

IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations

Sponsor

**Nuclear Power Engineering Committee
of the
IEEE Power Engineering Society**

Approved September 15, 1993

IEEE Standards Board

Abstract: Additional computer specific requirements to supplement the criteria and requirements of IEEE Std 603-1991 are specified. Within the context of this standard, the term *computer* is a system that includes computer hardware, software, firmware, and interfaces. The criteria contained herein, in conjunction with criteria in IEEE Std 603-1991, establish minimum functional and design requirements for computers used as components of a safety system.

Keywords: commercial grade item, diversity, safety systems, software tools

The Institute of Electrical and Electronics Engineers, Inc.
345 East 47th Street, New York, NY 10017-2394, USA

Copyright © 1994 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 1994. Printed in the United States of America.

ISBN 1-55937-370-9

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

IEEE Standards documents are developed within the Technical Committees of the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Board. Members of the committees serve voluntarily and without compensation. They are not necessarily members of the Institute. The standards developed within IEEE represent a consensus of the broad expertise on the subject within the Institute as well as those activities outside of IEEE that have expressed an interest in participating in the development of the standard.

Use of an IEEE Standard is wholly voluntary. The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of all concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason IEEE and the members of its technical committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration.

Comments on standards and requests for interpretations should be addressed to:

Secretary, IEEE Standards Board
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
USA

IEEE standards documents may involve the use of patented technology. Their approval by the Institute of Electrical and Electronics Engineers, Inc. does not mean that using such technology for the purpose of conforming to such standards is authorized by the patent owner. It is the obligation of the user of such technology to obtain all necessary permissions.

Introduction

(This introduction is not part of IEEE Std 7-4.3.2-1993, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.)

This standard specifies additional computer specific requirements (incorporating hardware, software, firmware, and interfaces) to supplement the criteria and requirements of IEEE Std 603-1991.* This standard should be used in conjunction with IEEE Std 603-1991 to assure the completeness of the safety system design when a computer is to be used as a component of the safety system.

The computer-specific requirements presented in this standard apply only to computers that are a component of a safety system, but do not necessarily apply to all computers required for complete plant operation. In this standard, subclauses 5.5 and 5.6 require that the computer that is a component of the safety system be protected from failures in nonsafety computers. There are no specific safety requirements placed on nonsafety computers. However, many of the principles have applicability to other important plant systems. These principles are consistent with the principles defined in IEEE Std 603-1991.

This standard specifies computer design requirements for the safety system level applications. Annexes have been included to provide detailed information on design techniques and methodologies for meeting various criteria and requirements. This standard recognizes that development processes for computer systems continue to evolve. As such, the information presented should not be viewed as the only possible solutions. This is in keeping with the desire to use advances in digital technology, so long as the criteria and requirements of IEEE Std 603-1991 and this standard are met. For example, while this standard does not address specifically artificial intelligence systems or fourth generation languages, their use is not precluded.

Please note that this standard is *not* applicable to engineering software used in the safety system design process. ASME NQA-2a-1990, Part 2.7 (referred to as Part 2.7) should be referenced for this type of software.

Evolution

This standard evolved from ANSI/IEEE-ANS-7-4.3.2-1982, Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations. It represents a continued effort by a joint IEEE/ANS working group to support the specification, design, and implementation of computers in safety systems of nuclear power generating stations.

ANSI/IEEE-ANS-7-4.3.2-1982 provides a detailed discussion for the development process, integrating separate software and hardware development paths into an integrated product. Inherent to this discussion are activities now detailed in Part 2.7. Reference is made to Part 2.7 to address specific software development requirements. The quality requirements are applied to the development of software for the purpose of developing reliable, high-quality software and to minimize design errors.

It should be clearly stated that this standard does not provide requirements associated with the operation and maintenance of the computer following installation (i.e., surveillance testing frequency). Any problems identified should be addressed through the appropriate requirements of ASME NQA-1-1989 and ASME NQA-2a-1990 Part 2.7, for hardware and software, respectively.

