savings estimates were provided by RES in the review package). RES noted that the current version of the proposed Reg. Guide is in essence a clean endorsement of the industry standard (ANSI/IEEE-ANS 7-4.3.2) and is forward fit only (i.e., applicable only to CP applications docketed after issuance of the Reg. Guide).

The following major points were raised during the discussion of the proposed Reg. Guide at this meeting:

1. The Committee expressed the view that the state-of-the-art of computer design and application has advanced to the point that the use of computers to assist plant operators in monitoring complex nuclear power plant systems and reacting to unexpected changes in plant conditions could be expected to be safety beneficial. CRGR recommended, therefore, that the Reg. Guide be strengthened by adding explicit wording to encourage (not require) the use of computers in nuclear power plants. RES agreed to develop appropriate wording for inclusion in the INTRODUCTION section of the Reg. Guide.

2. With regard to the scope of implementation of the proposed Reg. Guide, the Committee asked what staff practice would be concerning the review of operating reactor licensee proposed amendments for the use of computers in safety-related systems, and review of proposed amendments to new plant applications which propose use(s) of computers in safety-related systems where such use was not included previously in the design of those facilities. Specifically, since the staff is proposing that the Reg. Guide be implemented in a forward fit fashion only, the Committee wondered what software qualification methods or criteria would be applied by the staff in these backfit type contexts. The staff indicated that alternative methods (e.g., "mapping techniques," "sneak circuit" analysis, use of compilers for "self-checking," diverse software, etc.) could be used; but the verification and validation methods specified in ANSI/IEEE-ANS 7-4.3.2 and endorsed by the proposed Reg. Guide are the most efficient and are preferred by the staff in the backfit contexts of concern to the CRGR as well as the forward fit applications already covered by the proposed Reg. Guide. The Committee recommended, therefore, that the IMPLEMENTATION section of the proposed Reg. Guide be revised to indicate applicability in these backfit contexts, in addition to the forward fit applicability proposed. RES agreed to revise the wording accordingly.

3. There was much discussion of the caveat in the REGULATORY POSITIONS section of the proposed Reg. Guide stating that NRC endorsement of ANSI/IEEE-ANS 7-4.3.2 does not include endorsement of other standards referenced therein (specifically IEEE-Std 603 and ANSI/ASME NQA-1). CRGR

expressed the view that exclusion of the referenced standards without identifying explicitly alternative guidance that is acceptable to the staff could create doubt or confusion about what is expected by NRC in the areas addressed by the referenced standards. The staff responded that such caveat is necessary, because the staff review of the referenced standards is not completed so they have not been endorsed. Failure to include the caveat, therefore, could easily be misconstrued to indicate that the staff has endorsed them. As a more general comment, it was noted that, from past experience, such caveats have also been found necessary to avoid the "cascade" problem (e.g., if staff endorsement of ANSI/IEEE-ANS 7-4.3.2 implied endorsement of other standards referenced therein, would it also imply endorsement of yet other standards referenced in the referenced standards, etc, etc). The :taff also commented that, at least in this case, licensees and applicants should be expected to know the "alternative guidance" acceptable to the staff, because it is embodied in the regulations themselves. specifically, IEEE-279 applies in place of IEEE-603, and 10 CFR 50 Appendix B applies in place of NQA-1, because safety-related things are involved.

As a result of these discussions, it was agreed that the caveat in question is appropriate for inclusion in the Reg. Guide as proposed; but, RES agreed also to specify explicitly that IEEE-279 and 10 CFR 50, Appendix B, are applicable in place of the standards excluded from NRC endorsement by the caveat.

4. The Committee noted that the proposed Reg. Guide endorses an industry standard that appears to specify a very substantial amount of record-keeping. The Reg. Guide also contains a statement (in the INTRODUCTION section) that any guidance therein relating to information collection has been cleared under an OMB clearance. No evaluation of the costs involved was provided by RES in the CRGR review package; however, RES acknowledged the omission, and stated that an OMB clearance package will be prepared which includes estimates of projected costs. RES will coordinate with the ROGR staff on this action, so there will be opportunity for further review of this aspect of Reg. Guide impact if that is felt necessary.

