

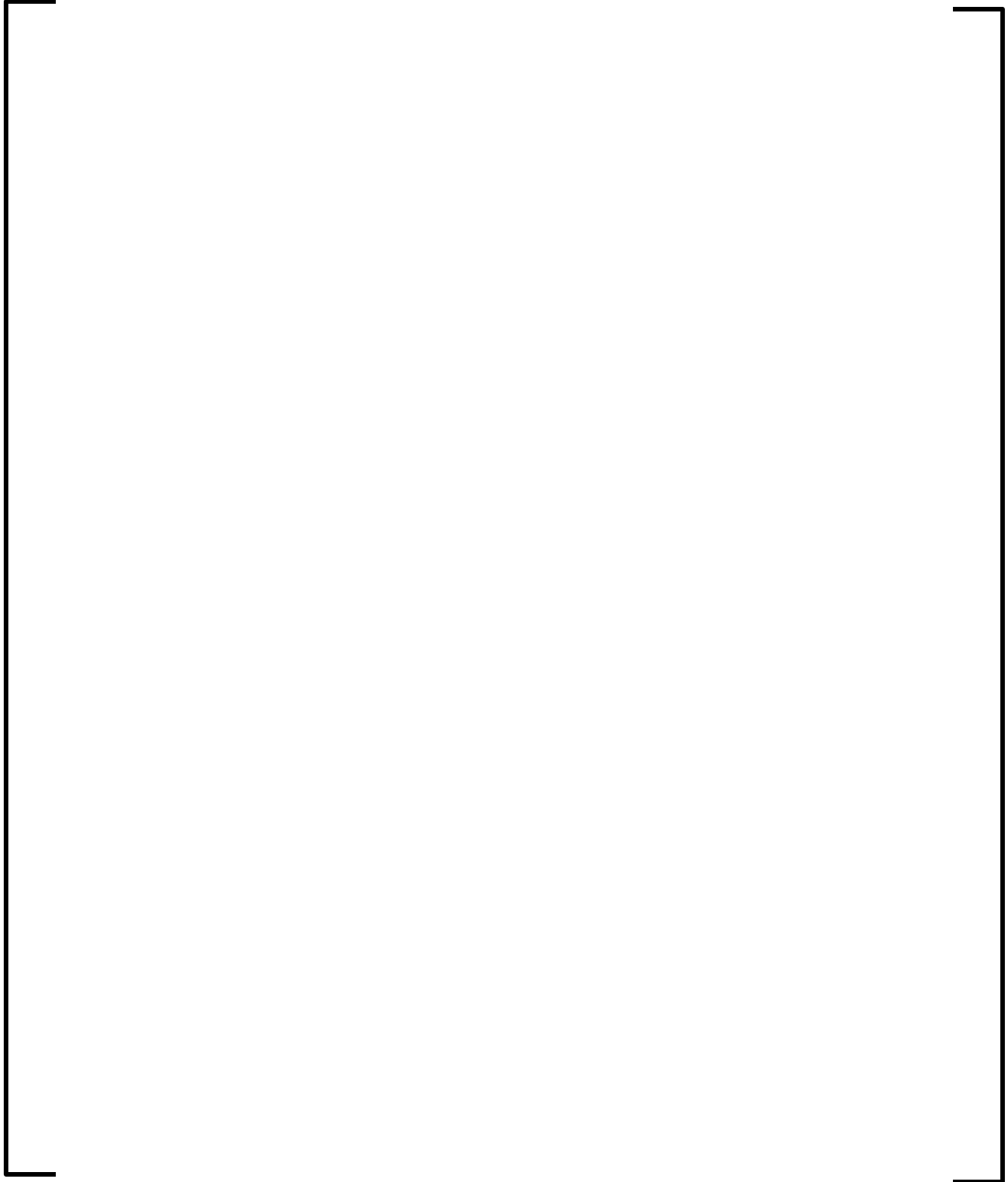
**Response to Request for Additional Information – ANP-10273P
“AV42 Priority Actuation and Control Module Topical Report” (TAC No. MD3867)**

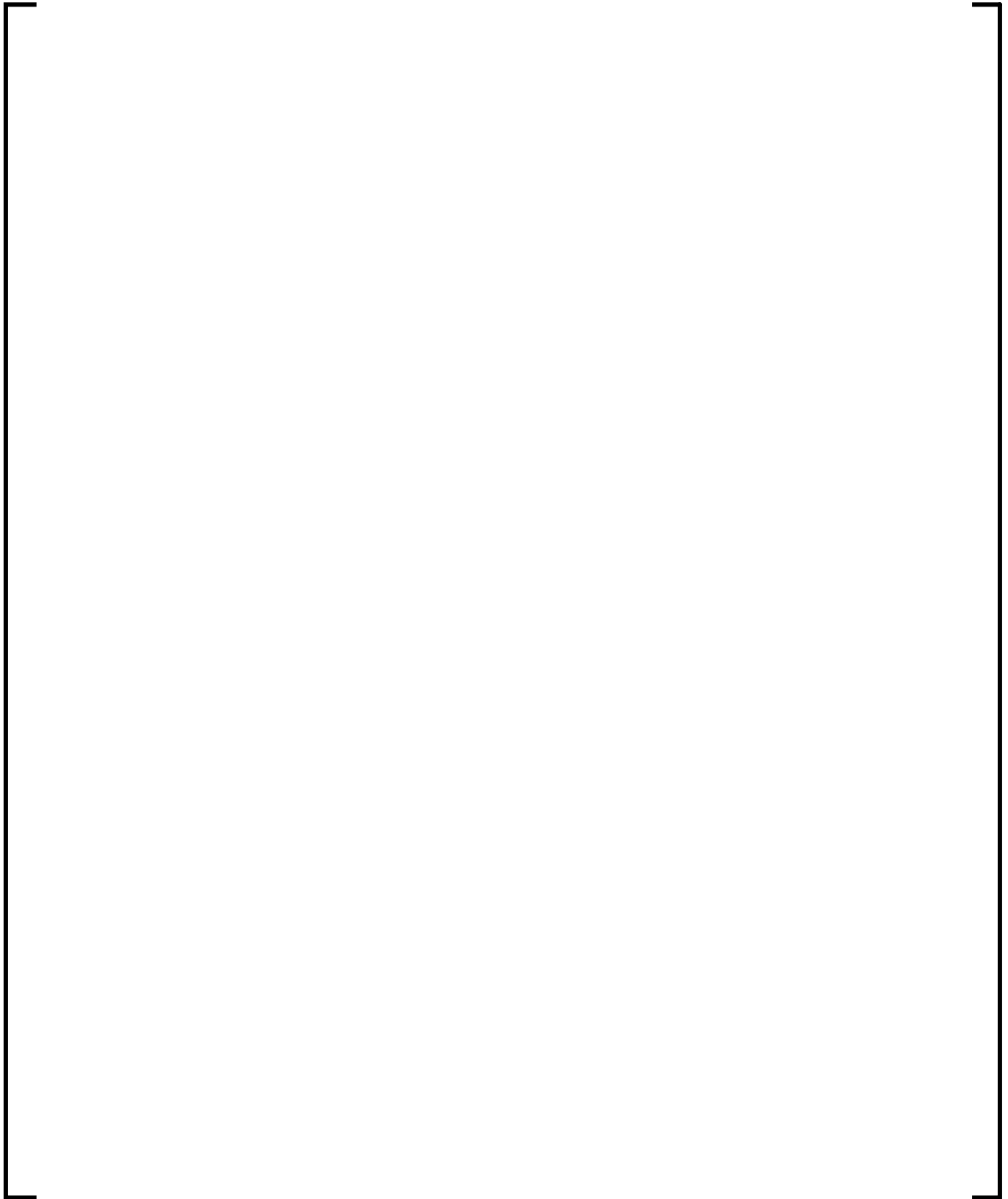
RAI 03: *The AV42 topical report does not contain enough information to determine the number of inputs or outputs of the AV42 module, not to mention the function of each input or output. Please provide a list and detail description of each input and output. What is the function of each?*

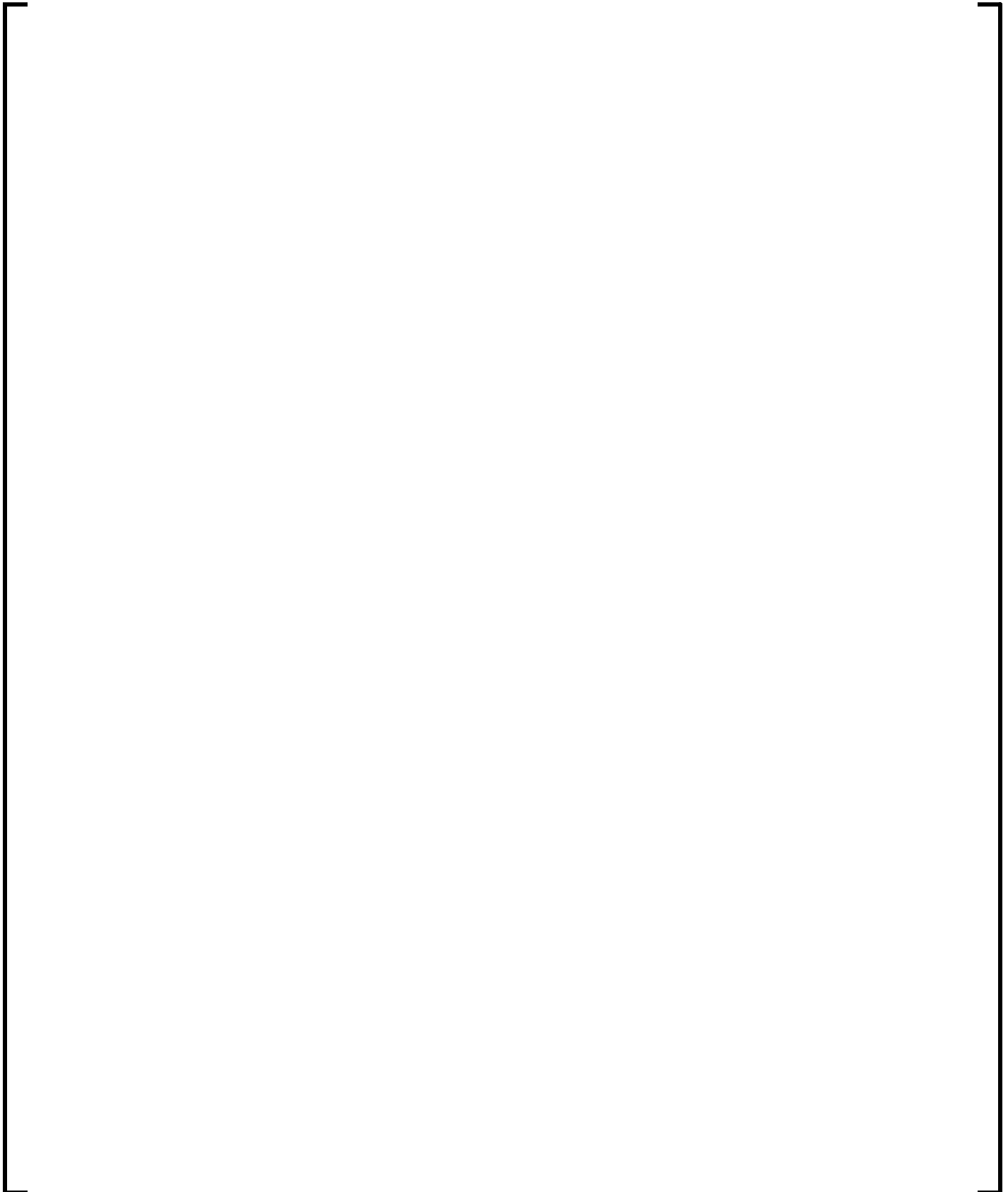
Response 03:

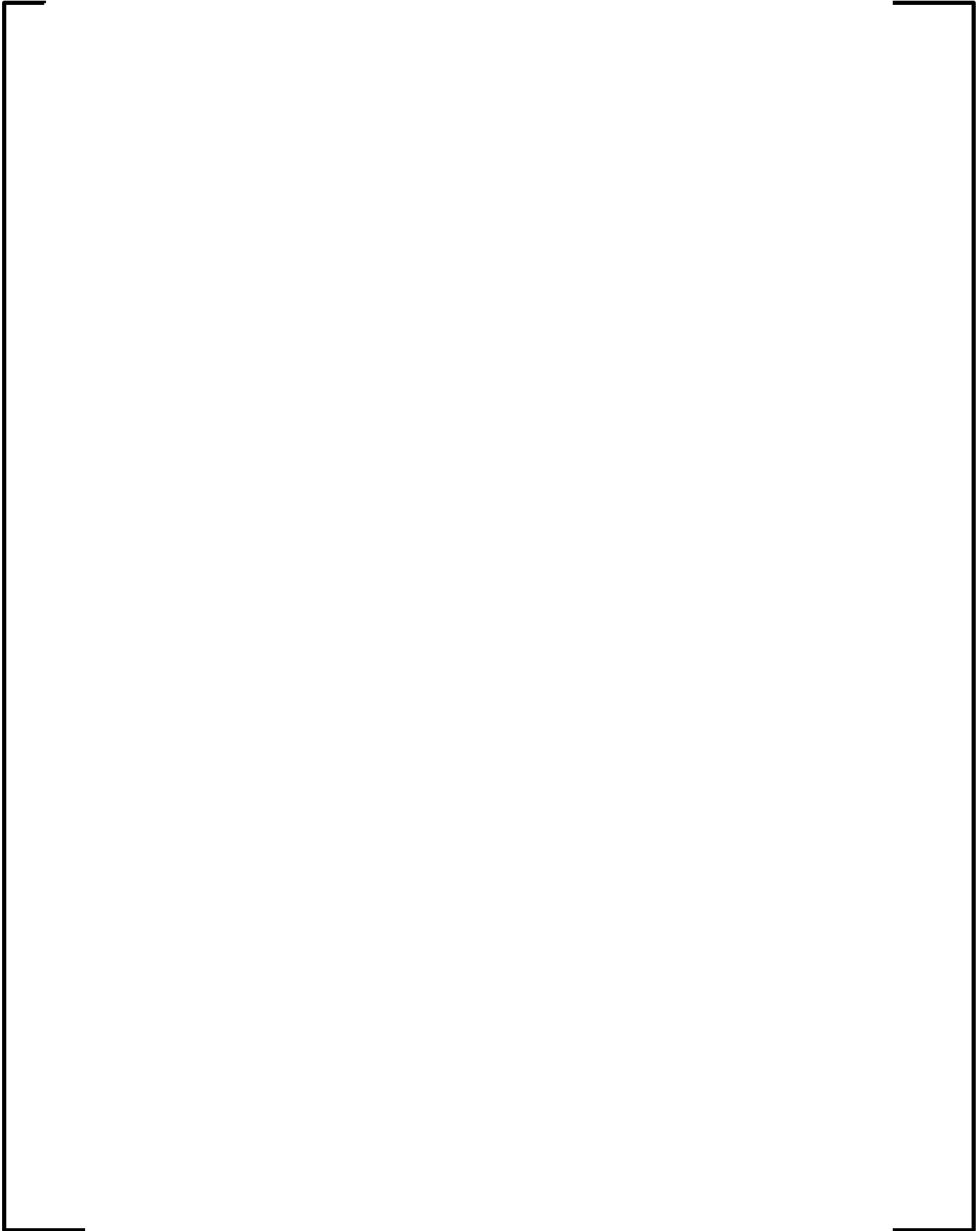
The AV42 has a 64 pin male connector on the back of the card. All hardwired Input and Output signals interface through this connector. The mating female connector will be wired to the respective I&C system or power supply on the back side of the subrack.

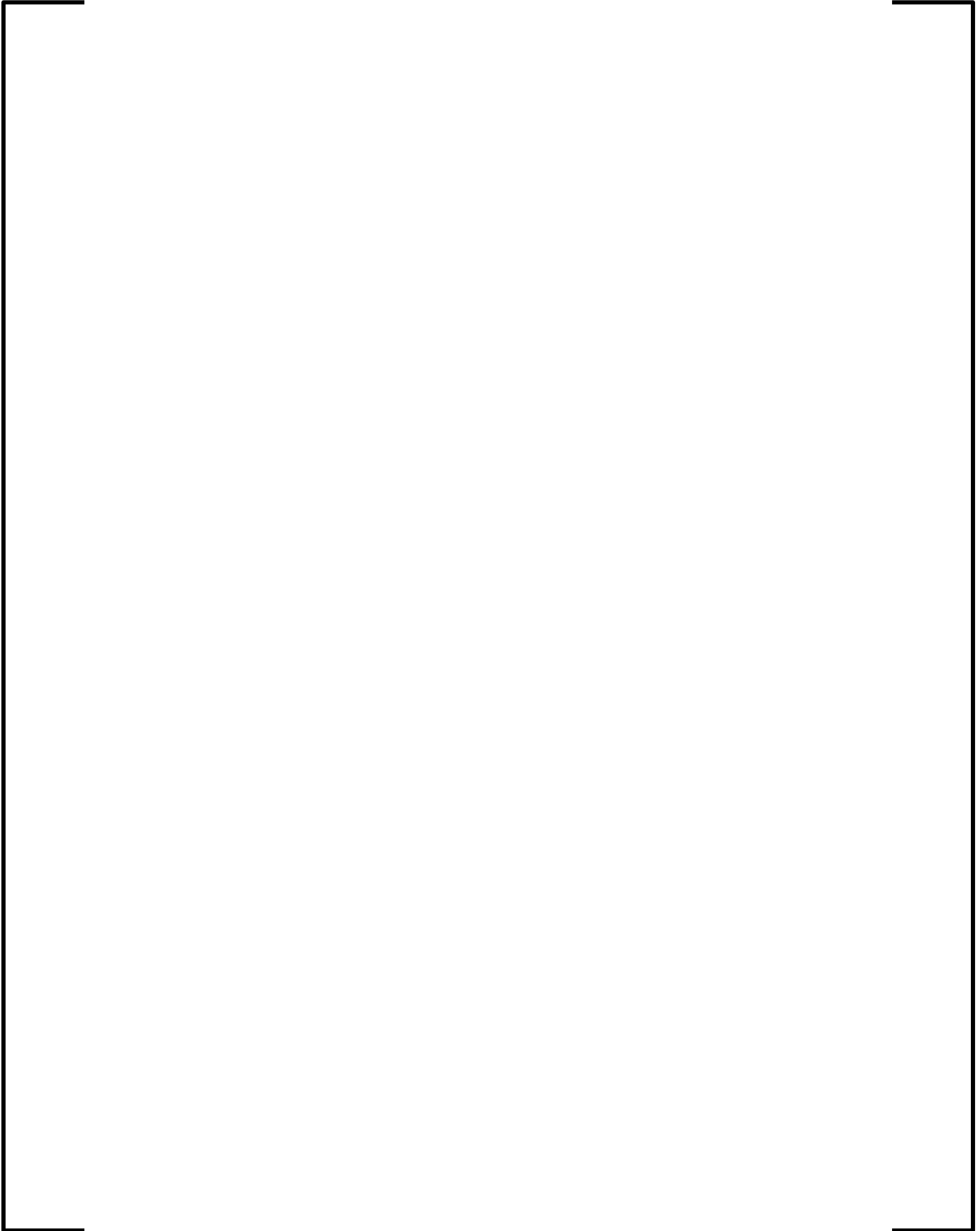
The following list is a description of the I/O pins of the 64 pin connector. This is solely for hardwired connections, not Profibus data communications. All of the I/O pins are binary; it is either 24 volts DC (logic “1”), or 0 volts DC (logic “0”). There are no analog signals interfacing with the AV42 (i.e. 4 - 20 mA signals). If a parameterization pin needs to be set to a “1” it will be wired to 24 volts DC; if it needs to be set to a “0,” it will be left unconnected. Internal pull-down resistors will force an unconnected pin to a “0.”

