



May 24, 2011
NRC:11:048

Document Control Desk
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555-0001

**Request for Alternatives to IEEE Std 603-1991 to Satisfy 10 CFR 50.55a(h)(3) Requirements –
U.S. EPR Design Certification**

Ref. 1: Letter, Sandra M. Sloan (AREVA NP Inc.) to Document Control Desk (NRC), "Conversion of ANP-10281P, "U.S. EPR Digital Protection System Topical Report" to ANP-10309P, "U.S. EPR Digital Protection System Technical Report" NRC:09:119, November 24, 2009.

Ref. 2: Letter, Sandra M. Sloan (AREVA NP Inc.) to Document Control Desk (NRC), " ANP-10309P, "U.S. EPR Digital Protection System Technical Report, Revision 1" NRC:11:022, March 15, 2011.

Ref. 3: Letter, Sandra M. Sloan (AREVA NP Inc.) to Document Control Desk (NRC), "Schedule for Alternative Request Associated with Closure Plan for U.S. EPR Instrumentation and Control Communications Independence Issues," NRC:11:036, April 14, 2011.

Pursuant to 10 CFR 50.55a(a)(3)(i) AREVA NP Inc. (AREVA NP) requests NRC approval to use alternatives to IEEE Std 603-1991 to satisfy the requirement of 10 CFR 50.55a(h)(3) for the U.S. EPR Design Certification. Two alternatives are requested from this code. First, with regard to safety related I&C and electrical systems described in the U.S. EPR Final Safety Analysis Report (FSAR), AREVA NP requests the use of IEEE Std 603-1998 in lieu of IEEE Std 603-1991. This request was originally submitted in Reference 1 and was removed in Reference 2 in order to include it in this submittal. The basis for this alternative and a comparison of the two standards is provided in Attachment 1. Second, as proposed in Reference 3, with regard to the self-powered neutron detector (SPND)-based reactor trip functions, AREVA NP requests the use of a conservative setpoint selection method to satisfy single failure requirements as an alternative to independence between redundant divisions required by IEEE Std 603-1991 Clause 5.6.1. The basis and technical justification for this alternative is provided in Attachment 2. In accordance with 10 CFR 50.55a(a)(3)(i), AREVA NP believes that these proposed alternatives provide an acceptable level of quality and safety.

AREVA NP requests approval of these alternative requests as part of the NRC staff's safety evaluation report for the U.S. EPR FSAR and supporting licensing documentation.

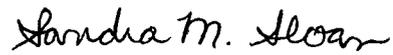
DOTT
MRO

AREVA INC.

3315 Old Forest Road, P.O. Box 10935, Lynchburg, VA 24506-0935
Tel.: 434 832 3000 www.aveva.com

Should you have any questions regarding this matter, please contact me by telephone at 434-832-2369, or by email at sandra.sloan@areva.com.

Sincerely,



Sandra M. Sloan
Regulatory Affairs Manager, New Plants
AREVA NP Inc.

Attachments (2)

cc: G. Tesfaye
Docket No. 52-020

Attachment 1 to NRC:11:048
U.S. EPR Design Certification
Proposed Alternative
in Accordance with 10 CFR 50.55a(a)(3)(i)

Use of IEEE Std. 603-1998 in Lieu of IEEE Std. 603-1991

**Proposed Alternative
in Accordance with 10 CFR 50.55a(3)(i)**

Use of IEEE Std. 603-1998 in Lieu of IEEE Std. 603-1991

SYSTEMS/COMPONENTS AFFECTED

Safety related I&C and electrical systems described in the U.S. EPR FSAR.

APPLICABLE CODE REQUIREMENT

IEEE Std. 603–1991 and the correction sheet dated January 30, 1995 is incorporated by reference in 10 CFR 50.55a(h) for applicability to the safety systems of design certifications and combined licenses issued under 10CFR 52.

REASON FOR REQUEST

Use of IEEE Std 603-1998 in lieu of IEEE Std 603-1991 provides additional criteria and consistency with other IEEE standards appropriate to the design of digital instrumentation and controls systems.

PROPOSED ALTERNATIVE AND BASIS FOR USE

Pursuant to 10 CFR 50.55a(3)(i), AREVA NP requests NRC approval to use IEEE Std 603-1998 in lieu of IEEE Std 603-1991 to satisfy the requirement of 10 CFR 50.55a(h)(3) for the U.S. EPR safety related I&C and electrical systems.

10 CFR 50.55a(h) requires protection and safety systems to meet the guidance of IEEE Std 603-1991. This standard is also endorsed by Regulatory Guide 1.153. The 1991 version of this IEEE standard has been upgraded to IEEE Std 603-1998. The stated purpose of this revision is to “clarify the application of this standard to computer-based safety systems and to advanced nuclear power generating station designs.” The U.S. EPR is an advanced nuclear reactor design and utilizes computer based safety systems; it is therefore appropriate to apply the requirements of IEEE Std. 603-1998 to the U.S. EPR design. Furthermore, Regulatory Guide (RG) 1.152, Revision 2, which endorses IEEE Std. 7-4.3.2-2003, makes numerous references to the 1998 version of IEEE Std. 603. For example, RG 1.152 endorses Annex A of IEEE 7-4.3.2-2003 which provides a mapping of IEEE Std. 603-1998 to IEEE Std. 7-4.3.2-2003.

Additionally, NUREG-0800 Appendix 7.1-D, “Guidance for the Evaluation of the Application of IEEE Std. 7-4.3.2” indicates the acceptability of use of criteria from IEEE Std. 603-1998:

“IEEE Std 603-1998, was evolved from IEEE Std 603-1991. The 1998 version of IEEE Std 603, was revised to clarify the application of the standard to computer-based safety systems and to advanced nuclear power generating station designs. IEEE Std. 603-1998 provides criteria for the treatment of electromagnetic and radio frequency interferences (EMI/RFI) and includes common-cause failure of digital computers in the single failure criterion. However, IEEE Std 603-1998 has neither been incorporated into the regulations nor endorsed by a

regulatory guide. Therefore, the use of criteria from IEEE Std 603-1998 by licensees and applicants may be acceptable, if appropriately justified, consistent with current regulatory practice.”

A technical comparison of IEEE Std. 603-1991 to IEEE Std. 603-1998 illustrates that the requirements contained in IEEE Std. 603-1998 meet or exceed the requirements contained in the 1991 version. Based on this comparison, the use of IEEE Std. 603-1998 as an alternative to IEEE Std. 603-1991 for the U. S. EPR FSAR provides an acceptable level of quality and safety. The comparison of the two versions of IEEE Std. 603 is provided in Table 1.

Table 1: Comparison of IEEE Std. 603-1991 to IEEE Std. 603-1998

IEEE 603-1991	IEEE 603-1998	Comment
<p>2. Definitions detectable failures. Failures that can be identified through periodic testing or can be revealed by alarm or anomalous indication. Component failures that are detected at the channel, division, or system level are detectable failures. NOTE: Identifiable, but nondetectable failures are failures identified by analysis that cannot be detected through periodic testing or cannot be revealed by alarm or anomalous indication. Refer to IEEE Std 379-1988.</p>	<p>3. Definitions 3.13 detectable failures. Failures that can be identified through periodic testing or can be revealed by alarm or anomalous indication. Component failures that are detected at the channel, division, or system level are detectable failures. NOTE-Identifiable, but nondetectable, failures are failures identified by analysis that cannot be detected through periodic testing or cannot be revealed by alarm or anomalous indication. Refer to IEEE Std 379-1994.</p>	<p>Only definitions with differences are listed. Regulatory Guide (RG) 1.53 Rev. 2 now endorses IEEE Std. 379-2000.</p>
<p>division. The designation applied to a given system or set of components that enables the establishment and maintenance of physical, electrical, and functional independence from other redundant sets of components.</p>	<p>3.14 division. The designation applied to a given system or set of components that enables the establishment and maintenance of physical, electrical, and functional independence from other redundant sets of components. NOTE - A division can have one or more channels.</p>	<p>Makes allowance for interchannel communication, used in some digital applications.</p>
<p>NOTE: The electrical portion of the safety systems, that perform safety functions, is classified as Class 1E.</p>	<p>NOTES: 1 -The electrical portion of the safety systems, that perform safety functions, is classified as Class 1E. 2-This definition of "safety system" agrees with the definition of "safety-related systems" used by the American Nuclear Society (ANS) and IEC 60231A.</p>	<p>Note 2 adds clarification on definition that has no impact on requirements.</p>

IEEE 603-1991	IEEE 603-1998	Comment
<p>4. Safety System Designation A specific basis shall be established for the design of each safety system of the nuclear power generating station. The design basis shall also be available as needed to facilitate the determination of the adequacy of the safety system, including design changes. The design basis shall be consistent with the requirements of ANSI/ANS 51.1-1983 or ANSI/ANS 52.1-1983 and shall document as a minimum:</p>	<p>4. Safety system design basis A specific basis shall be established for the design of each safety system of the nuclear power generating station. The design basis shall also be available as needed to facilitate the determination of the adequacy of the safety system, including design changes. The design basis shall be consistent with the requirements of ANSI/ANS 51.1-1983 or ANSI/ANS 52.1-1983 and shall document as a minimum:</p>	<p>No difference.</p>
<p>4.1 The design basis events applicable to each mode of operation of the generating station along with the initial conditions and allowable limits of plant conditions for each such event.</p>	<p>a) The design basis events applicable to each mode of operation of the generating station along with the initial conditions and allowable limits of plant conditions for each such event.</p>	<p>No difference.</p>
<p>4.2 The safety functions and corresponding protective actions of the execute features for each design basis event.</p>	<p>b) The safety functions and corresponding protective actions of the execute features for each design basis event.</p>	<p>No difference.</p>
<p>4.3 The permissive conditions for each operating bypass capability that is to be provided.</p>	<p>c) The permissive conditions for each operating bypass capability that is to be provided.</p>	<p>No difference.</p>
<p>4.4 The variables or combinations of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action; the analytical limit associated with each variable, the ranges (normal, abnormal, and accident conditions); and the rates of change of these variables to be accommodated until proper completion of the protective action is ensured.</p>	<p>d) The variables or combinations of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action; the analytical limit associated with each variable, the ranges (normal, abnormal, and accident conditions); and the rates of change of these variables to be accommodated until proper completion of the protective action is ensured.</p>	<p>No difference.</p>

