REAFFIRMED
August 16, 1990
ANSI/IEEE/ANS-7.4.3.2-1982
(R1990)

teria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations

WITHDRAWN
1993
ANSI/IEEE/
ANS-7.4.3.2-1982
(R2990) (W1993)

No longer being maintained as an American National Standard. This standard may contain outdated material or may have been superseded by another standard. Please contact the ANS Standards Administrator for details.

an American National Standard

CO-SPONSORED BY

The American Nuclear Society
555 North Kensington Avenue
La Grange Park, Illinois
60525

AND

The Institute of Electrical and Electronics Engineers, Inc.
345 East 47th Street
New York, N.Y. 10017

ANSI/IEEE-ANS-7-4.3.2-1982

American National Standard
Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations

Co-Sponsors
American Nuclear Society and
Institute of Electrical and Electronics Engineers, Inc.

Prepared by the
American Nuclear Society Standards Committee and the
Nuclear Power Engineering Committee of the
IEEE Power Engineering Society
Joint Working Group ANS-4.3.2/IEEE SC-6.4

Published by the
American Nuclear Society
555 North Kensington Avenue
La Grange Park, Illinois 60525 USA

Also available from:
The Institute of Electrical and Electronics Engineers, Inc.
345 East 47th Street
New York, New York 10017

Approved July 6, 1982
by the
American National Standards Institute, Inc.

American National Standard

An American National Standard implies a consensus of those substantially concerned with its scope and provisions. An American National Standard is intended as a guide to aid the manufacturer, the consumer, and the general public. The existence of An American National Standard does not in any respect preclude anyone, whether he has approved the standard or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standard. American National Standards are subject to periodic review and users are cautioned to obtain the latest editions.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken to reaffirm, revise, or withdraw this standard no later than five years from the date of publication. Purchasers of this standard may receive current information, including interpretation, on all standards published by the American Nuclear Society by calling or writing to the Society.

Printed by

American Nuclear Society
555 North Kensington Avenue, La Grange Park, Illinois 60525 USA

Price: $7.50

Copyright © 1982 by American Nuclear Society.

Any part of this standard may be quoted. Credit lines should read "Extracted from American National Standard, ANSI/IEEE-ANS-7-4.3.2-1982 with permission of the publisher, the American Nuclear Society." Reproduction prohibited under copyright convention unless written permission is granted by the American Nuclear Society.

Printed in the United States of America

Foreword

(This Foreword is not a part of American National Standard Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations, ANSI/IEEE-ANS-7-4.3.2-1982.)

This standard establishes application criteria for programmable digital computer systems in safety systems of nuclear power generating stations. These criteria are established to provide a means for promoting safe practices for design and evaluation of safety system performance and reliability. However, adhering to these will not necessarily fully establish the adequacy of any safety system's functional performance and reliability; nonetheless, omission of any of these criteria will, in most instances, be an indication of safety system inadequacy. This standard does not provide specific requirements for preparation or content of software quality assurance plans.

IEEE Std 603-1980, Standard Criteria for Safety Systems for Nuclear Power Generating Stations (Revision of IEEE Std 603-1977) establishes the functional and design criteria for the power, control, and instrumentation portion of safety systems for nuclear power generating stations. P742/ANS-4.3.2, now known as American National Standard Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations, ANSI/IEEE-ANS-7-4.3.2-1982, applies to all digital computer systems used in safety systems (for example, multiprocessor distributed systems as well as larger scale single central processor systems). It has been developed to amplify IEEE Std 603-1980 because of the unique nature of digital computer systems — specifically the software. As such, ANSI/IEEE-ANS-7-4.3.2-1982 establishes no additional functional criteria, or design basis requirements. These criteria are covered adequately by American National Standard Design Basis Criteria for Safety Systems in Nuclear Power Generating Stations, ANSI/ANS-4.1-1978, and IEEE Std 603-1980.

In reviewing areas of application criteria that need amplification when digital computers are utilized in safety systems, the following conclusions were reached:

(1) The criteria established in IEEE Std 603-1980 and supporting standards require no additional amplification for digital computer hardware.

(2) Because of inherent differences between hardware and software, IEEE Std 603-1980 does require amplification with regard to the method of designing and qualifying the software.

(3) Because of the high degree of interdependency between the hardware and software, the integration of these components is unique to digital systems, and in this area IEEE Std 603-1980 requires amplification.

Development of this standard began in 1974 under sponsorship of the American Nuclear Society. In 1978, a joint working group was formed that combined members of ANS and the Institute of Electrical and Electronics Engineers, Inc. (IEEE) with a charter to develop a joint standard.

