December 18, 1984

Docket No. ~~00007447~~ 50-447

Dr. Glenn G. Sherwood, Manager
Safety & Licensing Operations
Nuclear Power Systems Division
General Electric Company
175 Curtner Avenue, Mail Code 682
San Jose, California 95125

Dear Dr. Sherwood:

SUBJECT: DRAFT SER ON THE SAFETY PARAMETER DISPLAY SYSTEM FOR GESSAR II

Enclosed is a copy of the staff's safety evaluation related to the SPDS proposed for GESSAR II. Please review the safety evaluation and provide us with a schedule for responding to the open items addressed in the report. This schedule should be provided to the staff by December 31, 1984.

A copy of this report has been placed in the Commission's Public Document Room. If you should have any questions related to this request, please contact Dino Scaletti at (301) 492-9787,

Sincerely,

Original signed by
Cecil O. Thomas, Chief
Standardization and Special
Projects Branch
Division of Licensing

Enclosure:
As stated

DISTRIBUTION
Docket File
NRC PDR
SSPB/Reading file
DScaletti
PAnderson
CThomas
OELD
EWeinkan
LBeltracchi
JJoyce
GDick
MMcCoy
JCostello, I&E

DL:SSPB	DL:SSPB	DL:SSPB
DScaletti:ac	PAnderson	CThomas
12/18/84	12/18/84	12/18/84

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

December 18, 1984

Docket No. 00007447

Dr. Glenn G. Sherwood, Manager
Safety & Licensing Operations
Nuclear Power Systems Division
General Electric Company
175 Curtner Avenue, Mail Code 682
San Jose, California 95125

Dear Dr. Sherwood:

SUBJECT: DRAFT SER ON THE SAFETY PARAMETER DISPLAY SYSTEM FOR GESSAR II

Enclosed is a copy of the staff's safety evaluation related to the SPDS proposed for GESSAR II. Please review the safety evaluation and provide us with a schedule for responding to the open items addressed in the report. This schedule should be provided to the staff by December 31, 1984.

A copy of this report has been placed in the Commission's Public Document Room. If you should have any questions related to this request, please contact Dino Scaletti at (301) 492-9787,

Sincerely,

Cecil O. Thomas

Cecil O. Thomas, Chief
Standardization and Special
Projects Branch
Division of Licensing

Enclosure:
As stated

DRAFT INPUT

SAFETY EVALUATION REPORT FOR THE

GENERAL ELECTRIC COMPANY'S GESSAR II

SAFETY PARAMETER DISPLAY SYSTEM

I. INTRODUCTION AND BACKGROUND

All holders of operating licenses issued by the Nuclear Regulatory Commission (licensees) and applicants for an operating license (OL) must provide a Safety Parameter Display System (SPDS) in the control room of their plant. The Commission approved requirements for the SPDS are defined in Supplement 1 to NUREG-0737.

The purpose of the SPDS is to provide a concise display of critical plant variables to control room operators to aid them in rapidly and reliably determining the safety status of the plant. NUREG-0737, Supplement 1 requires licensees and applicants to prepare a written safety analysis describing the basis on which the selected plant variables are sufficient to assess the safety status of each identified function for a wide range of events, which include symptoms of severe accidents. Licensees and applicants shall also prepare an Implementation Plan for the SPDS which contains schedules for design, development, installation, and full operation of the SPDS as well as a design Verification and Validation Plan. The Safety Analysis and the Implementation Plan are to be submitted to the NRC for staff review. The results from the staff's review are to be published in a Safety Evaluation Report (SER).

The GESSAR II SPDS is described in NEDE-30284-P (Ref. 1), a proprietary topical report submitted by General Electric for staff review. The staff met with General Electric to discuss this report and minutes from this meeting are reported in Reference 2. A design verification audit of the display system was conducted during July 24-27, 1984, and the results from this audit are presented in Reference 3. This SER serves to document the staff's evaluation of this system to date. A supplement to this SER will be issued when the staff's review of this system is completed.

