



December 21, 2007
NRC:07:079

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

Response to Requests for Additional Information Regarding ANP-10273P, "AV42 Priority Actuation and Control Module Topical Report" (TAC MD3867)

- Ref. 1: Letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), "Request for Review and Approval of ANP-10273P, 'AV42 Priority Actuation and Control Module Topical Report'," NRC:06:054, November 28, 2006.
- Ref. 2: Letter, Getachew Tesfaye (NRC) to Ronnie L. Gardner (AREVA NP Inc.), "Request for Additional Information Regarding ANP-10273P, 'AV42 Priority Actuation and Control Module Topical Report (TAC MD3867)'," July 30, 2007.
- Ref. 3: Letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), "Request for Additional Information Regarding ANP-10273P, 'AV42 Priority Actuation and Control Module Topical Report (TAC MD3867)'," NRC:07:045, August 30, 2007.
- Ref. 4: Letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), "Response to a Request for Additional Information Regarding ANP-10273P, 'AV42 Priority Actuation and Control Module Topical Report (TAC MD3867)'," NRC:07:050, September 19, 2007.
- Ref. 5: Letter, Getachew Tesfaye (NRC) to Ronnie L. Gardner (AREVA NP Inc.), "Second Request for Additional Information Regarding ANP-10273P, 'AV42 Priority Actuation and Control Module Topical Report (TAC MD3867)'," November 1, 2007.

AREVA NP Inc. (AREVA NP) requested the NRC's review and approval of topical report ANP-10273(P), "AV42 Priority Actuation and Control Module Topical Report" in Reference 1. A request for additional information (RAI) was provided by the NRC in Reference 2. An extension to the RAI response was requested in Reference 3. Subsequently, a partial response to the RAI was provided in Reference 4. The responses to the remaining RAIs in References 2 and 5 are provided in Attachment A to this letter.

AREVA NP considers some of the material contained in the attachments to this letter to be proprietary. As required by 10 CFR 2.390(b), an affidavit is enclosed to support the withholding of the information from public disclosure. Proprietary and non-proprietary versions of the responses are enclosed with this letter.

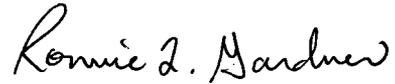
AREVA NP INC.
An AREVA and Siemens company

3315 Old Forest Road, P.O. Box 10935, Lynchburg, VA 24506-0935
Tel.: 434 832 3000 - Fax: 434 832 3840 - www.aveva.com

DO77
NRO

If you have any questions related to this submittal, please contact Ms. Sandra M. Sloan, Regulatory Affairs Manager for New Plants Deployment. She may be reached by telephone at 434-832-2369 or by e-mail at sandra.sloan@areva.com.

Sincerely,



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

Enclosures

cc: L. J. Burkhart
G. Tesfaye
Project 733

accordance with 10 CFR 2.390. The information for which withholding from disclosure is requested qualifies under 10 CFR 2.390(a)(4) "Trade secrets and commercial or financial information."

6. The following criteria are customarily applied by AREVA NP to determine whether information should be classified as proprietary:

- (a) The information reveals details of AREVA NP's research and development plans and programs or their results.
- (b) Use of the information by a competitor would permit the competitor to significantly reduce its expenditures, in time or resources, to design, produce, or market a similar product or service.
- (c) The information includes test data or analytical techniques concerning a process, methodology, or component, the application of which results in a competitive advantage for AREVA NP.
- (d) The information reveals certain distinguishing aspects of a process, methodology, or component, the exclusive use of which provides a competitive advantage for AREVA NP in product optimization or marketability.
- (e) The information is vital to a competitive advantage held by AREVA NP, would be helpful to competitors to AREVA NP, and would likely cause substantial harm to the competitive position of AREVA NP.

The information in the Document is considered proprietary for the reasons set forth in paragraphs 6(b), 6(c), 6(d), and 6(e) above.

7. In accordance with AREVA NP's policies governing the protection and control of information, proprietary information contained in this Document have been made available, on a limited basis, to others outside AREVA NP only as required and under suitable agreement providing for nondisclosure and limited use of the information.

8. AREVA NP policy requires that proprietary information be kept in a secured file or area and distributed on a need-to-know basis.

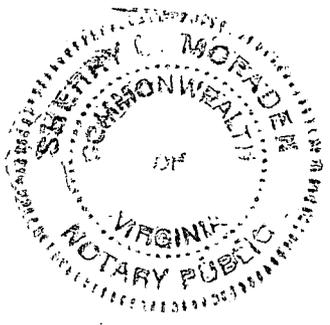
9. The foregoing statements are true and correct to the best of my knowledge, information, and belief.

George Marshall

SUBSCRIBED before me this 20th
day of December, 2007.

Sherry L. McFaden

Sherry L. McFaden
NOTARY PUBLIC, COMMONWEALTH OF VIRGINIA
MY COMMISSION EXPIRES: 10/31/2010
Registration #7079129



**Response to Request for Additional Information – ANP-10273P
“AV42 Priority Actuation and Control Module Topical Report” (TAC No. MD3867)**

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.

Response 01:

The AV42 does not directly control motive power. It is not considered an actuation device.

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).

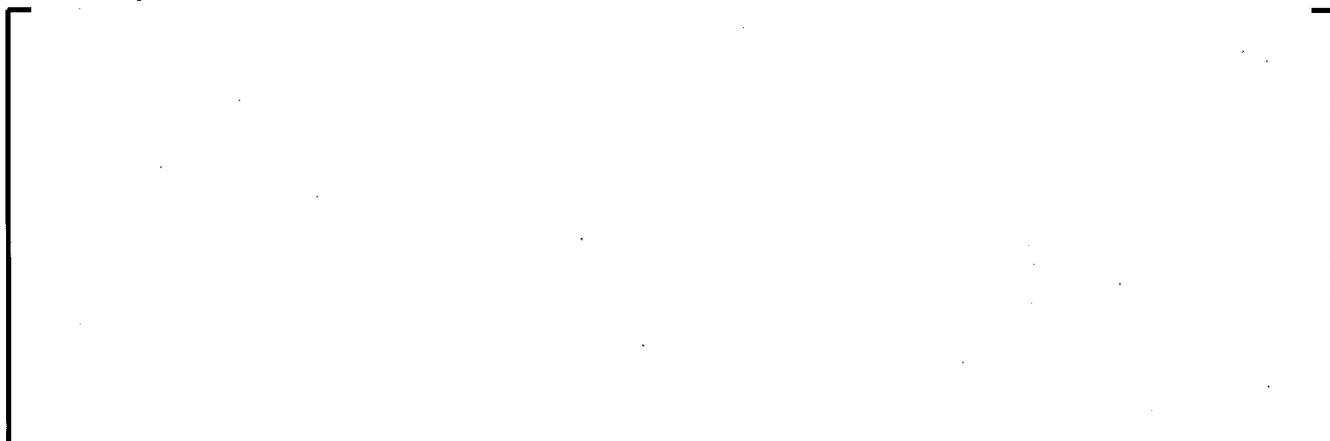
The AV42 is not used in any reactor trip functions. It can be used to satisfy 10 CFR 50.62 (c) (1).

For conditions indicative of an ATWS, the U.S. EPR Diverse Actuation System (DAS), a subsystem of the Operational I&C Process Automation System (PAS) will initiate the Emergency Feedwater System (EFW) either via the Profibus DP interface with the Priority and Actuator Control System (PACS) or via hardwiring to the PACS. Since PACS is implemented using the AV42, a diverse means is established to initiate EFW under ATWS conditions. Moreover, since the AV42 is a non-computerized based device, it is not subject to software-related common cause failure and provides a diverse actuation path for functions credited in diversity and defense-in-depth analyses (D3).

RAI 02: *In the publicly 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 ambiguous. 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.

Response 02:



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.*

Response 06:

[Empty response area]