IEEE 603-1991	IEEE 603-1998	Comment
4.5 The following minimum criteria for each action identified in 4.2 whose operation may be controlled by manual means initially or subsequent to initiation. See IEEE Std 494-1974.	e) The protective actions identified in item b) that may be controlled by manual means initially or subsequently to initiation. See IEEE Std 497-1981. The proactive actions are as follows:	RG 1.97 Rev. 4 now endorses IEEE Std. 497-2002.
4.5.1 The points in time and the plant conditions during which manual control is allowed.	1) The points in time and the plant conditions during which manual control is allowed.	No difference.
4.5.2 The justification for permitting initiation or control subsequent to initiation solely by manual means.	2) The justification for permitting initiation or control subsequent to initiation solely by manual means.	No difference.
4.5.3 The range of environmental conditions imposed upon the operator during normal, abnormal, and accident circumstances throughout which the manual operations shall be performed.	3) The range of environmental conditions imposed upon the operator during normal, abnormal, and accident conditions throughout which the manual operations shall be performed.	No difference.
4.5.4 The variables in 4.4 that shall be displayed for the operator to use in taking manual action.	4) The variables in item d) that shall be displayed for the operator to use in taking manual action.	No difference.
4.6 For those variables in 4.4 that have a spatial dependence (that is, where the variable varies as a function of position in a particular region), the minimum number and locations of sensors required for protective purposes.	f) For those variables in item d) that have a spatial dependence (i.e., where the variable varies as a function of position in a particular region), the minimum number and locations of sensors required for protective purposes.	No difference.
4.7 The range of transient and steady-state conditions of both motive and control power and the environment (for example, voltage, frequency, radiation, temperature, humidity, pressure, and vibration) during normal, abnormal, and accident circumstances throughout which the safety system shall perform.	g) The range of transient and steady-state conditions of both motive and control power and the environment (e.g., voltage, frequency, radiation, temperature, humidity, pressure, vibration, and electromagnetic interference) during normal, abnormal, and accident conditions throughout which the safety system shall perform.	No difference.

IEEE 603-1991	IEEE 603-1998	Comment
4.8 The conditions having the potential for functional degradation of safety system performance and for which provisions shall be incorporated to retain the capability for performing the safety functions (for example, missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non-safety-related systems).	h) The conditions having the potential for functional degradation of safety system performance and for which provisions shall be incorporated to retain the capability for performing the safety functions (e.g., missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non-safety-related systems).	No difference.
4.9 The methods to be used to determine that the reliability of the safety system design is appropriate for each safety system design and any qualitative or quantitative reliability goals that may be imposed on the system design.	i) The methods to be used to determine that the reliability of the safety system design is appropriate for each safety system design and any qualitative or quantitative reliability goals that may be imposed on the system design	No difference.
4.10 The critical points in time or the plant conditions, after the onset of a design basis event, including:	j) The critical points in time or the plant conditions, after the onset of a design basis event, including:	No difference.
4.10.1 The point in time or plant conditions for which the protective actions of the safety system shall be initiated.	1) The point in time or plant conditions for which the protective actions of the safety system shall be initiated.	No difference.
4.10.2 The point in time or plant conditions that define the proper completion of the safety function.	2) The point in time or plant conditions that define the proper completion of the safety function.	No difference.
4.10.3 The points in time or the plant conditions that require automatic control of protective actions.	3) The point in time or the plant conditions that require automatic control of protective actions.	No difference.
4.10.4 The point in time or the plant conditions that allow returning a safety system to normal.	4) The point in time or the plant conditions that allow returning a safety system to normal.	No difference.
4.11 The equipment protective provisions that prevent the safety systems from accomplishing their safety functions.	k) The equipment protective provisions that prevent the safety systems from accomplishing their safety functions.	No difference.

IEEE 603-1991	IEEE 603-1998	Comment
4.12 Any other special design basis that may be imposed on the system design (example: diversity, interlocks, regulatory agency criteria).	l) Any other special design basis that may be imposed on the system design (e.g., diversity, interlocks, regulatory agency criteria).	No difference.
5. Safety System Criteria The safety systems shall, with precision and reliability, maintain plant parameters within acceptable limits established for each design basis event. The power, instrumentation, and control portions of each safety system shall be comprised of more than one safety group of which any one safety group can accomplish the safety function. (See Appendix A for an illustrative example.)	5. Safety system criteria The safety systems shall, with precision and reliability, maintain plant parameters within acceptable limits established for each design basis event. The power, instrumentation, and control portions of each safety system shall be comprised of more than one safety group of which any one safety group can accomplish the safety function. (See Annex A for an illustrative example.)	No difference.
5.1 Single-Failure Criterion. The safety systems shall perform all safety functions required for a design basis event in the presence of:	5.1 Single-failure criterion. The safety systems shall perform all safety functions required for a design basis event in the presence of	No difference.
(1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures;	a) Any single detectable failure within the safety systems concurrent with all identifiable but nondetectable failures.	No difference.
(2) all failures caused by the single failure; and	b) All failures caused by the single failure.	No difference.
(3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions.	c) All failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions.	No difference.

IEEE 603-1991	IEEE 603-1998	Comment
<p>The single-failure criterion applies to the safety systems whether control is by automatic or manual means. IEEE Std 379-1988 provides guidance on the application of the single-failure criterion.</p>	<p>The single failure could occur prior to, or at any time during, the design basis event for which the safety system is required to function. The single-failure criterion applies to the safety systems whether control is by automatic or manual means. IEEE Std 379-1994 provides guidance on the application of the single-failure criterion. IEEE Std 7-4.3.2-1993 addresses common cause failures for digital computers.</p>	<p>The additional clarification on single failure does not affect requirements.</p> <p>RG 1.53 Rev. 2 now endorses IEEE Std. 379-2000.</p> <p>Added reference to IEEE Std. 7-4.3.2, which addresses digital I&C applications. RG 1.1.52 Rev. 2 now endorses IEEE Std.7-4.3.2-2003.</p>

IEEE 603-1991	IEEE 603-1998	Comment
<p>This criterion does not invoke coincidence (or multiple-channel) logic within a safety group; however, the application of coincidence logic may evolve from other criteria or considerations to maximize plant availability or reliability. An evaluation has been performed and documented in other standards to show that certain fluid system failures need not be considered in the application of this criterion. The performance of a probable assessment of the safety systems may be used to demonstrate that certain postulated failures need not be considered in the application of the criterion. A probable assessment is intended to eliminate consideration of events and failures that are not credible; it shall not be used in lieu of the single-failure criterion, IEEE Std 352-1987 and IEEE Std 577-1976 provide guidance for reliability analysis.</p>	<p>This criterion does not invoke coincidence (or multiple-channel) logic within a safety group; however, the application of coincidence logic may evolve from other criteria or considerations to maximize plant availability or reliability. An evaluation has been performed and documented in other standards to show that certain fluid system failures need not be considered in the application of this criterion. The performance of a probabilistic assessment of the safety systems may be used to demonstrate that certain postulated failures need not be considered in the application of the criterion. A probabilistic assessment is intended to eliminate consideration of events and failures that are not credible; it shall not be used in lieu of the single-failure criterion. IEEE Std 352-1987 and IEEE Std 577-1976 provide guidance for reliability analysis.</p>	<p>No difference.</p>
<p>Where reasonable indication exists that a design that meets the single-failure criterion may not satisfy all the reliability requirements specified in 4.9 of the design basis, a probable assessment of the safety system shall be performed. The assessment shall not be limited to single failures. If the assessment shows that the design basis requirements are not met, design features shall be provided or corrective modifications shall be made to ensure that the system meets the specified reliability requirements.</p>	<p>Where reasonable indication exists that a design that meets the single-failure criterion may not satisfy all the reliability requirements specified in Clause 4, item i) of the design basis, a probabilistic assessment of the safety system shall be performed. The assessment shall not be limited to single failures. If the assessment shows that the design basis requirements are not met, design features shall be provided or corrective modifications shall be made to ensure that the system meets the specified reliability requirements.</p>	<p>No difference.</p>

IEEE 603-1991	IEEE 603-1998	Comment
<p>5.2 Completion of Protective Action. The safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion. Deliberate operator action shall be required to return the safety systems to normal, This requirement shall not preclude the use of equipment protective devices identified in 4.11 of the design basis or the provision for deliberate operator interventions. Seal-in of individual channels is not required.</p>	<p>5.2 Completion of protective action. The safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion. Deliberate operator action shall be required to return the safety systems to normal. This requirement shall not preclude the use of equipment protective devices identified in Clause 4, item k) of the design basis or the provision for deliberate operator interventions. Seal-in of individual channels is not required.</p>	<p>No difference.</p>
<p>5.3 Quality. Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program (ANSI/ASME NQA1-1989).</p>	<p>5.3 Quality. Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program (See ASME NQA-1-1994).</p>	<p>Updates quality assurance guidance reference. No impact on digital I&C requirements.</p>
<p>(Not included in IEEE Std. 603-1991)</p>	<p>Guidance on the application of this criteria for safety system equipment employing digital computers and programs or firmware is found in IEEE Std 74.3.2-1993.</p>	<p>Added reference to IEEE Std. 7-4.3.2, which addresses digital I&C applications. RG 1.1.52 Rev. 2 now endorses IEEE Std. 7-4.3.2-2003.</p>

