

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 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

Copyright © 2016 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 25 August 2016. Printed in the United States of America.

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

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

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.

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 Ballasi
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 Heidarisa
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.

¹Information on references can be found in [Clause 2](#).

²Numbers 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

IMPORTANT NOTICE: IEEE Standards documents are not intended to ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

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™-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}

³Information on footnotes can be found in [Clause 2](#).

⁴IEEE publications are available from The Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA (<http://standards.ieee.org/>).

⁵The IEEE standards or products referred to in this clause are trademarks of The Institute of Electrical and Electronics Engineers, Inc.

IEEE Std 344™-2013, IEEE Standard for Seismic Qualification of Equipment for Nuclear Power Generating Stations.

IEEE Std 603™-2009, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.

IEEE Std 1012™-2012, IEEE Standard for System and Software Verification and Validation.

ISO/IEC 12207:2008 (IEEE Std 12207-2008), Second Edition, 2008-02-01, Systems and Software Engineering—Software life cycle processes.⁶

ISO/IEC 15288:2008 (Second Edition) (IEEE Std 15288-2008), Systems and Software Engineering—System Life Cycle Processes.

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.⁷

acceptance testing: **(A)** Formal testing conducted to determine whether a system satisfies its acceptance criteria and requirements; and to enable the customer to determine whether to accept the system. **(B)** Formal testing conducted to enable a user, customer, or other authorized entity to determine whether to accept a system or component.

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.

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.

⁶ISO/IEC publications are available from the ISO Central Secretariat, 1, ch. de la Voie-Creuse, CP 56, CH-1211 Geneva 20, Switzerland (<http://www.iso.org/>). ISO/IEC publications are available in the United States from the American National Standards Institute, 25 West 43rd Street, 4th Floor, New York, NY 10036, USA (<http://www.ansi.org/>).

⁷*IEEE Standards Dictionary Online* is available at: <http://ieeexplore.ieee.org/xpls/dictionary.jsp>.

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.

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.

configuration: (A) The arrangement of a digital safety 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.

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.

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.

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.

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.

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. (Adapted from EPRI NP-5652 [B3])

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. (Adapted from EPRI NP-5652 [B3])

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 licensee 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.

digital safety system: A collection of programmable digital devices performing safety functions.

digital security: Protection of digital 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.

engineering workstation: A 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. (Adapted from Adapted from the Instrument Engineer's Handbook, Fourth Edition, ed. by Béla Lipták [B36], and from US. CERT online document, Control Systems Security Program (CSS), Overview of Cyber Vulnerabilities [B37])

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. (Adapted from IEEE Std 323-2003)

firmware: The combination of a hardware device and computer instructions or computer data that reside as read-only software on the hardware device. For compliance with this standard, firmware shall be treated as software in a programmable device. (Adapted from IEEE Std 12207-2008)

functional states: Component or system operational states as defined by the programmable digital device (PDD) design including operational modes, fault tolerant modes, and test/diagnostic/fault detection modes.

hazard: **(A)** A condition that is a prerequisite to an undesirable behavior in a system. Hazards include external events as well as conditions internal to hardware or software. **(B)** An intrinsic property or condition that has the potential to cause harm or damage. (Adapted from IEEE Std 1012-2012) **(C)** A source of potential harm or a situation with a potential for harm in terms of human injury, damage to health, property, or the environment, or some combination of these. (Adapted from IEEE Std 1012-2012) **(D)** Any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment, or property; or damage to the environment. (Adapted from MIL-STD-882B [B23])

hazard analysis: A process of examining a system to identify inherent hazards and incorporating appropriate requirements, design, and other constraints to eliminate, prevent, or control the identified hazard.

hazard identification: The process of recognizing that a hazard exists and of defining its characteristics.

hazard and operability study (HAZOPS): concept of using teamwork, aided by a HAZOPS process expert, systematizing enquiry through keywords; systematizing understanding effects through understanding the associated deviations. (Adapted from USNRC Research Information Letter 1101 – USNRC ML14237A359 [B40])

programmable digital device: 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.

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

remote access: The ability to access a digital safety system, node, or network resource that performs a safety function or that can affect the safety function from a digital safety system or node that is located in an area with less physical security than the safety system (e.g., outside the protected area).

safe shutdown condition: Bringing the plant to those shutdown conditions specified in licensing basis documentation of the nuclear power generating station.

safe state: **(A)** A system state identified as safe by the context of its application. **(B)** A system condition consistent with the nuclear power plant safety analysis.