Relationship to other standards

IEEE and other consensus standards were used in the development of this standard. These are referenced throughout the standard and in the supporting annexes. As with IEEE Std 603-1991, ANSI/ANS 51.1-1983, and ANSI/ANS 52.1-1983, provide functional and design criteria for safety systems.

*Information on references can be found in clause 2.

As stated above, Part 2.7, with the exception of sections 7 and 10.2, has been invoked to address certain aspects of the quality criterion. The basis for this is as follows:

- a) Sections 3 and 4 of Part 2.7 clearly state that Verification and Validation (V&V) is performed throughout software development. Section 7 presents the requirements for the performance of verification reviews during software development. This could be interpreted as an additional requirement above those stated in sections 3 and 4. The working group therefore concluded that it could be interpreted that V&V, as stated in sections 3 and 4, is not sufficient to comply with the ASME NQA-1-1989 requirement for design verification. During the ballot of Part 2.7, IEEE NPEC noted a concern regarding the fact that V&V was discussed in multiple sections, and recommended that the requirements for V&V be consolidated.
- b) In discussions for commercial grade dedication, the working group considered the process defined in section 10.2 of Part 2.7 to address commercial grade dedication of software. ASME NQA is presently revising this section of Part 2.7 because it could be misapplied by the applicant. As such, the working group felt it inappropriate to endorse that section.

The working group, as a result of a NUPPSO negative ballot, recognized that section 4 of Part 2.7 utilizes the term *ensure*. This term is not found elsewhere in ASME NQA-1-1989, nor is it used in Appendix B of 10CFR50. Appendix B of 10CFR50 uses the phrase *adequate confidence*. For the purposes of the endorsement of Part 2.7, the phrase *adequate confidence* should be viewed as replacement for the term *ensure*.

Unintended functions

Section 4 of Part 2.7, utilizes the phrase *unintended functions*. Possible interpretations of this phrase include:

- a) *Unused resident functions*. The design process should address any unused resident functions (see 5.6 for guidance). In some cases, such as for operating systems and compilers, the V&V process is unsuitable for addressing unused resident functions as the total number may be unknown.
- b) *Unpredictable responses to external or internal conditions*. A documented effort to identify unpredictable responses to external or internal conditions should be made during the design process, and appropriate actions should be taken to resolve them. The V&V process should then confirm proper response to these conditions.
- c) *Defects due to design or implementation errors*. The V&V process is required to address defects due to design or implementation errors.
- d) *Development aids not removed from the software*. A documented decision should be made to state whether development aids will remain in the software. If the decision is made to leave the development aids in the software, they could be left active or made inactive. In either case, if development aids are to remain in the software, V&V is required.

Common cause failure/diversity

Section 5.1 in IEEE Std 603-1991 defines the single failure criterion. Guidance for the application of this criterion is provided in IEEE Std 379-1988, Standard Application of the Single Failure Criterion to Nuclear Power Generating Station Class 1E Systems. Section 5.5 of IEEE Std 379-1988 provides requirements for consideration of common cause failures in a single failure analysis. It states that common cause failures not subject to single failure analysis include those that can result from “design deficiencies, manufacturing errors.” Design qualification and quality assurance programs are intended to afford protection from “design deficiencies and manufacturing errors.” This approach is also appropriate for potential common cause failures associated with computer hardware and software that have been developed under the requirements of IEEE Std 603-1991 and this standard.

Throughout the development of this standard, the working group spent significant time discussing the need for diversity to address potential common cause failures. The working group believes that there are instances

where diversity is appropriate. A situation where all of the command features for a safety function are to be implemented using similar architecture would be one instance where diversity should be considered to provide assurance against common cause failures. This is predicated upon the foreword from IEEE Std 379-1988, which states “Other provisions may be utilized if it is determined that certain consequences may be unacceptable when the challenge rate and the common cause failure rate are considered together. In these cases, design techniques such as diversity are used to develop an acceptable design.” Annex B provides additional guidance for determination of the need for design diversity.