IEEE 603-1991	IEEE 603-1998	Comment
<p>5.4 Equipment Qualification, Safety system equipment shall be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting, on a continuing basis, the performance requirements as specified in the design basis. Qualification of Class 1E equipment shall be in accordance with the requirements of IEEE Std 323-1983 and IEEE Std 627-1980.</p>	<p>5.4 Equipment qualification. Safety system equipment shall be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting, on a continuing basis, the performance requirements as specified in the design basis. Qualification of Class 1E equipment shall be in accordance with the requirements of IEEE Std 323-1983 and IEEE Std 627-1980.</p>	<p>No difference.</p>
<p>(Not included in IEEE Std. 603-1991)</p>	<p>Guidance on the application of this criteria for safety system equipment employing digital computers and programs or firmware is found in IEEE Std 74.3.2-1993.</p>	<p>Added reference to IEEE Std. 7-4.3.2, which addresses digital I&C applications. RG 1.1.52 Rev. 2 now endorses IEEE Std. 7-4.3.2-2003.</p>
<p>5.5 System Integrity. The safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis.</p>	<p>5.5 System integrity. The safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis.</p>	<p>No difference.</p>
<p>(Not included in IEEE Std. 603-1991)</p>	<p>Guidance on the application of this criteria for safety system equipment employing digital computers and programs or firmware is found in IEEE Std 74.3.2-1993.</p>	<p>Added reference to IEEE Std. 7-4.3.2, which addresses digital I&C applications. RG 1.1.52 Rev. 2 now endorses IEEE STd. 7-4.3.2-2003.</p>
<p>5.6 Independence 5.6.1 Between Redundant Portions of a Safety System. Redundant portions of a safety system provided for a safety function shall be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring, that' safety function.</p>	<p>5.6 Independence 5.6.1 Between redundant portions of a safety system. Redundant portions of a safety system provided for a safety function shall be independent of, and physically separated from, each other to the degree necessary to retain the capability of accomplishing the safety function during and following any design basis event requiring that safety function.</p>	<p>No difference.</p>

IEEE 603-1991	IEEE 603-1998	Comment
<p>5.6.2 Between Safety Systems and Effects of Design Basis Event. Safety system equipment required to mitigate the consequences of a specific design basis event shall be independent of, and physically separated from, the effects of the design basis event to the degree necessary to retain the capability to meet the requirements of this standard. Equipment qualification in accordance with 5.4 is one method that can be used to meet this requirement.</p>	<p>5.6.2 Between safety systems and effects of design basis event. Safety system equipment required to mitigate the consequences of a specific design basis event shall be independent of, and physically separated from, the effects of the design basis event to the degree necessary to retain the capability of meeting the requirements of this standard. Equipment qualification in accordance with 5.4 is one method that can be used to meet this requirement.</p>	<p>No difference.</p>
<p>5.6.3 Between Safety Systems and Other Systems. safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard.</p>	<p>5.6.3 Between safety systems and other systems. The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in Clause 4, item h) of the design basis, shall not prevent the safety systems from meeting the requirements of this standard.</p>	<p>No difference.</p>
<p>5.6.3.1 Interconnected Equipment (1) Classification: Equipment that is used for both safety and nonsafety functions shall be classified as part of the safety systems, Isolation devices used to effect a safety system boundary shall be classified as part of the safety system.</p>	<p>5.6.3.1 Interconnected equipment a) Classification. Equipment that is used for both safety and nonsafety functions shall be classified as part of the safety systems. Isolation devices used to effect a safety system boundary shall be classified as part of the safety system.</p>	<p>No difference.</p>
<p>(2) Isolation: No credible failure on the non-safety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance requirements during and following any design basis event requiring that safety function. A failure in an isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system.</p>	<p>b) Isolation. No credible failure on the non-safety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance requirements during and following any design basis event requiring that safety function. A failure in an isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system.</p>	<p>No difference.</p>

IEEE 603-1991	IEEE 603-1998	Comment
<p>5.6.3.2 Equipment in Proximity (1) Separation: Equipment in other systems that is in physical proximity to safety system equipment, but that is neither an associated circuit nor another Class 1E circuit, shall be physically separated from the safety system equipment to the degree necessary to retain the safety systems' capability to accomplish their safety functions in the event of the failure of non-safety equipment. Physical separation may be achieved by physical barriers or acceptable separation distance. The separation of Class 1E equipment shall be in accordance with the requirements of IEEE Std 384-1981.</p>	<p>5.6.3.2 Equipment in proximity a) <i>Separation</i>. Equipment in other systems that is in physical proximity to safety system equipment, but that is neither an associated circuit nor another Class 1E circuit, shall be physically separated from the safety system equipment to the degree necessary to retain the safety systems' capability to accomplish their safety functions in the event of the failure of non-safety equipment. Physical separation may be achieved by physical barriers or acceptable separation distance. The separation of Class 1E equipment shall be in accordance with the requirements of IEEE Std 384-1992.</p>	<p>RG 1.75 Rev. 3 now endorses IEEE Std. 384-1992.</p>
<p>(2) Barriers: Physical barriers used to effect a safety system boundary shall meet the requirements of 5.3, 5.4 and 5.5 for the applicable conditions specified in 4.7 and 4.8 of the design basis.</p>	<p>b) <i>Barrier</i>. Physical barriers used to effect a safety system boundary shall meet the requirements of 5.3, 5.4 and 5.5 for the applicable conditions specified in Clause 4, items g) and h) of the design basis.</p>	<p>No difference.</p>
<p>5.6.3.3 Effects of a Single Random Failure. Where a single random failure in a nonsafety system can (1) result in a design basis event, and (2) also prevent proper action of a portion of the safety system designed to protect against that event, the remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate single failure. See IEEE Std 379-1988 for the application of this requirement.</p>	<p>5.6.3.3 Effects of a single random failure. Where a single random failure in a nonsafety system can result in a design basis event, and also prevent proper action of a portion of the safety system designed to protect against that event, the remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate single failure. See IEEE Std 379-1994 for the application of this requirement.</p>	<p>RG 1.53 Rev. 2 now endorses IEEE Std. 379-2000.</p>
<p>5.6.4 Detailed Criteria. IEEE Std 384-1981 provides detailed criteria for the independence of Class 1E equipment and circuits.</p>	<p>5.6.4 Detailed criteria. IEEE Std 384-1992 provides detailed criteria for the independence of Class 1E equipment and circuits.</p>	<p>RG 1.75 Rev. 3 now endorses IEEE Std. 384-1992.</p>

IEEE 603-1991	IEEE 603-1998	Comment
(Not included in IEEE Std. 603-1991)	IEEE Std 74.3.2-1993 provides guidance on the application of this criteria for the separation and isolation of the data processing functions of interconnected computers.	Added reference to IEEE Std. 7-4.3.2, which addresses digital I&C applications. RG 1.1.52 Rev. 2 now endorses IEEE Std. 7-4.3.2-2003.
<p>5.7 Capability for Test and Calibration. Capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. Testing of Class 1E systems shall be in accordance with the requirements of IEEE Std 338-1987. Exceptions to testing and calibration during power operation are allowed where this capability cannot be provided without adversely affecting the safety or operability of the generating station. In this case: (1) appropriate justification shall be provided (for example, demonstration that no practical design exists), (2) acceptable reliability of equipment operation shall be otherwise demonstrated, and (3) the capability shall be provided while the generating station is shut down.</p>	<p>5.7 Capability for testing and calibration. Capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. Testing of Class 1E systems shall be in accordance with the requirements of IEEE Std 338-1987. Exceptions to testing and calibration during power operation are allowed where this capability cannot be provided without adversely affecting the safety or operability of the generating station. In this case:</p> <ul style="list-style-type: none"> - Appropriate justification shall be provided (e.g., demonstration that no practical design exists), - Acceptable reliability of equipment operation shall be otherwise demonstrated, and - The capability shall be provided while the generating station is shut down. 	No difference.

IEEE 603-1991	IEEE 603-1998	Comment
<p>5.8 Information Displays 5.8.1 Displays for Manually Controlled Actions. The display instrumentation provided for manually controlled actions for which no automatic control is provided and that are required for the safety systems to accomplish their safety functions shall be part of the safety systems and shall meet the requirements of IEEE Std 497-1981. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator.</p>	<p>5.8 Information displays 5.8.1 Displays for manually controlled actions. The display instrumentation provided for manually controlled actions for which no automatic control is provided and the display instrumentation required for the safety systems to accomplish their safety functions shall be part of the safety systems and shall meet the requirements of IEEE Std 497-1981. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator.</p>	<p>No difference.</p>
<p>5.8.2 System Status Indication. Display instrumentation shall provide accurate, complete, and timely information pertinent to safety system status. This information shall include indication and identification of protective actions of the sense and command features and execute features. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator. The display instrumentation provided for safety system status indication need not be part of the safety systems.</p>	<p>5.8.2 System status indication. Display instrumentation shall provide accurate, complete, and timely information pertinent to safety system status. This information shall include indication and identification of protective actions of the sense and command features and execute features. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator. The display instrumentation provided for safety system status indication need not be part of the safety systems.</p>	<p>No difference.</p>
<p>5.8.3 Indication of Bypasses. If the protective actions of some part of a safety system have been bypassed or deliberately rendered inoperative for any purpose other than an operating bypass, continued indication of this fact for each affected safety group shall be provided in the control room.</p>	<p>5.8.3 Indication of bypasses. If the protective actions of some part of a safety system have been bypassed or deliberately rendered inoperative for any purpose other than an operating bypass, continued indication of this fact for each affected safety group shall be provided in the control room.</p>	<p>No difference.</p>
<p>5.8.3.1 This display instrumentation need not be part of the safety systems.</p>	<p>a) This display instrumentation need not be part of the safety systems.</p>	<p>No difference.</p>

IEEE 603-1991	IEEE 603-1998	Comment
<p>5.8.3.2 This indication shall be automatically actuated if the bypass or inoperative condition (a) is expected to occur more frequently than once a year, and (b) is expected to occur when the affected system is required to be operable.</p>	<p>b) This indication shall be automatically actuated if the bypass or inoperative condition is expected to occur more frequently than once a year, and is expected to occur when the affected system is required to be operable.</p>	<p>No difference.</p>
<p>5.8.3.3 The capability shall exist in the control room to manually activate this display indication.</p>	<p>c) The capability shall exist in the control room to manually activate this display indication.</p>	<p>No difference.</p>
<p>5.8.4 Location. Information displays shall be located accessible to the operator. Information displays provided for manually controlled protective actions shall be visible from the location of the controls used to effect the actions.</p>	<p>5.8.4 Location. Information displays shall be located accessible to the operator. Information displays provided for manually controlled protective actions shall be visible from the location of the controls used to affect the actions.</p>	<p>No difference.</p>
<p>5.9 Control of Access. The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof.</p>	<p>5.9 Control of access. The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof.</p>	<p>No difference.</p>
<p>5.10 Repair. The safety systems shall be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.</p>	<p>5.10 Repair. The safety systems shall be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.</p>	<p>No difference.</p>

