From: Getachew Tesfaye
To: DAFLUCAS Ronda M.
Date: 8/2/2007 8:28:45 AM
Subject: Draft RAI-2 Digital Protection System Topical Report (ANP 10281P)

Ronda,
Attached please find draft second round of RAIs for the Digital Protection System Topical Report (ANP 10281P). We will have our technical staff available to discuss them with you as soon as you are ready. Please call me with a proposed date and time for the telecon.

Please also review the RAI to ensure that we have not inadvertently included proprietary information. If there are any proprietary information, please let me know within the next ten days. If I do not hear from you within the next ten days, I will assume there are none and will make the draft RAI publicly available.

Thanks,
Getachew Tesfaye
Sr. Project Manager
NRO/DNRL/NARP

CC: Lois James; Norbert Carte

Mail Envelope Properties (46B1CDFD.9E4 : 24 : 8846)

Subject:	Draft RAI-2 Digital Protection System Topical Report (ANP 10281P)
Creation Date	8/2/2007 8:28:45 AM
From:	Getachew Tesfaye
Created By:	GXT2@nrc.gov

Recipients	**Action**	**Date & Time**
areva.com	Transferred	8/2/2007 8:29:12 AM
Ronda.Daflucas (DAFLUCAS Ronda M.)		
nrc.gov		
OWGWPO01.HQGWDO01	Delivered	8/2/2007 8:28:50 AM
NNC CC (Norbert Carte)	Opened	8/2/2007 8:39:50 AM
nrc.gov		
OWGWPO04.HQGWDO01	Delivered	8/2/2007 8:28:50 AM
LMJ CC (Lois James)	Opened	8/2/2007 8:29:06 AM

Post Office	**Delivered**	**Route**
		areva.com
OWGWPO01.HQGWDO01	8/2/2007 8:28:50 AM	nrc.gov
OWGWPO04.HQGWDO01	8/2/2007 8:28:50 AM	nrc.gov

Files	**Size**	**Date & Time**
MESSAGE	1180	8/2/2007 8:28:45 AM
Draft RAI-2 Digital Protection System TR.wpd	51049	8/2/2007 8:19:24 AM

Options

Auto Delete:	No
Expiration Date:	None
Notify Recipients:	Yes
Priority:	Standard
ReplyRequested:	No
Return Notification:	None
Concealed Subject:	No
Security:	Standard
To Be Delivered:	Immediate
Status Tracking:	Delivered & Opened

DRAFT

SECOND REQUEST FOR ADDITIONAL INFORMATION (RAI)

ANP-10281P, "U.S. EPR DIGITAL PROTECTION SYSTEM

TOPICAL REPORT" (TAC NO. MD4977)

PROJECT NUMBER 733

RAI 15) Please describe where AREVA plans to document the evaluation of the digital protection system (PS) against the Standard Review Plan.

10 CFR 50.34(h) "Conformance with the Standard Review Plan (SRP)." requires: "(1) (ii) Applications for ... design approvals ... shall include an evaluation of the facility against the SRP ..."

The Abstract of the U.S. EPR Digital Protection System (PS) Topical Report (TR) says: "This topical report describes the design of the U.S. EPR protection system and is provided to support the design certification application for the U.S. EPR." Therefore the PS TR is intended to be part of the application for design approval. However, it does not include an evaluation of the PS against the SRP.

RAI 16) Please describe the Design Acceptance Criteria (DAC) that AREVA plans to include in Design Certification Document (DCD).

The Abstract of the PS TR says: "This report ... presents the protection system architecture and the typical implementation of protective functions within this architecture." Therefore this report does not include the design of the PS. It is presumed that the design will not be included in the DCD either. If AREVA does not plan to include the PS design in the application for design certification, then AREVA must include DAC. When will AREVA propose DAC for the PS?

RAI 17) Describe the conventions for documenting requirements in the PS TR.

It is not clear what standards or conventions are followed in the PS TR, with respect to requirements documentation. For example: The PS TR contains a single "shall" in the paragraph on the cover - regarding proprietary information. There are also some "shalls" in Appendix B where IEEE Std 603 is quoted. The PS TR does contain twelve (12) "musts" in the body of the document, and some in Appendix A where the plant specific action items are quoted. Does AREVA have documentation that describes the convention that it follows in documenting requirements?

