



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

## IEEE Power & Energy Society

Sponsored by the  
Nuclear Power Engineering Committee

IEEE  
3 Park Avenue  
New York, NY 10016-5997, USA

2 August 2010



**IEEE Std 7-4.3.2™-2010**  
Revision of  
IEEE Std 7-4.3.2-2003)



**This is a Redline Document produced by Techstreet, a business of Thomson Reuters.**

This document is intended to provide users with an indication of changes from one edition to the next. It includes a full-text version of the new document, plus an indication of changes from the previous version.

Redlines are designed to save time and improve efficiencies by using the latest software technology to find and highlight document changes. More professionals are using valuable new technologies like redlines, to help improve outcomes in a fastpaced global business world.

Because it may not be technically possible to capture all changes accurately, it is recommended that users consult previous editions as appropriate. In all cases, only the current base version of this publication is to be considered the official document.

## Redline Processing Notes:

1. ~~Red Text~~ - Red strikethrough text denotes deletions.
2. Blue Text - Blue underlined text denotes modifications and additions.

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

Sponsor

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

Approved 17 June 2010

**IEEE-SA Standards Board**

**Abstract:** Additional computer specific requirements to supplement the criteria and requirements of IEEE Std 603™-2009 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 603-2009, establish minimum functional and design requirements for computers used as components of a safety system.

**Keywords:** commercial grade item, diversity, safety systems, software, software tools, software verification and validation

---

The Institute of Electrical and Electronics Engineers, Inc.  
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2010 by the Institute of Electrical and Electronics Engineers, Inc.  
All rights reserved. Published 2 August 2010. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by the Institute of Electrical and Electronics Engineers, Incorporated.

**PDF:** ISBN 978-0-7381-6316-1      STD96076  
**Print:** ISBN 978-0-7381-6317-8      STDPD96076

*IEEE prohibits discrimination, harassment and bullying. For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>. 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 IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied “**AS IS.**”

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, or every ten years for stabilization. When a document is more than five years old and has not been reaffirmed, or more than ten years old and has not been stabilized, 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.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon his or her independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

**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 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 societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration. A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal interpretation of the IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE.

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. Recommendations to change the status of a stabilized standard should include a rationale as to why a revision or withdrawal is required. Comments and recommendations on standards, and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board  
445 Hoes Lane  
Piscataway, NJ 08854  
USA

Authorization to photocopy portions of any individual standard for internal or personal use is granted by The Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

## Introduction

This introduction is not part of IEEE Std 7-4.3.2-2010, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.

This standard evolved from IEEE Std 7-4.3.2-2003. It represents a continued effort by an IEEE working group to support the specification, design, and implementation of 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 603-2009. This standard should be used in conjunction with IEEE Std 603-2009 for completeness of the safety system design when a computer is to be used as a component of a safety system.

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 solution. This is in keeping with the desire to use advances in digital technology, provided the criteria and requirements of IEEE Std 603-2009 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.

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 applicable standards that specifically address these requirements.

Subclause 5.1 in IEEE Std 603-2009 defines the single-failure criterion. Guidance for the application of this criterion is provided in IEEE Std 379™-2000 [B16]. The approach stated in Subclause 5.5 of IEEE Std 379-2000 is also appropriate for potential common-cause failures associated with computer hardware and software that have been developed under the requirements of IEEE Std 603-2009 and this standard. Additional guidance for determining the need for design diversity in safety-related computer systems is provided in 5.16 of this standard.

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 the scope of this revision.

In summary, the following major changes were implemented in this version of IEEE Std 7-4.3.2:

- The references were updated to include current IEEE standards.
- Subclause 5.6 is significantly enhanced to specify acceptable communication independence between safety divisions and between safety and non-safety systems. This also involved revising Annex E to be more specific on acceptable communication methods.
- The Nuclear Regulatory Commission (NRC) established seven task working groups (TWGs) to address seven specific areas of digital I&C where the industry requested more specific regulatory guidance. Utilities, Nuclear Steam Supply System (NSSS) vendors, Electric Power Research Institute (EPRI), Nuclear Energy Institute (NEI) and other industry representatives interfaced directly with the NRC in discussing six out of the seven specific areas. The NRC subsequently issued interim staff guidance (ISG) in these seven specific areas. Three of these impact this standard in four different areas of the standard:
  - Address the issue of computer security (see NRC Interim Staff Guidance DI&C-ISG-01 [B28] for more information regarding computer security for safety systems). Subclause 5.9 provides the requirements for computer security for safety systems.

- Define the requirements for common cause failure as it relates to computer in safety systems (see NRC Interim Staff Guidance DI&C-ISG-02 [B29] for more information). Added 5.16 Common Cause Failure criteria that augments IEEE Std 603-2009, 5.16. The contents of Annex B are removed because the information is now normative in 5.16.
- Address the issue of multidivisional control and display stations (see NRC Interim Staff Guidance DI&C-ISG-04 [B30] for more information). Expanded 5.8 Information Displays, to define these requirements.
- Address the issue of function prioritization (see NRC Interim Staff Guidance DI&C-ISG-04 [B30] for more information). A new subclause, 5.5.4 Prioritization of functions, was added to define these requirements.
- A new subclause, 5.17 Use of commercial digital equipment, was added to the standard to provide clarity on the unique requirements for commercial grade dedication of computer equipment and software. This subclause was reviewed for consistency with industry guidance. Annex C was revised to provide specific information for commercial dedication of computer systems in the United States.
- Removed Annex F because various NRC and industry efforts are underway to determine the methodologies for establishing computer reliability. The material in this annex therefore may become obsolete in its current form. This annex will be revised in a future edition of this standard.
- Implemented editorial and clarification changes throughout the standard.

## Notice to users

## Laws and regulations

Users of these documents should consult all applicable laws and regulations. Compliance with the provisions of this standard does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

## Copyrights

This document is copyrighted by the IEEE. It is made available for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making this document available for use and adoption by public authorities and private users, the IEEE does not waive any rights in copyright to this document.

## Updating of IEEE documents

Users of IEEE standards should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the

document together with any amendments, corrigenda, or errata then in effect. In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE Standards Association web site at <http://ieeexplore.ieee.org/xpl/standards.jsp>, or contact the IEEE at the address listed previously.

For more information about the IEEE Standards Association or the IEEE standards development process, visit the IEEE-SA web site at <http://standards.ieee.org>.

## Errata

Errata, if any, for this and all other standards can be accessed at the following URL: <http://standards.ieee.org/reading/ieee/updates/errata/index.html>. Users are encouraged to check this URL for errata periodically.

## Interpretations

Current interpretations can be accessed at the following URL: <http://standards.ieee.org/reading/ieee/interp/index.html>.

## Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

## Participants

This document was prepared by the Application of Programmable Digital Computers to Safety Systems Subcommittee Working Group 6.4 of the IEEE Nuclear Power Engineering Committee. At the time this standard was submitted to the IEEE-SA Standards Board for approval, the Subcommittee Working Group 6.4 had the following membership:

**Warren Odess-Gillett**, *Chair, Secretary*

David Curbo  
Ronald Greenthaler

David Herrell  
Ronald Jarrett  
Paul Loeser

Mark Santschi  
Mark Stofko

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

**David J. Zaprazny**, *Chair*

**Mark Santschi**, *Secretary*

Ijaz Ahmad  
David Curbo  
Patrick Gove  
Ronald Greenthaler  
Daryl Harmon

David Herrell  
Greg Hostetter  
Ronald Jarrett  
Paul Loeser  
Barry Marcus  
Warren Odess-Gillett

Ifti Rana  
Mark Stofko  
David Theriault  
Michael Waterman  
Paul Yanosy

The Nuclear Power Engineering Committee (NPEC) that recommended approval of this standard had the following membership:

**John D. MacDonald**, *Chair*

**Satish Aggarwal**, *Vice Chair*

**George Ballassi**, *Secretary*

Ijaz Ahmad  
George Attarian  
Farouk D. Baxter  
Mark D. Bowman  
Daniel F. Brosnan  
Nissen M. Burstein  
Robert C. Carruth  
John P. Carter  
Dennis Dellinger  
John Disosway  
Stephen Fleger

Robert J. Fletcher  
Robert B. Fuld  
James F. Gleason  
Dale T. Goodney  
Daryl Harmon  
Dirk C. Hopp  
David A. Horvath  
Paul R. Johnson  
Thomas Koshy  
Harvey C. Leake  
J. Scott Malcolm

Alexander Marion  
Michael H. Miller  
James Parelo  
Mansoor H. Sanwarwalla  
Glen E. Schinzel  
James E. Stoner, Jr.  
Marek Tengler  
James E. Thomas  
Paul Yanosy  
David J. Zaprazny

The following members of the individual balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

William J. Ackerman  
Satish K. Aggarwal  
Stan Arnot  
George Ballassi  
Royce Beacom  
Robert Beavers  
William Bloethe  
Wesley Bowers  
Thomas Brewington  
Daniel F. Brosnan  
Nissen M. Burstein  
Robert C. Carruth  
Suresh Channarasappa  
Tom Crawford  
Paul Croll  
David Curbo  
Alireza Daneshpooy  
Dennis Dellinger

Gary Engmann  
Stephen Fleger  
James Gleason  
Ron Greenthaler  
Randall Groves  
Daryl Harmon  
Hamidreza Heidarisafo  
David Herrell  
Werner Hoelzl  
David Horvath  
Greg Hostetter  
Peter Hung  
Ronald Jarrett  
Paul Johnson  
James Jones  
Tanuj Khandelwal  
Chad Kiger  
Joseph L. Koepfinger

G. Lang  
Jang-Soo Lee  
William Lumpkins  
G. Luri  
Faramarz Maghsoodlou  
Michael S. Newman  
Warren Odess-Gillett  
James Parello  
Ted Riccio  
Bartien Sayogo  
Glen Schinzel  
Gil Shultz  
James Smith  
Gary Stodter  
S. Thamilarasan  
James Thompson  
John Vergis  
David J. Zaprazny

When the IEEE-SA Standards Board approved this standard on 17 June 2010, it had the following membership:

**Robert M. Grow, *Chair***  
**Richard H. Hulett, *Vice Chair***  
**Steve M. Mills, *Past Chair***  
**Judith Gorman, *Secretary***

Karen Bartleson  
Victor Berman  
Ted Burse  
Clint Chaplin  
Andy Drozd  
Alexander Gelman  
Jim Hughes

Young Kyun Kim  
Joseph L. Koepfinger\*  
John Kulick  
David J. Law  
Hung Ling  
Oleg Logvinov  
Ted Olsen

Ronald C. Petersen  
Thomas Prevost  
Jon Walter Rosdahl  
Sam Sciacca  
Mike Seavey  
Curtis Siller  
Don Wright

\*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Satish Aggarwal, *NRC Representative*  
Richard DeBlasio, *DOE Representative*  
Michael Janezic, *NIST Representative*

Catherine Berger  
*IEEE Standards Project Editor*

Matthew J. Ceglia  
*IEEE Standards Program Manager, Technical Program Development*

## Contents

|                                                                              |    |
|------------------------------------------------------------------------------|----|
| 1. Scope .....                                                               | 1  |
| 2. Normative references .....                                                | 1  |
| 3. Definitions and abbreviations .....                                       | 2  |
| 3.1 Definitions .....                                                        | 2  |
| 3.2 Abbreviations and acronyms .....                                         | 5  |
| 4. Safety system design basis .....                                          | 5  |
| 5. Safety system criteria .....                                              | 5  |
| 5.1 Single-failure criterion .....                                           | 6  |
| 5.2 Completion of protective action .....                                    | 6  |
| 5.3 Quality .....                                                            | 6  |
| 5.4 Equipment qualification .....                                            | 10 |
| 5.5 System integrity .....                                                   | 10 |
| 5.6 Independence .....                                                       | 13 |
| 5.7 Capability for test and calibration .....                                | 18 |
| 5.8 Information displays .....                                               | 18 |
| 5.9 Control of access .....                                                  | 21 |
| 5.10 Repair .....                                                            | 25 |
| 5.11 Identification .....                                                    | 25 |
| 5.12 Auxiliary features .....                                                | 25 |
| 5.13 Multi-unit stations .....                                               | 25 |
| 5.14 Human factors considerations .....                                      | 25 |
| 5.15 Reliability .....                                                       | 26 |
| 5.16 Common Cause Failure criteria .....                                     | 26 |
| 5.17 Use of commercial digital equipment .....                               | 29 |
| 6. Sense and command features—functional and design requirements .....       | 36 |
| 7. Execute features—functional and design requirements .....                 | 36 |
| 8. Power source requirements .....                                           | 36 |
| Annex A (informative) Mapping of IEEE Std 603-2009 to IEEE Std 7-4.3.2 ..... | 37 |
| Annex B (informative) Diversity requirements determination .....             | 38 |
| Annex C (informative) Dedication of existing commercial computers .....      | 39 |
| C.1 Background .....                                                         | 39 |
| C.2 Discussion .....                                                         | 40 |
| Annex D (informative) Identification and resolution of hazards .....         | 44 |
| D.1 Background .....                                                         | 44 |
| D.2 Discussion .....                                                         | 44 |
| D.3 Purpose of hazard analysis .....                                         | 44 |
| D.4 Hazard analysis implementation guidelines .....                          | 45 |

|                                                        |    |
|--------------------------------------------------------|----|
| Annex E (informative) Communication independence ..... | 57 |
| E.1 Background .....                                   | 57 |
| E.2 Discussion .....                                   | 57 |
| Annex F (informative) Computer reliability.....        | 64 |
| Annex G (informative) Glossary .....                   | 65 |
| Annex H (informative) Bibliography .....               | 69 |

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

*IMPORTANT NOTICE: This standard is not intended to ensure safety, security, health, or environmental protection. Implementers of the standard are responsible for determining appropriate safety, security, environmental, and health practices or regulatory requirements.*

*This IEEE document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading “Important Notice” or “Important Notices and Disclaimers Concerning IEEE Documents.” They can also be obtained on request from IEEE or viewed at <http://standards.ieee.org/IPR/disclaimers.html>.*

## 1. Scope

This standard serves to amplify criteria in IEEE Std 603<sup>TM</sup>-~~1998~~ 2009, [IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations](#), to address the use of computers as part of safety systems in nuclear power generating stations. The criteria contained herein, in conjunction with criteria in IEEE Std 603- 2009, establish minimum functional and design requirements for computers used as components of a safety system.

## 2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

~~This guide shall be used in conjunction with the following standards:~~

IEEE Std 323<sup>TM</sup>-2003 (Reaff 2008), IEEE Standard ~~Criteria for Safety Systems~~ [Qualifying Class 1E Equipment](#) for Nuclear Power Generating Stations.<sup>1, 2</sup>

<sup>1</sup> IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA (<http://standards.ieee.org/>).