IEEE 603-1991	IEEE 603-1998	Comment
5.11 Identification. In order to provide assurance that the requirements given in this standard can be applied during the design, construction, maintenance, and operation of the plant, the following requirements shall be met:	5.11 Identification. In order to provide assurance that the requirements given in this standard can be applied during the design, construction, maintenance, and operation of the plant, the following requirements shall be met:	No difference.
(1) Safety system equipment shall be distinctly identified for each redundant portion of a safety system in accordance with the requirements of IEEE Std 384-1981 and IEEE Std 420-1982.	a) Safety system equipment shall be distinctly identified for each redundant portion of a safety system in accordance with the requirements of IEEE Std 384-1992 and IEEE Std 420-1982.	RG 1.75 Rev. 3 now endorses IEEE Std. 384-1992.
(2) Components or modules mounted in equipment or assemblies that are clearly identified as being in a single redundant portion of a safety system do not themselves require identification.	b) Components or modules mounted in equipment or assemblies that are clearly identified as being in a single redundant portion of a safety system do not themselves require identification.	No difference.
(3) Identification of safety system equipment shall be distinguishable from any identifying markings placed on equipment for other purposes (for example, identification of fire protection equipment, phase identification of power cables).	c) Identification of safety system equipment shall be distinguishable from any identifying markings placed on equipment for other purposes (e.g., identification of fire protection equipment, phase identification of power cables).	No difference.
(4) Identification of safety system equipment and its divisional assignment shall not require frequent use of reference material.	d) Identification of safety system equipment and its divisional assignment shall not require frequent use of reference material.	No difference.
(5) The associated documentation shall be distinctly identified in accordance with the requirements of IEEE Std 494-1974.	e) The associated documentation shall be distinctly identified in accordance with the requirements of IEEE Std 494-1974.	No difference.
(Not included in IEEE Std. 603-1991)	f) The versions of computer hardware, programs, and software shall be distinctly identified in accordance with IEEE Std 7-4.3.2-1993.	Added reference to IEEE 7-4.3.2, which addresses digital I&C applications. RG 1.1.52 Rev. 2 now endorses IEEE Std. 7-4.3.2-2003.

IEEE 603-1991	IEEE 603-1998	Comment
<p>5.12 Auxiliary Features 5.12.1 Auxiliary supporting features shall meet all requirements of this standard.</p>	<p>5.12 Auxiliary features. Auxiliary supporting features shall meet all requirements of this standard.</p>	<p>No difference.</p>
<p>5.12.2 Other auxiliary features that (1) perform a function that is not required for the safety systems to accomplish their safety function and (2) are part of the safety systems by association (that is, not isolated from the safety system) shall be designed to meet those criteria necessary to ensure that these components, equipment, and systems do not degrade the safety systems below an acceptable level. Examples of these other auxiliary features shown in Figure 3 and an illustration of the application of this criteria is contained in Appendix A.</p>	<p>Other auxiliary features that perform a function that is not required for the safety systems to accomplish their safety functions, and are part of the safety systems by association (i.e., not isolated from the safety system) shall be designed to meet those criteria necessary to ensure that these components, equipment, and systems do not degrade the safety systems below an acceptable level. . Examples of these other auxiliary features are shown in Figure 3 and an illustration of the application of this criteria is contained in Annex A.</p>	<p>No difference.</p>
<p>5.13 Multi-Unit Stations. The sharing of structures, systems, and components between units at multi-unit generating stations is permissible provided that the ability to simultaneously perform required safety functions in all units is not impaired. Guidance on the sharing of electrical power systems between units is contained in IEEE Std 308-1980. Guidance on the application of the single failure criterion to shared systems is contained in IEEE Std 379-1988.</p>	<p>5.13 Multi-unit stations. The sharing of structures, systems, and components between units at multi-unit generating stations is permissible provided that the ability to simultaneously perform required safety functions in all units is not impaired. Guidance on the sharing of electrical power systems between units is contained in IEEE Std 308-1991. Guidance on the application of the single failure criterion to shared systems is contained in IEEE Std 379-1994.</p>	<p>RG 1.32 Rev. 3 now endorses IEEE Std. 308-2001. RG 1.53 Rev. 2 now endorses IEEE Std. 379-2000.</p>

IEEE 603-1991	IEEE 603-1998	Comment
<p>5.14 Human Factors Considerations. Human factors shall be considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the human operator(s) and maintainer (s) can be successfully accomplished to meet the safety system design goals, in accordance with IEEE Std 1023-1988.</p>	<p>5.14 Human factors considerations. Human factors shall be considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the human operator(s) and maintainer(s) can be successfully accomplished to meet the safety system design goals, in accordance with IEEE Std 1023-1988.</p>	<p>No difference.</p>
<p>5.15 Reliability. For those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved. IEEE Std 352-1987 and IEEE Std 577-1976 provide guidance for reliability analysis.</p>	<p>5.15 Reliability. For those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved. IEEE Std 352-1987 and IEEE Std 577-1976 provide guidance for reliability analysis.</p>	<p>No difference.</p>
<p>(Not included in IEEE Std. 603-1991)</p>	<p>Guidance on the application of this criteria for safety system equipment employing digital computers and programs or firmware is found in IEEE Std 7-4.3.2-1993.</p>	<p>Added reference to IEEE Std. 7-4.3.2, which addresses digital I&C applications. RG 1.1.52 Rev. 2 now endorses IEEE Std. 7-4.3.2-2003.</p>
<p>(Not included in IEEE Std. 603-1991)</p>	<p>5.16 Common cause failure criteria. Plant parameters shall be maintained within acceptable limits established for each design basis event in the presence of a single common cause failure (See IEEE 379-1994).</p>	<p>RG 1.53 Rev. 2 now endorses IEEE Std. 379-2000.</p>
<p>(Not included in IEEE Std. 603-1991)</p>	<p>IEEE Std 7-4.3.2-1993 provides guidance on performing an engineering evaluation of software common cause failures, including use of manual action and non-safety-related systems, or components, or both, to provide means to accomplish the function that would otherwise be defeated by the common cause failure.</p>	<p>Added reference to IEEE Std. 7-4.3.2, which addresses digital I&C applications. RG 1.1.52 Rev. 2 now endorses IEEE Std. 7-4.3.2-2003.</p>

IEEE 603-1991	IEEE 603-1998	Comment
<p>6. Sense and Command Features - Functional and Design Requirements. In addition to the functional and design requirements in Section 5, the following requirements shall apply to the sense and command features:</p>	<p>6. Sense and command features-functional and design requirements. In addition to the functional and design requirements in Clause 5, the requirements listed in 6.1 through 6.8 shall apply to the sense and command features.</p>	<p>No difference.</p>
<p>6.1 Automatic Control. Means shall be provided to automatically initiate and control all protective actions except as justified in 4.5. The safety system design shall be such that the operator is not required to take any action prior to the time and plant conditions specified in 4.5 following the onset of each design basis event. At the option of the safety system designer, means may be provided to automatically initiate and control those protective actions of 4.5.</p>	<p>6.1 Automatic control. Means shall be provided to automatically initiate and control all protective actions except as justified in Clause 4, item e). The safety system design shall be such that the operator is not required to take any action prior to the time and plant conditions specified in Clause 4, item e) following the onset of each design basis event. At the option of the safety system designer, means may be provided to automatically initiate and control those protective actions of Clause 4, item e).</p>	<p>No difference.</p>
<p>6.2 Manual Control 6.2.1 Means shall be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions. The means provided shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment consistent with the constraints of 5.6.1.</p>	<p>6.2 Manual control. Means shall be provided in the control room to a) Implement manual initiation at the division level of the automatically initiated protective actions. The means provided shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment consistent with the constraints of 5.6.1.</p>	<p>No difference.</p>
<p>6.2.2 Means shall be provided in the control room to implement manual initiation and control of the protective actions identified in 4.5 that have not been selected for automatic control under 6.1. The displays provided for these actions shall meet the requirements of 5.8.1.</p>	<p>b) Implement manual initiation and control of the protective actions identified in Clause 4, item e) that have not been selected for automatic control under 6.1. The displays provided for these actions shall meet the requirements of 5.8.1.</p>	<p>No difference.</p>

IEEE 603-1991	IEEE 603-1998	Comment
<p>6.2.3 Means shall be provided to implement the manual actions necessary to maintain safe conditions after the protective actions are completed as specified in 4.10. The information provided to the operators, the actions required of these operators, and the quantity and location of associated displays and controls shall be appropriate for the time period within which the actions shall be accomplished and the number of available qualified operators. Such displays and controls shall be located in areas that are accessible, located in an environment suitable for the operator, and suitably arranged for operator surveillance and action.</p>	<p>c) Implement the manual actions necessary to maintain safe conditions after the protective actions are completed as specified in Clause 4, item j). The information provided to the operators, the actions required of these operators, and the quantity and location of associated displays and controls shall be appropriate for the time period within which the actions shall be accomplished and the number of available qualified operators. Such displays and controls shall be located in areas that are accessible, located in an environment suitable for the operator, and suitably arranged for operator surveillance and action.</p>	<p>No difference.</p>
<p>6.3 Interaction Between the Sense and Command Features and Other Systems 6.3.1 Where a single credible event, including all direct and consequential results of that event, can cause a non-safety system action that results in a condition requiring protective action and can concurrently prevent the protective action in those sense and command feature channels designated to provide principal protection against the condition, one of the following requirements shall be met:</p>	<p>6.3 Interaction between the sense and command features and other systems 6.3.1 Requirements Where a single credible event, including all direct and consequential results of that event, can cause a nonsafety system action that results in a condition requiring protective action, and can concurrently prevent the protective action in those sense and command feature channels designated to provide principal protection against the condition, one of the following requirements shall be met:</p>	<p>No difference.</p>
<p>(1) Alternate channels not subject to failure resulting from the same single event shall be provided to limit the consequences of this event to a value specified by the design basis. Alternate channels shall be selected from the following:</p>	<p>a) Alternate channels not subject to failure resulting from the same single event shall be provided to limit the consequences of this event to a value specified by the design basis. Alternate channels shall be selected from the following:</p>	<p>No difference.</p>