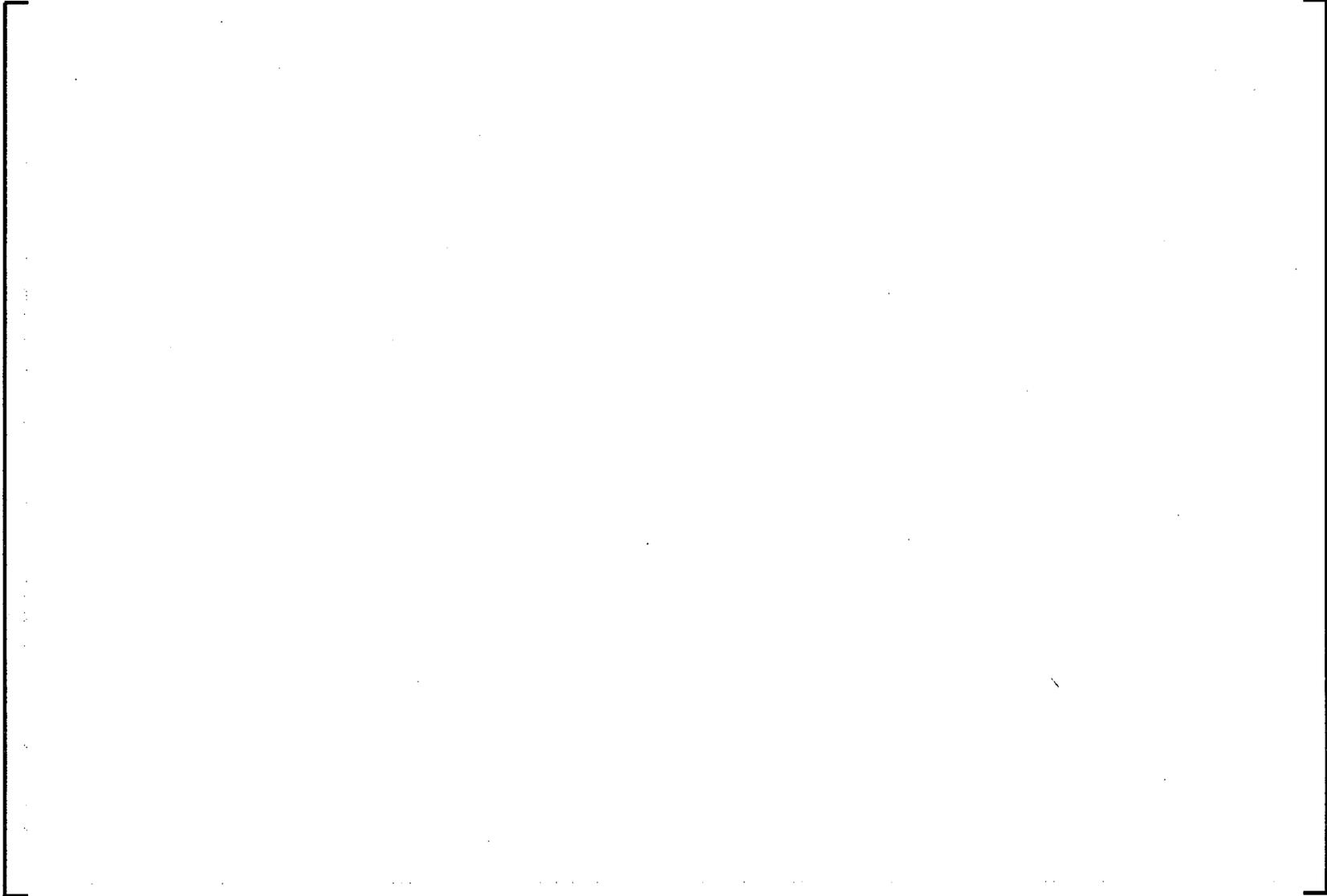


Figure 06-1: Example excerpt of Detailed Design Specification

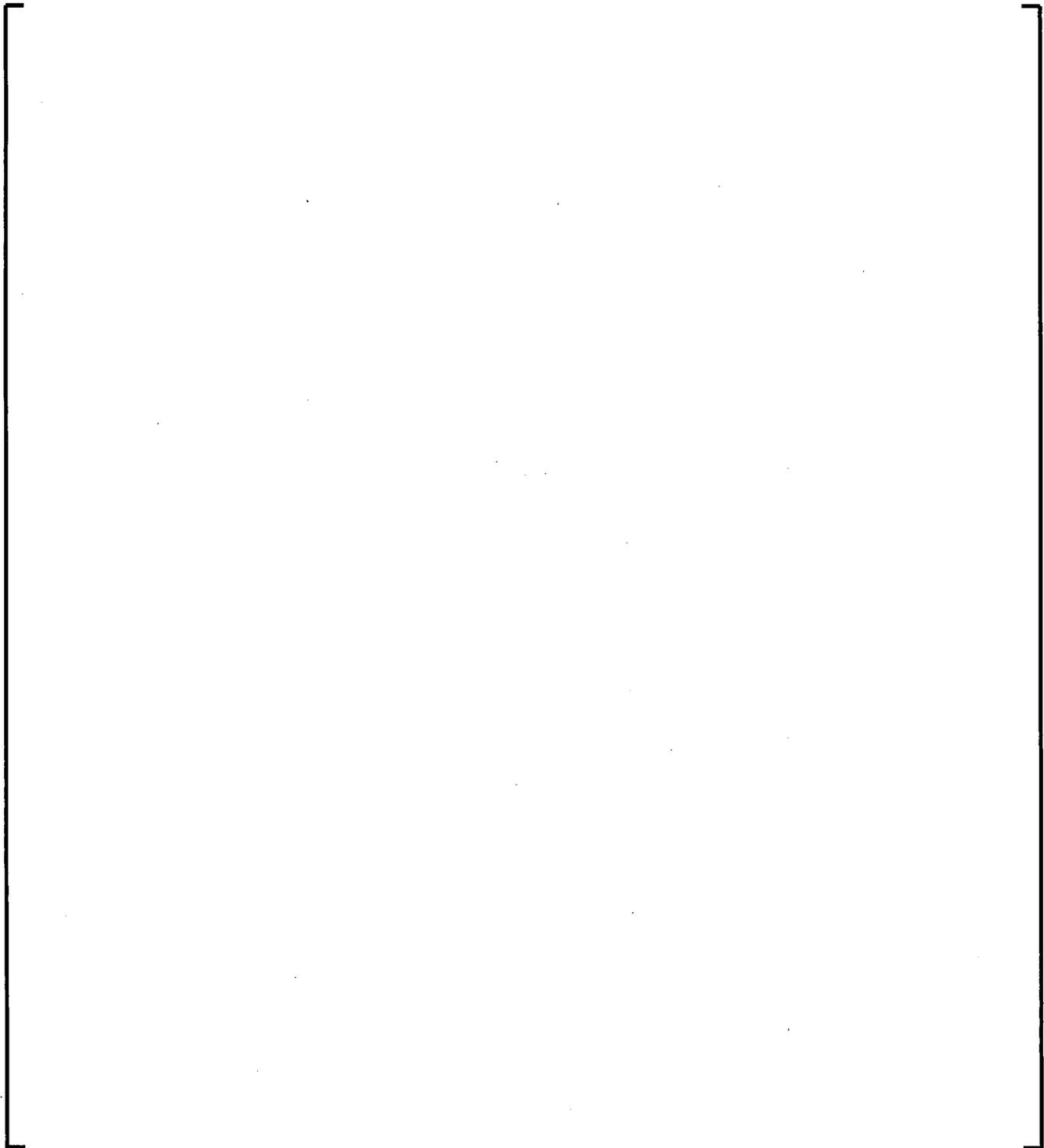
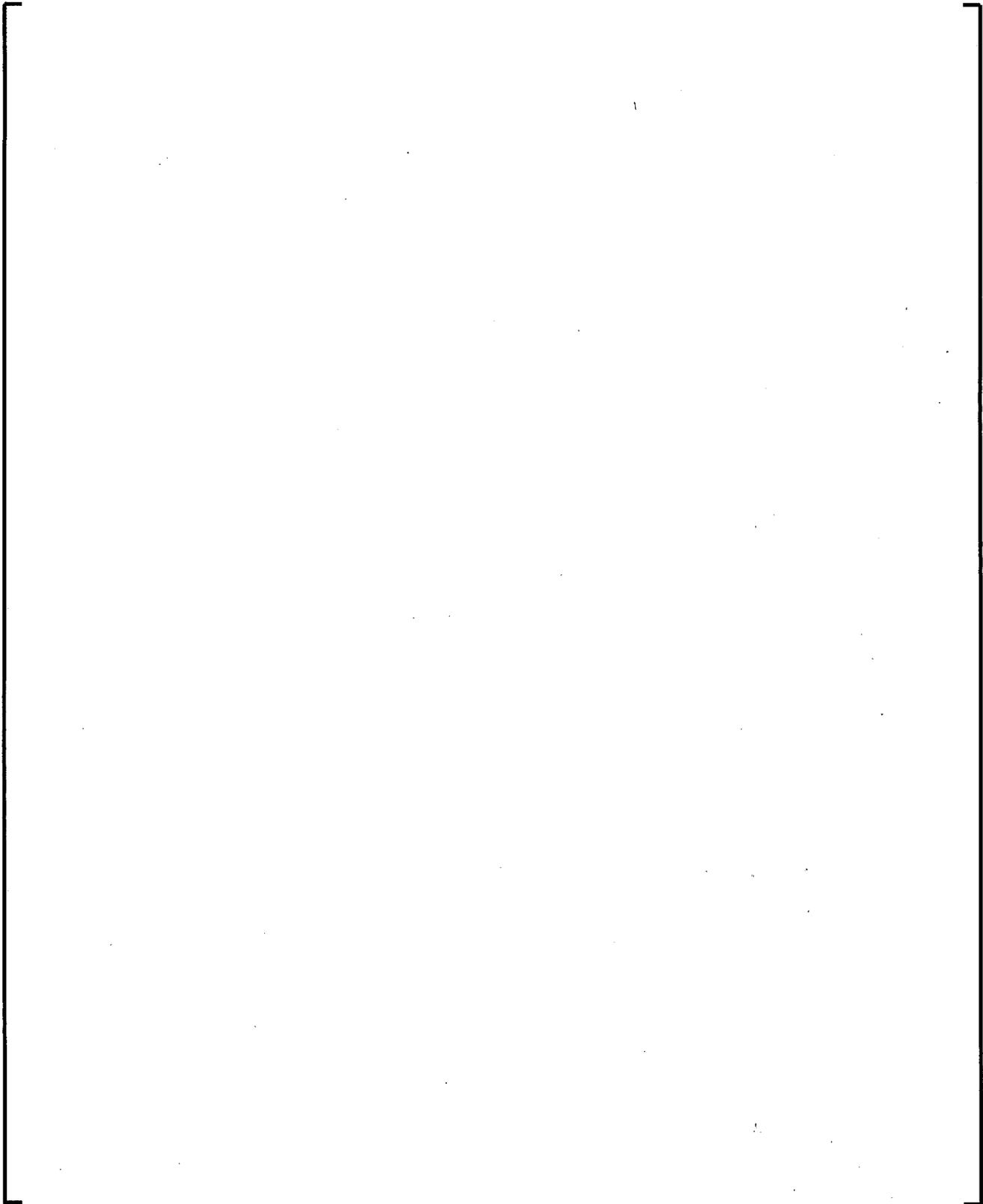


Table 06–1: Prioritization of operational commands for ON/OFF actuators for motor drives or solenoid valves (1 = highest priority, 6 = lowest priority)

Command Type	Priority
Undervoltage protection OFF	1
Mechanical Equipment Protection commands	2
Commands from automatic control system	3
Manual commands from desktile	4
Manual command from the OM	5
Automatic restart after undervoltage	6

Table 06–2: Prioritization of operational commands for open-loop-controlled actuators and closed-loop-controlled actuators in “Manual/open-loop” control mode (1 = highest priority, 5 = lowest priority)

Command Type	Priority
Countermanding manual commands	1
Mechanical Equipment Protection commands	2
Commands from automatic control system	3
Manual commands from desktile	4
Manual command from the OM	5



4. Signal SFEN (Pin F02) blocks all commands from the operational I&C (via Profibus DP) and from the desktils. This makes it possible to prevent a change in status of safety actuators, if required under certain conditions.

