From: Getachew Tesfaye
To: DAFLUCAS Ronda M.
Date: 6/28/2007 8:08:33 AM
Subject: Draft RAIs for AV42 Module TR

Ronda,
Attached please find draft RAIs for the AV42 Priority Module Topical Report (ANP-10273P). 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: Eugene Eagle; george.pannell@areva.com; Norbert Carte; SLOAN Sandra M

Mail Envelope Properties (4683A4C1.36A : 24 : 8846)

Subject:	Draft RAIs for AV42 Module TR
Creation Date	6/28/2007 8:08:33 AM
From:	Getachew Tesfaye
Created By:	GXT2@nrc.gov

Recipients	**Action**	**Date & Time**
areva.com	Transferred	6/28/2007 8:09:02 AM
george.pannell CC (george.pannell@areva.com)		
Ronda.Daflucas (DAFLUCAS Ronda M.)		
Sandra.Sloan CC (SLOAN Sandra M)		
nrc.gov		
OWGWPO01.HQGWDO01	Delivered	6/28/2007 8:08:40 AM
NNC CC (Norbert Carte)	Opened	6/28/2007 8:46:20 AM
nrc.gov		
OWGWPO02.HQGWDO01	Delivered	6/28/2007 8:08:40 AM
EOE CC (Eugene Eagle)	Opened	6/28/2007 4:13:32 PM

Post Office	**Delivered**	**Route**
		areva.com
OWGWPO01.HQGWDO01	6/28/2007 8:08:40 AM	nrc.gov
OWGWPO02.HQGWDO01	6/28/2007 8:08:40 AM	nrc.gov

Files	**Size**	**Date & Time**
MESSAGE	1151	6/28/2007 8:08:33 AM
Draft RAI - AV42 Module TR.wpd	36397	6/28/2007 8:06:10 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

REQUEST FOR ADDITIONAL INFORMATION (RAI)

ANP-10273P, "AV42 PRIORITY ACTUATION AND CONTROL MODULE TOPICAL REPORT" (TAC NO. MD3867)

PROJECT NUMBER 733

RAI-01: The Code of Federal Regulations (CFR), in 10 CFR 50.62 (c)(1), requires "equipment from sensor output to final actuation device, that is diverse from the reactor trip system, to automatically initiate the auxiliary (or emergency) feedwater system and initiate a turbine trip under conditions indicative of an Anticipated Transient Without Scram (ATWS). Further, this equipment must be designed to perform its function and be independent (from sensor output to the final actuation device) from the existing reactor trip system."

IEEE Std 603-1991 defines an "actuation device" as "A component or assembly of components that directly controls the motive power (electricity, compressed air, hydraulic fluid, etc.) for actuated equipment. NOTE: Examples of actuation devices are: circuit breakers, relays, and pilot valves." The AV42 does not appear to directly control motive power; please confirm or refute. If Areva considers the AV42 to be part of an "assembly of components that directly controls the motive power," then please provide a complete description of that assembly of components.

A detailed description of any use of the AV42 for ATWS is necessary since 10 CFR 50.62 in essence requires that the two independent and diverse systems can not use common components, except for the final actuation device. The wording in the CFR is further clarified by the notes for consideration for the ATWS rule:

1) 49 FR 26038: "Since it has the potential for spurious trip of the reactor which reduces its value/impact it should be designed to minimize these impacts."
2) 49 FR 26042: "Equipment diversity to the extent reasonable and practicable to minimize the potential for common cause failures is required from the sensors to, but not including, the final actuation device–e.g., existing circuit breakers may be used for auxiliary feedwater initiation ... Electrical independence from the existing reactor trip system {is} Required from sensor output to the final actuation device at which point non-safety related circuits must be isolated from safety related circuits ..."
3) 49 FR 26043: "The design should be such that the frequency of inadvertent actuation and challenges to other safety systems is minimized ..."
4) 49 FR 26044: "future reactors ...significant additional reductions in the ATWS risk can be achieved without incurring insurmountable economic costs if such measures are considered during the design phase."

