

2009 JAN 12 PM 3:23



January 8, 2009
NRC:09:002

RECEIVED

12/23/08
PFR 78856
①

Rulemaking, Directives, and Editing Branch
Office of Administration
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Comments on Draft Regulatory Guide DG-1190, "Manual Initiation of Protective Actions"

The NRC noted that public comments are being solicited on Draft Regulatory Guide DG-1190, "Manual Initiation of Protective Actions," and its associated regulatory analysis or value/impact statement. The NRC also noted that comments will be most helpful if received by February 20, 2009.

AREVA NP Inc. (AREVA NP) appreciates the opportunity to provide comments on DG-1190.

In general, AREVA has significant comments regarding two topic areas:

- The expansive new expectation for manual safety-related controls at the component level. This expectation is a significant expansion of the guidance in the existing Regulatory Guide 1.62, and beyond the scope of any IEEE 603-1991 requirement. The unbounded scope of additional controls required in the main control room has significant negative aspects associated with the added system design and human factors complexity. These negatives effects are not justified, since the added complexity has no clear and defined safety benefit.
- The misapplication of Branch Technical Position (BTP) 7-19 guidance to the topic of manual system level controls required by IEEE 603-1991 Clause 6.2. The manual controls used to address BTP 7-19 Point 4 (i.e., diverse controls) are not necessarily the same as those used to address IEEE Std 603-1991 Clause 6.2. Combining the two issues in this guidance further confuses the already complicated issue of defense-in-depth and diversity for digital I&C architectures.

Additional comments are included in the attachment to this letter.

If you have any questions related to this submittal, please contact Mr. Mark J. Burzynski, Product Licensing Manager at 434-832-4695 or by e-mail at mark.burzynski@areva.com.

Sincerely,

Ronnie L. Gardner

Ronnie L. Gardner, Manager
Corporate Regulatory Affairs
AREVA NP Inc.

SUNSI Review Complete

E-REDS = ADM-013

Redd = Khai Nguyen (Khn)

AREVA NP INC.

Template = ADM-013

An AREVA and Siemens company

Enclosure

cc: J. Rycyna
G. Tesfaye
Docket No. 52-020

Attachment

AREVA NP Comments on Draft Regulatory Guide DG-1190, "Manual Initiation of Protective Actions"

1. Section B, 1st paragraph, page 3 - This paragraph portrays digital instrumentation and control (I&C) systems in a negative way only. For balance, the positive capabilities of digital I&C should be included. The following modifications are suggested:

"Existing instrumentation and control (I&C) equipment in nuclear power plants is currently being replaced with computer-based digital I&C systems or advanced analog systems to increase reliability and plant safety. However, if designed or operated improperly, these technologies may pose new vulnerabilities for the nuclear power plant ~~in a number of aspects~~ compared to existing I&C systems."

2. Section B, 3rd paragraph, page 3 - This paragraph is confusing and does not provide any useful guidance. It is suggested that this entire paragraph be removed from the Draft Regulatory Guide (RG) for the following reasons:
 - The need for manual component-level control cannot be stated in a blanket manner. Instead, this need is dictated by the functional requirements and operating procedures for each plant design on a component-by-component basis.
 - This guidance expands manual control requirements in an unbounded manner. Is component-level control only suggested for those components that take part in a protective action, or does this suggestion extend beyond that? The language "...each appropriate plant system component" is ambiguous.
 - It is not clear whether the staff expects these manual component-level controls to be part of the safety system.
 - It is not clear if there is overlap between these component-level manual controls and those specified by item (3) in the previous paragraph.
 - It is not accurate to state that component-level controls are required to achieve completion of the safety function. For example, many components of the auxiliary supporting systems (e.g., heating, ventilation and air conditioning, diesel generators, and component cooling water) would not require manipulation, following actuation at the system level, to complete the safety function.
 - It is not clear how "high functional reliability of the protective system" constitutes a basis for requiring extensive manual component-level controls.

3. Section B, 4th paragraph, page 3 - The provision of manual, system level control of protective actions is required by IEEE Std 603-1991 Clause 6.2. Clause 6.2 does not provide any requirements that manual controls be provided to cope with failures of the automatic protective actions. Therefore, the use of the term "backup" in describing the manual controls is not consistent with Clause 6.2.

The use of the term "backup" is more appropriate in describing the diverse I&C provided specifically to cope with postulated software common cause failure (CCF) of the automatic protective actions. Diverse I&C is not the subject of IEEE Std 603-1991 Clause 6.2, and should not be the subject of RG 1.62.