<sup>2</sup> The IEEE standards or products referred to in this clause are trademarks of the Institute of Electrical and Electronics Engineers, Inc.

[IEEE Std 344<sup>TM</sup>-2004, IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations.](#)

[IEEE Std 603<sup>TM</sup>-2009, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating](#)

Stations. IEEE Std 1012™-2004, IEEE Standard for Software Verification and Validation.

IEEE Std 1042™-1987 (Reaff 1993) (withdrawn), IEEE Guide to Software Configuration Management.

ISO/IEC 12207:2008 (IEEE Std 12207-2008), Second Edition, 2008-02-01, Systems and Software Engineering—Software life cycle processes.

~~IEEE Std 1012™-1998, IEEE Standard for Software Verification and Validation.~~

~~IEEE Std 1042™-1987 (R1993), IEEE Guide to Software Configuration Management.<sup>3</sup>~~

~~IEEE/EIA Std 12207.0-1996 IEEE/EIA Standard—Industry Implementation of International Standard ISO/IEC 12207:1995 (ISO/IEC 12207), Standard for Information Technology—Software life cycle processes.~~

### 3. Definitions, acronyms and abbreviations

#### 3.1 Definitions

For the purposes of this ~~standard~~, document, the following terms and definitions apply. *The ~~Authoritative Dictionary of IEEE Standards~~ Dictionary: Glossary of Terms & Definitions should be referenced for terms not defined in this clause.*<sup>3</sup>

<sup>1</sup>IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA (<http://standards.ieee.org/>).

<sup>2</sup>The IEEE standards or products referred to in this clause are trademarks of the Institute of Electrical and Electronics Engineers, Inc.

<sup>3</sup>IEEE Std 1042-1987 (Reaff 1993) has been withdrawn; however, copies can be obtained from Global Engineering, 15 Inverness Way

East, Englewood, CO 80112-5704, USA, tel. (303) 792-2181 (<http://global.ihs.com/>).

<sup>4</sup>The numbers in brackets correspond to those of the bibliography in Annex G.

**3.1.1 acceptance testing: (A)** Formal testing conducted to determine whether ~~or not~~ a system satisfies its acceptance criteria and requirements; and to enable the customer to determine whether ~~or not~~ to accept the system. *See also:* equipment qualification testing, system testing. **(B)** Formal testing conducted to enable a user, customer, or other authorized entity to determine whether to accept a system or component.

**3.1.2 basic component:** For operating facilities, a structure, system, component (SSC), or part thereof that affects its safety function and is necessary to assure one or more of the conditions provided below is met. For new plant designs, a basic component is the design or procurement information approved or to be approved within the scope of the design certification or approval for a SSC or part thereof that affects its safety function and is necessary to meet one or more of the following conditions:

- The integrity of the reactor coolant pressure boundary;
- The capability to shut down the reactor and maintain it in a safe shutdown condition; or
- The capability to prevent or mitigate the consequences of accidents with significant potential for offsite exposures.

Basic components are items designed and manufactured under a nuclear quality assurance program, or commercial grade items that have successfully completed the commercial grade dedication process. A basic component includes the safety-related design, analysis, inspection, testing, fabrication, replacement of parts, or consulting services that are associated with the component hardware, software, design certification, or design approval, whether these services are performed by the component supplier or others.

<sup>3</sup>The IEEE Standards Dictionary: Glossary of Terms & Definitions is available at <http://shop.ieee.org/>.

~~**3.1.2 application software:** Software designed to fulfill specific needs of a user; for example, software for navigation, payroll, or process control.~~

**3.1.3 commercial grade dedication:** An acceptance process undertaken to provide reasonable assurance that a commercial grade item to be used as a basic component will perform its intended safety function and, in this respect, is deemed equivalent to an item designed and manufactured under a nuclear quality assurance program. This assurance is achieved by identifying the critical characteristics of the item and by verifying their acceptability by inspections, tests, or analyses performed by the purchaser or third party dedicating entity after delivery or through commercial grade surveys; product inspections or witness at hold points at the supplier's facility, and analysis of historical records for acceptable performance. In all cases, the dedication process must be conducted under a nuclear quality assurance program. The process is considered complete when the dedication activities are complete and the item is designated for use as a basic component.

~~**3.1.3 architecture:** The organizational structure of a system or component~~  
~~**3.1.4 commercial grade item:** An item that is a) not subject to design or specification requirements unique to nuclear facilities; and b) used in applications other than nuclear facilities; and c) ordered from the manufacturer/supplier on the basis of specifications set forth in the manufacturer's published product description (for example, a catalog).~~

**3.1.4 commercial grade item:** A structure, system, component, or part thereof that affects its safety function that was not designed and manufactured as a basic component. These do not include items where the design and manufacturing process require in-process inspections and verifications so that defects or failures to comply are identified and corrected where one or more of the item's critical characteristics cannot be verified. For digital items, the vendor's software life cycle processes can be included as critical characteristics.

~~An item that is a) not subject to design or specification requirements unique to nuclear facilities; and b) used in applications other than nuclear facilities; and c) ordered from the manufacturer/ supplier on the basis of specifications set forth in the manufacturer's published product description (for example, a catalog).~~

**3.1.5 commercial grade service:** A service or activity that affects the safety function of a basic component, performed by a commercial vendor not operating under a nuclear quality assurance program.

~~**3.1.5 commercial grade item dedication:** A process of evaluating and accepting commercial grade items to obtain adequate confidence of suitability for safety application.~~

**3.1.6 computer security:** Protection of digital computer-based systems throughout the development lifecycle of the system to prevent unauthorized, unintended, and unsafe modifications to the system; this includes protection of the safety system during operation and maintenance from inadvertent actions that result in unintended consequences.

~~**3.1.6 complexity:** (1) The degree to which a system or system component has a design or implementation that is difficult to understand and verify. (2) Pertaining to any set of structure-based metrics that measure the attribute in definition (1).~~

**3.1.7 configuration:** (A) The arrangement of a computer system or component as defined by the number, nature, and interconnections of its constituent parts. (B) In configuration management, the

functional and physical characteristics of hardware or software as set forth in technical documentation or achieved in a product.

~~**3.1.7 component:** One of the parts that make up a system. A component may be hardware or software and may be subdivided into other components.~~

~~NOTE—The terms “module,” “component,” and “unit” are often used interchangeably or defined to be supplements of one another in different ways dependent upon the context. The relationship of these terms is not yet standardized.~~

**3.1.8 configuration control:** An element of configuration management, consisting of the evaluation, coordination, approval or disapproval, and implementation of changes to configuration items after formal establishment of their configuration identification.

~~**3.1.8 computer:** A functional programmable unit that consists of one or more associated processing units and peripheral equipment, that is controlled by internally stored programs, and that can perform substantial computation, including numerous arithmetic or logic operations, without human intervention.~~

**3.1.9 configuration item:** An aggregation of hardware, software, or both, that is designated for configuration management and treated as a single entity in the configuration management process.

~~**3.1.9 computer instruction:** (1) A statement in a programming language, specifying an operation to be performed by a computer and the addresses or values of the associated operands; for example, Move A to B. (2) Loosely, any executable statement in a computer program.~~

**3.1.10 configuration management:** A discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements.

~~**3.1.10 computer program:** A combination of computer instructions and data definitions that enable computer hardware to perform computational or control functions.~~

**3.1.11 critical characteristics:** Important design, material, and performance (including design process) attributes of a commercial grade item that, once verified, will provide reasonable assurance that the item will perform its intended safety function. Used for the dedication of commercial grade services to confirm equivalent results are produced to those that would have been produced had the vendor been operating under a nuclear quality assurance program.