Regulatory Guide (RG) 1.172 endorses IEEE Std 830-1993 as providing an approach acceptable to the staff, subject to certain exceptions listed. IEEE Std 830-1993 implies that requirements are identified by the use of the word "shall", by using "shall" in all of its requirements examples. However, the RG, in Section C.2, implies that "must" is also an acceptable convention for identifying requirements. Therefore,

in order to clarify if one or both of these conventions are being followed, AREVA should identify the conventions that AREVA follows to identify requirements.

Note 1: The response to RAI No. 9 for the Software Program Manual (SPM), ANP-10272 Rev. 0, said: ' The AREVA NP Procedures and Policies Dictionary defines shall as "Denotes a requirement." ' Does the PS TR contain no requirements? Does the definition not apply to the PS TR? Are the SPM and the PS TR, both the same kind of document (e.g. containing programmatic requirements)?

Note 2: It appears that Area misunderstood RAI No. 9 of the SPM. The intent of that RAI, and of this one is NOT to proscribe a particular convention that must be followed by AREVA. Rather, this RAI is to ask AREVA to identify what convention is being followed, and where that convention is documented. The reason that this RAI is being ask for both the SPM and the PS TR is that it appears from the AREVA response to RAI No. 9 of the SPM that AREVA has different conventions for different kinds of documents.

RAI 18) Please clarify the processing of manual commands by the PS.

Section 3.1 says: "In addition to automatic functions, the PS can also process manual commands and issue corresponding actuation orders." It is not clear as to whether this statement is a statement of capability or permission. It is also not clear how the PS processing of manual commands satisfies the "minimum of equipment consistent with the constraints of 5.6.1" requirement of IEEE Std 603-1991.

IEEE Std 603-1991 Section 6.2.1 says: "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." The requirements contained in IEEE Std 603-1991 Section 5.6.1 are for 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, that' safety function."

A consistent interpretation of the requirement for the manual controls to be independent of the automatic portions can be found in IEEE Std 279-1971 and Regulatory Guide 1.62. IEEE Std 279-1971 Section 4.17 says: "Manual Initiation. The protection system shall include means for manual initiation of each protective action ... Manual Initiation should depend on the operation of a minimum of equipment." Regulatory Guide 1.62 clarified this requirement by stating: "The amount of equipment common to both manual and automatic initiation should be kept at a minimum. It is preferable to limit such common equipment to the final actuation device and the actuated equipment."

One of the major differences between IEEE 279 and IEEE 603 is that in IEEE 279 initiation is at the system level and in IEEE 603 initiation is at the division level.

RAI 19) Please describe the design features in the manual Engineered Safety Features (ESF) actuations ensure the completion of the protective action.

Section 8.5 describes the manual ESF actuations, but does not contain any description of the features that ensure that the completion of the protective action.

IEEE 603-1991 says: "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. ... 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."

RAI 20) Please describe when the implementation of each manual system level actuation of ESF functions will be determined.

Section 8.5 says: "The implementation of manual system level actuation of ESF functions is determined on a case-by-case basis. ... Therefore, several typical implementation designs are identified and applied to the manual initiation functions to satisfy the requirements imposed on each individual function." It is not clear how this level of description can not be considered conceptual. Please explain.

LIC-500 documents that the NRC, through it's website, provides guidance to applicants on the NRC's topical report (TR) program. Both the website and LIC-500 state that the report should contain complete and detailed information on the specific subject presented. LIC-500 says: 'The review of TRs, for the most part, follows the guidance for reviewing license amendments in Office Instruction LIC-101, "License Amendment Review Procedures" (Reference 2).' Section 4.1.1 of LIC-500 says: "(3) ... Conceptual or incomplete preliminary information will not be reviewed."

RAI 21) Please explain what AREVA believes can be approved in the design rules.

The PS TR has two sections that contain design rules: 1) Section 9.2, "Design Rules for Implementation of Permissive Signals, and 2) Section 10.2, "Design Rules."

It is conceivable that all design rules could be followed and the resulting design could still be unacceptable. Therefore if the design rules are approved, the resulting design still would need to be reviewed for acceptability, not just reviewed to ensure that the rules were followed. Therefore it is not clear what advantage AREVA sees in submitting these design rules for approval.

It is conceivable that one or more of the design rules could be violated, and the resulting design could still be acceptable. Therefore an acceptance of the design based solely on the design rules may not be desirable either.

