
**Response to Second Request for Additional Information – ANP-10281P
“U.S. EPR Digital Protection System” (TAC No. MD4977)**

RAI 15: Describe the conventions for documenting requirements in the protection system topical report (PS TR).

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

Regulatory Guide (RG) 1.172 endorses IEEE Std 830-1993 as providing an approach acceptable to the staff, subject to certain exceptions listed. IEEE Std 830-1993 implies that requirements are identified by the use of the word "shall", by using "shall" in all of its requirements examples. However, the RG, in Section C.2, implies that "must" is also an acceptable convention for identifying requirements. Therefore, in order to clarify if one or both of these conventions are being followed, AREVA should identify the conventions that AREVA follows to identify requirements.

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

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

Response 15:

The only place the term "shall" is used in the PS TR is in Appendix B where IEEE 603 is quoted. Furthermore, as noted in the AREVA NP response to NRC RAI 9 for ANP-10272, "Software Program Manual TELEPERM XSTM Safety Systems Topical Report" (Reference 1), the Software Program Manual is AREVA NP's upper tier requirements document for TXS application software development. The statements in the Software Program Manual are considered to be the programmatic requirements necessary to implement the TXS application software program. No specific convention was used to

denote requirements. Instead, optional or conditional items are described using the terminology 'may'.

RAI 16: *Please clarify the processing of manual commands by the PS.*

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

IEEE Std 603-1991 Section 6.2.1 says: "Means shall be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions. The means provided shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment consistent with the constraints of 5.6.1." The requirements contained in IEEE Std 603-1991 Section 5.6.1 are for independence between redundant portions of a safety system: "Redundant portions of a safety system provided for a safety function shall be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring, that safety function."

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

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

Response 16:

While Clause 6.2.a of IEEE 603-1998 refers to manual actuation of protective actions at the "division level," it is more accurate to use "system level" in the context of the U.S. EPR design. In many cases, providing division level actuation would not accomplish a protective action as more than one division is required. For example, at least two divisions of the PS must issue a command to close a single Main Steam Relief Train Isolation Valve (MSRTIV). The automatic protective function issues the command from all 4 PS divisions, and a 2 out of 4 solenoid valve configuration is used to close the MSRTIV. In this case, the "system level" manual initiation would use all 4 divisions of the PS to issue commands to the 4 solenoids associated with a single MSRTIV.

AREVA NP refers to the type of functionality required to meet the requirement of Clause 6.2.a of IEEE 603-1998 as “system level manual initiation.”

Section 3.1 of the PS TR states: “In addition to automatic functions, the PS can also process manual commands and issue corresponding actuation orders.” This is a statement of both capability and permission. The computerized portions of the EPR protection system (PS) process the majority of the system level manual initiations of ESF actuation functions. This functionality is implemented in the PS design consistent with the requirements contained in Clauses 5.6.1 and 6.2 of IEEE 603-1998.

No clause in either IEEE 279-1971 or IEEE 603-1998, or position statement in RG 1.62 requires independence between automatic protective functions and manual system level actuation. Independence is however required between redundant portions of a safety system by both IEEE 603 and IEEE 279 (clauses 5.6.1 and 4.6 respectively).

Clause 6.2.a of IEEE 603-1998 states: “Means shall be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions. The means provided shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment consistent with the constraints of 5.6.1.”

This excerpt from IEEE 603-1998 requires that, in the effort to minimize the number of operator actions and minimize the equipment used, the independence between redundant portions of the safety system shall not be compromised. This passage does not require that the manual initiation be independent from, or redundant to, the automatic functions of the safety system; instead, the implementation of manual capability cannot degrade or compromise the independence between divisions of the PS.

In the U.S. EPR design, the safety-related system level manual actions are not redundant to the automatic reactor trip (RT) or engineered safety feature (ESF) actuation functions. Credible single failures within the PS are mitigated by redundancy designed into the automatic functions of the PS. Software common-cause failures of the PS are mitigated by diverse automatic and manual functionality implemented in non-safety related I&C to satisfy regulatory positions concerning defense-in-depth and diversity. Safety related system level manual initiations are not credited to mitigate any type of PS failure.

Therefore, in the context of the U.S. EPR design, the use of common equipment to perform both the automatic and manual system level initiation functionality is acceptable because:

- The manual system level actuation is not relied upon to mitigate a failure of the automatic function.

- The implementation of the manual controls maintains the independence required between the redundant portions of the safety system (i.e., between the redundant divisions of the PS).
- No single failure can prevent either the manual or automatic initiation function.

RG 1.62 “Manual Initiation of Protective Actions” was issued by the U.S. Atomic Energy Commission (AEC) in 1973 to describe “a method acceptable to the AEC Regulatory staff for complying with the requirements of Section 4.17 of IEEE Std 279-1971.” Pursuant to 10 CFR 50.55a(h), IEEE Std 279-1971 is not applicable to the U.S. EPR design. Additionally, the requirement in Clause 4.17 of IEEE 279 is significantly dissimilar from that of Clause 6.2 of IEEE 603. For example:

- Clause 4.17 of IEEE 279 explicitly refers to “the automatic, manual, or common portions of the protection system,” while Clause 6.2 of IEEE 603 makes no mention of “common portions.”
- The IEEE 603 clause explicitly refers to clause 5.6.1 for independence between redundant portions of the safety system, while the IEEE 279 clause makes no mention of, or reference to, independence.

It is therefore not appropriate to use RG 1.62 as an interpretation of requirements in IEEE 603, because it was written specifically to address Clause 4.17 of IEEE 279. Additionally, RG 1.62 was issued in an era when digital safety systems were not yet conceived for use in nuclear power plants. Therefore, software common cause failures, and the additional design features required to mitigate them, were not considered in the AEC regulatory position of 1973. It is AREVA NP’s position that the RG 1.62 position 4 statement: “The amount of equipment common to both manual and automatic initiation should be kept to a minimum,” was intended to incorporate some degree of redundancy between the manual and automatic initiation functions. At the time, manual actuation of the safety functions at the system level was the primary means of coping with a protection system failure.

In the modern regulatory environment, the onus is on the designer to show that in the unlikely event of a software common cause failure that completely disables the safety related protection system, diverse means are available and adequate to maintain the plant in a safe state. If the means credited to mitigate a software common cause failure, or any other type of protection system failure, do not include the safety grade system level initiations, then incorporation of the above mentioned position 4 statement does not increase plant safety. In fact, several system level manual initiation functions included in the U.S. EPR design, if implemented in strict adherence to position 4 would unnecessarily increase the number of required operator actions, and introduce unnecessary complications in the safety system design.

However, in absence of a more modern regulatory interpretation regarding IEEE 603 system level manual initiation requirements, RG 1.62 was taken into consideration, and was applied in cases where it was prudent, given the overall plant design and the underlying basis for each particular manual initiation function. A description of the implementation of manual system level initiation functionality is given in the response to RAI 18.

RAI 17: *Please describe the design features in the manual Engineered Safety Features (ESF) actuations ensure the completion of the protective action.*

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

IEEE 603-1991 says: "7.3 Completion of Protective Action. The design of the execute features shall be such that once initiated, the protective actions of the execute features shall go to completion. ... When the sense and command features reset, the execute features shall not automatically return to normal; they shall require separate, deliberate operator action to be returned to normal. After the initial protective action has gone to completion, the execute features may require manual control or automatic control (that is, cycling) of specific equipment to maintain completion of the safety function."

Response 17:

When RT sense and command outputs are initiated, the RT breakers open to remove power from the control rod drive mechanisms, allowing the rods to fall by the force of gravity. For automatic RT, the sense and command outputs are automatically cleared (reset) when the initiating condition has returned within the RT setpoint plus some amount of hysteresis. For manually initiated RT, the sense and command outputs are reset manually. In both cases, the reset of the RT sense and command output does not result in closure of the main RT breakers. The breakers must be physically reset to be closed.

When an automatic ESF actuation function is initiated by the PS, the intended actions of the execute features proceed to completion. The return to normal state of ESF actuators requires deliberate operator intervention. In most cases, operator action is required to reset the sense and command output signal, and further operator action is required to change the state of the actuated device. For exceptional cases where operator action is not required to reset the actuation signal, operator action is required to change the state of the actuators after the reset of the actuation signal.

In all cases, measures are taken to provide for completion of the intended actions of the execute features before the sense and command actuation signal is allowed to be reset.

The following features provide for completion of the intended actions of the ESF execute features:

- Set-Reset latching logic, implemented in the Actuation Logic Units (ALUs), on sense and command output signals.
- Pulse-OR logic, implemented in the ALUs, on sense and command output signals.
- Seal-in of certain signals in the switchgear.
- Seal-in functionality in the Priority Actuation Control System (PACS) modules for manual inputs.

The nature of the final actuated device, and in certain cases the actuation path through the sense and command features, dictates which of the above features are used to assure completion of the intended actions of the execute features.

Motor Operated Valves:

Many of the final actuated devices that receive ESF actuation orders from the PS are motor operated valves (MOVs). The nature of MOVs dictates that after full closure or opening, a control order is required to begin travel in the other direction. When the initial control order that closes a MOV is removed, the MOV will not open until a separate specific control order is given to open the valve. In the majority of these cases, set-reset (SR) latching logic is used in the ALU to “memorize” the actuation order. When the initiating condition clears (i.e., process parameter returns within the actuation setpoint), the output of the SR logic maintains the actuation order to the PAC module associated with the MOV. An order from the operator is required to reset the SR logic and remove the actuation order from the PAC module. Once the operator has reset the SR logic, further action is then required to move the MOV to a position other than its completed protective action position.

Another provision for completion of protective actions using MOVs is the use of “pulse-OR” logic. The pulse-OR refers to a logical arrangement where an actuation order starts a pulse output with the duration of the pulse at least as long as the stroke time of the MOV. The output of the pulse is then combined with the actuation order itself in an OR logic. The pulse guarantees that the stroke of the MOV is completed, even if the actuation order clears before the valve stroke time is complete. The OR logic guarantees that as long as the actuation order is present (i.e., process variable is above the actuation setpoint) after the pulse has ended, the state of the MOV cannot be changed. This arrangement is used in exceptional cases to prevent the reset of a sense and command output until the process variable has returned within acceptable limits. Once the process variable is within acceptable limits, the actuation output is removed from the associated PAC modules automatically, and the operator is allowed to take further action to re-position the MOVs.

Pumps:

When a pump is started as part of an ESF actuation function, appropriate valves are also opened or closed for purposes such as configuring a proper flow path. For actuations that both start pumps and manipulate valves, the SR logic described above is used in the ALU to memorize the actuation order. This means that the actuation signal must be manually reset before the pump can be stopped or the associated valves can be repositioned. However, the need to reposition a valve after actuation does not necessarily coincide with the need to stop the pump. For this reason seal-in features are used in the switchgear for pumps actuated by the PS as part of an ESF function. This allows the operator to reset the actuation order, reposition valves as needed, and not inadvertently influence the pump operation. A specific operator action is then required to stop the pump.

Solenoid Operated Valves:

Certain ESF actuation functions utilize solenoid operated valves (SOVs) to move the main process valve. In many cases, the main process valve has a normal open or closed position; if the required number of SOVs are not energized, the process valve will default to its normal position. This requires that an actuation signal be maintained on the SOVs for as long as the process valve is required to maintain its abnormal position (e.g., its completed protective action position). If a sufficient number of signals are removed from the solenoid operators, the process valve will automatically return to its normal position. Therefore, in cases where the actuation function includes devices where removal of the PS actuation order from the associated PACS module would result in the actuator changing state (e.g., SOVs), seal-in features are incorporated in the switchgear. These seal-in features allow the reset of the actuation signal to the PACS modules while requiring additional operator action to affect the state of the actuated device.

Manual System Level Initiations Processed by the Computers of the Protection System:

The manual system level ESF actuations processed by Acquisition and Processing Units (APUs) and/or ALUs are described in the response to RAI 18. These manual functions are combined with the automatic logic in the ALUs such that completion of protective action is achieved using the same method as the corresponding automatic protective action.

