

November 1, 2007

Mr. Ronnie L. Gardner  
AREVA NP Inc.  
3315 Old Forest Road  
P.O. Box 10935  
Lynchburg, VA 24506-0935

SUBJECT: AREVA NP, INC. - SECOND REQUEST FOR ADDITIONAL INFORMATION  
REGARDING ANP-10273P, "AV42 PRIORITY ACTUATION AND CONTROL  
MODULE TOPICAL REPORT" (TAC NO. MD3867)

Dear Mr. Gardner:

By letter dated November 28, 2006, AREVA NP, Inc. (AREVA) submitted for U.S. Nuclear Regulatory Commission (NRC) staff review, ANP-10273P, "AV42 Priority Actuation and Control Module Topical Report [TR]." In the acceptance letter to review the TR, the NRC staff stated its expectation to issue any requests for additional information (RAIs) by July 31, 2007.

Accordingly, by letter dated July 30, 2007, the NRC staff issued its first set of RAIs to AREVA. AREVA provided a partial response by letter dated September 19, 2007. During a recent audit of the AV42 Priority Actuation and Control Module design documents at AREVA offices in Charlotte, NC, the NRC staff and an Oak Ridge National Laboratory (ORNL) contractor clarified the extent and level of detail to which the first RAIs should be answered. The NRC staff and the ORNL contractor also identified an additional set of RAIs needed for the review of the TR.

The possibility of issuing RAIs beyond our original estimated date of July 31, 2007, was communicated to you in our July 30, 2007, letter that transmitted the first set of RAIs. Our questions are provided in the enclosure. Your staff has agreed that your responses to both sets of RAIs will be provided within 60 days of the date of this letter.

If you have any questions regarding this matter, I may be reached at 301-415-3361.

Sincerely,

*/RA/*

Getachew Tesfaye, Sr. Project Manager  
EPR Projects Branch  
Division of New Reactor Licensing  
Office of New Reactors

Project No. 733

Enclosure: Request for Additional Information  
cc: See next page

Mr. Ronnie L. Gardner  
AREVA NP, Inc.  
3315 Old Forest Road  
P.O. Box 10935  
Lynchburg, VA 24506-0935

SUBJECT: AREVA NP, INC. - SECOND REQUEST FOR ADDITIONAL INFORMATION REGARDING ANP-10273P, "AV42 PRIORITY ACTUATION AND CONTROL MODULE TOPICAL REPORT" (TAC NO. MD3867)

Dear Mr. Gardner:

By letter dated November 28, 2006, AREVA NP, Inc. (AREVA) submitted for U.S. Nuclear Regulatory Commission (NRC) staff review, ANP-10273P, "AV42 Priority Actuation and Control Module Topical Report [TR]." In the acceptance letter to review the TR, the NRC staff stated its expectation to issue any requests for additional information (RAIs) by July 31, 2007.

Accordingly, by letter dated July 30, 2007, the NRC staff issued its first set of RAIs to AREVA. AREVA provided a partial response by letter dated September 19, 2007. During a recent audit of the AV42 Priority Actuation and Control Module design documents at AREVA offices in Charlotte, NC, the NRC staff and an Oak Ridge National Laboratory (ORNL) contractor clarified the extent and level of detail to which the first RAIs should be answered. The NRC staff and the ORNL contractor also identified an additional set of RAIs needed for the review of the TR.

The possibility of issuing RAIs beyond our original estimated date of July 31, 2007, was communicated to you in our July 30, 2007, letter that transmitted the first set of RAIs. Our questions are provided in the enclosure. Your staff has agreed that your responses to both sets of RAIs will be provided within 60 days of the date of this letter.

If you have any questions regarding this matter, I may be reached at 301-415-3361.