It is not clear how the AV42, as presented, can be used to meet this ATWS regulatory requirement. Please explain how the AV42 can be used to satisfy the ATWS regulation, and minimizes the potential spurious trips.

RAI-02: In the publically available material Areva identified one of the safety components as a "Programmable Logic Device (PLD)". This term has historically been used to refer to programmable devices that "consist of programmable AND arrays (product terms) and fixed fan-in programmable OR gates that are followed by flip-flops" (Reference 1). However, more recently PLDs have been used to refer to any field programmable device (Reference 2). Therefore, the public identification of this safety system device is ambagious. Areva, in the proprietary portion of the Topical Report (TR), did not identify the specific device, but rather only identified: 1) the manufacturer, 2) the type of memory used, and 3) the underlying architecture. There may be several families of components, produced by this manufacturer that use the identified memory and architecture. Areva has not identified the family of components actually used, let alone the specific component used. Please identify the specific PLD device used.

Functionally describe each PLD input and output, including inputs and outputs supporting test functions, and provide a detailed functional description or diagram of the logic within the PLD.

RAI-03: The AV42 topical report does not contain enough information to determine the number of inputs or outputs of the AV42 module, not to mention the function of each input or output. Please provide a list and detail description of each input and output. What is the function of each?

RAI-04: Figure 4-1, "AV42 Interfaces and Communications Links" shows communication from non-safety to safety and from safety to non-safety, as black arrows. **For non-Safety to Safety communication,** Section 4.8 contains a conceptual description of the control scheme. The AV42 TR does not contain a description of the number of inputs and outputs for performing this function, nor the functional meaning of each. Please provide sufficient details to allow the NRC staff to understand the function and arrive at an independent conclusion that the regulations and guidance for non-safety to safety communications are met. This needs to include, but is not limited to the logic design, what information is communicated, and how the safety function is protected.

RAI-05: The methods **for Safety to non-Safety communication** between the components of the AV42 is not explained in sufficient detail to allow the NRC staff to understand the function and arrive at an independent conclusion that the regulations and guidance for safety to non-safety communications are met. Please explain this interface and its functions in more detail.

RAI-06: Figure 4-4, "Priority Actuation and Control Logic example", shows inputs and outputs of the AV42 as black lines. It does not show what part of the logic or what components implemented these within the AV42. However, Section 4.1, "General," implies that at least some of the prioritization is done within non-safety software. The AV42 is an item that is designed and built and therefore information must be available. Figure 4-4 is the only representation of the logic contained within the

AV42. Please provide the design representation of the logic within the PLD and AV42 components, along with any documentation required to understand the design representation. Please provide several realistic examples of the logic similar to Figure 4-4 for actual equipment to allow sufficient understanding of the AV42.

RAI-07: Please provide details on the use of any simulation and testing features.

RAI-08: Please provide further details on any watchdog timers associated with the AV42.

RAI-9: The AV42 Topical Report (TR) seems to consider the AV42 to be an "execute feature". For example:

1) The Abstract of the AV42 TR says, "This report describes ... **the execute** features for actuation and driver devices ...".
2) The AV 42 TR Section 2.0, "Introduction" says : "This document provides the hardware design and licensing bases for the sense and command signal interface ... and the **execute feature** for actuation and driver devices to the safety-related components by using the AV42 priority actuation and control module. ... The AV42 prioritizes the various sense and command inputs and executes an output ...".
3) AV42 TR Section 8, "Conclusion", says: "In conclusion, the AV42 module provides the hardware design solution ... for ... the **execute feature** for actuation and driver devices ... to the safety-related actuation devices using the AV42 module.".

The AV42 contains complex decision logic and communication features, that per IEEE std 603-1991 definitions could categorize the AV42 as part of the sense and command features (See IEEE Std 603-1991 Figure 3 & Definitions section). The AV42 also performs other functions that are identified as sense and command features by IEEE 603.

The Areva conceptual implication will need to be clarified in order to prevent misinterpretations of this topical report in the future. This interpretation is important since IEEE 603 Section 6 contains requirements for sense and command features, and Sections 5.2 and 7 contain requirements for execute features. This interpretation will determine which requirements the AV42 will be checked against, or if both sets will be used. Explain and justify this apparent dual functionality.