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).

secure development environment: The condition of having appropriate physical, logical and programmatic controls during the system development phases (i.e., concept, requirements, design, implementation, testing) to preclude introduction of unwanted, unneeded (i.e., not requirements driven), and undocumented functionality (e.g., superfluous code) into digital safety systems.

secure development and operational environment (SDOE): (A) Measures and controls taken to establish a secure environment for development of the digital safety system against undocumented, unneeded (i.e., not requirements driven), and unwanted modifications and (B) protective actions taken against a predictable set of undesirable acts (e.g., inadvertent operator actions or the undesirable behavior of connected systems) that could challenge the integrity, reliability, or functionality of a digital safety system during operations. These SDOE actions may include adoption of protective design features into the digital safety system design to preclude inadvertent access to the system and/or protection against undesirable behavior from connected systems when operational.

secure operational environment: The condition of having appropriate physical, logical and administrative controls within a facility to support the reliable operation of digital safety systems by precluding undesirable behavior of connected systems and events that might be initiated by inadvertent access to the system.

software: The programs used to direct operations of a programmable digital device. Examples include computer programs and logic for programmable hardware devices, and data pertaining to its operation.

software tools: A sequence of instructions and commands used in the design, development, testing, review, analysis, or maintenance of a programmable digital device or its documentation. Examples include compilers, assemblers, linkers, comparators, cross-reference generators, decompilers, editors, flow charters, monitors, test case generators, integrated development environments, and timing analyzers. (Adapted from IEEE Std 610™-1990 [B17])

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 health and safety following such failure, destruction, or release.

3.2 Acronyms and abbreviations

The following abbreviations and acronyms appear in this standard:

ATWS	anticipated transient without scram
CCF	common cause failure
CDR	critical digital review
COTS	commercial off-the-shelf
D3	diversity and defense in depth
DPRAM	dual-ported random access memory
EMC	Electromagnetic compatibility
ESF	Engineered Safety Features (see IEEE Std 603-2009)
FMEA	failure modes and effects analysis
FTA	fault tree analysis

HA	hazard analysis
HAZOPS	hazard and operability study
IEC	International Electrotechnical Commission
JTAG	Joint Test Action Group (IEEE Std 1149.1™-2013 [B39])
M&TE	measurement and test equipment
NEI	Nuclear Energy Institute
PDD	programmable digital device
PLC	programmable logic controller
QA	quality assurance
QFR	reinforced functional qualification (translated from the French)
SAR	Safety Analysis Report
SDOE	secure development and operational environment
SER	Safety Evaluation Report
SSC	structure, system, component
V&V	verification and validation

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](#). [Subclause 5.17](#) does not exist in IEEE Std 603-2009.

5.1 Single-failure criterion

In addition to the requirements in IEEE Std 603-2009, the following criteria apply for programmable digital devices in safety systems:

- a) Functions that are assumed to malfunction independently in the safety analysis shall not be affected by failure of a single programmable digital device (PDD).
- b) Functions shall be configured (e.g., functionally distributed) such that a single PDD 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 a single PDD malfunction or software error.

See [5.16](#) to address the possibility and consequences of malfunction of multiple PDDs as a result of common software error.

5.2 Completion of protective action

No requirements beyond IEEE Std 603-2009 are necessary.

5.3 Quality

General quality criteria are addressed in IEEE Std 603-2009. Software quality is addressed in ISO/IEC 12207:2008 (IEEE Std 12207-2008) and supporting standards. Guidance on system quality can be found in ISO/IEC 15288:2008 (IEEE Std 15288-2008). These same standards apply to PDDs. PDD development activities shall include the development of hardware and software. The integration of the hardware and software and the integration of the PDD into the safety system shall be addressed in the development process.

A typical system development process should consist of the following life cycle processes:

- a) Creating the conceptual design of the system
- b) Translation of the concepts into specific system requirements
- c) Using the requirements to develop a detailed system design
- d) Implementing the design into hardware and software functions
- e) Testing the functions to confirm that the requirements have been correctly implemented
- f) Installing the system and performing site acceptance testing
- g) Operating and maintaining the system
- h) Retiring the system

The following activities shall be performed in addition to the quality criteria provided by IEEE Std 603-2009:

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

5.3.1 Software development

Software shall be developed, modified, or accepted in accordance with 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 PDD 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 Ed. 2 (2006-05) [B13] and IEEE Std 730™-2002 [B18].