Sincerely,

*/RA/*

Getachew Tesfaye, Sr. Project Manager  
EPR Projects Branch  
Division of New Reactor Licensing  
Office of New Reactors

Project No. 733

Enclosure: Request for Additional Information  
cc: See next page

DISTRIBUTION:

PUBLIC  
RidsAcrsAcnwMailCenter  
GTesfaye, NRO  
ADAMS Accession No.: ML072820008

NARP RF  
RidsOgcRp  
EEagle, NRO

RidsNroDnrlNarp  
JSmith, NRO

RidsNroDelce1  
DClarke, NRO

OFFICE	PM:DNRL/NARP	PM:DNRL/NARP	LA: DNRL/NARP	BC:DE/ICE1	BC:DNRL/NARP
NAME	JSmith	GTesfaye	DClarke	TJackson	JColaccino
DATE	10/ 09 /07	10/ 09 /07	10/ 22 /07	10/ 25 /07	11/ 01 /07

Official Record Copy

SECOND REQUEST FOR ADDITIONAL INFORMATION  
ANP-10273P, "AV42 PRIORITY ACTUATION AND CONTROL

MODULE TOPICAL REPORT"

(TAC NO. MD3867)

PROJECT NO. 733

By letter dated November 28, 2006 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML063380075), AREVA NP, Inc. (AREVA) submitted for Nuclear Regulatory Commission (NRC) staff review, ANP-10273P, "AV42 Priority Actuation and Control Module Topical Report [TR]." The NRC staff is reviewing ANP-10273P and has determined that the following additional information is needed in order for the staff to complete its review.

RAI-48 ANP-10273P, Section 4.1, "General" states:

*The AV42 consists of two major data processing components. The first major component is a PLD [programmable logic device]... Once the design is built neither component is changeable... Hardwired connections to the plug at the backplane of the AV42 are used to set the parameters that adapt the function of the PLD to the type of actuator.*

This statement needs clarification. First, the ability to "adapt the function of the PLD..." implies reconfigurability and, therefore, the presence of internal volatile memory. If there is an internal volatile memory, in which major component or subsystem is it located? How exactly does the setting of new parameters adapt the function of the PLD to the type of actuator? Second, how easy will it be to perform unintentional or malicious "reconfiguration" (such as a single disconnection) from the backplane once a module is in operation and what is the potential consequence of such an action?

ANP-10273P, Section 4.1, also states:

*... The PROFIBUS sets the parameters that adapt the function of the controller to the type of actuator.*

Does this, together with the previous quote in italics, mean that reconfiguration of the AV42 to adapt it to a particular actuator involves two steps; (a) via hardwire reconfiguration (to adapt the PLD to the particular actuator) from the backplane, and (b) reconfiguration via the PROFIBUS (to adapt the controller to the particular actuator)? How is this second reconfiguration performed? For example, is the configuration performed from the TELEPERM XP System (TXP) or is the configuration done via an interface that may be connected on the network? If two configuration procedures have to be performed as discussed, what will be the safety

Enclosure

impact of performing one and not the other, and what administrative procedures are in place to ensure that both procedures are performed?

- RAI-49 ANP-10273P, Section 5.1, "AV42 Quality," indicates that the PLD is based on a non-user programmable EEPROM, and implies that that the PLD's function is achieved by permanently programming it to perform particular logic functions. However, certain functions may still require timing circuitry and random access memory (RAM). An example of where such circuitry may be needed is the AV42's ability to recognize that a test input has persisted longer than 5 seconds during a test mode. It would be useful to list (e.g., in tabular form) the characteristics of the particular PLD that differentiate it from a more complex programmable device such as a field-programmable gate array (FPGA) or general purpose computer. Comparisons may include, but are not limited to (a) presence/absence of RAM and what it used for, if one exists; (b) presence/absence of timing circuitry such as a watch dog timer on-chip (i.e., in the PLD portion of the AV42); (c) presence/absence of programmed instruction in the PLD, etc. Such comparisons will help the NRC to independently assess how to address life cycle verification and validation (V&V) issues.
- RAI-50 Considering the electronics of the PLD device used, is it possible that it is susceptible to a "half-bit" phenomenon? In this situation a "digital" input voltage is rapidly moving between levels that the PLD device considers high and low. (This is an external fault and it is assumed that this behavior persists long enough to affect a trip decision by the AV42.) The result is that the input appears to be high and low for brief periods, and in effect is seen as hovering between the two values. The PLD's other internal gates located in different parts of the PLD, seeing the rapidly changing input through circuitry between themselves and the input, might read the input value differently at any point in time. Then the internal logic can see two values for the same input—the internal logic sees one value of the input in one part of the logic and another value of the input in another part of the logic. For example, TRIP could be seen at the input of one AND gate, and NOT\_TRIP could be seen at the same time at the input of another AND gate. The result of this error is not predictable without knowing how the signals are arranged internally in the PLD.
- AREVA should indicate whether or not the above scenario is plausible, given the electronics of the PLD device used and if so, whether any of the tests that the AV42 has been subjected to envelop such a potential error. If such a scenario is plausible, but constitutes an undetectable error, how is it addressed at the system level in the application in which the AV42 is used?
- RAI-51 According to Fig. 4-4, the safety-related portion (i.e., PLD implementation) of the AV42 module is purely combinatorial. For combinatorial logic, there is a possibility of glitches occurring at the PLD outputs when the inputs are changing regularly. Also, any glitch at the inputs caused by interference, crosstalk, or electro static discharge (ESD) may propagate through the combinatorial logic and show up at the PLD outputs. These glitches may potentially have adverse effects on the actuators controlled by the PLD. The NRC has audited a portion of a test report performed by an independent testing agency (Technischer Ueberwachungs Verein (German Technical Surveillance Association) (TUEV). The report indicated that the firmware