RAI-10: IEEE Std 603-1991, Sections 5.2 and 7.3 contain requirements for completion of protective action. Section 7.3 says, "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." However, there does not seem to be any documentation that the AV42 actually does not automatically return to normal. Please explain how the requirements of IEEE Std 601-1991 Sections 5.2 and 7.3 are satisfied for automatic, manual, and diverse initiations of the protective action.

RAI-11: Section 4.6, "Implementation," 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." Please clarify what is meant by the phrase: "the components as a whole". Is this statement saying that the AV42 has been tested to satisfy the requirements of IEEE Std 603-1991 Sections 5.2 and 7.3, "Completion of Protective Action."? Does this basically say the AV42 does not satisfy IEEE Std 603-1991 Sections 5.2 and 7.3, but the System will satisfy IEEE Std 603-1991 Sections 5.2 and 7.3? Therefore, does this place requirements on the inputs (i.e. TXS, manual controls, ...)? Please identify where the associated requirements on the other components, used to satisfy Sections 5.2 and 7.3, are documented. This appears to be one case where a statement in the AV42 places requirements on the context in which the AV42 would be implemented. Please identify all of the non-AV42 components and the associated requirements imposed on them, in the AV42 implementation context, in order to make statements in this topical report true.

RAI-12: The Abstract of the topical report says: "The AV42 module processes commands from all areas (e.g., inputs received from safety and non-safety-related instrumentation and control systems, the main control room and remote shutdown station). The AV42 module is designed for use in any safety-related or non-safety-related system." GDC 24 says: *"Criterion 24--Separation of protection and control systems.* The protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems **shall be limited** so as to assure that safety is not significantly impaired." Section 4.8 of the AV42 topical report addresses GDC 24, but is silent on the requirement imposed by the last sentence, and the abstract seems to imply no limitations. Please provide more information sufficient to justify how the AV42 meets the requirements of GDC 24.

RAI-13: The AV42 TR mentions that the AV42 module can be configured, in various ways, for use with different types of actuators and equipment, but does not provide any details on possible or allowable configurations. Please provide detail information for each allowable configuration, for each controlled component, and the processes to ensure the proper implementation of the allowable configurations.

RAI-14: Section 4.2, "General," says: "The AV42 design meets the manual and automatic

actuation requirements of both IEEE 279 and IEEE 603 and the guidance provided in Regulatory Guide 1.62." It is not clear how the AV42 meets the requirements without a description of how the AV42 is used (i.e. wired & configured). Please provide sufficient details on how the AV42 is used to allow verification that the requirements are met.

RAI-15: Section 4.4, "Testing" says: "The testing configuration of the AV42 follows the guidance provided in Regulatory Guides 1.118 ...". Regulatory Guide 1.118 endorses IEEE Std 338-1987, which says: "The safety systems shall be designed to be testable during operation of the nuclear power generating station as well as during those intervals when the station is shut down. This test ability shall permit the independent testing of redundant channels and load groups while (1) maintaining the capability of these systems to respond to bona fide signals, or (2) tripping the output of the channel being tested, if required, or (3) bypassing the equipment consistent with safety requirements and limiting conditions for operation." Please explain how the last sentence in the proprietary material on page 4-7 addresses these requirements.

RAI-16: Since some information from the AV42 is provided though the non-safety system, please explain why the status of safety related components can be conveyed through only the non-safety system. The acceptability of this aspect can only be made after a system level analysis. Please provide information that will provide assurances that the "non-safety' information will not be used for decision purposes in safety systems, or provide a justification for such use. If some of the information is required by safety system logic, how will it get there?

RAI-17: The AV42 TR has concluded that components in the AV42 will ensure that the non-safety connection will not inhibit the ability of the safety system to initiate protective actions, but the AV42 TR has not provided sufficient information to verify this nor does it explain in detail how spurious actuations from the non-safety side are avoided. Please provide sufficient details to permit the staff to reach the same conclusions.

