IEEE STANDARDS ASSOCIATION

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

IEEE Power and Energy Society

Sponsored by the
Nuclear Power Engineering Committee

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

IEEE Std 7-4.3.2™-2016
(Revision of IEEE Std 7-4.3.2-2010)

IEEE Std 7-4.3.2™-2016
(Revision of IEEE Std 7-4.3.2-2010)

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

Sponsor

Nuclear Power Engineering Committee
of the
IEEE Power and Energy Society

Approved 29 January 2016

IEEE-SA Standards Board

Abstract: Additional specific requirements to supplement the criteria and requirements of IEEE Std 603™ are specified for programmable digital devices. Within the context of this standard, the term programmable digital device is any device that relies on software instructions or programmable logic to accomplish a function. Examples include a computer, a programmable hardware device, or a device with firmware. Systems using these devices will also be referred to as digital safety systems in this standard. The criteria contained herein, in conjunction with criteria in IEEE Std 603, establish minimum functional and design requirements for programmable digital devices used as components of a safety system.

Keywords: commercial grade item, diversity, IEEE 7-4.3.2™, programmable digital devices, 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

PDF: ISBN 978-1-5044-0859-2 STD20898
Print: ISBN 978-1-5044-0860-8 STDPD20898

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading "Important Notice" or "Important Notices and Disclaimers Concerning IEEE Standards Documents."

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents (standards, recommended practices, and guides), both full-use and trial-use, are developed within IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association ("IEEE-SA") Standards Board. IEEE ("the Institute") develops its standards through a consensus development process, approved by the American National Standards Institute ("ANSI"), which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, 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.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. IEEE standards documents are supplied "AS IS" and "WITH ALL FAULTS."

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.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own 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.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of 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 of IEEE.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive 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 comments or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

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

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document 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

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted 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 these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Updating of IEEE Standards documents

Users of IEEE Standards documents 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.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, 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 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-SA Website at http://ieeexplore.ieee.org/Xplore/home.jsp or contact IEEE at the address listed previously. For more information about the IEEE SA or IEEE's standards development process, visit the IEEE-SA Website at http://standards.ieee.org.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE-SA Website at the following URL: http://standards.ieee.org/findstds/errata/index.html. Users are encouraged to check this URL for errata periodically.

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 by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE-SA Website at http://standards.ieee.org/about/sasb/patcom/patents.html. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. 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

At the time this standard was completed, the Subcommittee Working Group 6.4 had the following membership:

Warren Odess-Gillet, *Chair*

Akira Fukumoto
David Herrell
Ronald Jarret
Lee Meek
Kirklyn Melson
Ty Rogers
Richard Stattel
Masafumi Utsumi
Deanna Zhang

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

Satish K. Aggarwal
Angela Anuszewski
George Ballassi
Royce Beacom
Daniel Brosnan
Nissen Burstein
Robert Carruth
Suresh Channarasappa
Tom Crawford
Paul Croll
John Disosway
Neal Dowling
John Erinc
Stephen Fleger
James Gleason
Randall Groves
Ajit Gwal
Daryl Harmon
Hamidreza Heidarisafa
Raymond Herb
David Herrell
Werner Hoelzl
David Horvath
Greg Hostetter
Ronald Jarrett
Chad Kiger
G. Lang
William Lumpkins
John Macdonald
Michael May
Kirklyn Melson
Warren Odess-Gillett
Jan Pirrong
Bartien Sayogo
Raymond Senechal
John Vergis
Michael Waterman

When the IEEE-SA Standards Board approved this standard on 29 January 2016 it had the following membership:

Jean-Philippe Faure, *Chair*
Vacant Position, *Vice Chair*
John Kulick, *Past Chair*
Konstantinos Karachalios, *Secretary*

Chuck Adams
Masayuki Ariyoshi
Ted Burse
Stephen Dukes
Jianbin Fan
J. Travis Griffith
Gary Hoffman
Ronald W. Hotchkiss
Michael Janezik
Joseph L. Koepfinger*
Hung Ling
Kevin Lu
Annette D. Reilly
Gary Robinson
Mehmet Ulema
Yingli Wen
Howard Wolfman
Don Wright
Yu Yuan
Daidi Zhong

*Member Emeritus

Introduction

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

This standard evolved from IEEE Std 7-4.3.2-2010. It represents a continued effort by an IEEE working group to support the specification, design, and implementation of digital programmable devices in safety systems of nuclear power generating stations.