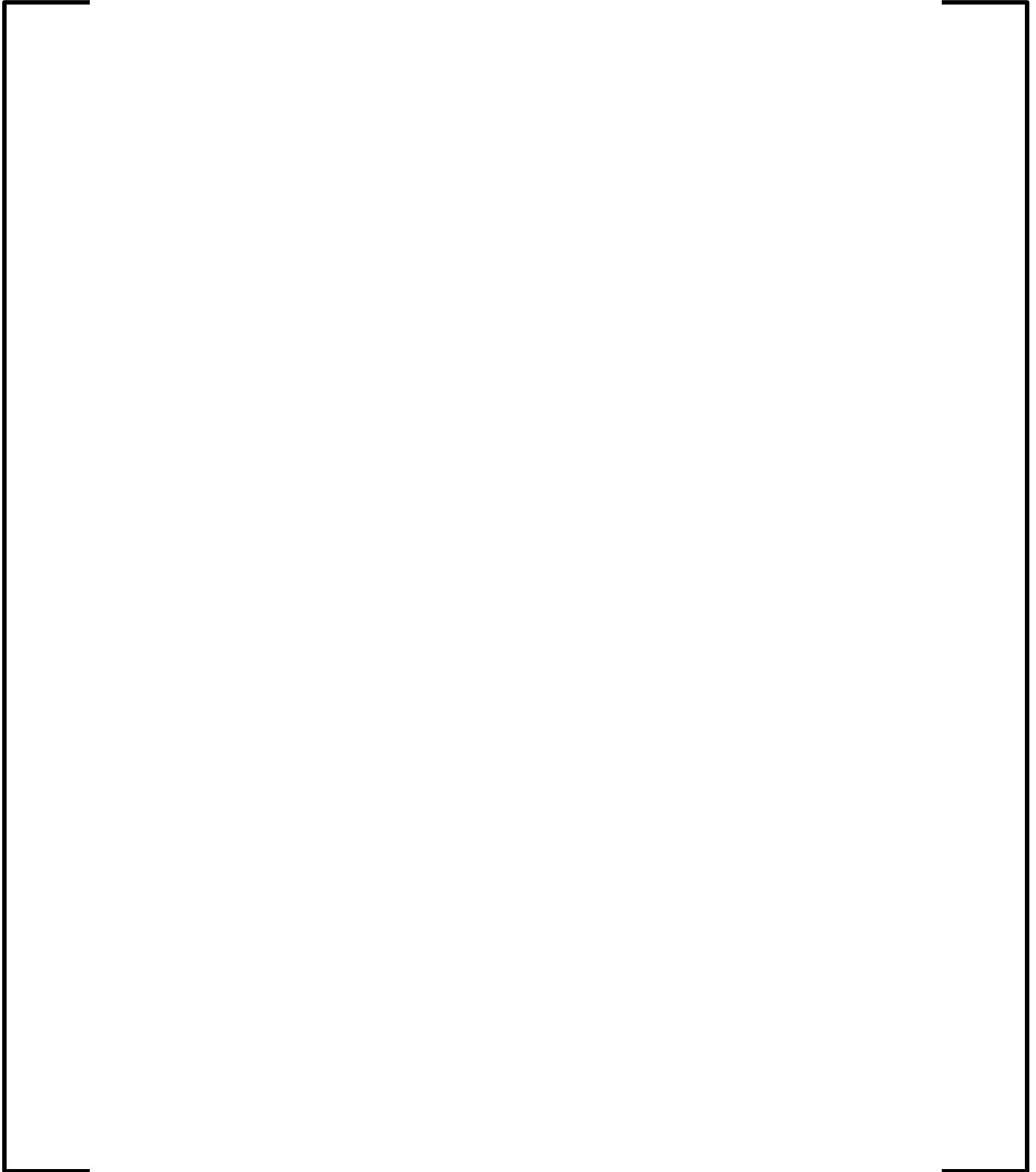


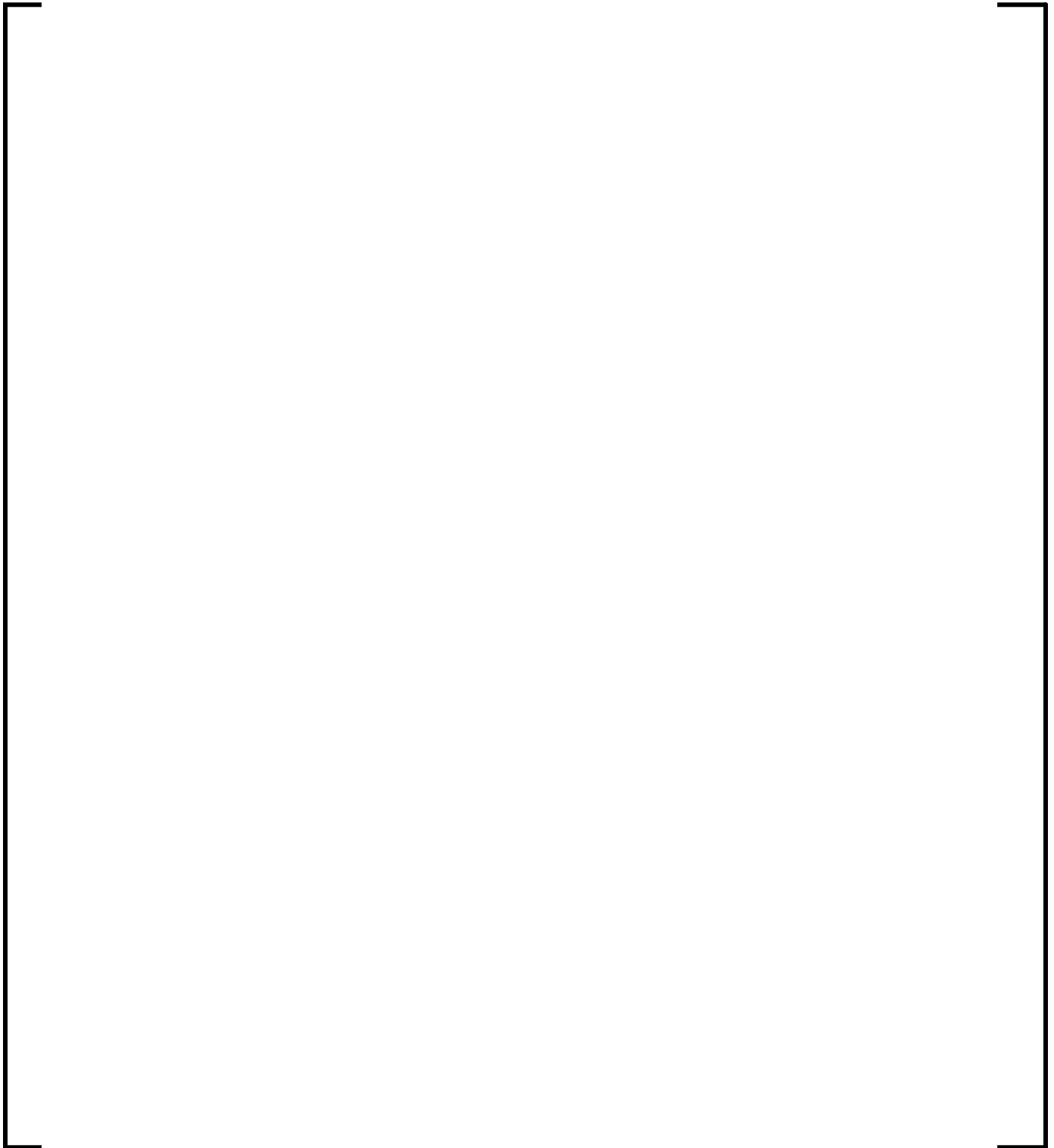


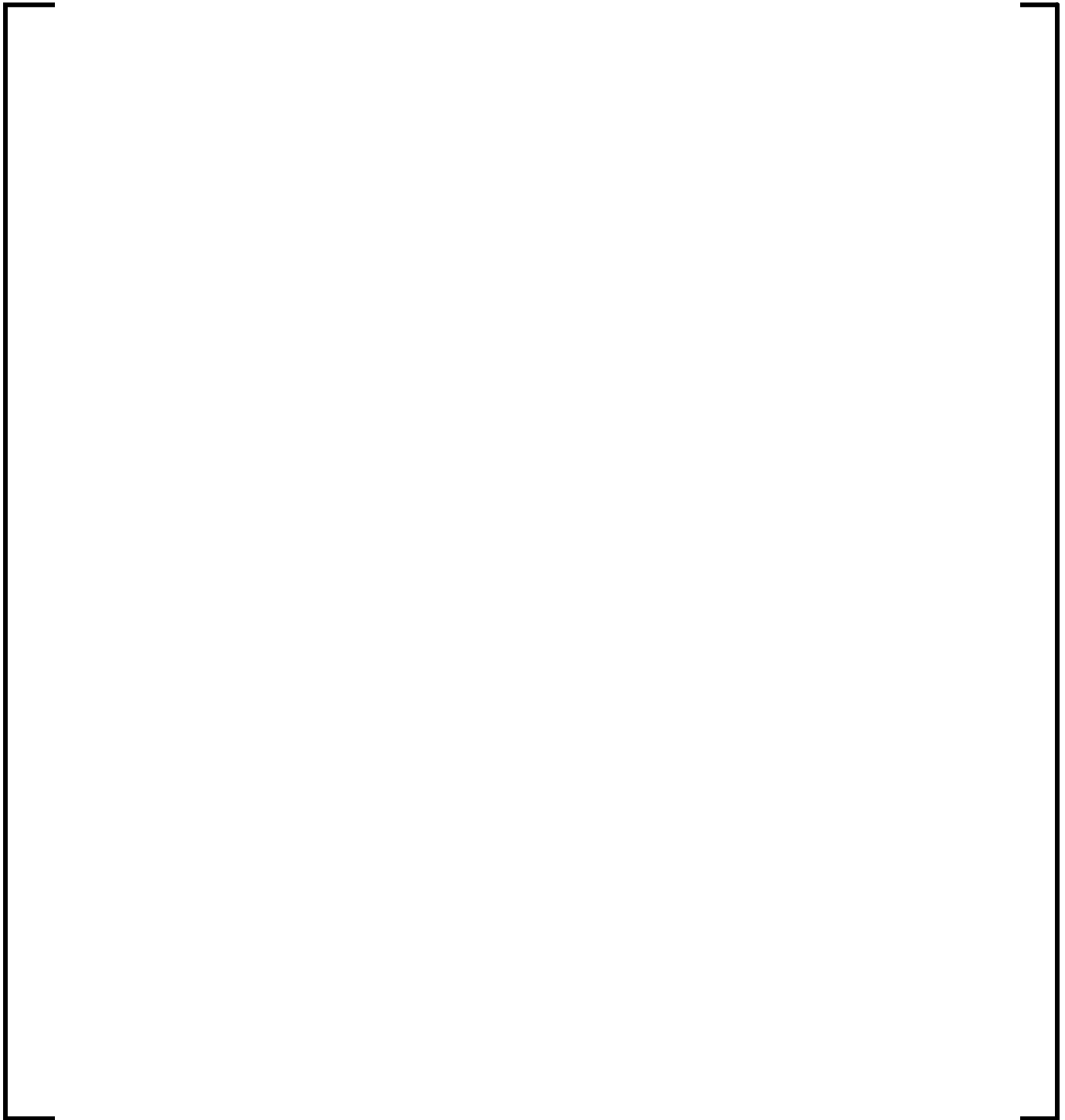


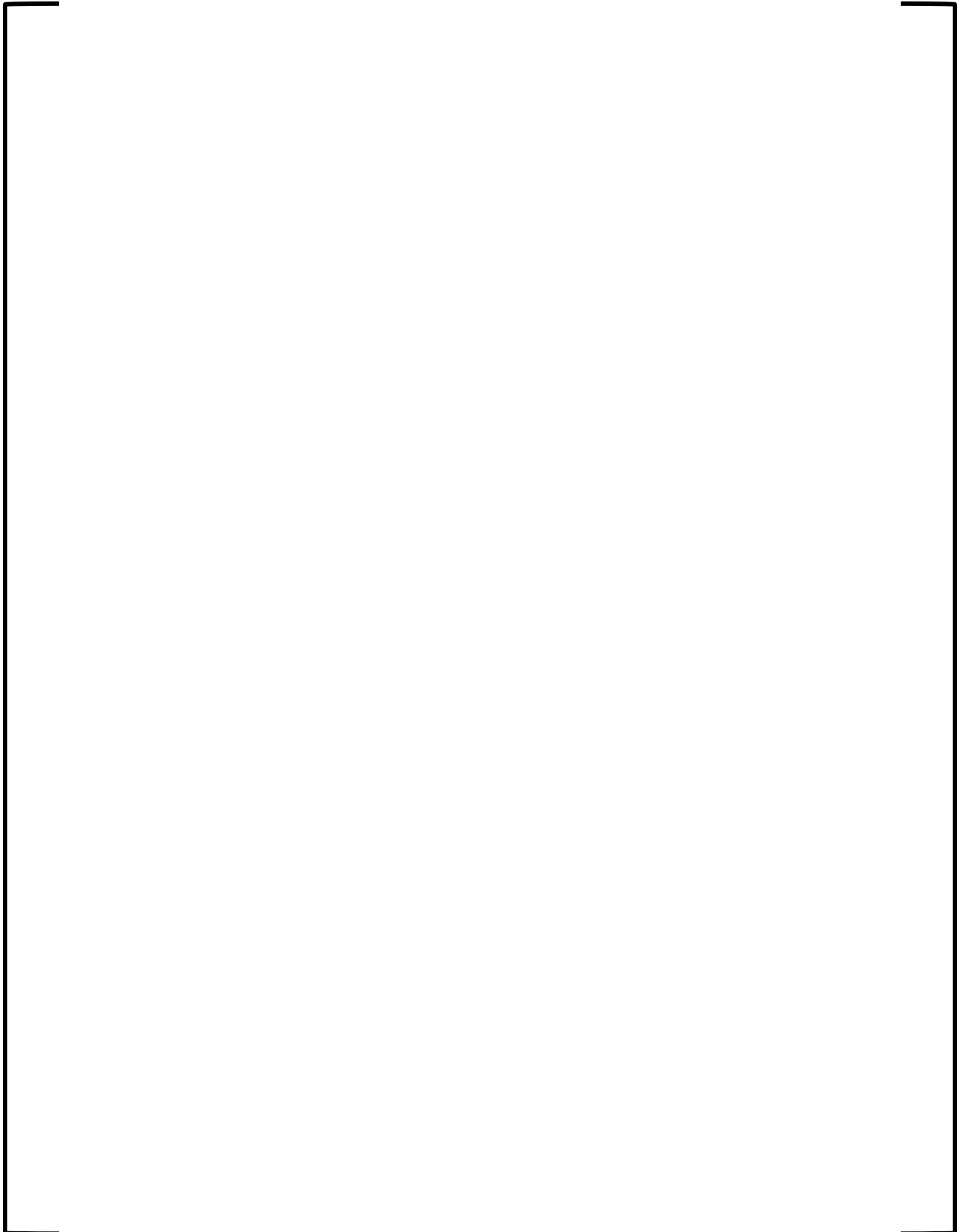


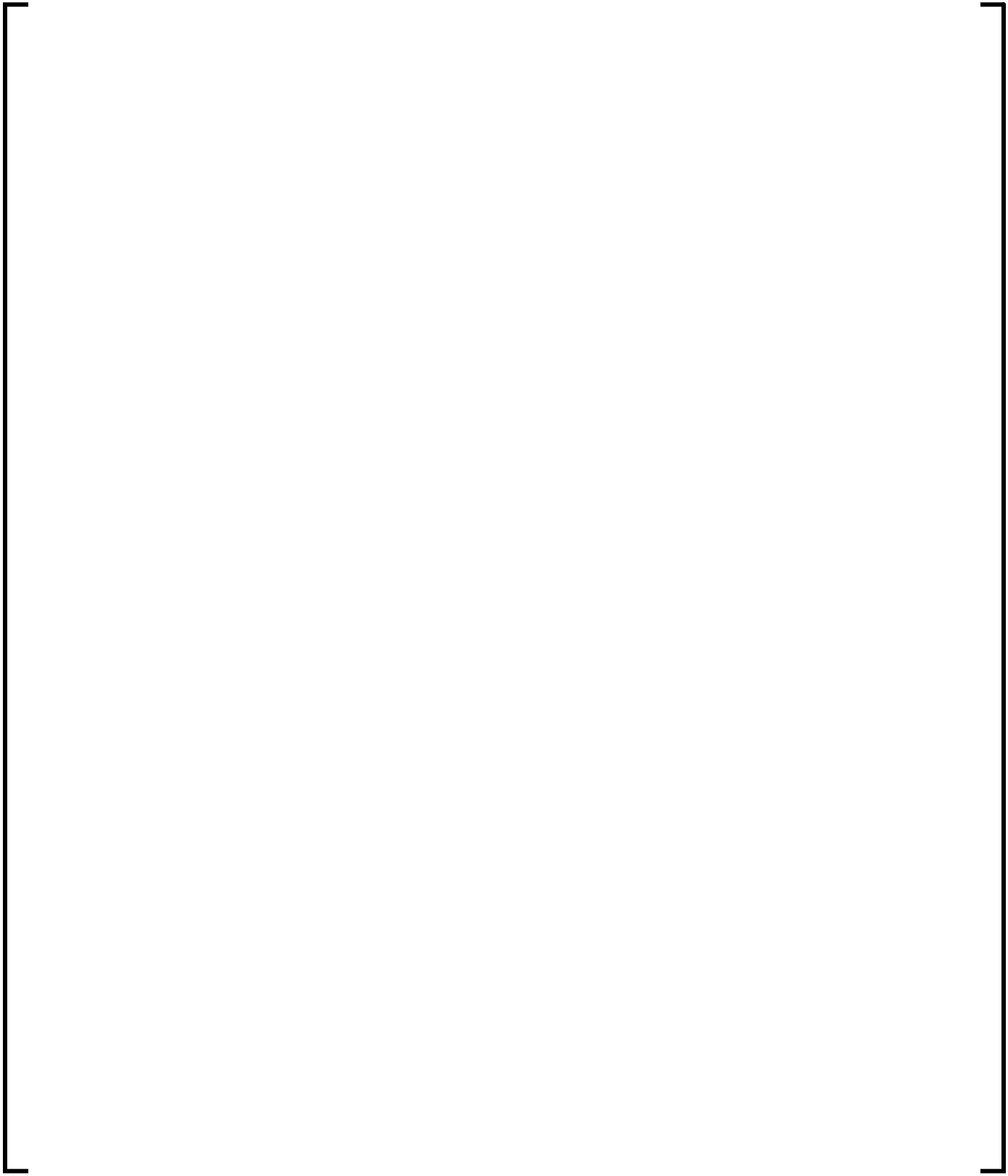


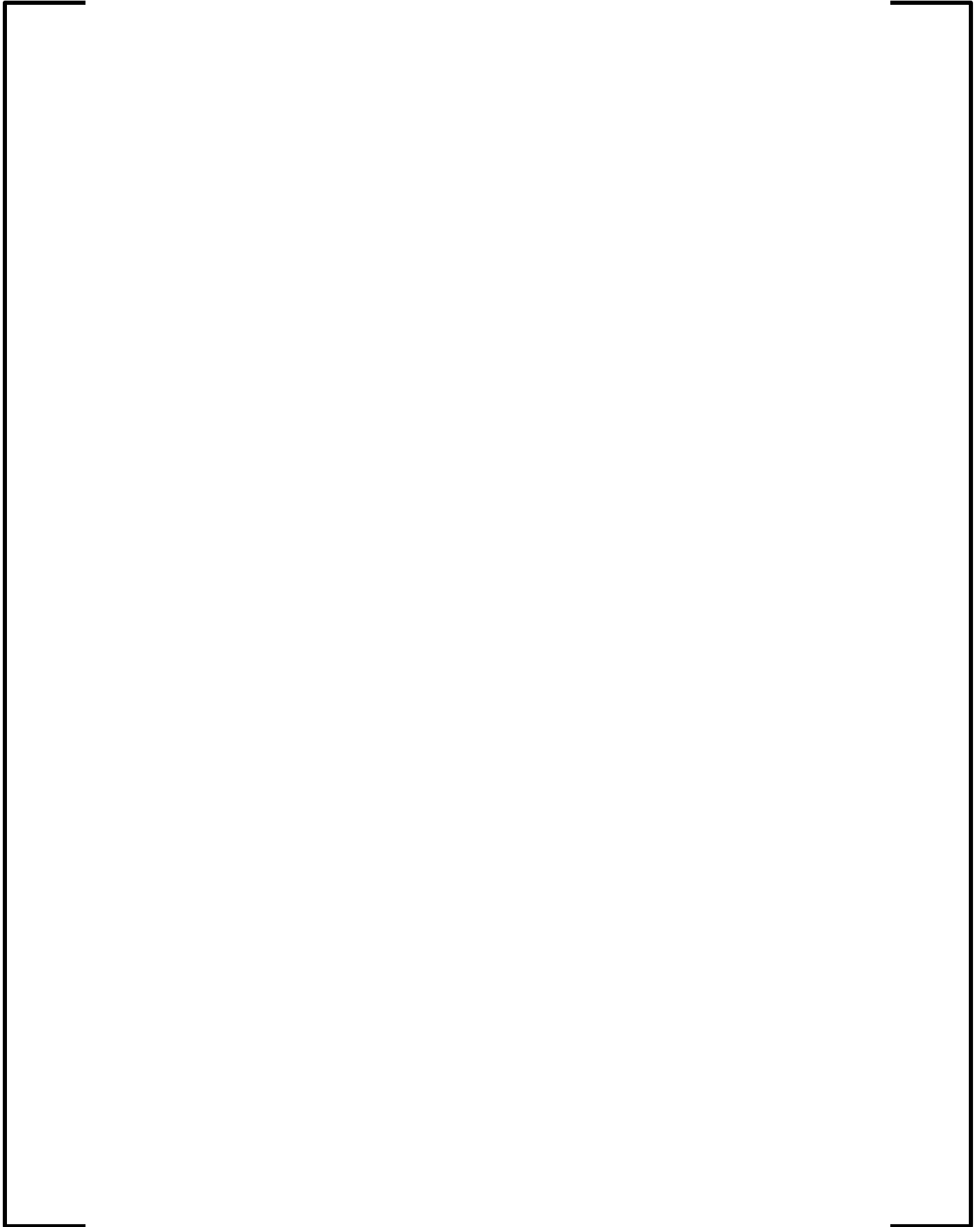


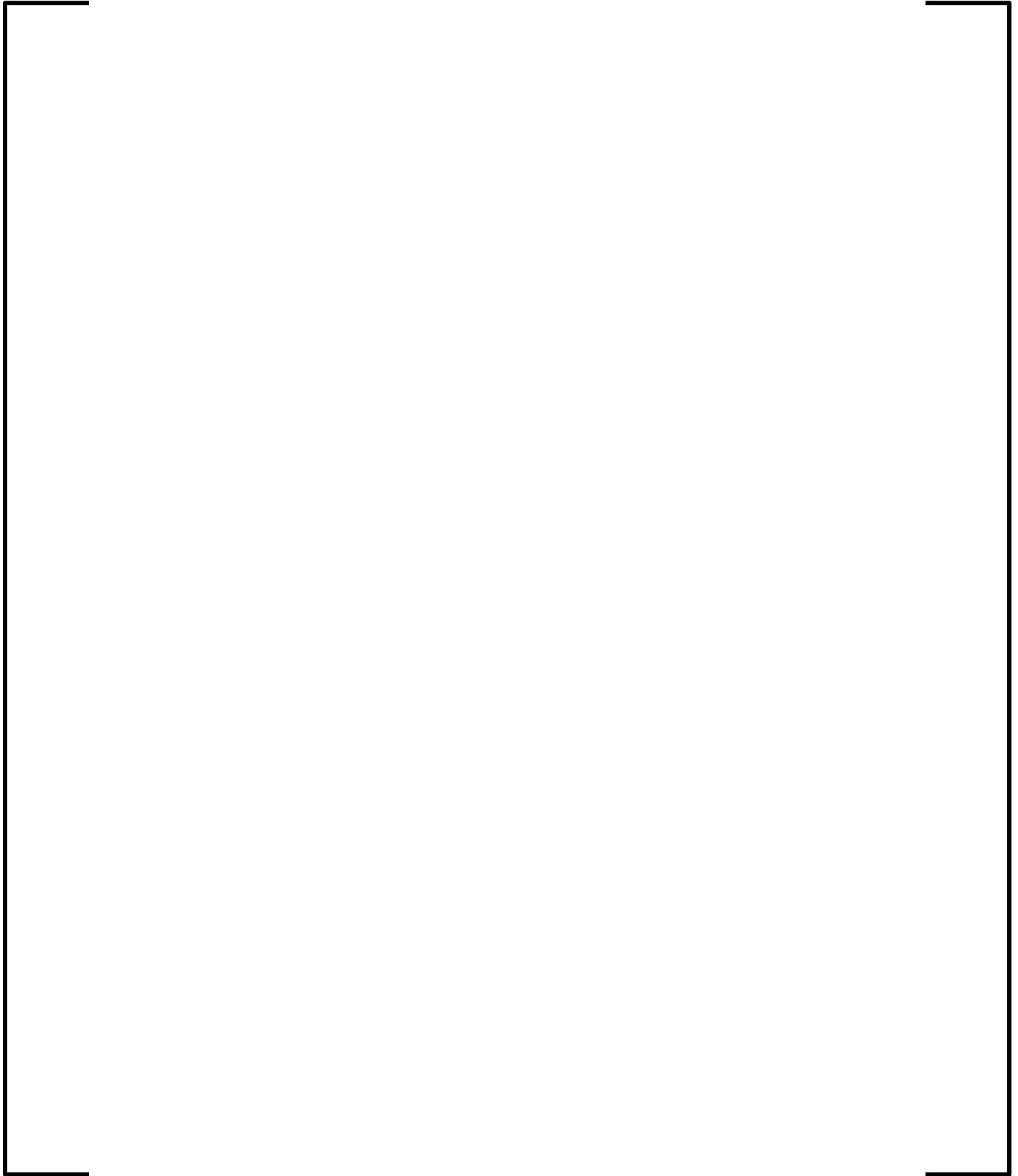


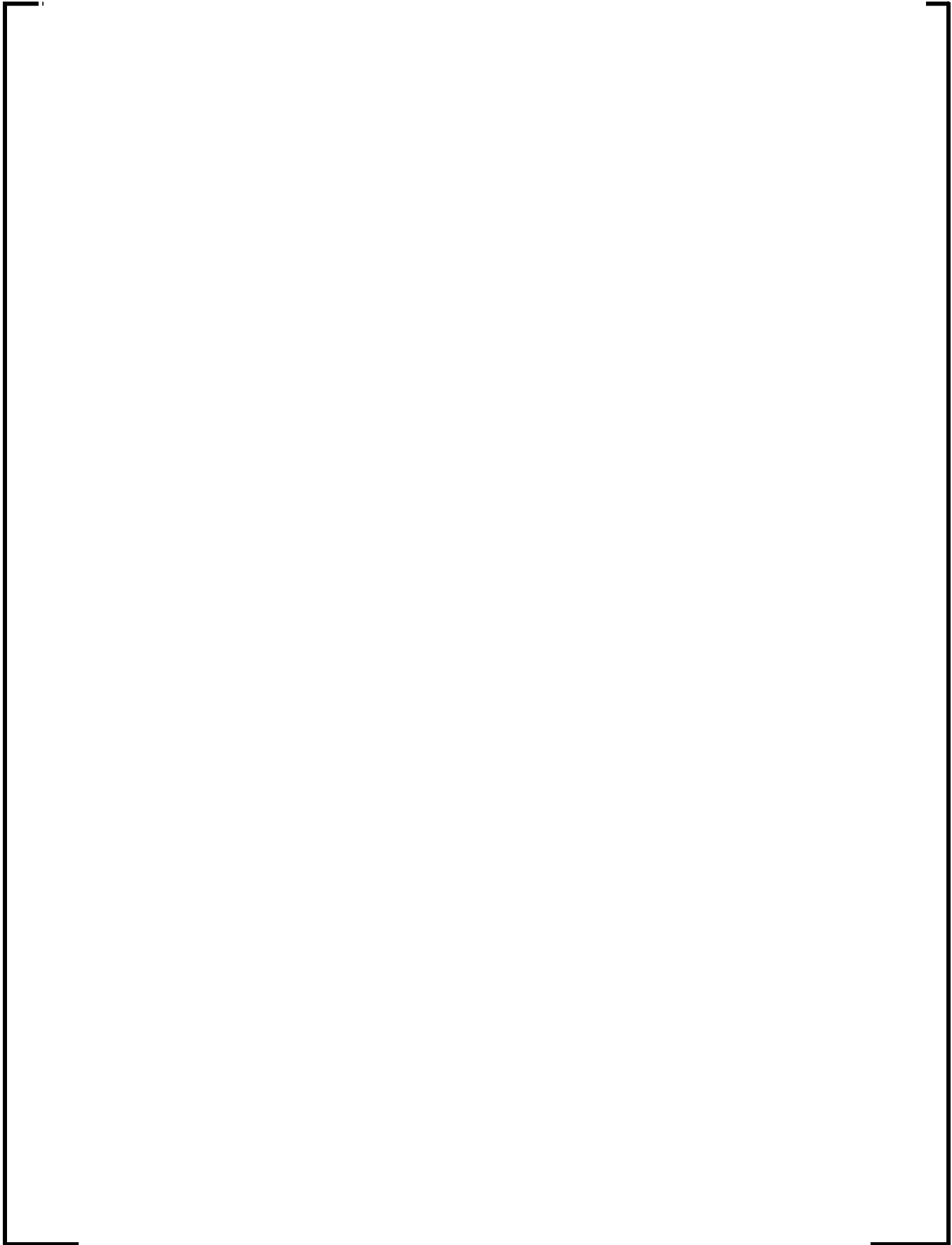


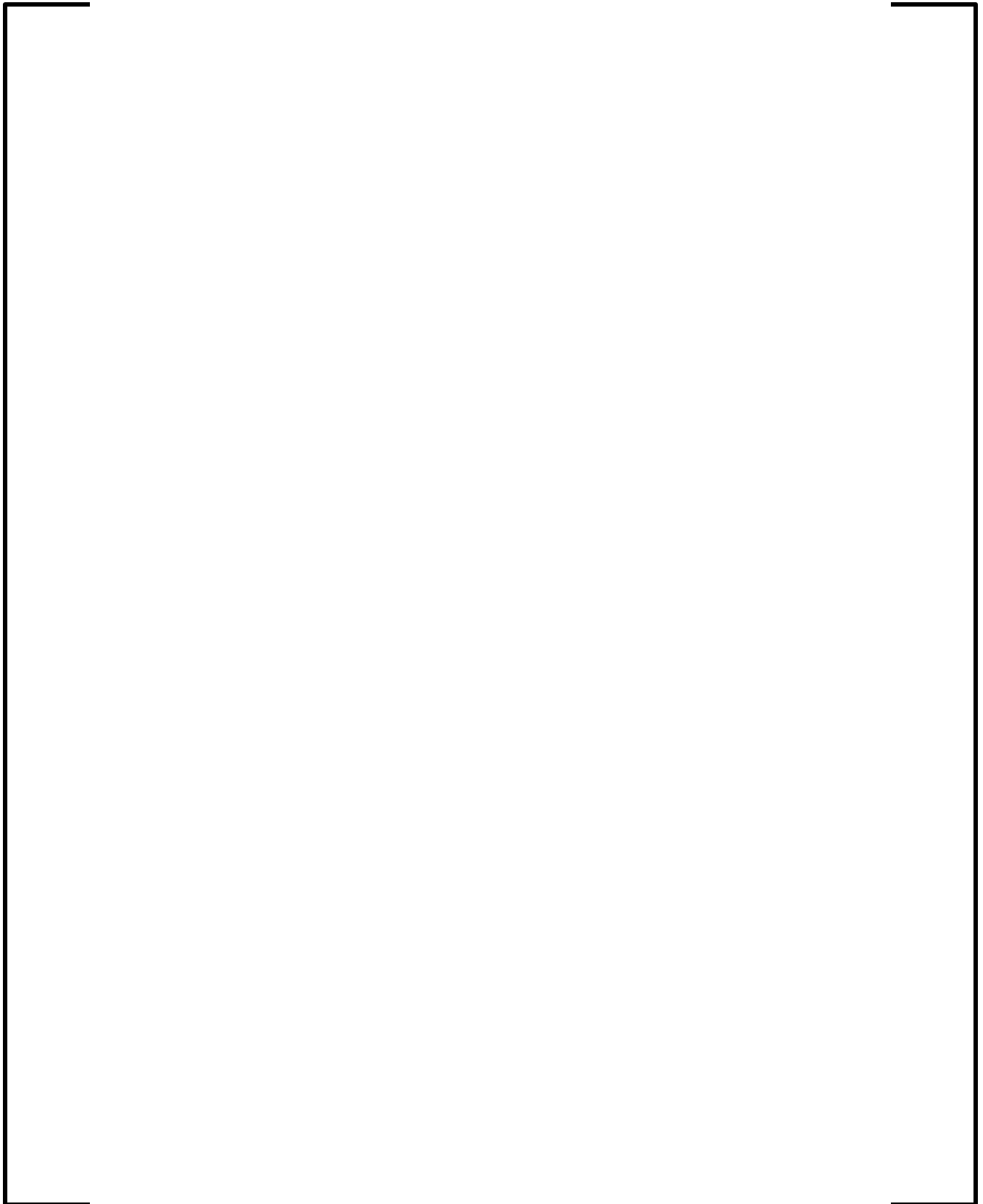














RAI 04: Figure 4-1, “AV42 Interfaces and Communications Links” shows communication from non-safety to safety and from safety to non-safety, as black arrows. **For non-Safety to Safety communication**, Section 4.8 contains a conceptual description of the control scheme. The AV42 TR does not contain a 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.

Response 04:

The Non-safety to Safety communication is performed through five (5) hardwired signal traces on the printed circuit board (PCB) of the AV42. These non-Safety to Safety signals originate from the Profibus Micro-controller and are sent to the PLD. The five signals are described below. Please refer to Figure 04-1 for a functional representation of the signals passed between the PLD and the Profibus Micro-controller. Also, please refer to RAI-03 for a description of each hardwired input and output pin as referenced in the text following Figure 04-1.