The following modification is suggested:

~~“The protective actions can involve automatic controls with backup manual controls be initiated automatically, or, in certain cases, can be accomplished solely by manual controls. Protective actions ~~selected to be controlled~~ initiated solely by manually controls are subject to consideration of...”~~

4. Section B, 6th paragraph, page 4 - This paragraph is confusing and does not provide any useful guidance. It is suggested that this entire paragraph be removed from the Draft RG for the following reasons:

- The reference to IEEE Std 603-1991 Clause 5.6.3.1 seems inappropriate. When would system-level manual initiation of protective actions be used as a non-safety function?
- It is not clear if the safety related classification is intended to apply to the system-level manual functions, or the component level manual functions, or both.
- This paragraph specifies that the manual controls and indications must contain safety related software (i.e., they are part of a digital safety system). However, Regulatory Position 4 states: “In the case of automated digital protection systems, the point at which the manual controls are connected to safety equipment should be downstream of the plant’s digital I&C safety system outputs.” How can the manual controls only be connected to safety equipment downstream of the digital I&C safety system outputs if the manual controls themselves are part digital I&C safety systems?

A better discussion is proposed as follows:

IEEE Std 603-1991, Section 5.6.3.1, specifies that equipment “... that is used for both safety and nonsafety functions shall be classified as part of the safety systems...” Therefore equipment that is not classified as part of a safety system must not be credited for performing safety functions, if it is the only equipment that supports those safety functions. Nevertheless, non-safety multidivisional control and display stations may be used to perform functions needed to support plant safety, if there is also safety-related equipment available to perform the same plant safety function. The control and monitoring of functions credited with the protection of the plant in the plant safety analyses must be capable of being performed utilizing only safety-related resources. Non-safety multidivisional control and display stations may supplement the safety related control and display equipment that is credited in the plant safety analyses.

When using non-safety multidivisional control and display stations to perform safety-related actions, plant operators are expected to confirm that appropriate responses have been achieved for the actions taken. If the operator observes or suspects that the non safety multidivisional control and display station is not responding as expected, or that the nonsafety indications may be inaccurate, or that the plant is not responding as expected, then the operator must utilize the safety-related controls and indications to perform the necessary actions and to assess plant conditions and responses.

5. Section B, 8th paragraph, page 4 - This paragraph states: "Credible common-mode failures should be compensated either by diversity or defense in depth." The use of the word "or" is incorrect. Diversity can not be separated from defense in depth in the context of coping with software CCF. Instead, diversity must be incorporated into the lines of defense.

The following modification is suggested:

"Credible common-mode failures should be compensated ~~either~~ by diversity and ~~or~~ defense in depth."

6. Section B, 11th paragraph, page 5 - This paragraph makes reference to NRC's Branch Technical Position (BTP) 7-19: "Guidance provided to NRC staff in BTP 7-19 asserts that manual controls for safety equipment should be connected downstream of the plant's digital I&C safety system outputs." This paragraph incorrectly interprets the guidance in BTP 7-19 to apply to all manual controls for safety equipment; it should be removed from this RG.

In many I&C designs, the manual controls used to address BTP 7-19 Point 4 are not the same as those used to address IEEE Std 603-1991 Clause 6.2 (i.e., diverse controls). Combining the two issues in this guidance is confusing and not useful. The purpose of RG 1.62 is to provide guidance on compliance with IEEE Std 603-1991 Clause 6.2, not BTP 7-19 Point 4.

Comment 11 also applies to this paragraph.

7. Section C, Regulatory Position 1, page 5 - The phrase, "on a system-level basis for each division" is very confusing. IEEE Std 279-1971 uses "system-level" and IEEE Std 603-1991 uses "division level" and certainly the difference in terminology should be addressed. However, simply combining the two provides no clarity on what is meant by either concept.

The Discussion section of this Draft RG should define "system-level" and "division level" specifically in terms that relate directly to manual initiation of protective functions.

8. Section C, Regulatory Position 1, page 5 - It is suggested that the following statement be removed, as it cannot be meaningfully applied:

"Individual means should also be provided for manual initiation of each plant system component required for... providing functional reliability for protective systems as set forth in GDC 13 and GDC 21..."

The wording is ambiguous and no applicant will be able to provide a meaningful list of "components required for providing functional reliability for protective systems" short of all components.

This requirement is a significant expansion of the requirement in the existing RG 1.62. The unbounded scope of additional of controls required in the main control room has significant negative aspects associated with the added system design and human factors complexity. These negatives effects are not justified, since the added complexity has no clear and defined safety benefit.

The requirement should be modified to focus on safety-related component-level controls for required manual actions to provide safety functions for accident and transient mitigation and to achieve safe-shutdown (in accordance with BTP 5-4).

Comment 2 also applies to this Regulatory Position.