II. SUMMARY

The staff audited and reviewed General Electric's design for the GESSAR II SPDS and concludes it is acceptable for the vendor to continue implementing its SPDS Program, but the open items defined in this report must be successfully resolved by General Electric. Licensees and applicants who install a General Electric GESSAR II SPDS may reference this SER in their submittal.

III. EVALUATION

The staff evaluated the topical report, NEDE-30284-P (Ref. 1) and considered the audit results in the preparation of this SER. The staff's evaluation considered the design process, the Verification and Validation Plan used in the design, the basis for plant variables selected for display, the methods used to validate data prior to its display, the human factors program used in the design of display

formats, and the qualification of the electrical and electronic isolation devices used in the system.

A. SPDS DESCRIPTION

General Electric has developed an Emergency Response Information System (ERIS), a display system which contains the SPDS function. ERIS is a computer-based system and consists of three subsystems which are a Data Acquisition System (DAS), a Data Processing System (DPS), and Data Output Peripherals (DOP). The Data Acquisition System gathers plant signals and converts these signals into a form usable by a digital computer. The Data Processing System prepares the signals for display upon CRTs and also stores the processed signals for later use. The Data Output Peripherals contain CRTs for the display of plant data. Keyboards are also provided as an operator interface to the display system.

General Electric stated that ERIS is based upon the symptom oriented Emergency Procedure Guidelines (EPGs). In the control room, ERIS assists the operating personnel in their assigned functions by displaying the following information on CRTs:

- Real-time plant status to aid in early emergency procedure entry condition recognition. These data may be displayed

continuously and are monitored by control room operators during normal operations,

- Data to assist the operator in following the emergency procedures (including current readings, trends of process variables, and status of major systems),

- Two-dimensional limits of process variables as defined in the emergency procedures. This assists the operator by precluding the need to perform manual calculations to determine margins to limits.

- Critical process variable validation status,

- Critical process variable trend plots.

B. DESIGN PROCESS

During the Design Verification Audit of the SPDS (Ref. 3), the staff evaluated the process used by General Electric to develop the system. We evaluated a Software Engineering Manual which contained guidelines on how to structure and document the design. We also evaluated specifications of functional requirements, specifications of software requirements for the Real Time Analysis and Display Processor, which is a key processor within the system. Further, we evaluated appendices

to the specifications and found guidelines on the use of color codes and on text abbreviations.

The staff found the Software Engineering Manual to be comprehensive in scope and to cover all phases of the software life cycle from the plan phase, to development, and to maintenance. We found the technical content of the specifications and appendices to be appropriate for the design of the display system. We also found the structure of the specifications responsive to the guidelines stated in the Software Engineering Manual. Based on the results from the staff's audit of the Software Engineering Manual and of the design specifications, we find the process used by General Electric in the design of the SPDS acceptable for the development of the system.

The staff also evaluated the display's design for provisions which allow for expansion of the system to accommodate future revisions to the Emergency Procedure Guidelines. We found the design of the display system to be modular in form, with provisions for the addition of future modules. We found the display's design to contain provisions to add modules for data acquisition functions, increased data storage, and new display formats. General Electric also stated that the design goal's maximum duty cycle for the Real Time Analysis and Display

Processor is 30 percent. Based on these data, the staff concludes that the design does provide provisions for the future expansion of the display system.

C. VERIFICATION AND VALIDATION PROGRAM

During the Design Verification Audit of the SPDS (Ref. 3), the staff evaluated the Verification and Validation Program (V&V) used by General Electric in the design of the system. General Electric described the V&V Program and stated that it was patterned after NSAC-39 (Ref. 4). In the program, a typical design verification activity consisted of a review of requirements on interface and interaction needs. A typical design validation activity consisted of test and evaluation of the integrated hardware/software system. The staff evaluated these data and concluded that the General Electric Verification and Validation Program is similar to the one described in NSAC-39 and it is acceptable for the development of an SPDS.