This standard specifies additional digital system requirements to supplement the criteria and requirements of IEEE Std 603™-2009.[1] This standard should be used in conjunction with IEEE Std 603-2009 for completeness of the safety system design when a programmable digital device is to be used for a safety system function.

This standard recognizes that development processes for programmable digital devices 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.

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™-2014 [B15].[2] The approach stated in 5.5 of IEEE Std 379-2014 is also appropriate for potential common-cause failures associated with programmable digital systems 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 digital systems is provided in 5.16 of this standard.

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.

— Changed title from computer to programmable digital devices to encompass technologies such as Field Programmable Gate Arrays (FPGAs).

— Enhanced draft standard to define unique requirements for programmable digital devices that are not computers.

— Provided more specific criteria on the use of software tools used for digital devices and development of hardware, software, firmware, and programmable logic (see 5.3.2).

— Updated 5.9 to define the criteria for a secure development environment.

— Moved simplicity discussion from 5.6 to 5.18.

— Updated Annex D, by restructuring the format so that it will be more useful also added an entire section to describe a process of performing hazard analysis activities in conjunction with software development processes.

— Added several clauses in areas where guidance was lacking and deleting portions considered un-useful or unproductive.

— Implemented editorial clarification changes throughout the standard.

[1]Information on references can be found in Clause 2.
[2]Numbers in brackets correspond with those of the bibliography in Annex H.

Contents

1. Scope 9

2. Normative references 9

3. Definitions, acronyms, and abbreviations 10
   3.1 Definitions 10
   3.2 Acronyms and abbreviations 13

4. Safety system design basis 14

5. Safety system criteria 14
   5.1 Single-failure criterion 14
   5.2 Completion of protective action 15
   5.3 Quality 15
   5.4 Equipment qualification 20
   5.5 System integrity 20
   5.6 Independence 22
   5.7 Capability for test and calibration 26
   5.8 Information displays 27
   5.9 Control of access 29
   5.10 Repair 35
   5.11 Identification 35
   5.12 Auxiliary features 35
   5.13 Multi-unit stations 35
   5.14 Human factors considerations 35
   5.15 Reliability 35
   5.16 Common cause failure criteria 35
   5.17 Use of commercial digital equipment 36
   5.18 Simplicity 43

6. Sense and command features—functional and design requirements 44

7. Execute features—functional and design requirements 44

8. Power source requirements 44

Annex A (informative) Mapping of IEEE Std 603-2009 to IEEE Std 7-4.3.2 45

Annex B (informative) Diversity requirements determination 47

Annex C (informative) Dedication of existing commercial computers 50

Annex D (informative) Identification and control of hazards 55

Annex E (informative) Communication independence 70

Annex F (informative) Computer reliability 77

Annex G (informative) Glossary 78

Annex H (informative) Bibliography 82

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

1. Scope

This standard serves to amplify criteria in IEEE Std 603™-2009, to address the use of programmable digital devices as part of safety systems in nuclear power generating stations.[3] The criteria contained herein, in conjunction with criteria in IEEE Std 603-2009, establish minimum functional and design requirements for programmable digital devices 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.

IEEE Std 323™-2003 (Reaff 2008), IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations.[4,5]

[3]Information on footnotes can be found in Clause 2.
[4]IEEE publications are available from The Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA (http://standardsieee.org/).
[5]The IEEE standards or products referred to in this clause are trademarks of The Institute of Electrical and Electronics Engineers, Inc.