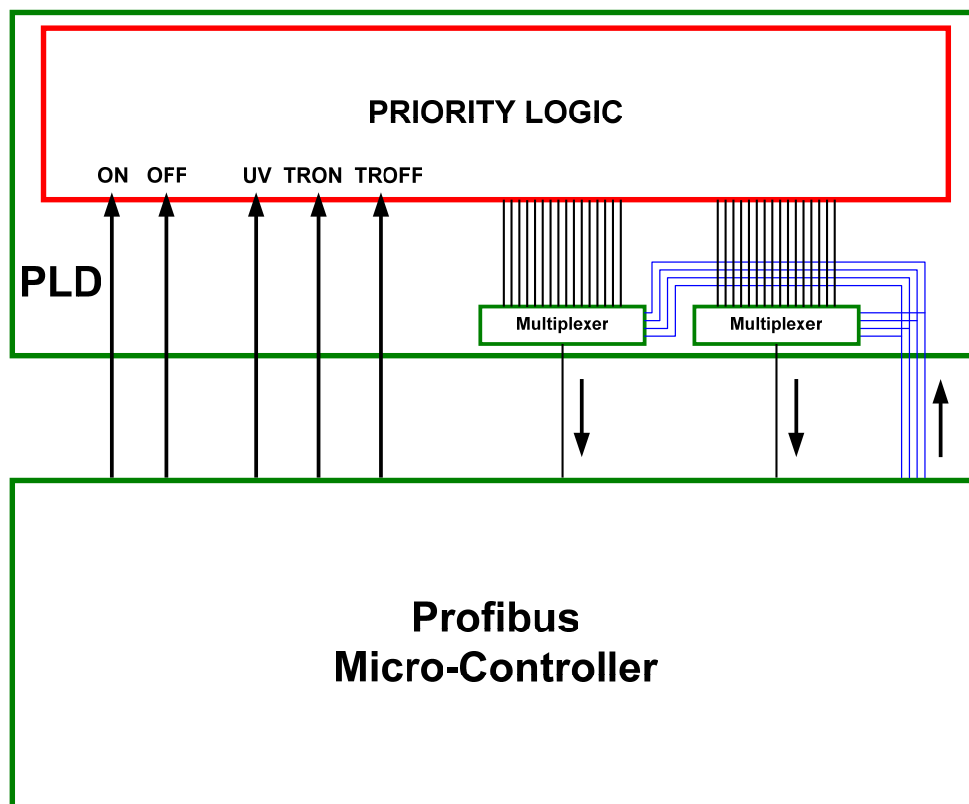
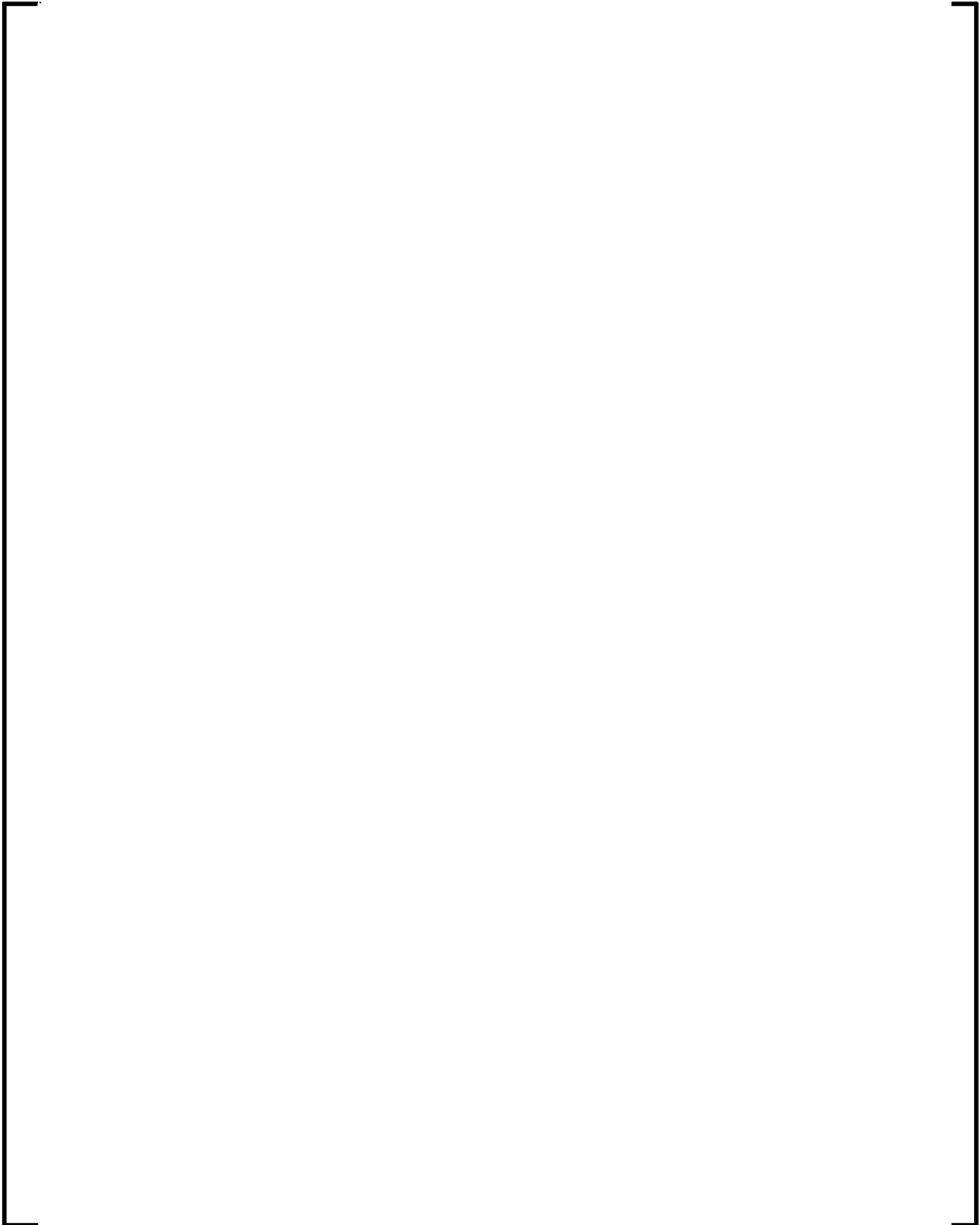
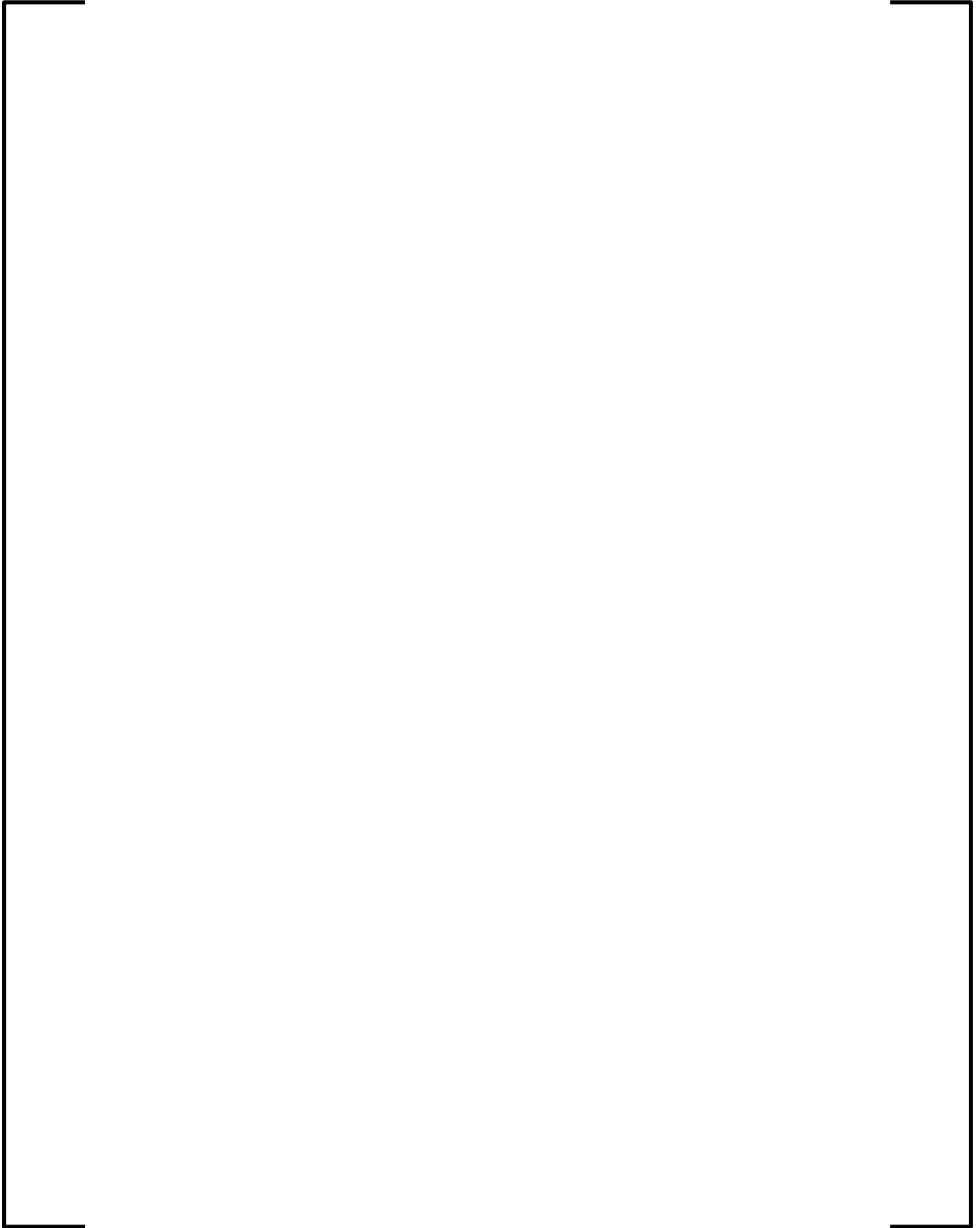


Figure 04-1

Functional representation of the signals passed between the PLD and the Profibus Micro-controller.





The safety function is protected by the priority logic of the PLD. Under no circumstances, can an operational command override a safety command. Safety commands always have priority over operational commands. The AV42 is 100% testable to ensure this feature. There is no parameter / setting that the user / installer could change that would result in an operational command overriding a safety command.

The logic configuration on the PLD is unaffected by communications commands. Commands from Profibus are forwarded to the PLD; the priority logic within the PLD will determine what command is sent to the actuator. If a safety command is issued, Profibus commands are blocked and the safety command is then sent to the actuator. The Profibus communications cannot alter the PLD logic, nor can it override a hardwired safety command.

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.

Response 05:

The Safety to Non-safety communication is performed through two 16-to-1 multiplexers. Please refer to Figure 04-1 for a functional representation of the signals passed between the PLD and the Profibus Micro-controller. These Safety to Non-safety signals originate from the PLD and are sent to the Profibus Micro-controller. The multiplexed signals are listed in Table 05-1.

The Profibus Micro-controller cyclically changes the address bus for the multiplexers. Depending on the 4 address bits (4 blue lines shown in Figure 04-1) the multiplexer will forward one of the sixteen bits to the Profibus Micro-controller. There are two multiplexers, therefore two bits will be sent concurrently. The data will be stored in the Profibus Micro-controller and will be used for processing of operational commands or forwarded to the Operational I&C system for diagnosis purposes.

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

Response 07:

Input simulations can be performed on the AV42 during maintenance and/or commissioning of the plant. There are three (3) simulation plugs located on the front of the AV42. A simulation plug is a two pin, female, shrouded connector. To issue a simulation command, a jumper wire will be inserted into the simulation plug to short the two pins together. The simulation commands are Open, Close, and Diagnosis. Shorting the Open or Close simulation plugs will cause the AV42 to issue an open or close command, respectively. Shorting the Diagnosis simulation plug will prevent any I&C system from exercising the actuator. The Diagnosis simulation plug is a lockout feature.

The simulation plugs are located on the front of the AV42. Simulation plugs are only used during maintenance and/or commissioning of the plant (not during normal operation of the plant). Administrative controls must be implemented in order to prevent simulations from being performed during normal operation of the plant.

Please refer to Figure 07-1 for a diagram of the AV42 front panel layout.

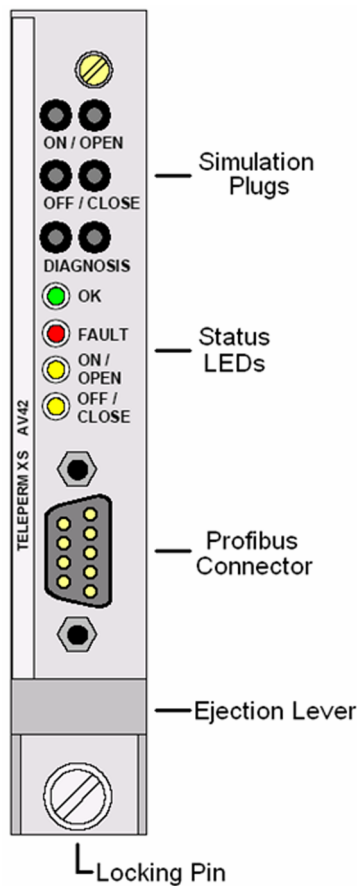


Figure 07-1
Front Panel of AV42.

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

Response 08:

There are two watchdog timers on the AV42. One of the timers monitors the Profibus Micro-controller. The other timer monitors the Profibus data connection.

The Profibus Micro-controller is monitored by an external watchdog timer. The external watchdog timer is implemented on a separate integrated circuit (IC) chip; which is independent from the PLD and the Profibus Micro-controller. The watchdog timer monitors the Profibus Micro-controller through the PLD. The watchdog monitors an output on the PLD which passes one of the address bits from the Profibus Micro-controller. The Multiplexers on the PLD are addressed by the Profibus Micro-controller, which cyclically changes the address bus. If the Profibus Micro-controller were to freeze or hang, the address bus would stop changing cyclically, and the output to the watchdog timer will remain constant. If the output to the external watchdog timer remains constant for more than 1.60 seconds, the watchdog timer will reset the Profibus Micro-controller. Please refer to Figure 08-1 for a functional representation of the external watchdog timer interface to the PLD and the Profibus Micro-controller.

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.

Response 19:

Section 4.2 of the proprietary version of the AV42 TR states that “the AV42 has the ability to block all non-safety inputs from the PROFIBUS controller. The manual actuation of the operation disable (OPDIS) signal is the hardwired input to the PLD that performs this function. The OPDIS switches are located in the MCR and RSS.”

For the U.S. EPR Design: A key switch or equivalent device is located in the MCR and RSS on a divisional basis. When a key switch in a division is activated, initiating an OPDIS input of “1” to the PLD, all operational commands from the PROFIBUS controllers within that division are ignored by the PLD.

This switch is available to the operator to isolate the Operational I&C signals from the PLD in the unlikely event of inadvertent operation of the Operational I&C system challenging a safety system. Use of the OPDIS command will be covered under plant operating procedures.

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.*

Response 20:

For the first sentence of the Abstract and second sentence of section 1.0 the term actuators does not have the same definition as “actuation device” as defined IEEE STD 603-1991. In this context, the term “actuators” was used incorrectly.

In this context, the term “actuators” was meant as sense and command features from the MCR (i.e. manual switches, buttons, etc) used to initiate a protective action.

The first sentence of the abstract will be changed as follows:

“This report describes the design features of selected signals from safety related Class 1E main control room and remote shutdown station devices used for manual initiation of a protective action, safety-related TXS system outputs and non-safety related control outputs.”

The second sentence of Section 1.0 will be changed as follows:

“The AV42 prioritizes the various input signals from safety related Class 1E main control room and remote shutdown station devices used for manual initiation of a protective action, safety-related TXS system outputs and non-safety related control outputs.”

The AV42 is not considered an actuation device as defined by IEEE 603-1991, but rather a sense and command feature that prioritizes “signals associated directly or indirectly with safety functions” and issues an output “to the execute features input terminals.”

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 with the criteria for electrical separation and independence of redundant systems.*

Response 21:

The AV42 module complies with IEEE Standard 384-1992 for electrical separation and independence of redundant systems. Electrical separation and independence is ensured by the proper installation and isolation of the AV42 using devices external to the AV42 module itself.

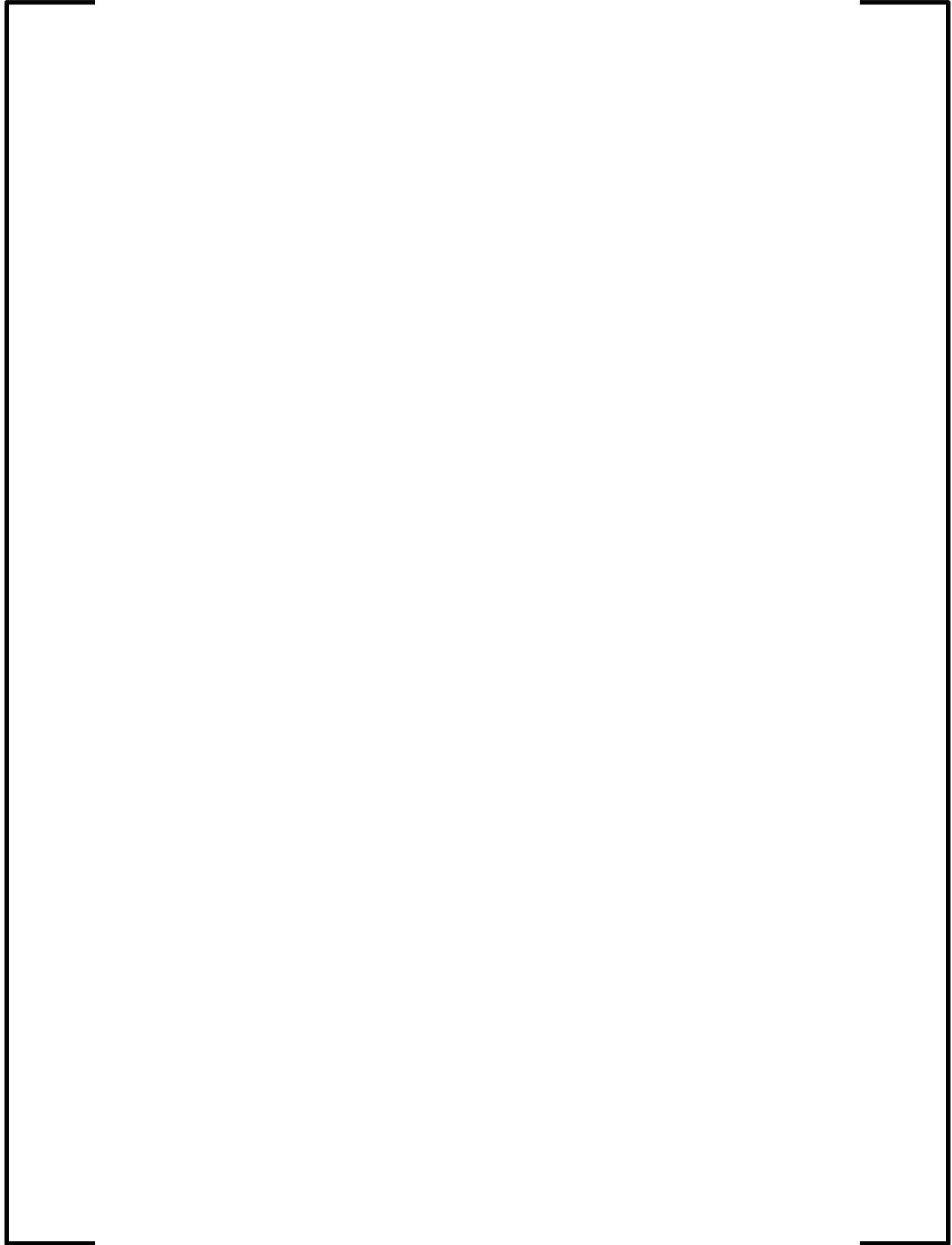
For the U.S. EPR design: Independence of redundant systems is met by having four redundant divisions, which are physically separated. For the most part the AV42 shall only interface with equipment in the same division. At the AV42 level, I&C system and actuator interfaces are completely divisionalized with few exceptions. Some exceptions are possible, and are implemented in order to comply with single failure criteria. Electrical isolation will be implemented on such exceptions to comply with IEEE Standard 384-1992.

Isolation of Networked (Profibus) Non-Safety Systems:

Electrical Isolation of the Profibus network is met by using optical cabling between the Operational I&C cabinets (non-safety) and the AV42 cabinets (safety). The use of the fiber optic isolation eliminates any credible electrical failure in the non-safety Operational I&C system from degrading the safety function of the AV42. Please refer to RAI-25 for a representation and further information on the use of optical cable between cabinets.

In addition to optical cabling, integrated opto-isolators are on the individual AV42 modules, which provide additional electrical isolation of the Profibus network. The Profibus connector and related circuitry is completely isolated from the rest of the AV42 components (PLD, Profibus Micro-Controller, Watchdog Timer, etc...). There are three optical isolators that are used to isolate the Profibus signals: Transmit, Receive, and Request to Send (RTS). There is an isolating voltage regulator that provides power to the isolated section of the AV42. The isolating voltage regulator and the three optical isolators are designed to withstand voltages up to 500 volts DC.





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.

Response 22:

The reference to section 6.7 will be removed.

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.

Response 23:

The reference in Section 3.0 is incorrect. The sentence will be changed as follows:

“Section 4.4, Testing, discusses the capability for testing and calibration considered during the design.”

