**GE Hitachi Nuclear Energy**

**Richard E. Kingston**
Vice President, ESBWR Licensing

P.O. Box 780 M/C A-65
Wilmington, NC 28402-0780
USA

T 910.675.6192
F 910.362.6192
rick.kingston@ge.com

MFN 10-304

Docket No. 52-010

October 11, 2010

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

Subject: **Transmittal of ESBWR DCD Tier 2, Chapter 7 Markups Related to GEH Internal Corrective Action**

The purpose of this letter is to submit markups to the ESBWR DCD, Tier 2, Chapter 7, which are the result of GEH internal review. These markups will be incorporated into the DCD, Revision 8. The markup pages are contained in Enclosure 1. Changes associated with this corrective action clarify the use of thermocouples versus temperature switches in some applications and typographical errors.

If you have any questions or require additional information, please contact me.

Sincerely,

Richard E. Kingston

Richard E. Kingston
Vice President, ESBWR Licensing

Enclosure:

1. Transmittal of ESBWR DCD Tier 2, Chapter 7 Markups Related to GEH Internal Corrective Action – DCD Markups

cc:

| | |
|---|---|
| AE Cubbage | USNRC (with enclosure) |
| JG Head | GEH/Wilmington (with enclosure) |
| DH Hinds | GEH/Wilmington (with enclosure) |
| PM Yandow | GEH/Wilmington (with enclosure) |
| eDRF Section | 0000-0124-1502 |
| | 0000-0123-2659 |

# Enclosure 1

# MFN 10-304

# Transmittal of ESBWR DCD Tier 2, Chapter 7 Markups Related to GEH Internal Corrective Action

# DCD Markups

Criterion 4.9 requires identification of the methods to be used to determine that the reliability of each safety system design is appropriate and any qualitative or quantitative reliability goals that may be imposed on the system design. The ESBWR Design Reliability Assurance Program (D-RAP) is a program utilized during detailed design and specific equipment selection phases to assure that the important ESBWR reliability assumptions of the Probabilistic Risk Assessment (PRA) are addressed throughout the plant life. The D-RAP is described in Section 17.4.

Criterion 4.10 requires identification of the critical points in time or the plant conditions, after the onset of a design basis event, including: (1) the point in time or plant conditions for which the protective actions of the safety system are initiated, (2) the point in time or plant conditions that define the proper completion of the safety function, (3) the point in time or the plant conditions that require automatic control of protective actions, and (4) the point in time or the plant conditions that allow returning a safety system to normal. The relevant points in time and plant conditions associated with each event, except for the allowable conditions for returning a plant to normal, are discussed in the relevant subsection describing the event as defined in Table 15.1-7. The allowable conditions for returning a plant to normal (i.e., return to service conditions) will be developed as part of the procedure development process described in Section 18.9.

Criterion 4.11 requires identification of the equipment protective provisions that prevent the safety systems from accomplishing their safety functions. The safety-related systems are designed to accomplish their safety-related functions in accordance with the single failure criterion, IEEE Std. 603, Section 5.1. Failure Modes and Effects Analyses (FMEAs) are performed on the safety-related system final design to ensure that no equipment protective provisions preclude correctly performing any safety-related function.

Criterion 4.12 requires identification of any other special design basis that may be imposed on the system design (e.g., diversity, interlocks, regulatory agency criteria). The design bases for each subsystem (including bases for diversity, interlocks, regulatory agency criteria) are identified within each applicable subsection of this chapter.

#### 7.1.6.6.1.2 Single Failure Criterion (IEEE Std. 603, Section 5.1)

The safety-related system designs are organized into four physically and electrically isolated divisions that use the principle of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally the design meets N-2 conditions (see Subsection 7.1.3.3.6).

The safety-related control systems include sufficient redundancy and independence to fulfill their intended safety function even when degraded by any single credible failure. The RTIF - NMS, SSLC/ESF, and ICP implement the single failure criterion of IEEE Std. 603 Section 5.1 using four independent and redundant divisions, which are provided in two-out-of-four trip logic. This ensures no single failure of or within any division prevents the system from performing its safety function or causing either an inadvertent reactor scram or an ECCS actuation. Redundancy begins with the sensors monitoring the variables and continues through the signal processing, output devices, and actuators.