Manual System Level Initiations that Bypass the Computers of the Protection System:

Certain manual system level initiations of ESF actuators bypass the computerized portions of the PS and are wired directly to the manual inputs of the PACs modules. These initiations are described in the response to RAI 18. To provide for completion of

protective action, this type of manual function utilizes the seal-in functionality available in the safety-related portion of the PACS module. This seal-in functionality is specifically designed for the manual inputs to the PACS module. Once the manual command has been received by the PACS module, the output of the PACS module is maintained even after the manual initiation command is cleared. This output is maintained until a different order of higher priority is received by the PACS module.

RAI 18: *Please describe when the implementation of each manual system level actuation of ESF functions will be determined.*

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

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

Response 18:

Section 8.5 of the PS TR describes manual initiation of ESF actuation functions at the system level. Three typical implementations were described and illustrated in subsequent figures. In many cases, the implementation of these system level actuations through a diverse safety-related "hardwired" path required a significant amount of PS logic to be recreated in the "hardwired" path. This added complexity to the overall safety system design, but provided a diverse path for system level initiation that could be used to satisfy position 4 of BTP 7-19.

The description of each typical implementation clarified the intent to credit these methods in a Defense in Depth and Diversity (D3) analysis. Since submittal of the PS TR, regulatory developments in the area of D3 (e.g., interim staff guidance, statements made by the staff in the transcript for the September 13, 2007 ACRS Digital I&C System Subcommittee meeting) have indicated that component level controls implemented through a diverse, non-safety related system are adequate to satisfy BTP 7-19 position 4.

These developments have allowed AREVA NP to increase the reliability of the system level manual initiations, while decreasing the complexity of the safety system as a whole, by utilizing the existing computerized portions of the PS for many of the manual

system level ESF actuation functions. This approach retains the ability of the operator to actuate ESF functions at the system level in a single failure tolerant capacity, and meets the specific requirements delineated by Clause 6.2.a of IEEE 603-1998.

The design for manual initiation of RT remains unchanged from that described in Section 7.6 of the TR.

Clause 6.2.a of IEEE 603-1998 states: "Means shall be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions. The means provided shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment consistent with the constraints of 5.6.1."

The second sentence of Clause 6.2.a requires that the number of operator manipulations and the amount of equipment used shall both be minimized. These goals contradict each other in several cases in the U.S. EPR plant design. But any solution, using any weighted combination of the two "minimums," is subject to the overriding requirement that independence be maintained between redundant portions of the safety system. This is the extent of the IEEE 603 requirement imposed on manual system (or divisional) level control of the automatically initiated protective actions.

Appendix 7.1-C, Section 6.2 of NUREG-0800 states: "Features for manual initiation of protective action should conform with RG 1.62..." AREVA NP's position that it is not appropriate to use RG 1.62 as an interpretation of requirements in IEEE 603 is described in the response to RAI 16. However, since the RG has been recently endorsed in the Standard Review Plan Chapter 7, and in absence of a RG specifically addressing the IEEE 603 requirement, the regulatory positions of RG 1.62 were considered in the design.

Taking into account the regulatory requirements, regulatory guidance and U.S. EPR plant functional requirements, the following design criteria were used to determine the implementation of system level manual initiation functions on a per-function basis (listed in order of decreasing priority):

1. Independence shall be maintained between redundant portions of the safety system.
2. The manual initiation function, from manual control mechanism to combination with the automatic function, shall be single failure tolerant.
3. No single failure related to the manual initiation function shall cause a spurious actuation that could jeopardize plant safety.
4. The number of discrete operator manipulations shall be minimized.
5. The amount of equipment used shall be minimized to increase reliability.

6. The manual initiation function should perform the same actions as the automatic protective function.
7. The amount of equipment common to the corresponding manual and automatic initiation functions should be minimized.

These criteria were applied to each protective function in the design, and three new typical implementations resulted that are consistent with regulatory requirements and satisfy the functionality required by the U.S. EPR process systems. The implementation of each function is described in Section 7.3 of the U.S. EPR design certification application. AREVA NP proposes to replace the current section 8.5 of the PS TR with the following:

“8.5 System Level Manual ESF Actuations

In addition to the automatic ESF actuation functions performed by the PS, the capability to manually initiate these functions at the system level is provided in the Main Control Room. While the U.S. EPR design includes the ability to manually manipulate these actuators at the individual component level from the non-safety related PICS (the component level manipulations are not processed through the PS), the system level actuations discussed in this section are implemented completely through Class 1E actuation paths and are single failure tolerant.

The manual ESF actuation functions are either processed by the PS equipment that performs the automatic function, or are implemented to bypass the computerized portions of the system. While it is desirable from the standpoint of diversity to have the manual initiations bypass the computerized portions of the PS, in many cases such an implementation would significantly complicate the design of the safety system as a whole, and reduce system reliability. However, recent regulatory developments in the area of D3 have reduced the need for crediting diverse system level initiations which allowed increased focus to be placed on simplification of the safety system design to improve overall system reliability. System level manual initiations which are processed by APUs and/or ALUs of the PS are not credited in the EPR D3 analysis.

The manual ESF actuation functions that are processed by the PS are implemented in one of two ways. The signals from the manual controls are either acquired by the APUs and treated similarly to typical sensor inputs (i.e., partial triggers generated and voted on at the ALU level), or are acquired directly at the ALU level and combined with the automatic function logic. These are designated as typical implementations 1 and 2 respectively.

The manual ESF actuation functions that bypass the computerized portions of the PS utilize the PAC modules. The signals from the manual controls are acquired by the PAC modules which interface to the desired actuators. This type of implementation is used in situations where very few actuators are required for a function, and there are no sequencing requirements.

The three typical implementations are described below.

8.5.1 Typical Manual ESF Actuation 1:

Figure 8-3 illustrates the implementation of a manual system level initiation function which utilizes both the APUs and ALUs of the PS. Redundant manual initiation controls in the MCR are acquired by APUs in different divisions of the PS. Each APU sends the status of a manual control to the ALUs in all 4 divisions. Voting is then performed in all divisions on the status of the redundant manual controls. This implementation is particularly suited to functions for which spurious actuation is of significant concern. It allows the manual initiation function to satisfy the single failure criteria, while taking advantage of ALU voting logic to significantly limit the probability of spurious actuation. In this implementation, independence is maintained between the redundant divisions of the PS in exactly the same manner as in an automatic ESF actuation function.

8.5.2 Typical Manual ESF Actuation 2:

Figure 8-4 illustrates the implementation of a manual system level initiation function which bypasses the APUs and utilizes the ALUs within the PS. Redundant manual initiation controls are acquired by ALUs in different PS divisions. When redundancy for the function is achieved between PS divisions (i.e., redundant actuators are powered from different electrical divisions), only one manual control is required for each PS division. In cases where it is desirable to utilize redundancy within a PS division (i.e., all actuators that perform the function are powered from the same electrical division), two controls are acquired by the ALUs of a division and a one out of two voting is performed. The typical 2 implementation is well suited for functions where spurious actuation is not a concern, but many actuators or sequencing are required to perform the function. The logic of the ALUs is taken advantage of while the equipment common to the automatic and manual functions is minimized (manual function bypasses the APUs).

8.5.3 Typical Manual ESF Actuation 3:

Figure 8-5 illustrates the implementation of a manual ESF initiation function that bypasses the computerized portions of the PS. A single

manual control is provided per actuator and is acquired by the relevant PAC module. Redundancy is achieved through the arrangement of the actuators themselves. This implementation is used when few actuators are required and when spurious actuation is not of particular concern (Pressurizer Safety Relief Valve opening is a special case. It uses the typical 3 implementation even though spurious actuation is a concern. This is due to unique requirements on the functionality of the PSRVs. Additional measures are taken, such as covers on the manual controls, to prevent spurious actuation)."

As a result of the above changes to Section 8.5, revised Figures 8-3, 8-4, and 8-5 have also been provided in this attachment.

RAI Examples of Manual System Level Initiation

To assist the staff in evaluation of the typical implementations, two examples of specific manual initiation functions are provided to supplement this RAI response. These examples are simplified but accurately reflect the detailed logic in the U.S. EPR design certification application. The examples provided are manual safety injection system (SIS) actuation and manual emergency feedwater (EFW) system actuation.

Safety Injection Actuation:

The automatic SIS actuation in the U.S. EPR design consists of the simultaneous start of four redundant, 100 percent capacity trains; there is no automatic protective action that starts only individual trains of SIS. Depending on the current state of the plant (determined by permissive statuses) one of three initiation parameters is used for the automatic actuation (low pressurizer pressure, low ΔP_{sat} , or low RCS loop level). The automatic function is never placed under an operating bypassed condition; it is active in all plant modes. Therefore, to duplicate the automatic functionality, the manual system level initiation function starts all four SIS trains simultaneously and is available to the operator in all plant modes.

The automatic function contains a considerable amount of sequencing to minimize the impact on the electrical systems of several large motors starting simultaneously. A large number of actuators are mobilized as part of the actuation to align the correct flow paths and start the auxiliary supporting systems. For these reasons, the manual typical initiation 3 is not considered for use in this function.

When an automatic SIS actuation signal is generated, the partial cooldown ESF function is initiated, the reactor is tripped, and the containment is isolated; all as a direct result of the SIS signal within the PS. Because of this, it is desirable to prevent a single failure from causing a plant transient as a result of spurious manual initiation of the SIS function. Therefore, the manual typical implementation 1 is selected for use. Four manual controls are provided, any two of which will start all four trains of SIS along with

the associated actions. The implementation of manual system level initiation of the SIS is illustrated in RAI Figure 18-1.

EFWS Actuation:

The automatic EFWS actuation in the U.S. EPR design consists of the start of one EFW train to feed a specific steam generator. The EFW pump is started and associated control and isolation valves are opened by the division of the PS corresponding to the EFW train (i.e., PS division 1 starts EFW train 1). As part of the EFW initiation function, the same PS division also isolates the hot and cold steam generator (SG) blowdown lines on the affected SG. A different PS division isolates the common SG blowdown line that is redundant to the hot and cold blowdown lines together (i.e., PS division 3 isolates the common blowdown line on SG 1 when EFW train 1 is actuated). The automatic EFWS actuation is bypassed by the P13 permissive when temperature conditions are below the P13 threshold. Therefore, to duplicate the automatic functionality, the manual system level initiation function starts any one desired train of EFW, and is disabled by the P13 permissive.

Spurious actuation is not detrimental for this function, so manual typical initiation 1 is not considered for use. The automatic function does not require sequencing, but redundancy is desired within a given PS division as the pump, control valve and isolation valve are actuated from the same division. Therefore, manual typical implementation 2 is selected for use. Three manual controls are provided per EFWS train. Two of these are acquired by the ALU's in the division corresponding to the EFW train to be actuated; either of the two controls provides the actuation. The third control is acquired by the ALUs in the division that provides the redundant closure of the common SG blowdown isolation valve. The implementation of manual system level initiation of EFWS train 1 is illustrated in RAI Figure 18-2.

RAI 19: *Please explain what AREVA believes can be approved in the design rules.*

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

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

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

LIC-500 documents that the NRC, through it's website, provides guidance to applicants on the NRC's topical report program. Both the website and LIC-500 state that the report

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

Response 19:

Design Rules - Section 9.2

Section 9 of the PS TR discusses the permissive signals generated in the PS that are used as operating bypasses or as interlocks. Section 9.2 is titled "Design Rules for Implementation of Permissive Signals" and describes the guidelines used to determine the voting logic and automatic or manual validation of each permissive signal. In Section 1 of the PS TR, AREVA NP requested approval of the design rules presented in Section 9.2. However, based on the following discussion, AREVA NP has decided not to seek approval of the design rules for permissive signals.

Each permissive generated by the PS is described in Section 7.2 of the U.S. EPR design certification application. The inputs used, calculations performed, voting logic, and method of validation (automatic or manual) are defined for each permissive signal. Additionally, functional logic used in the generation of each permissive is illustrated in Section 7.2 of the design certification application. Therefore, the review and approval of the permissive signals for the U.S. EPR is more appropriately undertaken as part of the U.S. EPR design certification application review.