Electromagnetic environment

This standard requires that the range of transient and steady state conditions shall include, as a supplement to the examples of section 4.7 of IEEE Std 603-1991, the electromagnetic environment (including electrostatic discharge). During the ballot of this standard, it was noted that this is a safety system issue and not one unique to computers. It was recommended, therefore, that the subject be deleted from this standard and included in a revision to IEEE Std 603-1991. The Chair of SC6 has agreed that the issue should be considered in conjunction with the next revision of IEEE Std 603-1991. However, the working group and the SC6 Chair agree that it is an important enough issue to be maintained in this standard, at least until it is addressed in IEEE Std 603-1991.

Commercial grade item dedication

During the ballot of this standard, concerns arose as to the necessity of requirements for commercial grade item dedication. As a result of reviewing ASME NQA-1c-1993, Appendix 7A-2, the working group determined that testing alone was insufficient to determine acceptability of the item for use in a safety system. As such, consideration of the software development method(s) has been included as an integral part of the commercial grade item dedication process. Resolution of the concerns for commercial grade item dedication led to the inclusion of requirements for a manufacturer’s qualification of an existing product. Both of these requirements provide a consistent basis for the use of computers developed outside of the requirements of this standard to be evaluated for use in a safety system.

Future work

Following the approval of the next revision to Part 2.7, the working group should consider the appropriateness of the present stated exceptions to Part 2.7. This should be with the intent to endorse Part 2.7 in its entirety.

During the development of this standard, the working group struggled with numerous human factor issues. With the issuance of IEEE Std 603-1991 this concern was highlighted. IEEE Std 603-1991 requires consideration of human factors with the safety system criteria. Discussions were held with members of SC-7 to determine what actions should be taken by the working group. SC-7 is presently involved in a reaffirmation effort and the development of a standard addressing CRTs. During the ballot of this standard, concerns were again raised regarding the issue of human factors. These ballots have been forwarded to SC-7 as input to their current work.

The working group recommends the addition of requirements grading or classification to IEEE Std 603-1991. This concept was endorsed by the Nuclear Regulatory Commission staff in SECY-91-192, Digital Computer Systems for Advanced Light Water Reactors. A similar concept of safety classification is presented in ANSI/ANS 51.1-1983 and ANSI/ANS 52.1-1983. If guidance is provided in a revision to IEEE Std 603-1991, efforts should then be undertaken to apply this concept in a revision to this standard.

Questions and concerns were also raised during the balloting of this standard regarding the concern of software common cause failures. While annex B presents some considerations for the need for diversity to address common cause failures, it does not address the extent to which diversity should be considered. The

working group and some of the balloters believe that the need for diversity is a safety-system-level issue. As such, the working group recommends that this issue be considered for a revision to IEEE Std 603-1991.

This standard does not address justification for the selection of software tools and acceptance criteria for compilers, operating systems, and libraries. The working group felt this subject was outside of its scope of responsibility. As such, the working group recommends that consensus standards be developed to address these needs.

During the ballot of this standard, concerns were raised regarding the adequacy of standards for proper grounding techniques. The working group felt that it was beyond the scope of this standard to attempt to address this concern. Therefore, the recommendation is made for the development of a consensus standard to address this issue.

During the ballot of this standard, a need was identified to differentiate between the requirements for safety software and nonsafety software executed at run time on the same computer. The concept of software barriers is introduced in 5.6 and in annex G as a means of segregating these two types of software. To the knowledge of the working group there are no industry standards that adequately address this issue. The working group recommends that standards to address this topic be considered for future development efforts.