Independence is implemented as described in Subsections 7.1.6.6.1.7 and 7.1.6.6.1.20.

Failure Modes and Effects Analyses (FMEAs) complying with IEEE Std. 379 are used to confirm the safety-related system designs' conformance to the single failure criterion.

~~inter-divisional.~~ The FMEA is consistent with the failure modes detectable by the self-diagnostic features of the hardware/software platforms and those detected by periodic surveillance.

Equipment is provided in accordance with a prescribed quality assurance program as described in Subsection 7.1.6.6.1.4.

#### 7.1.6.6.1.3 Completion of Protective Action (IEEE Std. 603, Sections 5.2 and 7.3)

After initiation by either automatic or manual means, the protective actions go to completion in conformance to IEEE Std. 603, Section 5.2. They go to completion by using one of the following: seal-in logic, non-resettable squib valves, manually reset valves, diverse functions, or a combination of logic, valves and functions. Deliberate operator action is required to reset the safety-related systems. Additionally, completion of protective actions for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).

#### 7.1.6.6.1.4 Quality (IEEE Std. 603, Section 5.3)

The Quality criterion requires that the Q-DCIS be consistent with minimum maintenance requirements and low failure rates and be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program. Q-DCIS meets this requirement through the application of the ESBWR Quality Assurance Program described in Chapter 17.

IEEE Std. 7-4.3.2 has additional quality assurance requirements related to software. Refer to LTRs "ESBWR - Software Management Program Manual" (Reference 7.1-12) and "ESBWR - Software Quality Assurance Program Manual" (Reference 7.1-10) for a description of the software plans that control the additional IEEE Std. 7-4.3.2 criteria related to the following hardware and software quality assurance requirements.

- IEEE Std. 7-4.3.2, Criterion 5.3.1, Software Development. The quality of software development activities is assured in accordance with the Software Quality Assurance Plan (SQAP).
- IEEE Std. 7-4.3.2, Criterion 5.3.2, Software Tools. Software tools are controlled in accordance with the Software Configuration Management Plan (SCMP).
- IEEE Std. 7-4.3.2, Criterion 5.3.3, Verification and Validation (V&V). Software V&V is performed in accordance with the Software V&V Plan (SVVP).
- IEEE Std. 7-4.3.2, Criterion 5.3.4, Independent V&V. Software Independent V&V is performed in accordance with the Software V&V Plan (SVVP).
- IEEE Std. 7-4.3.2, Criterion 5.3.5, Software Configuration Management. Software configuration is controlled in accordance with the Software Configuration Management Plan (SCMP).
- IEEE Std. 7-4.3.2, Criterion 5.3.6, Software Project Risk Management: Software project risk management is managed in accordance with the Software Management Plan (SMP).

Safety-related equipment is provided under the GEH 10 CFR 50, Appendix B Quality Assurance Program. The NRC accepted GEH Quality Assurance Program with its implementing procedures, constitutes the Quality Assurance system that is applied to the Q-DCIS design. It

- Prevent the inadvertent actuation of the deluge valves thus preventing inadvertent draining of the GDCS pools.
- Prevent any single control logic and instrumentation failure from inadvertently opening a GDCS injection valve or equalizing valve.
- Display GDCS valve positions and GDCS pool levels on the mimic on the WDP in the MCR.

#### 7.3.1.2.2 System Description

The GDCS system comprises the GDCS injection and equalization functions as well as the deluge subsystem. The injection and equalization functions are used to cool the core in the event of a LOCA. The deluge system is used to flood the containment floor in the event of a core breach.

The GDCS injection and equalization functions are implemented by four injection lines from the three GDCS pools to the RPV and four equalization lines from the suppression pool to the RPV. There are two valves on each injection line, with four squib initiators per valve (three divisional initiators and one from the DPS [see Section 7.8]), for a total of eight GDCS injection valves and 32 squib initiators. There is one squib valve on each of the four equalizing lines and four squib initiators per valve (three divisional initiators and one from the DPS [see Section 7.8]), for a total of four equalizing valves and 16 squib initiators. The equalizing valves are used after reactor core decay heat has boiled away sufficient vessel inventory added by the GDCS to again begin lowering the RPV water level. With three divisional initiators per valve, the system can be without two divisions of power and still perform its intended function.