Therefore, on page 1-1 of the PS TR, AREVA NP will remove the bulleted item that indicates a request for approval of the design rules for permissive signals as shown below:

"This report describes the PS architecture and the typical implementation of functionality within this architecture. AREVA NP requests NRC approval of the following aspects of the PS design presented in this report:

- PS architecture
- Specific network configurations
- Typical RT concepts and sequences
- Typical ESFAS concepts and sequences
- ~~Design rules for permissive signals~~
- Inter-channel communication independence
- Safety to non-safety system interfaces
- Conformance with relevant clauses of Institute of Electrical and Electronics Engineers (IEEE) Standard (Std.) 603"

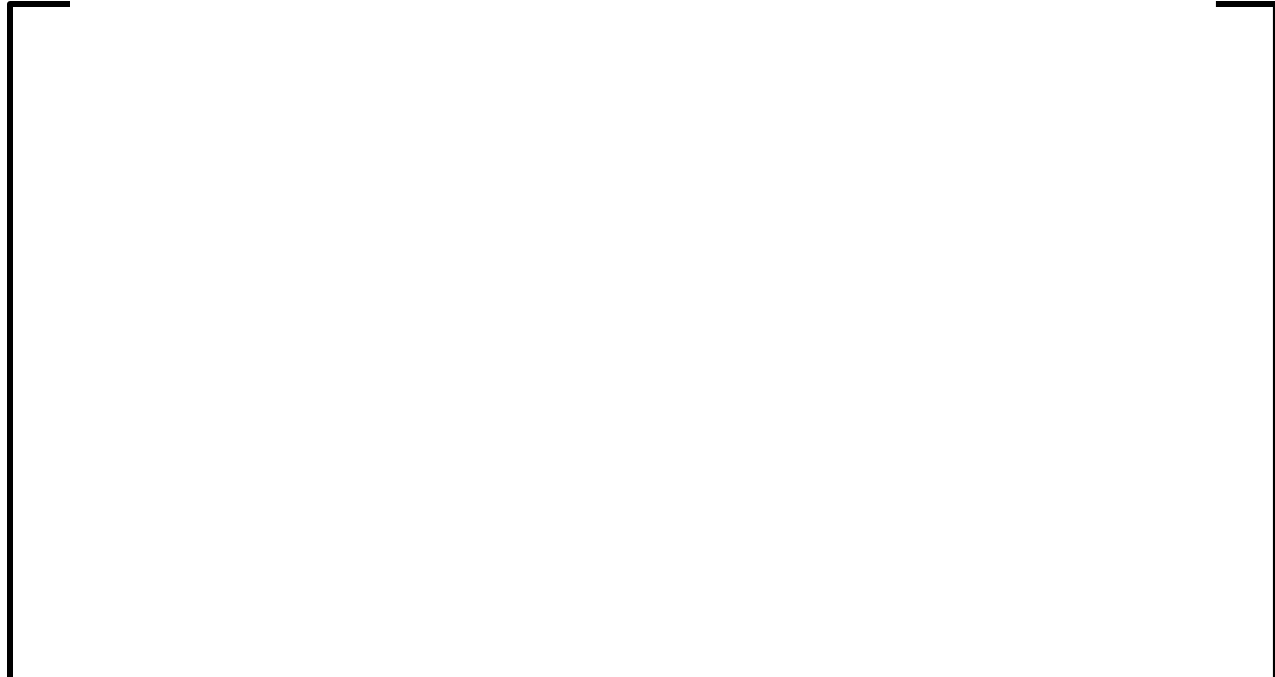
Section 9.1 and 9.2 will remain unchanged and included in the TR for informational purposes.

Design Rules – Section 10.2

Section 10 of the PS TR discusses the functional diversity used for RT functions between the subsystems in the PS. Section 10.2 is titled “Design Rules” and describes the guidelines used to establish independence between the subsystems, and criteria used to select the events to which functional diversity is applied. However, AREVA NP did not specifically request approval of the design rules regarding functional diversity; therefore nothing in the Section 10.2 design rules requires approval at this time. As noted in the cover letter transmitting the PS TR, AREVA NP asked for feedback from the NRC staff regarding the extent to which the functional diversity described in the TR could be credited in a defense-in-depth (D3) analysis.

The D3 analysis methodology for the U.S. EPR is described in AREVA NP TR ANP-10284 (Reference 2). As described in this methodology, AREVA NP is initially considering a software common cause failure that impairs the entire PS (both subsystems) as a bounding condition for a D3 analysis. This means that during the initial stages of the D3 analysis, no credit is being taken for functional diversity within the PS.

[] and AREVA NP remains interested in obtaining feedback from the NRC staff regarding how this type of functional diversity may be credited in a D3 analysis. AREVA NP will continue to assess how this type of functional diversity can be credited toward specific aspects of diversity, and may take advantage of this design feature as the D3 analysis progresses.



The remainder of Section 10.2 remains unchanged.

RAI 20: *Please describe communication independence guidance, in addition to that of IEEE Std 7-4.3.2-2003 Annex E, that was followed.*

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

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

Response 20:

The NRC statement of non-endorsement related to an informative annex of an IEEE Std. is understood by AREVA NP to be a policy position that is not the same as a conclusion that the information in the annex is technically wrong and cannot be used as guidance. AREVA NP did follow the endorsed guidance of RG 1.152 as described below. The endorsements within RG 1.152 led to the IEEE 7-4.3.2 communications independence annex as the only available source of guidance of the topic.

Section B of RG 1.152 Revision 2 does say that: “Annex E, Communications Independence, is not endorsed by the NRC.” Section B of RG 1.152 Revision 2 then states that guidance in the area of communications independence is provided in Appendix 7.0-A, Section 7.9, and Appendix 7.0-A of NUREG-0800. At the time that Revision 2 of RG 1.152 was issued, and at the time of submittal of the PS TR, Rev. 4 – June 1997 was the current version of all three referenced sections in chapter 7 of NUREG-0800.

Section C.3.5 of App. 7.0-A states that communications independence is a review topic that needs to be considered differently for digital systems. No specific guidance on achieving communications independence is provided. Sections 7.1-C and Section 7.9 are referenced as providing “Detailed regulatory bases, material to be reviewed, acceptance criteria, and review processes...” for communications independence. This is logical, given that these two sections were already referenced by RG 1.152, however App. 7.0-A provided no guidance on communications independence.

A search of Section 7.9 revealed no instances of the phrase “communications independence.” Independence is identified in 7.9 as one of the “major design considerations that should be emphasized in the review of DCS safety systems.” App. 7.1-C is then referenced for additional guidance. This is logical, given that RG 1.152 and App. 7.0-A both also refer to App. 7.1-C, however Section 7.9 provided no guidance on communications independence.

Section 11 of App. 7.1-C “Independence” stated that: “Annex G (communications independence annex) of IEEE 7-4.3.2...describes an acceptable means for providing communications independence.” No other reference is given for further guidance on the review of communications independence.

This means that between RG 1.152, SRP App. 7.1-C, SRP App. 7.0-A, and SRP Section 7.9, the only guidance on communications independence stated by the NRC staff to be “acceptable” was Annex G of IEEE 7-4.3.2-1993. However, RG 1.152 specifically endorses the 2003 version of IEEE 7-4.3.2.

A review of Annex G of IEEE 7-4.3.2-1993 against Annex E of IEEE 7-4.3.2-2003 (both titled Communication Independence) revealed that the two versions provided the same guidance relative to strategies for providing communications independence. Given that the only actual guidance endorsed by the NRC staff was in Annex G of the 1993 version, which was the same as the guidance in Annex E of the 2003 version, AREVA NP reached the only logical conclusion available; that Annex E of IEEE 7-4.3.2-2003 was “acceptable” guidance on communications independence (even though the same RG specifically did not endorse Annex E).

Therefore, the answer to the RAI question of “acceptable to who?” ... is... “Acceptable to the NRC staff”; given that the communications independence annex of IEEE 7-4.3.2, and no other guidance on communications independence, was endorsed by the staff.

Figure RAI 20-1 illustrates the path of regulatory guidance that AREVA NP used to reach this conclusion.

AREVA NP was aware of the staff’s concern that Annex E provided insufficient guidance. This concern was addressed in Sections 12 and 13 of the PS TR. AREVA NP used the general, but acceptable, concepts in Annex E as the foundation for providing communications independence. AREVA NP then provided a highly detailed description of how specific aspects of the TXS platform and U.S. EPR protection system design satisfy, and actually exceed, the concepts presented in Annex E. This was viewed by AREVA NP as an acceptable approach given the lack of any other regulatory guidance on methods to satisfy requirements on communications independence.

Since submittal of the PS TR, interim staff guidance has been issued in the area of digital communications. This interim guidance augmented the Annex E information with additional considerations to fully assess communications independence.

The principles found in Annex E of IEEE 7-4.3.2 are an integral part of the assessment. AREVA NP believes that the strategies for communications independence, as described in Sections 12 and 13 of the PS TR, are consistent with the principles of Annex E of IEEE 7-4.3.2 as amplified in the recently issued interim staff guidance.

RAI 21: *Please describe the specific of checkback signal used by the Maintenance and Service unit Interface - Auxiliary Unit (MSI-AU).*

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

Response 21:

The maintenance and service unit – auxiliary unit (MSI-AU) receives the checkback signals for periodic testing of the PACS modules. The output pins on the PACS module that provide these checkback signals are labeled CBSFTOFF and CBSFTON.

These signals are processed only by the functionally safety related portion (PLD) of the PACS module.

These two signals are described in the response to RAI 6 for the PS TR, and also in the response to RAI 3 for the AV-42 TR. The response to RAI 6 of the PS TR is expanded upon and clarified below:





RAI 22: *Please describe all non-safety information that is input into the PS. If there is no information of this type, then please provide a statement to that effect.*

Response 22:

Section 13.0 of the PS TR is titled “Safety to Non-Safety Interface.”

Section 13.1 describes the types of interfaces between the protection system and non-safety I&C systems. Section 13.1 also describes the system-level requirements applied to all safety to non-safety protection system interfaces.

Section 13.2 describes the PS interface with the service unit for monitoring, testing, diagnostics and application software modifications. This interface is detailed further in Section 2.5 of Siemens TR EMF-2210, Revision 1(Reference 3).

Section 13.3 describes the PS interface to the process information and control system (PICS). The information input to the PS from the PICS is the following:

- Signals to initiate periodic testing of the PS outputs to the RT devices.
- Signals to reset ESF actuation signals to allow manual operation of actuators in a post-accident management capacity.
- Signals to validate or inhibit permissives.

Section 13.4 describes the PS interface to other control systems. With the exception of the PICS signals described above, the PS does not receive input from these systems.

RAI 23: *Please describe the reliability analysis that has been performed on the PS.*

Section 5.15 of IEEE 603-1991 says: “Reliability. For those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved. IEEE Std 352-1987 and IEEE Std 577-1976 provide guidance for reliability analysis.”

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

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

Response 23:

The Probabilistic Risk Assessment (PRA) is not the only reliability analysis that is performed on the PS. Section B of RG 1.152 Revision 2 says: “The NRC’s acceptance of the reliability of computer systems is based on deterministic criteria for both hardware and software.” These deterministic criteria are essentially the system characteristics that, if exhibited by a safety system, provide reliability (e.g., redundancy, independence, single failure tolerance, the design processes used, etc). For this reason, the majority of Section 14.18 of the PS TR is dedicated to summarizing the system characteristics that are exhibited by the U.S. EPR PS that result in a reliable protection system. This is a form of qualitative analysis; however it is not the extent of the qualitative analysis that demonstrates compliance with Clause 5.15 of IEEE 603-1998.

The qualitative reliability analysis of the U.S. EPR PS consists of the following:

- Definition of the characteristics of the hardware and software used in the system that accommodate or limit the effects of failures or design errors.
- Definition of the characteristics of the system architecture, in which the hardware and software are applied, that accommodate or limit the effects of failures or design errors.
- Definition of postulated failure modes and the effects of those failure modes on the system taking into account the system functional requirements and the characteristics described above.