Members of the Working Group that participated in the development of this standard were:

J. Matras, IEEE Chair

L. Beltracchi
M. Coffing
L. Erin
N. Farr

R. Blauw, ANS Chair

M. Hecht
K. Holmstrom
K. Korsah

S. Koch
R. Reeves
R. Stevens
J. Stewart

At the time that this standard was prepared, Subcommittee 6 under the Nuclear Power Engineering Committee had the following membership:

W. Bowers, Chair

W. Boyer
G. Chisholm
B. Cook
R. Copyak
J. Disosway
G. Doman
E. Dowling

P. Duggan
M. Entenberg
N. Farr
B. Grim
W. Groszko
D. Horvath

P. Kelly
J. Matras
W. Messer
D. Sokolsky
J. Thomas
F. Volpe
M. Zar

At the time that this standard was prepared, MC-1 under the Nuclear Power Plant Standards Committee had the following membership:

J. T. Luke, Chair

J. C. Dempsey, Jr.
L. A. Ettlinger
J. C. Glynn
P. H. Hepner
R. A. Hill

L. A. Klosowski
G. B. Locklear
S. A. Nass
J. L. Saldarini
H. C. Shaffer

S. A. Shuman
M. D. Smith
R. C. Surman
E. W. Swanson
G. A. Zimmerman

At the time this standard was approved, the Nuclear Power Plant Standards Committee had the following membership:

W. H. D'Ardenne, Chair

J. A. Nevshemal, Vice Chair

M. D. Weber, Secretary

R. E. Allen
P. Ballinger
S. Bhattacharya
F. Boorboor
J. C. Bradford
T. W. Burnett
J. D. Cohen
J. B. Cotton
T. A. Daniels

L. E. Davis
S. B. Gerges
D. J. Gillispie
G. L. Gyorey
P. H. Hepner
C. E. Johnson
J. T. Luke
J. F. Mallay
R. E. Miller

T. T. Robin
J. C. Saldarini
R. E. Scott
D. J. Spellman
S. L. Stamm
J. D. Stevenson
G. P. Wagner
N. Weber
R. Weir

The following persons were on the balloting committee:

S. Aggarwal
R. Allen
V. Bacanskas
J. Bauer
F. Baxter
W. Bowers
D. Brosnan
N. Burstein
A. Candris
S. Carfagno
R. Carruth
R. Copyak
G. Doman
E. Dowling
A. Ducharme
R. Dulski

J. Forster
J. Gallagher
W. Gangloff
L. Gausa, Sr.
L. Gonzalez
L. Gradin
B. Grim
R. Hall
G. Henry
J. Hutson
S. Kasturi
J. Keiper
J. Lamont
A. Marion
R. E. Miller

R. B. Miller
B. Nemroff
M. Pai
J. Penland
C. Petrizzo
N. S. Porter
E. Rhoads
A. Roby
N. Smith
D. Spellman
P. Stevens
P. Szabados
J. Thomas
J. Ullo
F. Volpe
M. Zar

When the IEEE Standards Board approved this standard on Sept. 15, 1993, it had the following membership:

Wallace S. Read, Chair

Donald C. Loughry, Vice Chair

Andrew G. Salem, Secretary

Gilles A. Baril
José A. Berrios de la Paz
Clyde R. Camp
Donald C. Fleckenstein
Jay Forster*
David F. Franklin
Ramiro Garcia
Donald N. Heirman

Jim Isaak
Ben C. Johnson
Walter J. Karplus
Lorraine C. Kevra
E. G. "Al" Kiener
Ivor N. Knight
Joseph L. Koepfinger*
D. N. "Jim" Logothetis

Don T. Michael*
Marco W. Migliaro
L. John Rankine
Arthur K. Reilly
Ronald H. Reimer
Gary S. Robinson
Leonard L. Tripp
Donald W. Zipse

*Member Emeritus

Also included are the following nonvoting IEEE Standards Board liaisons:

Satish K. Aggarwal
James Beall
Richard B. Engelman
David E. Soffrin
Stanley I. Warshaw