was changed twice in earlier versions of the PLD due to errors that occurred during tests. The current firmware version passed the electromagnetic compatibility (EMC)/ESD tests. However, it is not clear whether these changes were made only to the test samples, to later versions of the AV42, or whether all AV42 modules — for example, those installed in the Atucha 1 plant in Argentina, for which claims of high reliability are made in the TR — also contain the latest firmware versions. AREVA should summarize the results of the EMC/ESD tests to address these concerns.

- RAI-52 ANP-10273P, Page 4-19, states, “Any hardware or data failure of a non-safety related data function or component does not affect the performance of the AV42 safety function. The safety function does not require input from the controller to perform the safety function.” However, there is a marginal probability that the nonsafety portion of the AV42 can affect the safety portion through increased power dissipation or increased probability of the ESD damage. These risks need to be evaluated. AREVA has performed environmental tests (e.g., circuit board temperature profiles as well as ESD tests) that address this issue but are not sufficiently documented in the TR. AREVA should summarize the results of tests performed to address this issue.
- RAI-53 Growth of tin whiskers in lead-free solder is especially critical for complex PLDs (CPLDs) due to the high pin count and the small pitch of the Pin Grid Array and Quad Flat packages. If lead-free solder is used during the module fabrication, the possibility of tin whisker growth and its potential effect on the performance of the CPLD and its ability to perform its safety function needs to be addressed. While the AV42 has been designed for application in mild environments, it is important to note that tin whiskers can grow in normal environmental conditions, and they grow with or without electric fields present. A discussion on tin whisker mitigation practices could be done by analysis or by actual tests. For example, Joint Electronic Devices Engineering Council (JEDEC) standard JESD22A121 addresses the test method for measuring whisker growth on tin and tin alloy surface finishes. Because there are currently no NRC guidelines on the tin whisker issue, AREVA may decide how they will address it (i.e., either by analysis or actual tests). It is also noted that tin whisker formation may not be an issue if AREVA does not use lead free solder (nor does it plan to use lead free solder in the future) in the fabrication of the AV42. Was lead-free solder used during the module fabrication of the AV42? Does AREVA foresee using lead-free solder in future module fabrication of the AV42? If so, the use of lead-free solder should be documented and mitigation strategies or non-applicability of the issue should be addressed in a formal response.
- RAI-54 ANP-10273P, Section 6.6, “Radiation,” (page 6-10, last paragraph), states, “the AV42 conforms to Regulatory Guide [RG] 1.89, [“Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants...]” However, RG 1.89 is for harsh environments, whereas the AV42 was designed to be used in a mild environment. Certainly the discussion in this section on radiation indicates that the AV42 was only analyzed for susceptibility to radiation levels in a typical benign environment, such as the control room, rather than a radiation-harsh environment, such as the containment. This implication that the AV42 meets RG 1.89 requirements should be deleted. It is the reviewer’s opinion that AREVA should

rather consider if the AV42 conforms to RG 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants."

RAI-55 ANP-10273P, Page 4-6, first paragraph, second sentence, states, "When the safety actuation command is in opposition to the PROFIBUS controller input, the priority portion of the logic is tested." AREVA should clarify what this sentence means.