The first two bullets above are what were summarized in Section 14.18 of the PS TR. These two bullets are clarified below. A discussion of the third bullet is also given below.

Characteristics of the hardware and software:

A discussion is presented in Section 2.4 of Reference 3 regarding the quantitative and qualitative reliability analyses performed on the TXS platform hardware and software. The relevant characteristics are identified and their roles in limiting the effects of failures and design errors are described.

Page 50 of the NRC Safety Evaluation Report (SER) approving TR EMF-2110, Revision 1 (Reference 4) describes the NRC staff's acceptance of the TXS equipment and software reliability analyses as satisfying the reliability criteria of IEEE 603 as well as the requirement of 10 CFR 50.55a(h). Additionally, page 52 of Reference 4 states:

“On the basis of its review of the software development plans and inspections of the computer development process and design outputs, the staff concludes that the TXS safety systems meet the guidance of RG 1.152. Therefore, the special characteristics of computer systems have been adequately addressed, and the staff finds that the TXS system satisfies the requirements of GDC 1 and 21.”

AREVA NP therefore concludes that adherence to the approved TXS design principles related to equipment and software design and development will result in an acceptable level of reliability in system components and software.

Characteristics of the system architecture:

The architecture of the U.S. EPR is described in Sections 3 and 4 of the PS TR. The architecture is illustrated in Figure 4-1 of the PS TR. The implementation of protective functions within this architecture is described in Sections 7 and 8 of the PS TR. These aspects of the system are fundamental to both qualitative and quantitative reliability assessments.

Section 4 of the PS TR describes characteristics of the PS architecture that support reliability of the system as a whole. These include:

- Highly redundant architecture.
- Physical separation between divisions.
- Independence of electrical supply to the divisions.
- Independent subsystems within each division.

Another characteristic of the PS architecture that supports reliability of the system is the independence that is maintained between redundant divisions of the PS and between the PS and non-safety related systems. The features that provide this independence are described in Sections 12 and 13 of the PS TR.

Failure modes and effects:

The functional requirements of the system dictate the inputs to the system, how each protective function is implemented within the system, and the outputs to be generated. The hardware, software and system characteristics described above are used in conjunction with the functional requirements of the system to perform a failure modes and effects analysis (FMEA).

The system-level FMEA that has been performed for the U.S. EPR protection system is described in the response to RAI 24. The results of the PS system level FMEA are summarized in Sections 7.2 and 7.3 of the U.S. EPR design certification application.

Quantitative Reliability Measures:

As described in Section 14.18 of the PS TR, the PS is analyzed in the U.S. EPR PRA to support the overall U.S. EPR probabilistic design objectives. Additionally, the reliability of the TXS platform is demonstrated by operating experience. The TXS operating experience is summarized in Section 15 of the PS TR.

RAI 24: *Why is the Failure Modes and Effects Analysis (FMEA) not mentioned as part of the single failure analysis?*

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

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

Response 24:

A system-level FMEA is performed on the PS to identify potential single point failures and their consequences. The architecture of the PS as defined in Section 4 of the PS

TR is used as the basis for the analysis. The FMEA considers each major part of the system, how it may fail, and the effect of the failure on the system.

Because the PS is an integrated RT system and engineered safety features actuation system (ESFAS), a single failure in the system has the potential to affect both types of functions. Therefore, a single FMEA is performed on the PS and the effects on both RT and ESFAS functions are considered.

To define the major parts of the system for which failures are assumed, a single division of the PS is divided into functional units as described in Section 5 of the TR. The PS consists of four identical divisions, so the definition of functional units is the same for each division. The functional units that participate in the generation of automatic RT or ESFAS functions are:

- Remote acquisition units (RAU).
- Rod control cluster assembly units (RCCA).
- APUs.
- ALUs.

In addition to the equipment defined as functional units of the system, certain other equipment also contributes to the automatic RT function and is analyzed as part of the system-level FMEA:

- Sensors that provide input measurements.
- Hardwired output logic.
- RT devices.
- PACS modules.

In order to bound the possible failures, both detected and undetected failures of sensors and functional units are analyzed and the worst case effect of each failure is identified. Detected failures are defined as those automatically detected by the inherent and engineered monitoring mechanisms of the system. Undetected failures are those not automatically detected by the system. Two types of undetected failures are analyzed. A failure denoted “undetected–spurious” is defined as a failure which results in a spurious partial trigger or actuation. A failure denoted “undetected–blocking” is defined as a failure which results in non-issuance of a partial trigger or actuation when needed.

For conservatism, it is assumed that failures in the hardwired output logic are not detected automatically by the PS. Therefore, only undetected single failures of these devices are considered. A failure of the output logic can result in a spurious actuation (“undetected–spurious”), or failure to actuate when needed (“undetected–blocking”).

Network failures within the PS allow the receiver of data to be affected in one of three ways. First, the network failure can result in an invalid message being received. By definition, invalid messages are always detected failures, and are analyzed as single failures. Second, a network failure can result in a message received as valid that contains spurious information. This type of failure is bounded by the “undetected–spurious” failure of the sending equipment, and is therefore not considered. Third, a network failure can result in a message received as valid that fails to request an action when one is needed. This type of failure is bounded by the “undetected–blocking” failure of the sending equipment, and is therefore not considered.

When referring to the nature of a single failure, the terms “detected” and “undetected” as used in the context of the PS FMEA do not correspond to the definition of a detectable failure in IEEE 603-1998. The failures denoted “undetected” in the FMEA are detectable through periodic testing. The terms “detected” and “undetected,” as used in the FMEA, refer to the ability of the PS to automatically detect a failure through self-surveillance.

The architecture of the PS allows APUs and ALUs to be analyzed for single failure without regard to which specific APU or ALU in the division is the failure point. For these single failures, all functions of the system are considered affected, as every function is processed by at least one APU and two ALU in a division. Considering the effect on every function of the system bounds all cases of specific APU and ALU single failures.

Certain ESF actuation functions are performed uniquely within the PS architecture. For these cases, exceptions to the typical FMEA results are annotated within the results table.

Failures affecting the power supply to the cabinets of the PS are addressed at the system level through assumptions and requirements imposed on the power supply systems. The safety related PS cabinets require redundant power supply, so that no single power supply failure results in loss of power to the cabinet. It is assumed that the distribution of power within the cabinet is such that no single power distribution failure can cause loss of more than one ALU functional unit that may be housed in the same cabinet. The validity of these assumptions will be verified in the course of performing a more detailed FMEA following equipment layout and function allocation to specific equipment of the system.

RAI 25: *Please describe how cyber security will be addressed in PS application development process.*

Section 14.8.1 says: “The TXS system design provides multiple, diverse levels of protection against cyber intrusion. These include administrative/procedural controls, TXS hardware controls, and TXS software controls. These security measures have

multiple levels of defense ...” This description does not provide any information on what will be done during the application development process to address cyber security.

10 CFR 50.34(h) “Conformance with the Standard Review Plan (SRP).” requires: “(1) (ii) Applications for ... design approvals ... shall include an evaluation of the facility against the SRP ... (2) The evaluation required by this section shall include an identification and description of all differences in design features, analytical techniques, and procedural measures proposed for a facility and those corresponding features, techniques, and measures given in the SRP acceptance criteria. Where such a difference exists, the evaluation shall discuss how the alternative proposed provides an acceptable method of complying with those rules or regulations of Commission, or portions thereof, that underlie the corresponding SRP acceptance criteria.” NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants,” Chapter 7, Table 7-1 identifies that Regulatory Guide 1.152 contains acceptance criteria applicable to Reactor Trip Systems and Engineered Safety Feature systems. Regulatory Guide 1.152, Revision 2 section C.2 says in part : “The digital safety system development process should address potential security vulnerabilities in each phase of the digital safety system lifecycle.” Since the PS TR will be incorporated into design certification application by reference, these acceptance criteria will need to be addressed at some point.

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

Response 25:

**Security-Related Information
Withheld in Accordance with 10CFR2.390**

**Security-Related Information
Withheld in Accordance with 10CFR2.390**

**Security-Related Information
Withheld in Accordance with 10CFR2.390**

**Security-Related Information
Withheld in Accordance with 10CFR2.390**

**Security-Related Information
Withheld in Accordance with 10CFR2.390**

**Security-Related Information
Withheld in Accordance with 10CFR2.390**

**Security-Related Information
Withheld in Accordance with 10CFR2.390**

**Security-Related Information
Withheld in Accordance with 10CFR2.390**

RAI 26: *What is the proposed design acceptance criteria for determining which ESF actuation signals can be reset by specific operator action and which one can be reset by the initiating plant variable returning to within an acceptable range?*

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

Response 26:

There are no design acceptance criteria (DAC) proposed related to determining which ESF actuation signals can be reset by operator action and which can be reset automatically. DAC are not needed in this case because the reset of each ESF actuation function is described in Section 7.3 of the U.S. EPR design certification application. The reset requirements for each function are described in text and illustrated in the functional logic for each actuation. The majority of the actuations require operator action to reset the PS output to the PACS modules.

There are three functions that do not require operator action to reset the output signal. These functions require automatic reset of the PS actuation output for the following reasons:



- A protective setpoint may be temporarily exceeded as a result of a plant transient that the protective action is not intended to mitigate (charging isolation on high

RAI 27: Which components assure the once initiated, protective actions go to completion?

IEEE STD 603-1991 Section 5.2 says: "The safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion."

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

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

Response 27:

See the response to RAI 17.

RAI 28: Please explain where an analysis of the entire safety system is documented.

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

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

Response 28:

Compliance with the requirements of IEEE 603-1998, for the safety systems within the scope defined in Figure 1 of IEEE 603-1998, is documented in the U.S. EPR design certification application. The instrumentation and control (I&C) portions of the safety systems are discussed in Chapter 7 of the design certification application. The electrical power portions of the safety systems are discussed in Chapter 8 of the design certification application. The safety related process equipment with interfaces to the I&C and electrical safety systems is discussed in the appropriate chapters throughout the design certification application.

The scope of the PS TR is limited primarily to the digital portions of the system that represent a departure from traditional analog protection systems currently used in U.S. nuclear power stations. Therefore, sections 14.3 through 14.18 primarily describe these portions of the safety system.

As part of RAI 2 for the PS TR, the NRC stated that sections 14.29 through 14.34 asserted compliance of equipment not described in the report with IEEE 603-1998. As a result, AREVA NP agreed to remove those sections from the PS TR.

Therefore, it is appropriate that sections 14.3 through 14.8 primarily describe compliance with IEEE 603-1998 for the portions of the system that are the subject of the report.

RAI 29: *Please describe the operating bypass features associated with the manual actuations.*

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

Response 29:

Manual initiation of protective actions is part of the PS as defined in the TR. Subsequent manual control of safety systems is processed through other safety related systems and is not a function of the PS.

The responses to RAIs 16 and 18 describe the means to manually initiate protective actions. As described in response 18, most ESF actuation functions are processed by

the APUs and/or ALUs of the protection system. For these functions, the manual initiation is combined with the automatic initiation logic so that the manual function is subject to the same operating bypasses as the automatic function.

The manual initiations of protective actions that are not processed by the APUs and/or ALUs (i.e., wired directly to PAC modules) are not subject to operating bypasses.

The statements in PS TR Sections 14.26 and 14.27 are true for both automatic and manual functions processed by the PS. PS TR Sections 14.33 and 14.34 have been deleted from the PS TR as part of the response to RAI 1.

RAI 30: *Please describe how the redundant ring network topology is immune to single failures.*

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

Response 30:

Section 6.1.2 of the PS TR does not claim that a redundant ring network is immune to single failures. Section 6.1.2 describes the features of the network topology that accommodate specific failures. These features add to overall system reliability.

A single redundant ring network, as used in the U.S. EPR PS architecture, is not required to demonstrate single failure tolerance. Single failure tolerance is required of the safety function as a whole, not of any individual segment of a system that contributes to the safety function. In the case of the U.S. EPR protection system, the complete loss of function of any single network within the system does not prevent the performance of any safety function by the system. The remaining portions of the system are adequate to perform the functions required of the system.