The software QA plan shall also address software tools used 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. Software quality metrics should be used to improve performance. The following life cycle phase characteristics should be considered:

- a) Correctness/Completeness (Requirements phase)
- b) Compliance with requirements (Design phase)
- c) Compliance with design (Implementation phase)
- d) Functional compliance with requirements (Test and Integration phase)
- e) On-site functional compliance with requirements (Installation and Checkout phase)
- f) 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 [B20] provides a methodology for the application of software quality metrics.

5.3.2 Software tools

When software tools are selected for use in a safety-related PDD development project, the benefits and risks associated with the tools use should be taken into consideration. The selected tools should limit the opportunity for making errors and introducing faults, while maximizing the opportunity for detecting faults in the resulting safety-related PDD.

There are several types of software tools that are commonly used throughout various phases of a digital safety system's development life cycle. Some tools are integral to the basic software development process while others are used in an indirect manner. It is therefore useful to categorize these tools into groupings based on the type of tool and the tasks the tool is performing. Identification of the tool outputs is also an important factor in determining the qualification level needed for any software tool. Once software tool categories are established, the tool limitations, usage, and qualification requirements can be determined to ensure proper application of each tool. The following software categorization scheme is presented as a means of identifying tool usage and outputs so that the subsequent criteria can be applied.

Type I – Software Development Tools –Type I tools are used by developers for the purpose of generating software, defining system architecture, or configuration data to be loaded into a PDD. Developers interface directly with software development tools using some sort of programming interface language such as C, C++, or by using a graphical interface such as drawing Function Block Diagrams. The development tool then converts this user input into a data form that can be loaded into a PDD. The output of a Type I tool is the object code or logic synthesis that will be executed within the target system hardware.

Type II – Surveillance and Maintenance Tools –Type II tools are those used for surveillance testing, changing configuration data, and/or loading software for safety systems. The output of a Type II tool may include safety system response to tool use and/or modified configuration of the safety system.

Type III – Development Process Support Tools –Type III tools are used in an off-line manner to support various development activities. These tools normally do not have any direct impact or interaction with the system or software development processes. As such, Type III tools normally do not have any capability for introducing errors into the safety PDD itself. Instead, Type III tools are used to create and maintain required documentation and configuration management aspects of the development process. The output of a Type III tool is documentation or specific file/data sets for the safety system. Type III tools can also be used to maintain configuration control over Type I, Type II, Type IV, and Type V tools.

Type IV – In-Line V&V Tools –Type IV tools receive input from the output of a Type I tool. The purpose of a Type IV tool is to perform or assist performance of a verification or validation activity. Type IV tools are often designed to make corrections to the safety system, either automatically, or manually as directed by the tool user based upon a pre-defined set of rules. The output of a Type IV tool is adjusted or modified software or system that has been corrected to meet the requirements programmed into the tool itself.

Type V – Off-Line V&V Tools –Type V tools receive input from the output of a Type I tool. Type V tools are similar to Type IV tools in that they are used to support V&V activities. However, they differ from Type IV tools in that they do not modify or manipulate the software or system that is being tested in a manner that could change or introduce errors into the safety system. Instead, Type V tools produce outputs in the form of test results which provide an operator with information needed to validate that the system is performing its required design functions. If a need for making corrections is identified, then this information is provided as feedback to the developer. The developer then uses the Type I tool in order to make necessary corrections and the V&V process is repeated in an iterative fashion until all requirements have been verified and validated.

If software tools are used during the life cycle process of safety-related PDD, 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 software tool shall be used in a manner such that defects not detected by the software tool will be detected by V&V activities.
- b) The tool shall be developed using a quality lifecycle process commensurate with the criticality of the safety functions performed by the end product.

The intended functionality and limitations of applicability for all software tools shall be identified and documented. The tools and their output shall not be used outside their documented functionality or limits of application without prior justification.

Software tools shall be assessed in a manner consistent with the category of tool, and the potential that the tool has to introduce faults into the safety-related PDD application.

The assessment process for software tools should take into account experience from prior use. The experience should include the experience of the developers as well as experience gained from the processes in which the tools are used.