LIC-500 documents that the NRC, through it's website, provides guidance to applicants on the NRC's topical report (TR) program. Both the website and LIC-500 state that the report should contain complete and detailed information on the specific

subject presented. LIC-500 says: 'The review of TRs, for the most part, follows the guidance for reviewing license amendments in Office Instruction LIC-101, "License Amendment Review Procedures" (Reference 2).' Section 4.1.1 of LIC-500 says: "(3) ... Conceptual or incomplete preliminary information will not be reviewed."

RAI 22) Please describe communication independence guidance, in addition to that of IEEE Std 7-4.3.2-2003 Annex E, that was followed.

Section 12.2 says: "The TXS communication techniques provide communications independence between redundant divisions and are consistent with the guidance of Reference 14 [i.e. IEEE 7-4.3.2-2003 Annex E]. The related figure from Reference 14 is duplicated in Figure 12-2. An equivalent figure describing the TXS communication is shown in Figure 12-3. Figure 12-3 depicts the use of buffering circuits and separation of data flow (communication isolation), which provide an acceptable method of communication independence and prevents adverse interactions." However, Section B of Regulatory Guide 1.152 Revision 2 says : 'Annex E, "Communication Independence," is not endorsed by the NRC because it provides insufficient guidance. Additional guidance is provided in Appendix 7.0-A, "Review Process for Digital Instrumentation and Control Systems," Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std 603," and Section 7.9, "Data Communication Systems," in NUREG-0800.'

Section 13.3 says: "Annex E .... describes an acceptable method of implementing the safety to non-safety interface." Please explain the use of the term "acceptable." That is, acceptable to who?

RAI 23) Please describe the specific of checkback signal used by the Maintenance and Service unit Interface - Auxiliary Unit (MSI-AU).

Section 5.4 says: "The MSI-AU's primary function is to acquire the checkback signals for periodic testing of the PAC [Priority Actuation and Control] modules." From ANP-10273P Revision 0, "AV42 Priority Actuation and Control Module," it is apparent that there may more than one checkback signal from an AV42 module, and that there may be more than one type (e.g. safety and non-safety) of checkback signal. All of the checkback signals are not identified or described in the AV42 topical report. Please identify and describe the specific checkback signals that will be used by the PS. Please confirm that the AV42 checkback signals used by the PS are never processed by non-safety components.

RAI 24) Please describe all non-safety information that is input into the PS. If there is no information of this type, then please provide a statement to that effect.

RAI 25) Please describe the Failure Modes and Effects Analysis (FMEA) and reliability analysis that has been performed on the PS.

Section 5.15 of IEEE 603-1991 says: "**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."

Section 14.18, "Sub-Clause 5.15 - Reliability," of the PS TR says: 'The PS is analyzed in the U.S. EPR probabilistic risk assessment to support the overall U.S. EPR probabilistic design objectives, which are described in AREVA NP report ANP-10274 "U.S. EPR Probabilistic Risk Assessment Methods Report" ...' This seems to imply that the PRA will be the only reliability analysis that will be performed on the PS. Is this correct?

Section B of Regulatory Guide 1.152 Revision 2 says: "The NRC does not endorse the concept of quantitative reliability goals as a sole means of meeting its regulations for reliability of digital computers used in safety systems." Please explain how the use of the PRA analysis in this case is not a case of "quantitative reliability goals as a sole means of meeting ... regulations."

Section 7.1 of the AV42 Topical Report (ANP-10273P Rev. 0) says: "A system level Failure Modes and Effects Analysis (FMEA) will be performed for plant specific applications which use the AV42." Since the PS will use the AV42, a FMEA will be performed on the PS. Why is this FMEA not mentioned in PS TR?

RAI 26) Why is the FMEA not mentioned as part of the single failure analysis?

IEEE 603-1991 Section 5.1 contains the single failure criterion requirement, which in part requires that an analysis be performed. Section 4.3.3, "Failure Modes and Effects Analysis," of the SPM (ANP-10272 Rev. 0) says: "The FMEA examines the effects of random single failures on the ability of the safety system to perform its required safety functions. The FMEA follows the guidance of IEEE 379 ..., which is endorsed by Regulatory Guide 1.53 ..." However, Section 14.4, "Sub-Clause 5.1 - Single Failure Criterion," of the PS TR does not reference the FMEA that was performed to arrive at the conclusions presented.

RAI 27) Please describe how cyber security will be addressed in PS application development process.

Section 14.8.1 says: "The TXS system design provides multiple, diverse levels of protection against cyber intrusion. These include administrative/procedural controls, TXS hardware controls, and TXS software controls. These security measures have multiple levels of defense ..." This description does not provide any information on what will be done during the application development process to address cyber security.