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.*

Response 24:

Multiple AV42s can be attached to a single non-safety network, but there are limits to how many can be attached to a network.

The AV42 Profibus address is set by wiring the 6 address pins to high or low. The address pins are pin B18 through B28 []. A 6-bit binary number has 64 possible combinations (0 through 63). Of these 64 possible combinations, only 30 are valid for use with the AV42. Therefore, up to 30 AV42s can be attached to a single Profibus segment. A Profibus segment is defined as a “data network” that creates a physical connection between a Profibus controller (could have redundant controllers) and slave modules (in this case the slave modules are the AV42s).



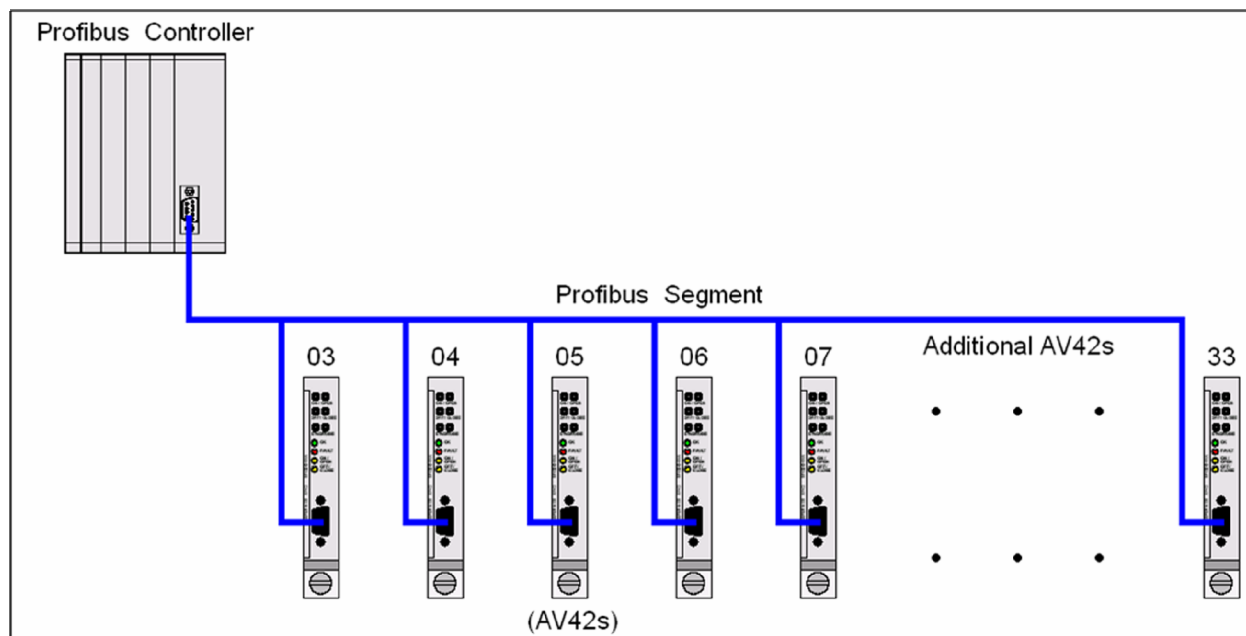


Figure 24-1
Representation of a general Profibus segment with AV42s.

For the U.S. EPR design: All AV42s, on a single Profibus segment, will be physically located and will control actuators within the same division as the respective Profibus controller. No Profibus segments for the AV42s will cross divisions. Also, a dedicated Profibus segment will be used for AV42s. If a Profibus segment is designated to interface AV42s, no other data acquisition or control modules (other than the AV42s and the Profibus controller) will be attached to the segment.

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.*

Response 25:

Connection of the AV42 to Operational I&C controllers is out of scope of the AV42 Topical Report, but examples are provided for the U.S. EPR design. Other network designs are acceptable and may vary based on the needs and architecture of a particular plant design

For the U.S. EPR design: All Profibus segments delegated to interface AV42s, will solely interface AV42s; no other data acquisition or control modules (other than the AV42s and the Profibus controller) will be attached to the dedicated Profibus network.

A maximum of 30 AV42s can be attached to a single Profibus segment; therefore if a network failure were to occur, it would only affect a maximum of 30 actuators. Please refer to RAI-24 for justification on the maximum number of AV42s on a Profibus segment.

Fiber optic cables will be used between the AV42 cabinets and the Operational I&C cabinets. Electrical Isolation is met using by using optical cabling between the cabinets. In addition to optical cabling, integrated opto-isolators are on the individual AV42 modules, which provide additional isolation. Please refer to RAI-21 for additional information on the integrated opto-isolators. Optical cabling is preferred for noise immunity. Optical Link Modules (OLMs) will be used to convert copper cabling to optical cabling.



Figure 25-1

Representation of a Master / Hot-Standby configuration with Y-circuit using optical cable.

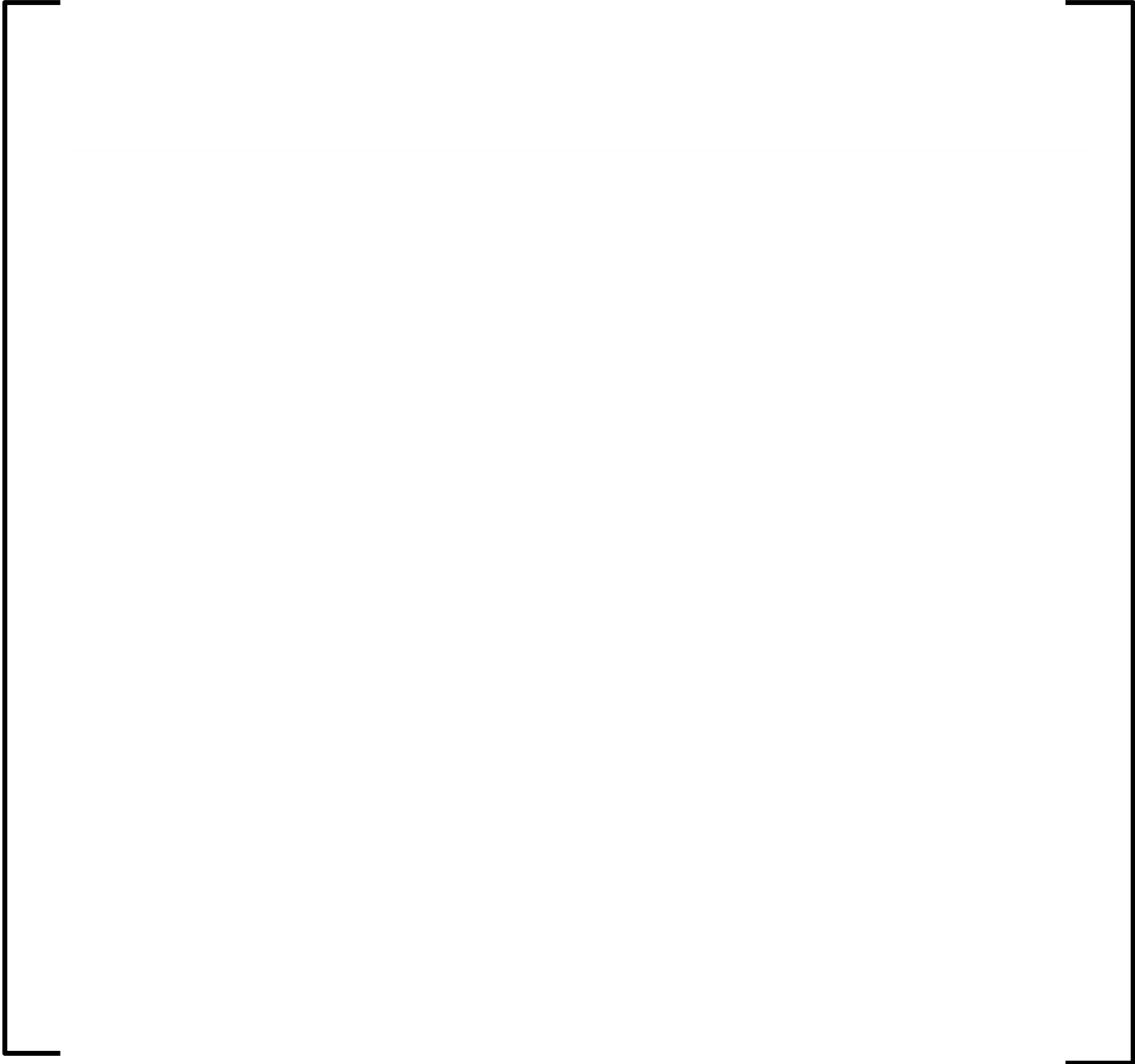


Figure 25-2
Example Configuration 2.

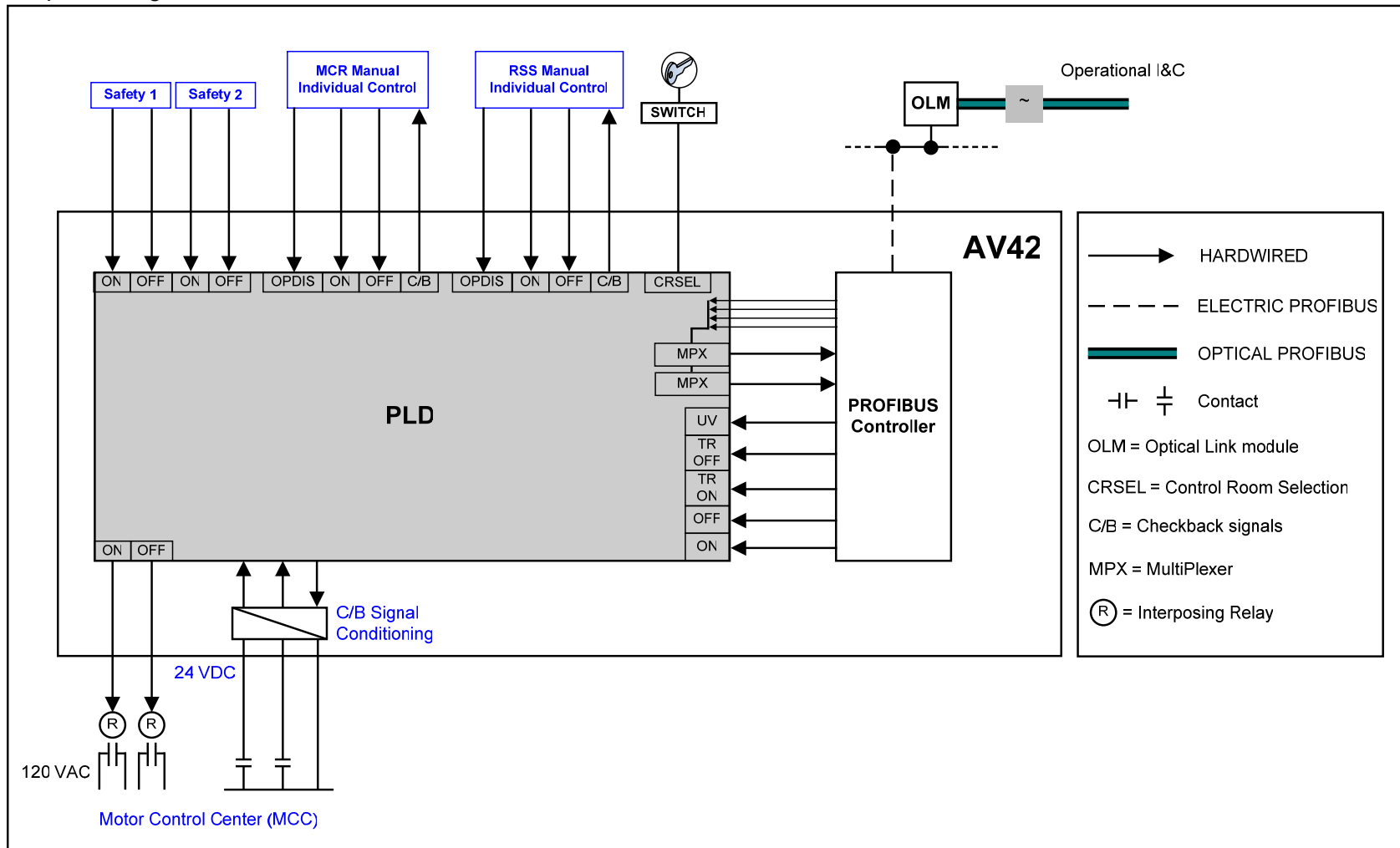


Figure 25-3
OLM and piggyback adaptor mounted in the Operational I&C cabinet.

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

Response 26:

See updated Figure 4-3 below.

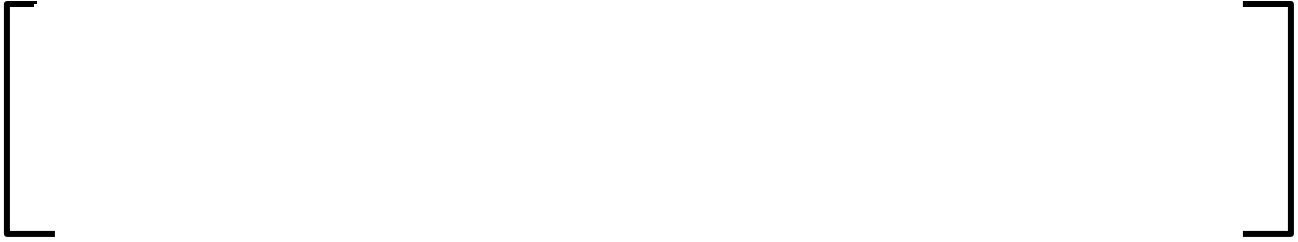


RAI-27: *Figure 4-4, "Priority Actuation and Control Logic Example," seems to be in incorrect or incomplete. Please provide a complete or corrected figure.*

Response 27:



Updated Figure 4-4



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

Response 32:

Switchover is accomplished by a hardwired input, which is initiated by manual action (i.e. keyswitch).

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.*

Response 39:

See updated Figure 4-3 above for legend of drawing symbols and abbreviations. Also, PIN abbreviations from the PROFIBUS Controller to the PLD are described in the response to RAI-04.

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.*

Response 41:

The AV42 can test the indicator lamps on the RPP, MCR, or RSS. There are three lamp test inputs for the AV42, one for each panel. Each input is wired directly to a momentary pushbutton on the respective panel (RPP, MCR, or RSS). When a lamp test input goes high ("1"), the indicator lamps related to the test input will also go high; when the lamp test input is removed (low), the lamps will return to their previous status (indication before the lamp test was activated). As long as the test input is high, the lamps will remain high, there is not a "time-out" associated with the lamp test function.

The lamp test function is used to ensure that the connection (wiring) between the AV42 and the indicator lamps are intact, in addition to the condition of the actual lamps (blown lights).

The lamp test function is used to ensure that the connection (wiring) between the AV42 and the indicator lamps are intact, in addition to the condition of the actual lamps (blown lights). It is also possible to have lamp test inputs from multiple AV42s connect to the same test switch/button on a panel; therefore, an entire panel can be tested at once. In this scenario, the lamp test inputs for the MCR would be wired to a button in the MCR, all the test inputs for the RSS would be wired to a button in the RSS, etc... A lamp test button should be physically located on the panel where the indicator lamps reside.

Please refer to RAI-03 for additional information on the input / output pins of the AV42.

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.*

Response 43:

The design details of fiber optic media converters are out of scope of the AV42 Topical Report, but information is provided to facilitate an understanding of these converters. The use of media converters will depend, and vary based on the needs and architecture of a particular plant design.

Fiber optic media converters are used for the sole purpose of converting an electric Profibus line to a fiber optic Profibus line. There are multiple reasons for using media converters in a particular network topology:

- Electrical isolation:

Fiber optic cable provides electrical isolation between the fiber optic media converters.

- A need for longer cable runs:

Fiber optic cable runs can be longer than electric cable runs.

- Redundant / dual feeds:

Most media converters offer the ability to have two fiber optic feeds connecting converters.

- Linking multiple electric networks together:

There is a limit of 32 nodes that can be attached to a single RS485 segment (electric Profibus network), but the actual Profibus protocol defines the node limit at 128. By using media converters and daisy-chaining them together using fiber optic cabling, multiple electric segments can be linked together forming one large Profibus network.

- Fiber optic ring network:

There is the option to create a fiber optic backbone in the form of a ring using media converters.

Currently, media converters are available in the commercial market, which are offered by multiple manufacturers. The design details of each of these converters, from each of these manufacturers, is unknown and is not important for application of the AV42.

AREVA offers a fiber optic media converter, which is part of the TXS platform, and is known as an Optical Link Module (OLM).




Figure 43-1
Optical Link Module and cable connections.

**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 US 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:

(1) In the current equipment version of AV42, the PLD family MAX 7000 A and the specific PLD device type EPM7512AETC144-xx are used. The PLD on the AV42 does not depend on memory to provide output to safety components.

(2) Binary inputs from field signals, from upstream I&C commands, and parameterization commands to the AV42, as well as its binary outputs are identified in the list of the pins of the male connector described in the response to RAI 03. Inputs that are routed to the PLD are identified in this list, as well as outputs of the PLD routed to the module's connector.

Additionally, a set of PLD inputs and outputs are assigned to the multiplexer function managing the information exchange between the PLD and the Profibus Controller. Details of this information exchange scheme are in the response to RAI 04 and RAI 05.

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:

1.) Request for a detailed design representation

The design of the AV42 PLD logics has been performed in three stages:

- (1) a requirement specification describing the functionality in plain text and case by case logic diagrams (available in German language)
- (2) a design specification again describing the functionality in text and case by case logic diagrams where appropriate (in addition to the requirement specification), including the signal names used and more specific details in selected logic diagrams where useful (available in German language)
- (3) detailed design specification, using the ALTERA tool for PLD programming with pre-defined function blocks. An example excerpt of this detailed design specification is provided in Figure 06-1 below (signal names in German language).

Experience shows that this detailed design specification (3), although showing the exact logics and functions of the PLD, is not adequate to provide a thorough understanding of the overall functionality to a user of the module or to a reviewer. However, the enclosed example sheet gives an impression of the nature of this design level. If required, more examples can be provided in the context of a clarification meeting.

The most adequate level of description is by identifying the pins, their roles, and a description of the functionality by text, tables and diagrams where applicable. Therefore, the explanation of the AV42 functionality is provided using text, tables and graphical presentations, so as to communicate a good understanding, in the same way as provided in the AV42 user manual.

These explanations have been derived and optimized based on the AV42 requirements (1) and design specifications (2), and only in exceptional cases from the detailed design specification (3) for specific details.



Figure 06-1: Example excerpt of Detailed Design Specification

2.) The following is a description of priority handling between the PLD and Profibus Controller.

There are two fundamental operating modes for the AV42 module, normal control mode prioritization when no safety signal is present and safety signal priority mode which blocks any software related control functions and uses only the PLD preprogrammed safety logic function.