~~**3.1.11 computer system:** A system containing one or more computers and associated software.~~

**3.1.12 critical characteristics for acceptance:** Those selected, identifiable, and measurable attributes and variables of a commercial grade item or service, when verified, provide reasonable assurance that the item received is the item specified.

NOTE—Adapted from EPRI NP-5652 [B3].<sup>4</sup>

<sup>4</sup>The numbers in brackets correspond to those of the bibliography in Annex H.

**3.1.13 critical characteristics for design:** Those selected properties or attributes which are essential for the item's form, fit, and functional performance. For design they are the identifiable and measurable attributes of a commercial grade item that provide reasonable assurance that the item will perform its design function. An example for design shall be design methods used to implement the various life cycle phases.

NOTE—Adapted from EPRI NP-5652 [B3].

**3.1.14 dedicating entity:** For operating facilities, the organization that performs the dedication process under a nuclear quality assurance program. Dedication may be performed by the manufacturer of the item, a third-party, or the utility itself. This organization is responsible for identifying and evaluating deviations, reporting defects and failures to comply for the dedicated item, and maintaining auditable records of the dedication process.

**3.1.15 engineering workstation:** A computer-based tool that performs engineering and maintenance functions, including creating new control functions, adding various input and output points, modifying sequential and continuous control logic, simulating the logic offline, supporting database engineering, and preparing such engineering documentation as input/output (I/O) lists and device summaries. It provides a means to monitor and troubleshoot various aspects of system operation including diagnostics, install and update program elements, recover from failures, and perform miscellaneous tasks associated with system administration.

NOTE—Adapted from the Instrument Engineer's Handbook, Fourth Edition, ed. by Béla Lipták, and from U.S. CERT online document, Control Systems Security Program (CSS), Overview of Cyber Vulnerabilities.

**3.1.16 equipment qualification:** The demonstration and documentation of the ability of the equipment, consisting of the integrated hardware and software, to perform its safety function or functions under applicable service conditions, including design basis events. Equipment Qualification is defined in IEEE Std 323-2003.

~~**3.1.16 correctness:** (1) The degree to which a system or component is free from faults in its specification, design, and implementation. (2) The degree to which software, documentation, or other items meet the specified requirements. (3) The degree to which software, documentation, or other items meet user needs and expectations, whether specified or not.~~

**3.1.17 firmware:** The combination of a hardware device, software and data that are incorporated into the hardware device. For compliance with this standard, firmware shall be treated as software in a programmable device.

NOTE—Adapted from IEEE Std 610.12™-1990 [B19].

~~**3.1.17 data:** (1) A representation of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automatic means. (2) Sometimes used as a synonym for documentation.~~

**3.1.18 hazard:** A condition that is a prerequisite to an accident. Hazards include external events as well as conditions internal to computer hardware or software.

~~**3.1.18 data structure:** A physical or logical relationship among data elements, designed to support specific data manipulation functions.~~

**3.1.19 hazard analysis:** A process that explores and identifies conditions that are not identified by the normal design review and testing process. The scope of hazard analysis extends beyond plant design basis events by including abnormal events and plant operations with degraded equipment and plant systems. Hazard analysis focuses on system failure mechanisms rather than verifying correct system operation.

~~**3.1.19 design:** (1) The process of defining the architecture, components, interfaces, and other characteristics of a system or component. (2) The result of the process in definition (1).~~

**3.1.20 protected area:** An area encompassed by physical barriers and to which access is controlled.

~~**3.1.20 document:** (1) A medium and the information recorded on it, that generally has permanence and can be read by a person or a machine. Examples in software engineering include project plans, specifications, test plans, user manuals. (2) To create a document as in definition (1). (3) To add comments to a computer program.~~

**3.1.21 safe shutdown condition:** Bringing the plant to those shutdown conditions specified in plant technical specifications as Hot Standby or Hot Shutdown, as appropriate.

~~**3.1.21 documentation:** (1) A collection of documents on a given subject. (2) Any written or pictorial information describing, defining, specifying, reporting or certifying activities, requirements, procedures, or results. (3) The process of generating or revising a document. (4) The management of documents, including identification, acquisition, processing, storage, and dissemination.~~

**3.1.22 safe state:** A state in which potential hazards and operational risks are minimized.

NOTE—Determining the safe state(s) of a device is a plant systems issue, which is outside the scope of this standard (i.e., not solely related to digital design).

~~**3.1.22 error:** (1) The difference between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition. For example, a difference of 30 meters between a computed result and the correct result. (2) An incorrect step, process, or data definition. For example, an incorrect instruction in a computer program. (3) An incorrect result. For example, a computed result of 12 when the correct result is 10. (4) A human action that produces an incorrect result. For example, an incorrect action on the part of a programmer or operator.~~

~~NOTE—While all four definitions are commonly used, one distinction assigns definition (1) to the word “error,” definition (2) to the word “fault,” definition (3) to the word “failure,” and definition (4) to the word “mistake.”~~

**3.1.23 software tools:** A computer program used in the design, development, testing, review, analysis, or maintenance of a program or its documentation. Examples include compilers, assemblers, linkers, comparators, cross-reference generators, decompilers, editors, flow charts, monitors, test case generators, integrated development environments, and timing analyzers.

NOTE—Adapted from IEEE Std 610.12-1990 [B19].

~~**3.1.23 execution:** The process of carrying out an instruction or the instructions of a computer program by a computer.~~

**3.1.24 vital area:** Any area that contains any equipment, system, device, or material, the failure, destruction, or release of which could endanger the public health and safety, directly or indirectly, by exposure to radiation (referred to as vital equipment), or equipment or systems that are required to function to protect public health and safety following such failure, destruction, or release.

~~**3.1.24 failure:** The inability of a system or component to perform its required functions within specified performance requirements.~~

~~NOTE—The fault tolerance discipline distinguishes between a human action (a mistake), its manifestation (a hardware or software fault), the result of the fault (a failure), and the amount by which the result is incorrect (the error).~~

~~**3.1.25 fault:** (1) A defect in a hardware device or component; for example, a short circuit or broken wire. (2) An incorrect step, process, or data definition in a computer program.~~

~~NOTE—This definition is used primarily by the fault tolerance discipline. In common usage, the terms “error” and “bug” are used to express this meaning.~~

**3.1.26 firmware:** The combination of a hardware device and computer instructions and data that reside as read-only software on that device.

**3.1.27 function:** A defined objective or characteristic action of a system or component. For example, a system may have inventory control as its primary function.

**3.1.28 functional unit:** An entity of hardware, software, or both capable of accomplishing a specified purpose.

**3.1.29 hardware:** Physical equipment used to process, store, or transmit computer programs or data.

**3.1.32 implementation:** (1) The process of translating a design into hardware components, software components, or both. (2) The result of the process in definition (1).

**3.1.33 interface:** (1) A shared boundary across which information is passed. (2) A hardware or software component that connects two or more other components for the purpose of passing information from one to the other. (3) To connect two or more components for the purpose of passing information from one to the other. (4) To serve as a connecting or connected component as in definition (2).

**3.1.34 module:** (1) A program unit that is discrete and identifiable with respect to compiling, combining with other units, and loading; for example, the input to, or output from an assembler, compiler, linkage editor, or executive routine. (2) A logically separable part of a program.