In evaluating the application of the V&V Program, we found that General Electric was able to demonstrate how staff selected problems, wherein the problems were defined in previous verification activities, were documented and adequately resolved. In evaluating the ERIS Validation and Test Requirement Document, the staff did successfully correlate test requirements with the functional requirements of the design. We

also learned that Validation Test Procedures are currently being prepared by General Electric. Based on the review of the V&V activities performed to date, the staff concludes that the V&V Program is being effectively applied.

The Validation Test for ERIS are to be conducted late this year (1984) with a test report on results due by February 1985. Based on the scope of the design verification audit, the staff concludes a design validation audit of General Electric's Generic SPDS is not necessary provided the following reports are submitted for staff review:

- A sample of test procedures with acceptance criteria for test runs,

- the Validation Test Report,

- a summary of the problems found during the tests and how they were resolved.

Upon completion of the staff's review of the reports, the results from the evaluation will be documented in a supplemental SER.

D. PROCESS VARIABLE SELECTION

Section 4.1(f) of Supplement 1 to NUREG-0737 states that:

"The minimum information to be provided shall be sufficient to provide information to plant operators about:

(i) Reactivity Control

(ii) Reactor core cooling and heat removal from the primary system

(iii) Reactor coolant system integrity

(iv) Radioactivity control

(v) Containment conditions."

For review purposes, these five items have been designated as Critical Safety Functions.

The selection of the SPDS process variables for display was made by GE based on the BWR generic Emergency Procedure Guidelines (EPGs) (Ref. 5). We have confirmed that the variables selected are consistent with the presently approved BWR EPGs (Revision 3) with one exception. Revision 3 contains a Radioactivity Release Control Guideline which contains an Entry Condition based on off-site radioactivity release rate. The GE basic SPDS display does not contain a monitored variable dealing directly with radiation measurement.

The SPDS variables and their relationship to the Critical Safety Functions are summarized in the attached Table 1. The grouping was made by the staff based on inspection of the first level SPDS display format and information furnished by GE at the Design Verification Audit. GE has grouped the individual variables to coordinate with the generic EPGs which include separate sequential procedural steps identified under the general functions of Reactor Pressure Vessel Control and Containment Control. These individual groups of variables are used for second-level display formats on the GE SPDS.

General Electric has taken the position that the Critical Safety Function Radioactivity Control is adequately covered by variables on second-level displays. We understand that optional enhanced display formats are available for purchase which include displays for process radiation, reactor building radiation and vent and exhaust radiation. We would find the SPDS variable selection acceptable for Radiation Control if these display formats were included.

Neutron flux is a fundamental variable for monitoring the status of the Reactivity Control Critical Safety Function. An indication of reactivity control should be provided for all power ranges. The GE SPDS provides monitoring of the power level by Average Power Range Monitors (APRMs) during powe

operation. For conditions below the APRM range, the GE SPDS does not monitor power level, but does provide scram status. GE has stated that the combination of power level and scram status is sufficient for monitoring the Reactivity Control Critical Safety Function. Following a reactor scram and a core-wide verification of rods-in status, the scram-status indicator on the SPDS will display "rods in." This display message will not change unless a rod is withdrawn or drifting in which case the data changes to an alarm (red) indication. Also, in the startup mode, the Intermediate Range Monitor (IRM) upscale trip results in a rod-withdraw block which will result in a scram displayed on the SPDS if a high-high setpoint (>120/125 of scale) is exceeded. During some plant conditions, such as performance of core alterations (e.g., fuel loading), if a signal from the neutron monitoring system exceeds a Source Range Monitor (SRM) high-high setpoint, this condition would be indicated on the SPDS scram-status indicator (Ref. 7). The staff concludes that since the scram signals are directed to the SPDS display, the combination of the APRMs and scram-status indicator provides adequate monitoring of the Reactivity Control Critical Safety Function. The staff also recognizes that during periods of startup and heatup, a portion of the plant operations staff would have attention focused on the neutron instrumentation in the control room.