The non-safety Controller generates commands, sent to the PLD, based on the following inputs:

- Commands from the Operational I&C system, received via Profibus DP. These are commands such as automatic start/stop commands or manual commands from a non-safety, screen-based Human-Machine Interface (HMI).
- Checkback signals (torque, limit)
- Desktille commands including control room selection input
- Undervoltage signal received by the AV42 via binary input or via Profibus DP

This processing considers the settings of the parameterization pins via the 64-pin connector and also the parameters received from the Operational I&C via Profibus DP. Resulting commands are output as binary signals to the PLD.

The PLD provides a command output based on the following inputs:

- Checkback signals (torque, limit)
- Simulation commands (from simulation pins on the front plate of the module)
- Safety I&C commands
- Desktille commands including control room selection input
- Non-safety Operational I&C commands, as a result of the processing in the Controller based on command inputs via Profibus DP from the Operational I&C system and the desktilles (above)
- command termination from non-safety Operational I&C (based on torque, travel limit), as a result of the processing in the Controller (above)
- Undervoltage signal as a result of the processing in the Controller (above)

The PLD only considers the settings received from the parameterization pins on the 64-pin connector.

3.) The following is a description of the priority handling in the Controller for commands via Profibus DP, Operational desktile commands, and undervoltage commands.

If the OPDIS signal is not present, the appropriate operational command is selected from the active commands based on the priorities listed in the tables below. The resulting Operational command is sent to the PLD by the Controller as an operational “ON” or operational “OFF” depending on the direction. See the response to RAI 04 for more information on these two inputs to the PLD.

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)

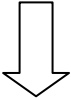
Command Type	Priority
Countermanding manual commands	1
Mechanical Equipment Protection commands	2
Commands from automatic control system	3
Manual commands from desktile	4
Manual command from the OM	5

Table 06–3: Prioritization of operational commands for closed-loop-controlled actuators in “Closed-loop” control mode (1 = highest priority, 2 = lowest priority)

Command Type	Priority
Mechanical Equipment Protection commands	1
Commands from automatic control system	2

4.) The following is a description of the overall priority handling of the AV42.

Table 06–4: Priority List for the PAC module

Priority 	Simulation Commands (using coding plugs on the AV42 front panel)	
	Safety I&C commands	
	Commands from the Monitoring Functions performed within the AV42	
	Commands from the Operational I&C via Profibus DP: <ul style="list-style-type: none"> • Equipment Protection • Closed-loop commands • Automatic commands 	
	Manual commands from desktils	Manual commands from the Operational I&C via Profibus DP

Notes:

- Depending on parameterization of the AV42, some monitoring functions performed within the AV42 can block the Operational I&C commands. Examples of such functions are discrepancy between limit switches, discrepancy of switch-over contacts, etc. This parameterization is unique to each actuator and is determined during the detailed design phase of the system. Once determined during detailed design, the type of setup for each AV42 module as relates to the type of device being controlled (MOV, Solenoid Valve, etc.) is set by the backplane wiring for a given AV42 card slot. Therefore, any AV42 module can be inserted into a specific slot and it will be appropriately configured for safety system actuation for the device actuated from that physical location in the cabinet, no reprogramming of the AV42 module is required.
- Commands in the shaded areas are not considered if the OPDIS signal is active. See the response to RAI 03 for more information on the OPDIS signal.
- During normal control mode, manual commands from the desktils and manual commands from the Operational I&C via Profibus DP are equivalent. However, desktils have priority over manual commands from the Operational I&C as long as the desktil command is active (OPDIS is inactive and no safety signal is present).

4. Signa 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.

For protective actions, the PLD provides a command output based on a safety system input. The output could be a result of an automatic safety system input or manually initiated input (See RAI 06 & RAI 27 responses for information on prioritization). The safety system actuation requests are input to the PLD via pins on the 64-pin connector (See the response to RAI 03 for more information on these inputs). When a protective action initiates an input high (24 VDC), the PLD provides a command output to the switchgear to drive the actuator to the proper state. For example, when the Protection System (PS) initiates a containment isolation function, the input to Pin F04 [] goes to 24 VDC. The PLD then initiates a command output from Pin Z20 [] to the electrical switchgear to close the isolation valve.

Once the protective action is complete (i.e. valve is shut, pump is running), torque and/or limit switch checkback signals input to the PLD indicate completion of the function and thus the protective action. For the example of the containment isolation valve, when the valve reaches its limit, PLD input Pins F18 [] and F26 [] provide torque and limit checkbacks to the PLD and corresponding command termination. (This is also dependent on the setting of the parameter pins. See RAI 03 and RAI 48 responses for more information).

Once the PS output has been reset, the PS output to the PLD is terminated and an additional deliberate command in the open direction is required to return the valve to normal. An additional command is also required for any closed loop control valves as the control loop is placed in the manual mode when a safety signal is generated therefore it remains in the safety position until the operator takes an action to reposition the valve. Therefore, in order to re-open a containment isolation valve after an isolation protective action, the Operator must manually initiate a command in the open direction; reset of the PS alone will not reposition the valve.

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 US 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.”

Per IEEE 603-1991 Section 5.2, the safety related PACS system (which is comprised of AV42 modules) performs its designated protective action once initiated automatically or manually by the Protection System (PS) or Safety Automation System (SAS) or manually from the desktils in the Main Control Room (MCR) or Remote Shutdown Station (RSS). The PACS performs the protective action until completion. See the response to RAI 10 for an example.

The PLD of the AV42 does not latch input signals from the PS or SAS. The inputs to the PLD are direct outputs from the PS or SAS (these inputs are []). Therefore, for commands initiated by the PS or SAS, the protective action is latched in the PS or SAS TXS logic and the command is not released until reset in the PS. This reset releases the input to the PACS by terminating the output command of the PS or SAS and therefore the input command to the PLD. Even when the PS or SAS are reset, the device being controlled by the PACS remains in the safety position.

For manually initiated protective actions wired directly from desktils in the MCR or RSS, the AV42 latches the input commands []. These commands remain active until deliberately reset by the operator. For an additional description, see the response to RAI 03, Pins F30 and D30.

Thus, the Priority and Actuator Control **System** complies with IEEE 603-1991 section 5.2. For protective actions initiated by the PS and SAS, safety actuation signals are latched in by the TXS system. For manual protective actions initiated from the desktils in the MCR or RSS and wired directly to the AV42, this is performed by the AV42.

Per IEEE 603-1991 Section 7.3, the execute features will perform a protective action to completion when commanded by the PACS system. When the sense and command features are reset (PS, SAS, PACS), the execute features do not automatically return to normal. Separate, deliberate operator action is required to return the execute features back to normal with the exception of the specialized ESF function for the CVCS pressurizer level control valve as described in the RAI responses to the US EPR, PS topical report. Ref

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 US 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)

These configurations are specified during the detailed design phase of the plant. Standard wiring and parameter schemes are developed and a project-specific specification of actuator control modes is produced for the plant. These standards will then be used to establish individual wiring drawings and parameter sets for every individual actuator. The parameter setup for each AV42 module is determined during detailed design and is implemented for a specific device by wiring the AV42 backplane slot in a specific way for the device being controlled from that card cage slot. Once this backplane wiring is done, any AV42 module may be used in that slot and it will operate the device being controlled in the proper manner.

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.



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."

To respond to bona fide safety signals, the safety I&C test initialization signal is cancelled by the safety I&C system if a valid safety command is present. This allows the AV42 to immediately respond to bona fide safety signals during testing intervals. See Figure 15-1 for a sample of the test logic.

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.

For testing connection to the AV42 module the following sequence is necessary:

- 1.) The Operator must initiate the test program ("test start")
- 2.) The AV42 module will be set to test mode by the "test initialization" signal ("test init").
- 3.) As long as the AV42 is in test mode, all normal control signals will be ignored by the AV42. In order to respond to bona fide safety actuation request, the test initialization signal is blocked by the PS upon a safety actuation request. (See Figure 15-1 above)
- 4.) As a confirmation of receiving the "test initialization" signal, the check back signals will be inverted.
- 5.) An actuation signal ("test on/open") will be sent to the priority module, which forces the check back signals to change state again. This is automatically evaluated by the test logic (which is not explained here); in case of fault, a failure signal is provided.
- 6.) The testing of the AV42 modules has to be aborted when a real actuation signal appears ("actuation on/open"), or when the operator manually stops the test ("test stop"). In this case the "test initialization" signal is blocked, and actuation signal will be sent.

The overlapping test initiated by the safety I&C is designed to be completed within 2.5 seconds of the safety I&C test initialization signal activation. After this short time, the AV42 will leave test mode independently from the test initialization signal.

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:

- 1.) via the status word of the Profibus DP message to the Operational I&C system and ultimately to the non-safety screen-based HMI in the MCR.
- 2.) via output pins hardwired to the safety related HMI and desktils in the control room or other safety I&C systems.

The Profibus Controller obtains information from the PLD via the multiplexer. A list of the multiplexed signals passed from the PLD to the Profibus Controller is given in the response to RAI 05. A description of each signal is provided in the response to RAI 03. These status signals, including other non-safety status information from the Controller, are sent in the status word to the Operational I&C system.

Status information received by the Operational I&C system from the AV42 via the status word is displayed on the non-safety plant displays or sent to non-safety archiving devices. This information is not sent to any I&C safety system and is therefore not used for any decision purposes in these safety systems.

Hardwired status signals are sent via output pins of the AV42 to a safety system. A description of each signal is provided in the response to RAI 03. These signals are 0 or 24VDC outputs from the PLD.

Since the safety status signal outputs are 0 or 24VDC outputs, the use of such signals is dependent on plant specific architecture. Signals could be sent to any safety I&C system and / or directly to desktils on a panel in a control room. Since the AV42 supports either configuration, plant specific architecture is considered outside the scope of the AV42 Topical Report but an example configuration is provided below for the U. S. EPR I&C architecture. For complete details on the architecture, see the U. S. EPR Protection System Topical Report, ANP-10281P and the U. S. EPR Final Safety Analysis Report.

Example configuration for the US EPR:

For the US EPR, the Protection System (PS) and Safety Automation System (SAS) do not receive status signals from the AV42. All safety status signals output from the AV42 are received by the safety related Safety Information and Control System (SICS) in the Main Control Room (MCR) or Remote Shutdown Station (RSS).

The PS and SAS send commands to the AV42 via hardwired inputs. The logic that originates these command inputs is not dependent on any status signal received from the AV42.

Status signals received by the SICS are used by the operators for decision purposes when initiating manual system level or component level safety commands. Status signals are obtained by either conventional I&C indicators (i.e. lamps) or a safety related Qualified Display System (QDS).

A simplified configuration is presented in Figure 16-1. This is a functional example only. Details on whether signals are obtained by QDS or conventional I&C devices are determined for each specific plant during its detailed design phase. Also, manual system level actuation that is initiated through the PS or SAS is not shown.

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.

Spurious orders created within the Operational I&C system are avoided to the point that the Operational I&C and Profibus DP messaging scheme allows. That is, if a properly configured Profibus DP control word is initiated by the Operational I&C system [

the AV42 will perform non-safety prioritization within the Profibus Controller and send a command to the PLD. For more information on the protective provisions used within the non-safety Operational I&C system and Profibus DP messaging scheme, see RAI 28, RAI 33 & RAI 34 responses.

The AV42, however, does ensure that safety orders are executed (due to the priority scheme) even in the case a spurious order is sent by the Operational I&C system. The priority scheme blocks any erroneous signals from the normal control system during a safety system actuation.

The normal control system signals are allowed to pass through the PLD if a safety signal is not present, normal control does not affect or control safety signal priority to the actuated device.

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 US 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:

- 1.) Cyclic messages between the non-safety I&C and the AV42 for the exchange of commands and status information
- 2.) Parameterization messages, based on cyclic or acyclic communication
- 3.) Diagnostic messages, based on cyclic or acyclic communication

Commands are sent using a cyclically transmitted 16 byte control message. Operational commands are the main entity being sent with 6 bytes reserved for the control word.

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.

- (1) For the implementation of the programming of the PLD, the standard tool MAX+plus II 9.6 or 10.2 provided by ALTERA has been used. (That is, version 9.6 was used for now obsolete AV42 version 6FK5249-8AA and version 10.2 is used for the current AV42 version 6FK5249-8CA).

ALTERA provides documentation about this tool and technical support for this tool.

No specific process of accepting this tool has been performed, taking into account its off the shelf nature, and its exclusivity to support MAX9000 PLD logics implementation. However, because of the simple design of the PLD and limited number of gates used, decomposition test cases are performed to confirm 100% of the intended software functional implementation. Please see 2, 3 and 4 below for a description of the testing.

- (2) For the functional programming, the tool set of the TELEPERM XS Core Software has been used, i.e., all signal processing has been specified using the graphical editor of TELEPERM XS, and the C-code executed on the microprocessor has been generated using the TELEPERM XS code generators. These tools are AREVA NP's standard tools for the implementation for application software for TELEPERM XS systems; maintained and continuously improved according to the configuration management and change procedures for TELEPERM XS.
- (3) A software development environment for C-language is used from KEIL. KEIL C tool suite is a recognized off-the-shelf development environment, supporting the microprocessor used in the AV42. (Note that this deals only with non-safety functions.)
- (4) SIETAL Test program AV42 for ERBUS PE2000 is used. SIETAL is a scripting language for implementation of automatic test programs. It has been used in AREVA NP GmbH (formerly Siemens KWU N) and other Siemens departments for many years in various types of test applications.

SIETAL+ has been used for periodic testing of safety I&C systems in Nuclear Power Plants for more than 20 years, in the framework of the ERBUS PE2000 test machine (product of AREVA NP GmbH).

The test scripts and script execution environment for the AV42 qualification testing has been verified by TÜV Rheinland and practically tested.

Overall Approach for Qualification Testing

The design of the AV42 module comprises three major domains:

- 1) Hardware design and implementation
- 2) Software design and implementation for the non-safety portion in the microprocessor
- 3) Configware (Note 1) design for the safety-related logics implemented in the PLD.

Note 1: The term Configware (derived from Configurable hardware) is used to differentiate the programming of a PLD from that of a computer or microprocessor with serially executed instructions. However, in most of the AV42 development documentation, the term 'firmware' is also used.

Module qualification for safety functions covers the safety-relevant domains in the following way:

- the hardware design is subject to an equipment qualification program, including theoretical evaluation (such as critical load analysis, verification of the manufacturing documentation) as well as practical testing comprising tests of electrical properties, climatic testing, EMC testing and seismic testing. This qualification is performed for the entire component without making a difference between safety-related and non-safety related portions.
- the qualification program of the safety functions implemented in the PLD was based on functional testing. Every AV42 function has been covered by a dedicated test. Priority management of safety, operational and manual commands has been subject to testing of the full set of input signal combinations for these commands.

Verification of PLD programming by 100% decomposition testing

The basis for this qualification approach relying on testing of the PLD functionality is the fact that the functions implemented in the PLD are well structured into sub-functions, with restricted interactions.

This allows decomposition of the total functionality into sub-functions with very limited interfaces. The number of inputs and outputs of every sub-function is intentionally limited so that full combinatorial testing of the priority handling is possible.

Additionally, the design is such that the module ensures proper priority handling of safety I&C signals. The logic is designed in such a way that in case of an active safety I&C actuation signal, all non-safety inputs are blocked. This is relatively easy to verify by test (the actuation outputs only depend on the safety I&C signal and the command termination).

Test environment used for functional testing

For the practical testing, an ERBUS test machine is used which sets test signals via binary output cards connected to the AV42, and to read back binary signals and compares them with the expected values. The test machine also allows setting of parameters for the microprocessor via acyclic Profibus DP services and to send cyclical control messages (e.g., operational I&C commands), and evaluate the cyclical check-back messages from the AV42.

The test cases have been implemented using a test programming language in a test script (test program), which runs all test cases automatically (with a few exceptions requiring manual intervention), and also automatically compares the check backs (binary signals and contents of Profibus DP messages) with the expected values.

Every test case is specified in detail in the test script, including the settings of parameters and all changes of input and interface signals to other sub-functions. The complete list of test cases used is provided below.

To understand the principle of de-composition into sub-functions, a few test cases from the list below are explained in more detail.

Test cases 2.1 – 2.6: Test of priority handling of the simulation commands

In this set of test cases, the handling of priority between the simulation signals on the front plate is verified.

Test case 2.1 verifies:

- the execution of the 'Simulation On' command
- command termination in 'on/open' direction on torque and travel limit signals
- priority of the 'Simulation On' command over the four safety I&C commands, the manual commands and operational I&C commands
- the output of hardwired status signals and Profibus status messages

In this test, only one of the safety I&C manual and operational I&C commands is set to "high" at one time; multiple commands set to "high" are not considered. This is due to the fact, that a separate set of test cases (18.1 – 18.11) has been specified where these command signals are permuted in all combinations.

Also not all permutations of command termination variants (travel limit only; travel limit with torque etc.) are considered. This is due to the fact that the handling of command termination is checked in a dedicated set of test cases (TC 19.1 – 19.11).

Test case 2.2 verifies the execution of the 'Simulation Off command', the command termination (one variant only), the priority over all other command signals, and the signaling.

Test cases 2.3 – 2.6 then verify the 'Diagnosis' command, the priority of the 'Simulation Off' over 'Simulation On' command, and the priority of the 'Simulation On' and respective 'Simulation Off' command over the 'Diagnosis' command.

Test cases 18.1 – 18.11: test of the priority handling between safety I&C, manual and operational I&C commands

In this group of test cases, the priority handling of all permutations of signal values of safety I&C commands, manual commands from desk tiles, and operational I&C commands are verified, as processed by the PLD. (Note that priority handling between different types of commands via Profibus DP, such as manual commands from screen-based HMI, automation commands, or component protection commands, is performed by the Profibus Controller, and only a result signal is forwarded to processing in the PLD.)

Test cases 18.1 – 18.4 verify the priority handling to generate a command signal between all combinations of the four safety I&C command signals (SFOFF1, SFON1, SFOFF2, SFON2) and of the manual commands from the desk tiles in the main control room, with commands via Profibus DP blocked (OPDIS = 1), and with all combinations of manual commands from the Remote Shutdown Station (RSS) blocked (RSS not selected, CRSEL = 0).

Test cases 18.5 – 18.8 check the same, but with the RSS selected.

