RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

APR1400 Design Certification

Korea Electric Power Corporation / Korea Hydro & Nuclear Power Co., LTD

Docket No. 52-046

RAI No.: 38-7878

SRP Section: 07.05 - information Systems Important to Safety

Application Section: 7.5

Date of RAI Issued: 06/18/2015

Question No. 07.05-2

Clarify why the APR1400 has no Type A variables when there are manual actions described in FSAR Tier 2, Chapter 15 (e.g., manual actions for a steam generator tube rupture).

10 CFR Part 50, Appendix A, General Design Criteria 13, "Instrumentation and Controls," requires, in part, instrumentation to be provided to monitor variables and systems over their anticipated ranges for normal operation, anticipated operational occurrences, and accident conditions. Staff regulatory guidance RG 1.97, Rev. 4 endorses IEEE 497-2002. IEEE 497-2002, Section 4.1, states "Type A variables are those variables that provide the primary information required to permit the control room operating staff to:

a) Take specific planned manually-controlled actions for which no automatic control is provided and that are required for safety systems to perform their safety-related functions as assumed in the plant Accident Analysis Licensing Basis.

b) Take specific planned manually-controlled actions for which no automatic control is provided and that are required to mitigate the consequences of an AOO.

Type A variables provide information essential for the direct accomplishment of specific safety-related functions that require manual action. These variables are a subset of those necessary to implement the plant specific emergency procedure guidelines (EPGs) or the plant specific emergency operating procedures (EOPs) or the plant abnormal operating procedures (AOPs)."

Specifically, Section 15.6.3.1.1, states "After a reactor trip, the operator begins to cool down the hot leg temperature using the turbine bypass valves to the saturation temperature corresponding to the main steam safety valve (MSSV) opening setpoint. The operator then cools the nuclear steam supply system (NSSS) to shutdown cooling entry conditions using the unaffected SG after isolating the affected SG or verifying that it is isolated.

The analysis conservatively assumes that operator action is delayed until 30 minutes after initiation of the event." Therefore, it appears to the staff that manual actions are credited in the plant safety analysis to address a steam generator tube rupture, but there are no Type A variables to support such manual actions within the AMI variable list. Clarify why the APR1400 has no Type A variables, when there are manual actions described in APR1400 FSAR Tier 2, Chapter 15.

Response

The IEEE 497-2002 definition of Type A variables is used in determining Type A variables for the APR1400. The following process was used to screen manually controlled actions to determine if information required by the control room operating staff to perform the actions meets the definition of Type A variables.

All manually controlled actions performed by control room operating staff during Design Basis Events (DBEs) are identified to form the body of actions whose associated information might meet the definition of Type A variables. Manually controlled actions performed by control room operating staff which occur during Beyond DBEs and severe accidents are not included in the body of actions due to being outside the definition of Type A variables, as presented in IEEE 497-2002. Actions performed by control room operating staff on systems which have automatic control are then eliminated from the body of actions due to being explicitly excluded in the standard. Control room operator staff actions which manipulate non-safety systems and actions which are not planned as part of the control room operators' response to DBEs are eliminated from the body of actions. Finally, operator actions which manipulate safety systems for purposes other than accomplishing the system safety function are eliminated from the body of actions.

The result of evaluating manually controlled actions performed by control room operating staff in this manner is that no Type A variables exist for the APR1400.

For the Steam Generator Tube Rupture (SGTR) event, the DCD describes that the event can be stabilized by proper manual cooldown operation. Operator actions for the cooldown include 1) ensuring heat removal (SG cooling) and 2) termination of safety injection.

As described in DCD Section 15.6.3, heat removal is primarily performed by operation of the turbine bypass valves and by opening of atmospheric dump valves when the main steam isolation valves are closed. Operator action to maintain heat removal capability is performed according to the cooldown process which is not a safety function.

Termination of safety injection (SI) is needed to limit the break flow, and eventually to meet the radiation release requirement. However, termination of SI is not to accomplish the safety function of the safety injection system. The safety function of the safety injection system is to makeup RCS inventory.

Impact on DCD

There is no impact on the DCD.

Impact on PRA

There is no impact on the PRA.

Impact on Technical Specifications

There is no impact on the Technical Specifications.