Item 12 in the staff position of Reference 6 provides examples of credible communication failures. These are the communication failures that are taken into account in the U.S. EPR safety systems design.

Network failures are addressed in the system level FMEA as described in the response to RAI 24. Bounding network failures are analyzed to demonstrate single failure tolerance at the system level. The specific failures described in Reference 6 will be verified to be bounded by the system level FMEA, or will be addressed specifically, as

part of a more detailed FMEA to be performed following equipment layout and software definition.

The communication failure described in NRC Information Notice 2007-15, "Effects of Ethernet-Based, Non-Safety Related Controls on the Safe and Continued Operation of Nuclear Power Stations," corresponds to the failure in position 12 of Reference 6, "Messages may occur at a high rate that degrades or causes the system to fail (i.e., broadcast storm)."

The communications within the PS that are the subject of this RAI are not ethernet-based, nor are they non-safety related. Specific features of the TXS platform related to interchannel communication methods (described in Section 12 of the PS TR and in Section 2.9 of Reference 3) preclude this type of failure from occurring. However, if this were a credible failure mode for a redundant ring network, as implemented in the PS, it would result in the failure of only one network. The remaining portions of the PS are adequate to perform the system's safety functions.

RAI 31: *Please describe all of the types of maintenance bypasses and their associated affect on the RT or ESF functions.*

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

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

5) *Are the functionally independent subsystems (A and B) redundant to each other?*

Response 31:

1. Sensor measurements that are redundant to one another are acquired in different divisions. If maintenance or testing is required to be performed on a given sensor, the service unit (SU) is used to access the PS unit that acquires the measurement and place that sensor in a lockout condition. [

] After the signal has been marked with a faulty status, it is disregarded in downstream processing. For example, a two out of four voting function that receives one faulty input votes two out of three on the remaining non-faulty inputs. No manual actions, beyond placing the sensor in lockout, are required for the downstream processing to properly accommodate the bypassed sensor. Administrative controls (e.g., plant technical specifications) prevent bypass of more than the allowable number of redundant sensors at any one time.

2. The different divisions of the PS are considered redundant to one another. There is no provision in the U.S. EPR design for allowing bypass of an entire PS division. Individual functional units within a division may be bypassed for maintenance or testing. The number and combinations of units within the system that can be bypassed at any one time are defined by the plant technical specifications and controlled accordingly.
3. When a PS functional unit is bypassed for testing or maintenance, any discrete digital or analog outputs via output modules are disabled. However, output of specific signals can be initiated as part of testing

[

] The remainder of the system continues to function normally and is capable of performing the system safety functions.

If electrical power is removed from a functional unit as part of the bypass, the bypassed unit ceases to provide or receive network communications. In this case the other units of the system recognize the last valid message received from the bypassed unit as out of date, and disregard the information until the bypassed unit resumes communication. The remainder of the system continues to function normally and is capable of performing the system safety functions.

[

]

4. OLMs are not bypassed for maintenance or testing. They are either in service, or are considered to have failed. The response of the affected network to a failed OLM is described in Section 6.1 of the PS TR.
5. The functionally independent subsystems (A and B) of the PS are not credited as being redundant to one another. In certain cases, an additional level of redundancy is achieved by using the two subsystems within a division. However, the minimum required redundancy for each safety function does not depend on a redundant relationship between the subsystems.

RAI 32: *Please clarify or correct the parenthetical bus numbering shown on the right side of Division 4 of Figure 4-1.*

Response 32:

The parenthetical bus numbering shown on the right side of Figure 4-1 is corrected in the attached revised figure 4-1.

RAI 33: *Are all PS Optical Link Modules (OLMs) shown in Figures 6-3 through 6-19? Are all instances where multiple PS units access a network through the same OLM explicitly shown in figures 6-3 through 6-19? Does the same OLM appear on more than one figure?*

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

Response 33:

All of the PS OLMs are shown in Figures 6-3 through 6-19. All instances of multiple PS functional units accessing a network through the same OLM are explicitly shown. The same OLM does not appear on any two separate figures.

RAI 34: *Are the PS networks considered to be part of the PS?*

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

Response 34:

The networks between functional units of the PS shown in Figures 6-3 through 6-20 are part of the PS.

The PS units are the major functional “boxes” on Figure 4-1. The units of the PS are a subset of the PS as a whole. The optical link modules are not part of any specific PS unit, but they are part of the PS along with the connections between them. The OLMs are considered a part of a PS division according to the electrical division from which they receive their power supply.

The intent of Section 5.0, “Protection System Units” is to define what is being referred to when terminology such as “functional unit”, “APU”, “ALU”, “RAU”, etc. is used. Section 5.0 is not intended to define the entire scope of what is included in the PS.

Everything shown in Figures 6-3 through 6-20, with the exception of the PIs in Figure 6-19, is part of the PS.

RAI 35: *Please define all items that could be considered to be a PS unit.*

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

Response 35:

Section 5.0 does not define all possible components or connections that are within the scope of the PS (see response to RAI 34). Section 5.0 does however describe all PS units that can possibly access a PS network through an OLM.

RAI 36: *Please discuss how the U.S. EPR design complies with IEEE 603-1991 Section 7.4.*

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

IEEE Std. 603-1991 Section 7, “Execute Features - Functional and Design Requirements,” says: “In addition to the functional and design requirements in Section 5, the following requirements shall apply to the execute features:” IEEE Std. 603-1991 Sub-Section 7.4, “Operating Bypass,” contains operating bypass requirements.

Therefore IEEE 603-1991 requires that the execute features contain operating bypass functionality. However, Section 14.33 "Sub-Clause 7.4 - Operating Bypass," says: "Operating bypass of protective actions are implemented in the sense and command features of the PS."

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

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

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

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

Response 36:

The U.S. EPR design complies with IEEE 603-1998 Clause 7.4 by not incorporating operating bypasses in the execute features. The statement in Section 14.33 of the PS TR which discussed Clause 7.4 was deleted in response to RAI 1.

Clause 7.4 requires that when applicable conditions are not met, the safety system shall prevent the activation of an operating bypass. Clause 7.4 also requires that, if an activated operating bypass is no longer permissible, the safety system shall accomplish one of three specified actions. Clause 7.4 does not require that operating bypass functionality exist in the execute features. In fact, no clause in IEEE 603-1998 requires the existence of operating bypasses in safety systems at all. The definition of operating bypass in IEEE 603-1998 includes a note stating that: "An operating bypass is not the same as a maintenance bypass. Different modes of plant operation may necessitate an automatic or manual bypass of a safety function."

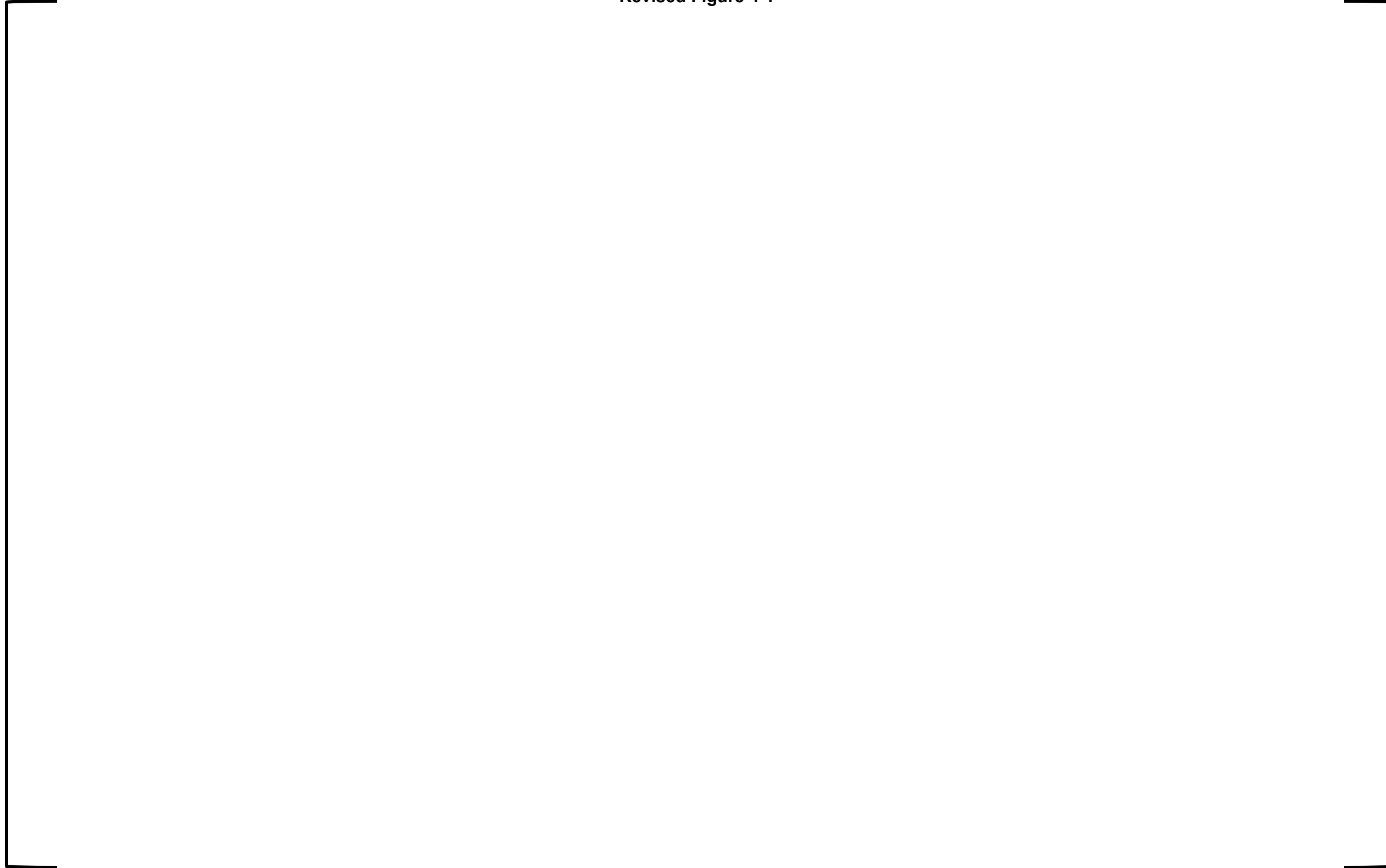
The two operating bypass clauses in IEEE 603-1998 (6.6 and 7.4) impose requirements to assure that, when operating bypass functionality is incorporated, it is incorporated in a manner to assure the availability of safety functions when they are required.

Operating bypasses are included in the design of the U.S. EPR protection system. They are implemented in the form of permissive signals in the sense and command portion of the system. The implementation of these operating bypasses is consistent with requirements of IEEE 603-1998 Clause 6.6. The operating bypass requirements for each RT and ESF actuation function are described in Sections 7.2 and 7.3 of the U.S. EPR design certification application.