RAI 09: *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.

Response 09:

The statements listed above and as listed in the Abstract and sections 2.0 and 8.0 of the AV42 Topical Report incorrectly imply that the AV42 is part of the execute features for a safety function.

According to the definitions presented in IEEE 603-1991, the AV42 module is part of the sense and command features for a safety function. The AV42 prioritizes the actuation requests for a single actuator from the various control systems and produces an actuation output that reflects the plant licensing requirements and operational preferences. The response to RAI 20 also contains more information on sense and command features.

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.

Response 10:

Per IEEE 603-1991 section 5.2, 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 7.3 states that when the sense and command features reset, the execute features shall not automatically return to normal; they shall require separate, deliberate operator action to return to normal.

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.

Response 11:

"The components as a whole" indicates the components that are required to complete a protective action (TXS processors, manual initiation devices, AV42, etc.), as they are implemented within the U. S. EPR architecture, satisfy the requirements of IEEE 603-1991. The four sentences of Section 4.6 leading up to the statement listed above explain the intent of the statement "the components as a whole."

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.

Response 12:

The AV42 provides an interface for protection and control within a single division. The functions of the PLD are classified as safety related and the functions of the Profibus Controller are classified as non-safety related. The PAC module is qualified as a Class 1E device. It complies with IEEE 603-1991 for safety systems and IEEE 384-1992 for associated circuits. Therefore, the AV42 module has been designed and qualified for safety applications to prevent control system and safety function interaction. In addition, the overall U. S. EPR architecture incorporates four redundant, independent safety system divisions, each of which is capable of accomplishing a given safety function.

The interface on the AV42 is designed to assure that safety is not significantly impaired, by requiring qualification of the Profibus Controller as an associated circuit. Signals exchanged between the PLD and Profibus Controller are not protocol or network based communications. A safety signal always has priority over any control commands sent via the Profibus Controller and the safety PLD functions are not dependent on Profibus DP communications.

Also, the AV42 complies with GDC 24 in that any failure of the non-safety functions within the Profibus Controller does not cause a failure of the safety function within the PLD.

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.*

Response 13:

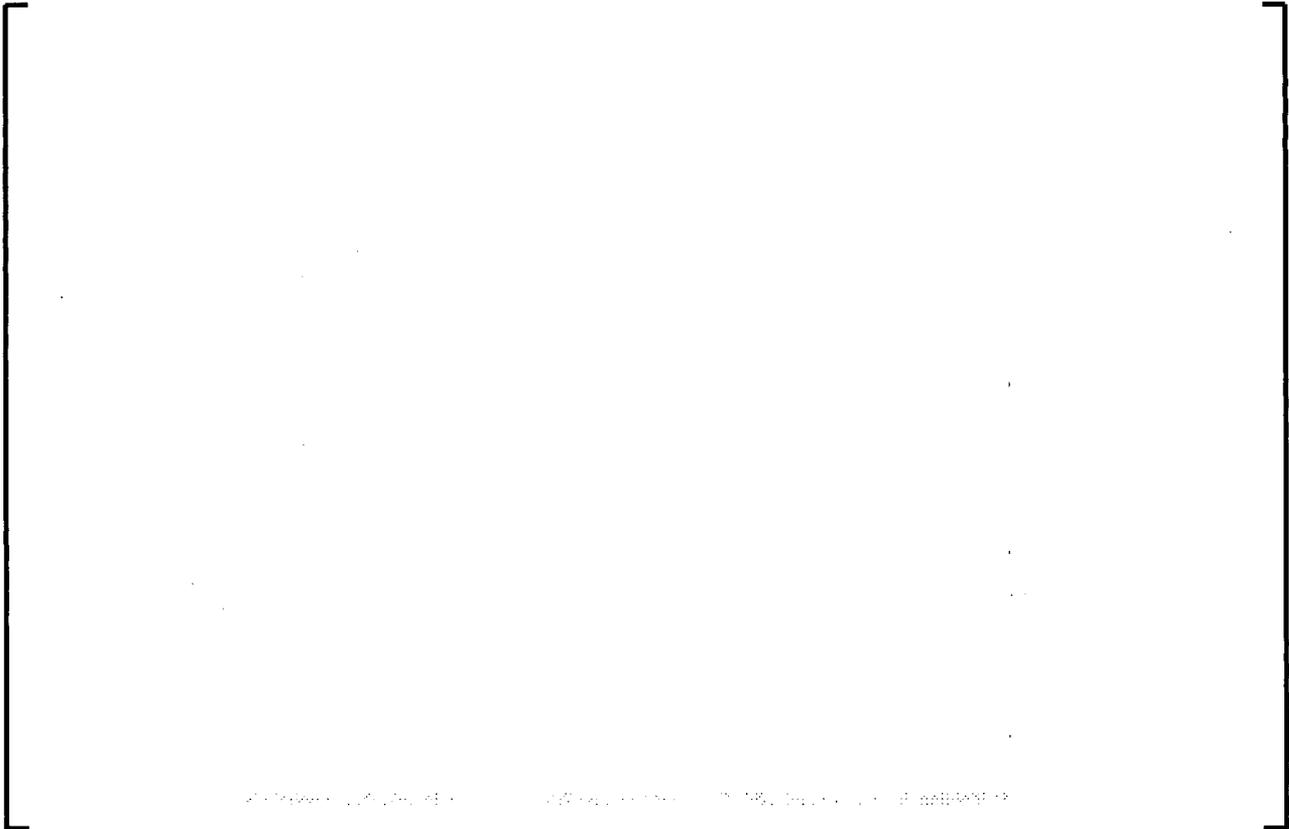
The AV42 module can be used to control the following types of actuators and drives:

- Solenoid Valves
- Motors (for pumps, fans, etc.)
- Open-loop controlled actuators (for isolation valves)
- Closed-loop controlled actuators (control valves)



Since the possible configurations for the AV42 are numerous and not specified until the detail design phase for each plant, providing information on each allowable configuration is not appropriate at this time. However, two "typical" arrangements are listed below for examples. More information is available in Section 4.0 of the AV42 User Manual Version 2.1. This manual is available for review at any time.

A description of the inputs and outputs is found in the response to RAI 03.



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.

Response 14:

Regulatory Guide 1.62 Section C states that "1.) means should be provided for manual initiation of each protective action at the system level regardless of whether means are also provided to initiate the protective action at the component or channel level..., 2.) manual initiation of a protective action at the system level should perform all actions performed by automatic initiation..., 3.) the switches for manual initiation of protective actions at the system level should be located in the control room....."IEEE Std. 279-1971 also indicates that no single failure shall prevent initiation of each protective action.

Clause 6.2.1 of IEEE 603-1991 states that "means shall be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions..."

The AV42 is used to operate safety I&C systems to meet the requirements stated above.

Manual system level actuation commands are sent to the safety system and outputs are generated from one of the safety systems via input pins SFON1, SFOFF1, SFON2, SFOFF2.

The AV42 processes these inputs at the same priority as automatically actuated inputs from the safety system; that is they are the highest and second highest set of inputs to the device.

To prevent a single failure of an AV42 from preventing completion of a safety function, system level redundancy is implemented to ensure the safety function is accomplished. The U. S. EPR system and I&C architecture incorporate four 100% independent divisions for safety functions.

The AV42 alone does not satisfy the requirements listed above; however, the AV42 is designed to meet the requirements stated above when implemented within the overall I&C architecture that meets the requirements for manual system level actuation. For more information on manual system level actuation and how the U. S. EPR I&C architecture meets the requirements listed above, please see RAI 16 & RAI 18 responses to the U. S. EPR Protection System Topical Report ANP-10281P.

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.*

Response 15:

The last sentence of the proprietary material on page 4-7 states "During this test, any actual safety and non-safety commands received will be executed immediately following the termination of the test."