We have verified that the GE ERIS design includes sufficient capability for expanding the system so that additional variables (such as hydrogen concentration) may be added as a result of future revisions to the generic EPGs.

The staff finds that the variables selected for the GE SPDS would be acceptable with the addition of radiation monitors to identify the status of the Radioactivity Control Safety Function.

E. DISPLAY DATA VALIDATION

The staff reviewed General Electric's SPDS design to determine that means are provided in the display's design to assure that the data displayed are valid. The staff audited the SPDS design and found that the top level display format of critical plant variables contains each plant variable used as an entry variable to the Emergency Operation Procedures. These data were presented as numerical data enclosed by a color coded status box. The code of the status box informs the operator on the validation status of the enclosed data.

As part of the real time processing of the data, the ERIS/SPDS performs the following checks on analog and digital input signals: redundancy, range check, zero adjust, density

correction, reference leg boiling, temperature compensation and instrument power as a means of data validation. Furthermore, secordary display formats which contained detailed data on the intermediate steps of the data validation process were available for each entry variable to the Emergency Operations Procedures. Properly implemented in a plant, the staff believes this intermediate data should prove valuable to a supervisor in evaluating the validity of the data for use in decision making tasks during emergencies.

Based on the information obtained during our audit of General Electric's SPDS, the staff confirms that means are provided in the SPDS design to assure that the data displayed are validated.

F. HUMAN FACTORS PROGRAM

The staff also evaluated General Electric's SPDS design for a commitment to a Human Factors Program in the development of the SPDS. During our Design Verification Audit, we learned that General Electric had hired ANACAPA Sciences, Inc., to conduct a human factors review of selected SPDS display formats. The staff evaluated a report titled "Human Factors and Performance Evaluations of the Emergency Response Information System (ERIS)," July 10, 1984, ANACAPA Sciences, Inc. We found the report to be comprehensive in its scope of review, and in the recording of review results, both positive and negative, and in

the recommendations made as a result of the evaluation. We evaluated several of the recommendations and noted that many had been already implemented into the design.

The staff evaluated the design for consistent use of colors in the various display formats. This evaluation effort focused upon the RPV CONTROL -- NR/TEMP display format and the CONTAINMENT CONTROL -- NR display format. The initial explanation of how color was used to highlight and code information in these display formats left the staff confused. The staff was concerned that a confused, complicated application of color would result in operator errors.

To clarify the issue, the staff requested an explanation of color codes in terms of the individual data sets for the selected display formats. After considerable explanation by General Electric, it appeared that a logical, consistent application of color had been made. To confirm this judgment, the staff requested that General Electric document how color is used to code information and submit the document to the staff for confirmatory review. General Electric responded (Ref. 6) by letter and provided a definition of how information was color coded. The staff reviewed the contents of the letter and confirms that it agrees with the information provided at the audit.

During the staff audit of the SPDS design, we evaluated some of the display formats within the system. For the most part, we found the majority of the display formats to be uncluttered and easy to read and comprehend. However, we found two display formats to be very dense with information. These display formats were the RPV CONTROL -- NR/TEMP display format and the CONTAINMENT CONTROL -- NR display format. Relative to other display formats, in the system, these display formats were very dense with data and information.

The structure of the data within each display format was the same. In the right-hand portion of the display screen, trend plots of process variables were presented whereas in the left-hand portion of the display screen, text was used to present information on several plant systems. The information on a system was grouped into boxes and the the box for the system was labeled. As data for several systems were presented, the dense concentration of text, boxes, and labels give the appearance of clutter.

General Electric stated that the data on plant systems were not a part of the SPDS requirements. The staff acknowledged this fact, however, we noted that the information on the status of these systems did impact the process variables displayed. This represents good integration of related data and would provide

useful to the operator in evaluating the performance of the emergency core cooling systems in the mitigation of an accident, if the data were not cluttered. Our concern is that in times of stress, the clutter will prove a detriment to operator performance through increased search time and errors in the location, comprehension, and use of data within the format.