IEEE 603-1991	IEEE 603-1998	Comment
(a) Channels that sense a set of variables different from the principal channels.	1) Channels that sense a set of variables different from the principal channels.	No difference.
(b) Channels that use equipment different from that of the principal channels to sense the same variable.	2) Channels that use equipment different from that of the principal channels to sense the same variable.	No difference.
(c) Channels that sense a set of variables different from those of the principal channels using equipment different from that of the principal channels.	3) Channels that sense a set of variables different from those of the principal channels using equipment different from that of the principal channels.	No difference.
Both the principal and alternate channels shall be part of the sense and command features.	4) Both the principal and alternate channels shall be part of the sense and command features.	No difference.
(2) Equipment not subject to failure caused by the same single credible event shall be provided to detect the event and limit the consequences to a value specified by the design bases. Such equipment is considered a part of the safety system.	b) Equipment not subject to failure caused by the same single credible event shall be provided to detect the event and limit the consequences to a value specified by the design bases. Such equipment is considered a part of the safety system.	No difference.
See Fig 5 for a decision chart for applying the requirements of this section.	See Figure 5 for a decision chart for applying the requirements of this clause.	No difference.
6.3.2 Provisions shall be included so that the requirements in 6.3.1 can be met in conjunction with the requirements of 6.7 if a channel is in maintenance bypass. These provisions include reducing the required coincidence, defeating the non-safety system signals taken from the redundant channels, or initiating a protective action from the bypassed channel.	6.3.2 Provisions. Provisions shall be included so that the requirements in 6.3.1 can be met in conjunction with the requirements of 6.7 if a channel is in maintenance bypass. These provisions include reducing the required coincidence, defeating the non-safety system signals taken from the redundant channels, or initiating a protective action from the bypassed channel.	No difference.
6.4 Derivation of System Inputs. To the extent feasible and practical, sense and command feature inputs shall be derived from signals that are direct measures of the desired variables as specified in the design basis.	6.4 Derivation of system inputs. To the extent feasible and practical, sense and command feature inputs shall be derived from signals that are direct measures of the desired variables as specified in the design basis.	No difference.

IEEE 603-1991	IEEE 603-1998	Comment
<p>6.5 Capability for Testing and Calibration 6.5.1 Means shall be provided for checking, with a high degree of confidence, the operational availability of each sense and command feature input sensor required for a safety function during reactor operation, This may be accomplished in various ways; for example:</p>	<p>6.5 Capability for testing and calibration 6.5.1 Checking the operational availability. Means shall be provided for checking, with a high degree of confidence, the operational availability of each sense and command feature input sensor required for a safety function during reactor operation. This may be accomplished in various ways; for example:</p>	<p>No difference.</p>
<p>(1) by perturbing the monitored variable,</p>	<p>a) By perturbing the monitored variable,</p>	<p>No difference.</p>
<p>(2) within the constraints of 6.6, by introducing and varying, as appropriate, a substitute input to the sensor of the same nature as the measured variable, or</p>	<p>b) Within the constraints of 6.6, by introducing and varying, as appropriate, a substitute input to the sensor of the same nature as the measured variable, or</p>	<p>No difference.</p>
<p>(3) by cross-checking between channels that bear a known relationship to each other and that have readouts available.</p>	<p>c) By cross-checking between channels that bear a known relationship to each other and that have readouts available.</p>	<p>No difference.</p>
<p>6.5.2 One of the following means shall be provided for assuring the operational availability of each sense and command feature required during the post-accident period:</p>	<p>6.5.2 Assuring the operational availability. One of the following means shall be provided for assuring the operational availability of each sense and command feature required during the post-accident period:</p>	<p>No difference.</p>
<p>(1) Checking the operational availability of sensors by use of the methods described in 6.5.1.</p>	<p>a) Checking the operational availability of sensors by use of the methods described in 6.5.1.</p>	<p>No difference.</p>
<p>(2) Specifying equipment that is stable and retains its calibration during the post-accident time period.</p>	<p>b) Specifying equipment that is stable and the period of time it retains its calibration during the post-accident time period.</p>	<p>No difference.</p>

IEEE 603-1991	IEEE 603-1998	Comment
<p>6.6 Operating Bypasses. Whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall automatically accomplish one of the following actions:</p>	<p>6.6 Operating bypasses. Whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall automatically accomplish one of the following actions:</p>	<p>No difference.</p>
<p>(1) Remove the appropriate active operating bypass(es).</p>	<p>a) Remove the appropriate active operating bypass(es).</p>	<p>No difference.</p>
<p>(2) Restore plant conditions so that permissive conditions once again exist.</p>	<p>b) Restore plant conditions so that permissive conditions once again exist.</p>	<p>No difference.</p>
<p>(3) Initiate the appropriate safety function(s).</p>	<p>c) Initiate the appropriate safety function(s).</p>	<p>No difference.</p>
<p>6.7 Maintenance Bypass. Capability of a safety system to accomplish its safety function shall be retained while sense and command features equipment is in maintenance bypass. During such operation, the sense and command features shall continue to meet the requirements of 5.1 and 6.3.</p>	<p>6.7 Maintenance bypass. Capability of a safety system to accomplish its safety function shall be retained while sense and command features equipment is in maintenance bypass. During such operation, the sense and command features should continue to meet the requirements of 5.1 and 6.3.</p>	<p>No difference.</p>
<p>EXCEPTION: One-out-of-two portions of the sense and command features are not required to meet 5.1 and 6.3 when one portion is rendered inoperable, provided that acceptable reliability of equipment operation is otherwise demonstrated (that is, that the period allowed for removal from service for maintenance bypass is sufficiently short to have no significantly detrimental effect on overall sense and command features availability).</p>	<p>NOTE - For portions of the sense and command features that cannot meet the requirements of 5.1 and 6.3 when in maintenance bypass, acceptable reliability of equipment operation shall be demonstrated (e.g., that the period allowed for removal from service for maintenance bypass is sufficiently short, or additional measures are taken, or both, to ensure there is no significant detrimental effect on overall sense and command feature availability).</p>	<p>No difference.</p>

IEEE 603-1991	IEEE 603-1998	Comment
<p>6.8 Setpoints 6.8.1 The allowance for uncertainties between the process analytical limit documented in Section 4.4 and the device setpoint shall be determined using a documented methodology. Refer to ISA S67.040-1987.</p>	<p>6.8 Setpoints. The allowance for uncertainties between the process analytical limit documented in Clause 4, item d) and the device setpoint shall be determined using a documented methodology. Refer to ANSI/ISA S67.04-1994.</p>	<p>RG 1.105 Rev. 3 now endorses ANSI/ISA S67.04-1994.</p>
<p>6.8.2 Where it is necessary to provide multiple setpoints for adequate protection for a particular mode of operation or set of operating conditions, the design shall provide positive means of ensuring that the more restrictive setpoint is used when required. The devices used to prevent improper use of less restrictive setpoints shall be part of the sense and command features.</p>	<p>Where it is necessary to provide multiple setpoints for adequate protection for a particular mode of operation or set of operating conditions, the design shall provide positive means of ensuring that the more restrictive setpoint is used when required. The devices used to prevent improper use of less restrictive setpoints shall be part of the sense and command features.</p>	<p>No difference.</p>
<p>7. Executive Features - Functional and Design Requirements In addition to the functional and design requirements in Section 5, the following requirements shall apply to the execute features:</p>	<p>7. Execute features (functional and design requirements) In addition to the functional and design requirements in Clause 5, the requirements listed in 7.1 through 7.5 shall apply to the execute features.</p>	<p>No difference.</p>
<p>7.1 Automatic Control, Capability shall be incorporated in the execute features to receive and act upon automatic control signals from the sense and command features consistent with 4.4 of the design basis.</p>	<p>7.1 Automatic control. Capability shall be incorporated in the execute features to receive and act upon automatic control signals from the sense and command features consistent with Clause 4, item d) of the design basis.</p>	<p>No difference.</p>

IEEE 603-1991	IEEE 603-1998	Comment
<p>7.2 Manual Control. If manual control of any actuated component in the execute features is provided, the additional design features in the execute features necessary to accomplish such manual control shall not defeat the requirements of 5.1 and 6.2. Capability shall be provided in the execute features to receive and act upon manual control signals from the sense and command features consistent with the design basis.</p>	<p>7.2 Manual control. If manual control of any actuated component in the execute features is provided, the additional design features in the execute features necessary to accomplish such manual control shall not defeat the requirements of 5.1 and 6.2. Capability shall be provided in the execute features to receive and act upon manual control signals from the sense and command features consistent with the design basis.</p>	<p>No difference.</p>
<p>7.3 Completion of Protective Action. The design of the execute features shall be such that once initiated, the protective actions of the execute features shall go to completion. This requirement shall not preclude the use of equipment protective devices identified in 4.11 of the design basis or the provision for deliberate operator interventions. When the sense and command features reset, the execute features shall not automatically return to normal; they shall require separate, deliberate operator action to be returned to normal. After the initial protective action has gone to completion, the execute features may require manual control or automatic control (that is, cycling) of specific equipment to maintain completion of the safety function.</p>	<p>7.3 Completion of protective action. The design of the execute features shall be such that, once initiated, the protective actions of the execute features shall go to completion. This requirement shall not preclude the use of equipment protective devices identified in Clause 4, item k) of the design basis or the provision for deliberate operator interventions. When the sense and command features reset, the execute features shall not automatically return to normal; they shall require separate, deliberate operator action to be returned to normal. After the initial protective action has gone to completion, the execute features may require manual control or automatic control (i.e., cycling) of specific equipment to maintain completion of the safety function.</p>	<p>No difference.</p>