RAI-56 Important findings of the failure modes and effects analysis (FMEA) are that the design does not result in any new failure modes, a single failure of an AV42 PLD will not affect the operation of other PLDs, and a failure within the PROFIBUS controller will not affect the safety functions. This section makes the following claims: "when installed in a plant specific redundant system, the failure of any AV42 component cannot prevent the system safety function from being correctly performed," and that the AV42 meets the requirements of IEEE 603 [IEEE Standard 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations] for this area." The implication is that the single-failure criterion (IEEE 603) for safety systems has been adequately addressed. However, completeness of the analysis is not provided. For example, have common cause failures (CCF) effects at the system level due to AV42s being (perhaps) used in redundant systems been evaluated? If the AV42 is employed as widely as its design allows, the following scenarios could occur:

1. It could be used in all parts of the plant, in all safety divisions and the control systems, so that common cause failures (CCFs) are a concern.
2. The AV42 would arbitrate all actuation inputs, so it is a single point of failure concern (like the actuator itself).
3. The design could have all AV42 modules (all actuators) in a plant connected to TXS systems in redundant divisions, as well as the TXP system(s), so that CCFs are a concern.

These scenarios highlight the need for an especially rigorous approach to reliability. Also, note that the report argues (see ANP-10273P, Section 4.11, page 4-22, paragraph 4) that the AV42 is a final actuation device and is therefore not subject to the diversity requirements of 10 CFR 50.62, "Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants," and therefore, can be used in both engineered safety features actuation system (ESFAS) and ATWS. If the scenarios enumerated above constitute plausible ways of using the AV42, a CCF could exist and the intent of 10 CFR 50.62 may be violated. AREVA should clarify the various practical ways of using the AV42 and the possibility of a CCF in the light of the discussions above.

RAI-57 The failure rate analysis (ANP-10273P, Section 7.2, page 7-1) predicts a mean time between failure (MTBF) of 127 years at 40°C (104°F) and a MTBF of 285 years at 35°C (95°F). The values provided are based on "a database of information for similar type of components." The conclusion is that the AV42 is highly reliable. For an independent assessment of the validity of the numbers provided in the report to be

made, AREVA should please discuss how identical are the AV42s used in the plants on which the data is based (e.g., identical versions of PLD, controller, other chips on the board, etc.)?

- RAI-58 ANP-10273P, Section 7.3, Operating History,” indicates that there are approximately 640 AV42 modules in operation. Was operating experience used to validate the numbers obtained using the “database of information for similar type of components ‘(Section 7.2, page 7-1)’?” The operating history also indicates that none of the failures of the 640 AV42 modules in operation affected the performance. Does this mean that failures were detected and the modules replaced? AREVA should provide more details to address these issues.
- RAI-59 The document’s view of cyber security threats (e.g., ANP-10273P, Section 4-7, second paragraph) is too narrowly focused to enable detailed “what-if” evaluations to be performed. For example, does the architecture of the PROFIBUS allow for external communications? The AV42 is a plant vulnerability if it has any flaw that could be exploited as part of a cyber attack. The flaw could be a design oversight resulting in a situation where malicious online modifications would not be necessary if a vulnerability already exists. The broader issue, in this case, is whether or not a design flaw exists that could be exploited via the TXP/ PROFIBUS connection. Verify that the PROFIBUS initiated functions of the AV42 priority logic module are accessible only through the operational instrumentation and controls system which is self-contained and not connected via two-way communication channels to outside networks.

cc:

Mr. Glenn H. Archinoff  
AECL Technologies  
481 North Frederick Avenue  
Suite 405  
Gaithersburg, MD 20877

Ms. Michele Boyd  
Legislative Director  
Energy Program  
Public Citizens Critical Mass Energy  
and Environmental Program  
215 Pennsylvania Avenue, SE  
Washington, DC 20003

Mr. Marvin Fertel  
Senior Vice President  
and Chief Nuclear Officer  
Nuclear Energy Institute  
1776 I Street, NW  
Suite 400  
Washington, DC 20006-3708

Mr. Ray Ganthner  
AREVA, Framatome ANP, Inc.  
3315 Old Forest Road  
P.O. Box 10935  
Lynchburg, VA 24506-0935

Mr. Paul Gaukler  
Pillsbury, Winthrop, Shaw, Pittman  
2300 N Street, NW  
Washington, DC 20037