**3.1.35 procedure:** (1) The course of action taken for the solution of a problem. A course of action taken to perform a given task. (2) A written description of a course of action as in definition (1) for example, a documented test procedure. (3) A portion of a computer program that is named and that performs a specific action.

**3.1.36 qualification testing:** Testing performed to demonstrate to the acquirer that the software item or system meets its specified requirements.

**3.1.37 requirement:** (1) A condition or capability needed by a user to solve a problem or achieve an objective. (2) A condition or capability that must be met or possessed by a system or system component to satisfy a contract, standard, specification, or other formally imposed documents. (3) A documented representation of a condition or capability as in definition (1) or definition (2).

**3.1.38 requirements specification:** A document that specifies the requirements for a system or component. Typically included are functional requirements, performance requirements, interface requirements, design requirements, and development standards.

**3.1.39 safety system:** A system that is relied upon to remain functional during and following design basis events to ensure: the integrity of the reactor coolant pressure boundary; the capability to shut down the reactor and maintain it in a safe shutdown condition; or the capability to prevent or mitigate the consequences of accidents that could result in potential off-site releases.

**3.1.40 software:** Computer programs, procedures, and associated documentation and data pertaining to the operation of a computer system.

**3.1.41 software maintenance:** (1) Modification of a software product after delivery to correct faults, to improve performance or other attributes, or to adapt the product to a modified environment. (2) The set of activities that takes place to ensure that software installed for operational use continues to perform as

~~intended and fulfill its intended role in system operation. Software maintenance includes improvements, aid to users, and related activities.~~

~~**3.1.42 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.~~

~~**3.1.43 specification:** A document that specifies, in a complete, precise, verifiable manner, the requirements, design, behavior, or other characteristics of a system or system, and, often, the procedures for determining whether these provisions have been satisfied.~~

~~**3.1.44 system:** A collection of components organized to accomplish a specific function or a set of functions.~~

~~**3.1.45 system software:** Software designed to facilitate the operation and maintenance of a computer system and its associated programs; for example, operating systems, assemblers, utilities.~~

~~**3.1.46 system testing:** Testing conducted on a complete, integrated system to evaluate the system's compliance with its specified requirements.~~

~~**3.1.47 testing:** (1) The process of operating a system or component under specified conditions, observing or recording the results, and making an evaluation of some aspect of the system or component. (2) The process of analyzing a software item to detect the difference between existing and required conditions (that is, bugs) and to evaluate the features of the software items.~~

~~**3.1.48 test plan:** (1) A document describing the scope, approach, resources, and schedule of intended test activities. It identifies test items, the features to be tested, the testing tasks, who will do each task, and any risks requiring contingency planning. (2) A document that describes the technical and management approach to be followed for testing a system or component. Typical contents identify the items to be tested, tasks to be performed, responsibilities, schedules, and required resources for the testing activity.~~

~~**3.1.49 validation:** The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements.~~

~~**3.1.50 verification:** (1) The process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase. (2) Formal proof of program correctness.~~

~~**3.1.51 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 Acronyms and abbreviations

The following abbreviations and acronyms appear in this standard:

|                |                                        |
|----------------|----------------------------------------|
| ATWS           | anticipated transient without scram    |
| <del>CFR</del> | <del>Code of Federal Regulations</del> |
| <del>CCF</del> | <del>Common Cause Failure</del>        |
| <del>CDR</del> | <del>critical digital review</del>     |
| COTS           | commercial off-the-shelf               |
| <del>CRC</del> | <del>eyelie redundancy check</del>     |

|                          |                                                                                  |
|--------------------------|----------------------------------------------------------------------------------|
| <del>FTA</del>           | <del>fault tree analysis</del>                                                   |
| <a href="#">D3</a>       | <a href="#">defense in depth and diversity</a>                                   |
| <a href="#">DPRAM</a>    | <a href="#">dual-ported random access memory</a>                                 |
| <a href="#">EIA</a>      | <a href="#">Electronic Industries Alliance</a>                                   |
| <a href="#">EPRI</a>     | <a href="#">Electric Power Research Institute</a>                                |
| <a href="#">EQ</a>       | <a href="#">equipment qualification</a>                                          |
| FMEA                     | failure modes and effects analysis                                               |
| <del>IV&amp;V</del>      | <del>independent verification and validation</del>                               |
| <del>MTBF</del>          | <del>mean time between failures</del>                                            |
| <del>PROM</del>          | <del>programmable read-only memory</del>                                         |
| <a href="#">FTA</a>      | <a href="#">fault tree analysis</a>                                              |
| <a href="#">IEC</a>      | <a href="#">International Electrotechnical Commission</a>                        |
| <a href="#">M&amp;TE</a> | <a href="#">measurement and test equipment</a>                                   |
| <a href="#">NEI</a>      | <a href="#">Nuclear Energy Institute</a>                                         |
| <a href="#">PLC</a>      | <a href="#">Programmable Logic Controller</a>                                    |
| QA                       | quality assurance                                                                |
| <a href="#">QFR</a>      | <a href="#">reinforced functional qualification (translated from the French)</a> |
| RAM                      | random access memory                                                             |
| <del>SAT</del>           | <del>site acceptance testing</del>                                               |
| <del>SVVP</del>          | <del>software verification and validation plan</del>                             |
| <del>USNRC</del>         | <del>United States Nuclear Regulatory Commission</del>                           |
| <del>V&amp;V</del>       | <del>verification and validation</del>                                           |
| <a href="#">SAR</a>      | <a href="#">Safety Analysis Report</a>                                           |
| <a href="#">SER</a>      | <a href="#">Safety Evaluation Report</a>                                         |
| <a href="#">SSC</a>      | <a href="#">structure, system, component</a>                                     |
| <a href="#">V&amp;V</a>  | <a href="#">verification and validation</a>                                      |

## 4. Safety system design basis

NOTE—See Annex A for more information about the relationship of this standard to IEEE Std 603- 2009.

No requirements beyond IEEE Std 603- 2009 are necessary.

## 5. Safety system criteria

The following subclauses list the safety system criteria in the order they are listed in IEEE Std 603- 2009. For some criteria, there are no additional requirements beyond what is stated in IEEE Std 603- 2009. For other criteria, additional requirements are described in 5.1 through 5.17.

### 5.1 Single-failure criterion

[In addition to the](#) ~~No~~ requirements ~~beyond in~~ IEEE Std 603-~~1998 are necessary~~ [2009, the following criteria apply for digital computers in safety systems](#) (see also 5.16):

- a) [Functions that are assumed to malfunction independently in the safety analysis shall not be affected by failure of a single control processor.](#)
- b) [Functions shall be configured \(e.g., functionally distributed\) such that a single processor malfunction or software error shall not result in spurious actuations that are not enveloped in the plant design bases, accident analyses, anticipated transient without scram \(ATWS\) provisions, or other provisions for abnormal conditions. This includes spurious actuation of more than one plant device or system as a result of processor malfunction or software error. The possibility and consequences of malfunction of multiple processors as a result of common software error shall](#)

[be addressed \(see 5.16\).](#)

## 5.2 Completion of protective action

No requirements beyond IEEE Std 603- 2009 are necessary.

## 5.3 Quality

Hardware quality is addressed in IEEE Std 603- 2009. Software quality is addressed in ISO/IEC 12207:2008 (IEEE Std 12207 -2008) and supporting standards. Computer development activities shall include the development of computer hardware and software. The integration of the computer hardware and software and the integration of the computer with the safety system shall be addressed in the development process.