Software tools used to support the software life cycle process of safety-related PDD shall be incorporated into the secure development and operational environment and controlled under configuration management. Only approved and documented software tools shall be used to support the development of safety-related PDD. The software tools shall be used within their design capabilities.

5.3.3 Verification and validation

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 shall be used to confirm that the development products of an activity conform to the requirements of that activity, and that the system performs according to its intended use and user needs. This determination of suitability shall include assessment, analysis, evaluation, review, inspection, and testing of products and processes.

This standard adopts the IEEE Std 1012-2012 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 hardware as it affects software and system, integration of the digital system components, and the interaction of the resulting PDD system with the nuclear power plant.

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

The V&V effort shall be performed in accordance with IEEE Std 1012-2012 for software V&V tasks. IEEE Std 1012 also addresses V&V activities for system and hardware. IEEE Std 1012 establishes an integrity level schema but states that other integrity schemas are acceptable. For any selected integrity schema, the selected integrity levels shall be mapped to the IEEE Std 1012's four-level schema to demonstrate that the minimum V&V requirements are satisfied. The safety system V&V plan shall define and justify the V&V integrity level applied to the system and the required documented outputs. See IEEE Std 1012-2012 for a definition of integrity level.

5.3.4 V&V independence requirements

Independent verification and validation is required for safety-related system. In order to have independent verification and validation, three different types of independence are required as follows:

- a) The verification and validation staff shall report to a separate organization with sufficient authority and organizational freedom, including sufficient independence from cost and schedule limitations, as defined in Annex C of IEEE Std 1012-2012.
- b) 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.
- c) The designers, people who contributed to the design, design and development project management, and staff supervising the designers shall not perform or oversee independent verification and validation on safety-related systems.

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.

IEEE Std 1012-2012 provides additional guidance.

5.3.5 Configuration management

Software configuration management shall be performed. IEEE Std 828™-2012 [B19] provides a standard for configuration management plans.

The minimum set of software activities shall address the following:

- a) Identification and control of all software designs and implementation
- b) Identification and control of all software design functional data (e.g., data templates and databases)
- 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 development activities for the supplied safety system software
- g) Control and retrieval of qualification information associated with software designs and implementation
- h) Software configuration audits
- i) Status accounting

Similar activities shall be performed for hardware and system configuration management.

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 system baseline shall be established at appropriate points in the development 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 system 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 system shall be formally documented and approved consistent with the system configuration management plan (see IEEE Std 828-2012 for criteria on change control and IEEE 1012-2012 for criteria on regression analysis and testing). The documentation revisions shall include the reason for the change. Additionally, the change control documentation shall identify the affected configuration item, and the impact of the change on the system including the hazards and risks analysis. The change control 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 life cycle activities such as V&V.

5.3.6 Project risk management

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 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. Project risks shall include technical, schedule, cost and resource-related risks that could compromise quality goals, and thereby affect the ability of the digital system or component to perform its safety-related functions. 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 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 PDD.
- b) Define and implement appropriate risk management strategies.
- c) Identify risks to the 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 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 PDD 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) and ISO/IEC 15288:2008 (IEEE Std 15288-2008).

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. The PDD functions necessary to perform safety functions and those PDD functions 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 logic, 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.

5.5 System integrity

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

- Design for PDD integrity
- Design for test and calibration
- Fault detection and self-diagnostics
- Prioritization of functions

5.5.1 Design for PDD integrity

The PDD shall be designed to perform its safety function when subjected to hazards, external or internal, that have significant potential for defeating the safety function. Such hazards 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 PDD shall not preclude the safety system from being placed in that mode. Performance of PDD restart operations shall not result in the safety system being inhibited from performing its function including causing a spurious safety system actuation.

A hazard analysis (see [Annex D](#) for guidance) shall be performed to identify and address potential hazards of the system.

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. The test and

calibration functions shall not affect system functions that are not included in a calibration change (e.g., set-point change).

V&V, configuration management, and QA shall be required for test and calibration functions on separate PDDs (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 PDD that is part of the safety system. The calibration shall be traceable to an appropriate national standard.

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

5.5.3 Fault detection and self-diagnostics

Self-diagnostics are a means to provide timely detection of failures. Self-diagnostics are not required for systems in which failures can be detected by alternate means in a timely manner. If self-diagnostic functions are integrated into the safety system, these functions shall be subject to the same V&V processes as the safety functions.