During the development of ANSI/IEEE-ANS-7-4.3.2-1982, the joint working group was greatly concerned with the level of detail and specific requirements that should be included in this standard. It was decided that the standard should not dictate how the system should be implemented since this would force system development in a rigid direction. Recognizing the dynamic nature of digital systems technology, the standard was structured to provide guidance in the application of future digital system technology to safety systems. This standard is not intended to be a detailed design procedure for computer systems engineers in applying digital computers to safety systems nor is it intended to dictate when a digital computer system is re-

quired as part of a safety system. The intent has been generally to amplify IEEE Std 603-1980 and not to restrict unduly the designers or engineers in implementation of digital systems, and also to permit the future application of new digital system technology.

Figure i of the foreword shows the development of the programmable digital computer system in relation to the development of the total safety system.

Figure 1 of the standard illustrates the inter-relationships among the various processes in the application of programmable digital computer systems in safety systems for nuclear power generating stations.

In the development of ANSI/IEEE-ANS-7-4.3.2-1982, the working group specified that verification and validation were essential processes in the development of computer systems utilized in safety systems. Verification and validation are extensions of the concept of testing software to determine that it will perform the correct functions.

Verification is the comparison of the stage-by-stage software development to determine that there is a faithful translation of one stage (such as the design) into the next stage (such as the implementation).

Verification is accomplished in the present state of the art through a communication of concepts, and an understanding of functions, between knowledgeable persons that draw from previous experience and supplementary information. If the translation of one stage to another can be understood by knowledgeable persons, other than the originator, and it is determined that a faithful and accurate translation has been performed, then that stage to stage verification can be considered satisfied. Discrepancies must be documented, and a decision must be made as to what previous stage or stages must be modified (or what action must be taken) to resolve any problems.

Validation assumes that the "Safety System Requirements for Programmable Digital Computer System" is the defining document and provides a comparison with the functions implemented by the computer program in the computer hardware. This validation process provides an overall assurance that the functions specified are implemented in the hardware-software. It also provides assurance that the overall accumulation of the undesired stage to stage side effects have been corrected.

The working group discussed independent verification in detail. Independence is needed:

(1) To meet the quality assurance provisions of Title 10, "Energy," Code of Federal Regulations, Part 50, "Licensing of Production and Utilization Facilities," Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," Section III, "Design Control," which should be extended to software, as follows:

> "The verifying or checking process shall be performed by individuals or groups other than those who performed the original design, but who may be from the same organization."

(2) Because analytic proof of correctness of a complex program is currently impossible, and

(3) To provide an in-depth second analysis of the software requirements and of the tests to confirm that they are met, including abnormal test cases.

One of the greatest advantages of digital computer systems is the flexibility offered by the software system. However, this flexibility has been a liability in balloting this standard. Due to differences in individual perception, one reviewer would classify the standard as "too general," whereas another reviewer would call the same document "too specific." Some reviewers have suggested that the standard should include more specific hardware requirements, including seismic requirements for the digital computer system, bypasses, access to setpoints, manual initiation, capability for test and calibration, etc. These areas have been reviewed by the joint working group during the development of the standard. The consensus of the group was that detailed hardware considerations as well as functional and design criteria for the safety system are fully covered by IEEE Std 603-1980 and other supporting industry standards; e.g., the following American National Standards: Design Basis Criteria for Safety Systems in Nuclear Power Generating Stations, ANSI/ANS-4.1-1978; Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants, N18.2-1973 (ANS-51.1); and Nuclear Safety Criteria for the Design of Stationary Boiling Water Reactor Plants, ANSI/ANS-52.1-1978.

The joint working group considers the process of software development to be analogous to that of hardware development. Consequently, the well-established principles and practices of engineering a hardware based system apply similarly to a software-based system.