10 CFR 50.34(h) "Conformance with the Standard Review Plan (SRP)." requires: "(1) (ii) Applications for ... design approvals ... shall include an evaluation of the facility against the SRP ... (2) The evaluation required by this section shall include an identification and description of all differences in design features, analytical techniques, and procedural measures proposed for a facility and those corresponding features, techniques, and measures given in the SRP acceptance criteria. Where such a difference exists, the evaluation shall discuss how the alternative proposed provides an acceptable method of complying with those rules or regulations of Commission, or portions thereof, that underlie the corresponding SRP acceptance criteria." NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," Chapter 7, Table 7-1 identifies that

Regulatory Guide 1.152 contains acceptance criteria applicable to Reactor Trip Systems and Engineered Safety Feature systems. Regulatory Guide 1.152, Revision 2 section C.2 says in part : "The digital safety system development process should address potential security vulnerabilities in each phase of the digital safety system lifecycle." Since the PS TR will be incorporated into design certification application by reference, these acceptance criteria will need to be addressed at some point.

Why is Section 9.3 of ANP-10272 Revision 0 not referenced?

RAI 28) What is the proposed design acceptance criteria for determining which ESF actuation signals can be reset by specific operator action and which one can be reset by the initiating plant variable returning to within an acceptable range?

Section 14.5 says: "System level ESF actuation signals can be reset by specific operator action or, in certain cases, by the initiating plant variable returning to within an acceptable range."

RAI 29) Which components assure the once initiated, protective actions go to completion?

IEEE STD 603-1991 Section 5.2 says: "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."

Section 14.5 says: "System level ESF actuation signals can be reset by specific operator action or, in certain cases, by the initiating plant variable returning to within an acceptable range. This system level reset does not stop the ESF actuators. Further operator actions are required to stop the actuators on a component-by-component basis after the system level signal is reset." This statement understood to mean that once initiated the intended sequence of protective actions shall continue until completion, but not which components will assure that it is satisfied, or how it is assured.

Section 4.6 of the AV42 TR says: "The AV42 Module is designed and tested to confirm that the components as a whole demonstrate acceptable module performance to ensure the completion of protective actions over the range of accident, transient, and steady-state conditions for a plant." This statement again does not indicate which components assure completion of the protective action, or how it is assured.

RAI 30) Please explain where an analysis of the entire safety system is documented.

Figure 1 of IEEE Std 603-1995 portrays the scope of the IEEE 603 safety system as being from sensors to actuated components. The criteria of IEEE 603 Section 5 are understood to apply to the entire safety system as defined in Figure 1. In other words, a safety system is a set of equipment required to accomplish a set of safety functions, and Section 5 applies to that entire set of equipment.

Sections 14.3 through 4.18 mostly describe the PS portion of the safety system. Where will an analysis of the entire safety system be documented.

RAI 31) Please describe the operating bypass features associated with the manual actuations.

Section 6 of IEEE 603-1991 contains functional and design requirements for the sense and command features of a safety system. Section 6.2 contains requirements for means to manual initiate and control protective actions. Are these manual means part of the PS as defined in this topical report? Section 6 also contain requirements for operating and maintenance bypasses. Do the statements of conformance to operating and maintenance bypasses in Section 14.26, 14.27, 14.33 and 14.34 apply to the manual means of initiation and control of the protective action?

RAI 32) Please describe how the redundant ring network topology is immune to single failures.

Section 6.1.2 says: "In this topology, a break in one of the double fiber optical connections, or a failure in one optical port of one OLM, does not affect network availability. If an OLM is lost, only the unit(s) directly connected to the failed OLM is affected." However, these are not the only failure modes that are possible in a network (e.g NRC Information Notice 2007-15). Please describe, or provide a reference, to a description of the possible failure modes in: 1) a profibus network, and 2) in a token ring network. How are each of these failure modes addressed by the AREVA design? Will this information be in the Failure Modes and Affects Analysis (FMEA)?

RAI 33) Please describe all of the types of maintenance bypasses and their associated affect on the RT or ESF functions.