NUREG-0737, Supplement 1 requires the coordination of the initiatives to achieve an integrated emergency response capability within a nuclear power plant. One of the initiatives is the Detailed Control Room Design Review (DCRDR). The object of the control room design review is to improve the ability of nuclear power plant control room operators to prevent accidents or cope with accidents if they occur by improving the information provided to them. This object is not met when an SPDS which contains display formats which are cluttered is integrated into the control room. Thus, the staff request thats General Electric provide information which clearly demonstrates that the RPV CONTROL -- NR/TEMP display format and the CONTAINMENT CONTROL -- NR display format will not result in operator errors due to clutter or redesign the display formats to eliminate the clutter.

Based on the information obtained during our audit of General Electric's SPDS, the staff confirms that General Electric did

commit to a Human Factors Program in the design of the SPDS. A large majority of the display formats appeared to be well designed, easy to read and comprehend. However, we noted that two display formats were very dense with information and our review of these display formats is incomplete. We are requesting additional information on these formats and we will report on our review of this information in a supplement to this SER.

G. ELECTRICAL AND ELECTRONIC ISOLATION

NUREG-0737, Supplement 1 requires that the SPDS be suitably isolated from electrical or electronic interference with equipment and sensors that are in use for safety systems. The staff audited the General Electric design for the adequacy of the isolators (fiber optics) between the safety systems and the SPDS. The fiber optics serve as the interface between Class 1E inputs and the data multiplexer within the ERIS. The fiber optics cable used in the system varies in length from two to 5000 feet. This unique isolator possesses inherent characteristics that cannot be found in other isolators within nuclear power plants. For example, one of the tests that must be performed to qualify an isolator is the application of maximum credible fault (voltage, current) to the output of the device to verify that the fault does not propagate or degrade

the input (Class 1E) side. This postulated failure does not affect fiber optic cable because optical fibers are totally dielectric (i.e., the electrical energy resulting from the fault will not propagate through the fiber). Another characteristic of the fiber optic cable is its non-susceptibility to the coupling of cross-talk and electromagnetic interference (EMI). Ground loop problems, inherent to copper cables, are also eliminated.

As part of the qualification program for the isolators, General Electric performed environmental (IEEE-323-1974) and seismic (IEEE-384-1975) qualification tests. Based on our audit of the above information, the staff concludes that the fiber optic cables are qualified isolation devices and are acceptable for interfacing the ERIS/SPDS with safety systems.

H. SYSTEM RELIABILITY

NUREG-0696 notes that the SPDS design should have an unavailability goal of 0.01 while the plant is operating at power. The analysis on availability for the General Electric ERIS hardware resulted in an expected value of 98.6 percent. The major contributors to the system unavailability were the six non-redundant components (i.e., the dual - port disk, two synchronous inter-faces, an output multiplexer, and two unibus

switches). These components contributed 59 to 99 percent of the system unavailability.

The Mean Time to Repair (MTTR) ranged from 1.0 to 6.0 hours for plug-in component replacement and 1.0 to 24 hours for equipment repair. A fault- tree analysis was performed for the vital portions of the ERIS and numerical values were assigned for the Mean Time Between Failures (MTBF). Based on this information, an unavailability calculation was performed using the ratio of MTTR/(MTTR + MTBF). The staff finds this methodology an acceptable approach and concludes that the 98.6 percent availability is acceptable for the SPDS.

With regard to plant specific SPDS reliability, the following items were not considered in the availability analysis: sensor availability, power supply configuration, and routine maintenance. The staff requires that these items be identified by General Electric as interface requirements. The staff will audit the plant-specific implementation program for utilities that reference the General Electric GESSAR II SPDS to verify that the interface requirements are implemented in order to maintain the system availability of 98.6 percent.

In addition, we request that General Electric evaluate the performance of the system up to and including the validation

tests. All failures in the system which occurred during these performance tests should be analyzed with regard to impact upon the reliability analysis, and results discussed.

