GE Energy

David H. Hinds
Manager, ESBWR

PO Box 780 M/C L60
Wilmington, NC 28402-0780
USA

T 910 675 6363
F 910 362 6363
david.hinds@ge.com

MFN 06-067 Docket No. 52-010

March 2, 2006

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

Subject: **Partial Response to NRC Request for Additional Information Letter No. 6 for the ESBWR Design Certification Application – Instrumentation and Control Systems – RAI Number 7.2-3**

Enclosure 1 contains GE's response to the subject NRC RAI transmitted via the Reference 1 letter. As indicated in the Reference 1 letter, GE had agreed to respond to RAIs 14.3-2 and 14.3-3, which relate to Tier 1, by the end of February 2006. We are currently in the process of finalizing Tier 1, Revision 1, and believe it will be more effective to delay these RAI responses until Tier 1, Revision 1 has been submitted.

If you have any questions about the information provided here, please let me know.

Sincerely,

David H. Hinds
Manager, ESBWR

General Electric Company

D068

Reference:

1. MFN 06-045, Letter from U.S. Nuclear Regulatory Commission to David Hinds, *Request for Additional Information Letter No. 6 Related to ESBWR Design Certification Application,* January 31, 2006

Enclosure:

1. MFN 06-067 – Partial Response to NRC Request for Additional Information Letter No. 6 for the ESBWR Design Certification Application – Instrumentation and Control Systems – RAI Number 7.2-3

| | | |
|---|---|---|
| cc: | WD Beckner | USNRC (w/o enclosures) |
| | AE Cubbage | USNRC (with enclosures) |
| | LA Dudes | USNRC (w/o enclosures) |
| | GB Stramback | GE/San Jose (with enclosures) |
| | eDRF | 0000-0051-5130 |

# ENCLOSURE 1

# MFN 06-067

# Partial Response to NRC Request for Additional Information Letter No. 6 for the ESBWR Design Certification Application Instrumentation and Control Systems - RAI Number 7.2-3

NRC RAI 7.2-3

*Provide detailed information and design basis on the RPS bypass provisions. The DCD states that the RPS includes two possible operator controlled bypasses. These are independently controlled by separate fiber optic "joystick" switches. Provide detailed information and the design basis of these bypass provisions.*

GE Response:

Background

The reactor protection system (RPS) is a hardware/software subfunction of safety system logic and control (SSLC) which is, in turn a subfunction of the essential distributed control and information system (E-DCIS); the general arrangement is shown in the attached Figure XX. The RPS controllers/logic are located in a cabinet (one per division in separate EDCIS rooms) that combines the RPS, LDIS (for MSIVs and drains only) and ATWS/SLCS functions; the cabinet is called the reactor trip and isolation function (RTIF) cabinet. Although all equipment located in the RTIF cabinet is appropriate for it's respective division and everything in the cabinet is powered by the appropriate divisional power (R13, R14, and R16), the ATWS/SLCS function is segregated to a separate chassis in the cabinet and does not use programmable logic, which is different from the rest of the equipment in the cabinet.

The ESBWR RPS design has several important differences from existing BWR scram logic and hardware (although many of these features were included in the approved ABWR design); these include:

Per parameter trip (specifically there must be (for example) two unbypassed level trips to scram; a single pressure trip and a single level trip will not cause a scram)

No operator manipulation of the division of sensors and/or division of logic bypass, nor any operation of the RPS back panel inop switches can reduce scram logic redundancy to less than – any two unbypassed same parameters can cause a trip and scram. Only one division at a time can be physically bypassed.

All communication with non-safety DCIS is one way through fiber optic isolation; the loss of this communication will not affect RPS functioning

All communication with other RPS divisions is one way and fiber optic isolated

Because all signals are actively transported, "fail safe" is not a "1" or a "0" but rather "trip on loss of communication". As a result loss of communication from another division is interpreted as a trip (unless that division is bypassed) and loss of communication with a bypass joystick switch is interpreted as "no bypass".

All RPS logic is powered redundantly with R13 and R14; R16 is used for the backup scram logic/solenoids.

The HCU solenoid power is provided locally in the reactor building and is switched (on or off) by the fiber optic driven 2/4 logic from the RPS (RTIF) cabinet in the control building. This configuration avoids the long distance voltage drops to the HCU solenoids in the old design and eliminates (along with using monitored, safety related inverters for solenoid power) the need for EPAs. Loss of communication from the control building RTIF cabinets is interpreted as a trip.