Section 14.4 says: "If one redundancy within the PS is bypassed for testing or maintenance, and a credible single failure occurs in another redundancy, the ability to perform the required protective actions is maintained." However it is not clear as to what redundancies can be bypassed, how bypassing is accomplished, or the affect of bypassing of each on system function:

1) Each division has separate sensors, and therefore the sensors can be considered redundant to each other. Can the sensors be bypassed? How is sensor bypass accomplished, and how does the system functionality change?
2) The divisions can be considered redundant to each other. Can a division be bypassed? How is division bypass accomplished, and how does the system functionality change?
3) Each division contains racks of equipment (e.g. Remote Acquisition Units, Acquisition and Processing Units, Actuation Logic Units, Power Supplies, Gateways, ...) that could be considered to be redundant to similar units in the other divisions. Can each rack of equipment be bypassed? How is the system functionality affected by bypassing this equipment? How is the functioning of the Optical Link Modules (OLMs) associated with each bypassed rack affected?
4) Each division contains Optical Link Modules (OLMs) that could be considered to be redundant to each other. Can these OLMs be bypassed? How does the network and system functionality change when these modules are bypassed?
5) Are the functionally independent subsystems (A and B) redundant to each other?

RAI 34) Please clarify or correct the parenthetical bus numbering shown on the right side of Division 4 of Figure 4-1.

RAI 35) Are all PS Optical Link Modules (OLMs) shown in Figures 6-3 through 6-19? Are all instances where multiple PS units access a network through the same OLM explicitly shown in figures 6-3 through 6-19? Does the same OLM appear on more than one figure?

Section 6.1 says: "Multiple PS units can access a network through the same OLM..." This statement is understood to describe a possibility. However, it may not be clear what will be implemented.

RAI 36) Are the PS networks considered to be part of the PS?

Section 6.1 says: "Multiple PS units can access a network through the same OLM; therefore, the OLMs are considered part of the network and are not part of any PS unit." Section 5.0, "Protection System Units," contains ten (10) subsections; none of these ten sections is a network. Therefore the PS networks are not considered to be PS units. Are the PS networks considered to be part of the PS? Are the OLMs considered to be part of a PS division?

RAI 37) Please define all items that could be considered to be a PS unit.

Section 6.1 says: "Multiple PS units can access a network through the same OLM; therefore, the OLMs are considered part of the network and are not part of any PS unit." Section 5.0, "Protection System Units," contains ten (10) subsections. Do the titles of these subsections define all possible PS units?

RAI 38) Please discuss how the U.S. EPR design complies with IEEE 603-1991 Section 7.4.

Figure 4 of IEEE Std. 603-1991 describes the general elements of a safety system to be "sense and command features," "execute features," and "power sources." IEEE 603-1991 Section 2, "Definitions" contains definitions for each of these general elements. Section 2 of IEEE Std. 603-1991 defines: "**protection system.** That part of the sense and command features involved in generating those signals used primarily for the reactor trip system and engineered safety features."

IEEE Std. 603-1991 Section 7, "Execute Features - Functional and Design Requirements," says: "In addition to the functional and design requirements in Section 5, the following requirements shall apply to the execute features:" IEEE Std. 603-1991 Sub-Section 7.4, "Operating Bypass," contains operating bypass requirements. Therefore IEEE 603-1991 requires that the execute features contain operating bypass functionality. However, Section 14.33 "Sub-Clause 7.4 - Operating Bypass," says: "Operating bypass of protective actions are implemented in the sense and command features of the PS."

10 CFR 50.55a(a)(2) says: "Protection systems of nuclear power reactors of all types must meet the requirements specified in paragraph (h) of this section." Paragraph (h) requires compliance with IEEE Std. 603-1991 including the correction sheet dated January 30, 1995.

10 CFR 50.55a(a)(3) says: "Proposed alternatives to the requirements of paragraphs ... (h) of this section or portions thereof may be used when authorized by the Director of the Office of Nuclear Reactor Regulation. The applicant shall demonstrate that: (i) The proposed alternatives would provide an acceptable level of quality and safety, or (ii) Compliance with the specified requirements of this section would result in hardship or unusual difficulty without a compensating increase in the level of quality and safety."

IEEE Std. 603-1991 Section 6, "Sense and Command Features - Functional and Design Requirements," says: "In addition to the functional and design requirements in Section 5, the following requirements shall apply to the sense and command features:". IEEE Std. 603-1991 Sub-Section 6.6, "Operating Bypasses," contains operating bypass requirements. Therefore IEEE 603-1991 requires that the sense and command features contain operating bypass functionality.

It appears that the paradigm for safety systems in IEEE 603 is that each safety system is composed of two portions: 1) sense and command features and 2) execute features. Each of these portions is envisioned to have both operating and maintenance bypass functionality. Please describe how the AREVA design corresponds to this paradigm.