Our concern is that unforeseen failures experienced during the test of the system may destroy the assumptions used in the reliability analysis and significantly reduce the predicted availability. We request that General Electric report to the staff on the method and results of this analysis. The staff will review the method and results of the analysis and report on our evaluation in a supplement to this SER.

IV. CONCLUSION

The NRC staff reviewed the design of General Electric's GESSAR II Safety Parameter Display System to confirm the adequacy of the variables selected to be displayed to monitor critical safety functions, to confirm that means are provided to assure that the data displayed are valid, to confirm that the licensee has committed to a Human Factors Program to ensure that the displayed information can be readily perceived and comprehended so as not to mislead the operator, and to confirm that the SPDS is suitably isolated.

Based on its review, the staff confirms that:

- Means are provided in the SPDS design to assure that the data displayed are valid.

- An appropriate commitment to a Human Factors Program was made in the design of the SPDS. However, the staff's review of the dense display formats in the system is incomplete, and we request additional information from General Electric to complete the review.

- The SPDS will be suitably isolated from electrical and electronic interference with equipment and sensors that are used in safety systems.

However:

- The staff finds that the variables selected for the GE SPDS would be acceptable with the addition of radiation monitors to identify the status of the Radioactivity Control Safety Function.

- We request that General Electric analyze and evaluate the performance of the system up to and including the validation tests. Our concern is that unforeseen failures experienced during the test of the system may invalidate the assumption used in the reliability analysis. We request that General Electric report to the staff on the method and results of the analysis.

- The staff concludes a design validation audit is not necessary provided the following reports are submitted for staff review:

    - A sample of test procedures with acceptance criteria for test runs,

    - the Validation Test Report,

    - a summary of the problems found during the tests and how they were resolved.

The staff's review of General Electric's GESSAR II SPDS is incomplete. We will report on the staff's evaluation of the completed design in a supplement to this SER.

V. REFERENCES

1. NEDE-30283-P, "Licensing Topical Report For the General Electric Emergency Response Information System, General Electric Company Proprietary Information," November 1983.

2. Memorandum for Cecil O. Thomas, NRC, from Dino C. Scaletti, NRC, Subject, "Meeting Summary, GESSAR II SPDS," June 11, 1984.

3. Memorandum for Cecil O. Thomas, NRC, from Voss A. Moore, NRC, Subject, "Design Verification Audit Report For The General Electric Safety Parameter Display System," to be published.

4. NSAC-39, "Verification and Validation for Safety Parameter Display Systems," December 1981, Nuclear Safety Analysis Center, Electric Power Research Institute.

5. Letter, T. J. Dente (BWR Owners' Group) to D. G. Eisenhut (NRC), dated December 22, 1982, transmitting "BWR Emergency Procedure Guidelines," Revision 3 (dated December 8, 1982).

6. Letter to U. S. Nuclear Regulatory Commission from D. Bitter, General Electric, Subject, "ERIS Color Coding," August 14, 1984.

7. Letter to M. McCoy, NRC, from D. B. Bitter, General Electric, Subject, "SCRAM Event Status Target/Source Range Monitor Inputs," August 29, 1984 (Ref. MFN-131-84).

ATTACHMENT

TABLE I

SPDS VARIABLES

GESSAR II

Critical Safety Function	Variables
Reactivity Control	APRMS Scram Status (All rods in)
Reactor Core Cooling and Heat Removal	Reactor Vessel Water Level Reactor Vessel Water Temperature Trend Plant
Reactor Coolant System Integrity	Reactor Vessel Pressure Reactor Vessel Isolation Status Drywell/Containment Pressure
Containment Integrity	Containment/Drywell Temperature Drywell Pressure Suppression Pool Water Level Suppression Pool Water Temperature Suppression Pool Makeup System Status Containment Isolation Status
Radioactivity Control	RPV Control Display* Containment Control Display*

*Refers to second level displays on ERIS associated with Emergency Procedure Guidelines for RPV Control and Containment Control