REQUEST FOR SUPPLEMENTAL INFORMATION

REVIEW OF PRESSURIZED WATER REACTOR OWNERS GROUP TOPICAL REPORT

WCAP-17261-P/NP, REVISION 0, "JUSTIFICATION FOR A TECHNICAL SPECIFICATION

ACTION FOR TWO INOPERABLE RTS [REACTOR TRIP SYSTEM] OR ESFAS

[ENGINEERED SAFETY FEATURES ACTUATION SYSTEM] INSTRUMENTATION

CHANNELS"

A. Instrumentation and Controls Branch (EICB) Request for Supplemental Information

Licensing Action: Topical Report (TR) WCAP-17261-P/NP, Revision 0, proposes to add an Action in the Westinghouse Electric Company (Westinghouse) standard technical specifications (STS), for two inoperable reactor trip system (RTS) or engineered safety features actuation system (ESFAS) functions for those functions with a two-out-of-four actuation logic. During the acceptance review, it was determined that the TR did not provide a description that clearly demonstrates how the proposed STS for Westinghouse designed plants will meet all current regulatory requirements in the General Design Criteria (GDCs) of Title 10 of the *Code of Federal Regulations* (10 CFR) and in 10 CFR 50.55a(h), which incorporates by reference Institute of Electrical and Electronics Engineers (IEEE) Standard (Std.) 279-1971.

Regulatory Design Requirements and the Technical Specifications (TS): The regulatory design criteria, GDCs and IEEE Std. 279, for the design of protection systems specifically include requirements to support the anticipated operation and maintenance of the protection system (e.g., Channel Bypass or Removal from Operation). However, these regulatory requirements do not explicitly specify limits regarding how long or under what conditions some of these design features are to be used. However, the TS take into consideration the specific equipment designs and associated plant operating modes and place restrictions on the use of these required features. The TS generally place limits on the length of time of operation in a condition where the single failure criterion is not met. The TS also generally require the plant to exit the modes in which a system is required to be operable if the system is no longer capable of performing its safety function.

Sharing of Components Results in Additional Operational Restrictions: If protection and control systems share common components (e.g., sensors) then additional design requirements are imposed (e.g., GDC 24 and IEEE Std. 279, Clause 4.7). To date, the action statements in the TS have not allowed operation in a condition where the "Separation of Protection and Control" requirements are not met.

1. Evaluation Against 10 CFR Part 50, Appendix A - GDCs

The underlined portions of both GDCs below, when considered simultaneously, in effect require that an additional failure be postulated, if there are common components between the protection and control systems. If a protection system has four channels and one of those channels has shared components with the control system, then in effect GDC 24

requires that the 2-out-of-4 system be treated as a 2-out-of-3 system when addressing the other requirements (e.g., minimum redundancy). This means that a single channel could be removed from service (i.e., a second inoperable channel – the first inoperable channel is postulated by GDC 24, which makes the 2-out-of-4 system into a 2-out-of-3 system) and the ability of the protection system to perform the protective function is preserved, but the system would no longer meet the single failure criterion when in this condition (in this case GDC 21 would require that acceptable reliability be demonstrated).

GDC 21, "Protection system reliability and testability," states:

"The protection system shall be designed for high functional reliability and inservice testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. The protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred."

GDC 24, "Separation of protection and control systems," states:

"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."

Evaluation of a two-out-of-four Logic System against the GDC Criteria

The requirements from the GDCs must all be met, simultaneously. The easiest way to understand the cumulative impact of multiple requirements is to first analyze one and then successively add additional requirements into consideration; this is the method followed in the five subsections (1.1 – 1.5) below. A table is included in each subsection to show the status of each of the four instrument channels.

1.1 Single Failure Criterion

GDC 21, "Protection system reliability and testability," states:

> "…Redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function…."