Impact on Technical/Topical/Environmental Reports

There is no impact on any Technical, Topical or Environmental Report.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

APR1400 Design Certification

Korea Electric Power Corporation / Korea Hydro & Nuclear Power Co., LTD

Docket No. 52-046

RAI No.:	**38-7878**
SRP Section:	**07.05 – Information Systems Important to Safety**
Application Section:	**7.05**
Date of RAI Issue:	**06/18/2015**

Question No. 07.05-03

Clarify the classification of bypassed and inoperable status indication (BISI); whether it is safety-related or non-safety-related.

10 CFR 50.55a(h)(3) requires compliance to IEEE Std 603-1991. Clause 5.6.3.1(1) of IEEE Std 603-1991 specifies, in part, that interconnected equipment that is used for both safety and nonsafety functions shall be classified as part of the safety systems. RG 1.47 states the following:

"If the bypass and inoperable status indication is part of the safety systems, then the single-failure criterion of IEEE Std 603-1991, Section 5.1, would apply to the indication system."

"In addition to meeting the single-failure criterion, if the bypass and inoperable status indication is part of the safety systems, then maintaining independence between redundant portions of the safety system is essential to the effective use of the single-failure criterion."

"If a bypass and inoperable status indication is part of the safety systems, the equipment qualification criterion of IEEE Std 603-1991, Section 5.4, would apply to the indication system."

APR1400 FSAR, Tier 2, Section 7.5.1, states that BISI is one of the systems that is used in "(1) assessing plant conditions and safety system performance, (2) making decisions related to plant responses to abnormal events, and (3) taking preplanned manual operator actions related to accident mitigation." FSAR Tier 2, Section 7.5.1.3, does not specifically state if the BISI fully complies with RG 1.47 or just partially. Revise the APR1400 FSAR to clarify the safety classification of BISI and demonstrate how BISI conforms to RG 1.47. Identify all signal paths in and out of BISI to safety and non safety systems.

In addition, APR1400 FSAR, Tier 2, Section 7.5.1.3, states "The trip logic is converted from a 2-out-of-4 to a 2-out-of-3 logic for the parameters being bypassed, while maintaining a coincidence of two for actuation." Describe how the trip logic is converted from a 2-out-of-4 to a 2-out-of-3 logic for the parameters being bypassed, while maintaining a coincidence of two for actuation.

Response

The followings are described in this response:

1. Classification of bypassed and inoperable status indication (BISI)
2. Demonstration of how BISI conforms to RG 1.47
3. Identification of all signal paths in and out of BISI to safety and non-safety systems
4. Description of how the trip logic is converted from a 2-out-of-4 to a 2-out-of-3 logic for the parameters being bypassed, while maintaining a coincidence of two for actuation.

1. The bypassed and inoperable status indication (BISI) system is a non-safety system because it is not necessarily required to operate during design basis accident (DBA) conditions to mitigate the accidents. The safety classification of BISI is added in DCD Tier 2, Subsection 7.5.1.3, as indicated in the attachment associated with this response. BISI is implemented in the information processing system (IPS). The IPS displays BISI on the information flat panel display (IFPD) and large display panel (LDP).

2. The BISI is designed to meet the requirement of RG 1.47 as follows:

Positions 1 and 2

BISI automatically indicates bypass or inoperability of safety systems and auxiliary or supporting systems in accordance with RG 1.47. BISI, at a system level, provides a continuous indication of the bypassed or inoperable status of safety systems and auxiliary or supporting systems on the LDP. The system level BISI page is also displayed on the IFPD. The operating bypass and trip channel bypass statuses are indicated at the maintenance and test panel (MTP) in the instrumentation and control (I&C) equipment room and operator module (OM) and IFPD in the main control room.

For inoperable indication, the switch of each component provides indication of inoperable status on the ESF-CCS soft control module (ESCM) for safety-related components and on the IFPD for non-safety related components. The flashing inoperable indication goes to steady when inoperable pushbutton is operated and to off when the inoperable condition returns to normal.

BISI, at a system level, has dedicated bypass switches. When a component is in maintenance, the operator manually sets the bypass switches to bypass mode. After maintenance is complete, the operator manually returns the bypass switches to normal status.

Position 3

The self-test and self-diagnostics of the digital computer-based I&C safety systems are described in DCD Tier 2, Subsections 7.2.2.5 and 7.3.2.5. When the plant protection system (PPS) and engineered safety features - component control system (ESF-CCS) are undergoing testing or experiencing trouble, they are indicated on the IFPD.