The GDCS pools are located within the drywell at an elevation above the top of active fuel (TAF) and provide core cooling water by the force of gravity. The suppression pool is located within the drywell, with its equalization lines located above the TAF.

Safety-related and nonsafety-related sensors continuously monitor the GDCS pool water level. These values are continuously shown on the safety-related and nonsafety-related displays. Both high and low pool levels result in alarms from the PCF (part of N-DCIS).

The overall design of the system assures that, when needed, all eight injection valves and all four equalizing valves are fired - even with a complete failure of any two divisions. However, no squib is fired inadvertently as a result of any single failure.

**Automatic Operation**

Actuation of the GDCS injection function is performed automatically, without need for operator action. The signal to open the GDCS injection valves is given after a time delay (Table 7.3-4) When the RPV water level drops below Level 1 sustained for 10 seconds, the GDCS time delay is initiated. For certain LOCA events where RPV water level does not drop below Level 1, GDCS injection valve time delay is also initiated on drywell pressure high signal, sustained for 60-minutes. With three divisional initiators per valve, the system can tolerate the complete loss of two divisions of power (one in bypass and one failure) and still perform its intended function.

Actuation of the GDCS equalizing function is performed automatically, without need for operator action. The GDCS equalizing valves initiation occurs automatically following a sustained RPV Level 1 signal, for 10 seconds, plus Table 7.3-4 time delay, and only after the

RPV water level decreases below RPV Level 0.5 (1m above TAF). This action results in the actuation of the four equalizing squib valves mounted on the suppression pool equalizing lines. With three divisional initiators per valve, the system can tolerate the complete loss of two divisions (one bypass and one failure) of power and still perform its intended function.

GDCS injection and equalize subsystem initiation is inhibited automatically under ATWS conditions as described in Subsection 7.8.1.1.1.2.

**Manual Operation**

Each safety-related VDU provides a display with an "arm/fire" switch (one per division, for a total of four) to manually initiate the GDCS sequence as a system. If the operator uses any two of the four switches, the GDCS sequence seals in and starts the GDCS valve sequencing. This manual actuation also is interlocked with RPV pressure. This requires four deliberate (two-arm and two-fire) operator actions. For all of the manual initiations, operator use of the "arm" portion of the display triggers a plant alarm.

The safety-related VDUs in the MCR provide a display format allowing the operator to manually open each GDCS injection valve independently, using the primary SSLC/ESF logic function. Likewise, each nonsafety-related VDU in the MCR provides a display format allowing the operator to individually open each GDCS injection valve independently, using the DPS logic function. Each display uses an "arm/fire" configuration (interlocked with a low reactor pressure signal) requiring at least two deliberate operator actions. Operator use of the "arm" portion of the display triggers a plant alarm. The two manual opening schemes from the SSLC/ESF (primary) and the DPS (backup) are diverse.

In addition the safety-related VDUs in the MCR provide a display format allowing the operator manually to open each GDCS equalizing valve independently, using the primary SSLC/ESF logic function. Likewise, each nonsafety-related VDU in the MCR provides a display format allowing the operator to individually open each GDCS equalizing valve independently, using the DPS logic function. Each display uses an "arm/fire" configuration requiring at least two deliberate operator actions (interlocked with a low reactor pressure signal). Operator use of the "arm" portion of the display triggers a plant alarm. The two manual opening schemes from the SSLC/ESF (primary) and the DPS (backup) are diverse.

**Actuation Logic**

The logic elements providing controls for the actuation of the GDCS injection and equalizing squib valves are contained in the SSLC/ESF platform within Q-DCIS, outside the drywell containment. The RPV water level sensors and the drywell pressure sensors used to initiate GDCS, are located on racks outside the drywell.

The GDCS injection and equalizing valve logic includes the SSLC/ESF "division of sensors" bypass switch, two-out-of-four trip decisions, and single failure proof actuation logic - with any three of the four divisions of safety-related power available. The valve logic also is single failure proof against inadvertent actuation, meaning each division of logic has three load drivers each of which must operate for the associated squib valves to fire.

The wide range level and drywell pressure sensors that are used for the ADS logic and fuel zone range RPV water level sensors are also used for the GDCS equalizing valve logic; these are

separate and independent from the sensors used for RPS functions and diverse from those used by the DPS. Both sets of RPV water level sensors belong to the NBS.