IEEE 603-1991	IEEE 603-1998	Comment
<p>7.4 Operating Bypass. Whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall automatically accomplish one of the following actions:</p>	<p>7.4 Operating bypass. Whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall automatically accomplish one of the following actions:</p>	<p>No difference.</p>
<p>(1) Remove the appropriate active operating bypass(es).</p>	<p>a) Remove the appropriate active operating bypass(es).</p>	<p>No difference.</p>
<p>(2) Restore plant conditions so that permissive conditions once again exist.</p>	<p>b) Restore plant conditions so that permissive conditions once again exist.</p>	<p>No difference.</p>
<p>(3) Initiate the appropriate safety function(s).</p>	<p>c) Initiate the appropriate safety function(s).</p>	<p>No difference.</p>
<p>7.5 Maintenance Bypass. The capability of a safety system to accomplish its safety function shall be retained while execute features equipment is in maintenance bypass. Portions of the execute features with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass (that is, reducing temporarily its degree of redundancy to zero), the remaining portions provide acceptable reliability.</p>	<p>7.5 Maintenance bypass. The capability of a safety system to accomplish its safety function shall be retained while execute features equipment is in maintenance bypass. Portions of the execute features with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass (i.e., reducing temporarily its degree of redundancy to zero), the remaining portions provide acceptable reliability.</p>	<p>No difference.</p>
<p>8. Power Source Requirements 8.1 Electrical Power Sources. Those portions of the Class 1E power system that are required to provide the power to the many facets of the safety system are governed by the criteria of this document and are a portion of the safety systems. Specific criteria unique to the Class 1E power systems are given in IEEE Std 308-1980.</p>	<p>8. Power source requirements 8.1 Electrical power sources. Those portions of the Class 1E power system that are required to provide the power to the many facets of the safety system are governed by the criteria of this document and are a portion of the safety systems. Specific criteria unique to the Class 1E power systems are given in IEEE Std 308-1991.</p>	<p>RG 1.32 Rev. 3 now endorses IEEE Std. 308-2001.</p>

IEEE 603-1991	IEEE 603-1998	Comment
<p>8.2 Non-electrical Power Sources. Non-electrical power sources, such as control-air systems, bottled-gas systems, and hydraulic systems, required to provide the power to the safety systems are a portion of the safety systems and shall provide power consistent with the requirements of this standard. Specific criteria unique to non-electrical power sources are outside the scope of this standard and can be found in other standards.</p>	<p>8.2 Non-electrical power sources. Non-electrical power sources, such as control-air systems, bottled-gas systems, and hydraulic systems, required to provide the power to the safety systems are a portion of the safety systems and shall provide power consistent with the requirements of this standard. Specific criteria unique to non-electrical power sources are outside the scope of this standard and can be found in other standards.</p>	<p>No difference.</p>
<p>8.3 Maintenance Bypass. The capability of the safety systems to accomplish their safety functions shall be retained while power sources are in maintenance bypass. Portions of the power sources with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass (that is, reducing temporarily its degree of redundancy to zero), the remaining portions provide acceptable reliability.</p>	<p>8.3 Maintenance bypass. The capability of the safety systems to accomplish their safety functions shall be retained while power sources are in maintenance bypass. Portions of the power sources with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass (i.e., reducing temporarily its degree of redundancy to zero), the remaining portions provide acceptable reliability.</p>	<p>No difference.</p>

U.S. EPR Design Certification
Proposed Alternative

Attachment 2 to NRC:11:048

U.S. EPR Design Certification

Proposed Alternative to IEEE Std. 603-1991 Clause 5.6.1 “Independence Between Redundant Portions of a Safety System” in Accordance with 10 CFR 50.55a(a)(3)(i)

Proposed Alternative to IEEE Std. 603-1991 Clause 5.6.1 “Independence between Redundant Portions of a Safety System” in Accordance with 10 CFR 50.55a(a)(3)(i)

SYSTEMS/COMPONENTS AFFECTED

U.S. EPR self-powered neutron detector (SPND)-based reactor trip functions.

APPLICABLE CODE REQUIREMENT

IEEE Std 603-1991 Clause 5.6.1: Independence between Redundant Portions of a Safety System. “Redundant portions of a safety system provided for a safety function shall be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring the safety function”.

Clause 5.6.1 is identical in both the 1991 and 1998 versions of IEEE Std. 603. This alternative request is applicable to both versions of the standard. AREVA NP has requested use of the 1998 version in lieu of the 1991 version of IEEE Std. 603 in a separate alternative request.

REASON FOR REQUEST

The U.S. EPR protection system (PS) design contains reactor trip (RT) functions that actuate upon detection of high linear power density (HLPD) or low departure from nucleate boiling ratio (LDNBR) conditions in the reactor core. These RT functions receive input from 72 incore self-powered neutron detectors (SPND), which provide spatially dependent measurements of neutron flux. To take advantage of the benefits of core-wide, incore monitoring, each redundant PS division receives input from all 72 SPND measurement sensors.

During an April 11, 2011 public meeting and in previous interactions, NRC staff has informed AREVA NP of the following points regarding their interpretation of IEEE-603 independence requirements:

- IEEE-603, Clause 5.6.1 implicitly requires each division of the PS must acquire measurements unique to that division and make a trip decision based only on the measurements it acquires.

The HLPD and LDNBR RT functional logic is performed redundantly in the four PS divisions; however, the logic in each division uses the same 72 SPND measurements as input. Although AREVA believes the SPND based trip functions are redundant and independent “to the degree necessary to retain the capability to accomplish the safety function,” this implementation does not conform to the NRC Staff interpretation. Therefore a request for an alternative to IEEE-603 Clause 5.6.1 is needed.

PROPOSED ALTERNATIVE AND BASIS FOR USE

1.0 INTRODUCTION

AREVA NP acknowledges the NRC staff position expressed during the April 11, 2011 public meeting that strict compliance to requirements for independence between redundant portions of a safety

system is one design method which provides assurance that failures will not propagate outside the division where they occur, and will not defeat redundancy in the design. AREVA NP also acknowledges the NRC staff position that independence affords protection against two distinct types of failures:

1. Single failures postulated in the design and addressed through the system failure modes and effects analysis.
2. Unanticipated failure modes that may not be envisioned or postulated in the design, including potential multiple failures.

For the HLPD and LDNBR RT functions, alternative design features which provide reasonable assurance of protection against both of these failure types are used in lieu of redundant and independent sensor measurements between PS divisions. A conservative setpoint selection method is used to mitigate postulated single SPND input channel failures. Compliance to the single failure criterion is discussed in Section 3. The specific design of the SPND input channels and the existence of multiple layers of backup protective functions provide reasonable assurance of protection against unanticipated failure modes in the SPND input channels. These design measures are discussed in Section 4.

The use of in-core SPND measurements as inputs to RT functions, and the use of the same 72 SPND in each of the PS divisions, is included in the U.S. EPR design to enhance overall plant safety. While the individual SPND are not redundant to each other due to their spatially dependent nature, they are used in a manner that allows the RT functions to satisfy the single failure criterion and operate in a highly reliable manner. The benefits of using SPND as inputs to RT functions, and of using the same 72 SPND in each of the four PS divisions, are described in Section 2.

2.0 BENEFITS OF SPND BASED CORE SURVEILLANCE AND PROTECTION

The use of in-core SPNDs, distributed radially (12 radial locations) and axially (6 elevations along a "string" at each radial location) throughout the reactor core, facilitates direct and accurate on-line monitoring of the core power distribution during steady state and transient conditions. The totality of the 72 measurements is used in three distinct ways:

- Individually, each of the 72 SPNDs measure neutron flux at specific points in the core which allows for continuous monitoring of the local hot spot in the core (HLPD protection).
- Each of the 12 strings of six SPND sensors provides information required to perform detailed axial power shape reconstruction for continuous evaluation of the minimum departure from nucleate boiling ratio (MDNBR) for the hot channel in the core (LDNBR protection).
- Collectively, the 72 SPND signals are arranged geometrically in the core to provide 36 pairs of symmetric neutron flux measurements. This allows the protection system to confirm symmetric distribution of power when it exists, and to respond appropriately when asymmetries are detected (imbalance protection).

2.1 Benefits Relative to Excore Detectors

The traditional use of excore detectors to provide similar protection relies on application of analytical assumptions and uncertainties to demonstrate protection of the fuel safety limits.

IEEE Std. 603 Clause 6.4, Derivation of System Inputs, requires that: "To the extent feasible and practical, sense and command feature inputs shall be derived from signals that are direct measures of the desired variables as specified in the design basis".

Indirect measurement of a parameter requires application of assumptions and uncertainties to account for the difference between the real value of a parameter and the value provided by indirect measurement. The IEEE Std. 603 Clause 6.4 requirement reflects the fact that reliance on assumptions and application of uncertainties can be reduced by using the most direct available measurement, which in turn minimizes potential system failures due to misapplied or misunderstood assumptions and uncertainties.

Because of their location around the periphery of the core, excore neutron detectors are most sensitive to the fuel assemblies at the periphery of the core which are typically not the limiting locations relative to protecting fuel safety limits. Uncertainties and assumptions must then be factored into the excore detector measurements to relate the indirect measurements to the calculated real conditions in fuel assemblies closer to the center of the core.

Consistent with the IEEE 603 Clause 6.4 requirement, the U.S. EPR design contains 72 incore SPNDs distributed throughout the core to achieve a more direct measurement of neutron flux. Compared to the traditional use of excore detectors, SPND-based protection offers a significant safety benefit relative to protection of the fuel by replacing assumptions and uncertainties with more direct knowledge of the true core conditions.

2.2 Benefits of 72 SPND in Each PS Division Relative to a Divisionalized Approach

AREVA NP considered alternate means to accomplish the HLPD and DNBR reactor trip functions, using direct incore measurements, which employed independent sensor measurement within each division. Two primary options were considered:

- 1.) The addition of more SPNDs (3 additional sets of 72) to achieve redundancy of measurement at each location within the core. The different redundancies of SPND could then be acquired by different PS divisions, and each division could make a trip decision based on a unique set of 72 inputs.
- 2.) The existing 72 SPNDs could be divided into smaller groupings (e.g., "divisionalized"). Each divisionalized grouping would be acquired by a PS division and each division would make a trip decision based only on the measurements it acquires.

The first possibility (adding more SPNDs to the design) was determined to be unfeasible because there is not sufficient physical space in the core to include 216 additional SPND (4 redundant measurements at each location).