Rachel A. Meisel
IEEE Standards Project Editor

Contents

CLAUSE	PAGE
1. Scope.....	1
2. References.....	1
3. Definitions and abbreviations	2
3.1 Definitions.....	2
3.2 Abbreviations.....	2
4. Safety system design basis.....	3
5. Safety system criteria.....	3
5.1 Single-failure	3
5.2 Completion of protective action	3
5.3 Quality	3
5.4 Equipment qualification	5
5.5 System integrity.....	5
5.6 Independence.....	6
5.7 Capability for test and calibration	6
5.8 Information displays.....	6
5.9 Control of access	6
5.10 Repair	7
5.11 Identification.....	7
5.12 Auxiliary features	7
5.13 Multi-unit stations	7
5.14 Human factor considerations.....	7
5.15 Reliability	7
6. Sense and command features—Functional and design requirements.....	7
7. Execute features—Functional and design requirements.....	7
8. Power source requirements	7
ANNEXES	
Annex A Relationship of this standard to IEEE Std 603-1991	8
Annex B Diversity needs determination	10
Annex C Electromagnetic compatibility.....	11
Annex D Qualification of existing commercial computers.....	14
Annex E Verification and validation	17
Annex F Identification and resolution of abnormal conditions and events.....	26
Annex G Communication independence.....	32
Annex H Computer reliability	35

IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations

1. Scope

The use of computers as part of safety systems elicits additional requirements not specifically addressed in IEEE Std 603-1991. This standard serves to amplify criteria in IEEE Std 603-1991 for computers used as components of safety systems in nuclear power generating stations. Within the context of this standard, the term *computer* is a system that includes computer hardware, software, firmware, and interfaces. The criteria contained herein, in conjunction with criteria in IEEE Std 603-1991, establish minimum functional and design requirements for computers used as components of a safety system.

2. References

ANSI/ANS 51.1-1983 (R1988), Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants.¹

ANSI/ANS 52.1-1983 (R1988), Nuclear Safety Criteria for the Design of Stationary Boiling Water Reactor Plants.

ASME NQA-1-1989, Quality Assurance Program Requirements for Nuclear Facilities.²

ASME NQA-2a-1990 Part 2.7, Quality Assurance Requirements of Computer Software for Nuclear Facility Applications.

IEC Std Pub 880, 1986, Software for Computers in the Safety Systems of Nuclear Power Stations.³

IEEE Std 603-1991, Standard Criteria for Safety Systems for Nuclear Power Generating Stations (ANSI).⁴

IEEE Std 610.12-1990, IEEE Standard Glossary of Software Engineering Terminology (ANSI).

IEEE Std 730-1989, IEEE Standard for Software Quality Assurance Plans (ANSI).

IEEE Std 828-1990, IEEE Standard for Software Configuration Management Plans (ANSI).

IEEE Std 1012-1986, IEEE Standard for Software Verification and Validation Plans (ANSI).

Title 10 of the Code of Federal Regulations (10CFR), Part 100, Reactor Site Criteria.⁵

¹ANSI publications are available from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA.

²ASME publications are available from the American Society of Mechanical Engineers, 22 Law Drive, Fairfield, NJ 07007, USA.

³IEC publications are available from IEC Sales Department, Case Postale 131, 3 rue de Varembe, CH-1211, Genève 20, Switzerland/Suisse. IEC publications are also available in the United States from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA.

⁴IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA.

⁵US Regulatory Guides are available from the Superintendent of Documents, US Government Printing Office, P.O. Box 37082, Washington, DC 20013-7082, USA.

3. Definitions and abbreviations

3.1 Definitions

3.1.1 commercial grade item:⁶ An item satisfying a), b), and c) below:

- a) Not subject to design or specification requirements that are unique to nuclear facilities
- b) Used in applications other than nuclear facilities
- c) Ordered from the manufacturer/supplier on the basis of specifications set forth in the manufacturer's published product description (for example, catalog)

3.1.2 commercial grade dedication: A process of evaluating (which includes testing) and accepting commercial grade items to obtain adequate confidence of their suitability for safety application.