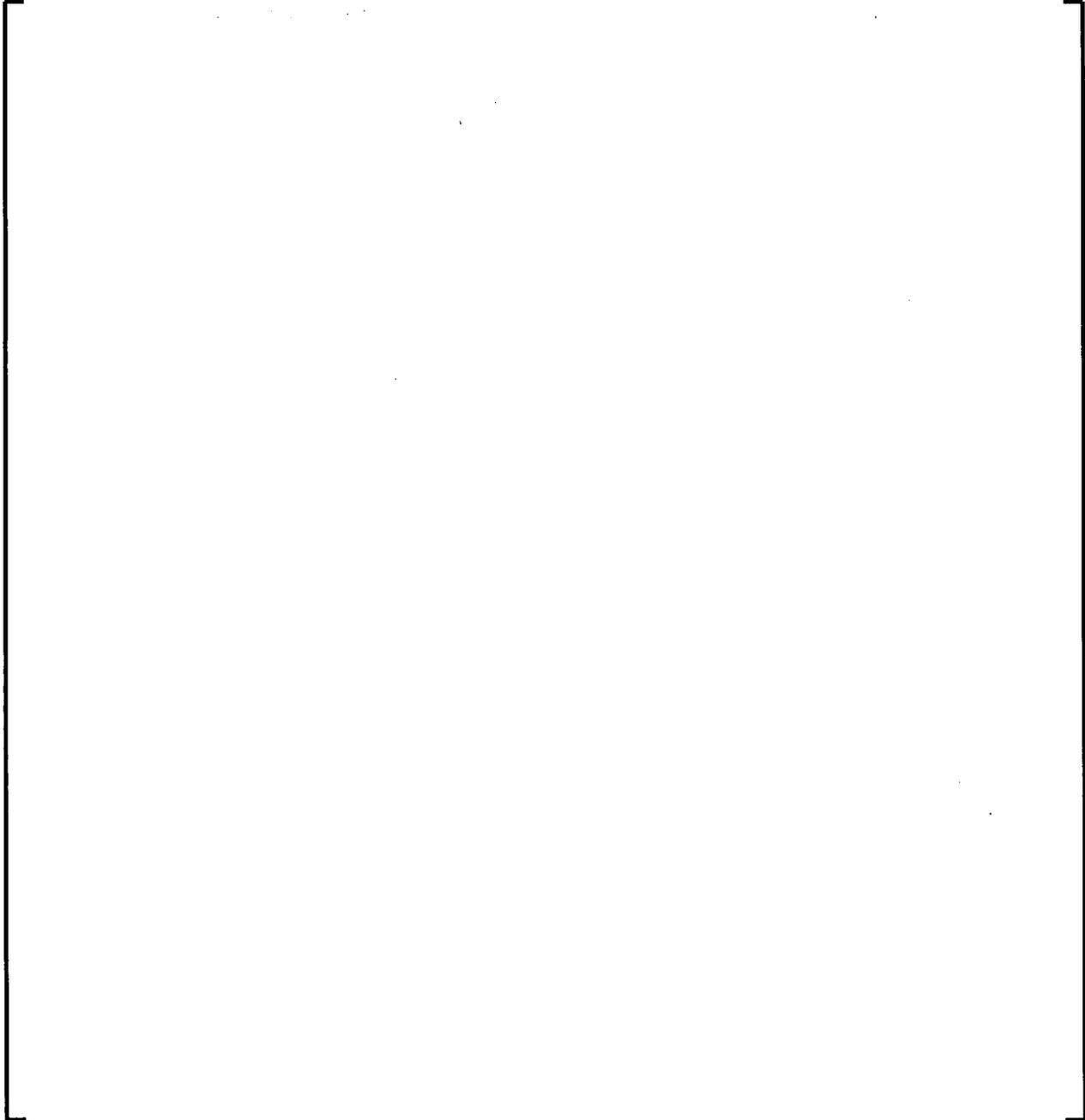


Figure 15-1: Protection System Test Initialization Logic

The overlapping test will always be initiated under control of an Operator.

As indicated in Figure 15-1, the test provisions are implemented in such a way that in case of an actuation request, the overlapping test is immediately stopped and the actuation request is performed.

RAI 16: *Since some information from the AV42 is provided through 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?*

Response 16:

The AV42 provides status information in the following two ways:

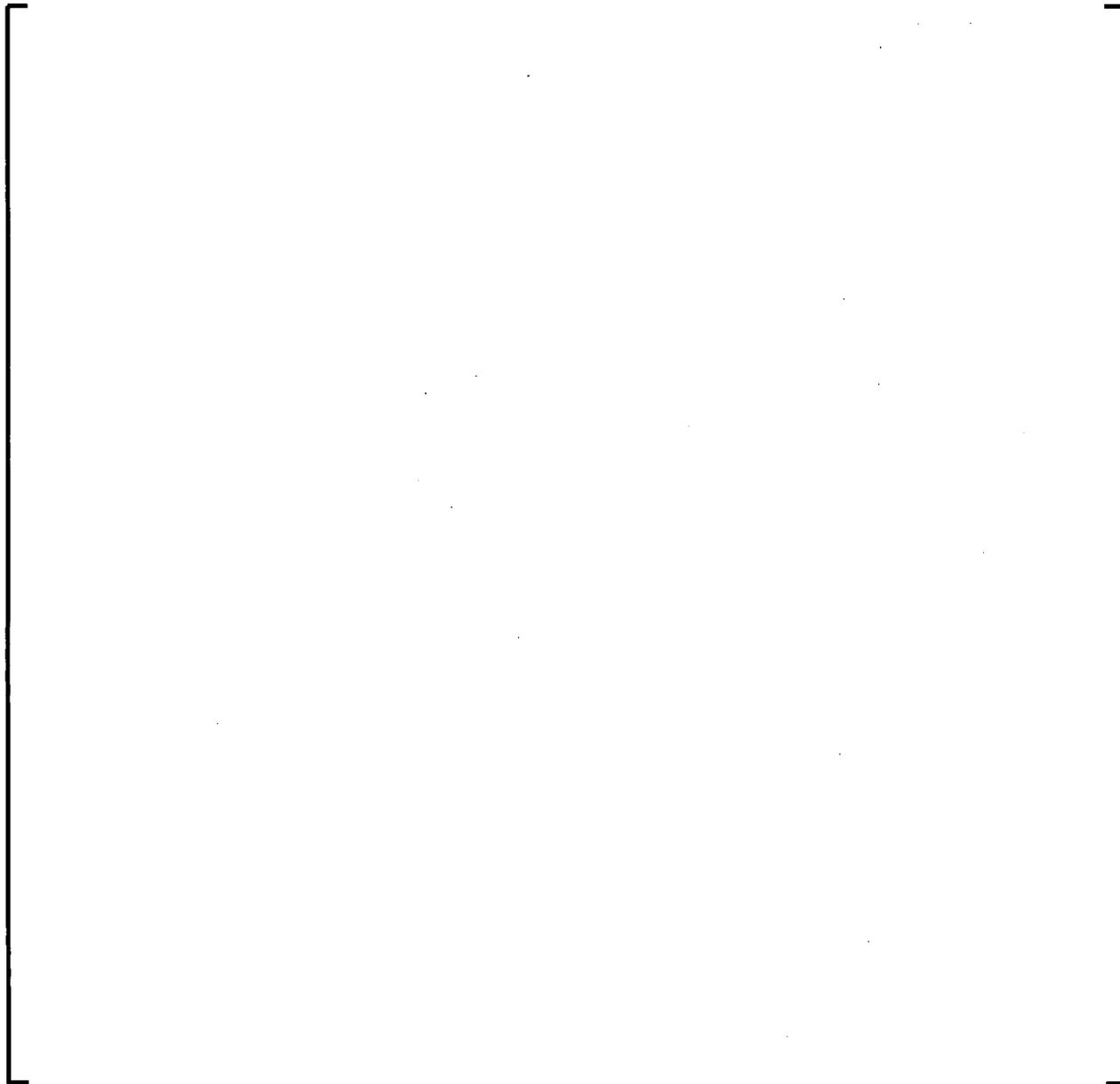




Figure 16-1
U. S. EPR functional representation of status signal outputs from AV42.

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.*

Response 17:

The AV42 ensures that non-safety commands can not block safety I&C commands by appropriately designed priority logic and interlocks. The principles for the priority handling between safety and non-safety commands are explained in detail in the response to RAI 06.



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 effect 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 rationale (e.g. "engineering judgment"), 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.

Response 18:

The failure mode of the AV42 is not configurable. The AV42 module is evaluated just as is any other component in the nuclear plant. The single failure of any safety component is factored into the overall plant safety analysis and is allowed by regulation and industry standards. The U. S. EPR incorporates a four division safety system architecture that complies with NRC regulations and industry standards with regard to ensuring that a safety function will be accomplished if a single failure occurs in any component/system that has a safety function.

If a single AV42 module fails to provide an output, then a pump fails to start/stop or a valve does not reposition. If it fails in a manner where it provides an output absent a demand signal then a pump starts/stops or a valve repositions when it should not. These potential failure modes and their effects on overall plant safety are evaluated during the normal course of performing the plant safety analysis. The AV42 module is therefore evaluated just as any other component in the plant and the consequences of its failure are properly evaluated from an overall plant safety perspective.

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.*

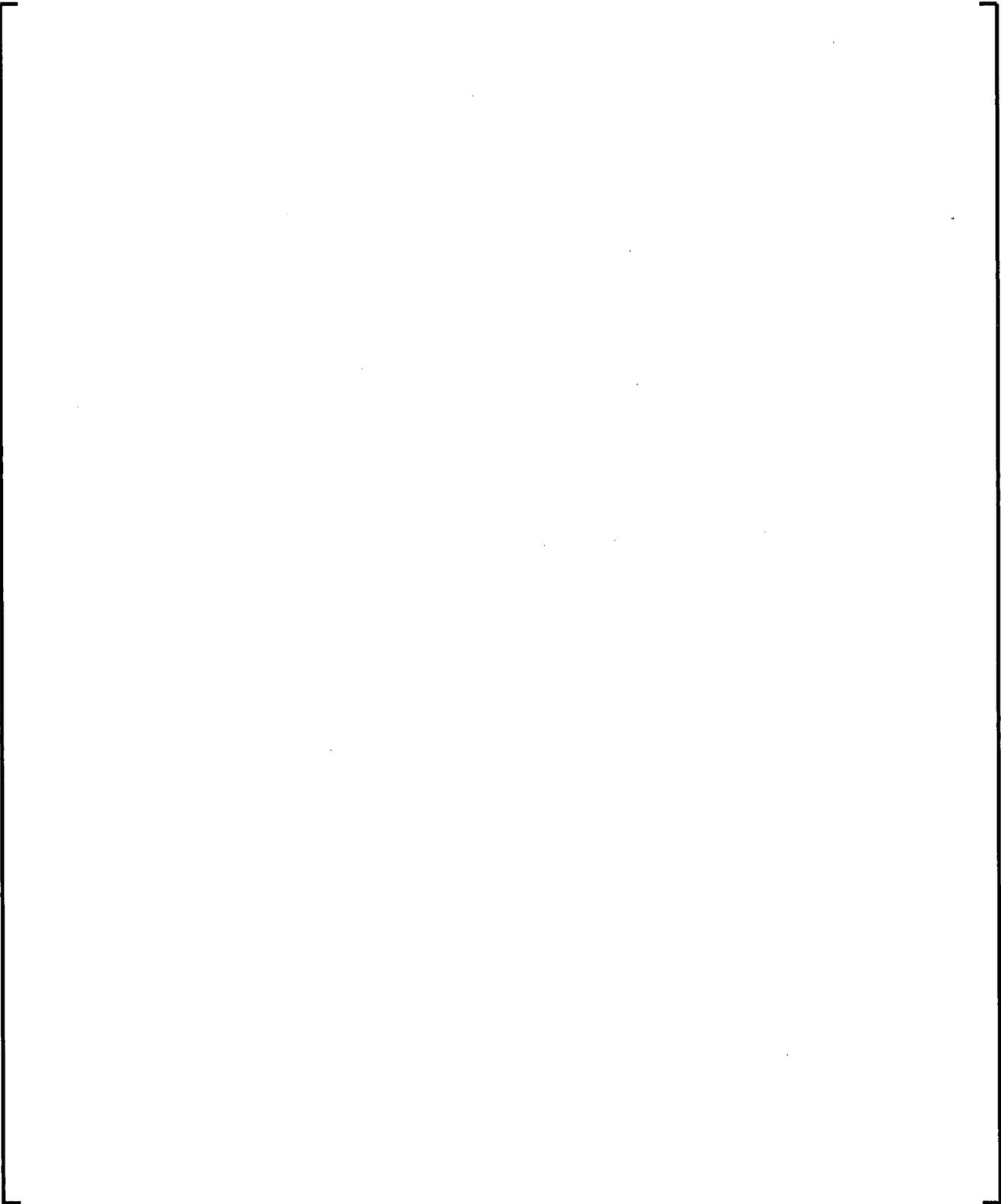
Response 28:

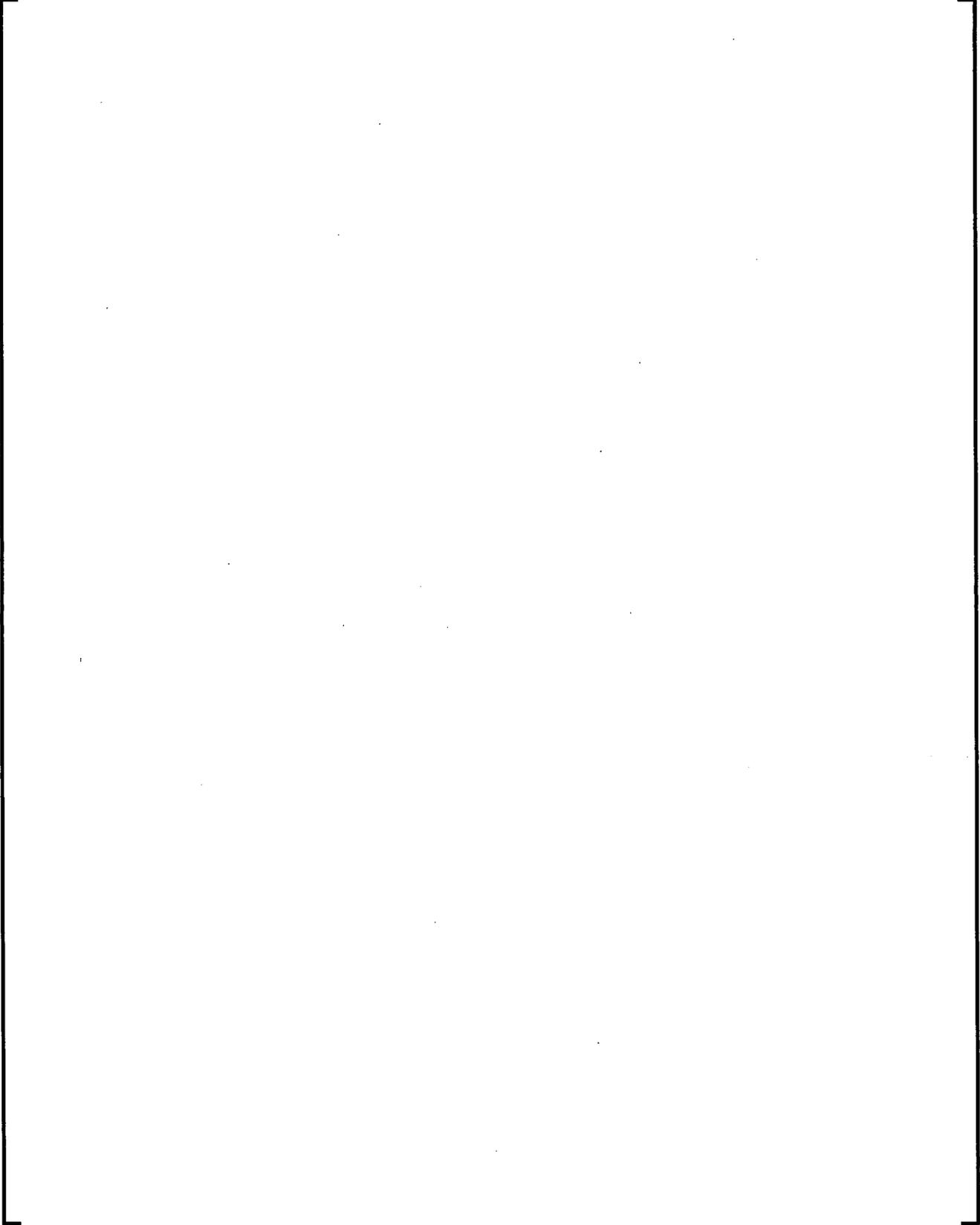
There are three different functions implemented in the Profibus DP interface:

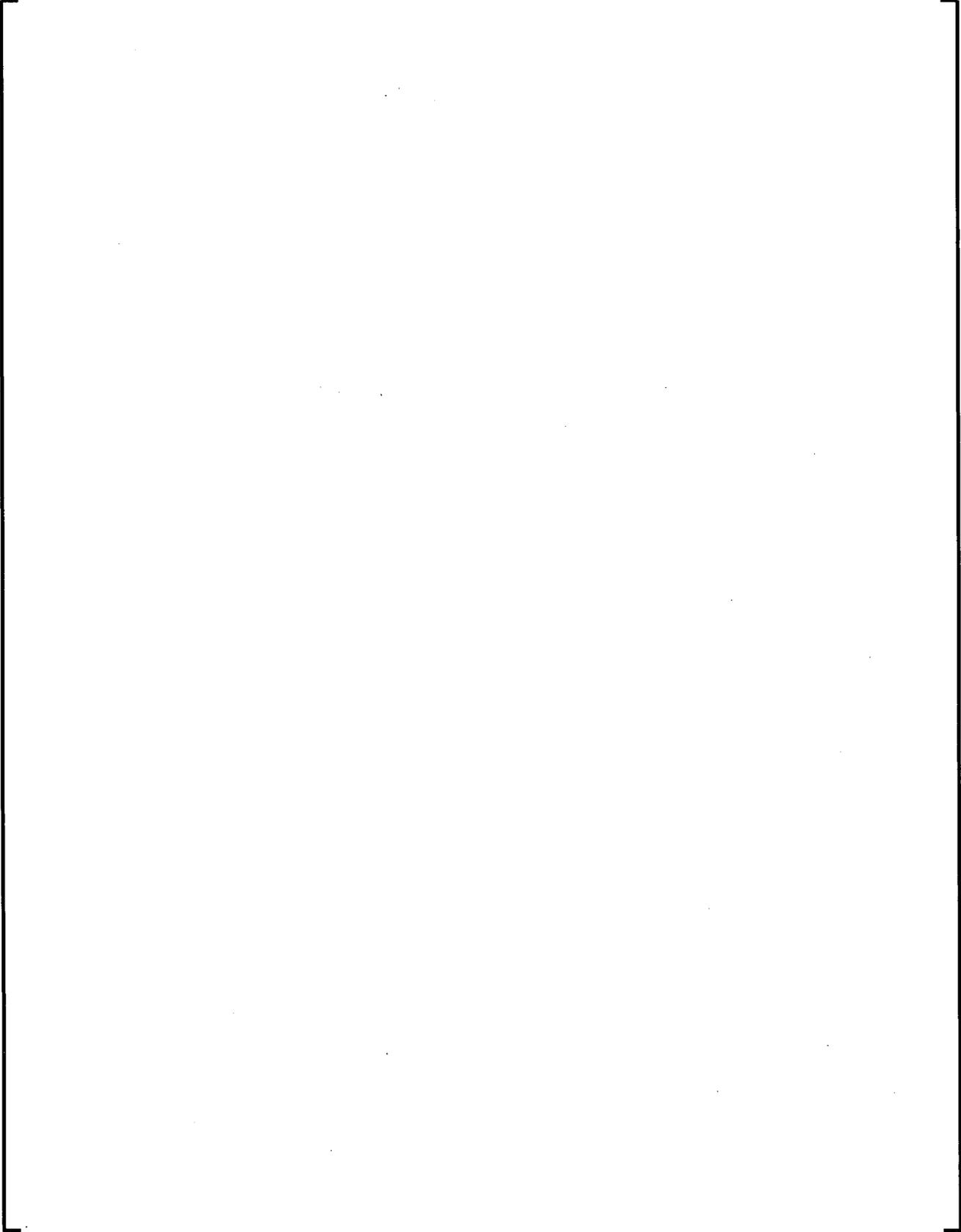
***RAI 29:** Describe the process for accepting any software tools used to assure the quality of the design and implementation of the AV42.*