The hardware, software and solenoid switching for the RPS system is both diverse and separate from the DPS (diverse protection system).

All four divisions of RPS power, sensor wiring and fiber optics are physically separate from the other RPS divisions and further the four scram groups supplying power to the HCU solenoids in division 1 and 2 are separated from each other. The four divisions of RPS sensors from the turbine and electrical buildings (including, for example, condenser vacuum and 13.8 kv bus voltage) are hardwired via separate conduits/raceways to the corresponding divisional RTIF cabinet in the control building. There is no connection to the non-safety DCIS other than through one-way fiber optics, nor is there connection to other RPS divisions except through fiber optics.

Discussion including bypasses

Finally, per division there is a "arm/fire" manual scram pushbutton switch that acts like a sensor input to RPS; if any two are actuated simultaneously, the reactor will scram using the RPS logic. Additionally there is one manual scram pushbutton in each division (division 1 and division 2) that when operated, directly open the current to the HCU scram solenoids. If these two pushbuttons are operated simultaneously, the reactor will scram in a way that completely bypasses the RPS logic. These features are in addition to the scram initiated from the diverse protection system logic and from the backup scram and the scram follow "scram" initiated from the RPS logic. The backup scram removes air from the scram solenoids whether or not the scram solenoids function, and the scram follow logic causes all of the FMCRD control rods to insert (as long as diesel or offsite power is available) using their motors, regardless of the (automatic/semiautomatic/manual) status of the RCIS system or any existing operator insert/withdraw command.

The attached Figure YY further details the division of sensors and division of logic bypass arrangements. The various sensors used for RPS (and LDIS) trips are input per division either to the reactor building remote multiplexers or hardwired from the turbine and electrical building; there are always four redundant sensors. Next in the signal path is the digital trip function where the discrete or analog RPS signals are compared to their trip setpoints. The trip decisions (and parameter values for monitoring) are sent to the other three divisions of RPS such that each RPS division can make a 2/4 per parameter trip decision. Included in this decision is the divisional bypass of sensors information

coming from the single joystick fiber optic switch on the main control console in the control room, which allows only one division of bypass at a time. Therefore, the actual output is "any two like unbypassed parameters exceeding their limits = trip". As previously described, loss of fiber optics communication from other divisions is interpreted as a "trip" and loss of fiber optics communication from the bypass of sensors switch is interpreted as "no bypass"; no RPS division is dependent on any other division for its trip decision.

At this level of logic, the trips from the neutron monitoring system (NMS) are input via one-way fiber from the NMS system in the same division; these APRM/SRNM trips have their own 2/4 logic and bypasses.