3.1.3 firmware: The combination of software and data that reside on read-only memory.

3.1.4 safety systems: Those systems that are relied upon to remain functional during and following design basis events to ensure a) the integrity of the reactor coolant pressure boundary, b) the capability to shut down the reactor and maintain it in a safe shutdown condition, or c) the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures comparable to the 10CFR Part 100 guidelines.

NOTE—In this standard, safety systems are equivalent to the definition of safety related systems as defined in ANSI/ANS 51.1-1983 and ANSI/ANS 52.1-1983.

3.1.5 software tools: A computer program used in the development, testing, analysis, or maintenance of a program or its documentation. Examples include comparator, cross reference generator, decompiler, driver, editor, flowcharter, monitor, test case generator, and timing analyzer.

NOTE—In this standard, software tools includes compilers.

3.1.6 system testing: Testing conducted on a complete, integrated system to evaluate the system's compliance with its specified requirements.

3.1.7 verification and validation (V&V): The process of determining whether the requirements for a system or component are complete and correct, the products of each development phase fulfill the requirements or conditions imposed by the previous phase, and the final system or component complies with specified requirements.

3.2 Abbreviations

The following abbreviations appear within this standard:

ACE	Abnormal Conditions and Events
FAT	Factory Acceptance Testing
FTA	Fault Tree Analysis
FMEA	Failure Modes and Effects Analysis
NQA	Nuclear Quality Assurance
SDD	Software Design Description

⁶This definition was taken directly from ASME NQA-1-1989.

4. Safety system design basis

NOTE—See annex A for more information about the relationship of this standard to IEEE Std 603-1991.

The safety system design basis shall be consistent with the requirements state in ANSI/ANS 51.1-1983, ANSI/ANS 52.1-9183, and IEEE Std 603-1991. In addition, the following requirement is necessary to meet the safety system design basis for computers.

In addition to the examples of section 4.7 of IEEE Std 603-1991, the range of transient and steady state conditions shall include the electromagnetic environment, including electrostatic discharge (see annex C).

5. Safety system criteria

Below are the safety system criteria in the order they are listed in IEEE Std 603-1991. For some criteria there are no additional requirements beyond what is stated in IEEE Std 603-1991. For other criteria additional requirements are described below.

5.1 Single-failure

No requirements beyond IEEE Std 603-1991 are necessary (see also annex B).

5.2 Completion of protective action

No requirements beyond IEEE Std 603-1991 are necessary.

5.3 Quality

Hardware quality is addressed in IEEE Std 603-1991 and ASME NQA-1-1989. Computer development activities shall include the development of computer hardware and software. The integration of the computer software and hardware and the integration of the computer with the safety system shall be addressed in the development process.

NOTE—A typical development process is depicted in figure E1 in annex E.

In addition to the requirements of IEEE Std 603-1991, the following requirements are necessary in order to meet the quality criterion.

- a) Software development
- b) Qualification of existing commercial computers
- c) Software tools
- d) Verification and validation
- e) Configuration management

5.3.1 Software development

Computer software shall be developed, modified, or accepted in accordance with an approved Software QA Plan consistent with the requirements of ASME NQA-2a-1990 Part 2.7 with the exception of section 7⁷ and section 10.2.⁸ The Software QA Plan shall address all software that is resident on the computer at run time

⁷Section 7 presents the requirements for the performance of verification reviews during software development. This could be interpreted as an additional requirement above those stated in sections 3 and 4 of ASME NQA-2a-1990 Part 2.7.

⁸Section 10.2 addresses commercial grade dedication of software, and is currently under revision by ASME NQA. This section is being revised because it was felt that it could be misapplied by the user.

(i.e., application software, network software, interfaces, operating systems, and diagnostics). Guidance for developing Software QA Plans can be found in IEEE Std 730-1989 and IEC Std Pub 880, 1986.

5.3.2 Qualification of existing commercial computers

NOTE—See annex D for more information about qualification of existing commercial computers.