Dr. Charles L. King  
Licensing Manager, IRIS Project  
Westinghouse Electric Company  
Science and Technology Department  
20 International Drive  
Windsor, CT 06095

Ms. Sherry McFaden  
Framatome NP, Inc.  
3315 Old Forest Road, OF-16  
Lynchburg, VA 24501

Mr. Steve Seitz  
AREVA  
100 Dean Road  
East Lyme, CT 06333

Mr. Robert E. Sweeney  
IBEX ESI  
4641 Montgomery Avenue  
Suite 350  
Bethesda, MD 20814

Mr. Gary Wright, Director  
Division of Nuclear Facility Safety  
Illinois Emergency Management Agency  
1035 Outer Park Drive  
Springfield, IL 62704

Email

APH@NEI.org (Adrian Heymer)  
awc@nei.org (Anne W. Cottingham)  
bennettS2@bv.com (Steve A. Bennett)  
bob.brown@ge.com (Robert E. Brown)  
BrinkmCB@westinghouse.com (Charles Brinkman)  
carey.fleming@constellation.com (Carey Fleming)  
chris.maslak@ge.com (Chris Maslak)  
cwaltman@roe.com (C. Waltman)  
david.hinds@ge.com (David Hinds)  
david.lewis@pillsburylaw.com (David Lewis)  
dlochbaum@UCSUSA.org (David Lochbaum)  
erg-xl@cox.net (Eddie R. Grant)  
frankq@hursttech.com (Frank Quinn)  
gcesare@enercon.com (Guy Cesare)  
greshaja@westinghouse.com (James Gresham)  
james.beard@gene.ge.com (James Beard)  
jcurtiss@winston.com (Jim Curtiss)  
jgutierrez@morganlewis.com (Jay M. Gutierrez)  
jim.riccio@wdc.greenpeace.org (James Riccio)  
JJD1@nrc.gov (John Donohue)  
JJNesrsta@cpsenergy.com (James J. Nesrsta)  
john.o'neil@pillsburylaw.com (John O'Neil)  
Joseph.savage@ge.com (Joseph Savage)  
Joseph\_Hegner@dom.com (Joseph Hegner)  
junichi\_uchiyama@mnes-us.com (Junichi Uchiyama)  
KSutton@morganlewis.com (Kathryn M. Sutton)  
kwaugh@impact-net.org (Kenneth O. Waugh)  
lynchs@gao.gov (Sarah Lynch - Meeting Notices Only)  
Margaret.Bennett@dom.com (Margaret Bennett)  
maria.webb@pillsburylaw.com (Maria Webb)  
mark.beaumont@wsms.com (Mark Beaumont)  
matias.travieso-diaz@pillsburylaw.com (Matias Travieso-Diaz)  
media@nei.org (Scott Peterson)  
mike\_moran@fpl.com (Mike Moran)  
mwetterhahn@winston.com (M. Wetterhahn)  
nirsnet@nirs.org (Michael Mariotte)  
patriciaL.campbell@ge.com (Patricia L. Campbell)  
paul.gaukler@pillsburylaw.com (Paul Gaukler)  
Paul@beyondnuclear.org (Paul Gunter)  
Petrovb@westinghouse.com (Bojan Petrovic)  
pshastings@duke-energy.com (Peter Hastings)  
RJB@NEI.org (Russell Bell)  
RKTemple@cpsenergy.com (R.K. Temple)  
roberta.swain@ge.com (Roberta Swain)  
rod.krich@constellation.com (Mr. Rod Krich)  
ronald.hagen@eia.doe.gov (Ronald Hagen)  
Ronda.Daflucas@areva.com (Ronda Daflucas)

sandra.sloan@areva.com (Sandra Sloan)  
sfrantz@morganlewis.com (Stephen P. Frantz)  
steven.hucik@ge.com (Steven Hucik)  
tkkibler@scana.com (Tria Kibler)  
tom.miller@hq.doe.gov (Tom Miller)  
trsmith@winston.com (Tyson Smith)  
VictorB@bv.com (Bill Victor)  
vijukrp@westinghouse.com (Ronald P. Vijuk)  
waraksre@westinghouse.com (Rosemarie E. Waraks)  
wayne.marquino@ge.com (Wayne Marquino)  
whorin@winston.com (W. Horin)