Channel 1	Channel 2	Channel 3	Channel 4
SF	Operable	Operable	Operable
SF Criterion Met			

Note: SF = Postulated to be failed due to the Single Failure Criterion

1.2 Single Failure Criterion and Removal of One Channel from Service

GDC 21, "Protection system reliability and testability," states:

> "…Redundancy and independence designed into the protection system shall be sufficient to assure that … (2) removal from service of any component or channel does not result in loss of the required minimum redundancy...."

Channel 1	Channel 2	Channel 3	Channel 4
SF	BP	Operable	Operable
SF & BP Criteria met			

Note: BP = Bypass or Removal from Service (i.e., not tripped, not operable)

1.3 Separation of Protection and Control

Certain words below are bolded in order to emphasize the explicit relationship between the two GDCs. GDC 21, "**Protection system reliability** and testability," states:

> "…**Redundancy and independence** designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function…."

GDC 24, "Separation of protection and control systems," states:

> "The protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure … 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**...."

Channel 1	Channel 2	Channel 3	Channel 4
SF	CC	Operable	Operable
SF & CC Criteria met			

Note: CC = A Component is Common to the Control and Protection Systems (the component that is postulated to fail per GDC 24)

1.4 Separation of Protection and Control and Removal of One Channel from Service

GDC 21, "Protection system reliability and testability," states:

> "…Redundancy and independence designed into the protection system shall be sufficient to assure that … (2) removal from service of any component or channel does not result in loss of the required minimum redundancy *unless the acceptable reliability of operation of the protection system can be otherwise demonstrated*...."

GDC 24, "Separation of protection and control systems," states:

> "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...."

Channel 1	Channel 2	Channel 3	Channel 4
SF	CC	BP per GDC 21 (2)	Operable
Criteria met only if it is additionally demonstrated that the protection system is acceptably reliable.			

1.5 Bypassing Two Channels

Topical Report WCAP-17261-P/NP, Revision 0, proposes that two channels are allowed to be in bypass simultaneously (i.e., not placed in trip) for a limited amount of time.

Channel 1	Channel 2	Channel 3	Channel 4
SF	CC	BP	BP
It is not clear how both GDC 21 and GDC 24 can be met under this proposal. Westinghouse should provide supplemental information demonstrating how these criteria are still met.			

EICB Question (1): Please describe how the proposed STS for Westinghouse designed plants would meet the GDCs quoted above for each of the five conditions (1.1 – 1.5) postulated.

2. Evaluation Against IEEE Std. 279, "Criteria for Protection Systems for Nuclear Power Generating Stations"

The underlined portions of IEEE Std. 279-1971 below, when considered simultaneously, require that an additional failure be postulated, for each adverse failure of common components within the protection and control systems. The second paragraph of Clause 4.7.3 requires that the requirements of the first paragraph of Clause 4.7.3 (i.e., two failures) be met while one channel is bypassed or removed from service.

Clause 4.2, "Single Failure Criterion," states:

"Any single failure within the protection system shall not prevent proper protective action at the system level when required...."

Clause 4.7, "Control and Protection System Interaction," includes Clause 4.7.3, "Single Random Failure," which states:

"Where a single random failure can cause a control system action that results in a generating station condition requiring protective action and can also prevent proper action of a protection system channel designed to protect against the condition, the remaining redundant protection channels shall be capable of providing the protective action even when degraded by a second random failure.

Provisions shall be included so that this requirement can still be met if a channel is bypassed or removed from service for test or maintenance purposes. Acceptable provisions include reducing the required coincidence, defeating the control signals taken from the redundant channels, or initiating a protective action from the bypassed channel."

Clause 4.11, "Channel Bypass or Removal from Operation," states:

"The system shall be designed to permit any one channel to be maintained, and when required, tested or calibrated during power operation without initiating a protective action at the systems level. During such operation the active parts of the system shall of themselves continue to meet the single failure criterion…."

Evaluation of a two-out-of-four Logic System against IEEE Std. 279-1971

The requirements from IEEE 279 must all be met, simultaneously. The easiest way to understand the cumulative impact of multiple requirements is to first analyze one and then successively add additional requirements into consideration; this is the method followed in the five subsections (2.1 – 2.5) below.