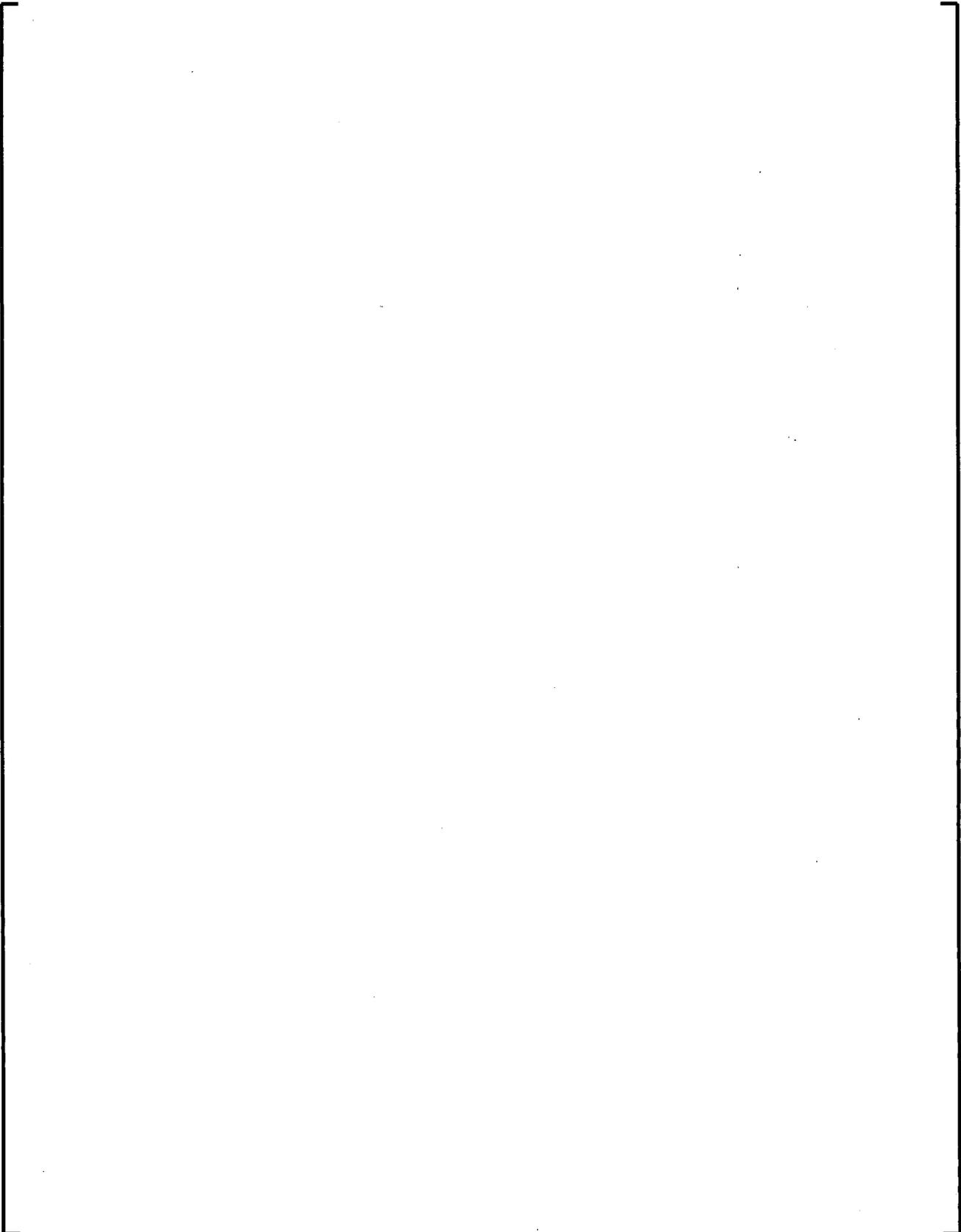
Response 29:

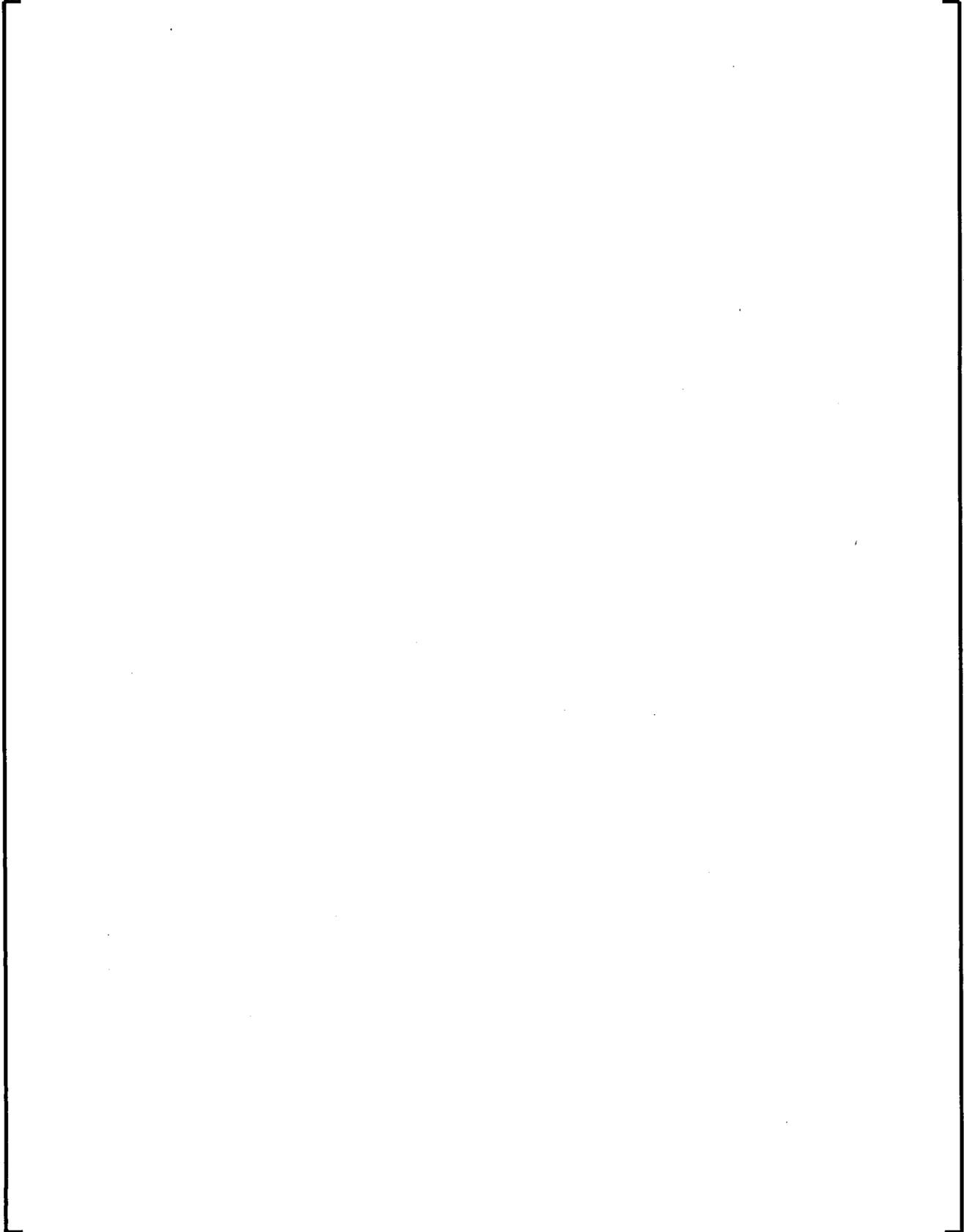
For the selection of software tools used for AV42 development and testing, emphasis was placed upon choosing off-the-shelf tools with a large application basis, or tools with a large experience base within AREVA NP.