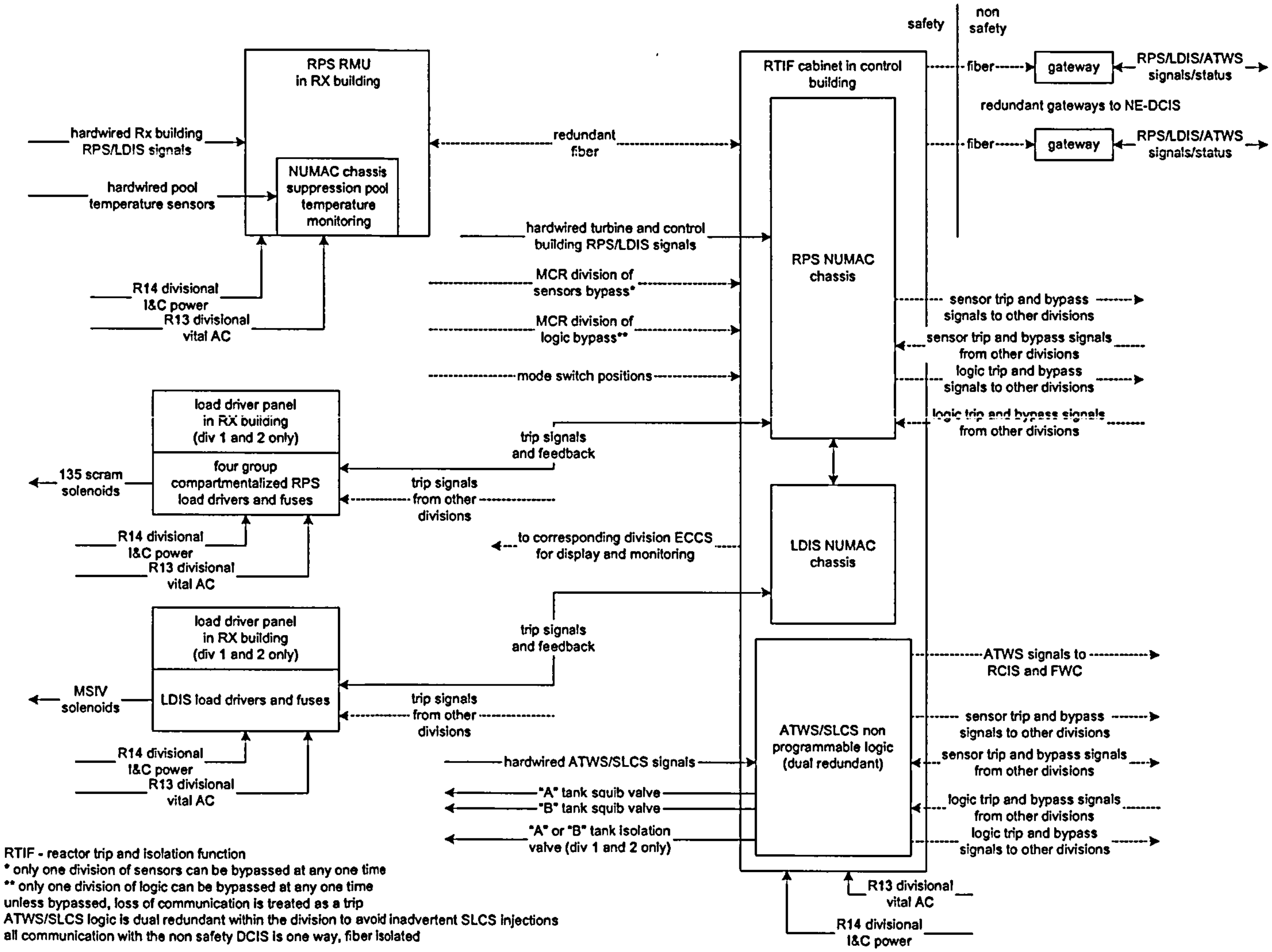
As described for other trip functions, the per division trip decision is shared with the other divisions at the output logic function level and the RPS load driver level (physically located in the reactor building) where it is voted on with 2/4 logic. These decisions include the divisional bypass of logic information coming from another single joystick fiber optic switch on the main control console, such that only one division can be bypassed at a time. The same loss of communication rules apply, so that the load driver output (to the HCU solenoids) can reflect a scram decision from any two unbypassed logics.

Note specifically that, even if any division of sensors has been bypassed, each of the four RPS divisions can still make a 2/4 (2/3) trip decision and even if any division of logic has been bypassed, each of the load drivers can still make a 2/4 (2/3) scram decision. There is no way that the RPS logic can ever be degraded to less than required by IEEE 279, specifically 2 out of 4 unbypassed like parameters exceeding their limits will always cause a scram.

The design basis for the bypass switches is to allow sensor calibration and/or hardware troubleshooting while completely eliminating their potential from causing a scram; however unlikely the chance that another parameter/logic would fail simultaneously.

Finally, although not shown in the attached drawings and not an operator function, the RPS hardware in the back panel area (four separate divisional EDCIS rooms) includes keylock switches to render the instruments "inop" (this is enforced for maintenance and calibration). Unless the appropriate division of logic bypass has been set, this will be interpreted as a trip; although it is physically possible to inop more than one division at a time (this is administratively controlled), should more than one division be inop'd without bypass, the reactor will scram.

Figure XX ESBWR E-DCIS (C63) - RPS/LDIS/ATWS SLCS SSLC - typical of four divisions




RTIF - reactor trip and isolation function
* only one division of sensors can be bypassed at any one time
** only one division of logic can be bypassed at any one time
unless bypassed, loss of communication is treated as a trip
ATWS/SLCS logic is dual redundant within the division to avoid inadvertent SLCS injections
all communication with the non safety DCIS is one way, fiber isolated

Figure YY ESBWR RPS/LDIS (div 1 - typical of 4 divisions)