5. The CRGR commented that it should be made clearer that the proposed Reg. Guide is applicable only to computers used in safety-related systems/functions in the <u>operation</u> of nuclear power plants, <u>not</u> to those used in the <u>design</u> of the plants. RES agreed to clarify the intent of the proposed Reg. Guide in this respect.

6. The CRGR recommended, and RES agreed, that the comments by the Division of Security, ADM (see Attachment 2 to this Enclosure), which were solicited and received late in the review process, should be incorporated into the proposed Reg. Guide.

In conclusion, on the basis of discussions at this meetinc the Committee recommended that the proposed Reg. Guide be issued, subject to completion of the changes/actions noted in the preceding. RES will coordinate with the ROGR staff in completing the changes/actions agreed upon.

Attachment 1 to Enclosure #4 of the minutes
of CRGR meeting # 73

ROUTING AND TRANSMITTAL SLIP

Date 2/22/85

TO: (Name, office symbol, room number, building, Agency/Post)	Initials	Date
1. Walter S. Schwink		
2. ✓cc: James H. Conran		
3.		
4.		
5.		

	Action		File		Note and Return
	Approval		For Clearance		Per Conversation
	As Requested		For Correction		Prepare Reply
	Circulate		For Your Information		See Me
	Comment		Investigate		Signature
	Coordination		Justify		

REMARKS

Regarding the transmittal of R. Minogue to V. Stello, dated November 29, 1984, enclosed are fifteen copies of revised Page 2 of Proposed Regulatory Guide (IC 127-5), "Criteria for Programmable Digital Computer Systems Software in Safety-Related Systems of Nuclear Power Plants," which was part of that transmittal. A bar in the margin indicates what has been changed.

DO NOT use this form as a RECORD of approvals, concurrences, disposals, clearances, and similar actions

FROM: (Name, org. symbol, Agency/Post) Alan S. Hintze, EEICB/DET	Room No.—Bldg. Phone No. 37860

testing, overall performance assurance, and documentation of software for programmable digital computer systems in safety-related systems of nuclear power *plants.* ~~generating stations.~~ Because of the unique nature of programmable digital computer systems, especially with respect to software, the standard was intended to supplement IEEE Std 603-1980, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations,"* which establishes the functional and design criteria for the power, control, and instrumentation portion of safety *related* systems for nuclear power *plants* ~~generating stations~~. This joint standard (designated in draft form as IEEE P 742/ANS 4.3.2) was approved by the IEEE Nuclear Power Engineering Committee and the ANS Nuclear Power Plant Standards Committee and has been published as ANSI/IEEE-ANS-7-4.3.2-1982, "Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations."**

It is noted that the standard does not address any follow-on activities (such as testing and validation of computer systems) beyond the design, implementation and integration phases. As with any other safety system, there is legitimate concern that measures be provided to ensure that computer systems will continue to perfrom as designed throughout the life of the plant. Assurance of continued performance is normally accomplished for other safety-related systems by periodic testing. The requirements for periodic testing of hardware and software (revalidation) are contained in the technical specifications. Additional guidance on periodic testing has been provided in Regulatory Guide 1.118.

C. REGULATORY POSITION

The requirements set forth in ANSI/IEEE-ANS-7-4.3.2-1982 establish a method acceptable to the NRC staff for designing software, *verifying software,* implementing software, and validating computer systems used in safety*-related* systems of nuclear *power plants* ~~generating stations~~, ~~subject to the following:~~ *This endorsement does not include other*

*Copies are available from the Institute of Electrical and Electronics Engineers, 345 East 47th Street, New York, N.Y. 10017.

**Copies are available from the American Nuclear Society, 555 North Kensington Avenue, La Grange Park, Ill. 60525, and the Institute of Electrical and Electronics Engineers, 345 East 47th Street, New York, N.Y. 10017.