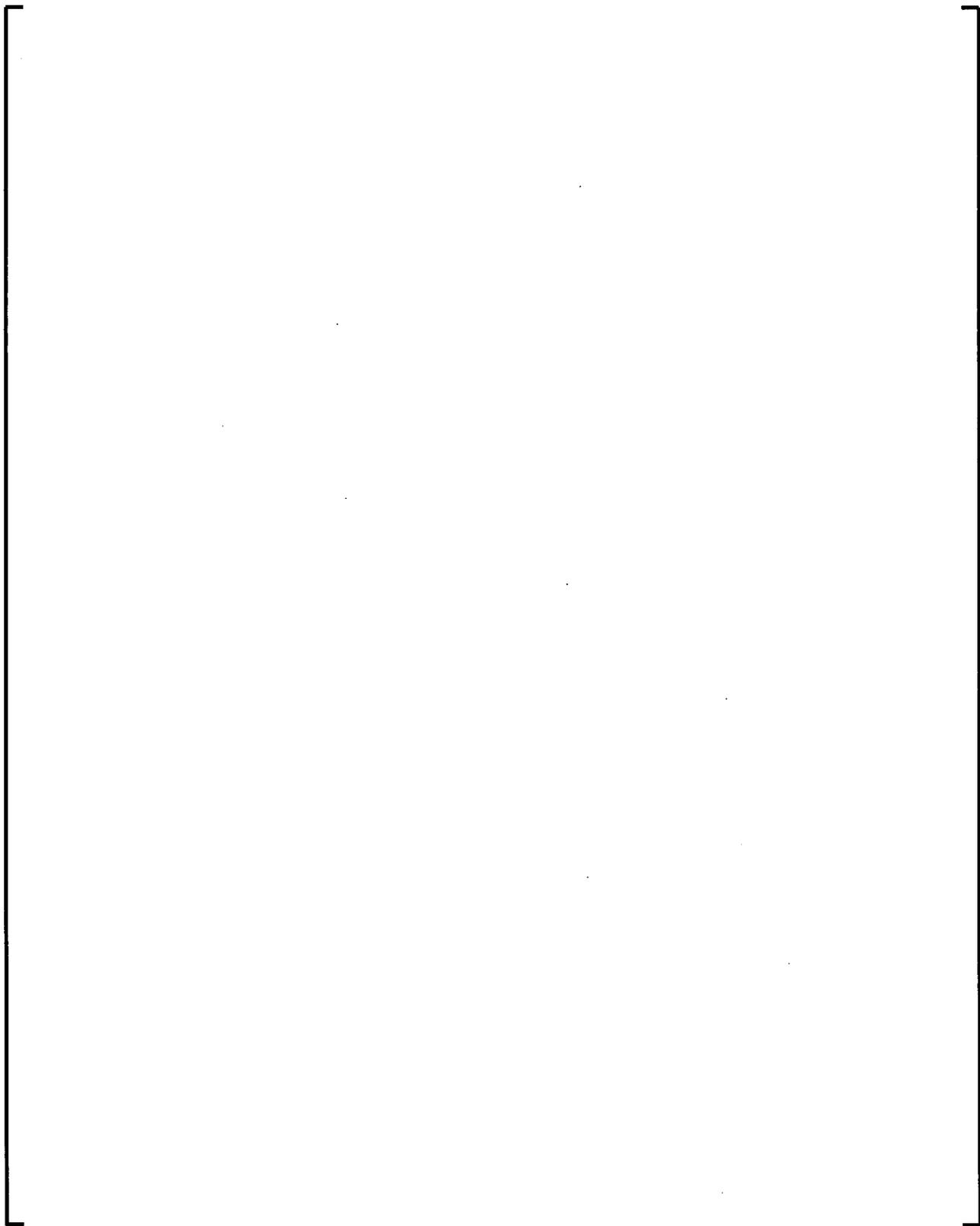


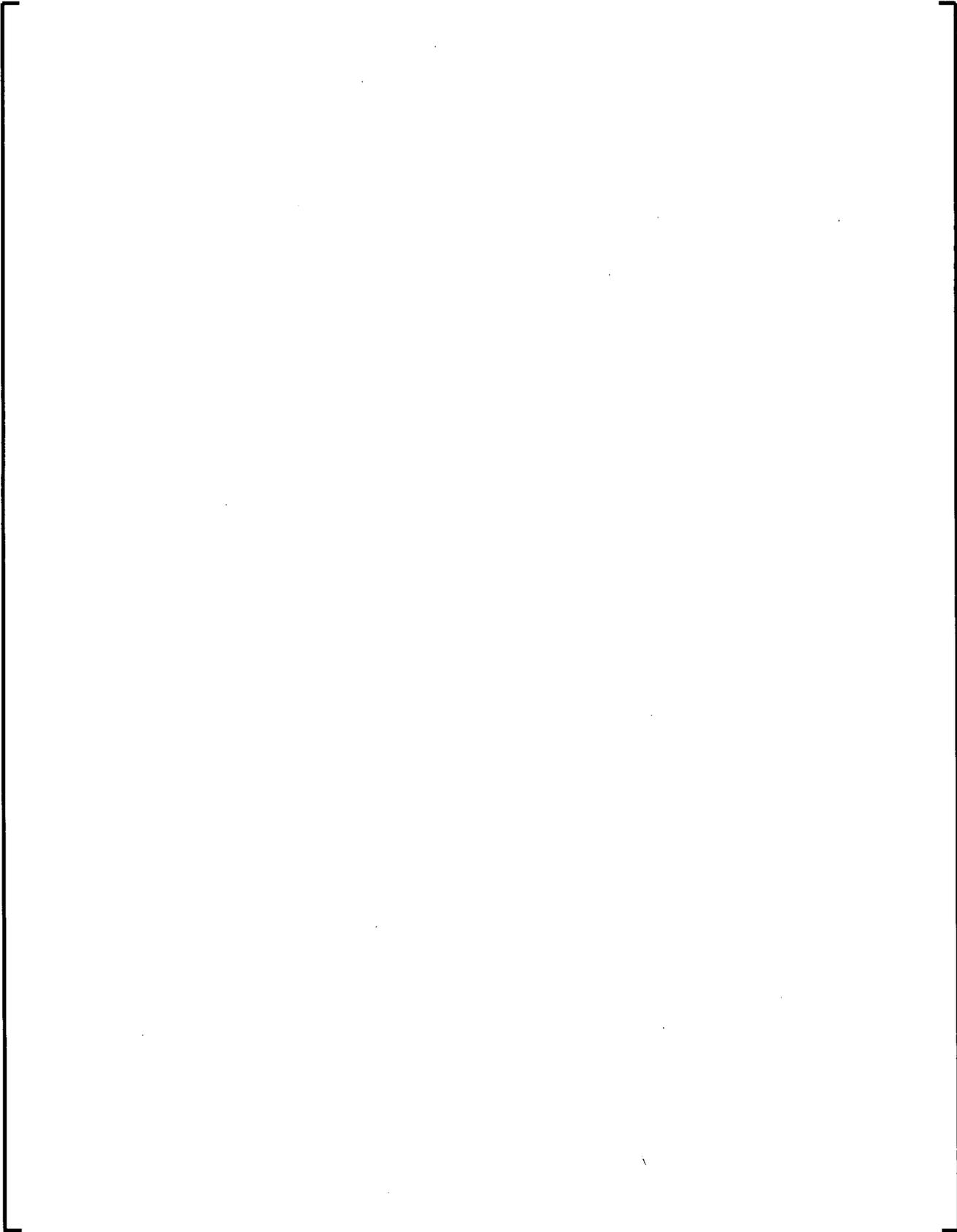


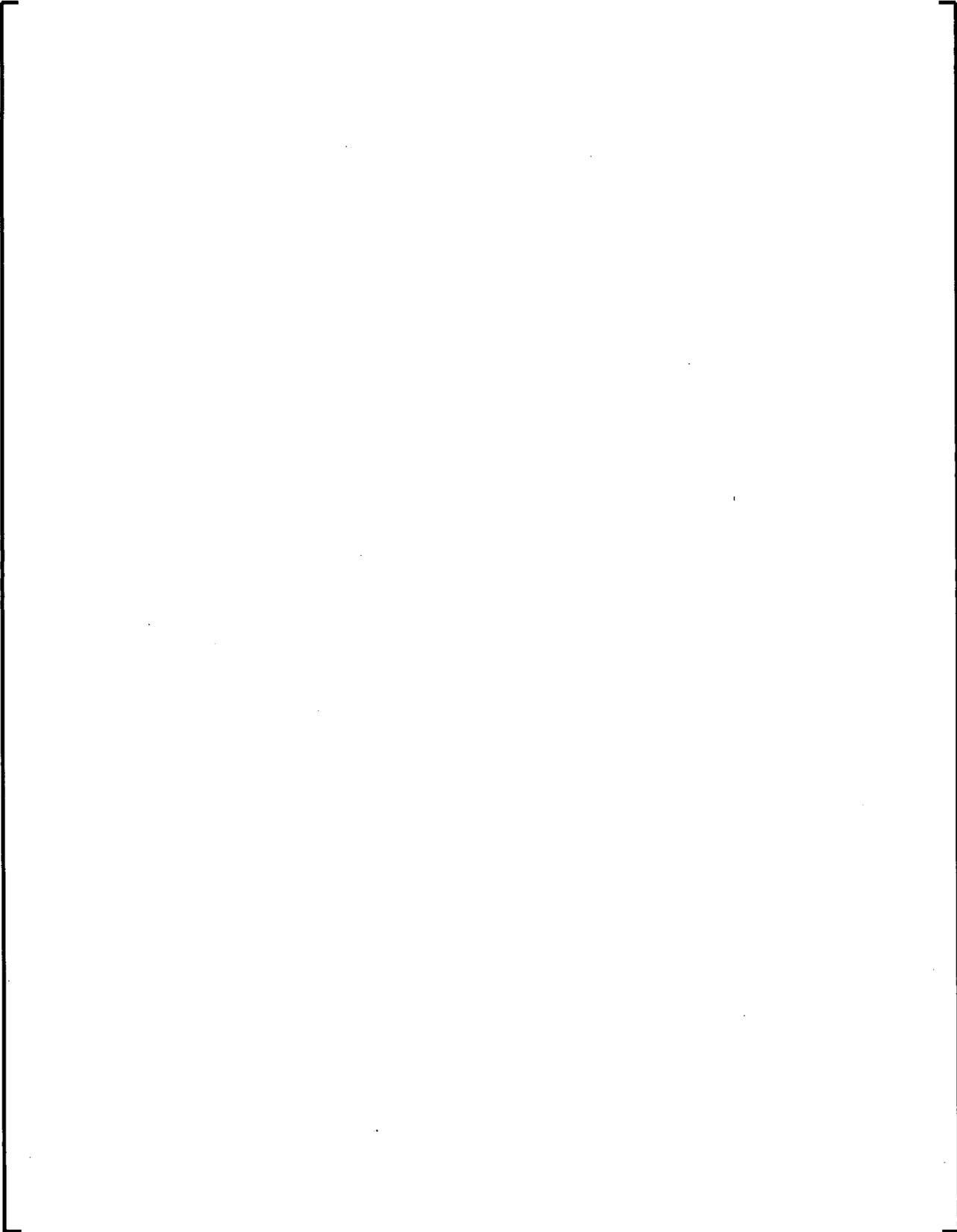


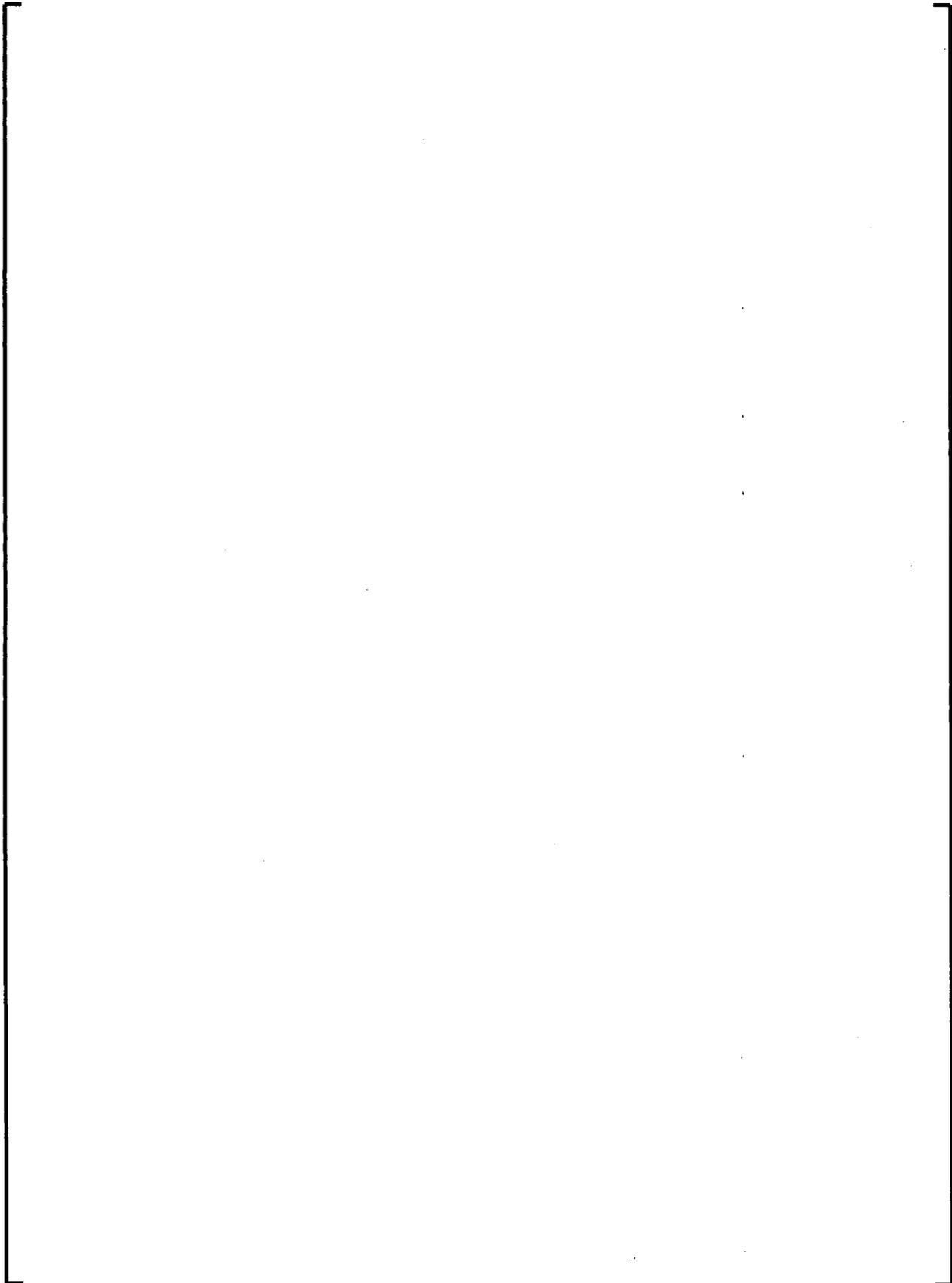












RAI 30: Section 4.6 says, "Manual controls enable the operator to initiate protective actions at the system level as well as the individual level". Please describe these design details and provide examples.

Response 30:

As indicated in the response to RAI 14, the AV42 supports manual initiation of protective actions at the system level in two ways. Manual system level and individual level control configurations are part of the overall I&C architecture for a given plant and are therefore outside the scope of this Topical Report; however, design details and examples on manual system level actuation are given in the response to RAI 18 of the U. S. EPR Protection System Topical Report RAI responses in ANP-10281P. A functional representation of typical system and component level actuation using the AV42 is presented in Figure 30-1 below. ("Component" being synonymous with "individual" as stated above and in section 4.6 of the topical report.)

Figure 30-1
U. S. EPR functional representation of Manual System and Component level actuation.

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

Response 31:

Since the AV42 is a component within the TXS system platform, it is part of the configuration management and change process of TXS. Modifications of the module may be implemented by specific project requirements, technological impacts related to the manufacturing of the module (i.e., obsolescence of an electronic component), or other similar issues.

Non-conformances are managed by the non-conformance handling procedures of AREVA NP GmbH. These procedures are maintained within the Areva NP QA program. Non-conformances and other modification needs are transformed into formal change requests and scheduled for implementation according to their importance and urgency.



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.

Response 33:



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

Response 34:

No network communications are passed between the non-safety and safety portions of the AV42. See response to RAI 33.

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)?

Response 35:

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.*

Response 36:

Section 4.10 is alluding to the use of the Functional Complex Number (FUNR) and Instance number (INSTNR). See the response to RAI 34 for more information on FUNR and INSTNR.

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?*

Response 37:

The tests described in section 4.4 are automatically performed by one of the TXS safety systems; however, tests are manually initiated from the TXS Service Unit under the control of an Operator. Tests can be performed one division at a time, with the TXS Service Unit physically preventing multiple divisions in test at one time (i.e. key switch). For further information on surveillance testing, see the response to RAI 03 of the U. S. EPR Protection System Topical Report RAI responses.

No other self-tests are associated with the AV42 other than what is mentioned in section 4.4 of the AV42 Topical Report.

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.*

Response 38:

The AV42 PLD is a non-computer based, 100% testable device. It is not subject to software common cause failure modes. One AV42 module is used per one field component (valve, pump, solenoid valve, etc.). The AV42 is evaluated as a potential single failure device just as any other component in the plant (such as a solenoid valve, a pump, a relay, etc.).

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.*

Response 40:



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.*

Response 42:

TELEPERM XS components are not sold as individual parts to be engineered by a customer. AREVA NP designs, engineers and implements safety I&C systems using TELEPERM XS components, and delivers the engineered system to the customer. This is typically done in the framework of a safety I&C project, by engineers trained in the TELEPERM XS components and project execution.

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.

Response 44:

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

Response 45:

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.

Response 46:

The testing features of the AV42 are presented in section 4.4 of the AV42 Topical Report and responses to various RAIs. ESF actuation output testing is also described in the response to RAI 03 of the U. S. EPR Protection System Topical Report, ANP-10281P.

Key steps to perform a periodic test are found in the response to RAI 15.

More information on test initialization including observed output conditions for a test is found in the response to RAI 03 under Pin F06.

Formal test procedures for use by Operations will be completed at a later date.

Information on the testing of lamps on the Reactor Protection Panel, Main Control Room or Remote Shutdown Station can be found in the response to RAI 41.