While this standard presents the general requirements for the development of computers, it is recognized that situations may exist where there is a need to qualify existing commercial computers for use in safety system applications. In such situations there are two methods of qualification.

- a) *Third-party qualification of a commercial grade item.* Guidance can be found in ASME NQA-1c-1993, Appendix 7A-2.
- b) *Qualification by a computer manufacturer who developed computers that are not under the requirements of this standard.*

The following fundamental requirements are the same for these two methods of qualification. The qualification process for the computer shall entail identification of functional and performance requirements necessary to provide adequate confidence that the safety function can be achieved. The qualification process shall apply to the computer hardware, software, or firmware that is required to execute to support accomplishing the safety function. In addition, the qualification process for software and firmware shall, whenever practicable, include the evaluation of the design process.

The qualification process shall be accomplished by comparing the hardware and software design to the design criteria of this standard. Exceptions to the development steps required by this standard or referenced documents may be taken as long as there are other compensating factors that serve to provide equivalent results. Select V&V activities may be necessary to provide adequate confidence that the item will meet functional and performance requirements.

Acceptance shall be based upon an engineering judgment that the available evidence provides adequate confidence that the existing commercial computer, including hardware, software, firmware, and interfaces, can perform its intended functions. The acceptance and its basis shall be documented and maintained with the qualification documentation. Required documentation and software resident on the computer at run time shall be placed under configuration management.

Design changes to the computer hardware, software, or firmware made following completion of the initial qualification shall be controlled in accordance with the requirements of this standard. Alternately a requalification, as per this subclause, shall be performed.

5.3.3 Software tools

Software tools shall be identified within the software development process. V&V tasks of witnessing, reviewing, and testing are not required for software tools, provided the software that is produced using the tools is subject to V&V activities that will detect flaws introduced by the tools. Software tools shall be identified and controlled under configuration management.

5.3.4 Verification and validation (V&V)

NOTE—See annex E for more information about verification and validation.

V&V, including regression testing, shall be performed in the development and modification of software. This shall be done in accordance with ASME NQA-2a-1990 Part 2.7, sections 3 and 4. Hardware verification shall be performed in accordance with ASME NQA-1-1989. V&V shall provide adequate confidence that the safety system requirements and requirements defined at each stage of development, including

handling of credible abnormal conditions, have been implemented. V&V shall address computer software and hardware, noncomputer hardware, and the integration of these items. V&V shall also include system testing of the final integrated hardware, software, firmware, and interfaces.

A V&V plan shall be prepared to confirm the correctness and completeness of the design. The V&V plan shall specify activities and tests that shall be inspected, witnessed, performed, or reviewed by competent individual(s) or group(s) other than those who developed the original design. The V&V plan shall be reviewed by competent individual(s) or group(s) other than those who developed the plan.⁹ Guidance for the development of V&V plans is available in IEEE Std 1012-1986 and IEC Std Pub 880, 1986. Within IEEE Std 1012-1986, the term *critical* is considered equivalent to the term *safety* as defined in IEEE Std 603-1991.

5.3.5 Software configuration management

Software configuration management shall be performed in accordance with ASME NQA-2a-1990 Part 2.7, section 5. Guidance for the development of software configuration management plans can be found in IEEE Std 828-1990.

Hardware configuration management shall be performed in accordance with ASME NQA-1-1989, Supplement 3S-1, section 5.

5.4 Equipment qualification

In addition to the requirements of IEEE Std 603-1991, the following requirement is necessary in order to meet the equipment qualification criterion.

Equipment qualification testing shall be performed with the computer functioning with software and diagnostics that are representative of those used in actual operation. All portions of the computer necessary to accomplish the safety function, or those portions whose operation or failure could impair the safety function, shall be exercised during testing. This includes, as appropriate, exercising and monitoring the memory, the CPU, inputs and outputs, display functions, diagnostics, associated components, communication paths, and interfaces. Testing shall demonstrate that the design basis performance requirements have been met.