The generation of the RPV-Level 1 or Drywell Pressure High signal for the GDCS is described above (Automatic Operation). The logic for all squib initiators is similar. The signals are acquired per division by RMUs of the same division. The data are sent via fiber-optic cables to the SSLC/ESF cabinets located in the corresponding divisional I&C equipment rooms in the Control Building (CB). Each division's logic compares the measured parameters to setpoints. If the measured parameter is at or past the setpoint, a divisional sensor trip is generated and sent both to its own division and to each of the other divisions by appropriately isolated fiber-optic cables.

Each division has access to all four divisional sensor trip signals, and performs a redundant two-out-of-four vote on the four sensor trip signals. (The vote is two-out-of-three if one division is bypassed, because no more than one division can be bypassed at any one time.)

Each division uses triply redundant logic to perform the two-out-of-four vote on the four divisional sensor trip signals. The effect is that any two divisions sensing the appropriate trip conditions results in all divisions providing a trip signal.

The existence of the multiple logic trips per division is necessitated by the requirement that no injection or equalizing squib valve inadvertently be fired as the result of a single failure.

For the eight GDCS injection squib valves logic, when a sustained RPV Level 1 is detected for 10 seconds or a sustained Drywell Pressure High is detected for 60 minutes, adjustable timers will be activated at a preset time delay (as specified in Table 7.3-4). After the time delay, a trip signal is output to the GDCS squib load drivers/discrete outputs. There are eight injection squib valves, each with three divisional squib initiators, and one DPS squib initiator.

Within the RMU, for each equalizing valve squib initiator, there is a series circuit of divisional power, three load drivers/discrete outputs in series, a current monitor, and a normally closed disable/test switch. The SSLC/ESF triply redundant ~~logic in the main SSLC/ESF~~ controller application processors must transmit separate close signals to each of the three load driver/discrete outputs. The effect is that two of the three triply redundant controller application processors must separately command all of the load drivers/discrete outputs to fire the divisional squib initiator, making the design single failure proof against inadvertent actuation. Because each GDCS injection squib valve has three squib initiators, powered by three different divisions, the design is also single failure proof if required to operate all eight valves, and even will initiate with the loss of two divisions of power.

The current monitor continuously verifies squib electrical continuity, and the disable/test switch is used when performing maintenance or surveillance testing, or testing the current monitor. If the disable/test switch opens the circuit, an alarm signal is sent to the MCR, indicating that the squib initiator (not the valve) is inoperable.

For diversity, the DPS also is able to fire its squib electrical initiator on each of the eight GDCS injection squib valves, using single failure proof logic (both to operate and to avoid inadvertent operation). This is accomplished using a completely separate squib initiator connected to the DPS system (see Figures 7.3-1b 1and 7.3-1c). The DPS system uses diverse (from the

SSLC/ESF) sensors, hardware, and software to operate the GDCS injection valves. Figure 7.3-2 shows the initiation logic of a typical equalizing squib valve.

Within the RMU, for each squib initiator, there is a series circuit of divisional power, three load drivers/discrete outputs in series, a current monitor, and a normally closed disable/test switch. To fire the equalizing valve squib initiator, the triply redundant logic in the SSLC/ESF must time out the post GDCS initiation signal permissive, acquire at least two of four fuel zone range signals, determine that the measured value is at or below Level .5 and two-out-of-four vote the resulting divisional sensor trips and transmit separate close signals to each of the three load driver/discrete outputs. The effect is that two of the three triply redundant controller application processors must separately command all of the load drivers/discrete outputs to fire the divisional squib initiator, making the design single failure proof against inadvertent actuation.

Because each equalizing valve has three divisional squib initiators powered by three different divisions, the design is also single failure proof whenever required to operate all four valves, with any three of the four divisions of safety-related power available. The equalizing valves are needed for the long term, so they are not automatically operated by the DPS system. The equalizing valves are included in the manually initiated GDCS valve logic, and also have capability to be fired individually from safety-related VDU displays or nonsafety-related VDU displays.