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

Response 47:

Details on self-testing of the AV42 are presented in section 4.4 of the Topical Report. Further details on testing are also found in RAI 15, RAI 37 and RAI 46 responses.

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

Response 48:

[Empty response area]

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.

Response 49:

The main elements of the PLD used in the AV42 are as follows:

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?

Response 50:

It is not plausible that the PLD within the AV42 is susceptible to the half-bit phenomenon. This phenomenon could only be created by rapidly moving external signals. All field signals are conditioned before being processed by the PLD-logic:



Figure 50-1: AV42 Signal conditioning

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.

Response 51:

Glitches

Glitches due to disturbances of the input signal do not need to be considered due to the conditioning performed on the input signals (see RAI 50 response).

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.

Response 52:

The AV42 module has been included in the equipment qualification program and has passed all tests related to ambient conditions (environmental, EMC, seismic). This includes both the safety and non-safety portions of the module.

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.*

Response 53:

The current version of AV42 is not manufactured using lead-free soldering. Currently, there are no plans to change the manufacturing process.

If, in the future, manufacturing would be changed to lead-free soldering, the use of lead-free soldering will be documented and appropriate tests and justification will be provided.

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."

Response 54:

The reference to Regulatory Guide 1.89 will be deleted from the Topical Report since the AV42 is not qualified for use in a harsh environment, and there is no intent to ever use it in a harsh environment. Regulatory Guide 1.209 is applicable to safety-related computer-based instrumentation and control systems. Since the AV42 is not a stand alone computer based device, it is not considered to be within the scope of this Regulatory Guide. Therefore, the addition of a compliance statement for Regulatory Guide 1.209 within the Topical Report is not applicable.

The AV42 does comply with the guidance presented in IEEE 323-2003 for satisfying the environmental qualification of Class 1E equipment for use in Nuclear Power Generating Stations. A compliance statement for IEEE 323-2003 is found in section 6.6 of the Topical Report.

The AV42 module was qualified to IEEE 323-1983. The current version of IEEE 323-2003 added caution regarding the sensitivity of digital systems to EMI/RFI environments and in fact allows for less stringent environmental testing requirements for mild environment equipment. Although tested to the older version of IEEE 323, the AV42 testing included test methods of adequate rigor to address the IEEE 323-2003 changes and has a documented qualification package indicating the equivalency to the more current standard. The reference to RG 1.89 was intended to convey that the AV42 is not used above the harsh environment threshold for radiation of 1000R and is therefore used in a mild environment. Therefore, the reference to RG 1.89 will be removed, as indicated above.

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.

Response 55:

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:

- 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.*
- the AV42 would arbitrate all actuation inputs, so it is a single point of failure concern (like the actuator itself).*
- 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.

Response 56:

For the U. S. EPR, it is proposed that the AV42 be used for each safety actuator in the plant that also interfaces with another safety I&C system or the Operational I&C system. This device will be used throughout each safety division but will also be implemented to the point that each division of PACS (which is comprised of AV42 modules) will be independent of the other PACS and PS divisions to satisfy single failure criteria for safety systems as described in IEEE 603-1991.



misleading. The AV42 falls outside the scope of 10 CFR 50.62 ATWS requirements since it is not used for any Reactor Trip function within the architecture of the U. S. EPR. See the response to RAI 01 for more information.

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.)?*

Response 57:

[Empty response box]

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.

Response 58:

See RAI 31 & RAI 57 responses for the information requested.

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.

Response 59:

The Profibus DP network is contained within the boundaries of the Operational I&C system and the PACS. No external communication is performed by the Operational I&C system via the Profibus DP network.