9. Section C, Regulatory Position 2, page 6 - The Regulatory Position contains the following statement: "Multiple initiations of safety systems (autosequencing) by distinct manual control manipulations are not precluded. It is not clear what type of functionality is being discussed in this sentence. The use of the term "autosequencing" is confusing. Is it different than "action-sequencing" as used in the previous sentence? The use of "multiple initiations" combined with "distinct manual control manipulations" is ambiguous.

The intent to allow a series of non-complex component-level actions in lieu of certain providing system-level manual controls should be clearly stated.

10. Section C, Regulatory Position 4, page 6 - The following statement from RG 1.62 was deleted from between the first two sentences on Regulatory Position 3:

"However, action-sequencing functions and interlocks (of position 2) associated with the final actuation devices and actuated equipment may be common if individual manual initiation at the component or channel level is provided in the control room."

This statement should be reinstated.

It should be noted that Regulatory Position 2 recognizes the existence (and need) for this additional control logic between the actuation system and the actuated devices.

"The Manual initiation of a protective action on a system-level basis for each division should perform all actions performed by automatic initiation such as starting auxiliary or supporting systems, sending signals to appropriate valve-actuating mechanisms to ensure correct valve position, and providing the required action-sequencing functions and interlocks."

In modern plants, this logic layer will be provided using software on safety function digital I&C processors. The net effect of the deletion of the noted sentence would be to preclude design using software logic for this functionality. Instead, new plant designs would be required to use conventional hardware equipment (e.g., relays and current-carrying wires) between the digital safety system and the final actuation device, with all related negative safety and reliability issues associated with this dated technology. This approach directly contradicts the "minimum of equipment" statement in Regulatory Position 4, unreasonably increases maintenance burden, decreases reliability of the protection functions, and therefore reduces plant safety.

11. Section C, Regulatory Position 4, page 6 - The following statement is a new requirement added to the Draft RG:

"In the case of automated digital protection systems, the point at which the manual controls are connected to safety equipment should be downstream of the plant's digital I&C safety system outputs. These connections should not

compromise the integrity of interconnecting cables and interfaces between local electrical or electronic cabinets and the plant's electromechanical equipment."

This passage incorrectly extends guidance in BTP 7-19 to cover all manual controls for safety equipment and should be removed from this RG.

BTP 7-19 suggests that: "displays and manual controls provided for compliance with Point 4 of the NRC position on diversity and defense in depth (D3)..." should be connected downstream of the plant's digital I&C safety system outputs. BTP 7-19 is silent on manual controls that are not credited for compliance with Point 4.

Manual controls that exist to cope with software CCF of a digital safety system (those discussed in BTP 7-19) must be independent of the digital safety system, and therefore connected downstream of the digital safety system outputs. There is no requirement for manual controls (component-level or system-level) of safety equipment to be independent of the digital safety system if they are not credited to cope with failure of the digital safety system.

In many I&C designs, the manual controls used to address BTP 7-19 Point 4 are not the same as those used to address IEEE 603 Clause 6.2. Combining the two issues in this guidance is confusing and not useful. The purpose of RG 1.62 is to provide guidance on compliance with IEEE Std 603-1991 Clause 6.2, not BTP 7-19 Point 4. Therefore, it is suggested that this paragraph and the entire discussion section on D3 be removed from this RG.

This passage also invokes the "downstream of digital system" requirement on individual component controls as well as the system level controls. Implementing this guidance for all component level controls of safety equipment would result in extensive addition of hardware between the digital safety system and the final actuation device, which unreasonably increases maintenance burden, decreases reliability of the I&C systems and therefore reduces plant safety.

12. Regulatory Analysis Section 3.2, page 8 – The following statement is made about the cost impact of the changes proposed in the Draft RG:

"Applicants would incur little or no cost and may, in fact, achieve cost savings."

Regulatory Analysis Section 4, page 8 – the following statement is made about the cost impact of the changes proposed in the Draft RG:

"It could also lead to cost savings for the industry, especially with regard to applications for standard plant design certifications and combined licenses."

These statements are only true if the new requirements proposed in the Draft RG are not applied to the existing fleet or any certified design or any design current submitted for design certification.

Section D of the Draft RG supports this perspective in the following statement:

"The NRC does not intend or approve any imposition or backfit in connection with its issuance."

However, the third request for additional information issued against ANP-10281P, *U.S. EPR Digital Protection System Topical Report*, indicates that NRC is already applying these new requirements to designs certification applications even though the guidance post dates the guidance applicable for the U.S. EPR based on 10 CFR 52.47 (a)(9).

Significant design modifications would be required to bring these designs into alignment with this guidance. Significant cost would be incurred, both in the design and licensing areas. This new guidance would certainly not result in cost savings for AREVA NP.