A typical computer system development process consists of the following life cycle processes:

- Creating the conceptual design of the system, translation of the concepts into specific system requirements
- Using the requirements to develop a detailed system design
- Implementing the design into hardware and software functions
- Testing the functions to confirm that the requirements have been correctly implemented
- Installing the system and performing site acceptance testing
- Operating and maintaining the system
- Retiring the system

In addition to the requirements of IEEE Std 603-2009, the following activities necessitate additional requirements that are necessary to meet the quality criterion:

- Software development
- Qualification of existing commercial computers (see 5.17)
- Use of software tools
- Verification and validation
- Configuration management
- Risk Management

### 5.3.1 Software development

Computer software shall be developed, modified, or accepted in accordance with ~~an approved~~ a software quality assurance (QA) plan consistent with the requirements of ISO/IEC 12207:2008 (IEEE Std 12207-2008). The software QA plan shall address all software that is resident on the computer at run time (i.e., application software, network software, interfaces, operating systems, and diagnostics). Guidance for developing software QA plans can be found in IEC 60880 (+986-09) [B4 Ed. 2, (2006-05) [B13] and IEEE Std 730™-1998 [B8] 2002 [B20].

[The software QA plan shall also address the software tools for system development and maintenance as described in 5.3.2.](#)

### 5.3.1.1 Software quality metrics

The use of software quality metrics shall be considered throughout the software life cycle to assess whether software quality requirements are being met. When software quality metrics are used, the following life cycle phase characteristics should be considered:

- Correctness/Completeness (Requirements phase)
- Compliance with requirements (Design phase)
- Compliance with design (Implementation phase)
- Functional compliance with requirements (Test and Integration phase)
- On-site functional compliance with requirements (Installation and Checkout phase)
- Performance history (Operation and Maintenance phase)

The basis for the metrics selected to evaluate software quality characteristics should be included in the software development documentation. IEEE Std 1061™-1998 [B23] provides a methodology for the application of software quality metrics.

### 5.3.2 Software tools

If software tools are used during the life cycle process of safety-related software, one or both of the following methods shall be used to confirm outputs of that software tool are suitable for use in safety-related systems:

- a) The output of the software tool shall be subject to the same level of verification and validation (V&V) as the safety-related software, to determine that the output of that tool meets the requirements established during the previous lifecycle phase.
- b) The tool shall be developed using the same or an equivalent high quality lifecycle process as required for the software upon which the tool is being used as described in this subclause (5.3) or commercially dedicated as in 5.17, to provide confidence that the necessary features of the software tool function as required.

Software tools used to support the software life cycle process of safety-related software shall be controlled under configuration management.

~~Software tools used to support software development processes and verification and validation (V&V) processes shall be controlled under configuration management.~~

~~One or both of the following methods shall be used to confirm the software tools are suitable for use:~~

- a) ~~A test tool validation program shall be developed to provide confidence that the necessary features of the software tool function as required.~~
- b) ~~The software tool shall be used in a manner such that defects not detected by the software tool will be detected by V&V activities.~~

~~Tool operating experience may be used to provide additional confidence in the suitability of a tool, particularly when evaluating the potential for undetected defects.~~

### 5.3.3 Verification and validation

NOTE—See IEEE Std 1012-1998 and IEEE Std 1012a™-1998 [B10] 2004 for more information about software V&V.

V&V is an extension of the program management and systems engineering team activities. V&V is used

to identify objective data and conclusions (i.e., proactive feedback) about digital system quality, performance, and development process compliance throughout the system life cycle. Feedback consists of anomaly reports, performance improvements, and quality improvements regarding the expected operating conditions across the full spectrum of the system and its interfaces.

V&V processes are used to confirm that the development products of an activity conform to the requirements of that activity, and ~~whether~~ that the system performs according to its intended use and user needs. This determination of suitability includes assessment, analysis, evaluation, review, inspection, and testing of products and processes.

This standard adopts the IEEE Std 1012-2004 terminology of process, activity and task, in which software V&V processes are subdivided into activities, which are further subdivided into tasks. The term V&V effort is used to reference this framework of V&V processes, activities, and tasks.

V&V processes shall address the computer hardware as it affects software, computer software, integration of the digital system components, and the interaction of the resulting computer system with the nuclear power plant.

The V&V activities and tasks shall include system testing of the final integrated hardware, software, firmware, and interfaces.

The software V&V effort shall be performed in accordance with IEEE Std 1012-2004. The IEEE Std 1012- 2004 V&V requirements for the highest integrity level (software integrity level 4) apply to systems developed using this standard (i.e., IEEE Std 7-4.3.2<sup>TM</sup>). See IEEE Std 1012- 2004 Annex B for a definition of integrity level 4 ~~software~~.

### 5.3.4 V&V independence requirements

~~The previous section addresses the V&V activities to be performed. This section defines the levels of Independent verification and validation is required for safety-related software. In order to have independent verification and validation, three different types of independence are required as follows:~~

- ~~1) The verification and validation staff shall report to a separate organization with sufficient authority and organizational freedom, including sufficient independence required for the V&V effort. IV&V activities are defined by three parameters: technical independence, managerial independence, and financial independence. These parameters are described from cost and schedule limitations, as defined~~ in Annex C of IEEE Std 1012- 2004.
- 2) The development activities and tests shall be verified and validated by individuals or groups with appropriate technical competence, other than those who developed the original design.
- ~~3) The original designers, people who contributed to the design, design and development project management, and staff supervising the original designers shall not perform or oversee independent verification and validation on safety-related software.~~

~~Oversight of the IV&V effort shall be vested in an organization separate from the development and program management organizations. The V&V effort shall independently select~~

- ~~a) The segments of the software and system to be analyzed and tested~~
- ~~b) The V&V techniques, and~~
- ~~c) The technical issues and problems upon which to act.~~

Testing throughout the life cycle process may be conducted by the V&V organization or the design organization or both. Regardless of who actually writes the procedures and/or conducts the tests, the test

[procedures and reports shall be independently verified by the alternate organization.](#)

~~The V&V effort shall be allocated resources that are independent of the development resources. See Annex C of IEEE Std 1012- 2004 provides additional guidance.~~

### 5.3.5 Software configuration management

Software configuration management shall be performed in accordance with IEEE Std 1042-1987. IEEE Std 828™ - 2005 [B21] provides guidance for the development of software configuration management plans.

The minimum set of activities shall address the following:

- a) Identification and control of all software designs and code
- b) Identification and control of all software design functional data (e.g., data templates and data bases)
- c) Identification and control of all software design interfaces
- d) Control of all software design changes
- e) Control of software documentation (user, operating, and maintenance documentation)
- f) Control of software vendor development activities for the supplied safety system software
- g) Control and retrieval of qualification information associated with software designs and code
- h) Software configuration audits
- i) Status accounting

Some of these functions or documents may be performed or controlled by other QA activities. In this case, the software configuration management plan shall describe the division of responsibility.

A software baseline shall be established at appropriate points in the software life cycle process to synchronize engineering and documentation activities. Approved changes that are created subsequent to a baseline shall be added to the baseline.

The labeling of the software for configuration control shall include unique identification of each configuration item, and revision and/or date time stamps for each configuration item.