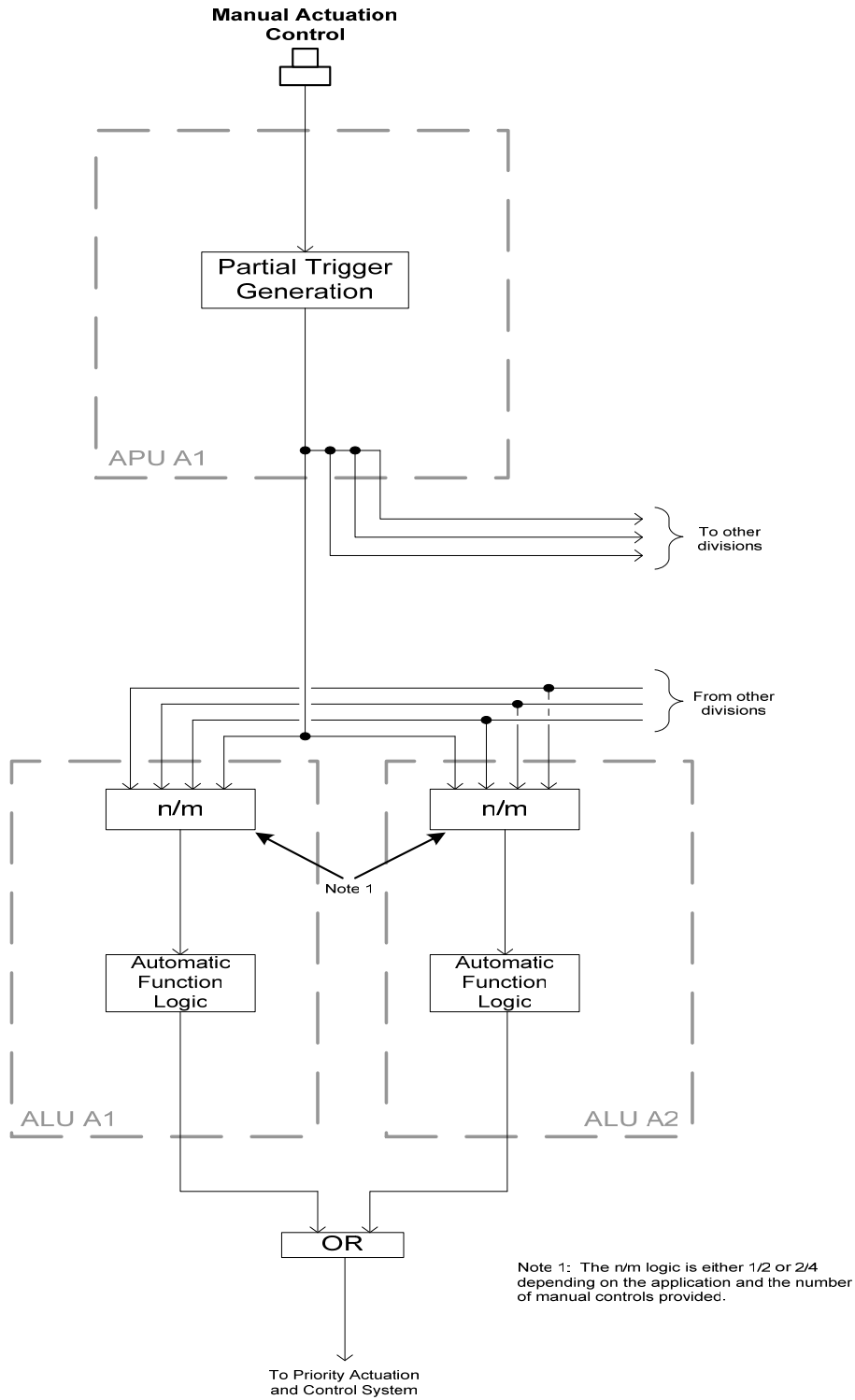
References:

1. Letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), "Response to a Request for Additional Information Regarding ANP-10272, 'Software Program Manual for TELEPERM XS™ Safety Systems Topical Report' (TAC No. MD3971)," NRC:07:020, May 22, 2007.
2. Letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), "Request for Review and Approval of ANP-10284, 'U.S. EPR Instrumentation and Control Diversity and Defense-in-Depth Methodology Topical Report'," NRC:07:022, June 20, 2007.
3. Letter, James F. Mallay (Siemens Power Corporation) to Document Control Desk (NRC), "Publication of EMF-2110(NP)(A) Revision 1, TELEPERM XS: A Digital Reactor Protection System," NRC:00:033, July 12, 2000).
4. Letter dated May 5, 2000, from Stuart A. Richards, NRC, to Jim Mallay (Siemens Power Corporation, "Acceptance for Referencing of Licensing Topical Report EMF-2110 (NP), Revision 1, "TELEPERM XS: A Digital Reactor Protection System," and associated Safety Evaluation Report.
5. Letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), "Request for Review and Approval of ANP-10272, 'Software Program Manual TELEPERM XS™ Safety Systems Topical Report'," NRC:06:061, December 21, 2006.
6. NRC Interim Staff Guidance (ISG) DI&C-ISG-04, Revision 0, Task Working Group #4, "Highly-Integrated Control Rooms – Communications Issues (HICRc), September 28, 2007.

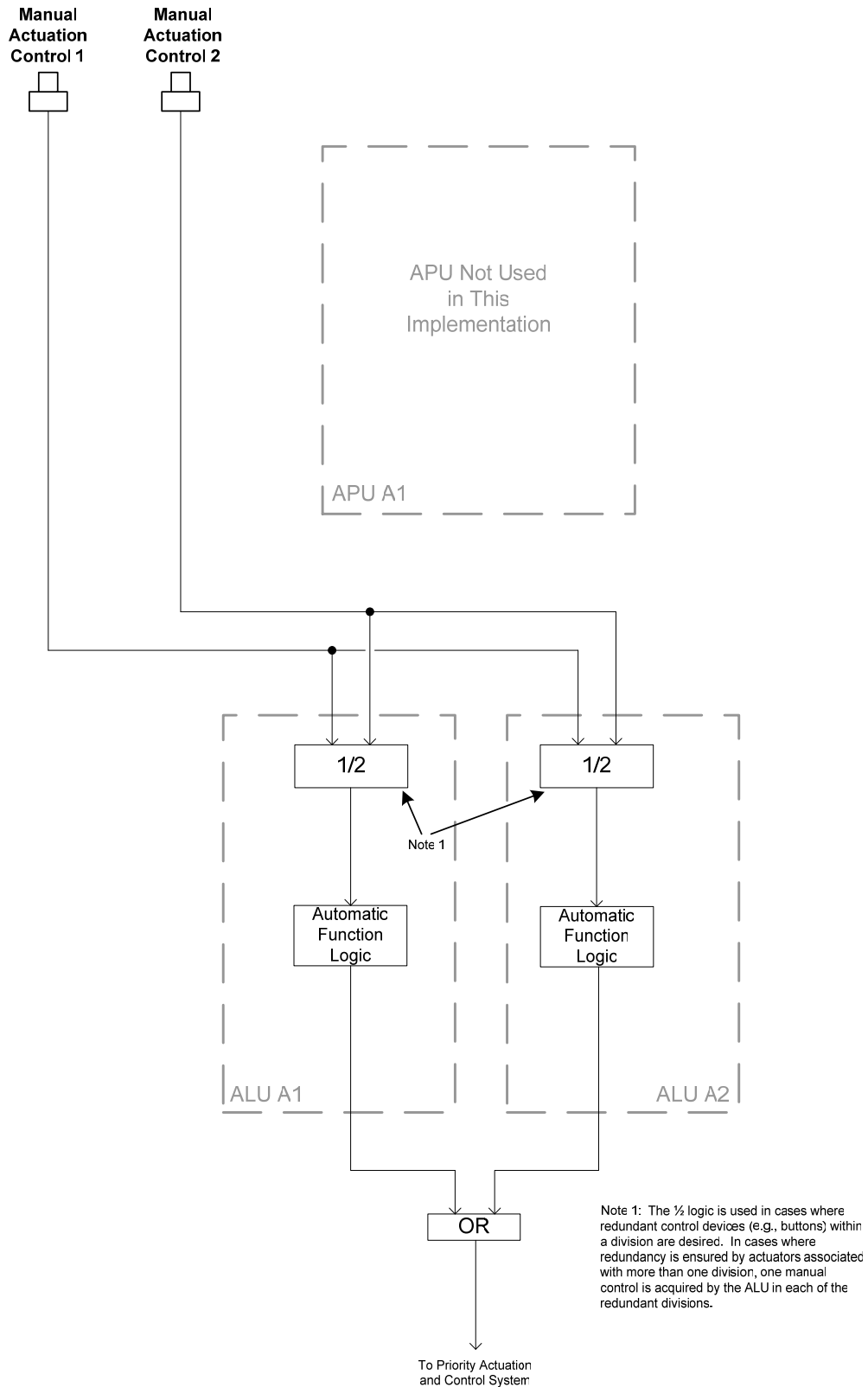
Revised Figure 4-1



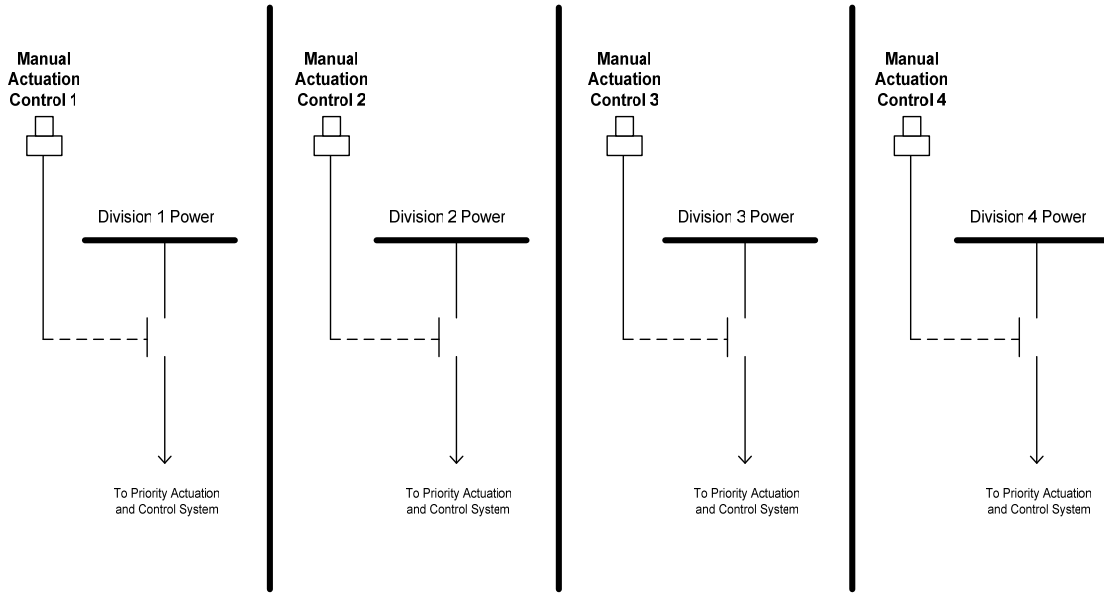
Revised Figure 8-3: Typical #1 for Manual System Level Initiation