The second possibility involves a hypothetical design solution where 18 SPND measurements would be acquired by each PS division, and each division would perform HLPD and LDNBR calculations and make a decision to trip based only on the 18 measurements it acquires. It was determined that implementation of such a design, while providing independent measurements at the sensor level, would not be prudent for the following reasons:

- The hypothetical design essentially nullifies the advantages of direct measurement. Because each division would only use 18 measurements, those 18 measurements would have to be representative of the entire core. This would result in additional uncertainty in the measurements,

similar to using excore detectors. Not only would this result in reduced operating margin, it would necessarily result in overly conservative RT setpoints which would increase potential for unnecessary challenges to the plant safety systems in the form of spurious reactor trips.

- The hypothetical design impairs the ability to detect asymmetric core conditions. Because the LDNBR function is performed on a per-SPND string basis, the 6 SPND on a string must be acquired by one division. The hypothetical divisionalized design would have 3 SPND strings acquired by each PS division. This is problematic because detection of asymmetric events relies on comparison of symmetric pairs of SPND across the core. To satisfy the need for performing the LDNBR function on a per-string basis, and the need to compare symmetric SPND, each division needs to acquire SPND strings in multiples of 2. This is not possible given the number of SPND strings in the U.S. EPR core design.
- In the hypothetical design, inoperability of other sensors would invalidate 18 SPND measurements for the LDNBR function. The DNBR calculation uses sensor inputs, in addition to SPND, to account for pressure, temperature and flow. These other sensors are strictly divisionalized. This means that, for example, if the division 1 pressurizer pressure sensor is removed from service, the DNBR calculation in division 1 is invalidated. Since the 18 SPND measurements acquired by division 1 would not be acquired by other divisions, the inoperability of the PZR pressure sensor would effectively result in loss of the benefit of one fourth of the total SPND measurements.
- The hypothetical design is less robust against multiple failures of SPND. If two or three SPND, each in a different division are out of service or failed, the ability of multiple divisions to respond to an event is impaired. This is due to the increased “importance” of each SPND to its division’s functions because the division has a smaller number of SPND to begin with. This is in contrast to a design where all 72 measurements are acquired by each PS division, allowing all divisions to perform the function with multiple failed SPND, because the contribution of a single SPND is less “important” to the overall function when all four divisions acquire all 72 measurements.

For the reasons cited above, AREVA NP concluded that a “divisionalized” design, while providing additional independence at the sensor level, is a less robust design that does not take advantage of the safety benefits provided by more direct measurement. Compared to the U.S. EPR design, a “divisionalized” design would have a negative effect on overall plant safety and reliability.

3.0 LDNBR AND HLPD RT FUNCTION-COMPLIANCE WITH SINGLE FAILURE CRITERION

Figure 1 is a simplified representation of the U.S. EPR protection system processing of the HLPD RT function provided to aid in understanding of the discussion in this section. Table 1 provides a summary of how single failures are accommodated for both the LDNBR and HLPD RT functions.

As previously discussed, each division of the PS receives all 72 SPND measurements for evaluating core conditions. To accomplish this while maintaining independence between PS divisions to the extent practical, the SPND signals are amplified and multiplied via analog hardware and 72 electrically isolated signals are provided to the acquisition and processing units (APU) in each PS division.

After acquisition by the APUs, each division of the PS independently performs the HLPD and LDNBR calculations and downstream voting logic. Therefore, the LDNBR and HLPD RT functions exhibit traditional redundancy and independence from APU acquisition of the SPND measurements through the RT breakers. A single failure within the APUs, actuation logic units (ALU) or RT devices does not

impact the ability of the redundant PS divisions to perform the function. However, a single failure in an upstream SPND input channel does impact all four PS divisions. For this reason, the remainder of this single failure discussion is focused on failures in the upstream SPND input channels.

Single failures in SPND input channels can be grouped into two categories: Those that are automatically detected by the protection system (detected failures) and those that are not (undetected failures). Both failure types can be detected during periodic surveillance testing required by the Technical Specifications. The conservative setpoint selection approach, which mitigates single failures in the input channels, can be summarized as follows: a detected failure results in an automatic transition to a more conservative setpoint in the PS logic; a single undetected failure is factored into determination of the setpoint values that exists in the PS logic. These concepts are described in more detail below.

3.1 DETECTED SPND FAILURE

Several mechanisms are used to facilitate the automatic detection of a faulty SPND input signal. Each of these mechanisms is implemented separately and independently in each division:

- Monitoring the status of the power supplies to amplifiers and signal multiplication devices for each SPND input channel.
- Self-monitoring features built into the APU signal acquisition and analog to digital conversion hardware
- APU function processor monitoring of availability and health of its analog input modules
- APU software-based monitoring of each SPND input signal to detect an out-of-range signal

A failure detected through any of these mechanisms results in an invalid status being assigned to the affected SPND measurement signal in the PS software in each PS division. If an SPND fault is detected via periodic surveillance testing, the affected signal is manually assigned an invalid status in each PS division. Once an SPND signal is assigned an invalid status, the PS logic automatically selects a more conservative RT setpoint as illustrated in Figure 1, and this transition is alarmed in the main control room.

ANP-10287P "Incore Trip Setpoint and Transient Methodology for U.S. EPR" defines the process for determining the RT setpoint values to be used for detected failed SPND signals for both the HLPD and LDNBR RT functions.

3.2 UNDETECTED SPND FAILURE

Low probability, non-self announcing failures may be postulated in the SPND amplification and signal multiplication equipment. While this type of non-self announcing failure within the signal conditioning modules is a low probability event, and would subsequently be detected through frequent surveillance testing in the Technical Specifications, such a failure could compromise the integrity of an SPND signal that is used to perform a safety function during the period between the surveillance testing intervals. Therefore, an undetected SPND input failure will be explicitly considered in the Chapter 15 analyses by factoring the most limiting single SPND failure into the determination of the setpoint values that exists in the PS logic and demonstrating that the safety limits remain satisfied. The demonstration is described below.

3.2.1 Use of Existing Setpoint Determination Methodology

The failure of an SPND results in a loss of the measured LPD reading from that sensor, and a loss of the calculated DNBR from the string containing the failed SPND. The sensed core condition may deviate from the real core condition as a result of this loss of information. As a result, a more conservative RT setpoint is required to ensure that the fuel safety limits are protected at the required levels of coverage and confidence. The methodology presented in the Incore Trip Setpoint and Transient Methodology for U.S.EPR (ANP-10287P) topical report defines the process for calculating RT setpoints for *detected* SPND failures.

The analysis methodology presented in ANP-10287P uses core power distribution information in the form of simulated static SPND responses as input. The simulated SPND responses are calculated in a three dimensional neutronics code and then provided as input to the code package that executes the setpoint determination and dynamic compensation confirmation calculations. This information facilitates the calculation of the reference core conditions and the core conditions as sensed by the protection system with the inclusion of the constituent uncertainties. To evaluate the impacts of a single undetected SPND failure on the Chapter 15 analyses, the framework of existing setpoint determination methodology will be employed. The simulated SPND responses for all of the power distributions used as input to the methodology will be modified as described below to conduct the evaluation.

The accident analyses presented in Chapter 15 of the U.S. EPR FSAR incorporate the most limiting active single failure of a safety related system. For the SPNDs this will be accomplished by deterministically identifying, and removing from consideration, the most limiting SPND response (or string of SPNDs for the DNBR calculation) in each of the power distributions that are included in the inputs to the RT setpoint determination and dynamic compensation confirmation calculations. The resulting RT setpoints will protect the integrity of the fuel safety limits while assuming that the most limiting SPND failure has occurred. Because the ANP-10287P methodology was designed to generate setpoints that provide the prescribed coverage and confidence against violation of the fuel safety limits, there will be no reduction in margin to the safety limits. However, the resultant values of the reactor trip setpoints themselves may be further reduced for LPD or increased for DNBR.

A revision to ANP-10287P will be issued to add the method for the consideration of the *undetected* SPND failure.

3.2.2 Impact on Chapter 15 Analysis Results

This section discusses the impact of the explicit inclusion of the undetected SPND failure on the RT setpoints and on the Chapter 15 results in the U.S. EPR FSAR, Revision 2, for events that rely on the SPND-based RT functions.

Symmetric Events

The symmetric event reactor trip setpoints will be largely unaffected by the inclusion of an undetected loss of the most limiting SPND response. This reflects the fact that, during a symmetric event, all of the SPNDs respond in a similar manner due global core power changes. The loss of information, due to an undetected failure, from the most limiting of the SPNDs will have a negligible impact on both the required symmetric event reactor trip setpoints and the safety analysis modeled reactor trip time. The U.S. EPR FSAR, Revision 2, Chapter 15 analyses of symmetric events will remain representative of the performance of the protection system.

Asymmetric Events

The purpose of the LDNBR IMBALANCE / ROD DROP 1 of 4 Divisions setpoints is to provide a more conservative protection system response when either: 1) conditions known to cause asymmetric core power distributions are detected (rod drop), or 2) an asymmetric power distribution (imbalance) is detected. Because asymmetric events lead to power distributions with more localized changes, the inclusion of an undetected loss of the most limiting SPND response will, in most cases, require the responses from SPNDs more distant from the location of maximum DNBR degradation to reach the reactor trip setpoint. Therefore, an increase of the LDNBR IMBALANCE / ROD DROP 1 of 4 setpoints will be required to account for loss of the most limiting SPND signal while respecting fuel safety limits.

The resultant change in these trip setpoints will translate to a change in the response of the protection system to asymmetric events. The events that credit the LDNBR IMBALANCE / ROD DROP 1 of 4 functionality will be re-analyzed to account for the change in protection system response. The new setpoints used in this re-analysis will be generated with the most limiting SPND response removed from consideration, and the dynamic compensation confirmation calculations will be performed for all asymmetric events that credited this functionality. The conclusions reached in the U.S. EPR FSAR, Revision 2, analyses for these events will not be changed with respect to non-violation of safety limits. Rather, the inclusion of an undetected failed SPND input in the setpoint and transient verification analysis will be accommodated by a decrease or an increase in the trip setpoints and resultant shift in the time to reach the trip thresholds.

4.0 PROTECTION AGAINST UNANTICIPATED FAILURE MODES

The only portion of the PS design where redundancy and independence are not present is the SPND input channels. From the point of acquisition of the SPND measurements through the RT breakers independence is implemented between redundant divisions. Accordingly, this discussion is limited to measures included in the U.S. EPR design which provide reasonable assurance of protection against unanticipated or multiple failures in the SPND input channels.