RAI-18: The AV42 is design to control certain types of components. The configured functionality for each type of component controlled is presumably known. The failure modes of the AV42 are also presumably known. Therefore the affect of each AV42 failure mode on each type of component can be described. Subsequent, plant specific Failure Modes and Affects Analysis (FMEA) could then determine if the failure mode or each controlled component is in fact safe. Is the failure mode of the AV42 configurable?

In *10 CFR 50 Appendix A:* "*Criterion 23--Protection system failure modes.* The protection system shall be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced." Please describe how it is, or will be, assured that the AV42 will fail into a safe state.

Section 3.0 says, "The AV42 design meets the applicable requirements of NRC General Design Criteria (GDC) ... 23 ...". The licensing Topical Report did not describe the failure modes of the AV42. (See 10 CFR 50 Appendix A GDC 23, NUREG-0800 Chapter 7 Section 7.9, and NUREG-0800 Chapter 7 Appendix 7.1-A: "Criterion 23 — Protection System Failure Modes ... Applicability — The protection systems, RTS, ESFAS, and supporting data communication systems.") The AV42 TR did provide a summary of the conclusions reached (See Section 7.1) and some rational (e.g. "engineering judgement"), but not enough information for the NRC to assess these conclusions, nor to reach them independently. Please provide further information to allow the NRC to independently reach the conclusion that the AV42 meets these requirements. Describe AV42 failure modes and the effect upon safety actuation.

RAI-19: Section 4.2, "Functions", says, "The AV42 has the ability to block all non-safety inputs". Please provide further details that sufficiently describe this function, any hardware controls and their location, and indicate what circumstances are envisioned to require its use.

RAI-20: IEEE Std 603-1991 defines "actuation device" and "actuated equipment". The AV42 TR Abstract says, "This report describes the design features of selected signals from safety-related Class 1E main control room **actuators**, remote shutdown station **actuators** ..." (Note: Section 1.0, "Executive Summary," uses the term "actuators" in the same way.) Confirm that the AV42 TR term "actuators" has the same definition as the IEEE Std 603-1991 defined "actuation device". If these terms do not have the same meaning, please define or describe what is meant by "actuators" in the AV42 TR context.

RAI-21: The AV42 TR Abstract says, "This report describes the design of the AV42 module and **demonstrates how the AV42 module complies to** Class 1E equipment design, qualification, and quality criteria as well as **criteria for** the prioritization of Engineered Safety Features Actuation System (ESFAS) signals and **for the electrical separation and independence of redundant systems.**" Please explain in more detail how this report demonstrates that the AV42 complies to the criteria for electrical separation and independence of redundant systems.

RAI-22: Section 4.7 says, "Section 6.7 discusses the evaluation further". There is no Section 6.7. Please correct, or provide the complete missing Section 6.7.

RAI-23: Section 3.0: "Section 4.3 discusses the capability for testing and calibration considered during the design." However, Section 4.3 is titled "Operations". Section 4.4 is titled "Testing". Please clarify.

RAI-24: The AV42 has the capability to be connected to a non-safety network. It is not clear from the description if: 1) each AV42 is connected to a single node (e.g. a point to

point network), 2) all AV42s in one safety division are connected to the same non-safety network, or 3) there is only one non-safety network that all AV42s are connected to. Please clarify the intended configuration. If multiple AV42s are connected to one non-safety network, then please provide any design criteria governing a set of allowable connected components.

RAI-25: In NUREG-0800 Chapter 7, Section 7.9: "A particular concern is that the transmission of multiple signals over a single path may constitute a single point of failure that may have a larger impact on plant safety than would occur in previous analog systems." Is the non-safety network a mono-master or a multi-master network? Please provide further details on the non-safety network with respect to Section 7.9 guidance.

RAI-26: Figure 4-3, "AV42 Module Application," seems to be incorrect or incomplete. Please provide a complete or corrected figure.

RAI-27: Figure 4-4, "Priority Actuation and Control Logic Example," seems to be in incorrect or incomplete. Please provide a complete or corrected figure.

RAI-28: Section 4.3 mentions the use of soft non-safety controls to issue commands and messages through the network. Please describe the message and data scheme to send these commands and include figures as required.