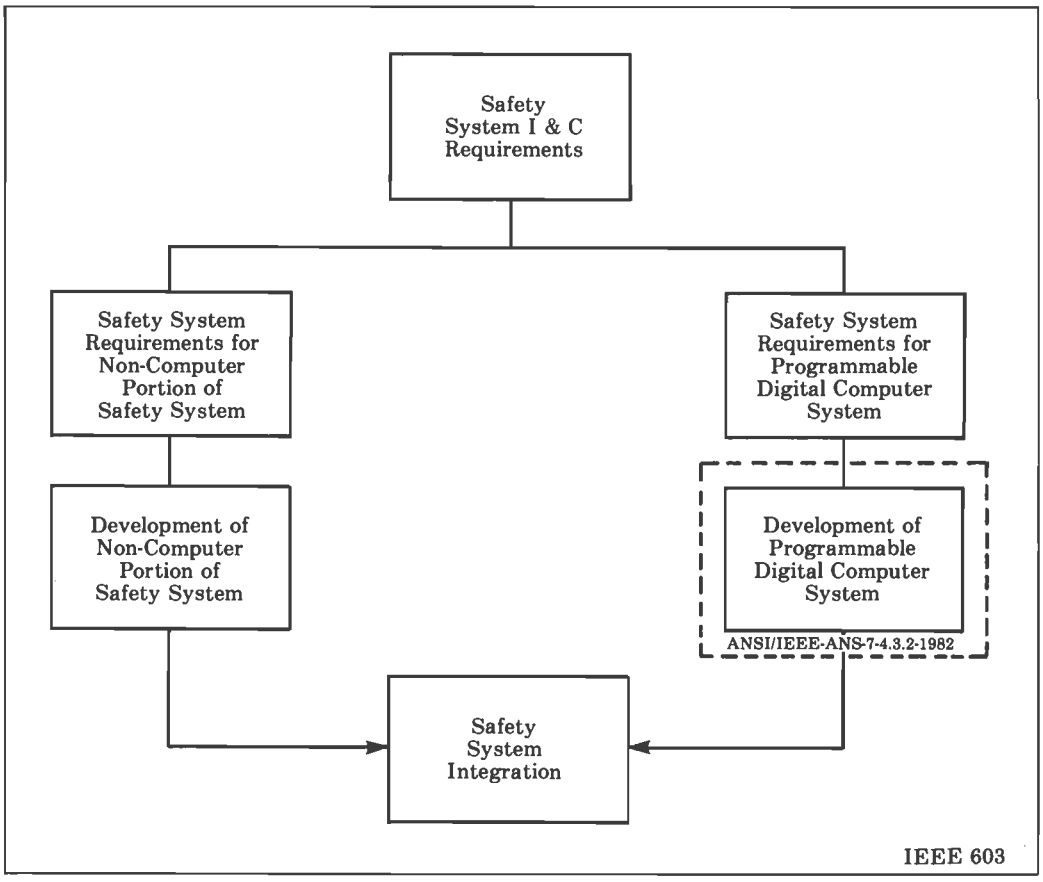

Fig. i
Development of Digital Computer System in Relation to Other I&C Portions of The Safety System

Much discussion during the development of this standard has centered around the capability for self-checking by digital systems and the extent to which this standard should require self-checking. The self-checking features of programmable digital computer systems may constitute a valid basis for their application in safety systems. However, extensive self-checking is not a requirement of safety systems design and this additional requirement should not be imposed on programmable digital computer systems applied in safety systems. Therefore, the joint working group has not specifically required self-checking features in this standard.

For the present, ANSI/IEEE-ANS-7-4.3.2-1982 will provide a basis for the current application of digital computers in safety systems. It is recognized that further effort will be required with increasing industry experience in the application of programmable digital computers to safety systems and the advancements in digital systems technology. Areas for future work are:

(1) Quantitative software standards
(2) Computer security
(3) Self testing
(4) Distributed computer systems
(5) Techniques for independent verification
(6) Firmware
(7) "Simplification" objectives.

Members of the combined Working Group IEEE SC-6.4/ANS-4.3.2 that participated in the development of this standard were:

E. M. Brown, Co-Chairman, *Combustion Engineering, Inc.*
J. E. Thomas, Co-Chairman, *Duke Power Company*
E. J. Bateman, *Babcock & Wilcox Company*
L. Beltracchi, *U.S. Nuclear Regulatory Commission*
J. B. Bullock, *Oak Ridge National Laboratory*
W. A. Coley, *Duke Power Company*
B. M. Cook, *Westinghouse Electric Corporation*
H. Hecht, *SoHar*
M. Kayton, *Systems Group of TRW, Inc.*
B. J. Lamb, *Tennessee Valley Authority*
B. A. Mutafelija, *Electronic Associates, Inc.*
H. L. Reeves, *Babcock & Wilcox Company*
I. L. Shaw, *Westinghouse Electric Corporation*
E. A. Straker, *Science Applications, Inc.*
J. P. Whooley, *Public Service Electric & Gas Company*

Subcommittee SC-6, Safety-Related Systems, of the Institute of Electrical and Electronics Engineers, Inc., had the following membership at the time of its approval of this standard:

T. M. Bates, Jr., Chairman

W. W. Bowers	R. S. Darke	P. M. Holzman	R. L. Thornton
E. M. Brown	E. F. Dowling	A. Laird	C. S. Walker
R. C. Carruth	P. M. Duggan	W. F. Schmauss	R. G. Walker
B. M. Cook	N. C. Farr	L. Stanley	G. O. Wilkinson
R. L. Copyak	B. P. Grimm	J. E. Thomas	

The Institute of Electrical and Electronics Engineers, Inc. Nuclear Power Engineering Committee (NPEC) had the following membership at the time of its approval of this standard:

R. E. Allen, Chairman — B. M. Rice, Vice Chairman

J. F. Bates	R. P. Daigle	A. Laird	W. S. Rautio
T. M. Bates, Jr.	A. C. D'Hoostelaere	L. C. Madison	H. V. Redgate
J. T. Bauer	J. J. Ferencsik	W. C. McKay	W. F. Sailer
F. D. Baxter	E. P. Fogarty	S. H. Moss	A. J. Spurgin
R. G. Benham	J. M. Gallagher	W. E. O'Neal	L. Stanley
J. T. Boettger	J. B. Gardner	R. W. Pack	H. K. Stolt
D. F. Brosnan	L. Hanes	M. Pai	D. F. Sullivan
D. G. Cain	R. I. Hayford	E. S. Patterson	P. Szabados
F. W. Chandler	I. M. Jacobs	J. R. Penland	L. D. Test
C. M. Chiappetta	R. F. Karlicek	N. S. Porter	F. J. Volpe
E. A. Corte	E. A. Kollitides		

Subcommittee ANS-4, Reactor Dynamics and System Criteria, of the American Nuclear Society Standards Committee had the following membership at the time of its approval of this standard:

E. R. Wiot, Chairman, *NUS Corporation*
P. H. Barton, *Duke Power Company*
B. J. Buescher, *Babcock and Wilcox Company*
T. R. England, *Los Alamos Scientific Laboratory*
R. L. Ferguson, *U.S. Nuclear Regulatory Commission*
J. M. Geets, *Westinghouse Electric Corporation*
C. W. Griffin, *Rockwell International*
L. K. Holland, *General Electric Company*
R. J. Klotz, *Combustion Engineering, Inc.*
R. O. Meyer, *U.S. Nuclear Regulatory Commission*
A. F. McFarlane, *Westinghouse Electric Corporation*
G. A. Randall, *Gibbs and Hill, Inc.*
H. L. Reeves, *Babcock and Wilcox Company*
V. E. Schrock, *University of California*
S. E. Turner, *NUS Corporation*

The American Nuclear Society's Nuclear Power Plant Standards Committee (NUPPSCO) had the following membership at the time of its approval of this standard.

J. F. Mallay, Chairman
M. D. Weber, Secretary

Name of Representative	*Organization Represented*
G. A. Arlotto	*U.S. Nuclear Regulatory Commission*
R. G. Benham	*General Atomic Company*
	(for the Institute of Electrical and Electronics Engineers, Inc.)
R. E. Allen (Alt.)	*United Engineers & Constructors, Inc.*
	(for the Institute of Electrical and Electronics Engineers, Inc.)
R. V. Bettinger	*Pacific Gas and Electric Company*
P. Bradbury	*Westinghouse Advanced Reactor Division*
D. A. Campbell	*Westinghouse Electric Corporation*
C. O. Coffer	*Kaiser Engineers*
L. J. Cooper	*Nebraska Public Power District*
W. H. D'Ardenne	*General Electric Company*
C. J. Gill	*Bechtel Power Corporation*
J. E. Smith	*Duke Power Company*
A. R. Kasper	*Combustion Engineering, Inc.*
R. W. Keaten	*GPU Services Corporation*
J. W. Lentsch	*Portland General Electric Company*
J. F. Mallay	*Babcock & Wilcox Company*
	(for the American Nuclear Society)
A. T. Molin	*United Engineers and Constructors, Inc.*
J. H. Noble	*Chas. T. Main, Inc.*
E. P. O'Donnell	*Ebasco Services, Inc.*
	(for the Atomic Industrial Forum)
T. J. Pashos	*Quadrex/Nuclear Services Corporation*
P. T. Reichert	*Catalytic, Inc.*
M. E. Remley	*Rockwell International*
J. Stacey	*Yankee Atomic Electric Company*
S. L. Stamm	*Stone & Webster Engineering Corporation*
L. J. Stanek	*Babcock & Wilcox Company*
J. D. Stevenson	*Structural Mechanics Associates*
	(for the American Society of Civil Engineers)
G. P. Wagner	*Commonwealth Edison Company*
G. L. Wessman	*Torrey Pines Technology*
J. E. Windhorst	*Southern Company Services, Inc.*
	(for the American Society of Mechanical Engineers)
E. R. Wiot	*NUS Corporation*

Contents

Section — Page

1. Scope . . . 1

2. Definitions . . . 1

3. Computer System Requirements . . . 1
   - 3.1 Hardware Requirements . . . 3
   - 3.2 Software Requirements . . . 3
   - 3.3 Hardware - Software Integration Requirements . . . 3

4. Software Development . . . 4
   - 4.1 Development Plan . . . 4
   - 4.2 Design . . . 4
   - 4.3 Implementation . . . 4

5. Hardware - Software Integration . . . 4

6. Computer System Validation . . . 4

7. Verification . . . 5
   - 7.1 Organization . . . 5
   - 7.2 Review and Audit Procedures . . . 5
   - 7.3 Software Test and Analysis . . . 5

Figure 1 Illustration of Processes Required by ANSI/IEEE-ANS-7-4.3.2-1982 . . . 2