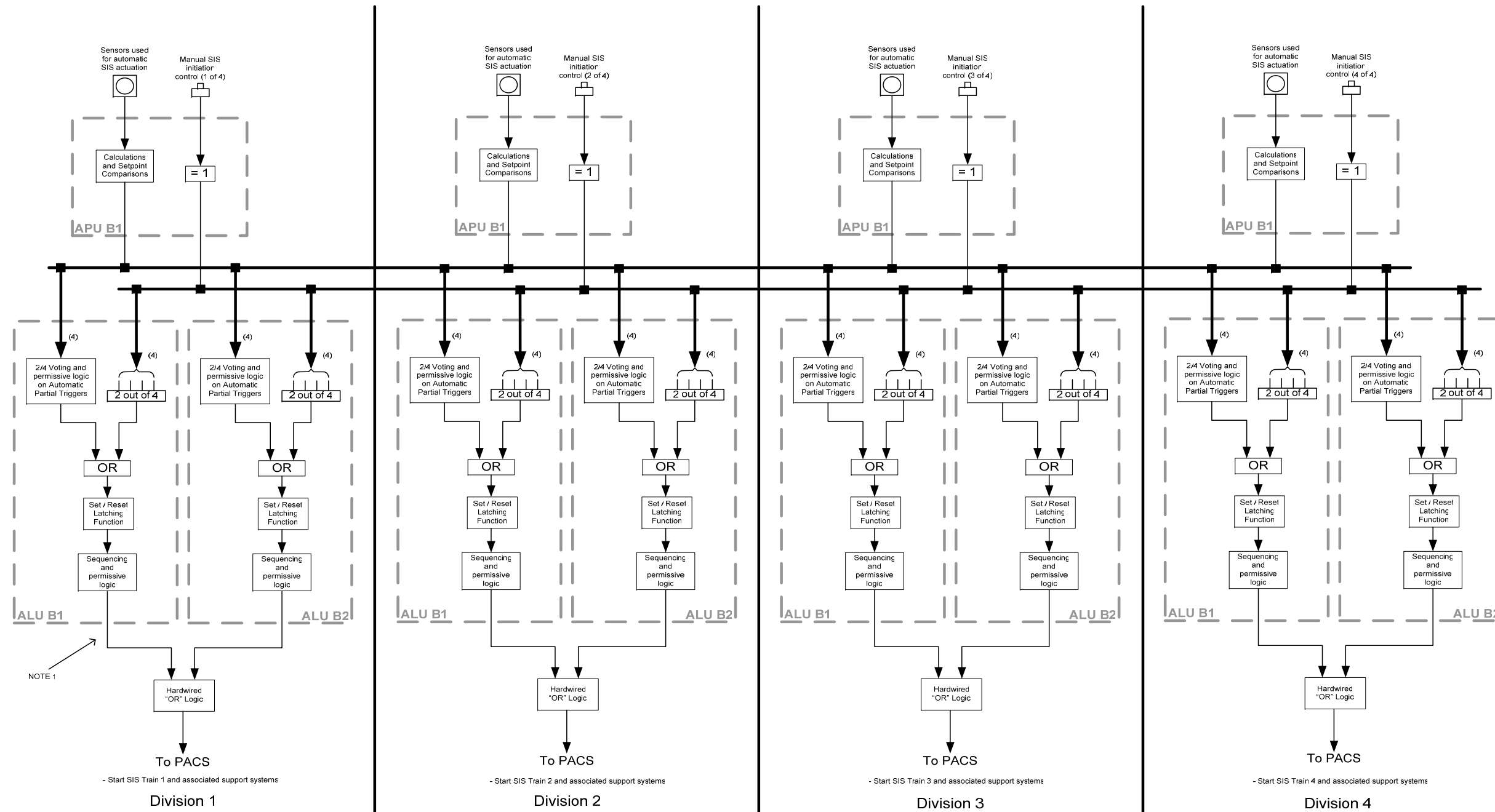
Revised Figure 8-4—Typical #2 for Manual System Level Initiation



Revised Figure 8-5—Typical #3 for Manual System Level Initiation

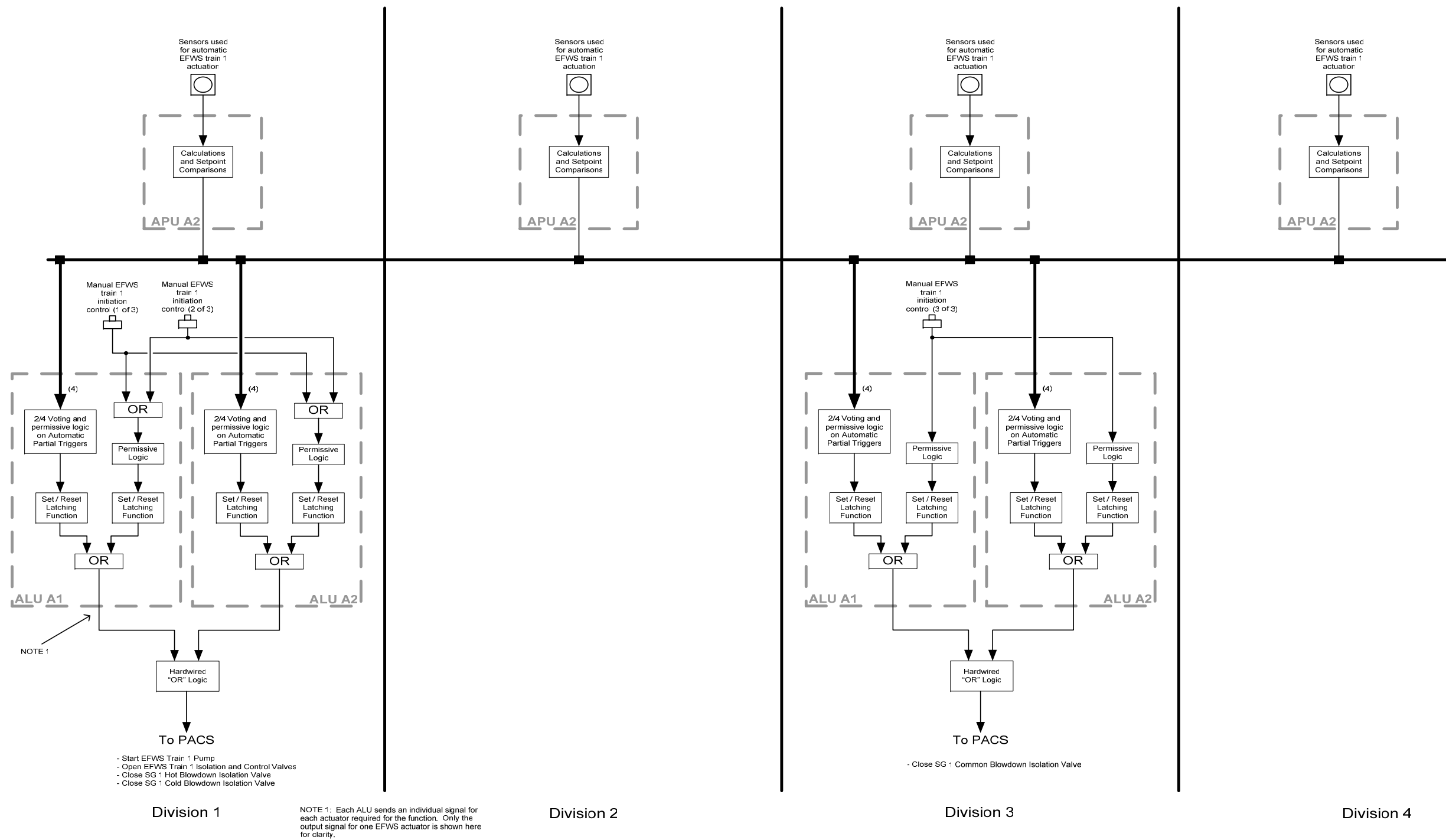


RAI Figure 18-1



NOTE 1 Each ALU sends as many individual signals as there are actuators required for the function. Only the output signal for one SIS actuator is shown here for clarity.

RAI Figure 18-2



RAI Figure 20-1

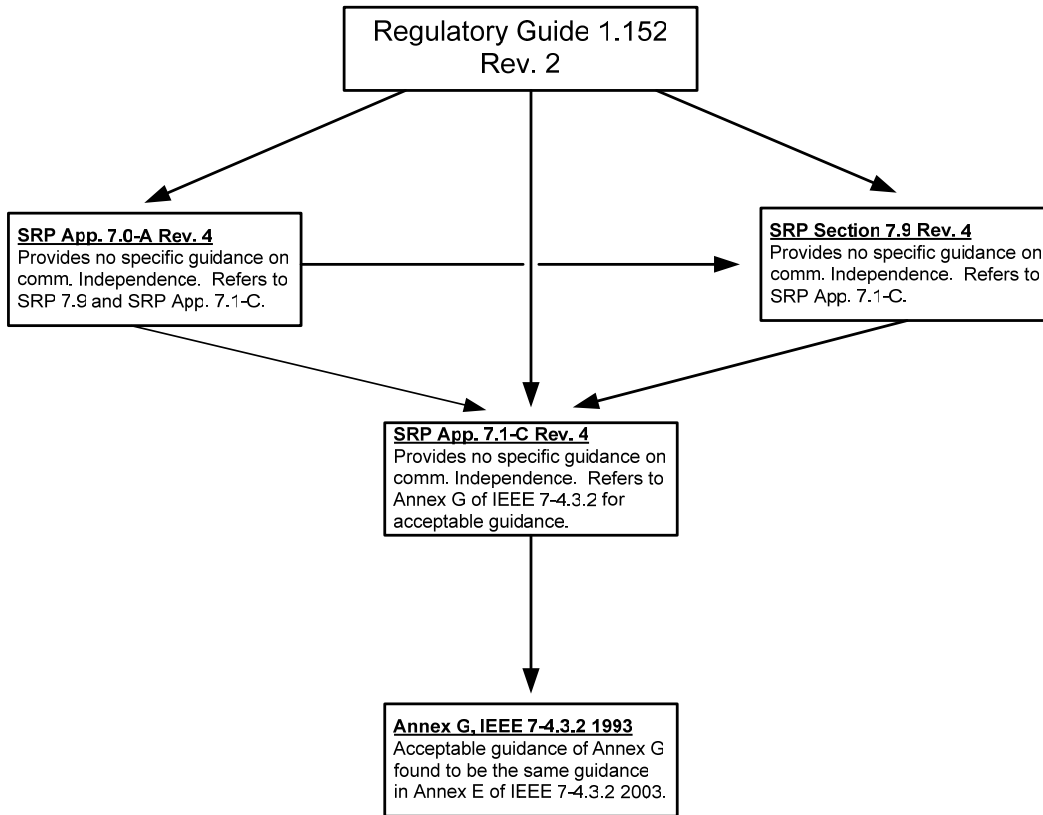
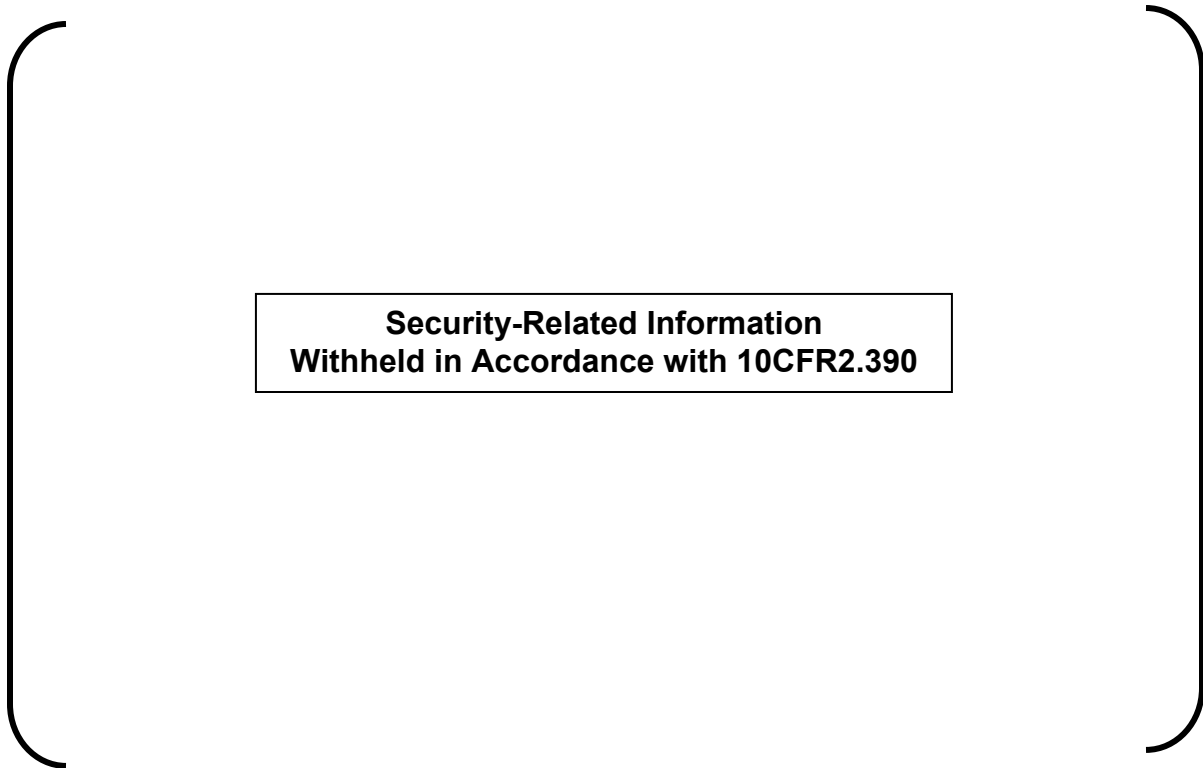


Figure RAI 25-1 - Diverse Means for Access Control to TXS Computers



Additional Information in Support of a Request for Additional Information – ANP-10281P, “U.S. EPR Digital Protection System” (TAC No. MD4977)

In the response to RAI 4 (see Reference 4 of the cover letter), AREVA NP stated that supporting documentation would be provided to the NRC detailing the allocation of time delays to the computerized portion of the PS. This information is provided below.