RAI-29: Describe the process for accepting any software tools used to assure the quality of the design and implementation of the AV42.

RAI-30: Section 4.6 says, "Manual controls enable the operator to initiate protective actions at the system level as well as the individual level". Please describe these design details and provide examples.

RAI-31: Describe the process for identifying and addressing any known issues with the AV42 components and programming tools. What significant issues were identified?

RAI-32: Section 4.3 mentions switching from the MCR to the RSS. Please provide further details on the process, methods, and hardware used.

RAI-33: Describe any provisions for ensuring the integrity (i.e., messages were not corrupted in transmission) and validity (i.e., messages belong to the set of legitimate messages) of messages passed between the non-safety and the safety portions.

RAI-34: Describe any provisions for ensuring the authenticity (i.e., messages originated from an expected network location) of messages passed.

RAI-35: Describe the AV42 response when field components do not respond to a control signal. For example, is the command sent until it is accomplished (e.g. closed loop control vs open loop control)? Does the AV42 store the command until either it is accomplished or withdrawn? Can memory of commands sent, but not completed result in unexpected action of field components when a safety actuation signal is reset (e.g. non-safety command causes component to change state when safety command is reset)?

RAI-36: Section 4.10 mentions one technique as a protective measure against the wrong module configuration being used during maintenance. Please provide a detail description of this, or additional schemes, used as protective measures.

RAI-37: Section 4.4 describes testing. Are these test automated or only manually initiated? Are there any other self-test associated with the AV42?

RAI-38: Are there any potential AV42 common cause failures that could result in spurious actuation of multiple ESF functions? If so describe such failures and any corrections.

RAI-39: In Section 4 Figure 4-3 uses a number of standard drawing symbols, but others need to be defined for clarity. Please provide a legend for the symbols and abbreviations used in Figure 4-3.

RAI-40: Since the AV42 has a network connection that is in compliance with a subset of the internet standards, please explain how, when the AV42 is connected to a internet compliant network, spurious activations are minimized.

RAI-41: In Section 4.4 the testing of lamps is discussed. Please provide further information on how this function operates and is accomplished with the AV42.

RAI-42: Describe and list any reference documents provided by Areva specific for the AV42 that provide guidance, requirements, and sample procedures for customers that plan to use the AV42 that will aid the customer in developing site specific procedures: 1) to prevent unauthorized or incorrect reconfiguration via the non-safety network; 2) to prevent assigning a AV42 to a function different than the one for which is configured; and 3) to prevent improper configuration of a AV42 in the field.

RAI-43: If fiber optic modems are used, will fiber optic ports of the fiber optic modems physically contain only a transmitter or receiver or will they contain optical transceivers which have been configured to perform only one or the other function? If

these ports are to contain transceivers, describe provisions to prevent reconfiguration.

RAI-44: Describe the response of the non-safety systems to receipt of corrupt, invalid, unauthentic, late, out of sequence, or no messages from the network.

RAI-45: Describe how priority of diverse actuation system commands over soft control commands is assured, for motor operated valves.

RAI-46: Section 4.4 discusses testing of the AV42 Module. Please provide an outline of the key steps of a typical procedure for periodic manual testing for personnel to accomplish this testing.

RAI-47: Please provide further details on any self-testing capability of the AV42 and its involvement with the system during such testing.

RAI-48: The topical report mentioned various types of actuators that can be controlled by the AV42. The AV42 can be configured in several ways. The valid configurations of the AV42 for each type of actuator controlled is not provided. No description was provided how the AV42 would fit into the arrangement of components that would be required to control each actuator type. Please provide information on other components required between the AV42 and the various actuators discussed, and the valid configurations of the AV42 for each actuator type and control mode.

References

1. "Digital Design Using Field Programmable Gate Arrays" Pak K. Chan / Samiha Mourad, PTR Prentice Hall, 1994
2. "Architecture of FPGAs and CPLDs: A Tutorial", Stephen Brown and Joanathan Rose, Department of Electrical and Computer Engineering, University of Toronto.