The design of the SPND input channels uses only analog signal conditioning equipment to amplify and then split each SPND measurement so that four hardwired, analog signals are generated and sent separately to each PS division. This eliminates concerns related to software failures in the signal conditioning equipment or data communication faults between divisions that may affect multiple SPND measurements. Using only analog equipment to provide the measurements to the PS divisions increases confidence that potential failure modes are understood, and mitigated in the design.

The U.S. EPR PS design includes two sub-systems which operate independently of one another. As described in ANP-10304, "U.S. EPR Diversity and Defense-in-Depth Assessment", these subsystems are provided to establish signal diversity for RT functions. This means that, for each AOO in the design basis, the primary RT function credited to mitigate the AOO resides on one sub-system and a secondary RT function that can mitigate the same AOO using different input sensors resides on the other sub-system. So, for each AOO in which the HLPD or LDNBR function is the primary RT function, another RT function which does not use SPNDs as input exists which is capable of bringing the plant to a hot standby condition following the AOO.

The U.S. EPR design also includes a diverse actuation system (DAS) that includes a substantial number of automatic protective functions. The DAS is designed to protect the plant in case of a software common cause failure of the PS concurrent with an AOO or PA requiring protective action. The DAS does not utilize the SPND as inputs, and would be unaffected by unanticipated failures in the SPND input channels. A scenario where multiple failures of SPND input channels occurs is, in

the worst case, equivalent a software common cause failure of the PS that prevents the HLPD or LDNBR functions from actuating. The U.S. EPR Diversity and Defense-in-Depth analysis demonstrates that, in such a scenario, the DAS provides adequate protection of fuel safety limits in accordance with BTP 7-19 acceptance criteria, and does so without relying on the SPND measurements.

As discussed in Section 2.2, while redundancy and independence is not provided in the SPND input channels, a design in which each PS division utilizes all 72 SPND measurements is more robust against multiple SPND failures than a design in which the SPND are divisionalized and independence is provided.

5.0 SUMMARY

Through SPND-based LDNBR and HLPD protective functions, the U.S. EPR protection system is able to replace traditional core power distribution uncertainty with direct real-time local and spatial neutron flux measurement, which is regarded as a benefit with respect to the protection of the fuel.

Although the spatially dependent nature of the SPNDs do not allow for provision of redundant and independent sensor input channels to satisfy the single failure criterion, the LDNBR and HLPD RT functions satisfy the single failure criterion through conservative setpoint selection. Detected SPND input failures are accommodated by automatic transition in the PS logic to a more conservative setpoint. Undetected SPND input failures will be explicitly considered in the Chapter 15 analyses by factoring the most limiting single failure into determination of the setpoint values in the PS logic and demonstrating that the applicable safety limits are maintained.

Additional measures in the U.S. EPR design provide reasonable assurance of protection against unanticipated or multiple SPND input channel failures. These measures include conservative design of the SPND input channels to prevent such failures, and multiple layers of backup protective functions if such a failure were to occur.

The U.S. EPR design takes advantage of the fuel protection benefits provided by incore neutron flux measurements, and implements the associated protective functions in a highly reliable manner. The U.S. EPR implementation of SPND-based RT functions is an acceptable alternative to independence between redundant divisions required by IEEE 603-1991, clause 5.6.1, and provides an acceptable level of quality and safety.

Figure 1: HLPD RT Function Processing
(Simplified)

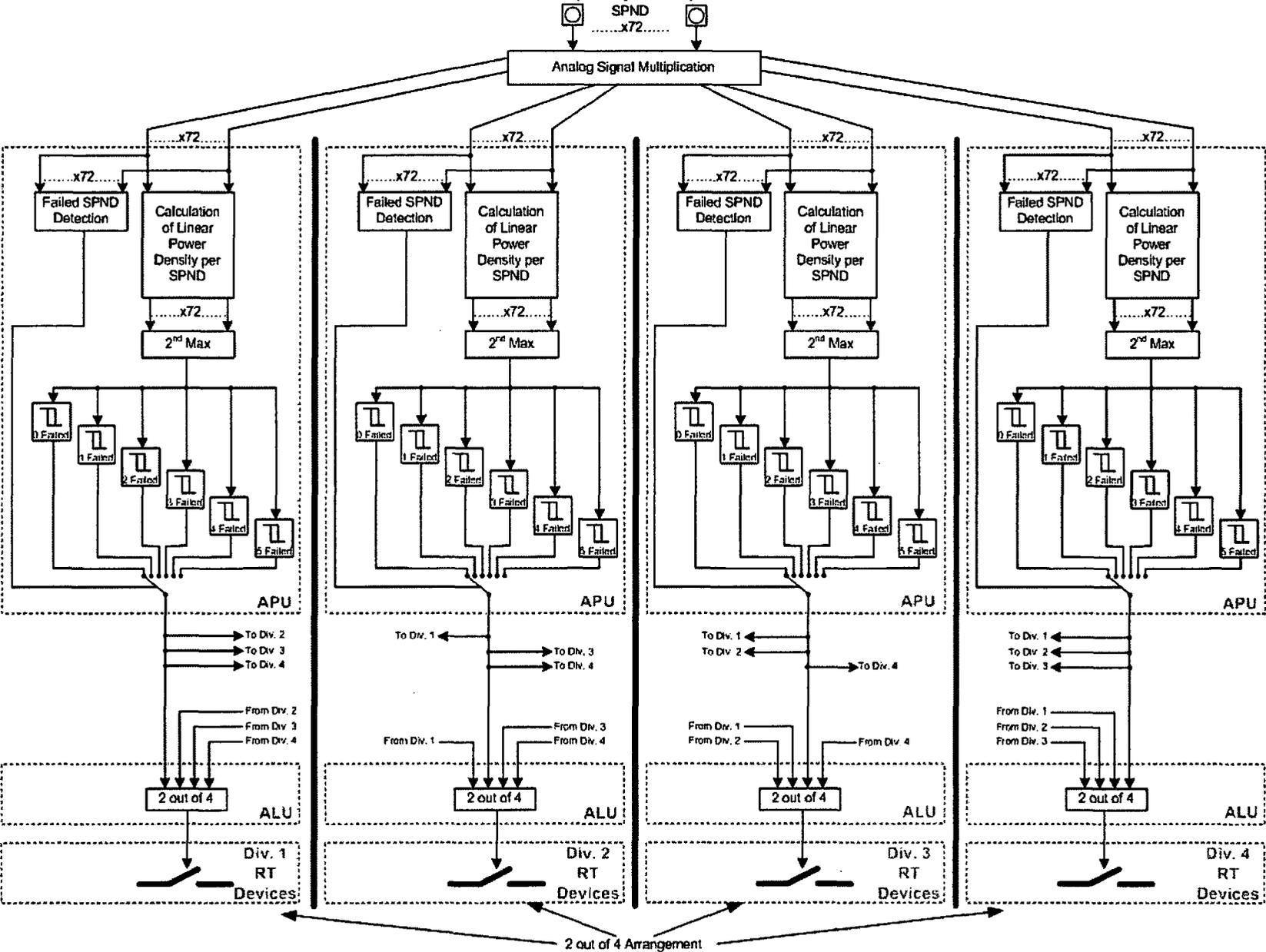


Table 1: Single Failure Summary for SPND Inputs and PS Equipment

Sensor, Functional Unit, or Equipment	Failure Mode	Method of Detection by PS	Inherent Compensating Provision	Effect
SPND Input Channel	Detected	TXS inherent self-monitoring or engineered fault detection mechanism	Failed SPND signal automatically assigned invalid status	More conservative "1 failed" RT setpoint automatically selected in all PS divisions. (Note 1) Safety function can still be performed
	Undetected - Spurious	None (Note 2)	Undetected SPND failure is assumed in safety analysis. "0 failed" setpoint includes uncertainty associated with undetected failure.	No effect on the PS. "0 failed" setpoint is still used. Safety function can still be performed.
	Undetected - Blocking	None (Note 2)	Undetected SPND failure is assumed in safety analysis. "0 failed" setpoint includes uncertainty associated with undetected failure.	No effect on the PS. "0 failed" setpoint is still used. Safety function can still be performed.
Acquisition and Processing Unit (APU) and communication from APU to ALUs	Detected	TXS inherent self-monitoring or engineered fault detection mechanism	Four redundant divisions and downstream voting.	Signals sent from affected APU are assigned faulty status. Downstream voting is modified to 2/3. Safety function can still be performed.
	Undetected - Spurious	None (Note 2)	Four redundant divisions and downstream voting	Signals from affected APU are "vote to trip". Downstream voting logic becomes 1/3. Safety function can still be performed.
	Undetected - Blocking	None (Note 2)	Four redundant divisions and downstream voting	Signals from affected APU fail to "vote to trip". Downstream voting logic becomes 2/3. Safety function can still be performed.

Sensor, Functional Unit, or Equipment	Failure Mode	Method of Detection by PS	Inherent Compensating Provision	Effect
Actuation Logic Unit (ALU)	Detected	TXS inherent self-monitoring or engineered fault detection mechanism	Redundant ALUs within each division. Four redundant divisions.	ALU RT output goes to "0" (trip state). Hardwired AND logic on output prevents trip device actuation. Redundant ALU in same division remains capable of issuing divisional RT signal. Safety function can still be performed.
	Undetected - Spurious	None (Note 2)	Redundant ALUs within each division. Four redundant divisions.	ALU RT output goes to "0" (trip state). Hardwired AND logic on output prevents trip device actuation. Redundant ALU in same division remains capable of issuing divisional RT signal. Safety function can still be performed.
	Undetected - Blocking	None (Note 2)	Four redundant divisions.	ALU cannot issue RT output. Hardwired AND logic prevents redundant ALU in the division from issuing divisional RT signal. Other 3 divisions remain functional. Safety function can still be performed.

Note 1: 1 to 5 invalid SPND signals result in conservative setpoint selection. 6 invalid SPND signals requires plant mode change per technical specifications. 7 or more invalid SPND signals results in automatic RT.

Note 2: Failure is detectable via periodic surveillance testing.