Scope of Digital Response Time Allocation

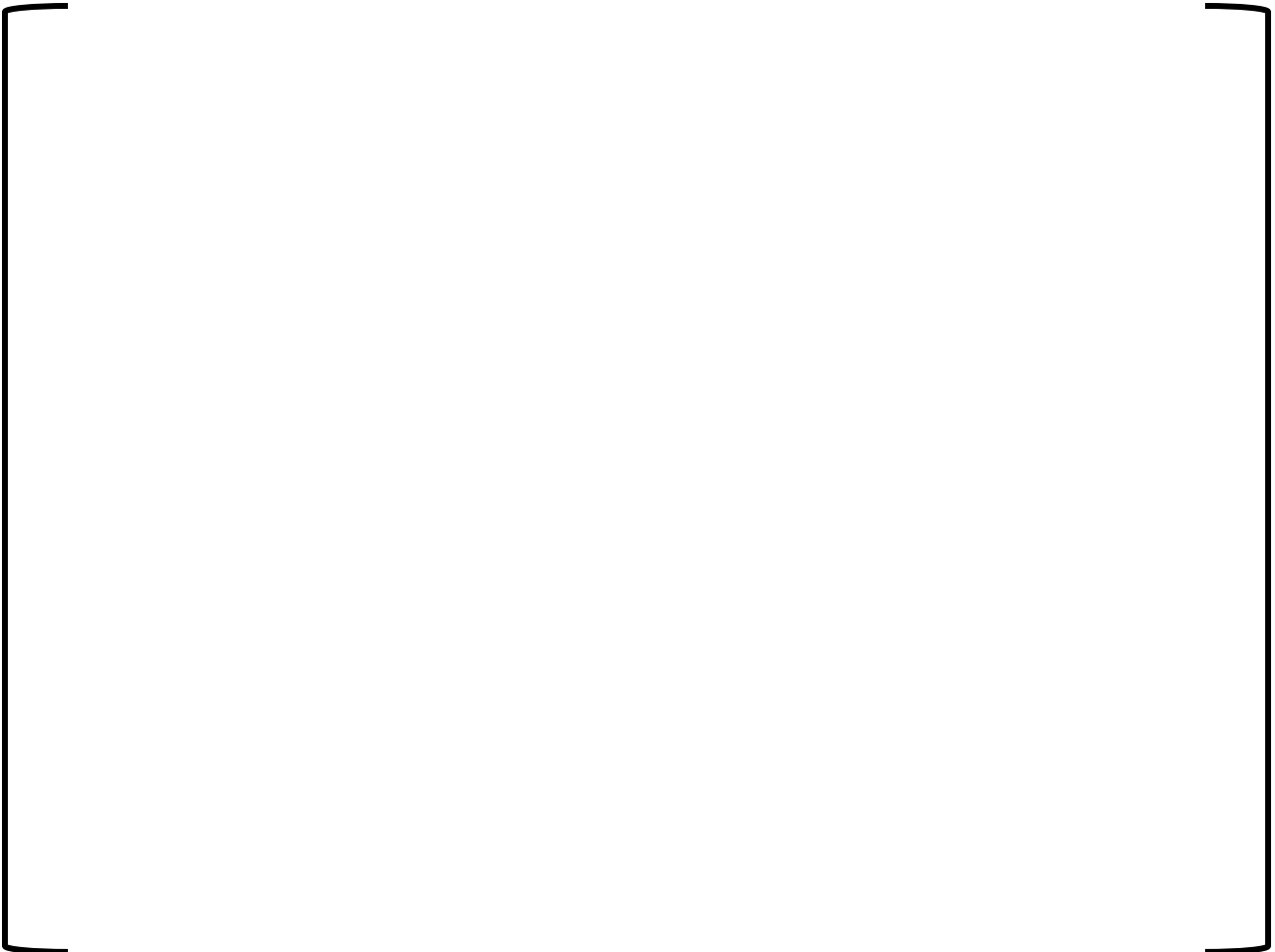


TELEPERM XS Timing Concepts





Limiting Response Time



Acquisition of an Input Signal (Time Fragment <1>)

--

Processing Within one FDG (Time Fragment <2>)

--

Signal Exchange between FDGs within the Same Processor (Time Fragment <3>)

--

Signal Exchange between Function Processors over a Network Link (Time Fragment <4>)

--



Generation of an Output Signal (Time Fragment <5>)



Timing Assumptions





Function Type 1: Typical Function not Using APU A3



Function Type 2: Typical Function Using APU A3





Function Type 3: Three Level Function not Using APU A3



Function Type 4: Three Level Function Using APU A3



Function Type 5: Special Case for Low DNBR Reactor Trip Function





Figure B-1



Figure B-2



Figure B-3



Figure B-4



Figure B-5



Figure B-6



Figure B-7

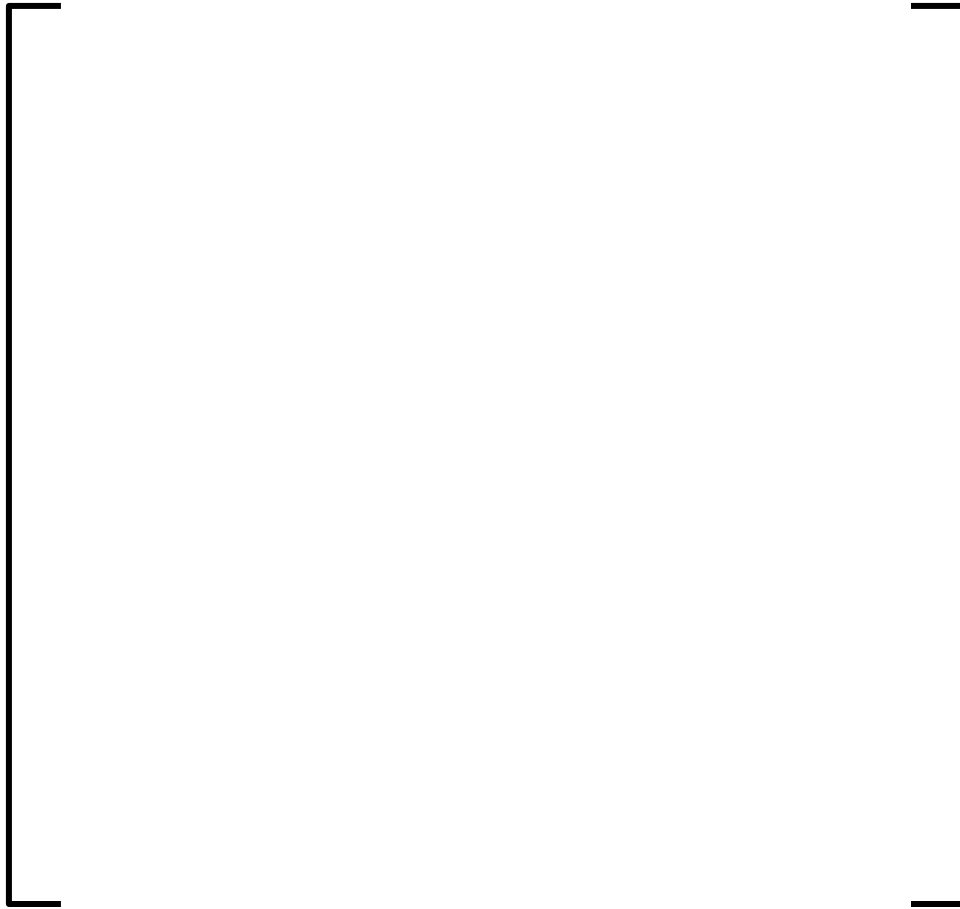


Figure B-8

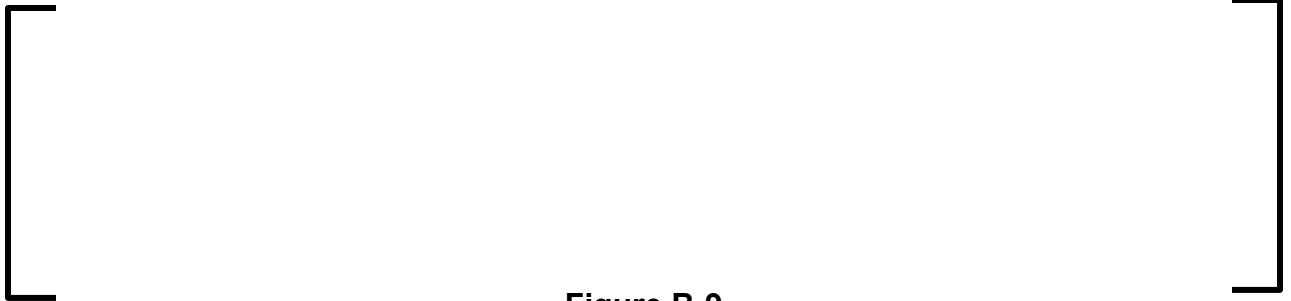


Figure B-9

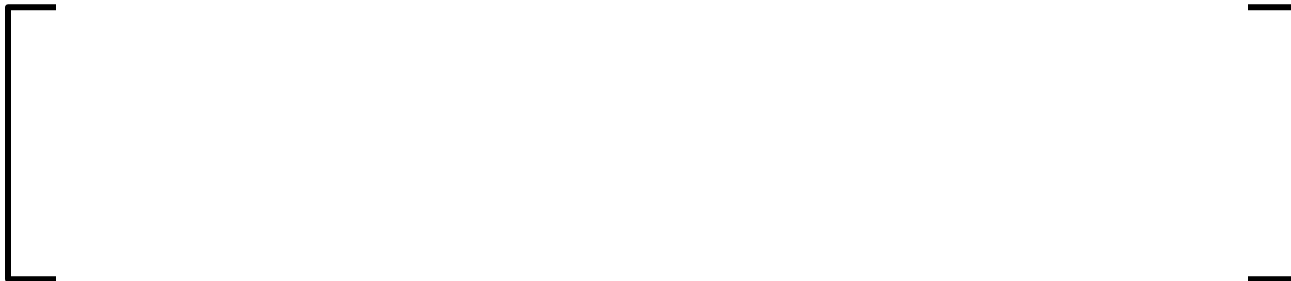


Figure B-10

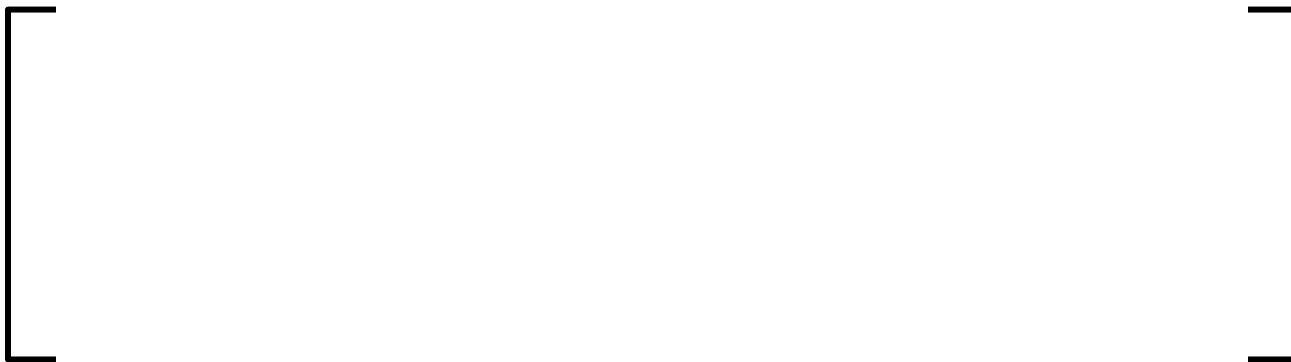


Figure B-11



Figure B-12