Changes to the software shall be formally documented and approved consistent with the software configuration management plan. The documentation shall include the reason for the change, identification of the affected software and the impact of the change on the system [including the hazards and risks analysis](#). Additionally, the documentation should include the plan for implementing the change in the system (e.g., immediately implementing the change, or scheduling the change for a future version) [along with updating documentation including the hazards and risk analyses and additional software life cycle activities such as V&V.](#)

### 5.3.6 Software project risk management

Software project risk management is a tool for problem prevention: identifying potential problems, assessing their impact, and determining which potential problems shall be addressed to assure that software quality goals are achieved. Risk management shall be performed at all levels of the digital system project to provide adequate coverage for each potential problem area. Software project risks shall include technical, schedule, ~~or cost and~~ resource-related risks that could compromise software quality goals, and thereby affect the ability of the ~~safety-computer~~ digital system ~~or component~~ to perform ~~its~~ safety-related functions. Software project risk management differs from hazard analysis (see Annex D) in that hazard analysis is focused solely on the technical aspects of system failure mechanisms [and their](#)

effect on plant safety, rather than risks to project execution. Overlap between the project risks and hazard analyses are possible when elements are common to both. Such overlaps shall be evaluated as software project risks as well as through the hazards analysis process.

Risk management shall include the following steps:

- a) Determine the scope of risk management to be performed for the digital system.
- b) Define and implement appropriate risk management strategies.
- c) Identify risks to the software project in the project risk management strategy and as they develop during the conduct of the project.
- d) Analyze risks to determine the priority for their mitigation.
- e) Develop risk mitigation plans for risks that have the potential to significantly impact software quality goals, with appropriate metrics for tracking resolution progress. (These risks may include technical, schedule, or resource-related project risks that could compromise the ability of the safety computer system to perform safety-related functions.)
- f) Take corrective actions when expected quality is not achieved.
- g) Establish a project environment that supports effective communications between individuals and groups for the resolution of software project risks.

Additional guidance on the topic of risk management is provided in ISO/IEC 12207 :2008 (IEEE Std 12207-2008).

## 5.4 Equipment qualification

The requirements in this subclause shall be applied in addition to the equipment qualification criteria provided by IEEE Std 603-2009, based on IEEE Std 323-2003.

Equipment qualification testing shall be performed with the system functioning with software and diagnostics representative of those intended to be used in actual operation. All portions of the computer necessary to accomplish safety functions and those portions whose operation or failure could impair safety functions shall be exercised during testing. This includes, as appropriate and practicable, exercising and monitoring the memory, the CPU, inputs and outputs, display functions, diagnostics, associated components, communication paths, and interfaces. Testing shall demonstrate that the performance requirements related to safety functions have been met in the presence of all defined environmental and plant input and output stressors. Equipment qualification is required for commercial grade items as well as equipment produced under a nuclear quality assurance program.

~~In addition to the equipment qualification criteria provided by IEEE Std 603-1998, the requirements listed in 5.4.1 and 5.4.2 are necessary to qualify digital computers for use in safety systems.~~

### 5.4.1 Computer system testing

~~Computer system qualification testing (see 3.1.36) 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 safety functions, or those portions whose operation or failure could impair safety functions, 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 performance requirements related to safety functions have been met.~~

## **5.4.2 Qualification of existing commercial computers**

NOTE— See Annex C for more information about commercial grade item dedication.

The qualification process shall be accomplished by evaluating the hardware and software design using the criteria of this standard. Acceptance shall be based upon evidence that the digital system or component, including hardware, software, firmware, and interfaces, can perform its required functions. The acceptance and its basis shall be documented and maintained with the qualification documentation.

In those cases in which traditional qualification processes cannot be applied, an alternative approach to verify a component is acceptable for use in a safety related application is commercial grade dedication. The objective of commercial grade dedication is to verify that the item being dedicated is equivalent in quality to equipment developed under a 10 CFR 50 Appendix B program [B16].

The dedication process for the computer shall entail identification of the physical, performance, and development process requirements necessary to provide adequate confidence that the proposed digital system or component can achieve the safety function. The dedication process shall apply to the computer hardware, software, and firmware that are required to accomplish the safety function. The dedication process for software and firmware shall, whenever possible, include an evaluation of the design process. There may be some instances in which a design process cannot be evaluated as part of the dedication process. For example, the organization performing the evaluation may not have access to the design process information for a microprocessor chip to be used in the safety system. In this case, it would not be possible to perform an evaluation to support the dedication. Because the dedication process involves all aspects of life cycle processes and manufacturing quality, commercial grade item dedication should be limited to items that are relatively simple in function relative to their intended use.

Commercial grade item dedication involves preliminary phase and detailed phase activities. These phase activities are described in 5.4.2.1 through 5.4.2.2.

### **5.4.2.1 Preliminary phase of the COTS dedication process**

In the preliminary phase, the risks and hazards are evaluated, the safety functions are identified, configuration management is established, and the safety category of the system is determined.

#### **5.4.2.1.1 Evaluate the system safety function risks and hazards**

An analysis shall be performed to identify the functional and performance requirements of the safety system. This analysis shall identify the risks and hazards that could interfere with accomplishing the safety function.

#### **5.4.2.1.2 Identify the safety function(s) the COTS item shall perform**

Once the system level functions have been identified and the risks and hazards have been evaluated, the dedicating organization shall identify the safety functions to be performed by the COTS item. This process shall address all safety functions to be performed by the COTS, and the potential affect of the COTS function(s) on other safety related functions or interfaces.

#### **5.4.2.1.3 Establish configuration management controls**

COTS items to be used in safety systems shall be controlled in a configuration management process that provides traceability of the COTS item development life cycle processes.

#### 5.4.2.2 Detailed phase of the COTS dedication process

Following this preliminary phase of commercial dedication, the commercial-grade item is evaluated for acceptability using detailed acceptance criteria. The critical characteristics by which a COTS item will be evaluated for use in a safety system shall be identified by a technical evaluation. Each critical characteristic shall be verifiable (e.g., by inspection, analysis, demonstration, or testing). This standard uses the following three categories of commercial-grade item critical characteristics:

- Physical characteristics include attributes such as physical dimensions, power requirements, part numbers, hardware and software model and version numbers, and data communication physical requirements.
- Performance characteristics include attributes such as response time, human-machine functional requirements, memory allocation, safety function performance during abnormal conditions, reliability, error handling, required imbedded functions, and environmental qualification requirements (e.g., seismic, temperature, humidity, and electromagnetic compatibility).
- Development process characteristics include attributes such as supporting life-cycle processes (e.g., verification and validation activities, configuration management processes, and hazard analyses), traceability, and maintainability.

As part of defining these critical characteristics, analyses shall identify potential hazards that could interfere with the safety functions (see Annex D).

Annex C describes the processes that should be used individually or in combination to evaluate the physical, performance, and development process critical characteristics.

#### 5.4.2.3 Maintenance of commercial dedication

If computer hardware, software, or firmware has been procured as a commercial-grade item and accepted through a commercial dedication process, then changes to the commercially dedicated computer hardware, software, or firmware shall be traceable through formal documentation.

Changes to the commercially dedicated computer hardware, software, or firmware shall be evaluated in accordance with the process that formed the basis for the original acceptance. Included in this evaluation shall be consideration of the potential impact that computer hardware revisions may have on software or firmware. If any elements of the approved process have been omitted during the computer hardware, software, or firmware revision process, further evaluation shall be required.

Commercial-grade dedication of computer hardware, software, or firmware is performed for a specific safety system application. Use of a commercially dedicated item in safety system applications beyond that included in the baseline dedication shall require additional evaluation for the new application.

Documentation supporting the commercial-grade item dedication shall be maintained as a configuration item.