If reliability requirements warrant self-diagnostics, then PDD software shall incorporate functions to detect and report PDD system faults and failures in a timely manner. Self-diagnostic functions shall not adversely affect the ability of the PDD 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 instruction set tests (e.g., calculation tests)
- PDD peripheral hardware tests (e.g., watchdog timer and keyboard tests)
- PDD architecture support hardware tests (e.g., address lines and shared memory interfaces)
- Communication link diagnostics (e.g., cyclic redundancy checks)
- Internal signal monitoring (e.g., JTAG)

Communication link failures that do not result in a system failure or a lack of system functionality shall be identified for licensee 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:

- Self-diagnostics during PDD system startup
- Periodic self-diagnostics while the PDD system is operating
- 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, control systems (e.g., feed-water control system), diverse actuation systems, etc. The following criteria shall apply to priority functions:

- a) A priority function shall be a safety-related function.
- b) The priority function used for a diverse actuation signal shall be independent of any postulated CCF of the remainder of the digital system, and shall function properly regardless of the state or condition of the digital system.
- c) When signals that originate from the safety system are combined with diverse actuation signals or non-safety control signals, priority shall be given to the signal that corresponds with the predetermined safe state of the controlled device(s) such 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 feed-water control 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 PDD 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.
- g) 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.
- h) 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.

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 PDD systems, software performing safety functions and software performing non-safety functions may reside on the same PDD and use the same PDD resources. The non-safety software functions shall be developed in accordance with the safety-related requirements of this standard.

The safety function of each safety channel shall be protected from adverse influence from outside the division of which that channel is a member. Information and signals originating outside the division shall not be able to inhibit or delay the safety function of that division. This protection shall be implemented within the affected division (rather than in the sources outside the division), and shall not itself be affected by any condition or information from outside the affected division. This protection shall be sustained despite any operation, mal-

function, design error, communication error, or software error or corruption existing or originating outside the division.

For legacy reactor protection and ESF systems with only two divisions, each division consisting of redundant channels, each of those channels is required to be capable of generating a single protective action signal regardless of the determination reached by other channels. Communications between those redundant channels shall be restricted in the same manner as described for inter-divisional communication in this standard.

Safety systems shall be designed such that no input from non-safety systems is required for the system to perform its safety functions. Data input (e.g., setpoints and scaling) from a non-safety system that receives verification equivalent to the quality of the safety system such as independent reviews and configuration controls is acceptable for use in a safety system (see 5.6.4.3 for detail criteria).

5.6.1 Between redundant portions of a safety system

See 5.6.4 for additional detailed criteria.

5.6.2 Between safety systems and effects of design basis event

No requirements beyond IEEE Std 603-2009 are necessary.

5.6.3 Between safety systems and other systems

See 5.6.4 and 5.9.3 for additional detailed criteria.

5.6.3.1 Interconnected equipment

See 5.6.4 for additional detailed criteria.

5.6.3.2 Equipment in proximity

No requirements beyond IEEE Std 603-2009 are necessary.

5.6.3.3 Effects of a single random failure

No requirements beyond IEEE Std 603-2009 are necessary.

5.6.4 Detailed criteria

5.6.4.1 Buffering function/circuit

A buffering function provides an interface between the communications link and the safety function. The primary function of the buffering function is to prevent faults and failures on the communication originating outside the safety division from propagating to the safety function within the division, maintaining the integrity of the safety function. See Annex E for guidance on communication function/buffers to meet this criteria. The following criteria shall be applied to the buffering function:

- a) The buffering function shall consist of two different circuits, one performing the safety function and one performing the data communication function. The buffering circuit shall be accessible from the PDD performing the safety function.
- b) The buffering function can be provided by a separate communications processor or separate logic within a PDD. The buffering function can be on the same printed circuit board or on a separate printed circuit board.
- c) The safety function processor shall operate asynchronously from the communication processor. A non-processor PDD shall have separate logic circuits for the safety function and the communication

function. The safety function requirements shall be clearly defined for the case where the data expected from the communication function is faulted (e.g., increased data rate to the buffer, data is not available or is old, corrupt data).