5.5 System integrity

In addition to the requirements of IEEE Std 603-1991, the following requirements are necessary in order to meet the system integrity criterion.

- a) Design for computer integrity
- b) Design for test and calibration

5.5.1 Design for computer integrity

In addition to design basis conditions identified in IEEE Std 603-1991, the computer shall be designed to perform its safety function when subjected to all conditions, external or internal, that have significant potential for defeating the safety function¹⁰ [e.g., input and output processing failures, precision or roundoff problems, improper recovery actions, electrical input voltage and frequency fluctuations, maximum credible number of coincident signal changes, electromagnetic interference (EMI),¹¹ and others].

⁹See NQA-1-1989 Basic Requirements 5 and 6.

¹⁰See annex F.

¹¹See annex C.

If the design basis identifies a safety system preferred failure mode, failures of the computer shall not preclude the safety system from being placed in that mode. Performance of the computer restart operations shall not result in the safety system being inhibited from performing its function.

5.5.2 Design for test and calibration

The test and calibration function shall not adversely affect the ability of the computer to perform its safety function. Appropriate bypass of one redundant channel is not considered an adverse effect in this context. It shall be verified that the test and calibration function does not affect any computer function not included in a calibration change (e.g., setpoint change).

V&V, configuration management, and QA shall be required for test and calibration functions on separate computers (e.g., test and calibration computer) that provide the sole verification of test and calibration data. V&V, configuration management, and QA shall be required when the test and calibration function is inherent to the computer that is part of the safety system.

V&V, configuration management, and QA are not required when the test and calibration function, resident on a separate computer, does not provide the sole verification of test and calibration data for the computer that is part of the safety system.

5.6 Independence

NOTE—See annex G for more information on the independence criterion.

In addition to the requirements of IEEE Std 603-1991, the following requirement is necessary in order to meet the independence criterion.

Data communication between safety channels or between safety and nonsafety systems shall not inhibit the performance of the safety function.

Safety and nonsafety portions of computer software or firmware may be difficult to separate. The following two approaches are acceptable to address this issue.

- a) *Identify barrier requirements to provide adequate confidence that the nonsafety portions cannot interfere with performance of the safety portion of the software or firmware.* The barriers shall be designed in accordance with the requirements of 5.3 and 5.5 of this standard. The nonsafety software is not required to meet these requirements.
- b) *Develop the nonsafety portions to the requirements of 5.3 and 5.5 of this standard.*

5.7 Capability for test and calibration

No requirements beyond IEEE Std 603-1991 are necessary.

5.8 Information displays

No requirements beyond IEEE Std 603-1991 are necessary.

5.9 Control of access

No requirements beyond IEEE Std 603-1991 are necessary.

5.10 Repair

No requirements beyond IEEE Std 603-1991 are necessary.

5.11 Identification

No requirements beyond IEEE Std 603-1991 are necessary.

5.12 Auxiliary features

No requirements beyond IEEE Std 603-1991 are necessary.

5.13 Multi-unit stations

No requirements beyond IEEE Std 603-1991 are necessary.

5.14 Human factor considerations

No requirements beyond IEEE Std 603-1991 are necessary.

5.15 Reliability

NOTE—See annex H for more information about the reliability criterion.

In addition to the requirements of IEEE Std 603-1991, the following requirement is necessary in order to meet the reliability criterion.

When qualitative or quantitative reliability goals are required, the proof of meeting the goals shall include software used with the hardware. The method for determining reliability may include combinations of analysis, field experience, or testing. Software error recording and trending may be used in combination with analysis, field experience, or testing.

6. Sense and command features—Functional and design requirements

No requirements beyond IEEE Std 603-1991 are necessary.

7. Execute features—Functional and design requirements

No requirements beyond IEEE Std 603-1991 are necessary.

8. Power source requirements

No requirements beyond IEEE Std 603-1991 are necessary.