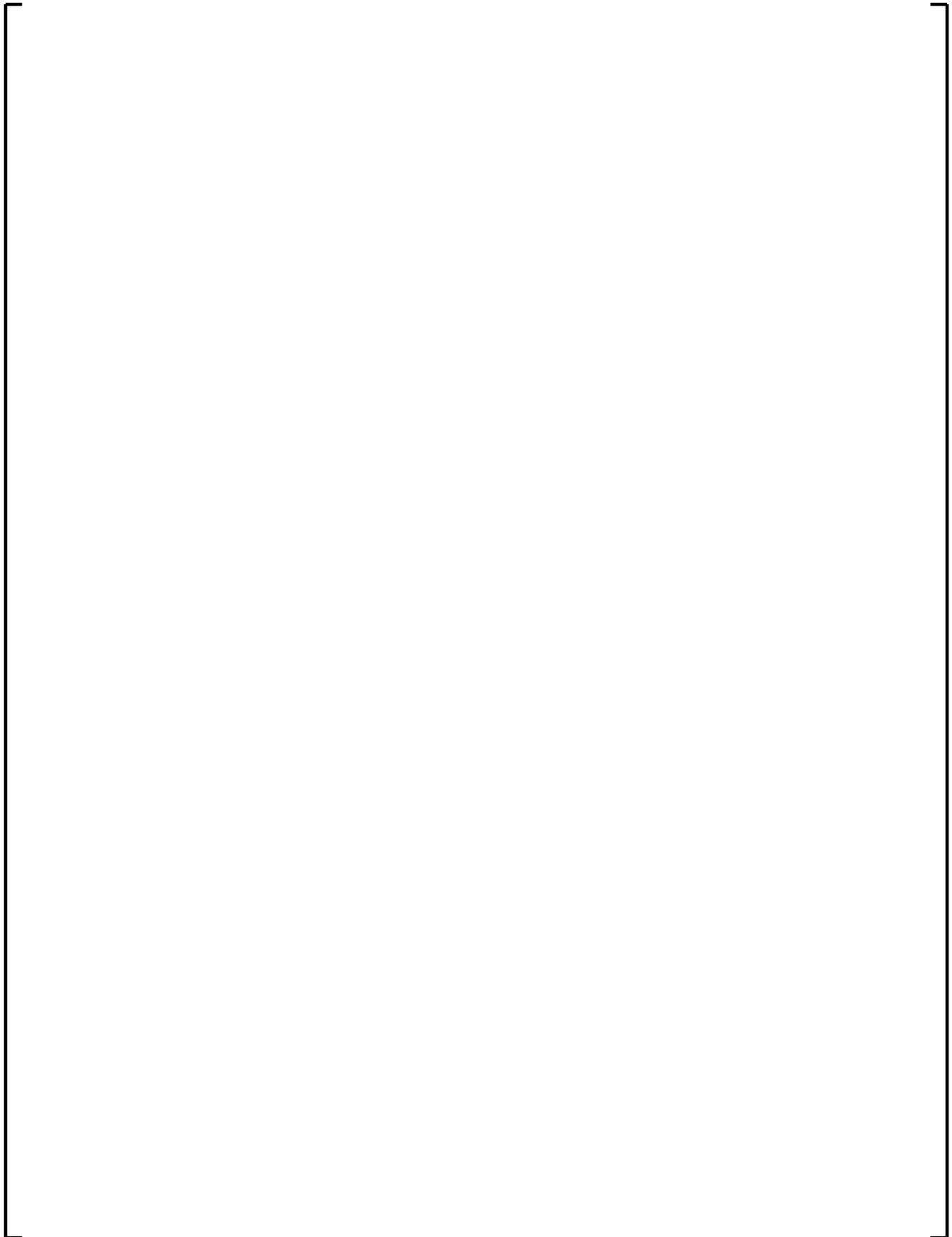
Test case 18.9 checks the proper priority of the safety I&C commands over the operational I&C

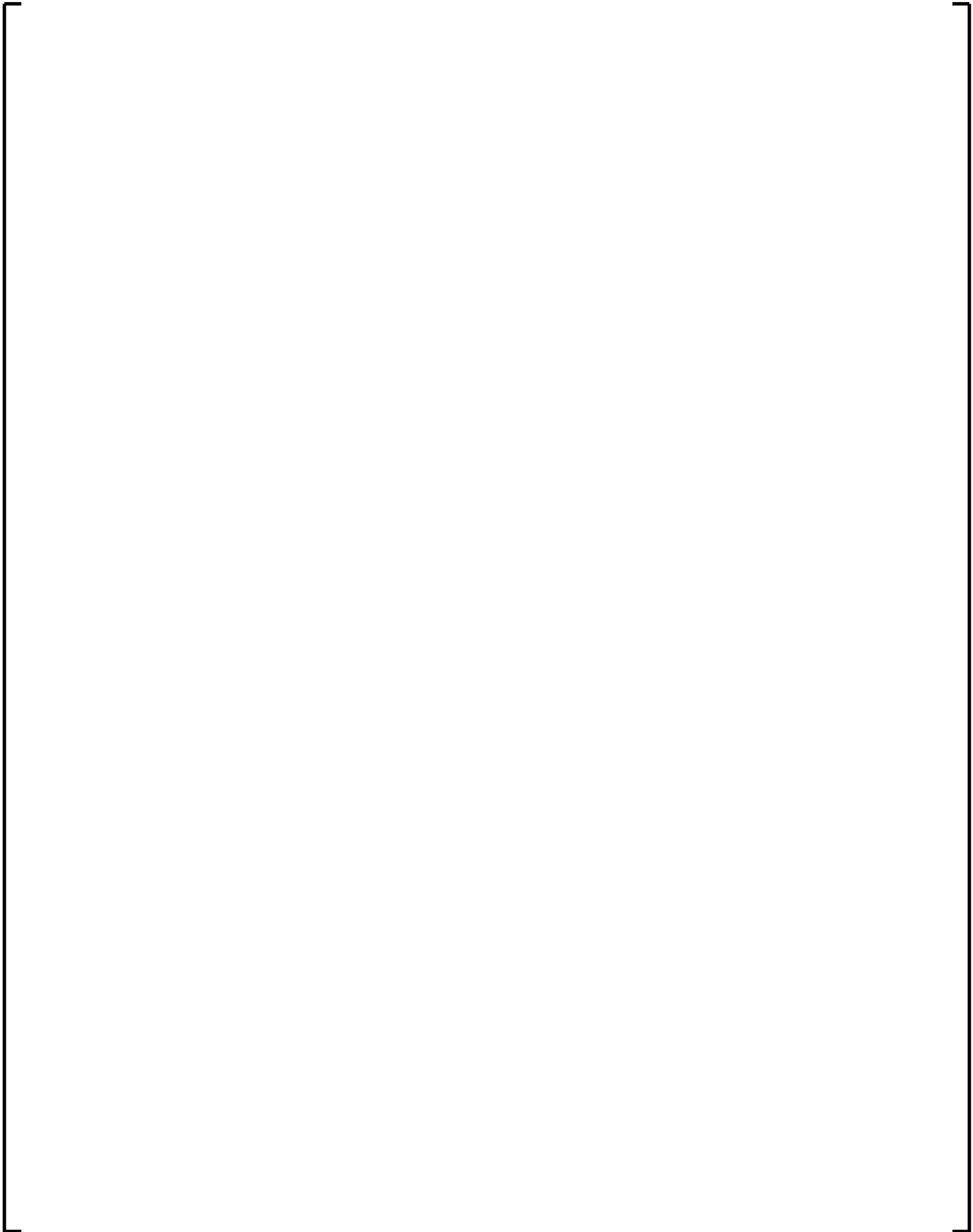
commands from Profibus DP. (Again, all combinations of the safety I&C commands and of the operational I&C commands via Profibus DP are considered.)

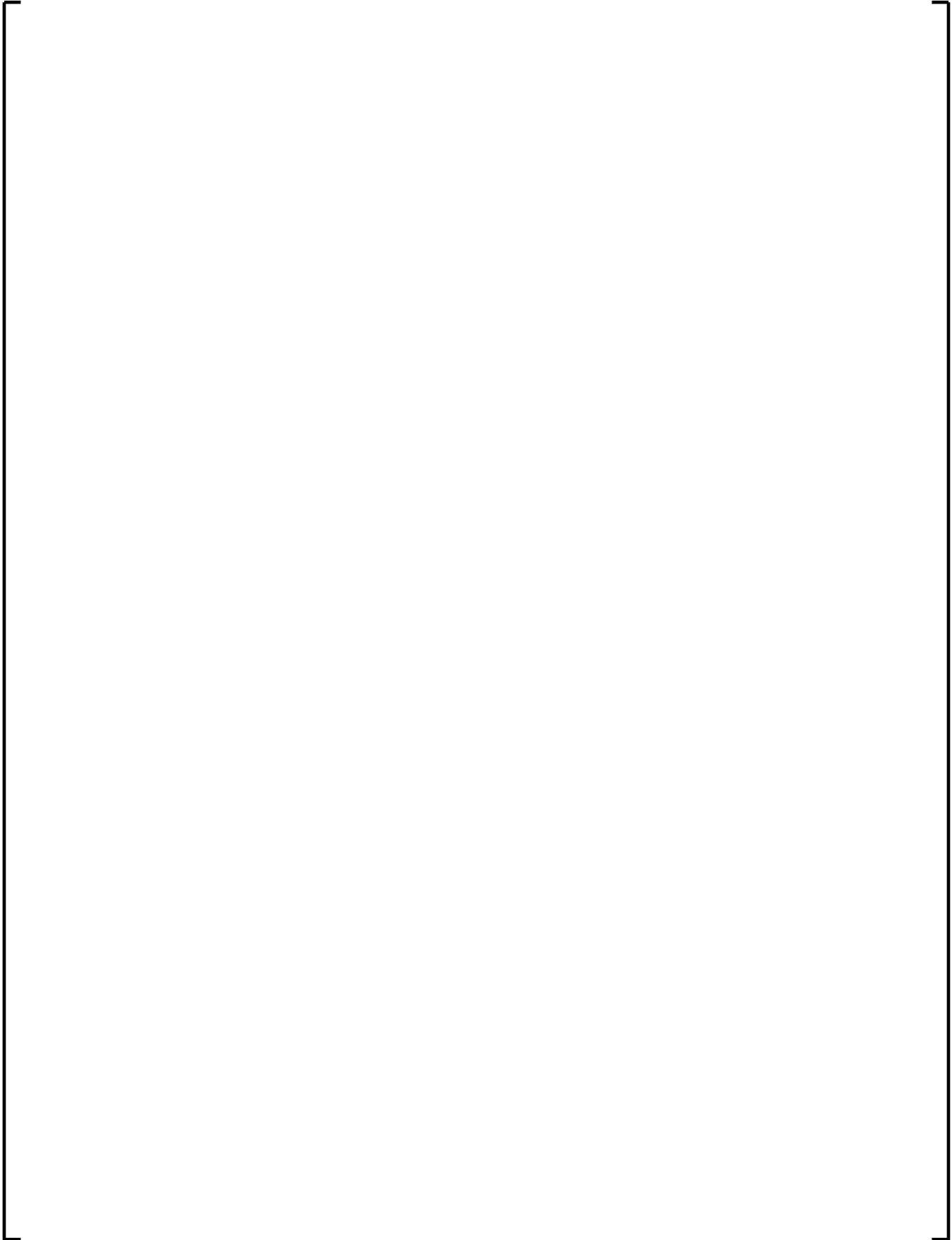
Finally, cases 18.10 and 18.11 check the proper handling of the STOP command from the MCR and RSS.

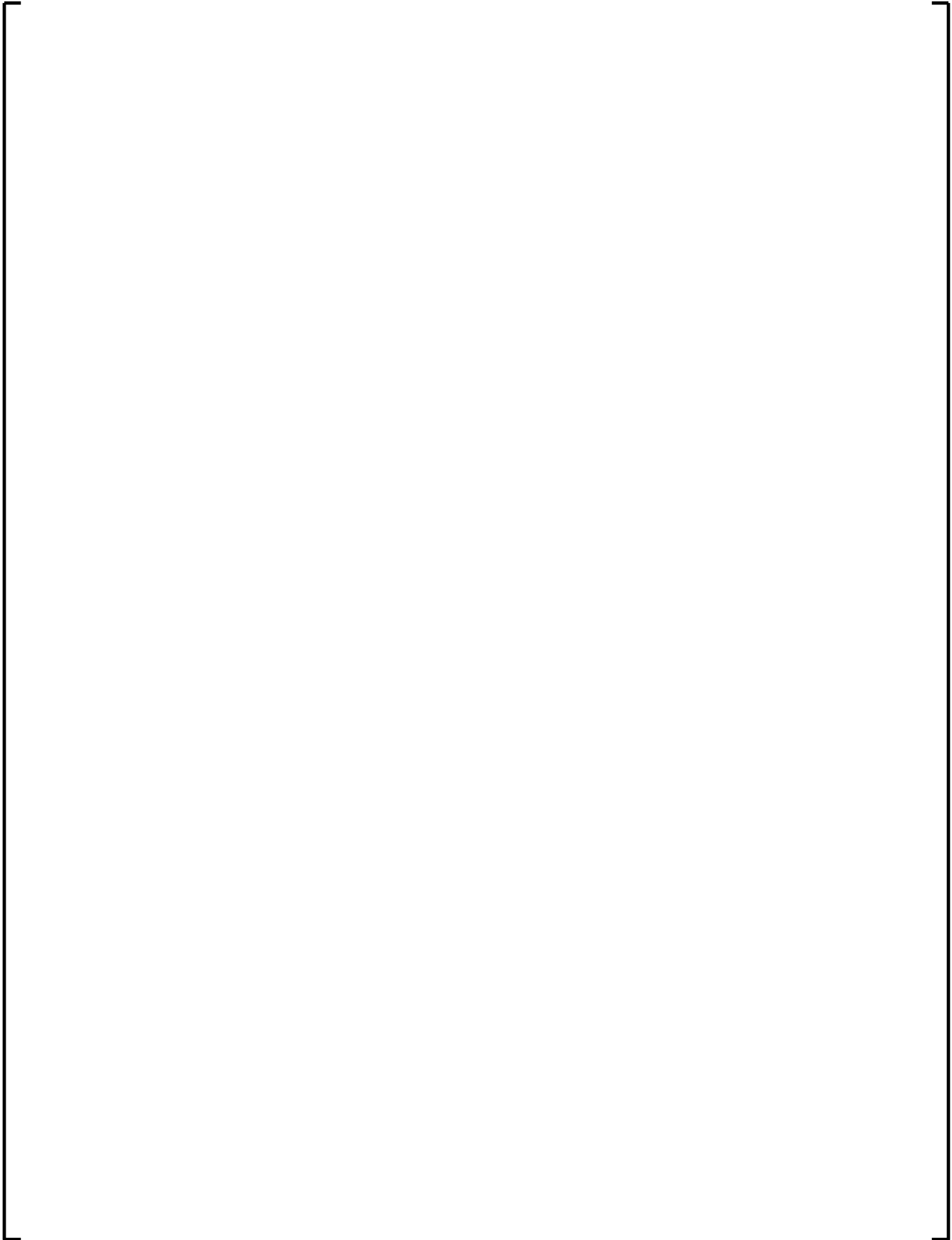
Permutations of the control room selection signal CRSEL and the OPDIS (disable commands via Profibus DP) are not checked in this set of test cases:

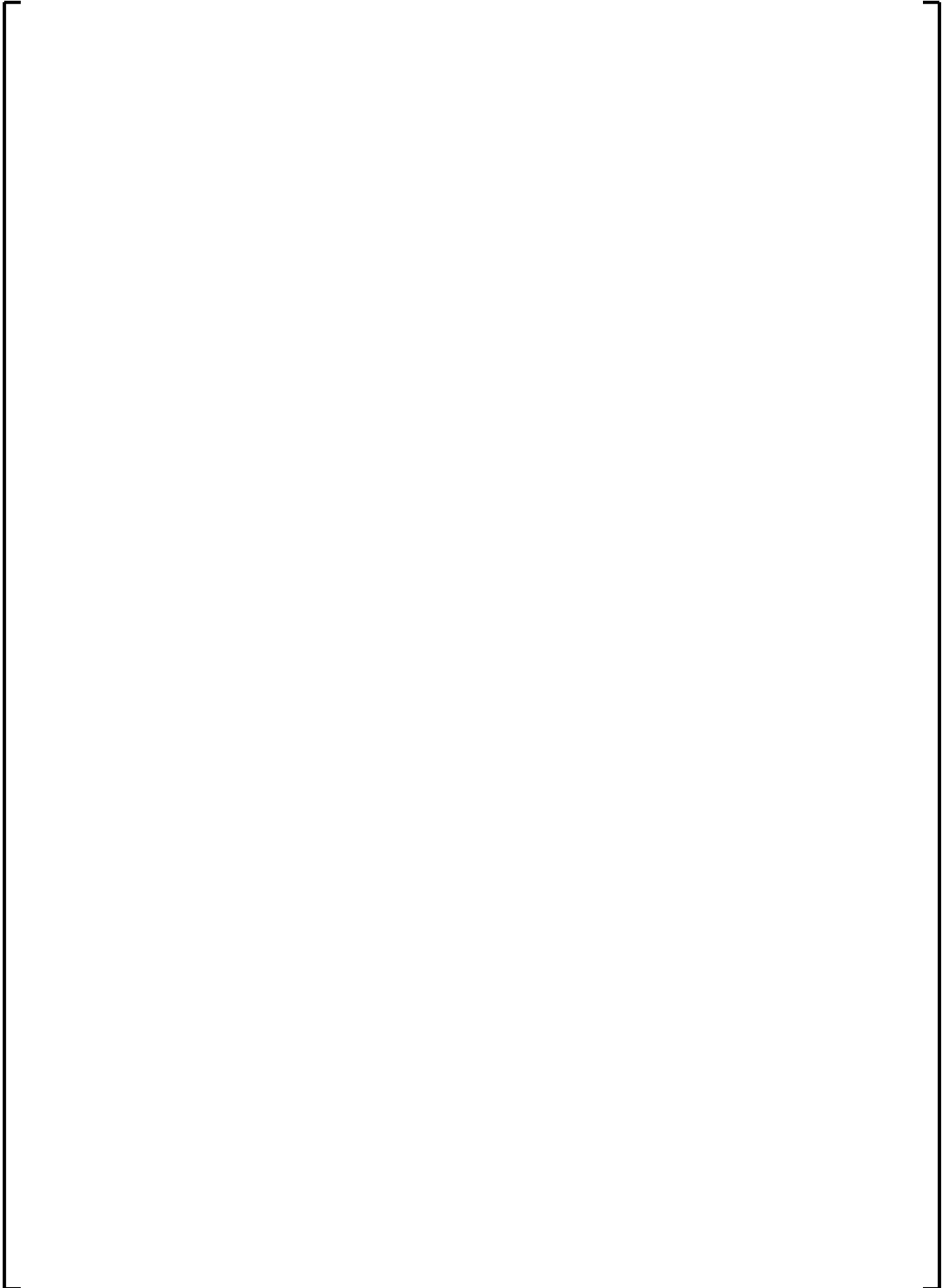
- 1) for this situation, a separate group of test cases (test cases 11.x) is performed
- 2) the design is done in such a way that the CRSEL and OPDIS signal have no interaction with the safety I&C signals.











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.)