**Deluge System**

The severe accident deluge system (GDCS subsystem) is designed to flood the containment floor in the event of a core breach that results in molten fuel on the containment floor. This system is made up of two individual and identical trains both of which contain an automatic actuation and manual actuation ability. There are 12 deluge valves each with four squib initiators (each valve train has a manual and automatic initiator). Each of these valves feeds the Basemat-Internal Melt Arrest Coolability (BiMAC) deluge system, which floods the containment floor following a severe accident. The BiMAC system is described in more detail in Subsection 6.2.1. The logic for the deluge valves is executed in a pair of dedicated nonsafety-related PLCs driver by nonsafety-related thermocouples in the drywell floor.~~and a pair of dedicated safety-related temperature switches~~.

Automatic actuation of the deluge valves is accomplished in concert with lower drywell high temperature. The containment floor area is divided into 30 cells, with two thermocouples installed in each cell. One thermocouple from each cell is monitored in one PLC, while the other thermocouple from each cell is monitored in a second PLC. When measured temperatures exceed the setpoint (see Table 7.3-4) at one set of thermocouples coincident with setpoints being exceeded at a second set of thermocouples in an adjacent cell, a trip signal is generated in each PLC.

The trip signal in each PLC starts an adjustable deluge squib valve non-bypassable timer. At the end of the deluge squib valve set time delay, each of the two timers outputs a trip signal to the respective deluge valve squib load driver/discrete output. The timer outputs are wired in series so each of the two timers must transmit a temperature trip signal to the corresponding series load driver/discrete output. Additionally, a pair of dedicated safety-related temperature switches monitor the drywell temperature below the RPV. Each temperature switch uses a capillary and bulb action to close a contact wired in series with the PLC timer outputs. The effect is that both

PLC timer outputs and both temperature switch outputs must operate to fire the squib initiator. The temperature switches serve as power permissives for the deluge ~~logic~~system squib initiated deluge valves. These temperature switches are safety-related to prevent inadvertent actuation of the deluge system, which could needlessly drain the GDCS pools.

An additional function of the PLC logic is to initiate operation of battery powered ignitors in the PCCS heat exchangers to prevent the accumulation of explosive mixtures of hydrogen (generated from the interaction with zircalloy) and oxygen (concrete containment floor) associated with the severe accident/core breach while the containment is at a high pressure. The ignitors will be pulsed at an appropriate rate after deluge system initiation and are powered from the same batteres that power the squib ignitors on the GDCS deluge valves. The severe accident deluge system is appropriate for this function since the PCCS heat exchangers are designed to withstand hydrogen/oxygen explosions at containment pressures associated with design basis accidents.

The deluge logic implemented in PLC is completely separate from and independent of the Q-DCIS and the N-DCIS, and is powered by dedicated pair of batteries supported by battery chargers operating on nonsafety-related power. In the event that this nonsafety-related primary electrical power is lost, deluge logic power is supplied from dedicated batteries for 72 hours. The deluge valves and PCCS ignitors are also ~~are~~ powered by a pair of dedicated batteries supported by battery chargers operating on nonsafety-related power. In the event that this nonsafety-related power is lost, deluge valve and ignitor power is supplied from each pair of dedicated batteries for 72 hours.

The batteries for the deluge valves and ignitor are separate from and independent of the batteries for the deluge logic. Each of these batteries can fire all 12 deluge valve squibs and operate the PCCS ignitors. All of the deluge valve/ignitor batteries are separate from and independent of the other plant batteries.

The logic elements providing the controls for the actuation of the deluge valves and ignitors are contained within a separate pair of dedicated nonsafety-related PLCs and a pair of dedicated safety-related temperature switches. The only safety-related function of the deluge and ignitor logic is prevention of inadvertent actuation. The deluge logic is independent from all the other plant controls, and also is located outside containment.

Temperature indications and alarms, as well as continuity alarms and valve open/close indications for each squib valve are available in the MCR. Each valve has a normally closed disable/test switch available for maintenance purposes.

Two control switches are furnished in the MCR, to allow the operator manually to open the 12 deluge valves. These switches are of the “arm/fire” type, and are wired in series such that four deliberate operator actions (two for “arm” and two for “fire”) and the safety-related temperature switches located under the RPV are required to operate the valves. These switches actuate the squib initiator on each deluge valve. A similar pair of MCR switches is used for manual initiation of the PCCS ignitors. Operator use of the “arm” portion of the switch triggers a plant alarm in the PCF.