Position 4

The BISI is implemented in the information processing system (IPS) as a part of systems. The IPS has several diagnostic tools available to determine the health of all servers and controllers on the DCN-I. The alarm server in the IPS allows for detecting and displaying abnormal conditions of system status as well as abnormal plant conditions on the IFPDs. The system status display shows detailed information about the status of the IPS servers. Therefore, the operator can acknowledge operable status of the BISI during normal operation.

Position 5

The BISI system receives the bypass and inoperable information from the ESF-CCS to provide the operator the following information to determine if continued reactor operation is permissible:

- ESF-CCS network failure by channel
- QIAS-N network failure
- MI switch operability by channel
- Status of each safety cabinet
- Status of each ESF-CCS controller
- Operability of each safety component

This BISI information is continuously displayed on the LDP and IFPD during normal and abnormal operation conditions.

Position 6

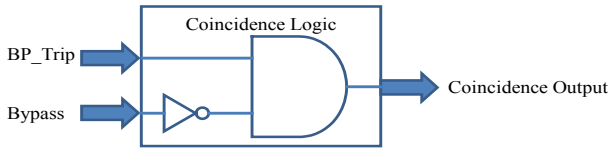
The BISI system only receives the bypassed and inoperable information from the safety systems through unidirectional communication and fiber optic isolation. No results from the BISI system are sent to the safety system for control and monitoring purposes. Therefore, any failures or mis-operation of the BISI system cannot adversely affect the performance of safety functions.

3. The PPS and the ESF-CCS, which are safety system, unidirectionally transmit BISI status to the IPS through the MTP and the distributed control system (DCS) gateway server. Fiber optic cable is used between the MTP and the DCS gateway server for electrical isolation. The P-CCS, which is a non-safety system, sends BISI status to the IPS. The IPS displays BISI on the IFPD and the LDP.

4. If one safety channel of the trip parameter is bypassed, then the 2-out-of-4 coincidence logic implemented in each LCL processor in all safety channels detects that safety channel of

the trip parameter as a bypassed channel and excludes the bypassed channel from the 2-out-of-4 coincidence logic.

If the bypassed channel is excluded from the 2-out-of-4 coincidence logic, then the 2-out-of-“4” coincidence logic automatically becomes 2-out-of-“3” coincidence logic because the bypassed channel is no longer contributing to the 2-out-of-4 coincidence logic for performing the proper safety function of the PPS. In other words, the LCL processors in the bypassed channel would ignore the valid trip signals coming from the bistable processors and output non-trip for the bypassed channel. See the following simplified coincidence logic diagram.



If one channel is in the channel bypass state (Bypass=TRUE), then the coincidence logic will generate FALSE as its coincidence output no matter what the BP_Trip status (FALSE or TRUE) is. This results in the 2-out-of-4 coincidence logic being converted to the 2-out-of-3 coincidence logic.

Impact on DCD

DCD Tier 2, Subsection 7.5.1.3 will be revised as indicated in the attachment associated with this response.

Impact on PRA

There is no impact on the PRA.

Impact on Technical Specifications

There is no impact on the Technical Specifications.

Impact on Technical /Topical/Environmental Reports.

There is no impact on any Technical, Topical, or Environmental Report.

The summary page includes the following information:

1) RCS/upper head saturation margin – the lower value of either the RCS saturation margin or upper head saturation margin

2) Reactor vessel level above the core

3) Representative core exit temperature

b. Backup ICC displays

The QIAS-P provides Class 1E backup displays for ICC variables, and is seismically and environmentally qualified. The displays of ICC variables are dedicated and integrated following the guidance of the Style Guide (Reference 6).

The QIAS-P displays are designed as follows:

1) To provide display of ICC variables

2) To provide indications in the event that the primary display becomes inoperable

3) To provide confirmatory indication to the primary display

The following information is available on the QIAS-P display pages:

1) RCS/Upper head saturation margin

2) Reactor vessel level above the core

3) Representative core exit temperature

7.5.1.3 Bypassed and Inoperable Status Indication

System-level automatic bypass indication is provided based on the guidance of NRC RG 1.47 (Reference 7). Compliance with NRC RG 1.47 is described as follows:

a. Flags are provided to indicate, at the system level, the bypass or deliberate inoperability of a protection system. The system-level alarms are actuated when a

The bypass and inoperable status indication (BISI) is a non-safety system because it is not required to operate during design basis accident (DBA) conditions to mitigate the accidents.