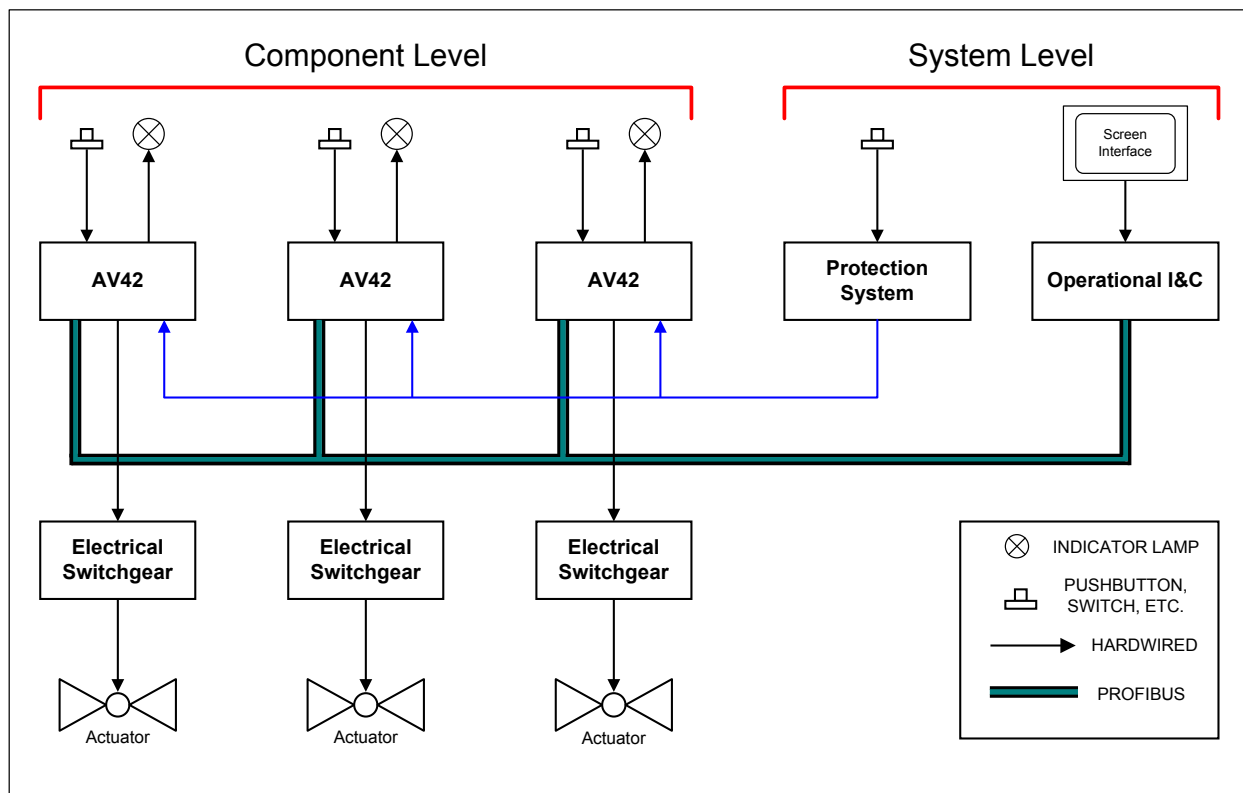


Figure 30-1
U. S. EPR functional representation of Manual System and Component level actuation.

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.

There have been two non-conformances concerning the AV42:

1. NCR 2006 004 refers to module versions 6FK5249-8AA and 6FK529-8BA.

These module versions showed a weak point in the hardware design: the bidirectional module pins were not properly designed and could supply the module with power when the module was not powered. This has been corrected, leading to a new module version.

2. NCR 2006 023 refers to module versions AV42 6FK5249-8AA, -8BA and -8CA.

An error in the programming of the PLD led to 1 sec. spurious command at the end of the overlapping test performed by the safety I&C. The programming of the PLD has been modified accordingly (leading to a new version of the module), and passed supplementary qualification procedure including independent assessment from TÜV Rheinland. Additionally, the behavior of the undervoltage signal processing during diagnosis mode was not addressed previously and has now been specified.

Customers are promptly informed about such issues and components already installed in the field are upgraded to correct known issues. Due to the 100% testability of the AV42, any non-conformances associated with the PLD programming that are a result of implementation errors will be identified during testing, investigated and corrected prior to release for field use. This process complies with the regulatory requirements for the manufacture, testing and corrective actions associated with any safety component intended for use in a nuclear plant.

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:

Information from the Profibus Controller (non-safety) to the PLD (safety) is passed as simple binary signals (see RAI 04 response). Information from the PLD to the Profibus Controller is transferred using a multiplexer (see RAI 05 response). No message passing via a serial communication scheme or other type of messaging scheme via a network takes place. The priority management within the PLD ensures that safety I&C commands will not be blocked by any faulty or erroneous signal transferred from the Profibus Controller to the PLD.

Normal control message integrity has no effect on safety function priority control, if a safety signal is present all normal control information is blocked.

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

Response 34:

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:

When a field component does not respond within a given time to a command, the non-safety portion of the AV42 creates a “run time fault/blocking” alarm (signaled on the desktille and sent to the Operational I&C via Profibus DP).

- (1) Safety I&C commands are not memorized in the AV42 module. Command memorization is managed in the safety I&C system / reactor protection system.

- (2) Normal control automation commands, component protection commands via Profibus DP are not memorized in the AV42 module (command memorization is managed in the non-safety I&C system).
- (3) Manual commands from the non-safety I&C (via Profibus DP) are not memorized in the AV42 but have to be sent cyclically until the command is terminated (e.g. by a checkback) in the non-safety I&C.
- (4) Manual commands from the desktils (hardwired manual inputs) can be memorized in the AV42. If memorized, the command memory is reset by:
 - desktil command in the counter-direction (any type of command)
 - stop-command (as far as applicable)
 - switch-over to other control room
 - safety I&C commands or cancellation of "enable operational I&C / desktils" SFEN
 - simulation inputs
 - non-safety I&C commands via Profibus DP in the counter direction []

When a safety signal is sent to the AV42, reset of the normal automatic control commands (sent to the AV42 from the Operational I&C system via Profibus DP) must be engineered into the non-safety Operational I&C system. This will ensure that upon safety signal reset (sense and command reset) no normal control commands are present at the AV42 and the execute features do not return to normal.

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.

For normal operational control, the use of these two parameters prevents incorrect parameters being used for operational tasks after inserting a new module or inserting an operational control parameterized module in a different slot.

The safety function parameterization for any AV42 module PLD is determined by the backplane wiring for the type of device being controlled.

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 US 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:

Profibus DP is not an internet compliant network. The AV42 is intended to be connected to Profibus DP segments of limited size according to the configuration listed in RAI 24 and RAI 25 responses. No components other than AV42 modules are to be used on these segments. Every message that is sent to an AV42 contains a Profibus DP message address that contains a Functional Complex Number (FUNR) and Instance Number (INSTNR) that is unique to that module. The AV42 module verifies the two numbers stored in memory on the Controller match the two numbers in the message. The PLD plays no active role in this message exchange. More information is contained in the response to RAI 34.

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.

Projects use, as a basic documentation, the AV42 product documentation including:

- AV42 data sheet
- AV42 installation guideline
- AV42 user manual (AV31 mode; AV42 mode for control modes 1, 2, 3 and 6).

Based on this, the project specifies the various types of standard configurations according to the field devices' characteristics as applicable to the project (typical document title "Concept of actuator control and variants"). This is then included in project procedures to be observed in the basic and detail design phases of a project.

User manual, conceptual design documents and engineering procedures are provided to the final customer for long term maintenance of the safety I&C system.

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:

The AV42 is a slave in the network and only sends cyclic status messages to the Operational I&C system. Failure of the cyclic status message has no effect on the safety functionality of the AV42.

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

Response 45:

The DAS will have priority over soft control commands for MOVs by interfacing the DAS with the hardwired inputs on the AV42. Since the DAS commands will be received by the PLD from the higher priority inputs [], the internal logic of the PLD will ensure that these commands have priority over soft control commands that are issued via Profibus DP.

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:

Part 1

The PLD does not contain any internal volatile memory. The AV42 does contain hardwired inputs to the PLD that allow for parameterization of the PLD depending on the type of actuator with which it is associated (i.e., solenoid, MOV, motor, etc.) Examples of such parameter pins and their functions are given below. This parameterization is accomplished via backplane wiring of the AV42 card slot for the specific type of device to be controlled.

Prevention of malicious reconfiguration of the AV42 is controlled by several means. First, the cabinets that house the AV42s are located in the US EPR safeguards buildings under locked access. Plant maintenance personnel must obtain a key from the Operators before entering the safeguards buildings. The AV42 cabinets are also locked and also contain door alarms.

The AV42 can be disconnected from the backplane by removal from the card rack during normal operation. However, per IEEE 603-1998, bypassed and inoperable status is available to the Operators in the control room. Also, the protective function associated with the bypassed PAC module is maintained at the system level via redundancy in the other divisions of the PACS and redundant components.

Part 2

Two steps are required to configure the AV42; however, they are independent of each other. The hardwired parameter inputs to the PLD are predetermined depending on the type of actuator with which it is associated (as explained in Part 1 above). These parameters are input to the PLD via backplane wiring to perform correct command termination and indicate which type of limit and/or torque switches are used for a specified actuator.

The PLD does not take into consideration any of the Controller parameters when performing its safety function.

The parameterization for the Profibus Controller for non-safety control is performed via a parameter word sent from the Operational I&C system. This parameter word provides parameters to the firmware within the Profibus Controller to perform Operational I&C functions.

The parameters are stored in the Operational I&C engineering system database and sent to the AV42 via the Operational I&C automation processor. Such parameters include open or closed-loop controlled actuator type, type of limit switch checkback contact, type of torque switch checkback contact, etc.

The Controller considers both the parameters received via the hardwired 64-pin connector and parameters received via the Profibus DP parameter word when performing its Operational processing.

Two such parameters that protect against incorrect parameterization for normal control and inserting incorrect modules is the functional complex number [] and the instance number []. Both parameters are transmitted in the cyclic control message (message sent from Operational I&C to AV42 for initiating Operational commands). If the numbers associated with [] in the control word deviate from what is set in the parameterization field within the Controller, no Operational commands are issued and the AV42 signals a fault. This function prevents incorrect parameters being used for operational functions after inserting a new module or after inserting a parameterized module in a different slot.

There is no safety impact of performing one parameterization and not the other. The PLD parameterization and Profibus Controller parameterization are independent of each other. The PLD safety parameters are hardwired in the cabinet and administrative controls prevent unauthorized access. Also, if operational parameters cause the AV42 normal control to function improperly, only the non-safety piece is affected and safety function and priority logic integrity is preserved in the PLD.

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:

- 1.) The PLD used in the AV42 consists of a set of macro-cells and interconnect wiring.
- 2.) The macro-cells are composed of logic arrays, product-term select matrix and registers (flip-flops).
- 3.) The programming is implemented by defining the interconnect wiring in accordance with the chosen functionality, which is then stored in EEPROM cells in a non-volatile way.

- 4.) The programming pattern is loaded into the PLD using the JTAG interface supporting serial loading.
- 5.) Any time-related functions (i.e., needed for creating a time-limited release for a test signal, or for delaying torque signals) are implemented using shift-registers. These registers are triggered by a clock signal from a multi-vibrator external to the PLD itself.

Features typical for the FPGAs that are not used in the AV42 PLD are:

- The PLD does not include any RAM.
- The PLD does not include a watchdog circuit; monitoring of the PLD is done through engineered means. In the AV42, an external watchdog circuit observes an oscillating output signal. See the response to RAI 08 for more information on the watchdog timers associated with the AV42.
- The PLD does not include a processor performing execution of programmed instructions or a digital signal processor or PLL circuitry, as found in FPGAs.

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:

- 1) signals are run through a Schmidt-trigger circuit before entering the PLD. This provides clean signal edges.
- 2) after entering the PLD, signals are fed into a D-flipflop, which ensures that signal edges are acknowledged only together with the clock signal.

3) a digital filter in the PLD is used for debouncing. This filter algorithm ensures that only signal changes having become stable for a minimum period of time are taken into account.

See Figure 50-1 for an illustration of items 1 – 3 above.

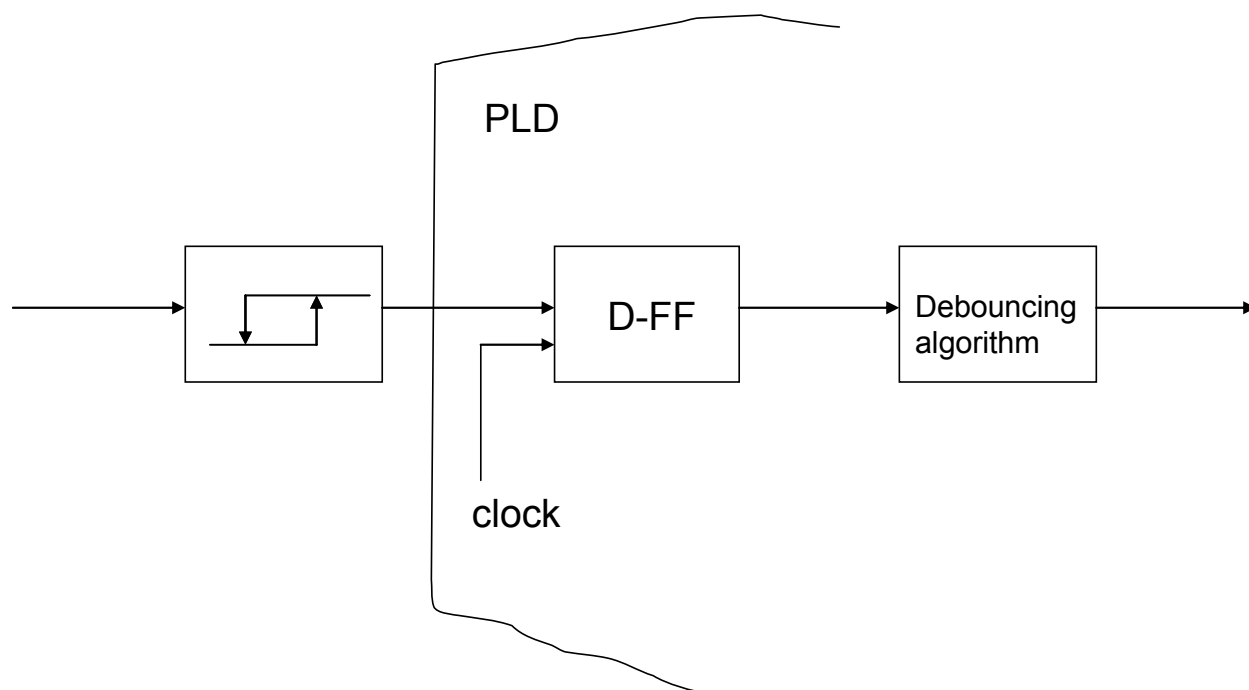


Figure 50-1: AV42 Signal conditioning

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).

Handling of modifications due to findings during qualification testing

Errors and faults detected during the equipment qualification program have been analyzed, and appropriate corrections have been implemented.

Corrections identified as necessary during qualification testing are included in the manufacturing documents of AV42. The qualification results are then only applicable to modules manufactured according to the upgraded version of the manufacturing documents. Only qualified versions are in field service.

Identification of Module Versions & Types by Version Identification and Ordering Number

Type testing reports clearly identify the module version having finally passed the test program, and the associated version of the manufacturing documentation.

Only this finally qualified version is released to be used in plants. This is controlled by the configuration management for TELEPERM XS hardware modules.

Every modification having an impact to performance or functionality leads to an increase of the module version number (minor modifications) or even order number (major modifications).

Every module type is identified by a "MLFB" number (machine readable product identification), and a "module version number" ES so as to be able to relate a given module to a set of manufacturing documents.

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.

In terms of hardware qualification, there are no differences between the safety and non-safety portion of the AV42.

Effects from the Profibus Controller on the PLD (i.e., by increased power dissipation or ESD effects) have not been considered or observed:

- during operation, the Controller on the AV42 is in cyclic operation, basically providing cyclically status messages to the operational I&C, and cyclically receiving command messages. Event-based processing (generation of event-triggered status messages on signal changes and faults) is included in the cyclically executed program of the Controller. Considering the functionality implemented in the Controller, there is no potential for significant changes of the load and hence thermal effects which might affect the PLD.
- the complete AV42 module passed the tests related to ambient conditions, including EMC. Any effects due to internal EMC effects (i.e., emissions of the Controller affecting the PLD) would have become evident in the test program as faults or spurious signals.

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:

When a GO test is initiated, the actuator is exercised by the Protection System. Both close and open commands are tested. If the Operational I&C system is sending a command in the opposite direction than that of the safety I&C system (the Operational I&C is commanding the AV42 to issue an open command and the safety I&C system is commanding the AV42 to issue a close command), the actuator will exercise in the direction that the safety I&C system is commanding (in this case close), and the prioritization logic within the PLD is confirmed. GO tests are initiated in accordance with IEEE 338-1987.

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.

The AV42 is a non-computerized based device and is not subject to software-related common cause failure. Therefore, item 1 as listed above, is not a concern for the PACS and AV42 modules. For item 2 above, the fact of the AV42 module arbitrating various inputs does not lead to a single point of failure concern. The use of the AV42 within the I&C architecture (one AV42 per one actuator) is a point of single failure for the component only. The single failure criteria for protective functions is upheld by the I&C architecture containing redundant, independent divisions that perform the same protective functions. That is, just as one valve could fail to close due to a mechanical failure, the AV42 could potentially fail to send an output command to close a valve. This failure scenario is a single, random component failure and sufficient redundancy within the I&C architecture ensures completion of the protective action at the system level.

Item 3, as stated above, is not plausible for the AV42. CCFs that could potentially prevent a protective action from being performed are analyzed within the I&C architecture and necessary diversity is implemented at the system level to avoid prevention of protective actions.

The information in section 4.11 of the AV42 Topical Report that states the AV42 is a final actuation device and is outside the scope of the diversity requirements of 10 CFR 50.62 is

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 US 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:

The calculation of the MTBF values is performed based on the part-count method, using the Siemens Standard SN 29500 series. These standards provide a data base of failure rates for all relevant types of electronic components.

These SN29500 standards are periodically updated, taking into account information and feedback from current electronic components. This is the "database of information for similar types of components" referred to in the topical report.

In addition to the calculation of the module failure rate, the feedback of experience is observed by recording the operating time, and recording all failures communicated by the customers.

Onsite repair of TELEPERM XS modules is not permitted; therefore, all customers send faulty modules for repair to AREVA, and this ensures consistency with AREVA's records of module faults during operation.

Data is regularly compiled (every three months) and published by AREVA NP internally.

The feedback of experience for the AV42 from plant operation refers to AV42 modules installed in plant I&C systems in commercial operation.

Today, there are 1318 modules in operation, with 0 failures recorded since start of commercial operation as follows:

Atucha 1: 38 Modules (since 3-2003)
Tianwan unit 1: 627 modules (since 8-2005)
Tianwan unit 2: 627 modules (since 8-2007)
Biblis B: 33 modules (since 12-2005)
Emsland: 10 modules (since 6-2005)

The product versions 6FK524-9AA from ES03 to ES07 are identical in hardware design. All modules listed above fall within this hardware design.

A redesign has recently been performed to incorporate the current version of the PLD, and to incorporate new functional requirements.

Equipment qualification of this module version 6FK524-9CA ES04 has been completed; however, modules of this version are not yet in commercial operation.

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.