### 5.5 System integrity

In addition to the system integrity criteria provided by IEEE Std 603-2009, the following **are necessary shall be considered** to achieve system integrity in digital equipment for use in safety systems:

- Design for computer integrity
- Design for test and calibration
- Fault detection and self-diagnostics
- [Prioritization of functions](#)

### 5.5.1 Design for computer integrity

The computer shall be designed to perform its safety function when subjected to conditions, external or internal, that have significant potential for defeating the safety function. Such conditions include input and output processing failures; precision or roundoff problems; improper recovery actions; electrical [supply](#), input voltage and frequency fluctuations; maximum credible number of coincident signal changes; [and environmental stressors](#).

If the system requirements identify a safety system preferred failure mode, failures of the computer shall not preclude the safety system from being placed in that mode. Performance of computer system restart operations shall not result in the safety system being inhibited from performing its function [including causing a spurious safety system actuation](#).

### 5.5.2 Design for test and calibration

Test and calibration functions shall not adversely affect the ability of the system 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 functions shall not affect system functions that are 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) [when the test and calibration functions](#) 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 is resident on a separate computer and does not provide the sole verification of test and calibration data for the computer that is part of the safety system.

### 5.5.3 Fault detection and self-diagnostics

Computer systems can experience partial failures that can degrade the capabilities of the computer system, but may not be immediately detectable by the system. Self-diagnostics are one means that can be used to assist in detecting these failures. Fault detection and self-diagnostics requirements are addressed in this subclause.

The reliability requirements of the safety system shall be used to establish the need for self-diagnostics [and the frequency of periodic manual testing](#). Self diagnostics are not required for systems in which failures can be detected by alternate means in a timely manner. If self-diagnostics are incorporated into the system requirements, these functions shall be subject to the same V&V processes as the safety system functions.

If reliability requirements warrant self-diagnostics, then computer programs shall incorporate functions to detect and report computer system faults and failures in a timely manner. Self-diagnostic functions shall not adversely affect the ability of the computer system to perform its safety function, or cause spurious actuations of the safety function. A typical set of self-diagnostic functions includes the following:

- Memory functionality and integrity tests (e.g., programmable read only memory checksum and random access memory tests)
- Computer system instruction set [tests](#) (e.g., calculation tests)
- Computer peripheral hardware tests (e.g., watchdog timers and keyboards)
- Computer architecture support hardware [tests](#) (e.g., address lines and shared memory interfaces)

- Communication link diagnostics (e.g., cyclic redundancy checks)

Infrequent communication link failures that do not result in a system failure or a lack of system functionality ~~do not require reporting~~ shall be identified for utility or vendor resolution, and should be evaluated to the extent practical.

When self-diagnostics are applied, the following self-diagnostic features shall be incorporated into the system design:

- a) Self-diagnostics during computer system startup
- b) Periodic self-diagnostics while the computer system is operating
- c) Self-diagnostic test failure reporting

#### **5.5.4 Prioritization of functions**

This subclause presents criteria applicable to prioritization of functions. A priority function receives device actuation commands from safety and non-safety sources, and sends the command having highest priority to one or more safety-related actuated devices. An actuated device is a safety-related component such as a motor actuated valve, a pump motor, a solenoid operated valve, etc. A non-safety source may be any non-safety component including operator or maintenance video display units, computerized procedure systems, control systems, diverse actuation systems, etc.

- a) A priority function shall be a safety-related function.
- b) The priority function used for a diverse actuation signal shall be independent of the postulated CCF of the remainder of the digital system, and shall function properly regardless of the state or condition of the digital system.
- c) Commands that originate in the safety system shall have priority over commands that originate in non-safety systems, with the exception of non-safety diverse actuation signals. When signals that originate from the safety system are combined with diverse actuation signals, priority shall be given to the signal that corresponds with the predetermined safe state of the controlled device(s) such that that the safe state will be achieved even in the presence of a CCF in the safety system that erroneously demands a non-safe state. For devices with more than one safe state (e.g., auxiliary feedwater isolation valves), this requires selection of the preferred safe state. Determining the safe state or the preferred safe state of a device is a plant systems issue, which is outside the scope of this standard (i.e., not a safety computer system design issue).
- d) A priority function may control one or more components. If a priority function controls more than one component, then all of these provisions contained in this section shall apply to each of the actuated components.
- e) Communication isolation for each priority function should be as described in 5.6.4 of this standard.
- f) Software tools used in the design, testing, maintenance, etc. of a priority function are subject to the requirements in 5.3.2, Software Tools. This includes software tools applicable to any programmable device used in support of the safety function of a prioritization function, such as programmable logic devices (PLDs), programmable gate arrays, or other such devices. Validation of design tools used for programming a priority function or a component of a priority function is not necessary if the device directly affected by those tools is 100% tested before being released for service. See item g) below for requirements for 100% testing. The testing should not involve the use of the design tool itself.
- g) If the priority function is to be 100% tested, testing shall include the application of every possible combination of inputs and the evaluation of all of the outputs that result from each combination of inputs. If a priority function includes state-based logic (that is, if the response to a particular

set of inputs depends upon past conditions), then all possible sequences of input sets shall be tested. If testing of all possible sequences of input sets is not considered practical, then the testing that is excluded shall be identified and the exclusion shall be justified. The testing planned or performed shall be shown to provide adequate assurance of proper operation under all conditions and sequences of conditions. It is possible that logic devices within the priority function include unused inputs. If those inputs are forced by the module circuitry to a particular known state, those inputs can be excluded from the “all possible combinations” criterion.

- h) Nonvolatile memory (such as burned-in or reprogrammable gate arrays or random-access memory) shall not be changeable while in service, either by design provisions requiring removal and replacement of the memory device, or through the use of physical restrictions such as those in 5.6.4.2 of this standard, i.e., physical cable disconnect, or keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic. The contents and configuration of field programmable memory shall be considered to be software, and shall be developed, maintained, and controlled accordingly.
- i) The priority function shall be tested through manual periodic tests and/or through automatic self-diagnostics. Automatic testing within a priority module, whether initiated from within the module or triggered from outside and including failure of automatic testing features, shall not inhibit the safety function.
- j) Software-based prioritization shall meet all requirements (quality requirements, V&V, documentation, etc.) applicable to safety-related software.

The priority function shall be implemented such that the completion of a protective action as required by IEEE Std 603-2009 is not interrupted by commands, conditions, or failures outside the function’s own safety division.

## 5.6 Independence

In addition to the requirements of IEEE Std 603-2009, data communication between safety divisions or between safety and non safety systems shall not inhibit the performance of the safety function.

IEEE Std 603-2009 requires that safety functions be separated from non-safety functions such that the non- safety functions cannot prevent the safety system from performing its intended functions. In digital systems, software performing safety functions and software performing non-safety functions may reside on the same computer and use the same computer resources.

~~Either of the following approaches is acceptable to address the previous issues:~~

- ~~a) Barrier requirements shall be identified to provide adequate confidence that the nonsafety functions cannot interfere with performance of the safety functions of the software or firmware. The barriers non-safety software functions shall be designed developed in accordance with the safety-related requirements of this standard. The nonsafety software is not required to meet these requirements.~~
- ~~b) If barriers between the safety software and nonsafety software are not implemented, the nonsafety software functions shall be developed in accordance with the requirements of this standard.~~

Safety systems should be as simple as possible; therefore, functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system. A safety system designed to perform functions not directly related to the safety function would be more complex than a system that performs the same safety function, but is not designed to perform other functions. The more