2.1 Single Failure Criterion

Clause 4.2, "Single Failure Criterion" (SF), states:

> "Any single failure within the protection system shall not prevent proper protective action at the system level when required…."

Channel 1	Channel 2	Channel 3	Channel 4
SF	Operable	Operable	Operable
SF Clause Met			

2.2 Single Failure Criterion and Removal of One Channel from Service

Clause 4.11, "Channel Bypass or Removal from Operation," states:

> "The system shall be designed to permit any one channel to be maintained, and when required, tested or calibrated during power operation without initiating a protective action at the systems level. <u>During such operation the active parts of the system shall of themselves continue to meet the single failure criterion…</u>"

Channel 1	Channel 2	Channel 3	Channel 4
SF	BP	Operable	Operable
SF & BP Clauses met			

2.3 Separation of Protection and Control

Clause 4.7, "Control and Protection System Interaction," includes Clause 4.7.3, "Single Random Failure," which states:

> "<u>Where a single random failure can</u> cause a control system action that results in a generating station condition requiring protective action and can also prevent proper action of a protection system channel designed to protect against the condition, <u>the remaining redundant protection channels shall be capable of providing the protective action even when degraded by a second random failure</u>…"

Channel 1	Channel 2	Channel 3	Channel 4
SRF	CC	Operable	Operable
SF & CC Clauses Met			

Note 1: CC = Common Component to the Control and Protection Systems (component postulated to fail per 4.7.3)
Note 2: SRF = Second Random Failure (per 4.7.3)

2.4 Separation of Protection and Control and Removal from Service

Clause 4.7, "Control and Protection System Interaction," includes Clause 4.7.3, "Single Random Failure," which states:

> "<u>Where a single random failure can</u> cause a control system action that results in a generating station condition requiring protective action and can also prevent proper action of a protection system channel designed to protect against the condition, <u>the remaining redundant protection channels shall be capable of providing the protective action even when degraded by a second random failure</u>…"

<u>Provisions shall be included so that this requirement can still be met if a channel is bypassed or removed from service for test or maintenance purposes</u>. Acceptable

provisions include reducing the required coincidence, defeating the control signals taken from the redundant channels, or initiating a protective action from the bypassed channel."

Channel 1	Channel 2	Channel 3	Channel 4
SRF	CC	BP	Operable
Without explicitly addressing the "provisions," the conditions of the first paragraph in the clause are **NOT** met if a channel is placed in bypass			

2.5 Bypassing Two Channels

Topical Report WCAP-17261-P/NP, Revision 0, proposes that two channels are allowed to be in bypass simultaneously for a limited amount of time.

Channel 1	Channel 2	Channel 3	Channel 4
SRF	CC	BP	BP
It is not clear how Clause 4.7.3 can be met under this proposal. Westinghouse should provide supplemental information demonstrating how these criteria are still met.			

EICB Question (2): Please describe how the proposed STS for Westinghouse designed plants would meet current regulatory requirements in IEEE Std. 279-1971 quoted above for each of the five conditions (2.1 – 2.5) postulated.

B. Probabilistic Risk Assessment Licensing Branch (APLA) Request for Supplemental Information

APLA Question (1): Regulatory Guides 1.174 and 1.177 consider the scope of evaluating the risk from all relevant hazards and modes of operation. Some of the proposed STS Conditions have an endstate of hot standby, hot shutdown, or cold shutdown.

a. Discuss the risk associated with a plant shutdown.

b. Discuss the risk associated with applicable modes other than mode 1 (which is included in TR WCAP-17261-P/NP) where the 24 hour completion time could apply.

APLA Question (2): Section 6.3.2 of Regulatory Guide 1.174 discusses cumulative risks. TR WCAP-17261-P/NP proposes risk increase associated with the reactor trip system and engineered safety features actuation signal channels. These systems have also been the subject of past TRs: WCAP-10271, WCAP-14333, and WCAP-15376. Please provide the calculated change in risk for each application (core damage frequency and large early release frequency).