- d) Communications between safety and communication functions shall use a buffer function that is dedicated exclusively to this exchange of information (e.g., dual-ported memory). The safety function, the communications function, and the buffering function, along with all supporting hardware and software, are all considered to be safety-related, and shall be designed, qualified, fabricated, etc. accordingly.
- e) The safety function shall have priority access to the buffer function to complete the safety function in a deterministic manner. Buffer function faults shall not prevent the safety function from executing within the established timeframe.
- f) The cycle time for the safety function processor shall be determined in consideration of the longest possible completion time for each access to the shared memory. This longest-possible completion time shall include the time of the memory itself and of the circuits associated with it, and shall also include the longest possible delay in access to the memory by the function processor, assuming worst-case conditions for the transfer of access from the communications processor to the function processor. Failure of the system to meet the limiting cycle time shall be detected and alarmed.
- g) If the buffering function provides data used in a safety function, the buffering function shall be built to the same V&V used for the safety functions. Otherwise, a graded V&V approach as defined in IEEE Std 1012-2012 may be used based upon required integrity level.
- h) The electrical isolation, separation and single failure requirements of IEEE Std 603-2009 apply to the communication links between safety and non-safety systems, and between divisions in a safety system.

5.6.4.2 Communications independence

A safety channel shall not receive any communication from outside its own safety division unless that communication supports the performance of the safety function. Receipt of information that does not support the safety function would involve the performance of functions that are not directly related to the safety function.

The following criteria apply to digital communications between redundant safety divisions and between safety and non-safety systems:

- a) A processor performing the safety function shall perform no communication handshaking or communication interrupts. If required, handshaking and interrupt functions shall be performed in a separate communications processor. A non-processor shall have separate logic circuits implementing communication and safety functions.
- b) Only predefined data sets shall be processed by the receiving safety system (i.e., the message format and protocol is pre-determined, that is, the same information is found in each section of every message). Unrecognized data shall be identified and processed by the receiving system in accordance with the defined design requirements.
- c) Within the PDD system performing the safety function, the data received and data transmitted is stored in separate, pre-determined locations. The pre-determined memory locations are used only for data receipt or transmission.
- d) All external signals shall be treated as data to be processed in accordance with the operational safety logic in the normal sequencing of that logic. Commands that could alter the safety logic or logic sequencing are not allowed.
- e) Safety division software shall be protected from alteration while the safety division is in operation. Hardwired interlocks or physical disconnection of incoming data transmission from the maintenance/

monitoring equipment is a preferred method for changes to safety system software to control these changes.

- f) Addressable constants, setpoints, parameters, and other settings associated with a safety function shall only be modified when the channel is bypassed or not in service.
- g) A tool deployed to make such modifications shall be physically restricted from making changes in more than one division at a time.
- h) The safety system shall be designed to protect channels still in operation from modification when a tool is connected to change parameters for another channel that is in bypass or out of service. This protection shall be safety-related.
- i) Credible communication faults shall not prevent performance of required safety functions. It shall be assumed that non-safety systems will have multiple and continual failures. The minimum lists of credible faults that shall be considered include the following:⁸
 - 1) Messages may be corrupted due to errors in communications processors, errors introduced in buffer interfaces, introduced in the transmission media, or from interference.
 - 2) Messages may be repeated at an incorrect point in time.
 - 3) Messages may be sent in the incorrect sequence.
 - 4) Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message.
 - 5) Messages may be delayed beyond their permitted arrival time window, including errors in the transmission medium, congested transmission lines, interference, or by delay in sending buffered messages.
 - 6) Messages may be inserted into the communication medium, from unexpected or unknown sources.
 - 7) Messages may masquerade as valid messages from an expected source, which includes intentional events (see 5.9 for protection from this condition).
 - 8) Messages may be sent to the wrong destination, which could treat the message as a valid message.
 - 9) Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption.
 - 10) Messages may contain data that is outside the expected range.
 - 11) Messages may appear valid, but data may be placed in incorrect locations within the message.
 - 12) Messages may occur at a high rate that degrades or causes the system to fail (i.e., broadcast storm).
 - 13) Message headers or addresses may be corrupted.
 - 14) Message reception when the safety system is not in the correct mode to process it.
- j) Communications that are needed to support a safety function, such as the sharing of channel trip decisions for the purpose of voting, shall include provisions for ensuring that received messages are correct and are correctly understood. Such communications should employ error-detecting coding along with means for dealing with corrupt, invalid, untimely or otherwise questionable data. The effectiveness of error detection should be demonstrated in the design and proof testing of the associated codes, but once demonstrated is not subject to periodic testing.

⁸Most of the listed credible faults originate from IEC 61784-3 [B14].